Nortel Secure Router 2330/4134

Release Notes

Release: 10.2
Document Revision: 04.02

www.nortel.com

NN47263-400

Nortel Secure Router 2330/4134
Release: 10.2
Publication: NN47263-400
Document release date: 7 October 2009

While the information in this document is believed to be accurate and reliable, except as otherwise expressly agreed to in writing NORTEL PROVIDES THIS DOCUMENT "AS IS" WITHOUT WARRANTY OR CONDITION OF ANY KIND, EITHER EXPRESS OR IMPLIED. The information and/or products described in this document are subject to change without notice.

Contents

New features

The Nortel Secure Router 2330/4134 Release 10.2 is for general use and is supported on the Secure Router 2330 Series and Secure Router 4134 platforms only.

New features for Release 10.2

The Nortel Secure Router 2330/4134 Release 10.2 provides interoperability of Secure Routers with other elements of the Nortel product and solutions families. Additionally, the new features address some regional requirements in markets outside of North America. This release makes feature support and deployment more consistent across the product range.

Navigation

- “IPv4 and IPv6 routing over VLAN interfaces” (page 10)
- “Selectable range for Ethernet ports” (page 10)
- “VLAN over GRE” (page 11)
- “DHCP and DHCP Relay over VLAN interfaces” (page 11)
- “DHCP Client on Ethernet Interfaces” (page 11)
- “Dial Backup through External Modem” (page 12)
- “VRRP over VLAN” (page 16)
- “ping to VRRP virtual IP” (page 18)
- “Multiple Syslog Server support” (page 19)
- “Multiple IP Helper Addresses on VLAN” (page 20)
- “OSPF NBMA over Ethernet” (page 22)
- “Source IP enhancements” (page 25)
- “Multiple SNTP Server support” (page 29)
- “Accounting under TACACS support” (page 31)
- “NAT ACL enhancements” (page 33)
- “Proxy DNS” (page 35)
- “ABOT Tunneling enhancement” (page 37)
- “PCAP over GRE” (page 38)
- “Displaying the active T38 fax call” (page 38)

Secure Router 2330 chassis

Release 10.2 supports the new Nortel Secure Router 2330 chassis.

The Secure Router 2330 is a modular, process-based multiservice platform designed to be used as customer premises equipment (CPE). The Secure Router 2330 provides multiservice capabilities for branch offices. It provides integrated LAN, security, and IP networking features in a low cost end router product. The Secure Router 2330 is capable of both Layer 2 and Layer 3 switching and also provides a platform for Metro Ethernet and for the delivery of Multiprotocol Label Switching (MPLS). It also supports WAN and voice interface connections in the form of interchangeable network modules.

For more information, see *Nortel Secure Router 2330 Installation — Chassis* (NN47263-304).

ADSL2+

With Release 10.2, the Secure Router 2330/4134 supports the Asymmetric Digital Subscriber Line (ADSL2+) small module. Digital Subscriber Line (DSL) technology enhances the data capacity of existing twisted-pair phone wire that runs between the local telephone company switching offices and most homes and offices.

For installation information, see *Nortel Secure Router 2330 Installation — Chassis* (NN47263-304).

For configuration information, see *Nortel Secure Router 2330/4134 Configuration — WAN Interfaces* (NN47263-500).

Nortel VPN client

Nortel virtual private network (VPN) client is a new feature for Release 10.2. With Nortel VPN client, remote users can securely connect to corporate resources by using a Nortel VPN client.

For more information, see *Nortel Secure Router 2330/4134 Security — Configuration and Management* (NN47263-600).

SIP Survivability

The SIP survivability feature is new for Secure Router 2330/4134 Release 10.2.

In a centralized SIP server architecture, the remote branches make use of the call processing resources available at a central location, generally located at the corporate headquarters. The SIP survivability feature enhances the feature set of the Secure Router 4134 (SR4134) and Secure Router 2330 (SR2330) by providing business continuity to the branch office in the event of a WAN connection outage to corporate headquarters. With this feature, employees at the branch office can continue to use SIP phones to place and receive intra-site calls and calls over the PSTN, including 911 calls.

The SIP survivability module (SSM) is a software-only subsystem on the Secure Router that provides SIP survivability capabilities. The SSM operates as a SIP Back to Back User Agent (B2BUA) that can back up a central SIP server by providing basic call services to connected endpoints at the branch if the WAN connection to the central SIP server fails.

For more information, see *Nortel Secure Router 2330/4134 Configuration — SIP Survivability* (NN47263-510).

SIP Media Gateway enhancements

Release 10.2 supports the following SIP Media Gateway enhancements:

- **CS 1000-specific Media Gateway configuration:**

Release 10.2 now supports additional Media Gateway configurations to provide specific support to the Nortel CS 1000 call server. These include configurations for keepalives, registration, and outbound proxy servers.

- **VoIP CDR:**

  Release 10.2 provides support for VoIP call detail records (CDR).

- **E1 R2 port configuration:**

  Release 10.2 provides support for R2 signaling on E1 ports. R2 signaling is a channel associated signaling (CAS) system developed in the 1960s that is still in use today in Europe, Latin America, Australia, and Asia. R2 signaling is defined in the ITU-T Q.400-Q.490 recommendations.

- **ISDN map:**

  Release 10.2 provides support to override the default ISDN type and plan generated by the router to configure custom values.

- **Enhancements for Mediation Server module midplane interface (servmod)**

  To provide further configuration flexibility, you can configure the Mediation server module midplane interface (**`interface servmod`**) for DHCP Relay. You can also add the interface to a VLAN.

For more information, see *Nortel Secure Router 2330/4134 Configuration — SIP Media Gateway* (NN47263-508).

OSPF demand circuits

Release 10.2 supports OSPF demand circuits, which are point-to-point links. The costs vary with usage. An example is an ISDN basic-rate service, whereby charges can be based both on connect time and on bytes/packets transmitted.

For more information, see *Nortel Secure Router 2330/4134 Configuration — IPv4 and Routing* (NN47263-502).

Multicast extensions to BGP

Release 10.2 supports Multicast extensions to BGP. You can direct all the multicast traffic to designated access points other than normal unicast forwarding paths using MBGP.

For more information, see *Nortel Secure Router 2330/4134 Configuration — IPv4 and Routing* (NN47263-502).

Multicast enhancements

Release 10.2 supports the following enhancements to multicast routing:

- **Static Multicast route:**

With release 10.2, the Secure Router 2330/4134 supports static multicast routes. Multicast static routes are unicast routes that allow multicast and unicast topologies to be incongruous. Multicast routing protocols use these routes to perform reverse-path forwarding (RPF) checks.

- **PIM-SM enhancements:**

  With Release 10.2, the Secure Router 2330/4134 supports additional PIM-SM features, including PIM multipath and Anycast RP.

- **DVMRP enhancements:**

  With Release 10.2, the Secure Router 2330/4134 supports additional configurable parameters for DVMRP.

- **IGMP enhancements:**

  With Release 10.2, the Secure Router 2330/4134 supports additional configurable parameters for IGMP, including the configuration of static IGMP groups and static SSM maps.

- **Multicast Routing over VLAN**

  With Release 10.2, you can enable multicast routing on VLAN interfaces.

For more information, see *Nortel Secure Router 2330/4134 Configuration — IPv4 Multicast Routing* (NN47263-504).

IPSec VPN without firewall

In Release 10.2, you can permit VPN to function with the firewall disabled on the Secure Router 2330/4134.

For more information, see *Nortel Secure Router 2330/4134 Security — Configuration and Management* (NN47263-600).

Self firewall policy with NAT for SIP ALG

Self-NAT allows the traffic generated from routers to be translated from a private IP address to a public IP address. You can use self-NAT to bind the Media Gateway and SSM to private IP addresses and handle the SIP ALG translation using a forward-NAT scenario.

For more information, see *Nortel Secure Router 2330/4134 Security — Configuration and Management* (NN47263-600).

Peer-to-peer RTP media

To provide support of Peer-Peer RTP media between trusted clients in the private realm, you can enable the Peer-Peer RTP media option **`sip-p2p-media`** under Global ALGs.

For more information, see *Nortel Secure Router 2330/4134 Security — Configuration and Management* (NN47263-600).

SIP ALG on TCP and UDP

In Release 10.2, you can enable the SIP ALG on TCP and UDP ports.

For more information, see *Nortel Secure Router 2330/4134 Security — Configuration and Management* (NN47263-600).

Traps generated when SFP inserted or removed

When traps are enabled, the Secure Router now generates a trap each time an SFP is inserted or removed from the chassis.

HDLC over MPLS pseudowire

Release 10.2 supports HDLC over MPLS pseudowire. With this feature, you can transmit HDLC traffic between sites over Ethernet packet-switched networks.

For more information, see *Nortel Secure Router 2330/4134 Configuration — MPLS* (NN47263-505).

MPLS over VLAN

Release 10.2 supports MPLS over VLAN interfaces. On the SR4134, the supported VLANs must consist of Chassis Ethernet ports only. VLANs containing any Module Ethernet ports cannot support MPLS. On the SR2330, VLANs containing any Ethernet port can support MPLS.

For more information, see *Nortel Secure Router 2330/4134 Configuration — MPLS* (NN47263-505).

IPv4 and IPv6 routing over VLAN interfaces

IPv4 and IPv6 routing are supported over VLAN interfaces.

For more information, see *Nortel Secure Router 2330/4134 Configuration — IPv4 and Routing* (NN47263-502) and *Nortel Secure Router 2330/4134 Configuration — IPv6 and Routing* (NN47263-503).

Selectable range for Ethernet ports

With Release 10.2 and later, you can specify a range of Ethernet ports to configure at the same time. To do so, you must use the **`interface range ethernet`** command.

For more information, see *Nortel Secure Router 2330/4134 Configuration — Layer 2 Ethernet* (NN47263-501).

VLAN over GRE

With Release 10.2, you can direct VLAN traffic over Ipv4 Generic Route Encapsulation (GRE) tunnels.

For more information, see *Nortel Secure Router 2330/4134 Security — Configuration and Management* (NN47263-600).

DHCP and DHCP Relay over VLAN interfaces

With Release 10.2, you can configure DHCP server and DHCP Relay on VLAN interfaces. For more information, see *Nortel Secure Router 2330/4134 Configuration — Network Management* (NN47263-602).

DHCP Client on Ethernet Interfaces

Secure Router 2330/4134 Release 10.2 provides support for Dynamic Host Configuration Protocol (DHCP) for IPv4 clients on Ethernet interfaces. A DHCP client obtains configuration parameters such as an IP address, default gateway, and DNS.

Using DHCP, a client can contact a central DHCP server that maintains a list of IP addresses available to be assigned on one or more subnets. The DHCP client requests an address from the pool and uses it temporarily to communicate on a network. In addition to this, the DHCP protocol is capable of supplying a client with important details about the network to which it is attached. This is important because a client can require these parameters during boot or normal run time.

The DHCP protocol client implementation allows the client to obtain an IP address and, if configured, a default gateway from the DHCP server. An interface specified as a DHCP client cannot be specified as a DHCP server. Likewise, an interface specified as a DHCP client cannot be specified as a relay agent.

As limitations, DHCP clients are not supported on sub-interfaces, and only works after the system has booted.

Configuring DHCP client on Ethernet interface

Use the following procedure to configure a DHCP client on an Ethernet interface.

Procedure steps

Step **Action**

1 To configure a DHCP client, enter Configuration Mode.

```
configure terminal
```

2 Enter Interface Mode.

```
interface <interface>
```

3 Specify a DHCP client lease.

```
dhcp-client lease <duration>
```

4 Specify a DHCP client hostname.

```
dhcp-client hostname <hostname>
```

5 Configure the client to request for the default router IP address to be provided by the server (if configured on the server).

```
dhcp-client request-default-router
```

6 Configure a route metric for the default route.

```
dhcp-client route-metric <route-metric>
```

7 Specify the retry interval.

```
dhcp-client retry-interval <interval>
```

8 Enable the DHCP client on the interface.

```
dhcp-client enable
```

--End--

Table 1
Variable definitions

Variable	Value
<duration>	Specifies the duration of the lease in the range 30–4294967.
<hostname>	Specifies the hostname of the DHCP client.
<interface>	Specifies the interface to work with.
<interval>	Specifies the timeout interval, in seconds, for the DHCPv4 client negotiation process.
<route-metric>	Specifies a route metric for the default route: 1–254. Default value is 254.

Dial Backup through External Modem

Release 10.2 provides Dial Backup support for the Secure Router 4134 only. Dial Backup support enables redundancy for routes by using PPP bundles created over a dialup connection. The dialup connection becomes active when a primary route goes down.

The Secure Router connects to an external modem through the Aux port and establishes a dialup connection to a phone number specified in the backup PPP configuration using a feature called Dial-on-Demand Routing (DDR). There are two types of Dial-on-Demand Routing:

- **Dial-on-Demand Routing**—Dials when traffic needs to traverse a link
- **Backup Dial-on-Demand Routing**—Dials when a designated primary interface goes down. You can configure a Backup Dial-on-Demand Routing interface by including the appropriate backup commands to a normal DDR interface configuration.

The IP address for the bundle is specified in the bundle configuration.

The Backup DDR mechanism

The Secure Routers use the Floating Static Route mechanism to automatically dialup to backup another route. To accomplish this, a secondary route is specified in addition to the primary route, with an administrative distance greater than the primary route. When the primary interface is functional, it is used to route traffic. If the primary interface goes down, packets are automatically sent to the backup interface where they trigger commands to dial a connection. A keepalive time is specified by the user during bundle configuration so that commands are automatically sent to disconnect a connection when there is no traffic for the allowed keepalive time period.

To allow this feature to function properly, the following Hayes AT commands are supported through the CLI:

Table 2
Supported Hayes AT commands

S0	Rings to auto answer
S1	Ring counter
S7	Wait for carrier after dialing
S9	Carrier detect response time
S10	Lost carrier hang up delay

Table 3
Programmed modem default settings

S2	Escape character
S3	Carriage return character
S4	Line feed character
S37	Line connection speed

Table 3
Programmed modem default settings (cont'd.)

V1	Result code is sent in work form
X1	Sends OK, CONNECT, RING, NO CARRIER, ERROR, NO ANSWER and CONNECT SPEED

Table 4
Operation commands

A	Cause modem to go off hook, works with ring detection
D	Dial digit
E0	Echo off
H0	On hook
H1	Off hook
N1	Enable auto mode
+++	Mode change between data or command mode

Users have the option of creating multiple PPP backup bundles containing different configuration criteria and specifying them by order of priority. At this time, the Secure Routers contain only one Aux port, however the design of the feature is easily scalable should the option of multiple Aux ports become available.

The modems currently supported by this feature include Creative Blaster V9.2, Diamond Supra Max V9.2 and Best Data 56 K v9.2/v4.4.

Configuring Dial Backup through external modem

Use the following procedure to configure Dial Backup through external modem.

Procedure steps

Step **Action**

1 To configure dial backup, enter Configuration Mode.

```
configure terminal
```

2 Create a dialer.

```
dialer <name>
```

3 Configure the UART baud rate.

```
async uart rate <baudrate>
```

4 Configure the UART parity setting.

```
async uart parity <setting>
```

5 Configure UART stop bits.

```
async uart stopbits <stopbits>
```

6 Configure the phone number to be called by the modem.

```
async modem phone-num <number>
```

7 Configure the number of rings before answering.

```
async modem answer <rings>
```

8 Configure the number of rings to wait during call setup.

```
async modem call-set-timeout <rings>
```

9 Configure the dial method.

```
async modem dial-method {tone | pulse}
```

10 Configure using an AT string.

```
modem async at <at_string>
```

11 Enable the async configuration.

```
async modem enable
```

12 Configure the dialer idle-timeout interval.

```
idle-timeout <timeout>
```

13 Configure management CLI service mode.

```
answer-mode [enable | disable] [priority {high | low}]
```

14 Exit back a level.

```
exit
```

15 To attach to a bundle, create a bundle.

```
interface bundle <bundlename>
```

16 Configure the bundle to use the dialer.

```
link dialer <dialer>
```

17 Continue normal configuration of the bundle.

--End--

Table 5
Variable definitions

Variable	Value
<at_string>	Specifies the AT string used to configure the dialer.
<baudrate>	Specifies the Baud rate of the modem. Default is 56000.
<bundlename>	Specifies the name of the bundle.
<databits>	Specifies the number of databits. Default is 8.

Table 5
Variable definitions (cont'd.)

Variable	Value
<dialer>	Specifies the dialer name to link, maximum 8 characters.
<name>	Specifies the dialer name, maximum 8 characters.
<number>	Specifies the phone number, maximum length 25 characters, with or without hyphens. Prepending p or t indicates pulse or tone dialing.
<rings>	Specifies the number of rings, in the range 1–255.
<setting>	Specifies the parity setting—none, even, or odd. Default is none.
<stopbits>	Specifies the number of stopbits—1, 2, or 3. Default is 1.
<timeout>	Specifies the idle timeout time, in the range 1–6000. Default is 180.

VRRP over VLAN

Secure Router 2330/4134 Release 10.2 provides support for VRRP over VLAN interfaces. By design, VRRP eliminates a common point of failure present in static routing environments by specifying an election protocol to dynamically assign routing responsibility to a VRRP router on a LAN. VRRP is used to maintain availability at the IP address level. In a VRRP setup, one router is elected the master. When the master goes down, backup routers hold an election for a replacement. VRRP is applicable only to primary ethernet interfaces and VLAN interfaces, with a maximum of 50 VRRP groups for each router. You can configure a maximum of 10 VRRP groups per interface.

The nature of VRRP has several routers performing as one virtual router that has a Virtual Router ID and virtual IP addresses. Any of these routers can act as master at any time, provided it wins the election. The master sends advertisements to backup routers informing them of its state. If advertisements fail to be received, an election is called. The backup with the highest priority value wins and assumes position as master. As of this release, the interval at which these advertisements are sent is configurable through CLI.

In this release, VRRP interface monitoring on VLAN interfaces functionality has been included. VRRP groups can be configured to monitor external interfaces in case they go down. The reason for this is to calculate VRRP priority based on a router's tracking priority. When a router's external interface goes down, the number value given to tracking priority is subtracted from the VRRP priority value, giving it a new priority and ultimately affecting its chances in an election.

Configuring VRRP over VLAN

Use the following procedure to configure VRRP over VLAN.

Procedure steps

Step	Action
1	To configure VRRP over VLAN, enter Configuration Mode. `configuration terminal`
2	Enter VLAN database configuration mode. `vlan database`
3	Create the VLAN. `vlan <vid>`
4	Exit VLAN database configuration mode. `exit`
5	Select a port to add to the VLAN. `interface <interface-type> <slot/port>`
6	Add the port to the VLAN. `switchport mode <mode> allowed vlan <vids>`
7	Exit from interface configuration mode. `exit`
8	Select the VLAN interface. `interface vlan vlan <vid>`
9	Assign an IP address to the VLAN `ip address <A.B.C.D> <subnet-mask>`
10	Specify a VRRP group. `vrrp <group>`
11	Specify a virtual IP address. `ipaddr <virtual IP>`
12	Configure tracking. `track <interface> <priority>`
13	Configure a priority level. `priority <level>`

14 Enable VRRP.

```
enable
```

--End--

Table 6
Variable definitions

Variable	Value
<A.B.C.D> <subnet-mask>	Specifies the IP address and subnet mask of the sub-interface.
<group>	Specifies the VRRP group number, in the range 1–255.
<interface>	Specifies the interface to work with.
<interface-type> <slot/port>	Specifies the interface type, slot, and port of the VLAN member port.
<level>	Specifies the priority level, in the range 1–254.
<mode>	Specifies the Layer 2 interface mode. Possible choices are: • access • hybrid • trunk • l2vpn
<priority>	Specifies the track priority.
<type>	Specifies the type of encapsulation to apply.
<vid>	Specifies the VLAN ID.
<virtual IP>	Specifies the virtual IP address to be used.

ping to VRRP virtual IP

Secure Router 2330/4134 Release 10.2 provides support for replies to ping packets sent to the VRRP virtual IP.

If a Secure Router is the master of the VRRP address but the VRRP address is virtual, in other words, the physical interface of the master 2330/4134 does not equal the VRRP address, you can configure the router to allow the VRRP master to respond to a ping to the VRRP address. This is accomplished through the CLI using the **vrrp-virtualip** configuration command.

Configuring ping to VRRP virtual IP

Use the following procedure to configure ping to VRRP virtual IP.

Procedure steps

Step	Action
1	To enter the configuration mode, enter: `configuration terminal`
2	To select ping to virtual IP configuration, enter: `vrrp-virtualip`
3	To enable ping to virtual IP, enter: `allow-ping`
4	To disable ping to virtual IP, enter: `no allow-ping`
5	To display the status of ping to virtual IP, enter: `show vrrp virtualip-setting`

--End--

Multiple Syslog Server support

Secure Router 2330/4134 Release 10.2 provides support for multiple Syslog server. A Syslog Server monitors incoming Syslog messages on UDP ports and decodes them for logging purposes. In addition, several network devices can be configured to generate Syslog messages. In the past, the Secure Router only provided support for logging on a single Syslog Server, but this enhancement allows for the configuration of up to five Syslog Servers. Because they are logged simultaneously, all Syslog servers contain the same Syslog records.

To achieve backward compatibility with the existing Syslog implementation, the provision of a port number during configuration of the host IP address remains optional. If a user does not specify a port during CLI configuration, UDP port 514 is used by default. In addition, the enabling of message logging remains unchanged.

As a limitation, all enable or disable functions apply to all configured servers. Configuration of Syslog message logging on selected servers is not supported.

When viewing Syslog Server information, the SNMP interface can only display information for one server at a time.

Configuring multiple Syslog servers

Use the following procedure to configure multiple Syslog servers.

Procedure steps

Step	Action
1	To configure multiple Syslog servers, enter Configuration Mode. `configuration terminal`
2	Enter the **`system logging`** command tree. `system logging`
3	Access the Syslog command tree. `syslog`
4	Specify a host IP address and UDP port. If a port number is not specified, port 514 is used by default. `host_ipaddr <A.B.C.D> [port]`
5	To add another Syslog server address, repeat step 4 until up to 5 Syslog servers are added.
6	Enable Syslog. `enable`

--End--

Table 7
Variable definitions

Variable	Value
<A.B.C.D>	Specifies the host IP address.
[port]	Specifies (optionally) the UDP port. If not specified, port 514 is used by default.

Multiple IP Helper Addresses on VLAN

Secure Router 2330/4134 Release 10.2 provides support for Multiple IP Helper. The Multiple IP Helper feature assists in broadcasting network traffic between client machines and servers residing on different subnets. There are situations in which a user can want to control which broadcast packets and protocols should be forwarded by the router. The Multiple IP Helper feature provides this functionality.

Multiple IP Helper is useful when UDP broadcasts are sent to a DNS server by a network host. If the network host happens to reside on a segment without a DNS server, the UDP broadcast fails. A helper address is configured and a protocol assigned to an interface. The exceptions to this are DHCP and BOOTP broadcasts, which are handled by DHCP Relay.

The Multiple IP Helper feature has been implemented on primary ethernet interfaces and VLAN-enabled ethernet sub-interfaces, with a maximum of six helper addresses can be configured for each interface.

Configuring multiple IP Helper addresses

Use the following procedure to configure IP Helper addresses.

Procedure steps

Step	Action
1	To configure IP Helper addresses, enter Configuration Mode. `configure terminal`
2	To configure an interface, enter Interface Mode. `interface vlan vlan <id>`
3	Specify an IP address. `ip address <A.B.C.D/M>`
4	Specify a Helper address. `ip helper-address <A.B.C.D> [service <service>] [protocol <protocol>] [port <port>]`
5	To add up to six Helper addresses, repeat the previous step.

--End--

Table 8
Variable definitions

Variable	Value
<A.B.C.D>	Specifies the IP address.
<A.B.C.D/M>	Specifies the IP address, followed by subnet mask.
<id>	Specifies the VLAN ID.
<port>	Specifies the port number in the range 1–65535..
<protocol>	Specifies the protocol to be used. Options available are: • **UDP**—to a specific UDP port.
<service>	Specifies the service name to specify IP helper for a service. Available options are: • **dns**—Domain Name Service • **netbios-dgm**—NetBIOS datagram service • **netbios-ns**—NetBIOS name service • **netbios-ss**—NetBIOS session service

Table 8
Variable definitions (cont'd.)

Variable	Value
	- **tftp**—Trivial File Transfer Protocol - **time**—Time

OSPF NBMA over Ethernet

Secure Router 2330/4134 Release 10.2 provides support for OSPF non-broadcast multi-access (NBMA) over Ethernet. While it is well known that OSPF operates in peer-to-peer and broadcast networks, its role in another kind of network can be just as important. A non-broadcast network operates between point-to-point and broadcast networks, and does not include broadcast or multicast functionality. Its purpose is to connect more than two devices to the same physical media device and, by nature, it is multi-access. Some examples of this are Frame Relay networks, ATM networks and x.25 networks.

To achieve this functionality, some components of OSPF have been modified in an attempt to mirror functionality found in OSPF broadcast networks. Two modes of operation on these types of OSPF networks are NBMA and P2MP. When using NBMA, operation over a broadcast network is emulated by OSPF. The NBMA network has a router designated to originate a network LSA. NBMA mode is the most efficient way to run OSPF over non-broadcast networks, both in terms of link-state database size and in terms of the amount of routing protocol traffic.

When deploying OSPF on a network, neighbor discovery is achieved using multicast hello packets. Designated Routers (DR) and Backup Designated Routers (BDR) are elected for each multicast network to optimize adjacency building. All routers in a segment communicate directly with a DR or BDR for proper adjacency. For a neighbor to be successfully discovered on a segment, broadcast and multicast packet sending must be allowed on the network.

When using NBMA technology, neighbors are not discovered automatically due to the non-broadcast nature of the feature. Instead, OSPF attempts to designate a DR and a BDR, but the election fails because no neighbors are discovered. To overcome this issue, neighbors must be manually configured.

Broadcast vs non-broadcast networks

One difference between broadcast and non-broadcast networks is in the functionality of the hello protocol. On a broadcast network, a router advertises itself using hello packets allowing itself to be discovered dynamically. These packets include the router's DR identity and a list of routers who have recently sent Hello packets. On NBMA networks, some configuration must take place before successful operation of the hello protocol. Routers that are potential DRs have a list of all other routers currently attached. If a DR candidate, a router sends Hello packets to other candidates in an attempt to find a DR. If elected DR, a router sends hello packets to all other routers on the network. To minimize the number of hello packets sent, the number of eligible routers on a NBMA network should be kept to a minimum.

The behavior of router’s hello packet sending depends on its status as potential DR. If eligible, it must send hello packets to eligible neighbors periodically. If the router becomes the DR or BDR, it expands distribution of hello packets to include all neighbors, regardless of eligibility. If a router is not eligible, it must send hello packets to the DR and BDR periodically, along with sending a reply hello packet to any hello packet received from an eligible neighbor. Frequency of hello packets depends on a neighbor’s state. When down, hello packets are sent at Poll Interval, otherwise they are sent at Hello Interval.

Another difference comes when identifying a neighbor address. In a point-to-point network or virtual link, the neighbor is identified by router ID. However, in a broadcast, point-to-multipoint or NBMA network, the neighbor is identified by IP source address.

Finally, in an OSPF operation specific to NBMA, OSPF generates a start event to a neighbor after the neighbor command is issued. Then hello packets begin to be sent to a neighbor using the Hello Interval as a frequency. This causes the neighbor to receive an ATTEMPT message that indicates no recent information has been received from the neighbor and that a greater effort is to be to contact that neighbor. To achieve this, up to four hello packets are sent to the neighbor. If no response is received, a DOWN state is entered, where packet frequency is reduced to that of the Poll Interval.

Configuring OSPF NBMA over Ethernet

Use the following procedure to configure OSPF NBMA over Ethernet. There are three main components to configuring OSPF NBMA. First, you specify the interface network type. This is followed by specifying neighbors and a poll interval.

Procedure steps

Step	Action
1	To configure OSPF NBMA, enter Configuration Mode. `configure terminal`
2	Specify a router ID for OSPF.

```
router router-id <X.X.X.X>
```

3 Enable OSPF.

```
router ospf <process-id>
```

4 Configure the OSPF area.

```
area <areaid>
```

5 Enable OSPF on a network.

```
network <network>
```

6 Exit from OSPF configuration mode.

```
exit
```

7 Select an interface in the OSPF network.

```
interface <interface-type> <interface>
```

8 Configure the OSPF network type.

```
ip ospf network <network-type>
```

9 Exit the interface configuration mode.

```
exit
```

10 Enter OSPF router configuration mode.

```
router ospf
```

11 Configure neighbors, repeating this step for each neighbor you want to add.

```
neighbor <A.B.C.D>
```

12 Configure the poll interval.

```
poll_interval <interval>
```

--End--

Table 9
Variable definitions

Variable	Value
<A.B.C.D>	Specifies the IP address.
<areaid>	Specifies the OSPF area ID.
<process-id>	Specifies the OSPF process ID; value ranges from 1–65535.
<interface>	Specifies the interface to work with.
<interface-type>	Specifies the type of the interface.
<interval>	Specifies the poll interval.

Table 9
Variable definitions (cont'd.)

Variable	Value
<network>	Specifies the network number <A.B.C.D> or the IP network prefix <A.B.C.D/M>.
<X.X.X.X>	Specifies the router ID IP address.
<network-type>	Specifies the OSPF network type. Available options are: • broadcast—OSPF broadcast multi-access • non-broadcast—OSPF NBMA network • point-to-multipoint—OSPF point-to-multipoint network • point-to-point—OSPF point-to-point network

Source IP enhancements

Secure Router 2330/4134 Release 10.2 provides support for adding source address information to existing services. The services modified to accept a source address are:

- File Transfer
- RADIUS
- SNMP
- SNTP
- Syslog
- TACACS

The source address parameter is configurable on a global basis, where all the above services are configured with the same source address. The exception to this is when the source address is configured separately for the service, in which case the service configuration takes precedence. The source address can be configured using the IP address or the interface name.

To accommodate this enhancement, all router output displays that contain a "source address" field displays the source IP address and the interface name associated with it. If the feature is configured by IP address, but has no associated interface specified, the interface shows as "not configured". Likewise, if the feature is configured by interface name, with no IP address specified, the IP address shows as "not configured". Global source address information can be found using the "show system configuration" command.

The new command "source-address" has been added to enable this feature. In the case of Radius and SNMP, the previous commands (src_address and snmp-source respectively) have been deprecated in lieu of this new command.

Because file transfer commands are not stored in a configuration, it uses the global source address if configured. Each of the file transfer commands accepts a source-address parameter to override the global source address.

WARNING
When a source address is configured for a service which is valid (IP address and interface associated with it) and the source-address interface is down, the service can fail to work if it is bi-directional. By using a loopback interface for the source address which is always up, it ensures that the above problem does not occur.

Source IP limitations

In Release 10.2 release, the following are the limitations for the Source IP feature:

- RADIUS: With RADIUS, the configured source IP address goes into the Network Access Server (NAS) IP address attribute.
- FTP: For FTP, the source IP feature accepts only the global source IP (system source IP) and does not accept an FTP-specific source IP.
- TFTP: The source IP feature is not supported for TFTP in this release.

Configuring global source address

Use the following procedure to configure source addresses on services.

Procedure steps

Step	Action
1	To configure source addresses for a service, enter Configuration Mode. **`configuration terminal`**
2	Configure the global source address. **`system source-address <[ip-address]	[interface-name]>`**

--End--

Table 10
Variable definitions

Variable	Value
[ip-address]	Specifies the source address by IP address.
[interface-name]	Specifies the source address by interface name.

Configuring Radius or TACACS source address

Use the following procedure to configure Radius or TACACS server source address for all services.

Procedure Steps

Step	Action
1	To configure source addresses for a service, enter Configuration Mode. `configuration terminal`
2	To configure Radius or TACACS source addresses, enter the **`aaa`** command sub-tree. `aaa`
3	Configure the source address. `source-address <[ip-address] | [interface-name]>`

--End--

Table 11
Variable definitions

Variable	Value
[ip-address]	Specifies the source address by IP address.
[interface-name]	Specifies the source address by interface name.

Configuring SNMP source address

Use the following procedure to configure SNMP server source address for all services.

Procedure Steps

Step	Action
1	To configure source addresses for a service, enter Configuration Mode. `configuration terminal`

2 Enter the `snmp-server` subtree.

```
snmp-server
```

3 Configure the source address.

```
source-address <[ip-address] | [interface-name]>
```

--End--

Table 12
Variable definitions

Variable	Value
[ip-address]	Specifies the source address by IP address.
[interface-name]	Specifies the source address by interface name.

Configuring SNTP source address

Use the following procedure to configure SNTP server source address for all services.

Procedure Steps

Step **Action**

1 To configure source addresses for a service, enter Configuration Mode.

```
configuration terminal
```

2 Enter the `sntp` subtree

```
sntp
```

3 Configure the source address.

```
source-address <[ip-address] | [interface-name]>
```

--End--

Table 13
Variable definitions

Variable	Value
[ip-address]	Specifies the source address by IP address.
[interface-name]	Specifies the source address by interface name.

Configuring Syslog source address

Use the following procedure to configure Syslog server source address for all services.

Procedure Steps

Step	Action
1	To configure source addresses for a service, enter Configuration Mode. `configuration terminal`
2	Enter the **`system logging`** subtree. `system logging`
3	Enter the **`syslog`** subtree. `syslog`
4	Configure the source address. `source-address <[ip-address]	[interface-name]>`

--End--

Table 14
Variable definitions

Variable	Value
[ip-address]	Specifies the source address by IP address.
[interface-name]	Specifies the source address by interface name.

Multiple SNTP Server support

Secure Router 2330/4134 Release 10.2 provides support for the Multiple Simple Network Time Protocol (SNTP) Server feature. SNTP is a simple form of the Network Time Protocol (NTP), which is an internet protocol used for synchronization of computer clocks.

The Multiple SNTP Server feature provides support for up to 10 SNTP servers. Multiple servers provide redundant backup for synchronizing time on the Secure Router. During configuration, servers can be specified by hostname or IP address, and a timeout value must be set for the query. The Multiple SNTP Server features operates by having the SNTP service query configured SNTP servers on a round-robin basis. If an SNTP server is queried and fails to respond, the router sends a request to the next configured SNTP server. The SNTP server support is not active until the service is enabled. While the service is enabled the configuration cannot be changed.

The "show sntp" command has been modified to display the current state of SNTP, the server it is contacting to receive the current time, as well as all configured servers. When specifying a server by domain name, DNS entries need to be configured before SNTP functions properly.

Configuring multiple SNTP servers

Use the following procedure to configure multiple SNTP servers.

Procedure steps

Step **Action**

1 To configure multiple SNTP servers, enter Configuration Mode.

```
configure terminal
```

2 Because DNS entries must be configured for SNTP to function properly, configure primary and secondary DNS servers.

```
ip pname_server <address>
ip name_server <address>
```

3 To configure an SNTP server, enter the sntp sub-tree.

```
sntp
```

4 Configure the source address of the SNTP client.

```
source-address <address>
```

5 Configure the number of retries for each SNTP server.

```
retries <count>
```

6 Configure an NTP server.

```
server <server> [timeout]
```

7 To add up to 10 SNTP servers, repeat step 6.

8 Enable the SNTP client.

```
enable
```

--End--

Table 15
Variable definitions

Variable	Value
<address>	Specifies an IP address.
<count>	Specifies the number of retries the NTP server performs, in the range 1–5. Default is 3.
<server>	Specifies the NTP server to use for updates.
<timeout>	Specifies the maximum response time, in the range 10–7200. Default is 1024.

Accounting under TACACS support

Secure Router 2330/4134 Release 10.2 provides support for Terminal Access Controller Access Control System (TACACS) accounting. This feature allows an administrator to audit user activity on a router at any date or time or both. TACACS accounting details what commands were issued by a particular user.

The TACACS accounting system tracks and stores Attribute Value data on a TACACS accounting server. This accounting data includes details such as user name, the user’s IP address, a timestamp and the activity—perhaps a Login or execution of a particular command. The data can then be analyzed for user activity on a router at any date or time. For example, when a user connects to an interface remotely through Telnet or SSH using the correct username and password, a log is written and can be viewed on the TACACS server.

All accounting methods must be defined through Authentication Authorization Accounting (AAA). Much like AAA, TACACS accounting is configured through the definition of a named list of accounting commands with specific methods, and then applying this list to one or more interfaces.

The two main TACACS accounting commands are as follows:

- **network**—If applied to an interface, enables accounting for user login and logout.
- **commands**—If applied to an interface, enables accounting for all commands executed by a user.

The methods of TACACS accounting are as follow:

- **stop-only**—If specified, sends a notice to stop record accounting at the end of the specified activity.
- **start-stop**—If specified, sends a notice to start record accounting after a process begins and sends a notice to stop record accounting at the end of the specified activity. This allows the requested user process to begin even if the start accounting record was not acknowledged by the accounting server.
- **wait-start**—If specified, sends a notice to start and stop accounting to the accounting server. In this scenario, the user service does not begin until the start accounting record is acknowledged.

  Note: If you create an accounting method list with a list name of "default", all interfaces uses this list without applying it on an interface. You can override this "default" list only when you create an explicit method list and apply it to the interface.

Configuring TACACS accounting

Use the following procedure to configure TACACS accounting.

Procedure steps

Step	Action
1	To configure TACACS accounting, enter Configuration Mode. `configure terminal`
2	Enter the aaa command sub-tree. `aaa`
3	Configure an access-list for commands. `accounting commands <listname| [default]> {start_stop|stop_only|wait-start}`
4	Configure an access-list for a network. `accounting network <listname| [default]> {start_stop|stop_only|wait-start}`
5	Exit back a level. `exit`
6	Enter Interface Mode. `interface <interface>`
7	Apply accounting to the interface. `aaa accounting {commands|network} <list>`

--End--

Table 16
Variable definitions

Variable	Value
{commands|networks}	Specifies the type of accounting to apply to the interface.
<interface>	Specifies the interface to work with.
<list>	Specifies the list to apply to the interface.

Table 16
Variable definitions (cont'd.)

Variable	Value
<listname>	Specifies the name of the accounting list. If list name is specified as "default", all interfaces use this list without further configuration.
{start_stop|stop_only|wait-start}	• start_stop—Start and Stop records are sent. • stop_only—Only Stop records are sent. • wait-start—Start and Stop records are sent, but service starts after acknowledgement.

NAT ACL enhancements

Secure Router 2330/4134 Release 10.2 provides support for NAT ACL enhancements. These enhancements add flexibility in configuring a network Access Control List (ACL). Access Control Lists are used to filter packets going to the global NAT subsystem. A separate ACL is allowed for static translation, dynamic port translation, and dynamic address translation modules. Access Control Lists are applied to both outbound and inbound traffic for translation.

If a packet matches a permit rule, the packet enters that NAT module. If a packet matches a deny rule, it is transmitted without being modified. In the event a packet traverses all NAT ACLs without a rule match, the packet is dropped. One single NAT ACL is allowed in the Global NAT module to control access. The Global NAT ACL can be applied selectively to an interface.

NAT ACL Packet Processing

The following section contains information about Packet Translation in a forwarding scenario for both incoming and outgoing packets.

Outgoing Packet Translation During outgoing packet translation, packets sent from a private client to a host on a public network are known as outgoing packets. NAT translation is enabled on the public interface. An ACL is applied if either the inbound interface ACL is enabled on a private interface or if the outbound interface filter is enabled on a public interface. A check is performed on the outgoing interface for NAT ability prior to the packet being sent out.

If an outgoing packet matches a static translation route, the packet is translated and sent. If ACL filters are configured for Address NAT, the following actions are taken:

- Packet is translated if it matches a permit rule
- Packet is forwarded, without being translated if it matches a deny rule

- Packet is forwarded to Address NAT module if no rule is matched.
- In the case of Dynamic Address NAT, if the module is not enabled the packet is dropped.

In the case of Dynamic Address NAT, if the module is not enabled the packet is dropped.

Incoming Packet Translation Packets returned to the private client from a host in a public network are known as Incoming Packets. After the packet is received, prior to route lookup, processing of address translation for the incoming packets takes place. All inbound packets are subjected to reverseACL to apply NAT translations; reverse ACL is enabled by default.

Configuring NAT ACL

Use the following procedure to manually configure a NAT ACL.

Procedure steps

Step	Action
1	To configure NAT ACL, enter Configuration Mode. `configure terminal`
2	Enter the **`ip nat`** subtree. `ip nat`
3	Create an access list. `access-list <listname>`
4	If applicable, specify an address or range to permit. `add permit ip <range-start> <range-end>`
5	If applicable, specify an address or range to deny. `add deny ip <range-start> <range-end>`
6	Exit the *access-list* configuration to finish or create another. `exit`
7	Create an address pool. `pool <poolname>`
8	Specify the address pool range. You can specify more than one range using the same command syntax. `range <range-start> <range-end> <mask>`
9	Exit the address pool configuration. `exit`
10	Configure an access group to use the address pool.

```
access-group <groupname> address-pool <poolname>
```

11 If applicable, configure ACL access to a specific NAT module.

```
access-group <groupname> {static | dynamic | address}
```

--End--

Table 17
Variable definitions

Variable	Value
<groupname>	Specifies the name of access group.
<listname>	Specifies the name of the Access Control List.
<mask>	Specifies the subnet mask of a supplied address range.
<poolname>	Specifies the identifying name of address pool.
<range-end>	Specifies the range end address used when configuring an ACL.
<range-start>	Specifies the address to add or range-start address used when configuring an ACL.
{static | dynamic | address}	Specifies the NAT module to which the ACL applies—static translation, dynamic port translation, or dynamic address translation.

Proxy DNS

Secure Router 2330/4134 Release 10.2 provides support for Proxy DNS. Proxy DNS receives a request from a host, resolves the domain name through communication with the DNS server, and sends the response to the host. Proxy DNS is disabled by default.

Previously, if a master link connected to an ISP-based DNS server went down, DNS queries could not be resolved. The solution to this issue would have been to change the DNS server IP address to the address of a backup link. Even though a Windows-based PC host can be configured with up to 10 DNS server entries, it is often not feasible to configure this many DNS servers on every available host. With the addition of Proxy DNS, the solution becomes much more simple.

Proxy DNS functions in such a way that it receives a request from a client and sends a response back. The DNS server is specified as the interface address connecting the PC to the router. Using Proxy DNS, clients do not need to worry about an ISP link or an exact DNS server, as the Proxy DNS feature handles these. In the case of a host, all that is required is configuration of the interface address of the router as the DNS server address.

The Proxy DNS feature supports multiple static (two) or dynamic (four) DNS server entries, of which any static entries have higher precedence. Dynamic entries can be added to the list of DNS servers by DHCP and PPPoE modules during registration of the module and can be removed when unregistered. When a client makes a request to Proxy DNS for the address of a particular domain name, Proxy DNS contacts a list of DNS servers in succession to resolve the domain name. When the domain has been resolved to an IP address, the entry is added to the cache and sent to the requesting client. When a DNS response is received from the DNS server, it is stored in the cache for the length of time specified by the TTL received for the particular name. The cache supports up to 80 entries. If a client queries for a previously cached domain, Proxy DNS responds with the cached entry. Removing the need to contact the DNS server for this entry reduces traffic. When the cache table reaches its 80 entry capacity, older dynamic cache entries are removed to accommodate the new entries.

The DNS client remains functioning as it did previously, as long as a primary and secondary name server exists.

Configuring Proxy DNS

Use the following procedure to manually configure the proxy DNS feature to cache an address.

Procedure steps

Step **Action**

1 To configure proxy DNS, enter Configuration Mode.

```
configure terminal
```

2 Ensure a DNS server has been configured.

```
ip name_server <address>
```

3 Optionally, add a second DNS server.

```
ip name_server <address>
```

4 Enable Proxy DNS.

```
ip proxy-dns enable
```

5 Add a DNS cache entry through the CLI.

```
ip proxy-dns add-cache <domain>
```

--End--

Table 18
Variable definitions

Variable	Value
<address>	Specifies the primary name server address.
<domain>	Specifies the domain to add to the proxy cache.

ABOT Tunneling enhancement

Secure Router 2330/4134 Release 10.2 contains enhancements to existing IPSec Asymmetric Branch Office Tunneling (ABOT) functionality. Because the Secure Router must be able to respond in multiple scenarios to match a CES-configured ID, a command "key-id" has been added. Further, because the Secure Router sends an INITIAL-CONTACT message at the end of negotiation that causes the CES to delete its SA, a CLI command has been added to disable the message.

Configuring ABOT tunneling enhancements

The following procedure describes how to configure the ABOT tunneling enhancement.

Procedure Steps

Step **Action**

1 To configure ABOT tunneling enhancements, enter Configuration Mode.

```
configure terminal
```

2 Enter the `crypto` subtree of commands.

```
crypto
```

3 Create a policy.

```
ike policy to-ces <address>
```

4 Configure the key-id to match.

```
local-id key-id <key>
```

5 Configure a local address.

```
local-address <local address>
```

6 Disable initial contact.

```
no initial-contact
```

7 Exit the `crypto` subtree.

```
exit
```

--End--

Table 19
Variable definitions

Variable	Value
<address>	Specifies the mapped address of the server.
<key>	Specifies the key to match.
<local address>	Specifies the local address of the server

PCAP over GRE

Packet Capture (PCAP) is now supported on GRE tunnels.

To configure a packet capture session for a GRE tunnel interface, use the following procedure.

Procedure 1
Procedure steps

Step	Action
1	To specify the PCAP name to configure, enter: `debug pcap capture <capture-name>`
2	To assign the PCAP name to the GRE tunnel interface, enter: `attach tunnel <tunnel-name>`

--End--

Displaying the active T38 fax call

To display information for the active T38 fax call, use the following procedure.

Procedure 2
Procedure steps

Step	Action
1	To display active T38 fax call information, enter: `show call active T38` This command does not display pass-through fax call information.

--End--

Scalability and important notices

This section contains information on scalability and important notices for certain features.

Supported software and hardware capabilities

The following tables list supported software and hardware capabilities for Secure Router 2330/4134 Software Release 10.2. For additional scaling information and design guidelines, contact your Nortel representative.

ATTENTION
No hard limits exist on the number of static routes supported on the Secure Router 2330/4134.

Table 20
Secure Router 2330 hardware and software capabilities

Feature	Maximum number supported
Ethernet Ports: Gigabit Fast Ethernet T1/E1 ports	 4 4 6
Serial ports	6
ISDN BRI (U/ST) ports	6
FXS/DID ports	12
SSH sessions	5
FTP sessions	4
TFTP sessions	4
Telnet sessions	15
DHCP: leases relay agents	 4000 255

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	100 (with optional crypto card)

Table 21
Secure Router 4134 hardware and software capabilities

Feature	Maximum number supported
Ethernet Ports:	
Gigabit	58
Fast Ethernet	72
PoE	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
relay agents	255

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 2330/4134 Release 10.2 supports the Small form-factor Pluggable (SFP) transceivers described in the following table.

Table 22
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 2330/4134 Installation — SFPs* (NN47263-303).

DSP channel licensing

Software licensing limits the number of DSP channels available on the Secure Router 2330/4134. If you boot the Secure Router 4134 with the PVM module only, or boot the Secure Router 2330 with the PVIM module only, the maximum number of DSP channels available is limited to 8.
To operate the Secure Router 2330/4134 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 16, 32, 64, or (on the SR4134 only) 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 23
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 2330/4134 before you contact Nortel Support), see *Nortel Secure Router 2330/4134 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 and Secure Router 2330 each support two Compact Flash card storage devices. In addition, the Secure Router 4134 supports 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: 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 or Secure Router 2330 cover 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 2330/4134 before you use the card.

The Secure Router 2330/4134 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)

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 10.2, see *Nortel Secure Router 2330/4134 Configuration — Network Management* (NN47263-602).

Reimaging the Mediation Server Module (SR4134 only)

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.

Upgrades and downgrades

This section describes the procedures for upgrading and downgrading the Secure Router software.

Secure Router 2330/4134 software file names and sizes

The Nortel Secure Router Release 10.2 software is supported only on the Secure Router 2330 and Secure Router 4134. The Release 10.2 software is available from the Nortel Technical Support Web site (www.nortel.com/support).

Table 24
Secure Router 2330/4134 software images

Description	File size (bytes)	Version	File name
Secure Router 4134 application image	25 502 761	10.2.0	SR4134.Z
Secure Router 4134 MIBs file	574 960	10.2.0	SR4134_MIBs_v1.0.zip
Secure Router 2330 application image	26 486 575	10.2.0	SR2330.Z
Secure Router 2330 MIBs file	574 958	10.2.0	SR2330_MIBs_v1.0.zip

Upgrading software and hardware on the Secure Router 2330/4134

The following two upgrade tasks cause an interruption in service for the Secure Router 2330/4134:

- An upgrade of the software on the Secure Router 2330/4134 requires that you reboot the router.
- An upgrade of the hardware on the Secure Router 2330/4134 may require that you power down the Secure Router 2330/4134. For example, Nortel strongly recommends that you power down the Secure Router 2330/4134 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 10.0.x or later software.

ATTENTION

The Telnet and FTP servers are disabled by default in Release 10.2 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 2330/4134 Release 10.2 and later, the software image file and boot image file are contained within one file. The image file name is SR4134.Z for the SR4134 and SR2330.Z for the SR2330. You can load an image file to a Nortel Secure Router 2330/4134 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 2330/4134 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 2330/4134 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 or SR2330.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 2330/4134. 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 2330/4134.

> **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 2330/4134 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 2330/4134 automatically updates the normal and golden bootrom images when you upgrade software. To ensure that the Secure Router 2330/4134 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 (SR4134 only), 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 or SR2330.Z) from the FTP server to the internal Compact Flash card (cf0), or copy the file from an external USB Flash drive (SR4134 only) 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 2330/4134.

> **ATTENTION**
> You require the internal Packetized Voice Module (PVM) on the SR4134 or the internal Packetized Voice Internal Module (PVIM) on the SR2330 for voice functionality.

> **ATTENTION**
> Nortel recommends that you power down the Secure Router 2330/4134 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 2330/4134. 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 55).

--End--

Example of upgrading software on the Secure Router 2330/4134 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.

This example uses the SR4134.Z file name for the SR4134 upgrade. To upgrade the SR2330, replace SR4134.Z with SR2330.Z.

Use the following procedure to copy the software image file from an FTP server to the Secure Router 2330/4134 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:

```
SR# file
```

4 To download the software image file, enter:

```
SR/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 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 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 image file (the default filename is SR4134.Z on the SR4134 and SR2330.Z on the SR2330).

```
Destination file '/cf0/SR4134.Z' exists, overwrite
?  (y/n) : y
```

8 The Secure Router 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 , enter:

```
SR/file# exit
SR# reboot
```

If you have the Mediation Server Module installed and operating on the SR4134, 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 2330/4134 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/.

This example uses the SR4134.Z file name for the SR4134 upgrade. To upgrade the SR2330, replace SR4134.Z with SR2330.Z.

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:

```
SR# file
```

4 To copy the software image file to the internal Compact Flash, enter:

```
SR/file# copy /usb0/SR4134.Z /cf0/SR4134.Z
```

5 The Secure Router 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 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 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-13-2009     18:47:02      SR4134.Z
```

8 To exit the file menu, enter:

```
SR/file# exit
```

9 To reboot the Secure Router, enter:

```
SR# reboot
```

If you have the Mediation Server Module installed and operating on the SR4134, 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 10.2 to 10.1.x:

- You have Release 10.2 software installed on your Secure Router 4134 and you must return to Release 10.1.x software for technical reasons.
- You want to move an interface module from a Secure Router 4134 that is running Release 10.2 software to a Secure Router that is running 10.1.x software.

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

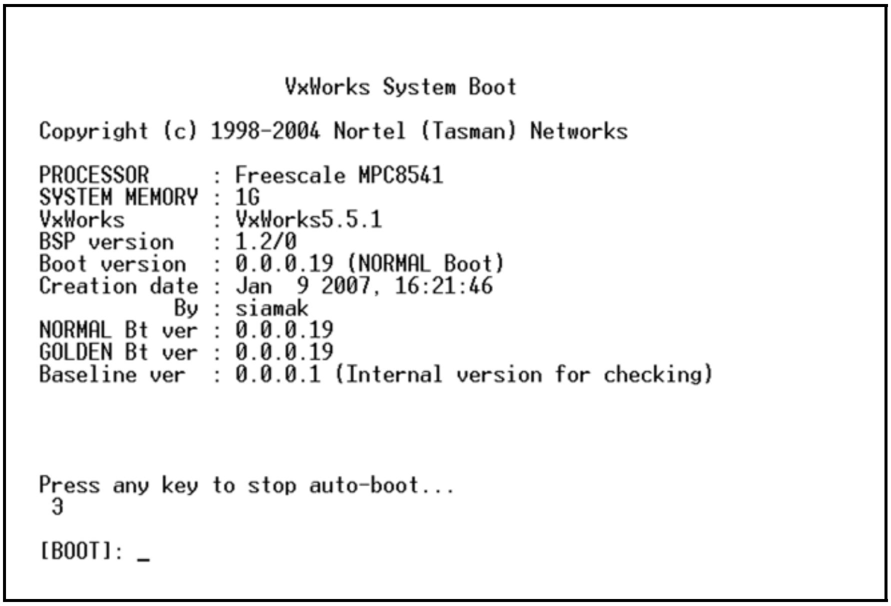
CAUTION
You must complete all steps of the downgrade process. If you stop the downgrade procedure before completion, the Secure Router 4134 can become unstable. Follow the upgrade procedures to return to Release 10.2 software.

Downgrading Secure Router 4134 software for technical reasons

Use the procedure in this section if you must downgrade your Secure Router 4134 from Release 10.2 to Release 10.1.x 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_2.Z
2	Download or copy the Release 10.1.x software file to an FTP server, a Compact Flash card, or a USB Flash drive. See "Upgrade procedure" (page 47).
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 10.2 software file on /cf0. Change the boot parameters to boot with the Release 10.1.x 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 10.1.x 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 55).

11 For the Secure Router 2330, ensure that the normal and golden bootrom partitions have a bootrom version of 0.0.0.32 or lower for Release 10.2.x software. For the Secure Router 4134, ensure that the normal and golden bootrom partitions have a bootrom version of 0.0.0.45 or lower for Release 10.2.x 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 10.2 chassis to a Release 10.1.x chassis

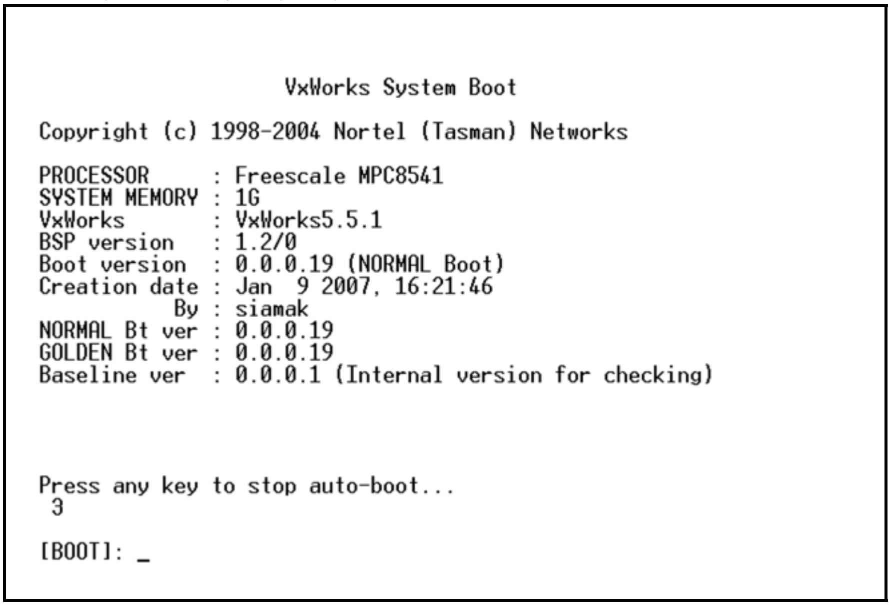
Use this procedure to move an external interface module from a Secure Router 4134 that is running Release 10.2 software to a Secure Router 4134 that is running Release 10.1.x software.

You can move an interface module from a Secure Router 4134 that is running Release 10.1.x software to a Secure Router 4134 that is running Release 10.2 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 10.2 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 10.1.x router.

6 Power up the Secure Router 4134 that is running Release 10.2 software.

Any interface modules installed in the Secure Router 4134 (Release 10.2 software) update to the Release 10.2 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 upgrade your Secure Router 4134 to Release 10.2.x software from 10.1.x, 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.x, 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 51) before you follow the steps in this section.

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

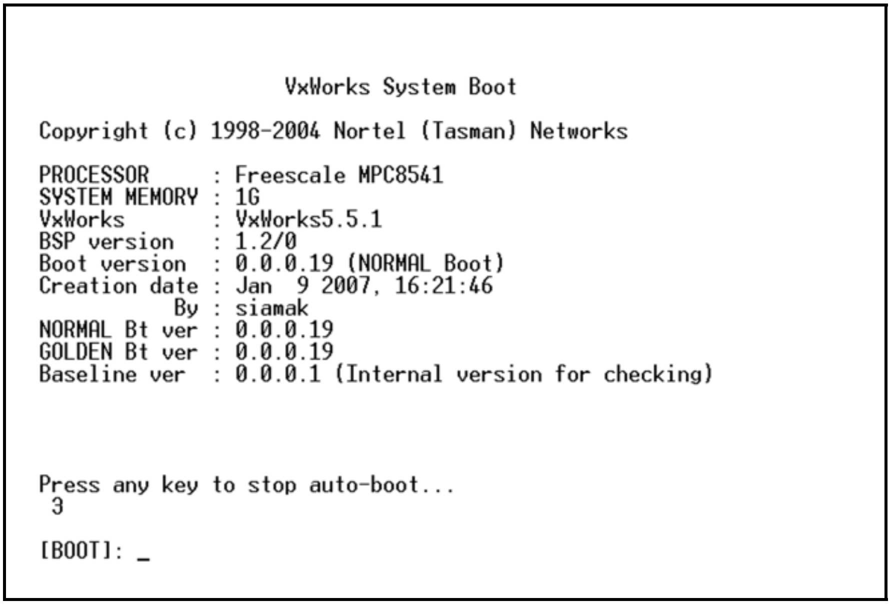
Use the **`show version`** command in the CLI to find information for the image version running on the normal and golden bootrom partitions of your Secure Router 4134.

> **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 (`SR/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).

Resolved issues

This section lists the resolved issues in Release 10.2 software.

Resolved issues

The following table describes issues that existed in prior releases that are resolved in Release 10.2.

Table 25
Resolved issues in Release 10.2

Change Request	Subsystem	Description
Q01838681	SNMP	Request for a command to enable all traps at once (`enable-all` option under `configure/snmp-server/enable/traps`).
Q01838608	CLI	Request for the description field on interfaces to be larger than 15 characters - up to 76 characters.
Q01838699	IP	Request for a show command to verify SNTP status (`show sntp`).
Q01839434	CLI	Request to see all available interfaces including SFPs, those configured and those not configured, to be added to the `show ip interface brief` command.
Q01789748-01	IP	Request to allow ping of the VRRP address of the Secure Router.
Q01837882	CLI	Request for ability to clear event logs (`clear event_log`).
Q01837886	CLI	Request to add a prompt that questions the admin user when they delete the system.cfg file.
Q01836509	Platform	Request to implement daylight saving time. (`configure# dst {set | enable}`).
Q01838687	CLI	Request for CLI to display highest capability for an interface, for example FE for Fast Ethernet and GE for Gig Ethernet interface.
Q01838694	CLI	Request for the `show system config` command to show the slot allocation in consecutive order.

Change Request	Subsystem	Description
Q01835481	Platform	Request for the ability to disable the USB port on the SR4134 (**`no usb enable`**).
Q01838670	SNMP	Request for a trap to be generated when an SFP is plugged into an SFP interface.
Q01838227	CLI	Request to enter banners in clear text without the need for delimiters like quotes ("").

Known issues

This section lists the known issues in Release 10.2 software.

Known issues

The following table describes issues and limitations known to exist in the Secure Router 2330/4134 Software Release 10.2, and provides guidelines for using Release 10.2 software.

Table 26
Known issues and limitations

Change Request	Subsystem	Description

Q01831324	CLI help	Better CLI context help requested similar to the SR1000 and SR3120.
		The SR2330/4134 CLI context sensitive help differs from the SR1000/SR3120 products.
		With the SR2330/4134, 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 SR2330/4134 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.

Change Request	**Subsystem**	**Description**
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.
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.
Q01783680	Ethernet CFM	No check on interface VLAN change even if associated with MA. The Secure Router 2330/4134 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 2330/4134 does not run a validation check or issue errors for the MA. Therefore, when a VLAN interface is changed on the Secure Router 2330/4134 (for example, VLAN X is changed to VLAN Y), ensure you update the VLAN associations for MAs as well (`SR/configure/oam/cfm/md MD1/ma MA1#` **`vlan <vid>`**).
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.

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 2330/4134 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.

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 SR2330/4134 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 SR2330/4134 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:

Change Request	Subsystem	Description

		`DUT1# show spanning-tree mstp instance ?`
		OR
		`DUT1# show spanning-tree mstp instance vlan ?`

10.2 issues:		
Q02045896	TFTP	When using a TFTP GUI (such as Pumpkin TFTP), a filename containing spaces is allowed to be transferred to /cf0 or /cf1. You are then unable to delete the filename from /cf0 or /cf1 because it contains spaces.
Q02003259 Q02003259-01	Ethernet CFM	With the connectivity fault management feature, the statistics of a maintenance end point are not available in this release. Hence, the command **`show cfm mep-stats mep <mep-id>`** does not yield any result. However, to see the count of continuity check messages transmitted from a maintenance end point and received from remote maintenance end points, you can issue the statistics command at the maintenance domain or maintenance association level. For example **`show cfm mep-stats md <md name>`** or **`show cfm mep-stats ma <ma name>`**. These commands show continuity check message statistics of all the end points under the specified domain or association.
Q02009278-01	Ethernet CFM	With Ethernet CFM, Nortel does not recommend transmitting Linktrace messages from both end stations simultaneously in this release.
Q02017146-01	Ethernet CFM	The following MIB Objects are not supported in the current release: • dot1agCfmMaMepListRowStatus • dot1agCfmVlanPrimaryVid • dot1agCfmVlanRowStatus • dot1agCfmConfigErrorListErrorType • dot1agCfmMepHighestPrDefect • dot1agCfmMepLowPrDef • dot1agCfmMaRowStatus • dot1agCfmMaIdPermission • dot1agCfmMepDbManAddressDomain • dot1agCfmMepDbManAddress

Change Request	Subsystem	Description
		• dot1agCfmMdRowStatus • dot1agCfmMdMaTableNextIndex
Q02041746 Q02041746-01	Ethernet CFM	Commands `show cfm ma <ma-id>` and `show cfm mep <mep-id>` show details for only one instance of the MA or MEP if the there are multiple MAs or MEPs configured with the same ID under different MDs. In order to get details for other instances, specify the specific MD for which the details need to be displayed using the following syntax: `show cfm ma <ma-id> md <md-id>`. For example: `show cfm ma ma1 md md1`.
Q01990569	MPLS	The implementation of LDP on the Secure Router expects the configured targeted prefix to match one of the following: 1. Address mentioned in IPv4 transport address TLV 2. Source address of the Targeted hello packet However, the Secure Router encodes the address configured as the transport address (at CLI level) as both 1 and 2. In order to resolve the problem related to interface targeted-peer, the interface address must also be set as the transport address for that node. For example, consider a targeted peer configured between Device 1 and Device 2 with interface addresses 12.1.1.1 and 13.1.1.1 respectively. On Device 1, set 12.1.1.1 as the transport address and configure 13.1.1.1 as the targeted peer. On Device 2, set 13.1.1.1 as the transport address and configure 12.1.1.1 as the targeted peer. The targeted adjacency then forms correctly.
Q02012468 Q02012468-01	RIPv1	The Secure Router sends out RIPv1 updates in their classful address format. Each route in the RIP database is converted to its classful address before being sent out in the update packet. If there is more than one route that falls in the same major network, then each of them is converted to its classful address. Hence update packets have more than one route to the same destination. These routes may have different metrics. When the receiving router processes these updates, it installs the first such route to its database. When the succeeding entries to the same destination are processed, the router changes the metrics each time and sends out a triggered update event. Due to this behavior, continuous triggered updates are sent from the Secure Router. The issue is seen only when classless addressing is used for the interfaces. Since RIPv1 is a classful routing protocol

Change Request	Subsystem	Description
		it is advised to use classful addresses for the interfaces. The Secure Router implementation of RIPv1 follows this assumption.
Q02015042-01	BGP	BGP does not redistribute static routes that have a global IPv6 address as the peer's next hop address. However, BGP does redistribute the static route if it has a link local IPv6 address as the peer's next hop address, as BGP has no information about the peer's link local next hop. Example: SR -----bgp------R2(any router) 1001::1/64 1001::2/64 fe80::0250:52ff:fef5:5d1d **`SR> ipv6 route 3002::/64 1001::2/64`** This route configured on SR will not get redistributed to R2, as SR is aware of the peer's global address 1001::2/64. **`SR> ipv6 route 3002::/64 fe80::0250:52ff:fef5:5d1d`** This route configured on SR will get distributed to R2, as SR is not aware of the peer's link local IPv6 address.
Q01986720 Q02000076	E1 HDLC	HDLC encapsulation over E1 does not interoperate with Juniper M10.
Q02019138 Q02019138-01	Source IP	The following are the limitations for the Source IP feature: 1. RADIUS: Configured Source IP address goes into the NAS IP address attribute of RADIUS . 2. FTP: The Source IP feature for FTP application takes only the global source IP (system source IP) and does not take the FTP-specific source IP. 3. TFTP: The source IP feature is not supported for the TFTP application in this release.
Q02016766-01	VOIP	While a fax call is active and in progress, the command **`show call active fax`** does not provide any output.
Q01983472	Port mirroring	When using the 10-port or 24-port Medium Module as the analyzer port in port mirroring, the VLAN tag of the mirrored traffic will be removed due to hardware design.
Q01986470-01	GVRP	With GVRP, dynamic VLANs are not learned when the destination interface is already a member of 1000 static VLANs.

Change Request	Subsystem	Description
Q02025923, Q02003336 Q02003336-01	RIPv1 with IPoA and IPoE	Secure Router 2330/4134 supports only RIPv2 with IPoA and IPoE in this release. RIPv1 with IPoA and IPoE is not supported.
Q02024929	ICMPv4 Router Discovery	Router part of the ICMPv4 Router Discovery Protocol is not a supported feature in the Secure Router.
Q02017298	Port mirroring	With port mirroring on the SR2330, the packets received at the analyzer port are tagged with the default PVID of the source interface. This limitation is due to Hardware Design
Q01986820, Q01986820-01	SNMP power supply	Issues exist with the following SNMP power supply variables: • The variables nnenvpowerdowntime and nnenvpowerfailcount are not supported for SR2330 and hence contain value 0. • The varbinds corresponding to failcount and downtime in traps are also null for SR2330.
Q01996415-01	BERT testing	With Layer 1 BERT tests on E1, if the interval time is configured as 1 min, the test runs for 1 min and 1 sec, and if configured for 2 min, the test runs for 2 min and 1 sec.
Q01992209 Q01992209-01	SNMP RMON	When executing the RMON statistics MIB (SNMP_GETBULK_RMON_GROUP1_MIB), the getbulk functionality may not work for the SR2330. Workaround: set the poll timeout value on properties->attributes->poll timeout to 3 seconds for the RMON statistics MIB when performing a getbulk using SNMPc.
Q01991907	RMON statistics	The Ethernet Stats counters are used for analyzing the number of RxBytes, Tx Bytes, Rx Packets, TxPackets, Oversize, and Jabber packets received. Due to hardware differences, the Jabber, Oversize and Receive Bytes counters have different behaviors on the SR4134 and the SR2330, as follows:

Counters	SR4134	SR2330

		Oversize	Increments for all packets that are greater than the system jumbo limit (between 1500 and 9216 bytes). When the system jumbo limit is set to 9216, then the Oversize and Jabber counters do not increment.	Increments for all packets which are greater than 1500 bytes in length. Also when the system jumbo limit is set to 1500, and packets of length greater than 1500 are sent, Oversize and Jabber counters do not increment. For all packets of less than 1500 bytes, RxPkts does not increment if the packet has a CRC error.
		Jabber	Increments for all packets that are oversize and sent with CRC error.	Increments for all packets that are greater than 1518 bytes with CRC error.
		Rx Bytes and Rx Packets	For packets with CRC errors (but not oversize), Rx Bytes and Rx Packet counters do not increment. Err packets increments. For all packets of length greater than the system jumbo limit, the packets are dropped. Rx Bytes and Rx Packets do not increment.	For the packets with CRC errors (but not oversize), Rx Bytes and Rx Packet counters increment. Err packets also increments For all packets of length greater than the system jumbo limit, the packets are dropped. Rx Bytes increments. Rx Packets does not increment. The Rx Bytes is

				always 1518000 irrespective of the packet size.
Q01811014-01	L2TP	L2TP server does not work with the local-untrusted interface as a loopback interface. In the field, there may be situations where-in multiple connections to the internet can be provided in the router for VPN failover or for clients coming in from different untrusted interfaces. Currently if the local-untrusted interface goes down, there is no way to establish L2TP through any other interface as only 1 L2TP server template can be configured. So we need an L2TP interface (software loopback) which is up irrespective of one physical interface going up or down. The support for Loopback interface failover exists for Remote-VPN using Mode-config and Site-to-Site VPN but not for L2TP.		
Q02057929	OSPF	If MD5 message-digest is enabled for OSPF, prior to upgrading store the password as plain text and save into running-config. Alternatively, prior to upgrade unconfigure the message-digest options, and reconfigure it after successful upgrades.		
Q01979248 Q01979248-01	Jumbo frames	The 24-port Fast Ethernet (FE) and Fast Ethernet/Power-Over-Ethernet (FE/PoE) Medium Modules do not support jumbo frame reception. The MTU on these module ports is 2000. Any packets larger than this size ingressing on these ports are dropped.		
Q02001746	QoS - Ethernet	When Layer 2 switching occurs between Ethernet ports on the SR2330 chassis, the packets are switched by the port network processor and do not reach the CPU for forwarding. SR2330 chassis QoS does not apply on packets switched to the egress direction by the port network processor.		
Q02007936	IPv6	Using the CLI, it is possible to: • configure an IPv6 address • configure IPv6 features (for example, MLD) • unconfigure the IPv6 address • save the running-config This in effect creates a configuration where the IPv6 feature exists on an interface with no IPv6 address configured, and in the case of Multicast, this is an error and error messages are generated when the running-config is replayed after restart. Workaround: if such an error is observed on configuration replay, this is a misconfiguration and the work around is to reconfigure the IPv6 address on the interface, and save the running-config.		

Q02015042	IPv6	When IPv6 static routes are redistributed over a BGP+ session using the IPv6 link-local address (of the neigboring interface) as the next hop, the neigboring connected router includes the route in its routing table, which is not expected. The route does not appear in the routing table of the neigboring router if the next hop is the global IPv6 address of the same neigboring interface. The problem is specific to link-local IPv6 addresses. The same problem is seen with multicast IPv6 static routes when redistributed over MBGP-v6. Before announcing the update to the peer, BGP compares the next hop with the peer’s IPv6 address. As a result, when a global address is used in the static route, the router drops the route finding that it is the same as the peer IPv6 address. However, the local next hop is also compared with the peer’s global IPv6 address, which is why the route never gets dropped and is propagated as a normal static route.
Q02016380	MLPPP	When an MLPPP bundle consisting of V.35 and RS-232 serial interfaces is configured between the SR4134 and a Cisco router, the MLPPP bundle comes up but the RS-232 serial link is down. The link comes up if the clock rate is configured as the default value of 9.6 KHz. But when the link is configured to maximum value of 115 KHz, the RS-232 link goes down. The same issue is seen if an X.21 or RS-449 interface is used with the RS-232 interface in the MLPPP bundle.
Q02017146	MIB	The following CFM MIB Objects are not supported in the current release: • dot1agCfmMaMepListRowStatus • dot1agCfmVlanPrimaryVid • dot1agCfmVlanRowStatus • dot1agCfmConfigErrorListErrorType • dot1agCfmMepHighestPrDefect • dot1agCfmMepLowPrDef • dot1agCfmMaRowStatus • dot1agCfmMaIdPermission • dot1agCfmMepDbManAddressDomain • dot1agCfmMepDbManAddress • dot1agCfmMdRowStatus • dot1agCfmMdMaTableNextIndex

Q02057665	Layer 2 features	If Layer 2 features are mistakenly enabled on an IP interface, for example, enabling Spanning-Tree features on an interface configured with an IP Address, the interface is reset and all IP properties are lost. In this case, you must reapply the IP properties.
Q02058723	RMON statistics	RMON statistics display only the Rx statistics and not the summation of Tx and Rx statistics.
Q02058893	Event log	The "event online" command, used to display the event log to the console, does not work if you use the "terminal length" command to modify the terminal display.
Q02060197	Spanning Tree/dot1x	Configuring Spanning Tree or dot1x on a range of ports is not supported. You can only configure these features on a single port at a time.
Q02058088 Q02058088-01	Ethernet	If you apply comments to an Ethernet interface configuration using the **`SYS_REM`** or **`SYS_REM_`** commands, and then delete the interface configuration (using the **`no interface Ethernet <slot/port>`** command), the **`SYS_REM`** and **`SYS_REM_`** comments are not deleted. If you reconfigure the same interface, the old comments appear for the new configuration. To delete the original comments, you must use the **`no SYS_REM`** and **`no SYS_REM_`** commands.
Q02069945	TFTP	TFTP file transfers are very slow when you use the default transfer file command. Workaround: Insert the text **`mode image`** at the end of the file transfer command.
Q02074470-01	SNMP	A new SNMP community string does not function when previously configured SNMP community strings are deleted. Workaround: Re-configure the deleted SNMP community strings.
Q02019239 Q02019239-01	CLI **`show`** commands	Some Secure Router 2330/4134 functions support the CLI optional command parameter value **`<WORD>`** that you can use to assign an alphanumeric name to a function. You must choose a unique name for the **`<WORD>`** value. Names that share partial or complete character strings with each other, or with other variables and functions, can produce unexpected **`show`** command results when used at the same level of the command tree. **Example:** You configure a QoS policy map named **`cl`**. You can use the optional variables for the CLI command **`show qos chassis policy-map [<WORD> <class-map> <detail>]`** to customize information display for specific chassis QOS policy map information, but you enter the command **`show qos chassis policy-map cl`** to display general details about the policy map named **`cl`**. Because one of the variables for the command is **`class-map`**

		and the Secure Router interprets the characters **`cl`** as **`class-map`**, the system does not display the policy map details, but instead, prompts you to enter a class map name.
Q02064248 Q02064248-01	SFP	If an SFP is not used with 44 port Ethernet modules and the terminal monitor is enabled on a telnet session, alert messages do not appear on the telnet session. An alert message appears on the console screen indicating that the SFP has been removed.
Q02076826	USB storage devices	The Secure Router 4134 does not support USB storage devices formatted as FAT 32.
Q02022175 Q02042482	CLI	The CLI commands **`show running-config`**, **`save local`**, or **`configure terminal`** cannot be issued from a telnet session after a console session is exited while displaying the running configuration in `configure terminal` mode.
Q02078090	SNMP	To delete an SNMP community with a privilege of (rw) from the Secure Router 4134, you must include the access privilege in the command. `SR4134/configure/snmp-server#` **`no community <community_name> rw`**.

Known limitations and general feature guidelines

This section provides information about known limitations, and general guidelines and considerations for Secure Router 2330/4134 features.

Known limitations

The following table provides information about design limitations known to exist in the Secure Router 2330/4134 Software Release 10.2.

Table 27
Design limitations for the Secure Router 2330/4134

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 2330/4134 (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 2330/4134 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.

Subsystem	Description
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.

General guidelines and considerations

The following table provides information to assist you with the configuration of Secure Router 2330/4134 features.

Table 28
General guidelines and considerations

Subsystem	Description
VoIP	For information about limitations related to VoIP configuration and the Secure Router 2330/4134, see *Nortel Secure Router 2330/4134 Configuration — SIP Media Gateway* (NN47263-508).
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 2330/4134 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".

Subsystem	Description
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. 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 2330/4134. 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.

Subsystem	Description
Interoperability with: MSTP LACP (dynamic link aggregation) VLAN forwarding of tagged and untagged Ethernet traffic	To interoperate with the Secure Router 2330/4134 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 2330/4134 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.

How to get help

How to get help

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

You can download the Secure Router 2330/4134 10.2 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 2330/4134

Release Notes

Release: 10.2
Publication: NN47263-400
Document revision: 04.02
Document release date: 7 October 2009

While the information in this document is believed to be accurate and reliable, except as otherwise expressly agreed to in writing NORTEL PROVIDES THIS DOCUMENT "AS IS" WITHOUT WARRANTY OR CONDITION OF ANY KIND, EITHER EXPRESS OR IMPLIED. The information and/or products described in this document are subject to change without notice.

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

www.nortel.com