# Abbreviated Table of Contents

About This Manual ........................................................................................................................................................................... xxxiii

## Part 1 Overview

Chapter 1 Network Interfaces and Class of Service Overview ........................................... 3

Chapter 2 Interfaces and Class of Service Configuration Statements ................................................................. 5

## Part 2 Router Interfaces

Chapter 3 Interfaces Overview ................................................................................................................................. 19

Chapter 4 Interfaces Configuration Statements ........................................................................................................... 29

Chapter 5 Configure Physical Interface Properties ................................................................. 39

Chapter 6 Configure Logical Interface Properties ........................................................................................................... 67

Chapter 7 Configure Protocol Family and Address Interface Properties ................................................................. 77
Chapter 8
Configure Circuit and Translational Cross-Connects .......................... 99

Chapter 9
Trace Interface Operations ........................................................................ 107

Part 3
Interface Types

Chapter 10
Configure Adaptive Services Interfaces ............................................. 111

Chapter 11
Configure ATM 1 and ATM 2 Interfaces ............................................... 117

Chapter 12
Channelized Interfaces Overview ........................................................... 163

Chapter 13
Configure Channelized E1 Interfaces .................................................. 173

Chapter 14
Configure Channelized OC-12 Interfaces ............................................. 183

Chapter 15
Configure Channelized STM-1 Interfaces ............................................ 205

Chapter 16
Configure Channelized T3 Interfaces ................................................... 221

Chapter 17
Configure Discard Interfaces ................................................................. 241

Chapter 18
Configure E1 Interfaces .......................................................................... 243

Chapter 19
Configure E3 Interfaces .......................................................................... 251
Chapter 20 Configure Encryption Interfaces .......................................................... 257
Chapter 21 Configure Ethernet Interfaces ............................................................... 263
Chapter 22 Configure Frame Relay ........................................................................ 303
Chapter 23 Configure the Loopback Interface ...................................................... 313
Chapter 24 Configure Monitoring Services Interfaces .......................................... 315
Chapter 25 Configure Multilink and Link Services Interfaces .............................. 319
Chapter 26 Configure Serial Interfaces .................................................................. 345
Chapter 27 Configure SONET/SDH Interfaces ..................................................... 359
Chapter 28 Configure T1 Interfaces ........................................................................ 387
Chapter 29 Configure T3 Interfaces ........................................................................ 395
Chapter 30 Configure Tunnel Interfaces .................................................................. 407
Chapter 31 Summary of Interface Configuration Statements ............................. 417
# Table of Contents

## About This Manual

- Objectives ........................................................................................................ xxxiii
- Audience ........................................................................................................... xxxiv
- Document Organization ................................................................................... xxxiv
- Part Organization ............................................................................................. xxxvi
- Using the Indexes ............................................................................................ xxxvii
- Documentation Conventions ............................................................................ xxxviii
  - General Conventions .................................................................................... xxxviii
  - Conventions for Software Commands and Statements ................................. xxxviii
- List of Technical Publications ........................................................................... xl
- Documentation Feedback .................................................................................. xli
- How to Request Support .................................................................................... xli

## Part 1 Overview

### Chapter 1

Network Interfaces and Class of Service Overview ........................................... 3

### Chapter 2

Interfaces and Class of Service Configuration Statements ................................. 5

- [edit class-of-service] Hierarchy Level ........................................................... 5
- [edit interfaces] Hierarchy Level .................................................................. 7
- [edit protocols connections] Hierarchy Level .............................................. 15
- [edit protocols vrrp] Hierarchy Level ............................................................ 16
Part 2
Router Interfaces

Chapter 3
Interfaces Overview

Types of Interfaces
Permanent Interfaces
Transient Interfaces
Services Interfaces
Interface Descriptors
Interface Naming
Physical Part of an Interface Name
Logical Part of an Interface Name
Separators in an Interface Name
Channel Part of an Interface Name
Examples: Interface Naming
How Interface Configurations Are Displayed
Interface and Router Clock Sources

Chapter 4
Interfaces Configuration Statements

Complete Interfaces Configuration Statements
Minimum Interface Configuration

Chapter 5
Configure Physical Interface Properties

Configure Aggregated Interfaces
Add an Interface Description to the Configuration
Example: Add an Interface Description to the Configuration
Configure the Link Characteristics
Configure the Media MTU
Configure Interface Encapsulation
Configure the Encapsulation on a Physical Interface
Encapsulation Capabilities
Example: Configure the Encapsulation on a Physical Interface
Configure PPP Challenge Handshake Authentication Protocol
Assign an Access Profile to an Interface
Configure the Local Name
Configure Passive Mode
Example: Configure PPP Challenge Handshake Authentication Protocol
Configure the Interface Speed
Configure Keepalives
Configure the Clock Source
Configure the Router as a DCE
Configure Receive and Transmit Leaky Bucket Properties
## Table of Contents

<table>
<thead>
<tr>
<th>Chapter 6</th>
<th>Configure Logical Interface Properties</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Configure Logical Interface Number</td>
</tr>
<tr>
<td></td>
<td>Add a Logical Unit Description to the Configuration</td>
</tr>
<tr>
<td></td>
<td>Configure a Point-to-Point Connection</td>
</tr>
<tr>
<td></td>
<td>Configure a Multipoint Connection</td>
</tr>
<tr>
<td></td>
<td>Configure Accounting for the Logical Interface</td>
</tr>
<tr>
<td></td>
<td>Apply an Accounting Profile to the Logical Interface</td>
</tr>
<tr>
<td></td>
<td>Example: Apply an Accounting Profile to the Logical Interface</td>
</tr>
<tr>
<td></td>
<td>Configure the Interface Bandwidth</td>
</tr>
<tr>
<td></td>
<td>Enable or Disable SNMP Notifications on Logical Interfaces</td>
</tr>
<tr>
<td></td>
<td>Configure Interface Encapsulation</td>
</tr>
<tr>
<td></td>
<td>Configure the Encapsulation on a Logical Interface</td>
</tr>
<tr>
<td></td>
<td>Disable a Logical Interface</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 7</th>
<th>Configure Protocol Family and Address Interface Properties</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Configure the Protocol Family</td>
</tr>
<tr>
<td></td>
<td>IPv6 Introduction</td>
</tr>
<tr>
<td></td>
<td>IPv4-to-IPv6 Transition</td>
</tr>
<tr>
<td></td>
<td>Configure the Interface Address</td>
</tr>
<tr>
<td></td>
<td>Configure the IPv6 Address on an Interface</td>
</tr>
<tr>
<td></td>
<td>Configure an Unnumbered Interface</td>
</tr>
<tr>
<td></td>
<td>Set the Protocol MTU</td>
</tr>
<tr>
<td></td>
<td>Disable the Removal of Address and Control Bytes</td>
</tr>
<tr>
<td></td>
<td>Disable the Sending of Asynchronous Notification Upon Link Failure</td>
</tr>
<tr>
<td></td>
<td>Disable the Sending of Redirect Messages on an Interface</td>
</tr>
<tr>
<td></td>
<td>Configure Default, Primary, and Preferred Addresses and Interfaces</td>
</tr>
<tr>
<td></td>
<td>Configure the Primary Interface for the Router</td>
</tr>
<tr>
<td></td>
<td>Configure the Primary Address for an Interface</td>
</tr>
<tr>
<td></td>
<td>Configure the Preferred Address for an Interface</td>
</tr>
<tr>
<td></td>
<td>Apply Policers</td>
</tr>
<tr>
<td></td>
<td>Apply a Filter to an Interface</td>
</tr>
<tr>
<td></td>
<td>Define Interface Groups in Firewall Filters</td>
</tr>
<tr>
<td></td>
<td>Apply an Accounting Profile to the Physical Interface</td>
</tr>
<tr>
<td></td>
<td>Example: Apply an Accounting Profile to the Physical Interface</td>
</tr>
<tr>
<td></td>
<td>Configure BERT Properties</td>
</tr>
<tr>
<td></td>
<td>Trace Operations of an Individual Router Interface</td>
</tr>
<tr>
<td></td>
<td>Damp Interface Transitions</td>
</tr>
<tr>
<td></td>
<td>Configure Multiservice Physical Interface Properties</td>
</tr>
<tr>
<td></td>
<td>Enable or Disable SNMP Notifications on Physical Interfaces</td>
</tr>
<tr>
<td></td>
<td>Disable a Physical Interface</td>
</tr>
<tr>
<td></td>
<td>Example: Disable a Physical Interface</td>
</tr>
<tr>
<td></td>
<td>Configure Accounting for the Physical Interface</td>
</tr>
<tr>
<td></td>
<td>Apply an Accounting Profile to the Physical Interface</td>
</tr>
<tr>
<td></td>
<td>Example: Apply an Accounting Profile to the Physical Interface</td>
</tr>
<tr>
<td></td>
<td>Configure Accounting for the Physical Interface</td>
</tr>
<tr>
<td></td>
<td>Apply an Accounting Profile to the Physical Interface</td>
</tr>
<tr>
<td></td>
<td>Example: Apply an Accounting Profile to the Physical Interface</td>
</tr>
<tr>
<td></td>
<td>Configure BERT Properties</td>
</tr>
<tr>
<td></td>
<td>Trace Operations of an Individual Router Interface</td>
</tr>
<tr>
<td></td>
<td>Damp Interface Transitions</td>
</tr>
<tr>
<td></td>
<td>Configure Multiservice Physical Interface Properties</td>
</tr>
<tr>
<td></td>
<td>Enable or Disable SNMP Notifications on Physical Interfaces</td>
</tr>
<tr>
<td></td>
<td>Disable a Physical Interface</td>
</tr>
<tr>
<td></td>
<td>Example: Disable a Physical Interface</td>
</tr>
</tbody>
</table>
Chapter 11 Configure ATM 1 and ATM 2 Interfaces ........................................... 117

ATM 1 Physical and Logical Interface Properties ........................................... 118
ATM 2 Physical and Logical Interface Properties ........................................... 120
Configure ATM 1 and ATM 2 Physical Interface Properties ......................... 125
  Configure Communication with Directly Attached ATM 1 and ATM 2 Switches ................................................................. 126
  Configure the ATM 1 and ATM 2 PIC Type ........................................... 126
  Example: Configure the ATM 1 and ATM 2 PIC Type ......................... 127
  Configure ATM 1 and ATM 2 Cell-Relay Promiscuous Mode ................. 127
    Example: Configure ATM 1 and ATM 2 Cell-Relay Promiscuous Mode .... 128
  Configure the Maximum Number of ATM 1 VCs on a VP ..................... 129
  Configure ATM 2 Layer 2 Circuit Transport Mode ................................ 130
    Example: Configure ATM 2 Layer 2 Circuit Transport Mode .............. 131
  Configure ATM 2 Layer 2 Circuit Cell-Relay Promiscuous Mode ............ 132
    Example: Configure ATM 2 Layer 2 Circuit Cell-Relay Promiscuous Mode 132
  Configure ATM 2 Layer 2 Circuit Cell-Relay Cell Maximum .................. 133
  Configure the ATM 2 OAM F4 Cell Flows .......................................... 133
  Define Virtual Path Tunnels on ATM 2 Interfaces ................................ 134
  Configure ATM 1 and ATM 2 Logical Interface Properties ...................... 135
  Configure a Point-to-Point ATM 1 or ATM 2 Connection ....................... 136
  Configure a Point-to-Multipoint ATM 1 or ATM 2 Connection ................. 136
  Configure a Multicast-Capable ATM 1 or ATM 2 Connection .................. 137
  Configure Inverse ATM 1 or ATM 2 ARP ........................................... 137
  Define the ATM 1 and ATM 2 Traffic-Shaping Profile ............................ 137
    Configure ATM 1 and ATM 2 CBR ............................................... 139
    Configure ATM 2 Real-Time VBR ............................................... 139
    Configure ATM 1 and ATM 2 VBR ............................................. 139
    Specify ATM 1 Shaping Values .................................................. 140
      Example: Specify ATM 1 Shaping Values ................................... 141
    Specify ATM 2 Shaping Values .................................................. 142
    Configure the ATM 1 Queue Length ............................................. 142
    Configure the ATM 2 EPD Threshold ........................................... 143
      Example: Configure the ATM 2 EPD Threshold ............................... 144
    Configure the ATM 2 Transmission Weight .................................... 144
    Define the ATM 1 and ATM 2 OAM F5 Loopback Cell Period ............... 144
    Configure the ATM 1 and ATM 2 OAM F5 Loopback Cell Threshold ......... 145
  Configure ATM 1 and ATM 2 Interface Encapsulation ............................ 146
    Configure an ATM 1 Cell-Relay Circuit ....................................... 148
      Examples: Configure an ATM 1 Cell-Relay Circuit ....................... 148
    Configure PPP over ATM 2 Encapsulation .................................... 150
      Example: Configure PPP over ATM 2 Encapsulation ....................... 150
    Configure E3 and T3 Parameters on ATM 1 Interfaces ....................... 153
    Configure SONET/SDH Parameters on ATM 1 and ATM 2 Interfaces ........... 154
    Configure ATM 2 VC Tunnel CoS Components .................................. 155
      Example: Configure ATM 2 VC Tunnel CoS Components ................... 158
    Examples: Configure ATM 1 Interfaces ....................................... 158
    Examples: Configure ATM 2 Interfaces ....................................... 161
# Channelized Interfaces Overview

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Channelized Interface Capabilities</td>
<td>164</td>
</tr>
<tr>
<td>Data Link Connection Identifiers on Channelized Interfaces</td>
<td>166</td>
</tr>
<tr>
<td>Clock Sources on Channelized Interfaces</td>
<td>166</td>
</tr>
<tr>
<td>Channelized QPP Interface Properties</td>
<td>169</td>
</tr>
<tr>
<td>Structure of Channelized PICs with QPP</td>
<td>170</td>
</tr>
</tbody>
</table>

## Chapter 13
Configure Channelized E1 Interfaces ...........................................173

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure Channelized E1 QPP Interfaces</td>
<td>173</td>
</tr>
<tr>
<td>Configure E1 QPP Interfaces</td>
<td>173</td>
</tr>
<tr>
<td>Configure Fractional E1 QPP Interfaces</td>
<td>174</td>
</tr>
<tr>
<td>Example: Configure Fractional E1 QPP Interfaces</td>
<td>174</td>
</tr>
<tr>
<td>Configure an NxDS-0 QPP Interface</td>
<td>174</td>
</tr>
<tr>
<td>Example: Configure an NxDS-0 QPP Interface</td>
<td>175</td>
</tr>
<tr>
<td>Configure Channelized E1 QPP Interface Properties</td>
<td>175</td>
</tr>
<tr>
<td>Specify Options at the Channelized E1 QPP Interface Level</td>
<td>175</td>
</tr>
<tr>
<td>Specify Options at the E1 QPP Interface Level</td>
<td>176</td>
</tr>
<tr>
<td>Specify Options at the NxDS-0 QPP Interface Level</td>
<td>177</td>
</tr>
<tr>
<td>Configure Channelized E1 Interfaces</td>
<td>178</td>
</tr>
<tr>
<td>Example: Configure Channelized E1 Interfaces</td>
<td>181</td>
</tr>
<tr>
<td>Example: Configure Channelized E1 QPP Interfaces</td>
<td>182</td>
</tr>
</tbody>
</table>

## Chapter 14
Configure Channelized OC-12 Interfaces .......................................183

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure Channelized OC-12 QPP Interfaces</td>
<td>184</td>
</tr>
<tr>
<td>Configure an OC-12 QPP Interface</td>
<td>185</td>
</tr>
<tr>
<td>Configure T3 QPP Interfaces</td>
<td>185</td>
</tr>
<tr>
<td>Example: Configure T3 QPP Interfaces</td>
<td>186</td>
</tr>
<tr>
<td>Configure OC-3 QPP Interfaces</td>
<td>186</td>
</tr>
<tr>
<td>Example: Configure OC-3 QPP Interfaces</td>
<td>187</td>
</tr>
<tr>
<td>Configure T1 QPP Interfaces</td>
<td>187</td>
</tr>
<tr>
<td>Example: Configure T1 QPP Interfaces</td>
<td>188</td>
</tr>
<tr>
<td>Configure NxDS-0 QPP Channels</td>
<td>189</td>
</tr>
<tr>
<td>Example: Configure an NxDS-0 QPP Interface</td>
<td>190</td>
</tr>
<tr>
<td>Configure Fractional T1 QPP Interfaces</td>
<td>191</td>
</tr>
<tr>
<td>Example: Configure Fractional T1 QPP Interfaces</td>
<td>191</td>
</tr>
<tr>
<td>Configure Channelized OC-12 QPP Interface Properties</td>
<td>192</td>
</tr>
<tr>
<td>Specify Options at the Channelized OC-12 QPP Level</td>
<td>192</td>
</tr>
<tr>
<td>Specify Options at the Channelized OC-1 QPP Level</td>
<td>193</td>
</tr>
<tr>
<td>Specify Options at the Channelized T3 QPP Level</td>
<td>194</td>
</tr>
<tr>
<td>Specify Options at the Channelized T1 QPP Level</td>
<td>194</td>
</tr>
<tr>
<td>Specify Options at the T3 QPP Interface Level</td>
<td>195</td>
</tr>
<tr>
<td>Specify Options at the T1 QPP Interface Level</td>
<td>196</td>
</tr>
<tr>
<td>Specify Options at the NxDS-0 QPP Interface Level</td>
<td>197</td>
</tr>
</tbody>
</table>
Configure Channelized OC-12 Interfaces ............................................................198
Example: Configure Channelized OC-12 QPP Interfaces ......................................199
Example: Configure Channelized OC-12 Interfaces .............................................203

Chapter 15

Configure Channelized STM-1 Interfaces .....................................................205

Configure Channelized STM-1 QPP Interfaces ...................................................205
  Configure an STM-1 QPP Interface ................................................................206
  Configure E1 QPP Interfaces ........................................................................206
  Example: Configure E1 QPP Interfaces ..........................................................207
  Configure Fractional E1 QPP Interfaces .........................................................207
  Example: Configure Fractional E1 QPP Interfaces ........................................208
  Configure an NxDS-0 QPP Interface ..............................................................208
  Example: Configure an NxDS-0 QPP Interface .............................................209
  Configure Channelized STM-1 QPP Interface Properties ..................................209
  Specify Options at the Channelized STM-1 QPP Level .....................................210
  Specify Options at the Channelized AU-4 QPP Level .....................................211
  Configure Virtual Tributary Mapping of
    Channelized STM-1 QPP Interface ................................................................211
  Specify Options at the E1 QPP Interface Level ..............................................212
  Specify Options at the NxDS-0 QPP Interface Level .......................................213
  Example: Configure Channelized STM-1 QPP Interfaces ..................................214

Configure Channelized STM-1 Interfaces ..........................................................215
  Configure Channelized STM-1 Interface Properties .......................................216
  Configure Virtual Tributary Mapping of
    Channelized STM-1 Interface ....................................................................217
  Example: Configure Channelized STM-1 Interfaces .......................................219

Chapter 16

Configure Channelized T3 Interfaces ............................................................221

Configure Channelized T3 QPP Interfaces .......................................................221
  Configure T3 QPP Interfaces .........................................................................221
  Configure T1 QPP Interfaces .........................................................................222
  Example: Configure T1 QPP Interfaces ..........................................................222
  Configure Fractional T1 QPP Interfaces ........................................................223
  Example: Configure Fractional T1 QPP Interfaces .........................................223
  Configure an NxDS-0 QPP Interface ..............................................................223
  Example: Configure an NxDS-0 QPP Interface .............................................224
  Configure Channelized T3 QPP Interface Properties .......................................225
  Specify Options at the Channelized T3 QPP Level ........................................225
  Specify Options at the Channelized T1 QPP Level ........................................226
  Specify Options at the T3 QPP Interface Level ..............................................226
  Specify Options at the T1 QPP Interface Level ..............................................227
  Specify Options at the NxDS-0 QPP Interface Level .....................................228
  Configure Channelized DS-3 to DS-0 Interfaces ..........................................229
  Configure Channelized DS-3 to DS-1 Interfaces ..........................................232
  Example: Configure Channelized T3 QPP Interfaces .....................................234
  Examples: Configure Channelized DS-3 to DS-0 Interfaces ........................235
  Examples: Configure Channelized DS-3 to DS-1 Interfaces ........................238
Chapter 17 Configure Discard Interfaces ................................................................. 241

Chapter 18 Configure E1 Interfaces ............................................................................ 243

- Configure E1 BERT Properties ................................................................. 244
- Configure the E1 Frame Checksum ............................................................. 245
- Configure E1 Framing ............................................................................. 246
- Configure the E1 Idle Cycle Flag ................................................................. 246
- Configure E1 Data Inversion ..................................................................... 246
- Configure E1 Loopback Capability .............................................................. 247
  Example: Configure E1 Loopback Capability ............................................. 248
- Configure E1 Start End Flags ..................................................................... 248
- Configure Fractional E1 Time Slots ............................................................. 249

Chapter 19 Configure E3 Interfaces ............................................................................ 251

- Configure E3 BERT Properties ................................................................. 252
- Configure the E3 CSU Compatibility Mode .................................................. 253
- Configure the E3 Frame Checksum ............................................................. 253
- Configure the E3 Idle Cycle Flag ................................................................. 254
- Configure E3 Loopback Capability .............................................................. 254
  Example: Configure E3 Loopback Capability ............................................. 255
- Configure E3 HDLC Payload Scrambling .................................................... 255
- Configure the E3 Start End Flags ................................................................. 256

Chapter 20 Configure Encryption Interfaces .......................................................... 257

- Configure an Encryption Interface ............................................................ 258
  Specify the Security Association Name ....................................................... 258
  Example: Configure an Encryption Interface .......................................... 259
- Configure ES PIC Redundancy ................................................................. 259
  Example: Configure ES PIC Redundancy ................................................... 259
- Configure IPSec Tunnel Redundancy ......................................................... 260
# Table of Contents

## Chapter 21

Configure Ethernet Interfaces ................................................................. 263

Configure Ethernet Physical Interface Properties ................................. 264
Configure Ethernet Link Aggregation ....................................................... 266
Configure Aggregated Ethernet Link Speed .......................................... 267
Configure Aggregated Ethernet Minimum Links ................................. 267
Configure Gigabit Ethernet QPP Interfaces ............................................ 267
   Example: Configure Gigabit Ethernet QPP MAC Address Filtering ........ 270
   Example: Configure Gigabit Ethernet QPP VLAN Tags ...................... 273
Configure Gigabit Ethernet QPP MAC Address Filtering ....................... 279
Configure Ethernet Loopback Capability .............................................. 280
Configure Flow Control .................................................................. 280
Configure the Link Characteristics ...................................................... 281
Configure Gratuitous ARP ................................................................. 281
Configure the Interface Speed .............................................................. 282
Configure the Ingress Rate Limit .......................................................... 282
Configure 802.1Q VLANs .................................................................. 282
   Enable VLAN Tagging ............................................................... 283
   Configure VLAN CCC or VPLS Encapsulation .............................. 284
      Example: Configure VLAN CCC or VPLS Encapsulation .......... 284
   Configure Extended VLAN CCC or VLAN VPLS Encapsulation ......... 285
      Example: Configure Extended VLAN CCC or VLAN VPLS Encapsulation 285
   Configure 802.1Q VLANs ............................................................ 282
Configure 802.1Q VLANs .................................................................. 282
   Enable VLAN Tagging ............................................................... 283
   Configure VLAN CCC or VPLS Encapsulation .............................. 284
      Example: Configure VLAN CCC or VPLS Encapsulation .......... 284
   Configure Extended VLAN CCC or VLAN VPLS Encapsulation ......... 285
      Example: Configure Extended VLAN CCC or VLAN VPLS Encapsulation 285
   Configure 802.1Q VLANs ............................................................ 282
Configure TCC and Layer 2.5 Switching .............................................. 286
   Configure Extended VLAN TCC Encapsulation ......................... 286
   Configure an Ethernet TCC or Extended VLAN TCC ................... 287
      Example: Configure an Ethernet TCC or Extended VLAN TCC ... 287
Configure Static ARP Table Entries ...................................................... 289
   Example: Configure Static ARP Table Entries ......................... 289
Configure VRRP .............................................................................. 290
   Configure Basic VRRP Support .................................................... 291
   Configure VRRP Authentication .................................................... 292
   Configure the Advertisement Interval for the VRRP Master Router .... 293
   Configure a Backup Router to Preempt the Master Router ............... 293
   Accept Packets Destined for the Virtual IP Address ....................... 294
   Configure a Logical Interface to Be Tracked .................................. 295
   Trace VRRP Operations .............................................................. 295
   Example: Configure VRRP ......................................................... 296
Configure the Management Ethernet Interface ..................................... 298
   Configure the MAC Address on the Management Ethernet Interface . 298
   Configure the Internal Ethernet Interface ...................................... 299
   Configure Aggregated Ethernet Interfaces .................................... 299
   Example: Configure Fast Ethernet Interfaces ............................. 301
   Example: Configure Gigabit Ethernet Interfaces ......................... 301
   Example: Configure Aggregated Ethernet Interfaces ..................... 302
Chapter 22
Configure Frame Relay ................................................................. 303
  Configure Frame Relay Interface Encapsulation ...................... 304
  Configure the Frame Relay Encapsulation on a Physical Interface ... 304
  Example: Configure the Encapsulation on a Physical Interface .... 304
  Configure the Frame Relay Encapsulation on a Logical Interface ... 305
  Configure Frame Relay Control Bit Translation ......................... 305
  Configure the Media MTU ........................................................ 306
  Set the Protocol MTU ............................................................. 306
  Configure Frame Relay Keepalives .......................................... 307
  Configure Tunable Keepalives for Frame Relay LMI .................. 307
  Configure Inverse Frame Relay ARP ....................................... 308
  Configure the Router as a DCE .............................................. 309
  Configure Frame Relay DLCIs ............................................... 309
    Configure a Point-to-Point Frame Relay Connection ................ 309
    Configure a Point-to-Multipoint Frame Relay Connection ......... 310
    Configure a Multicast-Capable Frame Relay Connection .......... 311

Chapter 23
Configure the Loopback Interface ............................................. 313
  Example: Configure the Loopback Interface .......................... 314

Chapter 24
Configure Monitoring Services Interfaces ............................... 315
  Minimum Traffic Sampling Configuration ............................... 315
  Configure Flow Monitoring .................................................. 316

Chapter 25
Configure Multilink and Link Services Interfaces ..................... 319
  Configure Multilink and Link Services Logical Interface Properties ...... 321
    Default Settings for Multilink and Link Services Logical Interfaces .. 322
    Configure a Link Services Point-to-Point DLCI ..................... 322
    Configure a Link Services Multicast-Capable DLCI .................. 323
    Configure a Multilink and Link Services Drop Timeout Period ....... 323
    Configure Multilink and Link Services Logical Interface Encapsulation ... 324
    Configure a Multilink and Link Services Fragmentation Threshold .... 325
    Configure Link Services Delay-Sensitive Packet Interleaving ....... 326
    Configure Multilink and Link Services Minimum Links ............. 326
    Configure Multilink and Link Services MRRU ....................... 326
    Configure Multilink and Link Services Sequence Format ........... 327
  Configure Link Services Physical Interface Properties ............ 327
    Default Settings for Link Services Interfaces ....................... 328
    Configure Link Services Physical Interface Encapsulation ....... 328
    Configure Link Services Acknowledgment Timers .................. 329
<table>
<thead>
<tr>
<th>Chapter 26 Configure Serial Interfaces</th>
<th>345</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure the Serial Line Protocol</td>
<td>347</td>
</tr>
<tr>
<td>Serial Interface Default Settings</td>
<td>347</td>
</tr>
<tr>
<td>Serial Interface Invalid Statements</td>
<td>349</td>
</tr>
<tr>
<td>Configure the Serial Clocking Mode</td>
<td>350</td>
</tr>
<tr>
<td>Invert the Serial Interface Transmit Clock</td>
<td>351</td>
</tr>
<tr>
<td>Configure the DTE Clock Rate</td>
<td>351</td>
</tr>
<tr>
<td>Configure the Serial Signal Handling</td>
<td>352</td>
</tr>
<tr>
<td>Configure the Serial DTR Circuit</td>
<td>355</td>
</tr>
<tr>
<td>Configure Serial Signal Polarities</td>
<td>355</td>
</tr>
<tr>
<td>Configure Serial Loopback Capability</td>
<td>356</td>
</tr>
<tr>
<td>Example: Configure Serial Loopback Capability</td>
<td>357</td>
</tr>
<tr>
<td>Configure Serial Line Encoding</td>
<td>357</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 27 Configure SONET/SDH Interfaces</th>
<th>359</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure SONET/SDH Physical Interface Properties</td>
<td>360</td>
</tr>
<tr>
<td>Configure SONET Header Byte Values</td>
<td>361</td>
</tr>
<tr>
<td>Configure an Incrementing STM ID</td>
<td>362</td>
</tr>
<tr>
<td>Configure the SONET Frame Checksum</td>
<td>363</td>
</tr>
<tr>
<td>Configure SONET Loopback Capability</td>
<td>364</td>
</tr>
<tr>
<td>Example: Configure SONET Loopback Capability</td>
<td>364</td>
</tr>
<tr>
<td>Configure the SONET Path Trace Identifier</td>
<td>365</td>
</tr>
<tr>
<td>Configure SONET HDLC Payload Scrambling</td>
<td>365</td>
</tr>
<tr>
<td>Configure SONET RFC 2615 Support</td>
<td>366</td>
</tr>
<tr>
<td>Configure Virtual Tributary Mapping</td>
<td>366</td>
</tr>
<tr>
<td>Configure APS</td>
<td>367</td>
</tr>
<tr>
<td>Configure Basic APS Support</td>
<td>368</td>
</tr>
<tr>
<td>Example: Configure Basic APS Support</td>
<td>369</td>
</tr>
<tr>
<td>Configure Switching between the Working and Protect Circuits</td>
<td>370</td>
</tr>
<tr>
<td>Configure Revertive Mode</td>
<td>371</td>
</tr>
<tr>
<td>Configure APS Timers</td>
<td>371</td>
</tr>
<tr>
<td>Configure APS Load Sharing between Circuit Pairs</td>
<td>372</td>
</tr>
<tr>
<td>Example: Configure APS Load Sharing between Circuit Pairs</td>
<td>373</td>
</tr>
<tr>
<td>Configure the Media MTU</td>
<td>373</td>
</tr>
<tr>
<td>Enable Passive Monitoring</td>
<td>374</td>
</tr>
<tr>
<td>Configure the Clock Source</td>
<td>374</td>
</tr>
<tr>
<td>Configure Receive and Transmit Leaky Bucket Properties</td>
<td>375</td>
</tr>
</tbody>
</table>
Chapter 28 Configure T1 Interfaces ............................................. 387

Configure T1 BERT Properties .................................................. 388
Configure T1 Buildout .............................................................. 389
Configure T1 Byte Encoding ...................................................... 389
Configure T1 Data Inversion ...................................................... 390
Configure T1 Frame Checksum ................................................ 390
Configure T1 Remote Loopback Response .............................. 390
Configure T1 Framing ............................................................... 391
Configure T1 Line Encoding ..................................................... 391
Configure T1 Loopback Capability ........................................... 392
Configure the T1 Idle Cycle Flag ............................................. 393
Configure T1 Start End Flags .................................................. 394
Configure Fractional T1 Time Slots ........................................ 394

Chapter 29 Configure T3 Interfaces ........................................... 395

Configure T3 BERT Properties .................................................. 396
Disable T3 C-Bit Parity Mode .................................................. 397
Configure the T3 CSU Compatibility Mode .............................. 398
Configure the T3 Frame Checksum ........................................ 399
Configure the T3 FEAC Response ............................................. 399
Configure the T3 Idle Cycle Flag ............................................. 400
Configure the T3 Line Buildout .............................................. 400
Configure the Channelized T3 Loop Timing ............................ 401
Configure T3 Loopback Capability .......................................... 401
Configure T3 HDLC Payload Scrambling ............................... 403
Configure the T3 Start End Flags ........................................... 403
Examples: Configure T3 Interfaces ......................................... 404
Chapter 30

Configure Tunnel Interfaces ................................................................. 407

Configure a Unicast Tunnel ................................................................. 408
Configure a Multicast Tunnel ............................................................... 409
Configure a Tunnel Interface for Routing Table Lookup .................... 409
Configure a Tunnel Interface for VRF Table Lookup ........................... 410
Configure PIM Tunnels ...................................................................... 411
Configure an IPv6-over-IPv4 Tunnel ................................................. 412
Example: Configure Unicast Tunnels ................................................. 412
Example: Configure a Virtual Loopback Tunnel Interface for VRF Table Lookup ......................................................... 414
Example: Configure an IPv6-over-IPv4 Tunnel ................................. 415

Chapter 31

Summary of Interface Configuration Statements ............................... 417

802.3ad .............................................................................................. 417
accept-data .......................................................................................... 418
accept-source-mac ............................................................................. 418
access-profile ..................................................................................... 419
accounting .......................................................................................... 419
accounting-profile ............................................................................. 420
acknowledge-retries ............................................................................ 420
acknowledge-timer .............................................................................. 421
action-red-differential-delay ............................................................... 421
address .............................................................................................. 422
advertise-interval ............................................................................ 423
advertise-interval (APS) ..................................................................... 423
advertise-interval (VRRP) ................................................................. 423
aggregate .......................................................................................... 424
aggregate (Gigabit Ethernet CoS Policer) ........................................... 424
aggregate (SONET/SDH) ................................................................. 424
aggregated-ether-options ................................................................. 425
aggregated-sonet-options ................................................................. 425
allow-any-vci .................................................................................... 425
aps ....................................................................................................... 426
arp ....................................................................................................... 427
atm-encapsulation ............................................................................ 427
atm-options ....................................................................................... 428
atm-scheduler-map .......................................................................... 429
authentication-key ............................................................................ 429
authentication-key (APS) ................................................................. 429
authentication-key (VRRP) ............................................................... 430
authentication-type ............................................................................ 431
auto-synchronize .............................................................................. 432
backup-destination .......................................................................... 432
backup-interface .............................................................................. 433
bandwidth ........................................................................................ 433
bert-algorithm ................................................................................... 434
bert-error-rate ................................................................................... 435
bert-period ....................................................................................... 435
boot-command .................................................................................... 436
mlfr-uni-nni-bundle-options ................................................................. 498
minimum-links .................................................................................. 498
mode ................................................................................................. 499
mrru ................................................................................................. 499
mtu ................................................................................................. 500
multicast-dlci ..................................................................................... 500
multicast-vci ..................................................................................... 501
multicasts-only .................................................................................. 501
multipoint .......................................................................................... 501
multipoint-destination ....................................................................... 502
multiservice-options .......................................................................... 503
n391 ................................................................................................. 503
n392 ................................................................................................. 504
n393 ................................................................................................. 504
neighbor ............................................................................................ 505
no-accept-data .................................................................................. 505
no-asynchronous-notification .............................................................. 505
no-cbit-parity ................................................................................... 505
no-core-dump .................................................................................... 505
no-ecfr-loop-respond ......................................................................... 506
no-flow-control .................................................................................. 506
no-gratuitous-arp-reply ..................................................................... 506
no-gratuitous-arp-request ................................................................. 506
no-keepalive ..................................................................................... 506
no-loopback ....................................................................................... 507
no-long-buildout ................................................................................ 507
no-mac-learn-enable .......................................................................... 507
no-partition ....................................................................................... 507
  no-partition (Channelized E1, OC-12, and T3 QPP interfaces) ............ 507
  no-partition (Channelized OC-1 QPP interfaces) .................................. 508
  no-partition (Channelized STM-1 QPP interfaces) ................................ 508
no-payload-scrambler ......................................................................... 508
no-preempt ....................................................................................... 509
no-redirects ...................................................................................... 509
no-source-filtering ............................................................................ 509
no-syslog ......................................................................................... 509
no-translate-discard-eligible ............................................................... 509
no-translate-fecn-and-becn ............................................................... 509
no-z0-increment ............................................................................... 509
oam-liveness ..................................................................................... 510
oam-period ....................................................................................... 511
oc-slice ............................................................................................ 511
open-timeout .................................................................................... 512
output ............................................................................................... 512
output-vlan-map ............................................................................... 512
overflow ............................................................................................ 513
paired-group ..................................................................................... 513
partition ............................................................................................ 514
passive ............................................................................................... 515
passive-monitor-mode ....................................................................... 515
path-trace ......................................................................................... 516
payload-scrambler ............................................................................ 517
per-unit-scheduler ............................................................................ 517
pic-type ............................................................................................. 518
point-to-point ..................................................................................... 518
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>policer</td>
<td>519</td>
</tr>
<tr>
<td>policer (CoS)</td>
<td>519</td>
</tr>
<tr>
<td>policer (interface)</td>
<td>520</td>
</tr>
<tr>
<td>policer (MAC)</td>
<td>520</td>
</tr>
<tr>
<td>pop</td>
<td>521</td>
</tr>
<tr>
<td>post-service-filter</td>
<td>521</td>
</tr>
<tr>
<td>ppp-options</td>
<td>522</td>
</tr>
<tr>
<td>preempt</td>
<td>522</td>
</tr>
<tr>
<td>preferred</td>
<td>523</td>
</tr>
<tr>
<td>premium</td>
<td>523</td>
</tr>
<tr>
<td>primary</td>
<td>524</td>
</tr>
<tr>
<td>priority</td>
<td>524</td>
</tr>
<tr>
<td>priority (schedulers)</td>
<td>524</td>
</tr>
<tr>
<td>priority (vrrp)</td>
<td>525</td>
</tr>
<tr>
<td>promiscuous-mode</td>
<td>525</td>
</tr>
<tr>
<td>protect-circuit</td>
<td>525</td>
</tr>
<tr>
<td>proxy</td>
<td>526</td>
</tr>
<tr>
<td>push</td>
<td>526</td>
</tr>
<tr>
<td>queue-depth</td>
<td>527</td>
</tr>
<tr>
<td>queue-length</td>
<td>528</td>
</tr>
<tr>
<td>rate</td>
<td>528</td>
</tr>
<tr>
<td>receive-bucket</td>
<td>529</td>
</tr>
<tr>
<td>red-differential-delay</td>
<td>529</td>
</tr>
<tr>
<td>remote</td>
<td>530</td>
</tr>
<tr>
<td>remote-loopback-respond</td>
<td>530</td>
</tr>
<tr>
<td>request</td>
<td>531</td>
</tr>
<tr>
<td>revert-time</td>
<td>531</td>
</tr>
<tr>
<td>rfc-2615</td>
<td>531</td>
</tr>
<tr>
<td>routing-instance</td>
<td>532</td>
</tr>
<tr>
<td>rpf-check</td>
<td>532</td>
</tr>
<tr>
<td>rts</td>
<td>532</td>
</tr>
<tr>
<td>rts-polarity</td>
<td>533</td>
</tr>
<tr>
<td>rtvbr</td>
<td>533</td>
</tr>
<tr>
<td>sampling</td>
<td>534</td>
</tr>
<tr>
<td>scheduler-maps</td>
<td>534</td>
</tr>
<tr>
<td>serial-options</td>
<td>535</td>
</tr>
<tr>
<td>service</td>
<td>536</td>
</tr>
<tr>
<td>service-domain</td>
<td>536</td>
</tr>
<tr>
<td>service-filter</td>
<td>537</td>
</tr>
<tr>
<td>service-set</td>
<td>537</td>
</tr>
<tr>
<td>service-options</td>
<td>538</td>
</tr>
<tr>
<td>services</td>
<td>538</td>
</tr>
<tr>
<td>shaping</td>
<td>539</td>
</tr>
<tr>
<td>short-sequence</td>
<td>540</td>
</tr>
<tr>
<td>sonet-options</td>
<td>540</td>
</tr>
<tr>
<td>source</td>
<td>541</td>
</tr>
<tr>
<td>source-address-filter</td>
<td>542</td>
</tr>
<tr>
<td>source-class-usage</td>
<td>543</td>
</tr>
<tr>
<td>source-filtering</td>
<td>543</td>
</tr>
<tr>
<td>speed</td>
<td>544</td>
</tr>
<tr>
<td>stacked-vlan-tagging</td>
<td>544</td>
</tr>
<tr>
<td>start-end-flag</td>
<td>544</td>
</tr>
<tr>
<td>swap</td>
<td>545</td>
</tr>
<tr>
<td>syslog</td>
<td>545</td>
</tr>
<tr>
<td>syslog (interfaces)</td>
<td>545</td>
</tr>
<tr>
<td>syslog (monitoring)</td>
<td>546</td>
</tr>
<tr>
<td>t1-options</td>
<td>547</td>
</tr>
</tbody>
</table>
t3-options .......................................................................................................... 548
 t391 ................................................................................................................... 548
 t392 ................................................................................................................... 549
 tag-protocol-id ............................................................................................... 549
 tag-protocol-id (TPIDs expected to be sent or received) ......................... 549
 tag-protocol-id (TPID to rewrite) ............................................................... 549
 threshold ........................................................................................................... 550
 timeslots ............................................................................................................ 550
 tm ...................................................................................................................... 551
 tm-polarity ......................................................................................................... 551
 traceoptions ..................................................................................................... 552
 traceoptions (individual interfaces) ............................................................. 552
 traceoptions (interface process) ................................................................. 553
 traceoptions (VRRP) ................................................................................. 554
 track ................................................................................................................ 555
 translate-discard-eligible ............................................................................. 556
 translate-fecn-and-becn ............................................................................. 556
 transmit-bucket ............................................................................................... 557
 transmit-clock ................................................................................................. 557
 transmit-weight ............................................................................................... 558
 transmit-weight (ATM 2 Virtual Circuit) ....................................................... 558
 transmit-weight (ATM 2 CoS Forwarding Class) ......................................... 558
 traps .................................................................................................................. 559
 ttl ....................................................................................................................... 559
 tunnel ................................................................................................................. 560
 unit ..................................................................................................................... 561
 vbr ....................................................................................................................... 564
 vc-cos-mode ................................................................................................. 565
 vci ....................................................................................................................... 565
 virtual-address ................................................................................................. 566
 vlan-id .............................................................................................................. 566
 vlan-id (VLAN ID to be bound to a logical interface) .................................. 566
 vlan-id (VLAN ID to rewrite) ................................................................. 567
 vlan-tag ............................................................................................................ 567
 vlan-tagging ..................................................................................................... 568
 vpi ....................................................................................................................... 568
 vrrp-group ....................................................................................................... 569
 vtmapping ......................................................................................................... 570
 working-circuit ................................................................................................. 570
 yellow-differential-delay .............................................................................. 571
 z0-increment ................................................................................................. 571
# Table of Contents

## Part 4

### CoS

#### Chapter 32

**CoS Overview** ................................................................. 575

- CoS Applications .............................................................................................................. 576
- JUNOS CoS Components ................................................................................................. 577
  - Traffic Classifiers ........................................................................................................ 578
    - Default Classifier ..................................................................................................... 579
    - Behavior Aggregate Classifier ................................................................................... 579
    - Multifield Classifier .................................................................................................. 580
  - Forwarding Classes ...................................................................................................... 580
  - Transmission Scheduling and Rate Control .................................................................. 581
    - Scheduling Priority ................................................................................................... 581
    - Fabric Priority Queuing ............................................................................................ 582
    - Transmission Rate Control ....................................................................................... 582
    - Allocation of Leftover Bandwidth ................................................................................ 582
    - Default Congestion and Transmission Control ......................................................... 582
    - RED Congestion Control ............................................................................................ 583
  - Rewrite Markers .......................................................................................................... 583
- Hardware Capabilities and Limitations ............................................................................. 583

#### Chapter 33

**CoS Configuration Guidelines** .......................................................................................... 585

- Hardware Capabilities and Limitations ............................................................................. 588
- Define Code-Point Aliases ................................................................................................. 589
- Configure Forwarding Classes ........................................................................................... 592
  - Override Fabric Priority Queuing ................................................................................ 594
- Classify Packets by Behavior Aggregate ........................................................................... 594
- Configure Scheduling Policy Maps .................................................................................... 596
  - Associate a Scheduler with a DLCI or VLAN on a Channelized QPP Interface .......... 597
  - Example: Associate a Scheduler with a Logical QPP Interface .................................. 598
  - Associate a Scheduler with a Fabric Priority ................................................................ 600
- Configure RED Drop Profiles ............................................................................................ 601
- Packet Loss Priority ........................................................................................................... 602
- Rewrite Packet Header Information .................................................................................. 602
  - Rewrite EXP Bits on a Particular Node ......................................................................... 603
  - Example: Rewrite EXP Bits on a Particular Node ......................................................... 604
  - Rewrite MPLS and IPv4 Packet Headers ....................................................................... 605
  - Example: Rewrite MPLS and IPv4 Packet Headers ....................................................... 606
  - Rewrite the EXP Bits of All Three Labels of an Outgoing Packet .................................. 607
  - Example: Rewrite the EXP Bits of All Three Labels of an Outgoing Packet .................. 608
  - Rewrite IEEE 802.1p Packet Headers with MPLS EXP Value ........................................ 609
- Configure CoS-Based Forwarding ....................................................................................... 610
  - Example: Configure CoS-Based Forwarding .................................................................. 612
  - Override the Input Classification .................................................................................... 616
  - Example: Configure Class of Service .......................................................................... 617

---

---
Chapter 34

Summary of CoS Configuration Statements

- bandwidth ................................................................. 623
- buffer-size ........................................................................ 623
- class .............................................................................. 624
- class-of-service ......................................................... 624
- classification-override ................................................ 624
- classifiers ................................................................. 625
  - classifiers (define) .................................................. 625
  - classifiers (apply) ................................................... 625
- code-point ....................................................................... 626
- code-point-aliases ........................................................ 626
- code-points .................................................................... 627
- drop-probability ........................................................... 627
  - drop-probability (percentage) .................................. 627
  - drop-probability (interpolated value) ....................... 627
- drop-profile ................................................................. 628
- drop-profile-map .......................................................... 628
- drop-profiles ............................................................... 629
- exp-push-push-push ..................................................... 629
- exp-swap-push-push ..................................................... 630
- fabric ........................................................................... 630
- fill-level ........................................................................ 630
  - fill-level (percentage) .............................................. 630
  - fill-level (interpolated value) .................................. 630
- forwarding-class .......................................................... 631
- forwarding-class (classifiers) ....................................... 631
- forwarding-class (forwarding policy) ............................ 632
- forwarding-classes ....................................................... 632
- forwarding-policy ....................................................... 633
- import .......................................................................... 633
  - import classifiers ....................................................... 633
  - import rewrite-rules .................................................. 634
- interfaces ...................................................................... 635
- interpolate .................................................................... 635
- loss-priority ................................................................. 636
- lsp-next-hop .............................................................. 636
- next-hop ..................................................................... 636
- next-hop-map .............................................................. 637
- priority ...................................................................... 637
  - priority (fabric queues) ............................................ 637
  - priority (forwarding classes) .................................... 638
  - priority (schedulers) ............................................... 638
- protocol ........................................................................ 639
- protocol (interfaces rewrite rules) ............................... 639
- protocol (schedulers) .................................................... 639
- queue .......................................................................... 640
- rewrite-rules ............................................................... 640
- rewrite-rules (interfaces) ............................................. 641
- scheduler ................................................................. 641
- scheduler (scheduler map) .......................................... 641
- scheduler (fabric queues) ............................................. 642
- scheduler-map ............................................................ 642
- scheduler-map (fabric queues) ..................................... 642
- scheduler-map (interfaces) .......................................... 642
**List of Figures**

<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Interface Slot, PIC, and Port Locations</td>
<td>26</td>
</tr>
<tr>
<td>2</td>
<td>Clock Sources</td>
<td>28</td>
</tr>
<tr>
<td>3</td>
<td>Unicast RPF with Routing Asymmetry</td>
<td>92</td>
</tr>
<tr>
<td>4</td>
<td>Prefix Accounting with Source and Destination Classes</td>
<td>94</td>
</tr>
<tr>
<td>5</td>
<td>Layer 2 Switching Circuit Cross-Connect</td>
<td>100</td>
</tr>
<tr>
<td>6</td>
<td>Example Topology of a Switching Circuit Cross-Connect with Frame Relay CCC Encapsulation</td>
<td>103</td>
</tr>
<tr>
<td>7</td>
<td>Layer 2.5 Switching Translational Cross-Connect</td>
<td>104</td>
</tr>
<tr>
<td>8</td>
<td>Structure of the Channelized OC-12 PIC with QPP</td>
<td>170</td>
</tr>
<tr>
<td>9</td>
<td>Structure of the Channelized STM-1 PIC with QPP</td>
<td>171</td>
</tr>
<tr>
<td>10</td>
<td>Structure of the Channelized DS-3 PIC with QPP</td>
<td>171</td>
</tr>
<tr>
<td>11</td>
<td>Structure of the Channelized E1 PIC with QPP</td>
<td>171</td>
</tr>
<tr>
<td>12</td>
<td>Sample Channelization of OC-12 PIC with QPP</td>
<td>183</td>
</tr>
<tr>
<td>13</td>
<td>Sample Channelization of OC-12 PIC</td>
<td>184</td>
</tr>
<tr>
<td>14</td>
<td>Configure T1 Interfaces on a Channelized OC-12 PIC</td>
<td>188</td>
</tr>
<tr>
<td>15</td>
<td>Configure NxDS-0 Interfaces on a Channelized OC-12 PIC</td>
<td>190</td>
</tr>
<tr>
<td>16</td>
<td>Sample Channelization of OC-12 PIC with QPP</td>
<td>199</td>
</tr>
<tr>
<td>17</td>
<td>Sample Channelization of DS-3 PIC with QPP</td>
<td>234</td>
</tr>
<tr>
<td>18</td>
<td>Remote and Local E1 Loopback</td>
<td>247</td>
</tr>
<tr>
<td>19</td>
<td>Remote and Local E3 Loopback</td>
<td>254</td>
</tr>
<tr>
<td>20</td>
<td>IPSec Tunnel Redundancy</td>
<td>260</td>
</tr>
<tr>
<td>21</td>
<td>Example Topology of Layer 2.5 Translational Cross-Connect</td>
<td>288</td>
</tr>
<tr>
<td>22</td>
<td>Multilink Interface Configuration</td>
<td>333</td>
</tr>
<tr>
<td>23</td>
<td>Serial Interface Clocking Mode</td>
<td>350</td>
</tr>
<tr>
<td>24</td>
<td>Serial Interface LIU Loopback</td>
<td>356</td>
</tr>
<tr>
<td>25</td>
<td>Serial Interface Local Loopback</td>
<td>356</td>
</tr>
<tr>
<td>26</td>
<td>APS Configuration Topologies</td>
<td>367</td>
</tr>
<tr>
<td>27</td>
<td>APS Load Sharing between Circuit Pairs</td>
<td>372</td>
</tr>
<tr>
<td>28</td>
<td>Remote and Local T1 Loopback</td>
<td>392</td>
</tr>
<tr>
<td>29</td>
<td>Remote and Local T3 Loopback</td>
<td>401</td>
</tr>
<tr>
<td>30</td>
<td>Packet Flow Through CoS Configurable Components</td>
<td>578</td>
</tr>
<tr>
<td>31</td>
<td>Segmented and Interpolated Drop Profiles</td>
<td>601</td>
</tr>
<tr>
<td>32</td>
<td>Sample CoS-Based Forwarding</td>
<td>613</td>
</tr>
</tbody>
</table>
List of Figures
List of Tables

Table 1: Juniper Networks Technical Documentation ........................................xl
Table 2: Statements for Physical Interface Properties ........................................42
Table 3: Media MTU Sizes by Interface Type for M5, M10, M20, and M40 Routers ...........................................................................47
Table 4: Media MTU Sizes by Interface Type for M40e Routers .......................47
Table 5: Media MTU Sizes by Interface Type for M160 Routers .......................48
Table 6: Media MTU Sizes by Interface Type for T320 Platforms ....................49
Table 7: Media MTU Sizes by Interface Type for T640 Platforms ....................49
Table 8: Encapsulation Overhead by Encapsulation Type...............................49
Table 9: BERT Capabilities by Interface Type ..................................................63
Table 10: Statements for Logical Interface Properties .....................................69
Table 11: System Log Priority Level Settings ................................................114
Table 12: ATM 1 and ATM 2 Configuration Differences ..................................122
Table 13: ATM Traffic-Shaping Rates ..............................................................141
Table 14: Supported Interfaces on Channelized PICs with QPP .......................165
Table 15: Frame Relay DLCI Limitations for Channelized Interfaces ...............166
Table 16: Clocking Capabilities by Channelized PIC Type ...............................167
Table 17: Structural Differences: Channelized PICs and Channelized PICs with QPP ..............................................................172
Table 18: Ranges for Channelized E1 Configuration ........................................179
Table 19: OC-12 to DS-3 Numbering Scheme ...............................................198
Table 20: Channelized STM-1 to E1 Channel Mapping ...................................217
Table 21: Ranges for Channelized DS-3 to DS0 Configuration .........................230
Table 22: Capabilities of the Gigabit Ethernet PIC with QPP ..........................268
Table 23: VLAN ID Range by Interface Type ...............................................319
Table 24: Multilink and Link Services Logical Interface Statements ..................322
Table 25: Link Services Physical Interface Statements for MLFR (FRF.16) .......328
Table 26: Multilink Services PIC Capacities ..................................................332
Table 27: Link Services Bundle .................................................................341
Table 28: Signal Handling by Serial Interface Type .........................................352
Table 29: SONET/SDH Framing Bytes for Specific Speeds ...............................362
Table 30: SONET Default Settings ..................................................................366
Table 31: Methods for Configuring Egress Filtering ........................................410
Table 32: Default IP Precedence Classifier ....................................................410
Table 33: CoS Hardware Capabilities and Limitations ....................................588
Table 34: Default DSCP Mappings ..............................................................589
Table 35: Default Forwarding Classes ..........................................................592
Table 36: Default Behavior Aggregate Classification ......................................594
Table 37: Scheduler Limitations for Channelized QPP Interfaces ....................598
Table 38: Default Packet Header Rewrite Mappings .......................................602
Table 39: Default MPLS EXP Rewrite Table ...............................................605
About This Manual

This chapter provides a high-level overview of the JUNOS Internet Software Configuration Guide: Network Interfaces and Class of Service:

- Objectives on page xxxiii
- Audience on page xxxiv
- Document Organization on page xxxiv
- Part Organization on page xxxvi
- Using the Indexes on page xxxvii
- Documentation Conventions on page xxxviii
- List of Technical Publications on page xl
- Documentation Feedback on page xli
- How to Request Support on page xli

Objectives

This manual provides an overview of the interface and class of service features of the JUNOS Internet software and describes how to configure these properties on the router.

This manual documents Release 6.0 of the JUNOS Internet software. To obtain additional information about the JUNOS software—either corrections to information in this manual or information that might have been omitted from this manual—refer to the software release notes.

To obtain the most current version of this manual and the most current version of the software release notes, refer to the product documentation page on the Juniper Networks Web site, which is located at http://www.juniper.net/.

To order printed copies of this manual or to order a documentation CD-ROM, which contains this manual, please contact your sales representative.
Audience

This manual is designed for network administrators who are configuring a Juniper Networks router. It assumes that you have a broad understanding of networks in general, the Internet in particular, networking principles, and network configuration. This manual assumes that you are familiar with one or more of the following Internet routing protocols: Border Gateway Protocol (BGP), Routing Information Protocol (RIP), Intermediate System-to-Intermediate System (IS-IS), Open Shortest Path First (OSPF), Internet Control Message Protocol (ICMP) router discovery, Internet Group Management Protocol (IGMP), Distance Vector Multicast Routing Protocol (DVMRP), Protocol-Independent Multicast (PIM), Multiprotocol Label Switching (MPLS), Resource Reservation Protocol (RSVP), and Simple Network Management Protocol (SNMP).

Document Organization

This manual is divided into several parts. Each part describes a major functional area of the JUNOS software, and the individual chapters within a part describe the software commands of that functional area.

This manual contains the following parts and chapters:

- Preface, “About This Manual” (this chapter), provides a brief description of the contents and organization of this manual and describes how to contact customer support.
- Part 1, “Overview,” provides an overview of how to configure the router’s interface and class of service properties:
  - Chapter 1, “Network Interfaces and Class of Service Overview,” describes the router’s interfaces and tools for processing traffic using class-of-service techniques.
  - Chapter 2, “Interfaces and Class of Service Configuration Statements,” lists all commands discussed in this manual and shows their hierarchy.
- Part 2, “Router Interfaces,” includes an overview chapter, chapters that describe physical, logical, and family interface statements and properties, and chapters that describe cross-connects and trace operations:
  - Chapter 3, “Interfaces Overview,” provides an overview of interfaces, including a description of the interfaces supported by the router and interface naming conventions.
  - Chapter 4, “Interfaces Configuration Statements,” lists all statements used to configure the interfaces.
  - Chapter 5, “Configure Physical Interface Properties,” provides a description of the interface statements used at the physical layer.
  - Chapter 6, “Configure Logical Interface Properties,” describes the process of configuring logical interfaces within a physical interface.
  - Chapter 7, “Configure Protocol Family and Address Interface Properties,” explains the assignment of a protocol family to an interface.
Chapter 8, "Configure Circuit and Translational Cross-Connects," explains the use of cross-connect techniques across Layer 2 physical interfaces.

Chapter 9, "Trace Interface Operations," describes how to trace interface operations.

Part 3, "Interface Types," includes chapters that describe each interface type and its associated statements and properties:

- Chapter 10, "Configure Adaptive Services Interfaces," documents the configuration of the adaptive services interface.
- Chapter 11, "Configure ATM 1 and ATM 2 Interfaces," explains interfaces designed for Asynchronous Transfer Mode encapsulation.
- Chapter 12, "Channelized Interfaces Overview," provides a high-level overview of channelized interfaces, focusing mainly on the capabilities, properties, and structure of Channelized QPP interfaces.
- Chapter 13, "Configure Channelized E1 Interfaces," details the configuration of the Channelized E1 and Channelized E1 QPP interface types, used outside North America.
- Chapter 14, "Configure Channelized OC-12 Interfaces," details the configuration of the Channelized OC-12 and Channelized OC-12 QPP interface types.
- Chapter 15, "Configure Channelized STM-1 Interfaces," details the configuration of the Channelized STM-1 and Channelized STM-1 QPP interface types.
- Chapter 16, "Configure Channelized T3 Interfaces," details the configuration of the Channelized T3 and Channelized T3 QPP interface types.
- Chapter 17, "Configure Discard Interfaces," details the configuration of the discard interface.
- Chapter 18, "Configure E1 Interfaces," details the configuration of the E1 interface type, used outside North America.
- Chapter 19, "Configure E3 Interfaces," details the configuration of the E3 interface type, used outside North America.
- Chapter 20, "Configure Encryption Interfaces," details the configuration of tunnel interfaces that use the ES PIC.
- Chapter 21, "Configure Ethernet Interfaces," provides configuration information about the Fast Ethernet and Gigabit Ethernet interface types.
- Chapter 22, "Configure Frame Relay," explains the configuration of Frame Relay interface encapsulation on logical interfaces.
- Chapter 23, "Configure the Loopback Interface," documents the configuration of the loopback interface and explains how to set loopback addresses.
- Chapter 24, "Configure Monitoring Services Interfaces," documents the configuration of flow monitoring and accounting interfaces.
Chapter 25, “Configure Multilink and Link Services Interfaces,” documents the configuration of multilink and link services interfaces and describes how to set up links and bundles.

Chapter 26, “Configure Serial Interfaces,” documents the configuration of the serial interface.

Chapter 27, “Configure SONET/SDH Interfaces,” documents the configuration of the various high-speed fiber-optic interface types.

Chapter 28, “Configure T1 Interfaces,” explains the use of the T1 interface type used in North America.

Chapter 29, “Configure T3 Interfaces,” explains the use of the DS-3 metallic interface type used in North America.

Chapter 30, “Configure Tunnel Interfaces,” explains how to use a Tunnel PIC to set up unicast, multicast, IPv6-over-IPv4, and PIM tunnels, and describes how to use a Tunnel PIC for route and VRF table lookups.

Chapter 31, “Summary of Interface Configuration Statements,” provides a detailed listing of all configuration statements used the “Router Interfaces” and “Interface Types” parts of the manual.

Part 4, “CoS,” describes how to configure and monitor the JUNOS software to support CoS decision-making:

Chapter 32, “CoS Overview,” introduces the concept of CoS.

Chapter 33, “CoS Configuration Guidelines,” describes how to configure CoS.

Chapter 34, “Summary of CoS Configuration Statements,” provides a detailed listing of all CoS-related configuration statements.

This manual also contains a glossary, a complete index, and an index of statements and commands.

Part Organization

The parts in this manual typically contain the following chapters:

Overview—Provides background information about and discusses concepts related to the software component described in that part of the book.

Configuration statements—Lists all the configuration statements available to configure the software component. This list is designed to provide an overview of the configuration statement hierarchy for that software component.

Configuration guidelines—Describes how to configure all the features of the software component. The first section of the configuration guidelines describes the minimum configuration for that component, listing the configuration statements you must include to enable the software component on the router with only the bare minimum functionality. The remaining sections in the configuration guidelines are generally arranged so that the most common features are near the beginning.
Statement summary—A reference that lists all configuration statements alphabetically and explains each statement and all its options. The explanation of each configuration statement consists of the following parts:

- Syntax—Describes the full syntax of the configuration statement. For an explanation of how to read the syntax statements, see “Documentation Conventions” on page xxxviii.

- Hierarchy level—Tells where in the configuration statement hierarchy you include the statement.

- Description—Describes the function of the configuration statement.

- Options—Describes the configuration statement’s options, if there are any. For options with numeric values, the allowed range and default value, if any, are listed. For multiple options, if one option is the default, that fact is stated. If a configuration statement is at the top of a hierarchy of options that are other configuration statements, these options are generally explained separately in the statement summary section.

- Usage guidelines—Points to the section or sections in the configuration guidelines section that describe how to use the configuration statement.

- Required privilege level—Indicates the permissions that the user must have to view or modify the statement in the router configuration. For an explanation of the permissions, see the JUNOS Internet Software Configuration Guide: Getting Started.

- See also—Indicates other configuration statements that might provide related or similar functionality.

Using the Indexes

This manual contains two indexes: a complete index, which contains all index entries, and an index that contains only statements and commands.

In the complete index, bold page numbers point to pages in the statement summary chapters. The index entry for each configuration statement always contains at least two entries. The first, with a bold page number on the same line as the statement name, references the statement summary section. The second entry, “usage guidelines,” references the section in a configuration guidelines chapter that describes how to use the statement.
Documentation Conventions

**General Conventions**

This manual uses the following text conventions:

- Statements, commands, filenames, directory names, IP addresses, and configuration hierarchy levels are shown in a sans serif font. In the following example, stub is a statement name and [edit protocols ospf area area-id] is a configuration hierarchy level:

  To configure a stub area, include the stub statement at the [edit protocols ospf area area-id] hierarchy level:

- In examples, text that you type literally is shown in bold. In the following example, you type the word show:

  [edit protocols ospf area area-id]
  cli# show
  stub <default-metric metric>

- Examples of command output are generally shown in a fixed-width font to preserve the column alignment. For example:

  
  
  `> show interfaces terse`
  
  ---------------  └─┬─┐  └─┬─┐  └─┬─┐
  Interface | Admin Link Proto Local | Remote
  -------------  └─┬─┐  └─┬─┐  └─┬─┐
  at-1/3/0    up up inet 1.0.0.1           --> 1.0.0.2
  is0
  fwp0      up up inet 192.168.5.59/24

**Conventions for Software Commands and Statements**

When describing the JUNOS software, this manual uses the following type and presentation conventions:

- Statement or command names that you type literally are shown nonitalicized. In the following example, the statement name is area:

  You configure all these routers by including the following area statement at the [edit protocols ospf] hierarchy level:

- Options, which are variable terms for which you substitute appropriate values, are shown in italics. In the following example, area-id is an option. When you type the area statement, you substitute a value for area-id.

  area area-id;

- Optional portions of a configuration statement are enclosed in angle brackets. In the following example, the “default-metric metric” portion of the statement is optional:

  stub <default-metric metric>;
For text strings separated by a pipe (|), you must specify either string1 or string2, but you cannot specify both or neither of them. Parentheses are sometimes used to group the strings.

```
string1 | string2
(string1 | string2 )
```

In the following example, you must specify either broadcast or multicast, but you cannot specify both:

```
broadcast | multicast
```

For some statements, you can specify a set of values. The set must be enclosed in square brackets. For example:

```
community name members [ community-ids ]
```

The configuration examples in this manual are generally formatted in the way that they appear when you issue a show command. This format includes braces ({}), and semicolons. When you type configuration statements in the CLI, you do not type the braces and semicolons. However, when you type configuration statements in an ASCII file, you must include the braces and semicolons. For example:

```
[edit]
cli# set routing-options static route default nexthop address retain
[edit]
cli# show
routing-options { static { route default { nexthop address; retain; } } }
```

Comments in the configuration examples are shown either preceding the lines that the comments apply to, or more often, they appear on the same line. When comments appear on the same line, they are preceded by a pound sign (#) to indicate where the comment starts. In an actual configuration, comments can only precede a line; they cannot be on the same line as a configuration statement. For example:

```
protocols { mpls { interface (interface-name | all); # Required to enable MPLS on the interface } rsvp { interface interface-name; # Required for dynamic MPLS only } }
```

The general syntax descriptions provide no indication of the number of times you can specify a statement, option, or keyword. This information is provided in the text of the statement summary.
List of Technical Publications

Table 1 lists the software and hardware books for Juniper Networks routers and describes the contents of each book.

<table>
<thead>
<tr>
<th>Book</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>JUNOS Internet Software Configuration Guides</strong></td>
<td></td>
</tr>
<tr>
<td>Feature Guide</td>
<td>Provides a detailed explanation and configuration examples for several of the most complex features in the JUNOS software.</td>
</tr>
<tr>
<td>Getting Started</td>
<td>Provides an overview of the JUNOS software and describes how to install and upgrade the software. This manual also describes how to configure system management functions and how to configure the chassis, including user accounts, passwords, and redundancy.</td>
</tr>
<tr>
<td>MPLS Applications</td>
<td>Provides an overview of traffic engineering concepts and describes how to configure traffic engineering protocols.</td>
</tr>
<tr>
<td>Multicast</td>
<td>Provides an overview of multicast concepts and describes how to configure multicast routing protocols.</td>
</tr>
<tr>
<td>Network Interfaces and Class of Service</td>
<td>Provides an overview of the network interface and class-of-service functions of the JUNOS software and describes how to configure the network interfaces on the router.</td>
</tr>
<tr>
<td>Network Management</td>
<td>Provides an overview of network management concepts and describes how to configure various network management features, such as SNMP, accounting options, and cflowd.</td>
</tr>
<tr>
<td>Policy Framework</td>
<td>Provides an overview of policy concepts and describes how to configure routing policy, firewall filters, and forwarding options.</td>
</tr>
<tr>
<td>Routing and Routing Protocols</td>
<td>Provides an overview of routing concepts and describes how to configure routing, routing instances, and unicast routing protocols.</td>
</tr>
<tr>
<td>Services Interfaces</td>
<td>Provides an overview of the services interfaces functions of the JUNOS software and describes how to configure the services interfaces on the router.</td>
</tr>
<tr>
<td><strong>VPNs</strong></td>
<td>Provides an overview of Layer 2 and Layer 3 Virtual Private Networks (VPNs), describes how to configure VPNs, and provides configuration examples.</td>
</tr>
<tr>
<td><strong>JUNOS Internet Software References</strong></td>
<td></td>
</tr>
<tr>
<td>Operational Mode Command Reference: Interfaces</td>
<td>Describes the JUNOS Internet software operational mode commands you use to monitor and troubleshoot network and services interfaces on Juniper Networks M-series and T-series routers.</td>
</tr>
<tr>
<td>Operational Mode Command Reference: Protocols, Class of Service, Chassis, and Management</td>
<td>Describes the JUNOS Internet software operational mode commands you use to monitor and troubleshoot most aspects of Juniper Networks M-series and T-series routers.</td>
</tr>
<tr>
<td>System Log Messages Reference</td>
<td>Describes how to access and interpret system log messages generated by JUNOS software modules and provides a reference page for each message.</td>
</tr>
<tr>
<td><strong>JUNOScript API Documentation</strong></td>
<td></td>
</tr>
<tr>
<td>JUNOScript API Guide</td>
<td>Describes how to use the JUNOScript API to monitor and configure Juniper Networks routers.</td>
</tr>
<tr>
<td>JUNOScript API Reference</td>
<td>Provides a reference page for each tag in the JUNOScript API.</td>
</tr>
<tr>
<td><strong>JUNOS Internet Software Comprehensive Index</strong></td>
<td></td>
</tr>
<tr>
<td>Comprehensive Index</td>
<td>Provides a complete index of all JUNOS Internet software books and the JUNOScript API Guide.</td>
</tr>
<tr>
<td>Book</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Hardware Documentation</strong></td>
<td></td>
</tr>
<tr>
<td>Hardware Guide</td>
<td>Describes how to install, maintain, and troubleshoot routers and router components. Each platform has its own hardware guide.</td>
</tr>
<tr>
<td>PIC Guide</td>
<td>Describes the router Physical Interface Cards (PICs). Each router platform has its own PIC guide.</td>
</tr>
<tr>
<td><strong>Release Notes</strong></td>
<td></td>
</tr>
<tr>
<td>JUNOS Internet Software Release Notes</td>
<td>Provide a summary of new features for a particular software release. Software release notes also contain corrections and updates to published JUNOS and JUNOScript manuals, provide information that might have been omitted from the manuals, and describe upgrade and downgrade procedures.</td>
</tr>
<tr>
<td>Hardware Release Notes</td>
<td>Describe the available documentation for the router platform and summarize known problems with the hardware and accompanying software. Each platform has its own release notes.</td>
</tr>
<tr>
<td><strong>JUNOScope Software</strong></td>
<td></td>
</tr>
<tr>
<td>JUNOScope Software Guide</td>
<td>Describes the JUNOScope software graphical user interface (GUI), how to install and administer the software, and how to use the software to manage router configuration files and monitor router operations.</td>
</tr>
</tbody>
</table>

**Documentation Feedback**

We are always interested in hearing from our customers. Please let us know what you like and do not like about the Juniper Networks documentation, and let us know of any suggestions you have for improving the documentation. Also, let us know if you find any mistakes in the documentation. Send your feedback to techpubs-comments@juniper.net.

**How to Request Support**

For technical support, contact Juniper Networks at support@juniper.net, or at 1-888-314-JTAC (within the United States) or 408-745-9500 (from outside the United States).
Part 1
Overview

- Network Interfaces and Class of Service Overview on page 3
- Interfaces and Class of Service Configuration Statements on page 5
Chapter 1  
Network Interfaces and Class of Service Overview

Routers typically contain several different types of interfaces suited to various functions. For the interfaces on a router to function, you must configure them, specifying properties such as the interface location (that is, which slot the FPC is installed in and which location on the FPC the PIC is installed in), the interface type (such as SONET or ATM), encapsulation, and interface-specific properties.

You can configure JUNOS class-of-service (CoS) properties to provide a variety of classes of service for different applications, including multiple forwarding classes for managing packet transmission, congestion management, and CoS-based forwarding.
Chapter 2

Interfaces and Class of Service Configuration Statements

This chapter shows the complete configuration statement hierarchy, listing all possible configuration statements and showing their level in the configuration hierarchy. When you are configuring the JUNOS software, your current hierarchy level is shown in the banner on the line preceding the user@host# prompt.

This chapter is organized as follows:

- [edit class-of-service] Hierarchy Level on page 5
- [edit interfaces] Hierarchy Level on page 7
- [edit protocols connections] Hierarchy Level on page 15
- [edit protocols vrrp] Hierarchy Level on page 16

[edit class-of-service] Hierarchy Level

class-of-service {
  classifiers {
    (dscp | exp | ieee-802.1 | inet-precedence) classifier-name {
      import (classifier-name | default);
      forwarding-class class-name {
        loss-priority (low | high) code-points { alias | bits };
      }
    }
  }
  code-point-aliases {
    (dscp | exp | ieee-802.1 | inet-precedence) {
      alias-name bits;
    }
  }
  drop-profiles {
    profile-name {
      fill-level percentage drop-probability percentage;
      interpolate {
        drop-probability value;
        fill-level value;
      }
    }
  }
}
fabric {
  scheduler-map {
    priority (low | high) scheduler scheduler-name;
  }
}
forwarding-classes {
  queue queue-number class-name priority (low | high);
}
forwarding-policy {
  next-hop-map map-name {
    forwarding-class class-name {
      next-hop [ next-hop-name ];
      lsp-next-hop [ lsp-regular-expression ];
    }
  }
  class class-name {
    classification-override {
      forwarding-class class-name;
    }
  }
}
interfaces
  interface-name {
    scheduler-map map-name;
    unit logical-unit-number {
      bandwidth rate;
      classifiers {
        (dscp | exp | ieee-802.1 | inet-precedence) (classifier-name | default)
      }
    }
    forwarding-class class-name;
    rewrite-rules {
      dscp (rewrite-name | default);
      exp (rewrite-name | default) protocol protocol-types;
      exp-push-push-push default;
      exp-swap-push-push default;
      ieee-802.1 default;
      inet-precedence (rewrite-name | default);
    }
    scheduler-map map-name;
  }
rewrite-rules {
  (dscp | exp | inet-precedence) rewrite-name {
    import (rewrite-name | default);
    forwarding-class class-name {
      loss-priority (low | high) code-point (alias | bits);
    }
  }
}
scheduler-maps {
  map-name {
    forwarding-class class-name scheduler scheduler-name;
  }
}
schedulers
scheduler-name {
    buffersize (percent percentage | remainder | temporal microseconds);
    drop-profile-map loss-priority (low | high) protocol (non-tcp | tcp | any)
        drop-profile profile-name;
    priority (low | high | strict-high);
    transmit-rate (rate | percent percentage | remainder | exact);
}
}

[edit interfaces] Hierarchy Level

interfaces {
    traceoptions {
        file filename <files number> <size size> <world-readable | no-world-readable>;
        flag flag <disable>;
    }
    interface-name {
        disable;
        accounting-profile name;
        description text;
        aggregated-ether-options {
            (flow-control | no-flow-control);
            link-speed speed;
            (loopback | no-loopback);
            minimum-links number;
            source-address-filter {
                mac-address;
            } (source-filtering | no-source-filtering);
        }
        aggregated-sonet-options {
            link-speed speed;
            minimum-links number;
        }
        atm-options {
            cell-bundle-size cells;
            ilmi;
            linear-red-profiles profile-name {
                high-plp-max-threshold percent;
                low-plp-max-threshold percent;
                queue-depth cells high-plp-threshold percent low-plp-threshold percent;
            }
            pic-type (atm1 | atm2);
            promiscuous-mode {
                [vpi vpi-identifier];
            }
        }
        scheduler-maps map-name {
            forwarding-class class-name {
                priority (low | high);
                transmit-weight (cells number | percent number);
                (epd-threshold cells | linear-red-profile profile-name);
            }
            vc-cos-mode (alternate | strict);
        }
    }
}
vpi vpi-identifier {
    maximum-vcs maximum-vcs;
    oam-liveness {
        up-count cells;
        down-count cells;
    }
    oam-period (disable | seconds);
    shaping {
        (cbr rate | rtvbr peak rate sustained rate burst length | vbr peak rate sustained rate burst length);
        queue-length number;
    }
}
}
clocking clock-source;
dce;
ds0-options {
    bert-algorithm algorithm;
    bert-error-rate rate;
    bert-period seconds;
    byte-encoding (nx64 | nx56);
    fcs (32 | 16);
    idle-cycle-flag (flags | ones);
    invert-data;
    loopback (payload | remote);
    start-end-flag (shared | filler);
}
e1-options {
    bert-error-rate rate;
    bert-period seconds;
    fcs (32 | 16);
    framing (g704 | g704-no-crc4 | unframed);
    idle-cycle-flag (flags | ones);
    invert-data;
    loopback (local | remote);
    start-end-flag (shared | filler);
    timeslots time-slot-range;
}
e3-options {
    atm-encapsulation (direct | PLCP);
    bert-algorithm algorithm;
    bert-error-rate rate;
    bert-period seconds;
    buildout feet;
    compatibility-mode (digital-link | kentrox | larscom) <subrate value>;
    fcs (32 | 16);
    framing (g751 | g832);
    idle-cycle-flag value;
    loopback (local | remote);
    (payload-scrambler | no-payload-scrambler);
    start-end-flag value;
}
encapsulation type;
es-options {
    backup-interface es-fpc/pic/port;
}
fastether-options {
    802.3ad aex;
    (flow-control | no-flow-control);
    ingress-rate-limit rate;
    (loopback | no-loopback);
    source-address-filter {
        mac-address;
    }
    (source-filtering | no-source-filtering);
}
gigether-options {
    802.3ad aex;
    ethernet-switch-profile {
        ethernet-policer-profile {
            ieee802.1-priority-map premium [ bits ];
            policer cos-policer-name {
                aggregate {
                    bandwidth-limit rate;
                    bandwidth-percent percent;
                    burst-size-limit length;
                }
                premium {
                    bandwidth-limit rate;
                    bandwidth-percent percent;
                    burst-size-limit length;
                }
            }
            (mac-learn-enable | no-mac-learn-enable);
            tag-protocol-id [ tpids ];
        }
        (flow-control | no-flow-control);
        (loopback | no-loopback);
        source-address-filter {
            mac-address;
        }
        (source-filtering | no-source-filtering);
    }
    (gratuitous-arp-reply | no-gratuitous-arp-reply);
    hold-time up milliseconds down milliseconds;
    keepalives <down-count number> <interval seconds> <up-count number>;
    link-mode mode;
    lmi {
        lmi-type (ansi | itu);
        n391dte number;
        n392dce number;
        n392dte number;
        n393dce number;
        n393dte number;
        t391dte seconds;
        t392dce seconds;
    }
    mac mac-address;
mlfr-uni-nni-bundle-options {
  acknowledge-retries number;
  acknowledge-timer milliseconds;
  action-red-differential-delay (disable-tx | remove-link);
  drop-timeout milliseconds;
  fragment-threshold bytes;
  hello-timer milliseconds;
  lmi-type (ansi | itu);
  minimum-links number;
  mrru bytes;
  n391 number;
  n392 number;
  n393 number;
  red-differential-delay milliseconds;
  t391 seconds;
  t392 seconds;
  yellow-differential-delay milliseconds;
}
mtu bytes;
multiservice-options {
  boot-command filename
  (core-dump | no-core-dump);
  (syslog | no-syslog);
}
no-gratuitous-arp-request;
no-keepalives;
no-partition {
  interface-type type;
}
partition partition-number oc-slice oc-slice-range interface-type type {
  timeslots time-slot-range;
}
passive-monitor-mode;
per-unit-scheduler;
ppp-options {
  chap {
    access-profile name;
    local-name name;
    passive;
  }
}
receive-bucket {
  overflow (tag | discard);
  rate percentage;
  threshold bytes;
}
serial-options {
    clock-rate rate;
    clocking-mode (dce | dte | loop);
    control-leads {
        control-signal (assert | de-assert | normal);
        cts (ignore | normal | require);
        dcd (ignore | normal | require);
        dsr (ignore | normal | require);
        dsr-signal-handling-option;
        ignore-all;
        indication (ignore | normal | require);
        rts (assert | de-assert | normal);
        tm (ignore | normal | require);
    }
    control-polarity (positive | negative);
    cts-polarity (positive | negative);
    dcd-polarity (positive | negative);
    dsr-polarity (positive | negative);
    dtr-circuit (balanced | unbalanced);
    dtr-polarity (positive | negative);
    encoding (nrz | nrzi);
    indication-polarity (positive | negative);
    line-protocol protocol;
    loopback mode;
    rts-polarity (positive | negative);
    tm-polarity (positive | negative);
    transmit-clock invert;
}

service-options {
    inactivity-timeout seconds;
    open-timeout seconds;
    syslog {
        host host-name {
            facility-override facility-name;
            log-prefix prefix-number;
            [ services priority-level ];
        }
    }
}

sonet-options {
    aggregate asx;
    aps {
        advertise-interval milliseconds;
        authentication-key key;
        force;
        hold-time milliseconds;
        lockout;
        neighbor address;
        paired-group group-name;
        protect-circuit group-name;
        request;
        revert-time seconds;
        working-circuit group-name;
    }

bytes {
    e1-quiet value;
    f1 value;
    f2 value;
    s1 value;
    z3 value;
    z4 value;
}
fcs (32 | 16);
loopback (local | remote);
path-trace trace-string;
(payload-scrambler | no-payload-scrambler);
rfc-2615;
vtmapping (itu-t | klm);
(z0-increment | no-z0-increment);
}
speed (10m | 100m);
stacked-vlan-tagging;
t1-options {
    bert-algorithm algorithm;
    bert-error-rate rate;
    bert-period seconds;
    buildout (0-132 | 133-265 | 266-398 | 399-531 | 532-655);
    byte-encoding (nx64 | nx56);
    fcs (32 | 16);
    framing (sf | esf);
    idle-cycle-flag (flags | ones);
    invert-data;
    line-encoding (ami | b8zs);
    loopback (local | payload | remote);
    remote-loopback-respond;
    start-end-flag (shared | filler);
    timeslots time-slot-range;
}
t3-options {
    atm-encapsulation (direct | PLCP);
    bert-algorithm algorithm;
    bert-error-rate rate;
    bert-period seconds;
    buildout feet;
    (cbit-parity | no-cbit-parity);
    compatibility-mode (adtran | digital-link | kentrox | larscom | verilink) <subrate value>;
    fcs (32 | 16);
    (feac-loop-respond | no-feac-loop-respond);
    idle-cycle-flag value;
    (long-buildout | no-long-buildout);
    loopback (local | payload | remote);
    (mac | no-mac);
    (payload-scrambler | no-payload-scrambler);
    start-end-flag value;
}
traceoptions {
    flag flag <flag-modifier> <disable>;
}
transmit-bucket {
    overflow (tag | discard);
    rate percentage;
    threshold bytes;
}
(traps | no-traps);
vlan-tagging;
unit logical-unit-number {
    accept-source-mac {
        mac-address mac-address {
            policer {
                input policer-name;
                output policer-name;
            }
        }
    }
    accounting-profile name;
    allow-any-vci;
    bandwidth rate;
    cell-bundle-size cells;
    description text;
    disable;
    dcli dcli-identifier;
    drop-timeout milliseconds;
    encapsulation type;
    epd-threshold cells;
    fragment-threshold bytes;
    input-vlan-map {
        pop;
        push;
        swap;
        vlan-id number;
        tag-protocol-id tpid;
    }  
    interleave-fragments;
    inverse-arp;
    minimum-links number;
    mrru bytes;
    multicast-dcli dcli-identifier;
    multicast-vci vpi-identifier.vci-identifier;
    multipoint;
    oam-liveness {
        up-count cells;
        down-count cells;
    }
    oam-period (disable | seconds);
    output-vlan-map {
        pop;
        push;
        swap;
        vlan-id number;
        tag-protocol-id tpid;
    }  
    passive-monitor-mode;
    point-to-point;
    service-domain (inside | outside);
    shaping {
        (cbr rate | rtvbr peak rate sustained rate burst length | vbr peak rate sustained rate burst length);
        queue-length number;
    }  
    short-sequence;
    transmit-weight number;
    (traps | no-traps);
tunnel {
    backup-destination address;
    destination destination-address;
    routing-instance destination routing-instance-name;
    source source-address;
    ttl number;
}

vci vpi-identifier.vci-identifier;
vlan-id number;
vlan-tag [tpid.vlan-id];
family family {
    accounting {
        destination-class-usage;
        source-class-usage {
            (input | output | [input output]);
        }
    }
    bundle (ml-fpc/ pic/ port | ls-fpc/ pic/ port);
    filter {
        input filter-name;
        output filter-name;
        group filter-group-number;
    }
    ipsec-sa sa-name;
    keep-address-and-control;
    mtu bytes;
    multicasts-only;
    no-asynchronous-notification;
    no-redirects;
    policer {
        arp policer-template-name;
        input policer-template-name;
        output policer-template-name;
    }
    primary;
    proxy inet-address address;
    remote (inet-address address | mac-address address);
    rpf-check <fail-filter filter-name> {
        <mode loose>;
    }
    sampling {
        [ input output ];
    }
    service {
        input {
            [ service-set service-set-name <service-filter filter-name> ];
            post-service-filter filter-name;
        }
        output {
            [ service-set service-set-name <service-filter filter-name> ];
        }
    }
    (translate-discard-eligible | no-translate-discard-eligible);
    (translate-fecn-and-becn | no-translate-fecn-and-becn);
address address {
    arp ip-address (mac | multicast-mac) mac-address <publish>;
    destination destination-address;
    eui-64;
    broadcast address;
    multipoint-destination destination-address (dlci dlci-identifier | vci vci-identifier);
    multipoint-destination destination-address {
        epd-threshold cells;
        inverse-arp;
        oam-liveness {
            up-count cells;
            down-count cells;
        }
        oam-period seconds;
        shaping {
            (cbr rate | rtvbr peak rate sustained rate burst length | vbr peak rate sustained rate burst length);
            queue-length number;
        }
        vci vpi-identifier.vci-identifier;
    }
    preferred;
    primary;
    vrrp-group group-number {
        virtual-address [addresses];
        priority number;
        (accept-data | no-accept-data);
        advertise-interval seconds;
        authentication-type authentication;
        authentication-key key;
        (preempt | no-preempt);
        track {
            interface interface-name priority-cost cost;
        }
    }
}

interface-switch connection-name {
    interface interface-name.unit-number;
    interface interface-name.unit-number;
}
[edit protocols vrrp] Hierarchy Level

traceoptions {
    file {
        filename filename;
        files number;
        size size;
        (world-readable | no-world-readable);
    }
    flag flag;
}
Part 2. Router Interfaces

- Interfaces Overview on page 19
- Interfaces Configuration Statements on page 29
- Configure Physical Interface Properties on page 39
- Configure Logical Interface Properties on page 67
- Configure Protocol Family and Address Interface Properties on page 77
- Configure Circuit and Translational Cross-Connects on page 99
- Trace Interface Operations on page 107
Chapter 3
Interfaces Overview

For the interfaces on a router to function, you must configure them, specifying properties such as the interface location (that is, which slot the Flexible PIC Concentrator (FPC) is installed in and which location on the FPC the Physical Interface Card (PIC) is installed in), the interface type (such as SONET or ATM), encapsulation, and interface-specific properties. You can configure the interfaces that are currently present in the router, and you can also configure interfaces that are not currently present but that you might add in the future. When a configured interface appears, the JUNOS software detects its presence and applies the appropriate configuration to it.

This chapter discusses the following topics:

- Types of Interfaces on page 19
- Interface Descriptors on page 21
- Interface Naming on page 23
- How Interface Configurations Are Displayed on page 27
- Interface and Router Clock Sources on page 27

Types of Interfaces

Interfaces can be can be permanent or transient, and are used for networking or services:

- Permanent interfaces—Interfaces that are always present in the router.
- Transient interfaces—Interfaces that can be inserted into or removed from the router depending on your network configuration needs.
- Networking interfaces—Interfaces, such as Ethernet or SONET interfaces, that primarily provide traffic connectivity.
- Services interfaces—Interfaces that provide specific capabilities for manipulating traffic before it is delivered to its destination.
Permanent Interfaces

Each router has two permanent interfaces:

- **Management Ethernet interface**—Provides an out-of-band method for connecting to the router. You can connect to the management interface over the network using utilities such as ssh and Telnet. SNMP can use the management interface to gather statistics from the router.

- **Internal Ethernet interface**—Connects the Routing Engine (the portion of the router running the JUNOS Internet software) to the System Control Board (SCB), the System and Switch Board (SSB), the Forwarding Engine Board (FEB), or the System and Forwarding Module (SFM), depending on router model, which is part of the Packet Forwarding Engine. The router uses this interface as the main communications link between the JUNOS software and the components of the Packet Forwarding Engine and runs the embedded microkernel.

  The JUNOS software boots the Packet Forwarding Engine hardware, including the control board (SCB, SSB, FEB, or SFM), FPCs, and PICs. When these components are running, the control board uses the internal Ethernet interface to transmit hardware status information to the JUNOS software. Information transmitted includes the internal router temperature, the condition of the fans, whether an FPC has been removed or inserted, and information from the craft interface on the LCD display panel. The internal Ethernet interface is configured automatically when the JUNOS software boots.

Each router also has two serial ports, labeled **console** and **auxiliary**, for connecting tty-type terminals to the router using standard PC-type tty cables. Although these ports are not network interfaces, they do provide access to the router.

Transient Interfaces

The router contains slots for installing FPC boards, and each FPC can accommodate up to four PICs, which provide the actual physical interfaces to the network. These physical interfaces are the router’s transient interfaces. They are referred to as transient because you can hot-swap an FPC and its PICs at any time.

You can insert any FPC into any of the router’s slots, and you can generally place any combination of PICs in any location on an FPC. (You are limited by the total FPC bandwidth, which cannot exceed the equivalent of an OC-48 link and by the fact that some PICs physically require two or four of the PIC locations on the FPC.)

You must configure each of the transient interfaces based on the slot in which the FPC is installed, the location in which the PIC is installed, and for some PICs, the port to which you are connecting.

You can configure the interfaces on PICs that are already installed in the router as well as interfaces on PICs that you plan to install later. The JUNOS software detects which interfaces are actually present, so when the software activates its configuration, it activates only present interfaces and retains the configuration information for the interfaces that are not present. When the JUNOS software detects that an FPC containing PICs has been inserted into the router, the software activates the configuration for those interfaces.
Interfaces Overview

Services Interfaces

Services interfaces enable you to incrementally add services to your network. The JUNOS software supports the following services PICs:

- **ES PIC**—Provides a security suite for the IPv4 and IPv6 network layers. The suite provides functionality such as authentication of origin, data integrity, confidentiality, replay protection, and non-repudiation of source. It also defines mechanisms for key generation and exchange, management of security associations, and support for digital certificates.

- **Multilink Services and Link Services PICs**—Enable you to split, recombine, and sequence datagrams across multiple logical data links. The goal of multilink operation is to coordinate multiple independent links between a fixed pair of systems, providing a virtual link with greater bandwidth than any of the members. The JUNOS software supports two multilink-based services PICs: the Multilink Services PIC and the Link Services PIC.

- **Monitoring Services PIC**—Enables you to monitor traffic flow and export the monitored traffic. Monitoring traffic allows you to gather and export detailed information about IPv4 traffic flows between source and destination nodes in your network; sample all incoming IPv4 traffic on the monitoring interface and present the data in cflowd record format; perform discard accounting on an incoming traffic flow; encrypt or tunnel outgoing cflowd records, intercepted IPv4 traffic, or both; and direct filtered traffic to different packet analyzers and present the data in its original format.

- **Tunnel Services PIC**—By encapsulating arbitrary packets inside a transport protocol, tunneling provides a private, secure path through an otherwise public network. Tunnels connect discontinuous subnetworks and enable encryption interfaces, virtual private networks (VPNs), and Multiprotocol Label Switching (MPLS).

For detailed information about configuring services, see the JUNOS Internet Software Configuration Guide: Services Interfaces.

Interface Descriptors

When you configure an interface, you are effectively specifying the properties for a physical interface descriptor. In most cases, the physical interface descriptor corresponds to a single physical device and consists of the following parts:

- The interface name, which defines the media type
- The slot in which the FPC is located
- The location on the FPC in which the PIC is installed
- The PIC port
- The interface’s channel and logical unit numbers (optional)

Each physical interface descriptor can contain one or more logical interface descriptors. These allow you to map one or more logical (or virtual) interfaces to a single physical device. Creating multiple logical interfaces is useful for ATM, Frame Relay, and Gigabit Ethernet networks, in which you can associate multiple virtual circuits, data-link connections, or VLANs with a single interface device.
Each logical interface descriptor can have one or more family descriptors to define the protocol family that is associated with and allowed to run over the logical interface. The following protocol families are supported:

- Internet Protocol, version 4 (IPv4)
- Internet Protocol, version 6 (IPv6)
- Circuit cross-connect (CCC)
- Translational cross-connect (TCC)
- International Organization for Standardization (ISO)
- Multilink Frame Relay End-to-End (MLFR End-to-End)
- Multilink Frame Relay UNI NNI (MLFR UNI NNI)
- Multilink PPP (MLPPP)
- Multiprotocol Label Switching (MPLS)
- Trivial Network Protocol (TNP)
- Virtual Private LAN Service (VPLS)

Finally, each family descriptor can have one or more address entries, which associate a network address with a logical interface and hence with the physical interface.

You configure the various interface descriptors as follows:

- You configure the physical interface descriptor by including the interfaces interface-name statement.
- You configure the logical interface descriptor by including the unit statement within the interfaces interface-name statement or by including the logical descriptor at the end of the interface name, as in ge-0/0/0.1 where the logical unit number is 1.
- You configure the family descriptor by including the family statement within the family statement.
- You configure address entries by including the address statement within the family statement.
- You configure tunnels by including the tunnel statement within the unit statement.
Interface Naming

Each interface has an interface name, which specifies the media type, the slot the FPC is located in, the location on the FPC that the PIC is installed in, and the PIC port. The interface name uniquely identifies an individual network connector in the system. You use the interface name when configuring interfaces and when enabling various functions and properties, such as routing protocols, on individual interfaces. The system uses the interface name when displaying information about the interface, for example, in the show interfaces command.

The interface name is represented by a physical part, a channel part, and a logical part in the following format:

physical:<channel>.logical

The channel part of the name is optional for all interfaces except Channelized DS-3, E1, OC-12, and STM-1 interfaces.

The following sections provide interface naming configuration guidelines:

- Physical Part of an Interface Name on page 23
- Logical Part of an Interface Name on page 25
- Separators in an Interface Name on page 25
- Channel Part of an Interface Name on page 26
- Examples: Interface Naming on page 26

Physical Part of an Interface Name

The physical part of an interface name identifies the physical device, which corresponds to a single physical network connector. This part of the interface name has the following format:

type-fpc/pic/port

type is the media type, which identifies the network device. It can be one of the following:

- ae—Aggregated Ethernet interface. This is actually a virtual aggregated link and has a different naming format; for more information, see “Configure Aggregated Interfaces” on page 45.
- as—Aggregated SONET/SDH interface. This is actually a virtual aggregated link and has a different naming format; for more information, see “Configure Aggregated Interfaces” on page 45.
- at—ATM 1 or ATM 2 interface.
- cau4—Channelized STM-1 QPP interface (configured on Channelized STM-1 PIC with QPP).
- coc1—Channelized OC-1 QPP interface (configured on Channelized OC-12 PIC with QPP).
- coc12—Channelized OC-12 QPP interface (configured on Channelized OC-12 PIC with QPP).
- cstm1—Channelized STM-1 QPP interface (configured on Channelized STM-1 PIC with QPP).
- ct1—Channelized T1 QPP interface (configured on Channelized DS-3 PIC with QPP or Channelized OC-12 PIC with QPP).
- ct3—Channelized T3 QPP interface (configured on Channelized DS-3 PIC with QPP or Channelized OC-12 PIC with QPP).
- cel—Channelized E1 QPP interface (configured on Channelized E1 PIC with QPP or Channelized STM-1 PIC with QPP).
- ds—DS-0 interface (configured on Channelized DS-3 to DS-0 PIC, Channelized E1 PIC, Channelized OC-12 PIC with QPP, Channelized DS-3 PIC with QPP, Channelized E1 PIC with QPP, or Channelized STM-1 PIC with QPP).
- dsc—Discard interface.
- e1—E1 interface (including Channelized STM-1 to E1 interfaces).
- e3—E3 interface.
- es—Encryption interface.
- fe—Fast Ethernet interface.
- fxp—Management and internal Ethernet interfaces.
- ge—Gigabit Ethernet interface.
- gr—Generic Route Encapsulation tunnel interface.
- gre—This interface is internally generated and not configurable.
- ip—IP-over-IP encapsulation tunnel interface.
- ipip—This interface is internally generated and not configurable.
- lo—Loopback interface.
- ls—Link services interface.
- lsi—This interface is internally generated and not configurable.
- ml—Multilink interface (including Multilink Frame Relay and Multilink PPP).
- mo—Monitoring services interface (including monitoring services and monitoring services II).
- mt—Multicast tunnel interface (internal router interface for VPNs).
- mtun—This interface is internally generated and not configurable.
- oc3—OC-3 QPP interface (configured on Channelized OC-12 PIC with QPP).
- **pe**—Encapsulates packets destined for the Rendezvous Point (RP) router. This interface is present on the first-hop router.

- **pd**—De-encapsulates packets at the RP. This interface is present on the RP.

- **pimd**—This interface is internally generated and not configurable.

- **prime**—This interface is internally generated and not configurable.

- **se**—Serial interface (including EIA-530, V.35, and X.21 interfaces).

- **so**—SONET/SDH interface.

- **sp**—Adaptive services interface.

- **t1**—T1 interface (including Channelized DS-3 to DS-1 interfaces).

- **t3**—T3 interface (including Channelized OC-12 to DS-3 interfaces).

- **tap**—This interface is internally generated and not configurable.

- **vt**—Virtual loopback tunnel interface.

**fpc** identifies the number of the FPC card on which the physical interface is located. Specifically, it is the number of the slot in which the FPC card is installed. M40, M40e, M160, T320, and T640 platforms each have eight FPC slots that are numbered 0 through 7, from left to right as you are facing the front of the chassis. The M20 router has four FPC slots that are numbered 0 through 3, from top to bottom as you are facing the front of the chassis. The slot number is printed adjacent to each slot. M5 and M10 routers do not use FPCs; you install the PICs individually. The M5 router has space for up to four PICs, and the M10 router has space for up to eight PICs.

**pic** identifies the number of the PIC card on which the physical interface is located. Specifically, it is the number of the PIC location on the FPC. The four PIC slots are numbered 0 through 3. The PIC location is printed on the FPC carrier board. For PICs that occupy more than one PIC location, use the lower location number.

**port** identifies a specific port on a PIC. The number of ports varies depending on the PIC. The port slot numbers are printed on the PIC.

### Logical Part of an Interface Name

The logical unit part of the interface name corresponds to the logical unit number, which can be a number in the range 0 through 16384.

### Separators in an Interface Name

There is a separator between each element of an interface name.

In the physical part of the name, a hyphen (-) separates the media type from the FPC number, and a slash (/) separates the FPC, PIC, and port numbers.

In the virtual part of the name, a period (.) separates the channel and logical unit numbers.

A colon (:) separates the physical and virtual parts of the interface name.
Channel Part of an Interface Name

The channel identifier part of the interface name is required only on channelized interfaces. For channelized interfaces, channel 0 identifies the first channelized interface. For channelized QPP interfaces, channel 1 identifies the first channelized interface. A nonconcatenated (that is, channelized) SONET/SDH OC-48 interface has four OC-12 channels, numbered 0 through 3.

To determine which types of channelized PICs are currently installed in the router, use the show chassis hardware command from the top level of the CLI. Channelized PICs with QPP are listed in the output with “QPP” in the description. For more information, see “Channelized Interfaces Overview” on page 163.

Examples: Interface Naming

This section provides examples of naming interfaces. See Figure 1 for an illustration of where slots, PICs, and ports are located.

Figure 1: Interface Slot, PIC, and Port Locations

For an FPC in slot 1 with two OC-3 SONET PICs in PIC positions 0 and 1, each PIC with two ports uses the following names:

- so-1/0/0.0
- so-1/0/1.0
- so-1/1/0.0
- so-1/1/1.0
An OC-48 SONET FPC in slot 1 and in concatenated mode appears as a single FPC with a single PIC, which has a single port. If this interface has a single logical unit, the name is:

```
so-1/0/0.0
```

An OC-48 SONET FPC in slot 1 and in channelized mode has a number for each channel. For example:

```
so-1/0/0:0
so-1/0/0:1
```

For an FPC in slot 1 with a Channelized OC-12 PIC in PIC position 2, the DS-3 channels are named:

```
t3-1/2/0:0
t3-1/2/0:1
t3-1/2/0:2
...
t3-1/2/0:11
```

For an FPC in slot 1 with four OC-12 ATM PICs (the FPC is fully populated), the four PICs, each with a single port and a single logical unit, have the following names:

```
at-1/0/0.0
at-1/1/0.0
at-1/2/0.0
at-1/3/0.0
```

**How Interface Configurations Are Displayed**

When you display a configuration, using either the `show` command in configuration mode or the `show configuration` top-level command, interfaces are listed in numerical order, from lowest to highest slot number, then from lowest to highest PIC number, and finally from lowest to highest port number.

**Interface and Router Clock Sources**

When configuring the router, you can configure the transmit clock on each interface; the transmit clock aligns each outgoing packet transmitted over the router’s interfaces. For both the router and interfaces, the clock source can be the router’s internal stratum 3 clock, which resides on the SCB, SSB, FEB, or MCS (depending on the router model), or an external clock that is received from the interface you are configuring. For example, interface A can transmit on interface A’s received clock (external, loop timing) or the stratum 3 clock (internal, line timing). Interface A cannot use a clock from any other source.

By default, each interface uses the router’s internal stratum 3 clock. To configure the clock source of each interface, include the `clocking` statement at the [edit interfaces interface-name] hierarchy level:

```
[edit interfaces interface-name]
clocking (internal | external);
```

Figure 2 illustrates the different clock sources.
Figure 2: Clock Sources

System reference clock

SCB
Stratum 3

From SCB

Per-interface clock
Configure with set interfaces clocking

PIC

External clock (loop timing)

Receive clock
Transmit clock
Transmitted bits

Internal clock (line timing, or normal)
When configuring the interfaces, you can configure the interfaces that are currently present in the router (that is, the PICs that are already installed in the router) as well as interfaces that you might be adding at some future time (that is, PICs that you plan to install). To determine which interfaces are currently installed in the router, use the `show interfaces terse` command from the top-level CLI. If an interface is listed in the output, it is installed in the router. If an interface is not listed, it is not present.

The router software automatically configures the router’s management Ethernet interface, fxp0, which is an out-of-band management interface, and the internal Ethernet interface, fxp1, which connects the Routing Engine to the control board (System Control Board (SCB), System and Switch Board (SSB), Forwarding Engine Board (FEB), or Switching and Forwarding Module (SFM)). The JUNOS software also automatically configures one loopback interface (lo0). If your router has a Tunnel PIC, the JUNOS software automatically configures one multicast tunnel interface (mt) for each VPN you configure. You do not need to configure multicast tunnel interfaces.

**Complete Interfaces Configuration Statements**

To configure router interfaces, you include statements at the `edit interfaces` hierarchy level of the configuration:

```
interfaces {
  traceoptions {
    file filename <files number> <size size> <world-readable | no-world-readable>;
    flag flag <disable>;
  }
  interface-name {
    disable;
    accounting-profile name;
    description text;
    aggregated-ether-options {
      (flow-control | no-flow-control);
      link-speed speed;
      (loopback | no-loopback);
      minimum-links number;
      source-address-filter {
        mac-address;
      }
      (source-filtering | no-source-filtering);
    }
}
```

aggregated-sonet-options {
  link-speed speed;
  minimum-links number;
}

atm-options {
  cell-bundle-size cells;
  ilmi;
  linear-red-profiles profile-name {
    high-pip-max-threshold percent;
    low-pip-max-threshold percent;
    queue-depth cells high-pip-threshold percent low-pip-threshold percent;
  }
  pic-type (atm1 | atm2);
  promiscuous-mode {
    [vpi vpi-identifier];
  }
  scheduler-maps map-name {
    forwarding-class class-name {
      priority (low | high);
      transmit-weight (cells number | percent number);
      (epd-threshold cells | linear-red-profile profile-name);
    }
  vc-cos-mode (alternate | strict);
  }
  vpi vpi-identifier {
    maximum-vcs maximum-vcs;
    oam-liveness {
      up-count cells;
      down-count cells;
    }
    oam-period (disable | seconds);
    shaping {
      (cbr rate | rtvbr peak rate sustained rate burst length | vbr peak rate sustained rate burst length);
      queue-length number;
    }
  }
  clocking clock-source;
  dce;
  ds0-options {
    bert-algorithm algorithm;
    bert-error-rate rate;
    bert-period seconds;
    byte-encoding (nx64 | nx56);
    fcs (32 | 16);
    idle-cycle-flag (flags | ones);
    invert-data;
    loopback (payload | remote);
    start-end-flag (shared | filler);
  }
Interfaces Configuration Statements

```
e1-options {
  bert-error-rate rate;
  bert-period seconds;
  fcs (32 | 16);
  framing (g704 | g704-no-crc4 | unframed);
  idle-cycle-flag (flags | ones);
  invert-data;
  loopback (local | remote);
  start-end-flag (shared | filler);
  timeslots time-slot-range;
}
e3-options {
  atm-encapsulation (direct | PLCP);
  bert-algorithm algorithm;
  bert-error-rate rate;
  bert-period seconds;
  compatibility-mode (digital-link | kentrox | larscom) <subrate value>;
  fcs (32 | 16);
  idle-cycle-flag value;
  loopback (local | remote);
  (payload-scrambler | no-payload-scrambler);
  start-end-flag value;
}
encapsulation type;
es-options {
  backup-interface es-fpc/pic/port;
}
fastether-options {
  802.3ad ae;
  (flow-control | no-flow-control);
  ingress-rate-limit rate;
  (loopback | no-loopback);
  source-address-filter {
    mac-address;
  }
  (source-filtering | no-source-filtering);
}
gigether-options {
  802.3ad ae;
  (flow-control | no-flow-control);
  (loopback | no-loopback);
  source-address-filter {
    mac-address;
  }
  (source-filtering | no-source-filtering);
  ethernet-switch-profile {
    ethernet-policer-profile {
      ieee802.1-priority-map premium [ bits ];
    }
  }
```
policer cos-policer-name {
    aggregate {
        bandwidth-limit rate;
        bandwidth-percent percent;
        burst-size-limit length;
    }
    premium {
        bandwidth-limit rate;
        bandwidth-percent percent;
        burst-size-limit length;
    }
}
(mac-learn-enable | no-mac-learn-enable);
tag-protocol-id [ tpids ];
(gratuitous-arp-reply | no-gratuitous-arp-reply);
hold-time up milliseconds down milliseconds;
keepalives <down-count number> <interval seconds> <up-count number>;
link-mode mode;
lmi {
    lmi-type (ansi | itu);
n391dte number;
n392dce number;
n392dte number;
n393dce number;
n393dte number;
t391dte seconds;
t392dce seconds;
}
mac mac-address;
mlfr-uni:nni-bundle-options {
    acknowledge-retries number;
    acknowledge-timer milliseconds;
    action-red-differential-delay (disable-tx | remove-link);
    drop-timeout milliseconds;
    fragment-threshold bytes;
    hello-timer milliseconds;
    lmi-type (ansi | itu);
    minimum-links number;
    mrru bytes;
n391 number;
n392 number;
n393 number;
    red-differential-delay milliseconds;
t391 seconds;
t392 seconds;
    yellow-differential-delay milliseconds;
}
mtu bytes;
multiservice-options {
    boot-command filename;
    (core-dump | no-core-dump);
    (syslog | no-syslog);
}
(gratuitous-arp-request | no-gratuitous-arp-request);
no-keepalives;
no-partition {
    interface-type type;
}
partition partition-number oc-slice oc-slice-range interface-type type {
    timeslots time-slot-range;
}

  passive-monitor-mode;
  per-unit-scheduler;
  ppp-options {
    chap {
      access-profile name;
      local-name name;
      passive;
    }
  }
  receive-bucket {
    overflow (tag | discard);
    rate percentage;
    threshold bytes;
  }

  serial-options {
    clock-rate rate;
    clocking-mode (dce | dte | loop);
    control-leads {
      control-signal (assert | de-assert | normal);
      cts (ignore | normal | require);
      dcd (ignore | normal | require);
      dsr (ignore | normal | require);
      dtr signal-handling-option;
      ignore-all;
      indication (ignore | normal | require);
      rts (assert | de-assert | normal);
      tm (ignore | normal | require);
    }
    control-polarity (positive | negative);
    cts-polarity (positive | negative);
    dcd-polarity (positive | negative);
    dsr-polarity (positive | negative);
    dtr-circuit (balanced | unbalanced);
    dtr-polarity (positive | negative);
    encoding (nrz | nrzi);
    indication-polarity (positive | negative);
    line-protocol protocol;
    loopback mode;
    rts-polarity (positive | negative);
    tm-polarity (positive | negative);
    transmit-clock invert;
  }

  service-options {
    inactivity-timeout seconds;
    open-timeout seconds;
    syslog {
      host host-name {
        facility-override facility-name;
        log-prefix prefix-number;
        [ services priority-level ];
      }
    }
  }
}
sonet-options {
  aggregate asx;
  aps {
    advertise-interval milliseconds;
    authentication-key key;
    force;
    hold-time milliseconds;
    lockout;
    neighbor address;
    paired-group group-name;
    protect-circuit group-name;
    request;
    revert-time seconds;
    working-circuit group-name;
  }
  bytes {
    e1-quiet value;
    f1 value;
    f2 value;
    s1 value;
    z3 value;
    z4 value;
  }
  fcs (32 | 16);
  loopback (local | remote);
  path-trace trace-string;
  (payload-scrambler | no-payload-scrambler);
  rfc-2615;
  vtmapping (itu-t | klm);
  (z0-increment | no-z0-increment);
}
speed (10m | 100m);
stacked-vlan-tagging;
t1-options {
  bert-algorithm algorithm;
  bert-error-rate rate;
  bert-period seconds;
  buildout (0-132 | 133-265 | 266-398 | 399-531 | 532-655);
  byte-encoding (nx64 | nx56);
  fcs (32 | 16);
  framing (sf | esf);
  idle-cycle-flag (flags | ones);
  invert-data;
  line-encoding (ami | b8zs);
  loopback (local | payload | remote);
  remote-loopback-respond;
  start-end-flag (shared | filler);
  timeslots time-slot-range;
}
t3-options {
    atm-encapsulation (direct | PLCP);
    bert-algorithm algorithm;
    bert-error-rate rate;
    bert-period seconds;
    (cbit-parity | no-cbit-parity);
    compatibility-mode (adtran | digital-link | kentrox | larscom | verilink) <subrate value>;
    fcs (32 | 16);
    (feac-loop-respond | no-feac-loop-respond);
    idle-cycle-flag value;
    (long-buildout | no-long-buildout);
    loopback (local | payload | remote);
    (mac | no-mac);
    (payload-scrambler | no-payload-scrambler);
    start-end-flag value;
}
traceoptions {
    flag flag <flag-modifier> <disable>;
}
transmit-bucket {
    overflow discard;
    rate percentage;
    threshold bytes;
}
(traps | no-traps);
vlan-tagging;
unit logical-unit-number {
    accept-source-mac {
        mac-address mac-address {
            policer {
                input policer-name;
                output policer-name;
            }
        }
    }
}
accounting-profile name;
allow-any-vci;
bandswidth rate;
cell-bundle-size cells;
description text;
disable;
dlci dlci-identifier;
drop-timeout milliseconds;
encapsulation type;
epd-threshold cells;
fragment-threshold bytes;
input-vlan-map {
    pop;
    push;
    swap;
    vlan-id number;
    tag-protocol-id tpid;
}
interleave-fragments;
inverse-arp;
minimum-links number;
mrru bytes;
multicast-dlci dlci-identifier;
multicast-vci vpi-identifier.vci-identifier;
multipoint;
oam-liveness {
  up-count cells;
  down-count cells;
}
oam-period (disable | seconds);
output-vlan-map {
  pop;
  push;
  swap;
  vlan-id number;
  tag-protocol-id tpid;
}
passive-monitor-mode;
point-to-point;
shaping {
  (cbr rate | rtvbr peak rate sustained rate burst length | vbr peak rate sustained rate burst length);
  queue-length number;
}
short-sequence;
transmit-weight number;
(traps | no-traps);
tunnel {
  backup-destination address;
  source source-address;
  destination destination-address;
  routing-instance {
    destination routing-instance-name;
  }
  ttl number;
}
vc vpi-identifier.vci-identifier;
vlan-id number;
vlan-tag [ tpid.vlan-id ];
family family {
  accounting {
    destination-class-usage;
    source-class-usage {
      (input | output | [input output]);
    }
  }
  bundle (ml-fpc/ pic/ port | ls-fpc/ pic/ port);
  filter {
    input filter-name;
    output filter-name;
    group filter-group-number;
  }
ipsec-sa sa-name;
keep-address-and-control;
mtu bytes;
multicasts-only;
no-asynchronous-notification;
no-redirects;
policer {
  arp policer-template-name;
  input policer-template-name;
  output policer-template-name;
}
primary;
proxy inet-address address;
remote (inet-address address | mac-address address);
rpf-check <fail-filter filter-name> {
  <mode loose>;
}
sampling {
  [ input output ];
}
service {
  input {
    [ service-set service-set-name <service-filter filter-name> ];
    post-service-filter filter-name;
  }
  output {
    [ service-set service-set-name <service-filter filter-name> ];
  }
}
(translate-discard-eligible | no-translate-discard-eligible);
(translate-fecn-and-becn | no-translate-fecn-and-becn);
address address {
  arp ip-address (mac | multicast-mac) mac-address <publish>;
  destination destination-address;
  eui-64;
  broadcast address;
  multipoint-destination destination-address (dlci dlci-identifier | vci vci-identifier);
  multipoint-destination destination-address {
    epd-threshold cells;
    inverse-arp;
    oam-liveness {
      up-count cells;
      down-count cells;
    }
    oam-period seconds;
    shaping {
      (cbr rate | rtvbr peak rate sustained rate burst length |
        vbr peak rate sustained rate burst length);
      queue-length number;
    }
    vci vpi-identifier.vci-identifier;
  }
  preferred;
  primary;
  vrrp-group group-number {
    virtual-address [addresses];
    priority number;
    (accept-data | no-accept-data);
    advertise-interval seconds;
    advertisement-type authentication;
    authentication-key key;
    (preempt | no-preempt);
    track {
      interface interface-name priority-cost cost;
    }
  }
}
Minimum Interface Configuration

For your router to function properly, you must configure each PIC interface that is present in the router. No PIC interfaces are preconfigured.
Chapter 5
Configure Physical Interface Properties

The software driver for each network media type sets reasonable default values for general interface properties, such as the interface’s maximum transmission unit (MTU) size, receive and transmit leaky bucket properties, link operational mode, and clock source. To modify any of the default general interface properties, include the appropriate statements at the [edit interfaces interface-name] hierarchy level:

interfaces {
  interface-name {
    accounting-profile name;
    aggregated-ether-options {
      aggregated-ether-interface-options;
    }
    aggregated-sonet-options {
      aggregated-sonet-interface-options;
    }
    atm-options {
      atm-interface-options;
    }
    clocking clock-source;
    dce;
    description text;
    disable;
    ds0-options {
      ds0-interface-options;
    }
    e1-options {
      e1-interface-options;
    }
    e3-options {
      e3-interface-options;
    }
    es-options {
      es-interface-options;
    }
    encapsulation type;
    fastether-options {
      fastether-interface-options;
    }
    gigether-options {
      gigether-interface-options;
    }
    (gratuitous-arp-reply | no-gratuitous-arp-reply);
    hold-time up milliseconds down milliseconds;
    keepalives <down-count number> <interval seconds> <up-count number>;
    link-mode mode;
lmi {
    lmi-type (ansi | itu);
    n391.dte number;
    n392.dce number;
    n392.dte number;
    n393.dce number;
    n393.dte number;
    t391.dte seconds;
    t392.dce seconds;
}
mac mac-address;
mtu bytes;
multiservice-options {
    boot-command filename;
    (core-dump | no-core-dump);
    (syslog | no-syslog);
}
no-gratuitous-arp-request;
nk-keepalives;
nk-partition {
    interface-type type;
}
partition partition-number oc-slice oc-slice-range interface-type type {
    timeslots time-slot-range;
}
passive-monitor-mode;
per-unit-scheduler;
ppp-options {
    chap {
        access-profile name;
        local-name name;
        passive;
    }
}
receive-bucket {
    overflow (tag | discard);
    rate percentage;
    threshold bytes;
}
serial-options {
    serial-interface-options;
}
service-options {
    service-interface-options;
}
sonet-options {
    sonet-interface-options;
}speed (10m | 100m);
stacked-vlan-tagging;
t1-options {
    t1-interface-options;
}
t3-options {
    t3-interface-options;
}traceoptions {
    flag flag <flag-modifier> <disable>;
transmit-bucket {
    overflow discard;
    rate percentage;
    threshold bytes;
}
(traps | no-traps);
unit {
    logical-interface-statements;
}
vlan-tagging;
}

This chapter discusses configuration of the following physical interface properties:

- Configure Aggregated Interfaces on page 45
- Add an Interface Description to the Configuration on page 46
- Configure the Link Characteristics on page 46
- Configure the Media MTU on page 47
- Configure Interface Encapsulation on page 51
- Configure PPP Challenge Handshake Authentication Protocol on page 55
- Configure the Interface Speed on page 57
- Configure Keepalives on page 58
- Configure the Clock Source on page 59
- Configure the Router as a DCE on page 59
- Configure Receive and Transmit Leaky Bucket Properties on page 60
- Configure Accounting for the Physical Interface on page 61
- Configure BERT Properties on page 62
- Trace Operations of an Individual Router Interface on page 64
- Damp Interface Transitions on page 64
- Configure Multiservice Physical Interface Properties on page 65
- Enable or Disable SNMP Notifications on Physical Interfaces on page 65
- Disable a Physical Interface on page 65

For information about interface-specific physical properties, see “Interface Types” on page 109.

Table 2 lists statements that you can use to configure physical interfaces.
Table 2: Statements for Physical Interface Properties

<table>
<thead>
<tr>
<th>Statement</th>
<th>Interface Types</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>access-profile name</td>
<td>Interfaces with PPP encapsulation</td>
<td>“Configure PPP Challenge Handshake Authentication Protocol” on page 55</td>
</tr>
<tr>
<td>accounting-profile</td>
<td>All</td>
<td>“Configure Accounting for the Physical Interface” on page 61</td>
</tr>
<tr>
<td>acknowledge-retries</td>
<td>Link services interface</td>
<td>“Configure Link Services Acknowledgment Timers” on page 329</td>
</tr>
<tr>
<td>acknowledge-timer</td>
<td>Link services interface</td>
<td>“Configure Link Services Acknowledgment Timers” on page 329</td>
</tr>
<tr>
<td>aggregated-ether-options</td>
<td>Aggregated Ethernet interfaces</td>
<td>“Configure Aggregated Ethernet Interfaces” on page 299</td>
</tr>
<tr>
<td>aggregated-sonet-options</td>
<td>Aggregated SONET/SDH interfaces</td>
<td>“Configure Aggregated SONET/SDH Interfaces” on page 380</td>
</tr>
<tr>
<td>atm-options</td>
<td>ATM 1 and ATM 2 interfaces</td>
<td>“Configure ATM 1 and ATM 2 Physical Interface Properties” on page 125</td>
</tr>
<tr>
<td>boot-command filename</td>
<td>Monitoring services interfaces</td>
<td>“Configure Multiservice Physical Interface Properties” on page 65</td>
</tr>
<tr>
<td>chap</td>
<td>Interfaces with PPP encapsulation types</td>
<td>“Configure PPP Challenge Handshake Authentication Protocol” on page 55</td>
</tr>
<tr>
<td>clock-rate</td>
<td>Serial interfaces (EIA-530 and V.35)</td>
<td>“Configure the DTE Clock Rate” on page 351</td>
</tr>
<tr>
<td>clocking-mode</td>
<td>Serial interfaces (EIA-530 and V.35)</td>
<td>“Configure the Serial Clocking Mode” on page 350</td>
</tr>
<tr>
<td>clocking clock-source</td>
<td>ATM, DS-0, E1, E3, SONET/SDH, T1, and T3 interfaces</td>
<td>“Configure the Clock Source” on page 59</td>
</tr>
<tr>
<td>control-leads</td>
<td>Serial interfaces (EIA-530, V.35, and X.21)</td>
<td>“Configure the Serial Signal Handling” on page 352</td>
</tr>
<tr>
<td>control-polarity</td>
<td>Serial interfaces (X.21)</td>
<td>“Configure Serial Signal Polarities” on page 355</td>
</tr>
<tr>
<td>control-signal</td>
<td>Serial interfaces (X.21)</td>
<td>“Configure the Serial Signal Handling” on page 352</td>
</tr>
<tr>
<td>(core-dump</td>
<td>no-core-dump)</td>
<td>Monitoring services interfaces</td>
</tr>
<tr>
<td>cts (ignore</td>
<td>normal</td>
<td>require)</td>
</tr>
<tr>
<td>cts-polarity</td>
<td>Serial interfaces (EIA-530 and V.35)</td>
<td>“Configure Serial Signal Polarities” on page 355</td>
</tr>
<tr>
<td>dcd (ignore</td>
<td>normal</td>
<td>require)</td>
</tr>
<tr>
<td>dcd-polarity</td>
<td>Serial interfaces (EIA-530 and V.35)</td>
<td>“Configure Serial Signal Polarities” on page 355</td>
</tr>
<tr>
<td>dce</td>
<td>Interfaces with Frame Relay encapsulation</td>
<td>“Configure the Router as a DCE” on page 59</td>
</tr>
<tr>
<td>description text</td>
<td>All</td>
<td>“Add an Interface Description to the Configuration” on page 46</td>
</tr>
<tr>
<td>disable</td>
<td>All</td>
<td>“Disable a Physical Interface” on page 65</td>
</tr>
<tr>
<td>ds0-options</td>
<td>DS-0 interfaces</td>
<td>“Channelized Interfaces Overview” on page 163</td>
</tr>
<tr>
<td>dsr (ignore</td>
<td>normal</td>
<td>require)</td>
</tr>
<tr>
<td>Statement</td>
<td>Interface Types</td>
<td>Usage Guidelines</td>
</tr>
<tr>
<td>----------------------------------------</td>
<td>---------------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>dsr-polarity (positive</td>
<td>negative)</td>
<td>Serial interfaces (EIA-530 and V.35)</td>
</tr>
<tr>
<td>dtr signal-handling-option</td>
<td>Serial interfaces (EIA-530 and V.35)</td>
<td>“Configure the Serial Signal Handling” on page 352</td>
</tr>
<tr>
<td>dtr-circuit (balanced</td>
<td>unbalanced)</td>
<td>Serial interfaces (EIA-530 and V.35)</td>
</tr>
<tr>
<td>dtr-polarity (positive</td>
<td>negative)</td>
<td>Serial interfaces (EIA-530 and V.35)</td>
</tr>
<tr>
<td>e1-options</td>
<td>E1 interfaces</td>
<td>“Configure E1 Interfaces” on page 243</td>
</tr>
<tr>
<td>e3-options</td>
<td>E3 interfaces</td>
<td>“Configure E3 Interfaces” on page 251</td>
</tr>
<tr>
<td>es-options</td>
<td>ES interfaces</td>
<td>“Configure ES PIC Redundancy” on page 259</td>
</tr>
<tr>
<td>encapsulation type</td>
<td>All interface types except aggregated Ethernet, loopback, and multicast tunnel</td>
<td>“Configure Interface Encapsulation” on page 51</td>
</tr>
<tr>
<td>encoding (nrz</td>
<td>nrzi)</td>
<td>Serial interfaces (EIA-530, V.35, and X.21)</td>
</tr>
<tr>
<td>fastether-options</td>
<td>Fast Ethernet interfaces</td>
<td>“Configure Ethernet Physical Interface Properties” on page 264</td>
</tr>
<tr>
<td>gigether-options</td>
<td>Gigabit Ethernet interfaces</td>
<td>“Configure Ethernet Physical Interface Properties” on page 264</td>
</tr>
<tr>
<td>(gratuitous-arp-reply</td>
<td>no-gratuitous-arp-reply)</td>
<td>Ethernet interfaces</td>
</tr>
<tr>
<td>hold-time up milliseconds down</td>
<td>All interface types except aggregated SONET/SDH, GRE tunnel, and IP tunnel</td>
<td>“Damp Interface Transitions” on page 64</td>
</tr>
<tr>
<td>indication (ignore</td>
<td>normal</td>
<td>require)</td>
</tr>
<tr>
<td>indication-polarity (positive</td>
<td>negative)</td>
<td>Serial interfaces (X.21)</td>
</tr>
<tr>
<td>interface-type type</td>
<td>Channelized QPP interfaces</td>
<td>“Channelized Interfaces Overview” on page 163</td>
</tr>
<tr>
<td>keepalives &lt;down-count number&gt; &lt;interval seconds&gt; &lt;up-count number&gt;</td>
<td>Aggregated SONET/SDH, DS-0, E1, E3, SONET, T1, and T3 interfaces</td>
<td>“Configure Keepalives” on page 58</td>
</tr>
<tr>
<td>line-protocol protocol</td>
<td>Serial interfaces (EIA-530, V.35, and X.21)</td>
<td>“Configure the Serial Line Protocol” on page 347</td>
</tr>
<tr>
<td>link-mode mode</td>
<td>Management Ethernet (fxp0) and Fast Ethernet interfaces</td>
<td>“Configure the Link Characteristics” on page 46</td>
</tr>
<tr>
<td>lmi</td>
<td>Interfaces with Frame Relay encapsulation</td>
<td>“Configure Frame Relay Keepalives” on page 307</td>
</tr>
<tr>
<td>lmi-type (ansi</td>
<td>itu)</td>
<td>Interfaces with Frame Relay encapsulation</td>
</tr>
<tr>
<td>local-name name</td>
<td>Interfaces with PPP encapsulation</td>
<td>“Configure PPP Challenge Handshake Authentication Protocol” on page 55</td>
</tr>
<tr>
<td>Statement</td>
<td>Interface Types</td>
<td>Usage Guidelines</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>--------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>mac mac-address</td>
<td>Management Ethernet interface (fxp0)</td>
<td>“Configure the MAC Address on the Management Ethernet Interface” on page 298</td>
</tr>
<tr>
<td>minimum-links</td>
<td>Multilink and link services interfaces</td>
<td>“Configure Multilink and Link Services Interfaces” on page 319</td>
</tr>
<tr>
<td>mtu bytes</td>
<td>All interface types except Management Ethernet (fxp0), loopback, multilink, and multicast tunnel</td>
<td>“Configure the Media MTU” on page 47</td>
</tr>
<tr>
<td>multiservice-options</td>
<td>Monitoring services interfaces</td>
<td>“Configure Multiservice Physical Interface Properties” on page 65</td>
</tr>
<tr>
<td>no-gratuitous-arp-request</td>
<td>Ethernet interfaces</td>
<td>“Configure Gratuitous ARP” on page 281</td>
</tr>
<tr>
<td>no-keepalives</td>
<td>Interfaces with PPP, Frame Relay, or Cisco HDLC encapsulation</td>
<td>“Configure Keepalives” on page 58</td>
</tr>
<tr>
<td>no-partition partition-number</td>
<td>Channelized QPP interfaces</td>
<td>“Channelized Interfaces Overview” on page 163</td>
</tr>
<tr>
<td>oc-slice oc-slice-range</td>
<td>Channelized OC-12 QPP interfaces</td>
<td>“Configure Channelized OC-12 Interfaces” on page 183</td>
</tr>
<tr>
<td>partition partition-number</td>
<td>Channelized QPP interfaces</td>
<td>“Channelized Interfaces Overview” on page 163</td>
</tr>
<tr>
<td>passive</td>
<td>Interfaces with PPP encapsulation</td>
<td>“Configure PPP Challenge Handshake Authentication Protocol” on page 55</td>
</tr>
<tr>
<td>per-unit-scheduler</td>
<td>QPP interfaces</td>
<td>“Associate a Scheduler with a DLCI or VLAN on a Channelized QPP Interface” on page 597</td>
</tr>
<tr>
<td>passive-monitor-mode</td>
<td>SONET/SDH interfaces</td>
<td>“Enable Passive Monitoring” on page 374</td>
</tr>
<tr>
<td>ppp-options</td>
<td>Interfaces with PPP encapsulation</td>
<td>“Configure PPP Challenge Handshake Authentication Protocol” on page 55</td>
</tr>
<tr>
<td>receive-bucket</td>
<td>All interface types except ATM, Fast Ethernet, and Gigabit Ethernet</td>
<td>“Configure Receive and Transmit Leaky Bucket Properties” on page 60</td>
</tr>
<tr>
<td>rts (assert</td>
<td>de-assert</td>
<td>normal)</td>
</tr>
<tr>
<td>rts-polarity (positive</td>
<td>negative)</td>
<td>Serial interfaces (EIA-530 and V.35)</td>
</tr>
<tr>
<td>serial-options</td>
<td>Serial interfaces (EIA-530, V.35, and X.21)</td>
<td>“Configure Serial Interfaces” on page 345</td>
</tr>
<tr>
<td>sonet-options</td>
<td>SONET interfaces</td>
<td>“Configure SONET/SDH Physical Interface Properties” on page 360</td>
</tr>
<tr>
<td>speed (10m</td>
<td>100m)</td>
<td>Management Ethernet interface (fxp0) and the Fast Ethernet 12-port and 48-port PIC</td>
</tr>
<tr>
<td>stacked-vlan-tagging</td>
<td>Gigabit Ethernet QPP interfaces</td>
<td>“Stack and Rewrite Gigabit Ethernet QPP VLAN Tags” on page 273</td>
</tr>
</tbody>
</table>
Configure Aggregated Interfaces

You specify aggregated interfaces by assigning a number for the aggregated interface. For aggregated Ethernet interfaces, configure aeX as in the following example:

```
[edit interfaces]
ae0 {
    ...
}
```

For aggregated SONET/SDH interfaces, configure asX as in the following example:

```
[edit interfaces]
as0 {
    ...
}
```

The maximum number of aggregated interfaces is 16, and the assigned number can range from 0 through 15. You should not mix SONET and SDH mode on the same aggregated interface.

**Note**

SONET aggregation is proprietary to the JUNOS software and might not work with other software.
For aggregated Ethernet interfaces, you must include the `vlan-tagging` statement at the `[edit interfaces ae]` hierarchy level to complete the association.

For more information, see “Configure Aggregated Ethernet Interfaces” on page 299 and “Configure Aggregated SONET/SDH Interfaces” on page 380.

Add an Interface Description to the Configuration

You can include a text description of each physical interface in the configuration file. Any descriptive text you include is displayed in the output of the `show interfaces` commands, and is also exposed in the `ifAlias` MIB object. It has no impact on the interface's configuration. To add a text description, include the description statement at the `[edit interfaces interface-name]` hierarchy level:

```
[edit interfaces interface-name]
description text;
```

The description can be a single line of text. If the text contains spaces, enclose it in quotation marks.

For information about describing logical units, see “Add a Logical Unit Description to the Configuration” on page 71.

Example: Add an Interface Description to the Configuration

Add a description to a SONET interface:

```
[edit interfaces so-1/1/0]
user@host# set description "BB: phl01 P12/0/0 - local wire"
[edit interfaces so-1/1/0]
user@host# commit
[edit interfaces so-1/1/0]
user@host# exit configuration-mode
cli> show interfaces so-1/1/0
so-1/1/0 {
    physical-interface index 9 snmp-ifindex 10;
    enabled physical-link up;
    description "BB: phl01 P12/0/0 - local wire";
    encapsulation cisco-hdlc;
    ...
```

Configure the Link Characteristics

By default, the router’s management Ethernet interface, `fxp0`, autonegotiates whether to operate in full-duplex or half-duplex mode. Fast Ethernet interfaces can operate in either full-duplex or half-duplex mode, and all other interfaces can operate only in full-duplex mode. For Gigabit Ethernet, the link partner must also be set to full duplex.

To explicitly configure an Ethernet interface to operate in either full-duplex or half-duplex mode, include the `link-mode` statement at the `[edit interfaces interface-name]` hierarchy level:

```
[edit interfaces interface-name]
link-mode (full-duplex | half-duplex);
```
Configure the Media MTU

The default media MTU size used on a physical interface depends on the encapsulation used on that interface. Table 3, Table 4, Table 5, Table 6, and Table 7 list the media MTU sizes by interface type, and Table 8 lists the encapsulation overhead by encapsulation type.

Table 3: Media MTU Sizes by Interface Type for M5, M10, M20, and M40 Routers

<table>
<thead>
<tr>
<th>Interface Type</th>
<th>Default Media MTU (Bytes)</th>
<th>Maximum MTU (Bytes)</th>
<th>Default IP Protocol MTU (Bytes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>ATM</td>
<td>4482</td>
<td>9192</td>
<td>4470</td>
</tr>
<tr>
<td>E1/T1</td>
<td>1504</td>
<td>9192</td>
<td>1500</td>
</tr>
<tr>
<td>E3/T3</td>
<td>4474</td>
<td>9192</td>
<td>4470</td>
</tr>
<tr>
<td>Fast Ethernet</td>
<td>1514</td>
<td>9192</td>
<td>1500 (IPv4)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1497 (ISO)</td>
</tr>
<tr>
<td>Gigabit Ethernet</td>
<td>1514</td>
<td>9192</td>
<td>1500 (IPv4)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1497 (ISO)</td>
</tr>
<tr>
<td>Serial</td>
<td>1504</td>
<td>9192</td>
<td>1500 (IPv4)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1497 (ISO)</td>
</tr>
<tr>
<td>SONET/SDH</td>
<td>4474</td>
<td>9192</td>
<td>4470</td>
</tr>
</tbody>
</table>

Table 4: Media MTU Sizes by Interface Type for M40e Routers

<table>
<thead>
<tr>
<th>Interface Type</th>
<th>Default Media MTU (Bytes)</th>
<th>Maximum MTU (Bytes)</th>
<th>Default IP Protocol MTU (Bytes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>ATM</td>
<td>4482</td>
<td>9192</td>
<td>4470</td>
</tr>
<tr>
<td>E1/T1</td>
<td>1504</td>
<td>4500</td>
<td>1500</td>
</tr>
<tr>
<td>E3/T3</td>
<td>4474</td>
<td>4500</td>
<td>4470</td>
</tr>
<tr>
<td>Fast Ethernet</td>
<td>1514</td>
<td>4500</td>
<td>1500 (IPv4)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1497 (ISO)</td>
</tr>
<tr>
<td>Gigabit Ethernet</td>
<td>1514</td>
<td>9192</td>
<td>1500 (IPv4)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1497 (ISO)</td>
</tr>
<tr>
<td>1- or 2-port</td>
<td>4500</td>
<td>1500 (IPv4)</td>
<td></td>
</tr>
<tr>
<td>4-port</td>
<td>1497 (ISO)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Table 5: Media MTU Sizes by Interface Type for M160 Routers

<table>
<thead>
<tr>
<th>Interface Type</th>
<th>Default Media MTU (Bytes)</th>
<th>Maximum MTU (Bytes)</th>
<th>Default IP Protocol MTU (Bytes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Serial</td>
<td>1504</td>
<td>9192</td>
<td>1500 (IPv4) 1497 (ISO)</td>
</tr>
<tr>
<td>SONET/SDH</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4-port OC-3</td>
<td>4474</td>
<td>4500</td>
<td>4470</td>
</tr>
<tr>
<td>4-port OC-3c</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1-port OC-12</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4-port OC-12</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4-port OC-12c</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1-port OC-48</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2-port OC-3</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2-port OC-3c</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1-port OC-12c</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1-port OC-48c</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1-port OC-192</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1-port OC-192c</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Interface Type Details

- **ATM**: 4482, 9192, 4470
- **E1/T1**: 1504, 4500, 1500
- **E3/T3**: 4474, 4500, 4470
- **Fast Ethernet**: 1514, 4500, 1500 (IPv4) 1497 (ISO)
- **Gigabit Ethernet**: 1514, 9192, 4500, 1500 (IPv4) 1497 (ISO)
- **Serial**: 1504, 9192, 1500 (IPv4) 1497 (ISO)
- **SONET/SDH**: 4474, 9192, 4470
Configure Physical Interface Properties

Table 6: Media MTU Sizes by Interface Type for T320 Platforms

<table>
<thead>
<tr>
<th>Interface Type</th>
<th>Default Media MTU (Bytes)</th>
<th>Maximum MTU (Bytes)</th>
<th>Default IP Protocol MTU (Bytes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>ATM</td>
<td>4482</td>
<td>9192</td>
<td>4470</td>
</tr>
<tr>
<td>Fast Ethernet</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>▪ 4-port</td>
<td>1514</td>
<td>4500</td>
<td>1500 (IPv4)</td>
</tr>
<tr>
<td>▪ 48-port</td>
<td></td>
<td>1532</td>
<td>1497 (ISO)</td>
</tr>
<tr>
<td>Gigabit Ethernet</td>
<td>1514</td>
<td>9192</td>
<td>1500 (IPv4)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1497 (ISO)</td>
</tr>
<tr>
<td>SONET/SDH</td>
<td>4474</td>
<td>9192</td>
<td>4470</td>
</tr>
</tbody>
</table>

Table 7: Media MTU Sizes by Interface Type for T640 Platforms

<table>
<thead>
<tr>
<th>Interface Type</th>
<th>Default Media MTU (Bytes)</th>
<th>Maximum MTU (Bytes)</th>
<th>Default IP Protocol MTU (Bytes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>48-port Fast Ethernet</td>
<td>1514</td>
<td>1532</td>
<td>1500 (IPv4)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1497 (ISO)</td>
</tr>
<tr>
<td>Gigabit Ethernet</td>
<td>1514</td>
<td>9192</td>
<td>1500 (IPv4)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1497 (ISO)</td>
</tr>
<tr>
<td>SONET/SDH</td>
<td>4474</td>
<td>9192</td>
<td>4470</td>
</tr>
</tbody>
</table>

Table 8: Encapsulation Overhead by Encapsulation Type

<table>
<thead>
<tr>
<th>Interface Encapsulation</th>
<th>Encapsulation Overhead (Bytes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>ATM Cell Relay</td>
<td>4</td>
</tr>
<tr>
<td>ATM PVC</td>
<td>12</td>
</tr>
<tr>
<td>Cisco HDLC</td>
<td>4</td>
</tr>
<tr>
<td>Frame Relay</td>
<td>4</td>
</tr>
<tr>
<td>Point-to-Point Protocol</td>
<td>4</td>
</tr>
<tr>
<td>Ethernet over ATM</td>
<td>28</td>
</tr>
<tr>
<td>Ethernet version 2</td>
<td>14</td>
</tr>
<tr>
<td>Ethernet 802.3</td>
<td>17</td>
</tr>
<tr>
<td>802.1Q/Ethernet version 2</td>
<td>18</td>
</tr>
<tr>
<td>802.1Q/Ethernet 802.3</td>
<td>21</td>
</tr>
<tr>
<td>Ethernet CCC and VPLS</td>
<td>4</td>
</tr>
<tr>
<td>Ethernet TCC</td>
<td>18</td>
</tr>
<tr>
<td>Ethernet SNAP</td>
<td>22</td>
</tr>
<tr>
<td>802.1Q/Ethernet SNAP</td>
<td>26</td>
</tr>
<tr>
<td>VLAN CCC and VPLS</td>
<td>4</td>
</tr>
<tr>
<td>Extended VLAN CCC and VPLS</td>
<td>4</td>
</tr>
<tr>
<td>Extended VLAN TCC</td>
<td>22</td>
</tr>
</tbody>
</table>
The default media MTU is calculated as follows:

Default media MTU = Default IP MTU + encapsulation overhead

When you are configuring point-to-point connections, the MTU sizes on both sides of the connections must be the same. Also, when you are configuring point-to-multipoint connections, all interfaces in the subnet must use the same MTU size.

For information about configuring the encapsulation on an interface, see “Configure Interface Encapsulation” on page 51.

To modify the default media MTU size for a physical interface, include the mtu statement at the [edit interfaces interface-name] hierarchy level:

```
[edit interfaces interface-name]
mtu bytes;
```

If you change the size of the media MTU, you must ensure that the size is equal to or greater than the sum of the protocol MTU and the encapsulation overhead. You configure the protocol MTU by including the mtu statement at the [edit interfaces interface-name unit logical-unit-number family family] hierarchy level, as discussed in “Set the Protocol MTU” on page 83.
Configure Interface Encapsulation

Point-to-Point Protocol (PPP) encapsulation is the default encapsulation type for physical interfaces. You need not configure encapsulation for any physical interfaces that support PPP encapsulation. If you do not configure encapsulation, PPP is used by default. For physical interfaces that do not support PPP encapsulation, you must configure an encapsulation to use for packets transmitted on the interface.

You can optionally configure an encapsulation on a logical interface, which is the encapsulation used within certain packet types. For more information about logical interface encapsulation, see “Configure the Encapsulation on a Logical Interface” on page 75.

This section is organized as follows:

- Configure the Encapsulation on a Physical Interface on page 51
- Encapsulation Capabilities on page 54
- Example: Configure the Encapsulation on a Physical Interface on page 55

Configure the Encapsulation on a Physical Interface

By default, Point-to-Point Protocol (PPP) is the encapsulation type for physical interfaces. To configure the encapsulation on a physical interface, include the encapsulation statement at the [edit interfaces interface-name] hierarchy level:

```
[edit interfaces interface-name]
```

The physical interface encapsulation can be one of the following:

- ATM Cell Relay—Connects two remote virtual circuits or ATM physical interfaces with a label-switched path (LSP). Traffic on the circuit is ATM cells.

You can configure an ATM 1 PIC to use cell-relay accumulation mode (CAM). In this mode, the incoming cells (1 to 8 cells) are packaged into a single packet and forwarded to the label-switched path (LSP). Cell-relay accumulation mode is not supported on ATM 2 PICs. You configure CAM as shown in the following example:

```
[edit chassis]
fpc 1 {
  pic 0 {
    atm-cell-relay-accumulation;
  }
}
```

For more information, see the JUNOS Internet Software Configuration Guide: Getting Started.
ATM PVC—Defined in RFC 1483, Multiprotocol Encapsulation over ATM Adaptation Layer 5. When you configure physical ATM interfaces with ATM PVC encapsulation, an RFC 2684-compliant ATM Adaptation Layer 5 (AAL5) tunnel is set up to route the ATM cells over an MPLS path that is typically established between two MPLS-capable routers using the Label Distribution Protocol (LDP).

Cisco HDLC—E1, E3, SONET, T1, and T3 interfaces can use Cisco HDLC encapsulation. Two related versions are supported:

- CCC version (cisco-hdlc-ccc)—The logical interfaces do not require an encapsulation statement. When you use this encapsulation type, you can configure the family ccc only.
- TCC version (cisco-hdlc-tcc)—Similar to CCC and has the same configuration restrictions, but used for circuits with different media on either side of the connection.

Ethernet over ATM—Allows ATM interfaces to connect to devices that support only bridged-mode protocol data units (PDUs).

Ethernet Cross-Connect—Ethernet interfaces without VLAN tagging can use Ethernet CCC encapsulation. Two related versions are supported:

- CCC version (ethernet-ccc)—Ethernet interfaces with standard Tag Protocol ID (TPID) tagging can use Ethernet CCC encapsulation. When you use this encapsulation type, you can configure the family ccc only.
- TCC version (ethernet-tcc)—Similar to CCC, but used for circuits with different media on either side of the connection. One-port Gigabit Ethernet, two-port Gigabit Ethernet, four-port Gigabit Ethernet, and four-port Fast Ethernet PICs can use Ethernet TCC encapsulation.

VLAN Circuit Cross-Connect (CCC) (vlan-ccc)—Ethernet interfaces with virtual local area network (VLAN) tagging enabled can use VLAN CCC encapsulation. VLAN CCC encapsulation supports TPID 0x8100 only. When you use this encapsulation type, you can configure the family ccc only.

Extended VLAN Cross-Connect—Gigabit Ethernet interfaces with virtual local area network (VLAN) 802.1Q tagging enabled can use extended VLAN cross-connect encapsulation. (Ethernet interfaces with standard TPID tagging can use VLAN CCC encapsulation.) Two related versions of extended VLAN cross-connect are supported:

- CCC version (extended-vlan-ccc)—Extended VLAN CCC encapsulation supports TPIDs 0x8100, 0x9100, and 0x9901. Extended VLAN CCC is not supported on four-port Gigabit Ethernet PICs. When you use this encapsulation type, you can configure the family ccc only.
- TCC version (extended-vlan-tcc)—Similar to CCC, but used for circuits with different media on either side of the connection. One-port Gigabit Ethernet, two-port Gigabit Ethernet, and four-port Fast Ethernet PICs can use Extended Ethernet TCC encapsulation.

Ethernet VPLS (ethernet-vpls)—Ethernet interfaces with Virtual Private LAN Service (VPLS) enabled can use Ethernet VPLS encapsulation. For more information about VPLS, see the JUNOS Internet Software Configuration Guide: VPNs and the JUNOS Internet Software Feature Guide.
- Ethernet VLAN VPLS (vlan-vpls)—Ethernet interfaces with virtual local area network (VLAN) tagging and VPLS enabled can use Ethernet VLAN VPLS encapsulation. For more information about VPLS, see the JUNOS Internet Software Configuration Guide: VPNs and the JUNOS Internet Software Feature Guide.

- Extended VLAN VPLS (extended-vlan-vpls)—Ethernet interfaces with virtual local area network (VLAN) 802.1Q tagging and VPLS enabled can use Ethernet Extended VLAN VPLS encapsulation. (Ethernet interfaces with standard TPID tagging can use Ethernet VLAN VPLS encapsulation.) Extended Ethernet VLAN VPLS encapsulation supports TPIDs 0x8100, 0x9100, and 0x9901. For more information about VPLS, see the JUNOS Internet Software Configuration Guide: VPNs and the JUNOS Internet Software Feature Guide.

- Frame Relay—Defined in RFC 1490, Multiprotocol Interconnect over Frame Relay. E1, E3, link services, SONET, T1, and T3 interfaces can use Frame Relay encapsulation. Two related versions are supported:
  - CCC version (frame-relay-ccc)—The same as standard Frame Relay for DLCIs 0 through 511. DLCIs 512 through 1022 are dedicated to CCC, and the logical interface must also have frame-relay-ccc encapsulation. When you use this encapsulation type, you can configure the family ccc only.
  - TCC version (frame-relay-tcc)—Similar to Frame Relay CCC and has the same configuration restrictions, but is used for circuits with different media on either side of the connection.

- Multilink Frame Relay (MLFR) User-to-Network Interface (UNI) and Network-to-Network Interface (NNI) (multilink-frame-relay-uni-nni)—Link services interfaces functioning as FRF.16 bundles can use multilink Frame Relay UNI NNI encapsulation. This encapsulation is also used on link services interfaces’ constituent T1, E1, or NxDS-0 interfaces.

- Point-to-Point Protocol (PPP)—Defined in RFC 1661, The Point-to-Point Protocol (PPP) for the Transmission of Multiprotocol Datagrams over Point-to-Point Links. PPP is the default encapsulation type for physical interfaces. E1, E3, SONET, T1, and T3 interfaces can use PPP encapsulation. Two related versions are supported:
  - Circuit cross-connect (CCC) version (ppp-ccc)—The logical interfaces do not require an encapsulation statement. When you use this encapsulation type, you can configure the family ccc only.
  - Translational cross-connect (TCC) version (ppp-tcc)—Similar to CCC and has the same configuration restrictions, but used for circuits with different media on either side of the connection.
Encapsulation Capabilities

When you configure a point-to-point encapsulation (such as PPP or Cisco HDLC) on a physical interface, the physical interface can have only one logical interface (that is, only one unit statement) associated with it. When you configure a multipoint encapsulation (such as Frame Relay), the physical interface can have multiple logical units, and the units can be either point-to-point or multipoint.

Ethernet CCC encapsulation for Ethernet interfaces with standard TPID tagging requires that the physical interface have only a single logical interface. Ethernet interfaces in VLAN mode can have multiple logical interfaces.

For Ethernet interfaces in VLAN mode, VLAN IDs are applicable as follows:

- VLAN ID 0 is reserved for tagging the priority of frames.
- For encapsulation type `vlan-ccc`, VLAN IDs from 1 through 511 are reserved for normal VLANs, and VLAN IDs 512 and above are reserved for CCC VLANs.
- For encapsulation type `vlan-vpls`, VLAN IDs 1 through 511 are reserved for normal VLANs, and VLAN IDs 512 and above are reserved for VPLS VLANs.
- For encapsulation types `extended-vlan-ccc` and `extended-vlan-vpls`, all VLAN IDs are valid.

The upper limits for configurable VLAN IDs vary by interface type. For more information, see “Configure 802.1Q VLANs” on page 282 and Table 23 on page 283.

When you configure a TCC encapsulation, some modifications are needed to handle VPN connections over unlike Layer 2 and Layer 2.5 links and terminate the Layer 2 and Layer 2.5 protocol locally. The router performs the following media-specific changes:

- PPP TCC—Both Link Control Protocol (LCP) and Network Control Protocol (NCP) are terminated on the router. Internet Protocol Control Protocol (IPCP) IP address negotiation is not supported. The JUNOS software strips all PPP encapsulation data from incoming frames before forwarding them. For output, the next hop is changed to PPP encapsulation.
- Cisco HDLC TCC—Keepalive processing is terminated on the router. The JUNOS software strips all Cisco HDLC encapsulation data from incoming frames before forwarding them. For output, the next hop is changed to Cisco HDLC encapsulation.
- Frame Relay TCC—All Local Management Interface (LMI) processing is terminated on the router. The JUNOS software strips all Frame Relay encapsulation data from incoming frames before forwarding them. For output, the next hop is changed to Frame Relay encapsulation.
- ATM—Operation, Administration, and Maintenance (OAM) and Interim Local Management Interface (ILMI) processing is terminated at the router. Cell relay is not supported. The JUNOS software strips all ATM encapsulation data from incoming frames before forwarding them. For output, the next hop is changed to ATM encapsulation.
Example: Configure the Encapsulation on a Physical Interface

Configure PPP encapsulation on a SONET interface. The second and third family statements allow IS-IS and MPLS to run on the interface.

[edit interfaces]
so-7/0/0 {
  encapsulation ppp;
  unit 0 {
    point-to-point;
    family inet {
      address 192.168.1.113/32 {
        destination 192.168.1.114;
      }
    }
    family iso;
    family mpls;
  }
}

Configure PPP Challenge Handshake Authentication Protocol

For interfaces with PPP encapsulation, you can configure interfaces to support PPP Challenge Handshake Authentication Protocol (CHAP), as defined in RFC 1994. When you enable CHAP on an interface, the interface can authenticate its peer and can be authenticated by its peer.

By default, PPP CHAP is disabled. If CHAP is not explicitly enabled, the interface makes no CHAP challenges and denies all incoming CHAP challenges. To enable CHAP, you must create an access profile, and you must configure the interfaces to use CHAP.

To configure a CHAP access profile, include the profile statement and specify a profile name at the [edit access] hierarchy level:

[edit access]
profile profile-name {
  client name chap-secret data;
}

For more information about configuring access profiles, see the JUNOS Internet Software Configuration Guide: Getting Started.

When you configure an interface to use CHAP, you must assign an access profile to the interface. When an interface receives CHAP challenges and responses, the access profile in the packet is used to look up the shared secret, as defined in RFC 1994.

To configure PPP CHAP on an interface with PPP encapsulation, include the chap statement at the [edit interfaces interface-name ppp-options] hierarchy level:

[edit interfaces interface-name ppp-options]
chap {
  access-profile name;
  local-name name;
  passive;
}
On each interface with PPP encapsulation, you can configure the following PPP CHAP properties:

- Assign an Access Profile to an Interface on page 56
- Configure the Local Name on page 56
- Configure Passive Mode on page 56

When you configure PPP over ATM or Multilink PPP over ATM encapsulation, you can enable CHAP on the logical interface. For more information, see “Configure PPP over ATM 2 Encapsulation” on page 150.

Assign an Access Profile to an Interface

To assign an access profile to an interface, include the `access-profile` statement at the `[edit interfaces interface-name ppp-options chap]` hierarchy level:

```plaintext
[edit interfaces interface-name ppp-options chap]
access-profile name;
```

You must include the `access-profile` statement when you configure the CHAP authentication method. If an interface receives a CHAP challenge or response from a peer that is not in the applied access profile, the link is immediately dropped.

Configure the Local Name

By default, when CHAP is enabled on an interface, the interface uses the router’s system hostname as the name sent in CHAP challenge and response packets.

To configure the name the interface uses in CHAP challenge and response packets, include the `local-name` statement at the `[edit interfaces interface-name ppp-options chap]` hierarchy level:

```plaintext
[edit interfaces interface-name ppp-options chap]
local-name name;
```

Configure Passive Mode

By default, when CHAP is enabled on an interface, the interface always challenges its peer and responds to challenges from its peer.

You can configure the interface not to challenge its peer, and only respond when challenged. To configure the interface not to challenge its peer, include the `passive` statement at the `[edit interfaces interface-name ppp-options chap]` hierarchy level:

```plaintext
[edit interfaces interface-name ppp-options chap]
passive;
```
Example: Configure PPP Challenge Handshake Authentication Protocol

Configure CHAP:

```
[edit access]
  profile pe-A-ppp-clients;
  client cpe-1 chap-secret "$1$dQYsZ$B5ojUeUjDsUo.yKwcZ0";  # SECRET-DATA
  client cpe-2 chap-secret "$1$kdAsfaDAfdkJdASxfafdKdFKJ";  # SECRET-DATA
}

[edit interfaces so-1/2/0]
encapsulation ppp;
ppp-options {
  chap {
    access-profile pe-A-ppp-clients;
    local-name "pe-A-so-1/1/1";
  }
}

[edit interfaces so-1/1/2]
encapsulation ppp;
ppp-options {
  chap {
    access-profile pe-A-ppp-clients;
    local-name "pe-A-so-1/1/2";
  }
}
```

Configure the Interface Speed

By default, the router’s management Ethernet interface, fxp0, autonegotiates whether to operate at 10 Mbps or 100 Mbps. All other interfaces automatically choose the correct speed based on the PIC type and whether the PIC is configured to operate in multiplexed mode (using the no-concatenate statement in the [edit chassis] configuration hierarchy, as described in the JUNOS Internet Software Guide: Getting Started).

To configure the management Ethernet interface to operate at 10 Mbps or 100 Mbps, include the speed statement at the [edit interfaces fxp0] hierarchy level:

```
[edit interfaces fxp0]
speed (10m | 100m);
```
Configure Keepalives

By default, physical interfaces configured with Cisco HDLC or PPP encapsulation send keepalive packets at 10-second intervals. The Frame Relay term for keepalives is Local Management Interface (LMI) packets; the JUNOS software supports both ANSI T1.617 Annex D LMIs and ITU Q933 Annex A LMIs. On ATM networks, Operation, Administration, and Maintenance (OAM) cells perform the same function. You configure OAM cells at the logical interface level; for more information, see “Define the ATM 1 and ATM 2 OAM F5 Loopback Cell Period” on page 144.

To disable the sending of keepalives on a physical interface, include the no-keepalives statement at the [edit interfaces interface-name] hierarchy level:

```
[edit interfaces interface-name]
no-keepalives;
```

When you configure PPP over ATM or Multilink PPP over ATM encapsulation, you can enable or disable keepalives on the logical interface. For more information, see “Configure PPP over ATM 2 Encapsulation” on page 150.

To explicitly enable the sending of keepalives on a physical interface, include the keepalives statement at the [edit interfaces interface-name] hierarchy level:

```
[edit interfaces interface-name]
keepalives;
```

To change one or more of the default keepalive values, include the appropriate option at the [edit interfaces interface-name] hierarchy level:

```
[edit interfaces interface-name]
keepalives <interval seconds> <down-count number> <up-count number>;
```

On interfaces configured with Cisco HDLC or PPP encapsulation, you can configure the following three keepalive statements; note that Frame Relay encapsulation is not affected by these statements:

- **interval seconds**—The time in seconds between successive keepalive requests. The range is 1 second through 32767 seconds, with a default of 10 seconds.
- **down-count number**—The number of keepalive packets a destination must fail to receive before the network takes a link down. The range is 1 through 255, with a default of 3.
- **up-count number**—The number of keepalive packets a destination must receive to change a link’s status from down to up. The range is 1 through 255, with a default of 1.

For information about Frame Relay keepalive settings, see “Configure Frame Relay Keepalives” on page 307.
Configure the Clock Source

For interfaces such as SONET that can use different clock sources, you can configure the source of the transmit clock on each interface. The source can be internal (also called line timing or normal timing) or external (also called loop timing). The default source is internal, which means that each interface uses the router’s internal stratum 3 clock.

For T3 channels on an Channelized OC-12 interface, T1 channels on an Channelized T3 interface, and DS-0 channels on an Channelized E1 interface, the clocking statement is supported only for channel 0; it is ignored if included in the configuration of other channels. The clock source configured for channel 0 applies to all channels on the Channelized OC-12, Channelized DS-3, and Channelized E1 interfaces. The individual DS-3, DS-1, and DS-0 channels use a gapped 45-MHz clock as the transmit clock. For more information, see “Clock Sources on Channelized Interfaces” on page 166.

To configure loop timing on an interface, include the clocking external statement at the [edit interfaces interface-name] hierarchy level:

```
[edit interfaces interface-name]
clocking external;
```

To explicitly configure line timing on an interface, include the clocking internal statement at the [edit interfaces interface-name] hierarchy level:

```
[edit interfaces interface-name]
clocking internal;
```

Configure the Router as a DCE

By default, when you configure an interface with Frame Relay encapsulation, the router is assumed to be data terminal equipment (DTE). That is, the router is assumed to be at a terminal point on the network. To configure the router to be data circuit-terminating equipment (DCE), include the dce statement at the [edit interfaces interface-name] hierarchy level:

```
[edit interfaces interface-name]
dce;
```

When you configure the router to be a DCE, keepalives are disabled by default.

For back-to-back Frame Relay connections, either disable the sending of keepalives on both sides of the connection, or configure one side of the connection as a DTE (the default JUNOS configuration) and the other as a DCE.
Configure Receive and Transmit Leaky Bucket Properties

Congestion control is particularly difficult in high-speed networks with high volumes of traffic. When congestion occurs in such a network, it is usually too late to react. You can avoid congestion by regulating the flow of packets into your network. Smoother flows prevent bursts of packets from arriving at (or being transmitted from) the same interface and causing congestion.

For all interface types except ATM, Channelized E1, E1, Fast Ethernet, Gigabit Ethernet, and Channelized QPP, you can configure leaky bucket properties, which allow you to limit the amount of traffic received on and transmitted by a particular interface. You effectively specify what percentage of the interface's total capacity can be used to receive or transmit packets. You might want to set leaky bucket properties to limit the traffic flow from a link that is known to transmit high volumes of traffic.

Instead of configuring leaky bucket properties, you can limit traffic flow by configuring policers. Policers work on all interfaces. For more information, see "Apply Policers" on page 87 and the JUNOS Internet Software Configuration Guide: Policy Framework.

The leaky bucket is used at the host-network interface to allow packets into the network at a constant rate. Packets might be generated in a bursty manner, but after they pass through the leaky bucket, they enter the network evenly spaced. In some cases, you might want to allow short bursts of packets to enter the network without smoothing them out. By controlling the number of packets that can accumulate in the bucket, the threshold property controls burstiness. The maximum number of packets entering the network in $t$ time units is $\text{threshold} + \text{rate} \times t$.

By default, leaky buckets are disabled, and the interface can receive and transmit packets at the maximum line rate.

To configure leaky bucket properties, include one or both of the receive-bucket and transmit-bucket statements at the [edit interfaces interface-name] hierarchy level:

```
[edit interfaces interface-name]
receive-bucket {
  overflow (tag | discard);
  rate percentage;
  threshold bytes;
}
transmit-bucket {
  overflow discard;
  rate percentage;
  threshold bytes;
}
```

In the rate statement, specify the percentage of the interface line rate that is available to receive or transmit packets. The percentage can be a value from 0 (none of the interface line rate is available) to 100 (the maximum interface line rate is available). For example, when you set the line rate to 33, the interface receives or transmits at one third of the maximum line rate.
In the threshold statement, specify the bucket threshold, which controls the burstiness of the leaky bucket mechanism. The larger the value, the more bursty the traffic, which means that over a very short amount of time the interface can receive or transmit close to line rate, but the average over a longer time is at the configured bucket rate. The threshold can be a value from 0 through 16777215 bytes. For ease of entry, you can enter number either as a complete decimal number or as a decimal number followed by the abbreviation k (1,000) or m (1,000,000). For example, the entry threshold 2m corresponds to a threshold of 2,000,000 bytes.

In the overflow statement, specify how to handle packets that exceed the threshold:

- **tag** (receive bucket only)—Tag, count, and process received packets that exceed the threshold.
- **discard**—Discard received packets that exceed the threshold. No counting is done.

Configure Accounting for the Physical Interface

Juniper Networks routers can collect various kinds of data about traffic passing through the router. You can set up one or more accounting profiles that specify some common characteristics of this data, including the following:

- The fields used in the accounting records
- The number of files that the router retains before discarding, and the number of bytes per file
- The polling period that the system uses to record the data

You configure the profiles and define a unique name for each profile using statements at the [edit accounting-options] hierarchy level. There are two types of accounting profiles: interface profiles and filter profiles. You configure interface profiles by including the interface-profile statement at the [edit accounting-options] hierarchy level. You configure filter profiles by including the filter-profile statement at the [edit accounting-options] hierarchy level. For more information, see the JUNOS Internet Software Configuration Guide: Network Management.

You apply interface profiles by including the accounting-profile statement at the [edit interfaces interface-name] and [edit interfaces interface-name unit number] hierarchy levels. You apply filter profiles by including the accounting-profile statement at the [edit firewall filter filter-name] and [edit firewall family family filter filter-name] hierarchy levels.

Apply an Accounting Profile to the Physical Interface

To enable accounting on an interface, include the accounting-profile statement at the [edit interfaces interface-name] hierarchy level:

```
[edit interfaces interface-name]
accounting-profile name;
```

You can also reference profiles by logical unit; for more information, see “Configure Accounting for the Logical Interface” on page 72. For information about configuring a firewall filter accounting profile, see the JUNOS Internet Software Configuration Guide: Network Management.
Example: Apply an Accounting Profile to the Physical Interface

Configure an accounting profile for an interface and apply it to a physical interface:

```plaintext
[edit]
accounting-options {
    file if_stats {
        size 4m files 10 transfer-interval 15;
        archive-sites {
            "ftp://login:password@host/path";
        }
    }
    interface-profile if_profile {
        interval 15;
        file if_stats {
            fields {
                input-bytes;
                output-bytes;
                input-packets;
                output-packets;
                input-errors;
                output-errors;
            }
        }
    }
}

[edit interfaces ge-1/0/1]
accounting-profile if_profile;
```

Configure BERT Properties

You can configure any of the following interfaces to execute a bit error rate test (BERT) when the interface receives a request to run this test: E1, E3, T1, T3, the Channelized DS-3, OC-3, OC-12, and STM-1 interfaces, and the Channelized DS-3, E1, and OC-12 QPP interfaces. On all of the specified interface types, you set the duration of the test and the error rate to include in the bit stream by including the `bert-period` and `bert-error-rate` statements at the `interface-options` hierarchy level:

```plaintext
[edit interfaces interface-name interface-options]
bert-error-rate rate;
bert-period seconds;
```

seconds is the duration of the BERT procedure. The test can last from 1 to 240 seconds; the default is 10 seconds.

rate is the bit error rate. This can be an integer in the range 0 through 7, which corresponds to a bit error rate in the range $10^{-0}$ (that is, 1 error per bit) to $10^{-7}$ (that is, 1 error per 10 million bits).
algorithm is the pattern to send in the bit stream. The algorithm for the E1 BERT procedure is pseudo-2e15-o151 (pattern is $2^{15} - 1$, as defined in the CCITT/ITU O.151 standard). On T1, E3, T3, NxDS-0, and Channelized E1 and T3 QPP interfaces, you can also select the pattern to send in the bit stream by including the bert-algorithm statement at the [edit interfaces interface-name interface-options] hierarchy level:

```
[edit interfaces interface-name interface-options]
bert-algorithm algorithm;
```

For a list of supported algorithms, see the CLI possible completions; for example:

```
user@host# set bert-algorithm ?
```

Possible completions:

- pseudo-2e11-o152 Pattern is $2^{11} - 1$ (per O.152 standard)
- pseudo-2e15-o151 Pattern is $2^{15} - 1$ (per O.152 standard)
- pseudo-2e20-o151 Pattern is $2^{20} - 1$ (per O.151 standard)
- pseudo-2e20-o153 Pattern is $2^{20} - 1$ (per O.153 standard)

...

See individual interface types for specific hierarchy information. For information about running the BERT procedure, see the JUNOS Internet Software Operational Mode Command Reference.

Table 9 shows the BERT capabilities for various interface types.

### Table 9: BERT Capabilities by Interface Type

<table>
<thead>
<tr>
<th>Interface</th>
<th>T1 BERT</th>
<th>T3 BERT</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>E1 or T1</td>
<td>Yes (port 0–3)</td>
<td>Yes (port 0–3)</td>
<td>Single port at a time</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Limited algorithms</td>
</tr>
<tr>
<td>E3 or T3</td>
<td>Yes (port 0–3)</td>
<td>Yes (port 0–3)</td>
<td>Single port at a time</td>
</tr>
<tr>
<td>Channelized OC-12</td>
<td>N/A</td>
<td>Yes (channel 0–11)</td>
<td>Single channel at a time</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Limited algorithms</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>No bit count</td>
</tr>
<tr>
<td>Channelized STM-1</td>
<td>Yes (channel 0–62)</td>
<td>N/A</td>
<td>Multiple channels</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Only one algorithm</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>No error insert</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>No bit count</td>
</tr>
<tr>
<td>Channelized T3 and Multichannel T3</td>
<td>Yes (channel 0–27)</td>
<td>Yes (port 0–3 on channel 0)</td>
<td>Multiple ports and channels</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Limited algorithms for T1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>No error insert for T1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>No bit count for T1</td>
</tr>
</tbody>
</table>

For information about BERT capabilities on channelized QPP interfaces, see “Channelized QPP Interface Properties” on page 169.
Trace Operations of an Individual Router Interface

To trace the operations of individual router interfaces, include the traceoptions statement at the [edit interfaces interface-name] hierarchy level:

```
[edit interfaces interface-name]
traceoptions {
    flag flag <disable>;
}
```

You can specify the following interface tracing flags:

- `all`—Trace all interface operations.
- `event`—Trace all interface events.
- `ipc`—Trace all interface IPC messages.
- `media`—Trace all interface media changes.

The interfaces traceoptions statement does not support a trace file. The logging is done by the kernel, so the tracing information is placed in the system syslog files.

For more information about trace operations, see “Trace Interface Operations” on page 107.

Damp Interface Transitions

By default, when an interface changes from being up to being down, or from down to up, this transition is advertised immediately to the router software and hardware. In some situations, for example, when an interface is connected to an ADM or WDM, or to protect against SONET framer holes, you might want to damp interface transitions, thereby not advertising the interface’s transition until a certain period of time has passed, called the hold-time. When you have damped interface transitions and the interface goes from up to down, the interface is not advertised to the rest of the system as being down until it has remained down for the hold-time period. Similarly when an interface goes from down to up, it is not advertised as being up until it has remained up for the hold-time period.

To damp interface transitions, include the hold-time statement at the [edit interfaces interface-name] hierarchy level:

```
[edit interfaces interface-name]
hold-time up milliseconds down milliseconds;
```

The time can be a value from 0 through 65,534 milliseconds. Upon execution, the time value that you specify is rounded up to the nearest whole second; therefore, we recommend that you configure the up and down options to multiples of 1000. The default value is 0, which means that interface transitions are not damped.
Configure Multiservice Physical Interface Properties

The monitoring services PIC is one of a group of multiservice PICs specifically designed to enable IP services. To configure multiservice physical interface properties on the monitoring services interface, include the multiservice-options statement at the [edit interfaces mo-fpc/ pic/ port] hierarchy level:

```
[edit interfaces mo-fpc/ pic/ port]
multiservice-options {
  boot-command filename
  (core-dump | no-core-dump);
  (syslog | no-syslog);
}
```

For more information about the monitoring services interface, see “Enable Passive Monitoring” on page 374.

Enable or Disable SNMP Notifications on Physical Interfaces

By default, SNMP notifications are sent when the state of an interface or a connection changes. To explicitly enable these notifications on the physical interface, include the traps statement at the [edit interfaces interface-name] hierarchy level. To disable these notifications on the physical interface, include the no-traps statement at the [edit interfaces interface-name] hierarchy level:

```
[edit interfaces interface-name]
(traps | no-traps);
```

Disable a Physical Interface

You can disable a physical interface, marking it as being down, without removing the interface configuration statements from the configuration. To do this, include the disable statement at the [edit interfaces interface-name] hierarchy level:

```
[edit interfaces interface-name]
disable;
```
Example: Disable a Physical Interface

Disable a physical interface:

```
[edit interfaces]
s0-1/1/0 {
    mtu 8000;
clocking internal;
encapsulation ppp;
sonet-options {
    fcs 16;
}
unit 0 {
    family inet {
    address 12.12.12.21/32 {
        destination 12.12.12.22;
    }
}
}
}
[edit interfaces]
user@host# set s0-1/1/0 disable
[edit interfaces]
user@host# show s0-1/1/0
s0-1/1/0 {
    disable; # Interface is marked as disabled
    mtu 8000;
clocking internal;
encapsulation ppp;
sonet-options {
    fcs 16;
}
unit 0 {
    family inet {
        address 12.12.12.21/32 {
            destination 12.12.12.22;
        }
    }
}
```

Chapter 6
Configure Logical Interface Properties

For a physical interface device to function, you must configure at least one logical interface on that device. For each logical interface, you must specify the protocol family that the interface supports. You can also configure other logical interface properties. These vary by PIC and encapsulation type, but include the IP address of the interface, whether or not the interface supports multicast traffic, DLCIs, VCI s and VPIs, and traffic shaping.

To configure logical interface properties, you include the following statements at the [edit interfaces interface-name unit logical-unit-number] hierarchy level:

```plaintext
[edit interfaces interface-name unit logical-unit-number]
accept-source-mac {
    mac-address mac-address {
        policer {
            input policer-name;
            output policer-name;
        }
    }
}
accounting-profile name;
bandwidth rate;
cell-bundle-size cells;
disable;
dlci dlci-identifier;
description text;
drop-timeout milliseconds;
encapsulation type;
epd-threshold cells;
family {
    protocol-family-statements;
}
fragment-threshold bytes;
input-vlan-map {
    pop;
    push;
    swap;
    vlan-id number;
    tag-protocol-id tpid;
}
interleave-fragments;
inverse-arp;
minimum-links number;
mrru bytes;
multicast-dlci dlci-identifier;
multicast-vci vci-identifier;
multipoint;
```
This chapter describes the configuration of the logical interface properties:

- Specify the Logical Interface Number on page 71
- Add a Logical Unit Description to the Configuration on page 71
- Configure a Point-to-Point Connection on page 72
- Configure a Multipoint Connection on page 72
- Configure Accounting for the Logical Interface on page 72
- Configure the Interface Bandwidth on page 74
- Enable or Disable SNMP Notifications on Logical Interfaces on page 74
- Configure Interface Encapsulation on page 74
- Disable a Logical Interface on page 76

For information about interface-specific logical properties, see “Interface Types” on page 109.

Table 10 lists statements that you can use to configure logical interfaces.
<table>
<thead>
<tr>
<th>Statement</th>
<th>Interface Types</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>accept-source-mac</td>
<td>Gigabit Ethernet QPP interfaces</td>
<td>“Configure Gigabit Ethernet QPP MAC Address Filtering” on page 270</td>
</tr>
<tr>
<td>accounting-profile name</td>
<td>All</td>
<td>“Configure Accounting for the Logical Interface” on page 72</td>
</tr>
<tr>
<td>backup-destination address</td>
<td>Encryption interfaces</td>
<td>“Configure IPSec Tunnel Redundancy” on page 260</td>
</tr>
<tr>
<td>bandwidth rate</td>
<td>All interface types except multilink and aggregated</td>
<td>“Configure the Interface Bandwidth” on page 74</td>
</tr>
<tr>
<td>cell-bundle-size cells</td>
<td>ATM 2 interfaces</td>
<td>“Configure the ATM 2 Layer 2 Circuit Cell-Relay Cell Maximum” on page 133</td>
</tr>
<tr>
<td>destination (destination-address</td>
<td>Routing-instance-name)</td>
<td>Encryption GRE tunnel, and IP tunnel interfaces</td>
</tr>
<tr>
<td>description</td>
<td>All</td>
<td>“Add a Logical Unit Description to the Configuration” on page 71</td>
</tr>
<tr>
<td>disable</td>
<td>All</td>
<td>“Disable a Logical Interface” on page 76</td>
</tr>
<tr>
<td>dlcI dlcI-identifier</td>
<td>Point-to-point interfaces with Frame Relay encapsulation</td>
<td>“Configure Frame Relay DLCIs” on page 309</td>
</tr>
<tr>
<td>drop-timeout milliseconds</td>
<td>Multilink interfaces</td>
<td>“Configure a Multilink and Link Services Drop Timeout Period” on page 323</td>
</tr>
<tr>
<td>encapsulation type</td>
<td>All interface types except aggregated SONET/SDH and loopback</td>
<td>“Configure the Encapsulation on a Logical Interface” on page 75</td>
</tr>
<tr>
<td>epd-threshold cells</td>
<td>ATM 2 interfaces</td>
<td>“Configure the ATM 2 EPD Threshold” on page 143</td>
</tr>
<tr>
<td>family</td>
<td>All</td>
<td>“Configure the Protocol Family” on page 79</td>
</tr>
<tr>
<td>fragment-threshold bytes</td>
<td>Multilink interfaces</td>
<td>“Configure a Multilink and Link Services Fragmentation Threshold” on page 325</td>
</tr>
<tr>
<td>input-vlan-map</td>
<td>Gigabit Ethernet QPP interfaces</td>
<td>“Stack and Rewrite Gigabit Ethernet QPP VLAN Tags” on page 273</td>
</tr>
<tr>
<td>inverse-arp</td>
<td>Interfaces with ATM and Frame Relay encapsulation</td>
<td>“Configure Inverse ATM 1 or ATM 2 ARP” on page 137 and “Configure Inverse Frame Relay ARP” on page 308</td>
</tr>
<tr>
<td>mac-address mac-address</td>
<td>Gigabit Ethernet QPP interfaces</td>
<td>“Configure Gigabit Ethernet QPP MAC Address Filtering” on page 270</td>
</tr>
<tr>
<td>minimum-links number</td>
<td>Multilink interfaces</td>
<td>“Configure Multilink and Link Services Minimum Links” on page 326</td>
</tr>
<tr>
<td>mrru bytes</td>
<td>Multilink interfaces</td>
<td>“Configure Multilink and Link Services MRRU” on page 326</td>
</tr>
<tr>
<td>multicast-dlcI dlcI-identifier</td>
<td>Point-to-multipoint Frame Relay interfaces</td>
<td>“Configure a Multicast-Capable Frame Relay Connection” on page 311</td>
</tr>
<tr>
<td>multicast-vci vpi-identifier.vci-identifier</td>
<td>Point-to-multipoint ATM 1 and ATM 2 interfaces</td>
<td>“Configure the ATM 1 and ATM 2 OAM F5 Loopback Cell Threshold” on page 145</td>
</tr>
<tr>
<td>multipoint</td>
<td>All</td>
<td>“Configure a Multipoint Connection” on page 72</td>
</tr>
<tr>
<td>oam-liveness</td>
<td>ATM 1 and ATM 2 interfaces</td>
<td>“Configure the ATM 1 and ATM 2 OAM F5 Loopback Cell Threshold” on page 145</td>
</tr>
<tr>
<td>Statement</td>
<td>Interface Types</td>
<td>Usage Guidelines</td>
</tr>
<tr>
<td>----------------------------------------</td>
<td>-----------------------------------------------------</td>
<td>---------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>oam-period (disable</td>
<td>seconds)</td>
<td>ATM 1 and ATM 2 interfaces</td>
</tr>
<tr>
<td>output-vlan-map</td>
<td>Gigabit Ethernet QPP interfaces</td>
<td>“Stack and Rewrite Gigabit Ethernet QPP VLAN Tags” on page 273</td>
</tr>
<tr>
<td>passive-monitor-mode</td>
<td>SONET interfaces</td>
<td>“Enable Passive Monitoring” on page 374</td>
</tr>
<tr>
<td>point-to-point</td>
<td>All</td>
<td>“Configure a Point-to-Point Connection” on page 72</td>
</tr>
<tr>
<td>policer</td>
<td>Gigabit Ethernet QPP interfaces</td>
<td>“Configure Gigabit Ethernet QPP MAC Address Filtering” on page 270</td>
</tr>
<tr>
<td>pop</td>
<td>Gigabit Ethernet QPP interfaces</td>
<td>“Stack and Rewrite Gigabit Ethernet QPP VLAN Tags” on page 273</td>
</tr>
<tr>
<td>push</td>
<td>Gigabit Ethernet QPP interfaces</td>
<td>“Stack and Rewrite Gigabit Ethernet QPP VLAN Tags” on page 273</td>
</tr>
<tr>
<td>queue-length number</td>
<td>ATM 1 interfaces</td>
<td>“Configure the ATM 1 Queue Length” on page 142</td>
</tr>
<tr>
<td>routing-instance</td>
<td>GRE tunnel and IP tunnel interfaces</td>
<td>“Configure a Unicast Tunnel” on page 408 and “Configure a Tunnel Interface for Routing Table Lookup” on page 409</td>
</tr>
<tr>
<td>shaping</td>
<td>ATM 1 and ATM 2 interfaces</td>
<td>“Define the ATM 1 and ATM 2 Traffic-Shaping Profile” on page 137</td>
</tr>
<tr>
<td>short-sequence</td>
<td>Multilink interfaces</td>
<td>“Configure Multilink and Link Services Sequence Format” on page 327</td>
</tr>
<tr>
<td>source address</td>
<td>Encryption, GRE tunnel, and IP tunnel interfaces</td>
<td>“Configure a Unicast Tunnel” on page 408, “Configure a Tunnel Interface for Routing Table Lookup” on page 409, and “Configure an Encryption Interface” on page 258</td>
</tr>
<tr>
<td>swap</td>
<td>Gigabit Ethernet QPP interfaces</td>
<td>“Stack and Rewrite Gigabit Ethernet QPP VLAN Tags” on page 273</td>
</tr>
<tr>
<td>tag-protocol-id tpid</td>
<td>Gigabit Ethernet QPP interfaces</td>
<td>“Stack and Rewrite Gigabit Ethernet QPP VLAN Tags” on page 273</td>
</tr>
<tr>
<td>transmit-weight number</td>
<td>ATM 2 interfaces</td>
<td>“Configure the ATM 2 Transmission Weight” on page 144</td>
</tr>
<tr>
<td>(traps</td>
<td>no-traps)</td>
<td>All</td>
</tr>
<tr>
<td>ttl number</td>
<td>GRE tunnel and IP tunnel interfaces</td>
<td>“Configure a Unicast Tunnel” on page 408</td>
</tr>
<tr>
<td>tunnel</td>
<td>Encryption, GRE tunnel, and IP tunnel interfaces</td>
<td>“Configure a Unicast Tunnel” on page 408, “Configure a Tunnel Interface for Routing Table Lookup” on page 409, or “Configure an Encryption Interface” on page 258</td>
</tr>
<tr>
<td>vci vpi-identifier.vci-identifier</td>
<td>ATM 1 and ATM 2 point-to-point interfaces</td>
<td>“Configure a Point-to-Point ATM 1 or ATM 2 Connection” on page 136</td>
</tr>
<tr>
<td>vlan-id number</td>
<td>Fast Ethernet and Gigabit Ethernet interfaces</td>
<td>“Configure 802.1Q VLANs” on page 282</td>
</tr>
<tr>
<td>vlan-tag [ tpid.vlan-id ]</td>
<td>Gigabit Ethernet QPP interfaces</td>
<td>“Stack and Rewrite Gigabit Ethernet QPP VLAN Tags” on page 273</td>
</tr>
</tbody>
</table>
Specify the Logical Interface Number

Each logical interface must have a logical unit number. The logical unit number corresponds to the logical unit part of the interface name. For more information, see “Configure Aggregated Interfaces” on page 45.

PPP, Cisco HDLC, and Ethernet CCC encapsulations support only a single logical interface, whose logical unit number must be 0. Frame Relay and ATM encapsulations support multiple logical interfaces, so you can configure one or more logical unit numbers.

You specify the logical unit number in the unit statement at the [edit interfaces interface-name] hierarchy level:

```
[edit interfaces]
interface-name {
  unit 0 {
    ...
  }
}
interface-name {
  unit logical-unit-number {
    ...
  }
}
```

The logical unit number can range from 0 through 16384.

Add a Logical Unit Description to the Configuration

You can include a text description of each logical unit in the configuration file. Any descriptive text you include is displayed in the output of the show interfaces commands, and is also exposed in the ifAlias MIB object. It has no impact on the interface’s configuration. To add a text description, include the description statement at the [edit interfaces interface-name unit logical-unit-number] hierarchy level:

```
[edit interfaces interface-name unit logical-unit-number]
description text;
```

The description can be a single line of text. If the text contains spaces, enclose it in quotation marks.

For information about describing physical interfaces, see “Add an Interface Description to the Configuration” on page 46.
Configure a Point-to-Point Connection

By default, all interfaces are assumed to be point-to-point connections. You must ensure that the MTU sizes on both sides of the connection are the same.

For all interfaces except aggregated Ethernet, Fast Ethernet, and Gigabit Ethernet, you can explicitly configure an interface to be a point-to-point connection by including the `point-to-point` statement at the [edit interfaces interface-name unit logical-unit-number] hierarchy level:

```plaintext
[edit interfaces interface-name unit logical-unit-number]
point-to-point;
```

Configure a Multipoint Connection

By default, all interfaces are assumed to be point-to-point connections. To configure an interface to be a multipoint connection, include the `multipoint` statement at the [edit interfaces interface-name unit logical-unit-number] hierarchy level:

```plaintext
[edit interfaces interface-name unit logical-unit-number]
multipoint;
```

Configure Accounting for the Logical Interface

Juniper Networks routers can collect various kinds of data about traffic passing through the router. You can set up one or more accounting profiles that specify some common characteristics of this data, including the following:

- The fields used in the accounting records
- The number of files that the router retains before discarding, and the number of bytes per file
- The period that the system uses to record the data

You configure the profiles and define a unique name for each profile using statements at the [edit accounting-options] hierarchy level. There are two types of accounting profiles: interface profiles and filter profiles. You configure interface profiles by including the `interface-profile` statement at the [edit accounting-options] hierarchy level. You configure filter profiles by including the `filter-profile` statement at the [edit accounting-options] hierarchy level. For more information, see the JUNOS Internet Software Configuration Guide: Network Management.

You apply interface profiles by including the `accounting-profile` statement at the [edit interfaces interface-name] and [edit interfaces interface-name unit number] hierarchy levels. You apply filter profiles by including the `accounting-profile` statement at the [edit firewall filter filter-name] and [edit firewall family family filter filter-name] hierarchy levels.
Apply an Accounting Profile to the Logical Interface

To enable accounting on an interface, include the `accounting-profile` statement at the
`[edit interfaces interface-name unit logical-unit-number]` hierarchy level:

```
[edit interfaces interface-name unit logical-unit-number]
accounting-profile name;
```

You can also reference profiles for the physical interface; for more information, see
“Configure Accounting for the Physical Interface” on page 61. For information about
configuring a firewall filter accounting profile, see the JUNOS Internet Software Configuration

Example: Apply an Accounting Profile to the Logical Interface

Configure an accounting profile for an interface and apply it to a physical interface:

```
[edit]
accounting-options {
  file if_stats {
    size 4m files 10 transfer-interval 15;
    archive-sites {
      "ftp://login:password@host/path";
    }
  }
  interface-profile if_profile {
    interval 15;
    file if_stats {
      fields {
        input-bytes;
        output-bytes;
        input-packets;
        output-packets;
        input-errors;
        output-errors;
      }
    }
  }
}

[edit interfaces ge-1/0/1 unit 1]
accounting-profile if_profile;
```

To reference profiles by physical interface, see “Apply an Accounting Profile to the Physical
Interface” on page 61. For information about configuring a firewall filter accounting profile,
see the JUNOS Internet Software Configuration Guide: Policy Framework.
Configure the Interface Bandwidth

By default, the JUNOS software uses the physical interface's speed for the MIB-II object, ifSpeed. You can configure the logical unit to populate the ifSpeed variable by configuring a bandwidth value for the logical interface. The bandwidth statement sets an informational-only parameter; you cannot adjust the actual bandwidth of an interface with this statement.

To configure the bandwidth value for a logical interface, include the bandwidth statement at the [edit interfaces interface-name unit logical-unit-number] hierarchy level:

```
[edit interfaces interface-name unit logical-unit-number]
  bandwidth rate;
```

rate is the peak rate, in bps or cps. You can specify a value in bits per second either as a complete decimal number or as a decimal number followed by the abbreviation k (1000), m (1,000,000), or g (1,000,000,000). You can also specify a value in cells per second by entering a decimal number followed by the abbreviation c; values expressed in cells per second are converted to bits per second using the formula 1 cps = 384 bps. The range is not limited. The bandwidth statement is valid for all logical interfaces, except multilink and aggregated interfaces.

Enable or Disable SNMP Notifications on Logical Interfaces

By default, SNMP notifications are sent when the state of an interface or a connection changes. To explicitly enable these notifications on the logical interface, include the traps statement at the [edit interfaces interface-name unit logical-unit-number] hierarchy level. To disable these notifications on the logical interface, include the no-traps statement at the [edit interfaces interface-name unit logical-unit-number] hierarchy level:

```
[edit interfaces interface-name unit logical-unit-number]
  traps | no-traps;
```

Configure Interface Encapsulation

Point-to-Point Protocol (PPP) encapsulation is the default encapsulation type for physical interfaces. You need not configure encapsulation for any physical interfaces that support PPP encapsulation. If you do not configure encapsulation, PPP is used by default. For physical interfaces that do not support PPP encapsulation, you must configure an encapsulation to use for packets transmitted on the interface. For more information about physical interface encapsulation, see “Configure the Encapsulation on a Physical Interface” on page 51.

You can optionally configure an encapsulation on a logical interface, which is the encapsulation used within certain packet types.
Configure the Encapsulation on a Logical Interface

Generally, you configure an interface’s encapsulation at the [edit interfaces interface-name] hierarchy level. However, for some encapsulation types, such as Frame Relay, ATM, and Ethernet VLAN encapsulations, you can also configure the encapsulation type that is used inside the Frame Relay, ATM, or VLAN circuit itself. To do this, include the encapsulation statement at the [edit interfaces interface-name unit logical-unit-number] hierarchy level:

```
[edit interfaces interface-name unit logical-unit-number]
```

Some of the ATM encapsulations are defined in RFC 1483, Multiprotocol Encapsulation over ATM Adaptation Layer 5.

The following restrictions apply to logical interface encapsulation:

- With the atm-nlpid, atm-cisco-nlpid, and atm-vc-mux encapsulations, you can configure the family inet only.
- With the circuit cross-connect (CCC) circuit encapsulations, you cannot configure a family on the logical interface.
- A logical interface cannot have frame-relay-ccc encapsulation unless the physical device also has frame-relay-ccc encapsulation.
- A logical interface cannot have frame-relay-tcc encapsulation unless the physical device also has frame-relay-tcc encapsulation. In addition, you must assign this logical interface a DLCI in the range 512 through 1022 and configure it as point-to-point.
- For interfaces that carry IPv4 traffic, you can configure ether-over-atm-llc encapsulation.
- When you use ether-over-atm-llc encapsulation, you cannot configure multipoint interfaces.
- A logical interface cannot have vlan-ccc or vlan-vpls encapsulation unless the physical device also has vlan-ccc or vlan-vpls encapsulation, respectively. In addition, you must assign this logical interface a VLAN ID in the range 512 through 1023; if the VLAN ID is 511 or lower, it is subject to the normal destination filter lookups in addition to source address filtering. For more information, see “Configure VLAN CCC or VPLS Encapsulation” on page 284.
- You can create an ATM cell-relay circuit by configuring an entire ATM physical device or an individual virtual circuit (VC). When you configure an entire device, only cell relay encapsulation is allowed on the logical interfaces. For more information, see “Configure an ATM 1 Cell-Relay Circuit” on page 148.

For more information about ATM encapsulations, see “Configure ATM 1 and ATM 2 Interface Encapsulation” on page 146.

For more information about Frame Relay encapsulations, see “Configure Frame Relay Interface Encapsulation” on page 304.

For more information about multilink encapsulations, see “Configure Multilink and Link Services Logical Interface Encapsulation” on page 324.
Disable a Logical Interface

You can unconfigure a logical interface, effectively disabling that interface, without removing the logical interface configuration statements from the configuration. To do this, include the disable statement at the [edit interfaces interface-name unit logical-unit-number] hierarchy level:

```
[edit interfaces interface-name unit logical-unit-number]
disable;
```
Chapter 7
Configure Protocol Family and Address Interface Properties

For each logical interface, you must configure one or more protocol families. You can also configure interface address properties. To do this, you can include the following statements at the [edit interfaces interface-name unit logical-unit-number] hierarchy level:

```conf
[edit interfaces interface-name unit logical-unit-number]
family family {
    accounting {
        destination-class-usage;
        source-class-usage {
            (input | output | [input output]);
        }
    }
    bundle (ml-fpc/pic/ port | ls-fpc/ pic/ port);
    filter {
        input filter-name;
        output filter-name;
        group filter-group-number;
    }
    ipsec-sa sa-name;
    keep-address-and-control;
    mtu bytes;
    multicasts-only;
    no-asynchronous-notification;
    no-redirects;
    policer {
        arp policer-template-name;
        input policer-template-name;
        output policer-template-name;
    }
    primary;
    proxy inet-address address;
    remote (inet-address address | mac-address address);
    rpf-check <fail-filter filter-name> {
        <mode loose>;
    }
    sampling {
        [ input output ];
    }
    (translate-discard-eligible | no-translate-discard-eligible);
    (translate-fecn-and-becn | no-translate-fecn-and-becn);
```
address address {
    arp ip-address (mac | multicast-mac) mac-address <publish>;
    destination destination-address;
    eui-64;
    broadcast address;
    multipoint-destination destination-address (dlci dlci-identifier | vci vci-identifier);
    multipoint-destination destination-address {
        epd-threshold cells;
        inverse-arp;
        oam-liveness {
            up-count cells;
            down-count cells;
        }
        oam-period seconds;
        shaping {
            (cbr rate | rtvbr peak rate sustained rate burst length | vbr peak rate sustained rate burst length);
            queue-length number;
        }
        vci vpi-identifier.vci-identifier;
    }
    preferred;
    primary;
    wrp-group group-number {
        virtual-address [addresses];
        priority number;
        (accept-data | no-accept-data);
        advertise-interval seconds;
        authentication-type authentication;
        authentication-key key key;
        (preempt | no-preempt);
        track {
            interface interface-name priority-cost cost;
        }
    }
}

This chapter describes the configuration of the interface protocol and address properties:

- Configure the Protocol Family on page 79
- Configure the Interface Address on page 81
- Configure an Unnumbered Interface on page 82
- Set the Protocol MTU on page 83
- Configure Default, Primary, and Preferred Addresses and Interfaces on page 84
- Disable the Sending of Redirect Messages on an Interface on page 84
- Configure Default, Primary, and Preferred Addresses and Interfaces on page 84
- Apply Policers on page 87
- Apply a Filter to an Interface on page 88
Configure the Protocol Family

For each logical interface, you can configure one or more of the following protocols that run on the interface:

- **ccc**—Circuit Cross-Connect (CCC). You can configure this protocol family for the logical interface of CCC physical interfaces. When you use this encapsulation type, you can configure the family ccc only.

- **inet**—IP (Internet Protocol). You must configure this protocol family for the logical interface to support IP protocol traffic, including OSPF, BGP, and ICMP.

- **inet6**—IP (Internet Protocol) version 6. You must configure this protocol family for the logical interface to support IPv6 protocol traffic, including RIPv6, IS-IS, and BGP. For more information about IPv6, see “IPv6 Introduction” on page 80.

- **iso**—ISO. You must configure this protocol family for the logical interface to support IS-IS traffic.

- **mlfr-uni-nni**—Multilink Frame Relay (MLFR) FRF.16 user-to-network network-to-network (UNI NNI). You must configure this protocol or mlfr-end-to-end for the logical interface to support link services bundling.

- **mlfr-end-to-end**—Multilink Frame Relay End-to-End. You must configure this protocol or MLPPP for the logical interface to support multilink bundling.

- **mlppp**—Multilink Point-to-Point Protocol (MLPPP). You must configure this protocol (or mlfr-end-to-end) for the logical interface to support multilink bundling.

- **mpls**—Multiprotocol Label Switching (MPLS). You must configure this protocol family for the logical interface to participate in an MPLS path.

- **tcc**—Translational Cross-Connect (TCC). You can configure this protocol family for the logical interface of TCC physical interfaces.

- **tnp**—Trivial Network Protocol. This protocol is used to communicate between the Routing Engine and the System Control Board (SCB), System and Switch Board (SSB), Forwarding Engine Board (FEB), or System and Forwarding Module (SFM), depending on router model, in the router’s Packet Forwarding Engine. The JUNOS software automatically configures this protocol family on the router’s internal interfaces only, as discussed in “Configure the Internal Ethernet Interface” on page 299.

- **vpls**—Virtual Private LAN Service (VPLS). You can optionally configure this protocol family for the logical interface on which you configure VPLS. VPLS provides an Ethernet-based point-to-multipoint Layer 2 VPN to connect customer edge (CE) routers across an MPLS backbone. When you configure a VPLS encapsulation type, the family vpls statement is assumed by default. For more information about VPLS, see the JUNOS Internet Software Configuration Guide: VPNs and the JUNOS Internet Software Feature Guide.
To configure the logical interface's protocol family, include the family statement at the `[edit interfaces interface-name unit logical-unit-number]` hierarchy level, specifying the selected family. To configure more than one protocol family on a logical interface, include multiple family statements. Following is the minimum configuration:

```
[edit interfaces interface-name unit logical-unit-number]
family family {
  mtu size;
  multicasts-only;
  no-redirects;
  primary;
  address address {
    destination address;
    broadcast address;
    preferred;
    primary;
  }
}
```

**IPv6 Introduction**

IPv4 has been widely deployed and used to network the Internet today. With the rapid growth of the Internet, enhancements to IPv4 are needed to support the influx of new subscribers, Internet-enabled devices, and applications. IPv6 is designed to enable the global expansion of the Internet.

IPv6 builds upon the functionality of IPv4, providing improvements to addressing, configuration and maintenance, and security.

IPv6 is defined in the following documents:

- RFC 2460, Internet Protocol, Version 6 (IPv6)
- RFC 2373, IP Version 6 Addressing Architecture

**IPv4-to-IPv6 Transition**

Implementing IPv6 requires a transition mechanism to allow interoperability between IPv6 nodes (both routers and hosts) and IPv4 nodes. The transition mechanism is the key factor in the successful deployment of IPv6. Because millions of IPv4 nodes already exist, upgrading every node to IPv6 at the same time is not feasible.

As a result, transition from IPv4 to IPv6 happens gradually, allowing nodes to be upgraded independently and without disruption to other nodes. While a gradual upgrade occurs, compatibility between IPv6 and IPv4 nodes becomes a requirement. Otherwise, an IPv6 node would not be able to communicate with an IPv4 node.

Transition mechanisms allow IPv6 and IPv4 nodes to coexist together in the same network, and make gradual upgrading possible. The transition mechanism supported by the JUNOS Internet software is tunneling. Tunnels allow IPv6 packets to be encapsulated into IPv4 headers and sent across an IPv4 infrastructure. For more information about configuring tunnels to support IPv4-to-IPv6 transition, see “Configure an IPv6-over-IPv4 Tunnel” on page 412.
Configure the Interface Address

You assign an address to an interface by specifying the address when configuring the protocol family. For the \texttt{inet} family, you configure the interface's IP address. For the \texttt{iso} family, you configure one or more addresses for the loopback interface. For the \texttt{ccc}, \texttt{tcc}, \texttt{mpls}, \texttt{tnp}, and \texttt{vpls} families, you never configure an address.

To assign an address to an interface, include the \texttt{address} statement at the \texttt{[edit interfaces interface-name unit logical-unit-number family family]} hierarchy level:

```plaintext
[edit interfaces interface-name unit logical-unit-number family family]
address address {
  destination address;
  eui-64;
  broadcast address;
  preferred;
  primary;
}
```

In the \texttt{address} statement, specify the network address of the interface.

For each address, you can optionally configure one or more of the following:

- **Address of the remote side of the connection (for point-to-point interfaces only)**—Specify this in the \texttt{destination} statement.

- **Whether the router automatically generates the host number portion of interface addresses**—The \texttt{eui-64} statement applies only to interfaces that carry IPv6 traffic, where the prefix length of the address is 64 bits or less, and the low-order 64 bits of the address are zero. This option does not apply to the loopback interface (\texttt{lo0}) because IPv6 addresses configured on the loopback interface must have a 128-bit prefix length.

- **Broadcast address for the interface's subnet**—Specify this in the \texttt{broadcast} statement; this applies only to Ethernet interfaces, such as the management interface \texttt{fxp0}, the Fast Ethernet interface, and the Gigabit Ethernet interface.

- **Whether this address is the preferred address**—Each subnet on an interface has a preferred local address. If you configure more than one address on the same subnet, the preferred local address is chosen by default as the source address when you originate packets to destinations on the subnet. For more information about preferred addresses, see “Configure Default, Primary, and Preferred Addresses and Interfaces” on page 84. By default, the preferred address is the lowest numbered address on the subnet. To override the default and explicitly configure the preferred address, include the \texttt{preferred} statement when configuring the address.

- **Whether this address is the primary address**—Each interface has a primary local address. If an interface has more than one address, the primary local address is used by default as the source address when you originate packets out the interface where the destination gives no hint about the subnet (for example, some ping commands). For more information about primary addresses, see “Configure Default, Primary, and Preferred Addresses and Interfaces” on page 84. By default, the primary address on an interface is the lowest numbered non-127 preferred address on the interface. To override the default and explicitly configure the preferred address, include the primary statement when configuring the address.
Configure the IPv6 Address on an Interface

You represent IPv6 addresses in hexadecimal notation using a colon-separated list of 16-bit values.

You assign a 128-bit IPv6 address to an interface by including the address statement at the [edit interfaces interface-name unit logical-unit-number family inet6] hierarchy level:

```
[edit interfaces interface-name unit logical-unit-number family inet6]
address aaaa::bfff:....:zzzz/nn;
```

The double colon (::) represents all bits set to 0, as shown in the following example:

```
interfaces fe-0/0/1 {
  unit 0 {
    family inet6 {
      address fec0:1:1:1::2/64;
    }
  }
}
```

Configure an Unnumbered Interface

When you need to conserve IP addresses, you can configure unnumbered interfaces. To do this, configure the protocol family, but do not include the address statement at the [edit interfaces interface-name unit logical-unit-number family] hierarchy level:

```
[edit interfaces interface-name unit logical-unit-number]
family family;
```

For example:

```
[edit]
interfaces {
  so-6/1/0 {
    unit 0 {
      family inet;
      family iso;
    }
  }
}
```

When configuring unnumbered interfaces, you must ensure that a source address is configured on some interface in the router. This address is the default address. We recommend that you do this by assigning an address to the loopback interface (lo0), as described in “Configure the Loopback Interface” on page 313. If you configure an address (other than a martian) on the lo0 interface, that address is always the default address, which is preferable because the loopback interface is independent of any physical interfaces and therefore is always accessible.
Set the Protocol MTU

For each interface, you can configure an interface-specific MTU by including the `mtu` statement at the [edit interfaces interface-name] hierarchy level. If you need to modify this MTU for a particular protocol family, include the `mtu` statement at the [edit interfaces interface-name unit logical-unit-number family family] hierarchy level:

```
[edit interfaces interface-name unit logical-unit-number family family]
mtu bytes;
```

The default protocol MTU is 4470 bytes for ATM PVC, Cisco HDLC, Frame Relay, and PPP encapsulations. For Ethernet encapsulation on IPv4, the default protocol MTU is 1500 bytes. For Ethernet encapsulation on ISO, the default protocol MTU is 1497 bytes.

For Ethernet encapsulation when the family is `mpls`, the default protocol MTU is 1500 bytes, including 4 to 12 bytes of overhead. The maximum number of DLCIs is determined by the MTU on the interface. If you have keepalives enabled, the maximum number of DLCIs is 1000, with the MTU set to 5012.

When you initially configure an interface, the protocol MTU is calculated automatically. However, if you subsequently change the media MTU, the protocol MTU on existing address families does not automatically adjust.

If you increase the size of the protocol MTU, you must ensure that the size of the media MTU is equal to or greater than the sum of the protocol MTU and the encapsulation overhead. If you reduce the media MTU size, but there are already one or more address families configured and active on the interface, you must also reduce the protocol MTU size. (You configure the media MTU by including the `mtu` statement at the [edit interfaces interface-name] hierarchy level, as discussed in “Configure the Media MTU” on page 47.)

For Ethernet encapsulation when the family is `mpls`, the default protocol MTU is 1500 bytes, including 4 to 12 bytes of overhead. The maximum number of DLCIs is determined by the MTU on the interface. If you have keepalives enabled, the maximum number of DLCIs is 1000, with the MTU set to 5012.

The actual frames transmitted also contain cyclic redundancy check (CRC) bits, which are not part of the MTU. For example, the default protocol MTU for a gigabit Ethernet interface is specified as 1500 bytes, but the largest possible frame size is actually 1504 bytes; you need to consider the extra bits in calculations of MTUs for interoperability.
Disable the Removal of Address and Control Bytes

For PPP CCC-encapsulated interfaces, the address and control bytes are removed by default before the packet is encapsulated into a tunnel.

You can disable the removal of address and control bytes. To do this, include the keep-address-and-control statement at the [edit interfaces interface-name unit logical-unit-number family ccc] hierarchy level:

```
[edit interfaces interface-name unit logical-unit-number family ccc]
keep-address-and-control;
```

When you use PPP CCC encapsulation, and one PE router is running JUNOS Software Release 5.7 or earlier and the other PE router is running JUNOS Software Release 6.0 or later, you must include the keep-address-and-control statement in the configuration of the PE router running JUNOS Software Release 6.0 or later.

Disable the Sending of Asynchronous Notification Upon Link Failure

For PPP- and Cisco HDLC-encapsulated serial interfaces on T-series platforms only, you can disallow sending of asynchronous notification upon link failure. To do this, include the no-asynchronous-notification statement at the [edit interfaces interface-name unit logical-unit-number family (ccc | tcc)] hierarchy level:

```
[edit interfaces interface-name unit logical-unit-number family (ccc | tcc)]
no-asynchronous-notification;
```

Disable the Sending of Redirect Messages on an Interface

By default, the interface sends protocol redirect messages. To disable the sending of these messages on an interface, include the no-redirects statement at the [edit interfaces interface-name unit logical-unit-number family family] hierarchy level:

```
[edit interfaces interface-name unit logical-unit-number family family]
no-redirects;
```

To disable the sending of protocol redirect messages for the entire router, include the no-redirects statement at the [edit system] hierarchy level.

Configure Default, Primary, and Preferred Addresses and Interfaces

The router has a default address and a primary interface, and interfaces have primary and preferred addresses.

The default address of the router is used as the source address on unnumbered interfaces. The routing protocol process tries to pick the default address as the router ID, which is used by protocols, including OSPF and IBGP.

The primary interface for the router is the interface that packets go out when no interface name is specified and when the destination address does not imply a particular outgoing interface.
An interface’s primary address is used by default as the local address for broadcast and multicast packets sourced locally and sent out the interface. An interface’s preferred address is the default local address used for packets sourced by the local router to destinations on the subnet.

The default address of the router is chosen using the following sequence:

1. The primary address on the loopback interface lo0 that is not 127.0.0.1 is used.
2. The primary address on the primary interface is used.

To configure these addresses and interfaces, you can do the following:

- Configure the Primary Interface for the Router on page 85
- Configure the Primary Address for an Interface on page 86
- Configure the Preferred Address for an Interface on page 86

**Configure the Primary Interface for the Router**

The primary interface for the router has the following characteristics:

- It is the interface that packets go out when you type a command such as ping 255.255.255.255—that is, a command that does not include an interface name (there is no interface type 0/0/0.0 qualifier) and where the destination address does not imply any particular outgoing interface.

- It is the interface on which multicast applications running locally on the router, such as SAP, do group joins by default.

- It is the interface from which the default local address is derived for packets sourced out an unnumbered interface if there are no non-127 addresses configured on the loopback interface, lo0.

By default, the multicast-capable interface with the lowest-index address is chosen as the primary interface. If there is no such interface, the point-to-point interface with the lowest index address is chosen. Otherwise, any interface with an address could be picked. In practice, this means that, on the router, the fxp0 interface is picked by default.

To configure a different interface to be the primary interface, include the primary statement at the [edit interfaces interface-name unit logical-unit-number family family] hierarchy level:

```
[edit interfaces interface-name unit logical-unit-number family family]
primary;
```
Configure the Primary Address for an Interface

The primary address on an interface is the address that is used by default as the local address for broadcast and multicast packets sourced locally and sent out the interface. For example, the local address in the packets sent by a ping interface `so-0/0/0.0 255.255.255.255` command is the primary address on interface `so-0/0/0.0`. The primary address flag also can be useful for selecting the local address used for packets sent out unnumbered interfaces when multiple non-127 addresses are configured on the loopback interface, `lo0`. By default, the primary address on an interface is selected as the numerically lowest local address configured on the interface.

To set a different primary address, include the `primary` statement at the `[edit interfaces interface-name unit logical-unit-number family family address address]` hierarchy level:

```
[edit interfaces interface-name unit logical-unit-number family family address address]
primary;
```

Configure the Preferred Address for an Interface

The preferred address on an interface is the default local address used for packets sourced by the local router to destinations on the subnet. By default, the numerically lowest local address is chosen. For example, if the addresses `128.100.1.1/24`, `128.100.1.2/24`, and `128.100.1.3/24` are configured on the same interface, the preferred address on the subnet (by default, `128.100.1.1`) would be used as a local address when you issue a ping `128.100.1.5` command.

To set a different preferred address for the subnet, include the `preferred` statement at the `[edit interfaces interface-name unit logical-unit-number family family address address]` hierarchy level:

```
[edit interfaces interface-name unit logical-unit-number family family address address]
preferred;
```
Apply Policers

Policers allow you to perform simple traffic policing on specific interfaces or Layer 2 VPNs without configuring a firewall filter. To apply policers, include the `policer` statement when configuring the logical interface at the `[edit interfaces interface-name unit logical-unit-number family (ccc | inet | tcc)]` hierarchy level:

```plaintext
[edit interfaces]
  interfaces interface-name {
    unit logical-unit-number {
      family (ccc | inet | tcc) {
        policer {
          arp policer-template-name;
          input policer-template-name;
          output policer-template-name;
        }
      }
    }
  }
```

To use policing on a CCC or TCC interface, you must include the `family (ccc | tcc)` statement at the `[edit interfaces interface-name unit logical-unit-number family inet]` hierarchy level.

In the `arp` statement, list the name of one policer template to be evaluated when Address Resolution Protocol (ARP) packets are received on the interface. By default, an ARP policer is installed that is shared among all the Ethernet interfaces on which you have configured the `family inet` statement. If you want more stringent or lenient policing of ARP packets, you can configure an interface-specific policer and apply it to the interface. You configure an ARP policer just as you would configure any other policer, at the `[edit firewall policer]` hierarchy level. If you apply this policer to an interface, the default ARP packet policer is overridden. If you delete this policer, the default policer takes effect again.

In the `input` statement, list the name of one policer template to be evaluated when packets are received on the interface.

In the `output` statement, list the name of one policer template to be evaluated when packets are transmitted on the interface.

You can configure a different policer on each protocol family under an interface. You can configure one input policer only and one output policer only for each protocol family. You can use the same policer one or more times. On M-series routers, you can apply to multiple interfaces a policer that polices the total traffic arriving on those interfaces. This does not work the same way on T-series platforms because interfaces can reside on different Packet Forwarding Engines (PFEs).

If you apply both policers and firewall filters to an interface, input policers are evaluated before input firewall filters, and output policers are evaluated after output firewall filters.

If you apply the policer to the interface `lo0`, it is applied to packets received or transmitted by the Routing Engine.

For more information about policers, see the JUNOS Internet Software Configuration Guide: Policy Framework.
Apply a Filter to an Interface

To apply firewall filters to an interface, include the filter statement at the [edit interfaces interface-name unit logical-unit-number family (inet | inet6 | mpls)] hierarchy level:

```
[edit interfaces]
  interfaces interface-name {
    unit logical-unit-number {
      family (inet | inet6 | mpls) {
        filter {
          group filter-group-number;
          input filter-name;
          output filter-name;
        }
      }
    }
  }
```

In the group statement, specify the interface group number to associate with the filter.

In the input statement, list the name of one firewall filter to be evaluated when packets are received on the interface.

In the output statement, list the name of one firewall filter to be evaluated when packets are transmitted on the interface.

You can use the same filter one or more times.

For filter-based forwarding (FBF), you can configure input packet filters only; FBF is not supported for output filters.

If you apply the filter to the interface lo0, it is applied to packets received or transmitted by the Routing Engine. You cannot apply MPLS filters to the management interface (fxp0) or the loopback interface (lo0).

For more information about firewall filters, see the JUNOS Internet Software Configuration Guide: Policy Framework. For more information about MPLS filters, see the JUNOS Internet Software Configuration Guide: MPLS Applications. For more information about FBF, see the JUNOS Internet Software Configuration Guide: Routing Protocols.
Define Interface Groups in Firewall Filters

When applying a firewall filter, you can define an interface to be part of an interface group. Packets received on that interface are tagged as being part of the group. You can then match these packets using the interface-group match statement, as described in the JUNOS Internet Software Configuration Guide: Policy Framework.

To define the interface to be part of an interface group, include the group statement at the [edit interfaces interface-name unit logical-unit-number family (inet | inet6 | mpls) filter] hierarchy level:

```plaintext
[edit interfaces]
interfaces interface-name {
  unit logical-unit-number {
    family (inet | inet6 | mpls) {
      filter {
        group filter-group-number;
      }
    }
  }
}
```

Configure Unicast RPF

For interfaces that carry IPv4 or IPv6 traffic, you can reduce the impact of denial of service (DoS) attacks by configuring unicast reverse path forwarding (RPF). Unicast RPF helps determine the source of attacks and rejects packets from unexpected source addresses on interfaces where unicast RPF is enabled.

If you want to configure unicast RPF, your router must be equipped with the Internet Processor II ASIC.

If you enable unicast RPF on live traffic, some packets are dropped while the Packet Forwarding Engine is updating.

The following sections describe unicast RPF in detail:

- Configure Unicast RPF Strict Mode on page 90
- Configure Unicast RPF Loose Mode on page 91
- Unicast RPF and Default Routes on page 91
- Unicast RPF with Routing Asymmetry on page 92
- Example: Configure Unicast RPF on page 93
Configure Unicast RPF Strict Mode

In strict mode, unicast RPF checks whether the incoming packet has a source address that matches a prefix in the routing table, and whether the interface expects to receive a packet with this source address prefix.

If the incoming packet fails the unicast RPF check, the packet is not accepted on the interface. When a packet is not accepted on an interface, unicast RPF counts the packet and sends it to an optional fail filter.

The optional fail filter allows you to apply a filter to packets that fail the unicast RPF check. You can define the fail filter to perform any filter operation, including accepting, rejecting, logging, sampling, or policing.

When unicast RPF is enabled on an interface, Bootstrap Protocol (BOOTP) packets and Dynamic Host Configuration Protocol (DHCP) packets are not accepted on the interface. To allow the interface to accept BOOTP packets and DHCP packets, you must apply a fail filter that accepts all packets with a source address of 0.0.0.0 and a destination address of 255.255.255.255. For a configuration example, see “Example: Configure Unicast RPF” on page 93.

For more information about defining fail filters, see the JUNOS Internet Software Configuration Guide: Policy Framework.

To configure unicast RPF, include the rpf-check statement at the [edit interfaces interface-name unit logical-unit-number family (inet | inet6)] hierarchy level:

[edit interfaces interface-name unit logical-unit-number family (inet | inet6)]
rpf-check <fail-filter filter-name>;

Using unicast RPF can have several consequences when implemented with traffic filters:

- RPF fail filters are evaluated after input filters and before output filters.
- If you configure a filter counter for packets dropped by an input filter, and you want to know the total number of packets dropped, you must also configure a filter counter for packets dropped by the RPF check.
- To count packets that fail the RPF check and are accepted by the RPF fail filter, you must configure a filter counter.
- If an input filter forwards packets anywhere other than the inet.0 or inet6.0 routing tables, the unicast RPF check is not performed.
- If an input filter forwards packets anywhere other than the routing instance the input interface is configured for, the unicast RPF check is not performed.
Configure Unicast RPF Loose Mode

By default, unicast RPF uses strict mode. Unicast RPF loose mode is similar to unicast RPF strict mode and has the same configuration restrictions. The only check in loose mode is whether the packet has a source address with a corresponding prefix in the routing table; loose mode does not check whether the interface expects to receive a packet with a specific source address prefix. If a corresponding prefix is not found, unicast RPF loose mode does not accept the packet. As in strict mode, loose mode counts the failed packet and optionally forwards it to a fail filter, which either accepts, rejects, logs, samples, or polices the packet.

To configure unicast RPF loose mode, include the mode statement at the [edit interfaces interface-name unit logical-unit-number family (inet | inet6) rpf-check] hierarchy level:

```
[edit interfaces interface-name unit logical-unit-number family (inet | inet6)]
rpf-check <fail-filter filter-name> {
    mode loose;
}
```

Unicast RPF and Default Routes

When the active route cannot be chosen from the routes in a routing table, the router chooses a default route. A default route is equivalent to an IP address of 0.0.0.0/0. If you configure a default route and you configure unicast RPF on an interface that the default route uses, unicast RPF behaves differently than it does otherwise. For information about configuring default routes, see the JUNOS Internet Software Configuration Guide: Routing and Routing Protocols. The following sections describe how unicast RPF behaves when a default route uses an interface and when a default route does not use an interface:

- **Unicast RPF Behavior with a Default Route** on page 91
- **Unicast RPF Behavior without a Default Route** on page 92

To determine whether the default route uses an interface, enter the show route command:

```
user@host> show route destination-address
```

destination-address is the next-hop address of the configured default route. The default route uses the interfaces shown in the output of the show route command.

Unicast RPF Behavior with a Default Route

If you configure a default route that uses an interface configured with unicast RPF, unicast RPF behaves as follows:

- **Strict mode**—If no corresponding route is found in the routing table, the packet is accepted. A packet is not accepted when:
  - The packet has a source address that matches a prefix in the routing table.
  - The interface does not expect to receive a packet with this source address prefix.

- **Loose mode**—All packets are automatically accepted. For this reason, we recommend that you not configure unicast RPF loose mode on interfaces that the default route uses.
Unicast RPF Behavior without a Default Route

If you do not configure a default route, or if the default route does not use an interface configured with unicast RPF, unicast RPF behaves as described in “Configure Unicast RPF Strict Mode” on page 90 and “Configure Unicast RPF Loose Mode” on page 91. To summarize, unicast RPF without a default route behaves as follows:

- **Strict mode**—The packet is not accepted when either of the following is true:
  - The packet has a source address that does not match a prefix in the routing table.
  - The interface does not expect to receive a packet with this source address prefix.

- **Loose mode**—The packet is not accepted when the packet has a source address that does not match a prefix in the routing table.

Unicast RPF with Routing Asymmetry

In general, we recommend that you not enable unicast RPF on interfaces that are internal to the network because internal interfaces are likely to have routing asymmetry. Routing asymmetry means that a packet’s outgoing and return paths are different. Routers in the core of the network are more likely to have asymmetric reverse paths than routers at the customer or provider edge. Figure 3 shows unicast RPF in an environment with routing asymmetry.

Figure 3: Unicast RPF with Routing Asymmetry

In Figure 3, if you enable unicast RPF on interface so-0/0/0, traffic destined for Router A is not rejected. If you enable unicast RPF on interface so-1/0/1, traffic from Router A is rejected.

If you need to enable unicast RPF in an asymmetric routing environment, you can use fail filters to allow the router to accept incoming packets that are known to be arriving by specific paths. For an example of a fail filter that accepts packets with a specific source and destination address, see “Example: Configure Unicast RPF” on page 93.
Example: Configure Unicast RPF

Configure unicast RPF strict mode, and apply a fail filter that allows the interface to accept BOOTP packets and DHCP packets. The filter accepts all packets with a source address of 0.0.0.0 and a destination address of 255.255.255.255.

```plaintext
[edit firewall]
filter rpf-special-case-dhcp-bootp {
    term allow-dhcp-bootp {
        from {
            source-address {
                0.0.0.0/32;
            }
            destination-address {
                255.255.255.255/32;
            }
        }
        then {
            count rpf-dhcp-bootp-traffic;
            accept;
        }
    }
    term default {
        then {
            log;
            reject;
        }
    }
}

[edit]
interfaces {
    so-0/0/0 {
        unit 0 {
            family inet {
                rpf-check fail-filter rpf-special-case-dhcp-bootp;
            }
        }
    }
}
```
Enable Source Class and Destination Class Usage

For interfaces that carry IPv4 traffic, you can maintain packet counts based on the entry and exit points for traffic passing through your network. Entry and exit points are identified by source and destination prefixes grouped into disjoint sets defined as source classes and destination classes. You can define classes based on a variety of parameters, such as routing neighbors, autonomous systems, and route filters.

Source class usage (SCU) counts packets sent to customers by performing lookup on the IP source address and the IP destination address. SCU makes it possible to track traffic originating from specific prefixes on the provider core and destined for specific prefixes on the customer edge. You must enable SCU accounting on both the inbound and outbound physical interfaces.

Destination class usage (DCU) counts packets from customers by performing lookup of the IP destination address. DCU makes it possible to track traffic originating from the customer edge and destined for specific prefixes on the provider core router.

Figure 4 illustrates an ISP network. In this topology, you can use DCU to count packets customers send to specific prefixes. For example, you can have three counters, one per customer, that count the packets destined for prefix 210.210/16 and 220.220/16.

You can use SCU to count packets the provider sends from specific prefixes. For example, you can count the packets sent from prefix 210.210/16 and 215.215/16 and transmitted on a specific output interface.
You can configure up to 126 source classes and 126 destination classes. For each interface on which you enable destination class usage and source class usage, the JUNOS software maintains an interface-specific counter for each corresponding class up to the 126 class limit.

To enable packet counting on an interface, include the `accounting` statement at the [edit interfaces interface-name unit logical-unit-number family inet] hierarchy level:

```plaintext
accounting {
    destination-class-usage;
    source-class-usage {
      (input | output | [input output]);
    }
}
```

For SCU to work, you must configure at least one input interface and at least one output interface. An incoming packet is counted only once, and SCU takes priority over DCU. This means that when a packet arrives on an interface on which you include the `source-class-usage input` and `destination-class-usage` statements in the configuration, and when the source and destination both match accounting prefixes, the JUNOS software associates the packet with the source class only. To ensure the outgoing packet is counted, include the `source-class-usage output` statements in the configuration of the outgoing interface.

Once you enable accounting on an interface, the JUNOS software maintains packet counters for that interface. You must then configure the source class and destination class attributes in policy action statements, which must be included in forwarding-table export policies. For a complete discussion about source and destination class accounting profiles, see the JUNOS Internet Software Configuration Guide: Network Management.

**Examples: Enable Source Class and Destination Class Usage**

Configure DCU and SCU output on one interface:

```plaintext
[edit]
interfaces {
  so-6/1/0 {
    unit 0 {
      family inet {
        accounting {
          destination-class-usage;
          source-class-usage {
            (input | output | [input output]);
          }
        }
      }
    }
  }
}
```
Configure SCU input on another interface

```
[edit]
interfaces {
    ge-0/1/0 {
        unit 0 {
            family inet {
                accounting {
                    source-class-usage {
                        input;
                    }
                }
            }
        }
    }
}
```

Optionally, you can include the input and output statements on a single interface

```
[edit]
interfaces {
    ge-0/1/2 {
        unit 0 {
            family inet {
                accounting {
                    source-class-usage {
                        input;
                        output;
                    }
                }
            }
        }
    }
}
```

Enable Packet Counting for Layer 3 VPNs

You can use SCU and DCU to count packets on Layer 3 VPNs. To enable packet counting for Layer 3 VPN implementations at the egress point of the MPLS tunnel, you must configure a virtual loopback tunnel interface (vt) on the PE router, map the VRF instance type to the virtual loopback tunnel interface, and send the traffic received from the VPN out the source class output interface, as shown in the following example:

1. Configure a virtual loopback tunnel interface on a provider edge router equipped with a tunnel PIC:

```
[edit interfaces]
vt-0/3/0 {
    unit 0 {
        family inet {
            accounting {
                source-class-usage {
                        input;
                    }
            }
        }
    }
}
```
2. Map the VRF instance type to the virtual loopback tunnel interface:

```
[edit]
routing-instances {
  VPN-A {
    instance-type vrf;
    interface at-2/1/1.0;
    interface vt-0/3/0.0;
    route-distinguisher 10.255.14.225:100;
    vrf-import import-policy-A;
    vrf-export export-policy-A;
    protocols {
      bgp {
        group to-r4 {
          local-address 10.27.253.1;
          peer-as 400;
          neighbor 10.27.253.2;
        }
      }
    }
  }
}
```

For SCU and DCU to work, you must not include the `vrf-table-label` statement at the `routing-instances instance-name` hierarchy level.

3. Send traffic received from the VPN out the source class output interface:

```
[edit interfaces]
at-1/1/0 {
  unit 0 {
    family inet {
      accounting {
        source-class-usage {
          output;
        }
      }
    }
  }
}
```

For more information about VPNs, see the JUNOS Internet Software Configuration Guide: VPNs. For more information about virtual loopback tunnel interfaces, see “Configure Tunnel Interfaces” on page 407.
Enable Source Class and Destination Class Usage
Chapter 8
Configure Circuit and Translational Cross-Connects

Circuit cross-connect (CCC) and translational cross-connect (TCC) allow you to configure transparent connections between two circuits, where a circuit can be a Frame Relay DLCI, an ATM VC, a PPP interface, a Cisco HDLC interface, or an MPLS label-switched path (LSP). Ethernet interfaces with VLAN tagging enabled can use Ethernet CCC encapsulation.

Using CCC or TCC, packets from the source circuit are delivered to the destination circuit with, at most, the Layer 2 address being changed. No other processing, such as header checksums, TTL decrementing, or protocol processing, is done.

To connect interfaces of the same type, use CCC. To connect unlike interfaces, use TCC.

CCC and TCC circuits fall into three categories: logical interfaces, which include ATM VCs and Frame Relay DLCIs; physical interfaces, which include PPP and Cisco HDLC; and paths, which include LSPs. The three circuit categories provide three types of cross-connect:

- Layer 2 switching (interface-to-interface)—Cross-connects between logical interfaces provide what is essentially Layer 2 switching.
- MPLS tunneling (interface-to-LSP)—Cross-connects between interfaces and LSPs allow you to connect two distant interface circuits by creating MPLS tunnels that use LSPs as the conduit.
- LSP stitching (LSP-to-LSP)—Cross-connects between LSPs provide a way to “stitch” together two label-switched paths, including paths that fall in two different TED areas.

The cross-connect is bidirectional, so packets received on the first interface are transmitted out the second interface, and those received on the second interface are transmitted out the first.

For all CCC connections that connect interfaces, the interfaces must be of the same type; that is, ATM to ATM, Frame Relay to Frame Relay, PPP to PPP, or Cisco HDLC to Cisco HDLC.

For all TCC connections that connect interfaces, the interfaces can be of unlike types. Mainly, TCC is used for Layer 2.5 VPNs, but it can also be used as a simple “unlike circuit” switch.

This chapter discusses the Layer 2 switching cross-connect configuration tasks. For information about MPLS tunneling and LSP stitching, see the JUNOS Internet Software Configuration Guide: MPLS Applications. For information about Layer 2 and Layer 2.5 virtual private networks (VPNs), see the JUNOS Internet Software Configuration Guide: VPNs.
Configure Switching Cross-Connects

Switching cross-connects join logical interfaces to form what is essentially Layer 2 switching.

Figure 5 illustrates a Layer 2 switching circuit cross-connect. In this topology, Router A and Router C have Frame Relay connections to Router B, which is a Juniper Networks router. CCC allows you to configure Router B to act as a Frame Relay (Layer 2) switch. To do this, you configure a circuit from Router A to Router C that passes through Router B, effectively configuring Router B as a Frame Relay switch with respect to these routers. This configuration allows Router B to transparently switch packets (frames) between Router A and Router C without regard to the packets’ contents or the Layer 3 protocols. The only processing that Router B performs is to translate DLCI 600 to 750.

Figure 5: Layer 2 Switching Circuit Cross-Connect

If the Router A–to–Router B and Router B–to–Router C circuits are PPP, for example, the Link Control Protocol and Network Control Protocol exchanges occur between Router A and Router C. These messages are handled transparently by Router B, allowing Router A and Router C to use various PPP options (such as header or address compression and authentication) that Router B might not support. Similarly, Router A and Router C exchange keepalives, providing circuit-to-circuit connectivity status.

You can configure Layer 2 switching cross-connects on PPP, Cisco HDLC, Frame Relay, Ethernet CCC, and ATM circuits. With CCC, only like interfaces can be connected in a single cross-connect. With TCC, unlike interfaces can be connected in a single cross-connect. In Layer 2 switching cross-connects, the exchanges take place between between point-to-point links.

To configure switching cross-connects, you must configure the following on the router that is acting as the switch (Router B in Figure 5):

- Define the Encapsulation for Switching Cross-Connects on page 101
- Define the Connection for Switching Cross-Connects on page 102
- Configure MPLS for Switching Cross-Connects on page 103

- Examples: Configure Switching Cross-Connects on page 103
Define the Encapsulation for Switching Cross-Connects

To configure Layer 2 or Layer 2.5 switching cross-connects, configure the CCC or TCC encapsulation on the router that is acting as the switch (Router B in Figure 5).

When you use CCC encapsulation, you can configure the family ccc only. Likewise, when you use TCC encapsulation, you can configure the family tcc only.

For PPP or Cisco HDLC circuits, specify the encapsulation in the encapsulation statement. This statement configures the entire physical device. For these circuits to work, you must configure a logical interface unit 0.

```
[edit]
interfaces {
  type fpc/pic/port {
    encapsulation (ppp-ccc | cisco-hdlc-ccc | ppp-tcc | cisco-hdlc-tcc);
    unit 0;
  }
}
```

For ATM circuits, specify the encapsulation when configuring the VC. For each VC, you configure whether it is a circuit or a regular logical interface. The default interface type is point-to-point.

```
[edit]
interfaces {
  at-fpc/pic/port {
    atm-options {
      vpi vpi-identifier maximum-vcs maximum-vcs;
    }
    unit logical-unit-number {
      point-to-point;
      encapsulation (atm-ccc-cell-relay | atm-ccc-vc-mux | atm-tcc-vc-mux | atm-tcc-snap);
      vci vci-identifier.vci-identifier;
    }
  }
}
```

For Frame Relay circuits, specify the encapsulation when configuring the DLCI. For each DLCI, you configure whether it is a circuit or a regular logical interface. The DLCI for regular interfaces must be in the range 1 through 511. For CCC and TCC interfaces, it must be in the range 512 through 1022. The default interface type is point-to-point.

```
[edit]
interfaces {
  encapsulation frame-relay-ccc;
  type fpc/pic/port {
    unit logical-unit-number {
      point-to-point;
      encapsulation (frame-relay-ccc | frame-relay-tcc);
      dci dci-identifier;
    }
  }
}
```
For Ethernet CCC circuits, specify the encapsulation in the `encapsulation` statement. This statement configures the entire physical device.

```conf
[edit]
interfaces fe-1/1/0 {
    encapsulation ethernet-ccc;
    unit 0 {
        ...
    }
}
```

For Ethernet VLAN circuits, specify the encapsulation in the `encapsulation` statement. This statement configures the entire physical device. You must also enable VLAN tagging. Ethernet interfaces in VLAN mode can have multiple logical interfaces. For encapsulation type `vlan-ccc`, VLAN IDs 1 through 511 are reserved for normal VLANs, and VLAN IDs 512 through 1023 are reserved for CCC VLANs. For encapsulation type `extended-vlan-ccc`, VLAN IDs 1 through 4094 are valid. VLAN ID 0 is reserved for tagging the priority of frames.

```conf
[edit]
interfaces ge-2/1/0 {
    vlan-tagging;
    encapsulation (extended-vlan-ccc | vlan-ccc);
    unit 0 {
        encapsulation vlan-ccc;
        vlan-id 600;
    }
}
```

Define the Connection for Switching Cross-Connects

To configure Layer 2 switching cross-connects, define the connection between the two circuits. You configure this on the router that is acting as the switch (Router B in Figure 5). The connection joins the interface that comes from the circuit’s source to the interface that leads to the circuit’s destination. When you specify the interface names, include the logical portion of the name, which corresponds to the logical unit number. The cross-connect is bidirectional, so packets received on the first interface are transmitted out the second interface, and those received on the second interface are transmitted out the first.

```conf
[edit]
protocols {
    connections {
        (remote-)interface-switch connection-name {
            interface interface-name.unit-number;
            interface interface-name.unit-number;
        }
    lsp-switch connection-name {
        transmit-lsp lsp-number;
        receive-lsp lsp-number;
    }
}
}
Configure MPLS for Switching Cross-Connects

For Layer 2 switching cross-connects to work, you must configure MPLS. The following is a minimal MPLS configuration:

```
[edit]
protocols {
    mpls {
        interface (interface-name | all);
    }
}
```

For more information, see the JUNOS Internet Software Configuration Guide: MPLS Applications.

Examples: Configure Switching Cross-Connects

Configure a full-duplex Layer 2 switching circuit cross-connect between Router A and Router C, using a Juniper Networks router, Router B, as the virtual switch. See the topology in Figure 6.

Figure 6: Example Topology of a Switching Circuit Cross-Connect with Frame Relay CCC Encapsulation

```
[edit]
interfaces {
    so-1/0/0 {
        encapsulation frame-relayccc;
        unit 1 {
            point-to-point;
            eui-64 frame-relayccc;
            dlci 600;
        }
    }
    so-2/0/0 {
        encapsulation frame-relayccc;
        unit 2 {
            point-to-point;
            encapsulation frame-relayccc;
            dlci 750;
        }
    }
}
```
Configure a full-duplex switching translational cross-connect with PPP TCC encapsulation between Router A and Router C, using a Juniper Networks router, Router B, as the virtual switch. See the topology in Figure 7.

In this topology, Router B has a PPP connection to Router A and an ATM connection to Router C.

Figure 7: Layer 2.5 Switching Translational Cross-Connect
On Router B

```
[edit]
interfaces {
  so-1/0/0 {
    description "to Router A so-0/1/0";
    encapsulation ppp-tcc;
    unit 0 {
      }
  }
  at-1/1/0 {
    description "to Router C at-0/3/0";
    atm-options {
      vpi 0 maximum-vcs 2000;
    }
    unit 32 {
      vci 32;
      encapsulation atm-tcc-vc-mux;
    }
  }
}
[edit]
protocols {
  mpls {
    interface so-1/0/0.0;
    interface at-1/1/0.32;
  }
  connections {
    interface-switch PPP-to-ATM {
      interface so-1/0/0.0;
      interface at-1/1/0.32;
    }
  }
}
```

On Router C

```
[edit]
interfaces {
  at-0/3/0 {
    description "to Router B at-1/1/0";
    atm-options {
      vpi 0 maximum-vcs 2000;
    }
    unit 32 {
      vci 32;
      encapsulation atm-vc-mux;
      family inet {
        address 1.1.1.2/30;
      }
    }
  }
}
```
Chapter 9

Trace Interface Operations

You can trace the operations of individual router interfaces and also those of the interface process (dcd). For a general discussion of tracing and of the precedence of multiple tracing operations, see “Tracing and Logging Operations” in the JUNOS Internet Software Configuration Guide: Getting Started.

This chapter discusses the following interface trace operation configuration tasks:

- Trace Operations of an Individual Router Interface on page 107
- Trace Operations of the Interface Process on page 108

For information about the operations of VRRP-enabled interfaces, see “Trace VRRP Operations” on page 295.

Trace Operations of an Individual Router Interface

To trace the operations of individual router interfaces, include the traceoptions statement at the [edit interfaces interface-name] hierarchy level:

```
[edit interfaces interface-name]
traceoptions {
  flag flag <disable>;
}
```

You can specify the following interface tracing flags:

- all—Trace all interface operations.
- event—Trace all interface events.
- ipc—Trace all interface IPC messages.
- media—Trace all interface media changes.

The interfaces traceoptions statement does not support a trace file. The logging is done by the kernel, so the tracing information is placed in the system syslog files.
Trace Operations of the Interface Process

To trace the operations of the router’s interface process, dcd, include the traceoptions statement at the [edit interfaces] hierarchy level:

```conf
[edit interfaces]
traceoptions {
    file filename <files number> <size size> <(world-readable | no-world-readable)>;
    flag flag <disable>;
}
```

By default, interface process operations are placed in the file named dcd and three 1-MB files of tracing information are maintained.

You can specify the following flags in the interfaces traceoptions statement:

- `change-events`—Log changes that produce configuration events
- `config-states`—Log the configuration state machine changes
- `kernel`—Log configuration IPC messages to kernel
- `kernel-detail`—Log details of configuration messages to kernel

For general information about tracing, see the tracing and logging information in the JUNOS Internet Software Configuration Guide: Getting Started.
Part 3
Interface Types

- Configure Adaptive Services Interfaces on page 111
- Configure ATM 1 and ATM 2 Interfaces on page 117
- Channelized Interfaces Overview on page 163
- Configure Channelized E1 Interfaces on page 173
- Configure Channelized OC-12 Interfaces on page 183
- Configure Channelized STM-1 Interfaces on page 205
- Configure Channelized T3 Interfaces on page 221
- Configure Discard Interfaces on page 241
- Configure E1 Interfaces on page 243
- Configure E3 Interfaces on page 251
- Configure Encryption Interfaces on page 257
- Configure Ethernet Interfaces on page 263
- Configure Frame Relay on page 303
- Configure the Loopback Interface on page 313
- Configure Monitoring Services Interfaces on page 315
- Configure Multilink and Link Services Interfaces on page 319
- Configure Serial Interfaces on page 345
- Configure SONET/SDH Interfaces on page 359
- Configure T1 Interfaces on page 387
- Configure T3 Interfaces on page 395
- Configure Tunnel Interfaces on page 407
- Summary of Interface Configuration Statements on page 417
Chapter 10
Configure Adaptive Services Interfaces

You can configure basic properties of the adaptive services interface on a global level, including default values for system logging, timeout, and intrusion detection properties. To configure properties for the entire interface, you include statements at the [edit interfaces] hierarchy level:

```
[edit]
interfaces interface-name {
    logical-unit-number {
        family inet {
            address address {
                ...
            }
            filter {
                input input-filter-name;
                output output-filter-name;
            }
            policer {
                input input-filter-name;
                output output-filter-name;
            }
            service {
                input {
                    [ service-set service-set-name <service-filter filter-name> ];
                    post-service-filter filter-name;
                }
                output {
                    [ service-set service-set-name <service-filter filter-name> ];
                }
            }
            service-domain (inside | outside);
        }
        service-options {
            inactivity-timeout seconds;
            open-timeout seconds;
            syslog {
                host host-name {
                    facility-override facility-name;
                    log-prefix prefix-number;
                    [ services priority-level ];
                }
            }
        }
    }
}
```
Configure Service Interface Properties

This chapter contains the following sections:

- Configure Service Interface Properties on page 112
- Apply Filters and Services to an Interface on page 114
- Example: Configure a Service Interface on page 115

For detailed information about configuring the Adaptive Services PIC, see the JUNOS Internet Software Configuration Guide: Services Interfaces.

Configure Service Interface Properties

This section describes the following tasks for configuring service sets:

- Configure the Interface Address and Domain on page 112
- Configure Default Timeout Settings on page 113
- Configure Default System Log Properties on page 113

Configure the Interface Address and Domain

Just as you do for other network interfaces, you configure an IP address for a service interface by including the address statement at the [edit interfaces interface-name unit logical-unit-number family inet] hierarchy level:

[edit interfaces interface-name unit logical-unit-number family inet]
address address 
...
}

Assign an IP address to the interface by configuring the address value. The GSP supports only IP4 addresses configured using the family inet statement.

For information on other addressing properties you can configure that are not specific to service interfaces, see “Configure the Interface Address” on page 81.

The service-domain statement specifies whether the interface is used within the network or to communicate with remote devices. The software uses this setting to determine which default stateful firewall rules to apply, and to determine the default direction for service rules. To configure, include the service-domain statement at the [edit interfaces interface-name unit logical-unit-number] hierarchy level:

[edit interfaces interface-name unit logical-unit-number]
service-domain (inside | outside);
Configure Default Timeout Settings

You can specify global default settings for certain timers that apply for the entire interface. There are two statements of this type:

- **inactivity-timeout**—Sets the inactivity timeout period for established flows, after which they are no longer valid.

- **open-timeout**—Sets the timeout period for TCP session establishment, for use with syn-cookie defenses against network intrusion.

To configure a setting for the inactivity timeout period, include the `inactivity-timeout` statement at the `[edit interfaces interface-name service-options]` hierarchy level:

```
[edit interfaces interface-name service-options]
inactivity-timeout seconds;
```

The default value is 30 seconds. The range of possible values is 4 through 65,535 seconds. Any value you configure in the application protocol definition at the `[edit applications]` hierarchy level overrides the value specified here.

To configure a setting for the TCP session establishment timeout period, include the `open-timeout` statement at the `[edit interfaces interface-name service-options]` hierarchy level:

```
[edit interfaces interface-name service-options]
open-timeout seconds;
```

The default value is 30 seconds. Any value you configure in the IDS service definition at the `[edit services ids]` hierarchy level overrides the value specified here.

Configure Default System Log Properties

You specify properties that control how system log messages are generated for the interface as a whole. If you configure different values for the same properties at the `[edit services service-set service-set-name]` hierarchy level, the service-set values override the values configured for the interface.

To configure interface-wide default system logging values, include the `syslog` statement at the `[edit interfaces interface-name service-options]` hierarchy level:

```
[edit interfaces interface-name service-options]
syslog {
    host host-name {
        facility-override facility-name;
        log-prefix prefix-number;
        [ services priority-level ];
    }
}
```

Configure the `host` statement with a hostname that specifies the system log target server. The `hostname local` directs system log messages to the Routing Engine.
You can configure one or more facilities with a specified priority level. The supported facilities are: any, authorization, change-log, conflict-log, cron, daemon, firewall, interactive-commands, kernel, pfe, and user. The valid priority settings are shown in Table 11 on page 114:

Table 11: System Log Priority Level Settings

<table>
<thead>
<tr>
<th>Priority Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>alert</td>
<td>Conditions that should be corrected immediately.</td>
</tr>
<tr>
<td>any</td>
<td>Matches any level.</td>
</tr>
<tr>
<td>critical</td>
<td>Critical conditions.</td>
</tr>
<tr>
<td>emergency</td>
<td>Panic conditions.</td>
</tr>
<tr>
<td>error</td>
<td>Error conditions.</td>
</tr>
<tr>
<td>info</td>
<td>Informational messages.</td>
</tr>
<tr>
<td>notice</td>
<td>Conditions that require special handling.</td>
</tr>
<tr>
<td>warning</td>
<td>Warning messages.</td>
</tr>
</tbody>
</table>

To use one particular facility code for all logging to the specified system log host, include the facility-override statement at the [edit interfaces interface-name service-options syslog host host-name] hierarchy level:

```
[edit interfaces interface-name service-options syslog host host-name]
facility-override facility-name;
```

To specify an address prefix for all logging to this system log host, include the log-prefix statement at the [edit interfaces interface-name service-options syslog host host-name] hierarchy level:

```
[edit interfaces interface-name service-options syslog host host-name]
log-prefix prefix-number;
```

Apply Filters and Services to an Interface

When you have defined and grouped the service rules by configuring the service-set definition, you need to apply services to one or more interfaces installed on the router. To associate a defined service set with an interface, include the service-set statement at the [edit interfaces interface-name unit logical-unit-number family inet service (input | output)] hierarchy level:

```
[edit interfaces interface-name unit logical-unit-number family inet service]
  input {
    [ service-set service-set-name <service-filter filter-name> ];
    post-service-filter filter-name;
  }
  output {
    [ service-set service-set-name <service-filter filter-name> ];
  }
```
You can configure different service sets on the input and output sides of the interface. You can optionally include filters before or after each service set to refine the target and additionally process the traffic. For an example, see “Example: Configure a Service Interface” on page 115.

Example: Configure a Service Interface

The following example applies `my-input-service-set` on an interface-wide basis. All traffic that is accepted by `my-input-filter` has `my-service-set` applied to it. After the service set is applied, additional filtering is done using `my-post-service-input-filter`.

```cml
[edit interfaces fe-0/0/0]
unit 0 {
    family inet {
        filter {
            input my-input-filter;
            output my-output-filter;
        }
        service {
            input {
                service-set my-input-service-set;
                post-service-filter my-post-service-input-filter;
            }
            output {
                service-set my-output-service-set;
            }
        }
    }
}
```
Example: Configure a Service Interface
Chapter 11

Configure ATM 1 and ATM 2 Interfaces

Asynchronous Transfer Mode (ATM) is a network protocol designed to facilitate the simultaneous handling of various types of traffic streams (voice, data, and video) at very high speeds over the same physical connection. By always using 53-byte cells, ATM simplifies the design of hardware, enabling it to quickly determine the destination address of each cell. This allows simple switching of network traffic at much higher speeds than are easily accomplished using protocols with variable sizes of transfer units, such as Frame Relay and TCP/IP.

Although ATM was designed to operate without the requirement of any other networking protocol, other protocols are frequently segmented and encapsulated across multiple, smaller ATM cells; in effect making ATM a transport mechanism for pre-existing technologies such as Frame Relay and the TCP/IP family of protocols.

ATM relies on the concepts of virtual paths and virtual circuits. A virtual path, represented by a specific virtual path identifier (VPI), establishes a route between two devices in a network. Each VPI can contain multiple virtual circuits, each represented by a virtual circuit identifier (VCI).

VPIs and VCIs are local to the router, which means that only the two devices connected by the VCI or VPI need know the details of the connection. In a typical ATM network, user data might traverse multiple connections, using many different VPI and VCI connections. Each end device, just as each device in the network, needs to know only the VCI and VPI information for the path to the next device.

With ATM 2 interfaces, you can configure virtual path (VP) shaping and operation, administration, and maintenance (OAM) F4 cell flows.

This chapter is organized as follows:

- ATM 1 Physical and Logical Interface Properties on page 118
- ATM 2 Physical and Logical Interface Properties on page 120
- Configure ATM 1 and ATM 2 Physical Interface Properties on page 125
- Configure ATM 1 and ATM 2 Logical Interface Properties on page 135
- Configure ATM 1 and ATM 2 Interface Encapsulation on page 146
- Configure E3 and T3 Parameters on ATM 1 Interfaces on page 153
- Configure SONET/SDH Parameters on ATM 1 and ATM 2 Interfaces on page 154
- Configure ATM 2 VC Tunnel CoS Components on page 155
ATM 1 Physical and Logical Interface Properties

To configure ATM 1 physical interface properties, include the atm-options, e3-options, t3-options, and sonet-options statements at the [edit interfaces atm/egp/port] hierarchy level:

[edit interfaces atm/egp/port]
atm-options {
  ilmi;
  pic-type atm1;
  promiscuous-mode {
    [vpi vpi-identifier];
  }
  vpi vpi-identifier {
    maximum-vcs maximum-vcs;
  }
}
e3-options {
  atm-encapsulation (plcp | direct);
  buildout feet;
  framing (g.751 | g.832);
  loopback (local | remote);
  (payload-scrambler | no-payload-scrambler);
}
t3-options {
  atm-encapsulation (plcp | direct);
  buildout feet;
  (cbit-parity | no-cbit-parity);
  loopback (local | remote);
  (payload-scrambler | no-payload-scrambler);
}
sonet-options {
  aps {
    advertise-interval milliseconds;
    authentication-key key;
    force;
    hold-time milliseconds;
    lockout;
    neighbor address;
    paired-group group-name;
    protect-circuit group-name;
    request;
    revert-time seconds;
    working-circuit group-name;
  }
}
bytes {
    e1-quiet value;
    f1 value;
    f2 value;
    s1 value;
    z3 value;
    z4 value;
}
fcs (32 | 16);
loopback (local | remote);
path-trace trace-string;
(paylload-scrambler | no-payload-scrambler);
rfc-2615;
(z0-increment | no-z0-increment);
}

To configure ATM 1 logical interface properties, include the following statements at the [edit interfaces at-fpc/pic/port unit logical-unit-number] hierarchy level:

[edit interfaces at-fpc/pic/port unit logical-unit-number]
allow-any-vci;
multicast-vci vpi-identifier.vci-identifier;
oam-liveness {
    up-count cells;
    down-count cells;
}
oam-period (disable | seconds);
shaping {
    (cbr rate | vbr peak rate sustained rate burst length);
    queue-length number;
}
vci vpi-identifier.vci-identifier;
vpi vpi-identifier;
family inet address address {
multipoint-destination destination-address {
    inverse-arp;
    oam-liveness {
        up-count cells;
        down-count cells;
    }
oam-period (disable | seconds);
    shaping {
        (cbr rate | vbr peak rate sustained rate burst length);
        queue-length number;
    }
vci vpi-identifier.vci-identifier;
}
ATM 2 Physical and Logical Interface Properties

To configure ATM 2 physical interface properties, include the `atm-options` and `sonet-options` statements at the `[edit interfaces atm fpc pic port]` hierarchy level:

```nmos
[edit interfaces atm fpc pic port]
  atm-options {
    cell-bundle-size cells;
    ilmi;
    linear-red-profiles profile-name {
      high-plp-max-threshold percent;
      low-plp-max-threshold percent;
      queue-depth cells high-plp-threshold percent low-plp-threshold percent;
    }
    pic-type atm2;
    promiscuous-mode {
      [vpi vpi-identifier];
    }
    scheduler-maps map-name {
      forwarding-class class-name {
        priority (low | high);
        transmit-weight (cells number | percent number);
        (epd-threshold cells | linear-red-profile profile-name);
      }
      vc-cos-mode (alternate | strict);
    }
    vpi vpi-identifier {
      oam-liveness {
        up-count cells;
        down-count cells;
      }
      oam-period (disable | seconds);
      shaping {
        (cbr rate | rtvbr peak rate sustained rate burst length | vbr peak rate sustained rate burst length);
      }
    }
  }
  sonet-options {
    aps {
      advertise-interval milliseconds;
      authentication-key key;
      force;
      hold-time milliseconds;
      lockout;
      neighbor address;
      paired-group group-name;
      protect-circuit group-name;
      request;
      revert-time seconds;
      working-circuit group-name;
    }
  }
```
ATM 2 Physical and Logical Interface Properties

Bytes

- e1-quiet value;
- f1 value;
- f2 value;
- s1 value;
- z3 value;
- z4 value;

FCS (32 | 16);

Loopback (local | remote);

Path-trace trace-string;

(Payload-scrambler | no-payload-scrambler);

RFC-2615;

(z0-increment | no-z0-increment);

ATM 2 Logical Interface Properties

To configure ATM 2 logical interface properties, include the following statements at the [edit interfaces at-fpc/pic/port unit logical-unit-number] hierarchy level:

- allow-any-vci;
- atm-scheduler-map (map-name | default);
- cell-bundle-size cells;
- epd-threshold cells;
- multicast-vci vpi-identifier.vci-identifier;
- oam-liveness {
  up-count cells;
  down-count cells;
}
- oam-period (disable | seconds);
- shaping {
  (cbr rate | rtvbr peak rate sustained rate burst length | vbr peak rate sustained rate burst length);
}
- transmit-weight number;
- vci vpi-identifier.vci-identifier;
- family inet address address {
  multipoint-destination destination-address
  epd-threshold cells;
  inverse-arp;
  oam-liveness {
    up-count cells;
    down-count cells;
  }
  oam-period (disable | seconds);
  shaping {
    (cbr rate | rtvbr peak rate sustained rate burst length | vbr peak rate sustained rate burst length);
  }
  transmit-weight number;
  vci vpi-identifier.vci-identifier;
}
Table 12 lists differences between ATM 1 and ATM 2 interfaces.

<table>
<thead>
<tr>
<th>Item</th>
<th>ATM 1</th>
<th>ATM 2</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encapsulation and Transport Modes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>■ ATM Adaptation Layer 5 (AAL5) CCC</td>
<td>Supported</td>
<td>Supported</td>
<td>For ATM 1 and ATM 2 PICs, you can configure any combination of AAL5 CCC, non-promiscuous cell relay, and AAL5 PVCs on the same PIC at the same time. See “Configure ATM 1 and ATM 2 Interface Encapsulation” on page 146.</td>
</tr>
<tr>
<td>■ Cell-Relay accumulation mode:</td>
<td>Supported</td>
<td>Not supported</td>
<td>Cell-relay accumulation mode is per PIC, not per port. If you configure accumulation mode, the entire ATM 1 PIC uses the configured mode. See “Configure ATM 1 and ATM 2 Interface Encapsulation” on page 146.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>■ Cell-Relay promiscuous VPI mode</td>
<td>Supported</td>
<td>Supported</td>
<td>For multiport PICs, you must configure all ports in either promiscuous mode or non-promiscuous mode. For promiscuous mode, you must configure all ports with atm-ccc-cell-relay encapsulation. When in promiscuous mode, no other non-promiscuous cell relay, AAL5 CCC, AAL5 PVCs, or Layer 2 Circuit modes are supported on the PIC at the same time. For ATM 1 and ATM 2 PICs, you can configure both VPI and port modes on different physical interfaces on the same PIC. See “Configure ATM 1 and ATM 2 Cell-Relay Promiscuous Mode” on page 127.</td>
</tr>
<tr>
<td>■ Cell-Relay promiscuous VPI mode</td>
<td>Supported</td>
<td>Supported</td>
<td></td>
</tr>
<tr>
<td>■ Cell-relay VCI mode:</td>
<td>Supported</td>
<td>Supported</td>
<td>For ATM 1 PICs, non-promiscuous cell-relay VCI, VPI and port modes are supported on the same PIC with ATM AAL5 PVCs or ATM AAL5 CCC.</td>
</tr>
<tr>
<td>■ Cell-relay VPI mode:</td>
<td>Supported</td>
<td>Not supported</td>
<td>For ATM 2 PICs, non-promiscuous cell-relay VCI mode is supported on the same PIC with ATM AAL5 PVCs or ATM AAL5 CCC. See “Configure ATM 1 and ATM 2 Interface Encapsulation” on page 146.</td>
</tr>
<tr>
<td>■ Cell-relay port mode:</td>
<td>Supported</td>
<td>Not supported</td>
<td></td>
</tr>
<tr>
<td>■ Ethernet over ATM encapsulation:</td>
<td>Supported</td>
<td>Supported</td>
<td>See “Configure ATM 1 and ATM 2 Interface Encapsulation” on page 146.</td>
</tr>
<tr>
<td>Item</td>
<td>ATM 1</td>
<td>ATM 2</td>
<td>Comments</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>------------------</td>
<td>------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Layer 2 circuit cell-relay and Layer 2 circuit AAL5 transport modes:</td>
<td>Not supported</td>
<td>Supported</td>
<td>Transport mode is per PIC, not per port. If you configure Layer 2 circuit cell-relay or Layer 2 circuit AAL5 transport mode, the entire ATM 2 PIC uses the configured transport mode. Layer 2 Circuit cell-relay mode supports both VP- and port-promiscuous modes. See “Configure ATM 2 Layer 2 Circuit Transport Mode” on page 130 and “Configure ATM 2 Layer 2 Circuit Cell-Relay Promiscuous Mode” on page 132.</td>
</tr>
<tr>
<td>Allows you to send ATM cells or AAL5 PDUs between ATM 2 interfaces</td>
<td></td>
<td></td>
<td>across a Layer 2 circuit-enabled network. Layer 2 circuits are designed to transport Layer 2 frames between provider edge (PE) routers across a Label Distribution Protocol (LDP)-signaled MPLS backbone.</td>
</tr>
<tr>
<td>Layer 2 VPN cell relay and Layer 2 VPN AAL5: Allow you to carry ATM cells or AAL5 PDUs over an MPLS backbone.</td>
<td>Supported</td>
<td>Supported</td>
<td>See the JUNOS Internet Software Guide: VPNs.</td>
</tr>
<tr>
<td>PPP over ATM encapsulation: Associates a PPP link with an ATM AAL5 PVC</td>
<td>Not supported</td>
<td>Supported</td>
<td>For ATM 2 interfaces, the JUNOS software supports three PPP over ATM encapsulation types: atm-ppp-llc—PPP over ATM adaptation layer 5 (AAL5) logical link control (LLC). atm-ppp-vc-mux—PPP over ATM adaptation layer 5 (AAL5) multiplex. atm-mlppp-llc—Multilink PPP over ATM adaptation layer 5 (AAL5) logical link control (LLC). Requires a Link Services PIC. See “Configure PPP over ATM 2 Encapsulation” on page 150.</td>
</tr>
<tr>
<td>OAM F4 Cell Flows: Identify and report virtual path connection (VPC) defects and failures.</td>
<td>Not supported</td>
<td>Supported</td>
<td>See “Configure the ATM 2 OAM F4 Cell Flows” on page 133.</td>
</tr>
<tr>
<td>OAM F5 Loopback Cell Responses</td>
<td>Supported</td>
<td>Supported</td>
<td>For ATM 1 interfaces, when an OAM F5 loopback request is received, the response cell is sent by the PIC. The request and response cells are not counted in the VC, logical interface, or physical interface statistics. For ATM 2 interfaces, when an OAM F5 loopback request is received, the response is sent by the routing engine. The OAM, VC, logical interface, and physical interface statistics are incremented. See “Define the ATM 1 and ATM 2 OAM F5 Loopback Cell Period” on page 144 and “Configure the ATM 1 and ATM 2 OAM F5 Loopback Cell Threshold” on page 145.</td>
</tr>
<tr>
<td>PIC Type</td>
<td>Supported</td>
<td>Supported</td>
<td>For ATM 1 interfaces, you can include the pic-type atm1 statement. For ATM 2 interfaces, you can include the pic-type atm2 statement. See “Configure the ATM 1 and ATM 2 PIC Type” on page 126.</td>
</tr>
</tbody>
</table>
For ATM 1 and ATM 2 interfaces, when you issue the ATM ping command, you must include a logical unit number in the interface name, as shown in the following example:

```
ping atm interface at-1/0/0.5 vci 0.123 count 3
```

The logical unit number is 5 on physical interface at-1/0/0.

See the JUNOS Operational Mode Command Reference: Protocols, Class of Service, Chassis, and Management.

<table>
<thead>
<tr>
<th>Item</th>
<th>ATM 1</th>
<th>ATM 2</th>
<th>Comments</th>
</tr>
</thead>
</table>
| Ping                                   | Supported | Supported | For ATM 1 and ATM 2 interfaces, when you issue the ATM ping command, you must include a logical unit number in the interface name, as shown in the following example:

```
ping atm interface at-1/0/0.5 vci 0.123 count 3
```

The logical unit number is 5 on physical interface at-1/0/0.

See the JUNOS Operational Mode Command Reference: Protocols, Class of Service, Chassis, and Management. |
| Queue Length: Limits the queue size in packets of a particular VC | Supported | Not Supported | See “Configure the ATM 1 Queue Length” on page 142. |
| EPD Threshold: Limits the queue size in ATM cells of a particular VC or forwarding class configured over a VC when using VC Tunnel CoS. When the first ATM cell of a new packet is received, the VC’s queue depth is checked against the EPD threshold. If the VC’s queue depth exceeds the EPD threshold, the first and all subsequent ATM cells in the packet are discarded. | Not Supported | Supported | If you are using VC Tunnel CoS, the EPD threshold configured at the logical unit level has no effect. You should configure each forwarding class for congestion management using either an individual EPD threshold (in other words, tail drop) or weighted random early detection (WRED) profile. See “Configure the ATM 2 EPD Threshold” on page 143 and “Configure ATM 2 VC Tunnel CoS Components” on page 155. |
| Real-time VBR: Supports variable bit rate data traffic with average and peak traffic parameters. | Not supported | Supported | Compared to non-real-time VBR, real-time VBR data is serviced at a higher priority. Real-time VBR is suitable for carrying packetized video and audio. See “Configure ATM 2 Real-Time VBR” on page 139. |
| VC Tunnel CoS: Allows VCs to be opened as VC tunnels. | Not supported | Supported | A VC tunnel can support four CoS queue. Within the VC tunnel, the class-based weighted fair queuing algorithm is used to schedule packet transmission from each queue. You can configure the queue admission policies, such as EPD or WRED, to control the queue size during congestion. See “Configure ATM 2 VC Tunnel CoS Components” on page 155. |
Configure ATM 1 and ATM 2 Physical Interface Properties

You can configure the following ATM 1- and ATM 2-specific physical interface properties:

- Configure Communication with Directly Attached ATM 1 and ATM 2 Switches on page 126
- Configure the ATM 1 and ATM 2 PIC Type on page 126
- Configure ATM 1 and ATM 2 Cell-Relay Promiscuous Mode on page 127

You can configure the following ATM 1-specific property:

- Configure the Maximum Number of ATM 1 VCs on a VP on page 129

You can configure the following ATM 2-specific properties:

- Configure ATM 2 Layer 2 Circuit Transport Mode on page 130
- Configure ATM 2 Layer 2 Circuit Cell-Relay Promiscuous Mode on page 132
- Configure the ATM 2 Layer 2 Circuit Cell-Relay Cell Maximum on page 133
- Configure the ATM 2 OAM F4 Cell Flows on page 133
- Define Virtual Path Tunnels on ATM 2 Interfaces on page 134

<table>
<thead>
<tr>
<th>Item</th>
<th>ATM 1</th>
<th>ATM 2</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>VCI Management</td>
<td>Supported.</td>
<td>Supported.</td>
<td>For ATM 1 interfaces, the allowable maximum number of VCs differs by interface type:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- ATM T3 and E3–4090</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- ATM OC-3–8180</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- ATM OC-12–16,360</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>See “Configure the Maximum Number of ATM 1 VCs on a VP” on page 129.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>For ATM 2 interfaces, the total number of VCIs that you can open on an ATM 2 port depends on two factors:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Number of tunnels</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Sparseness of VCI numbers (the more sparse, the fewer VCIs supported)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>For ATM 1 and ATM 2 interfaces with promiscuous mode, the allowable maximum number of VCIs is 65,535.</td>
</tr>
<tr>
<td>VCI Statistics</td>
<td>Supported</td>
<td>Supported</td>
<td>For ATM 1 interfaces, multipoint VCI statistics are collected from indirect sources.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>For ATM 2 interfaces, multipoint VCI statistics are collected directly from the PIC.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>For ATM 1 and ATM 2 interfaces, point-to-point VCI statistics are the same as logical interface statistics.</td>
</tr>
</tbody>
</table>
Configure Communication with Directly Attached ATM 1 and ATM 2 Switches

For ATM 1 and ATM 2 interfaces, you can configure communication to directly attached ATM switches to enable querying of the IP addresses and switch port numbers. You query the switch by entering the following `show` command:

```
user@host> show ilmi interface interface-name
```

The router uses VC 0.16 to communicate with the ATM switch.

To configure communication between the router and its directly attached ATM switches, include the `ilmi` statement at the `[edit interfaces interface-name atm-options]` hierarchy level:

```
[edit interfaces interface-name atm-options]
ilmi;
```

Configure the ATM 1 and ATM 2 PIC Type

For ATM 1 and ATM 2 interfaces, the JUNOS software does not determine from the interface name the PIC type. You can configure the PIC type as ATM 1 or ATM 2 by including the `pic-type` statement at the `[edit interfaces interface-name atm-options]` hierarchy level:

```
[edit interfaces interface-name atm-options]
pic-type (atm1 | atm2);
```

The following guidelines apply to configuring the ATM PIC type:

- If you include the `pic-type` statement in the configuration, and you include other statements at the `[edit interfaces interface-name atm-options]` hierarchy level that do not match the configured PIC type, the configuration does not commit; for example, you cannot commit a configuration that includes the `pic-type atm2` statement and the `maximum-vcs` statement.

- If you do not include the `pic-type` statement and you do include the `maximum-vcs` statement in the configuration, the JUNOS software assumes you are configuring an ATM 1 interface, and sets the PIC type option accordingly; if you do not include the `maximum-vcs` statement in the configuration, the JUNOS software assumes you are configuring an ATM 2 interface, and sets the PIC type option accordingly.

- If you include the `promiscuous-mode` statement in the configuration of an ATM 2 interface, you must also include the `pic-type atm2` statement.
Example: Configure the ATM 1 and ATM 2 PIC Type

Configure the PIC type on an ATM 1 and an ATM 2 interface.

On an ATM 1 interface

```conf
[edit interfaces]
at-1/0/0 {  
atm-options {  
    pic-type atm1;  
    vpi 0 maximum-vcs 256;  
    vpi 1 maximum-vcs 512;  
  }
  ...
}
```

On an ATM 2 interface

```conf
[edit interfaces]
at-1/1/0 {  
atm-options {  
    pic-type atm2;  
    vpi 0;  
    vpi 2 {  
        oam-period 6;  
    }
  }
  ...
}
```

Configure ATM 1 and ATM 2 Cell-Relay Promiscuous Mode

For ATM 1 and ATM 2 interfaces with atmccc-cell-relay encapsulation, you can map all incoming cells from either an interface port or a virtual path (VP) to a single LSP without restricting the VCI number. Promiscuous mode allows you to map traffic from all 65,535 VCIs to a single LSP, or from all 256 VPIs to a single LSP.

For ATM 1 and ATM 2 interfaces, changing modes between promiscuous and non-promiscuous causes all physical interfaces to be deleted and re-added.

To map incoming traffic from a port or VC to an LSP, include the promiscuous-mode statement at the [edit interfaces interface-name atm-options] hierarchy level:

```conf
[edit interfaces interface-name]
atm-options {  
    promiscuous-mode {  
        [vpi vpi-identifier];  
    }
}
```

For multiport PICs, all ports must be configured in either promiscuous mode or non-promiscuous mode. For promiscuous mode, you must configure all ports with atmccc-cell-relay encapsulation.

When you configure interfaces to use promiscuous mode, you cannot configure VCIs.

For the ATM 2 PIC, if you include the promiscuous-mode statement in the configuration, you must also include the pic-type atm2 statement. For more information, see “Configure the ATM 1 and ATM 2 PIC Type” on page 126.
Example: Configure ATM 1 and ATM 2 Cell-Relay Promiscuous Mode

To map incoming traffic from a port to an LSP, include the allow-any-vci statement at the
[edit interfaces interface-name unit 0] hierarchy level. When you include the allow-any-vci
statement, you cannot configure other logical interfaces in the same physical interface. Next,
you must map unit 0 to an LSP using the CCC connection.

[edit interfaces at-1/2/0]
encapsulation atm-ccc-cell-relay;
atm-options {
    promiscuous-mode;
}
unit 0 {
    allow-any-vci;
}

Map unit 0 to an LSP
protocols {
    connections {
        remote-interface-switch router-a-router-c {
            interface at-1/2/0.0;
        }
        lsp-switch router-a-router-c {
            transmit-lsp lsp1
            receive-lsp lsp2;
        }
    }
}

Map a VPI to an LSP
To map a VPI to an LSP, you must define the allowed VPIs. You can configure one or more
logical interfaces, each mapped to a different VPI. You can then route traffic from each of
these interfaces to different LSPs.

[edit interfaces at-1/1/0]
encapsulation atm-ccc-cell-relay;
atm-options {
    pic-type atm1;
    promiscuous-mode {
        vpi 10;
        vpi 20;
    }
}
unit 0 {
    encapsulation atm-ccc-cell-relay;
    vpi 10;
}
unit 1 {
    encapsulation atm-ccc-cell-relay;
    vpi 20;
}
Configure ATM 1 and ATM 2 Physical Interface Properties

[edit interfaces at-3/1/0]
encapsulation atm-ccc-cell-relay;
atm-options {
    pic-type atm2;
    promiscuous-mode {
        vpi 10;
        vpi 20;
    }
}
unit 0 {
    encapsulation atm-ccc-cell-relay;
    vpi 10;
}
unit 1 {
    encapsulation atm-ccc-cell-relay;
    vpi 20;
}
[edit protocols]
mpls {
    interface-switch router-a-router-c {
        interface at-1/1/0.0;
        interface at-3/1/0.0;
    }
    interface-switch router-a-router-d {
        interface at-1/1/0.1;
        interface at-3/1/0.1;
    }
}

Configure the Maximum Number of ATM 1 VCs on a VP

For ATM 1 interfaces, you must configure the maximum number of virtual circuits (VCs) allowed on a virtual path (VP) so that sufficient memory on the ATM 1 PIC can be allocated for each VC.

To configure the highest-numbered VCs on a VP, include the `vpi` and `maximum-vcs` statements at the `[edit interfaces interface-name atm-options]` hierarchy level:

```
[edit interfaces interface-name atm-options]
vpi vpi-identifier maximum-vcs maximum-vcs;
```

The VP identifier can be a value from 0 through 255. For most interfaces, you can define a maximum of 4090 VCs per interface. The highest-numbered VC value you can configure is 4089. For ATM OC-3 interfaces, you can define a maximum of 8180 VCs per interface. For ATM OC-12 interfaces, you can define a maximum of 16,360 VCs per interface. Promiscuous mode removes these limits. For more information, see “Configure ATM 1 and ATM 2 Cell-Relay Promiscuous Mode” on page 127.

All VPIs that you configure in the `atm-options` statement are stored in a single table. If you modify the VPIs—for example, by editing them in configuration mode or by issuing a `load override` command—all VCs on the interface are closed and then reopened, resulting in a temporary loss of connectivity for all the VCs on the interface.
You can also include some of the statements in the `sonet-options` statement to set SONET parameters on ATM interfaces, as described in "Configure SONET/SDH Parameters on ATM 1 and ATM 2 Interfaces" on page 154.

**Configure ATM 2 Layer 2 Circuit Transport Mode**

On ATM 2 interfaces only, you can configure Layer 2 circuit cell-relay or Layer 2 circuit ATM Adaptation Layer 5 (AAL5) transport mode, as defined in the Internet Engineering Task Force (IETF) document, *Encapsulation Methods for Transport of Layer 2 Frames Over IP and MPLS Networks*.

Layer 2 circuit cell-relay and Layer 2 circuit AAL5 transport modes allow you to send ATM cells between ATM 2 interfaces across a Layer 2 circuit-enabled network. Layer 2 circuits are designed to transport Layer 2 frames between provider edge (PE) routers across a Label Distribution Protocol (LDP)-signaled MPLS backbone. You use Layer 2 circuit AAL5 transport mode to send AAL5 SAR-PDUs (segmentation and reassembly protocol data units) over the Layer 2 circuit.

By default, ATM 2 PICs are in standard AAL5 transport mode. Standard AAL5 allows multiple applications to tunnel the protocol data units of their Layer 2 protocols over an ATM virtual circuit. Encapsulation of these Layer 2 protocol data units allows a number of these emulated virtual circuits to be carried in a single tunnel. Protocol data units are segmented at one end of the tunnel and reassembled at the other end. The ingress router reassembles the protocol data units received from the incoming VC and transports each PDU as a single packet.

In contrast, Layer 2 circuit cell-relay and Layer 2 circuit AAL5 transport modes accept a stream of ATM cells, convert these to an encapsulated Layer 2 format, then tunnel them over an MPLS or IP backbone, where a similarly configured router segments these packets back into a stream of ATM cells, to be forwarded to the virtual circuit configured for the far-end router.

In Layer 2 circuit cell-relay transport mode, ATM cells are bundled together and transported in packet form to the far-end router, where they are segmented back into individual ATM cells and forwarded to the ATM virtual circuit configured for the far-end router.

The uses for the three transport modes are defined as follows:

- To tunnel IP packets over an ATM backbone, use the default standard AAL5 transport mode.
- To tunnel a stream of AAL5-encoded ATM SAR-PDUs over an MPLS or IP backbone, use Layer 2 circuit AAL5 transport mode.
- To tunnel a stream of ATM cells over an MPLS or IP backbone, use Layer 2 circuit cell-relay transport mode.

You can transport AAL5-encoded traffic with Layer 2 circuit cell-relay transport mode, because Layer 2 circuit cell-relay transport mode ignores the encoding of the cell data presented to the ingress interface.

When you configure AAL5 mode Layer 2 circuits, the control word carries cell loss priority (CLP) information by default.
To configure Layer 2 circuit AAL5 or Layer 2 circuit cell-relay, you must include the atm-l2circuit-mode statement at the [edit chassis fpc fpc-slot pic pic-slot] hierarchy level, specifying aal5 or cell; identify the interface as an ATM 2 interface by including the pic-type atm2 statement at the [edit atm/fpc pic port atm-options] hierarchy level; and include the encapsulation statement at the [edit atm/fpc pic port unit logical-unit-number] hierarchy level, specifying atm-ccc-vc-mux for Layer 2 circuit AAL5 or atm-ccc-cell-relay for Layer 2 circuit cell-relay:

```
[edit chassis fpc slot-number pic pic-number]
atm-l2circuit-mode (cell | aal5);
```

```
[edit interfaces interface-name atm-options]
pic-type atm2;
```

```
[edit interfaces interface-name unit logical-unit-number]
encapsulation (atm-ccc-vc-mux | atm-ccc-cell-relay);
```

Transport mode is per PIC, not per port. If you do not include the atm-l2circuit-mode statement in the configuration, the ATM 2 PIC uses standard AAL5 transport mode. If you configure Layer 2 circuit cell-relay or Layer 2 circuit AAL5 transport mode, the entire ATM 2 PIC uses the configured transport mode.

For more information about Layer 2 circuits, see the JUNOS Internet Software Configuration Guide: VPNs and the JUNOS Internet Software Configuration Guide: Routing and Routing Protocols. For a comprehensive example, see the JUNOS Internet Software Feature Guide.

**Example: Configure ATM 2 Layer 2 Circuit Transport Mode**

Configure Layer 2 circuit AAL5 transport mode and cell-relay transport mode:

```
Configure Layer 2 circuit AAL5 transport mode
[edit chassis]
fpc 0 {
    pic 1 {
        atm-l2circuit-mode aal5;
    }
}

[edit interfaces]
at-o/1/0 {
    atm-options {
        pic-type atm2;
        vpi 0;
    }
    unit 0 {
        encapsulation atm-ccc-vc-mux;
        point-to-point;
        vci 0.32;
    }
}
```
Configure Layer 2 circuit cell-relay transport mode

```
[edit chassis]
fpc 0 {
    pic 1 {
        atm-l2circuit-mode cell;
    }
}

[edit interfaces]
at-0/1/0 {
    atm-options {
        pic-type atm2;
        vpi 0;
    }
    unit 0 {
        encapsulation atm-ccc-cell-relay;
        point-to-point;
        vci 0.32;
    }
}
```

**Configure ATM 2 Layer 2 Circuit Cell-Relay Promiscuous Mode**

By default, all incoming cells are mapped from a single VC to an external LSP. For ATM interfaces with Layer 2 circuit cell-relay transport mode and `atm-ccc-cell-relay` encapsulation, you can configure promiscuous mode. Promiscuous mode allows you to map all incoming cells from either an interface port or a VP to a single LSP without restricting the VCI number. You can map traffic from all 65,535 VCI s to a single LSP, or from all 256 VPI s to a single LSP. For promiscuous-mode configuration guidelines, see "Configure ATM 1 and ATM 2 Cell-Relay Promiscuous Mode" on page 127.

**Example: Configure ATM 2 Layer 2 Circuit Cell-Relay Promiscuous Mode**

Configure Layer 2 circuit cell-relay VP- and port-promiscuous mode:

```
VP-promiscuous mode
[edit interfaces]
at-0/1/0 {
    encapsulation atm-ccc-cell-relay;
    atm-options {
        pic-type atm2;
        cell-bundle-size 4;
        promiscuous-mode {
            vpi 0;
        }
    }
    unit 0 {
        encapsulation atm-ccc-cell-relay;
        point-to-point;
        vci 0.32;
    }
}
```
Port-promiscuous mode

```plaintext
[edit interfaces]
at-0/1/0 {
  encapsulation atm-ccc-cell-relay;
  atm-options {
    pic-type atm2;
    promiscuous-mode;
  }
  unit 0 {
    allow-any-vci;
  }
}
```

**Configure the ATM 2 Layer 2 Circuit Cell-Relay Cell Maximum**

By default, each frame contains up to one cell. For ATM interfaces with Layer 2 circuit cell-relay transport mode configured, you can configure the maximum number of ATM cells per frame on the physical or logical interface. To set the maximum number of cells per frame, include the `cell-bundle-size` statement at the [edit interfaces interface-name atm-options] or [edit interfaces interface-name unit logical-unit-number] hierarchy level:

```plaintext
cell-bundle-size cells;
```

The cell bundle size can be in the range 1 through 190.

If you include the `cell-bundle-size` statement at the [edit interfaces interface-name atm-options] hierarchy level, then the configured value becomes the default for all the logical interface units configured for this physical interface. If you include the `cell-bundle-size` statement at the [edit interfaces interface-name unit logical-unit-number] hierarchy level, then for this logical interface the configured value overrides the default value.

The transmit rates you configure on the routers at each end of the connection must be the same value.

**Configure the ATM 2 OAM F4 Cell Flows**

For ATM 2 interfaces, the F4 flow cell is used for management of the VP level. If your router is equipped with an ATM 2 PIC, you can configure OAM F4 cell flows to identify and report virtual path connection (VPC) defects and failures. The JUNOS software supports three types of OAM F4 cells in end-to-end F4 flows:

- Virtual Path Alarm Indication Signal (VP-AIS)
- Virtual Path Remote Defect Indication (VP-RDI)
- Virtual Path Loopback Cells

The JUNOS software does not support segment F4 flows, VPC continuity check, or VP performance management functions.

On each VP, you can configure an interval time during which to transmit loopback cells by including the `oam-period` statement at the [edit interfaces interface-name atm-options vpi vpi-identifier] hierarchy level:

```plaintext
[edit interfaces interface-name atm-options vpi vpi-identifier]
oam-period (disable | seconds);
```
When you add a VPI at the atm-options hierarchy, an end-to-end F4 VCI is automatically opened to send and receive OAM F4, VP-AIS, and VP-RDI cells. If you enable OAM by including the oam-period statement in the configuration, the router sends and receives OAM F4 loopback cells.

To modify OAM liveness values on a VP, include the oam-liveness statement at the [edit interfaces interface-name atm-options vpi vpi-identifier] hierarchy level:

```
[edit interfaces interface-name atm-options vpi vpi-identifier]
  oam-liveness {
    up-count cells;
    down-count cells;
  }
```

up-count is the minimum number of consecutive OAM F4 loopback cells received on a VPI before a VPI is declared up.

down-count is the minimum number of consecutive OAM F4 Loopback cells lost before a VPI is declared down.

When a VP-AIS or VP-RDI cell is received, the VPI is marked down. When a VP-AIS cell is received on a VPI, a VP-RDI is generated and transmitted on the same VPI. When an OAM F4 loopback request cell is received, the router sends a loopback reply cell, even if the oam-period statement is not included in the configuration of the VPI.

When a VPI is marked down because the VPI receives AIS or RDI cells, or because the VPI does not receive down-count consecutive OAM F4 loopback replies, all the VCIs that belong to the VPI are marked down. When a VPI is marked up, all the VCIs that belong to the VPI are marked up. The status of logical interfaces is also changed when the status of the last VCI on that interface is changed.

For a configuration example, see “Examples: Configure ATM 2 Interfaces” on page 161.

**Define Virtual Path Tunnels on ATM 2 Interfaces**

For ATM 2 interfaces, you can configure shaping on a VPI. When you do this, the VPI is called a VP tunnel. If your router is equipped with an ATM 2 PIC, you can configure VP tunnels and a weight for each VC. Each VC is serviced in weighted round robin (WRR) mode. When VCs have data to send, they send the number of cells equal to their weight before passing control to the next active VC. This allows proportional bandwidth sharing between multiple VCs within a rate-shaped VP tunnel. VP tunnels are not supported on point-to-multipoint interfaces.

If you change or delete VP tunnel traffic shaping, all logical interfaces on a VP are deleted and re-added.

All VPIs you configure at the [edit interfaces interface-name unit logical-unit-number] hierarchy level must also be configured at the [edit interfaces interface-name atm-options] hierarchy level.

When you configure a VPI without shaping parameters, the VPI is a regular VPI; no shaping is attached. VCIs that belong to non-shaped VPIs can have VCI shaping.
For point-to-point interfaces, include the shaping statement at the [edit interfaces interface-name atm-options vpi vpi-identifier] hierarchy level:

[edit interfaces interface-name atm-options vpi vpi-identifier]
shaping {
  (cbr rate | rtvbr peak rate sustained rate burst length |
    vbr peak rate sustained rate burst length);
  queue-length number;
}

For cbr, vbr, and burst statement usage guidelines, see “Define the ATM 1 and ATM 2 Traffic-Shaping Profile” on page 137. For information about ATM 2 shaping values, see “Specify ATM 2 Shaping Values” on page 142.

Configure ATM 1 and ATM 2 Logical Interface Properties

When you use ATM encapsulation on an interface, you must map each logical interface to a virtual circuit identifier (VCI). You can optionally map logical interfaces to a virtual path identifier (VPI).

An ATM interface can be a point-to-point interface or a point-to-multipoint (also called a multipoint nonbroadcast multiaccess [NBMA]) connection.

You can configure the following ATM 1- and ATM 2-specific logical interface properties:

- Configure a Point-to-Point ATM 1 or ATM 2 Connection on page 136
- Configure a Point-to-Multipoint ATM 1 or ATM 2 Connection on page 136
- Configure a Multicast-Capable ATM 1 or ATM 2 Connection on page 137
- Configure Inverse ATM 1 or ATM 2 ARP on page 137
- Define the ATM 1 and ATM 2 Traffic-Shaping Profile on page 137
- Configure the ATM 1 Queue Length on page 142
- Configure the ATM 2 EPD Threshold on page 143
- Configure the ATM 2 Transmission Weight on page 144
- Define the ATM 1 and ATM 2 OAM F5 Loopback Cell Period on page 144
- Configure the ATM 1 and ATM 2 OAM F5 Loopback Cell Threshold on page 145
Configure a Point-to-Point ATM 1 or ATM 2 Connection

For ATM 1 and ATM 2 interfaces, you can configure a VCI and a VPI on a point-to-point ATM interface by including the `vci` statement at the `[edit interfaces interface-name unit logical-unit-number]` hierarchy level:

```plaintext
  [edit interfaces interface-name unit logical-unit-number]
  vci vpi-identifier.vci-identifier;
```

For each VCI, you configure the VCI and VPI identifiers. The default VPI identifier is 0. For ATM 1 interfaces, the VCI identifier cannot exceed the highest-numbered VC configured for the interface with the `vpi` statement, as described in “Configure ATM 1 and ATM 2 Physical Interface Properties” on page 125.

VCIs 0 through 31 are reserved for specific ATM values designated by the ATM Forum.

When you are configuring point-to-point connections, the MTU sizes on both sides of the connections must be the same.

Configure a Point-to-Multipoint ATM 1 or ATM 2 Connection

For ATM 1 and ATM 2 interfaces, you can configure a point-to-multipoint (NBMA) ATM connection by including the following statements at the `[edit interfaces interface-name unit logical-unit-number family inet address address multipoint-destination destination-address]` hierarchy level:

```plaintext
  [edit interfaces interface-name unit logical-unit-number family inet address address multipoint-destination destination-address]
  multipoint-destination destination-address {
    epd-threshold cells;
    inverse-arp;
    oam-liveness {
      up-count cells;
      down-count cells;
    }
    oam-period seconds;
    shaping {
      (cbr rate | rtvbr peak rate sustained rate burst length | vbr peak rate sustained rate burst length);
      queue-length number;
    }
    vci vpi-identifier.vci-identifier;
  }
```

address is the interface’s address. The address must include the destination prefix (for example, /24).

For each destination, include one `multipoint-destination statement`. destination-address is the address of the remote side of the connection, and vci-identifier and vpi-identifier are the VCI and optional VPI identifiers for the connection.

When you configure point-to-multipoint connections, all interfaces in the subnet must use the same MTU size.
Configure a Multicast-Capable ATM 1 or ATM 2 Connection

For ATM 1 and ATM 2 interfaces, you can configure a multicast-capable connection. By default, ATM connections assume unicast traffic. If your ATM switch performs multicast replication, you can configure the connection to support multicast traffic by including the `multicast-vci` statement at the `[edit interfaces interface-name unit logical-unit-number]` hierarchy level:

```
[edit interfaces interface-name unit logical-unit-number]
multicast-vci vpi-identifier vci-identifier;
```

`vci-identifier` and `vpi-identifier` are the VCI and VPI identifiers, which define the ATM VCI over which the switch is expecting to receive multicast packets for replication.

You can configure multicast support only on point-to-multipoint ATM connections.

Configure Inverse ATM 1 or ATM 2 ARP

For ATM 1 and ATM 2 interfaces, you can configure inverse ATM ARP, as described in RFC 2225. When inverse ATM ARP is enabled, the router responds to received Inverse ATM ARP requests by providing IP address information to the requesting ATM device.

The router does not initiate inverse ATM ARP requests.

By default, inverse ATM ARP is disabled. To configure a VC to respond to inverse ATM ARP requests, include the `inverse-arp` statement at the `[edit interfaces interface-name unit logical-unit-number]` or `[edit interfaces interface-name unit logical-unit-number family inet address address multipoint-destination destination]` hierarchy level:

```
inverse-arp;
```

You must configure ATM LLC-SNAP encapsulation on the logical interface to support inverse ARP. No other ATM encapsulation types are allowed. For more information, see “Configure ATM 1 and ATM 2 Interface Encapsulation” on page 146.

Define the ATM 1 and ATM 2 Traffic-Shaping Profile

When you use an ATM encapsulation on ATM 1 and ATM 2 interfaces, you can define bandwidth utilization, which consists of either a constant rate or a peak cell rate, with sustained cell rate and burst tolerance.

These values are used in the ATM generic cell-rate algorithm, which is a leaky bucket algorithm that defines the short-term burst rate for ATM cells, the maximum number of cells that can be included in a burst, and the long-term sustained ATM cell traffic rate.

If your router is equipped with an ATM 2 PIC, each VC can have its own independent shaping parameters. For more information, see “Define Virtual Path Tunnels on ATM 2 Interfaces” on page 134.

By default, the bandwidth utilization is unlimited; that is, unspecified bit rate (UBR) is used. Also, by default, buffer usage by VCs is unregulated.
To define limits to bandwidth utilization on a point-to-point interface, include the shaping statement at the [edit interfaces interface-name unit logical-unit-number] hierarchy level:

[edit interfaces interface-name unit logical-unit-number]  
  shaping {  
    (cbr rate | rtvbr peak rate sustained rate burst length |  
     vbr peak rate sustained rate burst length);  
    queue-length number;  
  }

The rtvbr statement is supported on ATM 2 PICs only. The queue-length statement is supported on ATM 1 PICs only.

For virtual circuits that are part of a point-to-multipoint interface, include the shaping statement at the [edit interfaces interface-name unit logical-unit-number family family address multipoint-destination destination-address] hierarchy level:

[edit interfaces interface-name unit logical-unit-number family family address multipoint-destination destination-address]  
  shaping {  
    (cbr rate | rtvbr peak rate sustained rate burst length |  
     vbr peak rate sustained rate burst length);  
    queue-length number;  
  }

The rtvbr statement is supported on ATM 2 PICs only. The queue-length statement is supported on ATM 1 PICs only.

To configure VP tunnels on ATM 2 interfaces, include the shaping statement at the [edit interfaces interface-name atm-options vpi vpi-identifier] hierarchy level:

[edit interfaces interface-name atm-options vpi vpi-identifier]  
  shaping {  
    (cbr rate | rtvbr peak rate sustained rate burst length |  
     vbr peak rate sustained rate burst length);  
    queue-length number;  
  }

When configuring ATM traffic shaping, you can do the following:

- Configure ATM 1 and ATM 2 CBR on page 139
- Configure ATM 1 and ATM 2 VBR on page 139
- Specify ATM 1 Shaping Values on page 140
- Specify ATM 2 Shaping Values on page 142
**Configure ATM 1 and ATM 2 CBR**

For traffic that does not require the ability to periodically burst to a higher rate, you can specify a constant bit rate (CBR).

To specify a constant bit rate on ATM 1 and ATM 2 interfaces, include the `cbr` statement at the [edit interfaces interface-name unit logical-unit-number shaping], [edit interfaces interface-name unit logical-unit-number family family address address multipoint-destination destination-address shaping], or [edit interfaces interface-name atm-options vpi vpi-identifier shaping] hierarchy level:

```plaintext
cbr rate;
```

**Configure ATM 2 Real-Time VBR**

By default, ATM interfaces use unspecified bit rate (UBR); that is, bandwidth utilization is unlimited. For ATM 2 interfaces only, you can configure real-time variable bit rate (RTVBR), which supports variable bit rate data traffic with average and peak traffic parameters. Compared to non-real-time VBR, RTVBR data is serviced at a higher priority with a relatively small sustainable cell rate (SCR) limit to minimize the delay. Real-time VBR is suitable for carrying packetized video and audio.

To configure RTVBR, include the `rtvbr` statement at the [edit interfaces interface-name unit logical-unit-number shaping], [edit interfaces interface-name unit logical-unit-number family family address address multipoint-destination destination-address shaping], or [edit interfaces interface-name atm-options vpi vpi-identifier shaping] hierarchy level:

```plaintext
rtvbr peak rate sustained rate burst length;
```

When configuring RTVBR, you can define the following shaping properties:

- **Peak rate**—Top rate at which traffic can burst.
- **Sustained rate**—Normal traffic rate averaged over time.
- **Burst length**—Maximum number of cells that a burst of traffic can contain. It can be a value from 1 through 4000 cells.

**Configure ATM 1 and ATM 2 VBR**

By default, ATM interfaces use unspecified bit rate (UBR); that is, bandwidth utilization is unlimited. For ATM 1 and ATM 2 interfaces, you can configure non-real-time VBR, which supports variable bit rate data traffic with average and peak traffic parameters. Compared to RTVBR, non-real-time VBR is scheduled with a lower priority and with a larger SCR limit, allowing it to recover bandwidth if it falls behind. Non-real-time VBR is suitable for packet data transfers.

To define variable bandwidth utilization (VBR) on ATM 1 and ATM 2 interfaces, include the `vbr` statement at the [edit interfaces interface-name unit logical-unit-number shaping], [edit interfaces interface-name unit logical-unit-number family family address address multipoint-destination destination-address shaping], or [edit interfaces interface-name atm-options vpi vpi-identifier shaping] hierarchy level:

```plaintext
vbr peak rate sustained rate burst length;
```
When configuring VBR, you can define the following shaping properties:

- **Peak rate**—Top rate at which traffic can burst.
- **Sustained rate**—Normal traffic rate averaged over time.
- **Burst length**—Maximum number of cells that a burst of traffic can contain. It can be a value from 1 through 4000 cells.

### Specify ATM 1 Shaping Values

For ATM 1 interfaces, you can specify the rates in bits per second (bps) or cells per second (cps). For OC-3c interfaces, the highest rate is 135,631,698 bps (353,207.55 cps), which corresponds to 100 percent of the available line rate. For OC-12c interfaces, the highest rate is 271,263,396 bps (706,415.09 cps), which corresponds to 50 percent of the available line rate. Table 13 lists some of the other rates you can specify. If you specify a rate that is not listed, it is rounded to the nearest rate.

The exact number of values differs between OC-12c and OC-3c interfaces. OC-12c interfaces have about four times as many value increments as OC-3c interfaces. For OC-12c rates between 1/2 and 1/128 of the line rate, there are 128 steps between each 1/n value. For rates smaller than 1/128, there are (16,384 minus 128) or 16,256 values. The reason for this is that fractional shaping is ignored at rates below 1/128. This results in about 32,384 distinct rates for OC-12c. For OC-3c, the starting point is full line rate, the fraction/integer breakpoint is about 1/32, and there is a maximum of 4096 scheduler slots, producing about 8032 distinct values.

For ATM 1 interfaces, the actual packet rate on the interface is calculated with the following formula:

\[
\text{actual-rate} = \frac{(128 \times \text{line-rate})}{\text{trunc} \left(\frac{(128 \times \text{line-rate})}{\text{desired-rate}}\right)}
\]

\(\text{line-rate}\) is the maximum available rate on the interface (in bits per second) after factoring out the overhead for SONET and ATM (per-cell) overheads. For OC-3c interfaces, the line rate is calculated as follows:

\[
\text{line-rate} = 155,520,000 \text{ bps} \times \left(\frac{26}{27}\right) \times \left(\frac{48}{53}\right) = 135,631,698.1 \text{ bps}
\]

For OC-12c interfaces, the line rate is calculated as follows:

\[
\text{line-rate} = 622,080,000 \text{ bps} \times \left(\frac{26}{27}\right) \times \left(\frac{48}{53}\right) = 542,526,792.45 \text{ bps}
\]

\(\text{desired-rate}\) is the rate you enter in the vbr statement, in bits per second.

The \text{trunc} operator indicates that all digits to the right of the decimal point should be dropped.

Buffers are shared among all VCs, and by default, there is no limit to the buffer size for a VC. If a VC is particularly slow, it might use all the buffer resources.

Table 13 shows ATM 1 traffic-shaping rates.
Table 13: ATM 1 Traffic-Shaping Rates

<table>
<thead>
<tr>
<th>Interface Type</th>
<th>Line Rate (bps)</th>
<th>Line Rate (cps)</th>
<th>Percentage of Total Line Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>OC-3</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>135,600,000</td>
<td>353,125</td>
<td>100.00</td>
<td></td>
</tr>
<tr>
<td>134,542,320</td>
<td>350,370.66</td>
<td>99.22</td>
<td></td>
</tr>
<tr>
<td>133,511,760</td>
<td>347,686.88</td>
<td>98.46</td>
<td></td>
</tr>
<tr>
<td>132,494,760</td>
<td>345,038.44</td>
<td>97.71</td>
<td></td>
</tr>
<tr>
<td>131,491,320</td>
<td>342,425.31</td>
<td>96.97</td>
<td></td>
</tr>
<tr>
<td>130,501,440</td>
<td>339,847.5</td>
<td>96.24</td>
<td></td>
</tr>
<tr>
<td>129,525,120</td>
<td>337,305</td>
<td>95.52</td>
<td></td>
</tr>
<tr>
<td>128,562,360</td>
<td>334,797.81</td>
<td>94.81</td>
<td></td>
</tr>
<tr>
<td>127,626,720</td>
<td>332,361.25</td>
<td>94.12</td>
<td></td>
</tr>
<tr>
<td>126,691,080</td>
<td>329,924.69</td>
<td>93.43</td>
<td></td>
</tr>
<tr>
<td>OC-12</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>271,263,396</td>
<td>706,415.09</td>
<td>50.00</td>
<td></td>
</tr>
<tr>
<td>270,207,897</td>
<td>703,666.40</td>
<td>49.81</td>
<td></td>
</tr>
<tr>
<td>269,160,579</td>
<td>700,939.01</td>
<td>49.61</td>
<td></td>
</tr>
<tr>
<td>268,121,349</td>
<td>698,232.68</td>
<td>49.42</td>
<td></td>
</tr>
<tr>
<td>267,090,113</td>
<td>695,547.17</td>
<td>49.23</td>
<td></td>
</tr>
<tr>
<td>266,066,779</td>
<td>692,882.24</td>
<td>49.04</td>
<td></td>
</tr>
<tr>
<td>265,051,257</td>
<td>690,237.65</td>
<td>48.85</td>
<td></td>
</tr>
<tr>
<td>264,043,458</td>
<td>687,613.17</td>
<td>48.67</td>
<td></td>
</tr>
<tr>
<td>263,043,293</td>
<td>685,008.58</td>
<td>48.48</td>
<td></td>
</tr>
<tr>
<td>262,050,677</td>
<td>682,423.64</td>
<td>48.30</td>
<td></td>
</tr>
</tbody>
</table>

Example: Specify ATM 1 Shaping Values

Determine the actual rate in ATM 1 interfaces when the desired rate is 80 percent of the maximum rate:

OC-3c:
135,600,000 bps * 0.8 = 108,480,000 bps
actual-rate = (128 * 135,600,000.1) / (trunc ((128 * 135,600,000.1) / 108,480,000))
actual-rate = 17,356,800,013 / (trunc (17,356,800,013 / 108,480,000))
actual-rate = 17,356,800,013 / 160
actual-rate = 108,480,000 bps

OC-12c:
271,263,396 bps * 0.8 = 217,010,716.8 bps
actual-rate = (128 * 542,526,792.45) / (trunc ((128 * 542,526,792.45) / 217,010,716.8))
actual-rate = 69,443,429,434 / (trunc (69,443,429,434 / 217,010,716.8))
actual-rate = 69,443,429,434 / 320
actual-rate = 217,010,717 bps
**Specify ATM 2 Shaping Values**

For ATM 2 OC-3c interfaces, the maximum available rate is 100 percent of line rate, or 135,600,000 bps. For ATM 2 OC-12c interfaces, the maximum available rate is 100 percent of line rate, or 542,546,792 bps. You can specify the rates in bits per second (bps) or cells per second (cps). Fractional shaping is accurate within 0.5 percent of the desired rate.

**Configure the ATM 1 Queue Length**

ATM 1 PICs contain a transmit buffer pool of 16,382 buffers, which are shared by all the permanent virtual circuits (PVCs) that you configure on the PIC. Even multiple-port ATM PICs have a single buffer pool shared by all the ports.

By default, the ATM 1 PIC allows PVCs to consume all the buffers they require. If the sustained traffic rate for a PVC exceeds its shaped rate, buffers are consumed. Eventually, all buffers on the PIC are consumed, and the other PVCs are starved. This results in head-of-line blocking.

For each PVC, you prevent this situation by configuring the queue length of the PVC. The queue length is a limit on the number of transmit packets that can be queued. Packets that exceed the limit are dropped.

To limit the queue size of a PVC, include the queue-length statement at the [edit interfaces interface-name unit logical-unit-number shaping] or [edit interfaces interface-name unit logical-unit-number family family address address multipoint-destination destination-address shaping] hierarchy level:

```plaintext
    queue-length number;
```

The length can range from 1 through 16,383 packets. The default is 16,383 packets. You should include the queue-length statement in the configuration of all the PVCs that you configure on an ATM 1 PIC. The queue-length statement performs two functions:

- It prevents head-of-line blocking because it limits the number of packets and therefore buffers that can be consumed by each configured PVC.
- It sets the maximum lifetime that can be sustained by packets over the PVC when traffic has oversubscribed the configured shaping contract.

The total value of all the queue lengths must not exceed the total number of packets that can be held in the buffer space available on the PIC. The total number of packets the buffers can hold depends on the size of the physical interface MTU, including all encapsulation overhead. You can use the following formula to calculate the total number of packets the buffer space can hold:

```plaintext
    16,382 / ( Round Up ( MTU / 480 ) )
```

For example, assuming default MTU settings for all ATM 1 interfaces on a PIC, the total number of packets that can be held is:

```plaintext
    16,382 / ( Round Up ( 4,482 / 480 ) ) = 1,638 packets
```

Thus, you can configure up to 1,638 for the combined queue length of all the PVCs on an ATM 1 PIC that uses default MTU settings for all interfaces.

If you set a queue length to a very low value, small bursts in packets transiting the PVC might not be buffered.
The maximum lifetime that packets can sustain while transiting a PVC depends on the shaping rate you configure for the PVC, the setting for the queue-length statement, and the physical interface MTU. You can use the following formula to calculate the maximum lifetime that packets can sustain while transiting a PVC:

\[
\text{Maximum Lifetime} = \frac{\text{PVC queue-length in packets} \times \text{MTU}}{\left( \frac{\text{PVC shaping in bits per second}}{8} \right)}
\]

For example, if you configure a PVC on an ATM 1 interface with the default MTU, a CBR shaping rate of 3,840,000 bps (10,000 cells per second), and a queue length of 25 packets. The maximum lifetime is:

\[
\frac{25 \times 4,482}{3,840,000 / 8} = 233 \text{ ms}
\]

This is the worst-case lifetime assuming all packets in the queue are MTU sized, and the traffic using the PVC is oversubscribing its configured shaping contract.

In general, we recommend that you use a maximum lifetime under 500 ms.

**Configure the ATM 2 EPD Threshold**

By default, the ATM 2 PIC allows PVCs to consume all the buffers they require. If the sustained traffic rate for a PVC exceeds its shaped rate, buffers are consumed. Eventually, all buffers on the PIC are consumed, and the other PVCs are starved. This results in head-of-line blocking.

For each PVC, you prevent this situation by configuring the early packet discard (EPD) threshold of the PVC. The EPD threshold is a limit on the number of transmit packets that can be queued. Packets that exceed the limit are discarded.

To set the EPD threshold of a PVC, include the `epd-threshold` statement at the `[edit interfaces interface-name unit logical-unit-number]` or `[edit interfaces interface-name unit logical-unit-number family family address address multipoint-destination destination-address]` hierarchy level:

```
epd-threshold cells;
```

For one-port and two-port OC-12 interfaces, the allowable range is 1 through 425,984 cells. For two-port OC-3 interfaces, the allowable range is 1 through 212,992 cells.

You should include the `epd-threshold` statement in the configuration of all the PVCs that you configure on an ATM 2 PIC. The `epd-threshold` statement performs two functions:

- It prevents head-of-line blocking because it limits the number of packets and therefore buffers that can be consumed by each configured PVC.
- It sets the maximum lifetime that can be sustained by packets over the PVC when traffic has oversubscribed the configured shaping contract.
Example: Configure the ATM 2 EPD Threshold

Configure the EPD threshold for a point-to-point ATM 2 interface and a point-to-multipoint ATM 2 interface.

On a point-to-point ATM 2 interface

```
[edit interfaces at-1/0/0]
unit 0 {
  vci 0.123;
  epd-threshold 1300;
  ...
}
```

On a point-to-multipoint ATM 2 interface

```
[edit interfaces at-1/0/1]
unit 0 {
  multipoint;
  family inet address 12.12.12.24 {
    multipoint-destination 12.12.12.14 vci 0.123 epd-threshold 1300;
    ...
  }
}
```

Configure the ATM 2 Transmission Weight

For ATM 2 interfaces configured with VPI shaping, you can control the number of cells a VCI can send each time the VCI has a turn to transmit by including the `transmit-weight` statement at the `[edit interfaces interface-name unit logical-unit-number]` hierarchy level:

```
transmit-weight cells;
```

The number of cells can range from 1 through 32,000. For a configuration example, see “Examples: Configure ATM 2 Interfaces” on page 161.

Define the ATM 1 and ATM 2 OAM F5 Loopback Cell Period

For ATM 1 and ATM 2 interfaces with an ATM encapsulation, you can configure the OAM F5 loopback cell period on virtual circuits. This is the interval at which OAM F5 loopback cells are transmitted.

By default, no OAM F5 loopback cells are sent. To send OAM F5 loopback cells on a point-to-point interface, include the `oam-period` statement at the `[edit interfaces interface-name unit logical-unit-number]` hierarchy level:

```
[edit interfaces interface-name unit logical-unit-number]
oam-period (disable | seconds);
```

To send OAM F5 loopback cells on a virtual circuit that is part of a point-to-multipoint interface, include the `oam-period` statement at the `[edit interfaces interface-name unit logical-unit-number family family-address address multipoint-destination destination-address]` hierarchy level:

```
[edit interfaces interface-name unit logical-unit-number family family-address address multipoint-destination destination-address]
oam-period (disable | seconds);
```
Configure ATM 1 and ATM 2 Logical Interface Properties

The period can range from 1 through 900 seconds. You can also choose the disable option to disable the OAM loopback cell transmit feature.

OAM VC-AIS (alarm indication signal) and VC-RDI (remote defect indication) defect indication cells are used for identifying and reporting VC defects end-to-end. When a physical link or interface failure occurs, intermediate nodes insert OAM AIS cells into all the downstream VCs affected by the failure. Upon receiving an AIS cell on a VC, the router marks the logical interface down and sends an RDI cell on the same VC to notify the remote end of the error status. When an RDI cell is received on a VC, the router sets the logical interface status to down. When no AIS or RDI cells are received for 3 seconds, the router sets the logical interface status to up. You do not need to configure anything to enable defect indication.

Configure the ATM 1 and ATM 2 OAM F5 Loopback Cell Threshold

For ATM 1 and ATM 2 interfaces with an ATM encapsulation, you can configure the OAM F5 loopback cell threshold on VCs. This is the minimum number of consecutive OAM F5 loopback cells received before a VC is declared up, or the minimum number of consecutive OAM F5 loopback cells lost before a VC is declared down.

By default, when five consecutive OAM F5 loopback cells are received, the VC is considered to be up, and when five consecutive cells are lost, the VC is considered to be down. To modify these values on a point-to-point interface, include the oam-liveness statement at the [edit interfaces interface-name unit logical-unit-number] hierarchy level:

```
[edit interfaces interface-name unit logical-unit-number]
oam-liveness {
    up-count cells;
    down-count cells;
}
```

To modify the OAM F5 loopback cell count threshold on a virtual circuit that is part of a point-to-multipoint interface, include the oam-liveness statement at the [edit interfaces interface-name unit logical-unit-number family family address address multipoint-destination destination-address] hierarchy level:

```
[edit interfaces interface-name unit logical-unit-number family family address address multipoint-destination destination-address]
oam-liveness {
    up-count cells;
    down-count cells;
}
```

The cell count can be a value from 1 through 255.
Configure ATM 1 and ATM 2 Interface Encapsulation

To configure ATM encapsulation on a physical interface, include the encapsulation statement at the [edit interfaces interface-name] hierarchy level:

```
[edit interfaces interface-name]
encapsulation (atm-ccc-cell-relay | atm-pvc | ethernet-over-atm);
```

For ATM interfaces, the physical interface encapsulation can be one of the following:

- **ATM cell-relay**—This encapsulation connects two remote virtual circuits or ATM physical interfaces with a label-switched path (LSP). Traffic on the circuit is ATM cells.
- **ATM PVC**—ATM permanent virtual circuit (PVC) encapsulation is defined in RFC 1483, Multiprotocol Encapsulation over ATM Adaptation Layer 5.
- **Ethernet over ATM**—This encapsulation type allows ATM interfaces to connect to devices that support only bridged-mode protocol data units (PDUs).

Generally, you configure an interface’s encapsulation at the [edit interfaces interface-name] hierarchy level. However, for ATM encapsulations, you can also configure the encapsulation type that is used inside the ATM cell itself. To do this, include the encapsulation statement at the [edit interfaces interface-name unit logical-unit-number] hierarchy level:

```
[edit interfaces interface-name unit logical-unit-number]
```

The ATM encapsulations are defined in RFC 1483, Multiprotocol Encapsulation over ATM Adaptation Layer 5.

For ATM interfaces, the logical interface encapsulation can be one of the following:

- **ATM CCC VC multiplex**—Use ATM VC multiplex encapsulation on circuit cross-connect (CCC) circuits. When you use this encapsulation type, you can configure the family ccc_only.
- **ATM NLPID**—Use ATM NLPID encapsulation. When you use this encapsulation type, you can configure the family inet only.
- **ATM SNAP**—You can configure ATM SNAP encapsulation.
- **ATM SNAP encapsulation on translational cross-connect (TCC) circuits**—You can configure ATM SNAP encapsulation on TCC circuits.
- **ATM VC multiplex on TCC circuits**—You can configure ATM VC multiplex encapsulation on TCC circuits. When you use this encapsulation type, you can configure the family tcc only.
- **ATM VC multiplex**—When you use this encapsulation type, you can configure the family inet only.
- **Cisco ATM NLPID**—Use Cisco ATM NLPID encapsulation. When you use this encapsulation type, you can configure the family inet only.
- Ethernet VPLS over ATM—This encapsulation type enables a VPLS instance to support bridging between Ethernet interfaces and ATM interfaces, as described in RFC 2684, Multiprotocol Encapsulation over ATM Adaptation Layer 5. This encapsulation type is used only on ATM 2 interfaces. When you use this encapsulation type, you cannot configure multipoint interfaces.

- Multilink PPP over AAL5 logical link control (LLC)—For ATM 2 interface, you can configure Multilink PPP over AAL5 LLC. This encapsulation type is used only on ATM 2 interfaces. For this encapsulation type, your router must be equipped with a Link Services PIC.

- PPP over ATM adaptation layer 5 (AAL5) logical link control (LLC)—For ATM 2 interfaces, you can configure PPP over AAL5 LLC encapsulation.

- PPP over ATM adaptation layer 5 (AAL5) multiplex—For ATM 2 interfaces, you can configure PPP over AAL5 multiplex encapsulation.

- Cell-relay accumulation mode—For ATM 1 interfaces, you can configure cell-relay accumulation mode (CAM). In this mode, the incoming 1 to 8 cells are packaged into a single packet and forwarded to the label-switched path (LSP). You configure CAM as follows:

```plaintext
[edit chassis]
fpc 1 {
  pic 0 {
    atm-cell-relay-accumulation;
  }
}
```

CAM is not supported on ATM 2 interfaces. For more information about CAM, see the JUNOS Internet Software Configuration Guide: Getting Started.

With the atm-nlpid, atm-cisco-nlpid, and atm-vc-mux encapsulations, you can configure the family inet only. With the circuit cross-connect (CCC) circuit encapsulations, you can configure the family ccc only. With the translational cross-connect (TCC) circuit encapsulations, you can configure the family tcc only. With the ether-over-atm-llc, ether-vpls-atm-llc, atm-ppp-llc, atm-ppp-vc-mux encapsulation types, you cannot configure point-to-multipoint interfaces.
Configure an ATM 1 Cell-Relay Circuit

For ATM 1 interfaces, you can create an ATM cell-relay circuit by configuring an entire ATM physical device or an individual virtual circuit (VC). When you configure an entire device, only cell-relay encapsulation is allowed on the logical interfaces; for ATM 1 PICs, you use the atm-options statement to control the number and location of VCs. Allowed VCs on both ingress and egress ATM interfaces should be the same. For most interfaces, you can define a maximum of 4090 VCs per interface. The highest-numbered VC value you can configure is 4089. For ATM OC-3 interfaces, you can define a maximum of 8180 VCs per interface. For ATM OC-12 interfaces, you can define a maximum of 16,360 VCs per interface. Promiscuous mode removes these limits. For more information, see “Configure ATM 1 and ATM 2 Cell-Relay Promiscuous Mode” on page 127.

For ATM 1 interfaces, if you are dedicating the entire device to a cell-relay circuit, include the allow-any-vci statement at the [edit interfaces unit 0] hierarchy level:

```
[edit interfaces interface-name unit 0] {
  allow-any-vci;
}
```

Once you include this statement, you cannot configure other logical interfaces in the same physical interface.

When you use ATM CCC cell-relay encapsulation, you must configure both the physical and logical encapsulation with atm-ccc-cell-relay. You cannot mix different logical encapsulation types on an interface that you have configured with ATM CCC cell-relay physical encapsulation.

Examples: Configure an ATM 1 Cell-Relay Circuit

```
[edit interfaces at-1/2/0]
encapsulation atm-ccc-cell-relay;
atm-options {
  pic-type atm1;
  vpi 0 maximum-vcs 256;
}
unit 0 {
  point-to-point;
  encapsulation atm-ccc-cell-relay;
  allow-any-vci;
}
```

```
[edit interfaces at-1/1/0]
encapsulation atm-ccc-cell-relay;
atm-options {
  pic-type atm1;
  vpi 0 maximum-vcs 256;
}
unit 120 {
  encapsulation atm-ccc-cell-relay;
  vci 0.120;
}
```
Configure non-promiscuous port mode

```
[edit interfaces at-0/0/1]
encapsulation atm-ccc-cell-relay;
atm-options {
  pic-type atm1;
  vpi 0 {
    maximum-vcs 100;
  }
  vpi 1 {
    maximum-vcs 300;
  }
  vpi 4 {
    maximum-vcs 200;
  }
}
unit 0 {
  encapsulation atm-ccc-cell-relay;
  allow-any-vci;
}
```

Configure non-promiscuous VPI mode

```
[edit interfaces at-0/0/1]
encapsulation atm-ccc-cell-relay;
atm-options {
  pic-type atm1;
  vpi 0 {
    maximum-vcs 100;
  }
}
unit 0 {
  encapsulation atm-ccc-cell-relay;
  vpi 0;
}
```

Configure non-promiscuous VCI mode

```
[edit interfaces at-0/0/1]
encapsulation atm-ccc-cell-relay;
atm-options {
  pic-type atm1;
  vpi 0 {
    maximum-vcs 100;
  }
}
unit 0 {
  encapsulation atm-ccc-cell-relay;
  vci 0.50
}
```
Configure PPP over ATM 2 Encapsulation

For ATM 2 interfaces, you can configure PPP over ATM adaptation layer 5 (AAL5) encapsulation, as described in RFC 2364. PPP over ATM encapsulation associates a PPP link with an ATM AAL5 PVC.

The JUNOS software supports three PPP over ATM encapsulation types:

- **atm-ppp-llc**—PPP over ATM adaptation layer 5 (AAL5) logical link control (LLC).
- **atm-ppp-vc-mux**—PPP over ATM AAL5 multiplex.
- **atm-mlppp-llc**—Multilink PPP over ATM AAL5 LLC. For this encapsulation type, your router must be equipped with a Link Services PIC.

To enable PPP over ATM encapsulation, include the `encapsulation` statement at the `/edit interfaces interface-name unit logical-unit-number` hierarchy level, specifying the `atm-mlppp-llc`, `atm-ppp-llc`, or `atm-ppp-vc-mux` encapsulation type:

```
[edit interfaces interface-name unit logical-unit-number]
encapsulation (atm-mlppp-llc | atm-ppp-llc | atm-ppp-vc-mux);
```

When you configure PPP over ATM encapsulation, you can enable PPP Challenge Handshake Authentication Protocol (CHAP) and keepalives on the logical interface. For more information about PPP CHAP and keepalives, see “Configure PPP Challenge Handshake Authentication Protocol” on page 55 and “Configure Keepalives” on page 58.

**Note**

When you use PPP over ATM encapsulation, we recommend that you not include the `oam-period` statement in the configuration. Instead, we recommend that you enable keepalives to detect connection failures.

Example: Configure PPP over ATM 2 Encapsulation

Configure three logical interfaces with PPP over ATM encapsulation:

```
[edit interfaces]
at-0/1/0 {
  atm-options {
    pic-type atm2;
    vpi 0;
    vpi 2;
  }
  unit 0 {
    encapsulation atm-ppp-llc;
    ppp-options {
      chap {
        access-profile pe-B-ppp-clients;
        local-name "pe-A-at-0/1/0";
      }
    }
    keepalives interval 5 up-count 6 down-count 4;
    vci 0.120;
    family inet address 192.122.13.13/30;
  }
}
```
Configure ATM 1 and ATM 2 Interface Encapsulation

unit 1 {
  encapsulation atm-ppp-vc-mux;
  vci 2.120;
  keepalives interval 6 up-count 6 down-count 4;
  family inet address 192.122.14.13/30;
}
unit 2 {
  encapsulation atm-ppp-vc-mux;
  ppp-options {
    chap {
      passive;
      access-profile pe-A-ppp-clients;
      local-name "pe-A-at-0/1/0";
    }
  }
  keepalives interval 5 up-count 6 down-count 4;
  vci 2.121;
  family inet address 192.122.15.13/30;
}

Configure Multilink PPP over ATM 2 encapsulation

[edit interfaces]
at-0/0/0 {
  atm-options {
    pic-type atm2;
    vpi 10;
  }
  unit 0 {
    encapsulation atm-mlppp-llc;
    ppp-options {
      chap {
        access-profile pe-B-ppp-clients;
        local-name "pe-A-at-0/0/0";
      }
    }
    keepalive interval 5 up-count 6 down-count 4;
    vci 10.120;
    family mlppp {
      bundle ls-0/3/0.0;
    }
  }
}

at-0/0/1 {
    atm-options {
        pic-type atm2;
        vpi 11;
    }
    unit 1 {
        encapsulation atm-mlppp-llc;
        ppp-options {
            chap {
                access-profile pe-B-ppp-clients;
                local-name "pe-A-at-0/0/0";
            }
        }
        keepalive interval 5 up-count 6 down-count 4;
        vci 11.120;
        family mlppp {
            bundle ls-0/3/0.0;
        }
    }
}

at-1/2/3 {
    atm-options {
        pic-type atm2;
        vpi 12;
    }
    unit 2 {
        encapsulation atm-mlppp-llc;
        ppp-options {
            chap {
                access-profile pe-B-ppp-clients;
                local-name "pe-A-at-0/0/0";
            }
        }
        keepalive interval 5 up-count 6 down-count 4;
        vci 12.120;
        family mlppp {
            bundle ls-0/3/0.0;
        }
    }
}

...
ls-0/3/0 {
    encapsulation multilink-ppp;
    interleave-fragments;
    keepalive;
    unit 0 {
        mrru 4500;
        short-sequence;
        fragment-threshold 16320;
        drop-timeout 2000;
        encapsulation multilink-ppp;
        interleave-fragments;
        minimum-links 8;
        family inet {
            address 10.10.0.1/32 {
                destination 10.10.0.2;
            }
        }
        family iso;
        family inet6 {
            address 8090::0:1/128 {
                destination 8090::0:2;
            }
        }
    }
}
...

Configure E3 and T3 Parameters on ATM 1 Interfaces

For ATM 1 interfaces, you can configure ATM E3 and T3 interfaces by including the following statements at the [edit interfaces at-fpc/pic/port] hierarchy level:

[edit interfaces at-fpc/pic/port]
e3-options {
    atm-encapsulation (plcp | direct);
    buildout feet;
    framing (g.751 | g.832);
    loopback (local | remote);
    (payload-scrambler | no-payload-scrambler);
}
t3-options {
    atm-encapsulation (plcp | direct);
    buildout feet;
    (cbit-parity | no-cbit-parity);
    loopback (local | remote);
    (payload-scrambler | no-payload-scrambler);
}
Some of the options and default values vary from those described in the E3 and T3 interface sections:

- **atm-encapsulation**—PLCP is the default value. The E3 line-format option g.832 supports direct ATM-encapsulation only.

- **buildout**—The default value is 10 feet. Distance can be any integer value. The range is 0 through 450 feet.

- **cbit-parity**—The default option is to enable cbit parity.

- **framing**—There is no default option for E3 interfaces; T3 interfaces use the cbit-parity statement in place of framing.

- **loopback**—The default value is no loopback.

- **payload-scrambler**—The default option is to enable payload scrambling.

In addition, the ATM E3 and T3 PICs support the clocking statement at the interface level, as do the SONET PICs. For more information about E3- and T3-specific parameters, see “Configure E3 Interfaces” on page 251 and “Configure T3 Interfaces” on page 395.

---

**Note**

You must configure all the ports on an ATM E3 or T3 PIC with the same framing and encapsulation. Otherwise, the system will set all the ports on the PIC to the slowest framing and encapsulating configuration. For ATM T3, this is PLCP and for ATM E3, this is G.751 PLCP.

---

**Configure SONET/SDH Parameters on ATM 1 and ATM 2 Interfaces**

When configuring ATM 1 and ATM 2 SONET/SDH interfaces, you can also include the following statements in the `sonet-options` statement to set SONET/SDH parameters on ATM interfaces:

```plaintext
[edit interfaces at-fpc/pic/port]
sonet-options {
    aps {
        advertise-interval milliseconds;
        authentication-key key;
        force;
        hold-time milliseconds;
        lockout;
        neighbor address;
        paired-group group-name;
        protect-circuit group-name;
        request;
        revert-time seconds;
        working-circuit group-name;
    }
}
```
Configure ATM 1 and ATM 2 Interfaces

Configure ATM 2 VC Tunnel CoS Components

The ATM 2 interface allows multiple IP queues into each VC. A VC tunnel can support four class-of-service (CoS) queues. Within a VC tunnel, the weighted round robin (WRR) algorithm schedules the cell transmission of each queue. You can configure the queue admission policies, such as EPD or weighted random early detection (WRED), to control the queue size during congestion.

For information about CoS components that apply generally to all interfaces, see “CoS Overview” on page 575 and “CoS Configuration Guidelines” on page 585.

To configure ATM 2 VC tunnel CoS components, include the following statements at the [edit interfaces at-fpc/pic/port] hierarchy level:

```
[edit interfaces at-fpc/pic/port]
atm-options {
  linear-red-profiles profile-name {
    high-plp-max-threshold percent;
    low-plp-max-threshold percent;
    queue-depth cells high-plp-threshold percent low-plp-threshold percent;
  }
  scheduler-maps map-name {
    forwarding-class class-name {
      priority (low | high);
      transmit-weight (cells number | percent number);
      (epd-threshold cells | linear-red-profile profile-name);
    }
    vc-cos-mode (alternate | strict);
  }
}
unit logical-unit-number {
  atm-scheduler-map (map-name | default);
}
```
Linear random early discard (RED) profiles define CoS virtual circuit drop profiles. You can configure up to 32 linear RED profiles per port. When a packet arrives, RED checks the queue fill level. If the fill level corresponds to a nonzero drop probability, the RED algorithm determines whether to drop the arriving packet. You can define the following options for each RED profile:

- **Queue depth**—Define maximum queue depth in the CoS VC drop profile. Packets are always dropped beyond the defined maximum. The range you can configure is 1 through 64,000 cells.

- **High packet-loss priority (PLP) threshold**—Define CoS VC drop profile fill-level percentage when linear RED is applied to cells with high PLP. When the fill level exceeds the defined percentage, packets with high PLP are randomly dropped by RED.

- **Low PLP threshold**—Define CoS VC drop profile fill-level percentage when linear RED is applied to cells with low PLP. When the fill level exceeds the defined percentage, packets with low PLP are randomly dropped by RED.

- **High packet-loss priority (PLP) maximum threshold**—Define the drop profile fill-level for the high PLP CoS VC. When the fill level exceeds the defined percentage, all packets with high PLP are dropped.

- **Low PLP maximum threshold**—Define the drop profile fill-level for the low PLP CoS VC. When the fill level exceeds the defined percentage, all packets with low PLP are dropped.

To define a scheduler map, you associate it with a forwarding class. Forwarding classes can be best-effort, expedited-forwarding, assured-forwarding, or network-control, which are associated with the following four queues:

- **Queue 0**—best-effort
- **Queue 1**—expedited-forwarding
- **Queue 2**—assured-forwarding
- **Queue 3**—network-control

In ATM 2 PICs, the cell loss priority (CLP) bit is mapped to the PLP bit at ingress; at egress, the PLP bit is mapped to the CLP bit. You can set PLP by configuring a classifier or policer.
The JUNOS software creates these CoS queues for a VC when you include the `atm-scheduler-map` statement in the configuration. The JUNOS software prefixes each packet delivered to the VC with the next-hop rewrite data associated with each queue. You can define the following options for each forwarding class:

- **Priority**—Configure high or low queueing priority.

- **Transmit weight**—Configure the transmission weight in number of cells or percentage. Each CoS queue is serviced in WRR mode. When CoS queues have data to send, they send the number of cells equal to their weight before passing control to the next active CoS queue. This allows proportional bandwidth sharing between multiple CoS queues within a rate-shaped VC tunnel. A CoS queue can send from 1 through 32,000 cells or from 5 through 100 percent of queued traffic before passing control to the next active CoS queue within a VC tunnel.

The AAL5 protocol prohibits cells from being interleaved on a VC; therefore, a complete packet is always sent. If a CoS queue sends more cells than its assigned weight because of the packet boundary, the deficit is carried over to the next time the queue is scheduled to transmit. If the queue is empty after the cells are sent, the deficit is waived, and the queue’s assigned weight is reset.

- **EPD threshold or linear RED profile**—Define an EPD threshold or associate the forwarding class with a linear RED profile.

If the scheduler parameters of the forwarding class are not configured, the following defaults are used:

- **Priority**—High for queue 0, low for the remaining queues.

- **Transmit weight**—95 percent for queue 0, 5 percent for queue 3.

- **EPD threshold**—The EPD threshold is determined by the JUNOS software based on the available bandwidth.

For more information about forwarding classes, see “CoS Configuration Guidelines” on page 585.

VC CoS mode defines the CoS queue scheduling priority. Two modes of CoS scheduling priority are supported:

- **Alternate**—Assign high priority to one queue. The scheduling of the queues alternates between the high-priority queue and the remaining queues. Every other scheduled packet is from the high-priority queue.

- **Strict**—Assign strictly high priority to one queue. A queue with strictly high priority is always scheduled before the remaining queues. The remaining queues are scheduled in round-robin fashion.

By default, the VC CoS mode is alternate. When it is a queue’s turn to transmit, the queue transmits up to its weight in cells as specified by the `transmit-weight` statement. The number of cells transmitted can be slightly over the configured or default transmit weight, because the transmission always ends at a packet boundary.
Example: Configure ATM 2 VC Tunnel CoS Components

Configure ATM 2 VC tunnel CoS components:

```conf
ten interfaces
  at-1/2/0 {
    atm-options {
      vpi 0;
      linear-red-profiles red-profile-1 {
        queue-depth 35000 high-plp-threshold 75 low-plp-threshold 25;
      }
      scheduler-maps map1 {
        vc-cos-mode strict;
        forwarding-class best-effort {
          priority low;
          transmit-weight percent 25;
          linear-red-profile red-profile-1;
        }
      }
    }
    unit 0 {
      vci 0.128;
      shaping {
        vbr peak 20m sustained 10m burst 20;
      }
      atm-scheduler-map map-1;
      family inet {
        address 192.1.0.100/32 {
          destination 192.1.0.101;
        }
      }
    }
  }
```

Examples: Configure ATM 1 Interfaces

The following configuration is sufficient to get an ATM 1 OC-3 or OC-12 interface up and running. By default, ATM interfaces use ATM PVC encapsulation.

```conf
ten interfaces
  set interfaces at-fpc/ pic/ port atm-options vpi vpi-identifier
  maximum-vcs vcs-value
  set interfaces at-fpc/ pic/ port unit 0 vci vci-identifier
  set interfaces at-fpc/ pic/ port unit 0 family inet address local-address
  destination remote-address
  set interfaces at-fpc/ pic/ port unit 1 ...
  show
```

---

Example: Configure ATM 1 Interfaces

[49x768]JUNOS 6.0 Internet Software Configuration Guide: Interfaces and Class of Services

[158]
interfaces {
  at-fpc/pic/port {
    atm-options {
      vpi vpi-identifier maximum-vcs maximum-vcs value;
      unit 0 {
        vci vpi-identifier.vci-identifier;
        family inet {
          address local-address {
            destination destination-address;
          }
        }
      }
    }
    unit 1 {
      # second VC
      ...
    }
  }
}

Following is a more complex configuration example

interfaces {
  at-0/0/0 {
    encapsulation atm-pvc;
    atm-options {
      vpi 0 maximum-vcs 1200;
    }
    unit 2 {
      encapsulation atm-snap;
      inverse-arp;
      vci 0.80;
      family inet {
        mtu 1500;
        address 192.1.0.3/32 {
          destination 192.1.0.1;
        }
      }
    }
    unit 3 {
      encapsulation atm-snap;
      vci 0.32;
      oam-period 60;
      family inet {
        mtu 1500;
        address 193.123.4.3/32 {
          destination 193.123.4.2;
        }
      }
    }
  }
}
at-0/2/0 {
    encapsulation atm-pvc;
    atm-options {
        vpi 0 maximum-vcs 1200;
    }
    unit 2 {
        encapsulation atm-snap;
        inverse-arp;
        vci 0.82;
        family inet {
            mtu 1500;
            address 192.234.5.3/32 {
                destination 192.234.5.2;
            }
        }
    }
}
at-0/3/0 {
    encapsulation atm-pvc;
    atm-options {
        vpi 0 maximum-vcs 1200;
    }
    unit 140 {
        encapsulation atm-snap;
        multipoint;
        family inet {
            address 194.236.7.4/24 {
                multipoint-destination 194.236.7.5;
                vci 0.100;
                inverse-arp;
            }
        }
    }
}
at-7/3/0 {
    encapsulation atm-pvc;
    atm-options {
        vpi 0 maximum-vcs 1200;
    }
    unit 0 {
        encapsulation atm-snap;
        vci 0.32;
        family inet {
            address 192.168.12.3/32 {
                destination 192.168.12.2;
            }
        }
    }
}
Examples: Configure ATM 2 Interfaces

Configure VP tunnel-shaping and OAM F4 on an ATM 2 interface:

```
interfaces {
at-5/2/0 {
atm-options {
vpi 0 {
    shaping {
        vbr peak 10m sustained 6m burst 12;
    }
    oam-period 10;
    oam-liveness {
        up-count 6;
        down-count 5;
    }
}
vpi 4 {
    shaping {
        vbr peak 7m sustained 4m burst 24;
    }
}
vpi 5 {
    oam-period 10;
    oam-liveness {
        up-count 6;
        down-count 5;
    }
}
vpi 6;
}
unit 0 {
vci 0.128;
transmit-weight 20;
family inet {
    address 192.168.9.225/32 {
        destination 192.168.9.224;
    }
}
}
unit 1 {
vci 0.129;
transmit-weight 30;
family inet {
    address 192.168.9.226/32 {
        destination 192.168.9.227;
    }
}
}
```
unit 2 {
  vci 5.123;
  shaping {
    vbr peak 60m sustained 4m burst 24;
  }
  family inet {
    address 192.168.9.227/32 {
      destination 192.168.9.230;
    }
  }
}

Chapter 12

Channelized Interfaces Overview

Channelized interfaces enable you to configure a number of individual channels that subdivide the bandwidth of a larger interface and minimize the number of PICs that an installation requires.

Channelized QPP interfaces require M-series Enhanced FPCs.

Wherever the JUNOS Internet Software Configuration Guides refer to channelized interfaces and PICs without the “Q Performance Processor” or “QPP” descriptor, they are referring to the original channelized interfaces and PICs.

For channelized QPP logical interfaces, you can configure class of service (CoS). For more information, see “Associate a Scheduler with a DLCI or VLAN on a Channelized QPP Interface” on page 597.

This chapter provides a high-level overview of channelized interfaces, focusing mainly on the capabilities, properties, and structure of channelized QPP interfaces:

- Channelized Interface Capabilities on page 164
- Data Link Connection Identifiers on Channelized Interfaces on page 166
- Clock Sources on Channelized Interfaces on page 166
- Channelized QPP Interface Properties on page 169
- Structure of Channelized PICs with QPP on page 170
You can configure each port of a Channelized PIC with QPP as a single interface that uses the entire available bandwidth, or partition each port into smaller data channels. Following are the interface names associated with Channelized PICs with QPP:

- **coc12-fpc/ pic/ port**—On a Channelized OC-12 PIC
- **coc1-fpc/ pic/ port:channel**—On a Channelized OC-12 PIC
- **ct3-fpc/ pic/ port<:channel>**—On a Channelized OC-12 or Channelized DS-3 PIC
- **cstm1-fpc/ pic/ port**—On a Channelized STM-1 PIC
- **cau4-fpc/ pic/ port:channel**—On a Channelized STM-1 PIC
- **ct1-fpc/ pic/ port<:channel>**—On a Channelized OC-12 or Channelized DS-3 PIC
- **ce1-fpc/ pic/ port<:channel>**—On a Channelized E1 or a Channelized STM-1 PIC
- **so-fpc/ pic/ port**—One OC-12 channel on a Channelized OC-12 PIC or one STM-1 channel on a Channelized STM-1 PIC
- **t3-fpc/ pic/ port<:channel>**—On a Channelized OC-12 or Channelized DS-3 PIC
- **e1-fpc/ pic/ port<:channel>**—On a Channelized E1 a Channelized STM-1 PIC
- **so-fpc/ pic/ port:channel**—Four OC3 channels on a Channelized OC-12 PIC
- **t1-fpc/ pic/ port<:channel>**—On a Channelized OC-12 or Channelized DS-3 PIC
- **ds-fpc/ pic/ port<:channel>**—On a Channelized OC-12, Channelized STM-1, Channelized DS-3, or Channelized E1 PIC

Table 14 lists the number of supported interfaces on Channelized PICs with QPP.
Table 14: Supported Interfaces on Channelized PICs with QPP

<table>
<thead>
<tr>
<th>Interface Types</th>
<th>1-Port Channelized OC-12 PIC with QPP</th>
<th>1-port Channelized STM-1 PIC with QPP</th>
<th>4-Port Channelized DS-3 PIC with QPP</th>
<th>10-Port Channelized E1 PIC with QPP</th>
</tr>
</thead>
<tbody>
<tr>
<td>OC-12 interfaces</td>
<td>1</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>OC-3 interfaces</td>
<td>4</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>STM-1 interfaces</td>
<td>None</td>
<td>1</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>T3 interfaces</td>
<td>12</td>
<td>None</td>
<td>4</td>
<td>None</td>
</tr>
<tr>
<td>T1 interfaces</td>
<td>336</td>
<td>None</td>
<td>112</td>
<td>None</td>
</tr>
<tr>
<td>E1 interfaces</td>
<td>None</td>
<td>63</td>
<td>None</td>
<td>10</td>
</tr>
<tr>
<td>NxDS-0 interfaces</td>
<td>336</td>
<td>128</td>
<td>128—If the “N” in NxDS-0 is 8 or less.</td>
<td>310</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Maximum interfaces supported: 336</td>
<td>Maximum interfaces supported: 128</td>
<td>Maximum interfaces supported: 256</td>
</tr>
</tbody>
</table>

Following are the interfaces that you can configure on the Channelized PICs:

- T3 channels—t3-fpc/ pic/ port<channel> (on an Channelized OC-12 PIC)
- E1 channels—e1-fpc/ pic/ port (on a Channelized E1 or STM-1 PIC)
- T1 channels—t1-fpc/ pic/ port<channel> (on a Channelized DS-3 PIC)
- NxDS-0 channels—ds-fpc/ pic/ port<channel> (on a Channelized DS-3 or Channelized E1 PIC)
Table 15 shows the DLCIs that you can configure at each channel level.

<table>
<thead>
<tr>
<th>Channelized PICs</th>
<th>Number of DLCIs per level</th>
<th>Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Channelized DS-3</td>
<td>64 in regular mode; 3 in sparse mode</td>
<td>0 through 64 for regular mode; 0 through 1022 for sparse mode (0 is reserved for LMI)</td>
</tr>
<tr>
<td>Channelized STM-1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Multichannel DS-3</td>
<td>3</td>
<td>0 through 1022</td>
</tr>
<tr>
<td>Multichannel E1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Channelized PICs with QPP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Channelized OC-12</td>
<td>64 for T3, OC-3, SONET, and Channelized OC-12 interfaces; 16 for T1 and NxDS-0 interfaces</td>
<td>0 through 1022 for sparse mode (0 is reserved for LMI)</td>
</tr>
<tr>
<td>Channelized STM-1</td>
<td>64 for SONET interfaces; 16 for E1 and NxDS-0 interfaces</td>
<td>0 through 1022 for sparse mode (0 is reserved for LMI)</td>
</tr>
<tr>
<td>Channelized DS-3</td>
<td>64 for T3 interfaces; 16 for T1 and NxDS-0 interfaces</td>
<td>0 through 1022 for sparse mode (0 is reserved for LMI)</td>
</tr>
<tr>
<td>Channelized E1</td>
<td>16</td>
<td>0 through 1022 for sparse mode (0 is reserved for LMI)</td>
</tr>
</tbody>
</table>

Clock Sources on Channelized Interfaces

Channelized interfaces and channelized QPP interfaces have different clocking capabilities. For channelized QPP interfaces, you can configure clocking on each port independently by including the `clocking (internal | external)` statement at the `[edit interfaces interface-name]` hierarchy level.

For channelized QPP interfaces, clocking is provided as follows:

- **SONET-level** clocking is provided at the `[edit interfaces coc12-fpc/pic/port]` and `[edit interfaces cstm1-fpc/pic/port]` hierarchy levels.

- **T3-level** clocking is provided at the `[edit interfaces ct3-fpc/pic/port]` hierarchy level.

- **T1-level** clocking is provided at the `[edit interfaces t1-fpc/pic/port<:channel>]` hierarchy level.

- **E1-level** clocking is provided at the `[edit interfaces ce1-fpc/pic/port]` hierarchy level.

- **Clocking for all NxDs-0 channels** is provided at the `[edit interfaces ct1-fpc/pic/port<:channel>]` or `[edit interfaces ce1-fpc/pic/port]` hierarchy level.

- The `clocking` statement is ignored if you include it at the `[edit interfaces coc1-fpc/pic/port:channel]` or `[edit interfaces cau4-fpc/pic/port:channel]` hierarchy level.

- If you include the `clocking` statement at the channelized and interface levels—`coc12-fpc/pic/port` and `so-fpc/pic/port`, for example—the clocking configuration at the channelized level, `coc12-fpc/pic/port` in this example, takes precedence.
For channelized interfaces, clocking at each channel level is provided as follows:

- The clocking statement is supported only for channel 0; it is ignored if included in the configuration of other channels.

- The clock source configured for channel 0 applies to all channels on the channelized interfaces.

- When you configure the clock source for a channelized interface—`t3-fpc/pic/port:0`, for example—you must also include the channel-group statement at the [edit chassis] hierarchy level, and specify channel group 0.

- For Channelized T3 interfaces, you can configure external clocking (loop timing) on all T1 channels under the Channelized T3 interface. The `loop-timing` and `no-loop-timing` statements apply only to Channelized T3 interfaces. If you attempt to configure these statements on any other interface type, they are ignored. To configure loop timing for all T1 channels under the Channelized T3 interface, include the `loop-timing` statement at the [edit interfaces ct3-fpc/pic/port t3-options] hierarchy level.

- For Channelized STM-1 interfaces, you should configure the clock source at one side of the connection to be internal and configure the other side of the connection to be external.

Table 16 lists the clocking capabilities for each channelized PIC.

<table>
<thead>
<tr>
<th>PIC Type</th>
<th>SONET Level</th>
<th>DS-3 Level</th>
<th>DS-1/ E1 Level</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Channelized PICs</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Channelized OC-12</td>
<td>Not configurable.</td>
<td>The clocking statement is supported at the [edit interfaces t3-fpc/pic/port:0] hierarchy level.</td>
<td>Not applicable.</td>
</tr>
<tr>
<td>Channelized DS-3 and Multichannel DS-3</td>
<td>Not applicable.</td>
<td>The loop-timing statement is supported at the [edit interfaces t1-fpc/pic/port:0 t3-options] or [edit interfaces ds-fpc/pic/port:0:0 t3-options] hierarchy level.</td>
<td>The clocking statement is supported at the [edit interfaces t1-fpc/pic/port:0] or [edit interfaces ds-fpc/pic/port:0:0] hierarchy level.</td>
</tr>
<tr>
<td>Channelized STM-1</td>
<td>Not configurable.</td>
<td>Not applicable.</td>
<td>The clocking statement is supported at the [edit interfaces e1-fpc/pic/port:[0-62]] hierarchy level.</td>
</tr>
<tr>
<td>Channelized E1</td>
<td>Not applicable.</td>
<td>Not applicable.</td>
<td>The clocking statement is supported at the [edit interfaces e1-fpc/pic/port:[0-9]] or [edit interfaces ds-fpc/pic/port:0] hierarchy level.</td>
</tr>
</tbody>
</table>

Channelized PICs with QPP
<table>
<thead>
<tr>
<th>PIC Type</th>
<th>SONET Level</th>
<th>DS-3 Level</th>
<th>DS-1/ E1 Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Channelized OC-12 with QPP</td>
<td>The clocking statement is supported at the [edit interfaces coc12-fpc/pic/port]. The clocking statement is ignored if you include it at the [edit interfaces so-fpc/pic/port] hierarchy level.</td>
<td>The clocking statement is supported at the [edit interfaces t3-fpc/pic/port:1-12] hierarchy level. The clocking statement is ignored if you include it at the [edit interfaces coc1-fpc/pic/port:channel] hierarchy level.</td>
<td>The clocking statement is supported at the [edit interfaces ct1-fpc/pic/port:1-12]:[1-28] and [edit interfaces t1-fpc/pic/port:1-12]:[1-28] hierarchy levels.</td>
</tr>
<tr>
<td>Channelized STM-1 with QPP</td>
<td>The clocking statement is supported at the [edit interfaces cstm1-fpc/pic/port] hierarchy level. The clocking statement is ignored if you include it at the [edit interfaces cau4-fpc/pic/port:channel] or [edit interfaces so-fpc/pic/port] hierarchy levels.</td>
<td>Not applicable.</td>
<td>For E1 and NxDS-0 channels, the clocking statement is supported at the [edit interfaces ce1-fpc/pic/port:1-63]. The clocking statement is ignored if you include it at the [edit interfaces e1-fpc/pic/port] hierarchy level.</td>
</tr>
<tr>
<td>Channelized DS-3 with QPP</td>
<td>Not applicable.</td>
<td>The clocking statement is supported at the [edit interfaces t3-fpc/pic/port]. The clocking statement is ignored if you include it at the [edit interfaces t3-fpc/pic/port] hierarchy level.</td>
<td>For T1 channels, the clocking statement is supported at the [edit interfaces t1-fpc/pic/port:1-28] hierarchy level. For NxDS-0 channels, the clocking statement is supported at the [edit interfaces ct1-fpc/pic/port:1-28] hierarchy level.</td>
</tr>
<tr>
<td>Channelized E1 with QPP</td>
<td>Not applicable.</td>
<td>Not applicable.</td>
<td>For E1 and NxDS-0 channels, the clocking statement is supported at the [edit interfaces ce1-fpc/pic/port]. The clocking statement is ignored if you include it at the [edit interfaces e1-fpc/pic/port] hierarchy level.</td>
</tr>
</tbody>
</table>
Channelized QPP Interface Properties

On channelized QPP interfaces, you can specify options that are globally applied to all interface types associated with a channelized QPP interface. For example, e1-options statements that you include at the [edit interfaces cel-fpc/pic/port] hierarchy level apply globally to all E1 and NxDS-0 interfaces that you create by partitioning cel-fpc/pic/port. Likewise, t3-options statements that you include at the [edit interfaces ct3-fpc/pic/port] hierarchy level apply globally to all T1 and NxDS-0 interfaces that you create by partitioning ct3-fpc/pic/port.

You can also apply interface options at the channel level. For example, you can include t1-options statements at the [edit interfaces t1-fpc/pic/port] hierarchy level, and ds0-options statements at the [edit interfaces ds-0/1/1] hierarchy level.

Only a subset of the interface options is valid on each type of channelized QPP interface. You configure all HDLC information at the end data channel level, not at the parent level. For example, you configure HDLC information at the [edit interfaces ds-fpc/pic/port] hierarchy level, not at the [edit interfaces ct1-fpc/pic/port] hierarchy level.

Channelized QPP interfaces do not support receive buckets or transmit buckets.

There are some limitations for channelized QPP interfaces regarding where you place certain statements in the configuration. When you configure clocking, bit error rate testing (BERT), C-bit parity, and loopback statements on T3, T1, or DS-0 channels, you must follow these guidelines:

- For T3 QPP interfaces, you can include the loopback payload statement at the [edit interfaces ct3-fpc/pic/port] and [edit interfaces t3-fpc/pic/port] hierarchy levels. For T1 interfaces, you can include the loopback payload statement in the configuration at the [edit interfaces t1-fpc/pic/port] hierarchy level; it is ignored if included at the [edit interfaces ct1-fpc/pic/port] hierarchy level. For NxDS-0 interfaces, payload and remote loopback are the same. If you configure one, the other is ignored. NxDS-0 QPP interfaces do not support local loopback.

- If you include clocking, BERT, and C-bit parity configurations at both the [edit interfaces ct3-fpc/pic/port] and [edit interfaces t3-fpc/pic/port] hierarchy levels, the Channelized T3-level statements are valid, and the T3-level statements are ignored.

- If you include clocking, BERT, and C-bit parity configurations at both the [edit interfaces ct3-fpc/pic/port] and [edit interfaces t1-fpc/pic/port] hierarchy levels, the Channelized T3-level statements are operational for the T3 connections and the T1-level statements are operational for the T1 connections.

- Because DS-0 channels do not have clocking capability, you must configure clocking at the [edit interfaces ct1-fpc/pic/port] or [edit interfaces cel-fpc/pic/port] hierarchy level for Channelized NxDS-0 QPP interfaces.

- You can set BERT at the [edit interfaces t3-fpc/pic/port] hierarchy level or on any partitioned channel of the Channelized T3 interface. There are twelve BERT patterns available for NxDS-0 channels and twenty-eight BERT patterns for T1, Channelized T1, T3, and Channelized T3 interfaces within channelized QPP interfaces.

- For channelized interfaces that use Frame Relay encapsulation, the number of configurable data-link connection identifiers (DLCIs) varies by channelized interface type.
Structure of Channelized PICs with QPP

Figure 8, Figure 10, Figure 11, and Figure 11 show the structural organization of the Channelized OC-12 PIC with QPP, Channelized STM-1 PIC with QPP, Channelized DS-3 PIC with QPP, and Channelized E1 PIC with QPP. Table 17 on page 172 shows the structure of all channelized PICs, including channelized PICs with QPP and channelized PICs.

Figure 8: Structure of the Channelized OC-12 PIC with QPP

<table>
<thead>
<tr>
<th>SONET/SDH transport layer:</th>
<th>SONET/SDH path layer:</th>
<th>Clear-channel path layer OC-12 and OC-3:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>- so-fpc/pic/port[1-4]</td>
</tr>
<tr>
<td>SDH VT-mapped CT3:</td>
<td>M13-mapped CT3:</td>
<td>Clear-channel T3:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Clear-channel T3: T1:1-fpc/pic/port: [1-12][1-28]</td>
<td>Clear-channel T3: t3-fpc/pic/port[1-12]</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NxDS-0:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- ds-fpc/pic/port[1-12][1-28][1-24]</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

HDLC
Figure 9: Structure of the Channelized STM-1 PIC with QPP

SONET/SDH transport layer:
- cstm1-fpc/pic/port

SONET/SDH path layer:
- cau4-fpc/pic/port

Clear-channel path layer STM-1:
- so-fpc/pic/port

ITU-T Channelized E1:
- ce1-fpc/pic/port: [1-63]

KLM Channelized E1:
- ce1-fpc/pic/port: [1-63]

Clear-channel E1:
- e1-fpc/pic/port: [1-63]

NxDS-0:
- ds-fpc/pic/port: [1-63]: [1-31]

HDLC

Figure 10: Structure of the Channelized DS-3 PIC with QPP

CT3:
- ct3-fpc/pic/port

T3:
- t3-fpc/pic/port

CT1:
- ct1-fpc/pic/port: [1-28]

T1:
- t1-fpc/pic/port: [1-28]

NxDS-0:
- ds-fpc/pic/port: [1-28]: [1-24]

HDLC

Figure 11: Structure of the Channelized E1 PIC with QPP

CE1:
- ce1-fpc/pic/port

E1:
- e1-fpc/pic/port

NxDS-0:
- ds-fpc/pic/port: [1-31]

HDLC
### Table 17: Structural Differences: Channelized PICs and Channelized PICs with QPP

<table>
<thead>
<tr>
<th>PIC Type</th>
<th>Transport</th>
<th>Path</th>
<th>DS-3</th>
<th>DS-1/ E1</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Channelized PICs</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Channelized OC-12</td>
<td>t3-fpc/ pic/ port:0</td>
<td>t3-fpc/ pic/ port:[0-11]</td>
<td>t3-fpc/ pic/ port:[0-11]</td>
<td>Not applicable</td>
</tr>
<tr>
<td>Channelized T3 and Multichannel T3</td>
<td>Not applicable.</td>
<td>Not applicable.</td>
<td>t1-fpc/ pic/ port:0</td>
<td>t1-fpc/ pic/ port:[0-27]</td>
</tr>
<tr>
<td>Channelized STM-1</td>
<td>e1-fpc/ pic/ port:0</td>
<td>e1-fpc/ pic/ port:0</td>
<td>Not applicable.</td>
<td>e1-fpc/ pic/ port:[0-63]</td>
</tr>
<tr>
<td>Channelized E1</td>
<td>Not applicable.</td>
<td>Not applicable.</td>
<td>Not applicable.</td>
<td>e1-fpc/ pic/ port</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>ds-fpc/ pic/ port:0</td>
</tr>
<tr>
<td><strong>Channelized PICs with QPP</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>so-fpc/ pic/ port</td>
<td></td>
<td>t1-fpc/ pic/ port:[1-12];[1-28]</td>
</tr>
<tr>
<td>Channelized STM-1 with QPP</td>
<td>Not applicable.</td>
<td>cau4-fpc/ pic/ port so-fpc/ pic/ port</td>
<td>Not applicable.</td>
<td>ce1-fpc/ pic/ port:[1-63]</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>e1-fpc/ pic/ port:[1-63]</td>
</tr>
<tr>
<td>Channelized DS-3 with QPP</td>
<td>Not applicable.</td>
<td>Not applicable.</td>
<td>ct3-fpc/ pic/ port t3-fpc/ pic/ port</td>
<td>ct1-fpc/ pic/ port:[1-28]</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>t1-fpc/ pic/ port:[1-28]</td>
</tr>
<tr>
<td>Channelized E1 with QPP</td>
<td>Not applicable.</td>
<td>Not applicable.</td>
<td>Not applicable.</td>
<td>ce1-fpc/ pic/ port</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>e1-fpc/ pic/ port</td>
</tr>
</tbody>
</table>
Chapter 13
Configure Channelized E1 Interfaces

Each Channelized E1 PIC and Channelized E1 PIC with QPP has 10 E1 ports that you can channelize to the NxDS-0 level. Each E1 interface has 32 time slots (DS-0), in which time slot 0 is reserved. You can combine one or more of these DS-0 time slots (channels) to create a channel group (NxDS-0).

This chapter is organized as follows:

- Configure Channelized E1 QPP Interfaces on page 173
- Configure Channelized E1 QPP Interface Properties on page 175
- Configure Channelized E1 Interfaces on page 178

For examples of Channelized E1 interface configuration, see the following:

- Example: Configure Channelized E1 Interfaces on page 181
- Example: Configure Channelized E1 QPP Interfaces on page 182

Configure Channelized E1 QPP Interfaces

This section describes how to configure Channelized E1 QPP interfaces, discussing the following topics:

- Configure E1 QPP Interfaces on page 173
- Configure Fractional E1 QPP Interfaces on page 174
- Configure an NxDS-0 QPP Interface on page 174

Configure E1 QPP Interfaces

On a 10-port Channelized E1 PIC with QPP, you can configure up to 10 E1 interfaces. To configure an E1 interface, include the no-partition statement at the [edit interfaces ce1-fpc/ pic/ port] hierarchy level:

[edit interfaces ce1-fpc/ pic/ port]
no-partition;

This configuration creates interface e1-fpc/ pic/ port.
Configure Fractional E1 QPP Interfaces

On a Channelized E1 PIC with QPP, you can configure up to 10 fractional E1 interfaces. To configure a fractional E1 interface on a Channelized E1 PIC with QPP, you must perform the following tasks:

1. Include the no-partition statement at the [edit interfaces ce1-fpc/pic/port] hierarchy level:

   [edit interfaces ce1-fpc/pic/port]
   no-partition;

   This configuration creates interface e1-fpc/pic/port.

2. Configure the number of time slots allocated to the E1 QPP interface by including the timeslots statement at the [edit interfaces e1-fpc/pic/port e1-options] hierarchy level:

   [edit interfaces e1-fpc/pic/port e1-options]
   timeslots time-slot-range;

   For Channelized E1 QPP interfaces, the time-slot range is 2 through 31. The default is to use all the time slots. You can designate any combination of time slots for usage. You can configure a range of values with hyphens, and you can separate multiple values with commas. Do not include spaces when you specify time slot numbers.

   For more information about E1 time slots, see “Configure Fractional E1 Time Slots” on page 249.

Example: Configure Fractional E1 QPP Interfaces

Configure a fractional E1 interface that uses time slots 2 through 10:

   [edit interfaces ce1-0/0/0]
   no-partition;

   [edit interfaces e1-0/0/0 e1-options]
   timeslots 2-10;

Configure an NxDS-0 QPP Interface

On a Channelized E1 PIC with QPP, you can configure up to 310 NxDS-0 channels. To configure an NxDS-0 QPP interface on a Channelized E1 PIC with QPP, you must configure the number of time slots allocated to the NxDS-0 QPP interface by including the partition, timeslots, and interface-type statements at the [edit interfaces ce1-fpc/pic/port] hierarchy level, specifying the ds interface type:

   [edit interfaces ce1-fpc/pic/port]
   partition partition-number timeslots time-slot-range interface-type ds;

   For Channelized E1 QPP interfaces, the partition number range is 1 through 31; the time-slot range is 2 through 31. The default is to use all the time slots. You can designate any combination of time slots for usage. You can configure a range of values with hyphens, and you can separate multiple values with commas. Do not include spaces when you specify time slot numbers. For more information about E1 time slots, see “Configure Fractional E1 Time Slots” on page 249.
Example: Configure an NxDS-0 QPP Interface

Configure an NxDS-0 interface that uses time slots 2 through 10. This configuration creates the ds-0/0/0:1:1 interface.

```
[edit interfaces ce1-0/0/0:1]
partition 1 timeslots 2-10 interface-type ds;
```

Configure Channelized E1 QPP Interface Properties

This section lists the interface properties that are valid at each channel level on a Channelized E1 QPP interface, discussing the following topics:

- Specify Options at the Channelized E1 QPP Interface Level on page 175
- Specify Options at the E1 QPP Interface Level on page 176
- Specify Options at the NxDS-0 QPP Interface Level on page 177

For more information, see “Channelized QPP Interface Properties” on page 169.

Specify Options at the Channelized E1 QPP Interface Level

To specify options at the Channelized E1 interface level, include the following statements at the [edit interfaces ce1-fpc/pic/port] hierarchy level:

```
[edit interfaces ce1-fpc/pic/port]
clocking clock-source;
disable;
description text;
e1-options {
  bert-algorithm algorithm;
  bert-error-rate rate;
  bert-period seconds;
  fcs (32 | 16);
  framing (g704 | g704-no-crc4 | unframed);
  loopback (local | remote);
}
no-partition;
partition partition-number oc-slice oc-slice-range interface-type type;
traceoptions {
  flag flag <flag-modifier> <disable>;
}
```

For more information about specific parameters, see “Configure Physical Interface Properties” on page 39 and “Configure E1 Interfaces” on page 243.
Specify Options at the E1 QPP Interface Level

To specify options at the E1 interface level, include the following statements at the [edit interfaces e1-fpc/pic/port] hierarchy level:

```junos
[edit interfaces e1-fpc/pic/port]
clocking clock-source;
dce;
disable;
description text;
e1-options {
    bert-algorithm algorithm;
    bert-error-rate rate;
    bert-period seconds;
    byte-encoding (nx64 | nx56);
    fcs (32 | 16);
    framing (g704 | g704-no-crc4 | unframed);
    idle-cycle-flag (flags | ones);
    loopback (local | remote);
    start-end-flag (shared | filler);
    timeslots time-slot-range;
}
encapsulation type;
hold-time up milliseconds down milliseconds;
keepalives <interval seconds> <down-count number> <up-count number>;
lmi {
    lmi-type (ansi | itu);
    n391dte number;
    n392dce number;
    n392dte number;
    n393dce number;
    t391dte seconds;
    t392dce seconds;
}
mtu bytes;
no-keepalives;
ppp-options {
    chap {
        access-profile name;
        local-name name;
        passive;
    }
}
traceoptions {
    flag flag <flag-modifier> <disable>;
}
(traps | no-traps);
unit logical-unit-number {
    logical-interface-statements;
}
```

For more information about specific parameters, see “Configure Physical Interface Properties” on page 39 and “Configure E1 Interfaces” on page 243.
Specify Options at the NxDS-0 QPP Interface Level

To specify options at the NxDS-0 interface level, include the following statements at the [edit interfaces ds-fpc/ pic/ port<channel>] hierarchy level:

```
[edit interfaces ds-fpc/ pic/ port<:channel>]
accounting-profile name;
dce;
disable;
description text;
ds0-options {
  bert-algorithm algorithm;
  bert-error-rate rate;
  bert-period seconds;
  byte-encoding (nx64 | nx56);
  fcs (32 | 16);
  idle-cycle-flag (flags | ones);
  invert-data;
  loopback (payload | remote);
  start-end-flag (shared | filler);
}
encapsulation type;
hold-time up milliseconds down milliseconds;
keepalives <down-count number> <interval seconds> <up-count number>;
lmi {
  lmi-type (ansi | itu);
  n391dte number;
  n392dce number;
  n392dte number;
  n393dce number;
  t391dte seconds;
  t392dce seconds;
}
mtu bytes;
nok-keepalives;
ppp-options {
  chap {
    access-profile name;
    local-name name;
    passive;
  }
}
traceoptions {
  flag flag <flag-modifier> <disable>;
}
(traps | no-traps)
unit {
  logical-interface-statements;
}
```

For more information about specific parameters, see “Configure Physical Interface Properties” on page 39.
Configure Channelized E1 Interfaces

There can be a maximum of 24 channel groups per 10-port Channelized E1 interface. Thus, you can configure a maximum of 240 channel groups per PIC.

To specify the DS-0 channel group number in the interface name, include a colon (:) as a separator. For example, a Channelized E1 PIC might have the following physical and virtual interfaces:

```
ds-0/0/0:x
```

x is a DS-0 channel group ranging from 0 through 23 (see Table 18 on page 179 for more information about ranges).

You can use any of the values within the range available for x; you do not have to configure the links sequentially. In addition, the JUNOS software applies the interface options you configure according to the following rules:

- To configure the `e1-options` statement, you must set channel group x to 0:
  ```
ds-0/0/0:0
  ```
- There are no restrictions on configuring the `ds0-options` statement.
- If you delete a configuration you previously committed for channel group 0, the options return to default values.

To configure the channel groups and time slots for a Channelized E1 interface, include the following statements at the `[edit chassis]` hierarchy level:

```
[edit chassis]
fpc slot-number {
  pic pic-number {
    ce1 {
      e1 link-number {
        channel-group group-number timeslots time-slot-range;
      }
    }
  }
}
```

If you commit the interface name but do not include the `[edit chassis]` configuration, the Channelized E1 PIC behaves like a standard E1 PIC: None of the DS-0 functionality is accessible.
For example, the following configuration assigns channel groups and time slots for three interfaces:

```
[edit chassis]
fpc 0 {
pic 1 {
  cel1 {
    e1 0 {
      channel-group 1 timeslots 1;
      channel-group 5 timeslots 5-7;
    }
    e1 4 {
      channel-group 10 timeslots 11,17, 28-31;
    }
  }
}
}
```

This configuration results in the following interfaces:

- **ds-0/1/0:1**, with time slot 1 allocated
- **ds-0/1/0:5**, with time slots 5 through 7 allocated
- **ds-0/1/4:10**, with time slots 11, 17, and 28 through 31 allocated

Note that the remaining ports (other than 0 and 4) remain as regular E1 interfaces (and follow the e1/n/1/x naming convention).

Table 18 shows the ranges you can specify for each of the elements in the preceding configuration:

<table>
<thead>
<tr>
<th>Item</th>
<th>Option</th>
<th>Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>FPC slot</td>
<td>slot-number</td>
<td>0 through 7</td>
</tr>
<tr>
<td>PIC slot</td>
<td>pic-number</td>
<td>0 through 3</td>
</tr>
<tr>
<td>E1 link</td>
<td>link-number</td>
<td>0 through 9</td>
</tr>
<tr>
<td>DS-0 channel group</td>
<td>group-number</td>
<td>0 through 23</td>
</tr>
<tr>
<td>Time slot</td>
<td>time-slot-range</td>
<td>0 through 31 (with time slot 0 reserved)</td>
</tr>
</tbody>
</table>

FPC slot range depends on platform. The maximum range of 0 through 7 applies to M40 routers; for M20 routers, the range is 0 through 3; for M10 routers the range is 0 through 1; for M5 routers, the only applicable value is 0.

The theoretical maximum number of channel groups possible per PIC is $10 \times 24 = 240$. This is within the maximum bandwidth available.
There are 32 time slots on an E1 interface. The default is to use all the time slots; however, time slot 0 is reserved. You can designate any combination of time slots for usage. You can configure a range of values with hyphens, and you can separate multiple values with commas. Do not include spaces when you specify time slot numbers.

To use time slots 1 through 10, configure the time-slot range as follows:

```
[edit chassis fpc slot-number pic pic-number ce1 e1 link-number]
channel-group group-number timeslots 1-10;
```

To use time slots 1 through 5, time slot 10, and time slot 24, configure the time-slot range as follows:

```
[edit chassis fpc slot-number pic pic-number ce1 e1 link-number]
channel-group group-number timeslots 1-5,10,24;
```

For channelized fractional E1 interfaces only, when you include the timeslots statement at the [edit interfaces interface-name e1-options] hierarchy level, time slot 1 is reserved, so you must allocate time slots in the range of 2 through 31. Alternatively, you can configure time slots by including the channel-group and timeslots statements at the [edit chassis] hierarchy level, in which case you can allocate time slots in the range of 1 through 31.

To configure Channelized E1 interface properties, include the e1-options statement at the [edit interfaces interface-name] hierarchy level:

```
[edit interfaces interface-name]
e1-options {
  fcs (32 | 16);
  framing (g704 | g704-no-crc4 | unframed);
  idle-cycle-flag (flags | ones);
  loopback (local | remote);
  start-end-flag (shared | filler);
}
```

To specify options for each of the DS-0 channels, include the ds0-options statement at the [edit interfaces interface-name] hierarchy level:

```
[edit interfaces interface-name]
ds0-options {
  byte-encoding (nx64 | nx56);
  fcs (32 | 16);
  idle-cycle-flag (flags | ones);
  loopback (local | remote);
  start-end-flag (shared | filler);
}
```

The set of options the JUNOS software applies to the interface depends on how you specify the interface name. For more information, see “Examples: Interface Naming” on page 26.
For DS-0 channels on a Channelized E1 interface, the clocking statement is supported only for channel 0; it is ignored if included in the configuration of channels 1 through 11. The clock source configured for channel 0 applies to all channels on the Channelized E1 interface. The individual DS-0 channels use a gapped 45-MHz clock as the transmit clock. When you configure the clock source for a channelized interface—`ds-x/y/z:0`, for example—you must also include the channel-group statement at the `edit chassis` hierarchy level, and specify channel group 0. For more information, see “Clock Sources on Channelized Interfaces” on page 166.

Only a subset of the E1 options is valid for the channelized configuration; you specify the time slots using the `edit chassis` configuration described in “Examples: Interface Naming” on page 26. For more information about the E1 and DS-0 options, see “Configure E1 Interfaces” on page 243 and “Configure T1 Interfaces” on page 387.

Each E1 interface has 32 time slots (DS-0s), in which time slot 0 is reserved. You can combine one or more of these DS-0 time slots (channels) to create a channel group (`NxDS-0`). There can be a maximum of 24 channel groups per E1 interface.

Example: Configure Channelized E1 Interfaces

The following configuration is sufficient to get the Channelized E1 interface up and running:

```
[edit chassis]
 fpc 0 {
  pic 1 {
   ce1 {
    e1 0 {
     channel-group 0 timeslots 1;
     channel-group 1 timeslots 2;
     channel-group 5 timeslots 5-7;
    }
    e1 4 {
     channel-group 10 timeslots 11,17, 28-31;
    }
   }
  }
 };

[edit interfaces ds-0/1/0:0]
e1-options {
  fcs 32;
  framing g704-non-grc;
  loopback remote;
}

[edit interfaces ds-0/1/4:10]
ds0-options {
  byte-encoding nx56;
  start-end-flag filler;
}
```
Example: Configure Channelized E1 QPP Interfaces

The following configuration is sufficient to get the Channelized E1 QPP interface up and running:

```
[edit]
interfaces {
  ce1-1/2/3 {
    partition 1 timeslots 10 interface-type ds; #ds-1/2/3:1
    partition 2 timeslots 1-9 interface-type ds; #ds-1/2/3:2
  }
  ds-1/2/3:1 {
    unit 0 {
      family inet {
        address 10.25.1.2/24;
      }
    }
  }
  ds-1/2/3:2 {
    unit 0 {
      family inet {
        address 10.25.2.2/24;
      }
    }
  }
}[edit]
interfaces {
  ce1-1/2/6 {
    no-partition; #e1-1/2/6
  }
  e1-1/2/6 {
    e1-options {
      timeslots 1-2;
    }
    unit 0 {
      family inet {
        address 10.255.126.2/24;
      }
    }
  }
}[edit]
```
Chapter 14
Configure Channelized OC-12 Interfaces

Channelized QPP interfaces allow arbitrary and dynamic channelization of serial links, allowing greater flexibility than the channelized interfaces. For example, each Channelized OC-12 PIC with QPP is capable of supporting a full OC-12 interface or can be channelized into four OC-3 data channels, 12 T3 data channels, 336 T1 data channels, or 336 DS-0 data channels, or any combination of T1, T3, and NxDS-0, up to 336 channels. By comparison, the Channelized OC-12 PIC supports only 12 T3 channels. Figure 16 and Figure 13 on page 184 illustrate the difference in flexibility between a Channelized OC-12 PIC with QPP and an Channelized OC-12 PIC.

Figure 12: Sample Channelization of OC-12 PIC with QPP

In Figure 16, a Channelized OC-12 PIC with QPP is partitioned into the following OC slices:

a. An OC-3 interface.
b. Another OC-3 interface.
c. A Channelized OC-1 partitioned into T1 interfaces.
d. A Channelized OC-1 converted into a T3 interface.
e. A Channelized OC-1 partitioned into T1 interfaces and Channelized T1s, which are partitioned into NxDS-0 interfaces.
f. A Channelized OC-1 converted into a Channelized T3, which is partitioned into T1 interfaces.

**Bold** entries correspond to actual packet channels.
g. A Channelized OC-1 converted into a Channelized T3, which is partitioned into into T1 interfaces and a Channelized T1, which is partitioned into NxDS-0 interfaces.

h. A Channelized OC-1 partitioned into Channelized T1s, which are partitioned into NxDS-0 interfaces.

This is one of thousands of ways to configure a Channelized OC-12 PIC with QPP. To configure the interfaces shown in Figure 16, see “Example: Configure Channelized OC-12 QPP Interfaces” on page 199.

Figure 13: Sample Channelization of OC-12 PIC

Figure 2 shows five T3 channels configured on the Channelized OC-12 PIC. You can configure seven additional T3 channels. For more information about configuring Channelized OC-12 PICs, see “Configure Channelized OC-12 Interfaces” on page 183. To create the interfaces shown in Figure 13, see “Configure Aggregated SONET/SDH Interfaces” on page 380.

This chapter is organized as follows:

- Configure Channelized OC-12 QPP Interfaces on page 184
- Configure Channelized OC-12 QPP Interface Properties on page 192
- Configure Channelized OC-12 Interfaces on page 198

For examples of Channelized OC-12 interface configuration, see the following sections:

- Example: Configure Channelized OC-12 QPP Interfaces on page 199
- Example: Configure Channelized OC-12 Interfaces on page 203

Configure Channelized OC-12 QPP Interfaces

This section describes how to configure Channelized OC-12 QPP interfaces, discussing the following topics:

- Configure an OC-12 QPP Interface on page 185
- Configure T3 QPP Interfaces on page 185
- Configure OC-3 QPP Interfaces on page 186
- Configure T1 QPP Interfaces on page 187
- Configure NxDS-0 QPP Channels on page 189
- Configure Fractional T1 QPP Interfaces on page 191
Configure an OC-12 QPP Interface

On a one-port Channelized OC-12 PIC with QPP, you can configure one OC-12 interface. To configure an OC-12 interface, include the no-partition statement at the [edit interfaces coc12-fpc/pic/port] hierarchy level:

```
[edit interfaces coc12-fpc/pic/port]
no-partition;
```

This configuration creates interface so-fpc/pic/port.

Configure T3 QPP Interfaces

On a Channelized OC-12 PIC with QPP, you can configure up to 12 T3 interfaces.

To configure a T3 interface on an OC-12 PIC, include the partition, oc-slice, and interface-type statements at the [edit interfaces coc12-fpc/pic/port] hierarchy level, specifying the coc1 interface type:

```
[edit interfaces coc12-fpc/pic/port]
partition partition-number oc-slice oc-slice-range interface-type coc1;
```

This configuration creates interface coc1-fpc/pic/port:channel.

Then, include the no-partition interface-type statement at the [edit interfaces coc1-fpc/pic/port:channel] hierarchy level, specifying the t3 interface type:

```
[edit interfaces coc1-fpc/pic/port:channel]
no-partition interface-type t3;
```

This configuration creates interface t3-fpc/pic/port:channel.

The partition number is the sublevel interface partition index and correlates with the channel number. For Channelized OC-1 interfaces, the partition number can be in the range 1 through 12.

The OC-slice range is the range of SONET/SDH slices. For SONET/SDH interfaces, the OC-slice range specifies the bandwidth size required for the interface type you are configuring. For Channelized OC-1 interfaces, the OC slice can be in the range 1 through 12. You can configure only one OC slice per Channelized OC-1 interface.

The interface type is the channelized interface type or clear channel you are creating. For Channelized OC-12 interfaces, type can be so or coc1.
Example: Configure T3 QPP Interfaces

Configure a T3 interface using partition 3 and OC slice 3. This configuration creates interface t3-1/1/0:3.

```
[edit interfaces coc12-1/1/0]
partition 3 oc-slice 3 interface-type coc1;
```

```
[edit interfaces coc1-1/1/0:3]
no-partition interface-type t3;
```

Configure OC-3 QPP Interfaces

On a Channelized OC-12 PIC with QPP, you can configure up to four OC-3 QPP interfaces. To configure an OC-3 QPP interface, include the partition, oc-slice, and interface-type statements at the [edit interfaces coc12-fpc/pic/port] hierarchy level, specifying the so interface type:

```
[edit interfaces coc12-fpc/pic/port]
partition partition-number oc-slice oc-slice-range interface-type so;
```

The partition number is the sublevel interface partition index. For SONET/SDH interfaces, the partition number does not correlate with bandwidth size. For OC-3 interfaces, the partition number can be 1 through 4.

The OC-slice range is the range of SONET/SDH slices. For SONET/SDH interfaces, the OC-slice range specifies the bandwidth size required for the interface type you are configuring. OC-3 QPP interfaces must occupy three consecutive OC slices per interface, in one of the following forms:

- 1-3
- 4-6
- 7-9
- 10-12

By contrast, the T3 and OC-1 QPP interfaces each occupy one OC slice per interface.

The interface type is the channelized interface type or data channel you are creating. For Channelized OC-12 interfaces, the interface type can be coc1 or so.
Example: Configure OC-3 QPP Interfaces

Configure an OC-3 interface, using partition 1 and OC slices 4 through 6. This configuration creates interface so-1/1/0:1.

```
[edit interfaces coc12-1/1/0]
partition 1 oc-slice 4-6 interface-type so;
```

Configure T1 QPP Interfaces

On a Channelized OC-12 PIC with QPP, you can configure up to 336 T1 interfaces. To configure T1 interfaces on a Channelized OC-12 PIC with QPP, you perform the following tasks:

1. Partition the Channelized OC-12 interface into Channelized OC-1 interfaces by including the partition, oc-slice, and interface-type statements at the [edit interfaces coc12-fpc/ pic/port] hierarchy level, specifying the coc1 interface type:

   ````
   [edit interfaces coc12-fpc/ pic/port]
   partition partition-number oc-slice oc-slice-range interface-type coc1;
   ````

2. If your network equipment is M13 or C-bit parity mapped, you partition the Channelized OC-1 interface into T1 interfaces by including the partition and interface-type statements at the [edit interfaces coc1-fpc/ pic/ port:channel] hierarchy level, specifying the t1 interface type:

   ````
   [edit interfaces coc1-fpc/ pic/ port:channel]
   partition partition-number interface-type t1;
   ````

If your network equipment is VT mapped, you convert the Channelized OC-1 interface into a Channelized T3 interface by including the no-partition and interface-type statements at the [edit interfaces coc1-fpc/ pic/ port:channel] hierarchy level, specifying the ct3 interface type:

```
[edit interfaces coc1-fpc/ pic/ port:channel]
no-partition partition-number interface-type ct3;
```

Note that because the no-partition statement is included, this configuration does not create another level of channelization, as denoted by the number of colons in the resulting interface.

You then partition the Channelized T3 interface into T1 interfaces by including the partition and interface-type statements at the [edit interfaces ct3-fpc/ pic/ port:channel] hierarchy level, specifying the t1 interface type:

```
[edit interfaces ct3-fpc/ pic/ port:channel]
partition partition-number interface-type t1;
```

Figure 14 shows VT-mapped and M13- or C-bit parity-mapped configurations of T1 QPP channels.
Figure 14: Configure T1 Interfaces on a Channelized OC-12 PIC

**Example: Configure T1 QPP Interfaces**

Configure the following T1 interfaces:

- t1-0/0/0:1:1
- t1-0/0/0:1:2
- t1-0/0/0:1:3
- t1-0/0/0:1:4
- t1-0/0/0:1:5

**VT-Mapped Configuration**

```
[edit interfaces coc12-0/0/0]
partition 1 oc-slice 1 interface-type coc1;

[edit interfaces coc1-0/0/0:1]
partition 1-5 interface-type t1;
```

**M13 or C-bit Parity-Mapped Configuration**

```
[edit interfaces coc12-0/0/0]
partition 1 oc-slice 1 interface-type coc1;

[edit interfaces coc1-0/0/0:1]
no-partition interface-type ct3;

[edit interfaces ct3-0/0/0:1]
partition 1-5 interface-type t1;
```
Configure NxDS-0 QPP Channels

On a Channelized OC-12 PIC with QPP, you can configure up to 336 NxDS-0 channels. To configure NxDS-0 interfaces on a Channelized OC-12 PIC with QPP, you perform the following tasks:

1. Partition the Channelized OC-12 interface into Channelized OC-1 interfaces by including the partition, oc-slice, and interface-type statements at the [edit interfaces coc12-fpc/pic/port] hierarchy level, specifying the coc1 interface type:

   [edit interfaces coc12-fpc/pic/port]
   partition partition-number oc-slice oc-slice-range interface-type coc1;

2. If your network equipment is M13 or C-bit parity mapped, you partition the Channelized OC-1 interface into Channelized T1 interfaces by including the partition and interface-type statements at the [edit interfaces coc1-fpc/pic/port:channel] hierarchy level, specifying the ct1 interface type:

   [edit interfaces coc1-fpc/pic/port:channel]
   partition partition-number interface-type ct1;

   If your network equipment is VT mapped, you convert the Channelized OC-1 interface into a Channelized T3 interface by including the no-partition and interface-type statements at the [edit interfaces coc1-fpc/pic/port:channel] hierarchy level, specifying the ct3 interface type:

   [edit interfaces coc1-fpc/pic/port:channel]
   no-partition partition-number interface-type ct3;

   Note that because the the no-partition statement is included, this configuration task does not create another level of channelization, as denoted by the number of colons in the resulting interface.

   You then partition the Channelized T3 interface into Channelized T1 interfaces by including the partition and interface-type statements at the [edit interfaces ct3-fpc/pic/port:channel] hierarchy level, specifying the ct1 interface type:

   [edit interfaces ct3-fpc/pic/port:channel]
   partition partition-number interface-type ct1;

3. Configure Channelized NxDS-0 QPP interfaces on the Channelized T1 QPP interface by including the partition, timeslots, and interface-type statements at the [edit interfaces ct1-fpc/pic/port<:channel>] hierarchy level, specifying the ds interface type:

   [edit interfaces ct1-fpc/pic/port<:channel>]
   partition partition-number timeslots time-slot-range interface-type ds;

   Figure 15 shows VT-mapped and M13- or C-bit parity-mapped configurations of NxDS-0 QPP channels.
Figure 15: Configure NxDS-0 Interfaces on a Channelized OC-12 PIC

Example: Configure an NxDS-0 QPP Interface

Configure the following two NxDS-0 interfaces with 10 time slots and 4 time slots, respectively:

- ds-0/0/0:1:2:1
- ds-0/0/0:1:2:2

VT-Mapped Configuration

```plaintext
[edit interfaces coc12-0/0/0]
partition 1 oc-slice 1 interface-type coc1;

[edit interfaces coc1-0/0/0:1]
partition 2 interface-type ct1;

[edit interfaces ct1-0/0/0:1:2]
partition 1 timeslots 1-10 interface-type ds;
partition 2 timeslots 12-16 interface-type ds;
```

M13 or C-bit Parity-Mapped Configuration

```plaintext
[edit interfaces coc12-0/0/0]
partition 1 oc-slice 1 interface-type coc1;

[edit interfaces coc1-0/0/0:1]
no-partition interface-type ct3;

[edit interfaces ct3-0/0/0:1]
partition 2 interface-type ct1;

[edit interfaces ct1-0/0/0:1:2]
partition 1 timeslots 1-10 interface-type ds;
partition 2 timeslots 12-16 interface-type ds;
```
Configure Fractional T1 QPP Interfaces

On a Channelized OC-12 PIC with QPP, you can configure up to 336 fractional T1 interfaces. To configure a fractional T1 interface on a Channelized OC-12 PIC with QPP, you must perform the following tasks:

1. Configure a T1 QPP interface. For more information, see “Configure T1 QPP Interfaces” on page 187:

   This configuration creates interface t1-fpc/ pic/ port:channel:channel.

2. Configure the number of time slots allocated to the T1 QPP interface by including the timeslots statement at the [edit interfaces t1-fpc/ pic/ port<:channel> t1-options] hierarchy level:

   [edit interfaces t1-fpc/ pic/ port<:channel> t1-options]
   timeslots time-slot-range;

   For Channelized T1 QPP interfaces, the time-slot range is 1 through 24. You can designate any combination of time slots for usage. The default is to use all the time slots. For more information about T1 time slots, see “Configure Fractional T1 Time Slots” on page 394.

Example: Configure Fractional T1 QPP Interfaces

Configure a fractional T1 interface that uses time slots 1 through 10:

   [edit interfaces coc12-0/0/0]
   partition 1 oc-slice 1 interface-type coc1;

   [edit interfaces coc1-0/0/0:1]
   partition 1 interface-type t1;

   [edit interfaces t1-0/0/0:1:1 t1-options]
   timeslots 1-10;
Configure Channelized OC-12 QPP Interface Properties

This section lists the interface properties that are valid at each channel level on a Channelized OC-12 QPP interface, discussing the following topics:

- Specify Options at the Channelized OC-12 QPP Level on page 192
- Specify Options at the Channelized OC-1 QPP Level on page 193
- Specify Options at the Channelized T3 QPP Level on page 194
- Specify Options at the Channelized T1 QPP Level on page 194
- Specify Options at the T3 QPP Interface Level on page 195
- Specify Options at the T1 QPP Interface Level on page 196
- Specify Options at the NxDS-0 QPP Interface Level on page 197

For more information, see “Channelized QPP Interface Properties” on page 169.

Specify Options at the Channelized OC-12 QPP Level

To specify options at the Channelized OC-12 interface level, include the following statements at the [edit interfaces coc12-fpc/pic/port] hierarchy level:

```
[edit interfaces coc12-fpc/pic/port]
  clocking clock-source;
  disable;
  description text;
  no-partition;
  partition partition-number oc-slice oc-slice-range interface-type type;
  sonet-options {
    aps {
      advertise-interval milliseconds;
      authentication-key key;
      force;
      hold-time milliseconds;
      lockout;
      neighbor address;
      paired-group group-name;
      protect-circuit group-name;
      request;
      revert-time seconds;
      working-circuit group-name;
    }
    bytes {
      sonet-header-byte-options ;
    }
    loopback (local | remote);
    (z0-increment | no-z0-increment);
  }
  traceoptions {
    flag flag <flag-modifier> <disable>;
  }
```
For more information about specific parameters, see “Configure Physical Interface Properties” on page 39 and “Configure SONET/SDH Interfaces” on page 359.

For OC-12 and OC-3 SONET/SDH QPP interfaces (so-fpc/ pic/ port and so-fpc/ pic/ port:[1-4]), all physical interface properties and SONET/SDH interface properties are valid, except SONET link aggregation, receive bucket, and transmit bucket which are ignored if configured.

Specify Options at the Channelized OC-1 QPP Level

To specify options at the Channelized OC-1 interface level, include the following statements at the [edit interfaces coc1-fpc/ pic/ port:channel] hierarchy level:

```
[edit interfaces coc1-fpc/ pic/ port:channel]
clocking clock-source;
disable;
description text;
nopartition {
    interface-type type;
}
partition partition-number oc-slice oc-slice-range interface-type type;
sonet-options {
    bytes {
        sonet-header-byte-options;
    }
    loopback (local | remote);
    path-trace trace-string;
}
traceoptions {
    flag flag <flag-modifier> <disable>;
}
```

For more information about specific parameters, see “Configure Physical Interface Properties” on page 39 and “Configure SONET/SDH Interfaces” on page 359.
Specify Options at the Channelized T3 QPP Level

To specify options at the Channelized T3 interface level, include the following statements at the [edit interfaces ct3-fpc/pic/port:channel] hierarchy level:

```
[edit interfaces ct3-fpc/pic/port:channel]
clocking clock-source;
disable;
description text;
no-partition;
partition partition-number oc-slice oc-slice-range interface-type type;
t3-options {
    bert-algorithm algorithm;
    bert-error-rate rate;
    bert-period seconds;
    (cbit-parity | no-cbit-parity);
    (feac-loop-respond | no-feac-loop-respond);
    (long-buildout | no-long-buildout);
    loopback (local | payload | remote);
}
traceoptions {
    flag flag <flag-modifier> <disable>;
}
```

For more information about specific parameters, see “Configure Physical Interface Properties” on page 39 and “Configure T3 Interfaces” on page 395.

Specify Options at the Channelized T1 QPP Level

To specify options at the channelized T1 QPP interface level, include the following statements at the [edit interfaces ct1-fpc/pic/port:channel] hierarchy level:

```
[edit interfaces ct1-fpc/pic/port:channel]
clocking clock-source;
disable;
description text;
partition partition-number oc-slice oc-slice-range interface-type type;
t1-options {
    bert-algorithm algorithm;
    bert-error-rate rate;
    bert-period seconds;
    framing (esf | sf);
    line-encoding (ami | b8zs);
    loopback (local | payload | remote);
    remote-loopback-respond;
}
traceoptions {
    flag flag <flag-modifier> <disable>;
}
```

For more information about specific parameters, see “Configure Physical Interface Properties” on page 39 and “Configure T3 Interfaces” on page 395.
Specify Options at the T3 QPP Interface Level

To specify options at the T3 interface level, include the following statements at the \[edit interfaces t3-fpc/pic/port:channel\] hierarchy level:

\[
\begin{align*}
\text{[edit interfaces t3-fpc/pic/port:channel]} \\
\text{dce;} \\
\text{disable;} \\
\text{description text;} \\
\text{encapsulation type;} \\
\text{hold-time up milliseconds down milliseconds;} \\
\text{keepalives <interval seconds> <down-count number> <up-count number>;} \\
\text{mtu bytes;} \\
\text{no-keepalives;} \\
\text{ppp-options {} } \\
\text{chap {}} \\
\text{access-profile name;} \\
\text{local-name name;} \\
\text{passive;} \\
\text{}} \\
\text{t3-options {}} \\
\text{bert-algorithm algorithm;} \\
\text{bert-error-rate rate;} \\
\text{bert-period seconds;} \\
\text{(cbit-parity | no-cbit-parity);} \\
\text{compatibility-mode (adtran | digital-link | kentrox | larscom | verilink) <subrate value>;} \\
\text{fcs (32 | 16);} \\
\text{(feac-loop-respond | no-feac-loop-respond);} \\
\text{idle-cycle-flag value;} \\
\text{(long-buildout | no-long-buildout);} \\
\text{loopback (local | remote);} \\
\text{(payload-scrambler | no-payload-scrambler);} \\
\text{start-end-flag (shared | filler);} \\
\text{}} \\
\text{unit logical-unit-number {}} \\
\text{logical-interface-statements;} \\
\end{align*}
\]

For more information about specific parameters, see “Configure Physical Interface Properties” on page 39 and “Configure T3 Interfaces” on page 395.
Configure Channelized OC-12 QPP Interface Properties

Specify Options at the T1 QPP Interface Level

To specify options at the T1 interface level, include the following statements at the [edit interfaces t1-fpc/pic/port<:channel>] hierarchy level:

```
[edit interfaces t1-fpc/pic/port<:channel>]
clocking clock-source;
dce;
disable;
description text;
encapsulation type;
hold-time up milliseconds down milliseconds;
keepalives <interval seconds> <down-count number> <up-count number>;
lmi {
    lmi-type (ansi | itu);
    n391dte number;
    n392dce number;
    n392dte number;
    n393dce number;
    n393dte number;
    t391dte seconds;
    t392dce seconds;
}
mtu bytes;
no-keepalives;
ppp-options {
    chap {
        access-profile name;
        local-name name;
        passive;
    }
}
t1-options {
    bert-algorithm algorithm;
    bert-error-rate rate;
    bert-period seconds;
    byte-encoding (nx64 | nx56);
    fcs (32 | 16);
    framing (esf | sf);
    idle-cycle-flag (flags | ones);
    invert-data;
    line-encoding (ami | b8zs);
    loopback (local | payload | remote);
    start-end-flag (shared | filler);
    remote-loopback-respond;
    timeslots time-slot-range;
}
traceoptions {
    flag flag <flag-modifier> <disable>;
}
(traps | no-traps);
unit logical-unit-number {
    logical-interface-statements;
}
```

For more information about specific parameters, see “Configure Physical Interface Properties” on page 39 and “Configure T1 Interfaces” on page 387.
Specify Options at the NxDS-0 QPP Interface Level

To specify options at the NxDS-0 interface level, include the following statements at the [edit interfaces ds-fpc/ pic/ port<:channel>] hierarchy level:

```
[edit interfaces ds-fpc/ pic/ port<:channel>]
accounting-profile name;
dce;
disable;
description text;
ds0-options {
    bert-algorithm algorithm;
    bert-error-rate rate;
    bert-period seconds;
    byte-encoding (nx64 | nx56);
    fcs (32 | 16);
    idle-cycle-flag (flags | ones);
    invert-data;
    loopback (payload | remote);
    start-end-flag (shared | filler);
}
encapsulation type;
hold-time up milliseconds down milliseconds;
keepalives <down-count number> <interval seconds> <up-count number>;
lmi {
    lmi-type (ansi | itu);
    n391dte number;
    n392dce number;
    n392dte number;
    n393dce number;
    n393dte number;
    t391dte seconds;
    t392dce seconds;
}
mtu bytes;
noc-keepalives;
ppp-options {
    chap {
        access-profile name;
        local-name name;
        passive;
    }
}
traceoptions {
    flag flag <flag-modifier> <disable>;
}
(traps | no-traps);
unit {
    logical-interface-statements;
}
```

For more information about specific parameters, see “Configure Physical Interface Properties” on page 39.
Configure Channelized OC-12 Interfaces

On Channelized OC-12 PICs, you can configure 12 T3 channels per port. To configure Channelized OC-12 interface properties, you can include the `sonet-options` and `t3-options` statements at the `[edit interfaces interface-name]` hierarchy level. Some SONET options are ignored, and some can only be configured for channel 0, though they apply equally to all channels. The `long-buildout` statement under `t3-options` is also ignored.

For T3 channels on a Channelized OC-12 interface, the `clocking` statement is supported only for channel 0; it is ignored if included in the configuration of channels 1 through 11. The clock source configured for channel 0 applies to all channels on the Channelized OC-12 interface. The individual T3 channels use a gapped 45-MHz clock as the transmit clock. When you configure the clock source for a channelized interface—`ds-x/y/z:0`, for example—you must also include the `channel-group` statement at the `[edit chassis]` hierarchy level, and specify channel group 0. For more information, see “Clock Sources on Channelized Interfaces” on page 166.

For more information, see “Configure SONET/SDH Interfaces” on page 359, and “Configure T3 Interfaces” on page 395. For a configuration example, see “Configure Aggregated SONET/SDH Interfaces” on page 380.

Table 19 summarizes the OC-12 to DS-3 numbering scheme.

<table>
<thead>
<tr>
<th>Two-Level STS-1 Number (STS-3,STS-1)</th>
<th>One-Level STS Number</th>
<th>OC-12 to DS-3 PIC DS-3 Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>1,1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>1,2</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>1,3</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>2,1</td>
<td>4</td>
<td>3</td>
</tr>
<tr>
<td>2,2</td>
<td>5</td>
<td>4</td>
</tr>
<tr>
<td>2,3</td>
<td>6</td>
<td>5</td>
</tr>
<tr>
<td>3,1</td>
<td>7</td>
<td>6</td>
</tr>
<tr>
<td>3,2</td>
<td>8</td>
<td>7</td>
</tr>
<tr>
<td>3,3</td>
<td>9</td>
<td>8</td>
</tr>
<tr>
<td>4,1</td>
<td>10</td>
<td>9</td>
</tr>
<tr>
<td>4,2</td>
<td>11</td>
<td>10</td>
</tr>
<tr>
<td>4,3</td>
<td>12</td>
<td>11</td>
</tr>
</tbody>
</table>
Example: Configure Channelized OC-12 QPP Interfaces

In Figure 16, a Channelized OC-12 PIC with QPP is partitioned into multiple OC slices.

Figure 16: Sample Channelization of OC-12 PIC with QPP

**Bold** entries correspond to actual packet channels.

Figure 16 shows the following OC slices:

- **a.** An OC-3 interface.
- **b.** Another OC-3 interface.
- **c.** A Channelized OC-1 partitioned into T1 interfaces.
- **d.** A Channelized OC-1 converted into a T3 interface.
- **e.** A Channelized OC-1 partitioned into T1 interfaces and Channelized T1s, which are partitioned into NxDS-0 interfaces.
- **f.** A Channelized OC-1 converted into a Channelized T3, which is partitioned into T1 interfaces.
- **g.** A Channelized OC-1 converted into a Channelized T3, which is partitioned into T1 interfaces and a Channelized T1, which is partitioned into NxDS-0 interfaces.
- **h.** A Channelized OC-1 partitioned into Channelized T1s, which are partitioned into NxDS-0 interfaces.
The following example shows how to configure cases (a) through (h):

```
[edit interfaces]
oc12-1/1/0 {
    sonet-options {
        sonet-options-statements;
    }
    partition 1 oc-slice 1-3 interface-type so; # (a) so-1/1/0:1.
    partition 2 oc-slice 4-6 interface-type so; # (b) so-1/1/0:2
    partition 3 oc-slice 7 interface-type coc1; # (c) coc1-1/1/0:3
    partition 4 oc-slice 8 interface-type coc1; # (d) coc1-1/1/0:4
    partition 5 oc-slice 9 interface-type coc1; # (e) coc1/1/0:5
    partition 6 oc-slice 10 interface-type coc1; # (f) coc1-1/1/0:6
    partition 7 oc-slice 11 interface-type coc1; # (g) coc1-1/1/0:7
    partition 8 oc-slice 12 interface-type coc1; # (h) coc1-1/1/0:8
}

so-1/1/0:1 {
    description "(a) oc-slice 1-3 of coc12-1/1/0. COC12 > OC3.;"
    sonet-options {
        sonet-options-statements;
    }
}

so-1/1/0:2 {
    description "(b) oc-slice 4-6 of coc12-1/1/0. COC12 > OC3.;"
    sonet-options {
        sonet-options-statements;
    }
}

coc1-1/1/0:3 {
    description "(c) oc-slice 7 of coc12-1/1/0. COC12 to COC-1 VT-mapped to T1s.;"
    sonet-options {
        sonet-options-statements;
    }
    partition 1 - 10 interface-type t1; # t1-1/1/0:[1-10]
}

t1-1/1/0:3:1 {
    description "(c) oc-slice 7 of coc12-1/1/0. T1 interface config.;"
    t1-options {
        t1-options-statements;
    }
}
...

coc1-1/1/0:4 {
    description "(d) oc-slice 8 of coc12-1/1/0. COC12 to COC-1 converted to a T3.;"
    sonet-options {
        sonet-options-statements;
    }
    no-partition interface-type t3; # t3-1/1/0:4
}

t3-1/1/0:4 {
    description "(d) oc-slice 8 of coc12-1/1/0. T3 interface config.;"
}
```
Configure Channelized OC-12 Interfaces

Example: Configure Channelized OC-12 QPP Interfaces

coc1-1/1/0:5 {
  description "(e) oc-slice 9 of coc12-1/1/0. COC12 to COC-1 VT-mapped to T1s.";
  sonet-options {
    sonet-options-statements;
  }
  partition 1 - 3 interface-type t1; # t1-1/1/0:5:1
  partition 4 interface-type ct1; # ct1-1/1/0:5:4
}

t1-1/1/0:5:1 {
  description "(e) oc-slice 9 of coc12-1/1/0. T1 interface config.";
  t1-options {
    t1-options-statements;
  }
}

... ct1-1/1/0:5:4 {
  description "(e) oc-slice 9 of coc12-1/1/0. CT1 to NxDS-Os.";
  t1-options {
    t1-options-statements;
  }
  partition 1 timeslots 0 - 10 interface-type ds0; # ds-1/1/0:5:4:1
  partition 2 timeslots 11- 23 interface-type ds0; # ds-1/1/0:5:4:2
  ...
}

coc1-1/1/0:6 {
  description "(f) oc-slice 10 of coc12-1/1/0. COC12 to COC-1 converted to a CT3 to T1s.";
  sonet-options {
    sonet-options-statements;
  }
  no-partition interface-type ct3; # ct3-1/1/0:6
}

coc3-1/1/0:6 {
  description "(f) COC12 to CT3 M-13 and C-bit parity-mapped to T1s.";
  sonet-options {
    sonet-options-statements;
  }
  partition 1 - 10 interface-type t1; # t1-1/1/0:6:[1-10]
}

t1-1/1/0:6:1 {
  description "(f) T1 interface config.";
  t1-options {
    t1-options-statements;
  }
}

... coc1-1/1/0:7 {
  description "(g) oc-slice 11 of coc12-1/1/0. COC12 to COC-1 converted to a CT3 to T1s
  and CT1 to NxDS-Os.";
  sonet-options {
    sonet-options-statements;
  }
  no-partition interface-type ct3; # ct3-1/1/0:7
}
Example: Configure Channelized OC-12 QPP Interfaces

c3t-1/1/0:7 {
    description "(g) COC12 to CT3 M-13 and C-bit parity-mapped to T1s and CT1."
    sonet-options {
        sonet-options-statements;
    }
    partition 1 - 10 interface-type t1; # t1-1/1/0:7:[1-10]
    partition 2 interface-type ct1; # ct1-1/1/0:7:11
}
t1-1/1/0:7:1 {
    description "(g) T1 interface config."
    t1-options {
        t1-options-statements;
    }
}
...
ct1-1/1/0:7:11 {
    description "(g) CT1 to NxDS-Os."
    t1-options {
        t1-options-statements;
    }
    partition 1 timeslots 0 - 10 interface-type ds0; # ds-1/1/0:7:11:1
    partition 2 timeslots 11- 23 interface-type ds0; # ds-1/1/0:7:11:2
    ...
}
oc1-1/1/0:8 {
    description "(h) oc-slice 12 of coc12-1/1/0. COC12 to COC-1 VT-mapped to CT1 to 
NxDS-Os."
    sonet-options {
        sonet-options-statements;
    }
    partition 1 interface-type t1; # ct1-1/1/0:8:1
}
c1t1-1/1/0:8:1 {
    description "(h) CT1 to NxDS-Os."
    t1-options {
        t1-options-statements;
    }
    partition 1 timeslots 0 - 10 interface-type ds0; # ds-1/1/0:8:1:1
    partition 2 timeslots 11- 23 interface-type ds0; # ds-1/1/0:8:1:2
    ...
}
Example: Configure Channelized OC-12 Interfaces

The following configuration is sufficient to get the Channelized OC-12 interface up and running. The OC-12 interface can be divided into 12 channels. DS-3 channels can use the following encapsulation types:

- PPP, PPP CCC, and PPP TCC
- Frame Relay, Frame Relay CCC, and Frame Relay TCC
- Cisco HDLC, Cisco HDLC CCC, and Cisco HDLC TCC

The channels can also have logical interfaces.

```
[edit interfaces]
t3-fpc/pic/port:0 {
  encapsulation cisco-hdlc;
  t3-options {
    compatibility-mode larscom;
    payload-scrambler;
  }
  unit 0 {
    family inet {
      address 10.11.30.1/30;
    }
    family iso;
  }
}
t3-fpc/pic/port:1 {
  encapsulation ppp;
  t3-options {
    compatibility-mode larscom;
    payload-scrambler;
  }
  unit 0 {
    family inet {
      address 10.11.30.5/30;
    }
    family iso;
  }
}
t3-fpc/pic/port:2 {
  encapsulation frame-relay;
  t3-options {
    compatibility-mode larscom;
    payload-scrambler;
  }
  unit 0 {
    dlci 100;
    family inet {
      address 10.11.30.9/30;
    }
    family iso;
  }
```
```
unit 1 {
    dlci 101;
    family inet {
        address 10.11.31.9/30;
    }
    family iso;
}

t3-fpc/pic/port:3 {
    encapsulation cisco-hdlc-ccc;
    t3-options {
        compatibility-mode larscom;
        payload-scrambler;
    }
    unit 0;
}

t3-fpc/pic/port:4 {
    encapsulation ppp-ccc;
    t3-options {
        compatibility-mode larscom;
        payload-scrambler;
    }
    unit 0;
}

t3-fpc/pic/port:5 {
    dce;
    encapsulation frame-relay-ccc;
    t3-options {
        compatibility-mode larscom;
        payload-scrambler;
    }
    unit 0 {
        encapsulation frame-relay-ccc;
        dlci 1000;
    }
    unit 1 {
        encapsulation frame-relay-ccc;
        dlci 1001;
    }
}
```
Chapter 15
Configure Channelized STM-1 Interfaces

Each Channelized STM-1 PIC and Channelized STM-1 PIC with QPP has one STM-1 port. For both PIC types, you can configure up to 63 E1 channels.

For the Channelized STM-1 PIC with QPP, you can channelize the single port to the NxDS-0 level. Each E1 interface has 32 time slots (DS-0), in which time slot 0 is reserved. You can combine one or more of these DS-0 time slots (channels) to create a channel group (NxDS-0).

This chapter is organized as follows:
- Configure Channelized STM-1 QPP Interfaces on page 205
- Configure Channelized STM-1 QPP Interface Properties on page 209
- Configure Channelized STM-1 Interfaces on page 215

For examples of Channelized STM-1 interface configuration, see the following:
- Example: Configure Channelized STM-1 QPP Interfaces on page 214
- Example: Configure Channelized STM-1 Interfaces on page 219

Configure Channelized STM-1 QPP Interfaces

This section includes the following topics:
- Configure an STM-1 QPP Interface on page 206
- Configure E1 QPP Interfaces on page 206
- Configure Fractional E1 QPP Interfaces on page 207
- Configure an NxDS-0 QPP Interface on page 208
- Specify Options at the Channelized STM-1 QPP Level on page 210
- Specify Options at the Channelized AU-4 QPP Level on page 211
- Specify Options at the E1 QPP Interface Level on page 212
- Specify Options at the NxDS-0 QPP Interface Level on page 213
Configure an STM-1 QPP Interface

On a one-port Channelized STM-1 PIC with QPP, you can configure one SONET/SDH STM-1 interface. To configure a SONET/SDH STM-1 interface, include the no-partition interface-type statement at the [edit interfaces cstm1-fpc/pic/port] hierarchy level, specifying the so interface type:

```
[edit interfaces cstm1-fpc/pic/port]
no-partition interface-type so;
```

This configuration creates interface so-fpc/pic/port.

Configure E1 QPP Interfaces

On a Channelized STM-1 PIC with QPP, you can configure up to 63 E1 interfaces. To configure an E1 interface on a Channelized STM-1 PIC with QPP, you must perform the following tasks:

1. Include the no-partition and interface-type statements at the [edit interfaces cstm1-fpc/pic/port] hierarchy level, specifying the cau4 interface type:

   ```
   [edit interfaces cstm1-fpc/pic/port]
   no-partition interface-type cau4;
   ```

   This converts the Channelized STM-1 interface into a Channelized Administrative Unit 4 (AU-4) interface. The resulting interface name is cau4-fpc/pic/port.

2. Partition the Channelized AU-4 interface into E1 interfaces by including the partition and interface-type statements at the [edit interfaces cau4-fpc/pic/port] hierarchy level, specifying the e1 interface type:

   ```
   [edit interfaces cau4-fpc/pic/port]
   partition partition-number interface-type e1;
   ```

   This configuration creates interface e1-fpc/pic/port:channel.

   **Note**

   For Channelized STM-1 interfaces, channel numbering begins with 0 (:0). For Channelized STM-1 QPP interfaces, channel numbering begins with 1 (:1).

   The partition number is the sublevel interface partition index and correlates with the channel number. For Channelized E1 interfaces, the partition number can be in the range 1 through 63.

   The interface type is the channelized interface type or clear channel you are creating. For Channelized AU-4 interfaces, type can be ce1 or e1.
Example: Configure E1 QPP Interfaces

Configure the following five E1 interfaces:

```
e1-0/0/0:1  
e1-0/0/0:2  
e1-0/0/0:3  
e1-0/0/0:4  
e1-0/0/0:5  
```

```
[edit interfaces cstm1-0/0/0]
no-partition interface-type cau4;

[edit interfaces cau4-0/0/0]
partition 1-5 interface-type e1;
```

Configure Fractional E1 QPP Interfaces

On a Channelized STM-1 PIC with QPP, you can configure up to 63 fractional E1 interfaces. To configure a fractional E1 interface on a Channelized STM-1 PIC with QPP, you must perform the following tasks:

1. Include the no-partition and interface-type statements at the [edit interfaces cstm1-fpc/pic/port] hierarchy level, specifying the cau4 interface type:

   ```
   [edit interfaces cstm1-fpc/pic/port]
   no-partition interface-type cau4;
   ```

   This converts the Channelized STM-1 interface into a Channelized AU-4 interface. The resulting interface name is cau4-fpc/pic/port.

2. Partition the Channelized AU-4 interface into E1 interfaces by including the partition and interface-type statements at the [edit interfaces cau4-fpc/pic/port] hierarchy level, specifying the e1 interface type:

   ```
   [edit interfaces cau4-fpc/pic/port]
   partition partition-number interface-type e1;
   ```

   This configuration creates interface e1-fpc/pic/port:channel.

   The partition number is the sublevel interface partition index and correlates with the channel number. For Channelized E1 interfaces, the partition number can be in the range 1 through 63.

   The interface type is the channelized interface type or clear channel you are creating. For Channelized AU-4 interfaces, type can be ce1 or e1.

```
Note
For Channelized STM-1 interfaces, channel numbering begins with 0 (:0). For Channelized STM-1 QPP interfaces, channel numbering begins with 1 (:1).
```
3. Configure the number of time slots allocated to the E1 QPP interface by including the 
timeslots statement at the [edit interfaces e1-fpc/ pic/ port:channel e1-options] hierarchy 
level:

[edit interfaces e1-fpc/ pic/ port:channel e1-options] 
timeslots time-slot-range;

For Channelized E1 QPP interfaces, the time-slot range is 2 through 31. You can 
designate any combination of time slots for usage. The default is to use all the time slots.

For more information about E1 time slots, see “Configure Fractional E1 Time Slots” on 
page 249.

Example: Configure Fractional E1 QPP Interfaces

Configure a fractional E1 interface that uses time slots 2 through 10:

[edit interfaces cstm1-0/ 0/0] 
no-partition interface-type cau4;

[edit interfaces cau4-0/ 0/0] 
partition 1 interface-type e1;

[edit interfaces e1-0/ 0/0 e1-options] 
timeslots 2-10;

Configure an NxDS-0 QPP Interface

On a Channelized STM-1 PIC with QPP, you can configure up to 128 NxDS-0 channels. To 
configure an NxDS-0 QPP interface on a Channelized STM-1 PIC with QPP, you must perform 
the following tasks:

1. Include the partition and interface-type statements at the [edit interfaces 
cstm1-fpc/ pic/ port] hierarchy level, specifying the cau4 interface type:

[edit interfaces cstm1-fpc/ pic/ port] 
no-partition interface-type cau4;

This converts the Channelized STM-1 interface into a Channelized AU-4 interface. The 
resulting interface name is cau4-fpc/ pic/ port.

2. Partition the Channelized AU-4 interface into E1 interfaces by including the partition and 
interface-type statements at the [edit interfaces cau4-fpc/ pic/ port] hierarchy level, 
specifying the ce1 interface type:

[edit interfaces cau4-fpc/ pic/ port] 
partition partition-number interface-type ce1;

This configuration creates interface ce1-fpc/ pic/ port:channel.

The partition number is the sublevel interface partition index and correlates with the 
channel number. For Channelized E1 interfaces, the partition number can be in the 
range 1 through 63.
The interface type is the channelized interface type or clear channel you are creating. For Channelized AU-4 interfaces, type can be ce1 or e1.

For Channelized STM-1 interfaces, channel numbering begins with 0 (:0). For Channelized STM-1 QPP interfaces, channel numbering begins with 1 (:1).

3. Configure the number of time slots allocated to the NxDS-0 QPP interface by including the partition, timeslots, and interface-type statements at the [edit interfaces e1-fpc/pic/port:channel] hierarchy level, specifying the ds interface type:

   [edit interfaces ce1-fpc/pic/port:channel]
   partition partition-number timeslots time-slot-range interface-type ds;

For Channelized E1 QPP interfaces, the partition number range is 1 through 31; the time-slot range is 2 through 31. You can designate any combination of time slots for usage. The default is to use all the time slots.

For more information about E1 time slots, see “Configure Fractional E1 Time Slots” on page 249.

Example: Configure an NxDS-0 QPP Interface

Configure an NxDS-0 interface that uses time slots 2 through 10. This configuration creates the ds-0/0/0:1:1 interface.

   [edit interfaces cstm1-0/0/0]
   no-partition interface-type cau4;

   [edit interfaces cau4-0/0/0]
   partition 1 interface-type ce1;

   [edit interfaces ce1-0/0/0:1]
   partition 1 timeslots 2-10 interface-type ds;

Configure Channelized STM-1 QPP Interface Properties

This section lists the interface properties that are valid at each channel level on a Channelized STM-1 QPP interface, discussing the following topics:

- Specify Options at the Channelized STM-1 QPP Level on page 210
- Specify Options at the Channelized AU-4 QPP Level on page 211
- Specify Options at the E1 QPP Interface Level on page 212
- Specify Options at the NxDS-0 QPP Interface Level on page 213

For more information, see “Channelized QPP Interface Properties” on page 169.
Specify Options at the Channelized STM-1 QPP Level

To specify options at the Channelized STM-1 interface level, include the following statements at the [edit interfaces stm1-fpc/pic/port] hierarchy level:

```plaintext
[edit interfaces stm1-fpc/pic/port]
clocking clock-source;
description text;
disable;
no-partition interface-type type;
partition partition-number interface-type type;
sonet-options {
  aps {
    advertise-interval milliseconds;
    authentication-key key;
    force;
    hold-time milliseconds;
    lockout;
    neighbor address;
    paired-group group-name;
    protect-circuit group-name;
    request;
    revert-time seconds;
    working-circuit group-name;
  }
  bytes {
    e1-quiet value;
    f1 value;
    f2 value;
    s1 value;
    z3 value;
    z4 value;
  }
  loopback (local | remote);
  (z0-increment | no-z0-increment);
}
traceoptions {
  flag flag <flag-modifier> <disable>;
}
```

For more information about specific parameters, see “Configure Physical Interface Properties” on page 39 and “Configure SONET/SDH Interfaces” on page 359.
Specify Options at the Channelized AU-4 QPP Level

To specify options at the Channelized AU-4 QPP interface level, include the following statements at the [edit interfaces cau4-fpc/ pic/ port] hierarchy level:

```
[edit interfaces cau4-fpc/ pic/ port]
  clocking clock-source;
  description text;
  disable;
  partition partition-number interface-type type;
  sonet-options {
    bytes {
      f2 value;
      z3 value;
      z4 value;
    }
    loopback (local | remote);
    path-trace trace-string;
  }
  traceoptions {
    flag flag <flag-modifier> <disable>;
  }
```

For more information about specific parameters, see “Configure Physical Interface Properties” on page 39 and “Configure SONET/SDH Interfaces” on page 359.

Configure Virtual Tributary Mapping of Channelized STM-1 QPP Interface

You can configure virtual tributary mapping to use KLM mode or ITU-T mode. By default, virtual tributary mapping uses KLM mode.

For the Channelized STM-1 PIC with QPP, you can configure virtual tributary mapping by including the vtmapping statement at the [edit interfaces cau4-fpc/ pic/ port sonet-options] hierarchy level:

```
[edit interfaces cau4-fpc/ pic/ port sonet-options]
  vtmapping (klm | itu-t);
```

For the KLM mappings used by Channelized STM-1 to E1 PIC interfaces, see Table 20 on page 217.
Specify Options at the E1 QPP Interface Level

To specify options at the E1 interface level, include the following statements at the [edit interfaces e1-fpc/pic/port:channel] hierarchy level:

```plaintext
[edit interfaces e1-fpc/pic/port:channel]
clocking clock-source;
dce;
disable;
description text;
e1-options {
    bert-algorithm algorithm;
    bert-error-rate rate;
    bert-period seconds;
    byte-encoding (nx64 | nx56);
    fcs (32 | 16);
    framing (g704 | g704-no-crc4 | unframed);
    idle-cycle-flag (flags | ones);
    loopback (local | remote);
    start-end-flag (shared | filler);
    timeslots time-slot-range;
}
capsulation type;
hold-time up milliseconds down milliseconds;
keepalives <interval seconds> <down-count number> <up-count number>;
lmi {
    lmi-type (ansi | itu);
    n391dte number;
    n392dce number;
    n392dte number;
    n393dce number;
    n393dte number;
    t391dte seconds;
    t392dce seconds;
}
mtu bytes;
no-keepalives;
ppp-options {
    chap {
        access-profile name;
        local-name name;
        passive;
    }
}
traceoptions {
    flag flag <flag-modifier> <disable>;
}
(traps | no-traps);
unit logical-unit-number {
    logical-interface-statements;
}
```

For more information about specific parameters, see “Configure Physical Interface Properties” on page 39 and “Configure E1 Interfaces” on page 243.
Specify Options at the NxDS-0 QPP Interface Level

To specify options at the NxDS-0 interface level, include the following statements at the [edit interfaces ds-fpc/pic/port<channel>] hierarchy level:

[edit interfaces ds-fpc/pic/port<channel>]
accounting-profile name;
dce;
disable;
description text;
ds0-options {
  bert-algorithm algorithm;
  bert-error-rate rate;
  bert-period seconds;
  byte-encoding (nx64 | nx56);
  fcs (32 | 16);
  idle-cycle-flag (flags | ones);
  invert-data;
  loopback (payload | remote);
  start-end-flag (shared | filler);
}
encapsulation type;
hold-time up milliseconds down milliseconds;
keepalives <down-count number> <interval seconds> <up-count number>;
lmi {
  lmi-type (ansi | itu);
  n391dte number;
  n392dce number;
  n392dte number;
  n393dce number;
  n393dte number;
  t391dte seconds;
  t392dce seconds;
}
mtu bytes;
nokkeepalives;
ppp-options {
  chap {
    access-profile name;
    local-name name;
    passive;
  }
}
traceoptions {
  flag flag <flag-modifier> <disable>;
}
(traps | no-traps)
unit {
  logical-interface-statements;
}

For more information about specific parameters, see “Configure Physical Interface Properties” on page 39.
Example: Configure Channelized STM-1 QPP Interfaces

Configure STM-1, E1, fractional E1, and NxDSD-0 interfaces:

STM-1 interface
[edit interfaces]
cstm1-0/0/0 {
    no-partition interface-type so;
}
so-0/0/0 {
    unit 0 {
        family inet {
            address 10.10.12.1/30;
        }
    }
}

E1 interface
[edit interfaces]
cstm1-1/1/0 {
    no-partition interface-type cau4;
}
[edit interfaces]
cau4-1/1/0 {
    partition 1-63 interface-type e1;
}
[edit interfaces]
e1-1/1/0:1 {
    unit 0 {
        family inet {
            address 10.10.10.1/30;
        }
    }
}

Fractional E1 interface
[edit interfaces]
cstm1-1/0/0 {
    no-partition interface-type cau4;
}
[edit interfaces]
cau4-1/0/0 {
    partition 1-63 interface-type e1;
}
[edit interfaces]
e1-1/1/0:1 {
    e1-options {
        timeslots 2-10;
    }
    unit 0 {
        family inet {
            address 10.10.10.1/30;
        }
    }
}
DS-0 interface

[edit interfaces]
cstm1-2/0/0 {  
    no-partition interface-type cau4;
}

[edit interfaces]
cau4-2/0/0 {  
    partition 1-10 interface-type ce1;
}

[edit interfaces]
ce1-2/0/0:1 {  
    partition 1 interface-type ds timeslots 2-10
}

[edit interfaces]
ds-2/0/0:1:1 {  
    unit 0 {  
        family inet {  
            address 12.12.12.1/30;
        }
    }
}
...

Configure Channelized STM-1 Interfaces

You can configure up to 63 E1 channels per single-port Channelized STM-1 to E1 PIC. To specify the channel number, include it after the colon (:) in the interface name. For example, a Channelized STM-1 to E1 PIC in FPC 1 and slot 1 will have the following physical interface, depending on the media type:

e1-1/1/0:x

The E1 channel number can be from 0 through 62.

This section is organized as follows:

- Configure Channelized STM-1 Interface Properties on page 216
- Configure Virtual Tributary Mapping of Channelized STM-1 Interface on page 217
- Example: Configure Channelized STM-1 Interfaces on page 219
Configure Channelized STM-1 Interface Properties

To configure the interface properties for Channelized STM-1 to E1 PICs, you include the `e1-options` and `sonet-options` statements for both sides of the connection. The following configurations list all the valid statements.

To specify options for each of the E1 channels on the Channelized STM-1 to E1 PIC, include the `e1-options` statement at the `[edit interfaces interface-name] hierarchy level:

```
[edit interfaces interface-name]
e1-options {
    bert-error-rate;
    bert-period;
    fcs (32 | 16);
    framing (g704 | g704-no-crc4 | unframed);
    idle-cycle-flag (flags | ones);
    loopback (local | remote);
    start-end-flag (shared | filler);
    timeslots time-slot-number;
}
```

When a channelized STM-1 interface experiences a line transition, the E1 channels configured in unframed mode log a large number of drops (around 24,000) as the channelized STM-1 interface clocks resynchronize. This does not occur on framed channels, because the framing resynchronizes clocks very quickly.

To specify options for the SONET/SDH side of the connection, include the `sonet-options` statement at the `[edit interfaces interface-name] hierarchy level:

```
[edit interfaces interface-name]
sonet-options {
    bytes {
        e1-quiet value;
        f1 value;
        f2 value;
        s1 value;
        z3 value;
        z4 value;
    }
    loopback (local | remote);
}
```

On Channelized STM-1 interfaces, you should configure the clock source on one side of the connection to be internal (the default JUNOS configuration) and on the other side of the connection to be external.
By default, Channelized T3 and STM-1 interfaces can support a maximum of 64 Frame Relay data-link connection identifiers (DLCIs), numbered 0 through 63, per channel. In DLCI sparse mode, Channelized T3 and STM-1 interfaces support a maximum of three DLCIs, numbered 0 through 1,022, per channel. DLCI 0 is reserved for LMI. You configure the router to use DLCI sparse mode by including the sparse-dlcis statement at the [edit chassis fpc slot-number pic pic-number] hierarchy level. Channelized T3 QPP interfaces support a maximum of 64 DLCIs, numbered 0 through 1,022, and, therefore, do not require sparse mode. For more information about Frame Relay DLCIs, see “Configure a Point-to-Point Frame Relay Connection” on page 309. For more information about DLCI sparse mode, see the JUNOS Internet Software Configuration Guide: Getting Started.

For more information about specific statements, see “Configure E1 Interfaces” on page 243, “Configure SONET/SDH Interfaces” on page 359, and “Configure T1 Interfaces” on page 387. For a configuration example, see “Example: Configure Channelized STM-1 Interfaces” on page 219.

### Configure Virtual Tributary Mapping of Channelized STM-1 Interface

You can configure virtual tributary mapping to use KLM mode or ITU-T mode. To configure virtual tributary mapping, include the vtmapping statement at the [edit chassis fpc slot-number pic pic-number] hierarchy level:

```
[edit chassis fpc slot-number pic pic-number]
vtmapping (klm | itu-t);
```

By default, virtual tributary mapping uses KLM mode. For more information, see the JUNOS Internet Software Configuration Guide: Getting Started.

For the Channelized STM-1 PIC with QPP, you can configure virtual tributary mapping by including the vtmapping statement at the [edit interfaces cau4-fpc/pic/port sonet-options] hierarchy level:

```
[edit interfaces cau4-fpc/pic/port sonet-options]
vtmapping (klm | itu-t);
```

Table 20 lists the KLM mappings used by the Channelized STM-1 to E1 PIC interfaces. The PIC defaults to KLM numbering with an offset of -1; for example, KLM 1 = STM-1 PIC 0.

### Table 20: Channelized STM-1 to E1 Channel Mapping

<table>
<thead>
<tr>
<th>Channel Number</th>
<th>KLM Number</th>
<th>Tributary Unit Group 3</th>
<th>Tributary Unit Group 2</th>
<th>Virtual Tributary</th>
<th>ITU-T Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>22</td>
</tr>
<tr>
<td>2</td>
<td>3</td>
<td>1</td>
<td>1</td>
<td>3</td>
<td>43</td>
</tr>
<tr>
<td>3</td>
<td>4</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>4</td>
<td>5</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>25</td>
</tr>
<tr>
<td>5</td>
<td>6</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>46</td>
</tr>
<tr>
<td>6</td>
<td>7</td>
<td>1</td>
<td>3</td>
<td>1</td>
<td>7</td>
</tr>
<tr>
<td>7</td>
<td>8</td>
<td>1</td>
<td>3</td>
<td>2</td>
<td>28</td>
</tr>
</tbody>
</table>
Configure Channelized STM-1 Interfaces

<table>
<thead>
<tr>
<th>Channel Number</th>
<th>KLM Number</th>
<th>Tributary Unit Group 3</th>
<th>Tributary Unit Group 2</th>
<th>Virtual Tributary</th>
<th>ITU-T Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>9</td>
<td>1</td>
<td>3</td>
<td>3</td>
<td>49</td>
</tr>
<tr>
<td>9</td>
<td>10</td>
<td>1</td>
<td>4</td>
<td>1</td>
<td>10</td>
</tr>
<tr>
<td>10</td>
<td>11</td>
<td>1</td>
<td>4</td>
<td>2</td>
<td>31</td>
</tr>
<tr>
<td>11</td>
<td>12</td>
<td>1</td>
<td>4</td>
<td>3</td>
<td>52</td>
</tr>
<tr>
<td>12</td>
<td>13</td>
<td>1</td>
<td>5</td>
<td>1</td>
<td>13</td>
</tr>
<tr>
<td>13</td>
<td>14</td>
<td>1</td>
<td>5</td>
<td>2</td>
<td>34</td>
</tr>
<tr>
<td>14</td>
<td>15</td>
<td>1</td>
<td>5</td>
<td>3</td>
<td>55</td>
</tr>
<tr>
<td>15</td>
<td>16</td>
<td>1</td>
<td>6</td>
<td>1</td>
<td>16</td>
</tr>
<tr>
<td>16</td>
<td>17</td>
<td>1</td>
<td>6</td>
<td>2</td>
<td>37</td>
</tr>
<tr>
<td>17</td>
<td>18</td>
<td>1</td>
<td>6</td>
<td>3</td>
<td>58</td>
</tr>
<tr>
<td>18</td>
<td>19</td>
<td>1</td>
<td>7</td>
<td>1</td>
<td>19</td>
</tr>
<tr>
<td>19</td>
<td>20</td>
<td>1</td>
<td>7</td>
<td>2</td>
<td>40</td>
</tr>
<tr>
<td>20</td>
<td>21</td>
<td>1</td>
<td>7</td>
<td>3</td>
<td>61</td>
</tr>
<tr>
<td>21</td>
<td>22</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>22</td>
<td>23</td>
<td>2</td>
<td>1</td>
<td>2</td>
<td>23</td>
</tr>
<tr>
<td>23</td>
<td>24</td>
<td>2</td>
<td>1</td>
<td>3</td>
<td>44</td>
</tr>
<tr>
<td>24</td>
<td>25</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>5</td>
</tr>
<tr>
<td>25</td>
<td>26</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>26</td>
</tr>
<tr>
<td>26</td>
<td>27</td>
<td>2</td>
<td>2</td>
<td>3</td>
<td>47</td>
</tr>
<tr>
<td>27</td>
<td>28</td>
<td>2</td>
<td>3</td>
<td>1</td>
<td>8</td>
</tr>
<tr>
<td>28</td>
<td>29</td>
<td>2</td>
<td>3</td>
<td>2</td>
<td>29</td>
</tr>
<tr>
<td>29</td>
<td>30</td>
<td>2</td>
<td>3</td>
<td>3</td>
<td>50</td>
</tr>
<tr>
<td>30</td>
<td>31</td>
<td>2</td>
<td>4</td>
<td>1</td>
<td>11</td>
</tr>
<tr>
<td>31</td>
<td>32</td>
<td>2</td>
<td>4</td>
<td>2</td>
<td>32</td>
</tr>
<tr>
<td>32</td>
<td>33</td>
<td>2</td>
<td>4</td>
<td>3</td>
<td>53</td>
</tr>
<tr>
<td>33</td>
<td>34</td>
<td>2</td>
<td>5</td>
<td>1</td>
<td>14</td>
</tr>
<tr>
<td>34</td>
<td>35</td>
<td>2</td>
<td>5</td>
<td>2</td>
<td>35</td>
</tr>
<tr>
<td>35</td>
<td>36</td>
<td>2</td>
<td>5</td>
<td>3</td>
<td>56</td>
</tr>
<tr>
<td>36</td>
<td>37</td>
<td>2</td>
<td>6</td>
<td>1</td>
<td>17</td>
</tr>
<tr>
<td>37</td>
<td>38</td>
<td>2</td>
<td>6</td>
<td>2</td>
<td>38</td>
</tr>
<tr>
<td>38</td>
<td>39</td>
<td>2</td>
<td>6</td>
<td>3</td>
<td>59</td>
</tr>
<tr>
<td>39</td>
<td>40</td>
<td>2</td>
<td>7</td>
<td>1</td>
<td>20</td>
</tr>
<tr>
<td>40</td>
<td>41</td>
<td>2</td>
<td>7</td>
<td>2</td>
<td>41</td>
</tr>
<tr>
<td>41</td>
<td>42</td>
<td>2</td>
<td>7</td>
<td>3</td>
<td>62</td>
</tr>
<tr>
<td>42</td>
<td>43</td>
<td>3</td>
<td>1</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>43</td>
<td>44</td>
<td>3</td>
<td>1</td>
<td>2</td>
<td>24</td>
</tr>
<tr>
<td>44</td>
<td>45</td>
<td>3</td>
<td>1</td>
<td>3</td>
<td>45</td>
</tr>
<tr>
<td>45</td>
<td>46</td>
<td>3</td>
<td>2</td>
<td>1</td>
<td>6</td>
</tr>
<tr>
<td>46</td>
<td>47</td>
<td>3</td>
<td>2</td>
<td>2</td>
<td>27</td>
</tr>
</tbody>
</table>
Example: Configure Channelized STM-1 Interfaces

The following configuration is sufficient to get the Channelized STM-1 to E1 PIC interface up and running. The Channelized STM-1 to E1 interface is an STM-1 that is divided into 63 E1 interfaces. E1 interfaces can use the following encapsulation types:

- PPP, PPP CCC, and PPP TCC
- Frame Relay, Frame Relay CCC, and Frame Relay TCC
- Cisco HDLC, Cisco HDLC CCC, and Cisco HDLC TCC

The channels can also have logical interfaces. By default, Channelized T3 and STM-1 interfaces can support a maximum of 64 Frame Relay data-link connection identifiers (DLCIs), numbered 0 through 63, per channel. In DLCI sparse mode, Channelized T3 and STM-1 interfaces support a maximum of three DLCIs, numbered 0 through 1,022, per channel. DLCI 0 is reserved for LMI. You configure the router to use DLCI sparse mode by including the sparse-dlcs statement at the [edit chassis fpc slot-number pic [pic-number]] hierarchy level. Channelized T3 QPP interfaces support a maximum of 64 DLCIs, numbered 0 through 1,022, and, therefore, do not require sparse mode. For more information about Frame Relay DLCIs, see “Configure a Point-to-Point Frame Relay Connection” on page 309. For more information about DLCI sparse mode, see the JUNOS Internet Software Configuration Guide: Getting Started.
Configure Channelized STM-1 Interfaces

You apply all STM-1 interface SONET/SDH options to the first E1 interface in the configuration by including the sonet-options statement at the [edit interfaces e1-fpc/pic/port:channel] hierarchy level:

```
[edit]
interfaces {
    e1-fpc/pic/port:0 {
        encapsulation cisco-hdlc;
        sonet-options {
            no-z0-increment;
        }
        e1-options {
            framing g704;
        }
        unit 0 {
            family inet {
                address 10.11.30.1/30;
            }
        }
    }
    e1-fpc/pic/port:1 {
        encapsulation frame-relay;
        e1-options {
            framing g704;
        }
        unit 1 {
            dci 16;
            family inet {
                address 10.11.31.9/30;
            }
        }
    }
    e1-fpc/pic/port:2 {
        encapsulation ppp;
        no-keepalives;
        unit 0 {
            family inet {
                address 10.11.31.47/30;
            }
        }
    }
}
[edit]
chassis {
    fpc 2 {
        pic 0 {
            vtmapping klm;
        }
    }
}
```
Chapter 16
Configure Channelized T3 Interfaces

This chapter is organized as follows:

- Configure Channelized T3 QPP Interfaces on page 221
- Configure Channelized T3 QPP Interface Properties on page 225
- Configure Channelized DS-3 to DS-0 Interfaces on page 229
- Configure Channelized DS-3 to DS-1 Interfaces on page 232

For examples of Channelized T3 interface configuration, see the following sections:

- Example: Configure Channelized T3 QPP Interfaces on page 234
- Examples: Configure Channelized DS-3 to DS-0 Interfaces on page 235
- Examples: Configure Channelized DS-3 to DS-1 Interfaces on page 238

Configure Channelized T3 QPP Interfaces

This section describes how to configure Channelized T3 QPP interfaces, discussing the following topics:

- Configure T3 QPP Interfaces on page 221
- Configure T1 QPP Interfaces on page 222
- Configure Fractional T1 QPP Interfaces on page 223
- Configure an NxDS-0 QPP Interface on page 223

Configure T3 QPP Interfaces

On a four-port Channelized T3 PIC with QPP, you can configure up to four T3 interfaces. To configure an E1 interface, include the no-partition statement at the [edit interfaces ct3-fpc/pic/port] hierarchy level:

    [edit interfaces ct3-fpc/pic/port]
    no-partition;

This configuration creates interface t3-fpc/pic/port.
Configure T1 QPP Interfaces

On a Channelized DS-3 PIC with QPP, you can create up to 112 T1 interfaces. To configure a T1 interface on a Channelized DS-3 PIC with QPP, include the partition and interface-type statements at the [edit interfaces ct3-fpc/ pic/ port] hierarchy level, specifying the t1 interface type:

[edit interfaces ct3-fpc/ pic/ port]
partition partition-number interface-type t1;

This configuration creates interface t1-fpc/ pic/ port:channel.

The partition number is the sublevel interface partition index and correlates with the channel number. For Channelized T3 interfaces, the partition number can be in the range 1 through 28.

```
Note

For Channelized T3 interfaces, channel numbering begins with 0 (:0). For Channelized T3 QPP interfaces, channel numbering begins with 1 (:1).
```

The interface type is the channelized interface type or clear channel you are creating. For Channelized T3 interfaces, type can be ct1 or t1.

Example: Configure T1 QPP Interfaces

Configure the following five T1 interfaces:

```
t1-0/0/0:1
t1-0/0/0:2
t1-0/0/0:3
t1-0/0/0:4
t1-0/0/0:5
```

[edit interfaces ct3-0/0/0]
partition 1-5 interface-type t1;
Configure Fractional T1 QPP Interfaces

On a Channelized DS-3 PIC with QPP, you can configure up to 112 fractional T1 interfaces. To configure a fractional T1 interface on a Channelized DS-3 PIC with QPP, you must perform the following tasks:

1. Configure a T1 QPP interface. For more information, see “Configure T1 QPP Interfaces” on page 222:
   
   This configuration creates interface t1-fpc/pic/port:channel.

2. Configure the number of time slots allocated to the T1 QPP interface by including the timeslots statement at the [edit interfaces t1-fpc/pic/port:channel t1-options] hierarchy level:

   [edit interfaces t1-fpc/pic/port:channel t1-options]
   timeslots time-slot-range;

   For Channelized T1 QPP interfaces, the time-slot range is 1 through 24. The default is to use all the time slots. You can designate any combination of time slots for usage. You can configure a range of values with hyphens, and you can separate multiple values with commas. Do not include spaces when you specify time slot numbers.

   For more information about T1 time slots, see “Configure Fractional T1 Time Slots” on page 394.

Example: Configure Fractional T1 QPP Interfaces

Configure a fractional T1 interface that uses time slots 1 through 10:

```
[edit interfaces ct3-0/0/0:1]
partition 1 interface-type t1;
[edit interfaces t1-0/0/0:1:1 t1-options]
timeslots 1-10;
```

Configure an NxDS-0 QPP Interface

On a Channelized DS-3 PIC with QPP, you can configure up to 128 NxDS-0 channels. To configure an NxDS-0 QPP interface on a Channelized DS-3 PIC with QPP, you must perform the following tasks:

1. Partition the Channelized T3 interface into Channelized T1 interfaces by including the partition and interface-type statements at the [edit interfaces ct3-fpc/pic/port] hierarchy level, specifying the ct1 interface type:

   [edit interfaces ct3-fpc/pic/port]
   partition partition-number interface-type ct1;

   This configuration creates interface ct1-fpc/pic/port:channel.

   The partition number is the sublevel interface partition index and correlates with the channel number. For Channelized T1 interfaces, the partition number can be in the range 1 through 28.
The interface type is the channelized interface type or clear channel you are creating. For Channelized T3 interfaces, type can be ct1 or t1.

For Channelized T3 interfaces, channel numbering begins with 0 (:0). For Channelized T3 QPP interfaces, channel numbering begins with 1 (:1).

2. Configure the number of time slots allocated to the NxDS-0 QPP interface by including the partition, timeslots, and interface-type statements at the [edit interfaces ct1-fpc/ pic/ port:channel] hierarchy level, specifying the ds interface type:

[edit interfaces ct1-fpc/ pic/ port:channel]
partition partition-number timeslots time-slot-range interface-type ds;

For Channelized T1 QPP interfaces, the partition number range is 1 through 28; the time-slot range is 1 through 24. The default is to use all the time slots. You can designate any combination of time slots for usage. You can configure a range of values with hyphens, and you can separate multiple values with commas. Do not include spaces when you specify time slot numbers.

For more information about T1 time slots, see “Configure Fractional T1 Time Slots” on page 394.

Example: Configure an NxDS-0 QPP Interface

Configure the following two NxDS-0 interfaces with 10 time slots and 4 time slots, respectively:

ds-0/0/0:1:1
ds-0/0/0:1:2

[edit interfaces ct3-0/0/0]
partition 1 interface-type ct1;

[edit interfaces ct1-0/0/0:1]
partition 1 timeslots 1-10 interface-type ds;
partition 2 timeslots 12-16 interface-type ds;
Configure Channelized T3 QPP Interface Properties

This section lists the interface properties that are valid at each channel level on a Channelized T3 QPP interface, discussing the following topics:

- Specify Options at the Channelized T3 QPP Level on page 225
- Specify Options at the Channelized T1 QPP Level on page 226
- Specify Options at the T3 QPP Interface Level on page 226
- Specify Options at the T1 QPP Interface Level on page 227
- Specify Options at the NxDS-0 QPP Interface Level on page 228

For more information, see “Channelized QPP Interface Properties” on page 169.

Specify Options at the Channelized T3 QPP Level

To specify options at the Channelized T3 interface level, include the following statements at the [edit interfaces ct3-fpc/pic/port] hierarchy level:

```
[edit interfaces ct3-fpc/pic/port]
clocking clock-source;
disable;
description text;
no-partition;
partition partition-number oc-slice oc-slice-range interface-type type;
t3-options {
  bert-algorithm algorithm;
  bert-error-rate rate;
  bert-period seconds;
  (cbit-parity | no-cbit-parity);
  (feac-loop-respond | no-feac-loop-respond);
  (long-buildout | no-long-buildout);
  loopback (local | payload | remote);
}
traceoptions {
  flag flag <flag-modifier> <disable>;
}
```

For more information about specific parameters, see “Configure Physical Interface Properties” on page 39 and “Configure T3 Interfaces” on page 395.
Specify Options at the Channelized T1 QPP Level

To specify options at the channelized T1 QPP interface level, include the following statements at the [edit interfaces ct1-fpc/pic/port:channel] hierarchy level:

[edit interfaces ct1-fpc/pic/port:channel]
clocking clock-source;
disable;
description text;
partition partition-number oc-slice oc-slice-range interface-type type;
traceoptions {
    flag flag <flag-modifier> <disable>;
}
t1-options {
    bert-algorithm algorithm;
    bert-error-rate rate;
    bert-period seconds;
    framing (esf | sf);
    line-encoding (ami | b8zs);
    loopback (local | remote);
    remote-loopback-respond;
}

For more information about specific parameters, see “Configure Physical Interface Properties” on page 39 and “Configure T3 Interfaces” on page 395.

Specify Options at the T3 QPP Interface Level

To specify options at the T3 interface level, include the following statements at the [edit interfaces t3-fpc/pic/port] hierarchy level:

[edit interfaces t3-fpc/pic/port]
dce;
disable;
description text;
encapsulation type;
hold-time up milliseconds down milliseconds;
keepalives <interval seconds> <down-count number> <up-count number>;
mtu bytes;
no-keepalives;
ppp-options {
    chap {
        access-profile name;
        local-name name;
        passive;
    }
}
t3-options {
    bert-algorithm algorithm;
    bert-error-rate rate;
    bert-period seconds;
    (cbit-parity | no-cbit-parity);
    compatibility-mode (adtran | digital-link | kentrox | larscom | verilink) <subrate value>;
    fcs (32 | 16);
    (feac-loop-respond | no-feac-loop-respond);
    idle-cycle-flag value;
    (long-buildout | no-long-buildout);
    loopback (local | payload | remote);
    (payload-scrambler | no-payload-scrambler);
    start-end-flag (shared | filler);
}
unit logical-unit-number {
    logical-interface-statements;
}

For more information about specific parameters, see “Configure Physical Interface Properties” on page 39 and “Configure T3 Interfaces” on page 395.

Specify Options at the T1 QPP Interface Level

To specify options at the T1 interface level, include the following statements at the [edit interfaces t1-fpc/ pic/ port:channel] hierarchy level:

[edit interfaces t1-fpc/ pic/ port:channel]
clocking clock-source;
dce;
disable;
description text;
encapsulation type;
hold-time up milliseconds down milliseconds;
keepalives <interval seconds> <down-count number> <up-count number>;
lmi {
    lmi-type (ansi | itu);
    n391dte number;
    n392dce number;
    n392dte number;
    n393dce number;
    n393dte number;
    t391dce seconds;
    t392dce seconds;
}
mtu bytes;
no-keepalives;
ppp-options {
    chap {
        access-profile name;
        local-name name;
        passive;
    }
}

Configure Channelized T3 QPP Interface Properties
Configure Channelized T3 QPP Interface Properties

\[\text{t1-options \{}\]
  \hspace{1em} bert-algorithm \text{ algorithm;} \\
  \hspace{1em} bert-error-rate \text{ rate;} \\
  \hspace{1em} bert-period \text{ seconds;} \\
  \hspace{1em} byte-encoding (nx64 | nx56); \\
  \hspace{1em} fcs (32 | 16); \\
  \hspace{1em} framing (esf | sf); \\
  \hspace{1em} idle-cycle-flag (flags | ones); \\
  \hspace{1em} invert-data; \\
  \hspace{1em} line-encoding (ami | b8zs); \\
  \hspace{1em} loopback (local | payload | remote); \\
  \hspace{1em} remote-loopback-respond; \\
  \hspace{1em} start-end-flag (shared | filler); \\
  \hspace{1em} timeslots \text{ time-slot-range;} \\
\]

\[\text{traceoptions \{}\]
  \hspace{1em} flag \text{ flag <flag-modifier> <disable>;} \\
\]

\[\text{(traps | no-traps)}; \]

\[\text{unit logical-unit-number \{}\]
  \hspace{1em} logical-interface-statements; \\
\]

For more information about specific parameters, see “Configure Physical Interface Properties” on page 39 and “Configure T1 Interfaces” on page 387.

Specify Options at the NxDS-0 QPP Interface Level

To specify options at the NxDS-0 interface level, include the following statements at the [edit interfaces ds-fpc/ pic/ port:<channel>] hierarchy level:

\[\text{[edit interfaces ds-fpc/ pic/ port:<channel]>} \]
  \hspace{1em} accounting-profile \text{name;} \\
  \hspace{1em} dce; \\
  \hspace{1em} disable; \\
  \hspace{1em} description \text{ text;} \\
  \hspace{1em} ds0-options \{}\]
    \hspace{1em} bert-algorithm \text{ algorithm;} \\
    \hspace{1em} bert-error-rate \text{ rate;} \\
    \hspace{1em} bert-period \text{ seconds;} \\
    \hspace{1em} byte-encoding (nx64 | nx56); \\
    \hspace{1em} fcs (32 | 16); \\
    \hspace{1em} idle-cycle-flag (flags | ones); \\
    \hspace{1em} invert-data; \\
    \hspace{1em} loopback (payload | remote); \\
    \hspace{1em} remote-loopback-respond; \\
    \hspace{1em} start-end-flag (shared | filler); \\
  \}

\[\text{encapsulation \text{ type;} }\]
  \hspace{1em} hold-time up milliseconds down milliseconds; \\
  \hspace{1em} keepalive <down-count number> <interval seconds> <up-count number>;}
lmi {
    lmi-type (ansi | itu);
    n391dte number;
    n392dce number;
    n392dte number;
    n393dce number;
    n393dte number;
    t391dte seconds;
    t392dce seconds;
}
mtu bytes;
no-keepalives;
ppp-options {
    chap {
        access-profile name;
        local-name name;
        passive;
    }
}
traceoptions {
    flag flag <flag-modifier> <disable>;
}
(traps | no-traps);
unit {
    logical-interface-statements;
}

For more information about specific parameters, see “Configure Physical Interface Properties” on page 39.

Configure Channelized DS-3 to DS-0 Interfaces

For channelized interfaces, you can configure 28 T1 channels per T3 interface. Each T1 link can have up to eight DS-0 channel groups, and each channel group can hold any combination of DS-0 time slots. To specify the T1 link and DS-0 channel group number in the interface name, use colons (:) as separators. For example, a Channelized DS-3 to DS-0 PIC might have the following physical and virtual interfaces:

ds-0/0/0:x:y

x is a T1 link ranging from 0 through 27 and y is a DS-0 channel group ranging from 0 through 7 (see Table 21 on page 230 for more information about ranges).

You can use any of the values within the range available for x and y, and you do not have to configure the links sequentially. In addition, the JUNOS software applies the interface options you configure according to the following rules:

- To configure the T1 options, you must set channel group y to 0; the T1 link x can be any value:

  ds-0/0/0:0:x:0

- To configure the T3 options, you must set the T1 link x to 0 and channel group y to 0:

  ds-0/0/0:0:0:0.
Configure Channelized DS-3 to DS-0 Interfaces

- There are no restrictions on configuring the DS-0 options.
- If you delete a configuration you previously committed for channel group 0, the options return to default values.

To configure the channel groups and time slots for a Channelized DS-3 to DS-0 interface, include the channel-group and timeslots statements at the [edit chassis fpc slot-number pic pic-number ct3 port port-number t1 link-number] hierarchy level:

[edit chassis fpc slot-number pic pic-number ct3 port port-number t1 link-number]
channel-group group-number timeslots time-slot-range;

If you commit the interface name but do not include the [edit chassis] configuration, the Channelized DS-3 to DS-0 PIC behaves like a Channelized DS-3 to DS-1 PIC: none of the DS-0 functionality is accessible.

Table 21 shows the ranges you can specify for each of the elements in the preceding configuration.

Table 21: Ranges for Channelized DS-3 to DS-0 Configuration

<table>
<thead>
<tr>
<th>Item</th>
<th>Option</th>
<th>Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>FPC slot</td>
<td>slot-number</td>
<td>0 through 7 (see note below)</td>
</tr>
<tr>
<td>PIC slot</td>
<td>pic-number</td>
<td>0 through 3</td>
</tr>
<tr>
<td>Port</td>
<td>port-number</td>
<td>0 through 1</td>
</tr>
<tr>
<td>T1 link</td>
<td>link-number</td>
<td>0 through 27</td>
</tr>
<tr>
<td>DS-0 channel group</td>
<td>group-number</td>
<td>0 through 7</td>
</tr>
<tr>
<td>Time slot</td>
<td>time-slot-range</td>
<td>1 through 24</td>
</tr>
</tbody>
</table>

FPC slot range depends on platform. The maximum range of 0 through 7 applies to M40, M40e, M160, T320, and T640 platforms; for M20 routers, the range is 0 through 3; for M10 routers the range is 0 through 1; for M5 routers, the only applicable value is 0.

Bandwidth limitations restrict the interface to a maximum of 128 channel groups per T3 port, rather than the theoretical maximum of 8 * 28 = 224.

There are 24 time slots on a T1 interface. The default is to use all the time slots. You can designate any combination of time slots for usage. You can configure a range of values with hyphens, and you can separate multiple values with commas. Do not include spaces when you specify time slot numbers. You can use each time slot number on only one channel group within the same T1 link.
To use time slots 1 through 10, configure the time-slot range as follows:

```
[edit chassis fpc slot-number pic pic-number ct3 port port-number t1 link-number]
channel-group group-number timeslots 1-10;
```

To use time slots 1 through 5, time slot 10, and time slot 24, configure the time-slot range as follows:

```
[edit chassis fpc slot-number pic pic-number ct3 port port-number t1 link-number]
channel-group group-number timeslots 1,5,10,24;
```

To configure Channelized DS-3 to DS-0 interface properties, you can include the `t3-options`, `t1-options`, or `ds0-options` statements. Only a subset of the T3 options are valid for this configuration, and the `buildout`, `invert-data`, and `line-encoding` statements at the `[edit interfaces interface-name t1-options]` hierarchy level are ignored; likewise, only a subset of the DS-0 options are valid for this configuration, and the `bert-algorithm`, `bert-error-rate`, `bert-period`, and `loopback payload` statements at the `[edit interfaces interface-name ds0-options]` hierarchy level are ignored; the following configurations list all the valid parameters.

The set of options the JUNOS software applies to the interface depends on how you specify the interface name. For more information, see “Examples: Configure Channelized DS-3 to DS-0 Interfaces” on page 235.

To specify options for the T3 side of the connection, include the `t3-options` statement at the `[edit interfaces interface-name]` hierarchy level:

```
[edit interfaces interface-name]
t3-options {
  bert-algorithm algorithm;
  bert-error-rate rate;
  bert-period seconds;
  (cbit-parity | no-cbit-parity);
  (long-buildout | no-long-buildout);
  loopback (local | remote);
}
```

The statements at the `t3-options` hierarchy are supported only for channel 0; they are ignored if configured on other channels. To specify options for each of the T1 channels, include the `t1-options` statement at the `[edit interfaces interface-name]` hierarchy level:

```
[edit interfaces interface-name]
t1-options {
  byte-encoding (nx64 | nx56);
  fcs (32 | 16);
  framing (sf | esf);
  idle-cycle-flag (flags | ones);
  invert-data;
  loopback (local | remote);
  start-end-flag (shared | filler);
  timeslots time-slot-number;
}
```
To specify options for each of the DS-0 channels, include the ds0-options statement at the [edit interfaces interface-name] hierarchy level:

```
[edit interfaces interface-name]
    ds0-options {
        byte-encoding (nx64 | nx56);
        fcs (32 | 16);
        idle-cycle-flag (flags | ones);
        invert-data;
        start-end-flag (shared | filler);
    }
```

For more information about specific parameters, see “Configure E1 Interfaces” on page 243, “Configure E3 Interfaces” on page 251, “Configure T1 Interfaces” on page 387, and “Configure T3 Interfaces” on page 395. For a configuration example, see “Examples: Configure Channelized DS-3 to DS-0 Interfaces” on page 235.

By default, Channelized T3 and STM-1 interfaces can support a maximum of 64 Frame Relay data-link connection identifiers (DLCIs), numbered 0 through 63, per channel. In DLCI sparse mode, Channelized T3 and STM-1 interfaces support a maximum of three DLCIs, numbered 0 through 1,022, per channel. DLCI 0 is reserved for LMI. You configure the router to use DLCI sparse mode by including the sparse-dlcis statement at the [edit chassis fpc slot-number pic pic-number] hierarchy level. Channelized T3 QPP interfaces support a maximum of 64 DLCIs, numbered 0 through 1,022, and, therefore, do not require sparse mode. For more information about Frame Relay DLCIs, see “Configure a Point-to-Point Frame Relay Connection” on page 309. For more information about DLCI sparse mode, see the JUNOS Internet Software Configuration Guide: Getting Started.

Each T1 link can have up to eight DS-0 channel groups, and each channel group can hold any combination of DS-0 time slots.

Configure Channelized DS-3 to DS-1 Interfaces

You can configure 28 T1 channels per T3 interface, and each interface can have logical interfaces. To specify the channel number, include it after the colon (:) in the interface name. For example, a four-port T3 PIC in FPC 1 and slot 1 will have the following physical interfaces, depending on the media type:

```
t1-1/1/0:x
  t1-1/1/1:x
  t1-1/2/1:x
  t1-1/3/1:x
```

x is a channel number ranging from 0 through 27.

To configure Channelized DS-3 to DS-1 interface properties, you can include both the t1-options and t3-options statements. Only a subset of the T3 options is valid for this configuration, and the buildout, invert-data, and line-encoding statements at the [edit interfaces interface-name t1-options] hierarchy level are ignored; likewise, only a subset of the DS-0 options are valid for this configuration, and the bert-algorithm, bert-error-rate, bert-period, and loopback payload statements at the [edit interfaces interface-name ds0-options] hierarchy level are ignored; the following configuration lists all the valid parameters.
To specify options for the T3 side of the connection, include the `t3-options` statement at the `[edit interfaces interface-name]` hierarchy level:

```
[edit interfaces interface-name]
t3-options {
  bert-algorithm algorithm;
  bert-error-rate rate;
  bert-period seconds;
  (cbit-parity | no-cbit-parity);
  (feac-loop-respond | no-feac-loop-respond);
  loopback (local | remote);
}
```

The statements in the `t3-options` hierarchy are supported only for channel 0; they are ignored if configured on other channels.

To specify options for each of the T1 channels, include the `t1-options` statement at the `[edit interfaces interface-name]` hierarchy level:

```
[edit interfaces interface-name]
t1-options {
  byte-encoding (nx64 | nx56);
  fcs (32 | 16);
  framing (sf | esf);
  idle-cycle-flag (flags | ones);
  loopback (local | remote);
  start-end-flag (shared | filler);
  timeslots time-slot-number;
}
```

For T1 channels on a Channelized T3 interface, the clocking statement is supported only for channel 0; it is ignored if included in the configuration of channels 1 through 11. The clock source configured for channel 0 applies to all channels on the Channelized T3 interface. The individual T1 channels use a gapped 45-MHz clock as the transmit clock. When you configure the clock source for a channelized interface—`ds-x/y/z:0`, for example—you must also include the `channel-group` statement at the `[edit chassis]` hierarchy level, and specify channel group 0. For more information, see “Clock Sources on Channelized Interfaces” on page 166.

By default, Channelized T3 and STM-1 interfaces can support a maximum of 64 Frame Relay data-link connection identifiers (DLCIs), numbered 0 through 63, per channel. In DLCI sparse mode, Channelized T3 and STM-1 interfaces support a maximum of three DLCIs, numbered 0 through 1,022, per channel. DLCI 0 is reserved for LMI. You configure the router to use DLCI sparse mode by including the `sparse-dlcis` statement at the `[edit chassis fpc slot-number pic pic-number]` hierarchy level. Channelized T3 QPP interfaces support a maximum of 64 DLCIs, numbered 0 through 1,022, and, therefore, do not require sparse mode. For more information about Frame Relay DLCIs, see “Configure a Point-to-Point Frame Relay Connection” on page 309. For more information about DLCI sparse mode, see the JUNOS Internet Software Configuration Guide: Getting Started.

For more information about specific parameters, see “Configure T1 Interfaces” on page 387 and “Configure T3 Interfaces” on page 395. For a configuration example, see “Examples: Configure Channelized DS-3 to DS-1 Interfaces” on page 238.
Example: Configure Channelized T3 QPP Interfaces

In Figure 17, a Channelized DS-3 PIC with QPP is partitioned into multiple OC slices.

Figure 17: Sample Channelization of DS-3 PIC with QPP

- A Channelized T1, which is partitioned into N xDS-0 channels.
- T1 interfaces.

The following example shows how to configure cases (a) and (b):

```plaintext
[edit interfaces]
c3-1/1/0 {
    description "case (a) CT3 to CT1 and case (b) CT3 to T1.";
    t3-options {
        loopback remote;
        looptiming;
    }
    partition 1 interface-type ct1; # ct1-1/1/0:1.
    partition 2-28 interface-type t1; # t1-1/1/0:[2-28]
}
c3-1/1/0:1 {
    description "case (a) CT1s to NxDS-0s.";
    t1-options {
        bert-algorithm all-ones-repeating;
        framing sf;
        line-encoding ami;
    }
    partition 1 timeslots 2 - 10 interface-type ds0; # ds-1/1/0:1:1, channel group with 10
    DS-0s
    partition 2 timeslots 11 - 23 interface-type ds0; # ds-1/1/0:1:2, channel group with 13
    DS-0s
    ...
}
```
Examples: Configure Channelized DS-3 to DS-0 Interfaces

The following configuration is sufficient to get the Channelized DS-3 to DS-0 interface up and running. The T3 interface can be divided into 28 channels, each at T1 line rate. DS-3 channels can use the following encapsulation types for their logical interfaces:

- PPP, PPP CCC, and PPP TCC
- Frame Relay, Frame Relay CCC, and Frame Relay TCC
- Cisco HDLC, Cisco HDLC CCC, and Cisco HDLC TCC

For more information, see “Configure a Point-to-Point Frame Relay Connection” on page 309.

All these configuration examples specify channel group 0 in the interface address, which is required for configuring the t3-options and t1-options statements.

Configure Cisco HDLC encapsulation on a Channelized DS-3 to DS-0 interface:

```
[edit interfaces]
ds-2/0/1:20:0 {
  encapsulation cisco-hdlc;
  unit 0 {
    family inet {
      address 20.0.4.40/32 {
        destination 20.0.4.41;
      }
    }
  }
}

[edit chassis]
fpc 2 {
  pic 0 {
    ct3 {
      port 1 {
        t1 20 {
          channel-group 0 timeslots 1-5;
        }
      }
    }
  }
}
```
Configure PPP encapsulation on a Channelized DS-3 to DS-0 interface:

```c
[edit interfaces]
ds-2/0/1:20:0 {
    encapsulation ppp;
    unit 0 {
        family inet {
            address 20.0.4.40/32 {
                destination 20.0.4.41;
            }
        }
    }
}
[edit chassis]
fpc 2 {
    pic 0 {
        ct3 {
            port 1 {
                t1 20 {
                    channel-group 0 timeslots 1-5;
                }
            }
        }
    }
}
```

Configure three Frame Relay DLCIs on a Channelized DS-3 interface:

```c
[edit interfaces]
t1-5/1/3:0 {
    mtu 9192;
    encapsulation frame-relay;
    unit 1 {
        dlci 101;
        family inet {
            mtu 9000;
            address 10.123.1.2/32 {
                destination 10.123.1.1;
            }
        }
        family iso {
            mtu 9000;
        }
        family mpls {
            mtu 9000;
        }
    }
}
Examples: Configure Channelized DS-3 to DS-0 Interfaces

unit 2 {
    dlci 102;
    family inet {
        mtu 9000;
        address 10.123.1.4/32 {
            destination 10.123.1.3;
        }
    }
    family iso {
        mtu 9000;
    }
    family mpls {
        mtu 9000;
    }
}

unit 3 {
    dlci 103;
    family inet {
        mtu 9000;
        address 10.123.1.6/32 {
            destination 10.123.1.5;
        }
    }
    family iso {
        mtu 9000;
    }
    family mpls {
        mtu 9000;
    }
}

Configure Cisco HDLC encapsulation with byte-encoding:

[edit interfaces ds-0/1/0:5:0]
no-keepalives;
encapsulation cisco-hdlc;
ds0-options {
    byte-encoding nx56;
}
unit 0 {
    family inet {
        address 10.221.2.8/24;
    }
}

Configure Cisco HDLC encapsulation with byte-encoding and framing:

[edit interfaces ds-0/1/0:5:0]
no-keepalives;
encapsulation cisco-hdlc;
t1-options {
    byte-encoding nx56;
    framing sf;
}
unit 0 {
    family inet {
        address 10.221.2.8/24;
    }
}
Examples: Configure Channelized DS-3 to DS-1 Interfaces

The following configuration is sufficient to get the Channelized DS-3 interface up and running. The T3 interface can be divided into 28 channels, each at T1 line rate. DS-3 channels can use the following encapsulation types for their logical interfaces:

- PPP, PPP CCC, and PPP TCC
- Frame Relay, Frame Relay CCC, and Frame Relay TCC
- Cisco HDLC, Cisco HDLC CCC, and Cisco HDLC TCC

For more information, see “Configure a Point-to-Point Frame Relay Connection” on page 309.

Configure Cisco HDLC encapsulation on a Channelized DS-3 interface:

```plaintext
[edit interfaces]
t1-2/0/1:20 {
    encapsulation cisco-hdlc;
    unit 0 {
        family inet {
            address 20.0.4.40/32 {
                destination 20.0.4.41;
            }
        }
    }
}
```

Configure PPP encapsulation on a Channelized DS-3 interface:

```plaintext
[edit interfaces]
t1-2/0/1:20 {
    encapsulation ppp;
    unit 0 {
        family inet {
            address 20.0.4.40/32 {
                destination 20.0.4.41;
            }
        }
    }
}
```
Configure five Frame Relay DLCIs on a Channelized DS-3 interface:

[edit interfaces]
t1-5/1/3:0 {
    mtu 9192;
    encapsulation frame-relay;
    unit 1 {
        dlc 101;
        family inet {
            mtu 9000;
            address 10.123.1.2/32 {
                destination 10.123.1.1;
            }
        }
        family iso {
            mtu 9000;
        }
        family mpls {
            mtu 9000;
        }
    }
    unit 2 {
        dlc 102;
        family inet {
            mtu 9000;
            address 10.123.1.4/32 {
                destination 10.123.1.3;
            }
        }
        family iso {
            mtu 9000;
        }
        family mpls {
            mtu 9000;
        }
    }
    unit 3 {
        dlc 103;
        family inet {
            mtu 9000;
            address 10.123.1.6/32 {
                destination 10.123.1.5;
            }
        }
        family iso {
            mtu 9000;
        }
        family mpls {
            mtu 9000;
        }
    }
}
Configure Cisco HDLC encapsulation with byte-encoding:

```
[edit interfaces t1-1/1/0:1]
no-keepalives;
encapsulation cisco-hdlc;
t1-options {
    byte-encoding nx56;
}
unit 0 {
    family inet {
        address 10.221.2.8/24;
    }
}
```

Configure Cisco HDLC encapsulation with byte-encoding and framing:

```
[edit interfaces t1-1/1/0:1]
no-keepalives;
encapsulation cisco-hdlc;
t1-options {
    byte-encoding nx56;
    framing sf;
}
unit 0 {
    family inet {
        address 10.221.2.8/24;
    }
}
```
Chapter 17
Configure Discard Interfaces

On the router, you can configure one physical discard interface, dsc. The discard interface allows you to identify the ingress point of a denial of service (DoS) attack. When your network is under attack, the target host IP address is identified, and the local policy forwards attacking packets to the discard interface. When traffic is routed out of the discard interface, the traffic is silently discarded.

You can configure the inet or inet6 family protocol on the discard interface, which allows you to apply an output filter to the interface. If you apply an output filter to the interface, the action specified by the filter is executed before the traffic is discarded.

To configure a discard interface, include the following statements at the [edit interfaces] hierarchy level:

```
[edit interfaces]
dsc {
  unit 0 {
    family (inet | inet6) {
      filter {
        output filter-name;
      }
      address address {
        destination address;
      }
    }
  }
}
```

Keep the following guidelines in mind when configuring the discard interface:

- Only the logical interface unit 0 is supported.
- The filter and address statements are optional.
- Although you can configure an input filter and a filter group, these configuration statements have no effect because traffic is not transmitted from the discard interface.
- The show interface command is not relevant for the discard interface.

Once you configure this interface, you must then configure a local policy to forward attacking traffic to the discard interface. For a complete discussion about using the discard interface to protect your network against DoS attacks, see the JUNOS Internet Software Configuration Guide: Policy Framework.
Chapter 18
Configure E1 Interfaces

E1 is a standard WAN digital communication format designed to operate over copper facilities at a rate of 2.048 Mbps. Widely used outside North America, it is a basic time division multiplexing scheme used to carry digital circuits. The following standards apply to E1 interfaces:

- ITU-T Recommendation G.775, Loss of Signal (LOS) and Alarm Indication Signal (AIS) Defect Detection and Clearance Criteria, describes alarm reporting methods.

! The Juniper Networks E1 PIC does not support Channel Associated Signaling (CAS).

To configure E1-specific physical interface properties, include the `e1-options` statement at the `[edit interfaces interface-name]` hierarchy level:

```
[edit interfaces interface-name]
e1-options {
  bert-error-rate rate;
  bert-period seconds;
  fcs (32 | 16);
  framing (g704 | g704-no-crc4 | unframed);
  idle-cycle-flag (flags | ones);
  invert-data;
  loopback (local | remote);
  start-end-flag (shared | filler);
  timeslots time-slot-range;
}
```
You can configure the following E1-specific properties:

- Configure E1 BERT Properties on page 244
- Configure the E1 Frame Checksum on page 245
- Configure E1 Framing on page 246
- Configure the E1 Idle Cycle Flag on page 246
- Configure E1 Data Inversion on page 246
- Configure E1 Loopback Capability on page 247
- Configure E1 Start End Flags on page 248
- Configure Fractional E1 Time Slots on page 249

See also the following sections, which apply to a number of different interfaces:

- Configure the Media MTU on page 47
- Configure the Encapsulation on a Physical Interface on page 51
- Configure the Clock Source on page 59
- Configure Receive and Transmit Leaky Bucket Properties on page 60

### Configure E1 BERT Properties

You can configure an E1 interface to execute a bit error rate test (BERT) when the interface receives a request to run this test. You specify the duration of the test and the error rate to include in the bit stream by including the `bert-period` and `bert-error-rate` statements at the `edit interfaces interface-name e1-options` hierarchy level:

```
[edit interfaces interface-name e1-options]
  bert-error-rate rate;
  bert-period seconds;
```

- `seconds` is the duration of the BERT procedure. The test can last from 1 to 240 seconds; the default is 10 seconds.
- `rate` is the bit error rate. This can be an integer in the range 0 through 7, which corresponds to a bit error rate in the range $10^{-0}$ (that is, 0, which corresponds to no errors) to $10^{-7}$ (that is, 1 error per 10 million bits). The default is 0.

Individual concatenated E1 interfaces do not support the `bert-algorithm` configuration statement. For individual concatenated E1 interfaces, the `bert-algorithm` statement at the `edit interfaces interface-name e1-options` hierarchy level is ignored. The algorithm for the E1 BERT procedure is pseudo-2e15-o151 (pattern is $2^{15} - 1$, as defined in the CCITT/ITU O.151 standard).
Configure the E1 Frame Checksum

For Channelized E1 QPP interfaces, you can configure the BERT algorithm by including the `bert-algorithm` statement at the `[edit interfaces ce1-fpc/pic/port e1-options]` or `[edit interfaces e1-fpc/pic/port e1-options]` hierarchy level:

```conf
[edit interfaces ce1-fpc/pic/port e1-options]
bert-algorithm algorithm;
[edit interfaces e1-fpc/pic/port e1-options]
bert-algorithm algorithm;
```

For a list of supported algorithms, see the CLI possible completions; for example:

```conf
[edit interfaces ce1-0/0/0 e1-options]
user@host# set bert-algorithm ?
Possible completions:
pseudo-2e11-o152 Pattern is 2^{11} - 1 (per O.152 standard)
pseudo-2e15-o151 Pattern is 2^{15} - 1 (per O.152 standard)
pseudo-2e20-o151 Pattern is 2^{20} - 1 (per O.151 standard)
pseudo-2e20-o153 Pattern is 2^{20} - 1 (per O.153 standard)
```

Configure the E1 Frame Checksum

By default, the E1 interface supports a 16-bit checksum. You can configure a 32-bit checksum, which provides more reliable packet verification. However, some older equipment might not support 32-bit checksums.

To configure a 32-bit checksum, include the `fcs 32` statement at the `[edit interfaces interface-name e1-options]` hierarchy level:

```conf
[edit interfaces interface-name e1-options]
fcs 32;
```

To return to the default 16-bit frame checksum, delete the `fcs 32` statement from the configuration:

```conf
[edit]
user@host# delete interfaces e1-fpc/pic/port e1-options fcs 32
```

To explicitly configure a 16-bit checksum, include the `fcs 16` statement at the `[edit interfaces interface-name e1-options]` hierarchy level:

```conf
[edit interfaces interface-name e1-options]
fcs 16;
```
Configure E1 Framing

By default, E1 interfaces use the G704 framing mode. You can configure the alternative unframed mode if needed.

To have the interface use the unframed mode, include the framing statement at the hierarchy level, specifying the unframed option:

```
[edit interfaces interface-name e1-options]
framing unframed;
```

To explicitly configure G704 framing, include the framing statement at the hierarchy level, specifying the g704 option:

```
[edit interfaces interface-name e1-options]
framing g704;
```

By default, G704 framing uses CRC4. To explicitly configure an interface's G704 framing to not use CRC4, include the framing statement at the hierarchy level, specifying the g704-no-crc4 option:

```
[edit interfaces interface-name e1-options]
framing g704-no-crc4;
```

Configure the E1 Idle Cycle Flag

By default, an E1 interface transmits the value 0x7E in the idle cycles. To have the interface transmit the value 0xFF (all ones) instead, include the idle-cycle-flag statement at the hierarchy level, specifying the ones option:

```
[edit interfaces interface-name e1-options]
idle-cycle-flag ones;
```

To explicitly configure the default value of 0x7E, include the idle-cycle-flag statement with the flags option:

```
[edit interfaces interface-name e1-options]
idle-cycle-flag flags;
```

Configure E1 Data Inversion

By default, data inversion is disabled. To enable data inversion at the HDLC level, include the invert-data statement at the hierarchy level:

```
[edit interfaces interface-name e1-options]
invert-data;
```

When you enable data inversion, all data bits in the data stream are transmitted inverted; that is, zeroes are transmitted as ones and ones as zeroes. Data inversion is normally used only in AMI mode to guarantee ones density in the transmitted stream.
Configure E1 Loopback Capability

You can configure loopback capability between the local E1 interface and the remote channel service unit (CSU), as shown in Figure 18. You can configure the loopback to be local or remote. With local loopback, the E1 interface can transmit packets to the CSU, but receives its own transmission back again and ignores data from the CSU. With remote loopback, packets sent from the CSU are received by the E1 interface, forwarded if there is a valid route, and immediately retransmitted to the CSU.

Figure 18: Remote and Local E1 Loopback

To configure loopback capability on an E1 interface, include the `loopback` statement at the [edit interfaces interface-name e1-options] hierarchy level:

```
[edit interfaces interface-name e1-options]
loopback (local | remote);
```

Packets can be looped on either the local router or the remote CSU.

To turn off the loopback capability, remove the `loopback` statement from the configuration:

```
[edit]
user@host# delete interfaces e1-fpc/ pic/ port e1-options loopback
```
Example: Configure E1 Loopback Capability

To determine whether a problem is internal or external, loop packets on both the local and the remote router. To do this, you include the no-keepalives and encapsulation cisco-hdlc statements at the [edit interfaces interface-name] hierarchy level and the loopback local statement at the [edit interfaces interface-name e1-options] hierarchy level.

With this configuration, the link stays up, so you can loop ping packets to a remote router. The loopback local statement causes the interface to loop within the PIC just before the data reaches the transceiver.

    [edit interfaces]
    e1-1/0/0 {
        no-keepalives;
        encapsulation cisco-hdlc;
        e1-options {
            loopback local;
        }
        unit 0 {
            family inet {
                address 100.100.100.1/24;
            }
        }
    }

Check the error counters

You can determine whether there is an internal problem or an external problem by checking the error counters in the output of the show interface interface-name extensive command:

    > show interfaces e1-1/0/0 extensive

Configure E1 Start End Flags

By default, an E1 interface waits two idle cycles between sending start and end flags. To configure the interface to share the transmission of start and end flags, include the start-end-flag statement at the [edit interfaces interface-name e1-options] hierarchy level, specifying the shared option.

    [edit interfaces interface-name e1-options]
    start-end-flag shared;

To explicitly configure the default of waiting two idle cycles between the start and end flags, include the idle-cycle-flag statement with the filler option:

    [edit interfaces interface-name e1-options]
    start-end-flag filler;
Configure Fractional E1 Time Slots

To configure the number of time slots allocated to a fractional E1 interface, include the `timeslots` statement at the `[edit interfaces interface-name e1-options]` hierarchy level:

```
[edit interfaces interface-name e1-options]
timeslots time-slot-range;
```

For E1 interfaces, the time-slot range is 1 through 32. There are 32 time slots on an E1 interface. The default is to use all the time slots. You can designate any combination of time slots for usage. You can configure a range of values with hyphens, and you can separate multiple values with commas. Do not include spaces when you specify time slot numbers.

To use time slots 1 through 10, designate the time-slot range as follows:

```
[edit interfaces interface-name e1-options]
timeslots 1-10;
```

To use time slots 1 through 5, time slot 10, and time slot 24, designate the time-slot range as follows:

```
[edit interfaces interface-name e1-options]
timeslots 1-5,10,24;
```

Do not include spaces when you specify time slot numbers.

For fractional E1 interfaces only, if you connect to the interface a device that uses time slot numbering from 0 through 31, you must subtract 1 from the configured number of time slots. To do this, include the `timeslots` statement at the `[edit interfaces interface-name e1-options]` hierarchy level, and offset 1 from the specified slot number.

For example, to use time slots 3 through 5, time slot 10, and time slot 24, designate the time-slot range as follows:

```
[edit interfaces interface-name e1-options]
timeslots 4-6,11,25;
```

In this example, time slots are offset by 1 to compensate for a device attached to a fractional E1 interface.
Chapter 19
Configure E3 Interfaces

E3 is a high-speed WAN digital communication technique designed to operate over copper facilities at a rate of 34.368 Mbps. Widely used outside North America, it is the time division multiplexing scheme used to carry 16 E1 circuits. The following standards apply to E3 interfaces:


- ITU-T Recommendation G.775, Loss of Signal (LOS) and Alarm Indication Signal (AIS) Defect Detection and Clearance Criteria, describes alarm reporting methods.

To configure E3-specific physical interface properties, include the e3-options statement at the [edit interfaces interface-name] hierarchy level:

```plaintext
[edit interfaces interface-name]
e3-options {
    bert-algorithm algorithm;
    bert-error-rate rate;
    bert-period seconds;
    compatibility-mode (digital-link | kentrox | larscom) <subrate value>;
    fcs (32 | 16);
    idle-cycle-flag value;
    loopback (local | remote);
    (payload-scrambler | no-payload-scrambler);
    start-end-flag value;
}
```

You can configure the following E3-specific properties:

- Configure E3 BERT Properties on page 252
- Configure the E3 CSU Compatibility Mode on page 253
- Configure the E3 Frame Checksum on page 253
- Configure the E3 Idle Cycle Flag on page 254
- Configure E3 Loopback Capability on page 254
Configure E3 BERT Properties

You can configure an E3 interface to execute a bit error rate test (BERT) when the interface receives a request to run this test. You specify the duration of the test, the pattern to send in the bit stream, and the error rate to include in the bit stream by including the \texttt{bert-period}, \texttt{bert-algorithm}, and \texttt{bert-error-rate} statements at the [edit interfaces interface-name e3-options] hierarchy level:

```
[edit interfaces interface-name e3-options]
  bert-algorithm algorithm;
  bert-error-rate rate;
  bert-period seconds;
```

seconds is the duration of the BERT procedure. The test can last from 1 to 240 seconds; the default is 10 seconds.

rate is the bit error rate. This can be an integer in the range 0 through 7, which corresponds to a bit error rate in the range $10^{-0}$ (that is, 0, which corresponds to no errors) to $10^{-7}$ (that is, 1 error per 10 million bits).

algorithm is the pattern to send in the bit stream. On E3 interfaces, you can also select the pattern to send in the bit stream by including the \texttt{bert-algorithm} statement at the [edit interfaces interface-name interface-options] hierarchy level:

```
[edit interfaces interface-name interface-options]
  bert-algorithm algorithm;
```

For a list of supported algorithms, see the CLI possible completions; for example:

```
[edit interfaces e3-0/0/0 e3-options]
user@host# set bert-algorithm ?
Possible completions:
pseudo-2e11-o152 Pattern is $2^{11} - 1$ (per 0.152 standard)
pseudo-2e15-o151 Pattern is $2^{15} - 1$ (per 0.152 standard)
pseudo-2e20-o151 Pattern is $2^{20} - 1$ (per 0.151 standard)
pseudo-2e20-o153 Pattern is $2^{20} - 1$ (per 0.153 standard)
```

See individual interface types for specific hierarchy information. For information about running the BERT procedure, see the JUNOS Internet Software Operational Mode Command Reference.
Configure the E3 CSU Compatibility Mode

Subrating an E3 interface reduces the maximum allowable peak rate by limiting the HDLC-encapsulated payload. Subrate modes configure the PIC to connect with channel service units (CSUs) that use proprietary methods of multiplexing. For E3 interfaces, you can configure the interface to be compatible with a Digital Link, Kentrox, or Larscom CSU. To configure an E3 interface so that it is compatible with the CSU at the remote end of the line, include the compatibility statement at the [edit interfaces interface-name e3-options] hierarchy level:

[edit interfaces interface-name e3-options] compatibility-mode (digital-link | kentrox | larscom) <subrate value>;

The subrate of an E3 interface must exactly match that of the remote CSU. To specify the subrate, include the subrate statement in the configuration:

- For Digital Link CSUs only, you can specify the subrate value to match the data rate configured on the CSU in the format xkb or xMb. For a list of specific rate values, use the command completion feature in the CLI. The range is 358 kbps through 33.7 Mbps.

- Kentrox and Larscom CSUs do not support E3 subrate.

Configure the E3 Frame Checksum

You can configure a 32-bit checksum, which provides more reliable packet verification. However, some older equipment might not support 32-bit checksums.

On a Channelized OC-12 interface, the fcs statement is not supported. To configure FCS on each E3 channel, you must include the e3-options fcs statement in the configuration for each channel.

To configure a 32-bit checksum, include the fcs statement at the [edit interfaces interface-name E3-options] hierarchy level:

[edit interfaces interface-name e3-options] fcs 32;

To return to the default 16-bit frame checksum, delete the fcs 32 statement from the configuration:

[edit] user@host# delete interfaces e3-fc/pic/port e3-options fcs 32

To explicitly configure a 16-bit checksum, include the fcs statement at the [edit interfaces interface-name e3-options] hierarchy level:

[edit interfaces interface-name e3-options] fcs 16;
Configure the E3 Idle Cycle Flag

By default, a E3 interface transmits the value 0x7E in the idle cycles. To have the interface transmit the value 0xFF (all ones) instead, include the idle-cycle-flag statement at the [edit interfaces interface-name e3-options] hierarchy level, specifying the ones option:

```
[edit interfaces interface-name e3-options]
idle-cycle-flag ones;
```

To explicitly configure the default value of 0x7E, include the idle-cycle-flag statement with the flags option:

```
[edit interfaces interface-name e3-options]
idle-cycle-flag flags;
```

Configure E3 Loopback Capability

You can configure loopback capability between the local E3 interface and the remote CSU. You can configure the loopback to be local or remote. With local loopback, the E3 interface can transmit packets to the CSU, but receives its own transmission back again and ignores data from the CSU. With remote loopback, packets sent from the CSU are received by the E3 interface, forwarded if there is a valid route, and immediately retransmitted to the CSU (see Figure 19).

![Figure 19: Remote and Local E3 Loopback](image)

To configure loopback capability on an E3 interface, include the loopback statement at the [edit interfaces interface-name e3-options] hierarchy level:

```
[edit interfaces interface-name e3-options]
loopback (local | remote);
```

Packets can be looped on either the local router or the remote CSU.

To turn off the loopback capability, remove the loopback statement from the configuration:

```
[edit]
user@host# delete interfaces e3-fpc/ pic/ port e3-options loopback
```
Example: Configure E3 Loopback Capability

To determine whether a problem is internal or external, loop packets on both the local and the remote router. To do this, include the no-keepalives and encapsulation cisco-hdlc statements at the [edit interfaces interface-name] hierarchy level and the loopback local statement at the [edit interfaces interface-name e3-options] hierarchy level. With this configuration, the link stays up, so you can loop ping packets to a remote router. The loopback local statement causes the interface to loop within the PIC just before the data reaches the transceiver.

```
[edit interfaces]
e3-1/0/0 {
    no-keepalives;
    encapsulation cisco-hdlc;
    e3-options {
        loopback local;
    }
    unit 0 {
        family inet {
            address 100.100.100.1/24;
        }
    }
}
```

Check the error counters You can determine whether there is an internal problem or an external problem by checking the error counters in the output of the show interface interface-name extensive command:

```
> show interfaces e3-1/0/0 extensive
```

Configure E3 HDLC Payload Scrambling

E3 HDLC payload scrambling, which is disabled by default, provides better link stability. Both sides of a connection must either use or not use scrambling.

To configure scrambling on the interface, you can include the payload-scrambler statement at the [edit interfaces interface-name e3-options] hierarchy level:

```
[edit interfaces interface-name e3-options]
payload-scrambler;
```

To explicitly disable HDLC payload scrambling, include the no-payload-scrambler statement at the [edit interfaces interface-name e3-options] hierarchy level:

```
[edit interfaces interface-name e3-options]
no-payload-scrambler;
```

To disable payload scrambling again (return to the default), delete the payload-scrambler statement from the configuration:

```
[edit]
user@host# delete interfaces e3-fpc/ pic/ port e3-options payload-scrambler
```
Configure the E3 Start End Flags

By default, a E3 interface waits two idle cycles between sending start and end flags. To configure the interface to share the transmission of start and end flags, include the start-end-flag statement at the [edit interfaces interface-name e3-options] hierarchy level, specifying the shared option.

[edit interfaces interface-name e3-options]
start-end-flag shared;

To explicitly configure the default of waiting two idle cycles between the start and end flags, include the idle-cycle-flag statement with the filler option:

[edit interfaces interface-name e3-options]
start-end-flag filler;
Chapter 20

Configure Encryption Interfaces

The Internet Protocol Security (IPSec) architecture provides a security suite for the IPv4 and IPv6 network layers. The suite provides functionality such as authentication of origin, data integrity, confidentiality, replay protection, and non-repudiation of source. It also defines mechanisms for key generation and exchange, management of security associations, and support for digital certificates.

IPSec defines a security association (SA) and key management framework that can be used with any network layer protocol. The SA specifies what protection policy to apply to traffic between two IP-layer entities. For more information, see the JUNOS Internet Software Configuration Guide: Getting Started. The standards are defined in the following RFCs:

- RFC 2401, Security Architecture for the Internet Protocol
- RFC 2406, IP Encapsulating Security Payload (ESP)

To enable encryption interfaces, you can configure the following properties:

- Configure an Encryption Interface on page 258
- Configure ES PIC Redundancy on page 259
- Configure ES PIC Redundancy on page 259
- Configure IPSec Tunnel Redundancy on page 260

For detailed information about configuring the ES PIC, see the JUNOS Internet Software Configuration Guide: Services Interfaces.
Configure an Encryption Interface

When you configure the Encryption interface, you associate the configured SA with a logical interface. This configuration defines the tunnel, including the logical unit, tunnel addresses, maximum transmission unit (MTU), optional interface addresses, and the name of the IPSec SA to apply to traffic. To configure an Encryption interface, include the following statements at the `[edit interfaces es-fpc/pic/port unit logical-unit-number]` hierarchy level:

```
[edit interfaces es-fpc/pic/port unit logical-unit-number]
family inet {
  ipsec-sa ipsec-sa; # name of security association to apply to packet
  address address { # local interface address inside local VPN
    destination address; # destination address inside remote VPN
  }
}

You must configure the tunnel source address locally on the router, and the tunnel destination address must be a valid address for the security gateway terminating the tunnel.

The M5, M10, M20, and M40 routers support the ES PIC.
```

The addresses configured as the tunnel source and destination are the addresses in the outer IP header of the tunnel.

The SA must be a valid tunnel-mode SA. The interface address and destination address listed are optional. The destination address allows the user to configure a static route to encrypt traffic. If a static route uses that destination address as the next hop, traffic is forwarded through the portion of the tunnel in which encryption occurs.

Specify the Security Association Name

The security association is the set of properties that defines the protocols for encrypting internet traffic. To configure encryption interfaces, you specify the security association (SA) name associated with the interface by including the `ipsec-sa sa-name` statement at the `[edit interfaces es-fpc/pic/port unit logical-unit-number family inet]` hierarchy level:

```
[edit interfaces es-fpc/pic/port unit logical-unit-number family inet]
ipsec-sa sa-name;
```

For information about configuring the security association, see “Configure ES PIC Redundancy” on page 259.
Example: Configure an Encryption Interface

Configure an IPSec tunnel as a logical interface on the ES PIC. The logical interface specifies the tunnel through which the encrypted traffic travels. The `ipsec-sa` statement associates the security profile with the interface.

```
[edit interfaces]
es 0/0/0 {
    unit 0 {
        tunnel {
            source 10.5.5.5;                      # tunnel source address
            destination 10.6.6.6;                          # tunnel destination address
        }
        family inet {
            ipsec-sa manual-sa1; # name of security association to apply to packet
            mtu 3800;            # tunnel MTU
            address 10.1.1.8/32 {
                # local interface address inside local VPN
                destination 10.2.2.254;  # destination address inside remote VPN
            }
        }
    }
}
```

Configure ES PIC Redundancy

You can configure ES PIC redundancy for routers that can have multiple ES PICs. With ES PIC redundancy, one ES PIC is active and another ES PIC is on standby. When the primary ES PIC has a servicing failure, the backup becomes active, inherits all the tunnels and security associations (SAs), and acts as the new next hop for IPSec traffic. Reestablishment of tunnels on the backup ES PIC does not require new IKE negotiations. If the primary ES PIC comes online, it remains in standby and does not preempt the backup. To determine which PIC is currently active, use the `show ipsec redundancy` command.

ES PIC redundancy is supported on M-series routers only.

To configure an ES PIC as the backup, include the `backup-interface` statement at the `[edit interfaces es-fpc/pic/port es-options]` hierarchy level:

```
[edit interfaces es-fpc/pic/port es-options]
backup-interface es-fpc/pic/port;
```
Example: Configure ES PIC Redundancy

After you create the inbound firewall filter, apply it to the master ES PIC. Here, the inbound firewall filter (ipsec-decrypt-policy-filter) is applied on the decrypted packet to perform the final policy check. The IPSec manual-sa1 SA is referenced at the [edit interfaces es-1/2/0 unit 0 family inet] hierarchy level and decrypts the incoming packet. This example does not show SA and filter configuration. For information about SA and filter configuration, see the the JUNOS Internet Software Configuration Guide: Getting Started, the JUNOS Internet Software Configuration Guide: Policy Framework, and the JUNOS Internet Software Configuration Guide: Services Interfaces.

```
[edit interfaces]
es-1/2/0 {
    es-options {
        backup-interface es-1/0/0;
    }
}:
unit 0 {
    tunnel {
        source 10.5.5.5;
        destination 10.6.6.6;
    }
    family inet {
        ipsec-sa manual-sa1;
        filter {
            input ipsec-decrypt-policy-filter;
        }
        address 10.1.1.8/32 {
            destination 10.2.2.254;
        }
    }
}
```

Configure IPSec Tunnel Redundancy

You can configure IPSec tunnel redundancy by specifying a backup destination address. The local router sends keepalives to determine the remote site's reachability. When the peer is no longer reachable, a new tunnel is established. For up to 60 seconds during failover, traffic is dropped without notification being sent. Figure 20 shows IPSec primary and backup tunnels.

Figure 20: IPSec Tunnel Redundancy
To configure IPSec tunnel redundancy, include the `backup-destination` statement at the [edit interfaces unit logical-unit-number tunnel] hierarchy level:

```
[edit interfaces unit logical-unit-number]
tunnel {
    backup-destination address;
    destination address;
    source address;
}
```

Tunnel redundancy is supported on M-series routers only.

- The primary and backup destinations must be on different routers.
- The tunnels should be diverse and policies should match.

For more information about tunnels, see “Configure Tunnel Interfaces” on page 407.
Chapter 21
Configure Ethernet Interfaces

Ethernet was developed in the early 1970s at the Xerox Palo Alto Research Center as a
data-link control layer protocol for interconnecting computers. It was first widely used at
10 Mbps over coaxial cables and later over unshielded twisted pairs using 10BaseT. More
recently, 100BaseTX (Fast Ethernet, 100 Mbps), Gigabit Ethernet (1 Gbps), and 10-Gigabit
Ethernet (10 Gbps) have become available.

Juniper Networks routers support the following types of Ethernet interfaces:

- Fast Ethernet
- Gigabit Ethernet
- Gigabit Ethernet Q Performance Processor (QPP)
- 10-Gigabit Ethernet
- Management Ethernet interface, which is an out-of-band management interface within
  the router
- Internal Ethernet interface, which connects the Routing Engine to the Packet Forwarding
  Engine
- Aggregated Ethernet interface, a logical linkage of Fast Ethernet, Gigabit Ethernet, or
  10-Gigabit Ethernet physical connections

This chapter discusses the following topics specific to configuring the different types of
Ethernet interfaces in the router:

- Configure Ethernet Physical Interface Properties on page 264
- Configure 802.1Q VLANs on page 282
- Configure TCC and Layer 2.5 Switching on page 286
- Configure Static ARP Table Entries on page 289
- Configure VRRP on page 290
- Configure the Management Ethernet Interface on page 298
- Configure the Internal Ethernet Interface on page 299
- Configure Aggregated Ethernet Interfaces on page 299
Configure Ethernet Physical Interface Properties

For examples of Ethernet interface configuration, see the following sections:

- Example: Configure Fast Ethernet Interfaces on page 301
- Example: Configure Gigabit Ethernet Interfaces on page 301
- Example: Configure Aggregated Ethernet Interfaces on page 302

Configure Ethernet Physical Interface Properties

To configure Fast Ethernet-specific physical interface properties, include the fastether-options statement at the [edit interfaces fe-fpc/pic/port] hierarchy level:

```
[edit interfaces fe-fpc/pic/port]
link-mode (full-duplex | half-duplex);
speed (10m | 100m);
vlntagging;
fastether-options {
  802.3ad ae;
  (flow-control | no-flow-control);
  ingress-rate-limit rate;
  (loopback | no-loopback);
  source-address-filter {
    mac-address;
  }
  (source-filtering | no-source-filtering);
}
```

The statement `speed (10m | 100m)` applies only to the management Ethernet interface (fxp0) and to the Fast Ethernet 12-port and 48-port PICs. The 4-port and 8-port Fast Ethernet PICs support a speed of 100 Mbps only.

To configure Gigabit Ethernet- and 10-Gigabit Ethernet-specific physical interface properties, include the gigether-options statement at the [edit interfaces ge-fpc/pic/port] hierarchy level:

```
[edit interfaces ge-fpc/pic/port]
gigether-options {
  802.3ad ae;
  (flow-control | no-flow-control);
  (loopback | no-loopback);
  source-address-filter {
    mac-address;
  }
  (source-filtering | no-source-filtering);
}
```
To configure Gigabit Ethernet QPP-specific physical interface properties, include the `gigether-options` statement at the `[edit interfaces ge-fpc/ pic/ port]` hierarchy level and the `input-vlan-map` and `output-vlan-map` statements at the `[edit interfaces ge-fpc/ pic/ port unit logical-unit-number]` hierarchy level:

```plaintext
[edit interfaces ge-fpc/ pic/ port]
gigether-options {
    802.3ad aex;
    (flow-control | no-flow-control);
    (loopback | no-loopback);
    ethernet-switch-profile {
        ethernet-policer-profile {
            ieee802.1-priority-map premium [ bits ];
        }
        policer cos-policer-name {
            aggregate {
                bandwidth-limit rate;
                bandwidth-percent percent;
                burst-size-limit length;
            }
            premium {
                bandwidth-limit rate;
                bandwidth-percent percent;
                burst-size-limit length;
            }
        }
        (mac-learn-enable | no-mac-learn-enable);
        tag-protocol-id [ tpid ];
    }
}

[edit interfaces ge-fpc/ pic/ port unit logical-unit-number]
input-vlan-map {
    pop;
    push;
    swap;
    vlan-id number;
    tag-protocol-id tpid;
}
output-vlan-map {
    pop;
    push;
    swap;
    vlan-id number;
    tag-protocol-id tpid;
}
```
To configure aggregated Ethernet-specific physical interface properties, include the
aggregated-ether-options statement at the [edit interfaces aex] hierarchy level:

```
[edit interfaces aex]
aggregated-ether-options {
    (flow-control | no-flow-control);
    link-speed speed;
    (loopback | no-loopback);
    minimum-links number;
    source-address-filter {
        mac-address;
    }
    (source-filtering | no-source-filtering);
}
```

You can configure the following properties specific to aggregated Ethernet, Fast Ethernet,
Gigabit Ethernet, Gigabit Ethernet QPP, and 10-Gigabit Ethernet interfaces:

- Configure Ethernet Link Aggregation on page 266
- Configure Gratuitous ARP on page 281
- Configure Aggregated Ethernet Link Speed on page 267
- Configure Aggregated Ethernet Minimum Links on page 267
- Configure Gigabit Ethernet QPP Interfaces on page 267
- Configure Ethernet MAC Address Filtering on page 279
- Configure Ethernet Loopback Capability on page 280
- Configure Flow Control on page 280
- Configure the Link Characteristics on page 281
- Configure the Interface Speed on page 282
- Configure the Ingress Rate Limit on page 282

**Configure Ethernet Link Aggregation**

On Fast Ethernet, Gigabit Ethernet, and 10-Gigabit Ethernet interfaces, you can associate a
physical interface with an aggregated Ethernet interface. To enable the aggregated link,
include the 802.3ad statement at the [edit interfaces interface-name fastether-options] or [edit
interfaces interface-name gigether-options] hierarchy level:

```
802.3ad aex;
```

You specify the interface instance number x to complete the link association; x can range
from 0 through 15, for a total of 16 aggregated interfaces. You must also include a statement
defining aex at the [edit interfaces ] hierarchy level. For more information, see “Configure
Aggregated Ethernet Interfaces” on page 299. You can optionally specify other physical
properties that apply specifically to the aggregated Ethernet interfaces; for details, see
“Configure Ethernet Physical Interface Properties” on page 264, and for a sample
configuration, see “Example: Configure Aggregated Ethernet Interfaces” on page 302.
Configure Aggregated Ethernet Link Speed

On aggregated Ethernet interfaces, you can set the required link speed for all interfaces included in the bundle. All interfaces that make up a bundle must be the same speed. If you include in the aggregated Ethernet interface an individual link that has a speed different from the speed you specify in the \texttt{link-speed} parameter, an error message will be logged. To set the required link speed, include the \texttt{link-speed} statement at the \texttt{[edit interfaces interface-name aggregated-ether-options]} hierarchy level:

\begin{verbatim}
[edit interfaces interface-name aggregated-ether-options]
link-speed speed;
\end{verbatim}

speed can be in bits per second either as a complete decimal number or as a decimal number followed by the abbreviation \texttt{k} (1000), \texttt{m} (1,000,000), or \texttt{g} (1,000,000,000).

Configure Aggregated Ethernet Minimum Links

On aggregated Ethernet interfaces, you can configure the minimum number of links that must be up for the bundle as a whole to be labeled up. By default, the minimum number of links is one. The minimum number of links can be from one through eight.

To configure the minimum number of links, include the \texttt{minimum-links} statement at the \texttt{[edit interfaces interface-name aggregated-ether-options]} hierarchy level:

\begin{verbatim}
[edit interfaces interface-name aggregated-ether-options]
minimum-links number;
\end{verbatim}

Configure Gigabit Ethernet QPP Interfaces

The one-port and two-port Gigabit Ethernet PICs with QPP are primarily used for virtual metropolitan-area network (VMAN) aggregation and ISP peering applications. The Gigabit Ethernet PIC with QPP requires an enhanced FPC.

Table 22 lists the capabilities of the Gigabit Ethernet PIC with QPP.
Table 22: Capabilities of the Gigabit Ethernet PIC with QPP

<table>
<thead>
<tr>
<th>Layer 2</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>802.3ad link aggregation</td>
<td>Not applicable</td>
</tr>
<tr>
<td>Maximum VLANs per port</td>
<td>384</td>
</tr>
<tr>
<td>MTU size</td>
<td>9192</td>
</tr>
<tr>
<td>MAC filters:</td>
<td></td>
</tr>
<tr>
<td>Destinations per port</td>
<td>960</td>
</tr>
<tr>
<td>Sources per port</td>
<td>64</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Layer 2 VPNs</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN CCC</td>
<td>Yes</td>
</tr>
<tr>
<td>Port-based CCC</td>
<td>Yes</td>
</tr>
<tr>
<td>Extended VLAN CCC VMANs Tag Protocol</td>
<td>Yes</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CoS</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>PIC-based egress queues</td>
<td>Yes</td>
</tr>
</tbody>
</table>

On Gigabit Ethernet QPP interfaces, you can perform the following tasks:

- Configure a Gigabit Ethernet QPP Policer Profile on page 269
- Configure Gigabit Ethernet QPP MAC Address Filtering on page 270
- Configure Gigabit Ethernet QPP MAC Address Accounting on page 272
- Stack and Rewrite Gigabit Ethernet QPP VLAN Tags on page 273

For example configurations, see the following sections:

- Example: Configure Gigabit Ethernet QPP MAC Address Filtering on page 271
- Examples: Stack and Rewrite Gigabit Ethernet QPP VLAN Tags on page 274

You can also configure class of service (CoS) on logical QPP interfaces. For more information, see “Associate a Scheduler with a DLCI or VLAN on a Channelized QPP Interface” on page 597.
Configure a Gigabit Ethernet QPP Policer Profile

On Gigabit Ethernet QPP interfaces, you can define rate limits for premium and aggregate traffic received on the interface. These policers allow you to perform simple traffic policing on Gigabit Ethernet QPP interfaces without configuring a firewall filter. First you configure the Ethernet policer profile, then you can apply the policer to an interface. For information about applying the policer to an interface, see “Configure Gigabit Ethernet QPP MAC Address Filtering” on page 270.

To configure an Ethernet policer profile, include the ethernet-policer-profile statement at the [edit interfaces interface-name gigether-options] hierarchy level:

```
[edit interfaces interface-name gigether-options ethernet-switch-profile]
ethernet-policer-profile {
  ieee802.1-priority-map premium [ bits ];
  policer cos-policer-name {
    aggregate {
      bandwidth-limit rate;
      bandwidth-percent percent;
      burst-size-limit length;
    }
    premium {
      bandwidth-limit rate;
      bandwidth-percent percent;
      burst-size-limit length;
    }
  }
}
```

When configuring the bandwidth, use the bandwidth-limit statement and not the bandwidth-percent statement. If you include the bandwidth-percent statement at the [edit interfaces interface-name gigether-options ethernet-policer-profile policer (aggregate | premium)] hierarchy level, it currently has no effect.

In the Ethernet policer profile, the aggregate-priority policer is mandatory; the premium-priority policer is optional. If you include a premium-priority policer, you can specify premium IEEE 802.1p bits by including the ieee802.1-priority-map statement at the [edit interfaces interface-name gigether-options ethernet-policer-profile] hierarchy level:

```
[edit interfaces interface-name gigether-options ethernet-policer-profile]
  ieee802.1-priority-map premium [ bits ];
```

Specify values of the code-point bits, in binary code. The remaining bits are classified as nonpremium (or aggregate).

To configure rate limiting for premium and aggregate policers, you specify the bandwidth limit in bits per second. You can specify the value as a complete decimal number or as a decimal number followed by the abbreviation k (1000), m (1,000,000), or g (1,000,000,000). There is no absolute minimum value for bandwidth limit, but any value below 61,040 bps will result in an effective rate of 30,520 bps. The maximum bandwidth limit is 4.29 Gbps.

You can rate-limit based on port speed. You specify this port speed as a bandwidth percentage in a policer. The percentage must be a whole decimal number between 1 and 100.
The maximum burst size controls the amount of traffic bursting allowed. To determine the burst-size limit, you can multiply the bandwidth of the interface on which you are applying the filter by the amount of time you allow a burst of traffic at that bandwidth to occur:

\[
\text{burst size} = \text{bandwidth} \times \text{allowable time for burst traffic}
\]

If you do not know the interface bandwidth, you can multiply the maximum transmission unit (MTU) of the traffic on the interface by 10 to obtain a value. For example, the burst size for an MTU of 4700 would be 47,000 bytes. The burst size should be at least 10 interface MTUs. The maximum value for the burst-size limit is 100 MB.

**Configure Gigabit Ethernet QPP MAC Address Filtering**

On Gigabit Ethernet QPP interfaces, you can enable MAC address filtering to accept packets from specific MAC addresses, and then apply a policer to the accepted packets. To configure MAC address filtering, include the `accept-source-mac` statement at the `interface-name unit logical-unit-number` hierarchy level:

```yaml
[edit interfaces interface-name unit logical-unit-number]
accept-source-mac {
    mac-address mac-address {
        policer {
            input policer-name;
            output policer-name;
        }
    }
}
```

You can specify the MAC address as `nn:nn:nn:nn:nn` or `nnnn:nnnn:nnnn`, where `n` is a hexadecimal number. To specify more than one address, include multiple `mac-address` statements at the `interface-name unit logical-unit-number` hierarchy level.

If the remote Ethernet card is changed, the interface does not accept traffic from the new card because the new card has a different MAC address.

The MAC addresses you include in the configuration are entered into the router’s MAC database. To view the router’s MAC database, enter the `show interfaces mac-database interface-name` command:

```
user@host> show interfaces mac-address interface-name
```

Optionally, you can apply input and output policers that define rate limits for premium and aggregate traffic received on the interface. These policers allow you to perform simple traffic policing on Gigabit Ethernet QPP interfaces without configuring a firewall filter. For information about defining these policers, see “Configure a Gigabit Ethernet QPP Policer Profile” on page 269.

In the `input` statement, list the name of one policer template to be evaluated when packets are received on the interface.

In the `output` statement, list the name of one policer template to be evaluated when packets are transmitted on the interface.

You can use the same policer one or more times.

If you apply both policers and firewall filters to an interface, input policers are evaluated before input firewall filters, and output policers are evaluated after output firewall filters.
You cannot define traffic with specific MAC addresses to be rejected; however, you can block all incoming packets that do not have a source address specified at the [edit interfaces interface-name unit logical-unit-number accept-source-mac] hierarchy level. To enable this blocking, include the source-filtering statement at the [edit interfaces interface-name gigether-options] hierarchy level:

```
[edit interfaces interface-name gigether-options]
source-filtering;
```

For more information, see “Configure Ethernet MAC Address Filtering” on page 279.

To accept traffic even though it does not have a source address specified at the [edit interfaces interface-name unit logical-unit-number accept-source-mac] hierarchy level, include the no-source-filtering statement at the [edit interfaces interface-name gigether-options] hierarchy level:

```
[edit interfaces interface-name gigether-options]
no-source-filtering;
```

Example: Configure Gigabit Ethernet QPP MAC Address Filtering

Configure interface ge-6/0/0 to treat priority levels 2 and 3 as premium. On ingress, this means that IEEE 802.1p priority values 2 and 3 are premium. On egress, it means traffic classified into Queue 1 is premium. Define a policer that limits the premium bandwidth to 100 Mbps and burst size to 3 k, and the aggregate bandwidth to 200 Mbps and burst size to 3 k. Specify that frames received from the MAC address 00:01:02:03:04:05 and the VLAN ID 600 are subject to the policer on input and output. On input, this means frames received with the source MAC address 00:01:02:03:04:05 and the VLAN ID 600 are subject to the policer. On output, this means frames transmitted from the router with the destination MAC address 00:01:02:03:04:05 and the VLAN ID 600 are subject to the policer.

```
[edit interfaces]
ge-6/0/0 {
  gigether-options {
    ether-switch-profile {
      ether-policer-profile {
        ieee802.1-priority-map {
          premium [ 2 3 ];
        }
        policer policer-1 {
          premium {
            bandwidth-limit 100m;
            burst-size-limit 3k;
          }
          aggregate {
            bandwidth-limit 200m;
            burst-size-limit 3k;
          }
        }
      }
    }
  }
}
```
Configure Gigabit Ethernet QPP MAC Address Accounting

For Gigabit Ethernet QPP interfaces only, you can configure whether source and destination MAC addresses are dynamically learned. To configure MAC address accounting, include the mac-learn-enable statement at the [edit interfaces interface-name gigether-options ethernet-switch-profile] hierarchy level:

```
[edit interfaces interface-name gigether-options ethernet-switch-profile]
mac-learn-enable;
```

To prohibit the interface from dynamically learning source and destination MAC addresses, include the no-mac-learn-enable statement at the [edit interfaces interface-name gigether-options ethernet-switch-profile] hierarchy level:

```
[edit interfaces interface-name gigether-options ethernet-switch-profile]
no-mac-learn-enable;
```

MAC address learning is based on source addresses. You can start accounting for traffic after it has been sent from the MAC address. Once the MAC address is learned, the frames and bytes transmitted to or received from the MAC address can be tracked.
Stack and Rewrite Gigabit Ethernet QPP VLAN Tags

On Gigabit Ethernet QPP interfaces with encapsulation type `extended-vlan-ccc` or `vlan-ccc`, you can stack and rewrite VLAN tags. Stacking and rewriting VLAN tags allows you to use an additional (outer) VLAN tag to differentiate between customer edge (CE) routers that share one VLAN ID.

To stack and rewrite VLAN tags, include the `input-vlan-map` and `output-vlan-map` statements at the `[edit interfaces interface-name unit logical-unit-number]` hierarchy level:

```
[edit interfaces interface-name unit logical-unit-number]
input-vlan-map {
  pop;
  push;
  swap;
  vlan-id number;
  tag-protocol-id tpid;
}
output-vlan-map {
  pop;
  push;
  swap;
  vlan-id number;
  tag-protocol-id tpid;
}
```

To stack a VLAN tag on top of all tagged frames entering or exiting the interface, include the `push`, `vlan-id`, and `tag-protocol-id` statements at the `[edit interfaces interface-name unit logical-unit-number input-vlan-map]` or `[edit interfaces interface-name unit logical-unit-number output-vlan-map]` hierarchy level.

To remove a VLAN tag from all tagged frames entering or exiting the interface, include the `pop` statement at the `[edit interfaces interface-name unit logical-unit-number input-vlan-map]` or `[edit interfaces interface-name unit logical-unit-number output-vlan-map]` hierarchy level.

If you include the `push` statement in an interface's input VLAN map, you must include the `pop` statement in the interface's output VLAN map.

The VLAN IDs you define in the input and output VLAN maps are stacked on top of the VLAN ID you define at the `[edit interfaces interface-name unit logical-unit-number vlan-id number]` hierarchy level.

You can configure frames with particular TPIDs to be processed as tagged frames. To do this, you specify up to eight IEEE 802.1q TPID values per port; a frame with any of the specified TPIDs is processed as a tagged frame. To configure the TPID values, include the `tag-protocol-id` statement at the `[edit interfaces interface-name gigether-options ethernet-switch-profile ethernet-policer-profile]` hierarchy level:

```
[edit interfaces interface-name gigether-options ethernet-switch-profile]
tag-protocol-id [ tpids ];
```

All TPIDs you include in input and output VLAN maps must be among those you specify at the `[edit interfaces interface-name gigether-options ethernet-switch-profile tag-protocol-id [ tpids ]]` hierarchy level.

To rewrite the VLAN tag on all tagged frames entering the interface to a specified VLAN ID and TPID, include the `swap`, `tag-protocol-id`, and `vlan-id` statements at the `[edit interfaces interface-name unit logical-unit-number input-vlan-map]` hierarchy level.
To rewrite the VLAN tag on all tagged frames exiting the interface to a specified VLAN ID and TPID, include the `swap` and `tag-protocol-id` statements at the `[edit interfaces interface-name unit logical-unit-number output-vlan-map]` hierarchy level. The swap operation works on the outer tag only, independent of whether you include the `stacked-vlan-tagging` statement in the configuration. If you include the `swap` statement in the configuration, the VLAN ID in outgoing frames is rewritten to the VLAN ID you configure at the `[edit interfaces interface-name unit logical-unit-number]` hierarchy level.

To configure stacked VLAN tagging for all logical interfaces on a physical interface, include the `stacked-vlan-tagging` statement at the `[edit interfaces interface-name]` hierarchy level:

```
[edit interfaces interface-name]
stacked-vlan-tagging;
```

If you include the `stacked-vlan-tagging` statement in the configuration, you must configure dual VLAN tags for all logical interfaces on the physical interface. To configure dual VLAN tags on a logical interface, include the `vlan-tag` statement at the `[edit interfaces interface-name unit logical-unit-number]` hierarchy level:

```
[edit interfaces interface-name unit logical-unit-number]
vlan-tag {tpid.vlan-id};
```

Configure the outer tag first, then the inner tag. The outer tag VLAN ID range is 1 through 511 for normal interfaces, and 512 and above for VLAN CCC interfaces. The inner tag does not have this restriction. If you configure stacked VLAN tagging, you can configure a maximum of two TPID VLAN ID pairs.

Examples: Stack and Rewrite Gigabit Ethernet QPP VLAN Tags

Configure a VLAN CCC tunnel, in which Ethernet frames enter the tunnel at interface `ge-4/0/0` and exit the tunnel at interface `ge-4/2/0`. The following examples show how to perform the following tasks:

- Push a TPID and VLAN ID pair on ingress.
- Swap a VLAN ID on ingress.
- Swap a VLAN ID on egress.
- Swap a VLAN ID on both ingress and egress.
Push a TPID and VLAN ID pair on ingress

```
[edit interfaces]
ge-4/0/0 {
    vlan-tagging;
    encapsulation vlan-ccc;
    gigether-options {
        ethernet-switch-profile {
            tag-protocol-id 0x9909;
        }
    }
    unit 0 {
        encapsulation vlan-ccc;
        vlan-id 512;
        input-vlan-map {
            push;
            tag-protocol-id 0x9909;
            vlan-id 520;
        }
        output-vlan-map pop;
    }
}
ge-4/2/0 {
    vlan-tagging;
    encapsulation vlan-ccc;
    unit 0 {
        encapsulation vlan-ccc;
        vlan-id 520;
    }
}

[edit protocols]
mls {
    interface ge-4/0/0.0;
    interface ge-4/2/0.0;
}
connections {
    interface-switch vlan-tag-push {
        interface ge-4/0/0.0;
        interface ge-4/2/0.0;
    }
}
```
Swap a VLAN ID on ingress

[edit interfaces]
ge-4/0/0 {
 vlan-tagging;
 encapsulation vlan-ccc;
 gigether-options {
   ethernet-switch-profile {
     tag-protocol-id 0x9100;
   }
 }
...
unit 1 {
   encapsulation vlan-ccc;
   vlan-id 1000;
   input-vlan-map {
     swap;
     tag-protocol-id 0x9100;
     vlan-id 2000;
   }
 }
}
ge-4/2/0 {
 vlan-tagging;
 encapsulation vlan-ccc;
 ...
unit 1 {
   encapsulation vlan-ccc;
   vlan-id 2000;
 }
}

[edit protocols]
mpls {
 ...
 interface ge-4/0/0.1;
 interface ge-4/2/0.1;
 }
connections {
 ...
 interface-switch vlan-tag-swap {
   interface ge-4/2/0.1;
   interface ge-4/0/0.1;
 }
}
Swap a VLAN ID on egress

[edit interfaces]
ge-4/0/0 {
  vlan-tagging;
  encapsulation vlan-ccc;
  ...
  unit 1 {
    encapsulation vlan-ccc;
    vlan-id 1000;
  }
}
ge-4/2/0 {
  vlan-tagging;
  encapsulation vlan-ccc;
  gigether-options {
    ethernet-switch-profile {
      tag-protocol-id 0x8800;
    }
  }
  ...
  unit 1 {
    encapsulation vlan-ccc;
    vlan-id 2000;
    output-vlan-map {
      swap;
      tag-protocol-id 0x8800; # No egress VLAN ID rewrite support; only TPID rewrite support
    }
  }
}

[edit protocols]
mls {
  ...
  interface ge-4/0/0.1;
  interface ge-4/2/0.1;
}
connections {
  ...
  interface-switch vlan-tag-swap {
    interface ge-4/2/0.1;
    interface ge-4/0/0.1;
  }
}
Swap a VLAN ID on both ingress and egress

```
[edit interfaces]
ge-4/0/0 {
  vlan-tagging;
  encapsulation vlan-ccc;
  gigether-options {
    ethernet-switch-profile {
      tag-protocol-id [0x8800 0x9100];
    }
  }
  ...
  unit 1 {
    encapsulation vlan-ccc;
    vlan-id 1000;
    input-vlan-map {
      swap;
      tag-protocol-id 0x9100;
      vlan-id 2000;
    }
  }
}
ge-4/2/0 {
  vlan-tagging;
  encapsulation vlan-ccc;
  gigether-options {
    ethernet-switch-profile {
      tag-protocol-id [0x8800 0x9100];
    }
  }
  unit 1 {
    encapsulation vlan-ccc;
    vlan-id 2000;
    output-vlan-map {
      swap;
      tag-protocol-id 0x8800;
    }
  }
}
[edit protocols]
mpls {
  ...
  interface ge-4/0/0.1;
  interface ge-4/2/0.1;
}
connections {
  ...
  interface-switch vlan-tag-swap {
    interface ge-4/2/0.1;
    interface ge-4/0/0.1;
  }
}
```
Configure Ethernet MAC Address Filtering

By default, source address filtering is disabled. On aggregated Ethernet, Fast Ethernet, Gigabit Ethernet, 10-Gigabit Ethernet, and Gigabit Ethernet QPP interfaces, you can enable source address filtering, which blocks all incoming packets to that interface. To enable the filtering, include the source-filtering statement at the [edit interfaces interface-name aggregated-ether-options], [edit interfaces interface-name fastether-options], or [edit interfaces interface-name gigether-options] hierarchy level:

```
source-filtering;
```

This method of MAC address filtering is not supported on Gigabit Ethernet QPP interfaces. For more information, see "Configure Gigabit Ethernet QPP MAC Address Filtering" on page 270.

To explicitly disable filtering, include the no-source-filtering statement at the [edit interfaces interface-name aggregated-ether-options], [edit interfaces interface-name fastether-options], or [edit interfaces interface-name gigether-options] hierarchy level:

```
no-source-filtering;
```

When source address filtering is enabled, you can configure the interface to receive packets from specific MAC addresses. To do this, specify the MAC addresses in the source-address-filter statement at the [edit interfaces interface-name aggregated-ether-options], [edit interfaces interface-name fastether-options], or [edit interfaces interface-name gigether-options] hierarchy level:

```
source-address-filter {
  mac-address;
  <additional-mac-address;>
}
```

For Gigabit Ethernet QPP interfaces, you do this by including the accept-source-mac statement at the [edit interfaces interface-name unit logical-unit-number] hierarchy level:

```
[edit interfaces interface-name unit logical-unit-number]
accept-source-mac {
  mac-address mac-address {
    policer {
      input policer-name;
      output policer-name;
    }
  }
}
```

For more information, see "Configure Gigabit Ethernet QPP MAC Address Filtering" on page 270.

You can specify the MAC address as **nn:nn:nn:nn:nn:nn** or **nnnn:nnnn:nnnn**, where **n** is a hexadecimal number. To specify more than one address, include multiple mac-address statements in the source-address-filter statement.
If the remote Ethernet card is changed, the interface will not be able to receive packets from the new card because it will have a different MAC address.

**Note**
Support for source address filters is limited on the Fast Ethernet 12-port and 48-port PIC interfaces.

### Configure Ethernet Loopback Capability

By default, local aggregated Ethernet, Fast Ethernet, Gigabit Ethernet, and 10-Gigabit Ethernet interfaces connect to a remote system. To place an interface in loopback mode, include the `loopback` statement at the `[edit interfaces interface-name aggregated-ether-options]`, `[edit interfaces interface-name fastether-options]`, or `[edit interfaces interface-name gigether-options]` hierarchy level:

```
loopback;
```

To return to the default—that is, to disable loopback mode—delete the `loopback` statement from the configuration:

```
[edit]
user@host# delete interfaces fe-fpc/pic/port fastether-options loopback
```

To explicitly disable loopback mode, include the `no-loopback` statement at the `[edit interfaces interface-name aggregated-ether-options]`, `[edit interfaces interface-name fastether-options]`, or `[edit interfaces interface-name gigether-options]` hierarchy level:

```
no-loopback;
```

### Configure Flow Control

By default, the router imposes flow control to regulate the amount of traffic sent out a Fast Ethernet, Gigabit Ethernet, and 10-Gigabit Ethernet interface. This is useful if the remote side of the connection is a Fast Ethernet or Gigabit Ethernet switch.

You can disable flow control if you want the router to permit unrestricted traffic. To disable flow control, include the `no-flow-control` statement at the `[edit interfaces interface-name aggregated-ether-options]`, `[edit interfaces interface-name fastether-options]`, or `[edit interfaces interface-name gigether-options]` hierarchy level:

```
no-flow-control;
```

To explicitly reinstate flow control, include the `flow-control` statement at the `[edit interfaces interface-name aggregated-ether-options]`, `[edit interfaces interface-name fastether-options]`, or `[edit interfaces interface-name gigether-options]` hierarchy level:

```
flow-control;
```
Configure the Link Characteristics

By default, the router’s management Ethernet interface, fxp0, autonegotiates whether to operate in full-duplex or half-duplex mode. Fast Ethernet interfaces can operate in either full-duplex or half-duplex mode, and all other interfaces can operate only in full-duplex mode. For Gigabit Ethernet and 10-Gigabit Ethernet, the link partner must also be set to full duplex.

To explicitly configure an Ethernet interface to operate in either full-duplex or half-duplex mode, include the link-mode statement at the [edit interfaces interface-name] hierarchy level:

```
[edit interfaces interface-name]
link-mode (full-duplex | half-duplex);
```

Configure Gratuitous ARP

Gratuitous ARP requests provide duplicate IP address detection. A gratuitous ARP request is a broadcast request for a router’s own IP address. If a router sends an ARP request for its own IP address and no ARP replies are received, the router’s assigned IP address is not being used by other nodes. If a router sends an ARP request for its own IP address and an ARP reply is received, the router’s assigned IP address is already being used by another node.

By default, the router responds to gratuitous ARP requests. On Ethernet interfaces, you can disable responses to gratuitous ARP requests. To disable responses to gratuitous ARP requests, include the no-gratuitous-arp-request statement at the [edit interfaces interface-name] hierarchy level:

```
[edit interfaces interface-name]
no-gratuitous-arp-request;
```

To return to the default—that is, to respond to gratuitous ARP requests—delete the no-gratuitous-arp-request statement from the configuration:

```
[edit]
user@host# delete interfaces interface-name no-gratuitous-arp-request
```

Gratuitous ARP replies are reply packets sent to the broadcast MAC address with the target IP address set to be the same as the sender’s IP address. When the router receives a gratuitous ARP reply, the router can insert an entry for that reply in the ARP cache.

By default, updating the ARP cache on gratuitous ARP replies is disabled on the router. On Ethernet interfaces, you can enable handling of gratuitous ARP replies on a specific interface by including the gratuitous-arp-reply statement at the [edit interfaces interface-name] hierarchy level:

```
[edit interfaces interface-name]
gratuitous-arp-reply;
```

To restore the default behavior, include the no-gratuitous-arp-reply statement at the [edit interfaces interface-name] hierarchy level:

```
[edit interfaces interface-name]
no-gratuitous-arp-reply;
```
Configure 802.1Q VLANs

Configure the Interface Speed

On Fast Ethernet 12-port and 48-port PIC interfaces and the management Ethernet interface (fxp0) only, you can explicitly set the interface speed to either 10 Mbps or 100 Mbps.

To explicitly configure the speed on an interface, include the `speed` statement at the `edit interfaces interface-name` hierarchy level:

```
[edit interfaces interface-name]
speed (10m | 100m);
```

Configure the Ingress Rate Limit

On Fast Ethernet 8-port, 12-port, and 48-port PIC interfaces only, you can apply port-based rate limiting to the ingress traffic that arrives at the PIC.

To configure an ingress rate limit on a Fast Ethernet 8-port, 12-port, or 48-port PIC interface, include the `ingress-rate-limit` statement at the `edit interfaces interface-name fastether-options` hierarchy level:

```
[edit interfaces interface-name fastether-options]
ingress-rate-limit rate;
```

rate can range in value from 1 through 100 Mbps.

Configure 802.1Q VLANs

For Ethernet, Fast Ethernet, Gigabit Ethernet, and 10-Gigabit Ethernet interfaces, the JUNOS software supports a subset of the IEEE 802.1Q standard for channelizing an Ethernet interface into multiple logical interfaces, allowing many hosts to be connected to the same Gigabit Ethernet switch, but preventing them from being in the same routing or broadcast domain.

You can configure the following 802.1Q VLAN properties:

- Enable VLAN Tagging on page 283
- Configure VLAN CCC or VPLS Encapsulation on page 284
- Configure Extended VLAN CCC or VLAN VPLS Encapsulation on page 285

For examples of 802.1Q VLAN configuration, see the following sections:

- Example: Configure VLAN CCC or VPLS Encapsulation on page 284
- Example: Configure Extended VLAN CCC or VLAN VPLS Encapsulation on page 285
Enable VLAN Tagging

The JUNOS software supports receiving and forwarding routed Ethernet frames with 802.1Q virtual local area network (VLAN) tags, and running Virtual Router Redundancy Protocol (VRRP) over 802.1Q-tagged interfaces. To configure the router to receive and forward frames with 802.1Q VLAN tags, include the `vlan-tagging` statement at the `[edit interfaces interface-name]` hierarchy level:

```
[edit interfaces interface-name]
  vlan-tagging;
```

Gigabit Ethernet interfaces can be partitioned; you can assign up to 4095 different logical interfaces, one for each VLAN, but you are limited to a maximum of 1024 VLANs on any single Gigabit Ethernet or 10-Gigabit Ethernet port; and you are limited to a maximum of 384 (383 for tagged and 1 for untagged VLANs) on any single Gigabit Ethernet QPP port. Fast Ethernet interfaces can also be partitioned, with a maximum of 1024 logical interfaces for the 4-port Fast Ethernet PIC, and 16 logical interfaces for the 8-port, 12-port, and 48-port Fast Ethernet PICs. Table 23 lists VLAN ID range by interface type.

### Table 23: VLAN ID Range by Interface Type

<table>
<thead>
<tr>
<th>Interface Type</th>
<th>VLAN ID Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aggregated Ethernet</td>
<td>1 through 1023</td>
</tr>
<tr>
<td>4-port, 8-port, and 12-port Fast Ethernet</td>
<td>1 through 1023</td>
</tr>
<tr>
<td>48-port Fast Ethernet</td>
<td>1 through 4094</td>
</tr>
<tr>
<td>Gigabit Ethernet</td>
<td>1 through 4094</td>
</tr>
<tr>
<td>Gigabit Ethernet QPP</td>
<td>1 through 4094</td>
</tr>
<tr>
<td>10-Gigabit Ethernet</td>
<td>1 through 4094</td>
</tr>
<tr>
<td>Management and internal Ethernet interfaces</td>
<td>1 through 1023</td>
</tr>
</tbody>
</table>

VLAN ID 0 is reserved for tagging the priority of frames. To bind a VLAN ID to a logical interface, include the `vlan-id` statement at the `[edit interfaces interface-name unit logical-unit-number]` hierarchy level:

```
[edit interfaces interface-name unit logical-unit-number]
  vlan-id number;
```

Because IS-IS has an 8-bit limit for broadcast multiaccess media, you cannot set up more than 255 adjacencies over Gigabit Ethernet using VLAN tagging. For more information about IS-IS capabilities, see the JUNOS Internet Software Configuration Guide: Routing and Routing Protocols.
Configure VLAN CCC or VPLS Encapsulation

Ethernet interfaces with VLAN tagging enabled can use VLAN circuit cross-connect (CCC) or VLAN Virtual Private LAN Service (VPLS) encapsulation. To configure the encapsulation on a physical interface, include the encapsulation statement at the [edit interfaces interface-name] hierarchy level, specifying vlan-ccc or vlan-vpls:

```
[edit interfaces interface-name]
encapsulation (vlan-ccc | vlan-vpls);
```

Ethernet interfaces in VLAN mode can have multiple logical interfaces, but in CCC and VPLS modes VLAN IDs from 1 through 511 are reserved for normal VLANs, and VLAN IDs 512 and up are reserved for CCC VLANs.

In general, you configure an interface's encapsulation at the [edit interfaces interface-name] hierarchy level. However, for some encapsulation types, including Ethernet VLAN CCC and VLAN VPLS, you can also configure the encapsulation type that is used inside the VLAN circuit itself. To do this, include the encapsulation statement at the [edit interfaces interface-name unit logical-unit-number] hierarchy level:

```
[edit interfaces interface-name unit logical-unit-number]
encapsulation (vlan-ccc | vlan-vpls);
```

You cannot configure a logical interface with VLAN CCC or VLAN VPLS encapsulation unless you also configure the physical device with the same encapsulation. The logical interface must have a VLAN ID in the range from 512 or higher; if the VLAN ID is 511 or lower, it will be subject to the normal destination filter lookups in addition to source address filtering.

Example: Configure VLAN CCC or VPLS Encapsulation

Configure VLAN CCC encapsulation on a Gigabit Ethernet interface:

```
interfaces ge-2/1/0 {
  vlan-tagging;
  encapsulation vlan-ccc;
  unit 0 {
    encapsulation vlan-ccc;
    vlan-id 600;
  }
}
```
Configure Extended VLAN CCC or VLAN VPLS Encapsulation

Gigabit Ethernet and four-port Fast Ethernet interfaces with VLAN tagging enabled can use extended VLAN circuit cross-connect (CCC) or VLAN Virtual Private LAN Service (VPLS), which allow 802.1Q tagging. To configure the encapsulation on a physical interface, include the encapsulation statement at the [edit interfaces interface-name] hierarchy level, specifying extended-vlan-ccc or extended-vlan-vpls:

[edit interfaces interface-name]
encapsulation (extended-vlan-ccc | extended-vlan-vpls);

For extended VLAN CCC and extended VLAN VPLS encapsulation, all VLAN IDs 1 and higher are valid. VLAN ID 0 is reserved for tagging the priority of frames.

Example: Configure Extended VLAN CCC or VLAN VPLS Encapsulation

Configure extended VLAN CCC encapsulation on Gigabit Ethernet ingress and egress interfaces:

interfaces ge-0/0/0 {
    vlan-tagging;
    encapsulation extended-vlan-ccc;
    unit 0 {
        vlan-id 2;
        family ccc;
    }
}

interfaces ge-1/0/0 {
    vlan-tagging;
    encapsulation extended-vlan-ccc;
    unit 0 {
        vlan-id 2;
        family ccc;
    }
}

For extended VLAN CCC, the VLAN IDs on ingress and egress interfaces must be the same. For back-to-back connections, all VLAN IDs must be the same.
Configure TCC and Layer 2.5 Switching

Translational cross-connect (TCC) is a switching concept that allows you to establish interconnections between a variety of Layer 2 protocols or circuits. It is similar to its predecessor, circuit cross-connect (CCC). However, while CCC requires the same Layer 2 encapsulations on both sides of a router (such as PPP-to-PPP or Frame Relay-to-Frame Relay), TCC lets you connect different types of Layer 2 protocols interchangeably. With TCC, combinations such as PPP-to-ATM and Ethernet-to-Frame Relay cross-connections are possible.

You can configure the following Layer 2.5 switching properties:

- Configure Extended VLAN TCC Encapsulation on page 286
- Configure an Ethernet TCC or Extended VLAN TCC on page 287

For examples of Layer 2.5 switching configuration, see the following sections:

- Example: Configure an Ethernet TCC or Extended VLAN TCC on page 287
- Example: Configure Extended VLAN CCC or VLAN VPLS Encapsulation on page 285

Configure Extended VLAN TCC Encapsulation

One-port Gigabit Ethernet, two-port Gigabit Ethernet, and four-port Fast Ethernet PICs with VLAN tagging enabled can use extended VLAN TCC encapsulation, which allows circuits to have different media on either side of the connection. To configure the encapsulation on a physical interface, include the encapsulation extended-vlan-tcc statement at the [edit interfaces interface-name] hierarchy level:

```
[edit interfaces interface-name]
encapsulation extended-vlan-tcc;
```

For extended VLAN TCC encapsulation, all VLAN IDs from 1 through 1024 are valid. VLAN ID 0 is reserved for tagging the priority of frames.

Extended VLAN TCC is not supported on four-port Gigabit Ethernet PICs.
Configure an Ethernet TCC or Extended VLAN TCC

For Layer 2.5 VPNs employing an Ethernet interface as the TCC router, you can configure an Ethernet TCC or an extended VLAN TCC.

To configure an Ethernet TCC, include the `encapsulation ethernet-tcc` statement at the `[edit interfaces interface-name] hierarchy level. To configure an extended VLAN TCC, include the `encapsulation extended-vlan-tcc` statement at the `[edit interfaces interface-name] hierarchy level:

```
[edit interfaces interface-name]
encapsulation (ethernet-tcc | extended-vlan-tcc);
```

To configure an Ethernet TCC or an extended VLAN TCC, include the proxy and remote statements at the `[edit interfaces interface-name unit logical-unit-number family tcc] hierarchy level:

```
[edit interfaces interfaces interface-name unit logical-unit-number family tcc]
proxy {
  inet-address address;
}
remote {
  (inet-address address | mac-address address);
}
```

The proxy address is the IP address of the non-Ethernet TCC neighbor for which the TCC router is acting as a proxy.

The remote address is the IP or MAC address of the remote router. The remote statement provides ARP capability from the TCC switching router to the Ethernet neighbor. The MAC address is the physical Layer 2 address of the Ethernet neighbor, also known as the remote router.

Ethernet TCC is supported on interfaces that carry IPv4 traffic only. Ethernet TCC encapsulation is supported on one-port Gigabit Ethernet, two-port Gigabit Ethernet, four-port Gigabit Ethernet, and four-port Fast Ethernet PICs only.

Example: Configure an Ethernet TCC or Extended VLAN TCC

Configure a full-duplex Layer 2.5 translational cross-connect between Router A and Router C, using a Juniper Networks router, Router B, as the TCC interface. Ethernet TCC encapsulation provides an Ethernet wide area circuit for interconnecting IP traffic. (See the topology in Figure 21.)

The Router A-to-Router B circuit is PPP, and the Router B-to-Router C circuit accepts packets carrying standard TPID values.

If traffic flows from Router A to Router C, the JUNOS software strips all PPP encapsulation data from incoming packets and adds Ethernet encapsulation data before forwarding the packets. If traffic flows from Router C to Router A, the JUNOS software strips all Ethernet encapsulation data from incoming packets and adds PPP encapsulation data before forwarding the packets.
Configure an Extended VLAN TCC

Configure a full-duplex Layer 2.5 translational cross-connect between Router A and Router C, using a Juniper Networks router, Router B, as the TCC interface. Extended VLAN TCC encapsulation provides an Ethernet wide area circuit for interconnecting IP traffic. (See the topology in Figure 21).

The Router A-to-Router B circuit is PPP, and the Router B-to-Router C circuit is Ethernet with VLAN tagging enabled.

On Router B

```
interfaces ge-0/0/0 {
    vlan-tagging;
    encapsulation extended-vlan-tcc;
    unit 0 {
        vlan-id 1;
        family tcc {
            proxy {
                inet-address 10.10.10.3/24;
            }
            remote {
                inet-address 10.10.10.2/24;
            }
        }
    }
}
```
Configure Static ARP Table Entries

For Ethernet, Fast Ethernet, Gigabit Ethernet, and 10-Gigabit Ethernet interfaces, you can configure static ARP table entries, defining mappings between IP and MAC addresses. To configure static ARP table entries, include the arp statement at the [edit interfaces interface-name unit logical-unit-number family inet address address] hierarchy level:

[edit interfaces interface-name unit logical-unit-number family inet address address]
arp ip-address (mac | multicast-mac) mac-address <publish>;

The IP address that you specify must be part of the subnet defined in the enclosing address statement.

To associate a multicast MAC address with a unicast IP address, include the multicast-mac statement.

Specify the MAC address as six hexadecimal bytes in one of the following formats: nnnn.nnnn.nnnn or nn:nn:nn:nn:nn:nn. For example, 0011.2233.4455 or 00:11:22:33:44:55.

For unicast MAC addresses only, if you include the publish option, the router replies to proxy ARP requests.

By default, an ARP policer is installed that is shared among all the Ethernet interfaces on which you have configured the family inet statement. By including the arp statement at the [edit interfaces interface-name unit logical-unit-number family inet policer] hierarchy level, you can apply a specific ARP-packet policer to an interface. For more information, see “Apply Policers” on page 87.

Example: Configure Static ARP Table Entries

Configure two static ARP table entries on the router’s management interface:

[edit interfaces]
fxp0 {
  unit 0 {
    family inet {
      address 10.10.0.11/24 {
        arp 10.10.0.99 mac 0001.0002.0003;
        arp 10.10.0.101 mac 00:11:22:33:44:55 publish;
      }
    }
  }
}
Configure VRRP

For Ethernet, Fast Ethernet, Gigabit Ethernet, and 10-Gigabit Ethernet interfaces, you can configure the Virtual Router Redundancy Protocol (VRRP). VRRP allows hosts on a LAN to make use of redundant routers on that LAN without requiring more than the static configuration of a single default route on the hosts. The VRRP routers share the IP address corresponding to the default route configured on the hosts. At any time, one of the VRRP routers is the master (active) and the others are backups. If the master fails, one of the backup routers becomes the new master, thus always providing a virtual default router and allowing traffic on the LAN to be routed without relying on a single router.

VRRP is defined in RFC 2338, Virtual Router Redundancy Protocol.

To configure VRRP, include the vrrp-group statement at the [edit interfaces interface-name unit logical-unit-number family inet address address ] hierarchy level:

[edit interfaces interface-name unit logical-unit-number family inet address address ]
 vrrp-group group-number {
  (accept-data | no-accept-data);
  advertise-interval seconds;
  authentication-key key;
  authentication-type authentication;
  (preempt | no-preempt);
  priority number;
  track {
    interface interface-name priority-cost cost;
    virtual-address [ addresses ];
  }
}

To trace VRRP operations, include the traceoptions statement at the [edit protocols vrrp] hierarchy level:

[edit protocols vrrp traceoptions]
file {
  filename filename;
  files number;
  size size;
  (world-readable | no-world-readable);
}
flag flag;

For more information, see “Trace VRRP Operations” on page 295.
You can configure the following VRRP properties:

- Configure Basic VRRP Support on page 291
- Configure VRRP Authentication on page 292
- Configure the Advertisement Interval for the VRRP Master Router on page 293
- Configure a Backup Router to Preempt the Master Router on page 293
- Accept Packets Destined for the Virtual IP Address on page 294
- Configure a Logical Interface to Be Tracked on page 295
- Trace VRRP Operations on page 295

For a VRRP configuration example, see “Example: Configure VRRP” on page 296.

Configure Basic VRRP Support

To configure basic VRRP support, configure VRRP groups on interfaces by including the following statements at the [edit interfaces interface-name unit logical-unit-number family inet address address] hierarchy level:

```
[edit interfaces interface-name unit logical-unit-number family inet address address]
vrp-group group-number {
    priority number;
    virtual-address [ addresses ];
}
```

An interface can be a member of one or more VRRP groups. On a single router, you cannot configure the same VRRP group on multiple interfaces. For each group, you must configure the following:

- Group number—Identifies the VRRP group. It can be a value from 0 through 255.

If you also enable MAC source address filtering on the interface, as described in “Configure Ethernet MAC Address Filtering” on page 279, you must include the virtual MAC address in the list of source MAC addresses that you specify in the source-address-filter statement. MAC addresses ranging from 00:00:5e:00:01:00 through 00:00:5e:00:01:ff are reserved for VRRP, as defined in RFC 2338. The VRRP group number must be the decimal equivalent of the last hexadecimal byte of the virtual MAC address.
Configure VRRP

Addresses of one or more virtual routers that are members of the VRRP group—Virtual IP addresses associated with the virtual router in the VRRP group. Normally, you configure only one virtual IP address per group. The virtual IP addresses must be the same for all routers in the VRRP group. You can configure up to eight addresses.

In the addresses, specify the address only. Do not include a prefix length.

If you configure a virtual IP address to be the same as the interface’s address (the address configured with the address statement), the interface becomes the master virtual router for the group. In this case, you must configure the priority to be 255 and you must configure preemption by including the preempt statement. If you have multiple VRRP groups on an interface, the interface can be the master virtual router for only one of the groups.

If the virtual IP address you choose is not the same as the interface’s address, you must ensure that this address does not appear anywhere else in the router’s configuration. Check that you do not use this address for other interfaces, for the IP address of a tunnel, or for the IP address of static ARP entries.

Priority for this router to become the master virtual router—Value used to elect the master virtual router in the VRRP group. It can be a number from 1 through 255. The default value for backup routers is 100. A larger value indicates a higher priority. The router with the highest priority within the group becomes the master router.

Within a single VRRP group, the master and backup routers cannot be the same router.

Configure VRRP Authentication

All VRRP protocol exchanges can be authenticated to guarantee that only trusted routers participate in the AS’s routing. By default, VRRP authentication is disabled. You can configure one of the following authentication methods; each VRRP group must use the same method:

- Simple authentication—Uses a text password included in the transmitted packet. The receiving router uses an authentication key (password) to verify the packet.

- MD5 algorithm—Creates the authentication data field in the IP authentication header. This header is used to encapsulate the VRRP protocol data unit (PDU). The receiving router uses an authentication key (password) to verify the authenticity of the IP authentication header and VRRP PDU.

To enable authentication and specify an authentication method, include the authentication-type statement at the [edit interfaces interface-name unit logical-unit-number family inet address address vrrp-group group-number] hierarchy level:

[edit interfaces interface-name unit logical-unit-number family inet address address vrrp-group group-number] authentication-type authentication;

authentication can be none, simple, or md5. The authentication type must be the same for all routers in the VRRP group.
If you included the authentication-type statement to select an authentication method, you can configure a key (password) on each interface by including the authentication-key statement at the [edit interfaces interface-name unit logical-unit-number family inet address address vrrp-group group-number] hierarchy level:

```
[edit interfaces interface-name unit logical-unit-number family inet address address vrrp-group group-number]
advertising-key key;
```

The key (password) is an ASCII string. For simple authentication, it can be 1 through 8 characters long. For MD-5 authentication, it can be 1 through 16 characters long. If you include spaces, enclose all characters in quotation marks (" "). The key must be the same for all routers in the VRRP group.

### Configure the Advertisement Interval for the VRRP Master Router

By default, the master router sends VRRP advertisement packets every second to all members of the VRRP group. These packets indicate that the master router is still operational. If the master router fails or becomes unreachable, the backup router with the highest priority value becomes the new master router.

To modify the time between the sending of VRRP advertisement packets, include the advertise-interval statement at the [edit interfaces interface-name unit logical-unit-number family inet address address vrrp-group group-number] hierarchy level:

```
[edit interfaces interface-name unit logical-unit-number family inet address address vrrp-group group-number]
advertise-interval seconds;
```

The interval can range from 1 through 255 seconds. The interval must be the same for all routers in the VRRP group.

### Configure a Backup Router to Preempt the Master Router

By default, a higher priority backup router preempts a lower priority master router. To explicitly allow the master router to be preempted, include the preempt statement at the [edit interfaces interface-name unit logical-unit-number family inet address address vrrp-group group-number] hierarchy level:

```
[edit interfaces interface-name unit logical-unit-number family inet address address vrrp-group group-number]
preempt;
```

To prohibit a higher priority backup router from preempting a lower priority master router, include the no-preempt statement at the [edit interfaces interface-name unit logical-unit-number family inet address address vrrp-group group-number] hierarchy level:

```
[edit interfaces interface-name unit logical-unit-number family inet address address vrrp-group group-number]
no-preempt;
```
Accept Packets Destined for the Virtual IP Address

To configure an interface to accept packets destined for the virtual IP address, include the `accept-data` statement at the `[edit interfaces interface-name unit logical-unit-number family inet address address vrrp-group group-number]` hierarchy level:

```
[edit interfaces interface-name unit logical-unit-number family inet address address vrrp-group group-number]
accept-data;
```

To prohibit the interface from accepting packets destined for the virtual IP address, include the `no-accept-data` statement at the `[edit interfaces interface-name unit logical-unit-number family inet address address vrrp-group group-number]` hierarchy level:

```
[edit interfaces interface-name unit logical-unit-number family inet address address vrrp-group group-number]
no-accept-data;
```

The `accept-data` statement has the following consequences:

- You do not need to include the `accept-data` statement to activate this feature if the master router owns the virtual IP address.
- If you do not include the `accept-data` statement, and if the master router owns the virtual IP address, the master router responds to ICMP message requests only.
- You cannot include the `accept-data` statement when the priority of the master router is set to 255.
- To restrict incoming IP packets to ICMP only, you must configure firewall filters to accept only ICMP packets.
- If you include the `accept-data` statement, your router configuration will not comply with RFC 2338.
- If you include the `accept-data` statement, VRRP clients should be able to process Gratuitous ARP.
- If you include the `accept-data` statement, VRRP clients should not use packets other than ARP replies to update their ARP cache.
Configure a Logical Interface to Be Tracked

VRRP can track whether a logical interface is up, down, or not present and dynamically change the priority of the VRRP group based on the state of the tracked logical interface, which might trigger a new master router election.

When interface tracking is enabled, you cannot configure a priority of 255, thereby designating the master router. For each VRRP group, you can track up to 10 logical interfaces.

To configure a logical interface to be tracked, include the track statement at the [edit interfaces interface-name unit logical-unit-number family inet address address vrrp-group group-number] hierarchy level:

```plaintext
[edit interfaces interface-name unit logical-unit-number family inet address address vrrp-group group-number]
track {
  interface interface-name priority-cost cost;
}
```

The priority cost is the value to be subtracted from the configured VRRP priority when the tracked logical interface is down, forcing a new master router election. The value can range from 1 through 254. The sum of the costs for all tracked logical interfaces or routes must be less than or equal to the configured priority of the VRRP group.

Trace VRRP Operations

To trace VRRP operations, include the traceoptions statement at the [edit protocols vrrp] hierarchy level.

By default, VRRP logs the error, DCD configuration, and routing socket events in a file in the /var/log directory. By default, this file is named /var/log/vrrpd. The default file size is 1MB, and three files are created before the first one gets overwritten.

To change the configuration of the logging file, include the file statement at the [edit protocols vrrp traceoptions] hierarchy level:

```plaintext
[edit protocols vrrp traceoptions]
file {
  filename filename;
  files number;
  size size;
  (world-readable | no-world-readable);
}
flag flag;
```

You can specify the following VRRP tracing flags:

- **all**—Trace all VRRP operations.
- **database**—Trace all database changes.
- **general**—Trace all general events.
- **interfaces**—Trace all interface changes.
- **normal**—Trace all normal events.
Example: Configure VRRP

Configure one master (Router A) and one backup (Router B) router. Note that the address configured in the `virtual-address` statements differs from the addresses configured in the `address` statements.

On Router A

```
[edit]
interfaces {
  ge-0/0/0 {
    unit 0 {
      family inet {
        address 192.168.1.20/24 {
          vrrp-group 27 {
            virtual-address 192.168.1.15;
            priority 254;
            authentication-type simple;
            authentication-key boojum;
          }
        }
      }
    }
  }
}
```

On Router B

```
[edit]
interfaces {
  ge-4/2/0 {
    unit 0 {
      family inet {
        address 192.168.1.24/24 {
          vrrp-group 27 {
            virtual-address 192.168.1.15;
            priority 200;
            authentication-type simple;
            authentication-key boojum;
          }
        }
      }
    }
  }
}
```
When configuring multiple VRRP groups on an interface, configure one to be the master virtual router for that group.

```conf
e[edit]
  interfaces {
    ge-0/0/0 {
      unit 0 {
        family inet {
          address 192.168.1.20/24 {
            vrrp-group 2 {
              virtual-address 192.168.1.20;
              priority 255;
              announce-interval 3;
              preempt;
            }
            vrrp-group 10 {
              virtual-address 192.168.1.55;
              priority 201;
              announce-interval 3;
            }
            vrrp-group 1 {
              virtual-address 192.168.1.54;
              priority 22;
              announce-interval 4;
            }
          }
        }
      }
    }
  }
```

Configure VRRP and MAC source address filtering:

The VRRP group number is the decimal equivalent of the last byte of the virtual MAC address.

```conf
e[edit interfaces]
  ge-5/2/0 {
    gigether-options {
      source-filtering;
      source-address-filter {
        00:00:5e:00:01:0a;<!-- Virtual MAC address}
      }
    }
    unit 0 {
      family inet {
        address 192.168.1.10/24 {
          vrrp-group 10 {-- VRRP group number
            virtual-address 192.168.1.10;
            priority 255;
            preempt;
          }
        }
      }
    }
  }
```

Configure Ethernet Interfaces 297
Configure the Management Ethernet Interface

The router’s management Ethernet interface, fxp0, is an out-of-band management interface. You must configure an IP address and prefix length for this interface, which you commonly do when you first install the JUNOS software:

```
[edit]
user@host# set interfaces fxp0 unit 0 family inet address/ prefix-length
[edit]
user@host# show
interfaces {
  fxp0 {
    unit 0 {
      family inet {
        address/ prefix-length;
      }
    }
  }
}
```

The management Ethernet interface must be configured for the router to function.

Configure the MAC Address on the Management Ethernet Interface

By default, the router’s management Ethernet interface (fxp0) uses as its MAC address the MAC address that is burned into the Ethernet card. To display this address, enter the show interface fxp0 operational mode command.

To change the management Ethernet interface’s MAC address, include the mac statement at the [edit interfaces fxp0] hierarchy level:

```
[edit interfaces fxp0]
mac mac-address;
```

Specify the MAC address as six hexadecimal bytes in one of the following formats: nnnn.nnnn.nnnn (for example, 0011.2233.4455) or nn:nn:nn:nn:nn:nn (for example, 00:11:22:33:44:55).
Configure the Internal Ethernet Interface

The internal Ethernet interface, fxp1, connects the Routing Engine with the System Control Board (SCB), System and Switch Board (SSB), Forwarding Engine Board (FEB), or Switching and Forwarding Module (SFM), depending on router model, in the Packet Forwarding Engine. The router software automatically configures this interface.

**Caution**

Do not modify or remove the configuration for the internal Ethernet interface that the JUNOS software automatically configures. If you do, the router will stop functioning.

```
user@host> show configuration
...
interfaces {
...
fxp1 {
  unit 0 {
    family tnp {
      address 1;
    }
  }
}
...
```

Configure Aggregated Ethernet Interfaces

Link aggregation of Ethernet interfaces is defined in the IEEE 802.3ad standard. The JUNOS implementation of 802.3AD balances traffic across the member links within an aggregated Ethernet bundle based on the Layer 3 information carried in the packet. This implementation uses the same load balancing algorithm used for per-packet load balancing. For information about per-packet load balancing, see the JUNOS Internet Software Guide: Routing and Routing Protocols.

**Note**

The JUNOS software does not provide load balancing for multicast traffic on aggregated interfaces. If a link carrying multicast data goes down, another link carries the traffic. This provides redundancy, not more bandwidth.

The JUNOS software does not support the Link Aggregation Control Protocol (LACP).

You configure an aggregated Ethernet virtual link by specifying the link number as a physical device and then associating a set of ports that have the same speed and are in full-duplex mode. The physical interfaces can be either Fast Ethernet, Gigabit Ethernet, or 10-Gigabit Ethernet devices; however, do not use a combination of these within the same aggregated link.
To specify aggregated Ethernet interfaces, include the `vlan-tagging` statement at the `[edit interfaces ae]` hierarchy level and include the `vlan-id` statement at the `[edit interfaces ae unit logical-unit-number]` hierarchy level, as in the following example:

```
[edit interfaces]
ae0 {
    vlan-tagging;
    unit 0 {
        vlan-id 100;
        family inet {
            address 10.1.1.1/24;
        }
    }
}
```

By default, no aggregated Ethernet interfaces are created. You must define the number of aggregated Ethernet interfaces by including the `device-count` statement at the `[edit chassis aggregated-devices ethernet]` hierarchy level:

```
[edit chassis]
aggregated-devices {
    ethernet {
        device-count number;
    }
}
```

The maximum number of aggregated interfaces is 16, and the assigned number can range from 0 through 15. For information about configuring aggregated devices, see the JUNOS Internet Software Configuration Guide: Getting Started.

You must also specify the constituent physical links by including the `802.3ad` statement at the `[edit interfaces interface-name fastether-options]` or `[edit interfaces interface-name gigether-options]` hierarchy level; for more information, see “Configure Ethernet Link Aggregation” on page 266. You can optionally specify other physical properties that apply specifically to the aggregated Ethernet interfaces; for details, see “Configure Ethernet Physical Interface Properties” on page 264. For a sample configuration, see “Example: Configure Aggregated Ethernet Interfaces” on page 302.

To delete an aggregated Ethernet interface from the configuration, issue the `delete interfaces ae` command at the `[edit]` hierarchy level in configuration mode:

```
[edit]
user@host# delete interfaces ae
```

If you delete an aggregated Ethernet interface from the configuration, the JUNOS software removes the configuration statements related to `ae` and sets this interface to down state. However, the aggregated Ethernet interface is not deleted until you delete the `chassis aggregated-devices ethernet device-count` configuration statement.
Example: Configure Fast Ethernet Interfaces

The following configuration is sufficient to get a Fast Ethernet interface up and running. By default, IPv4 Fast Ethernet interfaces use 802.3 encapsulation.

```conf
[edit]
user@host# set interfaces fe-fpc/ pic/ port unit 0 family inet address local-address
user@host# show interfaces {
  fe-fpc/ pic/ port {
    unit 0 {
      family inet {
        address local-address;
      }
    }
  }
}
```

Example: Configure Gigabit Ethernet Interfaces

The following configuration is sufficient to get a Gigabit Ethernet or 10-Gigabit Ethernet interface up and running. By default, IPv4 Gigabit Ethernet interfaces use 802.3 encapsulation.

```conf
[edit]
user@host# set interfaces ge-fpc/ pic/ port unit 0 family inet address local-address
user@host# show interfaces {
  ge-fpc/ pic/ port {
    unit 0 {
      family inet {
        address local-address;
      }
    }
  }
}
```

The M160, T320, and T640 two-port Gigabit Ethernet PIC supports two independent Gigabit Ethernet links. This PIC is supported on the M160, T320, and T640 platforms only and it requires a Type 2 M160, Type 2 T320, or Type 2 T640 FPC.

Each of the two interfaces on the PIC is named:

```
ge-fpc/ pic/ [0.1]
```

Each of these interfaces has functionality identical to the Gigabit Ethernet interface supported on the single-port PIC.
Example: Configure Aggregated Ethernet Interfaces

The following set of configurations is sufficient to get an aggregated Gigabit Ethernet interface up and running.

```
[edit interfaces]
ea0 {
  vlan-tagging;
  unit 0 {
    vlan-id 100;
    family inet {
      address 10.1.1.1/24;
    }
  }
}

[edit chassis]
aggregated-devices {
  ethernet {
    device-count 15;
  }
}

[edit interfaces]
ge-1/3/0 {
  gigether-options {
    802.3ad ae0;
  }
}

[edit interfaces ae0]
aggregated-ether-options {
  link-speed 1g;
  minimum-links 5;
}
```
Chapter 22
Configure Frame Relay

The Frame Relay protocol allows network designers to reduce costs by using shared facilities that are managed by a Frame Relay service provider. Users pay fixed charges for the local connections from each site in the Frame Relay network to the first Point of Presence (POP) in which the provider maintains a Frame Relay switch. The portion of the network between the end point switches is shared by all the customers of the service provider, and individual Data-Link Connection Identifiers (DLCIs) are assigned to ensure each customer receives only their own traffic.

Users contract with their providers for a specific minimum portion of the shared bandwidth Committed Information Rate (CIR) and for a maximum allowable peak rate, Burst Information Rate (BIR). Depending on the terms of the contract, traffic exceeding the CIR can be marked as eligible for discard, in the event of network congestion, or a best effort term can apply up to the BIR rate.

Frame Relay does not require private and permanently connected Wide Area Network facilities, unlike some older WAN protocols.

Frame Relay was developed as a replacement for the older and much slower X.25 protocol. It scales to much higher data rates because it does not require explicit acknowledgment of each frame of data.

You can configure the Frame Relay protocol on SONET/SDH, E1/E3, and T1/T3 physical router interfaces, and on the Channelized DS-3, Channelized OC-12, Channelized T3 QPP, Channelized OC-12 QPP, and Channelized E1 QPP interfaces.

This chapter discusses configuration of the following Frame Relay properties:

- Configure Frame Relay Interface Encapsulation on page 304
- Configure the Media MTU on page 306
- Set the Protocol MTU on page 306
- Configure Frame Relay Keepalives on page 307
- Configure Inverse Frame Relay ARP on page 308
- Configure the Router as a DCE on page 309
- Configure Frame Relay DLCIs on page 309
Configure Frame Relay Interface Encapsulation

Point-to-Point Protocol (PPP) encapsulation is the default encapsulation type for physical interfaces. You need not configure encapsulation for any physical interfaces that support PPP encapsulation. If you do not configure encapsulation, PPP is used by default. For physical interfaces that do not support PPP encapsulation, you must configure an encapsulation to use for packets transmitted on the interface. You can optionally configure an encapsulation on a logical interface, which is the encapsulation used within certain packet types.

Configure the Frame Relay Encapsulation on a Physical Interface

For Frame Relay interfaces, you configure Frame Relay encapsulation on the physical interface. This encapsulation is defined in RFC 1490, Multiprotocol Interconnect over Frame Relay. SONET and T3 interfaces can use Frame Relay encapsulation.

To configure Frame Relay encapsulation on a physical interface, include the encapsulation statement at the [edit interfaces interface-name] hierarchy level, specifying the frame-relay, frame-relay-ccc, or frame-relay-tcc option:

```
[edit interfaces interface-name]
e encapsulation (frame-relay | frame-relay-ccc | frame-relay-tcc);
```

When you configure a multipoint encapsulation (such as Frame Relay), the physical interface can have multiple logical units, and the units can be either point to point or multipoint.

Example: Configure the Encapsulation on a Physical Interface

Configure Frame Relay encapsulation on a SONET interface. The second and third family statements allow IS-IS and MPLS to run on the interface.

```
[edit interfaces]
so-7/0/0 {
   encapsulation frame-relay;
   unit 0 {
      point-to-point;
      family inet {
         address 192.168.1.113/32 {
            destination 192.168.1.114;
         }
      }
      family iso;
      family mpls;
   }
}
```
Configure the Frame Relay Encapsulation on a Logical Interface

Generally, you configure an interface’s encapsulation at the [edit interfaces interface-name] hierarchy level. However, for Frame Relay encapsulation, you can also configure the encapsulation type that is used inside the Frame Relay packet itself. To do this, include the encapsulation statement at the [edit interfaces interface-name unit logical-unit-number] hierarchy level, specifying the frame-relay-ccc or frame-relay-tcc option:

    [edit interfaces interface-name unit logical-unit-number]
    encapsulation (frame-relay-ccc | frame-relay-tcc);

Configure Frame Relay Control Bit Translation

On interfaces with Frame Relay CCC encapsulation, you can configure Frame Relay control bit translation, as defined in the Internet Engineering Task Force (IETF) documents:

- Frame Relay Encapsulation over Pseudo-Wires
- Encapsulation Methods for Transport of Layer 2 Frames Over IP and MPLS Networks

To support Frame Relay services over IP and MPLS backbones using Layer 2 VPNs and Layer 2 circuits, you can configure translation of the Frame Relay control bits. When you configure translation of Frame Relay control bits, the bits are mapped into the Layer 2 circuit control word and preserved across the IP or MPLS backbone.

The JUNOS software allows you to translate the following Frame Relay control bits:

- Discard eligibility (DE)—A header bit used to identify lower-priority traffic that can be dropped during periods of congestion.
- Forward explicit congestion notification (FECN)—A header bit transmitted by the source router requesting that the destination router slow down its requests for data.
- Backward explicit congestion notification (BECN)—A header bit transmitted by the destination router requesting that the source router send data more slowly.

By default, translation of Frame Relay control bits is disabled. If you enable Frame Relay control bit translation, the bits are translated in both directions (CE to PE and PE to CE):

- From CE to PE—At ingress, the DE, FECN, and BECN header bits from the incoming Frame Relay header are mapped to the control word.
- From PE to CE—At egress, the DE, FECN, and BECN header bits from the control word are mapped to the outgoing Frame Relay header.

The Frame Relay control bits do not map to MPLS EXP labels, and do not affect CoS behavior inside the provider network.

You enable or explicitly disable translation of Frame Relay control bits by including the translate-discard-eligible and translate-fecn-and-becn statements at the [edit interfaces interface-name unit logical-unit-number family ccc] hierarchy level:

    [edit interfaces interface-name unit logical-unit-number family ccc]
    (translate-discard-eligible | no-translate-discard-eligible);
    (translate-fecn-and-becn | no-translate-fecn-and-becn);
If you enable or disable Frame Relay control bit translation on one CE-facing interface, you must configure the same Frame Relay control bit translation settings on the other CE-facing interface.

If you change the Frame Relay control bit translation settings, the circuit goes down and comes back up, which might result in traffic loss for a few seconds.

If you enable Frame Relay control bit translation, the number of supportable Layer 2 VPNs and Layer 2 circuits is reduced to one eighth of what the router can support without Frame Relay control bit translation enabled.

For ATM 2 interfaces, the control word contains a field to carry ATM cell loss priority (CLP) information by default. For more information, see “Configure ATM 2 Layer 2 Circuit Transport Mode” on page 130.

For more information about Layer 2 circuits, see the JUNOS Internet Software Configuration Guide: VPNs and the JUNOS Internet Software Configuration Guide: Routing and Routing Protocols. For a comprehensive example, see the JUNOS Internet Software Feature Guide.

**Configure the Media MTU**

For Frame Relay interfaces, the default media MTU is 4482 bytes. (For a complete list of MTU values, see Table 3 on page 47 and Table 8 on page 49.)

To modify the default media MTU size for a physical interface, include the `mtu` statement at the `[edit interfaces interface-name]` hierarchy level:

```plaintext
[edit interfaces interface-name]
mtu bytes;
```

If you change the size of the media MTU, you must ensure that the size is equal to or greater than the sum of the protocol MTU and the encapsulation overhead. You configure the protocol MTU by including the `mtu` statement at the `[edit interfaces interface-name unit logical-unit-number family family]` hierarchy level, as discussed in “Set the Protocol MTU” on page 306.

**Set the Protocol MTU**

For each interface, you can configure an interface-specific MTU by including the `mtu` statement at the `[edit interfaces interface interface-name]` hierarchy level. If you need to modify this MTU for a particular protocol family, include the `mtu` statement at the `[edit interfaces interface interface-name unit logical-unit-number family family]` hierarchy level:

```plaintext
[edit interfaces interface-name unit logical-unit-number family family]
mtu mtu;
```

For Frame Relay encapsulation, the default protocol MTU is 4470 bytes.

If you increase the size of the protocol MTU, you must ensure that the size of the media MTU is equal to or greater than the sum of the protocol MTU and the encapsulation overhead. (You configure the media MTU by including the `mtu` statement at the `[edit interfaces interface-name]` hierarchy level, as discussed in “Configure the Media MTU” on page 306.)

When the family is mpls, the default protocol MTU is 1488 bytes. MPLS packets are 1500 bytes and have 4 to 12 bytes of overhead.
Configure Frame Relay Keepalives

By default, physical interfaces configured with Cisco HDLC or PPP encapsulation send keepalive packets at 10-second intervals. The Frame Relay term for keepalives is Local Management Interface (LMI) packets; note that the JUNOS software supports both ANSI T1.617 Annex D LMIs and ITU Q933 Annex A LMIs.

To disable the sending of keepalives on a physical interface, include the no-keepalives statement at the [edit interfaces interface interface-name] hierarchy level:

```
[edit interfaces interface-name]
no-keepalives;
```

For back-to-back Frame Relay connections, either disable the sending of keepalives on both sides of the connection, or configure one side of the connection as a DTE (the default JUNOS configuration) and the other as a DCE.

If keepalives are enabled, the number of possible DLCI configurations on a multipoint or multicast connection is limited by the MTU size selected for the interface. To calculate the available DLCIs, use the formula \((\text{MTU} - 12) / 5\). To increase the number of possible DLCIs, disable keepalives.

Configure Tunable Keepalives for Frame Relay LMI

On interfaces configured with Frame Relay connections, you can tune the keepalive settings by using the lmi statement. A Frame Relay interface can be either data circuit-terminating equipment (DCE) or data terminal equipment (DTE) (the default JUNOS configuration). DTE acts as a master, requesting status from the DCE part of the link.

By default, the JUNOS software uses ANSI T1.617 Annex D LMIs. To change to ITU Q933 Annex A LMIs, include the lmi-type itu statement at the [edit interfaces interface-name lmi] hierarchy level:

```
[edit interfaces interface-name lmi]
lmi-type itu;
```

To configure Frame Relay keepalive parameters, include the lmi statement at the [edit interfaces interface-name] hierarchy level:

```
[edit interfaces interface-name]
lmi {
    lmi-type (ansi | itu);
    n391dte number;
    n392dce number;
    n392dte number;
    n393dce number;
    n393dte number;
    t391dte seconds;
    t392dce seconds;
}
```
Configure Inverse Frame Relay ARP

Frame Relay interfaces support inverse Frame Relay ARP, as described in RFC 2390. When inverse Frame Relay ARP is enabled, the router responds to received inverse Frame Relay ARP requests by providing IP address information to the requesting router on the other end of the Frame PVC (permanent virtual circuit).

The router does not initiate inverse Frame Relay ARP requests.

By default, inverse Frame Relay ARP is disabled. To configure a router to respond to inverse Frame Relay ARP requests, include the inverse-arp statement at the [edit interfaces interface-name unit logical-unit-number] or [edit interfaces interface-name unit logical-unit-number family inet address address multipoint-destination destination] hierarchy level:

```
[edit interfaces interface-name unit logical-unit-number]
inverse-arp;
```

You must configure Frame Relay encapsulation on the logical interface to support inverse ARP. For more information, see “Configure Frame Relay Interface Encapsulation” on page 304.
Configure the Router as a DCE

By default, when you configure an interface with Frame Relay encapsulation, the router is assumed to be data terminal equipment (DTE). That is, the router is assumed to be at a terminal point on the network. To configure the router to be data circuit-terminating equipment (DCE), include the `dce` statement at the `[edit interfaces interface-name]` hierarchy level:

```
[edit interfaces interface-name]
dce;
```

When you configure the router to be a DCE, keepalives are disabled by default.

For back-to-back Frame Relay connections, either disable the sending of keepalives on both sides of the connection, or configure one side of the connection as a DTE (the default JUNOS configuration) and the other as a DCE.

Configure Frame Relay DLCIs

When you are using Frame Relay encapsulation on an interface, each logical interface corresponds to one or more permanent virtual circuits (PVCs) or switched virtual circuits (SVCs). For each PVC or SVC, you must configure one data-link connection identifier (DLCI).

A Frame Relay interface can be a point-to-point interface or a point-to-multipoint (also called a multipoint nonbroadcast multiaccess [NBMA]) connection.

To configure Frame Relay DLCIs, you can do the following:

- Configure a Point-to-Point Frame Relay Connection on page 309
- Configure a Point-to-Multipoint Frame Relay Connection on page 310
- Configure a Multicast-Capable Frame Relay Connection on page 311

Configure a Point-to-Point Frame Relay Connection

To configure a point-to-point Frame Relay connection, include the `dcli` statement at the `[edit interfaces interface-name unit logical-unit-number]` hierarchy level:

```
[edit interfaces interface-name unit logical-unit-number]
dcli dcli-identifier;
```
The DLCI identifier is a value from 16 through 1022. Numbers 1 through 15 are reserved for future use. A point-to-point interface can have one DLCI.

**Note**

By default, Channelized T3 and STM-1 interfaces can support a maximum of 64 Frame Relay DLCIs, numbered 0 through 63, per channel. In DLCI sparse mode, Channelized T3 and STM-1 interfaces support a maximum of three DLCIs, numbered 0 through 1,022, per channel. DLCI 0 is reserved for LMI. You configure the router to use DLCI sparse mode by including the `sparse-dlcs` statement at the `[edit chassis fpc slot-number pic pic-number]` hierarchy level.

Channelized T3 QPP interfaces support a maximum of 64 DLCIs, numbered 0 through 1,022, and, therefore, do not require sparse mode. For more information about Frame Relay DLCIs, see “Configure a Point-to-Point Frame Relay Connection” on page 309. For more information about DLCI sparse mode, see the JUNOS Internet Software Configuration Guide: Getting Started.

When you are configuring point-to-point connections, the MTU sizes on both sides of the connection must be the same.

**Configure a Point-to-Multipoint Frame Relay Connection**

To configure a point-to-multipoint Frame Relay connection (also called a multipoint NBMA connection), include the `multipoint-destination` statement within the `address` statement at the `[edit interfaces interface-name unit logical-unit-number]` hierarchy level:

```
[edit interfaces interface-name unit logical-unit-number]
  address address {
    multipoint-destination destination-address dlci dlci-identifier;
  }
```

`address` is the interface’s address.

For each destination, include one `multipoint-destination` statement. `destination-address` is the address of the remote side of the connection, and `dlci-identifier` is the DLCI identifier for the connection.

When you are configuring point-to-multipoint connections, all interfaces in the subnet must use the same MTU size.

If keepalives are enabled, causing the interface to send LMI messages during idle times, the number of possible DLCI configurations is limited by the MTU selected for the interface. For more information, see “Configure Frame Relay Keepalives” on page 307.
Configure a Multicast-Capable Frame Relay Connection

By default, Frame Relay connections assume unicast traffic. If your Frame Relay switch performs multicast replication, you can configure the connection to support multicast traffic by including the `multicast-dlci` statement at the `[edit interfaces interface-name unit logical-unit-number]` hierarchy level:

```
[edit interfaces interface-name unit logical-unit-number]
multicast-dlci dlci-identifier;
```

The DLCI identifier is a value from 16 through 1022 that defines the Frame Relay DLCI over which the switch expects to receive multicast packets for replication.

You can configure multicast support only on point-to-multipoint Frame Relay connections.

If keepalives are enabled, causing the interface to send LMI messages during idle times, the number of possible DLCI configurations is limited by the MTU selected for the interface. For more information, see “Configure Frame Relay Keepalives” on page 307.
Chapter 23
Configure the Loopback Interface

On the router, you can configure one physical loopback interface, lo0, and one or more addresses on the interface. To do this, include the following statements at the [edit interfaces] hierarchy level:

```
[edit interfaces]
lo0 {
    unit 0 {
        family inet {
            address loopback-address;
            address <loopback-address2>;
            ...
        }
    }
}
```

When specifying the loopback address, do not include a destination prefix. Also, in most cases, do not specify a loopback address on any unit other than unit 0.

For Layer 3 virtual private networks (VPNs), you can configure multiple logical units for the loopback interface. This allows you to configure a logical loopback interface for each virtual routing and forwarding (VRF) routing instance. For more information, see the JUNOS Internet Software Configuration Guide: VPNs.

If you configure the loopback interface, it is automatically used for unnumbered interfaces. If you do not configure the loopback interface, the router chooses the first interface to come online as the default. If you configure more than one address on the loopback interface, we recommend that you configure one to be the primary address to ensure that it is selected for use with unnumbered interfaces. By default, the primary address is used as the source address when packets originate from the interface.

For more information about unnumbered interfaces, see “Configure an Unnumbered Interface” on page 82. For more information about primary addresses, see “Configure the Interface Address” on page 81.
Example: Configure the Loopback Interface

Configure two addresses on the loopback interface:

```plaintext
[edit]
user@host# edit interfaces lo0 unit 0 family inet
[edit interfaces lo0 unit 0 family inet]
user@host# set address 127.0.0.1
[edit interfaces lo0 unit 0 family inet]
user@host# set address 10.0.0.1
[edit interfaces lo0 unit 0 family inet]
user@host# top
[edit]
user@host# show
interfaces {
  lo0 {
    unit 0 {
      family inet {
        127.0.0.1;
        10.0.0.1;
      }
    }
  }
}
```
Chapter 24
Configure Monitoring Services Interfaces

This chapter describes the following tasks for configuring traffic sampling and flow-monitoring properties:

- Minimum Traffic Sampling Configuration on page 315
- Configure Flow Monitoring on page 316

For detailed information about configuring flow monitoring and accounting services, see the JUNOS Internet Software Configuration Guide: Services Interfaces.

Minimum Traffic Sampling Configuration

To configure traffic sampling on a logical interface, you must perform at least the following tasks:

- Create a firewall filter to apply to the logical interfaces being sampled by including the filter statement at the [edit firewall family family-name] hierarchy level. In the filter then statement, you must specify the action modifier sample and the action accept.

  [edit firewall family family-name]
  filter filer-name {
    term term-name {
      then {
        sample;
        accept;
      }
    }
  }

  For more information about firewall filter actions and action modifiers, see the JUNOS Internet Software Configuration Guide: Policy Framework.

Another option is to configure the direction of traffic to be sampled by including the sampling statement at the [edit interfaces interface-name unit logical-unit-number family inet] hierarchy level, specifying input, output, or both.

  [edit interfaces interface-name unit logical-unit-number family inet]
  sampling {
    input;
    output;
  }
Apply the filter to the interfaces on which you want to sample traffic by including the address and filter statements at the [edit interfaces interface-name unit logical-unit-number family family-name] hierarchy level:

```
[edit interfaces interface-name unit logical-unit-number family family-name]
  address address {
    destination destination-address;
  }
  filter {
    input filter-name;
  }
```

Enable sampling and specify a nonzero sampling rate by including the sampling statement at the [edit forwarding-options] hierarchy level:

```
[edit forwarding-options]
  sampling {
    input {
      family inet{
        max-packets-per-second number;
        rate number;
      }
    }
  }
```

Configure Flow Monitoring

The flow-monitoring application performs traffic flow monitoring and enables lawful interception of traffic between two routers. Traffic flows can either be passively monitored by an offline router or actively monitored by a router participating in the network.

To enable flow monitoring on the Monitoring Services PIC, include the following statements at the [edit interfaces] hierarchy level:

```
[edit interfaces]
  mo-fpc/ pic/ port {
    unit logical-unit-number {
      family inet {
        address address {
          destination address;
        }
        filter {
          group filter-group-number;
          input filter-name;
          output filter-name;
        }
        sampling {
          [ input output ];
        }
      }
    }
  }
  multiservice-options {
    boot-command filename;
    (core-dump | no-core-dump);
    (syslog | no-syslog);
  }
```
Specify the physical and logical location of the flow-monitoring interface. Unit 0 is not available, because it is already used by internal processes. Specify the source and destination addresses. The filter statement allows you to associate an input or output filter or a filter group that you have already configured for this purpose. The sampling statement specifies the traffic direction, either input, output, or both.

The multiservice-options statement allows you to configure properties related to flow-monitoring interfaces:

- Include the boot-command statement to specify a boot image for the Monitoring Services interface.
- Include the core-dump statement to enable storage of core files in /var/tmp.
- Include the syslog statement to enable storage of system logging information in /var/log.

To configure flow-monitoring properties, include the following statements at the [edit forwarding-options] hierarchy level:

```plaintext
[edit forwarding-options]
monitoring name;
  family inet {
    output {
      cflowd host-name {
        aggregation {
          autonomous-system;
          destination-prefix;
          protocol-port;
          source-destination-prefix {
            caida-compliant;
          }
          source-prefix;
        }
        port port-number;
      }
      export-format format;
      flow-active-timeout seconds;
      flow-inactive-timeout seconds;
      interface interface-name {
        engine-id number;
        engine-type number;
        input-interface-index number;
        output-interface-index number;
        source-address address;
      }
    }
  }
```

For more information about flow-monitoring properties, see the JUNOS Internet Software Configuration Guide: Services Interfaces.
Chapter 25
Configure Multilink and Link Services Interfaces

The Multilink Protocol (MP) enables you to split, recombine, and sequence datagrams across multiple logical data links. The goal of multilink operation is to coordinate multiple independent links between a fixed pair of systems, providing a virtual link with greater bandwidth than any of the members.

The JUNOS software supports two MP-based services PICs: the Multilink Services PIC and the Link Services PIC. The Multilink Services PIC and the Links Services PIC support the following MP encapsulation types at the logical unit level:

- Multilink Point-to-Point Protocol (MLPPP)
- Multilink Frame Relay (MLFR FRF.15)

The Link Services PIC also supports the Multilink Frame Relay User-to-Network Interface (UNI) and the Network-to-Network Interface (NNI) (MLFR FRF.16) encapsulation type at the physical interface level.

MLPPP and MLFR (FRF.15) are supported on interface types ml-fpc/pic/port and ls-fpc/pic/port. For MLFR (FRF.15), multiple permanent virtual circuits (PVCs) are combined into one aggregated virtual circuit (AVC). This provides fragmentation over multiple PVCs on one end and reassembly of the AVC on the other end.

MLFR (FRF.16) is supported on a channelized interface, ls-fpc/pic/port:channel, which denotes a single MLFR (FRF.16) bundle. For MLFR (FRF.16), multiple links are combined to form one logical link. Packet fragmentation and reassembly occur on a per-VC basis. Each bundle can support multiple VCs. Link Services PICs can support up to 256 DLCIs per MLFR (FRF.16) bundle. The physical connections must be E1, T1, Channelized DS-3 to DS-1, Channelized DS-3 to DS-0, Channelized E1, Channelized STM-1, or Channelized QPP interfaces. When you bundle channelized interfaces using the Link Services interface, the channelized interfaces require M-series Enhanced FPCs.

The standards for MLPPP, MLFR FRF.15, and MLFR FRF.16 are defined in the following specifications:

- RFC 1990, The PPP Multilink Protocol (MP)
- FRF.15, End-to-End Multilink Frame Relay Implementation Agreement
- FRF.16.1, Multilink Frame Relay UNI/NNI Implementation Agreement
To configure multilink and link services interface properties, include the \texttt{ml-fpc/pic/port} or \texttt{ls-fpc/pic/port:channel} statement at the [edit interfaces] hierarchy level:

\begin{verbatim}
[edit interfaces]
  (ml-fpc/pic/port | ls-fpc/pic/port) {
    unit logical-unit-number {
      dlci dlci-identifier;
      drop-timeout milliseconds;
      encapsulation type;
      fragment-threshold bytes;
      interleaves fragments;
      minimum-links number;
      mrru bytes;
      multicast-dlci dlci-identifier;
      short-sequence;
      family family {
        address address {
          destination address;
        }
        bundle (ml-fpc/pic/port | ls-fpc/pic/port);
      }
    }
  }
\end{verbatim}

To configure link services physical interface properties, include the \texttt{mlfr-uni-nni-bundle-options} statement at the [edit interfaces ls-fpc/pic/port:channel] hierarchy level:

\begin{verbatim}
[edit interfaces ls-fpc/pic/port:channel]
  encapsulation type;
  mlfr-uni-nni-bundle-options {
    acknowledge-retries number;
    acknowledge-timer milliseconds;
    action-red-differential-delay (disable-tx | remove-link);
    drop-timeout milliseconds;
    fragment-threshold bytes;
    hello-timer milliseconds;
    lmi-type (ansi | itu);
    minimum-links number;
    mrru bytes;
    n391 number;
    n392 number;
    n393 number;
    red-differential-delay milliseconds;
    t391 number;
    t392 number;
    yellow-differential-delay milliseconds;
  }
\end{verbatim}

This chapter is organized as follows:

- Configure Multilink and Link Services Logical Interface Properties on page 321
- Configure Link Services Physical Interface Properties on page 327
- Multilink and Link Services Interface Structure on page 332
- Configure Link Services CoS Components on page 335
For examples of multilink and link services interface configuration, see the following sections:

- Examples: Configure Multilink Interfaces on page 339
- Examples: Configure Link Services Interfaces on page 341

Configure Multilink and Link Services Logical Interface Properties

You configure multilink and link services interface properties at the logical unit level. Default settings for multilink and link services logical interface properties are described in the following section:

- Default Settings for Multilink and Link Services Logical Interfaces on page 322

You can configure the following multilink and link services logical interface properties:

- Configure a Link Services Point-to-Point DLCI on page 322
- Configure a Link Services Multicast-Capable DLCI on page 323
- Configure a Multilink and Link Services Drop Timeout Period on page 323
- Configure Multilink and Link Services Logical Interface Encapsulation on page 324
- Configure a Multilink and Link Services Fragmentation Threshold on page 325
- Configure Link Services Delay-Sensitive Packet Interleaving on page 326
- Configure Multilink and Link Services Minimum Links on page 326
- Configure Multilink and Link Services MRRU on page 326
- Configure Multilink and Link Services Sequence Format on page 327

For general information about logical unit properties, see “Configure Logical Interface Properties” on page 67. For general information about family inet properties, see “Configure Protocol Family and Address Interface Properties” on page 77. For information about multilink and link services properties you configure at the family inet hierarchy level, see “Configure Multilink and Link Services Bundles” on page 333.
Default Settings for Multilink and Link Services Logical Interfaces

Table 24 lists the default settings for multilink and link services statements, together with the other permitted values or value ranges.

### Table 24: Multilink and Link Services Logical Interface Statements

<table>
<thead>
<tr>
<th>Option</th>
<th>Default Value</th>
<th>Possible Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>DLCI (data-link connection identifier)</td>
<td>None</td>
<td>16 through 1022</td>
</tr>
<tr>
<td>Drop timeout period</td>
<td>0 milliseconds</td>
<td>0 through 2000 milliseconds</td>
</tr>
<tr>
<td>Encapsulation</td>
<td>For multilink interfaces, multilink-ppp. For link services interfaces, multilink-frame-relay-end-to-end.</td>
<td>multilink-frame-relay-end-to-end, multilink-ppp.</td>
</tr>
<tr>
<td>Fragmentation threshold</td>
<td>0 bytes</td>
<td>128 through 16,320 bytes (nx64)</td>
</tr>
<tr>
<td>Interleave fragments</td>
<td>disabled</td>
<td>enabled, disabled</td>
</tr>
<tr>
<td>Minimum links</td>
<td>1 link</td>
<td>1 through 8 links</td>
</tr>
<tr>
<td>MRRU (maximum received reconstructed unit)</td>
<td>1524 bytes</td>
<td>1500 through 4500 bytes</td>
</tr>
<tr>
<td>Sequence ID format for ML-PPP</td>
<td>24 bits</td>
<td>12 or 24 bits</td>
</tr>
<tr>
<td>Sequence ID format for MLFR (FRF.15 and FRF.16)</td>
<td>12 bits</td>
<td>12 bits</td>
</tr>
</tbody>
</table>

See Table 25 on page 328 for statements that apply to link services physical interfaces only.

Configure a Link Services Point-to-Point DLCI

For link services interfaces only, you can configure multiple DLCIs for each MLFR (FRF.16) or MLPPP bundle. A channelized interface, such as ls-1/1/1:0, denotes a single MLFR (FRF.16) bundle. To configure a DLCI, include the dlci statement at the [edit interfaces interface-name unit logical-unit-number] hierarchy level:

```plaintext
[edit interfaces interface-name unit logical-unit-number]
dlci dlci-identifier;
```

The DLCI identifier is a value from 16 through 1022. Numbers 1 through 15 are reserved for future use.

When you configure point-to-point connections, the MTU sizes on both sides of the connection must be the same.

DLCIs are not supported on multilink interfaces.
Configure a Link Services Multicast-Capable DLCI

For link services interfaces only, you can configure multiple multicast-capable DLCIs for each MLFR (FRF.16) bundle. A channelized interface, such as ls-1/1/1:0, denotes a single MLFR (FRF.16) bundle. By default, Frame Relay connections assume unicast traffic. If your Frame Relay switch performs multicast replication, you can configure the link services connection to support multicast traffic by including the multicast-dlci statement at the [edit interfaces interface-name unit logical-unit-number] hierarchy level:

[edit interfaces interface-name unit logical-unit-number]
multicast-dlci dlci-identifier;

The DLCI identifier is a value from 16 through 1022 that defines the Frame Relay DLCI over which the switch expects to receive multicast packets for replication.

You can configure multicast support only on point-to-multipoint link services connections. Multicast-capable DLCIs are not supported on multilink interfaces.

If keepalives are enabled, causing the interface to send Local Management Interface (LMI) messages during idle times, the number of possible DLCI configurations is limited by the maximum transmission unit (MTU) selected for the interface. For more information, see “Configure Link Services Keepalive Settings on Frame Relay LMI” on page 331.

Configure a Multilink and Link Services Drop Timeout Period

By default, the drop timeout parameter is disabled. You can configure a drop timeout value to provide a recovery mechanism if individual links in the multilink or link services bundle drop one or more packets. Make sure the value you set is larger than the expected differential delay across the links, although drop timeout is not a differential delay tolerance setting, and does not limit the overall latency. You can configure differential delay tolerance for link services interfaces only. For more information, see “Configure Link Services Differential Delay” on page 330.

To configure the drop timeout value, include the drop-timeout statement at the [edit interfaces ml-fpc/pic/port unit logical-unit-number] or [edit interfaces ls-fpc/pic/port unit logical-unit-number] hierarchy level:

drop-timeout milliseconds;

For link services interfaces, you also can configure the drop timeout value at the physical interface level also by including the drop-timeout statement at the [edit interfaces ls-fpc/pic/port:channel mlfr-uni-nni-bundle-options] hierarchy level:

[edit interfaces ls-fpc/pic/port:channel mlfr-uni-nni-bundle-options]
drop-timeout milliseconds;
The drop timer has the duration of 0 through 2000 milliseconds. Values less than 5 milliseconds are not recommended; a value of 0 disables the timer.

For multilink or link services interfaces, if a packet or fragment encounters an error condition and is destined for a disabled bundle or link, it does not contribute to the dropped packet and frame counts in the per-bundle statistics. The packet is counted under the global error statistics and is not included in the global output bytes and output packet counts. This unusual accounting happens only if the error conditions are generated inside the multilink interface, not if the packet encounters errors on the wire or elsewhere in the network.

---

**Configure Multilink and Link Services Logical Interface Encapsulation**

Multilink and Link Services interfaces support the following logical interface encapsulation types:

- **MLPPP**
- **MLFR End-to-End**

By default, the logical interface encapsulation type on multilink interfaces is MLPPP. The default logical interface encapsulation type on link services interfaces is MLFR End-to-End. For more information, see “Configure the Encapsulation on a Logical Interface” on page 75.

You can configure physical interface encapsulation on link services interfaces. For more information, see “Configure Link Services Physical Interface Encapsulation” on page 328.

To configure multilink or link services encapsulation, include the encapsulation statement at the [edit interfaces ml-fpc/pic/port unit logical-unit-number] or [edit interfaces ls-fpc/pic port unit logical-unit-number] hierarchy level:

```
encapsulation type;
```

You must also configure the T1, E1, or DS-0 physical interface with the same encapsulation type.
Configure a Multilink and Link Services Fragmentation Threshold

By default, the fragmentation threshold parameter is disabled. For interfaces with MLPPP encapsulation only, you can configure a fragmentation threshold to set a maximum size for packet payloads transmitted across the individual links within the multilink circuit. The software splits any incoming packet that exceeds the fragmentation threshold into smaller units suitable for the circuit size; it reassembles the fragments at the other end, but does not affect the output traffic stream. The threshold value affects the payload only; it does not affect the MLPPP header.

To configure a fragmentation threshold value, include the `fragment-threshold` statement at the hierarchy level:

```
[edit interfaces ml-fpc/pic/port unit logical-unit-number]
```

For link services interfaces, you can configure a fragmentation threshold value at the physical interface level by including the `fragment-threshold` statement at the hierarchy level:

```
[edit interfaces ls-fpc/pic/port:channel mlfr-uni-nni-bundle-options]
```

The maximum fragment size can be from 128 through 16,320 bytes. The JUNOS software automatically subdivides packet payloads that exceed this value. Any value you set must be a multiple of 64 bytes (Nx64). The default value, 0, results in no fragmentation.
Configure Link Services Delay-Sensitive Packet Interleaving

By default, packet interleaving is disabled. For link services FRF.15 and MLPPP interfaces only, you can interleave long packets with high-priority packets. This allows small delay-sensitive packets, such as Voice over IP (VoIP) packets, to interleave with long fragmented packets. This minimizes the latency of delay-sensitive packets. Single-link bundles are required for packet interleaving to work. For all Link Services PICs, you can configure up to 256 single-link bundles. For more information about bundles, see “Link Services PIC Capabilities” on page 333.

To interleave packets, include the `interleave-fragments` statement at the `[edit interfaces ls-fpc/pic/port unit logical-unit-number]` hierarchy level:

```
interleave-fragments;
```

Configure Multilink and Link Services Minimum Links

By default, the minimum number of links is 1. You can set the minimum number of links that must be up for the multilink bundle as a whole to be labeled up. To set the minimum number, include the `minimum-links` statement at the `[edit interfaces ml-fpc/pic/port unit logical-unit-number]` or `[edit interfaces ls-fpc/pic/port unit logical-unit-number]` hierarchy level:

```
minimum-links number;
```

For link services interfaces, you also can configure the minimum number of links at the physical interface level by including the `minimum-links` statement at the `[edit interfaces ls-fpc/pic/port:channel mlfr-uni-nni-bundle-options]` hierarchy level:

```
[edit interfaces ls-fpc/pic/port:channel mlfr-uni-nni-bundle-options]
minimum-links number;
```

You can set from 1 through 8 minimum links. When 8 is specified, all configured links of a bundle must be up.

Configure Multilink and Link Services MRRU

The maximum received reconstructed unit (MRRU) is similar to a maximum transmission unit (MTU), but applies only to multilink bundles; it is the maximum packet size that the multilink interface can process. By default, the MRRU is set to 1500 bytes; you can configure a different MRRU value if the peer equipment allows. The MRRU includes the original payload plus the 2-byte PPP header, but not the additional MLPPP or MLFR header applied while the individual multilink packets are traversing separate links in the bundle.

To configure a different MRRU value, include the `mrru` statement at the `[edit interfaces ml-fpc/pic/port unit logical-unit-number]` or `[edit interfaces ls-fpc/pic/port unit logical-unit-number]` hierarchy level:

```
mrru bytes;
```

For link services interfaces, you also can configure a different MRRU at the physical interface level by including the `mrru` statement at the `[edit interfaces ls-fpc/pic/port:channel mlfr-uni-nni-bundle-options]` hierarchy level:

```
[edit interfaces ls-fpc/pic/port:channel mlfr-uni-nni-bundle-options]
mrru bytes;
```
The MRRU size can be from 1500 through 4500 bytes.

If you set the MRRU on a bundle to a value larger than the MTU of the individual links within it, you must enable a fragmentation threshold for that bundle. Set the threshold to a value no larger than the smallest MTU of any link included in the bundle.

Determine the appropriate MTU size for the bundle by ensuring the MTU size does not exceed the sum of the encapsulation overhead and the MTU sizes for the links in the bundle.

**Configure Multilink and Link Services Sequence Format**

For MLPPP, the sequence header format is set to 24 bits by default. You can configure an alternative value of 12 bits, but 24 bits is considered the more robust value for most networks.

To configure a different sequence header value, include the `short-sequence` statement at the hierarchy level:

```
short-sequence;
```

For MLFR FRF.15, the sequence header format is set to 24 bits by default. This is the only valid option.

**Configure Link Services Physical Interface Properties**

You configure link services interface properties at the logical unit and physical interface level.

Default settings for link services physical interface properties are described in the following section:

- Default Settings for Link Services Interfaces on page 328

You can configure the following link services physical interface properties:

- Configure Link Services Physical Interface Encapsulation on page 328
- Configure Link Services Acknowledgment Timers on page 329
- Configure Link Services Differential Delay on page 330
- Configure Link Services Keepalive Settings on Frame Relay LMI on page 331

For descriptions of link services physical interface properties that also can be configured at the logical unit level, see “Configure Multilink and Link Services Logical Interface Properties” on page 321.
Default Settings for Link Services Interfaces

Table 25 lists the default settings for link services statements, together with the other permitted values or value ranges.

Table 25: Link Services Physical Interface Statements for MLFR (FRF.16)

<table>
<thead>
<tr>
<th>Option</th>
<th>Default Value</th>
<th>Possible Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Action red differential delay</td>
<td>disable-tx</td>
<td>disable-tx, remove-link</td>
</tr>
<tr>
<td>Red differential delay</td>
<td>10</td>
<td>1 through 2000</td>
</tr>
<tr>
<td>Yellow differential delay</td>
<td>6</td>
<td>1 through 2000</td>
</tr>
<tr>
<td>Drop timeout period</td>
<td>0 milliseconds</td>
<td>0 through 2000 milliseconds</td>
</tr>
<tr>
<td>Encapsulation</td>
<td>multilink-frame-relay-uni-nni</td>
<td>multilink-frame-relay-uni-nni</td>
</tr>
<tr>
<td>Fragmentation threshold</td>
<td>0 bytes</td>
<td>128 through 16,320 bytes (tx64)</td>
</tr>
<tr>
<td>LMI type</td>
<td>itu</td>
<td>ansi, itu</td>
</tr>
<tr>
<td>Minimum links</td>
<td>1 link</td>
<td>1 through 8 links</td>
</tr>
<tr>
<td>MRRU (maximum received reconstructed unit)</td>
<td>1524 bytes</td>
<td>1500 through 4500 bytes</td>
</tr>
<tr>
<td>n391 (full status polling counter)</td>
<td>6</td>
<td>1 through 255</td>
</tr>
<tr>
<td>n392 (LMI error threshold)</td>
<td>3</td>
<td>1 through 10</td>
</tr>
<tr>
<td>n393 (LMI monitored event count)</td>
<td>4</td>
<td>1 through 10</td>
</tr>
<tr>
<td>t391 (link integrity verify polling timer)</td>
<td>10</td>
<td>5 through 30</td>
</tr>
<tr>
<td>t392 (polling verification timer)</td>
<td>15</td>
<td>5 through 30</td>
</tr>
<tr>
<td>Sequence ID format for MLFR</td>
<td>12 bits</td>
<td>12 bits</td>
</tr>
</tbody>
</table>

Configure Link Services Physical Interface Encapsulation

Link services interfaces support the physical interface encapsulation MLFR UNI NNI. By default, the physical interface encapsulation on link services interfaces is MLFR UNI NNI. Multilink interfaces do not support physical interface encapsulation.

For more information, see “Configure the Encapsulation on a Physical Interface” on page 51.

You can configure logical interface encapsulation on multilink and link services interfaces. For more information, see “Configure Multilink and Link Services Logical Interface Encapsulation” on page 324.

To explicitly configure link services physical interface encapsulation, include the encapsulation statement at the [edit interfaces ls-fpc/ pic/ port:channel] hierarchy level:

```
[edit interfaces ls-fpc/ pic/ port:channel]
encapsulation type;
```

You must also configure the T1, E1, or DS-0 physical and physical interface with the same encapsulation type.
Configure Link Services Acknowledgment Timers

For link services interfaces configured with MLFR (FRF.16), each link end point in a bundle initiates a request for bundle operation with its peer by transmitting an add link message. A hello message notifies the peer end point that the local end point is up. Both ends of a link generate a hello message periodically, or as configured with the hello timer. A remove link message notifies the peer that the local end management is removing the link from bundle operation. End points respond to add link, remove link, and hello messages by sending acknowledgement messages.

You can configure the maximum period to wait for an add link acknowledgement, hello acknowledgement, or remove link acknowledgement by including the `acknowledge-timer` statement at the `interfaces ls-fpc pic port:channel mlfr-uni-nni-bundle-options` hierarchy level:

```
[edit interfaces ls-fpc pic port:channel mlfr-uni-nni-bundle-options]
acknowledge-timer milliseconds;
```

The acknowledgement timer can be from 1 through 10 milliseconds. The default is 4 milliseconds.

For link services interfaces, you can configure the number of retransmission attempts to be made for consecutive hello or remove link messages after the expiration of the acknowledgement timer by including the `acknowledge-retries` statement at the `interfaces ls-fpc pic port:channel mlfr-uni-nni-bundle-options` hierarchy level:

```
[edit interfaces ls-fpc pic port:channel mlfr-uni-nni-bundle-options]
acknowledge-retries number;
```

Acknowledgement retries can be a value from 1 through 5. The default is 2.

You can configure the rate at which hello messages are sent by including the `hello-timer` statement at the `interfaces ls-fpc pic port:channel mlfr-uni-nni-bundle-options` hierarchy level:

```
[edit interfaces ls-fpc pic port:channel mlfr-uni-nni-bundle-options]
hello-timer milliseconds;
```

A hello message is transmitted after the specified period (in milliseconds) has elapsed. The hello timer can be from 1 through 180 milliseconds; the default is 10 milliseconds. When the hello timer expires, a link end point generates an add-link message.
Configure Link Services Differential Delay

For link services interfaces configured with MLFR (FRF.16), the differential delay between links in a bundle is measured and warning is given when a link has a substantially greater differential delay than other links in the same bundle. The implementing end point can determine if the differential delay is in an acceptable range and decide to remove the link from the bundle, or to stop transmission on the link.

You can configure the yellow differential delay for links in a bundle by including the yellow-differential-delay statement at the [edit interfaces ls-fpc/ pic/ port:channel mifr-uni-nni-bundle-options] hierarchy level:

```plaintext
[edit interfaces ls-fpc/ pic/ port:channel mifr-uni-nni-bundle-options]
yellow-differential-delay milliseconds;
```

The yellow differential delay can be from 3 through 2000 milliseconds. The default is 6 milliseconds.

You can configure the red differential delay for links in a bundle to give warning by including the red-differential-delay statements at the [edit interfaces ls-fpc/ pic/ port:channel mifr-uni-nni-bundle-options] hierarchy level:

```plaintext
[edit interfaces ls-fpc/ pic/ port:channel mifr-uni-nni-bundle-options]
red-differential-delay milliseconds;
```

The red differential delay can be from 5 through 2000 milliseconds. The default is 10 milliseconds.

You can configure the action to be taken when differential delay exceeds the red limit by including the action-red-differential-delay red statements at the [edit interfaces ls-fpc/ pic/ port:channel mifr-uni-nni-bundle-options] hierarchy level:

```plaintext
[edit interfaces ls-fpc/ pic/ port:channel mifr-uni-nni-bundle-options]
action-red-differential-delay (disable-tx | remove-link);
```

The disable-tx option disables transmission on the link. The remove-link option removes the link from the bundle. The default action is disable-tx.
Configure Link Services Keepalive Settings on Frame Relay LMI

You can tune the keepalive settings on the physical link-services interface. By default, the JUNOS software uses ITU Q.933 Annex A LMIs for FRF.16. To use ITU Annex A LMIs, include the lmi-type ansi statement at the [edit interfaces ls-fpc/pic/port:channel mlfr-uni-nni-bundle-options] hierarchy level:

[edit interfaces ls-fpc/pic/port:channel mlfr-uni-nni-bundle-options]
lmi-type ansi;

To configure Frame Relay keepalive parameters on a link services interface, include the n391, n392, n393, t391 and t392 statements at the [edit interfaces ls-fpc/pic/port:channel mlfr-uni-nni-bundle-options] hierarchy level:

[edit interfaces ls-fpc/pic/port:channel mlfr-uni-nni-bundle-options]
n391 number;
n392 number;
n393 number;
t391 number;
t392 number;

You can set the following properties:

- **n391** — Full status polling interval. The data terminal equipment (DTE) sends a status inquiry to the data communication equipment (DCE) at the interval specified by t391. n391 specifies the frequency with which these inquiries expect a full status report; for example, an n391 value of 10 would specify a full status report in response to every tenth inquiry. The intermediate inquiries ask for a keepalive exchange only. The range is 1 through 255, with a default value of 6.

- **n392** — Error threshold. The number of errors required to bring down the link, within the event count specified by n393. The range is 1 through 10, with a default value of 3.

- **n393** — Monitored event count. The range is 1 through 10, with a default value of 4.

- **t391** — Keepalive timer. Interval at which the DTE sends out a keepalive response request to the DCE and updates status, depending on the error threshold value. The range is 5 through 30 seconds, with a default value of 10 seconds.

- **t392** — Keepalive timer. Period during which the DCE checks for keepalive responses from the DTE and updates status, depending on the DCE error threshold value. The range is 5 through 30 seconds, with a default value of 15 seconds.

For the LMI to work properly, you must configure one side of a link services bundle to be a DCE.
Multilink and Link Services Interface Structure

Each Multilink Services or Link Services PIC can support a number of bundles. A bundle can contain up to eight individual links. For Multilink Services PICs, the links can be T1, E1, or DS-0 physical interfaces, and each link is associated with a logical unit number that you configure. For Link Services PICs, the links can be E1, T1, Channelized DS-3 to DS-1, Channelized DS-3 to DS-0, Channelized E1, Channelized STM-1 interfaces, or Channelized QPP interfaces. For MLFR (FRF.16) bundles, each link is associated with a channel number that you configure.

You must configure a link before it can join a bundle. Each bundle should consist solely of one type of link; we recommend that you not mix physical interfaces of differing speeds within a bundle.

This section is organized as follows:

- Multilink Services and Link Services PIC Capacities on page 332
- Link Services PIC Capabilities on page 333
- Configure Multilink and Link Services Bundles on page 333

Multilink Services and Link Services PIC Capacities

Three versions of Multilink Services and three versions of Link Services PICs are available, as shown in Table 26. The PIC hardware is identical, except for different faceplates that enable you to identify which version you are installing. The software limits the unit numbers and maximum number of physical interfaces you assign to the PIC.

Table 26: Multilink Services PIC Capacities

<table>
<thead>
<tr>
<th>PIC Capacity</th>
<th>Unit Numbers</th>
<th>Maximum Number of T1/ DS-0 Interfaces</th>
<th>Maximum Number of E1 Interfaces</th>
</tr>
</thead>
<tbody>
<tr>
<td>4-bundle PIC</td>
<td>0 through 3</td>
<td>32 links</td>
<td>32 links</td>
</tr>
<tr>
<td>32-bundle PIC</td>
<td>0 through 31</td>
<td>256 links</td>
<td>219 links</td>
</tr>
<tr>
<td>128-bundle PIC</td>
<td>0 through 127</td>
<td>292 links</td>
<td>219 links</td>
</tr>
</tbody>
</table>

A single PIC can support an aggregate bandwidth of 450 Mbps.

You can configure a larger number of links, but the Multilink Services and Link Services PICs can reliably process only 450 Mbps of traffic. A higher rate of traffic might degrade performance.
**Link Services PIC Capabilities**

The default number of bundles per Link Services PIC is 16, ranging from ls-fpc/pic/port:0 to ls-fpc/pic/port:15.

To configure the number of bundles on a Link Services PIC, include the mlfr-uni-nni-bundles statement at the [edit chassis fpc slot-number pic pic-number] hierarchy level:

```
[edit chassis fpc slot-number pic pic-number]
mlfr-uni-nni-bundles number;
```

Each Link Services PIC can accommodate a maximum of 256 MLFR UNI NNI bundles. For more information, see the JUNOS Internet Software Guide: Getting Started.

A link can associate with one link services bundle only. All Link Services PICs support up to 256 single-link bundles and up to 256 DLCIs. For an example configuration, see “Examples: Configure Link Services Interfaces” on page 341.

**Configure Multilink and Link Services Bundles**

To complete a multilink or link services interface configuration, you need to configure both the physical interface and the multilink or link services bundle. For multilink interfaces, you configure the link bundle on the logical unit. For link services interfaces, you configure the link bundle as a channel (see Figure 22). The physical interface is usually connected to networks capable of supporting MLPPP or MLFR (FRF.15 or FRF.16).

**Figure 22: Multilink Interface Configuration**

![Multilink Interface Configuration Diagram](image-url)
Using the topology in Figure 22 as an example, configure a multilink or link services bundle over a T1 connection (for which you have already configured the T1 physical interface) with the following additional configuration statements:

1. To configure a physical T1 link for MLPPP, include the following statements at the [edit interfaces t1-fpc/pic/port] hierarchy level:

   ```
   [edit interfaces t1-fpc/pic/port]
   unit 0 {
      family mlppp {
         bundle (ml-fpc/pic/port | ls-fpc/pic/port);
      }
   }
   ```

   You do not need to configure an IP address on this link.

To configure a physical T1 link for MLFR (FRF.16), include the following statements at the [edit interfaces t1-fpc/pic/port] hierarchy level:

```
[edit interfaces t1-fpc/pic/port]
encapsulation multilink-frame-relay-uni-nni;
unit 0 {
   family mlfr-uni-nni {
      bundle ls-fpc/pic/port:channel;
   }
}
```

You do not need to configure an IP address nor a DLCI on this link.

2. To configure the logical address for the MLPPP bundle, include the address and destination statements at the [edit interfaces ml-fpc/pic/port unit logical-unit-number family inet] hierarchy level:

```
[edit interfaces ml-fpc/pic/port unit logical-unit-number family inet]
family inet {
   address address {
      destination address;
   }
}
```

When you add statements such as MRRU to the configuration and commit, the T1 interface becomes part of the multilink bundle.

To configure the logical address for the MLFR (FRF.15) bundle, include the address and destination statements at the [edit interfaces ml-fpc/pic/port unit logical-unit-number family inet] hierarchy level:

```
[edit interfaces ml-fpc/pic/port unit logical-unit-number]
family inet {
   address address {
      destination address;
   }
}
```
Configure Multilink and Link Services Interfaces

To configure the logical address for the MLFR (FRF.16) bundle, include the address and destination statements at the [edit interfaces ls-fpc/pic/port unit logical-unit-number family inet] hierarchy level:

```
[edit interfaces ls-fpc/pic/port unit logical-unit-number]
encapsulation multilink-frame-relay-uni-nni;
family inet {
  address address {
    destination address;
  }
}
```

For MLPPP and MLFR (FRF.15 and FRF.16) links, you must specify the subnet address as /32 or /30. Any other subnet designation is treated as a mismatch.

Configure Link Services CoS Components

Unlike networking interfaces, which handle packet input and output directly, the Link Services PIC provides preprocessing for input and output packets and then sends them to the networking interfaces. As a result, CoS components in the Link Services interfaces work differently than in networking interfaces and have the following characteristics:

- When packet interleaving is enabled, Link Services FRF.15 and MLPPP interfaces support CoS. Link Services FRF.16 interfaces do not support packet interleaving, and therefore do not support CoS.

- For link services FRF.16 interfaces with multiple DLCIs, you can use an output firewall filter to classify high-priority packet flows and normal-priority packet flows into two different DLCIs.

- For bundle link interfaces of Link Services PICs, you can configure standard scheduler maps.

- If your CoS configuration classifies VoIP traffic into queue 1, the VoIP packets receive the default classification to the class associated with queue 1. The resulting fragmentation affects jitter and delay. Therefore, for packets that originate from a general network interface, pass through a link services interface, and are destined for a constituent bundle link interface, we recommend applying an output firewall filter to the link services interface. The purpose of the output filter is to redirect the queue 1 traffic to a different forwarding class.

- For packets that originate from a constituent bundle link interface, pass through a link services interface, and are destined for a general network interface, we recommend applying a behavior aggregate (BA) classifier to the link services interface.

- For input packets and fragments received from bundle links, you can use regular input firewall filters and standard CoS classifiers on the link services interface.

- All traffic in queue 0 and queue 1 is fragmented. Traffic in queue 2 and queue 3 is not fragmented.
Routing protocol packets in queue 3 that exceed 128 bytes are automatically sent to queue 0 and fragmented accordingly. This rule does not apply to transit packets in queue 3.

You must configure classification for T1 egress traffic on the link services interface, not on the T1 interface directly.

For more information, see “Configure Link Services Delay-Sensitive Packet Interleaving” on page 326 and the JUNOS Internet Software Configuration Guide: Policy Framework.

Example: Configure Link Services CoS Components

Configure CoS on a link services interface and its bundle link interfaces. Packets that do not match the firewall filters are load-balanced by sending fragments to all bundle links. Packets that do match the firewall filters are not fragmented and reassembled; they are load balanced by sending each packet flow to a different bundle link. Each packet that matches a firewall filter is subjected to a hash on the IP source address and the IP destination address to determine the packet flow to which each packet belongs. When you configure the MLPPP encapsulation type or the multilink FRF.15 Frame Relay end-to-end encapsulation type, routing protocol packets are always transmitted to the network-control queue on the bundle link interface. This keeps routing protocols operating normally, even when low-speed links are congested by regular packets.

```
[edit interfaces]
ls-7/0/0 {
  unit 0 {
    encapsulation multilink-ppp;
    interleave-fragments;
    family inet {
      filter {
        output lfi_ls_filter;
      }
      address 10.54.0.2/32 {
        destination 10.54.0.1;
      }
    }
  }
}
ge-7/2/0 {
  unit 0 {
    family inet {
      address 192.2.1.1/24;
    }
  }
}
ce1-7/3/6 {
  no-partition interface-type e1;
}
e1-7/3/6 {
  encapsulation ppp;
  unit 0 {
    family mlppp {
      bundle ls-7/0/0.0;
    }
  }
}
```
Configure Multilink and Link Services Interfaces

Configure Link Services CoS Components

```conf
ce1-7/3/7 {
    no-partition interface-type e1;
}
e1-7/3/7 {
    encapsulation ppp;
    unit 0 {
        family mlppp {
            bundle ls-7/0/0.0;
        }
    }
}

[edit class-of-service]
classifiers {
    dscp dscp_default {
        import default;
    }
    inet-precedence inet-precedence_default {
        import default;
    }
}

code-point-aliases {
    dscp {
        af11 001010;
        af12 001100;
        af13 001110;
        af21 010010;
        af22 010100;
        af23 010110;
        af31 011010;
        af32 011100;
        af33 011110;
        af41 100010;
        af42 100100;
        af43 100110;
        be 000000;
        cs1 001000;
        cs2 010000;
        cs3 011000;
        cs4 100000;
        cs5 101000;
        cs6 110000;
        cs7 111000;
        ef 101110;
    }
    inet-precedence {
        af11 001;
        af21 010;
        af31 011;
        af41 100;
        be 000;
        cs6 110;
        cs7 111;
        ef 101;
        nc1 110;
        nc2 111;
    }
}
```

Configure Link Services CoS Components

forwarding-classes {
    queue 0 be;
    queue 1 ef;
    queue 2 af;
    queue 3 nc;
}

interfaces {
    ge-7/2/0 {
        scheduler-map sched-map;
        unit 0 {
            classifiers {
                dscp dscp_default;
            }
        }
    }
    e1-7/3/6 {
        scheduler-map sched-map;
    }
    e1-7/3/7 {
        scheduler-map sched-map;
    }
    ls-7/0/0 {
        unit 0 {
            classifiers {
                inet-precedence inet-precedence_default;
            }
        }
    }
}

scheduler-maps {
    sched-map {
        forwarding-class af scheduler af-scheduler;
        forwarding-class be scheduler be-scheduler;
        forwarding-class ef scheduler ef-scheduler;
        forwarding-class nc scheduler nc-scheduler;
    }
}

schedulers {
    af-scheduler {
        transmit-rate percent 25;
        buffer-size percent 25;
    }
    be-scheduler {
        transmit-rate percent 25;
        buffer-size percent 25;
    }
    ef-scheduler {
        transmit-rate percent 25;
        buffer-size percent 25;
    }
    nc-scheduler {
        transmit-rate percent 25;
        buffer-size percent 25;
    }
}
Examples: Configure Multilink Interfaces

These examples show only the multilink part of the configuration. To see the T1 configuration options, see “Configure T1 Interfaces” on page 387.

Configure an MLPPP interface:

```plaintext
[edit interfaces]
ml-1/0/0 {
    unit 1 {
        fragment-threshold 128;
        family inet {
            address 192.128.5.1/32 {
                destination 192.128.200.200;
            }
        }
    }
    unit 10 {
        family inet {
            address 128.1.1.3/32 {
                destination 128.1.1.2;
            }
        }
    }
}
t1-5/1/0 {
    unit 0 {
        family mlppp {
            bundle ml-1/0/0.1;
        }
    }
}
```
Examples: Configure Multilink Interfaces

```
t1-5/1/1 {
    unit 0 {
        family mlppp {
            bundle ml-1/0/0.1;
        }
    }
}
t1-5/1/2 {
    unit 0 {
        family mlppp {
            bundle ml-1/0/0.1;
        }
    }
}

Configure an MLFR (FRF.15) interface:

[edit interfaces]
ml-1/0/0 {
    unit 1 {
        encapsulation multilink-frame-relay-end-to-end;
        family inet {
            address 192.128.5.2/32 {
                destination 192.128.5.3;
            }
        }
    }
    unit 10 {
        encapsulation multilink-frame-relay-end-to-end;
        family inet {
            address 128.1.1.3/32 {
                destination 128.1.1.2;
            }
        }
    }
}
t1-5/1/0 {
    unit 0 {
        dlci 16;
        encapsulation multilink-frame-relay-end-to-end;
        family mlfr-end-to-end {
            bundle ml-1/0/0.1;
        }
    }
}
t1-5/1/1 {
    unit 0 {
        dlci 17;
        encapsulation multilink-frame-relay-end-to-end;
        family mlfr-end-to-end {
            bundle ml-1/0/0.10;
        }
    }
}
```
Examples: Configure Link Services Interfaces

This example shows only the link services part of the configuration. To see the the T1 configuration options, see “Configure T1 Interfaces” on page 387.

The four examples in this section show the following configurations:

- One bundle with two links, as listed in Table 27
- Link Services interface with MLPPP encapsulation
- Link Services interface with MLFR FRF.15 encapsulation
- Link Services interface with MLFR FRF.16 encapsulation

Table 27: Link Services Bundle

<table>
<thead>
<tr>
<th>Router A</th>
<th>Router B</th>
</tr>
</thead>
<tbody>
<tr>
<td>t1-0/1/0 (ls-1/1/0:3)</td>
<td>t1-0/3/0 (ls-0/0/0:10)</td>
</tr>
<tr>
<td>t1-0/1/1 (ls-1/1/0:3)</td>
<td>t1-0/3/1 (ls-0/0/0:10)</td>
</tr>
</tbody>
</table>

This configuration initiates the MLFR UNI NNI protocol between Router A and Router B and logically connects link services bundles ls-1/1/0.3 and ls-0/0/0.10.

For LMI to work properly, you must configure one router to be a DCE.

Configure a Link Services interface with two links

On Router A

```
[edit interfaces]
ls-1/1/0:3 {
    dce;
    encapsulation multilink-frame-relay-uni-nni;
    unit 0 {
        dci 16;
        family inet {
            address 3.3.3.1/32 {
                destination 3.3.3.2;
            }
        }
    }
}
```
t1-0/1/0 {
    encapsulation multilink-frame-relay-uni-nni;
    unit 0 {
        family mlfr-uni-nni {
            bundle ls-1/1/0:3;
        }
    }
}

t1-0/1/1 {
    encapsulation multilink-frame-relay-uni-nni;
    unit 0 {
        family mlfr-uni-nni {
            bundle ls-1/1/0:3;
        }
    }
}

On Router B
[edit interfaces]
l0-0/0/0:10 {
    encapsulation multilink-frame-relay-uni-nni;
    unit 0 {
        dcli 16;
        family inet {
            address 3.3.3.2/32 {
                destination 3.3.3.1;
            }
        }
    }
}

t1-0/3/0 {
    encapsulation multilink-frame-relay-uni-nni;
    unit 0 {
        family mlfr-uni-nni {
            bundle ls-0/0/0:10;
        }
    }
}

t1-0/3/1 {
    encapsulation multilink-frame-relay-uni-nni;
    unit 0 {
        family mlfr-uni-nni {
            bundle ls-0/0/0:10;
        }
    }
}
Configure a Link Services interface with MLPPP

```plaintext
[edit interfaces]
t1-0/0/0 {  
  encapsulation ppp;  
  unit 0 {  
    family mlppp {  
      bundle ls-0/3/0.0;  
    }  
  }  
}  
t1-0/0/1 {  
  encapsulation ppp;  
  unit 0 {  
    family mlppp {  
      bundle ls-0/3/0.0;  
    }  
  }  
}
ls-0/3/0 {  
  unit 0 {  
    encapsulation multilink-ppp;  
    family inet {  
      address 10.16.1.2/32 {  
        destination 10.16.1.1;  
      }  
    }  
    family iso;  
    family inet6 {  
      address 8016::1:2/126;  
    }  
  }  
}
```

Configure a Link Services interface with MFR FRF.15

```plaintext
[edit interfaces]
t1-0/0/0 {  
  encapsulation frame-relay;  
  unit 0 {  
    dci 16;  
    family mlfr-end-to-end {  
      bundle ls-0/3/0.0;  
    }  
  }  
}  
t1-0/0/1 {  
  encapsulation frame-relay;  
  unit 0 {  
    dci 16;  
    family mlfr-end-to-end {  
      bundle ls-0/3/0.0;  
    }  
  }  
}
```
ls-0/3/0 {
    unit 0 {
        encapsulation multilink-frame-relay-end-to-end;
        family inet {
            address 10.16.1.2/32 {
                destination 10.16.1.1;
            }
        }
        family iso;
        family inet6 {
            address 8016::1:2/126;
        }
    }
}

Configure a Link Services Interface with MLFR FRF.16

[edit chassis]
  fpc 1 {
    pic 2 {
        mlfr-uni-nni-bundles 5;
    }
  }

[edit interfaces]
  t1-0/0/0 {
    encapsulation multilink-frame-relay-uni-nni;
    unit 0 {
        family mlfr-uni-nni {
            bundle ls-0/3/0:0;
        }
    }
  }
  t1-0/0/1 {
    encapsulation multilink-frame-relay-uni-nni;
    unit 0 {
        family mlfr-uni-nni {
            bundle ls-0/3/0:0;
        }
    }
  }
  ls-1/2/0:0 {
    dce;
    encapsulation multilink-frame-relay-uni-nni;
    unit 0 {
        dlc 26;
        family inet {
            address 10.26.1.1/32 {
                destination 10.26.1.2;
            }
        }
    }
  }
Chapter 26
Configure Serial Interfaces

Devices that communicate over a serial interface are divided into two classes: data terminal equipment (DTE) and data circuit-terminating equipment (DCE). Juniper Networks Serial Physical Interface Cards (PICs) have two ports per PIC and support full-duplex data transmission. These PICs support DTE mode only. On the Serial PIC, you can configure three types of serial interfaces:

- **EIA-530**—An Electronics Industries Alliance (EIA) standard for the interconnection of DTE and DCE employing serial binary data interchange with control information exchanged on separate control circuits.

- **V.35**—An ITU-T standard describing a synchronous, physical layer protocol used for communications between a network access device and a packet network. V.35 is most commonly used in the United States and in Europe.

- **X.21**—An ITU-T standard for serial communications over synchronous digital lines. The X.21 protocol is used primarily in Europe and Japan.

The following standards apply to serial interfaces:

- **TIA/EIA Standard 530**, High-Speed 25-Position Interface for Data Terminal Equipment and Data Circuit-Terminating Equipment, defines the signals on the cable and specifies the connector at the end of the cable.

- **TIA/EIA Standard 232**, Interface between Data Terminal Equipment and Data Circuit-Terminating Equipment Employing Serial Binary Data Interchange, describes the physical interface and protocol for serial data communication.

- **ITU-T Recommendation V.35**, Data Transmission at 48 kbit/s Using 60-108 kHz Group Band Circuits. Note that the Juniper Networks Serial PIC supports V.35 interfaces with speeds higher than 48 kilobits per second.

To configure serial physical interface properties, include the `serial-options` statement at the
[edit interfaces se-fpc/ pic/ port] hierarchy level:

```
[edit interfaces se-fpc/ pic/ port]
serial-options {
    clock-rate rate;
clocking-mode (dce | dte | loop);
control-leads {
    control-signal (assert | de-assert | normal);
    cts (ignore | normal | require);
    dcd (ignore | normal | require);
    dsr (ignore | normal | require);
    dtr signal-handling-option;
    ignore-all;
    indication (ignore | normal | require);
    rts (assert | de-assert | normal);
    tm (ignore | normal | require);
}
clock-polarity (positive | negative);
cts-polarity (positive | negative);
dcd-polarity (positive | negative);
dsr-polarity (positive | negative);
dtr-circuit (balanced | unbalanced);
dtr-polarity (positive | negative);
encoding (nrz | nrzi);
indication-polarity (positive | negative);
line-protocol protocol;
loopback mode;
rts-polarity (positive | negative);
transmit-clock invert;
}
```

This chapter discusses configuration of the following serial interface properties:

- Configure the Serial Line Protocol on page 347
- Configure the Serial Clocking Mode on page 350
- Configure the Serial Signal Handling on page 352
- Configure the Serial DTR Circuit on page 355
- Configure Serial Signal Polarities on page 355
- Configure Serial Loopback Capability on page 356
- Configure Serial Line Encoding on page 357

There are no serial interface-specific logical properties. For information about general logical properties that you can configure, see “Configure Logical Interface Properties” on page 67.
Configure the Serial Line Protocol

By default, serial interfaces use the EIA-530 line protocol. You can configure each port on the PIC independently to use one of the following line protocols:

- EIA-530
- V.35
- X.21

To configure the serial line protocol, include the `line-protocol` statement at the [edit interfaces se-fpc/pic/port serial-options] hierarchy level, specifying the eia530, v.35, or x.21 option:

```
[edit interfaces se-fpc/pic/port serial-options]
line-protocol protocol;
```

Serial Interface Default Settings

The following sections show the default settings for serial interfaces.

**EIA-530 interface default settings**

If you do not include the `line-protocol` statement in the configuration or if you explicitly configure the default EIA-530 line protocol, the default settings are as follows:

```
[edit interfaces se-fpc/pic/port]
serial-options {
  control-leads {
    cts normal;
    dcd normal;
    dsr normal;
    dtr normal;
    rts normal;
    tm normal;
  }
  clock-rate 16.384mhz;
  clocking-mode loop;
  cts-polarity positive;
  dcd-polarity positive;
  dsr-polarity positive;
  dtr-circuit balanced;
  dtr-polarity positive;
  encoding nrz;
  rts-polarity positive;
  tm-polarity positive;
}
```
V.35 interface default settings

If you include the line-protocol v.35 statement in the configuration, the default settings are as follows:

```junos
[edit interfaces self/pc/pic/port]
serial-options {
    control-leads {
        cts normal;
        dcd normal;
        dsr normal;
        dtr normal;
        rts normal;
    }
    clock-rate 16.384mhz
    clocking-mode loop;
    cts-polarity positive;
    dcd-polarity positive;
    dsr-polarity positive;
    dtr-circuit balanced;
    rts-polarity positive;
    encoding nrz;
}
```

X.21 interface default settings

If you include the line-protocol x.21 statement in the configuration, the default settings are as follows:

```junos
[edit interfaces self/pc/pic/port]
serial-options {
    control-leads {
        control-signal normal;
        indication normal;
    }
    clock-rate 16.384mhz
    clocking-mode loop;
    control-signal-polarity positive;
    encoding nrz;
    indication-polarity positive;
}
Serial Interface Invalid Statements

The following sections show the invalid configuration statements for each type of serial interface. If you include the following statements in the configuration, an error message indicates the location of the error and the configuration is not activated.

EIA-530 interface invalid statements
If you do not include the line-protocol statement in the configuration or if you explicitly configure the default EIA-530 line protocol, the following statements are invalid:

```
[edit interfaces se-fpc/pic/port]
serial-options {
  control-leads {
    control-signal (assert | de-assert | normal);
    indication (ignore | normal | require);
  }
  control-signal-polarity (positive | negative);
  indication-polarity (positive | negative);
}
```

V.35 interface invalid statements
If you include the line-protocol v.35 statement in the configuration, the following statements are invalid:

```
[edit interfaces se-fpc/pic/port]
serial-options {
  control-leads {
    control-signal (assert | de-assert | normal);
    indication (ignore | normal | require);
    tm (ignore | normal | require);
  }
  control-signal-polarity (positive | negative);
  indication-polarity (positive | negative);
  loopback (dce-local | dce-remote);
  tm-polarity (positive | negative);
}
```

X.21 interface invalid statements
If you include the line-protocol x.21 statement in the configuration, the following statements are invalid:

```
[edit interfaces se-fpc/pic/port]
serial-options {
  control-leads {
    cts (ignore | normal | require);
    dcd (ignore | normal | require);
    dtr (assert | de-assert | normal);
    rts (assert | de-assert | normal);
    tm (ignore | normal | require);
  }
  clocking-mode (dce | dte);
  cts-polarity (positive | negative);
  dce-polarity (positive | negative);
  dsr-polarity (positive | negative);
  dtr-circuit (balanced | unbalanced);
  dtr-polarity (positive | negative);
  loopback (dce-local | dce-remote);
  rts-polarity (positive | negative);
  tm-polarity (positive | negative);
}
```
Configure the Serial Clocking Mode

By default, serial interfaces use loop clocking mode. For EIA-530 and V.35 interfaces, you can configure each port on the PIC independently to use loop, DCE, or DTE clocking mode. For X.21 interfaces, only loop clocking mode is supported.

The three clocking modes work as follows:

- Loop clocking mode—Uses the DCE’s RX clock to clock data from the DCE to the DTE.
- DCE clocking mode—Uses the TXC clock, which is generated by the DCE specifically to be used by the DTE as the DTE’s transmit clock.
- DTE clocking mode—Also known as line timing, uses an internally generated clock. You can configure the speed of this clock by including the clock-rate statement at the [edit interfaces se-fpc/ pic/ port serial-options] hierarchy level. For more information about the DTE clock rate, see “Configure the DTE Clock Rate” on page 351.

Note that DCE clocking mode and loop clocking mode use external clocks generated by the DCE. Figure 23 shows the clock sources of loop, DCE, and DTE clocking modes.

Figure 23: Serial Interface Clocking Mode

To configure the clocking mode of a serial interface, include the clocking-mode statement at the [edit interfaces se-fpc/ pic/ port serial-options] hierarchy level:

```plaintext
[edit interfaces se-fpc/ pic/ port serial-options]
clocking-mode (dce | dte | loop);
```
Invert the Serial Interface Transmit Clock

When an externally timed clocking mode (DCE or loop) is used, long cables might introduce a phase shift of the DTE-transmitted clock and data. At high speeds, this phase shift might cause errors. Inverting the transmit clock corrects the phase shift, thereby reducing error rates.

By default, the transmit clock is not inverted. To invert the transmit clock, include the transmit-clock invert statement at the [edit interfaces se-fpc/pic/port serial-options] hierarchy level:

```
[edit interfaces se-fpc/pic/port serial-options]
transmit-clock invert;
```

Configure the DTE Clock Rate

By default, the serial interface has a clock rate of 16.384 MHz. For EIA-530 and V.35 interfaces with DTE clocking mode configured, you can configure the clock rate. For more information about DTE clocking mode, see “Configure the Serial Clocking Mode” on page 350.

To configure the clock rate, include the clock-rate statement at the [edit interfaces se-fpc/pic/port serial-options] hierarchy level:

```
[edit interfaces se-fpc/pic/port serial-options]
clock-rate rate;
```

You can configure the following interface speeds:

- 2.048 MHz
- 2.341 MHz
- 2.731 MHz
- 3.277 MHz
- 4.096 MHz
- 5.461 MHz
- 8.192 MHz
- 16.384 MHz
Although the serial interface is intended for use at the default rate of 16.384 MHz, you might need to use a slower rate if any of the following conditions prevail:

- The interconnecting cable is too long for effective operation.
- The interconnecting cable is exposed to an extraneous noise source that might cause an unwanted voltage in excess of +1 volt measured differentially between the signal conductor and circuit common at the load end of the cable, with a 50-ohm resistor substituted for the generator.
- You need to minimize interference with other signals.
- You need to invert signals.

For detailed information about the relationship between signaling rate and interface cable distance, see the following standards:

- EIA-422-A, Electrical Characteristics of Balanced Voltage Digital Interface Circuits
- EIA-423-A, Electrical Characteristics of Unbalanced Voltage Digital Interface Circuits

Configure the Serial Signal Handling

By default, normal signal handling is enabled for all signals. For each signal, the normal option applies to the normal signal handling for that signal, as defined by the following standards:

- TIA/EIA Standard 530
- ITU-T Recommendation V.35
- ITU-T Recommendation X.21

Table 28 shows the serial interface modes that support each signal type.

Table 28: Signal Handling by Serial Interface Type

<table>
<thead>
<tr>
<th>Signal</th>
<th>Serial Interfaces</th>
</tr>
</thead>
<tbody>
<tr>
<td>From-DCE signals</td>
<td></td>
</tr>
<tr>
<td>Clear-to-send (CTS)</td>
<td>EIA-530 and V.35</td>
</tr>
<tr>
<td>Data-carrier-detect (DCD)</td>
<td>EIA-530 and V.35</td>
</tr>
<tr>
<td>Data-set-ready (DSR)</td>
<td>EIA-530 and V.35</td>
</tr>
<tr>
<td>Indication</td>
<td>X.21 only</td>
</tr>
<tr>
<td>Test-mode (TM)</td>
<td>EIA-530 only</td>
</tr>
<tr>
<td>To-DCE signals</td>
<td></td>
</tr>
<tr>
<td>Control-signal</td>
<td>X.21 only</td>
</tr>
<tr>
<td>Data-transfer-ready (DTR)</td>
<td>EIA-530 and V.35</td>
</tr>
<tr>
<td>Request-to-send (RTS)</td>
<td>EIA-530 and V.35</td>
</tr>
</tbody>
</table>
You configure serial interface signal characteristics by including the `control-leads` statement at the `[edit interfaces se-fpc/pic/port serial-options]` hierarchy level:

```plaintext
[edit interfaces se-fpc/pic/port serial-options]
control-leads {
  control-signal (assert | de-assert | normal);
  cts (ignore | normal | require);
  dcd (ignore | normal | require);
  dsr (ignore | normal | require);
  dtr signal-handling-option;
  ignore-all;
  indication (ignore | normal | require);
  rts (assert | de-assert | normal);
  tm (ignore | normal | require);
}
```

For EIA-530 and V.35 interfaces, you configure to-DCE signals by including the `dtr` and `rts` statements at the `[edit interfaces se-fpc/pic/port serial-options control-leads]` hierarchy level, specifying the `assert`, `de-assert`, or `normal` option:

```plaintext
[edit interfaces se-fpc/pic/port serial-options control-leads]
dtr (assert | de-assert | normal);
rts (assert | de-assert | normal);
```

For X.21 interfaces, you configure to-DCE signals by including the `control-signal` statement at the `[edit interfaces se-fpc/pic/port serial-options control-leads]` hierarchy level, specifying the `ignore`, `normal`, or `require` option:

```plaintext
[edit interfaces se-fpc/pic/port serial-options control-leads]
control-signal (assert | de-assert | normal);
```

Assertion is when the positive side of a given signal is at potential high-level output voltage ($V_{oh}$), while the negative side of the same signal is at potential low-level output voltage ($V_{ol}$). Deassertion is when the positive side of a given signal is at potential $V_{ol}$, while the negative side of the same signal is at potential $V_{oh}$.

For the DTR signal, you can configure normal signal handling using the signal for automatic resynchronization by including the `auto-synchronize` statement at the `[edit interfaces se-fpc/pic/port serial-options control-leads dtr]` hierarchy level:

```plaintext
[edit interfaces se-fpc/pic/port serial-options control-leads dtr]
auto-synchronize {
  duration milliseconds;
  interval seconds;
}
```

The pulse duration of resynchronization can be from 1 through 1000 milliseconds. The offset interval for resynchronization can be from 1 through 31 seconds.

For EIA-530 and V.35 interfaces, you configure from-DCE signals by including the `cts`, `dcd`, and `dsr` statements at the `[edit interfaces se-fpc/pic/port serial-options control-leads]` hierarchy level, specifying the `ignore`, `normal`, or `require` option:

```plaintext
[edit interfaces se-fpc/pic/port serial-options control-leads]
cts (ignore | normal | require);
dcd (ignore | normal | require);
dsrr (ignore | normal | require);
```
For X.21 interfaces, you configure from-DCE signals by including the indication statement at the [edit interfaces se-fpc/pic/port serial-options control-leads] hierarchy level, specifying the ignore, normal, or require option:

```
[edit interfaces se-fpc/pic/port serial-options control-leads]
  indication (ignore | normal | require);
```

For EIA-530 interfaces only, you can configure from-DCE test-mode (TM) signaling by including the tm statement at the [edit interfaces se-fpc/pic/port serial-options control-leads] hierarchy level, specifying the ignore, normal, or require option:

```
[edit interfaces se-fpc/pic/port serial-options control-leads]
  tm (ignore | normal | require);
```

To specify that the from-DCE signal must be asserted, you include the require option in the configuration. To specify that the from-DCE signal must be ignored, you include the ignore option in the configuration.

```
For V.35 and X.21 interfaces, you cannot include the tm statement in the configuration.

For X.21 interfaces, you cannot include the cts, dcd, dsr, dtr, and rts statements in the configuration.

For EIA-530 and V.35 interfaces, you cannot include the control-signal and indication statements in the configuration.

For a complete list of serial options statements that are not supported by each serial interface mode, see “Serial Interface Invalid Statements” on page 349.
```

To return to the default normal signal handling, delete the require, ignore, assert, de-assert, or auto-synchronize statement from the configuration, as shown in the following example:

```
[edit]
user@host# delete interfaces se-0/1/0 serial-options control-leads cts require
```

To explicitly configure normal signal handling, include the normal statement at the [edit interfaces se-fpc/pic/port serial-options control-leads signal] hierarchy level:

```
[edit interfaces se-fpc/pic/port serial-options control-leads signal]
  normal;
```

You can configure the serial interface to ignore all control leads by including the ignore-all statement at the [edit interfaces se-fpc/pic/port serial-options control-leads] hierarchy level:

```
[edit interfaces se-fpc/pic/port serial-options control-leads]
  ignore-all;
```

You can include the ignore-all statement in the configuration only if you do not explicitly enable other signal handling options at the [edit interfaces se-fpc/pic/port serial-options control-leads] hierarchy level.
Configure the Serial DTR Circuit

A balanced circuit has two currents that are equal in magnitude and opposite in phase. An unbalanced circuit has one current and a ground; if a pair of terminals is unbalanced, one side is connected to electrical ground and the other carries the signal. By default, the DTR circuit is balanced.

For EIA-530 and V.35 interfaces, you configure the DTR circuit by including the `dtr-circuit` statement at the `[edit interfaces se-fpc/ pic/ port serial-options]` hierarchy level:

```text
[edit interfaces se-fpc/ pic/ port serial-options]
dtr-circuit (balanced | unbalanced);
```

Configure Serial Signal Polarities

Serial interfaces use a differential protocol signaling technique. Of the two serial signals associated with a circuit, the one referred to as the A signal is denoted with a plus sign, and the one referred to as the B signal is denoted with a minus sign; for example, DTR+ and DTR−. If DTR is low, then DTR+ is negative with respect to DTR−. If DTR is high, then DTR+ is positive with respect to DTR−.

By default, all signal polarities are positive. You can reverse this polarity on a Juniper Networks serial interface. You might need to do this if signals are miswired as a result of reversed polarities.

For EIA-530 and V.35 interfaces, you configure signal polarities by including the `cts-polarity`, `dcd-polarity`, `dsr-polarity`, `dtr-polarity`, `rts-polarity`, and `tm-polarity` statements at the `[edit interfaces se-fpc/ pic/ port serial-options]` hierarchy level:

```text
[edit interfaces se-fpc/ pic/ port serial-options]
  cts-polarity (positive | negative);
  dcd-polarity (positive | negative);
  dsr-polarity (positive | negative);
  dtr-polarity (positive | negative);
  rts-polarity (positive | negative);
  tm-polarity (positive | negative);
```

For X.21 interfaces, you configure signal polarities by including the `control-polarity` and `indication-polarity` statements at the `[edit interfaces se-fpc/ pic/ port serial-options]` hierarchy level:

```text
[edit interfaces se-fpc/ pic/ port serial-options]
  control-polarity (positive | negative);
  indication-polarity (positive | negative);
```
Configure Serial Loopback Capability

From the router, line interface unit (LIU) loopback loops the TX (transmit) data and TX clock back to the router as RX (receive) data and RX clock. From the line, LIU loopback loops the RX data and RX clock back out the line as TX data and TX clock, as shown in Figure 24.

Figure 24: Serial Interface LIU Loopback

DCE local and DCE remote control the EIA-530 interface-specific signals for enabling local and remote loopback on the link partner DCE. Local loopback is shown in Figure 25.

Figure 25: Serial Interface Local Loopback

For EIA-530 interfaces, you can configure DCE local, DCE remote, LIU, and local loopback capability.

For V.35 and X.21 interfaces, you can configure LIU and local loopback capability. DCE local and DCE remote loopbacks are not supported on V.35 and X.21 interfaces.

To configure the loopback capability on a serial interface, include the `loopback` statement at the `[edit interfaces sfp/pic/port serial-options]` hierarchy level, specifying the `dce-local`, `dce-remote`, `liu`, or local option:

```
[edit interfaces sfp/pic/port serial-options]
loopback mode;
```

To disable the loopback capability, remove the `loopback` statement from the configuration:

```
[edit]
user@host# delete interfaces sfp/0/0 serial-options loopback
```
Example: Configure Serial Loopback Capability

To determine the source of a problem, loop packets on the local router, the local DCE, the remote DCE, and the line interface unit (LIU). To do this, include the no-keepalives and encapsulation cisco-hdlc statements at the [edit interfaces se-fpc/pic/port] hierarchy level, and the loopback local option at the [edit interfaces se-fpc/pic/port serial-options] hierarchy level. With this configuration, the link stays up, so you can loop ping packets to a remote router. The loopback local statement causes the interface to loop within the PIC just before the data reaches the transceiver.

```
[edit interfaces]
se-1/0/0 {
    no-keepalives;
    encapsulation cisco-hdlc;
    serial-options {
        loopback local;
    }
    unit 0 {
        family inet {
            address 100.100.100.1/24;
        }
    }
}
```

Check the error counters

You can determine whether there is an internal or external problem by checking the error counters in the output of the `show interfaces se-fpc/pic/port extensive` command:

```
> show interfaces se-1/0/0 extensive
```

Configure Serial Line Encoding

By default, serial interfaces use non-return to zero (NRZ) line encoding. You can configure non-return to zero inverted (NRZI) line encoding if necessary.

To have the interface use NRZI line encoding, include the encoding statement at the [edit interfaces se-fpc/pic/port serial-options] hierarchy level, specifying the nrzi option:

```
[edit interfaces se-fpc/pic/port serial-options]
encoding nrzi;
```

To explicitly configure the default NRZ line encoding, include the encoding statement at the [edit interfaces se-fpc/pic/port serial-options] hierarchy level, specifying the nrz option:

```
[edit interfaces se-fpc/pic/port serial-options]
encoding nrz;
```

When setting the line encoding parameter, you must set the same value for paired ports. Ports 0 and 1 must share the same value.
Synchronous Digital Hierarchy (SDH) is a CCITT standard for a hierarchy of optical transmission rates. Synchronous Optical Network (SONET) is a USA standard that is largely equivalent to SDH. Both are widely used methods for very high speed transmission of voice and data signals across the numerous world-wide fiber-optic networks.

SDH and SONET use light-emitting diodes or lasers to transmit a binary stream of light-on and light-off sequences at a constant rate. At the far end optical sensors convert the pulses of light back to electrical representations of the binary information.

In Wavelength Division Multiplexing (WDM), light at several different wavelengths (colors to a human eye) is transmitted on the same fiber segment, greatly increasing the throughput of each fiber cable.

In Dense Wavelength-Division Multiplexing (DWDM), many optical data streams at different wavelengths are combined into one fiber.

The basic building block of the SONET/SDH hierarchy in the optical domain is an OC-1; in the electrical domain, it is an STS-1. An OC-1 operates at 51.840 Mbps. OC-3 operates at 155.520 Mbps.

A SONET stream can consist of discrete lower-rate traffic flows that have been combined using Time-Division Multiplexing (TDM) techniques. This method is useful, but a portion of the total bandwidth is consumed by the TDM overhead. When a SONET stream consists of only a single, very high speed payload, it is referred to as operating in concatenated mode. A SONET interface operating in this mode has a “c” added to the rate descriptor. For example, a concatenated OC-48 interface is referred to as OC-48c.

SONET and SDH traffic streams exhibit very few differences in behavior that are significant to Juniper Networks SONET/SDH interfaces; in general, this chapter uses SONET/SDH to indicate behavior that is identical for the two standards. However, there is one important difference that requires you to configure the interface specifically for SONET or SDH mode. That difference is in the setting of two bits (the ss-bits) in the pointer. SONET equipment ignores these bits, but SDH equipment uses them to distinguish a VC-4 payload from other types. When configured in SDH mode, Juniper Networks SONET/SDH PICs set the ss-bits to s1s0 2 (binary 10). For more information, see the JUNOS Internet Software Guide: Getting Started.
This chapter discusses configuration of the following SONET/SDH interface properties:

- Configure SONET/SDH Physical Interface Properties on page 360
- Configure the Media MTU on page 373
- Enable Passive Monitoring on page 374
- Configure the Clock Source on page 374
- Configure Receive and Transmit Leaky Bucket Properties on page 375
- Damp Interface Transitions on page 376
- Configure Interface Encapsulation on page 377
- Configure Aggregated SONET/SDH Interfaces on page 380

For examples of SONET/SDH interface configuration, see the following sections:

- Example: Configure SONET Interfaces on page 379
- Example: Configure Aggregated SONET/SDH Interfaces on page 385

**Configure SONET/SDH Physical Interface Properties**

To configure SONET/SDH physical interface properties, include the `sonet-options` statement at the `[edit interfaces interface-name]` hierarchy level:

```conf
[edit interfaces so-fpc/pic/port]
sonet-options {
    aggregate asx;
    aps {
        advertise-interval milliseconds;
        authentication-key key;
        force;
        hold-time milliseconds;
        lockout;
        neighbor address;
        paired-group group-name;
        protect-circuit group-name;
        request;
        revert-time seconds;
        working-circuit group-name;
    }
    bytes {
        e1-quiet value;
        f1 value;
        f2 value;
        s1 value;
        z3 value;
        z4 value;
    }
    fcs (32 | 16);
    loopback (local | remote);
    path-trace trace-string;
    (payload-scrambler | no-payload-scrambler);
```
Configure SONET/SDH Interfaces

Configure SONET/SDH Physical Interface Properties

rfc-2615;
vtmapping (itu-t | klm);
(z0-increment | no-z0-increment);
}

Note that when you configure SONET/SDH OC-48 interfaces for channelized (multiplexed) mode (by including the no-concatenate statement at the [edit chassis fpc slot-number pic pic-number] hierarchy level), the bytes e1-quiet and bytes f1 options have no effect. The bytes f2, bytes z3, bytes z4, and path-trace options work correctly on channel 0 and work in the transmit direction only on channels 1, 2, and 3. When using no-concatenate, you must specify a channel. For more information, see the JUNOS Internet Software Guide: Getting Started.

For DS-3 channels on a Channelized OC-12 interface, the bytes e1-quiet, bytes f1, bytes f2, bytes z3, and bytes z4 options have no effect. The bytes s1 option is supported only for channel 0; it is ignored if configured on channels 1 through 11. The bytes s1 value configured on channel 0 applies to all channels on the interface.

You can also include some of the statements in the sonet-options statement to set SONET parameters on ATM interfaces.

You can configure the following SONET/SDH physical interface properties:

- Configure SONET Header Byte Values on page 361
- Configure an Incrementing STM ID on page 362
- Configure the SONET Frame Checksum on page 363
- Configure SONET Loopback Capability on page 364
- Configure the SONET Path Trace Identifier on page 365
- Configure SONET HDLC Payload Scrambling on page 365
- Configure SONET RFC 2615 Support on page 366
- Configure APS on page 367

Configure SONET Header Byte Values

To configure values in SONET header bytes, include the bytes statement at the [edit interfaces interface-name sonet-options] hierarchy level:

[edit interfaces so-fpc/ pic/ port sonet-options]
bytes {
  e1-quiet value;
  f1 value;
  f2 value;
  s1 value;
  z3 value;
  z4 value;
}
You can configure the following SONET header bytes:

- **e1-quiet**—Default idle byte sent on the orderwire SONET overhead bytes. The router does not support the orderwire channel, and hence sends this byte continuously. For the E1-quiet byte, value can be in the range 0 through 255. The default value is 0x7F.

- **f1, f2, z3, z4**—SONET overhead bytes. For these bytes, value can be in the range 0 through 255. The default value is 0x00.

- **s1**—Synchronization message SONET overhead byte. This byte is normally controlled as a side effect of the system reference clock configuration and the state of the external clock coming from an interface if the system reference clocks have been configured to use an external reference. For the s1 byte, value can be in the range 0 through 255.

On SONET OC-48 interfaces that you configure for channelized (multiplexed) mode (by including the no-concatenate statement at the [edit chassis fpc slot-number pic pic-number] hierarchy level), the bytes e1-quiet and bytes f1 options have no effect. The bytes f2, bytes z3, bytes z4, and path-trace options work correctly on channel 0 and work in the transmit direction only on channels 1, 2, and 3. Table 29 displays JUNOS software framing bytes for several specific speeds.

Table 29: SONET/SDH Framing Bytes for Specific Speeds

<table>
<thead>
<tr>
<th>Overhead Bytes</th>
<th>STM-4</th>
<th>STM-16</th>
<th>STM-64</th>
<th>OC-12</th>
<th>OC-48</th>
<th>OC-192</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1</td>
<td>F6</td>
<td>F6</td>
<td>F6</td>
<td>F6</td>
<td>F6</td>
<td>F6</td>
</tr>
<tr>
<td>A2</td>
<td>28</td>
<td>28</td>
<td>28</td>
<td>28</td>
<td>28</td>
<td>28</td>
</tr>
<tr>
<td>Z0</td>
<td>01/CC</td>
<td>01/CC</td>
<td>01/CC</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>C1</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>1.12</td>
<td>1.48</td>
<td>1.192</td>
</tr>
<tr>
<td>H1/H2</td>
<td>6A0A</td>
<td>6A0A</td>
<td>6A0A</td>
<td>620A</td>
<td>620A</td>
<td>620A</td>
</tr>
<tr>
<td>Concatenated</td>
<td>93FF</td>
<td>93FF</td>
<td>93FF</td>
<td>93FF</td>
<td>93FF</td>
<td>93FF</td>
</tr>
</tbody>
</table>

For DS-3 channels on a Channelized OC-12 interface, the bytes e1-quiet, bytes f1, bytes f2, bytes z3, and bytes z4 options have no effect. The bytes s1 option is supported only for channel 0; it is ignored if configured on channels 1 through 11. The bytes s1 value configured on channel 0 applies to all channels on the interface.

**Configure an Incrementing STM ID**

When configured in SDH framing mode, SONET/SDH interfaces on a Juniper Networks router might not interoperate with some older versions of ADMs or regenerators that require an incrementing STM ID.

Current SDH standards specify a set of 3*n overhead bytes in an STM-n that includes the J0 section trace byte. The rest are essentially unused (spare Z0) and contain hexadecimal values (0x01, 0xCC, 0xCC ... 0xCC). The older version of the standard specified that the same set of bytes should contain an incrementing sequence: 1, 2, 3, ..., 3*n. Their use was still unspecified although they might have been used to assist in frame alignment. You can configure an incrementing STM ID to enable your Juniper Networks router to interoperate with older equipment that relies on these bytes for frame alignment.
The STM identifier has a precise definition in the SDH specifications. In ITU-T Recommendation G.707, Network node interface for the synchronous digital hierarchy (SDH) (03/96), Section 9.2.2.2.

You can explicitly configure an incrementing STM ID rather than a static one in the SDH overhead by including the `z0-increment` statement at the `[edit interfaces interface-name sonet-options]` hierarchy level. You should include this statement only for SDH mode; do not use it for SONET mode:

```
[edit interfaces so-fpc/ pic/ port sonet-options]
z0-increment;
```

To explicitly disable incrementing of the STM ID, include the following statement:

```
[edit interfaces so-fpc/ pic/ port sonet-options]
no-z0-increment;
```

### Configure the SONET Frame Checksum

By default, SONET interfaces use a 16-bit frame checksum. You can configure a 32-bit checksum, which provides more reliable packet verification. However, some older equipment might not support 32-bit checksums.

To configure a 32-bit checksum, include the `fcs` statement at the `[edit interfaces interface-name sonet-options]` hierarchy level:

```
[edit interfaces so-fpc/ pic/ port sonet-options]
fcs 32;
```

To return to the default 16-bit frame checksum, delete the `fcs 32` statement from the configuration:

```
[edit]
user@host# delete interfaces so-fpc/ pic/ port sonet-options fcs 32
```

To explicitly configure a 16-bit checksum, include the `fcs` statement at the `[edit interfaces interface-name sonet-options]` hierarchy level:

```
[edit interfaces so-fpc/ pic/ port sonet-options]
fcs 16;
```

On a Channelized OC-12 interface, the SONET-options `fcs` statement is not supported. To configure FCS on each DS-3 channel, you must include the `t3-options fcs` statement in the configuration for each channel.
Configure SONET Loopback Capability

To configure loopback capability on a SONET interface, include the `loopback` statement at the [edit interfaces interface-name sonet-options] hierarchy level:

```plaintext
[edit interfaces so-fpc/ pic/ port sonet-options]
loopback (local | remote);
```

To turn off the loopback capability, remove the `loopback` statement from the configuration:

```plaintext
[edit]
user@host# delete interfaces so-fpc/ pic/ port sonet-options loopback
```

For channel 0 on channelized interfaces only, you can include the `loopback` statement at the [edit interfaces interface-name interface-type-options] hierarchy level. The loopback setting configured for channel 0 applies to all channels on the channelized interface. The loopback statement is ignored if you include it at this hierarchy level in the configuration of other channels. To configure loopbacks on individual channels, you must include the `channel-type-options loopback` statement in the configuration for each channel. This allows each channel to be put in loopback mode independently.

For example, for DS-3 channels on a Channelized OC-12 interface, the `sonet-options loopback` statement is supported only for channel 0; it is ignored if included in the configuration for channels 1 through 11. The SONET loopback configured for channel 0 applies to all 12 channels equally. To configure loopbacks on the individual DS-3 channels, you must include the `t3-options loopback` statement in the configuration for each channel. This allows each DS-3 channel can be put in loopback mode independently.

Example: Configure SONET Loopback Capability

To determine whether a problem is internal or external, loop packets on both the local and the remote router. To do this, include the `no-keepalives` and `encapsulation cisco-hdlc` statements at the [edit interfaces interface-name] hierarchy level, and the `loopback local` statement at the [edit interfaces interface-name sonet-options] hierarchy level. With this configuration, the link stays up, so you can loop ping packets to a remote router. The `loopback local` statement causes the interface to loop within the PIC just before the data reaches the transceiver.

```plaintext
[edit interfaces]
so-1/0/0 {
    no-keepalives;
    encapsulation cisco-hdlc;
    sonet-options {
        loopback local;
    }
    unit 0 {
        family inet {
            address 100.100.100.1/24;
        }
    }
}
```
Check the error counters You can determine whether there is an internal problem or an external problem by checking the error counters in the output of the show interface interface-name extensive command:

   > show interfaces so-1/0/0 extensive

**Configure the SONET Path Trace Identifier**

The SONET path trace identifier is a text string that identifies the circuit. If the string contains spaces, enclose it in quotation marks. The common convention is to use the circuit identifier as the path trace identifier. If you do not configure an identifier, the JUNOS software uses the system and interface names. The local system’s path trace identifier is displayed when a show interfaces command is issued on the remote system.

For DS-3 channels on a Channelized OC-12 interface, you can configure a unique path trace for each of the 12 channels. Each path trace can be up to 16 bytes. For channels on a Channelized OC-12 Q Performance Processor (QPP) interface, each path trace can be up to 64 bytes.

To configure a path trace identifier, include the path-trace statement at the [edit interfaces interface-name sonet-options] hierarchy level:

   [edit interfaces so-fpc/ pic/ port sonet-options]
   path-trace trace-string;

**Configure SONET HDLC Payload Scrambling**

SONET HDLC payload scrambling, which is enabled by default, provides better link stability. Both sides of a connection must either use or not use scrambling.

   HDLC payload scrambling conflicts with traffic shaping configured using leaky bucket properties. If you configure leaky bucket properties, you must disable payload scrambling, because the JUNOS software rejects configurations that have both features enabled. For more information, see “Configure Receive and Transmit Leaky Bucket Properties” on page 375.

On a Channelized OC-12 interface, the SONET payload-scrambler statement is ignored. To configure scrambling on the DS-3 channels on the interface, include the t3-options payload-scrambler statement in the configuration for each DS-3 channel.

To disable HDLC payload scrambling, include the no-payload-scrambler statement at the [edit interfaces interface-name sonet-options] hierarchy level:

   [edit interfaces so-fpc/ pic/ port sonet-options]
   no-payload-scrambler;

To return to the default, that is, to re-enable payload scrambling, delete the no-payload-scrambler statement from the configuration:

   [edit]
   user@host# delete interfaces so-fpc/ pic/ port sonet-options no-payload-scrambler
To explicitly enable payload scrambling, include the `payload-scrambler` statement at the
[edit interfaces interface-name sonet-options] hierarchy level:

```
[edit interfaces so-fpc/pic/port sonet-options]
payload-scrambler;
```

### Configure SONET RFC 2615 Support

RFC 2615 requires certain C2 header byte and Frame Checksum (FCS) settings that vary from
the default values configured in accordance with RFC 1619. The newer values are optimized
for stronger error detection, especially when combined with payload scrambling at higher bit
rate links.

Table 30 shows the older (RFC 1619) and newer (RFC 2615) values, together with the
Juniper Networks default values.

<table>
<thead>
<tr>
<th>Value</th>
<th>RFC 1619</th>
<th>Default</th>
<th>RFC 2615</th>
</tr>
</thead>
<tbody>
<tr>
<td>SONET C2 header byte</td>
<td>0xCF</td>
<td>0xCF</td>
<td>0x16</td>
</tr>
<tr>
<td>Frame checksum (bit)</td>
<td>16</td>
<td>16</td>
<td>32</td>
</tr>
<tr>
<td>Payload scrambling</td>
<td>n/a</td>
<td>Enabled</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

To enable support for the RFC 2615 features, include the `rfc-2615` statement at the
[edit interfaces interface-name sonet-options] hierarchy level:

```
[edit interfaces so-fpc/pic/port sonet-options]
rfc-2615;
```

### Configure Virtual Tributary Mapping

You can configure virtual tributary mapping to use KLM mode or ITU-T mode. By default,
virtual tributary mapping uses KLM mode.

For the Channelized STM-1 PIC with QPP, you can configure virtual tributary mapping by
including the `vtmapping` statement at the [edit interfaces cau4-fpc/pic/port sonet-options] hierarchy level:

```
[edit interfaces cau4-fpc/pic/port sonet-options]
vtmapping (klm | itu-t);
```

For the STM-1 PIC, you can configure virtual tributary mapping by including the `vtmapping
statement at the [edit chassis fpc slot-number pic pic-number] hierarchy level:

```
[edit chassis fpc slot-number pic pic-number]
vtmapping (klm | itu-t);
```

Table 20 on page 217 lists the KLM mappings used by the Channelized STM-1 to E1 PIC interfaces.
**Configure APS**

Automatic Protection Switching (APS) is used by SONET add/drop multiplexers (ADMs) to protect against circuit failures. The JUNOS implementation of APS allows you to protect against circuit failures between an ADM and one or more routers, and between multiple interfaces in the same router. When a circuit or router fails, a backup immediately takes over.

The JUNOS software supports APS 1+1 switching, bidirectional only, and either revertive or nonrevertive mode. The JUNOS software does not transmit identical data on the working and protect circuits, as the APS specification requires for 1+1 switching, but this causes no operational impact.

For DS-3 channels on a Channelized OC-12 interface, you can configure APS on channel 0 only. If you configure APS on channels 1 through 11, it is ignored.

With APS, you configure two circuits, a working circuit and a protect circuit. Normally, traffic is carried on the working circuit (that is, the working circuit is the active circuit), and the protect circuit is disabled. If the working circuit fails or degrades, or if the working router fails, the ADM and the protect router switch the traffic to the protect circuit, and the protect circuit becomes the active circuit.

To configure APS, you configure a working and a protect circuit, as shown in Figure 26. To protect against a router failure, you connect two routers to the ADM, configuring one of them as the working router and the second as the protect router. To protect against a PIC or an FPC failure, you connect one router to the ADM through both the working and protect circuits, configuring one of the PICs or FPCs as the working circuit and the second as the protect circuit.

![Figure 26: APS Configuration Topologies](image-url)

To protect against router failure

- ADM
  - Working circuit
  - Protect circuit
  - Router A
  - Router B

To protect against FPC or PIC failure

- ADM
  - Working circuit
  - Protect circuit
  - Router A
To configure APS, include the `aps` statement at the `[edit interfaces interface-name sonet-options]` hierarchy level:

```
[edit interfaces interface-name sonet-options]
aps {
  advertise-interval milliseconds;
  authentication-key key;
  force;
  hold-time milliseconds;
  lockout;
  neighbor address;
  paired-group group-name;
  protect-circuit group-name;
  request;
  revert-time seconds;
  working-circuit group-name;
}
```

You can configure the following APS properties:

- Configure Basic APS Support on page 368
- Configure Switching between the Working and Protect Circuits on page 370
- Configure Revertive Mode on page 371
- Configure APS Timers on page 371
- Configure APS Load Sharing between Circuit Pairs on page 372
- Example: Configure APS Load Sharing between Circuit Pairs on page 373

**Configure Basic APS Support**

To set up a basic APS configuration, configure one interface to be the working circuit and a second to be the protect circuit. If you are using APS to protect against router failure, configure one interface on each router. If you are using APS to protect against FPC failure, configure two interfaces on the router, one on each FPC.

For each working–protect circuit pair, configure the following:

- **Group name**—Creates the association between the two circuits. Configure the same group name for both the working and protect routers.

- **Authentication key**—You configure this on both interfaces. Configure the same key for both the working and protect routers.

- **Address of the other interface on the other router**—If you are configuring one router to be the working router and a second to be the protect router, you must configure the address of the remote interface. You configure this on one or both of the interfaces.

  The address you specify for the neighbor must never be routed through the interface on which APS is configured, or instability will result. APS neighbor only applies to inter-router configurations. We strongly recommend that you directly connect the working and protect routers and that you configure the interface address of this shared network as the neighbor address.
The working and protect configurations on the routers must match the circuit configurations on the ADM; that is, the working router must be connected to the ADM’s working circuit and the protect router must be connected to the protect circuit.

To set up a basic APS configuration, include the following statements at the [edit interfaces interface-name sonet-options] hierarchy level:

On the working router/circuit

```
[edit interfaces so-fpc/ pic/ port sonet-options]
aps {
    working-circuit group-name;
    authentication-key key;
    neighbor address; # Include only if protect circuit is on a different router
}
```

On the protect router/circuit

```
aps {
    protect-circuit group-name;
    authentication-key key;
    neighbor address; # Include only if working circuit is on a different router
}
```

Example: Configure Basic APS Support

Configure Router A to be the working router and Router B to be the protect router.

On Router A (the working router)

```
[edit interfaces so-6/1/1 sonet-options]
aps {
    working-circuit San-Jose;
    authentication-key "$9$B2612345";
}
```

On Router B (the protect circuit)

```
[edit interfaces so-0/0/0 sonet-options]
aps {
    protect-circuit San-Jose;
    authentication-key "$9$B2612345";
    neighbor 192.168.1.2; # address of Router B’s interface on the link between A and B
}
```

On a single router, configure one interface to be the working circuit and another interface to be the protect circuit

```
[edit interfaces so-2/1/1 sonet-options]
aps {
    working-circuit Hayward;
    authentication-key blarney;
}
[edit interfaces so-3/0/2 sonet-options]
aps {
    protect-circuit Hayward;
    authentication-key blarney;
}
```
Configure Switching between the Working and Protect Circuits

When there are multiple reasons to switch between the working and protect circuits, a priority scheme is used to decide which circuit to use. The routers and the ADM might automatically switch traffic between the working and protect circuits because of circuit and router failures. You can also choose to switch traffic manually between the working and protect circuits. There are three priority levels of manual configuration, listed here in order from lowest to highest priority:

- Request (also known as manual switch)—Overridden by signal failures, signal degradations, or any higher-priority reasons.
- Force (also known as forced switch)—Overrides manual switches, signal failures, and signal degradation.
- Lockout (also known as lockout of protection)—Do not switch between the working and protect circuits.

A router failure is considered to be equivalent to a signal failure on a circuit.

To perform a manual switch, include the `request` statement at the [edit interfaces interface-name sonet-options aps] hierarchy level. This statement is honored only if there are no higher-priority reasons to switch.

```
[edit interfaces so-fpc/ pic/ port sonet-options aps]
request (protect | working);
```

When the working circuit is operating in nonrevertive mode, use the `request working` statement to switch the circuit manually to being the working circuit or to override the revert timer.

To perform a forced switch, include the `force` statement at the [edit interfaces interface-name sonet-options aps] hierarchy level. This statement is honored only if there are no higher-priority reasons to switch. This configuration can be overridden by a signal failure on the protect circuit, thus causing a switch to the working circuit.

```
[edit interfaces so-fpc/ pic/ port sonet-options aps]
force (protect | working);
```

To configure a lockout of protection, forcing the use of the working circuit and locking out the protect circuit regardless of anything else, include the `lockout` statement at the [edit interfaces interface-name sonet-options aps] hierarchy level:

```
[edit interfaces so-fpc/ pic/ port sonet-options aps]
lockout;
```
Configure Revertive Mode

By default, APS is nonrevertive, which means that if the protect circuit becomes active, traffic is not switched back to the working circuit unless the protect circuit fails or you manually configure a switch to the working circuit. In revertive mode, traffic is automatically switched back to the working circuit.

You should configure the ADM and routers consistently with regard to revertive or nonrevertive mode.

To configure revertive mode, include the `revert-time` statement, specifying the amount of time to wait after the working circuit has again become functional before making the working circuit active again:

```
[edit interfaces sofpc/pic/port sonet-options aps]
revert-time seconds;
```

If you are using nonrevertive APS, you can use the `request working` statement to switch the circuit manually to being the working circuit or to override the revert timer (configured with the `revert-time` statement).

Configure APS Timers

The protect and working routers periodically send packets to their neighbors to advertise that they are operational. By default, these advertisement packets are sent every 1000 milliseconds. A router considers its neighbor to be operational for a period, called the hold time, that is, by default, three times the advertisement interval. If the protect router does not receive an advertisement packet from the working router within the hold time configured on the protect router, the protect router assumes that the working router has failed and becomes active.

APS is symmetric; either side of a circuit can time out the other side (for example, when detecting a crash of the other). Under normal circumstances, the failure of the protect router does not cause any changes because the traffic is already moving on the working router. However, if you had configured `request protect` and the protect router failed, the working router would enable its interface.

To modify the advertisement interval, include the `advertise-interval` at the `[edit interfaces interface-name sonet-options aps]` hierarchy level:

```
[edit interfaces sofpc/pic/port sonet-options aps]
advertise-interval milliseconds;
```

To modify the hold time, include the `hold-time` at the `[edit interfaces interface-name sonet-options aps]` hierarchy level:

```
[edit interfaces sofpc/pic/port sonet-options aps]
hold-time milliseconds;
```

The advertisement intervals and hold times on the protect and working routers can be different.
Configure APS Load Sharing between Circuit Pairs

When two routers are connected to a single ADM, you can have them back up each other on two different pairs of circuits. This arrangement provides load balancing between the routers if one of the working circuits fails.

Figure 27 illustrates load sharing between circuits on two routers. Router A has a working circuit “Start” and a protect circuit “Up,” and Router B has a working circuit “Up” and a protect circuit “Start.” Under normal circumstances, Router A carries the “Start” circuit traffic and Router B carries the “Up” circuit traffic. If the working circuit “Start” were to fail, Router B would end up carrying all the traffic for both the “Start” and “Up” circuits.

To balance the load between the circuits, you pair the two circuits. In this case, you pair the “Start” and “Up” circuits. Then, if the working circuit “Start” fails, the two routers automatically switch the “Up” traffic from the working to the protect circuit so that each router is still carrying only one circuit’s worth of traffic. That is, the working circuit on Router A would be “Up” and the working circuit on Router B would be “Start.”

Figure 27: APS Load Sharing between Circuit Pairs

To configure load sharing between two working-protect circuit pairs, include the paired-group statement when configuring one of the circuits on one of the routers. In this statement, the group-name is the name of the group you assigned to one of the circuits with the working-circuit and protect-circuit statements. The JUNOS software automatically configures the remainder of the load-sharing setup based on the group name.

```
[edit interfaces so-fpc/pic/port sonet-options aps]
  paired-group group-name;
```
**Example: Configure APS Load Sharing between Circuit Pairs**

Configure APS load sharing to match the configuration shown in Figure 27:

**On Router A**
```
[edit interfaces so-7/0/0 sonet-options aps]
user@host# set working-circuit start
[edit interfaces so-7/0/0 sonet-options aps]
user@host# set authentication-key linsey
[edit interfaces so-7/0/0 sonet-options aps]
user@host# set paired-group "Router A-Router B"
... 
[edit interfaces so-0/0/0 sonet-options aps]
user@host# set protect-circuit up
[edit interfaces so-0/0/0 sonet-options aps]
user@host# set authentication-key woolsey
[edit interfaces so-0/0/0 sonet-options aps]
user@host# set paired-group "Router A-Router B"
```

**On Router B**
```
[edit interfaces so-1/0/0 sonet-options aps]
user@host# set working-circuit up
[edit interfaces so-1/0/0 sonet-options aps]
user@host# set authentication-key woolsey
[edit interfaces so-1/0/0 sonet-options aps]
user@host# set paired-group "Router A-Router B"
... 
[edit interfaces so-6/0/0 sonet-options aps]
user@host# set protect-circuit start
[edit interfaces so-6/0/0 sonet-options aps]
user@host# set authentication-key linsey
[edit interfaces so-6/0/0 sonet-options aps]
user@host# set paired-group "Router A-Router B"
```

**Configure the Media MTU**

The default media MTU size used on a physical interface depends on the encapsulation being used on that interface. Table 3 on page 47 and Table 8 on page 49 list MTU sizes for each encapsulation type. For information about configuring the encapsulation on an interface, see “Configure Interface Encapsulation” on page 377.

To modify the default media MTU size for a physical interface, include the `mtu` statement at the `[edit interfaces interface-name]` hierarchy level:

```
[edit interfaces interface-name]
mtu bytes;
```

If you change the size of the media MTU, you must ensure that the size is equal to or greater than the sum of the protocol MTU and the encapsulation overhead. You configure the protocol MTU by including the `mtu` statement at the `[edit interfaces interface-name unit logical-unit-number family family]` hierarchy level, as discussed in “Set the Protocol MTU” on page 83.
Enable Passive Monitoring

The Monitoring Services I and Monitoring Services II PICs are designed to enable IP services. If you have a Monitoring Services PIC and a SONET/SDH PIC installed in an M160 or M40e router, you can monitor IPv4 traffic from another router.

Monitoring Services PICs must be mounted on an enhanced FPC.

On SONET interfaces, you enable packet flow monitoring by including the `passive-monitor-mode` statement at the [edit interfaces so-fpc/pic/port unit logical-unit-number] hierarchy level:

```
[edit interfaces so-fpc/pic/port unit logical-unit-number]
passive-monitor-mode;
```

If you include the `passive-monitor-mode` statement in the configuration, the SONET interface does not send keepalives or alarms, and does not participate actively on the network.

On monitoring services interfaces, you enable packet flow monitoring by including the `family` statement at the [edit interfaces mo-fpc/pic/port unit logical-unit-number] hierarchy level, specifying the `inet` option:

```
[edit interfaces mo-fpc/pic/port unit logical-unit-number]
family inet;
```

For the monitoring services interface, you can configure multiservice physical interface properties. For more information, see “Configure Multiservice Physical Interface Properties” on page 65.

Configure the Clock Source

For interfaces such as SONET that can use different clock sources, you can configure the source of the transmit clock on each interface. The source can be internal (also called line timing or normal) or external (also called loop timing). The default source is internal, which means that each interface uses the router’s internal stratum 3 clock.

For DS-3 channels on a Channelized OC-12 interface, the `clocking` statement is supported only for channel 0; it is ignored if included in the configuration of channels 1 through 11. The clock source configured for channel 0 applies to all channels on the Channelized OC-12 interface. The individual DS-3 channels use a gapped 45-MHz clock as the transmit clock. For more information, see “Clock Sources on Channelized Interfaces” on page 166.

On Channelized STM-1 interfaces, you should configure the clock source at one side of the connection to be internal (the default JUNOS configuration) and configure the other side of the connection to be external.
To configure loop timing on an interface, include the clocking external statement at the [edit interfaces interface-name] hierarchy level:

[edit interfaces interface-name]
clocking external;

To explicitly configure line timing on an interface, include the clocking internal statement at the [edit interfaces interface-name] hierarchy level:

[edit interfaces interface-name]
clocking internal;

Configure Receive and Transmit Leaky Bucket Properties

Congestion control is particularly difficult in high-speed networks with high volumes of traffic. When congestion occurs in such a network, it is usually too late to react. You can avoid congestion by regulating the flow of packets into your network. Smoother flows prevent bursts of packets from arriving at (or being transmitted from) the same interface and causing congestion.

For all interface types except ATM, Fast Ethernet, Gigabit Ethernet, and Channelized QPP, you can configure leaky bucket properties, which allow you to limit the amount of traffic received on and transmitted by a particular interface. You effectively specify what percentage of the interface's total capacity can be used to receive or transmit packets. You might want to set leaky bucket properties to limit the traffic flow from a link that is known to transmit high volumes of traffic.

The leaky bucket is used at the host-network interface to allow packets into the network at a constant rate. Packets might be generated in a bursty manner, but after they pass through the leaky bucket, they enter the network evenly spaced. In some cases, you might want to allow short bursts of packets to enter the network without smoothing them out. By controlling the number of packets that can accumulate in the bucket, the threshold property controls burstiness. The maximum number of packets entering the network in t time units is threshold + rate * t.

By default, leaky buckets are disabled and the interface can receive and transmit packets at the maximum line rate.

For each DS-3 channel on a Channelized OC-12 interface, you can configure unique receive and transmit buckets.

Instead of configuring leaky bucket properties, you can limit traffic flow by configuring policers. Policers work on all interfaces. For more information, see the JUNOS Internet Software Configuration Guide: Policy Framework.

HDLC payload scrambling conflicts with traffic shaping configured using leaky bucket properties. If you configure leaky bucket properties, you must disable payload scrambling, because the JUNOS software rejects configurations that have both features enabled. For more information, see “Configure SONET HDLC Payload Scrambling” on page 365.
To configure leaky bucket properties, include one or both of the receive-bucket and transmit-bucket statements at the [edit interfaces interface-name] hierarchy level:

```plaintext
[edit interfaces interface-name]
receive-bucket {
  overflow (tag | discard);
  rate percentage;
  threshold bytes;
}
transmit-buckets {
  overflow discard;
  rate percentage;
  threshold bytes;
}
```

In the rate statement, specify the percentage of the interface line rate that is available to receive or transmit packets. The percentage can be a value from 0 (none of the interface line rate is available) to 100 (the maximum interface line rate is available). For example, when you set the line rate to 33, the interface receives or transmits at one third of the maximum line rate.

In the threshold statement, specify the bucket threshold, which controls the burstiness of the leaky bucket mechanism. The larger the value, the more bursty the traffic, which means that over a very short amount of time the interface can receive or transmit close to line rate, but the average over a longer time is at the configured bucket rate. The threshold can be a value from 0 through 16777215 bytes. For ease of entry, you can enter number either as a complete decimal number or as a decimal number followed by the abbreviation k (1,000) or m (1,000,000). For example, the entry threshold 2m corresponds to a threshold of 2,000,000 bytes.

In the overflow option, specify how to handle packets that exceed the threshold:

- **tag**—(receive-bucket only) Tag, count, and process received packets that exceed the threshold.
- **discard**—Discard received packets that exceed the threshold. No counting is done.

### Damp Interface Transitions

By default, when an interface changes from being up to being down, or from down to up, this transition is advertised immediately to the router software and hardware. In some situations, for example, when an interface is connected to an ADM or WDM, or to protect against SONET framer holes, you might want to damp interface transitions, thereby not advertising the interface’s transition until a certain period of time has transpired.

When you have damped interface transitions and the interface goes from up to down, the interface is not advertised to the rest of the system as being down until it has remained down for the hold-time period. Similarly when an interface goes from down to up, it is not advertised as being up until it has remained up for the hold-time period.
To damp interface transitions, include the `hold-time` statement at the `[edit interfaces interface-name]` hierarchy level:

```
hold-time up milliseconds down milliseconds;
```

The time can be a value from 0 through 65,534 milliseconds. The time value that you specify is rounded up to the nearest whole second. The default value is 0, which means that interface transitions are not damped.

---

**Configure Interface Encapsulation**

Point-to-Point Protocol (PPP) encapsulation is the default encapsulation type for physical interfaces. You need not configure encapsulation for any physical interfaces that support PPP encapsulation. If you do not configure encapsulation, PPP is used by default. For physical interfaces that do not support PPP encapsulation, you must configure an encapsulation to use for packets transmitted on the interface. You can optionally configure an encapsulation on a logical interface, which is the encapsulation used within certain packet types.

---

**Configure the Encapsulation on a Physical Interface**

For SONET/SDH interfaces, the physical interface encapsulation can be one of the following:

- **Point-to-Point Protocol (PPP)**—PPP encapsulation is defined in RFC 1661, *The Point-to-Point Protocol (PPP) for the Transmission of Multiprotocol Datagrams over Point-to-Point Links*. PPP is the default encapsulation type for physical interfaces. Two related versions are supported:
  - Circuit cross-connect (CCC) version (`ppp-ccc`)—The logical interfaces do not require an encapsulation statement. When you use this encapsulation type, you can configure the family `ccc` only.
  - Translational cross-connect (TCC) version (`ppp-tcc`)—Similar to CCC and has the same configuration restrictions, but used for circuits with different media on either side of the connection.
- **Cisco HDLC**—E1, E3, SONET, T1, and T3 interfaces can use Cisco HDLC encapsulation. Two related versions are supported:
  - CCC version (`cisco-hdlc-ccc`)—The logical interfaces do not require an encapsulation statement. When you use this encapsulation type, you can configure the family `ccc` only.
  - TCC version (`cisco-hdlc-tcc`)—Similar to CCC and has the same configuration restrictions, but is used for circuits with different media on either side of the connection.
Frame Relay—Defined in RFC 1490, Multiprotocol Interconnect over Frame Relay. E1, E3, SONET, T1, and T3 interfaces can use Frame Relay encapsulation. Two related versions are supported:

- CCC version (frame-relay-ccc)—The same as standard Frame Relay for DLCIs 0 through 511. DLCIs 512 through 1022 are dedicated to CCC, and the logical interface must also have frame-relay-ccc encapsulation.

- TCC version (frame-relay-tcc)—Similar to Frame Relay CCC and has the same configuration restrictions, but used for circuits with different media on either side of the connection.

To configure the encapsulation on a physical interface, include the encapsulation statement at the [edit interfaces interface-name] hierarchy level:

```plaintext
[edit interfaces interface-name]
encapsulation (cisco-hdlc | cisco-hdlc-ccc | cisco-hdlc-tcc | frame-relay | frame-relay-ccc | frame-relay-tcc | frame-relay-tcc | ppp | ppp-ccc | ppp-tcc);
```

When you configure a point-to-point encapsulation (such as PPP or Cisco HDLC) on a physical interface, the physical interface can have only one logical interface (that is, only one unit statement) associated with it. When you configure a multipoint encapsulation (such as Frame Relay), the physical interface can have multiple logical units, and the units can be either point to point or multipoint. Use PPP if you are running Cisco IOS Release 12.0 or later. If you need to run Cisco HDLC, the JUNOS software automatically configures an ISO family MTU of 4469 in the router. This is due to an extra byte of padding used by Cisco.

For more information about physical interface encapsulation, see “Configure the Encapsulation on a Physical Interface” on page 51.

**Example: Configure the Encapsulation on a Physical Interface**

Configure PPP encapsulation on a SONET interface. The second two family statements allow IS-IS and MPLS to run on the interface.

```plaintext
[edit interfaces]
so-7/0/0 {  
  encapsulation ppp;
  unit 0 {
    point-to-point;
    family inet {
      address 192.168.1.113/32 {
        destination 192.168.1.114;
      }
    }
    family iso;
    family mpls;
  }
}
```
Configure the Encapsulation on a Logical Interface

Generally, you configure an interface's encapsulation at the [edit interfaces interface-name] hierarchy level. However, for Frame Relay encapsulation, you can also configure the encapsulation type that is used inside the Frame Relay packet itself. To do this, include the encapsulation statement at the [edit interfaces interface-name unit logical-unit-number] hierarchy level, specifying the frame-relay-ccc or frame-relay-tcc option:

```plaintext
[edit interfaces interface-name unit logical-unit-number]
encapsulation (frame-relay-ccc | frame-relay-tcc);
```

The ATM encapsulations are defined in RFC 1483, Multiprotocol Encapsulation over ATM Adaptation Layer 5.

With the atm-nlpid, atm-cisco-nlpid, and atm-vc-mux encapsulations, you can configure the family inet only. With the circuit cross-connect (CCC) encapsulations, you cannot configure a family on the logical interface. A logical interface cannot have frame-relay-ccc encapsulation unless the physical device also has frame-relay-ccc encapsulation. A logical interface cannot have frame-relay-tcc encapsulation unless the physical device also has frame-relay-tcc encapsulation. In addition, you must assign this logical interface a DLCI in the range 512 through 1022 and configure it as point-to-point.

For more information about logical interface encapsulation, see “Configure the Encapsulation on a Logical Interface” on page 75.

Example: Configure SONET Interfaces

SONET interfaces can use either PPP or Cisco HDLC encapsulation. Use PPP if you are running Cisco IOS Release 12.0 or later. If you need to run Cisco HDLC, the JUNOS software automatically configures an ISO family MTU of 4469 in the router. This is due to an extra byte of padding used by Cisco. The following configuration, which uses PPP encapsulation, is sufficient to get a SONET OC-3 or OC-12 interface up and running:

```plaintext
[edit interfaces]
so-fpc/ pic/ port {
  encapsulation ppp;
  unit 0 {
    family inet {
      address local-address {
        destination remote-address;
      }
    }
  }
}
```
Configure Aggregated SONET/SDH Interfaces

The JUNOS software enables link aggregation of SONET/SDH interfaces; this is similar to Ethernet link aggregation, but is not defined in a public standard. The JUNOS software balances traffic across the member links within an aggregated SONET/SDH bundle based on the Layer 3 information carried in the packet. This implementation uses the same load balancing algorithm used for per-packet load balancing. For information about per-packet load balancing, see the JUNOS Internet Software Guide: Routing and Routing Protocols.

You configure an aggregated SONET/SDH virtual link by specifying the link number as a physical device and then associating a set of physical interfaces that have the same speed.

By default, no aggregated SONET/SDH interfaces are created. You must define the number of aggregated SONET/SDH interfaces by including the `device-count` statement at the `[edit chassis aggregated-devices sonet]` hierarchy level:

```
[edit chassis aggregated-devices sonet]
device-count number;
```

The maximum number of aggregated interfaces is 16, and the assigned number can range from 0 through 15. For more information, see the JUNOS Internet Software Guide: Getting Started.

SONET aggregation is proprietary to the JUNOS software and might not work with other software.

To configure aggregated SONET/SDH interfaces, assign a number for the aggregated SONET/SDH interface as `x` at the `[edit interfaces]` hierarchy level:

```
[edit interfaces]
 as x {
      ...
  }
```
The following example shows an aggregated SONET/SDH configuration:

```conf
[edit interfaces]
as0 {
    aggregated-sonet-options {
        minimum-links 1;
        link-speed oc3;
    }
    unit 0 {
        family inet {
            address 10.2.11.1/32 {
                destination 10.2.11.3;
            }
        }
    }
}
```

You also need to specify the constituent physical interfaces by including the `aggregate` statement at the `[edit interfaces interface-name sonet-options]` hierarchy level; for more information, see “Configure SONET Link Aggregation” on page 382. You can optionally specify other physical properties that apply specifically to the aggregated SONET interfaces; for details, see “Configure SONET/SDH Physical Interface Properties” on page 360. For a sample configuration, see “Example: Configure Aggregated SONET/SDH Interfaces” on page 385.

To remove the configuration statements related to as0 and set the aggregated SONET/SDH interface to down state, delete the interface from the configuration:

```
[edit]
user@host# delete interfaces as0
```

However, the aggregated SONET/SDH interface is not deleted until you delete the chassis aggregated-devices sonet device-count configuration statement.

You can configure the following aggregated SONET/SDH properties:

- Configure SONET Link Aggregation on page 382
- Configure Aggregated SONET Link Speed on page 382
- Configure Aggregated SONET Minimum Links on page 383
- Configure Filters or Sampling on Aggregated SONET Links on page 383
Configure SONET Link Aggregation

On SONET/SDH interfaces, you can associate a physical interface with an aggregated SONET interface. To associate the interface with an aggregated SONET link, include the aggregate statement at the [edit interfaces interface-name sonet-options] hierarchy level:

```
[edit interfaces interface-name sonet-options]
aggregate as x;
```

x is the interface instance number and can range from 0 through 15, for a total of 16 aggregated interfaces. You should not mix SONET and SDH mode on the same aggregated interface. You must also include a statement configuring as x at the [edit interfaces] hierarchy level. For a sample configuration, see “Example: Configure Aggregated SONET/SDH Interfaces” on page 385.

You can combine like interfaces only, so each physical interface in the aggregate has to be the same speed.

Configure Aggregated SONET Link Speed

On aggregated SONET interfaces, you can set the required link speed for all interfaces included in the bundle. All interfaces that make up a bundle must be the same speed. If you include in the aggregated SONET interface an individual link that has a speed different from the speed you specify in the link-speed parameter, an error message will be logged.

```
[edit interfaces interface-name aggregated-sonet-options]
link-speed speed;
```

The link speed can be one of the following values:

- `oc3`—Links are OC-3c or STM-1c.
- `oc12`—Links are OC-12c or STM-4c.
- `oc48`—Links are OC-48c or STM-16c.
- `oc192`—Links are OC-192c or STM-64c.

For nonconcatenated interfaces on aggregated SONET interfaces, you can configure the link speed of the aggregate to match the speed of the nonconcatenated interface. For example, an OC-12 PIC can have nonconcatenated interfaces with a link speed of OC-3.
Configure Aggregated SONET Minimum Links

On aggregated SONET interfaces, you can set the minimum number of links that must be up for the bundle as a whole to be labeled up. To set the minimum number, include the minimum-links statement at the [edit interfaces interface-name aggregated-sonet-options] hierarchy level:

```
[edit interfaces interface-name aggregated-sonet-options]
minimum-links number;
```

By default, minimum-link has a value of 1. number can be a value from 1 through 8.

Configure Filters or Sampling on Aggregated SONET Links

To set up firewall filters or sampling on aggregated SONET interfaces, you must configure the asx interface with these properties. The filters function in the same manner as on other interfaces.

To configure a filter, include the filter statement at the [edit interfaces asx] hierarchy level:

```
[edit interfaces asx]
unit logical-unit-number {  
family family {  
    address address {  
        destination address;
    }  
    filter {  
        input input-filter-name;
        output output-filter-name;
    }
}
```

You must also configure separate statements that define the properties of the filter. For more information, see the JUNOS Internet Software Configuration Guide: Policy Framework and “Examples: Configure Filters or Sampling on Aggregated SONET Links” on page 383.

Examples: Configure Filters or Sampling on Aggregated SONET Links

Configure filtering on aggregated SONET/SDH interfaces:

```
[edit interfaces]
asx {  
    unit 0 {  
        family inet {  
            address 10.2.11.1/32 {  
                destination 10.2.11.3;
            }  
            filter {  
                input input-filter-name;
                output output-filter-name;
            }
        }
    }
}
```
Define the filter

```chef
[edit firewall]
filter input-filter-name {
  term match-any-input {
    then {
      accept;
    }
  }
}
filter output-filter-name {
  term match-any-output {
    then {
      accept;
    }
  }
}
```

Configure sampling on aggregated SONET/SDH interfaces

```chef
[edit interfaces]
as x {
  unit 0 {
    family inet {
      address 10.2.11.1/32 {
        destination 10.2.11.3;
      }
      filter {
        input input-sampler-name;
      }
    }
  }
}
```

Define the sampling filter and the forwarding action

```chef
[edit firewall]
filter input-sampler-name {
  term match-any-input {
    then {
      sample;
      accept;
    }
  }
}

[edit forwarding-options]
sampling {
  input {
    family inet {
      rate 10000;
      run-length 1;
    }
  }
}
```
Example: Configure Aggregated SONET/SDH Interfaces

The following configuration is sufficient to get an aggregated SONET/SDH interface up and running:

```
[edit interfaces]
as0 {
    aggregated-sonet-options {
        minimum-links 1;
        link-speed oc3;
    }
    unit 0 {
        family inet {
            address 10.2.11.1/32 {
                destination 10.2.11.3;
            }
        }
    }
}

[edit chassis]
aggregated-devices {
    sonet {
        device-count 15;
    }
}

[edit interfaces]
so-1/3/0 {
    sonet-options {
        aggregate as0;
    }
}
```
Chapter 28
Configure T1 Interfaces

T1 is the basic physical layer protocol used by the Digital Signal level 1 (DS-1) multiplexing method in North America. A T1 interface operates at a bit rate of 1.544 Mbps and can support 24 DS-0 channels. DS-1 standards supported include:

- ANSI T1.107, T1.102
- GR 499-core, GR 253-core
- AT&T Pub 54014
- ITU G.751, G.703

To configure T1-specific physical interface properties, include the `t1-options` statement at the [edit interfaces interface-name] hierarchy level:

```ini
[edit interfaces interface-name]
t1-options {
    bert-algorithm algorithm;
    bert-error-rate rate;
    bert-period seconds;
    buildout (0-132 | 133-265 | 266-398 | 399-531 | 532-655);
    byte-encoding (nx64 | nx56);
    fcs (32 | 16);
    framing (sf | esf);
    idle-cycle-flag (flags | ones);
    invert-data;
    line-encoding (ami | b8zs);
    loopback (local | remote);
    remote-loopback-respond;
    start-end-flag (shared | filler);
    timeslots time-slot-range;
}
```

You can configure the following T1 interface-specific properties:

- Configure T1 BERT Properties on page 388
- Configure T1 Buildout on page 389
- Configure T1 Byte Encoding on page 389
- Configure T1 Data Inversion on page 390
- Configure T1 Frame Checksum on page 390
Configure T1 BERT Properties

You can configure a T1 interface to execute a bit error rate test (BERT) when the interface receives a request to run this test. You specify the duration of the test and the error rate to include in the bit stream by including the `bert-period` and `bert-error-rate` statements at the `[edit interfaces interface-name t1-options]` hierarchy level:

```
[edit interfaces interface-name t1-options]
  bert-algorithm algorithm;
  bert-error-rate rate;
  bert-period seconds;
```

`seconds` is the duration of the BERT procedure. The test can last from 1 to 240 seconds; the default is 10 seconds.

`rate` is the bit error rate. This can be an integer in the range 0 through 7, which corresponds to a bit error rate in the range $10^{-0}$ (that is, 1 error per bit) to $10^{-7}$ (that is, 1 error per 10 million bits).

`algorithm` is the pattern to send in the bit stream. On T1 interfaces, you can also select the pattern to send in the bit stream by including the `bert-algorithm` statement at the `[edit interfaces interface-name interface-options]` hierarchy level:

```
[edit interfaces interface-name interface-options]
  bert-algorithm algorithm;
```
For a list of supported algorithms, see the CLI possible completions; for example:

```plaintext
[edit interfaces t1-0/0/0 t1-options]
user@host# set bert-algorithm ?
Possible completions:
pseudo-2e11-o152  Pattern is 2^11 -1 (per 0.152 standard)
pseudo-2e15-o151  Pattern is 2^15 - 1 (per 0.152 standard)
pseudo-2e20-o151  Pattern is 2^20 - 1 (per 0.151 standard)
pseudo-2e20-o153  Pattern is 2^20 - 1 (per 0.153 standard)
```

See individual interface types for specific hierarchy information. For information about running the BERT procedure, see the JUNOS Internet Software Operational Mode Command Reference: Interfaces.

Configure T1 Buildout

A T1 interface has five possible setting ranges for the T1 line buildout: 0-132, 133-265, 266-398, 399-531, or 532-655 feet. By default, the T1 interface uses the shortest setting (0-132).

To have the interface drive a line at one of the longer distance ranges, include the `buildout` statement with the appropriate value at the `[edit interfaces interface-name t1-options]` hierarchy level:

```plaintext
[edit interfaces interface-name t1-options]
buildout 532-655;
```

Configure T1 Byte Encoding

By default, T1 interfaces use a byte encoding of 8 bits per byte (nx64). You can configure an alternative byte encoding of 7 bits per byte (nx56).

To have the interface use 7 bits per byte encoding, include the `byte-encoding` statement at the `[edit interfaces interface-name t1-options]` hierarchy level, specifying the `nx56` option:

```plaintext
[edit interfaces interface-name t1-options]
byte-encoding nx56;
```

To explicitly configure nx64 byte encoding, include the `byte-encoding` statement at the `[edit interfaces interface-name t1-options]` hierarchy level, specifying the `nx64` option:

```plaintext
[edit interfaces interface-name t1-options]
byte-encoding nx64;
```
Configure T1 Data Inversion

By default, data inversion is disabled. To enable data inversion at the HDLC level, include the `invert-data` statement at the `[edit interfaces interface-name t1-options]` hierarchy level:

```
[edit interfaces interface-name t1-options]
  invert-data;
```

When you enable data inversion, all data bits in the data stream are transmitted inverted; that is, zeroes are transmitted as ones and ones as zeroes. Data inversion is normally used only in AMI mode to guarantee ones density in the transmitted stream.

Configure T1 Frame Checksum

By default, T1 interfaces use a 16-bit frame checksum. You can configure a 32-bit checksum, which provides more reliable packet verification. However, some older equipment might not support 32-bit checksums.

To configure a 32-bit checksum, include the `fcs 32` statement at the `[edit interfaces interface-name t1-options]` hierarchy level:

```
[edit interfaces interface-name t1-options]
  fcs 32;
```

To return to the default 16-bit frame checksum, delete the `fcs 32` statement from the configuration:

```
[edit]
user@host# delete interfaces t1-fpc/pic/port t1-options fcs 32
```

To explicitly configure a 16-bit checksum, include the `fcs 16` statement at the `[edit interfaces interface-name t1-options]` hierarchy level:

```
[edit interfaces interface-name t1-options]
  fcs 16;
```

Configure T1 Remote Loopback Response

The T1 facilities data link loop request signal is used to communicate various network information in the form of in-service monitoring and diagnostics. Extended super frame, through the facilities data link, supports nonintrusive signaling and control, thereby offering clear-channel communication. Remote loopback requests can be over the facilities data link or inband. To configure the router to respond to remote loopback requests, include the `remote-loopback-respond` statement at the `[edit interfaces interface-name t1-options]` hierarchy level:

```
[edit interfaces interface-name t1-options]
  remote-loopback-respond;
```

By default, the router does not respond to remote loopback requests.
Configure T1 Framing

By default, T1 interfaces use extended super frame framing format. You can configure SF (super frame) as an alternative.

To have the interface use the SF framing format, include the `framing` statement at the `[edit interfaces interface-name t1-options]` hierarchy level, specifying the `sf` option:

```
[edit interfaces interface-name t1-options]
framing sf;
```

To explicitly configure ESF framing, include the `framing` statement at the `[edit interfaces interface-name t1-options]` hierarchy level, specifying the `esf` option:

```
[edit interfaces interface-name t1-options]
framing esf;
```

Configure T1 Line Encoding

By default, T1 interfaces use B8ZS line encoding. You can configure AMI line encoding if necessary.

To have the interface use AMI line encoding, include the `line-encoding` statement at the `[edit interfaces interface-name t1-options]` hierarchy level, specifying the `ami` option:

```
[edit interfaces interface-name t1-options]
line-encoding ami;
```

To explicitly configure B8ZS line encoding, include the `line-encoding` statement at the `[edit interfaces interface-name t1-options]` hierarchy level, specifying the `b8zs` option:

```
[edit interfaces interface-name t1-options]
line-encoding b8zs;
```

When setting the line encoding parameter, you must set the same value for paired ports. Ports 0 and 1 must share the same value, and likewise ports 2 and 3 must share the same value, but ports 0 and 1 can have a different value from that of ports 2 and 3.
Configure T1 Loopback Capability

You can configure loopback capability between the local T1 interface and the remote channel service unit (CSU), as shown in Figure 28. You can configure the loopback to be local or remote. With local loopback, the T1 interface can transmit packets to the CSU, but receives its own transmission back again and ignores data from the CSU. With remote loopback, packets sent from the CSU are received by the T1 interface, forwarded if there is a valid route, and immediately retransmitted to the CSU.

Figure 28: Remote and Local T1 Loopback

To configure loopback capability on a T1 interface, include the `loopback` statement at the `[edit interfaces interface-name t1-options]` hierarchy level:

```
[edit interfaces interface-name t1-options]
loopback (local | remote);
```

Packets can be looped on either the local router or the remote CSU. Local and remote loopback loop back both data and clocking information.

For Channelized T3, T1, and NxDS-0 QPP interfaces only, you can include the `loopback` payload statement in the configuration to loop back data only (without clocking information) on the remote router’s PIC. In payload loopback, overhead is recalculated. For T3 QPP interfaces, you can include the `loopback payload` statement at the `[edit interfaces ct3-fpc/pic/port]` and `[edit interfaces t3-fpc/pic/port:channel]` hierarchy levels. For T1 interfaces, you can include the `loopback payload` statement in the configuration at the `[edit interfaces t1-fpc/pic/port:channel]` hierarchy level; it is ignored if included at the `[edit interfaces ct1-fpc/pic/port]` hierarchy level. For NxDS-0 interfaces, payload and remote loopback are the same. If you configure one, the other is ignored. NxDS-0 QPP interfaces do not support local loopback.
To determine whether a problem is internal or external, you can loop packets on both the local and the remote router. To do this, include the no-keepalives and encapsulation cisco-hdlc statements at the [edit interfaces interface-name] hierarchy level and the loopback local statement at the [edit interfaces interface-name t1-options] hierarchy level, as shown in the following example:

```
[edit interfaces]
t1-1/0/0 {
  no-keepalives;
  encapsulation cisco-hdlc;
  t1-options {
    loopback local;
  }
  unit 0 {
    family inet {
      address 100.100.100.1/24;
    }
  }
}
```

With this configuration, the link stays up, so you can loop ping packets to a remote router. The loopback local statement causes the interface to loop within the PIC just before the data reaches the transceiver. You can determine whether there is an internal problem or an external problem by checking the error counters in the output of the show interface interface-name extensive command, for example:

```
> show interfaces t1-1/0/0 extensive
```

To turn off the loopback capability, remove the loopback statement from the configuration:

```
[edit]
user@host# delete interfaces t1-fpc/pic/port t1-options loopback
```

Configure the T1 Idle Cycle Flag

By default, a T1 interface transmits the value 0x7E in the idle cycles. To have the interface transmit the value 0xFF (all ones) instead, include the idle-cycle-flag statement at the [edit interfaces interface-name t1-options] hierarchy level, specifying the ones option:

```
[edit interfaces interface-name t1-options]
idle-cycle-flag ones;
```

To explicitly configure the default value of 0x7E, include the idle-cycle-flag statement with the flags option:

```
[edit interfaces interface-name t1-options]
idle-cycle-flag flags;
```
Configure T1 Start End Flags

By default, a T1 interface waits two idle cycles between sending start and end flags. To configure the interface to share the transmission of start and end flags, include the start-end-flag statement at the [edit interfaces interface-name t1-options] hierarchy level, specifying the shared option:

```
[edit interfaces interface-name t1-options]
start-end-flag shared;
```

To explicitly configure the default of waiting two idle cycles between the start and end flags, include the idle-cycle-flag statement with the filler option:

```
[edit interfaces interface-name t1-options]
start-end-flag filler;
```

Configure Fractional T1 Time Slots

To configure the number of time slots allocated to a fractional T1 interface, include the timeslots statement at the [edit interfaces interface-name t1-options] hierarchy level:

```
[edit interfaces interface-name t1-options]
timeslots time-slot-range;
```

For T1 interfaces, the time-slot range is 1 through 24. There are 24 time slots on a T1 interface. The default is to use all the time slots. You can designate any combination of time slots for usage. You can configure a range of values with hyphens, and you can separate multiple values with commas. Do not include spaces when you specify time slot numbers.

To use time slots 1 through 10, designate the time-slot range as follows:

```
[edit interfaces interface-name t1-options]
timeslots 1-10;
```

To use time slots 1 through 5, time slot 10, and time slot 24, designate the time-slot range as follows:

```
[edit interfaces interface-name t1-options]
timeslots 1-5,10,24;
```

To use the first four odd-numbered time slots, designate the time-slot range as follows:

```
[edit interfaces interface-name t1-options]
timeslots 1,3,5,7;
```

Do not include spaces when you specify time slot numbers.
Chapter 29
Configure T3 Interfaces

T3 is the physical layer protocol used by the Digital Signal level 3 (DS-3) multiplexing method in North America. A T3 interface operates at a bit rate of 44.736 Mbps. The JUNOS software supports payload scrambling and subrate operation on each physical T3 interface. One encapsulation format, PPP, Frame Relay, or HDLC, must be configured for the interface. DS-3 standards supported include:

- ANSI TI.107, TI.102
- GR 499-core, GR 253-core
- Bellcore TR-TSY-000009
- AT&T Pub 54014
- ITU G.751, G.703, G823

To configure T3-specific physical interface properties, include the t3-options statement at the [edit interfaces interface-name] hierarchy level:

```plaintext
[edit interfaces interface-name]
t3-options {
    bert-algorithm algorithm;
    bert-error-rate rate;
    bert-period seconds;
    (cbit-parity | no-cbit-parity);
    compatibility-mode (adtran | digital-link | kentrox | larscom | verilink) <subrate value>;
    fcs (32 | 16);
    (feac-loop-respond | no-feac-loop-respond);
    idle-cycle-flag value;
    (long-buildout | no-long-buildout);
    (loop-timing | no-loop-timing);
    loopback (local | remote);
    (payload-scrambler | no-payload-scrambler);
    start-end-flag value;
}
```
You can configure the following T3 interface-specific properties:

- Configure T3 BERT Properties on page 396
- Disable T3 C-Bit Parity Mode on page 397
- Configure the T3 CSU Compatibility Mode on page 398
- Configure the T3 Frame Checksum on page 399
- Configure the T3 FEAC Response on page 399
- Configure the T3 Idle Cycle Flag on page 400
- Configure the T3 Line Buildout on page 400
- Configure the Channelized T3 Loop Timing on page 401
- Configure T3 Loopback Capability on page 401
- Configure T3 HDLC Payload Scrambling on page 403
- Configure the T3 Start End Flags on page 403

For an example of T3 interface configuration, see “Examples: Configure T3 Interfaces” on page 404.

**Configure T3 BERT Properties**

You can configure a T3 interface to execute a bit error rate test (BERT) when the interface receives a request to run this test. You specify the duration of the test, the pattern to send in the bit stream, and the error rate to include in the bit stream by including the `bert-period`, `bert-algorithm`, and `bert-error-rate` statements at the `[edit interfaces interface-name t3-options]` hierarchy level:

```
[edit interfaces interface-name t3-options]
burt-algorithm algorithm;
burt-error-rate rate;
burt-period seconds;
```

- seconds is the duration of the BERT procedure. The test can last from 1 to 240 seconds; the default is 10 seconds.
- rate is the bit error rate. This can be an integer in the range 0 through 7, which corresponds to a bit error rate in the range $10^{-0}$ (that is, 1 error per bit) to $10^{-7}$ (that is, 1 error per 10 million bits).
- algorithm is the pattern to send in the bit stream. The algorithm for the E1 BERT procedure is `pseudo2e15-o151` (pattern is $2^{15}-1$, as defined in the CCITT/ITU O.151 standard).

On T3 interfaces, you can also select the pattern to send in the bit stream by including the `bert-algorithm` statement at the `[edit interfaces interface-name interface-options]` hierarchy level:

```
[edit interfaces interface-name interface-options]
burt-algorithm algorithm;
```
Disable T3 C-Bit Parity Mode

C-bit parity mode controls the type of framing that is present on the transmitted T3 signal. When C-bit parity mode is enabled, the C-bit positions are used for the FEBE, FEAC, terminal data link, path parity, and mode indicator bits, as defined in ANSI T1.107a-1989. When C-bit parity mode is disabled, the basic T3 framing mode (M13) is used.

By default, C-bit parity mode is enabled. To disable C-bit parity mode and use M13 framing for your T3 link, include the no-cbit-parity statement at the [edit interfaces interface-name t3-options] hierarchy level:

```
[edit interfaces interface-name t3-options]
no-cbit-parity;
```

To return to the default, enabling C-bit parity mode, delete the no-cbit-parity statement from the configuration:

```
[edit]
user@host# delete interfaces t3-fpc/ pic/ port t3-options no-cbit-parity
```

To explicitly enable C-bit parity mode, include the cbit-parity statement at the [edit interfaces interface-name t3-options] hierarchy level:

```
[edit interfaces interface-name t3-options]
cbit-parity;
```
Configure the T3 CSU Compatibility Mode

Subrating a T3 interface reduces the maximum allowable peak rate by limiting the HDLC-encapsulated payload. Subrate modes configure the PIC to connect with channel service units (CSUs) that use proprietary methods of multiplexing. You can configure T3 interfaces to be compatible with a Digital Link, Kentrox, or Larscom CSU. For T3 QPP channels only, you can also configure Adtran or Verilink CSU compatibility. To configure a T3 interface so that it is compatible with the CSU at the remote end of the line, include the compatibility statement at the [edit interfaces interface-name t3-options] hierarchy level:

```
[edit interfaces interface-name t3-options]
compatibility-mode (adtran | digital-link | kentrox | larscom | verilink) <subrate value>;
```

The subrate of a T3 interface must exactly match that of the remote CSU. To specify the subrate, include the subrate statement in the configuration:

- For Adtran CSUs, specify the subrate as a number from 1 through 588 that exactly matches the value configured on the CSU. A subrate value of 588 corresponds to 44.2 Mbps, or 100 percent of the HDLC-encapsulated payload. A subrate value of 1 corresponds to 44.2 / 588, which is 75.17 kbps, or 0.17 percent of the HDLC-encapsulated payload.

- For Digital Link CSUs, specify the subrate as the data rate you configured on the CSU in the format xKb or x.xMb. For a list of specific rate values, use the command completion feature in the CLI. The range is 301 kbps through 44.2 Mbps.

- For Kentrox CSUs, specify the subrate as a number from 1 through 69 that exactly matches the value configured on the CSU. A subrate value of 69 corresponds to 34.995097 Mbps, or 79.17 percent of the HDLC-encapsulated payload (44.2 Mbps). A subrate value of 1 corresponds to 999.958 kbps, which is 2.26 percent of the HDLC-encapsulated payload. Each increment of the subrate value corresponds to a rate increment of about 0.5 Mbps. Kentrox subrate is supported on T3 QPP channels only.

- For Larscom CSUs, specify the subrate as a number from 1 through 14 that exactly matches the value configured on the CSU. A subrate value of 14 corresponds to 44.2 Mbps, or 100 percent of the HDLC-encapsulated payload. A subrate value of 1 corresponds to 44.2 / 14, which is 3.16 Mbps, 7.15 percent of the HDLC-encapsulated payload.

- For Verilink CSUs, specify the subrate as a number from 1 through 28 that exactly matches the value configured on the CSU. A subrate value of 28 corresponds to 44.2 Mbps, or 100 percent of the HDLC-encapsulated payload, and a subrate value of 1 corresponds to 1.57891765 Mbps, or 3.57 percent of the HDLC-encapsulated payload.
Configure the T3 Frame Checksum

By default, T3 interfaces use a 16-bit frame checksum. You can configure a 32-bit checksum, which provides more reliable packet verification. However, some older equipment might not support 32-bit checksums.

On a Channelized OC-12 interface, the `fcs` statement is not supported. To configure FCS on each DS-3 channel, you must include the `t3-options fcs` statement in the configuration for each channel.

To configure a 32-bit checksum, include the `fcs` statement at the `[edit interfaces interface-name t3-options]` hierarchy level:

```
[edit interfaces interface-name t3-options]
fcs 32;
```

To return to the default 16-bit frame checksum, delete the `fcs 32` statement from the configuration:

```
[edit]
user@host# delete interfaces t3-fpc/ pic/ port t3-options fcs 32
```

To explicitly configure a 16-bit checksum, include the `fcs` statement at the `[edit interfaces interface-name t3-options]` hierarchy level:

```
[edit interfaces interface-name t3-options]
fcs 16;
```

Configure the T3 FEAC Response

The T3 far-end alarm and control (FEAC) signal is used to send alarm or status information from the far-end terminal back to the near-end terminal and to initiate T3 loopbacks at the far-end terminal from the near-end terminal.

By default, the router does not respond to FEAC requests. To allow the remote CSU to place the local router into loopback, you must configure the router to respond to the CSU's FEAC request by including the `feac-loop-respond` statement at the `[edit interfaces interface-name t3-options]` hierarchy level:

```
[edit interfaces interface-name t3-options]
feac-loop-respond;
```

If you configure remote or local loopback with the `T3 loopback` statement, the router does not respond to FEAC requests from the CSU even if you include the `feac-loop-respond` statement in the configuration. For the router to respond, you must delete the loopback statement from the configuration.

To explicitly configure the router not to respond to FEAC requests, include the `no-feac-loop` statement at the `[edit interfaces interface-name t3-options]` hierarchy level:

```
[edit interfaces interface-name t3-options]
no-feac-loop-respond;
```
Configure the T3 Idle Cycle Flag

By default, a T3 interface transmits the value 0x7E in the idle cycles. To have the interface transmit the value 0xFF (all ones) instead, include the idle-cycle-flag statement at the [edit interfaces interface-name t3-options] hierarchy level, specifying the ones option:

```
[edit interfaces interface-name t3-options]
idle-cycle-flag ones;
```

To explicitly configure the default value of 0x7E, include the idle-cycle-flag statement with the flags option:

```
[edit interfaces interface-name t3-options]
idle-cycle-flag flags;
```

Configure the T3 Line Buildout

A T3 interface has two settings for the T3 line buildout: a short setting, which is less than 225 feet (about 68 meters), and a long setting, which is greater than 225 feet. By default, the interface uses the short setting.

The long-buildout and no-long-buildout statements apply only to copper-cable-based T3 interfaces. You cannot configure a line buildout for a DS-3 channel on a Channelized OC-12 interface, which runs over fiber-optic cable. If you configure this statement on a Channelized OC-12 interface, it is ignored.

To have the interface drive a line that is longer than 255 feet, include the long-buildout statement at the [edit interfaces interface-name t3-options] hierarchy level:

```
[edit interfaces interface-name t3-options]
long-buildout;
```

To explicitly configure the default short line buildout, include the no-long-buildout statement at the [edit interfaces interface-name t3-options] hierarchy level:

```
[edit interfaces interface-name t3-options]
no-long-buildout;
```
Configure the Channelized T3 Loop Timing

For channelized T3 interfaces, you can configure loop timing on all T1 channels under the Channelized T3 interface. The loop-timing and no-loop-timing statements apply only to channelized T3 interfaces. If you attempt to configure these statements on any other interface type, they are ignored.

To configure loop timing for all T1 channels under the Channelized T3 interface, include the loop-timing statement at the [edit interfaces ct3-fpc/pic/port t3-options] hierarchy level:

```
[edit interfaces ct3-fpc/pic/port t3-options]
loop-timing;
```

To explicitly configure the default no loop timing for all T1 channels under the Channelized T3 QPP interface, include the no-loop-timing statement at the [edit interfaces ct3-fpc/pic/port t3-options] hierarchy level:

```
[edit interfaces ct3-fpc/pic/port t3-options]
no-loop-timing;
```

Configure T3 Loopback Capability

You can configure loopback capability between the local T3 interface and the remote CSU, as shown in Figure 29. You can configure the loopback to be local or remote. With local loopback, the T3 interface can transmit packets to the CSU, but receives its own transmission back again and ignores data from the CSU. With remote loopback, packets sent from the CSU are received by the T3 interface, forwarded if there is a valid route, and immediately retransmitted to the CSU.

Figure 29: Remote and Local T3 Loopback

```
To configure loopback capability on a T3 interface, include the loopback statement at the [edit interfaces interface-name t3-options] hierarchy level:

```
[edit interfaces interface-name t3-options]
loopback (local | payload | remote);
```

Packets can be looped on either the local router or the remote CSU. Local and remote loopback loop back both data and clocking information.
Configure T3 Loopback Capability

For Channelized T3, T1, and NxDS-0 QPP interfaces only, you can include the loopback payload statement in the configuration to loopback data only (without clocking information) on the remote router’s PIC. In payload loopback, overhead is recalculated. For T3 QPP interfaces, you can include the loopback payload statement at the [edit interfaces ct3-fpc/pic/port] and [edit interfaces t3-fpc/pic/port:channel] hierarchy levels. For T1 interfaces, you can include the loopback payload statement in the configuration at the [edit interfaces t1-fpc/pic/port:channel] hierarchy level; it is ignored if included at the [edit interfaces ct1-fpc/pic/port] hierarchy level. For NxDS-0 interfaces, payload and remote loopback are the same. If you configure one, the other is ignored. NxDS-0 QPP interfaces do not support local loopback.

To determine whether a problem is internal or external, you can loop packets on both the local and the remote router. To do this, include the no-keepalives and encapsulation cisco-hdlc statements at the [edit interfaces interface-name] hierarchy level and the loopback local statement at the [edit interfaces interface-name t3-options] hierarchy level, as shown in the following example:

```plaintext
[edit interfaces]
t3-1/0/0 {
  no-keepalives;
  encapsulation cisco-hdlc;
  t3-options {
    loopback local;
  }
  unit 0 {
    family inet {
      address 100.100.100.1/24;
    }
  }
}
```

With this configuration, the link stays up, so you can loop ping packets to a remote router. The loopback local statement causes the interface to loop within the PIC just before the data reaches the transceiver. You can determine whether there is an internal problem or an external problem by checking the error counters in the output of the `show interface interface-name extensive` command, for example:

```
> show interfaces t3-1/0/0 extensive
```

To turn off the loopback capability, remove the loopback statement from the configuration:

```plaintext
[edit]
user@host# delete interfaces t3-fpc/pic/port t3-options loopback
```

For channel 0 on channelized interfaces only, you can include the loopback statement at the [edit interfaces interface-name interface-type-options] hierarchy level. The loopback setting configured for channel 0 applies to all channels on the channelized interface. The loopback statement is ignored if you include it at this hierarchy level in the configuration of other channels. To configure loopbacks on individual channels, you must include the channel-type-options loopback statement in the configuration for each channel. This allows each channel to be put in loopback mode independently.

For example, for DS-3 channels on a Channelized OC-12 interface, the sonet-options loopback statement is supported only for channel 0; it is ignored if included in the configuration for channels 1 through 11. The SONET loopback configured for channel 0 applies to all 12 channels equally. To configure loopbacks on the individual DS-3 channels, you must include the t3-options loopback statement in the configuration for each channel. This allows each DS-3 channel can be put in loopback mode independently.
Configure T3 HDLC Payload Scrambling

T3 HDLC payload scrambling, which is disabled by default, provides better link stability. Both sides of a connection must either use or not use scrambling.

On a Channelized OC-12 interface, the SONET payload-scrambler statement is ignored. To configure scrambling on the DS-3 channels on the interface, you can include the t3-options payload-scrambler statement at the [edit interfaces interface-name t3-options] hierarchy level for each DS-3 channel:

[edit interfaces interface-name t3-options]
payload-scrambler;

To explicitly disable HDLC payload scrambling, include the no-payload-scrambler statement at the [edit interfaces interface-name t3-options] hierarchy level:

[edit interfaces interface-name t3-options]
no-payload-scrambler;

To disable payload scrambling again (return to the default), delete the payload-scrambler statement from the configuration:

[edit]
user@host# delete interfaces t3-fpc/ pic/ port t3-options payload-scrambler

Configure the T3 Start End Flags

By default, a T3 interface waits two idle cycles between sending start and end flags. To configure the interface to share the transmission of start and end flags, include the start-end-flag statement at the [edit interfaces interface-name t3-options] hierarchy level, specifying the shared option.

[edit interfaces interface-name t3-options]
start-end-flag shared;

To explicitly configure the default of waiting two idle cycles between the start and end flags, include the idle-cycle-flag statement with the filler option:

[edit interfaces interface-name t3-options]
start-end-flag filler;
Examples: Configure T3 Interfaces

T3 interfaces can use PPP, Cisco HDLC, or Frame Relay encapsulation.

PPP encapsulation on a DS-3 PIC

```”
[edit]
interfaces {
  t3-fpc/pic/port {
    encapsulation ppp;
    t3-options {
      no-long-buildout;
      compatibility-mode larscom;
      payload-scrambler;
    }
    unit 0 {
      family inet {
        address 10.0.0.1/32 {
          destination 10.0.0.2;
        }
      }
      family iso;
    }
  }
```

Cisco HDLC encapsulation on a DS-3 PIC

```”
[edit]
interfaces {
  t3-fpc/pic/port {
    encapsulation cisco-hdlc;
    t3-options {
      no-long-buildout;
      compatibility-mode larscom;
      payload-scrambler;
    }
    unit 0 {
      family inet {
        address 10.0.0.1/32 {
          destination 10.0.0.2;
        }
      }
      family iso;
    }
  }
```

```
Frame Relay encapsulation on two routers, where one router is a DTE device and the other is a DCE device

**On DTE Router**

```
[edit]
interfaces {
  t3-fpc/pic/port {
    encapsulation frame-relay;
    t3-options {
      no-long-buildout;
      compatibility-mode larscom;
      payload-scrambler;
    }
    unit 1 {
      dcli 1;
      family inet {
        address 10.0.0.1/32 {
          destination 10.0.0.2;
        }
      }
      family iso;
    }
    unit 2 {
      dcli 2;
      family inet {
        address 10.0.0.3/32 {
          destination 10.0.0.4;
        }
      }
      family iso;
    }
  }
}
```

**On DCE Router**

```
[edit]
interfaces {
  t3-fpc/pic/port {
    dce;
    encapsulation frame-relay;
    t3-options {
      no-long-buildout;
      compatibility-mode larscom;
      payload-scrambler;
    }
    unit 1 {
      dcli 1;
      family inet {
        address 10.0.0.2/32 {
          destination 10.0.0.1;
        }
      }
      family iso;
    }
  }
}
```
unit 2 {
  dlci 2;
  family inet {
    address 10.0.0.4/32 {
      destination 10.0.0.3;
    }
  }
  family iso;
}

Chapter 30
Configure Tunnel Interfaces

By encapsulating arbitrary packets inside a transport protocol, tunneling provides a private, secure path through an otherwise public network. Tunnels connect discontinuous subnetworks and enable encryption interfaces, virtual private networks (VPNs), and Multiprotocol Label Switching (MPLS). If you have a Tunnel PIC installed in your router, you can configure unicast and multicast tunnels.

You can configure two types of tunnels for VPNs: one to facilitate routing table lookups and another to facilitate VPN routing and forwarding instance (VRF) table lookups.

For information about encryption interfaces, see “Configure Encryption Interfaces” on page 257 and the JUNOS Internet Software Configuration Guide: Getting Started. For information about VPNs, see the JUNOS Internet Software Configuration Guide: VPNs. For information about MPLS, see the JUNOS Internet Software Configuration Guide: MPLS Applications.

The JUNOS software supports the following tunnel encapsulations:

- Generic route encapsulation (GRE)
- IP over IP (IP-IP)
- Virtual Private Network (VPN)
- PIM encapsulation

This chapter discusses the following tunnel interface configuration tasks:

- Configure a Unicast Tunnel on page 408
- Configure a Multicast Tunnel on page 409
- Configure a Tunnel Interface for Routing Table Lookup on page 409
- Configure a Tunnel Interface for VRF Table Lookup on page 410
- Configure PIM Tunnels on page 411
- Configure an IPv6-over-IPv4 Tunnel on page 412
Configure a Unicast Tunnel

For examples of tunnel interface configuration, see the following sections:

- Example: Configure Unicast Tunnels on page 412
- Example: Configure a Virtual Loopback Tunnel Interface for VRF Table Lookup on page 414
- Example: Configure an IPv6-over-IPv4 Tunnel on page 415

Configure a Unicast Tunnel

To configure a unicast tunnel, you configure the `gr` interface (to use GRE encapsulation) or the `ip` interface (to use IP-IP encapsulation) and include the `tunnel` statement:

```
[edit interfaces]
gr-fpc/ pic/ port or ip-fpc/ pic/ port {
    unit logical-unit-number {
        tunnel {
            source address;
            destination address;
            routing-instance {
                destination routing-instance-name;
                ttl number;
            }
            family family {
                address address {
                    destination address;
                }
            }
        }
    }
}
```

You can configure multiple logical units for each GRE or IP-IP interface, and you can configure only one tunnel per unit.

Each tunnel interface must be a point-to-point interface. Point to point is the default interface connection type, so you do not need to include the `point-to-point` statement at the `[edit interfaces interface-name unit logical-unit-number]` hierarchy level.

You must specify the tunnel’s destination and source addresses. The remaining statements are optional.

To set the TTL field that is included in the encapsulating header, include the `ttl` statement. If you explicitly configure a TTL value for the tunnel, you must configure it to be one larger than the number of hops in the tunnel. For example, if the tunnel has seven hops, you must configure a TTL value of 8.

You must configure at least one family on the logical interface. To enable MPLS over GRE tunnel interfaces, you must include the `family mpls` statement in the GRE interface configuration. In addition, you must configure the `protocols` statements to enable RSVP, MPLS, and LSPs over GRE tunnels. Unicast tunnels are bidirectional.

A configured tunnel cannot go through Network Address Translation (NAT) at any point along the way to the destination. For more information, see “Example: Configure Unicast Tunnels” on page 412 and the JUNOS Internet Software Configuration Guide: MPLS Applications.
Configure a Multicast Tunnel

For interfaces that carry IPv4 or IPv6 traffic, you can configure multicast tunnels. To configure a multicast tunnel, include the `multicasts-only` statement at the `[edit interfaces interface-name unit logical-unit-number family inet]` or `[edit interfaces interface-name unit logical-unit-number family inet6]` hierarchy level:

```
multicasts-only;
```

Multicast tunnels filter all unicast packets; if an incoming packet is not destined for a 224/8 or greater prefix, the packet is dropped and a counter is incremented.

You can configure this property on GRE, IP-IP, PIM, and MT tunnels only.

Configure a Tunnel Interface for Routing Table Lookup

To configure tunnel interfaces to facilitate routing table lookups for VPNs, you specify a tunnel’s end point IP addresses and associate them with a routing instance that belongs to a particular routing table. This enables the JUNOS software to search in the appropriate routing table for the route prefix, because the same prefix can appear in multiple routing tables. To configure the destination VPN, include the `routing-instance` statement at the `[edit interfaces gr-fpc/pic/port unit logical-unit-number tunnel]` hierarchy level:

```
[edit interfaces]
gr-fpc/pic/port {
  unit logical-unit-number {
    tunnel {
      source address;
      destination address;
      routing-instance {
        destination routing-instance-name;
      }
    }
  }
}
```

This configuration indicates that the tunnel’s destination address is in routing instance `routing-instance-name`. By default, the tunnel route prefixes are assumed to be in the default Internet routing table `inet.0`.

For more information about VPNs, see the JUNOS Internet Software Configuration Guide: VPNs.
Configure a Tunnel Interface for VRF Table Lookup

To enable egress filtering, you can either configure filtering based on the IP header, or you can configure the virtual loopback tunnel interface on routers equipped with a Tunnel PIC. Table 31 describes each method.

Table 31: Methods for Configuring Egress Filtering

<table>
<thead>
<tr>
<th>Method</th>
<th>Interface Type</th>
<th>Configuration Guidelines</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter traffic based on the IP header</td>
<td>Non-channelized PPP/HDLC core-facing SONET interfaces</td>
<td>Include the vrf-table-label statement at the [edit routing-instances instance-name] hierarchy level. For more information, see the JUNOS Internet Software Configuration Guide: VPNS.</td>
<td>You cannot include the vrf-table-label statement when configuring the 10-port E1 PIC, aggregated interfaces, Fast Ethernet 12-port and 48-port PIC, Gigabit Ethernet 4-port PIC, or Gigabit Ethernet PIC with QPP. There is no restriction on CE router-to-PE router interfaces.</td>
</tr>
<tr>
<td>Configure the virtual loopback tunnel interface on routers equipped with a Tunnel PIC</td>
<td>All interfaces</td>
<td>See the guidelines in this section.</td>
<td>Router must be equipped with a Tunnel PIC. There is no restriction on the type of core-facing interface used or CE router-to-PE router interface used. If you configure a virtual loopback tunnel interface and the vrf-table-label statement at the same time, the the vrf-table-label statement takes precedence over the virtual loopback tunnel interface.</td>
</tr>
</tbody>
</table>

You can configure a virtual loopback tunnel interface to facilitate VPN routing and forwarding instance (VRF) table lookup based on MPLS labels. You might want to enable this functionality so you can do either of the following:

- Forward traffic on a PE-router-to-CE-device interface, in a shared medium, where the CE device is a Layer 2 switch without IP capabilities (for example, a metro Ethernet switch).

  The first lookup is done based on the VPN label to determine which VRF table to refer to, and the second lookup is done on the IP header to determine how to forward packets to the correct end hosts on the shared medium.

- Perform egress filtering at the egress PE router.

  The first lookup on the VPN label is done to determine which VRF table to refer to, and the second lookup is done on the IP header to determine how to filter and forward packets. You can enable this functionality by configuring output filters on the VRF interfaces.

To configure a virtual loopback tunnel interface to facilitate VRF table lookup based on MPLS labels, you specify a virtual loopback tunnel interface name and associate it with a routing instance that belongs to a particular routing table. The packet loops back through the virtual loopback tunnel interface for route lookup.
To specify a virtual loopback tunnel interface name, you configure the virtual loopback tunnel interface and include the family inet and family mpls statements:

```
[edit interfaces]
vt-fpc/pic/port {
  unit 0 {
    family inet;
    family mpls;
  }
  unit 1 {
    family inet;
  }
}
```

To associate the virtual loopback tunnel interface with a routing instance, include the virtual loopback tunnel interface name at the [edit routing-instances] hierarchy level:

```
[edit routing-instances] {
  interface vt-fpc/pic/port;
}
```

For the virtual loopback tunnel interface, none of the statements at the [edit interfaces interface-name unit logical-unit-number tunnel] hierarchy level are valid.

### Configure PIM Tunnels

PIM tunnels are enabled automatically on routers that have a tunnel PIC and on which you enable PIM sparse mode. You do not need to configure the tunnel interface.

PIM tunnels are unidirectional.

In PIM sparse mode, the first-hop router encapsulates packets destined for the Rendezvous Point (RP) router. The packets are encapsulated with a unicast header and are forwarded through a unicast tunnel to the RP. The RP then de-encapsulates the packets and transmits them through its multicast tree. To perform the encapsulation and de-encapsulation, the first-hop and RP routers must be equipped with Tunnel PICs.

The JUNOS Internet software creates two interfaces to handle PIM tunnels:

- **pe**—Encapsulates packets destined for the RP. This interface is present on the first-hop router.
- **pd**—De-encapsulates packets at the RP. This interface is present on the RP.
Configure an IPv6-over-IPv4 Tunnel

If you have a Tunnel PIC installed in your router, you can configure IPv6-over-IPv4 tunnels. To do this, you configure a unicast tunnel across an existing IPv4 network infrastructure. IPv6 packets are encapsulated in IPv4 headers and sent across the IPv4 infrastructure through the configured tunnel. You manually configure configured tunnels on each end point.

IPv6-over-IPv4 tunnels are defined in RFC 2893, Transition Mechanisms for IPv6 Hosts and Routers. For information about configuring a unicast tunnel, see “Configure a Unicast Tunnel” on page 408. For an IPv6-over-IPv4 tunnel configuration example, see “Example: Configure an IPv6-over-IPv4 Tunnel” on page 415.

Example: Configure Unicast Tunnels

Configure two unnumbered IP-IP tunnels:

```
[edit]
interfaces
ip-0/3/0 {
    unit 0 {
        tunnel {
            source 192.168.4.18;
            destination 192.168.4.253;
        }
        family inet;
        family iso;
    }
    unit 1 {
        tunnel {
            source 192.168.4.18;
            destination 192.168.4.254;
        }
        family inet;
        family iso;
    }
}
```
To configure a numbered tunnel interface, include an address under family inet:

```
[edit]
interfaces
  ip-0/3/0 {
    unit 0 {
      tunnel {
        source 192.168.4.18;
        destination 192.168.4.253;
      }
      family inet {
        address 5.5.5.1/30;
      }
      family iso;
    }
    unit 1 {
      tunnel {
        source 192.168.4.18;
        destination 192.168.4.254;
      }
      family inet {
        address 6.6.6.100/30;
      }
      family iso;
    }
  }
```

To configure MPLS over GRE tunnels, include the family mpls statement:

```
interfaces {
  gr-1/2/0 {
    unit 0 {
      tunnel {
        source 192.168.1.1;
        destination 192.168.1.2;
      }
      family inet {
        address 5.1.1.1/30;
      }
      family iso;
      family mpls;
    }
  }
```

Example: Configure a Virtual Loopback Tunnel Interface for VRF Table Lookup

Configure a virtual loopback tunnel interface for VRF table lookup:

```console
[edit routing-instances]
routing-instance-1 {
    instance-type vrf;
    interface vt-1/0/0.0;
    interface so-0/2/2.0;
    route-distinguisher 2:3;
    vrf-import VPN-A-import;
    vrf-export VPN-A-export;
    routing-options {
        static {
            route 10.0.0.0/8 next-hop so-0/2/2.0;
        }
    }
}

routing-instance-2 {
    instance-type vrf;
    interface vt-1/0/0.1;
    interface so-0/3/2.0;
    route-distinguisher 4:5;
    vrf-import VPN-B-import;
    vrf-export VPN-B-export;
    routing-options {
        static {
            route 10.0.0.0/8 next-hop so-0/3/2.0;
        }
    }
}
```

[edit interfaces]
`vt-1/0/0`:
```console
unit 0 {
    family inet;
    family mpls;
}
unit 1 {
    family inet;
}
```
Example: Configure an IPv6-over-IPv4 Tunnel

Configure a tunnel on both sides of the connection.

On Router A
```
[edit]
interfaces {
    gr-1/0/0 {
        unit 0 {
            tunnel {
                source 10.19.2.1;
                destination 10.19.3.1;
            }
            family inet6 {
                address 7019::1/126;
            }
        }
    }
}
```

On Router B
```
[edit]
interfaces {
    gr-1/0/0 {
        unit 0 {
            tunnel {
                source 10.19.3.1;
                destination 10.19.2.1;
            }
            family inet6 {
                address 7019::2/126;
            }
        }
    }
}
```
Example: Configure an IPv6-over-IPv4 Tunnel
Chapter 31

Summary of Interface Configuration Statements

The following descriptions explain each of the interface configuration statements. The statements are organized alphabetically.

802.3ad

Syntax  
802.3ad aex;

Hierarchy Level  
[edit interfaces interface-name gigether-options],  
[edit interfaces interface-name fastether-options]

Description  
Specify aggregated Ethernet logical interface number.

Options  
aex—Aggregated Ethernet logical interface number.  
Range: 0 through 15

Usage Guidelines  
See “Configure Ethernet Link Aggregation” on page 266 or “Configure Aggregated Ethernet Interfaces” on page 299.

Required Privilege Level  
interface—To view this statement in the configuration.  
interface-control—To add this statement to the configuration.
accept-data

Syntax  (accept-data | no-accept-data);

Hierarchy Level  [edit interfaces interface-name unit logical-unit-number family inet address address vrrp-group group-number]

Description  When configuring Virtual Router Redundancy Protocol (VRRP) on Fast Ethernet and Gigabit Ethernet interfaces, configure whether an interface accepts packets destined for the virtual IP address:

- accept-data—Allow the interface to accept packets destined for the virtual IP address.
- no-accept-data—Prohibit the interface from accepting packets destined for the virtual IP address.

Default  If the accept-data statement is not configured, and if the master router owns the virtual IP address, the master router responds to ICMP message requests only.

Usage Guidelines  See “Accept Packets Destined for the Virtual IP Address” on page 294.

Required Privilege Level  interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

accept-source-mac

Syntax  accept-source-mac {
  mac-address mac-address {
    policer {
      input policer-name;
      output policer-name;
    }
  }
}

Hierarchy Level  [edit interfaces interface-name unit logical-unit-number]

Description  For Gigabit Ethernet QPP interfaces only, accept traffic from and to the specified remote MAC address.

The accept-source-mac statement is equivalent to the source-address-filter statement, which is valid for aggregated Ethernet, Fast Ethernet, and Gigabit Ethernet interfaces only.

The statements are explained separately.

Usage Guidelines  See “Configure Gigabit Ethernet QPP MAC Address Filtering” on page 270.

Required Privilege Level  interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

See Also  source-filtering on page 543
access-profile

Syntax
access-profile name;

Hierarchy Level
[edit interfaces interface-name ppp-options chap],
[edit interfaces interface-name unit logical-unit-number ppp-options chap]

Description
Mapping between peer names (or “clients”) and the secrets associated with their respective
links. This statement is mandatory.

For ATM 2 interfaces only, you can configure a CHAP access profile on the logical interface
unit if the logical interface is configured with one of the following PPP over ATM
encapsulation types:

- atm-ppp-llc—PPP over ATM adaptation layer 5 (AAL5) logical link control (LLC)
  encapsulation.

- atm-ppp-vc-mux—PPP over ATM adaptation layer 5 (AAL5) multiplex encapsulation.

Options
name—Name of the access profile.

Usage Guidelines
See “Configure PPP Challenge Handshake Authentication Protocol” on page 55.

Required Privilege Level
interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

See Also
JUNOS Internet Software Configuration Guide: Getting Started.

accounting

Syntax
accounting {
  destination-class-usage;
  source-class-usage {
    (input | output | [input output]);
  }
}

Hierarchy Level
[edit interfaces interface-name unit logical-unit-number family (inet)]

Description
Enable IP packet counters on an interface.

The statements are explained separately.

Usage Guidelines
See “Enable Source Class and Destination Class Usage” on page 94.

Required Privilege Level
interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.
accounting-profile

Syntax

accounting-profile name;

Hierarchy Level

[edit interfaces interface-name],
[edit interfaces interface-name unit logical-unit-number]

Description
Enable collection of accounting data for the specified physical or logical interface.

Options
name—Name of the accounting profile.

Usage Guidelines
See “Apply an Accounting Profile to the Physical Interface” on page 61 and “Apply an Accounting Profile to the Logical Interface” on page 73.

Required Privilege Level
interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

acknowledge-retries

Syntax

acknowledge-retries number;

Hierarchy Level

[edit interfaces ls-fpc/ pic/ port:channel mlfr-uni-nni-bundle-options]

Description
For link services interfaces only, configure the number of retransmission attempts to be made for consecutive hello or remove link messages following the expiration of the acknowledgement timer.

Options
number—Number of retransmission attempts to be made following the expiration of the acknowledgement timer.
Range: 1 through 5
Default: 2

Usage Guidelines
See “Configure Link Services Acknowledgment Timers” on page 329.

Required Privilege Level
interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

See Also
action-red-differential-delay on page 421, hello-timer on page 473
acknowledge-timer

Syntax
acknowledge-timer milliseconds;

Hierarchy Level
[edit interfaces ls-fpc/ pic/ port:channel mlfr-uni-nni-bundle-options]

Description
For link services interfaces only, configure the maximum time, in milliseconds, to wait for an
add link acknowledgement, hello acknowledgement, or remove link acknowledgement
message.

Options
milliseconds—Time, in milliseconds, to wait for an add link acknowledgement, hello
acknowledgement, or remove link acknowledgement message.
  Range: 1 through 10 milliseconds
  Default: 4 milliseconds

Usage Guidelines
See “Configure Link Services Acknowledgment Timers” on page 329.

Required Privilege Level
interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

See Also
address on page 422, hello-timer on page 473

action-red-differential-delay

Syntax
action-red-differential-delay (disable-tx | remove-link);

Hierarchy Level
[edit interfaces ls-fpc/ pic/ port:channel mlfr-uni-nni-bundle-options]

Description
For link services interfaces only, configure the action to be taken when the differential delay
exceeds the red limit.

Options
disable-tx—Disable transmission on the bundle link.
remove-link—Remove bundle link from service.
  Default: disable-tx

Usage Guidelines
See “Configure Link Services Differential Delay” on page 330.

Required Privilege Level
interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

See Also
remote on page 530, yellow-differential-delay on page 571
address

Syntax
address address {
    arp ip-address (mac | multicast-mac) mac-address <publish>;
    destination address;
    eui-64;
    broadcast address;
    multipoint-destination destination-address dci dlci-identifier;
    multipoint-destination destination-address {
        epd-threshold cells;
        inverse-arp;
        oam-liveness {
            up-count cells;
            down-count cells;
        }
        oam-period seconds;
        shaping {
            (cbr rate | rtvbr peak rate sustained rate burst length | vbr peak rate sustained rate burst length);
            queue-length number;
        }
        vci vpi-identifier.vci-identifier;
    }
    primary;
    preferred;
    vrrp-group group-number {
        virtual-address [ addresses ];
        priority number;
        (accept-data | no-accept-data);
        advertise-interval seconds;
        authentication-type authentication;
        authentication-key key;
        (preempt | no-preempt);
        track {
            interface interface-name priority-cost cost;
        }
    }
}

Hierarchy Level [edit interfaces interface-name unit logical-unit-number family family]

Description Configure the interface address.

Options address—Address of the interface.

The remaining statements are explained separately.


Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.
advertise-interval

advertise-interval (APS)

Syntax
advertise-interval milliseconds;

Hierarchy Level [edit interfaces interface-name sonet-options aps]

Description Modify the APS interval at which the protect and working routers send packets to their neighbors to advertise that they are operational. A router considers its neighbor to be operational for a period, called the hold time, that is, by default, three times the advertisement interval.

Options milliseconds—Interval between advertisement packets.
Range: 1 through 65,535 milliseconds
Default: 1000 milliseconds

Usage Guidelines See “Configure APS Timers” on page 371.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

See Also hold-time on page 475

advertise-interval (VRRP)

Syntax advertise-interval seconds;

Hierarchy Level [edit interfaces interface-name unit logical-unit-number family inet address address vrrp-group group-number]

Description On Fast Ethernet and Gigabit Ethernet interfaces only, configure the interval between Virtual Router Redundancy Protocol (VRRP) advertisement packets.

All routers in the VRRP group must use the same advertisement interval.

Options seconds—Interval between advertisement packets.
Range: 1 through 255 seconds
Default: 1 second

Usage Guidelines See “Configure the Advertisement Interval for the VRRP Master Router” on page 293.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.
aggregateg

aggregate (Gigabit Ethernet CoS Policer)

Syntax  
aggregate {  
  bandwidth-limit rate;  
  bandwidth-percent percent;  
  burst-size-limit length;  
}

Hierarchy Level  [edit interfaces interface-name gigether-options ethernet-switch-profile ethernet-policer-profile policer cos-policer-name]

Description  Define a policer to apply to non-premium traffic.

Options  
bandwidth-limit rate—Bandwidth limit. You can specify rate in bits per second either as a complete decimal number or as a decimal number followed by the abbreviation k (1000), m (1,000,000), or g (1,000,000,000).  
  Range: 32 Kilobits per second through 32 Gigabits per second

bandwidth-percent percent—Bandwidth limit in percent.  
  Range: 1 through 100 percent

burst-size-limit length—Burst length, in bytes.  
  Range: 1500 through 100,000,000 bytes

Usage Guidelines  See “Configure a Gigabit Ethernet QPP Policer Profile” on page 269.

Required Privilege Level  
interface—To view this statement in the configuration.  
interface-control—To add this statement to the configuration.

See Also  premium on page 523, ieee802.1-priority-map on page 477

aggregate (SONET/SDH)

Syntax  aggregate asx;

Hierarchy Level  [edit interfaces interface-name sonet-options]

Description  Specify aggregated SONET/SDH logical interface number.

Options  asx—Aggregated SONET/SDH logical interface number.  
  Range: 0 through 15

Usage Guidelines  See “Configure Aggregated SONET/SDH Interfaces” on page 380.

Required Privilege Level  
interface—To view this statement in the configuration.  
interface-control—To add this statement to the configuration.
aggregated-ether-options

Syntax
taggregated-ether-options {
(flow-control | no-flow-control);
link-speed speed;
(loopback | no-loopback);
minimum-links number;
source-address-filter {
  mac-address;
}
(source-filtering | no-source-filtering);
}

Hierarchy Level [edit interfaces aex]

Description Configure aggregated Ethernet-specific interface properties.
The statements are explained separately.

Usage Guidelines See “Configure Ethernet Physical Interface Properties” on page 264.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

aggregated-sonet-options

Syntax
taggregated-sonet-options {
  link-speed speed;
  minimum-links number;
}

Hierarchy Level [edit interfaces asx]

Description Configure aggregated SONET-specific interface properties.
The statements are explained separately.

Usage Guidelines See “Configure Aggregated SONET/SDH Interfaces” on page 380.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

allow-any-vci

Syntax allow-any-vci;

Hierarchy Level [edit interfaces interface-name unit 0]

Description Dedicate entire ATM device to ATM cell relay circuit.

Usage Guidelines See “Configure ATM 1 and ATM 2 Interface Encapsulation” on page 146.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.
Syntax

aps {
  advertise-interval milliseconds;
  authentication-key key;
  force;
  hold-time milliseconds;
  lockout;
  neighbor address;
  paired-group group-name;
  protect-circuit group-name;
  request;
  revert-time seconds;
  working-circuit group-name;
}

Hierarchy Level [edit interfaces interface-name sonet-options]

Description Configure Automatic Protection Switching (APS) on the router.

For DS-3 channels on a Channelized OC-12 interface, you configure APS on channel 0 only. If you configure APS on channels 1 through 11, it is ignored.

The statements are explained separately.

Usage Guidelines See “Configure APS” on page 367.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.
arp

Syntax
arp ip-address (mac | multicast-mac) mac-address <publish>;

Hierarchy Level
[edit interfaces interface-name unit logical-unit-number family inet address address ]

Description
For Ethernet, Fast Ethernet, and Gigabit Ethernet interfaces only, configure ARP table entries,
mapping IP addresses to MAC addresses.

Options
ip-address—IP address to map to the MAC address. The IP address specified must be part of
the subnet defined in the enclosing address statement.

mac mac-address—MAC address to map to the IP address. Specify the MAC address as six
hexadecimal bytes in one of the following formats: nnnn.nnnn.nnnn or

multicast-mac—Multicast MAC address to map to the IP address. Specify the multicast MAC
address as six hexadecimal bytes in one of the following formats: nnnn.nnnn.nnnn or

publish—(Optional) Have the router reply to ARP requests for the specified IP address. If you
omit this option, the router uses the entry to reach the destination but does not reply to
ARP requests.

Usage Guidelines
See “Configure Static ARP Table Entries” on page 289.

Required Privilege Level
interface—to view this statement in the configuration.
interface-control—to add this statement to the configuration.

atm-encapsulation

Syntax
atm-encapsulation (direct | PLCP);

Hierarchy
[edit interfaces at-fpc/pic/port e3-options ]
[edit interfaces at-fpc/pic/port t3-options ]

Description
Configure encapsulation for E3/T3 traffic over ATM interfaces.

Default
PLCP is the default value for T3 traffic and for E3 traffic using G.751 framing.

Options
direct—Use direct encapsulation. G.832 framing on E3 interfaces requires direct
encapsulation.

PLCP—Use PLCP encapsulation.

Usage Guidelines
See “Configure E3 and T3 Parameters on ATM Interfaces” on page 153.

Required Privilege Level
interface—to view this statement in the configuration.
interface-control—to add this statement to the configuration.

See Also
encapsulation on page 457
atm-options

Syntax

atm-options {
  cell-bundle-size cells;
  ilmi;
  linear-red-profiles profile-name {
    high-plp-max-threshold percent;
    low-plp-max-threshold percent;
    queue-depth cells high-plp-threshold percent low-plp-threshold percent;
  }
  pic-type (atm1 | atm2);
  promiscuous-mode {
    [vpi vpi-identifier];
  }
  scheduler-maps map-name {
    forwarding-class class-name {
      priority (low | high);
      transmit-weight (cells number | percent number);
      (epd-threshold cells | linear-red-profile profile-name);
    }
    vc-cos-mode (alternate | strict);
  }
  vpi vpi-identifier {
    maximum-vcs maximum-vcs;
    oam-liveness {
      up-count cells;
      down-count cells;
    }
    oam-period (disable | seconds);
    shaping {
      (cbr rate | rtvbr peak rate sustained rate burst length |
       vbr peak rate sustained rate burst length);
      queue-length number;
    }
  }
}

Hierarchy
[edit interfaces interface-name]

Description
Configure ATM-specific physical interface properties.
The statements are explained separately.

Usage Guidelines
See “Configure ATM 1 and ATM 2 Physical Interface Properties” on page 125.

Required Privilege Level
interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

See Also
multipoint-destination on page 502, shaping on page 539, vci on page 565
atm-scheduler-map

Syntax atm-scheduler-map (map-name | default);

Hierarchy Level [edit interfaces interface-name unit logical-unit-number]

Description Associate a scheduler map with a virtual circuit on a logical interface.

Options map-name—Name of scheduler map that you define at the [edit interfaces interface-name atm-options scheduler-maps] hierarchy level.

default—The default scheduler mapping.


Required Privilege Level interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

See Also scheduler-maps on page 534

authentication-key

authentication-key (APS)

Syntax authentication-key key;

Hierarchy Level [edit interfaces interface-name sonet-options aps]

Description Configure the APS authentication key (password).

Options key—Authentication password. It can be 1 through 8 characters long. Configure the same key for both the working and protect routers.

Usage Guidelines See “Configure Basic APS Support” on page 368.

Required Privilege Level interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.
**authentication-key (VRRP)**

Syntax  
authentication-key key;

Hierarchy Level  
[edit interfaces interface-name unit logical-unit-number family inet address address vrrp-group group-number]

Description  
On Fast or Gigabit Ethernet interfaces, configure a Virtual Router Redundancy Protocol (VRRP) authentication key (password). For the key to work, you also must specify a VRRP authentication scheme by including the authentication-type statement in the vrrp-group statement.

All routers in the VRRP group must use the same authentication scheme and password.

Options  
key—Authentication password. For simple authentication, it can be 1 through 8 characters long. For MD-5 authentication, it can be 1 through 16 characters long. If you include spaces, enclose all characters in quotation marks (" ").

Usage Guidelines  
See “Configure VRRP Authentication” on page 292.

Required Privilege Level  
interface—to view this statement in the configuration.  
interface-control—to add this statement to the configuration.

See Also  
authentication-type on page 431
authentication-type

Syntax

```
authentication-type authentication;
```

Hierarchy Level

```
[edit interfaces interface-name unit logical-unit-number family inet address address]
vrp-group group-number]
```

Description

On Fast or Gigabit Ethernet interfaces only, enable Virtual Router Redundancy Protocol (VRRP) authentication and specify the authentication scheme for the VRRP group. If you enable authentication, you must specify a password by including the authentication-key statement in the vrrp-group statement.

All routers in the VRRP group must use the same authentication scheme and password.

Options

```
authentication

- none—Disable authentication.
- simple—Use a simple password. The password is included in the transmitted packet, making this method of authentication relatively insecure.
- md5—Use the MD5 algorithm to create an encoded checksum of the packet. The encoded checksum is included in the transmitted packet. The receiving router uses the authentication key to verify the packet, discarding it if the digest does not match. This algorithm provides a more secure authentication scheme.
```

Default: none (No authentication is performed.)

Usage Guidelines

See “Configure VRRP Authentication” on page 292.

Required Privilege Level

- interface—To view this statement in the configuration.
- interface-control—To add this statement to the configuration.

See Also

authentication-key on page 429
auto-synchronize

Syntax
auto-synchronize {
    duration milliseconds;
    interval seconds;
}

Hierarchy Level [edit interfaces interface-name serial-options control-leads dtr]

Description Use the signal for resynchronization to configure normal data-transmit-ready (DTR) signal handling.

Options duration—Pulse duration of resynchronization, in milliseconds.
    Range: 1 through 1000 milliseconds
    Default: 1000 milliseconds

interval—Offset interval for resynchronization, in seconds.
    Range: 1 through 31 seconds
    Default: 15 seconds

Usage Guidelines See “Configure the Serial Signal Handling” on page 352.

Required Privilege Level
interface—to view this statement in the configuration.
interface-control—to add this statement to the configuration.

backup-destination

Syntax backup-destination destination-address;

Hierarchy Level [edit interfaces interface-name unit logical-unit-number tunnel]

Description For tunnel interfaces, specify the remote address of the backup tunnel.

Options destination-address—Address of the remote side of the connection.

Usage Guidelines See “Configure IPSec Tunnel Redundancy” on page 260.

Required Privilege Level interface—to view this statement in the configuration.
interface-control—to add this statement to the configuration.

See Also destination on page 450
backup-interface

Syntax: backup-interface interface-name;

Hierarchy Level: [edit interfaces interface-name ppp-options]

Description: Configure a backup ES PIC. When the primary ES PIC has a servicing failure, the backup becomes active, inherits all the tunnels and security associations (SAs), and acts as the new next hop for IPsec traffic.

Options: interface-name—Name of ES interface to serve as the backup.


Required Privilege Level: interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

bandwidth

Syntax: bandwidth rate;

Hierarchy Level: [edit interfaces interface-name unit logical-unit-number]

Description: Configure an informational-only bandwidth value for an interface. This statement is valid for all logical interface types, except multilink and aggregated interfaces.

Options: rate—Peak rate, in bps or cps. You can specify a value in bits per second either as a complete decimal number or as a decimal number followed by the abbreviation k (1000), m (1,000,000), or g (1,000,000,000). You can also specify a value in cells per second by entering a decimal number followed by the abbreviation c; values expressed in cells per second are converted to bits per second by means of the formula 1 cps = 384 bps. Range: Not limited.

Usage Guidelines: See “Configure the Interface Bandwidth” on page 74.

Required Privilege Level: interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.
**Syntax**

`bert-algorithm algorithm;`

**Hierarchy Level**

- `[edit interfaces interface-name ds0-options]`
- `[edit interfaces interface-name t1-options]`
- `[edit interfaces interface-name e1-options]`
- `[edit interfaces interface-name e3-options]`
- `[edit interfaces interface-name t3-options]`

**Description**

Configure the pattern to send in the bit stream during a BERT test. Applies to T1, E3, T3, and Multichannel DS-3 interfaces, the channelized interfaces (DS-3, OC-12, STM-1), and also channelized QPP interfaces (E1 and DS-3).

**Options**

- `algorithm`—Pattern to send in the bit stream. There are two categories of test patterns: pseudorandom and repetitive. Both patterns conform to CCITT/ITU O.151, O.152, O.153, and O.161 standards. The algorithm can be one of the following patterns:
  - `all-ones-repeating`—Pattern is all ones.
  - `all-zeros-repeating`—Pattern is all zeros.
  - `alternating-double-ones-zeros`—Pattern is alternating pairs of ones and zeros.
  - `alternating-ones-zeros`—Pattern is alternating ones and zeros.
  - `repeating-1-in-8`—One bit in 8 is set.
    - `pseudo-2e10`—Pattern is $2^{10} - 1$.
    - `pseudo-2e11-o152`—Pattern is $2^{11} - 1$, as defined in the O152 standard.
    - `pseudo-2e15-o151`—Pattern is $2^{15} - 1$, as defined in the O151 standard.
    - `pseudo-2e17`—Pattern is $2^{17} - 1$.
    - `pseudo-2e18`—Pattern is $2^{18} - 1$.
    - `pseudo-2e20-o151`—Pattern is $2^{20} - 1$, as defined in the O151 standard.
    - `pseudo-2e20-o153`—Pattern is $2^{20} - 1$, as defined in the O153 standard.
    - `pseudo-2e21`—Pattern is $2^{21} - 1$.
    - `pseudo-2e22`—Pattern is $2^{22} - 1$.
    - `pseudo-2e23-o151`—Pattern is $2^{23} - 1$, as defined in the O151 standard.
    - `pseudo-2e25`—Pattern is $2^{25} - 1$.
    - `pseudo-2e28`—Pattern is $2^{28} - 1$.
    - `pseudo-2e29`—Pattern is $2^{29} - 1$.
    - `pseudo-2e3`—Pattern is $2^{3} - 1$.
    - `pseudo-2e31`—Pattern is $2^{31} - 1$.
    - `pseudo-2e32`—Pattern is $2^{32} - 1$.
    - `pseudo-2e4`—Pattern is $2^{4} - 1$.
    - `pseudo-2e5`—Pattern is $2^{5} - 1$.
    - `pseudo-2e6`—Pattern is $2^{6} - 1$.
    - `pseudo-2e7`—Pattern is $2^{7} - 1$.
    - `pseudo-2e9-o153`—Pattern is $2^{9} - 1$, as defined in the O153 standard.
  - `repeating-1-in-4`—One bit in four is set to 1; the others are set to 0.
  - `repeating-1-in-8`—One bit in eight is set to 1; the others are set to 0.
  - `repeating-3-in-24`—Three bits in twenty-four are set to 1; the others are set to 0.

Default: `pseudo-2e3`

**Usage Guidelines**


**Required Privilege Level**

- `interface`—To view this statement in the configuration.
- `interface-control`—To add this statement to the configuration.
bert-error-rate

Syntax
bert-error-rate rate;

Hierarchy Level
[edit interfaces interface-name ds0-options],
[edit interfaces interface-name e1-options],
[edit interfaces interface-name e3-options],
[edit interfaces interface-name t1-options],
[edit interfaces interface-name t3-options]

Description
Configure the bit error rate to use in a BERT procedure. Applies to E1, E3, T1, or T3 interfaces, and also to the channelized interfaces (DS-3, OC-3, OC-12, STM-1).

Options
rate—Bit error rate.
  Range: 0 through 7, which corresponds to 10–0 (that is, 1 error per bit) to 10–7 (that is, 1 error per 10 million bits)
  Default: 0

Usage Guidelines

Required Privilege Level
interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

See Also
bert-algorithm on page 434, bert-period on page 435

bert-period

Syntax
bert-period seconds;

Hierarchy Level
[edit interfaces interface-name ds0-options],
[edit interfaces interface-name e1-options],
[edit interfaces interface-name e3-options],
[edit interfaces interface-name t1-options],
[edit interfaces interface-name t3-options]

Description
Configure the duration of a BERT test. Applies to E1, E3, T1, or T3 interfaces, and also to the channelized interfaces (DS-3, OC-12, STM-1).

Options
seconds—Test duration.
  Range: 1 through 240 seconds
  Default: 10 seconds

Usage Guidelines

Required Privilege Level
interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

See Also
bert-algorithm on page 434, bert-error-rate on page 435
**boot-command**

**Syntax**

`boot-command` `filename;`

**Hierarchy Level**

`[edit interfaces m0-f0c/p0c/p0c/port multiservice-options]`

**Description**

For monitoring services interfaces only, the boot image for the monitoring services PIC. It specifies the filename containing the JUNOS software image for the monitoring services PIC relative to the directory path `/usr/share/pfe`.

**Options**

*filename*—Name of the boot image. Enclose the name within quotation marks. By default, the name of the boot image for the monitoring services PIC is `monitor.jbf`.

**Usage Guidelines**

See “Configure Multiservice Physical Interface Properties” on page 65 or “Configure Flow Monitoring” on page 316.

**Required Privilege Level**

*interface*—To view this statement in the configuration.

*interface-control*—To add this statement to the configuration.

**broadcast**

**Syntax**

`broadcast` `address;`

**Hierarchy Level**

`[edit interfaces interface-name unit logical-unit-number family family address address]`

**Description**

Set the broadcast address on the network or subnet. On a subnet you cannot specify a host address of 0, nor can you specify a broadcast address.

**Default**

The default broadcast address has a host portion of all ones.

**Options**

*address*—Broadcast address. The address must have a host portion of either all ones or all zeros. You cannot specify the addresses 0.0.0.0 or 255.255.255.255.

**Usage Guidelines**

See “Configure the Interface Address” on page 81.

**Required Privilege Level**

*interface*—To view this statement in the configuration.

*interface-control*—To add this statement to the configuration.
buildout

buildout (T1 interfaces)

Syntax
buildout (0-132 | 133-265 | 266-398 | 399-531 | 532-655);

Hierarchy Level
[edit interfaces interface-name t1-options]

Description
Set the buildout value, in feet, for a T1 interface.

Default
The default buildout value is 0-132 feet.

Options
0-132
133-265
266-398
399-531
532-655

Usage Guidelines
See “Configure T1 Buildout” on page 389.

Required Privilege Level
interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

buildout (E3 or T3 over ATM interfaces)

Syntax
buildout feet;

Hierarchy Level
[edit interfaces at-fpc/pic/port e3-options],
[edit interfaces at-fpc/pic/port t3-options]

Description
Set the buildout value, in feet, for E3 and T3 traffic over an ATM interface.

Options
distance—The buildout value in feet.
Range: 0 through 450 feet
Default: 10 feet

Usage Guidelines
See “Configure E3 and T3 Parameters on ATM 1 Interfaces” on page 153.

Required Privilege Level
interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.
bundle

Syntax bundle (ml-fpc/pic/port | ls-fpc/pic/port);

Hierarchy Level [edit interfaces interface-name unit logical-unit-number family mlfr-end-to-end],
[edit interfaces interface-name unit logical-unit-number family mlfr-uni-nni]

Description Associate the multilink interface with the logical interface it is joining.

Options ml-fpc/pic/port—Name of the multilink interface you are linking.
ls-fpc/pic/port—Name of the link services interface you are linking.

Usage Guidelines See “Configure Multilink and Link Services Bundles” on page 333.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

byte-encoding

Syntax byte-encoding (nx64 | nx56);

Hierarchy Level [edit interfaces interface-name ds0-options],
[edit interfaces interface-name t1-options]

Description Set the byte encoding on a DS-0 or T1 interface to use 7 bits per byte or 8 bits per byte.

Default The default byte encoding is 8 bits per byte (nx64).

Options nx56—Use 7 bits per byte.
nx64—Use 8 bits per byte.

Usage Guidelines See “Configure T1 Byte Encoding” on page 389.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.
bytes

Syntax

bytes {
  e1-quiet value;
  f1 value;
  f2 value;
  s0 value;
  s1 value;
  z3 value;
  z4 value;
}

Hierarchy Level
[edit interfaces interface-name sonet-options]

Description
Set values in some SONET header bytes.

On SONET OC-48 interfaces that you configure for channelized (multiplexed) mode (by including the no-concatenate statement at the [edit chassis fpc slot-number pic pic-number] hierarchy level), the bytes e1-quiet and bytes f1 options have no effect. The bytes f2, bytes z3, bytes z4, and path-trace options work correctly on channel 0 and work in the transmit direction only on channels 1, 2, and 3.

For DS-3 channels on a Channelized OC-12 interface, the bytes e1-quiet, bytes f1, bytes f2, bytes z3, and bytes z4 options have no effect. The bytes s1 option is supported only for channel 0; it is ignored if configured on channels 1 through 11. The bytes s1 value configured on channel 0 applies to all channels on the interface.

Options

e1-quiet value—Default idle byte sent on the orderwire SONET overhead bytes. The router does not support the orderwire channel, and hence sends this byte continuously.
  Range: 0 through 255
  Default: 0x7F

f1 value, f2 value, z3 value, z4 value—SONET overhead bytes.
  Range: 0 through 255
  Default: 0x00

s0 value—Set the hardware transmit s0 as an incrementing value rather than 0xCC. This value is used for compatibility between old and new ADMs, should only be used in SDH mode, and is ignored in SONET mode.
  Range: 0 through 55

s1 value—Synchronization message SONET overhead byte. This byte is normally controlled as a side effect of the system reference clock configuration and the state of the external clock coming from an interface if the system reference clocks have been configured to use an external reference.
  Range: 0 through 255
  Default: 0xCC

Usage Guidelines
See “Configure SONET/SDH Physical Interface Properties” on page 360.

Required Privilege Level
interface—to view this statement in the configuration.
interface-control—to add this statement to the configuration.

See Also
no-concatenate in JUNOS Internet Software Guide: Getting Started
cbit-parity

Syntax  (cbit-parity | no-cbit-parity);

Hierarchy Level  [edit interfaces interface-name t3-options]

Description  For T3 interfaces only, enable or disable C-bit parity mode, which controls the type of framing that is present on the transmitted T3 signal. When C-bit parity mode is enabled, the C-bit positions are used for the FEBE, FEAC, terminal data link, path parity, and mode indicator bits, as defined in ANSI T1.107a-1989. When C-bit parity mode is disabled, the basic T3 framing mode (M13) is used.

Default  C-bit parity mode is enabled.

Usage Guidelines  See “Configure E3 and T3 Parameters on ATM 1 Interfaces” on page 153 and “Disable T3 C-Bit Parity Mode” on page 397.

Required Privilege Level  interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

---

cbr

Syntax  cbr rate;

Hierarchy Level  [edit interfaces interface-name unit logical-unit-number shaping],
[edit interfaces interface-name unit logical-unit-number address address family family multipoint-destination address shaping],
[edit interfaces interface-name atm-options vpi vpi-identifier shaping]

Description  For ATM encapsulation only, define a constant bit rate bandwidth utilization in the traffic-shaping profile.

Default  Unspecified bit rate (UBR); that is, bandwidth utilization is unlimited.

Options  rate—Peak rate, in bps or cps. You can specify a value in bits per second either as a complete decimal number or as a decimal number followed by the abbreviation k (1000), m (1,000,000), or g (1,000,000,000). You can also specify a value in cells per second by entering a decimal number followed by the abbreviation c; values expressed in cells per second are converted to bits per second using the formula 1 cps = 384 bps. For OC-3 interfaces, the maximum available rate is 100 percent of line-rate, or 135,600,000 bps. For OC-12 interfaces, the maximum available rate is 50 percent of line-rate, or 271,263,396 bps.

Usage Guidelines  See “Define the ATM 1 and ATM 2 Traffic-Shaping Profile” on page 137.

Required Privilege Level  interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

See Also  rtvbr on page 533, shaping on page 539, vbr on page 564
cell-bundle-size

Syntax

cell-bundle-size cells;

Hierarchy Level

[edit interfaces interface-name atm-options],
[edit interfaces interface-name unit logical-unit-number]

Description

For ATM 2 interfaces only using ATM Layer 2 circuit cell-relay transport mode only, you can configure the maximum number of ATM cells per frame.

Options

cells—Maximum number of cells.
  Default: 1 cell
  Range: 1 through 190 cells

Usage Guidelines

See “Configure the ATM 2 Layer 2 Circuit Cell-Relay Cell Maximum” on page 133.

Required Privilege Level

interface—to view this statement in the configuration.
interface-control—to add this statement to the configuration.

chap

Syntax

chap {
  access-profile name;
  local-name name;
  passive;
}

Hierarchy Level

[edit interfaces interface-name ppp-options],
[edit interfaces interface-name unit logical-unit-number ppp-options]

Description

Allows each side of a link to challenge its peer, using a “secret” known only to the authenticator and that peer. The secret is not sent over the link.

By default, PPP CHAP is disabled. If CHAP is not explicitly enabled, the interface makes no CHAP challenges and denies all incoming CHAP challenges.

For ATM 2 interfaces only, you can configure CHAP on the logical interface unit if the logical interface is configured with one of the following PPP over ATM encapsulation types:

- atm-ppp-llc—PPP over ATM adaptation layer 5 (AAL5) logical link control (LLC) encapsulation.
- atm-ppp-vc-mux—PPP over ATM adaptation layer 5 (AAL5) multiplex encapsulation.

The statements are explained separately.

Usage Guidelines

See “Configure PPP Challenge Handshake Authentication Protocol” on page 55.

Required Privilege Level

interface—to view this statement in the configuration.
interface-control—to add this statement to the configuration.

See Also

JUNOS Internet Software Configuration Guide: Getting Started.
clock-rate

Syntax    clock-rate rate;

Hierarchy Level    [edit interfaces interface-name serial-options ]

Description    For EIA-530 and V.35 interfaces, configure the interface speed.

Options
rate—You can specify the one of the following rates:

- 2.048mhz—2.048 megabits per second (MHz)
- 2.341mhz—2.341 MHz
- 2.731mhz—2.731 MHz
- 3.277mhz—3.277 MHz
- 4.096mhz—4.096 MHz
- 5.461mhz—5.461 MHz
- 8.192mhz—8.192 MHz
- 16.384mhz—16.384 MHz

Default: 16.384mhz

Usage Guidelines
See “Configure the Serial Clocking Mode” on page 350.

Required Privilege Level
interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.
**clocking**

Syntax: `clocking (external | internal);`

Hierarchy Level: `[edit interfaces interface-name]`

Description: Clock source for the interface. You specify this statement for interfaces that can use various clock sources.

For DS-3 channels on a Channelized OC-12 interface, DS-1 channels on a Channelized DS-3 interface, and DS-0 channels on a Channelized E1 interface, the `clocking` statement is supported only for channel 0; it is ignored if included in the configuration of channels 1 through 11. The clock source configured for channel 0 applies to all channels on the Channelized OC-12, Channelized DS-3, and Channelized E1 interfaces. The individual DS-3, DS-1, and DS-0 channels use a gapped 45-MHz clock as the transmit clock.

On Channelized STM-1 interfaces, you should configure the clock source at one side of the connection to be internal (the default JUNOS configuration) and configure the other side of the connection to be external.

Options:
- `external`—The clock source is provided by the DCE.
- `internal`—Use the internal stratum 3 clock as the reference clock.

Default: `internal`

Usage Guidelines: See “Configure the Clock Source” on page 59 or page 374 and “Clock Sources on Channelized Interfaces” on page 166.

Required Privilege Level: `interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.`

**clocking-mode**

Syntax: `clocking-mode (dce | dte | loop);`

Hierarchy Level: `[edit interfaces interface-name serial-options]`

Description: For EIA-530 and V.35 interfaces, configure the clock mode.

Options:
- `dce`—DCE timing.
- `dte`—DTE timing.
- `loop`—Loop timing.

Default: `loop`


Required Privilege Level: `interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.`
compatibility-mode

Syntax  compatibility-mode (adtran | digital-link | kentrox | larscom | verilink) <subrate value>;

Hierarchy Level  [edit interfaces interface-name e3-options],
                  [edit interfaces interface-name t3-options]

Description  Configure the E3 or T3 interface to be compatible with the channel service unit (CSU) at the remote end of the line.

Default  If you omit this option, the full E3 or T3 rate is used.

Options  adtran—For T3 QPP interfaces only, configure compatibility with Adtran CSUs.

           digital-link—Configure compatibility with Digital Link CSUs. If you include this option on an E3 interface, you must also disable payload scrambling.

           kentrox—Configure compatibility with Kentrox CSUs. Kentrox subrate is valid for T3 QPP interfaces only.

           larscom—For T3 and T3 QPP interfaces only, configure compatibility with Larscom CSUs.

           verilink—For T3 QPP interfaces only, configure compatibility with Verilink CSUs.

           subrate value—Subrate of the E3 or T3 line.
              Range: For Adtran CSUs, 1 through 588
              For Digital Link CSUs, 301 kbps through 44.2 Mbps
              For Kentrox CSUs, 1 through 69
              For Larscom CSUs, 1 through 14
              For Verilink CSUs, 1 through 28

Usage Guidelines  See “Configure the E3 CSU Compatibility Mode” on page 253 and “Configure the T3 CSU Compatibility Mode” on page 398.

Required Privilege Level  interface—To view this statement in the configuration.
                          interface-control—To add this statement to the configuration.

See Also  payload-scrambler on page 517
connections

Syntax
connections {
    interface-switch connection-name {
        interface interface-name.unit-number;
        interface interface-name.unit-number;
    }
}

Hierarchy Level [edit protocols]

Description Define the connection between two circuits in a circuit cross-connect (CCC) connection.

The statements are explained separately.

Usage Guidelines See "Configure Switching Cross-Connects" on page 100.

Required Privilege Level routing—To view this statement in the configuration.
 routing-control—To add this statement to the configuration.

See Also JUNOS Internet Software Configuration Guide: MPLS Applications.

control-leads

Syntax
control-leads {
    control-signal (assert | de-assert | normal);
    cts (ignore | normal | require);
    dcd (ignore | normal | require);
    dsr (ignore | normal | require);
    dtr signal-handling-option;
    ignore-all;
    indication (ignore | normal | require);
    rts (assert | de-assert | normal);
    tm (ignore | normal | require);
}

Hierarchy Level [edit interfaces interface-name serial-options]

Description Configure the serial interface signal characteristics.

The statements are explained separately.

Usage Guidelines See “Configure the Serial Signal Handling” on page 352.

Required Privilege Level interface—To view this statement in the configuration.
 interface-control—To add this statement to the configuration.
control-polarity

Syntax  control-polarity (positive | negative);

Hierarchy Level  [edit interfaces interface-name serial-options ]

Description  For X.21 interfaces only, configure the control signal polarity.

Options  positive—Positive signal polarity.

          negative—Negative signal polarity.

Default: positive


Required Privilege Level  interface—To view this statement in the configuration.

                        interface-control—To add this statement to the configuration.

control-signal

Syntax  control-signal (assert | de-assert | normal);

Hierarchy Level  [edit interfaces interface-name serial-options control-leads ]

Description  For X.21 interfaces only, configure the to-DCE signal, control signal.

Options  assert—The to-DCE signal must be asserted.

          de-assert—The to-DCE signal must be deasserted.

          normal—Normal RTS signal handling, as defined by ITU-T Recommendation X.21.

Default: normal

Usage Guidelines  See “Configure the Serial Signal Handling” on page 352.

Required Privilege Level  interface—To view this statement in the configuration.

                        interface-control—To add this statement to the configuration.
core-dump

Syntax
(core-dump | no-core-dump);

Hierarchy Level
[edit interfaces mo-fpc/ pic/ port multiservice-options]

Description
For monitoring services interfaces only, a useful tool for isolating the cause of a problem. Core dumping is enabled by default. The directory /var/tmp contains core files. The JUNOS software saves the current core file (0) and the four previous core files, which are numbered 1 through 4 (from newest to oldest):

- core-dump—Enable the core dumping operation.
- no-core-dump—Disable the core dumping operation.

Usage Guidelines
See “Configure Multiservice Physical Interface Properties” on page 65 or “Configure Flow Monitoring” on page 316.

Required Privilege Level
interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

core-dump

ts

core-dump

Syntax
(core-dump | no-core-dump);

Hierarchy Level
[edit interfaces mo-fpc/ pic/ port multiservice-options]

Description
For monitoring services interfaces only, a useful tool for isolating the cause of a problem. Core dumping is enabled by default. The directory /var/tmp contains core files. The JUNOS software saves the current core file (0) and the four previous core files, which are numbered 1 through 4 (from newest to oldest):

- core-dump—Enable the core dumping operation.
- no-core-dump—Disable the core dumping operation.

Usage Guidelines
See “Configure Multiservice Physical Interface Properties” on page 65 or “Configure Flow Monitoring” on page 316.

Required Privilege Level
interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

core-dump

ts

Syntax
cts (ignore | normal | require);

Hierarchy Level
[edit interfaces interface-name serial-options control-leads]

Description
For EIA-530 and V.35 interfaces only, configure the from-DCE signal, clear-to-send (CTS).

Options
ignore—The from-DCE signal is ignored.

normal—Normal CTS signal handling as defined by the TIA/EIA Standard 530.

require—The from-DCE signal must be asserted.

Default: normal

Usage Guidelines
See “Configure the Serial Signal Handling” on page 352.

Required Privilege Level
interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.
cts-polarity

Syntax  
cts-polarity (positive | negative);

Hierarchy Level  
[edit interfaces interface-name serial-options ]

Description  
Configure clear-to-send (CTS) signal polarity.

Options  
positive—Positive signal polarity.

negative—Negative signal polarity.

Default: positive

Usage Guidelines  

Required Privilege Level  
interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

dcd

Syntax  
dcd (ignore | normal | require);

Hierarchy Level  
[edit interfaces interface-name serial-options control-leads ]

Description  
For EIA-530 and V.35 interfaces only, configure the from-DCE signal, data-carrier-detect (DCD).

Options  
ignore—The from-DCE signal is ignored.

normal—Normal DCD signal handling as defined by the TIA/EIA Standard 530.

require—The from-DCE signal must be asserted.

Default: normal

Usage Guidelines  
See “Configure the Serial Signal Handling” on page 352.

Required Privilege Level  
interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.
dcd-polarity

Syntax  
dcd-polarity (positive | negative);

Hierarchy Level  
[edit interfaces interface-name serial-options]

Description  
Configure data-carryer-detect (DCD) signal polarity.

Options  
positive—Positive signal polarity.

negative—Negative signal polarity.

Default: positive

Usage Guidelines  

Required Privilege Level  
interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

dce

Syntax  
dce;

Hierarchy Level  
[edit interfaces interface-name]

Description  
For Frame Relay only, respond to status query messages.

When you configure the router to be a DCE, keepalives are disabled by default.

Default  
The router operates in DTE mode.

Usage Guidelines  
See “Configure the Router as a DCE” on page 309.

Required Privilege Level  
interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

description

Syntax  
description text;

Hierarchy Level  
[edit interfaces interface-name],

[edit interfaces interface-name unit logical-unit-number]

Description  
Provide a textual description of the interface or the logical unit. Any descriptive text you include is displayed in the output of the show interfaces commands, and is also exposed in the ifAlias MIB object. It has no effect on the operation of the interface or the router.

Options  
text—Text to describe the interface. If the text includes spaces, enclose the entire text in quotation marks.

Usage Guidelines  
See “Add an Interface Description to the Configuration” on page 46 and “Add a Logical Unit Description to the Configuration” on page 71.

Required Privilege Level  
interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.
### destination

#### destination (address)

**Syntax**
```
destination destination-address;
```

**Hierarchy Level**
```
[edit interfaces interface-name unit logical-unit-number tunnel]
```

**Description**
For tunnel interfaces, specify the remote address of the tunnel.

**Options**
`destination-address` — Address of the remote side of the connection.

**Usage Guidelines**

**Required Privilege Level**
interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**See Also**
point-to-point on page 518

#### destination (routing instance)

**Syntax**
```
destination routing-instance-name;
```

**Hierarchy Level**
```
[edit interfaces interface-name unit logical-unit-number tunnel routing-instance]
```

**Description**
Specify the destination routing instance that points to the routing table containing the tunnel destination address.

**Default**
The default Internet routing table `inet.0`.

**Usage Guidelines**
See “Configure a Tunnel Interface for Routing Table Lookup” on page 409.

**Required Privilege Level**
interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

#### destination-class-usage

**Syntax**
```
destination-class-usage;
```

**Hierarchy Level**
```
[edit interfaces interface-name unit logical-unit-number family (inet) accounting]
```

**Description**
Enable packet counters on an interface that count packets that arrive from specific customers and are destined for specific prefixes on the provider core router.

**Usage Guidelines**
See “Enable Source Class and Destination Class Usage” on page 94.

**Required Privilege Level**
interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**See Also**
accounting on page 419, source-class-usage on page 543
disable

Syntax disable;

Hierarchy Level [edit interfaces interface-name],
[edit interfaces interface-name unit logical-unit-number]

Description Disable a physical or a logical interface, effectively unconfiguring it.

Usage Guidelines See “Disable a Physical Interface” on page 65 and “Disable a Logical Interface” on page 76.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

dlci

Syntax dlci dlci-identifier;

Hierarchy Level [edit interfaces interface-name unit logical-unit-number]

Description For Frame Relay and Multilink Frame Relay UNI NNI encapsulation only, and for link services and point-to-point interfaces only, configure the data-link connection identifier (DLCI) for a permanent virtual circuit (PVC) or an switched virtual circuit (SVC).

To configure a DLCI for a point-to-multipoint interface, use the multipoint-destination statement to specify the DLCI.

Options dlci-identifier—Data-link connection identifier.
Range: 16 through 1022

Usage Guidelines See “Configure Frame Relay DLCIs” on page 309, “Configure a Point-to-Point Frame Relay Connection” on page 309, “Configure a Link Services Point-to-Point DLCI” on page 322, and “Configure a Link Services Multicast-Capable DLCI” on page 323.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

See Also encapsulation on page 457, multipoint-destination on page 502, multicast-dlci on page 500
drop-timeout

Syntax    drop-timeout milliseconds;

Hierarchy Level    [edit interfaces (ml-fpc/ pic/ port | ls-fpc/ pic/ port) unit logical-unit-number],
                   [edit interfaces ls-fpc/ pic/ port:channel mlfruni-nni-bundle-options]

Description    For multilink and link services interfaces only, configure the drop timeout period, in milliseconds.

Options    milliseconds—Drop timeout period.
            Range: 0 through 2000 milliseconds
            Default: 0 ms (disabled)

Usage Guidelines    See “Configure a Multilink and Link Services Drop Timeout Period” on page 323.

Required Privilege Level    interface—To view this statement in the configuration.
                            interface-control—To add this statement to the configuration.

ds0-options

Syntax    ds0-options {
            bert-algorithm algorithm;
            bert-error-rate rate;
            bert-period seconds;
            byte-encoding (nx56 | nx 64)
            fcs (32 | 16);
            idle-cycle-flag (flags | ones);
            invert-data;
            loopback (local | payload | remote);
            start-end-flag (shared | filler);
        }

Hierarchy Level    [edit interfaces interface-name]

Description    Configure DS-0-specific physical interface properties.

The statements are explained separately.

Usage Guidelines    See “Specify Options at the NxDS-0 QPP Interface Level” on page 177, “Specify Options at the NxDS-0 QPP Interface Level” on page 197, “Specify Options at the NxDS-0 QPP Interface Level” on page 228, and “Configure Channelized DS-3 to DS-0 Interfaces” on page 229.

Required Privilege Level    interface—To view this statement in the configuration.
                            interface-control—To add this statement to the configuration.
**dsr**

Syntax: `dsr (ignore | normal | require);`

Hierarchy Level: `[edit interfaces interface-name serial-options control-leads]`

Description: For EIA-530 and V.35 interfaces only, configure the from-DCE signal, data-set-ready (DSR).

Options:
- **ignore** — The from-DCE signal is ignored.
- **normal** — Normal DSR signal handling as defined by the TIA/EIA Standard 530.
- **require** — The from-DCE signal must be asserted.

Default: `normal`

Usage Guidelines: See “Configure the Serial Signal Handling” on page 352.

Required Privilege Level:
- **interface** — To view this statement in the configuration.
- **interface-control** — To add this statement to the configuration.

---

**dsr-polarity**

Syntax: `dsr-polarity (positive | negative);`

Hierarchy Level: `[edit interfaces interface-name serial-options]`

Description: Configure data-set-ready (DSR) signal polarity.

Options:
- **positive** — Positive signal polarity.
- **negative** — Negative signal polarity.

Default: `positive`


Required Privilege Level:
- **interface** — To view this statement in the configuration.
- **interface-control** — To add this statement to the configuration.
dtr

Syntax:

```
dtr signal-handling-option;
```

Hierarchy Level:
```
[edit interfaces interface-name serial-options control-leads]
```

Description:
For EIA-530 and V.35 interfaces only, configure the to-DCE signal, data-transmit-ready (DTR).

Options:
```
signal-handling-option — Signal handling for the DTR signal. The signal handling can be one of
                        the following:

assert — The to-DCE signal must be asserted.

de-assert — The to-DCE signal must be deasserted

normal — Normal DTR signal handling as defined by the TIA/EIA Standard 530.

auto-synchronize — Normal DTR signal with automatic synchronization. This statement is
                   explained separately on page 432.
```

Default: normal

Usage Guidelines:
See “Configure the Serial Signal Handling” on page 352.

Required Privilege Level:
interface — To view this statement in the configuration.
interface-control — To add this statement to the configuration.

dtr-circuit

Syntax:

```
dtr-circuit (balanced | unbalanced);
```

Hierarchy Level:
```
[edit interfaces interface-name serial-options]
```

Description:
For EIA-530 and V.35 interfaces only, configure data-transmit-ready (DTR) circuit.

Options:
```
balanced — Balanced DTR signal.

unbalanced — Unbalanced DTR signal.
```

Default: balanced

Usage Guidelines:
See “Configure the Serial DTR Circuit” on page 355.

Required Privilege Level:
interface — To view this statement in the configuration.
interface-control — To add this statement to the configuration.
dtr-polarity

Syntax  
dtr-polarity (positive | negative);

Hierarchy Level  
[edit interfaces interface-name serial-options ]

Description  
Configure data-transmit-ready (DTR) signal polarity.

Options  
positive—Positive signal polarity.

negative—Negative signal polarity.

Default: positive

Usage Guidelines  

Required Privilege Level  
interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

e1-options

Syntax  
e1-options {
       bert-algorithm algorithm;
       bert-error-rate rate;
       bert-period seconds;
       fcs (32 | 16);
       framing (g704 | g704-no-crc4 | unframed);
       idle-cycle-flag (flags | ones);
       invert-data;
       loopback (local | remote);
       start-end-flag (shared | filler);
       timeslots time-slot-range;
   }

Hierarchy Level  
[edit interfaces interface-name ]

Description  
Configure E1-specific physical interface properties.

The statements are explained separately.

Usage Guidelines  
See “Configure Channelized E1 Interfaces” on page 173, “Configure Channelized STM-1 Interfaces” on page 205, “Configure E1 Interfaces” on page 243 and “Configure T1 Interfaces” on page 387.

Required Privilege Level  
interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.
e3-options

Syntax

```plaintext
e3-options {
  atm-encapsulation (direct | PLCP);
  bert-algorithm algorithm;
  bert-error-rate rate;
  bert-period seconds;
  buildout feet;
  compatibility-mode (digital-link | kentrox | larscom)<rate value>;
  fcs (32 | 16);
  framing (g751 | g832);
  idle-cycle-flag value;
  loopback (local | remote);
  (payload-scrambler | no-payload-scrambler);
  start-end-flag value;
}
```

Hierarchy Level

```
[edit interfaces interface-name]
```

Description

Configure E3-specific physical interface properties.

For ATM 1 interfaces, you can configure a subset of E3 options statements. The statements are explained separately.

Usage Guidelines

See “Configure E3 Interfaces” on page 251 and “Configure T3 Interfaces” on page 395.

Required Privilege Level

```
interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.
```

See Also

```
atm-options on page 428
```
encapsulation

**encapsulation (logical interface)**

**Syntax**

```
encapsulation (atm-ccc-cell-relay | atm-ccc-vc-mux | atm-tcc-vc-mux | atm-cisco-nlpid | atm-mlppp-llc
  | atm-nlpid | atm-ppp-llc | atm-ppp-vc-mux | atm-tcc-snap | atm-tcc-vc-mux | atm-snap | atm-wc-mux |
  ether-over-atm-llc | ether-vpls-over-atm-llc | frame-relayccc | frame-relaytcc |
  multilink-frame-relayend-to-end | multilink-ppp | vlan-ccc | vlan-vpls);
```

**Hierarchy Level**

```
[edit interfaces interface-name unit logical-unit-number]
```

**Description**

Logical link-layer encapsulation type

**Options**

- `atm-ccc-cell-relay`—Use ATM cell relay encapsulation.
  - `atm-ccc-vc-mux`—Use ATM VC multiplex encapsulation on circuit cross-connect (CCC) circuits. When you use this encapsulation type, you can configure the family `ccc` only.
  - `atm-cisco-nlpid`—Use Cisco ATM NLPID encapsulation. When you use this encapsulation type, you can configure the family `inet` only.
  - `atm-mlpp-llc`—Use Multilink PPP over ATM adaptation layer 5 (AAL5) logical link control (LLC). This encapsulation type is used only on ATM 2 interfaces. For this encapsulation type, your router must be equipped with a Link Services PIC.
  - `atm-nlpid`—Use ATM NLPID encapsulation. When you use this encapsulation type, you can configure the family `inet` only.
  - `atm-ppp-llc`—Use PPP over ATM adaptation layer 5 (AAL5) logical link control (LLC) encapsulation. This encapsulation type is used only on ATM 2 interfaces.
  - `atm-ppp-vc-mux`—Use PPP over ATM adaptation layer 5 (AAL5) multiplex encapsulation. This encapsulation type is used only on ATM 2 interfaces.
  - `atm-snap`—Use ATM SNAP encapsulation.
  - `atm-tcc-snap`—Use ATM SNAP encapsulation on translational cross-connect (TCC) circuits.
  - `atm-tcc-vc-mux`—Use ATM VC multiplex encapsulation on translational cross-connect (TCC) circuits. When you use this encapsulation type, you can configure the family `tcc` only.
  - `atm-vc-mux`—Use ATM VC multiplex encapsulation. When you use this encapsulation type, you can configure the family `inet` only.
  - `ether-over-atm-llc`—For interfaces that carry IPv4 traffic, use Ethernet over ATM LLC encapsulation. When you use this encapsulation type, you cannot configure multipoint interfaces.
  - `ether-vpls-over-atm-llc`—Use Ethernet VPLS over ATM LLC encapsulation. This encapsulation type enables a VPLS instance to support bridging between Ethernet interfaces and ATM interfaces, as described in RFC 2684, Multiprotocol Encapsulation over ATM Adaptation Layer 5. This encapsulation type is used only on ATM 2 interfaces. When you use this encapsulation type, you cannot configure multipoint interfaces.
  - `frame-relayccc`—Use Frame Relay encapsulation on circuit cross-connect (CCC) circuits. When you use this encapsulation type, you can configure the family `ccc` only.
frame-relay-tcc—Use Frame Relay encapsulation on TCC circuits for connecting unlike media. When you use this encapsulation type, you can configure the family tcc only.

multilink-frame-relay-end-to-end—Use Multilink Frame Relay (MLFR) FRF.15 encapsulation. This encapsulation is used only on multilink and link services interfaces and their constituent T1 or E1 interfaces.

multilink-ppp—Use Multilink Point-to-Point Protocol (MLPPP) encapsulation. This encapsulation is used only on multilink and link services interfaces and their constituent T1 or E1 interfaces.

vlan-ccc—Use Ethernet Virtual Local Area Network (VLAN) encapsulation on circuit cross-connect (CCC) circuits. When you use this encapsulation type, you can configure the family ccc only.

vlan-vpls—Use Ethernet Virtual Local Area Network (VLAN) encapsulation on Virtual Private LAN Service (VPLS) circuits.

Usage Guidelines


Required Privilege Level

interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.
encapsulation (physical interface)


Hierarchy Level: [edit interfaces interface-name]

Description: Physical link-layer encapsulation type.

Options:
- atm-ccc-cell-relay—Use ATM cell relay encapsulation.
- atm-pvc—Use ATM PVC encapsulation.
- cisco-hdlc—Use Cisco-compatible HDLC framing.
- cisco-hdlc-ccc—Use Cisco-compatible HDLC framing on circuit cross-connect (CCC) circuits.
- cisco-hdlc-tcc—Use Cisco-compatible HDLC framing on translational cross-connect (TCC) circuits for connecting unlike media.
- ethernet-ccc—Use Ethernet CCC encapsulation on Ethernet interfaces that must accept packets carrying standard Tag Protocol ID (TPID) values.
- ethernet-over-atm—For interfaces that carry IPv4 traffic, use Ethernet over ATM encapsulation. When you use this encapsulation type, you cannot configure multipoint interfaces.
- ethernet-tcc—For interfaces that carry IPv4 traffic, use Ethernet TCC encapsulation on interfaces that must accept packets carrying standard Tag Protocol ID (TPID) values. Ethernet TCC is not currently supported on Fast Ethernet 48-port PICs.
- ethernet-vpls—Use Ethernet Virtual Private LAN Service (VPLS) encapsulation on Ethernet interfaces that have VPLS enabled and that must accept packets carrying standard Tag Protocol ID (TPID) values.
- extended-vlan-ccc—Use extended VLAN encapsulation on CCC circuits with Gigabit Ethernet and four-port Fast Ethernet interfaces that must accept packets carrying 802.1Q values.
- extended-vlan-tcc—For interfaces that carry IPv4 traffic, use extended VLAN encapsulation on TCC circuits with Gigabit Ethernet interfaces on which you want to use 802.1Q tagging. Extended Ethernet TCC is not currently supported on Fast Ethernet 48-port PICs.
- extended-vlan-vpls—Use extended VLAN VPLS encapsulation on Ethernet interfaces that have VLAN 802.1Q tagging and VPLS enabled and that must accept packets carrying TPIDs 0x8100, 0x9100, and 0x9901.
- frame-relay—Use Frame Relay encapsulation.
- frame-relayccc—Use plain Frame Relay encapsulation or Frame Relay encapsulation on circuit cross-connect (CCC) circuits.
- frame-relaytcc—Use Frame Relay encapsulation on TCC circuits to connect unlike media.
- multilink-frame-relayuni-nni—Use Multilink Frame Relay (MLFR) UNI NNI encapsulation. This encapsulation is used only on link services interfaces functioning as FRF.16 bundles and their constituent T1 or E1 interfaces.
**ppp**—Use serial point-to-point (PPP) encapsulation.

**ppp-ccc**—Use serial PPP encapsulation on CCC circuits. When you use this encapsulation type, you can configure the family `ccc` only.

**ppp-tcc**—Use serial PPP encapsulation on TCC circuits for connecting unlike media. When you use this encapsulation type, you can configure the family `tcc` only.

**vlan-ccc**—Use Ethernet Virtual Local Area Network (VLAN) encapsulation on CCC circuits.

**vlan-vpls**—Use VLAN VPLS encapsulation on Ethernet interfaces with VLAN tagging and VPLS enabled. Interfaces with VLAN VPLS encapsulation accept packets carrying standard TPID values only.

**Default**
PPP encapsulation.

**Usage Guidelines**
See “Configure Interface Encapsulation” on page 51, “Configure Switching Cross-Connects” on page 100, “Configure ATM 1 and ATM 2 Interface Encapsulation” on page 146, “Configure VLAN CCC or VPLS Encapsulation” on page 284, and “Configure Extended VLAN CCC or VLAN VPLS Encapsulation” on page 285.

**Required Privilege Level**
interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

---

**encoding**

**Syntax**
```
encoding (nrz | nrzi);
```

**Hierarchy Level**
```
[edit interfaces interface-name serial-options]
```

**Description**
For serial interfaces, set the line encoding format.

**Default**
The default line encoding is non-return to zero (NRZ).

**Options**
- `nrz`—Use NRZ line encoding.
- `nrzi`—Use non-return to zero inverted (NRZI) line encoding.

**Usage Guidelines**
See “Configure Serial Line Encoding” on page 357.

**Required Privilege Level**
interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.
epd-threshold

epd-threshold (forwarding class)

Syntax  (epd-threshold cells | linear-red-profile profile-name);

Hierarchy Level  [edit interfaces interface-name atm-options scheduler-maps map-name forwarding-class
class-name]

Description  For ATM 2 interfaces only, define the early packet discard (EPD) threshold on a virtual circuit
(VC). When a beginning of packet (BOP) cell is received, the VC’s queue depth is checked
against the EPD threshold. If the VC’s queue depth exceeds the EPD threshold, the BOP cell
and all subsequent cells in the packet are discarded.

Default  EPD threshold is unregulated.

Options  cells—Maximum number of cells.

Range: For scheduling parameters associated with forwarding class, 0 through 32,768
cells.


Required Privilege Level  interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

See Also  linear-red-profile on page 487

epd-threshold (unit)

Syntax  epd-threshold cells;

Hierarchy Level  [edit interfaces interface-name unit logical-unit-number],
[edit interfaces interface-name unit logical-unit-number address address family family
multipoint-destination address]

Description  For ATM 2 interfaces only, define the early packet discard (EPD) threshold on a VC. When a
beginning of packet (BOP) cell is received, the VC’s queue depth is checked against the EPD
threshold. If the VC’s queue depth exceeds the EPD threshold, the BOP cell and all
subsequent cells in the packet are discarded.

Default  EPD threshold is unregulated.

Options  cells—Maximum number of cells.

Range: For one-port and two-port OC-12 interfaces, 0 through 425,984 cells.
For two-port OC-3 interfaces, 0 through 212,992 cells.

Usage Guidelines  See “Configure the ATM 2 EPD Threshold” on page 143.

Required Privilege Level  interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.
es-options

Syntax

```plaintext
es-options {
    backup-interface interface-name;
}
```

Hierarchy Level

```
[edit interfaces interface-name]
```

Description

On ES interfaces, configure ES interface-specific interface properties. The backup-interface statement is explained separately.

Usage Guidelines

See “Configure ES PIC Redundancy” on page 259.

Required Privilege Level

interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

ethernet-policer-profile

Syntax

```plaintext
ethernet-policer-profile {
    ieee802.1-priority-map premium [ bits ];
    policer cos-policer-name {
        aggregate {
            bandwidth-limit rate;
            bandwidth-percent percent;
            burst-size-limit length;
        }
        premium {
            bandwidth-limit rate;
            bandwidth-percent percent;
            burst-size-limit length;
        }
    }
}
```

Hierarchy Level

```
[edit interfaces interface-name gigether-options ethernet-switch-profile]
```

Description

For Gigabit Ethernet QPP interfaces only, configure a CoS-based policer. Policing applies to the inner VLAN identifiers, not to the outer tag.

The statements are explained separately.

Usage Guidelines

See “Configure a Gigabit Ethernet QPP Policer Profile” on page 269.

Required Privilege Level

interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.
**ethernet-switch-profile**

**Syntax**
```
ethernet-switch-profile {
  ethernet-policer-profile {
    ieee802.1-prioritymap premium [ bits ];
  }
  policer cos-policer-name {
    aggregate {
      bandwidth-limit rate;
      bandwidth-percent percent;
      burst-size-limit length;
    }
    premium {
      bandwidth-limit rate;
      bandwidth-percent percent;
      burst-size-limit length;
    }
  }
}
```

**Hierarchy Level**
```
[edit interfaces interface-name gigether-options]
```

**Description**
For Gigabit Ethernet QPP interfaces only, configure VLAN tag and MAC address accounting and filtering properties.

The statements are explained separately.

**Default**
If the `ethernet-switch-profile` statement is not configured, the Gigabit Ethernet PIC with QPP behaves like an Gigabit Ethernet PIC.

**Usage Guidelines**
See “Configure a Gigabit Ethernet QPP Policer Profile” on page 269, “Configure Gigabit Ethernet QPP MAC Address Filtering” on page 270, and “Stack and Rewrite Gigabit Ethernet QPP VLAN Tags” on page 273.

**Required Privilege Level**
```
interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.
```

**eui-64**

**Syntax**
```
eui-64;
```

**Hierarchy Level**
```
[edit interfaces interface-name unit number family ipv6 address address]
```

**Description**
For interfaces that carry IPv6 traffic, automatically generate the host number portion of interface addresses.

**Usage Guidelines**
See “Configure the Interface Address” on page 81.

**Required Privilege Level**
```
interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.
```

**See Also**
### facility-override

**Syntax**
```
facility-override facility-name;
```

**Hierarchy Level**
```
[edit interfaces interface-name service-options syslog host host-name]
```

**Description**
Overrides default facility for system log reporting.

**Options**
- `facility-name`—Name of facility that overrides the default assignment.

**Usage Guidelines**

**Required Privilege Level**
- `interface`—To view this statement in the configuration.
- `interface-control`—To add this statement to the configuration.
family

Syntax

family family {
    accounting {
        destination-class-usage;
        source-class-usage {
            (input | output | [input output]);
        }
    }
    bundle (ml-fpc/pic/ port | ls-fpc/ pic/ port);
    filter {
        input filter-name;
        output filter-name;
        group filter-group-number;
    }
    ipsec-sa sa-name;
    keep-address-and-control;
    mtu bytes;
    multicasts-only;
    no-redirects:
    policer {
        arp policer-template-name;
        input policer-template-name;
        output policer-template-name;
    }
    primary;
    proxy inet-address address;
    remote (inet-address address | mac-address address);
    rpf-check <fail-filter filter-name>;
    sampling {
        [ input output ];
    }
    service {
        input {
            [ service-set service-set-name <service-filter filter-name> ];
            post-service-filter filter-name;
        }
        output {
            [ service-set service-set-name <service-filter filter-name> ];
        }
    }
    (translate-discard-eligible | no-translate-discard-eligible);
    (translate-fecn-and-becn | no-translate-fecn-and-becn);
    address address {
        arp ip-address (mac | multicast-mac) mac-address <publish>;
        destination destination-address;
        eui-64;
        broadcast address;
        multipoint-destination destination-address dlci dlci-identifier;
        multipoint-destination destination-address {
            epd-threshold cells;
            inverse-arp;
            oam-liveness {
                up-count cells;
                down-count cells;
            }
            oam-period seconds;
        }
    }
}
shaping {
  (cbr rate | rtvbr peak rate sustained rate burst length | vbr peak rate sustained rate burst length);
  queue-length number;
}
 vci vpi-identifier:vci-identifier;
}
primary;
preferred;
vrp-group group-number {
  virtual-address [ addresses ];
  priority number;
  (accept-data | no-accept-data);
  advertise-interval seconds;
  authentication-type authentication;
  authentication-key key;
  (preempt | no-preempt);
  track {
    interface interface-name priority-cost cost;
  }
}

Hierarchy Level [edit interfaces interface-name unit logical-unit-number]

Description Configure protocol family information for the logical interface.

Options family—Protocol family:
  ■ ccc—Circuit cross-connect protocol suite
  ■ inet—Internet Protocol version 4 suite
  ■ inet6—Internet Protocol version 6 suite
  ■ iso—OSI ISO protocol suite
  ■ mlfr-end-to-end—Multilink Frame Relay FRF.15
  ■ mlfr-uni-nni—Multilink Frame Relay FRF.16
  ■ multilink-ppp—Multilink Point-to-Point Protocol
  ■ mpls—Multiprotocol Label Switching
  ■ tcc—Translational Cross Connect protocol suite
  ■ tnp—Trivial Network Protocol
  ■ vpls—Virtual Private LAN Service

The remaining statements are explained separately.

fastether-options

Syntax

```
fastether-options {
  802.3ad ae;
  (flow-control | no-flow-control);
  ingress-rate-limit rate;
  (loopback | no-loopback);
  source-address-filter {
    mac-address;
  }
  (source-filtering | no-source-filtering);
}
```

Hierarchy Level  [edit interfaces interface-name]

Description  Configure Fast Ethernet-specific interface properties.

The statements are explained separately.

Usage Guidelines  See “Configure Ethernet Physical Interface Properties” on page 264.

Required Privilege Level

interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.
**fcs**

**Syntax**

```plaintext
fcs (32 | 16);
```

**Hierarchy Level**

- [edit interfaces interface-name ds0-options],
- [edit interfaces interface-name e1-options],
- [edit interfaces interface-name e3-options],
- [edit interfaces interface-name sonet-options],
- [edit interfaces interface-name t1-options],
- [edit interfaces interface-name t3-options]

**Description**

For E1/E3, SONET/SDH, and T1/T3 interfaces, configure the frame checksum on the interface. The checksum must be the same on both ends of the interface.

On a Channelized OC-12 interface, the SONET fcs statement is not supported. To configure FCS on each DS-3 channel, you must include the t3-options fcs statement in the configuration for each channel. For SONET, the Channelized OC-12 interface supports DS-3 to STS-1 to OC-12. For SDH, the Channelized OC-12 interface supports nxDS-3 to nxVC3 to AU3 to STM-n.

**Options**

- **16**—Use a 16-bit frame checksum on the interface.
- **32**—Use a 32-bit frame checksum on the interface. Using a 32-bit checksum provides more reliable packet verification, but some older equipment might not support 32-bit checksums.

**Default:** 16

**Usage Guidelines**

See “Configure the E1 Frame Checksum” on page 245, “Configure the E3 Frame Checksum” on page 253, “Configure the SONET Frame Checksum” on page 363, “Configure T1 Frame Checksum” on page 390, and “Configure the T3 Frame Checksum” on page 399.

**Required Privilege Level**

- interface—to view this statement in the configuration.
- interface-control—to add this statement to the configuration.

---

**feac-loop-respond**

**Syntax**

```plaintext
(feac-loop-respond | no-feac-loop-respond);
```

**Hierarchy Level**

[edit interfaces interface-name t3-options]

**Description**

For T3 interfaces only, configure the router so a remote CSU can place the local router into loopback.

If you configure remote or local loopback with the T3 loopback statement, the router does not respond to FEAC requests from the CSU even if you include the feac-loop-respond statement in the configuration. For the router to respond, you must delete the loopback statement from the configuration.

**Default**

The router does not respond to FEAC requests.

**Usage Guidelines**

See “Configure the T3 FEAC Response” on page 399.

**Required Privilege Level**

- interface—to view this statement in the configuration.
- interface-control—to add this statement to the configuration.

**See Also**

loopback on page 492, remote-loopback-respond on page 530
filter

Syntax

filter {
    input filter-name;
    output filter-name;
    group filter-group-number;
}

Hierarchy Level [edit interfaces interface-name unit logical-unit-number family (inet | inet6 | mpls)]

Description Apply a filter to an interface. You can also use filters for encrypted traffic.

Options

- group filter-group-number—Define an interface to be part of a filter group. The default filter group number is 0.
- input filter-name—Name of one filter to evaluate when packets are received on the interface.
- output filter-name—Name of one filter to evaluate when packets are transmitted on the interface.

Usage Guidelines See “Apply a Filter to an Interface” on page 88 and “Configure Encryption Interfaces” on page 257, or “Configure Flow Monitoring” on page 316.

Required Privilege Level

- interface—To view this statement in the configuration.
- interface-control—To add this statement to the configuration.


flow-control

Syntax flow-control;

Hierarchy Level [edit interfaces interface-name aggregated-ether-options],
    [edit interfaces interface-name fastether-options],
    [edit interfaces interface-name gigether-options]

Description For aggregated Ethernet, Fast Ethernet, and Gigabit Ethernet interfaces only, explicitly enable flow control, which regulates the flow of packets from the router to the remote side of the connection. Enabling flow control is useful when the remote device is a Gigabit Ethernet switch.

Default Flow control is the default behavior.

Usage Guidelines See “Configure Flow Control” on page 280.

Required Privilege Level

- interface—To view this statement in the configuration.
- interface-control—To add this statement to the configuration.
force

Syntax
force (protect | working);

Hierarchy Level
[edit interfaces interface-name sonet-options aps]

Description
Perform a forced switch between the protect and working circuits. This statement is honored only if there are no higher-priority reasons to switch. It can be overridden by a signal failure on the protect circuit, thus causing a switch to the working circuit.

Options
protect—Request the circuit to become the protect circuit.
working—Request the circuit to become the working circuit.

Usage Guidelines
See “Configure Switching between the Working and Protect Circuits” on page 370.

Required Privilege Level
interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

See Also
request on page 531

forwarding-class

Syntax
forwarding-class (class-name | assured-forwarding | best-effort | expedited-forwarding | network-control) {
    priority (high | low);
    transmit-weight (cells number | percent number);
    (epd-threshold cells | linear-red-profile profile-name);
}

Hierarchy Level
[edit interfaces at-fpc/ pic/ port atm-options scheduler-maps map-name]

Description
For ATM 2 interfaces only, define forwarding class name and option values.

Options
class-name—Name of forwarding class.

The statements are explained separately.

Usage Guidelines
See “Configure ATM 2 VC Tunnel CoS Components” on page 155.

Required Privilege Level
interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

See Also
forwarding-class on page 470
fragment-threshold

Syntax

```
fragment-threshold bytes;
```

Hierarchy Level

```
[edit interfaces (ml-fpc/pic/port | ls-fpc/pic/port) unit logical-unit-number],
[edit interfaces ls-fpc/pic/port:channel mlfr-uni-nni-bundle-options]
```

Description

For multilink and link services interfaces only, set the fragmentation threshold, in bytes.

Options

```
bytes—Maximum size, in bytes, for multilink packet fragments. Any non-zero value must be a
multiple of 64 bytes.
Range: 128 through 16,320 bytes
Default: 0 bytes (no fragmentation)
```

Usage Guidelines

See “Configure a Multilink and Link Services Fragmentation Threshold” on page 325.

Required Privilege Level

interface—to view this statement in the configuration.
interface-control—to add this statement to the configuration.

framing

Syntax

```
framing (g704 | g704-no-crc4 | g751 | g832 | unframed | sf | esf);
```

Hierarchy Level

```
[edit interfaces interface-name e1-options],
[edit interfaces at-fpc/pic/port e3-options],
[edit interfaces interface-name t1-options]
```

Description

Configure the framing format.

Default

```
esf for T1 interfaces; g704 for E1 interfaces. There is no default value for E3 over ATM interfaces.
```

Options

```
esf—ESF (extended super frame) mode for T1 interfaces.
g704—G.704 framing format for E1 interfaces.
g704-no-crc4—G.704 framing with no CRC4 for E1 interfaces.
g751—G.751 framing format for E3 over ATM interfaces.
g832—G.832 framing format for E3 over ATM interfaces.
sf—SF (super frame) mode for T1 interfaces.
unframed—Unframed mode for E1 interfaces.
```

Usage Guidelines

See “Configure E1 Framing” on page 246, “Configure E3 and T3 Parameters on ATM 1 Interfaces” on page 153, and “Configure T1 Framing” on page 391.

Required Privilege Level

interface—to view this statement in the configuration.
interface-control—to add this statement to the configuration.
gigether-options

Syntax

```plaintext
802.3ad aex;
(flow-control | no-flow-control);
(loopback | no-loopback);
source-address-filter {
    mac-address;
}
(source-filtering | no-source-filtering);
ethernet-switch-profile {
    ethernet-policer-profile {
        ieee802.1-priority-map premium [ bits ];
    }
    policer cos-policer-name {
        aggregate {
            bandwidth-limit rate;
            bandwidth-percent percent;
            burst-size-limit length;
        }
        premium {
            bandwidth-limit rate;
            bandwidth-percent percent;
            burst-size-limit length;
        }
    }
    (mac-learn-enable | no-mac-learn-enable);
    tag-protocol-id [ tpids ];
}
```

Hierarchy Level

```
[edit interfaces interface-name]
```

Description

Configure Gigabit Ethernet-specific interface properties.

The statements are explained separately.

Usage Guidelines

See “Configure Ethernet Physical Interface Properties” on page 264.

Required Privilege Level

- Interface—to view this statement in the configuration.
- Interface-control—to add this statement to the configuration.
gratuitous-arp-reply

Syntax (gratuitous-arp-reply | no-gratuitous-arp-reply);

Hierarchy Level [edit interfaces interface-name]

Description For Ethernet interfaces, enable updating of the ARP cache for replies received in response to gratuitous ARP requests.

Default Updating of the ARP cache is disabled on all Ethernet interfaces.

Options gratuitous-arp-reply—Update the ARP cache.
no-gratuitous-arp-reply—Do not update the ARP cache.

Usage Guidelines See “Configure Gratuitous ARP” on page 281.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

See Also no-gratuitous-arp-request on page 506

hello-timer

Syntax hello-timer milliseconds;

Hierarchy Level [edit interfaces ls-fpc/ pic/ port:channel mlfr-uni-nni-bundle-options]

Description For link services interfaces only, configure the rate at which hello messages are sent. A hello message is transmitted after a period defined in milliseconds has elapsed.

Options milliseconds—The rate at which hello messages are sent.
Range: 1 through 180 milliseconds
Default: 10 milliseconds

Usage Guidelines See “Configure Link Services Acknowledgment Timers” on page 329.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

See Also address on page 422, acknowledge-timer on page 421
high-plp-max-threshold

Syntax
high-plp-max-threshold percent;

Hierarchy Level
[edit edit interfaces interface-name atm-options linear-red-profiles profile-name]

Description
For ATM 2 interfaces only, define the drop profile fill-level for the high packet-loss priority (PLP) CoS VC. When the fill level exceeds the defined percentage, all packets are dropped.

Options
percent—Fill-level percentage when linear RED is applied to cells with PLP.

Usage Guidelines
See “Configure ATM 2 VC Tunnel CoS Components” on page 155.

Required Privilege Level
interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

See Also
low-plp-max-threshold on page 494, low-plp-threshold on page 495, queue-depth on page 527

high-plp-threshold

Syntax
high-plp-threshold percent;

Hierarchy Level
[edit edit interfaces interface-name atm-options linear-red-profiles profile-name]

Description
For ATM 2 interfaces only, define class of service (CoS) VC drop profile fill-level percentage when linear random early discard (RED) is applied to cells with high packet-loss priority (PLP). When the fill level exceeds the defined percentage, packets with high PLP are randomly dropped by RED. This statement is mandatory.

Options
percent—Fill-level percentage when linear RED is applied to cells with PLP.

Usage Guidelines
See “Configure ATM 2 VC Tunnel CoS Components” on page 155.

Required Privilege Level
interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

See Also
high-plp-max-threshold on page 474, low-plp-max-threshold on page 494, low-plp-threshold on page 495, queue-depth on page 527
hold-time

**hold-time (physical interface)**

Syntax: `hold-time up milliseconds down milliseconds;`

Hierarchy Level: `[edit interfaces interface-name]`

Description: Hold-time value to use to damp interface transitions. When an interface goes from up to down, it is not advertised to the rest of the system as being down until it has remained down for the hold-time period. Similarly, an interface is not advertised as being up until it has remained up for the hold-time period.

Default: Interface transitions are not damped.

Options:
- `down milliseconds`: Hold time to use when an interface transitions from up to down. Upon execution, the time value that you specify is rounded up to the nearest whole second; therefore, we recommend that you configure the `down` option to multiples of 1000.
  - Range: 0 through 65,534
  - Default: 0 milliseconds (interface transitions are not damped)
- `up milliseconds`: Hold time to use when an interface transitions from down to up. Upon execution, the time value that you specify is rounded up to the nearest whole second; therefore, we recommend that you configure the `up` option to multiples of 1000.
  - Range: 0 through 65,534
  - Default: 0 milliseconds (interface transitions are not damped)

Usage Guidelines: See “Damp Interface Transitions” on page 64.

Required Privilege Level:
- interface—to view this statement in the configuration.
- interface-control—to add this statement to the configuration.

See Also: advertise-interval on page 423

**hold-time (APS)**

Syntax: `hold-time milliseconds;`

Hierarchy Level: `[edit interfaces interface-name sonet-options aps]`

Description: Hold-time value to use to determine whether a neighbor APS router is operational.

Options:
- `milliseconds`: Hold-time value.
  - Range: 1 through 65,534 milliseconds
  - Default: 3000 milliseconds (3 times the advertisement interval)


Required Privilege Level:
- interface—to view this statement in the configuration.
- interface-control—to add this statement to the configuration.

See Also: advertise-interval on page 423
host

Syntax

```plaintext
host host-name {
    facility-override;
    log-prefix prefix-number
    [ services priority-level ];
}
```

Hierarchy Level

```
[edit interfaces interface-name service-options syslog]
```

Description

Specify hostname for system logging utility.

Options

- **host-name**—Name of system logging utility host machine.
  - The remaining statements are explained separately.

Usage Guidelines

See “Apply Filters and Services to an Interface” on page 114.

Required Privilege Level

- interface—To view this statement in the configuration.
- interface-control—To add this statement to the configuration.

idle-cycle-flag

Syntax

```plaintext
idle-cycle-flag value;
```

Hierarchy Level

```
[edit interfaces interface-name ds0-options],
[edit interfaces interface-name e1-options],
[edit interfaces interface-name e3-options],
[edit interfaces interface-name t1-options],
[edit interfaces interface-name t3-options]
```

Description

Configure the value that the DS-0, E1, E3, T1, or T3 interface transmits during idle cycles.

Options

- **value**—Value to transmit in the idle cycles:
  - flags—Transmit the value 0x7E.
  - ones—Transmit the value 0xFF (all ones).

Default: flags

Usage Guidelines

See “Configure the E1 Idle Cycle Flag” on page 246, “Configure the E3 Idle Cycle Flag” on page 254, “Configure the T1 Idle Cycle Flag” on page 393, and “Configure the T3 Idle Cycle Flag” on page 400.

Required Privilege Level

- interface—To view this statement in the configuration.
- interface-control—To add this statement to the configuration.
ieee802.1-priority-map

Syntax

```
ieee802.1-priority-map premium [ bits ];
```

Hierarchy Level

```
[edit interfaces interface-name gigether-options ethernet-switch-profile ethernet-policer-profile]
```

Description

For Gigabit Ethernet QPP interfaces only, configure premium priority values for IEEE 802.1p bits.

Options

```
bits — Value of the code-point bits, in binary code.
```

Usage Guidelines

See “Configure a Gigabit Ethernet QPP Policer Profile” on page 269.

Required Privilege Level

```
interface — To view this statement in the configuration.
interface-control — To add this statement to the configuration.
```

ignore-all

Syntax

```
ignore-all;
```

Hierarchy Level

```
[edit interfaces interface-name serial-options control-leads]
```

Description

Ignore all control leads. You can include the ignore-all statement in the configuration only if you do not explicitly enable other signal handling options at the control-leads hierarchy level.

Usage Guidelines

See “Configure the Serial Signal Handling” on page 352.

Required Privilege Level

```
interface — To view this statement in the configuration.
interface-control — To add this statement to the configuration.
```

ilmi

Syntax

```
ilmi;
```

Hierarchy Level

```
[edit interfaces interface-name atm-options]
```

Description

Enable the router to communicate with directly attached ATM switches. The router uses the VC 0.16 to communicate with the ATM switch. Once configured, you can display the IP address and port number of an ATM switch using the show interfaces interface-name switch-id command.

Usage Guidelines

See “Configure Communication with Directly Attached ATM 1 and ATM 2 Switches” on page 126.

Required Privilege Level

```
interface — To view this statement in the configuration.
interface-control — To add this statement to the configuration.
```

See Also

show ilmi and show ilmi statistics commands in JUNOS Internet Software Operational Mode Command Reference.
inactivity-timeout

Syntax
inactivity-timeout seconds;

Hierarchy Level
[edit interfaces interface-name service-options]

Description
Configure inactivity timeout period for established flows. Timeout configured in the
application protocol definition overrides this value.

Options
seconds—Timeout period in seconds.
   Default: 60 seconds.

Usage Guidelines
See “Configure Default Timeout Settings” on page 113.

Required Privilege Level
interface—to view this statement in the configuration.
   interface-control—to add this statement to the configuration.

indication

Syntax
indication (ignore | normal | require);

Hierarchy Level
[edit interfaces interface-name serial-options control-leads]

Description
For X.21 interfaces only, configure the from-DCE signal, indication.

Options
ignore—The from-DCE signal is ignored.
   normal—Normal indication signal handling as defined by ITU-T Recommendation X.21.
   require—The from-DCE signal must be asserted.
   Default: normal

Usage Guidelines
See “Configure the Serial Signal Handling” on page 352.

Required Privilege Level
interface—to view this statement in the configuration.
   interface-control—to add this statement to the configuration.

indication-polarity

Syntax
indication-polarity (positive | negative);

Hierarchy Level
[edit interfaces interface-name serial-options]

Description
For X.21 interfaces only, configure the indication signal polarity.

Options
positive—Positive signal polarity.
   negative—Negative signal polarity.
   Default: positive

Usage Guidelines

Required Privilege Level
interface—to view this statement in the configuration.
   interface-control—to add this statement to the configuration.
### ingress-rate-limit

**Syntax**

`ingress-rate-limit rate;`

**Hierarchy Level**

```
[edit interfaces interface-name fastether-options]
```

**Description**

Perform port-based rate limiting on ingress traffic arriving on Fast Ethernet 8-port, 12-port, and 48-port PICs.

**Options**

- **rate**—Traffic rate in Mbps.
  - **Range:** 1 through 100 Mbps.

**Usage Guidelines**

See “Configure the Ingress Rate Limit” on page 282.

**Required Privilege Level**

- **interface**—To view this statement in the configuration.
- **interface-control**—To add this statement to the configuration.

### input

**Syntax**

```
input {
    service-set service-set-name <service-filter filter-name>;
    post-service-filter filter-name;
}
```

**Hierarchy Level**

```
[edit interface interface-name unit logical-unit-number family inet service]
```

**Description**

Define the input service sets and filters to be applied to traffic.

**Options**

The remaining statements are explained separately.

**Usage Guidelines**

See “Apply Filters and Services to an Interface” on page 114.

**Required Privilege Level**

- **interface**—To view this statement in the configuration.
- **interface-control**—To add this statement to the configuration.
input-vlan-map

Syntax

input-vlan-map {
pop;
push;
swap;
vlan-id number;
tag-protocol-id tpid;
}

Hierarchy Level  [edit interfaces interface-name unit logical-unit-number]

Description  For Gigabit Ethernet QPP interfaces only, define the rewrite profile to be applied to incoming frames on this logical interface.

The statements are explained separately.

Usage Guidelines  See “Stack and Rewrite Gigabit Ethernet QPP VLAN Tags” on page 273.

Required Privilege Level  interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

See Also  output-vlan-map on page 512
interface-type

Syntax
interface-type (coc1 | ct1 | ct3 | ds | so | t1 | t3);

Hierarchy Level
[edit interfaces interface-name partition partition-number],
[edit interfaces interface-name partition partition-number oc-slice oc-slice-range],
[edit interfaces interface-name no-partition]

Default
If you omit this statement, the Channelized PIC with QPP is not partitioned, and no data
channels are configured.

Description
For Q Performance Processor (QPP) interfaces only, configure the sublevel interface type.

Options
coc1—Channelized OC-1 interface type. You can specify this interface type at the [edit
interfaces interface-name partition partition-number oc-slice oc-slice-range interface-type
coc12-fpc/ pic/ port] hierarchy level.

t1—Channelized T1 interface type. You can specify this interface type at the [edit interfaces
interface-name partition partition-number interface-type ct3-fpc/ pic/ port<:channel>]
hierarchy level.

t3—Channelized T3 interface type. You can specify this interface type at the [edit interfaces
interface-name partition partition-number oc-slice oc-slice-range interface-type
coc1-fpc/ pic/ port:channel no-partition] hierarchy level.

ds—DS-0 interface type. You can specify this interface type at the [edit interfaces
interface-name partition partition-number interface-type (ce1-fpc/ pic/ port |
ct1-fpc/ pic/ port<:channel>)] hierarchy level.

so—SONET/SDH interface type. You can specify this interface type at the [edit interfaces
interface-name partition partition-number oc-slice oc-slice-range interface-type
coc12-fpc/ pic/ port] hierarchy level.

t1—T1 interface type. You can specify this interface type at the [edit interfaces interface-name
partition partition-number oc-slice oc-slice-range interface-type (coc12-fpc/ pic/ port |
coc1-fpc/ pic/ port)] hierarchy level.

t3—T3 interface type. You can specify this interface type at the [edit interfaces interface-name
partition partition-number oc-slice oc-slice-range interface-type (coc12-fpc/ pic/ port |
coc1-fpc/ pic/ port:channel no-partition)] hierarchy level.

Usage Guidelines
See “Configure Channelized E1 Interfaces” on page 173, “Configure Channelized OC-12
Interfaces” on page 183, and “Configure Channelized T3 Interfaces” on page 221.

Required Privilege Level
interface—to view this statement in the configuration.
interface-control—to add this statement to the configuration.
interfaces

Syntax  interfaces { ... }

Hierarchy Level  [edit]

Description  Configure interfaces on the router.

Default  The management and internal Ethernet interfaces are automatically configured. You must configure all other interfaces.

Usage Guidelines  See "Interfaces Configuration Statements" on page 29.

Required Privilege Level  interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

interface-switch

Syntax  interface-switch connection-name { interface interface-name.unit-number; interface interface-name.unit-number; }

Hierarchy Level  [edit protocols connections]

Description  Configure Layer 2 switching cross-connects. The cross-connect is bidirectional, so packets received on the first interface are transmitted out the second interface, and those received on the second interface are transmitted out the first.

For Layer 2 switching cross-connects to work, you must also configure MPLS.

Options  interface interface-name.unit-number—Interface name. Include the logical portion of the name, which corresponds to the logical unit number.

Usage Guidelines  See “Configure Switching Cross-Connects” on page 100.

Required Privilege Level  routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

See Also  JUNOS Internet Software Configuration Guide: MPLS Applications.

interleave-fragments

Syntax  interleave-fragments;

Hierarchy Level  [edit interfaces ls-fpc/pic/port unit logical-unit-number]

Description  For link services interfaces only, interleave long packets with high-priority packets.

Allows small delay-sensitive packets, such as Voice over IP (VoIP) packets, to interleave with long fragmented packets. This minimizes the latency of delay-sensitive packets.

Usage Guidelines  See “Configure Link Services Delay-Sensitive Packet Interleaving” on page 326.

Required Privilege Level  interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.
inverse-arp

Syntax
inverse-arp;

Hierarchy Level
[edit interfaces interface-name unit logical-unit-number],
[edit interfaces interface-name unit logical-unit-number family inet address address multipoint-destination destination]

Description
For ATM encapsulation, enable responses to received inverse ATM ARP requests. For Frame Relay encapsulation, enable responses to received inverse Frame Relay ARP requests.

Default
Inverse ARP is disabled on all ATM and Frame Relay interfaces.

Usage Guidelines
See “Configure Inverse ATM 1 or ATM 2 ARP” on page 137 or “Configure Inverse Frame Relay ARP” on page 308.

Required Privilege Level
interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

invert-data

Syntax
invert-data;

Hierarchy Level
[edit interfaces interface-name ds0-options],
[edit interfaces interface-name e1-options],
[edit interfaces interface-name t1-options]

Description
Invert the transmission of unused data bits on the DS-0, T1, or E1 interface.

Usage Guidelines
See “Configure E1 Data Inversion” on page 246 and “Configure T1 Data Inversion” on page 390.

Required Privilege Level
interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

ipsec-sa

Syntax
ipsec-sa sa-name;

Hierarchy Level
[edit interfaces es-fpc/pic/port unit logical-unit-number family inet]

Description
Specify the Internet Protocol security architecture (IPSec) security association (SA) name associated with the interface.

Options
sa-name—IPSEC security association name.

Usage Guidelines
See “Configure Encryption Interfaces” on page 257.

Required Privilege Level
interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

See Also
JUNOS Internet Software Configuration Guide: Getting Started
### keep-address-and-control

**Syntax**
```
keep-address-and-control;
```

**Hierarchy Level**
```
[edit interfaces interface-name unit logical-unit-number family ccc]
```

**Description**
For interfaces with encapsulation type PPP CCC, do not remove the address and control bytes before encapsulating the packet into a tunnel.

**Default**
If you do not include this statement, address and control bytes are removed before encapsulating the packet into a tunnel.

**Usage Guidelines**
See “Disable the Removal of Address and Control Bytes” on page 84.

**Required Privilege Level**
- `interface`—To view this statement in the configuration.
- `interface-control`—To add this statement to the configuration.
keepalives

Syntax
keepalives <interval seconds> <down-count number> <up-count number>;

Hierarchy Level
[edit interfaces interface-name],
[edit interfaces interface-name unit logical-unit-number ppp-options chap]

Description
Enable the sending of keepalives on a physical interface configured with PPP, Frame Relay,
or Cisco HDLC encapsulation.

For ATM 2 interfaces only, you can enable keepalives on a logical interface unit if the logical
interface is configured with one of the following PPP over ATM encapsulation types:

- atm-ppp-ilc—PPP over ATM adaptation layer 5 (AAL5) logical link control (LLC)
  encapsulation.
- atm-ppp-vc-mux—PPP over ATM adaptation layer 5 (AAL5) multiplex encapsulation.

Default
Sending of keepalives is enabled by default. The default keepalive interval is 10 seconds for
PPP, Frame Relay, or Cisco HDLC. The default down-count is 3 and the default up-count is 1
for PPP or Cisco HDLC.

Options
down-count number—The number of keepalive packets a destination must fail to receive
before the network takes down a link.
  Range: 1 through 255
  Default: 3

interval seconds—The time in seconds between successive keepalive requests.
  Range: 1 through 32767 seconds
  Default: 10 seconds

up-count number—The number of keepalive packets a destination must receive to change a
link’s status from down to up.
  Range: 1 through 255
  Default: 1

Usage Guidelines
See “Configure Keepalives” on page 58 or page 307.

Required Privilege Level
interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.
line-encoding

Syntax
line-encoding (ami | b8zs);

Hierarchy Level
[edit interfaces interface-name t1-options]

Description
Set the line encoding format on the T1 interface.

Default
The default line encoding is B8ZS.

Options
ami — Use AMI line encoding.

b8zs — Use B8ZS line encoding.

Usage Guidelines
See “Configure T1 Line Encoding” on page 391.

Required Privilege Level
interface — To view this statement in the configuration.
interface-control — To add this statement to the configuration.

line-protocol

Syntax
line-protocol protocol;

Hierarchy Level
[edit interfaces interface-name serial-options]

Description
For serial interfaces only, configure the line protocol.

Options
protocol — You can specify the one of the following line protocols:

  - eia530 — Line protocol EIA-530
  - v.35 — Line protocol V.35
  - x.21 — Line protocol X.21

Usage Guidelines
See “Configure the Serial Line Protocol” on page 347.

Required Privilege Level
interface — To view this statement in the configuration.
interface-control — To add this statement to the configuration.
linear-red-profile

Syntax  (epd-threshold cells | linear-red-profile profile-name);

Hierarchy Level  [edit interfaces interface-name atm-options scheduler-maps map-name forwarding-class class-name]

Description  For ATM 2 interfaces only, once you define a linear RED profile, you can include it in a scheduler map that is used to map a specified forwarding class to a scheduler configuration.

Options  profile-name—Name of the linear RED profile.

The linear-red-profile statement is explained separately.


Required Privilege Level  interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

linear-red-profiles

Syntax  linear-red-profiles profile-name { high-plp-threshold percent; low-plp-threshold percent; queue-depth cells; }

Hierarchy Level  [edit edit interfaces interface-name atm-options]

Description  For ATM 2 interfaces only, define CoS virtual circuit drop profiles for RED. When a packet arrives, RED checks the queue fill level. If the fill level corresponds to a nonzero drop probability, the RED algorithm determines whether to drop the arriving packet.

Options  profile-name—Name of the drop profile.

The statements are explained separately.


Required Privilege Level  interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.
link-mode

**Syntax**

```
link-mode (full-duplex | half-duplex);
```

**Hierarchy Level**

```
[edit interfaces interface-name]
```

**Description**

Set the device's link connection characteristic.

**Default**

The router's management Ethernet interface, fxp0, autonegotiates whether to operate in full-duplex or half-duplex mode. Fast Ethernet interfaces can operate in either full-duplex or half-duplex mode, and all other interfaces operate only in full-duplex mode.

**Options**

- **full-duplex**—Connection is full duplex.
- **half-duplex**—Connection is half duplex.

**Usage Guidelines**

See “Configure the Link Characteristics” on page 281.

**Required Privilege Level**

- interface—To view this statement in the configuration.
- interface-control—To add this statement to the configuration.

link-speed

**Syntax**

```
link-speed speed;
```

**Hierarchy Level**

```
[edit interfaces as x aggregated-sonet-options],
[edit interfaces as x aggregated-ether-options]
```

**Description**

For aggregated SONET/SDH and aggregated Ethernet interfaces only, set the required link speed.

**Options**

- **speed**—For aggregated Ethernet links, you can specify speed in bits per second either as a complete decimal number or as a decimal number followed by the abbreviation k (1000), m (1,000,000), or g (1,000,000,000).
  
  Aggregated SONET/SDH links can have one of the following speed values.
  - **oc3**—Links are OC-3c or STM-1c.
  - **oc12**—Links are OC-12c or STM-4c.
  - **oc48**—Links are OC-48c or STM-16c.
  - **oc192**—Links are OC-192c or STM-64c.

**Usage Guidelines**

See “Configure Aggregated Ethernet Link Speed” on page 267 and “Configure Aggregated SONET Link Speed” on page 382.

**Required Privilege Level**

- interface—To view this statement in the configuration.
- interface-control—To add this statement to the configuration.
Syntax

```
imi {
  lmi-type (ansi | itu);
  n391dte number;
  n392dce seconds;
  n392dte number;
  n393dce number;
  n393dte number;
  t391dte number;
  t392dce seconds;
}
```

Hierarchy Level
[edit interfaces interface-name]

Description
Set Frame Relay keepalive parameters.

Options

- **n391dte**—DTE full status polling interval.
  - Range: 1 through 255
  - Default: 6

- **n392dce**—DCE error threshold, in number of errors.
  - Range: 1 through 10
  - Default: 3

- **n392dte**—DTE error threshold, in number of errors.
  - Range: 1 through 10
  - Default: 3

- **n393dce**—DCE monitored event-count.
  - Range: 1 through 10
  - Default: 4

- **n393dte**—DTE monitored event-count.
  - Range: 1 through 10
  - Default: 4

- **t391dte**—DTE polling timer.
  - Range: 5 through 30 seconds
  - Default: 10 seconds

- **t392dce**—DCE polling timer.
  - Range: 5 through 30 seconds
  - Default: 15 seconds

The remaining statements are explained separately.

Usage Guidelines

Required Privilege Level
- **interface**—To view this statement in the configuration.
- **interface-control**—To add this statement to the configuration.

See Also
imi-type on page 490
**lmi-type**

**Syntax**  
lmi-type (ansi | itu);

**Hierarchy Level**  
[edit interfaces interface-name lmi],  
[edit interfaces ls-fpc/pic/port:channel mlfr-uni-nni-bundle-options]

**Description**  
Set Frame Relay LMI type.

**Options**  
ansi—Use ANSI T1.167 Annex D LMIs.

itu—Use ITU Q933 Annex A LMIs.

**Default:** itu

**Usage Guidelines**  
See “Configure Tunable Keepalives for Frame Relay LMI” on page 307, and “Configure Link Services Keepalive Settings on Frame Relay LMI” on page 331.

**Required Privilege Level**  
interface—To view this statement in the configuration.  
interface-control—To add this statement to the configuration.

---

**local-name**

**Syntax**  
local-name name;

**Hierarchy Level**  
[edit interfaces interface-name ppp-options chap],  
[edit interfaces interface-name unit logical-unit-number ppp-options chap]

**Description**  
Value sent in CHAP challenge and response packets on a per interface basis. If not included in the configuration, the interface sends the router's system hostname in CHAP challenge and response packets.

For ATM 2 interfaces only, you can configure a CHAP local name on the logical interface unit if the logical interface is configured with one of the following PPP over ATM encapsulation types:

- atm-ppp-llc—PPP over ATM adaptation layer 5 (AAL5) logical link control (LLC) encapsulation.
- atm-ppp-vc-mux—PPP over ATM adaptation layer 5 (AAL5) multiplex encapsulation.

**Usage Guidelines**  
See “Configure PPP Challenge Handshake Authentication Protocol” on page 55.

**Required Privilege Level**  
interface—To view this statement in the configuration.  
interface-control—To add this statement to the configuration.

**See Also**  
JUNOS Internet Software Configuration Guide: Getting Started.
lockout

Syntax  lockout;

Hierarchy Level  [edit interfaces interface-name sonet-options aps]

Description  Configure a lockout of protection, forcing the use of the working circuit and locking out the protect circuit regardless of anything else.

Usage Guidelines  See “Configure Switching between the Working and Protect Circuits” on page 370.

Required Privilege Level  interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

log-prefix

Syntax  log-prefix prefix-number;

Hierarchy Level  [edit interfaces interface-name service-options syslog host host-name]

Description  Set system logging prefix value.

Options  prefix-number—System logging prefix value.


Required Privilege Level  interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

long-buildout

Syntax  (long-buildout | no-long-buildout);

Hierarchy Level  [edit interfaces interface-name t3-options]

Description  Configure the T3 line buildout. A T3 interface has two settings for the T3 line buildout: a short setting, which is less than 225 feet (about 68 meters), and a long setting, which is greater than 225 feet.

This statement applies to copper-cable-based T3 interfaces only. You cannot configure a line buildout for a DS-3 channel on a Channelized OC-12 interface, which runs over fiber-optic cable.

Default  A T3 interface uses the short line buildout setting (no-long-buildout) for wires shorter than 225 feet (about 68 meters).

Usage Guidelines  See “Configure the T3 Line Buildout” on page 400.

Required Privilege Level  interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.
loop-timing

Syntax
(loop-timing | no-loop-timing);

Hierarchy Level
[edit interfaces ct3-fpc/ pic/ port t3-options]

Description
For Channelized T3 interfaces only, configure loop timing for all T1 channels under the Channelized T3 interface.

Options
loop-timing—Configure loop timing for all T1 channels under the Channelized T3 interface.
no-loop-timing—Do not configure loop timing for all T1 channels under the Channelized T3 interface.

Default:
no-loop-timing

Usage Guidelines
See “Configure the Channelized T3 Loop Timing” on page 401.

Required Privilege Level
interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

loopback

loopback (Aggregated Ethernet, Fast Ethernet, and Gigabit Ethernet)

Syntax
(loopback | no-loopback);

Hierarchy Level
[edit interfaces interface-name aggregated-ether-options],
[edit interfaces interface-name fastether-options],
[edit interfaces interface-name gigether-options]

Description
Enable or disable loopback mode.

Usage Guidelines
See “Configure Ethernet Loopback Capability” on page 280.

Required Privilege Level
interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.
**loopback (E1/E3, SONET, and T1/T3)**

**Syntax**

```
loopback (local | payload | remote);
```

**Hierarchy Level**

```
[edit interfaces interface-name ds0-options],
[edit interfaces interface-name e1-options],
[edit interfaces interface-name e3-options],
[edit interfaces interface-name sonet-options],
[edit interfaces interface-name t1-options],
[edit interfaces interface-name t3-options]
```

**Description**

Configure a loopback connection. To turn off the loopback capability, remove the `loopback` statement from the configuration.

**Options**

- **local**—Loop packets, including both data and timing information, back on the local router's PIC. NxDS-0 QPP interfaces do not support local loopback.
- **payload**—For Channelized T3, T1, and NxDS-0 QPP interfaces only, loop back data only (without clocking information) on the remote router's PIC. With payload loopback, overhead is recalculated.
- **remote**—Loop packets, including both data and timing information, back on the remote router's interface card.

**Usage Guidelines**


**Required Privilege Level**

- interface—To view this statement in the configuration.
- interface-control—To add this statement to the configuration.

**See Also**

`feac-loop-respond` on page 468
loopback (serial)

Syntax

```
loopback mode;
```

Hierarchy Level

```
[edit interfaces interface-name serial-options ]
```

Description

Configure a loopback connection.

Default

If you do not include this statement, there is no loopback connection.

Options

mode—You can specify the one of the following loopback modes:

- dce-local—For EIA-530 interfaces only, loop packets back on the local DCE.
- dce-remote—For EIA-530 interfaces only, loop packets back on the remote DCE.
- liu—Loop packets back on the line interface unit (LIU).
- local—Loop packets back on the local router's PIC.

Usage Guidelines

See “Configure Serial Loopback Capability” on page 356.

Required Privilege Level

interface—to view this statement in the configuration.
interface-control—to add this statement to the configuration.

low-plp-max-threshold

Syntax

```
low-plp-max-threshold percent;
```

Hierarchy Level

```
[edit edit interfaces interface-name atm-options linear-red-profiles profile-name]
```

Description

For ATM 2 interfaces only, define the drop profile fill-level for the low packet-loss priority (PLP) CoS VC. When the fill level exceeds the defined percentage, all packets are dropped.

Options

percent—Fill-level percentage when linear RED is applied to cells with PLP.

Usage Guidelines

See “Configure ATM 2 VC Tunnel CoS Components” on page 155.

Required Privilege Level

interface—to view this statement in the configuration.
interface-control—to add this statement to the configuration.

See Also

high-plp-max-threshold on page 474, low-plp-threshold on page 495, queue-depth on page 527
**low-plp-threshold**

**Syntax**
low-plp-threshold percent;

**Hierarchy Level**
[edit edit interfaces interface-name atm-options linear-red-profiles profile-name]

**Description**
For ATM 2 interfaces only, define CoS VC drop profile fill-level percentage when linear RED is applied to cells with low packet-loss priority (PLP). When the fill level exceeds the defined percentage, packets with low PLP are randomly dropped by RED. This statement is mandatory.

**Options**
percent—Fill-level percentage when linear RED is applied to cells with low packet-loss priority (PLP).

**Usage Guidelines**
See “Configure ATM 2 VC Tunnel CoS Components” on page 155.

**Required Privilege Level**
interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**See Also**
high-plp-max-threshold on page 474, high-plp-threshold on page 474, low-plp-maxthreshold on page 494, queue-depth on page 527

**mac**

**Syntax**
mac mac-address;

**Hierarchy Level**
[edit interfaces interface-name]

**Description**
Set the MAC address of the interface. You can configure the MAC address on the management Ethernet interface (fxp0) only.

**Options**
mac-address—MAC address. Specify the MAC address as six hexadecimal bytes in one of the following formats: nnnn.nnnn.nnnn or nn:nn:nn:nn:nn:nn. For example, 0011.2233.4455 or 00:11:22:33:44:55.

**Usage Guidelines**
See “Configure the MAC Address on the Management Ethernet Interface” on page 298.

**Required Privilege Level**
interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.
mac-address

Syntax  
mac-address mac-address;

Hierarchy Level  
[edit interfaces interface-name unit logical-unit-number accept source-mac]

Description  
For Gigabit Ethernet QPP interfaces only, specify a remote MAC address, on which to count incoming and outgoing packets.

Options  
mac-address — MAC address. Specify the MAC address as six hexadecimal bytes in one of the following formats: nnnn.nnnn.nnnn or nn:nn:nn:nn:nn:nn. For example, 0011.2233.4455 or 00:11:22:33:44:55.

Usage Guidelines  
See “Configure Gigabit Ethernet QPP MAC Address Filtering” on page 270.

Required Privilege Level  
interface—To view this statement in the configuration.  
interface-control—To add this statement to the configuration.

mac-learn-enable

Syntax  
(mac-learn-enable | no-mac-learn-enable);

Hierarchy Level  
[edit interfaces interface-name gigether-options ethernet-switch-profile]

Description  
For Gigabit Ethernet QPP interfaces only, configure whether source and destination MAC addresses are dynamically learned:

- mac-learn-enable—Allow the interface to dynamically learn source and destination MAC addresses.

- no-mac-learn-enable—Prohibit the interface from dynamically learning source and destination MAC addresses.

MAC address learning is based on source addresses. You can start accounting for traffic after there has been traffic sent from the MAC address. Once the MAC address is learned, the frames and bytes transmitted to or received from the MAC address can be tracked.

Usage Guidelines  
See “Configure Gigabit Ethernet QPP MAC Address Filtering” on page 270.

Required Privilege Level  
interface—To view this statement in the configuration.  
interface-control—To add this statement to the configuration.
maximum-vcs

Syntax  maximum-vcs maximum-vcs;

Hierarchy Level  [edit interfaces interface-name atm-options vpi vpi-identifier]

Description  For ATM 1 interfaces, configure the maximum number of virtual circuits (VCs) allowed on a virtual path (VP). When configuring ATM 1 interfaces on the router, you must include this statement.

For a configured virtual path identifier (VPI), valid virtual channel identifier (VCI) numbers are in the range 0 through (maximum-vcs value – 1). VCI numbers 0 through 31 are reserved by the ATM Forum. It is recommended that you use a VCI number higher than 31 when connecting to an ATM switch.

Options  maximum-vcs—Maximum number of VCs on the VP. For ATM E3 and T3 interfaces, you can define a maximum of 4090 VCs per interface. For ATM OC-3 interfaces, you can define a maximum of 8180 VCs per interface. For ATM OC-12 interfaces, you can define a maximum of 16,360 VCs per interface. With promiscuous mode, the range is 0 through 65,535 for all ATM interfaces.

Usage Guidelines  See “Configure ATM 1 and ATM 2 Physical Interface Properties” on page 125.

Required Privilege Level  interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

See Also  multipoint-destination on page 502, promiscuous-mode on page 525, vci on page 565
mlfr-uni-nni-bundle-options

Syntax
mlfr-uni-nni-bundle-options {
  acknowledge-retries number;
  acknowledge-timer milliseconds;
  action-red-differential-delay (disable-tx | remove-link);
  drop-timeout milliseconds;
  fragment-threshold bytes;
  hello-timer milliseconds;
  lmi-type (ansi | itu);
  minimum-links number;
  mrru bytes;
  n391 number;
  n392 number;
  n393 number;
  red-differential-delay milliseconds;
  t391 seconds;
  t392 number;
  yellow-differential-delay milliseconds;
}

Hierarchy Level
[edit interfaces ls-fpc/pic/port:channel]

Description
Configure link services interface management properties.
The statements are explained separately.

Usage Guidelines
See “Configure Link Services Physical Interface Properties” on page 327.

Required Privilege Level
interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

minimum-links

Syntax
minimum-links number;

Hierarchy Level
[edit interfaces ae|ax aggregated-ether-options ],
[edit interfaces as|ax aggregated-sonet-options ],
[edit interfaces (ml-fpc/pic/port | ml-fpc/pic/port) unit logical-unit-number ],
[edit interfaces ls-fpc/pic/port:channel mlfr-uni-nni-bundle-options ]

Description
For aggregated Ethernet, SONET/SDH, multilink, or link services interfaces only, set the minimum number of links that must be up for the bundle to be labeled up.

Options
number—Number of links.
  Range: 1 through 8
  Default: 1

Usage Guidelines

Required Privilege Level
interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.
mode

Syntax mode loose;

Hierarchy Level [edit interfaces interface-name unit logical-unit-number family inet rpf-check],
[edit interfaces interface-name unit logical-unit-number family inet6 rpf-check]

Description Check whether the packet has a source address with a corresponding prefix in the routing table. If a corresponding prefix is not found, unicast RPF loose mode does not accept the packet. Unlike strict mode, loose mode does not check whether the interface expects to receive a packet with a specific source address prefix.

Default If you do not include this statement, unicast RPF is in strict mode.

Usage Guidelines See “Configure Unicast RPF Strict Mode” on page 90 and “Configure Unicast RPF Loose Mode” on page 91.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

mrru

Syntax mrru bytes;

Hierarchy Level [edit interfaces (ml-fpc/pic/port | ls-fpc/pic/port) unit logical-unit-number ],
[edit interfaces ls-fpc/pic/port:channel mlfr-uni-nni-bundle-options ]

Description For multilink or link services interfaces only, set the maximum received reconstructed unit (MRRU). The MRRU is similar to the MTU, but is specific to multilink interfaces.

Options bytes—MRRU size.
  Range: 1500 through 4500 bytes
  Default: 1524 bytes

Usage Guidelines See “Configure Multilink and Link Services MRRU” on page 326.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

See Also mtu on page 500
mtu

Syntax

mtu bytes;

Hierarchy Level

[edit interfaces interface-name],
[edit interfaces interface-name unit logical-unit-number family family]

Description

Maximum transmission unit (MTU) size for the media or protocol. The default MTU size depends on the device type. Not all devices allow you to set an MTU value, and some devices have restrictions on the range of allowable MTU values.

Options

bytes—MTU size.
  Range: 0 through 5012 bytes

Usage Guidelines

See “Configure the Media MTU” on page 47 and “Set the Protocol MTU” on page 83.

Required Privilege Level

interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

multicast-dlci

Syntax

multicast-dlci dlci-identifier;

Hierarchy Level

[edit interfaces interface-name unit logical-unit-number]

Description

For point-to-multipoint Frame Relay and link services interfaces only, enable multicast support on the interface. You can configure multicast support on the interface if the Frame Relay switch performs multicast replication.

Options

dlci-identifier—DLCI identifier, a number from 16 through 1022 that defines the Frame Relay DLCI over which the switch expects to receive multicast packets for replication.

Usage Guidelines

See “Configure a Multicast-Capable Frame Relay Connection” on page 311 and “Configure a Link Services Multicast-Capable DLCI” on page 323.

Required Privilege Level

interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

See Also
dlcion page 451, multipoint-destination on page 502
**multicast-vci**

**Syntax**
multicast-vci vpi-identifier.vci-identifier;

**Hierarchy Level**
[edit interfaces interface-name unit logical-unit-number]

**Description**
For ATM encapsulation only, and for point-to-multipoint ATM logical interfaces only, enable
the support of multicast on the interface. You can configure multicast support on the
interface if the ATM switch performs multicast replication.

**Options**
  - vci-identifier—ATM virtual circuit identifier.
    Range: 0 through 16384
  - vpi-identifier—ATM virtual path identifier.
    Range: 0 through 255
    Default: 0

**Usage Guidelines**
See “Configure a Multicast-Capable ATM 1 or ATM 2 Connection” on page 137.

**Required Privilege Level**
interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**See Also**
multipoint-destination on page 502, vci on page 565

**multicasts-only**

**Syntax**
multicasts-only;

**Hierarchy Level**
[edit interfaces interface-name unit logical-unit-number family inet]

**Description**
Configure the unit and family so that it can transmit and receive multicast traffic only. You
can configure this property on the IP family only.

**Usage Guidelines**
See “Configure Tunnel Interfaces” on page 407.

**Required Privilege Level**
interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**See Also**
tunnel on page 560

**multipoint**

**Syntax**
multipoint;

**Hierarchy Level**
[edit interfaces interface-name unit logical-unit-number]

**Description**
Configure the interface unit as a multipoint connection.

**Default**
If you omit this statement, the interface unit is configured as a point-to-point connection.

**Usage Guidelines**
See “Configure a Multipoint Connection” on page 72.

**Required Privilege Level**
interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**See Also**
point-to-point on page 518
multipoint-destination

Syntax
multipoint-destination destination-address dci dci-identifier;
multipoint-destination destination-address {
  epd-threshold cells;
  inverse-arp;
  oam-liveness {
    up-count cells;
    down-count cells;
  }
  oam-period seconds;
  shaping {
    (cbr rate | rtvbr peak rate sustained rate burst length | vbr peak rate sustained rate burst length);
    queue-length number;
  }
  vci vpi-identifier.vci-identifier;
}

Hierarchy Level [edit interfaces interface-name unit logical-unit-number family family address address ]

Description
For point-to-multipoint Frame Relay or ATM interfaces only, enable the support of multicast on the interface. You can configure multicast support on the interface if the Frame Relay or ATM switch performs multicast replication.

Options
destination-address—Address of the remote side of the point-to-multipoint connection.

dci-identifier—For Frame Relay interfaces, the data-link connection identifier.
  Range: 0 through 0xFFFFFF (24 bits)

vci-identifier—For ATM interfaces, the virtual circuit identifier.
  Range: 0 through 16384

vpi-identifier—For ATM interfaces, the virtual path identifier.
  Range: 0 through 255
  Default: 0

The remaining statements are explained separately.

Usage Guidelines
See “Configure a Point-to-Point ATM 1 or ATM 2 Connection” on page 136, and “Configure a Point-to-Multipoint Frame Relay Connection” on page 310.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

See Also dci on page 451, encapsulation on page 457
multiservice-options

Syntax

multiservice-options {
    boot-command filename;
    (syslog | no-syslog);
    (core-dump | no-core-dump);
}

Hierarchy Level [edit interfaces mo-fpc/pic/port]

Description For monitoring services interfaces only, configure multiservice-specific interface properties. The statements are explained separately.

Usage Guidelines See “Configure Multiservice Physical Interface Properties” on page 65 or “Configure Flow Monitoring” on page 316.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

See Also passive-monitor-mode on page 515

n391

Syntax n391 number;

Hierarchy Level [edit interfaces ls-fpc/pic/port:channel mlfr-uni-nni-bundle-options]

Description For link services interfaces only, set the Frame Relay full status polling interval.

Options number—Number of polling interval.
    Range: 1 through 255
    Default: 6

Usage Guidelines See “Configure Link Services Keepalive Settings on Frame Relay LMI” on page 331.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

See Also n392 on page 504, n393 on page 504, timeslots on page 550, and t392 on page 549
Syntax  n392 number;

Hierarchy Level  [edit interfaces ls-fpc/pic/port:channel mlfr-uni-nni-bundle-options]

Description  For link services interfaces only, set the Frame Relay error threshold, in number of errors.

Options  number—Error threshold.
          Range: 1 through 10
          Default: 3

Usage Guidelines  See “Configure Link Services Keepalive Settings on Frame Relay LMI” on page 331.

Required Privilege Level  interface—To view this statement in the configuration.
                          interface-control—To add this statement to the configuration.

See Also  n391 on page 503, n393 on page 504, timeslots on page 550, t392 on page 549

Syntax  n393 number;

Hierarchy Level  [edit interfaces ls-fpc/pic/port:channel mlfr-uni-nni-bundle-options]

Description  For link services interfaces only, set the Frame Relay monitored event count.

Options  number—Number of event count.
          Range: 1 through 255
          Default: 6

Usage Guidelines  See “Configure Link Services Keepalive Settings on Frame Relay LMI” on page 331.

Required Privilege Level  interface—To view this statement in the configuration.
                          interface-control—To add this statement to the configuration.

See Also  n391 on page 503, n392 on page 504, timeslots on page 550, and t392 on page 549
neighbor

Syntax neighbor address

Hierarchy Level [edit interfaces interface-name sonet-options aps]

Description If you are configuring one router to be the working router and a second to be the protect router, configure the address of the remote interface. You configure this on one or both of the interfaces.

The address you specify for the neighbor must never be routed through the interface on which APS is configured, or instability will result. We strongly recommend that you directly connect the working and protect routers and that you configure the interface address of this shared network as the neighbor address.

Options address—Neighbor’s address.

Usage Guidelines See “Configure Basic APS Support” on page 368.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

no-accept-data

See accept-data on page 418

no-asynchronous-notification

Syntax no-asynchronous-notification;

Hierarchy Level [edit interfaces interface-name unit logical-unit-number family (ccc | tcc)]

Description For PPP- and Cisco HDLC-encapsulated serial interfaces, do not send asynchronous notification upon link failure.

Usage Guidelines See “Disable the Sending of Asynchronous Notification Upon Link Failure” on page 84.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

See Also JUNOS Internet Software Configuration Guide: Policy Framework.

no-cbit-parity

See cbit-parity on page 440

no-core-dump

See core-dump on page 447
no-feac-loop-respond

See feac-loop-respond on page 468

no-flow-control

See flow-control on page 469

no-gratuitous-arp-reply

See gratuitous-arp-reply on page 473

no-gratuitous-arp-request

Syntax no-gratuitous-arp-request;

Hierarchy Level [edit interfaces interface-name]

Description For Ethernet interfaces, do not respond to gratuitous ARP requests.

Default Gratuitous ARP responses are enabled on all Ethernet interfaces.

Usage Guidelines See “Configure Gratuitous ARP” on page 281.

Required Privilege Level interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

See Also gratuitous-arp-reply on page 473

no-keepalives

Syntax no-keepalives;

Hierarchy Level [edit interfaces interface-name],
[edit interfaces interface-name unit logical-unit-number ppp-options chap]

Description Disable the sending of keepalives on a physical interface configured with PPP, Frame Relay, or Cisco HDLC encapsulation. The default keepalive interval is 10 seconds.

For ATM 2 interfaces only, you can disable keepalives on a logical interface unit if the logical interface is configured with one of the following PPP over ATM encapsulation types:

- atm-ppp-llc—PPP over ATM adaptation layer 5 (AAL5) logical link control (LLC) encapsulation.
- atm-ppp-vc-mux—PPP over ATM adaptation layer 5 (AAL5) multiplex encapsulation.


Required Privilege Level interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.
no-loopback

See loopback on page 492

no-long-buildout

See long-buildout on page 491

no-mac-learn-enable

See mac-learn-enable on page 496

no-partition

no-partition (Channelized E1, OC-12, and T3 QPP interfaces)

Syntax  no-partition;

Hierarchy Level  [edit interfaces interface-name]

Description  For Q Performance Processor (QPP) PICs only, configure the OC-12, E1, or DS-3 PIC as an unpartitioned, clear channel.

Default  If you do not include either this statement or the oc-slice statement, the Channelized PIC with QPP is not partitioned, and no data channels are configured.

Usage Guidelines  See “Configure Channelized E1 Interfaces” on page 173, “Configure Channelized OC-12 Interfaces” on page 183, and “Configure Channelized T3 Interfaces” on page 221.

Required Privilege Level  interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

See Also  partition on page 514
**no-partition (Channelized OC-1 QPP interfaces)**

**Syntax**

```
no-partition interface-type (ct3 | t3);
```

**Hierarchy Level**

```
[edit interfaces coc1-fpc/pic/port:channel]
```

**Description**

For the Channelized OC-12 PIC with Q Performance Processor (QPP) only, convert the Channelized OC-1 QPP interface into a Channelized T3 interface or a T3 interface. You perform this configuration task for C-bit parity and M13-mapped configurations.

**Usage Guidelines**

See “Configure Channelized OC-12 Interfaces” on page 183.

**Default**

If you do not include either this statement or the `partition` statement, the Channelized PIC with QPP is not partitioned, and no data channels are configured.

**Options**

- `ct3` — Channelized T3 interface type.
- `t3` — T3 interface type.

**Required Privilege Level**

- `interface` — To view this statement in the configuration.
- `interface-control` — To add this statement to the configuration.

**See Also**

`partition` on page 514

**no-partition (Channelized STM-1 QPP interfaces)**

**Syntax**

```
no-partition interface-type (cau4 | so);
```

**Hierarchy Level**

```
[edit interfaces cstm1-fpc/pic/port]
```

**Description**

For the Channelized STM-1 PIC with Q Performance Processor (QPP) only, convert the Channelized STM-1 QPP interface into a Channelized Administrative Unit 4 (AU-4) interface or a SONET/SDH STM-1 interface.

**Usage Guidelines**

See “Configure Channelized STM-1 QPP Interfaces” on page 205.

**Default**

If you do not include either this statement or the `partition` statement, the Channelized PIC with QPP is not partitioned, and no data channels are configured.

**Options**

- `cau4` — Channelized AU-4 interface type.
- `so` — SONET/SDH STM-1 interface type.

**Required Privilege Level**

- `interface` — To view this statement in the configuration.
- `interface-control` — To add this statement to the configuration.

**See Also**

`partition` on page 514

**no-payload-scrambler**

See `payload-scrambler` on page 517
no-preempt

See preempt on page 522

no-redirects

Syntax no-redirects;

Hierarchy Level [edit interfaces interface-name unit number family family]

Description Do not send protocol redirect messages on the interface.

To disable the sending of protocol redirect messages for the entire router, include the no-redirects statement at the [edit system] hierarchy level.

Default Interfaces send protocol redirect messages.

Usage Guidelines See “Disable the Sending of Redirect Messages on an Interface” on page 84.

Required Privilege Level interface—to view this statement in the configuration.

interface-control—To add this statement to the configuration.

See Also JUNOS Internet Software Configuration Guide: Getting Started.

no-source-filtering

See source-filtering on page 543

no-syslog

See syslog on page 545

no-translate-discard-eligible

See translate-discard-eligible on page 556

no-translate-fecn-and-becn

See translate-fecn-and-becn on page 556

no-z0-increment

See z0-increment on page 571
**oam-liveness**

**Syntax**
```
oam-liveness {
  up-count cells;
  down-count cells;
}
```

**Hierarchy Level**
```
[edit interfaces interface-name unit logical-unit-number],
[edit interfaces interface-name unit logical-unit-number family family address address multipoint-destination address],
[edit interfaces interface-name atm-options vpi vpi-identifier]
```

**Description**
For ATM encapsulation only, configure OAM F5 loopback cell count thresholds.

For ATM 2 PICs only, configure OAM F4 loopback cell count thresholds at the [edit interfaces
interface-name atm-options vpi vpi-identifier] hierarchy level.

**Options**
- **down-count cells**—Minimum number of consecutive OAM F4 or F5 loopback cells lost before
  a VC is declared down.
  Range: 1 through 255
  Default: 5 cells

- **up-count cells**—Minimum number of consecutive OAM F4 or F5 loopback cells received
  before a VC is declared up.
  Range: 1 through 255
  Default: 5 cells

**Usage Guidelines**
See “Configure ATM 1 and ATM 2 Logical Interface Properties” on page 135 and “Configure the ATM 1 and ATM 2 OAM F5 Loopback Cell Threshold” on page 145.

**Required Privilege Level**
- **interface**—To view this statement in the configuration.
- **interface-control**—To add this statement to the configuration.
oam-period

Syntax: oam-period (disable | seconds);

Hierarchy Level: [edit interfaces interface-name unit logical-unit-number],
[edit interfaces interface-name unit logical-unit-number family family address address multipoint-destination address],
[edit interfaces interface-name atm-options vpi vpi-identifier]

Description: For ATM encapsulation only, configure the OAM F5 loopback cell period.
For ATM 2 PICs only, configure OAM F4 loopback cell period at the [edit interfaces interface-name atm-options vpi vpi-identifier] hierarchy level.

Default: If you omit this statement, OAM F5 loopback cells are not originated, but the interface still responds if it receives OAM F5 loopback cells.

Options: disable—Disable OAM loopback cell transmit feature.
seconds—OAM loopback cell period.
  Range: 1 through 900 seconds

Usage Guidelines: See “Configure ATM 1 and ATM 2 Logical Interface Properties” on page 135 and “Define the ATM 1 and ATM 2 OAM F5 Loopback Cell Period” on page 144.

Required Privilege Level: interface—to view this statement in the configuration.
interface-control—to add this statement to the configuration.

oc-slice

Syntax: oc-slice oc-slice-range interface-type type;

Hierarchy Level: [edit interfaces interface-name partition partition-number]

Description: For Channelized OC-12 Q Performance Processor (QPP) interfaces only, configure the range of SONET/SDH slices.

Default: If you do not include either this statement or the no-partition statement, the Channelized OC-12 PIC with QPP is not partitioned, and no data channels are configured.

Options: oc-slice-range—Range of SONET/SDH slices. OC-3 interfaces must occupy three consecutive OC slices per interface, in the form 1–3, 4–6, 7–9, or 10–12. The T3, T1, and DS-0 interface types each occupy one OC slice per interface.
  Range: For OC-3 interfaces, 1–3, 4–6, 7–9, or 10–12; for T3 interfaces, 1 through 12; for T1 interfaces, 1 through 336; for NxDS-0 interfaces, 1 through 336.

The remaining statement is explained separately.

Usage Guidelines: See “Configure Channelized OC-12 Interfaces” on page 183.

Required Privilege Level: interface—to view this statement in the configuration.
interface-control—to add this statement to the configuration.
open-timeout

Syntax open-timeout seconds;

Hierarchy Level [edit interfaces interface-name service-options]

Description Configure timeout period for TCP session establishment.

Options seconds—Timeout period in seconds.
    Default: 30 seconds.

Usage Guidelines See “Configure Default Timeout Settings” on page 113.

Required Privilege Level interface—To view this statement in the configuration.
    interface-control—To add this statement to the configuration.

output

Syntax output {
    [ service-set service-set-name <service-filter filter-name> ];
}

Hierarchy Level [edit interfaces interface-name unit logical-unit-number family inet service]

Description Define the output service sets and filters to be applied to traffic.

Options The remaining statements are explained separately.

Usage Guidelines See “Apply Filters and Services to an Interface” on page 114.

Required Privilege Level interface—To view this statement in the configuration.
    interface-control—To add this statement to the configuration.

output-vlan-map

Syntax output-vlan-map {
    pop;
    push;
    swap;
    vlan-id number;
    tag-protocol-id tpid;
}

Hierarchy Level [edit interfaces interface-name unit logical-unit-number]

Description For Gigabit Ethernet QPP interfaces only, define the rewrite profile to be applied to outgoing frames on this logical interface.

    The statements are explained separately.

Usage Guidelines See “Stack and Rewrite Gigabit Ethernet QPP VLAN Tags” on page 273.

Required Privilege Level interface—To view this statement in the configuration.
    interface-control—To add this statement to the configuration.

See Also input-vlan-map on page 480
**overflow**

**Syntax**
```
overflow (tag | discard);
```

**Hierarchy Level**
```
[edit interfaces interface-name receive-bucket],
[edit interfaces interface-name transmit-bucket]
```

**Description**
Specify how to handle packets that exceed the threshold for the receive and transmit leaky buckets.

**Options**
- `tag`—(receive-bucket only) Tag, count, and process received packets that exceed the threshold.
- `discard`—Discard received packets that exceed the threshold. No counting is done.

**Usage Guidelines**
See “Configure Receive and Transmit Leaky Bucket Properties” on page 60 or on page 375.

**Required Privilege Level**
- `interface`—To view this statement in the configuration.
- `interface-control`—To add this statement to the configuration.

**paired-group**

**Syntax**
```
paired-group group-name;
```

**Hierarchy Level**
```
[edit interfaces interface-name sonet-options aps]
```

**Description**
Configure load sharing between two working–protect circuit pairs.

**Options**
- `group-name`—Circuit’s group name, as configured with the `protect-circuit` or `working-circuit` statement.

**Usage Guidelines**
See “Configure APS Load Sharing between Circuit Pairs” on page 372.

**Required Privilege Level**
- `interface`—To view this statement in the configuration.
- `interface-control`—To add this statement to the configuration.

**See Also**
- `paired-group` on page 513, `working-circuit` on page 570
**partition**

**Syntax**

```
partition partition-number oc-slice oc-slice-range interface-type type timeslots time-slot-range;
```

**Hierarchy Level**

```
[edit interfaces interface-name]
```

**Description**

For Q Performance Processor (QPP) interfaces only, configure the channelized interface partition. The partition number correlates with the channel number. Partition and, therefore, channel numbering on QPP interfaces begins with :1, not :0.

**Default**

If you omit this statement, the Channelized PIC with QPP is not partitioned, and no data channels are configured.

**Options**

`partition-number`—Sublevel interface partition index.

**Ranges:**

- 1 through 4 for an OC-3 interface on a Channelized OC-12 QPP interface.
- 1 through 12 for a T3 interface on a Channelized OC-12 QPP interface.
- 1 through 4 for a a T3 interface on a Channelized T3 QPP interface.
- 1 through 28 for a T1 QPP interface on a Channelized OC-12 QPP or Channelized T3 QPP interface.
- 1 through 10 for an E1 interface on a Channelized E1 QPP interface.
- 1 through 24 for NxDS0 interfaces on either channelized OC-12 QPP or channelized DS3 QPP interfaces.
- 0 through 31 (with 0 reserved for framing) for NxDS0 interfaces on channelized E1 QPP interfaces.

The remaining statements are explained separately.

**Usage Guidelines**

See “Configure Channelized E1 Interfaces” on page 173, “Configure Channelized OC-12 Interfaces” on page 183, and “Configure Channelized T3 Interfaces” on page 221.

**Required Privilege Level**

`interface`—To view this statement in the configuration.

`interface-control`—To add this statement to the configuration.

**See Also**

`no-partition` on page 507
passive

Syntax    passive;

Hierarchy Level    [edit interfaces interface-name ppp-options chap],
                    [edit interfaces interface-name unit logical-unit-number ppp-options chap]

Description    Do not challenge the peer, but respond if challenged. If not included in the configuration, the
interface always challenges its peer.

For ATM 2 interfaces only, you can configure CHAP on the logical interface unit if the logical
interface is configured with one of the following PPP over ATM encapsulation types:

- atm-ppp-llc—PPP over ATM adaptation layer 5 (AAL5) logical link control (LLC) encapsulation.
- atm-ppp-vc-mux—PPP over ATM adaptation layer 5 (AAL5) multiplex encapsulation.


Required Privilege Level    interface—To view this statement in the configuration.
                            interface-control—To add this statement to the configuration.

See Also    JUNOS Internet Software Configuration Guide: Getting Started.

passive-monitor-mode

Syntax    passive-monitor-mode;

Hierarchy Level    [edit interfaces interface-name unit logical-unit-number]

Description    For SONET interfaces only, monitor packet flows from another router. If you include this
statement in the configuration, the SONET interface does not send keepalives or alarms, and
does not participate actively on the network.


Required Privilege Level    interface—To view this statement in the configuration.
                            interface-control—To add this statement to the configuration.

See Also    multiservice-options on page 503
**path-trace**

Syntax  
```plaintext
path-trace trace-string;
```

Hierarchy Level  
```plaintext
[edit interfaces interface-name sonet-options]
```

Description  
For SONET interfaces only, configure a path trace identifier, which is a text string that identifies the circuit.

On SONET OC-48 interfaces that are configured for channelized (multiplexed) mode (by including the `no-concatenate` statement at the `[edit chassis fpc slot-number pic pic-number]` hierarchy level), the bytes e1-quiet and bytes f1 options have no effect. The bytes f2, bytes z3, bytes z4, and path-trace options work correctly on channel 0 and work in the transmit direction only on channels 1, 2, and 3.

For DS-3 channels on a Channelized OC-12 interface, you can configure a unique path trace for each of the 12 channels. Each path trace can be up to 16 bytes. For channels on a Channelized OC-12 Q Performance Processor (QPP) interface, each path trace can be up to 64 bytes.

Options  
- `trace-string`—Text string that identifies the circuit. If the string contains spaces, enclose it in quotation marks. A common convention is to use the circuit identifier as the path trace identifier. If you do not configure an identifier, the JUNOS software uses the system and interface names.

Usage Guidelines  
See “Configure the SONET Path Trace Identifier” on page 365.

Required Privilege Level  
- `interface`—To view this statement in the configuration.
- `interface-control`—To add this statement to the configuration.

See Also  
sonet-options on page 540
payload-scrambler

Syntax (payload-scrambler | no-payload-scrambler);

Hierarchy Level [edit interfaces interface-name e3-options],
              [edit interfaces interface-name sonet-options],
              [edit interfaces interface-name t3-options]

Description Enable or disable HDLC scrambling on an E3, a SONET, or a T3 interface. This type of
scrambling provides better link stability. Both sides of a connection must either use or not
use scrambling.

Disable payload scrambling on an E3 interface if Digital Link compatibility mode is used.

On a Channelized OC-12 interface, the SONET payload-scrambler statement is ignored. To
configure scrambling on the DS-3 channels on the interface, you can include the t3-options
payload-scrambler statement in the configuration for each DS-3 channel.

Default Payload scrambling is disabled on all E3 and T3 interfaces; it is enabled by default on E3/T3
over ATM interfaces and on SONET/SDH interfaces.

Usage Guidelines See “Configure E3 and T3 Parameters on ATM 1 Interfaces” on page 153, “Configure E3
HDLC Payload Scrambling” on page 255, “Configure SONET HDLC Payload Scrambling” on
page 365, “Configure T3 HDLC Payload Scrambling” on page 403, and “Examples: Configure
T3 Interfaces” on page 404.

Required Privilege Level interface—to view this statement in the configuration.
interface-control—to add this statement to the configuration.

per-unit-scheduler

Syntax per-unit-scheduler;

Hierarchy Level [edit interfaces interface-name]

Description For Channelized OC-12 QPP, Channelized T3 QPP, Channelized E1 QPP, and Gigabit Ethernet
QPP interfaces only, enable association of scheduler map names with logical interfaces.

Usage Guidelines See “Associate a Scheduler with a DLCI or VLAN on a Channelized QPP Interface” on
page 597.

Required Privilege Level interface—to view this statement in the configuration.
interface-control—to add this statement to the configuration.
pic-type

Syntax pic-type atm1 | atm2;

Hierarchy Level [edit interfaces atm-fpc/pic/port atm-options]

Description For ATM interfaces, configure the type of ATM PIC installed in your router.

Options atm1—ATM 1 PIC.

        atm2—ATM 2 PIC

Usage Guidelines See “Configure the ATM 1 and ATM 2 PIC Type” on page 126.

Required Privilege Level interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

point-to-point

Syntax point-to-point;

Hierarchy Level [edit interfaces interface-name unit logical-unit-number]

Description For all interfaces except aggregated Ethernet, Fast Ethernet, and Gigabit Ethernet, configure
the interface unit as a point-to-point connection. This is the default connection type.

Default If you omit this statement, the interface unit is configured as a point-to-point connection.

Usage Guidelines See “Configure a Point-to-Point Connection” on page 72.

Required Privilege Level interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

See Also multipoint on page 501
policer (CoS)

Syntax

policer cos-policer-name {
    aggregate {
        bandwidth-limit rate;
        bandwidth-percent percent;
        burst-size-limit length;
    }
    premium {
        bandwidth-limit rate;
        bandwidth-percent percent;
        burst-size-limit length;
    }
}

Hierarchy Level
[edit interfaces interface-name gigether-options ethernet-switch-profile ethernet-policer-profile]

Description
For Gigabit Ethernet QPP interfaces only, define a CoS policer template to specify the premium bandwidth and burst-size limits, and the aggregate bandwidth and burst-size limits.

Options
cos-policer-name—Name of one policer to specify the premium bandwidth and burst-size limits, and the aggregate bandwidth and burst-size limits.

The remaining statements are explained separately.

Usage Guidelines
See “Configure a Gigabit Ethernet QPP Policer Profile” on page 269.

Required Privilege Level
interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.
**policer (interface)**

**Syntax**

```plaintext
policer {
policer-template-name;

template-name;

template-name;

}
```

**Hierarchy Level**

```
[edit interfaces interface-name unit logical-unit-number family (ccc | inet | tcc)]
```

**Description**

Apply a policer to an interface. You can configure a different policer on each protocol family on an interface. You can configure one Address Resolution Protocol (ARP) policer only for the family inet protocol. You can configure one input policer only and one output policer only for each protocol family.

**Options**

- **arp policer-template-name**—For family inet only, name of one policer to evaluate when ARP packets are received on the interface.
- **input policer-template-name**—Name of one policer to evaluate when packets are received on the interface.
- **output policer-template-name**—Name of one policer to evaluate when packets are transmitted on the interface.

**Usage Guidelines**

See “Apply Policers” on page 87 or “Apply Filters and Services to an Interface” on page 114.

**Required Privilege Level**

- interface—To view this statement in the configuration.
- interface-control—To add this statement to the configuration.

**See Also**


---

**policer (MAC)**

**Syntax**

```plaintext
policer {
	policer-name;

}
```

**Hierarchy Level**

```
[edit interfaces interface-name unit logical-unit-number accept-source-mac mac-address mac-address]
```

**Description**

For Gigabit Ethernet QPP interfaces only, configure MAC policing.

**Options**

- **input policer-name**—Name of one policer to specify the premium bandwidth and aggregate bandwidth.
- **output policer-name**—Name of one policer to specify the premium bandwidth and aggregate bandwidth.

**Usage Guidelines**

See “Configure Gigabit Ethernet QPP MAC Address Filtering” on page 270.

**Required Privilege Level**

- interface—To view this statement in the configuration.
- interface-control—To add this statement to the configuration.
pop

Syntax pop;

Hierarchy Level [edit interfaces interface-name unit logical-unit-number input-vlan-map],
[edit interfaces interface-name unit logical-unit-number output-vlan-map]

Description For Gigabit Ethernet QPP interfaces only, remove a VLAN tag from the top of the VLAN tag stack.

Usage Guidelines See “Stack and Rewrite Gigabit Ethernet QPP VLAN Tags” on page 273.

Required Privilege Level interface—to view this statement in the configuration.
interface-control—to add this statement to the configuration.

See Also push on page 527

post-service-filter

Syntax post-service-filter filter-name;

Hierarchy Level [edit interfaces interface-name unit logical-unit-number family inet service input]

Description Define the filter to be applied to traffic after service processing. The filter is applied only if a service set is configured and selected.

Options filter-name—Identifier for post-service filter.

Usage Guidelines See “Apply Filters and Services to an Interface” on page 114.

Required Privilege Level interface—to view this statement in the configuration.
interface-control—to add this statement to the configuration.
ppp-options

Syntax

ppp-options {
    chap {
        access-profile name;
        local-name name;
        passive;
    }
}

Hierarchy Level
[edit interfaces interface-name],
[edit interfaces interface-name unit logical-unit-number]

Description
On interfaces with PPP encapsulation, configure PPP-specific interface properties.

For ATM 2 interfaces only, you can configure PPP options on the logical interface unit if the logical interface is configured with one of the following PPP over ATM encapsulation types:

- atm-ppp-llc—PPP over ATM adaptation layer 5 (AAL5) logical link control (LLC) encapsulation.

- atm-ppp-vc-mux—PPP over ATM adaptation layer 5 (AAL5) multiplex encapsulation.

The remaining statements are explained separately.

Usage Guidelines
See “Configure PPP Challenge Handshake Authentication Protocol” on page 55.

Required Privilege Level
interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

preempt

Syntax
(preempt | no-preempt);

Hierarchy Level
[edit interfaces interface-name unit logical-unit-number family inet address address
vrrp-group group-number]

Description
When configuring Virtual Router Redundancy Protocol (VRRP) on Fast Ethernet and Gigabit Ethernet interfaces, configure whether a backup router can preempt a master router:

- preempt—Allow the master router to be preempted.

- no-preempt—Prohibit the preemption of the master router.

Default
If you omit this statement, the backup router can preempt a master router.

Usage Guidelines
See “Configure a Backup Router to Preempt the Master Router” on page 293.

Required Privilege Level
interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.
preferred

Syntax preferred;

Hierarchy Level [edit interfaces interface-name unit logical-unit-number family family address address ]

Description Configure this address to be the preferred address on the interface. If you configure more than one address on the same subnet, the preferred source address is chosen by default as the source address when you originate packets to destinations on the subnet.

Default The lowest numbered address on the subnet is the preferred address.

Usage Guidelines See “Configure the Interface Address” on page 81.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

premium

Syntax premium {
    bandwidth-limit rate;
    bandwidth-percent percent;
    burst-size-limit length;
}

Hierarchy Level [edit interfaces interface-name gigether-options ethernet-switch-profile ethernet-policer-profile policer cos-policer-name ]

Description Define a policer to apply to premium traffic.

Options bandwidth-limit rate—Bandwidth limit. You can specify rate in bits per second either as a complete decimal number or as a decimal number followed by the abbreviation k (1000), m (1,000,000), or g (1,000,000,000).
    Range: 32 Kilobits per second through 32 Gigabits per second

    bandwidth-percent percent—Bandwidth limit in percent.
    Range: 1 through 100 percent

    burst-size-limit length—Burst length, in bytes.
    Range: 1500 through 100,000,000 bytes

Usage Guidelines See “Configure a Gigabit Ethernet QPP Policer Profile” on page 269.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

See Also aggregate on page 424, ieee802.1-priority-map on page 477
primary

Syntax  primary;

Hierarchy Level  [edit interfaces interface-name unit logical-unit-number family family address address ]

Description  Configure this address to be the primary address of the protocol on the interface. If the logical unit has more than one address, the primary address is used by default as the source address when packets originate from the interface and the destination does not indicate the subnet.

Default  For unicast traffic, the primary address is the lowest non-127 preferred address on the unit.

Usage Guidelines  See “Configure the Interface Address” on page 81.

Required Privilege Level  interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

priority

priority (schedulers)

Syntax  priority (low | high);

Hierarchy Level  [edit interfaces interface-name atm-options scheduler-maps map-name forwarding-class class-name]

Description  For ATM 2 interfaces only, assign queueing priority to a forwarding class.

Options  low—Forwarding class has low priority.

| high—Forwarding class has high priority.


Required Privilege Level  interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.
**priority (vrrp)**

**Syntax**
```
priority priority;
```

**Hierarchy Level**
```
[edit interfaces interface-name]
```

**Description**
When configuring Virtual Router Redundancy Protocol (VRRP) on Fast Ethernet and Gigabit Ethernet interfaces, configure a VRRP router’s priority for becoming the master default router. The router with the highest priority within the group becomes the master.

**Options**
- **priority**—Router’s priority for being elected to be the master router in the VRRP group. A larger value indicates a higher priority for being elected.
  - Range: 1 through 255
  - Default: 100 (for backup routers)

**Usage Guidelines**
See “Configure Basic VRRP Support” on page 291.

**Required Privilege Level**
- **interface**—To view this statement in the configuration.
- **interface-control**—To add this statement to the configuration.

**promiscuous-mode**

**Syntax**
```
promiscuous-mode {
  vpi vpi-identifier;
}
```

**Hierarchy Level**
```
[edit interfaces interface-name atm-options]
```

**Description**
For ATM interfaces with atm-ccc-cell-relay encapsulation, map all incoming cells from either an interface port or a virtual path (VP) to a single LSP without restricting the VCI number. Promiscuous mode allows you to map traffic from all 65,535 VCIs to a single LSP, or from all 256 VPIs to a single LSP.

For multiport PICs, all ports must be configured in either promiscuous mode or non-promiscuous mode. When in promiscuous mode, all ports must also be configured with atm-ccc-cell-relay encapsulation.

For ATM 2 interfaces, changing modes between promiscuous and non-promiscuous causes all physical interfaces to be deleted and then re-added.

When interfaces are configured in promiscuous mode, you cannot configure VCIs.

**Options**
- **vpi-identifier**—Open this VPI in promiscuous mode.
  - Range: 0 through 255

**Usage Guidelines**
See “Configure ATM 1 and ATM 2 Cell-Relay Promiscuous Mode” on page 127.

**Required Privilege Level**
- **interface**—To view this statement in the configuration.
- **interface-control**—To add this statement to the configuration.

**See Also**
- **vpi** on page 568
**protect-circuit**

**Syntax**
protect-circuit group-name;

**Hierarchy Level**
[edit interfaces interface-name sonet-options aps]

**Description**
Configure the protect router in an APS circuit pair. When the working interface fails, APS brings up the protection circuit and the traffic is moved to the protection circuit.

**Options**
group-name—Circuit's group name.

**Usage Guidelines**
See “Configure Basic APS Support” on page 368.

**Required Privilege Level**
interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**See Also**
working-circuit on page 570

**proxy**

**Syntax**
proxy inet-address address;

**Hierarchy Level**
[edit interfaces interface-name unit logical-unit-number family tcc]

**Description**
For Layer 2.5 VPNs using an Ethernet interface as the TCC router, configure the IP address for which the TCC router is proxying. Ethernet TCC is supported on interfaces that carry IPv4 traffic only. Ethernet TCC encapsulation is supported on one-port Gigabit Ethernet, two-port Gigabit Ethernet, four-port Gigabit Ethernet, and four-port Fast Ethernet PICs only. Ethernet TCC is not supported on the T640 routing node.

**Options**
inet-address—Configure the IP address of the neighbor to the TCC router.

**Usage Guidelines**
See “Configure an Ethernet TCC or Extended VLAN TCC” on page 287 and “Example: Configure an Ethernet TCC or Extended VLAN TCC” on page 287.

**Required Privilege Level**
interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**See Also**
remote on page 530 and the JUNOS Internet Software Configuration Guide: VPNs.
**push**

**Syntax**

```
push;
```

**Hierarchy Level**

```
[edit interfaces interface-name unit logical-unit-number input-vlan-map],
[edit interfaces interface-name unit logical-unit-number output-vlan-map]
```

**Description**

For Gigabit Ethernet QPP interfaces only, add a new VLAN tag to the top of the VLAN stack. If you include the `push` statement in the configuration, you must also include the `pop` statement at the `[edit interfaces interface-name unit logical-unit-number output-vlan-map]` hierarchy level.

**Usage Guidelines**

See “Stack and Rewrite Gigabit Ethernet QPP VLAN Tags” on page 273.

**Required Privilege Level**

- `interface`—To view this statement in the configuration.
- `interface-control`—To add this statement to the configuration.

**See Also**

`pop` on page 521

---

**queue-depth**

**Syntax**

```
queue-depth cells;
```

**Hierarchy Level**

```
[edit edit interfaces interface-name atm-options linear-red-profiles profile-name]
```

**Description**

For ATM 2 interfaces only, define maximum queue depth in the CoS VC drop profile. Packets are always dropped beyond the defined maximum. This statement is mandatory; there is no default configuration.

**Default**

Buffer usage is unregulated.

**Options**

- `cells`—Maximum number of cells the queue can contain.
  - Range: 1 through 64,000 cells

**Usage Guidelines**

See “Configure ATM 2 VC Tunnel CoS Components” on page 155.

**Required Privilege Level**

- `interface`—To view this statement in the configuration.
- `interface-control`—To add this statement to the configuration.

**See Also**

`high-plp-threshold` on page 474, `low-plp-threshold` on page 495
queue-length

Syntax
queue-length number;

Hierarchy Level
[edit interfaces interface-name unit logical-unit-number shaping],
[edit interfaces interface-name unit logical-unit-number address family family
multipoint-destination address shaping]

Description
For ATM 1 interfaces only, define the maximum queue length in the traffic-shaping profile.
For ATM 1 PICs, each VC has its own independent shaping parameters.

Default
Buffer usage is unregulated.

Options
number—Maximum number of packets the queue can contain.
  Range: 1 through 16383 packets
  Default: 16383 packets

Usage Guidelines
See “Configure the ATM 1 Queue Length” on page 142.

Required Privilege Level
interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

rate

Syntax
rate percentage;

Hierarchy Level
[edit interfaces interface-name receive-bucket],
[edit interfaces interface-name transmit-bucket]

Description
Specify percentage of the interface line rate that is available to receive or transmit packets.

Options
percentage—Percentage of the interface line rate that is available to receive or transmit
  packets.
  Range: 0 through 100

Usage Guidelines
See “Configure Receive and Transmit Leaky Bucket Properties” on page 60 or on page 375.

Required Privilege Level
interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.
receive-bucket

Syntax
receive-bucket {
  overflow (tag | discard);
  rate percentage;
  threshold bytes;
}

Hierarchy Level [edit interfaces interface-name]

Description Set parameters for the receive leaky bucket, which specifies what percentage of the interface's total capacity can be used to receive packets.

For each DS-3 channel on an Channelized OC-12 interface, you can configure a unique receive bucket.

The statements are explained separately.

Usage Guidelines See “Configure Receive and Transmit Leaky Bucket Properties” on page 375.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

See Also transmit-bucket on page 557

red-differential-delay

Syntax red-differential-delay milliseconds;

Hierarchy Level [edit interfaces ls-fpc/pic/port:channel mlfr-uni-nni-bundle-options]

Description For link services interfaces only, configure the red differential delay among bundle links to give warning when a link has a differential delay that exceeds the configured threshold.

Options milliseconds—Red differential delay threshold.
  Range: 1 through 2000 milliseconds
  Default: 10 milliseconds

Usage Guidelines See “Configure Link Services Differential Delay” on page 330.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

See Also action-red-differential-delay on page 421, yellow-differential-delay on page 571
remote

Syntax
remote {
  (inet-address address | mac-address address);
}

Hierarchy Level [edit interfaces interface-name unit logical-unit-number family tcc]

Description For Layer 2.5 VPNs employing an Ethernet interface as the TCC router, configure the location
of the remote router. Ethernet TCC is supported on interfaces that carry IPv4 traffic only. Ethernet TCC encapsulation is supported on one-port Gigabit Ethernet, two-port Gigabit Ethernet, four-port Gigabit Ethernet, and four-port Fast Ethernet PICs only.

Options
mac-address—Configure the MAC address of the remote site.
inet-address—Configure the IP address of the remote site.

Usage Guidelines See “Configure an Ethernet TCC or Extended VLAN TCC” on page 287 and
“Example: Configure an Ethernet TCC or Extended VLAN TCC” on page 287.

Required Privilege Level interface—to view this statement in the configuration.
interface-control—to add this statement to the configuration.

See Also proxy on page 526 and JUNOS Internet Software Configuration Guide: VPNs.

remote-loopback-respond

Syntax remote-loopback-respond;

Hierarchy Level [edit interfaces interface-name t1-options]

Description For T1 interfaces only, configure the router to respond to remote loopback requests. Remote
loopback requests can be from the facility data link or inband.

Default The router does not respond to remote loop requests.

Usage Guidelines See “Configure T1 Remote Loopback Response” on page 390.

Required Privilege Level interface—to view this statement in the configuration.
interface-control—to add this statement to the configuration.

See Also loopback on page 492, feac-loop-respond on page 468
request

Syntax  request (protect | working);

Hierarchy Level  [edit interfaces interface-name sonet-options aps]

Description  Perform a manual switch between the protect and working circuits. This statement is honored only if there are no higher-priority reasons to switch.

Options  protect—Request the circuit to become the protect circuit.

working—Request the circuit to become the working circuit.

Usage Guidelines  See “Configure Switching between the Working and Protect Circuits” on page 370.

Required Privilege Level  interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

See Also  force on page 470

revert-time

Syntax  revert-time seconds;

Hierarchy Level  [edit interfaces interface-name sonet-options aps]

Description  Configure APS revertive mode.

Default  APS operates in nonrevertive mode.

Options  seconds—Amount of time to wait after the working circuit has again become functional before making the working circuit active again.

Range: 1 through 65,535 seconds

Default: none (APS operates in nonrevertive mode)

Usage Guidelines  See “Configure Revertive Mode” on page 371.

Required Privilege Level  interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

rfc-2615

Syntax  rfc-2615;

Hierarchy Level  [edit interfaces interface-name sonet-options]

Description  Include this statement to enable RFC 2615 features.

Default  Settings required by RFC 1619.

Usage Guidelines  See “Configure SONET RFC 2615 Support” on page 366.

Required Privilege Level  interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.
**routing-instance**

Syntax:

```
routing-instance { 
  destination routing-instance-name; 
}
```

Hierarchy Level: [edit interfaces interface-name unit logical-unit-number tunnel]

Description: Specify the destination routing instance that points to the routing table containing the tunnel destination address.

Default: The default Internet routing table inet.0.

Usage Guidelines: See “Configure a Tunnel Interface for Routing Table Lookup” on page 409.

Required Privilege Level: interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**rpf-check**

Syntax:

```
rpf-check fail-filter filter-name; 
```

Hierarchy Level: [edit interfaces interface-name unit logical-unit-number family inet], [edit interfaces interface-name unit logical-unit-number family inet6]

Description: Check whether traffic is arriving on an expected path.

Options: fail-filter—A filter to evaluate when packets are received on the interface. If the RPF check fails, this optional filter is evaluated.

Usage Guidelines: See “Configure Unicast RPF Strict Mode” on page 90.

Required Privilege Level: interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**rts**

Syntax:

```
rts (assert | de-assert | normal); 
```

Hierarchy Level: [edit interfaces interface-name serial-options control-leads]

Description: For EIA-530 and V.35 interfaces only, configure the to-DCE signal, request-to-send (RTS).

Options: assert—The to-DCE signal must be asserted.
        de-assert—The to-DCE signal must be deasserted.
        normal—Normal RTS signal handling, as defined by the TIA/EIA Standard 530.

Default: normal

Usage Guidelines: See “Configure the Serial Signal Handling” on page 352.

Required Privilege Level: interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.
rts-polarity

Syntax  
  rts-polarity (positive | negative);

Hierarchy Level  
  [edit interfaces interface-name serial-options ]

Description  
  Configure request-to-send (RTS) signal polarity.

Options  
  positive—Positive signal polarity.
  negative—Negative signal polarity.

Default: positive

Usage Guidelines  
  See “Configure Serial Signal Polarisations” on page 355.

Required Privilege Level  
  interface—To view this statement in the configuration.
  interface-control—To add this statement to the configuration.

rtvbr

Syntax  
  rtvbr peak rate sustained rate burst length;

Hierarchy Level  
  [edit interfaces interface-name unit logical-unit-number shaping],
  [edit interfaces interface-name unit logical-unit-number address address family family multipoint-destination address shaping],
  [edit interfaces interface-name atm-options vpi vpi-identifier shaping]

Description  
  For ATM 2 PICs only, define the real-time variable bandwidth utilization in the traffic-shaping profile.

When you configure the real-time bandwidth utilization, you must specify all three options (burst, peak, and sustained). You can specify rate in bits per second either as a complete decimal number or as a decimal number followed by the abbreviation k (1000), m (1,000,000), or g (1,000,000,000). You can also specify rate in cells per second by entering a decimal number followed by the abbreviation c; values expressed in cells per second are converted to bits per second using the formula 1 cps = 384 bps.

Default  
  Unspecified bit rate (UBR); that is, bandwidth utilization is unlimited.

Options  
  burst length—Burst length, in cells. If you set the length to 1, the peak traffic rate is used.
    Range: 1 through 4000 cells
  peak rate—Peak rate, in bps or cps.
    Range: 33 kbps through 135.6 Mbps (ATM OC-3); 33 kbps through 276 Mbps (ATM OC-12)
  sustained rate—Sustained rate, in bps or cps.
    Range: 33 kbps through 135.6 Mbps (ATM OC-3); 33 kbps through 276 Mbps (ATM OC-12)

Usage Guidelines  
  See “Configure ATM 2 Real-Time VBR” on page 139.

Required Privilege Level  
  interface—To view this statement in the configuration.
  interface-control—To add this statement to the configuration.

See Also  
  cbr on page 440, vbr on page 564
sampling

Syntax
sampling direction;

Hierarchy Level
[edit interfaces interface-name unit logical-unit-number family inet]

Description
For monitoring services and adaptive services interfaces only, configure direction of traffic to be sampled.

Options
input—Configure at least one expected ingress point.

output—Configure at least one expected egress point.

input output—On a single interface, configure at least one expected ingress point and one egress point.

Usage Guidelines
See “Configure Flow Monitoring” on page 316.

Required Privilege Level
interface—to view this statement in the configuration.
interface-control—to add this statement to the configuration.

scheduler-maps

Syntax
scheduler-maps map-name {
   forwarding-class (class-name | assured-forwarding | best-effort | expedited-forwarding | network-control);
   vc-cos-mode (alternate | strict);
}

Hierarchy Level
[edit interfaces interface-name atm-options]

Description
For ATM 2 interfaces only, define CoS parameters assigned to forwarding classes.

Options
map-name—Name of the scheduler map.

The remaining statements are explained separately.

Usage Guidelines
See “Configure ATM 2 VC Tunnel CoS Components” on page 155.

Required Privilege Level
interface—to view this statement in the configuration.
interface-control—to add this statement to the configuration.

See Also
atm-scheduler-map on page 429, scheduler-maps on page 643
serial-options

Syntax

serial-options {
  clock-rate rate;
  clocking-mode (dce | dte | loop);
  control-leads {
    control-signal (assert | de-assert | normal);
    cts (ignore | normal | require);
    dcd (ignore | normal | require);
    dsr (ignore | normal | require);
    dtr signal-handling-option;
    ignore-all;
    indication (ignore | normal | require);
    rts (assert | de-assert | normal);
    tm (ignore | normal | require);
  }
  control-polarity (positive | negative);
  cts-polarity (positive | negative);
  dcd-polarity (positive | negative);
  dsr-polarity (positive | negative);
  dtr-circuit (balanced | unbalanced);
  dtr-polarity (positive | negative);
  encoding (nrz | nrzi);
  indication-polarity (positive | negative);
  line-protocol protocol;
  loopback (dce-local | dce-remote | liu | local);
  rts-polarity (positive | negative);
  tm-polarity (positive | negative);
  transmit-clock invert;
}

Hierarchy Level [edit interfaces interface-name]

Description Configure serial-specific interface properties.
The statements are explained separately.

Usage Guidelines See “Configure Serial Interfaces” on page 345.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

See Also no-concatenate in JUNOS Internet Software Guide: Getting Started
service

Syntax

service {
  input {
    [ service-set service-set-name <service-filter filter-name> ];
    post-service-filter filter-name;
  }
  output {
    [ service-set service-set-name <service-filter filter-name> ];
  }
}

Hierarchy Level [edit interfaces interface-name unit logical-unit-number family inet]

Description Define the service sets and filters to be applied to an interface.

Options The remaining statements are explained separately.

Usage Guidelines See “Apply Filters and Services to an Interface” on page 114.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

service-domain

Syntax service-domain (inside | outside);

Hierarchy Level [edit interfaces interface-name unit logical-unit-number family inet]

Description Specify service interface domain. If you specify this interface using the next-hop-service statement at the [edit services service-set service-set-name] hierarchy level, the interface domain must match that used with the inside-service-interface and outside-service-interface statements.

Options inside—Interface used within the network.

outside—Interface used outside the network.

Usage Guidelines See “Configure the Interface Address and Domain” on page 112.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.
service-filter

Syntax:  service-filter filter-name;

Hierarchy Level: [edit interfaces interface-name unit logical-unit-number family inet service (input | output)]

Description: Define the filter to be applied to traffic before it is accepted for service processing. Configuration of a service filter is optional; if you include the service-set statement without a service-filter definition, the router software assumes the match condition is true and selects the service set for processing automatically.

Options: filter-name—Identifies the filter to be applied in service processing.

Usage Guidelines: See “Apply Filters and Services to an Interface” on page 114.

Required Privilege Level: interface—to view this statement in the configuration. interface-control—to add this statement to the configuration.

service-set

Syntax:  service-set service-set-name;

Hierarchy Level: [edit interfaces interface-name unit logical-unit-number family inet service (input | output)]

Description: Define one or more service sets to be applied to an interface. If you define multiple service sets, the router software evaluates the filters in the order in which they appear in the configuration.

Options: service-set-name—Identifies the service set.

Usage Guidelines: See “Apply Filters and Services to an Interface” on page 114.

Required Privilege Level: interface—to view this statement in the configuration. interface-control—to add this statement to the configuration.
service-options

Syntax

```
service-options {
    inactivity-timeout seconds;
    open-timeout seconds;
    syslog {
        host host-name {
            facility-override facility-name;
            log-prefix prefix-number;
            [ services priority-level ];
        }
    }
}
```

Hierarchy Level
[edit interfaces interface-name]

Description
Define the service options to be applied on an interface.

Options
The remaining statements are explained separately.

Usage Guidelines
See “Configure Service Interface Properties” on page 112.

Required Privilege Level
interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

services

Syntax

```
services priority-level;
```

Hierarchy Level
[edit interfaces interface-name service-options syslog host host-name]

Description
Specify system logging priority level.

Options
priority-level—Assigns a priority level to the facility. Valid entries are:

- alert—Conditions that should be corrected immediately
- any—Matches any level.
- critical—Critical conditions.
- emergency—Panic conditions.
- error—Error conditions.
- info—Informational messages.
- notice—Conditions that require special handling.
- warning—Warning messages.

Usage Guidelines

Required Privilege Level
interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.
shaping

Syntax

shaping {  
  (cbr rate | rtvbr peak rate sustained rate burst length |  
    vbr peak rate sustained rate burst length);  
  queue-length number;  
}

Hierarchy Level

[edit interfaces interface-name unit logical-unit-number]  
[edit interfaces interface-name unit logical-unit-number address family family  
  multipoint-destination address],  
[edit interfaces interface-name atm-options vpi vpi-identifier]

Description

For ATM encapsulation only, define the traffic-shaping profile.

For ATM 2 interfaces, changing or deleting virtual path (VP) tunnel traffic shaping causes all  
logical interfaces on a VP to be deleted and then re-added.

VP tunnels are not supported on multipoint interfaces.

The statements are explained separately.

Usage Guidelines

See “Define Virtual Path Tunnels on ATM 2 Interfaces” on page 134 and “Define the ATM 1  
and ATM 2 Traffic-Shaping Profile” on page 137.

Required Privilege Level

interface—To view this statement in the configuration.  
interface-control—To add this statement to the configuration.

short-sequence

Syntax

short-sequence;

Hierarchy Level

[edit interfaces (ml-fpc/pic/port | ls-fpc/pic/port) unit logical-unit-number ]

Description

For multilink interfaces only, set the length of the packet sequence identification number to  
12 bits.

Default

If not included in the configuration, the length is set to 24 bits.

Usage Guidelines

See “Configure Multilink and Link Services Sequence Format” on page 327.

Required Privilege Level

interface—To view this statement in the configuration.  
interface-control—To add this statement to the configuration.
sonet-options

Syntax

sonet-options {
  aps {
    advertise-interval milliseconds;
    authentication-key key;
    force;
    hold-time milliseconds;
    lockout;
    neighbor address;
    paired-group group-name;
    protect-circuit group-name;
    request;
    revert-time seconds;
    working-circuit group-name;
  }
  bytes {
    e1-quiet value;
    f1 value;
    f2 value;
    s1 value;
    z3 value;
    z4 value;
  }
  fcs (32 | 16);
  loopback (local | remote);
  path-trace trace-string;
  (payload-scrambler | no-payload-scrambler);
  rfc2615;
  vtmapping (itu-t | klm);
  (z0-increment | no-z0-increment);
}

Hierarchy Level

[edit interfaces interface-name]

Description

Configure SONET-specific interface properties.

On SONET OC-48 interfaces that you configure for channelized (multiplexed) mode (by including the no-concatenate statement at the [edit chassis fpc slot-number pic pic-number] hierarchy level), the bytes e1-quiet and bytes f1 options have no effect. The bytes f2, bytes z3, bytes z4, and path-trace options work correctly on channel 0 and work in the transmit direction only on channels 1, 2, and 3.

On a Channelized OC-12 interface, the bytes e1-quiet, bytes f1, bytes f2, bytes z3, and bytes z4 options are not supported. The fcs and payload-scrambler statements are also not supported; you must configure these for each DS-3 channel using the t3-options fcs and t3-options payload-scrambler statements. The aps and loopback statements are supported only on channel 0 and are ignored if included in the configurations for channels 1 through 11. You can configure loopbacks for each DS-3 channel with the t3-options loopback statement. The path-trace statement can be included in the configuration for each DS-3 channel, thereby configuring a unique path trace for each channel.

If you are running IS-IS over SONET interfaces, use PPP if you are running Cisco IOS Release 12.0 or later. If you need to run HDLC, configure an ISO family MTU of 4469 on the router.

The statements are explained separately.
Usage Guidelines

See “Configure Channelized OC-12 Interfaces” on page 183, “Configure Channelized STM-1 Interfaces” on page 205, and “Configure SONET/SDH Physical Interface Properties” on page 360.

Required Privilege Level

interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

See Also

no-concatenate in JUNOS Internet Software Guide: Getting Started

source

Syntax

source source-address;

Hierarchy Level

[edit interfaces interface-name unit logical-unit-number tunnel destination-address ]

Description

Specify the source address of the tunnel.

Default

If you do not specify a source address, the tunnel uses the unit’s primary address as the source address of the tunnel.

Options

source-address—Address of the local side of the tunnel. This is the address that is placed in the outer IP header’s source field.

Usage Guidelines

See “Configure Tunnel Interfaces” on page 407.

Required Privilege Level

interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

See Also

multicasts-only on page 501, primary on page 524
source-address-filter

Syntax
source-address-filter {
    mac-address;
}

Hierarchy Level
[edit interfaces interface-name aggregated-ether-options],
[edit interfaces interface-name fastether-options],
[edit interfaces interface-name gigether-options]

Description
For aggregated Ethernet, Fast Ethernet, and Gigabit Ethernet interfaces only, specify the MAC
addresses from which the interface can receive packets. For this statement to have any effect,
you must include the source-filtering statement in the configuration to enable source address
filtering.

Options
mac-address — MAC address filter. You can specify the MAC address as nn:nn:nn:nn:nn:nn
or nnn.nnn.nnn, where n is a decimal digit. To specify more than one address, include
multiple mac-address options in the source-address-filter statement.

If you enable Virtual Router Redundancy Protocol (VRRP) on a Fast or Gigabit Ethernet
interface, as described in “Configure VRRP” on page 290, and if you enable MAC source
address filtering on the interface, you must include the virtual MAC address in the list of
source MAC addresses that you specify in the source-address-filter statement. MAC
addresses ranging from 00:00:5e:00:01:00 through 00:00:5e:00:01:ff are reserved for
VRRP, as defined in RFC 2338. When you configure the VRRP group, the group number
must be the decimal equivalent of the last hexadecimal byte of the virtual MAC address.

Usage Guidelines
See “Configure Ethernet MAC Address Filtering” on page 279.

Required Privilege Level
interface — To view this statement in the configuration.
interface-control — To add this statement to the configuration.

See Also
source-filtering on page 543
source-class-usage

Syntax

source-class-usage { (input | output | [input output]) }

Hierarchy Level
[edit interfaces interface-name unit logical-unit-number family (inet) accounting]

Description
Enable packet counters on an interface that count packets that arrive from specific prefixes on
the provider core router and are destined for specific prefixes on the customer edge router.

Options
input—Configure at least one expected ingress point.
output—Configure at least one expected egress point.
input output—On a single interface, configure at least one expected ingress point and one
expect egress point.

Usage Guidelines
See “Enable Source Class and Destination Class Usage” on page 94 or “Configure Flow
Monitoring” on page 316.

Required Privilege Level
interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

See Also
accounting on page 419, destination-class-usage on page 450

source-filtering

Syntax
(source-filtering | no-source-filtering);

Hierarchy Level
[edit interfaces interface-name aggregated-ether-options],
[edit interfaces interface-name fastether-options],
[edit interfaces interface-name gigether-options]

Description
For aggregated Ethernet, Fast Ethernet, Gigabit Ethernet, and Gigabit Ethernet QPP interfaces
only, enable the filtering of MAC source addresses, which blocks all incoming packets to that
interface. To allow the interface to receive packets from specific MAC addresses, include the
source-address-filter statement.

If the remote Ethernet card is changed, the interface will no longer be able to receive packets
from the new card because it will have a different MAC address.

Default
Source address filtering is disabled.

Usage Guidelines
See “Configure Ethernet MAC Address Filtering” on page 279.

Required Privilege Level
interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

See Also
accept-source-mac on page 418, source-address-filter on page 542,
speed

Syntax  speed (10m | 100m);

Hierarchy Level  [edit interfaces interface-name]

Description  Configure the interface's speed. This statement applies only to the management Ethernet interface (fxp0) and to the Fast Ethernet 12-port and 48-port PICs.

Options  You can specify the speed as either 10m or 100m (values in Mbps).

Usage Guidelines  See “Configure the Interface Speed” on page 57 or on page 282.

Required Privilege Level  interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

stacked-vlan-tagging

Syntax  stacked-vlan-tagging;

Hierarchy Level  [edit interfaces interface-name]

Description  For Gigabit Ethernet QPP interfaces, enable stacked VLAN tagging for all logical interfaces on the physical interface.

Usage Guidelines  See “Stack and Rewrite Gigabit Ethernet QPP VLAN Tags” on page 273.

Required Privilege Level  interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

See Also  vlan-tag on page 567

start-end-flag

Syntax  start-end-flag (shared | filler);

Hierarchy Level  [edit interfaces interface-name ds0-options],
[edit interfaces interface-name e1-options],
[edit interfaces interface-name e3-options],
[edit interfaces interface-name t1-options],
[edit interfaces interface-name t3-options]

Description  For DS-0, E1, E3, T1, or T3 interfaces, configure the interface to share the transmission of start and end flags.

Options  filler—Wait two idle cycles between the start and end flags.
shared—Share the transmission of the start and end flags.

Usage Guidelines  See “Configure E1 Start End Flags” on page 248, “Configure the E3 Start End Flags” on page 256, “Configure T1 Start End Flags” on page 394, and “Configure the T3 Start End Flags” on page 403.

Required Privilege Level  interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.
swap

Syntax
swap;

Hierarchy Level
[edit interfaces interface-name unit logical-unit-number input-vlan-map],
[edit interfaces interface-name unit logical-unit-number output-vlan-map]

Description
For Gigabit Ethernet QPP interfaces only, replace a VLAN tag. All tagged frames entering or exiting the interface are converted to a specified VLAN ID and TPID.

You cannot include both the the swap statement and the vlan-id statement at the [edit interfaces interface-name unit logical-unit-number output-vlan-map] hierarchy level. If you include the swap statement in the output VLAN map, the VLAN ID in the outgoing frame is rewritten to the vlan-id statement you include at the [edit interfaces interface-name unit logical-unit-number] hierarchy level.

Usage Guidelines
See “Stack and Rewrite Gigabit Ethernet QPP VLAN Tags” on page 273.

Required Privilege Level
interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

See Also
pop on page 521, push on page 527, tag-protocol-id on page 549, vlan-id on page 566

syslog

syslog (interfaces)

Syntax
syslog {
host host-name {
   facility-override facility-name;
   log-prefix prefix-number;
   [ services priority-level ];
}
}

Hierarchy Level
[edit interfaces interface-name service-options]

Description
Configure generation of system log messages for the service set. System log information is passed to the kernel for logging in the /var/log directory. Any values configured in the service set definition override these values.

Options
The remaining statements are explained separately.

Usage Guidelines

Required Privilege Level
interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.
**syslog (monitoring)**

**Syntax**  
(syslog | no-syslog);

**Hierarchy Level**  
[edit interfaces mo-fpc/ pic/ port multiservice-options]

**Description**  
System logging is enabled by default. The system log information of the monitoring services PIC is passed to the kernel for logging in the /var/log directory.

- **syslog**—Enable PIC system logging.
- **no-syslog**—Disable PIC system logging.

**Usage Guidelines**  
See “Configure Multiservice Physical Interface Properties” on page 65 or “Configure Flow Monitoring” on page 316.

**Required Privilege Level**  
interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.
t1-options

Syntax  
t1-options {
  bert-algorithm algorithm;
  bert-error-rate rate;
  bert-period seconds;
  buildout (0-132 | 133-265 | 266-398 | 399-531 | 532-655);
  byte-encoding (nx64 | nx56);
  fcs (32 | 16);
  framing (sf | esf);
  idle-cycle-flag (flags | ones);
  invert-data;
  line-encoding (ami | b8zs);
  loopback (local | remote);
  remote-loopback-respond;
  start-end-flag (shared | filler);
  timeslots time-slot-range;
}

Hierarchy Level  [edit interfaces interface-name]

Description  Configure T1-specific physical interface properties.

The statements are explained separately.

Usage Guidelines  See “Configure T1 Interfaces” on page 387.

Required Privilege Level  interface—To view this statement in the configuration.
  interface-control—To add this statement to the configuration.
**t3-options**

**Syntax**

```
t3-options {
  bert-algorithm algorithm;
  bert-error-rate rate;
  bert-period seconds;
  (cbit-parity | no-cbit-parity);
  compatibility-mode (digital-link | kentrox | larscom) <subrate value>;
  fcs (32 | 16);
  (feac-loop-respond | no-feac-loop-respond);
  idle-cycle-flag value;
  (long-buildout | no-long-buildout);
  loopback (local | remote);
  start-end-flag value;
}
```

**Hierarchy Level**

```
[edit interfaces interface-name]
```

**Description**

Configure T3-specific physical interface properties, including the properties of DS-3 channels on a Channelized OC-12 interface. The `long-buildout` statement is not supported for DS-3 channels on a channelized OC-12 interface.

On T3 interfaces, the default encapsulation is PPP.

For ATM 1 interfaces, you can configure a subset of E3 options statements. The statements are explained separately.

**Usage Guidelines**

See “Configure T3 Interfaces” on page 395.

**Required Privilege Level**

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

---

**t391**

**Syntax**

```
t391 seconds;
```

**Hierarchy Level**

```
[edit interfaces ls-fpc/pic/port:channel mlfr-uni-nni-bundle-options]
```

**Description**

For link services interfaces only, set Frame Relay link integrity polling interval.

**Options**

- `number`—Number of link integrity polling interval.
  - Range: 5 through 30 seconds
  - Default: 10 seconds

**Usage Guidelines**

See "Configure Link Services Keepalive Settings on Frame Relay LMI" on page 331.

**Required Privilege Level**

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

**See Also**

n391 on page 503, n392 on page 504, n393 on page 504, t392 on page 549
t392

Syntax  t392 seconds;

Hierarchy Level  [edit interfaces ls-fpc/ pic/ port:channel mfr-uni-nni-bundle-options]

Description  For link services interfaces only, set Frame Relay polling verification interval.

Options  number—Number of polling verification interval.
  Range: 5 through 30 seconds
  Default: 15 seconds

Usage Guidelines  See “Configure Link Services Keepalive Settings on Frame Relay LMI” on page 331.

Required Privilege Level  interface—To view this statement in the configuration.
  interface-control—To add this statement to the configuration.

See Also  n391 on page 503, n392 on page 504, n393 on page 504, timeslots on page 550

tag-protocol-id

tag-protocol-id (TPIDs expected to be sent or received)

Syntax  tag-protocol-id [ tpids ];

Hierarchy Level  [edit interfaces interface-name gigether-options ethernet-switch-profile]

Description  For Gigabit Ethernet QPP interfaces only, define the TPIDs expected to be sent or received on a particular VLAN. For each Gigabit Ethernet QPP port, you can configure up to eight TPIDs.

Options  tpids—Tag protocol IDs to be accepted on the VLAN.

Usage Guidelines  See “Stack and Rewrite Gigabit Ethernet QPP VLAN Tags” on page 273.

Required Privilege Level  interface—To view this statement in the configuration.
  interface-control—To add this statement to the configuration.

tag-protocol-id (TPID to rewrite)

Syntax  tag-protocol-id tpid;

Hierarchy Level  [edit interfaces interface-name unit logical-unit-number input-vlan-map],
  [edit interfaces interface-name unit logical-unit-number output-vlan-map]

Description  For Gigabit Ethernet QPP interfaces only, configure the outer Tag Protocol identifier (TPID) value. All TPIDs you include in input and output VLAN maps must be among those you specify at the [edit interfaces interface-name gigether-options ethernet-switch-profile tag-protocol-id [ tpids ]] hierarchy level.

Default  If the tag-protocol-id statement is not configured, the TPID value is 0x8100.

Usage Guidelines  See “Stack and Rewrite Gigabit Ethernet QPP VLAN Tags” on page 273.

Required Privilege Level  interface—To view this statement in the configuration.
  interface-control—To add this statement to the configuration.
threshold

Syntax  
threshold bytes;

Hierarchy Level  [edit interfaces interface-name]

Description  Specify the bucket threshold, which controls the burstiness of the leaky bucket mechanism. The larger the value, the more bursty the traffic, which means that over a very short amount of time, the interface can receive or transmit close to line rate, but the average over a longer time is at the configured bucket rate.

Options  
bytes—Maximum size, in bytes, for traffic bursts.
  Range: 0 through 16777215 bytes

Usage Guidelines  See “Configure Receive and Transmit Leaky Bucket Properties” on page 60 or on page 375.

Required Privilege Level  interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

timeslots

Syntax  
timeslots time-slot-range;

Hierarchy Level  [edit interfaces interface-name e1-options],
  [edit interfaces interface-name t1-options],
  [edit interfaces interface-name partition partition-number]

Description  For E1 and T1 interfaces, allocate the specific time slots by number. For E1 interfaces, time slot 0 is reserved.

Options  
time-slot-range—Actual time slot numbers allocated:
  Range: 1 through 24 for T1 interfaces, 2 through 31 for E1 interfaces.

Usage Guidelines  See “Configure Fractional E1 QPP Interfaces” on page 174, “Configure Fractional T1 QPP Interfaces” on page 223, “Configure Fractional E1 Time Slots” on page 249, “Configure Fractional T1 Time Slots” on page 394.

Required Privilege Level  interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.
tm

Syntax  tm (ignore | normal | require);

Hierarchy Level  [edit interfaces interface-name serial-options control-leads ]

Description  For EIA-530 interfaces only, configure the from-DCE signal, test-mode (TM).

Options  ignore—The from-DCE signal is ignored.

         normal—Normal TM signal handling as defined by the TIA/EIA Standard 530.

         require—The from-DCE signal must be asserted.

Default: normal

Usage Guidelines  See “Configure the Serial Signal Handling” on page 352.

Required Privilege Level  interface—To view this statement in the configuration.

                        interface-control—To add this statement to the configuration.

tm-polarity

Syntax  tm-polarity (positive | negative);

Hierarchy Level  [edit interfaces interface-name serial-options ]

Description  Configure test-mode (TM) signal polarity.

Options  positive—Positive signal polarity.

         negative—Negative signal polarity.

Default: positive


Required Privilege Level  interface—To view this statement in the configuration.

                        interface-control—To add this statement to the configuration.
traceoptions

**traceoptions (individual interfaces)**

- **Syntax**

  ```
  traceoptions {
      flag flag <disable>;
  }
  ```

- **Hierarchy Level**

  ```
  [edit interfaces interface-name]
  ```

- **Description**

  Define tracing operations for individual interfaces.

  To specify more than one tracing operation, include multiple flag statements.

- **Default**

  If you do not include this statement, no interface-specific tracing operations are performed.

- **Options**

  - `disable` — (Optional) Disable the tracing operation. You can use this option to disable a single operation when you have defined a broad group of tracing operations, such as all.

  - `flag` — Tracing operation to perform. To specify more than one tracing operation, include multiple flag statements. The following are the interface-specific tracing options.
    - `all` — All interface tracing operations
    - `event` — Interface events
    - `ipc` — Interface IPC messages
    - `media` — Interface media changes

- **Usage Guidelines**


- **Required Privilege Level**

  - `interface` — To view this statement in the configuration.
  - `interface-control` — To add this statement to the configuration.
traceoptions (interface process)

Syntax

traceoptions {
    file filename <files number> <size size> <(world-readable | no-world-readable)>;
    flag flag <disable>;
}

Hierarchy Level
[edit interfaces]

Description
Define tracing operations for the interface process (dcd).

Default
If you do not include this statement, no interface-specific tracing operations are performed.

Options
disable—(Optional) Disable the tracing operation. You can use this option is to disable a single operation when you have defined a broad group of tracing operations, such as all.

filename—Name of the file to receive the output of the tracing operation. Enclose the name within quotation marks. All files are placed in the directory /var/log. By default, interface process tracing output is placed in the file dcd.

files number—(Optional) Maximum number of trace files. When a trace file named trace-file reaches its maximum size, it is renamed trace-file.0, then trace-file.1, and so on, until the maximum number of trace files is reached. Then, the oldest trace file is overwritten.

If you specify a maximum number of files, you also must specify a maximum file size with the size option.

Range: 2 through 1,000
Default: 3 files

flag—Tracing operation to perform. To specify more than one tracing operation, include multiple flag statements. You can include the following flags:

- change-events—Log changes that produce configuration events
- config-states—Log the configuration state machine changes
- kernel—Log configuration IPC messages to kernel
- kernel-detail—Log details of configuration messages to kernel

no-world-readable—(Optional) Disallow any user to read the log file.

size size—(Optional) Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named trace-file reaches this size, it is renamed trace-file.0. When the trace-file again reaches its maximum size, trace-file.0 is renamed trace-file.1 and trace-file is renamed trace-file.0. This renaming scheme continues until the maximum number of trace files is reached. Then, the oldest trace file is overwritten.

If you specify a maximum file size, you also must specify a maximum number of trace files with the files option.

Syntax: xk to specify KB, xm to specify MB, or xg to specify GB
Range: 10 KB through the maximum file size supported on your router
Default: 1 MB

world-readable—(Optional) Allow any user to read the log file.
traceoptions

Usage Guidelines

Required Privilege Level
interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

traceoptions (VRRP)

Syntax
traceoptions {
  file {
    filename filename;
    files number;
    size size;
    (world-readable | no-world-readable);
  }
  flag flag;
}

Hierarchy Level
[edit protocols vrrp]

Description
Define tracing operations for Virtual Router Redundancy Protocol (VRRP).

To specify more than one tracing operation, include multiple flag statements.

By default, VRRP logs the error, dcd configuration, and routing socket events in a file in the directory /var/log.

Default
If you do not include this statement, no VRRP-specific tracing operations are performed.

Options
filename filename—Name of the file to receive the output of the tracing operation. Enclose the name within quotation marks. All files are placed in the directory /var/log. By default, interface process tracing output is placed in the file vrrpd.

files number—(Optional) Maximum number of trace files. When a trace file named trace-file reaches its maximum size, it is renamed trace-file.0, then trace-file.1, and so on, until the maximum number of trace files is reached. Then, the oldest trace file is overwritten.

If you specify a maximum number of files, you also must specify a maximum file size with the size option.

Range: 2 through 1,000
Default: 3 files

flag flag—Tracing operation to perform. To specify more than one tracing operation, include multiple flag statements. These are the VRRP-specific tracing options.

- all—All VRRP tracing operations
- database—Database changes
- general—General events
- interfaces—Interface changes
- normal—Normal events
- packets—Packets sent and received
track

Syntax: track {
    interface interface-name priority-cost cost;
}

Hierarchy Level: [edit interfaces interface-name unit logical-unit-number family inet address address vrrp-group group-number]

Description: On Fast Ethernet and Gigabit Ethernet interfaces only, enable logical interface tracking for a Virtual Router Redundancy Protocol (VRRP) group.

Options:
- interface interface-name—Interface to be tracked for this VRRP group
  Range: Up to 10 interfaces can be tracked

- priority-cost cost—The value subtracted from the configured VRRP priority when the tracked interface is down, forcing a new master router election. The sum of all the costs for all interfaces or routes that are tracked must be less than or equal to the configured priority of the VRRP group.
  Range: 1 through 254

Usage Guidelines: See “Configure a Logical Interface to Be Tracked” on page 295.

Required Privilege Level:
- interface—To view this statement in the configuration.
- interface-control—To add this statement to the configuration.
**translate-discard-eligible**

Syntax: (translate-discard-eligible | no-translate-discard-eligible);

Hierarchy Level: [edit interfaces interface-name unit logical-unit-number family ccc]

Description: For interfaces with encapsulation type Frame Relay CCC, enable or disable translation of Frame Relay discard eligible (DE) control bits.

Default: DE bit translation is disabled.

Usage Guidelines: See “Configure Frame Relay Control Bit Translation” on page 305.

Required Privilege Level: interface—to view this statement in the configuration.
interface-control—to add this statement to the configuration.

**translate-fecn-and-becn**

Syntax: (translate-fecn-and-becn | no-translate-fecn-and-becn);

Hierarchy Level: [edit interfaces interface-name unit logical-unit-number family ccc]

Description: For interfaces with encapsulation type Frame Relay CCC, enable or disable translation of Frame Relay forward explicit congestion notification (FECN) control bits and Frame Relay backward explicit congestion notification (BECN) control bits.

Default: FECN and BECN bit translation is disabled.

Usage Guidelines: See “Configure Frame Relay Control Bit Translation” on page 305.

Required Privilege Level: interface—to view this statement in the configuration.
interface-control—to add this statement to the configuration.
transmit-bucket

Syntax
transmit-bucket {
  overflow discard;
  rate percentage;
  threshold bytes;
}

Hierarchy Level [edit interfaces interface-name]

Description Set parameters for the transmit leaky bucket, which specifies what percentage of the interface's total capacity can be used to transmit packets.

For each DS-3 channel in an Channelized OC-12 interface, you can configure a unique transmit bucket.

The statements are explained separately.

Usage Guidelines See “Configure Receive and Transmit Leaky Bucket Properties” on page 60 or on page 375.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

See Also receive-bucket on page 529

transmit-clock

Syntax
transmit-clock invert;

Hierarchy Level [edit interfaces interface-name serial-options]

Description Configure the transmit clock signal.

Options invert—Shift the clock phase 180 degrees.

Usage Guidelines See “Configure the Serial Clocking Mode” on page 350.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.
transmit-weight

transmit-weight (ATM 2 Virtual Circuit)

Syntax transmit-weight number;

Hierarchy Level [edit interfaces interface-name unit logical-unit-number]

Description For ATM 2 PICs only, configure the transmission weight.

Each VC is serviced in weighted round robin (WRR) mode. When VCs have data to send, they send the number of cells equal to their weight before passing control to the next active VC. This allows proportional bandwidth sharing between multiple VCs within a rate-shaped VP tunnel. VP tunnels are not supported on multipoint interfaces.

Options number—Number of cells a VC sends before passing control to the next active VC within a VP tunnel.

Range: 1 through 32,767

Usage Guidelines See “Define the ATM 1 and ATM 2 Traffic-Shaping Profile” on page 137.

Required Privilege Level interface—to view this statement in the configuration.

interface-control—to add this statement to the configuration.

transmit-weight (ATM 2 CoS Forwarding Class)

Syntax transmit-weight (cells number | percent number);

Hierarchy Level [edit interfaces interface-name atm-options scheduler-maps map-name forwarding-class class-name]

Description For ATM 2 interfaces only, assign a transmission weight to a forwarding class.

Default 95 percent for queue 0, 5 percent for queue 3.

Options percent percent—Transmission weight of the forwarding class is a percentage of the total bandwidth.

Range: 5 through 100

cells number—Transmission weight of the forwarding class is in number of cells.

Range: 0 through 32,000


Required Privilege Level interface—to view this statement in the configuration.

interface-control—to add this statement to the configuration.
**traps**

**Syntax**
(traps | no-traps);

**Hierarchy Level**
[edit interfaces interface-name],
[edit interfaces interface-name unit logical-unit-number]

**Description**
Enable or disable the sending of SNMP notifications when the state of the connection changes.

**Usage Guidelines**
See “Enable or Disable SNMP Notifications on Physical Interfaces” on page 65 and “Enable or Disable SNMP Notifications on Logical Interfaces” on page 74.

**Required Privilege Level**
interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**ttl**

**Syntax**
ttl value;

**Hierarchy Level**
[edit interfaces interface-name unit number tunnel]

**Description**
Set the time-to-live value bit in the header of the outer IP packet.

**Options**
value—Time-to-live value.
  Range: 0 through 255
  Default: 64

**Usage Guidelines**
See “Configure Tunnel Interfaces” on page 407.

**Required Privilege Level**
interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.
**tunnel**

**Syntax**
```
tunnel {
    backup-destination destination-address;
    destination destination-address;
    routing-instance {
        destination routing-instance-name;
    }
    source source-address;
    ttl number;
}
```

**Hierarchy Level**
```
[edit interfaces interface-name unit logical-unit-number]
```

**Description**
Configure a tunnel. You can use the tunnel for unicast and multicast traffic or just for multicast traffic. You can also use tunnels for encrypted traffic or VPNs.

The statements are explained separately.

**Usage Guidelines**
See “Configure Encryption Interfaces” on page 257 and “Configure Tunnel Interfaces” on page 407.

**Required Privilege Level**
- `interface`—To view this statement in the configuration.
- `interface-control`—To add this statement to the configuration.

**See Also**
multicasts-only on page 501 or JUNOS Internet Software Configuration Guide: VPNs.
unit

Syntax  unit logical-unit-number {  
disable;  
accept-source-mac {  
  mac-address mac-address {  
    policer {  
      input policer-name;  
      output policer-name;  
    }  
  }  
}  
accounting-profile name;  
allow-any-vci;  
description text;  
dlci dlci-identifier;  
drop-timeout milliseconds;  
encapsulation type;  
fragment-threshold bytes;  
input-vlan-map {  
  pop;  
  push;  
  swap;  
  vlan-id number;  
  tag-protocol-id tpid;  
}  
interleave-fragments;  
inverse-arp;  
mrru bytes;  
multicast-dlci dlci-identifier;  
multicast-vci vpi-identifier.vci-identifier;  
multipoint;  
oam-liveness {  
  up-count cells;  
  down-count cells;  
}  
oam-period (disable | seconds);  
output-vlan-map {  
  pop;  
  push;  
  swap;  
  vlan-id number;  
  tag-protocol-id tpid;  
}  
point-to-point;  
service-domain (inside | outside);  
shaping {  
  (cbr rate | rtvbr peak rate sustained rate burst length |  
    vbr peak rate sustained rate burst length);  
  queue-length number;  
}  
short-sequence;  
transmit-weight number;  
(traps | no-traps);
tunnel {
    backup-destination destination-address;
    destination destination-address;
    routing-instance {
        destination routing-instance-name;
    }
    source source-address;
    ttl number;
}

vci vpi-identifier.vci-identifier(
}

vlan-id number;
vlan-tag [ tpid.vlan-id ];

family family {
    bundle (ml-fpc/pic/port | ls-fpc/pic/port);
    destination-class-usage;
    filter {
        input filter-name;
        output filter-name;
        group filter-group-number;
    }

    ipsec-sa sa-name;
    mtu bytes;
    multicasts-only;
    no-redirects:
    post-service-filter {
        input filter-name;
        output filter-name;
    }

    primary;
    service {
        input {
            [ service-set service-set-name <service-filter filter-name> ];
            post-service-filter filter-name;
        }
        output {
            [ service-set service-set-name <service-filter filter-name> ];
        }
    }

    address address {
        arp ip-address (mac | multicast-mac) mac-address <publish>;
        destination destination-address;
        eui-64;
        broadcast address;
        multipoint-destination destination-address dlc dlci-identifier;
        multipoint-destination destination-address {
            epd-threshold cells;
            inverse-arp;
            oam-liveness {
                up-count cells;
                down-count cells;
            }

            oam-period seconds;
        }
    }
}
shaping {
  (cbr rate | rtvbr peak rate sustained rate burst length | vbr peak rate sustained rate burst length);
  queue-length number;
}

vci vpi-identifier:vci-identifier;

preferred;
primary;

vrp-group group-number {
  virtual-address [addresses];
  priority number;
  (accept-data | no-accept-data);
  advertise-interval seconds;
  authentication-type authentication;
  authentication-key key;
  (preempt | no-preempt);
  track {
    interface interface-name priority-cost cost;
  }
}

Hierarchy Level [edit interfaces interface-name]
Description Configure a logical interface on the physical device. You must configure a logical interface to be able to use the physical device.
Options logical-unit-number—Number of the logical unit.
Range: 0 through 16384
The remaining statements are explained separately.
Usage Guidelines See “Configure Logical Interface Properties” on page 67 or “Configure Service Interface Properties” on page 112.
Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.
vbr

Syntax  

vbr peak rate sustained rate burst length;

Hierarchy Level  

[edit interfaces interface-name unit logical-unit-number shaping],
[edit interfaces interface-name unit logical-unit-number address address family family
multipoint-destination destination-address shaping],
[edit interfaces interface-name atm-options vpi vpi-identifier shaping]

Description  

For ATM encapsulation only, define the variable bandwidth utilization in the traffic-shaping profile.

When you configure the variable bandwidth utilization, you must specify all three options (burst, peak, and sustained). You can specify rate in bits per second either as a complete decimal number or as a decimal number followed by the abbreviation k (1000), m (1,000,000), or g (1,000,000,000). You can also specify rate in cells per second by entering a decimal number followed by the abbreviation c; values expressed in cells per second are converted to bits per second by means of the formula 1 cps = 384 bps.

Default  

Unspecified bit rate (UBR); that is, bandwidth utilization is unlimited.

Options  

burst length—Burst length, in cells. If you set the length to 1, the peak traffic rate is used.
  Range: 1 through 4000 cells

peak rate—Peak rate, in bps or cps.
  Range: 33 kbps through 135.6 Mbps (ATM OC-3); 33 kbps through 276 Mbps (ATM OC-12)

sustained rate—Sustained rate, in bps or cps.
  Range: 33 kbps through 135.6 Mbps (ATM OC-3); 33 kbps through 276 Mbps (ATM OC-12)

Usage Guidelines  

See “Define the ATM 1 and ATM 2 Traffic-Shaping Profile” on page 137.

Required Privilege Level  

interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

See Also  

cbr on page 440, rtvbr on page 533, shaping on page 539
vc-cos-mode

Syntax

vc-cos-mode (alternate | strict);

Hierarchy Level
[edit interfaces interface-name atm-options scheduler-maps map-name]

Description
For ATM 2 interfaces only, specify packet-scheduling priority value for ATM 2 VC tunnels.

Options
alternate—VC CoS queue has high priority. The scheduling of the queues alternates between the high-priority queue and the remaining queues, so every other scheduled packet is from the high-priority queue.

strict—VC CoS queue has strictly high priority. A queue with strict high priority is always scheduled before the remaining queues. The remaining queues are scheduled in round-robin fashion.

Default: alternate

Usage Guidelines
See “Configure ATM 2 VC Tunnel CoS Components” on page 155.

Required Privilege Level
interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

vci

Syntax

vci vpi-identifier.vci-identifier;

Hierarchy Level
[edit interfaces interface-name unit logical-unit-number],
[edit interfaces interface-name unit logical-unit-number family family address address multipoint-destination address]

Description
For ATM point-to-point logical interfaces only, configure the virtual circuit identifier (VCI) and virtual path identifier (VPI).

To configure a VPI for a point-to-multipoint interface, specify the VPI in the multipoint-destination statement.

VCIs 0 through 31 are reserved for specific ATM values designated by the ATM Forum.

Options
vci-identifier—ATM virtual circuit identifier. Unless you configure the interface to use promiscuous mode, this value cannot exceed the largest numbered VC configured for the interface with the maximum-vcs option of the vpi statement.
Range: 0 through 4089 or 0 through 65,535 with promiscuous mode, with VCIs 0 through 31 reserved.

vpi-identifier—ATM virtual path identifier.
Range: 0 through 255
Default: 0

Usage Guidelines
See “Configure a Point-to-Point ATM 1 or ATM 2 Connection” on page 136.

Required Privilege Level
interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

See Also
multipoint-destination on page 502, promiscuous-mode on page 525, vpi on page 568
virtual-address

Syntax  virtual-address [addresses];

Hierarchy Level  [edit interfaces interface-name unit logical-unit-number family inet address address
vrrp-group group-number]

Description  When you are configuring VRRP on Fast Ethernet and Gigabit Ethernet interfaces only,
configure the addresses of the virtual routers in a VRRP group. You can configure up to eight
addresses.

Options  addresses—Addresses of one or more virtual routers. Do not include a prefix length. If the
address is the same as the interface’s physical address, the interface becomes the
master virtual router for the group.

Usage Guidelines  See “Configure Basic VRRP Support” on page 291.

Required Privilege Level  interface—to view this statement in the configuration.
interface-control—to add this statement to the configuration.

vlan-id

vlan-id (VLAN ID to be bound to a logical interface)

Syntax  vlan-id number;

Hierarchy Level  [edit interfaces interface-name unit logical-unit-number]

Description  For Fast Ethernet and Gigabit Ethernet interfaces only, binds a 802.1Q VLAN tag ID to a
logical interface.

Options  number—a valid VLAN identifier.
  Range: For aggregated Ethernet, 4-port, 8-port, and 12-port Fast Ethernet PICs, and for
management and internal Ethernet interfaces, 1 through 1023.
  For 48-port Fast Ethernet and Gigabit Ethernet PICs, 1 through 4094.
  VLAN ID 0 is reserved for tagging the priority of frames.

Usage Guidelines  See “Configure 802.1Q VLANs” on page 282.

Required Privilege Level  interface—to view this statement in the configuration.
interface-control—to add this statement to the configuration.
**vlan-id (VLAN ID to rewrite)**

**Syntax**

```
vlan-id number;
```

**Hierarchy Level**

```
[edit interfaces interface-name unit logical-unit-number input-vlan-map],
[edit interfaces interface-name unit logical-unit-number output-vlan-map]
```

**Description**

For Gigabit Ethernet QPP interfaces only, specify the line VLAN identifiers to be rewritten at the input or output interface.

You cannot include both the the swap statement and the vlan-id statement at the [edit interfaces interface-name unit logical-unit-number output-vlan-map] hierarchy level. If you include the swap statement in the output VLAN map, the VLAN ID in the outgoing frame is rewritten to the vlan-id statement you include at the [edit interfaces interface-name unit logical-unit-number] hierarchy level.

**Usage Guidelines**

See “Stack and Rewrite Gigabit Ethernet QPP VLAN Tags” on page 273.

**Required Privilege Level**

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

---

**vlan-tag**

**Syntax**

```
vlan-tag [tpid vlan-id ];
```

**Hierarchy Level**

```
[edit interfaces interface-name unit logical-unit-number]
```

**Description**

For Gigabit Ethernet QPP interfaces only, binds TPIDs and 802.1Q VLAN tag IDs to a logical interface.

**Options**

tpid.vlan-id—A TPID and a valid VLAN identifier. Configure the outer tag first, then the inner tag.

Range: If you include the stacked-vlan-tagging statement in the configuration, you can include up to two TPID VLAN ID pairs. The outer tag VLAN ID range is 1 through 511 for normal interfaces, and 512 and above for VLAN CCC interfaces. The inner tag does not have this restriction.

**Usage Guidelines**

See “Stack and Rewrite Gigabit Ethernet QPP VLAN Tags” on page 273.

**Required Privilege Level**

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

**See Also**

stacked-vlan-tagging on page 544
**vlan-tagging**

**Syntax**
```
vlan-tagging;
```

**Hierarchy Level**
```
[edit interfaces interface-name]
```

**Description**
For Fast Ethernet and Gigabit Ethernet interfaces only, enables the reception and transmission of 802.1Q VLAN-tagged frames on the interface.

**Usage Guidelines**
See “Configure 802.1Q VLANs” on page 282.

**Required Privilege Level**
- interface—to view this statement in the configuration.
- interface-control—to add this statement to the configuration.

---

**vpi**

**Syntax**
```
vpi vpi-identifier { 
  maximum-vcs maximum-vcs;
  oam-liveness {
    up-count cells;
    down-count cells;
  } 
  oam-period (disable | seconds);
  shaping {
    (cbr rate | rtvbr peak rate sustained rate burst length | vbr peak rate sustained rate burst length);
    queue-length number;
  }
}
```

**Hierarchy Level**
```
[edit interfaces interface-name atm-options]
```

**Description**
For ATM interfaces, configure the virtual path (VP).

**Options**
- **vpi-identifier**—ATM virtual path identifier. This is one of the VPIs that you define in the vci statement.
  - Range: 0 through 255

  The remaining statements are explained separately.

**Usage Guidelines**
See “Configure ATM 1 and ATM 2 Physical Interface Properties” on page 125.

**Required Privilege Level**
- interface—to view this statement in the configuration.
- interface-control—to add this statement to the configuration.

**See Also**
- multipoint-destination on page 502, promiscuous-mode on page 525, vci on page 565
vrrp-group

Syntax

vrrp-group group-number {
    virtual-address [addresses];
    priority number;
    (accept-data | no-accept-data);
    advertise-interval seconds;
    authentication-type authentication;
    authentication-key key;
    (preempt | no-preempt);
    track {
        interface interface-name priority-cost cost;
    }
}

Hierarchy Level  [edit interfaces interface-name unit logical-unit-number family inet address address]

Description  For Fast Ethernet and Gigabit Ethernet interfaces only, configure a VRRP group. On a single router, you cannot configure the same VRRP group on multiple interfaces.

Options  group-number—VRRP group identifier. If you enable MAC source address filtering on the interface, as described in “Configure Ethernet MAC Address Filtering” on page 279, you must include the virtual MAC address in the list of source MAC addresses that you specify in the source-address-filter statement. MAC addresses ranging from 00:00:5e:00:01:00 through 00:00:5e:00:01:ff are reserved for VRRP, as defined in RFC 2338. The VRRP group number must be the decimal equivalent of the last hexadecimal byte of the virtual MAC address.

Range: 0 through 255

The remaining statements are explained separately.

Usage Guidelines  See “Configure VRRP” on page 290.

Required Privilege Level  interface—to view this statement in the configuration.

interface-control—to add this statement to the configuration.
vtmapping

Syntax  vtmapping (itu-t | klm);

Hierarchy Level  [edit interfaces interface-name sonet-options]

Description  For the Channelized STM-1 PIC with QPP only, configure virtual tributary mapping.

For the Channelized STM-1 PIC, you configure virtual tributary mapping at the [edit chassis fpc number pic number] hierarchy level.

Options  itu-t—International Telephony Union standard

klm—KLM standard

Default: klm

Usage Guidelines  See “Configure Virtual Tributary Mapping of Channelized STM-1 QPP Interface” on page 211.

Required Privilege Level  interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

See Also  JUNOS Internet Software Configuration Guide: Getting Started.

working-circuit

Syntax  working-circuit group-name;

Hierarchy Level  [edit interfaces interface-name sonet-options aps]

Description  Configure the working router in an APS circuit pair.

Options  group-name—Circuit’s group name.

Usage Guidelines  See “Configure Basic APS Support” on page 368.

Required Privilege Level  interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

See Also  protect-circuit on page 526
yellow-differential-delay

Syntax: yellow-differential-delay milliseconds;

Hierarchy Level: [edit interfaces ls-fpc/pic/port:channel mfr-uni-nni-bundle-options]

Description: For link services interfaces only, configure the yellow differential delay among bundle links to give warning when a link has a differential delay that exceeds the configured threshold.

Options: milliseconds — Yellow differential delay threshold.
  Range: 1 through 2000 milliseconds
  Default: 6 milliseconds


Required Privilege Level: interface—To view this statement in the configuration.
  interface-control—To add this statement to the configuration.

See Also: action-red-differential-delay on page 421, remote on page 530

z0-increment

Syntax: (z0-increment | no-z0-increment);

Hierarchy Level: [edit interfaces interface-name sonet-options]

Description: Configure an incrementing STM ID rather than a static one.

Usage Guidelines: See “Configure an Incrementing STM ID” on page 362.

Required Privilege Level: interface—To view this statement in the configuration.
  interface-control—To add this statement to the configuration.

See Also: sonet-options on page 540
Part 4

CoS

- CoS Overview on page 575
- CoS Configuration Guidelines on page 585
- Summary of CoS Configuration Statements on page 623
Chapter 32
CoS Overview

For interfaces that carry IPv4, IPv6, or MPLS traffic, you can configure JUNOS class-of-service (CoS) features to provide multiple classes of service for different applications. On the router, you can configure multiple forwarding classes for transmitting packets, define which packets are placed into each output queue, schedule the transmission service level for each queue, and manage congestion using a Random Early Detection (RED) algorithm.

The JUNOS CoS features are not supported on ATM interfaces. ATM has traffic-shaping capabilities that would override CoS, because ATM traffic shaping is performed at the ATM layer and CoS is performed at the IP layer. For more information about ATM traffic shaping, see “Define the ATM 1 and ATM 2 Traffic-Shaping Profile” on page 137 and “Configure ATM 2 VC Tunnel CoS Components” on page 155.

The JUNOS CoS features provide a set of mechanisms that you can use to provide differentiated services when best-effort traffic delivery is insufficient. In designing CoS applications, you must give careful consideration to your service needs, and you must thoroughly plan and design your CoS configuration to ensure consistency across all routers in a CoS domain. You must also consider all the routers and other networking equipment in the CoS domain to ensure interoperability among all equipment.

The Internet community has little experience with CoS and quality of service (QoS). However, because Juniper Networks routers implement CoS in hardware rather than in software, you can experiment with and deploy CoS features without adversely affecting packet forwarding and routing performance.

The standards are defined in the following RFCs:

- RFC 2474, Definition of the Differentiated Services Field in the IPv4 and IPv6 Headers
- RFC 2598, An Expedited Forwarding PHB
- RFC 2597, Assured Forwarding PHB Group
This chapter discusses the following topics:

- CoS Applications on page 576
- JUNOS CoS Components on page 577
- Hardware Capabilities and Limitations on page 583

For information about CoS components that you apply to the ATM 2 interface specifically, see “Configure ATM 2 VC Tunnel CoS Components” on page 155.

CoS Applications

CoS mechanisms are useful for two broad classes of applications. These applications can be referred to as in the box and across the network.

In-the-box applications use CoS mechanisms to provide special treatment for packets passing through a single node on the network. You can monitor the incoming traffic on each interface, using CoS to provide preferred service to some interfaces (that is, to some customers) while limiting the service provided to other interfaces. You can also filter outgoing traffic by the packet’s destination, thus providing preferred service to some destinations.

Across-the-network applications use CoS mechanisms to provide differentiated treatment to different classes of packets across a set of nodes in a network. In these types of applications, you typically control the ingress and egress routers to a routing domain and all the routers within the domain. You can use JUNOS CoS features to modify packets traveling through the domain to indicate the packet’s priority across the domain. Specifically, you modify the precedence bits in the IPv4 type-of-service (ToS) field, remapping these bits to values that correspond to levels of service. When all routers in the domain are configured to associate the precedence bits with specific service levels, packets traveling across the domain receive the same level of service from the ingress point to the egress point. For CoS to work in this case, the mapping between the precedence bits and service levels must be identical across all routers in the domain.

JUNOS CoS applications support the following range of mechanisms:

- Differentiated Services—The CoS application supports DiffServ as well as six-bit IP header ToS byte settings. The configuration uses DiffServ Code Points (DSCPs) in the IP ToS field to determine the forwarding class associated with each packet.

- Layer 2 to Layer 3 CoS Mapping—The CoS application supports mapping of Layer 2 (IEEE 802.1p) packet headers to router forwarding class and loss-priority values.

Layer 2 to Layer 3 CoS mapping involves setting the forwarding class and loss priority based on information in the Layer 2 header. Output involves mapping the forwarding class and loss priority to a Layer 2-specific marking. You can mark the Layer 2 and Layer 3 headers simultaneously.

- MPLS EXP—Supports configuration of mapping of MPLS experimental (EXP) bit settings to router forwarding classes and vice versa.

- VPN Outer-Label Marking—Supports setting of outer-label EXP bits, also known as CoS bits, based on MPLS EXP mapping.
JUNOS CoS Components

You can configure CoS features to meet your application needs. Because the components are generic, you can use a single CoS configuration syntax across multiple platforms. The JUNOS CoS features include:

- **Classifiers**—Allow you to associate incoming packets with a forwarding class and loss priority and, based on the associated forwarding class, assign packets to output queues. Two general types of classifiers are supported:
  - **Behavior aggregate (BA) or code point traffic classifiers**—Code points determine each packet’s forwarding class and loss priority. BA classifiers allow you to set the forwarding class and loss priority of a packet based on DiffServ code point (DSCP) bits, IP precedence bits, MPLS EXP bits, and IEEE 802.1p bits. The default classifier is based on IP precedence bits.
  - **Multifield (MF) traffic classifiers**—Allow you to set the forwarding class and loss priority of a packet based on firewall filter rules. For more information about configuring MF classifiers, see the JUNOS Internet Software Configuration Guide: Policy Framework.

- **Forwarding classes**—Also known as ordered aggregates in the IETF’s DiffServ architecture. Affect the forwarding, scheduling, and marking policies applied to packets as they transit a router. Four forwarding classes are supported: best effort, assured forwarding, expedited forwarding, and network control. The forwarding class plus the loss priority define the per-hop behavior.

- **Loss priorities**—Allow you to set the priority of dropping a packet. Typically you mark packets exceeding some service level with a high loss priority. Loss priority affects the scheduling of a packet without affecting the packet’s relative ordering. You set loss priority by configuring a classifier or a policer.

- **Forwarding policy options**—Allow you to associate forwarding classes with next hops. Forwarding policy also allows you to create classification overrides, which assign forwarding classes to sets of prefixes.

- **Transmission scheduling and rate control**—Provide you with a variety of tools to manage traffic flows:
  - **Schedulers**—Allow you to define the priority, bandwidth, delay buffer size, rate control status, and RED drop profiles to be applied to a particular forwarding class for packet transmission.
  - **Fabric schedulers**—For T-series platforms only, fabric schedulers allow you to identify a packet as high or low priority based on its forwarding class, and to associate schedulers with the fabric priorities.
  - **Policers for traffic classes**—Allow you to limit traffic of a certain class to a specified bandwidth and burst size. Packets exceeding the policer limits can be discarded, or can be assigned to a different forwarding class or to a different loss priority, or to both. You define policers with filters that can be associated with input or output interfaces. For information about configuring policers, see the JUNOS Internet Software Configuration Guide: Policy Framework.
  - **Rewrite markers**—Allow you to redefine the code-point value of outgoing packets. Rewriting or marking outbound packets is useful when the router is at the border of a network and must alter the code points to meet the policies of the targeted peer.
Figure 30 shows the components of the JUNOS CoS features, illustrating the sequence in which they interact.

The JUNOS CoS components are discussed in the following sections:

- Traffic Classifiers on page 578
- Forwarding Classes on page 580
- Transmission Scheduling and Rate Control on page 581
- Rewrite Markers on page 583

Traffic Classifiers

By default, all logical interfaces are assigned an IP precedence classifier for incoming IP packets.

At the core router, the JUNOS software matches the classifier to a code point to determine each packet’s forwarding class and loss priority. This classifier is called the behavior aggregate (BA) classifier. Supported code points include the DiffServ Code Point (DSCP) for IP DiffServ, IP precedence bits, MPLS EXP bits, and IEEE 802.1p CoS bits.

In an edge router, a multifield (MF) classifier provides the filtering functionality that scans through a variety of packet fields to determine the forwarding class for a packet. Typically, a classifier performs matching operations on the selected fields against a configured value.

Only four classes can forward traffic independently. Therefore, you must configure additional classes to be aggregated into one of these classes. You use the BA classifier to configure class aggregation. For more information, see “Forwarding Classes” on page 580.
The following sections discuss classifiers in more detail:

- Default Classifier on page 579
- Behavior Aggregate Classifier on page 579
- Multifield Classifier on page 580

**Default Classifier**

When you install a classifier, it becomes effective on any interface for which you configure it.

By default, all logical interfaces are assigned an IP precedence classifier. The default IP precedence classifier maps IP precedence bits to forwarding classes and loss priorities as shown in Table 32.

Table 32: Default IP Precedence Classifier

<table>
<thead>
<tr>
<th>IP Precedence Code Point</th>
<th>Forwarding Class</th>
<th>Loss Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>000</td>
<td>best-effort</td>
<td>low</td>
</tr>
<tr>
<td>001</td>
<td>best-effort</td>
<td>high</td>
</tr>
<tr>
<td>010</td>
<td>best-effort</td>
<td>low</td>
</tr>
<tr>
<td>011</td>
<td>best-effort</td>
<td>high</td>
</tr>
<tr>
<td>100</td>
<td>best-effort</td>
<td>low</td>
</tr>
<tr>
<td>101</td>
<td>best-effort</td>
<td>high</td>
</tr>
<tr>
<td>110</td>
<td>network-control</td>
<td>low</td>
</tr>
<tr>
<td>111</td>
<td>network-control</td>
<td>high</td>
</tr>
</tbody>
</table>

**Behavior Aggregate Classifier**

A behavior aggregate classifier uses IP DSCPs, IP precedence bits, the MPLS EXP field, or Layer 2 CoS indication (IEEE 802.1p) to determine the forwarding treatment for each packet, called a per-hop behavior (PHB). A PHB defines how a particular router in a DiffServ domain treats a packet. A BA classifier can aggregate multiple DiffServ PHBs into a single one if the router cannot support multiple simultaneous PHBs.

The BA classifier maps a code point to a loss priority. The loss priority is used later in the work flow to select one of the two drop profiles employed by RED.

Decoding the EXP header field can also determine the packet loss priority (PLP) status.

For a specified interface, you can configure both an MF classifier and a BA classifier without conflicts. Because the classifiers are always applied in sequential order, the BA classifier followed by the MF classifier, any BA classification result is overridden by an MF classifier if they conflict.

For information about configuring BA classifiers, see “Classify Packets by Behavior Aggregate” on page 594 and “Example: Configure Class of Service” on page 617.
**Multifield Classifier**

A multifield classifier examines one or more packet fields to determine the forwarding treatment that a packet receives. An MF classifier typically matches one or more of the six packet header fields: destination address, source address, IP protocol, source port, destination port, and DSCP. MF classifiers are used when a simple BA classifier is insufficient to classify a packet.

From a CoS perspective, MF classifiers (or firewall filter rules) provide the following services:

- Classify packets to a forwarding class and loss priority.
- Police traffic to a specific bandwidth and burst size. Packets exceeding the policer limits can be discarded, or can be assigned to a different forwarding class or to a different loss priority, or to both.

To activate an MF classifier, you must configure it on a logical interface. There is no restriction on the number of MF classifiers you can configure.

For information about configuring MF classifiers, see the JUNOS Internet Software Configuration Guide: Policy Framework.

**Forwarding Classes**

For a classifier to assign an output queue to each packet, it must associate the packet with one of the following forwarding classes:

- Expedited Forwarding (EF)—Provides a low loss, low latency, low jitter, assured bandwidth, end-to-end service.
- Assured Forwarding (AF)—Provides a group of values you can define and includes four subclasses, AF1, AF2, AF3, and AF4, each with three drop probabilities, low, medium, and high.
- Best Effort (BE)—Provides no service profile. For the BE forwarding class, loss priority is typically not carried in a code point and RED drop profiles are more aggressive.
- Network Control (NC)—The NC forwarding class is typically low priority because it is adaptive.

For each forwarding class, you can configure high or low loss priority. By default, the loss priority is low. For information about configuring forwarding classes, see “Configure Forwarding Classes” on page 592 and “Example: Configure Class of Service” on page 617.
Transmission Scheduling and Rate Control

You use schedulers to configure transmission scheduling and rate control parameters. Schedulers define the priority, bandwidth, delay buffer size, rate control status, and RED drop profiles to be applied to a particular class of traffic.

You associate the schedulers with forwarding classes by means of scheduler maps. You can then associate each scheduler map with an interface, thereby configuring the hardware queues, packet schedulers, and RED processes that operate according to this mapping.

The following sections describe these processes in more detail:

- Scheduling Priority on page 581
- Fabric Priority Queuing on page 582
- Transmission Rate Control on page 582
- Allocation of Leftover Bandwidth on page 582
- Default Congestion and Transmission Control on page 582
- RED Congestion Control on page 583

Scheduling Priority

The scheduling priority determines the order of transmission from the forwarding classes associated with an output interface. Three levels of transmission priority are currently supported: low, high, and strictly high.

High-priority forwarding classes transmit packets ahead of low-priority forwarding classes as long as the forwarding class retains enough bandwidth credit. When you configure a high-priority forwarding class with a significant fraction of the transmission bandwidth, the forwarding class might lock out low-priority traffic.

Strictly high-priority forwarding classes receive precedence over low-priority forwarding classes as long as the forwarding class has traffic waiting to be sent, irrespective of bandwidth credit. We recommend that you do not configure strictly high and high transmission priorities on a single interface, unless the interface sends network-control traffic with a need for 5 percent of the transmission bandwidth.

Strictly high-priority forwarding classes supersede bandwidth guarantees for low-priority forwarding classes; therefore, we recommend that you use this feature to ensure proper ordering of special traffic, such as voice traffic. You can preserve bandwidth guarantees for low-priority forwarding classes by allocating to the strictly high-priority forwarding class only the amount of bandwidth that you generally require for that forwarding class. For example, consider the following allocation of transmission bandwidth:

- Q0 BE—20 percent, low priority
- Q1 EF—30 percent, strictly high priority
- Q2 AF—40 percent, low priority
- Q3 NC—10 percent, low priority
This allocation of bandwidth assumes that, in general, the EF forwarding class requires only 30 percent of an interface’s transmission bandwidth. However, if short bursts of traffic are received on the EF forwarding class, 100 percent of the bandwidth is given to the EF forwarding class by way of the strictly high-priority setting.

For information about configuring scheduling priority, see “Configure Scheduling Policy Maps” on page 596 and “Example: Configure Class of Service” on page 617.

**Fabric Priority Queuing**

On T-series platforms, the default behavior is for fabric priority queuing on egress interfaces to match the scheduling priority you assign. High-priority egress traffic is automatically assigned to high-priority fabric queues. Likewise, low-priority egress traffic is automatically assigned to low-priority fabric queues.

For information about overriding automatic fabric priority queuing, see “Override Fabric Priority Queuing” on page 594 and “Associate a Scheduler with a Fabric Priority” on page 600.

**Transmission Rate Control**

The transmission rate control determines the actual traffic bandwidth from each of the forwarding classes you configure. The rate is specified in bits per second. You can limit the transmission bandwidth to the exact value you configure, or allow it to exceed the configured rate if additional bandwidth is available from other queues.

For information about configuring transmission rate control, see “Configure Scheduling Policy Maps” on page 596.

**Allocation of Leftover Bandwidth**

When a forwarding class fails to fully use the allocated transmission bandwidth, the remaining bandwidth can be taken by other forwarding classes if they receive a larger amount of offered load than the bandwidth allocated. This use of leftover bandwidth is the default behavior. If you want a forwarding class to not take any extra bandwidth, you must configure it for strict allocation. With rate control in place, the specified bandwidth is strictly observed.

When you configure more than one forwarding class to use leftover bandwidth, the high-priority forwarding class takes the bandwidth first. Forwarding classes with equal priority share the bandwidth through round robin.

For information about configuring leftover bandwidth allocation, see “Configure Scheduling Policy Maps” on page 596.

**Default Congestion and Transmission Control**

A default congestion and transmission control mechanism is needed when an output interface is not configured for a certain forwarding class, but receives packets destined for that unconfigured forwarding class. This default mechanism uses the delay buffer and WRR credit allocated to the designated forwarding class, with a default drop profile. Because the buffer and WRR credit allocation is minimal, packets might be lost if a larger number of packets are forwarded without configuring the forwarding class for the interface.
**RED Congestion Control**

You can configure two parameters to control congestion at the output stage. The first parameter defines the delay-buffer bandwidth, which provides packet buffer space to absorb burst traffic up to the specified duration of delay. Once the specified delay buffer becomes full, packets with 100 percent drop probability are dropped from the head of the buffer.

The second parameter defines the drop probabilities across the range of delay-buffer occupancy, supporting the RED process. Depending on the drop probabilities, RED might drop packets aggressively long before the buffer becomes full, or it might drop only a few packets even if the buffer is almost full.

You specify the delay-buffer size for each scheduler associated with an output interface configuration in temporal units of 1 through 200,000 microseconds, or as a percentage of the entire interface buffer space. You specify drop probabilities in the drop profile section of the CoS configuration hierarchy and reference them in each scheduler configuration. For each scheduler, you can configure four separate drop profiles, one for each combination of loss priority (low or high) and IP transport protocol (TCP or non-TCP).

You can configure a maximum of 32 different drop profiles.

For information about configuring delay buffers and drop profiles, see “Configure Scheduling Policy Maps” on page 596 and “Configure RED Drop Profiles” on page 601.

**Rewrite Markers**

A marker reads the current forwarding class and loss priority information associated with a packet and finds the chosen code point from a table. It then writes the code point information into the packet header. Entries in a marker configuration represent the mapping of the current forwarding class into a new forwarding class, to be written into the header.

You define markers in the rewrite rules section of the CoS configuration hierarchy and reference them in the logical interface configuration. When an interface is not associated with any marker, the code point is not rewritten; instead, the old marking information is preserved.

This model supports marking on the DSCP, IP Precedence, and MPLS EXP bits CoS indications.

For information about configuring rewrite markers, see “Rewrite Packet Header Information” on page 602 and “Example: Configure Class of Service” on page 617.

**Hardware Capabilities and Limitations**

Juniper Networks T-series platforms and M-series platforms with an enhanced FPC have more CoS capabilities than the M-series platforms that employ the earlier FPC model. Table 33 on page 588 lists the differences between the FPC and the enhanced FPC.
To configure CoS properties, you can include the following statements at the [edit class-of-service] hierarchy level of the configuration:

class-of-service {
    classifiers {
        type classifier-name {
            import (classifier-name | default);
            forwarding-class class-name {
                loss-priority (low | high) code-points [ alias | bits ];
            }
        }
    }
    code-point-aliases {
        (dscp | exp | ieee-802.1 | inet-precedence) {
            alias-name bits;
        }
    }
    drop-profiles {
        profile-name {
            fill-level percentage drop-probability percentage;
            interpolate {
                drop-probability value;
                fill-level value;
            }
        }
    }
    fabric {
        scheduler-map {
            priority (low | high) scheduler scheduler-name;
        }
    }
    forwarding-classes {
        queue queue-number class-name priority (low | high);
    }
    forwarding-policy {
        next-hop-map map-name {
            forwarding-class class-name {
                next-hop [ next-hop-name ];
                lsp-next-hop [ lsp-regular-expression ];
            }
        }
    }
}
class class-name {
    classification-override {
        forwarding-class class-name;
    }
}

interfaces {
    interface-name {
        scheduler-map map-name;
        unit logical-unit-number {
            bandwidth rate;
            classifiers {
                (dscp | exp | ieee-802.1 | inet-precedence) (classifier-name | default);
            }
            forwarding-class class-name;
            per-unit-scheduler;
            rewrite-rules {
                dscp (rewrite-name | default);
                exp (rewrite-name | default) protocol protocol-types;
                exp-push-push-push default;
                exp-swap-push-push default;
                ieee-802.1 default;
                inet-precedence (rewrite-name | default);
            }
            scheduler-map map-name;
        }
    }
}

rewrite-rules {
    (dscp | exp | inet-precedence) rewrite-name {
        import (rewrite-name | default);
        forwarding-class class-name {
            loss-priority (low | high) code-point (alias | bits);
        }
    }
}

scheduler-maps {
    map-name {
        forwarding-class class-name scheduler scheduler-name;
    }
}

schedulers {
    scheduler-name {
        buffer-size (percent percentage | remainder | temporal microseconds);
        drop-profile-map loss-priority (low | high) protocol (non-tcp | tcp | any)
        drop-profile profile-name;
        priority (low | high | strict-high);
        transmit-rate (rate | percent percentage | remainder | exact);
    }
}

The following RFCs define the standards supported by certain aspects of the CoS software:

- RFC 2474, Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers
- RFC 2598, An Expedited Forwarding PHB (see also draft-ietf-diffserv-rfc2598bis-01.txt)
- RFC 2597, Assured Forwarding PHB Group

RFC 2983, Diffserv and Tunnels, is not supported.

The JUNOS software supports only two loss priorities and, by default, supports only one assured forwarding (AF) class, although you can configure more at the expense of other class types.

This chapter includes the following sections:

- Hardware Capabilities and Limitations on page 588
- Define Code-Point Aliases on page 589
- Configure Forwarding Classes on page 592
- Classify Packets by Behavior Aggregate on page 594
- Configure Scheduling Policy Maps on page 596
- Configure RED Drop Profiles on page 601
- Rewrite Packet Header Information on page 602
- Configure CoS-Based Forwarding on page 610
- Example: Configure Class of Service on page 617
Hardware Capabilities and Limitations

Juniper Networks T-series platforms and M-series platforms with an enhanced FPC have more CoS capabilities than the M-series platforms that employ the earlier FPC model. Table 33 lists the differences between the FPC and the enhanced FPC.

Table 33: CoS Hardware Capabilities and Limitations

<table>
<thead>
<tr>
<th>Feature</th>
<th>M-series FPC</th>
<th>M-series Enhanced FPC</th>
<th>T-series FPC</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Classifiers</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Limit per FPC or PIC</td>
<td>1</td>
<td>8</td>
<td>64</td>
<td>For M-series FPC, the one-classifier limit includes the default IP precedence classifier. If you create a new classifier and apply it to an interface, the new classifier does not override the default classifier for other interfaces on the same FPC. The general rule for classifier replacement is that the first classifier associated with a logical interface is the one that is used. The default classifier can be replaced only when a single interface is associated with the default classifier.</td>
</tr>
<tr>
<td>dscp</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>For M-series FPC and T-series FPC, the loss priority cannot be arbitrarily decoded from the code point.</td>
</tr>
<tr>
<td>ieee-802.1p</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td></td>
</tr>
<tr>
<td>inet-precedence</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>For M-series FPC and T-series FPC, the loss priority cannot be arbitrarily decoded from the code point.</td>
</tr>
<tr>
<td>mpls-exp</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>For M-series FPC, only the default MPLS EXP classifier is supported; the default MPLS EXP classifier takes the EXP bits 1 and 2 as the output queue number.</td>
</tr>
<tr>
<td>Rewrite Markers</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Limit per FPC or PIC</td>
<td>none</td>
<td>none</td>
<td>64</td>
<td>For T-series FPC, you must decode the loss priority using the firewall filter before you can use loss priority to select the rewrite code point.</td>
</tr>
<tr>
<td>dscp</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>For M-series Enhanced FPC and T-series FPC, fixed rewrite loss priority determines the value for bit 0; queue number (forwarding class) determines bits 1 and 2.</td>
</tr>
<tr>
<td>ieee-802.1</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>For M-series Enhanced FPC, fixed rewrite loss priority determines the value for bit 0; queue number (forwarding class) determines bits 1 and 2.</td>
</tr>
<tr>
<td>inet-precedence</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>For M-series FPC, fixed rewrite loss priority determines the value for bit 0; queue number (forwarding class) determines bits 1 and 2.</td>
</tr>
<tr>
<td>mpls-exp</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>For M-series FPC, fixed rewrite loss priority determines the value for bit 0; queue number (forwarding class) determines bits 1 and 2.</td>
</tr>
<tr>
<td>Queuing</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Priority</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td></td>
</tr>
<tr>
<td>Drop Profiles</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Define Code-Point Aliases

A code-point alias is a name you assign to a set of DiffServ code-point (DSCP) bits. When you configure classes and define classifiers, you can refer to the code points by these alias names. You can configure user-defined classifiers in terms of alias names. If the value of an alias changes, it alters the behavior of any classifier that references that alias.

Table 34 shows the default mappings between the bit values and standard aliases. For example, it is widely accepted that the alias for DSCP 101110 is ef (expedited forwarding).

<table>
<thead>
<tr>
<th>DiffServ Code Designator</th>
<th>Mapping</th>
</tr>
</thead>
<tbody>
<tr>
<td>ef</td>
<td>101110</td>
</tr>
<tr>
<td>af11</td>
<td>001010</td>
</tr>
<tr>
<td>af12</td>
<td>001100</td>
</tr>
<tr>
<td>af13</td>
<td>001110</td>
</tr>
<tr>
<td>af21</td>
<td>010010</td>
</tr>
<tr>
<td>af22</td>
<td>010100</td>
</tr>
<tr>
<td>af23</td>
<td>010110</td>
</tr>
<tr>
<td>af31</td>
<td>011010</td>
</tr>
<tr>
<td>af32</td>
<td>011100</td>
</tr>
<tr>
<td>af33</td>
<td>011110</td>
</tr>
<tr>
<td>af41</td>
<td>100010</td>
</tr>
<tr>
<td>af42</td>
<td>100100</td>
</tr>
<tr>
<td>af43</td>
<td>100110</td>
</tr>
<tr>
<td>be</td>
<td>000000</td>
</tr>
<tr>
<td>cs1</td>
<td>001000</td>
</tr>
<tr>
<td>cs2</td>
<td>010000</td>
</tr>
<tr>
<td>cs3</td>
<td>011000</td>
</tr>
<tr>
<td>cs4</td>
<td>100000</td>
</tr>
<tr>
<td>cs5</td>
<td>101000</td>
</tr>
<tr>
<td>nc1/cs6</td>
<td>110000</td>
</tr>
<tr>
<td>nc2/cs7</td>
<td>111000</td>
</tr>
</tbody>
</table>
Define Code-Point Aliases

You use code-point aliases to do the following:

- Define an alias for bits that currently have no alias
- Define multiple aliases for the same bits
- Redefine an alias name to mean a different set of bits than the default

<table>
<thead>
<tr>
<th>DiffServ Code Designator</th>
<th>Mapping</th>
</tr>
</thead>
<tbody>
<tr>
<td>MPLS EXP Code Points</td>
<td></td>
</tr>
<tr>
<td>be</td>
<td>000</td>
</tr>
<tr>
<td>be1</td>
<td>001</td>
</tr>
<tr>
<td>ef</td>
<td>010</td>
</tr>
<tr>
<td>ef1</td>
<td>011</td>
</tr>
<tr>
<td>af11</td>
<td>100</td>
</tr>
<tr>
<td>af12</td>
<td>101</td>
</tr>
<tr>
<td>nc1/cs6</td>
<td>110</td>
</tr>
<tr>
<td>nc2/cs7</td>
<td>111</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>IEEE 802.1 Code Points</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>be</td>
<td>000</td>
</tr>
<tr>
<td>be1</td>
<td>001</td>
</tr>
<tr>
<td>ef</td>
<td>010</td>
</tr>
<tr>
<td>ef1</td>
<td>011</td>
</tr>
<tr>
<td>af11</td>
<td>100</td>
</tr>
<tr>
<td>af12</td>
<td>101</td>
</tr>
<tr>
<td>nc1/cs6</td>
<td>110</td>
</tr>
<tr>
<td>nc2/cs7</td>
<td>111</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Legacy IP Precedence Code Points</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>be</td>
<td>000</td>
</tr>
<tr>
<td>be1</td>
<td>001</td>
</tr>
<tr>
<td>ef</td>
<td>010</td>
</tr>
<tr>
<td>ef1</td>
<td>011</td>
</tr>
<tr>
<td>af11</td>
<td>100</td>
</tr>
<tr>
<td>af12</td>
<td>101</td>
</tr>
<tr>
<td>nc1/cs6</td>
<td>110</td>
</tr>
<tr>
<td>nc2/cs7</td>
<td>111</td>
</tr>
</tbody>
</table>
To define a code-point alias, include the `code-point-aliases` statement at the `[edit class-of-service]` hierarchy level:

```
[edit class-of-service]
code-point-aliases {
    (dscp | exp | ieee-802.1 | inet-precedence) {
        alias-name bits;
    }
}
```

For example, you might set up the following configuration:

```
[edit class-of-service]
code-point-aliases {
    dscp {
        my1 110001;
        my2 101110;
        be 000001;
        cs7 110000;
    }
}
```

The sample configuration produces this mapping:

```
user@host>show class-of-service code-point-aliases dscp
Code point type: dscp
Alias               Bit pattern
  ef/ my2           101110
  af11              001010
  af12              001100
  af13              001110
  af21              010010
  af22              010100
  af23              010110
  af31              011010
  af32              011100
  af33              011110
  af41              100010
  af42              100100
  af43              100110
  be                000001
  cs1               001000
  cs2               010000
  cs3               011000
  cs4               100000
  cs5               101000
  nc1/cs6/cs7       110000
  nc2               111000
  my1               110001
```
The following notes explain certain results in the mapping:

- **my1 110001**:  
  110001 was not mapped to anything before, and my1 is a new alias.  
  Nothing in the default mapping table is changed by this statement.

- **my2 101110**:  
  101110 is now mapped to my2 as well as ef.

- **be 000001**:  
  be is now mapped to 000001.
  The old value of be, 000000, is not associated with any alias. Packets with this DSCP value are now classified to the default forwarding class.

- **cs7 110000**:  
  cs7 is now mapped to 110000, as well as nc1 and cs6.
  The old value of cs7, 111000, is still mapped to nc2.

### Configure Forwarding Classes

Forwarding classes replace output queues from the previous CoS configuration command set. You assign each forwarding class to an internal queue number by including the forwarding-classes statement at the [edit class-of-service] hierarchy level:

```
[edit class-of-service]
forwarding-classes {
  queue queue-number class-name priority (high | low);
}
```

You cannot commit a configuration that assigns the same forwarding class to two different queues.

Table 35 shows the four forwarding classes defined by default.

**Table 35: Default Forwarding Classes**

<table>
<thead>
<tr>
<th>Queue</th>
<th>Forwarding Class Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>queue 0</td>
<td>best-effort</td>
</tr>
<tr>
<td>queue 1</td>
<td>expedited-forwarding</td>
</tr>
<tr>
<td>queue 2</td>
<td>assured-forwarding</td>
</tr>
<tr>
<td>queue 3</td>
<td>network-control</td>
</tr>
</tbody>
</table>
The following rules govern queue assignment:

- If classifiers fail to classify a packet, the packet always receives the default classification to the class associated with queue 0.

- The number of queues is dependent on the hardware plugged into the chassis. CoS configurations are inherently contingent on the number of queues on the system. Only two classes, best-effort and network-control, are actually referenced in the default configuration. The default configuration works on any platform.

- CoS configurations that specify more queues than the platform can support are not accepted. The commit fails with a detailed message that states the total number of queues available.

- All default CoS configuration is based on queue number. The name of the forwarding class that shows up when the default configuration is displayed is the forwarding class currently associated with that queue.

This is the default configuration for forwarding-classes:

```
[edit class-of-service]
forwarding-classes {
  queue 0 best-effort;
  queue 1 expedited-forwarding;
  queue 2 assured-forwarding;
  queue 3 network-control;
}
```

If you reassign the forwarding-class names, the best-effort forwarding-class name appears in the locations in the configuration previously occupied by network-control as follows:

```
forwarding-classes {
  queue 0 network-control;
  queue 1 assured-forwarding;
  queue 2 expedited-forwarding;
  queue 3 best-effort;
}
```

All the default rules of classification and scheduling that applied to queue 3 still apply. Queue 3 is simply now renamed best-effort.

- In the current default configuration:
  
  - Only IP precedence classifiers are associated with interfaces.
  
  - The only classes designated are best-effort and network-control.
  
  - Schedulers are not defined for the expedited-forwarding or assured-forwarding classes.

You must make a conscious effort to classify packets to the expedited-forwarding or assured-forwarding class and define schedulers for these classes.
Override Fabric Priority Queuing

For T-series platforms only, you can override automatic fabric priority queuing. For egress interfaces, fabric priority queuing matches the queue priority you assign at the [edit class-of-service schedulers scheduler-name] hierarchy level. High-priority egress traffic is automatically assigned to high-priority fabric queues. Likewise, low-priority egress traffic is automatically assigned to low-priority fabric queues.

You can override the default fabric priority queuing of egress traffic by including the priority statement at the [edit class-of-service forwarding-classes queue queue-number class-name] hierarchy level:

```
[edit class-of-service forwarding-classes queue queue-number class-name]
priority (low | high);
```

For information about associating a scheduler with a fabric priority, see “Associate a Scheduler with a Fabric Priority” on page 600.

Classify Packets by Behavior Aggregate

The simplest way to classify a packet is to use behavior aggregate classification. The DSCP or IP precedence bits of the IP header convey the behavior aggregate class information. The information might also be found in the MPLS EXP bits or IEEE 802.1p CoS bits.

Table 36 shows the default system classification scheme for the well-known DSCPs.

<table>
<thead>
<tr>
<th>DSCP</th>
<th>Forwarding Class</th>
<th>PLP</th>
</tr>
</thead>
<tbody>
<tr>
<td>ef</td>
<td>expedited-forwarding</td>
<td>low</td>
</tr>
<tr>
<td>af11</td>
<td>assured-forwarding</td>
<td>low</td>
</tr>
<tr>
<td>af12</td>
<td>assured forwarding</td>
<td>high</td>
</tr>
<tr>
<td>af13</td>
<td>assured forwarding</td>
<td>high</td>
</tr>
<tr>
<td>af21</td>
<td>best-effort</td>
<td>low</td>
</tr>
<tr>
<td>af22</td>
<td>best-effort</td>
<td>low</td>
</tr>
<tr>
<td>af23</td>
<td>best-effort</td>
<td>low</td>
</tr>
<tr>
<td>af31</td>
<td>best-effort</td>
<td>low</td>
</tr>
<tr>
<td>af32</td>
<td>best-effort</td>
<td>low</td>
</tr>
<tr>
<td>af33</td>
<td>best-effort</td>
<td>low</td>
</tr>
<tr>
<td>af41</td>
<td>best-effort</td>
<td>low</td>
</tr>
<tr>
<td>af42</td>
<td>best-effort</td>
<td>low</td>
</tr>
<tr>
<td>af43</td>
<td>best-effort</td>
<td>low</td>
</tr>
<tr>
<td>be</td>
<td>best-effort</td>
<td>low</td>
</tr>
<tr>
<td>cs1</td>
<td>best-effort</td>
<td>low</td>
</tr>
<tr>
<td>cs2</td>
<td>best-effort</td>
<td>low</td>
</tr>
<tr>
<td>cs3</td>
<td>best-effort</td>
<td>low</td>
</tr>
<tr>
<td>cs4</td>
<td>best-effort</td>
<td>low</td>
</tr>
</tbody>
</table>
All af classes other than af1X are mapped to best-effort, since RFC 2597 prohibits a node from aggregating classes. In effect, mapping to best-effort implies that the node does not support that class.

To define new classifiers for all code-point types, include the classifiers statement at the [edit class-of-service] hierarchy level:

```plaintext
[edit class-of-service]
classifiers {
    (dscp | exp | ieee-802.1 | inet-precedence) classifier-name {
        import [classifier-name | default];
        forwarding-class class-name {
            loss-priority (low | high) code-points [alias | bits];
        }
    }
}
```

A classifier takes a specified bit pattern as either the literal pattern or as a defined alias and attempts to match it to the type of packet arriving on the interface. If the information in the packet’s header matches the specified pattern, the packet is sent to the appropriate queue, defined by the forwarding class associated with the classifier.

You can use any table, including the default, in the definition of a new classifier by including the import statement. The imported classifier is used as a template and is not modified. Whenever you commit a configuration that assigns a new class-name and loss-priority value to a code-point alias or set of bits, it replaces that entry in the imported classifier template. As a result, you must explicitly specify every code point in every designation that requires modification.

If an interface is mounted on an M-series FPC, you can apply to the interface the default exp classifier only. If an interface is mounted on an enhanced FPC, you can define and apply to it a new exp classifier.
You can apply the classification map to a logical interface by including the classifiers statement in the following configuration:

```
[edit class-of-service]
interfaces {
    interface-name {
        unit logical-unit-number {
            classifiers (dscp | exp | ieee-802.1 | inet-precedence) (classifier-name | default);
        }
    }
}
```

You can use interface wildcards for `interface-name` and `logical-unit-number`.

The `dscp` classifier classifies all incoming IPv4 packets, while the `exp` classifier handles MPLS packet classification.

You cannot mix L2 and L3 classification on an interface. For the purposes of this configuration, MPLS is considered L3 classification.

**Configure Scheduling Policy Maps**

You use scheduling policy maps to configure the forwarding classes that represent packet queues and associate them with physical interfaces.

A scheduler configuration block specifies the buffer size, bandwidth, and priority for a queue. It also specifies the RED drop profile for packets that fall within specification and out of specification. To configure schedulers, include the `schedulers` statement at the `[edit class-of-service]` hierarchy level:

```
[edit class-of-service]
schedulers {
    scheduler-name {
        buffer-size (percent percentage | remainder | temporal microseconds);
        drop-profile-map loss-priority (low | high) protocol (non-tcp | tcp | any)
        drop-profile-name;
        priority (low | high | strict-high);
        transmit-rate (rate | percent percentage | remainder | exact);
    }
}
```

Once you define a scheduler, you can include it in a scheduler map that is used to map a specified forwarding class to a scheduler configuration:

```
[edit class-of-service]
scheduler-maps {
    map-name {
        forwarding-class class-name scheduler scheduler-name;
    }
}
```
When you have defined the map-name, you can associate it with an output interface:

```
[edit class-of-service]
interfaces {
    interface-name {
        scheduler-map map-name;
    }
}
```

Interface wildcards are supported.

You must configure each forwarding class in turn. The following default scheduler is provided with the installation. These settings are not visible in the output of the `show class-of-service` command; rather, they are implicit.

```
[edit class-of-service]
schedulers {
    network-control {
        transmit-rate percent 5;
        buffer-size percent 5;
        priority low;
        drop-profile-map loss-priority any protocol any;
        drop-profile terminal;
    }
    best-effort {
        transmit-rate percent 95;
        buffer-size percent 95;
        priority low;
        drop-profile-map loss-priority any protocol any;
        drop-profile terminal;
    }
}
drop-profiles {
    terminal {
        fill-level 100 drop-probability 100;
    }
}
```

**Associate a Scheduler with a DLCI or VLAN on a Channelized QPP Interface**

For Channelized OC-12 QPP, Channelized STM-1 QPP, Channelized T3 QPP, Channelized E1 QPP, and Gigabit Ethernet QPP interfaces with Frame Relay or VLAN encapsulation, you can associate a scheduler map name with a logical interface. To activate transmission scheduling on a logical interface, include the `per-unit-scheduler` statement at the `[edit interfaces interface-name]` hierarchy level, and the `scheduler-map` statement at the `[edit class-of-service interfaces interface-name unit logical-unit-number]` hierarchy level:

```
[edit interfaces interface-name]
per-unit-scheduler;

[edit class-of-service interfaces interface-name unit logical-unit-number]
scheduler-map map-name;
```

For each port, the maximum number of scheduled DLCIs or VLANs is 383.

For channelized QPP interfaces, the number of schedulers you can apply varies by channel level. Table 37 shows the number of schedulers you can apply at each channel level.
Table 37: Scheduler Limitations for Channelized QPP Interfaces

<table>
<thead>
<tr>
<th>Channelized PICs with QPP</th>
<th>Number of DLCIs per level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Channelized OC-12</td>
<td>63 for T3, OC-3, SONET, and Channelized OC-12 interfaces</td>
</tr>
<tr>
<td>Channelized T3</td>
<td>63 for T3 interfaces</td>
</tr>
<tr>
<td>Channelized STM-1</td>
<td>63 for STM-1 interfaces and 15 for E1 interfaces</td>
</tr>
<tr>
<td>Channelized E1</td>
<td>15 for E1 interfaces</td>
</tr>
</tbody>
</table>

You can associate up to four forwarding classes per physical interface.

To specify the amount of bandwidth allocated to the logical interface, you must also include the bandwidth statement at the [edit class-of-service interfaces interface-name unit logical-unit-number] hierarchy level:

```
[edit class-of-service interfaces interface-name unit logical-unit-number]
bandwidth rate;
```

You can specify a peak bandwidth rate in bps, either as a complete decimal number or as a decimal number followed by the abbreviation k (1000), m (1,000,000), or g (1,000,000,000). The range is 1000 through 32,000,000,000 bps.

If you do not include the bandwidth statement in the configuration, the logical interface might not be able to transmit traffic unless surplus bandwidth is available on the physical interface. The sum of the bandwidth you allocate to all of the logical interfaces on a physical interface should not exceed the bandwidth of the physical interface.

**Example: Associate a Scheduler with a Logical QPP Interface**

Associate one scheduler with logical interface unit 0, and another with logical interface unit 1. The scheduler sched-map-logical-0 is associated with t3-1/0/0.0, and sched-map-logical-1 is associated with t3-1/0/0.1. The logical interface units 0 and 1 are allocated transmission bandwidths of 10 Mbit per second and 20 Mbit per second, respectively.

The allocated bandwidth is shared among the individual forwarding classes in the scheduler map. Although these schedulers are configured on a single physical interface, they are independent from each other. Traffic on one logical interface unit does not affect the transmission priority, bandwidth allocation, or drop behavior on the other logical interface unit.

```
[edit interfaces]
t3-1/0/0.0 {  
  encapsulation frame-relay;
  per-unit-scheduler;
}
```
CoS Configuration Guidelines

Configure Scheduling Policy Maps

```
[edit class-of-service]
interfaces {
  t3-1/0/0:1 {
    unit 0 {
      dlci 1022;
      scheduler-map sched-map-logical-0;
      bandwidth 10m;
    }
    unit 1 {
      dlci 1021;
      scheduler-map sched-map-logical-1;
      bandwidth 20m;
    }
  }
}

scheduler-maps {
  sched-map-logical-0 {
    forwarding-class best-effort scheduler sched-best-effort-0;
    forwarding-class assured-forwarding scheduler sched-bronze-0;
    forwarding-class expedited-forwarding scheduler sched-silver-0;
    forwarding-class network-control scheduler sched-gold-0;
  }
  sched-map-logical-1 {
    forwarding-class best-effort scheduler sched-best-effort-1;
    forwarding-class assured-forwarding scheduler sched-bronze-1;
    forwarding-class expedited-forwarding scheduler sched-silver-1;
    forwarding-class network-control scheduler sched-gold-1;
  }
}

schedulers {
  sched-best-effort-0 {
    transmit-rate 4m;
  }
  sched-bronze-0 {
    transmit-rate 3m;
  }
  sched-silver-0 {
    transmit-rate 2m;
  }
  sched-gold-0 {
    transmit-rate 1m;
  }
  sched-best-effort-1 {
    transmit-rate 8m;
  }
  sched-bronze-1 {
    transmit-rate 6m;
  }
  sched-silver-1 {
    transmit-rate 4m;
  }
  sched-gold-1 {
    transmit-rate 2m;
  }
}
```
Associate a Scheduler with a Fabric Priority

On T-series platforms only, you can associate a scheduler with a class of traffic that has a specific priority while transiting the fabric. Traffic transiting the fabric can have two priority values: low or high. To associate a scheduler with a fabric priority, include the priority and scheduler statements at the [edit class-of-service fabric scheduler-map] hierarchy level:

```
[edit class-of-service fabric scheduler-map]
priority (low | high) scheduler scheduler-name;
```

For fabric CoS configuration, schedulers are restricted to transmit rates and drop profiles. Only the percent and remainder options are supported for transmit rates.

You might set up the following configuration:

```
[edit class-of-service]
schedulers {
  fab-be-scheduler {
    drop-profile-map loss-priority low protocol any drop-profile fab-be-profile;
    drop-profile-map loss-priority high protocol any drop-profile fab-be-profile;
  }
  fab-ef-scheduler {
    drop-profile-map loss-priority low protocol any drop-profile fab-ef-profile;
    drop-profile-map loss-priority high protocol any drop-profile fab-ef-profile;
  }
}
drop-profiles {
  fab-ef-profile {
    fill-level 100 drop-probability 100;
    fill-level 95 drop-probability 50;
  }
  fab-be-profile {
    fill-level 100 drop-probability 100;
    fill-level 85 drop-probability 50;
  }
}
fabric {
  scheduler-map {
    priority low scheduler fab-be-scheduler;
    priority high scheduler fab-ef-scheduler;
  }
}
```

For a scheduler that you associate with a fabric priority, you cannot include the buffer-size, transmit-rate, and priority statements at the [edit class-of-service schedulers scheduler-name] hierarchy level.

Note

For information about associating a forwarding class with a fabric priority, see “Override Fabric Priority Queuing” on page 594.
Configure RED Drop Profiles

RED drop profiles are associated with the forwarding classes and loss priorities from the scheduler-map you configured on the interface. To configure the drop profiles themselves, include the drop-profiles statement at the [edit class-of-service] hierarchy level:

```
[edit class-of-service]
drop-profiles {
    profile-name {
        fill-level percentage drop-probability percentage;
        interpolate {
            fill-level value;
            drop-probability value;
        }
    }
}
```

In this configuration, you include either the interpolate statement and its options, or the fill-level and drop-probability percentage values. These two alternatives enable you to configure either each drop probability at up to 64 fill-level/drop-probability paired values, or a profile represented as a series of line segments.

![Note: If you configure the interpolate statement, you can specify more than 64 pairs, but the system generates only 64 discrete entries.]

The line segments are defined in terms of the following graphical model: in the first quadrant, the x axis represents the fill level and the y axis represents the drop probability.

The initial line segment spans from the origin (0,0) to the point (<l1>, <p1>); a second line runs from (<l1>, <p1>) to (<l2>, <p2>) and so forth, until a final line segment connects (100, 100). The system automatically constructs a drop profile containing 64 fill levels at drop probabilities that approximate the calculated line segments.

Figure 31 shows sample line graphs comparing use of the segment percentages (on the left) and interpolated values (on the right):

![Figure 31: Segmented and Interpolated Drop Profiles](image)
**Packet Loss Priority**

The system supports two packet loss priority (PLP) designations, low and high.

The packet loss priority is used to determine the RED drop profile when queuing a packet. You can set it by configuring a classifier or policer.

**Rewrite Packet Header Information**

You can rewrite the packet header bits because the logical interface transmits the packet along with the forwarding-class and PLP information associated with the packet. If the packet's header field is blank, the forwarding class and PLP information specified in the rule are entered, or if the forwarding class and PLP information are already present, they are replaced with the new values. The traffic is then classified accordingly. The rewrite-rules configurations define the mappings.

Table 38 shows the default mappings.

<table>
<thead>
<tr>
<th>Map To DSCP/EXP/IEEE/IP</th>
<th>Map From Forwarding Class</th>
<th>PLP Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ef</td>
<td>expedited-forwarding</td>
<td>low</td>
</tr>
<tr>
<td>ef</td>
<td>expedited-forwarding</td>
<td>high</td>
</tr>
<tr>
<td>af11</td>
<td>assured-forwarding</td>
<td>low</td>
</tr>
<tr>
<td>af12 (DSCP/EXP)</td>
<td>assured-forwarding</td>
<td>high</td>
</tr>
<tr>
<td>be</td>
<td>best-effort</td>
<td>low</td>
</tr>
<tr>
<td>be</td>
<td>best-effort</td>
<td>high</td>
</tr>
<tr>
<td>nc1/cs6</td>
<td>network-control</td>
<td>low</td>
</tr>
<tr>
<td>nc2/cs7</td>
<td>network-control</td>
<td>high</td>
</tr>
</tbody>
</table>

See “Define Code-Point Aliases” on page 589 for the default bit definitions of DSCP, EXP, and IEEE code points.

To configure a rewrite-rules mapping and associate it with the appropriate forwarding class and code-point alias or bit set, include the rewrite-rules statement at the [edit class-of-service] hierarchy level:

```plaintext
[edit class-of-service]
rewrite-rules {
    (dscp | exp | inet-precedence) rewrite-name {
        import (rewrite-name | default);
        forwarding-class class-name {
            loss-priority (low | high) code-point alias | bits;
        }
    }
}
```
To assign the rewrite-rules configuration to the output logical interface, include the following configuration:

```
[edit class-of-service]
  interfaces {
    interface-name {
      unit logical-unit-number {
        rewrite-rules {
          dscp (rewrite-name | default);
          exp (rewrite-name | default) protocol protocol-types;
          exp-push-push-push default;
          exp-swap-push-push default;
          ieee-802.1 default;
          inet-precedence (rewrite-name | default);
        }
      }
    }
  }
```

You can include interface wildcards for `interface-name` and `logical-unit-number`. You can also include Layer 2 and Layer 3 rewrite information in the same configuration.

The following sections explain several rewrite rule applications you can configure:

- **Rewrite EXP Bits on a Particular Node on page 603**
- **Rewrite MPLS and IPv4 Packet Headers on page 605**
- **Rewrite the EXP Bits of All Three Labels of an Outgoing Packet on page 607**
- **Rewrite IEEE 802.1p Packet Headers with MPLS EXP Value on page 609**

**Rewrite EXP Bits on a Particular Node**

To configure a custom table to rewrite the EXP bits, also known as CoS bits, on a particular node, the classifier table and the rewrite table must specify exactly the same code points.

In addition, the least significant bit of the code point itself must represent the PLP value. For example, code point 000 must be associated with PLP low, 001 must be associated with PLP high, and so forth.
Example: Rewrite EXP Bits on a Particular Node

Configure a custom table to rewrite the EXP bits on a particular node:

```junos
[edit class-of-service]
classifiers {
  exp exp-class {
    forwarding-class be {
      loss-priority low code-points 000;
      loss-priority high code-points 001;
    }
    forwarding-class af {
      loss-priority low code-points 010;
      loss-priority high code-points 011;
    }
    forwarding-class ef {
      loss-priority low code-points 100;
      loss-priority high code-points 101;
    }
    forwarding-class nc {
      loss-priority low code-points 110;
      loss-priority high code-points 111;
    }
  }
}
rewrite-rules {
  exp exp-rw {
    forwarding-class be {
      loss-priority low code-point 000;
      loss-priority high code-point 001;
    }
    forwarding-class af {
      loss-priority low code-point 010;
      loss-priority high code-point 011;
    }
    forwarding-class ef {
      loss-priority low code-point 100;
      loss-priority high code-point 101;
    }
    forwarding-class nc {
      loss-priority low code-point 110;
      loss-priority high code-point 111;
    }
  }
}
```
Rewrite MPLS and IPv4 Packet Headers

You can apply a rewrite rule to MPLS and IPv4 packet headers simultaneously. This allows you to initialize MPLS EXP and IP precedence bits at LSP ingress. You can configure different rewrite rules depending on whether the traffic is VPN or non-VPN.

The default MPLS EXP rewrite table contents are shown in Table 39.

Table 39: Default MPLS EXP Rewrite Table

<table>
<thead>
<tr>
<th>Forwarding Class</th>
<th>Loss Priority</th>
<th>Code Point</th>
</tr>
</thead>
<tbody>
<tr>
<td>best-effort</td>
<td>low</td>
<td>000</td>
</tr>
<tr>
<td>best-effort</td>
<td>high</td>
<td>001</td>
</tr>
<tr>
<td>expedited-forwarding</td>
<td>low</td>
<td>010</td>
</tr>
<tr>
<td>expedited-forwarding</td>
<td>high</td>
<td>011</td>
</tr>
<tr>
<td>assured-forwarding</td>
<td>low</td>
<td>100</td>
</tr>
<tr>
<td>assured-forwarding</td>
<td>high</td>
<td>101</td>
</tr>
<tr>
<td>network-control</td>
<td>low</td>
<td>110</td>
</tr>
<tr>
<td>network-control</td>
<td>high</td>
<td>111</td>
</tr>
</tbody>
</table>

To override the default MPLS EXP rewrite table and rewrite MPLS and IPv4 packet headers simultaneously, include the protocol statement at the [edit class-of-service interfaces interface-name unit logical-unit-number rewrite-rules exp rewrite-rule-name] hierarchy level:

```
[edit class-of-service interfaces interface-name unit logical-unit-number rewrite-rules exp rewrite-rule-name]
protocol types;
```

The protocol statement defines the types of MPLS packets and packet headers to which the specified rewrite rule is applied. The MPLS packet can be a standard MPLS packet or an MPLS packet with an IPv4 payload. Specify the type of MPLS packet using the following options:

- **mpls-any**—Applies the rewrite rule to MPLS packets and writes the code point value to MPLS headers.
- **mpls-inet-both**—Applies the rewrite rule to VPN MPLS packets with IPv4 payloads. On T-series platforms, writes the code point value to the MPLS and IPv4 headers. On M-series routers, causes all ingress MPLS LSP packets with IPv4 payloads to be initialized with 000 code points for IP precedence and MPLS EXP values.
- **mpls-inet-both-non-VPN**—Applies the rewrite rule to non-VPN MPLS packets with IPv4 payloads. On T-series platforms, writes the code point value to the MPLS and IPv4 headers. On M-series routers, causes all ingress MPLS LSP packets with IPv4 payloads to be initialized with 000 code points for IP precedence and MPLS EXP values.

An alternative to overwriting the default with a rewrite-rules mapping is to configure the default packet header rewrite mappings, as shown in Table 38 on page 602.
Example: Rewrite MPLS and IPv4 Packet Headers

On a T-series platform, configure rewrite tables and apply them in various ways to achieve the following results:

- For interface so-3/1/0, the three EXP rewrite tables are applied to packets, depending on the protocol of the payload:
  - IPv4 packets (VPN) that enter the LSPs on interface so-3/1/0 are initialized with values from rewrite table exp-inet-table. An identical three-bit value is written into the IP precedence and MPLS EXP bit fields.
  - IPv4 packets (non-VPN) that enter the LSPs on interface so-3/1/0 are initialized with values from rewrite table rule-non-vm. An identical three-bit value is written into the IP precedence and MPLS EXP bit fields.
  - Non-IPv4 packets that enter the LSPs on interface so-3/1/0 are initialized with values from rewrite table rule1, and written into the MPLS EXP header field only. The statement exp rule1 has the same result as exp rule1 protocol mpls-any.

- For interface so-3/1/0, IPv4 packets transmitted over a non-LSP layer are initialized with values from IP precedence rewrite table rule2.

- For interface so-3/1/1, IPv4 packets that enter the LSPs are initialized with values from EXP rewrite table exp-inet-table. An identical 3-bit value is written into the IP precedence and MPLS EXP bit fields.

- For interface so-3/1/1, MPLS packets other than IPv4 Layer 2 types are also initialized with values from table exp-inet-table. For VPN MPLS packets with IPv4 payloads, the code point value is written to MPLS and IPv4 headers. For VPN MPLS packets without IPv4 payloads, the code point value is written to MPLS headers only.

```plaintext
[edit class-of-service]
rewrite-rules { exp exp-inet-table { forwarding-class best-effort { loss-priority low code-point 000; loss-priority high code-point 001; } forwarding-class assured-forwarding { loss-priority low code-point 010; loss-priority high code-point 011; } forwarding-class expedited-forwarding { loss-priority low code-point 111; loss-priority high code-point 110; } forwarding-class network-control { loss-priority low code-point 100; loss-priority high code-point 101; } } exp rule1 { ...
```
Rewrite the EXP Bits of All Three Labels of an Outgoing Packet

In interprovider, carrier-of-carrier, and complex traffic engineering scenarios, it is sometimes necessary to push three labels on the next hop, using a swap-push-push or triple-push operation.

By default, on M-series routers, the top MPLS EXP label of an outgoing packet is not rewritten when you configure swap-push-push and triple-push operations. On M-series routers, you can rewrite the EXP bits of all three labels of an outgoing packet, thereby maintaining CoS of an incoming MPLS or non-MPLS packet.

To do this on incoming MPLS packets, include the exp-swap-push-push-push default statement at the [edit class-of-service interfaces interface-name unit logical-unit-number rewrite-rules] hierarchy level:

```
[edit class-of-service interfaces interface-name unit logical-unit-number rewrite-rules]
exp-swap-push-push default;
```

To do this on incoming non-MPLS packets, include the exp-push-push-push-push default statement at the [edit class-of-service interfaces interface-name unit logical-unit-number rewrite-rules] hierarchy level:

```
[edit class-of-service interfaces interface-name unit logical-unit-number rewrite-rules]
exp-push-push-push-push default;
```

These configurations apply the default MPLS EXP rewrite table, as shown in Table 39 on page 605. You can configure these operations and also override the default MPLS EXP rewrite table with a custom table. For more information about writing and applying a custom rewrite table, see “Rewrite Packet Header Information” on page 602.
Example: Rewrite the EXP Bits of All Three Labels of an Outgoing Packet

Configure a swap-push-push operation, and override the default rewrite table with a custom table:

```conf
[edit class-of-service]
forwarding-classes {
  queue 0 be;
  queue 1 ef;
  queue 2 af;
  queue 3 nc;
}
interfaces {
  so-1/1/3 {
    unit 0 {
      rewrite-rules {
        exp exp_rew; #Apply custom rewrite table
        exp-swap-push-push default;
      }
    }
  }
}
rewrite-rules {
  exp exp_rew {
    forwarding-class be {
      loss-priority low code-point 000;
      loss-priority high code-point 100;
    }
    forwarding-class ef {
      loss-priority low code-point 001;
      loss-priority high code-point 101;
    }
    forwarding-class af {
      loss-priority low code-point 010;
      loss-priority high code-point 110;
    }
    forwarding-class nc {
      loss-priority low code-point 011;
      loss-priority high code-point 111;
    }
  }
}
```
Rewrite IEEE 802.1p Packet Headers with MPLS EXP Value

For Ethernet interfaces installed on a T-series platform with a peer connection to an M-series router or a T-series platform, you can rewrite both MPLS EXP and IEEE 802.1p bits to a configured value. This allows you to pass the configured value to the Layer 2 VLAN path.

To rewrite both the MPLS EXP and IEEE 802.1p bits, you must include EXP and IEEE 802.1p rewrite rules in the interface configuration. To configure EXP and IEEE 802.1p rewrite rules, include the rewrite-rules statement at the [edit class-of-service interfaces interface-name unit logical-unit-number] hierarchy level, specifying the exp and ieee-802.1 options:

[edit class-of-service interfaces interface-name unit logical-unit-number]
rewrite-rules {
    exp rewrite-rule-name;
    ieee-802.1 default;
}

When you combine these two rewrite rules, only the EXP rewrite table is used for rewriting packet headers. If you do not configure a VLAN on the interface, only the EXP rewriting is in effect. If you do not configure an LSP on the interface or if the MPLS EXP rewrite rule mapping is removed, the IEEE 802.1p default rewrite rules mapping takes effect.

You can also combine other rewrite rules. IP, DSCP, and MPLS EXP are associated with Layer 3 packet headers, and IEEE 802.1p is associated with the Layer 2 packet header.

- If you combine IEEE 802.1p and IP rewrite rules, the Layer 3 packets and Layer 2 headers are rewritten with the IP rewrite rule.
- If you combine IEEE 802.1p and DSCP rewrite rules, three bits of the Layer 2 header and six bits of the Layer 3 packet header are rewritten with the DSCP rewrite rule.

The following example shows how to configure an EXP rewrite rule and apply it to both MPLS EXP and IEEE 802.1p bits:

[edit class-of-service]
rewrite-rules {
    exp exp-ieee-table {
        forwarding-class best-effort {
            loss-priority low code-point 000;
            loss-priority high code-point 001;
        }
        forwarding-class assured-forwarding {
            loss-priority low code-point 010;
            loss-priority high code-point 011;
        }
        forwarding-class expedited-forwarding {
            loss-priority low code-point 111;
            loss-priority high code-point 110;
        }
    }
}
Configure CoS-Based Forwarding

CoS-based forwarding (CBF) enables you to control next-hop selection based on a packet's class of service and, in particular, the value of the IP packet's precedence bits.

For example, you might want to specify a particular interface or next hop to carry high-priority traffic while all best-effort traffic takes some other path. When a routing protocol discovers equal cost paths, it can pick a path at random or load-share across the paths either through hash selection or round robin. CBF allows path selection based on class.

You can apply CBF only to a defined set of routes. Therefore you must configure a policy statement as in the following example:

```
[edit]
policy-options {
  policy-statement my-cos-forwarding {
    from {
      route-filter filter-name;
    }
    then {
      cos-next-hop-map map-name;
    }
  }
}
```

This configuration specifies that routes matching the route filter will be subject to the CoS next-hop mapping specified by map-name. For more information about configuring policy statements, see the JUNOS Internet Software Configuration Guide: Policy Framework.
To specify a CoS next-hop map, include the forwarding-policy statement at the [edit class-of-service] hierarchy level:

```plaintext
[edit class-of-service]
forwarding-policy {
    next-hop-map map-name {
        forwarding-class class-name {
            next-hop [ next-hop-name ];
            lsp-next-hop [ lsp-regular-expression ]
        }
    }
}
```

When you configure CBF with OSPF as the IGP, you must specify the next hop as an interface name or next-hop alias, not as an IP address. For an example configuration, see “Example: Configure CoS-Based Forwarding” on page 612.

You cannot configure packet classification for IPv6. Only IP precedence classifiers are supported. For an example configuration, see “Configure CoS-Based Forwarding for IPv6” on page 615.

The JUNOS software applies the CoS next-hop map to the set of next hops previously defined; the next hops themselves can be located across any outgoing interfaces on the router. For example, the following configuration associates a set of forwarding classes and next-hop identifiers:

```plaintext
[edit class-of-service forwarding-policy]
next-hop-map map1 {
    forwarding-class expedited-forwarding {
        next-hop next-hop1;
        next-hop next-hop2;
    }
    forwarding-class best-effort {
        next-hop next-hop3;
        lsp-next-hop lsp-next-hop4;
    }
}
```

In this example, next-hopN is either an IP address or an egress interface for some next hop, and lsp-next-hop4 is a regular expression corresponding to any next hop with that label. Q1 through QN are a set of forwarding classes that map to the specific next hop. That is, when a packet is switched with Q1 through QN, it will be forwarded out the interface associated with the associated next hop.

This configuration has the following implications:

- A single forwarding class can map to multiple standard next hops or LSP next hops. This implies that load sharing is done across standard next hops or LSP next hops servicing the same class value. To make this work properly, the JUNOS software creates a list of the equal-cost next hops and forwards packets according to standard load-sharing rules for that forwarding class.

- If a forwarding class configuration includes LSP next hops and standard next hops, the LSP next hops are preferred over the standard next hops. In the preceding example, if both next-hop3 and lsp-next-hop4 are valid next hops for a route to which map1 is applied, the forwarding table includes entry lsp-next-hop4 only.
If next-hop-map does not specify all possible forwarding classes, the default forwarding class is selected as the default. If the default forwarding class is not specified in the next-hop map, a default is designated randomly. The default forwarding class is the class associated with queue 0.

For LSP next hops, the JUNOS software uses UNIX regex(3)-style regular expressions. For example, if the following labels exist: lsp, lsp1, lsp2, lsp3, the statement lsp-next-hop lsp matches lsp, lsp1, lsp2, and lsp3. If you do not desire this behavior, you must use the anchor characters lsp-next-hop "^lsp\$", which match lsp only.

The final step is to apply the route filter to routes exported to the forwarding engine. This is shown in the following example:

```
routing-options {
    forwarding-table {
        export my-cos-forwarding;
    }
}
```

This configuration instructs the routing process to insert routes to the forwarding engine matching my-cos-forwarding with the associated next-hop CBF rules.

The following algorithm is used when you apply a configuration to a route:

- If the route is a single next-hop route, all traffic will go to that route; that is, no CBF will take effect.

- For each next hop, associate the proper forwarding class. If a next hop appears in the route but not in the cos-next-hop map, it will not appear in the forwarding table entry.

- The default forwarding class is used if all forwarding classes are not specified in the next-hop map. If the default is not specified, one is chosen randomly.

**Example: Configure CoS-Based Forwarding**

Router A has two routes to destination 10.255.71.208 on Router D. One route goes through Router B, and the other goes through Router C, as shown in Figure 32.

Configure Router A with CBF to select Router B for queue 0 and queue 2, and Router C for queue 1 and queue 3.
When you configure CBF with OSPF as the IGP, you must specify the next hop as an interface name, not as an IP address. The next hops in this example are specified as ge-2/0/0.0 and so-0/3/0.0.

```
[edit class-of-service]
forwarding-policy {
  next-hop-map my_cbf {
    forwarding-class be {
      next-hop ge-2/0/0.0;
    }
    forwarding-class ef {
      next-hop so-0/3/0.0;
    }
    forwarding-class af {
      next-hop ge-2/0/0.0;
    }
    forwarding-class nc {
      next-hop so-0/3/0.0;
    }
  }
}

classifiers {
  inet-precedence inet {
    forwarding-class be {
      loss-priority low code-points [ 000 100 ];
    }
    forwarding-class ef {
      loss-priority low code-points [ 001 101 ];
    }
    forwarding-class af {
      loss-priority low code-points [ 010 110 ];
    }
    forwarding-class nc {
      loss-priority low code-points [ 011 111 ];
    }
  }
}
```
Configure CoS-Based Forwarding

forwarding-classes {
    queue 0 be;
    queue 1 ef;
    queue 2 af;
    queue 3 nc;
}

interfaces {
    at-4/2/0 {
        unit 0 {
            classifiers {
                inet-precedence inet;
            }
        }
    }
}

[edit policy-options]
policy-statement cbf {
    from {
        route-filter 10.255.71.208/32 exact;
    }
    then cos-next-hop-map my_cbf;
}

[edit routing-options]
graceful-restart;
forwarding-table {
    export cbf;
}

[edit interfaces]
traceoptions {
    file trace-intf size 5m world-readable;
    flag all;
}
so-0/3/0 {
    unit 0 {
        family inet {
            address 10.40.13.1/30;
        }
        family iso;
        family mpls;
    }
}
ge-2/0/0 {
    unit 0 {
        family inet {
            address 10.40.12.1/30;
        }
        family iso;
        family mpls;
    }
}
at-4/2/0 {
    atm-options {
        vpi 1 {
            maximum-vcs 1200;
        }
    }
}
Configure CoS-Based Forwarding for IPv6

Configure CBF next-hop maps and CBF LSP next-hop maps for IPv6 addresses. The following example shows a CBF next-hop map for IPv6 addresses.

You can configure a next-hop map with both IPv4 and IPv6 addresses, or you can configure separate next-hop maps for IPv4 and IPv6 addresses and include the from family (inet | inet6) statements at the [edit policy-options policy-options policy-statement term] hierarchy level to ensure that only next-hop maps of a specified protocol are applied to a specified route.

If you do not configure separate next-hop maps and include the from family (inet | inet6) statements in the configuration, when a route uses two next hops (whether IPv4, IPv6, interface, or LSP next hop) in at least two of the specified forwarding classes, CBF is used for the route; otherwise, the CBF policy is ignored.

1. Define the CBF next-hop map:

   [edit class-of-service]
   forwarding-policy {
       next-hop-map cbf-map {
           forwarding-class best-effort {
               next-hop [:192.168.139.38 192.168.139.38 ];
           }
           forwarding-class expedited-forwarding {
               next-hop [:192.168.140.5 192.168.140.5 ];
           }
           forwarding-class assured-forwarding {
               next-hop [:192.168.145.5 192.168.145.5 ];
           }
           forwarding-class network-control {
               next-hop [:192.168.141.2 192.168.141.2 ];
           }
       }
   }

2. Define the CBF forwarding policy:

   [edit policy-options]
   policy-statement ls {
       then cos-next-hop-map cbf-map;
   }

3. Export the CBF forwarding policy:

   [edit routing-options]
   forwarding-table {
       export ls;
   }
Override the Input Classification

For IPv4 or IPv6 packets, you can override the incoming classification, assigning them to the same forwarding class based on their input interface, input precedence bits, or destination address. You do so by defining a policy class when configuring CoS properties and referencing this class when configuring a routing policy.

When you override the classification of incoming packets, any mappings you configured for associated precedence bits or incoming interfaces to output transmission queues are ignored. Also, if the packet loss priority (PLP) bit was set in the packet by the incoming interface, the PLP bit is cleared.

To override the input packet classification, do the following:

1. Define the policy class by including the class statement at the [edit class-of-service policy] hierarchy level:

   ```
   [edit class-of-service]
   forwarding-policy {
     class class-name {
       classification-override {
         forwarding-class class-name;
       }
     }
   }
   
   class-name is a name that identifies the class.
   ```

2. Associate the policy class with a routing policy by including it in a policy-statement statement at the [edit policy-options] hierarchy level. Specify the destination prefixes in the route-filter statement and the CoS policy class name in the then statement.

   ```
   [edit policy-options]
   policy-statement policy-name {
     term term-name {
       from {
         route-filter destination-prefix match-type <class class-name>;
       }
       then class class-name;
     }
   }
   
   [edit policy-options]
   policy-statement policy-name {
     term term-name {
       from {
         route-filter destination-prefix match-type <class class-name>;
       }
       then class class-name;
     }
   }
   ```

3. Apply the policy by including the export statement at the [edit routing-option] hierarchy level:

   ```
   [edit routing-options]
   forwarding-table {
     export policymame;
   }
   ```
Example: Configure Class of Service

The following example includes classifiers, rewrite markers, and schedulers to configure a class of service policy.

1. Define a classifier that matches IP traffic arriving on the interface. The affected IP traffic has IP precedence bits with patterns matching those defined by aliases A or B. The loss priority of the matching packets is set to low, and the forwarding class is mapped to best effort (queue 0):

```
[edit]
class-of-service {
    classifiers {
        inet-precedence normal-traffic {
            forwarding-class best-effort {
                loss-priority low code-points [my1 my2];
            }
        }
    }
}
```

Following are the code-point alias and forwarding-class mappings referenced in the normal-traffic classifier:

```
[edit]
class-of-service {
    code-point-aliases {
        inet-precedence {
            my1 000;
            my2 001;
            ...
        }
    }
}
```

```
[edit]
class-of-service {
    forwarding-classes {
        queue 0 best-effort;
        queue 1 expedited-forwarding;
    }
}
```
2. Use rewrite markers to redefine the bit pattern of outgoing packets. Assign the new bit pattern based on specified forwarding classes, regardless of the loss priority of the packets:

```
[edit]
  class-of-service {
    rewrite-rules {
      inet-precedence clear-prec {
        forwarding-class best-effort {
          loss-priority low code-point 000;
          loss-priority high code-point 000;
        }
        forwarding-class expedited-forwarding {
          loss-priority low code-point 100;
          loss-priority high code-point 100;
        }
      }
    }
  }
```

3. Configure a scheduler map associating forwarding classes with schedulers and drop-profiles:

```
[edit]
  class-of-service {
    scheduler-maps {
      one {
        forwarding-class expedited-forwarding scheduler special;
        forwarding-class best-effort scheduler normal;
      }
    }
  }
```

Schedulers establish how to handle the traffic within the output queue for transmission onto the wire. Following is the scheduler referenced in scheduler map one:

```
[edit]
  class-of-service {
    schedulers {
      special {
        transmit-rate percent 30;
        priority high;
      }
      normal {
        transmit-rate percent 70;
        priority low;
      }
    }
  }
```
4. Apply the normal-traffic classifier to all SONET/SDH interfaces and all logical interfaces of SONET/SDH interfaces; apply the clear-prec rewrite marker to all Gigabit Ethernet interfaces and all logical interfaces of Gigabit Ethernet interfaces; and apply the one scheduler map to all interfaces:

```
[edit]
 class-of-service {
    interfaces {
        so-0/0/0 {
            scheduler-map one;
            unit 0 {
                classifiers {
                    inet-precedence normal-traffic;
                }
            }
        }
        so-0/0/1 {
            scheduler-map one;
            unit 1 {
                classifiers {
                    inet-precedence normal-traffic;
                }
            }
        }
        ge-1/0/0 {
            scheduler-map one;
            unit 0 {
                rewrite-rules {
                    inet-precedence clear-prec;
                }
            }
            unit 1 {
                rewrite-rules {
                    inet-precedence clear-prec;
                }
            }
        }
        ge-1/0/1 {
            scheduler-map one;
            unit 0 {
                rewrite-rules {
                    inet-precedence clear-prec;
                }
            }
            unit 1 {
                rewrite-rules {
                    inet-precedence clear-prec;
                }
            }
        }
    }
}```
Following is the complete configuration:

```plaintext
[edit class-of-service]
classifiers {
    inet-precedence normal-traffic {
        forwarding-class best-effort {
            loss-priority low code-points [my1 my2];
        }
    }
}
code-point-aliases {
    inet-precedence {
        my1 000;
        my2 001;
        cs1 010;
        cs2 011;
        cs3 100;
        cs4 101;
        cs5 111;
        cs6 111;
    }
}
drop-profiles {
    high-priority {
        fill-level 20 drop-probability 100;
    }
    low-priority {
        fill-level 90 drop-probability 95;
    }
    big-queue {
        fill-level 100 drop-probability 100;
    }
}
forwarding-classes {
    queue 0 best-effort;
    queue 1 expedited-forwarding;
}
interfaces {
    so-0/0/0 {
        scheduler-map one;
        unit 0 {
            classifiers {
                inet-precedence normal-traffic;
            }
        }
    }
    so-0/0/1 {
        scheduler-map one;
        unit 1 {
            classifiers {
                inet-precedence normal-traffic;
            }
        }
    }
}
```
ge-1/0/0 {
    scheduler-map one;
    unit 0 {
        rewrite-rules {
            inet-precedence clear-prec;
        }
    }
    unit 1 {
        rewrite-rules {
            inet-precedence clear-prec;
        }
    }
}
ge-1/0/1 {
    scheduler-map one;
    unit 0 {
        rewrite-rules {
            inet-precedence clear-prec;
        }
    }
    unit 1 {
        rewrite-rules {
            inet-precedence clear-prec;
        }
    }
}
rewrite-rules {
    inet-precedence clear-prec {
        forwarding-class best-effort {
            loss-priority low code-point 000;
            loss-priority high code-point 000;
        }
        forwarding-class expedited-forwarding {
            loss-priority low code-point 100;
            loss-priority high code-point 100;
        }
    }
}
scheduler-maps {
    one {
        forwarding-class expedited-forwarding scheduler special;
        forwarding-class best-effort scheduler normal;
    }
}
schedulers {
    special {
        transmit-rate percent 30;
        priority high;
    }
    normal {
        transmit-rate percent 70;
        priority low;
    }
}
Example: Configure Class of Service
Chapter 34
Summary of CoS Configuration Statements

The following sections explain each of the CoS configuration statements. The statements are organized alphabetically.

**bandwidth**

Syntax

```plaintext
bandwidth rate;
```

Hierarchy Level

```
[edit class-of-service interfaces interface-name unit logical-unit-number]
```

Description

For logical interfaces on which you configure packet scheduling, configure the amount of bandwidth to be allocated to the logical interface.

Options

rate—Peak rate, in bps. You can specify a value in bits per second either as a complete decimal number or as a decimal number followed by the abbreviation k (1000), m (1,000,000), or g (1,000,000,000).

Range: 1000 through 32,000,000,000 bps.

Usage Guidelines

See “Associate a Scheduler with a DLCI or VLAN on a Channelized QPP Interface” on page 597.

Required Privilege Level

`interface`—To view this statement in the configuration.

`interface-control`—To add this statement to the configuration.

**buffer-size**

Syntax

```plaintext
buffer-size (percent percentage | remainder | temporal microseconds);
```

Hierarchy Level

```
[edit class-of-service schedulers scheduler-name]
```

Description

Specify buffer size as a percentage.

Options

percentage—Buffer size as a percentage of total buffer.

remainder—Remaining buffer available.

temporal—Buffer size as a temporal value from 1 through 200,000 microseconds.

Usage Guidelines

See “RED Congestion Control” on page 583 and “Configure Scheduling Policy Maps” on page 596.

Required Privilege Level

`interface`—To view this statement in the configuration.

`interface-control`—To add this statement to the configuration.
class

Syntax class class-name {
    classification-overide {
        forwarding-class class-name;
    }
}

Hierarchy Level [edit class-of-service forwarding-policy]

Description Configure CoS-based forwarding class.

Options class-name—Name of the routing policy class.

The remaining statements are explained separately.


Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

class-of-service

Syntax class-of-service { ... }

Hierarchy Level [edit]

Description Configure JUNOS CoS features.

Default If you do not configure any CoS features, all packets are transmitted from output transmission queue 0.


Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

classification-overide

Syntax classification-overide {
    forwarding-class class-name;
}

Hierarchy Level [edit class-of-service forwarding-policy class class-name]

Description For IPv4 packets, override the incoming packet classification, assigning all packets sent to a destination prefix to the same output transmission queue.

Usage Guidelines See “Configure CoS-Based Forwarding” on page 610.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

See Also policy-statement in the JUNOS Internet Software Configuration Guide: Routing and Routing Protocols
classifiers

**classifiers (define)**

Syntax  
```
classifiers {
    type classifier-name {
        import (classifier-name | default);
        forwarding-class class-name {
            loss-priority (low | high) code-points [ alias | bits ];
        }
    }
}
```

Hierarchy Level  
[edit class-of-service]

Description  
Define a CoS aggregate behavior classifier for classifying packets. You can associate the classifier with a forwarding class or code-point mapping, and import a default classifier or one that is previously defined.

Options  
- classifier-name—Name of the aggregate behavior classifier.
- type—Traffic type.
  Values: dscp, exp, ieee-802.1, inet-precedence

The remaining statements are explained separately.

Usage Guidelines  
See “Classify Packets by Behavior Aggregate” on page 594.

Required Privilege Level  
- interface—To view this statement in the configuration.
- interface-control—To add this statement to the configuration.

**classifiers (apply)**

Syntax  
```
classifiers {
    type (classifier-name | default);
}
```

Hierarchy Level  
[edit class-of-service interfaces interface-name unit logical-unit-number]

Description  
Apply a CoS aggregate behavior classifier to a logical interface. You can apply a default classifier or one that is previously defined.

Options  
- classifier-name—Name of the aggregate behavior classifier.
- type—Traffic type.
  Values: dscp, exp, ieee-802.1, inet-precedence

Usage Guidelines  
See “Classify Packets by Behavior Aggregate” on page 594.

Required Privilege Level  
- interface—To view this statement in the configuration.
- interface-control—To add this statement to the configuration.
**code-point**

Syntax  
```
code-point [ alias | bits ];
```

Hierarchy Level  
```
[edit class-of-service rewrite-rules type rewrite-name forwarding-class class-name]
```

Description  
Specify one or more DSCP code-point aliases or bit sets for association with a forwarding class.

Options  
- **alias** — Name of the DSCP alias.
- **bits** — Value of the code-point bits, in binary code.

Usage Guidelines  
See “Rewrite Packet Header Information” on page 602.

Required Privilege Level  
interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**code-point-aliases**

Syntax  
```
code-point-aliases {
    type {
        alias-name bits;
    }
}
```

Hierarchy Level  
```
[edit class-of-service]
```

Description  
Define an alias for a DSCP bit set.

Options  
- **alias-name** — Name of the DSCP alias.
- **bits** — Six-bit value of the code-point bits, in binary code.
- **type** — Traffic type.
  Values: dscp, exp, ieee-802.1, inet-precedence

Usage Guidelines  
See “Define Code-Point Aliases” on page 589.

Required Privilege Level  
interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.
code-points

Syntax code-points [ alias | bits ];

Hierarchy Level [edit class-of-service classifiers type classifier-name forwarding-class class-name]

Description Specify one or more DSCP code-point aliases or bit sets for association with a forwarding class.

Options alias — Name of the DSCP alias.

bits — Value of the code-point bits, in binary code.

Usage Guidelines See “Classify Packets by Behavior Aggregate” on page 594.

Required Privilege Level interface — To view this statement in the configuration.
interface-control — To add this statement to the configuration.

drop-probability

drop-probability (percentage)

Syntax drop-probability percentage;

Hierarchy Level [edit class-of-service drop-profiles profile-name]

Description Define drop probability percentage.

Options percentage — Probability that a packet will be dropped, expressed as a percentage. A value of 0 means that a packet will never be dropped, and a value of 100 means that all packets will be dropped.

Range: 0 through 100 percent

Usage Guidelines See “Configure RED Drop Profiles” on page 601.

Required Privilege Level interface — To view this statement in the configuration.
interface-control — To add this statement to the configuration.

drop-probability (interpolated value)

Syntax drop-probability value;

Hierarchy Level [edit class-of-service drop-profile profile-name interpolate]

Description Define up to 64 values for interpolating drop probabilities.

Options value — Data point for interpolated packet drop probability.

Range: 0 through 100

Usage Guidelines See “Configure RED Drop Profiles” on page 601.

Required Privilege Level interface — To view this statement in the configuration.
interface-control — To add this statement to the configuration.
drop-profile

Syntax
drop-profile profile-name;

Hierarchy Level
[edit class-of-service schedulers scheduler-name drop-profile-map loss-priority (low | high | any) protocol (any | non-tcp | tcp)]

Description
Define drop profiles for RED. When a packet arrives, RED checks the queue fill level. If the fill level corresponds to a nonzero drop probability, the RED algorithm determines whether to drop the arriving packet.

Options
profile-name—Name of the drop profile.

Usage Guidelines
See “Configure Scheduling Policy Maps” on page 596.

Required Privilege Level
interface—to view this statement in the configuration.
interface-control—to add this statement to the configuration.

drop-profile-map

Syntax
drop-profile-map loss-priority (low | high) protocol (non-tcp | tcp | any) drop-profile profile-name;

Hierarchy Level
[edit class-of-service schedulers scheduler-name]

Description
Define loss priority value for drop profile.

The statements are explained separately.

Usage Guidelines
See “Configure Scheduling Policy Maps” on page 596.

Required Privilege Level
interface—to view this statement in the configuration.
interface-control—to add this statement to the configuration.
drop-profiles

Syntax

drop-profiles {
  profile-name {
    fill-level percentage drop-probability percentage;
    interpolate {
      fill-level value
      drop-probability value;
    }
  }
}

Hierarchy Level [edit class-of-service]

Description

Define drop profiles for RED.

For a packet to be dropped, it must match the drop profile. When a packet arrives, RED checks the queue fill level. If the fill level corresponds to a nonzero drop probability, the RED algorithm determines whether to drop the arriving packet.

Options

profile-name—Name of the drop profile.

The remaining statements are explained separately.

Usage Guidelines

See “Configure RED Drop Profiles” on page 601.

Required Privilege Level

interface—to view this statement in the configuration.
interface-control—to add this statement to the configuration.

exp-push-push-push

Syntax

exp-push-push-push default;

Hierarchy Level [edit class-of-service interfaces interface-name unit logical-unit-number rewrite-rules]

Description

For M-series routers, rewrite the EXP bits of all three labels of an outgoing packet, thereby maintaining CoS of an incoming non-MPLS packet.

Options

default—Apply the default MPLS EXP rewrite table.

Usage Guidelines

See “Rewrite the EXP Bits of All Three Labels of an Outgoing Packet” on page 607.

Required Privilege Level

interface—to view this statement in the configuration.
interface-control—to add this statement to the configuration.

See Also

exp-swap-push-push on page 630
exp-swap-push-push

Syntax
exp-swap-push-push default;

Hierarchy Level [edit class-of-service interfaces interface-name unit logical-unit-number rewrite-rules]

Description For M-series routers, rewrite the EXP bits of all three labels of an outgoing packet, thereby maintaining CoS of an incoming MPLS packet.

Options default—Apply the default MPLS EXP rewrite table.

Usage Guidelines See “Rewrite the EXP Bits of All Three Labels of an Outgoing Packet” on page 607.

Required Privilege Level interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

See Also exp-push-push-push on page 629

fabric

Syntax
fabric {
  scheduler-map {
    priority (low | high) scheduler scheduler-name;
  }
}

Hierarchy Level [edit class-of-service]

Description For T-series platforms only, associate a scheduler with a fabric priority. The statements are explained separately.

Usage Guidelines See “Associate a Scheduler with a Fabric Priority” on page 600.

Required Privilege Level interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

fill-level

fill-level (percentage)

Syntax
fill-level percentage;

Hierarchy Level [edit class-of-service drop-profiles profile-name]

Description When configuring RED, map the fullness of a queue to a drop probability.

Options percentage—How full the queue is, expressed as a percentage. To specify multiple fill levels, include multiple fill-level options. List the fill levels incrementally in increasing order.

Range: 0 through 100 percent

Usage Guidelines See “Configure RED Drop Profiles” on page 601.

Required Privilege Level interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
fill-level (interpolated value)

Syntax  fill-level value;

Hierarchy Level  [edit class-of-service drop-profile profile-name interpolate]

Description  Define up to 64 values for interpolating queue fill level.

Options  value—Data point for mapping queue fill percentage.
          Range: 0 through 100

Usage Guidelines  See “Configure RED Drop Profiles” on page 601.

Required Privilege Level  interface—To view this statement in the configuration.
                          interface-control—To add this statement to the configuration.

forwarding-class

forwarding-class (classifiers)

Syntax  forwarding-class class-name {
          loss-priority (low | high) code-points [ alias | bits ];
        }

Hierarchy Level  [edit class-of-service classifiers type classifier-name]

Description  Define forwarding class name and option values.

Options  class-name—Name of forwarding class.

          The remaining statements are explained separately.

Usage Guidelines  See “Classify Packets by Behavior Aggregate” on page 594.

Required Privilege Level  interface—To view this statement in the configuration.
                          interface-control—To add this statement to the configuration.
forwarding-class (forwarding policy)

Syntax
forwarding-class class-name {
  next-hop [ next-hop-name ];
  lsp-next-hop [ lsp-regular-expression ];
}

Hierarchy Level [edit class-of-service forwarding-policy next-hop-map map-name]

Description Define forwarding class name and associated next hops.

Options
class-name—Name of forwarding class.

The remaining statement is explained separately.

Usage Guidelines See “Configure CoS-Based Forwarding” on page 610.

Required Privilege Level
interface—to view this statement in the configuration.
interface-control—to add this statement to the configuration.

forwarding-classes

Syntax
forwarding-classes {
  queue queue-number class-name priority (low | high);
}

Hierarchy Level [edit class-of-service]

Description Associate forwarding class with queue name and number. For T-series platforms only, you can configure fabric priority queuing by including the priority statement at the [edit class-of-service forwarding-classes queue queue-number class-name] hierarchy level.

The statements are explained separately.

Usage Guidelines See “Configure Forwarding Classes” on page 592 and “Override Fabric Priority Queuing” on page 594.

Required Privilege Level
interface—to view this statement in the configuration.
interface-control—to add this statement to the configuration.
forwarding-policy

Syntax
forwarding-policy {
  next-hop-map map-name {
    forwarding-class class-name {
      next-hop [ next-hop-name ];
      lsp-next-hop [ lsp-regular-expression ];
    }
  }
  class class-name {
    classification-override {
      forwarding-class class-name;
    }
  }
}

Hierarchy Level [edit class-of-service]

Description Define CoS-based forwarding policy options.
The statements are explained separately.

Usage Guidelines See "Configure CoS-Based Forwarding" on page 610.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

import

import classifiers

Syntax import (classifier-name | default);

Hierarchy Level [edit class-of-service classifiers type classifier-name]

Description Specify a default or previously defined classifier to import.

Options classifier-name—Name of previously defined classifier mapping.

default—The default classifier mapping.

Usage Guidelines See "Classify Packets by Behavior Aggregate" on page 594.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.
import rewrite-rules

Syntax  import (rewrite-name | default);

Hierarchy Level  [edit class-of-service rewrite-rules type rewrite-name]

Description  Specify a default or previously defined rewrite-rules mapping to import.

Options  rewrite-name—Name of previously defined rewrite-rules mapping.
  default—The default rewrite-rules mapping.

Usage Guidelines  See “Rewrite Packet Header Information” on page 602.

Required Privilege Level  interface—To view this statement in the configuration.
  interface-control—To add this statement to the configuration.
interfaces

Syntax

```plaintext
interfaces {
    interface-name {
        scheduler-map map-name;
        unit logical-unit-number {
            classifiers {
                type (classifier-name | default);
            }
            forwarding-class class-name;
            rewrite-rules {
                type (rewrite-name | default);
            }
        }
    }
}
```

Hierarchy Level [edit class-of-service]

Description
Configure interface-specific CoS properties for incoming packets. Associate forwarding-class definition and RED mapping with an interface on the router.

Options
- interface-name—Name of the interface
- The remaining statements are explained separately.

Usage Guidelines
See "Classify Packets by Behavior Aggregate" on page 594 and "Rewrite Packet Header Information" on page 602.

Required Privilege Level
- interface—To view this statement in the configuration.
- interface-control—To add this statement to the configuration.

interpolate

Syntax

```plaintext
interpolate {
    fill-level value;
    drop-probability value;
}
```

Hierarchy Level [edit class-of-service drop-profiles profile-name]

Description
Specify values for interpolating relationship between queue fill level and drop probability.

The statements are explained separately.

Usage Guidelines
See "Configure RED Drop Profiles" on page 601.

Required Privilege Level
- interface—To view this statement in the configuration.
- interface-control—To add this statement to the configuration.
loss-priority

Syntax  loss-priority (low | high | any);

Hierarchy Level [edit class-of-service classifiers type classifier-name forwarding-class class-name],
[edit class-of-service schedulers scheduler-name drop-profile-map]

Description Specify packet loss priority value.

Options any—Use any loss priority.

low—Packet has low loss priority.

high—Packet has high loss priority.

Usage Guidelines See “Classify Packets by Behavior Aggregate” on page 594.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

lsp-next-hop

Syntax  lsp-next-hop [ lsp-regular-expression ];

Hierarchy Level [edit class-of-service forwarding-policy next-hop-map map-name forwarding-class class-name]

Description Specify the LSP regular expression to which to map forwarded traffic.

Options lsp-regular-expression—Next-hop LSP label.

Usage Guidelines See “Configure CoS-Based Forwarding” on page 610.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

next-hop

Syntax  next-hop [ next-hop-name ];

Hierarchy Level [edit class-of-service forwarding-policy next-hop-map map-name forwarding-class class-name]

Description Specify the next-hop name or address to which to map forwarded traffic.

Options next-hop-name—Next-hop alias or IP address.

Usage Guidelines See “Configure CoS-Based Forwarding” on page 610.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.
next-hop-map

Syntax
next-hop-map { 
  forwarding-class class-name { 
    next-hop next-hop-name; 
    lsp-next-hop [ lsp-regular-expression ]; 
  } 
}

Hierarchy Level [edit class-of-service forwarding-policy]

Description Specify the map for CoS forwarding routes.

Options map-name—Map that defines next-hop routes.

Usage Guidelines See “Configure CoS-Based Forwarding” on page 610.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

priority

priority (fabric queues)

Syntax priority (low | high) scheduler scheduler-name;

Hierarchy Level [edit class-of-service fabric scheduler-map]

Description For T-series platforms only, specify the fabric priority with which a scheduler is associated.

For a scheduler that you associate with a fabric priority, you cannot include the buffer-size, transmit-rate, or priority statements at the [edit class-of-service schedulers scheduler-name] hierarchy level.

Options low—Scheduler has low priority.
high—Scheduler has high priority.

The remaining statements are explained separately.

Usage Guidelines See “Associate a Scheduler with a Fabric Priority” on page 600.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.
priority (forwarding classes)

Syntax  
priority (low | high);

Hierarchy Level  
[edit class-of-service forwarding-classes queue queue-number class-name]

Description  
For T-series platforms only, specify packet priority value.

Options  
low—Forwarding class’s fabric queuing has low priority.

high—Forwarding class’s fabric queuing has high priority.

Usage Guidelines  
See “Override Fabric Priority Queuing” on page 594.

Required Privilege Level  
interface—to view this statement in the configuration.
interface-control—to add this statement to the configuration.

priority (.schedulers)

Syntax  
priority (low | high | strict-high);

Hierarchy Level  
[edit class-of-service schedulers scheduler-name]

Description  
Specify packet-scheduling priority value.

Options  
low—Scheduler has low priority.

high—Scheduler has high priority.

strict-high—Scheduler has strictly high priority. The queue receives precedence over all high-
and low-priority queues, as long as strictly high-priority traffic is waiting to be sent,
regardless of the strictly high-priority queue’s bandwidth credit.

Usage Guidelines  
See “Configure Scheduling Policy Maps” on page 596.

Required Privilege Level  
interface—to view this statement in the configuration.
interface-control—to add this statement to the configuration.
**protocol**

**protocol (interfaces rewrite rules)**

**Syntax**

```
protocol protocol-types;
```

**Hierarchy Level**

[edit class-of-service interfaces interface-name unit logical-unit-number rewrite-rules exp rewrite-name]

**Description**

Apply a rewrite rule to MPLS packets only, and write the code point value to MPLS headers only; or apply a rewrite rule to MPLS and IPv4 packets, and write the code point value to MPLS and IPv4 headers.

**Options**

`protocol-types` can be one of the following:

- `mpls-any`—Apply the rewrite rule to MPLS packets and writes the code point value to MPLS headers.
- `mpls-inet-both`—Apply the rewrite rule to VPN MPLS packets with IPv4 payloads. On T-series platforms, write the code point value to the MPLS and IPv4 headers. On M-series routers, initialize all ingress MPLS LSP packets with IPv4 payloads with 000 code points for IP precedence and MPLS EXP values.
- `mpls-inet-both-non-vpn`—Apply the rewrite rule to non-VPN MPLS packets with IPv4 payloads. On T-series platforms, write the code point value to the MPLS and IPv4 headers. On M-series routers, initialize all ingress MPLS LSP packets with IPv4 payloads with 000 code points for IP precedence and MPLS EXP values.

**Usage Guidelines**

See “Rewrite MPLS and IPv4 Packet Headers” on page 605.

**Required Privilege Level**

- `interface`—To view this statement in the configuration.
- `interface-control`—To add this statement to the configuration.

---

**protocol (schedulers)**

**Syntax**

```
protocol (non-tcp | tcp | any);
```

**Hierarchy Level**

[edit class-of-service schedulers scheduler-name drop-profile-map]

**Description**

Specify the protocol type for the specified scheduler.

**Options**

- `any`—Accept any protocol type.
- `non-tcp`—Accept any protocol type other than TCP/IP.
- `tcp`—Accept only TCP/IP protocol.

**Usage Guidelines**

See “Configure Scheduling Policy Maps” on page 596.

**Required Privilege Level**

- `interface`—To view this statement in the configuration.
- `interface-control`—To add this statement to the configuration.
queue

Syntax
queue queue-number class-name;

Hierarchy Level
[edit class-of-service forwarding classes]

Description
Specify the output transmission queue to which to map all input from an associated forwarding class.

Options
- class-name—Name of forwarding class.
- queue-number—Output queue number. Range: 0 through 65,535

Usage Guidelines
See “Configure Forwarding Classes” on page 592.

Required Privilege Level
interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

rewrite-rules

Syntax
rewrite-rules {
  type rewrite-name {
    import (rewrite-name | default);
    forwarding-class class-name {
      loss-priority (low | high) code-point (alias | bits);
    }
  }
}

Hierarchy Level
[edit class-of-service]

Description
Specify the rewrite-rules mapping for the entire traffic stream that passes through all queues on the interface.

Options
- rewrite-name—Name of the rewrite-rules mapping.
- type—Traffic type.
  Values: dscp, exp, inet-precedence

The remaining statements are explained separately.

Usage Guidelines
See “Rewrite Packet Header Information” on page 602.

Required Privilege Level
interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.
**rewrite-rules (interfaces)**

**Syntax**
```
rewrite-rules {
    dscp (rewrite-name | default);
    exp (rewrite-name | default) protocol protocol-types;
    exp-push-push-push default;
    exp-swap-push-push default;
    ieee-802.1 default;
    inet-precedence (rewrite-name | default);
}
```

**Hierarchy Level**
```
[edit class-of-service interfaces interface-name unit logical-unit-number]
```

**Description**
Associate a rewrite-rules configuration or default mapping with a specific interface.

**Options**
- `rewrite-name` — Name of the rewrite-rules mapping.
- `default` — The default mapping.

The remaining statements are explained separately.

**Usage Guidelines**
See “Rewrite Packet Header Information” on page 602.

**Required Privilege Level**
- `interface` — To view this statement in the configuration.
- `interface-control` — To add this statement to the configuration.

---

**scheduler**

**scheduler (scheduler map)**

**Syntax**
```
scheduler scheduler-name;
```

**Hierarchy Level**
```
[edit class-of-service scheduler-maps map-name]
```

**Description**
Associate a scheduler with a scheduler map.

**Options**
- `scheduler-name` — Name of the scheduler configuration block.

**Usage Guidelines**
See “Configure Scheduling Policy Maps” on page 596.

**Required Privilege Level**
- `interface` — To view this statement in the configuration.
- `interface-control` — To add this statement to the configuration.
scheduler (fabric queues)

Syntax: `scheduler scheduler-name;`

Hierarchy Level: `[edit class-of-service fabric scheduler-map priority (low | high)]`

Description: For T-series platforms only, specify a scheduler to be associated with a fabric queue. For fabric CoS configuration, schedulers are restricted to transmit rates and drop profiles.

Options: `scheduler-name`—Name of the scheduler configuration block.

Usage Guidelines: See “Associate a Scheduler with a Fabric Priority” on page 600.

Required Privilege Level: `interface`—To view this statement in the configuration.
`interface-control`—To add this statement to the configuration.

scheduler-map

scheduler-map (fabric queues)

Syntax: `scheduler-map priority (low | high) scheduler scheduler-name;`

Hierarchy Level: `[edit class-of-service fabric]`

Description: For T-series platforms only, associate a scheduler with a fabric priority. The statements are explained separately.

Usage Guidelines: See “Associate a Scheduler with a Fabric Priority” on page 600.

Required Privilege Level: `interface`—To view this statement in the configuration.
`interface-control`—To add this statement to the configuration.

scheduler-map (interfaces)

Syntax: `scheduler-map map-name;`

Hierarchy Level: `[edit class-of-service interfaces interface-name], [edit class-of-service interfaces interface-name unit logical-unit-number]`

Description: Associate a scheduler map name with an interface. For Channelized OC-12 QPP, Channelized T3 QPP, Channelized E1 QPP, and Gigabit Ethernet QPP interfaces only, you can associate a scheduler map name with a logical interface.

Options: `map-name`—Name of the scheduler map.

Usage Guidelines: See “Configure Scheduling Policy Maps” on page 596.

Required Privilege Level: `interface`—To view this statement in the configuration.
`interface-control`—To add this statement to the configuration.
scheduler-maps

Syntax

```
scheduler-maps {
  map-name {
    forwarding-class class-name scheduler scheduler-name;
  }
}
```

Hierarchy Level  [edit class-of-service]

Description Specify scheduler map name and associate it with the scheduler configuration and forwarding class.

Options map-name—Name of the scheduler map.

The remaining statements are explained separately.

Usage Guidelines See “Configure Scheduling Policy Maps” on page 596.

Required Privilege Level  interface—To view this statement in the configuration.
  interface-control—To add this statement to the configuration.

.schedulers

Syntax

```
schedulers {
  scheduler-name {
    buffer-size (seconds | percent | percentage | remainder | temporal microseconds);
    drop-profile-map loss-priority (low | high) protocol (non-tcp | tcp | any)
      drop-profile profile-name;
    priority (low | high | strict-high);
    transmit-rate (rate | percent | percentage | remainder | exact);
  }
}
```

Hierarchy Level  [edit class-of-service]

Description Specify scheduler name and parameter values.

Options scheduler-name—Name of the scheduler to be configured.

The remaining statements are explained separately.

Usage Guidelines See “Configure Scheduling Policy Maps” on page 596.

Required Privilege Level  interface—To view this statement in the configuration.
  interface-control—To add this statement to the configuration.
transmit-rate

Syntax: transmit-rate (rate | percent percentage | remainder | exact);

Hierarchy Level: [edit class-of-service schedulers scheduler-name]

Description: Specify the transmit rate or percentage for a scheduler.

Options:
- exact—Enforce the exact transmission rate.
- rate—Transmission rate, in bits per second.
- remainder—Use remaining rate available.
- percent percentage—Transmission percentage.
  Range: 0 through 100 percent

Usage Guidelines: See “Configure Scheduling Policy Maps” on page 596.

Required Privilege Level:
- interface—to view this statement in the configuration.
- interface-control—to add this statement to the configuration.

unit

Syntax:

unit logical-unit-number {
  classifiers {
    type (classifier-name | default);
  }
  forwarding-class class-name;
  rewrite-rules {
    type (rewrite-name | default);
  }
}

Hierarchy Level: [edit class-of-service interfaces interface-name]

Description: Configure a logical interface on the physical device. You must configure a logical interface to be able to use the physical device.

Options:
- logical-unit-number—Number of the logical unit.
  Range: 0 through 16,384

The remaining statements are explained separately.

Usage Guidelines: See “Classify Packets by Behavior Aggregate” on page 594 and “Rewrite Packet Header Information” on page 602.

Required Privilege Level:
- interface—to view this statement in the configuration.
- interface-control—to add this statement to the configuration.
Part 5
Appendix

- Glossary on page 647
## Glossary

### A

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAL</td>
<td>ATM adaptation layer. A series of protocols enabling various types of traffic, including voice, data, image, and video, to run over an ATM network.</td>
</tr>
<tr>
<td>active route</td>
<td>Route chosen from all routes in the routing table to reach a destination. Active routes are installed into the forwarding table.</td>
</tr>
<tr>
<td>add/drop multiplexer</td>
<td>See ADM.</td>
</tr>
<tr>
<td>Address Resolution Protocol</td>
<td>See ARP.</td>
</tr>
<tr>
<td>adjacency</td>
<td>Portion of the local routing information that pertains to the reachability of a single neighbor over a single circuit or interface.</td>
</tr>
<tr>
<td>ADM</td>
<td>Add/drop multiplexer. SONET functionality that allows lower-level signals to be dropped from a high-speed optical connection.</td>
</tr>
<tr>
<td>aggregation</td>
<td>Combination of groups of routes that have common addresses into a single entry in the routing table.</td>
</tr>
<tr>
<td>AH</td>
<td>Authentication Header. A component of the IPSec protocol used to verify that the contents of a packet have not been changed, and to validate the identity of the sender. See also ESP.</td>
</tr>
<tr>
<td>ANSI</td>
<td>American National Standards Institute. The United States’ representative to the ISO.</td>
</tr>
<tr>
<td>APQ</td>
<td>Alternate Priority Queuing. Dequeueing method that has a special queue, similar to SPQ, which is visited only 50 percent of the time. The packets in the special queue still have a predictable latency, although the upper limit of the delay is higher than that with SPQ. Since the other configured queues share the remaining 50 percent of the service time, queue starvation is usually avoided. See also SPQ.</td>
</tr>
<tr>
<td>APS</td>
<td>Automatic Protection Switching. Technology used by SONET ADMs to protect against circuit faults between the ADM and a router and to protect against failing routers.</td>
</tr>
<tr>
<td>area</td>
<td>Routing subdomain that maintains detailed routing information about its own internal composition and that maintains routing information that allows it to reach other routing subdomains. In IS-IS, an area corresponds to a Level 1 subdomain. In IS-IS and OSPF, a set of contiguous networks and hosts within an autonomous system that have been administratively grouped together.</td>
</tr>
<tr>
<td>area border router</td>
<td>Router that belongs to more than one area. Used in OSPF.</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>ARP</strong></td>
<td>Address Resolution Protocol. Protocol for mapping IP addresses to MAC addresses.</td>
</tr>
<tr>
<td><strong>AS</strong></td>
<td>Autonomous system. Set of routers under a single technical administration. Each AS normally uses a single interior gateway protocol (IGP) and metrics to propagate routing information within the set of routers. Also called routing domain.</td>
</tr>
<tr>
<td><strong>AS boundary router</strong></td>
<td>In OSPF, routers that exchange routing information with routers in other ASs.</td>
</tr>
<tr>
<td><strong>AS external link advertisements</strong></td>
<td>OSPF link-state advertisement sent by AS boundary routers to describe external routes that they know. These link-state advertisements are flooded throughout the AS (except for stub areas).</td>
</tr>
<tr>
<td><strong>AS path</strong></td>
<td>In BGP, the route to a destination. The path consists of the AS numbers of all routers a packet must go through to reach a destination.</td>
</tr>
<tr>
<td><strong>ASIC</strong></td>
<td>Application-specific integrated circuit. Specialized processors that perform specific functions on the router.</td>
</tr>
<tr>
<td><strong>ATM</strong></td>
<td>Asynchronous Transfer Mode. A high-speed multiplexing and switching method utilizing fixed-length cells of 53 octets to support multiple types of traffic.</td>
</tr>
<tr>
<td><strong>atomic</strong></td>
<td>Smallest possible operation. An atomic operation is performed either entirely or not at all. For example, if machine failure prevents a transaction from completing, the system is rolled back to the start of the transaction, with no changes taking place.</td>
</tr>
<tr>
<td><strong>Authentication Header</strong></td>
<td>See AH.</td>
</tr>
<tr>
<td><strong>Automatic Protection Switching</strong></td>
<td>See APS.</td>
</tr>
<tr>
<td><strong>autonomous system</strong></td>
<td>See AS.</td>
</tr>
<tr>
<td><strong>autonomous system boundary router</strong></td>
<td>In OSPF, routers that exchange routing information with routers in other ASs.</td>
</tr>
<tr>
<td><strong>autonomous system external link advertisements</strong></td>
<td>OSPF link-state advertisement sent by autonomous system boundary routers to describe external routes that they know. These link-state advertisements are flooded throughout the autonomous system (except for stub areas).</td>
</tr>
<tr>
<td><strong>autonomous system path</strong></td>
<td>In BGP, the route to a destination. The path consists of the autonomous system numbers of all the routers a packet must pass through to reach a destination.</td>
</tr>
<tr>
<td><strong>backbone area</strong></td>
<td>In OSPF, an area that consists of all networks in area ID 0.0.0.0, their attached routers, and all area border routers.</td>
</tr>
<tr>
<td><strong>backplane</strong></td>
<td>On an M40 router, component of the Packet Forwarding Engine that distributes power, provides signal connectivity, manages shared memory on FPCs, and passes outgoing data cells to FPCs.</td>
</tr>
<tr>
<td><strong>bandwidth</strong></td>
<td>The range of transmission frequencies a network can use, expressed as the difference between the highest and lowest frequencies of a transmission channel. In computer networks, greater bandwidth indicates faster data-transfer rate capacity.</td>
</tr>
<tr>
<td><strong>Bellcore</strong></td>
<td>Bell Communications Research. Research and development organization created after the divestiture of the Bell System. It is supported by the regional Bell holding companies (RBHCs), which own the regional Bell operating companies (RBOCs).</td>
</tr>
<tr>
<td>Term</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>BERT</strong></td>
<td>Bit error rate test. A test that can be run on a T3 interface to determine whether it is operating properly.</td>
</tr>
<tr>
<td><strong>BGP</strong></td>
<td>Border Gateway Protocol. Exterior gateway protocol used to exchange routing information among routers in different autonomous systems.</td>
</tr>
<tr>
<td><strong>bit error rate test</strong></td>
<td>See BERT.</td>
</tr>
<tr>
<td><strong>BITS</strong></td>
<td>Building Integrated Timing Source. Dedicated timing source that synchronizes all equipment in a particular building.</td>
</tr>
<tr>
<td><strong>Border Gateway Protocol</strong></td>
<td>See BGP.</td>
</tr>
<tr>
<td><strong>broadcast</strong></td>
<td>Operation of sending network traffic from one network node to all other network nodes.</td>
</tr>
<tr>
<td><strong>bundle</strong></td>
<td>Collection of software that makes up a JUNOS software release.</td>
</tr>
<tr>
<td><strong>CB</strong></td>
<td>Control Board. Part of the host subsystem that provides control and monitoring functions for router components.</td>
</tr>
<tr>
<td><strong>CCC</strong></td>
<td>Circuit cross-connect. A JUNOS software feature that allows you to configure transparent connections between two circuits, where a circuit can be a Frame Relay DLCI, an ATM VC, a PPP interface, a Cisco HDLC interface, or an MPLS label-switched path (LSP).</td>
</tr>
<tr>
<td><strong>CE device</strong></td>
<td>Customer edge device. Router or switch in the customer's network that is connected to a service provider's provider edge (PE) router and participates in a Layer 3 VPN.</td>
</tr>
<tr>
<td><strong>CFM</strong></td>
<td>Cubic feet per minute. Measure of air flow in volume per minute.</td>
</tr>
<tr>
<td><strong>Challenge Handshake Authentication Protocol</strong></td>
<td>See CHAP.</td>
</tr>
<tr>
<td><strong>channel service unit</strong></td>
<td>See CSU/DSU.</td>
</tr>
<tr>
<td><strong>CHAP</strong></td>
<td>A protocol that authenticates remote users. CHAP is a server-driven, three-step authentication mechanism that depends on a shared secret password that resides on both the server and the client.</td>
</tr>
<tr>
<td><strong>CIDR</strong></td>
<td>Classless interdomain routing. A method of specifying Internet addresses in which you explicitly specify the bits of the address to represent the network address instead of determining this information from the first octet of the address.</td>
</tr>
<tr>
<td><strong>CIP</strong></td>
<td>Connector Interface Panel. On an M160 router, the panel that contains connectors for the Routing Engines, BITS interfaces, and alarm relay contacts.</td>
</tr>
<tr>
<td><strong>circuit cross-connect</strong></td>
<td>See CCC.</td>
</tr>
<tr>
<td><strong>class of service</strong></td>
<td>See CoS.</td>
</tr>
<tr>
<td><strong>CLEC</strong></td>
<td>(Pronounced “see-lek”) Competitive Local Exchange Carrier. Company that competes with the already established local telecommunications business by providing its own network and switching.</td>
</tr>
<tr>
<td><strong>CLEI</strong></td>
<td>Common language equipment identifier. Inventory code used to identify and track telecommunications equipment.</td>
</tr>
</tbody>
</table>
CLI  Command-line interface. Interface provided for configuring and monitoring the routing protocol software.

client peer  In a BGP route reflection, a member of a cluster that is not the route reflector. See also nonclient peer.

CLNP  Connectionless Network Protocol. ISO-developed protocol for OSI connectionless network service. CLNP is the OSI equivalent of IP.

cluster  In BGP, a set of routers that have been grouped together. A cluster consists of one system that acts as a route reflector, along with any number of client peers. The client peers receive their route information only from the route reflector system. Routers in a cluster do not need to be fully meshed.

community  In BGP, a group of destinations that share a common property. Community information is included as one of the path attributes in BGP update messages.

confederation  In BGP, a group of systems that appears to external autonomous systems to be a single autonomous system.

constrained path  In traffic engineering, a path determined using RSVP signaling and constrained using CSPF. The ERO carried in the packets contains the constrained path information.

core  The central backbone of the network.

CoS  Class of service. The method of classifying traffic on a packet-by-packet basis using information in the ToS byte to provide different service levels to different traffic.

CPE  Customer premises equipment. Telephone or other service provider equipment located at a customer site.

craft interface  Mechanisms used by a Communication Workers of America craftsperson to operate, administer, and maintain equipment or provision data communications. On a Juniper Networks router, the craft interface allows you to view status and troubleshooting information and perform system control functions.

CSCP  Class Selector Codepoint.

CSNP  Complete sequence number PDU. Packet that contains a complete list of all the LSPs in the IS-IS database.

CSPF  Constrained Shortest Path First. An MPLS algorithm that has been modified to take into account specific restrictions when calculating the shortest path across the network.

CSU/DSU  Channel service unit/data service unit. Channel service unit connects a digital phone line to a multiplexer or other digital signal device. Data service unit connects a DTE to a digital phone line.

customer edge device  See CE device.

daemon  Background process that performs operations on behalf of the system software and hardware. Daemons normally start when the system software is booted, and they run as long as the software is running. In the JUNOS software, daemons are also referred to as processes.
damping  Method of reducing the number of update messages sent between BGP peers, thereby reducing the load on these peers without adversely affecting the route convergence time for stable routes.

data circuit-terminating equipment  See DCE.

data-link connection identifier  See DLCI.

data service unit  See CSU/DSU.

Data Terminal Equipment  See DTE.

dcd  The JUNOS software interface process (daemon).

dense wavelength-division multiplexing  See DWDM.

designated router  In OSPF, a router selected by other routers that is responsible for sending link-state advertisements that describe the network, which reduces the amount of network traffic and the size of the routers' topological databases.

destination prefix length  Number of bits of the network address used for host portion of a CIDR IP address.

DHCP  Dynamic Host Configuration Protocol. Allocates IP addresses dynamically so that they can be reused when they are no longer needed.

Diffie-Hellman  A public key scheme, invented by Whitfield Diffie and Martin Hellman, used for sharing a secret key without communicating secret information, thus precluding the need for a secure channel. Once correspondents have computed the secret shared key, they can use it to encrypt communications.

DiffServ  Differentiated Service (based on RFC 2474). DiffServ uses the ToS byte to identify different packet flows on a packet-by-packet basis. DiffServ adds a Class Selector Codepoint (CSCP) and a Differentiated Services Codepoint (DSCP).

Dijkstra algorithm  See SPF.

DIMM  Dual inline memory module. 168-pin memory module that supports 64-bit data transfer.

direct routes  See interface routes.

DLCI  Data-link connection identifier. Identifier for a Frame Relay virtual connection (also called a logical interface).
DoS  Denial of service. System security breach in which network services become unavailable to users.

DRAM  Dynamic random-access memory. Storage source on the router that can be accessed quickly by a process.

drop profile  Drop probabilities for different levels of buffer fullness that are used by RED to determine from which queue to drop packets.

DSCP  Differentiated Services Codepoint.

DSU  Data service unit. A device used to connect a DTE to a digital phone line. Converts digital data from a router to voltages and encoding required by the phone line. See also CSU/DSU.

DTE  Data Terminal Equipment. RS-232-C interface that a computer uses to exchange information with a serial device.

DVMRP  Distance Vector Multicast Routing Protocol. Distributed multicast routing protocol that dynamically generates IP multicast delivery trees using a technique called reverse path multicasting (RPM) to forward multicast traffic to downstream interfaces.

DWDM  Dense wavelength-division multiplexing. Technology that enables data from different sources to be carried together on an optical fiber, with each signal carried on its own separate wavelength.

Dynamic Host Configuration Protocol  See DHCP.

EBGP  External BGP. BGP configuration in which sessions are established between routers in different ASs.

ECSA  Exchange Carriers Standards Association. A standards organization created after the divestiture of the Bell System to represent the interests of interexchange carriers.

edge router  In MPLS, a router located at the beginning or end of a label-switching tunnel. When at the beginning of a tunnel, an edge router applies labels to new packets entering the tunnel. When at the end of a tunnel, the edge router removes labels from packets exiting the tunnel. See also MPLS.

EGP  Exterior gateway protocol, such as BGP.

egress router  In MPLS, last router in a label-switched path (LSP). See also ingress router.

EIA  Electronic Industries Association. A United States trade group that represents manufacturers of electronics devices and sets standards and specifications.

EMI  Electromagnetic interference. Any electromagnetic disturbance that interrupts, obstructs, or otherwise degrades or limits the effective performance of electronics or electrical equipment.

encapsulating security payload  See ESP.

end system  In IS-IS, network entity that sends and receives packets.

ERO  Explicit Route Object. Extension to RSVP that allows an RSVP PATH message to traverse an explicit sequence of routers that is independent of conventional shortest-path IP routing.
Glossary

ESP  Encapsulating security payload. A fundamental component of IPSec-compliant VPNs, ESP specifies an IP packet's encryption, data integrity checks, and sender authentication, which are added as a header to the IP packet. See also AH.

explicit path  See signaled path.

Explicit Route Object  See ERO.

export  To place routes from the routing table into a routing protocol.

external BGP  See EBGP.

external metric  A cost included in a route when OSPF exports route information from external autonomous systems. There are two types of external metrics: Type 1 and Type 2. Type 1 external metrics are equivalent to the link-state metric; that is, the cost of the route, used in the internal autonomous system. Type 2 external metrics are greater than the cost of any path internal to the autonomous system.

fast reroute  Mechanism for automatically rerouting traffic on an LSP if a node or link in an LSP fails, thus reducing the loss of packets traveling over the LSP.

FEAC  Far-end alarm and control. T3 signal used to send alarm or status information from the far-end terminal back to the near-end terminal and to initiate T3 loopbacks at the far-end terminal from the near-end terminal.

FEB  Forwarding Engine Board. In M5 and M10 routers, provides route lookup, filtering, and switching to the destination port.

firewall  A security gateway positioned between two different networks, usually between a trusted network and the Internet. A firewall ensures that all traffic that crosses it conforms to the organization's security policy. Firewalls track and control communications, deciding whether to pass, reject, discard, encrypt, or log them. Firewalls also can be used to secure sensitive portions of a local network.

FIFO  First in, first out.

flap damping  See damping.

flapping  See route flapping.

Flexible PIC Concentrator  See FPC.

Forwarding Engine Board  See FEB.

forwarding information base  See forwarding table.

forwarding table  JUNOS software forwarding information base (FIB). The JUNOS routing protocol process installs active routes from its routing tables into the Routing Engine forwarding table. The kernel copies this forwarding table into the Packet Forwarding Engine, which is responsible for determining which interface transmits the packets.

FPC  Flexible PIC Concentrator. An interface concentrator on which PICs are mounted. An FPC inserts into a slot in a Juniper Networks router. See also PIC.
| **FRU** | Field-replaceable unit. Router component that customers can replace onsite. |
| **group** | A collection of related BGP peers. |
| **hash** | A one-way function that takes a message of any length and produces a fixed-length digest. In security, a message digest is used to validate that the contents of a message have not been altered in transit. The Secure Hash Algorithm (SHA-1) and Message Digest 5 (MD5) are commonly used hashes. |
| **Hashed Message Authentication Code** | See HMAC. |
| **HDLC** | High-level data link control. An International Telecommunication Union (ITU) standard for a bit-oriented data link layer protocol on which most other bit-oriented protocols are based. |
| **HMAC** | Hashed Message Authentication Code. A mechanism for message authentication that uses cryptographic hash functions. HMAC can be used with any iterative cryptographic hash function—for example, MD5 or SHA-1—in combination with a secret shared key. The cryptographic strength of HMAC depends on the properties of the underlying hash function. |
| **hold time** | Maximum number of seconds allowed to elapse between the time a BGP system receives successive keepalive or update messages from a peer. |
| **host module** | On an M160 router, provides routing and system management functions of the router. Consists of the Routing Engine and Miscellaneous Control Subsystem (MCS). |
| **host subsystem** | Provides routing and system-management functions of the router. Consists of a Routing Engine and an adjacent Control Board (CB). |
| **IANA** | Internet Assigned Numbers Authority. Regulatory group that maintains all assigned and registered Internet numbers, such as IP and multicast addresses. See also NIC. |
| **IBGP** | Internal BGP. BGP configuration in which sessions are established between routers in the same ASs. |
| **ICMP** | Internet Control Message Protocol. Used in router discovery, ICMP allows router advertisements that enable a host to discover addresses of operating routers on the subnet. |
| **IDE** | Integrated Drive Electronics. Type of hard disk on the Routing Engine. |
| **IEC** | International Electrotechnical Commission. See ISO. |
| **IEEE** | Institute of Electronic and Electrical Engineers. International professional society for electrical engineers. |
| **IETF** | Internet Engineering Task Force. International community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet. |
| **IGMP** | Internet Group Membership Protocol. Used with multicast protocols to determine whether group members are present. |
| **IGP** | Interior gateway protocol, such as IS-IS, OSPF, and RIP. |
IKE Internet Key Exchange. The key management protocol used in IPSec. IKE combines the ISAKMP and Oakley protocols to create encryption keys and security associations.

import To install routes from the routing protocols into a routing table.

ingress router In MPLS, first router in a label-switched path (LSP). See also egress router.

inter-AS routing Routing of packets among different ASs. See also EBGP.

intercluster reflection In a BGP route reflection, the redistribution of routing information by a route reflector system to all nonclient peers (BGP peers not in the cluster). See also route reflection.

interface routes Routes that are in the routing table because an interface has been configured with an IP address. Also called direct routes.

intermediate system In IS-IS, network entity that sends and receives packets and that can also route packets.

internal BGP See IBGP.

Internet Key Exchange See IKE.

Internet Protocol Security See IPSec.

Internet Security Association and Key Management Protocol See ISAKMP.

intra-AS routing The routing of packets within a single AS. See also IBGP.

IP Internet Protocol. The protocol used for sending data from one point to another on the Internet.

IPSec Internet Protocol Security. The industry standard for establishing VPNs. IPSec comprises a group of protocols and algorithms that provide authentication and encryption of data across IP-based networks.

ISAKMP Internet Security Association and Key Management Protocol. A protocol that allows the receiver of a message to obtain a public key and use digital certificates to authenticate the sender's identity. ISAKMP is designed to be key exchange independent; that is, it supports many different key exchanges. See also IKE and Oakley.

IS-IS Intermediate System-to-Intermediate System protocol. Link-state, interior gateway routing protocol for IP networks that also uses the shortest-path first (SPF) algorithm to determine routes.

ISO International Organization for Standardization. Worldwide federation of standards bodies that promotes international standardization and publishes international agreements as International Standards.

ISP Internet service provider. Company that provides access to the Internet and related services.

ITU International Telecommunications Union (formerly known as the CCITT). Group supported by the United Nations that makes recommendations and coordinates the development of telecommunications standards for the entire world.
jitter Small random variation introduced into the value of a timer to prevent multiple timer expirations from becoming synchronized.

kernel forwarding table See forwarding table.

label In MPLS, 20-bit unsigned integer in the range 0 through 1048575, used to identify a packet traveling along an LSP.

label-switched path (LSP) Sequence of routers that cooperatively perform MPLS operations for a packet stream. The first router in an LSP is called the ingress router, and the last router in the path is called the egress router. An LSP is a point-to-point, half-duplex connection from the ingress router to the egress router. (The ingress and egress routers cannot be the same router.)

label switching See MPLS.

label-switching router See LSR.

link Communication path between two neighbors. A link is up when communication is possible between the two end points.

link-state PDU (LSP) Packets that contain information about the state of adjacencies to neighboring systems.

local preference Optional BGP path attribute carried in internal BGP update packets that indicates the degree of preference for an external route.

loose In the context of traffic engineering, a path that can use any route or any number of other intermediate (transit) points to reach the next address in the path. (Definition from RFC 791, modified to fit LSPs.)

LSP See label-switched path (LSP) or link-state PDU (LSP).

LSR Label-switching router. A router on which MPLS and RSVP are enabled and is thus capable of processing label-switched packets.

martian address Network address about which all information is ignored.

mask See subnet mask.

MBGP Multiprotocol BGP. An extension to BGP that allows you to connect multicast topologies within and between BGP ASs.

MBone Internet multicast backbone. An interconnected set of subnetworks and routers that support the delivery of IP multicast traffic. The MBone is a virtual network that is layered on top of sections of the physical Internet.

MCS Miscellaneous Control Subsystem. On an M160 router, provides control and monitoring functions for router components and SONET clocking for the router.

MD5 Message Digest 5. A one-way hashing algorithm that produces a 128-bit hash. It is used in AH and ESP. See also SHA-1.

MDRR Modified Deficit Round Robin. A method for selecting queues to be serviced.
MED  Multiple exit discriminator. Optional BGP path attribute consisting of a metric value that is used to determine the exit point to a destination when all other factors in determining the exit point are equal.

mesh  Network topology in which devices are organized in a manageable, segmented manner with many, often redundant, interconnections between network nodes.

Message Digest 5  See MD5.

MIB  Management Information Base. Definition of an object that can be managed by SNMP.

midplane  Forms the rear of the PIC cage on M5 and M10 routers and the FPC card cage on M20 and M160 routers. Provides data transfer, power distribution, and signal connectivity.

Miscellaneous Control Subsystem  See MCS.

MPLS  Multiprotocol Label Switching. Mechanism for engineering network traffic patterns that functions by assigning to network packets short labels that describe how to forward them through the network. Also called label switching. See also traffic engineering.

MTBF  Mean time between failure. Measure of hardware component reliability.

MTU  Maximum transfer unit. Limit on segment size for a network.

multicast  Operation of sending network traffic from one network node to multiple network nodes.

multicast distribution tree  The data path between the sender (host) and the multicast group member (receiver or listener).

multiprotocol BGP  See MBGP.

Multiprotocol Label Switching  See MPLS.

N  neighbor  Adjacent system reachable by traversing a single subnetwork. An immediately adjacent router. Also called a peer.

NET  Network entity title. Network address defined by the ISO network architecture and used in CLNS-based networks.

network layer reachability information  See NLRI.

network link advertisement  An OSPF link-state advertisement flooded throughout a single area by designated routers to describe all routers attached to the network.

Network Time Protocol  See NTP.

NIC  Network Information Center. Internet authority responsible for assigning Internet-related numbers, such as IP addresses and autonomous system numbers. See also IANA.

NLRI  Network layer reachability information. Information that is carried in BGP packets and is used by MBGP.
nonclient peer  In a BGP route reflection, a BGP peer that is not a member of a cluster. See also client peer.

not-so-stubby area  See NSSA.

NSAP  Network service access point. Connection to a network that is identified by a network address.

n-selector  Last byte of an nonclient peer address.

NSSA  Not-so-stubby area. In OSPF, a type of stub area in which external routes can be flooded.

NTP  Network Time Protocol. Protocol used to synchronize computer clock times on a network.

Oakley  A key determination protocol based on the Diffie-Hellman algorithm that provides added security, including authentication. Oakley was the key-exchange algorithm mandated for use with the initial version of ISAKMP, although various algorithms can be used. Oakley describes a series of key exchanges called “modes” and details the services provided by each; for example, Perfect Forward Secrecy for keys, identity protection, and authentication. See also ISAKMP.

OC  Optical Carrier. In SONET, Optical Carrier levels indicate the transmission rate of digital signals on optical fiber.

OSI  Open System Interconnection. Standard reference model for how messages are transmitted between two points on a network.

OSPF  Open Shortest Path First. A link-state IGP that makes routing decisions based on the shortest-path-first (SPF) algorithm (also referred to as the Dijkstra algorithm).

package  A collection of files that make up a JUNOS software component.

Packet Forwarding Engine  The architectural portion of the router that processes packets by forwarding them between input and output interfaces.

path attribute  Information about a BGP route, such as the route origin, AS path, and next-hop router.


PCMCIA  Personal Computer Memory Card International Association. Industry group that promotes standards for credit card-size memory or I/O devices.

PDU  Protocol data unit. IS-IS packets.

PE router  Provider edge router. A router in the service provider’s network that is connected to a customer edge (CE) device and that participates in a Virtual Private Network (VPN).

PEC  Policing Equivalence Classes. In traffic policing, a set of packets that is treated the same by the packet classifier.

peer  An immediately adjacent router with which a protocol relationship has been established. Also called a neighbor.

Perfect Forward Secrecy  See PFS.
PFE  See Packet Forwarding Engine.

PFS  A condition derived from an encryption system that changes encryption keys often and ensures that no two sets of keys have any relation to each other. The advantage of PFS is that if one set of keys is compromised, only communications using those keys are at risk. An example of a system that uses PFS is Diffie-Hellman.

**Physical Interface Card**  See PIC.

PIC  Physical Interface Card. A network interface–specific card that can be installed on an FPC in the router.

PIM  Protocol Independent Multicast. A protocol-independent multicast routing protocol. PIM Sparse Mode routes to multicast groups that might span wide-area and interdomain internets. PIM Dense Mode is a flood-and-prune protocol.

PLP  Packet Loss Priority.

PLP bit  Packet Loss Priority bit. Used to identify packets that have experienced congestion or are from a transmission that exceeded a service provider’s customer service license agreement. This bit can be used as part of a router’s congestion control mechanism and can be set by the interface or by a filter.

policing  Applying rate limits on bandwidth and burst size for traffic on a particular interface.

pop  Removal of the last label, by a router, from a packet as it exits an MPLS domain.

PPP  Point-to-Point Protocol. Link-layer protocol that provides multiprotocol encapsulation. It is used for link-layer and network-layer configuration.

precedence bits  The first three bits in the ToS byte. On a Juniper Networks router, these bits are used to sort or classify individual packets as they arrive at an interface. The classification determines the queue to which the packet is directed upon transmission.

preference  Desirability of a route to become the active route. A route with a lower preference value is more likely to become the active route. The preference is an arbitrary value in the range 0 through 255 that the routing protocol process uses to rank routes received from different protocols, interfaces, or remote systems.

preferred address  On an interface, the default local address used for packets sourced by the local router to destinations on the subnet.

primary address  On an interface, the address used by default as the local address for broadcast and multicast packets sourced locally and sent out the interface.

primary interface  Router interface that packets go out when no interface name is specified and when the destination address does not imply a particular outgoing interface.

Protocol-Independent Multicast  See PIM.

provider edge router  See PE router.

provider router  Router in the service provider’s network that does not attach to a customer edge (CE) device.

PSNP  Partial sequence number PDU. Packet that contains only a partial list of the LSPs in the IS-IS link-state database.
**push**  Addition of a label or stack of labels, by a router, to a packet as it enters an MPLS domain.

**QoS**  Quality of service. Performance, such as transmission rates and error rates, of a communications channel or system.

**quality of service**  See QoS.

**RADIUS**  Remote Authentication Dial-In User Service. Authentication method for validating users who attempt to access the router using Telnet.

**Random Early Detection**  See RED.

**rate limiting**  See policing.

**RBOC**  (Pronounced “are-bock”) Regional Bell operating company. Regional telephone companies formed as a result of the divestiture of the Bell System.

**RDRAM**  RAMBUS dynamic random access memory.

**RED**  Random Early Detection. Gradual drop profile for a given class that is used for congestion avoidance. RED tries to anticipate incipient congestion and reacts by dropping a small percentage of packets from the head of the queue to ensure that a queue never actually becomes congested.

**Rendezvous Point**  See RP.

**Resource Reservation Protocol**  See RSVP.

**RFC**  Request for Comments. Internet standard specifications published by the Internet Engineering Task Force.

**RFI**  Radio frequency interference. Interference from high-frequency electromagnetic waves emanating from electronic devices.

**RIP**  Routing Information Protocol. Distance-vector interior gateway protocol that makes routing decisions based on hop count.

**route flapping**  Situation in which BGP systems send an excessive number of update messages to advertise network reachability information.

**route identifier**  IP address of the router from which a BGP, IGP, or OSPF packet originated.

**route reflection**  In BGP, configuring a group of routers into a cluster and having one system act as a route reflector, redistributing routes from outside the cluster to all routers in the cluster. Routers in a cluster do not need to be fully meshed.

**router link advertisement**  OSPF link-state advertisement flooded throughout a single area by all routers to describe the state and cost of the router’s links to the area.

**routing domain**  See AS.
<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Routing Engine</strong></td>
<td>Architectural portion of the router that handles all routing protocol processes, as well as other software processes that control the router’s interfaces, some of the chassis components, system management, and user access to the router.</td>
</tr>
<tr>
<td><strong>routing instance</strong></td>
<td>A collection of routing tables, interfaces, and routing protocol parameters. The set of interfaces belongs to the routing tables and the routing protocol parameters control the information in the routing tables.</td>
</tr>
<tr>
<td><strong>routing table</strong></td>
<td>Common database of routes learned from one or more routing protocols. All routes are maintained by the JUNOS routing protocol process.</td>
</tr>
<tr>
<td><strong>RP</strong></td>
<td>For PIM-SM, a core router acting as the root of the distribution tree in a shared tree.</td>
</tr>
<tr>
<td><strong>rpd</strong></td>
<td>JUNOS software routing protocol process (daemon). User-level background process responsible for starting, managing, and stopping the routing protocols on a Juniper Networks router.</td>
</tr>
<tr>
<td><strong>RPM</strong></td>
<td>Reverse path multicasting. Routing algorithm used by DVMRP to forward multicast traffic.</td>
</tr>
<tr>
<td><strong>SA</strong></td>
<td>Security association. An IPSec term that describes an agreement between two parties about what rules to use for authentication and encryption algorithms, key exchange mechanisms, and secure communications.</td>
</tr>
<tr>
<td><strong>SAP</strong></td>
<td>Session Announcement Protocol. Used with multicast protocols to handle session conference announcements.</td>
</tr>
<tr>
<td><strong>SAR</strong></td>
<td>Segmentation and reassembly. Buffering used with ATM.</td>
</tr>
<tr>
<td><strong>SCB</strong></td>
<td>System Control Board. On an M40 router, the part of the Packet Forwarding Engine that performs route lookups, monitors system components, and controls FPC resets.</td>
</tr>
<tr>
<td><strong>SCG</strong></td>
<td>SONET Clock Generator. Provides Stratum 3 clock signal for the SONET/SDH interfaces on the router. Also provides external clock inputs.</td>
</tr>
<tr>
<td><strong>SDH</strong></td>
<td>Synchronous Digital Hierarchy. CCITT variation of SONET standard.</td>
</tr>
<tr>
<td><strong>SDP</strong></td>
<td>Session Description Protocol. Used with multicast protocols to handle session conference announcements.</td>
</tr>
<tr>
<td><strong>SDRAM</strong></td>
<td>Synchronous dynamic random access memory.</td>
</tr>
<tr>
<td><strong>Secure Hash Algorithm</strong></td>
<td>See SHA-1.</td>
</tr>
<tr>
<td><strong>secure shell</strong></td>
<td>See SSH.</td>
</tr>
<tr>
<td><strong>security association</strong></td>
<td>See SA.</td>
</tr>
<tr>
<td><strong>Security Parameter Index</strong></td>
<td>See SPI.</td>
</tr>
<tr>
<td><strong>SFM</strong></td>
<td>Switching and Forwarding Module. On an M160 router, a component of the Packet Forwarding Engine that provides route lookup, filtering, and switching to FPCs.</td>
</tr>
</tbody>
</table>
SHA-1 Secure Hash Algorithm. A widely used hash function for use with Digital Signal Standard (DSS). SHA-1 is more secure than MD5.

shortest-path-first algorithm See SPF.

signaled path In traffic engineering, an explicit path; that is, a path determined using RSVP signaling. The ERO carried in the packets contains the explicit path information.

SIB Switch Interface Board. Provides the switching function to the destination Packet Forwarding Engine.

simplex interface An interface that assumes that packets it receives from itself are the result of a software loopback process. The interface does not consider these packets when determining whether the interface is functional.


SONET Synchronous Optical Network. High-speed (up to 2.5 Gbps) synchronous network specification developed by Bellcore and designed to run on optical fiber. STS-1 is the basic building block of SONET. Approved as an international standard in 1988. See also SDH.

SPF Shortest-path first, an algorithm used by IS-IS and OSPF to make routing decisions based on the state of network links. Also called the Dijkstra algorithm.

SPI Security Parameter Index. A portion of the IPSec Authentication Header that communicates which security protocols, such as authentication and encryption, are used for each packet in a VPN connection.

SPQ Strict Priority Queuing. Dequeuing method that provides a special queue that is serviced until it is empty. The traffic sent to this queue tends to maintain a lower latency and more consistent latency numbers than traffic sent to other queues. See also APQ.

SSB System and Switch Board. On an M20 router, Packet Forwarding Engine component that performs route lookups and component monitoring and monitors FPC operation.

SSH Secure shell. Software that provides a secured method of logging in to a remote network system.

SSRAM Synchronous Static Random Access Memory.

static LSP See static path.

static path In the context of traffic engineering, a static route that requires hop-by-hop manual configuration. No signaling is used to create or maintain the path. Also called a static LSP.

STM Synchronous Transport Module. CCITT specification for SONET at 155.52 Mbps.

strict In the context of traffic engineering, a route that must go directly to the next address in the path. (Definition from RFC 791, modified to fit LSPs.)

STS Synchronous Transport Signal. Synchronous Transport Signal level 1. Basic building block signal of SONET, operating at 51.84 Mbps. Faster SONET rates are defined as STS-\(n\), where \(n\) is a multiple of 51.84 Mbps. See also SONET.

stub area In OSPF, an area through which, or into which, AS external advertisements are not flooded.
**subnet mask** Number of bits of the network address used for host portion of a Class A, Class B, or Class C IP address.

**summary link advertisement** OSPF link-statement advertisement flooded throughout the advertisement’s associated areas by area border routers to describe the routes that they know about in other areas.

**sysid** System identifier. Portion of the ISO nonclient peer. The sysid can be any 6 bytes that are unique throughout a domain.

**System and Switch Board** See SSB.

**TACACS+** Terminal Access Controller Access Control System Plus. Authentication method for validating users who attempt to access the router using Telnet.

**TCP** Transmission Control Protocol. Works in conjunction with Internet Protocol (IP) to send data over the Internet. Divides a message into packets and tracks the packets from point of origin to destination.

**ToS** Type of service. The method of handling traffic using information extracted from the fields in the ToS byte to differentiate packet flows.

**traffic engineering** Process of selecting the paths chosen by data traffic in order to balance the traffic load on the various links, routers, and switches in the network. (Definition from http://www.ietf.org/internet-drafts/draft-ietf-mpls-framework-04.txt.) See also MPLS.

**transit area** In OSPF, an area used to pass traffic from one adjacent area to the backbone or to another area if the backbone is more than two hops away from an area.

**transit router** In MPLS, any intermediate router in the LSP between the ingress router and the egress router.

**transport mode** An IPSec mode of operation in which the data payload is encrypted, but the original IP header is left untouched. The IP addresses of the source or destination can be modified if the packet is intercepted. Because of its construction, transport mode can be used only when the communication end point and cryptographic end point are the same. VPN gateways that provide encryption and decryption services for protected hosts cannot use transport mode for protected VPN communications. See also tunnel mode.

**Triple-DES** A 168-bit encryption algorithm that encrypts data blocks with three different keys in succession, thus achieving a higher level of encryption. Triple-DES is one of the strongest encryption algorithms available for use in VPNs.

**tunnel** Private, secure path through an otherwise public network.

**tunnel mode** An IPSec mode of operation in which the entire IP packet, including the header, is encrypted and authenticated and a new VPN header is added, protecting the entire original packet. This mode can be used by both VPN clients and VPN gateways, and protects communications that come from or go to non-IPSec systems. See also transport mode.

**Tunnel PIC** A physical interface card that allows the router to perform the encapsulation and de-encapsulation of IP datagrams. The Tunnel PIC supports IP-IP, GRE, and PIM register encapsulation and de-encapsulation. When the Tunnel PIC is installed, the router can be a PIM rendezvous point (RP) or a PIM first-hop router for a source that is directly connected to the router.

**type of service** See ToS.
unicast  Operation of sending network traffic from one network node to another individual network node.

UPS  Uninterruptible power supply. Device that sits between a power supply and a router (or other piece of equipment) to prevent undesired power-source events, such as outages and surges, from affecting or damaging the device.

vapor corrosion inhibitor  See VCI.

VCI  Vapor corrosion inhibitor. Small cylinder packed with the router that prevents corrosion of the chassis and components during shipment.

VCI  Virtual circuit identifier. 16-bit field in the header of an ATM cell that indicates the particular virtual circuit the cell takes through a virtual path. Also called a logical interface. See also VPI.

virtual circuit identifier  See VCI.

virtual link  In OSPF, a link created between two routers that are part of the backbone but are not physically contiguous.

virtual path identifier  See VPI.

virtual private network  See VPN.

Virtual Router Redundancy Protocol  See VRRP.

VPI  virtual path identifier. 8-bit field in the header of an ATM cell that indicates the virtual path the cell takes. See also VCI.

VPN  virtual private network. A private data network that makes use of a public TCP/IP network, typically the Internet, while maintaining privacy with a tunneling protocol, encryption, and security procedures.

VRRP  Virtual Router Redundancy Protocol. On Fast Ethernet and Gigabit Ethernet interfaces, allows you to configure virtual default routers.

VRRP  Weighted round-robin. Scheme used to decide the queue from which the next packet should be transmitted.
Part 6
Index

- Index on page 667
- Index of Statements and Commands on page 685
Index

Symbols

# in configuration statements .................................. xxxix
in syntax descriptions ........................................ xxxix
( ) in syntax descriptions ...................................... xxxix
< >, in syntax descriptions ................................... xxxviii
[ ] in configuration statements ................................ xxxix
{ }, in configuration statements ................................ xxxix
| in syntax descriptions ...................................... xxxix

Numerics

128-bit IPv6 address .............................................. 82
802.1Q VLANs
  VLAN IDs .................................................. 566, 567
  VLAN tagging ............................................. 282, 286, 568
802.1Q/Ethernet 802.3 encapsulation
  encapsulation overhead ................................... 49
802.1Q/Ethernet SNAP encapsulation
  encapsulation overhead ................................... 49
802.3ad statement ............................................. 417
  usage guidelines ........................................ 266, 267

A

accept-data statement ........................................... 418
  usage guidelines ........................................ 294
accept-source-mac statement ................................... 418
  usage guidelines ........................................ 270
access profile, configuring .................................... 56
access-profile statement ...................................... 419
  usage guidelines ........................................ 55
accounting profile
  logical interfaces ........................................ 73
    example configuration ................................ 73
  physical interfaces ..................................... 61
    example configuration ................................ 62
accounting statement .......................................... 419
  usage guidelines ........................................ 94

accounting-profile statement .................................. 420
  usage guidelines ........................................ 61, 73
acknowledge-retries statement ............................... 420
  usage guidelines ........................................ 329
acknowledge-timer statement ................................. 421
  usage guidelines ........................................ 329
across-the-network applications ............................. 576
action-red-differential-delay statement .................... 421
  usage guidelines ........................................ 330
adaptive services interface .................................. 111
  address entries ........................................ 21
  address statement ........................................ 422
  usage guidelines ........................................ 81, 82
advertise-interval statement .................................. 423
  APS
    usage guidelines ....................................... 371
  VRRP
    usage guidelines ....................................... 293
advertisement intervals
  APS interfaces ............................................ 371
  VRRP master routers ..................................... 293
aggregate statement ........................................... 424
  usage guidelines ........................................ 269, 382
aggregated Ethernet interfaces .............................. 266
  configuring ............................................ 299
  example configuration ................................ 302
  link speed ............................................. 267
  minimum links ........................................ 267
aggregated interfaces, configuring ............................ 45
aggregated SONET interfaces ................................. 382
  configuring ............................................ 380
  example configuration ................................ 385
  firewall filters ........................................ 383
    example configuration ................................ 383
  link speed ............................................. 382
  minimum links ........................................ 383
aggregated-ether-options statement ......................... 425
  usage guidelines ........................................ 264
aggregated-sonet-options statement ......................... 425
  usage guidelines ........................................ 380
all (tracing flag) interfaces .................................................. 64, 107
VRPP ................................................................. 295
allow-any-vci statement ....................................................425
usage guidelines ............................................................. 146
APS
basic support .......................................................... 368
circuit pairs .......................................................... 367, 368
configurations, switching between ......................... 370
configuration example .......................................................... 369
example configuration .......................................................... 373
load sharing .............................................................. 372
overview ................................................................. 367
revertive mode ............................................................ 371
timers ................................................................. 371
aps statement ............................................................. 426
usage guidelines ............................................................. 368
arp option
policers ......................................................................... 87
arp statement ............................................................. 427
usage guidelines ............................................................. 289
ARP table, static
Ethernet interfaces ............................................................. 289
ATM 1 and ATM 2 configuration differences ......................... 122
ATM 1 interfaces
cell-relay circuit .......................................................... 148
example configuration .......................................................... 148
example configuration .......................................................... 158
shaping values ............................................................. 140
example calculation .......................................................... 141
ATM 2
shaping values ............................................................. 142
ATM 2 interfaces
early packet discard threshold ....................................... 143
example configuration .......................................................... 144
example configuration .......................................................... 161
Layer 2 Circuit cell-relay promiscuous mode ................. 132
example configuration .......................................................... 132
Layer 2 Circuit transport mode ........................................ 130
example configuration .......................................................... 131
ATM cell-relay encapsulation
encapsulation overhead .................................................. 49
ATM encapsulation
ATM CCC VC multiplex ................................................. 146
ATM cell-relay ............................................................. 146
ATM NLPIID ............................................................. 146
ATM PVC ................................................................. 146
ATM PVC encapsulation .................................................. 49, 51
ATM SNAP ................................................................. 146
ATM TCC SNAP ............................................................. 146
ATM TCC SNAP multiplex .................................................. 146
ATM VC multiplex ............................................................. 146
cell-relay accumulation mode ........................................ 146
Cisco ATM NLPIID ..................................................... 146
Ethernet over ATM ......................................................... 146
Ethernet VPLS over ATM .................................................. 146
keepalives ................................................................. 58
Layer 2 switching cross-connects ..................................... 101
Multilink PPP over ATM .................................................. 146
PPP over ATM ............................................................. 146
PPP over ATM multiplex .................................................. 146
See also ATM interfaces .................................................. 117
ATM interfaces ............................................................. 143
ATM overview ............................................................. 117
communication with routers ............................................ 126
encapsulation ............................................................. 51
inverse ARP ............................................................... 137, 308
MTU sizes ................................................................. 47, 48, 49
multicast-capable connections ........................................ 137
OAM F5 loopback cells ................................................. 144
PIC type ................................................................. 126
dexample configuration ................................................. 127
point-to-multipoint connections ...................................... 136
point-to-point connections .............................................. 136
PPP over ATM encapsulation ......................................... 150
dexample configuration .................................................. 150
SONET/SDH parameters .................................................. 154, 361
virtual circuits ............................................................. 127, 129
dexample configuration .................................................. 128
virtual paths ............................................................. 127, 129
dexample configuration .................................................. 128
See also ATM encapsulation ............................................. 146
ATM OAM F4 cells flows .................................................. 133
ATM PVC encapsulation .................................................. 49, 51
atm-encapsulation statement ........................................... 427
usage guidelines ............................................................. 153
atm-12circuit-mode statement
usage guidelines ............................................................. 130
atm-options statement .................................................... 428
usage guidelines ............................................................. 125, 135
atm-scheduler-map statement ........................................... 429
usage guidelines ............................................................. 155
authentication, VRPP statement ........................................ 292
authentication-key statement ........................................... 429
APS
usage guidelines ............................................................. 368
VRPP
usage guidelines ............................................................. 292
authentication-type statement ........................................... 431
usage guidelines ............................................................. 292
Automatic Protection Switching See APS
auto-synchronize statement ............................................. 432
usage guidelines ............................................................. 352
Index

Channelized T1 QPP interfaces
  interface options .................................................. 194, 211, 226
  M13 or C-bit parity mapping ........................................ 188
  VT mapping .................................................................. 188, 190
Channelized T3 interfaces
  loop timing .................................................................. 401
Channelized T3 QPP interfaces
  example configuration .................................................. 186, 234
  interface options ........................................................ 194, 210, 225
CHAP
  example configuration .................................................. 57
chap statement ................................................................ 441
  usage guidelines .......................................................... 55
checksums See frame checksums
  circuit cross-connect See CCC
  circuit pairs, APS ....................................................... 367, 368
Cisco HDLC encapsulation
  configuring on physical interfaces .................................. 51
  encapsulation overhead .................................................. 49
  example configuration .................................................... 404
  keepalives .................................................................. 58
  Layer 2 switching cross-connect ..................................... 101
class of service See CoS
class statement ............................................................... 624
  usage guidelines .......................................................... 616
classification-override statement ..................................... 624
  usage guidelines .......................................................... 610
classifiers statement ........................................................ 625
  usage guidelines .......................................................... 594
class-of-service statement ................................................ 624
  usage guidelines .......................................................... 585
clock rates ..................................................................... 351
clock sources .................................................................. 27, 59, 374, 443
  channelized interfaces .................................................... 166
clocking modes ................................................................ 351
clocking statement ............................................................ 443
  usage guidelines .......................................................... 27, 59, 374
clocking-mode statement ................................................... 443
  usage guidelines .......................................................... 350
clock-rate statement .......................................................... 442
  usage guidelines .......................................................... 351
code-point statement ........................................................ 626
  usage guidelines .......................................................... 602
code-point-aliases statement .......................................... 626
  usage guidelines .......................................................... 589
code-points statement ....................................................... 627
  usage guidelines .......................................................... 594
comments, in configuration statements ......................... xxxix
compatibility-mode statement .......................................... 444
  E3 interfaces, usage guidelines ........................................ 253
  T3 interfaces, usage guidelines ........................................ 398
congestion avoidance
  See CoS .................................................................... 575
connections
  configuration statements ................................................ 15
  connections statement ..................................................... 445
  usage guidelines .......................................................... 102
constant bit rate .............................................................. 139
control leads
  serial interfaces ............................................................. 352
control-leads statement .................................................... 445
  usage guidelines .......................................................... 352
control-polarity statement ................................................ 446
  usage guidelines .......................................................... 355
control-signal statement .................................................... 446
  usage guidelines .......................................................... 352
conventions, documentation ........................................... xxxviii
core-dump statement ........................................................ 447
  usage guidelines .......................................................... 65
CoS
  ATM 2 example configuration ........................................ 158
  channelized QPP interfaces .......................................... 597
  classifiers ................................................................. 594
  configuration statements .............................................. 5, 623
  congestion avoidance .................................................... 582
  Gigabit Ethernet QPP interfaces ..................................... 597
  interfaces, example configuration .................................. 617
  IPv4 packets ................................................................ 594
  mechanism, applications of .......................................... 576
  overriding input classification ........................................ 616
  rewrite rules ................................................................ 602
    EXP bits by node ....................................................... 603, 604
    EXP bits of all three labels .......................................... 607
    MPLS EXP and IEEE 802.1p ........................................ 609
    MPLS EXP and IPv4 .................................................. 605
CoS-based forwarding See CBF
CSU compatibility
  E3 interfaces ................................................................. 253
  T3 interfaces ................................................................. 398
cts statement .................................................................. 447
  usage guidelines .......................................................... 352
cts-polarity statement ..................................................... 448
  usage guidelines .......................................................... 355
curly braces, in configuration statements ......................... xxxix
customer support
  contacting ................................................................... xli
damping, interface transitions ......................................... 64, 376
data circuit-terminating equipment See DCE
  data inversion ................................................................. 246, 390
data terminal equipment See DTE
database (tracing flag) ....................................................... 295
dcd statement .................................................................. 448
  usage guidelines .......................................................... 352
dcd-polarity statement ..................................................... 449
  usage guidelines .......................................................... 355
DCE .............................................................................. 59, 309, 404, 449
dce statement .................................................................. 449
  usage guidelines .......................................................... 59, 309
default router addresses .................................................... 84
dense wavelength-division multiplexing See DWDM
encapsulation
    CCC .................................................. 101
    Ethernet 802.3 ............................................. 49
    example configuration .................................. 55, 378
    extended-vlan-ccc .................................. 285, 286
    media MTU size and .................................. 50
    on logical interfaces .................................. 75, 379
    on physical interfaces ................................ 51, 377
    overheads ................................................. 49

See also ATM encapsulation; Cisco HDLC	
    encapsulation; Frame Relay encapsulation;
    Point-to-Point Protocol encapsulation

encapsulation statement .................................. 457
Layer 2 switching cross-connect ........................ 101
logical interfaces
    usage guidelines ...................................... 75, 305, 379
physical interfaces
    usage guidelines ...................................... 51, 304, 377
encoding
    byte .................................................. 389, 438
    line .................................................. 357, 391
encoding statement ...................................... 460
usage guidelines ........................................... 357
Encryption interface ..................................... 258
epd-threshold statement .................................. 461
usage guidelines ........................................... 143, 155
ES interface
example configuration .................................... 259
ES PIC
    PIC redundancy ....................................... 259
    redundancy
        example configuration .................................. 260
        tunnel redundancy .................................. 260
es-options statement .................................. 462
usage guidelines ........................................... 259
Ethernet CCC and TCC encapsulation
physical interfaces ...................................... 51
Ethernet CCC encapsulation
    encapsulation overhead ................................ 49
Ethernet interfaces
    configuration statements ............................ 264
    example configuration .................................. 301
Fast Ethernet See Fast Ethernet interfaces
    Gigabit Ethernet See Gigabit Ethernet interfaces
    gratuitous ARP ......................................... 281
    internal Ethernet interface ............................ 20, 299
    management See management Ethernet interface
    static ARP table entries .................................. 289
    VLAN IDs ............................................... 566, 567
    VLAN tagging ........................................... 282, 286, 568
    VRRP .................................................. 290
Ethernet link aggregation .................................. 266
Ethernet over ATM encapsulation
    encapsulation overhead ................................ 49
    physical interfaces .................................. 51
Ethernet SNAP encapsulation
    encapsulation overhead ................................ 49

    encapsulation........................................... 51

encapsulation overhead.................................................. 49

Ethernet TCC
    applying ............................................... 287
    encapsulation
        encapsulation overhead ................................ 49
        example configuration .................................. 287
    Ethernet TCC encapsulation .................................. 286
    ethernet-policer-profile statement ..................... 462
    usage guidelines ........................................... 269
    ethernet-switch-profile statement .................... 463
    usage guidelines ........................................... 269–273
eui-64 statement ............................................. 463
usage guidelines .......................................... 81
event (tracing flag) ........................................... 64, 107
export-format statement
    usage guidelines ........................................... 316
exp-push-push-push statement .................................. 629
usage guidelines ........................................... 607
exp-swap-push-push statement .................................. 630
usage guidelines ........................................... 607
extended VLAN
    CCC
        applying ............................................... 285
        encapsulation........................................... 51
        encapsulation overhead ................................ 49
        example configuration .................................. 285
    TCC
        applying ............................................... 286, 287
        encapsulation........................................... 51, 286
        encapsulation overhead ................................ 49
        example configuration .................................. 288
external clock sources ....................................... 59, 374, 443
f1 SONET header byte ........................................... 362
f2 SONET header byte ........................................... 362
fabric priority queueing
    overriding ............................................... 582
fabric statement ............................................. 630
usage guidelines ........................................... 600
facility statement ........................................... 538
facility-override statement ................................. 464
fail-filter statement ....................................... 532
usage guidelines ........................................... 89
family descriptors ........................................... 21
family statement ............................................. 465
usage guidelines ........................................... 79
interfaces
    usage guidelines ........................................... 112, 114, 316
monitoring
    usage guidelines ........................................... 316
far-end alarm and control signal See FEAC response
Fast Ethernet interfaces
  configuration statements ........................................... 264
  Ethernet link aggregation ......................................... 266
  example configuration ............................................. 301
  ingress rate-limit ................................................. 282
  link modes ................................................................ 46, 281
  loopback mode .......................................................... 280
  MAC address filtering ................................................ 279
  MTU sizes .................................................................... 47, 48
  physical interface properties ........................................ 264
  speed ......................................................................... 282
  static ARP table entries ................................................. 289
  usage guidelines ......................................................... 286
  VLAN IDs .................................................................... 566, 567
  VLAN tagging ............................................................. 282, 286, 568
  VRRP ......................................................................... 290
fastether-options statement ............................................. 467
usage guidelines ........................................................... 264
fcs statement .................................................................. 468
  E1 interfaces
    usage guidelines ....................................................... 245
  E3 interfaces
    usage guidelines ....................................................... 253
  SONET interfaces
    usage guidelines ....................................................... 363
  T1 interfaces
    usage guidelines ....................................................... 390
  T3 interfaces
    usage guidelines ....................................................... 399
FEAC response .................................................................. 399
feac-loop-respond statement .......................................... 468
usage guidelines ........................................................... 399
FECN, BECN, and DE bits
  Frame Relay encapsulation ......................................... 305
fill-level statement ........................................................... 630
usage guidelines ........................................................... 601
filter statement .............................................................. 469
usage guidelines ........................................................... 88
filters on aggregated links ............................................... 383
example configuration .................................................... 383
firewall filters
  applying ................................................................. 88
  in traffic sampling ................................................... 315
  logical interfaces ....................................................... 88
flow control .................................................................. 280
flow monitoring .............................................................. 317
flow-control statement .................................................... 469
usage guidelines ........................................................... 280
force statement ............................................................. 470
usage guidelines ........................................................... 370
forwarding-class statement ............................................. 470, 631
usage guidelines ........................................................... 155, 594
forwarding-classes statement .......................................... 632
usage guidelines ........................................................... 592
forwarding-options statement
  usage guidelines ........................................................... 315
forwarding-policy statement ............................................. 633
usage guidelines ........................................................... 610
fractional E1 QPP interfaces
  example configuration .................................................. 174, 208
  time slots .................................................................... 174, 191, 207, 223
fractional T1 QPP interfaces
  example configuration .................................................. 191, 223
  time slots .................................................................... 191, 223
fragment-threshold statement ......................................... 471
usage guidelines ........................................................... 325
frame checksums
  E1 interfaces .............................................................. 245
  E3 interfaces .............................................................. 253
  SONET interfaces ....................................................... 363, 366
  T1 interfaces .............................................................. 390
  T3 interfaces .............................................................. 399
Frame Relay connections
  DLCIs ......................................................................... 309
  point-to-point connections ......................................... 309, 322
  Frame Relay encapsulation
    DCE ...................................................................... 59, 309, 449
    encapsulation overhead ............................................. 49
    example configuration ............................................... 304, 404
    FECN, BECN, and DE bits ............................................ 305
    Frame Relay protocol ................................................ 303
    keepalives .................................................................. 58, 307
    Layer 2 switching cross-connect .................................... 101
    logical interfaces ....................................................... 305, 379
    MTUs ........................................................................ 306
    multicast-capable connections ..................................... 311, 323
    physical interfaces ..................................................... 51, 304, 377
    point-to-multipoint connections .................................... 310
    framing bytes, SONET interfaces .................................. 362
    framing statement ....................................................... 471
      E1 interfaces
        usage guidelines ..................................................... 246
      T1 interfaces
        usage guidelines ..................................................... 391
      usage guidelines ..................................................... 153
      framing, E3 interfaces ................................................. 153
      ffp0 interface See management Ethernet interface
## Index

**Gigabit Ethernet interfaces**
- configuration statements ............................................................. 264
- Ethernet link aggregation .......................................................... 266
- example configuration ............................................................... 301
- flow control ............................................................................... 280
- loopback mode ........................................................................... 280
- MAC address filtering ............................................................... 279, 297
- MTU sizes ................................................................................. 47, 48
- static ARP table entries ............................................................ 289
- VLAN IDs ................................................................................... 566, 567
- VLAN tagging ............................................................................ 282, 286, 568
- VRRP .......................................................................................... 290

**Gigabit Ethernet QPP interfaces**
- CoS ............................................................................................ 597
- MAC address accounting ............................................................ 272
- MAC address filtering ............................................................... 269, 270
- VLAN tag stacking and rewriting ................................................ 273
- gratuitous ARP ........................................................................... 281
- gratuitous-arp-reply statement .................................................. 473
- usage guidelines ......................................................................... 281
- group option
  - firewall filters .......................................................................... 88

**HDLC encapsulation**

See Cisco HDLC encapsulation

**HDLC payload scrambling**
- E3 interfaces ............................................................................. 255
- SONET interfaces ....................................................................... 365, 366
- T3 interfaces ............................................................................... 403
- header byte values ..................................................................... 361, 366
- hello-timer statement .................................................................. 473
- usage guidelines ......................................................................... 329
- high-plp-max-threshold statement ............................................ 474
- usage guidelines ......................................................................... 155
- high-plp-threshold statement .................................................... 474
- usage guidelines ......................................................................... 155
- hold-time statement ................................................................... 475
- APS
  - usage guidelines ..................................................................... 371
  - damping interface transitions
    - usage guidelines .................................................................. 64, 376
- host statement ............................................................................. 476

**idle-cycle-flag statement** .......................................................... 476

**E1 interfaces**
- usage guidelines ........................................................................ 246

**E3 interfaces**
- usage guidelines ........................................................................ 254

**T1 interfaces**
- usage guidelines ........................................................................ 393

**T3 interfaces**
- usage guidelines ........................................................................ 400

**IEEE802.1-priority-map statement** ............................................ 477
- usage guidelines .......................................................................... 269
- ignore-all statement ..................................................................... 477
- usage guidelines ......................................................................... 352
- ilmi statement ............................................................................. 477
- usage guidelines .......................................................................... 126

**import statement** ...................................................................... 633
- usage guidelines ......................................................................... 594
- inactivity-timeout statement ...................................................... 478
- incrementing STM ID ................................................................ 362
- indication statement ...................................................................... 478
- usage guidelines ......................................................................... 352
- indication-polarity statement ..................................................... 478
- usage guidelines ......................................................................... 355

**inet protocol family**
- interface addresses .................................................................... 81
- on logical interfaces .................................................................... 79

**inet6 protocol family**
- interface addresses .................................................................... 82
- on logical interfaces .................................................................... 79
- ingress-rate-limit statement ....................................................... 479
- usage guidelines ......................................................................... 282

**input option**
- firewall filters ............................................................................. 88
- policers ......................................................................................... 87

**input statement** ......................................................................... 479
- traffic sampling ........................................................................... 479

**input-vlan-map statement** ........................................................ 480
- usage guidelines ......................................................................... 273

**interface addresses**
- logical interfaces ........................................................................ 81
- preferred interface addresses .................................................... 84, 86
- primary interface addresses ...................................................... 84, 85
- interface groups .......................................................................... 89
- interface processes, trace operations ......................................... 108

**interface statement**
- monitoring, output
  - usage guidelines ..................................................................... 316
- interface transitions, damping .................................................. 64, 376
IPv6 over-IPv4 tunnel example configuration ........................................ 415
standards supported ............................................................... 412
ISO protocol family .................................................................. 79, 81
ITU-T standards
E1 interfaces ............................................................................ 243
E3 interfaces ............................................................................ 251

Layer 2 Circuit cell-relay promiscuous mode
ATM 2 interfaces example configuration ........................................ 132
Layer 2 Circuit transport mode
ATM 2 interfaces example configuration ........................................ 131
Layer 2 switching cross-connect
CCC connections ...................................................................... 102
CCC encapsulation example configuration .................................... 103
MPLS router configuration .......................................................... 103
Layer 2.5 VPNs
Ethernet .................................................................................... 285, 286, 287
leaky bucket properties ........................................................... 60, 375
line protocol ............................................................................... 357, 391
line buildout
T3 interfaces ............................................................................... 400
linear-red-profile statement usage guidelines ................................ 155
linear-red-profiles statement usage guidelines .............................. 155
line-encoding statement usage guidelines .................................... 391
line-protocol statement usage guidelines .................................... 347
line-vlan-id statement usage guidelines ...................................... 273
link aggregation .......................................................................... 266
SONET interfaces ......................................................................... 382
link modes .................................................................................... 46, 281

K
keep-address-and-control statement ............................................. 484
usage guidelines ........................................................................... 84
keepalives disabling ....................................................................... 58
keepalives statement usage guidelines ............................................ 58, 307
keepalives disabling ....................................................................... 307

L
Layer 2.5 VPNs
Ethernet .................................................................................... 285, 286, 287
leaky bucket properties ........................................................... 60, 375
line protocol ............................................................................... 357, 391
line buildout
T3 interfaces ............................................................................... 400
linear-red-profile statement usage guidelines ................................ 155
linear-red-profiles statement usage guidelines .............................. 155
line-encoding statement usage guidelines .................................... 391
line-protocol statement usage guidelines .................................... 347
line-vlan-id statement usage guidelines ...................................... 273
link aggregation .......................................................................... 266
SONET interfaces ......................................................................... 382
link modes .................................................................................... 46, 281
link services interface
interleave fragments ........................................ 326
link services interfaces
CoS components .................................................. 335
example configuration ........................................ 336, 341
link speed
Ethernet aggregation ............................................. 267
SONET aggregation ............................................. 382
link-mode statement ............................................. 488
usage guidelines ............................................... 46, 281
link-speed statement ............................................. 488
usage guidelines ............................................... 267, 382
LMI packets See keepalives
Imi statement ..................................................... 489
usage guidelines ............................................... 307
Imi-type statement .............................................. 490
usage guidelines ............................................... 307, 331
lo0 interface ..................................................... 241, 313
load sharing, APS .................................................. 372
Local Management Interface packets See keepalives
local name, configuring ........................................ 56
local-name statement ............................................ 490
usage guidelines ............................................... 55
lockout statement ............................................... 491
usage guidelines ............................................... 370
logical interface properties, statements for ................ 69
logical interfaces
accounting profile ................................................ 73
example configuration ........................................ 73
CCC .......................................................... 99, 103
configuration statements ........................................ 67
default router addresses ........................................ 84
descriptive text ................................................... 71
descriptors ......................................................... 21
disabling ............................................................ 76
encapsulation See encapsulation ................................ 74
firewall filters .................................................... 88
Frame Relay encapsulation .................................... 305
interface addresses ............................................. 81, 84
interface bandwidth ............................................ 74
inverse ARP ...................................................... 137, 308
Layer 2 switching cross-connect ................................ 100
logical interface properties .................................... 67
multicast-capable connections ............................... 137, 311, 323
multipoint connections ........................................ 72
OAM F5 loopback cells ......................................... 144
point-to-multipoint connections ............................. 136, 310
point-to-point connections .................................... 72, 136
policers ............................................................. 87
PPP over ATM encapsulation .................................. 150
example configuration ........................................ 150
preferred interface addresses ............................... 84, 86
primary interface addresses ................................. 84, 86
primary router addresses ..................................... 84
primary router interfaces ..................................... 85
protocol families .................................................. 77, 79
protocol MTU ..................................................... 83
protocol redirect messages ..................................... 84
SNMP notifications ............................................. 74
static ARP table entries ....................................... 74
unit numbers ...................................................... 71
unnumbered interfaces ......................................... 82
VLAN IDs ....................................................... 566, 567
See also names of specific interfaces
logical part of interface name .................................... 25
log-prefix statement ............................................ 491
long-buildout statement ........................................ 491
usage guidelines ............................................... 400
loop timing
Channelized T3 interfaces ...................................... 401
loopback capability ............................................... 356, 364
E1 interfaces ..................................................... 247
time example configuration .................................... 248
E3 interfaces ..................................................... 254
time example configuration .................................... 255
serial interfaces
time example configuration .................................... 357
SONET interfaces
time example configuration .................................... 364
T1 interfaces ..................................................... 392
T3 interfaces ..................................................... 401
loopback interface ............................................... 241, 313
time example configuration .................................... 314
loopback mode ................................................... 280
loopback statement ............................................. 492, 494
E1 interfaces
usage guidelines ............................................... 247
E3 interfaces
usage guidelines ............................................... 254
Fast Ethernet interfaces
usage guidelines ............................................... 280
Gigabit Ethernet interfaces
usage guidelines ............................................... 280
serial interfaces
usage guidelines ............................................... 356
SONET interfaces
usage guidelines ............................................... 364
T1 interfaces
usage guidelines ............................................... 392
T3 interfaces
usage guidelines ............................................... 401
loopback tunnels ............................................... 410
loop-timing statement ........................................... 492
usage guidelines ............................................... 401
loss-priority statement ......................................... 636
usage guidelines ............................................... 401
low-plp-max-threshold statement ........................... 494
usage guidelines ............................................... 594
low-plp-threshold statement .................................. 495
usage guidelines ............................................... 155
lsp-next-hop statement ........................................ 636
usage guidelines ............................................... 610
M13 framing........................................................................397
M13 or C-bit parity mapping
  Channelized T1 QPP interfaces ..................................188
  NxDS-0 QPP interfaces..............................................190
MAC address accounting
  Gigabit Ethernet QPP interfaces ..................................272
MAC address filtering
  example configuration ..............................................271
  Fast Ethernet interfaces.........................................279
  Gigabit Ethernet interfaces .....................................279, 297
  Gigabit Ethernet QPP interfaces ..............................269, 270
MAC addresses
  management Ethernet interface .................................279, 298
  mapping to IP addresses .......................................289
mac statement..................................................................495
  usage guidelines ................................................298
mac-address statement..............................................496
  usage guidelines ................................................270
mac-learn-enable statement.........................................496
  usage guidelines ................................................272
management Ethernet interface
  configuring ..........................................................298
  interface speed .....................................................57
  link modes ..........................................................46, 281
  MAC address .........................................................298
overview ......................................................................20
master routers, VRRP ..................................................290, 293, 294, 297
maximum transmission units See MTUs
maximum-vcs statement See MTUs
media MTUs
  Frame Relay encapsulation ....................................306
  SONET interfaces ...................................................373
  See also MTUs ......................................................47
minimum links for aggregation
  Ethernet links ........................................................267
  SONET links ..........................................................383
minimum links for Link Services interfaces ....................326
minimum links for Multilink interfaces .........................326
minimum-links statement ..........................................498
  usage guidelines ................................................326, 383
mlfr-uni-uni-bundle-options statement ........................498
  usage guidelines ................................................327–331
mode statement ..........................................................499
  usage guidelines ..................................................91
monitoring services interfaces, physical interface
  properties ..................................................................65
monitoring statement
  usage guidelines ...................................................316
MPLS
  Layer 2 switching cross-connect ................................103
  mpls protocol family .............................................79, 81
mrru statement ..........................................................499
  usage guidelines ..................................................326
usage guidelines .........................................................500
  Frame Relay encapsulation
    usage guidelines ................................................306
  logical interfaces
    usage guidelines ..................................................83
  SONET interfaces
    usage guidelines ................................................373
  usage guidelines ..................................................47
MTUs
  Frame Relay encapsulation ....................................306
  logical interfaces ..................................................83
  media MTUs ..........................................................306, 373
  physical interfaces ...............................................47, 373
  protocol MTUs .......................................................83, 306
  SONET interfaces ...................................................373
  multicast tunnels ...................................................409
  multicast-capable connections
    ATM interfaces ...................................................137
    Frame Relay encapsulation .................................311, 323
  multicast-dlc statement .........................................500
    usage guidelines .................................................311, 323
  multicast-only statement ........................................501
    usage guidelines ................................................409
  multicast-vci statement ..........................................501
    usage guidelines ................................................137
  multilink interface
    minimum links ...................................................326
  multilink interfaces
    example configuration ........................................339
  multipoint connections ..........................................72
  See also point-to-multipoint connections ...................136
  multipoint nonbroadcast multi-access connections See
    point-to-multipoint connections ................................136
  multipoint statement ..............................................501
    usage guidelines ................................................72
  multipoint-destination statement .............................502
  ATM interfaces
    usage guidelines ................................................136
    point-to-multipoint Frame Relay connections
      usage guidelines .................................................310
    Multiprotocol Label Switching See MPLS ..................103
  multiservice-options statement ...............................503
    usage guidelines .................................................65, 317
usage guidelines .........................................................503
  usage guidelines ..................................................331
n392 statement ..........................................................504
  usage guidelines ..................................................331
n393 statement ..........................................................504
  usage guidelines ..................................................331
names, interface .......................................................23–27
NBMA connections See point-to-multipoint connections
neighbor statement ..................................................505
  usage guidelines ..................................................368
next-hop statement ........................................... 636
  usage guidelines ........................................ 610
next-hop-map statement .................................... 637
  usage guidelines ........................................ 610
no-accept-data statement .................................. 505
  usage guidelines ........................................ 294
no-asynchronous-notification statement ............... 505
  usage guidelines ........................................ 84
no-cbit-parity statement ................................ 440, 505
  usage guidelines ........................................ 397
no-core-dump statement .................................. 447, 505
  usage guidelines ........................................ 65
no-feac-loop-respond statement ......................... 468, 506
  usage guidelines ........................................ 399
no-flow-control statement ................................ 506
  usage guidelines ........................................ 280
no-gratuitous-arp-reply statement ....................... 473
  usage guidelines ........................................ 281
no-gratuitous-arp-request statement .................... 506
  usage guidelines ........................................ 281
no-keepalives statement ................................ 506
  usage guidelines ........................................ 58, 307
no-long-buildout statement ................................ 491, 507
  usage guidelines ........................................ 400
no-loopback statement .................................... 492, 507
  usage guidelines ........................................ 280
no-loop-timing statement ................................ 492
  usage guidelines ........................................ 401
no-mac-learn-enable statement .......................... 507
  usage guidelines ........................................ 272
nonbroadcast multiaccess connections See
  point-to-multipoint connections
no-partition statement ..................................... 507
  Channelized E1 QPP interfaces
    usage guidelines ....................................... 173
  Channelized OC-12 QPP interfaces
    usage guidelines ....................................... 185
  Channelized T3 QPP interfaces
    usage guidelines ....................................... 185, 206, 221
no-payload-scrambler statement .......................... 508, 517
  ATM 1 interfaces
    usage guidelines ....................................... 153
  E3 interfaces
    usage guidelines ....................................... 255
  SONET interfaces
    usage guidelines ....................................... 365
  T3 interfaces
    usage guidelines ....................................... 403
no-preempt statement ..................................... 509, 522
  usage guidelines ....................................... 293, 294
no-redirects statement ................................... 509
  usage guidelines ....................................... 84
normal (tracing flag) ..................................... 295
no-source-filtering statement ............................ 509
  usage guidelines ....................................... 279
no-syslog statement ...................................... 509, 545
  usage guidelines ....................................... 65
no-translate-discard-eligible statement ............... 556
  usage guidelines ....................................... 305
no-translate-fecn-and-becn statement ................. 556
  usage guidelines ....................................... 305
no-traps statement ....................................... 559
  usage guidelines ....................................... 65, 74
no-z0-increment statement ................................ 509, 571
  usage guidelines ....................................... 362
NxDS-0 QPP interfaces
  example configuration ..................................... 209, 224
  interface options ....................................... 228
  M13 or C-bit parity mapping ............................ 190
  VT mapping ............................................... 190
OAM cells See keepalives ................................ 58
OAM F5 loopback cells
  loopback cell period ..................................... 144
  loopback cell threshold ................................ 145
oam-liveness statement .................................. 510
  usage guidelines ....................................... 133, 134, 145
oam-period statement ...................................... 511
  usage guidelines ....................................... 144
OC-12 interfaces
  example configuration ..................................... 198
  traffic-shaping rates ................................... 141
OC-3 interfaces .......................................... 141
  example configuration ..................................... 158, 379
OC-48 interfaces
  SONET header bytes ....................................... 362
oc-slice statement
  Channelized OC-3 QPP interfaces
    usage guidelines ....................................... 186
open-timeout statement .................................... 512
output option
  firewall filters .......................................... 88
  policers .................................................. 87
output statement ........................................... 512
  interface
    usage guidelines ....................................... 114
    monitoring
      usage guidelines ..................................... 316
  output-interface-index statement
    usage guidelines ....................................... 316
  output-vid-map statement ................................ 512
    usage guidelines ....................................... 273
overflow option ............................................ 60, 376
overflow statement ....................................... 513
  usage guidelines ....................................... 60, 375
packets ................................. 575
packets (tracing flag) ....................... 295
paired-group statement .................. 513
usage guidelines .......................... 372
partition statement ......................... 511, 514
Channelized OC-3 QPP interfaces
usage guidelines ............................ 186
Channelized T1 QPP interfaces
usage guidelines ............................ 187, 206, 222
NxDS-0 QPP interfaces
usage guidelines ............................ 189
NxDS-0 QPP interfaces
usage guidelines ............................ 186
passive access, configuring ................. 56
passive statement ............................ 515
usage guidelines ............................ 55
passive-monitor-mode statement ............ 515
usage guidelines ............................ 374
path trace identifier ......................... 365
path-trace statement ....................... 516
usage guidelines ............................ 365
payload-scrambler statement ............... 517
ATM 1 interfaces
usage guidelines ............................ 153
E3 interfaces
usage guidelines ............................ 255
SONET interfaces
usage guidelines ............................ 365
T3 interfaces
usage guidelines ............................ 403
permanent interfaces ......................... 19, 20
Permanent Virtual Circuit encapsulation See ATM PVC encapsulation
per-unit-scheduler statement ............... 517
usage guidelines ............................ 597
physical interfaces
accounting profile ............................ 61
element configuration ....................... 62
APS See APS
ATM interfaces .................................. 125, 135
BERT properties ............................. 252, 396
buildout ........................................ 153, 389
byte encoding ............................... 389, 438
C-bit parity mode ............................. 397, 440
clock rates ...................................... 351
clock sources ................................. 27, 59, 374, 443
clocking mode .................................. 351
configuration statements .................... 39
CSU compatibility ............................ 253, 398
data inversion .................................. 246, 390
DCE ......................................... 59, 309, 449
descriptive text .................................. 46, 449
descriptors ....................................... 21
disabling ......................................... 65
DTR circuit ........................................ 355
encapsulation See encapsulation ............. 51
Ethernet link aggregation .................... 266
FEAC response .................................. 399
flow control ..................................... 280
frame checks See frame checksums
Frame Relay encapsulation ................... 304
framing ........................................... 153
framing modes ................................. 246, 391
HDLC payload scrambling .................... 255, 365, 366, 403
header byte values ............................ 361, 366
idle cycle flag .................................... 246, 254, 393, 400
keepalives ....................................... 58, 307
leaky bucket properties ....................... 60, 375
line buildout ..................................... 400
line encoding ..................................... 357, 391
line protocol ...................................... 347
link modes ........................................ 46, 281
loop timing ........................................ 401
loopback capability ............................ 247, 254, 356, 364, 392, 401
loopback mode .................................... 280
MAC address filtering ......................... 279
media MTU size ................................... 47, 373
path trace identifier ......................... 365
physical interface properties ................ 39
PPP CHAP ........................................ 55
remote loopback response ..................... 390
revertive mode, APS ......................... 371
RFC 2615 support ............................... 366
signal polarity ..................................... 355
SNMP notifications ............................. 65
SONET link aggregation ....................... 382
speed ............................................. 57
start-end flag ..................................... 248, 256, 394, 403
statements ......................................... 42
time slots ........................................ 174, 191, 207, 208, 223, 249, 394
transitions, damping ......................... 64
virtual circuits, ATM ......................... 129
virtual paths, ATM ............................. 129
VLAN tagging ..................................... 282, 286, 568
See also names of specific interfaces
physical part of interface name .............. 23
pic-type statement ............................ 518
usage guidelines .............................. 126
PIM tunnels ....................................... 411
point-to-multipoint connections
ATM interfaces ................................. 136
Frame Relay encapsulation ................... 310
point-to-point connections
ATM interfaces ................................. 136
Frame Relay encapsulation ................... 309, 322
logical interfaces ............................... 72
Point-to-Point Protocol encapsulation
capsulation overhead ......................... 49
keepalives ....................................... 58
on physical interfaces ....................... 51, 377, 404
PPP CHAP ........................................ 55
Index

point-to-point statement ........................................ 518
usage guidelines ........................................ 72
policer statement ........................................... 519
usage guidelines ........................................ 87, 269, 270
policers
applying ....................................................... 87
arp option ...................................................... 87
input option .................................................... 87
logical interfaces ........................................... 87
output option .................................................. 87
pop statement .................................................. 521
usage guidelines ........................................... 273
PPP over ATM encapsulation ................................ 150
example configuration ....................................... 150
ppp-options statement .................................... 522
usage guidelines .......................................... 55
preempt statement ........................................... 522
usage guidelines ........................................... 293
preempting master routers ................................ 293, 294
preferred interface addresses ................................ 84, 86
preferred statement .......................................... 523
usage guidelines ........................................... 81, 86
premium statement .......................................... 523
usage guidelines ........................................... 269
primary interface addresses ................................ 84, 86
primary router addresses ................................... 84
primary router interfaces ................................... 85
primary statement ........................................... 524
usage guidelines ........................................... 81, 85, 86
priorities, VRRP .......................................... 291, 295
priority statement ........................................... 524, 637
usage guidelines ........................................... 155, 291, 594, 600
promiscuous-mode statement ............................. 525
usage guidelines ........................................... 125, 135
protect circuit, APS
configuring ..................................................... 368
load sharing between paired groups ..................... 372
overview ......................................................... 367
paired groups, switching between ....................... 370
protect-circuit statement .................................. 526
usage guidelines ........................................... 368
protocol line ..................................................... 347
protocol families
configuration statements ..................................... 77
logical interfaces ........................................... 77, 79
protocol MTUs ............................................... 83
unnumbered interfaces ..................................... 82
protocol MTUs
Frame Relay encapsulation ................................ 306
logical interfaces ........................................... 83
See also MTUs ................................................ 47
protocol redirect messages ................................ 84
protocol statement .......................................... 639
usage guidelines ........................................... 596, 605
protocols
families See protocol families ................................ 77
protocols connections
configuration statements .................................... 15
protocols VRRP
configuration statements .................................... 16
proxy statement ............................................. 526
usage guidelines ........................................... 287
push statement ............................................... 527
usage guidelines ........................................... 273
PVC encapsulation See ATM PVC encapsulation
queue statement ............................................. 640
usage guidelines ........................................... 592
queue-depth statement ..................................... 527
low-plp-threshold statement
usage guidelines ........................................... 155
queue-length statement ................................... 528
usage guidelines ........................................... 142
random Early Detection mechanism See RED
rate statement ................................................ 640
usage guidelines ........................................... 60, 375
real-time variable bandwidth rate See RTVBR
receive (tracing flag modifier) ............................ 64, 107
receive-bucket statement ................................ 529
usage guidelines ........................................... 60, 375
RED
dropping packets ............................................. 583
drop-probability statement ................................ 627
usage guidelines ........................................... 601
drop-profile statement ..................................... 628
usage guidelines ........................................... 596
drop-profiles statement ................................... 629
usage guidelines ........................................... 601
red-differential-delay statement ......................... 529
usage guidelines ........................................... 330
redirect messages ........................................... 84
remote loopback response ................................ 390
remote statement ........................................... 530
usage guidelines ........................................... 285, 286, 287
remote-loopback-respond statement .................. 530
usage guidelines ........................................... 390
request statement ........................................... 531
usage guidelines ........................................... 370
revertive mode, APS .......................................... 371
revert-time statement ....................................... 531
usage guidelines ........................................... 371
rewrite-on-egress statement
usage guidelines ........................................... 273
rewrite-on-ingress statement
usage guidelines ........................................... 273
rewrite-rules statement ................................... 640
usage guidelines ........................................... 602
Index

RFC 2615 support, SONET interfaces .................. 366
rfc-2615 statement .............................................. 531
usage guidelines ................................................. 366
routers
  default addresses ........................................ 84
  primary addresses ....................................... 84
  primary interfaces ....................................... 85
routing-instance statement .................................... 532
usage guidelines ................................................. 409
rpf-check statement ............................................. 532
usage guidelines ................................................. 89
rts statement ..................................................... 532
usage guidelines ................................................. 352
rts-polarity statement .......................................... 533
usage guidelines ................................................. 355
RTVBR
  rtvbr statement .............................................. 533
  usage guidelines ..............................................

S
s1 SONET header byte .......................................... 362
sample (firewall filter action) ......................... 315
sampling on aggregated links .............................. 383
example configuration .......................................... 383
sampling statement .............................................. 534
usage guidelines ................................................. 315
sampling, monitoring interface ............................. 316
scheduler statement ............................................. 641
usage guidelines ................................................. 596, 600
scheduler-map statement ....................................... 642
usage guidelines ................................................. 596, 597, 600
scheduler-maps statement ..................................... 534, 643
usage guidelines ................................................. 155, 596
schedulers statement ............................................ 643
usage guidelines ................................................. 596
SDH interfaces
  configuration statements ..................................... 360
  MTU sizes ....................................................... 47, 48
  overview ....................................................... 359
  physical properties ........................................ 360
  See also SONET interfaces .................................. 359
send (tracing flag modifier) ................................... 64, 107
separators, in interface names .............................. 25
serial interfaces
  clock rates ...................................................... 351
  clocking mode ............................................... 350
  clocking modes ............................................. 351
  configuration statements ................................. 345
  control leads ................................................ 352
  correcting phase shift ...................................... 351
  default settings ............................................. 347
  DTR circuit .................................................... 355
  invalid statements .......................................... 349
  line encoding ............................................... 357
  line protocol ............................................... 347
  loopback capability ........................................ 356
  physical interface properties ................................ 345
  signal polarity ................................................. 355
  serial-options statement ................................... 535
  usage guidelines .............................................. 345
  service level See CoS ........................................ 575
  service statement ............................................. 536
  service-domain statement ................................... 536
  service-filter statement ..................................... 537
  service-options statement ................................... 538
  services interfaces .......................................... 21
  service-set statement ........................................ 521, 537
  shaping statement ............................................. 539
  short-sequence statement .................................... 539
  usage guidelines .............................................. 134, 137
  signal polarity, serial interfaces ........................ 539
  usage guidelines .............................................. 327
SONET interfaces
  APS See APS
  clock sources ............................................... 59, 374
  configuration statements ................................... 360
  damping interface transitions ................................ 376
  encapsulation ............................................... 51, 377
  example configuration ....................................... 379
  frame checksum .............................................. 363, 366
  framing bytes ............................................... 362
  HDLC payload scrambling .................................... 365, 366
  header byte values .......................................... 361, 366
  incrementing STM ID ........................................ 362
  leaky bucket properties .................................... 375
  link aggregation .............................................. 382
  loopback capability ........................................ 364
  MTU sizes ....................................................... 47, 48, 373
  overview ....................................................... 359
  path trace identifier ....................................... 365
  physical interface properties ................................ 360
  RFC 2615 support .............................................. 366
  See also SDH interfaces .................................... 359
SONET parameters
  on ATM interfaces ............................................ 154, 361
  on Channelized OC-12 interfaces .......................... 198
  sonet-options statement ..................................... 540
  usage guidelines .............................................. 154, 198, 205, 360
  source address filtering
    Fast Ethernet interfaces .................................. 266, 267, 279
    Gigabit Ethernet interfaces .............................. 266, 267, 279, 297
  source statement ............................................. 541
  usage guidelines .............................................. 260, 407
  source-address statement
    usage guidelines .............................................. 316
  source-address-filter statement .......................... 542
  usage guidelines .............................................. 266, 267, 279
  source-class usage
    example configuration ...................................... 95, 96
    for Layer 3 VPNs ............................................ 96
  source-class-usage statement ................................ 543
  usage guidelines .............................................. 94
source-filtering statement ........................................ 543
usage guidelines........................................ 266, 267, 279
speed statement .................................................. 544
usage guidelines........................................ 57, 282
stacked-vlan-tagging statement ................................ 544
usage guidelines........................................ 273
start-end flag
  E1 interfaces ........................................ 248
  E3 interfaces ........................................ 256
  T1 interfaces .......................................... 394
  T3 interfaces .......................................... 403
start-end-flag statement ........................................ 544
  E1 interfaces
    usage guidelines........................................ 248
  E3 interfaces
    usage guidelines........................................ 256
  T1 interfaces
    usage guidelines........................................ 394
  T3 interfaces
    usage guidelines........................................ 403
state (tracing flag) ........................................... 295
static ARP table entries
  Ethernet interfaces ...................................... 289
  example configuration ................................... 289
STM-1 interfaces
  example configuration ................................... 205
substrate option ............................................. 398
support, technical
  customer support, contacting......................... xli
swap statement ............................................... 545
  usage guidelines........................................ 273
Synchronous Digital Hierarchy See SDH interfaces
Synchronous Optical Network See SONET interfaces
syslog statement ............................................... 545
  usage guidelines........................................ 65
t1-options statement .......................................... 547
  usage guidelines........................................ 387
T3 interfaces
  BERT properties ......................................... 396
  buildout .................................................. 153
  C-bit parity mode ....................................... 397, 440
  configuration statements............................. 395
  CSU compatibility ....................................... 398
  encapsulation .......................................... 51, 404
  example configuration ................................... 404
  FEAC response .......................................... 399
  frame checksum ......................................... 399
  HDLC payload scrambling ................................ 403
  idle cycle flag .......................................... 400
  line buildout .......................................... 400
  loopback capability .................................... 401
  MTU sizes ................................................. 47, 48
  overview .................................................. 395
  start-end flag .......................................... 403
T3 QPP interfaces
  interface options ....................................... 195, 226
t391 statement ............................................... 548
  usage guidelines........................................ 331
t392 statement ............................................... 549
  usage guidelines........................................ 331
t3-options statement ........................................ 548
  usage guidelines........................................ 389
tag-protocol-id statement .................................. 549
  usage guidelines........................................ 273
TCC .......................................................... 99–103
  encapsulation .......................................... 54
  technical support
    customer support, contacting....................... xli
threshold statement ........................................... 550
  usage guidelines........................................ 60, 375
time slots
  Channelized E1 QPP interfaces ....................... 174, 207
  Channelized NxDS-0 QPP interfaces .................. 174, 208
  E1 interfaces .......................................... 249
  fractional E1 QPP interfaces ......................... 174, 191, 207, 223
  fractional T1 QPP interfaces .......................... 191, 223
  T1 interfaces .......................................... 394
timer (tracing flag) ......................................... 295
timers, APS.................................................. 371
T1 interfaces
  buildout ................................................... 389
  byte inversion .......................................... 389, 438
  configuration statements............................. 387
  data inversion .......................................... 390
  frame checksum ......................................... 390
  framing modes .......................................... 391
  idle cycle flag .......................................... 393
  line encoding .......................................... 391
  loopback capability .................................... 392
  MTU sizes ................................................. 47, 48
  overview .................................................. 387
  remote loopback response ................................ 390
  start-end flag .......................................... 394
time slots ................................................... 394
T1 QPP interfaces
  example configuration ................................... 222
  interface options ....................................... 196, 227
timeslots statement........................................550
Channelized E1 QPP interfaces
  usage guidelines........................................174, 207
Channelized NxDS-0 QPP interfaces
  usage guidelines........................................174, 208
E1 interfaces
  usage guidelines...........................................249
fractional E1 QPP interfaces
  usage guidelines........................................174, 191, 207, 223
fractional T1 QPP interfaces
  usage guidelines........................................191, 223
NxDS-0 QPP interfaces
  usage guidelines.............................................189
T1 interfaces
  usage guidelines...........................................394
tm statement................................................551
  usage guidelines...........................................352
tm-polarity statement......................................551
  usage guidelines...........................................355
tnp protocol family
  interface addresses.....................................81
  on logical interfaces.................................79
trace operations
  interface processes....................................108
  interfaces..................................................107
  VRRP..........................................................295
traceoptions statement
  interface processes.....................................553
  usage guidelines.........................................108
  interfaces..................................................552
  usage guidelines.........................................64, 107
  VRRP..........................................................554
  usage guidelines.........................................295
tracing flags
  all..........................................................64, 107
  event..........................................................64, 107
  ipc..............................................................64, 107
  media..........................................................64, 107
  VRRP
    all..........................................................295
    database....................................................295
    general.....................................................295
    interfaces..................................................295
    normal......................................................295
    packets.....................................................295
    state.........................................................295
    timer.........................................................295
tracing operations
  BGP..........................................................108
  track statement..........................................555
  usage guidelines.........................................295
  tracking logical interface status..................295
  traffic sampling
    configuring................................................315
  transient interfaces....................................19, 20
  transitions, damping..................................64, 376
translate-discard-eligible statement........................................556
  usage guidelines..........................................305
translate-fecn-and-becn statement........................................556
  usage guidelines..........................................305
translational cross-connect encapsulation See TCC encapsulation
translational cross-connect See TCC
transmit clock sources........................................59, 374
transmit-bucket statement........................................557
  usage guidelines..........................................60, 375
transmit-clock statement........................................557
  usage guidelines..........................................351
transmit-rate statement........................................644
  usage guidelines..........................................596
transmit-weight statement........................................558
  usage guidelines..........................................134, 144, 155
traps statement................................................559
  usage guidelines..........................................65, 74
Trivial Network Protocol See tnp protocol family
ttl statement..................................................559
  usage guidelines..........................................407
tunnel interfaces
  configuration statements...........................408, 409, 410
  example configuration...................................412
  loopback tunnels.........................................410
  multicast tunnels........................................409
  PIM tunnels.................................................411
  unicast tunnels..........................................408
  tunnel statement...........................................560
  usage guidelines..........................................408, 260, 408
  typefaces, documentation conventions..............xxxviii
  unicast RPF....................................................89
  example configuration...................................93
  fail filters..................................................92, 93
  loose mode...................................................91
  routing asymmetry........................................92
  strict mode..................................................90
  unicast tunnels.............................................408
  unit numbers.................................................71
  unit statement
    CoS..........................................................644
    usage guidelines..........................................594, 602
    logical interfaces........................................561
    usage guidelines..........................................67, 71
  unnumbered interfaces.....................................82
variable bandwidth rate See VBR

VBR ......................................................... 139
vbr statement ........................................ 564
  usage guidelines .................................. 139
vc-cos-mode statement ............................. 565
  usage guidelines .................................. 155
vci statement ........................................ 565
  usage guidelines .................................. 136
VCIs ...................................................... 117
VCs ....................................................... 127, 128, 129
virtual circuits, ATM See VCs ................. 117
virtual loopback tunnel
  VRF table lookup
    example configuration ...................................... 414
  virtual paths, ATM See VPs .......................... 117
Virtual Router Redundancy Protocol See VRRP 290
virtual-address statement ...................... 566
  usage guidelines .................................. 291
VLAN
  CCC configuration guidelines .................. 284
  example configuration ..................................... 284
VLAN CCC encapsulation
  encapsulation overhead ............................. 49
  physical interfaces ..................................... 51
VLAN IDs .............................................. 566, 567
VLAN tag stacking and rewriting
  example configuration ...................................... 274
Gigabit Ethernet QPP interfaces ................. 273
VLAN tagging ........................................ 282, 286, 568
VLAN VPLS
  configuration guidelines ......................... 284
  example configuration ..................................... 284
vlan-id statement ................................... 566
  Ethernet interfaces ................................... 566, 567
  usage guidelines ..................................... 282, 286
  Fast Ethernet interfaces
    usage guidelines ..................................... 282, 286
  Gigabit Ethernet interfaces
    usage guidelines ..................................... 282
    usage guidelines ..................................... 270, 273
vlan-tag statement ................................ 567
  usage guidelines ..................................... 284
vlan-tagging statement ............................ 568
  Ethernet interfaces
    usage guidelines ..................................... 282, 286
  Fast Ethernet interfaces
    usage guidelines ..................................... 282, 286
  Gigabit Ethernet interfaces
    usage guidelines ..................................... 282
vpi statement ........................................ 568
  physical interfaces
    usage guidelines ..................................... 127, 129
  point-to-point connections
    usage guidelines ..................................... 136
VPIs ...................................................... 117
vpl protocol family
  interface addresses ................................... 81
  on logical interfaces ................................... 79
VPs ...................................................... 127, 128, 129
VRRP
  advertisement interval .............................. 293
  authentication ........................................ 292
  backup router ......................................... 293, 294, 297
  basic configuration .................................. 291
  configuration statements .......................... 16
  example configuration .................................. 296
  trace operations ...................................... 295
  tracing flag ........................................... 295
  tracking logical interface status .................. 295
vrrp-group statement ............................. 569
  usage guidelines ..................................... 290, 291
VT mapping
  Channelized T1 QPP interfaces .................. 188, 190
  NxDS-0 QPP interfaces .................................. 190
vtmapping statement ................................ 570
  usage guidelines ..................................... 211
Wavelength-division multiplexing See WDM
WDM ....................................................... 359
working circuit, APS
  configuring ........................................... 368
  load sharing between paired groups .............. 372
  overview .............................................. 367
  paired groups, switching between ............... 370
  working-circuit statement ....................... 570
  usage guidelines ..................................... 368
yellow-differential-delay statement .......... 571
  usage guidelines ..................................... 330
z0-increment statement ........................... 571
  usage guidelines ..................................... 362
z3 SONET header byte ............................... 362
z4 SONET header byte ............................... 362
Index of Statements and Commands

A
accept-data statement ................................................................. 418
accept-source-mac statement .............................................................. 418
access-profile statement ............................................................... 419
accounting statement ................................................................. 419
accounting-profile statement ............................................................. 420
acknowledge-retries statement ........................................................... 420
acknowledge-timer statement ............................................................ 421
action-red-differential-delay statement ............................................... 421
address statement ............................................................................ 422
advertise-interval statement ............................................................... 423
aggregate statement ........................................................................ 424
aggregated-ether-options statement ...................................................... 425
aggregated-sonet-options statement ...................................................... 425
allow-any-vci statement .................................................................. 427
aps statement .................................................................................. 427
atm-encapsulation statement .............................................................. 427
atm-options statement ..................................................................... 428
atm-scheduler-map statement ............................................................. 429
authentication-key statement ............................................................. 429
authentication-type statement ............................................................. 431
auto-synchronize statement ................................................................. 432

B
backup-destination statement ........................................................... 432
backup-interface statement ................................................................. 433
bandwidth statement ....................................................................... 433, 623
bert-algorithm statement ................................................................. 434
bert-error-rate statement ................................................................. 435
bert-period statement ...................................................................... 435
boot-command statement ................................................................. 436
broadcast statement ......................................................................... 436
buffer-size statement ....................................................................... 623
buildout statement .......................................................................... 437
bundle statement .............................................................................. 438
byte-encoding statement ................................................................... 438
bytes statement ................................................................................ 439

c
802.3ad statement .............................................................................. 417
cbit-parity statement ......................................................................... 440
cbr statement .................................................................................... 440
cell-bundle-size statement ................................................................ 441
chap statement .................................................................................. 441
class statement ................................................................................ 624
classification-override statement ....................................................... 624
classifiers statement ........................................................................ 625
class-of-service statement ................................................................ 624
clocking statement ........................................................................... 443
clocking-mode statement .................................................................. 443
clock-rate statement ......................................................................... 442
code-point statement ........................................................................ 626
code-point-aliases statement ............................................................... 626
code-points statement ...................................................................... 627
compatibility-mode statement ............................................................. 444
connections statement ...................................................................... 445
control-leads statement .................................................................... 445
control-polarity statement ................................................................ 446
control-signal statement ................................................................... 446
core-dump statement ......................................................................... 447
cts statement .................................................................................... 447
cts-polarity statement ...................................................................... 448

d
dcd statement ................................................................................... 448
dcd-polarity statement ...................................................................... 449
dce statement .................................................................................... 449
description statement ....................................................................... 449
destination statement ........................................................................ 450
destination-class-usage statement ....................................................... 450
disable statement ............................................................................... 451
dlic statement ................................................................................... 451
drop-probability statement ................................................................. 627
drop-profile statement ...................................................................... 628
drop-profile-map statement ................................................................ 628
drop-profiles statement ..................................................................... 629
drop-timeout statement ..................................................................... 452
ds0-options statement ...................................................................... 452
dsr statement .................................................................................... 453
dsr-polarity statement ....................................................................... 453
dtr statement ....................................................................................... 454
dtr-circuit statement ......................................................................... 454
### Index of Statements and Commands

- `dtr-polarity statement` ............................................. 455
- `e1-options statement` ............................................. 455
- `e3-options statement` ............................................. 456
- `encapsulation statement` ........................................... 457
- `encoding statement` .................................................. 460
- `epd-threshold statement` ........................................... 461
- `es-options statement` ................................................ 462
- `ethernet-policer-profile statement` ............................. 462
- `ethernet-switch-profile statement` ............................... 463
- `eui-64 statement` ..................................................... 463
- `exp-push-push-push statement` ..................................... 629
- `exp-swap-push-push statement` ..................................... 630
- `fabric statement` ..................................................... 630
- `facility statement` .................................................... 538
- `facility-override statement` ................................ ...... 464
- `fail-filter statement` ................................................ 532
- `family statement` ..................................................... 465
- `fastether-options statement` ....................................... 467
- `fcs statement` ......................................................... 468
- `feac-loop-respond statement` ..................................... 468
- `fill-level statement` .................................................. 630
- `filter statement` ....................................................... 469
- `flow-control statement` ............................................. 469
- `force statement` ....................................................... 470
- `forwarding-class statement` ...................................... 470, 631
- `forwarding-classes statement` .................................... 632
- `forwarding-policy statement` ..................................... 633
- `fragment-threshold statement` .................................... 471
- `framing statement` .................................................... 471
- `gigether-options statement` ....................................... 472
- `gratuitous-arp-reply statement` .................................. 473
- `hello-timer statement` .............................................. 473
- `high-plp-max-threshold statement` .............................. 474
- `high-plp-threshold statement` .................................... 474
- `hold-time statement` ................................................ 475
- `host statement` ......................................................... 476
- `idle-cycle-flag statement` .......................................... 476
- `ignore-all statement` ................................................ 477
- `ilmi statement` ......................................................... 477
- `import statement` ...................................................... 633
- `inactivity-timeout statement` ..................................... 478
- `indication statement` ............................................... 478
- `indication-polarity statement` .................................... 478
- `ingress-rate-limit statement` ..................................... 479
- `input statement` ....................................................... 479
- `input-vlan-map statement` ....................................... 480
- `interfaces statement` ............................................... 482, 635
- `interface-switch statement` ....................................... 482
- `interface-type statement` .......................................... 481
- `interleave-fragments statement` ................................ 482
- `interpolate statement` .............................................. 635
- `inverse-arp statement` ............................................. 483
- `inverte-data statement` ............................................ 483
- `ipsec-sa statement` ................................................... 483
- `keep-address-and-control statement` ............................ 484
- `keepalive statement` ................................................. 485
- `keepalives statement` ............................................... 485
- `linear-red-profile statement` .................................... 487
- `linear-red-profiles statement` ................................... 487
- `line-encoding statement` .......................................... 486
- `line-protocol statement` .......................................... 486
- `link-mode statement` ............................................... 488
- `link-speed statement` .............................................. 488
- `limi statement` ....................................................... 489
- `limi-type statement` ................................................ 490
- `local-name statement` .............................................. 490
- `lockout statement` ................................................... 491
- `log-prefix statement` ............................................... 490
- `long-prefix statement` .............................................. 491
- `lsp-buildout statement` ............................................ 491
- `loopback statement` ................................................. 492, 494
- `loop-timing statement` ............................................... 492
- `loss-priority statement` ............................................ 636
- `low-plp-max-threshold statement` ............................... 494
- `low-plp-threshold statement` ..................................... 495
- `lsp-next-hop statement` ........................................... 636
- `mac statement` ......................................................... 495
- `mac-address statement` ............................................ 496
- `mac-learn-enable statement` ..................................... 496
- `maximum-vcs statement` .......................................... 497
- `minimum-links statement` ....................................... 498
- `mfruni-uni-bundle-options statement` .......................... 498
- `mode statement` ....................................................... 499
- `mrru statement` ....................................................... 499
- `mtu statement` ......................................................... 500
- `multicast-dcli statement` ....................................... 500
- `multicasts-only statement` ....................................... 501
- `multicast-vci statement` .......................................... 501
- `multipoint statement` ............................................... 501
<table>
<thead>
<tr>
<th>Statement</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>multipoint-destination statement</td>
<td>502</td>
</tr>
<tr>
<td>multiservice-options statement</td>
<td>503</td>
</tr>
<tr>
<td>n391 statement</td>
<td>503</td>
</tr>
<tr>
<td>n392 statement</td>
<td>504</td>
</tr>
<tr>
<td>n393 statement</td>
<td>504</td>
</tr>
<tr>
<td>neighbor statement</td>
<td>505</td>
</tr>
<tr>
<td>next-hop statement</td>
<td>636</td>
</tr>
<tr>
<td>next-hop-map statement</td>
<td>637</td>
</tr>
<tr>
<td>no-accept-data statement</td>
<td>505</td>
</tr>
<tr>
<td>no-asynchronous-notification statement</td>
<td>505</td>
</tr>
<tr>
<td>no-cbit-parity statement</td>
<td>440, 505</td>
</tr>
<tr>
<td>no-core-dump statement</td>
<td>447, 505</td>
</tr>
<tr>
<td>no-feac-loop-respond statement</td>
<td>468, 506</td>
</tr>
<tr>
<td>no-flow-control statement</td>
<td>506</td>
</tr>
<tr>
<td>no-gratuitous-arp-reply statement</td>
<td>473</td>
</tr>
<tr>
<td>no-gratuitous-arp-request statement</td>
<td>506</td>
</tr>
<tr>
<td>no-keepalives statement</td>
<td>506</td>
</tr>
<tr>
<td>no-long-buildout statement</td>
<td>491, 507</td>
</tr>
<tr>
<td>no-loopback statement</td>
<td>492, 507</td>
</tr>
<tr>
<td>no-loop-timing statement</td>
<td>492</td>
</tr>
<tr>
<td>no-mac-learn-enable statement</td>
<td>507</td>
</tr>
<tr>
<td>no-partition statement</td>
<td>507</td>
</tr>
<tr>
<td>no-payload-scrambler statement</td>
<td>508, 517</td>
</tr>
<tr>
<td>no-preempt statement</td>
<td>509, 522</td>
</tr>
<tr>
<td>no-redirects statement</td>
<td>509</td>
</tr>
<tr>
<td>no-source-filtering statement</td>
<td>509</td>
</tr>
<tr>
<td>no-syslog statement</td>
<td>509, 545</td>
</tr>
<tr>
<td>no-translate-discard-eligible statement</td>
<td>556</td>
</tr>
<tr>
<td>no-translate-fecn-and-becn statement</td>
<td>556</td>
</tr>
<tr>
<td>no-traps statement</td>
<td>559</td>
</tr>
<tr>
<td>no-z0-increment statement</td>
<td>509, 571</td>
</tr>
<tr>
<td>oam-liveness statement</td>
<td>510</td>
</tr>
<tr>
<td>oam-period statement</td>
<td>511</td>
</tr>
<tr>
<td>open-timeout statement</td>
<td>512</td>
</tr>
<tr>
<td>output statement</td>
<td>512</td>
</tr>
<tr>
<td>output-vlan-map statement</td>
<td>512</td>
</tr>
<tr>
<td>overflow statement</td>
<td>513</td>
</tr>
<tr>
<td>paired-group statement</td>
<td>513</td>
</tr>
<tr>
<td>partition statement</td>
<td>511, 514</td>
</tr>
<tr>
<td>passive statement</td>
<td>515</td>
</tr>
<tr>
<td>passive-monitor-mode statement</td>
<td>515</td>
</tr>
<tr>
<td>path-trace statement</td>
<td>516</td>
</tr>
<tr>
<td>payload-scrambler statement</td>
<td>517</td>
</tr>
<tr>
<td>per-unit-scheduler statement</td>
<td>517</td>
</tr>
<tr>
<td>pic-type statement</td>
<td>518</td>
</tr>
<tr>
<td>point-to-point statement</td>
<td>518</td>
</tr>
<tr>
<td>policer statement</td>
<td>519</td>
</tr>
<tr>
<td>pop statement</td>
<td>521</td>
</tr>
<tr>
<td>ppp-options statement</td>
<td>522</td>
</tr>
<tr>
<td>preempt statement</td>
<td>522</td>
</tr>
<tr>
<td>preferred statement</td>
<td>523</td>
</tr>
<tr>
<td>premium statement</td>
<td>523</td>
</tr>
<tr>
<td>primary statement</td>
<td>524</td>
</tr>
<tr>
<td>priority statement</td>
<td>524, 637</td>
</tr>
<tr>
<td>promiscuous-mode statement</td>
<td>525</td>
</tr>
<tr>
<td>protect-circuit statement</td>
<td>526</td>
</tr>
<tr>
<td>protocol statement</td>
<td>639</td>
</tr>
<tr>
<td>proxy statement</td>
<td>526</td>
</tr>
<tr>
<td>push statement</td>
<td>527</td>
</tr>
<tr>
<td>oam-liveness statement</td>
<td>510</td>
</tr>
<tr>
<td>oam-period statement</td>
<td>511</td>
</tr>
<tr>
<td>open-timeout statement</td>
<td>512</td>
</tr>
<tr>
<td>output statement</td>
<td>512</td>
</tr>
<tr>
<td>output-vlan-map statement</td>
<td>512</td>
</tr>
<tr>
<td>overflow statement</td>
<td>513</td>
</tr>
<tr>
<td>paired-group statement</td>
<td>513</td>
</tr>
<tr>
<td>partition statement</td>
<td>511, 514</td>
</tr>
<tr>
<td>passive statement</td>
<td>515</td>
</tr>
<tr>
<td>passive-monitor-mode statement</td>
<td>515</td>
</tr>
<tr>
<td>path-trace statement</td>
<td>516</td>
</tr>
<tr>
<td>payload-scrambler statement</td>
<td>517</td>
</tr>
<tr>
<td>per-unit-scheduler statement</td>
<td>517</td>
</tr>
<tr>
<td>pic-type statement</td>
<td>518</td>
</tr>
<tr>
<td>point-to-point statement</td>
<td>518</td>
</tr>
<tr>
<td>policer statement</td>
<td>519</td>
</tr>
<tr>
<td>pop statement</td>
<td>521</td>
</tr>
<tr>
<td>ppp-options statement</td>
<td>522</td>
</tr>
<tr>
<td>preempt statement</td>
<td>522</td>
</tr>
<tr>
<td>preferred statement</td>
<td>523</td>
</tr>
<tr>
<td>premium statement</td>
<td>523</td>
</tr>
<tr>
<td>primary statement</td>
<td>524</td>
</tr>
<tr>
<td>priority statement</td>
<td>524, 637</td>
</tr>
<tr>
<td>promiscuous-mode statement</td>
<td>525</td>
</tr>
<tr>
<td>protect-circuit statement</td>
<td>526</td>
</tr>
<tr>
<td>protocol statement</td>
<td>639</td>
</tr>
<tr>
<td>proxy statement</td>
<td>526</td>
</tr>
<tr>
<td>push statement</td>
<td>527</td>
</tr>
<tr>
<td>queue statement</td>
<td>640</td>
</tr>
<tr>
<td>queue-depth statement</td>
<td>527</td>
</tr>
<tr>
<td>queue-length statement</td>
<td>528</td>
</tr>
<tr>
<td>rate statement</td>
<td>528</td>
</tr>
<tr>
<td>receive-bucket statement</td>
<td>529</td>
</tr>
<tr>
<td>RED</td>
<td></td>
</tr>
<tr>
<td>drop-probability statement</td>
<td>627</td>
</tr>
<tr>
<td>drop-profile statement</td>
<td>628</td>
</tr>
<tr>
<td>drop-profiles statement</td>
<td>629</td>
</tr>
<tr>
<td>red-differential-delay statement</td>
<td>529</td>
</tr>
<tr>
<td>remote statement</td>
<td>530</td>
</tr>
<tr>
<td>remote-loopback-respond statement</td>
<td>530</td>
</tr>
<tr>
<td>request statement</td>
<td>531</td>
</tr>
<tr>
<td>revert-time statement</td>
<td>531</td>
</tr>
<tr>
<td>rewrite-rules statement</td>
<td>640</td>
</tr>
<tr>
<td>rfc-2615 statement</td>
<td>531</td>
</tr>
<tr>
<td>routing-instance statement</td>
<td>532</td>
</tr>
<tr>
<td>rpf-check statement</td>
<td>532</td>
</tr>
<tr>
<td>rts statement</td>
<td>532</td>
</tr>
<tr>
<td>rts-polarity statement</td>
<td>533</td>
</tr>
<tr>
<td>rtvbr statement</td>
<td>533</td>
</tr>
<tr>
<td>sampling statement</td>
<td>534</td>
</tr>
<tr>
<td>scheduler statement</td>
<td>641</td>
</tr>
<tr>
<td>scheduler-map statement</td>
<td>642</td>
</tr>
<tr>
<td>scheduler-maps statement</td>
<td>534, 643</td>
</tr>
<tr>
<td>schedulers statement</td>
<td>643</td>
</tr>
<tr>
<td>serial-options statement</td>
<td>535</td>
</tr>
<tr>
<td>service statement</td>
<td>536</td>
</tr>
<tr>
<td>service-domain statement</td>
<td>536</td>
</tr>
<tr>
<td>service-filter statement</td>
<td>537</td>
</tr>
<tr>
<td>service-options statement</td>
<td>538</td>
</tr>
<tr>
<td>service-set statement</td>
<td>521, 537</td>
</tr>
<tr>
<td>shaping statement</td>
<td>539</td>
</tr>
<tr>
<td>short-sequence statement</td>
<td></td>
</tr>
<tr>
<td>sonet-options statement</td>
<td>539</td>
</tr>
<tr>
<td>sonet-options statement</td>
<td>540</td>
</tr>
<tr>
<td>Statement</td>
<td>Page</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>source statement</td>
<td>541</td>
</tr>
<tr>
<td>source-address-filter statement</td>
<td>542</td>
</tr>
<tr>
<td>source-class-usage statement</td>
<td>543</td>
</tr>
<tr>
<td>source-filtering statement</td>
<td>543</td>
</tr>
<tr>
<td>speed statement</td>
<td>544</td>
</tr>
<tr>
<td>stacked-vlan-tagging statement</td>
<td>544</td>
</tr>
<tr>
<td>start-end-flag statement</td>
<td>544</td>
</tr>
<tr>
<td>swap statement</td>
<td>545</td>
</tr>
<tr>
<td>syslog statement</td>
<td>545</td>
</tr>
<tr>
<td>source statement</td>
<td>541</td>
</tr>
<tr>
<td>source-address-filter statement</td>
<td>542</td>
</tr>
<tr>
<td>source-class-usage statement</td>
<td>543</td>
</tr>
<tr>
<td>source-filtering statement</td>
<td>543</td>
</tr>
<tr>
<td>speed statement</td>
<td>544</td>
</tr>
<tr>
<td>stacked-vlan-tagging statement</td>
<td>544</td>
</tr>
<tr>
<td>start-end-flag statement</td>
<td>544</td>
</tr>
<tr>
<td>swap statement</td>
<td>545</td>
</tr>
<tr>
<td>syslog statement</td>
<td>545</td>
</tr>
<tr>
<td>t1-options statement</td>
<td>547</td>
</tr>
<tr>
<td>t391 statement</td>
<td>548</td>
</tr>
<tr>
<td>t392 statement</td>
<td>549</td>
</tr>
<tr>
<td>t3-options statement</td>
<td>548</td>
</tr>
<tr>
<td>tag-protocol-id statement</td>
<td>549</td>
</tr>
<tr>
<td>threshold statement</td>
<td>550</td>
</tr>
<tr>
<td>timeslots statement</td>
<td>550</td>
</tr>
<tr>
<td>tm statement</td>
<td>551</td>
</tr>
<tr>
<td>tm-polarity statement</td>
<td>551</td>
</tr>
<tr>
<td>traceoptions statement</td>
<td>551</td>
</tr>
<tr>
<td>interface processes</td>
<td>553</td>
</tr>
<tr>
<td>interfaces</td>
<td>552</td>
</tr>
<tr>
<td>VRRP</td>
<td>554</td>
</tr>
<tr>
<td>track statement</td>
<td>555</td>
</tr>
<tr>
<td>translate-discard-eligible statement</td>
<td>556</td>
</tr>
<tr>
<td>translate-fecn-and-becn statement</td>
<td>556</td>
</tr>
<tr>
<td>transmit-bucket statement</td>
<td>557</td>
</tr>
<tr>
<td>transmit-clock statement</td>
<td>557</td>
</tr>
<tr>
<td>transmit-rate statement</td>
<td>644</td>
</tr>
<tr>
<td>transmit-weight statement</td>
<td>558</td>
</tr>
<tr>
<td>traps statement</td>
<td>559</td>
</tr>
<tr>
<td>ttl statement</td>
<td>559</td>
</tr>
<tr>
<td>tunnel statement</td>
<td>560</td>
</tr>
<tr>
<td>unit statement</td>
<td>561</td>
</tr>
<tr>
<td>CoS</td>
<td>644</td>
</tr>
<tr>
<td>logical interfaces</td>
<td>561</td>
</tr>
<tr>
<td>vbr statement</td>
<td>564</td>
</tr>
<tr>
<td>vc-cos-mode statement</td>
<td>565</td>
</tr>
<tr>
<td>vc1 statement</td>
<td>565</td>
</tr>
<tr>
<td>virtual-address statement</td>
<td>566</td>
</tr>
<tr>
<td>vlan-id statement</td>
<td>566</td>
</tr>
<tr>
<td>vlan-tag statement</td>
<td>567</td>
</tr>
<tr>
<td>vlan-tagging statement</td>
<td>567</td>
</tr>
<tr>
<td>vpi statement</td>
<td>568</td>
</tr>
<tr>
<td>vrrp-group statement</td>
<td>569</td>
</tr>
<tr>
<td>vtmapping statement</td>
<td>570</td>
</tr>
<tr>
<td>working-circuit statement</td>
<td>570</td>
</tr>
<tr>
<td>yellow-differential-delay statement</td>
<td>571</td>
</tr>
<tr>
<td>z0-increment statement</td>
<td>571</td>
</tr>
</tbody>
</table>