Nortel Secure Router 4134

Release Notes — Software Release 10.1.1

Release: 10.1.1
Document Revision: 03.02

www.nortel.com

NN47263-400

Nortel Secure Router 4134
Release: 10.1.1
Publication: NN47263-400
Document status: Standard
Document release date: 5 September 2008

Sourced in Canada and the United States of America.

Contents

Secure Router 4134 Release Notes

This document provides summary information about the following topics:

- 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 Release 10.1.1 is for general use and is supported on the Secure Router 4134 platform only. Release 10.1.1 software does not support the Secure Router 3120 or 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 10.1.1.

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 10.1.1 software features

The following sections describe the software features introduced with Secure Router 4134 Release 10.1.1:

- “Euro ISDN” (page 6)
- “QSIG” (page 7)
- “ISDN overlap receiving for voice” (page 9)
- “PRI dial-in aggregator” (page 14)
- “DHCP relay over VLAN” (page 20)

Euro ISDN

With release 10.1.1, the Secure Router 4134 (SR4134) SIP Media Gateway supports Euro ISDN voice connections on E1 PRI and BRI interfaces. The Euro ISDN voice ports interwork with previously supported T1 CAS, FXS, and FXO voice ports and SIP call features.

As with other ISDN voice connections on the SR4134, there is no network side support for Euro ISDN. The SR4134 only supports user side ISDN voice connections.

To support Euro ISDN in the CLI, under the **`interface bundle`** subtree, the **`link pri_e1`** command now supports the **`voice`** option. In addition, under the **`isdn`** subtree, two new **`switch-type`** options are supported: **`basic-euro`** for Euro ISDN on BRI and **`primary-euro`** for Euro ISDN on PRI.

Linking a Euro ISDN bundle to a BRI or E1 port for voice

Use the following procedure to configure a Euro ISDN voice bundle on a BRI or E1 port.

When you configure ISDN voice ports, be sure to specify the network clock using the **`network-clock-select`** command.

Step	Action
1	To enter configuration mode, enter: **`configure terminal`**
2	To configure a WAN bundle, enter: **`interface bundle <bundle-name>`**
3	To link the bundle to an E1 or BRI port for voice, enter:

```
link {pri_e1 <slot/port [<:timeslots>]> |
bri <slot/port:links>} voice
```

4 To specify ISDN configuration, enter:

```
isdn
```

5 To specify the switch type, enter:

```
switch-type <switch-type>
```

6 To activate the bundle, enter:

```
activate
```

--End--

Table 1
Variable definitions

Variable	Value
pri_e1 <slot/port [<:timeslots>]>	Specifies an E1 link and timeslots for ISDN PRI.
bri <slot/port:links>	Specifies an ISDN BRI link. You can specify 1 (64 Kb/s) or 2 (128 Kb/s) links.
<switch-type>	Valid switch-type values for Euro ISDN voice are as follows: • basic-euro: EURO ISDN for BRI • primary-euro: EURO ISDN for PRI

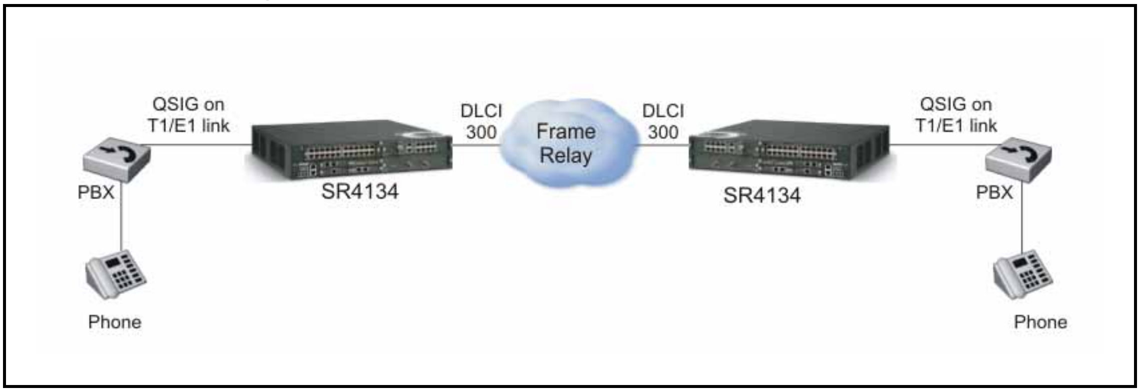
QSIG

With release 10.1.1, the SR4134 supports QSIG on E1 and T1 PRI interfaces. Q Signaling (QSIG) is a variant of ISDN Q.921 and ISDN Q.931 D-channel signaling for use in private integrated services networks. QSIG operates between nodal entities known as private integrated network exchanges (PINX), such as PBXs or key systems.

With QSIG signaling, the SR4134 can emulate PSTN functionality. The router can route incoming PINX voice calls across a WAN connection to a peer router, which can then forward the call to another PINX. The QSIG messages pass transparently across the WAN link between the QSIG routers and the call flow remains compliant with Q.931. This functionality provides toll bypass between the two PINXs.

The following figure shows a sample topology that uses QSIG connections to route PBX calls over a WAN link.

Figure 1
QSIG sample topology



The SR4134 supports only basic QSIG services; it does not support supplementary services.

The QSIG protocol was originally specified by the European Computer Manufacturers Association (ECMA). It has since been adopted by European Telecommunications Standards Institute (ETSI) and the International Organization for Standardization (ISO). It is becoming the standard for PBX interoperability in Europe and North America.

QSIG limitations

The following list describes QSIG limitations:

- The SR4134 supports QSIG as a switch type for voice bundles on PRI interfaces only.
- The SR4134 does not support supplementary services for QSIG.
- The SR4134 does not send a FAC REJ reply to a supplementary service request from the far end.

QSIG standards compliance

The following list describes the supported QSIG standards:

- ETS 300 403: Integrated Services Digital Network (ISDN); Digital Subscriber Signaling System No. one (DSS1) protocol; Signaling network layer for circuit-mode basic call control
- ETS 300 267-1: Integrated Services Digital Network (ISDN); Telephony 7 kHz and video telephony teleservices; Digital Subscriber Signaling System No. one (DSS1) protocol; Part 1: Protocol specification
- ETS 300 171/172 – QSIG Basic Call
- Multiple ETS standards for QSIG Supplementary Services

- ETS 300 125 – QSIG Layer 2
- ETS 300 012 – QSIG Layer 1

Configuring QSIG switch type support

Use the following procedure to configure QSIG on a T1 PRI or E1 PRI port.

When you configure ISDN voice ports, be sure to specify the network clock using the **network-clock-select** command.

Step **Action**

1 To enter configuration mode, enter:

```
configure terminal
```

2 To configure a WAN bundle, enter:

```
interface bundle <bundle-name>
```

3 To link the bundle to an ISDN port for voice, enter:

```
link {pri_e1 <slot/port [<:timeslots>]> |
pri_t1 <slot/port [<:timeslots>]>} voice
```

4 To specify ISDN configuration, enter:

```
isdn
```

5 To specify QSIG as the switch type, enter:

```
switch-type primary-qsig
```

6 To activate the bundle, enter:

```
activate
```

--End--

ISDN overlap receiving for voice

With Release 10.1.1, the SR4134 supports overlap receiving as an alternative signaling method to en bloc signaling for call establishment of ISDN voice calls. While most modern switches use en bloc signaling, many European countries continue to support overlap signaling. The SR4134 supports overlap receiving on BRI ports configured for Euro ISDN and on E1 PRI ports configured for Euro ISDN or QSIG.

> **ATTENTION**
> The SR4134 does not support overlap sending. The router always uses en bloc sending.

ATTENTION
The SR4134 supports overlap receiving on BRI ports configured for Euro ISDN and on E1 PRI ports configured for Euro ISDN or QSIG. You cannot enable overlap receiving on other ISDN switch types.

With en bloc signaling, the setup message used for connection requests contains the complete called party information. In overlap signaling, the setup message contains no or only some information about the called party. The remaining information needed to complete the connection establishment is sent in one or more subsequent information messages. Overlap signaling assures reservation of channels and connection establishment before the entire called party number is dialed or received.

When you enable overlap receiving on the D-channel, you change the way the SR4134 behaves when it receives ISDN calls. The router responds to the setup message with a setup ack. The setup ack informs the network that it is ready to receive further information messages that contain additional called party digits.

To implement overlap receiving, the SR4134 supports a t302 timer. After the router receives a setup message and sends a setup ack in response, the t302 timer starts. The timer limits the period that the router waits for call control information from the Network side. The router on the User side restarts this timer each time it receives an information message.

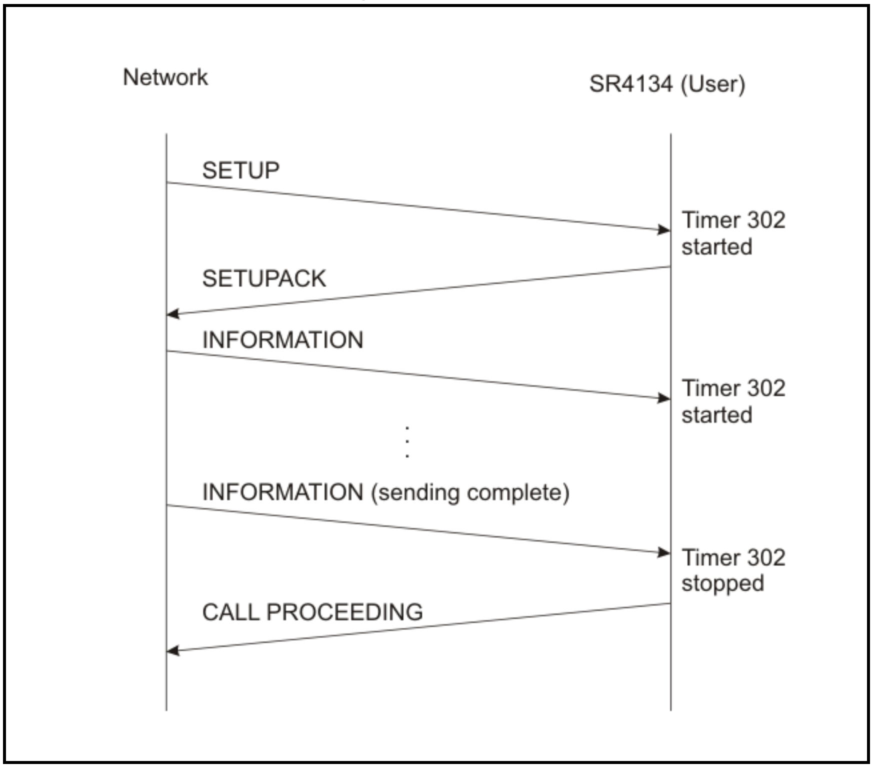
The default value of the t302 timer is 15 seconds.

ISDN overlap receiving call flows

The following figures show ISDN call flows with overlap signaling and how the t302 timer operates during the call.

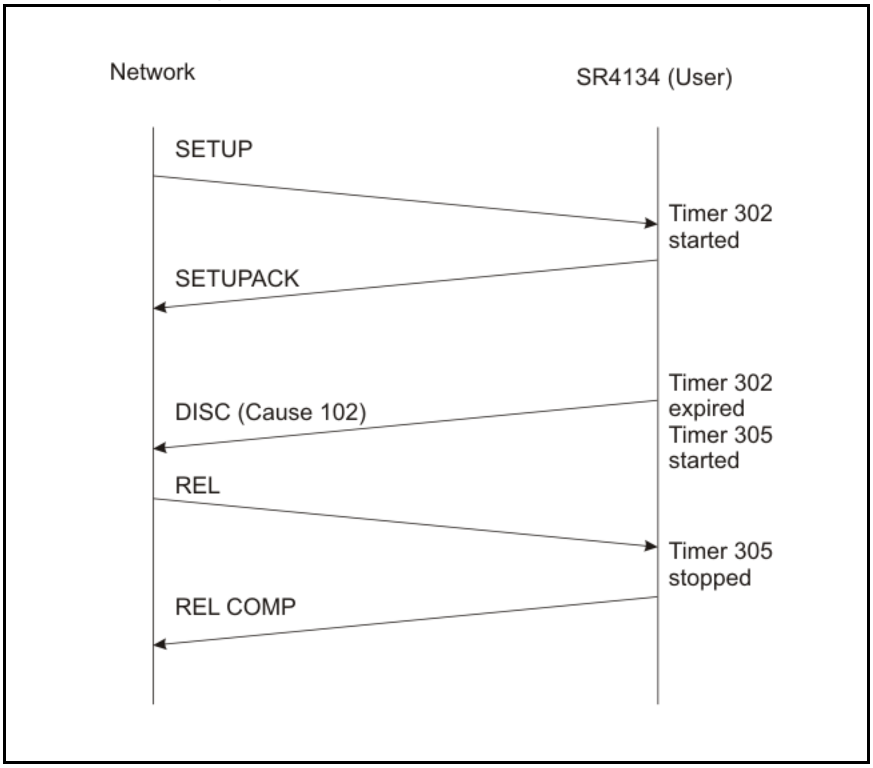
The following figure shows a successful overlap receiving call flow.

Figure 2
Successful overlap receiving call flow



The following figure shows an overlap receiving call flow in which the t302 timer expires.

Figure 3
Overlap receiving call flow with t302 expiry



With t302 timer expiry and call clearing, be aware of the following:

- The Network can also initiate call clearing if the t304 timer maintained at the network end expires.
- When the t302 timer expires, call control checks if it has sufficient digits to reach the destination. If it does, it sends a CALL PROC message; otherwise, it sends a DISCONNECT message.

Configuring ISDN overlap receiving for voice

Use the following procedure to configure overlap receiving on an ISDN voice bundle. Overlap Receiving is supported on BRI and E1 PRI ports configured for Euro ISDN.

By default, ISDN ports use en bloc signaling.

When you configure ISDN voice ports, be sure to specify the network clock using the **`network-clock-select`** command.

Step	Action
1	To enter configuration mode, enter:

```
configure terminal
```

2 To configure a WAN bundle, enter:

```
interface bundle <bundle-name>
```

3 To link the bundle to an ISDN port for voice, enter:

```
link {pri_e1 <slot/port [<:timeslots>]> |
bri <slot/port:links>} voice
```

4 To specify ISDN configuration, enter:

```
isdn
```

5 To specify the switch type, enter:

```
switch-type {basic-euro | primary-euro | primary-qsig}
```

6 To specify overlap receiving, enter:

```
[no] overlap-receive
```

7 To specify q931-timers configuration, enter:

```
q931-timers
```

8 To configure the t302 timer, enter:

```
t302 <t302-timer>
```

9 To exit q931 timers configuration, enter:

```
exit
```

10 To activate the ISDN bundle, enter:

```
activate
```

--End--

Table 2
Variable definitions

Variable	Value
[no] overlap-receive	The no form of the command changes the mode of signaling to en bloc.
t302 <t302-timer>	Specifies the t302 timer value. Range is from 3 to 15 seconds. Default: 15 seconds.

Displaying the ISDN voice port configuration

The commands that display the ISDN PRI or BRI bundle configuration include the following:

- **`show interface bundles`**: displays the bundle configurations
- **`show interface bundle <bundle-name>`**: displays a specific bundle configuration

- `show isdn interfaces`: displays the ISDN properties for all bundles
- `show isdn interface <bundle-name>`: displays the ISDN properties for a specific bundle
- `show voice port <slot/[subslot]port:[<d-channel>]`: displays the voice port configuration (for E1 PRI, <d-channel> = 15)
- `show module configuration all`: displays the module configuration (not applicable to BRI modules)

PRI dial-in aggregator

With Release 10.1.1, the SR4134 supports PRI dial-in aggregator on T1 and E1 interfaces.

With PRI dial-in aggregator, the SR4134 can connect multiple remote ISDN BRI connections to a single local ISDN PRI bundle. The SR4134 acts as a dial-in gateway for the BRI clients. BRI clients call in to the SR4134, and the SR4134 aggregates the BRI clients into a single PRI WAN pipe. BRI clients can then connect to the remote locations using Telnet, FTP, or SCP.

While the PRI aggregator can only connect to 30 E1 or 23 T1 BRI links concurrently, no fixed limit exists on the number of BRI links you can configure to dial in to the PRI aggregator because the BRI links are not tied to a given PRI aggregator channel.

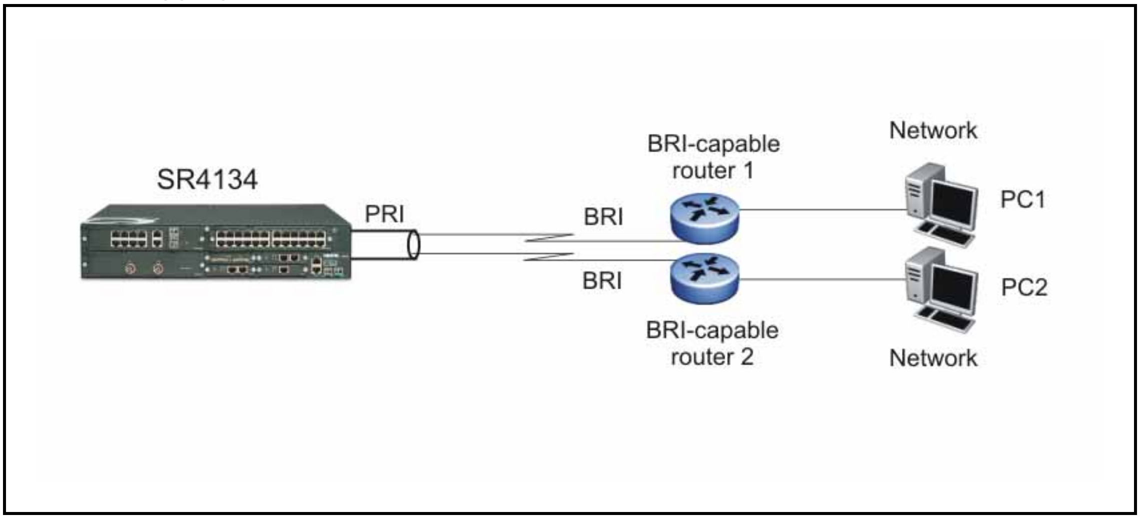
The IP addresses at either end of the link need not be part of the same subnet for reachability. This allows any number of BRI peers to be configured to dial into the PRI aggregator.

Because the SR4134 acts as an aggregator, it is configured to accept calls from the clients. The clients can call the SR4134 using any of the available free channels. The aggregator accepts the call and processes the client request; however, it cannot terminate the call. After data is sent, the aggregator idles the channels but does not disconnect. As a result, the client must handle the termination of the call.

The PRI aggregator does not accept calls based on bandwidth on demand (BoD). An incoming call on a channel is accepted if that channel is free and available.

The following figure shows a PRI interface aggregating two incoming BRI links.

Figure 4
PRI dial-in aggregator



PRI dial-in aggregator limitations

The following limitations apply to the PRI dial-in aggregator:

- On a PRI aggregator port, the individual bundle links must be 64 Kb/s and you must configure the bundle encapsulation to PPP. A 128 Kb/s client cannot dial in because MLPPP encapsulation is not supported.
- On each bundle, configure a 30-bit subnet mask to provide a two-host subnet.
- Because of the 30-bit subnet mask, you must use multiple subnets across the bundles on the same PRI dial-in aggregator port.
- Although multiple bundles are aggregated, the D-channel used for signaling is the same. All the D-channel properties, such as switch type, are shared across the bundles configured on an aggregator port.
- Because D-channel properties are all common on the aggregator port, you cannot configure different values under the `isdn` command tree for the individual bundles.
- If any bundle on an aggregator port is activated, the D-channel becomes active for all the bundles on that port. However, if you deactivate a bundle on the port (using the `no activate` command), the D-channel remains active for the remaining bundles. The D-channel deactivates only after you deactivate the last bundle on the port.
- With PRI dial-in aggregator bundles, you cannot use the following ISDN commands:

  - **call-back**
  - **callednum**
  - **caller**
  - **callingnum**
  - **connect-delay**
  - **idle-timeout**
- This is a dial-in-only feature.

Configuring the PRI dial-in aggregator

To configure the PRI dial-in aggregator, you must first specify a T1 or E1 port as the PRI aggregator. Then you must configure a separate single-link bundle for each channel that you want to aggregate (up to 30 for E1 and 23 for T1).

> **ATTENTION**
> If you configure QoS and firewall parameters on the aggregated SR4134 links, you must configure identical QoS and firewall parameters for all bundles.

On each bundle, configure a 30-bit subnet mask to provide a two-host subnet.

Step **Action**

1 To enter configuration mode, enter:

```
configure terminal
```

2 To identify a T1/E1 port as a PRI aggregator, enter:

```
pri-aggregator <slot/port>
```

3 To create a new bundle for a BRI link, enter:

```
interface bundle <bundle-name>
```

4 To link the new bundle to a single PRI aggregator channel, enter:

```
link {pri_e1|pri_t1} <slot/port:timeslot>
```

5 To specify the encapsulation (PPP), enter:

```
encapsulation ppp
```

6 To assign an IP address with a 30-bit subnet mask to the new bundle, enter:

```
ip address <ip-address> 30
```

7 To specify ISDN configuration for the bundle, enter.

```
isdn
```

8 To configure the ISDN switch type, enter:

```
switch-type <switch-type>
```

> **ATTENTION**
> Configure the ISDN switch type only on the first bundle before you activate it. If you attempt to configure the switch type on additional bundles, the router displays an error because the D-channel is already active.

9 To activate ISDN on the bundle, enter:

```
activate
```

10 For each additional link you want to aggregate, repeat steps 3 through 9 (skipping step 8).

11 To exit the bundle configuration, enter `exit` twice.

12 Add a static route from the SR4134 to each of the client networks using the peer WAN IP address as the gateway:

```
ip route <destprefix> <netmask>
<gatewayip> <distvalue>
```

13 On each of the peer WAN routers, add static routes to the SR4134 aggregator.

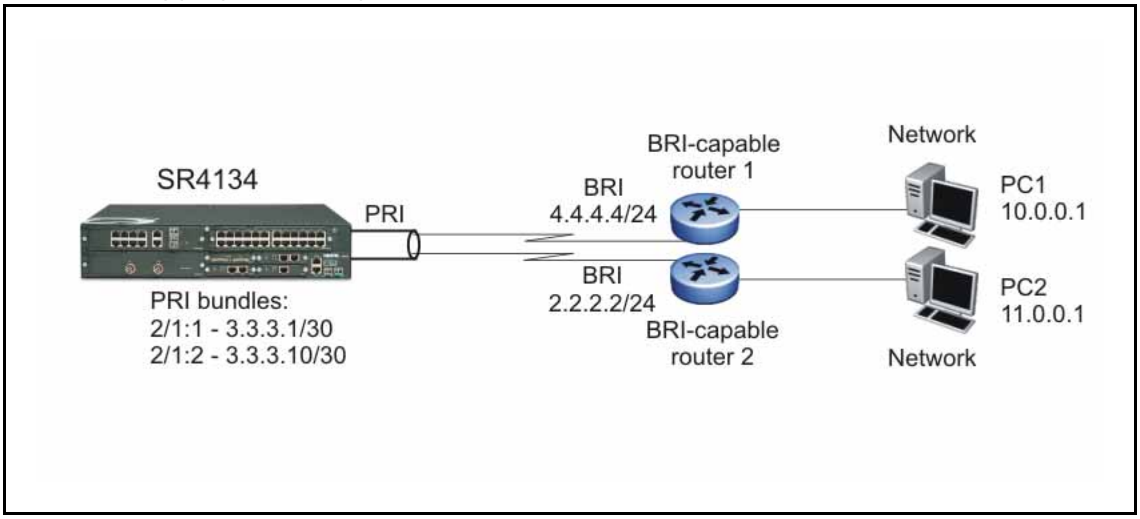
14 To test the configuration, initiate connections from the client sites.

--End--

Example of configuring the PRI dial-in aggregator

The following figure shows a simple topology example with an SR4134 configured as a PRI dial-in aggregator.

Figure 5
PRI dial-in aggregator configuration example



The following sections show the detailed configuration required on the SR4134 for this example.

Port 2/1 configuration as the PRI aggregator

```
SR# configure terminal
SR/configure# pri-aggregator 2/1
```

Bundle 1 configuration

```
SR/configure# interface bundle b1
configuring new WAN bundle interface b1
SR/configure/interface/bundle b1# link pri_e1 2/1:1
SR/configure/interface/bundle b1# encapsulation ppp
SR/configure/interface/bundle b1# ip address 3.3.3.1 30
SR/configure/interface/bundle b1# isdn
SR/configure/interface/bundle b1/isdn# switch-type
primary-euro
SR/configure/interface/bundle b1/isdn# activate
SR/configure/interface/bundle b1/isdn# exit
SR/configure/interface/bundle b1# exit
```

Bundle 2 configuration

```
SR/configure# interface bundle b2
configuring new WAN bundle interface b2
SR/configure/interface/bundle b2# link pri_e1 2/1:2
SR/configure/interface/bundle b2# encapsulation ppp
SR/configure/interface/bundle b2# ip address 3.3.3.10 30
SR/configure/interface/bundle b2# isdn
```

```
SR/configure/interface/bundle b2/isdn# activate
SR/configure/interface/bundle b2/isdn# exit
SR/configure/interface/bundle b2# exit
```

Static routes configuration

```
SR/configure# ip route 10.0.0.0/8 4.4.4.4
SR/configure# ip route 11.0.0.0/8 2.2.2.2
```

Peer router configuration

On the peer routers, add static routes to the SR4134 aggregator.

For example, if router 1 is an SR4134, add the following route:

```
ip route 3.3.3.0/24 bri1
```

Similarly, on router 2, add the following route:

```
ip route 3.3.3.0/24 bri2
```

Here bri1 and bri2 are the names of BRI bundles configured on the respective routers.

On PC1, which is on subnet 1, 10.0.0.0/8, router 1 can serve as the gateway to reach the PRI aggregator. Similarly on PC2, which is on subnet 2, 11.0.0.0/8, router 2 can serve as the gateway to reach the PRI aggregator.

If you ping from PC1 to 3.3.3.1, router 1 dials in to the aggregator. Similarly, when you ping from PC2, router 2 dials in. If a Telnet server is enabled, any host in subnet 1 or subnet 2 can Telnet into the aggregator.

Displaying PRI aggregators

You can use the **`show module configuration all`** command to display the PRI module configuration and the **`show interface bundle <bundle-name>`** command to display the individual bundle configurations. In addition, you can use the **`show pri-aggregator`** command to display which T1/E1 ports are configured as PRI aggregators.

Step	Action
1	To display the PRI aggregator ports, enter:

```
show pri-aggregator
```

--End--

DHCP relay over VLAN

In previous releases of SR4134 software, DHCPv4 relay was supported on Ethernet interfaces only. With release 10.1.1, the SR4134 now supports DHCPv4 relay on VLAN interfaces.

A DHCP server can assign key parameters to a DHCP client including IP address, default gateway, and domain-name server. The client needs these parameters to communicate with the network to which it is connected.

If the client is connected to a network that contains a DHCP server, the server can reply directly to the client requests. But if the DHCP server is in a remote network, the client requests cannot reach the server.

To allow local client requests to reach the remote DHCP server, you can configure an SR4134 interface in the local network as a DHCP relay agent. The relay agent can forward DHCP client requests from the local network to a DHCP server in the remote network. When the server replies, the relay agent forwards the responses back to the client on the local network.

For the DHCP server to accept requests from a DHCP relay agent, you must specify the relay agent IP address on the DHCP server.

Configuring DHCP relay on a VLAN

Use this procedure to specify a VLAN interface as a DHCP relay agent and to specify the address of the DHCP server to which DHCP packets are to be relayed. A maximum of four DHCP server addresses can be configured on an interface.

You can also optionally specify the gateway address. If this address is specified, it is used as the source IP address of the DHCP broadcasts to be relayed; otherwise, the interface IP address is used. The DHCP server uses the gateway address to communicate with the relay agent.

Prerequisites

- On the DHCP server, you must specify the IP address of the SR4134 interface that is serving as the DHCP relay agent.

Step	Action
1	To access configuration mode, enter: `configure terminal`
2	To access the VLAN configuration, enter: `interface vlan <vlan-id>`
3	To configure DHCP relay on the VLAN, enter: `[no] dhcp-relay <server-address> [<gateway>]`

--End--

Table 3
Variable definitions

Variable	Value
<server-address>	Specifies the IP address of the DHCP server (A.B.C.D).
[<gateway>]	Specifies the gateway IP address (A.B.C.D).
[no]	Removes the specified DHCP server address.

Displaying DHCP relay

Use this procedure to display the current DHCP relay configuration.

Step	Action
1	To display the DHCP relay configuration, enter: `show dhcp-relay`

--End--

Procedure job aid: sample command output

The following sample shows output from the **show dhcp-relay** command.

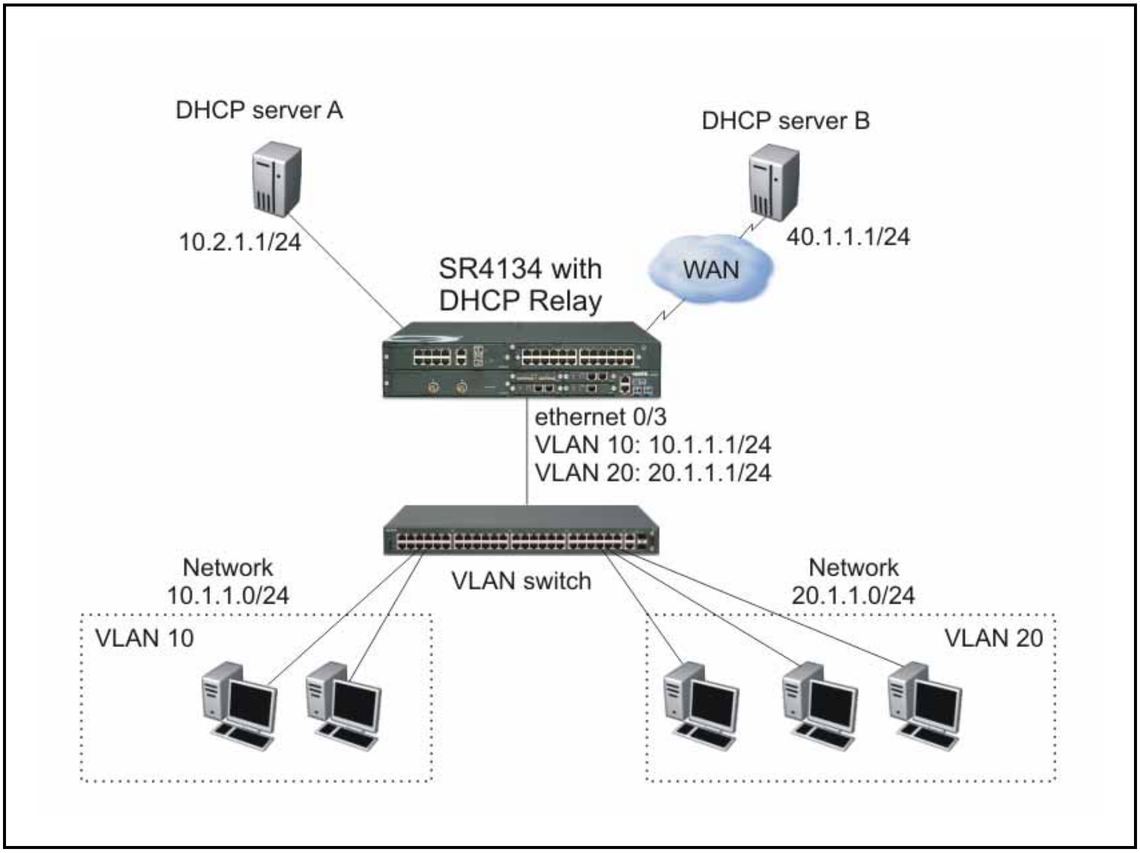
```
DHCP RELAY CONFIGURATION
------------------------
Interface DHCP Server Address Gateway Address
-------------------------------------------------------
vlan10 10.2.1.1 10.1.1.1
```

```
vlan10 40.1.1.1 10.1.1.1
vlan20 10.2.1.1 20.1.1.1
vlan20 40.1.1.1 20.1.1.1
```

Example of configuring DHCP relay on a VLAN

The following figure shows a sample topology in which an SR4134 VLAN interface is configured as a DHCP relay agent.

Figure 6
DHCP relay over VLAN configuration example



The following shows the configurations required on the SR4134 trunk port to enable DHCP relay for the connected VLANs. DHCP servers A and B operate as the remote DHCP servers. In this case, DHCP server A is configured as the preferred server and, if A is unreachable, DCHP server B provides service.

DHCP Relay configuration

```
SR/configure# interface ethernet 0/3
Configuring existing Ethernet interface
SR/configure/interface/ethernet (0/3)# switchport mode
trunk
```

```
SR/configure/interface/ethernet (0/3)# switchport trunk
allow vlan 10,20
SR/configure/interface/ethernet (0/3)# exit

SR/configure# interface vlan vlan10
SR/configure/interface/vlan vlan10# ip address 10.1.1.1 24
SR/configure/interface/vlan vlan10# dhcp-relay 10.2.1.1
10.1.1.1
DHCP RELAY: Server address set to 10.2.1.1
SR/configure/interface/vlan vlan10# dhcp-relay 40.1.1.1
10.1.1.1
DHCP RELAY: Server address set to 40.1.1.1
SR/configure/interface/vlan vlan10# exit

SR/configure# interface vlan vlan20
SR/configure/interface/vlan vlan20# ip address 20.1.1.1 24
SR/configure/interface/vlan vlan20# dhcp-relay 10.2.1.1
20.1.1.1
DHCP RELAY: Server address set to 10.2.1.1
SR/configure/interface/vlan vlan20# dhcp-relay 40.1.1.1
20.1.1.1
DHCP RELAY: Server address set to 40.1.1.1
```

DHCP Server A configuration

In this topology, if DHCP Server A is an SR4134, the following configuration can be used to specify address pools, enable the DHCP server on an interface, and specify the DHCP relay interface. DCHP Server A provides service for both VLAN 10 and VLAN 20.

DHCP pool configuration for subnet 10.1.1.0/24

```
ServerA/configure# ip dhcps
ServerA/configure/ip/dhcps# pool pool1
ServerA/configure/ip/dhcps/pool pool1# network
10.1.1.0 24
ServerA/configure/ip/dhcps/pool pool1# lease 1000
ServerA/configure/ip/dhcps/pool pool1# default_router
10.1.1.1
ServerA/configure/ip/dhcps/pool pool1# netbios_name_
server 120.1.1.1
ServerA/configure/ip/dhcps/pool pool1# tftpserver
64.64.11.11
ServerA/configure/ip/dhcps/pool pool1# dnsserver
164.164.4.5
ServerA/configure/ip/dhcps/pool pool1# exclude-range
10.1.1.1 10.1.1.10
ServerA/configure/ip/dhcps/pool pool1# domain Nortel
```

```
ServerA/configure/ip/dhcps/pool pool1# commit
ServerA/configure/ip/dhcps/pool pool1# exit
ServerA/configure/ip/dhcps# enable
```

DHCP pool configuration for subnet 20.1.1.0/24

```
ServerA/configure# ip dhcps
ServerA/configure/ip/dhcps# pool pool2
ServerA/configure/ip/dhcps/pool pool2# network
20.1.1.0 24
ServerA/configure/ip/dhcps/pool pool2# lease 1000
ServerA/configure/ip/dhcps/pool pool2# default_router
20.1.1.1
ServerA/configure/ip/dhcps/pool pool2# netbios_name_
server 120.1.1.1
ServerA/configure/ip/dhcps/pool pool2# tftpserver
64.64.11.11
ServerA/configure/ip/dhcps/pool pool2# dnsserver
164.164.4.5
ServerA/configure/ip/dhcps/pool pool2# exclude-range
20.1.1.1 20.1.1.10
ServerA/configure/ip/dhcps/pool pool2# domain Nortel
ServerA/configure/ip/dhcps/pool pool2# commit
ServerA/configure/ip/dhcps/pool pool2# exit
ServerA/configure/ip/dhcps# enable
```

Enabling the DHCP server on an interface

```
ServerA/configure# interface ethernet 0/1
ServerA/configure/interface/ethernet 0/1# ip address
10.2.1.1 24
ServerA/configure/interface/ethernet 0/1# exit
ServerA/configure# ip dhcps
ServerA/configure/ip/dhcps# interface ethernet0/1
ServerA/configure/ip/dhcps# enable
```

Specifying the DHCP relay agents on DHCP server A

```
ServerA/configure/ip/dhcps# relay 10.1.1.1 10.1.1.0
ServerA/configure/ip/dhcps# relay 20.1.1.1 20.1.1.0
```

Enabling DHCP client and relay debug messages

Use this procedure to enable DHCP client and relay debug messages. Use the no version of the command to disable the debug messages.

Step	Action
1	To enable the DHCP relay debug messages, enter:

```
[no] debug dhcp_relay enable_debug
```

--End--

Table 4
Variable definitions

Variable	Value
[no]	Disables DHCP relay debug messages.

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 runs more complex codecs.

Table 5
Maximum DSP capacity

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 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 you contact Nortel Support), see *Nortel Secure Router 4134 Configuration — SIP Media Gateway* (NN47263-508).

Default settings

The default system 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 one USB Flash drive device and two Compact Flash card storage devices.

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

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

Upgrading the Secure Router 4134

The Nortel Secure Router Release 10.1.1 software is supported only on the Secure Router 4134. The Release 10.1.1 software is available from the Nortel Technical Support Web site (www.nortel.com/support).

Table 6
Secure Router 4134 software images

Description	File size (bytes)	Version	File name
Secure Router application image	19 406 478	10.1.1 (r10.1.1.0)	SR4134.Z
Secure Router MIBs file	429 023	10.1.1	SR4134_R10.1.1MIBs.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 before you install an interface module in a slot in which you did not previously install 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.

CAUTION

Risk of damage to equipment

Secure Router 4134 Release 10.1 and later includes a bootrom image that is updated from the 10.0 release. When you install software Release 10.1.x, it updates the EEPROM on each module 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.x software.

ATTENTION

The Telnet and FTP servers are disabled by default in Release 10.1.0 and later 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 you upgrade software because of the size of the image file.

For Secure Router 4134 Release 10.1.0 and later, 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 you download 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

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

> **ATTENTION**
> Nortel recommends that you create a backup file that contains your router configuration before you upgrade 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.

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 (www.nortel.com/support) and place it on a USB Flash drive, Compact Flash card, or on a server that is running an FTP daemon.
3	If you use the FTP option, ping the server from the Secure Router to verify 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.

> **ATTENTION**
> To download the software image from an FTP server, be sure to set the FTP transfer mode to binary, otherwise the transferred image has more bytes then the original and this corrupted image results in a crash on boot.

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 Release 10.1 and later 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 10.1.0 or later software).

For more information, see "Upgrading or downgrading the bootrom image version" (page 37).

--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 Flash drive, or an external Compact Flash card storage device.

2 Download the image file from the Nortel Support page (www.nortel.com/support) and place 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 that 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 Flash 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 Flash drive, or an external Compact Flash card storage device.

2 Download the image file from the Nortel Support page (www.nortel.com/support) and place 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.x to 10.0:

- You have Release 10.1.x software installed on your Secure Router 4134 and you must return to Release 10.0 software for technical reasons.
- You want to move an interface module from a Secure Router 4134 that is running Release 10.1.x 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.x 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.x 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 Flash drive. See "Upgrade procedure" (page 29).

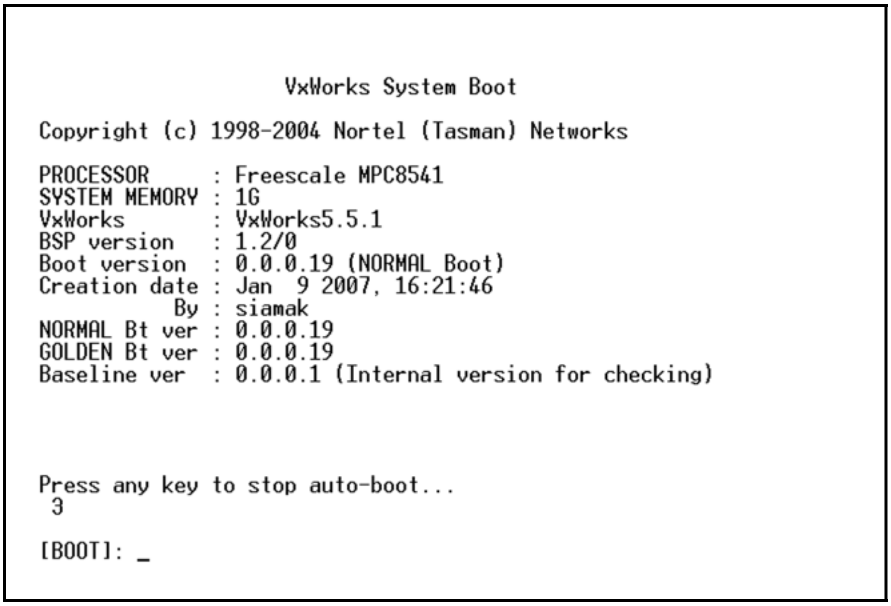
3 Change the bootrom update flag (the "Save bootrom image" parameter in the boot parameters) to `1:NormalBTupd`.

4 (Optional) You can omit this step if you renamed the Release 10.1.x 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 redirects 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`

The Secure Router 4134 boots 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 37).

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 the Secure Router 4134 software to move an interface module from a Release 10.1.x chassis to a Release 10.0 chassis

Use this procedure to move an external interface module from a Secure Router 4134 that is running Release 10.1.x 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.x 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.

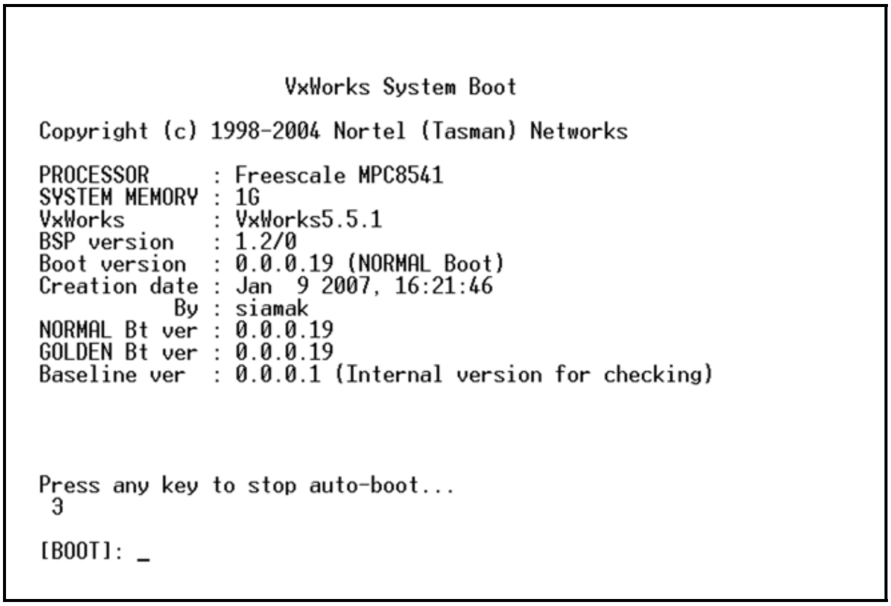
Procedure steps

Step **Action**

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

Any interface modules installed in the Secure Router 4134 (Release 10.1.x software) update to the Release 10.1.x 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.x software includes a bootrom version that is updated from the 10.0.0 release. If you upgrade your Secure Router 4134 to Release 10.1.x software from 10.0, you must ensure you update the normal and golden bootrom partitions on the router.

If you are upgrading from release 10.1.0 to release 10.1.1, this procedure is not required.

If you configured the bootrom image update setting to AutoUpdate (0), the normal and golden bootrom partitions update automatically when you upgrade 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.x 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 33) before you follow the steps in this section.

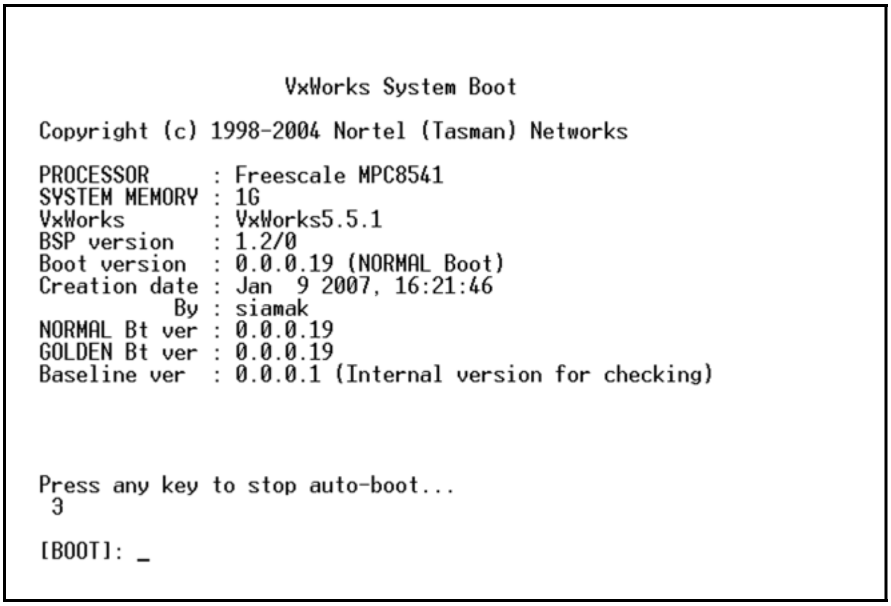
You must upgrade or downgrade both the normal and golden bootroms to prevent a bootrom mismatch.

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 redirects 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 to boot:
`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, you do not have 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 (only if you selected **`ftp`** as your boot device):
`Server name:` **`sunserver`**

7 Enter the FTP server IP address (only 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 previously configured)
`My IP address:` **`10.10.13.14`**

9 Enter the subnet mask (the router provides this information if previously configured):
`My subnet mask:` **`255.255.255.0`**

10 Enter the gateway IP address (the router provides this information if previously configured):
`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 want to upgrade or downgrade (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)
```

Ensure you 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
After you successfully update the bootrom partitions, enter the **`boot_params`** command (`SR4134/configuration#` **`boot_params`**), or 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 you upgrade to Release 10.1.1, 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.

Generating 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--

Enabling 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--

Generating 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--

Enabling 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--

Saving the configuration and rebooting 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 10.1.1. For additional scaling information and design guidelines, contact your Nortel representative.

> **ATTENTION**
> The VoIP Media Gateway solution is only supported for USA and Canadian markets in Release 10.1.1.

> **ATTENTION**
> No hard limits exist on the number of static routes supported on the Secure Router 4134.

Table 7
Hardware and software capabilities

Feature	Maximum number supported
Ethernet Ports: Gigabit Fast Ethernet PoE	 58 72 72 72 is the maximum number of Power over Ethernet (PoE) ports supported. For detailed information about 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	 4000

Table 7
Hardware and software capabilities (cont'd.)

Feature	Maximum number supported
relay agents	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 Release 10.1.1 supports the Small form-factor Pluggable (SFP) transceivers described in the following table.

Table 8
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).

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 10.1.1, see *Nortel Secure Router 4134 Configuration — Network Management* (NN47263-602).

Issues resolved since last release

The following table describes issues that existed in Release 10.1.0 software that are resolved in Release 10.1.1.

Table 9
Issues in Release 10.0 that are resolved in Release 10.1.1

Change Request	Subsystem	Description
Q01831303	Bootrom	When the **X** Boot CLI command is entered to reset the system to default settings, the SR4134 fails to boot properly.
Q01832002	Bootrom	When the SR4134 fails to boot a network image or an image on one of the devices, the router does not attempt to boot the default image of /cf0/SR4134.Z.
Q01563009	CLI	The SR4134 stops responding when **save local** is executed with very large configurations.
Q01723361	CLI	The **show running-config** CLI command output is slow.
Q01727800	CLI	When invalid command syntax is entered, the caret points to the beginning of the command and not to the location of the invalid syntax.
Q01785424	CLI/syslog	When you save your configuration for the first time, the router adds syslog settings to the system.cfg file. Those settings result in errors at boot.
Q01826852	CLI	The SR4134 configuration file contains an invalid command syntax that causes errors on boot.
Q01831327	CLI	The SR1000 and SR3120 support a command at the root of the tree to change the command prompt. This command is not supported on the SR4134. The command is **prompt-pointer**.
Q01831945	CLI	The **file version** command displays unnecessary information.
Q01831995	CLI	The **show version** command displays unnecessary information.
Q01832047	CLI	The CLI help menu on the SR4134 displays the yellow alarm as disabled by default, when the default is actually generate/detect.
Q01832050	CLI	When you configure the terminal display using the **terminal length** command, the **show events** command is not affected. The display continues to stop at the default 25 lines.
Q01831310	Console	The default console timeout should match the default Telnet timeout (900 seconds).
Q01680944-01	DHCP	DHCP relay is not supported on VLAN interfaces.
Q01828412	IP	The SR4134 with approximately 210k routes freezes when **no ip address** is executed.
Q01828427	IP	The SR4134 with approximately 210k routes produces errors if IP address configuration is attempted.

Table 9
Issues in Release 10.0 that are resolved in Release 10.1.1 (cont’d.)

Change Request	Subsystem	Description
Q01825278	ISDN PRI	Only one BRI connection at a time can connect to an E1 PRI circuit.
Q01831316	Logging	System console logging is not enabled by default.
Q01826855	SNMP	Trap configuration is lost after reboot.
Q01831261-01	SNMP	SR4134 enterprise MIBS are incompatible with the SR1xxx and SR3xxx.
Q01757251	SSH	When used with SSH, the MOTD is not formatted correctly.
Q01826858	TACACS	When AAA is enabled with TACACS as the primary authentication and local authentication as the back-up, if the TACACS login fails, the local login is attempted. The local authentication should only occur if the TACACS server is inaccessible.
Q01823635	Telnet	The SSH and MOTD banners are not large enough and only appear after login.
Q01826860	Telnet	Reverse Telnet does not display the banner with initial login.
Q01826861	Telnet	The Reverse Telnet login prompt collides with the system message, not providing a readable login/password sequence.
Q01826864	Telnet	Reverse Telnet does not clear the call on the Telnet side of the router on exit.
Q01831913	Telnet	Telnet connections display an invalid Beta software banner at login.
Q01817949	VoIP-CALL CONTROL	The SR4134 sends a SIP invite with the from number as a 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 a 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.

Table 9
Issues in Release 10.0 that are resolved in Release 10.1.1 (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.
Q01807142	VoIP-FXS/FXO	The following issue is resolved by using rev. 10 of the FXS 2-port cards and rev. 12 of the FXS 4-port cards: A hissing sound is played to the caller before the ringback tone when set to A-law. In a hairpin call scenario between two FXS ports, if the compand-type on the called port is configured 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 only occurs when configuring A-law, which is used in Europe. The Release 10.1 (and 10.1.1) scope is limited to North America.
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.
Q01817111	VoIP-ISDN	The secure router 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.
Q01831290	VRRP	The **`show vrrp`** command does not display the Ethernet interface associated with each of the VRRP groups.

Known issues, limitations, and guidelines

The following table describes issues and limitations known to exist in the Secure Router 4134 Software Release 10.1.1, and provides guidelines for using Release 10.1.1 software.

Table 10
Known issues and limitations

Change Request	Subsystem	Description

Q01831324	CLI help	Better CLI context help requested similar to the SR1000 and SR3120.
		The SR4134 CLI context sensitive help differs from the SR1000/SR3120 products.
		With the SR4134, help text for mandatory parameters is displayed one at a time. To get help for the next mandatory parameter, enter "?" after the command.
		To get help for all optional parameters, enter "?" after the last mandatory parameter.
		
		For example, the following sample displays the SR4134 help for a command with two mandatory parameters and two optional parameters
		
		`SR4K/configure>` **`command ?`**
		`MandatoryParam1 Help for MandatoryParam1`
		
		`SR4K/configure>` **`command MandatoryParam1 ?`**
		`MandatoryParam2 Help for MandatoryParam2`
		
		`SR4K/configure>` **`command MandatoryParam1 MandatoryParam2 ?`**
		`OptionalParameter1 Help for OptionalParameter1`
		`OptionalParameter2 Help for OptionalParameter2`

Q01832669	CLI	No **`reload`** command.
Q01837875	CLI-Infrastructure	Enhancement request: allow multiple users to enter **`show running-config`**.
Q01838249	CLI	Enhancement request: allow more than one person in configuration mode at the same time.
Q01831322	Ethernet	Ethernet ports not enabled by default.

Table 10
Known issues and limitations (cont'd.)

Change Request	Subsystem	Description
Q01793197	CT3	Connecting CT3 to multiplexer 28 T1s alternately showing rais and rlof. This issue does not occur on active IN-SERVICE T1s. The issue occurs only on NON-ACTIVE T1s where no cables are connected to the mux (multiplexer). The issue is intermittent, and occurs only momentarily, and then recovers with the correct status.
Q01905118	DHCP relay	When the IP address is removed from an interface serving as a DHCP relay agent, the associated DHCP relay configuration is not removed.
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 nonexistent 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.
Q01909667	ISDN interface	The status of the ISDN interface does not display if the interface is looped. If the physical T1/E1 interface is looped, the interface status is not displayed on the console and the link does not come up. The engineer must recheck the pin configuration.

Table 10
Known issues and limitations (cont'd.)

Change Request	Subsystem	Description
Q01783728	LDP	The LDP FEC table does not remove an entry even though the Routing Table removed an 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 configure the Router ID on an interface IP address. You can use only loopback IP addresses as the Router ID. A feature enhancement that allows you to configure the Router ID using any interface IP address is planned for the next release of Secure Router 4134 software.
Q01793375	PSS	The multicast traffic is not forwarded to any interface, if one of the output interfaces has an MTU less than the packet size. In this scenario, the input interface is a 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 (with jumbo frames enabled) does not receive the packets.

Table 10
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: Regroup/pack the traffic flows so that there are fewer priority groups. For example, create only four priority groups.
Q01826857	SNMP	Traps do not display correctly on the console.
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.
Q01911622	VoIP-ISDN	Request for CLI command to control numbering plan for ISDN calls. The SR4134 does not support numbering plan configuration for ISDN Trunk. Dialed Number are always sent as UNKNOWN.
Q01912458	VoIP-ISDN	With calls between a SIP phone and an ISDN PRI circuit, the SR4134 does not transmit a BYE when the Content Length specified in the ACK message from the SIP phone does not match the exact length of the SDP.

Q01810252	xSTP	Show commands duplicate help and display different outputs.
		
		The display error is shown when you attempt a partial completion of the CLI command, as in the following example:
		
		`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:

Table 10
Known issues and limitations (cont'd.)

Change Request	Subsystem	Description
		DUT1# **show spanning-tree mstp instance ?** **OR** DUT1# **show spanning-tree mstp instance vlan ?**

Reimaging 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 reimage the module.

Nortel strongly recommends that you perform the following tasks 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 (www.update.microsoft.com) to obtain 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 10.1.1.

Table 11
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.
	Two-port ISDN BRI S/T small module for Secure Router 4134 (SR0000009E5) is currently on hold. Regulatory compliance testing for ISDN BRI S/T is in progress and is expected to achieve certification soon. A software patch will be made available to support ISDN BRI S/T after certification is complete.
PSS	IGMP multicast groups are 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 period of time, there is a chance that not all multicast addresses are learned. In this scenario, clear the multicast group so relearning of the multicast addresses can occur.
VLAN	A protocol-based VLAN classification rule can be successfully applied to an interface without the need to preconfigure the VLAN. In this scenario, the protocol-based rule will be inactive. Workaround: Create the VLAN (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 12
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 12
General guidelines and considerations for the Secure Router 4134 (cont'd.)

Subsystem	Description
cRTP	When cRTP is disabled on the bundle and 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 hot swap operation is performed on the primary interface (using the "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 to restore 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 removed from the **show module** submenu. Nortel no longer supports AT&T statistics reporting.
RMON	A hardware issue is preventing the acquisition of "drop event counter" information.
SNMP	You must disable memory protection before you access 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 12
General guidelines and considerations for the Secure Router 4134 (cont’d.)

Subsystem	Description
	This is a design limitation. 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 according to design and implementation.
DS3	The Clear Channel DS3 interface module does not currently support the use of the M13 framing format. Only use the default framing format of C-BIT on Clear Channel DS3 interface modules.
RSVP-TE	MPLS does not interwork correctly with interfaces where Firewall is enabled. In case of issues, 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.
ethernet0/0 and Layer 3	The management port (ethernet 0/0) does not support Layer 2 or 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 later) 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 that remain applicable for the 10.1.1 release.

Publications

See 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)
- *Nortel 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 Secure Router 4134 10.1.1 software from the Customer Service Portal site, atwww.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:

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 10.1.1

Release: 10.1.1
Publication: NN47263-400
Document status: Standard
Document revision: 03.02
Document release date: 5 September 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.