Nortel Secure Router 4134

Release Notes — Software Release 10.0

NN47263-400 (323250-A)

Document status: Standard
Document version: 01.01
Document date: 28 August 2007

Contents

Secure Router 4134 Release Notes

The Release Notes for Secure Router 4134, Software Release 10.0, provide summary information on the following:

- features offered in this release
- capacities and limitations of the hardware and software
- the software file names and file sizes
- guidelines for using the Secure Router 4134
- related publications

Introduction

The Nortel Secure Router 10.0 release is for general use and is supported on the Secure Router 4134 platform only. The Secure Router 3120 and Secure Router 1000 Series do not support Release 10.0 software.

You use the Command Line Interface (CLI) to configure the Secure Router 4134. The Secure Router 4134 does not support a Graphical User Interface (GUI) in Release 10.0.

The Nortel Secure Router 4134 is a high-performance system that integrates multiple branch office functions (including routing, WAN, Ethernet switching, security, and Voice over IP [VoIP]) into a single device.

The Secure Router 4134 delivers the low latency and small packet throughput that real-time voice and multimedia applications demand. The Secure Router 4134 can support the demands of the integrated branch, and can also act as the regional or headquarters router for most enterprises: it can cost-effectively and securely concentrate traffic from hundreds of remote sites.

Software Release 10.0 is the initial release of the Secure Router 4134.

Secure Router 4134 Release 10.0 features

Hardware features

This section describes hardware features supported on Nortel Secure Router 4134, Software Release 10.0.

Chassis

- Two rack units high
- Mounts in a 19-inch rack
- Four small slots and three medium slots for hot swappable interface modules. Two medium slots can be converted to accommodate one Large Module.
- Supports Compact Flash cards and USB Flash drive storage devices

Power supplies

- Supports dual hot swappable power supply modules
- Power supply modules available in 250 W AC, 660 W AC (to support PoE), and 250 W DC

Interface modules

- Hot swappable interface modules
- Six Small Modules, seven Medium Modules, and one Large Module are available for Release 10.0. For detailed information on interface modules, see Nortel Secure Router 4134 Installation — Hardware Components (NN47263-301)

Software features

This section describes software features supported on Nortel Secure Router 4134, Software Release 10.0.

WAN

- Point-to-Point Protocol (PPP), including PPP over Ethernet (PPPoE)
- Frame Relay (including FRF.12 fragmentation)
- HDLC
- Bridge Control Protocol (BCP)
- Internet Protocol Control Protocol (IPCP)
- IPv6 Control Protocol (IPv6CP)
- MPLS Control Protocol (MPLSCP)

The Secure Router 4134 offers the following WAN interface modules:

- Serial
- Clear Channel DS3
- Channelized T3
- HSSI
- T1/E1
- ISDN PRI
- ISDN BRI

Multilink WAN support

- Multilink PPP (MLPPP)
- Multilink Frame Relay (MFR), including FRF.15 (end-to-end) and FRF.16 (UNI/NNI)
- Bonding of T1/E1, Serial, or DS3 interfaces

Ethernet switching

- LAN and MAC bridging
- Spanning Tree Protocol (STP) including Rapid and Multiple Spanning Tree Protocols (RSTP and MSTP)
- VLAN bridging, tagging, retagging, Generic VLAN Registration Protocol (GVRP)
- 802.3ad link aggregation
- 802.3af-2003 (PoE)
- VLAN-802.1Q tagging and forwarding, double tagging for VLAN stacking
- VLAN classification
- IGMP Snooping

Layer 3

- IPv4 and IPv6 support, including support for IPv4/IPv6 tunneling
- Static routing, RIPv1/2, RIPng for IPv6, OSPFv2 and v3, BGP4/4+
- Policy-based routing
- Inter-VLAN routing (IPv4 only)
- High availability: VRRP, redundant router connections
- ACL, NAT, tunneling (GRE, IPIP, IPv6 over IP, IPv6 over GRE, Auto6to4)
- MPLS-Martini Pseudo-Wire

- RSVP-TE, LDP, OSPF-TE extension, and static LSP

Quality of Service/traffic management

- RED, WRED, DiffServ, bandwidth guarantee/sharing, flow monitoring
- Traffic policing
- 8-level priority class based queuing (per IP address/subnets, ports, DSCP and ToS bits, VLAN ID (802.1q), VLAN priority (802.1p)
- Frame Relay traffic shaping and policing

Firewall

- Stateful packet inspection firewall
- 25-zone support (including corporate, Internet, DMZ)
- Policy-based NAT/PAT
- 60+ distributed Denial of Service (DDoS) attack preventions
- 30+ application level gateway support (including SIP)
- PPP over Ethernet (PPPoE)

VoIP-friendly features

- Low-latency packet forwarding
- SIP application level gateway for NAT and firewall
- Cone NAT (for Nortel Unistim protocol) with NAT hairpinning
- Frame Relay fragmentation (FRF.12)
- Compressed RTP (cRTP)

Security (without High Performance bi-directional VPN encryption Internal Module)

- SSH server support for secure configuration
- 802.1X authentication of clients
- Generalized Packet Filter for IPv4 on any port
- Hardware accelerated IPv4/IPv6 Packet Filters on Ethernet module cards

Security (with High Performance bi-directional VPN encryption Internal Module)

- IPsec VPN with hardware acceleration
- IKE authentication through Pre-Shared-Key or Digital Signature with RSA or DSA

- Cryptographic support for DES, 3DES, AES-128, AES-192, AES-256, MD5, SHA1, and DH groups 1, 2, and 5
- L2TP+IPsec (RFC 3193) remote access server
- PKI certificate and key management with enrollment using "cut-and-paste" PEM, or SCEP
- IPsec protection of GRE/IPIP tunnels

IP multicast

- IGMPv1/2/3 for IPv4; MLDv1/2 for IPv6
- PIM-SM for IPv4/v6
- DVMRPv3 for IPv4

Service provisioning

- Management Telnet, SSHv2, SFTP, PAP, CHAP, SNMPv2, Syslog, DHCP, RADIUS, TACACS+, TCL scripting support
- Monitoring syslog, statistics, alarm
- Diagnostics BERT, loopback testing, trace route, packet capture

Default settings

The default settings are as follows:

- Telnet server is disabled
- Telnet client is enabled
- TFTP server is disabled
- FTP server is disabled
- SSH server is disabled
- SNMP is disabled

Use the Command Line Interface (CLI) to change default settings.

Memory requirements

The Secure Router 4134 supports two Compact Flash card storage devices and one USB Flash drive device.

USB Flash drives

The USB Flash drive connector is located on the rear panel of the Secure Router 4134. The USB Flash drive is identified in the system as /usb0. The USB Flash drive is hot-swappable. The Secure Router 4134 supports USB

Flash drives manufactured by Nortel-qualified vendors only. You can use devices with a size of 16 MB to 1 GB only. Specifically, Nortel supports the following USB storage devices:

- Sandisk: 64MB, 128MB, 256MB, 512MB, 1GB
- Sandisk U3: 512MB, 1GB
- Kingston: 512MB, 1GB
- PNY: 256MB, 512MB
- Memorex: 256MB

ATTENTION

If file operations on your USB flash device fail when used on the Secure Router 4134, format the USB device using the Secure Router 4134. Ensure you back up your data before formatting.

Compact Flash cards

The Secure Router 4134 has one external Compact Flash drive and one internal Compact Flash drive. The internal device is identified in the system as /cf0; the external device is identified in the system as /cf1.

ATTENTION

Only the external Compact Flash device is hot-swappable. Do not open the Secure Router 4134 service access panel while the unit is powered. The internal Compact Flash card is not hot-swappable.

The Secure Router 4134 supports Compact Flash devices manufactured by Nortel-qualified vendors only. Specifically, Nortel supports the following Compact Flash cards:

- Sandisk: 128MB, 256MB, 512MB, 1GB, 2GB
- Sandisk Ultra-II: 512MB, 1GB
- Kingston: 512MB, 2GB
- White Electronics: 128MB (default CF)

Software upgrade process

The Nortel Secure Router Release 10.0 is only supported on the Secure Router 4134. The Release 10.0 software is located on the CD and on the Nortel Technical Support Web site.

Table 1
Secure Router 4134 software images

Description	File size (bytes)	Version	File name
Secure Router application image	15 275 682	10.0 (r10.0)	SR4134.Z

The MIBs file for release 10.0 is SR4134_R10.0MIBs.zip.

Upgrading software on the Secure Router 4134

ATTENTION
The Telnet and FTP servers are disabled by default in Release 10.0 software.

ATTENTION
Although the Secure Router 4134 supports TFTP, Nortel recommends that you use an FTP server when upgrading software.

For Secure Router 4134, Release 10.0, the software image file and boot image file are contained within one file. The image file name is SR4134.Z. You can load an image file to a Nortel Secure Router 4134 from any of the following devices:

- accessible FTP server
- external USB Flash drive
- external Compact Flash card

The Nortel Command Line Interface (CLI) provides commands that allow you to upgrade the Secure Router 4134 with new software, to verify that the file has successfully loaded, and to specify the location of the image file from which the router boots.

The Secure Router 4134 supports two or more software versions (dependent on the capacity of the storage device). However, the software image file name for every version is SR4134.Z. To avoid overwriting a previous version of software, you must rename the old version of software before downloading the upgrade software version.

If you download the image file from the Nortel Support Web site to an FTP server, you can use the **`file download`** command to load the image to the Secure Router 4134. If you download the image file from the Nortel Support Web site to a USB Flash drive or Compact Flash card, use the **`file copy`** command to load the image file to the Secure Router 4134.

ATTENTION

If you experience any issues with a downloaded file (incomplete or corrupt file), begin the download process again.

Upgrading software

ATTENTION

Nortel recommends that you create a backup file containing your router configuration before upgrading software.

The procedure in this section describes the basic steps to follow to upgrade your Secure Router 4134 software.

Procedure steps

Step	Action
1	Create a backup copy of your router configuration by saving the configuration file to a TFTP or FTP server, a USB Flash drive storage device, or an external Compact Flash card storage device.
2	Download the image file from the Nortel Support page (www.nortel.com/support), placing it on a USB Flash drive, or on a Compact Flash card, or on a server that is running a TFTP daemon.
3	Ensure that network connectivity exists between the Secure Router being upgraded and the FTP server, if you use that option. You can ping the server from the Secure Router to prove connectivity.
4	Download the image file (SR4134.Z) from the FTP server to the internal Compact Flash card (cf0), or copy the file from an external USB Flash drive or Compact Flash card to cf0.
5	Reboot the Secure Router.

—End—

Example of upgrading software on the Secure Router 4134 using an FTP server and overwriting the existing image

In this example, a version of the SR4134.Z software image file already exists on the internal Compact Flash card. When you update a new version of the software, it overwrites the version on the card, unless you first re-name the older version of the software.

Use this procedure to copy the software image file from an FTP server to the Secure Router 4134 internal Compact Flash card.

Procedure steps

Step	Action
1	Create a backup copy of your router configuration by saving the configuration file to a TFTP or FTP server, a USB Flash drive, or an external Compact Flash card storage device.
2	Download the image file from the Nortel Support page (www.nortel.com/support), placing it on an FTP server.
3	From the root of the CLI, enter file mode: `SR4134# file`

4	To download the software image file, enter:
	`SR4134/file# download <ftp ipaddr> SR4134.Z /cf0/SR4134.Z mode image`
	The Secure Router 4134 sends a message indicating it has received your request:
	`Handling tftp request !`

5	At the prompt, enter **y** to continue to download the file: `Continue with the download ? (y/n) : y`

6	The Secure Router 4134 returns a message, and again requests your input to proceed:
	`WARNING:`
	`Do not remove the Compact Flash during this process`
	`Do not reboot this device during this process`
	`Note that copying files may take 3 – 5 minutes per megabyte`
	`Proceed(y/n)? y`

7	The Secure Router 4134 returns a message indicating that the file already exists on /cf0, and requests input to proceed: `Destination file '/cf0/SR4134.Z' exists, overwrite ? (y/n) : y`

8 The Secure Router 4134 returns a message while transferring the file, and indicates when the download is complete:

```
Download in progress...
Loading [100]
Loading [100]
Download successful
```

9 To exit the file menu and reboot the Secure Router 4134, enter:

```
SR4134/file# exit
SR4134# reboot
```

—End—

Example of upgrading software on the Secure Router 4134 using an external Compact Flash card or USB Flash drive

The following procedure uses an external USB for loading the image file to the internal Compact Flash. If you choose to use an external Compact Flash for loading the image to the Secure Router, the procedure is the same, except the location from which to copy the file is identified as /cf1/.

Procedure steps

Step	Action
1	Create a backup copy of your router configuration by saving the configuration file to a TFTP or FTP server, a USB, or an external Compact Flash card.
2	Download the image file from the Nortel Support page (www.nortel.com/support), placing it on a USB storage device.
3	From the root of the CLI, enter file mode: `SR4134# file`
4	To copy the software image file to the internal Compact Flash, enter: `SR4134/file# copy /usb0/SR4134.Z /cf0/SR4134.Z`

5	The Secure Router 4134 returns a message, and requests your input to proceed:
	`WARNING:`
	`Do not remove the USB device during this process`
	`Do not reboot this device during this process`
	`Note that copying files may take 3 - 5 minutes per megabyte`
	`Proceed(y/n)? y`

6	The Secure Router 4134 returns a message, and requests your input to proceed:

```
WARNING:
Do not remove the Compact Flash device during this
process
Do not reboot this device during this process
Note that copying files may take 3 - 5 minutes per
megabyte
Proceed(y/n)?  y
```

7 The Secure Router 4134 returns a prompt when the file is copied to the internal Compact Flash card.
Enter the list command to verify the file copied successfully:
`ls cf0`
The router returns a warning message, and lists the contents of the Compact Flash card:

```
WARNING:
Do not remove the Compact Flash during this
process
Do not reboot this device during this process
CONTENTS OF /cf0:

     size          date          time          name
  ----------    ----------    ----------    ----------
  15112338     APR-27-2007    18:47:02      SR4134.Z
```

8 To exit the file menu, enter:
`SR4134/file#` **`exit`**

9 To reboot the Secure Router 4134, enter:
`SR4134#` **`reboot`**

—End—

Using SSH

To generate a key and enable SSH, use the procedures in this section.

Procedure steps

Step	Action
1	To access configuration mode, enter: **`configure terminal`**
2	To access the SSH key generation subtree, enter: **`ssh_keygen`**
3	To generate the DSA key, enter: **`generate dsa`**

4 To generate the RSA key, enter:
```
generate rsa
```

5 To enable the SSH connection, enter:
```
ssh_server
enable
```

6 Save the configuration:
```
save local
```

—End—

Supported software and hardware capabilities

The following table lists some of the supported software and hardware capabilities for Secure Router 4134 Software Release 10.0. For additional scaling information and design guidelines, please contact your Nortel representative.

Table 2
Hardware and software capabilities

Feature	Maximum number supported
Ethernet Ports:	
Gigabit	58
Fast Ethernet	72
PoE	72* *This is the maximum number of Power over Ethernet (PoE) ports supported. For detailed information on PoE power distribution and the number of PoE ports and powered devices that the Secure Router 4134 can support, see Secure Router 4134 Configuration — Layer 2 Ethernet (NN47263-501).
T1/E1 ports	31
DS3 ports	3
CT3 ports	3
HSSI ports	3
Serial ports	7
ISDN BRI (U/ST) ports	7
SSH sessions	5
FTP sessions	4
TFTP sessions	3

Feature	Maximum number supported
Telnet sessions	15
DHCP: leases relay agents	 4000 255
VLANs	4000, up to 16 000 with VLAN stacking **Note:** The range for VLAN IDs is 1- 4000. VLAN 1 is the default VLAN, which cannot be deleted.
VLAN terminated interfaces	256
Dynamic VLANs (GVRP)	1000
VPN tunnels	1000 (with optional crypto card)

Supported SFPs

The Secure Router 4134 software, Release 10.0, supports the Small form-factor Pluggable (SFP) transceivers described in the following table.

Table 3
Supported SFPs

Nortel product code	Wavelength	Description	Manufacturer
AA1419048-E6	850 nm	FO, XCVR, SFP, MM, 1 GBE-SX, 850 nm, DDI, BAIL	Finisar FTLF8519P2BNL-N2
AA1419049-E6	1310 nm	FO, XCVR, SFP, SM, 1 GBE-LX, 1310 nm, DDI, BAIL	Avago AFCT-5715PZ-NT1

For detailed information about the SFPs, see Nortel Secure Router 4134 Installation — SFPs (NN47263-303).

Jumbo frame support

The Secure Router 4134 supports jumbo frames.

ATTENTION

The Secure Router 4134 management Ethernet interface (FE 0/0) on the rear panel does not support jumbo frames. Therefore, the management port Maximum Transmission Unit (MTU) can be configured with a value in the range of 64 to 1500 bytes.

Use the procedure in this section to configure the Secure Router 4134 system settings to support jumbo frames.

Procedure steps

Step	Action
1	To access configuration mode, enter: `configure`
2	To configure the system settings to support jumbo frames, enter: `system jumbo-mtu-limit <value>`
3	Reboot the system.

—End—

Table 4
Variable definitions

Variable	Value
<value>	Valid values for the jumbo MTU limit are 1500 and 9216 bytes. The default value is 1500 bytes.

SNMP MIBs

The Secure Router supports various SNMP standards defined by the RFC documents published by the Internet Engineering Task Force (IETF). The Secure Router also supports a set of enterprise-defined MIBs, which ensures compatibility with existing network management tools. For detailed information about SNMP standards and MIBs supported in Release 10.0, refer to Nortel Secure Router 4134 Configuration — Network Management (NN47263-602).

Known issues, limitations, and guidelines

The following table describes issues and limitations known to exist in the Secure Router 4134 Software Release 10.0, and provides guidelines for using Release 10.0 software.

Table 5
Known issues and limitations

Change Request	Subsystem	Description
Q01684695	802.1x	Dot1x : Port remains in down state if configured as “Force Authorized” and it is administratively shut down (shutdown) and brought back up (no shutdown).

Change Request	Subsystem	Description
		There are two workarounds for this issue: • Enabling Force Authorized option on an interface is the same as disabling Dot1x on that interface. For this reason the preferred workaround is to disable Dot1x by using **`no dot1x enable`** command. • Set port control first to force-unauthorize and then to force-authorize.
Q01562527	CLI	Help string "bgp dampening <half life timer>?" is not showing relevant information. The "bgp dampening <half life timer>?" help string now displays relevant information. However, you may encounter this issue with other commands, such as the **`ip route`** command.
Q01678631	cRTP	cRTP and MLPPP issue CRTP may not work on MLPPP bundles for the following reasons: cRTP has a 4-bit sequence number in each compressed packet. If the sequence number mismatch is detected at the receiver end, it is dropped and a context-state packet is sent to the compressor. In the case of MLPPP bundles, the differential delay between constituent links can result in the cRTP packets being delivered out of order. This out of order delivery results in packets being dropped at the receiver.
Q01680944	DHCP	SR4134 10.0 cannot configure DHCP Relay under VLAN DHCP relay is not supported on VLAN interfaces. Other features in Release 10.0 that are not supported on VLAN interfaces include the following: • routing protocols • firewall • AAA
Q01673884	DHCPv6	DHCP v6 server preference shows a negative value The preference value for enabling a server, when configured with the rapid-commit option, is displayed as -1 in the **`show`** command (irrespective of the value given in the server CLI), which indicates that the preference option is not set in the packet. This happens because the rapid-commit takes the higher precedence between the two and preference is not set when both are configured simultaneously.

Change Request	Subsystem	Description
Q01582735	DS3	Test running in DS3 gets deactivated when the test is run/stop in Cisco When you connect a Secure Router 4134 DS3 interface to a Cisco device (for example, the Cisco 7206), and run a BERT test on both devices simultaneously, the BERT test on the Secure Router 4134 stops. This applies to the loopback test, as well. Workaround: To run BERT and loopback tests successfully, you must first run the test on the Cisco device, and then run the test on the Secure Router 4134.
Q01685793	Firewall	Connection-reservation for an IP address is not configurable Firewall does not allow you to reconfigure the connection-re servation limit for a particular IP address. To reconfigure the connection-reservation, remove the current reservation limit by using **`no connection-reservation`**, and then configure the new reservation limit. Although the firewall shows the maximum connection limit that you can configure using connection-reservation for a particular firewall map and IP address to be 2500, it supports only up to 2499.
Q01679657	Firewall	SIP trunk is not supported on plain Firewall policies. SIP trunk is not supported with firewall policies without NAT.
Q01638787	FR	Interoperability issues for FRF20 with Cisco The Secure Router 4134 cRTP implementation adds 16 bit CIDs in the FULL HEADER packet. Cisco receives this and returns 8 bit CIDs in the packets from the Cisco unit to the Secure Router. This is an error from the Cisco side as it should accept both 8 and 16 bit CIDs.
Q01645692	GVRP	With GVRP, if the first 1000 learned VLANs are deleted, on relearning the next 1000 VLANs, some VLANs flap After learning the first 1000 VLANs using GVRP, learning of additional VLANs in different ranges might not occur. If you observe this scenario, first disable GVRP globally on both the DUTs and then re-enable it. Assume a simple two nodes topology as shown below: DUT1 ---------- DUT2 DUT1 advertises 1000 VLANs (for example, VLANs 1–1000) to DUT2. If the 1000 VLANs are then deleted from DUT1 and a new, but different, set of 1000 VLANs is created on DUT1 (for example,

Change Request	Subsystem	Description
		VLANs 1001-2000), the new VLANs may not be learned on DUT2. However, if the newly added VLANs are the same as the deleted ones (for example, 1-1000), then DUT2 relearns them.
Q01680411	ISDN	Bundle will remain up even after shutting down the bundle when there are incalls This behavior depends on when you issue the **shut** command on the ISDN bundle. If all links in the bundle are up, the **shut** command brings down all the links and the bundle. If you issue the **shut** command on the ISDN bundle when there are incoming calls, a few links are in the up state and the remaining links are in the down state—this can result in unpredictable behavior. Issue the **shut** command on the ISDN bundle when all the links are up.
Q01590257	NAT	Cannot configure nat-failover on tunnel interfaces The Secure Router 4134 does not support the configuration of a tunnel interface as the secondary interface for a NAT failover of a primary interface.
Q01567026	PBR	Fragmentation of traffic does not happen with PBR enabled on a module This is a Release 10.0 design limitation. For packets coming in on module LAN interfaces, PBR does not work when the packets must be fragmented.
Q01619303	PIM-SM6	PIM-SM6 interoperability with Cisco fails for BGP+ routes Currently, BGP supports only Unicast Subsequent Address Family Identifier (SAFI), and does not support Multicast SAFI. Because there is no Multicast SAFI support, commands such as **address-family (ipv4/ipv6/all) multicast** are not supported, while **address-family (ipv4/ipv6/all) unicast** is supported. BGP Multicast SAFI functionality and use: Normally, BGP carries two sets of routes: one set for unicast routing and one set for multicast routing. The routes associated with multicast routing are used by Protocol Independent Multicast (PIM) to build data distribution trees. BGP multicast address family support allows you to have a unicast routing topology different from a multicast routing topology, giving you more control over the network and resources. Additional info can be found from: http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120t/120t7/mbgp.htm

Change Request	Subsystem	Description
Q01563009	Platform	When save local is executed with large configurations, a longer response time is observed If you use the **`save local`** command to save a large configuration (for example, you have at least 255 FR bundles), it can take up to an hour to save the file.
Q01720768	PoE	Incorrect LED display for Power Supply 0 (PS0) A problem may be seen with incorrect or no LED status on the second 660 watt AC power supply (PoE) when two power supplies are inserted and the system is brought up. This does not occur with the regular 250 watt AC power supply. Workaround: To avoid this issue, you can hot insert the PoE power supply. If you bring up the system with a PoE power supply installed and there is incorrect LED activity, pull out the power supply and reinsert it.
Q01687503	PPP	IPv6CP does not come up if first link configured in the MLPPP bundle is down. When links are added to the MLPPP bundle and the first link is down, IPv6CP does not come up. Workaround: Use the shut/no-shut command sequence to re-trigger IPv6CP on the bundle.
Q01677561	PPP	Additional DS0s in a fractional single link MLPPP bundle are not allowed. The Secure Router 4134 does not support this combination.
Q01645589	QoS	Hardware does not perform metering in certain scenarios unless CIR is reset to 30Kbps The following two scenarios are known scenarios in which the metering for srTCM does not happen: Scenario 1: 1. Configure Policer with billing/accounting enabled. 2. Configure trtcm with CIR = PIR = 400000 Kbps and CBS=PBS=99968 Bytes (trTCM metering works fine) 3. Delete trtcm configuration with "no trtcm 400000 400000" command

Change Request	Subsystem	Description
		4. Configure srtcm with CIR=400000 Kbps and CBS=EBS=99968 Bytes (No metering happens. All packets are either green or yellow. There are no red packets.) Scenario 2: 1. Configure Policer with billing/accounting enabled. 2. Configure srTCM with CIR=13Kbps, CBS=1625Bytes and EBS=3250Bytes (Policing works fine — limits traffic to 13 Kbps.) 3. Update srTCM config with CIR=70000 Kbps, CBS=EBS=100000 Bytes (Policing does not happen.) Workaround: In the above two scenarios, when you reset srTCM with CIR=30Kbps and then configure the error scenario steps (step 4 in scenario 1 and step 3 in scenario 2), the policing functionality works fine. Use as the workaround for proper policing functionality.
Q01656954	QoS	In color-aware mode, the Ethernet module QoS policer drops all ingress packets With Ethernet module QoS, the current implementation does not derive the color from the DSCP value in the packet while doing the color aware policing. It derives the previous color from the Drop Precedence (DP) assigned by the previous stages of the packet processing. Drop precedence can be derived for a traffic flow by assigning the flow with the required DP based on matching criteria. For example to derive the drop precedence for the AF classes the following configuration can be done for proper functioning of color-aware policing:

Change Request	Subsystem	Description
		policy-map policy-1 class-map afx1 police srtcm 30 cbs 30 ebs 60 color-aware exit police match ipv4 dscp af11 match ipv4 dscp af21 match ipv4 dscp af31 match ipv4 dscp af41 assign-drop-precedence low exit class-map class-map afx2 police srtcm 20 cbs 20 ebs 40 color-aware exit police match ipv4 dscp af12 match ipv4 dscp af22 match ipv4 dscp af32 match ipv4 dscp af42 assign-drop-precedence medium exit class-map class-map afx3 police srtcm 10 cbs 10 ebs 20 color-aware exit police match ipv4 dscp af13 match ipv4 dscp af23 match ipv4 dscp af33 match ipv4 dscp af43 assign-drop-precedence high exit class-map exit policy-map

General guidelines and considerations

The following table provides information to assist you with the configuration of Secure Router 4134 features.

Table 6
General guidelines and considerations for the Secure Router 4134

Subsystem	Description
cRTP	When cRTP is disabled on the bundle and if the peer system is also a Secure Router product, then cRTP must also be disabled on the peer-router (that is, the Secure Router acting as peer).
Firewall	In the case of a Network Address Translation (NAT) failover configuration, if a hotswap operation is performed on the primary interface (using "shut" command under the "module" tree), the secondary interface fails to handle the NAT traffic.
IGMP Snooping	When IGMP Snooping is globally disabled, the IGMP messages received by the Secure Router 4134 are flooded to all the ports. If you enable IGMP Snooping on a VLAN after globally disabling that feature, IGMP messages are not properly flooded to LAG and module Ethernet interfaces. Workaround: Enable IGMP Snooping globally and then disable IGMP Snooping globally. This restores the flooding of IGMP messages to the ports.
LDP	The IP address of inactive interfaces can inadvertently be used as the transport address of an LDP session, causing failure in establishing the LDP session. Workaround: Explicitly configure the transport address of LDP as the Loopback IP address.
ECMP with LDP	To use ECMP with LDP, you must configure all interfaces used in ECMP with "mpls protocol-ldp".
Platform	The **`attstats`** selection is now removed from the **`show module`** submenu. Nortel no longer supports AT&T stats reporting.
RMON	A hardware issue is preventing the acquisition of "drop event counter" information.
SNMP	You must disable memory protection before accessing shell-related commands.
IPv4/IPv6 traps	Administratively shutting down PPP bundle with IPv6 address does not trigger a trap. When a WAN (bundle) interface is ADMIN down, in a normal scenario, two traps can be sent: (1) bundle down cause as "admin down" (2) bundle down cause as "l2 negotiation fail" When a WAN bundle is Admin UP, a single "bundle up" trap (3) is sent that signifies l2 negotiation success. This is true for an IPv4 bundle. In the case of an IPv6 bundle, no traps are sent for "l2 negotiation" status. Therefore, bundle down due to l2 negotiation fail (2) and bundle up due to l2 negotiation success (3) are not sent.

Subsystem	Description
	This is a design limitation and no fix is planned for Release 10.0. Note that in the case of bundle down due to Admin shut down, only the bundle down trap due to "admin down" (1) is sent. This behavior is as per design and implementation.
DS3	The Clear Channel DS3 interface module does not currently support the use of the M13 framing format. Only the default framing format of C-BIT should be used on Clear Channel DS3 interface modules.
RSVP-TE	MPLS does not interwork correctly with interfaces where Firewall is enabled. In case any issues are observed, please clear and recreate the MPLS LSP.
SNMP	SNMP SET operations are not supported for Secure Router 4134 in Release 10.0. Read-write access type for community configuration is provided only for logical completeness of the community string. If the SET operation is performed on any of the RW MIB objects, the behavior of the agent is unpredictable.
Tunneling	Tunnel PMTU discovery is not working. When a router inside an IPv4 tunnel sends an ICMP_TOO_BIG message with an MTU value, the tunnel interface is not updated with this value because of a 3rd party/OS dependency that does not supply this functionality.
ethernet0/0 and Layer 3	The management port (ethernet 0/0) does not support Layer 3 features, including VRRP.
Interoperability with: MSTP LACP (dynamic link aggregation) VLAN forwarding of tagged and untagged Ethernet traffic	To interoperate with the SR4134 implementation of MSTP, LACP, and VLANs, the following products must run the minimum (or newer) software versions listed below: • Cisco Catalyst 3750: IOS version 12.2r(25) • Nortel Ethernet Routing Switch 8600: Software version 4.1.1.0 FCS • Nortel Ethernet Routing Switch 5510: Software version 5.0.5.000
Interoperability with 802.1x	To interoperate with the SR4134 implementation of 802.1x, the following products must run the minimum (or newer) software versions listed below: • Windows XP: Version 5.1.2600, service pack 2 • AEGIS client: Version 2.0.1

Related information

This section lists the documents that relate to the Secure Router 4134 Software Release 10.0, and provides information related to getting technical assistance from Nortel.

Publications

Refer to the following publications for information about the Secure Router 4134 Software Release 10.0:

- Secure Router 4134 Documentation Roadmap (NN47263-103)
- Secure Router 4134 Quick Start (NN47263-100)
- Secure Router 4134 Installation – Chassis (NN47263-300)
- Nortel Secure Router 4134 Installation — Hardware Components (NN47263-301)
- Nortel Secure Router 4134 Installation — SFPs (NN47263-303)
- Secure Router 4134 Commissioning (NN47263-302)
- Secure Router 4134 Configuration — WAN Interfaces (NN47263-500)
- Secure Router 4134 Configuration — Layer 2 Ethernet (NN47263-501)
- Secure Router 4134 Configuration — IPv4 and Routing (NN47263-502)
- Secure Router 4134 Configuration — IPv6 and Routing (NN47263-503)
- Secure Router 4134 Configuration — IPv4 Multicast Routing (NN47263-504)
- Secure Router 4134 Configuration — MPLS (NN47263-505)
- Secure Router 4134 Using the Command Line Interface (NN47263-506)
- Nortel Secure Router 4134 Command Line Reference (NN47263-507)
- Secure Router 4134 Security — Configuration and Management (NN47263-600)
- Secure Router 4134 Performance Management — Quality of Service (NN47263-601)

- Nortel Secure Router 4134 Configuration — Network Management (NN47263-602)
- Secure Router 4134 Troubleshooting (NN47263-700)

How to get help

This section explains how to get help for Nortel products and services.

You can download the 10.0 software release from the Customer Service Portal site, www.nortel.com/support. Select "Product Categories", and then "Routers and Routing Switches". Scroll down to the Secure Router family.

Getting help from the Nortel Web site

The best way to get technical support for Nortel products is from the Nortel Technical Support web site:

www.nortel.com/support

This site provides quick access to software, documentation, bulletins, and tools to address issues with Nortel products. From this site, you can:

- download software, documentation, and product bulletins
- search the Technical Support Web site and the Nortel Knowledge Base for answers to technical issues
- sign up for automatic notification of new software and documentation for Nortel equipment
- open and manage technical support cases

Getting help over the phone from a Nortel Solutions Center

If you do not find the information you require on the Nortel Technical Support web site, and you have a Nortel support contract, you can also get help over the phone from a Nortel Solutions Center.

In North America, call 1-800-4NORTEL (1-800-466-7835).

Outside North America, go to the following web site to obtain the phone number for your region:

www.nortel.com/callus

Getting help from a specialist using an Express Routing Code

To access some Nortel Technical Solutions Centers, you can use an Express Routing Code (ERC) to quickly route your call to a specialist in your Nortel product or service. To locate the ERC for your product or service, go to:

www.nortel.com/erc

Getting help through a Nortel distributor or reseller

If you purchased a service contract for your Nortel product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller.

Nortel Secure Router 4134

Release Notes — Software Release 10.0

Publication: NN47263-400
Document status: Standard
Document version: 01.01
Document date: 28 August 2007

To provide feedback or report a problem in this document, go to www.nortel.com/documentfeedback.