

## Chapter 34

# Router Chassis Configuration Guidelines

You can configure properties of the router chassis, including the clock source, conditions that activate the red and yellow alarm LEDs on the router's craft interface, and SONET/SDH framing and concatenation properties for individual Physical Interface Cards (PICs).

To configure router chassis properties, include the following statements at the [edit chassis] hierarchy level:

```
chassis {
  aggregated-devices {
    ethernet {
      device-count number;
    }
    sonet {
      device-count number;
    }
  }
  alarm {
    interface-type {
      alarm-name (red | yellow | ignore);
    }
  }
  fpc slot-number {
    pic pic-number {
      atm-cell-relay-accumulation;
      atm-l2circuit-mode (cell | aal5 | trunk trunk);
      vtmapping number;
      ce1 {
        e1 port-number {
          channel-group group-number timeslots slot-number;
        }
      }
      ct3 {
        port port-number {
          t1 link-number {
            channel-group group-number timeslots slot-number;
          }
        }
      }
    }
  }
}
```

```

framing (sdh | sonet);
idle-cell-format {
    itu-t;
    payload-pattern;
}
max-queues-per-interface (8 | 4);
mlfr-uni-nni-bundles number;
no-concatenate;
t1;
vtmapping (itu-t | klm);
}
}
lcc number {
    fpc number {
        pic number {
            atm-cell-relay-accumulation;
            atm-l2-circuit-mode (cell | aal5 | trunk trunk);
            framing (sdh | sonet);
            idle-cell-format {
                itu-t;
                payload-pattern payload-pattern-byte;
            }
            max-queues-per-interface (8 | 4);
            no-concatenate;
        }
    }
    offline;
    online-expected;
}
(packet-scheduling | no-packet-scheduling);
no-concatenate;
(source-route | no-source-route);
redundancy {
    failover {
        on-loss-of-keepalives;
        on-disk-failure;
    }
    graceful-switchover (disable | enable);
    keepalive-time seconds;
    routing-engine slot-number (master | backup | disabled);
    sfm slot-number (always | preferred);
    ssb slot-number (always | preferred);
}
vrf-mtu-check;
}

```



**NOTE:** The configuration statements at the [edit chassis lcc] hierarchy apply only to a routing matrix. For information about a routing matrix, see the “TX Matrix Platform and T640 Routing Node Configuration Guidelines” on page 742 and the *TX Matrix Platform Hardware Guide*.

---

This chapter describes the following tasks for configuring the router chassis:

Minimum Chassis Configuration on page 698

Configuring Aggregated Devices on page 698

Configuring ATM Cell-Relay Accumulation Mode on an ATM1 PIC on page 699

Configuring Conditions That Trigger Alarms on page 699

Configuring SONET/SDH Framing on page 720

Configuring Sparse DLCI Mode on page 721

Configuring Channelized PIC Operation on page 722

Configuring Channelized DS3-to-DS0 Naming on page 723

Configuring Eight Queues on IQ Interfaces on page 725

Configuring Channelized E1 Naming on page 725

Configuring Channelized STM1 Interface Virtual Tributary Mapping on page 727

Configuring ATM2 Intelligent Queuing Layer 2 Circuit Transport Mode on page 728

Enabling ILMI for Cell Relay on page 729

Configuring the Drop Policy for Traffic with Source-Route Constraints on page 729

Configuring Packet Scheduling on page 730

Configuring the Link Services PICs on page 730

Configuring the Idle Cell Format on page 731

Configuring an MTU Path Check for a Routing Instance on page 732

Configuring Redundancy on page 733

TX Matrix Platform and T640 Routing Node Configuration Guidelines on page 742

## Minimum Chassis Configuration

---

All of the statements at the [edit chassis] hierarchy level of the configuration are optional.

## Configuring Aggregated Devices

---

JUNOS software supports the aggregation of physical devices into defined virtual links, such as the link aggregation of Ethernet interfaces defined by the IEEE 802.3ad standard. To define the virtual links, you need to specify the associations between physical and logical devices within the [edit interfaces] hierarchy, and assign the correct number of logical devices by including the device-count statement at the [edit chassis aggregated-devices ethernet] and [edit chassis aggregated-devices sonet] hierarchy levels:

```
[edit chassis]
aggregated-devices {
  ethernet {
    device-count number;
  }
  sonet {
    device-count number;
  }
}
```

The maximum number of Ethernet logical interface you can configure is 128. The aggregated Ethernet interfaces are numbered from ae0 through ae127. The maximum number of SONET/SDH logical interfaces is 16. The aggregated SONET/SDH interfaces are numbered from as0 through as15.

For more information on physical and logical interfaces using aggregated links, including sample configurations, see the *JUNOS Network Interfaces and Class of Service Configuration Guide*.

## Configuring ATM Cell-Relay Accumulation Mode on an ATM1 PIC

You can configure Asynchronous Transfer Mode (ATM) 1 PIC to use cell-relay accumulation mode. In this mode, the incoming cells (1 to 8 cells) are packaged in to a single packet and forwarded to the label-switched path (LSP). At the edge router, this packet is divided in to individual cells and transmitted over the ATM interface.



**NOTE:** When you configure an ATM PIC to use cell-relay accumulation, all ports on the ATM PIC use cell-relay accumulation mode.

To configure an ATM PIC to use cell-relay accumulation mode, include the `atm-cell-relay-accumulation` statement at the `[edit chassis fpc slot-number pic pic-number]` hierarchy level:

```
[edit chassis fpc slot-number pic pic-number ]
atm-cell-relay-accumulation;
```

On a TX Matrix platform, include the `atm-cell-relay-accumulation` statement at the `[edit chassis lcc number fpc slot-number pic pic-number]` hierarchy level:

```
[edit chassis lcc number fpc slot-number pic pic-number]
atm-cell-relay-accumulation;
```

For more information about configuring a TX Matrix platform, see the “TX Matrix Platform and T640 Routing Node Configuration Guidelines” on page 742.

## Configuring Conditions That Trigger Alarms

For the different types of PICs, you can configure which conditions trigger alarms and whether they trigger a red or yellow alarm. Red alarm conditions light the RED ALARM LED on the router’s craft interface and trigger an audible alarm if one is connected to the contacts on the craft interface. Yellow alarm conditions light the YELLOW ALARM LED on the router’s craft interface and trigger an audible alarm if one is connected to the craft interface.



**NOTE:** By default, any failure condition on the integrated-services interface (Adaptive Services PIC) triggers a red alarm.

To configure conditions that trigger alarms and that can occur on any interface of the specified type, include the alarm statement at the `[edit chassis]` hierarchy level:

```
[edit chassis]
alarm {
  interface-type {
    alarm-name (red | yellow | ignore);
  }
}
```

*alarm-name* is the name of an alarm. Table 27 lists the systemwide alarms and the alarms for each interface type.

Table 27: Configurable PIC Alarm Conditions

Interface/System	Alarm Condition	Configuration Option
<b>SONET/SDH and ATM</b>	Link alarm indication signal	ais-l
	Path alarm indication signal	ais-p
	Signal degrade (SD)	ber-sd
	Signal fail (SF)	ber-sf
	Loss of cell delineation (ATM only)	locd
	Loss of framing	lof
	Loss of light	lol
	Loss of pointer	lop-p
	Loss of signal	los
	Phase locked loop out of lock	pll
	Synchronous transport signal (STS) payload label (C2) mismatch	plm-p
	Line remote failure indication	rfl-l
	Path remote failure indication	rfl-p
	STS path (C2) unequipped	uneq-p
<b>E3/T3</b>	Alarm indicator signal	ais
	Excessive numbers of zeros	exz
	Failure of the far end	ferf
	Idle alarm	idle
	Line code violation	lcv
	Loss of frame	lof
	Loss of signal	los
	Phase locked loop out of lock	pll
Yellow alarm	ylw	
<b>Ethernet</b>	Link has gone down	link-down
<b>DS1</b>	Alarm indicator signal	ais
	Yellow alarm	ylw
<b>Integrated-services</b>	Hardware or software failure	failure
<b>Management-Ethernet</b>	Link has gone down	link-down

## Chassis Conditions That Trigger Alarms

Various conditions related to the chassis components trigger yellow and red alarms. You cannot configure these conditions. Table 28 through Table 34 list the alarms that the chassis components can generate. For information about chassis alarms for J-series Services routers, see the *J-series Services Router User Guide*. For information about chassis alarms for the TX Matrix platform, see the *TX Matrix Platform Hardware Guide*.

Table 28 lists the alarms that the chassis components can generate on an M5 or M10 Internet router.

**Table 28: Chassis Components Alarm Conditions on an M5 or M10 Router**

Chassis Component	Alarm Condition	Remedy	Alarm Severity
<b>Alternative media</b>	The router boots from an alternate boot device, the hard disk. Typically, the router boots from the flash drive. If you configure your router to boot from the hard disk, ignore this alarm condition. For more information about alternate boot devices, see “Boot Devices” on page 304.	Open a support case using the Case Manager link at <a href="http://www.juniper.net/support/">http://www.juniper.net/support/</a> or call 1-888-314-JTAC (within the United States) or 1-408-745-9500 (from outside the United States).	Yellow
<b>Craft interface</b>	The craft interface has failed.	Replace failed craft interface.	Red
<b>Fan trays</b>	One fan tray has been removed from the chassis.	Install missing fan tray.	Yellow
	Two or more fan trays have been removed from the chassis.	Install missing fan trays.	Red
	One fan in the chassis is not spinning or spinning below required speed.	Replace failed fan tray.	Red
<b>Forwarding Engine Board (FEB)</b>	The control board has failed. If this occurs, the board attempts to reboot.	Replace failed FEB.	Red
<b>Flexible PIC Concentrator (FPC)</b>	An FPC has failed. If this occurs, the FPC attempts to reboot. If the FEB sees that an FPC is rebooting too often, it shuts down the FPC.	Replace failed FPC.	Red
<b>Hot swapping</b>	Too many hot-swap interrupts are occurring. This message generally indicates that a hardware component that plugs into the router’s backplane from the front (generally, an FPC) is broken.	-----	Red

Chassis Component	Alarm Condition	Remedy	Alarm Severity
<b>Routing Engine</b>	Error in reading or writing compact flash.	Reformat compact flash and install bootable image. If this fails, replace failed Routing Engine.	Yellow
	System booted from hard disk.	Install bootable image on compact flash. If this fails, replace failed Routing Engine.	Yellow
	Compact flash missing in boot list.	Replace failed Routing Engine.	Red
	Hard disk missing in boot list.	Replace failed Routing Engine.	Red
<b>Power supplies</b>	A power supply has been removed from the chassis.	Install missing power supply.	Yellow
	A power supply has failed.	Replace failed power supply.	Red
<b>Temperature</b>	The chassis temperature has exceeded 55 degrees C, the fans have been turned on to full speed, and one or more fans have failed.	Check room temperature. Check air filter and replace it. Check air flow. Check fan.	Yellow
	The chassis temperature has exceeded 65 degrees C and the fans have been turned on to full speed.	Check room temperature. Check air filter and replace it. Check air flow. Check fan.	Yellow
	The chassis temperature has exceeded 65 degrees C and a fan has failed. If this condition persists for more than 4 minutes, the router shuts down.	Check room temperature. Check air filter and replace it. Check air flow. Check fan.	Red
	The chassis temperature has exceeded 75 degrees C. If this condition persists for more than 4 minutes, the router shuts down.	Check room temperature. Check air filter and replace it. Check air flow. Check fan.	Red
	The temperature sensor has failed.	Open a support case using the Case Manager link at <a href="http://www.juniper.net/support/">http://www.juniper.net/support/</a> or call 1-888-314-JTAC (within the United States) or 1-408-745-9500 (from outside the United States).	Red

Table 29 lists the alarms that the chassis components can generate on an M7i or M10i Internet router.

**Table 29: Chassis Components Alarm Conditions on an M7i or M10i Router**

Chassis Component	Alarm Condition	Remedy	Alarm Severity
<b>Alternative media</b>	The router has a optional flash disk and boots from an alternate boot device. If you configure your router to boot from the hard disk, ignore this alarm condition. For more information about alternate boot devices, see “Boot Devices” on page 304.	Open a support case using the Case Manager link at <a href="http://www.juniper.net/support/">http://www.juniper.net/support/</a> or call 1-888-314-JTAC (within the United States) or 1-408-745-9500 (from outside the United States).	Yellow
<b>Compact FEB (CFEB)</b>	For an M7i router, CFEB has failed. If this occurs, the board attempts to reboot.	Replace failed CFEB.	Red
	For an M10i router, both control boards have been removed or have failed.	Replace failed or missing CFEB.	Red
	Too many hard errors in CFEB memory.	Replace failed CFEB.	Red
	Too many soft errors in CFEB memory.	Replace failed CFEB.	Red
	A CFEB microcode download has failed.	Replace failed CFEB.	Red
<b>Fan trays</b>	A fan has failed.	Replace failed fan tray.	Red
	For an M7i router, a fan tray has been removed from the chassis.	Install missing fan tray.	Red
	For an M10i router, both fan trays are absent from the chassis.	Install missing fan tray.	Red
<b>Hot swapping</b>	Too many hot-swap interrupts are occurring. This message generally indicates that a hardware component that plugs into the router's midplane from the front is broken.	-----	Red
<b>Power supplies</b>	A power supply has been removed.	Insert missing power supply.	Yellow
	A power supply has failed.	Replace failed power supply.	Red
	For an M10i router, only one power supply is operating.	Insert or replace secondary power supply.	Red

Chassis Component	Alarm Condition	Remedy	Alarm Severity
<b>Routing Engine</b>	Error in reading or writing hard disk.	Reformat hard disk and install bootable image. If this fails, replace failed Routing Engine.	Yellow
	Error in reading or writing compact flash.	Reformat compact flash and install bootable image. If this fails, replace failed Routing Engine.	Yellow
	System booted from hard disk. This alarm only applies, if you have an optional flash drive.	Install bootable image on compact flash. If this fails, replace failed Routing Engine.	Yellow
	Compact flash missing in boot list.	Replace failed Routing Engine.	Red
	Hard disk missing in boot list.	Replace failed Routing Engine.	Red
	Routing Engine failed to boot.	Replace failed Routing Engine.	Red
<b>Temperature</b>	The chassis temperature has exceeded 55 degrees C, the fans have been turned on to full speed and one or more fans have failed.	Check room temperature. Check air filter and replace it. Check air flow. Check fan.	Yellow
	The chassis temperature has exceeded 65 degrees C and the fans have been turned on to full speed.	Check room temperature. Check air filter and replace it. Check air flow. Check fan.	Yellow
	The chassis temperature has exceeded 65 degrees C and a fan has failed. If this condition persists for more than 4 minutes, the router shuts down.	Check room temperature. Check air filter and replace it. Check air flow. Check fan.	Red
	The chassis temperature has exceeded 75 degrees C. If this condition persists for more than 4 minutes, the router shuts down.	Check room temperature. Check air filter and replace it. Check air flow. Check fan.	Red
	The temperature sensor has failed.	Open a support case using the Case Manager link at <a href="http://www.juniper.net/support/">http://www.juniper.net/support/</a> or call 1-888-314-JTAC (within the United States) or 1-408-745-9500 (from outside the United States).	Red

Table 30 lists the alarms that the chassis components can generate on an M20 Internet router.

**Table 30: Chassis Components Alarm Conditions for an M20 Router**

Chassis Component	Alarm Condition	Remedy	Alarm Severity
<b>Alternative media</b>	The router boots from an alternate boot device, the hard disk. Typically, the router boots from the flash drive. If you configure your router to boot from the hard disk, ignore this alarm condition. For more information about alternate boot devices, see “Boot Devices” on page 304.	Open a support case using the Case Manager link at <a href="http://www.juniper.net/support/">http://www.juniper.net/support/</a> or call 1-888-314-JTAC (within the United States) or 1-408-745-9500 (from outside the United States).	Yellow
<b>Craft interface</b>	The craft interface has failed.	Replace failed craft interface.	Red
<b>Fan trays</b>	One fan tray has been removed from the chassis.	Install missing fan tray.	Yellow
	Two or more fan trays have been removed from the chassis.	Install missing fan trays.	Red
	One fan in the chassis is not spinning or spinning below requires speed.	Replace fan tray.	Red
<b>FPC</b>	An FPC has failed. If this occurs, the FPC attempts to reboot. If the System and Switch Board (SSB) sees that an FPC is rebooting too often, it shuts down the FPC.	Replace failed FPC.	Red
<b>Hot swapping</b>	Too many hot-swap interrupts are occurring. This message generally indicates that a hardware component that plugs in to the router’s backplane from the front (generally, an FPC) is broken.	-----	Red

Chassis Component	Alarm Condition	Remedy	Alarm Severity
<b>Routing Engine</b>	Error in reading or writing hard disk.	Reformat hard disk and install bootable image. If this fails, replace failed Routing Engine.	Yellow
	Error in reading or writing compact flash.	Reformat compact flash and install bootable image. If this fails, replace failed Routing Engine.	Yellow
	System booted from default backup Routing Engine. If you manually switched mastership, ignore this alarm condition.	Install bootable image on default master Routing Engine. If this fails, replace failed Routing Engine.	Yellow
	System booted from hard disk.	Install bootable image on compact flash. If this fails, replace failed Routing Engine.	Yellow
	Compact flash missing in boot list.	Replace failed Routing Engine.	Red
	Hard disk missing in boot list.	Replace failed Routing Engine.	Red
	Routing Engine failed to boot.	Replace failed Routing Engine.	Red
<b>Power supplies</b>	A power supply has been removed from the chassis.	Insert power supply into empty slot.	Yellow
	A power supply has failed.	Replace failed power supply.	Red
<b>SSB</b>	The control board has failed. If this occurs, the board attempts to reboot.	Replace failed control board.	Red

Chassis Component	Alarm Condition	Remedy	Alarm Severity
Temperature	The chassis temperature has exceeded 55 degrees C, the fans have been turned on to full speed, and one or more fans have failed.	Check room temperature. Check air filter and replace it. Check air flow. Check fan.	Yellow
	The chassis temperature has exceeded 65 degrees C and the fans have been turned on to full speed.	Check room temperature. Check air filter and replace it. Check air flow. Check fan.	Yellow
	The chassis temperature has exceeded 65 degrees C and a fan has failed. If this condition persists for more than 4 minutes, the router shuts down.	Check room temperature. Check air filter and replace it. Check air flow. Check fan.	Red
	The chassis temperature has exceeded 75 degrees C. If this condition persists for more than 4 minutes, the router shuts down.	Check room temperature. Check air filter and replace it. Check air flow. Check fan.	Red
	The temperature sensor has failed.	Open a support case using the Case Manager link at <a href="http://www.juniper.net/support/">http://www.juniper.net/support/</a> or call 1-888-314-JTAC (within the United States) or 1-408-745-9500 (from outside the United States).	Red

Table 31 lists the alarms that the chassis components can generate on an M40 Internet router.

**Table 31: Chassis Component Alarm Conditions for an M40 Router**

Chassis Component	Alarm Condition	Remedy	Alarm Severity
<b>Air filter</b>	Change air filter.	Change air filter.	-----
<b>Alternative media</b>	The router boots from an alternate boot device, the hard disk. Typically, the router boots from the flash drive. If you configure your router to boot from the hard disk, ignore this alarm condition. For more information about alternate boot devices, see "Boot Devices" on page 304.	Open a support case using the Case Manager link at <a href="http://www.juniper.net/support/">http://www.juniper.net/support/</a> or call 1-888-314-JTAC (within the United States) or 1-408-745-9500 (from outside the United States).	Yellow
<b>Craft interface</b>	The craft interface has failed.	Replace failed craft interface.	Red
<b>Fan trays</b>	One fan tray has been removed from the chassis.	Install missing fan tray.	Yellow
	Two or more fan trays have been removed from the chassis.	Install missing fan trays.	Red
	One fan in the chassis is not spinning or spinning below required speed.	Replace fan tray.	Red
<b>FPC</b>	An FPC has an out of range or invalid temperature reading.	Replace failed FPC.	Yellow
	An FPC microcode download has failed.	Replace failed FPC.	Red
	An FPC has failed. If this occurs, the FPC attempts to reboot. If the SCB sees that an FPC is rebooting too often, it shuts down the FPC.	Replace failed FPC.	Red
	Too many hard errors in FPC memory.	Replace failed FPC.	Red
	Too many soft errors in FPC memory.	Replace failed FPC.	Red
<b>Hot swapping</b>	Too many hot-swap interrupts are occurring. This message generally indicates that a hardware component that plugs into the router's backplane from the front (generally, an FPC) is broken.	-----	Red

Chassis Component	Alarm Condition	Remedy	Alarm Severity
Power supplies	A power supply has been removed from the chassis.	Insert power supply into empty slot.	Yellow
	A power supply temperature sensor has failed.	Replace failed power supply or power entry module.	Yellow
	A power supply fan has failed.	Replace failed power supply fan.	Yellow
	A power supply has high temperature.	Replace failed power supply or power entry module.	Red
	A 5V power supply has failed.	Replace failed power supply or power entry module.	Red
	A 3.3V power supply has failed.	Replace failed power supply or power entry module.	Red
	A 2.5V power supply has failed.	Replace failed power supply or power entry module.	Red
	A power supply input has failed.	Check power supply input connection.	Red
	A power supply has failed.	Replace failed power supply or power entry module.	Red
	Routing Engine	Error in reading or writing hard disk.	Reformat hard disk and install bootable image. If this fails, replace failed Routing Engine.
Error in reading or writing compact flash.		Reformat compact flash and install bootable image. If this fails, replace failed Routing Engine.	Yellow
System booted from default backup Routing Engine. If you manually switched mastership, ignore this alarm condition.		Install bootable image on default master Routing Engine. If this fails, replace failed Routing Engine.	Yellow
System booted from hard disk.		Install bootable image on compact flash. If this fails, replace failed Routing Engine.	Yellow
Compact flash missing in boot list.		Replace failed Routing Engine.	Red
Hard disk missing in boot list.		Replace failed Routing Engine.	Red
Routing Engine failed to boot.		Replace failed Routing Engine.	Red
SCB	The System Control Board (SCB) has failed. If this occurs, the board attempts to reboot.	Replace failed SCB.	Red

Chassis Component	Alarm Condition	Remedy	Alarm Severity
Temperature	The chassis temperature has exceeded 55 degrees C, the fans have been turned on to full speed, and one or more fans have failed.	Check room temperature. Check air filter and replace it. Check air flow. Check fan.	Yellow
	The chassis temperature has exceeded 65 degrees C and the fans have been turned on to full speed.	Check room temperature. Check air filter and replace it. Check air flow. Check fan.	Yellow
	The chassis temperature has exceeded 65 degrees C and a fan has failed. If this condition persists for more than 4 minutes, the router shuts down.	Check room temperature. Check air filter and replace it. Check air flow. Check fan.	Red
	The chassis temperature has exceeded 75 degrees C. If this condition persists for more than 4 minutes, the router shuts down.	Check room temperature. Check air filter and replace it. Check air flow. Check fan.	Red
	The temperature sensor has failed.	Open a support case using the Case Manager link at <a href="http://www.juniper.net/support/">http://www.juniper.net/support/</a> or call 1-888-314-JTAC (within the United States) or 1-408-745-9500 (from outside the United States).	Red

Table 32 lists the alarms that the chassis components can generate on an M40e or M160 Internet router.

**Table 32: Chassis Component Alarm Conditions for an M40e or M160 Router**

Chassis Component	Alarm Condition	Remedy	Alarm Severity
Air filter	Change air filter.	Change air filter	----- -
Alternative media	The router boots from an alternate boot device, the hard disk. Typically, the router boots from the flash drive. If you configure your router to boot from the hard disk, ignore this alarm condition. For more information about alternate boot devices, see "Boot Devices" on page 304.	Open a support case using the Case Manager link at <a href="http://www.juniper.net/support/">http://www.juniper.net/support/</a> or call 1-888-314-JTAC (within the United States) or 1-408-745-9500 (from outside the United States).	Yellow

Chassis Component	Alarm Condition	Remedy	Alarm Severity
<b>Connector Interface Panel (CIP)</b>	A CIP is missing.	Insert CIP into empty slot.	Red
<b>Craft interface</b>	The craft interface has failed.	Replace failed craft interface.	Red
<b>Fan trays</b>	One fan tray has been removed from the chassis.	Install missing fan tray.	Yellow
	Two or more fan trays have been removed from the chassis.	Install missing fan trays.	Red
	One fan in the chassis is not spinning or spinning below required speed.	Replace fan tray.	Red
<b>FPC</b>	An FPC has an out of range or invalid temperature reading.	Replace failed FPC.	Yellow
	An FPC microcode download has failed.	Replace failed FPC.	Red
	An FPC has failed. If this occurs, the FPC attempts to reboot. If the MCS sees that an FPC is rebooting too often, it shuts down the FPC.	Replace failed FPC.	Red
	Too many hard errors in FPC memory.	Replace failed FPC.	Red
	Too many soft errors in FPC memory.	Replace failed FPC.	Red
<b>Hot swapping</b>	Too many hot-swap interrupts are occurring. This message generally indicates that a hardware component that plugs into the router's backplane from the front (generally, an FPC) is broken.	-----	Red
<b>Miscellaneous Control Subsystem (MCS)</b>	An MCS has an out of range or invalid temperature reading.	Replace failed MCS.	Yellow
	MCS0 has been removed.	Reinstall MCS0.	Yellow
	An MCS has failed.	Replace failed MCS.	Red
<b>Packet Forwarding Engine Clock Generator (PCG)</b>	A backup PCG is offline.	Set backup PCG online.	Yellow
	A PCG has an out of range or invalid temperature reading.	Replace failed PCG.	Yellow
	A PCG has been removed.	Insert PCG into empty slot.	Yellow
	A PCG has failed to come online.	Replace failed PCG.	Red

<b>Chassis Component</b>	<b>Alarm Condition</b>	<b>Remedy</b>	<b>Alarm Severity</b>
<b>Routing Engine</b>	Error in reading or writing hard disk.	Reformat hard disk and install bootable image. If this fails, replace failed Routing Engine.	Yellow
	Error in reading or writing compact flash.	Reformat compact flash and install bootable image. If this fails, replace failed Routing Engine.	Yellow
	System booted from default backup Routing Engine. If you manually switched mastership, ignore this alarm condition.	Install bootable image on default master Routing Engine. If this fails, replace failed Routing Engine.	Yellow
	System booted from hard disk.	Install bootable image on compact flash. If this fails, replace failed Routing Engine.	Yellow
	Compact flash missing in boot list.	Replace failed Routing Engine.	Red
	Hard disk missing in boot list.	Replace failed Routing Engine.	Red
	Routing Engine failed to boot.	Replace failed Routing Engine.	Red
<b>Power supplies</b>	A power supply has been removed from the chassis.	Insert power supply into empty slot.	Yellow
	A power supply has failed.	Replace failed power supply.	Red
<b>Switching and Forwarding Module (SFM)</b>	A SFM has an out of range or invalid temperature reading on SPP.	Replace failed SFM.	Yellow
	A SFM has an out of range or invalid temperature reading on SPR.	Replace failed SFM.	Yellow
	A SFM is offline.	Set SFM online.	Yellow
	A SFM has failed.	Replace failed SFM.	Red
	A SFM has been removed from the chassis.	Insert SFM into empty slot.	Red
	All SFMs are offline or missing from the chassis.	Insert SFMs into empty slots or set all SFMs online.	Red

Chassis Component	Alarm Condition	Remedy	Alarm Severity
Temperature	The chassis temperature has exceeded 55 degrees C, the fans have been turned on to full speed, and one or more fans have failed.	Check room temperature. Check air filter and replace it. Check air flow. Check fan.	Yellow
	The chassis temperature has exceeded 65 degrees C and the fans have been turned on to full speed.	Check room temperature. Check air filter and replace it. Check air flow. Check fan.	Yellow
	The chassis temperature has exceeded 65 degrees C and a fan has failed. If this condition persists for more than 4 minutes, the router shuts down.	Check room temperature. Check air filter and replace it. Check air flow. Check fan.	Red
	The chassis temperature has exceeded 75 degrees C. If this condition persists for more than 4 minutes, the router shuts down.	Check room temperature. Check air filter and replace it. Check air flow. Check fan.	Red
	The temperature sensor has failed.	Open a support case using the Case Manager link at <a href="http://www.juniper.net/support/">http://www.juniper.net/support/</a> or call 1-888-314-JTAC (within the United States) or 1-408-745-9500 (from outside the United States).	Red

Table 33 lists the alarms that the chassis components can generate on an M320 Internet router.

**Table 33: Chassis Component Alarm Conditions for an M320 Router**

Chassis Component	Alarm Condition	Remedy	Alarm Severity
<b>Air filters</b>	Change air filter.	Change air filter.	-----
<b>Alternative media</b>	The router boots from an alternate boot device, the hard disk. Typically, the router boots from the flash drive. If you configure your router to boot from the hard disk, ignore this alarm condition. For more information about alternate boot devices, see “Boot Devices” on page 304.	Open a support case using the Case Manager link at <a href="http://www.juniper.net/support/">http://www.juniper.net/support/</a> or call 1-888-314-JTAC (within the United States) or 1-408-745-9500 (from outside the United States).	Yellow
<b>Control Board (CB)</b>	A CB has been removed.	Insert CB into empty slot.	Yellow
	A CB temperature sensor alarm has failed.	Replace failed CB.	Yellow
	A CB has failed.	Replace failed CB.	Red
<b>CIP</b>	A CIP is missing.	Insert CIP into empty slot.	Red
<b>Craft interface</b>	The craft interface has failed.	Replace failed craft interface.	Red
<b>Fan trays</b>	One fan tray has been removed from the chassis.	Install missing fan tray.	Yellow
	Two or more fan trays have been removed from the chassis.	Install missing fan trays.	Red
	One fan in the chassis is not spinning or spinning below required speed.	Replace fan tray.	Red
<b>FPC</b>	An FPC has an out of range or invalid temperature reading.	Replace failed FPC.	Yellow
	A FPC microcode download has failed.	Replace failed FPC.	Red
	An FPC has failed. If this occurs, the FPC attempts to reboot. If the CB sees that an FPC is rebooting too often, it shuts down the FPC.	Replace failed FPC.	Red
	Too many hard errors in FPC memory.	Replace failed FPC.	Red
	Too many soft errors in FPC memory.	Replace failed FPC.	Red

Chassis Component	Alarm Condition	Remedy	Alarm Severity
<b>Hot swapping</b>	Too many hot-swap interrupts are occurring. This message generally indicates that a hardware component that plugs into the router's backplane from the front (generally, an FPC) is broken.	-----	Red
<b>Power supplies</b>	A power supply has been removed from the chassis.	Insert power supply into empty slot.	Yellow
	A power supply has failed.	Replace failed power supply.	Red
<b>Routing Engine</b>	Error in reading or writing hard disk.	Reformat hard disk and install bootable image. If this fails, replace failed Routing Engine.	Yellow
	Error in reading or writing compact flash.	Reformat compact flash and install bootable image. If this fails, replace failed Routing Engine.	Yellow
	System booted from default backup Routing Engine. If you manually switched mastership, ignore this alarm condition.	Install bootable image on default master Routing Engine. If this fails, replace failed Routing Engine.	Yellow
	System booted from hard disk.	Install bootable image on compact flash. If this fails, replace failed Routing Engine.	Yellow
	Compact flash missing in boot list.	Replace failed Routing Engine.	Red
	Hard disk missing in boot list.	Replace failed Routing Engine.	Red
	Routing Engine failed to boot.	Replace failed Routing Engine.	Red
<b>Switch Interface Board (SIB)</b>	A spare SIB is missing.	Insert spare SIB in to empty slot.	Yellow
	An SIB has failed.	Replace failed SIB.	Yellow
	A spare SIB has failed.	Replace failed SIB.	Yellow
	An SIB has an out of range or invalid temperature reading.	Replace failed SIB.	Yellow
	An SIB is missing.	Insert SIB into empty slot.	Red
	An SIB has failed.	Replace failed SIB.	Red

Chassis Component	Alarm Condition	Remedy	Alarm Severity
Temperature	The chassis temperature has exceeded 55 degrees C, the fans have been turned on to full speed, and one or more fans have failed.	<p>Check room temperature.</p> <p>Check air filter and replace it.</p> <p>Check air flow.</p> <p>Check fan.</p>	Yellow
	The chassis temperature has exceeded 65 degrees C and the fans have been turned on to full speed.	<p>Check room temperature.</p> <p>Check air filter and replace it.</p> <p>Check air flow.</p> <p>Check fan.</p>	Yellow
	The chassis temperature has exceeded 65 degrees C and a fan has failed. If this condition persists for more than 4 minutes, the router shuts down.	<p>Check room temperature.</p> <p>Check air filter and replace it.</p> <p>Check air flow.</p> <p>Check fan.</p>	Red
	Chassis temperature has exceeded 75 degrees C. If this condition persists for more than 4 minutes, the router shuts down.	<p>Check room temperature.</p> <p>Check air filter and replace it.</p> <p>Check air flow.</p> <p>Check fan.</p>	Red
	The temperature sensor has failed.	Open a support case using the Case Manager link at <a href="http://www.juniper.net/support/">http://www.juniper.net/support/</a> or call 1-888-314-JTAC (within the United States) or 1-408-745-9500 (from outside the United States).	Red

Table 34 lists the alarms that the chassis components can generate on a T320 or T640 Internet routing platform.

**Table 34: Chassis Component Alarm Conditions for the T320 or T640 Routing Platform**

Chassis Component	Alarm Condition	Remedy	Alarm Severity
<b>Air filter</b>	Change air filter.	Change air filter.	-----
<b>Alternative media</b>	The router boots from an alternate boot device, the hard disk. Typically, the router boots from the flash drive. If you configure your router to boot from the hard disk, ignore this alarm condition. For more information about alternate boot devices, see "Boot Devices" on page 304.	Open a support case using the Case Manager link at <a href="http://www.juniper.net/support/">http://www.juniper.net/support/</a> or call 1-888-314-JTAC (within the United States) or 1-408-745-9500 (from outside the United States).	Yellow
<b>CB</b>	A CB has been removed.	Insert CB into empty slot.	Yellow
	A CB temperature sensor alarm has failed.	Replace failed CB.	Yellow
	A CB has failed.	Replace failed CB.	Red
<b>CIP</b>	A CIP is missing.	Insert CIP into empty slot.	Red
<b>Craft interface</b>	The craft interface has failed.	Replace failed craft interface.	Red
<b>Fan trays</b>	One fan tray has been removed from the chassis.	Install missing fan tray.	Yellow
	Two or more fan trays have been removed from the chassis.	Install missing fan trays.	Red
	One fan in the chassis is not spinning or spinning below required speed.	Replace fan tray.	Red
<b>FPC</b>	An FPC has an out of range or invalid temperature reading.	Replace failed FPC.	Yellow
	An FPC microcode download has failed.	Replace failed FPC.	Red
	An FPC has failed. If this occurs, the FPC attempts to reboot. If the CB sees that an FPC is rebooting too often, it shuts down the FPC.	Replace failed FPC.	Red
	Too many hard errors in FPC memory.	Replace failed FPC.	Red
	Too many soft errors in FPC memory.	Replace failed FPC.	Red
<b>Hot swapping</b>	Too many hot-swap interrupts are occurring. This message generally indicates that a hardware component that plugs into the router's backplane from the front (generally, an FPC) is broken.	-----	Red

Chassis Component	Alarm Condition	Remedy	Alarm Severity
<b>Routing Engine</b>	Error in reading or writing hard disk.	Reformat hard disk and install bootable image. If this fails, replace failed Routing Engine.	Yellow
	Error in reading or writing compact flash.	Reformat compact flash and install bootable image. If this fails, replace failed Routing Engine.	Yellow
	System booted from default backup Routing Engine. If you manually switched mastership, ignore this alarm condition.	Install bootable image on default master Routing Engine. If this fails, replace failed Routing Engine.	Yellow
	System booted from hard disk.	Install bootable image on compact flash. If this fails, replace failed Routing Engine.	Yellow
	Compact flash missing in boot list.	Replace failed Routing Engine.	Red
	Hard disk missing in boot list.	Replace failed Routing Engine.	Red
	Routing Engine failed to boot.	Replace failed Routing Engine.	Red
<b>Power supplies</b>	A power supply has been removed from the chassis.	Insert power supply into empty slot.	Yellow
	A power supply has failed.	Replace failed power supply.	Red
<b>SONET Clock Generator (SCG)</b>	A backup SCG is offline.	Set backup SCG online.	Yellow
	An SCG has an out of range or invalid temperature reading.	Replace failed SCG.	Yellow
	An SCG has been removed.	Insert SCG into empty slot.	Yellow
	All SCGs are offline or missing.	Insert SCGs into empty slots or set all SCGs online.	Red
	An SCG has failed.	Replace failed SCG.	Red
<b>SIB</b>	A spare SIB is missing.	Insert spare SIB into empty slot.	Yellow
	An SIB has failed.	Replace failed SIB.	Yellow
	A spare SIB has failed.	Replace failed SIB.	Yellow
	A SIB has an out of range or invalid temperature reading.	Replace failed SIB.	Yellow
	An SIB is missing.	Insert SIB into empty slot.	Red
	An SIB has failed.	Replace failed SIB.	Red
<b>Switch Processor Mezzanine Board (SPMB)</b>	A local SPMB is offline.	Reset control board. If this fails, replace control board.	Red

Chassis Component	Alarm Condition	Remedy	Alarm Severity
Temperature	The chassis temperature has exceeded 55 degrees C, the fans have been turned on to full speed, and one or more fans have failed.	Check room temperature. Check air filter and replace it. Check air flow. Check fan.	Yellow
	The chassis temperature has exceeded 65 degrees C and the fans have been turned on to full speed.	Check room temperature. Check air filter and replace it. Check air flow. Check fan.	Yellow
	The chassis temperature has exceeded 65 degrees C and a fan has failed. If this condition persists for more than 4 minutes, the router shuts down.	Check room temperature. Check air filter and replace it. Check air flow. Check fan.	Red
	Chassis temperature has exceeded 75 degrees C. If this condition persists for more than 4 minutes, the router shuts down.	Check room temperature. Check air filter and replace it. Check air flow. Check fan.	Red
	The temperature sensor has failed.	Open a support case using the Case Manager link at <a href="http://www.juniper.net/support/">http://www.juniper.net/support/</a> or call 1-888-314-JTAC (within the United States) or 1-408-745-9500 (from outside the United States).	Red

### Silencing External Devices

You can manually silence external devices connected to the alarm relay contacts by pressing the alarm cutoff button located on the craft interface front panel. Silencing the device does not remove the alarm messages from the display (if present on the router) or extinguish the alarm LEDs. In addition, new alarms that occur after an external device is silenced reactivate the external device.

## Configuring SONET/SDH Framing

---

By default, SONET/SDH PICs use SONET framing. For a discussion of the differences between the two standards, see the *JUNOS Network Interfaces and Class of Service Configuration Guide*. To configure a PIC to use SDH framing, include the framing statement at the [edit chassis fpc slot-number pic pic-number] hierarchy level, specifying the sdh option:

```
[edit chassis]
user@host# set fpc slot-number pic pic-number framing sdh
[edit chassis]
user@host# show
fpc slot-number {
  pic pic-number {
    framing sdh;
  }
}
```

On a TX Matrix platform, include the framing statement at the [edit chassis lcc number fpc slot-number pic pic-number] hierarchy level, specifying the sdh option:

```
[edit chassis lcc number]
user@host# set fpc slot-number pic pic-number framing sdh
[edit chassis lcc number]
user@host# show
fpc slot-number {
  pic pic-number {
    framing sdh;
  }
}
```

To explicitly configure a PIC to use SONET framing, include the framing statement at the [edit chassis fpc slot-number pic pic-number] hierarchy level, specifying the sonet option:

```
[edit chassis]
user@host# set fpc slot-number pic pic-number framing sonet
[edit chassis]
user@host# show
fpc slot-number {
  pic pic-number
    framing sonet;
  }
}
```

On a TX Matrix platform, include the framing statement at the [edit chassis lcc number fpc slot-number pic pic-number] hierarchy level, specifying the sonet option: [edit chassis lcc number]

```
user@host# set fpc slot-number pic pic-number framing sonet
[edit chassis lcc number]
user@host# show
fpc slot-number {
    pic pic-number
    framing sonet;
}
```

For information about configuring a TX Matrix platform, see the “TX Matrix Platform and T640 Routing Node Configuration Guidelines” on page 742.

## Configuring Sparse DLCI Mode

---

By default, original channelized DS3 and original channelized STM1-to-E1 (or T1) interfaces can support a maximum of 64 data-link connection identifiers (DLCIs) per channel—as many as 1792 DLCIs per DS3 interface or 4032 DLCIs per STM1 interface (0 through 63).

In sparse DLCI mode, the full DLCI range (1 through 1022) is supported. This allows you to use circuit cross-connect (CCC) and translation cross-connect (TCC) features by means of Frame Relay on T1 and E1 interfaces. For more information about CCC and DLCIs, see the *JUNOS Network Interfaces and Class of Service Configuration Guide*.



**NOTE:** Sparse DLCI mode requires a Channelized STM1 or Channelized DS3 PIC.

DLCI 0 is reserved for Local Management Interface (LMI) signaling.

Channelized T3 intelligent queuing (IQ) and STM1 IQ interfaces support a maximum of 64 DLCIs, numbered 0 through 1022, and therefore do not require sparse mode.

---

To configure the router to use sparse DLCI mode, include the sparse-dlcis statement at the [edit chassis fpc slot-number pic pic-number] hierarchy level:

```
[edit chassis fpc slot-number pic pic-number ]
sparse-dlcis;
```

## Configuring Channelized PIC Operation

---

By default, SONET PICs (interfaces with names *so-fpc/pic/port*) operate in concatenated mode, a mode in which the bandwidth of the interface is in a single channel.

To configure a PIC to operate in channelized (multiplexed) mode, include the `no-concatenate` statement at the `[edit chassis fpc slot-number pic pic-number]` hierarchy level:

```
[edit chassis]
user@host# set fpc slot-number pic pic-number no-concatenate
[edit chassis]
user@host# show
fpc slot-number {
  pic pic-number {
    no-concatenate;
  }
}
```

On a TX Matrix platform, include the `no-concatenate` statement at the `[edit chassis lcc number fpc slot-number pic pic-number]` hierarchy level:

```
[edit chassis lcc number]
user@host# set fpc slot-number pic pic-number no-concatenate
[edit chassis lcc number]
user@host# show
fpc slot-number {
  pic pic-number
  no-concatenate;
}
}
```

When configuring and displaying information about interfaces that are operating in channelized mode, you must specify the channel number in the interface name (*physical:channel*); for example, `so-2/2/0:0` and `so-2/2/0:1`. For more information about interface names, see the *JUNOS Network Interfaces and Class of Service Configuration Guide*. For information about the TX Matrix platform, see the “TX Matrix Platform and T640 Routing Node Configuration Guidelines” on page 742.

### Concatenated and Nonconcatenated Mode

On SONET OC48 interfaces that are configured for channelized (multiplexed) mode, the `bytes e1-quiet` and `bytes f1` options in the `sonet-options` statement have no effect. The `bytes f2`, `bytes z3`, `bytes z4`, and `path-trace` options work correctly on channel 0. These bytes work in the transmit direction only on channels 1, 2, and 3.

The M160 four-port SONET/SDH OC12 PIC can run each of the OC12 links in concatenated mode only and requires a Type 2 M160 FPC. Similarly, the four-port SONET/SDH OC3 PIC cannot run in nonconcatenated mode on any platform.

## Configuring Channelized DS3-to-DS0 Naming

You can configure 28 T1 channels per T3 interface. Each T1 link can have up to eight channel groups, and each channel group can hold any combination of DS0 timeslots. To specify the T1 link and DS0 channel group number in the name, use colons (:) as separators. For example, a Channelized DS3-to-DS0 PIC might have the following physical and virtual interfaces:

```
ds-0/0/0:x:y
```

where *x* is a T1 link ranging from 0 through 27 and *y* is a DS0 channel group ranging from 0 through 7 (see Table 35 on page 724 for more information about ranges).

You can use any of the values within the range available for *x* and *y*; you do not have to configure the links sequentially. The software applies the interface options you configure according to the following rules:

You can configure t3-options for t1 link 0 and channel group 0 only; for example, ds-/0/0/0:0:0.

You can configure t1-options for any t1 link value, but only for channel group 0; for example, ds-0/0/0:x:0.

There are no restrictions on changing the default ds0-options.

If you delete a configuration you previously committed for channel group 0, the options return to the default values.

To configure the channel groups and timeslots for a channelized DS3 interface, include the channel-group and timeslots statements at the [edit chassis fpc slot-number pic *pic-number* ct3 port *port-number* t1 *link-number*] hierarchy level:

```
[edit chassis fpc slot-number pic pic-number ct3 port port-number t1 link-number]
fpc slot-number {
  pic pic-number {
    ct3 {
      port port-number {
        t1 link-number {
          channel-group group-number timeslots slot-number;
        }
      }
    }
  }
}
```



**NOTE:** If you commit the interface name but do not include the [edit chassis] configuration, the Channelized DS3-to-DS0 PIC behaves like a Channelized DS3-to-DS1 PIC: none of the DS0 functionality is accessible.

Table 35 shows the ranges for each of the quantities in the preceding configuration.

**Table 35: Ranges for Channelized DS3-to-DS0 Configuration**

Item	Variable	Range
FPC slot	<i>slot-number</i>	0 through 7(see note below)
PIC slot	<i>pic-number</i>	0 through 3
Port	<i>port-number</i>	0 through 1
T1 link	<i>link-number</i>	0 through 27
DS0 channel group	<i>group-number</i>	0 through 7
timeslot	<i>slot-number</i>	1 through 24



**NOTE:** The FPC slot range depends on the platform. The maximum range of 0 through 7 applies to M40 routers; for M20 routers, the range is 0 through 3; for M10 routers the range is 0 through 1; for M5 routers, the only applicable value is 0. The Multichannel DS3 (Channelized DS3-to-DS0) PIC is not supported on M160 routers.

Bandwidth limitations restrict the interface to a maximum of 128 channel groups per T3 port, rather than the theoretical maximum of  $8 \times 28 = 224$ .

There are 24 timeslots on a T1 interface. You can designate any combination of timeslots for usage, but you can use each timeslot number on only one channel group within the same T1 link.

To use timeslots 1 through 10, designate *slot-number* as follows:

```
[edit chassis fpc slot-number pic pic-number ct3 port port-number t1 link-number]
channel-group group-number timeslots 1-10;
```

To use timeslots 1 through 5, timeslot 10, and timeslot 24, designate *slot-number* as follows:

```
[edit chassis fpc slot-number pic pic-number ct3 port port-number t1 link-number]
channel-group group-number timeslots 1-5,10,24;
```

Note that spaces are not allowed when you specify timeslot numbers. For more information about these interfaces, see the *JUNOS Network Interfaces and Class of Service Configuration Guide*.

## Configuring Eight Queues on IQ Interfaces

---

By default, IQ PICs on T-series and M320 routing platforms are restricted to a maximum of four egress queues per interface. To configure a maximum of eight egress queues on IQ interfaces, include the `max-queues-per-interface` statement at the `[edit chassis fpc slot-number pic pic-number]` hierarchy level:

```
[edit chassis fpc slot-number pic pic-number]
max-queues-per-interface (8 | 4);
```

On a TX Matrix platform, include the `max-queues-per-interface` statement at the `[edit chassis lcc number fpc slot-number pic pic-number]` hierarchy level:

```
[edit chassis lcc number fpc slot-number pic pic-number]
max-queues-per-interface (8 | 4);
```



**NOTE:** The configuration at the `[edit class-of-service]` hierarchy level must also support eight queues per interface.

---

The maximum number of queues per IQ PIC can be 4 or 8.

If you include the `max-queues-per-interface` statement, all ports on the IQ PIC use configured mode and all interfaces on the IQ PIC have the same maximum number of queues.

When you change modes between four queues and eight queues, all physical interfaces on the PIC are deleted and re-added.

For more information about how to configure eight queues on each interface, see the *JUNOS Network Interfaces and Class of Service Configuration Guide*. For information about the TX Matrix platform, see the “TX Matrix Platform and T640 Routing Node Configuration Guidelines” on page 742.

## Configuring Channelized E1 Naming

---

Each Channelized E1 PIC has 10 E1 ports that you can channelize to the `NxDS0` level. Each E1 interface has 32 timeslots (DS0), in which timeslot 0 is reserved. You can combine one or more of these DS0 (channels) to create a channel group (`NxDS0`). There can be a maximum of 24 channel groups per E1 interface. Thus, you can configure as many as 240 channel groups per PIC (10 ports x 24 channel groups per port).

To specify the DS0 channel group number in the interface name, include a colon (:) as a separator. For example, a Channelized E1 PIC might have the following physical and virtual interfaces:

```
ds-0/0/0:x
```

where `x` is a DS0 channel group ranging from 0 through 23 (see Table 36 on page 726 for more information about ranges).

You can use any of the values within the range available for *x*; you do not have to configure the links sequentially. The software applies the interface options you configure according to the following rules:

You can configure the `e1-options` statement for channel group 0 only; for example, `ds-0/0/0:0`.

There are no restrictions on changing the default `ds0-options`.

If you delete a configuration you previously committed for channel group 0, the options return to the default values.

To configure the channel groups and timeslots for a Channelized E1 interface, include the `channel-group` and `timeslots` statements at the `[edit chassis fpc slot-number pic pic-number ce1 e1 port-number]` hierarchy level:

```
[edit chassis fpc slot-number pic pic-number ce1 e1 port-number]
  fpc slot-number {
    pic pic-number {
      ce1 {
        e1 port-number {
          channel-group group-number timeslots slot-number;
        }
      }
    }
  }
}
```



**NOTE:** If you commit the interface name but do not include the `[edit chassis]` configuration, the Channelized E1 PIC behaves like a standard E1 PIC: none of the DS0 functionality is accessible.

Table 36 shows the ranges for each of the quantities in the preceding configuration.

**Table 36: Ranges for Channelized E1 Configuration**

Item	Variable	Range
FPC slot	<i>slot-number</i>	0 through 7 (see note below)
PIC slot	<i>pic-number</i>	0 through 3
E1 port	<i>port-number</i>	0 through 9
DS0 channel group	<i>group-number</i>	0 through 23
Timeslot	<i>slot-number</i>	1 through 32



**NOTE:** The FPC slot range depends on the platform. The maximum range of 0 through 7 applies to M40 routers; for M20 routers, the range is 0 through 3; for M10 routers the range is 0 through 1; for M5 routers, the only applicable value is 0. The Channelized E1 PIC is not supported on M160 routers.

The theoretical maximum number of channel groups possible per PIC is  $10 \times 24 = 240$ . This is within the maximum bandwidth available.

There are 32 timeslots on an E1 interface. You can designate any combination of timeslots for usage.

To use timeslots 1 through 10, designate *slot-number* as follows:

```
[edit chassis fpc slot-number pic pic-number ce1 e1 port-number]
channel-group group-number timeslots 1-10;
```

To use timeslots 1 through 5, timeslot 10, and timeslot 24, designate *slot-number* as follows:

```
[edit chassis fpc slot-number pic pic-number ce1 e1 port-number]
channel-group group-number timeslots 1-5,10,24;
```

Note that spaces are not allowed when you specify timeslot numbers.

For further information about these interfaces, see the *JUNOS Network Interfaces and Class of Service Configuration Guide*.

## Configuring Channelized STM1 Interface Virtual Tributary Mapping

---

By default, virtual tributary mapping uses KLM mode. You can configure virtual tributary mapping to use KLM or ITU-T mode. On the original Channelized STM1 PIC, to configure virtual tributary mapping, include the *vtmapping* statement at the [edit chassis fpc *slot-number* pic *pic-number*] hierarchy level:

```
[edit chassis fpc slot-number pic pic-number]
vtmapping (klm | itu-t);
```

For the Channelized STM1 PIC with IQ, you can configure virtual tributary mapping by including the *vtmapping* statement at the [edit interfaces cau4 fpc *slot-number* pic *pic-number* sonet-options] hierarchy level. For more information, see the *JUNOS Network Interfaces and Class of Service Configuration Guide*.

## Configuring ATM2 Intelligent Queuing Layer 2 Circuit Transport Mode

---

On ATM2 IQ PICs only, you can configure Layer 2 circuit cell relay, Layer 2 circuit ATM Adaptation Layer 5 (AAL5), or Layer 2 circuit trunk mode.

Layer 2 circuit cell relay and Layer 2 circuit AAL5 are defined in the Internet draft draft-martini-l2circuit-encap-mpls-04.txt, *Encapsulation Methods for Transport of Layer 2 Frames Over IP and MPLS Networks*.

Layer 2 circuit trunk mode allows you to send ATM cells over Multiprotocol Label Switching (MPLS) trunking.

The four transport modes are defined as follows:

To tunnel IP packets over an ATM backbone, use the default standard AAL5 transport mode.

To tunnel a stream of AAL5-encoded ATM segmentation-and-reassembly protocol data units (SAR-PDUs) over an MPLS or IP backbone, use Layer 2 circuit AAL5 transport mode.

To tunnel a stream of ATM cells over an MPLS or IP backbone, use Layer 2 circuit cell-relay transport mode.

To transport ATM cells over an MPLS core network that is implemented on some other vendor switches, use Layer 2 circuit trunk mode.



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

When you configure AAL5 mode Layer 2 circuits, the control word carries cell loss priority (CLP) information by default.

By default, ATM2 IQ PICs are in standard AAL5 transport mode. Standard AAL5 allows multiple applications to tunnel the protocol data units of their Layer 2 protocols over an ATM virtual circuit. To configure the Layer 2 circuit transport modes, include the `atm-l2circuit-mode` statement at the `[edit chassis fpc slot-number pic pic-number]` hierarchy level:

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

On a TX Matrix platform, include the `atm-l2circuit-mode` statement at the `[edit chassis lcc number fpc slot-number pic pic-number]` hierarchy level:

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

`aal5` tunnels a stream of AAL5-encoded ATM cells over an IP backbone.

`cell` tunnels a stream of ATM cells over an IP backbone.

trunk transports ATM cells over an MPLS core network that is implemented on some other vendor switches. Trunk mode can be user-to-network interface (UNI) or network-to-network interface (NNI).



**NOTE:** To determine which vendors support Layer 2 circuit trunk mode, contact Juniper Networks customer support.

---

For more information about ATM Layer 2 circuit transport mode, see the *JUNOS Network Interfaces and Class of Service Configuration Guide* and the *JUNOS Feature Guide*. For information about the TX Matrix platform, see the “TX Matrix Platform and T640 Routing Node Configuration Guidelines” on page 742.

## Enabling ILMI for Cell Relay

---

Integrated Local Management Interface (ILMI) is supported on AAL5 interfaces, regardless of transport mode. To enable ILMI on interfaces with cell-relay encapsulation, you must configure an ATM2 IQ PIC to use Layer 2 circuit trunk transport mode.

To configure ILMI on an interface with cell-relay encapsulation, include the following statements:

```
[edit chassis fpc slot-number pic pic-number]
atm-l2circuit-mode trunk trunk;

[edit interfaces at-fpc/pic/port]
encapsulation atm-ccc-cell-relay;
atm-options {
    ilmi;
    pic-type atm2;
}
unit logical-unit-number {
    trunk-id number;
}
```

For an example on how to enable ILMI for Cell Relay, see the *JUNOS Network Interfaces and Class of Service Configuration Guide*.

## Configuring the Drop Policy for Traffic with Source-Route Constraints

---

By default, the router forwards IP traffic that has either loose or strict source-route constraints. However, you might want the router to use only the IP destination address on transit traffic for forwarding decisions. You can configure the router to discard IP traffic with source-route constraints by including the `no-source-route` statement at the `[edit chassis]` hierarchy level:

```
[edit chassis]
no-source-route;
```

## Configuring Packet Scheduling

---

By default, packet scheduling is disabled. To configure a router to operate in packet-scheduling mode, include the packet-scheduling statement at the [edit chassis] hierarchy level:

```
[edit chassis]
packet-scheduling;
```

To explicitly disable the packet-scheduling statement, include the no-packet-scheduling statement at the [edit chassis] hierarchy level:

```
[edit chassis]
no-packet-scheduling;
```

When you enable packet-scheduling mode, the Packet Director application-specific integrated circuit (ASIC) schedules packet dispatches to compensate for transport delay differences. This preserves the interpacket gaps as the packets are distributed from the Packet Director ASIC to the Packet Forwarding Engine.

Whenever you change the configuration for packet-scheduling, the system stops all SFMs and FPCs and restarts them in the new mode.



**NOTE:** Packet scheduling is for M160 routers only.

---

## Configuring the Link Services PICs

---

The Multilink Protocol enables you to split, recombine, and sequence datagrams across multiple logical data links. The goal of multilink operation is to coordinate multiple independent links between a fixed pair of systems, providing a virtual link with greater bandwidth than any of the members.

The Link Services PIC supports the following Multilink Protocol encapsulation types at the logical unit level:

- Multilink Point-to-Point Protocol (MLPPP)

- Multilink Frame Relay (MLFR FRF.15)

The Link Services PIC also supports the Multilink Frame Relay UNI and NNI (MLFR FRF.16) encapsulation type at the physical interface level.

MLFR (FRF.16) is supported on a channelized interface, *ls-fpc/pic/port:channel*, which denotes a single MLFR (FRF.16) bundle. For MLFR (FRF.16), multiple links are combined to form one logical link. Packet fragmentation and reassembly occur on a per-virtual circuit (VC) basis. Each bundle can support multiple VCs. The physical connections must be E1, T1, channelized DS3 to DS1, channelized DS3 to DS0, channelized E1, channelized STM 1, or channelized IQ interfaces.

The default number of bundles per Link Services PIC is 16, ranging from *ls-fpc/pic/port:0* to *ls-fpc/pic/port:15*.

To configure the number of bundles on a Link Services PIC, include the `mfr-uni-nni-bundles` statement at the `[edit chassis fpc slot-number pic pic-number]` hierarchy level:

```
[edit chassis fpc slot-number pic pic-number]
mfr-uni-nni-bundles number;
```

The maximum number of MLFR UNI NNI bundles each Link Services PIC can accommodate is 128. A link can associate with one link services bundle only. For more information, see the *JUNOS Network Interfaces and Class of Service Configuration Guide*.



**NOTE:** The Link Services PIC is not compatible with the M160 or T-series routing platforms.

---

## Configuring the Idle Cell Format

---

ATM devices send idle cells to enable the receiving ATM interface to recognize the start of each new cell. The receiving ATM device does not act on the contents of idle cells and does not pass them up to the ATM layer in the ATM protocol stack.

By default, the idle cell format for ATM cells is (4 bytes): 0x00000000. For ATM 2 PICs only, you can configure the format of the idle cell header and payload bytes.

To configure the idle cell header to use the International Telecommunications Union (ITU-T) standard of 0x00000001, include the `itu-t` statement at the `[edit chassis fpc slot-number pic number idle-cell-format]` hierarchy level:

```
[edit chassis fpc slot-number pic pic-number idle-cell-format]
itu-t;
```

On a TX Matrix platform, include the `itu-t` statement at the `[edit chassis lcc number fpc slot-number pic pic-number idle-cell-format]` hierarchy level:

```
[edit chassis lcc number fpc slot-number pic pic-number idle-cell-format]
itu-t;
```

By default, the payload pattern is cell payload (48 bytes). To configure the idle cell payload pattern, include the `payload-pattern` statement at the `[edit chassis fpc slot-number pic number idle-cell-format]` hierarchy level:

```
[edit chassis fpc slot-number pic pic-number idle-cell-format]
payload-pattern payload-pattern-byte;
```

On a TX Matrix platform, include the `payload-pattern` statement at the `[edit chassis lcc number fpc slot-number pic pic-number idle-cell-format]` hierarchy level:

```
[edit chassis lcc number fpc slot-number pic pic-number]
payload-pattern payload-pattern-byte;
```

The payload pattern byte can range from 0x00 through 0xff.

For information about the TX Matrix platform, see the “TX Matrix Platform and T640 Routing Node Configuration Guidelines” on page 742.

## Configuring an MTU Path Check for a Routing Instance

By default, the maximum transmission unit (MTU) check for a routing instance is not enabled.



**NOTE:** The MTU check is automatically present for interfaces belonging to the main router.

On M-series routers (except the M320 router) you can configure MTU path checks on the outgoing interface for unicast traffic routed on a virtual private network (VPN) routing and forwarding (VRF) routing instance. When you enable MTU check, the routing platform sends an Internet Control Message Protocol (ICMP) message when the size of a unicast packet traversing a VRF routing instance or virtual-router routing instance has exceeded the MTU size and when an IP packet is set to "do not fragment". The ICMP message uses the routing instance local address as its source address.

For an MTU check to work in a routing instance, you must include the `vrf-mtu-check` statement at the [edit chassis] hierarchy level and assign at least one interface containing an IP address to the routing instance.

To configure path MTU checks, do the following:

Enabling MTU Check for a Routing Instance on page 732

Assigning an IP Address to an Interface in the Routing Instance on page 732

### ***Enabling MTU Check for a Routing Instance***

To enable MTU check for a routing instance, include the `vrf-mtu-check` statement at the [edit chassis] hierarchy level:

```
[edit chassis]
vrf-mtu-check;
```

### ***Assigning an IP Address to an Interface in the Routing Instance***

To assign an IP address to an interface in the VRF or virtual-router routing instance, configure the local address for that routing instance. A local address is any IP address derived from an interface that is assigned to the routing instance.

To assign an interface to a routing instance, include the interface statement at the [edit routing-instances *instance-name*] hierarchy level:

```
[edit routing-instances instance-name]
interface interface-name;
```

To configure an IP address for a loopback interface, include the address statement at the [edit interfaces *interface-name* unit *logical-unit-number* family inet] hierarchy level:

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



**NOTE:** If you are assigning Internet Protocol Security (IPSec) or generic routing encapsulation (GRE) tunnel interfaces without IP addresses in the routing instance, include a loopback interface to the routing instance. To do this, include the *lo0.n* option at the [edit routing-instances *instance-name* interface] hierarchy level. *n* cannot be 0, because *lo0.0* is reserved for the main router (and not appropriate for use with routing instances). Also, an IP address must be assigned to this loopback interface in order to work. To set an IP address for a loopback interface, include the address statement at the [edit interfaces *lo0* unit *logical-unit-number* family inet] hierarchy level.

For more information about assigning an IP address to an interface in the VRF, see the *JUNOS VPNs Configuration Guide*.

## Configuring Redundancy

For routers that have multiple Routing Engines or multiple SFMs or SSBs, you can configure redundancy properties. A separate log file is provided for redundancy logging, located at */var/log/mastership*.

This section describes the following tasks for configuring redundancy:

Configuring Routing Engine Redundancy on page 733

Default Routing Engine Redundancy Behavior on page 739

Configuring SFM Redundancy on page 740

Configuring SSB Redundancy on page 740

Running Different JUNOS Software Releases on the Routing Engines on a TX Matrix Platform on page 741

For information about how to synchronize Routing Engines, see “Synchronizing Routing Engines” on page 241.

### Configuring Routing Engine Redundancy

For routers with two Routing Engines, you can configure which Routing Engine is the master and which is the backup. By default, the Routing Engine in slot 0 is the master (RE0) and the one in slot 1 is the backup (RE1).

To modify the default configuration, include the routing-engine statement at the [edit chassis redundancy] hierarchy level:

```
[edit chassis redundancy]
routing-engine slot-number (master | backup | disabled);
```

*slot-number* can be 0 or 1. To configure the Routing Engine to be the master, specify the master option. To configure it to be the backup, specify the backup option. To switch between the master and the backup Routing Engines, you must modify the configuration and then activate it by issuing the commit command.



**NOTE:** All master Routing Engines on a routing matrix must use the same version of JUNOS software. The software version must be release 7.0 or later. For information about the routing matrix, see “TX Matrix Platform and T640 Routing Node Configuration Guidelines” on page 742.

---

You can use either the console port or the management Ethernet (fxp0) port to establish connectivity between the two Routing Engines. You can then copy or ftp the configuration from the master to the backup, and load the file and commit it in the normal way.

To make a vty connection to the other Routing Engine using the router’s internal Ethernet network, issue the following command:

```
user@host > request routing-engine login (other-routing-engine | re0 | re1)
```

On a TX Matrix platform, to make connections to the other Routing Engines using the router’s internal Ethernet network, issue the following command:

```
user@host > request routing-engine login ( backup | lcc number | master |
other-routing-engine | re0 | re1)
```

For more information about the request routing-engine login command, see the *JUNOS Protocols, Class of Service, and System Basics Command Reference*.



**NOTE:** If your routing platform contains two Routing Engines, you can halt the primary and backup Routing Engine at the same time. To halt both Routing Engines simultaneously, issue the request system halt both-routing-engines command.

If you want to reboot a router that has two Routing Engines, reboot the backup Routing Engine (if you have upgraded it) and then the master Routing Engine.

---



**CAUTION:** Halt the primary and backup Routing Engine before you remove or shut off the power to the router; otherwise you might need to reinstall the JUNOS software.

---

You can configure Routing Engine redundancy in the following ways:

Copying a Configuration File from One Routing Engine to the Other on page 735

Loading a Package from the Other Routing Engine on page 736

Changing to the Backup Routing Engine if It Detects Loss of KeepAlive Signal on page 737

Changing to the Backup Routing Engine Without Interruption to Packet Forwarding (Graceful Switchover) on page 738

Changing to the Backup Routing Engine Without Interruption to Packet Forwarding (Graceful Switchover) on page 738

### Copying a Configuration File from One Routing Engine to the Other

To copy a configuration file from one Routing Engine to the other, you use the existing file copy command:

```
user@host > file copy source destination
```

In this case, *source* is the name of the configuration file. These files are stored in the directory `/config`. The active configuration is `/config/juniper.conf`, and older configurations are in `/config/juniper.conf {1...9}`. The *destination* is a file on the other Routing Engine.

The following is an example of copying a configuration file from Routing Engine 0 to Routing Engine 1:

```
user@host> file copy /config/juniper.conf re1:/var/tmp/copied-juniper.conf
```

The following is an example of copying a configuration file from Routing Engine 0 to Routing Engine 1 on a TX Matrix platform:

```
user@host>file copy /config/juniper.conf scc-re1:/var/tmp/copied-juniper.conf
```

To load the file into configuration mode, use the load replace configuration mode command:

```
user@host% load replace /var/tmp/copied-juniper.conf
```



**CAUTION:** Make sure you change any IP addresses specified in `fxp0` on Routing Engine 0 to addresses appropriate for Routing Engine 1.

You can use configuration groups to ensure that the correct IP addresses are used for each Routing Engine and to maintain a single configuration file for both Routing Engines.

The following example defines configuration groups re0 and re1 with separate IP addresses. These well-known configuration group names take effect only on the appropriate Routing Engine.

```

groups {
  re0 {
    system {
      host-name my-re0;
    }
    interfaces {
      fxp0 {
        description "10/100 Management interface";
        unit 0 {
          family inet {
            address 10.255.2.40/24;
          }
        }
      }
    }
  }
  re1 {
    system {
      host-name my-re1;
    }
    interfaces {
      fxp0 {
        description "10/100 Management interface";
        unit 0 {
          family inet {
            address 10.255.2.41/24;
          }
        }
      }
    }
  }
}

```

For more information about the configuration groups feature, see “Configuration Groups” on page 535.

### Loading a Package from the Other Routing Engine

You can load a package from the other Routing Engine onto the local Routing Engine using the existing request system software add *package-name* command:

```
user@host > request system software add re(0|1):/filename
```

In the re portion of the URL, specify the number of the other Routing Engine. In the *filename* portion of the URL, specify the path to the package. Packages are typically in the directory `/var/sw/pkg.`

### Changing to the Backup Routing Engine if It Detects Loss of KeepAlive Signal

Once you have configured a backup Routing Engine, you can direct it to assume mastership automatically if it detects loss of keepalive signal from the master. By default, this feature is disabled; to enable it, include the `on-loss-of-keepalives` statement at the `[edit chassis redundancy failover]` hierarchy level:

```
[edit chassis redundancy failover]
on-loss-of-keepalives;
```

By default, failover will occur after 300 seconds (5 minutes). To change the keepalive time period, include the `keepalive-time` statement at the `[edit chassis redundancy]` hierarchy level:

```
[edit chassis redundancy]
keepalive-time seconds;
```

The range for `keepalive-time` is from 2 through 10,000 seconds.

If you configure the keepalive time for 2 seconds, the sequence of events is as follows:

1. After 2 seconds of keepalive loss, a message is logged.
2. After 2 seconds of keepalive loss, the backup Routing Engine attempts to assume mastership. An alarm is generated whenever the backup is active and the display is updated with current status.
3. Once the backup Routing Engine assumes mastership, it continues to function as master even after the originally configured master Routing Engine has successfully resumed operation. You must intervene to restore its previous backup status. However, if at any time one of the Routing Engines is not present, the other one becomes master automatically, regardless of how redundancy is configured.



**NOTE:** Packet forwarding is interrupted when you enable this feature. To configure a backup Routing Engine to assume mastership automatically without any interruption to packet forwarding, see “Changing to the Backup Routing Engine Without Interruption to Packet Forwarding (Graceful Switchover)” on page 738.

---

If you are configuring a TX Matrix platform, see “Running Different JUNOS Software Releases on the Routing Engines on a TX Matrix Platform” on page 741.

### Changing to the Backup Routing Engine if It Detects a Hard Disk Error on the Master Routing Engine

Once you have configured a backup Routing Engine, you can direct it to assume mastership automatically if it detects a hard disk error from the master Routing Engine. To enable this feature, include the `on-disk-failure` statement at the `[edit chassis redundancy failover]` hierarchy level:

```
[edit chassis redundancy failover]
on-disk-failure;
```



**NOTE:** To enable this feature, you must also configure graceful switchover. For information about graceful switchover, see “Changing to the Backup Routing Engine Without Interruption to Packet Forwarding (Graceful Switchover)” on page 738.

This feature is not available on a routing matrix. For information about a routing matrix, see the “TX Matrix Platform and T640 Routing Node Configuration Guidelines” on page 742.

### Changing to the Backup Routing Engine Without Interruption to Packet Forwarding (Graceful Switchover)

For routers with two Routing Engines, you can configure graceful switchover. When you enable this feature, the backup Routing Engine automatically synchronizes its configuration and state with the master Routing Engine. Any update to the master Routing Engine state is replicated on the backup Routing Engine. When the backup Routing Engine assumes mastership, the Packet Forwarding Engine deletes its connection with the old master Routing Engine and reconnects with the new master Routing Engine. If the new master Routing Engine detects that the Packet Forwarding Engine state is not up to date, it resends state update messages.

The master Routing Engine sends periodic keepalives to the backup Routing Engine. If the backup Routing Engine does not receive a keepalive after 2 seconds (the default value) from the master Routing Engine, it assumes that the master Routing Engine has failed and assumes mastership without interruption to packet forwarding. The backup Routing Engine does not receive a keepalive signal when the master Routing Engine has failed or is removed. If this happens, the backup Routing Engine assumes mastership. When you reboot the master Routing Engine, mastership switches over to the backup Routing Engine. For more information about keepalive signals, see “Changing to the Backup Routing Engine if It Detects Loss of KeepAlive Signal” on page 737.

When you enable graceful switchover, the master Routing Engine configuration is copied and loaded to the backup Routing Engine. User files, for example, accounting and traceoptions, are not replicated to the backup Routing Engine. Local statistics, for example, rpd and lsp statistics, are not maintained.

When graceful switchover occurs, some offline field-replaceable units (FRUs) might come online. On T-series routing platforms, SIBs restart one at a time.

If you modify the configuration after you have enabled graceful switchover, you must issue the `commit synchronize` command to synchronize both Routing Engines. We recommend issuing the `commit synchronize` command on the master Routing Engine. If you issue this command on the backup Routing Engine, the JUNOS software displays a warning and commits the candidate configuration. You cannot issue the `commit` command without the `commit synchronize` option after you enabled graceful switchover. If you issue this command, the JUNOS software displays a warning. For information about the `commit synchronize` command, see “Synchronizing Routing Engines” on page 241.

A newly inserted backup Routing Engine automatically synchronizes its configuration with the master Routing Engine. When you enable graceful switchover, the command-line interface (CLI) indicates which Routing Engine you are using. For example:

```
{master} [edit]
user@host#
```



**NOTE:** You must use the same version of JUNOS software on both Routing Engines. If you are performing a software upgrade, disable graceful switchover.

To enable switchover when a software process fails, include the `other-routing-engine` option at the `[edit system processes process-name failure]` hierarchy level. For example, if you want graceful switchover to take place when the routing process fails, include the `other-routing-engine` option at the `[edit system processes routing failure]` hierarchy level.

You must enable graceful restart on all the protocols you have configured at the `[edit protocols]` hierarchy level. If you have configured a protocol that does not support graceful restart, graceful switchover might not work. For information about graceful restart, see the *JUNOS Routing Protocols Configuration Guide*.

---

By default, graceful switchover is disabled. To enable it, include the `graceful-switchover` statement and specify `enable` at the `[edit chassis redundancy]` hierarchy level:

```
[edit chassis redundancy]
graceful-switchover (disable | enable)
```

### Default Routing Engine Redundancy Behavior

By default, the JUNOS software uses re0 as the master Routing Engine and re1 as the backup Routing Engine. Unless otherwise specified in the configuration, re0 will always assume mastership if the acting-master Routing Engine is rebooted.

Take the following steps to see how the default routing engine redundancy setting works:

1. Make sure the router is running on re0 as the master Routing Engine.
2. Manually switch the state of Routing Engine mastership. re0 is now the backup Routing Engine and re1 is the master Routing Engine. For information about switching routing engine mastership, see the *JUNOS Protocols, Class of Service, and System Basics Command Reference*.



**NOTE:** On the next reboot of the master Routing Engine, the JUNOS software returns the router to the default state because you have not configured the Routing Engines to maintain this state after a reboot.

---

3. Reboot the master Routing Engine re1. When you do this, the Routing Engine boots up and reads the configuration. Because you have not specified in the configuration which Routing Engine is the master, re1 uses the default configuration as the backup. Now both re0 and re1 are in a backup state. The JUNOS software detects this conflict and, to prevent a no-master state, reverts to the default configuration to direct re0 to assume mastership.



**CAUTION:** Before you remove the Routing Engine or shut the power off to a routing platform that has two Routing Engines, you must first halt the backup Routing Engine and then the master Routing Engine. To halt the Routing Engine, issue the request system halt command.

---



**CAUTION:** Halt the primary and backup Routing Engine before you remove it or shut off the power; otherwise you might need to reinstall the JUNOS software.

---

### Configuring SFM Redundancy

For M40e Internet routers with two SFMs, you can configure which SFM is the master and which is the backup. By default, the SFM in slot 0 is the master and the one in slot 1 is the backup. To modify the default configuration, include the `sfm` statement at the [edit chassis redundancy] hierarchy level:

```
[edit chassis redundancy]
  sfm slot-number (always | preferred);
```

*slot-number* can be 0 or 1.

`always` defines the SFM as the sole device.

`preferred` defines a preferred SFM.



**NOTE:** SFM redundancy is for M40e routers only.

---

### Configuring SSB Redundancy

For M20 routers with two SSBs, you can configure which SSB is the master and which is the backup. By default, the SSB in slot 0 is the master and the one in slot 1 is the backup. To modify the default configuration, include the `ssb` statement at the [edit chassis redundancy] hierarchy level:

```
[edit chassis redundancy]
  ssb slot-number (always | preferred);
```

*slot-number* can be 0 or 1.

`always` defines the `ssb` as the sole device.

`preferred` defines a preferred `ssb`.



**NOTE:** SSB redundancy is for M20 routers only.

---

## ***Running Different JUNOS Software Releases on the Routing Engines on a TX Matrix Platform***

On a routing matrix, all master Routing Engines in the TX Matrix platform and connected T640 routing nodes must run the same JUNOS software release. Likewise, all backup Routing Engines in a routing matrix must run the same JUNOS software release. If they do not, there are consequences described below:

If the on-loss-of-keepalives statement is included at the [edit chassis redundancy failure] hierarchy level, consider the following:

If you or a host subsystem initiates a change in mastership to the backup Routing Engine in the TX Matrix platform, the master Routing Engines in the T640 routing nodes detect a software release mismatch with the new master Routing Engine in the TX Matrix platform and switch mastership to their backup Routing Engines.

If you attempt to initiate a change in mastership to a backup Routing Engine in a T640 routing node, the new master Routing Engine in the T640 routing node detects a software release mismatch with the master Routing Engine in the TX Matrix platform and relinquishes mastership to the original master Routing Engine. (Routing Engine mastership in the TX Matrix platform does not switch in this case.)

If a host subsystem initiates a change in mastership to a backup Routing Engine in a T640 routing node because the master Routing Engine has failed, the T640 routing node is logically disconnected from the TX Matrix platform. To reconnect the T640 routing node, initiate a change in mastership to the backup Routing Engine in the TX Matrix platform, or replace the failed Routing Engine in the T640 routing node and switch mastership to it (the replacement Routing Engine must be running the same software release as the master Routing Engine in the TX Matrix platform).

If the on-loss-of-keepalives statement is not included at the [edit chassis redundancy failure] hierarchy level, consider the following:

If you initiate a change in mastership to the backup Routing Engine in the TX Matrix platform, all T640 routing nodes are logically disconnected from the TX Matrix platform. To reconnect the T640 routing nodes, switch mastership of all master Routing Engines in the T640 routing nodes to their backup Routing Engines.

If you initiate a change in mastership to a backup Routing Engine in a T640 routing node, the T640 routing node is logically disconnected from the TX Matrix platform. To reconnect the T640 routing node, switch mastership of the new master Routing Engine in the T640 routing node back to the original master Routing Engine.

For more information about the on-loss-of-keepalives statement, see “Changing to the Backup Routing Engine if It Detects Loss of KeepAlive Signal” on page 737 and the *TX Matrix Platform Hardware Guide*. For information about the request chassis routing-engine master command, see the *JUNOS Protocols, Class of Service, and System Basics Command Reference*.

## TX Matrix Platform and T640 Routing Node Configuration Guidelines

---

To configure a T640 routing node that is connected to a TX Matrix platform within a routing matrix, include the following statements at the [edit chassis *lcc number*] hierarchy level:

```
[edit chassis lcc number ]
fpc slot-number {
  pic pic-number {
    atm-cell-relay-accumulation;
    atm-l2-circuit-mode (cell | aal5 | trunk trunk);
    framing (sdh | sonet);
    idle-cell-format {
      itu-t;
      payload-pattern payload-pattern-byte;
    }
    max-queues-per-interface (8 | 4);
    no-concatenate;
  }
}
offline;
online-expected;
}
```

This section includes only configuration guidelines that are unique to the TX Matrix platform and its connected T640 routing nodes. The remaining statements are explained separately in this chapter.

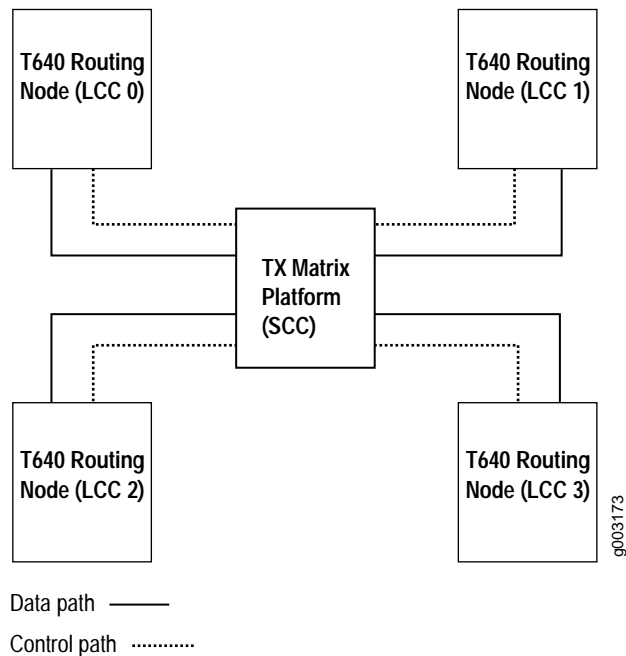
This section contains the following topics:

- Routing Matrix Overview on page 743
- Running Different JUNOS Software Releases on page 744
- Software Upgrades and Reinstallation on page 744
- Committing Configurations on page 744
- Configuring a T640 Routing Node Within a Routing Matrix on page 745
- Chassis and Interface Names on page 746
- Configuring the Online Expected Alarm on page 748
- Creating Configuration Groups on page 748
- Configuring Syslog Messages on page 748

## Routing Matrix Overview

A routing matrix is a multichassis architecture that consists of a TX Matrix platform and from one to four T640 routing nodes. From the perspective of the user interface, the routing matrix appears as a single router. The TX Matrix platform controls all the T640 routing nodes in the routing matrix, as shown in Figure 12 on page 743.

**Figure 12: Routing Matrix**



You configure and manage the TX Matrix platform and its T640 routing nodes in the routing matrix through the CLI on the TX Matrix platform. This means that the configuration file on the TX Matrix platform is used for the entire routing matrix.

Because all configuration, troubleshooting, and monitoring is performed through the TX Matrix platform, we do not recommend accessing its T640 routing nodes directly (through the console port or management Ethernet (fxp0)). If you do, the following messages appear when you first start the CLI through a T640 routing node:

```
% cli
warning: This chassis is a Line Card Chassis (LCC) in a multichassis system.
warning: Use of interactive commands should be limited to debugging.
warning: Normal CLI access is provided by the Switch Card Chassis (SCC).
warning: Use 'request routing-engine login scc' to log into the SCC.
{master}
```

These messages appear because any configuration you commit on a T640 routing node is not propagated to the TX Matrix platform or other T640 routing nodes. For details, see [Committing Configurations](#) on page 744.

## Running Different JUNOS Software Releases

On a routing matrix, if you elect to run different JUNOS software releases on the TX Matrix platform and T640 Routing Engines, a change in Routing Engine mastership can cause one or all T640 routing nodes to be logically disconnected from the TX Matrix platform. For more information, see “Running Different JUNOS Software Releases on the Routing Engines on a TX Matrix Platform” on page 741.



**NOTE:** The routing matrix supports Release 7.0 and later versions of the JUNOS software. All the master Routing Engines on the routing matrix must use the same software version. For information about hardware and software requirements, see the *TX Matrix Platform Hardware Guide*.

---

## Software Upgrades and Reinstallation

By default, when you upgrade or reinstall software on the TX Matrix platform, the new software image is distributed to the connected T640 routing nodes. Software installed on a primary TX Matrix platform is distributed to all connected primary T640 nodes and the backup is distributed to all connected backup nodes.

## Rebooting Process

When you reboot the TX Matrix platform master Routing Engine, all the master Routing Engines in the connected T640 routing nodes reboot. In addition, you can selectively reboot the master Routing Engine or any of the connected T640 routing nodes.

## Committing Configurations

In a routing matrix, all configuration must be performed on the TX Matrix platform. Any configuration you commit on a T640 routing node is not propagated to the TX Matrix platform or other T640 routing nodes. Only configuration changes you commit on the TX Matrix platform are propagated to all T640 routing nodes. A commit on a TX Matrix platform overrides any changes you commit on a T640 routing node.

If you issue the commit command, you commit the configuration to all the master Routing Engines in the routing matrix.

```
user@host# commit
scc-re0:
configuration check succeeds
lcc0-re0:
commit complete
lcc1-re0:
commit complete
scc-re0:
commit complete
```



**NOTE:** If a commit operation fails on any node, then the commit operation is not completed for the entire TX Matrix platform.

---

If you issue the `commit synchronize` command on the TX Matrix platform, you commit the configuration to all the master and backup Routing Engines in the routing matrix.

```

user@host# commit synchronize
scc-re0:
configuration check succeeds
lcc0-re1:
commit complete
lcc0-re0:
commit complete
lcc1-re1:
commit complete
lcc1-re0:
commit complete
scc-re1:
commit complete
scc-re0:
commit complete

```

### Configuring a T640 Routing Node Within a Routing Matrix

A routing matrix supports the same chassis configuration statements as a standalone routing platform (except `ce1`, `ct3`, `mlfr-uni-nni-bundles`, `sparse-dlcis`, and `vtmapping`). By including the `lcc` statement at the `[edit chassis]` hierarchy level, you configure PIC-specific features, such as framing, on specific T640 routing nodes. In addition, a routing matrix has two more chassis configuration statements, `online-expected` and `offline`.

To configure a T640 routing node that is connected to a TX Matrix platform, include the `lcc` statement at the `[edit chassis]` hierarchy level:

```

[edit chassis]
lcc number;

```

*number* can be 0 through 3.

To configure a T640 routing node within a routing matrix, include the following statements:

```

[edit chassis lcc number]
fpc slot-number { # Use the hardware FPC slot number
  pic pic-number {
    atm-cell-relay-accumulation;
    atm-l2circuit-mode (cell | aal5 | trunk trunk);
    framing (sdh | sonet);
    idle-cell-format {
      itu-t;
      payload-pattern payload-pattern-byte;
    }
    max-queues-per-interface (8 | 4);
    no-concatenate;
  }
}
offline;
online-expected;

```




---

**NOTE:** For the FPC slot number, specify the actual hardware slot number (numbered 0 through 7) as labeled on the T640 routing node chassis. Do not use the corresponding software FPC number shown in the “T640 to Routing Matrix FPC Conversion Chart” on page 747

---

For information about how to configure the online-expected and offline configuration statements, see the “Configuring the Online Expected Alarm” on page 748.

## Chassis and Interface Names

The output from some CLI commands uses the terms SCC and scc (for *switch-card chassis*) to refer to the TX Matrix platform. Similarly the terms LCC, and lcc as a prefix (for *line-card chassis*) refer to a T640 routing node in a routing matrix.

T640 routing nodes are assigned LCC index numbers, 0 through 3, depending on the hardware setup to the TX Matrix platform. A routing matrix can have up to four T640 routing nodes, and each T640 routing node has up to eight FPCs. Therefore, the routing matrix can have up to 32 FPCs (0 through 31). The FPCs are configured at the [edit chassis lcc *number*] hierarchy level.

In the JUNOS CLI, an interface name has the following format:

*type-fpc/pic/port*

When you specify the FPC number, the JUNOS software determines which T640 routing node contains the specified FPC based on the following assignment:

On LCC 0, FPC hardware slots 0 through 7 correspond to FPC software numbers 0 through 7.

On LCC 1, FPC hardware slots 0 through 7 correspond to FPC software numbers 8 through 15.

On LCC 2, FPC hardware slots 0 through 7 correspond to FPC software numbers 16 through 23.

On LCC 3, FPC hardware slots 0 through 7 correspond to FPC software numbers 24 through 31.

To convert FPC numbers in the T640 routing nodes to the correct FPC in a routing matrix, use the conversion chart shown in Table 37. You can use the converted FPC number to configure the interfaces on the TX Matrix platform in your routing matrix.

Table 37: T640 to Routing Matrix FPC Conversion Chart

FPC Numbering	T640 Routing Nodes								
	LCC 0								
T640 FPC Slots	0	1	2	3	4	5	6	7	
Routing Matrix FPC Slots Equivalent	0	1	2	3	4	5	6	7	
	LCC 1								
T640 FPC Slots	0	1	2	3	4	5	6	7	
Routing Matrix FPC Slots Equivalent	8	9	10	11	12	13	14	15	
	LCC 2								
T640 FPC Slots	0	1	2	3	4	5	6	7	
Routing Matrix FPC Slots Equivalent	16	17	18	19	20	21	22	23	
	LCC 3								
T640 FPC Slots	0	1	2	3	4	5	6	7	
Routing Matrix FPC Slots Equivalent	24	25	26	27	28	29	30	31	

Some examples include:

In a routing matrix that contains lcc 0 through lcc 2, so-20/0/1 refers to FPC slot 4 of lcc 2.

If you have a Gigabit Ethernet interface installed in FPC slot 7, PIC slot 0, port 0 of T640 routing node LCC 3, you can configure this interface on the TX Matrix platform by including the ge-31/0/0 statement at the [edit interfaces] hierarchy level.

```
[edit]
interfaces {
  ge-31/0/0 {
    unit 0 {
      family inet {
        address ip-address;
      }
    }
  }
}
```

For more information about the interface-naming conventions for a routing matrix, see the *JUNOS Network Interfaces and Class of Service Configuration Guide*. For information about CLI enhancements for the TX Matrix platform and its connected T640 routing nodes, see “Routing Matrix CLI Enhancements” on page 183.

## Configuring the Online Expected Alarm

By default, the JUNOS software allows all the T640 routing nodes in the routing matrix to come online. The JUNOS software also allows you to configure all the T640 routing nodes so that if they do not come online, an alarm is sent by the TX Matrix platform. To configure this, include the online-expected statement at the [edit chassis lcc *number*] hierarchy level:

```
[edit chassis lcc number]  
online-expected;
```

If you do not want a T640 routing node to be part of the routing matrix, you can configure it to be offline. This is useful when you are performing maintenance on a T640 routing node. When the T640 routing is ready to come back online, delete the offline configuration statement.

To configure a T640 routing so that it is offline, include the offline statement at the [edit chassis lcc *number*] hierarchy level:

```
[edit chassis lcc number]  
offline;
```



**NOTE:** If you do not configure the online-expected or offline statement, any T640 routing node that is part of the routing matrix is allowed to come online. However, if a T640 routing node does not come online, the TX Matrix platform does not generate an alarm.

---

## Creating Configuration Groups

For routers that include two Routing Engines, you can specify two special group names—re0 and re1. These two special group names apply to the Routing Engines in slots 0 and 1 of the TX Matrix platform. In addition, the routing matrix supports group names for the Routing Engines for each T640 routing node: lcc*n*-re0 and lcc*n*-re1. *n* identifies a T640 routing node from 0 through 3. For more information about configuration groups, see “Creating a Configuration Group” on page 538, and “Example: Creating and Applying Configuration Groups on a TX Matrix Platform” on page 541.

## Configuring Syslog Messages

You configure the T640 routing nodes to forward their system log messages to the TX Matrix platform at the [edit system syslog host scc-master] hierarchy level. For information about how to configure system log messages in a routing matrix, see “Configuring System Log Messages” on page 401 and “Configuring System Logging for a Routing Matrix” on page 418.