JUNIPER NETWORKS

Junos® Space

Network Director Build Mode User Guide

Release
1.5

Published: 2013-10-15

Copyright © 2013, Juniper Networks, Inc.

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Copyright © 2013, Juniper Networks, Inc. All rights reserved.

Juniper Networks, Junos, Steel-Belted Radius, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. The Juniper Networks Logo, the Junos logo, and JunosE are trademarks of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Products made or sold by Juniper Networks or components thereof might be covered by one or more of the following patents that are owned by or licensed to Juniper Networks: U.S. Patent Nos. 5,473,599, 5,905,725, 5,909,440, 6,192,051, 6,333,650, 6,359,479, 6,406,312, 6,429,706, 6,459,579, 6,493,347, 6,538,518, 6,538,899, 6,552,918, 6,567,902, 6,578,186, and 6,590,785.

Junos® Space Network Director Build Mode User Guide
1.5
Copyright © 2013, Juniper Networks, Inc.
All rights reserved.

The information in this document is current as of the date on the title page.

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at http://www.juniper.net/support/eula.html. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

About the Documentation xxi
Documentation and Release Notes xxi
Documentation Conventions xxi
Documentation Feedback xxiii
Requesting Technical Support xxiii
Self-Help Online Tools and Resources xxiv
Opening a Case with JTAC xxiv

Part 1 Overview

Chapter 1 **Build Mode Overview 3**

Understanding Build Mode in Network Director 3
Discovering Devices 3
Building the Logical, Location, and Custom Views 4
Configuring Devices 4
Deploying Device Configurations 5
Importing Device Configurations 5
Out-of-Band Configuration Changes 6
Managing Devices 7
Understanding the Build Mode Tasks Pane 8

Chapter 2 **Device Configuration Overview 15**

Understanding Profiles 15
Understanding Access Profiles 21
Understanding Authentication Profiles 22
802.1X Authentication 22
MAC RADIUS Authentication 23
Captive Portal Authentication 23
Last Resort Authentication 23
Understanding Authorization Profiles 24
Understanding Auto AP Profiles 24
How Are Specifically Configured Access Points Different From Access Points Configured With Auto AP? 24
How Should I Use Auto AP Profiles? 25
How Does Auto AP Work? 25
Understanding Class of Service (CoS) Profiles 26
How Would I Use CoS? 26
How Do I Create CoS Groups? 27
How is CoS Different Than QoS? 27
How Does CoS Work? 27
What Wireless Network Traffic Aspects Can I Control With CoS? 28

Copyright © 2013, Juniper Networks, Inc.

What CoS Parameters Can I Control? . . . 28
What Are the Default CoS Traffic Types? . . . 29
Data Center Switching CoS Configuration . . . 30
How Do I Implement Class of Service? . . . 30
Understanding Device Common Settings Profiles . . . 30
Understanding Fabric Profiles . . . 30
Understanding Filter Profiles . . . 32
Understanding How To Add Access Points to a Wireless Network With Network Director . . . 33
Understanding Link Aggregation . . . 34
Understanding Multichassis Link Aggregation . . . 35
Understanding Port Profiles . . . 36
Interface Settings Configured in the Port Profile . . . 36
Interface Settings Configured by Referencing Other Profiles . . . 37
Data Center Device Port Profile Settings . . . 37
Default Port Profiles . . . 38
Understanding QFabric Setup . . . 41
Understanding Radio Profiles . . . 42
RF Scanning . . . 42
Spectral Scanning . . . 42
Dynamic Frequency Selection (DFS) Channels . . . 43
RFID Asset Tracking . . . 43
WMM Power Save . . . 44
Countermeasures . . . 44
Limiting Client Power . . . 44
802.11n Channel Width . . . 44
Automatic Channel Tuning . . . 44
Automatic Power Tuning . . . 45
IEEE 802.11 . . . 45
Long and Short Preamble Length . . . 45
Understanding Central Network Access With RADIUS and TACACS+ . . . 46
Why Do I Want Remote Authentication ? . . . 46
Why Not Just Rely on Firewalls and Filters for Access Control? . . . 46
What About Using LDAP For Authentication? . . . 47
Where Is RADIUS Installed on the Network? . . . 47
How Is TACACS+ Installed on the Network? . . . 47
A Comparison of RADIUS and TACACS+ . . . 48
Understanding VLAN Profiles . . . 49
Understanding WLAN Service Profiles . . . 52
SSID . . . 53
Beaconing the SSID Name . . . 53
Mapping WLAN Service Profiles to Additional Profiles . . . 53
SSID Encryption . . . 53
Authentication Used for Encryption Methods . . . 54
Associated Authentication Profile . . . 54
Associated Authorization Profile . . . 54
VLAN Use . . . 54
Bandwidth Limit For Client Sessions . . . 54
Load Balancing Between Access Points . . . 54

Copyright © 2013, Juniper Networks, Inc.

Using Proxy ARP . . . 54
Restricting DHCP . . . 55
Client Types . . . 55
Call Admission Control Settings For Voice . . . 55
Retry Count . . . 56
Client Timeouts . . . 56
802.11n Settings . . . 56
Guard Intervals . . . 56
Frame Aggregation . . . 56
MAC Service Data Unit (MSDU) Length . . . 57
MPDU Length . . . 57
Maximum Bandwidth Used by an SSID . . . 57
Maximum Transmission Unit Parameter . . . 57
Client Probing of Idle Clients . . . 57
Enable Pre-shared Key (PSK) For WPA or WPA2 . . . 57
Create a Pre-shared Key (PSK) Phrase For WPA or WPA2 . . . 58
Create a Pre-shared Key (PSK) Raw Phrase For WPA or WPA2 . . . 58
Enforce Data Rates . . . 58
Retry Count For Sending Frames . . . 58
WPA Encryption Type Used . . . 58
Shared Key Authentication Values . . . 58
Radio Transmit Rates Used . . . 59
WMM Power Save . . . 59
Understanding Network Director SSID Configuration With Profiles . . . 59
Configuring an SSID with Network Director . . . 60
SSID Access Information . . . 61
SSID Authentication Information . . . 61
SSID WLAN Information . . . 61
SSID Radio Information . . . 61
What Do I Do When All of These Profiles Are Complete? . . . 62

Chapter 3 Topology View Overview . . . 63

Understanding the Location View . . . 63
Understanding the Network Topology in Network Director . . . 65
Understanding the Topology View Tasks pane . . . 68

Chapter 4 Virtual View Overview . . . 71

Understanding Virtual Networks . . . 71
Understanding Virtual Network Management . . . 72
Understanding the Build Mode Tasks Pane for Virtual View . . . 74

Chapter 5 Custom View Overview . . . 77

Understanding Custom Groups . . . 77
Where is the Custom Group Function Located in Network Director? . . . 77
How Do Custom Group Rules Work? . . . 78
What Happens When I Edit a Custom Group Rule? . . . 79
When Are Rules Executed? . . . 79

Chapter 6 Mobility Domain Overview . . . 81

Understanding Mobility Domains . . . 81

Copyright © 2013, Juniper Networks, Inc.

Chapter 7 Additional Wireless Configuration Concepts 83

Understanding Access Point Bias for Controllers 84
How Do I Determine The Bias Settings I should Use? 84
Example of a Layer 3 Network With Multiple Controllers 85
A Third Option for Access Point Bias - Sticky 85
How Do I Set the Controller Bias for an Access Point? 85
How Can I Determine the Bias of an Access Point By Looking at a Controller? 86
What About Controller Clusters? 86
Understanding Channel Auto-Tuning and Adaptive Channel Planner on Wireless Networks 86
Why Use Channel Auto-Tuning? 87
When Should I Use Channel Auto-Tuning? 87
Channel Auto-Tuning to Improve Performance 87
Channel Auto-Tuning to Resolve Interference 88
Channel Auto-Tuning Is Used by Dynamic Frequency Selection to Comply With Country Regulations 88
How Does Channel Auto-Tuning Work? 88
How Do I Configure Automatic Channel Tuning? 89
What Are The Results of Auto-Tuning? 89
When is Auto-Tuning Most Beneficial? 90
What Happens when Severe Interference is Detected? 90
Understanding Automatic Power Tuning for Wireless Radios 91
How Does Wireless Transmit Power Work? 91
How Does Power Tuning Work? 92
When is Power Tuning Most Helpful? 92
How Do I Turn Off Power Tuning? 92
What Changes Can I Make to Automatic Power Tuning? 92
Understanding Call Admission Control 93
What Radios Does Call Admission Control Affect? 93
How Do I Configure Call Admission Control? 94
Understanding Distributed Access Point Behavior on a Layer 3 Network 94
What Is a Layer 3 Network? 94
How Does an Access Point Find a Controller on a Layer 3 Network? 95
Understanding Load Balancing for Wireless Radios 97
Why Would I Need Load Balancing? 97
When Would I Avoid Load Balancing? 97
How Load Balancing Works 97
Where Do I Configure Load Balancing? 98
Understanding WPA-PSK and WPA2-PSK Authentication 98
What are WPA PSK and WPA2 PSK? 99
How Do WPA-PSK and WPA2-PSK Work? 99
When Would I Use PSK Authentication? 99
Why Would I Not Use PSK Authentication? 99
How Is WPA Encryption Different Than WPA-PSK Encryption? 100
Understanding the IEEE 802.11 Standard for Wireless Networks 100
Differences Between 802.11 Standards 101
802.11 Divides Each Frequency Band into Channels 102
What is 802.11i Security? 102

Copyright © 2013, Juniper Networks, Inc.

What is 802.1X? . . . 102
Understanding the Network Terms SSID, BSSID, and ESSID . . . 103
An SSID is the Name of a Network . . . 103
BSSIDs Identify Access Points and Their Clients . . . 104
Ad-Hoc Networks Do Not Have a MAC Address . . . 105
An ESS Consists of BSSs . . . 105
Understanding Voice Clients and Voice Traffic . . . 105
What is Voice Over IP? . . . 106
Voice over Wireless Phones . . . 106
Private Branch Exchange (PBX) . . . 106
How is Voice Traffic Different Than Data Traffic? . . . 106
Latency, Jitter, and Packet Loss Affect Voice Traffic . . . 106
Voice Traffic is Susceptible to Roaming Issues . . . 106
What Protocols are Used for Voice? . . . 107
What is Different About Configuring For Voice Traffic? . . . 107
Consider Using Call Admission Control (CAC) to Limit Clients Per Access Point . . . 107
Ensure That Network Equipment Supports Seamless Roaming . . . 108
Support Quality of Service on all Hardware Used for Voice . . . 108
Use Automatic Power Save Delivery to Preserve the Battery Life of Phones . . . 108
Create a Unique WLAN Service Profile for Voice . . . 108
Create a Unique Radio Profile for Voice . . . 108
Understanding Wireless Encryption and Ciphers . . . 109
Wired Equivalent Privacy (WEP) Was the Original Wireless Encryption . . . 109
WPA Encryption Replaced WEP . . . 110
WPA2 is the Strongest Encryption Available . . . 110
Security Ciphers For WPA and WPA2 . . . 110
Which Encryption Method Should I Use? . . . 111
Understanding Wireless Interference . . . 112
What Causes Wireless Radio Frequency Interference? . . . 112
Effects of Interference Seen By Clients . . . 113
You Can Monitor RF Interference With Network Director . . . 113
What is RF Jamming? . . . 113
Understanding Wireless Radio Channels . . . 114
What WLAN Channels Are Available? . . . 114
What Channels Are Not Available? . . . 115
How Do I Know Which Channels I Should Use? . . . 115
How Do I Avoid Co-Channel Interference? . . . 116
DFS Channels . . . 116
802.11n Channels Can Be Wider and Work on Both Bands . . . 116
How Are Channel Numbers Assigned? . . . 117
How Do I know What Channel an Access Point is Using? . . . 117
Understanding Wireless Scanning . . . 117
What is the Difference Between Passive and Active Scanning? . . . 118
What Channels Are Scanned? . . . 118
How Does Scanning Work? . . . 118
How Does Active Scanning Work? . . . 119
What Additional Information is Learned By An Active Scan? . . . 119

Copyright © 2013, Juniper Networks, Inc.

What Happens to Scanned Information? . . . 119
CTS-to-self During Scanning . . . 120
What is Spectral RF Scanning? . . . 120
Understanding WMM Power Save and WLAN Client Battery Life . . . 121
How Does WMM Power Save Extend Battery Life? . . . 121
Where is WMM Defined? . . . 122
How is WMM Power Save Implemented on Juniper WLANs? . . . 122
WMM Power Save is Disabled by Default . . . 122
Why Should I Enable WMM Power Save in a Radio Profile? . . . 122

Part 2 Configuration

Chapter 8 **Device Configuration . . . 125**

Adding and Managing an Access Point . . . 126
Configuring Individual Access Points . . . 127
Configuring Access Point Options . . . 128
Adding an Access Point to a Wireless Network . . . 129
Defining an Access Point . . . 129
Defining Access Point Radios . . . 130
Configuring Fibre Channel Gateways . . . 132
Using the FC Gateway Service Profile to Configure FC Gateways . . . 132
Using a Combination of Profiles to Configure FC Gateways . . . 132
Configuring a Voice SSID with Network Director . . . 133
Creating a CoS Profile Dedicated to Voice . . . 133
Creating a WLAN Service Profile Dedicated to Voice . . . 134
Creating and Managing Access Profiles . . . 136
Managing Access Profiles . . . 136
Creating an Access Profile . . . 137
Specifying Basic Settings for an EX Series Switching or Data Center Switching Access Profile . . . 139
Specifying RADIUS Accounting Settings for an EX Switching or Data Center Switching Access Profile . . . 141
Specifying Basic Settings for a Wireless Access Profile . . . 143
Specifying Server Group Settings for a Wireless Access Profile . . . 144
Specifying Basic Settings for a Campus Switching ELS Access Profile . . . 151
Specifying RADIUS and LDAP Settings for Campus Switching ELS . . . 151
Reviewing and Modifying the Access Profile Settings . . . 156
What To Do Next . . . 157
Creating and Managing Authentication Profiles . . . 157
Managing Authentication Profiles . . . 158
Creating an Authentication Profile . . . 159
Specifying Authentication Settings for Switches . . . 160
Specifying Authentication Settings for Wireless . . . 163
What To Do Next . . . 167
Creating and Managing Wireless Authorization Profiles . . . 167
Managing Authorization Profiles . . . 168
Creating a Wireless Authorization Profile . . . 169
Specifying Settings for a Wireless Authorization Profile . . . 171
What To Do Next . . . 174

Copyright © 2013, Juniper Networks, Inc.

Creating and Managing Wireless Auto AP Profiles 174
Managing Wireless Auto AP Profiles 175
Creating a Wireless Auto AP Profile 177
Specifying Basic Settings for a Wireless Auto AP Profile 178
Specifying LLDP & Remote AP Settings for a Wireless Auto AP Profile 179
Specifying Advanced Settings for a Wireless Auto AP Profile 181
Reviewing a Wireless Auto AP Profile 183
What To Do Next 183
Creating and Managing CoS Profiles 184
Managing CoS Profiles 184
Using the Default CoS Profiles for Switches 185
Default CoS Profiles for Data Center Switching 186
Creating a CoS Profile 187
Specifying Settings for a Switching CoS Profile 188
Specifying Settings for a Wireless CoS Profile 192
Specifying Settings for a Data Center Switching CoS Profile 194
What To Do Next 198
Creating and Managing Device Common Settings 198
Managing Device Common Settings 199
Creating Device Common Settings Profiles 200
Specifying Basic Settings for Device Common Settings 202
Specifying Management Settings for EX Switching Device Common Settings 205
Specifying Management Settings for Wireless Device Common Settings . . 208
Specifying Management Settings for Campus Switching ELS Device Common Settings 211
Specifying Management Settings for Data Center Device Common Settings 214
Specifying Protocol Settings for EX Switching Device Common Settings . . 216
Specifying DNS Settings for Wireless Device Common Settings 218
Specifying DHCP Relay/DNS Settings for Campus Switching ELS Device Common Settings 219
Specifying Protocol Settings for Data Center Switching Device Common Settings 220
Reviewing and Saving a Device Common Settings Configuration 222
What To Do Next 222
Creating and Managing Fabric Profiles 223
Managing Fabric Profiles 223
Creating Fabric Profiles 224
Specifying Settings for a Fabric profile 225
What to Do Next 227
Creating and Managing FC Gateway Service Profiles 228
Managing FC Gateway Service Profiles 228
Creating FC Gateway Service Profiles 229
Specifying Settings for an FC Gateway Service Profile 230
What to Do Next 230

Copyright © 2013, Juniper Networks, Inc.

Creating and Managing Filter Profiles . . . 231
Managing Filter Profiles . . . 231
Creating a Filter Profile . . . 232
Specifying Settings for an EX Series Switch Filter Profile . . . 233
Specifying Settings for a Wireless Filter Profile (WLC) . . . 245
Specifying Settings for a Campus Switching ELS Switch Filter Profile . . . 250
Specifying Settings for Creating a Data Center Switching Filter Profile . . . 262
What To Do Next . . . 273
Creating and Managing LDAP Profiles . . . 273
Managing LDAP Profiles . . . 274
Creating LDAP Profiles . . . 275
Specifying Settings for an LDAP Profile . . . 275
What to Do Next . . . 277
Managing and Creating a Link Aggregation Group . . . 278
Link Aggregation Group Options . . . 279
Creating a Link Aggregation Group . . . 280
Managing ICCP Settings . . . 282
What To Do Next . . . 282
Creating and Managing Port Profiles . . . 283
Managing Port Profiles . . . 283
Creating Port Profiles . . . 285
Specifying Settings for an EX Switching Port Profile . . . 286
Specifying Settings for a Campus Switching ELS Port Profile . . . 295
Specifying Settings for the Data Center Switching Port Profile . . . 305
What to Do Next . . . 315
Creating and Managing a Radio Profile . . . 315
Managing Radio Profiles . . . 316
Before You Create a Radio Profile . . . 317
Creating a Radio Profile . . . 318
Specifying Radio Profile Basic Settings . . . 319
Specifying the Power & RF Settings . . . 321
Specifying Radio Profile Radio Options . . . 322
Reviewing the Radio Profile Configuration . . . 325
What To Do Next . . . 325
Creating and Managing RADIUS Profiles . . . 326
Managing RADIUS Profiles . . . 326
Creating RADIUS Profiles . . . 327
Specifying Settings for a RADIUS profile . . . 328
What to Do Next . . . 329
Creating a Radio Profile for Voice Clients Only . . . 329
Creating and Managing VLAN Profiles . . . 330
Managing VLAN Profiles . . . 331
Creating a VLAN Profile . . . 332
Specifying Basic EX Switching VLAN Settings . . . 334
Specifying Basic Wireless VLAN Settings . . . 335
Specifying Basic Campus Switching ELS VLAN Settings . . . 335
Specifying Basic VLAN Settings for Data Center Switching . . . 337
Specifying Advanced VLAN Profile Settings for EX Series Switches . . . 338
Specifying Advanced VLAN Profile Settings for Wireless VLANs . . . 340

Copyright © 2013, Juniper Networks, Inc.

Specifying Advanced VLAN Settings for a Campus Switching ELS Profile . . 344
Specifying Advanced VLAN Profile Settings for Data Center Switching . . . 346
Reviewing and Saving the VLAN Profile Configuration 350
What To Do Next 350
Creating and Managing a WLAN Service Profile 350
Managing WLAN Service Profiles 351
Before You Create a WLAN Service Profile 352
Creating a WLAN Service Profile 353
Specifying the Basic Settings for a WLAN Service Profile 354
Mapping an Authentication Profile to the WLAN Service Profile 356
Mapping an Authorization Profile to the WLAN Service Profile 359
Specifying Security Settings for a WLAN Service Profile 360
Specifying the Advanced Settings for a WLAN Service Profile 362
Reviewing the WLAN Service Profile Summary 367
What To Do Next 367
Creating a WLAN Service Profile Dedicated to Voice 368
Assigning Authorization Profiles to Controllers 369
Assigning Authorization Profiles 369
Editing Authorization Profile Assignments 371
Assigning an Auto AP Profile to Controllers 371
Controller Selection for Auto AP Assignment 372
Assigning the Auto AP Profile to Controllers 373
Reviewing and Assigning the Auto AP Profile Configuration 374
Editing Auto AP Profile Assignments 374
What To Do Next 375
Assigning Device Common Settings to Devices 375
Assigning Device Common Settings 375
Editing the Assignments of the Device Common Setting 377
Assigning a Fabric Profile to Devices and Ports 377
Assigning a Fabric Profile 378
Editing the Assignments of a Fabric Profile 380
Assigning an FC Gateway Service Profile to Ports 381
Assigning an FC Gateway Service Profile 381
Editing the Assignments of an FC Gateway Service Profile 383
Assigning a Port Profile to Interfaces 383
Selecting Devices for Assignment 384
Assigning a Port Profile to Interfaces 385
Reviewing and Accepting the Assignments 387
Editing Profile Assignments 387
Assigning a Radio Profile to Radios 389
Selecting the Controllers for Radio Profile Assignment 390
Assigning the Radio Profile to Radios 390
Editing Radio Profile Assignments 392
Assigning a VLAN Profile to Devices or Ports 392
Assigning a VLAN Profile 393
Editing Profile Assignments 395

Copyright © 2013, Juniper Networks, Inc.

Chapter 9 Network Domain and Mobility Domain Configuration 397
Creating a Mobility Domain for Wireless LAN Controllers 398
Creating Network Domains for Wireless LAN Controllers 401
Chapter 10 Topology View Configuration 403
Assigning and Unassigning Devices to a Location 403
How to Assign or Unassign Devices 404
Assigning Devices 404
Changing the Location of a Device 405
How to Move a Device to a New Location 405
Changing the Location of a Device 405
Configuring Buildings 406
How to Add or Edit a Building 406
Adding or Editing a Building for a Location 406
Configuring Floors 407
How to Add or Edit a Floor 407
Adding or Editing a Building Floor for a Location 408
Configuring Outdoor Areas 408
How to Configure an Outdoor Area 409
Configuring an Outdoor Area 409
Creating a Site 409
How to Add or Edit a Location Site 410
Creating or Editing a Site 410
Deleting Sites, Buildings, Floors, Wiring Closets, and Devices 410
How to Delete a Location Object 411
Deleting Sites 411
Deleting Buildings 411
Deleting Floors 411
Deleting Closets 411
Deleting Devices 412
Setting Up Closets 412
How to Add or Edit a Closet 412
Adding or Editing a Wiring Closet 413
Setting Up the Location View 414
Setting Up and Managing the Topology View 417
Viewing the Network Topology 417
Refreshing the Device Discovery 419
Viewing Topology 420
Viewing Topology Discovery Job 420
Setting Up the Location View 421
Viewing the Alarm Details 421
Displaying Device Connectivity 422
Displaying QFabric Connectivity 424
Uploading Floor Plans 426
Uploading Topology Map 426

Copyright © 2013, Juniper Networks, Inc.

Chapter 11 Virtual View Configuration 429
Guidelines for Migrating from Virtual Control to Network Director 430
Discovering Devices in a Virtual Network 430
Specifying the vCenter Targets 431
Specifying the Virtual Network Credentials 432
Reviewing the Virtual Network Discovery Options 432
Viewing the Discovery Status 433
Managing Virtual Networks 434
Modify Virtual Network Details 434
Configure Orchestration Mode 435
Delete Virtual Networks 436
Resynchronize Virtual Networks 436
Viewing the Virtual Machine Inventory in a Virtual Network 437
Viewing the Virtual Switch Inventory in a Virtual Network 438
Viewing the Host Inventory in a Virtual Network 439
Managing Network Adapter Associations 440
Manage Network Adapter Associations 441
Configure Network Adapter Associations 441
Delete Network Adapter Associations 442
Viewing Connections Between Virtual Machines and a Physical Switch 443
Viewing Network Connectivity of a Virtual Machine 443
Viewing Connections Between a Physical Switch and Virtual Machines . . . 443
Viewing Virtual Port Groups 444
Chapter 12 Custom Group Configuration 447
Creating Custom Groups 447
Creating Custom Groups 447
Specifying Settings for a Custom Group 448
Part 3 Administration
Chapter 13 Device Discovery 455
Discovering Devices in a Physical Network 455
Specifying the Target Devices 456
Specifying the Discovery Options 457
Specifying the Schedule Options 459
Reviewing the Device Discovery Options 459
Viewing the Discovery Status 459
Discovering Devices in a Virtual Network 460
Specifying the vCenter Targets 461
Specifying the Virtual Network Credentials 462
Reviewing the Virtual Network Discovery Options 462
Viewing the Discovery Status 463
Chapter 14 Device Management 465
Accessing a Device's CLI from Network Director 465
Accessing a Device's Web-Based Interface from Network Director 466

Copyright © 2013, Juniper Networks, Inc.

Assigning Devices to Logical Category 467
Creating and Managing Multichassis Link Aggregation Groups (MC-LAGs) 468
Selecting Devices for the MC-LAG 468
Configuring MC-LAG Settings 469
Managing MC-LAGs 470
What To Do Next 470
Deleting Devices 471
Rebooting Devices 472
Setting Up QFabrics 472
Managing Node Aliases 472
Managing Node Groups 473
Identifying CPE Switches 474
Reviewing the QFabric Summary and Deploying Changes 474
Viewing the Device Inventory Page 475
Viewing the Physical Inventory of Devices 477
Viewing a Device's Current Configuration from Network Director 478
Viewing Licenses With Network Director 478
Viewing Profiles Assigned to a Device 480

Part 4 Troubleshooting

Chapter 15 **Troubleshooting Device Discovery 485**

Troubleshooting Device Discovery Error Messages 485

Copyright © 2013, Juniper Networks, Inc.

List of Figures

Part 1 Overview

Chapter 1 **Build Mode Overview . . . 3**

Figure 1: Manage VLAN Profiles Page . . . 5

Chapter 2 **Device Configuration Overview . . . 15**

Figure 2: Profile Relationships . . . 17
Figure 3: VLANs Are Specific to Device Families and Function Levels . . . 50
Figure 4: SSID Information is Located in These Profiles . . . 60
Figure 5: Relationship Between Profiles Needed to Create an SSID . . . 61

Chapter 3 **Topology View Overview . . . 63**

Figure 6: Typical Floor Plan Displaying the Closets and Devices . . . 66
Figure 7: Typical Floor Plan Displaying the Racks and QFX Devices . . . 67

Chapter 4 **Virtual View Overview . . . 71**

Figure 8: Virtualized Server . . . 72
Figure 9: Network View of Virtual Machines . . . 73

Chapter 7 **Additional Wireless Configuration Concepts . . . 83**

Figure 10: Controllers With High Bias and Low Bias For an Access Point . . . 85
Figure 11: Access Point Booting Over a Layer 3 Network . . . 95
Figure 12: Radios can have up to 32 SSIDs . . . 103
Figure 13: Each Access Point Has Its Own BSS . . . 104
Figure 14: Network Security is Provided by Encryption, Authentication and Authorization . . . 109
Figure 15: Scanned Data is Stored in the Station Databases and Sent to the Controller . . . 119

Part 2 Configuration

Chapter 10 **Topology View Configuration . . . 403**

Figure 16: Main Topology Window . . . 418
Figure 17: Displaying the Connection Details for an EX4200 Switch in Graphical View . . . 423
Figure 18: Displaying the Connection Details for an EX4200 Switch in Grid View . . . 423
Figure 19: Displaying the Connection Details for a QFabric Switch in Graphical View . . . 425

Copyright © 2013, Juniper Networks, Inc.

Copyright © 2013, Juniper Networks, Inc.

List of Tables

About the Documentation xxi

Table 1: Notice Icons xxii
Table 2: Text and Syntax Conventions xxii

Part 1 Overview

Chapter 1 Build Mode Overview 3

Table 3: Device Discovery Tasks 9
Table 4: Device Management Tasks 9
Table 5: Domain Management Tasks 10
Table 6: Location Management Tasks 11
Table 7: Connectivity Tasks 12
Table 8: Profile and Configuration Management Tasks 12

Chapter 2 Device Configuration Overview 15

Table 9: Profile Associations at Various Levels 18
Table 10: 3-Bit CoS Field in Ethernet Header With VLAN Tagging 27
Table 11: Adding Access Points to a Wireless Network With Network Director . . . 33
Table 12: Maximum Interfaces per LAG and Maximum LAGs per Switch 34
Table 13: Default Port Profiles 38
Table 14: RADIUS and TACACS+ 48

Chapter 3 Topology View Overview 63

Table 15: Topology View Tasks 68

Chapter 4 Virtual View Overview 71

Table 16: Virtual Networks Management Tasks 74
Table 17: Inventory Tasks 75
Table 18: Connectivity Tasks 75

Chapter 5 Custom View Overview 77

Table 19: Three Options of a Rule Statement 78

Chapter 7 Additional Wireless Configuration Concepts 83

Table 20: Configuring Bias on Controllers and Access Points 84
Table 21: Access Point Connecting to a Controller in a Layer 3 Network 96
Table 22: Differences Between 802.11 Protocols 101
Table 23: Channels a Device Can Use 116

Part 2 Configuration

Chapter 8 Device Configuration 125

Table 24: Manage Access Point Fields 129

Copyright © 2013, Juniper Networks, Inc.

Table 25: Access Point Configuration 129
Table 26: Access Point Radio Settings 131
Table 27: Manage Access Profile Fields 137
Table 28: Access Profile Basic Settings for EX Series Switches and Data Center Switching 139
Table 29: Accounting Settings for an EX Switching and Data Center Switching Access Profile 141
Table 30: Access Profile Basic Settings for Wireless 143
Table 31: Server Group Settings 146
Table 32: Access Profile Basic Settings for Campus Switching ELS 151
Table 33: Authentication and Accounting Server Settings for ELS Campus Switching 152
Table 34: Manage Authentication Profile Fields 158
Table 35: Authentication Profile Settings for Switches 160
Table 36: Authentication Profile Advanced Settings for Switches 162
Table 37: Authentication Profile Wireless Settings 164
Table 38: Wireless Access Rule Settings 164
Table 39: Wireless Web Portal Authentication 166
Table 40: Manage Authorization Profile Fields 168
Table 41: Authorization Profile Basic Settings (WLC) 172
Table 42: Authorization Profile Advanced Settings (WLC) 173
Table 43: Manage Auto AP Profiles Fields 175
Table 44: Wireless Auto AP Basic Settings 178
Table 45: Wireless Auto AP LLDP & Remote AP Settings 179
Table 46: Wireless Auto AP Profile Advanced Settings 181
Table 47: Manage CoS Profile Fields 185
Table 48: CoS Profile Settings for EX and ELS Switching 188
Table 49: Traffic Configuration and Shaping for EX Switching and Campus Switching ELS 188
Table 50: CoS Rewrite Rules for EX and ELS Switching 191
Table 51: CoS Profile Basic Settings for Wireless 192
Table 52: CoS Profile Basic Settings for Data Center Switching 194
Table 53: Add Priority Group and Traffic Control Profile Window 194
Table 54: Priority Group and Traffic Settings Table Properties 195
Table 55: Edit and Add Traffic Classification and Shaping for priority group Window 195
Table 56: PFC Settings for Data Center Switching Hierarchical Port Scheduling (ETS) CoS Profile 197
Table 57: PFC Settings for Data Center Switching Non-Hierarchical Port Scheduling CoS Profile 197
Table 58: Rewrite Rule Settings for Data Center Switching CoS Profile 197
Table 59: Manage Device Common Settings Fields 199
Table 60: Device Profile Basic Settings 202
Table 61: Device Profile Management Settings for EX Switching 206
Table 62: Device Profile Management Settings for Wireless 209
Table 63: Management Settings for ELS Switching Device Profile 212
Table 64: Device Profile Management Settings for Data Center 215
Table 65: Device Profile Protocol Settings for EX Switching 217
Table 66: Device Profile DNS Settings for Wireless 218

Copyright © 2013, Juniper Networks, Inc.

Table 67: Device Profile Protocol Settings for ELS Switching 219
Table 68: Device Profile Protocol Settings for Data Center 221
Table 69: Fabric Profile Information 224
Table 70: Fabric Profile Settings 225
Table 71: FC Gateway Service Profile Information 229
Table 72: FC Gateway Service Profile Settings 230
Table 73: Manage Filter Profile Fields 232
Table 74: Create Term Fields for EX Switching 234
Table 75: Term Fields for Wireless 246
Table 76: Create Term Fields for Campus Switching ELS 251
Table 77: Create Term Fields for Data Center 263
Table 78: LDAP Profile Information 274
Table 79: LDAP Profile Settings 276
Table 80: LACP (Link Aggregation Control Protocol) Configuration Fields 279
Table 81: ICCP Settings 282
Table 82: Manage Port Profiles Table 284
Table 83: Port Profile Basic Settings for an EX Switching Port Profile 286
Table 84: Port Profile Advanced Settings 293
Table 85: Port Profile Basic Settings For Campus Switching ELS 296
Table 86: Port Profile Advanced Settings for Campus Switching ELS 302
Table 87: Port Profile Basic Settings for Data Center Ports 306
Table 88: Port Profile Settings for Data Center Ethernet Ports 310
Table 89: Port Profile Advanced Settings for Data Center Ethernet Ports 312
Table 90: Port Profile Settings for Data Center FC Ports 314
Table 91: Radio Profile Fields 317
Table 92: Radio Profile Basic Settings 319
Table 93: Radio Power & RF Settings 321
Table 94: Radio Options 323
Table 95: RADIUS Profile Information 327
Table 96: RADIUS Profile Settings 328
Table 97: Manage VLAN Profile Fields 331
Table 98: VLAN Profile Basic Settings for EX Switching 334
Table 99: VLAN Wireless Profile Basic Settings 335
Table 100: VLAN Profile Basic Settings for Campus Switching ELS 335
Table 101: VLAN Profile Basic Settings 337
Table 102: VLAN Profile Advanced Settings for an EX Series Switch 338
Table 103: VLAN Profile Advanced Settings for a Wireless LAN Controller 340
Table 104: VLAN Profile Advanced Settings for Campus Switching ELS 344
Table 105: VLAN Profile Advanced Settings for a Data Center Switching Ethernet VLAN 346
Table 106: VLAN Profile Advanced Settings for a Data Center Switching FCoE VLAN 348
Table 107: Manage WLAN Service Profile Fields 351
Table 108: WLAN Service Profile Basic Settings 354
Table 109: Options for Mapping an Authentication Profile to a WLAN Service Profile 356
Table 110: Options for Linking the WLAN Service Profile to an Authorization Profile 359
Table 111: WLAN Service Profile Security Settings 361

Copyright © 2013, Juniper Networks, Inc.

Table 112: WLAN Service Profile Advanced Settings 363
Table 113: Fabric Profile Object-Specific Interface Attributes 380
Table 114: Configure Device Attributes for Port Profile Assignments 386
Table 115: Edit Assignment for Port Profile Fields 388

Chapter 10 **Topology View Configuration 403**

Table 116: Contents of Selected Device Details 405
Table 117: Add or Edit Building Fields 406
Table 118: Floor Field Descriptions 408
Table 119: Outdoor Area Fields 409
Table 120: Site Creation Fields 410
Table 121: Devices that can be Assigned to each Location Component 414
Table 122: Refresh Topology Job Details 420
Table 123: Job Details for Topology Discovery 421

Chapter 11 **Virtual View Configuration 429**

Table 124: Viewing Device Discover Jobs 433
Table 125: Modify Virtual Network Credentials Field Descriptions 434
Table 126: Manage Virtual Machines Page Field Descriptions 437
Table 127: Manage Virtual Switches Page Field Descriptions 438
Table 128: Manage Hosts Page Field Descriptions 439
Table 129: Manage Physical Switch Associations 441
Table 130: View Virtual Port Group Field Descriptions 444

Chapter 12 **Custom Group Configuration 447**

Table 131: Three Options of a Rule Statement 449

Part 3 Administration

Chapter 13 **Device Discovery 455**

Table 132: Viewing Device Discover Jobs 459
Table 133: Viewing Device Discover Jobs 463

Chapter 14 **Device Management 465**

Table 134: MC-LAG Settings 469
Table 135: ICCP-LAG Settings 470
Table 136: Manage Node Alias Table 473
Table 137: Fields in the Device Inventory Table 475
Table 138: Fields in the Device Physical Inventory Table 477
Table 139: Viewing Licenses with Network Director 478
Table 140: Additional Licensing Information 479
Table 141: Details of Assigned Profiles to a Device 480

Copyright © 2013, Juniper Networks, Inc.

About the Documentation

- Documentation and Release Notes on page xxi
- Documentation Conventions on page xxi
- Documentation Feedback on page xxiii
- Requesting Technical Support on page xxiii

Documentation and Release Notes

To obtain the most current version of all Juniper Networks® technical documentation, see the product documentation page on the Juniper Networks website at http://www.juniper.net/techpubs/.

If the information in the latest release notes differs from the information in the documentation, follow the product Release Notes.

Juniper Networks Books publishes books by Juniper Networks engineers and subject matter experts. These books go beyond the technical documentation to explore the nuances of network architecture, deployment, and administration. The current list can be viewed at http://www.juniper.net/books.

Documentation Conventions

Table 1 on page xxii defines notice icons used in this guide.

Copyright © 2013, Juniper Networks, Inc.

Table 1: Notice Icons

Icon	Meaning	Description
	Informational note	Indicates important features or instructions.
	Caution	Indicates a situation that might result in loss of data or hardware damage.
	Warning	Alerts you to the risk of personal injury or death.
	Laser warning	Alerts you to the risk of personal injury from a laser.

Table 2 on page xxii defines the text and syntax conventions used in this guide.

Table 2: Text and Syntax Conventions

Convention	Description	Examples
Bold text like this	Represents text that you type.	To enter configuration mode, type the **configure** command: user@host> **configure**
`Fixed-width text like this`	Represents output that appears on the terminal screen.	`user@host>` **show chassis alarms** `No alarms currently active`
Italic text like this	• Introduces or emphasizes important new terms. • Identifies guide names. • Identifies RFC and Internet draft titles.	• A policy *term* is a named structure that defines match conditions and actions. • *Junos OS CLI User Guide* • RFC 1997, *BGP Communities Attribute*
Italic text like this	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name: [edit] root@# **set system domain-name** *domain-name*
Text like this	Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components.	• To configure a stub area, include the **stub** statement at the **[edit protocols ospf area area-id]** hierarchy level. • The console port is labeled **CONSOLE**.
< > (angle brackets)	Enclose optional keywords or variables.	**stub <default-metric** *metric***>;**

Copyright © 2013, Juniper Networks, Inc.

Table 2: Text and Syntax Conventions *(continued)*

Convention	Description	Examples
| (pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	**broadcast | multicast** **(*string1* | *string2* | *string3*)**
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	**rsvp { # Required for dynamic MPLS only**
[ ] (square brackets)	Enclose a variable for which you can substitute one or more values.	**community name members [*community-ids*]**

Indention and braces ({ })	Identify a level in the configuration hierarchy.	[edit]
		routing-options {
		  static {
		  route default {
		  nexthop *address*;
		  retain;
		  }
		  }
		}

; (semicolon)	Identifies a leaf statement at a configuration hierarchy level.	
GUI Conventions		
Bold text like this	Represents graphical user interface (GUI) items you click or select.	• In the Logical Interfaces box, select **All Interfaces**. • To cancel the configuration, click **Cancel**.
> (bold right angle bracket)	Separates levels in a hierarchy of menu selections.	In the configuration editor hierarchy, select **Protocols>Ospf**.

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can send your comments to **techpubs-comments@juniper.net**, or fill out the documentation feedback form at https://www.juniper.net/cgi-bin/docbugreport/ . If you are using e-mail, be sure to include the following information with your comments:

- Document or topic name
- URL or page number
- Software release version (if applicable)

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or JNASC support contract,

Copyright © 2013, Juniper Networks, Inc.

or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at http://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf.
- Product warranties—For product warranty information, visit http://www.juniper.net/support/warranty/.
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: http://www.juniper.net/customers/support/
- Search for known bugs: http://www2.juniper.net/kb/
- Find product documentation: http://www.juniper.net/techpubs/
- Find solutions and answer questions using our Knowledge Base: http://kb.juniper.net/
- Download the latest versions of software and review release notes: http://www.juniper.net/customers/csc/software/
- Search technical bulletins for relevant hardware and software notifications: https://www.juniper.net/alerts/
- Join and participate in the Juniper Networks Community Forum: http://www.juniper.net/company/communities/
- Open a case online in the CSC Case Management tool: http://www.juniper.net/cm/

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: https://tools.juniper.net/SerialNumberEntitlementSearch/

Opening a Case with JTAC

You can open a case with JTAC on the Web or by telephone.

- Use the Case Management tool in the CSC at http://www.juniper.net/cm/.
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, see http://www.juniper.net/support/requesting-support.html.

Copyright © 2013, Juniper Networks, Inc.

PART 1

Overview

- Build Mode Overview on page 3
- Device Configuration Overview on page 15
- Topology View Overview on page 63
- Virtual View Overview on page 71
- Custom View Overview on page 77
- Mobility Domain Overview on page 81
- Additional Wireless Configuration Concepts on page 83

Copyright © 2013, Juniper Networks, Inc.

Copyright © 2013, Juniper Networks, Inc.

CHAPTER 1

Build Mode Overview

- Understanding Build Mode in Network Director on page 3
- Understanding the Build Mode Tasks Pane on page 8

Understanding Build Mode in Network Director

In Build mode, you build the network managed by Junos Space Network Director. It provides you with the ability to use device discovery to bring devices under Network Director management, to customize your view of the devices, to configure devices, and to perform some common device management tasks.

This topic describes:

- Discovering Devices on page 3
- Building the Logical, Location, and Custom Views on page 4
- Configuring Devices on page 4
- Managing Devices on page 7

Discovering Devices

Device discovery finds your network devices and brings them under Network Director management. You provide Network Director with identifying information about the devices you want Network Director to manage—an IP address or hostname, an IP address range, an IP subnetwork, or a CSV file that contains this information. Network Director uses the information to probe the devices by using either ping or SNMP get requests. If a device probe is successful, Network Director then attempts to make an SSH connection to the device using the login credentials you supply. If the connection is successful and the device is a supported device, Network Director adds the device to its database of managed devices. Network Director uses Juniper Network's Device Management Interface (DMI), which is an extension to the NETCONF network configuration protocol, to connect to and configure its managed devices.

You can also discover devices using the device discovery feature provided by the Junos Space Network Management Platform. Devices you discover using Junos Space device discovery are brought under Network Director management if they are supported by Network Director.

Besides bringing your devices under Network Director management, device discovery:

Copyright © 2013, Juniper Networks, Inc.

- Reads the device configuration and saves it in the Junos Space configuration database. Network Director uses this record of the device configuration to determine what configuration commands it needs to send to a device when you deploy the configuration on the device. For this reason, it is important for the Junos Space configuration record to match, or be in sync with, the device configuration. For more information about how the Junos Space configuration record and device configuration are kept in sync, see *Understanding Resynchronization of Device Configuration*.
- Imports the device configuration into the Build mode configuration. For more information about importing device configurations, see "Importing Device Configurations" on page 5.

Building the Logical, Location, and Custom Views

When a device is discovered in the physical network mode, it is added to the network tree in the View pane. In Logical view, all switches are added to the Unassigned node under the switching network. You can then assign them to the Access, Aggregation, or Core nodes to complete the Logical view of the switching network. The Logical view of the wireless network is built for you.

Similarly, in Location view, all discovered devices are added to the Unassigned node. You can use Build mode to create your Location view—that is, create the sites, buildings, floors, closets, and outdoor areas that reflect the physical location of your network devices—and to assign the discovered devices to these locations.

The Custom Group view displays only the top level—My Network—until you create one or more custom groups. Custom group is another way of grouping your devices based on your business needs. You can create custom groups and add devices to each custom group. You can manually add devices to a custom group or you can define rules to add devices, that match the rule condition, to the custom group once they are discovered by Network Director. You can view the custom groups and devices that are assigned to each group in the Custom Group view.

NOTE: This section does not apply to virtual devices that Network Director manages.

Configuring Devices

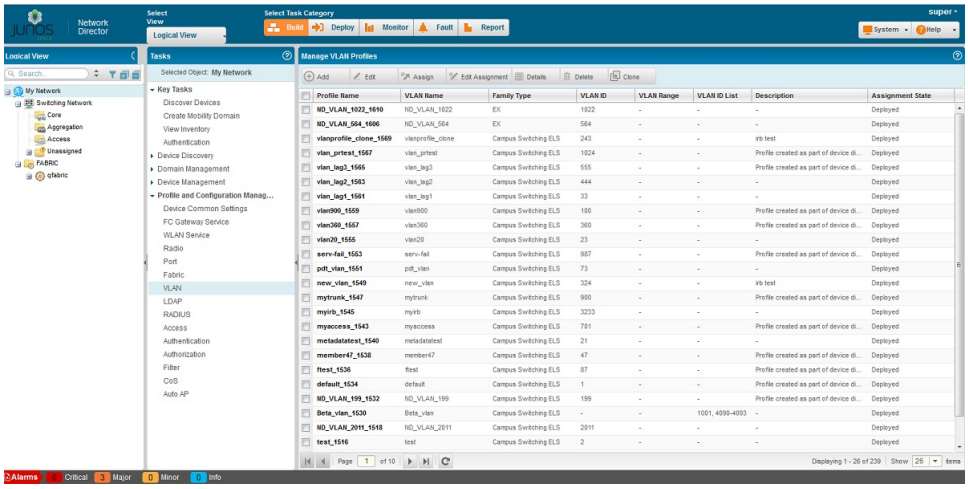
In Build mode, you can define the configuration of network devices in your Physical network. To support rapid, large-scale deployment of devices, you can define much of your Build mode configuration in a set of profiles. You can reference profiles in other profiles or apply them to multiple objects in your network—devices, ports, radios, logical entities. For example, you can create a Port profile that sets up class-of-service (CoS), authentication, firewall filters, and Ethernet switching settings that are appropriate for access ports that connect to employee desktop VoIP phones and then assign that profile to access ports across multiple switches.

Copyright © 2013, Juniper Networks, Inc.

NOTE: This section does not apply to virtual devices that Network Director manages.

Figure 1 on page 5 shows an example landing page for profile configuration, in this case VLAN profiles. This page lists all existing VLAN profiles. From this page you can create new profiles, modify or delete existing profiles, assign profiles to objects, and change or view assignments. For more information about profiles, see "Understanding Profiles" on page 15.

Figure 1: Manage VLAN Profiles Page



In addition to creating configuration profiles, in Build mode you can configure wireless mobility and network domains, enable Smart Mobile Virtual Controller Clustering, configure access points on controllers, configure Link Aggregation Groups (LAGs) on switches, and so on.

Deploying Device Configurations

After you build your device configurations in Build mode, you need to deploy the configurations on the devices. None of the configurations you create in Build mode affect your devices until the configurations are actually deployed on the devices.

To deploy the configuration on devices, use Deploy mode. When you change a device's configuration in Build mode, the device becomes available in Deploy mode for configuration deployment.

For more information about deploying configuration changes, see *Understanding Deploy Mode in Network Director*.

Importing Device Configurations

As part of device discovery, Network Director analyzes the configuration of a newly discovered device and automatically imports the configuration into the Build mode configuration for that device. For example, as part of the discovery of a wireless LAN controller, Network Director imports the configurations of wireless access points from

Copyright © 2013, Juniper Networks, Inc.

the controller and makes them available for viewing and modification under the Manage Access Point task for that controller.

As it imports the device configuration, Network Director automatically creates profiles to match the configuration. It first determines whether any existing profiles match the configuration, and if so, assigns those profiles to the device. It then creates and assigns new profiles as needed. For example, if an access switch has some ports that match the configuration of an existing Port profile, Network Director assigns the existing Port profile to those ports. For the other ports, Network Director creates as many Port profiles as needed to match the port configurations and assigns them to the ports.

You can manage the profiles that Network Director creates as part of device discovery in the same way that you manage user-created profiles—that is, you can modify, delete, or assign them to other devices.

Out-of-Band Configuration Changes

Out-of-band configuration changes are configuration changes made to a device outside of Network Director. Examples include changes made by:

- Using the device CLI.
- Using the device Web-based management interface (the J-Web interface or Web View).
- Using the Junos Space Network Management Platform configuration editor.

NOTE: **You cannot use the Junos Space configuration editor to configure wireless LAN controllers.**

- Using RingMaster software.
- Restoring or replacing device configuration files.

When an out-of-band change is made, the device configuration no longer matches the Build mode configuration, and the device configuration state changes to out of sync. You cannot deploy configuration on a device that is out of sync. Use the Resynchronize Device Configuration task in Deploy mode to resynchronize the device configuration. For more information about how Network Director resolves out-of-band configuration changes and synchronizes the Build mode configuration with the device configuration, see *Understanding Resynchronization of Device Configuration*.

TIP: **Before you make configuration changes in Build mode, make sure that devices that will be affected are in sync. Resynchronizing the device configuration can result in losing pending Build mode configuration changes for that device.**

Copyright © 2013, Juniper Networks, Inc.

Managing Devices

In addition to the tasks that allow you to build your network, Build mode provides a number of tasks for day-to-day device management. For example, you can:

- View a device's hardware component inventory or its installed licenses
- Reboot a device or groups of devices
- Connect to a device's CLI through SSH or to its web-based management interface
- View the profiles assigned to a device
- Set up QFabric devices.

Related Documentation

- Understanding the Build Mode Tasks Pane on page 8
- *Understanding the Network Director User Interface*
- Understanding Profiles on page 15
- *Understanding Deploy Mode in Network Director*
- *Understanding Resynchronization of Device Configuration*

Copyright © 2013, Juniper Networks, Inc.

Understanding the Build Mode Tasks Pane

The Tasks pane in Build mode contains all the tasks you can do in Build mode. Click a specific task to begin that task.

The tasks listed in the Tasks pane depend on the scope you select in the View pane—that is, what view (Logical, Location, Device, Virtual, or Custom Group) you have selected and what object you have selected. Not all tasks are available in all scopes. As you change your selections in the View pane, the contents of the Tasks pane also change.

Build mode tasks are divided into the following categories in the Tasks pane.

Network Director enables you to perform the following tasks for devices in your physical network:

- **Device Discovery**—Before your devices can be managed by Network Director, you must use device discovery to discover them. As Network Director discovers devices, it adds them to your network view in the View pane. Table 3 on page 9 describes the device discovery tasks.
- **Device Management**—After devices have been discovered, you can perform administrative tasks on them, such as viewing a list of the device's physical components, connecting to a device using SSH, rebooting a device, or assigning a switch to its logical role in the network. Table 4 on page 9 describes the device management tasks.
- **Domain Management**—You can create and modify mobility and network domains in your wireless network. Table 5 on page 10 describes the domain management tasks.
- **Location Management**—You can build your Location view of the network by creating sites, buildings, floors, closets, and outdoor areas and assigning devices to these locations. Table 6 on page 11 describes the location management tasks.
- **Connectivity**—For switches in your network that are connected to your virtual network, you can view the connectivity between a given switch and the corresponding virtual switch and between the virtual switch and the virtual machine. Table 7 on page 12 describes the connectivity tasks.
- **Profile and Configuration Management**—Network Director provides a set of configuration profiles that you can create to provision multiple devices in your network. Table 8 on page 12 describes the profile and configuration management tasks.
- **Key Tasks**—Network Director enables you to group the tasks that you perform frequently and create a list of key tasks. You can add any task from the Tasks pane to the Key Tasks list by selecting a task and clicking the plus (+) sign that appears adjacent to the task. For some modes, you can see that Network Director has predefined some key tasks for you. You can modify this set of tasks to suit your requirements. This feature is available in Task pane irrespective of your current mode, scope, or view.

For more information about Build mode features, see "Understanding Build Mode in Network Director" on page 3.

Table 3 on page 9 through Table 8 on page 12 describe the tasks that you can perform in the physical network category, including the scope in the View pane that you must

 Copyright © 2013, Juniper Networks, Inc.

select to access the task.

Table 3: Device Discovery Tasks

Task	Description	Scope
Discover Devices	Discovers supported switches and wireless LAN controllers in the network and brings them under Network Director management. Access points are discovered when their associated controllers are discovered.	Any
View Discovery Status	Displays the status of device discovery jobs.	Any

Table 4: Device Management Tasks

Task	Description	Scope
Assign Device to Logical Category	Assigns switches to one of the following logical categories within the switching network: Core, Aggregation, Access.	View: Logical Object: Switching Network, Core, Aggregation, Access, Unassigned, or an individual switch
Change Location of Device	Changes where a device is located in Location view.	View: All Object: Individual switch, controller, or access point
Create MC-LAG	Configures multichassis link aggregation groups (MC-LAG).	View: All Object: All
Delete Devices	Deletes a switch or a wireless LAN controller as a managed device from Network Director. If you select a scope that contains more than one switch or controller, you can choose which devices are deleted.	View: All Object: All, except access points
Launch RingMaster	Launches Juniper Networks RingMaster, using the URL set under Preferences.	View: All Object: Wireless Network, wireless domains and clusters, wireless devices
Launch Web View	Launches the Web-based management interface for the selected device in a separate window: the J-Web interface for EX Series switches and Web View for wireless LAN controllers.	View: All Object: Individual switch or controller
Manage Access Point	Adds an access point to the selected wireless LAN controller or cluster. Also, deletes an access point from the selected controller or cluster or changes the access point configuration.	View: Logical Object: Controller or cluster
Manage Port Groups	Enables you to create and manage port groups. Port groups enable you to configure a group of ports with a single configuration.	View: Logical Object: Switching Network, Core, Aggregation, Access, Unassigned, an individual switch (both EX Series and QFX Series)

Copyright © 2013, Juniper Networks, Inc.

Table 4: Device Management Tasks *(continued)*

Task	Description	Scope
Reboot Devices	Reboots devices. If you select a scope that contains more than one switch or controller, you can choose which devices get deleted.	View: All Object: All
Setup QFabric	Sets up a QFabric device.	View: All Object: QFabric device
Show Current Configuration	Shows the running configuration on a switch or a wireless LAN controller.	View: All Object: Individual switch or controller
SSH to Device	Launches an SSH connection to the selected device.	View: All Object: Individual switch or controller
Validate Pending Configuration	Validates configuration changes that have not yet been deployed on devices.	View: All Object: All
View Assigned Profiles	Displays the profiles assigned to the selected device.	View: All Object: Individual switch, controller, or radio
View Inventory	Displays information about all the devices in the currently selected object and all its child objects.	View: All Object: All
View License Information	View the licenses installed on the device and their status.	View: All Object: Individual switch or controller
View Physical Inventory	Displays information about the selected device's hardware components.	View: All Object: Individual switch or controller

Table 5: Domain Management Tasks

Task	Description	Scope
Create Mobility Domain	Creates a mobility domain within the wireless network and optionally enables clustering.	View: Logical Object: My Network or Wireless Network only
Create Network Domain	Creates a network domain within the wireless network.	View: Logical Object: My Network or Wireless Network only
Delete Mobility Domain Edit Mobility Domain	Modifies or deletes a mobility domain.	View: Logical Object: A mobility domain
Delete Network Domain Edit Network Domain	Modifies or deletes a network domain.	View: Logical Object: A network domain node

Copyright © 2013, Juniper Networks, Inc.

Table 6: Location Management Tasks

Task	Description	Scope
Add Building	Creates a new building in the selected site. NOTE: Use this task only to create the building. Floors and closets in the building must be created separately.	View: Location Object: A site
Add Closet	Creates a new closet in the selected floor.	View: Location Object: A floor
Add Floor	Creates a new floor in the selected building. NOTE: Use this task only to create the floor. Closets in the building must be created separately.	View: Location Object: A building
Add Outdoor Area	Creates a new outdoor area in the selected site.	View: Location Object: A site
Add Site	Creates a new site in Location view. NOTE: Use this task only to create the site object. Buildings, floors, closets, and outdoor areas in the site must be created separately.	View: Location Object: My Network only
Delete Building/Edit Building	Deletes or modifies the selected building.	View: Location Object: A building
Delete Closet/Edit Closet	Deletes or modifies the selected closet.	View: Location Object: A closet
Delete Floor/Edit Floor	Deletes or modifies the selected floor.	View: Location Object: A floor
Delete Outdoor Area/Edit Outdoor Area	Deletes or modifies the selected outdoor area.	View: Location Object: An outdoor area
Delete Site/Edit Site	Deletes or modifies the selected site.	View: Location Object: A site
Assign Devices to Building	Assigns switches or wireless LAN controllers to a building. You cannot assign access points to a building.	View: Location Object: A building
Assign Devices to Closet	Assigns switches or wireless LAN controllers to a closet. You cannot assign access points to a closet.	View: Location Object: A closet
Assign Devices to Floor	Assigns access points, switches, or wireless LAN controllers to a floor.	View: Location Object: A floor
Assign Devices to Outdoor Area	Assigns access points to an outdoor area.	View: Location Object: An outdoor area

Copyright © 2013, Juniper Networks, Inc.

Table 6: Location Management Tasks *(continued)*

Task	Description	Scope
Setup Locations	Opens the page by using which you can create an entire site—that is, define buildings, floors, closets, outdoor areas and to assign devices to these locations. NOTE: Use this task only to create a site. Do not use it to modify an existing site.	View: Location Object: My Network and any location node within an existing site.

Table 7: Connectivity Tasks

Task	Description	Scope
View Virtual Network Connectivity	Pictorially displays the network connectivity between the selected switch and the virtual switch and between the virtual switch and the virtual machine. If the selected switch is not connected to a virtual network, Network Director displays the standalone switch.	View: Logical, Location, Device Object: Individual switch
View Virtual Machines	Displays the virtual machines that are connected to the selected switch.	View: Logical, Location, Device Object: Individual switch

Table 8: Profile and Configuration Management Tasks

Task	Description	Device Family	Scope
Access	Creates and manages Access profiles. Use Access profiles to configure authentication methods (RADIUS, LDAP, and local), accounting methods (RADIUS and LDAP), and authentication/accounting servers.	EX Series QFX Series WLC Series	Any
Authentication	Creates and manages Authentication profiles. Use Authentication profiles to specify authentication method and authentication parameters for authenticating clients and users who connect to a WLAN or to an access port on a switch.	EX Series QFX Series WLC Series	Any
Authorization	Creates and manages authorization profiles. Use Authorization profiles to configure authorization attributes for users, such as the VLAN to place the users in, firewall filters to apply to the user traffic, time-of-day access restrictions, and so forth.	WLC Series	Any
Auto AP	Creates and manages Auto AP profiles. Use Auto AP profiles to define the configuration of distributed access points that are not explicitly configured on the controller.	WLC Series	Any
CoS	Creates and manages CoS profiles. Use CoS profiles to configure class-of-service (CoS) attributes to be applied to interfaces or to user traffic.	EX Series QFX Series WLC Series	Any

Copyright © 2013, Juniper Networks, Inc.

Table 8: Profile and Configuration Management Tasks *(continued)*

Task	Description	Device Family	Scope
Device Common Settings	Creates and manages Device Common Settings profiles. Use Device Common Settings profiles to configure basic system settings, such as users, time and time servers, SNMP, system logging, and so on.	EX Series QFX Series WLC Series	Any
Fabric	Creates and manages Fabric profiles. Use Fabric profiles to configure gateway FC fabrics on QFX Series devices that act as a FCoE-FC gateway.	QFX Series	Any
FC Gateway Service	Provides a quick way to configure Fibre Channel (FC) gateways on Data Center Switching devices.	QFX Series	Any
Filter	Creates and manages Filter profiles. Use Filter profiles to define Layer 2 and Layer 3 firewall filters (ACLs).	EX Series QFX Series WLC Series	Any
LDAP	Creates and manages LDAP profiles. Use LDAP profiles to specify details about your LDAP authentication and accounting server. LDAP profiles can then be linked to an access profile.		Any
Port	Creates and manages Port profiles for EX Series switches. Use Port profiles to configure interface settings, such as PoE settings, protocol family, port mode, physical link settings, firewall filters, and port security settings for interfaces.	EX Series QFX Series	Any
Radio	Creates and manages Radio profiles. Use Radio profiles to specify radio behavior that is in common across multiple radios, including the SSIDs advertised by the radio.	WLC Series	Any
Radius	Creates and manages Radius profiles. Use Radius profiles to specify details about your RADIUS authentication and accounting server. Radius profiles can then be linked to an access profile.		
VLANs	Creates and manages VLAN profiles. Use VLAN profiles to define VLANs, including the firewall filters to be applied to the VLANs and other settings.	EX Series QFX Series WLC Series	Any
WLAN Service	Creates and manages WLAN Service profiles. Use WLAN Service profiles to create SSIDs and their attributes, such as beaconing, encryption, and default authorization for users accessing the SSID.	WLC Series	Any

Related Documentation

- Understanding Build Mode in Network Director on page 3
- Understanding Profiles on page 15
- *Understanding the Network Director User Interface*

Copyright © 2013, Juniper Networks, Inc.

- Understanding the Build Mode Tasks Pane for Virtual View on page 74

Copyright © 2013, Juniper Networks, Inc.

CHAPTER 2

Device Configuration Overview

- Understanding Profiles on page 15
- Understanding Access Profiles on page 21
- Understanding Authentication Profiles on page 22
- Understanding Authorization Profiles on page 24
- Understanding Auto AP Profiles on page 24
- Understanding Class of Service (CoS) Profiles on page 26
- Understanding Device Common Settings Profiles on page 30
- Understanding Fabric Profiles on page 30
- Understanding Filter Profiles on page 32
- Understanding How To Add Access Points to a Wireless Network With Network Director on page 33
- Understanding Link Aggregation on page 34
- Understanding Multichassis Link Aggregation on page 35
- Understanding Port Profiles on page 36
- Understanding QFabric Setup on page 41
- Understanding Radio Profiles on page 42
- Understanding Central Network Access With RADIUS and TACACS+ on page 46
- Understanding VLAN Profiles on page 49
- Understanding WLAN Service Profiles on page 52
- Understanding Network Director SSID Configuration With Profiles on page 59

Understanding Profiles

To support rapid network deployment, Junos Space Network Director enables you to define your network configuration in a set of profiles that you can apply to multiple objects in your network. For example, you can define a Port profile to set up class-of-service (CoS), authentication, firewall filters, and Ethernet switching settings that are appropriate for all access ports in your network that connect to employee desktop VoIP phones.

After you have defined a profile, you can associate it with devices in one of two ways:

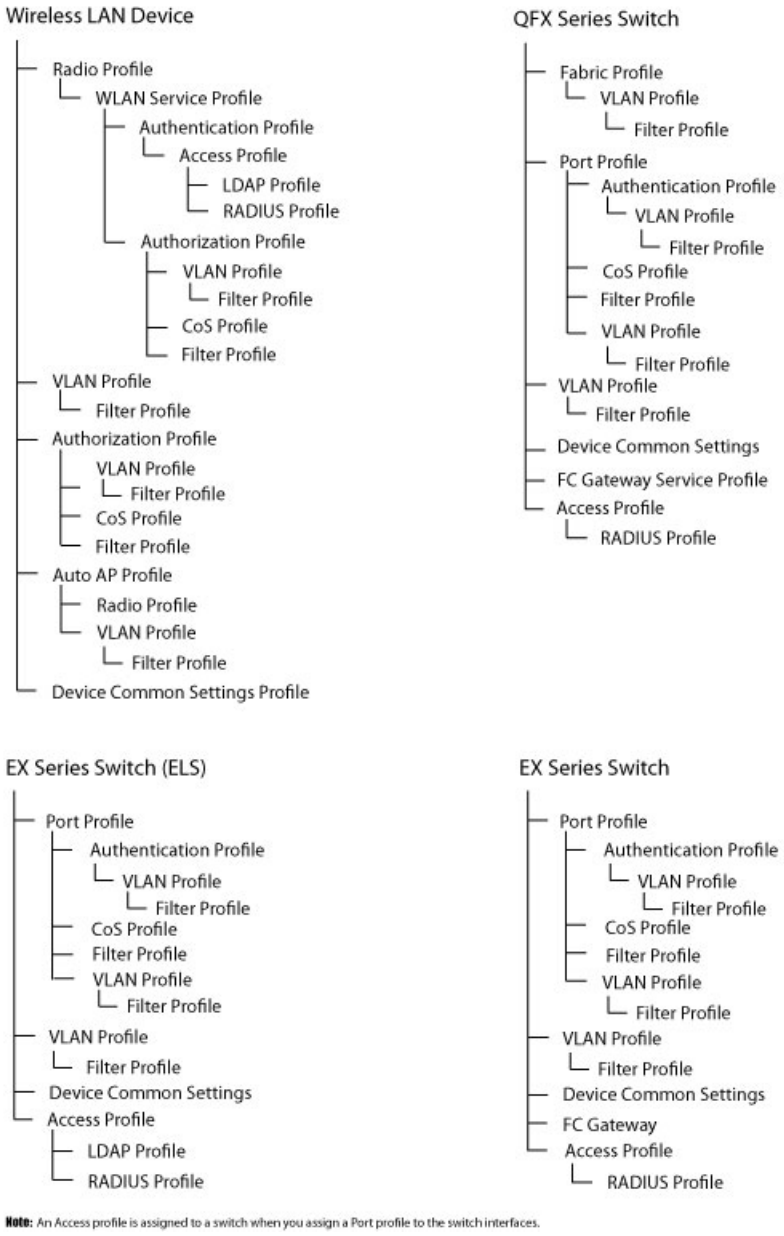
Copyright © 2013, Juniper Networks, Inc.

- By directly assigning it to a device (or to ports or radios on the device). When you assign a profile to a device, you can configure certain device-specific parameters. For example, when you assign a VLAN profile to a device, you can configure the IP address for that VLAN on that device. Or when you assign a Port profile for a Layer 3 interface to the interface, you can configure the IP address for that interface.
- By referencing the profile in another profile. Some profiles are not assigned directly to network devices—instead they are referenced from other profiles that are, in turn, assigned to network devices. For example, the settings in the CoS, Filter, and Authentication profiles are assigned indirectly to a port by the profiles being included in the Port profile.

Figure 2 on page 17 shows the relationship between profiles and devices—which profiles are contained within other profiles and which profiles can be assigned to devices.

 Copyright © 2013, Juniper Networks, Inc.

Figure 2: Profile Relationships



Note: An Access profile is assigned to a switch when you assign a Port profile to the switch interfaces.

Because a child profile might be a required setting in its parent profile, you must create the child profiles before you create the parent profiles. For example, to create a Radio profile, create the profiles in this order:

1. Access, VLAN, CoS, and Filter profiles
2. Authentication and Authorization profiles

Copyright © 2013, Juniper Networks, Inc.

3. WLAN Service profile
4. Radio profile

Network Director also includes six predefined Port profiles and one predefined CoS profile for EX Series switches. You can choose to apply the Port profiles to one or more ports of a single device or a group of devices, and the CoS profile to a Port profile or a Radio profile (using a WLAN profile and an Authorization profile).

After you have created and included the child profiles in to parent profiles, you can assign these parent profiles at various levels in your wired and wireless networks. Table 9 on page 18 shows the levels at which you can assign each of these parent profiles.

Table 9: Profile Associations at Various Levels

Name of the Profile	Wireless Network (WLC)	EX Series Ethernet Switches (With or Without ELS)	QFX Series Switches and QFabrics
Device Profile	Device	Device	Device
Radio Profile	Radio	Not applicable	Not applicable
VLAN Profile	Device, Access Point, Port	Device, Port	Device, Port
Authorization Profile	Device	Not applicable	Not applicable
Port Profile	Not applicable	Port	Port
Fabric Profile	Not applicable	Not applicable	Device, Port
Auto AP Profile	Device	Not applicable	Not applicable
FC Gateway Service	Not applicable	Not applicable	Port

Once you have assigned profiles to devices, radios, ports, or access points, you can view the profile associations in the **Profiles Assigned to the Device** page. For more information, see "Viewing Profiles Assigned to a Device" on page 480.

In addition to the profiles you create yourself, Network Director creates profiles for you from existing device configuration. Typically, you create profiles and associations manually when you are setting up a new network from scratch, adding a new device to your existing network, or when you want to make certain customized changes to the way your network is currently operating. Network Director creates profiles for you when:

- You discover existing devices in your network. As part of device discovery, Network Director examines the configurations present in the discovered device or devices. If configurations match existing profiles, Network Director assigns the matching profiles to the appropriate levels on the devices. If configurations do not match existing profiles, Network Director creates the required profiles and associates them at the appropriate levels. For more information about device discovery, see "Discovering Devices in a Physical Network" on page 455.

Copyright © 2013, Juniper Networks, Inc.

NOTE: If Network Director fails to read the configuration of one or more devices after the device discovery, such devices are not displayed in the Assign Profile page. You will not be able to assign profiles to such devices. The Manage Jobs page in System mode displays details of the device discovery jobs. Use the information displayed on this page to take appropriate corrective steps to enable Network Director to reread the configuration of the failed device. For more information, see "Troubleshooting Device Discovery Error Messages" on page 485.

- You first install Network Director and supported devices are already being managed by Junos Space. In this case, Network Director imports the device configurations into profiles the same way it does when you discover devices with Network Director.
- You resynchronize the Network Director configuration with the device configuration in order to resolve out-of-band configuration changes—that is, configuration changes that are not made with Network Director. Out-of-band configuration changes result in the device configuration not matching or being in sync with the Network Director configuration for the device. When you resynchronize the Network Director configuration with the device configuration, Network Director creates and associates new profiles if none of the existing profiles match the changed configuration. For more information about resynchronization of device configuration, see *Understanding Resynchronization of Device Configuration*.

After a profile is created, you can edit it from the Manage Profile page by selecting the profile and clicking Edit. The only exception is when the profile that you want to edit is part of a job that is scheduled for deployment. When you schedule a deployment job, that job and any profiles assigned to that job are locked. You cannot edit the job or any of its assigned profiles until the job is completed or gets cancelled. For more information, see *Understanding Deploy Mode in Network Director*.

When you delete a device in Network Director, the system deletes only the device and the profile associations. The profiles are retained in the system. If you rediscover the deleted devices into the system at a later stage, without making any configuration changes on the device, Network Director identifies this and reinstates the previous profile associations.

Related Documentation

- Understanding Access Profiles on page 21
- Understanding Authentication Profiles on page 22
- Understanding Authorization Profiles on page 24
- Understanding Auto AP Profiles on page 24
- Understanding Class of Service (CoS) Profiles on page 26
- Understanding Device Common Settings Profiles on page 30
- Understanding Fabric Profiles on page 30
- Understanding Filter Profiles on page 32
- Understanding Port Profiles on page 36

Copyright © 2013, Juniper Networks, Inc.

- Understanding Radio Profiles on page 42
- Understanding VLAN Profiles on page 49
- Understanding WLAN Service Profiles on page 52
- Creating and Managing FC Gateway Service Profiles on page 228

Copyright © 2013, Juniper Networks, Inc.

Understanding Access Profiles

Access profiles enable access configuration on the network—this consists of authentication configuration and accounting configuration. Network Director supports RADIUS, Lightweight Directory Access Protocol (LDAP), and local authentication as authentication methods, and RADIUS for accounting.

Authentication prevents unauthorized devices and users from gaining access to your network. Authentication controls access to your network using authentication methods such as 802.1X, MAC RADIUS, or captive portal. For 802.1X and MAC RADIUS authentication, end devices or users must be authenticated before they receive an IP address from a DHCP server. For captive portal authentication, the switch or the controller enables the end devices to obtain an IP address, after which these devices can forward packets such as DHCP, DNS, and ARP.

Accounting servers collect and send information used for billing, auditing, and reporting, such as:

- User identity
- Connection start and stop times
- Number of packets received and sent
- Number of transferred bytes

The accounting information is stored locally or on a remote RADIUS server. You can track sessions by using this information. As network users roam through a Network or Mobility Domain, accounting records can be used to track their network usage.

RADIUS is an authentication and accounting server used for validating users who attempt to access the wireless controller or switch. RADIUS is a distributed client-server system—the RADIUS client runs on the controller or the switch, and the server runs on a remote network system.

LDAP is an Internet protocol for accessing and updating information in an X.500-compliant directory. Network administrators for LDAP clients can connect to X.500 directory service and add, delete, modify, or search for information if they have the required access rights to the directory. LDAP is designed to run over TCP/IP and can access information in both X.500 directories and many non-X.500 directories.

NOTE: **LDAP is supported as an authentication and accounting method for Campus Switching ELS and wireless devices.**

With local authentication, you configure a password for each user allowed to log in to the controller or switch.

You can define one or more Access profiles. Each Access profile is specific to a device family. Use the Manage Access Profiles page to create, modify, view, and delete existing Access profiles.

Copyright © 2013, Juniper Networks, Inc.

Related Documentation

- Creating and Managing Access Profiles on page 136
- Creating and Managing RADIUS Profiles on page 326
- Creating and Managing LDAP Profiles on page 273

Understanding Authentication Profiles

Authentication profiles include the authentication method and authentication parameters to be used for client authentication. Available authentication methods are 802.1X (dot1x), MAC-RADIUS, captive portal, and last-resort. You can configure last-resort authentication only on wireless devices. 802.1X is the default authentication method for all device types but you can change this or add additional authentication types. If you configure multiple authentication methods on a single interface, the system tries the first method listed and then falls back to another method if the first method is unsuccessful.

You can create one or more Authentication profiles to specify different authentication methods based on client devices or sessions.

Each Authentication profile is specific to a device family. After you create an Authentication profile, you can include it in a WLAN Service profile or a Port profile. The Authentication profile specified in a WLAN profile or a Port profile is used to authenticate all the users and devices that connect to that WLAN or on the port.

- 802.1X Authentication on page 22
- MAC RADIUS Authentication on page 23
- Captive Portal Authentication on page 23
- Last Resort Authentication on page 23

802.1X Authentication

Newer equipment supports the IEE standard called 802.1X. 802.1X is basically an Enterprise, per-user (username and password) authentication mechanism – it is both the newest and strongest authentication you can use. Since 802.1X authentication is the most secure authentication option, it is preferable to the older PSK authentication, Web Portals, MAC authentication, or open authentication, which really means no authentication.

802.1X authentication involves three entities, a supplicant, an authenticator, and an authentication server. The supplicant is a client device, such as a laptop, that wishes to attach to a network. The authenticator would be either a switch or an access point. The authentication server is usually a RADIUS server, which can interpret 802.1X EAP modes.

- *Single supplicant mode* authenticates only the first end device that connects to an authenticator port. All other end devices connecting to the authenticator port after the first has connected successfully, whether they are 802.1X-enabled or not, are permitted free access to the port without further authentication. If the first authenticated end device logs out, all other end devices are locked out until an end device authenticates.

Copyright © 2013, Juniper Networks, Inc.

- *Single-secure supplicant mode* authenticates only one end device to connect to an authenticator port. No other end device can connect to the authenticator port until the first logs out.
- *Multiple supplicant mode* authenticates multiple end devices individually on one authenticator port. If you configure a maximum number of devices that can be connected to a port through port security, the lesser of the configured values is used to determine the maximum number of end devices allowed per port.

MAC RADIUS Authentication

A media access control address (MAC address) is a unique identifier assigned to network interfaces for communications on the physical network segment. MAC addresses are used as a network address for most IEEE 802 network technologies, including Ethernet. A client's MAC address can be used for authentication by mapping a password to the client's entry in the MAC address table. MAC authentication can be done either locally or with a RADIUS server.

Captive Portal Authentication

Captive Portals are frequently used to authenticate hotspots, forcing all users to use the configured logon web page. Many companies use captive portals to authenticate guest users for temporary use of the company network. The Captive Portal has one password for all users, which should be changed frequently.

Last Resort Authentication

You can configure last-resort authentication only on wireless devices.

Related Documentation

- Creating and Managing Authentication Profiles on page 157

Copyright © 2013, Juniper Networks, Inc.

Understanding Authorization Profiles

Once the user is authenticated, Network Director looks for the authorization attributes assigned to the user. Authorization profiles specify the access permissions and authorization attributes for authenticated users or devices. Authorization attributes specify the network resources available to the user. The VLAN profile is a mandatory attribute in order to place the user in the appropriate VLAN. You can provide further access controls using an Authorization profile by specifying encryption types, linking a class-of-service (CoS) profile, specifying the days and times during which the user can access the network, and so on.

You can create Authorization profiles only for wireless devices. After you create a Authorization profile, you can link it to a WLAN profile or assign it to a controller or a cluster. Once you assign an Authorization profile to a controller or a cluster, the VLAN, CoS, and Filter settings that you have defined within that profile are applied on the WLC or the cluster. These settings can then be used for dynamic users who are authenticated through RADIUS or LDAP servers.

Related Documentation

- Creating and Managing Wireless Authorization Profiles on page 167

Understanding Auto AP Profiles

If you set up an Auto AP profile for a wireless controller, discovered distributed access points that are not specifically configured on that controller use a temporary configuration from the Auto AP profile. When you set up an Auto AP profile for these distributed access points, you provide only the basic information that an access point needs to operate. Auto AP access points do not include all the information that individually configured access points do. In addition, these Auto AP access point configurations are not persistent on the controller—they go away when the access points are not present.

NOTE: **A controller can have only one Auto AP profile.**

This topic describes:

- How Are Specifically Configured Access Points Different From Access Points Configured With Auto AP? on page 24
- How Should I Use Auto AP Profiles? on page 25
- How Does Auto AP Work? on page 25

How Are Specifically Configured Access Points Different From Access Points Configured With Auto AP?

Controllers give preference to specifically configured, persistent access points over those access points using an Auto AP profile. If a configured access point is discovered by a fully utilized controller, the controller disconnects an access point using an Auto AP profile and accepts connection from the configured access point instead.

Copyright © 2013, Juniper Networks, Inc.

In this case, the disconnected access point begins the boot process again to find another controller with an Auto AP profile. When the access point is disconnected, the access point clients experience a service disruption, and attempt to associate with another available access point to reconnect to the SSID. If another access point is not available to a client, the client can still reconnect after the disconnected access point locates a new controller and finishes the boot and configuration process.

How Should I Use Auto AP Profiles?

The Auto AP feature is useful when you need to add multiple access points all at once. Typical use of the Auto AP profile would be to:

- Configure an Auto AP profile, assign the profile to a controller, and then deploy the controller configuration. To configure an Auto AP profile, see "Creating and Managing Wireless Auto AP Profiles" on page 174. To assign an Auto AP profile to a controller, see "Assigning an Auto AP Profile to Controllers" on page 371. To deploy the controller configuration, see *Deploying Configuration to Devices*.
- Convert access points found by Auto AP on that controller to persistently configured access points following the directions *Converting Automatically Discovered Access Points to Manually Configured Access Points With Network Director*.
- Turn off the Auto AP profile by editing the profile—see "Creating and Managing Wireless Auto AP Profiles" on page 174.

How Does Auto AP Work?

When an Auto AP profile is assigned to a controller, the controller assigns a valid number and a name to unassigned, distributed access points. The controller also configures the access point settings and radio parameter settings supplied in the Auto AP profile.

NOTE: **The Auto AP profile does not configure SSIDs, encryption parameters, or any other parameters managed by the WLAN Service profile. You still need to configure a WLAN Service profile for each SSID.**

Related Documentation

- Creating and Managing Wireless Auto AP Profiles on page 174
- Assigning an Auto AP Profile to Controllers on page 371
- *Deploying Configuration to Devices*
- *Converting Automatically Discovered Access Points to Manually Configured Access Points With Network Director*

Copyright © 2013, Juniper Networks, Inc.

Understanding Class of Service (CoS) Profiles

When a network experiences congestion and delay, some packets must be prioritized to avoid random loss of data. Class of service (CoS) accomplishes this prioritization by dividing similar types of traffic, such as email, streaming video, voice, large document file transfer, into classes. You then apply different levels of priority, such as throughput and packet loss, to each group. When packets must be dropped, packet loss takes place according to your configured rules. CoS also enables you to rewrite the Differentiated Service Code Point (DSCP), IP precedence, or 802.1p CoS bits of packets egressing out of a specific interface, thus allowing you to tailor outgoing packets for the remote peers' network requirements.

On data center switching devices, CoS can be used to configure Ethernet interfaces to support Fibre Channel over Ethernet (FCoE) traffic.

- How Would I Use CoS? on page 26
- How Does CoS Work? on page 27
- What Wireless Network Traffic Aspects Can I Control With CoS? on page 28
- What CoS Parameters Can I Control? on page 28
- What Are the Default CoS Traffic Types? on page 29
- Data Center Switching CoS Configuration on page 30
- How Do I Implement Class of Service? on page 30

How Would I Use CoS?

On an Ethernet trunk, you can mark frames with a class of service (CoS) value. CoS is used to define trunk connections as full-duplex, incoming only, or outgoing only.

Network devices such as routers and switches can be configured to use existing CoS values on incoming packets from other devices (trust mode), or can rewrite the CoS value to something completely different. Layer 2 markings also can extend to the WAN, for example with a frame relay network. CoS is usually limited to use within an organization's intranet.

With legacy telephone systems, CoS can be used to define the permissions an extension will have on a PBX or Centrex. Some users might need extended voicemail message retention or the ability to forward calls to a cell phone, while others have no need to make calls outside the office. Permissions for a group of extensions can be changed by modifying a CoS variable applied to the entire group.

NOTE: **CoS configurations can be quite complicated, so unless it is required by your scenario, we recommend that you not alter the default class names or queue number associations.**

Copyright © 2013, Juniper Networks, Inc.

How Do I Create CoS Groups?

Use 802.1Q tagged VLANs to group users and enable CoS to set priorities supported by downstream devices.

How is CoS Different Than QoS?

CoS operates only on 802.1Q VLAN Ethernet at the data link layer (layer 2), while quality-of-service (QoS) mechanisms operate at the IP network layer (layer 3). 802.1p Layer 2 tagging can be used by QoS to differentiate and shape network traffic.

How Does CoS Work?

CoS is a 3-bit field in an Ethernet frame header when 802.1Q VLAN tagging has been applied. The 3-bit field specifies a priority value between 0 and 7 that can be used by QoS to differentiate and shape network traffic. CoS tags 0 through 3 are normal priority, and tags 4 through 7 are high priority.

It is helpful to think of forwarding classes as output queues. In effect, the end result of classification is the identification of an output queue for a particular packet. For a classifier to assign an output queue to each packet, it must associate the packet with one of the forwarding classes listed in Table 10 on page 27.

Table 10: 3-Bit CoS Field in Ethernet Header With VLAN Tagging

CoS Value	Priority Applied
0	Best-effort is a backward compatibility feature.
1	Assured-forwarding offers a high-level of assurance that the packets are delivered as long as the packet flow from the client stays within a certain Service profile that you define.
2	Multicast assured-forwarding offers a high level of assurance that the multicast packets are delivered as long as the packet flow from the customer stays within a certain service profile that you define. The software accepts excess traffic, but it applies a tail drop profile to determine if the excess packets are dropped and not forwarded. Up to two drop probabilities (low and high) are defined for this service class. Multicast expedited-forwarding delivers assured bandwidth, low loss, low delay, and low delay variation (jitter) end-to-end for multicast packets in this service class. The software accepts excess traffic in this class, but in contrast to the multicast assured forwarding class, out-of-profile multicast expedited-forwarding class packets can be forwarded out of sequence or dropped. Multicast best-effort does not apply any special CoS handling to the multicast packets. These packets are usually dropped under congested network conditions.
3	
4	
5	Expedited-forwarding delivers assured bandwidth, low loss, low delay, and low delay variation (jitter) end-to-end for packets in this service class.
6	

Copyright © 2013, Juniper Networks, Inc.

Table 10: 3-Bit CoS Field in Ethernet Header With VLAN Tagging *(continued)*

CoS Value	Priority Applied
7	Network-connect

Note: The forwarding classes multicast expedited-forwarding, multicast assured-forwarding, and multicast best-effort are applicable only to Juniper Networks EX8200 Ethernet Switches and Juniper Networks EX9200 Ethernet Switches.

Differentiated Services indicate how a packet is forwarded. Because the three bits used in Layer 2 simple priority tagging provide minimal direction in managing traffic, the protocol Differentiated Services (DS or DiffServ) was developed to enhance traffic differentiation.

What Wireless Network Traffic Aspects Can I Control With CoS?

In addition to separating traffic into classes, you can also optionally configure these settings with CoS:

- Apply a bandwidth limit to the data sessions and to aggregated categories such as trunk interfaces, Layer 3 interfaces, access interfaces, and routed VLAN interfaces.
- Assign the same CoS level to all traffic on the Service profile SSID. This is called static CoS and overrides settings indicated on the 802.1p, overrides DSCP markings in the packets themselves, and disregards any filters that mark CoS. You indicate the value assigned to all user traffic.
- Allow the controller to use the client DSCP for radio ingress traffic and ignore Wi-Fi Multimedia (WMM).
- Specify a traffic class for voice traffic and optionally apply a bandwidth limit to the voice sessions and to aggregated categories. You can also enable static CoS for voice traffic, which overrides settings indicated on the 802.1p, overrides DSCP markings in the packets themselves, and disregards any filters that mark CoS. You indicate the value assigned to all voice traffic.
- Specify which of 11 forwarding queues are used. You can modify the action corresponding to each forwarding queue to suit your requirements. This is referred to as access categories.

What CoS Parameters Can I Control?

You can use CoS profiles to group a set of class-of-service (CoS) parameters and apply it to one or more interfaces. You can configure the following parameters within a CoS profile:

- Classifiers—Packet classification refers to the examination of an incoming packet. This function associates the packet with a particular CoS servicing level.
- Scheduler maps—Schedulers define the properties of output queues. These properties include the amount of interface bandwidth assigned to the queue, the size of the memory buffer allocated for storing packets, the priority of the queue, and the drop profiles associated with the queue. You associate the schedulers with forwarding

Copyright © 2013, Juniper Networks, Inc.

classes by means of scheduler maps. You can then associate each scheduler map with an interface, thereby configuring the queues, packet schedulers, and tail drop processes that operate according to this mapping.

- Rewrite values—A rewrite rule modifies the appropriate CoS bits in an outgoing packet. Modification of CoS bits enables the next downstream device to classify the packet into the appropriate service group. Rewriting or marking outbound packets is useful when the device is at the border of a network and must alter the CoS values to meet the policies of the targeted peer.
- Traffic-control profile—Traffic-control profiles enable traffic limitation of a certain class to a specified bandwidth and burst size. Packets exceeding the limits can be discarded, or can be assigned to a different forwarding class, a different loss priority, or both.

What Are the Default CoS Traffic Types?

On EX Series switches, the system provides you with these four predefined traffic types—Data, Voice, Video, and Network Control—with these default traffic configuration and shaping details:

- Data—Forwarding queue 0 (nd_best-effort), Buffer size 50%, Bandwidth reserved 30%
- Voice—Forwarding queue 5 (nd_expedited-forwarding), Buffer size 20%, Bandwidth reserved 0%
- Video—Forwarding queue 4 (nd_video-forwarding), Buffer size 20%, Bandwidth reserved 70%
- Network Control—Forwarding queue 7 (nd_network-control), Buffer size 10%, Bandwidth reserved 0%

For Campus Switching ELS, the system provides you with these four predefined traffic types—Data, Voice, Video, and Network Control—with these default traffic configuration and shaping details:

- Data—Forwarding queue 0 (nd_best-effort), Buffer size 50%, Bandwidth reserved 30%
- Voice—Forwarding queue 1 (nd_expedited-forwarding), Buffer size 20%, Bandwidth reserved 0%
- Video—Forwarding queue 2 (nd_video-forwarding), Buffer size 20%, Bandwidth reserved 70%
- Network Control—Forwarding queue 3 (nd_network-control), Buffer size 10%, Bandwidth reserved 0%

You can modify and customize each of these traffic types. If you want to add more traffic types you can do so—see "Creating and Managing CoS Profiles" on page 184.

On data center switches, the system provides you with predefined traffic types nd_dc_best-effort, nd_dc_network-control, nd_dc_fcoe, nd_dc_no-loss, and nd_dc_mcast.

Copyright © 2013, Juniper Networks, Inc.

Data Center Switching CoS Configuration

For data center switching devices, these additional CoS features are available:

- Hierarchical Port Scheduling (ETS)—Hierarchical port scheduling (Enhanced Transmission Selection, or ETS) is a two-tier process that provides better port bandwidth utilization and greater flexibility to allocate resources to queues and to groups of queues.
- Priority-based flow control (PFC)—A link-level flow control mechanism.

How Do I Implement Class of Service?

CoS can be implemented from the MSS CLI, from Network Director. RingMaster configures unicast traffic but does not configure multicast traffic. For directions to implement CoS from Network Director, see "Creating and Managing CoS Profiles" on page 184.

Related Documentation

- Creating and Managing CoS Profiles on page 184

Understanding Device Common Settings Profiles

Network Director enables you to configure device-level settings for switches and wireless LAN controllers in the Device Common Settings profile. Once you create the profiles, you can assign the profiles to a switch or a controller and you can deploy the profiles using the Deploy mode tasks.

Network Director also creates Device Common Settings profiles when it discovers devices. It creates a Device Common Settings profile for each device it discovers, importing the device-level settings from the device into the profile.

While configuring the profiles, you can specify the basic settings, which includes the profile name, device user list, and time settings. Apart from the basic settings, you can optionally specify the management and protocol settings too.

Related Documentation

- Creating and Managing Device Common Settings on page 198
- Assigning Device Common Settings to Devices on page 375
- Understanding Profiles on page 15

Understanding Fabric Profiles

A Fabric profile contains configuration settings for a gateway Fibre Channel (FC) fabric. You assign Fabric profiles to QFX Series devices that act as a FCoE-FC gateway, to configure gateway FC fabrics.

A gateway FC fabric is a QFX Series configuration construct. It is not the same thing as an FC fabric in the storage area network (SAN); the gateway FC fabric is local to the switch. It creates associations that connect FCoE devices with converged network

Copyright © 2013, Juniper Networks, Inc.

adapters (CNAs) on the Ethernet network to an FC switch on the Fibre Channel network. A gateway FC fabric consists of:

- A unique fabric name.
- A unique fabric ID.
- At least one dedicated VLAN for FCoE traffic. VLANs that carry FCoE traffic must not carry any other type of traffic.

  NOTE: On a QFX3500 or QFabric system Node device, the same VLAN cannot be used in both transit switch mode and FCoE-FC gateway mode.

- At least one FCoE VLAN interface (Layer 3 VLAN interface) that includes one or more 10-Gigabit Ethernet interfaces connected to FCoE devices. The FCoE VLANs transport traffic between the FCoE servers and the FCoE-FC gateway. Each FCoE VLAN must carry only FCoE traffic. You cannot mix FCoE traffic and standard Ethernet traffic on the same VLAN.

  The 10-Gigabit Ethernet interfaces that connect to FCoE devices must include a native VLAN to transport FIP traffic because FIP VLAN discovery and notification frames are exchanged as untagged packets.

  Each FCoE VLAN interface can present multiple VF_Port interfaces to the FCoE network.

  NOTE: Storm control must be disabled on all Ethernet interfaces that belong to the FCoE VLAN to prevent FCoE traffic from being dropped.

- One or more native FC interfaces. The native FC interfaces transport traffic between the gateway and the FC switch.

  TIP: If the network does not use a dual-rail architecture for redundancy, configure more than one native FC interface for each FC fabric to create redundant connections between the FCoE devices and the FC switch. If one physical link goes down, any sessions it carried can log in again and connect to the FC switch on a different interface. Even in dual-rail architecture networks, creating redundant connections between the QFabric system and the FC switch is the best practice.

You can configure FIP parameters for the fabric or accept the default FIP parameters. VN_Port to VF_Port (VN2VF_Port) FIP snooping is automatically enabled on all server-facing ports because all ports are untrusted by default. You can disable VN2VF_Port FIP snooping on a port-by-port basis by marking a port as an FCoE trusted interface. You can disable VN2VF_Port FIP snooping on all Ethernet ports in an FC fabric by configuring the fabric as FCoE trusted.

Because the switch has 12 native FC ports and each FC fabric requires a minimum of one native FC port, the switch supports a maximum of 12 FC fabrics. However, as a best

Copyright © 2013, Juniper Networks, Inc.

practice for redundancy, we recommend that you assign at least two native FC interfaces to each FC fabric.

On a QFabric system, all of the FC and FCoE traffic that belongs to a particular gateway FC fabric must ingress and egress the same gateway Node device. Gateway FC fabrics do not span across Node devices. All of the native FC interfaces and the Ethernet interfaces that belong to the FCoE VLAN must reside on the same gateway Node device to be included in an FC fabric on that Node device.

Traffic from FC and FCoE devices that are not in the same FC fabric remain separate and cannot communicate with each other through the gateway.

Related Documentation

- Creating and Managing Fabric Profiles on page 223

Understanding Filter Profiles

Filter profiles are a set of rules that define whether to accept or discard packets that are transiting on an interface on a Juniper Networks EX Series Ethernet Switch or on a radio connected to a Wireless LAN Controller. You configure Filter profiles to determine whether to accept or decline traffic before it enters or exits a port or a radio to which the Filter profile is applied to.

A Filter profile must contain at least one term. Each term consists of the following components:

- Match conditions—Specify the values or fields that the packet must contain. You can define various match conditions, depending on the device for which you are defining these conditions. For example, for EX Series switches, you can specify a match condition based on the IP source address field, IP destination address field, Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) source port field, IP protocol field, Internet Control Message Protocol (ICMP) packet type, TCP flags, interfaces, and so on. For a wireless device, the match conditions can be based on the source and destination IP or MAC address, and EtherTypes.
- Action—Specifies what to do if a packet matches the match conditions. Possible actions are to accept or discard the packet or to send the packet to a specific virtual routing interface. In addition, packets can be counted to collect statistical information. If no action is specified for a term, the default action is to accept the packet.
- Action modifier—Specifies one or more actions for the switch if a packet matches the match conditions. You can specify action modifiers such as the loss priority, policer details, and forwarding class, depending on the type of device on which you are creating the Filter profile.

The maximum number of terms allowed per Filter profile for EX Series switches is:

- 512 for EX2200 switches
- 1,436 for EX3300 switches

Copyright © 2013, Juniper Networks, Inc.

NOTE: On EX3300 switches, if you add and delete filters with a large number of terms (on the order of 1000 or more) in the same commit operation, not all the filters are installed. You must add filters in one commit operation, and delete filters in a separate commit operation.

- 7,042 for EX3200 and EX4200 switches—as allocated by the dynamic allocation of ternary content addressable memory (TCAM) for firewall filters.
- 1,200 for EX4500 and EX4550 switches
- 1,400 for EX6200 switches
- 32,768 for EX8200 switches

NOTE: The on-demand dynamic allocation of the shared space TCAM in EX8200 switches is achieved by assigning free space blocks to firewall filters. Firewall filters are categorized into two different pools. Port and VLAN filters are pooled together (the memory threshold for this pool is 22K) while router firewall filters are pooled separately (the threshold for this pool is 32K). The assignment happens based on the filter pool type. You can share free space blocks only among the firewall filters belonging to the same filter pool type. An error message is generated if you attempt to configure a firewall filter beyond the TCAM threshold.

The Manage Filter Profiles page enables you create, modify, view, and delete Filter profiles.

Related Documentation

- Creating and Managing Filter Profiles on page 231

Understanding How To Add Access Points to a Wireless Network With Network Director

There are two ways to add an access point to your wireless network. Both methods have advantages and disadvantages as shown in Table 11 on page 33.

Table 11: Adding Access Points to a Wireless Network With Network Director

Method	What You Do	Pros and Cons
The controller discovers access points and provides the list to Network Director. You can convert any or all of these temporary configurations to persistent configurations.	Enable automatic access point discovery on a controller by following the directions "Creating and Managing Wireless Auto AP Profiles" on page 174. Convert the automatically discovered access points to persistent configurations by following the directions *Converting Automatically Discovered Access Points to Manually Configured Access Points With Network Director*. (For an explanation of auto AP profiles, see "Understanding Auto AP Profiles" on page 24.)	All access points in range are automatically discovered and listed first as access points on the controller and then as devices in Network Director. This method is very efficient. The drawback to this method is that non-company access points can be discovered and added if they are in range. You can overcome this drawback by converting the access points that belong to your network.

Copyright © 2013, Juniper Networks, Inc.

Table 11: Adding Access Points to a Wireless Network With Network Director *(continued)*

Method	What You Do	Pros and Cons
You add an access point one at a time.	See "Adding and Managing an Access Point" on page 126 for directions for this method of adding access points.	Adding one access point at a time can be tedious if you need to add a large number of access points. However, adding one access point at a time from Network Director is more explicit because that method inputs more information and does more configuration. Controllers give preference to specifically configured, persistent access points over those access points using an Auto AP profile. If a configured access point is discovered by a fully utilized controller, the controller disconnects an access point using an Auto AP profile and accepts connection from the configured access point instead.

Related Documentation

- Adding and Managing an Access Point on page 126
- Creating and Managing Wireless Auto AP Profiles on page 174
- *Converting Automatically Discovered Access Points to Manually Configured Access Points With Network Director*.
- Understanding Auto AP Profiles on page 24

Understanding Link Aggregation

You can combine multiple physical Ethernet ports to form a logical point-to-point link, known as a link aggregation group (LAG) or bundle. A LAG provides more bandwidth than a single Ethernet link can provide. Additionally, link aggregation provides network redundancy by load-balancing traffic across all available links. If one of the links fails, the system automatically load-balances traffic across all remaining links. In a Virtual Chassis, LAGs can be used to load-balance network traffic between member switches.

The maximum number of interfaces that can be grouped into a LAG and the maximum number of LAGs supported on a Juniper Networks EX Series Ethernet Switch varies according to the switch model and the version of and the version of Juniper Networks Junos operating system (Junos OS) that is running on that switch. Table 12 on page 34 lists the maximum number of interfaces per LAG and the maximum number of LAGs that are supported on EX Series switches running Junos OS Release 12.3. If your switch is running a different version of Junos OS, refer to the device specific documentation, EX Series Ethernet Switches, before implementing LAG in your network.

Table 12: Maximum Interfaces per LAG and Maximum LAGs per Switch

Switch	Maximum Interfaces per LAG	Maximum LAGs
EX2200	8	32
EX3200	8	32

Copyright © 2013, Juniper Networks, Inc.

Table 12: Maximum Interfaces per LAG and Maximum LAGs per Switch *(continued)*

Switch	Maximum Interfaces per LAG	Maximum LAGs
EX3300 (Standalone and Virtual Chassis)	8	111
EX4200 (Standalone and Virtual Chassis)	8	111
EX4500 and EX4550 (Standalone and Virtual Chassis)	8	111
EX6200	8	111
EX8200	12	255
EX8200 Virtual Chassis	12	239

Related Documentation

- Managing and Creating a Link Aggregation Group on page 278

Understanding Multichassis Link Aggregation

Layer 2 networks are increasing in scale mainly because of technologies such as virtualization. Protocol and control mechanisms that limit the disastrous effects of a topology loop in the network are necessary. Spanning Tree Protocol (STP) is the primary solution to this problem because it provides a loop-free Layer 2 environment. STP has gone through a number of enhancements and extensions, and although it scales to very large network environments, it still provides only one active path from one device to another, regardless of the number of actual connections existing in the network. Although STP is a robust and scalable solution to redundancy in a Layer 2 network, the single logical link creates two problems: At least half of the available system bandwidth is off-limits to data traffic, and network topology changes occur. The Rapid Spanning Tree Protocol (RSTP) reduces the overhead of the rediscovery process and allows a Layer 2 network to reconverge faster, but the delay is still high.

Link aggregation (IEEE 802.3ad) solves some of these problems by enabling users to use more than one link connection between switches. All physical connections are considered one logical connection. The problem with standard link aggregation is that the connections are point to point.

Multichassis link aggregation groups (MC-LAGs) enable a client device to form a logical LAG interface between two MC-LAG peers (QFX3500 and QFX3600 devices). An MC-LAG provides redundancy and load balancing between the two MC-LAG peers, multihoming support, and a loop-free Layer 2 network without running STP.

Copyright © 2013, Juniper Networks, Inc.

On one end of an MC-LAG, there is an MC-LAG client device, such as a server, that has one or more physical links in a link aggregation group (LAG). This client device does not need to have an MC-LAG configured. On the other side of the MC-LAG, there are two MC-LAG peers. Each of the MC-LAG peers has one or more physical links connected to a single client device.

The MC-LAG peers use Interchassis Control Protocol (ICCP) to exchange control information and coordinate with each other to ensure that data traffic is forwarded properly.

Link Aggregation Control Protocol (LACP) is a subcomponent of the IEEE 802.3ad standard. LACP is used to discover multiple links from a client device connected to an MC-LAG peer. LACP must be configured on all member links for an MC-LAG to work correctly.

Related Documentation

- Creating and Managing Multichassis Link Aggregation Groups (MC-LAGs) on page 468

Understanding Port Profiles

Port profiles provide a convenient way of provisioning interfaces on switches. You can either use predefined port profiles, or you can define your own custom port profile.

After you create a Port profile, you can assign it to interfaces on one or more switches, including aggregated interfaces. For the configuration created by the profile to take effect on the devices, you must use Deploy mode to deploy the configuration on the devices.

This topic describes:

- Interface Settings Configured in the Port Profile on page 36
- Interface Settings Configured by Referencing Other Profiles on page 37
- Data Center Device Port Profile Settings on page 37
- Default Port Profiles on page 38

Interface Settings Configured in the Port Profile

You can configure the following interfaces settings in a Port profile:

- Interface protocol family—You can configure an interface to be either an Ethernet switching interface, an IPv4 routing interface, or an IPv6 routing interface.
- Port mode—You can configure a switching interface port mode to be an access, trunk, or tagged-access interface for EX Series switches. Campus Switching ELS supports access mode and trunk mode. For more information about port modes, see *Ethernet Switching*.
- PoE settings—The factory default configuration of switches enables PoE on all interfaces that support PoE. For many implementations, no further configuration is necessary. You can, however, override the default settings for PoE interfaces in the Port profile. Most switch models have interfaces that support Power over Ethernet

Copyright © 2013, Juniper Networks, Inc.

(PoE), but the EX9200 does not support PoE. For more information about PoE, see *Power over Ethernet (PoE)*.

If you do not explicitly configure PoE in the Port profile, the existing PoE interface settings on the switch remain in effect. Device-wide PoE settings are configured in the Device Common Settings profile.

NOTE: **PoE settings are not available for Data Center devices.**

- Physical link settings—On switches, the autonegotiation of port speed and duplex mode is enabled by default. You can disable autonegotiation and set port speed and duplex mode in the Port profile. Other link settings you can configure include flow control, which is disabled by default, and maximum transmission unit (MTU).
- Port security settings—You can optionally enable port security on switched access ports. Port security features help protect the access ports on your switch against address spoofing (forging) and Layer 2 denial-of-service (DoS) attacks. For more information about port security on switches, see *Port Security*.

Interface Settings Configured by Referencing Other Profiles

You can optionally configure other interface-related settings in the Port profile by referencing other profiles. These profiles are:

- CoS profile—Configures class-of-service settings on the interface.
- Filter profile—Configures firewall filters (often called ACLs) on the interface.
- Authentication profile—(Switching interfaces only) Enables 802.1X authentication on an interface and configures related settings, such as captive portal authentication.
- Access profile—Configures the access server settings used by all 802.1X authenticator interfaces on a switch. This profile is not included in the Port profile. Instead, you assign it to a device as part of the process of assigning a Port profile to the interfaces on the device.
- VLAN profile for Campus Switching ELS is mandatory.

If you want to use one or more of these profiles with the Port profile, be sure to create them before you create and assign the Port profile.

Data Center Device Port Profile Settings

Port profiles for data center switching devices include settings for the following features:

- Configuring Fibre Channel (FC) ports.
- Configuring Data Center Bridging Capability Exchange (DCBX) protocol for Ethernet interfaces.

Copyright © 2013, Juniper Networks, Inc.

Default Port Profiles

To help with the rapid provisioning of interfaces on switches, Network Director provides default Port profiles that contain settings for common uses of switch interfaces. You can modify or assign these default profiles to interfaces using the same method used for user-created profiles. Table 13 on page 38 describes the default Port profiles.

Table 13: Default Port Profiles

Profile Name	Description	Summary of Settings
Desktop_Port	Configures an untagged port that connects to desktop computer.	• Family Type—switching • Port Mode—access • Auto Negotiation—enabled • Flow Control—enabled • Maximum Bytes—no default provided • Speed—no default provided • Link Mode—no default provided • Trust DHCP—no • MAC Limit—1 • MAC Limit Action—drop • CoS Profile—no default provided
Desktop_ Phone_Port	Configures an untagged port that connects to a combined desktop and phone port.	• Family Type—switching • Port Mode—access • Auto Negotiation—enabled • Flow Control—enabled • Maximum Bytes—no default provided • Speed—no default provided • Link Mode—no default provided • Trust DHCP—no • MAC Limit—2 • MAC Limit Action—drop • CoS Profile—juniper_CoS_template

Copyright © 2013, Juniper Networks, Inc.

Table 13: Default Port Profiles *(continued)*

Profile Name	Description	Summary of Settings
FCoE Gateway	Configures an Ethernet port for an FCoE gateway. Available for data center switching profiles only.	• Port Type—Ethernet Port • CoS Profile—juniper_DC_Hier_CoS • Family Type—switching • Port Mode—trunk • Filters—no default provided • VLAN Options—no default provided • DCBX Version—Auto • Disable DCBX—disabled • Disable Priority Flow Control—disabled • ETS No Auto Negotiation—disabled • Recommendation TVL—no default provided • Auto Negotiation—enabled • Flow Control—disabled • Maximum Size—2500 • Speed—no default provided • Link Mode—no default provided
Fibre Channel Port	Configures a Fibre Channel (FC) port. Available for data center switching profiles only.	• Port Type—Fibre Channel Port • Speed—4Gbps • Buffer to Buffer State Change Number—no default provided • Loopback Setting—no default provided
FCoE Transit Port	Configures an Ethernet port for an FCoE transit switch. Available for data center switching profiles only.	• Port Type—Ethernet Port • CoS Profile—juniper_DC_Hier_CoS • Family Type—switching • Port Mode—trunk • Filters—no default provided • VLAN Options—no default provided • DCBX Version—Auto • Disable DCBX—disabled • Disable Priority Flow Control—disabled • ETS No Auto Negotiation—disabled • Recommendation TVL—no default provided • Auto Negotiation—enabled • Flow Control—disabled • Maximum Size—2500 • Speed—no default provided • Link Mode—no default provided • Port Security—enabled • Trust DHCP—disabled • FCoE Trusted—enabled • MAC Limit—no default provided • MAC Limit Action—no default provided • Allowed MAC List—no default provided

Copyright © 2013, Juniper Networks, Inc.

Table 13: Default Port Profiles *(continued)*

Profile Name	Description	Summary of Settings
Server_Port	Configures a tagged port that connects to a server.	• References the default CoS profile, juniper_CoS_template • Sets protocol family to Ethernet switching • Sets port mode to trunk • Enables port security with trust DHCP enabled
Switched_Downlink	Configures a tagged port that connects to endpoint devices in a branch environment or servers in a data center environment.	• Family Type—switching • Port Mode—trunk • Auto Negotiation—enabled • Flow Control—enabled • Maximum Bytes—no default provided • Speed—no default provided • Link Mode—no default provided • Trust DHCP—yes • MAC Limit—no default provided • MAC Limit Action—no default provided • CoS Profile—juniper_CoS_template
Switched_Uplink	Configures a tagged port that connects a switch to another switch or larger network. For example, a port that connects an access switch to an aggregation switch.	• Family Type—switching • Port Mode—trunk • Auto Negotiation—enabled • Flow Control—enabled • Maximum Bytes—no default provided • Speed—no default provided • Link Mode—no default provided • Trust DHCP—yes • MAC Limit—no default provided • MAC Limit Action—no default provided • CoS Profile—juniper_CoS_template
Wireless_ Access_Port	Configures an untagged port that connects to a wireless access point.	• Family Type—switching • Port Mode—access • Auto Negotiation—enabled • Flow Control—enabled • Maximum Bytes—no default provided • Speed—no default provided • Link Mode—no default provided • Trust DHCP—no default provided • MAC Limit—no default provided • MAC Limit Action—no default provided • CoS Profile—no default provided

Related Documentation

- Creating and Managing Port Profiles on page 283
- Understanding Access Profiles on page 21

Copyright © 2013, Juniper Networks, Inc.

- Understanding Authentication Profiles on page 22
- Understanding Class of Service (CoS) Profiles on page 26
- Understanding Filter Profiles on page 32

Understanding QFabric Setup

The QFabric Setup task allows you to set up these components of a QFabric system:

- Node aliases—Aliases replace the hardware serial numbers of components, making it easier to identify system devices and simplify configuration tasks.
- Node groups—Node groups help you combine multiple Node devices into a single virtual entity within the QFabric system to enable redundancy and scalability at the edge of the data center. There are three types of Node groups in a QFabric system:
  - Automatically generated server Node groups—By default, every Node device that joins the QFabric system is placed within an automatically generated server Node group that contains one Node device (the device itself). Server Node groups connect to servers and storage devices.
  - Network Node groups—You can assign up to eight Node devices to a network Node group. When grouped together, the Node devices within a network Node group connect to other routers running routing protocols such as OSPF and BGP.
  - Redundant server Node groups—You can assign two Node devices to a redundant server Node group. When grouped together, you can create link aggregation groups (LAGs) that span the interfaces on both Node devices to provide resiliency and redundancy.
- Control plane network—The control plane network is an out-of-band Gigabit Ethernet management network that connects all QFabric system components. The EX Series switches and Virtual Chassis that comprise this network are called Control Plane Ethernet (CPE) switches. The control plane network connects the Director group to the management ports of the Node and Interconnect devices.

  In Network Director, you discover the control plane switches or Virtual Chassis as separate devices. Then you use QFabric setup to map the discovered switches or Virtual Chassis to the QFabric to which they are acting as CPE switches.

Related Documentation

- Setting Up QFabrics on page 472

Copyright © 2013, Juniper Networks, Inc.

Understanding Radio Profiles

Radio profiles contain configuration information for radios. A single Radio profile can be applied to many radios that share a common configuration. This topic describes Radio profile configuration concepts. To create, assign, or delete a Radio profile, see "Creating and Managing a Radio Profile" on page 315.

This topic describes:

- RF Scanning on page 42
- Spectral Scanning on page 42
- Dynamic Frequency Selection (DFS) Channels on page 43
- RFID Asset Tracking on page 43
- WMM Power Save on page 44
- Countermeasures on page 44
- Limiting Client Power on page 44
- 802.11n Channel Width on page 44
- Automatic Channel Tuning on page 44
- Automatic Power Tuning on page 45
- IEEE 802.11 on page 45
- Long and Short Preamble Length on page 45

RF Scanning

All wireless radios continually scan for other RF transmitters. While 802.11b/g radios scan in the 2.4-GHz to 2.4835-GHz spectrum, 802.11a radios scan in the 5.15-GHz to 5.85-GHz spectrum. There are two scanning methods, passive scanning and active scanning. By default, radios perform both types of scans on all channels allowed by the country of operation. (The country of operation is the regulatory domain set during initial access point deployment.)

While both types of scanning are on by default, active scanning is done only on channels on which local government regulations allow it to transmit. Channels that are not authorized for unlicensed use and channels that require radar detection with dynamic frequency selection (DFS) are excluded from active scanning.

For more information, about scanning see "Understanding Wireless Scanning" on page 117.

Spectral Scanning

The electromagnetic spectrum includes all possible frequencies of electromagnetic radiation. Wireless communication uses unlicensed radio bands where different types of devices (microwave ovens, cordless phones, video surveillance cameras for example) might emit radio signals that interfere with Wi-Fi service. Spectral analysis detects and reports on radio transmissions in the frequency bands used by Wi-Fi equipment. For more information, about scanning see "Understanding Wireless Scanning" on page 117 and *Monitoring the RF Spectrum of a Radio*.

Copyright © 2013, Juniper Networks, Inc.

Dynamic Frequency Selection (DFS) Channels

The regulatory bodies of most countries now allow many 5-GHz (802.11a) channels that are assigned for use by radar systems to be used for by 802.11 wireless networking, provided there is no radar operating in the vicinity of the wireless network deployment. To use these channels, the wireless access point must implement radar detection and immediately vacate any channel on which radar is active. This requirement is referred to as Dynamic Frequency Selection (DFS). To accomplish this, a DFS mechanism was created to have unlicensed devices detect the presence of a radar system on the device channel and, if the level of the radar is above a certain threshold, vacate that channel and select an alternate channel.

When you deploy an access point, you must configure the correct country of operation to ensure compliance with local government regulations. Failing to do so might cause harmful interference to other systems. In certain countries, such as the United States, access point models are country-specific and will not operate if you configure a different country of operation. Since the corresponding DFS requirements for each available country of operation are programmed into the access point, you do not have to specifically configure the DFS channels. All you need to do is enable DFS in a Radio profile and the appropriate channel avoidance will be implemented.

RFID Asset Tracking

RFID stands for Radio-Frequency Identification. RFID tracking devices consist of transponders, capable of carrying as much as 2,000 bytes of data, with an attached antenna. These devices provide a unique identifier for the object they are attached to.

There are various kinds of RFID, such as the card readers on the doors at companies—the Juniper wireless system does not support those kinds of RFIDs. Juniper access points are capable of reading 802.11 RFID tags that *chirp* short 802.11 messages periodically, for example AeroScout tags. Because the RFID tag must be scanned by an access point radio to retrieve the identifying information, you must configure RFID scanning in a Radio profile. Then the information can be scanned by access points in that Radio profile and fed to a transceiver to interpret the information.

RFID tags replace traditional barcode solutions for inventory and tracking, and provide the following advantages:

- You can track items without climbing ladders, crawling under furniture, or having to be in the direct line of sight of tracked items.
- Most things can be tracked, including people.
- The time it takes to conduct a complete inventory is significantly reduced, while the accuracy of the data is greatly increased.
- The time it takes to locate an asset, for example an expensive medical device, is greatly reduced.

Copyright © 2013, Juniper Networks, Inc.

WMM Power Save

The receiver portion of an 802.11 radio consumes considerable battery power if it is left on all the time. WMM Power Save enables mobile devices to minimize the length of time a receiver is fully powered on, thereby extending extend battery life. With WMM Power Save, the same amount of data can be transmitted in fewer frames in a shorter time, while allowing the Wi-Fi device to preserve power in a low-power, dozing state in between transmissions. To take advantage of WMM Power Save functionality, both the Wi-Fi client and access point must use WMM Power Save. In addition, the applications used also need to support WMM Power Save to inform the client of the requirements of the traffic they generate. WMM is a required feature for 802.11n capable devices—almost all modern Wi-Fi devices support it.

For more information about WMM Power Save, see "Understanding WMM Power Save and WLAN Client Battery Life" on page 121.

Countermeasures

Countermeasures are actions used by controllers and access points to thwart rogue devices attempting to use your network. You can also apply countermeasures to suspect devices. Countermeasures are enabled in a Radio profile and take place automatically when an access point discovers a device.

NOTE: **Countermeasures cannot be configured using Network Director Release 1.0. Use the MSS CLI to configure countermeasures.**

Limiting Client Power

In Radio profiles, you can limit the maximum power level allowed on clients that associate to your access points. Then, when a client associates with an access point, the access point transmits the maximum power level setting allowed in that country to the client. Clients automatically configure their power to match the access point requirements.

802.11n Channel Width

802.11n channels can be either 40 MHz or 20 MHz wide if you use the 5-GHz radio band. See "Understanding Wireless Radio Channels" on page 114 for more information and for instructions to indicate a 40 MHz channel width.

Automatic Channel Tuning

Channel auto-tuning automatically makes channel tuning decisions for access point radios based on the RF data gathered by access points. Channel auto-tuning is configured in a Radio profile and constantly operates on all access point radios by default. For more information about automatic channel tuning, see "Understanding Channel Auto-Tuning and Adaptive Channel Planner on Wireless Networks" on page 86.

Copyright © 2013, Juniper Networks, Inc.

Automatic Power Tuning

The amount of power an access point uses affects the coverage area of the access point. The higher the power level, the larger the coverage area of an access point. Usually, you want your access points to cover all areas with minimal overlap. With automatic power tuning, which is controlled by the Radio profile, access points adjust the power levels of radios automatically, based on the power levels of all neighboring access points. For more information about automatic power tuning, see "Understanding Automatic Power Tuning for Wireless Radios" on page 91.

IEEE 802.11

IEEE 802.11 is a set of standards for implementing wireless local area network (WLAN) computer communication in the 2.4-GHz and 5-GHz frequency bands. For more information about IEEE 802.11, see "Understanding the IEEE 802.11 Standard for Wireless Networks" on page 100.

Long and Short Preamble Length

The preamble is part of the IEEE 802.11b physical layer specification. Specifically, the preamble is a data header section that contains information the access point and clients need when both sending and receiving packets.

In general, use the short preamble type in high network traffic areas, and use the long preamble to provide more reliable communication in noisy (high interference) networks.

Note that all 802.11b devices must support the long preamble format, but can also optionally support the short preamble. Because the short preamble is default, if an 802.11b device has trouble communicating with other 802.11b devices, try using the long preamble.

Related Documentation

- *Understanding the Network Director User Interface*
- Creating and Managing a Radio Profile on page 315
- Creating a Radio Profile for Voice Clients Only on page 329
- Understanding Wireless Scanning on page 117
- Understanding the IEEE 802.11 Standard for Wireless Networks on page 100
- Understanding Call Admission Control on page 93
- Understanding Automatic Power Tuning for Wireless Radios on page 91
- Understanding WMM Power Save and WLAN Client Battery Life on page 121
- Understanding Wireless Radio Channels on page 114

Copyright © 2013, Juniper Networks, Inc.

Understanding Central Network Access With RADIUS and TACACS+

Remote Access Dial In User Service (RADIUS) and Terminal Access Controller Access-Control System Plus (TACACS+) are two common security protocols used to provide centralized access into networks. RADIUS was designed to authenticate and log remote network users, while TACACS+ is most commonly used for administrator access to network devices like routers and switches. Both protocols provide centralized Authentication, Authorization, and Accounting (AAA) management for computers that connect and use a network service.

- *Authentication* - Who is allowed to gain access to the network? Traditionally authorized users provide a username and password to verify their identity for both RADIUS and TACACS+.
- *Authorization* - What services can a user access once they are authenticated? It is unlikely that you want your finance people to have access to the developer database. Visitors may have access only to the Internet, while only IT staff can access the entire passwords database.
- *Accounting* - What services did each user access and for how long? Accounting records record the user's identification, network address, point of attachment and a unique session identifier—these statistics are tracked and added to the user's record. This is useful when time on the system is billed to individuals or departments.

- Why Do I Want Remote Authentication ? on page 46
- Where Is RADIUS Installed on the Network? on page 47
- How Is TACACS+ Installed on the Network? on page 47
- A Comparison of RADIUS and TACACS+ on page 48

Why Do I Want Remote Authentication ?

Remote authentication enables you to keep your username and passwords in one place, on a central server. The advantage to using RADIUS or TACACS+ on this central server is that you don't configure changes on each separate network device when a user is added or deleted, or when a user changes a password. You only make one change to the configuration on the server and then devices continue to access the server for authentication. Although authentication is the most well known function of RADIUS and TACACS+, there are two additional functions provided, authorization and accounting.

NOTE: **Instead of using a flat database on the RADIUS server, you can refer to external sources such as SQL, Kerberos, LDAP, or Active Directory servers to verify user credentials.**

Why Not Just Rely on Firewalls and Filters for Access Control?

Routers and firewalls usually control access to services using filters based on source and/or destination IP addresses and ports. This means that restrictions are applied to devices and not to individual clients. For example if I enable traffic from 10.1.0.255 to

Copyright © 2013, Juniper Networks, Inc.

access a particular web server, then anyone who is sitting at the machine with the address of 10.1.0.255 automatically has access to this server. Using RADIUS or TACACS+, that same person sitting at the machine with the address of 10.1.0.255 also has to provide a username and password to access a service.

What About Using LDAP For Authentication?

Lightweight Directory Access Protocol (LDAP) is a client/server protocol used to access and manage directory information. It reads and edits directories over IP networks and runs directly over TCP/IP using simple string formats for data transfer. Directory servers include information about various entities on your network, such as user names, passwords, rights associated with user names, metadata associated with user names, devices connected to the network, and device configuration.

Use LDAP to obtain directory information, such as email addresses and public keys. If you want to make directory information available over the Internet, this is the way to do it. LDAP works well for captive portal authentication. However, LDAP does not implement 802.1X security easily. 802.1X was essentially designed with RADIUS in mind, so 802.1X challenge/response protocols like MSCHAPv2 work well with RADIUS.

Where Is RADIUS Installed on the Network?

RADIUS includes three components: an authentication server, client protocols, and an accounting server. The RADIUS server portion of the protocol is usually a background process running on a UNIX or Microsoft Windows server.

With RADIUS, the term client refers to a network access device (NAD) that provides the client part of the RADIUS service—wireless access points, a modem pool, a switch, a network firewall, or any other device that needs to authenticate users can be configured as a NAD to recognize and process connection requests from outside the network edge. When a NAD receives a user's connection request, it may perform an initial access negotiation with the user to obtain identity/password information. Then the NAD passes this information to the RADIUS server as part of an authentication/authorization request.

NOTE: **RADIUS requires that each network client device be configured.**

How Is TACACS+ Installed on the Network?

TACACS+ logon authentication protocol uses software running on a central server to control access by TACACS-aware devices on the network. The server communicates with switches or other TACACS-aware devices automatically—these devices do not require further configuration if they are TACACS-aware. The TACACS+ protocol is supported by most enterprise and carrier-grade devices.

Install the TACACS+ Service as close as possible to the user database, preferably on the same server. TACACS+ needs to be closely synchronized with your Domain, and any network connection issues, DNS problems, or even time discrepancies can cause a critical service failure. Installing TACACS+ on the same server as the user database can also improve performance.

Copyright © 2013, Juniper Networks, Inc.

TACACS+ servers should be deployed in a fully trusted internal network. If you keep your TACACS+ service within your trusted network, you need to open only one port, TCP 49. There should not be any direct access from untrusted or semi-trusted networks.

NOTE: **RADIUS is typically deployed in a semi-trusted network, and TACACS+ uses internal administrative logins, so combining these services on the same server could potentially compromise your network security.**

A Comparison of RADIUS and TACACS+

Table 14: RADIUS and TACACS+

	RADIUS	TACACS+
Primary Use	Authenticate and log remote network users	Provide administrator access to network devices like routers and switches
Authentication and Authorization	Authentication and Authorization checking are bundled together. When the client device requests authentication from the server, the server replies with both authentication attributes and authorization attributes. These functions can not be performed separately.	All three AAA functions (authentication, authorization, and accounting) can be used independently. Therefore, one method such as kerberos can be used for authentication, and a separate method such as TACACS+ can be used for authorization.
Accounting	The accounting features of the RADIUS protocol can be used independently of RADIUS authentication or authorization.	
Protocol	User Datagram Protocol (UDP)/IP with best-effort is used for delivery on ports 1645/1646, 1812/1813	TCP used for delivery on port 49. Also has multiprotocol support for AppleTalk Remote Access (ARA) protocol, NetBIOS Frame Protocol Control protocol, Novell Asynchronous Services Interface (NASI), and X.25 PAD connection.
Encryption applied to	Password	Username and password
802.1X Security	If you want to use 802.1x port-based network access control, you have to use the RADIUS client because the TACACS+ client does not support that feature.	
Model	client/server	
Recommended Environment	semi-trusted	trusted

Related Documentation

- Creating and Managing RADIUS Profiles on page 326

Copyright © 2013, Juniper Networks, Inc.

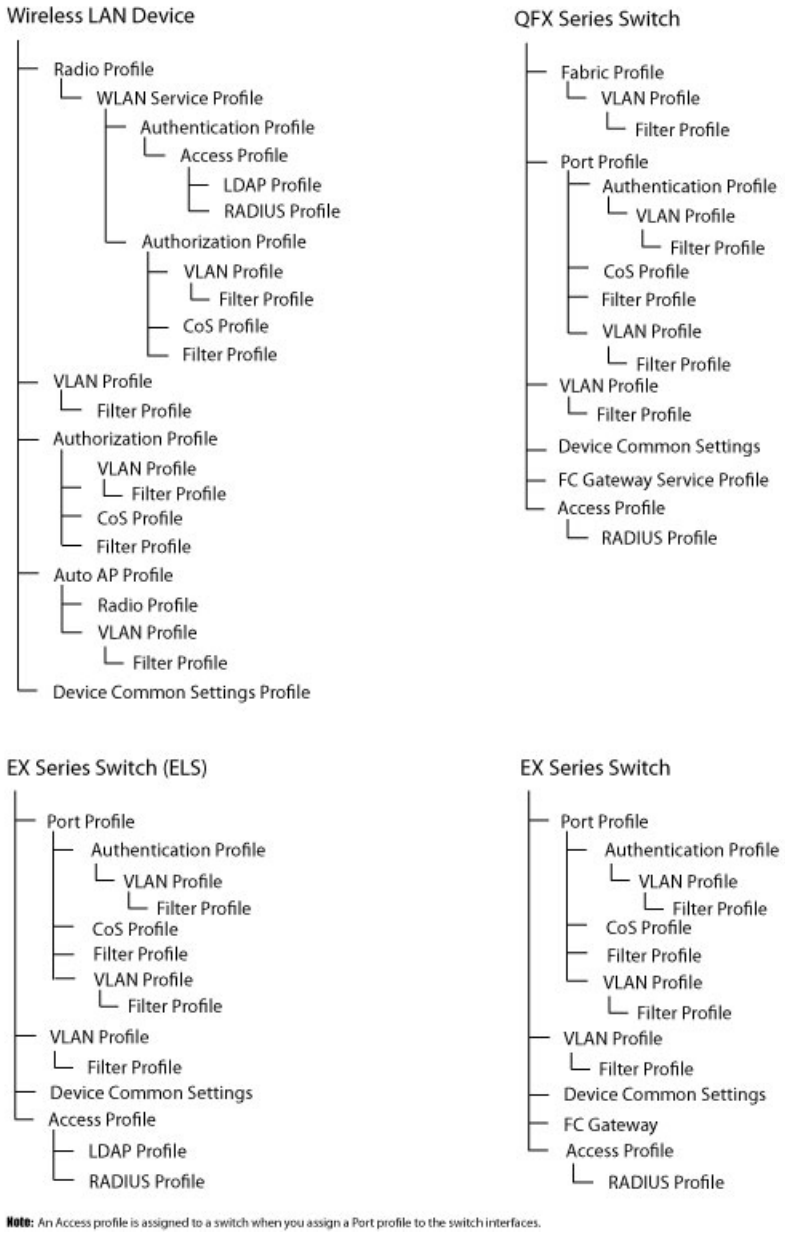
Understanding VLAN Profiles

A virtual LAN (VLAN) is a Layer 2 broadcast domain that can span multiple wired or wireless LAN segments. Each VLAN is a separate logical network, grouping hosts with common requirements, regardless of their physical location

VLAN profiles in Network Director enable multiple VLAN configuration from a single profile. Each VLAN profile is specific to a device family, either EX Switching, Wireless, Campus Switching ELS, or Data Center Switching Non-ELS. In addition, the VLANs are created for different purposes at different levels, as shown in Figure 3 on page 50.

Copyright © 2013, Juniper Networks, Inc.

Figure 3: VLANs Are Specific to Device Families and Function Levels



Note: An Access profile is assigned to a switch when you assign a Port profile to the switch interfaces.

After a VLAN profile is created, you assign it to either wireless ports, switches, controllers, custom groups, port groups with wireless ports, or access points that are managed by controllers or clusters. You can also assign VLAN profiles to controller-managed access points and cluster-managed access points for local switching on the access points.

For EX Series Switches and Campus Switching ELS, apart from the basic settings, you can specify:

Copyright © 2013, Juniper Networks, Inc.

- MAC parameters
- Switching and routing parameters
- L2 and L3 Filters
- VLAN security DHCP, ARP inspection, and MAC movement.

For controllers, apart from the basic settings, you can specify:

- Filter details
- Routing
- DHCP enabled
- IGMP settings
- Spanning tree protocol settings

For data center switching devices, apart from the basic settings, you can specify:

- MAC parameters
- Switching and routing parameters
- Filters
- VLAN security settings
- Fibre Channel over Ethernet (FCoE) Initialization Protocol (FIP) settings

TIP: Single VLAN IDs can be configured for all products and circumstances. VLAN lists or VLAN ranges of IDs are available for some products, depending on the technology used for implementation. For example, EX Switching does not support a VLAN list. Campus Switching ELS supports a VLAN ID range only as part of a VLAN ID list. You will only see the available configurations for the selected device family.

Related Documentation

- Creating and Managing VLAN Profiles on page 330
- Assigning a VLAN Profile to Devices or Ports on page 392
- Understanding Profiles on page 15
-

Copyright © 2013, Juniper Networks, Inc.

Understanding WLAN Service Profiles

A wireless LAN (WLAN) Service profile is a set of configurations, including a unique SSID, that provides clients part of a wireless connection to the wireless network. You must have at least one WLAN Service profile/SSID on your wireless network for operation. Note that there are no default profiles provided by MSS—you must configure each WLAN Service profile. This topic describes the parameters configured in a WLAN Service profile.

There are many parameters, either optional or mandatory, that are associated with every SSID. The WLAN Service profile provides some of these parameters but not all of them.

This topic describes the parameters configured in a WLAN Service profile:

- SSID on page 53
- Mapping WLAN Service Profiles to Additional Profiles on page 53
- SSID Encryption on page 53
- Associated Authentication Profile on page 54
- Associated Authorization Profile on page 54
- VLAN Use on page 54
- Bandwidth Limit For Client Sessions on page 54
- Load Balancing Between Access Points on page 54
- Using Proxy ARP on page 54
- Restricting DHCP on page 55
- Client Types on page 55
- Call Admission Control Settings For Voice on page 55
- Retry Count on page 56
- Client Timeouts on page 56
- 802.11n Settings on page 56
- Maximum Bandwidth Used by an SSID on page 57
- Maximum Transmission Unit Parameter on page 57
- Client Probing of Idle Clients on page 57
- Enable Pre-shared Key (PSK) For WPA or WPA2 on page 57
- Create a Pre-shared Key (PSK) Phrase For WPA or WPA2 on page 58
- Create a Pre-shared Key (PSK) Raw Phrase For WPA or WPA2 on page 58
- Enforce Data Rates on page 58
- Retry Count For Sending Frames on page 58
- WPA Encryption Type Used on page 58
- Shared Key Authentication Values on page 58
- Radio Transmit Rates Used on page 59
- WMM Power Save on page 59

Copyright © 2013, Juniper Networks, Inc.

SSID

The SSID name is the most important configuration in a WLAN Service profile. Only the SSID name and WLAN name are actually required to create a WLAN Service profile—the other parameters have default values.

Wireless networks are identified by unique network names such as juniper_meetings or employee_patio. The unique name is known as a service set identifier, or SSID and this electronic identifier serves as a password for certain online communications. Most routers are set to broadcast their SSID using WPA or WPA2 encryption. This allows nearby computers to find and connect to nearby networks. If an SSID is not broadcast, you must manually configure one or more SSIDs on clients so that the client automatically finds and connects to those SSIDs when it is in range of the networks. On a Windows PC, this setting is typically found in the Network Control Panel.

Beaconing the SSID Name

By default, SSIDs are beaconed, meaning that an SSID advertises its name on the air. You might want to disable beaconing for security reasons, although doing so can make it more difficult for clients to access the WLAN. When you disable beaconing for an SSID, the radio still sends beacon frames, but the SSID name in the frames is blank. For a non-beaconed SSID, radios only respond to directed 802.11 probe requests that match the non-beaconed SSID string.

NOTE: **Disabling beaconing is not particularly effective as a security measure because any sniffer can easily detect the name of the SSID.**

Mapping WLAN Service Profiles to Additional Profiles

WLAN Service Profiles rely on other profiles, such as Authentication profiles and Authorization profiles, to provide additional parameters for the SSID. You link these other profiles as part of the WLAN configuration. (For more information, see "Understanding Network Director SSID Configuration With Profiles" on page 59.) The completed WLAN Service profile is then mapped to a Radio profile during configuration of the Radio profile. It is the Radio profile that is actually deployed to controllers, pulling all of the other mapped profiles along with it.

SSID Encryption

Encryption protects information within a wireless session by reading that information in a data stream and altering it to make it unreadable to users outside the network.

Encryption (ssid-type) is either on (Crypto) or off (Clear). If encryption is on, additional configuration indicates the type of encryption (WPA and/or WPA2), any added ciphers such as TKIP (tkip-mc-time) or CCMP. For more information, see "Understanding Wireless Encryption and Ciphers" on page 109.

Both WPA and WPA2 are enabled by default in Network Director. Clients that use only WPA associate using WPA and all clients capable of using WPA2 associate using WPA2.

Copyright © 2013, Juniper Networks, Inc.

NOTE: The original wireless encryption method, WEP, is not supported in Network Director.

Authentication Used for Encryption Methods

The standard for wireless LAN authentication is the IEEE 802.1x standard, which is based on the IETF's Extensible Authentication Protocol (EAP). EAP and 802.1x together provide an authentication framework.

The second way to authenticate encrypted traffic is pre-selected key (PSK) authentication. If you use PSK, you must also provide the key or password. For more information, see "Understanding Wireless Encryption and Ciphers" on page 109.

Associated Authentication Profile

An Authentication profile must be associated with each WLAN Service profile—you do this by selecting an Authentication profile while configuring the WLAN. Authentication profiles are described in "Understanding Authentication Profiles" on page 22.

Associated Authorization Profile

An Authorization profile is also mapped to WLAN Service Profiles—you do this by selecting an Authorization profile while configuring the WLAN. Authorization profiles are described in "Understanding Authorization Profiles" on page 24.

VLAN Use

Clients usually switch VLANs when they switch controllers, usually as a result of roaming, but you can make initially assigned VLANs persist over different controllers. If an 802.1X user is not assigned to a VLAN by AAA, and subsequently roams to a controller where the VLAN he was in does not exist, a tunnel is set up so that he stays in that VLAN. This does not work for Web portal clients, however.

Bandwidth Limit For Client Sessions

You can limit bandwidth for clients to prevent one client from hogging bandwidth.

Load Balancing Between Access Points

RF load balancing is the ability to reduce network congestion over an area by distributing client sessions across the access point radios with overlapping coverage in the area. Load balancing automatically occurs on the mobility domain to ensure maximum failover capability. For more information, see "Understanding Load Balancing for Wireless Radios" on page 97.

Using Proxy ARP

Proxy address resolution protocol (ARP) is a technique by which a device on a network answers requests for a different device. Because the proxy knows the location of the traffic's destination, it offers its own IP address then sends the traffic on to the true destination.

Copyright © 2013, Juniper Networks, Inc.

Usually, wireless clients receive an IP address from a router. If you want to, you can have the controller respond to wireless clients' search for a destination, and then forward the traffic to the router.

Restricting DHCP

The dynamic host configuration protocol (DHCP) is used to configure network devices with IP addresses from a DHCP server.

You can configure a controller to capture but not forward any wireless client traffic except DHCP traffic during authentication and authorization. This is referred to as restricting DHCP and enables a controller to authenticate and authorize new clients more quickly.

Client Types

You decide which client types to support on a WLAN. If you put all clients on one WLAN, they will be reduced to the speed of the slowest client—we do not recommend doing this.

Possible client types are:

- 802.11n clients use newer technology that can produce throughput link rates above 54 MBps, if you select only this client type and enforce the data rate (speed). Typical clients include laptops, PCs, and streaming video.

  NOTE: **The Wi-Fi Alliance requires that high-throughput (802.11n) transmissions use WPA2 and CCMP.**

- 802.11g clients can have throughput link rates as fast as 54 MBps, with a more average rate of 19 MBps. Typical clients include older laptops and PCs.
- 802.11a clients can have throughput link rates as fast as 54 MBps, with a more average rate of 19 MBps.
- 802.11b clients can have throughput link rates as fast as 10 MBps.

Call Admission Control Settings For Voice

Call admission control (CAC) regulates the addition of new real-time media sessions on access point radios, guaranteeing a higher quality of service to a fixed number of clients by limiting either the number of concurrent sessions or the number of concurrent phone calls.

There are two CAC methods, WMM and SVP. WMM is enabled by default and is used by all newer 802.11n devices. SVP includes all the configurations of WMM, but adds Spectralink phones at the top of the priority list. SVP is a legacy technology—Spectralink's new phones use WMM.

As the name indicates, call admission control applies to real-time media traffic as opposed to data traffic. Call admission control mechanisms and Quality of Service settings work together to protect voice traffic from the negative effects of other voice traffic and keep

Copyright © 2013, Juniper Networks, Inc.

excess voice traffic off the network. For more information, see "Understanding Call Admission Control" on page 93.

Retry Count

The retry count is the number of times a channel resends a frame without getting a response. You can configure 1 - 15 attempts, with each attempt taking more time and affecting throughput. We recommend configuring five attempts.

You can also specify either a long retry count or a short retry count. The difference between the two methods is the length of the pause between attempts. In general, a short retransmission works best in heavy traffic and is used most often. You might want to try a long transmission if the network is experiencing a lot of interference.

Client Timeouts

Timeouts are used to disconnect clients under certain circumstances. You can change the timeframes for these timeouts:

- User Idle—180 seconds
- Handshake attempt (logon)—20 milliseconds
- Web portal session—zero seconds (meaning no timeout)

802.11n Settings

802.11n is the most recent wireless technology that utilizes different mechanisms than previous versions of 802.11. Therefore, there are settings that apply only to 802.11n traffic.

Guard Intervals

A guard interval is the interval is observed before the next bit of traffic is transmitted. This guard interval ensures that bit transmissions do not interfere with one another. As long as the echoes fall within this interval, they do not affect the receiver's ability to safely decode the actual data, because data is only interpreted outside the guard interval—it eliminates intersymbol interference. In normal 802.11 operation, the guard interval is 800 ns. In 802.11n operation, short guard intervals of 400 ns are supported. Shorter guard interval between symbols increases throughput. Legacy devices may require long guard intervals. By reducing this interval (called **short guard interval**), data bits are transmitted in shorter intervals and provide for increased throughput.

Frame Aggregation

You can enable frame aggregation for certain frame types in 802.11n. Multiple packets of application data can be aggregated into a single packet called an aggregated MAC protocol data Unit (A-MPDU). This improves performance because the number of packets is reduced.

After transmission of every frame, an idle time called Interframe Spacing (IFS) is observed before transmitting the subsequent frame. When frames are aggregated, fewer IFS intervals are used, which in turn reduces the time for data transmission. In addition, when clients operating in 802.11n send acknowledgement for block of aggregated packets

Copyright © 2013, Juniper Networks, Inc.

instead of individual packets, overhead involved in frame acknowledgements and increasing overall throughput is reduced.

MAC Service Data Unit (MSDU) Length

With 802.11n, you can change the maximum length for a MAC service data unit (MSDU) to reduce the overhead associated with each transmission. An MSDU is the service data unit received from the logical link control (LLC) sub-layer which lies above the medium access control (MAC) sub-layer in a protocol stack. When 802.11n is an enabled client type for this WLAN, you can configure the maximum aggregated MSDU packet length. This enables joining multiple packets together into a single transmission unit, which reduces the overhead associated with each transmission. MSDU default length is 4K.

MPDU Length

MPDU can have a maximum length for frame aggregation.

Maximum Bandwidth Used by an SSID

The speed of a computer network is most commonly stated in bandwidth units of Megabits/ Gigabits (Mbps /Gbps) per second. This standard measure of communication capacity (data rate) is advertised by all computer networking equipment. When you indicate a maximum bandwidth for a WLAN, you are indicating the highest data rate you support with a given WLAN Service profile. Devices in each category have a maximum bandwidth, so the maximum bandwidth also determines which devices are supported. For example, the 802.11g standard for wireless networking supports a maximum bandwidth of 54 Mbps, including overhead. 802.11n supports a maximum bandwidth of 600 Mbps.

Maximum Transmission Unit Parameter

The maximum transmission unit (MTU) of the communications protocol of a layer is the size (in bytes) of the largest protocol data unit that the layer can forward. MTU parameters usually appear in association with a communications interface such as a NIC card or serial port.

Client Probing of Idle Clients

Idle client probing sends periodic keepalives from a radio to non-transmitting clients. By default, a radio sends idle-client probes every 10 seconds to each client with a session on the radio to verify that the client is still active. The probes are unicast null-data frames. Normally, an active client sends an ACK in reply to an idle-client probe. If a client does not send any data or respond to idle-client probes before the user idle timeout expires, the client session is disassociated.

Enable Pre-shared Key (PSK) For WPA or WPA2

WPA-PSK is an authentication mechanism in which users provide credentials to verify whether or not to allow them access to a network. This requires that a single password be entered into each WLAN node (access points, wireless routers, client adapters, bridges). When the passwords match, a client is granted access to a WLAN.

Copyright © 2013, Juniper Networks, Inc.

Create a Pre-shared Key (PSK) Phrase For WPA or WPA2

A pre-shared key (PSK) phrase is the hexadecimal secret phrase used for authenticating WPA or WPA2 clients. Note that either WPA or WPA2 security must be enabled for this to have any effect.

Create a Pre-shared Key (PSK) Raw Phrase For WPA or WPA2

A pre-shared key (PSK) raw phrase is the raw hexadecimal secret phrase used for authenticating WPA or WPA2 clients. Note that either WPA or WPA2 security must be enabled for this to have any effect.

Enforce Data Rates

By default, a client can associate with and transmit data to an access point using a slower data rate than the mandatory or standard rate, although the access point does not necessarily transmit data back to the client at the slower rate.

When you enforce data rates, a connecting client must transmit at one of the mandatory or standard rates to associate with the access point. Clients transmitting at slower rates are not allowed to associate with the access point.

Retry Count For Sending Frames

Retry-count settings indicate how many times that the network sends either a long unicast frame or short unicast frame without receiving an acknowledgement. If you set retry count to zero, frames are sent once with no retries.

NOTE: The fragmentation threshold uses the short-retry-count for frames shorter than 2346 bytes and uses the long-retry-count for frames that are 2346 bytes or longer.

WPA Encryption Type Used

Enable and choose WPA encryption—either WPA or WPA2. Either or both TKIP and CCMP cipher algorithms for WPA and WPA2 can be added.

NOTE: The Wi-Fi Alliance requires that high-throughput (802.11n) transmissions use WPA2 and CCMP.

Shared Key Authentication Values

Shared key authentication is a process by which a client gains access to a WLAN using an encryption key. The key, obtained in advance by the client, must match a key stored at the access point. To begin the connection process, the client sends a request for authentication to the access point. The access point responds by generating a sequence of characters called a challenge text for the computer. The computer encrypts the challenge text with the key and transmits the message back to the access point. The

Copyright © 2013, Juniper Networks, Inc.

access point decrypts the message and compares the result with the original challenge text. If there are no discrepancies, the access point sends an authentication code to the connecting computer. Finally, the computer accepts the authentication code and becomes part of the network for the duration of the session or for as long as it remains within range of the original access point. If the decrypted message does not precisely agree with the original text, the access point does not allow the computer to become part of the network.

Radio Transmit Rates Used

Radio transmit rates supported by access point radios have defaults, but you can change the transmit rates for the radios. Each type of radio (802.11a, 802.11b, 802.11g, and 802.11n) providing service to an SSID has a set of rates the radio is enabled to use for sending beacons, multicast frames, and unicast data. The rate you set also specifies the rates clients must support to associate with a radio.

WMM Power Save

WMM Power Save is disabled by default, even though it saves client battery life, because clients using power save must send a separate PSpoll to retrieve each unicast packet buffered by the access point radio. This increases bandwidth and affects performance. For more information, see "Understanding WMM Power Save and WLAN Client Battery Life" on page 121.

Related Documentation

- Creating and Managing a WLAN Service Profile on page 350
- Understanding WMM Power Save and WLAN Client Battery Life on page 121
- Understanding Authorization Profiles on page 24
- Understanding Wireless Encryption and Ciphers on page 109
- *Understanding the Network Director User Interface*
- Understanding Network Director SSID Configuration With Profiles on page 59

Understanding Network Director SSID Configuration With Profiles

Service set identifiers (SSIDs) uniquely identify a set of profile configurations with names up to 32 characters long. SSIDs are broadcast to clients by access points—the SSID name appears in the list of available wireless networks on clients' laptops or other devices. For a wireless user, connecting to an SSID is as easy as selecting a name from the list. However, creating that SSID involves more steps.

This topic describes:

- Configuring an SSID with Network Director on page 60
- SSID Access Information on page 61
- SSID Authentication Information on page 61
- SSID WLAN Information on page 61
- SSID Radio Information on page 61
- What Do I Do When All of These Profiles Are Complete? on page 62

Copyright © 2013, Juniper Networks, Inc.

Configuring an SSID with Network Director

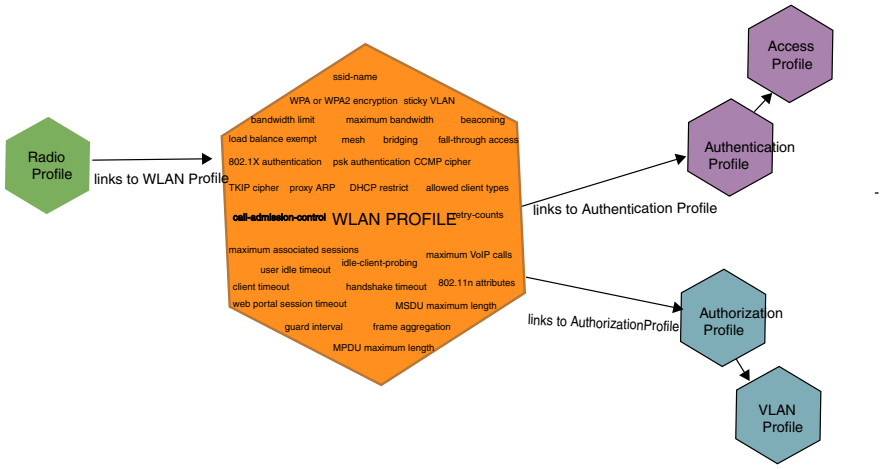
Configuring an SSID is more complicated than connecting to an SSID. You could think of the SSID as needing a number of puzzle pieces (called profiles) that fit together to form the SSID. You typically associate all of the following profiles with each SSID:

- VLAN profile
- Access information in an Access profile
- Authentication information in an Authentication profile
- Authorization information in an Authorization profile
- WLAN configuration in a WLAN Service profile
- Radio configuration in a Radio profile

Figure 4 on page 60 illustrates the connections between profiles.

NOTE: Some profiles are optional, depending on your configuration.

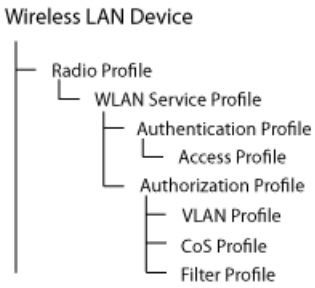
Figure 4: SSID Information is Located in These Profiles



Another way to think of the relationship between profiles is shown in Figure 5 on page 61. You build the needed profiles, starting with profiles at the far right of the chart and working your way to the left. When the Radio profile is assigned to radios discovered by the controller, the profile configuration is complete.

Copyright © 2013, Juniper Networks, Inc.

Figure 5: Relationship Between Profiles Needed to Create an SSID



SSID Access Information

Access profiles include details about authentication methods and accounting servers used by an SSID. Radius, LDAP, and local authentication are the supported authentication methods and RADIUS and LDAP are the supported accounting methods. For more information about Access profiles, see "Understanding Access Profiles" on page 21 or "Creating and Managing Access Profiles" on page 136.

SSID Authentication Information

Authentication profiles include the authentication method and authentication parameters used for SSID client authentication. Available authentication methods are 802.1X (dot1x), MAC-RADIUS, Captive Portal, and Last Resort. 802.1X is the default authentication method for all device types. For more information about Authentication profiles, see "Understanding Authentication Profiles" on page 22. To create, edit, or delete an Authentication profile, see "Creating and Managing Authentication Profiles" on page 157.

SSID WLAN Information

You name SSIDs in the WLAN Service profile, in addition to configuring the encryption method (WPA or WPA2), and beaconing. Typically, you also indicate VLAN use, SSID bandwidth limits, radio load balancing, proxy ARP, DHCP restrictions, and permitted client types.

Call admission control, retry counts, guard interval, frame aggregation, MSDU, MPDU, client bandwidth limits, MTU, idle client probing, data rates, and WMM Power Save are also configured in the WLAN Service profile.

For more information, see "Understanding WLAN Service Profiles" on page 52 or "Creating and Managing a WLAN Service Profile" on page 350.

SSID Radio Information

Radio-profiles are used to form groups of radios and define which wireless services are broadcast by the group. Additional radio related parameters are also configured at this level.

For more information, see "Understanding Radio Profiles" on page 42 or "Creating and Managing a Radio Profile" on page 315.

Copyright © 2013, Juniper Networks, Inc.

What Do I Do When All of These Profiles Are Complete?

If you are using Network Director, radios only actually broadcast an SSID after you assign a Radio profile to a controller (see "Assigning a Radio Profile to Radios" on page 389, then deploy the controller configuration (see *Deploying Configuration to Devices*.) At this time, all associated profiles also go into effect.

Related Documentation

- Understanding Access Profiles on page 21
- Creating and Managing Access Profiles on page 136
- Understanding Radio Profiles on page 42
- Creating and Managing a Radio Profile on page 315
- Understanding WLAN Service Profiles on page 52
- Creating and Managing a WLAN Service Profile on page 350
- Understanding the Network Terms SSID, BSSID, and ESSID on page 103
- Understanding Authentication Profiles on page 22
- Creating and Managing Authentication Profiles on page 157
- *Deploying Configuration to Devices*

Copyright © 2013, Juniper Networks, Inc.

CHAPTER 3

Topology View Overview

- Understanding the Location View on page 63
- Understanding the Network Topology in Network Director on page 65
- Understanding the Topology View Tasks pane on page 68

Understanding the Location View

The Location View is one of the perspectives that Network Director enables you to view and analyze your network. Using this view, you can view devices and data based on their physical location and proximity in the network. By physical location, we mean the buildings, floors, aisles, racks, wiring closets, and outdoor areas where the devices reside. After these locations are defined and devices assigned, the Location View gives you a visual representation of your devices based on where they reside.

You can define the physical location where the devices in the network are deployed in a hierarchical way, and define location entities from a site down to the wiring closet. When in the Location View, the network tree shows the network in terms of buildings, floors, aisles, racks, wiring closets, and outdoor areas nested beneath the building. The hierarchy of the locations is:

- Site—Your campus or data center; the highest node in your location.
- Building—One entry for every building at your site. Buildings are listed in alphabetical order, not by address or the order in which you identified them to the system.
- Floors—One entry for each floor within the building; Floors are nested within the building.
- Aisles—One entry for each aisle in a floor. Aisles are nested within the floor.
- Racks—One entry for each rack in an aisle. Racks are nested within the aisle.
- Outdoor Area—One entry for each named area; Outdoor areas are associated with buildings.
- Devices—Most are assigned to buildings, floors, outdoor areas, or racks. Access points can be assigned only to outdoor areas and floors. Devices are not assigned at the site level; those devices are considered unassigned.

The hierarchical model enables you to define a location by using either of these methods:

Copyright © 2013, Juniper Networks, Inc.

- Using the Location Setup wizard to set up a location in a single process, starting at the site level and progressing to the racks and outdoor areas. The wizard also provides an option to create part of the location, such as defining the site and building, then to use the individual procedures to create floors and wiring closets for the building you created.
- Using separate tasks to create location entities in sequence in a top-to-bottom order. You can create the higher level entities such as a site or building first and save them. Later, you can add floors and wiring closets when information about them becomes available.

Related Documentation

- Setting Up the Location View on page 414
- Creating a Site on page 409

Copyright © 2013, Juniper Networks, Inc.

Understanding the Network Topology in Network Director

Junos Space Network Director provide features for monitoring and managing Juniper Networks EX Series Ethernet Switches, QFX Series Switches, and Juniper Networks WLC Series Wireless LAN Controllers (WLCs) besides enabling connectivity visualization between discovered and managed devices such as routers, switches, controllers, and access points. Connectivity between devices and their association with their location provide the foundation for rendering topology in a complete manner.

As a network administrator, you must have a clear understanding of the various networking devices in your network, their physical locations, and how these devices are interconnected in your network. The network topology represents the interconnection between various devices in your network, which are managed by Network Director, based on their connectivity and association to their physical surroundings. The network topology provides a visual insight into the network, which is useful for debugging, troubleshooting, planning, and executing administrative actions.

Before you access the topological view of your network, you must:

- Connect to the Internet before accessing the Topology View in Network Director as this feature works only while connected to the Internet.
- Discover the devices managed by Network Director in your network. For details about discovering devices, see "Discovering Devices in a Physical Network" on page 455.

  NOTE: **You must specify the SNMP parameters during device discovery to have all the devices discovered and managed by Network Director available in the topology view. However, you can specify the SNMP parameters in the Refresh Discovery task from the Topology View also.**

  NOTE: **Ensure that you have specified the LLDP and STP parameters while configuring the devices as Network Director uses these parameters to determine the connectivity of devices with their neighbors in the network.**

- Set up the physical location of the devices in your network based on the geographical location of the devices. Some examples of location nodes are: sites, buildings, floors, closets, and aisles. You can set up one location node within another location node as in buildings within a site or floors within a building. You can then assign the network devices based on their location in buildings, floors, outdoor areas, closets, and racks. Apart from using the Location Management tasks in the Location View, you can set up the location details of the network devices managed by Network Director by using the *Setup Locations* task from the Task menu in the topology view. For details, see "Setting Up the Location View" on page 414. The device-to-topology-group location relationship is established when a device is placed at a specific location on a topology map.

Network topology enables you to view all the discovered devices in your network, overlaid on a map where the devices are located across sites, buildings, floors, outdoor area,

Copyright © 2013, Juniper Networks, Inc.

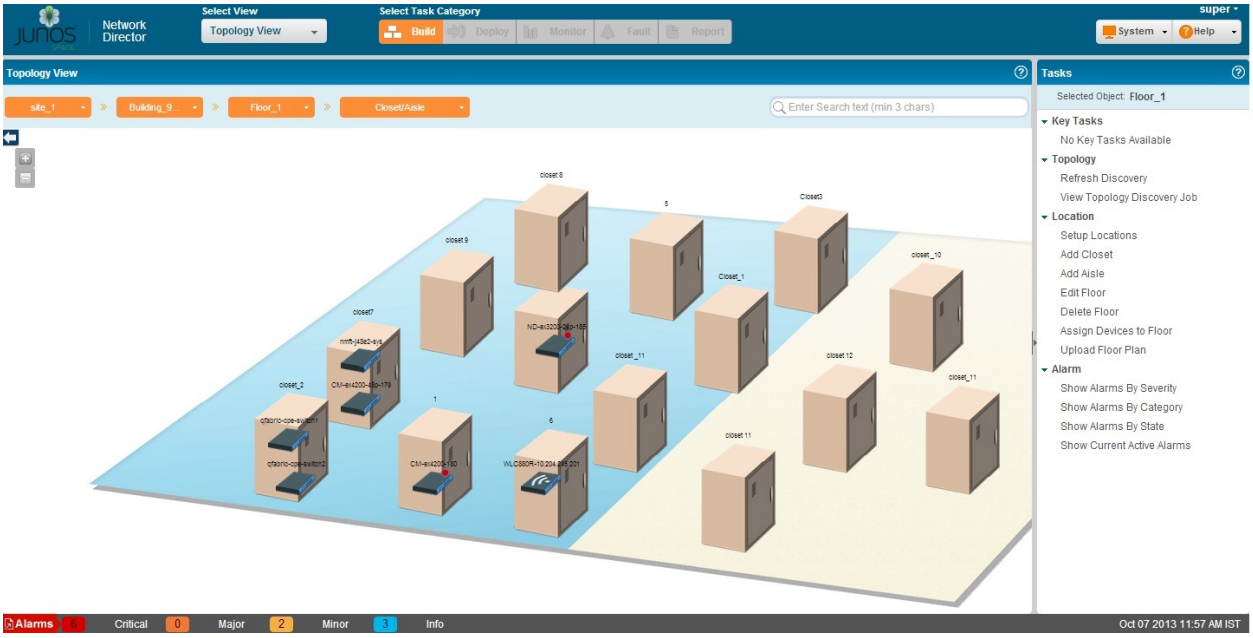
closets, and racks along with their physical interconnection with other devices in your network. Topology also provides visualization around physical connectivity between various discovered interconnected devices. You can use the topology view to zoom in or zoom out of a site to a building and a building to a site. In the topology view, you can also double-click a node such site, buildings, and so on to navigate to the next node. You can also see the connectivity between a device and its immediate neighbors, alarms details, and so on. Network Director also enables you to assign devices to buildings, floors, closets, and outdoor areas on the map.

Network topology also provides visualization around physical connectivity between various discovered interconnected devices. You can upload a floor plan at the floor level or a map at the outdoor area if you already have the floor plan or map available. You can then move the nodes in the topology view page based on the floor plan.

Network Director supports QFabric internal topology.

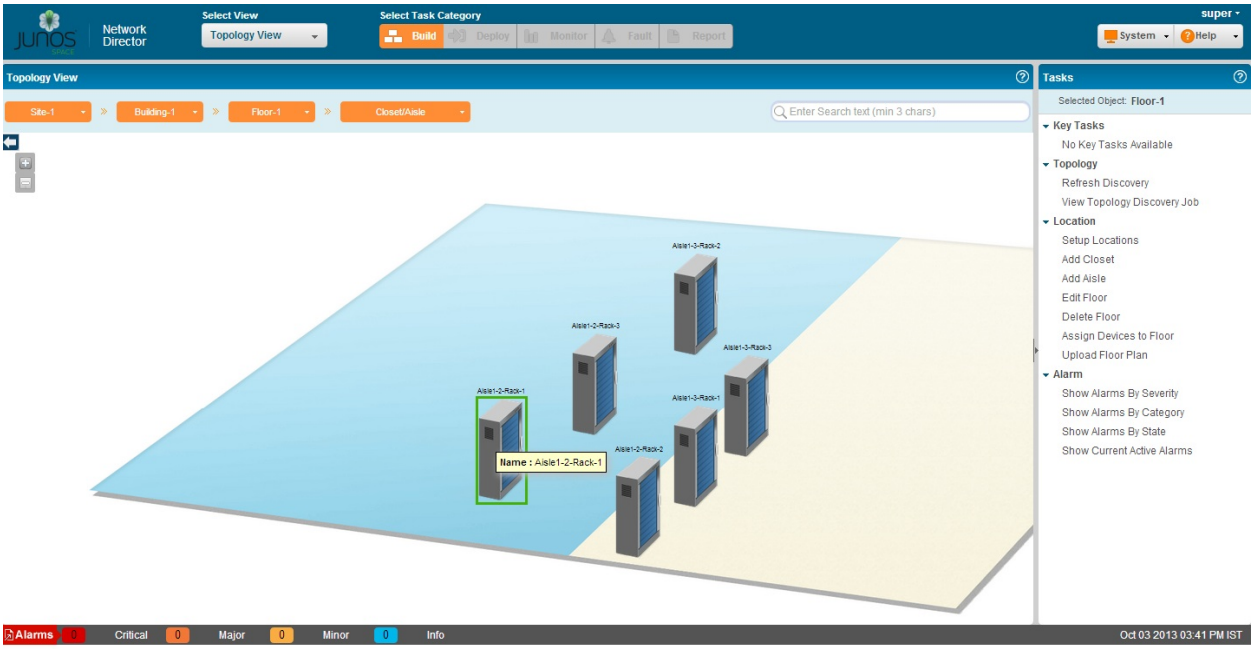
The topology display is created by layering the device images on top of the imported floor plan images as shown in Figure 6 on page 66 and Figure 7 on page 67.

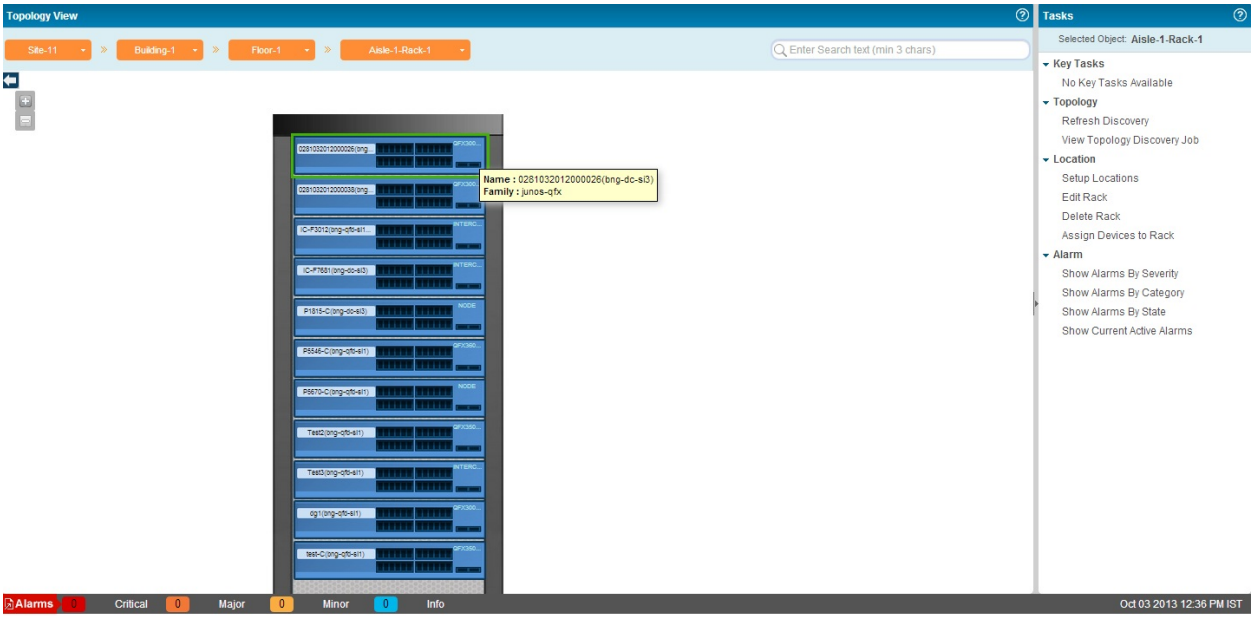
Figure 6: Typical Floor Plan Displaying the Closets and Devices



Copyright © 2013, Juniper Networks, Inc.

Figure 7: Typical Floor Plan Displaying the Racks and QFX Devices





Related Documentation

- Discovering Devices in a Physical Network on page 455
- Setting Up the Location View on page 414
- Setting Up and Managing the Topology View on page 417

Copyright © 2013, Juniper Networks, Inc.

Understanding the Topology View Tasks pane

The Tasks pane in Topology View contains all the tasks you can do in the Topology View. Click a specific task to begin that task.

Not all tasks are available in the Topology View. As you change your selections in the Topology map pane, the tasks in the Tasks pane also change—that is, some tasks such as Show Device Connectivity and Show QFabric Connectivity are available only after you select a device or a QFabric device, and Alarm tasks are available only after you select a site, building, floor, closet, or device.

Topology View tasks are divided into the following categories in the Tasks pane.

- Key Tasks—The most preferred tasks that you want to do while using the topology view. You can add important tasks from the topology task menu and hence the Key Tasks are a duplicate of select tasks from the Topology and Location tasks menu.
- Topology—The tasks you do to create the topology of your network.
- Location—The tasks you do to create a location such as a site, building, floor, closet, aisle, rack, and outdoor area.
- Alarm—The tasks that enable you to monitor the fault alarm details of the devices.

Table 15 on page 68 describes the topology view tasks.

Table 15: Topology View Tasks

Task	Description
Key Tasks	A duplicate of the most important tasks from other tasks menu. You can add your frequently used tasks to the key tasks menu.
Topology: Displays the device discovery tasks	
Show Device Connectivity	Displays the connection details of a device with its neighbors in graphical and grid views. If the selected device is connected to more than 60 devices, then the connection details are displayed only in grid view.
Show QFabric Connectivity	Displays the dataplane connectivity details between the Interconnects and Nodes.
Refresh Discovery	Refreshes the devices discovered and managed by Network Director earlier from Build mode. This task also refreshes the device connectivity.
View Topology Discovery Job	Displays the discovery jobs in the topology view pane.
Location: Displays the location related tasks	
Setup Locations	Creates a new location. This task has sub tasks to add sites, buildings, floors, outdoor area, and closets. NOTE: You cannot create aisles and racks from Topology View. You must create the aisles and racks from the Location View work flow.

Copyright © 2013, Juniper Networks, Inc.

Table 15: Topology View Tasks *(continued)*

Task	Description
Add Site	Creates a new site in Location view. NOTE: Use this task only to create the site object. Buildings, floors, closets, and outdoor areas in the site must be created separately.
Add Building	Creates a new building in the selected site. NOTE: Use this task only to create the building. Floors and closets in the building must be created separately.
Add Outdoor Area	Creates a new outdoor area in the selected site.
Upload Floor Plans	Enables you to upload a floor plan for a floor in a building, if you already have a floor plan.
Upload map	Enables you to upload a map to an outdoor area.
Delete Site/Edit Site	Deletes or modifies the selected site.
Alarm: Displays the alarm related tasks	
Show Alarms by Severity	Displays the fault alarm details sorted based on the severity, that is from critical, major, minor, and info.
Show Alarms By Category	Displays the fault alarm details sorted based on the category, that is from active, acknowledged, and cleared.
Show Alarms By State	Displays the fault alarm details sorted based on the state, that is from active, acknowledged, and cleared.
Show Current Active Alarms	Displays any active alarm that has not yet been cleared.

Related Documentation

- Understanding the Network Topology in Network Director on page 65
- Setting Up and Managing the Topology View on page 417

Copyright © 2013, Juniper Networks, Inc.

Copyright © 2013, Juniper Networks, Inc.

CHAPTER 4

Virtual View Overview

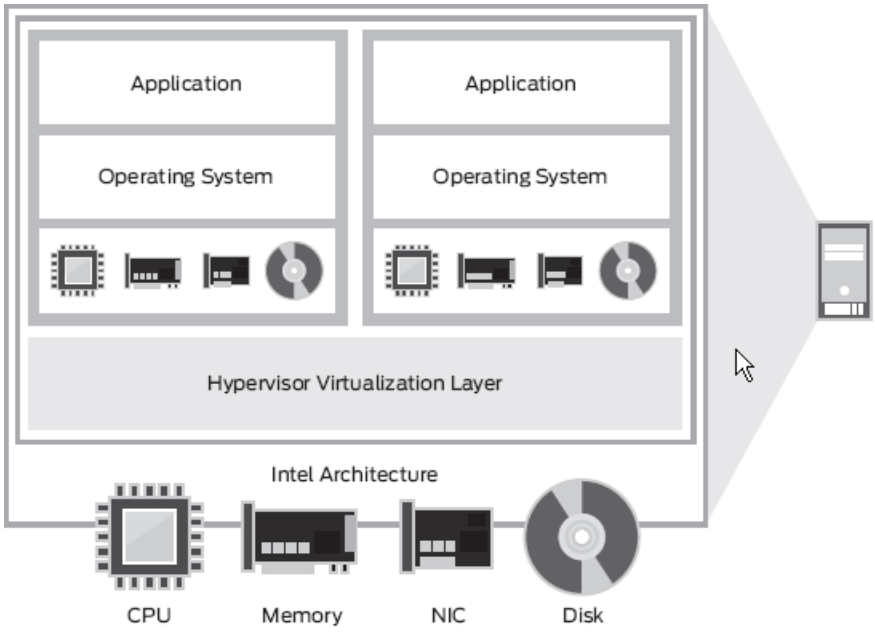
- Understanding Virtual Networks on page 71
- Understanding Virtual Network Management on page 72
- Understanding the Build Mode Tasks Pane for Virtual View on page 74

Understanding Virtual Networks

Virtual networks consist of virtual devices that are connected together in a virtual environment. Virtual machines (VMs), rendered by hypervisors, enable different VMs to share underlying hardware resources. Hypervisors (virtual machine monitors) are small-footprint software applications that reside between the hardware and the installed operating system, and sometimes behave as an extension of the BIOS. These applications divide the hardware resources (or host) into logical partitions (LPARs) and allocate dedicated or shared slices of these resources to each LPAR. Each VM (or guest) shares the physical resources of the host system. These include the CPU, memory, network interface card (NIC), and storage space. Figure 8 on page 72 illustrates the logical partitioning of hardware resources into virtual devices.

Copyright © 2013, Juniper Networks, Inc.

Figure 8: Virtualized Server



Each VM is assigned a MAC address, is logically connected to virtual ports or switches, and initiates traffic from a virtual NIC. Virtual switches enables VMs on the different hosts to communicate with each other using the same protocols as physical switches. In addition, VMs can be configured with one or more virtual Ethernet adapters, each with its own MAC address and IP address. Virtual networks and virtual machines, therefore, have the same networking capabilities as physical networks built around physical devices.

The increase in the number of virtual switches in the data center presents Data Center (DC) operators with the challenge of having to manage these virtual network resources in addition to their physical networks. Network operators are unable to apply the tools that they currently use for managing the physical infrastructure to managing the virtual infrastructure.

Related Documentation

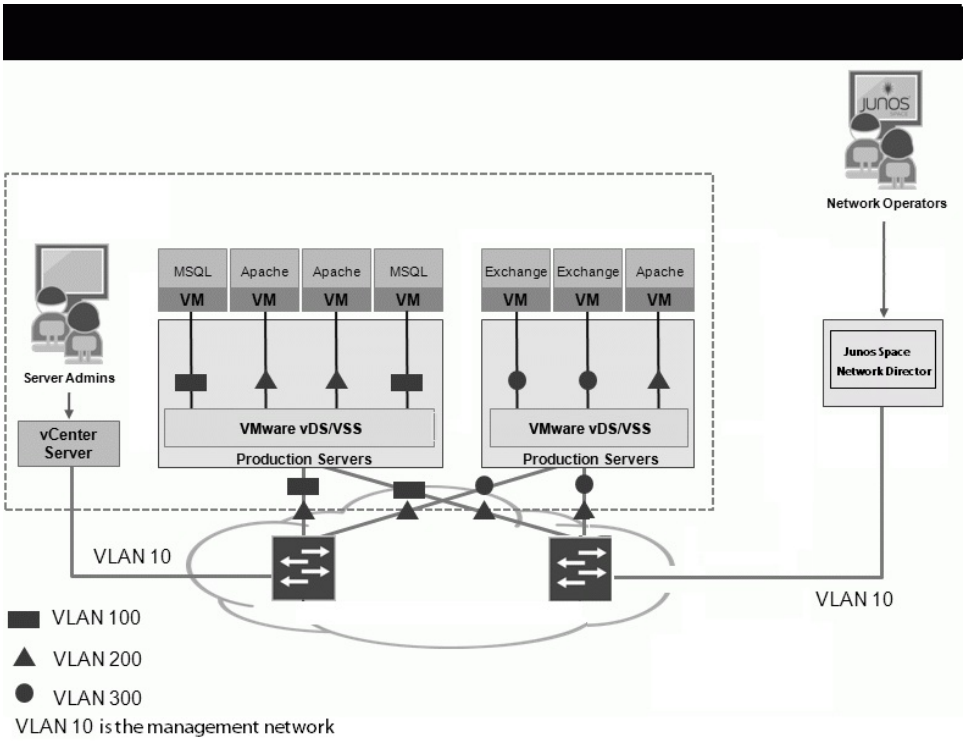
- Understanding Virtual Network Management on page 72

Understanding Virtual Network Management

Network Director unifies the physical, wireless, and virtual networks and provides network operators with a comprehensive view of the complete end-to-end network infrastructure. You can use the Virtual View perspective in Network Director to view and manage virtual networks deployed in virtualized environments in data centers. This ensures that network policies are consistently and automatically applied across physical, wireless, and virtual networks. Figure 9 on page 73 illustrates the virtual machines and physical interfaces in a virtual network.

Copyright © 2013, Juniper Networks, Inc.

Figure 9: Network View of Virtual Machines



Virtual machines residing on a host connect to ports in a virtual switch. Virtual switches, in turn, are associated with port groups that have a fixed number of ports. Ethernet adapters (also called Uplink adapters) connect the virtual environment to the physical network. These elements constitute the inventory of the virtual network.

You can use Network Director to discover and monitor the virtual resources in your virtual environment. Network Director also provides consistent orchestration and operation of the physical and virtual components of the environment.

Network Director enables you to use the services and functionality of other Junos Space applications to manage and monitor the virtual network just as you would do with a physical network.

Related Documentation

- Discovering Devices in a Virtual Network on page 430
- Managing Virtual Networks on page 434
- Viewing the Virtual Switch Inventory in a Virtual Network on page 438
- Viewing the Host Inventory in a Virtual Network on page 439
- Managing Network Adapter Associations on page 440
- Viewing Connections Between Virtual Machines and a Physical Switch on page 443
- Guidelines for Migrating from Virtual Control to Network Director on page 430

Copyright © 2013, Juniper Networks, Inc.

Understanding the Build Mode Tasks Pane for Virtual View

The Tasks pane in Build mode contains all the tasks you can do in Build mode. Click a specific task to begin that task.

Network Director enables you to perform the following tasks for devices in your virtual network:

- **Virtual Networks Management**—You can discover and manage devices that are part of your virtual network using the tasks listed in this section. Table 16 on page 74 describes the virtual network management tasks.
- **Inventory**—View and manage the inventory of virtual centers, hosts, and virtual switches that are part of your virtual network. You can also view the port groups that are associated with each virtual switch. Table 17 on page 75 describes the hypervisor host management tasks.
- **Connectivity**—Manage network adapter associations. Table 18 on page 75 describes the connectivity tasks.
- **Key Tasks**—Network Director enables you to group the tasks that you perform frequently and create a list of key tasks. You can add any task from the Tasks pane to the Key Tasks list by selecting a task and clicking the plus (+) sign that appears adjacent to the task.. This feature is available in Task pane irrespective of your current mode, scope, or view.

For more information about Build mode features, see "Understanding Build Mode in Network Director" on page 3.

Tables below describe the tasks that you can perform in the virtual network category, including the scope in the View pane that you must select to access the task.

Table 16: Virtual Networks Management Tasks

Task	Description	Scope
Manage Virtual Networks	Enables you to modify the VMware vCenter login credentials, set the orchestration mode, delete a VMware vCenter server from Network Director, and resynchronize vCenter configuration with Network Director.	View: Virtual Object: Virtual Networks > Virtual Network Management
Discover Virtual Networks	Discovers supported virtual network vCenter servers in the network and brings them under Network Director management. Hosts and virtual switches are discovered when their vCenters are discovered.	View: Virtual Object: Virtual Networks > Virtual Network Management
View Discovery Status	Displays the status of device discovery jobs.	View: Virtual Object: Virtual Networks > Virtual Network Management

Copyright © 2013, Juniper Networks, Inc.

Table 17: Inventory Tasks

Task	Description	Scope
View Virtual Machines	Displays one of the following depending on the scope: • Details of all the virtual machines that are part of your network. • Details of virtual machines that are part of the selected host. You can select a virtual machine and click **Show Connectivity** to view the network connectivity between the virtual machine and the host.	View: Virtual Object: Virtual Networks > Inventory View: Virtual > *vCenter hostname* > Hosts > *host name* Object: Inventory
View Virtual Switches	Displays one of the following depending on the scope: • Details of all the virtual switches that are part of the selected virtual network. • Details of virtual switches that are part of the selected host.	View: Virtual > *vCenter hostname* Object: Virtual Networks > Inventory View: Virtual > *vCenter hostname* > Virtual Switches Object: Inventory
View Hosts	Displays details of all the virtual hosts that are part of the selected virtual network.	View: Virtual > *vCenter hostname* Object: Virtual Networks > Inventory View: Virtual > *vCenter hostname* > Virtual Switches Object: Inventory
View Virtual Port Group	Displays details of port groups defined for a given virtual switch.	View: Virtual > *vCenter hostname* > Virtual Switches > *Switch host name* Object: *Switch hostname* > View Virtual Port Group

Table 18: Connectivity Tasks

Task	Description	Scope
Manage Network Adapter Associations	Enables you to view and manage the connectivity between a virtual host and the physical network objects (network adapter on a physical switch).	View: Virtual > *vCenter hostname* > Hosts > *host name* Object: *hostname* > Host Management
Import Network Adapter Associations	Enables you to import association details, between a virtual host network adapter and the corresponding network adapter on the physical switch, from a CSV file.	View: Virtual Object: Virtual Networks > Virtual Network Management

Related Documentation

- Understanding Virtual Network Management on page 72
- Discovering Devices in a Virtual Network on page 430
- Managing Virtual Networks on page 434
- Viewing the Virtual Switch Inventory in a Virtual Network on page 438
- Viewing the Host Inventory in a Virtual Network on page 439
- Managing Network Adapter Associations on page 440

Copyright © 2013, Juniper Networks, Inc.

Copyright © 2013, Juniper Networks, Inc.

CHAPTER 5

Custom View Overview

- Understanding Custom Groups on page 77

Understanding Custom Groups

Custom group is way of grouping your devices based on your business needs. You can create custom groups and add devices to each custom group. You can manually add devices to a custom group or you can define rules to add devices, that match the rule condition, to the custom group once they are discovered by Network Director. You can view the custom groups and devices that are assigned to each group in the Custom Group view.

A custom group can include devices such as switches, wireless controllers, and access points. Creating custom device groups enables the configuration of multiple devices simultaneously—you can create multiple custom groups and directly associate devices at any level. Up to this point, Custom Groups are the same as selecting related items in the location view tree. What makes Custom Groups special is that you can also configure a custom group to automatically add devices after discovery. You indicate the criteria for additional devices using rules. Custom groups can then be created in a hierarchy up to eight levels deep. Each layer can contain up to 32 peer containers under a single parent container.

- Where is the Custom Group Function Located in Network Director? on page 77
- How Do Custom Group Rules Work? on page 78
- What Happens When I Edit a Custom Group Rule? on page 79
- When Are Rules Executed? on page 79

Where is the Custom Group Function Located in Network Director?

Network Director has different views that you select to see different aspects of your data. You select one of these views at a time from the Select View option in the Network Director banner. The options are Logical View, Location View, Device View, Custom Group View, Virtual View, and Topology View. To create a Custom Group, Network Director must be in Custom Group View. The Custom Group view displays only the top level—My Network—until you create one or more custom groups.

Copyright © 2013, Juniper Networks, Inc.

Once Custom Groups are created, they appear in all views as options for profile assignment—assigning a profile to a Custom Group assigns that profile to all members of the group.

How Do Custom Group Rules Work?

Adding rules to a Custom group consists of creating a three part rule statement, with a rule basis, an operator, and matching criteria. Possible combinations are shown in Table 19 on page 78.

Table 19: Three Options of a Rule Statement

Rule Basis	Operator	Matching Criteria
Device Role	Equals	Access
		Aggregation
		Core
		Unassigned (available only for EX switches for which logical category can be defined)
Device Type	Equals or Not Equals	Access Point
		Qfabric Member
		Qfabric
		Switch
		Virtual Chassis
		Wireless Controller
Serial Number	Equals or Contains	*You provide serial numbers or letters*
SKU or Model	Equals or Contains	*You provide model numbers or letters*
Management IP Address	Equals or Regex	*You provide IP address*
Location	Select a previously configured location: NOTE: For location directions, see "Setting Up the Location View" on page 414. 1. Click *Please Select* 2. From the Select Location window, select a location. 3. Click **OK.**	
Device Role	Equals	*You provide pre-configured device role*

Copyright © 2013, Juniper Networks, Inc.

Table 19: Three Options of a Rule Statement *(continued)*

Rule Basis	Operator	Matching Criteria
Device Type	Equals or Not Equals	Access Point Qfabric Member Qfabric Switch Virtual Chassis Wireless Controller
Firmware Version	Equals or Contains	*You provide a full or partial firmware version for devices.*

What Happens When I Edit a Custom Group Rule?

When you edit a rule, devices that were added to the group but no longer qualify because of the rule edit are not automatically removed from the group. You must remove those devices manually. If more devices are now qualified to join the group because of your rule edit, the devices are added to the group on the next device notification change to the network.

When Are Rules Executed?

The option **Associate devices based on the rules for the custom groups while saving group information** is enabled by default. If the option is disabled, the rule engine will be activated only when there is some change in the device property. When a device property change occurs, rules are processed and devices are added to the group, if the group has a rule for those actions.

Related Documentation

- Creating Custom Groups on page 447

Copyright © 2013, Juniper Networks, Inc.

Copyright © 2013, Juniper Networks, Inc.

CHAPTER 6

Mobility Domain Overview

- Understanding Mobility Domains on page 81

Understanding Mobility Domains

The Mobility Domain is a virtual grouping of Wireless LAN Controllers (WLCs) that enable roaming and maintain user session information to provide for seamless roaming through identity-based networking. It also provide resiliency and scalability. Common configuration is shared dynamically between all members of the cluster and provides a single point of configuration for all members.

A Mobility Domain enables users to roam geographically across the system while maintaining data sessions and VLAN or subnet membership, including IP address, regardless of connectivity to the network backbone. When users move from one area of a building or campus to another, client associations with servers or other resources do not change. When users access a controller in a Mobility Domain, they become members of the VLAN designated through their authorized identity. If a native VLAN is not present on the accessed controller, the controller forms a tunnel to another controller in the Mobility Domain that includes the native VLAN.

In a Mobility Domain, one controller acts as a primary seed device, and distributes information to all other controllers defined in the Mobility Domain. Otherwise, the seed controller operates as any other Mobility Domain member.

The clustering feature between the controllers ensure smooth mobility across an entire wireless network. With clustering, you can create logical groups of controllers and access points, which share network and user information for continuous and uninterrupted support.

Related Documentation

- Creating a Mobility Domain for Wireless LAN Controllers on page 398

Copyright © 2013, Juniper Networks, Inc.

Copyright © 2013, Juniper Networks, Inc.

CHAPTER 7

Additional Wireless Configuration Concepts

- Understanding Access Point Bias for Controllers on page 84
- Understanding Channel Auto-Tuning and Adaptive Channel Planner on Wireless Networks on page 86
- Understanding Automatic Power Tuning for Wireless Radios on page 91
- Understanding Call Admission Control on page 93
- Understanding Distributed Access Point Behavior on a Layer 3 Network on page 94
- Understanding Load Balancing for Wireless Radios on page 97
- Understanding WPA-PSK and WPA2-PSK Authentication on page 98
- Understanding the IEEE 802.11 Standard for Wireless Networks on page 100
- Understanding the Network Terms SSID, BSSID, and ESSID on page 103
- Understanding Voice Clients and Voice Traffic on page 105
- Understanding Wireless Encryption and Ciphers on page 109
- Understanding Wireless Interference on page 112
- Understanding Wireless Radio Channels on page 114
- Understanding Wireless Scanning on page 117
- Understanding WMM Power Save and WLAN Client Battery Life on page 121

Copyright © 2013, Juniper Networks, Inc.

Understanding Access Point Bias for Controllers

In wireless networks, distributed access points can have a bias for different controllers, which means they can have a preference for some controllers. Bias is used only when access points are distributed over the network, not when access points are directly plugged into a configured port on a controller. Bias does not effect the initial controller discovery process performed by the access point. Instead, for distributed access points only, bias is referenced by the controllers and the first controller an access point finds relays the bias settings to an access point.

This topic describes:

- How Do I Determine The Bias Settings I should Use? on page 84
- Example of a Layer 3 Network With Multiple Controllers on page 85
- A Third Option for Access Point Bias - Sticky on page 85
- How Do I Set the Controller Bias for an Access Point? on page 85
- How Can I Determine the Bias of an Access Point By Looking at a Controller? on page 86
- What About Controller Clusters? on page 86

How Do I Determine The Bias Settings I should Use?

Table 20: Configuring Bias on Controllers and Access Points

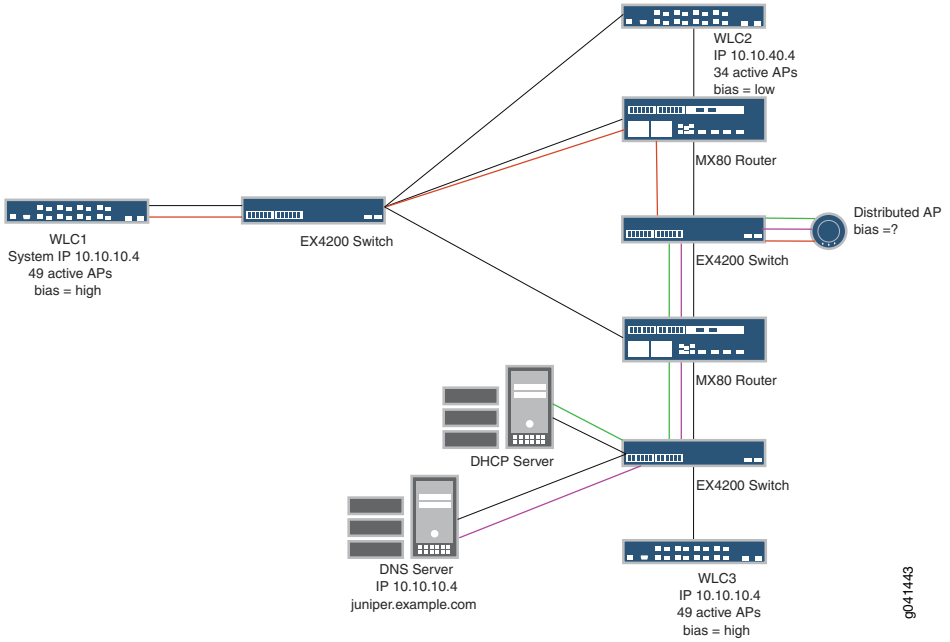
Situation	What You Should Do	Result
Access point is directly wired and connected to a controller. Controller ports are configured as direct attach ports.	Bias settings are ignored in this case. You do not need to configure the access point bias. If you do configure it, that configuration is ignored.	The access point associates directly to the connected controller. An access point always attempts to boot on access point port 1 first, and if a controller is directly attached on access point port 1, the access point boots from there regardless of the bias settings.
There is one controller on the network.	Configure access points as usual. Bias will have no effect since there is only one controller.	Access points will associate to the controller, using one of these methods to discover the controller: static configuration, DHCP option 43, DNS, or subnet directed broadcast.
There are three controllers on the network, set up as shown in Figure 10 on page 85.	In this situation, bias will make a difference. The access point has a high bias for WLC1 and WLC3, and a low bias for WLC2.	Since the controllers are in another subnet, the access points locate a controller and receive the bias settings and the capacity of each controller. Access points are then directed to associate to a high bias controller (WLC1 or WLC3 in this case) if one is available . When the bias for two controllers is the same, as it is in this illustration, the controller with the greatest capacity to add more active access points is selected.

Copyright © 2013, Juniper Networks, Inc.

Example of a Layer 3 Network With Multiple Controllers

This Layer 3 network would make use of bias settings since there are several controllers that access points could associate to.

Figure 10: Controllers With High Bias and Low Bias For an Access Point



A Third Option for Access Point Bias - Sticky

Access points actually have three bias options for controllers, high, low, and sticky. The third option, sticky, means that an access point stays on whatever controller it is associated to, regardless of whether a high bias controller is available or not. Even if a sticky access point is using a low bias controller when a high bias controller becomes available, the sticky access point stays with the low bias controller. The sticky option is useful because it avoids unscheduled access point resets that would normally occur as the access point transitions from one controller to another.

An access point with a sticky bias stays on the controller until an administrator intervenes by resetting the access point to have it discover and connect to a high bias controller.

How Do I Set the Controller Bias for an Access Point?

When you add an access point, you must first select a controller—this controller is the one you are setting the bias for. If you want the access point to be able to use different controllers, you must set the bias for each controller. You would add the access point to each controller following the directions "Adding and Managing an Access Point" on page 126.

Copyright © 2013, Juniper Networks, Inc.

How Can I Determine the Bias of an Access Point By Looking at a Controller?

If an access point is associated with a controller, it appears on the list you see when you click **Wireless Network > View Inventory** (under Device Management) in Network Director. If the access point is using that controller, the Connection field on the controller will indicate Up. If the controller's Connection field indicates Up/Redundant, it means that cluster/network resiliency is enabled. In that case, each access point has a primary link to one controller and a backup/redundant link to another controller. The redundant controller connection is also listed as Up/Redundant.

What About Controller Clusters?

Clusters are a subset of a mobility domain. Clustering creates a logical group of controllers (and their associated access points) that share network and user information for failover support. Every access point in a cluster has a primary access point manager—this can be any controller in the cluster. For more information, see "Creating a Mobility Domain for Wireless LAN Controllers" on page 398.

The concept of bias is superceded in cluster configuration scenarios by automatic redundancy and/or optional access point affinity configuration. Access point affinity is configured per controller in a cluster, so bias has no bearing or effect.

Related Documentation

- Adding and Managing an Access Point on page 126
- Creating a Mobility Domain for Wireless LAN Controllers on page 398
- Understanding Distributed Access Point Behavior on a Layer 3 Network on page 94

Understanding Channel Auto-Tuning and Adaptive Channel Planner on Wireless Networks

Channel auto-tuning automatically makes channel-tuning decisions for access point radios on the basis of the RF data gathered by access points. Channel auto-tuning is configured in a Radio profile in Network Director and operates on all access point radios by default. This topic explains channel automatic tuning.

NOTE: **In the CLI versions 8.0 and later of MSS, channel auto-tuning is no longer part of the Radio profile. The feature is called Adaptive Channel Planner and the new CLI command is set radio-profile auto-tune channel-config.**

This topic describes:

- Why Use Channel Auto-Tuning? on page 87
- When Should I Use Channel Auto-Tuning? on page 87
- How Does Channel Auto-Tuning Work? on page 88
- How Do I Configure Automatic Channel Tuning? on page 89
- What Are The Results of Auto-Tuning? on page 89

Copyright © 2013, Juniper Networks, Inc.

- When is Auto-Tuning Most Beneficial? on page 90
- What Happens when Severe Interference is Detected? on page 90

Why Use Channel Auto-Tuning?

The state of a wireless network is dynamic—to continually tune each access point radio for optimum performance would be time consuming. Auto-tuning performs the following tuning based on feedback from access point scanning:

- Chooses a random starting channel for newly deployed access points
- Automatically tunes channels of access points to minimize co-channel interference
- Mitigates spectral interference

You can specify which channels auto-tuning can choose from.

In addition, auto-tuning maintains tuning configurations across access point and controller reboots. (For more information about scanning, see "Understanding Wireless Scanning" on page 117.

When Should I Use Channel Auto-Tuning?

Channel auto-tuning is beneficial in these situations:

- When you are deploying a new network—no channel configuration exists yet.
- When you add or move access points.
- When the performance of an existing configuration needs improvement.
- When the network is experiencing interference.
- When you need to tune around channels used by radar, if there is weather or military radar operating in your area. Weather radar frequently operates at large commercial airports.
- When interference makes a channel unusable. For example, a continuous wave transmitter, like some video surveillance cameras, will make a channel unusable.

Channel Auto-Tuning to Improve Performance

Auto-tuning optimizes performance—you do not need to make repeated channel changes in a reactive mode. Channel tuning for performance operates best over a regular time frame, such as a day. We recommend that you schedule auto-tuning to collect data over a long period of time, then make changes at a time when only a few users are affected.

The duration of the sample period must match the retuning period so that the algorithm does not generate a reactive response to short term-transients. For example, the whole network should not retune each time a door opens or closes. Instead, it would be better to choose and maintain a tuning that takes into account how much of the time the door is open and closed (average samples over a long period). Changing channels can be disruptive to active clients, so it is best not to do it frequently and at times when service disruptions can be tolerated.

Copyright © 2013, Juniper Networks, Inc.

Channel Auto-Tuning to Resolve Interference

If a channel becomes unusable, the wireless auto-tuning algorithm immediately changes the radio to a working channel but the changes do not persist. The algorithm tries to revert to the configured channel at intervals. This emergency tuning is similar to DFS channel handling.

Channel Auto-Tuning Is Used by Dynamic Frequency Selection to Comply With Country Regulations

If an access point detects radar on a channel it is currently using, regulations require that it cease using the channel immediately. Auto tune enables the radio to be switched to a usable channel rather than taking the radio out of service.

Dynamic Frequency Selection (DFS) requirements apply only to radios operating in the 5-GHz band (802.11a radios). Auto-tuning enables the system to retune channels in the 5-GHz band when radar is detected and regulations require the system to cease using a channel.

When the controller learns that an access point 802.11a radio has detected radar on a channel, the auto-tune module immediately switches the radio to another channel. The event is time stamped along with the state of the channel. For the next 30 minutes, the controller blacklists the radar channel—after this, the channel is automatically added back to the eligible channel list.

NOTE: If radar is detected on a radio with auto-tune channel disabled, the radio goes out of service as required by the Federal Communications Commission (FCC) and European Telecommunications Standards Institute (ETSI).

DFS is configured in a Radio profile—see "Creating and Managing a Radio Profile" on page 315.

How Does Channel Auto-Tuning Work?

The controller evaluates the radios' scanning results for possible channel changes every 3600 seconds (1 hour). An algorithm running as a distributed algorithm on controllers and access points uses the following parameters to determine whether to change the channel on a radio:

- Amount of noise on the channel
- Packet retransmission count—see *Monitoring the Percentage of RF Packet Retransmissions* for more information.
- Utilization calculated on the number of multicast packets per second that a radio can send on a channel while continuously sending fixed-size frames over a period of time.

Copyright © 2013, Juniper Networks, Inc.

- Phy error count, which is the number of frames received by the radio with physical layer errors. A high number of Phy errors can indicate the presence of a non-802.11 device using the same RF spectrum.
- Received CRC error count. A high number of CRC errors can indicate a hidden node or co-channel interference.

The thresholds for these parameters are not configurable. RF auto tuning also can change a radio channel when the channel tuning interval expires, if a channel with less disturbance is detected. Disturbance is based on the number of neighbors the radio has and the RSSI of each neighbor. A radio also can change channels before the channel expires to respond to interference or radar.

How Do I Configure Automatic Channel Tuning?

The automatic channel tuning feature is called Tune Channel and it is configured in the Power & RF Settings tab of Create Radio Profile for controllers—see "Creating and Managing a Radio Profile" on page 315. In addition to disabling and enabling Tune Channel, you can change these settings:

- Tune Transmit Power
- Ignore Clients
- Tune Channel Range (11a)
- Channel Tuning Interval
- Channel Tuning Holddown
- TX Power Backoff Timer
- Power Tuning Interval
- Power Ramp Interval

For descriptions of these settings and directions for creating Radio profiles, including automatic channel tuning, see "Creating and Managing a Radio Profile" on page 315.

What Are The Results of Auto-Tuning?

Because auto-tuning automatically optimizes channels used by an access point, the following results occur:

- Co-channel interference is minimized. Co-channel interference occurs when multiple neighboring radios use the same frequency (channel). Excessive co-channel interference occurs if a poor channel plan is used. Auto-tune channel optimizes the channel plan such that nearby access points avoid using the same channel.
- Spectral interference from non-802.11 devices, such as instruments, microwaves, cordless phones, and surveillance cameras, is mitigated.
- The interference domain is defined. An interference domain is a set of radios in a mobile domain that could interfere with each other. Interference domains are temporary and non-configurable.

Copyright © 2013, Juniper Networks, Inc.

- Tuning is maintained across access point and controller reboots.
- Newly deployed access points are assigned a random starting channel. This also happens at the first invocation. The purpose is to quickly choose a reasonable channel rather than waiting for the tuning algorithm to do its next update. It turns out that just choosing random channels for all radios usually results in a reasonably good tuning. The old method of setting the channel to a single default channel guaranteed that the system started at the worst possible tuning—all radios on the same channel.

NOTE: Keep in mind Bluetooth devices and frequency hopping cordless phones spread their communications over the entire 2.4-GHz frequency band, so it is not possible to avoid them by changing channels. However, they are designed to coexist with other transmitters, so their interference is minimal.

When is Auto-Tuning Most Beneficial?

The most beneficial time to turn on auto-configuration is when you first deploy your wireless network or after you make significant changes to you network or facilities. Turn on auto-configuration of channels when you:

- First deploy your wireless network or after you make significant changes to your network or facilities.
- Deploy new access points that have not had channels configured.
- Add more access points to an existing configuration or move existing access points, for example during a remodel.
- Discover that a neighboring organization deployed or changed a wireless network in close proximity to some of your access points.
- Have reason to believe the current tuning is sub-optimal, for example when users experience poor service in certain locations.

During regular network operation, there is usually no need to retune channels frequently. A working network should be in data collection mode most of the time. It is better to configure channel auto-tune to collect data over a long period of time and then make changes at a time when only a few users are affected. If you do not have a time when disruptions can be tolerated, you might want to run it only occasionally, on demand.

What Happens when Severe Interference is Detected?

Severe interference usually occurs only when something changes in the interference domain. For example, a neighboring company could reconfigure their wireless channels, or a new source of interference, such as a continuously transmitting video surveillance camera, is deployed.

If RF scanning detects severe interference, auto-tuning will immediately choose a new temporary channel assignment to mitigate the problem. Auto-tuning will become active, even if you have configured it to wait. If the interference persists, auto-tune will take it into account the next time it retunes channels. In this case, auto-tuning uses the tuning

Copyright © 2013, Juniper Networks, Inc.

algorithm to change to a usable channel if one is available. Otherwise, the channel will revert back to the previously tuned channel. The difference with auto-tuning done in a crisis is that the emergency changes are not saved, and auto-tuning will periodically try to revert the network to the saved channels. Only changes made by you are saved.

Related Documentation

- Creating and Managing a Radio Profile on page 315
- Understanding Automatic Power Tuning for Wireless Radios on page 91

Understanding Automatic Power Tuning for Wireless Radios

The amount of power an access point uses affects the coverage area of the wireless network. The higher the power level on access points, the larger the coverage area of a wireless network. Usually, you want your wireless network to cover all areas, but with minimal overlap between access points that share the same channel—this minimizes co-channel interference. Configuring each access point radio's power manually can be time consuming and tedious for a large installation. For one thing, in order to ensure complete coverage while minimizing co-channel interference, you need to consider nearby access points sharing the same channel as well as understand signal propagation issues. For example, the walls and windows in your facility affect signals. Instead of manually configuring power, you can configure access points to automatically tune their radios' power based on RF data they collect about neighboring access points. With automatic power tuning, which is configured in the Network Director Radio profile under the Power & RF Settings tab, access points adjust their radios' power levels automatically, based on the power levels of all neighboring access points.

Radios get most configurations, including power tuning, from the associated Radio profile. For directions to create a Network Director Radio profile, see "Creating and Managing a Radio Profile" on page 315.

NOTE: **Automatic channel tuning is also available, and automatic power tuning and channel tuning can be used together. For more information about automatic channel tuning, see** "Understanding Channel Auto-Tuning and Adaptive Channel Planner on Wireless Networks" on page 86.

This topic describes:

- How Does Wireless Transmit Power Work? on page 91
- How Does Power Tuning Work? on page 92
- When is Power Tuning Most Helpful? on page 92
- How Do I Turn Off Power Tuning? on page 92
- What Changes Can I Make to Automatic Power Tuning? on page 92

How Does Wireless Transmit Power Work?

Transmit power, like other sound pressure, is measured in decibels. Because the measurement is logarithmic instead of linear, an increase of 6 dB will double the range

Copyright © 2013, Juniper Networks, Inc.

of coverage of a radio. Valid power values depend on the country of operation. The default transmit power on all access point radio types is either the highest setting allowed for the country of operation or highest setting supported on the hardware, whichever is lower.

How Does Power Tuning Work?

Power tuning computation is performed on the access point itself without any help from the controller. Access points listen for nearby access points on the same channel and then adjust their power to provide good coverage while avoiding co-channel interference.

The power tuning algorithm automatically adjusts to changes when needed, for example when one access point is removed.

Auto-tuned power settings are not persistent—auto-tuning must be enabled for the changes to occur. If you turn off auto-tuning, the access point will go back to the configured power setting.

When is Power Tuning Most Helpful?

When an access point radio is first enabled, automatic power tuning can assign initial power settings compatible with surrounding access points.

How Do I Turn Off Power Tuning?

You turn off power tuning by editing Radio profiles. See "Creating and Managing a Radio Profile" on page 315.

What Changes Can I Make to Automatic Power Tuning?

When power tuning is enabled in a Radio profile, you can change the wireless transmit power backoff timer, power tuning interval and the power ramp interval for that Radio profile.

- *Transmit Power Backoff Timer* changes the interval at which radios reduce power after temporarily increasing the power to maintain the minimum data rate for an associated client. At the end of each power-backoff interval, radios that temporarily increased their power reduce it by 1 dBm every 10 seconds. The power backoff continues in 1 dBm increments after each interval until the power returns to expected setting.
- *Power Tuning Interval* is the number of seconds between reevaluations of power. Power changes can only take place after an evaluation or when an anomaly occurs. You can change the wait interval between evaluations from the default 600 seconds.
- *Power Ramp Interval* is the rate at which power is increased or decreased on radios in a Radio profile until the optimum power level calculated by RF auto-tuning is reached. You can change the 1 dBm increment to increase and decrease in larger or smaller steps.

Related Documentation

- Creating and Managing a Radio Profile on page 315
- Understanding Channel Auto-Tuning and Adaptive Channel Planner on Wireless Networks on page 86

Copyright © 2013, Juniper Networks, Inc.

Understanding Call Admission Control

Call admission control (CAC) regulates the addition of new voice over IP (VoIP) sessions on access point radios, guaranteeing a higher quality of service to a fixed number of voice clients by limiting the number of calls. Call admission control is configured in the WLAN Service profile using either Wi-Fi Multimedia (WMM) or, for older equipment, the legacy SpectraLink Voice Priority (SVP). CAC is used in the call setup step and applies only to real-time media traffic as opposed to data traffic.

NOTE: SVP is a legacy technology—Spectralink's new phones use WMM.

You can turn off call admission control (set it to none), or you can enable either session-based admission control or VoIP-based admission control:

- **None** (default)
- **Session-based:** Session-based call admission control limits the number of sessions (14 by default) on one WLAN Service profile. When used in conjunction with QoS, a small number of clients (0 through 100) are given priority access, while clients on other WLAN Service profiles are forced to use best effort. Configure session-based call admission control when an SSID will handle both data and voice.
- **Voip-call**: Call admission control limits only the number of voice sessions on one WLAN Service profile. VoIP-call is designed to be used with a voice-only Radio profile and SSID.

NOTE: We recommend creating voice-only SSIDs, either WMM VoIP-call or SVP VoIP call, for best performance.

This topic describes:

- What Radios Does Call Admission Control Affect? on page 93
- How Do I Configure Call Admission Control? on page 94

What Radios Does Call Admission Control Affect?

Call admission control is enabled in a WLAN Service profile and affects radios using the Radio profile associated with the WLAN Service profile (SSID).

NOTE: To ensure voice quality, do not map other WLAN Service profiles to a Radio profile you plan to use for dedicated voice traffic or use QoS to force all packets on other WLAN Service profiles to use best-effort priority.

Copyright © 2013, Juniper Networks, Inc.

How Do I Configure Call Admission Control?

Call admission control is enabled in a WLAN Service profile (SSID) and configured in the associated Radio profile.

For information about enabling call admission control, see "Creating and Managing a WLAN Service Profile" on page 350. For information about configuring call admission control, see "Creating and Managing a Radio Profile" on page 315.

Related Documentation

- Creating and Managing a WLAN Service Profile on page 350
- Creating and Managing a Radio Profile on page 315

Understanding Distributed Access Point Behavior on a Layer 3 Network

Access Points can be connected to a wireless network two different ways, either directly to a controller or through a switch. When an access point is connected directly to a controller, operation is straightforward—the access point communicates with the controller by default.

An access point that is connected to a network instead of directly to a controller is referred to as a distributed access point—the operation of a distributed access point is more complex because the access point has to complete a number of steps to find, then connect to, a working controller. This topic describes how a distributed access point boots on a Layer 3 network.

This topic describes:

- What Is a Layer 3 Network? on page 94
- How Does an Access Point Find a Controller on a Layer 3 Network? on page 95

What Is a Layer 3 Network?

Layer 2 networks forward all broadcast traffic so that any broadcast traffic is transmitted. A large Layer 2 network, forwarding all of this data, can suffer from congestion and decreased network efficiency. In contrast, Layer 3 devices restrict broadcast traffic such as ARP and DHCP broadcasts to the local network. This reduces overall traffic levels by allowing administrators to segment networks into subnetworks and restrict broadcasts to that subnetwork. This means there is a limit to the size of a Layer 2 network, but a Layer 3 network, properly configured, can grow to any size.

This explanation uses the following hardware components to form a typical Layer 3 network:

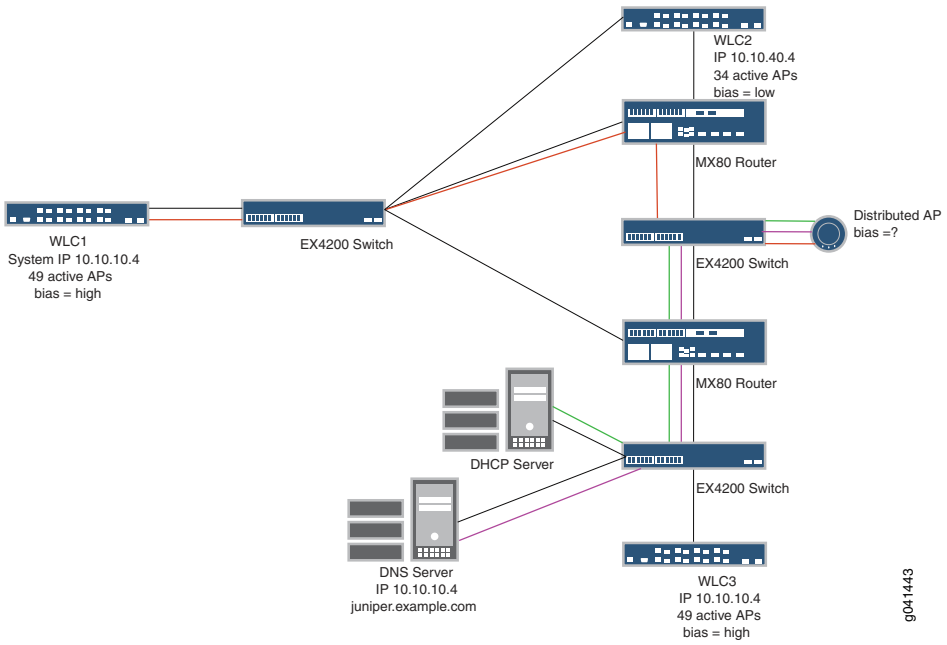
- One DHCP server
- One DNS server
- Two routers
- Two switches

Copyright © 2013, Juniper Networks, Inc.

- Three controllers
- One access point set to Distributed Connection and High Bias for controller1 and controller3. The access point is set to low bias for controller2. For more information about bias, see "Understanding Access Point Bias for Controllers" on page 84.

Figure 11 on page 95 illustrates this network topology. As you can see, the access point is in a different subnet than the controllers, so the access point must negotiate its way to one of the controllers. In this case, the access point must also select one of three available controllers using the bias settings on the access point and controllers.

Figure 11: Access Point Booting Over a Layer 3 Network



How Does an Access Point Find a Controller on a Layer 3 Network?

In a Layer 3 network, a distributed access point behaves as described in Table 21 on page 96. Interactions are color coded as indicated in the table. Interaction begins with the first action in the table (access point sends a discover message to the DHCP server) and ends with a list of SSIDs on the access point.

Copyright © 2013, Juniper Networks, Inc.

Table 21: Access Point Connecting to a Controller in a Layer 3 Network

Access Point Action	Response	Color of Route in Figure
Access point sends a discover message from port 1 on the access point to the DHCP server.	DHCP server replies with a DHCP offer message containing: • IP address for the access point • Default router IP address for the access point IP subnet • DNS server address • Domain name NOTE: DHCP can optionally provide Option 43 information to the access point, which specifies controller information directly without need for the DNS step.	green
Access point sends a DHCP request message to the DHCP server.	DHCP server sends an ACK to the access point.	green
Access point sends a broadcast find controller message to the IP subnet broadcast address. When the access point is unable to locate an controller on the subnet connected to it, the access point sends a DNS request for wlan-switch.	The DNS server sends the system IP address of the controller mapped to wlan-switch. DNS returns controller1 in this example.	purple
Access point sends a unicast find controller message to controller1.	Controller1 receives the find controller message and compares the bias settings on each controller. More than one controller has a high bias for this access point, therefore controller1 selects the controller with the greatest capacity to add new active access point connections. In this example, controller1 has more capacity. Controller1 sends its own IP address to the access point in the find controller reply message.	orange
Access point contacts controller1 and determines whether to use a locally stored operational image or download an image from the controller.	Controller1 sends an access point image if requested.	orange
Once the operational image is loaded, the access point requests configuration information from controller1.	Controller1 sends SSID information to the access point.	orange

Related Documentation

- Mobility System Software Quick Start Guide, *Preparing the Network for Distributed APs*
- Mobility System Software Quick Start Guide, *Using the Quickstart Command.*
- Adding and Managing an Access Point on page 126
- Understanding Access Point Bias for Controllers on page 84

Copyright © 2013, Juniper Networks, Inc.

Understanding Load Balancing for Wireless Radios

Load balancing distributes a workload across multiple wireless radios to achieve optimal utilization, maximize throughput, minimize response time, and avoid overload.

RF load balancing for access points has the ability to reduce network congestion over an area by distributing client sessions across access point radios with overlapping coverage. With load balancing, you can ensure that all access points on the network handle a proportionate share of wireless traffic, and that no single access point gets overloaded. Load balancing of access points is enabled by default in WLAN Service profiles—that means that all access points using a WLAN Service profile are load balanced.

This topic describes:

- Why Would I Need Load Balancing? on page 97
- When Would I Avoid Load Balancing? on page 97
- How Load Balancing Works on page 97
- Where Do I Configure Load Balancing? on page 98

Why Would I Need Load Balancing?

As new clients arrive, load balancing distributes the clients among access points such that the access points share the client load. The wireless operating system, MSS, encourages clients to associate with the least loaded (by client count) access point, so that clients are well distributed across access points. This way, no one access point is more overloaded and there is less interruption of wireless services on the network. For example, in an auditorium or lecture hall, there might be a large number of clients in a relatively small amount of space. While a single access point might be sufficient for providing an RF signal to the entire area, more access points might be required to deliver enough aggregate bandwidth for all of the clients. When additional access points are installed in the room, RF load balancing spreads clients evenly across the access points, increasing the available aggregate bandwidth by increasing the number of access points. Without load balancing, you could still have two access points in a classroom, but all clients have associated to just one access point.

When Would I Avoid Load Balancing?

We do not recommend load balancing for low-latency applications such as voice or live-streaming (unbuffered) video. Load balancing is not advisable for voice transmission because load balancing can impact roam times, which can impact voice quality for roaming clients. Load balancing can also make streaming video jittery with dropped frames.

How Load Balancing Works

The wireless operating system, MSS, balances the client load by adjusting how access points are perceived by clients advertising the same SSID. The capacity of an access point handling new clients is compared to other access points in the SSID. As new clients arrive, MSS encourages them to associate with the least loaded (by client count) access points, such that clients are well distributed across access points. By default, MSS only

Copyright © 2013, Juniper Networks, Inc.

encourages clients to associate with an access point if there are access points available with capacity to accept more clients. Clients are never prevented from associating with an access point if it is the only one available.

Where Do I Configure Load Balancing?

Load balancing is enabled and configured in multiple places for several kinds of load balancing. The load balancing option discussed here applies to wireless access points and radios.

NOTE: **Load balancing configured in Access profiles applies to the RADIUS servers configured within that profile. For details, see** "Creating and Managing Access Profiles" on page 136.

RF load balancing for access points is enabled by default in Juniper WLAN mobility domains, affecting all radios within that domain. You can, however, disable load-balancing in a WLAN Service profile. If you want an WLAN's SSID on access points to be exempt from load balancing, you can indicate that a WLAN Service profile is *Load Balancing Exempt*—see the directions for Network Director "Creating and Managing a WLAN Service Profile" on page 350.

You can also assign a single access point to a specific load balance group when you add that access point to a controller—see "Adding and Managing an Access Point" on page 126.

Related Documentation

- Creating and Managing a WLAN Service Profile on page 350
- Understanding Access Profiles on page 21
- Creating and Managing Access Profiles on page 136

Understanding WPA-PSK and WPA2-PSK Authentication

Pre-Shared Key (PSK) is a client authentication method that uses a plain-English passphrase, containing up to 133 characters, to generate unique encryption keys for each wireless client. PSK is one of two available authentication methods used for WPA and WPA2 encryption on Juniper Networks wireless networks. PSK is not the default authentication method when creating a WLAN Service profile because the other choice, 802.1X authentication, is the both 802.11 standard and is stronger.

NOTE: **802.1X and PSK authentication types can be applied simultaneously—clients will use the most secure option that they are capable of using. For more information about 802.1X authentication, see** "Understanding the IEEE 802.11 Standard for Wireless Networks" on page 100.

This topic describes:

- What are WPA PSK and WPA2 PSK? on page 99
- How Do WPA-PSK and WPA2-PSK Work? on page 99

Copyright © 2013, Juniper Networks, Inc.

- When Would I Use PSK Authentication? on page 99
- Why Would I Not Use PSK Authentication? on page 99
- How Is WPA Encryption Different Than WPA-PSK Encryption? on page 100

What are WPA PSK and WPA2 PSK?

There are two forms of encryption available when using Network Director, Wi-Fi Protected Access (WPA) and the newer WPA2. Pre-shared key (PSK), a shared secret method, can be used with either encryption method:

- WPA/WPA2 Enterprise (requires a RADIUS server) and provides coverage for large entities.
- WPA/WPA2 Personal (also known as WPA-PSK) is appropriate for use in most residential and small business settings.

How Do WPA-PSK and WPA2-PSK Work?

With WPA-PSK, you configure each WLAN node (access points, wireless routers, client adapters, bridges) not with an encryption key, but rather with a plain-English passphrase that contains up to 133 characters. Using a technology called TKIP (Temporal Key Integrity Protocol), that passphrase, along with the network SSID, is used to generate unique encryption keys for each wireless client. Those encryption keys are constantly changed. When clients connect, the WPA-PSK authentication users provide the password to verify whether to allow them access to a network. As long as the passwords match, a client is granted access to the WLAN.

NOTE: **You have the option to encrypt the PSK plain-English passphrase.**

When Would I Use PSK Authentication?

PSK was designed for home and small office networks that do not require the complexity of an 802.1X authentication server. Some reasons to use PSK authentication are:

- PSK is simple to implement, as opposed to 802.1X authentication, which requires a RADIUS server.
- Your legacy clients might not support 802.1X or the latest WPA2 standard.

Why Would I Not Use PSK Authentication?

Even if you have a small company, there are drawbacks to using PSK authentication. For example:

- If an administrator leaves the company, you should reset the PSK key. This can become tiresome and be skipped.
- If one user is compromised, then all users can be hacked.
- PSK cannot perform machine authentication the way that IEEE 802.1X authentication can.

Copyright © 2013, Juniper Networks, Inc.

- Keys tend to become old because they are not dynamically created for users upon login, nor are the keys rotated frequently. You must remember to change the keys and create keys long enough to be a challenge to hackers. PSK is subject to brute force key space search attacks and to dictionary attacks.
- Because WPA2-Personal uses a more advanced encryption type, additional processing power is required to keep the network functioning at full speed. Wireless networks that use legacy hardware for access points and routers can suffer speed reductions when using WPA2-Personal instead of WPA, especially when several users are connected or a large amount of data is moving through the network. Because WPA2-Personal is a newer standard, firmware upgrades can also be required for some hardware that previously used WPA exclusively.

How Is WPA Encryption Different Than WPA-PSK Encryption?

The primary difference between WPA and WPA2-Personal are the encryption ciphers used to secure the network. WPA can use only the encryption cipher Temporal Key Integrity Protocol (TKIP). WPA2-Personal can use TKIP, but because TKIP security keys are less secure, the WPA2 protocol usually uses the Advanced Encryption Standard. AES uses a much more advanced encryption algorithm that cannot be defeated by the tools that overcome TKIP security, making it a much more secure encryption method.

Related Documentation

- Understanding the IEEE 802.11 Standard for Wireless Networks on page 100
- Understanding WLAN Service Profiles on page 52
- Creating and Managing a WLAN Service Profile on page 350

Understanding the IEEE 802.11 Standard for Wireless Networks

The IEEE 802.11 standard consists of a series of technological advances that have been developed over many years. Each new advancement is defined by an amendment to the standard that is identified by a one or two letter suffix to "802.11." The original 802.11 standard allowed up to 2 Mbps on only the 2.4-GHz band. 802.11b added new coding schemes to increase throughput to 6 Mbps. 802.11a added support on the 5-GHz band and Orthogonal Frequency Division Multiplexing (OFDM) coding schemes that increase throughput to 54 Mbps. 802.11g brought OFDM from 802.11a to the 2.4-GHz band. 802.11n added an assortment of high throughput advances to increase throughput roughly 10 times, such that high-end enterprise access points achieve signaling throughputs of 450 Mbps. The emerging 802.11ac standard promises to exceed 1 Gbps of throughput. The individual standards in use now are 802.11a, 802.11b, 802.11g, and 802.11n (which uses a more advanced technology than the others). A new standard, 802.11ac, a new, even faster, standard, is being developed, which is an improvement over 802.11n.

The segment of the radio frequency spectrum used by 802.11 varies between countries.

This topic describes:

- Differences Between 802.11 Standards on page 101
- 802.11 Divides Each Frequency Band into Channels on page 102

 Copyright © 2013, Juniper Networks, Inc.

- What is 802.11i Security? on page 102
- What is 802.1X? on page 102

Differences Between 802.11 Standards

The newer the 802.11 standard, the faster it is and the greater its capacity. Theoretically, the new 802.11ac specification will enable multi-station WLAN throughput of at least 1 gigabit per second. Table 22 on page 101 lists the differences between current 802.11 standards. The draft 802.11ac estimates are given in the last row of the table for comparison.

Table 22: Differences Between 802.11 Protocols

802.11 Protocol	Frequency Band Used	Bandwidth	Data Rate per Stream
n Up to 4 streams of data	2.4 GHz 5 GHz	20 MHz	7.2 mbps 14.4 mbps, 21.7 mbps 28.9 mbps, 43.3 mbps 57.8 mbps, 65 mbps, 72.2 mbps
		40 MHz	15 mbps, 30 mbps, 45 mbps, 60 mbps, 90 mbps, 120 mbps, 135 mbps, 150 mbps
g 1 stream of data	2.4 GHz	20	6, 9, 12, 18, 24, 36, 48, 54
b 1 stream of data	2.4 GHz	20 MHz	1 mbps, 2 mbps, 5.5 mbps, 11 mbps
a 1 stream of data	5 GHz 3.7 GHz	20 MHz	6 mbps, 9 mbps, 12 mbps, 18 mbps, 24 mbps, 36 mbps, 48 mbps, 54 mbps
ac (draft) Up to 8 streams of data	5 GHz	20 MHz 40 MHz 60 MHz 80 MHz	up to 87.6 mbps up to 200 mbps up to 433.3 mbps up to 866.7 mbps

NOTE: 802.11ng and 802.11na are Juniper terminology and not part of the 802.11 standard. It is simply Juniper notation for indicating 802.11n use on the 2.4-GHz band (11ng) or 802.11n use on the 5-GHz band (11na).

Copyright © 2013, Juniper Networks, Inc.

802.11 Divides Each Frequency Band into Channels

802.11 divides each of the frequency bands listed in Table 22 on page 101 into channels.

802.11 divides each frequency band into channels in a different way. For example the 2.4000-2.4835 GHz band is divided into 13 channels spaced 5 MHz apart. Channels 1, 6, and 11 were originally the only non-overlapping channels, but with the newer 802.11g standard there are now four non-overlapping channels—1, 5, 9 and 13. (There are now four because the orthogonal frequency-division multiplexing (OFDM) modulated 802.11g channels are 20 MHz wide.)

NOTE: **Many countries, including US allow use of channels 1 - 11 only.**

The amount of available spectrum for unlicensed use, which varies by country, in the 5-GHz band is much greater, and typical supports many more channels than in the 2.4-GHz band.

Availability of channels is regulated by country and can change. Japan permits the use of 14 channels in the 2.4-GHz band, while other countries such as Spain initially allowed the use of only channels 10 and 11. Europe and Asia now allow channels 1 through 13. North America and some Central and South American countries allow only channels 1 through 11.

What is 802.11i Security?

Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access II (WPA2) are two security standards and security certification programs developed by the Wi-Fi Alliance to address security issues found in Wired Equivalent Privacy (WEP). Where WPA encryption was specifically designed to work with some wireless devices that support WEP, while WPA2 encryption does not work on any device that supports only WEP. For more information about encryption, see "Understanding Wireless Encryption and Ciphers" on page 109.

What is 802.1X?

802.1X is an authentication protocol supported by the 802.11 standards that enables mobile devices to be authenticated by username and password or by various types of credentials such as an X.509 certificate, or SIM in cellular phones. 802.1X authentication works in conjunction with an AAA server (typically RADIUS) that provides centralized authentication and user management.

Related Documentation

- Understanding Wireless Encryption and Ciphers on page 109
- Creating and Managing Authentication Profiles on page 157
- Understanding Authentication Profiles on page 22

Copyright © 2013, Juniper Networks, Inc.

Understanding the Network Terms SSID, BSSID, and ESSID

The terms BSSID, ESSID, and SSID are all used to describe sections of a wireless network (WLAN)—the three terms have slightly different meanings. As a wireless user you are concerned only with the broadcast SSIDs that let you connect to a wireless network. As an administrator, you also need to keep track of BSSIDs and, to a lesser degree, ESSIDs.

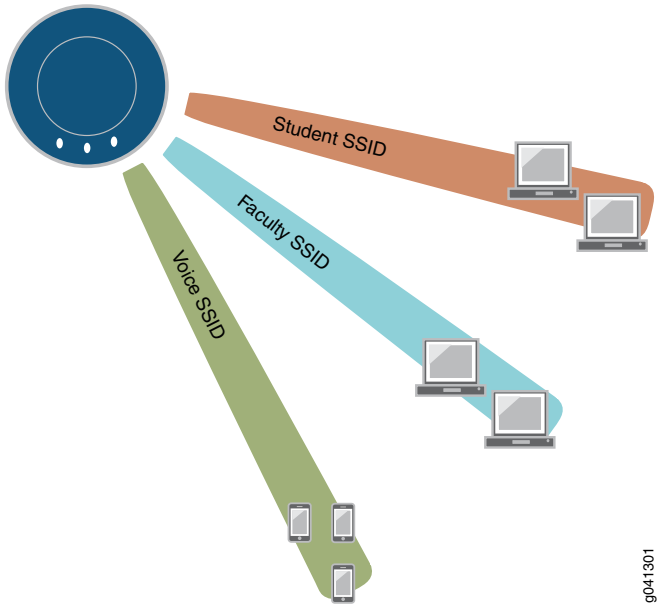
This topic describes:

- An SSID is the Name of a Network on page 103
- BSSIDs Identify Access Points and Their Clients on page 104
- An ESS Consists of BSSs on page 105

An SSID is the Name of a Network

Because multiple WLANs can coexist in one airspace, each WLAN needs a unique name—this name is the service set ID (SSID) of the network. Your wireless device can see the SSIDs for all available networks—therefore, when you click a wireless icon, the SSIDs recognized by device are listed. For example, suppose your wireless list consists of three SSIDs named Student, Faculty, and Voice. This means that an administrator has created three WLAN Service profiles and, as part of each WLAN service profile, provided the SSID name Student, Faculty, or Voice. (For directions to create a WLAN Service profile, see "Creating and Managing a WLAN Service Profile" on page 350.)

Figure 12: Radios can have up to 32 SSIDs



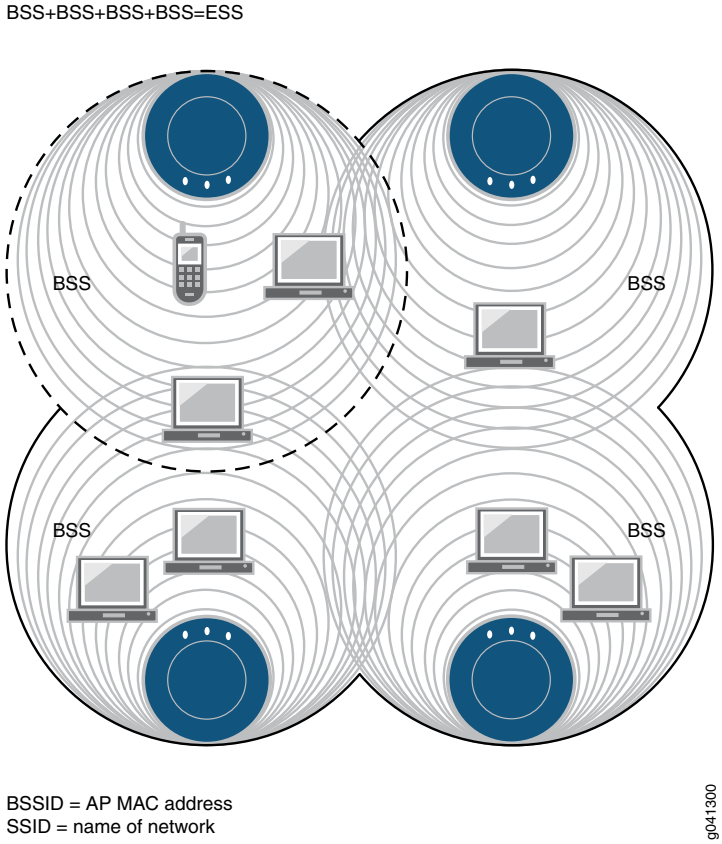
As a WLAN user, you are concerned only with the SSIDs. You select one from the list on your laptop or other device, provide your username and a password, and use the SSID. You might not have access to all SSIDs—the authentication and access privileges are usually different for different WLANs and their associated SSIDs.

Copyright © 2013, Juniper Networks, Inc.

BSSIDs Identify Access Points and Their Clients

Packets bound for devices within the WLAN need to go to the correct destination. The SSID keeps the packets within the correct WLAN, even when overlapping WLANs are present. However, there are usually multiple access points within each WLAN, and there has to be a way to identify those access points and their associated clients. This identifier is called a basic service set identifier (BSSID) and is included in all wireless packets.

Figure 13: Each Access Point Has Its Own BSS



As a user, you are usually unaware of which basic service set (BSS) you currently belong to. When you physically move your laptop from one room to another, the BSS you use could change because you moved from the area covered by one access point to the area covered by another access point, but this does not affect the connectivity of your laptop.

As an administrator, you are interested in the activity within each BSS. This tells you what areas of the network might be overloaded, and it helps you locate a particular client. By convention, an access point's MAC address is used as the ID of a BSS (BSSID). Therefore, if you know the MAC address, you know the BSSID—and, because all packets contain the originator's BSSID, you can trace a packet. This works fine for an access point with one radio and one WLAN configured.

Copyright © 2013, Juniper Networks, Inc.

Most often, there are different BSSIDs on an access point for each WLAN configured on a radio. If you have an access point with 2 radios and 32 WLANs configured on each, you would have 64 BSSIDs plus the base access point BSSID. To accommodate the multiple BSSIDs, each access point is assigned a unique block of 64 MAC addresses. Each radio has 32 MAC addresses and supports up to 32 service set identifiers (SSIDs), with one MAC address assigned to each SSID as a basic service set identification (BSSID). All MAC addresses for an access point are assigned based on the base MAC address of the access point.

NOTE: **The access point MAC address block is listed on a label on the back of the access point.**

To view a list of SSIDs for a network, look at the list of WLAN Service Profiles in Network Director.

Ad-Hoc Networks Do Not Have a MAC Address

Every BSS needs a BSSID, and using the access point's MAC address works fine most of the time. However, an ad-hoc network, a network that forwards traffic from node to node, has no access point. When a BSS does not have a physical access point, in an ad-hoc network for example, the network generates a 48-bit string of numbers that looks and functions just like a MAC address, and that BSSID goes in every packet.

An ESS Consists of BSSs

An extended basic service set (ESS) consists of all of the BSSs in the network. For all practical purposes, the ESSID identifies the same network as the SSID does. The term SSID is used most often.

Related Documentation

- Creating and Managing a WLAN Service Profile on page 350

Understanding Voice Clients and Voice Traffic

Voice, like all other information, travels in packets over IP networks with fixed maximum capacity. The major difference between voice and data traffic is the fact that data packets can be re-sent if they are dropped, and then applied to the empty spots in data, thereby producing complete information. With voice, there is no point in resending packets because voice only makes sense in a stream of contiguous packets. Because resending voice packets is not an option with voice over IP (VoIP), voice traffic must be more carefully configured.

This topic applies to the transmission of voice, multimedia sessions, and video, which are all part of VoIP.

This topic describes:

- What is Voice Over IP? on page 106
- How is Voice Traffic Different Than Data Traffic? on page 106

Copyright © 2013, Juniper Networks, Inc.

- What Protocols are Used for Voice? on page 107
- What is Different About Configuring For Voice Traffic? on page 107

What is Voice Over IP?

VoIP refers to the communication protocols, technologies, methodologies, and transmission techniques involved in the delivery of voice communications and multimedia sessions over Internet Protocol (IP) networks. VoIP systems use session control protocols to control the setup and tear-down of calls as well as audio codecs that encode speech, allowing transmission over an IP network as digital audio using an audio stream.

Voice over Wireless Phones

A VoWiFi phone is similar to a cell phone except that the radio is an 802.11 radio instead of a cellular radio. VoWiFi phones are 802.11 client stations that communicate through an access point.

VoIP is also available on smart phones and Internet devices, making it possible for users of portable devices that are not phones to place calls or send text messages over 3G, 4G, or Wi-Fi.

Private Branch Exchange (PBX)

Private Branch Exchanges (PBXs) are telephone exchanges that serve a particular business or office. The PBX makes the connections for internal phone calls and provides a way to dial out to the public network.

How is Voice Traffic Different Than Data Traffic?

Voice transmission has different issues than data transmission because voice traffic cannot be re-sent if it is lost. Three unique problems that affect call quality are latency, jitter, and packet loss.

In addition, voice traffic can have roaming issues because people are more apt to walk around with phones.

Latency, Jitter, and Packet Loss Affect Voice Traffic

Latency, or delay, is the amount of time it takes the sound of your voice to reach the ear of the other person. Maximum acceptable latency limits for VoIP are 150-200 ms, depending on your call quality requirements.

Jitter is the variation in delay between packets. The jitter buffer holds packets so that they are received at consistent intervals. Significant jitter might cause the jitter buffer to increase to the point that delay reaches unacceptable levels.

Packet loss occurs when the maximum delay specified in the jitter buffer is exceeded. Packet loss above 5% is considered unacceptable when using the G.711 codec.

Voice Traffic is Susceptible to Roaming Issues

A key advantage of voice over WLAN is mobility, but voice roaming is potentially incompatible with 802.11i. In accordance with 802.11i, users traversing a network negotiate

Copyright © 2013, Juniper Networks, Inc.

new encryption keys with every access point they encounter. If this does not happen quickly enough, voice quality is affected.

The 802.11i fast roaming specification eliminates delays associated with re-authenticating roaming clients. Instead of generating a new encryption key with each access point, the VoIP client can use the same key because the pairwise master keys (PMKs) used are cached at the controller.

What Protocols are Used for Voice?

Voice solutions require two types of protocol. Signaling protocols are used during call setup, management and teardown. These protocols generally require low bandwidth, might use a connection-oriented model (TCP), and are typically not delay sensitive. Bearer protocols actually carry the stream of voice samples. Bearer protocols are delay sensitive, are connectionless (UDP) and require special treatment to ensure prioritization over other types of traffic. A separate stream is usually required in each direction. Spectralink Radio Priority (SRP) is a legacy bearer protocol that you can configure.

What is Different About Configuring For Voice Traffic?

Voice traffic needs more bandwidth than data traffic, and that bandwidth needs to be protected so it remains constant and prevents degradation. For these reasons, voice traffic works best when the WLAN Service profile (SSID) and Radio profile used are dedicated to and designed for voice traffic. We recommend that you separate voice and data by SSID and preferably by RF band. Also, be sure to ensure adequate coverage at -60 dBm to -70 dBm level and capacity for the expected voice load.

To optimize voice, also follow these suggestions:

- Consider Using Call Admission Control (CAC) to Limit Clients Per Access Point on page 107
- Ensure That Network Equipment Supports Seamless Roaming on page 108
- Support Quality of Service on all Hardware Used for Voice on page 108
- Use Automatic Power Save Delivery to Preserve the Battery Life of Phones on page 108
- Create a Unique WLAN Service Profile for Voice on page 108
- Create a Unique Radio Profile for Voice on page 108

Consider Using Call Admission Control (CAC) to Limit Clients Per Access Point

Call admission control, configured in the WLAN Service profile, limits the number of concurrent phone calls. Some VoIP devices use Wi-Fi Multimedia (WMM) to provide call admission control for voice clients and some devices use Spectralink voice protocol SVP to provide call admission control for voice clients. Both methods work—which one you use is dictated by your voice clients. The only difference between WMM and SVP is that SVP gives highest priority to Spectralink traffic and WMM does not. If your network has both WMM (most common) and Spectralink voice devices, we suggest that you provide a dedicated SSID for each type.

Copyright © 2013, Juniper Networks, Inc.

Ensure That Network Equipment Supports Seamless Roaming

Voice traffic must use seamless roaming so no call is interrupted. You can achieve seamless roaming with:

- At least 20% overlap between access points
- Between -60 dBm and -70 dBm signal strength wherever voice is required
- Roaming achieved within 50 ms
- Minimized number of router hops between the handsets and the PBX

Support Quality of Service on all Hardware Used for Voice

QoS should be supported end-to-end with voice traffic. Ensure that infrastructure switches and routers support and preserve data prioritization across the full path of any voice streams.

Use Automatic Power Save Delivery to Preserve the Battery Life of Phones

Handset battery life is a major problem. Unscheduled–using Automatic Power Save Delivery (U-APSD) provides dramatic improvements in battery life, for example, from 2 hours talk time to over 10 hours.

NOTE: **Handsets that support WMM/802.11e are increasingly available.**

Create a Unique WLAN Service Profile for Voice

Create a unique WLAN profile for voice—see "Creating a WLAN Service Profile Dedicated to Voice" on page 134 and "Configuring a Voice SSID with Network Director" on page 133.

Create a Unique Radio Profile for Voice

Create a unique Radio profile for voice—see "Creating a Radio Profile for Voice Clients Only" on page 329.

Related Documentation

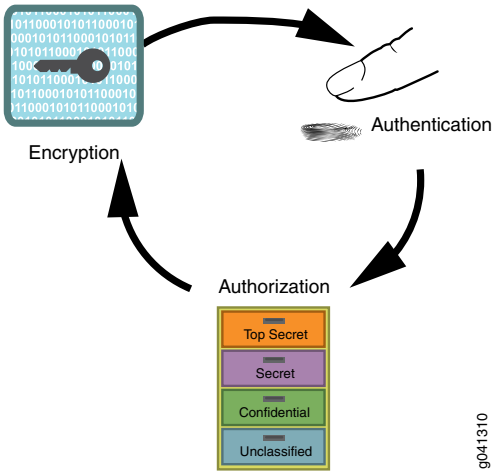
- Configuring a Voice SSID with Network Director on page 133
- Creating a WLAN Service Profile Dedicated to Voice on page 134
- Creating a Radio Profile for Voice Clients Only on page 329

Copyright © 2013, Juniper Networks, Inc.

Understanding Wireless Encryption and Ciphers

Wireless network security relies on a combination of encryption, authentication, and authorization to provide maximum protection for a WLAN. Encryption is focused on protecting the information within a session, reading information in a data stream and altering it to make it unreadable to users outside the network. This topic discusses encryption.

Figure 14: Network Security is Provided by Encryption, Authentication and Authorization



Juniper access points support two standard types of wireless access point-client encryption, Wi-Fi Protected Access (WPA) and WPA2 (also called RSN). Encryption for these two encryption types is configured in WLAN Service profiles under the Security Settings tab. For information about applying encryption, see "Creating and Managing a WLAN Service Profile" on page 350.

NOTE: **You can still configure the legacy encryption, WEP, with the MSS CLI.**

This topic describes:

- Wired Equivalent Privacy (WEP) Was the Original Wireless Encryption on page 109
- WPA Encryption Replaced WEP on page 110
- WPA2 is the Strongest Encryption Available on page 110
- Security Ciphers For WPA and WPA2 on page 110
- Which Encryption Method Should I Use? on page 111

Wired Equivalent Privacy (WEP) Was the Original Wireless Encryption

WEP was the original security algorithm for IEEE 802.11 wireless networks, introduced as part of the original 802.11 standard. Juniper access points support WEP, but you cannot

Copyright © 2013, Juniper Networks, Inc.

configure WEP using Network Director—you must use the CLI. Network Director can configure the stronger encryption schemes, WPA and WPA2.

WPA Encryption Replaced WEP

WPA addressed the vulnerabilities of WEP, the original, less secure 40 or 104-bit encryption scheme in the IEEE 802.11 standard. WPA also provides user authentication—WEP lacks any means of authentication.

WPA replaced WEP with a stronger encryption technology called Temporal Key Integrity Protocol (TKIP) with Message Integrity Check (MIC). It also provides a scheme of mutual authentication using either IEEE 802.1X/Extensible Authentication Protocol (EAP) authentication or pre-shared key (PSK) technology.

NOTE: **You can simultaneously apply both WPA and WPA2 to an SSID. Clients use WPA2 if they have the capability—otherwise the client uses WPA. WPA2 is recommended unless you need to provide access to for legacy devices. All 802.11n devices support WPA2.**

WPA2 is the Strongest Encryption Available

WPA2 is the certified version of the full IEEE 802.11i specification. Like WPA, WPA2 supports either IEEE 802.1X/EAP authentication or PSK technology. It also includes a new advanced encryption mechanism using the Counter-Mode/CBC-MAC Protocol (CCMP) called the Advanced Encryption Standard (AES).

WPA was based on the 802.11i draft, while WPA2 is based on 802.11i final standard. Where WPA encryption was specifically designed to work with some wireless hardware that supported WEP, WPA2 offers stronger security but is not supported by earlier hardware designed for WEP.

NOTE: **The Wi-Fi Alliance requires that high-throughput (802.11n) transmissions use WPA2 and CCMP. You can simultaneously apply both WPA and WPA2 to an SSID. Clients use WPA2 if they have the capability—otherwise the client uses WPA.**

Security Ciphers For WPA and WPA2

Standard security ciphers are part of both WPA and WPA2 encryption. You choose whether you want to apply either the newer CCMP (with WPA2), TKIP (with WPA), or both for each WLAN Service profile. Both cipher suites dynamically generate unique session keys for each session and periodically changes the keys to reduce the likelihood of a network intruder intercepting enough frames to decode a key. The two available ciphers are:

- *Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP)*—CCMP provides Advanced Encryption Standard (AES) data encryption for

Copyright © 2013, Juniper Networks, Inc.

WPA and WPA2. To provide message integrity, CCMP also uses the Cipher Block Chaining Message Authentication Code (CBC-MAC).

A radio using WPA/WPA2 with CCMP encrypts traffic for only WPA CCMP clients but not for TKIP clients. The radio disassociates from TKIP clients unless you selected both CCMP and TKIP.

NOTE: The Wi-Fi Alliance requires that high-throughput (802.11n) transmissions use WPA2 and CCMP.

- *Temporal Key Integrity Protocol (TKIP)*—TKIP uses the RC4 encryption algorithm, a 128-bit encryption key, a 48-bit initialization vector (IV), and a message integrity code (MIC). A radio using WPA/WPA2 with TKIP encrypts traffic for only WPA TKIP clients but not for CCMP clients. The radio disassociates from CCMP clients unless you selected both CCMP and TKIP.

NOTE: TKIP is not permitted for 802.11n-based transmissions. It is only supported for legacy (802.11b, 802.11g and 802.11a) transmissions, which are limited to a maximum of 54 Mbps.

Which Encryption Method Should I Use?

WPA2 is the most secure encryption method available for wireless networks—we recommend using WPA2 with the CCMP cipher whenever possible. WPA2 with CCMP is the only option permitted for high throughput 802.11n transmissions.

If you need to accommodate legacy devices with an SSID, enable WPA encryption with the TKIP cipher. Keep in mind that this has an effect on performance.

NOTE: You can create different WLAN Service profiles (SSIDs) for different levels of encryption. This maximizes the use of WPA2 security.

Related Documentation

- Creating and Managing a WLAN Service Profile on page 350

Copyright © 2013, Juniper Networks, Inc.

Understanding Wireless Interference

Wi-Fi interference is a common and troublesome issue. The lack of wires that makes WLAN so attractive is also the feature that makes other consumer devices capable of causing Wi-Fi interference. Your WLAN network might be working fine one day and sluggish the next day, without you having made any network changes, all due to interference.

This topic describes:

- What Causes Wireless Radio Frequency Interference? on page 112
- Effects of Interference Seen By Clients on page 113
- You Can Monitor RF Interference With Network Director on page 113
- What is RF Jamming? on page 113

What Causes Wireless Radio Frequency Interference?

Because the air is shared by all transmitters, transmissions by any device at the same frequency as an access point's radio can cause interference. Because 802.11 wireless networks operate in unlicensed bands used by many technologies, such as microwave ovens, video surveillance cameras, cordless phones, they are subject to interference. In addition, wireless access points sharing the same channel might interfere with each other. The effect of interference is highly dependent on the strength of the transmission and the distance from the interferer. Access points closest to and on the same channel as an interferer will be affected more than those that are further away.

These are some common causes of wireless interference:

- Leaving the channel number on each radio set to the default value can result in high interference among the radios because too many radios are sharing the bandwidth on one channel.
- Hidden nodes in a wireless network referring to nodes that are out of range of other nodes or a collection of nodes. A hidden node can generate a high number of cyclic redundancy check (CRC) code errors.
- Co-channel interference or adjacent channel interference can result from setting radios to bands that have overlapping channels. The channels might not all be in use by your network—neighboring company signals can also cause interference.
- Some non-network devices, such as microwave ovens, car alarms, cordless phones, or wireless video cameras can interfere with wireless channels. Most often, these devices are using the 2.4-GHz frequency.
- Bad electrical connections can cause broad RF spectrum emissions.
- RF jamming is a deliberate attempt to disrupt the network with a powerful signal.

Copyright © 2013, Juniper Networks, Inc.

Effects of Interference Seen By Clients

Your network clients might notice the results of interference before you do. They might complain of network slowdown, but not of data loss. This slowdown might not be immediately obvious with low capacity data transmission because, if interference is intermittent, packets eventually get through. Therefore, there is no packet loss, just retransmissions that take time. Another possibility is that some devices, such as microwaves, reduce throughput without blocking it entirely. Complaints will increase when more users log on, increasing data capacity until data loss occurs, or when Voice Over IP calls are placed. VoIP requires significant bandwidth because resending voice is not an option—the result is dropped or jittery voice transmission.

You Can Monitor RF Interference With Network Director

Network Director includes a Monitor Mode that displays the compiled RF data gathered by scanning the mobility domain of your network. There are two monitors that indicate network interference for access points and radios:

- AP Interference Sources—On this chart, interference sources for each radio or each access point (either one can be selected) are sorted into categories such as Microwave Oven, Phone FHSS, and Continuous Wave. The occurrences of each source are tracked and added—the sum appears on a bar chart. The categories with the tallest bars are those causing the most interference on this radio or access point, but the sum of all interference is what really matters. For more information, see *Monitoring RF Interference Sources on Wireless Devices*.
- Radio Interference Sources—The pie chart for radio interference is also sorted into categories such as Microwave Oven, Phone FHSS, and Continuous Wave. In addition, a list of details are provided about each source of interference—time last seen, transmitter ID, listener MAC address of the access point that found the interference, channel, RSSI, duty cycle, and percentage of compliance to the common information model (CIM). For more information, see *Monitoring RF Interference Sources on One Radio*.
- RF Interference For Radios on One Access Point—The bar chart that displays each radio on an access point lets you compare the interference experienced on two radios when the access point has dual radios. With single radio access points, you see the same data as you do for the radio interference pie chart, but in bar chart format. For more information, see *Monitoring RF Interference Sources For Radios on One Access Point*.

What is RF Jamming?

RF jamming is a DoS attack. The goal of RF jamming is to take down an entire WLAN by overwhelming the radio environment with high-power noise. A symptom of an RF jamming attack is excessive interference. If an access point radio detects excessive interference on a channel, and channel auto-tuning is enabled, the radio changes to a different channel. The radio continues to scan on an active data channel and on other channels and reports the results to the controller.

Copyright © 2013, Juniper Networks, Inc.

Jamming occurs at the physical layer of the network, saturating the channel or band with noise and making it difficult or impossible for a receiving radio to detect a real transmission. Think of jamming as trying to hear someone talking as a siren goes off. The increased noise floor results in a poor signal-to-noise ratio (SNR), usually detected by the clients as poor signal quality. Jamming can also be detected by an access point, which then triggers dynamic temporary tuning of the channel if automatic channeling is enabled. However, selecting a different channel does not always stop jamming. An experienced attacker will often use all available channels in the attack.

Related Documentation

- *Monitoring RF Interference Sources on Wireless Devices*
- *Monitoring RF Interference Sources on One Radio*
- *Monitoring RF Interference Sources For Radios on One Access Point*
- *Troubleshooting Excessive Wireless Interference*

Understanding Wireless Radio Channels

Each wireless radio operates on a configured radio frequency (RF) channel identified by numbers. A radio assigned to a particular channel both transmits and receives all traffic on that channel.

Depending upon the network configuration, some channels might have less interference than others. Choosing the right channel lets you optimize performance.

This topic describes:

- What WLAN Channels Are Available? on page 114
- What Channels Are Not Available? on page 115
- How Do I Know Which Channels I Should Use? on page 115
- How Do I Avoid Co-Channel Interference? on page 116
- DFS Channels on page 116
- 802.11n Channels Can Be Wider and Work on Both Bands on page 116
- How Are Channel Numbers Assigned? on page 117
- How Do I know What Channel an Access Point is Using? on page 117

What WLAN Channels Are Available?

There are 14 channels designated for wireless networks in the 2.4-GHz frequency band and 42 channels in the 5-GHz frequency band.

The 14 channels in the 2.4-GHz band are spaced 5 MHz apart. The protocol requires 25 MHz of channel separation, meaning that it is possible for adjacent channels to overlap and then interfere with each other. For this reason, only channels 1, 6, 11 are typically used in the US to avoid interference. In the rest of the world, the four channels 1, 5, 9, 13 are typically recommended. The 2.4-GHz frequency band is heavily used because most devices can operate on that band.

Copyright © 2013, Juniper Networks, Inc.

The 5-GHz band is actually four frequency bands: 5.1 GHz, 5.3 GHz, 5.4 GHz, and 5.8 GHz. The 5-GHz band has a total of 24 channels with 20- MHz bandwidth available. Unlike the 2.4-GHz band, the channels are non-overlapping, therefore all channels have the potential to be used in a single wireless system. Because only 802.11a devices formerly used this band (occasionally 802.11n uses it also) this band is less crowded and targeted for increased use for new 802.11 technologies under development.

What Channels Are Not Available?

Because each country has different regulatory requirements, the country code determines which channels you can configure on the radios. When you specify the country of operation for an access point, the radios are restricted to using the valid channels for that country.

The FCC (United States) requires that devices operating the 5-GHz band must employ dynamic frequency selection (DFS) and transmit power control (TPC) capabilities. This is to avoid interference with weather-radar and military applications. Additional channels in the 5-GHz band are restricted to avoid interference with Terminal Doppler Weather Radar (TDWR) systems. This eliminates the use of channels 120, 124, and 128. Channels 116 and 132 can be used if they are separated by more than 30 MHz (center-to-center) from a TDWR located within 35 km of the device.

How Do I Know Which Channels I Should Use?

For best performance, choose a channel at least 5 channels apart from your neighbors' networks. Determine this by completing a site survey—a site survey includes a test for RF interference.

Try to use non-overlapping channels (1, 6, 11 typically in the US), or minimize overlap of signals by using channels as far apart as possible from other networks in range.

You also need to know what channel your clients are capable of using, so that you can provide connection for that channel. For example, you can use Microsoft Windows 7 Device Manager to find the channel number at which your Microsoft Windows client can operate by following these steps:

1. Click **Start** > **Control Panel**.
2. Click **Device Manager** > **Network Adapters**.
3. Right-click the link describing Wi-Fi and select **Properties** from the menu.
4. Click the **Advanced** tab.

Two columns are displayed, Property and Value. The list under Property tells you the wireless capabilities of the computer. The current operating properties are highlighted—this tells you the current mode of operation.

Once you know the networking transmission standards used by clients (802.11n, 802.11g, 802.11b, or 802.11a) you can determine which channels the device can use—see Table 23 on page 116 for details.

Copyright © 2013, Juniper Networks, Inc.

Table 23: Channels a Device Can Use

Device Capability	Band and Channel Width used:	Typical Channel Use
802.11b	2.4-GHz band, 20-MHz channel width	1, 6, 11 (US) or 1, 5, 9, 13
802.11g	2.4-GHz band, 20-MHz channel width	1, 6, 11 (US) or 1, 5, 9, 13
802.11n	2.4-GHz band, 20-MHz channel width	1, 6, 11 (US) or 1, 5, 9, 13
	5-GHz band, 40-MHz channel width	(36,1) (40,-1) (44,1) (48,-1) (52, 1) (56,-1) (60,1) (64,-1) (100,1) (104,-1) (108,1) (112,-1) (116,1) (120,-1) (124,1) (128,-1) (132,1) (136,1) (149,1) (153,-1) (157,1) (161,-1)
802.11a	5-GHz band, 40-MHz channel width	3, 11

How Do I Avoid Co-Channel Interference?

Prevent interference and signal overlapping by doing an initial site survey of your wireless spectrum before deploying a wireless network. Once you discover all nearby signals, you can choose an optimum wireless channel that will provide the best performance with the least signal interference.

To automatically avoid co-channel interference, enable automatic channel tuning in a Radio profile—all radios using that Radio profile will then use algorithms to switch to optimum channels. See “Creating and Managing a Radio Profile” on page 315 to enable automatic channel tuning.

DFS Channels

In countries where Dynamic Frequency Selection (DFS) is required, Juniper Networks devices perform the appropriate check for radar on the 802.11a band. If radar is detected on a channel, the access point radio stops using the channel for the amount of time specified in the country’s regulations. Log messages are generated when this occurs. To enable DFS, see “Creating and Managing a Radio Profile” on page 315.

802.11n Channels Can Be Wider and Work on Both Bands

802.11n devices work on the 5-GHz radio band as well as the more-populated 2.4-GHz radio band. On the 5-GHz band, 802.11n channels can be either 40 MHz or 20 MHz wide as shown in Table 23 on page 116. This is one reason that 802.11n devices can be faster.

NOTE: **40 MHz channels work only with 802.11n on the 5-GHz band—40 MHz channels cannot not be configured on a 2.4-GHz radio.**

802.11n radios configured for the 5-GHz band have a primary channel and a secondary channel. The primary channel is listed using the channel number, and the secondary channel adds another 20 MHz to make the channel 40 MHz. Therefore, the secondary channel is either the channel above (1) or the channel below (-1) the primary channel. This notation keeps you from configuring non-contiguous channels. For example, if the

Copyright © 2013, Juniper Networks, Inc.

primary channel is 36 and the secondary channel is 40, the combination would be (36,1). If the primary channel is 44 and the secondary channel is 40, the notation would be (44,-1).

The following channels, listed as (primary channel, secondary channel) are supported for 802.11n at 5 GHz with 40 MHz bandwidth: (36,1) (40,-1) (44,1) (48,-1) (52, 1) (56,-1) (60,1) (64,-1) (100,1) (104,-1) (108,1) (112,-1) (116,1) (120,-1) (124,1) (128,-1) (132,1) (136,1) (149,1) (153,-1) (157,1) (161,-1)

How Are Channel Numbers Assigned?

Juniper Networks access point radios use channel auto-tuning by default. You can change the channel tuning interval, channel tuning range, or the channel tuning holddown settings. You can also turn off auto-tuning. For more information, see "Understanding Channel Auto-Tuning and Adaptive Channel Planner on Wireless Networks" on page 86 and to turn off channel auto tuning, see "Creating and Managing a Radio Profile" on page 315.

How Do I know What Channel an Access Point is Using?

If the access point is already installed and operating, use the Equipment tab of the monitor mode in Network Director to view the access point channel numbers.

Related Documentation

- Creating and Managing a Radio Profile on page 315
- Understanding Channel Auto-Tuning and Adaptive Channel Planner on Wireless Networks on page 86

Understanding Wireless Scanning

All wireless access point radios continually scan for other RF transmitters. While 802.11b/g/n radios scan in the 2.4-GHz to 2.4835 GHz spectrum, 802.11a radios (and sometimes 802.11n radios) scan in the 5.15 GHz to 5.85 GHz spectrum. There are two scanning methods, passive scanning and active scanning. By default, radios perform both types of scans on all channels allowed by the country of operation, which is the regulatory domain set during initial access point deployment. While both types of scanning are on by default, active scanning is performed only on channels on which local government regulations allow it to transmit. Channels that are not authorized for unlicensed use and channels that require radar detection with dynamic frequency selection (DFS) are excluded from active scanning.

This topic describes:

- What is the Difference Between Passive and Active Scanning? on page 118
- What Channels Are Scanned? on page 118
- How Does Scanning Work? on page 118
- What Additional Information is Learned By An Active Scan? on page 119
- What Happens to Scanned Information? on page 119
- CTS-to-self During Scanning on page 120
- What is Spectral RF Scanning? on page 120

Copyright © 2013, Juniper Networks, Inc.

What is the Difference Between Passive and Active Scanning?

During passive scans, the radio listens for beacons and probe responses. If you use only passive mode, the radio scans once per second, and audits packets on the wireless network. Passive scans are always enabled and cannot be disabled because this capability is also used to connect clients to access points.

Active scans are enabled by default but can be disabled in a Radio profile. During active scans, the radio sends probe-any requests (probe requests with a null SSID name) to solicit probe responses from other devices. In other words, access points actively look for other devices, in addition to listening for them.

What Channels Are Scanned?

RF scanning can be performed on a variety of different sets of channel ranges or frequencies. The scan can be configured in the Radio profile to scan either operating channels, regulatory channels, or all channels.

NOTE: **An access point will never transmit on channels that are not authorized for transmission.**

In a Radio profile, you can change the channels a radio actively scans. These are the three options for active scanning :

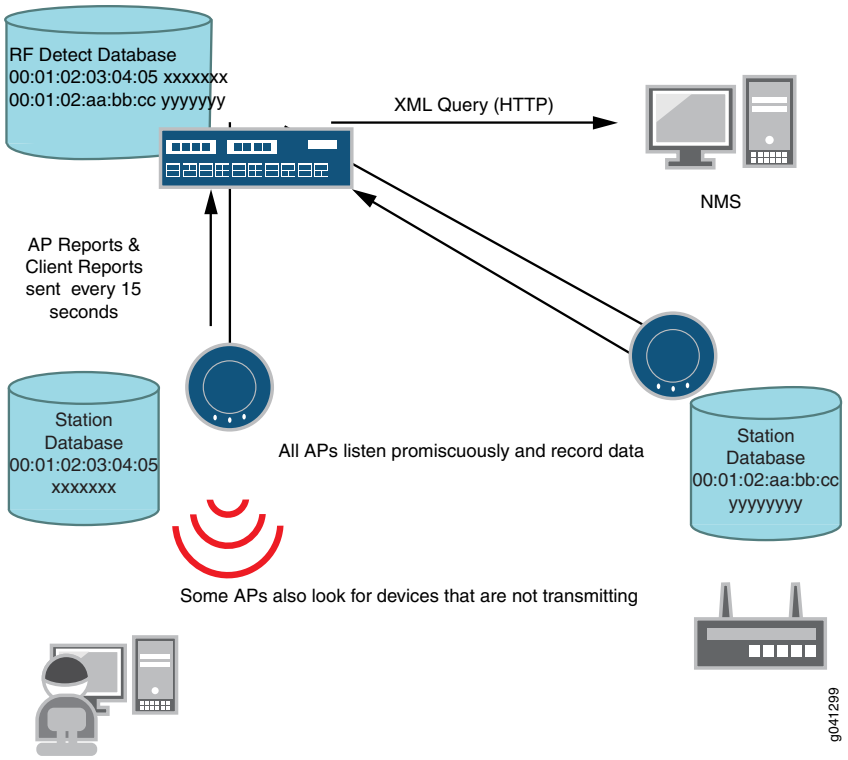
- Operating: Only the current channel is scanned and audited.
- Regulatory: Only regulatory channels are scanned and audited. If the radio is configured for 802.11b/g/n, the most commonly used channels, such as 1, 6, or 11, are scanned and audited more frequently.
- All: All channels are scanned and audited.

How Does Scanning Work?

To scan outside of the operating range, the access point must change channels. These off-channel scans are performed once per second, and a different channel in the range is scanned each second until it cycles through all in-scope channels. The access point will go off channel for about 30ms (3% of the time). Scans are scheduled to avoid interfering with beacon transmission. Radio transmit queues are drained prior to channel change. Then the probes are sent once channel change is completed. Note that the scan frequency is reduced if voice, video traffic, or heavy load is detected. Also, the CTS-to-self feature can be configured to silence clients on the operating channel while access point goes off channel.

Copyright © 2013, Juniper Networks, Inc.

Figure 15: Scanned Data is Stored in the Station Databases and Sent to the Controller



How Does Active Scanning Work?

The active-scan algorithm is sensitive to high-priority (voice or video) traffic or heavy data traffic. Active-scan scans for 30 milliseconds once every second, unless either of the following conditions is true:

- High-priority traffic (voice or video) is present at 64 Kbps or higher. In this case, active-scan scans for 30 milliseconds every 60 seconds.
- Heavy data traffic is present at 4 Mbps or higher. In this case, active-scan scans for 30 milliseconds every 5 seconds.

What Additional Information is Learned By An Active Scan?

Active scanning is more thorough and provides more information than passive scanning. If you select active mode, the radio actively sends probes on other channels and then audits the packets on the wireless network. The probe response received by an active scan normally contains the BSSID and WLAN SSID of the access point answering the probe. This is how the Permitted SSID list gets a list of all SSIDs on the air, even if a device is not currently sending signals.

What Happens to Scanned Information?

Scanned information is stored and used by the:

Copyright © 2013, Juniper Networks, Inc.

- Network security system to identify rogue access points (see *Understanding Fault Mode in Network Director*).
- Network Director reports (see *Alarm Summary Report*, *Audit Trail Report*, and *Alarm History Report*).
- Automatic access point power feature (see "Understanding Automatic Power Tuning for Wireless Radios" on page 91).
- Automatic access point channel feature (see "Understanding Channel Auto-Tuning and Adaptive Channel Planner on Wireless Networks" on page 86).
- RF Neighborhood monitoring (see *Monitoring the RF Neighborhood*).
- Spectral RF scanning feature (see *Monitoring the RF Spectrum of a Radio*.
- Spectral RF scanning feature (see *Monitoring the RF Spectrum of a Radio*).

CTS-to-self During Scanning

The clear to scan CTS-to-self feature can be configured in a Radio profile to silence clients on the operating channel while an access point goes off channel to scan. This option is also part of the Radio profile.

What is Spectral RF Scanning?

The electromagnetic spectrum includes all possible frequencies of electromagnetic radiation. Wireless communication uses the low frequencies used for radio communication, but other objects can affect these frequencies. Spectral analysis reports objects with any electromagnetic properties.

Spectral analysis starts with the RF detect function. The primary function of RF detect is to detect and classify 802.11 devices, but for spectral analysis, that function is extended to recognize non-802.11 sources of interference. Because the primary function of RF detect is to locate 802.11 devices, interfaces are wireless-LAN-centric; for example, frequencies are displayed in terms of 802.11 channels.

In Network Director, two spectrograms are provided under monitoring, one for a radio's channels and one for the results of a spectrum sweep. The second spectrogram also includes graphing of the duty cycle of the radio.

Channel auto-tuning (see "Understanding Channel Auto-Tuning and Adaptive Channel Planner on Wireless Networks" on page 86) defines a transmission ID for access point radios. With spectral analysis, that definition is extended to all interference sources.

With spectral monitoring enabled, an enabled access point radio will drop the current clients and scan for any device with a radio signal. For directions to implement spectral monitoring, see *Monitoring the RF Spectrum of a Radio*.

Related Documentation

- *Monitoring the RF Spectrum of a Radio*
- *Alarm Summary Report*
- *Audit Trail Report*
- *Alarm History Report*

Copyright © 2013, Juniper Networks, Inc.

- Understanding Automatic Power Tuning for Wireless Radios on page 91
- Understanding Channel Auto-Tuning and Adaptive Channel Planner on Wireless Networks on page 86

Understanding WMM Power Save and WLAN Client Battery Life

Wi-Fi mobile devices need as much battery power as possible because the power demands of voice, audio, and video applications are ever-increasing. To maintain laptop battery life in these situations, WMM Power Save was certified by the Wi-Fi Alliance. WMM Power Save is an addition to WMM, the technology that enables Quality of Service (QoS) functionality in Wi-Fi networks by prioritizing traffic from different applications. WMM is a required feature for 802.11n capable devices—almost all modern Wi-Fi devices support it.

WMM Power Save is optimized for latency-sensitive applications such as voice, audio, or video, but benefits any Wi-Fi device. With WMM Power Save, the same amount of data can be transmitted in fewer frames in a shorter time, while enabling the Wi-Fi device to preserve power in a low-power, dozing state in between transmissions.

This topic describes:

- How Does WMM Power Save Extend Battery Life? on page 121
- Where is WMM Defined? on page 122
- How is WMM Power Save Implemented on Juniper WLANs? on page 122
- WMM Power Save is Disabled by Default on page 122
- Why Should I Enable WMM Power Save in a Radio Profile? on page 122

How Does WMM Power Save Extend Battery Life?

Power save uses mechanisms from 802.11e and legacy 802.11 to save power for battery powered equipment and fine-tune power consumption. Products targeted for power-critical applications such as mobile phones, smart phones, and other portable power devices typically use WMM Power Save.

The underlying concept of WMM Power Save is that the client triggers the release of buffered data from the access point by sending an uplink data frame. Upon receipt of that data trigger frame, the access point releases previously buffered data stored in each of its four queues. Queues can be configured to be either trigger enabled (receipt of a data frame corresponding to each queue acts as a trigger), or delivery enabled (data stored in all queues is released upon receipt of a frame).

WMM operates by dividing traffic into four access categories: background, best effort, video, and voice. QoS policy determines the different handling of each access category. The result is that different packets are handled differently.

Copyright © 2013, Juniper Networks, Inc.

Where is WMM Defined?

WMM was a precursor to the 802.11e standard. Before the 802.11e standard could be ratified, a few organizations came together and published a draft standard called WMM. Once the 802.11e standard was finalized, WMM became an enhancement to the 802.11e standard, and was referred to as 802.11e quality of service (QoS) enhancements. Both the original WMM standard and 802.11e are now deprecated, but the industry continues to use that terminology.

How is WMM Power Save Implemented on Juniper WLANs?

To take advantage of WMM Power Save functionality, both the Wi-Fi client and the access point must be Wi-Fi CERTIFIED for WMM Power Save. In addition, the applications used also need to support WMM Power Save to inform the client of the requirements of the traffic they generate.

WMM is supported by Radio profiles, along with the corresponding QoS policies that describe access classes. When a wireless client using WMM Power Save associates with an access point using a Radio profile that includes WMM, the client selects the access classes (voice, video, best effort, background) in WMM Power Save.

WMM Power Save is Disabled by Default

WMM Power Save is disabled by default on access points, even though it saves client battery life, because clients using Power Save must send a separate PSpoll to retrieve each unicast packet buffered by the access point radio. This can sometimes slow performance, depending on the network configuration. Also, your applications need to support WMM Power Save to inform the client of the requirements of the traffic they generate.

Why Should I Enable WMM Power Save in a Radio Profile?

WMM Power Save preserves client battery life, especially for applications such as voice and video. Wi-Fi CERTIFIED for WMM Power Save devices can operate in any Wi-Fi network and coexist with 802.11 legacy power save mechanisms.

Related Documentation

- Creating and Managing a Radio Profile on page 315

Copyright © 2013, Juniper Networks, Inc.

PART 2

Configuration

- Device Configuration on page 125
- Network Domain and Mobility Domain Configuration on page 397
- Topology View Configuration on page 403
- Virtual View Configuration on page 429
- Custom Group Configuration on page 447

Copyright © 2013, Juniper Networks, Inc.

Copyright © 2013, Juniper Networks, Inc.

CHAPTER 8

Device Configuration

- Adding and Managing an Access Point on page 126
- Configuring Fibre Channel Gateways on page 132
- Configuring a Voice SSID with Network Director on page 133
- Creating and Managing Access Profiles on page 136
- Creating and Managing Authentication Profiles on page 157
- Creating and Managing Wireless Authorization Profiles on page 167
- Creating and Managing Wireless Auto AP Profiles on page 174
- Creating and Managing CoS Profiles on page 184
- Creating and Managing Device Common Settings on page 198
- Creating and Managing Fabric Profiles on page 223
- Creating and Managing FC Gateway Service Profiles on page 228
- Creating and Managing Filter Profiles on page 231
- Creating and Managing LDAP Profiles on page 273
- Managing and Creating a Link Aggregation Group on page 278
- Creating and Managing Port Profiles on page 283
- Creating and Managing a Radio Profile on page 315
- Creating and Managing RADIUS Profiles on page 326
- Creating a Radio Profile for Voice Clients Only on page 329
- Creating and Managing VLAN Profiles on page 330
- Creating and Managing a WLAN Service Profile on page 350
- Creating a WLAN Service Profile Dedicated to Voice on page 368
- Assigning Authorization Profiles to Controllers on page 369
- Assigning an Auto AP Profile to Controllers on page 371
- Assigning Device Common Settings to Devices on page 375
- Assigning a Fabric Profile to Devices and Ports on page 377
- Assigning an FC Gateway Service Profile to Ports on page 381
- Assigning a Port Profile to Interfaces on page 383

Copyright © 2013, Juniper Networks, Inc.

- Assigning a Radio Profile to Radios on page 389
- Assigning a VLAN Profile to Devices or Ports on page 392

Adding and Managing an Access Point

You can explicitly configure access points with enough information to uniquely identify them. This method prevents other access points from being erroneously added, either by accident or by intruders using access point spoofing. These access points are persistent—the configuration does not go away if an access point is not seen by the controller.

NOTE: The feature Auto AP adds access points to controllers temporarily—see "Understanding Auto AP Profiles" on page 24 and "Creating and Managing Wireless Auto AP Profiles" on page 174.

This topic describes using Network Director to add specified access points.

- Configuring Individual Access Points on page 127
- Configuring Access Point Options on page 128
- Adding an Access Point to a Wireless Network on page 129
- Defining an Access Point on page 129
- Defining Access Point Radios on page 130

Copyright © 2013, Juniper Networks, Inc.

Configuring Individual Access Points

To configure individual access points with Network Director:

1. Gather this information:
   - Access point model—for example, WLA321. The model is listed on the back of the access point.
   - Access point IDs that have already been assigned, for example, 1, 2, and so on. You cannot repeat these numbers for new assignments.

     TIP: Some controllers keep track of the IDs that are in use, and suggest an unused ID during installation.

   - Serial number from the label on the back of the access point.

     TIP: Serial numbers never contain spaces.

   - Optionally, for increased security, you can configure the access point fingerprint, which is an encryption key pair generated at the factory. The fingerprint for the public key is displayed on a label on the back of the access point, in the following format: RSA a:aaaa:aaaa:aaaa: aaaa:aaaa:aaaa:aaaa
   - Optionally, if you added an external antenna or plan to add an external antenna to the access point, you need the model number of the antenna.

     TIP: If you do not specify an antenna, the access point's internal antenna is used.

2. Click

in the Network Director banner.
3. Under Select View, select either Logical View, Location View, Device View or Custom Group View.

   TIP: Do not select Virtual View or Topology View.

4. Under the Wireless Network in the View pane, select either a controller, a custom group with controllers, or a cluster of controllers.

   TIP: Do not select the whole wireless network or an individual access point—these selections are not viable for adding an access point, because access points cannot be added to an entire network nor to individual access points. You do not see **Manage Access Point** unless you select a viable selection.

Copyright © 2013, Juniper Networks, Inc.

5. Click **Manage Access Point** under Device Management in the Tasks pane.

   The Manage Access Point page is displayed.

6. Click **Add** on the Manage Access Point page.

   The Add AP dialog box opens with the Access Point tab selected.

7. Complete the Add AP procedure as described in both online help and "Defining an Access Point" on page 129.

   NOTE: **Once you select an access point model, configuration tabs appear for one or two radios.**

8. Click the **Radio 1** tab and complete the radio information as described in both online help and "Defining Access Point Radios" on page 130.

9. If it is displayed, click the **Radio 2** tab and complete that radio information as described in both online help and "Defining Access Point Radios" on page 130.

10. Click **OK**.

    The access point is added to the Manage Access Points list on the screen.

11. Add as many access points as needed, and then click **Done**.

    The access point appears on the inventory list, but has not been added to the network yet—the access point becomes part of the network when you deploy the controller.

    WARNING: **You must click Done to add the access point. If you skip clicking Done, the configuration disappears.**

12. Deploy the controller or controller cluster, following the directions *Deploying Configuration to Devices*.

    The access points become part of the network when you deploy the associated controller or cluster.

Configuring Access Point Options

From the **Manage Access Points** page, you can:

- Manually add an access point to a controller by clicking **Add**. For detailed steps, see "Adding an Access Point to a Wireless Network" on page 129.
- Modify an existing access point configuration by selecting it and clicking **Edit**.
- Delete manually configured access points by selecting an access point and clicking **Delete**.

TIP: **You can delete access points that are in use—the clients from the access point re-associate to another access point.**

Copyright © 2013, Juniper Networks, Inc.

Table 24 on page 129 describes the information provided about access points on the Manage Access Points page, which is available only in Logical View. The access points displayed are those managed by the controller or cluster selected in the View pane.

Table 24: Manage Access Point Fields

Field	Description
AP Name	Name given to the access point when the access point was created.
AP ID	Number from 1 through 9999 that identifies an access point.
Model	Juniper access point model number
Serial Number	Serial number on the back of the access point
Fingerprint	Access points are configured with an encryption key pair at the factory. The fingerprint for the public key is displayed on a label on the back of the access point, in the format: RSA a:aaaa:aaaa:aaaa: aaaa:aaaa:aaaa:aaaa TIP: This field might be blank because a fingerprint is optional during access point configuration.
Connection	Distributed access points are connected to the network. Direct access points are connected to a controller on port 1, 2, 3, 4, 5, or 6.

Adding an Access Point to a Wireless Network

You can explicitly configure access points with enough information to uniquely identify them. This method prevents other access points from being erroneously added, either by accident or by intruders. To do this, you add access points manually, using the Add AP feature, so that the network only finds your specific access point. These configurations are persistent—they don't disappear when the access point loses contact with the controller.

Defining an Access Point

To configure an access point, enter the settings described in Table 25 on page 129. Required settings are indicated by a red asterisk (*) that appears next to the field label in the user interface.

Table 25: Access Point Configuration

Field	Description
AP Name	Type a unique name that identifies the access point. You can use up to 16 characters, but spaces are not allowed.
AP ID	Type an ID number from 1 - 99999 that has not yet been assigned.
Connection	Distributed access points are connected to the network. Direct access points are connected to a controller on port 1, 2, 3, 4, 5, or 6.

Copyright © 2013, Juniper Networks, Inc.

Table 25: Access Point Configuration *(continued)*

Field	Description
Model	Select the access point model from the list. When you do this, the correct number of radio tabs appear, either one (Radio 1) or two (Radio 1 and Radio 2) tabs.
Serial Number	Type the serial number found on the back of the access point.
Fingerprint	Optionally, type the fingerprint for the access point public key, which is displayed on a label on the back of the access point, in the following format: RSA a:aaaa:aaaa:aaaa: aaaa:aaaa:aaaa:aaaa
Bias (default is high)	If this access point is directly connected to the selected controller, leave this field blank. If the access point is indirectly connected to the selected controller, you can indicate that the access point has a high bias for the controller, or has a low bias. Bias matters only for access points indirectly connected to the controller through an intermediate layer 2 or layer 3 network. An access point always attempts to boot on AP port 1 first, and if a controller is directly attached on AP port 1, the access point boots from there regardless of the bias settings. Set the access point's bias to high or low for the selected controller. Set the bias to sticky to have the access point continue to use the current controller for the active data link even if another controller configured with high bias becomes available. For more explanation, see "Understanding Access Point Bias for Controllers" on page 84.
Country Code	Select the country where the access point will be operating. Different countries have different regulations and Juniper devices will not allow violations based on the country code you select.
Enable Firmware Update	Select for automatic firmware updates. When the controller receives a newer copy of the access point firmware, this access point will be updated.
Force Image Download	Select for automatic image updates. When the controller receives a newer copy of the access point image, this access point will be updated.

Click the **Radio 1** tab to add the access point's radio information. Click **Help** for details.

Defining Access Point Radios

Access points can have one radio or two radios, depending on the model. Provide the settings for each radio, as described in Table 26 on page 131.

Copyright © 2013, Juniper Networks, Inc.

Table 26: Access Point Radio Settings

Field	Action
Radio Type	Select one of the radio types, 11a, 11b, 11g, 11na, or 11ng. For a description of these radio types, see "Understanding the IEEE 802.11 Standard for Wireless Networks" on page 100.
Radio Mode	Turn on the radio by selecting **Enable**. Turn off the radio by selecting **Disable**. Put the radio into sentry mode, meaning the radio scans for interference but does not transmit user traffic, by selecting **Sentry**.
Channel Number	Select a channel number for the radio. For more information about radio channels, see "Understanding Wireless Radio Channels" on page 114. NOTE: If auto-channel is enabled, the radio might change channels after it is deployed. For more information about radio channels, see "Understanding Channel Auto-Tuning and Adaptive Channel Planner on Wireless Networks" on page 86.
Transmit Power	Select the transmit power for the radio. The range available is 1 milliwatt (dBm) through 14 milliwatts (dBm). Transmit power is limited by some country codes. Unless you have a reason to do otherwise, we recommend that you set the power as high as possible. NOTE: If power auto-tuning is enabled, the radio might change transmit power after it is deployed. For more information about automatic power tuning , see "Understanding Automatic Power Tuning for Wireless Radios" on page 91.
Antenna Location	Select **Indoor** if you are using an indoor antenna—this includes the built-in antenna. If you added an outdoor antenna, select **Outdoor** from the list.
Antenna Type	If you did not add any additional antenna, select **Internal** to use the built-in antenna. If you added an antenna to the radio, select one of the supported add-on antenna models from the list.
Load Balance Group Name	You can create a load balancing group and assign this access point to it by selecting this option and providing a group name. You can also add this radio to an existing load balance group by selecting this option and providing an existing group name.

If the access point has two radios, click the **Radio 2** tab to add the other radio's information. Then, click **OK**.

Related Documentation

- *Understanding the Network Director User Interface*
- Understanding Auto AP Profiles on page 24
- Understanding Access Point Bias for Controllers on page 84
- Understanding Automatic Power Tuning for Wireless Radios on page 91

Copyright © 2013, Juniper Networks, Inc.

- Understanding Wireless Radio Channels on page 114
- Understanding the IEEE 802.11 Standard for Wireless Networks on page 100

Configuring Fibre Channel Gateways

This topic describes the methods Network Director provides to configure Fibre Channel (FC) gateways on data center switching devices.

This topic describes:

- Using the FC Gateway Service Profile to Configure FC Gateways on page 132
- Using a Combination of Profiles to Configure FC Gateways on page 132

Using the FC Gateway Service Profile to Configure FC Gateways

An FC Gateway Service profile provides a quick way to configure Fibre Channel (FC) gateways on Data Center Switching devices. It is intended for FC gateway devices that are connected directly to the FCoE network, without transit switches. In addition to the settings you can specify, the profile creates an FC gateway configuration with some default settings that cannot be modified. For example, you cannot specify any CoS settings for the FC gateway; only the default settings are available.

For information about using the FC Gateway Service profile, see "Creating and Managing FC Gateway Service Profiles" on page 228.

Using a Combination of Profiles to Configure FC Gateways

If you want to configure an FC gateway that does not meet the requirements of the FC Gateway Service profile, you can use a combination of other profiles to configure the components of the FC gateway and assign them to the appropriate devices, ports, and profiles.

The profiles you use to configure an FC gateway include:

- CoS profile—Configures CoS on the FC gateway Ethernet interfaces that is required to support FCoE. You assign the CoS profile to the port profiles you assign to the Ethernet ports in the FC gateway.
- VLAN profiles—Configure the FCoE VLANs used to carry FCoE traffic on the FC gateway and the native VLAN used to transport FIP traffic. You assign the FCoE VLAN profile to the Fabric profile and the Port profiles assigned to the FC and Ethernet ports in the FC gateway. You assign the native VLAN profile to the port profile for the ports in the FC gateway.
- Port profiles—Configure FC and Ethernet ports as FC gateway ports, and configure Ethernet port VLAN membership and FIP settings. You assign Port profiles to the FC and Ethernet ports in the FC gateway. The Port profile includes the CoS and VLAN profiles assigned to it.
- Fabric profile—Configures the FC gateway fabric. The Fabric profile includes the FCoE VLAN profile assigned to it.

Copyright © 2013, Juniper Networks, Inc.

Related Documentation

- Creating and Managing FC Gateway Service Profiles on page 228
- Creating and Managing CoS Profiles on page 184
- Creating and Managing Fabric Profiles on page 223
- Creating and Managing Port Profiles on page 283
- Creating and Managing VLAN Profiles on page 330

Configuring a Voice SSID with Network Director

Voice over IP has different requirements than data traffic and therefore has unique configuration requirements. For an explanation of voice traffic, see "Understanding Voice Clients and Voice Traffic" on page 105.

If your network is supporting both wireless data clients and voice clients, we recommend that you have two WLAN Service profiles, one for data and one for voice—this topic describes creating a WLAN Service profile for voice clients.

NOTE: **WLAN Service profiles define the SSID name.**

This topic describes:

- Creating a CoS Profile Dedicated to Voice on page 133
- Creating a WLAN Service Profile Dedicated to Voice on page 134

Creating a CoS Profile Dedicated to Voice

To be able to support latency-sensitive traffic such as voice traffic, you must create a dedicated CoS profile by entering voice-specific settings. This topic describes the typical settings that you can use to create a CoS profile dedicated to voice.

To create a CoS profile dedicated to voice:

1. Click the Build Mode icon

in the Network Director banner.
2. Click **CoS** under Profile and Configuration Management in the Tasks pane.

   The Manage CoS Profiles page opens, displaying the list of current CoS profiles.
3. Click **Add** on the Manage CoS Profiles page and select **Wireless Controller (WLC)** in the Device Family Chooser page.

   The Create CoS Profile for Wireless Controllers (WLC) wizard opens.
4. Configure the following settings:
   - Provide a name for the CoS profile.
   - In the Voice CoS section, select **VoIP-data**.

Copyright © 2013, Juniper Networks, Inc.

- (Optional) In the Voice CoS section, select **Enable Bandwidth Limit** and specify the maximum bandwidth that you want the system to reserve for voice traffic.
- In the Access Categories section, make sure that the action corresponding to the Access Category—Voice is **Permit**.

5. Click **Done** to save the settings.

For an explanation of all the CoS profile parameters, see "Creating and Managing CoS Profiles" on page 184.

After you create the CoS profile, you then associate the CoS profile with an Authorization profile during creation of the Authorization profile. Next, you associate the Authorization profile with a WLAN Service profile to apply the CoS settings to all the users who connect to that SSID. For information on creating a WLAN Service profile (including mapping the Authorization profile) dedicated to voice, see "Creating a WLAN Service Profile Dedicated to Voice" on page 134.

Creating a WLAN Service Profile Dedicated to Voice

If your network is supporting both wireless data clients and voice clients, we recommend that you have two WLAN Service profiles, one for data and one for voice—this topic describes creating a WLAN Service profile for voice clients.

NOTE: You will need to link an existing Authorization profile and Authentication profile during WLAN creation. For directions to create an Authorization profile, see "Creating and Managing Wireless Authorization Profiles" on page 167. For directions to create an Authentication profile, see "Creating and Managing Authentication Profiles" on page 157.

Create a WLAN Service profile for voice clients:

1. Click **Build** mode in the Network Director banner.

TIP: WLAN Service profiles can be created in any view—Device View, Logical View, or Location View.

2. Click **WLAN Service** under Profile and Configuration Management in the Tasks pane.

   The Manage WLAN Service Profiles page opens, displaying the list of currently configured WLAN Service profiles.

3. Click **Add** on the Manage WLAN Service Profiles page.

   The Create WLAN Service Profile for Wireless Controllers (WLC) wizard opens with the **Basic Settings** tab displayed.

4. In the Basic Settings tab of the Create WLAN Service Profile wizard, configure these settings:

Copyright © 2013, Juniper Networks, Inc.

- Provide a name for the WLAN.
- Set SSID Type to **Crypto**.
- Select the previously created Authorization profile and Authentication profile.
- Set Fall Through Access to **Last Resort**.

5. Click the **Security Settings** tab of the Create WLAN Service Profile wizard, and configure these settings:
   - Ideally, enable RSN (WPA2) **802.1X Auth** with CCMP. You might also need to configure PSK authentication depending on the capabilities of the client devices.
   - Disable WPA **802.1X Auth**.
6. Click the **Advanced Settings** tab of the Create WLAN Service Profile wizard, and configure these settings:
   - Enable **Proxy ARP** to help preserve client battery life and to allow the access points to respond to ARPs on behalf of the clients.
   - Enable **No Broadcast** to help preserve client battery life and to convert ARP and DHCP broadcast messages to unicast.
   - Set **Short Retry Count** to 3.
   - Set **Long Retry Count** to 3.
   - Set **CAC Mode** to VoIP Session.

     NOTE: **Restricting sessions on the access point applies to both data and voice clients, which is one reason we recommend separate profiles for voice and data.**

   - Enable **Load Balancing Exempt** to prevent dynamic load balancing of clients on the service and ensure the fastest possible association .
   - Beacon the service at a higher data rate to encourage faster roaming. Beacons sent at a higher data rate can be heard over a shorter distance, so the client will scan for new access points sooner and roam more quickly
7. Click **Review**, check the configuration, then click **Finish**.

A WLAN Service profile is not used automatically. You must link a Radio profile to the WLAN Service profile, then link the Radio profile to radios to apply WLAN Service profile settings. Next, create a Radio profile to use with the WLAN Service profile.

For an explanation of all WLAN Service profile parameters, see "Understanding WLAN Service Profiles" on page 52. To create a radio profile for voice, see "Creating a Radio Profile for Voice Clients Only" on page 329.

Related Documentation

- Understanding Voice Clients and Voice Traffic on page 105
- Creating a Radio Profile for Voice Clients Only on page 329
- Creating and Managing CoS Profiles on page 184

Copyright © 2013, Juniper Networks, Inc.

- Creating a WLAN Service Profile Dedicated to Voice on page 134
- Creating and Managing Wireless Authorization Profiles on page 167
- Creating and Managing Authentication Profiles on page 157
- Understanding WLAN Service Profiles on page 52

Creating and Managing Access Profiles

Access profiles enable authentication configuration for both methods and servers. Network Director supports the configuration of RADIUS, Lightweight Directory Access Protocol (LDAP), and local authentication as authentication methods, and RADIUS as an accounting method.

Use the Manage Access Profiles page to create new Access profiles and manage existing Access profiles.

To display the Manage Access Profiles page: In Build mode, select **Access** from Profile and Configuration Management in the Tasks pane. The Manage Access Profiles page appears.

This topic describes:

- Managing Access Profiles on page 136
- Creating an Access Profile on page 137
- Specifying Basic Settings for an EX Series Switching or Data Center Switching Access Profile on page 139
- Specifying RADIUS Accounting Settings for an EX Switching or Data Center Switching Access Profile on page 141
- Specifying Basic Settings for a Wireless Access Profile on page 143
- Specifying Server Group Settings for a Wireless Access Profile on page 144
- Specifying Basic Settings for a Campus Switching ELS Access Profile on page 151
- Specifying RADIUS and LDAP Settings for Campus Switching ELS on page 151
- Reviewing and Modifying the Access Profile Settings on page 156
- What To Do Next on page 157

Managing Access Profiles

From the Manage Access Profiles page, you can:

- Create a new Access profile by clicking **Add**. For details, see "Creating an Access Profile" on page 137.
- Modify an existing profile by selecting it and clicking **Edit**.
- View information about an Access profile, including the interfaces it is associated with, by either clicking the profile name or by selecting the profile and clicking **Details**.
- Delete an Access profile by selecting the Access profile and clicking **Delete**.

Copyright © 2013, Juniper Networks, Inc.

TIP: You cannot delete profiles that are in use—that is, assigned to objects or used by other profiles. To see the current assignments for an Access profile, select the Access profile and click **Details**.

- Clone a profile by selecting a profile and clicking **Clone**.

TIP: The default Access profile named *juniper-access-profile* is always available.

Table 27 on page 137 describes the information provided about Access profiles on the Manage Access Profiles page. This page lists all Access profiles defined for your network, regardless of the scope you selected in the network view.

Table 27: Manage Access Profile Fields

Field	Description
Profile Name	Name given to the profile when the profile was created.
Description	Description of the profile that was entered when the profile was created. TIP: To display the entire description, you might need to resize the Description column by clicking the column border in the heading and dragging it.
Family Type	The device family on which the profile was created: EX Switching, Wireless, Campus Switching ELS, or Data Center Switching Non-ELS.
Creation Time	Date and time when this profile was created.
Update Time	Date and time when this profile was last modified.
User Name	The username of the user who created or modified the profile.

TIP: All columns might not be displayed. To show or hide fields listed in the Manage Authorization Profiles table, click the down arrow on the field header, select **Columns**, and select or clear the check box adjacent to the field that you want to show or hide.

Creating an Access Profile

In Network Director, you create an Access profile that is then used to authenticate network users. You can also specify servers to be used for user accounting purposes. You can create Access profiles for these kinds of hardware devices:

- EX Series Switches—configure Basic Settings and optional Accounting Settings.
- Wireless (WLC)—configure Basic Settings and Server Group Settings.

Copyright © 2013, Juniper Networks, Inc.

- EX Series switches with ELS—configure Basic Settings and Server Settings.
- Data Center Switching Non-ELS—configure Basic Settings and optional Accounting Settings.

To create an Access profile, follow these steps:

1. Click

in the Network Director banner.
2. Under Select View, select either **Logical View**, **Location View**, **Device View** or **Custom Group** View.

   TIP: **Do not select Virtual View or Topology View.**
3. Click **Access** under Profile and Configuration Management in the Tasks pane.

   The Manage Access Profiles page appears, displaying the list of currently configured Access profiles.
4. Click **Add**.

   The Device Family Chooser window opens.
5. From the Device Family Chooser, select the device family for which you want to create a profile. The available device families are **Switching EX**, **Wireless (WLC)**, **Campus Switching ELS**, and **Data Center Switching Non-ELS**.
6. Click **OK**.

   The Create Access Profile wizard for the selected device family opens—it consists of two sections, Basic Settings and RADIUS and LDAP configuration.
7. Specify the access settings for the Access profile by doing one of the following:
   - For either EX Series switches or Data Center Switching, specify the access settings described in "Specifying Basic Settings for an EX Series Switching or Data Center Switching Access Profile" on page 139 and "Specifying RADIUS Accounting Settings for an EX Switching or Data Center Switching Access Profile" on page 141.
   - For controllers, specify the access settings as described in "Specifying Basic Settings for a Wireless Access Profile" on page 143 and "Specifying Server Group Settings for a Wireless Access Profile" on page 144.
   - For Campus Switching ELS, specify the access settings as described in "Specifying Basic Settings for a Campus Switching ELS Access Profile" on page 151 and "Specifying RADIUS and LDAP Settings for Campus Switching ELS" on page 151.
8. Click either **Next** or **Review**. The Review page appears.

   You can either save your profile or make changes to your profile from the Review page. For details, see "Reviewing and Modifying the Access Profile Settings" on page 156.
9. Click **Done** to save the Access profile.

   The system saves the Access profile and then displays the Manage Access Profiles page. Your new or modified Access profile is listed in the table of Access profiles.

Copyright © 2013, Juniper Networks, Inc.

Specifying Basic Settings for an EX Series Switching or Data Center Switching Access Profile

Basic settings for EX Series switching or data center switching Access profile include the profile name, authentication server order, and the RADIUS authentication details.

To configure the basic settings for an EX switch or data center switching Access profile, enter the settings described in Table 28 on page 139. Required settings are indicated in the user interface by a red asterisk (*) that appears next to the field label.

Table 28: Access Profile Basic Settings for EX Series Switches and Data Center Switching

Field	Action
Access Profile Details	
Profile Name	Type the name of the profile.
Description	Type the description of the profile.
Revert Interval (Sec)	Specify the number of seconds the switch waits after an authentication server becomes unreachable. The switch rechecks the connection to the server when the specified interval expires. Default is 3 seconds.
RADIUS Servers: Authentication	
View	Select a server entry from the list and then click **View** to see the details of that entry.

Copyright © 2013, Juniper Networks, Inc.

Table 28: Access Profile Basic Settings for EX Series Switches and Data Center Switching *(continued)*

Field	Action
Task: Create and add a new RADIUS server configuration	To both create and add a RADIUS server configuration to this Access profile for authentication: 1. Click **Add** > **Create RADIUS**. The Create RADIUS Server window opens. 2. Complete these fields: • **Server Name**—Type the name of the RADIUS server that you want to create. • **Server Address**—Type the IP address of the RADIUS server. • **Authentication Port**—The default RADIUS authentication port is 1812. You can change the port number by using the up and down arrows. • **Secret**—Provide a password. If the password contains spaces, enclose it in quotation marks. The secret password used by the switch must match the one used by the server. 3. Expand the RADIUS server and change any of these configurations: • **Accounting Port**—You can change the default port number (1813) by using the up and down arrows. • **Retry Count**—Specify the number of times that a device attempts to contact the LDAP authentication server. The default retry count is 3. You can change this value by using the up and down arrows to 1 through 10 times. • **Timeout** (seconds)—Specify the number of seconds the switch waits to receive a response from a RADIUS server. The default timeout is 5 seconds. You can change this value, using the up and down arrows, to 1 through 90 seconds. 4. Click **OK**. The RADIUS server is automatically added to the list of authentication servers assigned to this Access profile. 5. If you have more than one RADIUS server listed, you can use the arrows to reorder the list priority so that the most preferred RADIUS server is listed first.

Copyright © 2013, Juniper Networks, Inc.

Table 28: Access Profile Basic Settings for EX Series Switches and Data Center Switching *(continued)*

Field	Action
Task: Add a previously configured RADIUS server for authentication	The RADIUS tab is selected by default for server configuration and configured RADIUS servers are listed on this Server Settings page. To add a previously configured RADIUS server to this Access profile for authentication: 1. Click **Add** > **Select RADIUS**. A list of available configured RADIUS servers is displayed. Servers in this list were either automatically discovered or created by using the directions in "Creating and Managing RADIUS Profiles" on page 326. 2. Select one or more RADIUS servers from the list of Available servers and use the arrows to move the server to the Selected list. 3. Click **OK**. The RADIUS server is added to the list of authentication servers to be used with this Access profile. 4. If you have more than one RADIUS server listed, you can use the arrows to reorder the login priority so that the most preferred RADIUS server is listed first.
Task: Delete a server	To delete a RADIUS server from this Access profile: 1. Select a RADIUS server from the list. 2. Click **Delete**. The RADIUS server is removed from the list of authentication servers to be used with this Access profile.

Proceed to the RADIUS Accounting settings for EX switching Access profiles by clicking either **Accounting Settings** or **Next**. These settings are described in "Specifying RADIUS Accounting Settings for an EX Switching or Data Center Switching Access Profile" on page 141.

Specifying RADIUS Accounting Settings for an EX Switching or Data Center Switching Access Profile

Configure the settings listed in Table 29 on page 141 for the Access profile Accounting Settings page. Accounting settings are optional in an Access profile. You can also specify accounting settings later by modifying an existing Access profile.

Table 29: Accounting Settings for an EX Switching and Data Center Switching Access Profile

Task	Description
View	Select a RADIUS server entry from the list and then click **View** to see the details of that entry.

Copyright © 2013, Juniper Networks, Inc.

Table 29: Accounting Settings for an EX Switching and Data Center Switching Access Profile *(continued)*

Task	Description
Create a new RADIUS server for both authentication and accounting	To both create and add a RADIUS server configuration to this Access profile for both authentication and accounting: NOTE: A RADIUS profile must be configured for authentication in addition to accounting. 1. Click **Add** > **Create RADIUS**. The Add RADIUS Server window opens. 2. Complete these settings: • **Server Name**—Type the name of the RADIUS server that you want to create. • **Server Address**—Type the IP address of the RADIUS server. • **Authentication Port**—The default RADIUS authentication port is 1812. You can change the port number by using the up and down arrows. • **Secret**—Provide a password. If the password contains spaces, enclose it in quotation marks. The secret password used by the switch must match that used by the server. 3. Expand the Advanced Settings section and change any default settings, including the accounting port: NOTE: If you do not change the accounting configuration, default values are used. • **Accounting Port**—The default RADIUS accounting port is 1813. You can change the port number by using the up and down arrows. • **Retry Count**—Specify the number of times that a device attempts to contact the RADIUS server. The default retry count is 3. You can change this value by using the up and down arrows to 1 through 10 times. • **Timeout** (seconds)—Specify the number of seconds the switch waits to receive a response from the RADIUS server. The default timeout is 5 seconds. You can change this value, using the up and down arrows, to 1 through 90 seconds. 4. Click **OK**. The RADIUS server is automatically added to the list of RADIUS accounting servers assigned to this Access profile. 5. If you have more than one RADIUS server listed, you can use the arrows to reorder the list priority so that the most preferred RADIUS server is listed first.

Copyright © 2013, Juniper Networks, Inc.

Table 29: Accounting Settings for an EX Switching and Data Center Switching Access Profile *(continued)*

Task	Description
Add a previously configured RADIUS server for accounting	A RADIUS server must already be configured before you can add that server for accounting. If the server was previously configured only for authentication, default accounting settings are applied. To add a RADIUS server for accounting: 1. Expand the Accounting Settings section of the Server Settings page. This is where RADIUS accounting is configured. A list of configured RADIUS servers is displayed. 2. Click **Add** > **Select RADIUS**. A list of eligible RADIUS servers is displayed. Servers on this list were either automatically discovered, created using the directions "Creating and Managing RADIUS Profiles" on page 326, or created on this page following the directions *Create and add a new RADIUS server configuration*. If the server was configured only for authentication, default accounting settings were applied—you can use those default settings. 3. Select a RADIUS server from the list of Available servers and then use the arrows to move it to the list of Selected servers. 4. Click **OK**. The RADIUS server is added to the list of accounting servers to be used with this Access profile. If the RADIUS server was previously configured only for authentication, default accounting settings are applied. 5. If you have more than one RADIUS server listed, you can use the arrows to reorder the login priority so that the most preferred RADIUS server is listed first for accounting.
Delete a server	To delete a server from this Access profile: 1. Select a server from the list. 2. Click **Delete**. The server is removed from the list of servers to be used with this Access profile.

Proceed to the Access profile review by clicking either **Review** or **Next**.

Specifying Basic Settings for a Wireless Access Profile

To configure the basic settings for a wireless Access profile, enter the settings described in Table 30 on page 143. Required settings are indicated by a red asterisk (*) that appears next to the field label in the user interface.

Table 30: Access Profile Basic Settings for Wireless

Field	Action
Profile Name	Type the name of the profile.
Description	Type the description of the profile.

Copyright © 2013, Juniper Networks, Inc.

Proceed to the server group settings for wireless Access profiles by either clicking **Server Group Settings** or by clicking **Next**. These settings are described in "Specifying Server Group Settings for a Wireless Access Profile" on page 144.

Specifying Server Group Settings for a Wireless Access Profile

You can add RADIUS or LDAP servers to an Access profile for wireless authentication. You can add a RADIUS profile for accounting.

Copyright © 2013, Juniper Networks, Inc.

To configure RADIUS or LDAP servers for a wireless Access profile, enter the settings described in Table 31 on page 146. Required settings are indicated in the user interface by a red asterisk (*) that appears next to the field label.

Copyright © 2013, Juniper Networks, Inc.

Table 31: Server Group Settings

Field	Action
Configure Server Group	
Group Name	Type a name for the server group.
Server Group Type	Select the type of server group that you want to create: • **Accounting**—Only RADIUS servers perform user accounting services, and they must also be configured for authentication to do accounting. • **Authentication**—Both RADIUS and LDAP servers perform user authentication services. • **Both**—Only RADIUS servers perform both user accounting services and authentication.
Server Type	Select either **RADIUS** or **LDAP**. TIP: If the Server Group Type is accounting, you can select LDAP but accounting will be done with a RADIUS server. LDAP servers do not perform accounting functions.
Enable Load Balance	Select to enable load balancing for the servers that are part of the given server group. Load balancing enables the controller to distribute authentication requests across the authentication servers in a server group. Distributing the authentication process across multiple authentication servers significantly reduces the load on individual servers while increasing resiliency on a system-wide basis.
Server Configuration	
View	Select a server entry from the list and then click **View** to see the details of that entry.

Copyright © 2013, Juniper Networks, Inc.

Table 31: Server Group Settings *(continued)*

Field	Action
Task: Configure a new RADIUS server for this Access profile	To both create and add a RADIUS server to this Access profile: a. Click **Add** > **Create RADIUS**. The Create RADIUS Server window opens. b. Complete these fields: • **Server Name**—Type the name of the RADIUS server that you want to create. • **Server Address**—Type the IP address of the RADIUS server. • **Authentication Port**—The default RADIUS authentication port is 1812. You can change the port number by using the up and down arrows. • **Secret**—Provide a password. If the password contains spaces, enclose it in quotation marks. The secret password used by the switch must match that used by the server. c. Click **OK**. The Create RADIUS Server window closes and the RADIUS server is automatically added to the list of authentication servers assigned to this Access profile. d. Optionally, if you have more than one RADIUS server listed, use the arrows to reorder the list priority so that the most preferred RADIUS server is listed first.
Task: Add a previously configured RADIUS server for authentication	To add a previously configured RADIUS server to this Access profile: a. Click **Add** > **Select RADIUS**. The Select RADIUS Server window opens. b. Select a RADIUS server from the available column—any RADIUS server that you created by using Add > Create RADIUS is listed here. c. Click the right arrow to move the highlighted RADIUS server from the Available column to the Selected column. d. Click **OK**. The Select RADIUS Server window closes and the RADIUS server is added to the list of authentication servers to be used with this Access profile.

Copyright © 2013, Juniper Networks, Inc.

Table 31: Server Group Settings *(continued)*

Field	Action
Task: Configure a new LDAP server for this Access profile	

Copyright © 2013, Juniper Networks, Inc.

Table 31: Server Group Settings *(continued)*

Field	Action
	To both create and add an LDAP server to this Access profile: a. Click **Add** > **Create LDAP**. The Create LDAP Server window opens. b. Complete these fields for an LDAP server: • **Server Name**—Type the name of the LDAP server that you want to create. • **Server Address**—Type the IP address of the LDAP server. • **Server Port**—The default LDAP authentication port is 389. You can change the port number by using the up and down arrows. c. Optionally, expand the Advanced Settings section and provide any of the following advanced LDAP server configuration: • **FQ Domain Name**—A fully qualified domain name specifies an exact location in the tree hierarchy of the Domain Name System (DNS), including all domain levels such as the top-level domain and the root zone. A fully qualified domain name can only be interpreted one way. • **Dead Time**—When a server does not respond for this number of seconds, it is removed from the list of authentication servers for this Access profile. The default dead time is 5 seconds. You can change this value by using the up and down arrows. • **Timeout**—The default timeout is 5 seconds. You can change this value by using the up and down arrows to 1 through 90 seconds. • **Bind Mode**—When an LDAP session is created (LDAP client connects to a server) the authentication state of the session is set to anonymous. BIND mode establishes the authentication state for a session and sets the LDAP protocol version. The default is **Simple bind**—you can change this to **StartTLS bind**. With Simple bind, the users' credentials are sent to the LDAP Directory Service in clear text. With StartTLS bind, the users' credentials are encrypted using Transport Layer Security (TLS) before sending it to the LDAP Directory Service. • **MAC Address Format**—The default address format is **None**, meaning that the MAC address is stated in a single stream, with no subgrouping of the numbers. You can change this setting to **Hyphens**, **Colons**, **One-Hyphen**, or **Raw**. • **Base Domain**—Enter a base domain name, for example, DC=eng, DC=Juniper, or DC=com. • **Domain Prefix**—AD or NT domains use the NetBIOS name. • **Use MAC as Password**—Select this option to use the MAC address of devices as the password for authentication purposes. • **Authorization Password**—If MAC addresses are not used as passwords, provide a password to be used for authentication purposes. d. Click **OK**. The LDAP server is automatically added to the list of authentication servers assigned to this Access profile. e. Optionally, if you have more than one LDAP server listed, use the

Copyright © 2013, Juniper Networks, Inc.

Table 31: Server Group Settings *(continued)*

Field	Action
	arrows to reorder the list priority so that the most preferred LDAP server is listed first.
Task: Add a previously configured LDAP server for authentication	To add a previously configured LDAP server to this Access profile: a. Click **Add** > **Select LDAP**. b. Select an LDAP server from the Available column—any LDAP server that you created by using Add > Create LDAP is listed here in addition to any created with "Creating and Managing LDAP Profiles" on page 273. c. Click the right arrow to move the highlighted LDAP server from the Available column to the Selected column. d. Click **OK**. The LDAP server is added to the list of authentication servers to be used with this Access profile.
Task: Delete any server	To delete a server from this Access profile: a. Select a server from the list. b. Click **Delete**. The server is removed from the list of authentication servers to be used with this Access profile.

The system adds the server details to the Server Configuration table.

NOTE: Use the UP and DOWN arrows to reorder the server groups. User authentication is first attempted with the server listed first. If that authentication fails, the next method on the list is used.

Proceed to the review for wireless Access profiles by either clicking **Review** or by clicking **Next**. For directions for this section, see "Reviewing and Modifying the Access Profile Settings" on page 156.

Copyright © 2013, Juniper Networks, Inc.

Specifying Basic Settings for a Campus Switching ELS Access Profile

To configure the basic settings for a Campus Switching ELS Access profile:

1. Complete the basic settings details and authentication order on the Create Access Profile for Campus Switching ELS page, as described in Table 32 on page 151. Required settings are indicated by a red asterisk (*) that appears next to the field label in the user interface.

Table 32: Access Profile Basic Settings for Campus Switching ELS

Field	Action
Access Profile Details	
Profile Name	Type the name of the profile.
Description	Type the description of the profile.
Authentication Order Server settings depend on which authentication is done first, RADIUS or LDAP.	
Authentication Order	Indicate whether to authenticate first with configured RADIUS servers or with configured LDAP servers by selecting the method from *Based On*. By default, RADIUS authentication using no password is selected for initial authentication. You can change this to RADIUS authentication with a password by selecting **Password**. Select **LDAP** to authenticate first with configured LDAP servers. TIP: LDAP is not supported for Data Center or EX Switching devices.

Proceed to the Server Settings for Campus Switching ELS Access profiles by clicking either **Server Settings** or **Next**. The settings are described in "Specifying RADIUS and LDAP Settings for Campus Switching ELS" on page 151.

Specifying RADIUS and LDAP Settings for Campus Switching ELS

Configure either a RADIUS server, an LDAP server, or both, on the Server Settings page. A RADIUS server can provide both user accounting services and user authentication but you must be using the RADIUS server for authentication in order to use it for accounting. An LDAP server, WHEN AVAILABLE, provides only user authentication. The server settings in this section determine the options used for the access servers in this Access profile.

Configure the Server settings for a Campus Switching ELS Access profile by following the directions in Table 33 on page 152.

Copyright © 2013, Juniper Networks, Inc.

Table 33: Authentication and Accounting Server Settings for ELS Campus Switching

Task	Action
AAA: Authentication Server RADIUS servers are selected for configuration by default. RADIUS servers can do both authentication and accounting.	
View configured servers in this profile	Select a server entry from the list and then click **View** to see the details of that entry.
Create and add a new RADIUS server for authentication	The RADIUS tab is selected by default for AAA Authentication Server configuration. To configure a RADIUS accounting server and add it to this Access profile: 1. Click **Add** > **Create RADIUS** on the RADIUS tab. The Create RADIUS Server window opens. 2. Provide the following RADIUS authentication server details: • **Server Name** • **Server Address** • **Authentication Port**—The default RADIUS authentication port is 1812. You can change the port number by using the up and down arrows. • **Secret**—Provide the authentication secret password. If the password contains spaces, enclose it in quotation marks. The secret password used by the local router must match the one used by the server. 3. Optionally, expand the Advanced Settings for a RADIUS server and change any of these configurations: • **Accounting Port**—You can change the default accounting port number (1813) by using the up and down arrows. • **Retry Count**—Specify the number of times that a device attempts to contact the LDAP authentication server. The default retry count is 3. You can change this value by using the up and down arrows to 1 through 10 times. • **Timeout** (seconds)—Specify the number of seconds the switch waits to receive a response from a RADIUS server. The default timeout is 5 seconds. You can change this value, using the up and down arrows, to 1 through 90 seconds. 4. Click **OK**. The Create RADIUS Server window closes and the RADIUS server is automatically added to the list of RADIUS servers assigned to this Access profile. 5. If you have more than one RADIUS server listed, you can use the arrows to reorder the list priority so that the most preferred RADIUS server is listed first.

Copyright © 2013, Juniper Networks, Inc.

Table 33: Authentication and Accounting Server Settings for ELS Campus Switching *(continued)*

Task	Action
Add a previously configured RADIUS server for authentication	The RADIUS tab is selected by default for server configuration and configured RADIUS servers are listed on this Server Settings page. To add a previously configured RADIUS server to this Access profile: 1. Click **Add** > **Select RADIUS** on the RADIUS tab. The Select RADIUS Server window opens with a list of available RADIUS servers is displayed. Servers on this list were either automatically discovered, created using the directions "Creating and Managing RADIUS Profiles" on page 326, or created on this page following the directions *Create and add a new RADIUS server configuration*. 2. Select one or more RADIUS servers from the list of previously configured RADIUS servers. 3. Click **OK**. The Select RADIUS Server window closes and the RADIUS server is added to the list of RADIUS authentication servers to be used with this Access profile. 4. Optionally, if you have more than one RADIUS server listed, use the arrows to reorder the login priority so that the most preferred RADIUS server is listed first.
Add a previously configured RADIUS server for accounting	A RADIUS server can provide both authentication and accounting. To configure accounting settings for a RADIUS server: TIP: In order to provide accounting, authentication must also be configured. 1. Expand the **RADIUS Accounting Servers** section of the Server Settings. A list of RADIUS servers configured for accounting is displayed. 2. Click **Add** > **Select RADIUS**. The Select RADIUS Server window opens with a list of eligible RADIUS servers is displayed. Servers on this list were either automatically discovered, created using the directions "Creating and Managing RADIUS Profiles" on page 326, or created on this page following the directions *Create and add a new RADIUS server configuration*. 3. Select one or more RADIUS servers from the list of previously configured RADIUS servers. 4. Click **OK**. The Select RADIUS Server window closes and the RADIUS server is added to the list of RADIUS Accounting Servers to be used with this Access profile. 5. Optionally, if you have more than one RADIUS server listed, use the arrows to reorder the login priority so that the most preferred RADIUS server is listed first.

Copyright © 2013, Juniper Networks, Inc.

Table 33: Authentication and Accounting Server Settings for ELS Campus Switching *(continued)*

Task	Action
Create and add a new RADIUS server for both authentication and accounting	RADIUS is the only server selection available for accounting. To configure a RADIUS server for both authentication and accounting, and add it to this Access profile: 1. Under RADIUS Accounting Server, click **Add** > **Create RADIUS**. The Create RADIUS Server window opens. 2. Provide the following RADIUS authentication server details: • **Server Name** • **Server Address** • **Authentication Port**—The default RADIUS authentication port is 1812. You can change the port number by using the up and down arrows. • **Secret**—Provide the authentication secret password. If the password contains spaces, enclose it in quotation marks. The secret password used by the local router must match that used by the server. 3. Expand the Advanced Settings and change any of these configurations: • **Accounting Port**—You can change the default port number (1813) by using the up and down arrows. • **Retry Count**—Specify the number of times that a device attempts to contact the LDAP authentication server. The default retry count is 3. You can change this value by using the up and down arrows to 1 through 10 times. • **Timeout** (seconds)—Specify the number of seconds the switch waits to receive a response from a RADIUS server. The default timeout is 5 seconds. You can change this value, using the up and down arrows, to 1 through 90 seconds. 4. Click **OK**. The Create RADIUS Server window closes and the RADIUS server is automatically added to the list of RADIUS Accounting Servers assigned to this Access profile. 5. If you have more than one RADIUS accounting server listed, you can use the arrows to reorder the list priority so that the most preferred RADIUS server is listed first.

Copyright © 2013, Juniper Networks, Inc.

Table 33: Authentication and Accounting Server Settings for ELS Campus Switching *(continued)*

Task	Action
Create and add a new LDAP authentication server	TIP: LDAP servers can be configured for wireless and for Campus Switching ELS. To configure a new LDAP authentication server and add it to this Access profile: 1. Click the **LDAP** tab to display the LDAP settings. 2. Provide a Base Distinguished Name for the LDAP server. LDAP APIs reference an LDAP object by its distinguished name (DN), which is a sequence of relative distinguished names (RDN) connected by commas—for example, DC=eng, DC=Juniper, DC=com. You can do an LDAP query to determine the DN for the LDAP server. 3. Click **Add** > **Create LDAP**. The Create LDAP Server window opens. 4. Provide the following LDAP server details: • **Server Name** • **Server Address** • **Server Port**—The default LDAP server port is 389. You can change the port number by using the up and down arrows. 5. Optionally provide the following Advanced LDAP server details after expanding the Advanced Settings section: • **Timeout** (seconds)—Specify the number of seconds the switch waits to receive a response from a RADIUS server. The default timeout is 5 seconds. You can change this value, using the up and down arrows, to 1 through 90 seconds. • **Retry**—Specify the number of times that a device attempts to contact the LDAP authentication server. The default retry count is 5. You can change this value by using the up and down arrows to 1 through 10 times. 6. Click **OK**. The Create LDAP Server window closes and the LDAP server is added to the list of LDAP servers.

Copyright © 2013, Juniper Networks, Inc.

Table 33: Authentication and Accounting Server Settings for ELS Campus Switching *(continued)*

Task	Action
Add a previously configured LDAP server for authentication	TIP: LDAP servers can be configured for wireless and for Campus Switching ELS. To add a previously configured LDAP authentication server to this Access profile: 1. Click the **LDAP** tab to display the LDAP settings. 2. Provide a Base Distinguished name for the LDAP server. LDAP APIs reference an LDAP object by its distinguished name (DN), which is a sequence of relative distinguished names (RDN) connected by commas. You can do an LDAP query to determine the DN for the LDAP server. 3. Click **Add** > **Select LDAP**. The Select LDAP Server window opens with a list of configured LDAP servers displayed. Servers on this list were either automatically discovered, or created using the directions "Creating and Managing LDAP Profiles" on page 273, or created using Add > Create LDAP on this page. 4. Select one or more LDAP servers from the list. 5. Click **OK**. The Select LDAP Server window closes and selected LDAP servers are added to the list of LDAP authentication servers to be used with this Access profile. 6. Optionally, use the arrows to reorder the LDAP servers so that the most preferred LDAP server is listed first. TIP: LDAP is not supported for Data Center or EX Switching devices.
Delete a server	To delete any server from this Access profile: 1. Select a server from the list. 2. Click **Delete**. The server is removed from the list of servers to be used with this Access profile.

Proceed to the review for wireless Access profiles by either clicking **Review** or by clicking **Next**. For directions for this section, see "Reviewing and Modifying the Access Profile Settings" on page 156.

Reviewing and Modifying the Access Profile Settings

From this page, you can save or make changes to a Access profile:

- To make changes to the profile, click **Edit** associated with the configuration to be changed.

Copyright © 2013, Juniper Networks, Inc.

Alternatively, you can click the appropriate sections in the profile workflow at the top of the page that corresponds to the configuration to be changed.

When you are finished with your modifications, click **Review** to return to this page.

- To save a new profile or to save modified settings to an existing profile, click **Finish**.

  You will be returned to the Manage Access Profiles page. Your new or modified Access profile is listed in the table of Access profiles.

What To Do Next

After you create an Access profile, you can do one of the following:

- For wireless devices, link the Access profile to an Authentication profile that is created for the same device family. For more details see "Creating and Managing Authentication Profiles" on page 157.
- For switching devices, configure Access profile as a attribute while assigning Port profiles to interfaces. For more details see "Creating and Managing Port Profiles" on page 283.

Related Documentation

- Understanding Access Profiles on page 21
- Creating and Managing LDAP Profiles on page 273
- Creating and Managing RADIUS Profiles on page 326

Creating and Managing Authentication Profiles

Authentication profiles enable specification of the authentication method and authentication parameters to be used for authenticating clients and users who connect to a WLAN or an access port switch.

Use the Manage Authentication Profiles page to create new Authentication profiles and manage existing Authentication profiles.

To display the Manage Authentication Profiles page: In Build mode, select Authentication from Profile and Configuration Management in the Tasks pane. The Manage Authentication Profiles page appears.

This topic describes:

- Managing Authentication Profiles on page 158
- Creating an Authentication Profile on page 159
- Specifying Authentication Settings for Switches on page 160
- Specifying Authentication Settings for Wireless on page 163
- What To Do Next on page 167

Copyright © 2013, Juniper Networks, Inc.

Managing Authentication Profiles

From the Manage Authentication Profiles page, you can:

- Create a new Authentication profile by clicking **Add**. For directions, see "Creating an Authentication Profile" on page 159.
- Modify an existing profile by selecting it and clicking **Edit**.
- View information about a profile, including the interfaces it is associated with, by clicking the profile name or by selecting the profile and clicking **Details**.
- Delete an Authentication profile by selecting a profile and clicking **Delete**.

TIP: You cannot delete profiles that are in use—that is, assigned to objects or used by other profiles. To see the current assignments for a profile, select the profile and click **Details**.

- Clone a profile by selecting a profile and clicking **Clone**.

Table 34 on page 158 describes the information provided about Authentication profiles on the Manage Authentication Profiles page. This page lists all Authentication profiles defined for your network, regardless of the scope you selected in the network view.

Table 34: Manage Authentication Profile Fields

Field	Description
Profile Name	Name given to the profile when the profile was created.
Family Type	The device family on which the profile was created.
Description	Description of the profile that was entered when the profile was created. TIP: To display the entire description, you might need to resize the Description column by clicking the column border in the heading and dragging it.
Creation Time	Date and time when this profile was created.
Update Time	Date and time when this profile was last modified.
User Name	The username of the user who created or modified the profile.

TIP: All columns might not be displayed. To show or hide fields in the Manage Authentication Profiles table, click the down arrow on the field header, select **Columns**, and select or clear the check box adjacent to the field that you want to show or hide.

Copyright © 2013, Juniper Networks, Inc.

Creating an Authentication Profile

In Network Director, you can create an Authentication profile to configure methods to be used to authenticate users. You can also specify details about the accounting servers to be used for accounting purposes.

For an Authentication profile, you must specify the following:

- A profile name
- At least one access rule

After you create an Authentication profile, you can include it in a WLAN profile or a Port profile. The Authentication profile specified in a WLAN profile or a Port profile acts as the default profile for all the users and devices that connect to that WLAN or on the port.

To create an Authentication profile:

1. Click

in the Network Director banner.
2. Under Select View, select either **Logical View**, **Location View**, **Device View** or **Custom Group** View.

   TIP: **Do not select Virtual View or Topology View.**
3. Click **Authentication** under Profile and Configuration Management in the Tasks pane.

   The Manage Authentication Profiles page appears, displaying the list of currently configured Authentication profiles.
4. Click **Add** on the Manage Authentication Profiles page.

   The Device Family Chooser window opens.
5. From the Device Family Chooser, select the device family for which you want to create a profile. The available device families are **Switching (EX)**, **Wireless (WLC)**, **Campus Switching ELS**, and **Data Center Switching Non-ELS**.
6. Click **OK**.

   The Create Authentication Profile window for the selected device family is displayed.
7. Specify authentication settings by doing one of the following:
   - For EX Series switches, Campus Switching Enhanced Layer 2 Software, or Data Center Switching profiles, specify the settings as described in "Specifying Authentication Settings for Switches" on page 160.
   - For controllers, specify the settings as described in "Specifying Authentication Settings for Wireless" on page 163.
8. Click **Done** to save the Authentication profile.

Copyright © 2013, Juniper Networks, Inc.

The system saves the Authentication profile and displays the Manage Authentication Profiles page. Your new or modified Authentication profile is listed in the table of Authentication profiles.

Specifying Authentication Settings for Switches

To configure an Authentication profile for switching devices, enter the Create Authentication Profile page settings described in Table 35 on page 160 for creating Authentication profiles on switches. Required settings are indicated by a red asterisk (*) that appears next to the field label in the user interface.

Table 35: Authentication Profile Settings for Switches

Field	Action
Profile Name	Type the name of the profile.
Description	Type a short description for the profile.
802.1X Authenticator	
Enable 802.1X	802.1X authentication is enabled by default for a switching profile. 802.1X authentication works by using an Authenticator Port Access Entity (the switch) to block all traffic to and from a supplicant (end device) at the port until the supplicant's credentials are presented and matched on the Authentication server (a RADIUS server). When authenticated, the switch stops blocking traffic and opens the port to the supplicant. Network access can be further defined using VLANs. NOTE: If you disable 802.1X authentication, several related settings become unavailable.
Enable MAC-RADIUS	Select to enable MAC-RADIUS based authentication for this profile. MAC RADIUS authentication enables LAN access to permitted MAC addresses. When a new MAC address appears on an interface, the switch consults the RADIUS server to check whether the MAC address is a permitted address. If the MAC address is configured on the RADIUS server, the device is allowed access to the LAN. TIP: You can combine 802.1X and MAC-RADIUS authentication.
Supplicant Mode	Specify the mode authentication supplicants use, either **Single**, **Multiple**, or **Single-Secure**. • **Single**—Allows only one host for authentication. • **Single-Secure**—Allows only one end device to connect to the port. No other end device is enabled to connect until the first logs out. • **Multiple**—Allows multiple hosts for authentication. Each host is checked before being admitted to the network.
Guest VLAN	Click **Select** and then select the VLAN to which an interface is moved when no 802.1X supplicants are connected on the interface. The VLAN specified must already exist on the switch.

Copyright © 2013, Juniper Networks, Inc.

Table 35: Authentication Profile Settings for Switches *(continued)*

Field	Action
Reject VLAN	Click **Select** and then select the VLAN to which an interface is moved when the switch receives an Extensible Authentication Protocol Over LAN (EAPoL) Access-Reject message during the authentication process between the switch and the RADIUS authentication server.
Server Fail Type	Specify the server fail fallback action the switch takes when all RADIUS authentication servers are unreachable, either **None**, **Deny**, **Permit**, **Use cache**, or **VLAN Name**. • **Deny**—Force fail the supplicant authentication. No traffic will flow through the interface. • **Permit**—Force succeed the supplicant authentication. Traffic will flow through the interface as if it were successfully authenticated by the RADIUS server. • **Use cache**—Force succeed the supplicant authentication only if it was previously authenticated successfully. This action ensures that already authenticated supplicants are not affected. • **VLAN Name**—Move supplicant on the interface to the VLAN specified by this name. This action is allowed only if it is the first supplicant connecting to an interface. If an authenticated supplicant is already connected, then the supplicant is not moved to the VLAN and is not authenticated. If you select this option, also provide a **Fail VLAN** name.
Captive Portal A Captive Portal is a special web page used for authentication by turning a web browser into an authentication mechanism.	
Enable Captive-Portal	Enable this option to display the captive portal setting for supplicant mode. When this option is enabled, additional captive portal settings are also available under Advanced Settings.
Supplicant Mode	Specify the mode to be used for Captive Portal supplicants, either **Single**, **Multiple**, or **Single-Secure**. • **Single**—Allows only one host for authentication. • **Multiple**—Allows multiple hosts for authentication. Each host is checked before being admitted to the network. • **Single-Secure** —Allows only one end device to connect to the port. No other end device is allowed to connect until the first logs out.

To skip configuring the advanced settings and accept the default settings, click **Done**. You can now link the Authentication profile to a Port profile. For directions, see "Creating and Managing Port Profiles" on page 283.

To configure advanced switch settings, click **Advanced Settings** and enter the Advanced Settings described in Table 36 on page 162.

Copyright © 2013, Juniper Networks, Inc.

Table 36: Authentication Profile Advanced Settings for Switches

Field	Action
802.1X Settings These settings are available only when 802.1X authentication is enabled for this Authentication profile. You can use the default settings or you can change them.	
Transmit Period (default is 30 seconds)	Specify how long, in seconds, the interface waits before retransmitting the initial EAPOL PDUs to the supplicant. The default is 30 seconds.
Maximum Requests (default is 2 requests)	Specify the maximum number of times an EAPOL request packet is transmitted to the supplicant before the authentication session times out. The default is 2 requests.
Retries (default is 3 retries)	Specify the number of times you want the switch to attempt to authenticate the port after an initial failure. The port remains in a wait state during the quiet period after the authentication attempt. The default is 3 retries.
Quiet Period (default is 60 seconds)	Specify the number of seconds the interface remains in the wait state following a failed authentication attempt by a supplicant before reattempting authentication. The default is 60 seconds.
No Reauthentication (default is unselected)	Select this check box if you do not want the switch to reauthenticate the supplicant after the Quiet Period elapses.
Reauthentication Interval (default is 3600 seconds)	If the No Reauthentication option is not checked, specify the number of seconds after which the authentication session times out. The default is 3600 seconds.
Supplicant Timeout (default is 30 seconds)	Specify how long the port waits for a response when relaying a request from the authentication server to the supplicant before resending the request. The default is 30 seconds.
RADIUS Server Timeout (default is 30 seconds)	Specify the length of time that the switch waits for a response from the RADIUS server. The default is 30 seconds.
MAC Restrict (Switches using MAC RADIUS only)	When MAC-RADIUS is enabled in this Authentication profile, select this option to restrict authentication to MAC RADIUS only. When MAC-RADIUS restrict is configured, the switch drops all 802.1X packets. This option is useful when no other 802.1X authentication methods, such as guest VLAN, are needed on the interface, and eliminates the delay that occurs while the switch determines that a connected device is a non-802.1X-enabled host. Optionally enable **Flap-On-Disconnect**. When the RADIUS server sends a disconnect message to a supplicant, the switch resets the interface on which the supplicant is authenticated. If the interface is configured for multiple supplicant mode, the switch resets all the supplicants on the specified interface. This option takes effect only when the MAC Restrict option is also set.
Captive Portal If Captive Portal is enabled in this Authentication profile in the basic settings, you can either use the default advanced Captive Portal settings or change them as indicated.	

Copyright © 2013, Juniper Networks, Inc.

Table 36: Authentication Profile Advanced Settings for Switches *(continued)*

Field	Action
Quiet Period (default is 60 seconds)	Configure the time, in seconds, between when a user exceeds the maximum number of retries and when they can again attempt to authenticate. Range: 1 through 65,535 Default: 60
Retries (default is 3 retries)	Configure the number of times the user can attempt to submit authentication information. Range: 1 through 65,535 Default: 3
Session Expiry (default is 3600 seconds)	Configure the maximum duration in seconds of a session. Range: 1 through 65,535 Default: 3600
Server Time Out (default is 30 seconds)	Configure the time in seconds an interface will wait for a reply when relaying a response from the client to the authentication server before timing out and invoking the server-fail action. Range: 1 through 65,535 Default: 30

Click **OK**.

The Advanced Settings window closes and you once again see the Create Authentication Profile for Switching page.

Click **Done**.

The Manage Authentication Profiles page reappears with your new Authentication profile listed.

You can now link the Authentication profile to a Port profile. For more details, see "Creating and Managing Port Profiles" on page 283.

Specifying Authentication Settings for Wireless

While configuring an Authentication profile for wireless devices, you define one or more access rules. Each access rule is specific to an access type or authentication mechanism, such as 802.1X, MAC, Web, and open authentication. All authentication mechanisms are supported in a chain and are allowed in any sequence with one exception—Web authentication and Open authentication must not be configured simultaneously in one Authentication profile.

Copyright © 2013, Juniper Networks, Inc.

To configure an Authentication profile for wireless:

1. Enter the wireless authentication settings described in Table 37 on page 164. Required settings are indicated by a red asterisk (*) that appears next to the field label in the user interface.

Table 37: Authentication Profile Wireless Settings

Field	Description
Profile Name	Type the name of the profile.
Description	Type the description of the profile.

2. Add at least one access rule by clicking **Add** under Access Rule.

   The Add Access Rules window opens.

3. Enter the access rule settings described in Table 38 on page 164. Required settings are indicated by a red asterisk (*) that appears next to the field label in the user interface.

Table 38: Wireless Access Rule Settings

Field	Description
Access Type	Select the type of access for the rule, either **802.1X Access** (default), **MAC Access**, **Web Access**, or **Open Access**: • **802.1X Access**—Select to authenticate the client using 802.1X authentication method. For more information, see "Understanding the IEEE 802.11 Standard for Wireless Networks" on page 100. • **MAC Access**—Select to authenticate the client using MAC RADIUS authentication method. • **Web Access**—Select to have the client log in to a web page before granting access to the SSID. • **Open Access**—Select to automatically authenticate the client and enable access to the SSID requested by the client, without requiring a username and password from the client. If you select open access as the access type, you must either *enable local accounting* or *specify an Access profile* to be able to save the access rule. The remaining options in this window vary, depending on which Access Type you choose.

Copyright © 2013, Juniper Networks, Inc.

Table 38: Wireless Access Rule Settings *(continued)*

Field	Description
Matching Glob (all)	Type the user glob for the access rule. A user glob is shorthand method for matching an authentication, authorization, and accounting (AAA) command to either a single user or a set of users. A user glob can contain up to 80 characters long and cannot include spaces or tabs. The double-asterisk (**) wildcard characters with no delimiter characters match all user names. The single-asterisk (*) wildcard character matches any number of characters up to, but not including, a delimiter character in the glob. Valid user glob delimiter characters are the at (@) sign and the period (.). NOTE: The matching glob value that you specify must be unique and cannot be used for any other access rules within the given authentication profile.
EAP Type (801.X Access)	If you selected **802.1X Access**, you also need to indicate an EAP type. Extensible Authentication Protocol (EAP) is a generic point-to-point protocol that supports multiple authentication mechanisms. Select the EAP type that you want to use for this access rule: • **PEAP Offload**—Select if you want to offload all EAP processing from server groups. In this case, the RADIUS server is not required to communicate using the EAP protocols. • **Local EAP-TLS**—Select if you want to use a local database to authenticate clients. EAP-TLS provides encryption and data integrity checking for the connection. Local EAP-TLS can only be used with Local Authentication. • **External Authentication Server**(default)—Select if you want to use an external server for authentication. NOTE: If you select to use an external server for authentication, you must not select the **Enable Local Authentication**.
Enable Authentication	Selected by default to enable authentication for this access rule.
Enable Local Authentication	Select to have users authenticated against the local database on the controller. TIP: Network Director displays this check box only if you selected **Enable Authentication**.
MAC Prefix (MAC Access)	If MAC Access is the access type, you can enable MAC prefix authentication.

Copyright © 2013, Juniper Networks, Inc.

Table 38: Wireless Access Rule Settings *(continued)*

Field	Description

Enable Accounting	Select to enable accounting for this access rule and display the accounting settings. Accounting collects and sends information used for billing, auditing, and reporting. Accounting can be done using RADIUS or by using local accounting.
	
	If **Enable Accounting** is selected, you can configure these additional accounting parameters:
	
	• **Enable Local Accounting**—Select if you want to enable local accounting. If you select local accounting, the accounting information is stored locally on the controller.
	• **Record Type**—Select the local accounting mode to be used for this access rule:
	  ◦ **Start-Stop**—When this mode is selected, a start record is generated when a user is first connected, and an update record is generated when a user roams from one wireless access point to another. A stop record is generated when a user terminates the session.
	  ◦ **Stop-Only**—When this mode is selected, a stop record is generated when a user terminates the session.

Access Profile	Specify an Access profile (default is **None**) to use for this access rule. Network Director displays the Access Profile field when you have enabled authentication, accounting, or both, for the given access rule. Specify an Access profile for each access rule, unless: • **Open Access** is the access type. • **802.1X Access** is the access type and **Local EAP-TLS** as the EAP type.

4. Click **OK** to save and add the wireless access rule to the list of access rules in the Create Authentication Profile page. You can create one or more access rules and authenticate each user or device group differently depending on your security policy and requirements.
5. You can configure a wireless web portal by providing the information listed in Table 39 on page 166.

Table 39: Wireless Web Portal Authentication

Web Portal Settings A web portal is a web site that brings information together from diverse sources in a uniform way. The following Web Portal settings are valid only when the corresponding WLAN Service Profile has Fall Through Access set to **web-portal**. See "Creating and Managing a WLAN Service Profile" on page 350 for more information and directions.	
Web Portal Login Page	Type the name of a Web portal login page, for example, *http://www.example.com*. Web traffic will be directed to this location for logging into the Web portal. For more information about Web login, see "Configuring Web Portal Web AAA" in the *Mobility System Software Configuration Guide*. TIP: Web Portal settings are valid only when Fall Through Access is set to **WEB Portal** in a WLAN Service Profile. When you link this Authentication Profile to a WLAN Service Profile with Fall Through Access set to **WEB Portal**, the settings are used.

Copyright © 2013, Juniper Networks, Inc.

Table 39: Wireless Web Portal Authentication *(continued)*

Web Portal Logout	Optionally, enable Web Portal Logout, and provide the name of the Web Portal Logout Page, for example, *http://www.example.com*.

6. Click **Done**.

   The Manage Authentication Profiles for Wireless (WLC) page reappears with your new wireless Authentication profile listed. You can now link the Authentication profile to a WLAN profile. For more details, see "Creating and Managing a WLAN Service Profile" on page 350.

What To Do Next

After you create an Authentication profile, you can do the following:

- For switching devices, link the Authentication profile to a Port profile. For more details, see "Creating and Managing Port Profiles" on page 283.
- For wireless devices, link the Authentication profile to a WLAN profile. For more details, see "Creating and Managing a WLAN Service Profile" on page 350.

Related Documentation

- Understanding Authentication Profiles on page 22
- Creating and Managing Port Profiles on page 283
- Creating and Managing a WLAN Service Profile on page 350

Creating and Managing Wireless Authorization Profiles

Authorization profiles specify the access permission for authenticated users or devices.

Use the Manage Authorization Profiles page to create new wireless Authorization profiles and manage existing wireless Authorization profiles.

To display the Manage Authorization Profiles page: In Build mode, select Authorization from Profile and Configuration Management in the Tasks pane. The Manage Authorization Profiles page appears.

This topic describes:

- Managing Authorization Profiles on page 168
- Creating a Wireless Authorization Profile on page 169
- Specifying Settings for a Wireless Authorization Profile on page 171
- What To Do Next on page 174

Copyright © 2013, Juniper Networks, Inc.

Managing Authorization Profiles

From the Manage Authorization Profiles page, you can:

- Create a new wireless Authorization profile by clicking **Add**. For directions, see "Creating a Wireless Authorization Profile" on page 169.
- Modify an existing Authorization profile by selecting it and clicking **Edit**.
- Associate an Authorization profile to specific devices or clusters by selecting it and clicking **Assign**. For directions, see "Assigning Authorization Profiles to Controllers" on page 369.
- Change the current assignment of an Authorization profile by selecting it and clicking **Edit Assignment**. For directions, see "Assigning Authorization Profiles to Controllers" on page 369.
- View information about an Authorization profile, including the interfaces it is associated with, by clicking the profile name or by selecting the profile and clicking **Details**.
- Delete an Authorization profile by selecting a profile and clicking **Delete**.

TIP: You cannot delete profiles that are in use—that is, assigned to objects or used by other profiles. To see the current assignments for an Authorization profile, select the Authorization profile and click Details.

- Clone a profile by selecting a profile and clicking **Clone**.

Table 40 on page 168 describes the information provided about Authorization profiles on the Manage Authorization Profiles page. This page lists all Authorization profiles defined for your network, regardless of the scope you selected in the network view.

Table 40: Manage Authorization Profile Fields

Field	Description
Profile Name	Name given to the profile when the profile was created.
Family Type	The device family on which the profile was created.
VLAN Profile	The required VLAN profile associated with the Authorization profile. You specify a VLAN profile while creating an Authorization profile. For directions, see "Creating and Managing VLAN Profiles" on page 330.
CoS Profile	The optional CoS profile associated with the Authorization profile. For directions, see "Creating and Managing CoS Profiles" on page 184.
Description	Description of the profile that was entered when the profile was created. TIP: To display the entire description, you might need to resize the Description column by clicking the column border in the heading and dragging it.

Copyright © 2013, Juniper Networks, Inc.

Table 40: Manage Authorization Profile Fields *(continued)*

Assignment State	Displays the assignment state of the profile. A profile can be: • Unassigned—When the profile is not assigned to any object • Assigned—When the profile is assigned, but not deployed in the network. • Deployed—When the profile is assigned and is deployed from the Deploy mode • Pending Deployment—When the profile is assigned, but not yet deployed in the network.
Creation Time	Date and time when this profile was created.
Update Time	Date and time when this profile was last modified.
User Name	The username of the user who created or modified the profile.

TIP: All columns may not be displayed—this is configurable. To show or hide fields listed in the Manage Authorization Profiles table, click the down arrow on the field header, select Columns, and select or clear the check box adjacent to the field that you want to show or hide.

Creating a Wireless Authorization Profile

In Network Director, you can create a wireless Authorization profile with access permissions for either wireless users or devices. You can also link a VLAN profile and a CoS profile to the Authorization profile to ensure that each user session is assigned to an appropriate VLAN and it gets the required class-of-service.

For an Authorization profile, you must specify the following:

- A profile name
- An associated VLAN profile

You can optionally specify additional configurations such as:

- An associated CoS profile
- Ingress and egress Filter profiles
- User and session timeouts
- Accounting update interval
- Timeout action
- Encryption settings
- Date and time restrictions for accessing the network

Copyright © 2013, Juniper Networks, Inc.

To create an Authorization profile for wireless users or devices:

1. Click in the Network Director banner.
2. Under Select View, select either **Logical View**, **Location View**, **Device View** or **Custom Group** View.

   TIP: **Do not select Virtual View or Topology View.**

3. Click **Authorization** under Profile and Configuration Management in the Tasks pane.

   The Manage Authorization Profiles page appears, displaying the list of currently configured wireless Authorization profiles.

4. Click **Add**.

   The Create Authorization Profile for Wireless page appears.

5. Specify the settings as described in the "Specifying Settings for a Wireless Authorization Profile" on page 171.
6. Click **Done** to save the Authorization profile.

   The system saves the Authorization profile and displays the Manage Authorization Profiles page. Your new or modified Authorization profile is listed in the table of Authorization profiles.

Copyright © 2013, Juniper Networks, Inc.

Specifying Settings for a Wireless Authorization Profile

While creating an Authorization profile, you will have to specify a VLAN profile. Make sure that you have created a wireless VLAN profile before you attempt to create an Authorization profile. For directions, see "Creating and Managing VLAN Profiles" on page 330.

Copyright © 2013, Juniper Networks, Inc.

1. Enter the settings described in Table 41 on page 172 to create an Authorization profile. Required settings are indicated by a red asterisk (*) that appears next to the field label in the user interface.

Table 41: Authorization Profile Basic Settings (WLC)

Field	Action
Name	Type the name of the profile.
Description	Type a short description for the profile.
VLAN Profile	Click **Select** and then select a VLAN profile to include in the Authorization profile. When a VLAN profile is applied to a port or a wireless access point, the VLAN is initiated when clients are connected and are authorized on the VLAN.
CoS Profile	Click **Select** and then select an optional CoS profile to include in the Authorization profile. CoS profiles enable the grouping of class of service parameters and the application of it to one or more network sessions. You can configure policers, classifiers, scheduler maps, rewrite rules and a traffic-control profile within CoS-profile.
Filters	
Ingress Filter	Click **Select** and then select a Filter profile to filter traffic that enters the controller from users through an access port, from a wired authentication port, or from the network through a network port.
Egress Filter	Click **Select** and then select a Filter profile to filter traffic sent from the controller to users through an access port, from a wired authentication port, or from the network through a network port.
Simultaneous Login	Restrict the number of concurrent sessions that a user can have on the network, by selecting the number of concurrent sessions for users of this Authorization profile.
Service Type	Select the type of access that you want the users of the Authorization profile to have: • 2 (Framed)—Select to grant network user access. • 6 (Administrative)—Select to grant administrative access to the controller with authorization to access enabled (configuration) mode. The user must enter the enable command and the correct enable password to access enabled mode. • 7 (NAS-Prompt)—Select to grant administrative access to nonenabled mode only. In this mode, a user cannot enter the enable command nor the enable password to access the enabled mode.

To configure advanced settings, click **Advanced Settings**. To skip changing the default advanced settings and save the profile, click **Done**.

2. Enter the advanced settings described in Table 42 on page 173 to modify the default

Copyright © 2013, Juniper Networks, Inc.

advanced settings for the Authorization profile.

Table 42: Authorization Profile Advanced Settings (WLC)

Field	Action
User Idle Timeout (default is 3600 seconds)	Specify the length of time that a user or device can remain idle before the controller disconnects the user or device.
Session Timeout (default is 180 seconds)	Specify the length of time a user or device can remain connected to the network before re-authenticating the session.
Termination Action	Select the action to be taken when the session expires: • **0 (Disconnect)**—Select to indicate that the session is to be terminated. • **1 (Re-authenticate)**—Select to indicate that the user or device must reauthenticate when the session expires.
Uniform Resource Locator (URL)	Specify the URL that the user is to be redirected after successful authentication. Use the following format: *http://www.example.com*
Accounting Interim Interval	
Enable Updates Update Interval (default is 180 seconds)	Select **Enable Updates** to enable accounting updates for the Authorization profile. TIP: Accounting updates are applicable only if you have enabled accounting and selected START-STOP as the record type in the corresponding Authentication profile. If updates are enabled. you can modify the time in seconds between accounting updates. Specify a value from 180 through 3,600 seconds. NOTE: If both a RADIUS server and a controller supply a value for the Accounting Interim Interval, then the value from the controller takes precedence.
Encryption Type	
Encryption Type	Select the type of encryption supported for clients using this Authorization profile. You can select a combination of encryption types. Clients who attempt to use an unauthorized encryption method are rejected. Network Director supports the following encryption types: • **AES-CCMP**—AES-CCMP (Advanced Encryption Standard using Counter with CBC-MAC) is the standard encryption protocol for use with the WPA2 standard and is much more secure than the TKIP protocol. • **TKIP**—TKIP (Temporal Key Integrity Protocol) is a security protocol used in the IEEE 802.11 wireless networking standard. It uses the same underlying mechanism as the original WEP encryption, and consequently is vulnerable to the same attacks that WEP is vulnerable to. • **None**—No encryption is used.

Copyright © 2013, Juniper Networks, Inc.

Table 42: Authorization Profile Advanced Settings (WLC) *(continued)*

Field	Action
Start and End Dates for Authorization	
Start Date	Select the date and 24-hour time from which users of this authorization profile are authorized to access the network.
End Date	Select the last date and 24-hour time that users of this authorization profile are authorized to access the network.
Time of Day Settings	
Time of Day	Indicate the time of day the user is permitted to log into the network. The default is **Any** and the other options are **Never** and **Day**.

3. Click **OK** to save the advanced settings and close the Advanced Settings window.
4. Click **Done** to save the authorization profile and add it to the Manage Authorization Profiles list.

What To Do Next

After you have created an Authorization profile, you can:

- Associate it with a WLAN profile. For directions, see "Creating and Managing a WLAN Service Profile" on page 350.
- Assign it to one or more controllers. For directions, see "Assigning Authorization Profiles to Controllers" on page 369.

Related Documentation

- Understanding Authorization Profiles on page 24
- Assigning Authorization Profiles to Controllers on page 369
- Creating and Managing a WLAN Service Profile on page 350

Creating and Managing Wireless Auto AP Profiles

An Auto AP profile is a set of configurations applied to access points on a controller that have not been specifically configured. These access points were, instead, discovered by the controller. If you create an Auto AP profile, then assign and deploy the Auto AP profile to a controller, that controller applies the Auto AP profile to any access points that are discovered. If the access point is not seen by the controller at any point, the Auto AP configured access point is removed from the list of access points—they have no persistent configuration on the controller. For more information about Auto AP profiles, see "Understanding Auto AP Profiles" on page 24.

NOTE: A controller can have only one Auto AP profile assigned.

Copyright © 2013, Juniper Networks, Inc.

If you do not want an Auto-AP profile applied to access points, you can add and configure individual access points by "Adding and Managing an Access Point" on page 126.

This topic describes:

- Managing Wireless Auto AP Profiles on page 175
- Creating a Wireless Auto AP Profile on page 177
- Specifying Basic Settings for a Wireless Auto AP Profile on page 178
- Specifying LLDP & Remote AP Settings for a Wireless Auto AP Profile on page 179
- Specifying Advanced Settings for a Wireless Auto AP Profile on page 181
- Reviewing a Wireless Auto AP Profile on page 183
- What To Do Next on page 183

Managing Wireless Auto AP Profiles

From the Manage Auto AP Profiles page, you can:

- Configure one Auto AP profile per controller by selecting a controller in the View pane, and then clicking **Add**. For directions, see "Creating a Wireless Auto AP Profile" on page 177.
- Modify an existing Auto AP profile by selecting it and clicking **Edit**.
- **Assign** an existing Auto AP profile to a controller.
- Edit the assignment of an Auto AP profile to a controller by selecting the profile and clicking **Edit Assignment**.
- View the current assignments for a profile by selecting the profile and clicking **Details**.
- Delete an Auto AP profile by selecting a profile and clicking **Delete**.

TIP: **You cannot delete a profile that is in use—that is, assigned to access points.**

- Clone a profile by selecting a profile and clicking **Clone**.

Table 43 on page 175 describes the information provided about an Auto AP profile on the Manage Auto AP Profiles page.

Table 43: Manage Auto AP Profiles Fields

Field	Description
Profile Name	Name given to the Auto AP profile when the profile was created.
Device Family	Wireless (controller)
Description	Any description provided during creation of the Auto AP profile.

Copyright © 2013, Juniper Networks, Inc.

Table 43: Manage Auto AP Profiles Fields *(continued)*

Field	Description
Enable Auto AP	Indicates whether the Auto AP profile is enabled or disabled.
Assignment State	Indicates whether or not the Auto AP profile is deployed to a controller.
Creation Time	Date and time when this profile was created.
Last Updated Time	Date and time when this profile was last modified.
User Name	The username of the user who created or modified the profile.

TIP: Some columns might be hidden—this is configurable. To show or hide fields listed in the Manage Authorization Profiles table, click the down arrow on the field header, select **Columns**, and select or clear the check box adjacent to the field that you want to show or hide.

Copyright © 2013, Juniper Networks, Inc.

Creating a Wireless Auto AP Profile

In Network Director, you can configure an automatic AP profile and assign it to a controller. This Auto AP profile becomes the default configuration for all access points that are discovered but not configured on the controller. This way, all access points, even those not configured by you, have a configuration. The Auto AP profile will also act as a template if you convert an Auto AP to a configured, persistent access point.

At minimum, when creating an Auto AP, you must specify a profile name, and also provide the names of an associated VLAN Profile and a Radio profile. You can use default settings for the rest of the Auto AP profile, or you can optionally change or add Auto AP profile configurations such as:

- Radio Type
- AP bias for the controller
- Radio mode (enabled, disabled, or sentry) for each radio
- Radio profile for each radio
- LLDP settings
- Remote AP settings for outage duration and connection evaluation
- Blinking
- Data Security
- High latency mode
- Automatic firmware updates
- Local switching tunnel settings
- Associated VLAN profiles

To create an Auto AP profile:

1. Click

in the Network Director banner.
2. Under Select View, select either **Logical View**, **Location View**, **Device View** or **Custom Group** View.

   TIP: **Do not select Virtual View or Topology View.**
3. Click **Auto AP** under Profile and Configuration Management in the Tasks pane.

   The Manage Auto AP Profiles page opens, displaying the list of currently configured Auto AP profiles.
4. Click **Add**.

   The Create Auto AP Profile for Wireless Controllers (WLC) wizard opens. The wizard has four sections, Basic Settings (this one is selected), LLDP & Remote AP Settings, Advanced Settings, and Review.

Copyright © 2013, Juniper Networks, Inc.

5. Complete the sections of the Auto AP wizard described in both online help and "Specifying Basic Settings for a Wireless Auto AP Profile" on page 178, "Specifying LLDP & Remote AP Settings for a Wireless Auto AP Profile" on page 179, "Specifying Advanced Settings for a Wireless Auto AP Profile" on page 181, and "Reviewing a Wireless Auto AP Profile" on page 183.
6. Click **Finish**.

   The Auto AP profile is added to the list of Auto AP profiles.

Next, assign the Auto AP configuration to one or more controllers, following the directions "Assigning an Auto AP Profile to Controllers" on page 371.

Specifying Basic Settings for a Wireless Auto AP Profile

For an Auto AP in use (either enabled or in sentry mode), the required basic Auto AP profile settings are a name for the profile and a reference to a Radio profile for each radio—for the rest of the settings, you can use the default settings.

The basic settings for the Auto AP profile are described in Table 44 on page 178. Required settings are indicated by a red asterisk (*) that appears next to the field label in the user interface.

Table 44: Wireless Auto AP Basic Settings

Field	Description
Profile Name	The Auto AP profile name can consist of up to 32 characters with no special characters other than _ - (underscore or dash).
Description	Optionally provide up to 255 characters.
Enable Auto AP (default is enabled)	Clear this check box to disable Auto AP without deleting the Auto AP profile.
Radio Type (default is 802.11g)	Radio type applied to radios with no other specific configuration. Select **802.11a**, **802.11b**, or **802.11g**. For more explanation, see "Understanding the IEEE 802.11 Standard for Wireless Networks" on page 100.
Bias (default is High)	Select **High**, **Low**, or **Low-Sticky** bias. Bias matters only for access points indirectly connected to the controller through an intermediate layer 2 or layer 3 network. An access point always attempts to boot on AP port 1 first, and if a controller is directly attached on AP port 1, the access point boots from there regardless of the bias settings. Set the access point's bias to **High** or **Low** for the controllers in this profile. Alternately, set the bias to **Low-Sticky** to have the access point continue to use the current controller for the active data link even if another controller configured with high bias becomes available. For more explanation, see "Understanding Access Point Bias for Controllers" on page 84.

Radio Settings

If an access point has two radios, both Radio 1 and Radio 2 are displayed and can be reconfigured from the defaults.

Copyright © 2013, Juniper Networks, Inc.

Table 44: Wireless Auto AP Basic Settings *(continued)*

Field	Description
Radio Type (default is 802.11g for Radio 1 and 802.11a for Radio 2)	Radio type applied to each radio that has no other specific configuration. Select either **802.11a**, **802.11b**, or **802.11g**.
Radio Mode (default is Disabled)	Radio mode defines the functioning state of the radios in this profile. Select **Sentry** or **Enabled** to enable the radios. Select **Disabled** to disable the radios. TIP: A radio in sentry mode scans for interference but does not transmit user traffic.
Radio Profile	A controller needs a Radio profile if radio mode is set to either Enabled or Sentry. Provide the name of an associated Radio profile. For more explanation, see "Understanding Radio Profiles" on page 42. To create a Radio profile, see "Creating and Managing a Radio Profile" on page 315. TIP: To avoid failure during deployment, select a Radio Profile if the Radio Mode is enabled for any of the radios.

Click either **Next** or **LLDP & Remote AP Settings** to continue configuring the Auto AP. Follow the directions "Specifying LLDP & Remote AP Settings for a Wireless Auto AP Profile" on page 179 to complete that section of the wizard.

Specifying LLDP & Remote AP Settings for a Wireless Auto AP Profile

To configure the LLDP & Remote AP Settings for the Auto AP profile, enter the settings described in Table 45 on page 179.

Table 45: Wireless Auto AP LLDP & Remote AP Settings

Field	Description
LLDP Settings Link Layer Discovery Protocol (LLDP) is a Layer 2 protocol that enables a network device to advertise its identity and capabilities on the local network. These attributes are used to discover neighbor devices. The attributes contain type, length, and value descriptions and are referred to as type-length-values (TLVs). Devices that support LLDP use TLVs to receive and send information to neighboring devices. Details such as configuration information, device capabilities, and device identity can be advertised using this protocol.	
LLDP Mode (default is TX)	Select either transmit (**TX**) or **None** to specify the LLDP operational mode on access points. Link Layer Discovery Protocol (LLDP) is a link layer protocol used by network devices for advertising their identity, capabilities, and neighbors on a WLAN. NOTE: LLDP and LLDP-MED cannot operate simultaneously on a network. By default, a network device sends only LLDP packets until LLDP-MED packets are received from an endpoint device, after which the network device sends out LLDP-MED packets until it receives LLDP packets.

Copyright © 2013, Juniper Networks, Inc.

Table 45: Wireless Auto AP LLDP & Remote AP Settings *(continued)*

Field	Description
LLDP-MED Mode (default is enabled)	LLDP-MED, an extension to LLDP that operates between endpoint devices such as IP phones, and network devices, such as switches, is enabled by default. Specifically, it provides support for voice over IP (VoIP) applications and provides additional TLVs for the capabilities discover, network policy, Power over Ethernet (PoE), and inventory management. Options are enabled and disabled. NOTE: LLDP and LLDP-MED cannot operate simultaneously on a network. By default, a network device sends only LLDP packets until LLDP-MED packets are received from an endpoint device, after which the network device sends out LLDP-MED packets until it receives LLDP packets.
Power via MDI (default is disabled)	Select **Enable** to have LLDP-MED use the medium dependent interface (MDI) power management TLV for power over Ethernet (PoE).
Enable Inventory (default is disabled)	Select **Enable Inventory** to have LLDP-MED use the Inventory TLV, enabling you to track inventory for network devices, including their manufacturer, software and hardware versions, and serial or asset number. Options for inventory are enabled and disabled if you have enabled LLDP-MED.
Enable Remote AP Settings Remote AP Settings, enabled by default, apply to access points connected by a WAN link to a central network. If the WAN link becomes unavailable, then the remote sites with access points remain active and continue to provide connectivity to wireless clients, using the settings indicated here.	
Outage Duration (default is 0 hours)	Select the amount of time in hours that remote sites with access points should remain active and continue to provide connectivity to wireless clients if the WAN link becomes unavailable. If Enable Remote AP Settings is selected, outage duration indicates the number of hours that access points remain in outage mode once they lose connection with a controller. The valid times are from 0 to 120 hours (5 days). The default setting, zero, means access points stay in outage mode indefinitely.
Connection Evaluation Period (default is 300 seconds)	Select the amount of time in seconds that a keep-alive interval of pings is sent to detect an active link for remote access points. The default value is 300 seconds and the range is 5 through 86400 seconds. When Enable Remote AP Settings is selected and an outage occurs, a periodic timer sends discovery messages to the primary access manager (PAM) to determine when the controller is available on the network again. This timer, called an evaluation timer, is configurable and can be used as a hold-down timer to confirm detection of the WAN outage and as a mechanism to detect when the connection is restored.

Copyright © 2013, Juniper Networks, Inc.

Click either **Next** or **Advanced Settings** to continue configuring the Auto AP. Follow the directions "Specifying Advanced Settings for a Wireless Auto AP Profile" on page 181 to complete that section of the wizard.

Specifying Advanced Settings for a Wireless Auto AP Profile

Advanced Auto AP settings include broadcast settings, client types, and voice configuration. The only required configuration here is the name of a VLAN profile to use with the Auto AP profile. Table 46 on page 181 lists the advanced settings and how to configure them.

Table 46: Wireless Auto AP Profile Advanced Settings

Field	Action
Blink (disabled by default)	Enable LED blink mode on access points to make them easy to identify. When blink mode is enabled on supporting models, the health and radio LEDs alternately blink green and amber. When blink mode is enabled on an AP2750, the 802.11a LED blinks on and off.
Data Security (disabled by default)	Enable data security to configure access points with data path encryption.
High Latency Mode (disabled by default)	Enable high latency mode to mitigate access point association problems on a high latency network.
Firmware Update (enabled by default)	Disable this option if you do not want the controller to update access points with firmware upgrades.
LED Mode (default is Auto)	Select the LED behavior for access points in this profile, **Auto**, **Static**, or **Off**. **Auto** is standard behavior. **Static** LEDs do not flash when traffic is on the network but all other behavior is standard. Selecting **Off** turns LEDs off.
AP Communication Timeout (default is 25 seconds)	Indicate the length of time in seconds that an access point waits for communication from a controller before timing out.

Copyright © 2013, Juniper Networks, Inc.

Table 46: Wireless Auto AP Profile Advanced Settings *(continued)*

Field	Action	
Enable Local Switching (default is enabled)	Local switching causes traffic that was tunneled to a controller to be locally switched by access points. Local switching includes the following additional settings:	
	Tunnel Affinity (default is 4)	If Local Switching is enabled, tunnel affinity enables access points with Local Switching enabled to create and terminate client VLAN tunnels—a VLAN is not required on these access points. Affinity is the capacity that an AP has for tunnels. An AP can have affinity for 0 (none) to 10 tunnels, with the default of 4 tunnels. Zero indicates that the access point is not used as a tunnel endpoint.
	AP Tunneling (default is disabled)	If Local Switching is enabled, AP Tunneling configures tunneling on the access points in this profile. If a client connects to an access point that has local switching enabled on a VLAN, and the VLAN does not exist in the VLAN profile, then the client connects in overlay mode. This setting enables clients to still connect if the tunnel limits (set by the Tunnel Affinity value) are reached. If a client cannot connect, an appropriate error message is recorded in the event log.
	VLAN Profiles When a VLAN profile is applied to an access point, traffic for that VLAN is locally switched by the access point—that is, traffic directly exits the access point into the VLAN instead of tunneling back to a controller for switching.	
	Add a VLAN profile to this Auto AP profile	

Copyright © 2013, Juniper Networks, Inc.

Table 46: Wireless Auto AP Profile Advanced Settings *(continued)*

Field	Action
	If Local Switching is enabled, you can apply a VLAN profile to access points to use with local switching: 1. Click **Add**. 2. Select an existing VLAN profile from the list. 3. Click **OK**. The VLAN profile is now associated with this Auto AP profile and will be used to locally switch traffic between access points. The VLAN profile name, VLAN name, device family, VLAN ID and device description are added to the list of VLAN profiles.
Remove	If Local Switching is enabled and a VLAN has been added here, you can select a VLAN profile from the list, and then click **Remove** to remove the VLAN from local switching in this Auto AP profile.

Click either **Next** or **Review** to continue configuring the Auto AP. Follow the directions "Reviewing a Wireless Auto AP Profile" on page 183 to complete that section of the wizard.

Reviewing a Wireless Auto AP Profile

Before you create the Auto AP profile, check the configuration:

1. Review your Auto AP service profile selections by scrolling to the bottom of the screen.
2. Make any needed changes by clicking **Edit** in the appropriate section. Make the changes, and then return to the Review tab.
3. Click **Finish**. The Auto AP profile appears in the Auto AP profile list.

What To Do Next

Next, assign the Auto AP configuration to one or more controllers, following the directions "Assigning an Auto AP Profile to Controllers" on page 371.

Related Documentation

- Understanding Auto AP Profiles on page 24
- Adding and Managing an Access Point on page 126
- Understanding the IEEE 802.11 Standard for Wireless Networks on page 100
- Understanding Access Point Bias for Controllers on page 84

Copyright © 2013, Juniper Networks, Inc.

- Understanding Radio Profiles on page 42
- Creating and Managing a Radio Profile on page 315
- Assigning an Auto AP Profile to Controllers on page 371
- *Converting Automatically Discovered Access Points to Manually Configured Access Points With Network Director*

Creating and Managing CoS Profiles

CoS profiles enable the grouping of class-of-service (CoS) parameters and apply them to one or more interfaces. Network Director provides you with predefined traffic types for each CoS profile that you create. These traffic types represent the most common types of traffic for the device type. Each of these templates has preconfigured values for all CoS parameters based on the typical application requirements. You can change the preconfigured values of these parameters to suit your requirements.

To display the CoS Profiles page: In build mode, select **CoS** under Profile and Configuration Management in the Tasks pane. The Manage CoS Profiles page appears.

This topic describes:

- Managing CoS Profiles on page 184
- Using the Default CoS Profiles for Switches on page 185
- Default CoS Profiles for Data Center Switching on page 186
- Creating a CoS Profile on page 187
- Specifying Settings for a Switching CoS Profile on page 188
- Specifying Settings for a Wireless CoS Profile on page 192
- Specifying Settings for a Data Center Switching CoS Profile on page 194
- What To Do Next on page 198

Managing CoS Profiles

From the Manage CoS Profiles page, you can:

- Create a new CoS profile by clicking **Add**. For details, see "Creating a CoS Profile" on page 187.
- Modify an existing CoS profile by selecting it and clicking **Edit**.
- View information about a profile by selecting the profile and clicking **Details**.
- Delete a CoS profile by selecting a profile and clicking **Delete**.

Copyright © 2013, Juniper Networks, Inc.

TIP: You cannot delete profiles that are in use—that is, assigned to objects or used by other profiles. To see the current assignments for a profile, select the profile and click **Details**.

- Clone an existing CoS profile by selecting it and clicking **Clone**.

Table 47 on page 185 describes the information provided about CoS profiles on the Manage CoS Profiles page. This page lists all CoS profiles defined for your network, regardless of the scope you selected in the network view.

Table 47: Manage CoS Profile Fields

Field	Description
Profile Name	Name given to the profile when the profile was created.
Family Type	The device family on which the profile was created, either EX Series Switches, Wireless LAN Controllers, Campus Switching ELS, or Data Center Switching.
Description	Description of the profile that was entered when the profile was created. If the profile was created using the CLI and then discovered by Network Director, the description is *Profile created as part of device discovery*. TIP: To display the entire description, you might need to resize the Description column by clicking the column border in the heading and dragging it.
Creation Time	Date and time when this profile was created.
Update Time	Date and time when this profile was last modified.
User Name	The username of the user who created or modified the profile.

TIP: All columns might not be displayed. To show or hide fields listed in the Manage Authorization Profiles table, click the down arrow on the field header, select **Columns**, and select or clear the check box adjacent to the field that you want to show or hide.

Using the Default CoS Profiles for Switches

When you install Network Director, a default CoS profile (juniper_CoS_template) is added to the Manage CoS Profiles page for EX Series switches and another with the same name is added for Campus Switching ELS. Default CoS profiles have most basic settings preconfigured. For example, the forwarding classes in the default CoS profile have already been assigned with default scheduler values. However, you can use the Edit CoS Profile page to optimize your communication with the network by customizing the bandwidth and buffer size assigned to each of the forwarding classes in the default CoS profile.

Copyright © 2013, Juniper Networks, Inc.

The default CoS profile for most switches has the following forwarding classes and settings:

- Data—Best effort forwarding, forwarding queue 0, is a backward compatibility feature. Provides no service profile. Loss priority is typically not carried in a CoS value. For a best effort scheduler, the transmission rate is set to 35 percent, the buffer size to 50 percent, and priority to low.
- Voice—Expedited forwarding, forwarding queue 5, gets low-latency, strict high priority treatment through the fabric and where the packet was sent. Provides a low loss, low latency, low jitter, assured bandwidth, end-to-end service. Transmission rate is set to 10 percent and buffer size to 20 percent.
- Video—Video forwarding, forwarding queue 4, delivers assured bandwidth, low loss, low delay, and low delay variation (jitter) end-to-end for packets in this service class. For an expedited scheduler, the transmission rate is set to 30 percent, the buffer size to 30 percent, and priority to low.
- Network-Control—Network control, forwarding queue 7, offers a high-level of assurance that the packets are delivered as long as the packet flow from the customer stays within a certain Service profile that you define. The software delivers packets in this service class with a high priority. (These packets are not delay-sensitive.) Typically, these packets represent routing protocol hello or keep alive messages. Because loss of these packets jeopardizes proper network operation, packet delay is preferable to packet discard for these packets. For assured scheduler, the transmission rate is set to 25 percent, the buffer size to 25 percent, and priority to low.

EX4300 switches have four additional default classes and settings:

- Multicast network connect—Supports protocol control and thus is typically high priority.
- Multicast expedited forwarding—The software delivers assured bandwidth, low loss, low delay, and low delay variation (jitter) end-to-end for multicast packets in this service class. The software accepts excess traffic in this class, but in contrast to the multicast assured forwarding class, out-of-profile multicast expedited-forwarding class packets can be forwarded out of sequence or dropped.
- Multicast assured forwarding—The software offers a high level of assurance that the multicast packets are delivered as long as the packet flow from the customer stays within a certain service profile that you define. The software accepts excess traffic, but it applies a tail-drop profile to determine if the excess packets are dropped and not forwarded. Two drop probabilities (low and high) are defined for this service class.
- Multicast best effort forwarding is a backward compatibility feature. The software does not apply any special CoS handling to multicast packets. These packets are usually dropped under congested network conditions.

Default CoS Profiles for Data Center Switching

When you install Network Director, the following default CoS profiles are installed for Data Center Switching:

Copyright © 2013, Juniper Networks, Inc.

- juniper_DC_NonHier_Ethernet_CoS
- juniper_DC_Hier_Ethernet_CoS
- juniper_DC_NonHier_CoS
- juniper_DC_Hier_CoS
- juniper_DC_Hier_FCoE_CoS

To see the settings configured for a default profile, select it on the Manage CoS Profiles page, then click **Details**.

Creating a CoS Profile

In Network Director, you can create a CoS profile to group a set of Class of Service parameters and apply it to one or more network sessions.

For a CoS profile, you must specify the profile name. You can optionally specify additional configurations such as:

- Traffic Classifications and their corresponding shaping details for switches.
- Traffic rewrite rules for switches.
- Per Session CoS settings for data and voice traffic for controllers.
- Forwarding queue action corresponding to the predefined queues for controllers. Either 0-8, 0-10, or 0-11 queues are supported for forwarding class creation, depending on the switch.

To create a CoS profile:

1. Click

in the Network Director banner.
2. Under Select View, select either **Logical View**, **Location View**, **Device View** or **Custom Group** View.

   TIP: **Do not select Virtual View or Topology View.**
3. Click **CoS** under Profile and Configuration Management in the Tasks pane.

   The Manage CoS Profiles page appears, displaying the list of currently configured CoS profiles.
4. Click **Add**.

   The Device Family Chooser window opens.
5. From the Device Family Chooser, select the device family for which you want to create a CoS profile. The available device families are **Switching (EX)**, **Wireless (WLC)**, **Campus Switching ELS**, and **Data Center Switching**.
6. Click **OK**.

   The Create CoS Profile wizard for the selected device family is displayed.

Copyright © 2013, Juniper Networks, Inc.

7. Specify the CoS settings. Do one of the following:
   - For either EX Series switches or ELS campus switching, specify the settings as described in "Specifying Settings for a Switching CoS Profile" on page 188.
   - For controllers, specify the settings as described in "Specifying Settings for a Wireless CoS Profile" on page 192.
   - For Data Center Switching, "Specifying Settings for a Data Center Switching CoS Profile" on page 194.
8. Click **Done** to save the CoS profile.

   The system saves the CoS profile and displays the Manage CoS Profiles page. Your new or modified CoS profile is listed in the table of CoS profiles.

Specifying Settings for a Switching CoS Profile

Create a CoS profile for switching by providing a profile name and, optionally, changing any default settings for Traffic Configuration and Shaping.

1. Enter the CoS switching settings described in Table 48 on page 188. Required settings are indicated by a red asterisk (*) that appears next to the field label in the user interface.

Table 48: CoS Profile Settings for EX and ELS Switching

Field	Action
Profile Name	Type the name of the profile.
Description	Type a description of the profile.

2. Network Director includes four predefined traffic types, Data, Voice, Video, and Network Control. You can either modify those traffic types or you can create your own traffic type. Modify and customize any listed traffic type by selecting the traffic type from the list and clicking **Edit**, then changing any of the settings described in Table 49 on page 188.
3. To create your own traffic type, click **Add** and then configure the settings described in Table 49 on page 188.

Table 49: Traffic Configuration and Shaping for EX Switching and Campus Switching ELS

Field	Description
Traffic Type	If you are editing a Network Director default traffic type, this field cannot be changed. If you are adding a traffic type, indicate the type of traffic—this can be any value, such as a server name or something to do with your business.

Copyright © 2013, Juniper Networks, Inc.

Table 49: Traffic Configuration and Shaping for EX Switching and Campus Switching ELS *(continued)*

Field	Description
Forwarding Name	If you are editing a Network Director default traffic type, this field cannot be changed. If you are adding a traffic type, you can use one of the predefined forwarding classes for your switch or you can create your own forwarding class. These forwarding classes are always provided: **nd_best-effort**, **nd_network-control**, **nd_video-forwarding**, and **nd_expedited-forwarding**. To create your own forwarding class, type a name instead of selecting an option. Most switches support the four predefined forwarding classes listed above. The exception is the EX4300 switch, which has eight default forwarding classes, including the standard four classes, plus **multicast-network-connect**, **multicast-assured-forwarding**, **multicast-expedited-forwarding**, and **multicast-network-connect**.
Forwarding Queue	Existing forwarding classes already have associated queues that cannot be altered. If you defined a new forwarding class by specifying your own Forwarding Name, then select an internal queue number to which forwarding classes are assigned. Most switches support queues 0 - 10. The exception is the EX4300 switch, which supports queues 0 - 11. By default, if a packet is not classified, it is assigned to the class associated with queue 0. You can assign more than one forwarding class to a queue number.
Scheduler Map A note in the Scheduler Map section indicates how much buffer size and bandwidth you have available to configure. For example, the message "You have been left with 0 percent buffer size and 0 percent bandwidth." means that you have no available buffer or bandwidth, and you must reconfigure existing traffic types to free some bandwidth before configuring additional traffic types.	
Strict High	Enable **Strict High** if you want the queue to receive preferential treatment over a low-priority queue. Unlimited bandwidth is assigned to a strict-high priority queue. NOTE: You can modify this field in the Traffic Configuration and Shaping table or from the Traffic Configuration and Shaping window.
Buffer Size (%)	**Buffer Size (%)** is the size of the memory buffer allocated for storing packets. Use the slider to specify the scheduler **Buffer Size** percentage. NOTE: You can modify this value by double-clicking this field in the Traffic Configuration and Shaping table or by sliding the bar in the Traffic Configuration and Shaping window.

Copyright © 2013, Juniper Networks, Inc.

Table 49: Traffic Configuration and Shaping for EX Switching and Campus Switching ELS *(continued)*

Field	Description
Bandwidth Reserved (%)	**Bandwidth Reserved (%)** is the amount of interface bandwidth assigned to the queue. Move the slider to specify the **Bandwidth Reserved** percentage. Defaults are: • Data: 30% • Voice: Strict High • Video: 70% • Network control: 0% If **Strict-High** is enabled for this traffic type, you cannot reserve bandwidth. NOTE: This field displays the value based on either your input or on the **transmit-rate** parameter from the switch, if that parameter is configured. While specifying **transmit-rate** on the EX Series switch, if you choose to specify the value as an exact rate, Network Director converts this value and displays it as a percentage in the **Bandwidth Reserved (%)** field. You can modify this percentage value from the CoS Profile page.
Shaping Rate	Move the **Shaping Rate** slider to throttle the rate of packet transmission by setting a maximum bandwidth (rate in bits per second) or a maximum percentage of bandwidth for a queue or a forwarding class.
Traffic Classification Behavior aggregate classification classifies packets. The DSCP or DSCP IPv6 precedence bits of the IP header convey the behavior aggregate class information. The information might also be found in the IEEE 802.1ad, or IEEE 802.1p CoS bits.	
Classifier Type	If you are editing a Network Director default traffic type, this field cannot be changed. If this is a new traffic type, select a classifier type to map packets to a forwarding class, either **DSCP**, **DSCP-IPv6**, **INET-precedence**, or **IEEE-802.1**. • DSCP—Differentiated services code point, a field in IPv4 headers, is used to classify traffic. • DSCP-IPv6—Differentiated services code point, a field in IPv6 headers, is used to classify traffic. • INET precedence—Field that indicates class of service rewrite rules are used to classify traffic. • IEEE-802.1—IEEE 802.1ad, or IEEE 802.1p CoS bits are used to classify traffic.
Classifier Code Points	
Code Points	The code points list includes all available and unselected code points for the selected classifier type. Specify one or more code-point aliases or bit sets to associate with a forwarding class by moving the value to one of the two lists, Loss Priority Low or Loss Priority High.

Copyright © 2013, Juniper Networks, Inc.

Table 49: Traffic Configuration and Shaping for EX Switching and Campus Switching ELS *(continued)*

Field	Description
Loss Priority Low	Indicate that packets have low loss priority by selecting code-point aliases from the Code Points table and using the LEFT and RIGHT arrows to move them into the appropriate loss priority table.
Loss Priority High	Indicate that packets have high loss priority by selecting code-point aliases from the **Code Points** table and using the LEFT and RIGHT arrows to move them into the appropriate loss priority table.

4. Click **OK** to close the Add Traffic and Classification window and save your configuration.

   Your changes are added to this CoS profile.

NOTE: If all bandwidth has already been reserved, your changes are not made. Reduce the bandwidth reserved from another Traffic Type, then repeat the configuration.

5. To configure rewrite rules for a forwarding queue, click **Configure Rewrite Rules** at the bottom of the screen. The Configure Rewrite Rules window appears. Double-click the configurable settings as described in Table 50 on page 191 to alter CoS values in outgoing packets on the outbound interfaces of an edge switch.

Table 50: CoS Rewrite Rules for EX and ELS Switching

Field	Description
Forwarding Name	The name of the forwarding classes in this CoS profile. You cannot modify this field.
Queue	The number corresponding to each forwarding queue (0-10). You cannot modify this field.
Rewrite Type	Select a Rewrite Type for the traffic that passes through the various queues on the interface, either None, **DSCP**, **INET Precendence**, **DSCP IPv6**, or **IEEE 802.1**. TIP: Rewrite Type and Loss Priority Code Point are Mandatory fields for Rewrite rules
Egress Code Point - Loss Priority Low	For any rewrite type other than **None**, select a code-point alias for association with a forwarding class for Loss Priority Low. TIP: Rewrite Type and Loss Priority Code Point are Mandatory fields for Rewrite rules
Egress Code Point - Loss Priority High	For any rewrite type other than **None**, select a code-point alias for association with a forwarding class for Loss Priority High. TIP: Rewrite Type and Loss Priority Code Point are Mandatory fields for Rewrite rules

Copyright © 2013, Juniper Networks, Inc.

6. Click **OK** to save the rewrite rules and close the Configure Rewrite Rules window.

   The system saves the rewrite rules and returns to the **Create CoS Profile** page.

7. Click **Done**.

After you create a CoS profile for switching devices, associate the CoS profile with a Port profile. For directions, see "Creating and Managing Port Profiles" on page 283.

Specifying Settings for a Wireless CoS Profile

To configure a wireless CoS profile:

1. Enter the settings described in Table 51 on page 192. Required settings are indicated by a red asterisk (*) that appears next to the field label in the user interface.

Table 51: CoS Profile Basic Settings for Wireless

Field	Action
Profile Name	Type the name of the profile.
Description	Type a description of the profile.
Session CoS	
Enable Bandwidth Limit	Select **Enable Bandwidth Limit** if you want to specify a bandwidth limit for a given session, and then type the **Maximum Bandwidth (Kb/s)** (full duplex rate) for aggregates of access categories (ACs) for a wireless client. Downstream packets are shaped and upstream packets are policed.
Enable Static CoS	Select **Enable Static CoS** to assign the same CoS level to all traffic on the Service profile SSID, regardless of 802.1p or DSCP markings in the packets themselves, and regardless of any filters that mark CoS. This option provides a simple way to configure an SSID for priority traffic such as VoIP traffic. Select the **CoS Value** that you want the controller to assign to all user traffic.
Trust Client DSCP	Select **Trust Client DSCP** to enable the controller to use the client DSCP (differentiated services code point) for radio ingress traffic and ignore Wi-Fi Multimedia (WMM).
Voice CoS	

Copyright © 2013, Juniper Networks, Inc.

Table 51: CoS Profile Basic Settings for Wireless *(continued)*

Field	Action
Traffic Class	Specify the traffic class for the data type voice: • **None**—Select to indicate that no traffic class is required for voice traffic. • **VoIP-Data**—Select to indicate that you want to enable a traffic class for voice traffic. If you selected **VoIP-Data**, you can additionally select **Enable Bandwidth Limit** if you want to specify a bandwidth limit for voice traffic, and then type the maximum bandwidth (full duplex rate) for aggregates of access categories (ACs) for a wireless client. Downstream packets are shaped and upstream packets are policed. If you selected **VoIP-Data**, you can additionally select **Enable Static CoS** to assign the same CoS level to all traffic on the service profile SSID, regardless of 802.1p or DSCP markings in the packets themselves, and regardless of any firewall filters that mark CoS. This option provides a simple way to configure an SSID for priority traffic such as VoIP traffic. Select the CoS value that you want the controller to assign to all user traffic.
Access Categories	**Access Categories** includes up to four access categories for QoS. You can modify the action (**Permit** or **Demote**) corresponding to each forwarding queue to suit your requirements. If you remove any of the four default types (Background, Best Effort, Voice, and Video) by selecting it and clicking **Remove**, you can add additional categories until there are four. To add a category: a. Click **Add** in the Access Categories box. The Add Access Category window appears. b. Select an Access Category, **Background**, **Best-Effort**, **Voice**, or **Video**. c. Select an action to be applied to packets in the forwarding queue, either **Permit** or **Demote**. d. Click **OK**. The Add Access Category window closes and the access category is added to the list of Access Categories.

2. Click **Done**.

After you create a CoS profile for wireless devices, associate the CoS profile with an Authorization profile during Authorization profile creation. This Authorization profile is then associated with a WLAN profile (during WLAN profile creation) to apply the CoS settings to all the users who connect to the WLAN SSID. For directions, see "Creating and Managing Wireless Authorization Profiles" on page 167 and"Creating and Managing a WLAN Service Profile" on page 350.

Copyright © 2013, Juniper Networks, Inc.

Specifying Settings for a Data Center Switching CoS Profile

You can create a CoS profile by specifying the profile settings and the traffic configuration and shaping details.

To specify the settings for the CoS profile:

1. Enter the settings described in Table 52 on page 194. Required settings are indicated by a red asterisk (*) that appears next to the field label in the user interface.

Table 52: CoS Profile Basic Settings for Data Center Switching

Field	Action
Profile Name	Type the name of the profile.
Description	Type the description of the profile.

2. In the Traffic Classification and Shaping Settings section, select one of these options:
   - **Hierarchical Port Scheduling (ETS)**—Hierarchical port scheduling (Enhanced Transmission Selection, or ETS) is a two-tier process that provides better port bandwidth utilization and greater flexibility to allocate resources to queues and to groups of queues (for QFX and QFabric devices).
   - **Non Hierarchical Port Scheduling**—Non-hierarchical scheduling is a one-tier process that provides port bandwidth utilization and allocates resources to queues (for EX4500 and EX4550 Series transit switches).
3. If you selected Hierarchical Port Scheduling (ETS), specify settings in the Priority Group and Traffic Settings section.

   The table lists priority groups and the forwarding classes they contain in an expandable list. Priority groups refer to forwarding class sets in the device. You can perform these tasks on priority groups and forwarding classes:

   - To add a new priority group, click **Add Priority Group**. The Add Priority Group and Traffic Control Profile Window opens. Enter the settings as described in Table 53 on page 194.

Table 53: Add Priority Group and Traffic Control Profile Window

Field	Description
Priority Group Name	Enter a name for the priority group.
Traffic Control Profile Settings	
Transmit Rate (%)	Select a transmit rate percentage for the priority group.
Shaping Rate (%)	Select a shaping rate percentage for the priority group.

   - To edit a priority group or forwarding class's properties, edit cells in its table row. The properties are described in Table 54 on page 195.

Copyright © 2013, Juniper Networks, Inc.

Table 54: Priority Group and Traffic Settings Table Properties

Field	Description
No Loss	Select to make the forwarding class lossless. Not applicable to priority groups.
Strict High	Select to cause the forwarding class to receive preferential treatment over a low-priority queue. Unlimited bandwidth is assigned to a strict-high priority queue. Not applicable to priority groups.
Transmit Rate (%)	Select the percentage of interface bandwidth assigned to the forwarding class or priority group. If you have enabled **Strict-High**, you cannot reserve bandwidth for this traffic type.
Shaping Rate (%)	Select a shaping rate percentage for the forwarding class or priority group.
Buffer Size (%)	Select the percentage of the memory buffer allocated for storing packets for the forwarding class. Not applicable to priority groups.

- To edit a forwarding class's properties, click its name. The Edit Traffic Classification and Shaping for priority group window opens. Enter the settings as described in Table 55 on page 195.

Table 55: Edit and Add Traffic Classification and Shaping for priority group Window

Field	Description
Forwarding Class Name	Select or specify a name for the forwarding class.
Forwarding Class Queue	Specify the internal queue numbers to which forwarding classes are assigned.
No Loss	Select to make the forwarding class lossless.
Scheduler Map	
Strict High	Select if you want the queue to receive preferential treatment over a low-priority queue. Unlimited bandwidth is assigned to a strict-high priority queue.
Transmit Rate	Select the percentage of interface bandwidth assigned to the forwarding class. If you have enabled **Strict-High**, you cannot reserve bandwidth for this traffic type.
Shaping Rate	Select a shaping rate percentage for the forwarding class.
Buffer Size (%)	Select the percentage of the memory buffer allocated for storing packets for the forwarding class.
Traffic Classification	
Classifier Type	Select the classifier type that maps packets to a forwarding class and a loss priority.
Code Points	Specify one or more code-points for associating with a forwarding class.

Copyright © 2013, Juniper Networks, Inc.

Table 55: Edit and Add Traffic Classification and Shaping for priority group Window *(continued)*

Field	Description
Loss Priority Low	Indicates that packets have low loss priority. Select code points from the Code Points table and use the LEFT and RIGHT arrows to move them into the appropriate loss priority table.
Loss Priority Medium High	Indicates that packets have medium high loss priority. Select code points from the Code Points table and use the LEFT and RIGHT arrows to move them into the appropriate loss priority table.
Loss Priority High	Indicates that packets have high loss priority. Select code points from the Code Points table and use the LEFT and RIGHT arrows to move them into the appropriate loss priority table.

- To add a forwarding class to a priority group, click the **Add Forwarding Class** link at the end of the priority group's list of forwarding classes. The Add Traffic Classification and Shaping for priority group window opens. Enter the settings as described in Table 55 on page 195.
- To remove a priority group or forwarding class, click the **X** at the end of its table row.

4. If you selected Non Hierarchical Port Scheduling, specify settings in the Traffic Configuration and Shaping table.

   The table lists forwarding classes. You can perform these tasks on forwarding classes:

   - To add traffic configuration and shaping details for different types of traffic, click **Add** in the Traffic Configuration and Shaping box. The Add Traffic Classification and Shaping window opens.
   - To modify the details of an existing traffic configuration, select the traffic configuration from the list and click **Edit**. The Edit Traffic Classification and Shaping window opens.

     NOTE: **You can modify some of the details in the Traffic Configuration and Shaping table without having to open the Edit Traffic Classification and Shaping window—by clicking on the field that you want to modify.**

   - To delete a traffic configuration entry, select the traffic configuration from the list and click **Remove**.

     The system deletes the selected traffic configuration entry.

   Enter or modify the settings as described in Table 55 on page 195.

5. If you selected Hierarchical Port Scheduling (ETS), specify priority-based flow control (PFC) settings in the PFC Settings section. Enter the settings as described in Table 56 on page 197.

Copyright © 2013, Juniper Networks, Inc.

Table 56: PFC Settings for Data Center Switching Hierarchical Port Scheduling (ETS) CoS Profile

Field	Description
Input Cable Length (meter)	Enter the length of the cable attached to the input interface, in meters.
Input	
Add	Click to add an input congestion notification profile (CNP). A new entry appears in the table.
Remove	Click to remove the selected input CNP.
IEEE Code Point	Select the IEEE code point for the input CNP.
Maximum Receive Size (bytes)	Enter the maximum receive unit (MRU) on an interface for traffic that matches the PFC priority, in bytes.
Output	
Add	Click to add an output CNP. A new entry appears in the table.
Remove	Click to remove the selected output CNP.
IEEE Code Point	Select the IEEE code point for the output CNP.
Queue List	Select output queues on which to enable flow control (PFC pause).

6. If you selected Non-Hierarchical Port Scheduling, specify priority-based flow control (PFC) settings in the PFC Settings section. Enter the settings as described in Table 57 on page 197.

Table 57: PFC Settings for Data Center Switching Non-Hierarchical Port Scheduling CoS Profile

Field	Description
Input	
Add	Click to add an input congestion notification profile (CNP). A new entry appears in the table.
Remove	Click to remove the selected input CNP.

7. Specify rewrite rule settings in the Rewrite Rule Settings section. Enter the settings as described in Table 58 on page 197.

Table 58: Rewrite Rule Settings for Data Center Switching CoS Profile

Field	Description
Forwarding Name	The name of the forwarding class.

Copyright © 2013, Juniper Networks, Inc.

Table 58: Rewrite Rule Settings for Data Center Switching CoS Profile *(continued)*

Field	Description
Queue	The number corresponding to the forwarding queue. You cannot modify this field.
Rewrite Type	Select a rewrite-rules mapping for the traffic that passes through the various queues on the interface.
Egress Code Point - Loss Priority Low	Specify a code-point for association with a forwarding class for loss priority low.
Egress Code Point - Loss Priority Medium High	Specify a code-point for association with a forwarding class for loss priority medium high.
Egress Code Point - Loss Priority High	Specify a code-point for association with a forwarding class for loss priority high.

8. Click **Done** to save the changes to the profile.

What To Do Next

After you have created a CoS profile, you can do one of the following depending on the device family for which the profile was created:

- For switching devices, associate the CoS profile with a Port profile.
- For wireless devices, associate the CoS profile with an Authorization profile. This Authorization profile can then be associated with a WLAN profile to apply the CoS settings to all the users who connect to that SSID.

Related Documentation

- Understanding Class of Service (CoS) Profiles on page 26

Creating and Managing Device Common Settings

Use the Manage Device Common Settings page to create new device common settings for switching and wireless devices and to manage the existing device common settings.

To display the Manage Device Common Settings page: In Build mode, select **Device Common Settings** from Profile and Configuration Management in the Tasks pane. The Manage Device Common Settings page appears.

This topic describes:

- Managing Device Common Settings on page 199
- Creating Device Common Settings Profiles on page 200
- Specifying Basic Settings for Device Common Settings on page 202
- Specifying Management Settings for EX Switching Device Common Settings on page 205
- Specifying Management Settings for Wireless Device Common Settings on page 208

Copyright © 2013, Juniper Networks, Inc.

- Specifying Management Settings for Campus Switching ELS Device Common Settings on page 211
- Specifying Management Settings for Data Center Device Common Settings on page 214
- Specifying Protocol Settings for EX Switching Device Common Settings on page 216
- Specifying DNS Settings for Wireless Device Common Settings on page 218
- Specifying DHCP Relay/DNS Settings for Campus Switching ELS Device Common Settings on page 219
- Specifying Protocol Settings for Data Center Switching Device Common Settings on page 220
- Reviewing and Saving a Device Common Settings Configuration on page 222
- What To Do Next on page 222

Managing Device Common Settings

From the Manage Device Common Settings page, you can:

- Create a new common settings profile by clicking **Add**. For details, see "Creating Device Common Settings Profiles" on page 200.
- Modify an existing common settings profile by selecting it and clicking **Edit**.
- Assign a common settings profile to a device by selecting a profile and clicking **Assign**.
- Modify an existing assignment of common settings by selecting the profile and clicking **Edit Assignment**.
- View information about a common settings profile by either double-clicking the profile name or by selecting the profile and clicking **Details**.
- Delete a common settings profile by selecting a profile and clicking **Delete**.

TIP: You cannot delete common settings profiles that are in use—that is, assigned to devices or used by other profiles. To see the current assignments for a profile, select the profile and click **Details**.

- Clone a common settings profile by selecting a profile and clicking **Clone**.

Table 59 on page 199 describes the device information available on the Manage Device Common Settings page. This page lists all device profiles defined for your network, regardless of your current selected scope in the network view.

Table 59: Manage Device Common Settings Fields

Field Name	Action
Profile Name	Name given to the profile when the profile was created.
Family Type	The device family; EX Series switch, Campus Switching ELS, wireless LAN controller (WLC), Data Center Switching.

Copyright © 2013, Juniper Networks, Inc.

Table 59: Manage Device Common Settings Fields *(continued)*

Field Name	Action
Description	Description of the device profile entered when the profile was created.
Assignment State	Displays the assignment state of the profile. A profile can be: • Unassigned—when the profile is not assigned to any device. • Assigned—When the profile is assigned to a device, but not deployed in the network. • Deployed—When the profile is assigned to a device and is deployed from the Deploy mode. • Pending Deployment—When the profile is assigned to a device, but not yet deployed in the network.
Creation Time	Date and time when this profile was created.
Last Updated Time	Date and time when this profile was last modified.
User Name	The username of the user who created or modified the profile.

TIP: All columns might not be displayed. To show or hide fields listed in the Manage Authorization Profiles table, click the down arrow on the field header, select Columns, and select or clear the check box adjacent to the field that you want to show or hide.

Creating Device Common Settings Profiles

In Network Director, as an administrator, you can configure device profiles by using the Create Device Profile page for either switches or wireless LAN controllers. You can view the summary of the configurations before saving the device profile.

At minimum, you must specify the device profile and profile name in the workflow. You can include additional configuration such as:

- Device users
- Management services
- Multicast, spanning-tree protocol (STP)
- Domain Name Server
- DHCP servers, DHCP Relay servers, Login Banner, and Global PoE settings for switches

You can create profiles on the basis of the device family and each device profile is specific to a device family. After you create a device profile, you assign the profiles to different devices.

Copyright © 2013, Juniper Networks, Inc.

NOTE: You can assign only one profile to a device. However, you can assign the same profile to multiple devices.

To create a device profile:

1. Click in the Network Director banner.
2. Under Select View, select either **Logical View**, **Location View**, **Device View** or **Custom Group** View.

   TIP: Do not select **Virtual View** or **Topology View**.
3. Click **Device Common Settings** under Profile and Configuration Management in the Tasks pane.

   The Manage Device Common Settings page appears, displaying the list of currently configured Device Common Settings profiles.
4. Click **Add**.

   The Device Family Chooser window opens.
5. From the Device Family Chooser, select the device family for which you want to create a profile. The available device families are **Switching (EX)**, **Wireless (WLC)**, **Campus Switching ELS** (Enhanced Layer 2 Software), and **Data Center Switching Non ELS**.
6. Click **OK**.

   The Create Device Common Settings wizard for the selected device family is displayed. It consists of four sections, Basic Settings, Management Settings, Protocol Settings, and Review.
7. Specify the basic settings. Complete the Basic Setting wizard page as described in "Specifying Basic Settings for Device Common Settings" on page 202.
8. When you have completed the basic settings, either click **Next** or click **Management Settings** at the top of the wizard window.
9. Complete the Management Settings described in the sections "Specifying Management Settings for EX Switching Device Common Settings" on page 205, "Specifying Management Settings for Wireless Device Common Settings" on page 208, "Specifying Management Settings for Campus Switching ELS Device Common Settings" on page 211, and "Specifying Management Settings for Data Center Device Common Settings" on page 214.
10. When you have completed the management settings, click **Next**.
11. Complete the protocol settings as described in the sections "Specifying Protocol Settings for EX Switching Device Common Settings" on page 216, "Specifying DNS Settings for Wireless Device Common Settings" on page 218, "Specifying DHCP Relay/DNS Settings for Campus Switching ELS Device Common Settings" on page 219,

Copyright © 2013, Juniper Networks, Inc.

and "Specifying Protocol Settings for Data Center Switching Device Common Settings" on page 220.

12. When you have completed the protocol settings, either click **Next** or click **Review** at the top of the wizard window.
13. You can either save your profile or make changes to your profile from the Review page. For more details, see "Reviewing and Saving a Device Common Settings Configuration" on page 222.
14. Click **Finish** to save the device profile configuration.

    The system saves the device profile and displays the Manage Device Common Settings page. Your new or modified device profile is listed in the table.

Specifying Basic Settings for Device Common Settings

To configure the basic settings for the Device Common Settings profile, enter the settings described in Table 60 on page 202. Mandatory settings are indicated by a red asterisk (*) that appears next to the field label in the user interface.

Table 60: Device Profile Basic Settings

Field	Action
Profile Name	Type a name for the profile. • For both EX Series switches and Campus Switching Enhanced Layer 2 Software, the name can contain up to 64 alphanumeric characters. • For both wireless controllers and Data Center Switching devices, the name can contain up to 32 alphanumeric characters with only the underscore as a special character. For example: **device_profile_wlc**.
Description	Type a description, up to 256 characters long, of the profile.
Login Banner for EX Series switches, Campus Switching ELS, and Data Center Switching	Enter the banner text—this text is displayed in the banner when you log in to the device.
Country Code for wireless LAN controllers only	Select the country code for the wireless LAN controllers. Country code settings are required on the primary wireless seed controller. TIP: Do not set the country code if you plan to provision the device profile for active secondary and member nodes that will be part of a cluster.
AP Security Mode for wireless LAN controllers only	You can indicate that access point security is **Required**, **Optional**, or **None**.
Device Users	

Copyright © 2013, Juniper Networks, Inc.

Table 60: Device Profile Basic Settings *(continued)*

Field	Action
Add a Device User	To add a device user: 1. Click **Add** under Device Users. The Add User window opens. 2. Provide a username and password. Confirm the password. Enter a combination of 6 through 128 alphanumeric characters and special characters. The password is case sensitive and must be a combination of at least two different types of characters or a combination of upper case and lower case letters. TIP: Do not create a user with the name *root*. 3. Select a role for the user: • For switches, the role options are: **Operator**, **Read-only**, **Super-user**, or **Unauthorized**. Operators have clear, network, reset, trace, and view privileges. Super-Users have all privileges. • For wireless controllers, the role options are: **Framed**, **Administrative**, or **NAS-Prompt**. Framed users have network user access only. Administrative users have access to the controller, including the enabled (configuration) mode. NAS-Prompt users have administrative access to the controller, excluding enabled mode. 4. Click **OK**. The user is added to the list of Device Users. TIP: To edit an entry, select a row from the Device Users table and click **Edit** to modify the details. To delete an entry select a row from the Device Users table and click **Delete** to delete the user.
Time Settings Time Settings are available only for wireless controllers.	
Time Zone	Select a country and time zone from the list.
Add a Time Server	To add a time server: 1. Click **Add** under Time Server. The Add Time Server window opens. 2. Provide an IP address and, optionally for switches only, mark the corresponding time server as **Preferred**. TIP: Valid IP addresses are 1.0.0.1 through 255.255.255.254 excluding 127.x.x.x and 224.0.0.0 through 239.255.255.255 3. Click **OK**. The server is added to the list of Time Servers. TIP: To edit the settings of a time server, select it and then click **Edit**.

Copyright © 2013, Juniper Networks, Inc.

To configure management settings, click **Next** or click **Management Settings** at the top of the wizard window. To skip the management settings and protocol settings, click **Review** at the top of the wizard window.

Management Settings are described in the sections "Specifying Management Settings for EX Switching Device Common Settings" on page 205, "Specifying Management Settings for Wireless Device Common Settings" on page 208, "Specifying Management Settings for Campus Switching ELS Device Common Settings" on page 211, "Specifying Protocol Settings for Data Center Switching Device Common Settings" on page 220 and "Specifying Management Settings for Data Center Device Common Settings" on page 214.

Copyright © 2013, Juniper Networks, Inc.

Specifying Management Settings for EX Switching Device Common Settings

To configure the management settings for an EX switching device profile:

Copyright © 2013, Juniper Networks, Inc.

1. Enter the settings described in Table 61 on page 206. All settings are optional. Default values are applied to the configuration if you skip the management settings configuration.

Table 61: Device Profile Management Settings for EX Switching

Task	Action
Enable Services	You can enable one or more network protocol services for this Device profile: **FTP**, **TELNET**, **HTTPS**, or **HTTP**. NOTE: HTTP and HTTPS are not available for EX 9200 Series switches.
Configure PoE	To add Power over Ethernet (PoE) configuration for EX switching, enable **Configure PoE** and provide these settings: NOTE: PoE configuration will be added only to switches that support PoE. a. Using the arrows, adjust the **Guard Band** value from zero through 19 watts. A guard band reserves a specified amount of power from the PoE power budget for the switch or line card in case of a spike in PoE consumption. For switches with multiple PoE line cards, such as the EX6200 switch, the guard band wattage is set to the specified value on all line cards, unless a line card has been explicitly configured with a different value. TIP: The valid guard band range (in watts) for EX6200 and EX8200 switches is 0 through 15. Any value outside this range causes the profile deployment to fail. b. Select a Management Mode for PoE, either **Class** or **Static**: • Class Management—In class PoE management mode, the maximum power for an interface is determined by the class of the connected powered device. • Static Management—In the static PoE management mode, you specify the maximum power for each PoE interface. The PoE controller then allocates this amount of power to the interface from its total budget. c. For PoE Global, you can indicate **Enable All**, **Disable All**, or **None**. NOTE: If you deselect **Configure PoE**, PoE is disabled and the global PoE settings supported by this profile (poe guard-band, poe fpc all guard-band, poe management, poe fpc all management, and poe interface all) are deleted from the switch when the profile is deployed on the switch.
Syslog Settings	Optionally, expand the Syslog Settings and provide the following system logging settings.

Copyright © 2013, Juniper Networks, Inc.

Table 61: Device Profile Management Settings for EX Switching *(continued)*

Task	Action
Enable Device Logging for Switches	To enable device logging for switches: a. Under Enable Device Log, click **Add**. The Add Log window opens. b. Select the log type for switching, either **Console**, **File**, **User**, or **Host**. • Console logging sends system log messages to the console. • File logging sends system log messages to the file you specify in **File Name**. • User logging sends system log messages to the terminal session of the user specified in **User Name**. You will also need to provide the name of the user. • Host logging sends system log messages to the server specified in **Host**. Host can be either an IP address or host name. c. Under Services, click **Add**. The phrase *Click to enter value* appears in both the Service column and Severity Filter column. d. Click the phrase *Click to enter value* in the Service column. A drop-down list appears under Services. e. From the Service drop-down list, select a logging service: **Any**, **Authorization**, **Change-log**, **Conflict-log**, **Daemon**, **DFC**, **External**, **Firewall**, **FTP**, **Interactive-commands**, **Kernel**, **NTP**, **PFE**, **Security** or **User**. f. Click the phrase *Click to enter value* in the Severity Filter column. A drop-down list appears under Severity Filter. g. Select an available severity filter from the list, either **Alert**, **Any**, **Critical**, **Emergency**, **Error**, **Info**, **None**, **Notice**, or **Warning**. The filter is added to the list of Severity Filters. The filter is activated when the corresponding service is triggered. h. Click **OK**. The log is added to the Enable Device Log list.
Edit Logging Settings	Select a Log Type from the Enable Device Log list and click **Edit** to change the configuration.
Delete Logging Settings	Select a Log Type from the Enable Device Log list and click **Delete** to remove the server configuration.

To configure protocol settings, either click **Next** or click **Protocol Settings**. To use the default protocol settings, skip to final review by clicking **Review** at the top of the wizard window.

Protocol Settings options are described in the section "Specifying Protocol Settings for EX Switching Device Common Settings" on page 216,

Copyright © 2013, Juniper Networks, Inc.

Specifying Management Settings for Wireless Device Common Settings

To configure the management settings for a wireless device profile:

Copyright © 2013, Juniper Networks, Inc.

1. Enter the settings described in Table 62 on page 209. All settings are optional. Default values are accepted in the configuration settings if you skip the management settings options.

Table 62: Device Profile Management Settings for Wireless

Task	Action
Enable Services	You can enable one or more network protocol services for this Device profile: **Telnet**, **HTTPS**, **HTTP**, and **TFTPD**. You can also change the default port numbers by clicking them.
Syslog Settings Optionally, expand **Syslog Settings** and enable a device log and/or configure a syslog server.	
Enable Device Logging for Wireless	To enable device logging for wireless devices: a. Under Enable Device Log, click **Add**. The Add Log window opens. b. Select a wireless log type, either **Console**, **Session**, or **Trace**. • Console logging sends system log messages to the console. • With session logging, each main session event—create, close, and deny—creates a log entry. • Trace operations record more detailed information about the operations, including packet forwarding and routing information. c. Select a Severity Filter for this log from the list, either **Alert**, **Critical**, **Debug all**, **Emergency**, **Error**, **Info**, **Notice**, or **Warning**. d. Click **OK**. The device log appears in the Enable Device Log list with its log type and severity filter. The filter will be activated when the corresponding service is triggered. TIP: To edit logging settings, select an entry from the Enable Device Log table and click **Edit**. To delete a logging setting, select an entry from the Enable Device Log table and click **Delete**.

Copyright © 2013, Juniper Networks, Inc.

Table 62: Device Profile Management Settings for Wireless *(continued)*

Task	Action
Add a Syslog Server	To add a syslog server to the common settings: a. Under Syslog Servers, click **Add**. The Add Server window opens. b. Type the IP address of the server. c. Select a Severity Filter from the list, either **Alert** (default), **Critical**, **Debug All**, **Emergency**, **Error**, **Info**, **Notice**, or **Warning**. TIP: The filter will be activated when the corresponding service is triggered. d. Click **OK**. The server is added to the list of Syslog Servers. TIP: To edit a syslog server, select a server and click **Edit**. To delete a syslog server, select a server from the Syslog Servers list, and then click **Delete** to remove the server. details.

To configure wireless DNS settings, either click **Next** or click **DNS Settings**. To skip the DNS settings, click **Review** at the top of the wizard window.

DNS settings are described in the section "Specifying DNS Settings for Wireless Device Common Settings" on page 218.

 Copyright © 2013, Juniper Networks, Inc.

Specifying Management Settings for Campus Switching ELS Device Common Settings

To configure the management settings for an ELS campus switching device common setting profile:

Copyright © 2013, Juniper Networks, Inc.

1. Enter the settings described in Table 63 on page 212. All settings are optional—default values are applied to the configuration if you skip the management settings.

Table 63: Management Settings for ELS Switching Device Profile

Task	Action
Enable Services	You can enable one or more network protocol services for this Device profile: **FTP**, **Telnet**, **HTTPS**, or **HTTP**. By default, none are selected.
Configure PoE	To add Power over Ethernet (PoE) configuration for ELS Switching, enable **Configure PoE** and provide these settings: NOTE: PoE configuration will be added only to switches that support PoE. a. Using the arrows, adjust the **Guard Band** value from zero through 19 watts. A guard band reserves a specified amount of power from the PoE power budget for the switch or line card in case of a spike in PoE consumption. For switches with multiple PoE line cards, such as the EX6200 switch, the guard band wattage is set to the specified value on all line cards, unless a line card has been explicitly configured with a different value. TIP: The valid guard band rang (in watts) for EX6200 and EX8200 switches is 0 through 15. Any value outside this range causes the profile deployment to fail. b. Select a Management Mode for PoE, either **Class** or **Static**: • Class Management—In class PoE management mode, the maximum power for an interface is determined by the class of the connected powered device. • Static Management—In the static PoE management mode, you specify the maximum power for each PoE interface. The PoE controller then allocates this amount of power to the interface from its total budget. c. For PoE Global, you can indicate **Enable All**, **Disable All**, or **None**. NOTE: If you deselect **Configure PoE**, PoE is disabled and the global PoE settings supported by this profile (poe guard-band, poe fpc all guard-band, poe management, poe fpc all management, and poe interface all) are deleted from the switch when the profile is deployed on the switch.
Syslog Settings	Optionally, expand the system logging section and configure device logging.

Copyright © 2013, Juniper Networks, Inc.

Table 63: Management Settings for ELS Switching Device Profile *(continued)*

Task	Action
Enable Device Logging for ELS Switches	To enable device logging for ELS switches: a. Under Enable Device Log, click **Add**. The Add Log window opens. b. Select the log type for ELS switching, either **Console**, **File**, **User**, or **Host** (default). • Console logging sends system log messages to the console. • File logging sends system log messages to the file you specify for **File Name**. • User logging sends system log messages to the terminal session of the user you specify for **User Name**. You will also need to provide the name of the user. • Host logging sends system log messages to the server you specify for **Host**. Host can be either an IP address or host name. c. Under Services, click **Add**. The phrase *Click to enter value* appears in both the Service column and Severity Filter column. d. Click on the phrase *Click to enter value* in the Service column. A drop-down list appears under Service. e. From the Service drop-down list, select a logging service: **Any**, **Authorization**, **Change-log**, **Conflict-log**, **Daemon**, **DFC**, **External**, **Firewall**, **FTP**, **Interactive-commands**, **Kernel**, **NTP**, **PFE Security** or **User**. f. Click on the phrase *Click to enter value* in the Severity Filter column. A drop-down list appears under Severity Filter. g. Select a Severity Filter from the list, either **Alert**, **Any**, **Critical**, **Emergency**, **Error**, **Info**, **Notice**, or **Warning**. h. Click **OK**. The filter is added to the list of Enabled Device Logs with entries in the Log Type column and filter name column. The filter will be activated when the corresponding log type is triggered.
Edit Logging Settings	Select an entry from the Enable Device Log table and click **Edit** to change the settings.
Delete Logging Settings	Select an entry from the Enable Device Log table and click **Delete** to remove the server settings.

To configure DHCP Relay and DNS, either click **Next** or click **DHCP Relay/DNS Settings**. To skip the protocol settings, click **Review** at the top of the wizard window.

DHCP Relay and DNS options are described in the section "Specifying DHCP Relay/DNS Settings for Campus Switching ELS Device Common Settings" on page 219.

Copyright © 2013, Juniper Networks, Inc.

Specifying Management Settings for Data Center Device Common Settings

To configure the management settings for a Data Center Management device profile:

Copyright © 2013, Juniper Networks, Inc.

1. Enter the settings described in Table 64 on page 215. All settings are optional—default values are applied to the configuration if you skip the management settings.

Table 64: Device Profile Management Settings for Data Center

Field	Action
Enable Services	You can enable one or more network protocol services for this Device profile: • For Data Center Switching, **FTP**, **Telnet**, **HTTP**.
System Logging Settings Optionally, for either switches or wireless, expand the Syslog Settings and provide the following system logging settings:	
Enable Device Logging for Switches	To enable device logging for switches: a. Under Enable Device Log, click **Add**. The Add Log window opens. b. Select the log type for switching, either **Console**, **File**, **User**, or **Host**. • Console logging sends system log messages to the console. • File logging sends system log messages to the file you specify in **File Name**. • User logging sends system log messages to the terminal session of the user specified in **User Name**. You will also need to provide the name of the user. • Host logging sends system log messages to the server specified in **Host**. Host can be either an IP address or host name. c. Under Services, click **Add**. The phrase *Click to enter value* appears in both the Service column and Severity Filter column. d. Click on the phrase *Click to enter value* in the Service column. A drop-down list appears under Services. e. From the Services drop-down list, select a logging service: **any**, **Authorization**, **Change-log**, **Conflict-log**, **Daemon**, **DFC**, **External**, **Firewall**, **FTP**, **Interactive-commands**, **Kernel**, **NTP**, **PFE** or **Security**. f. Click on the phrase *Click to enter value* in the Severity Filter column. A drop-down list appears under Severity Filter. g. Select a Severity Filter from the list, either **Alert**, **Critical**, **Debug All**, **Emergency**, **Error**, **Info**, **Notice**, or **Warning**. The filter is added to the list of Severity Filters. The filter is activated when the corresponding service is triggered. h. Click **OK**.

Copyright © 2013, Juniper Networks, Inc.

Table 64: Device Profile Management Settings for Data Center *(continued)*

Field	Action
Enable Device Logging for Wireless	To enable device logging for wireless devices: a. Under Enable Device Log, click **Add**. The Add Log window opens. b. Select a wireless log type, either **Console**, **Session**, or **Trace**. • Console logging sends system log messages to the console. • With session logging, each main session event—create, close, and deny—creates a log entry. • Trace operations record more detailed information about the operations, including packet forwarding and routing information. c. Select a Severity Filter from the list, either **Alert**, **Critical**, **Debug All**, **Emergency**, **Error**, **Info**, **Notice**, or **Warning**. The filter is added to the list of Severity Filters. The filter is activated when the corresponding service is triggered. d. Click **OK**.
Edit Logging Settings	Select a Log Type from the Enable Device Log table and click **Edit** to change the details.
Delete Logging Settings	Select a Log Type from the Enable Device Log table and click **Delete** to remove the server details.

To configure protocol settings, either click **Next** or click **Protocol Settings**. To skip the protocol settings, click **Review** at the top of the wizard window.

Protocol Settings options are described in the section "Specifying Protocol Settings for Data Center Switching Device Common Settings" on page 220.

Specifying Protocol Settings for EX Switching Device Common Settings

To configure the protocol settings for an EX Switching device profile, enter the settings described in Table 65 on page 217. All settings are optional.

Copyright © 2013, Juniper Networks, Inc.

Table 65: Device Profile Protocol Settings for EX Switching

Field	Action
Spanning Tree Settings	
Spanning Tree Protocol Settings for switches only	Select one of spanning-tree protocol (STP) settings for switches: **STP**, **RSTP** (default), **MSTP**, or **None of these**. • Spanning Tree Protocol—With STP configured, the switches use the IEEE 802.1D 2004 specification, force version 0. This configuration runs a version of RSTP that is compatible with classic, basic STP as defined in the 802.1D 1998 specification. • Rapid Spanning Tree Protocol—RSTP provides faster reconvergence time than the original STP by identifying certain links as point-to-point and by using protocol handshake messages rather than fixed timeouts. VLAN Spanning Tree Protocol (VSTP) and RSTP can be configured concurrently. You can selectively configure up to 253 VLANs using VSTP; the remaining VLANs will be configured using RSTP. VSTP and RSTP are the only spanning-tree protocols that can be configured concurrently on a switch. • Multiple Spanning Tree Protocol—MSTP enables multiple VLANs to be mapped to the same spanning-tree instance, reducing the number of spanning-tree instances needed to support a large number of VLANs. MSTP provides multiple forwarding paths for data traffic and enables load balancing. It improves the fault tolerance of the network because a failure in one instance, or forwarding path, does not affect other instances. You can also select the **Enable VSTP** check box to enable VSTP.
Multicast Settings	
Enable IGMP	Selecting this option enables Internet Group Management Protocol (IGMP) on all the interfaces for the selected device. Default is disabled. IGMP is a communications protocol used by both hosts and adjacent routers on IP networks to establish multicast group memberships.
Enable IGMP Snooping	Enables IGMP snooping on all VLANs. Default is enabled.
Enable DHCP Relay Select this option to display the DHCP Relay settings.	
Add DHCP Relay to Device Profile	To add DHCP Relay to this Device Profile: 1. Select **Legacy DHCP Relay** (default). 2. Add one or more DHCP servers to the Device Common Settings profile: a. Click **Add** under DHCP Servers. The Add Server window opens. b. Type an IP Address. c. Click **OK**. The server is added to the list of DHCP Servers.

Copyright © 2013, Juniper Networks, Inc.

Table 65: Device Profile Protocol Settings for EX Switching *(continued)*

Field	Action
Spanning Tree Settings	
Add Extended DHCP Relay to Device Profile	To add Extended DHCP Relay to this Device Profile: 1. Select **Extended DHCP Relay** instead of Legacy DHCP Relay. 2. Add one or more DHCP Server Groups to the Device Common Settings profile: a. Click **Add** under Add DHCP Servers Group. The Add Server Group window opens. b. Provide a name for the server group. c. Optionally, make this an active server group by checking **Active Group**. d. Add servers to the group by clicking **Add** under DHCP Servers. The phrase *Click to enter value* appears in the IP Address column. e. Select *Click to enter value* and then enter an IP Address. f. Click **OK**. The server is added to the DHCP server group list. g. Add a relay interface group by clicking **Add** under Add Relay Interface Group. The Add DHCP Relay Interface window opens. h. Type a DHCP interface group name. i. Select a server group from the Server Group list. j. Click **OK**. The group is added to the Relay Interface Group list.

Click either **Next** or **Review**, to see the Review page. For review directions, see "Reviewing and Saving a Device Common Settings Configuration" on page 222.

Specifying DNS Settings for Wireless Device Common Settings

To configure the DNS settings for a wireless device profile, enter the settings described in Table 66 on page 218. All settings are optional.

Table 66: Device Profile DNS Settings for Wireless

Task	Action
DNS Settings	

Copyright © 2013, Juniper Networks, Inc.

Table 66: Device Profile DNS Settings for Wireless *(continued)*

Task	Action
Add a Domain Name Server	To add a Domain Name Server (DNS) for wireless common settings: 1. Click **Add** under Domain Name Servers. The Add Server window opens. 2. Enter the IP address of the DNS server. 3. Select a preference for the server, either **Primary** (default) or **Secondary**. TIP: You can add only one primary IP address, but can add several secondary IP addresses. 4. Click **OK**. The IP address and preference are now listed in the list of Domain Name Servers. TIP: To modify an IP address, select it from the Domain Name Servers table and click **Edit**. To delete an IP address, select it from the Domain Name Servers table and click **Delete**.

Click either **Next** or **Review**, to see the Review page. For review directions, see "Reviewing and Saving a Device Common Settings Configuration" on page 222.

Specifying DHCP Relay/DNS Settings for Campus Switching ELS Device Common Settings

To configure the DHCP relay and DNS settings for a Campus Switching ELS device profile, enter the settings described in Table 67 on page 219. All settings are optional.

Table 67: Device Profile Protocol Settings for ELS Switching

Task	Action
DHCP Relay DHCP relay enables a switch to relay DHCP requests from a client to a DHCP server when the client and server do not reside on the same VLAN. You define the client interfaces for DHCP relay as part of the process of assigning the profile to a device. Select **Enable DHCP Relay** to enable DHCP Relay and view the DHCP Relay configuration.	
Configure Legacy DHCP Relay for ELS Switches	To configure Legacy DHCP Relay for Campus Switching ELS: 1. Select **Legacy DHCP Relay** (default). 2. Add DHCP servers for Legacy DHCP Relay: a. Click **Add** under DHCP Servers. The Add Server window opens. b. Enter the IP address of the DHCP server and then click **OK**. The DHCP server name appears in the list of DHCP servers. TIP: You can add more than one DHCP server.

Copyright © 2013, Juniper Networks, Inc.

Table 67: Device Profile Protocol Settings for ELS Switching *(continued)*

Task	Action
Configure Extended DHCP Relay for Campus Switching ELS	To add Extended DHCP Relay to this Campus Switching ELS Device Profile: 1. Select **Extended DHCP Relay**. 2. Add one or more DHCP Servers Groups to the Device Common Settings profile: a. Click **Add** under Add DHCP Servers Group. The Add Server Group window opens. b. Provide a name for the server group. c. Optionally, make this an active server group by checking **Active Group**. d. Add servers to the group by clicking **Add** under DHCP Servers. The phrase *Click to enter value* appears in the IP Address column. e. Select *Click to enter value* and then enter an IP Address. f. Click **OK**. The server is added to the DHCP server group list. g. Add a relay interface group by clicking **Add** under Add Relay Interface Group. The Add DHCP Relay Interface window opens. h. Type a group name for the DHCP interface. i. Select a server group from the Server Group list. j. Click **OK**. The group is added to the Relay Interface Group list.
DNS Settings	
Add a domain name server	To add a domain name server to the Campus Switching ELS Common Settings: 1. Click **Add** under Domain Name Servers. The Add Server window opens. 2. Provide an IP address for the DNS server. 3. Click **OK**. The server is added to the Domain Name Servers list. TIP: To edit a DNS server's settings, select it and then click **Edit**. To delete a DNS server, select it and then click **Delete**.

Click either **Next** or **Review**, to see the Review page. For review directions, see "Reviewing and Saving a Device Common Settings Configuration" on page 222.

Specifying Protocol Settings for Data Center Switching Device Common Settings

To configure the protocol settings for a device profile, enter the settings described in Table 68 on page 221. All settings are optional.

Copyright © 2013, Juniper Networks, Inc.

Table 68: Device Profile Protocol Settings for Data Center

Field	Action
Spanning Tree Protocol Settings	Select one of spanning-tree protocol (STP) settings for switches: **STP**, **RSTP**, **MSTP**, or **None of these**. • Spanning Tree Protocol—With STP configured, the switches use the IEEE 802.1D 2004 specification, force version 0. This configuration runs a version of RSTP that is compatible with classic, basic STP as defined in the 802.1D 1998 specification. • Rapid Spanning Tree Protocol—RSTP provides faster reconvergence time than the original STP by identifying certain links as point-to-point and by using protocol handshake messages rather than fixed timeouts. VLAN Spanning Tree Protocol (VSTP) and RSTP can be configured concurrently. You can selectively configure up to 253 VLANs using VSTP; the remaining VLANs will be configured using RSTP. VSTP and RSTP are the only spanning-tree protocols that can be configured concurrently on a switch. • Multiple Spanning Tree Protocol—MSTP enables multiple VLANs to be mapped to the same spanning-tree instance, reducing the number of spanning-tree instances needed to support a large number of VLANs. MSTP provides multiple forwarding paths for data traffic and enables load balancing. It improves the fault tolerance of the network because a failure in one instance, or forwarding path, does not affect other instances. Select the **Enable VSTP** check box to enable VSTP.
Multicast Settings	Select a multicast setting for switches: • Enable IGMP—Enables IGMP on all the interfaces for the selected device. (Default is disabled.) • Enable IGMP Snooping—Enables IGMP snooping IGMP snooping on all VLANs. (Default is enabled.)
DCBX Settings	Select the Data Center Bridging Capability Exchange (DCBX) protocol features that you want to enable: • **Enable DCBX**—DCBX is a discovery and exchange protocol for conveying configuration and capabilities among neighbors to ensure consistent configuration across the network. It is an extension of Link Layer Discovery Protocol (LLDP). • **Enable LLDP Snooping**—LLDP is a discovery and exchange protocol for conveying configuration and capabilities among neighbors to ensure consistent configuration across the network.
Enable DHCP Relay	Select **Enable DHCP Relay** to enable DHCP relay. DHCP relay enables a switch to relay DHCP requests from a client to a DHCP server when the client and server do not reside on the same VLAN. You will define the client interfaces for DHCP relay as part of the process of assigning the profile to a device.

Copyright © 2013, Juniper Networks, Inc.

Table 68: Device Profile Protocol Settings for Data Center *(continued)*

Field	Action
Add DHCP Relay Servers	To add DHCP servers: 1. Click **Add**. The Add Server window opens. 2. Enter the IP address of the DHCP server and then click **OK**. The DHCP server name appears in the list of DHCP servers. 3. You can enter more than one DHCP server. TIP: Select an IP Address from the DHCP Servers table and click **Edit** if you want to modify the IP address. Select an IP Address from the DHCP Servers table and click **Delete** to remove from the table.
DNS Settings	To configure DNS: 1. Click **Add** to add a DNS server. The Add Server window opens. 2. Enter the IP address of the DNS server. 3. Click **OK**. TIP: Select an IP Address from the Domain Name Servers table and click **Edit** if you want to modify the IP address. Select an IP Address from the Domain Name Servers table and click **Delete** to remove from the table.

Click either **Next** or **Review**, to see the Review page. For review directions, see "Reviewing and Saving a Device Common Settings Configuration" on page 222.

Reviewing and Saving a Device Common Settings Configuration

From this page, you can save or make changes to Device Common Settings:

- To make changes to the settings, click the **Edit** associated with the configuration you want to change.

  Alternatively, you can also click appropriate sections of the workflow at the top of the page that corresponds to the configuration you want to change.

  When you have completed your modifications, click **Review** to return to this page.
- To save a new profile or to save modified settings to an existing profile, click **Finish**.

  The Manage Device Common Settings page is displayed with the new or modified profile listed

What To Do Next

Once the Device Common Settings profile is created, you must assign the profile to the required device using the Manage Device Profile page and then deploy the device profile using the **Deploy** mode. To assign a Device Common Settings profile to a device, see

Copyright © 2013, Juniper Networks, Inc.

"Assigning Device Common Settings to Devices" on page 375. For details about deploying your configurations, see *Deploying Configuration to Devices*.

NOTE: **A device can have only one device profile assigned to it. However, you can assign the same device profile to multiple devices.**

Related Documentation

- Assigning Device Common Settings to Devices on page 375
- *Deploying Configuration to Devices*

Creating and Managing Fabric Profiles

A Fabric profile contains configuration settings for a gateway Fibre Channel (FC) fabric. A gateway FC fabric creates associations that connect Fibre Channel over Ethernet (FCoE) devices with converged network adapters (CNAs) on the Ethernet network to an FC switch on the Fibre Channel network. You can assign Fabric profiles to QFX Series devices that act as a FCoE-FC gateway, to configure gateway FC fabrics.

This topic describes:

- Managing Fabric Profiles on page 223
- Creating Fabric Profiles on page 224
- Specifying Settings for a Fabric profile on page 225
- What to Do Next on page 227

Managing Fabric Profiles

From the Manage Fabric Profiles page, you can:

- Create a new profile by clicking **Add**.
- Modify an existing profile by selecting it and clicking **Edit**.
- Associate a profile to specific interfaces by selecting it and clicking **Assign**.

  During the assignment process, you will have the option to configure interface-specific settings.
- Change a profile's current interface assignments by selecting it and clicking **Edit Assignments**.
- View information about a profile by selecting the group and clicking **Details** or by clicking the profile name.
- Clone a profile by selecting a profile and clicking **Clone**.
- Delete profiles by selecting the profile and clicking **Delete**.

Copyright © 2013, Juniper Networks, Inc.

TIP: You cannot delete profiles that are in use—that is, assigned to objects or used by other profiles. To see the current assignments for a profile, select the profile and click **Details**.

Table 69 on page 224 describes the information provided about Fabric profiles on the Manage Fabric Profiles page. This page lists all Fabric profiles defined for your network, regardless of your current selected scope in the network view.

Table 69: Fabric Profile Information

Field	Description
Fabric Name	Name given to the profile when it was created.
Fabric ID	Number from 1 through 4094 assigned to the Fabric profile when it was created.
Device Family	Device family to which the profile applies.
Description	Any description added when the profile was created.
Assignment State	One of the following: • Deployed—The profile has been assigned to interfaces and the configuration has been deployed on the devices. • Pending Deployment—The profile has been assigned to interfaces or its previous assignments have been changed, but the new or modified configuration has not yet been deployed on the devices. • Unassigned—The profile has not yet been assigned to interfaces.
Creation Time	Date and time when this profile was created.
Last Updated Time	Date and time when this profile was last modified.
Username	The username of the user who created or modified the profile.

TIP: All columns might not be displayed. To show or hide fields in the table, click the down arrow on the field header, select Columns, and select or clear the check box adjacent to the field that you want to show or hide.

Creating Fabric Profiles

To create a Fabric profile:

1. From the Network Director Banner, select **Build** mode.
2. Click **Fabric** under Profile and Configuration Management in the Tasks pane.

   The Manage Fabric profiles page appears.

Copyright © 2013, Juniper Networks, Inc.

3. Click **Add**.

   The Create Fabric Profile page appears.

4. Enter settings for the Fabric profile as described in "Specifying Settings for a Fabric profile" on page 225.

5. Click **Done**.

Specifying Settings for a Fabric profile

Use the Create Fabric profile page to define a common set of attributes in a Fabric profile, which you can then apply to Fibre Channel (FC) interfaces on Data Center Switching devices.

TIP: You can reference VLAN profiles in a Fabric profile. Create these profiles before you create Fabric profiles.

After you create a Fabric profile, you can assign it to devices, individual interfaces, or port groups. During this process, you can also configure interface-specific attributes. You can assign only one Fabric profile to an interface or port group.

Table 70 on page 225 describes the Fabric profile settings. Mandatory settings are indicated by a red asterisk (*) that appears next to the field label in the user interface.

Table 70: Fabric Profile Settings

Field	Action
Fabric Name	Type a name for the profile. The value must be a string between 2 and 64 characters long, begin with a letter, and consist of letters, numbers, periods, dashes, and underscores only.
Fabric ID (1-4096)	Type an ID number from 1 through 4094.
Description	Type a description of the Fabric profile, which will appear on the Manage Fabric Profiles page.
Max Login Sessions (128-2500)	Set the maximum number of FCoE initialization protocol (FIP) session logins permitted for the FCoE-FC gateway fabric. The range is 128 through 2500. The default is 2500.
VLAN Profiles	
Add	Click **Add** to select FCoE VLAN profiles to assign to the Fabric profile. Select the VLAN profiles from the list, then click **OK**.
Remove	To remove VLAN profiles, select one or more profiles, then click **Remove**.
Proxy Settings	

Copyright © 2013, Juniper Networks, Inc.

Table 70: Fabric Profile Settings *(continued)*

Field	Action
Load Balance Algorithm	Set the load-balancing algorithm that the QFX Series uses to distribute FCoE sessions (FLOGI and FDISC sessions from the FCoE devices in the Ethernet network) among the NP_Port links to the FC switch. NOTE: Changing the load-balancing algorithm when FCoE sessions are running forces the FCoE sessions to log out, and then log in again. Select one of the following: • simple—Load balancing is based on the weighted utilization (load) of the NP_Ports connected to an FC fabric. Each new FLOGI or FDISC is assigned to the least-loaded link. When a link load rebalance occurs, the system minimizes disruption by using an algorithm to log out only the sessions that need to be moved to other links to balance the link load. To further minimize disruption, the algorithm logs out the sessions with the fewest dependencies (for example, FDISC sessions are logged out before FLOGI sessions). When the sessions log in again, they are placed on NP_Port interfaces in a manner that balances the link loads. This is the default load-balancing algorithm. • enode-based—Load balancing is based on the ENode FLOGI. When an ENode logs in to the fabric, all subsequent FDISC sessions (VN_Port sessions) associated with that ENode are placed on the same link as the ENode FLOGI session, regardless of the link load. New ENode FLOGIs are placed on the least-loaded link. When a link load rebalance occurs, the system logs off all sessions. The sessions log in again and are placed on NP_Port interfaces in a balanced manner. • flogi-based—FLOGI-based load balancing is similar to ENode-based load balancing, but the behavior when the loads are rebalanced is different. Load balancing is based on the ENode FLOGI. When an ENode logs in to the fabric, all subsequent FDISC sessions associated with that ENode are placed on the same link as the ENode FLOGI session, regardless of the link load. New ENode FLOGIs are placed on the least-loaded link. When a link load rebalance occurs, the system minimizes disruption by using an algorithm to log out only the sessions that need to be moved to other links to balance the link load. When the logged out sessions log back in, they are placed on NP_Port interfaces in a manner that balances the link loads.
Disable Worldwide Name Verification (default is disabled)	Select to Disable the fabric worldwide name (WWN) verification check in the fabric login accept message (FLOGI-ACC) for implicit FLOGIs. If you enable this option, when a QFX Series NP_Port performs a FLOGI to the FC fabric, the QFX Series does not verify the fabric WWN in the FLOGI-ACC against the current fabric WWN. NOTE: Disabling or enabling the fabric WWN verification check logs out all FCoE sessions.
FIP Settings	
FCoE Trusted (default is disabled)	Select to enable the specified 10-Gigabit Ethernet interface to trust Fibre Channel over Ethernet (FCoE) traffic. If an interface is connected to another switch such as an FCoE forwarder (FCF) or a transit switch, you can configure the interface as trusted so that the interface forwards FCoE traffic from the switch to the FCoE devices without installing FIP snooping filters. Configure the specified local Fibre Channel fabric to trust FCoE traffic on all ports in the fabric. Changing the fabric ports from untrusted to trusted removes any existing FIP snooping filters from the ports. Changing the fabric ports from trusted to untrusted by removing the fcoe-trusted configuration from the fabric forces all of the FCoE sessions on those ports to log out so that when the ENodes and VN_Ports log in again, the switch can build the appropriate FIP snooping filters.

Copyright © 2013, Juniper Networks, Inc.

Table 70: Fabric Profile Settings *(continued)*

Field	Action
FCoE Mapped Address	Set the FCoE mapped address prefix (FC-MAP) value for the FCoE VLAN to match the FC switch (or FCoE forwarder) FC-MAP value for the FC fabric. The FC-MAP value is a unique MAC address prefix an FC switch uses to identify FCoE traffic for a given FC fabric (traffic on a particular FCoE VLAN). Enter an FC-MAP value, which is a hexadecimal value preceded by "0x". The range is 0x0EFC00 through 0x0EFCFF. The default value is 0xEFC00. You can configure the FC-MAP value or use the default value. The FC switch provides the FC-MAP value to FCoE nodes (ENodes) in the FIP discovery advertisement message. If the EX Series switch or the QFX Series FCoE VLAN FC-MAP value does not match the FC switch FC-MAP value, neither device discovers the FC switch on that VLAN, and the ENodes on that VLAN cannot access the FC switch. The FC switch accepts only FCoE traffic that uses the correct FC-MAP value as part of the VN_Port MAC address. When the QFX Series acts as an FCoE-FC gateway, the FC-MAP value for the gateway and the FCoE devices must match the FC switch FC-MAP value in order to communicate with the FC switch. NOTE: Changing the FC-MAP value causes all logins to drop and forces the ENodes to log in again.
Keep Alive Interval (default is 8000)	Set the global interval between periodic FIP keepalive advertisements, in milliseconds. The range is 250 through 90000 milliseconds. The default is 8000 milliseconds.
Priority (default is 0)	Set the global priority value associated with the switch FCF-MAC. CNAs use the priority value to determine the switch with which they will perform FIP FLOGI. The lower the value, the higher the priority. The switch advertises this value to the server ENodes on the FCoE network. The range is 0 through 255. The default value is 128.
Max Sessions Per Node	Set the maximum number of FCoE login sessions (FLOGI plus FDISC) from a single ENode allowed on the gateway FC fabric (the fabric configured on the QFabric system). The maximum number of logins per ENode is 2000 sessions. NOTE: A session is a FLOGI or FDISC login to the FC SAN fabric. Session does not refer to end-to-end storage sessions. There is no limit to the number of end-to-end storage sessions.

What to Do Next

Once the Fabric profile is created, you must assign the profile using the Assign Device Profile page to the required devices and then deploy the device configuration changes using the Deploy mode. To assign a Fabric profile, see "Assigning a Fabric Profile to Devices and Ports" on page 377. For information about deploying your configurations, see *Deploying Configuration to Devices*.

Related Documentation

- Understanding Fabric Profiles on page 30
- Assigning a Fabric Profile to Devices and Ports on page 377

Copyright © 2013, Juniper Networks, Inc.

Creating and Managing FC Gateway Service Profiles

An FC Gateway Service profile provides a quick way to configure Fibre Channel (FC) gateways on Data Center Switching devices. It is intended for FC gateway devices that are connected directly to the FCoE network, without transit switches. In addition to the settings you can specify, the profile creates an FC gateway configuration with some default settings that cannot be modified. For example, you cannot specify any CoS settings for the FC gateway; only the default settings are available.

If you want to configure an FC gateway that does not meet these requirements, you can use other profiles to configure the components of the FC gateway and assign them to the appropriate devices, ports, and profiles. See "Configuring Fibre Channel Gateways" on page 132 for more information.

To manage or create FC Gateway Service profiles: In Build mode, select **FC Gateway Service** from Profile and Configuration Management in the Tasks pane. The FC Gateway Service Profile page appears.

This topic describes:

- Managing FC Gateway Service Profiles on page 228
- Creating FC Gateway Service Profiles on page 229
- Specifying Settings for an FC Gateway Service Profile on page 230
- What to Do Next on page 230

Managing FC Gateway Service Profiles

From the FC Gateway Service Profile page, you can:

- Create a new profile by clicking **Add**.
- Modify an existing profile by selecting it and clicking **Edit**.
- Associate a profile to specific interfaces by selecting it and clicking **Assign**.

  During the assignment process, you will have the option to configure interface-specific settings.
- Change a profile's current interface assignments by selecting it and clicking **Edit Assignments**.
- View information about a profile by selecting the group and clicking **Details** or by clicking the profile name.
- Clone a profile by selecting a profile and clicking **Clone**.
- Delete profiles by selecting the profiles and clicking **Delete**.

TIP: You cannot delete profiles that are in use—that is, assigned to objects or used by other profiles. To see the current assignments for a profile, select the profile and click **Details**.

Copyright © 2013, Juniper Networks, Inc.

Table 71 on page 229 describes the information provided about FC Gateway Service profiles on the Manage FC Gateway Service Profile page. This page lists all FC Gateway Service profiles defined for your network, regardless of your current selected scope in the network view.

Table 71: FC Gateway Service Profile Information

Field	Description
Profile Name	Name given to the profile when it was created.
Fabric ID	Fabric ID number assigned to the profile.
FCoE VLAN Name	Name of the FCoE VLAN assigned to the profile.
FCoE VLAN Id	ID of the FCoE VLAN assigned to the profile.
Native VLAN Name	Name of the native VLAN assigned to the profile.
Native VLAN Id	ID of the native VLAN assigned to the profile.
Description	Description given to the profile when it was created.
Assignment State	Profile assignment state. One of the following: • Deployed—The profile has been assigned and the configuration has been deployed on the devices. • Pending Deployment—The profile has been assigned or its previous assignments have been changed, but the new or modified configuration has not yet been deployed on the devices. • Unassigned—The profile has not yet been assigned.

TIP: All columns might not be displayed. To show or hide fields in the table, click the down arrow on the field header, select Columns, and select or clear the check box adjacent to the field that you want to show or hide.

Creating FC Gateway Service Profiles

To create an FC Gateway Service profile:

1. From the Network Director Banner, select **Build** mode.
2. Click **FC Gateway Service** under Profile and Configuration Management in the Tasks pane.

   The FC Gateway Service Profiles page appears.
3. Click **Add**.

   The Create Gateway Profile page appears.

Copyright © 2013, Juniper Networks, Inc.

4. Enter settings for the FC Gateway Service profile as described in "Specifying Settings for an FC Gateway Service Profile" on page 230.
5. Click **Done**.

Specifying Settings for an FC Gateway Service Profile

Use the Create Gateway Profile page to define specify settings for an FC Gateway Service profile, which you can then assign to interfaces on Data Center Switching devices.

Table 72 on page 230 describes the settings.

Table 72: FC Gateway Service Profile Settings

Field	Description
Profile Name	Enter a name for the profile.
Description	Enter a description for the profile.
Fabric ID	Enter an FC gateway fabric ID number from 1 through 4094.
FCoE VLAN Name and ID	Enter an FCoE VLAN Name and ID.
Native VLAN Name and ID	Enter a native VLAN Name and ID.
FC Map	The FC-MAP value is a unique MAC address prefix an FC switch uses to identify FCoE traffic for a given FC fabric (traffic on a particular FCoE VLAN). Range: 0x0EFC00 through 0x0EFCFF. Default: 0xEFC00
Priority	Set the global priority value associated with the switch FCF-MAC. CNAs use the priority value to determine the switch with which they will perform FIP FLOGI. The lower the value, the higher the priority. The switch advertises this value to the server ENodes on the FCoE network. Range: 0 through 255. Default: 128
FCoE Trusted	Select to enable the interface to trust FCoE traffic. If an interface is connected to another switch such as an FCoE forwarder (FCF) or a transit switch, you can configure the interface as trusted so that the interface forwards FCoE traffic from the switch to the FCoE devices without installing FIP snooping filters.
Port Max Packet Size	Select the maximum packet size. Range: 256-9216. Default: 2400

What to Do Next

Once the FC Gateway Service profile is created, you must assign the profile to the required devices by using the Assign Device Profile page and then deploy the device configuration changes by using Deploy mode. To assign an FC Gateway Service profile, see "Assigning an FC Gateway Service Profile to Ports" on page 381. For information about deploying your configurations, see *Deploying Configuration to Devices*.

Copyright © 2013, Juniper Networks, Inc.

Related Documentation

- Assigning an FC Gateway Service Profile to Ports on page 381

Creating and Managing Filter Profiles

Filter profiles are a set of rules that determine whether to accept or discard packets transiting on either a switch or wireless radio interface.

Use the Manage Filter Profiles page to create new Filter profiles and manage existing Filter profiles.

To display the Manage Filter Profiles page: In Build mode, select **Filter** from Profile and Configuration Management in the Tasks pane. The Manage Filter Profiles page appears.

This topic describes:

- Managing Filter Profiles on page 231
- Creating a Filter Profile on page 232
- Specifying Settings for an EX Series Switch Filter Profile on page 233
- Specifying Settings for a Wireless Filter Profile (WLC) on page 245
- Specifying Settings for a Campus Switching ELS Switch Filter Profile on page 250
- Specifying Settings for Creating a Data Center Switching Filter Profile on page 262
- What To Do Next on page 273

Managing Filter Profiles

From the Manage Filter Profiles page, you can:

- Create a new Filter profile by clicking **Add**. For directions, see "Creating a Filter Profile" on page 232.
- Modify an existing Filter profile by selecting it and clicking **Edit**.
- View information about a Filter profile, including the associated interfaces, by either clicking the profile name or by selecting the profile and clicking **Details**.
- Delete a Filter profile by selecting a profile and clicking **Delete**.

TIP: **You cannot delete profiles that are in use—that is, profiles assigned to objects or used by other profiles. To see the current assignments for a profile, select the profile and click Details.**

- Clone a Filter profile by selecting a profile and clicking **Clone**.

Table 73 on page 232 describes the information provided about Filter profiles on the Manage Filter Profiles page. This page lists all Filter profiles defined for your network, regardless of the scope you selected in the network view.

Copyright © 2013, Juniper Networks, Inc.

Table 73: Manage Filter Profile Fields

Field	Description
Profile Name	Name given to the profile when the profile was created.
Family Type	The device family on which the profile was created, either **Switching (EX)**, **Wireless (WLC)**, **Campus Switching ELS**, or **Data Center Switching Non ELS**.
Description	Description of the profile entered when the profile was created. TIP: To display the entire description, you might need to resize the Description column by clicking the column border in the heading and dragging it.
Filter Family	The filter family for which the Filter profile was created. The filter family can be either **Ethernet switching**, **INET**, **INET6**, or **NA** (for wireless).
Creation Time	Date and time when this profile was created.
Update Time	Date and time when this profile was last modified.
User Name	The username of the user who created or modified the profile.

TIP: **All columns may not be displayed. To show or hide fields in the table, click the down arrow on the field header, select Columns, and select or clear the check box adjacent to the field that you want to show or hide.**

Creating a Filter Profile

To create a Filter profile, you must provide a filter name and configure at least one term. A term is a collection of one or more match conditions, and actions that the system takes when match conditions are met. A term must have at least one match condition.

To create a Filter profile:

1. Click

in the Network Director banner.
2. Under Select View, select either **Logical View**, **Location View**, **Device View** or **Custom Group** View.

   TIP: **Do not select Virtual View or Topology View.**
3. Click **Filter** under Profile and Configuration Management in the Tasks pane.

   The Manage Filter Profiles page appears.
4. Click **Add**.

Copyright © 2013, Juniper Networks, Inc.

The Device Family Chooser window opens.

5. From the Device Family Chooser, select the device family for which you want to create a Filter profile. The available device families are **Switching (EX)**, **Wireless (WLC)**, **Campus Switching ELS**, and **Data Center Switching Non-ELS**.
6. Click **OK**.

   The Create Filter Profile wizard for the selected device family is displayed.
7. Specify the filter settings by following these directions:
   - For EX Series switches, specify the settings as described in "Specifying Settings for an EX Series Switch Filter Profile" on page 233.
   - For controllers, specify the settings as described in "Specifying Settings for a Wireless Filter Profile (WLC)" on page 245.
   - For Campus Switching ELS, specify the settings as described in "Specifying Settings for a Campus Switching ELS Switch Filter Profile" on page 250.
   - For Data Center Switching, specify the settings as described in "Specifying Settings for Creating a Data Center Switching Filter Profile" on page 262.
8. Click **Done** to save the Filter profile.

   The system saves the Filter profile and displays the Manage Filter Profiles page. Your new or modified Filter profile is listed in the table of Filter profiles.

Specifying Settings for an EX Series Switch Filter Profile

A Filter profile must have at least one term in it. Each term has one filtering function. For example, if a term is evaluating the source of packets, then that term cannot also evaluate the protocols used by the packets. Some switch models do accommodate multiple terms in one filter. When you have more than one term in a filter, the ordering of the terms is important. The system evaluates multiple filter terms as follows:

- The packet is evaluated against the first term's conditions. If the packet matches all of the conditions in that term, the action specified for that condition is taken and evaluation ends. Subsequent terms in the filter are not evaluated.
- If a packet does not match all conditions in the first term, the packet is then evaluated against the conditions in the second term. This process continues until either the packet matches all conditions in a term or there are no more terms in the filter. Whenever a match occurs, the term's corresponding action is taken and evaluation ends—subsequent terms in the filter are not evaluated.
- If a packet passes through all the terms in the filter without a match, the packet is discarded.

To configure a Filter profile for EX Series switches:

1. Specify a filter name and description for the Filter profile.
2. Select the switch filter family for which you want to create the profile:
   - If you want to create a Layer 2 based filter, select **Ethernet switching**.

Copyright © 2013, Juniper Networks, Inc.

- If you want to create a Layer 3 based filter for IPv4, select **INET**.
- If you want to create a Layer 3 based filter for IPv6, select **INET6**.

3. Under Terms, click **Add** to add one or more terms with match condition(s) for this filter.

   The Create Term window opens with a section for each type of term you can create, Source and Destination Parameters, Protocols, DSCP Settings, TCP Settings, and ICMP Settings. The Action section applies to all of those types.

   NOTE: **The order of the terms within a Filter profile configuration is important. Packets are tested against each term in the order in which terms are listed.**

4. Enter a name for the filter term.
5. Specify the match condition(s) for the filter term as described in Table 74 on page 234. Required settings are indicated by a red asterisk (*) that appears next to the field label in the user interface.

Table 74: Create Term Fields for EX Switching

Task	Description
Source and Destination Parameters	
You can specify match conditions for either packets' origin (source) or packets' destination, or both. You are indicating the location of the filtering here—either specifying that packets that originate at a specific place (source) will be filtered or packets destined for a specific location (destination) will be filtered. You can have multiple sources and destinations for one filter term.	

Copyright © 2013, Juniper Networks, Inc.

Table 74: Create Term Fields for EX Switching *(continued)*

Task	Description
Add Source Parameters and Destination Parameters	To add source and destination parameters to the named filter term: a. Click **Add** to the right of the Destination Parameters list. The Add Source/Destination Parameter window appears. b. Select either **Source** (default) or **Destination** from the Add Source/Destination Parameter page. c. Select one of following available Parameter Types from the Add Source/Destination Parameter page and provide the corresponding information: TIP: Available parameter types vary. • **IP Address**—also provide the IP address of the source or destination device • **MAC Address**—also provide the MAC address of the source or destination device • **Port**—also provide the port type of the source or destination port. Select either **AFS** (Andrew File System), **BGP** (Border Gateway Protocol), **BIFF** (UNIX mail notification), **Bootpc** (bootstrap protocol client), **Bootps**, **Cmd**, **CVS pserver**, **DHCP**, **Domain**, **EK login**, **EK shell**, **EXEC**, **Finger** (protocol), or **FTP**. NOTE: If you selected Port as the parameter and do not find the type of port that you want to add from the Port list, then select **Other** and enter a port number. d. Click **OK** The parameter term is added to the appropriate list, either Source Parameters or Destination Parameters.
Protocols and EtherTypes For either INET family, you can apply a filter term based on protocols being used by packets. For the Ethernet-switching family, you can apply a filter term based on either the protocols being used by packets or on the EtherTypes being used by packets. EtherType indicates a protocol that is encapsulated in the payload of an Ethernet Frame. Expand the Protocols section to see the configuration.	
Add a Protocol Match Condition (Ethernet-switching family or INET family)	To add a protocol match condition to the named filter term: a. Expand the Protocols and EtherTypes section. b. Click **Add** under Protocols. The Select Protocols window opens with a list of protocols. c. From the list of protocols, select one or more. The options are **AH**, **DSTOPTS**, **EGP**, **ESP**, **Fragment**, **GRE**, **Hop-by-hop**, **ICMP**, **ICMP6**, **IPIP**, **IPv6**, **No-text-header**, **OSPF**, **PIM**, **Routing**, **RSVP**, **SCTP**, **TCP**, **UDP**, and **VRRP**. d. Click **OK**. The protocols are added to the Protocols list.

Copyright © 2013, Juniper Networks, Inc.

Table 74: Create Term Fields for EX Switching *(continued)*

Task	Description
Add an EtherType Match Condition (Ethernet-switching family)	To add an EtherType match condition to the named filter Ethernet-switching family term: a. Expand the Protocols and EtherTypes section. b. Click **Add** under EtherTypes. The Select EtherTypes window opens with a list of protocols. c. From the list of EtherTypes, select one or more. The options are **AARP**, **AppleTalk**, **ARP**, **IPv4**, **IPv6**, **MPLS multicast**, **MPLS unicast**, **OAM**, **PPP**, **PPPOE discovery**, **PPPOE session**, and **SNA**. d. Click **OK**. The EtherTypes are added to the EtherTypes list.

DSCP Settings

Expand this section to see the DSCP term settings. DiffServ is a simple mechanism for classifying and managing network traffic and providing quality of service (QoS) on IP networks. DiffServ can, for example, be used to apply low-latency to critical network traffic such as voice or streaming media while providing simple best-effort service to non-critical services such as Web traffic. Here, you can apply a filter term based on the Differentiated Services code point (DSCP) which is a field in IPv4 and IPv6 headers.

NOTE: With IPv6 packets, the DS field and ECN field replace the IPv4 TOS field.

Copyright © 2013, Juniper Networks, Inc.

Table 74: Create Term Fields for EX Switching *(continued)*

Task	Description
Add a DSCP Match Condition	To add a DSCP match condition to the named filter term: NOTE: A DSCP IP match condition and a precedence match condition cannot be both specified for the same term. a. Click **Add** in the DSCP section to see a list of match conditions. The Select DSCP list appears. b. Select one or more of the following DSCP types from the list: • **AF11**—Assured forwarding class 1, low drop precedence • **AF12**—Assured forwarding class 1, medium drop precedence • **AF21**—Assured forwarding class 2, low drop precedence • **AF22**—Assured forwarding class 2, medium drop precedence • **AF23**—Assured forwarding class 2, high drop precedence • **AF31**—Assured forwarding class 3, low drop precedence • **AF32**—Assured forwarding class 3, medium drop precedence • **AF33**—Assured forwarding class 3, high drop precedence • **AF41**—Assured forwarding class 4, low drop precedence • **AF42**—Assured forwarding class 4, medium drop precedence • **AF43**—Assured forwarding class 4, high drop precedence • **BE**—Best effort (default) • **EF**-Expedited forwarding • **CS0**—Class selector 0 • **CS1**—Class selector 1 • **CS2**—Class selector 2 • **CS3**—Class selector 3 • **CS4**—Class selector 4 • **CS5**—Class selector 5 • **CS6**—Class selector 6 • **CS7**—Class selector 7 c. Click **OK**. The DSCP code term for the named filter is added to the DSCP list.

Copyright © 2013, Juniper Networks, Inc.

Table 74: Create Term Fields for EX Switching *(continued)*

Task	Description
Add a Precedence match condition	You can apply an IP precedence match condition to the named term. With IP precedence, a device prioritizes traffic by class first. Then it differentiates and prioritizes same-class traffic. NOTE: The two match conditions IP Precedence and DSCP cannot be simultaneously applied to a term. To apply an IP precedence value match condition to the named term: a. Click **Add** in the Precedence section. The Select Precedence list appears. b. Select one of the following precedence settings from the list: **Routine** (0 or lowest, also called Best Effort), **Priority** (1), **Immediate** (2), **Flash** (3, mainly used for voice signaling or for video), **Flash-override** (4), **Critical-ECP** (5, mainly used for voice RTP), **Internet-control** (6, used for IP routing protocols), or **Net-control** (7 or highest, used for link layer and routing protocol keep alive). c. Click **OK**. The precedence match condition is added to the named term, and the condition is listed in the Precedence list.
TCP Settings Expand this section to see the TCP term settings. The Transmission Control Protocol (TCP) is the most common core protocol of the Internet protocol suite (IP). TCP provides reliable, ordered, error-checked delivery of a stream of octets between programs running on computers connected to the Internet or an intranet. You can use the TCP initial flag for a match condition.	
Enable TCP Initial flag match condition	Select to use the TCP initial flag for a match condition. The TCP flags option becomes unavailable as a result.
Enable other TCP flag match conditions	If you are not using the TCP initial flag for a match condition, select one of the TCP flags from the list—**RST**, **ACK**, **SYN**, **Urgent**, **Push**, **FIN**, **None**. These flags have the following meaning: • RST—Reset flag indicates that the TCP connection will be reset. • ACK—Third step in TCP three-way handshake for connection. In response to a server's SYN-ACK, the client replies with an ACK. • SYN—First step in TCP three-way handshake for connection. The active open is performed by the client sending a SYN to the server. • Urgent—If the URG flag is set, then the 16-bit field is an offset from the sequence number indicating the last urgent data byte. • Push—Push flags request that buffered data to the receiving application be sent now. • FIN—The final flag indicates that no more data will be sent.

Copyright © 2013, Juniper Networks, Inc.

Table 74: Create Term Fields for EX Switching *(continued)*

Task	Description
ICMP Settings Expand the ICMP Settings section to select an ICMP code value for the filter item's match condition. The Internet Control Message Protocol (ICMP) is one of the core IP protocols used by operating systems of networked computers to send error messages. ICMP can also be used to relay query messages.	
Add an ICMP Code match condition	To apply an ICMP code match condition to the named term: a. Click **Add** in the ICMP Codes section. The Select ICMP Code list appears. b. Select one or more ICMP codes from the list. These codes vary, depending on the Filter Family you selected. c. Click **OK**. The ICMP code match condition is listed in the ICMP Code list and added to the named term. NOTE: ICMP code specifies more specific information than ICMP type. Because the value's meaning depends upon the associated ICMP type, you must specify an ICMP type along with an ICMP code. The keywords are grouped by the ICMP type with which they are associated.
Add an ICMP Type match condition	NOTE: ICMP type specifies the ICMP packet type field. Typically, you specify this match condition in conjunction with the protocol match condition to determine which protocol is being used on the port. ICMP code specifies more specific information than ICMP type. Because the value's meaning depends upon the associated ICMP type, you must specify an ICMP type along with the ICMP code. The keywords are grouped by the ICMP type with which they are associated. To apply an ICMP type match condition to the named term: a. Click **Add** in the ICMP Type section. The Select ICMP Type list appears. b. Select one or more ICMP types from the list. Options vary, depending on which Filter Family you selected. c. Click **OK**. The ICMP type match condition is listed in the ICMP Type list and is added to the named term.
Action Select the action that the system performs on an IP packet if all match conditions that you specified above are met. Possible actions are Discard and Accept. The default action is to discard a packet that matches the filter term's conditions.	

Copyright © 2013, Juniper Networks, Inc.

Table 74: Create Term Fields for EX Switching *(continued)*

Task	Description
Action	Select either **Discard** or **Accept** to indicate what the filter term does with a packet when a match is made. NOTE: The remaining fields in this section are enabled only if you select **Accept** as the action.
Counter Name	When **Accept** is the action, specify a counter name.
Loss Priority	When **Accept** is the action, specify the packet loss priority, **Low**, **High**, or **None**. NOTE: Forwarding class and loss priority must be specified together for the same term.

Copyright © 2013, Juniper Networks, Inc.

Table 74: Create Term Fields for EX Switching *(continued)*

Task	Description
Policer	When you create a Filter profile, you can specify a policer action for any term or terms within the filter. Policing, or rate limiting, enables you to limit the amount of traffic that passes into or out of an interface. All traffic that matches a term that contains a policer action goes through the policer that the term references. You have two options with a policer. You can specify that an existing policer be used for the packet that matches the match condition. Or, you can create a new policer for the packet that matches the match condition. To select a policer from an existing list of policers, click **Select**. The Select Policer page appears. Select the policer that you want to use for the term and click **OK**. The system displays the selected policer in the Policer field in the Create Term page.

Copyright © 2013, Juniper Networks, Inc.

Table 74: Create Term Fields for EX Switching *(continued)*

Task	Description
	To create a new policer: a. Click **Create**. The Create Policer page appears. b. Type a name for the policer—you can use this policer again in the future. c. Select a policer type from the list, either a **single-rate-two-color** policer, or a **three-color-policer**. The type of policer that you select here affects the rest of the configurations available for the policer. If you selected a three-color-policer, then also select a rate for it, either **single-rate** or **two-rate**. • Single-rate two-color—A two-color policer (sometimes called simply *policer*) meters the traffic stream and classifies packets into two categories of packet loss priority (PLP) according to a configured bandwidth and burst-size limit. You can mark packets that exceed the bandwidth and burst-size limit or simply discard them. A two-color policer is most useful for metering traffic at the port (physical interface) level. • Single-Rate Three-color—This type of policer is defined in RFC 2697, A Single Rate Three Color Marker, as part of an assured forwarding (AF) per-hop-behavior (PHB) classification system for a Differentiated Services (DiffServ) environment. This type of policer meters traffic based on the configured committed information rate (CIR), committed burst size (CBS), and the excess burst size (EBS). Traffic is marked as belonging to one of three categories (green, yellow, or red) based on whether the packets are arriving at rates that are below the CBS (green), exceed the CBS but not the EBS (yellow), or exceed the EBS (red). A single-rate three-color policer is most useful when a service is structured according to packet size and not according to peak arrival rate. • Two-rate three-color—This type of policer is defined in RFC 2698, A Two Rate Three Color Marker, as part of an assured forwarding (AF) per-hop-behavior (PHB) classification system for a Differentiated Services (DiffServ) environment. This type of policer meters traffic based on the configured CIR and the peak information rate (PIR), along with their associated burst sizes; the CBS, and the peak burst size (PBS). Traffic is marked as belonging to one of three categories (green, yellow, or red) based on packets are arriving at rates that are below the CIR (green), exceed the CIR but not the PIR (yellow), or exceed the PIR (red). A two-rate three-color policer is most useful when a service is structured according to arrival rates and not to packet size. NOTE: The system displays and hides various fields in the Create Policer page depending on the type of policer that you want to create. d. Configure these fields for a single-rate-two-color policer: • Bandwidth Limit—Specify the traffic rate in bits per second, 1000 through 102,300,000,000 (102.3g) bps. • Burst Size Limit—Specify the maximum number of bytes allowed for incoming packets to burst above the peak information rate (PIR) and still be marked with medium-high packet loss priority (yellow). Packets that exceed the peak burst size (PBS) are marked with high packet loss priority (red). The range is 1500 through 100,000,000,000 bytes. • Action—Select either **Discard** or **None**.

Copyright © 2013, Juniper Networks, Inc.

Table 74: Create Term Fields for EX Switching *(continued)*

Task	Description
	• Loss Priority—Select either **High** or **None**. e. Configure these fields for a single-rate-three-color policer: • Committed Information Rate—Specify the guaranteed bandwidth (in bits per second) under normal line conditions and the average rate up to which packets are marked with low packet loss priority (green). The range is 32,000 through 40,000,000,000 bps. • Committed Burst Size—Specify the maximum number of bytes allowed for incoming packets to burst above the committed information rate (CIR) and still be marked with low packet loss priority (green). The range is 1500 through 100,000,000,000 bytes. • Excess Burst Size—Specify the maximum number of bytes allowed for incoming packets to burst above the committed information rate and still be marked with medium-high packet loss priority (yellow). Packets that exceed the excess burst size (EBS) are marked with high packet loss priority (red). The range is 1500 through 100,000,000,000 bytes. • Color Mode—Select the way the preclassified packets are to be metered: ◦ **Color-aware**—The local switch can assign a higher packet loss priority but cannot assign a lower packet loss priority. ◦ **Color-blind**—The local switch ignores the preclassification of packets and can assign a higher or lower packet loss priority. ◦ **None**—The preclassified packets are not metered. • Action—Options are **Discard** and **None**. • Loss Priority—Options are **High** and **None**.

Copyright © 2013, Juniper Networks, Inc.

Table 74: Create Term Fields for EX Switching *(continued)*

Task	Description
	f. Configure these fields for a three-color two-rate policer: • Committed Information Rate—Specify the guaranteed bandwidth (in bits per second) under normal line conditions and the average rate up to which packets are marked with low packet loss priority (green). The range is 32,000 through 40,000,000,000 bps. • Committed Burst Size—Specify the maximum number of bytes allowed for incoming packets to burst above the committed information rate (CIR) and still be marked with low packet loss priority (green). The range is 1500 through 100,000,000,000 bytes. • Peak Burst Size—Specify the maximum number of bytes allowed for incoming packets to burst above the peak information rate (PIR) and still be marked with medium-high packet loss priority (yellow). Packets that exceed the peak burst size (PBS) are marked with high packet loss priority (red). The range is 1500 through 100,000,000,000 bytes. • Peak Information Rate—Specify the maximum achievable rate in bits per second. Packets that exceed the peak information rate (PIR) are marked with high packet loss priority (red). You can configure a discard action for packets that exceed the PIR. The range is 32,000 through 40,000,000,000 bps. • Color Mode—Select the way the preclassified packets are to be metered: ◦ **Color-aware**—The local switch can assign a higher packet loss priority but cannot assign a lower packet loss priority. ◦ **Color-blind**—The local switch ignores the preclassification of packets and can assign a higher or lower packet loss priority. ◦ **None**—The preclassified packets are not metered. • Action—Options are **Discard** and **None**. • Loss Priority—Options are **High** and **None**. g. Click **OK**. The policer is added to the list of applied policers and the list of available policers.

Copyright © 2013, Juniper Networks, Inc.

Table 74: Create Term Fields for EX Switching *(continued)*

Task	Description
Forwarding Class	When **Accept** is the action, specify the forwarding class (or output queue) that is to be used for the packet that matches the match condition. You can create a new forwarding class or select from a list of available forwarding classes. To select a forwarding class from an existing list of classes, click **Select**. The Select Forwarding Class page appears. Select the forwarding class that you want to use for the packet and click **OK**. The system displays the selected forwarding class in the Forwarding Class field in the Create Term page. To create a new forwarding class: a. Click **Create**. The Create Forwarding Class page appears. b. Type a name for the forwarding class—you can use this forwarding class again in the future. c. Select a queue number from the list, and then click **OK**. The system creates a new forwarding class and displays it in the Forwarding Class field in the Create Term page.

Click **OK** to save the term and return to the Create Filter Profile page.

Specifying Settings for a Wireless Filter Profile (WLC)

A Filter profile must have at least one term in it. Each term has only one filtering function. For example, if a term is evaluating the source of packets, then that term cannot also evaluate the protocols used by the packets. Some switch models accommodate multiple terms in one filter. When you have more than one term in a filter, the ordering of the terms is important. The system evaluates multiple filter terms as follows:

- A packet is evaluated against the conditions in the first term of the filter. If the packet matches the conditions in the term, the corresponding action is executed and the evaluation ends. Subsequent terms in the filter are not evaluated.
- If a packet does not match the conditions in the first term, the packet is evaluated against the conditions in the second term. This process continues until either the packet matches conditions in one of the subsequent terms or there are no more terms in the filter. If a match is found, the corresponding action is executed and the evaluation ends. Subsequent terms in the filter are not evaluated.
- If a packet passes through all the terms in the filter without a match, the packet is discarded.

To configure a Filter profile on a controller:

1. Specify a filter name and description for the wireless Filter profile.
2. Click **Add** under Terms to add at least one term to the wireless filter. The Create Term window opens.

Copyright © 2013, Juniper Networks, Inc.

TIP: The order of the terms within a Filter profile configuration is important. Packets are tested against each term in the order in which the terms are listed in the Filter profile.

3. Enter the settings described in Table 75 on page 246 to create a wireless term. Required settings are indicated by a red asterisk (*) that appears next to the field label in the user interface.

Table 75: Term Fields for Wireless

Field	Description
Term name (all)	Provide a name for this term
Rule type (all)	Select the type of rule (or term) that you want to create. You can create an **IP-based** rule or a **MAC-based** rule. The rule type you select affects the rest of the configuration.
IP Type (IP-based)	If you are creating an IP-based rule, indicate the IP type, either **IPv4** or **IPv6**.
Source IP Address (IP-based)	Type the source IP address of the term. This parameter specifies the match conditions for packets that originate from the given IP address.
Destination IP Address (IP-based)	Type the destination IP address of the term. This parameter specifies the match conditions for packets that terminate at the given IP address.

Copyright © 2013, Juniper Networks, Inc.

Table 75: Term Fields for Wireless *(continued)*

Field	Description
Protocol (IP-based)	Select a protocol for the filter term. Select **Any** to include packets that use any supported protocols to be part of the rule or select **None** to discard protocol based filtering. Other options are **ICMP**, **TCP**, **UDP**, and **Other**. The protocol that you select here affects the rest of the settings in this window. If you selected **ICMP** as the protocol: a. Optionally, change the default protocol number for ICMP, which is 1. b. Indicate an ICMP Code number. ICMP code specifies more specific information than ICMP type. Because the value's meaning depends upon the associated ICMP type, you must specify an ICMP type along with an ICMP code. The keywords are grouped by the ICMP type with which they are associated. c. Indicate an ICMP Type number. ICMP Type specifies the ICMP packet type field. Typically, you specify this match condition in conjunction with the protocol match condition to determine which protocol is being used on the port. d. Indicate a DSCP number. DSCP filters packets by Differentiated Services Code Point (DSCP) value. You can specify a number from 0 to 63, in decimal or binary format. NOTE: You cannot use the DSCP option along with the Precedence and TOS options in the same term. e. Indicate a precedence for the term, either **Routine (0)**, **Priority (1)**, **Immediate (2)**, **Flash (3)**, **Flash Override (4)**, **Critical ECP (5)**, **Internet Control (6)**, **Net Control (7)** or **None** (default). f. Indicate a ToS number. The ToS number specifies the type of service (ToS) level to filter packets. Specify one of the following values, or any sum of these values up to 15: • **8**—minimum delay • **4**—maximum throughput • **2**—maximum reliability • **1**—minimum monetary cost • **0**—normal For example, a ToS value of 9 filters packets with the ToS levels minimum delay (8) and minimum monetary cost (1) NOTE: You cannot use the DSCP option along with the Precedence and ToS options in the same term. g. Click **OK**. The term is added to the filter.

Copyright © 2013, Juniper Networks, Inc.

Table 75: Term Fields for Wireless *(continued)*

Field	Description
	If you selected **TCP** or **UDP** as the protocol: a. Optionally, change the default protocol number for TCP (6) or UDP (17). b. Indicate a source port operator. Options are **None** (default), **Less than**, **Greater than**, **Equal**, or **Not equal**. For any option other than None, also indicate a source port name and a source port number. c. Indicate a destination port operator. Options are **None** (default), **Less than**, **Greater than**, **Equal**, or **Not equal**. For any option other than None, also indicate a source port name and a source port number. d. Indicate a DSCP number. DSCP filters packets by Differentiated Services Code Point (DSCP) value. You can specify a number from 0 to 63, in decimal or binary format. NOTE: You cannot use the DSCP option with the Precedence and TOS options in the same term. e. Indicate a precedence for the term, either **Routine (0)**, **Priority (1)**, **Immediate (2)**, **Flash (3)**, **Flash Override (4)**, **Critical ECP (5)**, **Internet Control (6)**, **Net Control (7)** or **None** (default). f. Indicate a ToS number. The ToS number specifies the type of service (TOS) level to filter packets. Specify one of the following values, or any sum of these values up to 15: • **8**—minimum delay • **4**—maximum throughput • **2**—maximum reliability • **1**—minimum monetary cost • **0**—normal For example, a TOS value of 9 filters packets with the TOS levels minimum delay (8) and minimum monetary cost (1) NOTE: You cannot use the DSCP option along with the Precedence and TOS options in the same term. g. Click **OK**. The term is added to the filter.

Copyright © 2013, Juniper Networks, Inc.

Table 75: Term Fields for Wireless *(continued)*

Field	Description
	If you selected **Any** as the protocol: a. Indicate a DSCP number. DSCP filters packets by Differentiated Services Code Point (DSCP) value. You can specify a number from 0 to 63, in decimal or binary format. NOTE: You cannot use the DSCP option along with the Precedence and TOS options in the same term. b. Indicate a precedence for the term, either **Routine (0)**, **Priority (1)**, **Immediate (2)**, **Flash (3)**, **Flash Override (4)**, **Critical ECP (5)**, **Internet Control (6)**, **Net Control (7)** or **None**. c. Indicate a ToS number. The ToS number specifies the type of service (TOS) level to filter packets. Specify one of the following values, or any sum of these values up to 15: • **8**—minimum delay • **4**—maximum throughput • **2**—maximum reliability • **1**—minimum monetary cost • **0**—normal For example, a TOS value of 9 filters packets with the TOS levels minimum delay (8) and minimum monetary cost (1) NOTE: You cannot use the DSCP option along with the Precedence and TOS options in the same term. d. Click **OK**. The term is added to the filter.
Source MAC Address (MAC-based)	Type the source MAC address of the term. This parameter specifies the match conditions for packets that originate from the given MAC address.
Destination MAC Address (MAC-based)	Type the destination MAC address of the term. This parameter specifies the match conditions for packets that terminate at the given MAC address.
EtherType (MAC-based)	Specify EtherType filtering for the term. EtherType indicates the protocol that is encapsulated in the payload of an Ethernet Frame. Select **Any** to include packets that use any EtherType to be part of the rule or **None** to discard EtherType-based filtering.
Action	Select the action that the system performs on an IP packet if the match conditions that you specified above are met. Possible actions are **Discard** and **Accept**. The default action is to discard the packet. NOTE: Forwarding Class is enabled only if you select **Accept** as the action.

Copyright © 2013, Juniper Networks, Inc.

Table 75: Term Fields for Wireless *(continued)*

Field	Description
Forwarding Class	Specifies the forwarding class (or output queue) that is to be used for the packet that matches the condition. You can create a new forwarding class or select from a list of available forwarding classes only if you specified the action as Accept. To create a new forwarding class, click **Create**. The Create Forwarding Class page appears. Specify a name for the forwarding class and the corresponding output queue number and click OK. The system creates a new forwarding class and displays it in the Forwarding Class field in the Create Term page. To select a forwarding class from an existing list of classes, click **Select**. The Select Forwarding Class page appears. Select the forwarding class that you want to use for the packet and click **OK**. The system displays the selected forwarding class in the Forwarding Class field in the Create Term page.

Click **OK** to save the wireless filter term and return to the Create Filter Profile page.

Specifying Settings for a Campus Switching ELS Switch Filter Profile

A Filter profile must have at least one term in it. Each term has one filtering function. For example, if a term is evaluating the source of packets, then that term cannot also evaluate the protocols used by the packets. Some switch models accommodate multiple terms in one filter. When you have more than one term in a filter, the ordering of the terms is important. The system evaluates multiple filter terms as follows:

- The packet is evaluated against the first term's conditions. If the packet matches all of the conditions in that term, the corresponding action for that condition is taken and evaluation ends. Subsequent terms in the filter are not evaluated.
- If the packet does not match all conditions in the first term, the packet is evaluated against the conditions in the second term. This process continues until either the packet matches all the conditions in one of the subsequent terms or there are no more terms in the filter. If a match is found, the action specified in the Action section of the matched term is taken and the evaluation ends. Subsequent terms in the filter are not evaluated.
- The term conditions for protocol, EtherType, DSCP, precedence, ICMP code and ICMP type must all be either match conditions or except conditions.
- If a packet passes through all the terms in the filter without a match, the packet is discarded.

To configure a Filter profile for Campus switching ELS:

1. Specify a filter name and description for the Filter profile.
2. Select the switch filter family for which you want to create the profile:
   - If you want to create a Layer 2 based filter, select **Ethernet switching**.
   - If you want to create a Layer 3 based filter for IPv4, select **INET**.
   - If you want to create a Layer 3 based filter for IPv6, select **INET6**.

Copyright © 2013, Juniper Networks, Inc.

3. Under Terms, click **Add** to add one or more terms with match condition(s) to the named filter. You need at least one term for this filter.

   The Create Term window opens.

NOTE: **The order of the terms within a Filter profile configuration is important. Packets are tested against each term in the order in which the terms are listed.**

4. Enter a name for the filter term.
5. Specify the match condition(s) for the filter term as described in Table 76 on page 251. Required settings are indicated by a red asterisk (*) that appears next to the field label in the user interface.

Table 76: Create Term Fields for Campus Switching ELS

Field	Description
Source and Destination Parameters	
	You can specify match conditions based on the packets' origin (source) or the packets' destination, or both. You are indicating the location of the filtering here—either specifying that packets that originate at a specific place (source) will be filtered or packets destined for a specific location (destination) will be filtered. You can have multiple sources and destinations for one filter.

Copyright © 2013, Juniper Networks, Inc.

Table 76: Create Term Fields for Campus Switching ELS *(continued)*

Field	Description
Source Parameters and Destination Parameters	To add source and destination parameters to the named filter term: a. Click **Add** to the right of the Destination Parameters lists. The Add Source/Destination Parameter window opens. b. Select either **Source** (default) or **Destination** from the Add Source/Destination Parameter window. c. Select one of following available Parameter Types from the Add Source/Destination Parameter page and provide the corresponding information: • **IP Address**—Provide the IP address of the source or destination device. • **MAC Address**—Provide a MAC address. • **Port**—Provide the port type of the source or destination port. Select either **AFS** (Andrew File System), **BGP** (Border Gateway Protocol), **BIFF** (UNIX mail notification), **Bootpc** (bootstrap protocol client), **Bootps**, **Cmd**, **CVS pserver**, **DHCP**, **Domain**, **EK login**, **EK shell**, **EXEC**, **Finger** protocol, **FTP**, **FTP data**, **HTTP**, **HTTPS**, **Ident** protocol, **IMAP** (Internet Message Access protocol), **Kerberos-sec** (Kerberos security), **Klogin** forwarding, **Kpasswd** command, **KRB-prop** (Kerberos database propagation), **Krbupdate** (Kerberos database update), **Kshell** (Kerberos rsh), **LDAP**, **Login** (UNIX rlogin), **Mobilip-agent** (Mobile IP agent), **Mobilip-mn** (Mobile IP MN), **MSDP** (Multicast Source Discovery Protocol),**NetBIOS dgm**, **NetBIOS-ns** (NetBIOS name service), **NetBIOS-ssn** (NetBIOS session service), **NFSD**, **NNTP** (Network News Transport Protocol), **Ntalk**, **NTP** (Network Time Protocol), **POP3** (Post Office Protocol3), **PPTP**, **Printer**, **RADacct** (RADIUS accounting), **RADIUS**, **RIP**, **RKINIT** (Kerberos remote kinit), **SMTP**, **SNMP trap**, **SNPP**, **SUNRPC**, **Syslog**, **TACACS**, **TACACS-ds**, **Talk** (UNIX Talk),**Telnet**, **TFTP**, **Timed** (UNIX time daemon), **Who** (UNIX rwho), **XDMCP** (X Display Manager Control Protocol), **Zephyr-clt** (Zephyr serv-hm connection), **Zephyr-hm** (Zephyr hostmanager), **Zephyr-srv** (Zephyr server), or **Other**. NOTE: If you selected Port as the parameter and do not find the type of port that you want to add from the Port list, then select **other** and enter a port number. d. To select any other source/destination than the one indicated, enable **Except**. TIP: You cannot indicate both matching and except for a parameter. e. Click **OK** The parameter term is added to the appropriate list, either Source Parameters or Destination Parameters.

Protocols and EtherTypes

Depending on the Filter Family you selected, you can sometimes apply a filter term based on either protocols being used by packets or on EtherTypes being used by packets. Recognized protocols are listed where applicable. Recognized EtherTypes, which indicate the protocol that is encapsulated in the payload of an Ethernet Frame, are also listed where applicable.

Copyright © 2013, Juniper Networks, Inc.

Table 76: Create Term Fields for Campus Switching ELS *(continued)*

Field	Description
Protocols (apply to Ethernet and INET filter families)	To add a protocol match condition to the named filter term: a. Expand the Protocols and EtherTypes section. b. Click **Add** under Protocols. The Select Protocols window opens with a list of protocols. c. From the list of protocols, select one or more. The options are **AH**, **DSTOPTS**, **EGP**, **ESP**, **Fragment**, **GRE**, **Hop-by-hop**, **ICMP**, **IPIP**, **IPv6**, **No-text-header**, **OSPF**, **PIM**, **Routing**, **RSVP**, **SCTP**, **TCP**, **UDP**, and **VRRP**. d. To make the filter exclude the specified protocol, select **Except**. NOTE: The term conditions for protocol, EtherType, DSCP, precedence, ICMP code and ICMP type must all be either match conditions or except conditions. e. Click **OK**. The protocols are added to the Protocols list.
EtherTypes (apply to Ethernet filter family)	To add an EtherTypes match condition to the named filter term: a. Expand the Protocols and EtherTypes section. b. Click **Add** under EtherTypes. The Select EtherTypes window opens with a list of protocols. c. From the list of EtherTypes, select one or more. The options are **AARP**, **AppleTalk**, **ARP**, **IPV4**, **MPLS multicast**, **MPLS unicast**, **OAM**, **PPP**, **PPPOE discovery**, **PPPOE session**, and **SNA**. d. To make the filter exclude the specified EtherType, select **Except**. NOTE: Term values must all be either match conditions or all except conditions. e. Click **OK**. The EtherTypes are added to the EtherTypes list.

DSCP Settings

Expand the DSCP section to see the DSCP match settings. DiffServ is a simple mechanism for classifying and managing network traffic and providing quality of service (QoS) on IP networks. DiffServ can, for example, be used to apply low-latency to critical network traffic such as voice or streaming media while providing simple best-effort service to non-critical services such as web traffic. Here, you can apply a filter term based on the Differentiated Services code point (DSCP) which is a field in IPv4 and IPv6 headers.

NOTE: With IPv6 packets, the DS field and ECN field replace the IPv4 TOS field.

Copyright © 2013, Juniper Networks, Inc.

Table 76: Create Term Fields for Campus Switching ELS *(continued)*

Field	Description
DSCP (Ethernet and INET filter families)	To add a DSCP match condition to the named filter term: NOTE: A DSCP IP match condition and a precedence match condition cannot be both specified for the same term. a. Click **Add** in the DSCP section. The Select DSCP Match Condition list appears. b. Select one of the following DSCP types from the list: • **AF11**—Assured forwarding class 1, low drop precedence • **AF12**—Assured forwarding class 1, medium drop precedence • **AF21**—Assured forwarding class 2, low drop precedence • **AF22**—Assured forwarding class 2, medium drop precedence • **AF23**—Assured forwarding class 2, high drop precedence • **AF31**—Assured forwarding class 3, low drop precedence • **AF32**—Assured forwarding class 3, medium drop precedence • **AF33**—Assured forwarding class 3, high drop precedence • **AF41**—Assured forwarding class 4, low drop precedence • **AF42**—Assured forwarding class 4, medium drop precedence • **AF43**—Assured forwarding class 4, high drop precedence • **BE**—Best effort (default) • **EF**-Expedited forwarding • **CS0**—Class selector 0 • **CS1**—Class selector 1 • **CS2**—Class selector 2 • **CS3**—Class selector 3 • **CS4**—Class selector 4 • **CS5**—Class selector 5 • **CS6**—Class selector 6 • **CS7**—Class selector 7 c. To make the filter exclude a specified DSCP type, select **Except**. NOTE: Term values must all be either match conditions or all of them need to be except conditions. d. Click **OK**. The DSCP code term for the named filter is added to the DSCP list.

Copyright © 2013, Juniper Networks, Inc.

Table 76: Create Term Fields for Campus Switching ELS *(continued)*

Field	Description
Precedence for DSCP (Ethernet and INET filter families)	You can apply an IP precedence match condition to the named term. With IP precedence, a device prioritizes traffic by class first. Then it differentiates and prioritizes same-class traffic. NOTE: The match conditions IP Precedence and DSCP cannot be simultaneously applied to a term. To apply an IP precedence value match condition to the named term: a. Click **Add** in the Precedence section. The Select Precedence list appears. b. Select one of the following precedence settings from the list: **Routine** (0 or lowest, also called Best Effort), **Priority** (1), **Immediate** (2), **Flash** (3, mainly used for voice signaling or for video), **Flash-override** (4), **Critical-ECP** (5, mainly used for voice RTP), **Internet-control** (6, used for IP routing protocols), or **Net-control** (7 or highest, used for link layer and routing protocol keep alive). c. To make the filter exclude the specified IP precedence value, select **Except**. NOTE: Term values must all be either match conditions or all of them need to be except conditions. d. Click **OK**. The precedence match condition is added to the named term, and the condition is listed in the Precedence list.
TCP Settings Expand this section to access the TCP settings. The Transmission Control Protocol (TCP) is the most common core protocol of the Internet protocol suite (IP). TCP provides reliable, ordered, error-checked delivery of a stream of octets between programs running on computers connected to the Internet or an intranet. You can use the TCP initial flag for a match condition.	
Enable TCP Initial (all families)	Select to use the TCP initial flag for an Ethernet, INET, or INET6 match condition. TIP: If you use the TCP initial flag for filtering, you cannot use any other TCP flag.
TCP Flags	If you are not using the TCP initial flag for a match condition, you can select one of the TCP flags from the list for a match condition—**RST**, **ACK**, **SYN**, **Urgent**, **Push**, **FIN**, or **None**. These flags have the following meaning: • RST—Reset flag indicates that the TCP connection will be reset. • ACK—Third step in TCP three-way handshake for connection. In response to a server's SYN-ACK, the client replies with an ACK. • SYN—First step in TCP three-way handshake for connection. The active open is performed by the client sending a SYN to the server. • Urgent—If the URG flag is set, then the 16-bit field is an offset from the sequence number indicating the last urgent data byte. • Push—Push flags request that buffered data to the receiving application be sent now. • FIN—The final flag indicates that no more data will be sent.

Copyright © 2013, Juniper Networks, Inc.

Table 76: Create Term Fields for Campus Switching ELS *(continued)*

Field	Description
ICMP Settings You can select the ICMP code value for the filter item's match condition—expand this section to access the ICMP settings. The Internet Control Message Protocol (ICMP) is one of the core IP protocols used by operating systems of networked computers to send error messages. ICMP can also be used to relay query messages.	
ICMP Code	To apply an ICMP code match condition to the named term: a. Click **Add** in the ICMP Code section. The Select ICMP Code window appears. b. Select one or more ICMP codes from the list. These codes vary, depending on the Filter Family you selected. c. To make the filter exclude the specified ICMP code, select **Except**. NOTE: Term values must all be either match conditions or all of them need to be except conditions. d. Click **OK**. The ICMP code match condition is added to the named term, and the condition is listed in the ICMP Code list. You can now enable **Except**. NOTE: An ICMP code specifies more specific information than an ICMP type. Because the value's meaning depends upon the associated ICMP type, you must specify and ICMP type along with ICMP code. The keywords are grouped by the ICMP type with which they are associated.
ICMP Type	NOTE: ICMP type specifies the ICMP packet type field. Typically, you specify this match condition in conjunction with the protocol match condition to determine which protocol is being used on the port. ICMP code specifies more specific information than ICMP type. Because the value's meaning depends upon the associated ICMP type, you must specify ICMP type along with ICMP code. The keywords are grouped by the ICMP type with which they are associated. To apply an ICMP type match condition to the named term: a. Click **Add** in the ICMP Type section. The Select ICMP Types window appears. b. Select one or more ICMP types from the list. These types vary, depending on the Filter Family selected. c. To make the filter exclude the specified ICMP type, select **Except**. NOTE: Term values must all be either match conditions or all of them need to be except conditions. d. Click **OK**. The ICMP type match condition is added to the named term, and the condition is listed in the ICMP Type list. You can now enable **Except**.

Copyright © 2013, Juniper Networks, Inc.

Table 76: Create Term Fields for Campus Switching ELS *(continued)*

Field	Description
Action Select the action that the system performs on an IP packet if all match conditions that you specified above are met. Possible actions are Discard and Accept. The default action is to discard packet that matches the filter term conditions.	
Action	Select either **Discard** or **Accept** to indicate what the filter term does with a packet when a match is made. NOTE: All other fields in this section are enabled only if you select **Accept** as the action.
Counter Name	When the action selected is accept, specify the maximum packet count for this filter, term, or policer.
Loss Priority	When the action selected is accept, specify the packet loss priority, **Low**, **High**, **Medium-low**, **Medium-high**, or **None**. NOTE: Forwarding class and loss priority must be specified together for the same term.

Copyright © 2013, Juniper Networks, Inc.

Table 76: Create Term Fields for Campus Switching ELS *(continued)*

Field	Description
Policer	When you create a Filter profile with the action accept, you can specify a policer action for any term or terms within the filter. Policing, or rate limiting, enables you to limit the amount of traffic that passes into or out of an interface. All traffic that matches a term that contains a policer action goes through the policer that the term references. You have two options with a policer. You can specify that an existing policer be used for the packet that matches the match condition. Or, you can create a new policer for the packet that matches the match condition. To select an existing policer: a. Click **Select**. The Select Policer page appears. b. Click **OK**. The policer is added to the list of applied policers.

Copyright © 2013, Juniper Networks, Inc.

Table 76: Create Term Fields for Campus Switching ELS *(continued)*

Field	Description
	To create a new policer: a. Click **Create**. The Create Policer page appears. b. Type a name for the policer—you can use this policer again in the future. c. Select a policer type from the list, either a **single-rate-two-color** policer, or a **three-color-policer**. The type of policer that you select here affects the rest of the configurations available for the policer. If you selected a three-color-policer, then also select a rate for it, either **single-rate** or **two-rate**. • Single-rate two-color—A two-color policer (sometimes called simply *policer*) meters the traffic stream and classifies packets into two categories of packet loss priority (PLP) according to a configured bandwidth and burst-size limit. You can mark packets that exceed the bandwidth and burst-size limit or simply discard them. A two-color policer is most useful for metering traffic at the port (physical interface) level. • Single-Rate Three-color—This type of policer is defined in RFC 2697, A Single Rate Three Color Marker, as part of an assured forwarding (AF) per-hop-behavior (PHB) classification system for a Differentiated Services (DiffServ) environment. This type of policer meters traffic based on the configured committed information rate (CIR), committed burst size (CBS), and the excess burst size (EBS). Traffic is marked as belonging to one of three categories (green, yellow, or red) based on whether the packets are arriving at rates that are below the CBS (green), exceed the CBS but not the EBS (yellow), or exceed the EBS (red). A single-rate three-color policer is most useful when a service is structured according to packet size and not according to peak arrival rate. • Two-rate three-color—This type of policer is defined in RFC 2698, A Two Rate Three Color Marker, as part of an assured forwarding (AF) per-hop-behavior (PHB) classification system for a Differentiated Services (DiffServ) environment. This type of policer meters traffic based on the configured CIR and the peak information rate (PIR), along with their associated burst sizes; the CBS, and the peak burst size (PBS). Traffic is marked as belonging to one of three categories (green, yellow, or red) based on packets are arriving at rates that are below the CIR (green), exceed the CIR but not the PIR (yellow), or exceed the PIR (red). A two-rate three-color policer is most useful when a service is structured according to arrival rates and not to packet size. NOTE: The system displays and hides various fields in the Create Policer page depending on the type of policer that you want to create. d. Configure these fields for a single-rate-two-color policer: • Bandwidth Limit—Specify the traffic rate in bits per second, 1000 through 102,300,000,000 (102.3g) bps. • Burst Size Limit—Specify the maximum number of bytes allowed for incoming packets to burst above the peak information rate (PIR) and still be marked with medium-high packet loss priority (yellow). Packets that exceed the peak burst size (PBS) are marked with high packet loss priority (red). The range is 1500 through 100,000,000,000 bytes. • Action—Select either **Discard** or **None**.

Copyright © 2013, Juniper Networks, Inc.

Table 76: Create Term Fields for Campus Switching ELS *(continued)*

Field	Description
	• Loss Priority—Select either **High** or **None**. e. Configure these fields for a single-rate-three-color policer: • Committed Information Rate—Specify the guaranteed bandwidth (in bits per second) under normal line conditions and the average rate up to which packets are marked with low packet loss priority (green). The range is 32,000 through 40,000,000,000 bps. • Committed Burst Size—Specify the maximum number of bytes allowed for incoming packets to burst above the committed information rate (CIR) and still be marked with low packet loss priority (green). The range is 1500 through 100,000,000,000 bytes. • Excess Burst Size—Specify the maximum number of bytes allowed for incoming packets to burst above the committed information rate and still be marked with medium-high packet loss priority (yellow). Packets that exceed the excess burst size (EBS) are marked with high packet loss priority (red). The range is 1500 through 100,000,000,000 bytes. • Color Mode—Select the way the preclassified packets are to be metered: ◦ **Color-aware**—The local switch can assign a higher packet loss priority but cannot assign a lower packet loss priority. ◦ **Color-blind**—The local switch ignores the preclassification of packets and can assign a higher or lower packet loss priority. ◦ **None**—The preclassified packets are not metered. • Action—Options are **Discard** and **None**. • Loss Priority—Options are **High** and **None**.

Copyright © 2013, Juniper Networks, Inc.

Table 76: Create Term Fields for Campus Switching ELS *(continued)*

Field	Description
	f. Configure these fields for a three-color two-rate policer: • Committed Information Rate—Specify the guaranteed bandwidth (in bits per second) under normal line conditions and the average rate up to which packets are marked with low packet loss priority (green). The range is 32,000 through 40,000,000,000 bps. • Committed Burst Size—Specify the maximum number of bytes allowed for incoming packets to burst above the committed information rate (CIR) and still be marked with low packet loss priority (green). The range is 1500 through 100,000,000,000 bytes. • Peak Burst Size—Specify the maximum number of bytes allowed for incoming packets to burst above the peak information rate (PIR) and still be marked with medium-high packet loss priority (yellow). Packets that exceed the peak burst size (PBS) are marked with high packet loss priority (red). The range is 1500 through 100,000,000,000 bytes. • Peak Information Rate—Specify the maximum achievable rate in bits per second. Packets that exceed the peak information rate (PIR) are marked with high packet loss priority (red). You can configure a discard action for packets that exceed the PIR. The range is 32,000 through 40,000,000,000 bps. • Color Mode—Select the way the preclassified packets are to be metered: ◦ **Color-aware**—The local switch can assign a higher packet loss priority but cannot assign a lower packet loss priority. ◦ **Color-blind**—The local switch ignores the preclassification of packets and can assign a higher or lower packet loss priority. ◦ **None**—The preclassified packets are not metered. • Action—Options are **Discard** and **None**. • Loss Priority—Options are **High** and **None**. g. Click **OK**. The policer is added to the list of applied policers and the list of available policers.

Copyright © 2013, Juniper Networks, Inc.

Table 76: Create Term Fields for Campus Switching ELS *(continued)*

Field	Description
Forwarding Class	Specify the forwarding class (or output queue) that is to be used for the packet that matches the match condition. You can either select from a list of available forwarding classes or create a new forwarding class. To select a forwarding class from an existing list of classes, click **Select**. The Select Forwarding Class page appears. Select the forwarding class that you want to use for the packet and click **OK**. The system displays the selected forwarding class in the Forwarding Class field in the Create Term page. To create a new forwarding class: a. Click **Create**. The Create Forwarding Class page appears. b. Type a name for the forwarding class—you can use this forwarding class again in the future. c. Select a queue number from the list, and then click **OK**. The system creates a new forwarding class and displays it in the Forwarding Class field in the Create Term page.

6. Click **OK** to save the term and return to the Create Filter Profile page.
7. Click **Done**.

   The new filter is added to the Mnage Filter Profile list.

Specifying Settings for Creating a Data Center Switching Filter Profile

A Filter profile must have at least one term in it. Each term has one filtering function. For example, if a term is evaluating the source of packets, then that term cannot also evaluate the protocols used by the packets. Some switch models accommodate multiple terms in one filter. When you have more than one term in a filter, the ordering of the terms is important. The system evaluates multiple filter terms as follows:

- The packet is evaluated against the first term's conditions. If the packet matches all of the conditions in that term, the action specified for that condition is taken and evaluation ends. Subsequent terms in the filter are not evaluated.
- If the packet does not match all conditions in the first term, the packet is evaluated against the conditions in the second term. This process continues until either the packet matches all the conditions in one of the subsequent terms or there are no more terms in the filter. If a match is found, the action specified in the Action section of the matched term is taken and the evaluation ends. Subsequent terms in the filter are not evaluated.
- Term values (protocol, EtherType, DSCP, precedence, ICMP code and ICMP type) must all be either match conditions or all of them need to be except conditions.
- If a packet passes through all the terms in the filter without a match, the packet is discarded.

Copyright © 2013, Juniper Networks, Inc.

To configure a Filter profile:

1. Specify a filter name and description for the Filter profile.
2. Select the switch filter family for which you want to create the profile:
   - If you want to create a Layer 2 based filter, select **Ethernet switching**.
   - If you want to create a Layer 3 based filter for IPv4, select **INET**.
   - If you want to create a Layer 3 based filter for IPv6, select **INET6**.
3. Under Terms, click **Add** to add one or more terms with match condition(s) to the named filter.

   The Create Term window opens.

NOTE: **The order of the terms within a Filter profile configuration is important. Packets are tested against each term in the order in which the terms are listed.**

4. Enter a name for the filter term.
5. Specify the match condition(s) for the filter term as described in Table 77 on page 263. Required settings are indicated by a red asterisk (*) that appears next to the field label in the user interface.

Table 77: Create Term Fields for Data Center

Field	Description
Source and Destination Parameters	
You can specify match conditions for either the packets' origin (source) or the packets' destination, or both. You are indicating the location of the filtering here—either specifying that packets that originate at a specific place (source) will be filtered or packets destined for a specific location (destination) will be filtered. You can have multiple sources and destinations for one filter.	

Copyright © 2013, Juniper Networks, Inc.

Table 77: Create Term Fields for Data Center *(continued)*

Field	Description
Source Parameters and Destination Parameters	To add source and destination parameters to the named filter term: a. Click **Add** to the right of the Destination Parameters lists. The Add Source/Destination Parameter page appears. b. Select either **Source** (default) or **Destination** from the Add Source/Destination Parameter page. c. Select one of following available Parameter Types from the Add Source/Destination Parameter page and provide the corresponding information: • **IP Address**—Provide the IP address of the source or destination device • MAC Address—MAC address of the source or destination device • **Port**—Port type of the source or destination port. Select either **AFS** (Andrew File System), **BGP** (Border Gateway Protocol), **BIFF** (UNIX mail notification), **Bootpc** (bootstrap protocol client), **Bootps**, **Cmd**, **CVS pserver**, **DHCP**, **Domain**, **EK login**, **EK shell**, **EXEC**, **Finger** (protocol), or **FTP**. NOTE: If you selected Port as the parameter and do not find the type of port that you want to add from the Port list, then select **other** and enter a port number. d. Click **OK** The parameter term is added to the appropriate list, either Source Parameters or Destination Parameters.
Protocols and EtherTypes You can apply a filter term that is based on either the protocols being used by packets or on the EtherTypes being used by packets. Protocols such as AH, DSTOPTS, EGP, ESP, FRAGMENT, GRE, HOP-BY-HOP, ICMP, ICMP6, IPIP, IPv6, no-text-header, OSPF, PIM, ROUTING, RSVP, SCTP, TCP, UDP, and VRRP are recognized. EtherType indicates the protocol that is encapsulated in the payload of an Ethernet Frame.	
Protocols	To add a protocol match condition to the named filter term: a. Expand the Protocols and EtherTypes section. b. Click **Add** under Protocols. The Select Protocols window opens, displaying a list of protocols. c. From the list of protocols, select one or more. The options are **AH**, **DSTOPTS**, **EGP**, **ESP**, **fragment**, **GRE**, **Hop-by-hop**, **ICMP**, **IPIP**, **IPv6**, **No-text-header**, **OSPF**, **PIM**, **routing**, **RSVP**, **SCTP**, **TCP**, **UDP**, and **VRRP**. d. Click **OK**. The protocols are added to the Protocols list.

Copyright © 2013, Juniper Networks, Inc.

Table 77: Create Term Fields for Data Center *(continued)*

Field	Description
EtherTypes	To add an EtherTypes match condition to the named filter term: a. Expand the Protocols and EtherTypes section. b. Click **Add** under EtherTypes. The Select EtherTypes window opens, displaying a list of protocols. c. From the list of EtherTypes, select one or more. The options are **AARP**, **AppleTalk**, **ARP**, **IPV4**, **FCOE**, **FIP**, **MPLS multicast**, **MPLS unicast**, **OAM**, **PPP**, **PPPOE discovery**, **PPPOE session**, **SNA**, and **VLAN**. d. Click **OK**. The protocols are added to the Protocols list.

DSCP Settings

DiffServ is a simple mechanism for classifying and managing network traffic and providing quality of service (QoS) on IP networks. DiffServ can, for example, be used to apply low-latency to critical network traffic such as voice or streaming media while providing simple best-effort service to non-critical services such as web traffic. Here, you can apply a filter term based on the Differentiated Services code point (DSCP) which is a field in IPv4 and IPv6 headers.

NOTE: With IPv6 packets, the DS field and ECN field replace the IPv4 TOS field.

Copyright © 2013, Juniper Networks, Inc.

Table 77: Create Term Fields for Data Center *(continued)*

Field	Description
DSCP	To add a DSCP match condition to the named filter term: NOTE: A DSCP IP match condition and a precedence match condition cannot be both specified for the same term. a. Expand the DSCP Settings section. b. Click **Add** in the DSCP section. The Select DSCP Match Condition list appears. c. Select one of the following DSCP types from the list: • **AF11**—Assured forwarding class 1, low drop precedence • **AF12**—Assured forwarding class 1, medium drop precedence • **AF21**—Assured forwarding class 2, low drop precedence • **AF22**—Assured forwarding class 2, medium drop precedence • **AF23**—Assured forwarding class 2, high drop precedence • **AF31**—Assured forwarding class 3, low drop precedence • **AF32**—Assured forwarding class 3, medium drop precedence • **AF33**—Assured forwarding class 3, high drop precedence • **AF41**—Assured forwarding class 4, low drop precedence • **AF42**—Assured forwarding class 4, medium drop precedence • **AF43**—Assured forwarding class 4, high drop precedence • **BE**—Best effort (default) • **EF**-Expedited forwarding • **CS0**—Class selector 0 • **CS1**—Class selector 1 • **CS2**—Class selector 2 • **CS3**—Class selector 3 • **CS4**—Class selector 4 • **CS5**—Class selector 5 • **CS6**—Class selector 6 • **CS7**—Class selector 7 d. Click **OK**. The DSCP code term for the named filter is added to the DSCP list.

Copyright © 2013, Juniper Networks, Inc.

Table 77: Create Term Fields for Data Center *(continued)*

Field	Description
Precedence	You can apply an IP precedence match condition to the named term. With IP precedence, a device prioritizes traffic by class first. Then it differentiates and prioritizes same-class traffic. NOTE: The match conditions IP Precedence and DSCP cannot be simultaneously applied to a term. To apply an IP precedence value match condition to the named term: a. Expand the DSCP Settings section. b. Click **Add** in the Precedence section. The Select Precedence list appears. c. Select one of the following precedence settings from the list: **Routine** (0 or lowest, also called Best Effort), **Priority** (1), **Immediate** (2), **Flash** (3, mainly used for voice signaling or for video), **Flash-override** (4), **Critical-ECP** (5, mainly used for voice RTP), **Internet-control** (6, used for IP routing protocols), or **Net-control** (7 or highest, used for link layer and routing protocol keep alive). d. Click **OK**. The precedence match condition is added to the named term, and the condition is listed in the Precedence list.
TCP Settings The Transmission Control Protocol (TCP) is the most common core protocol of the Internet protocol suite (IP). TCP provides reliable, ordered, error-checked delivery of a stream of octets between programs running on computers connected to the Internet or an intranet. You can use the TCP initial flag for a match condition.	
Enable TCP Initial	Select to use the TCP initial flag for a match condition.
TCP Flags	If you are not using the TCP initial flag for a match condition, select one of the TCP flags from the list—**RST**, **ACK**, **SYN**, **Urgent**, **Push**, **Fin**, **None**. These flags have the following meaning: • RST—Reset flag indicates that the TCP connection will be reset. • ACK—Third step in TCP three-way handshake for connection. In response to a server's SYN-ACK, the client replies with an ACK. • SYN—First step in TCP three-way handshake for connection. The active open is performed by the client sending a SYN to the server. • Urgent—If the URG flag is set, then the 16-bit field is an offset from the sequence number indicating the last urgent data byte. • Push—Push flags request that buffered data to the receiving application be sent now. • FIN—The final flag indicates that no more data will be sent.
ICMP Settings You can select the ICMP code value for the filter item's match condition. The Internet Control Message Protocol (ICMP) is one of the core IP protocols used by operating systems of networked computers to send error messages. ICMP can also be used to relay query messages.	

Copyright © 2013, Juniper Networks, Inc.

Table 77: Create Term Fields for Data Center *(continued)*

Field	Description
ICMP Code	To apply an ICMP code match condition to the named term: a. Expand the ICMP Settings section. b. Click **Add** in the ICMP Codes section. The Select ICMP Codes list appears. c. Select one or more ICMP codes from the list. These codes vary, depending on the Filter Family you selected. d. Click **OK**. The ICMP code match condition is added to the named term, and the condition is listed in the ICMP Code list. NOTE: ICMP code specifies more specific information than ICMP type. Because the value's meaning depends upon the associated ICMP type, you must specify ICMP type along with ICMP code. The keywords are grouped by the ICMP type with which they are associated.
ICMP Type	NOTE: ICMP type specifies the ICMP packet type field. Typically, you specify this match condition in conjunction with the protocol match condition to determine which protocol is being used on the port. ICMP code specifies more specific information than ICMP type. Because the value's meaning depends upon the associated ICMP type, you must specify an ICMP type along with the ICMP code. The keywords are grouped by the ICMP type with which they are associated. To apply an ICMP type match condition to the named term: a. Expand the ICMP Settings section. b. Click **Add** in the ICMP Type section. The Select ICMP Types list appears. c. Select one or more ICMP types from the list: **echo-reply**, **echo-request**, **info-reply**, **info-request**, **mask-reply**, **mask-request**, **parameter-problem**, **redirect**, **router-advertisement**, **router-solicit**, **source-quench**, **time-exceeded**, **timestamp**, **timestamp-reply**, or **unreachable**. d. Click **OK**. The ICMP type match condition is added to the named term, and the condition is listed in the ICMP Type list.
Qfabric Settings These settings apply only when the profile is applied to a QFabric device.	
Enable-from-fabric	Select to create a match condition that matches packets coming from the fabric.
Enable-to-fabric	Select to create a match condition that matches packets going to the fabric.

Copyright © 2013, Juniper Networks, Inc.

Table 77: Create Term Fields for Data Center *(continued)*

Field	Description
except	Select to create a match condition that matches all packets that are not going to the fabric.
Action Select the action that the system performs on an IP packet if all match conditions that you specified above are met. Possible actions are Discard and Accept. The default action is to discard packet that match the filter term's conditions.	
Action	Select either **Discard** or **Accept** to indicate what the filter term does with a packet when a match is made. NOTE: All other fields in this section are enabled only if you select **Accept** as the action.
Counter Name	Specify the maximum packet count for this filter, term, or policer.
Loss Priority	Specify the packet loss priority, **low**, **high**, or **none**. NOTE: Forwarding class and loss priority must be specified together for the same term.

Copyright © 2013, Juniper Networks, Inc.

Table 77: Create Term Fields for Data Center *(continued)*

Field	Description
Policer	

Copyright © 2013, Juniper Networks, Inc.

Table 77: Create Term Fields for Data Center *(continued)*

Field	Description
	When you create a Filter profile, you can specify a policer action for any term or terms within the filter. Policing, or rate limiting, enables you to limit the amount of traffic that passes into or out of an interface. All traffic that matches a term that contains a policer action goes through the policer that the term references. You have two options with a policer. You can specify that an existing policer be used for the packet that matches the match condition. Or, you can create a new policer for the packet that matches the match condition. To select a policer from an existing list of policers, click **Select**. The Select Policer page appears. Select the policer that you want to use for the term and click **OK**. The system displays the selected policer in the Policer field in the Create Term page. To create a new policer: a. Click **Create**. The Create Policer page appears. b. Type a name for the policer—you can use this policer again in the future. c. Select a policer type from the list, either a **single-rate-two-color** policer, a **single-rate-three-color** policer, or a **three-color-policer**. and then click **OK**. The type of policer that you select here affects the rest of the configurations available for the policer. You can create the following three type of policers: • Single-rate two-color—A two-color policer (sometimes called simply *policer*) meters the traffic stream and classifies packets into two categories of packet loss priority (PLP) according to a configured bandwidth and burst-size limit. You can mark packets that exceed the bandwidth and burst-size limit or simply discard them. A two-color policer is most useful for metering traffic at the port (physical interface) level. • Single-rate three-color—This type of policer is defined in RFC 2697, A Single Rate Three Color Marker, as part of an assured forwarding (AF) per-hop-behavior (PHB) classification system for a Differentiated Services (DiffServ) environment. This type of policer meters traffic based on the configured committed information rate (CIR), committed burst size (CBS), and the excess burst size (EBS). Traffic is marked as belonging to one of three categories (green, yellow, or red) based on whether the packets are arriving at rates that are below the CBS (green), exceed the CBS but not the EBS (yellow), or exceed the EBS (red). A single-rate three-color policer is most useful when a service is structured according to packet size and not according to peak arrival rate. • Two-rate three-color—This type of policer is defined in RFC 2698, A Two Rate Three Color Marker, as part of an assured forwarding (AF) per-hop-behavior (PHB) classification system for a Differentiated Services (DiffServ) environment. This type of policer meters traffic based on the configured CIR and the peak information rate (PIR), along with their associated burst sizes; the CBS, and the peak burst size (PBS). Traffic is marked as belonging to one of three categories (green, yellow, or red) based on packets are arriving at rates that are below the CIR (green), exceed the CIR but not the PIR (yellow), or exceed the PIR (red). A two-rate three-color policer is most useful when a service is structured according to arrival rates and not to packet size.

Copyright © 2013, Juniper Networks, Inc.

Table 77: Create Term Fields for Data Center *(continued)*

Field	Description
	NOTE: The system displays and hides various fields in the Create Policer page depending on the type of policer that you want to create. d. Configure the appropriate fields for the policer: • Bandwidth Limit—Specify the traffic rate in bits per second, 1000 through 102,300,000,000 (102.3g) bps. • Burst Size Limit—Specify the maximum number of bytes allowed for incoming packets to burst above the peak information rate (PIR) and still be marked with medium-high packet loss priority (yellow). Packets that exceed the peak burst size (PBS) are marked with high packet loss priority (red). The range is 1500 through 100,000,000,000 bytes. • Committed Information Rate—Specify the guaranteed bandwidth (in bits per second) under normal line conditions and the average rate up to which packets are marked with low packet loss priority (green). The range is 32,000 through 40,000,000,000 bps. • Committed Burst Size—Specify the maximum number of bytes allowed for incoming packets to burst above the committed information rate (CIR) and still be marked with low packet loss priority (green). The range is 1500 through 100,000,000,000 bytes. • Peak Burst Size—Specify the maximum number of bytes allowed for incoming packets to burst above the peak information rate (PIR) and still be marked with medium-high packet loss priority (yellow). Packets that exceed the peak burst size (PBS) are marked with high packet loss priority (red). The range is 1500 through 100,000,000,000 bytes. • Excess Burst Size—Specify the maximum number of bytes allowed for incoming packets to burst above the committed information rate and still be marked with medium-high packet loss priority (yellow). Packets that exceed the excess burst size (EBS) are marked with high packet loss priority (red). The range is 1500 through 100,000,000,000 bytes. • Peak Information Rate—Specify the maximum achievable rate in bits per second. Packets that exceed the peak information rate (PIR) are marked with high packet loss priority (red). You can configure a discard action for packets that exceed the PIR. The range is 32,000 through 40,000,000,000 bps • Color Mode—Select the way the preclassified packets are to be metered: ◦ **Color-aware**—The local switch can assign a higher packet loss priority but cannot assign a lower packet loss priority. ◦ **Color-blind**—The local switch ignores the preclassification of packets and can assign a higher or lower packet loss priority. ◦ **None**—The preclassified packets are not metered. e. Click **OK**. The policer is added to the list of applied policers and the list of available policers.

Copyright © 2013, Juniper Networks, Inc.

Table 77: Create Term Fields for Data Center *(continued)*

Field	Description
Forwarding Class	Specify the forwarding class (or output queue) that is to be used for the packet that matches the match condition. You can create a new forwarding class or select from a list of available forwarding classes. To select a forwarding class from an existing list of classes, click **Select**. The Select Forwarding Class page appears. Select the forwarding class that you want to use for the packet and click **OK**. The system displays the selected forwarding class in the Forwarding Class field in the Create Term page. To create a new forwarding class: a. Click **Create**. The Create Forwarding Class page appears. b. Type a name for the forwarding class—you can use this forwarding class again in the future. c. Select a queue number from the list, and then click **OK**. The system creates a new forwarding class and displays it in the Forwarding Class field in the Create Term page.

Click **OK** to save the term and return to the Create Filter Profile page.

What To Do Next

After you create a Filter profile, you can do one of the following:

- For wireless devices, link the Filter profile as ingress and egress filters to an Authorization profile. For more details, see "Creating and Managing Wireless Authorization Profiles" on page 167.
- For switching devices, link the Filter profile as ingress and egress filters to a Port profile. For more details, see "Creating and Managing Port Profiles" on page 283.
- For switching and wireless devices, link the Filter profile as ingress and egress filters to a VLAN profile. For more details, see "Creating and Managing VLAN Profiles" on page 330. You can then assign the VLAN profile to a device or port in case of switching devices and to a device, port, or access point in case of a wireless network.

Related Documentation

- Understanding Filter Profiles on page 32

Creating and Managing LDAP Profiles

Lightweight Directory Access Protocol (LDAP) is an Internet protocol that email and other programs use to look up information from a server. Use LDAP to look up encryption certificates, pointers to printers and other services on a network, in addition to providing a single logon where one user password is used for different services. LDAP authentication is appropriate for any kind of directory-like information where fast lookups and infrequent

Copyright © 2013, Juniper Networks, Inc.

updates are used. From Network Director, you can create and manage LDAP profiles for both wireless and EX Switching ELS.

TIP: In addition to an LDAP server, you can configure a RADIUS server for both authentication and accounting purposes—for directions, see "Creating and Managing RADIUS Profiles" on page 326.

This topic describes:

- Managing LDAP Profiles on page 274
- Creating LDAP Profiles on page 275
- Specifying Settings for an LDAP Profile on page 275
- What to Do Next on page 277

Managing LDAP Profiles

From the Manage LDAP Profiles page, you can:

- Create a new LDAP profile by clicking **Add**. For directions to add an LDAP profile, see "Creating LDAP Profiles" on page 275.
- Modify an existing LDAP profile by selecting it and clicking **Edit**.
- View information about a profile by selecting the group and clicking **Details** or by clicking the profile name.
- Delete LDAP profiles by selecting the profile and clicking **Delete**.

TIP: You cannot delete profiles that are in use—that is, assigned to objects or used by other profiles. To see the current assignments for a profile, select the profile and click **Details**.

- Clone an LDAP profile by selecting a profile and clicking **Clone**.

Table 78 on page 274 describes the information provided about LDAP profiles on the Manage LDAP Profiles page. This page lists all LDAP profiles defined for your network, regardless of your current selected scope in the network view.

Table 78: LDAP Profile Information

Field	Description
LDAP Name	Name given to the LDAP server profile when it was created.
Server Address	IP address of the LDAP server.
Server Port	UDP port being used by the LDAP server.
Domain Name	Domain using the LDAP server.

Copyright © 2013, Juniper Networks, Inc.

Table 78: LDAP Profile Information *(continued)*

Field	Description
Creation Time	Date and time when this profile was created.
Update Time	Date and time when this profile was last modified.
User Name	The username of the user who created or modified the profile.

TIP: All columns of information may not be displayed. To show or hide fields in the table, click the down arrow on the field header, select **Columns**, and select or clear the check box adjacent to the field that you want to show or hide.

Creating LDAP Profiles

To create an LDAP profile:

1. Click Build in the Network Director banner.
2. Under Select View, select either **Logical View**, **Location View**, **Device View** or **Custom Group** View.

   TIP: **Do not select Virtual View or Topology View.**

3. Click **LDAP** under Profile and Configuration Management in the Tasks pane.

   The Manage LDAP Profiles page appears.

4. Click **Add**.

   The Create LDAP Profile wizard appears.

5. Enter settings for the LDAP profile as described in "Specifying Settings for an LDAP Profile" on page 275.
6. Click **Done**.

Specifying Settings for an LDAP Profile

Use the Create LDAP Profile page to define LDAP directory information services over an IP network.

Table 79 on page 276 describes the LDAP settings.

Copyright © 2013, Juniper Networks, Inc.

Table 79: LDAP Profile Settings

Field	Action
Server Name	Type a name for the server, using up to 64 alphanumeric characters and no special characters other than an underscore. The name must be unique among servers.
Server Address	Type the IP address of the LDAP server.
Server Port (default is 389)	Using the arrows, adjust the number of the UDP port to use for LDAP authentication messages. The default port is 389 for unencrypted LDAP servers and 636 for unencrypted LDAP servers.
Advanced LDAP Settings	
Fully Qualified Domain Name	Type a fully qualified domain name (FQDN)—this is the complete domain name for a specific computer, or host, on the Internet. The FQDN consists of two parts: the host name and the domain name. For example, an FQDN for a server might be ldap12.juniper.net. The host name is ldap12, and the host is located within the domain juniper.net. This domain name specifies all domain levels, including the top-level domain and the root zone. A fully qualified domain name is specified with a trailing dot, for example: **ldap12.juniper.net.**
Dead Time (default is 5 seconds)	Using the arrows, adjust the number of seconds before Network Director checks an LDAP server that was previously unresponsive. The default value is 5 seconds.
Timeout (default is 5 seconds)	Using the arrows, adjust the number of seconds Network Director tries to establish connection with RADIUS server before giving an unreachable error.
Bind Mode (default is SASL-MD5)	Select either **SASL-MD5** or **SIMPLE-AUTH** to establish authentication for an LDAP session. Simple Authentication and Security Layer (SASL) is a framework for authentication and data security in Internet protocols. It decouples authentication mechanisms from application protocols, in theory enabling any authentication mechanism supported by SASL to be used in any application protocol that uses SASL. SIMPLE-AUTH sends the user's domain name and password in plain text. The server then checks the password against the password attribute in the named entry. TIP: We recommend that connections using SIMPLE-AUTH be encrypted using Transport Layer Security (TLS).

Copyright © 2013, Juniper Networks, Inc.

Table 79: LDAP Profile Settings *(continued)*

Field	Action
MAC Address Format (default is Hyphens)	Select **None**, **Hyphens**, **Colons**, **One-Hyphen**, or **Raw** to determine the MAC address format used with the LDAP server. For example: • **None**: For unicast IPv4, an example MAC address is 0123456789ab. For unicast IPv6, an example MAC address is 20010db8000000000000ff0000428329. • **Hyphens**: For unicast IPv4, an example MAC address with hyphens is 01-23-45-67-89-ab. For unicast IPv6, an example MAC address with hyphens is 2001-0db8-0000-0000-0000-ff00-0042-8329. • **Colons**: For unicast IPv4, an example MAC address with colons is 01:23:45:67:89:ab. For unicast IPv6, an example MAC address with colons is 2001:0db8:0000:0000:0000:ff00:0042:8329. • **One-Hyphen**: IPv6 unicast addresses other than those that start with binary 000 are logically divided into two parts: a 64-bit (sub-)network prefix, and a 64-bit interface identifier used to identify a host's network interface. The hyphen is placed between the two parts. • **Raw**: The IPv6 address is represented by all numbers—no sections containing all zeros are skipped and then represented by a double colon. For example, this is a raw IPv6 address: 2001:0000:0234:C1AB:0000:00A0:AABC:003F. TIP: A media access control address (MAC address) is a unique identifier assigned to network interfaces for communications on the physical network segment. MAC addresses are used as a network address for most IEEE 802 network technologies, including Ethernet.
Base Domain	Base domains contain no extra dots. For example, example.com is a base domain, but www.example.com is not because it contains an extra dot.
Domain Prefix (default is cn)	Enter a domain prefix to identify a subdomain. The subdomain name can be used to identify services, devices, or regions.
Use MAC as Password (default is unchecked)	Check this option if you want each client device to use its MAC address as its password for the LDAP server.
Authorization Password	If you are not using individual MAC addresses as passwords for the LDAP server, provide a common password here.

Click **Done** to create the LDAP Server Profile.

What to Do Next

Link the LDAP server to an Access profile for either wireless or EX Series Switching with ELS. For directions, see "Creating and Managing Access Profiles" on page 136.

Related Documentation

- Creating and Managing Access Profiles on page 136
- Creating and Managing RADIUS Profiles on page 326

Copyright © 2013, Juniper Networks, Inc.

Managing and Creating a Link Aggregation Group

IEEE 802.3ad link aggregation enables you to group Ethernet interfaces to form a single link layer interface, also known as a link aggregation group (LAG) or bundle.

Aggregating multiple links between physical interfaces creates a single logical point-to-point trunk link or a LAG. Link Aggregation Control Protocol (LACP), a component of IEEE 802.3ad, provides additional functionality for LAGs.

LACP ensures that both ends of the Ethernet link are functional and are members of the aggregation group before the link is added to the LAG. If you use LACP, make sure that LACP is enabled at both the local and remote ends of the link. When LACP is configured, it detects misconfigurations on the local end or the remote end of the link. Thus, LACP can help to prevent communication failure. When LACP is not enabled, a local LAG might attempt to transmit packets to a remote single interface, which causes the communication to fail. However, when LACP is enabled, a local LAG cannot transmit packets unless a LAG with LACP is also configured on the remote end of the link.

The maximum number of interfaces that can be grouped into a LAG and the maximum number of LAGs supported on a switch varies according to the switch model and the version of Juniper Networks Junos operating system (Junos OS) that is running on that switch. Be aware of the maximum number of interfaces per LAG and the maximum number of LAGs that are supported on your switches by referring to your device specific documentation before implementing LAG in your network.

NOTE: **You only see the Manage Lag option under Device Management when a qualified switch is selected in the View Pane.**

When creating LAGs, follow these guidelines:

- You must configure the LAG on both sides of the link.
- You must set the interfaces on either side of the link to the same speed.
- You can configure and apply firewall filters on a LAG.

NOTE: **You only see the Manage Lag option under Device Management when a qualified switch is selected in the View Pane.**

Copyright © 2013, Juniper Networks, Inc.

NOTE: MC-LAG, or Multi-Chassis Link Aggregation Group, is a type of LAG with constituent ports that terminate on separate chassis, thereby providing node-level redundancy. Unlike link aggregation in general, MC-LAG is not covered under IEEE 802.1AX-2008. Its implementation varies by vendor. For directions to create an MC-LAG, see "Creating and Managing Multichassis Link Aggregation Groups (MC-LAGs)" on page 468.

This topic includes:

- Link Aggregation Group Options on page 279
- Creating a Link Aggregation Group on page 280
- Managing ICCP Settings on page 282
- What To Do Next on page 282

Link Aggregation Group Options

From the Manage LAG page, you can:

- Create a new Link Aggregation by clicking **Create**. The Create Link Aggregation window opens—for directions, see "Creating a Link Aggregation Group" on page 280.
- Modify an existing Link Aggregation by selecting it and clicking **Edit**. The Modify Link Aggregation window opens. You can modify all the fields in the Modify Link Aggregation window, except the Interface Name field.
- Delete a Link Aggregation Group by selecting it and clicking **Delete**.
- Manage ICCP settings for the selected device by clicking **Manage ICCP Settings**. See "Managing ICCP Settings" on page 282 for more information.

Table 80 on page 279 describes the information provided about the link aggregation configurations on the LACP (Link Aggregation Control Protocol) Configuration page. This page lists all link aggregation groups defined on the selected device.

Table 80: LACP (Link Aggregation Control Protocol) Configuration Fields

Field	Description
Logical Interface Name	Name given to the aggregated interface when the LAG was created.
Member Interfaces	Names of individual member interfaces.
LACP Mode	Mode in which LACP packets are exchanged between the interfaces. The possible modes are: • Active—Indicates that the interface initiates transmission of LACP packets • Passive—Indicates that the interface responds only to LACP packets.

Copyright © 2013, Juniper Networks, Inc.

Table 80: LACP (Link Aggregation Control Protocol) Configuration Fields *(continued)*

Field	Description
Description	The description for the LAG. TIP: If you cannot view the entire description, you can resize the **Description** column by clicking on the column border in the heading and dragging it.
Deployment State	The deployment state of the link aggregation. Deployment state can be: • Pending Deployment—Indicates that the LAG is not yet deployed on the device. • Deployed—Indicates that the LAG is deployed on the device. • Pending Removal—Indicates that the LAG is deleted.
Creation Time	Date and time when this profile was created.
Update Time	Date and time when this profile was last modified.
User Name	The username of the user who created or modified the profile.

TIP: All columns might not be displayed. To show or hide fields in the LACP (Link Aggregation Control Protocol) Configuration table, click the DOWN arrow on the field header, select Columns, and select or clear the check box adjacent to the field that you want to show or hide.

Creating a Link Aggregation Group

You can create one or more LAGs in Network Director. The number of interfaces that can be grouped into a LAG and the total number of LAGs supported on a switch varies according to switch model.

TIP: You can also create one or more MC-LAGs for Virtual Chassis—see "Creating and Managing Multichassis Link Aggregation Groups (MC-LAGs)" on page 468.

Copyright © 2013, Juniper Networks, Inc.

To create a link aggregation group:

1. In the View pane, select a switch for link aggregation.

   NOTE: You only see the Manage Lag option under Device Management when a qualified switch is selected in the View Pane.

2. Click in the Network Director banner.

3. Under Select View, select either **Logical View**, **Location View**, **Device View** or **Custom Group** View.

   TIP: Do not select Virtual View or Topology View.

4. Select **Manage LAG** under Device Management in the Tasks pane.

   The Manage LAG page appears.

   NOTE: If you do not see the Manage LAG option under Device Management, then you did not select a switch in the first step.

5. Click **Create**.

   The Create Link Aggregation window opens.

6. Use the up and down arrows to select an AE Name for the aggregation interface. The interface name begins with *ae* followed by an interface number.

7. Select the mode in which LACP packets are to be exchanged between interfaces, either **Active** or **Passive**.

   - **Active**—Indicates that the interface initiates transmission of LACP packets
   - **Passive**—Indicates that the interface responds only to LACP packets.

8. Enter a description for the link aggregation.

9. Configure up to eight available interfaces on the LAG. Select one or more interfaces from the Available list and then click the RIGHT arrow to move them to the Selected list.

   NOTE: The Available interfaces list displays only those interfaces that are not part of any link aggregation.

10. Click **OK** to save the link aggregation configuration.

Copyright © 2013, Juniper Networks, Inc.

A message confirms that the link aggregation is created successfully and ready to be deployed to a device. If the configuration contains an error, the message instead indicates the error.

11. Click **OK** to close the information message.

    The LAG appears in the Manage LAG list.

Managing ICCP Settings

When a QFX Series device is the selected scope, you can use the ICCP LAG Settings window to manage ICCP on the selected device. Table 81 on page 282 describes the fields in this window.

Table 81: ICCP Settings

Field	Description
Disable (Delete) ICCP Settings	Disable ICCP on the device.
AE Name	Select the aggregated Ethernet interface to use for the ICCP connection.
Local IP	Configure the local IP address to be used by all switches hosting the MC-LAG.
Peer IP	Configure the IP address of the ICCP peer.
VLAN	Enter the name of the VLAN to use for the ICCP connection.
VLAN ID	Enter the ID of the VLAN to use for the ICCP connection.
Liveness detection min receive interval	Configure the minimum interval at which the switch must receive a reply from the other switch with which it has established a Bidirectional Forwarding Detection (BFD) session.
Liveness detection min transmit interval	Configure the minimum transmit interval during which a switch must receive a reply from a switch with which it has established a BFD session.
Liveness detection backup peer IP	Configure the IP address of the liveness detection backup.
Session establish hold time	Configure the time during which an ICCP connection must succeed between the switches hosting the MC-LAG. Configured session establishment hold time results in faster ICCP connection establishment. The recommended value is 50 seconds.

What To Do Next

The configuration changes that you make in the Build mode are not deployed to devices automatically. After you create a link aggregation group, you must manually deploy the changes to the switches in Deploy mode. For details, see *Deploying Configuration to Devices*.

Copyright © 2013, Juniper Networks, Inc.

TIP: Even though link aggregation configuration is not contained within a profile, you can view the link aggregation groups assigned to a switch by using the View Assigned Profiles task in Build mode.

Related Documentation

- Understanding Link Aggregation on page 34
- Viewing Profiles Assigned to a Device on page 480
- Creating and Managing Multichassis Link Aggregation Groups (MC-LAGs) on page 468

Creating and Managing Port Profiles

Port profiles provide a way to provision multiple switch interfaces, including Ethernet interfaces on EX Series switches, Campus Switching ELS, Data Center Switching devices, and fibre channel (FC) interfaces on Data Center Switching devices. In a Port profile, you can define a set of attributes to be shared by multiple interfaces. For example, you could create a Port profile for all access interfaces that connect to VoIP desk phones, configuring the appropriate class-of-service (CoS), authentication, and port security settings for these interfaces in the Port profile. You then assign the Port profile to those interfaces and deploy the resulting configuration on the interfaces.

Port profiles define only the shared attributes. You can configure specific attributes for an interface or a switch during the process of assigning a Port profile to an interface.

To manage or create Port profiles: In Build mode, select **Port** from Profile and Configuration Management in the Tasks pane. The Manage Port Profiles page appears.

This topic describes:

- Managing Port Profiles on page 283
- Creating Port Profiles on page 285
- Specifying Settings for an EX Switching Port Profile on page 286
- Specifying Settings for a Campus Switching ELS Port Profile on page 295
- Specifying Settings for the Data Center Switching Port Profile on page 305
- What to Do Next on page 315

Managing Port Profiles

Use the Manage Port Profiles page to manage existing Port profiles and to create new ones. Port profiles enable the definition and application of a common set of attributes to interfaces.

From the Manage Port Profiles page, you can:

- Create a new profile by clicking **Add**. For details, see "Creating Port Profiles" on page 285.
- Modify an existing profile by selecting it and clicking **Edit**.
- Associate a Port profile to specific interfaces by selecting it and clicking **Assign**.

Copyright © 2013, Juniper Networks, Inc.

During the assignment process, you will have an opportunity to configure interface-specific settings, such as IP address.

- Change a Port profile's current interface assignments by selecting it and clicking **Edit Assignments**.
- View information about a profile, including the interfaces it is associated with, by selecting the profile and clicking **Details** or by clicking the profile name.
- Delete profiles by selecting the profiles and clicking **Delete**.

TIP: You cannot delete profiles that are in use—that is, assigned to objects or used by other profiles. To see the current assignments for a profile, click the profile name.

- Clone a profile by selecting a profile and clicking **Clone**.

Network Director provides a set of default Port profiles: Desktop Port, Desktop and Phone Port, Server Port, Switched Downlink, Switched Uplink, Wireless Access Port, and Custom Port. These profiles contain configuration appropriate for the named port role. You can manage these profiles the same way that you manage a user-created profile. For more information about these profiles, see "Understanding Port Profiles" on page 36.

Table 82 on page 284 describes the information provided about Port profiles on the Manage Port Profiles page. This page lists all Port profiles defined for your network, regardless of your current selected scope in the network view.

Table 82: Manage Port Profiles Table

Column	Description
Profile Name	Name given to the profile when the profile was created. Click the profile name to view profile details.
Family Type	One of the following: • EX—for EX Series switches • ELS—for Campus Switching ELS • Data Center Switching—for Data Center Switching devices
Description	Description of the Port profile that was entered when the profile was created.
Port Family	One of the following: • Switching—for Port profiles that configure Layer 2 interfaces. • Routing—for Port profiles that configure Layer 3 interfaces. • FIBRE—for Port profiles that configure fibre channel (FC) interfaces.

Copyright © 2013, Juniper Networks, Inc.

Table 82: Manage Port Profiles Table *(continued)*

Column	Description
Assignment State	One of the following states: • Deployed—The profile has been assigned to interfaces and the configuration has been deployed on the devices. • Pending Deployment—The profile has been assigned to interfaces or its previous assignments have been changed, but the new or modified configuration has not yet been deployed on the devices. • Unassigned—The profile has not yet been assigned to interfaces.
Creation Time	Date and time when this profile was created.
Update Time	Date and time when this profile was last modified.
User Name	The username of the user who created or modified the profile.

TIP: All columns might not be currently displayed. To show or hide fields in the table, click the down arrow on the field header, select Columns, and select or clear the check box adjacent to the field that you want to show or hide.

Creating Port Profiles

To create a Port profile for EX Series switches, Campus Switching ELS, or Data Center Switching:

1. Click Build in the Network Director banner.
2. Under Select View, select either **Logical View**, **Location View**, **Device View** or **Custom Group** View.

   TIP: Do not select **Virtual View** or **Topology View**.

3. Click **Port** under Profile and Configuration Management in the Tasks pane.

   The Manage Port Profiles page appears.

4. Click **Add**.

   The Device Family Chooser appears.

5. Select **Switching (EX)**, **Campus Switching ELS**, or **Data Center Switching Non_ELS**.

   The Create Port Profile page appears for the selected family with the appropriate fields for configuring that family.

6. Enter settings for the Port profile. For information about the Port profile settings, select the section for the type of port you are configuring:

   - Specifying Settings for an EX Switching Port Profile on page 286

Copyright © 2013, Juniper Networks, Inc.

- Specifying Settings for a Campus Switching ELS Port Profile on page 295
- Specifying Settings for the Data Center Switching Port Profile on page 305

Specifying Settings for an EX Switching Port Profile

Use the Create Port Profile page to define a common set of port attributes, which you can then apply to a group of interfaces. These directions address creating a Port profile for EX Series switches.

TIP: You can reference a CoS profile, ingress and egress Filter profiles, and an Authentication profile in a Port profile. Create these profiles before you create Port profiles. You can also enable power over Ethernet (PoE).

After you create a Port profile, you assign it to individual interfaces or to members of a port group. During this process, you can also configure interface-specific attributes, such as IP address, and certain device-specific attributes, such as the Access profile to use for all ports on the device. You can assign only one Port profile to an interface.

Table 83 on page 286 describes the basic settings available in a Port profile. Table 84 on page 293 describes the advanced settings. The defaults for these options depend on which Service Type you select.

Table 83: Port Profile Basic Settings for an EX Switching Port Profile

Field	Action
Profile Name	A default name that corresponds to the Service Type is displayed—when you change the Service Type, this default profile name changes. You can also change the name of profile, using up to 64 alphanumeric characters and no special characters other than an underscore. The name must be unique among Port profiles.
Description	A default description of the preconfigured service types appears by default. You can change the description of the Port profile, which will appear on Manage Port Profiles page. You can use up to 256 characters.

Copyright © 2013, Juniper Networks, Inc.

Table 83: Port Profile Basic Settings for an EX Switching Port Profile *(continued)*

Field	Action
Service Type	Select one the preconfigured switching options, **Desktop Port**, **Desktop Phone Port**, **Switched Uplink**, **Switched Downlink**, **Server Port**, or **Wireless Access Port**. To create your own switching or routing service type, select **Custom**. TIP: No preconfigured routing Service Types are provided. You must create them using the Custom option.
	Desktop Port default service type has the following default settings: • CoS Profile—no default provided • Family Type—switching • Port Mode—access • Power over Ethernet—disabled • Auto Negotiation—enabled • Flow Control—enabled • Maximum Size—no default provided • Speed—no default provided • Link Mode—no default provided • Port Security—enabled • Trust DHCP—disabled • MAC Limit—1 • MAC Limit Action—drop • Allowed MAC List—no default provided
	Desktop Phone Port preconfigured service type has the following default settings: • CoS Profile—juniper_CoS_template • Family Type—switching • Port Mode—access • Power over Ethernet—disabled • Auto Negotiation—enabled • Flow Control—enabled • Maximum Size—no default provided • Speed—no default provided • Link Mode—no default provided • Port Security—enabled • Trust DHCP—disabled • MAC Limit—2 • MAC Limit Action—drop • Allowed MAC List—no default provided

Copyright © 2013, Juniper Networks, Inc.

Table 83: Port Profile Basic Settings for an EX Switching Port Profile *(continued)*

Field	Action
	Switched Uplink preconfigured service type has the following default settings: • CoS Profile—juniper_CoS_template • Family Type—switching • Port Mode—trunk • Power over Ethernet—disabled • Auto Negotiation—enabled • Flow Control—enabled • Maximum Size—no default provided • Speed—no default provided • Link Mode—no default provided • Port Security—enabled • MAC Limit—no default provided • MAC Limit Action—no default provided • Allowed MAC List—no default provided
	Switched Downlink preconfigured service type has the following default settings: • CoS Profile—juniper_CoS_template • Family Type—switching • Port Mode—trunk • Power over Ethernet—disabled • Auto Negotiation—enabled • Flow Control—enabled • Maximum Size—no default provided • Speed—no default provided • Link Mode—no default provided • MAC Limit—no default provided • MAC Limit Action—no default provided • Allowed MAC list—no default provided

Copyright © 2013, Juniper Networks, Inc.

Table 83: Port Profile Basic Settings for an EX Switching Port Profile *(continued)*

Field	Action
	Server Port preconfigured service type has the following default settings: • CoS Profile—juniper_CoS_template • Family Type—switching • Port Mode—trunk • Power over Ethernet—disabled • Auto Negotiation—enabled • Flow Control—enabled • Maximum Size—no default provided • Speed—no default provided • Link Mode—no default provided • Port Security—enabled • MAC Limit—no default provided • MAC Limit Action—no default provided • Allowed MAC list—no default provided
	Wireless Access Port preconfigured service type has the following default settings: • Family Type—switching • Port Mode—Access • Power over Ethernet—disabled • Auto Negotiation—enabled • Flow Control—enabled • Maximum Size—no default provided • Speed—no default provided • Link Mode—no default provided • Trust DHCP—disabled • MAC Limit—no default provided • MAC Limit Action—no default provided • Allowed MAC List—no default provided
CoS Profile	Click **Select** to choose from existing CoS profiles. The CoS configuration contained in the CoS profile will be applied to the interfaces that the Port profile is assigned to when you deploy the configuration. Click **OK**. Some preconfigured Service Types have a default CoS profile—see Service Types for details.
Port Family Options The available settings and defaults for these options depend on which Service Type you selected—see Service Type for details.	

Copyright © 2013, Juniper Networks, Inc.

Table 83: Port Profile Basic Settings for an EX Switching Port Profile *(continued)*

Field	Action
Family Type	This setting cannot be changed if any preconfigured Service Type was selected. If you selected the Custom Service Type, indicate whether the interface operates as a Layer 2 (**Switching**) or a Layer 3 (**Routing**) interface. TIP: All preconfigured Service Types are for switching. If you select **Routing**, you configure an IP address on a per-interface basis when you assign the profile to individual interfaces. TIP: Service Type must be set to Custom to configure a routing interface.
Port Mode	This setting cannot be changed if any preconfigured Service Type was selected. If you selected the Custom Service Type, select the port mode for the EX Series switching interface, either **Access**, **Trunk**, or **Tagged Access**. • **Access**—Use for interfaces that connect to an end device, such as a desktop computer, an IP telephone, a wireless access point, a printer, or a security camera. The interface must belong to a single VLAN. Frames sent and received over the over the interface are untagged Ethernet frames. This is the default for a Desktop Port, Desktop Phone Port, and Wireless Access Port. • **Trunk**—Use for interfaces that connect to a switch or router. Trunk interfaces can belong to more than one VLAN, enabling VLAN traffic to be multiplexed on a single physical interface. The Ethernet frames sent and received over the interface are tagged frames, in which IEEE 802.1Q tagging is used to segregate the traffic from each VLAN. This is the default for Switched Uplink, Switched Downlink, Server Port, and Wireless Access Port. • **Tagged Access**—Use for access interfaces where VLAN tagging is required, typically when the interface connects to a server running virtual machines using virtual Ethernet port aggregator (VEPA) technology. The traffic generated by the server can contain an aggregation of VLAN packets from different virtual machines on that server, requiring that packets be tagged.
Authentication Profile for these switching interfaces only: (Desktop Port, Desktop Phone Port, Wireless Access Port, Custom Port)	Select the Authentication profile for the interface from a list of existing profiles by clicking **Select**, selecting one of the listed profiles, and then clicking **OK**. By assigning an Authentication profile to the Port profile, you can enable 802.1X and captive portal authentication on interfaces. If you do not specify an Authentication profile, the interface is an open port and no authentication is required to connect. NOTE: You cannot configure 802.1X authentication on aggregated Ethernet interfaces. If you attempt to deploy a Port profile that contains an Authentication profile on an aggregated Ethernet interface, the deployment will fail.

Copyright © 2013, Juniper Networks, Inc.

Table 83: Port Profile Basic Settings for an EX Switching Port Profile *(continued)*

Field	Action
Ingress Filter (available for all Service Types, including Custom for routing)	Select an Ingress Filter for the interface by clicking **Select**, selecting one of the listed filters, and then clicking **OK**.
Egress Filters (available for all Service Types, including Custom for routing)	Select an egress Filter for the interface by clicking **Select**, selecting one of the listed filters, and then clicking **OK**.
VLAN Options Available VLAN options depend on the Service Type selected.	
Member VLANs (available for Desktop Port, Desktop Phone Port, Wireless Access Port, Custom Port)	Select a VLAN for the interface by clicking **Select**, selecting one of the listed filters, and then clicking **OK**. The VLAN is added to the Member VLANS list.
Voice VLAN (available for Desktop Phone Port, Custom Port)	Select a voice VLAN for the interface by clicking **Select**, selecting one of the listed filters, and then clicking **OK**. The VLAN is added to the Member VLANS list.
VLAN Options (available for Switched Uplink, Switched Downlink, Server Port)	This configuration includes both member VLANs and a Native VLAN option for Trunk ports and Tagged Access ports. 1. Click **Add** to open the Choose VLAN Profile window. 2. Select one or more of the listed VLAN profiles. 3. Click **OK**. The VLAN is added to the Member VLANS list. 4. For Native VLAN, click **Select** to open the Choose VLAN Profile window. 5. Select one of the listed VLAN profiles. 6. Click **OK**.
Power over Ethernet (PoE) You can enable PoE and display the configuration options by enabling **Configure Power over Ethernet**.	

Copyright © 2013, Juniper Networks, Inc.

Table 83: Port Profile Basic Settings for an EX Switching Port Profile *(continued)*

Field	Action
Configure Power over Ethernet	Enable to configure PoE settings. If you do not enable this option, Network Director will not send any PoE configuration commands to the device when the profile is deployed on the device. For example, if PoE is enabled on an interface, it will remain enabled. On EX Series switches, the factory default configuration enables PoE on all interfaces that support PoE. If you enable this option, the PoE settings in this profile will be deployed on the interfaces that support PoE. If you assign this Port profile to interfaces that do not support PoE, the profile will be deployed successfully on those interfaces, but the PoE settings will not take effect.
Maximum Power (W)	Use the arrows to adjust the maximum PoE power in watts allocated to a PoE port. The powered device cannot draw more power than the wattage specified. If it does so, PoE power to the port is shut down. Maximum power for PoE is 15.4W, Extended PoE is 18.6W and PoE+ is 30W. The Maximum Power setting has no effect when the PoE management mode for a switch or line card is class mode, which is the default mode. In class mode, the power allocated to a PoE port is determined either by LLDP negotiation with the powered device or by the PoE class of the powered device if LLDP is not supported. You must set the PoE power management mode for the switch or line card to static mode for the Maximum Power setting to take effect. Do this in the Device Common Settings profile. If you specify a maximum wattage that is greater than the maximum wattage that can be supplied by the port, your configuration is accepted when the Port profile is deployed on the port. However, the maximum wattage is set to the port's maximum supported wattage. The maximum supported wattages for PoE ports are: • 15.4W for ports that support IEEE 802.3af only • 18.6W for IEEE 802.3af ports on switches that support enhanced PoE • 30W for ports that support IEEE 802.3at Default: 15.4W
Priority	Select a power priority for the PoE port—either **Low** or **High**. If there is a shortage of PoE power on the switch, power to low priority ports is shut down before power to high priority ports. Within ports with the same assigned priority, power priority is determined by port number—ports with a lower port number have a higher power priority. Default: low priority
Disable PoE	Select to disable PoE on the interfaces using this port profile.

Copyright © 2013, Juniper Networks, Inc.

To use default Port profile Advanced Settings, click **Done** to create the Port profile. To configure Advanced Settings, click **Advanced Settings** and then provide the information in Table 84 on page 293.

Table 84: Port Profile Advanced Settings

Field	Action
Advanced Settings Expand Advanced Settings to configure link settings and port security. The defaults for these options depend on which Service Type you selected.	
Enable Auto Negotiation	Autonegotiation of link speed and duplex mode is enabled by default; clear to disable autonegotiation. If you disable autonegotiation, you must set link speed and link mode. You cannot disable autonegotiation if a link speed of 1 Gbps is configured. This configuration might be accepted, but autonegotiation will not be disabled. NOTE: This setting is ignored when you assign a Port profile to an Aggregated Ethernet interface.
Enable Flow Control	Select to enable flow control on the interface, which permits the switch suspend packet transmission for a set period of time in response to a PAUSE frame sent by a congested switch. Flow control applies only to links operating in 1 Gbps, full-duplex mode.
Maximum Size (bytes)	Using the arrows, indicate the maximum transmission unit (MTU), which is the maximum size of Ethernet frames sent by the interface. To calculate the MTU, add 14 bytes overhead to the maximum payload you want sent. Range: 256 through 9216 bytes
Speed	Select the link speed. If you select a link speed when autonegotiation is enabled, autonegotiation remains enabled and the interface will advertise the link speed that you specify as its maximum link speed. NOTE: This setting is ignored when you assign a Port profile to an Aggregated Ethernet interface.
Link Mode	Select the duplex mode, either **Automatic**, **Full Duplex**, or **Half Duplex**. Select **Automatic** to enable auto-negotiation when autonegotiation is enabled. NOTE: This setting is ignored when you assign a Port profile to an Aggregated Ethernet interface. You cannot select Half Duplex when link speed Autonegotiation or 1 Gbps.

Copyright © 2013, Juniper Networks, Inc.

Table 84: Port Profile Advanced Settings *(continued)*

Field	Action
Port Security (Switching Interfaces Only) Select to enable port security (default); clear to disable port security. When port security is enabled, you can configure port security options such as learned MAC address limits on an interface. When port security is disabled, no port security is applied to the interface, including the default port security options.	
Trust DHCP	Select to permit messages from a DHCP server to be received on the interface—this is the default. Clear to block all messages from a DHCP server from being received on the interface. TIP: For this port security feature to work, DHCP snooping must be enabled on the VLAN the interface belongs to. You can enable DHCP snooping on the VLAN in the VLAN profile. For directions, see "Creating and Managing VLAN Profiles" on page 330.
MAC Limit	Type the number of MAC address that can be dynamically learned on the interface. Range: 1 through 163839 Default: For Desktop Ports, 1. For Desktop Phone Ports, 2. For all others, none.
MAC Limit Action	Select the action to be taken if the MAC address limit is exceeded: • **Drop**—Drop any packet with a previously unlearned MAC address and generate a system log entry, and SNMP trap, or an alarm. This is the default for a Desktop Port and Desktop Phone Ports. • **Log**—Accept packets with new MAC addresses and learn the addresses, but generate a system log entry, and SNMP trap, or an alarm. • **Shutdown**—Shut down the interface and generate a system log message, SNMP trap, or an alarm. If an interface is shut down because the MAC address limit has been exceeded, you must use the CLI command **clear ethernet-switching port-error interface *name*** to clear the error and bring the interface back into service. TIP: You can use the CLI to configure auto-recovery on an interface that has been shut down by a MAC limit error. • **None**—No action. This selection effectively disables MAC address limiting on the interface. This is the default for Switched Uplink Ports, Switched Downlink Ports, and Server Ports.

Copyright © 2013, Juniper Networks, Inc.

Table 84: Port Profile Advanced Settings *(continued)*

Field	Action
Allowed MAC List	Indicate the MAC addresses of devices that are allowed access to the interface in the Allowed MAC List. Any device whose MAC address does not match an address in the list will not be allowed access to the interface. A list with no entries means that a client with any MAC address is permitted to access the interface. To enter a MAC address, click **Add** and then type the MAC addresses in the field provided. Enter MAC addresses as two-character hexadecimal numbers separated by colons. Click **Save** to save the entry. NOTE: Configuring an allowed MAC address list does not block the switch from receiving Layer 2 control packets—such as Link Layer Discovery Protocol (LLDP) packets—transmitted from MAC addresses that are not specified in the address list. Control packets do not undergo the MAC address check. However, the switch does not forward them to another destination. Default: No entries

If you configured Advanced Settings, click **OK**.

Click **Done** to create the port profile.

Specifying Settings for a Campus Switching ELS Port Profile

Use the Create Port Profile page to define a common set of port attributes in a Port profile. You can then apply the Port profile to interfaces on a group of Campus Switching ELS devices.

TIP: In a Port profile, you can reference a CoS profile, ingress and egress filters, and an Authentication profile. You must reference a VLAN profile. Create these profiles before you create the Port profile. You can also enable power over Ethernet (PoE).

After you create a Port profile, you can assign it to individual interfaces or to members of a Port group. During this assignment process, you can also configure interface-specific attributes, such as IP address, and certain device-specific attributes, such as the Access profile to use for all ports on the device. You can assign only one Port profile to an interface.

Table 85 on page 296 describes the basic settings available in a Port profile.
Table 86 on page 302 describes the advanced settings. The defaults for these options depend on which Service Type you select.

Copyright © 2013, Juniper Networks, Inc.

Table 85: Port Profile Basic Settings For Campus Switching ELS

Field	Action
Profile Name	Type the name of profile, using up to 64 alphanumeric characters and no special characters other than an underscore. The name must be unique among Port profiles.
Description	Type a description of the Port profile, which will appear on Manage Port Profiles page. You can use up to 256 characters.

Copyright © 2013, Juniper Networks, Inc.

Table 85: Port Profile Basic Settings For Campus Switching ELS *(continued)*

Field	Action
Service Type	Select one the preconfigured options **Desktop Port**, **Desktop Phone Port**, **Switched Uplink**, **Switched Downlink**, **Server Port**, or **Wireless Access Port**. To create your own service type, select **Custom**. **Desktop Port** service type has the following default settings: • CoS Profile—no default provided • Family Type—switching • Port Mode—access • Power over Ethernet—disabled • Auto Negotiation—enabled • Flow Control—enabled • Maximum Size—no default provided • Speed—no default provided • Link Mode—no default provided • Port Security—enabled • Trust DHCP—disabled • MAC Limit—1 • MAC Limit Action—drop • Allowed MAC List—no default provided **Desktop Phone Port** service type has the following default settings: • CoS Profile—juniper_CoS_template • Family Type—switching • Port Mode—access • Power over Ethernet—disabled • Auto Negotiation—enabled • Flow Control—enabled • Maximum Size—no default provided • Speed—no default provided • Link Mode—no default provided • Port Security—enabled • Trust DHCP—disabled • MAC Limit—2 • MAC Limit Action—drop • Allowed MAC List—no default provided

Copyright © 2013, Juniper Networks, Inc.

Table 85: Port Profile Basic Settings For Campus Switching ELS *(continued)*

Field	Action
	Switched Uplink service type has the following default settings: • CoS Profile—juniper_CoS_template • Family Type—switching • Port Mode—trunk • Power over Ethernet—disabled • Auto Negotiation—enabled • Flow Control—enabled • Maximum Size—no default provided • Speed—no default provided • Link Mode—no default provided • Port Security—enabled • MAC Limit—no default provided • MAC Limit Action—no default provided • Allowed MAC List—no default provided
	Switched Downlink service type has the following default settings: • CoS Profile—juniper_CoS_template • Family Type—switching • Port Mode—trunk • Power over Ethernet—disabled • Auto Negotiation—enabled • Flow Control—enabled • Maximum Size—no default provided • Speed—no default provided • Link Mode—no default provided • MAC Limit—no default provided • MAC Limit Action—no default provided • Allowed MAC list—no default provided

Copyright © 2013, Juniper Networks, Inc.

Table 85: Port Profile Basic Settings For Campus Switching ELS *(continued)*

Field	Action
	Server Port service type has the following default settings: • CoS Profile—juniper_CoS_template • Family Type—switching • Port Mode—trunk • Power over Ethernet—disabled • Auto Negotiation—enabled • Flow Control—enabled • Maximum Size—no default provided • Speed—no default provided • Link Mode—no default provided • Port Security—enabled • MAC Limit—no default provided • MAC Limit Action—no default provided • Allowed MAC list—no default provided
	Wireless Access Port service type has the following default settings: • Family Type—switching • Port Mode—Access • Power over Ethernet—disabled • Auto Negotiation—enabled • Flow Control—enabled • Maximum Size—no default provided • Speed—no default provided • Link Mode—no default provided • Trust DHCP—disabled • MAC Limit—no default provided • MAC Limit Action—no default provided • Allowed MAC List—no default provided
CoS Profile	Click **Select** to choose from existing CoS profiles. The CoS configuration contained in the CoS profile will be applied to the interfaces that the Port profile is assigned to when you deploy the configuration. Most Service Types use a default CoS Profile—for details, see Service Type.
Port Family Options The available settings and defaults for these options depend on which Service Type you selected.	

Copyright © 2013, Juniper Networks, Inc.

Table 85: Port Profile Basic Settings For Campus Switching ELS *(continued)*

Field	Action
Family Type: Switching or Routing	This setting cannot be changed if any preconfigured Service Type was selected. If you selected the Custom Service Type, indicate whether the interface operates as a Layer 2 (Switching) or a Layer 3 (Routing) interface. TIP: Service Type must be set to Custom to configure a routing interface. If you select routing, you configure an IP address on a per-interface basis when you assign the profile to individual interfaces.
Port Mode for switching interfaces only	This setting cannot be changed if any preconfigured Service Type was selected. If you selected the Custom Service Type, select the port mode for the interface, either **Access**, **Trunk**, or **Tagged Access**. • **Access**—Use for interfaces that connect to an end device, such as a desktop computer, an IP telephone, a wireless access point, a printer, or a security camera. The interface must belong to a single VLAN. Frames sent and received over the over the interface are untagged Ethernet frames. • **Trunk**—Use for interfaces that connect to a switch or router. Trunk interfaces can belong to more than one VLAN, enabling VLAN traffic to be multiplexed on a single physical interface. The Ethernet frames sent and received over the interface are tagged frames, in which IEEE 802.1Q tagging is used to segregate the traffic from each VLAN. • **Tagged Access**—Use for access interfaces where VLAN tagging is required, typically when the interface connects to a server running virtual machines using virtual Ethernet port aggregator (VEPA) technology. The traffic generated by the server can contain an aggregation of VLAN packets from different virtual machines on that server, requiring that packets be tagged.
Authentication Profile for these switching interfaces only: Desktop Port, Desktop Phone Port, Wireless Access Port, Custom Port	Select the Authentication profile for the interface from a list of existing profiles by clicking **Select**. By assigning an Authentication profile to the Port profile, you can enable 802.1X and captive portal authentication on interfaces. If you do not specify an Authentication profile, the interface is an open port and no authentication is required to connect. NOTE: You cannot configure 802.1X authentication on aggregated Ethernet interfaces. If you attempt to deploy a Port profile that contains an Authentication profile on an aggregated Ethernet interface, the deployment will fail.
Ingress Filter (available for all Service Types including Custom for routing)	Select an Ingress Filter for the interface by clicking **Select**, selecting one of the listed filters, and then clicking **OK**.
Egress Filters (available for all Service Types)	Select an Egress Filter for the interface by clicking **Select**, selecting one of the listed filters, and then clicking **OK**.

Copyright © 2013, Juniper Networks, Inc.

Table 85: Port Profile Basic Settings For Campus Switching ELS *(continued)*

Field	Action
VLAN Options Available VLAN options depend on the Service Type selected. VLAN association is required for Campus Switching ELS.	
Member VLAN (all Service Types)	This configuration is for one VLAN. Select a VLAN for the interface by clicking **Select**, selecting one of the listed filters, and then clicking **OK**.
Voice VLAN (Desktop Phone Port, Custom Port)	This configuration is for one VLAN. Select a voice VLAN for the interface by clicking **Select**, selecting one of the listed filters, and then clicking **OK**.
Native VLAN (Switched Uplink, Switched Downlink)	These configurations include both member VLANs and a Native VLAN option. To configure the Native VLAN: 1. Click **Add** under VLAN Options to open the Choose VLAN Profile window. 2. Select one or more of the listed VLAN profiles. 3. Click **OK**. 4. Click **Select** for Native VLANs to open the Choose VLAN Profile window. 5. Select one of the listed VLAN profiles. 6. Click **OK**.
Power over Ethernet (PoE)	
Configure Power over Ethernet	Enable to configure PoE settings. If you do not enable this option, Network Director will not send any PoE configuration commands to the device when the profile is deployed on the device. For example, if PoE is enabled on an interface, it will remain enabled. If you enable this option, the PoE settings in this profile will be deployed on the interfaces that support PoE. If you assign this Port profile to interfaces that do not support PoE, the profile can be deployed successfully on those interfaces, but the PoE settings do not take effect. TIP: EX 9200 does not support PoE.

Copyright © 2013, Juniper Networks, Inc.

Table 85: Port Profile Basic Settings For Campus Switching ELS *(continued)*

Field	Action
Maximum Power (W)	Use the arrows to adjust the maximum PoE power allocated to a PoE port in watts. The powered device cannot draw more power than the wattage specified. If it does so, PoE power to the port is shut down. The Maximum Power setting has no effect when the PoE management mode for the switch or line card is class mode, which is the default mode. In class mode, the power allocated to a PoE port is determined either by LLDP negotiation with the powered device or by the PoE class of the powered device if LLDP is not supported. You must set the PoE power management mode for the switch or line card to static mode for the Maximum Power setting to take effect. You can do so in Device Common Settings profile. If you specify a maximum wattage that is greater than the maximum wattage that can be supplied by the port, your configuration is accepted when the Port profile is deployed on the port. However, the maximum wattage is set to the port's maximum supported wattage. The maximum supported wattages for PoE ports are: • 15.4W for ports that support IEEE 802.3af only • 18.6W for IEEE 802.3af ports on switches that support enhanced PoE • 30W for ports that support IEEE 802.3at Default: 15.4W
Priority	Select a power priority for the PoE port—either **Low** or **High**. If there is a shortage of PoE power on the switch, power to low priority ports is shut down before power to high priority ports. Within ports with the same assigned priority, power priority is determined by port number—ports with a lower port number have a higher power priority. Default: low priority
Disable PoE	Select to disable PoE on the interface.

To skip Advanced Settings and use default Advanced Settings, click **Done** to create the port profile. To configure Advanced Settings, click **Advanced Settings** and then provide the information in Table 86 on page 302.

Table 86: Port Profile Advanced Settings for Campus Switching ELS

Field	Action
Link Settings The defaults for these settings depend on which Service Type you selected.	

Copyright © 2013, Juniper Networks, Inc.

Table 86: Port Profile Advanced Settings for Campus Switching ELS *(continued)*

Field	Action
Enable Auto Negotiation	Autonegotiation of link speed and duplex mode is enabled by default; remove the check mark to disable autonegotiation. TIP: If you disable autonegotiation, you must set link speed and link mode. You cannot disable autonegotiation if a link speed of 1 Gbps is configured. This configuration might be accepted, but autonegotiation will not be disabled. NOTE: This setting is ignored when you assign a Port profile to an Aggregated Ethernet interface.
Enable Flow Control	Select to enable flow control on the interface, which permits the switch suspend packet transmission for a set period of time in response to a PAUSE frame sent by a congested switch. Flow control applies only to links operating in 1 Gbps, full-duplex mode.
Maximum Size (bytes)	Type the maximum transmission unit (MTU), which is the maximum size of Ethernet frames sent by the interface. To calculate the MTU, add 14 bytes overhead to the maximum payload you want sent. Range: 256 through 9216 bytes
Speed	Select the link speed. If you select a link speed when autonegotiation is enabled, autonegotiation remains enabled and the interface will advertise the link speed that you specify as its maximum link speed. NOTE: This setting is ignored when you assign a Port profile to an Aggregated Ethernet interface.
Link Mode	Select the duplex mode. Select **Automatic** to enable auto-negotiation when autonegotiation is enabled. NOTE: This setting is ignored when you assign a Port profile to an Aggregated Ethernet interface. You cannot select Half Duplex when link speed Autonegotiation or 1 Gbps.
Port Security (Switching Interfaces Only) The defaults for these settings depend on which Service Type you selected.	

Copyright © 2013, Juniper Networks, Inc.

Table 86: Port Profile Advanced Settings for Campus Switching ELS *(continued)*

Field	Action
Port Security	Select to enable port security; clear to disable port security. When port security is enabled, you can configure port security options on an interface, such as learned MAC address limits. When port security is disabled, no port security is applied to the interface, including the default port security options. Default: Port security is disabled
Trust DHCP	Select to permit messages from a DHCP server to be received on the interface. Clear to block all messages from a DHCP server from being received on the interface. TIP: For this port security feature to work, DHCP snooping must be enabled on the VLAN the interface belongs to. You can enable DHCP snooping on the VLAN in the VLAN profile.
MAC Limit	Using the arrows, indicate the number of MAC addresses that can be dynamically learned on the interface. NOTE: This setting is required when you enable port security. Range: 1 through 163839
MAC Limit Action	Select the actions to be taken if the MAC address limit is exceeded: • **Drop**—Drop any packet with a previously unlearned MAC address and generate a system log entry, and SNMP trap, or an alarm. • **Log**—Accept packets with new MAC addresses and learn the addresses, but generate a system log entry, and SNMP trap, or an alarm. • **Shutdown**—Shut down the interface and generate a system log message, SNMP trap, or an alarm. If an interface is shut down because the MAC address limit has been exceeded, you must use the CLI command **clear ethernet-switching port-error interface *name*** to clear the error and bring the interface back into service. TIP: You can use the CLI to configure auto-recovery on an interface that has been shutdown by a MAC limit error. • **None**—No action. This selection effectively disables MAC address limiting on the interface.

Copyright © 2013, Juniper Networks, Inc.

Table 86: Port Profile Advanced Settings for Campus Switching ELS *(continued)*

Field	Action
Allowed MAC List	Add the MAC addresses of devices that are allowed access to the interface in the Allowed MAC List. Any device whose MAC address does not match an address in the list will not be allowed access to the interface. However, a list with no entries means that a client with any MAC address is permitted to access the interface. To add a MAC address, click **Add** and type the MAC addresses in the *Enter MAC addresses here...* field. Enter MAC addresses as two-character hexadecimal numbers separated by colons. Click **Save** to save the entry. NOTE: Configuring an allowed MAC address list does not block the switch from receiving Layer 2 control packets—such as Link Layer Discovery Protocol (LLDP) packets—transmitted from MAC addresses that are not specified in the address list. Control packets do not undergo the MAC address check. However, the switch does not forward them to another destination.

Click **OK** to close the Advanced Settings window.

Click **Done** to save the Port profile for Campus Switching ELS.

Specifying Settings for the Data Center Switching Port Profile

Use the Create Port Profile page to define a common set of attributes in a Port profile, which you can then apply to a group of interfaces on Data Center Switching devices. Data Center Switching Port profiles can be one of two types, Ethernet Port or Fibre Channel (FC) Port.

TIP: You can reference the following profile types in an Ethernet Port profile: CoS, Filter (ingress and egress), Authentication, and VLAN. Create these profiles and maps before you create Port profiles.

After you create a Port profile, you can assign it to either individual interfaces or to members of port groups. During this process, you can also configure interface-specific attributes, such as IP address, and certain device-specific attributes, such as the Access profile to use for all ports on the device. You can assign only one Port profile to either an interface or port group.

Table 87 on page 306 describes the basic settings available in the data center Port profile. Table 88 on page 310 describes the standard settings available for an Ethernet port profile. Table 89 on page 312 describes the advanced settings available for an Ethernet port profile. Table 90 on page 314 describes the settings available for an FC port profile.

Copyright © 2013, Juniper Networks, Inc.

Table 87: Port Profile Basic Settings for Data Center Ports

Field	Action
Profile Name	Type the name of profile, using up to 64 alphanumeric characters and no special characters other than an underscore. The name must be unique among Port profiles.
Description	Type a description of the Port profile, which will appear on Manage Port Profiles page. You can use up to 256 characters.

Copyright © 2013, Juniper Networks, Inc.

Table 87: Port Profile Basic Settings for Data Center Ports *(continued)*

Field	Action
Service Type	Select a service type for the profile. The service type describes the function that the port will serve. Selecting a service type automatically configures some of the other page fields to support that service type. Some of the automatic settings are mandatory for the service type, so you cannot edit those fields. Select one the preconfigured switching options, **Desktop Port**, **Desktop Phone Port**, **Switched Uplink**, **Switched Downlink**, **Server Port**, **FCoE Gateway**, **Fibre Channel Port**, or **FCoE Transit Port**. To create your own switching or routing service type, select **Custom**. TIP: No preconfigured routing Service Types are provided. You must create them using the Custom option. **Desktop Port** service type has the following default settings: • CoS Profile—no default provided • Family Type—switching • Port Mode—access • Auto Negotiation—enabled • Flow Control—enabled • Maximum Size—no default provided • Speed—no default provided • Link Mode—no default provided • Port Security—enabled • Trust DHCP—disabled • MAC Limit—1 • MAC Limit Action—drop • Allowed MAC List—no default provided **Desktop Phone Port** service type has the following default settings: • CoS Profile—juniper_CoS_template • Family Type—switching • Port Mode—access • Auto Negotiation—enabled • Flow Control—enabled • Maximum Size—no default provided • Speed—no default provided • Link Mode—no default provided • Port Security—enabled • Trust DHCP—disabled • MAC Limit—2 • MAC Limit Action—drop • Allowed MAC List—no default provided

Copyright © 2013, Juniper Networks, Inc.

Table 87: Port Profile Basic Settings for Data Center Ports *(continued)*

Field	Action
	Switched Uplink service type has the following default settings: • CoS Profile—juniper_CoS_template • Family Type—switching • Port Mode—trunk • Auto Negotiation—enabled • Flow Control—enabled • Maximum Size—no default provided • Speed—no default provided • Link Mode—no default provided • Port Security—enabled • MAC Limit—no default provided • MAC Limit Action—no default provided • Allowed MAC List—no default provided
	Switched Downlink service type has the following default settings: • CoS Profile—juniper_CoS_template • Family Type—switching • Port Mode—trunk • Auto Negotiation—enabled • Flow Control—enabled • Maximum Size—no default provided • Speed—no default provided • Link Mode—no default provided • MAC Limit—no default provided • MAC Limit Action—no default provided • Allowed MAC list—no default provided
	Server Port service type has the following default settings: • CoS Profile—juniper_CoS_template • Family Type—switching • Port Mode—trunk • Auto Negotiation—enabled • Flow Control—enabled • Maximum Size—no default provided • Speed—no default provided • Link Mode—no default provided • Port Security—enabled • MAC Limit—no default provided • MAC Limit Action—no default provided • Allowed MAC list—no default provided

Copyright © 2013, Juniper Networks, Inc.

Table 87: Port Profile Basic Settings for Data Center Ports *(continued)*

Field	Action
	FCoE Gateway service type has the following default settings: • Port Type—Ethernet Port • CoS Profile—juniper_DC_Hier_CoS • Family Type—switching • Port Mode—trunk • Filters—no default provided • VLAN Options—no default provided • DCBX Version—Auto • Disable DCBX—disabled • Disable Priority Flow Control—disabled • ETS No Auto Negotiation—disabled • Recommendation TVL—no default provided • Auto Negotiation—enabled • Flow Control—disabled • Maximum Size—2500 • Speed—no default provided • Link Mode—no default provided
	Fibre Channel Port service type has the following default settings: • Port Type—Fibre Channel Port • Speed—4Gbps • Buffer to Buffer State Change Number—no default provided • Loopback Setting—no default provided

Copyright © 2013, Juniper Networks, Inc.

Table 87: Port Profile Basic Settings for Data Center Ports *(continued)*

Field	Action
	FCoE Transit Port service type has the following default settings: • Port Type—Ethernet Port • CoS Profile—juniper_DC_Hier_CoS • Family Type—switching • Port Mode—trunk • Filters—no default provided • VLAN Options—no default provided • DCBX Version—Auto • Disable DCBX—disabled • Disable Priority Flow Control—disabled • ETS No Auto Negotiation—disabled • Recommendation TVL—no default provided • Auto Negotiation—enabled • Flow Control—disabled • Maximum Size—2500 • Speed—no default provided • Link Mode—no default provided • Port Security—enabled • Trust DHCP—disabled • FCoE Trusted—enabled • MAC Limit—no default provided • MAC Limit Action—no default provided • Allowed MAC List—no default provided
Port Type	If you selected the service type Custom, select the port type. If you selected a service type other than Custom, you cannot edit this field. Each port type has a different set of fields to configure. The options are **Ethernet Port** or **Fibre Channel Port**.

Table 88: Port Profile Settings for Data Center Ethernet Ports

Field	Action
CoS Profile	Click **Select** to choose from existing CoS profiles. The CoS configuration contained in the CoS profile will be applied to the interfaces that the Port profile is assigned to when you deploy the configuration. For QFX Series and QFabric devices, only a Hierarchical CoS profile is applicable. For EX4500 and EX4550 Series devices, only a Non Hierarchical CoS profile is applicable.
Port Family Options The available settings and defaults for these options depend on which Service Type you selected.	
Switching Routing	Select whether the interface operates as a Layer 2 (switching) or a Layer 3 (routing) interface. TIP: If you select routing, you configure an IP address on a per-interface basis when you assign the profile to individual interfaces.

Copyright © 2013, Juniper Networks, Inc.

Table 88: Port Profile Settings for Data Center Ethernet Ports *(continued)*

Field	Action
Port Mode	(Switching interfaces only) Select the port mode for the interface: • Access—Use for interfaces that connect to an end device, such as a desktop computer, an IP telephone, a wireless access point, a printer, or a security camera. The interface must belong to a single VLAN. Frames sent and received over the over the interface are untagged Ethernet frames. • Trunk—Use for interfaces that connect to a switch or router. Trunk interfaces can belong to more than one VLAN, enabling VLAN traffic to be multiplexed on a single physical interface. The Ethernet frames sent and received over the interface are tagged frames, in which IEEE 802.1Q tagging is used to segregate the traffic from each VLAN. • Tagged Access—Use for access interfaces where VLAN tagging is required, typically when the interface connects to a server running virtual machines using VEPA technology. The traffic generated by the server can contain an aggregation of VLAN packets from different virtual machines on that server, requiring that packets be tagged.
Authentication Profile	(Applicable to switching interfaces on EX4500 and EX4550 switches only) Select the Authentication profile for the interface from a list of existing profiles by clicking **Select**. By assigning an Authentication profile to the Port profile, you can enable 802.1X and captive portal authentication on interfaces. If you do not specify an Authentication profile, the interface is an open port and no authentication is required to connect. NOTE: You cannot configure 802.1X authentication on aggregated Ethernet interfaces. If you attempt to deploy a Port profile that contains an Authentication profile on an aggregated Ethernet interface, the deployment will fail.
Ingress Filter	Select an ingress Filter profile for the interface from a list of existing profiles by clicking **Select**.
Egress Filters	Select an egress Filter profile for the interface from a list of existing profiles by clicking **Select**.
VLAN Options Available VLAN options depend on the Service Type selected.	
VLAN Profile	(Access ports only) Select a VLAN profile for the interface from a list of existing profiles by clicking **Select**.
VLAN profile list	(Trunk and Tagged Access ports only) Select a set of VLAN profiles for the interface from a list of existing profiles by using the **Add** and **Remove** functions.
Native VLAN	(Trunk and Tagged Access ports only) Select a native VLAN profile for the interface from a list of existing profiles by clicking **Select**.
Voice VLAN	(Applicable to access ports on EX4500 and EX4550 switches only) Select a voice VLAN for the interface by clicking **Select**, selecting one of the listed profiles, and then clicking **OK**.
DCBX Settings Data Center Bridging Capability Exchange protocol is a discovery and exchange protocol for conveying configuration and capabilities among network neighbors to ensure consistent configuration across the network. It is an extension of the Link Layer Data Protocol (LLDP, described in IEEE 802.1AB). The defaults for these settings depend on which Service Type you selected.	

Copyright © 2013, Juniper Networks, Inc.

Table 88: Port Profile Settings for Data Center Ethernet Ports *(continued)*

Field	Action
DCBX Version	Select one of the following versions of the Data Center Bridging Capability Exchange protocol: • **Auto**—automatic configuration • **DCBX v1.01**—The Converged Enhanced Ethernet (CEE) version of DCBX. It has a subtype of 2 and an IEEE DCBX Organizationally Unique Identifier (OUI) of 0x001b21. • **IEEE DCBX**—The newest DCBX version. Different TLVs have different subtypes (for example, the subtype for the ETS configuration TLV is 9); the OUI is 0x0080c2.
Disable DCBX	Select this option to turn off Data Center Bridging Capability Exchange protocol.
Disable Priority Flow Control	Select this option to turn off priority flow control. Priority-based flow control (PFC) is a link-level flow control mechanism defined by IEEE 802.1Qbb that enables independent flow control for each class of service (as defined in the 3-bit CoS field of the Ethernet header by IEEE 802.1Q tags) to ensure that no frame loss from congestion occurs in DCB networks.
ETS No Auto Negotiation	Select this option to turn off ETS auto-negotiation. Enhanced transmission selection (ETS) is a mechanism that provides finer granularity of bandwidth management within a link.
Recommendation TLV	Select either Enable TLV or Disable TLV. The enhanced transmission selection (ETS) Recommendation TLV communicates the ETS settings that the switch wants the connected peer interface to use. If the peer interface is "willing," the peer interface changes its configuration to match the configuration in the ETS Recommendation TLV. By default, the switch interfaces send the ETS Recommendation TLV to the peer. The settings communicated are the egress ETS settings defined by configuring hierarchical scheduling on the interface.
Advanced Settings	Click to set advanced settings. See Table 89 on page 312 for information about the advanced settings.

Table 89: Port Profile Advanced Settings for Data Center Ethernet Ports

Field	Action
Link Settings Options The defaults for these settings depend on which Service Type you selected.	
Enable Auto Negotiation	Select to enable autonegotiation of link speed and duplex mode; clear to disable autonegotiation. If you disable autonegotiation, you must set link speed and link mode. You cannot disable autonegotiation if a link speed of 1 Gbps is configured. This configuration might be accepted, but autonegotiation will not be disabled. NOTE: This setting is ignored when you assign a Port profile to an Aggregated Ethernet interface.

Copyright © 2013, Juniper Networks, Inc.

Table 89: Port Profile Advanced Settings for Data Center Ethernet Ports *(continued)*

Field	Action
Enable Flow Control	Select to enable flow control on the interface, which permits the switch suspend packet transmission for a set period of time in response to a PAUSE frame sent by a congested switch. Flow control applies only to links operating in 1 Gbps, full-duplex mode.
Maximum Size (bytes)	Type the maximum transmission unit (MTU), which is the maximum size of Ethernet frames sent by the interface. To calculate the MTU, add 14 bytes overhead to the maximum payload you want sent. Range: 256 through 9216 bytes
Speed	Select the link speed. If you select a link speed when autonegotiation is enabled, autonegotiation remains enabled and the interface will advertise the link speed that you specify as its maximum link speed. NOTE: This setting is ignored when you assign a Port profile to an Aggregated Ethernet interface.
Link Mode	Select the duplex mode. Select **Automatic** to enable autonegotiation when autonegotiation is enabled. NOTE: This setting is ignored when you assign a Port profile to an Aggregated Ethernet interface. You cannot select Half Duplex when link speed Autonegotiation or 1 Gbps.
Port Security Options (Switching Interfaces Only) The defaults for these settings depend on which Service Type you selected.	
Port Security	Select to enable port security; clear to disable port security. When port security is enabled, you can configure port security options on an interface, such as learned MAC address limits. When port security is disabled, no port security is applied to the interface, including the default port security options.
Trust DHCP	Select to permit messages from a DHCP server to be received on the interface. Clear to block all messages from a DHCP server from being received on the interface. TIP: For this port security feature to work, DHCP snooping must be enabled on the VLAN the interface belongs to. You can enable DHCP snooping on the VLAN in the VLAN profile.
FCoE Trusted	Select to configure the interface to trust Fibre Channel over Ethernet (FCoE) traffic. If an interface is connected to another switch such as an FCoE forwarder (FCF) or a transit switch, you can configure the interface as trusted so that the interface forwards FCoE traffic from the switch to the FCoE devices without installing FIP snooping filters.

Copyright © 2013, Juniper Networks, Inc.

Table 89: Port Profile Advanced Settings for Data Center Ethernet Ports *(continued)*

Field	Action
MAC Limit	Type the number of MAC address that can be dynamically learned on the interface. This setting is disabled if the port is set to Trunk mode. NOTE: This setting is required when you enable port security. Range: 1 through 163839
MAC Limit Action	Select the actions to be taken if the MAC address limit is exceeded. This setting is disabled if the port is set to Trunk mode. • Drop—Drop any packet with a previously unlearned MAC address and generate a system log entry, and SNMP trap, or an alarm. • Log—Accept packets with new MAC addresses and learn the addresses, but generate a system log entry, and SNMP trap, or an alarm. • Shutdown—Shut down the interface and generate a system log message, SNMP trap, or an alarm. If an interface is shut down because the MAC address limit has been exceeded, you must use the CLI command **clear ethernet-switching port-error interface *name*** to clear the error and bring the interface back into service. TIP: You can use the CLI to configure auto recovery on an interface that has been shutdown by a MAC limit error. • None—No action. This selection effectively disables MAC address limiting on the interface.
Allowed MAC List	Enter the MAC addresses of devices that are allowed access to the interface in the Allowed MAC List. Any device whose MAC address does not match an address in the list will not be allowed access to the interface. A list with no entries means that a client with any MAC address is permitted to access the interface. This setting is disabled if the port is set to Trunk mode. To enter a MAC address, click **Add** and type the MAC addresses in the field provided. Enter MAC addresses as two-character hexadecimal numbers separated by colons. Click **Save** to save the entry. NOTE: Configuring an allowed MAC address list does not block the switch from receiving Layer 2 control packets—such as Link Layer Discovery Protocol (LLDP) packets—transmitted from MAC addresses that are not specified in the address list. Control packets do not undergo the MAC address check. However, the switch does not forward them to another destination.

Table 90: Port Profile Settings for Data Center FC Ports

Field	Action
Profile Name	Type the name of profile, using up to 64 alphanumeric characters and no special characters other than an underscore. The name must be unique among Port profiles.

Copyright © 2013, Juniper Networks, Inc.

Table 90: Port Profile Settings for Data Center FC Ports *(continued)*

Field	Action
Description	Type a description of the port profile, which will appear on Manage Port Profiles page. You can use up to 256 characters.
Port Type	Select **Fibre Channel Port**. The remaining settings change to fibre channel settings.
Fibre Channel Settings	
Speed	Select the FC speed, **Auto** (default), 2Gbps, 4Gbps, or 8Gbps.
Buffer to Buffer State Change Number	Configure the buffer-to-buffer credit state change number to prevent the permanent loss of Fibre Channel credits over time (buffer-to-buffer credit recovery). Select a number from 0 through 15.
Loopback Setting	Select **Loopback** to configure an FC loopback interface.

What to Do Next

After you create a Port profile, you can assign it to interfaces or members of port groups. During this process, you can also configure interface-specific attributes, such as IP address, and certain device-specific attributes, such as which Access profile to use for all ports on the device. For more information, see "Assigning a Port Profile to Interfaces" on page 383.

Related Documentation

- Understanding Port Profiles on page 36
- Assigning a Port Profile to Interfaces on page 383
- *Creating and Managing Port Groups*
- Creating and Managing VLAN Profiles on page 330
- Creating and Managing Authentication Profiles on page 157
- Creating and Managing CoS Profiles on page 184
- Assigning a Port Profile to Interfaces on page 383

Creating and Managing a Radio Profile

Radio profiles control aspects of radio behavior for radios in a WLAN. A radio can have only one profile at a time. Use the Network Director Radio profile wizard to both create a Radio profile and link it to existing WLAN Service profiles (SSIDs). For more information about the aspects and parameters of a radio file, see "Understanding Radio Profiles" on page 42.

Radio profiles can be used by multiple WLAN Service profiles, so you really only need to create one Radio profile for wireless operation. However, there are a number of reasons to create multiple Radio profiles:

Copyright © 2013, Juniper Networks, Inc.

- For best network performance, use separate Radio profiles for transmissions using long and short guard intervals. The guard interval is the space between symbols (characters) being transmitted—it eliminates intersymbol interference. In normal 802.11 operation, the guard interval is 800 ns. In 802.11n operation, short guard intervals of 400 ns are supported. Shorter guard interval between symbols increases throughput. Guard intervals are configured in WLAN Service profiles.
- For best network performance, use separate Radio profiles for voice and data traffic because network issues such as packet loss, latency, and jitter affect VoIP much more than they affect data. With separate profiles, you can optimize settings for data in one profile and VoIP in another profile that includes call admission control and user idle timeout. These parameters are configured in Radio profiles.
- When all radios are using one channel, that channel becomes crowded. Channel use is determined in Radio profiles.
- 802.11n devices cannot perform at optimum speed when a radio also services slower 802.11b/g devices. Separate Radio profiles should be used for 802.11n and 802.11b/g devices.

Once a Radio profile is completed, the next step is to assign the profile to radios.

This topic describes:

- Managing Radio Profiles on page 316
- Before You Create a Radio Profile on page 317
- Creating a Radio Profile on page 318
- Specifying Radio Profile Basic Settings on page 319
- Specifying the Power & RF Settings on page 321
- Specifying Radio Profile Radio Options on page 322
- Reviewing the Radio Profile Configuration on page 325
- What To Do Next on page 325

Managing Radio Profiles

From the Manage Radio Profiles page, you can:

- Create a new Radio profile by clicking **Add**. For details, see "Creating a Radio Profile" on page 318.
- Modify an existing profile by selecting it and clicking **Edit**.
- Assign the Radio profile to radios by selecting a Radio profile, and clicking **Assign**. For directions, see "Assigning a Radio Profile to Radios" on page 389.
- Change Radio profile assignments by selecting a Radio profile, and clicking **Edit Assignment**.
- View information about a profile by selecting a Radio profile and clicking **Details**.
- Delete profiles by selecting a Radio profile and clicking **Delete**.

Copyright © 2013, Juniper Networks, Inc.

TIP: You cannot delete profiles that are in use—that is, assigned to objects or used by other profiles. To see the current assignments for a profile, select the profile and click **Details**.

- Clone a profile by selecting a profile and clicking **Clone**.

Table 91 on page 317 describes the information provided about Radio profiles on the Manage Radio Profiles page. This page lists all Radio profiles defined for your network, regardless of your current selected scope in the network view.

Table 91: Radio Profile Fields

Field	Description
Profile Name	Name given to the profile when the profile was created.
Device Family	Wireless controllers (WLC)
Description	Up to 256 alphanumeric characters, provided when the profile was created, including spaces and special characters.
Spectral Scan	Indicates whether spectral scanning is Enabled or Disabled. For more information, about scanning see "Understanding Wireless Scanning" on page 117.
WLAN Service Profiles	Lists associated WLAN Service profiles. For more information, about WLAN Service profiles, see "Understanding WLAN Service Profiles" on page 52.
Assignment State	A Radio profile can be Deployed on a controller, Unassigned, or Pending Deployment. For deployment directions, see *Deploying Configuration to Devices*.
Creation Time	Date and time when this profile was created.
Update Time	Date and time when this profile was last modified.
User Name	The username of the user who created or modified the profile.

TIP: All columns may not be currently displayed. To show or hide fields in the table, click the down arrow on the field header, select **Columns**, and select or clear the check box adjacent to the field that you want to show or hide.

Before You Create a Radio Profile

You need at least one WLAN Service profile to create a Radio profile—they are mapped during configuration of the Radio profile.

Copyright © 2013, Juniper Networks, Inc.

NOTE: If your wireless network does not include at least one WLAN Service profile, stop now and follow the directions "Creating and Managing a WLAN Service Profile" on page 350.

Creating a Radio Profile

Radio profiles provide a set of radio parameters that can be applied to multiple radios. At minimum, you must:

- Specify a unique Radio profile name.
- Link at least one WLAN Service profile to the Radio profile.

You can optionally include additional radio configuration such as:

- Enable dynamic frequency selection (DFS) channels to meet regulatory requirements.
- Enable RFID to track tags such as inventory tags.
- Enable unscheduled automatic power save delivery (UAPSD) to accommodate clients using power save mode for batteries. For a description of power save, see "Understanding WMM Power Save and WLAN Client Battery Life" on page 121.
- Specify when automatic countermeasures are to be used, never (**None**), in **All cases**, or only for **Rogue devices**. Note that configuring the countermeasures is not supported in Network Director.
- Limit client power for devices using this Radio profile so that access points and clients use the same transmit power.
- Specify an 802.11n channel width—the 802.11n channel is the only channel that can be either 20 MHz or 40 MHz. For more information, see "Understanding Wireless Radio Channels" on page 114.
- Configure automatic channel tuning and automatic power tuning settings. For more information about automatic channel tuning, see "Understanding Channel Auto-Tuning and Adaptive Channel Planner on Wireless Networks" on page 86. For more information about automatic power tuning, see "Understanding Automatic Power Tuning for Wireless Radios" on page 91.
- Select an RF scanning method (either active or passive) and provide settings such as scanning scope, clear-to send signals (CTS-to-self), and spectral scanning. For more information about scanning, see "Understanding Wireless Scanning" on page 117.
- Select a QoS mode for prioritizing traffic, either WMM or legacy SVP and provide the corresponding configuration.

NOTE: SVP is a legacy technology—Spectralink's new phones use WMM.

- Change 802.11 attributes such the beacon interval, DTIM interval, maximum amount of time an outbound frame is held in buffer storage, and maximum amount of time an

Copyright © 2013, Juniper Networks, Inc.

inbound frame is held in buffer storage. See "Understanding the IEEE 802.11 Standard for Wireless Networks" on page 100.

To create a Radio profile:

1. Click in the Network Director banner.
2. Under Select View, select either **Logical View**, **Location View**, **Device View** or **Custom Group** View.

   TIP: **Do not select Virtual View or Topology View.**
3. Click **Radio** under Profile and Configuration Management in the Tasks pane.

   The Manage Radio Profiles page opens, displaying the list of currently configured Radio profiles.
4. Click **Add**.

   The Create Radio Profile for Wireless Controllers (WLC) wizard opens. It consists of four sections, Basic Settings, Power & RF Settings, Radio Options, and Review.
5. Complete the Create a Radio Profile for Wireless Controllers (WLC) wizard pages as described in both online help (click **Help**) and the directions "Specifying Radio Profile Basic Settings" on page 319, "Specifying the Power & RF Settings" on page 321, "Managing Radio Profiles" on page 316, and "Reviewing the Radio Profile Configuration" on page 325.
6. Click **Review** and check your settings. If you need to change a setting click **Edit** in the corresponding section, make changes, and then return to the Review tab.
7. Click **Finish**.

   The Radio profile appears in the list on the screen. You can now assign this profile to radios by following the directions "Assigning a Radio Profile to Radios" on page 389.

Specifying Radio Profile Basic Settings

Basic radio settings include a Radio profile name (required) and options to enable DFS, RFID, UAPSD, countermeasures, and client power constraint. In addition, this is where 40 MHz channel width for 802.11n is configured and WLAN Service profiles are mapped to the Radio profile.

Enter the settings described in Table 92 on page 319. Required settings are indicated by a red asterisk (*) that appears next to the field label in the user interface.

Table 92: Radio Profile Basic Settings

Field	Action
Name	Type a unique name that identifies the Radio profile. You can use up to 32 characters and the special underscore character _ No other special characters are allowed.

Copyright © 2013, Juniper Networks, Inc.

Table 92: Radio Profile Basic Settings *(continued)*

Field	Action
Description	Range: 0 through 256 alphanumeric characters, including spaces and special characters.
DFS Channel (default is disabled)	Select **Enable** to enable dynamic frequency selection (DFS) channels to meet regulatory requirements as assigned by the access point country code.
RFID (default is disabled)	Select **Enable** to enable tracking of mobile assets using RFID tags.
U-APSD (default is disabled)	Select **Enable** to enable Unscheduled automatic power save delivery (U-APSD), which buffers unicast packets on access points until clients request transmission. There are two methods for requesting buffered unicast packets from access point radios, either the Wi-Fi Multimedia (WMM) method (default) or the Spectralink Voice Priority (SVP) method. NOTE: Only clients using power save mode are affected by this setting.
Countermeasures (default is None)	Select which clients receive countermeasures, **None**, **All** or **Rogue** (only rogue devices). Countermeasures are packets sent by a radio to mitigate interfering devices. NOTE: Configuring the actual countermeasure actions is not supported in Network Director.
Client TX Power Constraint (default is None)	Select **Link Balance** to balance power between access points and clients on all client links. To accomplish this, access points transmit the maximum power setting to potential clients. You might want to limit client power in places like auditoriums, airports, and dorms where there are a high number of clients.
802.11n Attributes	
Channel Width (default is 40 MHz)	Select the radio channel width for 802.11n clients using the 5-GHz band, either **20 MHz** or **40 MHz**.
WLAN Service Profiles	
WLAN Service Profiles (no default)	Click **Add** and then select any or all listed WLAN Service profiles to associate with this Radio profile—all WLAN Service profiles are all listed here. Clients using the SSID named in the WLAN Service profile(s) will use this Radio profile. NOTE: WLAN profiles must be created previously. Also, you can associate multiple WLAN Service profiles to a Radio profile.

To configure power and RF settings, click either **Next** or click **Power & RF Settings** at the top of the wizard window. For directions to complete that section, see "Specifying the Power & RF Settings" on page 321.

Copyright © 2013, Juniper Networks, Inc.

Specifying the Power & RF Settings

To configure the radio power and RF settings, enter the settings described in Table 93 on page 321. All settings are optional.

Table 93: Radio Power & RF Settings

Field	Action
Auto Tune Settings	
Tune Channel (default is enabled)	To disable channel auto-tuning, remove the check mark from **Enable**. Auto-tuning automatically changes access point radio channels if other devices interfere on the current channel, or if the current channel is overloaded. For more information, see "Understanding Channel Auto-Tuning and Adaptive Channel Planner on Wireless Networks" on page 86. NOTE: Tune Channel must be enabled for DFS to operate.
Tune Transmit Power (default is disabled)	Click **Enable** to enable automatic power tuning for radios. Access point radios are initially set to maximum power for the country's regulatory domain. Radios maintain maximum power, which is recommended, unless a conflict or other event causes them to change. For more information, see "Understanding Automatic Power Tuning for Wireless Radios" on page 91.
Ignore Clients (default is disabled)	If Tune Channel is enabled, you can click **Enable** to change channels even when clients are connected to the original channel. Clients must then reconnect to the new channel.
Tune Channel Range (11a) (default is Lower_Bands)	When Tune Channel is enabled, change this option to limit 802.11a channel selection. Select **Lower_Bands** to limit channel selection to the lower eight 802.11a bands (36, 40, 44, 48, 52, 56, 60, or 64). Select **All_Bands** to allow channel selection from all 802.11a channels (36, 40, 44, 48, 52, 60, 64, 149, 153, 157, or 161).
Channel Tuning Interval (default is 3600 seconds)	When Tune Channel is enabled, select the number of seconds (0 - 65535) between channel reevaluations. Setting channel tuning interval to 0 means that reevaluation only takes place if anomalies occur. We recommend an interval of at least 300 seconds to provide network stability by preventing the radio from changing channels too rapidly.
Channel Tuning Holddown (default is 900 seconds)	When Tune Channel is enabled, select the minimum number of seconds (0 to 65535) a radio must remain at its current channel assignment before channel auto-tuning can change the channel. The channel holddown provides additional stability to the network by preventing the radio from changing channels too rapidly in response to anomalies such as short-duration channel interference.

Copyright © 2013, Juniper Networks, Inc.

Table 93: Radio Power & RF Settings *(continued)*

TX Power Backoff Timer (default is 10 seconds)	When Tune Transmit Power is enabled, optionally change the interval at which radios reduce power after temporarily increasing the power to maintain the minimum data rate for an associated client. At the end of each power-backoff interval, radios that temporarily increased their power reduce it by 1 dBm every 10 seconds. The power backoff continues in 1 dBm increments after each interval until the power returns to expected setting.
Power Tuning Interval (default is 600 seconds)	When Tune Transmit Power is enabled, optionally change the number of seconds between reevaluations of power. Power changes only take place after an evaluation or when an anomaly occurs.
Power Ramp Interval (default is 60 seconds)	When Tune Transmit Power determines that a change in power is required, that change takes place at 1 dBm per power ramp interval. The power ramp interval is the interval at which power is increased or decreased, in 1 dBm increments, on radios until the optimum power level calculated by automatic tuning is reached. After each power ramp interval, the radio increases or decreases the power by another 1 dB until the radio reaches the power level selected by automatic tuning.
RF Scanning Settings	
Mode (default is active)	Select **Passive** to make scanning detect only active WLAN devices. (Passive scanning cannot be turned off.) Select **Active** to make scanning detect all wireless devices, even if they are not currently transmitting.
Channel Scope (default is regulatory)	Select the range of access point radio channels to be scanned and audited—**Regulatory** (channels required by country of operation), **All**, or **Operating** (active channels).
CTS-to-Self (default is disabled)	Select **Enable** to have access points send clear-to-send packets to themselves on the new channel before switching an access point radio to another channel. This action confirms that both the send and receive are working on the access point before it attempts communication with other devices.
Spectral Scan (default is disabled)	Select **Enable** to enable access points to scan their coverage area for all electronic devices, not just wireless devices.

To configure radio options for the Radio profile, click **Next** or click **Radio Options** at the top of the wizard window. For directions to complete that section, see "Specifying Radio Profile Radio Options" on page 322.

Specifying Radio Profile Radio Options

Radio options directly affect the radios that use this profile, configuring features like QoS mode, beacon interval, WMM configuration, and other communication settings. Enter the settings described in Table 94 on page 323.

Copyright © 2013, Juniper Networks, Inc.

Table 94: Radio Options

Field	Action
Voice Configuration	
QoS Mode (default is WMM)	Select **WMM** (default) quality of service mode to prioritize VoIP traffic, unless you are using Spectralink phones. In that case only, select **SVP**. In either case WMM CAC configurations apply to traffic. The only difference is that SVP also gets highest priority when SVP is selected. For more information, see "Understanding Call Admission Control" on page 93.
802.11 Attributes	
Beacon-Interval (default is 100)	Select the interval rate at which the radio advertises the associated SSID.
DTIM-Interval (default is 1)	Select the Delivery Traffic Indication Map (DTIM) interval, which is the number of times (1 - 31) after every beacon that a radio sends a delivery traffic indication map. Listen intervals are set on clients and DTIM intervals are set on the AP. We recommend that you set DTIM interval to be greater than clients' listen interval.
Maximum Received Lifetime (default is 2000 milliseconds)	Type the number of milliseconds that a frame received by a radio remains in the buffer memory.
Maximum Transmitted Lifetime (default is 2000 milliseconds)	Select the number of milliseconds that a frame scheduled to be transmitted by a radio can remain in buffer memory.
Long Preamble Length (default is short preamble length)	Select **Enable** to change the advertised preamble length from short to long—the default is short. In general, use the short preamble type in high network traffic areas, and use the long preamble to provide more reliable communication in noisy (high interference) networks. Also, all 802.11b devices must support the long preamble format, but might also optionally support the short preamble. Because the short preamble is default, if an 802.11b device is having trouble getting communicating with other 802.11b devices, try using the long preamble.
Rate Enforcement (default is disabled)	Select **Enable** to limit client connection to clients operating at mandatory or standard rates. Clients operating at any disabled rates cannot associate with radios using this profile.
RTS Threshold (default is 65535 bytes)	Select the request to send threshold value, which indicates the size at which packets are transmitted. A lower value means RTS packets are send more often, consuming bandwidth. A higher value means that a busy network can recover faster from interference.
Fragment Threshold (default is 2346 bytes)	Select the maximum frame size that MSS can send without fragmenting the packet—the default (2346) is rarely changed.

Copyright © 2013, Juniper Networks, Inc.

Table 94: Radio Options *(continued)*

Field	Action
WMM Call Admission Control (CAC) Configuration Sending (WMM) and Receiving (Policing) Packets provides levels of service that vary with the type of data sent on an access point. By default, access points deliver the same service to all packets—you must configure admission control for CAC to work properly. For more information, see "Understanding Call Admission Control" on page 93. NOTE: If Voice configuration QoS mode is set to SVP, SVP is also given highest priority and the CAC settings still apply.	
Background Admission Control (ACM) Background 0 ACM Mode (default is disabled) Background 0 ACM Limit (%) (default is zero) Background 0 ACM Policing (default is enabled)	Background has the longest fixed wait time before forwarding queued packets, giving it lowest priority. Select **Background 0 ACM Mode** to enable background admission control mode for downstream traffic. Type a value from 1 through 100 for the **Background 0 ACM Limit** to limit downstream background mode to a percentage of bandwidth. Select **Background 0 ACM Policing** to enable background mode for upstream traffic.
Best Effort Admission Control (ACM) Best Effort 1 ACM Mode (default is disabled) Best Effort 1 ACM Limit (%) (default is zero) Best Effort 1 ACM Policing (default is enabled)	Best effort provides QoS by providing more resources than are needed by the network. This simple method provides high quality service to all packets on an IP backbone and is therefore frequently used on the network core. Select **Best Effort 1 ACM Mode** to enable best-effort admission control mode for downstream traffic. Type a value from 1 through 100 for the **Best Effort 1 ACM Limit** to limit downstream best-effort mode to a percentage of bandwidth. Select **Best Effort 1 ACM Policing** to enable best-effort mode for upstream traffic.
Video Admission Control (ACM) Video 2 ACM Mode (default is disabled) Video 2 ACM Limit (%) (default is zero) Video 2 ACM Policing (default is enabled)	Video streaming has the shortest fixed wait time before forwarding queued packets, giving it highest priority. Select **Video 2 ACM Mode** to enable video admission control mode for downstream traffic. Type a value from 1 through 100 for the **Video 2 ACM Limit** to limit downstream video mode to a percentage of bandwidth. Select **Video 2 ACM Policing** to enable video mode for upstream traffic.

Copyright © 2013, Juniper Networks, Inc.

Table 94: Radio Options *(continued)*

Field	Action
Voice Admission Control (ACM) Voice 3 ACM Mode (default is disabled) Voice 3 ACM Limit (%) (default is zero) Voice 3 ACM Policing (default is enabled)	Voice transmission has the shortest fixed wait time before forwarding queued packets, giving it highest priority. Select **Voice 3 ACM Mode** to enable voice admission control mode for downstream traffic. Type a value from 1 through 100 for the **Voice 3 ACM Limit** to limit downstream voice mode to a percentage of bandwidth. Select **Voice 3 ACM Policing** to enable voice mode for upstream traffic.

NOTE: When SVP is selected instead of WMM, SVP voice transmission also has highest priority in addition to voice and video. The rest of the WMM QoS settings still apply. SVP is needed only for legacy equipment.

Click **Next** or click **Review** at the top of the wizard window. For directions to complete that section, see "Reviewing the Radio Profile Configuration" on page 325.

Reviewing the Radio Profile Configuration

Before you create the Radio profile, check the configuration:

1. Review your selections by scrolling to the bottom of the screen.
2. Make any needed changes by clicking **Edit** next to the appropriate section. Make the changes, and then return to the Review tab.
3. Click **Finish**.

   After you click Finish, the Create Profile Assignments Job Details window opens, which reports on the status of the profile assignment job. If you have assigned the profile to a large number of objects, the profile assignment job can take some time to complete. Instead of waiting for the Job Details window to report job completion status, you can close it and check the details of the profile assignment job at a later time using the Manage Job task in System mode.

   NOTE: If any assignment fails, the profile assignment job fails and none of the assignments are created. Check the details for the profile assignment job for reasons the assignment failed.

What To Do Next

Next, you assign this Radio profile to radios. For directions, see "Assigning a Radio Profile to Radios" on page 389.

Related Documentation

- *Understanding the Network Director User Interface*

Copyright © 2013, Juniper Networks, Inc.

- Creating and Managing a WLAN Service Profile on page 350
- Understanding WMM Power Save and WLAN Client Battery Life on page 121
- Understanding Channel Auto-Tuning and Adaptive Channel Planner on Wireless Networks on page 86
- Understanding Automatic Power Tuning for Wireless Radios on page 91
- Understanding the IEEE 802.11 Standard for Wireless Networks on page 100
- Creating a Radio Profile for Voice Clients Only on page 329
- *Deploying Configuration to Devices*

Creating and Managing RADIUS Profiles

Remote Authentication Dial In User Service (RADIUS) is a networking protocol that provides centralized authentication, authorization, and accounting (AAA) management for computers to connect and use a network service. By default, RADIUS servers are used for both accounting and authentication. From Network Director, you can create and manage RADIUS profiles that configure RADIUS server settings.

TIP: In addition to your RADIUS server, you can configure an LDAP server for either wireless and EX Series ELS switch authentication—for directions, see "Creating and Managing LDAP Profiles" on page 273.

This topic describes:

- Managing RADIUS Profiles on page 326
- Creating RADIUS Profiles on page 327
- Specifying Settings for a RADIUS profile on page 328
- What to Do Next on page 329

Managing RADIUS Profiles

From the Manage RADIUS Profiles page, you can:

- Create a new profile by clicking **Add**. For directions, see "Creating RADIUS Profiles" on page 327.
- Modify an existing profile by selecting it and clicking **Edit**.
- View information about a profile by selecting the group and clicking **Details** or by clicking the profile name.
- Delete profiles by selecting the profile and clicking **Delete**.

Copyright © 2013, Juniper Networks, Inc.

TIP: You cannot delete profiles that are in use—that is, assigned to objects or used by other profiles. To see the current assignments for a profile, select the profile and click **Details**.

- Clone a profile by selecting the profile and clicking **Clone**.

Table 95 on page 327 describes the information provided about RADIUS profiles on the Manage RADIUS Profiles page. This page lists all RADIUS profiles defined for your network, regardless of your current selected scope in the network view.

Table 95: RADIUS Profile Information

Field	Description
RADIUS Profile Name	Name given to the RADIUS profile when it was created.
Server Address	IP address of the RADIUS server.
Server Port	UDP port being used by the RADIUS server.
Creation Time	Date and time when this profile was created.
Update Time	Date and time when this profile was last modified.
User Name	The username of the user who created or modified the profile.

TIP: All columns may not be currently displayed. To show or hide fields in the table, click the down arrow on the field header, select **Columns**, and select or clear the check box adjacent to the field that you want to show or hide.

Creating RADIUS Profiles

To create a RADIUS profile:

1. Click Build in the Network Director banner.
2. Under Select View, select either **Logical View**, **Location View**, **Device View** or **Custom Group** View.

   TIP: Do not select **Virtual View** or **Topology View**.

3. Click **RADIUS** under Profile and Configuration Management in the Tasks pane.

   The Manage RADIUS Profiles page appears.

4. Click **Add**.

Copyright © 2013, Juniper Networks, Inc.

The Create RADIUS Profile page appears.

5. Enter settings for the RADIUS profile as described in "Specifying Settings for a RADIUS profile" on page 328.
6. Click **Done**.

Specifying Settings for a RADIUS profile

Use the Create RADIUS Profile page to define authentication, authorization, and accounting settings for a RADIUS server.

Table 96 on page 328 describes the RADIUS Profile settings.

Table 96: RADIUS Profile Settings

Field	Action
Server Name	Type a name for the server, using up to 64 alphanumeric characters and no special characters other than an underscore. The name must be unique among servers.
Server Address	Type the IP address of the RADIUS server.
Authentication Port (default is 1812)	Using the arrows, adjust the number of the UDP port to use for RADIUS authentication messages. The default UDP port is 1812, and the range is from 0 to 65535.
Secret	Provide a password for the RADIUS server.
Advanced Settings You can change the advanced settings for a RADIUS server, or you can use the default settings.	
Accounting Port (default is 1813)	Using the arrows, adjust the number of the UDP port to use for RADIUS accounting messages. The default UDP port is 1813, and the range is from 0 to 65535.
Retry Count (default is 3)	Using the arrows, adjust the retry count until it reflects the number of times Network Director retries connecting to the RADIUS server when the RADIUS server is unavailable.
Timeout (default is 5 seconds)	Using the arrows, adjust the timeout value. Timeout indicates how many seconds Network Director allows for RADIUS server connection before giving an unreachable error.
Server Priority (default is 1)	Enter a server priority to indicate the order in which RADIUS servers are accessed. Entering a one means that this server is checked first.

Click **OK** to add the RADIUS server to the EX Switching Access profile. You can add more RADIUS servers if needed.

The RADIUS server name appears in the list of RADIUS servers.

Copyright © 2013, Juniper Networks, Inc.

If you have multiple RADIUS servers, you can prioritize them in the Authentication Server Order section, using the arrows.

Click **Finish** to create the RADIUS server profile.

What to Do Next

Link the RADIUS server to an Access profile. For directions, see "Creating and Managing Access Profiles" on page 136.

Related Documentation

- Creating and Managing Access Profiles on page 136
- Creating and Managing LDAP Profiles on page 273
- Understanding Central Network Access With RADIUS and TACACS+ on page 46

Creating a Radio Profile for Voice Clients Only

Voice over IP has different requirements than data—for an explanation, see "Understanding Voice Clients and Voice Traffic" on page 105. If your network is supporting both wireless data clients and voice clients, we recommend that you have two radio profiles, one for data and one for voice—this topic describes wireless radio profiles for voice clients.

Before you begin:

- Create at least one WLAN profile optimized for voice—for directions, see "Configuring a Voice SSID with Network Director" on page 133 and "Creating a WLAN Service Profile Dedicated to Voice" on page 134.

To create a radio profile for voice and assign it to radios:

1. Click

in the Network Director banner.
2. Under Select View, select either **Logical View**, **Location View**, **Device View** or **Custom Group** View.

   TIP: **Do not select Virtual View or Topology View.**
3. Click **Radio** under Profile Management in the tasks pane.

   The **Manage Radio Profiles** page appears.
4. Click **Add**.

   The radio profile wizard opens at the Basic Settings tab.
5. Configure the radio profile, setting these options for voice traffic:
   - Do not use auto-tune
   - Scan for rogues on the 'operating' channel only.

Copyright © 2013, Juniper Networks, Inc.

- Configure the appropriate quality of service (QoS) method (WMM or Spectralink) for your phones.
- Enable U-APSD for optimum powersave.

6. Click **Review** and check your settings. If you need to change a setting click **Edit** in the corresponding section, make changes, and then return to the Review tab.
7. Click **Finish**.

   The radio profile appears in the list on the screen. You can now assign this profile to radios.
8. Select a radio profile, and then click **Assign**.
9. Select at least radio from the object list, and then click either **Profile Association** or **Next**.
10. Click **Review** and make any needed changes by clicking **Edit**. Return to the Review tab.
11. Click **Finish**.

    The radio profile assignment appears next to the AP or radios in the list.

Related Documentation

- Configuring a Voice SSID with Network Director on page 133
- Understanding Voice Clients and Voice Traffic on page 105
- Creating a WLAN Service Profile Dedicated to Voice on page 134
- Creating and Managing a Radio Profile on page 315
- Understanding Radio Profiles on page 42

Creating and Managing VLAN Profiles

You can create and manage VLAN profiles on switches, wireless LAN controllers, and QFX Series devices by using the Manage VLAN Profiles window. Each VLAN profile is specific to a device family. After you create a VLAN profile, you can assign the profile at port level, switch level, or controller level. You can also assign VLAN profiles to controller managed access points and cluster managed access points.

Use the Manage VLAN Profiles page to create new VLAN profiles and to manage existing VLAN profiles.

To display the Manage VLAN Profiles page: In Build mode, select **VLANs** from Profile and Configuration Management in the Tasks pane. The Manage VLAN Profiles page appears.

This topic describes:

- Managing VLAN Profiles on page 331
- Creating a VLAN Profile on page 332
- Specifying Basic EX Switching VLAN Settings on page 334
- Specifying Basic Wireless VLAN Settings on page 335

Copyright © 2013, Juniper Networks, Inc.

- Specifying Basic Campus Switching ELS VLAN Settings on page 335
- Specifying Basic VLAN Settings for Data Center Switching on page 337
- Specifying Advanced VLAN Profile Settings for EX Series Switches on page 338
- Specifying Advanced VLAN Profile Settings for Wireless VLANs on page 340
- Specifying Advanced VLAN Settings for a Campus Switching ELS Profile on page 344
- Specifying Advanced VLAN Profile Settings for Data Center Switching on page 346
- Reviewing and Saving the VLAN Profile Configuration on page 350
- What To Do Next on page 350

Managing VLAN Profiles

From the Manage VLAN Profiles page, you can:

- Create a new profile by clicking **Add**. For details, see "Creating a VLAN Profile" on page 332.
- Modify an existing profile by selecting a profile and clicking **Edit**.
- Assign a profile to a port, a switch, access point, or a controller by selecting a profile and clicking **Assign**.
- Modify an existing assignment of a profile by selecting the profile and clicking **Edit Assignment**.
- View information about a VLAN profile, including the interfaces it is associated with, by either clicking the profile name or by selecting the profile and clicking **Details**.
- Delete profiles by selecting the profiles and clicking **Delete**.

TIP: You cannot delete profiles that are in use—that is, assigned to objects or being used by other profiles. To see the current assignments for a profile, select the profile, click **Details**, and then click the Assigned Objects Tab in the Details window.

- Clone a VLAN profile by selecting a profile and clicking **Clone**.

Table 97 on page 331 describes the fields in the Manage VLAN Profiles page. This page lists all VLAN profiles defined for your network.

Table 97: Manage VLAN Profile Fields

Field	Description
Profile Name	Name given to the profile when the profile was created.
VLAN Name	Name given to the VLAN when the VLAN profile was created.
Family Type	The device family; an EX Series switch, wireless LAN controller (WLC), Campus Switching ELS, or Data Center Switching.

Copyright © 2013, Juniper Networks, Inc.

Table 97: Manage VLAN Profile Fields *(continued)*

Field	Description
VLAN ID	VLAN ID assigned when the profile was created.
VLAN Range	Range of VLAN IDs assigned when the profile was created. TIP: If a VLAN ID is displayed, VLAN range will be null. Also, Campus Switching ELS supports a VLAN ID range only as part of a VLAN ID list.
VLAN ID List	VLAN IDs can be either individually listed (with a space to separate each ID), an inclusive list separating the starting VLAN ID and ending VLAN ID with a hyphen, or a combination of both. TIP: If a VLAN ID is displayed, VLAN range will be null. Also, this column will never have a value for EX Switching because it is not available.
Description	Description of the VLAN profile entered when the profile was created.
Assignment State	Displays the assignment state of the profile. A profile can be: • Unassigned—When the profile is not assigned to any object • Deployed—When the profile is assigned and is deployed from the Deploy mode • Pending Deployment—When the profile is assigned, but not yet deployed in the network.
Creation Time	Date and time when this profile was created.
Update Time	Date and time when this profile was last modified.
User Name	The username of the user who created or modified the profile.

TIP: All columns might not be displayed. To show or hide fields listed in the Manage Authorization Profiles table, click the down arrow on the field header, select Columns, and select or clear the check box adjacent to the field that you want to show or hide.

Creating a VLAN Profile

To create a VLAN profile, at minimum, you must specify the VLAN name and the IEEE 802.1Q VLAN tag for the profile. You also must indicate a device family for the VLAN: EX Series Switches, Wireless (WLC), Campus Switching ELS, or Data Center Switching.

In the VLAN, you can specify additional VLAN profile configuration such as:

- Ingress or egress filters to be used on the VLAN
- Parameters for handling the MAC forwarding table

Copyright © 2013, Juniper Networks, Inc.

To create a VLAN profile:

1. Click in the Network Director banner.
2. Under Select View, select either **Logical View**, **Location View**, **Device View** or **Custom Group** View.

   TIP: **Do not select Virtual View or Topology View.**

3. Click **VLAN** under Profile and Configuration Management in the Tasks pane.

   The Manage VLAN Profiles page appears, displaying the list of currently configured VLAN profiles.

4. Click **Add**.

   The Device Family Chooser window opens.

5. From the Device Family Chooser, select the device family for which you want to create a profile. The available device families are **Switching (EX)**, **Wireless (WLC)**, **Campus Switching ELS**, and **Data Center Switching Non ELS**.
6. Click **OK**.

   The Create VLAN Profile wizard for the selected device family is displayed. It consists of three sections, Basic Settings, Advanced Settings, and Review.

7. Specify the basic settings by using the appropriate Basic Settings wizard:
   - Specifying Basic EX Switching VLAN Settings on page 334
   - Specifying Basic Wireless VLAN Settings on page 335
   - Specifying Basic Campus Switching ELS VLAN Settings on page 335
   - Specifying Basic VLAN Settings for Data Center Switching on page 337
8. When you have completed the basic settings, click **Next** or click **Advanced Settings** at the top of the wizard window.
9. Specify the advanced settings. Complete the Advanced Settings options as described in:
   - "Specifying Advanced VLAN Profile Settings for EX Series Switches" on page 338 for EX Series switches.
   - "Specifying Advanced VLAN Profile Settings for Wireless VLANs" on page 340 for wireless LAN controllers.
   - "Specifying Advanced VLAN Settings for a Campus Switching ELS Profile" on page 344 for Campus Switching ELS.
   - "Specifying Advanced VLAN Profile Settings for Data Center Switching" on page 346 for Data Center Switching.
10. When you have completed the advanced settings, click **Next** or click **Review** at the top of the wizard window.

Copyright © 2013, Juniper Networks, Inc.

11. You can make changes to your profile from the **Review** page. Click **Save** > **Finish** to save the profile. For details, see "Reviewing and Saving the VLAN Profile Configuration" on page 350.

12. Click **Finish**.

    The system saves the VLAN profile and displays the Manage VLAN Profiles page. Your new or modified VLAN profile is listed in the table of VLAN profiles.

Specifying Basic EX Switching VLAN Settings

To configure the basic settings for an EX Switching VLAN profile, enter the settings described in Table 98 on page 334. Required settings are indicated by a red asterisk (*) that appears next to the field label.

Table 98: VLAN Profile Basic Settings for EX Switching

Field	Action
Profile Name	Type a name for the profile. The name can be up to 64 for EX Series switches and up to 32 for wireless devices alphanumeric characters with an underscore (_) to separate the words. For example: **vlan_profile_ex**
VLAN Name	Type the name of VLAN. The profile name and the VLAN name can be the same or different.
Description	Type a description to identify the group or function the VLAN will be part of. The character limit is 256 characters.
VLAN ID You can indicate a single VLAN ID or a VLAN Range for EX Switching.	
Single VLAN ID	To specify a single VLAN ID, type the single unique IEEE 802.1Q identifier for the VLAN (VLAN tag). The range for VLAN IDs is 1 through 4094.
Range of VLAN IDs	To indicate a range of VLAN IDs for EX Series switches, follow these steps: 1. Select **Range** instead of Single in the VLAN ID section. 2. Provide the first and last VLAN IDs in the range. TIP: For example, if you enter 10 and 12, when you deploy the profile on a device, three VLANs are created with VLAN IDs 10, 11, and 12. The names of the VLANs are created from the name you specified by adding the VLAN ID as a suffix to the name, for example **vlanname_10**.

Click **Next** or click **Advanced Settings** at the top of the wizard window to configure advanced VLAN EX Switching profile settings. Advanced Settings are described in "Specifying Advanced VLAN Profile Settings for EX Series Switches" on page 338.

Copyright © 2013, Juniper Networks, Inc.

Specifying Basic Wireless VLAN Settings

To configure the basic settings for a wireless VLAN profile, enter the settings described in Table 99 on page 335. Required settings are indicated by a red asterisk (*) that appears next to the field label.

Table 99: VLAN Wireless Profile Basic Settings

Field	Action
Profile Name	Type a name for the profile. The name can be up to 64 for EX Series switches and up to 32 for wireless devices alphanumeric characters with an underscore (_) to separate the words. For example: **vlan_profile_wlc**
VLAN Name	Type the name of VLAN. The profile name and the VLAN name can be the same or different.
Description	Type a description to identify the group or function the VLAN will be part of. The character limit is 256 characters.
VLAN ID	
Single VLAN ID	Type a single unique IEEE 802.1Q identifier for the VLAN (VLAN tag). The range for VLAN IDs is 1 through 4094.

Click **Next** or click **Advanced Settings** at the top of the wizard window to configure advanced wireless VLAN profile settings. Wireless Advanced Settings are described in "Specifying Advanced VLAN Profile Settings for Wireless VLANs" on page 340.

Specifying Basic Campus Switching ELS VLAN Settings

To configure the basic settings for a Campus Switching ELS VLAN profile, enter the settings described in Table 100 on page 335. Required settings are indicated by a red asterisk (*) that appears next to the field label.

Table 100: VLAN Profile Basic Settings for Campus Switching ELS

Field	Action
Profile Name	Type a name for the profile. The name can consist of up to 64 characters with an underscore (_) to separate the words. For example: **vlan_profile_els**
VLAN Name	Type the name of VLAN. The profile name and the VLAN name can be the same or be different.
Description	Type a description to identify the group or function of the VLAN. The character limit is 256 characters.

Copyright © 2013, Juniper Networks, Inc.

Table 100: VLAN Profile Basic Settings for Campus Switching ELS *(continued)*

Field	Action
VLAN ID NOTE: Campus Switching ELS supports a VLAN ID range only as part of a VLAN ID list. Follow the directions for adding a list of VLAN IDs if you are adding a VLAN range.	
Single VLAN ID	To specify a single VLAN ID (default), type the single unique IEEE 802.1Q identifier for the VLAN—the VLAN tag. The range for VLAN IDs is 1 through 4094.
List of VLAN IDs	To create a list of VLAN IDs for switches, follow these steps: 1. Select **List** instead of Single in the VLAN ID section. 2. Click **Add** under VLAN IDs. The Add VLAN Details window opens. 3. To add a single VLAN ID to the list, type the VLAN ID and then click either **Add** which closes this window or **Add More** which allows you to continue adding to the list. 4. To add a range of VLAN IDs to this list: a. In the Add VLAN Details window, select **Range** to add VLAN IDs in the range format 1 - 3. b. In the Add VLAN Details window, provide the first and last VLAN IDs in the range. TIP: For example, if you enter 10 and 12, when you deploy the profile on a device, three VLANs are created with VLAN IDs 10, 11, and 12. The names of the VLANs are created from the name you specified by adding the VLAN ID as a suffix to the name, for example **vlanname_10**. c. Click either **Add** which closes this window or **Add More** which allows you to continue adding to the list. 5. When you are finished creating the list, click .
Ethernet VLAN and FCoE VLAN (applies to Data Center Switching only)	Select the type of VLAN, either **Ethernet** or Fibre Channel Over Ethernet (**FCoE**).

Click **Next** or click **Advanced Settings** at the top of the wizard window to configure advanced VLAN profile settings. Advanced Setting are described in these sections:

- "Specifying Advanced VLAN Profile Settings for EX Series Switches" on page 338 for EX Series switches
- "Specifying Advanced VLAN Profile Settings for Wireless VLANs" on page 340 for wireless LAN controllers

Copyright © 2013, Juniper Networks, Inc.

- "Specifying Advanced VLAN Settings for a Campus Switching ELS Profile" on page 344 for Campus Switching ELS
- "Specifying Advanced VLAN Profile Settings for Data Center Switching" on page 346 for Data Center Switching.

Specifying Basic VLAN Settings for Data Center Switching

To configure the basic settings for a data center switching VLAN profile, enter the settings described in Table 101 on page 337. Required settings are indicated by a red asterisk (*) that appears next to the field label.

Table 101: VLAN Profile Basic Settings

Field	Action
Profile Name	Type a name for the profile. The name can be up to 64 for EX Series switches and up to 32 for wireless devices alphanumeric characters with an underscore (_) to separate the words. For example: **vlan_profile_wlc**
VLAN Name	Type the name of VLAN. The profile name and the VLAN name can be the same or different.
Description	Type a description to identify the group or function the VLAN will be part of. The character limit is 256 characters.
VLAN Type	Select the type of VLAN, either **Ethernet** or Fibre Channel Over Ethernet (**FCoE**).
VLAN ID You can always indicate a single VLAN ID. You can specify a VLAN List or VLAN Range for some products. The VLAN List or VLAN Range options are listed when they apply to the VLAN profile.	
Single VLAN ID	To specify a single VLAN ID, type the single unique IEEE 802.1Q identifier for the VLAN (VLAN tag). The range for VLAN IDs is 1 through 4094.

Copyright © 2013, Juniper Networks, Inc.

Table 101: VLAN Profile Basic Settings *(continued)*

Field	Action
Range of VLAN IDs	To indicate a range of VLAN IDs for switches, follow these steps: 1. Select **List** instead of Single in the VLAN ID section. 2. Click **Add** under VLAN IDs. The Add VLAN Details window opens. 3. In the Add VLAN Details window, select **Range** instead of Single. 4. In the Add VLAN Details window, provide the first and last VLAN IDs in the range. TIP: For example, if you enter 10 and 12, when you deploy the profile on a device, three VLANs are created with VLAN IDs 10, 11, and 12. The names of the VLANs are created from the name you specified by adding the VLAN ID as a suffix to the name, for example **vlanname_10**. 5. In the Add VLAN Details window, click **Add**. The Add VLAN Details window closes and the VLANs are added to the VLAN IDs list.

Click **Next** or click **Advanced Settings** at the top of the wizard window to configure advanced VLAN profile settings. Advanced Setting are described in these sections:

- "Specifying Advanced VLAN Profile Settings for EX Series Switches" on page 338 for EX Series switches.
- "Specifying Advanced VLAN Profile Settings for Wireless VLANs" on page 340 for wireless LAN controllers.
- "Specifying Advanced VLAN Settings for a Campus Switching ELS Profile" on page 344 for Campus Switching ELS.
- "Specifying Advanced VLAN Profile Settings for Data Center Switching" on page 346 for Data Center Switching.

Specifying Advanced VLAN Profile Settings for EX Series Switches

To configure the EX Switching advanced settings for the VLAN profile, enter the MAC parameters and Layer 2 filters described in Table 102 on page 338 for EX Series switching. All settings are optional.

Table 102: VLAN Profile Advanced Settings for an EX Series Switch

EX Switching MAC Parameters	
MAC Limit	Type the number of dynamic MAC addresses that can be learned on the VLAN. If this number is exceeded, packets containing new MAC addresses are dropped and an alarm is raised. Setting a limit on the number of dynamic MAC addresses protects against an Ethernet switching table overflow attack.

Copyright © 2013, Juniper Networks, Inc.

Table 102: VLAN Profile Advanced Settings for an EX Series Switch *(continued)*

MAC Aging Time (ms)	Indicate the number of milliseconds that unused dynamic MAC addresses remain in the MAC forwarding table before being deleted. If you specify the time as **unlimited**, entries are never removed from the table. Generally, use this setting only if the switch or the VLAN has a fairly static number of end devices—otherwise the table will eventually fill up. You can use this setting to minimize traffic loss and flooding that might occur when traffic arrives for MAC addresses that have been removed from the table. The range is from 60 through 1,000,000.
EX Switching L2 Filters	
L2 Ingress Filter	Click **Select** to choose from existing Filter profiles. Select a profile from the Choose Filter Profile window and click **OK**. The filter configuration contained in the profile will be applied to ingress traffic on the VLAN. To remove the selected Filter profile, click **Clear**.
L2 Egress Filter	Click **Select** to choose from existing Filter profiles. Select a profile from the Choose Filter profile window and click **OK**. The filter configuration contained in the profile will be applied to egress traffic on the VLAN. To remove the selected Filter profile, click **Clear**.
EX Switching L3 Routing Filters If you indicated a single VLAN ID under the Basic Settings, you can specify one or more routing parameters (Layer 3 filters) for the profile.	
L3 Ingress Filter L3 IPv6 Ingress Filter	Click **Select** to choose from existing Filter profiles. Select a profile from the Choose Filter profile window and click **OK**. The filter configuration contained in the profile will be applied to ingress traffic on the VLAN. To remove the selected Filter profile, click **Clear**.
L3 Egress Filter L3 IPv6 Egress Filter	Click **Select** to choose from existing Filter profiles. Select a profile from the Choose Filter profile window and click **OK**. The filter configuration contained in the profile will be applied to egress traffic on the VLAN. To remove the selected Filter profile, click **Clear**.
VLAN Security Settings Optionally, select VLAN Security Settings to display the security options DHCP, ARP inspection, and MAC movement limit for VLAN profiles for EX switching.	
Enable DHCP Snooping	Check to apply a series of security techniques to the DHCP infrastructure.

Copyright © 2013, Juniper Networks, Inc.

Table 102: VLAN Profile Advanced Settings for an EX Series Switch *(continued)*

Enable ARP Inspection	The Address Resolution Protocol (ARP), which provides IP communication within a Layer 2 broadcast domain by mapping an IP address to a MAC address, has security issues. Select this option to apply inspection to untrusted interfaces.
MAC Movement Limit	Indicate the number of times a MAC address entry can be moved in the MAC address table without consequences.
MAC Movement Action	When MAC Movement Limit is enabled, select an action to be applied to MAC addresses that exceed the MAC Movement Limit, either **None**, **Log**, **Drop**, **Shut Down**, or **Drop and Log**.

Click **Next** or click **Review** to see the Review page of the wizard. For review directions, see "Reviewing and Saving the VLAN Profile Configuration" on page 350.

Specifying Advanced VLAN Profile Settings for Wireless VLANs

To configure the advanced settings for the wireless VLAN profile, enter the settings described in Table 103 on page 340 for a wireless LAN controller. All fields are optional.

Table 103: VLAN Profile Advanced Settings for a Wireless LAN Controller

Field	Action
Filter	
Filter	Click **Select** to choose from existing Filter profiles. Select a profile from the Choose Filter profile window and click **OK**. The filter configuration contained in the profile will be applied to ingress traffic or egress traffic or both based on the selected direction. To remove the selected Filter profile, click **Clear**.
Direction	If you added a filter, select the direction of the traffic towards which the filter will be applied. The options are: • **In**—to apply the filter to ingress traffic only. • **Out**—to apply the filter to egress traffic only. • **Both**—to apply the filter for both ingress and egress traffic. • **None**—if you do not want to apply the filter to either ingress or egress traffic. The default value is *Both*, which means the filter is applied for both ingress and egress traffic. NOTE: The direction *None* is applicable only when no Filter profile is selected.
Routing	

Copyright © 2013, Juniper Networks, Inc.

Table 103: VLAN Profile Advanced Settings for a Wireless LAN Controller *(continued)*

Field	Action
Enable DHCP (Disabled by default)	Enable DHCP client for the VLAN. By selecting the check box, you enable VLAN to obtain the Layer 3 interface IP address from the DHCP server.
IGMP Settings Optionally, expand the IGMP Settings section and modify the default settings. Internet Group Management Protocol (IGMP) snooping controls multicast traffic on a controller by forwarding packets for a multicast group only on the ports that are connected to members of the group. The controller listens for multicast packets and maintains a table of multicast groups, as well as their sources and receivers, based on the traffic.	
Enabled	IGMP is enabled by default. You can disable it by removing the check mark.
Version (default is Version 2)	Select the IGMP version, **Version 1** or **Version 2**, from the list.
Querier Enabled (default is disabled)	Select the check box to enable pseudo-query. TIP: The IGMP querier enables IGMP snooping to operate in a VLAN without a multicast router to send IGMP general queries to clients. Juniper Networks recommends that you enable the querier only when the VLAN contains local multicast traffic sources and no multicast router is supporting the subnet.
Query Interval (default is 125 seconds)	Enter or select the number of seconds that elapse between general queries sent by the controller to advertise multicast groups. You can specify a value from 1 through 65,535. The default is 125 seconds.
Other Querier Present Interval (default is 255 seconds)	Enter or select the number of seconds that the controller waits for a general query to arrive from another querier before becoming the querier. You can specify a value from 1 through 65,535. The default is 255 seconds.

Copyright © 2013, Juniper Networks, Inc.

Table 103: VLAN Profile Advanced Settings for a Wireless LAN Controller *(continued)*

Field	Action
Query Response Interval (default is 1 second)	Enter or select the number of seconds, in tenths, that the controller waits for a receiver to respond to a group-specific query message before removing the receiver from the group receiver list. You can specify a value from 1 through 255 tenths of a second. The default is 100 tenths of a second (10 seconds). TIP: The query interval, other-querier-present interval, and query response interval are applicable only when the controller is the querier for the subnet. For the controller to become the querier, the querier feature must be enabled on the controller and the controller must have the lowest IP address among all the devices eligible to become a querier.
Last Member Query Interval (default is 1 second)	Enter or select the number of tenths of a second that the controller waits for a response to a group-specific query after receiving a leave message for that group, before removing the receiver that sent the leave message from the list of receivers for the group. If there are no more receivers for the group, the controller also sends a leave message for the group to multicast routers. You can specify a value from 1 through 255 tenths of a second. The default is 10 tenths of a second (1 second).
Robustness Value (default is 2)	Enter or select a number used as a multiplier to adjust the IGMP timers to the amount of traffic loss that occurs on the network. Set a higher value to adjust for more traffic loss. You can specify a value from 2 through 255. The default is 2.
Proxy Request (default is enabled)	Enable or disable proxy request. Proxy request is enabled by default. Proxy request reduces multicast overhead by sending only one request for each active group to the multicast routers, instead of sending a separate request from each multicast receiver.
Multicast Router Solicitation (default is disabled)	Enable or disable multicast router solicitation. Router solicitation is disabled by default. A controller can search for multicast routers by sending multicast router solicitation messages. This message invites multicast routers receiving the message and support router solicitation to immediately advertise themselves to the controller.

Copyright © 2013, Juniper Networks, Inc.

Table 103: VLAN Profile Advanced Settings for a Wireless LAN Controller *(continued)*

Field	Action
Solicitation Interval (default is 30 seconds)	If you enabled Multicast Router Solicitation, enter or select the multicast router solicitation interval in seconds. You can specify a value from 1 through 65,535 seconds. The default multicast router solicitation interval is 30 seconds.
Spanning Tree Protocol Settings Optionally, expand Spanning Tree Protocol to enable and configure STP on this VLAN.	
Enabled	Select the check box to enable the Spanning Tree Protocol (STP) on the VLAN profile.
Instance Number	The VLAN ID you indicated under basic settings is reflected here. You cannot change this number.
Bridge Priority (default is 32768)	Enter or select a bridge priority number from 0 through 65,535. The default bridge priority for all devices is 32,768. The bridge priority determines the controllers eligibility to become the root bridge. You can set this parameter globally or on individual VLANs. The root bridge is elected on the basis of the bridge priority of each device in the spanning tree. The device with the highest bridge priority is elected to be the root bridge for the spanning tree. The bridge priority is a numeric value from 0 through 65,535. Lower numeric values represent higher priorities. The highest priority is 0, and the lowest priority is 65,535. If more than one device has the highest bridge priority (lowest numeric value), the device with the lowest MAC address becomes the root bridge. If the root bridge fails, STP elects a new root bridge on the basis of the bridge priorities of the remaining bridges.
Protocol (default is PVST)	Enter the protocol for the VLAN. Network Director supports 802.1D and Per-VLAN Spanning Tree plus (PVST+).

Copyright © 2013, Juniper Networks, Inc.

Table 103: VLAN Profile Advanced Settings for a Wireless LAN Controller *(continued)*

Field	Action
Max Age (default is 20 seconds)	Enter or select an age from 6 through 40 seconds. The default is 20 seconds. The period of time that a controller acting as a designated bridge waits for a new hello packet from the root bridge before determining that the root bridge is no longer available and is initiating a topology change. You can specify a range from 6 through 40 seconds. The default is 20 seconds.
Hello Time (default is 2 seconds)	Enter or select an interval from 1 through 10 seconds. The default is 2 seconds. The interval between configuration messages sent by a controller when the controller is acting as the root bridge. You can specify an interval from 1 through 10 seconds. The default is 2 seconds.
Forward Delay (default is 15 seconds)	Enter or a select a time delay from 4 through 30 seconds. The default is 15 seconds. The period of time a bridge other than the root bridge waits after receiving a topology change notification to begin forwarding data packets. You can specify a delay from 4 through 30 seconds. The default is 15 seconds. (The root bridge always forwards traffic.)

Click **Next** or click **Review** to see the Review page of the wizard. For review directions, see "Reviewing and Saving the VLAN Profile Configuration" on page 350.

Specifying Advanced VLAN Settings for a Campus Switching ELS Profile

To configure the advanced settings for a Campus Switching ELS VLAN profile, specify the parameters described in Table 104 on page 344 for Campus Switching ELS. All settings are optional.

Table 104: VLAN Profile Advanced Settings for Campus Switching ELS

Field	Action
Campus Switching ELS Switching MAC Parameters	
Interface MAC Limit	Indicate the number of dynamic MAC addresses that can be learned on the VLAN. If this number is exceeded, packets containing new MAC addresses are dropped and an alarm is raised. Setting a limit on the number of dynamic MAC addresses protects against an Ethernet switching table overflow attack.

Copyright © 2013, Juniper Networks, Inc.

Table 104: VLAN Profile Advanced Settings for Campus Switching ELS *(continued)*

Field	Action
Packet Action	Indicate the packet action for MAC addresses that exceed the Interface MAC Limit, either **None**, **Log**, **Drop**, **Shut Down**, or **Drop and Log**.
MAC Table Size	If you indicated an Interface MAC limit, provide a table size here using the up and down arrows. The MAC table must allow for at least 16 entries—you can increase this limit using the arrow.
L2 Filters	
Ingress Filter profile	Click **Select** to choose from existing Filter profiles. Select a profile from the Choose Filter Profile window and then click **OK**. The filter configuration contained in the profile will be applied to ingress traffic on the VLAN. To remove a selected Filter profile, click **Clear**.
Egress Filter profile	Click **Select** to choose from existing Filter profiles. Select a profile from the Choose Filter profile window and then click **OK**. The filter configuration contained in the profile will be applied to egress traffic on the VLAN. To remove a selected Filter profile, click **Clear**.
Routing If you selected a single VLAN ID under Basic Settings, you can specify Layer 3 filter routing parameters for the VLAN profile. NOTE: If an IP address is configured for a VLAN on some devices, then the configured IP address will be retained and a DHCP client will not be enabled on those devices. Also, if you indicated a VLAN range for basic ELS switching configuration, this option is not available.	
Routing L3 Filters	
Ingress Filter IPv6 Ingress Filter	Click **Select** to choose from existing Filter profiles. Select a profile from the Choose Filter profile window and click **OK**. The filter configuration contained in the profile will be applied to ingress traffic on the VLAN. To remove the selected Filter profile, click **Clear**.
Egress Filter IPv6 Egress Filter	Click **Select** to choose from existing Filter profiles. Select a profile from the Choose Filter profile window and click **OK**. The filter configuration contained in the profile will be applied to egress traffic on the VLAN. To remove the selected Filter profile, click **Clear**.
VLAN Security Settings Optionally, enable VLAN Security Settings to display the security options DHCP, ARP inspection, and MAC movement limit for VLAN profiles for ELS switching.	

Copyright © 2013, Juniper Networks, Inc.

Table 104: VLAN Profile Advanced Settings for Campus Switching ELS *(continued)*

Field	Action
Enable DHCP Snooping	Check to apply a series of security techniques to the DHCP infrastructure.
Enable ARP Inspection	The Address Resolution Protocol (ARP), which provides IP communication within a Layer 2 broadcast domain by mapping an IP address to a MAC address, has security issues. Select this option to apply inspection to untrusted interfaces.
MAC Movement Limit	Indicate the number of times a MAC address entry can be moved in the MAC address table without consequences.
MAC Movement Action	When MAC Movement Limit is enabled, select an action to be applied to MAC addresses that exceed the MAC Movement Limit, either **None**, **Log**, **Drop**, **Shut Down**, or **Drop and Log**.

Click **Next** or click **Review** to see the Review page of the wizard. For review directions, see "Reviewing and Saving the VLAN Profile Configuration" on page 350.

Specifying Advanced VLAN Profile Settings for Data Center Switching

To configure the advanced settings for a data center switching VLAN profile:

1. Enter advanced settings for the profile on the Advanced Setting page.

   The settings that are available depend on which types of VLAN you are configuring—Ethernet or FCoE. Settings for Ethernet VLANs are described in Table 105 on page 346. Settings for FCoE VLANs are described in Table 106 on page 348. All settings are optional.

Table 105: VLAN Profile Advanced Settings for a Data Center Switching Ethernet VLAN

Field	Action
Switching	Specify the switching parameters (MAC parameters and Layer 2 filters) for the profile.
MAC Parameters	
MAC Limit	Type the number of dynamic MAC addresses that can be learned on the VLAN. If this number is exceeded, packets containing new MAC addresses are dropped and an alarm is raised. Setting a limit on the number of dynamic MAC addresses protects against an Ethernet switching table overflow attack.

Copyright © 2013, Juniper Networks, Inc.

Table 105: VLAN Profile Advanced Settings for a Data Center Switching Ethernet VLAN *(continued)*

Field	Action
MAC Aging Time (ms)	Indicate the number of milliseconds unused dynamic MAC addresses remain in the MAC forwarding table before being deleted. If you specify the time as **unlimited**, entries are never removed from the table. Generally, use this setting only if the switch or the VLAN has a fairly static number of end devices—otherwise the table will eventually fill up. You can use this setting to minimize traffic loss and flooding that might occur when traffic arrives for MAC addresses that have been removed from the table. The range is from 60 through 1,000,000.
L2 Filters	
Ingress Filter	Click **Select** to choose from existing Filter profiles. Select a profile from the Choose Filter Profile window and click **OK**. The filter configuration contained in the profile will be applied to ingress traffic on the VLAN. To remove the selected Filter profile, click **Clear**.
Egress Filter	Click **Select** to choose from existing Filter profiles. Select a profile from the Choose Filter profile window and click **OK**. The filter configuration contained in the profile will be applied to egress traffic on the VLAN. To remove the selected Filter profile, click **Clear**.
VLAN Security Settings	
Enable DHCP Snooping	Select the check box to enable DHCP snooping.
Enable ARP Inspection	Select the check box to enable ARP Inspection.
MAC Movement Limit	Enter the MAC movement limit.
Fabric Limit	Specify the maximum number of times a MAC address can move in a QFabric system. If no fabric limit is specified then the value given for the mac-move-limit applies to the QFabric system.
MAC Movement Action	Select one of the options. The options are: None, Log, Drop, and Shutdown.
FIP Snooping Settings	
Enable V2V2N Snooping	Select to enable VN_Port to VN_Port (VN2VN) FIP snooping on the VLAN.
Beacon Period (ms)	Set the interval between periodic beacons, in milliseconds. Beacons perform virtual link maintenance for VN_Ports in a way that is similar to FIP keepalive advertisements. Range: 250 through 90000 milliseconds. Default: 8000 milliseconds

Copyright © 2013, Juniper Networks, Inc.

Table 105: VLAN Profile Advanced Settings for a Data Center Switching Ethernet VLAN *(continued)*

Field	Action
FC Map	Set the FCoE mapped address prefix (FC-MAP) value for the FCoE VLAN to match the FC switch (or FCoE forwarder) FC-MAP value for the FC fabric. The FC-MAP value is a unique MAC address prefix an FC switch uses to identify FCoE traffic for a given FC fabric (traffic on a particular FCoE VLAN). Range: 0x0EFC00 through 0x0EFCFF. Default: 0xEFC00
Routing	Specify the routing parameters (Layer 3 filters) for the profile.
L3 Filters	
Ingress Filter L3 IPv6 Ingress Filter	Click **Select** to choose from existing Filter profiles. Select a profile from the Choose Filter profile window and click **OK**. The filter configuration contained in the profile will be applied to ingress traffic on the VLAN. To remove the selected Filter profile, click **Clear**.
Egress Filter L3 IPv6 Engress Filter	Click **Select** to choose from existing Filter profiles. Select a profile from the Choose Filter profile window and click **OK**. The filter configuration contained in the profile will be applied to egress traffic on the VLAN. To remove the selected Filter profile, click **Clear**.

Table 106: VLAN Profile Advanced Settings for a Data Center Switching FCoE VLAN

Field	Action
Switching	Specify the switching parameters (MAC parameters and Layer 2 filters) for the profile.
MAC Parameters	
MAC Limit	Type the number of dynamic MAC addresses that can be learned on the VLAN. If this number is exceeded, packets containing new MAC addresses are dropped and an alarm is raised. Setting a limit on the number of dynamic MAC addresses protects against an Ethernet switching table overflow attack.
MAC Aging Time (ms)	Indicate the number of milliseconds unused dynamic MAC addresses remain in the MAC forwarding table before being deleted. If you specify the time as **unlimited**, entries are never removed from the table. Generally, use this setting only if the switch or the VLAN has a fairly static number of end devices—otherwise the table will eventually fill up. You can use this setting to minimize traffic loss and flooding that might occur when traffic arrives for MAC addresses that have been removed from the table. The range is from 60 through 1,000,000.

Copyright © 2013, Juniper Networks, Inc.

Table 106: VLAN Profile Advanced Settings for a Data Center Switching FCoE VLAN *(continued)*

Field	Action
L2 Filters	
Ingress Filter	Click **Select** to choose from existing Filter profiles. Select a profile from the Choose Filter Profile window and click **OK**. The filter configuration contained in the profile will be applied to ingress traffic on the VLAN. To remove the selected Filter profile, click **Clear**.
Egress Filter	Click **Select** to choose from existing Filter profiles. Select a profile from the Choose Filter profile window and click **OK**. The filter configuration contained in the profile will be applied to egress traffic on the VLAN. To remove the selected Filter profile, click **Clear**.
VLAN Security Settings	
Enable DHCP Snooping	Select the check box to enable DHCP snooping.
Enable ARP Inspection	Select the check box to enable ARP Inspection.
MAC Movement Limit	Enter the MAC movement limit.
Fabric Limit	Specify the maximum number of times a MAC address can move in a QFabric system. If no fabric limit is specified then the value given for the mac-move-limit applies to the QFabric system.
MAC Movement Action	Select one of the options. The options are: None, Log, Drop, and Shutdown.
FIP Snooping Settings Selecting the FIP Snooping checkbox enable FIP snooping with the default FC-Map. This stops access for all traffic other than FCoE traffic.	
Enable VN2VN Snooping	Select to enable VN_Port to VN_Port (VN2VN) FIP snooping on the VLAN.
Beacon Period (ms)	Set the interval between periodic beacons, in milliseconds. Beacons perform virtual link maintenance for VN_Ports in a way that is similar to FIP keepalive advertisements. Range: 250 through 90000 milliseconds. Default: 8000 milliseconds
FC Map	Set the FCoE mapped address prefix (FC-MAP) value for the FCoE VLAN to match the FC switch (or FCoE forwarder) FC-MAP value for the FC fabric. The FC-MAP value is a unique MAC address prefix an FC switch uses to identify FCoE traffic for a given FC fabric (traffic on a particular FCoE VLAN). Range: 0x0EFC00 through 0x0EFCFF. Default: 0xEFC00

Copyright © 2013, Juniper Networks, Inc.

2. Click **Next** or click **Review** to see the Review page of the wizard. For review directions, see "Reviewing and Saving the VLAN Profile Configuration" on page 350.

   You can either save your profile or make changes to your profile from the **Review** page.

Reviewing and Saving the VLAN Profile Configuration

From this page, you can save or make changes to a VLAN profile:

- To make changes to the profile, click the **Edit** associated with the configuration you want to change.

  Alternatively, you can click **Basic Settings** or **Advanced Settings** from the wizard workflow at the top of the page and make changes there.

  When you are finished with your modifications, click **Review** to return to this page.

- To save a new profile or to save modified settings to an existing profile, click **Finish**.

  The Manage VLAN Profiles page is displayed and your new or modified VLAN profile will be listed in the table of VLAN profiles.

What To Do Next

Once the VLAN profile is created, you must assign the VLAN profile using the Assign VLAN Profile page to the required ports, switches, or controllers. You can also assign VLAN profiles to controller managed access points and cluster managed access points. To assign a VLAN profile, see "Assigning a VLAN Profile to Devices or Ports" on page 392. After you assign a VLAN profile to a port, switch, access point, or controller, you must deploy the profile configuration using the Deploy mode. For details on deploying your configurations, see *Deploying Configuration to Devices*.

FCoE VLANs are assigned to Fabric profiles, where they define the FCoE VLAN for a gateway FC fabric.

Related Documentation

- Assigning a VLAN Profile to Devices or Ports on page 392
- *Deploying Configuration to Devices*
- Understanding VLAN Profiles on page 49

Creating and Managing a WLAN Service Profile

WLAN Service profiles create an SSID and provide many of the parameters the SSID needs to operate—you must have at least one WLAN Service profile in your wireless network. Note that there are no default profiles provided in Network Director. Therefore, you must create at least one WLAN Service profile using the WLAN Service Profile Wizard. For more information about the individual WLAN Service profile parameters, see "Understanding WLAN Service Profiles" on page 52.

Copyright © 2013, Juniper Networks, Inc.

To display the Manage WLAN Service Profiles page: In Build mode, select **WLAN Service** from Profile and Configuration Management in the Tasks pane. The Manage WLAN Service Profiles page appears.

This topic describes:

- Managing WLAN Service Profiles on page 351
- Before You Create a WLAN Service Profile on page 352
- Creating a WLAN Service Profile on page 353
- Specifying the Basic Settings for a WLAN Service Profile on page 354
- Mapping an Authentication Profile to the WLAN Service Profile on page 356
- Mapping an Authorization Profile to the WLAN Service Profile on page 359
- Specifying Security Settings for a WLAN Service Profile on page 360
- Specifying the Advanced Settings for a WLAN Service Profile on page 362
- Reviewing the WLAN Service Profile Summary on page 367
- What To Do Next on page 367

Managing WLAN Service Profiles

From the Manage WLAN Service Profiles page, you can:

- Create a new WLAN Service profile by clicking **Add**. For directions, see "Creating a WLAN Service Profile" on page 353.
- Modify an existing profile by selecting it and then clicking **Edit**.
- View information about a WLAN Service profile, including the interfaces it is associated with, by either clicking the profile name or by selecting the profile and clicking **Details**.
- Delete profiles by selecting a profile and clicking **Delete**.

TIP: You cannot delete profiles that are in use—that is, assigned to objects or used by other profiles. To see the current assignments for a profile, click the hyperlink provided for the profile name to display the details.

- Clone a profile by selecting a profile and clicking **Clone**.

Table 107 on page 351 describes the information provided about WLAN Service Profiles on the Manage WLAN Service Profiles page. This page lists all WLAN Service profiles defined for your network, regardless of your current selected scope in the network view.

Table 107: Manage WLAN Service Profile Fields

Field	Description
Profile Name	Name given to the profile when the profile was created.
Device Family	Wireless controllers (WLC)

Copyright © 2013, Juniper Networks, Inc.

Table 107: Manage WLAN Service Profile Fields *(continued)*

Field	Description
SSID	Name broadcast by access points to radios.
SSID Type	SSID type refers to encryption. Encryption is either on (Crypto) or off (Clear). For more information, see "Understanding Wireless Encryption and Ciphers" on page 109.
Authorization Profile Name	Associated Authorization profile name. Authorization refers to the levels of information available to each client. For more information, see "Understanding Authorization Profiles" on page 24.
Authentication Profile Name	Associated Authentication profile name. Authentication is the process of identifying yourself to the network, for example logging on. For more information, see "Understanding Authentication Profiles" on page 22.
CoS Profile	Class of Services profile associated with this WLAN Service profile. For more information, see "Understanding Class of Service (CoS) Profiles" on page 26.
Description	Any description provided during creation of the WLAN Service profile.
Creation Time	Date and time when this profile was created.
Update Time	Date and time when this profile was last modified.
User Name	The username of the user who created or modified the profile.

TIP: All columns may not be currently displayed. To show or hide fields in the table, click the down arrow on the field header, select **Columns**, and select or clear the check box adjacent to the field that you want to show or hide.

Before You Create a WLAN Service Profile

You need at least one Authentication profile and one Authorization profile to create a WLAN Service profile—these profiles are mapped to the WLAN Service profile to create an SSID. The wizard will request the profiles during configuration. If you have not already created an Authentication profile ("Creating and Managing Authentication Profiles" on page 157) or an Authorization profile ("Creating and Managing Wireless Authorization Profiles" on page 167), you can create them from the WLAN Service profile wizard. However, you must have a configured Access Profile to create an Authentication profile—see "Creating and Managing Access Profiles" on page 136.

Copyright © 2013, Juniper Networks, Inc.

Creating a WLAN Service Profile

In Network Director, you configure wireless SSIDs by creating WLAN Service profiles. In a WLAN Service profile, at minimum, you specify:

- A WLAN name
- An SSID name
- Encryption setting (on or off)
- Name of an Authentication profile to use for client connection.
- Name of an Authorization profile to use for client connection.

You can optionally include additional WLAN configuration such as:

- Keep initial VLAN, meaning that if an 802.1X user is not assigned to a VLAN by AAA, and subsequently roams to a controller where the current VLAN does not exist, a tunnel is set up so that the user stays in that VLAN. This, however, does not work for Web portal clients.
- A specific bandwidth limit for the WLAN Service profile clients.
- Whether or not SSID traffic is load balanced between access points.
- Broadcast or hide the name of the SSID.
- A wireless software bridge to connect WLAN networks.
- A fall-through access mechanism for logon if authentication fails. This can be either a Web portal for login or just enabling logon with open access.
- Encryption parameters.
- Broadcast settings such as proxy ARP or DHCP restrict.
- Allowed client types for the WLAN Service profile.
- Voice configuration such as call admission control (CAC) and retry count.
- Client timeout settings.
- 802.11n attributes such as ng mode or na mode, guard interval, frame aggregation, A-MSDU and MPDU settings.

To create a WLAN Service profile:

1. Click

in the Network Director banner.
2. Under Select View, select either **Logical View**, **Location View**, **Device View** or **Custom Group** View.

   TIP: **Do not select Virtual View or Topology View.**
3. Click **WLAN Service** under Profile and Configuration Management in the Tasks pane.

Copyright © 2013, Juniper Networks, Inc.

The Manage WLAN Service Profiles page opens, displaying the list of currently configured WLAN Service profiles.

4. Click **Add**.

   The Create WLAN Profile wizard is displayed. It consists of six sections, Basic Settings, Authentication Profile, Authorization Profile, Security Settings, Advanced Settings, and Review.

5. Complete the wizard pages for each section of the WLAN Service profile as described in both online help (click **?**) and in these tables included below: "Specifying the Basic Settings for a WLAN Service Profile" on page 354, "Mapping an Authentication Profile to the WLAN Service Profile" on page 356, "Mapping an Authorization Profile to the WLAN Service Profile" on page 359, "Specifying Security Settings for a WLAN Service Profile" on page 360, and "Specifying the Advanced Settings for a WLAN Service Profile" on page 362.

   NOTE: **If encryption is off (set to Clear) in the basic settings. then security settings are unavailable.**

6. Click the **Review** tab and check your WLAN Service profile settings. If you need to change a setting click **Edit** in the corresponding section, make changes, and then return to the **Review** tab.

7. Click **Finish**.

   The WLAN Service profile is added to the list of profiles that you can include in a Radio Profile.

Specifying the Basic Settings for a WLAN Service Profile

Required basic WLAN settings include the profile name, SSID name, and encryption setting. All other settings are optional.

The basic settings page is also where the optional settings for keeping the initial VLAN, setting a bandwidth limit, and turning off load balancing for the SSID are configured.

To configure the basic settings for the WLAN Service profile, enter the settings described in Table 108 on page 354. Required settings are indicated by a red asterisk (*) that appears next to the field label in the user interface.

Table 108: WLAN Service Profile Basic Settings

Field	Action
Name	Type a unique name that identifies the WLAN Service profile. You can use up to 32 characters and the special character _. No other special characters are allowed.
Description	Range: 0 through 256 alphanumeric characters, including spaces and special characters.

Copyright © 2013, Juniper Networks, Inc.

Table 108: WLAN Service Profile Basic Settings *(continued)*

Field	Action
SSID	Type a unique name to be broadcast from access points and selected by clients. Use up to 32 characters and only the special character _. For more information about SSIDs, see "Understanding Network Director SSID Configuration With Profiles" on page 59 and "Understanding the Network Terms SSID, BSSID, and ESSID" on page 103.
SSID Type (default is Crypto)	Select either **Crypto** (encryption applied to data traffic) or **Clear** (no encryption applied). For more information, see "Understanding Wireless Encryption and Ciphers" on page 109. If encryption is off (set to Clear) then the security settings are unavailable.
Settings	
Keep Initial VLAN (default is disabled)	Select this check box to specify that VLANs persist over different controllers. If an 802.1X user is not assigned to a VLAN by AAA, and subsequently roams to a controller where the VLAN he was in does not exist, a tunnel is set up so that the user stays in that VLAN. This, however, does not work for Web portal clients. For more information about configuring VLANs in Network Director, see "Understanding VLAN Profiles" on page 49, and "Creating and Managing VLAN Profiles" on page 330.
Bandwidth Limit (default is disabled)	Select this check box to limit the bandwidth of any client session connected to an access point with this given WLAN Service profile (SSID). You must also indicate a Max Bandwidth for this setting to take effect.
Max Bandwidth (default is 1)	If Bandwidth Limit is selected, select a maximum bandwidth in kilobytes per second to limit any client session connected to an access point with this given WLAN Service profile (SSID). This bandwidth setting in a WLAN Service profile overrides any bandwidth setting configured in a CoS profile as part of an Authorization profile.
Load Balance Exempt (default is disabled)	Select this check box to prevent access points from sharing the data traffic load for this SSID. This only has an effect if the associated Access profile has load balancing enabled. For more information about load balancing, see "Understanding Load Balancing for Wireless Radios" on page 97.
Beacon (default is selected)	Select this check box to indicate that the name SSID of this WLAN will be broadcast. Clear this check box to hide the name of the SSID. See "Understanding Network Director SSID Configuration With Profiles" on page 59.
Fall Through Access (default is None)	Select the action the system will take when authentication fails. You can indicate that a Web Portal be used login or you can just enable login with open access (Last Resort). The default is None. If you select Web Portal, you must also complete the additional Web Portal Settings under the Authentication Profile tab—see "Creating and Managing Authentication Profiles" on page 157.

Copyright © 2013, Juniper Networks, Inc.

To continue, click either **Next** or **Authentication Profile**. For directions to complete that section, see "Mapping an Authentication Profile to the WLAN Service Profile" on page 356.

Mapping an Authentication Profile to the WLAN Service Profile

Authentication for the WLAN Service profile's SSID is provided by an Authentication profile. You can either link to an existing Authentication profile or you can configure authentication for this WLAN Service profile from here. You should be aware of two things:

- The directions here for creating Authentication profiles within the WLAN Service profile include the steps but do not include full explanations—for more detailed directions, see "Creating and Managing Authentication Profiles" on page 157.
- To use any authentication other than open authentication, you must have a pre-existing Access profile—to create an Access profile, follow the directions "Creating and Managing Access Profiles" on page 136.

For more information about Authentication profiles, see "Understanding Authentication Profiles" on page 22.

The Options for Mapping the WLAN Service Profile to an Authentication Profile are listed in Table 109 on page 356.

Table 109: Options for Mapping an Authentication Profile to a WLAN Service Profile

Field	Action
Choose an existing Authentication Profile	To use an existing Authentication profile, leave this default option selected—**Choose existing Authentication profile**. Click **Select**, and then select the name of the separate, preconfigured Authentication profile that determines the login authentication mechanism used for this WLAN Service profile. Click **OK**.

Copyright © 2013, Juniper Networks, Inc.

Table 109: Options for Mapping an Authentication Profile to a WLAN Service Profile *(continued)*

Field	Action
Create a new Authentication profile	

Copyright © 2013, Juniper Networks, Inc.

Table 109: Options for Mapping an Authentication Profile to a WLAN Service Profile *(continued)*

Field	Action
	To configure a new Authentication profile, select **Create new Authentication profile**. NOTE: You need a previously configured Access profile if you select the authentication types **802.1X Access**, **MAC Access**, or **Web Access**. If you select **Open Access**, you do not reference an existing Access profile. Follow these steps to create an Authentication profile for this WLAN Service profile: 1. Provide a new Authentication profile name and optional description. 2. Under Access Rule, click **Add**. The Add Access Rules window opens—add access rules for either authentication or accounting. 3. Select an Access Type from the list. If you select the **802.1X Access**, **MAC Access**, or **Web Access** you will need to reference an existing Access profile. If you select **Open Access**, you will not have to reference an existing Access profile. 4. Provide details for the selected access method: • If 802.1X is the Access Type, provide a **Matching Glob** such as ** and then select an **Access Profile** from the list. The option **Enable Authentication** is selected by default and you can optionally also select **Enable Local Authentication**, **Enable Accounting**, and/or **Enable Local Accounting**. Click **OK**. • If MAC Access is the Access Type, provide a **Matching Glob** such as ** and then select an **Access Profile** from the list. The option **Enable Authentication** is selected by default and you can optionally also select **Enable Local Authentication**, **MAC Prefix**, **Enable Accounting**, and/or **Enable Local Accounting**. Click **OK**. • If Web Access is the Access Type, provide a **Matching Glob**, and select an **Access Profile** from the list. The option **Enable Authentication** is selected by default and you can optionally also select **Enable Local Authentication**, **Enable Accounting**, and/or **Enable Local Accounting** with a Record Type (**Start-Stop** or **Stop-Only**). Click **OK**. • If Open Access is the Access Type, the option **Enable Accounting** is selected. You can optionally select **Enable Local Accounting**, select a Record Type (either **Start-Stop** or **Stop-Only**), and optionally select an Access profile from the list and provide Web Portal Settings. Click **OK**. NOTE: For an explanation of all authentication options, see "Creating and Managing Authentication Profiles" on page 157. 5. If Fall Through Access (in the Basic Settings tab) is set to Web Portal, complete the Web Portal Settings here. Indicate the Web Portal Login Page name. To add a Web Portal Logout page, select **Web Portal Logout** and indicate the Web Portal Logout Page name.

Copyright © 2013, Juniper Networks, Inc.

Table 109: Options for Mapping an Authentication Profile to a WLAN Service Profile *(continued)*

Field	Action
	6. Click **OK**.

To continue, click either **Next** or **Authorization Profile**. For directions to complete that section, see "Mapping an Authorization Profile to the WLAN Service Profile" on page 359.

Mapping an Authorization Profile to the WLAN Service Profile

Authorization for the WLAN Service profile's SSID is provided by an Authorization profile. You can either link to an existing Authorization profile or you can configure an Authorization profile for this WLAN Service profile here—see Table 110 on page 359 for details.

NOTE: **Directions to create Authorization profiles within the WLAN Service profile do not have full explanations—for more detailed directions, see** "Creating and Managing Wireless Authorization Profiles" on page 167.

For more information about Authorization profiles, see "Understanding Authorization Profiles" on page 24.

Table 110: Options for Linking the WLAN Service Profile to an Authorization Profile

Field	Action
Choose existing Authorization profile	To use an Authorization profile that is already configured, leave the default option selected—**Choose Existing Authorization profile**. Click **Select**, and then select the name of the separate, preconfigured Authorization profile that determines the permissions used for this WLAN Service profile. Click **OK**.

Copyright © 2013, Juniper Networks, Inc.

Table 110: Options for Linking the WLAN Service Profile to an Authorization Profile *(continued)*

Field	Action
Create new Authorization profile	To create an Authorization profile for this WLAN Service profile, select **Create New Authorization profile**, Follow these steps to create an Authorization profile for this WLAN profile: 1. Provide a new Authorization profile name and description. 2. Under VLAN, specify a VLAN profile to be used with this WLAN profile. There are two ways to do this. To use an existing VLAN profile, leave the default selection set to **Choose existing VLAN profile**. Click **Select**, and then select the name of the separate, preconfigured VLAN to use for this WLAN. To create a new VLAN profile from here, select **Create new VLAN profile**. Provide a VLAN **Name** and **ID** number. 3. Add an existing CoS Profile to the SSID by clicking **Select** and choosing an existing CoS profile. TIP: The CoS profile must have been created previously. You can also complete the WLAN Service profile now and add a CoS profile later by editing the WLAN Service profile. 4. Add an existing Ingress Filter or Egress Filter to the SSID by clicking **Select** and choosing an existing filter. TIP: The filters must have been created previously. You can also complete the WLAN Service profile now and add filters later by editing the WLAN Service profile. 5. Indicate how many users can log in simultaneously by selecting a number for Simultaneous Login. 6. Select a Service Type for the VLAN profile, either **2 (framed)**, **6 (administrative)**, or **7 (NAS-prompt)**.

To continue, click either **Next** or **Security Settings**. For directions to complete that section, see "Specifying Security Settings for a WLAN Service Profile" on page 360.

Specifying Security Settings for a WLAN Service Profile

When the Basic Setting SSID Type is set to Crypto, encryption algorithms are applied to data streams, scrambling information while it is in transit between access points and clients. If SSID Type is Clear, then the security settings are unavailable.

Access points use the authentication methods selected under each encryption method in the security settings dialog window and disassociate from clients using unselected methods. When multiple authentication methods are checked, clients authenticate using whatever checked methods they are capable of using—802.1X has priority.

By default, both WPA and WPA2 encryption are enabled using 802.1X authentication.

Copyright © 2013, Juniper Networks, Inc.

To configure the encryption and associated authentication security settings for the WLAN Service profile, enter the settings described in Table 111 on page 361. Access points use authentication methods selected under each encryption method and disassociate from clients using the unselected methods. When multiple methods are used by a client, WPA2 authentication with 802.1X authentication has priority.

Table 111: WLAN Service Profile Security Settings

Field	Action
Authentication for the WLAN Service profile is 802.1X by default—it is both the 802.11 standard and is stronger than the alternative. The alternative, PSK authentication, is simpler and does not require a RADIUS or LDAP server. For more information about 802.1X authentication, see "Understanding the IEEE 802.11 Standard for Wireless Networks" on page 100. NOTE: RSN (WPA2) Wi-Fi Encryption Parameters and WPA Wi-Fi Encryption Parameters are encryption options that you can configure only when the SSID Type chosen in Basic Settings is Crypto—when encryption is enforced (Crypto), you must select WPA or WPA2, along with a cipher (CCMP or TKIP). For more information, see "Understanding Wireless Encryption and Ciphers" on page 109.	
802.1X Auth (enabled by default for both WPA2 and WPA)	Select **WPA 802.1X** or **WPA2 802.1X** authentication to enable access points or clients whose 802.11 beacon or probe response frames contain the authentication suite of type 1 (802.1X) within the Robust Secure Network (RSN) information element (IE). Users are authenticated by a RADIUS or LDAP server, and the Extensible Authentication Protocol (EAP) is used for message exchange during authentication. NOTE: 802.1X and PSK authentication types can be applied simultaneously. Clients select the authentication that they are capable of—if a client can use either type, 802.1X is selected.
PSK Auth (disabled by default for both WPA2 and WPA)	When PSK is enabled, 802.11 clients associate with either an access point or peer whose 802.11 beacon or probe response frames contain the authentication suite of type 2 (preshared key) within the RSN IE. Select to use the authentication method based on a preshared key configured by you and exchanged between access points and clients before logon. If you select this method, provide a preshared key or phrase below. This method does not require a RADIUS or LDAP server. For more information, see "Understanding WPA-PSK and WPA2-PSK Authentication" on page 98. NOTE: 802.1X and PSK authentication types can be applied simultaneously. Clients select the authentication that they are capable of—if a client can use either type, 802.1X is selected.

Copyright © 2013, Juniper Networks, Inc.

Table 111: WLAN Service Profile Security Settings *(continued)*

Field	Action
RSN AES (CCMP) or WPA AES (CCMP) Ciphers (disabled by default for both WPA2 and WPA)	CCMP encryption ciphers are part of WPA2 (RSN) encryption. Counter Cipher Mode with Block Chaining Message Authentication Code Protocol (CCMP) implements the standards of the IEEE 802.11i amendment to the original IEEE 802.11 standard and is based on the Counter Mode with CBC-MAC (CCM) of the AES standard. For more information, see "Understanding Wireless Encryption and Ciphers" on page 109. NOTE: CCMP and TKIP ciphers can be applied simultaneously. In this case, clients will authenticate to the CCMP version if possible, otherwise they will use the TKIP version.
RSN (WPA2) TKIP or WPA TKIP (disabled by default for both WPA2 and WPA)	TKIP encryption ciphers are part of WPA encryption. Temporal Key Integrity Protocol (TKIP) provides link-layer security without requiring replacement of legacy hardware the way CCMP does. For more information, see "Understanding Wireless Encryption and Ciphers" on page 109. NOTE: CCMP and TKIP ciphers can be applied simultaneously. In this case, clients will authenticate to the CCMP version if possible, otherwise they will use the TKIP version.
Pre-shared Key	If PSK authentication is selected for either WPA2 or WPA, type the 8 - 63 character string of text an access point expects to receive from a client before it receives any other credentials such as a username and password. Optionally, click **Encrypt** to encrypt the key—the encrypted key is then displayed. NOTE: For more information about PSK, see "Understanding WPA-PSK and WPA2-PSK Authentication" on page 98.
TKIP Countermeasures Time (default is 6000 milliseconds)	If either RSN (WPA2) TKIP or WPA TKIP are selected, indicate the length of time that radios use countermeasures if two message integrity code (MIC) failures occur within 60 seconds. When countermeasures are in effect, radios dissociate all TKIP and WPA WEP clients and refuse all association and re-association requests until the countermeasures end. These countermeasures apply only to TKIP clients. CCMP clients are not affected. NOTE: Both the TKIP cipher suite and WPA/RSN must be selected in order to set countermeasure time.

To continue, click either **Next** or **Advanced Settings**. For directions to complete that section, see "Specifying the Advanced Settings for a WLAN Service Profile" on page 362.

Specifying the Advanced Settings for a WLAN Service Profile

Advanced WLAN Service profile settings include broadcast settings, client types, and voice configuration. Table 112 on page 363 lists the advanced settings and how to configure them.

Copyright © 2013, Juniper Networks, Inc.

Table 112: WLAN Service Profile Advanced Settings

Field	Action
Broadcast Settings Broadcast Settings are mechanisms to reduce overhead caused by wireless broadcast traffic or traffic from unauthenticated clients. One or more of the following can be enabled:	
Proxy ARP (disabled by default)	Select to have the controller respond on behalf of wireless clients to ARP requests for IP addresses.
DHCP Restrict (disabled by default)	Select to have controller capture but not forward any traffic except DHCP traffic for a wireless client during authentication and authorization.
No Broadcast (disabled by default)	Select to send unicasts to clients for ARP requests and DHCP offers. Send ACKs instead of forwarding them as multicasts.
Allowed Client Types Allowed Client Types are clients supported by this WLAN Service profile. Any or all of the following can be enabled:	
802.11a (enabled by default)	Select to support 802.11a clients in the 5-GHz band.
802.11b (enabled by default)	Select to support 802.11b clients in the 2.4-GHz (802.11g and 802.11ng wireless stations can still be used if they can operate in 802.11b mode.)
802.11g (enabled by default)	Select to support 802.11g clients—802.11n wireless stations can still be used if they can operate in 802.11g mode. The presence of a legacy 802.11b participant significantly reduces overall speed of the 802.11g network.
802.11n @ 2.4 GHz (enabled by default)	Select to support 802.11n clients on the 2.4-GHz band. Note that combining 802.11n clients with 802.11b/g clients is not advised because it slows performance for the much faster 802.11n clients. We recommend that you create a WLAN Service profile dedicated to 802.11n clients.
802.11n @ 5 GHz (enabled by default)	Select to support 802.11n on the 2.4-GHz band. Note that combining 802.11n clients with 802.11a clients is not advised because it slows performance for the much faster 802.11n clients.
Voice Configuration	
CAC Mode (default is None)	Select either **None** (no call admission control constraint), **Session** (call admission constrained by total number of sessions on this WLAN), or **VoIP Session** (call admission constrained by total number of voice over IP sessions on this WLAN). For more information about call admission control, see "Understanding Call Admission Control" on page 93.
Max Associated Sessions (default is 14)	If call admission control (CAC) is set to Session, select a number from 0 through 500 to limit the number of sessions using this WLAN Service profile.

Copyright © 2013, Juniper Networks, Inc.

Table 112: WLAN Service Profile Advanced Settings *(continued)*

Field	Action
Max VoIP Calls (default is 12)	If call admission control (CAC) is set to VoIP. select a number from 0 through 100 to limit the voice over IP calls using this WLAN Service profile.
Short Retry Count (default is 5)	Select the number of times (1 through 15) a channel tries to send a frame without getting a response—the default is 5. By default, the frag-threshold setting uses the short-retry-count for frames less than 2346 bytes.
Long Retry Count (default is 5)	Select number of times (1 through 15) a channel tries to send a frame without getting a response—the default is 5. By default, the frag-threshold setting uses the long-retry-count for frames 2346 bytes or longer.
Client Timeout Client Timeout settings determine when clients are dropped by the network. One or more of the following can be configured:	
User Idle Timeout (default is 180 seconds)	Select the number of seconds (20 through 86400) that a voice call can be idle before it is dropped. Default is 180.
Idle Client Probing (default is enabled)	Select to send keepalives from radios to idle clients on the SSID to check for rogue devices.
Web Portal Session Timeout (default is 5 seconds)	If a Web portal is configured, select the maximum number of seconds (5 through 28800) a user session on a Web portal can last before it is dropped. Default is 5 seconds. NOTE: Web portals are configured in Authentication profiles.
Handshake Timeout (default is 20 milliseconds)	Select the maximum number of milliseconds (20 through 5000) an authentication handshake can last before it is dropped. Default is 20 milliseconds and zero indicates no limit.
802.11n Attributes For more information about 802.11n, see "Understanding the IEEE 802.11 Standard for Wireless Networks" on page 100.	
802.11ng Mode (default is Enabled)	When 802.11n is an enabled client type for this WLAN, enable 802.11ng Mode to accept additional connections from 802.11g clients.
802.11na Mode (default is Enabled)	When 802.11n is an enabled client type for this WLAN, enable 802.11na Mode to accept additional connections from 802.11a clients.

Copyright © 2013, Juniper Networks, Inc.

Table 112: WLAN Service Profile Advanced Settings *(continued)*

Field	Action
Guard Interval (default is Short)	Select a guard interval value (**Long** or **Short**). The guard interval is the space between symbols (characters) being transmitted—it eliminates inter-symbol interference. In normal 802.11 operation, the guard interval is 800 ns (**Long**). In 802.11n operation, short guard intervals of 400 ns are supported. By reducing this interval (by selecting **Short**), data bits are transmitted in shorter intervals and provide increased throughput. TIP: Legacy devices may require long guard intervals.

Copyright © 2013, Juniper Networks, Inc.

Table 112: WLAN Service Profile Advanced Settings *(continued)*

Field	Action
Frame Aggregation	Select frame aggregation when 802.11n is an enabled client type to enable frame aggregation for the indicated frame types (All/ MSDU/ MPDU/ Disable). For frame aggregation with A-MPDU, after transmission of every frame, an idle time called Interframe Spacing (IFS) is observed before transmitting the subsequent frame. In 802.11n, multiple packets of application data are aggregated into a single packet called an A-MPDU (Aggregated - MAC Protocol Data Unit). which reduces the number of IFS, which in turn provides more time for data transmission. In addition, clients operating in 802.11n send acknowledgement for block of packets instead of individual packet acknowledgement, reducing overhead involved in frame acknowledgements and increasing overall throughput. Default is **All**.

Copyright © 2013, Juniper Networks, Inc.

Table 112: WLAN Service Profile Advanced Settings *(continued)*

Field	Action
(default is All)	
A-MSDU Max Length (default is 4K)	Select a maximum length for a MAC service data unit (MSDU)—4K or 8K. An MSDU is the service data unit received from the logical link control (LLC) sub-layer which lies above the medium access control (MAC) sub-layer in a protocol stack. When 802.11n is an enabled client type for this WLAN, you can configure the maximum aggregated MSDU packet length. This enables joining multiple packets together into a single transmission unit, in order to reduce the overhead associated with each transmission. Default is 4K.
A-MPDU Max Length (default is 64K)	Select the MPDU maximum length for frame aggregation—8K, 16K, 32K, or 64K. An idle time called Interframe Spacing (IFS) is observed before transmitting a data frame. When 802.11n is an enabled client type for this WLAN, multiple packets of application data are aggregated into a single packet. This is called A-MPDU (Aggregated - MAC Protocol Data Unit). This reduces the number of IFS, which in turn provides more time for data transmission. In addition, clients operating in 802.11n send acknowledgement for block of packets instead of individual packet acknowledgement. This reduces the overhead involved in frame acknowledgements and increases the overall throughput.

To continue, click either **Next** or **Review**. For directions to complete that section, see "Reviewing the WLAN Service Profile Summary" on page 367.

Reviewing the WLAN Service Profile Summary

Before you create the WLAN file, check the configuration:

1. Review your WLAN Service profile selections by scrolling to the bottom of the screen.
2. Make any needed changes by clicking **Edit** in the appropriate section. Make the changes, then return to the Review tab.
3. Click **Finish**. The WLAN Service profile assignment appears next to the access point or radios in the list.

What To Do Next

Next, you can either create a new Radio profile and select the WLAN Service profile during creation, or you can edit an existing Radio profile and add the WLAN Service profile to the existing Radio profile. See "Creating and Managing a Radio Profile" on page 315 for directions.

Related Documentation

- *Understanding the Network Director User Interface*
- Understanding WLAN Service Profiles on page 52
- Understanding Wireless Encryption and Ciphers on page 109
- Understanding the Network Terms SSID, BSSID, and ESSID on page 103

Copyright © 2013, Juniper Networks, Inc.

- Understanding Network Director SSID Configuration With Profiles on page 59
- Understanding Authentication Profiles on page 22
- Understanding Load Balancing for Wireless Radios on page 97
- Understanding the IEEE 802.11 Standard for Wireless Networks on page 100
- Creating and Managing a Radio Profile on page 315
- Creating and Managing Authentication Profiles on page 157
- Understanding Network Director SSID Configuration With Profiles on page 59

Creating a WLAN Service Profile Dedicated to Voice

Create a WLAN Service profile for voice:

1. Click

in the Network Director banner.
2. Under Select View, select either **Logical View**, **Location View**, **Device View** or **Custom Group** View.

   TIP: **Do not select Virtual View or Topology View.**
3. Click **WLAN Service profile** under Profile and Configuration Management in the Tasks pane.

   The Manage WLAN Service profiles page is displayed in the work area.
4. Click **Add** on the Manage WLAN Service profiles pane.

   The Create WLAN Service profile for Wireless (WLC) wizard opens with four sections, Basic Settings (displayed), Security Settings, Advanced Settings, and Review.
5. In the Basic Settings tab of the Create WLAN Service profile wizard, configure these settings:
   - Provide a name for the WLAN.
   - Set SSID Type to Clear.
   - Select the previously created Authorization Profile.
   - Set Fall Through Access to **Last Resort**.
6. Click the **Security Settings** tab of the Create WLAN Service profile wizard, and configure these settings:
   - Disable RSN (WPA2) 802.1X Auth.
   - Disable WPA2 802.1X Auth.
7. Click the **Advanced Settings** tab of the Create WLAN Service profile wizard, and configure these settings:

Copyright © 2013, Juniper Networks, Inc.

- Enable **Proxy ARP**.
- Enable **No Broadcast**.
- Set **Short Retry Count** to **3**.
- Set **Long Retry Count** to **3**.
- Set **CAC Mode** to **VoIP Session**.

8. Click **Review**, check the configuration, then click **Finish**.

A WLAN Service profile is not used automatically. You must link a radio profile to the WLAN Service profile, then link the radio profile to radios in an AP to apply WLAN Service profile settings. For directions to both link a WLAN Service profile and link radios, see "Understanding WLAN Service Profiles" on page 52.

Related Documentation

- Creating and Managing a WLAN Service Profile on page 350
- Understanding Voice Clients and Voice Traffic on page 105
- Creating a Radio Profile for Voice Clients Only on page 329
- Understanding WLAN Service Profiles on page 52

Assigning Authorization Profiles to Controllers

After creating an Authorization profile, assign it to a wireless device (controller), a cluster of controllers, or the members of a group of controllers. A cluster is a logical grouping of wireless LAN controllers that ensures load balancing and seamless mobility within the wireless domain. Configure a mobility domain to be a cluster from the Create Mobility Domain page. For directions, see "Creating a Mobility Domain for Wireless LAN Controllers" on page 398. For directions to create device groups, see "Creating Custom Groups" on page 447.

The following sections describe how to assign an Authorization profile and edit existing Authorization profile assignments.

- Assigning Authorization Profiles on page 369
- Editing Authorization Profile Assignments on page 371

Assigning Authorization Profiles

To assign an Authorization profile to controllers:

1. Click

in the Network Director banner.
2. Under Select View, select either **Logical View**, **Location View**, **Device View** or **Custom Group** View.

TIP: **Do not select Virtual View or Topology View.**

3. Click **Authorization** under Profile and Configuration Management in the Tasks pane.

Copyright © 2013, Juniper Networks, Inc.

The Manage Authorization Profiles page appears.

4. Select an Authorization profile that you want to assign and click **Assign**.

   The Assign Authorization Profile page appears displaying a hierarchal list of network objects, including the network, mobility domain, controllers and clusters that are already defined or discovered for your network.

5. Select a level and click **Next** to view the objects available at that level. If you select a network or a mobility domain, all the controllers or clusters that are part of that network or mobility domain are also selected.

6. Select one or more devices, groups, or clusters from the list.

   NOTE: If Network Director fails to read the configuration of one or more devices after the device discovery, such devices are not displayed in the Assign Profile page. You will not be able to assign profiles to such devices. The Manage Jobs page in System mode displays details of the device discovery jobs. Use the information displayed on this page to take appropriate corrective steps to enable Network Director to reread the configuration of the failed device. For more information, see "Discovering Devices in a Physical Network" on page 455.

7. If you want to view the existing assignment of a device or a cluster, select it and click **View Assignments**.

   The Profile Details window opens displaying the device's current profile assignment.

   Click **Close** to close the window.

8. If you want to remove an existing assignment from a device or a cluster, select it and click **Remove**. The system removes the assignment from the selected device or cluster.

9. Do one of the following to assign the Authorization profile to a device or a cluster:

   - Click **Assign** > **Assign to Device** to assign the Authorization profile to the selected devices.
   - Click **Assign** > **Assign to Cluster** to assign the Authorization profile to the selected clusters.

10. Click **Next** or **Review**.

    The system displays the associations that you created. To modify any of these assignments, click **Edit** or **Profile Association**.

11. Click **Finish** to save the profile associations.

    After you click Finish, the Create Profile Assignments Job Details window opens with a report on the status of the profile assignment job. If you have assigned the profile to a large number of objects, the profile assignment job can take some time to complete. Instead of waiting for the Job Details window to report job completion status, you can close it and check the details of the profile assignment job at a later time using the Manage Job task in System mode.

Copyright © 2013, Juniper Networks, Inc.

NOTE: If any assignment fails, the profile assignment job fails and none of the assignments are created. Check the details for the profile assignment job for information about why the assignment failed.

Editing Authorization Profile Assignments

You can modify the Authorization profile assignments that you made to a device or a cluster using the Edit Assignments page.

To edit a profile assignment:

1. Click Build in the Network Director banner.
2. Under Select View, select either **Logical View**, **Location View**, **Device View** or **Custom Group** View.

   TIP: Do not select **Virtual View** or **Topology View**.

3. Click **Authorization** under Profile and Configuration Management in the Tasks pane.

   The Manage Authorization Profiles page appears.

4. Select the Authorization profile for which you want to edit assignments and click **Edit Assignment**.

   The device categories to which the selected Authorization profile is assigned are displayed. Expand the device category to view the device details and the association status.

5. To delete an existing assignment from a device or a cluster, select it and then click **Delete**.

   The Record Status field is updated for status of the record. A cross mark indicates a deleted record or assignment.

6. Click **Apply** to save the changes and close the page.

Related Documentation

- Understanding Authorization Profiles on page 24
- Creating and Managing Wireless Authorization Profiles on page 167

Assigning an Auto AP Profile to Controllers

For configured Auto AP profiles to take effect, they must be assigned to a controller, and then the controller's configuration must be deployed. This topic describes assigning an Auto AP profile to either a controller, or a controller cluster. You must have a completed Auto AP profile to complete this task—for information about creating an Auto AP profile, see "Creating and Managing Wireless Auto AP Profiles" on page 174. For a description of Auto AP profiles and how they work, see "Understanding Auto AP Profiles" on page 24.

Copyright © 2013, Juniper Networks, Inc.

This topic describes how to use the Assign Auto AP Profile wizard and the Edit Assignments page.

NOTE: If a controller already has an Auto AP profile assigned and you assign another Auto AP profile, then the new profile overrides the existing profile on the controller.

To assign an Auto AP profile to a controller:

1. In any view in the View pane, expand the Wireless Network and then select a wireless object. You can select one controller or a group of controllers. The Auto AP profile will be applied to the selected controllers, and any unconfigured access point connected to those controllers will use the Auto AP profile.
2. Click

in the Network Director banner.
3. Click **Auto AP** under Profile and Configuration Management in the Tasks pane.

   The Manage Auto AP Profiles page opens with a list of existing Auto AP profiles.
4. Select the Auto AP profile you want to assign and click **Assign**.

   The Assign Auto AP Profile wizard opens. It consists of three parts, Device Selection (controller selection), Auto AP Profile Assignment, and Review. You can click the help icon (**?**) to get help on these steps or you can follow the directions "Controller Selection for Auto AP Assignment" on page 372 and "Assigning an Auto AP Profile to Controllers" on page 371.

NOTE: After you assign an Auto AP profile to controllers, you can modify your assignments by selecting the Auto AP profile from the Manage Auto AP Profiles page and clicking **Edit Assignments**.

The following sections describe how to use the Assign Auto AP Profile wizard and the Edit Assignments page.

- Controller Selection for Auto AP Assignment on page 372
- Assigning the Auto AP Profile to Controllers on page 373
- Reviewing and Assigning the Auto AP Profile Configuration on page 374
- Editing Auto AP Profile Assignments on page 374
- What To Do Next on page 375

Controller Selection for Auto AP Assignment

The first step of the Assign Auto AP Profile wizard is selecting the controllers that will assign the Auto AP profile to unconfigured access points. You can assign an Auto AP profile to a single controller or to controllers associated with a domain or cluster.

Copyright © 2013, Juniper Networks, Inc.

To select an object from the network tree:

1. Expand the tree and then select a controller from the list by placing a check mark in the corresponding box. Any controllers below the selected object in the hierarchy are automatically selected.

   NOTE: Simply highlighting an object does not select the object. A check mark must appear in the corresponding box or you will get a message in the next step that says **Please select at least one object.**

2. Click either **Profile Assignment** or **Next** when you have finished selecting the objects.

   The next step of the wizard, Profile Assignment, appears. Follow the directions "Assigning the Auto AP Profile to Controllers" on page 373 to complete Profile Assignment.

Assigning the Auto AP Profile to Controllers

Use the Profile Assignment step of the Assign Auto AP Profile wizard to the controllers for Auto AP profile assignment.

TIP: Controllers can have only one Auto AP. Any Auto AP profile assignments you define for a controller during this procedure will replace the existing ones. Existing profile assignments are not displayed.

To assign an Auto AP profile to one or more controllers:

1. From the Assignments list, select one or more controllers by placing a check mark in the corresponding box of the object containing controllers.

   NOTE: If Network Director fails to read the configuration of one or more devices after device discovery, those devices are not displayed in the Assign Profile page and you will not be able to assign profiles to the devices. The Manage Jobs page in System mode displays details of the device discovery jobs. Use the information displayed on this page to take appropriate corrective steps to enable Network Director to reread the configuration of the failed device. For more information, see "Discovering Devices in a Physical Network" on page 455.

2. Click either **Assign to Device** or **Assign to Cluster**, depending on whether you selected a controller or a controller cluster.

   The third column, Assigned To, reflects either Device or Cluster.

3. Click **OK** to close the Job Details window.

   The Auto AP profile now appears in the Manage Auto AP Profiles list with the status *Pending Deployment*.

Copyright © 2013, Juniper Networks, Inc.

4. To delete an existing assignment, select an assignment from the list and then click **Remove**. To see all existing assignments, click **View Assignments**.
5. Click either **Review** or **Next**.

   The next step of the wizard, Review, appears. For directions, see "Reviewing and Assigning the Auto AP Profile Configuration" on page 374.

Reviewing and Assigning the Auto AP Profile Configuration

Review the Auto AP profile assignment. If you do not need to make changes, click **Finish**. If you need to make a change, click **Edit**, make the changes, and then click **Finish**.

After you click Finish, the Create Profile Assignments Job Details window opens, which reports on the status of the profile assignment job. If you have assigned the profile to a large number of controllers, the profile assignment job can take some time to complete. Instead of waiting for the Job Details window to report job completion status, you can close it and check the details of the profile assignment job at a later time using the Manage Job task in System mode.

NOTE: If any assignment fails, the profile assignment job fails and none of the assignments are created. Check the details for the profile assignment job for information about why the assignment failed.

Editing Auto AP Profile Assignments

For Auto AP profiles to function, they must be assigned to either controllers or controller clusters. You can, however, change these assignments to additional or different controllers, even while the controllers are operating.

To change a controller's Auto AP profile:

1. Select an Auto AP profile from the Manage Auto AP profiles list.
2. Click **Edit**.

   A list of the Auto AP profile's assignments is displayed.
3. Make any needed changes, and then click **Finish**.

   After you click Finish, the Create Profile Assignments Job Details window opens, which reports on the status of the profile assignment job. If you have assigned the profile to a large number of objects, the profile assignment job can take some time to complete. Instead of waiting for the Job Details window to report job completion status, you can close it and check the details of the profile assignment job at a later time using the Manage Job task in System mode.

NOTE: If any assignment fails, the profile assignment job fails and none of the assignments are created. Check the details for the profile assignment job for information about why the assignment failed.

Copyright © 2013, Juniper Networks, Inc.

What To Do Next

Next, deploy the configuration changes you made to the controller or controller cluster—for directions, see *Deploying Configuration to Devices*.

Related Documentation

- Understanding Auto AP Profiles on page 24
- Creating and Managing Wireless Auto AP Profiles on page 174
- *Converting Automatically Discovered Access Points to Manually Configured Access Points With Network Director*

Assigning Device Common Settings to Devices

Once a Device Common Settings profile is created or discovered (system-created profile), you must assign it to devices using the steps described in this topic. You can assign a Device profile to a either single device, a series of single devices, or a Custom Group of devices (see "Creating Custom Groups" on page 447).

NOTE: **A device can have only one Device Common Settings profile assigned to it.**

You must have one or more device profiles created or discovered before you can assign a device profile to a device. When you deploy an assigned device profile, the configuration is pushed onto the device.

This topic describes:

- Assigning Device Common Settings on page 375
- Editing the Assignments of the Device Common Setting on page 377

Assigning Device Common Settings

To assign device common settings to either a single device, a series of single devices, or members of a Custom Group:

1. Click

in the Network Director banner.
2. Select **Device Common Settings** from the Profile and Configuration Management menu in the Tasks pane.

   The Manage Device Common Settings page is displayed. The page displays all the device profiles that you configured as well as the system-created profiles detected during device discovery.
3. Select an undeployed profile from the list of profiles and then click **Assign**.

   The Assign Device Profile page for the selected device family appears with a wizard consisting of three parts, Device Selection, Profile Assignment, and Review. Device Selection is displayed.

Copyright © 2013, Juniper Networks, Inc.

4. Expand the Device Selection object tree and select one or more objects to receive the device profile. You must place a check next to a device to select it—simply highlighting the device does not select it.

   NOTE: If Network Director fails to read the configuration of one or more devices after device discovery, those devices are not displayed in the Device Selection list. You will not be able to assign profiles to those devices. The Manage Jobs page in System mode displays details of the device discovery jobs. Use the information displayed on this page to take appropriate corrective steps to enable Network Director to reread the configuration of the failed device. For more information, see "Discovering Devices in a Physical Network" on page 455.

5. Click either **Next** or click **Profile Assignment** from the wizard workflow.

   The Profile Assignment page opens, displaying your selections, including their Device (name), Type, Assigned To, and Attributes. The Assigned To column now has the entry DEVICE and the Attributes column has the entry Undefined.

6. Click **Define** in the **Attributes** column in the Assignments table to configure the attributes.

   The Configure Attributes window opens, listing all the Layer 3 interfaces available on the device.

   a. Select the Layer 3 interfaces that are required for DHCP relay from the Available list and using the right arrow, move them to the Selected list. You can reorder the interfaces using the UP and DOWN arrows.

   b. Click **Save** to save the interface list and close the Configure Attributes window.

7. You can view the assignment details for the selected device and also remove any assignments:

   - To view the assignment details, select the device and click **View Assignments**.

     The Profile Details page for selected device appears. Expand the **Device** name to view the details of the assignment. The assignment status displays the status whether the device is deployed or is pending device update, and so on.

   - To delete a device common setting assignment for a device, select the device from the Assignments table and click **Remove**.

8. Click **Next** or click **Review** from the wizard workflow to review the assignments. On the Review page, click **Edit** to edit the profile assignment.

9. Click **Finish** once you are done reviewing the profile assignment.

   The Create Profile Assignments Job Details window appears with a status report for the profile assignment job—click **OK** to close this window. If you have assigned the profile to a large number of objects, the profile assignment job can take some time to complete. Instead of waiting for the Job Details dialog box to report job completion

Copyright © 2013, Juniper Networks, Inc.

status, you can close it and check the details of the profile assignment job at a later time using the Manage Job task in System mode.

NOTE: If any assignment fails, the profile assignment job fails and none of the assignments are created. Check the details for the profile assignment job for information about why the assignment failed.

An assigned Device profile has the Assignment State *Pending Deployment* in the Manage Device Common Settings list. Deploy any device profile in this state by following the directions *Deploying Configuration to Devices*.

To view the details of a profile, select the profile from the Manage Device Common Settings page and then click **Details**.

Editing the Assignments of the Device Common Setting

Use the Edit Assignments page to change device common setting assignments. To edit an existing assignment:

1. Select a profile from the **Manage Device Common Settings** page and click **Edit Assignment**.

   The Edit Assignments page for the selected device appears.

2. Expand the **Devices** cabinet and make the desired change from the **Operation** column of the table.

3. Click **Define** from the **Attributes** column of the table to modify the attributes.

   The Configure attributes page is displayed listing all the Layer 3 interfaces available on the device.

   - Select the Layer 3 interfaces that are required for DHCP relay from the Available box and using the right arrow, move them to the Selected box.

     You can rearrange the order of the interfaces using the Up and Down arrows.

   - Click **Save** after you are done with selecting the interfaces.

4. Click **Apply** once you are done with the changes.

   The Manage Device Common Settings page is displayed.

Related Documentation

- Creating and Managing Device Common Settings on page 198
- Creating Custom Groups on page 447

Assigning a Fabric Profile to Devices and Ports

A Fabric profile contains configuration settings for a gateway Fibre Channel (FC) fabric. You can assign an existing user-created or system-created Fabric profile to devices and FC ports to configure FC fabrics, using the steps described in this topic. A Fabric profile can be assigned to a QFX3500 device in standalone mode or to a QFabric Node.

Copyright © 2013, Juniper Networks, Inc.

Gateway FC fabrics on a QFabric system are called local FC fabrics. A local FC fabric does not span Node devices and does not span the fabric Interconnect device. Local FC fabrics are entirely contained on a single Node device. You can assign multiple interfaces on one Node device to a gateway FC fabric.

This topic describes:

- Assigning a Fabric Profile on page 378
- Editing the Assignments of a Fabric Profile on page 380

Assigning a Fabric Profile

To assign a Fabric profile:

1. While in Build mode, select **Fabric** from the Profile and Configuration Management menu in the Tasks pane.

   The Manage Fabric Profiles page opens. The page displays all the Fabric profiles that you configured as well as the system-created profiles detected during device discovery.

2. Select a profile from the list of profiles and click **Assign**.

   The Assign Fabric Common Settings page opens to the Object Selection page.

   NOTE: If Network Director fails to read the configuration of one or more devices after the device discovery, such devices are not displayed in the Assign Profile page. You will not be able to assign profiles to such devices. The Manage Jobs page in System mode displays details of the device discovery jobs. Use the information displayed on this page to take appropriate corrective steps to enable Network Director to reread the configuration of the failed device. For more information, see "Discovering Devices in a Physical Network" on page 455.

3. Enable either **Select Devices** or **Select Port Groups**.

4. If you enabled **Select Devices**, expand the list of devices and select the devices to which to assign the profile by selecting the check box next to the plus sign for the device.

   TIP: Be sure that a check mark appears in the corresponding check box—highlighting the object name is not sufficient. Also, selecting a parent device also selects the child devices under it.

5. If you enabled **Select Port Groups**, select one or more port groups from the Select Port Group list.

6. Click either **Next** or **Profile Assignment**.

   The Profile Assignment page displays the list of existing assignments in the Assignments table.

Copyright © 2013, Juniper Networks, Inc.

7. To assign the profile to an entire device, select the device from the Assignments table, then click the **Assign** button, then select **Assign to Device**.

   NOTE: If you assign the profile to a device but not to ports on the device, the fabric will be created on the device, but no FC ports will be assigned to the fabric. You must assign FC ports to the profile to add them to the fabric.

8. To assign the profile to FC ports on a device:
   a. Select the device from the Assignments table.
   b. Click the **Assign** button; then select **Assign to Port** from the list.

      The Assign Profile to Ports window opens.

   c. Select the FC ports from the list; then click **Assign**.
9. To configure object-specific attributes for an interface:
   a. Click **Define** from the interface's **Attributes** column in the Assignments table.

      The Configure attributes page opens.

   b. Configure the attributes.

      For information about these attributes, see Table 113 on page 380.

   c. Click **Save**.
10. On the Profile Assignment page, you can view the assignment details for the selected device and also remove any assignments:
    - To view the assignment details, select the device and click **View Assignments**.

      The Profile Details page for selected device appears. Expand the **Device** name to view the details of the assignment. The assignment status displays the status whether the device is deployed or is pending device update, and so on.
    - To delete a device from the assignment list, select the device from the Assignments table and click **Remove**.
11. Click **Next** or click **Review** from the top wizard workflow to review the assignments. Use the **Edit** button if you want to edit the profile assignment.
12. Click **Finish** once you are done reviewing the profile assignment.

    After you click Finish, the Create Profile Assignments Job Details dialog box appears, which reports on the status of the profile assignment job. If you have assigned the profile to a large number of objects, the profile assignment job can take some time to complete. Instead of waiting for the Job Details dialog box to report job completion status, you can close it and check the details of the profile assignment job at a later time using the Manage Job task in System mode.

Copyright © 2013, Juniper Networks, Inc.

NOTE: If any assignment fails, the profile assignment job fails and none of the assignments are created. Check the details for the profile assignment job for information about why the assignment failed.

Table 113: Fabric Profile Object-Specific Interface Attributes

Field	Description
Keep Alive Interval	Set the global interval between periodic FIP keepalive advertisements, in milliseconds. The range is 250 through 90,000 milliseconds. The default is 8000 milliseconds.
Priority	Set the global priority value associated with the switch FCF-MAC. CNAs use the priority value to determine the switch with which they will perform FIP FLOGI. The lower the value, the higher the priority. The switch advertises this value to the server ENodes on the FCoE network. The range is 0 through 255. The default value is 128.

After you assign a Fabric profile to a device, you can deploy the profile from the **Deploy** mode. For details, see *Deploying Configuration to Devices*.

To view the details of a profile, select the profile from the Manage Fabric Profiles page and click the **Details** button.

Editing the Assignments of a Fabric Profile

To edit a Fabric profile's device and port assignments:

1. Select a profile from the Manage Fabric Profile page and click **Edit Assign**.

   The Edit Assignments page opens.

2. Expand the nodes in the list to locate the devices and ports you want to change.
3. To delete a device or port from a profile, click **Delete** in the **Operation** column of the device or port.

   An X appears in the Record Status column.

4. To delete multiple devices or ports from a profile, select the devices or ports, then click the **Delete** button.

   An X appears in the Record Status column of the deleted devices or ports.

5. To change a device or port's attributes, click **Define** in the **Attributes** column of the device or port, then modify the attributes using the Configure attributes window.

   A pencil icon appears in the Record Status column of the edited device or port.

6. When you are done making assignment changes, click **Apply**.

   The Manage Fabric Profile page opens.

Related Documentation

- Understanding Fabric Profiles on page 30
- Creating and Managing Fabric Profiles on page 223

Copyright © 2013, Juniper Networks, Inc.

- *Deploying Configuration to Devices*

Assigning an FC Gateway Service Profile to Ports

You assign an FC Gateway Service profile to the ports on Data Center Switching devices that you want to include in a Fibre Channel (FC) gateway. You must assign the profile to at least one FC port and at least one Ethernet or aggregated Ethernet interface on the device. In a QFabric fabric, an FC gateway cannot span multiple nodes.

This topic describes:

- Assigning an FC Gateway Service Profile on page 381
- Editing the Assignments of an FC Gateway Service Profile on page 383

Assigning an FC Gateway Service Profile

To assign an FC Gateway Service profile:

1. While in Build mode, select **FC Gateway Service** from the Profile and Configuration Management menu in the Tasks pane.

   The Manage FC Gateway Service Profiles page opens. The page displays all the FC Gateway Service profiles that you configured as well as the system-created profiles detected during device discovery.

2. Select a profile from the list of profiles and click **Assign**.

   The Assign FC Gateway Service Common Settings page opens to the Object Selection page.

   NOTE: If Network Director fails to read the configuration of one or more devices after the device discovery, such devices are not displayed in the Assign Profile page. You will not be able to assign profiles to such devices. The Manage Jobs page in System mode displays details of the device discovery jobs. Use the information displayed on this page to take appropriate corrective steps to enable Network Director to reread the configuration of the failed device. For more information, see "Discovering Devices in a Physical Network" on page 455.

3. Enable either **Select Devices** or **Select Port Groups**.

4. If you enabled **Select Devices**, expand the list of devices and select the devices to which to assign the profile by selecting the check box next to the plus sign for the device.

   TIP: Be sure that a check mark appears in the corresponding check box—highlighting the object name is not sufficient. Also, selecting a parent device also selects the child devices under it.

Copyright © 2013, Juniper Networks, Inc.

5. If you enabled **Select Port Groups**, select one or more port groups from the Select Port Group list.
6. Click either **Next** or **Profile Assignment**.

   The Profile Assignment page displays the list of existing assignments in the Assignments table.
7. To assign the profile to ports on a device:
   a. Select the device from the Assignments table.
   b. Click the **Assign to Port** button from the list.

      The Assign Profile to Ports window opens.
   c. Select ports from the list, then click **Assign**.
8. Click **Save**.
9. On the Profile Assignment page, you can view the assignment details for the selected device and also remove any assignments:
   - To view the assignment details, select the device and click **View Assignments**.

     The Profile Details page for selected device appears. Expand the **Device** name to view the details of the assignment. The assignment status displays the status whether the device is deployed or is pending device update, and so on.
   - To delete a device from the assignment list, select the device from the Assignments table and click **Remove**.
10. Click **Next** or click **Review** from the top wizard workflow to review the assignments. Use the **Edit** button if you want to edit the profile assignment.
11. Click **Finish** once you are done reviewing the profile assignment.

    After you click Finish, the Create Profile Assignments Job Details dialog box appears, which reports on the status of the profile assignment job. If you have assigned the profile to a large number of objects, the profile assignment job can take some time to complete. Instead of waiting for the Job Details dialog box to report job completion status, you can close it and check the details of the profile assignment job at a later time using the Manage Job task in System mode.

NOTE: If any assignment fails, the profile assignment job fails and none of the assignments are created. Check the details for the profile assignment job for information about why the assignment failed.

After you assign an FC Gateway Service profile to a device, you can deploy the profile from the **Deploy** mode. For details, see *Deploying Configuration to Devices*.

To view the details of a profile, select the profile from the Manage Fabric Profiles page and click the **Details** button.

Copyright © 2013, Juniper Networks, Inc.

Editing the Assignments of an FC Gateway Service Profile

To edit an FC Gateway Service profile's port assignments:

1. Select a profile from the Manage FC Gateway Service Profile page and click **Edit Assign**.

   The Edit Assignments page opens.

2. Expand the nodes in the list to locate the devices and ports you want to change.
3. To delete a device or port from a profile, click **Delete** in the **Operation** column of the device or port.

   An X appears in the Record Status column.

4. To delete multiple devices or ports from a profile, select the devices or ports, then click the **Delete** button.

   An X appears in the Record Status column of the deleted devices or ports.

5. When you are done making assignment changes, click **Apply**.

   The Manage FC Gateway Service Profile page opens.

Related Documentation

- Creating and Managing FC Gateway Service Profiles on page 228
- *Deploying Configuration to Devices*

Assigning a Port Profile to Interfaces

You can assign an existing user-created or system-created Port profile to network Ethernet interfaces, aggregated Ethernet interfaces, or Port Group member interfaces on one or more switches.

During the process of assigning a Port profile to interfaces, you can also:

- Configure IPv4 or IPv6 addresses on interfaces to which you have assigned a routing Port profile.

  TIP: **IPv4 filters are separate from IPv6 filters.**

- Configure certain authentication attributes—such as the RADIUS server or servers to use—for all 802.1X interfaces on the device. Because configuring these attributes involves assigning an Access profile to the device, you must have previously created an Access profile.

To assign a Port profile to interfaces:

1. Click

in the Network Director banner.
2. Under Select View, select either **Logical View**, **Location View**, **Device View** or **Custom Group** View.

Copyright © 2013, Juniper Networks, Inc.

TIP: Do not select Virtual View or Topology View.

3. Select **Port** under Profile and Configuration Management in the Tasks pane.

   The Manage Port Profile page is displayed.

4. Select the Port profile you want to assign and then click **Assign**.

   The Assign Port Profile wizard appears. It has three parts—Device Selection, Profile Assignment, and Review.

5. Complete device selection for assignment by following the directions "Selecting Devices for Assignment" on page 384.

6. Assign the port profile to one or more objects by following the directions "Assigning a Port Profile to Interfaces" on page 385.

7. Review your configuration by following the directions "Reviewing and Accepting the Assignments" on page 387.

8. Click **Finish**.

After you assign a Port profile to ports, you can modify your assignments by selecting the Port profile from the Manage Port Profiles page and clicking **Edit Assignments**.

The following sections describe how to use the Assign Port Profile wizard and the Edit Assignments page.

- Selecting Devices for Assignment on page 384
- Assigning a Port Profile to Interfaces on page 385
- Reviewing and Accepting the Assignments on page 387
- Editing Profile Assignments on page 387

Selecting Devices for Assignment

Use Device Selection in the Assign Port Profile wizard to select one or more devices that have ports. You can select either individual devices or port groups. For more information about Port Groups, see *Creating and Managing Port Groups*.

To select devices for Port profile assignment:

1. Enable either **Select Devices** or **Select Port Groups**.

2. If you enabled **Select Devices**, expand the list of objects and select an object by clicking the check box next to the plus sign for the interface to assign the Port profile to. If you select a container node, all switches under that node are selected.

3. If you enabled **Select Port Groups**, select one or more port groups from the Select Port Group list.

4. Click either **Next** or **Profile Assignment** to proceed to the next step in the wizard, Profile Assignment.

Copyright © 2013, Juniper Networks, Inc.

For directions to complete Port Profile Assignment, see "Assigning a Port Profile to Interfaces" on page 385.

Assigning a Port Profile to Interfaces

Use Profile Assignment in the Assign Port Profile wizard to select the interfaces to which you want to assign the Port profile. After you have selected the interfaces, you can configure specific attributes on the interfaces or on the devices to which the interfaces belong.

TIP: Before you start the procedure below, you might want to select a device and click **View Assignments** to view what profiles and attributes are already configured on the device. Any profile assignments or attributes you define during this procedure replace the existing ones.

One optional attribute you can configure for switching interfaces is the Access profile that defines RADIUS server authentication for 802.1X ports. If you will be configuring this optional attribute, make sure that an Access profile has been created.

If you enabled **Select Port Groups** during Object Selection, you can assign the Port profile to any or all existing port groups. If you enabled **Select Devices** during Object Selection, assign the Port profile to interfaces and configure the port-specific or device-specific attributes:

1. Select either a device from the Assignments list:
   - To assign the profile to nonconsecutive interfaces or to aggregated Ethernet interfaces, select a single device.
   - To assign the profile to interfaces in same consecutive interface range (for example, ge-0/0/0 through ge-0/0/15) on one or more devices, select one or more devices. To make multiple selections, press Shift or Ctrl while making the selections.

   NOTE: If Network Director fails to read the configuration of one or more devices after the device discovery, such devices are not displayed in the Assignments list. You will not be able to assign profiles to such devices. The Manage Jobs page in System mode displays details of the device discovery jobs. Use the information displayed on this page to take appropriate corrective steps to enable Network Director to reread the configuration of the failed device. For more information, see "Discovering Devices in a Physical Network" on page 455.

2. Click **Assign to Port**.

   The Assign Profile to Ports window opens.

3. Select either **Ports** (default) or **Port Range**. If you selected multiple devices in the previous step, you cannot choose the Port option.

Copyright © 2013, Juniper Networks, Inc.

4. Select the ports from the list of ports (if you selected the Port option) or enter the port range (if you selected the Port Range option).

   TIP: By default, aggregated Ethernet interfaces are listed after the ge- and xe- interfaces in the list of ports. Members of aggregated Ethernet interfaces are not included in the port list.

   TIP: You can assign the port profile to the same interface on multiple devices by entering the interface name in the both fields of the port range.

5. Click **Assign** to complete the port assignments and close the window.

   The port assignment appears in the list of Assignments, with the Device, Type, and Assigned To, and Attributes columns completed. In the Attributes column, you see a triangle and the link **Define**.

6. Configure the following port-specific or device-specific attributes:

   - If the Port profile is a switching profile that contains an Authentication profile—in other words, the profile is enabling 802.1X authentication on ports—click the **Define** link in the Attributes column for a device to define additional authentication attributes.

     The Configure attributes window opens. Fill in the fields described in Table 114 on page 386.

Table 114: Configure Device Attributes for Port Profile Assignments

Field	Action
Access Profile	Select an Access profile. The RADIUS server attributes defined in the Access profile will be configured on the device when you deploy the configuration.
Radius Server Source IP Address	Type an IP address to be used as the source IP address for RADIUS server requests sent by the switch. The source address must a valid IPv4 or IPv6 (either format) address configured on one of the switch interfaces.
Post authentication URL	Type a URL to be used for the captive portal post-authentication website.

TIP: If you see the message *Port profile does not have an associated Authentication profile. Please configure the Authentication profile.*, then click **OK**, and edit the Port profile by selecting **Port** under Profile and Configuration Management, selecting the Port profile from the list and clicking **Edit**. The Authentication profile association is located in the Port Family Options section.

Copyright © 2013, Juniper Networks, Inc.

NOTE: The attributes you define for the device apply to all 802.1X authenticator interfaces on the switch. Different sets of interfaces on the switch cannot have different attributes.

- If the Port profile is a routing profile, click the **Define** link in the port's Attributes field to configure an IPv4 or IPv6 address on the interface.

  Repeat this step for all the ports on which you want to configure IPv4 or IPv6 interfaces.

7. Repeat the previous steps as needed to complete the port assignments and then click either **Next** or **Review**.

   For review directions, see "Reviewing and Accepting the Assignments" on page 387.

Reviewing and Accepting the Assignments

Use the Review step of the Assign Port Profile wizard to review and accept your assignments:

- Click **Edit** to return to the Profile Assignment step and make changes to your assignments.
- Click **Finish** to accept the assignments.

  After you click Finish, the Create Profile Assignments Job Details window opens, which reports on the status of the profile assignment job. If you have assigned the profile to a large number of objects, the profile assignment job can take some time to complete. Instead of waiting for the Job Details window to report job completion status, you can close it and check the details of the profile assignment job at a later time using the Manage Job task in System mode.

NOTE: If any assignment fails, the profile assignment job fails and none of the assignments are created. Check the details for the profile assignment job for information about why the assignment failed.

After the profile assignment job completes, you can deploy the configuration defined in the Port profile and in the port-specific and device-specific attributes on the affected devices. See *Deploying Configuration to Devices*.

Editing Profile Assignments

Use the Edit Assignments page to change Port profile assignments. You can:

- Delete a port from the profile assignments.

  If the profile has been already deployed on the port, then the configuration is removed from the port when you next deploy the configuration on the device. The configuration removed includes any port configuration that was defined in associated profiles, such as the CoS, Authentication, and IPv4 or IPv6 Filter profiles.

Copyright © 2013, Juniper Networks, Inc.

- Change the IPv4 or IPv6 address for ports associated with a routing Port profile.
- Change the device-specific authentication attributes, such as the Access profile associated with the device. For more information about these attributes, see Table 114 on page 386.

NOTE: You cannot assign the Port profile to additional ports using the Edit Assignment page. To add port assignments, use the Assign Port Profile wizard.

Table 115 on page 388 describes the fields in the Edit Assignments page and how to use them to change the profile assignments. When you are finished with your modifications, click **Apply**. You can then deploy your modifications on the affected devices.

Table 115: Edit Assignment for Port Profile Fields

Field	Description
Objects	Expand the device nodes to see the ports or port group the profile is assigned to.
Assigned State	Indicates the current state of profile assignment on the port: • Deployed—The profile configuration has already been deployed on the port. • Pending—The profile configuration has not yet been deployed on the port. • Pending Removal—The profile configuration was deployed on this port, but will be removed from the port the next time the device configuration is deployed.
Attributes	If the attributes for a port or device are currently undefined, you can click the **Define** link to define them. If attributes have been defined and you want to view them or change them, click the **Change** link.
Operation	Click the **Delete** link to delete the profile assignment from the port.
Record Status	Shows the current assignment status: • An X indicates that you have marked a port for deletion. • A pencil indicates that you have modified the associated attribute. After you apply your assignment changes, these indicators disappear.

Related Documentation

- Creating and Managing Port Profiles on page 283
- Creating and Managing Access Profiles on page 136
- *Creating and Managing Port Groups*
- *Creating and Managing Port Groups*

Copyright © 2013, Juniper Networks, Inc.

Assigning a Radio Profile to Radios

To operate, configured Radio profiles must be assigned to a controller, and then the controller must be deployed. This topic describes assigning a Radio profile to a controller.

NOTE: You must have a previously configured Radio profile to assign—if you do not, stop now and follow the directions "Creating and Managing a Radio Profile" on page 315 or "Creating a Radio Profile for Voice Clients Only" on page 329.

The following sections describe how to use the Assign Radio Profile wizard and the Edit Assignments page.

NOTE: If a radio already has a profile assigned and you assign another profile to its controller, then the new Radio profile overrides the existing Radio profile on the radio.

To assign a Radio profile to controllers:

1. In the View pane, expand the Wireless Network and then select a controller or a controller cluster. If you select a controller cluster, all controllers in that cluster are selected. If you select a Custom Group. all members of that Custom Group are selected.
2. Click

in the Network Director banner.
3. Under Select View, select either **Logical View**, **Location View**, **Device View** or **Custom Group** View.

   TIP: Do not select Virtual View or Topology View.

4. Click **Radio** under Profile and Configuration Management in the Tasks pane.

   The **Manage Radio Profiles** page appears. Here, you see a list of all existing Radio profile assignments and options to add, edit, or delete Radio profiles.
5. Select the Radio profile you wish to assign and click **Assign**.

   The Assign Radio Profile wizard guides you through three parts—Object Selection (controller selection), Radio Profile Assignment, and Review. You can either click the help icon (**?**) for information on these steps or read the next three sections in this topic.

NOTE: After you assign a Radio profile to controllers, you can modify your assignments by selecting the Radio profile from the Manage Radio Profiles page and clicking Edit Assignments.

Copyright © 2013, Juniper Networks, Inc.

The following sections describe how to use the Assign Radio Profile wizard and the Edit Assignments page.

- Selecting the Controllers for Radio Profile Assignment on page 390
- Assigning the Radio Profile to Radios on page 390
- Editing Radio Profile Assignments on page 392

Selecting the Controllers for Radio Profile Assignment

The Assign Radio Profile wizard guides you through Object Selection, the selection of controllers to be assigned this Radio profile.

Select wireless controllers from the network tree:

1. Select controllers from the list by placing a check mark in the corresponding box. If you select a group or cluster, all members are selected.

   NOTE: Simply highlighting a controller will not work, a check mark must appear in the corresponding box or you will get a message in the next step that says “Please select at least one object type.”

2. Click either **Profile Assignment** or **Next** when you have finished selecting the devices.

   The next step of the wizard, Profile Assignment, appears.

Assigning the Radio Profile to Radios

Use the Profile Assignment step of the Assign Radio Profile wizard to select specific radios on the selected controller for assignment.

TIP: Any profile assignments or attributes you define during this procedure will replace the existing ones. Existing profile assignments are not shown.

Copyright © 2013, Juniper Networks, Inc.

To assign a Radio profile to controllers:

1. From the Assignments list, select a controller or a controller cluster by placing a check mark in the corresponding box.

   NOTE: If Network Director fails to read the configuration of one or more devices after the device discovery, those devices are not displayed in the Assign Profile page and you will not be able to assign profiles to the devices. The Manage Jobs page in System mode displays details of the device discovery jobs. Use the information displayed on this page to take appropriate corrective steps to enable Network Director to reread the configuration of the failed device. For more information, see "Discovering Devices in a Physical Network" on page 455.

   After you assign a Radio profile to controllers, you can still modify your assignments by selecting the Radio profile from the Manage Radio Profiles page and clicking **Edit Assignments**.

2. Click **Assign > Assign to Radio**.

   A list of access point radios on the selected controller is displayed

3. Select one or more radios from the list of radios, and then click **Assign**.

   Under assignments, the controller, the access points, and the radios that are assigned this Radio profile are listed.

4. Click **Review** or **Next**.

   The next step of the wizard, Review, appears.

5. Look over the Radio profile assignment. If it is correct, click **Finish**. If you need to make a change, click **Edit**, make the changes, and then click **Finish**.

   After you click Finish, the Create Profile Assignments Job Details window opens, which reports on the status of the profile assignment job. If you have assigned the profile to a large number of objects, the profile assignment job can take some time to complete. Instead of waiting for the Job Details window to report job completion status, you can close it and check the details of the profile assignment job at a later time using the Manage Job task in System mode.

   NOTE: If any assignment fails, the profile assignment job fails and none of the assignments are created. Check the details for the profile assignment job for information about why the assignment failed.

You must deploy the controller configuration for it to take effect. For directions to deploy the controller's configuration, see *Deploying Configuration to Devices*.

Copyright © 2013, Juniper Networks, Inc.

Editing Radio Profile Assignments

Radio profiles must be assigned to radios for them to function. You can, however, change these assignments to additional or different radios, even while the radios are operating.

To change a radio's Radio profile:

1. Select a Radio profile from the list Manage Radio Profiles.
2. Click **Edit**.

   A list of the Radio profile's assignments is displayed.
3. Make any needed changes, and then click **Finish**.

   After you click Finish, the Create Profile Assignments Job Details window opens, which reports on the status of the profile assignment job. If you have assigned the profile to a large number of objects, the profile assignment job can take some time to complete. Instead of waiting for the Job Details window to report job completion status, you can close it and check the details of the profile assignment job at a later time using the Manage Job task in System mode.

NOTE: If any assignment fails, the profile assignment job fails and none of the assignments are created. Check the details for the profile assignment job for information about why the assignment failed.

Next, deploy the configuration changes you made on the controller—see *Deploying Configuration to Devices*.

Related Documentation

- Creating and Managing a Radio Profile on page 315
- *Deploying Configuration to Devices*
- Understanding Radio Profiles on page 42
- Creating and Managing Wireless Auto AP Profiles on page 174

Assigning a VLAN Profile to Devices or Ports

After a VLAN profile is created, assign it to wireless ports, switches, controllers, members of custom groups, members of port groups with wireless ports, or access points managed by controllers or clusters. You can also assign VLAN profiles to controller managed access points and cluster managed access points for local switching on the access points.

You must have one or more existing VLAN profiles, either user-configured or system-created, before you can assign a VLAN profile to a switch, wireless port, or controller, access point, or member of a custom group or port group. For further directions,

Copyright © 2013, Juniper Networks, Inc.

see "Creating and Managing VLAN Profiles" on page 330, "Creating Custom Groups" on page 447, and *Creating and Managing Port Groups*.

- Assigning a VLAN Profile on page 393
- Editing Profile Assignments on page 395

Assigning a VLAN Profile

To assign a VLAN profile:

1. Click

in the Network Director banner.
2. Select **VLAN** from the Profile and Configuration Management menu in the Tasks pane.

   The Manage VLAN profiles page is displayed. The page displays all user-configured and system-created VLAN profiles for discovered devices.
3. Select a VLAN profile from the list of VLAN profiles and then click **Assign**.

   The Assign VLAN Profile page for the selected VLAN appears.

   NOTE: If Network Director fails to read the configuration of one or more devices after the device discovery, those devices are not displayed in the Assign Profile page. You will not be able to assign profiles to those devices. The Manage Jobs page in System mode displays details of the device discovery jobs. Use the information displayed on this page to take appropriate corrective steps to enable Network Director to reread the configuration of the failed device. For more information, see "Discovering Devices in a Physical Network" on page 455.
4. If you are assigning a VLAN profile to devices, a tree is displayed. Choose at least one device or cluster for VLAN assignment. Be sure that a checkmark appears in front of the device - just highlighting the name does not select it.

   If you are assigning a VLAN profile to members of a Custom Group or Port Group, selecting the group selects all members of that group.
5. Click either **Next** or **Profile Assignment**.

   The Profile Assignment page displays the list of existing assignments in the Assignments table.
6. Select a device from the Assignments table and click **Assign to Device**.

   NOTE: When you assign a VLAN profile to a wireless port, only those ports, with unit value 0 or none, and the family Ethernet-switching or none, will be available.
7. Click **Define** from the **Attributes** column in the Assignments table to modify the attributes. The Configure Attributes page is displayed:

Copyright © 2013, Juniper Networks, Inc.

For a wireless LAN controller, specify the following details:

- Enter the Layer 3 interface IP address and logical interface number (between 0 through 32).
- Select the tunnel affinity using the spinner. The available range is from 0 through 10.
- Select the check box to enable the DHCP server.
- Enter the starting IP address for the DHCP server.
- Enter the ending (stop) IP address for the DHCP server.
- Enter the default gateway IP address for the DHCP server.
- Enter the DNS name of the DHCP server.
- Enter the primary DNS address for the DHCP server.
- Enter the secondary DNS server for the DHCP server.
- Click **Save** once you are done with specifying the attributes.

For the wireless port level attributes of a VLAN profile for a controller, specify the following:

- Select the Tag check box to tag the port.
- Select the check box to enable the STP port.
- Select the port priority using the spinner. The available range is from 0 through 255.
- Select the port path cost using the spinner. The available range is from 0 through 65,535

While assigning to an access point specify the following the attributes:

- Select the Tag check box to tag the port.
- Enter the tag value. The range is from 1 through 4093.

For switches, specify the following details:

- Enter the Layer 3 interface IP address and port number (between 0 through 32).
- Enter the unit number. By default, the VLAN ID is populated in this field. You can optionally change the value.

8. You can view the assignment details for the selected device or delete any assignments.
   - To view assignment details, select a device and click **View Assignments**.

     The Profile Details page for selected device appears. Expand the **Device** name to see the details of the assignment. The assignment status displays the status whether the device is deployed or is pending device update, etc.
   - To delete a VLAN profile assignment for a device, select the device from the Assignments table and click **Remove**.

Copyright © 2013, Juniper Networks, Inc.

9. Click **Next** or click **Review** from the top wizard workflow to review the assignments. Alternately, click **Edit** to edit the profile assignment.
10. Click **Finish** once you are done reviewing the profile assignment.

    After you click Finish, the Create Profile Assignments Job Details dialog box appears, which reports on the status of the profile assignment job. If you have assigned the profile to a large number of objects, the profile assignment job can take some time to complete. Instead of waiting for the Job Details dialog box to report job completion status, you can close it and check the details of the profile assignment job at a later time using the Manage Job task in System mode.

NOTE: **If any assignment fails, the profile assignment job fails and none of the assignments are created. Check the details for the profile assignment job for information about why the assignment failed.**

After you assign a VLAN profile to a device or port, you can deploy the VLAN profile from the **Deploy** mode. For details, see *Deploying Configuration to Devices*.

Editing Profile Assignments

You can edit VLAN assignments from the Manage VLAN Profiles page. To edit an existing assignment:

1. Select a profile from the Manage VLAN profiles page and then click **Edit Assignment**.

   The Edit Assignments page for the selected device appears.
2. Expand the **Devices** cabinet select a device.
3. Make the required changes in the **Operation** column of the table.

   To change the attributes, see step 7, from the Assign VLAN profiles tasks.
4. Click **Apply**.

   The Manage VLAN Profiles page reappears.

Related Documentation

- Creating and Managing VLAN Profiles on page 330
- *Deploying Configuration to Devices*
- Creating Custom Groups on page 447
- *Creating and Managing Port Groups*
- Understanding VLAN Profiles on page 49

Copyright © 2013, Juniper Networks, Inc.

Copyright © 2013, Juniper Networks, Inc.

CHAPTER 9

Network Domain and Mobility Domain Configuration

- Creating a Mobility Domain for Wireless LAN Controllers on page 398
- Creating Network Domains for Wireless LAN Controllers on page 401

Copyright © 2013, Juniper Networks, Inc.

Creating a Mobility Domain for Wireless LAN Controllers

A Mobility Domain enables users to roam geographically across the system while maintaining data sessions and VLAN or subnet membership, including IP address, regardless of connectivity to the network backbone. As users move from one area of a building or campus to another, client associations with servers or other resources remains the same.

The clustering functionality ensures mobility across an entire wireless network. With clustering, you can effortlessly create logical groups of controllers and access points, which share network and user information in a proactive manner for continuos and uninterrupted support.

You can create a mobility domain using the Create Mobility Domain window from the Network Director user interface.

A Mobility Domain group consists of a primary seed controller that contains the IP address of all controller members. A secondary controller might be optionally assigned. You must specify the primary seed while creating the mobility domain. A mobility domain cannot exist without the primary seed. You must explicitly configure only one controller per domain as the primary seed. All other controllers in the domain receive their Mobility Domain information from the seed.

You can optionally specify a secondary seed in a Mobility Domain. The secondary seed provides redundancy for the primary seed switch in the Mobility Domain. If the primary seed becomes unavailable, the secondary seed assumes the role of the seed controller. This allows the Mobility Domain to continue functioning if the primary seed becomes unavailable. When the primary seed fails, the remaining members form a Mobility Domain, with the secondary seed taking over as the primary seed controller.

TIP: **Even though selecting a secondary seed for mobility domain is optional, Network Director does not assign a secondary seed by default.**

Enabling cluster for the mobility domain enables cluster mode for both primary and secondary seed. To include the other domain controllers in cluster, set the cluster mode for the domain controllers using the Cluster Mode column in the Controllers in Mobility Domain table. Only after enabling cluster for the mobility domain can the cluster mode for the other mobility domain controllers be set.

1. Enter a name for the mobility domain. The name can contain alphanumeric characters (up to 32 character length) and all special characters except space.

   This is a mandatory field.

2. To select a primary seed, click **Select** next to **Primary Seed**. The Select Primary Seed for Mobility Domain window is displayed. Select a controller from the list of host names.

   This is a mandatory field.

Copyright © 2013, Juniper Networks, Inc.

3. To select a secondary seed, click **Select** next to **Secondary Seed**. The Select Secondary Seed for Mobility Domain window is displayed. Select a controller from the list of host names.

   This is an optional field. However, If you do not select a secondary seed, the domain will be nonoperational during failure.

   To delete an already specified secondary seed, click the **Clear** button next to Secondary Seed.

4. Select the **Enable Cluster** check box if you want to enable clustering for both primary and secondary seeds.

   The *Cluster Mode* column in the Controllers in Mobility Domain table is displayed only if you select the Enable Cluster check box.

5. To add controllers to the mobility domain, click **Add** from the Controllers in Mobility Domain table. The Select Controllers for Mobility Domain window is displayed. Select the controllers from the table. You can select more than one controller.

   To enable cluster mode for the mobility domain members, select **enable** in the Cluster Mode column from the Controllers in the Mobility Domain table.

   TIP: **The table displays the list of available devices. The devices you had selected as the primary and secondary seeds will not be displayed again. Also, if you select a device and click OK, then the selected device is not displayed in the available Select Controllers for Mobility Domain window.**

6. Click **Done** to create the mobility domain with the specified configuration. The message: **Domain saved successfully** is displayed.
7. If you want to remove any controllers from the mobility domain, select the controller from the Controllers in Mobility Domain table and click **Delete**.

You can edit or delete the mobility domain that you created.

To edit a mobility domain:

1. Select **Wireless Network** from My Network in Logical View pane and select the mobility domain that you want to edit.

   Network Director lists the mobility domains that you created earlier.

2. Select **Edit Mobility Domain** from Domain Management in the Tasks pane. The Edit Mobility Domain page for the selected mobility domain is displayed.
3. Follow the tasks described above in the Creating Mobility Domain procedure.

To delete a mobility domain:

1. Select **Wireless Network** from My Network in Logical View pane and select the mobility domain that you want to delete.
2. Select **Delete Mobility Domain** from Domain Management in the Tasks pane. The following confirmation message is displayed:

Copyright © 2013, Juniper Networks, Inc.

```
If mobility domain has cluster please disable cluster for the domain and deploy
 the changes and then delete mobility domain. Do you want to continue?
```

3. Click **Yes** if you want to delete the mobility domain and the mobility domain doesn't contain a cluster.

   Click **No** if you want to delete the mobility domain but the domain contains a cluster.

   To delete a mobility domain that contains a cluster:

   a. Select **Edit Mobility Domain** from Domain Management in the Tasks pane.

   b. Disable clustering by unselecting **Enable Cluster** and clicking **Done**.

   c. Deploy the changed configuration on the affected wireless LAN controllers in Deploy mode.

   d. Now delete the mobility domain by selecting **Delete Mobility Domain** again and click **Yes** in response to the confirmation message.

Related Documentation

- Understanding Mobility Domains on page 81
- Creating Network Domains for Wireless LAN Controllers on page 401

Copyright © 2013, Juniper Networks, Inc.

Creating Network Domains for Wireless LAN Controllers

A Network Domain enables the functionality of Mobility Domains to be extended over a multiple-site installation. In a Network Domain, one or more controllers act as a seed device. A Network Domain seed stores information about all of the VLANs on the Network Domain members. The Network Domain seeds share this information to create an identical database on each seed.

Each Network Domain member maintains a TCP connection to one of the seeds. When a Network Domain member needs information about a VLAN in a remote Mobility Domain, the member consults a connected Network Domain seed. If the seed has information about the remote VLAN, it responds with the controller's IP address to the VLAN. A VLAN tunnel is then created between the seed controller and the remote controller.

When there are multiple Network Domain seeds in an installation, a Network Domain member connects to the seed with the highest configured affinity. If that seed is unavailable, the Network Domain member connects to the seed with the next highest affinity.

You can configure multiple seeds in a Network Domain. If you configure multiple Network Domain seeds, a member consults the seed with the highest configured affinity. To configure multiple seeds in the same Network Domain (for example, a seed on each physical site in the Network Domain), you must establish a peer relationship among the seeds.

If you configure multiple controllers as seed devices in a Network Domain, the controllers establish a peer relationship to share information about the VLANs configured on the member devices of the network to create identical VLAN databases. Sharing information in this way provides redundancy in case one of the seed peers becomes unavailable.

In a Network Domain, a member controller consults a seed controller to determine a user VLAN membership in a remote Mobility Domain. You can create a network domain using the Create Network Domain page from the Network Director user interface.

1. Enter a name for the network domain. The name can contain up to 16 characters including alphanumeric values and all special characters except space.
2. Add controllers in the network domain. To add controllers:
   - Click **Add** from Controllers in Network Domain table. The Select Controllers for Network Domain page appears.
   - Select the devices or controllers that you want add to the network domain by selecting the check boxes. You can select more than one device.
   - Click **OK**. The selected devices appear in the Controllers in Network Domain table.
3. Select the role for each device or controller from the **Role** column in the Controllers in Network Domain table. The available roles are:
   - Seed
   - Member

Copyright © 2013, Juniper Networks, Inc.

- Seed and Member

TIP: You must select at least one device as the seed for the network domain. In a Network Domain, at least one seed device must be aware of each member device. The seed is required to maintain an active TCP connection with each member controllers. To configure a controller as a member of a Network Domain, you must specify one or more Network Domain seeds.

4. To delete a controller from the Controllers in Network Domain table, select the controller by clicking the check box and click **Delete**.

You can edit or delete the network domain that you created.

To edit a network domain:

1. Select **Wireless Network** from My Network in Logical View pane and select the network domain that you want to edit.

   Network Director lists the network domains that you created earlier.

2. Select **Edit Network Domain** from Domain Management in the Tasks pane. The Edit Network Domain page for the selected network domain is displayed.
3. Follow the tasks described above in the Creating Network Domain procedure.

To delete a network domain:

1. Select **Wireless Network** from My Network in Logical View pane and select the network domain that you want to delete.

   Network Director lists the mobility domains that you created earlier.

2. Select **Delete Network Domain** from Domain Management in the Tasks pane. The message: **Deleting domain "domain-name". Do you want to continue?** is displayed.
3. Click **Yes** if want to delete the network domain.

Related Documentation

- Understanding Mobility Domains on page 81
- Creating a Mobility Domain for Wireless LAN Controllers on page 398

Copyright © 2013, Juniper Networks, Inc.

CHAPTER 10

Topology View Configuration

- Assigning and Unassigning Devices to a Location on page 403
- Changing the Location of a Device on page 405
- Configuring Buildings on page 406
- Configuring Floors on page 407
- Configuring Outdoor Areas on page 408
- Creating a Site on page 409
- Deleting Sites, Buildings, Floors, Wiring Closets, and Devices on page 410
- Setting Up Closets on page 412
- Setting Up the Location View on page 414
- Setting Up and Managing the Topology View on page 417

Assigning and Unassigning Devices to a Location

You can assign devices or remove assignments from devices by their location. Your choices for device assignment are dependent upon the type of device and your position in the site. For example, you cannot assign access points to buildings or closets. However, you can assign access points to floors or outdoor areas. For details on which devices can be assigned to a location node, see the Devices that can be Assigned to each Location Component table from the "Setting Up the Location View" on page 414.

This topic describes:

- How to Assign or Unassign Devices on page 404
- Assigning Devices on page 404

Copyright © 2013, Juniper Networks, Inc.

How to Assign or Unassign Devices

To assign devices to a specific location:

While in Build mode,

1. Select **Location View** from the list in the View pane.

   The network tree displays discovered devices under the physical locations already defined in Network Director. The root node (for example, My Network) is selected by default. The devices that are assigned to the locations are displayed under the nodes for respective locations, such as buildings and floors. All devices that are not assigned to any location are displayed under the Unassigned node.

2. Navigate the network tree to the location where you want to add a device.

   Both the Tasks pane and Device Inventory page update to reflect the location's current configuration.

3. Select one of the following tasks in the pane to open Add/Remove Devices for Selected Location.

   - Assign Devices to Building
   - Assign Device to a Floor
   - Assign Devices to a Wiring Closet
   - Assign Devices to an Outdoor Location

4. Navigate the tree to find an available device under Unassigned in the left portion of the page.

5. Select the device and click the double right arrows to assign it to the target location on the right. To unassign a device, select the device in the Assigned Devices to Selected Location column and click the double left arrows. Repeat this step until you have finished assigning and unassigning devices.

6. Click **OK** at the bottom of the page to save the assignment. The network tree refreshes to display the device in the new location.

Assigning Devices

Use the Add/Remove Devices for Selected Location to find a device and assign it to a location within a site. Locate the device in the Available Devices column and assign it by clicking the double right arrows. Use the same method to unassign a device by selecting it in the Assigned Devices to Selected Location column and double clicking the double left arrows.

Related Documentation

- Understanding the Location View on page 63
- Configuring Buildings on page 406
- Configuring Floors on page 407
- Setting Up Closets on page 412

Copyright © 2013, Juniper Networks, Inc.

- Configuring Outdoor Areas on page 408

Changing the Location of a Device

The Change Location of Device task is an easy way to move a device address to another building, floor, or wiring closet location within the site. You can move an access point to another floor or to another outdoor area. However, you cannot move an access point to a building or wiring closet. The Change Location of Device task is available whenever you select an assigned device in the Location or Logical views.

This topic describes:

- How to Move a Device to a New Location on page 405
- Changing the Location of a Device on page 405

How to Move a Device to a New Location

To move a device address to another location:

1. Select a device in the network tree that is currently assigned to a building, floor, or closet.
2. Click **Change Location of Device** to open the Change Location of Device page.
3. Using the Location View, navigate the tree and select the new location for the device. You can move an access point, only to another floor or outdoor area.
4. Click **OK** to move the device assignment and to save the new configuration.

Changing the Location of a Device

The Change Location of Device page consists of two components: Selected Device Details and Location View. Use the Selected Device Details portion of the page to review information about the device and its current location. The fields in Selected Device Details page are described in Table 116 on page 405.

Table 116: Contents of Selected Device Details

Field	Description
Device Name	Hostname
Device IP	Device Address
Device Family	Hardware family of products, for example, Junos EX Series
Location	Gives the current location of the device in the format of site/building/floor/cabinet

Location View is a copy of the network tree for you to navigate and designate the new location for the device.

Copyright © 2013, Juniper Networks, Inc.

Related Documentation

- Understanding the Location View on page 63
- Assigning and Unassigning Devices to a Location on page 403

Configuring Buildings

At any time after you create a site, you can grow your location by adding buildings. You add a building to a site either from within the Location wizard or independently from the Add Building page.

This topic describes:

- How to Add or Edit a Building on page 406
- Adding or Editing a Building for a Location on page 406

How to Add or Edit a Building

To add or change a building definition:

1. Ensure you are in the Build mode and Location view. Click **Build** in the Network Director banner to enter Build mode; select **Location View** from the list in the View pane.
2. If you want to add a building to a site:
   a. Select the site in the Tasks pane , for example, Main Campus.

      The Tasks pane refreshes to show your selected site and the tasks available at the site node.

   b. Click **Add Building** in the Tasks pane to open the **Add Building** page.
3. If you want to edit an existing building definition:
   a. Select the building within the site, for example, Headquarters Building.

      The Tasks pane refreshes to show your selected building and the available tasks that you can perform at the building node.

   b. Click **Edit Building** in the Tasks pane to open the **Edit Building** page.
4. Fill in the fields and click **Done** to submit the information and to refresh the network tree.

Adding or Editing a Building for a Location

Table 117 on page 406 describes the fields needed to establish a building.

Table 117: Add or Edit Building Fields

Field	Description
Building Name	Type a representative name for the building. The Building Name is a required field.

Copyright © 2013, Juniper Networks, Inc.

Table 117: Add or Edit Building Fields *(continued)*

Field	Description
Address	Type an address. The address can be the street address, building number, or any other identification that helps distinguish it from other buildings.
Done	Click to submit the information. Your view updates to reflect the building change under the site name in the network tree.
Cancel	Click to close the window without changes.

Related Documentation

- Understanding the Location View on page 63
- Configuring Floors on page 407
- Assigning and Unassigning Devices to a Location on page 403

Configuring Floors

You can refine the a building location and designate floors within the building. Use the Add Floor page to:

- Name a floor
- Note the floor level
- Upload a floor plan for viewing
- View an uploaded floor plan

This topic describes:

- How to Add or Edit a Floor on page 407
- Adding or Editing a Building Floor for a Location on page 408

How to Add or Edit a Floor

Within each building you can define the number of floors and attach the floor plan for online viewing.

1. Click the Build Mode icon

in the Network Director banner.
2. Select **Location View** from the list in the View pane.
3. If you want to add a floor to a building:
   a. Select the building in the network tree to which you want to add floors, for example, Headquarters.

      The Tasks pane refreshes to show your selected building and the available tasks for the building.

Copyright © 2013, Juniper Networks, Inc.

b. Click **Add Floor** in the Tasks pane to add a new floor to the building.

4. If you want to edit an existing floor definition:
   a. Select the floor within the building, for example, Lobby-Floor 1.

      The Tasks pane refreshes to display the selected building floor and the available tasks that you can perform at the floor node.

   b. Click **Edit Floor** in the Tasks pane to open the Edit Floor page.
5. Fill in the fields for the floor name and level.
6. (Optional) Upload an image of the floor plan.
7. (Optional) View the floor plan, if available.
8. Click **Done** to submit the information and to refresh the network tree.

Adding or Editing a Building Floor for a Location

To add or change information about a building floor, use the fields in Table 118 on page 408.

Table 118: Floor Field Descriptions

Field	Description
Floor Name	Type the name of the floor. This field is required.
Floor Level	Use the arrow keys to set the floor number.
Add/Update	Upload a image of the floor plan.
View	View an existing floor plan.
Done	Saves the floor configuration information, and returns you to **Device Inventory** page in the default view.
Cancel	Discards any configuration changes.

Related Documentation

- Understanding the Location View on page 63
- Setting Up Closets on page 412
- Configuring Buildings on page 406
- Assigning and Unassigning Devices to a Location on page 403

Configuring Outdoor Areas

You can associate an outdoor area to a site or a building for wireless coverage and upload an image or map of that area. After you designate an outdoor area, you can edit or view the map using the Edit Outdoor Area task.

Copyright © 2013, Juniper Networks, Inc.

This topic describes:

- How to Configure an Outdoor Area on page 409
- Configuring an Outdoor Area on page 409

How to Configure an Outdoor Area

To create an outdoor area without using the wizard:

- Ensure you are in Build mode and Location view. Click **Build** in the Network Director banner to enter Build mode; select **Location View** from the list in the View pane.
- Click **Add Outdoor Area** in the Tasks pane. The Add Outdoor Area page opens.
- Fill in the name and upload the optional map.
- Click **Done** to save the data and to return to the default view.

Configuring an Outdoor Area

Table 119 on page 409 describes the fields and buttons necessary to create or change an outdoor area.

Table 119: Outdoor Area Fields

Field	Description
Outdoor Area Name	Type the name of the outdoor area. Network Director associates the outdoor area with the building.
Upload	Optional step to upload an image of the outdoor area. Use the Upload Map window to navigate to the image file location.
Done	Click to save the configuration. The network tree is updated to reflect the change.
Add/Update	Click to add a map or overlay an existing map of the area.

Related Documentation

- Understanding the Location View on page 63
- Setting Up the Location View on page 414
- Assigning and Unassigning Devices to a Location on page 403

Creating a Site

A site is the cornerstone of the location-based view of your network. Until you define a site, the default view of your network tree merely shows you a list of your unassigned devices. After you define a location site, you can build a tree structure of buildings, floors, wiring closets, and outdoor areas that can each be assigned devices. You are able to view the devices in the network by expanding and collapsing these location nodes. To setup a location in Network Director, the first step is to create a site.

Copyright © 2013, Juniper Networks, Inc.

This topic describes:

- How to Add or Edit a Location Site on page 410
- Creating or Editing a Site on page 410

How to Add or Edit a Location Site

1. Click the Build Mode icon

in the Network Director banner.
2. Select **Location View** from the list in the View pane.
3. Click **Add Site** to add a new site or click **Edit Site** in the Tasks pane.
4. Fill in or change the fields on the page that opens.
5. Click **Done** to define the site and to save the configuration.

Creating or Editing a Site

Only a few fields are required to establish a site as shown in Table 120 on page 410.

Table 120: Site Creation Fields

Site Name	A descriptive name for the site. This field is mandatory.
City	The city where the site is located.
State	The state where the site is located.
Country	The country where the site is located. Select the country from the list. This field is mandatory because it sets the regulatory country code for wireless devices. Network Director validates the country code against the country codes in the network's controllers and access points. If the codes do not match, a warning message is sent.

Related Documentation

- Understanding the Location View on page 63
- Configuring Buildings on page 406

Deleting Sites, Buildings, Floors, Wiring Closets, and Devices

From the Build mode Tasks pane, you can delete any sites, buildings, floors, wiring closets and their associated devices . When you delete one of these objects, it removes not only that item but all child objects within the node. All associations related to the node and below are also removed. Devices are moved to the Unassigned node in the network tree. Be sure you understand what is being deleted on the node when you choose to delete a node.

Copyright © 2013, Juniper Networks, Inc.

For example, if you delete a building, it deletes the building, all floors, all wiring closets in that building. All of the devices in the building are moved to Unassigned in the network tree. When you delete a building, the site and any other buildings and their associations remain.

- How to Delete a Location Object on page 411
- Deleting Sites on page 411
- Deleting Buildings on page 411
- Deleting Floors on page 411
- Deleting Closets on page 411
- Deleting Devices on page 412

How to Delete a Location Object

1. Ensure you are in the Build mode and Location view. Click **Build** in the Network Director banner to enter Build mode; select **Location View** from the list in the View pane.
2. Select any object within the site. The option to delete the object appears in the Tasks pane.
3. Confirm the deletion of the object.

Deleting Sites

There is only one method of deleting a site: select the site in the Tasks pane and click **Delete Site**. Use caution with this selection. When you click **Delete Site** you are given the opportunity to confirm or cancel the deletion. If you confirm the deletion, you remove the site and everything in the site. All devices become unassigned and are not associated with any buildings, floors, or wiring closets.

Deleting Buildings

When you delete a building, it removes the building, all floors, and all wiring closets within that building. All devices become unassigned and are not associated with the building, its floors, or its wiring closets. Only one building can be deleted at a time. To delete a building, select the building in the network tree and click **Delete Building**. Confirm the deletion to remove the objects and to disassociate the devices. If a site is deleted, all of the buildings within the site are also deleted.

Deleting Floors

When you delete a floor, it removes the selected floor and all wiring closets on that floor. All devices assigned to the floor or to the closets on that floor become unassigned and become available for reassignment. To delete a floor, select the floor in the network tree and click **Delete Floor**. Confirm the deletion to remove the objects and to disassociate the devices. If a site or building is deleted, the floors are also deleted.

Deleting Closets

When you delete a closet, it removes the selected closet and unassigns the devices in the closet. Those devices then become available for reassignment. To delete a closet,

Copyright © 2013, Juniper Networks, Inc.

select the closet in the network tree and click **Delete Closet**. Confirm the deletion to remove the objects and to disassociate the devices. If a site, building, or floor is deleted, the associated closets are also deleted.

Deleting Devices

At every node in the network tree, you can choose to delete devices directly.

BEST PRACTICE: **However, it is usually best to select the node directly above the device so that you do not accidently unassign more devices than desired.**

- Select the node (site, building, floor, or closet) directly above the device.
- Click **Delete Devices** to open the Delete Devices page.
- Click the plus signs to expand the node until you locate the device.
- Click one or more boxes to select the devices. If you do not navigate down to the device level and select a node at a higher level (such a closet or floor), the system selects all devices at and below the node.
- Click **OK** and confirm your selection to remove the assignment. The devices are moved to the Unassigned node of the network tree.

Related Documentation

- Understanding the Location View on page 63

Setting Up Closets

Use the Add Closet or Edit Closet tasks to create or change the name of a wiring closet. These tasks are visible only from a floor node in a building.

This topic describes:

- How to Add or Edit a Closet on page 412
- Adding or Editing a Wiring Closet on page 413

How to Add or Edit a Closet

To add or change a wiring closet:

1. Click the Build Mode icon

in the Network Director banner.
2. Select **Location View** from the list in the View pane.
3. Navigate to the building and floor where you are adding or changing the closet.
4. If you are adding a wiring closet:
   a. Select a building floor in the network tree to which you want to add a wiring closet.

      The Tasks pane refreshes to show your selected floor and the available tasks for the floor.

Copyright © 2013, Juniper Networks, Inc.

b. Click **Add Closet** in the Tasks pane.

5. If you are changing a wiring closet, click **Edit Closet** in the Tasks pane.
6. Type the closet name and click **Done** to save the configuration.

   The closet appears with the change in the network tree.

Adding or Editing a Wiring Closet

The Add Wiring Closet or Edit Wiring Closet pages allow you to name a wiring closet. Simply type the name of the new or changed wiring closet and click **Done** to submit the information to the system. Your network tree refreshes to show the wiring closet.

Related Documentation

- Understanding the Location View on page 63
- Configuring Floors on page 407
- Assigning and Unassigning Devices to a Location on page 403

Copyright © 2013, Juniper Networks, Inc.

Setting Up the Location View

You can build a new location site by the individual nodes, or you can use the Location Setup page. The wizard guides you though the top-down process from the site node down to the assignment of devices.

NOTE: **Use the Location Setup page only to design new sites; it is not meant for editing existing sites. If you enter data for an existing site, it is rejected when you attempt to commit the data.**

A site is the cornerstone of the location-based view of your network. Until you define a site, the default view of your network tree only shows you a list of your unassigned devices. After you define a site, you can build a tree structure of buildings, floors, wiring closets, aisles, and outdoor areas. As you define your network, you can assign devices to the various components of your network. Table 121 on page 414 describes the devices that you can assign to each of the location component.

Table 121: Devices that can be Assigned to each Location Component

Component	Devices that can be assigned
Site	None
Building	EX Series switches, QFX Series switches, QFabric components (Interconnects, Directors, Node devices, Control Plane devices), Wireless Controllers
Floor	EX Series switches, QFX Series switches, QFabric components (Interconnects, Directors, Node devices, Control Plane devices), Wireless Controllers, Access Points
Closet	EX Series switches, QFX Series switches, QFabric components (Interconnects, Directors, Node devices, Control Plane devices), Wireless Controllers
Aisle	None
Rack	EX Series switches, QFX Series switches, QFabric components (Interconnects, Directors, Node devices, Control Plane devices), Wireless Controllers
Outdoor Area	EX Series switches, QFX Series switches, QFabric components (Interconnects, Directors, Node devices, Control Plane devices), Wireless Controllers, Access Points

The Location Setup page displays the network tree as you add components to your network. Use the buttons on this page to add various components—such as, buildings, outdoor areas, floors, aisles, racks—to your network. These buttons change depending on the component that you select in the network tree.

After the location is set up, you can view the devices in the network by expanding and collapsing these location nodes in the Location view.

To set up your location view:

Copyright © 2013, Juniper Networks, Inc.

1. Ensure you are in the Build mode and Location or Topology view. Click **Build** in the Network Director banner to enter Build mode; select **Location** view or **Topology** view from the View selector.
2. If you are accessing the Location Setup page from the Location view, select the root node (for example, My Network) in the View pane.
3. Do one of the following depending on the view you are in:
   - From the Tasks pane in the Location view, select **Location Management** > **Setup Locations**.
   - From the Tasks pane in the Topology view, select **Location** > **Setup Locations**.

   The Location Setup page opens.
4. Click **Add Site** to add a new site.

   Network Director adds a new site under the root node and names it as **Site-1**.
5. Select the new site and perform any of the following actions:
   - Click **Edit Site** to modify the name of the site and specify the site address. The Edit Site window opens.

     Topology view uses this address to place the devices assigned to this site on the topology map. For more details on editing a site, see "Creating a Site" on page 409.
   - Click **Add Building** to add a building to your site.

     Network Director adds a new building under the site and names it as **Building-1**.
   - Click **Outdoor Area** to add an outdoor area to your site. Network Director adds a new outdoor area under the site and names it as **Outdoor Area-1**. You can associate an outdoor area to a site or a building for wireless coverage and upload an image or map of that area. After you designate an outdoor area, you can edit or view the map using the Edit Outdoor Area task.
   - Click **Delete** to delete the site.
6. If you added a building, select the building and perform any of the following actions to continue building your network:
   - Click **Add Floor** to add floors to the building.
   - Click **Assign Device** to assign devices to the selected building. The Associate Devices to Building window opens displaying all the unassigned devices in your network. Select the devices that you want to add to the building and click **Add**.

     Network Director adds the selected devices to the network tree.
   - Click **Edit Building** to edit the name and address of the building. For more details on editing a building, see "Configuring Buildings" on page 406.
   - Click **Delete** to delete the building.
7. If you added an outdoor area, select the outdoor area and perform any of the following actions to continue building your network:

Copyright © 2013, Juniper Networks, Inc.

- Click **Assign Device** to assign devices to the selected outdoor area. The Associate Devices to Outdoor window opens displaying all the unassigned devices in your network. Select the devices that you want to add to the building and click **Add**.
- Click **Edit Outdoor Area** to edit the name of the outdoor area and to upload the image of the outdoor area. For more details on editing an outdoor area, see "Configuring Outdoor Areas" on page 408.
- Click **Delete** to delete the building.

8. If you added a floor to the building, select the floor and perform any of the following actions to continue building your network:
   - Click **Add Closet** to add a wiring closet to the floor.
   - Click **Add Aisle** to add an aisle to the floor.
   - Click **Assign Device** to assign devices to the selected floor. The Associate Devices to Floor window opens displaying all the unassigned devices in your network. Select the devices that you want to add to the floor and click **Add**.
   - Click **Edit Floor** to modify the name of the floor, floor level and upload the floor plan. For more details on editing a floor, see "Configuring Floors" on page 407.
   - Click **Delete** to delete the floor.
9. If you added a wiring closet, select the wiring closet and perform any of the following actions:
   - Click **Assign Device** to assign devices to the selected closet. The Associate Devices to Closet window opens displaying all the unassigned devices in your network. Select the devices that you want to add to the closet and click **Add**.
   - Click **Edit Closet** to modify the name of the wiring closet. In the Edit Closet window, modify the wiring closet name and click **Done**.
   - Click **Delete** to delete the wiring closet.
10. If you added an aisle, select the aisle and perform any of the following actions:
    - Click **Add Rack** to add a rack to the aisle.
    - Click Edit Aisle to modify the name of the aisle. In the Edit Aisle window, modify the name and click **Done**.
    - Click **Delete** to delete the aisle.
11. If you added a rack, select the rack and perform any of the following actions:
    - Click **Assign Device** to assign devices to the selected rack. The Associate Devices to Rack window opens displaying all the unassigned devices in your network. Select the devices that you want to add to the rack and click **Add**.
    - Click **Edit Closet** to modify the name of the rack. In the Edit Rack window, modify the name and click **Done**.
    - Click **Delete** to delete the rack.
12. Click **Done** to save the location details.

Copyright © 2013, Juniper Networks, Inc.

Network Director displays the location details along with the assigned devices in the location view.

Related Documentation

- Understanding the Location View on page 63
- Deleting Sites, Buildings, Floors, Wiring Closets, and Devices on page 410
- Changing the Location of a Device on page 405
- Configuring Buildings on page 406
- Configuring Floors on page 407
- Setting Up Closets on page 412

Setting Up and Managing the Topology View

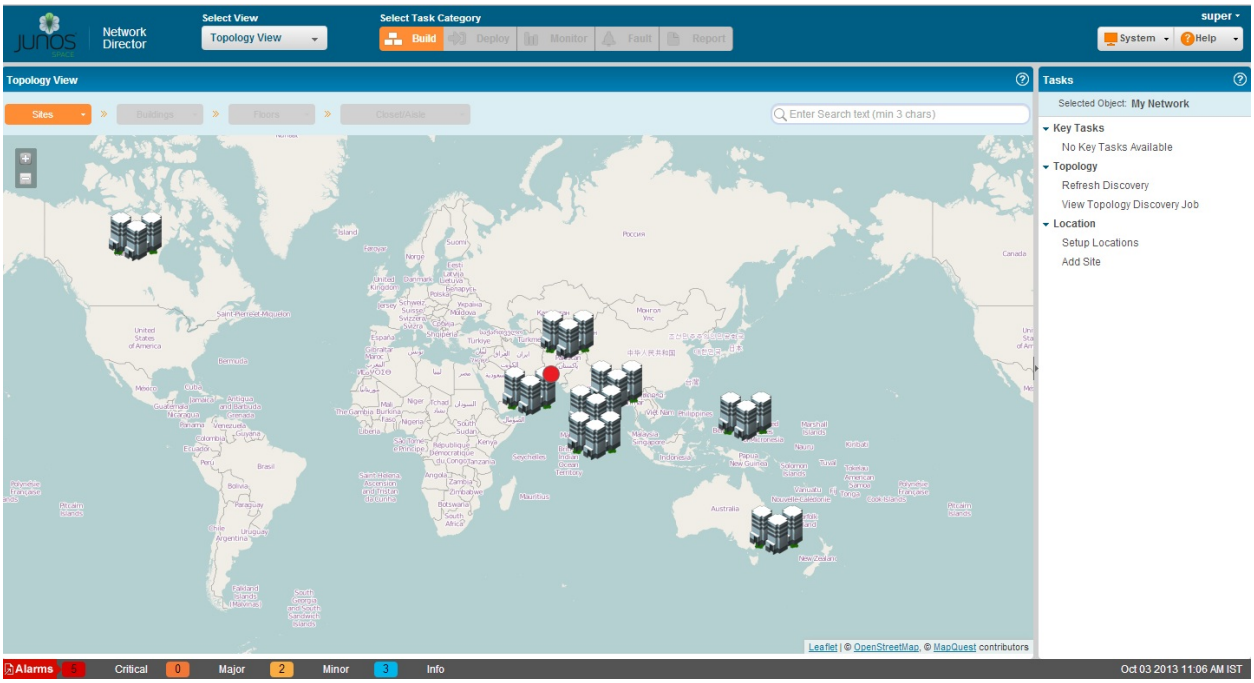
- Viewing the Network Topology on page 417
- Refreshing the Device Discovery on page 419
- Viewing Topology on page 420
- Viewing Topology Discovery Job on page 420
- Setting Up the Location View on page 421
- Viewing the Alarm Details on page 421
- Displaying Device Connectivity on page 422
- Displaying QFabric Connectivity on page 424
- Uploading Floor Plans on page 426
- Uploading Topology Map on page 426

Viewing the Network Topology

Topology View enables you to view all the discovered devices in your network, overlaid on a map. You can create sites, buildings, floors, outdoor areas, closets, and racks by using the Location wizard in the topology view. You can use the topology view to zoom in or zoom out of a site or a building. You can also see the connectivity between a device and its immediate neighbors, alarms details, port details, and so on. An example of how the topology map looks like after you have added the location details is shown in Figure 16 on page 418.

Copyright © 2013, Juniper Networks, Inc.

Figure 16: Main Topology Window



The topology display is created by layering the device images on top of the imported floor plan images.

After you access the topology view from View pane, you can select your location on the map by using one of the following methods:

- Optical Zoom: You can zoom in or zoom out to get a detailed or high-level view.
- Pan: Network Director enables you to pan the topology and allows you to move the devices to different parts on the topology by holding the mouse button down and dragging to a specific part of the map.

  Network Director displays the sites, buildings, and geographical coordinates on the topology map based on the address specified while setting up the locations. However, you can move the devices around to another location by selecting, dragging, and dropping the device to the correct location. For example, you can move a site from a US site to a Bangalore site on the topology using the pan feature. This helps to determine the correct location of a site because while setting up the location details, it is not mandatory to provide the address information.
- Search and Locate: You can search for all nodes such as sites, building, floors, specific devices, all devices in a floor, and so on by entering a search keyword or the complete name of the device in the Search field. On entering the search criteria, you might see the list of nodes or just one node based on the search criteria. When you select the node, Network Director locates the node and the topology view is panned to ensure the selected node is centered on the page. In cases where a device is at the edge of the map the corner is aligned accordingly to bring device in view.

Copyright © 2013, Juniper Networks, Inc.

- Mouse Hover on a Device: If you mouse over a device, the device gets highlighted and Network Director displays the IP address and the fault alarm details.
- Highlight and select Show Device Connectivity: Select a device and click **Show Device Connectivity** to highlight the device's connectivity with other devices. The device images are displayed along with details such as name, IP address, and the connectivity link between the devices.
- Use the navigation breadcrumbs at the top of the page to navigate through sites, buildings, floors, closets, or aisles.

Refreshing the Device Discovery

You can refresh the devices discovered and managed by Network Director from the Tasks pane in the Topology View. You can add the Refresh Discovery task to the Key tasks in the topology view if you would use this task frequently.

To refresh the device discovery process:

1. Click **Refresh Discovery** from Key Tasks or Topology task.

   The Refresh Discovery pop-up window is displayed along with the SNMP details specified that you specified while specifying the discovery options in the Device Discovery task page.

   If you have not specified the SNMP details while discovering the devices, proceed to Step 3.

2. Select the **SNMP version** from the SNMP version table and click **Discover**. The Refresh Topology window is displayed along with the details.
3. If SNMP version details are not displayed in the SNMP version table, click **Add** on the Refresh Discovery pop-up window.

   The Add SNMP Settings dialog box is displayed.

   Select either **SNMP V1/V2C** or **SNMP V3**. Based on the selection, you need to enter the details as follows:

   - If you selected SNMP V1/V2C, specify a community string, which can be *public*, *private*, or a predefined string.

     Click **Add** in the Add SNMP Settings dialog box or click **Add More** to add more strings to the community. If you click **Add More**, when you are done adding all the strings, click **Add** to save the SNMP settings for V1/V2C.

   - If you selected SNMP V3, specify the following:
     - Enter a username
     - Select the privacy type (AES 128, DES, or None).
     - Enter the privacy password (if AES 128 or DES). If you specify none for the privacy type, the privacy function is disabled.
     - Select the authentication type (MD5, SHA, or none).

Copyright © 2013, Juniper Networks, Inc.

- Enter the authentication password (if MD5 or SHA). If you specify none for the authentication type, the authentication function is disabled.
- Click **Add** to save the SNMP settings and close the dialog box, or click **Add More** to add additional configurations. If you clicked Add More, click **Add** to save the settings and close the dialog box.

The specified details are displayed in the SNMP version table.

4. Click **Discover**. The Refresh Topology window is displayed along with the details.

Viewing Topology

The Refresh Topology pop-up window displays the refresh device discovery job details as described in the Table 122 on page 420.

Table 122: Refresh Topology Job Details

Field	Description
Job Name	The Refresh topology job name along with the Job ID.
Start Time	The time at which the refresh discovery job is initiated.
End Time	The time at which the refresh discovery job is completed.
Percentage Progress	Displays the progress of the job in percentage. When the job is completed, displays 100 percentage.
Status	The status of the job. The status is *In Progress* until the job is completed.
Target Devices Count	The total number of targets for the discovery of devices.
Discovered Devices Count	The total number of discovered devices for which the SNMP parameters are specified. NOTE: In the Topology View, you can view the network connections of only those discovered devices for which LLDP, SNMP, and STP parameters are set.
Discovered Subnets Count	The total number of subnets discovered.
Targets	The Targets table displays the Management IP addresses of the devices discovered along with the status of the discovery process.

Use the right and left arrows to navigate through the discovered pages. You can specify the details to be displayed in a page by selecting the **show items** list box and specifying the number of items to be displayed in one page.

Click **Close** to close the Refresh Topology page and return to the main Topology page.

Viewing Topology Discovery Job

To view the discovery jobs in the topology view, click **View Topology Discovery Job**. The Topology Discovery Jobs window opens displaying details of the topology related jobs

Copyright © 2013, Juniper Networks, Inc.

as described in Table 123 on page 421. To view any hidden column, keep the mouse on the column heading, select the down arrow, and then click **Columns**. Select the check box to display the hidden columns.

Table 123: Job Details for Topology Discovery

Field	Description
Job ID	For each job-based task, the audit log includes a job ID.
Job Name	The name of the job.
Percent	The percentage of completion of the job.
State	The status of the job: • Success—Job completed successfully • Failure—Job failed and was terminated • Job Scheduled—Job is scheduled but has not yet started • In progress—Job is has started, but not completed • Cancelled—Job is cancelled
Summary	Summary of the job scheduled and executed with status.
Scheduled Start Time	The UTC time on the client computer when the job is scheduled to start.
Actual Start Time	The actual time when the job started.
End Time	The time when the job was completed.
User	The login ID of the user that initiated the task.
Recurrence	The recurrent time when the job will be restarted.

To view the details of a topology discovery job, select a row and click **Show Details**. To cancel a scheduled job, select a job that is scheduled for a later time or a job that is in progress and click **Cancel**.

Setting Up the Location View

To set up the location view, see "Setting Up the Location View" on page 414.

Viewing the Alarm Details

You can view the alarm details at site, building, floor, closet, aisle and rack levels. Based on the location node, the alarms are aggregated and displayed. That is, all the alarms for a particular building is aggregated and displayed at the building level. The alarms are indicated by red, orange, yellow, and blue balls indicating critical, major, minor, and info alarms. To view the Alarm details for a device, navigate down to the device level, select a device, and click one of the following options from Alarm in the Tasks pane:

Copyright © 2013, Juniper Networks, Inc.

- Show Alarms By Severity, see *Alarms by Severity Monitor*
- Show Alarms By Category, see *Alarms by Category Monitor*
- Show Alarms By State, see *Alarms by State Monitor*
- Show Current Active Alarms, see *Current Active Alarms Monitor*

Displaying Device Connectivity

At the device level, you can view the connectivity details of a device and the details of all the devices that are connected to the specified device by using the Topology View in Network Director. It also displays the connection details of assigned and unassigned devices located in different floors and buildings that are connected to the specified device.

To view the connectivity details of a device:

1. In the Topology View, navigate to a device in a building, floor, outdoor area, closet or rack and select the device for which you want to view the connectivity details.

   The Show Device Connectivity task is displayed in Topology in the Tasks pane.

   NOTE: **The Show Device Connectivity task is available only after you select a device.**

2. Click the device. The selected device is highlighted by a green colored rectangle.
3. Click **Show Device Connectivity** from Topology under the Tasks pane. You can view the device connectivity details either in a graphical view or in a grid view. The default view is in graphical form.

   The device is displayed at the center of the page and its network connectivity to all the connected devices are displayed as in Figure 17 on page 423 in the graphical view. Mouse over on a device to view the port details of the highlighted device. Figure 18 on page 423 represents the network connectivity in grid view.

Copyright © 2013, Juniper Networks, Inc.

Figure 17: Displaying the Connection Details for an EX4200 Switch in Graphical View

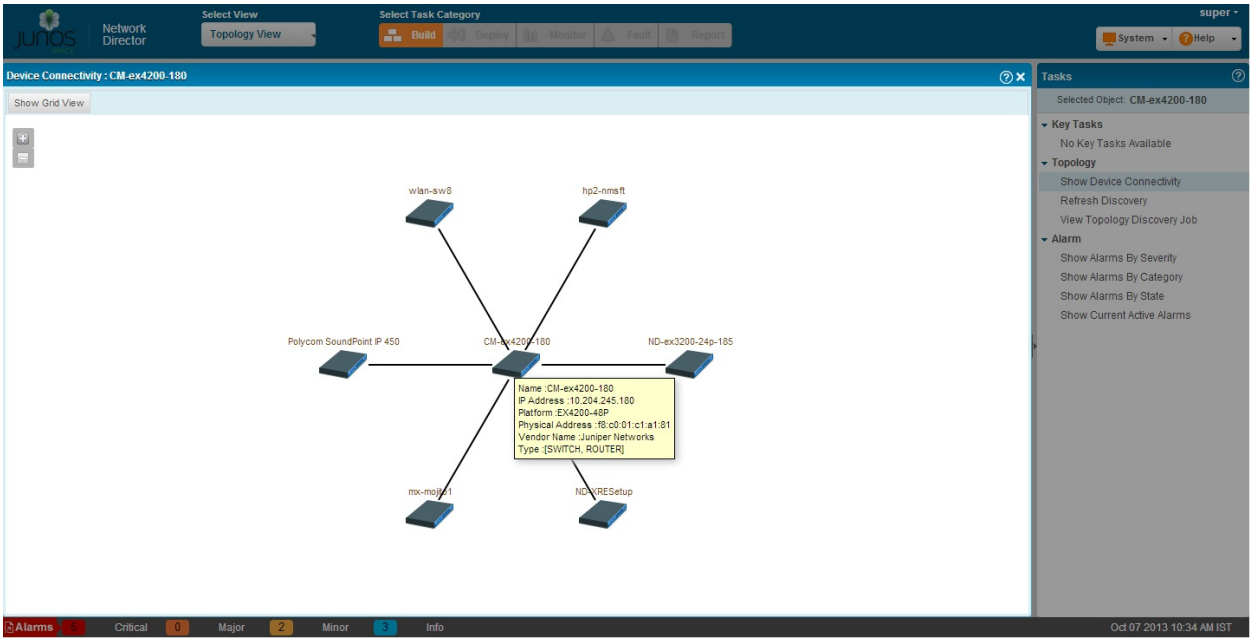
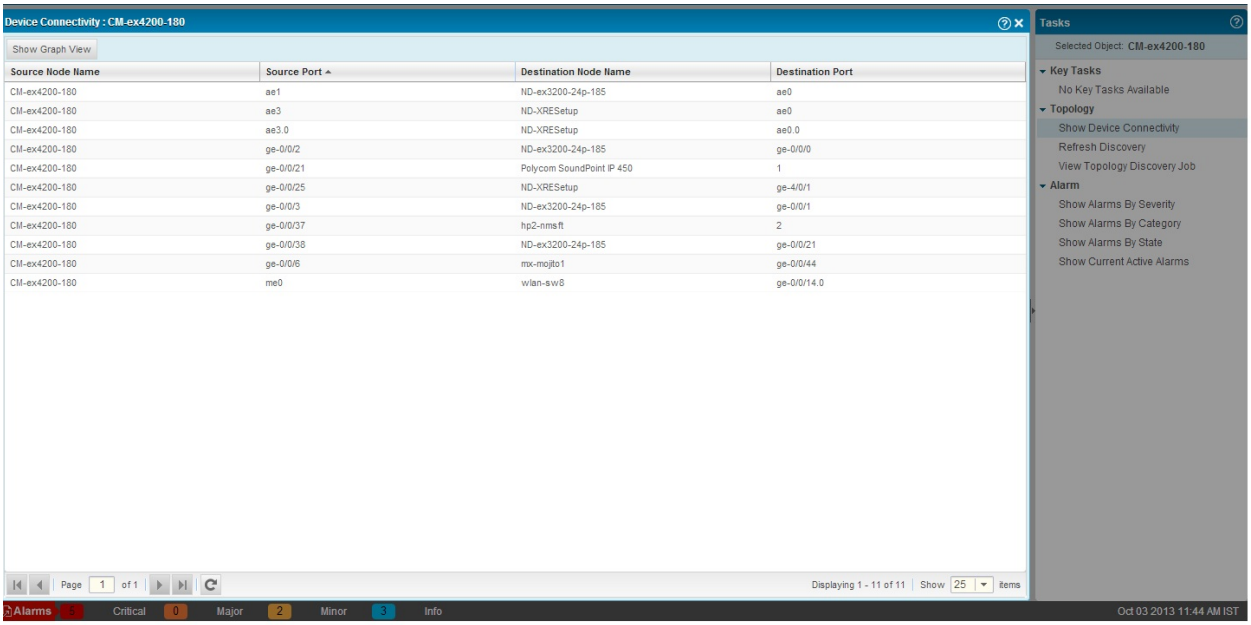


Figure 18: Displaying the Connection Details for an EX4200 Switch in Grid View



If the selected device is connected to more than sixty devices, then all the connected devices are highlighted in a circular form or a grid form. If the selected device is connected to less than 60 devices, then the links between the interconnected devices are displayed.

Copyright © 2013, Juniper Networks, Inc.

The device images are displayed along with details such as name, IP address, and alarm state information in colored labels that provide health and reachability information.

The following details are displayed for each device, if the details are configured on the device:

- Name: The name of the device provided while configuring the device. The device name is displayed as a label.
- IP: The IP address of the device.
- Family: The family or platform to which the device belongs to. It can be an EX Series switch, QFX Series Switch, Wireless LAN Controller, and access point.
- Serial Number: Physical address or MAC address of the device for switches and controllers.
- Alarms: The alarm details displaying the number of critical, major, minor alarms, or info for the device.

4. Click **Show Grid View** to view the device connectivity details in a tabular format as displayed in Figure 18 on page 423.

   The following details are displayed in the table:

   - Source Node Name: Name of the device specified at the time of configuring the device.
   - Source Port: source port of the device.
   - Destination Node Name: Name of the device or devices the device is connected to.
   - Destination port: The port number on the destination device to which the source device is connected to.

   You can sort the details in the table in the ascending order or descending order for each column. You can also use filters to display only the desired device connectivity details.

Displaying QFabric Connectivity

You can view the QFabric devices available in your network by navigating to the rack, closet, or floors from the Topology View. Alternatively, you can search for the QFabric devices by entering a search criteria in the Search field. You can also assign the QFabric devices to a rack, closet, or floor from the topology view.

You can view the connection details of the QFabric Interconnects with the nodes by using the Topology View.

To view the connection details of the QFabric devices:

1. In the Topology View, navigate to the floor, rack, or closet level from **Site** and **Building**.
2. Click the device for which you want to view the connectivity details. The selected device is highlighted by a green colored rectangle.

Copyright © 2013, Juniper Networks, Inc.

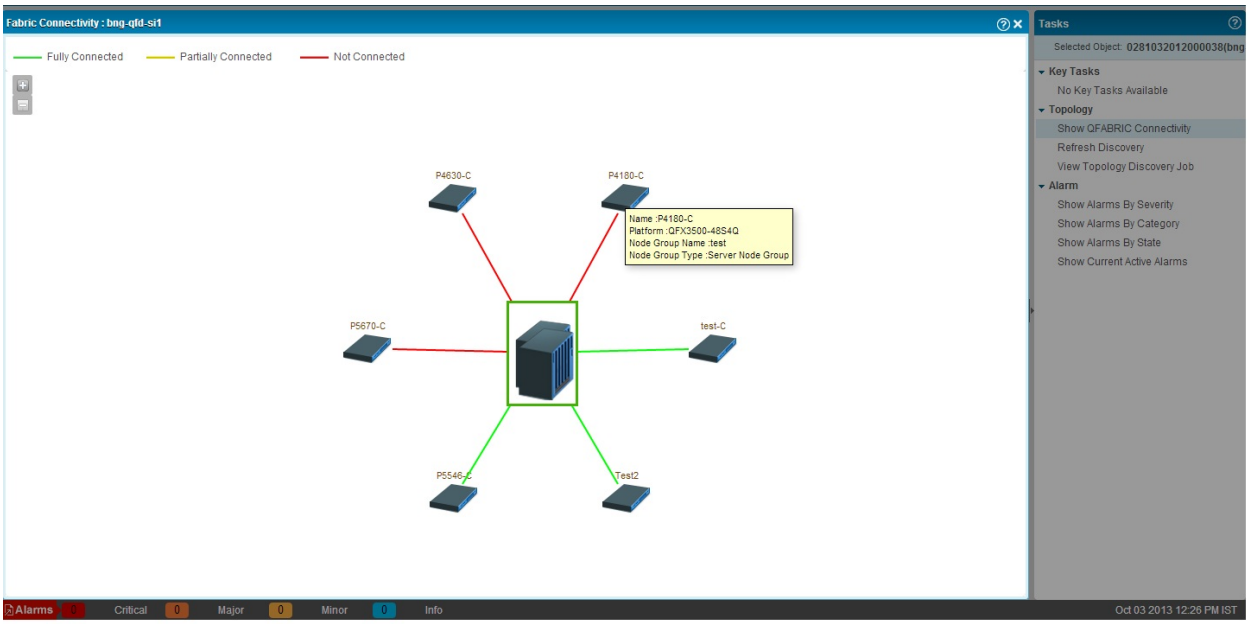
The Show QFabric Connectivity task is displayed under Topology menu in Tasks pane.

NOTE: **The Show QFabric Connectivity task is available only after you select a device.**

3. Click **Show QFabric Connectivity** from Topology under the Tasks pane. You can view the QFabric connectivity details either in a graphical view.

   The QFabric Interconnect is displayed at the center of the page and its network connectivity to all the connected nodes are displayed as in Figure 19 on page 425. Hover the mouse on a device to view the port details of the highlighted device.

Figure 19: Displaying the Connection Details for a QFabric Switch in Graphical View



In the Figure 19 on page 425, the connection details are represented by green, yellow, and red lines.

- The green line indicates that the node is connected to all the Interconnects properly and all functions are normal.
- The yellow line indicates that the node is only partially connected to the Interconnect. That is, the node may be connected to one Interconnect, but not all the Interconnects.
- The red line indicates that the node is not connected to any of the interconnects.

The following details are displayed for each device, if the details are configured on the device:

Copyright © 2013, Juniper Networks, Inc.

- Name of the device provided while configuring the device. The device name is displayed as a label.
- Platform of the device. It can be QFX3500 or QFX3600 switches.
- Node group name. The name of the node group to which this device belongs to.
- Node group type. The server name of the node group to which this device belongs to.
- Source Port: source port of the device.
- Destination port: The port number on the destination device to which the source device is connected to.

Uploading Floor Plans

You can upload the floor plan from the Topology View if you already have a floor plan for a specified building in a site.

To upload the floor plan:

1. Select a **Site** > **Building** > **Floor**. Alternatively, create a site, building, and floor. Click the **Upload Floor Plan** task from the Location task in the Tasks pane.

   The Upload Floor Plan dialog box is displayed.
2. Click **Browse** next to Image File to choose a floor plan file.
3. Navigate to the folder where you have saved the floor plan on your system and click **Open**.
4. Click **Upload** to upload the floor plan image.
5. Click **Cancel** if you do not want to upload the floor plan and quit the Upload Floor Plan dialog box.

Uploading Topology Map

You can upload a topology map for an outdoor area from the Topology View.

To upload the map:

1. Select a **Site** > **Outdoor area**. Alternatively, create an outdoor area within a site. Click the **Upload map** task from the Location task in the Tasks pane.

   The Upload Map dialog box is displayed.
2. Click **Browse** next to Image File to choose a map file.
3. Navigate to the folder where you have saved the topology map for an outdoor area on your system and click **Open**.
4. Click **Upload** to upload the topology map image.
5. Click **Cancel** if you do not want to upload the map and quit the Upload Map dialog box.

Copyright © 2013, Juniper Networks, Inc.

Related Documentation

- Discovering Devices in a Physical Network on page 455
- Setting Up the Location View on page 414
- Understanding the Network Topology in Network Director on page 65

Copyright © 2013, Juniper Networks, Inc.

Copyright © 2013, Juniper Networks, Inc.

CHAPTER 11

Virtual View Configuration

- Guidelines for Migrating from Virtual Control to Network Director on page 430
- Discovering Devices in a Virtual Network on page 430
- Managing Virtual Networks on page 434
- Viewing the Virtual Machine Inventory in a Virtual Network on page 437
- Viewing the Virtual Switch Inventory in a Virtual Network on page 438
- Viewing the Host Inventory in a Virtual Network on page 439
- Managing Network Adapter Associations on page 440
- Viewing Connections Between Virtual Machines and a Physical Switch on page 443
- Viewing Virtual Port Groups on page 444

Copyright © 2013, Juniper Networks, Inc.

Guidelines for Migrating from Virtual Control to Network Director

Use the following guidelines for migrating from Junos Space Virtual Control to Network Director

- Uninstall Virtual Control from the Junos Space appliance.
- Download the Virtual Control cleanup script and run it from the Junos Space console.

  This must be done before you install Network Director Release 1.5 on the Junos Space appliance.
- Install Network Director.
- Import the virtual network inventory—Use the virtual network discovery to discover the vCenter from Network Director. You must specify the IP address, username and password for the vCenter server while performing the discovery. For detailed steps, see "Discovering Devices in a Virtual Network" on page 430.
- Set up physical switch to host associations—If the virtual distributed switch uses Version 5.0 or later, and if LLDP is enabled both on the virtual switch and the physical switch, then Network Director discovers the associations automatically. But, if the virtual switch uses a Version earlier than 5.0 or if it is standalone virtual switch, then you must manually set up the physical switch to host associations. For detailed steps, see "Managing Network Adapter Associations" on page 440.
- Virtual Switch and Port Group profiles—Network Director Release 1.5 does not support virtual switch and port group profiles. So it is not necessary to import this data in to Network Director.

Related Documentation

- Understanding Virtual Network Management on page 72

Discovering Devices in a Virtual Network

You use virtual network discovery to add virtual networks to Network Director. Discovery is the process of finding and adding a virtual network (VMWare vCenter server) and then synchronizing its inventory and configuration with Network Director. To use virtual network discovery, Network Director must be able to connect to the vCenter server.

When discovery succeeds, Network Director creates an object in its database to represent the vCenter server and maintains a connection between the object and the vCenter server to maintain the information flow.

When configuration changes are made on the vCenter server, Network Director automatically resynchronizes with the vCenter server so that the inventory information in the Junos Space database matches the current vCenter server inventory and the configuration information. You can also manually synchronize the vCenter server configuration changes to the configuration stored in the corresponding Network Director object.

Copyright © 2013, Juniper Networks, Inc.

At a high level, the following vCenter server inventory and configuration data is captured and stored in relational tables in the Junos Space database:

- Virtual Switches: Port groups, interfaces, VLANs, and other configuration details such as QoS parameters, teaming, and failover details
- Hosts: Physical NICs and virtual machines
- Virtual Machines: Virtual adapters and their associations

Virtual network discovery is a three-step process in which you specify the target devices, the credentials of devices to be discovered, and review the discovery options.

While in Build mode with Virtual view selected, from the Tasks pane, click **Discover Virtual Network** from Virtual Network Management menu. The Discover Virtual Network page is displayed.

This topic describes:

- Specifying the vCenter Targets on page 431
- Specifying the Virtual Network Credentials on page 432
- Reviewing the Virtual Network Discovery Options on page 432
- Viewing the Discovery Status on page 433

Specifying the vCenter Targets

You can add VMware vCenter servers to Network director by specifying the hostname or the IP address of one or more vCenters.

To specify the target devices that you want Network Director to discover:

1. In the vNetwork Targets and Credential tab, enter a name for the virtual network discovery job. The default name is vNetwork Discovery.
2. Click **Add** in the vNetwork Targets table.

   The Add vNetwork Target dialog box appears.
3. Choose one of the following options to specify the target vCenter server that you want to discover:
   - Select the **IP** option and enter the IP address of the vCenter server.
   - Select the **HostName** option and enter the hostname of the vCenter server.
4. Specify the port that Network Director uses to connect to the vCenter server. The default port is 443.

NOTE: You can modify this and specify a port of your choice. If you do so, make sure to manually change the Junos Space firewall settings and apply to this port.

Copyright © 2013, Juniper Networks, Inc.

5. Click **Add** to save the target vCenter server that you specified, or click **Add More** to add more target vCenter servers. When you have added all target devices that you want Network Director to discover, click **Add**.

   The vNetwork Targets table displays the addresses of the configured target devices.

6. • To edit a target vCenter server, select a row from the vNetwork Targets table and click **Edit**. Make the required changes and click **Add** to display the changes in the vNetwork Targets table.

   • To delete a target vCenter server, select a row from the vNetwork Targets table and click **Delete**.

7. Click **Next** or **vNetwork Credentials** from the top wizard workflow to go to the vNetwork Credentials page. Specify the options as described in the "Specifying the Virtual Network Credentials" on page 432.

Specifying the Virtual Network Credentials

1. Add the vCenter server credentials. To add the credentials, click **Add** from the Device Credentials table.

   The Add vNetwork Credentials dialog box is displayed.

   • Specify the administrator username and password, and confirm the password. The username and password must match the name and password configured on the device. The username is a mandatory field.

   • Click **Add** to save the username and password that you specified or click **Add More** to add another username and password.

   Click **Add** after you have finished adding all login credentials. The Device Credentials table displays the usernames that you configured.

2. Click **Next** or click **Review** from the top wizard workflow to go to the Review page.

Reviewing the Virtual Network Discovery Options

From the review page, you can save or make changes to the virtual network discovery options.

- To make changes to the virtual network discovery options, click the **Edit** button associated with the configuration you want to change.

  Alternatively, click the appropriate buttons in the profile workflow at the top of the page that corresponds to the configuration you want to change.

  When you are finished with your modifications, click **Review** to return to this page.

- Click **Finish** when you are done with the configurations.

  A message window opens, displaying the status of the virtual network discovery job name and job ID. Click **OK**.

  You can view the status of the discovery job in the Virtual Network Discovery Jobs page.

Copyright © 2013, Juniper Networks, Inc.

Viewing the Discovery Status

After you have configured the virtual network discovery options, you can view the discovery status from the **View Discovery Status** option from the **virtual network discovery** menu.

The **Virtual Network Discovery Jobs** page displays all the discovery jobs. You can view the following details from the Virtual Network Discovery Jobs page as described in Table 124 on page 433.

Table 124: Viewing Device Discover Jobs

Field	Description
Job ID	An identifier assigned to the job.
Job Name	The name of the job (user-created).
Percent	Percentage of the job that is complete.
Status	Job status. The possible states are: • CANCELLED—The job was cancelled by a user. • FAILURE—The job failed. This state is displayed if any of the devices in the job failed. But some of the devices might have completed successfully. View the job details for the status of each device. • INPROGRESS—The job is running. • SCHEDULED—The job is scheduled but has not run yet. • SUCCESS—The job completed successfully. This state is displayed if all of the devices in the job completed successfully.
Summary	Summary of the job scheduled and executed with status.
Scheduled Start Time	The UTC time on the client computer when the job is scheduled to start.
Actual Start Time	The actual time when the job started.
End Time	The time when the job was completed.
User	The login ID of the user that initiated the job.
Recurrence	The recurrent time when the job will be restarted.

To view the details of a job, select the check box against Job ID or Job Name and click **Show Details**. The Discover Network Elements window displays details of the virtual network discovery job.

Copyright © 2013, Juniper Networks, Inc.

NOTE: During virtual network discovery, if Network Director is unable to read the device configurations, then the status displays Failed state. For such failures, you can check the reason for failure from the Manage Jobs page in System mode. You must make the required changes to the device configuration using the CLI so that Network Director can read the configuration. Network Director automatically resynchronizes once you enable a virtual network discovery job. If Network Director cannot discover the device even after resynchronization, then you must rediscover the device after making the appropriate changes in the device configurations using the CLI.

Related Documentation

- Troubleshooting Device Discovery Error Messages on page 485

Managing Virtual Networks

You can view information about all the VMware vCenter servers managed by Network Director in the Manage Virtual Networks page. Network Director uses information from the virtual network to create an inventory view with a detailed list of all the elements in each virtual network. This includes the name of the vCenter server, the hostname or the IP address, ESXi version that is running on the vCenter server, the connection status, and the current orchestration mode.

While in Build mode with Virtual view selected, from the Tasks pane, click **Manage Virtual Networks** from Virtual Network Management menu to open the Manage Virtual Networks page. You can do the following from the Manage Virtual Networks page:

- Modify Virtual Network Details on page 434
- Configure Orchestration Mode on page 435
- Delete Virtual Networks on page 436
- Resynchronize Virtual Networks on page 436

Modify Virtual Network Details

You can modify some of the details of an existing virtual network.

To modify credentials for a virtual network:

1. Select the virtual network that you want to modify and click **Edit**.

   The Edit Virtual Network dialog box is displayed.

2. Modify the fields, as explained in Table 125 on page 434.

Table 125: Modify Virtual Network Credentials Field Descriptions

Field	Description
Virtual Network Name/IP Address	Name or IP address of the host machine to be used as the VMWare vCenter server. This field cannot be modified.

Copyright © 2013, Juniper Networks, Inc.

Table 125: Modify Virtual Network Credentials Field Descriptions *(continued)*

Field	Description
Port	Port used for connection. The default value is 443. NOTE: You can modify this and specify a port of your choice. If you do so, make sure to manually change the Junos Space firewall settings to allow for this port.
Username	Username to be used to connect to the VMWare vCenter server.
Password	Password to be used with the name provided in the previous field.
Confirm password	Repeat the password provided in the previous field to confirm.

3. Click **Modify** to submit the changes that you made.

Configure Orchestration Mode

Orchestration applies aggregated VLAN configurations (including private VLAN) of the required port groups to the appropriate ports of the physical switch. Using Network Director, you can seamlessly orchestrate across physical and virtual network elements.

Each virtual switch can span across one or more hosts and is configured to have a minimum of one uplink port per host. A distributed virtual switch can span across multiple hosts, whereas a standalone virtual switch can be associated with only one host. A virtual switch comprises one or more port groups each of which is a collection of ports. Each of these ports can, in turn, be associated with a virtual machine or host kernel. Traffic coming from these ports is sent out of one of the uplink ports of the virtual switch, which is configured on the same host where the virtual machine or kernel resides.

Each physical NIC in a host is connected to an access port in the physical switch. Any configuration or restrictions that needs to be applied to the physical NIC to manage traffic is applied to the access port of the physical switch.

To set the orchestration mode operable on the virtual network:

1. Select a virtual network and click **Configure Orchestration**.

   The **Orchestration Mode** dialog box is displayed.

2. Select if you want to enable or disable orchestration for the virtual network.

NOTE: When you select value, the description field displays a short description about your selection. We recommend that you read this carefully before making a choice.

3. Click **OK** to set the virtual network to the desired orchestration mode.

Copyright © 2013, Juniper Networks, Inc.

Network Director displays a message to indicate the successful modification of orchestration mode.

Network Director tracks the status of orchestration using an orchestration job. After an orchestration job is completed successfully, you must manually resynchronize the physical switch's configuration with Network Director. If the system of record (SOR) mode set for the Junos Space Network Management Platform is:

- Network as system of record (NSOR), then performing a resynchronization ensures that Junos Space automatically resynchronizes its configuration record to match the device configuration and sets the device configuration state to In Sync when the synchronization completes. For more details, see *Resynchronizing Device Configuration*.
- Junos Space as system of record (SSOR), then you must perform a resynchronization and accept the out-of-band changes. Both the Junos Space configuration record and the Network Director Build mode configuration are resynchronized to reflect the out-of-band configuration changes. For more details, see *Resynchronizing Device Configuration*

Delete Virtual Networks

You can dissociate a virtual network from Network Director by deleting it from the system.

To delete a virtual network:

1. Select a virtual network and click **Delete**.

   Network Director displays the Delete Virtual Network dialog box.

2. In the Delete Virtual Network dialog box, click **Delete** to delete the virtual network from Network Director.

Resynchronize Virtual Networks

You can resynchronize virtual networks registered with Network Director. During resynchronization, the vCenter configuration replaces the corresponding configuration available in Network Director. Any changes that you may have made to the vCenter using Network Director may be lost after a resynchronization.

Synchronization is run as a job and is managed by the Job Manager in Network Director.

To initiate resynchronizing:

1. Select a virtual networks and click **Resynchronize**.

   The **Status** dialog box is displayed with the corresponding Job ID.

2. In the **Job Information** dialog box, click the job ID link.

   The **Job Details** page displays details about the resynchronization job.

Related Documentation

- Understanding Virtual Network Management on page 72
- Discovering Devices in a Virtual Network on page 430

Copyright © 2013, Juniper Networks, Inc.

Viewing the Virtual Machine Inventory in a Virtual Network

You may be having one or more virtual machines configured on a host machine. Once you have discovered a VMware vCenter in Network Director, the hosts, virtual machines and virtual switches also come under the Network Director management. You can use the View virtual machine inventory task to view details of virtual machines.

You can also view the network connectivity of a virtual machine with the host, virtual switch and physical switch from this page.

To view the virtual machine Inventory:

1. While in Build mode with Virtual view selected, do one of the following:
   - Click **Inventory > View Virtual Machine** from the Tasks pane to view details of all the virtual machines in your virtual network.
   - Select a host from the Virtual view and click **Inventory > View Virtual Machine** from the Tasks pane to view details of the virtual machines that belong to the selected host.
2. The Virtual Machine Inventory table displays the details for all the virtual machines. Table 126 on page 437 describes the fields in this table:

Table 126: Manage Virtual Machines Page Field Descriptions

Field	Description
Name	Name assigned to the virtual machine.
Host	Name of the host on which the virtual machine is running. This field is not available if you access the View Virtual Machine page for a specific host.
Virtual Network	Name of the virtual network to which the host belongs.
Guest Operating System	The operating system that is installed and running on the virtual machine.
IP Address	IP address of the virtual machine
MAC Address	The MAC address of the virtual machine.
Connection Status	The connection status of the virtual machine.
Power Status	Indicates if the virtual machine is powered on or off.

3. To view the network connectivity of a virtual machine, select the virtual machine and click **Show Network Connectivity**.

   The Network Connectivity page opens displaying the network connectivity and VLAN associations for the selected virtual machine. For more details, see "Viewing Connections Between Virtual Machines and a Physical Switch" on page 443.

Copyright © 2013, Juniper Networks, Inc.

Related Documentation

- Understanding Virtual Network Management on page 72

Viewing the Virtual Switch Inventory in a Virtual Network

Using virtual switches, virtual machines on the different hosts can communicate with each other using the same protocols that would be used over physical switches, without the need for any additional networking hardware. Once you have discovered a VMware vCenter in Network Director, the hosts, virtual machines and virtual switches also come under the Network Director management. You can use the View virtual switch inventory task to view details of all the virtual switches in your virtual network infrastructure.

To view the virtual switch Inventory:

1. While in Build mode with Virtual view selected, click the Virtual Center for which you want to view the virtual switch inventory details. From the Tasks pane, click **View Virtual Switches** from the Inventory menu to open the View Virtual Switches page.
2. The virtual switch inventory table displays the details for all the virtual switches in the Network. Table 127 on page 438 describes the fields in this table:

Table 127: Manage Virtual Switches Page Field Descriptions

Field	Description
Name	Name assigned to the virtual switch. If it is a standalone virtual switch, the hostname on which the vSwitch resides is also displayed.
Version	Indicates the vSphere version.
Type	The type of virtual switch. The switch type can be: • Standalone vSwitch—The traditional virtual switch where the administrator configures and maintains a virtual switch for each host. • Distributed vSwitch— A distributed switch spans multiple hosts at the virtual network level. It is created by abstracting individual host-level virtual switches into a single large distributed switch. This considerably simplifies the virtual machine networking by enabling you to set up virtual machine access switching for your entire datacenter from a centralized interface.
MTU	Maximum Transmission Unit—The maximum size of a protocol data unit that can be transmitted.
Number of Ports	Total number of ports held in the port groups configured for this switch.
LLDP Status	Indicates if Link Layer Discovery Protocol (LLDP) is enabled on the given virtual switch.

Copyright © 2013, Juniper Networks, Inc.

Table 127: Manage Virtual Switches Page Field Descriptions *(continued)*

Field	Description
LLDP Operation	If LLDP is enabled, this field indicates the LLDP operation mode. The operation mode can be one of the following: • **Listen**—Detects and displays information about the associated physical switch port, but information about the vSphere distributed switch is not available to the physical switch. • **Advertise**—Makes information about the vSphere distributed switch available to the physical switch, but does not detect and display information about the physical switch. • **Both**—Detects and displays information about the associated physical switch and makes information about the vSphere distributed switch available to the physical switch. • **Not applicable**—Indicates that LLDP is not enabled. NOTE: If you plan to use the Orchestration and Topology features extensively, then we recommend that you set the LLDP operation mode to Both.

Related Documentation

- Understanding Virtual Network Management on page 72

Viewing the Host Inventory in a Virtual Network

The host inventory displays a list of all the virtual machines on a host and the physical NICs that serve the virtual infrastructure.

The Manage Hosts page lists all the hosts in the infrastructure. For each host, the detailed inventory provides information about the port number of each virtual machine in the host along with its MAC address, virtual switch, and the virtual network it belongs to.

To view the host inventory:

1. While in Build mode with Virtual view selected, click the Virtual Center for which you want to view the host inventory details. From the Tasks pane, click **View Hosts** from the Inventory menu to open the View Hosts page.

The Host Inventory table displays the host inventory details. Table 128 on page 439 describes the fields in this table:

Table 128: Manage Hosts Page Field Descriptions

Field	Description
Host	Name or the IP address of the host.
Number of PNICs	Total number of physical NICs existing on the host.
Number of VMs	Total number of virtual machines existing on the host.

Copyright © 2013, Juniper Networks, Inc.

Table 128: Manage Hosts Page Field Descriptions *(continued)*

Field	Description
Connection State	One of the following: • Connected—The host is connected to the vCenter server. • Disconnected—The user has explicitly taken down the host and the host is not connected to the vCenter server. • Not responding—The host is connected to the vCenter server, but the server is not receiving heartbeats from the host. The connection state automatically changes to Connected when heartbeats are received again.
Maintenance Mode	Indicates whether the host is in maintenance mode or not.
Datacenter	Name of the data center on which the host resides.
Virtual Network	Name of the virtual network on which the host resides.
Vendor	Name of the hardware vendor of the host.
Model	Name of the host hardware model.
Type	Type of hypervisor. For example, ESX/ESXi, which is the hypervisor for the VMware.

Related Documentation
- Understanding Virtual Network Management on page 72

Managing Network Adapter Associations

Network Director enables you to configure and view the connectivity or association between a host network adapter and the corresponding physical network adapter on the physical switch. If LLDP is enabled on the physical switch and the virtual switch, Network Director automatically discovers and displays the host network adapter to physical network adapter connection. However, if LLDP is not enabled, you must manually configure these connections by importing the connection details in to Network Director.

You can automate orchestration using Network Director only if the host to physical switch connectivity is established. Using the Manage Physical Switch Association table, you can view the connectivity between a host network adapter and a physical switch port. You can also view the virtual switch that is bound to the given host network adapter. If any of the host network adapters is not connected to a corresponding the physical switch port, then follow the steps mentioned in "Configure Network Adapter Associations" on page 441 to manually configure network adapter associations.

After you make any change to the network adapter association, Network Director initiates an orchestration job, if orchestration is enabled for the given virtual network.

Copyright © 2013, Juniper Networks, Inc.

You can do the following tasks to manage network adapter associations:

- Manage Network Adapter Associations on page 441
- Configure Network Adapter Associations on page 441
- Delete Network Adapter Associations on page 442

Manage Network Adapter Associations

To view and manage the host associations:

1. Select the virtual network or the host for which you want to view and manage the associations from the View pane and click **Connectivity > Manage Network Adapter Associations** from the Tasks pane.

   The Manage Network Adapter Associations page opens. Table 129 on page 441 describes the fields in this table:

Table 129: Manage Physical Switch Associations

Field	Description
Network Adapter Name	Network adapter of the host to which the virtual switch is connected.
MAC Address	MAC address of the host.
Physical Switch	IP address or the name of the physical switch to which the virtual switch is connected.
Physical Switch Port	Number of the physical switch port that the virtual switch is connected.
Discovered Through	Displays how the association was discovered: • **LLDP**—Indicates that the association was automatically discovered by Network Director using LLDP. • **Manual**—Indicates that the association was manually configured using the Import Associations feature. For detailed steps on importing network adapter associations, see "Configure Network Adapter Associations" on page 441. • Blank—Indicates that the association was not discovered or was deleted.
Virtual Switch	Name assigned to the virtual switch. If it is a standalone virtual switch, then the hostname on which the virtual switch resides is also displayed.

Configure Network Adapter Associations

Network Director does not automatically discover and display virtual network adapter to physical network adapter associations if LLDP is not enabled on the physical switch and the virtual switch. In this scenario, you can identify the connection details outside of Network Director and do one of the following:

- Use the Edit Association window from the Manage Network Adapter Associations page to edit individual associations.

Copyright © 2013, Juniper Networks, Inc.

- Use the Import Network Adapter Associations page to import one or more associations into Network Director to establish these associations manually.

To manually configure individual network associations:

1. Select **Virtual Networks** in the View pane.
2. To edit individual associations, from the Manage Network Associations page, select a row and click **Edit Association**.
3. in the Edit Associations window, select the host name of the physical switch and the switch port to which you want the selected virtual network adapter to be connected to.
4. Click Update to save the details and update the Manage Network Adapter Associations table.

To manually configure multiple network associations:

1. Select **Virtual Networks** in the View pane.
2. Click **Connectivity > Import Network Adapter Associations** from the Tasks pane. The Import Network Adapter Associations page opens.
3. Click **Browse** and select the CSV file in which you have specified the network adapter associations that you want to import.

   You can download a sample CSV file by clicking Download Sample CSV button.

Network Director imports the associations after checking the connectivity and changes the status of the successful associations to Manual in the Manage Network Adapter Associations page.

Delete Network Adapter Associations

You can delete the network adapter associations that you no longer want to use, from the Manage Network Adapter Associations page.

NOTE: **You cannot delete LLDP associations that are automatically created by Network Director.**

To delete a network adapter association:

1. Select the row corresponding to the network adapter association that you want to delete and click **Delete Association**.
2. Confirm the deletion.

   Network Director deletes the selected association.

Related Documentation

- Understanding Virtual Network Management on page 72

Copyright © 2013, Juniper Networks, Inc.

Viewing Connections Between Virtual Machines and a Physical Switch

You can pictorially view the virtual machines to physical switch connectivity and virtual machine to virtual machine connectivity using the Virtual View Connectivity page. This page also displays the VLAN connectivity between these entities.

You can open the Virtual Network Connectivity page from the Physical Network view (Logical, Location, Device) or from the Virtual Network view. The level of detail that is displayed depends on the view from which you open this page:

- When you open this page from the Virtual Network view, you can view the connectivity from the selected virtual machine to the virtual switch.
- When you open this page from the Physical Network view, you can view the connectivity from the selected physical switch to a distributed virtual switch and to the virtual machines that are connected to the virtual switch.

This topic describes:

- Viewing Network Connectivity of a Virtual Machine on page 443
- Viewing Connections Between a Physical Switch and Virtual Machines on page 443

Viewing Network Connectivity of a Virtual Machine

To view the connections between a virtual machine and a virtual switch:

1. While in Build mode with Virtual view selected, do one of the following:
   - Click **Inventory > View Virtual Machine** from the Tasks pane to view details of all the virtual machines in your virtual network.
   - Select a host from the Virtual view and click **Inventory > View Virtual Machine** from the Tasks pane to view details of the virtual machines that belong to the selected host.
2. To view the network connectivity of a virtual machine, select the virtual machine and click **Show Connectivity**.

   The Virtual Network Connectivity page opens displaying the network connectivity and VLAN associations for the selected virtual machine.

Viewing Connections Between a Physical Switch and Virtual Machines

To view the connections between a physical switch and virtual machines:

1. While in Build mode with Logical view selected, select the switch for which you want to view the virtual network connectivity from the View pane.
2. From the Tasks pane, select **Connectivity** > **View Virtual Network Connectivity**.

   The Virtual Network Connectivity page opens displaying the virtual switch and the virtual machines that are connected to the selected physical switch. You can also view the VLAN associations for the selected switch.

Copyright © 2013, Juniper Networks, Inc.

If the selected switch is not connected to a virtual network, Network Director displays the standalone switch and all the open ports.

Related Documentation

- Understanding Virtual Network Management on page 72

Viewing Virtual Port Groups

Each virtual switch can have one or more port groups defined for it. Port group is a template that stores a set of configuration that is used to create virtual switch ports on a virtual switch. In other words, a port group captures all the settings necessary for a virtual switch port such as the virtual switch name, VLAN IDs and policies for tagging and filtering, teaming policy, Layer 2 security options, and traffic shaping parameters. When you want to connect a virtual machine to a particular kind of port, you can simply specify the name of a port group with an appropriate definition.

Network Director enables you to view details about all the port groups that are defined for a given virtual switch using the View Virtual Port Group page.

1. While in Build mode with Virtual view selected, navigate to **Virtual Network** > **vCenter IP address** > **vSwitches** and select the virtual switch for which you want to view the virtual port details. From the Tasks pane, click **View Virtual Port Groups** from the Virtual Network Management menu to open the View Virtual Port Group page.
2. The View Virtual Port Groups page displays the details for all the virtual port groups for the selected virtual switch. Table 130 on page 444 describes the fields in this page:

Table 130: View Virtual Port Group Field Descriptions

Field	Description
Name	Name assigned to the virtual port group.
Number of Ports	Number of ports configured on this port group. This field is not applicable for standalone virtual switches.
VLAN Range	The VLAN type and the applicable VLAN range. The VLAN type can be: • Private VLAN • Access VLAN • Trunk VLAN The Trunk VLAN is recommended for uplink port groups. For a standalone virtual switch, only Access VLAN is applicable.
Group Type	The type of port group. Port group type can be Uplink or Access.

Copyright © 2013, Juniper Networks, Inc.

Table 130: View Virtual Port Group Field Descriptions *(continued)*

Field	Description
Switch Type	The type of virtual switch. The switch type can be: • Standalone vSwitch—The traditional virtual switch where the administrator configures and maintains a virtual switch for each host. • Distributed vSwitch—A distributed switch spans multiple hosts at the virtual network level. It is created by abstracting individual host-level virtual switches into a single large distributed switch. This considerably simplifies the virtual machine networking by enabling you to set up virtual machine access switching for your entire datacenter from a centralized interface.

Related Documentation

- Understanding Virtual Network Management on page 72

Copyright © 2013, Juniper Networks, Inc.

Copyright © 2013, Juniper Networks, Inc.

CHAPTER 12

Custom Group Configuration

- Creating Custom Groups on page 447

Creating Custom Groups

From Network Director, you can create a custom group, then add devices such as switches, wireless controllers, and access points to the group, and then name that group. Creating custom device groups enables the configuration of multiple devices simultaneously—you can also create multiple custom groups and directly associate devices at any level. Up to this point, Custom Groups behave the same way as selecting related items in the location view tree. What makes Custom Groups special is that you can also configure a custom group to automatically add devices after discovery. You indicate the criteria for additional devices using rules. Custom groups can then be created in a hierarchy up to eight levels deep. Each layer can contain up to 32 peer containers under a single parent container.

NOTE: **A device can be part of a group at only one level in a hierarchy.**

This topic describes:

- Creating Custom Groups on page 447
- Specifying Settings for a Custom Group on page 448

Creating Custom Groups

To create custom groups:

1. In the Network Views option, select **Custom Group View**.
2. Click Build in the Network Director banner.
3. Under Select View, select either **Logical View**, **Location View**, **Device View** or **Custom Group** View.

TIP: **Do not select Virtual View or Topology View.**

Copyright © 2013, Juniper Networks, Inc.

4. Click **Set Up Custom Group** either under Key Tasks in the Tasks pane or under Custom Group Management in the Tasks pane. (It appears in both places.)

   The Set Up Custom Groups page appears with a network tree displayed.

5. To set up a custom group, follow the directions "Specifying Settings for a Custom Group" on page 448.

6. Click **Done**.

   The new custom group appears in the Groups List.

Specifying Settings for a Custom Group

Use the Set Up Custom Group page to define a group of devices that you can configure simultaneously.

To add a new custom group:

1. Type a name for the new group and then click **Add**.

   The Custom Group tree is displayed with your new group both added and selected. The options **Add Child Group**, **Assign Devices**, and **Add/Edit Rule** appear at the top of the tree.

2. To add a child group under the new custom group:

   a. Be sure the correct custom group is selected. This group will become the parent group.

   b. Click **Add Child Group**.

      The Add Child Group window opens with a with a default child group name such as Group-0.

   c. Optionally, replace the default child group name.

   d. Click **Add**.

      The new child group appears in the Custom Group list tree under the parent group.

TIP: **Custom groups can be created in a hierarchy up to eight levels deep. Each layer can contain up to 32 peer containers under a single parent container.**

3. To assign devices to a custom group:

   a. Select a custom group, either a parent or child group, and then click **Assign Devices**.

      The Assign Devices To Custom Group window opens, displaying a list of discovered network devices, their IP addresses, and their platforms. Platforms include junos-ex, junos-qfx, junos-qf, wlc-ap, and mssos. These are devices that can be added to the group.

Copyright © 2013, Juniper Networks, Inc.

b. Select one or more devices and then click **Add**.

The devices are listed under the appropriate group in the Custom Groups List.

NOTE: A device can be part of a group at only one level in a hierarchy.

4. To add a rule that will automatically add devices to a parent or child custom group:

a. Select a custom group, either a parent or child group, that will have devices added to it automatically when a specific rule has been met.

b. Click **Add/Edit Rule**.

The Add/Edit Rules window opens.

c. Click **Add Rule**.

A rule statement is displayed with three columns—two columns are labelled **Please select...**. The third column is blank.

d. From the first **Please select...** option in the rule statement, select the basis for the rule. You are indicating that automatic additions to the list will be based on either **Device Type**, **Firmware Version**, **Device Role**, **Serial Number**, **SKU/Model**, **Management IP**, or **Location**.

e. From the second **Please select...** option in the rule statement, select an available operator, either **Equals**, **Not Equals** ,**Like**, **Regex**, or **Contains**—the operators presented depend on the basis you selected in the first column. For example, if the basis for the rule is **SKU/Model**, then the only operator options are **Equals** and **Not Equals**.

TIP: The Equals operation matches all characters of the matching criteria. The Like operation matches the first few characters of the matching criteria.

f. For the third option in the rule statement, provide a matching criteria. Matching criteria are indicated in the third column of the list shown in Table 131 on page 449.

Table 131: Three Options of a Rule Statement

Rule Basis	Operator	Matching Criteria
Device Role	Equals	Access
		Aggregation
		Core
		Unassigned (available only for EX switches for which logical category can be defined)

Copyright © 2013, Juniper Networks, Inc.

Table 131: Three Options of a Rule Statement *(continued)*

Rule Basis	Operator	Matching Criteria
Device Type	Equals or Not Equals	Access Point
		Qfabric Member
		Qfabric
		Switch
		Virtual Chassis
		Wireless Controller
Serial Number	Equals or Contains	*You provide serial numbers or letters*
SKU or Model	Equals or Contains	*You provide model numbers or letters*
Management IP	Equals or Regex TIP: Regex, a regular expression, consists of a sequence of characters that forms a search pattern.	*You provide IP address or regular expression* TIP: For example, (?<=\.) {2,}(?=[A-Z]) is a regular expression.
Location	Select a previously configured location: NOTE: For location directions, see "Setting Up the Location View" on page 414. i. Click *Please Select*. ii. From the Select Location window, select a location. iii. Click **OK.**	
Device Role	Equals	*You provide a pre-configured device role.*
Device Type	Equals or Not Equals	Access Point Qfabric Member Qfabric Switch Virtual Chassis Wireless Controller
Firmware Version	Equals or Contains	*You provide a full or partial firmware version for devices.*

g. Click **OK**.

Rules are executed when new devices are discovered. Devices that match the defined rules are added to the group dynamically once discovery is complete.

Copyright © 2013, Juniper Networks, Inc.

TIP: If you add more than one rule to a Custom Group, then all rules must be met for a device to join the group.

5. The option **Associate devices based on the rules for the custom groups while saving group information** is enabled by default. When a device property change occurs, rules are processed and devices are added to the group, if the group has a rule for those actions. If the option is disabled, the rule engine will be activated only when there is some change in the device property.
6. Click **Done**.

   A Status window opens with either the message *Data saved successfully* or with an error message. Click **OK**.
7. To edit a rule, select the appropriate custom group and then click **Add/Edit Rule**. When you edit a rule, devices in the group that no longer qualify because of the rule change are not automatically removed from the group. You must remove those devices manually. If more devices are now qualified to join the group because of your rule edit, the devices are added to the group on the next device notification change to the network.

TIP: To delete a device from the group, select the device and then click **Delete**. To delete an entire Custom Group, select the group and then click **Delete**. You are asked to confirm the deletion—click **OK**.

Related Documentation

- *Creating and Managing Port Groups*
- Assigning a VLAN Profile to Devices or Ports on page 392
- Assigning Device Common Settings to Devices on page 375
- Assigning and Unassigning Devices to a Location on page 403
- Understanding Custom Groups on page 77

Copyright © 2013, Juniper Networks, Inc.

Copyright © 2013, Juniper Networks, Inc.

PART 3

Administration

- Device Discovery on page 455
- Device Management on page 465

Copyright © 2013, Juniper Networks, Inc.

Copyright © 2013, Juniper Networks, Inc.

CHAPTER 13

Device Discovery

- Discovering Devices in a Physical Network on page 455
- Discovering Devices in a Virtual Network on page 460

Discovering Devices in a Physical Network

You can discover and synchronize physical devices such as EX Series switches, QFX Series switches, EX Series switches with ELS, wireless LAN controllers, and access points in your network that are managed by Network Director.

NOTE: To discover devices in your virtual network, follows the steps described in "Discovering Devices in a Virtual Network" on page 430.

NOTE: To discover wireless LAN controllers and access points, Network Director connects to port *8889* of the wireless LAN controller for sending an *HTTPS* request to the controller. Therefore, port *8889* must be open on the wireless LAN controller for Network Director to discover wireless LAN devices. From the Junos Space JA1500 Appliance or the Junos Space Virtual Appliance, you can verify the availability of port 8889 using the CLI command **root@space# nmap <IP address of controller> -p 8889**.

On EX Series switches, Network Director connects to port *22* (the default port) on the Junos Space JA1500 Appliance or the Junos Space Virtual Appliance by using SSH. You can configure port *22* on the Junos Space appliances through **Administration** > **Applications** in the Junos Space Platform page. Select **Network Application Platform** and click **Actions** > **Modify Application Settings**. Change SSH port for device connection field to *22*.

Device discovery is a three-step process in which you specify the target devices, the discovery options, and the schedule options.

While in Build mode, from the Tasks pane, click **Discover Devices** from Device Discovery menu. The Discover Devices page is displayed.

Copyright © 2013, Juniper Networks, Inc.

This topic describes:

- Specifying the Target Devices on page 456
- Specifying the Discovery Options on page 457
- Specifying the Schedule Options on page 459
- Reviewing the Device Discovery Options on page 459
- Viewing the Discovery Status on page 459

Specifying the Target Devices

You can add devices to Network director for device discovery by using either the Import from CSV icon or the Add icon, or both together. Use the Import from CSV icon to add devices in bulk. You can add hundreds of devices to Network Director using a CSV file that contains information extracted from an LDAP repository.

To specify the target devices that you want Network Director to discover:

1. Enter a name for the device discovery job. The default name is ND Discovery.
2. To add devices in bulk, click **Import from CSV** from the Device Targets window. The Upload CSV File dialog box is displayed.
3. Click **Browse**. The File Upload dialog box is displayed.
4. Navigate to the target CSV file on your computer, select the file and click **Open**. The CSV File Upload dialog box reappears, this time displaying the name of the selected file.

   NOTE: **The selected CSV file must follow the same file format as that of the sample CSV file.**

5. Click **Upload** to upload the selected CSV file.
6. To add individual devices by specifying the IP address credentials, click **Add** in the Device Targets table.

   The Add Device Target dialog box appears.
7. Choose one of the following options to specify the target devices:
   - Select the **IP** option and enter the IP address of the device.
   - Select the **IP-Range** option and enter a range of IP addresses for the devices. The maximum number of IP addresses for an IP range target is 1024.
   - Select the **IP-Subnet** option and enter an IP subnet for the devices.
   - Select the **HostName** option and enter the hostname of the device.
   - Click **Add** to save the target devices that you specified, or click **Add More** to add more target devices. When you have added all target devices that you want Network Director to discover, click **Add**.

   The Discover Targets table displays the addresses of the configured target devices.

Copyright © 2013, Juniper Networks, Inc.

8. • To edit a target device, select a row from the Device Targets table and click **Edit**. Make the required changes and click **Add** to display the IP addresses in the Device Targets table
   • To delete a target device, select a row from the Device Targets table and click **Delete**.
   • To view and download a sample CSV file, click **CSV Sample**. The Opening Device_Discovery_CSV.csv file dialog box is displayed. You can open the sample CSV file or save the sample CSV file.
9. Click **Next** or click **Discovery Options** from the top wizard workflow to go to the Discovery Options page. Specify the options as described in the "Specifying the Discovery Options" on page 457.

Specifying the Discovery Options

To add the device credentials and specify the probes:

1. Add the device credentials. To add the credentials, click **Add** from the Device Credentials table.

   The Add Device Credentials dialog box is displayed.

   NOTE: **If the credentials were specified in the CSV file, the Credentials table displays those values. If the credentials were not specified in the CSV file, then enter the values in the Add Device Credentials dialog box.**

   • Specify the administrator username and password, and confirm the password. The username and password must match the name and password configured on the device. The username is a mandatory field.
   • Click **Add** to save the username and password that you specified or click **Add More** to add another username and password.

     Click **Add** after you have finished adding all login credentials. The Device Credentials table displays the usernames that you configured.
2. Specify the probes from the Specify Probes table. Select a probe method to discover the target devices.
   • Select **Use Ping** if SNMP is not configured for the device and clear the **Use SNMP** check box.

     Network Director uses the Juniper Networks Device Management Interface (DMI) to directly connect to and discover devices. DMI is an extension to the NETCONF network management protocol.
   • Select **Use SNMP** if SNMP is configured for the device, and clear the **Use Ping** check box.

     Network Director uses the **SNMP GET** command to discover the target devices.

Copyright © 2013, Juniper Networks, Inc.

- Select both the **Use Ping** and the **Use SNMP** check boxes, to enable Network Director for faster discovery of the target devices, provided the device is pingable and also SNMP is enabled on the device.

NOTE: Network Director uses the Juniper Networks Device Management Interface (DMI) adapter to manage devices that do not run the Junos OS software. Wireless LAN controllers are not DMI-complaint and use the MSS OS software. However, if you enable Use SNMP, then Network Director detects whether the device is running a DMI-complaint software or not. The controllers always use a DMI adapter and hence can be detected.

If you have not enabled Use SNMP, then Network Director assumes that all devices that failed during device discovery are controllers and retry the process if the port 8889 is open.

3. Click **Add** if you have selected the Use SNMP check box.

   The Add SNMP Settings dialog box is displayed.

   Select either **SNMP V1/V2C** or **SNMP V3**. Based on the selection, you need to enter the details as follows:

   - If you selected SNMP V1/V2C, specify a community string, which can be *public*, *private*, or a predefined string.

     Click **Add** in the Add SNMP Settings dialog box or click **Add More** to add more strings to the community. If you click **Add More**, when you are done adding all the strings, click **Add** to save the SNMP settings for V1/V2C.

   - If you selected SNMP V3, specify the following:
     - Enter a username
     - Select the privacy type (AES 128, DES, or None).
     - Enter the privacy password (if AES 128 or DES). If you specify none for the privacy type, the privacy function is disabled.
     - Select the authentication type (MD5, SHA, or none).
     - Enter the authentication password (if MD5 or SHA). If you specify none for the authentication type, the authentication function is disabled.
     - Click **Add** to save the SNMP settings and close the dialog box, or click **Add More** to add additional configurations. If you clicked Add More, click **Add** to save the settings and close the dialog box.

     The Specify Probes table displays the configured SNMP settings.

4. Click **Next** or click **Schedule Options** from the top wizard workflow to go to the Discovery Schedule Options page. Specify the options as described in the "Specifying the Schedule Options" on page 459.

Copyright © 2013, Juniper Networks, Inc.

Specifying the Schedule Options

To specify the scheduler details:

1. Click **Run Now** if you want to discover the devices immediately or Click **Schedule at a later time** if you want to schedule the device discovery for a future time.

   If you select **Schedule at a later time**, specify the date and time to run the device discovery.

2. Click **Next** or click **Review** from the top wizard workflow to view the configuration. See the "Reviewing the Device Discovery Options" on page 459.

Reviewing the Device Discovery Options

From this page, you can save or make changes to the device discovery options.

- To make changes to the device discovery options, click the **Edit** button associated with the configuration you want to change.

  Alternatively, you can click the appropriate buttons in the profile workflow at the top of the page that corresponds to the configuration you want to change.

  When you are finished with your modifications, click **Review** to return to this page.

- Click **Finish** when you are done with the configurations.

  A message window opens, displaying the status of the device discovery job name and job ID. Click **OK**.

  The Device Discovery Jobs page is displayed with the list of jobs scheduled.

Viewing the Discovery Status

After you have configured the device discovery options, you can view the device discovery status from the **View Discovery Status** option from the **Device Discovery** menu.

The **Device Discovery Jobs** page displays all the scheduled device discovery jobs. You can view the following details from the Device Discovery Jobs page as described in Table 132 on page 459

Table 132: Viewing Device Discover Jobs

Field	Description
Job ID	An identifier assigned to the job.
Job Name	The name of the job (user-created).
Percent	Percentage of the job that is complete.

Copyright © 2013, Juniper Networks, Inc.

Table 132: Viewing Device Discover Jobs *(continued)*

Field	Description
Status	Job status. The possible states are: • CANCELLED—The job was cancelled by a user. • FAILURE—The job failed. This state is displayed if any of the devices in the job failed. But some of the devices might have completed successfully. View the job details for the status of each device. • INPROGRESS—The job is running. • SCHEDULED—The job is scheduled but has not run yet. • SUCCESS—The job completed successfully. This state is displayed if all of the devices in the job completed successfully.
Summary	Summary of the job scheduled and executed with status.
Scheduled Start Time	The UTC time on the client computer when the job is scheduled to start.
Actual Start Time	The actual time when the job started.
End Time	The time when the job was completed.
User	The login ID of the user that initiated the job.
Recurrence	The recurrent time when the job will be restarted.

To view the details of a job, select the check box against Job ID or Job Name and click **Show Details**. The Discover Network Elements window displays details of the device discovery job.

NOTE: During device discovery, if Network Director is unable to read the device configurations, then the status displays Failed state. For such failures, you can check the reason for failure from the Manage Jobs page in System mode. You must make the required changes to the device configuration using the CLI so that Network Director can read the configuration. Network Director automatically resynchronizes once you enable a device discovery job. If Network Director cannot discover the device even after resynchronization, then you must rediscover the device after making the appropriate changes in the device configurations using the CLI.

Related Documentation

- Viewing the Device Inventory Page on page 475
- Troubleshooting Device Discovery Error Messages on page 485

Discovering Devices in a Virtual Network

You use virtual network discovery to add virtual networks to Network Director. Discovery is the process of finding and adding a virtual network (VMWare vCenter server) and then

Copyright © 2013, Juniper Networks, Inc.

synchronizing its inventory and configuration with Network Director. To use virtual network discovery, Network Director must be able to connect to the vCenter server.

When discovery succeeds, Network Director creates an object in its database to represent the vCenter server and maintains a connection between the object and the vCenter server to maintain the information flow.

When configuration changes are made on the vCenter server, Network Director automatically resynchronizes with the vCenter server so that the inventory information in the Junos Space database matches the current vCenter server inventory and the configuration information. You can also manually synchronize the vCenter server configuration changes to the configuration stored in the corresponding Network Director object.

At a high level, the following vCenter server inventory and configuration data is captured and stored in relational tables in the Junos Space database:

- Virtual Switches: Port groups, interfaces, VLANs, and other configuration details such as QoS parameters, teaming, and failover details
- Hosts: Physical NICs and virtual machines
- Virtual Machines: Virtual adapters and their associations

Virtual network discovery is a three-step process in which you specify the target devices, the credentials of devices to be discovered, and review the discovery options.

While in Build mode with Virtual view selected, from the Tasks pane, click **Discover Virtual Network** from Virtual Network Management menu. The Discover Virtual Network page is displayed.

This topic describes:

- Specifying the vCenter Targets on page 461
- Specifying the Virtual Network Credentials on page 462
- Reviewing the Virtual Network Discovery Options on page 462
- Viewing the Discovery Status on page 463

Specifying the vCenter Targets

You can add VMware vCenter servers to Network director by specifying the hostname or the IP address of one or more vCenters.

To specify the target devices that you want Network Director to discover:

1. In the vNetwork Targets and Credential tab, enter a name for the virtual network discovery job. The default name is vNetwork Discovery.
2. Click **Add** in the vNetwork Targets table.

   The Add vNetwork Target dialog box appears.
3. Choose one of the following options to specify the target vCenter server that you want to discover:

Copyright © 2013, Juniper Networks, Inc.

- Select the **IP** option and enter the IP address of the vCenter server.
- Select the **HostName** option and enter the hostname of the vCenter server.

4. Specify the port that Network Director uses to connect to the vCenter server. The default port is 443.

NOTE: You can modify this and specify a port of your choice. If you do so, make sure to manually change the Junos Space firewall settings and apply to this port.

5. Click **Add** to save the target vCenter server that you specified, or click **Add More** to add more target vCenter servers. When you have added all target devices that you want Network Director to discover, click **Add**.

   The vNetwork Targets table displays the addresses of the configured target devices.

6. - To edit a target vCenter server, select a row from the vNetwork Targets table and click **Edit**. Make the required changes and click **Add** to display the changes in the vNetwork Targets table.
   - To delete a target vCenter server, select a row from the vNetwork Targets table and click **Delete**.

7. Click **Next** or **vNetwork Credentials** from the top wizard workflow to go to the vNetwork Credentials page. Specify the options as described in the "Specifying the Virtual Network Credentials" on page 432.

Specifying the Virtual Network Credentials

1. Add the vCenter server credentials. To add the credentials, click **Add** from the Device Credentials table.

   The Add vNetwork Credentials dialog box is displayed.

   - Specify the administrator username and password, and confirm the password. The username and password must match the name and password configured on the device. The username is a mandatory field.
   - Click **Add** to save the username and password that you specified or click **Add More** to add another username and password.

     Click **Add** after you have finished adding all login credentials. The Device Credentials table displays the usernames that you configured.

2. Click **Next** or click **Review** from the top wizard workflow to go to the Review page.

Reviewing the Virtual Network Discovery Options

From the review page, you can save or make changes to the virtual network discovery options.

- To make changes to the virtual network discovery options, click the **Edit** button associated with the configuration you want to change.

Copyright © 2013, Juniper Networks, Inc.

Alternatively, click the appropriate buttons in the profile workflow at the top of the page that corresponds to the configuration you want to change.

When you are finished with your modifications, click **Review** to return to this page.

- Click **Finish** when you are done with the configurations.

  A message window opens, displaying the status of the virtual network discovery job name and job ID. Click **OK**.

  You can view the status of the discovery job in the Virtual Network Discovery Jobs page.

Viewing the Discovery Status

After you have configured the virtual network discovery options, you can view the discovery status from the **View Discovery Status** option from the **virtual network discovery** menu.

The **Virtual Network Discovery Jobs** page displays all the discovery jobs. You can view the following details from the Virtual Network Discovery Jobs page as described in Table 124 on page 433.

Table 133: Viewing Device Discover Jobs

Field	Description
Job ID	An identifier assigned to the job.
Job Name	The name of the job (user-created).
Percent	Percentage of the job that is complete.
Status	Job status. The possible states are: • CANCELLED—The job was cancelled by a user. • FAILURE—The job failed. This state is displayed if any of the devices in the job failed. But some of the devices might have completed successfully. View the job details for the status of each device. • INPROGRESS—The job is running. • SCHEDULED—The job is scheduled but has not run yet. • SUCCESS—The job completed successfully. This state is displayed if all of the devices in the job completed successfully.
Summary	Summary of the job scheduled and executed with status.
Scheduled Start Time	The UTC time on the client computer when the job is scheduled to start.
Actual Start Time	The actual time when the job started.
End Time	The time when the job was completed.
User	The login ID of the user that initiated the job.
Recurrence	The recurrent time when the job will be restarted.

Copyright © 2013, Juniper Networks, Inc.

To view the details of a job, select the check box against Job ID or Job Name and click **Show Details**. The Discover Network Elements window displays details of the virtual network discovery job.

NOTE: During virtual network discovery, if Network Director is unable to read the device configurations, then the status displays Failed state. For such failures, you can check the reason for failure from the Manage Jobs page in System mode. You must make the required changes to the device configuration using the CLI so that Network Director can read the configuration. Network Director automatically resynchronizes once you enable a virtual network discovery job. If Network Director cannot discover the device even after resynchronization, then you must rediscover the device after making the appropriate changes in the device configurations using the CLI.

Related Documentation

- Troubleshooting Device Discovery Error Messages on page 485

Copyright © 2013, Juniper Networks, Inc.

CHAPTER 14

Device Management

- Accessing a Device's CLI from Network Director on page 465
- Accessing a Device's Web-Based Interface from Network Director on page 466
- Assigning Devices to Logical Category on page 467
- Creating and Managing Multichassis Link Aggregation Groups (MC-LAGs) on page 468
- Deleting Devices on page 471
- Rebooting Devices on page 472
- Setting Up QFabrics on page 472
- Viewing the Device Inventory Page on page 475
- Viewing the Physical Inventory of Devices on page 477
- Viewing a Device's Current Configuration from Network Director on page 478
- Viewing Licenses With Network Director on page 478
- Viewing Profiles Assigned to a Device on page 480

Accessing a Device's CLI from Network Director

Network Director enables you to connect to the command-line interface (CLI) for switches and wireless LAN controllers in your network using SSH.

This topic describes the steps to connect to a switch or a controller using SSH (Secure Shell). SSH is a cryptographic network protocol for used for remote shell services or command execution. SSH is one of the many access services that are supported on the Juniper Networks devices. All Juniper Network devices have SSH enabled by default.

To connect to a device using SSH:

1. In the View pane, select the device to which you want to connect.
2. In Build mode, select **Tasks** pane > **Device Management** > **SSH to Device**.

   The SSH to Device dialog box appears.
3. Enter the username and password to connect to the selected device and click **Connect**.

NOTE: Ensure that you have removed Pop-Up blockers, if any, before you click Connect.

Copyright © 2013, Juniper Networks, Inc.

The SSH console to the switch or controller opens in a separate browser tab or window depending on your browser settings. Refer to the EX Series documentation or the Wireless LAN Services (WLS) Product Documentation for more information on the using the CLI for EX Series switches and WLC wireless LAN controllers respectively.

NOTE: Any configuration changes you make to a device using the CLI qualify as out-of-band changes in Network Director. Out-of-band configuration changes can cause the configuration state of a managed device to become out of sync, which indicates that the device configuration no longer matches the Build mode configuration for the device. Use the Resynchronize Device Configuration task in Deploy mode to resynchronize the device configuration.

Related Documentation

- *Understanding Resynchronization of Device Configuration*
- Accessing a Device's Web-Based Interface from Network Director on page 466

Accessing a Device's Web-Based Interface from Network Director

Network Director enables you to connect to the switches and wireless LAN controllers in your network using the device Web-based interface.

This topic describes the steps to connect to a switch using the J-Web interface or to a controller using Web View. The J-Web interface is a graphical user interface using which you can monitor, configure, troubleshoot, and manage switches. Web View is a web-based management application that enables you to perform common configuration and management tasks on wireless devices.

You can connect and configure a device using the J-Web interface or Web View only if the device is configured to accept HTTP or HTTPS as a management service. You can configure HTTP or HTTPS as a management service using the Device Common Settings profile. For more information, see "Creating and Managing Device Common Settings" on page 198.

To connect to a device using the J-Web interface or Web View:

1. In the View pane, select the device to which you want to connect.
2. In Build mode, select **Tasks** pane > **Device Management** > **Launch Web View**.

   The Web View or J-Web Login page appears.
3. Enter the username and password to connect to the selected switch and click **Login**.

   If the credentials that you entered are valid, the system displays the the J-Web or Web View home page for the selected device.

Copyright © 2013, Juniper Networks, Inc.

NOTE: Any configuration changes you make to a device using the Web interface qualify as out-of-band changes in Network Director. Out-of-band configuration changes can cause the configuration state of a managed device to become out of sync, which indicates that the device configuration no longer matches the Build mode configuration for the device. Use the Resynchronize Device Configuration task in Deploy mode to resynchronize the device configuration.

Related Documentation

- *Understanding Resynchronization of Device Configuration*
- Accessing a Device's CLI from Network Director on page 465

Assigning Devices to Logical Category

Network Director enables you to tag the available EX Series switches to different categories—Core, Aggregation, Access, or Unassigned categories. Once you tag a switch, it appears under the tagged category after refreshing the screen.

To assign a group of EX Series switches under Core, Aggregation, Access, or Unassigned category, select Logical View in Build mode (available only in Build mode) and select one of the cabinets under the Switching Network cabinet:

1. Select **Assign Device to Logical Category** under Device Management from the Tasks pane.

   The Assign Device to Logical category page is displayed.

2. Click **Add** from the Selected Devices table. The Please select devices dialog box is displayed.

3. Select the device or devices that you want to assign by selecting the check box next to the hostname. Click **OK**. The selected device or devices with the details appears in the Selected Devices table.

4. Select a role from the New Role drop-down list.

   The available roles are: Access, Aggregation, Core, and Unassigned.

5. Click **Done** to change the role or click **Cancel** if you do not want to change the role. The message: **Device Role successfully changed** appears if you have selected Done.

To assign an EX Series switch under Core, Aggregation, Access, or Unassigned category, select Logical View in Build mode (available only in Build mode) and select any EX series switch from the one of the cabinets under the Switching Network cabinet:

1. Select **Assign Device to Logical Category** under Device Management from the Tasks pane.

   The Assign Device to Logical category page is displayed. The page displays the name of the selected device and the current role of the device.

2. Select a role from the New Role list to change the current role.

Copyright © 2013, Juniper Networks, Inc.

The available roles are: Access, Aggregation, Core, and Unassigned.

3. Click **Done** to change the role or click **Cancel** if you do not want to change the role. The message: **Device Role successfully changed** appears if you have selected Done.

Related Documentation

- Viewing Profiles Assigned to a Device on page 480

Creating and Managing Multichassis Link Aggregation Groups (MC-LAGs)

Multichassis link aggregation groups (MC-LAGs) enable a client device to form a logical LAG interface between two switches. An MC-LAG provides redundancy and load balancing between the two switches, multihoming support, and a loop-free Layer 2 network without running the Spanning Tree Protocol (STP).

The MC-LAG switches use the Interchassis Control Protocol (ICCP) to exchange the control information between two MC-LAG switches.

On one end of an MC-LAG is an MC-LAG client device, such as a server, that has one or more physical links in a link aggregation group (LAG). This client device does not need to detect the MC-LAG. On the other side of MC-LAG are two MC-LAG switches. Each of the switches has one or more physical links connected to a single client device. The switches coordinate with each other to ensure that data traffic is forwarded properly.

You can create MC-LAGs on QFX3500 and QFX3600 Series devices.

To start creating an MC-LAG:

1. Click the Build Mode icon

in the Network Director banner.
2. Select **Device Management** > **Create MC-LAG** in the Tasks pane.

   The Create MC-LAG wizard opens to the Device Selections page.
3. Continue with the section "Selecting Devices for the MC-LAG" on page 468.

This topic includes:

- Selecting Devices for the MC-LAG on page 468
- Configuring MC-LAG Settings on page 469
- Managing MC-LAGs on page 470
- What To Do Next on page 470

Selecting Devices for the MC-LAG

To select devices for the MC-LAG in the Device Selections page:

1. Click **Select Devices**.

   The Select Two Devices for MC-LAG window opens, listing the devices on which you can create an MC-LAG.
2. Select two devices from the list.

Copyright © 2013, Juniper Networks, Inc.

3. Click **Done**.

   The devices appear in the Devices selected for MC-LAG list.

4. Click either **Next** or **MC-LAG Settings**.

   The MC-LAG Settings page opens. Continue with the section "Configuring MC-LAG Settings" on page 469.

Configuring MC-LAG Settings

On the MC-LAG Settings page you configure MC-LAG and ICCP settings for both selected switches. Some MC-LAG and ICCP settings must be coordinated between the two switches, so when you specify such a setting for one switch, that setting is automatically specified for the other switch.

To configure MC-LAG settings:

1. Enter settings in the MC-LAG section for both switches.

   The MC-LAG settings configure the connection between the client device and the switch. Table 134 on page 469 describes the fields in this section.

2. Enter settings in the ICCP-LAG section for both switches.

   The ICCP settings configure the connection between the peer switches in the MC-LAG. Table 135 on page 470 describes the fields in this section.

3. Select the ports for the MC-LAG and the ICCP LAG in the Port Selection section.

   Each selected device has a tab. For each device, move ports between the **Available Ports** list and the **MC-LAG** or **ICCP-LAG** lists using the arrow keys.

4. Click the **Finish** button.

Table 134: MC-LAG Settings

Field	Description
AE Name	Select the aggregated Ethernet interface to use in the MC-LAG.
LACP Mode	Select the LACP mode for the MC-LAG.
Description	Enter a description for the MC-LAG.
VLAN	Select the same VLAN profile to associate to the aggregated Ethernet (ae) interface on each switch.
LACP System ID	Specify the same LACP system ID on each switch.
LACP Admin Key	Specify the same LACP administration key on each switch.
AE ID	Specify the same multichassis aggregated Ethernet identification number for the MC-LAG that the aggregated Ethernet interface belongs to on each switch.

Copyright © 2013, Juniper Networks, Inc.

Table 134: MC-LAG Settings *(continued)*

Field	Description
Chassis ID	Specify a unique chassis ID for the MC-LAG that the aggregated Ethernet interface belongs to on each switch.
Control Status	Specify whether the aggregated Ethernet interface participating in the MC-LAG is primary or secondary. Primary is active, and secondary is standby.
Init Delay Time (seconds)	Specify an initialization delay time, in seconds.

Table 135: ICCP-LAG Settings

Field	Description
AE Name	Select the aggregated Ethernet interface to use for the ICCP connection.
LACP Mode	Select the LACP mode for the ICCP connection.
Description	Enter a description for the ICCP connection.
VLAN Name	Enter the name of the VLAN to use for the ICCP connection.
Vlan ID	Enter the same VLAN ID to use for the ICCP connection on each switch.
Local IP	Configure the local IP address to be used by all switches hosting the MC-LAG.
Liveness min. receive interval (ms)	Configure the minimum interval at which the switch must receive a reply from the other switch with which it has established a Bidirectional Forwarding Detection (BFD) session.
Liveness min. transmit interval (ms)	Configure the minimum transmit interval during which a switch must receive a reply from a switch with which it has established a BFD session.
Session establish hold time (ms)	Configure the time during which an ICCP connection must succeed between the switches hosting the MC-LAG. Configured session establishment hold time results in faster ICCP connection establishment. The recommended value is 50 seconds.

Managing MC-LAGs

You manage MC-LAGs using the Manage LAG task.

What To Do Next

The configuration changes that you make in the Build mode are not deployed to devices automatically. After you create an MC-LAG, you must deploy it on the switches. You must manually deploy the changes to devices in Deploy mode. For details, see *Deploying Configuration to Devices*.

Copyright © 2013, Juniper Networks, Inc.

TIP: Even though MC-LAG configuration is not contained within a profile, you can view the MC-LAGs assigned to a switch by using the View Assigned Profiles task in Build mode.

Related Documentation

- Understanding Link Aggregation on page 34
- Managing and Creating a Link Aggregation Group on page 278
- Viewing Profiles Assigned to a Device on page 480

Deleting Devices

You can delete devices that are no longer used from Network Director. Deleting a device removes all device configuration and device inventory information from the Junos Space database. Once a device is deleted from the database, all the profiles associations, device configurations, and inventory information of the deleted device are also deleted. However, the system maintains the audit logs and monitoring data for the device even after the device is deleted.

Use the Delete Devices page to delete devices from Network Director. While in Build mode, click **Delete Devices** from the **Tasks > Device Management** menu. The Delete Devices page appears.

The Delete Devices page displays the devices contextually depending on your selection in the View pane. For example, if you select a site in Location view and click Delete Devices, Network Director displays all the devices that are assigned to the buildings or floors in the selected site in the Delete Devices page. If you select a particular switch family in Device view and click Delete Devices, only switches that belong to that switch family are displayed.

To delete devices, complete the following tasks:

1. Select the check box adjacent to the switch, controller, or a group of access points that you want to delete.
2. Click **Done**.

   Network Director prompts you to confirm the deletion. Click **Yes** to confirm the deletion or **No** to go back and make changes to the selection.

Related Documentation

- *Understanding the Network Director User Interface*
- Discovering Devices in a Physical Network on page 455
- Viewing the Device Inventory Page on page 475

Copyright © 2013, Juniper Networks, Inc.

Rebooting Devices

Use the Reboot Devices task to immediately reboot the selected device. This task is available in all scopes when in Build mode. To reboot one or more devices immediately:

1. Select the scope in the View pane that contains the devices you want to reboot.
2. Select Reboot Devices from the Tasks pane.
3. Expand the tree on the page as needed to locate the available devices.
4. Select the check box for one or more devices.
5. Click **Done** to start the reboot or click **Cancel** to return to the Device Inventory page.

The rebooting process triggers a Cold Start Alarm that can be seen in Fault mode.

Related Documentation

- Understanding the Build Mode Tasks Pane on page 8
- *Understanding the Network Director User Interface*

Setting Up QFabrics

This topic describes how to set up a QFabric using Network Director.

To start setting up a QFabric:

1. Select **Build** from the Network Director banner.
2. Select the QFabric to set up in the View pane.
3. Select **Setup QFabric** from the Device Management section of the Task pane.

   The Node Alias page of the Setup QFabric wizard opens.

This topic describes:

- Managing Node Aliases on page 472
- Managing Node Groups on page 473
- Identifying CPE Switches on page 474
- Reviewing the QFabric Summary and Deploying Changes on page 474

Managing Node Aliases

Use the Node Alias page to manage aliases for QFabric nodes.

For a description of the information shown in the Manage Node Alias table, see Table 136 on page 473.

To assign aliases to nodes:

1. To change one node's alias, click its **Alias (To edit, click individual cell)** table cell, then enter the new alias.

Copyright © 2013, Juniper Networks, Inc.

2. To assign automatic aliases to a group of nodes:

   a. Select the nodes from the list by selecting their check boxes.

   b. Click **Auto-alias selected devices**.

      The Auto-alias selected devices window opens.

   c. Enter auto-aliasing parameters in the window:

      The Selected Devices field shows the number of selected devices. All selected devices will be auto-aliased.

      - Node Name—Enter a string to use as a prefix in the automatically generated node names.
      - Starts With—Enter a number. This number is appended to the alias prefix of the first node that is automatically aliased. The number is incremented in the alias of the remaining selected nodes.

      The New Aliases field shows a preview of the new aliases as you change the parameters.

   d. Click **OK**.

      Alias are automatically assigned to the selected nodes.

3. Click **Next** to continue the wizard.

   The Node Groups page opens.

Table 136: Manage Node Alias Table

Column	Description
Device Serial Number	Serial number of the node.
Alias (To edit, click individual cell)	Alias of the node. Click the alias name to edit it.
Device Type	Device type of the node.
Connection State	Connection state of the node.

Managing Node Groups

Use the Node Groups page to manage QFabric node groups.

This step of the Setup QFabric wizard is the same as the separate Manage Node Groups task. You can manage node groups by using either method. For information about managing node groups, see *Creating and Managing Node Groups* .

Click **Next** to continue the wizard.

The Selected CPE Switch(es) page opens.

Copyright © 2013, Juniper Networks, Inc.

Identifying CPE Switches

Use the Identify CPE Switch(es) page to identify the switches that comprise the QFabric system control plane network.

To identify the control plane switches:

1. To add a control plane switch
   a. Click **Add**. The Please Select Devices window opens.
   b. Select the control plane switches from the list.
   c. Click **OK**.
2. To remove a control plane switch, select it from the list, then click **Remove**.
3. Click **Next** to continue the wizard.

   The Review page opens.

Reviewing the QFabric Summary and Deploying Changes

In the Review page, review the QFabric setup with the changes you made. Expand the folders under the QFabric icon to see the fabric's components. To make any changes, click the **Back** button to return to a previous step, or click the step in the wizard flowchart at the top of the page.

To deploy the changes you made to the QFabric, click **Deploy**.

Related Documentation

- Understanding QFabric Setup on page 41

Copyright © 2013, Juniper Networks, Inc.

Viewing the Device Inventory Page

The Device Inventory page lists devices managed by Network Director and provides basic information about the devices, such as IP address and current operating status. The Device Inventory page is available in Build and Deployment mode and is the default landing page for Build mode.

The scope you have selected in the View pane determines which devices are listed in the Device Inventory page. For example:

- If you select My Network, all devices managed by Network Director are listed.
- If you select a building in Location view, only those devices assigned to that building (including the floors and closets in the building) are listed.
- If you select a wireless LAN controller, only that wireless LAN controller and any access points it manages are listed.

NOTE: **If you have configured access points using the Manage Access Point task but have not yet deployed the configuration on the wireless LAN controller, the Device Inventory page does not list those access points.**

The Device Inventory page provides three pie charts that summarize the status of the devices in your selected scope:

- Devices by Family—Indicates the proportion of devices in each device family.
- Connection State—Shows the proportion of devices that are up or down. In this chart, Virtual Chassis count as one device.
- Configuration State—Shows the proportion of devices in each configuration state. See the Config State entry in Table 137 on page 475 for definitions of the configuration states.

Mouse over a pie segment to view the actual number of devices and the percentage represented by that pie segment.

Table 137 on page 475 describes the fields in the Device Inventory table.

Table 137: Fields in the Device Inventory Table

Field	Description
Hostname	Configured name of the device or IP address if no hostname is configured.
IP Address	IP Address of the device.
Serial Number	Serial number of device chassis.
Platform	Model number of the device.
OS Version	Operating system version running on the device.

Copyright © 2013, Juniper Networks, Inc.

Table 137: Fields in the Device Inventory Table *(continued)*

Field	Description
Device Family	Device family of the device: • JUNOS-EX for EX Series switches • JUNOS for EX Series switches with ELS • JUNOS-QFX for QFX Series switches and QFabric members • JUNOS-QF for QFabric systems • MSSOS for WLC Series wireless LAN controllers • WLC-AP for access points managed by WLC Series wireless LAN controllers
Device Type	Type of the device: • AP—Wireless LAN access point • Fabric Member—QFabric member switch • QFabric—QFabric system • Switch—Standalone switch • VC—Virtual Chassis master • VC Member—Virtual Chassis member switch • WLC—Wireless LAN controller • XRE—External Routing Engine for EX8200 Virtual Chassis
Connection State	Connection status of the device in Network Director: • UP—Device is connected to Network Director. • DOWN—Device is not connected to Network Director. • N/A—Access point state is unavailable to Network Director.
Config State	Displays the configuration status of the device: • In Sync—The configuration on the device is in sync with the Network Director configuration for the device. • Out Of Sync—The configuration on the device does not match the Network Director configuration for the device. This state is usually the result of the device configuration being altered outside of Network Director. You cannot deploy configuration on a device from Network Director when the device is Out Of Sync. To resolve this state, use the Resynchronize Device Configuration task in Deploy mode. • Sync failed—An attempt to resynchronize an Out Of Sync device failed. • Synchronizing—The device configuration is in the process of being resynchronized. • N/A—The device is down or is an access point.
Manageability State	Displays if the device is directly manageable or not. This is a hidden field. To display the Manageability State field, click any column, click the down arrow to expand the list, select **Columns** from the list, and then enable **Manageability State**.

Related Documentation

- *Understanding the Network Director User Interface*
- *Understanding Resynchronization of Device Configuration*

Copyright © 2013, Juniper Networks, Inc.

- *Device Inventory Report*

Viewing the Physical Inventory of Devices

You can view the physical inventory of all the devices in your network in the Device Physical Inventory page. The Device Physical Inventory page displays information about the slots that are available for a device and provides information about power supplies, chassis cards, fans, part numbers, and so on. Network Director displays hardware inventory by device name, based on data retrieved both from the device during discovery and resynchronizing operations, and from the data stored in the hardware catalog. For each managed device, the physical inventory page provides descriptions for field replaceable units (FRUs), part numbers, model numbers, and the pluggable locations from which empty slots are determined.

To view the Device Physical Inventory page, while in the Build mode select a standalone EX Series switch, a Virtual Chassis, or a wireless LAN controller (WLC) from the View pane and select **Device Management** > **Physical Inventory** from the Tasks pane.

The physical inventory page displays the model number, part number, serial number, and description for the following, depending on the device that you selected:

- For standalone EX Series switches and Virtual Chassis, the page displays details of the switch, the chassis, the Flexible PIC Concentrator (FPC), the PIC slot, the PIC installed in the PIC slot, the power supply, the fan tray, and the routing engine.
- For a controller, the page displays details about the fan and optics used by the controller.

You can view the following details from the Device Physical Inventory page as described in Table 138 on page 477.

Table 138: Fields in the Device Physical Inventory Table

Field	Description
Item	Name of the device and the components that are part of the device. By default, Network Director displays the device and components in an expanded tree structure. You can click a device or component to collapse or expand the sub-components.
Model Number	• For standalone EX Series switches and Virtual Chassis, the full Junos EX Series model number of the device. • For a controller, the model number of the controller.
Part Number	Part number of the EX Series switch chassis component.
Serial Number	The hardware serial number of the device.
Description	The description about the component.

Related Documentation

- *Understanding the Network Director User Interface*

Copyright © 2013, Juniper Networks, Inc.

Viewing a Device's Current Configuration from Network Director

You can view a device's current configuration from Network Director. This is a convenient way to view device configurations without leaving Network Director.

To view a device's current configuration:

1. Click **Build** or **Deploy** in the Network Director banner.
2. Select the device in the View pane.
3. Select **Device Management > Show Current Configuration** in the Tasks pane.
4. The device's current configuration displays in the main window.

Related Documentation

- *Understanding the Network Director User Interface*
- Understanding the Build Mode Tasks Pane on page 8

Viewing Licenses With Network Director

Juniper Networks devices require a license to operate some features. You can view the licenses for devices connected to Network Director.

To view the license for a Juniper Networks device on your network:

1. Select the **Build** icon in the Network Director banner.
2. In the View pane, select a wireless or wired device.
3. In the Tasks pane, select **View License Information**.

   The Licenses page for that object is displayed with the fields listed in Table 139 on page 478.

Table 139: Viewing Licenses with Network Director

Field	Description
Feature Name	Name of the licensed SKU or feature. It can be used to look up the license with Juniper Networks. Not all devices support this.
License Count	Number of times an item has been licensed. This value can have contributions from more than one licensed SKU or feature. Alternatively, it can be 1, no matter how many times it has been licensed.
Used Count	Number of times the feature is used. For some types of licenses, the license count will be 1, no matter how many times it is used. For capacity-based licensable items, if infringement is supported, the license count can exceed the given count, which has a corresponding effect on the need count.
Need Count	Number of times the feature is used without a license. Not all devices can provide this information.

Copyright © 2013, Juniper Networks, Inc.

Table 139: Viewing Licenses with Network Director *(continued)*

Field	Description
Given Count	Number of instances of the feature that are provided by default.

NOTE: If a device does not have a license, a blank page is displayed with the message, **No license is installed on this device.** If you are sure the device has a license, try resynchronizing the device before displaying the license again.

4. Optionally, expand the license information by feature name to view the feature SKU information. Table 140 on page 479 describes the additional fields that are displayed.

Table 140: Additional Licensing Information

Field	Description
Validity Type	Validity type can be Databased (license expires on end date), Permanent, Countdown (license expires when time remaining is zero), or Trial. If the validity type is either Databased or Countdown, more information is displayed—License Name, License Version, License State, and Time Remaining. Additional information can be added in the details grid based on the SKU type (SKU or Feature)—Start Date, End Date, or Original Time Allowed.
License Name	If the validity type is either Databased or Countdown, the identifier associated with a license key is displayed.
License Version	If the validity type is either Databased or Countdown, the version of a license is displayed. The version indicates how the license is validated, the type of signature, and the signer of the license key.
License State	If the validity type is either Databased or Countdown, the state of the license is displayed—Valid, Invalid, or Expired.
Time Remaining	If the validity type is either Databased or Countdown, the remaining time left on the license is displayed. For a trial license, the number of days remaining after you installed the device is displayed. For a commercial license, the time remaining is unlimited.
Start Date	Based on the SKU type, the start date of the license can be displayed in the details grid.
End Date	Based on the SKU type, the end date of the license can be displayed in the details grid.
Original Time Allowed	Based on the SKU type, the original license timeframe can be displayed here.

Copyright © 2013, Juniper Networks, Inc.

NOTE: If you apply a new license to an existing wireless LAN controller, you must resynchronize the device before the new license is seen in Network Director. For directions, see *Resynchronizing Device Configuration*.

Related Documentation

- *Resynchronizing Device Configuration*

Viewing Profiles Assigned to a Device

View Assigned Profile page list all the profiles associated with a selected device or with an object such as ports, access points, or radios within that device. To view the profiles assigned to a device, you must have the profiles already assigned to the devices, ports, access points, or radios within that device. Only those profiles that are assigned to a specified object will be displayed in the Profiles Assigned to the Device page. In addition to displaying profiles assigned to objects, the Profiles Assigned to Device page also shows link aggregation groups (LAGs) assigned to devices.

The View Assigned Profiles task is available in the Logical, Location, and Device panes for EX Series switches. For wireless LAN controllers, the View Assigned Profiles task is available only in the Logical pane as cluster functionality is available only in Logical pane.

You can access the View Assigned Profiles page by selecting the object (device, port, or radio) and clicking the View Assigned profiles menu. However, view assigned profiles task is unavailable for auto access point (Auto AP) profiles.

You can view the profiles assigned to an EX Series switch or a wireless LAN controller. To view the assigned profiles to a particular device:

While in Build mode, select an EX Series switch from the Switching Network cabinet or a controller from the Wireless Network cabinet under the View pane and select **View Assigned profiles** from the Tasks pane.

The Profiles Assigned to the Device page displays a list of profiles that are already assigned to the selected device. The details displayed are described in Table 141 on page 480.

Table 141: Details of Assigned Profiles to a Device

Field	Description
Profile Type	The type of the profile. The profiles are grouped based on the type of the profile. The profiles that are directly deployed on the device are displayed in the list. For example, Device, VLAN, Port, Radio and so on.
Profile Name	Name of the profile that was specified at the time of creating the profile.
Object	The name of the device (EX Series switch or a wireless LAN controller), port, access point, or radio.

Copyright © 2013, Juniper Networks, Inc.

Table 141: Details of Assigned Profiles to a Device *(continued)*

Field	Description
Object Type	Specifies whether the object is a device (EX series switch or a controller), a port, an access point, or a radio. TIP: For an EX series switch, the object type is the device or a port For a wireless LAN controller, the object type is a controller, an access point, a radio, or a port.
Assignment State	The status of the profile whether it is deployed or in progress. • Deployed—the profile is provisioned to the device • Pending deployment—the profile is assigned to the device, but pending provisioning.

Related Documentation

- Assigning Device Common Settings to Devices on page 375
- Assigning a VLAN Profile to Devices or Ports on page 392

Copyright © 2013, Juniper Networks, Inc.

Copyright © 2013, Juniper Networks, Inc.

PART 4

Troubleshooting

- Troubleshooting Device Discovery on page 485

Copyright © 2013, Juniper Networks, Inc.

Copyright © 2013, Juniper Networks, Inc.

CHAPTER 15

Troubleshooting Device Discovery

- Troubleshooting Device Discovery Error Messages on page 485

Troubleshooting Device Discovery Error Messages

While you are discovering devices by using Network Director, you might encounter some issues. Network Director enables you to detect the errors and provide solutions to the potential errors that you encounter.

Error Message	Solution
Error Messages Displayed During Discovery of Wireless LAN Controllers	
User authentication failed.	This message is displayed when SNMP option is not enabled during the device discovery process. Check whether the firewall is disabled on Junos Space Virtual Machine or the JA1500 Appliance on port 8889 (outbound), if not, disable the firewall. Port 8889 is opened during Network Director installation, but in case of a failure, you must check whether this port is open or not.
Adapter mssos cannot manage the device - Either the Device is down or the port 8889 is not reachable.	This message is displayed when SNMP is enabled during the device discovery process. Check whether port 8889 is open or not. You can check using the CLI command **root@space# nmap <IP address of controller> -p 8889** from the Junos Space JA1500 Appliance or Junos Space Virtual Appliance.
Adapter mssos cannot manage the device-Can't manage Device, Wrong Credentials.	Check the credentials entered during the device discovery process. Always select the *Enable Password* credential for device discovery in Network Director.

Copyright © 2013, Juniper Networks, Inc.

Error Message	Solution
Check if adapter is running or Platform can't connect to it.	Check whether the MSSOS adapter process is running on Junos Space JA1500 Appliance or the Junos Space Virtual Appliance. Verify using the CLI command **root@space# ps -ef | grep mssos** . If no process is running, restart the adapter service by using the CLI command **root@space# service mssosadapter start**.
Device is not reachable.	If ping is enabled during device discovery, then check whether the controller is reachable using the CLI command **ping**.
Junos Space is unable to query the device information through SNMP. Check the SNMP settings on the device to verify SNMP is not blocked and the SNMP settings specified in Junos Space match the device SNMP settings.	If the SNMP option is enabled in Network Director during device discovery, then check and ensure that SNMP is enabled on the controller. Also, ensure that he SNMP settings on Network Director and Junos Space match with the SNMP settings on the controller.
Error Messages Displayed During Discovery of EX Series Switches	
SSH connection failed. Device might not be reachable.	For EX Series switches, Network Director connects to port *22* (default port) on the JA1500 Appliance or the Junos Space Virtual Appliance by using SSH. Ensure that you have configured port *22* on the Space appliance through **Administration** > **Applications** in the Junos Space Plattform page. To do this, select **Network Application Platform** and click **Actions** > **Modify Application Settings**. Change SSH port for device connection field to *22*. If port 22 is open on the Junos Space Appliance, and you still get the error, then check if port 22 is open on the switch and if the switch is accepting SSH connections on port 22.
User Authentication failed.	Check the read and write credentials used during device discovery.
Device is not reachable.	If ping is enabled during device discovery, then check whether the switch is reachable using the CLI command **ping**.
Junos Space is unable to query the device information through SNMP. Check the SNMP settings on the device to verify SNMP is not blocked and the SNMP settings specified in Junos Space match the device SNMP settings.	If the SNMP option is enabled in Network Director during device discovery, check and ensure that SNMP is enabled on the switch. Also, check and ensure that the SNMP settings on Network Director and Junos Space match with the SNMP settings on the switch.
General Error Messages	

Copyright © 2013, Juniper Networks, Inc.

Error Message	Solution
Device Failed to return System information.	This message is displayed if the switch is too busy to respond to operational commands. Try discovering the device again.
Failed to configure device, Check Device state.	Check whether the Edit lock is open on the switch and close it if it is open. The configuration commit fails if the Edit lock is open.
Device has been added, but failed to synchronize. Please try manual re-synchronization. Error while reading config from device: device_name, Detail - Fail while executing following RPC: <get-configuration database=committed><configuration></configuration></get-configuration>	Try to resynchronize the devices manually. For details, see *Resynchronizing Device Configuration*.
Error while reading config from device: device-name Failed while executing the following RPC: <get-hardware-inventory/>	Check the hardware details of the switch using the CLI command **show chassis hardware detail**. If the output displays a message **error: command is not valid**, then the Junos image on the specified switch is corrupted and you need to upgrade to the latest version of Junos.

Related Documentation

- Discovering Devices in a Physical Network on page 455
- *Resynchronizing Device Configuration*

Copyright © 2013, Juniper Networks, Inc.

Copyright © 2013, Juniper Networks, Inc.