Nortel Secure Router 4134

Release Notes — Software Release 10.1

Release: 10.1
Document Revision: 02.01

www.nortel.com

Nortel Secure Router 4134
Release: 10.1
Publication: NN47263-400
Document status: Standard
Document release date: 24 March 2008

Sourced in Canada and the United States of America.

Contents

Secure Router 4134 Release Notes 5
Introduction 5
Secure Router 4134 Release 10.1 features 6
Hardware features 6
Software features 8
Default settings 10
Memory requirements 10
USB Flash drives 10
Compact Flash cards 10
Upgrading the Secure Router 4134 11
Upgrading software and hardware on the Secure Router 4134 11
Downgrading the Secure Router 4134 software 17
Downgrading Secure Router 4134 software for technical reasons 18
Downgrading Secure Router 4134 software to move an interface module from a Release 10.1 chassis to a Release 10.0 chassis 20
Upgrading or downgrading the bootrom image version 21
Using SSH 25
Supported software and hardware capabilities 27
Supported SFPs 28
Firewall ALG behavior 28
Default behavior of the firewall ALG 28
Updates to the DNS ALG 29
SNMP MIBs 31
Issues resolved since last release 31
Known issues, limitations, and guidelines 36
Re-imaging the Mediation Server Module 41
General guidelines and considerations 41

Related information 45
Publications 45
How to get help 46
Getting help from the Nortel Web site 46
Getting help over the phone from a Nortel Solutions Center 46
Getting help from a specialist using an Express Routing Code 47

Getting help through a Nortel distributor or reseller 47

Secure Router 4134 Release Notes

The Release Notes for Secure Router 4134, Software Release 10.1, 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 10.1 release is for general use and is supported on the Secure Router 4134 platform only. Release 10.1 software does not support the Secure Router 3120 and Secure Router 1000 Series hardware platforms.

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 10.1.

The Nortel Secure Router 4134 is a high-performance system that integrates multiple branch office functions (including routing, Wide Area Network [WAN], high-density Ethernet switching [Layer 2 and Layer 3], Power over Ethernet [PoE], Voice over IP [VoIP] and security) 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. The Secure Router 4134 can cost-effectively and securely concentrate traffic from hundreds of remote sites.

Secure Router 4134 Release 10.1 features

The Nortel Secure Router 4134 is a multipurpose router that integrates multiple network technologies into a single device.

Secure Router 4134 Release 10.1 adds integrated VoIP and Microsoft® capabilities to the Secure Router 4134 platform, including media gateway (for example, FXS and FXO) and Microsoft Office Communications Server (OCS) mediation services. The VoIP Media Gateway solution is only supported for USA and Canadian markets in Release 10.1.

The following sections describe the hardware and software features for Secure Router 4134 Release 10.1.

Hardware features

This section describes hardware features supported on Nortel Secure Router 4134, Software Release 10.1.

Interface modules

Secure Router 4134 Release 10.1 introduces the following optional external interface modules:

- 2-port FXS Small Module
- 4-port FXS Small Module
- 2-port FXO Small Module
- 4-port FXO Small Module
- Mediation Server Module for Office Communications Server (OCS)
- Voice Carrier Medium Module (a voice expansion module—carries up to four FXS or FXO Small Modules)

For information about the Secure Router 4134 modules (internal and external), and for installation instructions, see *Nortel Secure Router 4134 Installation — Hardware Components* (NN47263-301).

For information about configuring the Secure Router 4134 voice-type modules, see *Nortel Secure Router 4134 Configuration — SIP Media Gateway* (NN47263-508).

Mediation Server Module for OCS

The Mediation Server Module is a blade server module that runs the Microsoft Mediation Server software on top of Microsoft Windows Server 2003. The Mediation Server software performs the necessary signaling and media transcoding for calls between the OCS network and the Media Gateway.

The Mediation Server translates SIP and PSTN calls to OC client connections and translates calls from OC clients to the Media Gateway for routing to the PSTN or SIP network.

The Mediation Server Module supports traffic up to the equivalent of one T1 or 24 simultaneous calls.

ATTENTION
Nortel strongly recommends the following procedures to protect the software on the Mediation Server Module:

- Create at least one additional user account with administrator privileges on the Microsoft Windows Server 2003 running on the Mediation Server Module for OCS. If you lose or forget the administrator password, you can log in using another user account. Similar to other Operating Systems, the administrator password cannot be recovered.
- Enable auto updates on Windows Server 2003 and the Mediation server running on the Mediation Server Module.
- Make a backup copy of the Mediation Server Module software and configuration.
- Install third-party antivirus software (not supplied) on the Mediation Server Module and run periodic scans of the disk to ensure it remains free of viruses. Nortel does not recommend running antivirus software continuously because doing so impedes the performance of the module.

For more information, see "Re-imaging the Mediation Server Module" (page 41).

For detailed information about the Mediation Server Module and its configuration, see *Nortel Secure Router 4134 Configuration — SIP Media Gateway* (NN47263-508).

Internal PVM

Secure Router 4134 Release 10.1 also introduces the internal Packetized Voice Module (PVM). You must install the internal PVM to implement the voice functionality and features available in the Release 10.1 software.

The PVM is factory-installed with new orders, or you can install it in the field on previously purchased routers (for information about field installation, see *Nortel Secure Router 4134 Installation — Hardware Components* (NN47263-301).

The PVM module provides the voice conversion from Time-Division Multiplexing (TDM) signals to IP Real-time Transport Protocol (RTP) packets, as well as the reverse. The PVM also provides digital signal processing (DSP) functions including echo cancellation, voice activity detection (VAD), comfort noise generation (CNG), tone detection and generation, and dual-tone multifrequency (DTMF) digit collection. The

PVM can support fax over IP using T.38 fax relay or fax pass-through, as well as modem over IP using modem pass-through. The PVM has a timeslot interchanger for TDM to TDM switching.

Software features

With Release 10.1, Nortel adds support for integrated media gateway modules (for example, FXS and FXO modules) to the Secure Router 4134, as well as Microsoft® mediation technology.

This section describes new software features supported on Nortel Secure Router 4134, Software Release 10.1.

SIP media gateway

The Secure Router 4134 Release 10.1 supports an optional voice subsystem that allows the router to operate as a SIP-PSTN Media Gateway. With the SIP-PSTN Media Gateway features enabled, the Secure Router 4134 can connect SIP VoIP telephony networks with the PSTN and transcode the PSTN connections and SIP signaling, as necessary. The Secure Router 4134 can also provide direct connections for analog phones, faxes, and modems.

An external SIP server provides the required call control and routing in the SIP network. To provide SIP call routing, the Secure Router 4134 Media Gateway supports interoperation with the following systems:

- Nortel CS 1000 (Releases 4.5 and 5.0)
- Microsoft Office Communications Server (OCS) 2007
- Sylantro (Release 4.1.1)
- BroadSoft (Release 14.0 SP1)

To implement the voice subsystem, you must install the internal PVM, as well as voice connection modules. The Secure Router 4134 supports FXO, T1 (ISDN PRI or T1 CAS), and ISDN BRI modules to provide access to the PSTN. The Secure Router 4134 also supports FXS modules to provide direct connections for analog phone, fax, and modem lines.

For detailed information about the SIP media gateway, see *Nortel Secure Router 4134 Configuration — SIP Media Gateway* (NN47263-508).

DSP channel licensing

Software licensing limits the number of DSP channels available on the Secure Router 4134. If you boot the Secure Router 4134 with the PVM module only, the maximum number of DSP channels available is limited to 8. To operate the Secure Router 4134 with additional channels, you must obtain a license key. Contact Nortel Support to obtain a license key appropriate for your needs.

License keys can expand the maximum DSP channel capacity to support 8, 16, 32, 64, or up to a maximum of 128 channels (when the G.711 [20 ms] codec is used).

As described in the following table, the maximum DSP capacity available is lower if the router is running more complex codecs.

Codec	**Maximum number of DSP channels supported**				
	128-channel license	**64-channel license**	**32-channel license**	**16-channel license**	**8-channel license**
G.711 (20 ms)	128	64	32	16	8
G.711 (10 ms)	96	48	24	12	6
G.726	64	32	16	8	4
G.723.1	64	32	16	8	4
G.729A	64	32	16	8	4
T38	32	16	8	4	2

For detailed information about the DSP channel licensing, how to determine which license is appropriate for your circumstances, and how to obtain the license (you require information about your Secure Router 4134 before contacting Nortel Support), see *Nortel Secure Router 4134 Configuration — SIP Media Gateway* (NN47263-508).

Ethernet Connectivity Fault Management

Secure Router 4134 supports the 802.1ag protocol, which provides operation, administration, maintenance (OAM) functionality for Ethernet. Specifically, IEEE 802.1ag Connectivity Fault Management (CFM) provides OAM tools for the service layer, which allows you to monitor and troubleshoot an end-to-end Ethernet service instance.

Ethernet CFM uses a ’heartbeat’ mechanism—Continuity Check Messages (CCM)—for fault detection. Ethernet CFM also provides ’tools’ such as Loopback Messages (LBM) for fault verification and isolation, and Linktrace Messages (LTM) for path discovery.

Nortel supports Ethernet CFM on chassis Gigabit Ethernet (GbE) ports only for Release 10.1 software.

For detailed information about Ethernet CFM and its configuration, see *Nortel Secure Router 4134 Configuration — Layer 2 Ethernet* (NN47263-501).

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 drive is identified in the system as /cf0; the external drive 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.

ATTENTION
Ensure you format your Compact Flash card using the Secure Router 4134 before you use the card.

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)

Upgrading the Secure Router 4134

The Nortel Secure Router Release 10.1 software is supported only on the Secure Router 4134. The Release 10.1 software is located on the CD and on the Nortel Technical Support Web site (http://www.nortel.com/support).

Table 1
Secure Router 4134 software images

Description	File size (bytes)	Version	File name
Secure Router application image	19 346 728	10.1 (r10.1)	SR4134.Z

The MIBs file for release 10.1 is SR4134_R10.0MIBs.zip.

Upgrading software and hardware on the Secure Router 4134

The following two upgrade tasks cause an interruption in service for the Secure Router 4134:

- An upgrade of the software on the Secure Router 4134 requires that you reboot the router.
- An upgrade of the hardware on the Secure Router 4134 may require that you power down the Secure Router 4134. For example, Nortel strongly recommends that you power down the Secure Router 4134 if you are installing an interface module in a slot in which you have not previously installed that module type. If you do not power down the router to install a module, you must reboot the router to use the

card. (After a module is installed and initialized, you can hot swap that module.) Also, to install an internal module of any type, you must power down the router.

WARNING
Risk of damage to equipment
Secure Router 4134 Release 10.1 includes updates to the bootrom image. Installing software Release 10.1 updates the EEPROM on each module that is installed in the Secure Router 4134 at the time of upgrade. Ensure you have only modules installed that you plan to use with Release 10.1 software.

ATTENTION
The Telnet and FTP servers are disabled by default in Release 10.1 software. To enable the Telnet server, enter `telnet_server` from configuration mode. To enable the FTP server, enter `ftp_server` from configuration mode.

ATTENTION
Nortel recommends that you use an FTP server when upgrading software because of the size of the image file.

For Secure Router 4134, Release 10.1, 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 using any of the following methods:

- 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 filename 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.

Upgrade procedure

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

ATTENTION
By default, the Secure Router 4134 automatically updates the normal and golden bootrom images when you upgrade software. To ensure that the Secure Router 4134 updates the normal and golden bootrom image automatically, enter the **`show boot_params`** command and ensure that the parameter `Save bootrom image [0:AutoUpdate, 1:NormalBTupd, 2:GoldenBTupd, 3:NoUpd]` is set to **`0 (AutoUpdate)`**. Use the **`boot_params`** command (in configuration mode) if you must edit the setting for this parameter.

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

Procedure steps

Step	Action
1	Create a backup copy of your router configuration by saving the configuration file to an 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 (http://www.nortel.com/support), placing it on a USB Flash drive, or on a Compact Flash card, or on a server that is running an FTP daemon.
3	Ensure that network connectivity exists between the Secure Router being upgraded and the FTP server, if you use that option. 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 To perform a hardware upgrade, power down the Secure Router 4134.

> **ATTENTION**
> You require the internal Packetized Voice Module (PVM) for voice functionality and features available in the Release 10.1 software.

> **ATTENTION**
> Nortel recommends that you power down the Secure Router 4134 if you are installing an interface module in a slot in which you have not previously installed that module type.

6 Install new hardware.

7 Power up the Secure Router 4134. If you did not power down the router, reboot the router to initialize the software upgrade.

8 Ensure the normal and golden bootroms are updated, and that they are running the same bootrom image version (version 0.0.0.29 or higher for Release 10.1 software). For more information, see "Upgrading or downgrading the bootrom image version" (page 21).

--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 upgrade to a new version of the software, the new file overwrites the older version that is on the card.

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

Procedure steps

Step **Action**

1 Create a backup copy of your router configuration by saving the configuration file to an FTP server, a USB drive, or an external Compact Flash card storage device.

2 Download the image file from the Nortel Support page (http://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 ftp 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. The message is received only when you have not renamed the existing Secure Router 4134 image file (the default filename is SR4134.Z).

```
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
```

If you have the Mediation Server Module installed and operating, there is a 2-minute delay after you issue the `reboot` command while the router waits for the module to shut down. The chassis reboots automatically when the Mediation Server Module completes shutdown.

--End--

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

The following example procedure uses an external USB drive for loading the image file to the internal Compact Flash. If you choose to use an external Compact Flash card 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/.

To avoid overwriting a previous version of software, rename the old version of software before downloading the upgrade software version.

Procedure steps

Step Action

1 Create a backup copy of your router configuration by saving the configuration file to an FTP server, a USB drive, or an external Compact Flash card.

2 Download the image file from the Nortel Support page (http://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       FEB-13-2008       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
```

If you have the Mediation Server Module installed and operating, there is a 2-minute delay after you issue the `reboot` command while the router waits for the module to shut down. The chassis reboots automatically when the Mediation Server Module completes shutdown.

--End--

Downgrading the Secure Router 4134 software

There are two scenarios in which you must downgrade the Secure Router 4134 software from Release 10.1 to 10.0:

- You have Release 10.1.0 software installed on your Secure Router 4134 and you must return to Release 10.0.0 software for technical reasons.
- You want to move an interface module from a Secure Router 4134 that is running Release 10.1.0 software to a Secure Router that is running 10.0.0 software.

CAUTION
Read this section carefully—failure to follow the steps as described in this section can result in system failure.

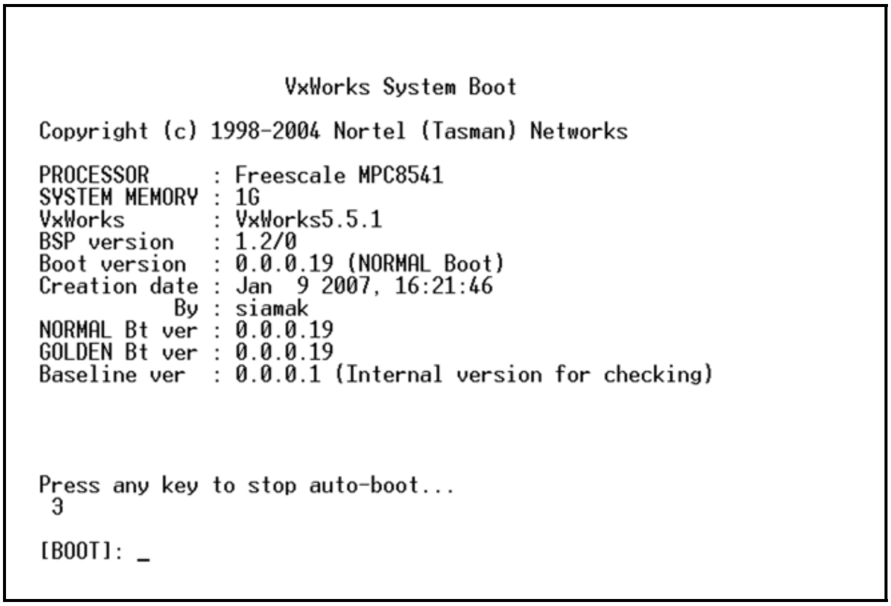
CAUTION
You must complete all steps of the downgrade process. If you stop the downgrade procedure before completion, the Secure Router 4134 can become unstable. Follow the upgrade procedures to return to Release 10.1.0 software.

Downgrading Secure Router 4134 software for technical reasons

Use the procedure in this section if you must downgrade your Secure Router 4134 from Release 10.1.0 to Release 10.0.0 software.

Procedure steps

Step	Action
1	Nortel recommends that you rename the existing operating software filename on /cf0. For example, rename SR4134.Z to SR4134_10_1.Z
2	Download or copy the Release 10.0.0 software file to an FTP server, a Compact Flash card, or a USB drive. See “Upgrade procedure” (page 13).
3	Change the bootrom update flag (the "Save bootrom image" parameter in the boot parameters) to **`1:NormalBTupd`**.
4	(Optional) You can omit this step if you renamed the Release 10.1 software file on /cf0. Change the boot parameters to boot with the Release 10.0.0 software.
5	Reboot the chassis.
6	Access the bootrom command menu by pressing any key at the beginning of the boot sequence. The Secure Router 4134 stops the auto-boot sequence and re-directs you to the bootrom prompt. The following figure shows you the prompt at which you can enter the bootrom command menu by pressing any key.



```
                        VxWorks System Boot

Copyright (c) 1998-2004 Nortel (Tasman) Networks

PROCESSOR     : Freescale MPC8541
SYSTEM MEMORY : 1G
VxWorks       : VxWorks5.5.1
BSP version   : 1.2/0
Boot version  : 0.0.0.19 (NORMAL Boot)
Creation date : Jan  9 2007, 16:21:46
           By : siamak
NORMAL Bt ver : 0.0.0.19
GOLDEN Bt ver : 0.0.0.19
Baseline ver  : 0.0.0.1 (Internal version for checking)



Press any key to stop auto-boot...
 3

[BOOT]: _
```

7 To downgrade all modules installed in the Secure Router 4134, enter:
E

8 To continue the boot sequence, enter:
D

This boots the Secure Router 4134 with the Release 10.0.0 software.

9 When the chassis completes the boot sequence, enter the following command to confirm that all installed modules are available in the chassis:
show chassis

10 Downgrade the normal and golden bootrom partitions. For instructions to downgrade the bootrom partitions, see “Upgrading or downgrading the bootrom image version” (page 21).

11 Ensure that the normal and golden bootrom partitions have a bootrom version of 0.0.0.25 or lower for Release 10.0.0 software. To verify the bootrom version on the bootrom partitions, enter:
show version

The following output shows an example of the successful downgrade of both the normal and golden bootrom partitions.

```
PROCESSOR : Freescale MPC8541
SYSTEM MEMORY : 1G
VxWorks :  VxWorks5.5.1
BSP version :  1.2/0
Boot version :  0.0.0.25 (NORMAL Boot)
Creation date :  Dec 12 2007, 19:26:37
By :  kevz
NORMAL Bt ver :  0.0.0.25
GOLDEN Bt ver :  0.0.0.25
```

```
Baseline ver :  0.0.0.25 (Internal version for
checking)
```

The following example shows a partial completion of the downgrade procedure. If the image version displayed for "NORMAL bt ver" and "GOLDEN Bt ver" do not match, you must continue the downgrade procedure to correct the mismatch. In this example, the golden bootrom partition must be downgraded to match the image version on the normal bootrom partition.

```
PROCESSOR : Freescale MPC8541
SYSTEM MEMORY : 1G
VxWorks :  VxWorks5.5.1
BSP version :  1.2/0
Boot version :  0.0.0.29 (GOLDEN Boot)
Creation date :  Dec 12 2007, 19:26:37
By :  kevz
NORMAL Bt ver :  0.0.0.25
GOLDEN Bt ver :  0.0.0.29
Baseline ver :  0.0.0.29 (Internal version for
checking)
```

--End--

Downgrading Secure Router 4134 software to move an interface module from a Release 10.1 chassis to a Release 10.0 chassis

Use the procedure in this section if you must move an external interface module from a Secure Router 4134 that is running Release 10.1.0 software to a Secure Router 4134 that is running Release 10.0.0 software.

You can move an interface module from a Secure Router 4134 that is running Release 10.0.0 software to a Secure Router 4134 that is running Release 10.1.0 software—no special steps are required. Nortel strongly recommends that you power down the Secure Router 4134 if you are installing an interface module in a slot in which you have not previously installed that module type. If you do not power down the router to install a module, you must reboot the router to use the module.

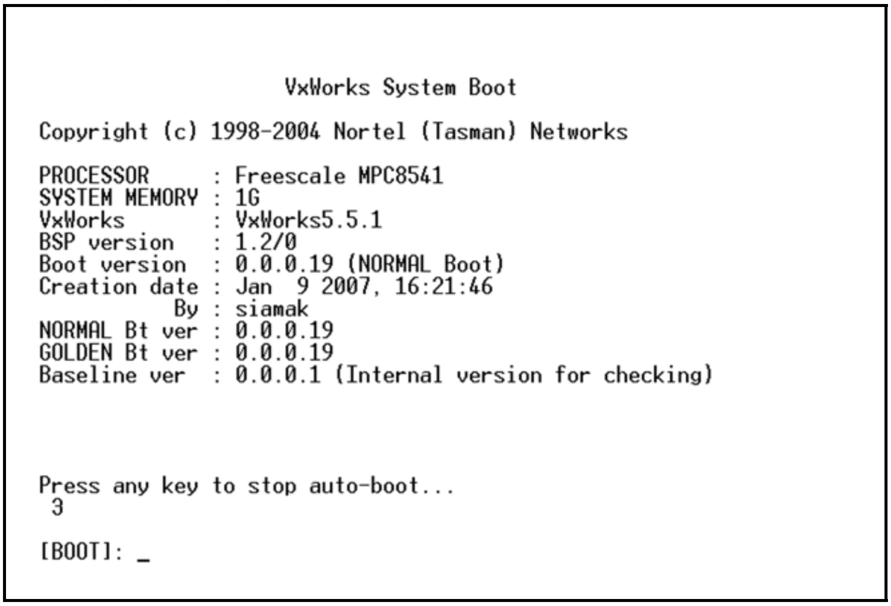
Procedure steps

Step **Action**

1 Reboot the Secure Router 4134 that runs the Release 10.1 software.

2 Access the bootrom command menu by pressing any key at the beginning of the boot sequence.

The Secure Router 4134 stops the auto-boot sequence and re-directs you to the bootrom prompt. The following figure shows you the prompt at which you can enter the bootrom command menu by pressing any key.



```
                     VxWorks System Boot

Copyright (c) 1998-2004 Nortel (Tasman) Networks

PROCESSOR      : Freescale MPC8541
SYSTEM MEMORY  : 1G
VxWorks        : VxWorks5.5.1
BSP version    : 1.2/0
Boot version   : 0.0.0.19 (NORMAL Boot)
Creation date  : Jan  9 2007, 16:21:46
            By : siamak
NORMAL Bt ver  : 0.0.0.19
GOLDEN Bt ver  : 0.0.0.19
Baseline ver   : 0.0.0.1 (Internal version for checking)



Press any key to stop auto-boot...
 3

[BOOT]: _
```

3 To downgrade all modules installed in the Secure Router 4134, enter:
E

4 Power down the Secure Router 4134.

For instructions to safely power down the Secure Router 4134, see *Nortel Secure Router 4134 — Commissioning* (NN47263-302).

5 Remove the interface modules that you intend to install in a Release 10.0.0 router.

6 Power up the Secure Router 4134 that is running Release 10.1.0 software.

Any interface modules installed in the Secure Router 4134 (Release 10.1.0 software) update to the Release 10.1.0 firmware automatically when the router boots.

For instructions to install interface modules in the Secure Router 4134, see *Nortel Secure Router 4134 Installation — Hardware Components* (NN47263-301).

--End--

Upgrading or downgrading the bootrom image version

The Secure Router 4134 Release 10.1 software includes an updated bootrom version. If you upgrade your Secure Router 4134 to Release 10.1 software, you must ensure you update the normal and golden bootrom partitions on the router. If you have set the bootrom image update setting to AutoUpdate (0), the normal and golden bootrom partitions are updated automatically when upgrading the Secure Router 4134 software.

If the normal or golden bootrom partition image version does not automatically update, use the procedure in this section to update the image. Note that the normal bootrom partition should be updated before the golden (if the normal bootrom image is incorrect).

If you must downgrade your Secure Router 4134 from Release 10.1 to Release 10.0 software, you use the procedure in this section to downgrade the image version on the normal and golden bootrom partitions. If you are downgrading the Release software, ensure you read "Downgrading the Secure Router 4134 software" (page 17) before following the steps in this section.

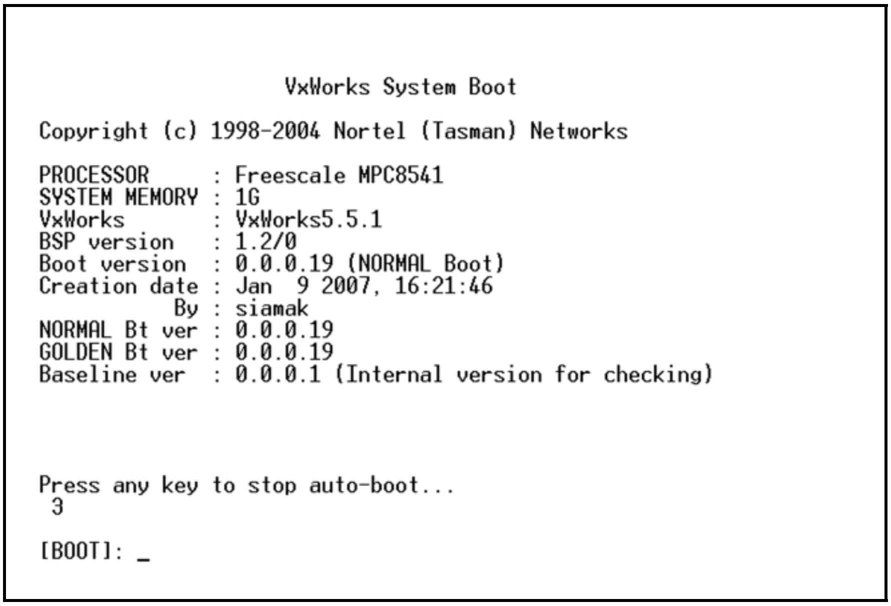
It is important to upgrade or downgrade both the normal and golden bootroms to prevent a bootrom mismatch.

Use the **show version** command in the CLI to find information for the image version running on the normal and golden bootrom partitions of your Secure Router 4134.

> **ATTENTION**
> If you have the Mediation Server Module installed, there is a 2-minute delay after you issue the **reboot** command while the router waits for the module to shut down. The chassis reboots automatically when the Mediation Server Module completes shutdown.

Procedure steps

Step	Action
1	Download the new software image file (SR4134.Z) to your FTP server.
2	Access the bootrom command menu by booting the Secure Router 4134 and pressing any key at the beginning of the boot sequence. The Secure Router 4134 stops the auto-boot sequence and re-directs you to the bootrom prompt. The following figure shows you the prompt at which you can enter the bootrom command menu by pressing any key.



```
                    VxWorks System Boot

Copyright (c) 1998-2004 Nortel (Tasman) Networks

PROCESSOR     : Freescale MPC8541
SYSTEM MEMORY : 1G
VxWorks       : VxWorks5.5.1
BSP version   : 1.2/0
Boot version  : 0.0.0.19 (NORMAL Boot)
Creation date : Jan  9 2007, 16:21:46
           By : siamak
NORMAL Bt ver : 0.0.0.19
GOLDEN Bt ver : 0.0.0.19
Baseline ver  : 0.0.0.1 (Internal version for checking)



Press any key to stop auto-boot...
 3

[BOOT]: _
```

3 At the prompt, enter **`c`** to change the boot parameters:

`[BOOT]:` **`c`**

4 When prompted, enter the name of the device from which you prefer the router boots:

`Boot dev [ftp,cf0,cf1,usb0]:` **`cf0`**

Pressing **Enter** after each entry or selection saves that information to the router. For example, if you select **`cf0`** as the boot device, it is not necessary to enter information for the FTP server because the Secure Router 4134 checks only the CF0 device for the image.

5 Enter the image filename (enter the full directory path if you selected **`ftp`** as the boot device):

`Boot file name:` **`SR4134.Z`**

6 Enter the name of the FTP server you use (it is only necessary to configure this if you selected **`ftp`** as your boot device):

`Server name:` **`sunserver`**

7 Enter the FTP server IP address (it is only necessary to configure this if you selected **`ftp`** as your boot device):

`Server IP address:` **`10.10.11.12`**

8 Enter the router IP address (the router provides this information if you have previously configured it)

`My IP address:` **`10.10.13.14`**

9 Enter the subnet mask (the router provides this information if you have previously configured it):

`My subnet mask:` **`255.255.255.0`**

10 Enter the gateway IP address (the router provides this information if you have previously configured it):

`Gateway IP address:` **`10.10.13.1`**

11 Enter your user name and password:

```
User name: kevz
Password: kevz
```

12 Enter 0 to disable or 1 to enable the checksum feature:

```
Checksum enable [0:Disable,1:Enable]:  1
```

13 Enter 0 to disable or 1 to enable the display of the image header contents:

```
Show header enable [0:Disable,1:Enable]:  1
```

14 Enter the number that corresponds to the bootrom partition that you are upgrading or downgrading (enter `1` for the normal bootrom; enter `2` for the golden bootrom):

```
Save bootrom image [0:AutoUpdate,1:NormalBTupd,
2:GoldenBTupd,3:NoUpd]:1
```

15 To complete the update of the selected bootrom partition, enter `D` at the prompt to reboot the router:

```
[BOOT]: D
```

Allow the boot sequence to complete.

16 When the boot sequence is complete, the Secure Router 4134 returns a message verifying the boot image is updated and that the system must reboot.

The Secure Router 4134 reboots. Allow the boot sequence to complete.

17 To display the bootrom version numbers and the active boot partition, use the **`show version`** command in the CLI, or access the bootrom command menu and enter `v` at the prompt:

```
[BOOT]: v
```

```
PROCESSOR : Freescale MPC8541
SYSTEM MEMORY : 1G
VxWorks :  VxWorks5.5.1
BSP version :  1.2/0
Boot version :  0.0.0.29 (NORMAL Boot)
Creation date :  Dec 12 2007, 19:26:37
By :  kevz
NORMAL Bt ver :  0.0.0.29
GOLDEN Bt ver :  0.0.0.29
Baseline ver :  0.0.0.29 (Internal version for
checking)
```

It is important to upgrade or downgrade both the normal and golden bootroms to prevent a bootrom mismatch.

18 Repeat this procedure to update the golden bootrom partition, if necessary.

--End--

ATTENTION
When you have successfully completed the update of the bootrom partitions, remember to enter the `boot_params` command (`SR4134/configuration# boot_params`), or to access the bootrom command menu (that is, interrupt the auto-boot sequence to access the boot parameters), to revert the bootrom image update feature to AutoUpdate (0).

Using SSH

Before upgrading to Release 10.1, you can enable SSH and save the secure router configuration. The following steps describe the basic procedure:

1. Generate the key (RSA or DSA).
2. Enable the SSH server.
3. Save the router configuration.
4. Reboot the device.

Use the procedures in this section to complete the preceding steps.

Generate an RSA key

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 RSA key, enter: **`generate rsa`**

--End--

Enable the SSH server using an RSA key

Step	Action
1	To access configuration mode, enter: **`configure terminal`**
2	To access the SSH server command set, enter: **`ssh_server`**
3	To configure the host key filename, enter: **`hostfile shrsakey`** By default, the Secure Router 4134 looks for a DSA key. To use an RSA key, you must enter the RSA host key filename.

4	To enable the SSH connection, enter: **`enable`**

--End--

Generate a DSA key

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`**

--End--

Enable the SSH server using a DSA key

Step	Action
1	To access configuration mode, enter: **`configure terminal`**
2	To access the SSH server command set, enter: **`ssh_server`**
3	To enable the SSH connection, enter: **`enable`**

--End--

Save the configuration and reboot the router

Step	Action
1	Save the configuration: **`save local`**
2	To reboot the Secure Router 4134, enter: **`reboot`**

--End--

Supported software and hardware capabilities

The following table lists supported software and hardware capabilities for Secure Router 4134 Software Release 10.1. For additional scaling information and design guidelines, please contact your Nortel representative.

> **ATTENTION**
> The VoIP Media Gateway solution is only supported for USA and Canadian markets in Release 10.1.

Table 2
Hardware and software capabilities

Feature	Maximum number supported
Ethernet Ports: Gigabit Fast Ethernet PoE	 58 72 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
FXS/FXO ports	16
SSH sessions	5
FTP sessions	4
TFTP sessions	3
Telnet sessions	15
DHCP: leases relay agents	 4000 255

Table 2
Hardware and software capabilities (cont'd.)

Feature	Maximum number supported
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 10.1, 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-NT 1

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

Firewall ALG behavior

This section describes updates to firewall ALG behavior.

Default behavior of the firewall ALG

This section describes the Secure Router 4134 Release 10.1.0 support for ALG behavior.

All firewall ALGs are disabled by default.

To use the typical ALG set, a new CLI command (that is, **`enable-typical`**) has been added. This command enables the following specific set of ALGs:

- aim
- aimudp
- ftp

- msn
- pptp
- rpc
- rtsp554
- rtsp7070
- smtp
- tftp
- web
- ike

The remaining ALGs (h323, gatekeeper, msnudp, dns, n2p, pcanywhere, sql, msgtcp, irc, n2pe, ils, cuseeme, mszone, ils2, nntp, sip, sip-tcp) are in the disabled state.

Use the following procedure to configure the typical ALG set.

Procedure steps

Step	Action
1	To access Configuration Mode, enter: **`configure terminal`**
2	To access the `firewall global` subtree, enter: **`firewall global`**
3	To configure the typical ALG set, enter the `algs` command subtree: **`algs`**
4	To enable the typical ALG set, enter: **`enable-typical`**

--End--

Updates to the DNS ALG

The Secure Router 4134 Release 10.1.0 provides support for a DNS ALG.

The DNS ALG is used when the DNS client in the untrusted side wants to access the DNS server behind NAT in the trusted side.

A DNS client in the untrusted side sends a "DNS Standard Query" to the Secure Router. The Secure Router receives the DNS query with the destination port 53. The Secure Router translates the IP header based on the reverse NAT policy. When the response comes from the DNS server (that is present in the trusted side), the Secure Router translates the header based on the reverse NAT policy, and the DNS payload is translated from the private IP record to the global IP record, which is taken from the DNS pool database.

A DNS client in the untrusted side sends a "DNS Reverse Query" to the Secure Router. The Secure Router translates the IP header based on the reverse NAT policy, and the DNS payload is translated from the global IP record to the private IP record (both of which were added using the CLI). When the response comes from the DNS server (that is present in the trusted side), the Secure Router translates the header based on the reverse NAT policy, and the DNS payload is translated from the private IP record to the global IP record, which is taken from the DNS pool database.

To translate the IP address in the DNS payload, follow the configuration in the next section.

Configuring DNS ALG

Use the procedure in this section to configure a DNS ALG.

Procedure steps

Step	Action
1	To access Configuration Mode, enter: **`configure terminal`**
2	To access the `firewall global` subtree, enter: **`firewall global`**
3	To configure the DNS ALG pool, enter the `algs` command subtree: **`algs`**
4	Enter the `dns` subtree: **`dns`**
5	To enable the DNS ALG, enter: **`enable`**
6	To ensure the DNS pool has been configured, enter: **`pool <pool-name> <private-ip> <global-ip>`**
7	To display information for the specific static pool name, enter: **`show firewall dns-alg translate-pool pool-name <pool-name>`**
8	To display information for all configured static pool names, enter: **`show firewall dns-alg translate-pool`**

--End--

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 10.1, refer to *Nortel Secure Router 4134 Configuration — Network Management* (NN47263-602).

Issues resolved since last release

The following table describes issues that existed in Release 10.0 software, and which have been resolved for Release 10.1.

Table 4
Issues in Release 10.0 that are resolved in Release 10.1

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). 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>timer>?" is not showing relevant information. The "bgp dampening <half life timer>timer>?" help string now displays relevant information. However, you may encounter this issue with other commands, such as the **`ip route`** command.

Table 4
Issues in Release 10.0 that are resolved in Release 10.1 (cont'd.)

Change Request	Subsystem	Description
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.
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.
Q01685793	Firewall	Connection-reservation for an IP address is not configurable Firewall does not allow you to reconfigure the connection-reservation 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.

Table 4
Issues in Release 10.0 that are resolved in Release 10.1 (cont'd.)

Change Request	Subsystem	Description
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, 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.
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.

Table 4
Issues in Release 10.0 that are resolved in Release 10.1 (cont'd.)

Change Request	Subsystem	Description
		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	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.
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 4. Configure srtcm with CIR=400000 Kbps and CBS=EBS=99968 Bytes (No metering happens. All

Table 4
Issues in Release 10.0 that are resolved in Release 10.1 (cont’d.)

Change Request	Subsystem	Description
		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:

Table 4
Issues in Release 10.0 that are resolved in Release 10.1 (cont'd.)

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

Known issues, limitations, and guidelines

The following table describes issues and limitations known to exist in the Secure Router 4134 Software Release 10.1, and provides guidelines for using Release 10.1 software.

Table 5
Known issues and limitations

Change Request	Subsystem	Description
Q01793197	CT3	Connecting ct3 to multiplexer 28 T1s alternately showing rais and rlof This issue is not seen on active IN-SERVICE T1s. The issue occurs only on NON-ACTIVE T1s where there are no cables connected to the mux (multiplexer). The issue is intermittent, and happens only momentarily and then recovers with the correct status.
Q01680944-01	DHCP	Cannot configure DHCP relay under VLAN DHCP relay is not supported on VLAN interfaces.
Q01783680	Ethernet CFM	No check on interface VLAN change even if associated with MA The Secure Router 4134 performs a check or validation when adding a non-existent VLAN to a Connectivity Fault Management (CFM) Maintenance Association (MA) for a particular Maintenance End Point (MEP) interface. However, if you create an interface with VLAN "X" and associate an MA with VLAN "X", and then change the interface VLAN to "Y", the Secure Router 4134 does not run a validation check or issue errors for the MA. Therefore, when a VLAN interface is changed on the Secure Router 4134 (for example, VLAN "X" is changed to VLAN "Y"), ensure you update the VLAN associations for MAs, as well (`SR4134/configure/oam/cfm/md MD1/ma MA1#` **`vlan <vid>`**).
Q01812273	Ethernet CFM	CC or LTM multicast messages when Rxed through Marvell ports are dropped Nortel does not support the transmission of Continuity Check Messages (CCM), Linktrace Messages (LTM), or Loopback Messages (LBM) on Ethernet interface module interfaces in Release 10.1. Nortel supports MIP configurations on chassis Gigabit Ethernet (GbE) ports only in Release 10.1.

Table 5
Known issues and limitations (cont'd.)

Change Request	Subsystem	Description
Q01783728	LDP	LDP FEC table is NOT removing entry even though Routing Table has removed entry When interoperating LDP with Cisco routers, there are occasions when the LDP Label Release is sent by the Cisco router on a delay. This results in stale FEC entries being retained in the LDP Control Plane, visible through the LDP show commands. Workaround: 1. Wait for the delayed Label Release messages. 2. Issue the **`clear ldp adjacency`** command for this session to clean up all associated FEC learned from the Cisco router.
Q01728651-01	MPLS	No option to config RouterID on IP address You can use only loopback IP addresses as the RouterID. A feature enhancement that allows you to configure the RouterID using any interface IP address is planned for the next release of Secure Router 4134 software.
Q01793375	PSS	mcast traffic is not fwded to any IF if one of OIFs has MTU lesser than pkt size In this scenario, the input interface is an interface module Ethernet interface with jumbo frames enabled, and there are two output interfaces (OIF): one with normal MTU size and one with jumbo frames enabled. If the normal MTU interface is removed from the OIF list, everything works as expected. If the normal interface is part of the OIF, then the other Ethernet module interface (that has jumbo frames enabled) does not get the packets.

Table 5
Known issues and limitations (cont'd.)

Change Request	Subsystem	Description
Q01764294	QoS	With CBQ, low priority classes are not getting CR with high packet size traffic The chances of this issue occurring are less than 1%. Meeting the defect reproduction criteria is very rare. However, the issue is that the least priority flows can fall short of their expected committed rate bandwidth. Workaround: Re-group/pack the traffic flows so that there are fewer priority groups. For example, create only four priority groups.
Q01812350	SSH	Encrypted private key cannot be restored after command {change "null" "" } The encrypted private key cannot be restored after the command **`change "null" "" <value>`** is executed. That is, if the output passphrase is specified with a **`""`** (null string) instead of entering **`"null"`**, then the key cannot be restored.
Q01817949	VoIP-CALL CONTROL	DUT sends SIP invite with from number as SIP binded address NULL replace string is not supported. If the intention is to send the caller ID as anonymous, you must configure Caller ID block.
Q01822353	VoIP - FXS/FXO	CAMA calls are not successful when trunk group is created If a Centralized Automatic Message Accounting (CAMA) port must be used as part of a Trunk group, then all CAMA trunk members must use the same signaling.
Q01807142	VoIP - FXS/FXO	Hissing sound is played to the caller before ring back tone when set to A-law In a hairpin call scenario between two FXS ports, if the compand-type on the called port is set to A-law and the other to U-law, sometimes a hiss noise is heard before the ringback tone on the caller side. The issue is only seen when configuring A-law, which is used in Europe. The Release 10.1 scope is limited to North America.

Table 5
Known issues and limitations (cont'd.)

Change Request	Subsystem	Description
Q01833008	VoIP - FXS/FXO	Intermittent ability to send fax The Secure Router 4134 Media Gateway does not support switching of calls to T.38 fax if, in response to a SIP Re-invite for T.38, a peer sends a 2000K SIP response with a port value of 0 in the audio m-line. Workaround: Enable fax pass-through on the Secure Router 4134. Alternatively, if you do not configure the Secure Router for fax, ensure you configure the peer to detect the fax tone and send the Re-invite/Update for T.38.
Q01817111	VoIP - ISDN	DUT enters an invalid state when channel selection is preferred with "any channels" If a SETUP message with the "any channel" option is received on a BRI line, then that call is dropped.
Q01815683	VoIP-ISDN	Simultaneous BRI U to SIP call issues with Basic NI and dms 100 point to point This is a very unlikely scenario because it involves origination of the two calls at the same instance. When two calls originate in the same instant, one of the two calls is dropped. If a call is dropped for this reason, the caller can retry the call.

Q01810252	xSTP	Show commands showing duplicate help and displaying different outputs
		
		The display error is shown when you attempt a partial completion of the CLI command, as in the following case:
		
		`DUT1#` **`show spanning-tree mstp instance vlan?`**
		`vlan vlans in all instances`
		`vlan vlans in the instance`
		
		Workaround:
		Avoid partial completion of show commands. For example:
		
		`DUT1#` **`show spanning-tree mstp instance ?`**
		or
		`DUT1#` **`show spanning-tree mstp instance vlan ?`**

Re-imaging the Mediation Server Module

If you lose the administrator password for your Mediation Server Module (and have no other account with administrator privileges), or if the software image becomes corrupt on the module, you must re-image the module.

Nortel strongly recommends the following procedures to protect the software on the Mediation Server Module:

- Create at least one additional user account with administrator privileges on the Microsoft Windows Server 2003 running on the Mediation Server Module for OCS. If you lose or forget the administrator password, you can log in using another user account. Similar to other Operating Systems, the administrator password cannot be recovered.
- Make a backup copy of the Mediation Server Module software and configuration using a third-party application such as Ghost software from Symantec Corporation.
- Install third-party antivirus software (not supplied) on the Mediation Server Module and run periodic scans of the disk to ensure it remains free of viruses. Nortel does not recommend running antivirus software continuously because doing so impedes the performance of the module.
- Enable auto updates on Windows Server 2003 and on the Mediation server running on the Mediation Server Module.
  "High Priority" updates for Windows Server 2003 and the Mediation Server are automatically downloaded and auto-installed (identical to the Windows updates process) when you enable the Microsoft auto update feature on each. "Optional" updates must be done manually—you are only alerted to their availability. You must go to the Microsoft update Web site (http://www.update.microsoft.com) to get a description of the optional updates. You can then decide if the update is necessary for your system.

General guidelines and considerations

The following table provides information about design limitations known to exist in the Secure Router 4134 Software Release 10.1.

Table 6
Design limitations for the Secure Router 4134

Subsystem	Description
Hardware	You cannot enable the management port on the rear of the Secure Router 4134 (Ethernet 0/0) if you have a PVM installed (this is related to hardware design). Ensure you use Ethernet 0/1, 0/2, 0/3, or 0/4 for management if you use a PVM in the router.
	For Secure Router Release 10.1, Nortel Secure Router 4134 FXO cards (SR0000042E5 and SR0000044E5) do not fully meet the provisions of Section 4.7.2.1 of the TIA-968-A standard. The modules are intended for connectivity to Private Branch Exchange (PBX) systems, key systems, and private copper facilities in campus applications. The FXO modules should not be directly connected to the PSTN unless the connectivity is through a SmartJack, Network Interface Device, or other telephone company approved device that is TIA-968-A compliant. FXO modules will be fully compliant with the TIA-968-A standard beginning in Release 10.1.1.
PSS	IGMP multicast groups not added to hardware when reports are from different VLANs In the unusual scenario where the Secure Router 4134 receives a flood of multicast addresses within a very short duration of time, there is a chance that not all multicast addresses are learned. In this scenario, you should clear the multicast group so re-learning of the multicast addresses can occur.
VLAN	A protocol-based VLAN classification rule can be successfully applied to an interface without the need to pre-configure the VLAN. In this scenario, the protocol-based rule will be inactive. Workaround: Create the VLAN (that is, add the VLAN to the database) and assign a port to the VLAN after you have created and applied the protocol-based VLAN classification rule.
	The MAC address discard command (**`mac address <macaddr> discard <interface id> vlan <vid>`**) is a global command (that is, the specified MAC address is discarded from all interfaces), although an interface must be specified as part of the command syntax.

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

Table 7
General guidelines and considerations for the Secure Router 4134

Subsystem	Description
VoIP	For information about limitations related to VoIP configuration and the Secure Router 4134, see *Nortel Secure Router 4134 Configuration — SIP Media Gateway* (NN47263-508).

Table 7
General guidelines and considerations for the Secure Router 4134 (cont'd.)

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.

Table 7
General guidelines and considerations for the Secure Router 4134 (cont'd.)

Subsystem	Description
	This is a design limitation. 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. 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 2/Layer 3 features, including VRRP.
Interoperability with: MSTP LACP (dynamic link aggregation) VLAN forwarding of tagged and untagged Ethernet traffic	To interoperate with the Secure Router 4134 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	The following clients have been verified with the Secure Router 4134 implementation of 802.1x: • Windows XP: Version 5.1.2600, service pack 2 • AEGIS client: Version 2.0.1 This is a reference set of possible clients, and interoperability is not limited to these clients.

Related information

This section lists the documents that relate to the Secure Router 4134 Software Release 10.1, 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 10.1:

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

- *Nortel Secure Router 4134 Configuration — SIP Media Gateway* (NN47263-508)
- *Nortel Secure Router 4134 Security — Configuration and Management* (NN47263-600)
- *Nortel Secure Router 4134 Performance Management — Quality of Service* (NN47263-601)
- *Nortel Secure Router 4134 Configuration — Network Management* (NN47263-602)
- *NortelSecure 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 Secure Router 4134 10.1 software from the Customer Service Portal site, http://www.nortel.com/support.

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:

http://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:

http://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:

http://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 10.1

Release: 10.1
Publication: NN47263-400
Document status: Standard
Document revision: 02.01
Document release date: 24 March 2008

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

www.nortel.com

Sourced in Canada and the United States of America.