Commands: show g through show j

COMMAND DESCRIPTION

Copyright

Disclaimer

The contents of this document are subject to revision without notice due to continued progress in methodology, design and manufacturing. Ericsson shall have no liability for any error or damage of any kind resulting from the use of this document.

Trademark List

SmartEdge	is a registered trademark of Telefonaktiebolaget LM Ericsson.
NetOp	is a trademark of Telefonaktiebolaget LM Ericsson.

Contents

1 Command Descriptions

Commands starting with “show g” through commands starting “show j” are included.

This document applies to both the Ericsson SmartEdge® and SM family routers. However, the software that applies to the SM family of systems is a subset of the SmartEdge OS; some of the functionality described in this document may not apply to SM family routers.

For information specific to the SM family chassis, including line cards, refer to the SM family chassis documentation.

For specific information about the differences between the SmartEdge and SM family routers, refer to the Technical Product Description *SM Family of Systems* (part number 5/221 02-CRA 119 1170/1) in the **`Product Overview`** folder of this Customer Product Information library.

1.1 show gre

show gre [*slot/port:ch:sub*] [bvi *bvi-name* | l2vpn-cross-connect | lg *lg-name*]

1.1.1 Purpose

Displays a Generic Routing Encapsulation (GRE) tunnel or tunnel circuit information.

1.1.2 Command Mode

All modes

1.1.3 Syntax Description

slot/port:ch:sub	Specifies the slot, port, channel, and subchannel for which the command displays GRE tunnel information.
bvi *bvi-name*	Specifies the name of the bridged virtual interface (BVI) for which the command displays GRE tunnel information.
l2vp-cross-connect	Specifies the command displays GRE tunnel information only for L2VPN cross connects.
lg *lg-name*	Specifies the name of the link group for which the command displays GRE tunnel information.

1.1.4 Default

Displays information for all GRE tunnels in the current context.

1.1.5 Usage Guidelines

Use the **show gre** command to display a GRE tunnel or tunnel circuit information.

Table 1 Field Descriptions for the show gre Command

Field	Description
Name	Name of the GRE tunnel.
Context	Context in which the GRE tunnel was created.
MTU	Maximum transmission unit (MTU) of GRE tunnel.
Local IP	Local IP address of the GRE tunnel.
Remote IP	Remote IP address of the GRE tunnel.
Bound to	Interface and context to which GRE tunnel circuit is bound as entered in the **bind interface** command (in tunnel configuration mode).
State	You can see the following states: • Shut—Tunnel is disabled by shutdown command. • Up—Tunnel can send and receive traffic. • Down—Tunnel cannot send and receive traffic.

Note: If the GRE tunnel has no circuits configured, the state is always down, even after you have entered the **no shutdown** command in (GRE peer configuration mode).

Note: By default, most **show** commands (in any mode) display information for the current context only or, depending on the command syntax, for all contexts. If you are an administrator for the local context, you can insert the optional **context** ***ctx-name*** construct, preceding the **show** command, to view output for the specified context without entering that context. For more information about using the **context** ***ctx-name*** construct, see the **context** command description.

Note: By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information, see "*Modifying Output of show Commands*" in the document, *Using the CLI*.

1.1.6 Examples

The following example displays configuration information for the GRE tunnel circuit with key 1:

```
[local]Redback>show gre
Tunnel/Context        Key        Remote-IP       State      Bound to
toBoston@local        1          172.16.1.2      Down       CorpA@VPNa
```

1.2 show gre counters

`show gre counters [detail] [persistent]`

1.2.1 Purpose

Displays general counters and counters specific to Generic Routing Encapsulation (GRE) tunnel circuits for all GRE tunnel circuits in the system.

1.2.2 Command Mode

All modes

1.2.3 Syntax Description

`detail`	Optional. Specifies that more details are displayed for each tunnel circuit.
`persistent`	Optional. If omitted, displays values since the counters were last cleared. If specified, displays values since the system was last reloaded.

1.2.4 Default

None

1.2.5 Usage Guidelines

Use the **`show gre counters`** command to display general counters and counters specific to GRE tunnel circuits for all GRE tunnel circuits in the system.

Use the **`detail`** keyword to display detailed information about each tunnel circuit.

Use the **`persistent`** keyword to display values since the system was last reloaded.

Each tunnel circuit is identified by its key and the remote IP address of the tunnel for which the tunnel circuit is configured.

Note: This command is an alias for the **`show circuit counters gre`** command (in exec mode).

Note: By appending a space followed by the pipe (I) character at the end of a **`show`** command, you can filter the output using a set of modifier keywords and arguments. For more information, see the "*Modifying Output of show Commands*" in the document, *Using the CLI*.

1.2.6 Examples

The following example displays GRE counters for all tunnel circuits:

```
[local]Redback>show gre counters

Circuit                      Packets/Bytes Sent  Packets/Bytes Received

GRE to 172.16.1.2      key 1                  0                       0

                                              0                       0

GRE to 172.16.1.2      key 2                  0                       0

                                              0                       0
```

1.3 show hardware

show hardware [**alarm-card** |**backplane** | **card** *slot* | **fantray**] [**detail**]

1.3.1 Purpose

Displays information about the system hardware.

1.3.2 Command Mode

All modes

1.3.3 Syntax Description

alarm-card	Optional. Displays information about the alarm card for a SmartEdge 400 chassis. This keyword is not available for the SmartEdge 100 or SmartEdge 800 chassis.
backplane	Optional. Displays information about the backplane.
card *slot*	Optional. Chassis slot number. Displays information about the card in the specified slot only.
fantray	Optional. Displays information about the fantray or the fan and alarm unit. This keyword is not available for the SmartEdge 100 chassis.
detail	Optional. Displays detailed information.

1.3.4 Default

When used without any optional syntax, this command displays a summary of all the hardware in the system.

1.3.5 Usage Guidelines

Use the **show hardware** command to display information about the system hardware. Use the optional syntax to widen or narrow the scope of the display.

Note: By default, most **show** commands (in any mode) display information for the current context only or, depending on the command syntax, for all contexts. If you are an administrator for the local context, you can insert the optional **context** *ctx-name* construct, preceding the **show** command, to view output for the specified context without entering that context. For more information about using the **context** *ctx-name* construct, see the **context** command description.

Note: By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information, see "*Modifying Output of show Commands*" in the document, *Using the CLI*.

Table 2 describes the output fields for the **show hardware** command without the **detail** keyword.

- The EEPROM ID and version are displayed with the **detail** keyword.
- Readings for voltage sources are displayed with the **detail** keyword along with the percentage over or under the nominal value.
- See Table 5 for temperature definitions for each condition. The command displays the actual temperature reading in degrees Celsius when entered with the **detail** keyword.

Table 2 Field Descriptions for the show hardware Command without the detail keyword

Field Name	Field Data Reported and Data Descriptions
Fan Tray Status	• Present—Fan and alarm unit (SmartEdge 800 chassis) or fan tray (SmartEdge 400 chassis) is installed. • Not Present—Fan and alarm unit (SmartEdge 800 chassis) or fan tray (SmartEdge 400 chassis) is not installed or not working.
Fan(s) Status	• Failed—At least one fan is not working. • Normal—All fans are working.
SmartEdge 100 chassis: • AC Power Supply Status • DC Power Supply A Status • DC Power Supply B Status	SmartEdge 100 chassis: • No Power—Power has failed, is disconnected, or is not installed. • Normal—Power is being supplied by this power supply.

Table 2 Field Descriptions for the show hardware Command without the detail keyword

Field Name	Field Data Reported and Data Descriptions
SmartEdge 400 chassis: • Power Supply A Status • Power Supply B Status	SmartEdge 400 with AC Power Supply: • AC Unit No Power—The AC power supply is not installed or is not fully inserted. • AC Unit High Temp—High temperature has been detected at the AC source. • AC Unit Failure—AC power source has failed. • AC Unit Normal—Power is being supplied by the AC source. SmartEdge 400 with DC Power Supply: • DC Unit Normal—Power is being supplied by the DC source. • No Power—DC Power has failed, is disconnected, or is not installed.
SmartEdge 600 chassis: • Power Supply A Status • Power Supply B Status	SmartEdge 600 with AC Power Supply: • AC Unit No Power—The AC power supply is not installed or is not fully inserted. • AC Unit High Temp—High temperature has been detected at the AC source. • AC Unit Failure—AC power source has failed. • AC Unit Normal—Power is being supplied by the AC source. SmartEdge 400 with DC Power Supply: • DC Unit Normal—Power is being supplied by the DC source. • No Power—DC Power has failed, is disconnected, or is not installed.
SmartEdge 800 chassis: • Power Supply A Status • Power Supply B Status	SmartEdge 800 chassis: • No Power—Power has failed, is disconnected, or is not installed. • Normal—Power is being supplied by this power supply.
SmartEdge 1200 chassis: • Power Supply A1 Status • Power Supply A2 Status • Power Supply B1 Status • Power Supply B2 Status	SmartEdge 1200 chassis: • No Power—Power has failed, is disconnected, or is not installed. • Normal—Power is being supplied by this power supply.

Table 2 Field Descriptions for the show hardware Command without the detail keyword

Field Name	Field Data Reported and Data Descriptions
SmartEdge 1200H chassis: • Power Supply A1 Status • Power Supply A2 Status • Power Supply B1 Status • Power Supply B2 Status	SmartEdge 1200H chassis: • No Power—Power has failed, is disconnected, or is not installed. • Normal—Power is being supplied by this power supply.
Active Alarms	Alarm conditions for this unit: • NONE—No alarm conditions exist. • ***condition***—Alarm condition is in effect. For a complete list of conditions that can cause an alarm, see *Alarms and Probable Causes*.
Slot	• ***slot***—Slot number for this unit. • N/A—No slot number for this unit.
Type	Unit: • alarm card—Alarm card (SmartEdge 400 chassis only) is installed. • backplane—Backplane. • carrier—I/O carrier card (SmartEdge 100 chassis only). • ***controller-card-type***—Controller card is installed (XCRP type). • fan tray—Fan and alarm unit (SmartEdge 800 chassis) or fan tray (SmartEdge 400 and SmartEdge 1200 chassis) is installed. • ***traffic-card-type***—Traffic card is installed; see Table 13. • ***MIC-type***—MIC is installed; for a list of MIC types, see Table 13Table 12. • sse—SmartEdge Storage Engine is installed. • unknown—Controller card is inserted but not initialized.
Mfg Date	***dd/mm/yyyy***—Date unit was manufactured.

Table 2 Field Descriptions for the show hardware Command without the detail keyword

Field Name	Field Data Reported and Data Descriptions
Voltage	• N/A—Voltage is not applicable for this unit. • NOT OK—Voltage for this card is outside its operating range. • OK—Voltage for this card is within its operating range.
Temperature	Temperature condition and actual temperature reading in degrees Celsius: • Cold—Temperature is colder than normal. • Normal—Temperature is within normal operating range for this unit. • Hot—Temperature is hotter than normal. • Extreme—Temperature is much hotter than normal. • N/A—Temperature does not apply to this unit. Table 4 lists descriptions of each temperature condition. Table 5 lists temperature ranges for card types.

Table 3 describes the output fields for the **`show hardware`** command with the **`detail`** keyword.

Table 3 Field Descriptions for the show hardware Command with the detail Keyword

Field Name	Field Data Reported and Data Descriptions
Active Alarms(1)	Alarm conditions for this unit: • NONE—No alarm conditions exist. • *`condition`*—Alarm condition is in effect. For a complete list of conditions that can cause an alarm, see *Alarms and Probable Causes*.
Air filter date	*`yyyy-mm`*—Date the air filter is due to be replaced (SmartEdge 400 and SmartEdge 800 chassis).
Alarm Card Status	• Present—Alarm card is installed and working (SmartEdge 400 chassis only). • Not Present—Alarm card is not installed (SmartEdge 400 chassis only).

Table 3 Field Descriptions for the show hardware Command with the detail Keyword

Field Name	**Field Data Reported and Data Descriptions**
Card Status	For traffic cards only: • FPGA mismatch—Card needs an FPGA upgrade. • FPGA upgrade—FPGA upgrade has been started. • HW detected—Card is detected and being initialized. • HW failure—Card has experienced a failure. • HW initialized—Card is initialized and ready.
Chass Entitlement	Type of chassis for which this card is intended: • All—Card is entitled in every chassis. • List of chassis, separated by slashes (/)—Listed chassis only.
Chassis Type	Type of chassis in which the backplane is installed: • SE100—SmartEdge 100 chassis. • SE400—SmartEdge 400 chassis. • SE800—SmartEdge 800 chassis. • SE1200—SmartEdge 1200 chassis.
Connector Type	MIC port connector: • Copper—RJ-45 connector. • Optical—SFP optical transceiver (LC) connector.
CPLD Version	*n*—Version of the complex programmable logic device (CPLD) on the MIC.
DimFpga rev DimFpga file rev	Dim FPGA revision and file revision; N/A or not displayed if not applicable for this card.
Disk	SSE disk number; 1 or 2.
EEPROM id/ver	*nnnn/n*—Version of the unit EEPROM.
EPPA memory	*nnn* MB—Size of ingress and egress PPA memory.
Ericsson Approved	State of transceiver testing for this SFP optical transceiver in SmartEdge router: • No—Not tested. • Yes—Tested.

Table 3 Field Descriptions for the show hardware Command with the detail Keyword

Field Name	Field Data Reported and Data Descriptions
Fan Tray Status	• Present—Fan and alarm unit (SmartEdge 800 chassis) or fan tray (SmartEdge 400, SmartEdge 600, SmartEdge 1200, or SmartEdge 1200H chassis) is installed. • Not Present—Fan and alarm unit (SmartEdge 800 chassis) or fan tray (SmartEdge 400, SmartEdge 600, SmartEdge 1200, or SmartEdge 1200H chassis) is not installed or not working.
Fan(s) Status	• Failed—At least one fan is not working. • Normal—All fans are working.
FlipFpga rev	FLIP FPGA revision and file revision; N/A or not displayed if not applicable for this traffic card.
ForteFpga rev	Forte FPGA revision and file revision; applicable to XCRP only. This FPGA controls power on/reset for all devices.
Hardware Rev	*n*—Hardware revision level for this unit; single digit.
HubFpga rev HubFpga file rev	Hub FPGA revision and file revision; N/A or not displayed if not applicable for this card.
IPPA memory	*nnn* MB—Size of ingress and egress PPA memory.
ITU ch	International Telecommunications Union (ITU) channel number (corresponds to the wavelength displayed in the Wavelength field); not displayed if not applicable for the transceiver installed in this port.
LEDs	State of Fail, Active, Standby, and Sync LEDs: • Blink—ODD test is in progress. • On—LED is lit. • Off—LED is not lit. Sync LED is for controller cards only.
LimFpga rev	LIM FPGA revision and file revision; N/A or not displayed if not applicable for this traffic card.
MAC Address	*nn:nn:nn:nn:nn:nn*—Medium access control (MAC) address of the system (stored in the EEPROM); displayed using the backplane keyword only.
MaxFpga rev	Max FPGA revision and file revision; applicable to XCRP controller card only. This FPGA controls access to the CPU bus.
Memory	Memory for which this controller card is entitled: • Max—All memory on the controller card is enabled. • *nnnn* MB—Size in MB of enabled memory.

Table 3 Field Descriptions for the show hardware Command with the detail Keyword

Field Name	**Field Data Reported and Data Descriptions**
Mfg Date	*`dd/mm/yyyy`*—Date this unit was manufactured.
MIC *`n`*	For each MIC slot *`n:`* • *`MIC-type`*—For a list of MIC types, see Table 12. • Not Present—MIC is not installed.
MinnowCPLD Ver	Minnow CPLD revision; applicable to the SmartEdge 100 chassis slot 1 only.
Model	SSE disk model; vendor in parentheses.
ODD Status	Status of the on-demand diagnostics (ODD) tests: • Aborted—The session was terminated by the user or, for controller cards only, by the standby controller card being removed. • Incomplete—At least one of the requested tests could not be run. • In-progress—Session is currently in progress. • Not available—No session of the ODD has been run for this unit. • Passed—All tests have passed. • *`n`* Failure(s)—One or more tests have failed.
OpusFpga rev	Opus FPGA revision and file revision; applicable to XCRP only. This FPGA manages peripherals such as the front panel LEDs and the CRAFT ports.
POD Status	Status of the power-on diagnostics (POD) tests: • Success—Unit passed all POD tests. • Failure—Unit failed one or more POD tests.
Port	*`n`*—Port number if hardware data is port specific; not displayed if not applicable for this card.
Ports Configurable	Number of ports on this line card that have been specified as software configurable (ATM DS-3 line card only).
Ports Entitled	List of ports that are entitled on this traffic card or MIC: • *`n1, n2, n3,...`*—Entitled ports. • All—All physical ports on the traffic card are entitled.

Table 3 Field Descriptions for the show hardware Command with the detail Keyword

Field Name	Field Data Reported and Data Descriptions
SmartEdge 100 chassis: • AC Power Supply Status • DC Power Supply A Status • DC Power Supply B Status	SmartEdge 100 chassis: • No Power—Power has failed, is disconnected, or is not installed. • Normal—Power is being supplied by this power supply.
SmartEdge 400 chassis: • Power Supply A Status • Power Supply B Status	SmartEdge 400 with AC Power Supply: • AC Unit No Power—The AC power supply is not installed or is not fully inserted. • AC Unit High Temp—High temperature has been detected at the AC source. • AC Unit Failure—AC power source has failed. • AC Unit Normal—Power is being supplied by the AC source. SmartEdge 400 with DC Power Supply: • DC Unit Normal—Power is being supplied by the DC source. • No Power—DC Power has failed, is disconnected, or is not installed.
SmartEdge 800 chassis: • Power Supply A Status • Power Supply B Status	SmartEdge 800 chassis: • No Power—Power has failed, is disconnected, or is not installed. • Normal—Power is being supplied by this power supply.
SmartEdge 1200 chassis: • Power Supply A1 Status • Power Supply A2 Status • Power Supply B1 Status • Power Supply B2 Status	SmartEdge 1200 chassis: • No Power—Power has failed, is disconnected, or is not installed. • Normal—Power is being supplied by this power supply.
RxPwrMin[dbm][(2)] RxPwrMax[dbm]	*-nn.nn*—Receiver sensitivity (minimum) and overload level (maximum) for the version of the SFP transceiver installed in this port.
S3Fpga rev	S3 FPGA revision and file revision; applicable to XCRP only. This FPGA manages the control and phase alignment of the Stratum-3 PLL.

Table 3 Field Descriptions for the show hardware Command with the detail Keyword

Field Name	Field Data Reported and Data Descriptions
SAR Image Type	ATM mode currently loaded; applicable to second-generation ATM OC traffic cards only:[3] • atm priority—ATM priority mode. • ip-priority—IP priority mode. • vc-fair—Virtual circuit (VC) fairness mode. • hsvc-fair—Hierarchical shaping virtual circuit (HSVC) fairness mode.
SAR Image Version	*n.n.n.n*—Version of the image.
SARC memory	*nnn* MB—Size of segmentation and reassembly controller (SARC) memory; applicable to ATM traffic cards only.
SARC status	Status of the segmentation and reassembly controller (SARC): • OK—SARC is ready. • Not Ready—SARC is not ready. • Unknown—Unable to read SARC status.
SCC id	ID for the system communication controller (SCC) ASIC on a controller card; the SCC controls and communicates with the traffic cards.
Serial No	*nnnnnnnnnnnnnn*—Unique identifier for this unit; 14 alphanumeric characters.
N/A	Temperature does not apply to this unit, or this unit does not have a built-in temperature sensor.

Table 3 Field Descriptions for the show hardware Command with the detail Keyword

Field Name	Field Data Reported and Data Descriptions
SFP / Media type	SFP Transceivers—Ethernet line cards: • FX / MM—Short reach transceiver, multimode fiber. • LX10 / SM—Long reach transceiver, single-mode fiber. • SX / MM—Short reach transceiver, multimode fiber. • LX / SM—Long reach transceiver, single-mode fiber. • ZX / SM—Extended long reach transceiver, single-mode fiber. • BX / SM—Bidirectional transceiver, single-mode fiber. • T / Cat5—Copper-based transceiver. • CWDM / SM—Coarse wavelength-division multiplexing (CWDM) transceiver, single-mode fiber. • DWDM / SM—Dense wavelength-division multiplexing (DWDM) transceiver, single-mode fiber.
	SFP transceivers—SONET/SDH OC-n (OC-48c/STM-16c, OC-12c/STM-4c, and OC-3c/STM-1c) cards: • SR / MM—Short reach transceiver, multimode fiber. • SR / SM—Short reach transceiver, single-mode fiber. • IR / SM—Intermediate reach transceiver, single-mode fiber. • LR / SM—Long reach transceiver, single-mode fiber.
SFP Serial No	nnnnnnnnnn—Unique identifier for this transceiver; 10 alphanumeric characters.
Slot	• *slot*—Slot number for this unit. • N/A—No slot number for this unit.
SlipFpga file rev	SLIP FPGA revision; applicable to the SmartEdge 100 I/O carrier card functions only (slot 1).
Spec Capacity	SSE disk hardware specification capacity.
SpiFpga file rev	System Packet Interface File revision.
SpiFpga rev	System Packet Interface Fpga.
Start/Stop count	Number of times the SSE disk has been started/stopped; maximum number of starts/stops in disk lifetime in parentheses.
SXC id	ID of the SONET cross-connect (SXC) ASIC on a controller card; the SXC cross-connects traffic between some traffic cards.

Table 3 Field Descriptions for the show hardware Command with the detail Keyword

Field Name	Field Data Reported and Data Descriptions
SysFpga rev	System FPGA revision and file revision; N/A or not displayed if not applicable for this traffic card.
Temperature	Temperature condition and actual temperature reading in degrees Celsius: • Cold—Temperature is colder than normal. • Normal—Temperature is within normal operating range for this unit. • Hot—Temperature is hotter than normal. • Extreme—Temperature is much hotter than normal. • N/A—Temperature does not apply to this unit. Table 4 lists descriptions of each temperature condition. Table 5 lists temperature ranges for card types.
TxPwrMin[dbm][2] TxPwrMax[dbm]	*-nn.nn*—Transmitter optical output power (minimum and maximum) for the version of the SFP transceiver installed in this port.
Type	Unit: • alarm card—Alarm card (SmartEdge 400 chassis only) is installed. • backplane—Backplane. • carrier—I/O carrier card (SmartEdge 100 chassis only). • ***controller-card-type***—Controller card is installed; see Table 12 for the SmartEdge 100 chassis and Table 13 for all other SmartEdge chassis. • fan tray—Fan and alarm unit (SmartEdge 800 chassis) or fan tray (SmartEdge 400 and SmartEdge 1200 chassis) is installed. • ***traffic-card-type***—Traffic card is installed; see Table 13. • ***MIC-type***—MIC is installed; see Table 12.
Voltage	Readings for voltage sources 1.5V, 1.8V, 2.6V, 3.3V, 5V, and 12V along with the percentage over or under the nominal value.

Table 3 Field Descriptions for the show hardware Command with the detail Keyword

Field Name	Field Data Reported and Data Descriptions
Wavelength[2]	Center wavelength for the version of the SFP optical transceiver installed in this port: • 0.00 [nm]—Wavelength is not reported by this transceiver. • *nnnn.nn* [nm]—Wavelength for this transceiver version. See *Transceivers for SmartEdge and SM Family Line Cards* for wavelength data for each type of transceiver and its versions.
XFP / Media type	10-Gbps SFP (XFP) transceivers—10-GE and SONET/SDH OC-192 line cards: • SR / SM—Short reach transceiver, single-mode fiber. • SW / SM—Short reach transceiver, single-mode fiber. • SR / MM—Short reach transceiver, multimode fiber. • IR / SM—Intermediate reach transceiver, single-mode fiber. • LR / SM—Long reach transceiver, single-mode fiber. • LW / SM—Long reach transceiver, single-mode fiber. • ER / SM—Extended long reach transceiver, single-mode fiber. • EW / SM—Extended long reach transceiver, single-mode fiber. • ZR / SM—Extreme reach transceiver, single-mode fiber.[4] • ZW / SM—Extreme reach transceiver, single-mode fiber.[5] • DWDM / SM—Dense wavelength-division multiplexing (DWDM) transceiver, single-mode fiber.[6][7] • 10000Base-DWDM—OTN Dense wavelength-division multiplexing (DWDM) transceiver, single-mode fiber.[8]

(1) Alarm severities conform to the definitions provided in Generic Requirements, GR-474-CORE, Issue 1, December 1997, Network Maintenance: Alarm and Control for Network Elements.

(2) Measured or reported values meet or exceed the transceiver specifications that are documented in Transceivers for SmartEdge and SM Family Cards.

(3) The 8-port ATM OC-3c/STM-1c (atm-oc3e-8-port) and 2-port ATM OC-12c/STM-4c cards support only the “vc-fair" and "hsvc-fair" atm modes.

(4) Use part number XFP-OC192-LR2 when ordering the XFP transceivers with 10GE ZR functionality.

(5) Use part number XFP-OC192-LR2 when ordering the XFP transceivers with 10GE ZR functionality.

(6) In Releases 6.1.4 and 6.1.5, 10GE DWDM XFP transceivers support only ITU channels 35,36,37,53,and 54.

(7) In Release 6.4.1, 10GE OTN XFP transceivers support only ITU channels 35,36,37,53,and 54.

(8) In Releases 6.4.1, 10GE OTN DWDM XFP transceivers support only ITU channels 35,36,37,53,and 54.

Note: Alarm severities conform to the definitions provided in Generic Requirements, GR-474-CORE, Issue 1, December 1997, `Network Maintenance:  Alarm and Control for Network Elements`.

See the *Card Types* section in the *Configuring Cards* document for complete list of slot cards that the system supports and their CLI names.

Table 5 lists the definitions of the temperature range for each condition. The actual temperature reading in degrees Celsius displays with the detail keyword.

The temperature ranges listed in Table 5 can vary slightly, depending on the version of the controller or traffic card.

Table 4 Descriptions of Temperature Conditions

Condition	Description
COLD	Expected when the system first powers up in a cool or well air-conditioned environment.
NORMAL	Normal operating temperature.
HOT	The card is running above normal operating temperature. The lifespan of the card will likely be reduced if this condition persists. The ambient temperature of the room could be too hot, or the chassis air filter or fans might need cleaning or replacing. When the card temperature is greater than TEMP_HOT for longer than 5 minutes, the system generates a minor alarm; if the condition persists longer than 1 hour, it generates a major alarm.
EXTREME	The card is running well above normal operating temperature. The lifespan of the card will be reduced if this condition persists. The ambient temperature of the room is likely too hot, or the chassis air filter or fans might need cleaning or replacing. When the card temperature reaches TEMP_EXTREME, the system generates a major alarm.
N/A	Temperature does not apply to this unit, or this unit does not have a built-in temperature sensor.

Table 5 Temperature Ranges for Card Types

Card Type	Temperature Ranges

atm-oc3e-8-port
atm-oc12e-2-port
oc3e-8-port
oc12e-4-port
oc48e-4-port
	COLD ≤ 20°C
	NORMAL = 21 - 71°C
	HOT = 72 - 93°C
	EXTREME ≥ 94°C

Table 5 Temperature Ranges for Card Types

Card Type	Temperature Ranges

oc192-1-port
ge-10-port
ge-20-port[1]
ge-5-port
ge2-10-port
10ge-1-port
10ge-oc192-1-port
	COLD ≤ 20°C
	NORMAL = 21 - 84°C
	HOT = 85 - 94°C
	EXTREME ≥ 95°C

fege-60-2-port	COLD ≤ 20°C
	NORMAL = 21 - 89°C
	HOT = 90 - 103°C
	EXTREME ≥ 104°C

ch-oc3oc12-8or2-port[2]	COLD ≤ 20°C
	NORMAL = 21 - 89°C
	HOT = 90 - 105°C
	EXTREME ≥ 105°C

ge4-20-port[3][1]
10ge-4-port
	COLD ≤ 20°C
	NORMAL = 21 - 85°C
	HOT = 86 - 103°C
	EXTREME ≥ 104°C

ase	COLD ≤ 20°C
	NORMAL = 21 - 70°C
	HOT = 71- 76°C
	EXTREME ≥ 77°C

ase2[3]	COLD ≤ 20°C
	NORMAL = 21 - 75°C
	HOT = 76 - 85°C
	EXTREME ≥ 86°C

Table 5   Temperature Ranges for Card Types

Card Type	Temperature Ranges

sse[3]	COLD ≤ 20°C
	NORMAL = 21 - 75°C
	HOT = 76- 80°C
	EXTREME ≥ 81°C

xc4	COLD ≤ 20°C
	NORMAL = 21 - 90°C
	HOT = 91- 100°C
	EXTREME ≥ 100°C

(1) Because the TX SFP is larger than a standard SFP, you cannot insert two TX SFPs side by side on the 20-port GE1020 and 20-port GE line cards.
(2) To use ports 5 through 8 on a Channelized 8-port OC-3/STM-1 or 2–port OC-12/STM-4 line card (ROA1283420/1), an all-ports software license (FAL1241079/1) is needed. A separate software license (FAL1240782/1) is required for the Channelized 4-port OC-3/STM-1 or 1-port OC-12/STM-4 line card (ROA1283420/2).
(3) This card is not supported in the SmartEdge 400 and SmartEdge 800 chassis.

1.3.6 Examples

The following example displays output from the show hardware command for a SmartEdge 800 chassis:

```
[local]Redback>show hardware

Fan Tray Status            Present
Fan(s) Status              Normal
Power Supply A Status      Normal
Power Supply B Status      No Power
Active Alarms              NONE

Slot Type                 Serial No      Rev Ver Mfg Date    Voltage  Temp
---- -------------------- -------------- --- --- ----------- -------- -------
N/A  backplane            9C2B4090100100   2   2 13-OCT-2001 N/A      N/A
N/A  fan tray             9D034090100100   3   2 13-OCT-2001 N/A      N/A
1    oc3e-8-port          8J0O8040200063  15   4 30-APR-2004 Ok       Normal
3    atm-oc3e-8-port      7Q0E5060200025   5   4 01-JUL-2004 Ok       Normal
4    atm-oc3-2-port       8F0P8070210270  16   4 07-AUG-2004 Ok       Normal
5    ge-10-port           7UAA8070200197  27   4 30-JUL-2005 Ok       Normal
7    xcrp4                6Y0O5060300038  15   4 09-APR-2003 N/A      Normal
8    xcrp4                6Y0O5060300064  15   4 02-APR-2005 N/A      Normal
10   ge-5-port            8I018050200080   1   4 31-MAY-2008 Ok       Normal
11   oc12e-4-port         7P0F8050200058   6   4 29-MAY-2006 Ok       Normal
14   gigaether-4-port     8K0X8050200139  24   4 16-MAY-2005 Ok       Normal
```

The following example displays detailed output for the SFP/media type on a traffic card for the SmartEdge 800 chassis:

```
[local]Redback#show hardware card 10 detail

Slot                : 10                Type              : ge-20-port
Serial No           : B10D5050500014    Hardware Rev      : 4
EEPROM id/ver       : 0x5a/4            Mfg Date          : 21-MAY-2005
HubFpga rev         : 0x3b              HubFpga file rev  : 0x3b
SpiFpga rev         : 0x6               SpiFpga file rev  : 0x6
IPPA memory         : 1024 MB           EPPA memory       : 1024 MB
Voltage 1.5V        : 1.523 (+2%)       Voltage 1.8V      : 1.813 (+1%)
Voltage 2.6V        : 2.480 (-1%)       Voltage 3.3V      : 3.304 (+0%)
Temperature         : NORMAL (52 C)     SFP
Card Status         : HW initialized    POD Status        : Success
ODD Status          : Not Available
Fail LED            : Off               Active LED        : On
Standby LED         : N/A
Chass Entitlement   : SE400/SE800
Ports Entitled      : All
Active Alarms       : NONE
Port                : 1                 SFP / Media Type  : CWDM / MM
RedbackApproved     : Y                 Wavelength        : 1591.00[nm]
CLEI code           :                   RxPwrMin/Max[dbm] :   1995 / -    39
ITU ch              : 7
TxPwrMin/Max[dbm]   :  31622 / - 10000
```

The following example displays detailed output for the alarm card in a SmartEdge 400 chassis:

```
[local]Redback>show hardware alarm-card detail

Slot                : N/A               Type              : alarm card
Serial No           : 0D0B5060300017    Hardware Rev      : 2
EEPROM id/ver       : 0x5a/4            Mfg Date          : 21-jun-2003
Air filter date     : 2005-10
ODD Status          : N/A
Temperature         : NORMAL (24 C)
```

The following example displays detailed output for a controller card in a SmartEdge 800 chassis:

```
[local]Redback>show hardware card 7 detail

Slot                : 7                 Type              : xcrp - T1 BITS
Serial No           : 8S018040200129    Hardware Rev      : 1
EEPROM id/ver       : 0x5a/2            Mfg Date          : 09-APR-2002
OpusFpga Ver        : 0x7               S3Fpga Ver        : 0x7
MaxFpga Ver         : 0x3               ForteFpga Ver     : 0x6
SCC id              : 0x0               SXC id            : 0x1f
Temperature         : Normal (38 C)     POD Status        : Success
ODD Status          : N/A
Fail LED            : Off               Active LED        : On
Standby LED         : Off               Sync LED          : Off
Chass Entitlement   : SE400/SE800       Memory            : Max
Active Alarms       : NONE
```

The following example displays detailed output for the fan tray in a SmartEdge 400 chassis:

```
[local]Redback>show hardware fantray detail

Slot                : N/A               Type              : fan tray
Serial No           : 0D0A5040300002    Hardware Rev      : 1
EEPROM id/ver       : 0x5a/4            Mfg Date          : 01-MAY-2003
Air filter date     : 2005-10
ODD Status          : N/A
```

The following example shows detailed output for an ATM OC-3e 8-port card in a SmartEdge 800 chassis. Only the first of the eight ports of the card are shown in this example:

```
[local]Redback>show hardware card 3 detail

Slot              : 3               Type              : atm-oc3e-8-port
Serial No         : 9X60D260721655  Hardware Rev      : 60
EEPROM id/ver     : 0x5a/4          Mfg Date          : 29-JUN-2007
SysFpga rev       : 0x7             SysFpga file rev  : N/A
LimFpga rev       : 0x6             LimFpga file rev  : 0x6
IPPA memory       : 512 MB           EPPA memory       : 512 MB
SARC memory       : 16 MB
Voltage 1.5V      : 1.509 (+1%)     Voltage 1.8V      : 1.802 (+0%)
Voltage 2.6V      : 2.612 (-0%)     Voltage 3.3V      : 3.413 (+0%)
Temperature       : NORMAL (32 C)
Card Status       : HW initialized  POD Status        : Success
ODD Status        : Not Available
Fail LED          : Off             Active LED        : On
Standby LED       : Off
Chass Entitlement : All (0x0)
Ports Entitled    : All
SAR Image Type    : vc-fair
SAR Image Version : 1.7.144.4.0
Clock Source      : local
Active Alarms     : NONE

Port              : 1               SFP / Media Type  : OC-3 / IR-1
CLEI code         : VAUIAAWEAA      RedbackApproved   : Yes
SFP Serial No     : P882GL2
Wavelength        : 850.00[nm]
TxPwrMin[dbm]     : -9.50           TxPwrMax[dbm]     : 0.00
RxPwrMin[dbm]     : -17.01          RxPwrMax[dbm]     : 0.00
```

The following example shows detailed output for a GE4 20-port card in a SmartEdge 800 or SmartEdge 1200 chassis:

```
[local]Redback>show hardware card 2 detail

Slot                : 2                Type                : ge4-20-port
Serial No           : F10R5230800040   Hardware Rev        : 00R
EEPROM id/ver       : 0x5a/4           Mfg Date            : 22-JUN-2008
HubFpga rev         : 0x5              HubFpga file rev    : 0x5
SpiFpga rev         : 0x0              SpiFpga file rev    : N/A
IPPA memory         : N/A              EPPA memory         : N/A
Voltage 1.200V      : 1.201 (+0%)      Voltage 1.200V      : 1.206 (+1%)
Voltage 1.200V      : 1.201 (+0%)      Voltage 1.250V      : 1.245 (-0%)
Temperature         : NORMAL (53 C)
Card Status         : HW initialized   POD Status          : Success
ODD Status          : Not Available
Fail LED            : Off              Active LED          : On
Standby LED         : Invalid
Chass Entitlement   : All (0x0)
Ports Entitled      : All
Active Alarms       : NONE

Port                : 1                SFP / Media Type    : FX / MM
CLEI code           :                  RedbackApproved     : Yes
SFP Serial No       : 3577343
Wavelength          : 1310.00[nm]
TxPwrMin[dbm]       : -19.03           TxPwrMax[dbm]       : -14.00
RxPwrMin[dbm]       : -32.22           RxPwrMax[dbm]       : -14.00

Port                : 2                SFP / Media Type    : SX / MM
CLEI code           : VAUIAAWEAA       RedbackApproved     : Yes
SFP Serial No       : PCN2YTE
Wavelength          : 850.00[nm] TxPwrMin[dbm]       : -11.74           TxPwrMax[dbm]  : -2.00
RxPwrMin[dbm]       : -20.00           RxPwrMax[dbm]       : 1.00

Port                : 3                SFP / Media Type    : SX / MM
CLEI code           : VAUIAAWEAA       RedbackApproved     : Yes
SFP Serial No       : PCN2ZK4
```

```
Wavelength          : 850.00[nm]
TxPwrMin[dbm]       : -11.74            TxPwrMax[dbm]       : -2.00
RxPwrMin[dbm]       : -20.00            RxPwrMax[dbm]       : 1.00
Port                : 4                 SFP / Media Type    : SX / MM

CLEI code           : VAUIAAWEAA        RedbackApproved     : Yes
SFP Serial No       : PCN2YUZ
Wavelength          : 850.00[nm]
TxPwrMin[dbm]       : -11.74            TxPwrMax[dbm]       : -2.00
RxPwrMin[dbm]       : -20.00            RxPwrMax[dbm]       : 1.00

Port                : 5                 SFP / Media Type    : SX / MM
CLEI code           : VAUIAAWEAA        RedbackApproved     : Yes
SFP Serial No       : PDC22ZG
Wavelength          : 850.00[nm]
TxPwrMin[dbm]       : -11.74            TxPwrMax[dbm]       : -2.00
RxPwrMin[dbm]       : -20.00            RxPwrMax[dbm]       : 1.00
Port                : 6                 SFP / Media Type    : SX / MM
CLEI code           : VAUIAAWEAA        RedbackApproved     : Yes
SFP Serial No       : F721470200E5
Wavelength          : 850.00[nm]
TxPwrMin[dbm]       : -9.50             TxPwrMax[dbm]       : -1.00
RxPwrMin[dbm]       : -13.01            RxPwrMax[dbm]       : 0.00

Port                : 8                 SFP / Media Type    : LX / SM
CLEI code           : VAUIAAXEAA        RedbackApproved     : Yes
SFP Serial No       : 74VT200402
Wavelength          : 1310.00[nm]
TxPwrMin[dbm]       : -6.31             TxPwrMax[dbm]       : 3.69
RxPwrMin[dbm]       : -17.26            RxPwrMax[dbm]       : 5.74

Port                : 9                 SFP / Media Type    : LX / SM
CLEI code           :                   RedbackApproved     : Yes
SFP Serial No       : 4755100006
Wavelength          : 1310.00[nm]
TxPwrMin[dbm]       : -7.05             TxPwrMax[dbm]       : 2.95
RxPwrMin[dbm]       : -13.60            RxPwrMax[dbm]       : 7.58

Port                : 10                SFP / Media Type    : LX / SM
CLEI code           : VAUIAAXEAA        RedbackApproved     : Yes
SFP Serial No       : P7D28AA
Wavelength          : 1310.00[nm]
TxPwrMin[dbm]       : -9.65             TxPwrMax[dbm]       : 4.64
RxPwrMin[dbm]       : -17.93            RxPwrMax[dbm]       : 6.95

Port                : 11                SFP / Media Type    : LX / SM
CLEI code           : VAUIAAXEAA        RedbackApproved     : Yes
SFP Serial No       : 74VT200388
Wavelength          : 1310.00[nm]
TxPwrMin[dbm]       : -6.00             TxPwrMax[dbm]       : 4.00
RxPwrMin[dbm]       : -17.06            RxPwrMax[dbm]       : 5.85

Port                : 13                SFP / Media Type    : LX / SM
CLEI code           : VAUIAAXEAA        RedbackApproved     : Yes
SFP Serial No       : 74VT200492
Wavelength          : 1310.00[nm]
TxPwrMin[dbm]       : -7.21             TxPwrMax[dbm]       : 2.79
RxPwrMin[dbm]       : -16.46            RxPwrMax[dbm]       : 6.51

Port                : 14                SFP / Media Type    : LX / SM
CLEI code           :                   RedbackApproved     : Yes
SFP Serial No       : 4756020020
Wavelength          : 1310.00[nm]
TxPwrMin[dbm]       : -5.84             TxPwrMax[dbm]       : 4.16
RxPwrMin[dbm]       : -13.66            RxPwrMax[dbm]       : 7.01

Port                : 15                SFP / Media Type    : LX / SM
CLEI code           : VAUIAAXEAA        RedbackApproved     : Yes
SFP Serial No       : 75PT200042
Wavelength          : 1310.00[nm]
TxPwrMin[dbm]       : -8.59             TxPwrMax[dbm]       : 1.41
RxPwrMin[dbm]       : -16.72            RxPwrMax[dbm]       : 6.07

Port                : 16                SFP / Media Type    : LX / SM
CLEI code           : VAUIAAXEAA        RedbackApproved     : Yes
SFP Serial No       : 74VT200488
```

```
Wavelength          : 1310.00[nm]
TxPwrMin[dbm]       : -6.16             TxPwrMax[dbm]       : 3.84
RxPwrMin[dbm]       : -16.72            RxPwrMax[dbm]       : 6.20

Port                : 17                SFP / Media Type    : LX / SM
CLEI code           : VAUIAAXEAA        RedbackApproved     : Yes
SFP Serial No       : 74VT200062
Wavelength          : 1310.00[nm]
TxPwrMin[dbm]       : -6.74             TxPwrMax[dbm]       : 3.26
RxPwrMin[dbm]       : -16.99            RxPwrMax[dbm]       : 6.01

Port                : 18                SFP / Media Type    : LX / SM
CLEI code           : VAUIAAXEAA        RedbackApproved     : Yes
SFP Serial No       : 74VT200528
Wavelength          : 1310.00[nm]
TxPwrMin[dbm]       : -5.24             TxPwrMax[dbm]       : 4.76
RxPwrMin[dbm]       : -17.03            RxPwrMax[dbm]       : 5.87

Port                : 20                SFP / Media Type    : FX / MM
CLEI code           :                   RedbackApproved     : Yes
SFP Serial No       : 3577404
Wavelength          : 1310.00[nm]
TxPwrMin[dbm]       : -19.03            TxPwrMax[dbm]       : -14.00
RxPwrMin[dbm]       : -32.22            RxPwrMax[dbm]       : -14.00
```

The following example displays detailed output for an SSE card:

```
[local]Redback>show hardware card 3 detail

Slot                : 3                 Type                : sse
Serial No           : G30EF4208F000W    Hardware Rev        : 0001
EEPROM id/ver       : 0x5a/4            Mfg Date            : 27-OCT-2008
HubFpga rev         : 0x1e              HubFpga file rev    : 0x1e
SpiFpga rev         : 0xa9
Voltage 1.000V      : 1.000 (+0%)       Voltage 1.200V      : 1.198 (-0%)
Voltage 1.800V      : 1.798 (-0%)       Voltage 2.500V      : 2.502 (+0%)
Voltage 3.300V      : 3.300 (+0%)       Voltage 12.000V     : 11.710 (-2%)
Temperature         : NORMAL (53 C)
Card Status         : HW initialized    POD Status          : Success
ODD Status          : Not Available
Fail LED            : Off               Active LED          : On
Standby LED         : Off
Chass Entitlement   : All (0x0)
Active Alarms       : NONE

Disk                : 1                 Type                : sse
Hardware Rev        : 11                Model               : MBB2147RC(FUJITSU)
Spec Capacity       : 147GB             RedbackApproved     : Yes
CLEI code           : SOUCAJWTAA        Serial No           : G4111111111122
Mfg Date            : NOV 2011          Start/Stop count    : 1188 (max. 50000)
Voltage 3.300V      : 3.312 (+0%)       Voltage 5.000V      : 5.010 (+0%)
Voltage 12.000V     : 11.729 (-2%)
Temperature         : NORMAL (25 C)     LED                 : Green
POD Status          : Success           ODD Status          : Not Available
Active Alarms       : NONE

Disk                : 2                 Type                : sse
Hardware Rev        : 1                 Model               : MBB2147RC(FUJITSU)
Spec Capacity       : 147GB             RedbackApproved     : Yes
CLEI code           : SOUCAJWTAA        Serial No           : G4019100865437
Mfg Date            : OCT 2008          Start/Stop count    : 1106 (max. 50000)
Voltage 3.300V      : 3.312 (+0%)       Voltage 5.000V      : 4.998 (-0%)
Voltage 12.000V     : 11.729 (-2%)
Temperature         : NORMAL (24 C)     LED                 : Green
POD Status          : Success           ODD Status          : Not Available
Active Alarms       : NONE
```

1.4 show history

`show history` [**`configuration`**]

1.4.1 Purpose

Displays the command history for the current session.

1.4.2 Command Mode

All modes

1.4.3 Syntax Description

`configuration`	Optional. Displays a list of configuration commands entered during the current session. This keyword is available only in exec mode.

1.4.4 Default

Displays a list of commands entered during the current session within the current mode group (exec or configuration).

1.4.5 Usage Guidelines

Use the **`show history`** command to display the command history for the current session. The history log contains up to 40 commands. To restrict the history to only the configuration commands entered during the session, use the optional **`configuration`** keyword, which is only available in exec mode.

Note: By default, most **`show`** commands (in any mode) display information for the current context only or, depending on the command syntax, for all contexts. If you are an administrator for the local context, you can insert the optional **`context`** ***`ctx-name`*** construct before the **`show`** command to view output for the specified context without entering that context. For more information about the **`context`** ***`ctx-name`*** construct, see the **`context`** command description.

1.4.6 Examples

The following example displays output from the **`show history`** command (in global configuration mode):

```
[local]Redback(config)#show history


config

show clock
```

1.5 show http-redirect circuit

`show http-redirect circuit`

1.5.1 Purpose

Displays HTTP redirect circuit information.

1.5.2 Command Mode

All modes

1.5.3 Syntax Description

This command has no keywords or arguments.

1.5.4 Default

None

1.5.5 Usage Guidelines

Use the **`show http-redirect circuit`** command to display HTTP redirect circuit information.

Note: By default, most **`show`** commands (in any mode) display information for the current context only or, depending on the command syntax, for all contexts. If you are an administrator for the local context, you can insert the optional **`context`** ***`ctx-name`*** construct, preceding the **`show`** command, to view output for the specified context without entering that context. For more information about using the **`context`** ***`ctx-name`*** construct, see the **`context`** command description.

Note: By appending a space followed by the pipe (|) character at the end of a **`show`** command, you can filter the output using a set of modifier keywords and arguments. For more information, see *Modifying Output of show Commands*in the document, *Using the CLI*.

1.5.6 Examples

The following example displays HTTP redirect circuit information:

```
[local]Redback>show http-redirect circuit

Circuit Handle(internal    User Name / URL     Redir Count     Drop Count

10/6 vlan-id 2             user@local          0               0

                           http://www.redback.com/user@local
```

1.6 show icmp statistics

show icmp statistics

1.6.1 Purpose

Displays Internet Control Message Protocol (ICMP) statistics.

1.6.2 Command Mode

All modes

1.6.3 Syntax Description

This command has no keywords or arguments.

1.6.4 Default

None

1.6.5 Usage Guidelines

Use the **show icmp statistics** command to display ICMP statistics.

Note: By default, most **show** commands (in any mode) display information for the current context only or, depending on the command syntax, for all contexts. If you are an administrator for the local context, you can insert the optional **context** ***ctx-name*** construct, preceding the **show** command, to view output for the specified context without entering that context. For more information about using the **context** ***ctx-name*** construct, see the **context** command description.

Note: By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information, see *Modifying Output of show Commands*in the document, *Using the CLI*.

1.6.6 Examples

The following example displays output from the **show icmp statistics** command:

```
[local]Redback>show icmp statistics
```

```
icmp:
        6 calls to icmp_error
        0 errors not generated because old message was icmp
        Output histogram:
                destination unreachable: 6
        0 messages with bad code fields
        0 messages < minimum length
        0 bad checksums
        0 messages with bad length
        Input histogram:
                destination unreachable: 6
        0 message responses generated
icmp6:
        0 calls to icmp6_error
        0 errors not generated because old message was icmp6 or so
        0 errors not generated because rate limitation
        Output histogram:
                multicast listener report: 18
                router advertisment: 856
                neighbor solicitation: 4105
                neighbor advertisment: 2065
        0 messages with bad code fields
        0 messages < minimum length
        0 bad checksums
        0 messages with bad length
        Input histogram:
                packet too big: 77900
                router advertisment: 423
                neighbor solicitation: 2075
                neighbor advertisment: 4091
        0 message responses generated
        0 messages with too many ND options
```

1.7 show igmp bandwidth-profile

show igmp bandwidth-profile [*slot*/*port*[:*chan-num*[:*sub-chan-num*]]]

1.7.1 Purpose

Displays the configured Internet Group Management Protocol (IGMP) bandwidth profiles for ports.

1.7.2 Command Mode

All modes

1.7.3 Syntax Description

slot	Optional. Chassis slot number of the card with the port for which IGMP bandwidth profiles are displayed.
port	Optional. Card port number of the port for which IGMP bandwidth profiles are displayed.

1.7.4 Default

None

1.7.5 Usage Guidelines

Use the **show igmp bandwidth-profile** command to display the configured IGMP bandwidth profiles for ports.

Note: By default, most **show** commands (in any mode) display information for the current context only or, depending on the command syntax, for all contexts. If you are an administrator for the local context, you can insert the optional **context** *ctx-name* construct, preceding the **show** command, to view output for the specified context without entering that context. For more information about using the **context** *ctx-name* construct, see the **context** command description.

Note: By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information, see "*Modifying Output of show Commands*" in the document, *Using the CLI*.

1.7.6 Examples

The following example displays configured IGMP bandwidth profiles for ports:

```
[local]Redback>show igmp bandwidth-profile

  IGMP bandwidth profile


  slot/port:channel:subchannel      Bandwidth(in Kbps)
                                    Allowed/Used
  1/9                               100/40
  1/10                              100/0
```

1.8 show igmp circuit

```
show igmp circuit
```

1.8.1 Purpose

Displays circuit-specific information for the Internet Group Management Protocol (IGMP).

1.8.2 Command Mode

All modes

1.8.3 Syntax Description

This command has no keywords or arguments.

1.8.4 Default

None

1.8.5 Usage Guidelines

Use the **show igmp circuit** command to display circuit-specific information for the IGMP.

Note: By default, most **show** commands (in any mode) display information for the current context only or, depending on the command syntax, for all contexts. If you are an administrator for the local context, you can insert the optional **context** ***ctx-name*** construct, preceding the **show** command, to view output for the specified context without entering that context. For more information about using the **context** ***ctx-name*** construct, see the **context** command description.

Note: By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information, see "*Modifying Output of show Commands*" in the document, *Using the CLI*.

1.8.6 Examples

The following example displays circuit-specific information for the IGMP:

```
[local]Redback>show igmp circuit
```

```
  Number of circuits: 4

    1/9:1023:63/1/1/5, fxp1, Up, recv permit/send permit/unsol permit

    1/11:1023:63/1/1/13, fxp2, Up, recv permit/send permit/unsol permit

    12/1:1:63/1/2/18, fxp3, Up, recv permit/send permit/unsol permit

    12/1:1:63/1/2/19, fxp3, Up, recv permit/send permit/unsol permit
```

The following example displays output from the **`show igmp circuit`** command when a port pseudowire is configured:

```
[local]Redback>show igmp circuit

Flags: P - CLIPs Enabled, C - CLIPs Subscriber, A - AAA Provisioned,
       L - LNS Session, Q - Qos Rate Adjusted, B - Bulkstats Enabled
  Number of circuits: 2
  Context circuits: 2
    255/2:1:1/1/1/22, RP, Up, recv permit/send permit/unsol permit flags:
    255/25:1:2/1/1/41, PPW1, Up, recv permit/send permit/unsol permit flags:
```

1.9 show igmp group

show igmp group [*group-addr*] [**circuit** *circuit-handle* | **count** | **detail** | **subscriber** {**agent-circuit-id** *agent-circuit-id* | **agent-remote-id** *remote-circuit-id* | **username** *subscriber-username* [**detail**]}]

1.9.1 Purpose

Displays Internet Group Management Protocol (IGMP)-connected group membership information.

1.9.2 Command Mode

All modes

1.9.3 Syntax Description

group-addr	Optional. IP address of the IGMP group.
`circuit` *circuit-handle*	Optional. Displays a list of the IGMP groups joined to the specified circuit. Use the **show igmp circuit all** command to see the circuit handles for all IGMP circuits configured on the system.
`count`	Optional. Displays IGMP group membership count.
`detail`	Optional. Displays detailed group membership information, including membership tracking and IGMP Version 3 (IGMPv3) source lists.
`subscriber`	Optional. Displays the groups that are joined to subscribers based on the specified agent circuit ID, remote circuit ID, or subscriber username.
`agent-circuit-id` *agent-circuit-id*	Limits the command output to a specified agent circuit attribute for a subscriber session. Replace the *agent-circuit-id* argument with a text string of up to 63 alphanumeric characters.
`agent-remote-id` *remote-circuit-id*	Limits the command output to a specified remote circuit attribute for a subscriber session. Replace the *remote-circuit-id* argument with a text string of up to 63 alphanumeric characters.
`username` *subscriber-username*	Limits the command output to a specific subscriber name. Use the **show subscribers** command to see a list of all subscribers configured on the system.

1.9.4 Default

None

1.9.5 Usage Guidelines

Use the **show igmp group** command to display IGMP-connected group membership information.

Use the *group-addr* argument to display IGMP-connected group membership information for only the specified group.

Use the **detail** keyword to enable the explicit tracking of IGMP group membership for all hosts in a multiaccess network. Group membership information is displayed for hosts running IGMP Version 3 (IGMPv2), and group membership and source list information is displayed for hosts running IGMPv3.

Note: By default, most **`show`** commands (in any mode) display information for the current context only or, depending on the command syntax, for all contexts. If you are an administrator for the local context, you can insert the optional **`context`** ***`ctx-name`*** construct, preceding the **`show`** command, to view output for the specified context without entering that context. For more information about using the **`context`** ***`ctx-name`*** construct, see the **`context`** command description.

Note: By appending a space followed by the pipe (|) character at the end of a **`show`** command, you can filter the output using a set of modifier keywords and arguments. For more information, see “*Modifying Output of show Commands*” in the document, *Using the CLI*.

1.9.6 Examples

The following example displays output from the **`show igmp group`** command:

```
[local]Redback>show igmp group


IGMP Connected Group Membership
FLAGS: C - Connected, H - Static, L - Local, V - version 3 connected
Group Address    Flags/               Last Reporter/   Uptime     Expires
                 Interface            Circuit
224.1.1.1        C                    4.1.1.3          00:18:44   00:04:08
                 1                    1/1:511:63:31/7/2/2
```

The following example displays output from the **`show igmp group detail`** command:

```
[local]Redback>show igmp group detail

Group              : 224.1.1.1
  Interface        : 1
  Circuit          : 1/1:511:63:31/7/2/2
  Uptime           : 00:20:10
  Expires          : 00:02:41
  Last reporter    : 4.1.1.3
  Running version  : v2
  Compatible mode  : v2
  Host Count       : 1
  Host List :
   4.1.1.3, MAC: 00:00:69:4f:01:02
```

The following example displays output from the **show igmp group subscriber username** command:

```
[local]Redback>show igmp group subscriber username  00:00:69:4f:01:02

IGMP Connected Group Membership
FLAGS: C - Connected, H - Static, L - Local, V - version 3 connected
Group Address    Flags/                 Last Reporter/   Uptime     Expires
                 Interface              Circuit
224.1.1.1        C                      4.1.1.3          00:27:07   00:04:05
                 1                      1/1:511:63:31/7/2/2
```

The following example displays output from the **show igmp group** command when a port pseudowire is configured:

```
[local]Redback>show igmp group

IGMP Connected Group Membership
FLAGS: C - Connected, H - Static, L - Local, V - version 3 connected
Group Address    Flags/                 Last Reporter/   Uptime     Expires
                 Interface              Circuit
228.128.28.8     C                      21.1.1.2         00:00:28   00:03:52
                 PPW1                   255/25:1:2/1/1/41
```

1.10 show igmp group-bandwidth

show igmp group-bandwidth [*group-addr*]

1.10.1 Purpose

Displays bandwidth recommendations for multicast groups.

1.10.2 Command Mode

All modes

1.10.3 Syntax Description

group-addr

Optional. IP address of the multicast group for which information is to be displayed.

1.10.4 Default

None

1.10.5 Usage Guidelines

Use the **show igmp group-bandwidth** command to display bandwidth recommendations for multicast groups.

Specifying the *group-addr* argument displays bandwidth recommendations only for the specified group.

Use the **igmp group-bandwidth** command (in context configuration mode) to configure bandwidth recommendations for multicast groups.

Note: By default, most **show** commands (in any mode) display information for the current context only or, depending on the command syntax, for all contexts. If you are an administrator for the local context, you can insert the optional **context** *ctx-name* construct, preceding the **show** command, to view output for the specified context without entering that context. For more information about using the **context** *ctx-name* construct, see the **context** command description.

Note: By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information, see “*Modifying Output of show Commands*” in the document, *Using the CLI*.

1.10.6 Examples

The following example displays bandwidth recommendations for multicast groups:

```
[local]Redback>show igmp group-bandwidth

  IGMP bandwidth mapping

  Group prefix          Bandwidth

                        (in Kbps)

  224.1.1.0/24          20

  224.121.121.0/24      100
```

1.11 show igmp interface

`show igmp interface` [***`if-name`***] [**`brief`**]

1.11.1 Purpose

Displays Internet Group Management Protocol (IGMP) interface information.

1.11.2 Command Mode

All modes

1.11.3 Syntax Description

`if-name`	Optional. Name of the IGMP interface.
`brief`	Optional. Displays minimal IGMP interface information.

1.11.4 Default

None

1.11.5 Usage Guidelines

Use the **`show igmp interface`** command to display IGMP interface information.

Use the ***`if-name`*** argument to display information for only the specified IGMP interface.

Note: By default, most **`show`** commands (in any mode) display information for the current context only or, depending on the command syntax, for all contexts. If you are an administrator for the local context, you can insert the optional **`context`** ***`ctx-name`*** construct, preceding the **`show`** command, to view output for the specified context without entering that context. For more information about using the **`context`** ***`ctx-name`*** construct, see the **`context`** command description.

Note: By appending a space followed by the pipe (|) character at the end of a **`show`** command, you can filter the output using a set of modifier keywords and arguments. For more information, see "*Modifying Output of show Commands*" in the document, *Using the CLI*.

1.11.6 Examples

The following example displays information for the IGMP interface, `fxp1`:

```
[local]Redback>show igmp interface fxp1

Interface fxp1
  IP addrss is 103.1.1.2
  Multicast routing is enabled on the interface
  IGMP is enabled on the interface
  IGMP interface status is up
  IGMP configured version is 2
  IGMP running version is 2
  IGMP query interval is 125 seconds
  IGMP query response interval is 10 seconds
  IGMP last member query interval is 1000 milli-seconds
  Multicast designated router (DR) is 103.1.1.2 (this system)
  IGMP querier is 103.1.1.1
  IGMP robust value is 2
  Number of ccts bound: 1 <----- new
  No multicast groups joined
```

1.12 show igmp profile

show igmp profile {*prof-name* [*if-name*] | **circuit** [*if-name*]}

1.12.1 Purpose

Displays service profile information, bandwidth usage, and statistics generated for all circuits.

1.12.2 Command Mode

All modes

1.12.3 Syntax Description

prof-name	Service profile name. Specifies the service profile for which information is to be displayed.
if-name	Optional. Displays information only for the specified interface.
circuit	Displays bandwidth usage for all circuits.

1.12.4 Default

None

1.12.5 Usage Guidelines

Use the **show igmp profile** command to display service profile information, bandwidth usage, and statistics generated for all circuits.

Use the optional *if-name* argument to display information only for the specified interface.

Note: By default, most **show** commands (in any mode) display information for the current context only or, depending on the command syntax, for all contexts. If you are an administrator for the local context, you can insert the optional **context** *ctx-name* construct, preceding the **show** command, to view output for the specified context without entering that context. For more information about using the **context** *ctx-name* construct, see the **context** command description.

Note: By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information, see "*Modifying Output of show Commands*" in the document, *Using the CLI*.

1.12.6 Examples

The following example displays information about the current state of the service profile, `servpro1`, and all interfaces that are members of that service profile:

For information about how to configure and verify IGMP SSM mapping, see the **`ssm-map`** command at *Commands: shoz through sz*.

```
[local]Redback>show igmp profile servpro1


Service Profile : servpro1
      Circuit (Interface) : 2/3:511:63:31/6/2/121 (fxp4)
       Bandwidth used (kbps)/svlan used (kbps)/port percent (%): 1/0/0
       Groups (Max Allowed/Joined/Sticky) : 0/1/0
       Priority        : 0
       Joins received  : 148
       Leaves received : 0
       Groups dropped
        Max count exceeded       : 0
        Port Bandwidth exceeded : 0
        Vlan Bandwidth exceeded : 0
        Priority drops           : 0
        No bandwidth             : 0
        Access denied            : 0
```

The following example displays information for service profile, `servpro2`, on the `fxp4` interface:

```
[local]Redback>show igmp profile servpro2 fxp4


Service Profile : servpro1
      Circuit (Interface) : 2/3:511:63:31/6/2/121 (fxp4)
       Bandwidth used (kbps)/svlan used (kbps)/port percent (%): 1/0/0
       Groups (Max Allowed/Joined/Sticky) : 0/1/0
       Priority        : 0
       Joins received  : 150
       Leaves received : 0
       Groups dropped
        Max count exceeded       : 0
        Port Bandwidth exceeded : 0
        Vlan Bandwidth exceeded : 0
        Priority drops           : 0
        No bandwidth             : 0
        Access denied            : 0
```

The following example displays bandwidth usage information for the `fxp4` IGMP interface:

```
[local]Redback>show igmp profile circuit fxp4


       Circuit (Interface) : 2/1:511:63:31/1/1/5 (fxp4)
       Bandwidth used (kbps)/svlan used (kbps)/port percent (%): 0/0/0
       Groups (Max Allowed/Joined/Sticky) : 0/0/0
       Priority        : 0
       Joins received  : 0
       Leaves received : 0
       Groups dropped
        Max count exceeded      : 0
        Port Bandwidth exceeded : 0
        Vlan Bandwidth exceeded : 0
        Priority drops          : 0
        No bandwidth            : 0
        Access denied           : 0
```

The following example displays information for service profile `test1`, on the `one` interface when statistics are enabled for IGMP Call Admission Control (CAC) on a subscriber circuit:

```
[local]Redback>show igmp profile test1 one


Service Profile : test1
 Circuit (Interface) : 2/5:511:63:31/1/1/6 (one)
  Bandwidth used (kbps)/svlan bandwidth used (kbps)/port percentr (%):
 0/0/0%
  Groups (Max Allowed/Joined/Sticky) : 10/0/0

Priority                : 1
Joins received:         : 1
Leaves received:        : 1
Groups dropped
   Max count exceeded   : 0
   Port Bandwidth exceeded   : 0
   Vlan Bandwidth exceeded   : 0
   Priority drops            : 0
   No bandwidth              : 0
   Access denied             : 0
```

1.13 show igmp snooping access-group name

show igmp snooping access-group name ***group-name*** [**detail**]

1.13.1 Purpose

Displays information about a specified access list that is associated with an Internet Group Management Protocol (IGMP) snooping instance.

1.13.2 Command Mode

All modes

1.13.3 Syntax Description

group-name	Identifies an access group that is associated with an IGMP snooping instance.
detail	Optional. Displays detailed information for the specified access group.

1.13.4 Default

None

1.13.5 Usage Guidelines

Use the **show igmp snooping access-group** command to display information about a specified access list that is associated with an IGMP snooping instance.

1.13.6 Examples

The following example displays information for an access list called `acl1`:

```
[local]Redback#show igmp snooping access-group name acl1

access list acl1

Hit Count:          0   seq 10    deny   host 234.1.2.3

Hit Count:         16   seq 20  permit   any
```

1.14 show igmp snooping bridge

show igmp snooping bridge [*bridge-name*] [detail]

1.14.1 Purpose

Displays Internet Group Management Protocol (IGMP) snooping information for a specific bridge interface or all bridge interfaces that are currently configured on the router.

1.14.2 Command Mode

All modes

1.14.3 Syntax Description

bridge-name	Identifies an IGMP snooping bridge interface.
detail	Optional. Displays detailed information for the specified IGMP snooping bridge.

1.14.4 Default

Displays summary IGMP snooping information for all bridge interfaces that are currently configured on the router.

1.14.5 Usage Guidelines

Use the **show igmp snooping bridge** command to display IGMP snooping information for a specific bridge interface or all bridge interfaces that are currently configured on the router.

1.14.6 Examples

The following example displays IGMP snooping information for all bridge interfaces currently configured on the router:

```
[local]Redback#show igmp snooping bridge

IGMP Snooping:

Version Cct   Snooping

Bridge                         Cfg/Run Count Mode

----------------------------------------------------------

b2                               2/2    0     snooping

br1                              2/2    0     passive proxy  snooping

igmp-blue-bridge                 2/2    7     snooping

test                             3/3    4     snooping
```

The following example displays IGMP snooping information for a bridge interface called `igmp-blue-bridge`:

```
[local]Redback#show igmp snooping bridge igmp-blue-bridge

IGMP Snooping:

Version Cct   Snooping

Bridge                         Cfg/Run Count Mode

----------------------------------------------------------

igmp-blue-bridge                 2/2    7     snooping
```

The following example displays detailed IGMP snooping information for the bridge interface called `igmp-blue-bridge`:

```
[local]Redback#show igmp snooping bridge igmp-blue-bridge detail

IGMP Snooping:

Bridge: igmp-blue-bridge (mfib_id 0x20000001)  Version Cfg/Run: 2/2

Snooping: enabled     Proxy Mode: disabled    Robust:   2

Qry Intvl: 125s   Qry Resp Intvl: 10s   Last Member Qry Intvl: 1000ms

Mrouter count: 0    (*, G) count:  0    (S, G) count:  0

Packets sent/received/error:       0/0/0

Queries sent/received/error:       0/1/0

Reports sent/received/error:       0/0/0

 Leaves  sent/received/error:       0/0/0
```

1.15 show igmp snooping circuit

show igmp snooping circuit [*slot/port* [**vlan** *begin-range* **:** *end-range*]] [**counter** | **group** | **detail**]

1.15.1 Purpose

Displays IGMP snooping-related information about circuits that are bound to bridge interfaces that have IGMP snooping enabled.

1.15.2 Command Mode

All modes

1.15.3 Syntax Description

slot/port	Optional. Specifies a particular circuit whose IGMP snooping information you want to display. Replace the *slot* argument with the chassis slot number that hosts the circuit whose IGMP snooping output you want to display. Replace the *port* argument with the number that identifies the port whose IGMP snooping output you want to display. (1)
vlan *begin-range* **:** *end-range*	Optional. Displays (*,G) and (S,G) information for a specified range of IGMP snooping VLAN circuits.
counter	Optional. Displays IGMP counters for a specified IGMP snooping circuit or all IGMP snooping circuits currently configured on the router.
group	Optional. Displays detailed group membership information for a specified IGMP snooping circuit or all IGMP snooping circuits currently configured on the router.
detail	Optional. Displays IGMP counters and detailed group membership information for a specified IGMP snooping circuit or all IGMP snooping circuits currently configured on the router.

(1) To see a list of all IGMP snooping circuits currently configured on the router, use the show igmp snooping circuit command without any of the optional keywords or arguments.

1.15.4 Default

Displays a list of all circuits that are bound to bridge interfaces that have IGMP snooping enabled.

1.15.5 Usage Guidelines

Use the **show igmp snooping circuit** command to display IGMP snooping-related information about circuits that are bound to bridge interfaces that have IGMP snooping enabled.

1.15.6 Examples

The following example displays a list of all circuits that are bound to bridges that have IGMP snooping enabled:

```
[local]Redback#show igmp snooping circuit

Circuit                       Bridge              Profile             Flags

-----------------------------------------------------------------------

1/1:1023:63/1/1/4             igmp-test-bridge

4/3:1023:63/1/2/16            igmp-test-bridge

4/3:1023:63/1/2/17            igmp-test-bridge    mrouter

4/3:1023:63/1/2/18            igmp-test-bridge    bar

4/3:1023:63/1/2/19            igmp-test-bridge    bar

4/3:1023:63/1/2/20            igmp-test-bridge

4/3:1023:63/1/2/21            igmp-test-bridge

4/3:1023:63/1/2/22            test

4/3:1023:63/1/2/23            test

4/3:1023:63/1/2/24            test

4/3:1023:63/1/2/25            test                mrouter
```

The following example displays IGMP snooping information for the circuit 1 on the card that is installed in slot 1 of the router:

```
[local]Redback#show igmp snooping circuit 1/1

Circuit                      Bridge              Profile             Flags

----------------------------------------------------------------------

1/1:1023:63/1/1/4            igmp-test-bridge
```

The following example displays IGMP counters and detailed group membership information for the IGMP snooping circuit `1` on the card installed in slot `1` of the router:

```
[local]Redback#show igmp snooping circuit 1/1 detail


IGMP Snooping Cct:

Circuit: 1/1:1023:63/1/1/4

Snooping: enabled     Version Cfg/Run:  2/2   Cct state:      down

Robust: 2    Qry Intvl: 125s   Last Member Qry Intvl: 1000ms

IGMP Snooping reports received/error:       0/0

IGMP Snooping queries received/error:       0/0

IGMP Snooping leaves received/error:        0/0

Mrouter Monitoring: enabled   Attached: no
```

The following example displays IGMP counters for the IGMP snooping circuit `1` on the card installed in slot `1` of the router:

```
[local]Redback#show igmp snooping circuit 1/1 counter

IGMP Snooping Cct:

Circuit: 1/1:1023:63/1/1/4

Snooping: enabled     Version Cfg/Run:  2/2   Cct state:      down

Robust: 2    Qry Intvl: 125s   Last Member Qry Intvl: 1000ms

IGMP Snooping reports received/error:       0/0

IGMP Snooping queries received/error:       0/0

IGMP Snooping leaves received/error:        0/0

Mrouter Monitoring: enabled   Attached: no
```

The following example displays detailed group membership information for the IGMP snooping circuit `4` on the card installed in slot `3` of the router:

```
[local]Redback#show igmp snooping circuit 4/3 group

IGMP Snooping Cct:

Circuit: 4/3:1023:63/1/2/16

Snooping: enabled     Version Cfg/Run:  2/2   Cct state:      up

Robust: 2    Qry Intvl: 125s   Last Member Qry Intvl: 1000ms

Mrouter Monitoring: enabled   Attached: no

Circuit: 4/3:1023:63/1/2/17

Snooping: enabled     Version Cfg/Run:  2/2   Cct state:      up

Robust: 2    Qry Intvl: 125s   Last Member Qry Intvl: 1000ms

Mrouter Monitoring: static

Circuit: 4/3:1023:63/1/2/18

Snooping: enabled     Version Cfg/Run:  2/2   Cct state:      up

Robust: 2    Qry Intvl: 125s   Last Member Qry Intvl: 1000ms
```

```
Mrouter Monitoring: enabled   Attached: no
Flags: S - static
Groups                             State          Uptime/Expires   Flags
(*, 233.1.1.1)                     FORWARD       5d22h   /00:00:00    S
(*, 234.1.1.3)                     FORWARD       5d22h   /00:00:00    S
(*, 233.1.1.5)                     FORWARD       5d22h   /00:00:00    S
(*, 233.1.1.2)                     FORWARD       5d22h   /00:00:00    S
(*, 233.1.1.6)                     FORWARD       5d22h   /00:00:00    S
(*, 233.1.1.4)                     FORWARD       5d22h   /00:00:00    S
Circuit: 4/3:1023:63/1/2/19
Snooping: enabled     Version Cfg/Run:  2/2   Cct state:      up
Robust: 2    Qry Intvl: 125s   Last Member Qry Intvl: 1000ms
Mrouter Monitoring: enabled   Attached: no
Flags: S - static
Groups                             State          Uptime/Expires   Flags
(*, 233.1.1.1)                     FORWARD       5d22h   /00:00:00    S
(*, 234.1.1.3)                     FORWARD       5d22h   /00:00:00    S
(*, 233.1.1.5)                     FORWARD       5d22h   /00:00:00    S
(*, 233.1.1.2)                     FORWARD       5d22h   /00:00:00    S
(*, 233.1.1.6)                     FORWARD       5d22h   /00:00:00    S
(*, 233.1.1.4)                     FORWARD       5d22h   /00:00:00    S
Circuit: 4/3:1023:63/1/2/20
Snooping: enabled     Version Cfg/Run:  2/2   Cct state:      up
Robust: 2    Qry Intvl: 125s   Last Member Qry Intvl: 1000ms
Mrouter Monitoring: enabled   Attached: no
```

```
Circuit: 4/3:1023:63/1/2/21
Snooping: enabled     Version Cfg/Run:  2/2   Cct state:      up
Robust: 2    Qry Intvl: 125s   Last Member Qry Intvl: 1000ms
Mrouter Monitoring: enabled   Attached: no
Circuit: 4/3:1023:63/1/2/22
Snooping: enabled     Version Cfg/Run:  3/3   Cct state:      up
Robust: 2    Qry Intvl: 125s   Last Member Qry Intvl: 1000ms
Mrouter Monitoring: enabled   Attached: no
Circuit: 4/3:1023:63/1/2/23
Snooping: enabled     Version Cfg/Run:  3/3   Cct state:      up
Robust: 2    Qry Intvl: 125s   Last Member Qry Intvl: 1000ms
Mrouter Monitoring: enabled   Attached: no
Circuit: 4/3:1023:63/1/2/24
Snooping: enabled     Version Cfg/Run:  3/3   Cct state:      up
Robust: 2    Qry Intvl: 125s   Last Member Qry Intvl: 1000ms
Mrouter Monitoring: enabled   Attached: no
Circuit: 4/3:1023:63/1/2/25
Snooping: enabled     Version Cfg/Run:  3/3   Cct state:      up
Robust: 2    Qry Intvl: 125s   Last Member Qry Intvl: 1000ms
Mrouter Monitoring: static
```

1.16 show igmp snooping group

show igmp snooping group [*group-address* [**source** *source-address*]] **bridge** *bridge-name* [**count**]

1.16.1 Purpose

Displays a per-bridge list of IGMP groups and their associated circuits.

1.16.2 Command Mode

All modes

1.16.3 Syntax Description

group-address	Optional. IP address of the group whose configuration information you want to display.
source *source-address*	Optional. Source for a multicast group. Replace the argument with the IP address of a source as desired.
bridge *bridge-name*	IGMP snooping bridge interface.
count	Optional. Displays the number of circuits currently subscribed to the specified bridge group.

1.16.4 Default

None

1.16.5 Usage Guidelines

Use the **show igmp snooping group** command to display a per-bridge list of IGMP groups and their associated circuits.

1.16.6 Examples

The following example displays information about the multicast state of the IGMP snooping bridge called `igmp-green-bridge`:

For information about how to configure and verify IGMP SSM mapping, see the **ssm-map** command at *Commands: shoz through sz*.

```
[local]Redback#show igmp snooping group bridge igmp-green-bridge
```

```
IGMP Snooping Groups on Bridge:(*, 234.1.1.3), 0x280002
4/3:1023:63/1/2/17, MROUTER
4/3:1023:63/1/2/18, STATIC
4/3:1023:63/1/2/19, STATIC
(*, 233.1.1.2), 0x280005
4/3:1023:63/1/2/17, MROUTER
4/3:1023:63/1/2/18, STATIC
4/3:1023:63/1/2/19, STATIC
(*, 233.1.1.1), 0x280001
4/3:1023:63/1/2/17, MROUTER
4/3:1023:63/1/2/18, STATIC
4/3:1023:63/1/2/19, STATIC
(*, 233.1.1.6), 0x280006
4/3:1023:63/1/2/17, MROUTER
4/3:1023:63/1/2/18, STATIC
4/3:1023:63/1/2/19, STATIC
(*, 233.1.1.5), 0x280004
4/3:1023:63/1/2/17, MROUTER
  4/3:1023:63/1/2/18, STATIC
  4/3:1023:63/1/2/19, STATIC
(*, 233.1.1.4), 0x280003
  4/3:1023:63/1/2/17, MROUTER
  4/3:1023:63/1/2/18, STATIC, DYNAMIC
  4/3:1023:63/1/2/19, STATIC
```

The following example displays the number of circuits currently subscribed to the bridge group called `igmp-green-bridge`:

```
[local]Redback#show igmp snooping group bridge igmp-green-bridge count
IGMP Snooping Groups on Bridge:
Group                                 Packets/Bytes     Number of circuits
(*, 234.1.1.3)                              0/0          3
(*, 233.1.1.2)                              0/0          3
(*, 233.1.1.1)                              0/0          3
(*, 233.1.1.6)                              0/0          3
(*, 233.1.1.5)                              0/0          3
(*, 233.1.1.4)                              0/0          3
```

1.17 show igmp snooping mrouter

show igmp snooping mrouter [**bridge** ***bridge-name***]

1.17.1 Purpose

Displays a per-bridge list of circuits that are facing multicast routers.

1.17.2 Command Mode

All modes

1.17.3 Syntax Description

bridge ***bridge-name***	IGMP snooping bridge interface.

1.17.4 Default

None

1.17.5 Usage Guidelines

Use the **show igmp snooping mrouter** command to display a per-bridge list of circuits that are facing multicast routers.

Enter the **show igmp snooping mrouter** command without the optional **bridge** ***bridge-name*** construct to display a list of all circuits that are currently facing multicast routers. Include the optional **bridge** ***bridge-name*** construct in the **show igmp snooping mrouter** command to display a list of multicast router-facing circuits that are bound to a specific bridge.

Note: The **show igmp snooping mrouter** command displays mrouter information only for those bridges that are configured in the current context. To display mrouter information for bridges that are configured in a different context, use the **context** command in global configuration mode to change to the appropriate context and before entering the show igmp snooping mrouter command.

1.17.6 Examples

The following example displays mrouter information all bridges configured in the current context:

```
[local]Redback#show igmp snooping mrouter

FLAGS: S - Static

Bridge Name          Circuit Handle                Timeout   Flags

-----------------------------------------------------------------

igmp-test-bridge     4/3:1023:63/1/2/17                        S

test                 4/3:1023:63/1/2/25                        S
```

The following example displays mrouter information for a bridge called `igmp-red-bridge`:

```
[local]Redback#show igmp snooping mrouter bridge igmp-red-bridge

FLAGS: S - Static

Bridge Name          Circuit Handle                Timeout   Flags

-----------------------------------------------------------------

igmp-red-bridge     4/3:1023:63/1/2/17                        S
```

1.18 show igmp traffic

show igmp traffic

1.18.1 Purpose

Displays Internet Group Management Protocol (IGMP) traffic statistics.

1.18.2 Command Mode

All modes

1.18.3 Syntax Description

This command has no keywords or arguments.

1.18.4 Default

None

1.18.5 Usage Guidelines

Use the **show igmp traffic** command to display IGMP traffic statistics.

Note: By default, most **show** commands (in any mode) display information for the current context only or, depending on the command syntax, for all contexts. If you are an administrator for the local context, you can insert the optional **context** ***ctx-name*** construct, preceding the **show** command, to view output for the specified context without entering that context. For more information about using the **context** ***ctx-name*** construct, see the **context** command description.

Note: By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information, see “*Modifying Output of show Commands*” in the document, *Using the CLI*.

1.18.6 Examples

The following example displays output from the **show igmp traffic** command:

```
[local]Redback>show igmp traffic
```

```
IGMP statistics:

 Sent:   Total:  61       Query: 57          Report: 3        Leave: 1

 Rcvd:   Total:  25       Query: 15          Report: 8        Leave: 2

 Error:  Total:  0        Query: 0           Report: 0        Cksum: 0

         System: 0        Tooshort: 0        Others: 0

Input Queue:
         Current: 0       Max size: 3        Overflows: 0

         ReportIPCs: 0

Statistics Buffers:
         Maximum: 5       Total Used: 1      Context Used: 1
```

1.19 show inverse-arp counters

show inverse-arp counters [**all-contexts**] [[*slot*/*port*] [**vpi** *vpi* [**vci** *vci*]]] [**sum**]

1.19.1 Purpose

Displays inverse Address Resolution Protocol (ARP) counters.

This command applies only to ATM cards.

1.19.2 Command Mode

All modes

1.19.3 Syntax Description

all-contexts	Optional. Displays inverse ARP counters for all contexts. This option is available only if you are a local administrator. If omitted, displays inverse ARP counters for the current context only.
slot	Optional. Chassis slot number. If omitted, displays inverse ARP counters for all ports on all traffic cards.
port	Optional. Traffic card port number; required when the *slot* argument is included.
vpi *vpi*	Optional. Virtual path identifier (VPI) for the Asynchronous Transfer Mode (ATM) permanent virtual circuit (PVC) for which to display inverse ARP counters. The range of values is 0 to 255. If omitted, displays counters for all virtual paths (VPs) on the port.
vci *vci*	Optional. Virtual circuit identifier (VCI) for the ATM PVC for which to display inverse ARP counters. The range of values is 1 to 65,535. If omitted, displays counters for all ATM PVCs on the VP.
sum	Optional. Displays summary information for inverse ARP counters.

1.19.4 Default

When entered without any optional syntax, the **show inverse-arp counters** command displays inverse ARP counters for all ports on all traffic cards for the current context only.

1.19.5 Usage Guidelines

Use the **show inverse-arp counters** command to display inverse ARP counters. Counters include total counts for received, dropped, and sent packets. Local administrators have privileges that are not available to other administrators.

Note: The SmartEdge 100 router limits the value of the ***slot*** argument to 2.

Note: By default, most **show** commands (in any mode) display information for the current context only or, depending on the command syntax, for all contexts. If you are an administrator for the local context, you can insert the optional **context** ***ctx-name*** construct, preceding the **show** command, to view output for the specified context without entering that context. For more information about using the **context** ***ctx-name*** construct, see the **context** command description.

Note: By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information, see "*Modifying Output of show Commands*" in the document, *Using the CLI*.

1.19.6 Examples

The following example displays inverse ARP counters for ATM PVCs configured on port 1 on the traffic card in slot 4 in the current context:

```
[local]Redback>show inverse-arp counters 4/1

current time: Mon Jun  6 01:31:59 2005
                      Pkts             Pkts             Pkts
  Slot/Port VPI VCI   Received         Replied          Dropped
   4/1      100 32    306              0                306

Totals
  Packets Rcvd:                    306 Packets Replied:0
  Rcv Packets Dropped:             306
```

1.20 show ip access-list

show ip access-list [{[**summary**] [*acl-name*] | **first-match** *acl-name* [*protocol*] {*src-addr* [**port** *port*]} [*dest-addr* [**port** *port*] [**dscp** *dscp-value*] [**established** | **setup** | **invalid-tcp-flags**] [**length** *length*] [**precedence** *prec-value*] [**tos** *tos-value*] [[**fragments**] | [**ip-options**]]}]

1.20.1 Purpose

Displays the status of configured IP access control lists (ACLs).

1.20.2 Command Mode

All modes

1.20.3 Syntax Description

summary	Optional. Excludes the ACL statements from the display. Optionally, you can follow this keyword with the *acl-name* argument, naming a particular ACL for which you want summary information displayed.
acl-name	Optional. Name of the ACL for which you want information displayed. To display summary information about a specific list, you must enter the **summary** keyword first, followed by the *acl-name* argument.
first-match *acl-name*	Optional. Name of the ACL for which you want to find the first statement matched by the criteria that follows the **first-match** *acl-name* construct.

protocol	Optional. Number indicating a protocol as specified in RFC 1700, `Assigned Numbers`. The range of values is 0 to 255. In place of the ***protocol*** argument, you can use any of the following keywords: • **ahp**—Specifies the Authentication Header Protocol. • **esp**—Specifies the encapsulation security payload. • **gre**—Specifies Generic Routing Encapsulation. • **host**—Specifies the host source address. • **icmp**—Specifies the Internet Control Message Protocol. • **igmp**—Specifies the Internet Group Management Protocol. • **ip**—Uses any IP protocol. • **ipinip**—Specifies IP-in-IP tunneling. • **ospf**—Specifies the Open Shortest Path First protocol. • **pcp**—Specifies the Payload Compression Protocol. • **pim**—Specifies Protocol Independent Multicast. • **tcp**—Specifies the Transmission Control Protocol. • **udp**—Specifies the User Datagram Protocol.
src-addr	Source address to be included in the criteria for a match. An IP address in the form ***A.B.C.D***.
port ***port***	Optional. TCP or UDP port to be considered a match for either the source or destination IP address. This construct is only available if you specified TCP or UDP as the protocol. The range of values is 1 to 65,535. You can also substitute a keyword for the ***port*** argument as listed in Table 6 and Table 7 in the “Usage Guidelines” section for this command.
dest-addr	Optional. Destination address to be included in the criteria for a match. An IP address in the form ***A.B.C.D***.
dscp ***dscp-value***	Optional. Differentiated Services Code Point (DSCP) to be included in the criteria for a match. The range of values is 0 to 63. You can also substitute a keyword for the ***dscp-value*** argument as listed in Table 8 in the “Usage Guidelines” section for this command.
established	Optional. Specifies that only established connections are to be matched. This keyword is only available if you specify **tcp** for the ***protocol*** argument.

`invalid-tcp-flags`	Optional. Specifies that TCP packets with flag combinations other than the following are a match: • SYN • SYN+ACK • ACK • PSH+ACK • URG+ACK • URG+PSH+ACK • FIN • FIN+ACK • RST • RST+ACK Only the lower-order 6 bits (for example, FIN, SYN, RST, PSH, ACK, and URG) in the TCP Flags field are considered for validation. The higher order 6-bits (ECN bits defined by RFC 3168, *The Addition of Explicit Congestion Notification (ECN) to IP*, and the reserved bits) are ignored. This keyword is only available if you specify **`tcp`** for the ***`protocol`*** argument.
`setup`	Optional. Specifies that TCP packets with SYN set and ACK not set in the Flags field are a match. This keyword is only available if you specify **`tcp`** for the ***`protocol`*** argument.
`length` ***`length`***	Packet length. The length of the network-layer packet, beginning with the IP header. The range of values is 20 to 65,535.

`precedence` *`prec-value`*	Optional. Precedence value of packets to be included in the criteria for a match. The range of values is 0 to 7, with 7 being the highest precedence. In place of the *`prec-value`* argument, you can enter any of the following keywords: • **`routine`**—Specifies routine precedence (value = 0). • **`priority`**—Specifies priority precedence (value = 1). • **`immediate`**—Specifies immediate precedence (value = 2). • **`flash`**—Specifies flash precedence (value = 3). • **`flash-override`**—Specifies flash override precedence (value = 4). • **`critical`**—Specifies critical precedence (value = 5). • **`internet`**—Specifies internetwork control precedence (value = 6). • **`network`**—Specifies network control precedence (value = 7).
`tos` *`tos-value`*	Optional. Type of service (ToS) to be included in the criteria for a match. The range of values is 0 to 15. In place of the *`tos-value`* argument, you can enter any of the following keywords: • **`max-reliability`**—Specifies maximum reliable ToS (value = 2). • **`max-throughput`**—Specifies maximum throughput ToS (value = 4). • **`min-delay`**—Specifies minimum delay ToS (value = 8). • **`min-monetary-cost`**—Specifies minimum monetary cost ToS (value = 1). • **`normal`**—Specifies normal ToS (value = 0). To specify both a precedence and a ToS, you must enter the **`precedence`** *`prec-value`* construct first, followed by the **`tos`** *`tos-value`* construct.

1.20.4 Default

When entered without any optional syntax, the **`show ip access-list`** command displays information for all IP ACLs in the context, including the statements in each list.

1.20.5 Usage Guidelines

Use the **`show ip access-list`** command to display the status of configured IP ACLs.

Use the **`first-match`** ***`acl-name`*** construct to display the first statement in the ACL that is matched by the criteria that follows the **`first-match`** ***`acl-name`*** construct.

Table 6 lists the valid keyword substitutions for the *`port`* argument when the argument is used to specify a TCP port.

Table 6 Valid Keyword Substitutions for the port Argument (TCP Port)

Keyword	Definition	Corresponding Port Number
`bgp`	Border Gateway Protocol	179
`chargen`	Character generator	19
`cmd`	Remote commands (rcmd)	514
`daytime`	Daytime	13
`discard`	Discard	9
`domain`	Domain Name System	53
`echo`	Echo	7
`exec`	Exec (rsh)	512
`finger`	Finger	79
`ftp`	File Transfer Protocol	21
`ftp-data`	FTP data connections (used infrequently)	20
`gopher`	Gopher	70
`hostname`	Network interface card (NIC) hostname server	101
`ident`	Identification protocol	113
`irc`	Internet Relay Chat	194
`klogin`	Kerberos login	543
`kshell`	Kerberos Shell	544
`login`	Login (rlogin)	513
`lpd`	Printer service	515
`nntp`	Network News Transport Protocol	119
`pim-auto-rp`	Protocol Independent Multicast Auto-RP	496
`pop2`	Post Office Protocol Version 2	109
`pop3`	Post Office Protocol Version 3	110
`shell`	Remote Command Shell	514
`smtp`	Simple Mail Transport Protocol	25
`ssh`	Secure Shell	22

Table 6 Valid Keyword Substitutions for the port Argument (TCP Port)

Keyword	Definition	Corresponding Port Number
`sunrpc`	Sun Remote Procedure Call	111
`syslog`	Syslog	514
`tacacs`	Terminal Access Controller Access Control System	49
`talk`	Talk	517
`telnet`	Telnet	23
`time`	Time	37
`uucp`	Unix-to-Unix Copy Program	540
`whois`	Nickname	43
`www`	World Wide Web (HTTP)	80

Table 7 lists the valid keyword substitutions for the *port* argument when the argument is used to specify a UDP port.

Table 7 Valid port Argument Keyword Substitution Values for UDP Ports

Keyword	Definition	Corresponding Port Number
`biff`	Biff (Mail Notification, Comsat)	512
`bootpc`	Bootstrap Protocol client	68
`bootps`	Bootstrap Protocol server	67
`discard`	Discard	9
`dnsix`	DNSIX Security Protocol Auditing	195
`domain`	Domain Name System	53
`echo`	Echo	7
`isakmp`	Internet Security Association and Key Management Protocol (ISAKMP)	500
`mobile-ip`	Mobile IP registration	434
`nameserver`	IEN116 Name Service (obsolete)	42
`netbios-dgm`	NetBIOS Datagram Service	138
`netbios-ns`	NetBIOS Name Service	137
`netbios-ss`	NetBIOS Session Service	139
`ntp`	Network Time Protocol	123
`pim-auto-rp`	Protocol Independent Multicast Auto-RP	496

Table 7 Valid port Argument Keyword Substitution Values for UDP Ports

Keyword	Definition	Corresponding Port Number
rip	Router Information Protocol (router, in.routed)	520
snmp	Simple Network Management Protocol	161
snmptrap	SNMP traps	162
sunrpc	Sun Remote Procedure Call	111
syslog	System logger	514
tacacs	Terminal Access Controller Access Control System	49
talk	Talk	517
tftp	Trivial File Transfer Protocol	69
time	Time	37
who	Who Service (rwho)	513
xdmcp	X Display Manager Control Protocol	177

Table 8 lists the valid keyword substitutions for the ***dscp-value*** argument.

Table 8 Valid Keyword Substitutions for the dscp-value Argument

Keyword	Definition
af11	Assured Forwarding—Class 1/Drop Precedence 1
af12	Assured Forwarding—Class 1/Drop Precedence 2
af13	Assured Forwarding—Class 1/Drop Precedence 3
af21	Assured Forwarding—Class 2/Drop Precedence 1
af22	Assured Forwarding—Class 2/Drop Precedence 2
af23	Assured Forwarding—Class 2/Drop Precedence 3
af31	Assured Forwarding—Class 3/Drop Precedence 1
af32	Assured Forwarding—Class 3/Drop Precedence 2
af33	Assured Forwarding—Class 3/Drop Precedence 3
af41	Assured Forwarding—Class 4/Drop Precedence 1
af42	Assured Forwarding—Class 4/Drop Precedence 2
af43	Assured Forwarding—Class 4/Drop Precedence 3
cs0	Class Selector 0
cs1	Class Selector 1
cs2	Class Selector 2

Table 8 Valid Keyword Substitutions for the dscp-value Argument

Keyword	Definition
`cs3`	Class Selector 3
`cs4`	Class Selector 4
`cs5`	Class Selector 5
`cs6`	Class Selector 6
`cs7`	Class Selector 7
`df`	Default Forwarding (same as cs0)
`ef`	Expedited Forwarding

Note: By default, most **`show`** commands (in any mode) display information for the current context only or, depending on the command syntax, for all contexts. If you are an administrator for the local context, you can insert the optional **`context`** ***`ctx-name`*** construct, preceding the **`show`** command, to view output for the specified context without entering that context. For more information about using the **`context`** ***`ctx-name`*** construct, see the **`context`** command description.

Note: By appending a space followed by the pipe (|) character at the end of a **`show`** command, you can filter the output using a set of modifier keywords and arguments. For more information, see the "*Modifying Output of show Commands*" in the document, *Using the CLI*.

1.20.6 Examples

The following example displays output from the **`show ip access-list`** command:

```
[local]Redback>show ip access-list

ip access-list client1_list:
 count: 1, sequences: 10 - 10, client count: 0
 modified: 01:36:56 (hh:mm:ss) ago
 counting: disabled, logging: disabled
 seq 10 permit ip any any
ip access-list test_list:
 count: 4, sequences: 10 - 40, client count: 0
 modified: 01:36:56 (hh:mm:ss) ago
 counting: disabled, logging: disabled
 description: test list
  seq 10 permit ip any any
  seq 20 deny ip any any
  seq 30 permit ip any any
  seq 40 permit ip any any
ip access-list test2_list:
 count: 0, sequences: 0 - 0, client count: 0
 modified: 01:36:56 (hh:mm:ss) ago
 counting: disabled, logging: disabled
 description: test 2 list
total ip access lists: 3
```

The following example displays the statements and conditions configured for the policy ACL, `ipacl_cond`:

```
[local]Redback>show ip access-list ipacl_cond

ip access-list ipacl_cond:
  count: 2, sequences: 10 - 20, client count: 1
  modified: 00:10:21 (hh:mm:ss) ago, version: 14
   condition 100 time-range
    absolute start 2005:01:01:01:00 end 2005:01:01:01:01 deny
   seq 10 permit tcp any any eq www condition 100
   seq 20 deny ip any any
```

1.21 show ip host

show ip host

1.21.1 Purpose

Displays all static hostname-to-IP Version 4 (IPv4) address mappings stored in the local host table for the current context.

1.21.2 Command Mode

All modes

1.21.3 Syntax Description

This command has no keywords or arguments.

1.21.4 Default

None

1.21.5 Usage Guidelines

Use the **show ip host** command to display all static hostname-to-IPv4 address mappings stored in the local host table for the current context.

Note: By default, most **show** commands (in any mode) display information for the current context only or, depending on the command syntax, for all contexts. If you are an administrator for the local context, you can insert the optional **context** ***ctx-name*** construct, preceding the **show** command, to view output for the specified context without entering that context. For more information about using the **context** ***ctx-name*** construct, see the **context** command description.

Note: By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information, see “*Modifying Output of show Commands*” in the document, *Using the CLI*.

1.21.6 Examples

The following example displays output from the **show ip host** command:

```
[local]Redback>show ip host

Host Name                IP Address       Type        TTL

host1                    172.2.3.1        static      0

host2                    172.2.3.2        static      0

host3                    172.2.3.3        static      0
```

1.22 show ip interface

show ip interface [*if-name* | **all-context** | **brief** | **xcrp**]

1.22.1 Purpose

Displays information about interfaces, including the interface bound to the Ethernet management port on the controller card.

1.22.2 Command Mode

All modes

1.22.3 Syntax Description

if-name	Optional. Name of the interface to be displayed.
all-context	Optional. Displays interface information for all contexts.
brief	Optional. Displays the name, IP address, and other information (in brief) for all configured interfaces in the current context.
xcrp	Optional. Displays incoming and outgoing packets, errors, and collisions for the interface to which the Ethernet management port on the controller cards is bound, including incoming and outgoing packets, errors, dropped bytes, and collisions.

1.22.4 Default

Displays detailed information for all configured interfaces.

1.22.5 Usage Guidelines

Use the **show ip interface** command to display information about all interfaces, including those on the controller card. Use this command without optional syntax to display detailed information on all configured interfaces. This command is also related to the **ip tcp mss** command.

Note: By default, most **show** commands (in any mode) display information for the current context only or, depending on the command syntax, for all contexts. If you are an administrator for the local context, you can insert the optional **context** *ctx-name* construct before the **show** command to view output for the specified context without entering that context. For more information about the **context** *ctx-name* construct, see the **context** command description.

Note: By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information, see "*Modifying Output of show Commands*" in the document, *Using the CLI*.

An interface can be in any of the following states:

- Unbound—The interface is not currently bound to any port or circuit.
- Bound—The interface is bound to at least one port or circuit; however, none of the bound circuits are up; therefore, the interface is not up.
- Up—At least one of the bound circuits is in the up state; therefore, the interface is also up and traffic can be sent over the interface.

1.22.6 Examples

The following example displays output from the **show ip interface** command with the **brief** keyword:

```
[local]Redback>show ip interface brief

Mon Jun 27 06:38:05 2005

Name            Address                  MTU    State      Bindings

fe13/3          3.2.13.3/16              1500   Up         ethernet 13/3

fe13/4          4.2.13.4/16              1500   Up         ethernet 13/4

5/1             10.13.49.166/24          1500   Up         ethernet 5/1

12/1            10.1.1.1/16              0      UnBound

un1             (Un-numbered)            0      UnBound

lo1             100.1.1.1/16             1500   Up         (Loopback)
```

The following example displays information for the mss-test interface:

```
[local]Redback#show ip interface mss-test


Intf name:        mss2
Intf state:       Up                         MTU:                800
IP address:       1.1.2.1                    Prefix len:         24
Resoln type:      Arp                        ARP timeout:        3600
ARP proxy:        Disabled                   ARP secured:        Disabled
TCP MSS In:       replace                    size:             1024
TCP MSS Out:      replace                    size:             1024
Number of Bound Circuits (incl. dynamic) = 1
Bindings:  (Total Bound Circuits 1)
Encapsulation     Circuit
ethernet          2/2
```

The following example displays packet information for the interface to which the Ethernet management port is bound:

```
[local]Redback>show ip interface xcrp
```

```
Name   Mtu    Network            Address              Ipkts      Opkts     Colls
                                                      Ierrs      Oerrs     Drops
fxp0   1500   <Link>             00:30:88:00:03:6f    62716      22871         0
                                                          2          0         0
fxp0   1500   10.13.49/24        10.13.49.166         62716      22871         0
                                                          2          0         0
ipc0   8192   <Link>                                  32078      26862         0
                                                          0          0         0
ipc0   8192   127                127.0.2.5            32078      26862         0
                                                          0          0         0
lo0    33228  <Link>                                      0          0         0
                                                          0          0         0
lo0    33228  127                127.0.0.1                0          0         0
                                                          0          0         0
xcrp   65535  <Link>                                      0          0         0
                                                          0          0         0
lc12   65535  <Link>                                   2461       2452         0
                                                          0          0         0
```

The following example displays byte information for the interface to which the Ethernet management port is bound:

```
[local]Redback>show ip interface xcrp bytes
```

```
Name   Mtu    Network      Address                 Ibytes      Obytes
fxp0   1500   <Link>       00:30:88:00:03:6f     55787738     2053859
fxp0   1500   10.13.49/24  10.13.49.166          55787738     2053859
ipc0   8192   <Link>                           3665494016    77265152
ipc0   8192   127          127.0.2.5           3665494016    77265152
lo0    33228  <Link>                                    0           0
lo0    33228  127          12.0.0.1                     0           0
xcrp   65535  <Link>                                    0           0
lc12   65535  <Link>                                    0           0
```

1.23 show ip mfib

show ip mfib [*group-addr* [*src-addr*]] [**detail**]

1.23.1 Purpose

Displays routes from the IP multicast manager database.

1.23.2 Command Mode

All modes

1.23.3 Syntax Description

group-addr	Optional. IP address of the Internet Group Management Protocol (IGMP) group.
src-addr	Optional. IP address of the multicast source.
detail	Optional. Displays detailed information about IP multicast manager routes.

1.23.4 Default

None

1.23.5 Usage Guidelines

Use the **show ip mfib** command to display routes from the IP multicast manager database.

Note: By default, most **show** commands (in any mode) display information for the current context only or, depending on the command syntax, for all contexts. If you are an administrator for the local context, you can insert the optional **context** *ctx-name* construct, preceding the **show** command, to view output for the specified context without entering that context. For more information about using the **context** *ctx-name* construct, see the **context** command description.

Note: By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information, see "*Modifying Output of show Commands*" in the document, *Using the CLI*.

1.23.6 Examples

The following example displays all routes from the IP multicast manager database. The first route entry (*, 226.0.0.1) is a (*, G) entry. Protocol Independent Multicast (PIM) sent the route to the multicast manager. MFIB_ID provides the multicast route table ID to be programmed into the Packet Processing ASIC (PPA). The "C" flag indicates that this route is a connected multicast route entry. The incoming circuit for the first route entry is invalid. An outgoing interface list provides the outgoing interfaces that exist for the route entry.

```
[local]Redback>show ip mfib


             IP MFIB Routing Table
             Flags: M - MDT group, C - Connected,
             Zp - Dual Join (Primary RPF), Zs - Dual Join(Secondary RPF)
             R - Register, L - Locally connected
             Table version: 6

             (*, 226.0.0.1) [0x200000], Owner:PIM, MFIB_ID:0x10080001 , C
                Incoming circuit: Cct invalid
                Outgoing interface list:
                   255/22:1:26/1/2/5

             (20.2.0.2, 226.0.0.1) [0x200001], Owner:PIM, MFIB_ID:0x10080001 , C
                Incoming circuit: 1/1:511:63:31/1/2/10
                Outgoing interface list:
                   255/22:1:26/1/2/5
```

The following example displays routes from the IP multicast manager database when a port pseudowire is configured.

```
[local]Redback>show ip mfib
```

```
IP MFIB Routing Table
Flags: C - Connected, L - Locally connected, M - MDT group,
       N - RPF monitor, R - Register, X - Learning oif information,
       Zp - Dual Join (Primary RPF), Zs - Dual Join (Secondary RPF)
Table version: 2259

(*, 228.128.28.8) [0x200000], Owner:PIM, MFIB_ID:0x10080001 , C
  Incoming circuit: Cct invalid
  Outgoing interface list:
    255/25:1:2/1/1/41, flags:

(44.37.135.2, 228.128.28.8) [0x200001], Owner:PIM, MFIB_ID:0x10080001
  Incoming circuit: 5/2:511:63:31/1/1/31
  Outgoing interface list:
    255/25:1:2/1/1/41, flags:
```

1.24 show ip mroute

show ip mroute [*group-addr* [*src-addr*]] [**count**]

1.24.1 Purpose

Displays the Protocol Independent Multicast (PIM) routing table.

1.24.2 Command Mode

All modes

1.24.3 Syntax Description

group-addr	Optional. IP address of the Internet Group Management Protocol (IGMP) group.
src-addr	Optional. IP address of the multicast source.
count	Optional. Displays statistics about the group and source, including number of packets, packets per second, average packet size, and bits per second.

1.24.4 Default

None

1.24.5 Usage Guidelines

Use the **`show ip mroute`** command to display the PIM routing table.

Note: By default, most **`show`** commands (in any mode) display information for the current context only or, depending on the command syntax, for all contexts. If you are an administrator for the local context, you can insert the optional **`context`** ***`ctx-name`*** construct, preceding the **`show`** command, to view output for the specified context without entering that context. For more information about using the **`context`** ***`ctx-name`*** construct, see the **`context`** command description.

Note: By appending a space followed by the pipe (|) character at the end of a **`show`** command, you can filter the output using a set of modifier keywords and arguments. For more information, see "*Modifying Output of show Commands*" in the document, *Using the CLI*.

1.24.6 Examples

The following example displays output from the **`show ip mroute`** command when PIM-SSM auto-discovery is enabled:

```
[local]dallas#show ip mroute
IP Multicast Routing Table
Flags: AW(L) - Assert Winner(Loser), C(c) - Connected(RPF), D - Dense,
       E - SSM MDT, F - Register flag, H(h) - Static(RPF),
       J(j) - Join SPT(RPF), K - State war suppressed, L(l) - Local(RPF),
       m - MSDP learned, M - MDT group, N - RPF monitor, P - Pruned,
       r - RMR, R - RP-bit set, S - Sparse, T - SPT-bit set,
       U - Static Join upstream, V(v) - IGMPv3(RPF), Z(z) - Dual Join(RPF),
       . - No forwarding activity
Timers: Uptime/Expires
Interface state: Interface, State, Timers, flags
Table version: 14

(*, 232.90.90.90), 00:01:23/00:02:57, RP: 0.0.0.0, Flags: PM
  Incoming interface: NULL, RPF neighbor: 0.0.0.0, Next join: 00:00:37
  Incoming circuit: Cct invalid
  Outgoing interface list: NULL

(10.0.0.3, 232.90.90.90), 00:01:22/00:02:57, Flags: M
  Incoming interface: ic-vpn2, RPF neighbor: 0.0.0.0
  Incoming circuit: 255/19:1:1/1/1/3
  Outgoing interface list:
    to_P, 12/6:511:63:31/1/1/18, Forward, 00:01:22/00:02:57, sparse

(10.0.0.2, 232.90.90.90), 00:01:23/00:02:06, Flags: E
  Incoming interface: to_P, RPF neighbor: 10.10.10.2
  Incoming circuit: 12/6:511:63:31/1/1/18
  Outgoing interface list:
    ic-vpn2, 255/19:1:1/1/1/3, Forward, 00:01:23/00:02:06, sparse, M
```

The following example displays output from the **`show ip mroute`** command when a port pseudowire is configured:

```
[local]Redback>show ip mroute
IP Multicast Routing Table
Flags: AW(L) - Assert Winner(Loser), C(c) - Connected(RPF), D - Dense,
       E - SSM MDT, F - Register flag, H(h) - Static(RPF),
       J(j) - Join SPT(RPF), K - State war suppressed, L(l) - Local(RPF),
       m - MSDP learned, M - MDT group, N - RPF monitor, P - Pruned,
       r - RMR, R - RP-bit set, S - Sparse, T - SPT-bit set,
       U - Static Join upstream, V(v) - IGMPv3(RPF), Z(z) - Dual Join(RPF),
       . - No forwarding activity
Timers: Uptime/Expires
Interface state: Interface, State, Timers, flags
Table version: 1507

(*, 228.128.28.8), 00:03:23/00:00:06, RP: 70.70.70.70, Flags: SC
  Incoming interface: NULL, RPF neighbor: 0.0.0.0, Next join: 00:00:37
  Incoming circuit: Cct invalid
  Outgoing interface list:
    PPW1, 255/25:1:2/1/1/41, Forward, 00:03:42/00:00:06, sparse, C

(44.37.135.2, 228.128.28.8), 00:01:07/00:02:22, Flags: SC
  Incoming interface: to_se5, RPF neighbor: 19.1.1.2
  Incoming circuit: 5/2:511:63:31/1/1/31
  Outgoing interface list:
    PPW1, 255/25:1:2/1/1/41, Forward, 00:01:07/00:01:54, sparse, C
```

1.25 show ip pool

show ip pool [*name*] [**context** *summary*] [**falling-threshold**]

1.25.1 Purpose

Displays the status of the IP addresses in the specified IP pool, in all IP pools in the specified interface, or in all IP pools in the current context or range.

1.25.2 Command Mode

All modes

1.25.3 Syntax Description

name	Optional. Name of the IP pool or interface for which the status of its IP addresses displays.
context *summary*	Optional. Summary information for all context level IP pool thresholds for the named context.
falling-threshold	Optional. Displays IP pool threshold data for all interfaces in the current context or for the specified interface only.

1.25.4 Default

None

1.25.5 Usage Guidelines

Use the **show ip pool** command to display the status of the IP addresses in the specified IP pool, in all IP pools in the specified interface, or in all IP pools in the current context. The status of the IP addresses includes the number of addresses in use, available, and reserved. Reserved addresses include those used by an interface or the all ones or all zeros address for the interface.

Note: By default, most **show** commands (in any mode) display information for the current context only or, depending on the command syntax, for all contexts. If you are an administrator for the local context, you can insert the optional **context** ***ctx-name*** construct before the **show** command to view output for the specified context without entering that context. For more information about the **context** ***ctx-name*** construct, see the **context** command description.

Note: By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information, see "*Modifying Output of show Commands*" in the document, *Using the CLI*.

1.25.6 Examples

The following example displays status for all IP address pools in the `ip-dial` context, including a range of IP addresses for the `isp1.net` interface:

```
[local]Redback>context ip-dial
```

```
[ip-dial]Redback>show ip pool
```

```
Interface "subscribers-am":
        192.168.1.48     255.255.255.248    0 in use,    5 free, 3 reserved.
Interface "subscribers-mr":
        10.142.119.80    255.255.255.240    0 in use,   13 free, 3 reserved.
Interface "subscribers-sz":
        192.168.2.0      255.255.255.0      0 in use, 253 free, 3 reserved.

Interface "isp1.net":

10.1.1.2        10.1.1.100 0 in use,  99 free,   0 reserved
```

The following example displays the falling threshold data for all IP address pools in the `ip-dial` context:

```
[ip-dial]Redback>show ip pool falling-threshold
```

```
Context "ip-dial": falling-threshold 17 trap log
Interface "subscribers-am":
        192.168.1.48     255.255.255.248  falling-threshold   3 trap
Interface "subscribers-mr":
        10.142.119.80    255.255.255.240  falling-threshold   5 trap log
Interface "subscribers-sz":
        192.168.2.0      255.255.255.0    falling-threshold   33 log
```

The following example displays the status of the IP addresses in the `ip-pool` pool for the `isp1.net` context:

```
[local]Redback>context isp1.net
```

```
[isp1.net]Redback>show ip pool ip-pool
```

```
Interface "isp1.net":
   10.1.1.0        /24  ip-pool 0 in use, 253 free,   3 reserved
```

The following example displays a summary of all contexts in the IP pool for the `isp1.net` context:

```
[local]Redback>show ip pool context summary
falling-threshold absolute     1 759        trap log
falling-threshold percentage   1 98         trap
falling-threshold percentage   2 97         trap log


9         in use, 750       free, 9         reserved
768       total,  97  available percentage
```

1.26 show ip prefix-list

`show ip prefix-list` [*`pl-name`* | **`first-match`** *`pl-name`* *`ip-addr/prefix-length`* | **`summary`** [*`pl-name`*]]

1.26.1 Purpose

Displays information about configured IP prefix lists.

1.26.2 Command Mode

All modes

1.26.3 Syntax Description

`pl-name`	Optional. IP prefix list name.
`first-match`	Optional. Searches for the line in the IP prefix list specified by the *`pl-name`* argument.
`ip-addr/prefix-length`	Specifies the IP address, in the form *`A.B.C.D`*, and the prefix length, separated by the slash (/) character. The range of values for the *`prefix-length`* argument is 0 to 32.
`summary`	Optional. Displays summary information for all configured IP prefix lists.

1.26.4 Default

None

1.26.5 Usage Guidelines

Use the **`show ip prefix-list`** command to display information about configured IP prefix lists.

Note: By default, most **`show`** commands (in any mode) display information for the current context only or, depending on the command syntax, for all contexts. If you are an administrator for the local context, you can insert the optional **`context`** *`ctx-name`* construct, preceding the **`show`** command, to view output for the specified context without entering that context. For more information about using the **`context`** *`ctx-name`* construct, see the **`context`** command description.

Note: By appending a space followed by the pipe (|) character at the end of a **`show`** command, you can filter the output using a set of modifier keywords and arguments. For more information, see “*Modifying Output of show Commands*” in the document, *Using the CLI*.

1.26.6 Examples

The following example displays output from the **show ip prefix-list** command:

```
[local]Redback>show ip prefix-list

ip prefix-list slash9:
 count: 1, sequences: 10 - 10, client count: 1
 modified: 2 day(s), 6 hour(s) ago
   seq 10 permit 17.0.0.0/9  (hit count: 6)

ip prefix-list slash18:
 count: 1, sequences: 10 - 10, client count: 1
 modified: 2 day(s), 6 hour(s) ago
   seq 10 permit 192.28.0.0/18  (hit count: 11)

ip prefix-list /15-deny:
 count: 2, sequences: 10 - 20, client count: 1
 modified: 2 day(s), 6 hour(s) ago
   seq 10 deny 0.0.0.0/0 eq 15  (hit count: 2171)
   seq 20 permit 0.0.0.0/0 le 32  (hit count: 699090)

ip prefix-list 2.0.0.0/8:
 count: 1, sequences: 10 - 10, client count: 1
 modified: 2 day(s), 6 hour(s) ago
   seq 10 permit 2.0.0.0/8  (hit count: 0)
```

```
ip prefix-list /22-permit:
 count: 1, sequences: 10 - 10, client count: 1
 modified: 2 day(s), 6 hour(s) ago
   seq 10 permit 0.0.0.0/0 eq 22  (hit count: 46181)

ip prefix-list deny-slash-13:
 count: 2, sequences: 10 - 20, client count: 0
 modified: 2 day(s), 6 hour(s) ago
   seq 10 deny 139.112.0.0/13  (hit count: 0)
   seq 20 permit 0.0.0.0/0 le 32  (hit count: 0)

ip prefix-list deny-slash-14:
 count: 2, sequences: 10 - 20, client count: 0
 modified: 2 day(s), 6 hour(s) ago
   seq 10 deny 141.40.0.0/14  (hit count: 0)
   seq 20 permit 0.0.0.0/0 ge 1  (hit count: 0)

total ip prefix lists: 7
```

1.27 show ip route

show ip route [*ip-addr* [/*prefix-length* [**longer-prefixes** | **shorter-prefixes**]] [**detail**]

1.27.1 Purpose

Displays information about all IP routes or routes for only the specified IP address or IP prefix.

1.27.2 Command Mode

All modes

1.27.3 Syntax Description

ip-addr	Optional. IP address, in the form *A.B.C.D*, of the route to be displayed.
prefix-length	Optional. Prefix length. The range of values is 0 to 32.
longer-prefixes	Optional. Displays the route and more-specific routes.
shorter-prefixes	Optional. Displays the route and less-specific routes.
detail	Optional. Displays detailed information.

1.27.4 Default

When entered with no keywords or arguments, this command displays all IP routes.

1.27.5 Usage Guidelines

Use the **show ip route** command to display information about all IP routes or for only the specified IP address or IP prefix.

Note: By default, most **show** commands (in any mode) display information for the current context only or, depending on the command syntax, for all contexts. If you are an administrator for the local context, you can insert the optional **context** *ctx-name* construct, preceding the **show** command, to view output for the specified context without entering that context. For more information about using the **context** *ctx-name* construct, see the **context** command description.

Note: By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information, see “*Modifying Output of show Commands*” in the document, *Using the CLI*.

1.27.6 Examples

The following example displays output from the **show ip route** command:

```
[local]Redback>show ip route

Codes: C - connected, S - static, S dv - dvsr, R - RIP, e B - EBGP, i B - IBGP
       O   - OSPF, IA - OSPF inter area, N1  - OSPF NSSA external type 1
       N2  - OSPF NSSA external type 2,  E1  - OSPF external type 1
       E2  - OSPF external type 2
       i   - IS-IS, L1 - IS-IS level-1,  L2  - IS-IS level-2
       >   - Active Route

Gateway of last resort is 155.53.39.254 to network 0.0.0.0

Type    Network             Next Hop        Dist  Metric    UpTime  Interface

> S dv  0.0.0.0/0           155.53.39.254      1       0  00:00:36  op-net-lan
> S dv  100.100.0.0/16      155.53.39.254      1       0  00:00:31  op-net-lan
> C     155.53.32.0/21                         0       0  00:01:09  op-net-lan
> S     200.200.0.0/16                       255       0     1d02h  null0
```

The following example displays information for the IP route, `4.4.4.0/24`:

```
[local]Redback>show ip route 4.4.4.0/24

   Best match Routing entry for 4.4.4.0/24 is 4.4.4.0/24 , version 8
   Route Uptime 01:19:17
   Paths: total 1, best path count 1

   Route has been downloaded to following slots
    04/0

   Path information :

     Active path :
     Known via bgp 2, type-External BGP, distance 20, metric 0,
     Tag 0, Originating AS # : 1, Next-hop 20.1.1.1, NH-ID 0x31100003, Interface eth42
     Circuit 4/2:2047:31/1/2/6
     dscp ef
```

1.28 show ip route all

`show ip route all`

1.28.1 Purpose

Displays information about all IP routes.

1.28.2 Command Mode

All modes

1.28.3 Syntax Description

This command has no keywords or arguments.

1.28.4 Default

None

1.28.5 Usage Guidelines

Use the **`show ip route all`** command to display information about all IP routes.

Note: By default, most **`show`** commands (in any mode) display information for the current context only or, depending on the command syntax, for all contexts. If you are an administrator for the local context, you can insert the optional **`context`** ***`ctx-name`*** construct, preceding the **`show`** command, to view output for the specified context without entering that context. For more information about using the **`context`** ***`ctx-name`*** construct, see the **`context`** command description.

Note: By appending a space followed by the pipe (|) character at the end of a **`show`** command, you can filter the output using a set of modifier keywords and arguments. For more information, see “*Modifying Output of show Commands*” in the document, *Using the CLI*.

1.28.6 Examples

The following example displays output from the **show ip route all** command:

```
[local]Redback>show ip route all

Codes: C - connected, S - static, S dv - dvsr, R - RIP, e B - EBGP, i B - IBGP
       A,H - derived hidden
       O   - OSPF, IA - OSPF inter area, N1  - OSPF NSSA external type 1
       N2  - OSPF NSSA external type 2,  E1  - OSPF external type 1
       E2  - OSPF external type 2
       i   - IS-IS, L1 - IS-IS level-1,  L2  - IS-IS level-2
       >   - Active Route
Type   Network           Next Hop         Dist   Metric     UpTime    Interface
> S    0.0.0.0/0         10.13.49.254        1         0   00:00:20   mgmt
> R    1.1.1.0/24        100.1.1.1           1         0   00:00:03   five
> R    1.1.2.0/24        100.1.1.1           1         0   00:00:03   five
> R    1.1.3.0/24        100.1.1.1           1         0   00:00:03   five
> R    1.1.4.0/24        100.1.1.1           1         0   00:00:03   five
> R    1.1.5.0/24        100.1.1.1           1         0   00:00:03   five
> S    5.6.7.8/32                            211       0   00:00:20   null0
> C    10.1.7.0/24                           0         0   00:00:20   seven
> C H  10.1.7.0/32                           0         0   00:00:20   Local host
> C H  10.1.7.255/32                         0         0   00:00:20   Local host
> C    10.1.10.0/24                          0         0   00:00:20   ten
> C H  10.1.10.0/32                          0         0   00:00:20   Local host
> C H  10.1.10.255/32                        0         0   00:00:20   Local host
> C    10.13.49.0/24                         0         0   00:00:20   mgmt
> C H  10.13.49.0/32                         0         0   00:00:20   Local host
> C H  10.13.49.158/32                       0         0   00:00:20   Local host
> A H  10.13.49.254/3    10.13.49.254        254       0   00:00:20   mgmt
> C H  10.13.49.255/32                       0         0   00:00:20   Local host
> A H  100.1.1.1/32      100.1.1.1           254       0   00:00:03   five
```

1.29 show ip route bgp

show ip route bgp

1.29.1 Purpose

Displays information about Border Gateway Protocol (BGP) routes.

1.29.2 Command Mode

All modes

1.29.3 Syntax Description

This command has no keywords or arguments.

1.29.4 Default

None

1.29.5 Usage Guidelines

Use the **show ip route bgp** command to display information about BGP routes.

Note: By default, most **show** commands (in any mode) display information for the current context only or, depending on the command syntax, for all contexts. If you are an administrator for the local context, you can insert the optional **context** ***ctx-name*** construct, preceding the **show** command, to view output for the specified context without entering that context. For more information about using the **context** ***ctx-name*** construct, see the **context** command description.

Note: By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information, see the "*Modifying Output of show Commands*" in the document, *Using the CLI*.

1.29.6 Examples

The following example displays information about BGP routes:

```
[local]Redback>show ip route bgp

Codes: C - connected, S - static, S dv - dvsr, R - RIP, e B - EBGP, i B - IBGP
       A,H - derived hidden
       O    - OSPF, IA - OSPF inter area, N1  - OSPF NSSA external type 1
       N2  - OSPF NSSA external type 2,  E1  - OSPF external type 1
       E2  - OSPF external type 2
       i    - IS-IS, L1 - IS-IS level-1,  L2  - IS-IS level-2
       >    - Active Route

Type    Network            Next Hop         Dist   Metric     UpTime   Interface
> e B   3.0.0.0/8          155.53.1.235       20        0      1d14h
> e B   4.0.0.0/8          155.53.1.235       20        0   22:17:18
> e B   4.21.132.0/23      155.53.0.1         20        0   22:21:03
> e B   6.1.0.0/16         155.53.1.235       20        0       1w1d
> e B   6.2.0.0/22         155.53.0.1         20        0   22:21:03
> e B   6.3.0.0/18         155.53.1.235       20        0       1w1d
```

1.30 show ip route client

show ip route client [*client-id*]

1.30.1 Purpose

Displays information about Routing Information Base (RIB) clients.

1.30.2 Command Mode

All modes

1.30.3 Syntax Description

client-id	Optional. Client ID for which RIB client information is displayed. The range of values is 0 to 256.

1.30.4 Default

None

1.30.5 Usage Guidelines

Use the **show ip route client** command to display information about RIB clients.

Note: By default, most **show** commands (in any mode) display information for the current context only or, depending on the command syntax, for all contexts. If you are an administrator for the local context, you can insert the optional **context** *ctx-name* construct, preceding the **show** command, to view output for the specified context without entering that context. For more information about using the **context** *ctx-name* construct, see the **context** command description.

Note: By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information, see the "*Modifying Output of show Commands*" in the document, *Using the CLI*.

1.30.6 Examples

The following example displays information about RIB clients:

```
[local]Redback>show ip route client
```

```
Rt Tbl Version:      1820518, Nh Tbl Version: 9453
Protocol(ids)        Tot Routes   InQ  OutQ   Redist Ver  State    Ref
connected  (1/0)             11     0     0            0  Reg UP     0
adjacency  (2/0)              0     0     0            0  Reg UP     0
static  (3/0)                14     0     0            0  Reg UP     0
isis A2-wtn  (4/0)           45     0     0            0  Reg UP     0
isis new  (5/0)               0     0     0            0  Reg UP     0
bgp 64001  (6/0)         101560     0     0            0  Reg UP     0
```

1.31 show ip route connected

```
show ip route connected
```

1.31.1 Purpose

Displays information about IP routes from directly connected networks.

1.31.2 Command Mode

All modes

1.31.3 Syntax Description

This command has no keywords or arguments.

1.31.4 Default

None

1.31.5 Usage Guidelines

Use the **show ip route connected** command to display information about IP routes from directly connected networks.

Note: By default, most **show** commands (in any mode) display information for the current context only or, depending on the command syntax, for all contexts. If you are an administrator for the local context, you can insert the optional **context** ***ctx-name*** construct, preceding the **show** command, to view output for the specified context without entering that context. For more information about using the **context** ***ctx-name*** construct, see the **context** command description.

Note: By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information, see "*Modifying Output of show Commands*" in the document, *Using the CLI*.

1.31.6 Examples

The following example displays information about IP routes from directly connected networks:

```
[local]Redback>show ip route connected

Codes: C - connected, S - static, S dv - dvsr, R - RIP, e B - EBGP, i B - IBGP
       A,H - derived hidden
       O   - OSPF, IA - OSPF inter area, N1  - OSPF NSSA external type 1
       N2  - OSPF NSSA external type 2,  E1  - OSPF external type 1
       E2  - OSPF external type 2
       i   - IS-IS, L1 - IS-IS level-1,  L2  - IS-IS level-2
       >   - Active Route

Type    Network            Next Hop         Dist  Metric    UpTime  Interface
> C     10.12.208.0/21                         0       0      1w4d  redback
> C H   10.12.208.0/32                         0       0      1w4d  Local host
> C H   10.12.208.79/32                        0       0      1w4d  Local host
> C H   10.12.215.255/32                       0       0      1w4d  Local host
> C     10.100.1.5/32                          0       0      1w4d  lo1
> C     10.100.11.8/29                         0       0      1w4d  1/1
```

1.32 show ip route fib-client

show ip route fib-client [*client-id*]

1.32.1 Purpose

Displays information about Forwarding Information Base (FIB) clients.

1.32.2 Command Mode

All modes

1.32.3 Syntax Description

client-id	Optional. Client ID for which FIB client information is displayed. The range of values is 0 to 256.

1.32.4 Default

None

1.32.5 Usage Guidelines

Use the **show ip route fib-client** command to display information about FIB clients.

Note: By default, most **show** commands (in any mode) display information for the current context only or, depending on the command syntax, for all contexts. If you are an administrator for the local context, you can insert the optional **context** *ctx-name* construct, preceding the **show** command, to view output for the specified context without entering that context. For more information about using the **context** *ctx-name* construct, see the **context** command description.

Note: By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information, see “*Modifying Output of show Commands*” in the document, *Using the CLI*.

1.32.6 Examples

The following example displays information about FIB clients:

```
[local]Redback>show ip route fib-client
```

```
Route table version 27113/778
    Total route for FIB 19937

Slot Name             State  OutQ   MsgSent  Version
FIB SLOT 02/0(0)      Up        0      1612  27113/778
FIB SLOT 02/1(1)      Up        0         1  0/778
FIB SLOT 10/0(2)      Up        0      1612  27113/778
FIB SLOT 10/1(3)      Up        0       184  0/778
```

1.33 show ip route hidden

`show ip route hidden`

1.33.1 Purpose

Displays information about hidden IP routes; that is, routes that are added internally.

1.33.2 Command Mode

All modes

1.33.3 Syntax Description

This command has no keywords or arguments.

1.33.4 Default

None

1.33.5 Usage Guidelines

Use the **`show ip route hidden`** command to display information about hidden IP routes.

Note: By default, most **`show`** commands (in any mode) display information for the current context only or, depending on the command syntax, for all contexts. If you are an administrator for the local context, you can insert the optional **`context`** ***`ctx-name`*** construct, preceding the **`show`** command, to view output for the specified context without entering that context. For more information about using the **`context`** ***`ctx-name`*** construct, see the **`context`** command description.

Note: By appending a space followed by the pipe (|) character at the end of a **`show`** command, you can filter the output using a set of modifier keywords and arguments. For more information, see "*Modifying Output of show Commands*" in the document, *Using the CLI*.

1.33.6 Examples

The following example displays information about hidden IP routes:

```
[local]Redback>show ip route hidden

Codes: C - connected, S - static, S dv - dvsr, R - RIP, e B - EBGP, i B - IBGP
       A,H - derived hidden
       O   - OSPF, IA - OSPF inter area, N1  - OSPF NSSA external type 1
       N2  - OSPF NSSA external type 2,  E1  - OSPF external type 1
       E2  - OSPF external type 2
       i   - IS-IS, L1 - IS-IS level-1,  L2  - IS-IS level-2
       >   - Active Route

Type    Network             Next Hop        Dist  Metric    UpTime  Interface
> C H   10.12.192.0/32                         0       0  05:23:19  Local host
> A H   10.12.192.1/32      10.12.192.1      254       0  05:25:44  mgmt
> C H   10.12.192.73/32                        0       0  05:23:19  Local host
> C H   10.12.199.255/32                       0       0  05:23:19  Local host
> C H   10.12.208.0/32                         0       0  05:25:56  Local host
> A H   10.12.208.1/32      10.12.208.1      254       0  05:25:44  lab
```

1.34 show ip route iphost

show ip route iphost

1.34.1 Purpose

Displays the IP hosts that are in an "up" state for all interfaces bound to a port or permanent virtual circuit (PVC).

1.34.2 Command Mode

All modes

1.34.3 Syntax Description

This command has no keywords or arguments.

1.34.4 Default

None

1.34.5 Usage Guidelines

Use the **show ip route iphost** command to display the IP hosts that are in an "up" state for all interfaces bound to a port or PVC. (This command does not show any IP hosts that are in a "down" state.) IP hosts are remote endpoints configured locally and connected physically to the port or PVC where they are configured. To configure an IP host, use the **ip host** command.

Note: By default, most **show** commands (in any mode) display information for the current context only or, depending on the command syntax, for all contexts. If you are an administrator for the local context, you can insert the optional **context** ***ctx-name*** construct, preceding the **show** command, to view output for the specified context without entering that context. For more information about using the **context** ***ctx-name*** construct, see the **context** command description.

Note: By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information, see “*Modifying Output of show Commands*” in *Using the CLI*.

1.34.6 Examples

The following example displays output from the **show ip route iphost** command. The entries with the **IPH** prefix are IP hosts manually defined using the **ip host** command.

```
[local]Redback>show ip route iphost

Codes: C - connected, S - static, S dv - dvsr, R - RIP, e B - EBGP, i B - IBGP
        A,H - derived hidden
        O   - OSPF, O3  - OSPFv3, IA - OSPF(v3) inter-area,
        N1  - OSPF(v3) NSSA external type 1, N2  - OSPF(v3) NSSA external type 2
        E1  - OSPF(v3) external type 1, E2  - OSPF(v3) external type 2
        i   - IS-IS, L1 - IS-IS level-1,  L2  - IS-IS level-2, N - NAT
        IPH - IP Host, SUB A - Subscriber address, SUB S - Subscriber static
        M F - Mobile Sub Foreign Agent, M H - Mobile Sub Home Agent
        A - Derived Default, MeH - Media Nexthop
        >   - Active Route, * - LSP

Type    Network             Next Hop        Dist  Metric    UpTime  Interface
 > IPH   100.0.0.4/32        100.0.0.4         16       0  00:10:43  ift1
 > IPH   100.0.0.10/32       100.0.0.10        16       0  00:10:43  ift1
 > IPH   200.0.0.20/32       200.0.0.20        16       0  00:04:11  ift2
 > IPH   200.0.0.30/32       200.0.0.30        16       0  00:04:11  ift2
 > IPH   200.0.0.40/32       200.0.0.40        16       0  00:02:24  ift2
```

1.35 show ip route isis

`show ip route isis`

1.35.1 Purpose

Displays information about Intermediate System-to-Intermediate System (IS-IS) routes.

1.35.2 Command Mode

All modes

1.35.3 Syntax Description

This command has no keywords or arguments.

1.35.4 Default

None

1.35.5 Usage Guidelines

Use the **`show ip route isis`** command to display information about IS-IS routes.

Note: By default, most **`show`** commands (in any mode) display information for the current context only or, depending on the command syntax, for all contexts. If you are an administrator for the local context, you can insert the optional **`context`** ***`ctx-name`*** construct, preceding the **`show`** command, to view output for the specified context without entering that context. For more information about using the **`context`** ***`ctx-name`*** construct, see the **`context`** command description.

Note: By appending a space followed by the pipe (|) character at the end of a **`show`** command, you can filter the output using a set of modifier keywords and arguments. For more information, see *Modifying Output of show Commands* in the document *Using the CLI*. For information about troubleshooting IS-IS, see *Troubleshooting IS-IS*.

1.35.6 Examples

The following example displays information about IS-IS routes:

```
[local]Redback>show ip route isis

Codes: C - connected, S - static, S dv - dvsr, R - RIP, e B - EBGP, i B - IBGP
       A,H - derived hidden
       O   - OSPF, IA - OSPF inter area, N1  - OSPF NSSA external type 1
       N2  - OSPF NSSA external type 2,  E1  - OSPF external type 1
       E2  - OSPF external type 2
       i   - IS-IS, L1 - IS-IS level-1,  L2  - IS-IS level-2
       >   - Active Route

Type    Network             Next Hop         Dist  Metric    UpTime  Interface
> i L1  10.100.1.3/32       10.100.11.25      115       12       1w1d  2/1
> i L1  10.100.1.5/32       10.100.11.27      115       13   20:46:52  2/1
> i L1  10.100.1.102/32     10.100.11.25      115       40   20:46:52  2/1
>                           10.100.11.27                             2/1
> i L1  10.100.11.8/29      10.100.11.27      115       22   20:46:52  2/1
> i L1  10.100.11.32/29     10.100.11.25      115       39       1w1d  2/1
```

1.36 show ip route martian

show ip route martian

1.36.1 Purpose

Displays information about IP martian routes.

1.36.2 Command Mode

All modes

1.36.3 Syntax Description

This command has no keywords or arguments.

1.36.4 Default

None

1.36.5 Usage Guidelines

Use the **show ip route martian** command to display information about IP martian routes.

Note: By default, most **show** commands (in any mode) display information for the current context only or, depending on the command syntax, for all contexts. If you are an administrator for the local context, you can insert the optional **context** ***ctx-name*** construct, preceding the **show** command, to view output for the specified context without entering that context. For more information about using the **context** ***ctx-name*** construct, see the **context** command description.

Note: By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information, see "*Modifying Output of show Commands*" in the document, *Using the CLI*.

1.36.6 Examples

The following example displays information about IP martian routes:

```
[local]Redback>show ip route martian
```

```
  0.0.0.0/8         orlonger   --  disallowed
127.0.0.0/8         orlonger   --  disallowed
```

1.37 show ip route mobile-ip

show ip route mobile-ip [**foreign-agent** | **home-agent**]

1.37.1 Purpose

Displays IP routes for mobile nodes for an foreign-agent (FA) instance or home-agent (HA) instance.

1.37.2 Command Mode

All modes

1.37.3 Syntax Description

foreign-agent	Displays IP route information for an FA instance.
home-agent	Displays IP route information for a HA instance.

1.37.4 Default

None

1.37.5 Usage Guidelines

Use the **show ip route mobile-ip** command to display IP routes for an foreign-agent (FA) instance or home-agent (HA) instance.

To see a summary of IP routes, use the **show ip route** command (in any mode) with the **summary** keyword.

Note: By default, most **show** commands (in any mode) display information for the current context only or, depending on the command syntax, for all contexts. If you are an administrator for the local context, you can insert the optional **context** ***ctx-name*** construct, preceding the **show** command, to view output for the specified context without entering that context. For more information about using the **context** ***ctx-name*** construct, see the **context** command description.

Note: By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information, see "*Modifying Output of show Commands*" in the document, *Using the CLI*.

1.37.6 Examples

The following example shows how to display IP routes for an HA instance:

```
[local]Redback>show ip route mobile-ip home-agent
Codes: C - connected, S - static, S dv - dvsr, R - RIP, e B - EBGP, i B
- IBGP
       A,H - derived hidden
       O - OSPF, O3  - OSPFv3, IA - OSPF(v3) inter-area,
       N1 - OSPF(v3) NSSA external type 1, N2  - OSPF(v3) NSSA external type 2
       E1 - OSPF(v3) external type 1, E2 - OSPF(v3) external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, N - NAT
       IPH - IP Host, SUB A - Subscriber address, SUB S - Subscriber static
       MIP F - Mobile-IP Foreign Agent, MIP H - Mobile-IP Home Agent
       A - Derived Default, MH - Media Nexthop
       > - Active Route, * - LSP

Type       Network             Next Hop    Dist     Metric       UpTime
Interface  SUB A 16.1.1.1/32   16.1.1.1    15         0  02:51:03  mip1
```

1.38 show ip route multicast

show ip route multicast [*ip-addr*[/*prefix-length*]] [**bgp**] [**isis**] [**martian**] [**next-hop**] [**static**] [**summary**]

1.38.1 Purpose

Displays all unicast-dependent multicast routing table information.

1.38.2 Command Mode

All modes

1.38.3 Syntax Description

ip-addr	Optional. IP address, in the form *A.B.C.D*, of the route to be displayed.
prefix-length	Optional. Prefix length. The range of values is 0 to 32.
bgp	Optional. Displays Border Gateway Protocol (BGP) routing information.
isis	Optional. Displays Intermediate System-to-Intermediate System (IS-IS) routing information.
martian	Optional. Displays configured Martian Networks information.
next-hop	Optional. Displays next-hop information.
static	Optional. Displays static route information.
summary	Optional. Displays summary information for all routes.

1.38.4 Default

None

1.38.5 Usage Guidelines

Use the **show ip route multicast** command to display all unicast-dependent multicast routing table information.

Note: By default, most **show** commands (in any mode) display information for the current context only or, depending on the command syntax, for all contexts. If you are an administrator for the local context, you can insert the optional **context** *ctx-name* construct, preceding the **show** command, to view output for the specified context without entering that context. For more information about using the **context** *ctx-name* construct, see the **context** command description.

Note: By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information, see "*Modifying Output of show Commands*" in the document, *Using the CLI*.

1.38.6 Examples

The following example displays output from the **show ip route multicast** command issued on a router configured with three BGP multicast routes and two `mstatic` routes:

```
[local]Redback>show ip route multicast

Codes: e MB - Multicast EBGP, i MB - Multicast IBGP, S - mstatic
       >    - Active Route

Type    Network         Next Hop      Dist  Metric    UpTime  Interface
> S     1.1.1.1/32      10.200.1.1       1       0  00:07:46
> e B   11.1.1.0/24     10.200.1.1      20       0  00:03:46
> i B   103.1.1.0/24    10.200.1.3     200       0  00:08:52
> i B   105.1.1.0/24    10.200.1.3     200       0  00:08:52
> S     192.64.1.0/24   10.200.1.1       1       0  00:07:46
```

1.39 show ip route next-hop

show ip route next-hop [*next-hop-id* | *next-hop-ip-addr*] [**detail**]

1.39.1 Purpose

Displays information about IP route next hops.

1.39.2 Command Mode

All modes

1.39.3 Syntax Description

next-hop-id	Optional. Next-hop ID in hexadecimal format. The range of values is 0x0 to 0xffffffff.
next-hop-ip-addr	Optional. Next-hop IP address.
detail	Optional. Displays detailed information.

1.39.4 Default

None

1.39.5 Usage Guidelines

Use the **show ip route next-hop** command to display information about IP route next hops.

Note: By default, most **show** commands (in any mode) display information for the current context only or, depending on the command syntax, for all contexts. If you are an administrator for the local context, you can insert the optional **context** *ctx-name* construct, preceding the **show** command, to view output for the specified context without entering that context. For more information about using the **context** *ctx-name* construct, see the **context** command description.

Note: By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information, see "*Modifying Output of show Commands*" in the document, *Using the CLI*.

1.39.6 Examples

The following example displays summary information about all IP route next hops:

```
[local]Redback>show ip route next-hop

** = Via interface
    Next Hop Tbl Version :        778
    Current Next Hops    :         41

NH-ID                 Ref Cnt   NH-IP             Via-NH     Interface
0x30D00002               47/0                                Local host
0x31100001                1/0                                test
0x31100002                1/0                                lab
0x31100003                1/0   10.12.208.81                 lab
0x31100004                1/0   10.12.210.27                 lab
0x31100005                2/2   10.12.208.1                  lab
0x31100006                2/0   10.12.192.1                  mgmt
0x31100007                1/0   10.12.208.170                lab
```

The following example displays detailed information about the IP route next hop, `0x31100001`:

```
[local]Redback>show ip route next-hop 0x31100001 detail

    ** = Via interface
    Next Hop Tbl Version :          5
    Current Next Hops    :          4

NH-ID                 Ref Cnt NH-IP           Via-NH     Interface

0x31100001                1/0                            test
Adj-id         : 0xFF400008
Info-Version   : 5                   Node-Version   : 5
Fib Card bits  : 0x100010            Nh Client bits : 0x0
Info flags     : 0x1                 Lsp ifgrid     : 0x0
Spg-id         : 0x1
IF-GRID        : 0x10000001
Circuit id     : 255/22:1:26/1/1/4


Next-hop has been downloaded to following slots  05/0, 05/1
```

1.40 show ip route ospf

show ip route ospf

1.40.1 Purpose

Displays information about Open Shortest Path First (OSPF) routes.

1.40.2 Command Mode

All modes

1.40.3 Syntax Description

This command has no keywords or arguments.

1.40.4 Default

None

1.40.5 Usage Guidelines

Use the **show ip route ospf** command to display information about OSPF routes.

Note: By default, most **show** commands (in any mode) display information for the current context only or, depending on the command syntax, for all contexts. If you are an administrator for the local context, you can insert the optional **context** ***ctx-name*** construct, preceding the **show** command, to view output for the specified context without entering that context. For more information about using the **context** ***ctx-name*** construct, see the **context** command description.

Note: By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information, see "*Modifying Output of show Commands*" in the document, *Using the CLI*.

1.40.6 Examples

The following example displays information about OSPF routes:

```
[local]Redback>show ip route ospf

Codes: C - connected, S - static, S dv - dvsr, R - RIP, e B - EBGP, i B - IBGP
       A,H - derived hidden
       O   - OSPF, IA - OSPF inter area, N1  - OSPF NSSA external type 1
       N2  - OSPF NSSA external type 2,  E1  - OSPF external type 1
       E2  - OSPF external type 2
       i   - IS-IS, L1 - IS-IS level-1,  L2  - IS-IS level-2
       >   - Active Route

Type    Network             Next Hop         Dist   Metric   UpTime   Interface
> O     10.100.1.102/32     10.100.11.50     110         2     1w4d   fa3/1
  O     10.100.11.8/29      10.100.11.10     110         1            1/1
  O     10.100.11.24/29     10.100.11.27     110         1            2/1
> O     10.100.11.32/29     10.100.11.50     110         2     1w4d   fa3/1
  O     10.100.11.48/29     10.100.11.49     110         1            fa3/1
```

1.41 show ip route registered

show ip route registered {**next-hop** | **prefix**}

1.41.1 Purpose

Displays next-hop or prefix information registered in the Routing Information Base (RIB).

1.41.2 Command Mode

All modes

1.41.3 Syntax Description

next-hop	Displays RIB-registered next-hop information.
prefix	Displays RIB-registered prefix information.

1.41.4 Default

None

1.41.5 Usage Guidelines

Use the **show ip route registered** command to display next-hop or prefix information registered in the RIB.

Note: Bidirectional Forwarding Detection (BFD) information is displayed in the **show ip route registered** command output only when there are active BFD clients (routing protocols that have BFD enabled).

Note: By default, most **show** commands (in any mode) display information for the current context only or, depending on the command syntax, for all contexts. If you are an administrator for the local context, you can insert the optional **context** ***ctx-name*** construct, preceding the **show** command, to view output for the specified context without entering that context. For more information about using the **context** ***ctx-name*** construct, see the **context** command description.

Note: By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information, see "*Modifying Output of show Commands*" in the document, *Using the CLI*.

1.41.6 Examples

The following example displays next-hop information registered in the RIB:

```
[local]Redback>show ip route registered next-hop

Next-hop:           Registered Client(s):

1.1.1.2             bgp 1
BFD Clients    : bgp
Query flags    : 0x40             Version        : 0x0
Adj-id         : 0xFFFFFFFF       Conn Adj-id    : 0xFFFFFFFF
NH Magic       : 0x1000400        Default flag   : 0x0
Protocol       : 0x1              IGP Metric     : 0
Conn IF-GRID   : 0x10000001       Conn cct id    : 255/11:1023:63/1/2/5
IGP IF-GRID    : 0x10000001       IGP cct id     : 255/11:1023:63/1/2/5
Reslov cntxt   : 0x40080001       IGP MTU        : 1500
IGP first hop  : 0.0.0.0          IGP next hop   : 0.0.0.0
slot 1: 2 constituent circuits
```

The following example displays prefix information registered in the RIB:

```
[local]Redback>show ip route registered prefix

Prefix:             Registered Client(s):

1.1.1.0/24          ldp
Verion         : 0x1                Lookup type    : 0x2
Return pfx ver : 0x1C               Return pfx     : 1.1.1.0/24
Default flag   : 0x0

10.12.49.0/24       ldp
Verion         : 0x2                Lookup type    : 0x2
Return pfx ver : 0x1                Return pfx     : 10.12.49.0/24
Default flag   : 0x0
```

1.42 show ip route rip

show ip route rip

1.42.1 Purpose

Displays information about Routing Information Protocol (RIP) routes.

1.42.2 Command Mode

All modes

1.42.3 Syntax Description

This command has no keywords or arguments.

1.42.4 Default

None

1.42.5 Usage Guidelines

Use the **show ip route rip** command to display information about RIP routes.

Note: By default, most **show** commands (in any mode) display information for the current context only or, depending on the command syntax, for all contexts. If you are an administrator for the local context, you can insert the optional **context** ***ctx-name*** construct, preceding the **show** command, to view output for the specified context without entering that context. For more information about using the **context** ***ctx-name*** construct, see the **context** command description.

Note: By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information, see "*Modifying Output of show Commands*" in the document, *Using the CLI*.

1.42.6 Examples

The following example displays information about RIP routes:

```
[local]Redback>show ip route rip
```

```
Codes: C - connected, S - static, S dv - dvsr, R - RIP, e B - EBGP, i B - IBGP
       A,H - derived hidden
       O   - OSPF, IA - OSPF inter area, N1  - OSPF NSSA external type 1
       N2  - OSPF NSSA external type 2,  E1  - OSPF external type 1
       E2  - OSPF external type 2
       i   - IS-IS, L1 - IS-IS level-1,  L2  - IS-IS level-2
       >   - Active Route

Start loop Old index =0xa4
Type    Network             Next Hop        Dist  Metric    UpTime  Interface
> R     1.1.1.0/24          100.1.1.1          1       0  00:21:58  five
> R     1.1.2.0/24          100.1.1.1          1       0  00:21:58  five
> R     1.1.3.0/24          100.1.1.1          1       0  00:21:58  five
```

1.43 show ip route static

show ip route static

1.43.1 Purpose

Displays information about static IP routes.

1.43.2 Command Mode

All modes

1.43.3 Syntax Description

This command has no keywords or arguments.

1.43.4 Default

None

1.43.5 Usage Guidelines

Use the **show ip route static** command to display information about static IP routes.

Note: By default, most **show** commands (in any mode) display information for the current context only or, depending on the command syntax, for all contexts. If you are an administrator for the local context, you can insert the optional **context** ***ctx-name*** construct, preceding the **show** command, to view output for the specified context without entering that context. For more information about using the **context** ***ctx-name*** construct, see the **context** command description.

Note: By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information, see "*Modifying Output of show Commands*" in the document, *Using the CLI*.

1.43.6 Examples

The following example displays information about static IP routes:

```
[local]Redback>show ip route static

Codes: C - connected, S - static, S dv - dvsr, R - RIP, e B - EBGP, i B - IBGP
       A,H - derived hidden
       O   - OSPF, IA - OSPF inter area, N1  - OSPF NSSA external type 1
       N2  - OSPF NSSA external type 2,  E1  - OSPF external type 1
       E2  - OSPF external type 2
       i   - IS-IS, L1 - IS-IS level-1,  L2  - IS-IS level-2
       >   - Active Route

Type    Network             Next Hop        Dist  Metric     UpTime    Interface
> S     10.89.0.0/16                           1       0   05:28:55    null0
> S     10.89.89.0/24                          1       0   05:28:55    null0
> S     155.53.0.0/16       10.12.208.1        1       0   05:28:43    lab
> S     155.53.32.55/32     10.12.192.1        1       0   05:28:43    mgmt
> S dv  100.100.0.0/16      155.53.39.254      1       0   05:27:56    op-net-lan
```

1.44 show ip route subscriber

show ip route subscriber [**address** | **static** | **aggregate**]

1.44.1 Purpose

Displays information about all subscriber routes.

1.44.2 Command Mode

All modes

1.44.3 Syntax Description

`address`	Optional. Displays only subscriber address route information.
`static`	Optional. Displays only subscriber static route information.
`aggregate`	Optional. Displays only subscriber route information.

1.44.4 Default

When entered with no keywords, this command displays all subscriber routes.

1.44.5 Usage Guidelines

Use the **show ip route subscriber** command to display information about all subscriber routes.

Note: By default, most **show** commands (in any mode) display information for the current context only or, depending on the command syntax, for all contexts. If you are an administrator for the local context, you can insert the optional **context** *ctx-name* construct, preceding the **show** command, to view output for the specified context without entering that context. For more information about using the **context** *ctx-name* construct, see the **context** command description.

Note: By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information, see "*Modifying Output of show Commands*" in the document, *Using the CLI*.

1.44.6 Examples

The following example displays output from the **show ip route subscriber** command:

```
[local]Redback>show ip route subscriber
Codes: C - connected, S - static, S dv - dvsr, R - RIP, e B - EBGP, i B - IBGP
       O   - OSPF, O3  - OSPFv3, IA - OSPF(v3) inter-area,
       N1  - OSPF(v3) NSSA external type 1, N2  - OSPF(v3) NSSA external type 2
       E1  - OSPF(v3) external type 1, E2  - OSPF(v3) external type 2
       i   - IS-IS, L1 - IS-IS level-1,  L2  - IS-IS level-2, N - NAT
       IPH - IP Host, SUB A - Subscriber address, SUB S - Subscriber static
       SUB P - AAA downloaded aggregate subscriber routes
       A - Derived Default, MeH - Media Nexthop
       >   - Active Route, * - LSP
```

The following example displays output from the **show ip route subscriber address** command:

```
[local]Redback>show ip route subscriber address

Codes: C - connected, S - static, S dv - dvsr, R - RIP, e B - EBGP, i B - IBGP
       A,H - derived hidden
       O   - OSPF, IA - OSPF inter area, N1  - OSPF NSSA external type 1
       N2  - OSPF NSSA external type 2,  E1  - OSPF external type 1
       E2  - OSPF external type 2
       i   - IS-IS, L1 - IS-IS level-1,  L2  - IS-IS level-2
       IPH - IP Host, SUB A - Subscriber address, SUB S - Subscriber static
       A - Derived Default
       >   - Active Route

Type    Network             Next Hop        Dist  Metric    UpTime  Interface
> SUB A 20.1.1.2/32         20.1.1.2          15       0  00:01:40  to-dhcpclient
```

The following example displays output from the **show ip route subscriber static** command:

```
[local]Redback>show ip route subscriber static


Codes: C - connected, S - static, S dv - dvsr, R - RIP, e B - EBGP, i B - IBGP

       A,H - derived hidden

       O   - OSPF, IA - OSPF inter area, N1  - OSPF NSSA external type 1

       N2  - OSPF NSSA external type 2,  E1  - OSPF external type 1

       E2  - OSPF external type 2

       i   - IS-IS, L1 - IS-IS level-1,  L2  - IS-IS level-2

       IPH - IP Host, SUB A - Subscriber address, SUB S - Subscriber static

       A - Derived Default

       >   - Active Route


Type    Network             Next Hop        Dist  Metric    UpTime  Interface

> SUB S 30.1.1.0/24         20.1.1.2          17       0  00:02:01  to-dhcpclient
```

The following example displays output from the **`show ip route subscriber aggregate`** command. In this command, `SUB P` entries indicates AAA downloaded aggregate subscriber routes:

```
[local]Redback>show ip route subscriber aggregate

Codes: C - connected, S - static, S dv - dvsr, R - RIP, e B - EBGP, i B - IBGP
       A,H - derived hidden
       O   - OSPF, O3   - OSPFv3, IA - OSPF(v3) inter-area,
       N1  - OSPF(v3) NSSA external type 1, N2  - OSPF(v3) NSSA external type 2
       E1  - OSPF(v3) external type 1, E2  - OSPF(v3) external type 2
       i   - IS-IS, L1 - IS-IS level-1,  L2  - IS-IS level-2, N - NAT
       IPH - IP Host, SUB A - Subscriber address, SUB S - Subscriber static
       SUB P - AAA downloaded aggregate subscriber routes
       M F - Mobile Sub Foreign Agent, M H - Mobile Sub Home Agent
       M G - Mobile Sub GTP
       A - Derived Default, MeH - Media Nexthop
       >   - Active Route, * - LSP

Type    Network             Next Hop        Dist  Metric    UpTime  Interface
> SUB P 15.1.0.0/24                          253       1  00:09:00  null0
> SUB P 15.1.1.0/24                          253       1  00:09:00  null0
> SUB P 15.1.2.0/24                          253       1  00:09:00  null0
> SUB P 15.1.3.0/24                          253       1  00:09:00  null0
> SUB P 15.1.4.0/24                          253       1  00:09:00  null0
> SUB P 15.1.5.0/24                          253       1  00:09:00  null0
> SUB P 15.1.6.0/24                          253       1  00:09:00  null0
> SUB P 15.1.7.0/24                          253       1  00:09:00  null0
> SUB P 15.1.8.0/24                          253       1  00:09:00  null0
> SUB P 15.1.9.0/24                          253       1  00:09:00  null0
> SUB P 15.1.10.0/24                         253       1  00:09:00  null0
> SUB P 15.1.11.0/24                         253       1  00:09:00  null0
> SUB P 15.1.12.0/24                         253       1  00:09:00  null0
> SUB P 15.1.13.0/24                         253       1  00:09:00  null0
> SUB P 15.1.14.0/24                         253       1  00:09:00  null0
> SUB P 15.1.15.0/24                         253       1  00:09:00  null0
```

1.45 show ip route summary

show ip route summary

1.45.1 Purpose

Displays summary information for all IP routes.

1.45.2 Command Mode

All modes

1.45.3 Syntax Description

This command has no keywords or arguments.

1.45.4 Default

None

1.45.5 Usage Guidelines

Use the **show ip route summary** command to display summary information for all IP routes.

Note: By default, most **show** commands (in any mode) display information for the current context only or, depending on the command syntax, for all contexts. If you are an administrator for the local context, you can insert the optional **context** ***ctx-name*** construct, preceding the **show** command, to view output for the specified context without entering that context. For more information about using the **context** ***ctx-name*** construct, see the **context** command description.

Note: By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information, see "*Modifying Output of show Commands*" in the document, *Using the CLI*.

1.45.6 Examples

The following example displays summary information for all IP routes:

```
[local]Redback>show ip route summary
```

```
Rt Tbl Version:      27144, Nh Tbl Version: 786
FIB Rt Tbl Version:  27144
Route Source             Tot-Routes     Act-Routes      Max Ever Reached
Connected                43             43              43
Static                    4              4               4
```

1.46 show ip route summary all-context

show ip route summary all-context

1.46.1 Purpose

Displays summary information for IP routes in all contexts.

1.46.2 Command Mode

All modes

1.46.3 Syntax Description

This command has no keywords or arguments.

1.46.4 Default

None

1.46.5 Usage Guidelines

Use the **show ip route summary all-context** command to display summary information for IP routes in all contexts.

Note: By default, most **show** commands (in any mode) display information for the current context only or, depending on the command syntax, for all contexts. If you are an administrator for the local context, you can insert the optional **context** ***ctx-name*** construct, preceding the **show** command, to view output for the specified context without entering that context. For more information about using the **context** ***ctx-name*** construct, see the **context** command description.

Note: By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information, see "*Modifying Output of show Commands*" in the document, *Using the CLI*.

1.46.6 Examples

The following example displays summary information for all IP routes in the `local` and `new` contexts:

```
[local]Redback>show ip route summary all-context
```

```
Context:   local                          Context id:   0x40080001
------------------------------------------------------------------
Rt Tbl Version:      9, Nh Tbl Version: 5
FIB Rt Tbl Version:  9
Route Source                  Tot-Routes     Act-Routes  Max Ever Reached

Connected                              2              2                 2
Static                                 2              2                 2

Context:   new                            Context id:   0x40080002
------------------------------------------------------------------
Rt Tbl Version:      0, Nh Tbl Version: 0
FIB Rt Tbl Version:  0
                 No routes in Table
```

1.47 show ip route xcrp

`show ip route xcrp`

1.47.1 Purpose

Displays IP route information for the controller card.

1.47.2 Command Mode

All modes

1.47.3 Syntax Description

This command has no keywords or arguments.

1.47.4 Default

None

1.47.5 Usage Guidelines

Use the **`show ip route xcrp`** command to display IP route information for the controller card.

Note: By default, most **`show`** commands (in any mode) display information for the current context only or, depending on the command syntax, for all contexts. If you are an administrator for the local context, you can insert the optional **`context`** ***`ctx-name`*** construct, preceding the **`show`** command, to view output for the specified context without entering that context. For more information about using the **`context`** ***`ctx-name`*** construct, see the **`context`** command description.

Note: By appending a space followed by the pipe (|) character at the end of a **`show`** command, you can filter the output using a set of modifier keywords and arguments. For more information, see "*Modifying Output of show Commands*" in the document, *Using the CLI*.

1.47.6 Examples

The following example displays output from the **`show ip route xcrp`** command:

```
[local]Redback>show ip route xcrp
```

```
Routing tables

Internet:
Destination        Gateway            Flags    Refs      Use   Cntxt   Interface
default            10.12.208.1        UG1         4    17882       1   fxp0
3                  155.53.1.235       UG1         0        0       1   fxp0
4                  155.53.1.236       UG1         0        0       1   fxp0
4.21.132/23        155.53.1.236       UG1         0        0       1   fxp0
6.1/16             155.53.1.235       UG1         0        0       1   fxp0
6.2/22             155.53.1.236       UG1         0        0       1   fxp0
```

1.48 show ip statistics xcrp

show ip statistics xcrp

1.48.1 Purpose

Displays IP traffic statistics on the active controller card.

1.48.2 Command Mode

All modes

1.48.3 Syntax Description

This command has no keywords or arguments.

1.48.4 Default

None

1.48.5 Usage Guidelines

Use the **show ip statistics xcrp** command to display IP traffic statistics on the active controller card. The IP traffic statistics display does not include statistics for forwarded traffic. The display shows only traffic whose destination or source addresses are on the system itself.

Note: By default, most **show** commands (in any mode) display information for the current context only or, depending on the command syntax, for all contexts. If you are an administrator for the local context, you can insert the optional **context** ***ctx-name*** construct, preceding the **show** command, to view output for the specified context without entering that context. For more information about using the **context** ***ctx-name*** construct, see the **context** command description.

Note: By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information, see "*Modifying Output of show Commands*" in the document, *Using the CLI*.

1.48.6 Examples

The following example displays all IP traffic destined to or source by transmit or receive addresses in to, or sourced by, the system:

```
[local]Redback>show ip statistics xcrp

ip:
        331718 total packets received
        0 bad header checksums
        0 with size smaller than minimum
        0 with data size < data length
        0 with length > max ip packet size
        0 with header length < data size
        0 with data length < header length
        0 with bad options
        0 with incorrect version number
        0 fragments received    0 fragments dropped (dup or out of space)
        0 malformed fragments dropped
        0 fragments dropped after timeout
        0 packets reassembled ok
        314961 packets for this host
        11722 packets for unknown/unsupported protocol
        6 packets forwarded (0 packets fast forwarded)
        5129 packets not forwardable
        5 redirects sent
        88051 packets sent from this host
        17 packets sent with fabricated ip header
        0 output packets dropped due to no bufs, etc.
        0 output packets discarded due to no route
        0 output datagrams fragmented
```

```
0 fragments created

0 datagrams that can't be fragmented
```

1.49 show ipv6 access-list

`show ipv6 access-list`

1.49.1 Purpose

Displays the status of configured IPv6 ACLs.

1.49.2 Command Mode

exec

1.49.3 Syntax Description

This command has no keywords or arguments.

1.49.4 Default

None

1.49.5 Usage Guidelines

Use the **`show ipv6 access-list`** command to display the status of configured IPv6 ACLs.

1.49.6 Examples

The following example displays output from the **`show ipv6 access-list`** command:

```
[local]Redback#show ipv6 access-list
ipv6 access-list list100:
 count: 9, sequences: 10 - 90, client count: 0
 modified: 00:00:03 (hh:mm:ss) ago, version: 19
  seq 10 permit ipv6 any 11::1/128
  seq 20 permit ipv6 any 11::2/128
  seq 30 permit ipv6 any 11::3/128
  seq 40 permit ipv6 any 11::4/128
  seq 50 permit ipv6 any 11::5/128
  seq 60 permit ipv6 any 11::6/128
  seq 70 permit ipv6 any 11::7/128
  seq 80 permit ipv6 any 11::8/128
  seq 90 deny ipv6 any any

ipv6 access-list list6:
 count: 1, sequences: 88 - 88, client count: 0
 modified: 01:54:25 (hh:mm:ss) ago, version: 3
  seq 88 permit ipv6 any any

total ipv6 access lists: 2
```

1.50 show ipv6 all-host

show ipv6 all-host

1.50.1 Purpose

Displays a list of all static and dynamic IPv6 hosts in the current context.

1.50.2 Command Mode

All modes

1.50.3 Syntax Description

This command has no keywords or arguments.

1.50.4 Default

None

1.50.5 Usage Guidelines

Use the **show ipv6 all-host** command to display a list of all static and dynamic IPv6 hosts in the current context. The output of this command maps host names to their IPv6 addresses.

1.50.6 Examples

The following example shows how to use the **show ipv6 all-host** command:

```
[local]Redback>show ipv6 all-host
```

1.51 show ipv6 dynamic-host

`show ipv6 dynamic-host`

1.51.1 Purpose

Displays a list of all dynamic IPv6 hosts in the current context.

1.51.2 Command Mode

All modes

1.51.3 Syntax Description

This command has no keywords or arguments.

1.51.4 Default

None

1.51.5 Usage Guidelines

Use the **`show ipv6 dynamic-host`** command to display a list of all dynamic IPv6 hosts in the current context. The output of this command maps host names to their IPv6 addresses.

1.51.6 Examples

The following example shows how to use the **`show ipv6 dynamic-host`** command:

```
[local]Redback>show ipv6 dynamic-host
```

1.52 show ipv6 host

`show iv6p host`

1.52.1 Purpose

Displays all static hostname-to-IP Version 6 (IPv6) address mappings stored in the local host table for the current context.

1.52.2 Command Mode

All modes

1.52.3 Syntax Description

This command has no keywords or arguments.

1.52.4 Default

None

1.52.5 Usage Guidelines

Use the **`show ipv6 host`** command to display all static hostname-to-IPv6 address mappings stored in the local host table for the current context.

Note: By default, most **`show`** commands (in any mode) display information for the current context only or, depending on the command syntax, for all contexts. If you are an administrator for the local context, you can insert the optional **`context`** ***`ctx-name`*** construct, preceding the **`show`** command, to view output for the specified context without entering that context. For more information about using the **`context`** ***`ctx-name`*** construct, see the **`context`** command description.

Note: By appending a space followed by the pipe (|) character at the end of a **`show`** command, you can filter the output using a set of modifier keywords and arguments. For more information, see "*Modifying Output of show Commands*" in the document, *Using the CLI*.

1.52.6 Examples

The following example displays output from the **`show ipv6 host`** command:

```
[local]Redback>show ipv6 host

Host Name                IP Address       Type        TTL
host1                    172.2.3.1        static      0
host2                    172.2.3.2        static      0
host3                    172.2.3.3        static      0
```

1.53 show ipv6 interface

show ipv6 interface [{*if-name* | **brief**}]

1.53.1 Purpose

Displays information about IP Version 6 (IPv6) interfaces, including the interface bound to the Ethernet management port on the controller card.

1.53.2 Command Mode

All modes

1.53.3 Syntax Description

if-name	Optional. Name of the IPv6 interface to be displayed.
brief	Optional. Displays the name, IPv6 address, and other information (in brief) for all configured IPv6 interfaces in the current context.

1.53.4 Default

Displays detailed information for all configured IPv6 interfaces.

1.53.5 Usage Guidelines

Use the **show ipv6 interface** command to display information about all IPv6 interfaces, including those on the controller card. Use this command without optional syntax to display detailed information on all configured IPv6 interfaces.

Note: By default, most **show** commands (in any mode) display information for the current context only or, depending on the command syntax, for all contexts. If you are an administrator for the local context, you can insert the optional **context** *ctx-name* construct before the **show** command to view output for the specified context without entering that context. For more information about the **context** *ctx-name* construct, see the **context** command description.

Note: By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information, see "*Modifying Output of show Commands*" in the document, *Using the CLI*.

An interface can be in any of the following states:

- Unbound—The interface is not currently bound to any port or circuit.

- Bound—The interface is bound to at least one port or circuit; however, none of the bound circuits are up, and therefore, the interface is not up.
- Up—At least one of the bound circuits is in the up state; therefore, the interface is also up and traffic can be sent over the interface.

1.53.6 Examples

The following example displays output from the **show ipv6 interface** command with the **brief** keyword:

```
[local]Redback>show ipv6 interface brief:
```

```
Mon Jun 27 06:38:05 2005

Name             Address                  MTU    State      Bindings

fe13/3           3.2.13.3/16              1500   Up         ethernet 13/3

fe13/4           4.2.13.4/16              1500   Up         ethernet 13/4

5/1              10.13.49.166/24          1500   Up         ethernet 5/1

12/1             10.1.1.1/16              0      UnBound

un1              (Un-numbered)            0      UnBound

lo1              100.1.1.1/16             1500   Up         (Loopback)
```

The following example displays information for the `fe13/4` interface:

```
[local]Redback>show ipv6 interface fe13/4
```

```
Intf name:        fe13/4
Intf state:       Up                        MTU:                1500
IP address:       4.2.13.4                  Prefix len:         16
ISIS Tag:         1                         Levels:             level-1-2
ISIS Metric:      10                        Authentication:     none
OSPF instance:    1                         OSPF net type:      broadcast
OSPF cost:        1                         OSPF state          BDR
Resoln type:      Arp                       ARP timeout         3600
ARP Proxy:        Enabled

Bindings:
Encapsulation     Circuit
ethernet          13/4
```

1.54 show ipv6 mroute

show ipv6 mroute [*first-ipv6-address second-ipv6-address*] [**count** | **detail**]

1.54.1 Purpose

Displays information about the IPv6 multicast routes configured on the system.

1.54.2 Command Mode

All modes

1.54.3 Syntax Description

second-ipv6-address	Specifies a second IPv6 address in the format A:B:C:D:E:F:G:H.
first-ipv6-address	Specifies an IPv6 address in format A:B:C:D:E:F:G:H.
count	Displays IPv6 multicast counters.
detail	Displays detailed information for the specified IPv6 routes or for all IPv6 routes configured on the system.

1.54.4 Default

Enter the **show ipv6 mroute** command without any of the optional keyword or arguments to display summarized information for all IPv6 multicast routes on the system.

1.54.5 Usage Guidelines

Use the **show ipv6 mroute** command to display information about the IPv6 multicast routes configured on the system.

1.54.6 Examples

The following example shows how to use the **show ipv6 mroute** command:

```
[local]Redback>show ipv6 mroute
```

1.55 show ipv6 policy access-list

```
show ipv6 policy access-list[[summary] [acl-name] | first-match
acl-name {[protocol]{src-addr} [dest-addr]
[traffic-class class] [fragments]
```

1.55.1 Purpose

Displays the status of configured IPv6 access control lists (ACLs).

1.55.2 Command Mode

EXEC

1.55.3 Syntax Description

summary	Optional. Excludes the ACL statements from the display. Optionally, you can follow this keyword with the *acl-name* argument, naming a particular ACL for which you want summary information displayed.
	Optional. Name of the ACL for which you want information displayed. To display summary information about a specific list, you must enter the **summary** keyword first, followed by the *acl-name* argument.
	Optional. Name of the ACL for which you want to find the first statement matched by the criteria that follows the **first-match acl-*name*** construct.

protocol	Optional. Number indicating a protocol as specified in RFC 1700, Assigned Numbers. The range of values is 0 to 255. In place of the protocol argument, you can use any of the following keywords: • **ahp**—Specifies the Authentication Header Protocol. • **esp**—Specifies the encapsulation security payload. • **hop-by-hop**—Specifies hop-by-hop options. • **icmpv6**—Specifies the Internet Control Message Protocol version 6 (ICMPv6). • **ipv6**—Uses any IPv6 protocol. • **none**—Specifies no next-header. • **ospf**—Specifies the Open Shortest Path First protocol. • **pcp**—Specifies the Payload Compression Protocol. • **pim**—Specifies Protocol Independent Multicast. • **routing**—Specifies the routing header • **tcp**—Specifies the Transmission Control Protocol. • **udp**—Specifies the User Datagram Protocol.
src-addr	Source address to be included in the criteria for a match. An IPv6 address in the form A:B:C:D:E:F:G.
dest-addr	Optional. Destination address to be included in the criteria for a match. An IPv6 address in the form A:B:C:D:E:F:G.
traffic-class *class*	Optional.Type of traffic class to be matched. Table 9 describes the possible traffic classes.
fragments	Optional. Includes fragment headers in the criteria for a match.

1.55.4 Default

None

1.55.5 Usage Guidelines

Use the **show ipv6 policy access-list** command to display the status of configured IPv6 ACLs.

Table 9 lists the valid keyword values for the **traffic-class** *class* construct.

Table 9 Valid Keyword Values for the traffic-class class Construct

Keyword	Definition
af11	Assured Forwarding—Class 1/Drop precedence 1
af12	Assured Forwarding—Class 1/Drop precedence 2
af13	Assured Forwarding—Class 1/Drop precedence 3
af21	Assured Forwarding—Class 2/Drop precedence 1
af22	Assured Forwarding—Class 2/Drop precedence 2
af23	Assured Forwarding—Class 2/Drop precedence 3
af31	Assured Forwarding—Class 3/Drop precedence 1
af32	Assured Forwarding—Class 3/Drop precedence 2
af33	Assured Forwarding—Class 3/Drop precedence 3
af41	Assured Forwarding—Class 4/Drop precedence 1
af42	Assured Forwarding—Class 4/Drop precedence 2
af43	Assured Forwarding—Class 4/Drop precedence 3
cs0	Class Selector 0
cs1	Class Selector 1
cs2	Class Selector 2
cs3	Class Selector 3
cs4	Class Selector 4
cs5	Class Selector 5
cs6	Class Selector 6
cs7	Class Selector 7
df	Default Forwarding (same as cs0)
ef	Expedited Forwarding

1.55.6 Examples

The following example shows how to display the status of an IPv6 ACL called `ipv6_acc`:

```
[local]Redback#show ipv6 policy access-list ipv6_acc

policy access-list ipv6_acc:
 count: 3, sequences: 10 - 30, client count: 0
 modified: 00:07:13 (hh:mm:ss) ago, version: 1203, grid: 0x40030003
  seq 10 permit tcp any any class data
  seq 20 permit tcp any any class data
  seq 30 permit udp any any eq 1000 class voip
```

1.56 show ipv6 pool

show ipv6 pool[[**dhcpv6**] [*pool-name*]**thresholds** | **summary**]

1.56.1 Purpose

Displays allocation information about the shared IPv6 and DHCPv6 PD prefix pools configured in the current context.

1.56.2 Command Mode

All modes

1.56.3 Syntax Description

dhcpv6	Displays information about DHCPv6-PD pools.
pool-name	Name of the pool for which you want to display information.
thresholds	Displays threshold information for a specific IPv6 pool, or for all IPv6 pools configured in the current context.
summary	Displays summarized information about all IPv6 pools configured in the current context.

1.56.4 Default

When entered without any optional keywords or arguments, this command displays summarized information for all shared IPv6 pools configured in the current context.

1.56.5 Usage Guidelines

Use the **show ipv6 pool** command to display allocation information about the shared IPv6 and DHCPv6 PD prefix pools configured in the current context..

1.56.6 Examples

The following example displays information about the shared IPv6 prefix pools configured in the local context:

```
[local]Redback#show ipv6 pool

Interface "subs":
  2001:db8:1::/64    2001:db8:1:4::/64          0 in-use, 20480 free,    0 reserved
```

The following example displays information for the DHCPv6 PD pools configured in the context **m1**:

```
[local]Redback#context m1

[m1]Redback#show ipv6 pool dhcpv6

Interface "subs":
  3001:db8:1:1::/64    3001:db8:1:100::/64               0 in-use, 4096 free,   0
  3002:db8:1:1::/64    3002:db8:1:100::/64               0 in-use, 4096 free,   0
```

1.57 show ipv6 prefix-list

show ipv6 prefix-list [*pl-name* | **first-match** *pl-name* *ipv6-addr/prefix-length* | **summary** [*pl-name*]]

1.57.1 Purpose

Displays information about configured IP Version 6 (IPv6) prefix lists.

1.57.2 Command Mode

All modes

1.57.3 Syntax Description

pl-name	Optional. IPv6 prefix list name.
first-match	Optional. Searches for the line in the IPv6 prefix list specified by the *pl-name* argument.
ipv6-addr/prefix-length	Specifies the IPv6 address, in the form *A*:*B*:*C*:*D*:*E*:*F*:*G*:*H*, and the prefix length, separated by the slash (/) character. The range of values for the *prefix-length* argument is 0 to 128.
summary	Optional. Displays summary information for all configured IPv6 prefix lists.

1.57.4 Default

None

1.57.5 Usage Guidelines

Use the **show ipv6 prefix-list** command to display information about configured IPv6 prefix lists.

Note: By default, most **show** commands (in any mode) display information for the current context only or, depending on the command syntax, for all contexts. If you are an administrator for the local context, you can insert the optional **context** *ctx-name* construct, preceding the **show** command, to view output for the specified context without entering that context. For more information about using the **context** *ctx-name* construct, see the **context** command description.

Note: By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information, see "*Modifying Output of show Commands*" in the document, *Using the CLI*.

1.57.6 Examples

The following example displays output from the **show ipv6 prefix-list** command:

```
[local]Redback>show ipv6 prefix-list


ipv6 prefix-list list1:

 count: 2, sequences: 10 - 20, client count: 0

 modified: 00:00:13 (hh:mm:ss) ago

   seq 10 permit a001::/64 ge 64 le 128  (hit count: 0)

   seq 20 permit b002::/48 ge 48 le 128  (hit count: 0)
```

1.58 show ipv6 route

show ipv6 route [*ipv6-addr* [/*prefix-length* [**longer-prefixes** | **shorter-prefixes** | **detail**]] | **all** | **bgp** | **connected** | **context** | **fib-client** *client-id* | **hidden** | **interface** [*nexthop-id*][**detail**] | **iphost** | **isis** | **multicast** [*ip-addr*[/*prefix-length*]] [**bgp**] [**next-hop**] [**ripng**] [**static**] [**summary**] | **next-hop** | **ospf3** | **registered** | **ripng** | **static** | **subscriber** [**address** | **aggregate** | **dhcp-pd** | **nd** | **static**] | **summary** | **xcrp**]

1.58.1 Purpose

Displays information about IP version 6 (IPv6) routes.

1.58.2 Command Mode

All modes

1.58.3 Syntax Description

ipv6-addr	Optional. IPv6 address, in the form ***A*:*B*:*C*:*D*:*E*:*E*:*F*:*G***, of the route to be displayed.
prefix-length	Optional. Prefix length. The range of values is 0 to 128.
longer-prefixes	Optional. Displays the route and more-specific routes.
shorter-prefixes	Optional. Displays the route and less-specific routes.
detail	Optional. Displays detailed information.
all	Optional. Displays information about all IPv6 routes.
bgp	Optional. Displays Border Gateway Protocol (BGP) route information.
connected	Optional. Displays information about IPv6 routes from directly connected networks.
context	Optional. Displays information about an IPv6 route context.
fib-client	Optional. Displays RIB FIB client information.
hidden	Optional. Displays information about hidden IPv6 routes; that is, routes that are added internally.
interface	Optional. Displays information about the interfaces in the RIB. You can display information for a particular nexthop ID, and you can display details for all interfaces in the RIB.
nexthop-id	Nexthop identifier, expressed in hexadecimal format.
iphost	Optional. Displays information about IP host address routes.
isis	Optional. Displays information about IS-IS IPv6 routes.

`multicast`	Optional. Displays unicast-dependent multicast routing table information.
`next-hop`	Optional. Displays next-hop information.
`ospf3`	Optional. Displays information about OSPFv3 IPv6 routes.
`ripng`	Optional. Displays next Routing Information Protocol next generation (RIPng) route information.
`static`	Optional. Displays static route information.
`subscriber`	Optional. Displays information about IPv6 subscriber routes, which can be filtered using the following options: • `address`—Displays subscriber address routes. • `aggregate`—Displays subscriber aggregate routes. • `dhcp-pd`—Displays subscriber DHCP Prefix Delegation. • `nd`—Displays subscriber Neighbor Discovery routes. • `static`—Displays subscriber static routes.
`summary`	Optional. Displays summary route information.
`registered`	Optional. Displays registered IPv6 route information.
`xcrp`	Optional. Displays IPv6 route information for the controller card.

1.58.4 Default

When entered with no keywords or arguments, this command displays all IP routes.

1.58.5 Usage Guidelines

Use the **show ipv6 route** command to display information about IPv6 routes.

Note: By default, most **show** commands (in any mode) display information for the current context only or, depending on the command syntax, for all contexts. If you are an administrator for the local context, you can insert the optional **context** ***ctx-name*** construct, preceding the **show** command, to view output for the specified context without entering that context. For more information about using the **context** ***ctx-name*** construct, see the **context** command description.

Note: By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information, see "*Modifying Output of show Commands*" in the document, *Using the CLI*.

1.58.6 Examples

The following example displays output from the **`show ipv6 route`** command:

```
[local]Redback>show ipv6 route

Codes: C - connected, S - static, S dv - dvsr, R - RIP, e B - EBGP, i B - IBGP
       O   - OSPF, O3  - OSPFv3, IA - OSPF(v3) inter-area,
       N1  - OSPF(v3) NSSA external type 1, N2  - OSPF(v3) NSSA external type 2
       E1  - OSPF(v3) external type 1, E2  - OSPF(v3) external type 2
       i   - IS-IS, L1 - IS-IS level-1,  L2  - IS-IS level-2, N - NAT
       IPH - IP Host, SUB A - Subscriber address, SUB S - Subscriber static
       A - Derived Default
       >   - Active Route, * - LSP

Type    Network             Next Hop         Dist  Metric    UpTime  Interface
> C     4001::/64                               0       0     1d02h  to-peer
> C     5001:2201:ff31:9900::/64                0       0     1d02h  to-core
> S     6001:aaaa:bbbb:cccc::/64
                            4001::2             1       0  05:11:09  to-peer
> C     7001::/112                              0       0  00:17:47  to-nbor
> S     7001:dddd:eeee:ffff:1::/112             1       0  05:11:09  to-core
> C     8001::1/128                             0       0  00:15:39  lo
> R     8001::2/128         fe80::230:88ff:fe00:3294
                                              120       1  00:08:09  to-nbor
> e B   9001::/64           7001::ff           20       0  00:01:51  to-nbor
> e B   9002::/64           7001::ff           20       0  00:01:51  to-nbor
> C     fe80::230:88ff:fe00:1104/128            0       0     1d02h  to-peer
> C     fe80::230:88ff:fe00:1105/128            0       0     1d02h  to-core
> C     fe80::230:88ff:fe00:1109/128            0       0  00:17:47  to-nbor
```

The following example displays information for the IPv6 route, `8001::2/128`:

```
[local]Redback>show ipv6 route 8001::2/128

    Best match Routing entry for 8001::2/128 is 8001::2/128 , version 21
    Route Uptime 00:08:45
    Paths: total 1, best path count 1

    Route has been downloaded to following slots
     03/0

    Path information :

      Active path :
      Known via rip 1, distance 120, metric 1,
      Tag 0, Next-hop fe80::230:88ff:fe00:3294, NH-ID 0x31100005, Adj ID: 0x2000
001, Lsp ifgrid: 0x201FFFF, Interface to-nbor
      Circuit 3/6:1023:63/1/1/11
```

The following example displays information for all IPv6 routes:

```
[local]Redback>show ipv6 route all

Codes: C - connected, S - static, S dv - dvsr, R - RIP, e B - EBGP, i B - IBGP
       A,H - derived hidden
       O   - OSPF, O3  - OSPFv3, IA - OSPF(v3) inter-area,
       N1  - OSPF(v3) NSSA external type 1, N2  - OSPF(v3) NSSA external type 2
       E1  - OSPF(v3) external type 1, E2  - OSPF(v3) external type 2
       i   - IS-IS, L1 - IS-IS level-1,  L2  - IS-IS level-2, N - NAT
       IPH - IP Host, SUB A - Subscriber address, SUB S - Subscriber static
       A - Derived Default
       >   - Active Route, * - LSP

Type    Network             Next Hop        Dist  Metric    UpTime  Interface
> C     4001::/64                              0       0     1d02h  to-peer
> C H   4001::/128                             0       0     1d02h  to-peer
> C H   4001::1/128                            0       0     1d02h  to-peer
> A H   4001::2/128         4001::2          254       0  05:11:58  to-peer
> C     5001:2201:ff31:9900::/64               0       0     1d02h  to-core
> C H   5001:2201:ff31:9900::/128              0       0     1d02h  to-core
> C H   5001:2201:ff31:9900::fe/128            0       0     1d02h  to-core
> S     6001:aaaa:bbbb:cccc::/64
                            4001::2            1       0  05:11:58  to-peer
> C     7001::/112                             0       0  00:18:36  to-nbor
> C H   7001::/128                             0       0  00:18:36  to-nbor
> C H   7001::1/128                            0       0  00:18:36  to-nbor
> A H   7001::ff/128        7001::ff         254       0  00:11:36  to-nbor
> S     7001:dddd:eeee:ffff:1::/112            1       0  05:11:58  to-core
> C     8001::1/128                            0       0  00:16:28  lo
> R     8001::2/128  fe80::230:88ff:fe00:3294 120      1  00:08:58  to-nbor
> e B   9001::/64           7001::ff          20       0  00:02:40  to-nbor
> e B   9002::/64           7001::ff          20       0  00:02:40  to-nbor
> C     fe80::230:88ff:fe00:1104/128           0       0     1d02h  to-peer
> C     fe80::230:88ff:fe00:1105/128           0       0     1d02h  to-core
> C     fe80::230:88ff:fe00:1109/128           0       0  00:18:36  to-nbor
> A H   fe80::230:88ff:fe00:3294/128
        fe80::230:88ff:fe00:3294             254       0  00:11:36  to-nbor
```

The following example displays information for the BGP routes:

```
[local]Redback>show ipv6 route bgp

Codes: C - connected, S - static, S dv - dvsr, R - RIP, e B - EBGP, i B - IBGP
       A,H - derived hidden
       O   - OSPF, O3  - OSPFv3, IA - OSPF(v3) inter-area,
       N1  - OSPF(v3) NSSA external type 1, N2  - OSPF(v3) NSSA external type 2
       E1  - OSPF(v3) external type 1, E2  - OSPF(v3) external type 2
       i   - IS-IS, L1 - IS-IS level-1,  L2  - IS-IS level-2, N - NAT
       IPH - IP Host, SUB A - Subscriber address, SUB S - Subscriber static
       A - Derived Default
       >   - Active Route, * - LSP

Type    Network             Next Hop        Dist  Metric    UpTime  Interface
> e B   9001::/64           7001::ff          20       0  00:02:59  to-nbor
> e B   9002::/64           7001::ff          20       0  00:02:59  to-nbor
```

The following example displays information for the connected IPv6 routes:

```
[local]Redback>show ipv6 route connected

Codes: C - connected, S - static, S dv - dvsr, R - RIP, e B - EBGP, i B - IBGP
       A,H - derived hidden
       O   - OSPF, O3  - OSPFv3, IA - OSPF(v3) inter-area,
       N1  - OSPF(v3) NSSA external type 1, N2  - OSPF(v3) NSSA external type 2
       E1  - OSPF(v3) external type 1, E2  - OSPF(v3) external type 2
       i   - IS-IS, L1 - IS-IS level-1,  L2  - IS-IS level-2, N - NAT
       IPH - IP Host, SUB A - Subscriber address, SUB S - Subscriber static
       A - Derived Default
       >   - Active Route, * - LSP

Type    Network             Next Hop        Dist  Metric    UpTime  Interface
> C     4001::/64                              0       0     1d02h  to-peer
> C H   4001::/128                             0       0     1d02h  to-peer
> C H   4001::1/128                            0       0     1d02h  to-peer
> C     5001:2201:ff31:9900::/64               0       0     1d02h  to-core
> C H   5001:2201:ff31:9900::/128              0       0     1d02h  to-core
> C H   5001:2201:ff31:9900::fe/128            0       0     1d02h  to-core
> C     7001::/112                             0       0  00:19:06  to-nbor
> C H   7001::/128                             0       0  00:19:06  to-nbor
> C H   7001::1/128                            0       0  00:19:06  to-nbor
> C     8001::1/128                            0       0  00:16:58  lo
> C     fe80::230:88ff:fe00:1104/128           0       0     1d02h  to-peer
> C     fe80::230:88ff:fe00:1105/128           0       0     1d02h  to-core
> C     fe80::230:88ff:fe00:1109/128           0       0  00:19:06  to-nbor
```

The following example displays information for the hidden IPv6 routes:

```
[local]Redback>show ipv6 route hidden

Codes: C - connected, S - static, S dv - dvsr, R - RIP, e B - EBGP, i B - IBGP
       A,H - derived hidden
       O   - OSPF, O3  - OSPFv3, IA - OSPF(v3) inter-area,
       N1  - OSPF(v3) NSSA external type 1, N2  - OSPF(v3) NSSA external type 2
       E1  - OSPF(v3) external type 1, E2  - OSPF(v3) external type 2
       i   - IS-IS, L1 - IS-IS level-1,  L2  - IS-IS level-2, N - NAT
       IPH - IP Host, SUB A - Subscriber address, SUB S - Subscriber static
       A - Derived Default
       >   - Active Route, * - LSP

Type    Network             Next Hop        Dist  Metric    UpTime  Interface
> C H   4001::/128                             0       0     1d02h  to-peer
> C H   4001::1/128                            0       0     1d02h  to-peer
> A H   4001::2/128         4001::2          254       0  05:12:43  to-peer
> C H   5001:2201:ff31:9900::/128              0       0     1d02h  to-core
> C H   5001:2201:ff31:9900::fe/128            0       0     1d02h  to-core
> C H   7001::/128                             0       0  00:19:21  to-nbor
> C H   7001::1/128                            0       0  00:19:21  to-nbor
> A H   7001::ff/128        7001::ff         254       0  00:12:21  to-nbor
> A H   fe80::230:88ff:fe00:3294/128
        fe80::230:88ff:fe00:3294             254       0  00:12:21  to-nbor
```

The following example displays information about next-hop IPv6 routes:

```
[local]Redback>show ipv6 route next-hop

    ** = Via interface
    Next Hop Tbl Version :         14
    Current Next Hops    :          7

NH-ID                 Ref Cnt NH-IP           Via-NH     Interface
0x30D00003               10/0                            Local host
0x31100001                1/0                            to-peer
0x31100002                2/0                            to-core
0x31100003                2/0 4001::2                    to-peer
0x31100004                1/0                            to-nbor
0x31100005                2/0 fe80::230:88ff:fe00:3294           to-nbor
0x31100006                3/0 7001::ff                   to-nbor
```

The following example displays information for registered next-hop IPv6 routes:

```
[local]Redback>show ipv6 route registered next-hop

Next-hop:           Registered Client(s):

4001::2             static
Query flags    : 0x40                Version        : 0x1
Adj-id         : 0x2000000           Conn Adj-id    : 0x2000008
NH Magic       : 0x1000000           Default flag   : 0x0
Protocol       : 0x1                 IGP Metric     : 0
Conn IF-GRID   : 0x10000001          Conn cct id    : 3/1:1023:63/1/1/5
IGP IF-GRID    : 0x10000001          IGP cct id     : 3/1:1023:63/1/1/5
Reslov cntxt   : 0x40080001          IGP MTU        : 1500
IGP first hop  : 0.0.0.0             IGP next hop   : 0.0.0.0

5001::1             static
Query flags    : 0x0                 Version        : 0x0
Adj-id         : 0xFFFFFFFF          Conn Adj-id    : 0xFFFFFFFF
NH Magic       : 0x0                 Default flag   : 0x0
Protocol       : 0x0                 IGP Metric     : -1
Conn IF-GRID   : 0x0                 Conn cct id    : Cct invalid
IGP IF-GRID    : 0x0                 IGP cct id     : Cct invalid
Reslov cntxt   : 0x40080001          IGP MTU        : 0
IGP first hop  : 0.0.0.0             IGP next hop   : 0.0.0.0

7001::ff            bgp 100
Query flags    : 0x40                Version        : 0x0
Adj-id         : 0x2000002           Conn Adj-id    : 0x200000A
NH Magic       : 0x1000000           Default flag   : 0x0
Protocol       : 0x1                 IGP Metric     : 0
Conn IF-GRID   : 0x10000003          Conn cct id    : 3/6:1023:63/1/1/11
IGP IF-GRID    : 0x10000003          IGP cct id     : 3/6:1023:63/1/1/11
Reslov cntxt   : 0x40080001          IGP MTU        : 1500
IGP first hop  : 0.0.0.0             IGP next hop   : 0.0.0.0
```

The following example displays information about RIP routes:

The following example displays information for the static IPv6 routes:

```
[local]Redback>show ipv6 route static

Codes: C - connected, S - static, S dv - dvsr, R - RIP, e B - EBGP, i B - IBGP
       A,H - derived hidden
       O   - OSPF, O3  - OSPFv3, IA - OSPF(v3) inter-area,
       N1  - OSPF(v3) NSSA external type 1, N2  - OSPF(v3) NSSA external type 2
       E1  - OSPF(v3) external type 1, E2  - OSPF(v3) external type 2
       i   - IS-IS, L1 - IS-IS level-1,  L2  - IS-IS level-2, N - NAT
       IPH - IP Host, SUB A - Subscriber address, SUB S - Subscriber static
       A - Derived Default
       >   - Active Route, * - LSP

Type    Network             Next Hop        Dist  Metric    UpTime  Interface
> S     6001:aaaa:bbbb:cccc::/64
                            4001::2            1       0    05:14:38  to-peer
> S     7001:dddd:eeee:ffff:1::/112            1       0    05:14:38  to-core
```

The following example displays subscriber aggregate routes:

```
[local]Redback>show ipv6 route subscriber aggregate
Codes: C - connected, S - static, S dv - dvsr, R - RIP, e B - EBGP, i B - IBGP
       A,H - derived hidden
       O   - OSPF, O3  - OSPFv3, IA - OSPF(v3) inter-area,
       N1  - OSPF(v3) NSSA external type 1, N2  - OSPF(v3) NSSA external type 2
       E1  - OSPF(v3) external type 1, E2  - OSPF(v3) external type 2
       i   - IS-IS, L1 - IS-IS level-1,  L2  - IS-IS level-2, N - NAT
       IPH - IP Host, SUB A - Subscriber address, SUB S - Subscriber static
       SUB P - AAA downloaded aggregate subscriber routes
       SUB N - Subscriber ND, SUB D - Subscriber DHCP-PD
       M F - Mobile Sub Foreign Agent, M H - Mobile Sub Home Agent,
       M G - Mobile Sub GTP
       E P - EPS Aggregate(Prefix), E A - EPS Address, E S - EPS Static
       A - Derived Default, MeH - Media Nexthop
       TSC - tunnel shortcut
       >   - Active Route, * - LSP

Type    Network             Next Hop        Dist    Metric    UpTime  Interface
> SUB P 2001:1508:1003::/69                  253         2  19:43:11  null0
> SUB P 2001:1508:1003:0:800::/69            253         2  19:51:07  null0
> SUB P 2001:1508:1003:0:1000::/69           253         2  19:51:07  null0
> SUB P 2001:1508:1003:0:1800::/69           253         2  19:51:07  null0
```

1.59 show isis adjacency

show isis [*instance-name*] [**multicast**] **adjacency** [**detail**]

1.59.1 Purpose

Displays information about Intermediate System-to-Intermediate System (IS-IS) neighbors.

1.59.2 Command Mode

All modes

1.59.3 Syntax Description

instance-name	Optional. IS-IS instance name. Displays information only about neighbors for the specified instance.
multicast	Optional. Displays multitopology IS-IS (M-ISIS) information.
detail	Optional. Displays additional information about IS-IS neighbors.

1.59.4 Default

Displays information for all IS-IS neighbors.

1.59.5 Usage Guidelines

Use the **show isis adjacency** command to display information about IS-IS neighbors.For information about troubleshooting IS-IS, see *Troubleshooting IS-IS*.

Note: By default, most **show** commands (in any mode) display information for the current context only or, depending on the command syntax, for all contexts. If you are an administrator for the local context, you can insert the optional **context** *ctx-name* construct, preceding the **show** command, to view output for the specified context without entering that context. For more information about using the **context** *ctx-name* construct, see the **context** command description.

Note: By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information, see "*Modifying Output of show Commands*" in the document, *Using the CLI*.

Table 10 describes the output fields for the **show isis adjacency** command.

Table 10 Field Descriptions for the show isis adjacency Command

Field	Description
SystemId	ID of an IS-IS in an area.
Interface	Interface advertising the IS-IS.
L	Level 1 routing only (1), level 2 routing only (2), or levels 1 and 2 (3) routing. Point-to-point adjacency is indicated with the letter p; for example, a level 2 routing with point-to-point adjacency displays as 2p.
MT	Multi-Topology. Indicates whether each IS-IS instance performs unicast (U), multicast (M), or unicast and multicast (UM) topology-based routing. Displays no value when the default routing topology, unicast, is used.
Stat	IS-IS adjacency state.
Hold	Time, in seconds, before an adjacency timeout occurs.
SNPA	Subnetwork Point of Attachment (SNPA) or the data-link address of the remote system.
Uptime	Time that the adjacency has been up.

1.59.6 Examples

The following example displays output from the **show isis adjacency** command:

```
[local]Redback>show isis adjacency

IS-IS Adjacenc(ies) for tag 6:

SystemId        Interface          L  MT   Stat Hold   SNPA            Uptime

dtse            5                  1  U    Up   28     0030.8800.1115  03:44:46

Area Address(es): 47.0001

IP Address(es): 11.1.1.1

IPv6 Address: fe80::290:69ff:fea1:dc00

BFD state N/A

adj nh-id 6, neighbor sent re-start tlv

Total IS-IS Adjacenc(ies):   1
```

The following example displays output from the show isis adjacency detail command:

```
[local]Redback>show isis adjacency detail

IS-IS Adjacenc(ies) for tag 1:

SystemId Interface L MT Stat Hold SNPA Uptime

dtse p2p 3p U Up 24 1111.1111.1111 01d23h17

Area Address(es): 47.0001

IP Address(es): 13.13.13.1

BFD state N/A

neighbor IIH current seq 17085, total iih pkt miss 0

adj nh-id 7

GR enabled state fresh

Total IS-IS Adjacenc(ies): 3
```

1.60 show isis adj-log

show isis [*instance-name*] **adj-log** [**interface** *if-name* | **is** *sys-id*]

1.60.1 Purpose

Displays adjacency logs.

1.60.2 Command Mode

All modes

1.60.3 Syntax Description

instance-name	Optional. IS-IS instance name. Only adjacency logs for the specified instance are displayed.
interface *if-name*	Optional. Interface name. Only adjacency logs for the specified interface are displayed.
is *sys-id*	Optional. System ID. Only adjacency logs for the specified system are displayed. The *sys-id* argument is either specified in **xxxx.xxxx.xxxx** format or as the hostname.

1.60.4 Default

Displays the last adjacency event for all IS-IS interfaces.

1.60.5 Usage Guidelines

Use the **show isis adj-log** command to display adjacency logs. For information about troubleshooting IS-IS, see *Troubleshooting IS-IS*.

Note: By default, most **show** commands (in any mode) display information for the current context only or, depending on the command syntax, for all contexts. If you are an administrator for the local context, you can insert the optional **context** *ctx-name* construct, preceding the **show** command, to view output for the specified context without entering that context. For more information about using the **context** *ctx-name* construct, see the **context** command description.

Note: By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information, see “*Modifying Output of show Commands*” in the document, *Using the CLI*.

Table 11 describes the output fields for the **show isis adj-log** command.

Table 11 Field Descriptions for the show isis adj-log Command

Field	Description
Interface	Name of the interface to which the adjacency log belongs.
Type	Type of interface (LAN or point-to-point).
State	Interface state when the event occurred (up or down).
Adjs	Number of adjacencies when the event occurred.
Neighbor ID	System ID or the dynamic hostname of the neighbor system.
L	Level of the IS-IS adjacency (level 1, level 2, or levels 1 and 2).
Time	Amount of time that passed since the adjacency event.
MT	Multi-Topology. Indicates whether each IS-IS instance performs unicast (U), multicast (M), or unicast and multicast (UM) topology-based routing. Displays no value when the default routing topology, unicast, is used.
Action	Reason for the adjacency event.

1.60.6 Examples

The following example displays adjacency logs for the `gre0` interface:

```
[local]Redback>show isis adj-log interface gre0
```

```
IS-IS tag test Adjacency log of events on interface gre0:
Interface    Type State Adjs NeighborID   L Time      MT  Action
gre0         p2p  Up    1    ns--edge     2 00:19:06      adj cleared
                  Up    1    ns--edge     2 00:26:33      adj is up
                  Up    1    ns--edge     3 01:25:27      adj is up
                  Up    0                 0 01:25:37      interface created
```

1.61 show isis database

show isis [*instance-name*] **database** [**detail** | **extensive**] [**level-1** | **level-2**] {*lsp-id* | *sys-id*}

1.61.1 Purpose

Displays information about the Intermediate System-to-Intermediate System (IS-IS) link-state database.

1.61.2 Command Mode

All modes

1.61.3 Syntax Description

instance-name	Optional. IS-IS instance name. Displays database information only for the specified instance.
detail	Optional. Displays the content of each link-state protocol data unit (LSP).
extensive	Optional. Displays the context of each LSP and traffic engineering (TE) sub type-length-value (TLV) object for extended IS reachability TLVs.
level-1	Optional. Displays the link-state database for level 1 only.
level-2	Optional. Displays the link-state database for level 2 only.
lsp-id	LSP ID in the format *nnnn.nnnn.nnnn.xx-yy*. Displays only information pertaining to the specified LSP.
sys-id	IS-IS system ID in the format *nnnn.nnnn.nnnn*. Displays only information pertaining to all LSP IDs for the specified IS-IS system.

1.61.4 Default

Displays information for the LSP database.

1.61.5 Usage Guidelines

Use the **show isis database** command to display information about the IS-IS link-state database. For information about troubleshooting IS-IS, see *Troubleshooting IS-IS*.

The output from the **show isis database detail** command displays the greater than (>) symbol next to the extended IS reachability TLV when it has traffic engineering information for the interface. Use the **show isis**

database extensive command (in any mode) to see the detail traffic engineering information.

Note: By default, most **show** commands (in any mode) display information for the current context only or, depending on the command syntax, for all contexts. If you are an administrator for the local context, you can insert the optional **context** ***ctx-name*** construct, preceding the **show** command, to view output for the specified context without entering that context. For more information about using the **context** ***ctx-name*** construct, see the **context** command description.

Note: By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information, see "*Modifying Output of show Commands*" in the document, *Using the CLI*.

1.61.6 Examples

The following example displays output from the **show isis database** command:

```
[local]Redback>show isis database

S-IS level 1 link-state database for tag 1:
LSPID                  Sequence   Checksum   Holdtime   AT/OL   Len
samedi.00-00*          0x62c      0x2ee7     1196       1/0     139

Total IS-IS LSP(s) for tag 1 in Level-1:   1

IS-IS level 2 link-state database for tag 1:
LSPID                  Sequence   Checksum   Holdtime   AT/OL   Len
m5-4.00-00             0x791f     0x45a3     1058       0/0     216
samedi.00-00*          0x503      0x3485     1195       0/0     583
samedi.02-00*          0xcac      0x15bb     399        0/0     55

Total IS-IS LSP(s) for tag 1 in Level-2:   3
```

The following example displays output from the **show isis database detail** command for IS-IS `level-1` routing:

```
[local]Redback>show isis database detail level-1
LSPID                  Sequence    Checksum    Holdtime    AT/OL   Len
dtse.00-00             0x9d        0x5ca1      439         0/0     297
Area Address: 47.0001
NLPID:  IP
Hostname: dtse
Router ID: 10.14.100.1
IP Address: 11.11.11.1
M-Topology:
Metric: 10          IS-Extended sierra.01 >
Metric: 13          IS-Extended samedi.01 >
Metric: 10          IS-Extended sierra.02 >
Metric: 10          IP 11.11.11.0/24
Metric: 13          IP 5.5.5.0/24
Metric: 10          IP 12.12.12.0/24
sierra.00-00           0x88        0x37bf      952         0/0     240
Area Address: 47.0001
NLPID:  IP
Hostname: sierra
Router ID: 10.14.200.1
IP Address: 11.11.11.2
M-Topology:
Metric: 10          IS-Extended sierra.01 >
Metric: 10          IS-Extended sierra.02 >
Metric: 10          IP 11.11.11.0/24
```

```
Metric: 10          IP 12.12.12.0/24
Metric: 10          IP 100.1.1.0/24
Metric: 10          IP 200.1.1.0/24
sierra.01-00           0x6f       0xfd4e     952        0/0     53
Metric: 0           IS-Extended sierra.00
Metric: 0           IS-Extended dtse.00
sierra.02-00           0x6c       0xfc51     952        0/0     53
Metric: 0           IS-Extended sierra.00
Metric: 0           IS-Extended dtse.00
samedi.00-00*          0xdd       0xadf7     599        0/0     141
Area Address: 47.0001
NLPID:  IP
Hostname: samedi
Router ID: 6.6.6.6
IP Address: 5.5.5.6
M-Topology:
Metric: 20          IS-Extended samedi.01 >
Metric: 20          IP 5.5.5.0/24
samedi.01-00*          0x84       0x6d96     599        0/0     53
Metric: 0           IS-Extended samedi.00
Metric: 0           IS-Extended dtse.00

Total IS-IS LSP(s) for tag 6 in Level-1:   6
```

The following example displays output from the **`show isis database extensive`** command:

```
[local]Redback#show isis database extensive

IS-IS level 1 link-state database for tag 1:
LSPID                  Sequence   Checksum   Holdtime   AT/OL   Len
samedi.00-00*          0x62d      0x2ce8     1192       1/0     139
Area Address: 47.0001
NLPID:  IP  IPv6
Hostname: samedi
IP Address: 1.1.1.1
M-Topology: ucast mcast v6ucast v6mcast
Local Interface IPv6 Address: 200:2003::2
Metric: 10          IP 13.1.0.0 255.255.0.0
Metric: 1           IP 1.1.1.1 255.255.255.255
Metric: 10          IP 12.1.0.0 255.255.0.0
Metric: 10          Ucast-IPv6 2000:2002::/64

Total IS-IS LSP(s) for tag 1 in Level-1:  1

IS-IS level 2 link-state database for tag 1:
LSPID                  Sequence   Checksum   Holdtime   AT/OL   Len
m5-4.00-00             0x791f     0x45a3     946        0/0     216
Area Address: 47.0001
NLPID:  IP  IPv6
M-Topology: ucast mcast v6ucast
Hostname: m5-4
Metric: 10          IS samedi.02
Metric: 10          IS-v6ucast  samedi.02
```

```
Metric: 10          IS-Mcast  samedi.02

Metric: 0           IP 10.14.200.10 255.255.255.255

Metric: 10          IP 11.1.0.0 255.255.0.0

Metric: 0           Ucast-IPv6 9000:9001::1/128

Metric: 0           Ucast-IPv6 8000:8001::1/128

Metric: 15          Ucast-IPv6-Ext 123:123::/64

Metric: 10          Ucast-IPv6 50:1:1::/64

Metric: 10          Ucast-IPv6 fe00::/102

samedi.00-00*          0x504      0x3286     1184       0/0     583

Area Address: 47.0001

NLPID:  IP  IPv6

Hostname: samedi

IP Address: 1.1.1.1

M-Topology: ucast mcast v6ucast v6mcast

Local Interface IPv6 Address: 2000:2001::2

Metric: 63          IS samedi.02

Metric: 2000        IS-Mcast  samedi.02

Metric: 1999        IS-v6ucast  samedi.02

Metric: 63          IP 11.1.0.0 255.255.0.0

Metric: 10          IP 13.1.0.0 255.255.0.0

Metric: 1           IP 1.1.1.1 255.255.255.255

Metric: 10          IP 12.1.0.0 255.255.0.0

Metric: 2000        MCast-IP 11.1.0.0/16

Metric: 0           IP-External 9.9.9.0 255.255.255.0

Metric: 0           IP-External 99.99.1.0 255.255.255.0
```

```
Metric: 0           IP-External 99.99.2.0 255.255.255.0

Metric: 0           IP-External 99.99.3.0 255.255.255.0

Metric: 0           IP-External 99.99.4.0 255.255.255.0

Metric: 0           IP-External 99.99.5.0 255.255.255.0

Metric: 0           IP-External 99.99.6.0 255.255.255.0

Metric: 0           IP-External 99.99.99.0 255.255.255.0

Metric: 1           IP 1.1.1.1 255.255.255.255

Metric: 10          IP 12.1.0.0 255.255.0.0

Metric: 10          IP 13.1.0.0 255.255.0.0

Metric: 1999        Ucast-IPv6 2000:2001::/64

Metric: 10          Ucast-IPv6 2000:2002::/64

Metric: 0           Ucast-IPv6 555:555::/100

Metric: 0           Ucast-IPv6 666:666::/100

Metric: 0           Ucast-IPv6 777:777::/100

Metric: 0           Ucast-IPv6 888:888::/100

Metric: 0           Ucast-IPv6 50:1:1::/64

Metric: 0           Ucast-IPv6 123:123::/64

Metric: 0           Ucast-IPv6 2000:2001::/64

Metric: 10          Ucast-IPv6 2000:2002::/64

Metric: 0           Ucast-IPv6 8000:8001::1/128

Metric: 0           Ucast-IPv6 9000:9001::1/128

Metric: 0           Ucast-IPv6 fe00::/102

Metric: 0           Ucast-IPv6 999:999::/64

samedi.02-00*          0xcad      0x13bc     1184       0/0      55

Metric: 0           IS samedi.00

Metric: 0           IS m5-4.00
```

```
Total IS-IS LSP(s) for tag 1 in Level-2:   3
```

1.62 show isis debug-setting

show isis [*instance-name*] **debug-setting**

1.62.1 Purpose

Displays all enabled debugging settings.

1.62.2 Command Mode

All modes

1.62.3 Syntax Description

instance-name	Optional. Intermediate System-to-Intermediate System (IS-IS) instance name. Displays only debug setting information for the specified instance.

1.62.4 Default

When entered without specifying an IS-IS instance, this command displays debug settings for all configured IS-IS instances. For information about troubleshooting IS-IS, see *Troubleshooting IS-IS*.

1.62.5 Usage Guidelines

Use the **show isis debug-setting** command to display all enabled debugging settings.

Note: By default, most **show** commands (in any mode) display information for the current context only or, depending on the command syntax, for all contexts. If you are an administrator for the local context, you can insert the optional **context** *ctx-name* construct, preceding the **show** command, to view output for the specified context without entering that context. For more information about using the **context** *ctx-name* construct, see the **context** command description.

Note: By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information, see "*Modifying Output of show Commands*" in the document, *Using the CLI*.

1.62.6 Examples

The following example displays output from the **show isis debug-setting** command:

```
[local]Redback>show isis debug-setting

debug isis adjacency

debug isis policy

debug isis protocol-errors

debug isis routes

debug isis spf-events
```

1.63 show isis dynamic-hostname

show isis [*instance-name*] **dynamic-hostname**

1.63.1 Purpose

Displays Intermediate System-to-Intermediate System (IS-IS) dynamic hostname and system ID mapping.

1.63.2 Command Mode

All modes

1.63.3 Syntax Description

instance-name	Optional. IS-IS instance name. Displays dynamic hostname and system ID mapping information for the only specified instance.

1.63.4 Default

When entered without specifying an IS-IS instance, this command displays dynamic hostname and system ID mapping information for all configured IS-IS instances.

1.63.5 Usage Guidelines

Use the **show isis dynamic-hostname** command to display IS-IS dynamic hostname and system ID mapping. For information about troubleshooting IS-IS, see *Troubleshooting IS-IS*.

Note: By default, most **show** commands (in any mode) display information for the current context only or, depending on the command syntax, for all contexts. If you are an administrator for the local context, you can insert the optional **context** *ctx-name* construct, preceding the **show** command, to view output for the specified context without entering that context. For more information about using the **context** *ctx-name* construct, see the **context** command description.

Note: By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information, see "*Modifying Output of show Commands*" in the document, *Using the CLI*.

Table 12 describes the output fields for the **show isis dynamic-hostname** command.

Table 12 Field Descriptions for the show isis dynamic-hostname Command

Field	Description
System ID	A 6-byte value that identifies an IS-IS system in the domain. The plus (+) symbol denotes the locally defined mapping.
Level	The level of the IS-IS routing domain.
Updated	The last time the dynamic hostname type-length-value (TLV) was presented in a link-state protocol data unit (LSP) of the system.
Hostname	The symbolic name advertised by the system.

1.63.6 Examples

The following example displays output from the **show isis dynamic-hostname** command:

```
[local]Redback>show isis dynamic-hostname

System ID              Level    Updated        Hostname

02aa.0002.0002         2        00:00:14       nyc-border3

02aa.0a00.0001+        2        00:00:22       wtn-core1


Total IS-IS Dynamic Hostname entries: 2
```

1.64 show isis interfaces

show isis [*instance-name*] [**multicast**] **interfaces** [*if-name*] [**intercontext** [*group-id*]] [**all**] [**detail**] [**extensive**]

1.64.1 Purpose

Displays information about Intermediate System-to-Intermediate System (IS-IS) interfaces.

1.64.2 Command Mode

All modes

1.64.3 Syntax Description

instance-name	Optional. IS-IS instance name. Displays information about interfaces for only the specified instance.
multicast	Optional. Displays multitopology IS-IS (M-ISIS) information.
if-name	Optional. Interface name. Displays information only for the specified interface.
intercontext	Optional. Displays IS-IS intercontext interfaces.
group-id	Optional. Group ID. If the *group-id* argument is specified, then only the IS-IS intercontext interfaces that belong to the intercontext group ID are displayed.
all	Optional. Displays IS-IS interface information for all contexts.
detail	Optional. Displays detailed IS-IS interface information.
extensive	Optional. Displays information about Label Distribution Protocol (LDP)-Interior Gateway Protocol (IGP) synchronization states.

1.64.4 Default

Provides summary information if no options are specified.

1.64.5 Usage Guidelines

Use the **show isis interfaces** command to display information about IS-IS interfaces.

The states displayed for LDP-IGP synchronization are as follows:

- Advertises maximum interface metric

- Advertises normal interface metric
- No LDP-IGP sync configuration
- LDP-IGP sync request sent
- LDP sync notification received

The display may show more than one state line.

Note: By default, most **show** commands (in any mode) display information for the current context only or, depending on the command syntax, for all contexts. If you are an administrator for the local context, you can insert the optional **context** ***ctx-name*** construct, preceding the **show** command, to view output for the specified context without entering that context. For more information about using the **context** ***ctx-name*** construct, see the **context** command description.

Note: By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information, see *Modifying Output of show Commands* in the document, *Using the CLI*. For information about troubleshooting IS-IS, see *Troubleshooting IS-IS*.

Table 13 describes the output fields for the **show isis interface** command.

Table 13 Field Descriptions for the show isis interface Command

Field	Description
Interface	Interface advertising the IS-IS.
L	Level 1 routing only (1), level 2 routing only (2), or levels 1 and 2 (3) routing.
MT	Multi-topology. Indicates whether each IS-IS instance performs unicast (U), multicast (M), or unicast and multicast (UM) topology-based routing. Displays no value when the default routing topology, unicast, is used.
State	IS-IS adjacency state.
Level-1-DR	IS-IS level 1 designated router (DR) for the interface.
Level-2-DR	IS-IS level 1 designated router (DR) for the interface.
Metric	Routing metric. A value inside the brackets is a multicast metric, and a value without brackets, or outside the brackets, is a unicast metric.

1.64.6 Examples

The following example displays output from the **show isis interfaces** command:

```
[local]Redback>show isis interfaces

IS-IS interface(s) for tag testbed:

Interface    L   MT  State  Level-1-DR        Level-2-DR         Metric

lo           3       Up     passive                              1

to-foo-10/   1p  UM  Up     up                                   10

to_dopey_1   3p      Up                                          10

to_dopey_4   3p      Up                       up                 10

to_pc6_7/2   3   UM  Up     sierra.01         sierra.01          10

to_pc7_7/2   3       Up     sierra.02         sierra.02          10
```

The following example displays output from the **show isis interfaces detail** command:

```
[local]Redback>show isis interfaces detail

IS-IS interface(s) for tag 1:

p2p

Up, level: 3, Ckt Id: 2, p2p, Ucast IP address: 13.13.13.2/24

mtu: 1500, speed 100000, Grid: 0x10000003, nh-id: 3, ckt 10/11

metrics[L1/L2]: v4 ucast[10/10]

GR Normal

Level Adjs Priority Hello Hold Auth Blocked Metric

3 1 64 2 30 10

Total IS-IS Interface(s): 2
```

The following example displays the IS-IS inter-context interfaces with group `30` in all contexts. The greater than symbol (>) indicates that the interface is an `intercontext` type:

```
[local]Redback>show isis int intercontext 30 all
```

```
Context   :local                          Context id  : 0x40080001
------------------------------------------------------------------
IS-IS interface(s) for tag test:
Interface    L   MT  State  Level-1-DR        Level-2-DR         Metric
blue         2 >     Up                       foo-target1.01     10

Total IS-IS Interface(s):   1

Context   :foo                            Context id  : 0x40080002
------------------------------------------------------------------
IS-IS interface(s) for tag testfoo:
Interface    L   MT  State  Level-1-DR        Level-2-DR         Metric
bluefoo      2 >     Up                       foo-target1.01     10

Total IS-IS Interface(s):   1
```

1.65 show isis protocol-summary

show isis [*instance-name*] **protocol-summary** [**l1** | **l2** | **level-1** | **level-2**]

1.65.1 Purpose

Displays Intermediate System-to-Intermediate System (IS-IS) protocol summary information.

1.65.2 Command Mode

All modes

1.65.3 Syntax Description

instance-name	Optional. IS-IS instance name. Displays protocol summary information for only the specified instance.
l1	Optional. Displays only IS-IS level 1 protocol summary information; see the "Usage Guidelines" section for more information on IS-IS levels.
l2	Optional. Displays only IS-IS level 2 protocol summary information; see the "Usage Guidelines" section for more information on IS-IS levels.
level-1	Optional. Displays only IS-IS level 1 protocol summary information; see the "Usage Guidelines" section for more information on IS-IS levels.
level-2	Optional. Displays only IS-IS level 2 protocol summary information; see the "Usage Guidelines" section for more information on IS-IS levels.

1.65.4 Default

Provides protocol summary information for all IS-IS instances on all levels.

1.65.5 Usage Guidelines

Use the **show isis protocol-summary** command to display IS-IS protocol summary information.

An autonomous system (AS) running IS-IS can be partitioned into multiple level 1 areas and a level 2 subset that interconnects all of the level 1 areas. Within each level 1 area, all routers exchange link-state information. Level 2 routers also exchange level 2 link-state information to compute routes between areas. You can use the **l1** or **level-1** keyword to show only level 1 information, or you can use the **l2** or **level-2** keyword to show only level 2 information.

Note: By default, most **show** commands (in any mode) display information for the current context only or, depending on the command syntax, for all contexts. If you are an administrator for the local context, you can insert the optional **context** ***ctx-name*** construct, preceding the **show** command, to view output for the specified context without entering that context. For more information about using the **context** ***ctx-name*** construct, see the **context** command description.

Note: By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information, see "*Modifying Output of show Commands*" in the document, *Using the CLI*. For information about troubleshooting IS-IS, see *Troubleshooting IS-IS*.

1.65.6 Examples

The following example displays output from the **show isis protocol-summary** command for the ip-trans IS-IS instance on the dynamic host (router), opt-core2:

```
[local]Redback>show isis ip-trans protocol-summary
```

```
  --- ISIS Instance: ip-trans / systemID: 1010.1010.c1c1(opt-core2) ---

Area  21.2425.2627.2829.3031.3233, level-1-2, metric short-wide, distance 115

Lsp   L1 total 14, pnode 7. local lsp total 1, pnode 0

      L2 total 26, pnode 10. local lsp total 2, pnode 0

Route isis total 104. level-1 87, level-2 17, interface route 23

      L2 redist route 0, leak route 87, summary route 0

SPF   L1 holddown 10, interval 5

         last time 00:01:25, duration 4, nodes 14, routes 87

      L2 holddown 10, interval 5

         last time 00:01:13, duration 10, nodes 21, routes 17

Adj   total 62, L1-LAN 20, L2-LAN 24, p2p 18

      last uptime 00:02:29, on intf to-edge1, neighbor 1010.1010.d1d1(opt-edge1)

Intf  total 24(down 1), LAN 4, p2p 20(down 1), passive 2

Time  router uptime 01d16h07, instance uptime 00:32:07
```

The previous example shows that the router has the following characteristics:

- The router runs level 1 and level 2 with both short and wide metric style.
- The router has 14 level 1 link-state protocol data units (LSPs), and 26 level 2 LSPs.
- The router has 104 IS-IS routes: 87 level 1 routes and 17 level 2 routes.
- 87 routes are leaked from level 1 into level 2 without summary information.
- The last Shortest Path First (SPF) calculation on level 1 was run one minute 25 seconds ago, with a duration of 4 milliseconds.
- There are 14 nodes in the level 1 area.
- The last level 2 SPF duration was 10 milliseconds, with 21 nodes and 17 routes.
- The router has 62 adjacencies: 20 level 1 LAN adjacencies, 24 level 2 LAN adjacencies, and 18 point-to-point adjacencies.

- The last “UP” adjacency was 2 minutes and 29 seconds ago on the interface named `to-edge1` from neighbor `opt-edge1`.

- The router has 24 IS-IS interfaces: 4 LAN interfaces and 20 point-to-point interfaces.

- The router has been up for 1 day 16 hours 7 minutes, and the IS-IS instance has been up for 32 minutes 7 seconds.

The following example displays output from the **`show isis protocol-summary`** command for the `new-net` IS-IS instance on the dynamic host (router), `opt-core2`:

```
[local]Redback>show isis new-net protocol-summary

  --- ISIS Instance: new-net / systemID: 0008.0008.0008(opt-core2) ---

Area  47.0008, level-1-2, metric wide-only, distance 115
Lsp   L1 total 1, pnode 0. local lsp total 1, pnode 0
      L2 total 4, pnode 1. local lsp total 2, pnode 1
Route isis total 4. level-1 1, level-2 3, interface route 1
      L2 redist route 0, leak route 1, summary route 0
SPF   L1 holddown 4, interval 2
         last time 00:02:14(periodic), duration 0, nodes 1, routes 1
      L2 holddown 4, interval 2
         last time 00:01:14(periodic), duration 0, nodes 3, routes 3
Adj   total 1, L1-LAN 0, L2-LAN 1, p2p 0
      last uptime 01d10h10, on intf to-e2, neighbor 1111.2222.3333(vpn-e2)
Intf  total 1, LAN 1, p2p 0
GR Enabled
Time  router uptime 11d03h12, instance uptime 12:42:22
```

This example shows that the router has the following characteristics:

- The router runs level 1 and level 2 with wide metric style only.
- The router has one level 1 LSP and four level 2 LSPs.
- The router has four IS-IS routes.
- The last level 1 SPF calculation was run two minutes and 14 seconds ago and was a periodic SPF.
- The last level 2 SPF calculation was run one minute and 14 seconds ago and was a periodic SPF.
- The router has one level 2 LAN adjacency that was up one day and 10 hours ago on interface `to-e2` with neighbor `vpn-e2`.
- The router has only one IS-IS interface on LAN.
- The router has IS-IS graceful restart enabled.
- The router has been up for 11 days 3 hours 12 minutes, and the IS-IS instance has been up for 12 hours 42 minutes 22 seconds.

1.66 show isis routes

show isis [*instance-name*] [**ipv4** {**unicast** | **multicast**} | **ipv6 unicast**] **routes** [[**l1** | **l2** | **level-1** | **level-2**] | *ip-addr* | *ip-addr/prefix-length* | **redistribute** [**l1** | **l2** | **level-1** | **level-2**] | **summary**]

1.66.1 Purpose

Displays Intermediate System-to-Intermediate System (IS-IS) routes.

1.66.2 Command Mode

All modes

1.66.3 Syntax Description

instance-name	Optional. IS-IS instance name. Displays information about routes for only the specified instance.
ipv4	Optional. Displays information about IP Version 4 (IPv4) routes.
unicast	Optional. Displays information about unicast routes.
multicast	Optional. Displays information about multicast routes. Not available with the **ipv6** keyword.
ipv6	Optional. Displays information about IP Version 6 (IPv6) routes.
l1	Optional. When used with the **routes** keyword, displays only IS-IS level 1 routes. When used with the **redistribute** keyword, displays only IS-IS level 1 routes redistributed from other routing protocols into the IS-IS domain, or leaked from other IS-IS levels.
l2	Optional. When used with the **routes** keyword, displays only IS-IS level 2 routes. When used with the **redistribute** keyword, displays only IS-IS level 2 routes redistributed from other routing protocols into the IS-IS domain, or leaked from other IS-IS levels.
level-1	Optional. When used with the **routes** keyword, displays only IS-IS level 1 routes. When used with the **redistribute** keyword, displays only IS-IS level 1 routes redistributed from other routing protocols into the IS-IS domain, or leaked from other IS-IS levels.
level-2	Optional. When used with the **routes** keyword, displays only IS-IS level 2 routes. When used with the **redistribute** keyword, displays only IS-IS level 2 routes redistributed from other routing protocols into the IS-IS domain, or leaked from other IS-IS levels.
ip-addr	Optional. Longest matched IS-IS route for the IP address. The IP address is specified in the form *A.B.C.D*.

ip-addr/prefix-length	Prefix length. Exactly matched IS-IS route for the IP address and prefix length. The IP address is specified in the form *A.B.C.D*. The range of values for the prefix length is 0 to 32.
redistribute	Optional. Displays IS-IS routes redistributed from other routing protocols into the IS-IS domain, or leaked from other IS-IS levels.
summary	Optional. Displays the number of routes that are summarized.

1.66.4 Default

Provides summary information about all IPv4 unicast routes if no options are specified.

1.66.5 Usage Guidelines

Use the **show isis routes** command to display IS-IS routes. If entered without any optional keywords, this command displays IPv4 unicast routes only.

Note: By default, most **show** commands (in any mode) display information for the current context only or, depending on the command syntax, for all contexts. If you are an administrator for the local context, you can insert the optional **context** *ctx-name* construct, preceding the **show** command, to view output for the specified context without entering that context. For more information about using the **context** *ctx-name* construct, see the **context** command description.

Note: By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information, see “*Modifying Output of show Commands*” in the document, *Using the CLI*. For information about troubleshooting IS-IS, see *Troubleshooting IS-IS*.

Table 14 describes the output fields for the **show isis routes** command using the *ip-addr/prefix-length* construct.

Table 14 Field Descriptions for the show isis routes Command

Field	Description
Prefix	IP prefix.
Level	IS-IS level.
Metric	Metric used to reach this prefix.
Interface	Interface used to reach this prefix.
Nexthop	IP nexthop used to reach this prefix.
LSP ID	Link state protocol data unit (LSP) ID that advertised this prefix.
Seq #	Sequence number of the LSP.

Table 14 *Field Descriptions for the show isis routes Command*

Field	Description
System Name	Router that advertised the LSP and prefix.
Arrive	Last time the system received this LSP.
Interface	Interface from which the last LSP arrived.

Table 15 describes the output fields for the **`show isis routes summary`** command.

Table 15 *Field Descriptions for the show isis routes summary Command*

Field	Description
Route Type	Route type. The route type can be IS-IS, redistributed, interarea, or summary.
Level-1	Number of routes, per route type, in level 1 area.
Level-2	Number of routes, per route type, in level 2 domain.
Summarize (L1/L2)	Number of routes, per route type, that are summarized in each level. The *x/y* output (for example, 0/1) indicates number of routes summarized in Level 1/ number of routes summarized in Level 2.
L2-to-L1 Leak	Number of IS-IS routes distributed from level 2 to level 1. These routes are not leaded on this system, but are leaked from level 2 into level 1 from other systems.

1.66.6 Examples

The following example displays output from the **`show isis routes`** command:

```
[local]Redback>show isis routes
```

```
IS-IS IP route(s) for tag 1

Prefix               L  Metric     Interface          Nexthop          Context

1.1.1.1/32           1  1          lo1                0.0.0.0

9.9.9.0/24           2  0                             0.0.0.0

10.14.200.10/32      2  63         2                  11.1.1.1

11.1.0.0/16          2  63                            0.0.0.0

12.1.0.0/16          1  10         to_vendridi        0.0.0.0

13.1.0.0/16          1  10         ix                 0.0.0.0

99.99.1.0/24         2  0                             0.0.0.0

99.99.2.0/24         2  0                             0.0.0.0

99.99.3.0/24         2  0                             0.0.0.0

99.99.4.0/24         2  0                             0.0.0.0

99.99.5.0/24         2  0                             0.0.0.0

99.99.6.0/24         2  0                             0.0.0.0

99.99.99.0/24        2  0                             0.0.0.0


Total IS-IS Route(s) for tag 1:    13
```

The following example displays output from the **`show isis ipv6 unicast routes`** command:

```
[local]Redback(config-ctx)#show isis ipv6 unicast routes

IS-IS ipv6 IP route(s) for tag 1

Prefix                L  Metric     Interface            Nexthop            Context

50:1:1::/64           2  1999       2                    fe80::290:69ff:

123:123::/64          2  1999       2                    fe80::290:69ff:

555:555::/100         2  0                               ::

666:666::/100         2  0                               ::

777:777::/100         2  0                               ::

888:888::/100         2  0                               ::

999:999::/64          2  0                               ::

2000:2001::/64        2  0                               ::

2000:2002::/64        1  0                               ::

8000:8001::1/128      2  1999       2                    fe80::290:69ff:

9000:9001::1/128      2  1999       2                    fe80::290:69ff:

fe00::/102            2  1999       2                    fe80::290:69ff:

Total IS-IS Route(s) for tag 1:     12
```

The following example displays output from the **show isis ipv4 multicast routes** command:

```
[local]Redback(config-ctx)#show isis ipv4 multicast routes

IS-IS  multicast IP route(s) for tag 1
Prefix               L  Metric     Interface          Nexthop            Context
11.1.0.0/16          2  2000       2                  0.0.0.0

Total IS-IS Route(s) (multicast) for tag 1:     1
```

The following example displays output from the **show isis routes redistribute** command:

```
[local]Redback>show isis routes redistribute

IS-IS Redistributed route(s) for tag A2-wtn, on Level-2
Prefix          L  Type  Source    Metric  M-Type   Summarized
23.4.5.6/32     2  Ext   static    4       Int
44.1.1.0/24     2  Ext   static    4       Int


Total IS-IS Redistributed Routes in level-2:     2
```

The following example displays output from the **show isis routes** command using the ***ip-addr/prefix-length*** construct:

```
[local]Redback>show isis routes 11.11.11.4/30
```

```
IS-IS prefix for tag test:

Prefix               Level  Metric   Interface    Nexthop

11.11.11.4/30        2      20       redback      192.168.1.5

  Is sourced from LSP(s):

  LSP ID                Seq #      System Name      Arrive(ago)  Interface(from)

  1111.2222.3333.00-01  0x4        ns-c1100         00:00:50     redback
```

The IP prefix `11.11.11.4/30` is a level 2 domain with a metric of `20`. The next hop for this prefix is the `redback` interface and the IP address is `192.168.1.5`. This prefix is advertised by system `ns-c1100` in LSP `1111.2222.3333.00-01`. This LSP has the sequence number of `0x4` and it arrived `50` seconds ago on the `redback` interface:

The following example displays output from the **`show isis routes`** command using the **`summary`** keyword:

```
[local]Redback>show isis routes summary


IS-IS route(s) summary for tag 1:

Route Type       Level-1    Level-2    Summarize(L1/L2)  L2-to-L1 Leak

IS-IS Route      3          10         -                 0

Redistribute     0          8          0/0

Inter-area       0          3          0/0

Summary Address  0          0          0/0

IS-IS interface routes: 3

Redistributed protocols: ospf static static
```

1.67 show isis spf-log

show isis [*instance-name*] [**ipv4 {unicast | multicast} | ipv6 unicast**] **spf-log** [**l1** | **l2** | **level-1** | **level-2**]

1.67.1 Purpose

Displays a history of the Intermediate System-to-Intermediate System (IS-IS) Shortest Path First (SPF) calculation results.

1.67.2 Command Mode

All modes

1.67.3 Syntax Description

instance-name	Optional. IS-IS instance name. Displays SPF information for only the specified instance.
ipv4	Optional. Displays the SPF events for IP Version 4 (IPv4) routing.
unicast	Optional. Displays the SPF events for unicast topologies.
multicast	Optional. Displays the SPF events for multicast topologies. Not available with the **ipv6** keyword.
ipv6	Optional. Displays the SPF events for IP Version 6 (IPv6) routing.
l1	Optional. Displays the SPF events for level 1 only.
l2	Optional. Displays the SPF events for level 2 only.
level-1	Optional. Displays the SPF events for level 1 only.
level-2	Optional. Displays the SPF events for level 2 only.

1.67.4 Default

Provides summary information about IS-IS SPF calculation results for both levels and all configured instances of IS-IS.

1.67.5 Usage Guidelines

Use the **show isis spf-log** command to display a history of the IS-IS SPF calculation results.

Note: By default, most **show** commands (in any mode) display information for the current context only or, depending on the command syntax, for all contexts. If you are an administrator for the local context, you can insert the optional **context** ***ctx-name*** construct, preceding the **show** command, to view output for the specified context without entering that context. For more information about using the **context** ***ctx-name*** construct, see the **context** command description.

Note: By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information, see "*Modifying Output of show Commands*" in the document, *Using the CLI*. For information about troubleshooting IS-IS, see *Troubleshooting IS-IS*.

Table 16 describes the output fields for the **show isis spf-log** command.

Table 16 Field Descriptions for the show isis spf-log Command

Field	Description
When	Time elapsed since the last SPF calculation took place.
Duration	Duration, in milliseconds, of an SPF calculation.
Nodes	Number of nodes involved in an SPF calculation.
Count	Number of times an SPF calculation was initiated.
Routes	Number of routes involved in an SPF calculation.
Last Trigger LSP	LSP ID that initiated the last SPF calculation.
Reasons	Reason for the last SPF calculation; see Table 17 for a list of explanations.

Table 17 describes the reasons and explanations for the **show isis spf-log** SPF recalculation.

Table 17 SPF Recalculation Reasons and Explanations

Reason ID	Explanation
ADMINDIST	The administrative distance was reconfigured.
AREASET	A set of areas was changed.
ATTACHFLAG	A Level 2 attachment has changed.
DISELECT	Designated IS (DIS) election was rerun.
IPRTLEAK	Routes were leaked between levels.
LOSTADJ	Adjacency has been lost.
LSPHEADER	An LSP header has changed.
NEWADJ	A new neighbor has come up.
NEWAREA	A new area has come up.

Table 17 SPF Recalculation Reasons and Explanations

Reason ID	Explanation
NEWLSP	A new LSP has arrived.
NEWMETRIC	A metric has changed.
OVLD	Overload.
PERIODIC REDIST	An internal LSP has been regenerated.
PREFIX	An SPF prefix has changed.
PURGELSP	An LSP was purged.
REDIST	A route was redistributed.
RTCLEARED	Routes were manually cleared.
TLVCONTENT	The content of an LSP changed.
TLVROUTES	An LSP route changed.
ADJNEXTHOP	A new next hop was added.
USERTRIG	The SPD recalculation was triggered by the user.
TOPOCHG	The network topology changed.
SYSCHG	The system ID changed.

1.67.6 Examples

The following example displays output from the **show isis spf-log** command:

```
[local]Redback>show isis spf-log

IS-IS tag 1 level 1 SPF ipv4(unicast)log:
When          Duration  Nodes  Count  Routes Last Trigger LSP   Reasons
00:08:55.327  1         1      1      0      Re-1.00-00         PERIODIC
(92)
22:35:47.653  0         1      2      0      Re-1.00-00         REDIST
22:36:02.734  0         1      1      0      Re-1.00-00         ATTACHFLAG
22:36:12.735  0         1      7      0      Re-1.00-00         NEWAREA
                                                                NEWLSP
                                                                PREFIX
                                                                SYSCHG
                                                                REDIST

IS-IS tag 1 level 2 SPF ipv4(unicast)log:
When          Duration  Nodes  Count  Routes Last Trigger LSP   Reasons
00:10:35.379  0         1      1      1      Re-1.00-00         PERIODIC
(92)
22:36:12.763  1         1      8      1      Re-1.00-00         NEWAREA
                                                                NEWLSP
                                                                PREFIX
                                                                SYSCHG
                                                                REDIST
```

1.68 show isis statistics

show isis [*instance-name*] **statistics** [**detail**]

1.68.1 Purpose

Displays Intermediate System-to-Intermediate System (IS-IS) traffic information.

1.68.2 Command Mode

All modes

1.68.3 Syntax Description

instance-name	Optional. IS-IS instance name. Displays traffic information for only the specified instance.
detail	Optional. Displays detailed traffic information.

1.68.4 Default

Provides summary information if no options are specified.

1.68.5 Usage Guidelines

Use the **show isis statistics** command to display IS-IS traffic information.

Note: By default, most **show** commands (in any mode) display information for the current context only or, depending on the command syntax, for all contexts. If you are an administrator for the local context, you can insert the optional **context** *ctx-name* construct, preceding the **show** command, to view output for the specified context without entering that context. For more information about using the **context** *ctx-name* construct, see the **context** command description.

Note: By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information, see "*Modifying Output of show Commands*" in the document, *Using the CLI*. For information about troubleshooting IS-IS, see *Troubleshooting IS-IS*.

1.68.6 Examples

The following example displays output from the **show isis statistics** command:

```
[local]Redback>show isis statistics

IS-IS Router: ip-backbone
System Id: 0003.0003.0003        Type: Level-1    SPF runs: 16
PDU Type      Received      Processed    Drops       Sent
LSP           25            18           7           16
IIH           1290          1216         74          721
CSNP          17            0            17          442
PSNP          0             0            0           0
Total         1332          1234         98          1179
                                 Type: Level-2   SPF runs: 16
PDU Type      Received      Processed    Drops       Sent
LSP           10            10           0           18
IIH           629           629          0           726
CSNP          0             0            0           453
PSNP          0             0            0           0
Total         639           639          0           1197

Total Received: 1971; Total Sent: 2376
```

1.69 show isis summary-address

show isis [*instance-name*] [{**ipv4** {**unicast** | **multicast**} | **ipv6 unicast**}] **summary-address** [**l1** | **l2** | **level-1** | **level-2**]

1.69.1 Purpose

Displays information about Intermediate System-to-Intermediate System (IS-IS) IP summary addresses.

1.69.2 Command Mode

All modes

1.69.3 Syntax Description

instance-name	Optional. IS-IS instance name. Displays information about summary addresses for only the specified instance.
ipv4	Optional. Displays information for IP Version 4 (IPv4) summary addresses.
unicast	Optional. Displays information for unicast summary addresses.
multicast	Optional. Displays information for multicast summary addresses.
ipv6 unicast	Optional. Displays information for IP Version 6 (IPv6) unicast summary addresses.
l1	Optional. Displays only information about level 1 summary addresses.
l2	Optional. Displays only information about level 2 summary addresses.
level-1	Optional. Displays only information about level 1 summary addresses.
level-2	Optional. Displays only information about level 2 summary addresses.

1.69.4 Default

Provides summary information if no options are specified.

1.69.5 Usage Guidelines

Use the **show isis summary-address** command to display information about IS-IS IP summary addresses.

Note: By default, most **show** commands (in any mode) display information for the current context only or, depending on the command syntax, for all contexts. If you are an administrator for the local context, you can insert the optional **context** ***ctx-name*** construct, preceding the **show** command, to view output for the specified context without entering that context. For more information about using the **context** ***ctx-name*** construct, see the **context** command description.

Note: By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information, see "*Modifying Output of show Commands*" in the document, *Using the CLI*. For information about troubleshooting IS-IS, see *Troubleshooting IS-IS*.

Table 18 describes the output fields for the **show isis summary-address** command.

Table 18 Field Descriptions for the show isis summary-address Command

Field	Description
Prefix	Summary address.
Level	IS-IS level to which the summary address is applied.
Metric	Metric used for the summary address.
Num-Routes	Number of more-specific routes that are suppressed by the summary address.
Active	Status flag that indicates whether the summary address is being used.

1.69.6 Examples

The following example displays output from the **show isis summary-address** command. In level 2, two summary addresses are displayed. The summary address `64.0.0.0/16` is not active. The summary address `44.1.0.0/23` is active and one route has an IS-IS metric of `3`:

```
[local]Redback>show isis summary-address
```

```
Total IS-IS Summary Addresses in level-1: 0
IS-IS Summary Addresses, on Level-2
Prefix             Level     Metric     Num-Routes   Active
64.0.0.0/16         2                    0
44.1.0.0/23         2         3          1            Y

Total IS-IS-Summary Addresses in Level 2: 2
```

1.70 show isis topology

show isis [*instance-name*] [{**ipv4** {**unicast** | **multicast**} | **ipv6 unicast**}] **topology** [**l1** | **l2** | **level-1** | **level-2**]

1.70.1 Purpose

Displays the Intermediate System-to-Intermediate System (IS-IS) topology information.

1.70.2 Command Mode

All modes

1.70.3 Syntax Description

instance-name	Optional. IS-IS instance name. Displays topology information for only the specified instance.
ipv4	Optional. Displays information for IP Version 4 (IPv4) topologies.
unicast	Optional. Displays information for unicast topologies.
multicast	Optional. Displays information for multicast topologies. Not available with the **ipv6** keyword.
ipv6 unicast	Optional. Displays information for IP Version 6 (IPv6) unicast topologies.
l1	Optional. Displays only IS-IS level 1 protocol summary information; see the “Usage Guidelines” section for more information on IS-IS levels.
l2	Optional. Displays only IS-IS level 2 protocol summary information; see the “Usage Guidelines” section for more information on IS-IS levels.
level-1	Optional. Displays only IS-IS level 1 protocol summary information; see the “Usage Guidelines” section for more information on IS-IS levels.
level-2	Optional. Displays only IS-IS level 2 protocol summary information; see the “Usage Guidelines” section for more information on IS-IS levels.

1.70.4 Default

None

1.70.5 Usage Guidelines

Use the **show isis topology** command to display IS-IS topology information.

An autonomous system (AS) running IS-IS can be partitioned into multiple level 1 areas, and a level 2 subset that interconnects all of the level 1 areas. Within each level 1 area, all routers exchange link-state information. Level 2 routers also exchange level 2 link-state information to compute routes between areas. You can use the **l1** or **level-1** keyword to show only level 1 information, or you can use the **l2** or **level-2** keyword to show only level 2 information.

Note: By default, most **show** commands (in any mode) display information for the current context only or, depending on the command syntax, for all contexts. If you are an administrator for the local context, you can insert the optional **context** ***ctx-name*** construct, preceding the **show** command, to view output for the specified context without entering that context. For more information about using the **context** ***ctx-name*** construct, see the **context** command description.

Note: By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information, see "*Modifying Output of show Commands*" in the document, *Using the CLI*. For information about troubleshooting IS-IS, see *Troubleshooting IS-IS*.

Table 19 describes the output fields for the **show isis topology** command.

Table 19 Field Descriptions for the show isis topology Command

Field	Description
System	System ID or dynamic hostname.
Distance	IS-IS metric to reach the system.
Routes	Number of IP prefixes advertised by the system.
IS	Number of IS neighbors advertised by the system.
Next-Hop	Next-hop router to reach the system.
Interface	Interface used to reach the system.
IP-Gateway	IP next-hop address used to reach the system.

1.70.6 Examples

The following example displays output from the **show isis topology** command:

```
[local]Redback>show isis topology
```

```
IS-IS ipv4 unicast topology for tag 1:
System         Distance Route     IS  Next-Hop       Interface IP-Gateway
samedi         0        6         0

Total level-1 IS-IS systems:   1

IS-IS ipv4 unicast topology for tag 1:
System         Distance Route     IS  Next-Hop       Interface IP-Gateway
m5-4           63       2         0   m5-4           2         11.1.1.1
samedi         0        17        1

Total level-2 IS-IS systems:   2
```

The following example displays output from the **show isis topology** command with the **ipv4** keyword:

```
[local]Redback>show isis ipv4 unicast topology

IS-IS ipv4 unicast topology for tag 6:
System         Distance Route     IS  Next-Hop       Interface IP-Gateway
dtse           20       3         2   dtse           5         5.5.5.1
sierra         30       4         0   dtse           5         5.5.5.1
samedi         0        2         1

Total level-1 IS-IS systems:   3
```

1.71 show ism circuit

show ism circuit [log|summary|*circ-handle-id* detail]

1.71.1 Purpose

Displays Interface and Circuit State Manager (ISM) circuit information.

Warning!

Use the **show ism circuit** command for debug purposes only to collect data when a problem or outage occurs at the customer node.

1.71.2 Command Mode

All modes (10)

1.71.3 Syntax Description

log	Optional. Displays circuit log information.
summary	Optional. Displays summary information for all circuits.
circ-handle-id detail	Optional. Displays detailed information for the specified circuit.

1.71.4 Default

None

1.71.5 Usage Guidelines

Use the **show ism circuit** command to collect data when a problem or outage is seen at the customer node. Because the output is intended for use by the support engineers, the format might differ from typical **show** command output and might not be readable.

1.71.6 Examples

The following example shows partial output for the **show ism circuit** command:

```
[local]Redback#show ism circuit
Circuit handle          Type    Hardware address  State Intf Bound

2/255:1023:63/1/0/1     Card    00:00:00:00:00:00 Up
2/1:1023:63/1/0/25      Port    00:30:88:14:0a:44 Up
2/1:1023:63/1/1/26      Circuit 00:30:88:14:0a:44 Up
2/1:1023:63/1/2/27      Circuit 00:30:88:14:0a:44 Up    to-core@adsl
2/1:1023:63/1/2/28      Circuit 00:30:88:14:0a:44 Up    lns@local
2/1:1023:63/1/2/29      Circuit 00:30:88:14:0a:44 Up    l2tp-tunnel@lns1
2/1:1023:63/1/2/30      Circuit 00:30:88:14:0a:44 Up    l2tp-tunnel@lns2
2/1:1023:63/1/2/31      Circuit 00:30:88:14:0a:44 Up    l2tp-tunnel@lns3
2/1:1023:63/1/2/32      Circuit 00:30:88:14:0a:44 Up    l2tp-tunnel@lns11
2/1:1023:63/1/2/33      Circuit 00:30:88:14:0a:44 Up    l2tp-tunnel@lns12
3/255:1023:63/1/0/1     Card    00:00:00:00:00:00 Down
3/1:1023:63/1/0/34      Port    00:00:00:00:00:00 Down
3/1:1023:63/1/1/35      Circuit 00:00:00:00:00:00 Down
6/255:1023:63/1/0/1     Card    00:00:00:00:00:00 Down
7/255:1023:63/1/0/1     Card    00:00:00:00:00:00 Up
7/1:1023:63/1/0/36      Port    00:30:88:22:52:43 Up
7/1:1023:63/1/1/37      Circuit 00:30:88:22:52:43 Up    mgmt@local

(continues...)
```

The following example shows partial output for the **show ism circuit log** command:

```
[local]Redback#show ism circuit log
Circuit handle          Type    Hardware address  State Intf Bound

2/255:1023:63/1/0/1     Card    00:00:00:00:00:00 Up
     1    CRD state  CRD attr      CSM/IFM
          ISM2_PVT_REASON_OK
          secs 1300998082, usecs 29930, Mar 24 20:21:22
     2    CRD state  CRD attr      CSM/IFM
          ISM2_PVT_REASON_OK
          secs 1301018267, usecs 111603, Mar 25 01:57:47
     3    CRD state  CRD attr      CSM/IFM
          ISM2_PVT_REASON_OK
          secs 1301018267, usecs 179258, Mar 25 01:57:47
     4    CRD state  CRD attr      CSM/IFM
          ISM2_PVT_REASON_OK
          secs 1301018267, usecs 283043, Mar 25 01:57:47
     5    CRD state  CRD attr      CSM/IFM
          ISM2_PVT_REASON_OK
          secs 1301018267, usecs 283115, Mar 25 01:57:47

(continues...)
```

The following example shows partial output for the **show ism circuit summary** command:

```
[local]Redback#show ism circuit summary
Circuit handle          Type    Hardware address  State Intf Bound

2/255:1023:63/1/0/1     Card    00:00:00:00:00:00 Up
2/1:1023:63/1/0/25      Port    00:30:88:14:0a:44 Up
2/1:1023:63/1/1/26      Circuit 00:30:88:14:0a:44 Up
2/1:1023:63/1/2/27      Circuit 00:30:88:14:0a:44 Up    to-core@adsl
2/1:1023:63/1/2/28      Circuit 00:30:88:14:0a:44 Up    lns@local
2/1:1023:63/1/2/29      Circuit 00:30:88:14:0a:44 Up    l2tp-tunnel@lns1
2/1:1023:63/1/2/30      Circuit 00:30:88:14:0a:44 Up    l2tp-tunnel@lns2
2/1:1023:63/1/2/31      Circuit 00:30:88:14:0a:44 Up    l2tp-tunnel@lns3
2/1:1023:63/1/2/32      Circuit 00:30:88:14:0a:44 Up    l2tp-tunnel@lns11
2/1:1023:63/1/2/33      Circuit 00:30:88:14:0a:44 Up    l2tp-tunnel@lns12
3/255:1023:63/1/0/1     Card    00:00:00:00:00:00 Down
3/1:1023:63/1/0/34      Port    00:00:00:00:00:00 Down
3/1:1023:63/1/1/35      Circuit 00:00:00:00:00:00 Down
6/255:1023:63/1/0/1     Card    00:00:00:00:00:00 Down
7/255:1023:63/1/0/1     Card    00:00:00:00:00:00 Up
7/1:1023:63/1/0/36      Port    00:30:88:22:52:43 Up
7/1:1023:63/1/1/37      Circuit 00:30:88:22:52:43 Up    mgmt@local

(continues...)
```

The following example shows partial output for the **`show ism circuit detail`** command:

```
[local]Redback#show ism circuit 255/11:5:18/1/2/24 detail
Circuit: 255/11:5:18/1/2/24, Len 64 (Circuit), state: Up, addr: 0xfffd2e4340
----------------------------------------------------------
interface bound   : l2tp-tunnel@lns12
bind type         : interface
admin state       : 0                 hardware address   : 02:01:11:22:52:43
media type        : ethernet          encap type         : ether-dot1q
mode type         : 0x1               port type          : link share dot1q
mtu size          : 1700              cfg mtu size       : 1700
ipv6 mtu size     : 1700              ipv6 cfg mtu size  : 1700
cct speed         : 10000000          cct rx speed       : 0
cct flags (attr)  : 0x0               cct flags2 (attr)  : 0x0
L3 proto flags    : 0x0               L3 proto valid     : NO
L3 v4 proto       : DISABLED          L3 v6 proto        : DISABLED
L3 v4 proto       : DOWN              L3 v6 proto        : DOWN
slot mask         : 0x102             parent slot mask   : 0x0

(continues...)
```

1.72 show ism global

`show ism global [complete log|dropped log|error log]`

1.72.1 Purpose

Displays global ISM information.

Warning!

Use the **`show ism global`** command for debug purposes only to collect data when a problem or outage occurs at the customer node.

1.72.2 Command Mode

All modes (10)

1.72.3 Syntax Description

`complete log`	Optional. Displays the complete event log.
`dropped log`	Optional. Displays dropped events only.
`error log`	Optional. Displays error events only.

1.72.4 Default

None

1.72.5 Usage Guidelines

Use this command to collect data when a problem or outage is seen at the customer node. Because the output is intended for use by the support engineers, the format might differ from typical **`show`** command output and might not be readable.

1.72.6 Examples

The following example shows partial output for the **`show ism global`** command:

```
[local]Redback#show ism global
Number of clients : 29

ISM Restarted              : FALSE
Receive EOF from IFM       : TRUE secs 1300998014, usecs 17596, Mar 24 20:20:14
Receive EOF from CSM       : TRUE secs 1300998013, usecs 976624, Mar 24 20:20:13
Processed EOF from IFM     : TRUE secs 1300998014, usecs 93010, Mar 24 20:20:14
Processed EOF from CSM     : TRUE secs 1300998014, usecs 75732, Mar 24 20:20:14
Receive EOF from all MBE's : TRUE secs 1300998023, usecs 610620, Mar 24 20:20:23
Receive EOF from all PPA's : TRUE secs 1300998023, usecs 648675, Mar 24 20:20:23
Sent EOF to all Clients    : TRUE secs 1300998023, usecs 674266, Mar 24 20:20:23
Sent EOF to all PPA's      : TRUE
Sent EOF to standby ISM    : TRUE
IFM download triggered     : TRUE
OK for client updates      : TRUE
CSM is alive               : TRUE
Signal sent to main        : TRUE

MBE EOF Timer started      : FALSE
Client EOF Timer started   : FALSE
MBE Wait Timer started     : FALSE
XC DONE Timer started      : FALSE
XC Switchover Processing   : FALSE
RCM Re-sync Sent           : FALSE secs 0, usecs 0, Jan 1 00:00:00
CSM Re-sync Sent           : FALSE
AAA XC Done Sent           : FALSE secs 0, usecs 0, Jan 1 00:00:00
RCM XC Done Sent           : FALSE secs 0, usecs 0, Jan 1 00:00:00
SNMP XC Done Sent          : FALSE
Table Version Wrap         : FALSE

(continues...)
```

The following example shows partial output for the **`show ism global complete log`** command:

```
[local]Redback#show ism global complete log

Log for: complete
Total events: 77312, EOF index: N/A

Idx  Hdrid Subid Len Data

  1      5     b  96 CCT state  SUB down cplt 255/16:1023:63/5/2/1171
  2-     6     e 404 CCT cfg    CCT cfg       255/16:1023:63/5/2/2797
  3      5     b  96 CCT state  SUB down cplt 255/16:1023:63/5/2/2797
  4-     6     e 404 CCT cfg    CCT cfg       255/16:1023:63/5/2/28
  5      5     b  96 CCT state  SUB down cplt 255/16:1023:63/5/2/28
  6-     6     e 404 CCT cfg    CCT cfg       255/16:1023:63/5/2/1187
  7      5     b  96 CCT state  SUB down cplt 255/16:1023:63/5/2/1187
  8-     6     e 404 CCT cfg    CCT cfg       255/16:1023:63/5/2/3613
  9      5     b  96 CCT state  SUB down cplt 255/16:1023:63/5/2/3613
 10-     6     e 404 CCT cfg    CCT cfg       255/16:1023:63/5/2/1221
 11      5     b  96 CCT state  SUB down cplt 255/16:1023:63/5/2/1221
 12-     6     e 404 CCT cfg    CCT cfg       255/16:1023:63/5/2/62
 13      5     b  96 CCT state  SUB down cplt 255/16:1023:63/5/2/62
 14-     6     e 404 CCT cfg    CCT cfg       255/16:1023:63/5/2/3567
 15      5     b  96 CCT state  SUB down cplt 255/16:1023:63/5/2/3567

(continues...)
```

The following example shows output for the **`show ism global dropped log`** command:

```
[local]Redback#show ism global dropped log

Log for: dropped
Total events: 0, EOF index: N/A

Idx  Hdrid Subid Len Data
```

The following example shows output for the **show ism global error log** command:

```
[local]Redback#show ism global error log

Log for: error
Total events: 3, EOF index: N/A

Idx  Hdrid Subid Len Data

  1      a    10 276 PRT cfg    PRT ethcfg    9/1:1023:63/1/0/38 (16) flag 0x2
  2      a    10 276 PRT cfg    PRT ethcfg    9/1:1023:63/1/0/38 (16) flag 0x2
  3      a    10 276 PRT cfg    PRT ethcfg    2/1:1023:63/1/0/25 (16) flag 0x2
```

1.73 show ism interface

show ism interface [log|summary|*interface-grid*|*interface-name*]

1.73.1 Purpose

Displays ISM interface information.

Warning!

Use the **show ism interface** command for debug purposes only to collect data when a problem or outage occurs at the customer node.

1.73.2 Command Mode

All modes (10)

1.73.3 Syntax Description

log	Optional. Displays interface log information.
summary	Optional. Displays summary information for all interfaces.
interface-grid	Optional. Displays information for the specified interface grid only.
interface-name	Optional. Displays information for the specified interface name only.

1.73.4 Default

None

1.73.5 Usage Guidelines

Use this command to collect data when a problem or outage is seen at the customer node. Because the output is intended for use by the support engineers, the format might differ from typical **`show`** command output and might not be readable.

1.73.6 Examples

The following example shows partial output for the **`show ism interface`** command:

```
[local]Redback#show ism interface
Interface: lns, state: Up, version: 422065
--------------------------------------------------
Primary IP          : 20.1.1.2/24
Grid                : 0x10000000    Ref IF grid       : 0x0
Context id          : 0x40080001
Node Flags          : 0x48          IP flags          : 0x1
IP calc mtu         : 1700          IP cfg mtu        : 0
DHCP relay sz       : 0             DHCP server IP    : 0.0.0.0
DHCPV6 server IP    : ::
DHCP svr grp        : 0x0
# of sec IP         : 0             # of bound ccts   : 3
# cct change q cnt: 0
ipv4: Ingress class map grid: 0
ipv4: Egress class map grid: 0
ipv6: Ingress class map grid: 0
ipv6: Egress class map grid: 0
TCP MSS ingress     : 0             TCP MSS egress    : 0

(continues...)
```

The following example shows partial output for the **`show ism interface log`** command:

```
[local]Redback#show ism interface log
Interface: lns, state: Up, version: 422065
--------------------------------------------------
Primary IP          : 20.1.1.2/24
Grid                : 0x10000000    Ref IF grid       : 0x0
Context id          : 0x40080001
Node Flags          : 0x48          IP flags          : 0x1
IP calc mtu         : 1700          IP cfg mtu        : 0
DHCP relay sz       : 0             DHCP server IP    : 0.0.0.0
DHCPV6 server IP    : ::
DHCP svr grp        : 0x0
# of sec IP         : 0             # of bound ccts   : 3
# cct change q cnt: 0
ipv4: Ingress class map grid: 0
ipv4: Egress class map grid: 0
ipv6: Ingress class map grid: 0
ipv6: Egress class map grid: 0
TCP MSS ingress     : 0             TCP MSS egress    : 0
     1    I/F state  I/F create    CSM/IFM
          ISM2_PVT_REASON_OK
          secs 1300998014, usecs 76240, Mar 24 20:20:14
     2    I/F state  I/F down      CSM/IFM
          ISM2_PVT_REASON_OK
          secs 1300998014, usecs 76271, Mar 24 20:20:14

(continues...)
```

The following example shows partial output for the **`show ism interface summary`** command:

```
[local]Redback#show ism interface summary
Interface: lns, state: Up, version: 422065
------------------------------------------------------
Primary IP        : 20.1.1.2/24
Grid              : 0x10000000    Ref IF grid       : 0x0
Context id        : 0x40080001
Node Flags        : 0x48          IP flags          : 0x1
IP calc mtu       : 1700          IP cfg mtu        : 0
DHCP relay sz     : 0             DHCP server IP    : 0.0.0.0
DHCPV6 server IP  : ::
DHCP svr grp      : 0x0
# of sec IP       : 0             # of bound ccts   : 3
# cct change q cnt: 0
ipv4: Ingress class map grid: 0
ipv4: Egress class map grid: 0
ipv6: Ingress class map grid: 0
ipv6: Egress class map grid: 0
TCP MSS ingress   : 0             TCP MSS egress    : 0

(continues...)
```

1.74 show ism linkgroups

show ism linkgroups

1.74.1 Purpose

Displays link group information for all interfaces.

Warning!

Use the **show ism linkgroups** command for debug purposes only to collect data when a problem or outage occurs at the customer node.

1.74.2 Command Mode

All modes (10)

1.74.3 Syntax Description

This command has no keywords or arguments.

1.74.4 Default

None

1.74.5 Usage Guidelines

Use this command to collect data when a problem or outage is seen at the customer node. Because the output is intended for use by the support engineers, the format might differ from typical **show** command output and might not be readable.

1.74.6 Examples

The following example shows partial output for the **show ism linkgroups** command:

```
[local]Redback#show ism linkgroups
255/6:5:18/1/1/17, lg_id 273, Ccct count 2, ifgrid 0x0, cct_hdr_flags 0x20,
min_links 1, max_links 8, rebalance off, num_active_ccct 2
 egress: none, hit model: hitless
  1: 2/1:1023:63/1/1/26, lg_id 273, ifgrid 0x0, cct_hdr_flags 0x40, active
  2: 9/1:1023:63/1/1/39, lg_id 273, ifgrid 0x0, cct_hdr_flags 0x40, active

255/11:5:18/1/2/18, lg_id 273, Ccct count 2, ifgrid 0x1000001e, cct_hdr_flags 0x20,
min_links 1, max_links 0, rebalance off, num_active_ccct 2
 egress: none, hit model: hitless
  1: 2/1:1023:63/1/2/27, lg_id 273, ifgrid 0x1000001e, cct_hdr_flags 0x40, active
  2: 9/1:1023:63/1/2/40, lg_id 273, ifgrid 0x1000001e, cct_hdr_flags 0x40, active

255/11:5:18/1/2/19, lg_id 273, Ccct count 2, ifgrid 0x10000000, cct_hdr_flags 0x20,
min_links 1, max_links 0, rebalance off, num_active_ccct 2
 egress: none, hit model: hitless
  1: 2/1:1023:63/1/2/28, lg_id 273, ifgrid 0x10000000, cct_hdr_flags 0x40, active
  2: 9/1:1023:63/1/2/41, lg_id 273, ifgrid 0x10000000, cct_hdr_flags 0x40, active

(continues...)
```

1.75 show isp-log

show isp-log

1.75.1 Purpose

Displays the contents of the ISP log file.

1.75.2 Command Mode

All modes

1.75.3 Syntax Description

This command has no keywords or arguments.

1.75.4 Default

None

1.75.5 Usage Guidelines

Use the **show isp-log** command to display the contents of the ISP log file.

Note: By default, most **show** commands (in any mode) display information for the current context only or, depending on the command syntax, for all contexts. If you are an administrator for the local context, you can insert the optional **context** ***ctx-name*** construct, preceding the **show** command, to view output for the specified context without entering that context. For more information about using the **context** ***ctx-name*** construct, see the **context** command description.

Note: By appending a space followed by the pipe (|) character at the end of a **show** command, you can filter the output using a set of modifier keywords and arguments. For more information, see *Modifying Output of show Commands* in the document, *Using the CLI*.

1.75.6 Examples

The following example displays output from the **show isp-log** command:

```
[local]Redback>show isp-log
16Dec21:10:002009user1;Upgrade;System;2010-01-25 19:32:22 UTC;Regular,
 6.3.1.1;Manual;3419857;
16Dec21:10:002009user1;Node_down;system;2010-01-25 19:32:24 UTC;;Manual;
3419858;
6.3.1.1;Node_up;system;2010-01-25 19:34:36 UTC;;Manual;119;
6.3.1.1;Hostname;System;2010-01-25 19:34:54 UTC;System1;Manual;138;
6.3.1.1;Hostname;System;2010-01-25 19:34:57 UTC;System2;Manual;141;
6.3.1.1;Proc_down;System;2010-01-25 19:36:38 UTC;System3;Manual;243;
6.3.1.1;Proc_up;System;2010-01-25 19:36:51 UTC;System3;Manual;256;
6.3.1.1;Linecard_down;System;2010-01-25 19:38:31 UTC;Slot 1,
atm-oc3e-8-port;Manual;356;
6.3.1.1;Linecard_up;System;2010-01-25 19:38:47 UTC;Slot 1,
atm-oc3e-8-port;Manual;371;
6.3.1.1;Cli_comment;CLI;2010-01-25 19:39:46 UTC;;Manual;431;This is an
 example comment from CLI;
6.3.1.1;Hostname;System;2010-01-25 19:40:35 UTC;System4;Manual;479;
6.3.1.1;Proc_down;System;2010-01-25 19:40:44 UTC;System3;Manual;488;
6.3.1.1;Hostname;System;2010-01-25 19:40:52 UTC;System2;Manual;496;
6.3.1.1;Proc_up;System;2010-01-25 19:40:56 UTC;System3;Manual;500;
6.3.1.1;Node_down;system;2010-01-25 19:41:20 UTC;;Manual;525;
6.3.1.1;Node_up;system;2010-01-25 19:43:31 UTC;;Manual;118;
6.3.1.1;Hostname;System;2010-01-25 19:43:49 UTC;System1;Manual;137;
6.3.1.1;Hostname;System;2010-01-25 19:43:51 UTC;System2;Manual;140;
[local]Redback#
```

1.76 show isp-log state

`show isp-log state`

1.76.1 Purpose

Displays information about the ISP log file.

1.76.2 Command Mode

All modes

1.76.3 Syntax Description

This command has no keywords or arguments.

1.76.4 Default

None

1.76.5 Usage Guidelines

Use the **`show isp-log state`** keyword to display information about the ISP log, including whether the ISP log is enabled, the size of the file, and the size limit.

Note: By default, most **`show`** commands (in any mode) display information for the current context only or, depending on the command syntax, for all contexts. If you are an administrator for the local context, you can insert the optional **`context`** ***`ctx-name`*** construct, preceding the **`show`** command, to view output for the specified context without entering that context. For more information about using the **`context`** ***`ctx-name`*** construct, see the **`context`** command description.

Note: By appending a space followed by the pipe (|) character at the end of a **`show`** command, you can filter the output using a set of modifier keywords and arguments. For more information, see *Modifying Output of show Commands* in the document, *Using the CLI*.

1.76.6 Examples

The following example displays output from the **`show isp-log state`** command:

```
[local]Redback>show isp-log state
Displaying ISP states:
             ISP Logging                    : Enabled
             File Size                      : 1618 bytes
             File Limit                     : 4096 bytes
             Number of Entries              : 18
             File Full?                     : FALSE
             Percent Full                   : 39%
```