Secure Router 3120 and Secure Router 1000 Series

Release 9.3 Release Notes

NN47260-400

Document status: Standard
Document version: 03.01
Document date: 28 March 2008

Trademarks

Restricted rights legend

Statement of conditions

Nortel Networks software license agreement

you a license to use the Software only in the country where you acquired the Software. You obtain no rights other than those granted to you under this License Agreement. You are responsible for the selection of the Software and for the installation of, use of, and results obtained from the Software.

1. Licensed Use of Software. Nortel grants Customer a non-exclusive license to use a copy of the Software on only one machine at any one time or to the extent of the activation or authorized usage level, whichever is applicable. To the extent Software is furnished for use with designated hardware or Customer furnished equipment ("CFE"), Customer is granted a non-exclusive license to use Software only on such hardware or CFE, as applicable. Software contains trade secrets and Customer agrees to treat Software as confidential information using the same care and discretion Customer uses with its own similar information that it does not wish to disclose, publish or disseminate. Customer will ensure that anyone who uses the Software does so only in compliance with the terms of this Agreement. Customer shall not a) use, copy, modify, transfer or distribute the Software except as expressly authorized; b) reverse assemble, reverse compile, reverse engineer or otherwise translate the Software; c) create derivative works or modifications unless expressly authorized; or d) sublicense, rent or lease the Software. Licensors of intellectual property to Nortel are beneficiaries of this provision. Upon termination or breach of the license by Customer or in the event designated hardware or CFE is no longer in use, Customer will promptly return the Software to Nortel or certify its destruction. Nortel Networks may audit by remote polling or other reasonable means to determine Customer's Software activation or usage levels. If suppliers of third party software included in Software require Nortel Networks to include additional or different terms, Customer agrees to abide by such terms provided by Nortel with respect to such third party software.

2. Warranty. Except as may be otherwise expressly agreed to in writing between Nortel Networks and Customer, Software is provided "AS IS" without any warranties (conditions) of any kind. NORTEL DISCLAIMS ALL WARRANTIES (CONDITIONS) FOR THE SOFTWARE, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OF NON-INFRINGEMENT. Nortel Networks is not obligated to provide support of any kind for the Software. Some jurisdictions do not allow exclusion of implied warranties, and, in such event, the above exclusions may not apply.

3. Limitation of Remedies. IN NO EVENT SHALL NORTEL NETWORKS OR ITS AGENTS OR SUPPLIERS BE LIABLE FOR ANY OF THE FOLLOWING: a) DAMAGES BASED ON ANY THIRD PARTY CLAIM; b) LOSS OF, OR DAMAGE TO, CUSTOMER'S RECORDS, FILES OR DATA; OR c) DIRECT, INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE, OR CONSEQUENTIAL DAMAGES (INCLUDING LOST PROFITS OR SAVINGS), WHETHER IN CONTRACT, TORT OR OTHERWISE (INCLUDING NEGLIGENCE) ARISING OUT OF YOUR USE OF THE SOFTWARE, EVEN IF NORTEL NETWORKS, ITS AGENTS OR SUPPLIERS HAVE BEEN ADVISED OF THEIR POSSIBILITY. The foregoing limitations of remedies also apply to any developer and/or supplier of the Software. Such developer and/or supplier is an intended beneficiary of this Section. Some jurisdictions do not allow these limitations or exclusions and, in such event, they may not apply.

4. General

a. If Customer is the United States Government, the following paragraph shall apply: All Nortel Networks Software available under this License Agreement is commercial computer software and commercial computer software documentation and, in the event Software is licensed for or on behalf of the United States Government, the respective rights to the software and software documentation are governed by Nortel Networks standard commercial license in accordance with U.S. Federal Regulations at 48 C.F.R. Sections 12.212 (for non-DoD entities) and 48 C.F.R. 227.7202 (for DoD entities).

b. Customer may terminate the license at any time. Nortel Networks may terminate the license if Customer fails to comply with the terms and conditions of this license. In either event, upon termination, Customer must either return the Software to Nortel Networks or certify its destruction.

c. Customer is responsible for payment of any taxes, including personal property taxes, resulting from Customer's use of the Software. Customer agrees to comply with all applicable laws including all applicable export and import laws and regulations.

d. Neither party may bring an action, regardless of form, more than two years after the cause of the action arose.

e. The terms and conditions of this License Agreement form the complete and exclusive agreement between Customer and Nortel Networks.

f. This License Agreement is governed by the laws of the country in which Customer acquires the Software. If the Software is acquired in the United States, then this License Agreement is governed by the laws of the state of New York.

Contents

Secure Router 3120 and Secure Router 1000 Series Release Notes

Navigation

Preface

Navigation

How to get help

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

The 9.3 software release will be downloadable from the Customer Service Portal site; www.nortel.com/support, Select "Product Categories" and then "Routers and Routing Switches". Scroll down to the Secure Router family.

Getting help from the Nortel web site

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

www.nortel.com/support

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

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

Getting help over the phone from a Nortel Solutions Center

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

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

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

www.nortel.com/callus

Getting help from a specialist using an Express Routing Code

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

www.nortel.com/erc

Getting help through a Nortel distributor or reseller

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

Introduction

The Nortel Secure Router 9.3 release is for general use and is supported on the Secure Router 3120 and Secure Router 1000 Series platforms only.

New Features for Release 9.3

The 9.3 software release contains all of the features included in previous software releases.

The Nortel Secure Router 1001, 1001s, 1002 and 1004 and the Secure Router 3120 software release 9.3 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. These releases deliver feature parity across all SR1000 Series and SR3120 platforms and make feature support and deployment more consistent across the product range.

Navigation

Default settings

The default settings for some features change in this release. The default settings are as follows:

- WebUI is disabled
- SNMP is disabled
- Telnet server is disabled

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

Use the CLI to change the default settings.

Smartjack Remote Loopback

The Secure Router 1000 Series and 3120 9.3 release will provide support for remote loopback testing on a smartjack device. This will enable a Router using T1 inband control to send smartjack loopup or loopdown code to a remote smartjack device.

This feature is a component of the "**`test`**" CLI tree of commands and is configurable on T1 and CT3 interfaces. Requests are sent to connected smartjack T1 devices only.

Configuring Smartjack Remote Loopback

Use the following procedure to configure a Smartjack remote loopback test.

Procedure steps

Step	Action
1	To configure a Smartjack remote loopback test, enter Test Mode. **`test`**
2	Specify the interface to run the test on. **`<interface> <slot/port>`**
3	Specify a loopback remote test. **`loopback remote`**
4	Specify a smartjack interface. For T1 interface: **`smartjack`** For T1 interface in CT3: **`smartjack_t1 <t1>`**

—End—

Table 1
Variable definition

Variable	Value
<interface>	The interface to run the test on. T1 or CT3.
<slot/port>	The slot/port to run the test on.
<t1>	The T1 number to be tested.

DHCP Client on Ethernet Interfaces

The Secure Router 1000 Series and 3120 9.3 release will provide support for Dynamic Host Configuration Protocol (DHCP) for IPv4 clients on Ethernet interfaces. A DHCP client obtains configuration parameters such as an IP address.

Using DHCP, a client can contact a central DHCP server that is responsible for maintaining 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 since a client may 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 default router IP source to be the server.

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

6 Specify the retry interval.

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

7 Enable the DHCP client on the interface.

```
dhcp-client enable
```

—End—

Table 2
Variable definition

Variable	Value
<duration>	The duration of the lease in the range 30 to 4294967.
<hostname>	The hostname of the DHCP client.
<interface>	The interface to work with.
<interval>	The timeout interval, in seconds, for the DHCPv4 client negotiation process.

Dial Backup via External Modem

The Secure Router 1000 Series and 3120 9.3 release will provide support for Dial Backup, which enables redundancy for routes. Backup routes using PPP bundles created over a dialup connection will become active when a primary route goes down.

The Secure Router connects to an external modem via the Aux port and will establish 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 will 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 will be supported via the CLI:

Table 3
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 4
Programmed modem default settings

S2	escape character
S3	carriage return character
S4	line feed character
S37	line connection speed
V1	result code will be sent in work form
X1	send OK, CONNECT, RING, NO CARRIER, ERROR, NO ANSWER and CONNECT SPEED

Table 5
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 via external modem

Use the following procedure to configure dial backup via external modem.

Procedure steps

Step	Action
1	To configure dial backup, enter Configuration Mode. `configure terminal`
2	Create a dialer. `dialer <name>`
3	Configure async parameters. `async`
4	Configure the async port. `port <port>`
5	Configure the baud rate. `rate <baudrate>`
6	Configure data bits. `databits <databits>`
7	Configure the parity setting. `parity <setting>`
8	Configure stop bits. `stopbits <stopbits>`
9	Exit back a level. `exit`

10 Begin configuring the modem.

```
modem
```

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

```
phonenum <number>
```

12 Configure the number of rings before answering.

```
answer <rings>
```

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

```
call-setup-timeout <rings>
```

14 Configure the "lost carrier" hang up delay.

```
hangup <delay>
```

15 Configure the carrier detect response time.

```
detect <responsetime>
```

16 Configure the "wait for carrier" after dial delay.

```
wait <wait>
```

17 Configure using an AT string.

```
at <at_string>
```

18 Exit back a level.

```
exit
```

19 Configure the dialer idle-timeout interval.

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

20 Exit back a level.

```
exit
```

21 To attach to a bundle, create a bundle.

```
interface bundle <bundlename>
```

22 Configure the bundle to use the dialer.

```
link dialer <dialer>
```

23 Continue normal configuration of the bundle.

—End—

Table 6
Variable definition

Variable	Value
<at_string>	The AT string used to configure the dialer.
<baudrate>	The Baud rate of the modem, default 56000.
<bundlename>	The name of the bundle.
<databits>	The number of databits, default 8.
<delay>	The lost carrier hang up delay, in the range 1 to 255. Default is 14.
<dialer>	The dialer name to link, maximum 8 characters.
<name>	The dialer name, maximum 8 characters.
<number>	The phone number, maximum length 25 characters, with or without hyphens. Prepending p or t indicates pulse or tone dialing.
<port>	The port description, maximum 10 characters.
<responsetime>	The carrier detect response time, in the range 1 to 255. Default is 6.
<rings>	The number of rings, in the range 1 to 255.
<setting>	The parity setting - none, even, or odd. Default is none.
<stopbits>	The number of stopbits - 1, 2, or 3. Default is 1.
<timeout>	The idle timeout time, in the range 1 to 6000. Default is 180.
<wait>	The length of time to wait for dial delay, in the range 1 to 255. Default is 50.

VRRP enhancements

The Secure Router 1000 Series and 3120 9.3 release will provide support for multiple VRRP enhancements. 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 enabled sub-interfaces, with a maximum of 10 VRRP groups per router.

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 could act as master at any given 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 via CLI.

New to Release 9.3 are VRRP authentication types "no authentication" and "clear text password authentication" for VLAN enabled sub-interfaces. Using the "no authentication" type, VRRP exchanges are not authenticated, while with "clear text password authentication", the receiver checks to make sure VRRP authentication packet data matches the configured authentication string. If there is no match, the exchange is discarded.

In addition to this, VRRP interface monitoring on VLAN enabled sub-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 as new priority and ultimately affecting its chances in an election.

Finally, several VRRP load-balancing mode types are present so users can choose which mode best suits their needs. Full load-balancing is supported, and users can further choose from one of the following options:

- **Mode 0: Gratuitous ARP Mode** - Relies on gratuitous ARP to redirect traffic in the event of a failover. This mode uses the MAC address of a physical ethernet port as a virtual MAC.
- **Mode 1: Active/Standby Mode** - Applicable to primary ethernet interfaces only, this mode allows a VRRP interface to participate in a single VRRP group at any given time using a virtual MAC address. If Active/Standby Mode is used, only 1 VRRP group can be configured.
- **Mode 2: Promiscuous Mode** - All packets that reach the interface are accepted, including packets not intended for it. Potentially generates performance overhead as packets are processed.

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 Interface Mode. `interface <interface>`

3 In the case of a 802.1q (VLAN) interface/sub-interface, apply encapsulation.

```
encapsulation <type>
```

4 In the case of a sub-interface, specify an IP address.

```
ip address <A.B.C.D>
```

5 Specify VRRP mode.

```
vrrp_mode <mode>
```

6 Specify a VRRP group.

```
vrrp <group>
```

7 Specify a virtual IP address.

```
ipaddr <virtual IP>
```

8 Configure tracking.

```
track <interface> <priority>
```

9 Configure a priority level.

```
priority <level>
```

10 Enable VRRP.

```
enable
```

—End—

Table 7
Variable definition

Variable	Value
<A.B.C.D>	The IP address of the sub-interface.
<group>	The VRRP group number, in the range 1 to 255.
<interface>	The interface to work with.
<level>	The priority level, in the range 1 to 254.
<mode>	The VRRP mode. Possible choices are: • **0** - Gratuitous ARP • **1** - Active/Standby Mode • **2** - Promiscuous Mode
<priority>	The track priority.

Variable	Value
<type>	The type of encapsulation to apply.
<virtual IP>	The virtual IP address to be used.

Multiple Syslog Server support

The Secure Router 1000 Series and 3120 9.3 release will provide support for multiple Syslog servers. A Syslog Server monitors incoming Syslog messages on UDP ports and decodes them for logging purposes. In addition, several network devices are now able to be configured to generate Syslog messages. In the past, the Secure Router 1000 Series and 3120 only provided support for logging on a single Syslog Server, but this enhancement allows for the configuration of up to 5 Syslog Servers. Since they are logged simultaneously, all Syslog servers will 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 will remain 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 will remain unchanged.

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

Note that 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`** sub-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 will be 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 8
Variable definition

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

Multiple IP Helper Addresses on VLAN

The Secure Router 1000 Series and 3120 9.3 release will provide 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 may 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 will fail. When this occurs, 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 6 helper addresses able to be configured per 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 <interface>
```

3 Specify an IP address.

```
ip address <A.B.C.D/M>
```

4 Specify a Helper address.

```
ip helper-address <A.B.C.D>
```

5 To configure a sub-interface, exit back a level.

```
exit
```

6 Specify the sub-interface.

```
interface <sub-interface>
```

7 Add encapsulation.

```
encapsulation <type>
```

8 Specify an IP address.

```
ip address <A.B.C.D/M>
```

9 Specify a Helper address.

```
ip helper-address <A.B.C.D>
```

10 If desired, specify a Helper address for a service.

```
ip helper-address <A.B.C.D> service <service>
```

11 If desired, specify a Helper address for a protocol or port.

```
ip helper-address <A.B.C.D> protocol <protocol> port
<port>
```

—End—

Table 9
Variable definition

Variable	Value
<A.B.C.D>	The IP address.
<A.B.C.D/M>	The IP address, followed by subnet mask.
<interface>	The interface to work with.
<port>	The port number in the range 1 to 65535..

Variable	Value
<protocol>	The protocol to be used. Options available are: • **UDP** - to a specific UDP port.
<service>	Service name to specify IP helper for a service. Options available are: • **dns** -- Domain Name Service • **netbios-dgm** -- NetBIOS datagram service • **netbios-ns** -- NetBIOS name service • **netbios-ss** -- NetBIOS session service • **tftp** -- Trivial File Transfer Protocol • **time** -- Time
<sub-interface>	The sub-interface IP address.
<type>	The type of encapsulation to apply.

IP Packet Filtering on VLAN sub-interfaces

The Secure Router 1000 Series and 3120 9.3 release will provide support for IP packet filtering over VLAN sub-interfaces. IP packet filtering involves the use of Access Control Lists (ACL) to filter network traffic by permitting or blocking packets at a router's interface.

Previously, the Secure Router 1000 Series and 3120 allowed configuration of sub-interfaces, but did not contain support for attaching ACLs to the VLAN sub-interfaces. Packet filters could only be attached to main interfaces. Adding this support allows for the attachment of ACLs to these VLAN sub-interfaces, which enabled the use of packet filtering over such interfaces. No existing functionality has been affected.

To accommodate these enhancements, existing CLI commands have been modified for additional support of VLAN sub-interfaces. The existing "access-group" command which was used to attach an access-list to an interface has now been modified to support a range of VLAN sub-interfaces. This provides the user ease of attaching a single access-list to multiple VLAN sub-interfaces, instead of issuing the command uniquely for each VLAN sub-interface.

The maximum number of rule sets supported per system is 50, while the maximum number of filter rules per set is 2000. Users can configure up to 98 VLAN sub-interfaces per Ethernet interface.

Some limitations of this feature include the lack of support for VLAN ID-based filtering, and the behavior to ignore any non-configured VLAN sub-interface that falls within the range of the access-group.

Configuring IP packet filtering on VLAN sub-interfaces

Use the following procedure to configure IP packet filtering on VLAN sub-interfaces.

Procedure steps

Step	Action
1	To configure IP packet filtering on VLAN sub-interfaces, enter Configuration Mode. `configure terminal`
2	Create an access list. `ip access-list <listname>`
3	Add a rule to the current filter list. `add <rule_action> <protocol> <source> <destination> [sport] [dport] [icmptype] [icmpcode] [precedence] [tos] [flags] [log] [expire]`
4	Exit back a level. `exit`
5	Attach to a sub-interface. `ip access-group <VLAN sub-interface> <listname> <direction>`

—End—

Table 10
Variable definition

Variable	Value
<destination>	IP destination address (a.b.c.d/a.b.c.d or a.b.c.d/0-32 or any).
<direction>	The direction of packets to filter, in or out.
<listname>	The ACL name.
<protocol>	The protocol, tcp/udp/icmp/ip or 0-255.
<rule_action>	**permit** rule or **deny** rule or **reject** rule (reject rule can be specified only with ICMP protocol).
<source>	IP source address (a.b.c.d/a.b.c.d or a.b.c.d/0-32 or any).
<VLAN sub-interface>	The sub-interface to apply the ACL.

Inserting a new rule to an already configured access list

Procedure steps

Step	Action
1	Enter Configuration Mode. `configuration terminal`
2	Select the access-list. `ip access-list <listname>`
3	Insert the rule at a specific line number in the access-list. `insert <rule_lineno> <rule_action> <protocol> <source> <destination> [sport] [dport] [icmptype] [icmpcode] [precedence] [tos] [flags] [log] [expire]`

—End—

Table 11
Variable definition

Variable	Value
<destination>	IP destination address (a.b.c.d/a.b.c.d or a.b.c.d/0-32 or any)
<listname>	The access-list name.
<protocol>	The protocol, tcp/udp/icmp/ip or 0-255
<rule_action>	**permit** rule or **deny** rule or **reject** rule (reject rule can be specified only with ICMP protocol).
<rule_lineno>	The line number, in the range 1 to 65535.

Deleting a rule from a rule list

Procedure steps

Step	Action
1	Enter Configuration Mode. `configuration terminal`
2	Select the access list. `ip access-list <listname>`
3	Delete the rule. `delete <rule_lineno>`

—End—

Table 12
Variable definition

Variable	Value
<listname>	The access-list name.
<rule_lineno>	The line number, in the range 1 to 65535.

Displaying access lists, rule sets and statistics

Procedure steps

Step	Action
1	Display all access lists. `show ip access-lists all`
2	Display access list rules. `show ip access-list-rules <all|[VLAN sub-interface]>`
3	Display access list statistics. `show ip access-list-stats <VLAN sub-interface>`

—End—

Table 13
Variable definition

Variable	Value
<VLAN sub-interface>	A single sub-interface name or a range of sub-interfaces (specified as ethernet0.1-5 which implies range of sub-interfaces starting from ethernet0.1 till ethernet0.5.)

OSPF NBMA over Ethernet

The Secure Router 1000 Series and 3120 9.3 release will provide support for OSPF non-broadcast multi-access (NBMA) over Ethernet. While it's 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 doesn't 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 in order to optimize adjacency building. All routers in a segment should 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 since no neighbors are discovered. In order 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 send 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 any 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 when the neighbor command is issued. When this occurs, 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 3 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`
4	Configure the OSPF area. `interface <interface> area <areaid>`
5	Specify the network type. `network <type>`
6	Configure neighbors, repeating this step for each neighbor you want to add..

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

7 Configure the poll interval.

```
poll_interval <interval>
```

—End—

Table 14
Variable definition

Variable	Value
<A.B.C.D>	The IP address.
<areaid>	The OSPF area ID.
<interface>	The interface to work with.
<interval>	The poll interval.
<type>	The network type.
<X.X.X.X>	The router ID IP address.

Firewall ALG behavior

This describes changes made to firewall ALG behavior.

Default behavior of firewall ALG

In the 9.3 release of the Secure Router 1000 Series and 3120 firewall ALGs are disabled by default. To use the typical ALG set, a new cli command (i.e., enable-typical) has been added. This command enables only a specific set of ALGs as follows:
aim, aimudp , ftp , l2tp, msn, pptp, rpc, rtsp554, rtsp7070, smtp, web, ike, tftp
Remaining ALGs (sip, sip-tcp, h323, gatekeeper, msnudp, dns, n2p, pcanywhere, sql, msgtcp, irc, n2pe, ils, cuseeme, mszone, ils2, nntp) are in the disabled state.

Configuring a typical ALG set Use the following procedure to configure a typical ALG set.

Procedure steps

Step	Action
1	Enter Configuration Mode. `configuration terminal`
2	Navigate to the **`firewall global`** sub-tree. `firewall global`

3 Disable all ALGs.

```
no enable-all
```

4 Enable the typical ALG set.

```
enable-typical
```

—End—

Changes to the DNS ALG

The Secure Router 1000 Series and 3120 9.3 release will provide support for DNS ALG. The DNS ALG is used when a DNS client on an untrusted side wants to access a DNS server behind a NAT in trusted side.

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

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

Configuring DNS ALG

Procedure steps

Step	Action
1	Enter Configuration Mode. `configuration terminal`
2	Enter the **`firewall global`** sub-tree. `firewall global`
3	Enter the **`algs`** sub-tree. `algs`

4 Enter the **dns** sub-tree.

```
dns
```

5 Enable the DNS ALG.

```
enable
```

6 Ensure the DNS pool has been configured.

```
pool <pool-name> <private-ip> <global-ip>
```

7 Display the pool name.

```
show firewall dns-alg translate-pool pool-name
```

8 Display all static pool names which were added.

```
show firewall dns-alg translate-pool
```

—End—

Table 15
Variable definition

Variable	Value
<global-ip>	The global IP address for the pool.
<pool-name>	The identifying name for the pool.
<private-ip>	The private IP address for the pool.

T1 BERT Testing support

The Secure Router 1000 Series and 3120 9.3 release will provide support for uninterrupted T1 BERT and Loopback testing. This addition provides ability to run BERT or Loopback tests on a T1, E1, CT3, or DS3 link while in a bundled interface without breaking the link or disrupting traffic. This functionality applies to single and multi-linked bundles and assists customers in troubleshooting remote units. As a rule, BERT test should be run on the local box after making sure that the remote box is in loopback.

BERT/Loopback Test Support allows tests to run on links in a bundled interface. Since BERT patterns are treated as errored packets by the HDLC controller, the HDLC channel on the link on the local box is disabled to prevent the receipt of HDLC errors. By design, a link is automatically taken out of a bundle when an HDLC channel receives a large number of errors. When you disable the receiver component of the HDLC controller, the link enters a DOWN state, but the bundle remains in a UP state in the case of a multilink bundle. The HDLC channel is enabled and the link returns to an UP state after the test is finished. In the case of a single link bundle,

when a test is run, the link goes to a DOWN state, which in turn leads the bundle to a DOWN state. The link and bundle both return to an UP state once the test is completed.

Note that when displaying bundle information using the **`show interface bundle <bundlename>`** command, the link status will show as "*loopback detected*" when a loopback test is issued, or as "*link in test mode*" when a BERT test is issued.

Configuring T1 BERT testing

Use the following procedure to configure T1 BERT testing.

Procedure steps

Step	Action
1	To configure T1 BERT testing, enter Test Mode. **`test`**
2	Specify an interface and slot/port. **`<interface> <slot/port>`**
3	Configure BERT testing. **`bert <t1> [pattern] [interval]`** ***Note:*** If a test is issued on a link that is part of a bundle, the user will be given the option to continue or abort.

—End—

Table 16
Variable definition

Variable	Value
<interface>	The interface to work with.
[interval]	The test interval, in the range 1 to 1092.
[pattern]	The test pattern to use. Available options are: • 2^11 • 2^15 • 2^20 • QRSS
<slot/port>	The slot/port combination to use.
<t1>	The T1 or range of T1s for testing.

Configuring loopback testing

Use the following procedure to configure loopback testing.

Procedure steps

Step	Action
1	To configure loopback testing, enter Test Mode. `test`
2	Specify an interface and slot/port. `<interface> <slot/port>`
3	Configure loopback testing. `loopback [line_ct3] [line_t1 <t1>] [payload_t1 <t1>] [remote <line_ct3> <line_t1> <payload_t1> <type>]` ***Note:*** If a test is issued on a link that is part of a bundle, the user will be given the option to continue or abort.

—End—

Table 17
Variable definition

Variable	Value
<interface>	The interface to test.
[interval]	The test interval, in the range 1 to 1092.
[line_ct3]	Configure a CT3 for loopback line testing.
[line_t1]	Configure a T1 for loopback line testing.
[payload_t1]	Configure a T1 for loopback payload testing.
[remote]	Configure interface for remote loopback testing.
<slot/port>	The slot/port combination to use.
<t1>	The T1 or range of T1s for testing.
<type>	The loopcode for testing. Available option is `ansi_fdl`.

Source IP Enhancements

The Secure Router 1000 Series and 3120 9.3 release will provide support for adding source address information to existing services. The services modified to accept a source address are:

- File Transfer

- QoS Historical Statistics
- 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 will display 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 will show as "not configured". Likewise, if the feature is configured by interface name, with no IP address specified, the IP address will show 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.

Since file transfer commands are not stored in a configuration it will use 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 may fail to work if it is bi-directional. By using a loopback interface for the source address which is always up it will insure that the above problem does not occur.

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 18
Variable definition

Variable	Value
[ip address]	Specify source address by IP address.
[interface name]	Specify 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 19
Variable definition

Variable	Value
[ip address]	Specify source address by IP address.
[interface name]	Specify 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 20
Variable definition

Variable	Value
[ip address]	Specify source address by IP address.
[interface name]	Specify 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

3 Configure the source address.

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

—End—

Table 21
Variable definition

Variable	Value
[ip address]	Specify source address by IP address.
[interface name]	Specify 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 22
Variable definition

Variable	Value
[ip address]	Specify source address by IP address.
[interface name]	Specify source address by interface name.

Configuring QoS Historical Statistics source address

Use the following procedure to configure QoS Historical Stats 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 **qos** subtree. `qos`
3	Enter the **historical-stats** subtree. `historical-stats`
4	Configure the source address. `source-address <[ip address]|[interface name]>`

—End—

Table 23
Variable definition

Variable	Value
[ip address]	Specify source address by IP address.
[interface name]	Specify source address by interface name.

Multiple SNTP Server support

The Secure Router 1000 Series and 3120 9.3 release will provide 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 any SNTP server is queried and fails to respond, the router will send 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 can not 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, note that DNS entries need to be configured before SNTP will function 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	Since 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 per 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 24
Variable definition

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

Accounting under TACACS support

The Secure Router 1000 Series and 3120 9.3 release will provide 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 and/or time. 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 via Telnet or SSH using the correct username and password, a log will be 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, then applying this list to one or more interfaces.

There are two main TACACS accounting commands:

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

There are three methods of TACACS accounting:

- **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 when 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 will use this list without applying in 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 25
Variable definition

Variable	Value
<commands|networks>	The type of accounting to apply to the interface.
<interface>	The interface to work with.
<list>	The list to apply to the interface.
<listname>	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

The Secure Router 1000 Series and 3120 9.3 release will provide support for NAT ACL enhancements. These enhancements add flexibility in configuring a network Access Control List. Access Control Lists are used to filter packets going to the global NAT subsystem. A separate ACL is allowed for static and dynamic address 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 may be applied selectively to any interface.

NAT ACL Packet Processing

This section contains information on 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. When 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; reverseACL 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 IP mode. `ip`
3	Enter the **nat** subtree. `nat`
4	Create an access list. `access-list <listname>`
5	If applicable, specify an address or range to permit. `add permit ip <range-start> <range-end>`
6	If applicable, specify an address or range to deny. `add deny ip <range-start> <range-end>`
7	Exit the *access-list* configuration to finish or create another.

```
exit
```

8 Create an address pool.

```
pool <poolname>
```

9 Specify the address pool range. Note that you can specify more than one range using the same command syntax.

```
range <range-start> <range-end> <mask>
```

10 Configure an access group to use the address pool.

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

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

```
access-group <groupname> static
```

—End—

Table 26
Variable definition

Variable	Value
<groupname>	The name given to an access group.
<listname>	The name given to the Access Control List.
<mask>	The subnet mask of a supplied address range.
<poolname>	The identifying name given to an address pool.
<range-end>	The range end address used when configuring an ACL.
<range-start>	The address to add or range-start address used when configuring an ACL.

ISDN enhancements

The Secure Router 1000 Series 9.3 release provides support for multiple ISDN enhancements.

Unnumbered IP over ISDN interfaces will now be supported, as well as the ability to modify the ISDN parameters SWITCH TYPE, TEI TYPE, and TEI without having to reboot the router. The purpose of unnumbered IP over ISDN is to conserve IP addresses by borrowing an IP address from another configured interface. The unnumbered interface is the interface that borrows, and it should do so from an interface that is physically up and running. In the event the unnumbered interface attempts to borrow from an non-functioning interface, the unnumbered interface will not function.

The activate command is introduced in Release 9.3 and is used to activate and change ISDN configurations. ISDN configurations not affected by this command are callingnum, callednum,, idle-timeout, and connect-delay.

Finally, Release 9.3 allows configuration of the calling party number and various ISDN timers. In the past, the calling party number has been provided automatically. This is now user configurable. Similarly, ISDN layer 2 and 3 timers were not configurable. This has changed in release 9.3, allowing the user to maximize performance of the ISDN network.

Three items users should note prior to implementation are:

- When configuring unnumbered IP over ISDN, the loopback interface cannot be used as the source.
- When users upgrade to Release 9.3 they will need to reconfigure any existing ISDN parameters. This is a result of changes in the way ISDN is configured.
- Only static routing is supported on ISDN interface.

Configuring Unnumbered IP over ISDN BRI

Use the following procedure to configure unnumbered IP over ISDN BRI.

Procedure steps

Step	Action
1	Enter Configuration Mode. **`configure terminal`**
2	Enter Interface Mode. **`interface <interface>`**
3	Configure an IP address for the Ethernet interface. **`ip address <address>`**
4	Give a name to the ISDN interface. **`interface bundle <bundle_name>`**
5	Provide BRI link bandwidth. **`link bri <link-spec>`**
6	Add encapsulation. **`encapsulation <encap-type>`**
7	Borrow an IP address from the Ethernet interface. **`ip unnumbered <interface>`**

8 Enter the **isdn** sub-tree.

```
isdn
```

9 Configure sub-tree commands.

```
switch-type <type>
idle-timeout <timeout>
connect-delay <delay>
callednum <number>
tei <tei-type>
```

10 Activate the ISDN interface.

```
activate
```

—End—

Table 27
Variable definition

Variable	Value
<address>	The IP address.
<bundle_name>	The bundle name, maximum 8 characters.
<delay>	The connect delay in seconds, in the range 1 to 60.
<encap_type>	The encapsulation protocol. Only PPP is supported.
<interface>	The interface name.
<link-spec>	BRI bandwidth, 64 or 128.
<number>	The called number, maximum 20 digits.
<tei-type>	The ISDN TEI type. Options are: • **multipoint** - Automatic TEI • **point-to-point** - Static TEI
<timeout>	The idle timeout in minutes, in the range 0 to 60. 0 disables the feature.
<type>	The ISDN switch type. Available options are: • *basic-ni* - National ISDN Switch Type • *basic-dms* - NT DMS-100 switch type • *basic-5ess* - AT & T basic rate switch type (default) • *basic-1tr6* - German 1tr6 switch type • *basic-ntt* - ntt switch type

Variable	Value
	• *basic-vn3* - French vn3 switch type • *basic-etsi* - ETSI [EURO] basic switch type • *basic-ccitt* - CCITT basic switch type

Proxy DNS

The Secure Router 1000 Series and 3120 9.3 release will provide 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 (2) or dynamic (4) DNS server entries, of which any static entries have higher precedence. Dynamic entries can be added to the list of DNS servers by DHCP & 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 also 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 will remain 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	Enter the **ip** sub-tree. `ip`
3	Ensure a DNS server has been configured. `pname_server <address>`
4	Optionally, add a second DNS server. `name_server <address>`
5	Enter the **proxy-dns** sub-tree. `proxy-dns`
6	Enable Proxy DNS. `enable`
7	Add a DNS cache entry via the CLI. `add-cache <domain>`

—End—

Table 28
Variable definition

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

ABOT Tunneling enhancement

The Secure Router 1000 Series and 3120 9.3 release 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 new 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.

If a DHCP client is used to configure an Ethernet IP address that will be used as the tunnel source dynamic IP support must be present. To address this, the tunnel source command has been modified to accept an interface name, as well as an IP address.

Configuring ABOT tunneling enhancements

The following procedure describes how to configure ABOT tunneling enhancement as described above.

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 29
Variable definition

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

QoS DSCP Values

There are many network related protocols that are generated by the router which in Release R9.2 did not have any DSCP values applied to them. This could cause network services to have their traffic dropped under load. The table below shows the DSCP values that will be set for packet originating from the router for the following network protocols:

Table 30
QoS DSCP Values

Protocol	QoS DSCP Value
RIP	CS6
OSPF (Keepalive)	CS7
OSPF (Other)	CS6
BGP (Keepalive)	CS7
BGP (Other)	CS6
PIM	CS6
IGRP, IGRP1	CS6
IGMP	CS6
VRRP	CS6
ICMP	CS6
DHCP	CS6
ISAKMP (IKE/IPSEC) port 500 UDP	CS6
NAT Traversal - ISAKMP (IKE/IPSEC) port 4500 UDP	CS6
Telnet	CS7

Memory Requirements

The SR3120 ships with 16MB of flash memory and 256MB DRAM.

The SR1001 and SR1001S ships with 16MB of flash memory and 128MB of DRAM. The SR1002 ships with 16MB of flash memory and 256MB of DRAM. The SR1004 ships with 32MB of flash memory and 256MB of DRAM.

USB and Compact Flash

You can use the following USB and compact flash memory with the SR3120, SR1001 and SR1001S:

USB

You can use USB only with the SR3120.

- Lexar: 1G, 512M
- Sandisk:(MICRO) 2G, 1G, 512M
- (MINI) 512M

Compact Flash

- Sandisk 1G, 512M
- White electronics design: 4G, 2G, 1G, 512M

Software Upgrade Process

The Nortel Secure Router 9.3 release is only supported on the Secure Router 3120 and 1000 Series models. The software is located on the CD and on the Nortel Technical Support website.

See the *Secure Router 3120 Installation Guide (NN47260-300)* or *Secure Router 1000 Series Installation Guide (NN47262-300)* for detailed instructions on how to upgrade the software.

CAUTION

It is recommended that you install the version 9.3 software upgrade through the console port. By default, telnet, SSH, SNMP agent and WebGUI services are disabled. However, if any of these services is explicitly enabled and the configuration is saved in the current software image prior to upgrading to 9.3, they will continue to remain enabled after upgrading.

SR3120 and SR1000 Series Routers software images

Description	File Size	Version	File Name
SR 3120 Application image	9446277	9.3 (r9.3)	H1000.Z

Description	File Size	Version	File Name
SR 3120 Field Upgradeable BootROM image	416592	9.3 (r9.3)	3120_r9.3.bin
SR 1001 Series Application image	9428777	9.3 (r9.3)	J1100.Z
SR 1001 Field Upgradeable BootROM image	374848	9.3 (r9.3)	1001_r9.3.bin
SR 1001s Series Application image	9884073	9.3 (r9.3)	JP1010.Z
SR 1001s Field Upgradeable BootROM image	415088	9.3 (r9.3)	1001S_r9.3 .bin
SR 1002/1004 Series Application image	8729096	9.3 (r9.3)	T1000.Z
SR 1002/1004 Series Field Upgradeable BootROM image	255764	9.3 (r9.3)	1000_r9.3.bin

Note 1: All existing SR 3120 and SR1000 Series units must download the new boot image file.

Note 2: Files ending with ".Z" are executable images, Files ending with ".bin" are the Boot ROM image.

Configuring SSH

Before upgrading to version 9.3, you can enable SSH and save the secure router configuration. You need to generate the key, then enable the SSH server, save the router configuration and then reboot the device.

To generate a key and enable SSH, use the following procedures.

Generate a RSA key

Step	Action
1	`router > config t`
2	`router/configure > ssh_keygen`
3	`Router/configure/ssh_keygen > generate rsa` Generate RSA host key

—End—

Enable the SSH server with RSA key

Step	Action
1	`Router/configure/ssh_server > hostfile shrsakey`
2	`Router/configure/ssh_server > enable` Secure shell server is enabled
3	`Router/configure/ssh_server >`

—End—

Generate a DSA key

Step	Action
1	`router > config t`
2	`router/configure > ssh_keygen`
3	`Router/configure/ssh_keygen > generate dsa` Generate DSA host key

—End—

Enable the SSH server with DSA key

Step	Action
1	`Router/configure/ssh_server > enable` Secure shell server is enabled
2	`Router/configure/ssh_server >`

—End—

Adding a pass phrase to the host file

Step	Action
1	`Router/configure/ssh_server > hostfile <filename> <phrase>`

—End—

Table 31
Variable definition

Variable	Value
<filename>	The host file name.
<phrase>	The rsa/dsa pass phrase.

SNMP MIBs

The Secure Routers SR3120 and SR1000 Series are SNMPv1/v2/v2c agents with Industry Standard MIBs, as well as private MIB extensions, which ensures compatibility with existing network management tools.

These MIBs are provided with different versions of code. Consult the Nortel website where a file named mib.zip will contain all these MIBs, and a special file named manifest for the order of the MIB compilation.

Standard MIBs

Refer to the README file for details. Be sure to compile rfc1213.mib before you compile any standard MIBs. The Standard MIB folder contains the following MIBs:

MIBs in the Standard MIB folder

Standard MIB name	RFC	File name
IANA Interface type	n/a	iana-iftype.mib
MIB for network management of TCP/IP based Internet MIBs	RFC1213	rfc1213.mib
Manages Frame Relay DLCI parameters	RFC1315	rfc1315.mib
MIB objects for DS1 interface	RFC1406	rfc1406.mib
MIB objects for DS3 interface	RFC1407	rfc1407.mib
Definitions of Managed Objects for the Ethernet-like Interface types	RFC1643	rfc1643.mib
Definitions of Managed Objects for the Fourth Version of the Border Gateway Protocol (BGP-4) using SMIv2	RFC1657	rfc1657.mib
RIP version 2 MIB extensions	RFC1724	rfc1724.mib

Standard MIB name	RFC	File name
OSPF Version 2 Management Information Base	RFC1850	rfc1850.mib
The Interfaces Group MIB using SMIv2	RFC2233	rfc2233.mib
Objects used for managing Virtual Router Redundancy Protocol (VRRP) routers	RFC2787	rfc2787.mib

Proprietary MIBs

Proprietary MIBs were known as Enterprise MIBs in previous releases of the Secure Router documentation.

Proprietary MIBs (formerly Enterprise MIBs)

Proprietary MIB name	File name
	nortel.mib
bundle.mib	ntEnterpriseDataTasmanMgmtbundle.mib
chassis.mib	ntEnterpriseDataTasmanMgmtchassis.mib
config.mib	ntEnterpriseDataTasmanMgmtconfig.mib
dos.mib	ntEnterpriseDataTasmanMgmtdos.mib
dsx-tc.mib	ntEnterpriseDataTasmanMgmtdsx-tc.mib
dsx-te1.mib	ntEnterpriseDataTasmanMgmtdsx-te1.mib
dsx-te3.mib	ntEnterpriseDataTasmanMgmtdsx-te3.mib
environment.mib	ntEnterpriseDataTasmanMgmtenvironment.mib
ethernet.mib	ntEnterpriseDataTasmanMgmtethernet.mib
fr.mib	ntEnterpriseDataTasmanMgmtfr.mib
ghdlc.mib	ntEnterpriseDataTasmanMgmtghdlc.mib
ip.mip	ntEnterpriseDataTasmanMgmtip.mip
ppp.mib	ntEnterpriseDataTasmanMgmtppp.mib
ntEnterpriseData.mib	ntEnterpriseData.mib
qos.mib	ntEnterpriseDataTasmanMgmtqos.mib
snAg.mib	ntEnterpriseDataTasmanMgmtsnAg.mib
snmp.mib	ntEnterpriseDataTasmanMgmtsnmp.mib
system.mib	ntEnterpriseDataTasmanMgmtsystem.mib
serial.mib	ntEnterpriseDataTasmanMgmtMgmtserial.mib

MIBs

Secure Routers support standard and proprietary MIBs. By default, the SNMP agent is disabled on the device. You can enable and disable the SNMP agent using the CLI.

The following tables provide information about supported MIBs. All proprietary MIBs are now compliant to SNMPv2 framework as defined in RFC 1908 (coexistence between Version 1 and Version 2 of the Internet-standard Network Management Framework). The different MIBs which define these standards are: RFC 1902, RFC 1903, RFC 1904, RFC 1905, RFC 1907, and RFC 1908.

Information about Standard MIBS

Standard MIB	Description
RFC 1213	Standard MIB-II objects. The following groups or variables are not supported for this MIB: • egp • at
RFC 1315	MIB objects for frame relay DTE interface. The following SNMP SET operation variables on frDlcmiTable are not supported for this MIB: • frDlcmiAddress • frDlcmiAddrsssLen • frDlcmiMaxSupportedVCs • frDlcmiMulticast
RFC 1406	MIB objects for DS1 interface. The following Far End tables are not supported for this MIB: • dsx1FarEndCurrentTable • dsx1FarEndIntervalTable • dsx1FarEndTotalTable
RFC 1407	MIB objects for DS3 interface.
RFC 1643	MIB objects for Ethernet-like interface. The following variables are supported for this MIB: • dot3StatsFCSErrors • dot3StatsDeferredTransmissions • dot3StatsFrameTooLongs The remainder are not supported.
RFC 1657	Describes MIB objects used for BGP4 routing protocol.

Standard MIB	Description
RFC 1724	Describes MIB objects used for RIP routing protocol.
RFC 1850	Describes MIB objects used for OSPF routing protocol.
RFC 2127	Describes MIB objects used for ISDN interfaces. Supported on SR1001 and SR1001s Series routers having an ISDN S/T or U interface.
RFC 2233	MIB objects for interface table extensions including StackTable and ifXTable. IfStackTable shows the sub-layer relationships of interfaces. The following groups or variables are not supported for this MIB3: • ifTestTable • ifRcvAddressTable • In the ifXTable, all High Counters (HC)(ifHC***) variables requiring 64-bit counters are not supported.
RFC 2787	Describes MIB objects used for managing Virtual Redundancy Protocol (VRRP) routers.

Information about Nortel Proprietary MIBs

Nortel MIB	Description
bundle.mib	Defines objects related to bundle and link configuration.
chassis.mib	Defines objects related to chassis serial number and model number.
config.mib	Defines objects related to saving configurations for network and flash.
dsx-te1.mib	Defines objects for interface cards that support TE1. These include configuration and statistics for ANSI/ATT/IETF and USER. These objects only pertain to Layer 1.
environment.mib	Defines environment-related objects, e.g., temperature, fans, etc.
ethernet.mib	Defines objects related to configuration and statistics for Ethernet interfaces.
fr.mib	Defines objects related to configuration and statistics for frame relay and MFR bundles.
ghdlc.mib	Defines objects related to configuration and statistics for generic HDLC bundles.
ip.mib	Defines objects related to IP addressable interfaces and static routes.
ntEnterpriseDataTasmanMgmtsystem.mib	Defines system objects such as IP Address, hostName and DNS server.

Nortel MIB	Description
ppp.mib	Defines objects related to PPP/MLPPP bundles for configuration and statistics.
products.mib	Defines registration objects (sysObjectID) for various Nortel products.
qos.mib	Defines objects related to QOS monitoring and configuration. This release contains only Random Early Detect (RED) objects and class-based queuing.
smi.mib	Defines the top-level object assignments for the Nortel MIB tree. This MIB should be compiled before any other Nortel MIBs are compiled. This MIB does not contain any objects that can be used for management operations.
snmp.mib	Defines objects related to SNMP community and trap_host configurations.
system.mib	Defines objects related to system information, e.g., IP address, host name, and DNS.
Serial.mib	Defines objects related to configuration and statistics for Serial interfaces.

Resolved Issues

The following table lists customer issues resolved in Release 9.3

Note: Resolved issues that begin with "Q0xxxxxx" are located in the Nortel Clarify system. Resolved issues shown with a 5 digit reference are located in the ClearQuest system.

Issues resolved since release 9.2 for Secure Router 3120 and Secure Router 1000 Series

Reference #	Subsystem	Description
10937	BGP4	rxpoll crashes when aggregate address is configured in bgp session between R1 and IXIA. The AS number in the AS set was in the same place as in the other route stream configured
11723	BGP4	The router does not flush an aggregate address configured in BGP even after removing BGP from the device under test. The workaround is to remove the aggregate first and remove BGP.
11686	PIM-SM	Assert fails in "pimsm_rpcs.c", line 222: "grp" in the particular scenario where RIP, PIM, CBSR, CRP, and IGMP were enabled

Reference #	Subsystem	Description
11835	PIM-SM	Assert fails in gated[-1940978832]: file "pimsm_wc_assert .c", line 850: "ifsp->assert_winner" in a particular scenario where RIP, PIM, CBSR, CRP, and IGMP were enabled and RIP on the serial bundle was unconfigured with traffic passing.
11836	PIM-SM	Task "tGateDTask" crashes in PIM in a particular scenario where RIP, PIM, CBSR, CRP, and IGMP were enabled and RIP on the serial bundle was unconfigured with traffic passing.
11878	PIM-SM	Task "tGateDTask" crashes in PIM whenever doing shut on bundle on which crp/cbsr has been configured and again doing no shut after 7 min
11894	PIM-SM	"tGateDTask crashes in PIM whenever IGMP group timer expires in the Box which is RP for the group in a particular scenario.
13287	QOS-PPP	Deleting class leads to decrement of packet count in previously collected samples. Save samples prior to deleting a class.
13556	Ethernet	Sub-interface won't display proxy arp when it is enabled on the same
13301	RIP/RIP2	RIP compatibility feature is not according to RFC.It fails 1 and 3 combination.
13551	CT3	Different Invalid messages are coming up while doing shut/no shut the CT3 multilink bundle while inserting errors from Cerjac
13555	HDLC	There is no warning message indicating that HDLC bundles cannot be configured as IP unnumbered interfaces.
13578	BGP4	origin and path info of an aggregated route are altered if a route belonging to the subnet of the aggrt route exists locally
13239	Platform	Bundle of dissimilar interfaces not supported
14046	OSPF	Area0 routes are not deleted in ABR even the connectivity to backbone is broken (in the transit area) to the remote area ABR. If an area is connected to backbone area by a virtual link by the ABR through a transit area, even through the transit area itself loses connection to backbone area, the routes are not deleted from ABR which is configured for virtual link in remote area. The routes are deleted in the remote area except the ABR.
14266	IP	IP load balancing is not working in per flow mode with 2 MLPPP CT3 bundles Static routes are added on for destination network

Reference #	Subsystem	Description
14274	Platform	Some links of a MLPPP bundle configured with 28 links flap due to keepalive failure when traffic is sent at a very high rate (packets in the range 64-256 at rate of 100 Mbps from one end and packet sized 1280-1500 at 100 Mbps from the other end)
14282	IP	tftpGet: Error occurred while transferring the file" for upload and download operations. Current TFTP server design will support only 3 active connections
14289	DS3	MLPPP bundle on DS3 links flaps due to keepalive failure when traffic consisting low packets lengths are sent at wire rate. Bi-directional Traffic consisting of 128 byte packets were sent at both ends at about 88 Mbps.Links of the MLPPP flapped due to keepalive failure.
14318	FireWall	MCS Instant Messaging (IM) does not work in a Secure Router trunk SIP configuration. SIP Line side is supported.
14355	CLI	Sys Obj Id changes itself back to the wrong number. The model number for Opal Jr Plus is 1001S according to the Customer Specific Definition (CSD). When we made the correction to the model number, the system changed itself back 1010.
14356	BUNDLE	BCP bundle is flapping due to keepalive failure when the traffic is passed through the bundle at wire rate for a long time.
14398	RIP	Assertion failed file "rip.c", line 1345. Intermittent in nature
14456	PIM-SM	When a static RP is configured on non-CRP/non-BSR router, dynamically learnt RPS are converted to static RP
14457	Device Manager	From GUI configuring Site to Site ike or IPsec policy with remote or Local gateway Ip address as 0.0.0.0 fails. Policy can be configured from CLI.
14469	VPN	user-grp firewall polciy is not working. 1.Configure user-grp policy. 2.Configure firewall policy for that user-grp. 3.Router skips that policy.
14505	ISDN	Unable to configure BGP routing on SR1001 with an ISDN Card
13297	CLI	The password command does not return the correct display on Secure Router 1001
13640	SNMP	SR 3120 and 1000 Series do not support the following mibs when walking the mibs via mib browser: ethernetIpFilterListName ethernetIpFilterPacketDirection. These above mibs are located in the ntEnterpriseDataTasmanMgmtethernet.mib file.

Reference #	Subsystem	Description
13753	IP	SR1001/1001S hostname of 10 characters causes telnet instability -- Q01415185. Host names should be less than 10 characters
14296	FireWall	When removing policies from the firewall the router locked up and had to be rebooted to get back operational.
13187	SNMP	Incorrect LMI timers values are displayed in SNMP manager
13764	MLPPP	Cannot ping with packet sizes greater than 1472 bytes destined from a BayRS Router to a Secure Router 3120. Pinging from a Secure Router 3120 to a BayRS router, can only ping up to 1500 byte packets. The workaround is done under the MLPPP bundle. Add the following line - "pppconfig mtu-mru-magic mtu 64-1600-4500." This line increases the default MTU size from 1500 to 1600. After this save the config, reboot or bring down & bring up the MLPPP connection and now one can ping from both sides with large packet sizes without a problem.
14144	Device Manager	Cannot telnet to the router from GUI with Microsoft Internet Explorer version 7. Microsoft IE 7 is not currently supported. Use an earlier version of Microsoft Internet Explorer
14284	Device Manager	GUI displays page expired on right click of any links in the tree. User must left click on the GUI links.
14315	Device Manager	NAT IP address configured for firewall policy corp for a policy priority 1024 (default) cannot be un-configured from GUI. User must use the CLI to un-configure the firewall policy priority 1024.
14421	Platform	“hdlc” command is missing in “show system” tree for SR1000 series platforms. The command is present in the SR3120 version.
13117	QOS-PPP	crash :tcliCo ;when interface enabled for network type broadcast and deleting the bundle.
14172	PKI	Secure Router is not able Enroll PKI Certificate Request to Entrust using SCEP. Refer to the SR1000 Series or SR3120 Configuration Guides for complete details on PKI configuration.
12713	VLAN	Creating a VLAN management interface and passing inbound management traffic through the FR bundle causes the bundle to stop transmitting.
12725	Serial	Bundles not coming up for serial V.35 when the interface is configured as a DCE under various clock rates.
12757	SNMP	Serial MIBs does not display proper values

Reference #	Subsystem	Description
12758	MLPPP	In a couple of scenarios, MLPPP bundle configured on a DS3 links flaps.
12068	MLFR	LMI parameters values are getting retained even when Interface type or LMI type is changed
12403	MLFR	Individual PVC flap when traffic is sent at more than wire speed in FR bundle configured on serial links.
12592	MLPPP	PAP/CHAP parameters are retained when encapsulation of the bundle is removed by deletion of links of the bundle
12131	BGP	eBGP and iBGP sessions are getting established even though the router-id is same in both the peer.
12306	BGP	Assert fails in gated]: file "str.c", line 1347 after executing "show ip bgp table" if BGP peer sends a route with 70 AS-PATH
12532	Bundle	Disabling and enabling RED feature on a bcp bundle stops transmitting traffic(able to receive traffic)
12405	Compact Flash	Box not bootable from image in the Compact Flash -- Often Reproducible
12430	DHCP Server	DHCP Server is not getting unconfigured using command "no ip dhcp" if the remote database is not reachable in a particular scenario.
12485	DHCP Server	DHCP Server assigns ip-address to dhcp-client which is being used by some other host in the network in a particular scenario.
12620	IP	With per_flow IP load balancing, it does not distribute the traffic flows among all PVCs in FR bundles.
12490	SNMP	TAIS and TRAI alarm traps are not shown in SR1001.
12640	VRRP	After shutting down an ethernet interface and enabling VRRP in the same, the state changes to MASTER and tries to send VRRP
12657	VRRP	VRRP WAN interface tracking does not detect the change when the WAN interface is deleted.
14783	Frame Relay	The frame size for FRF.12 should not be configured lower than 60 bytes. The minimum recommended frame size for FRF.12 with voice traffic is 80 bytes.
Q01546613	DHCP Relay	Users may see an error when trying to configure DHCP relay on an Ethernet port with v9.2. The following error may show when trying to add DHCP relay, "DHCP RELAY: MHU is enabled - cannot configure the DHCP server", even though DHCP Relay is operating correctly.

Reference #	Subsystem	Description
Q01557644	BGP	Defining a BGP route_map that references a non-existent ip_access_list may cause issues displaying and saving other ip_access_lists.
Q01559936	Firewall-NAT	In certain specific cases, HTTPS connections may hang sometimes when using Firewall NAT. If outbound Firewall NAT is in use, when loading multiple pages from a single secure (HTTPS) public-side Web server, the private-side Web client may hang. This only happens for some Web browsers and some Web servers. The Firefox Web browser is unaffected and not all Web servers will hang connections. With the Secure Router NAT port reuse policy, old NAT ports which have been cleaned up recently may be reused again with no hold-down time. This can cause the TCP state machine on some vendor' Web servers to reject the new connection from the old port. Workaround: Secure Routers may be set to send TCP:RST packets to the Web servers in this condition thus forcing the Web server to clean up old connections and accept new connections from the client on an old port. This configuration option is not currently available in the standard CLI or WebUI. It is only available in the engineering/debug mode of the Secure Router. Contact Nortel Technical Support for assistance if required. A patch release making the CLI command available will be issued.
Q01637120	Documentation	The Secure Router 1000 and 3120 Routing Guides state that multicast over GRE is supported. This statement is not correct. Multicast over GRE is not currently supported on the Secure Router 1000 and 3120 products.
Q01726245	Documentation	The cable-type command has been removed from optional module configuration parameters. The cable type is automatically detected. Use of a TRUE balun capable of converting between 75 Ohm E1 and 120 Ohm E1 is required. The TRUE balun must also provide impedence transformation between 75 Ohm and 120 Ohm.
Q01766324	Security	The followings commands have been removed from the **`ip access-list`** forward rule configuration: • finterface • faddress • rule_type

Reference #	Subsystem	Description
Q01831261	SNMP	Enterprise Mibs are incompatiabe with SR4134. Users should obtain the latest set of MIB files.
Q01810469	DSCP	DSCP markings for self-generated packets have been modified to the following: • BGP Hellos: CS7 • BGP Updates (non-keepalives): CS6 • OSPF Hellos: CS7 • OSPF Updates (non-keepalives): CS6 • RIP: CS6 • PIM: CS6 • IGRP, IGRP1: CS6 • IGMP: CS6 • ISAKMP IKE/IPSEC (udp port 500): CS6 • NAT-traversal ISAKMP/IPSEC (udp port 4500): CS6 • DHCP: CS6 • ICMP (non-echo-ping): CS6 • VRRP: CS6 • Telnet: CS7

Note: Stored configurations for ike policies, prior to release 9.2, which specified a remote-id parameter will not load properly. Release 9.2 introduced a new parameter “der-encoded-dn” which requires a quoted string to allow spaces to be specified. Additionally, the email and domain-name parameters must now be quoted strings.
Prior crypto example:
crypto
ike policy site64 64.1.1.1
local-address 20.1.1.10
remote-id email me@acme.com <mailto:me@acme.com>
Must be converted to the following to work properly in Release 9.3.
crypto
ike policy site64 64.1.1.1
local-address 20.1.1.10
remote-id email "me@acme.com"

Known Issues, Limitations, and Guidelines

The following known issues, limitations, and guidelines apply to Release 9.3:

Note: Known Issues that begin with "Q0xxxxxx" are located in the Nortel Clarify system. Known issues shown with a 5 digit reference are located in the ClearQuest system.

Known Issues and Limitations

Reference #	Subsystem	Description
11690	PIM-SM	Assert fails in "mrt.c", line 1114: "!s"in the particular scenario where RIP, PIM, CBSR, CRP, and IGMP were enabled and the serial link and then ppp3 were shutdown.
Q01763585	BGP	1001 and 1001s support a maximum prefix threshold of up to 4000 on BGP routes
Q01825080	Miscellaneous	Source address obtained from a "down" interface should not be used. Always use a loopback address.
Q01773361	BGP	BGP routes are not sent through IP-IP tunnel.
Q01783871	Routing	An error message should be shown when trying to configure routing on an ethernet sub-interface.
Q01636896	SNMP	The ethernetDhcpRelayServerAddr MIB displays an address of 0.0.0.0 when Ethernet interface is configured.
Q01826457	BGP	BGP cannot be configured after configuring NAT. Configure BGP before NAT.
Q01774970	Ethernet	Due to a platform limitation with 1000 Series routers, MTU option is limited to 64-1500-1600 on T1/E1 interfaces.
Q01820014	PIM-SM	tGateDTask crashes in PIM-SM with multicast traffic if RIP is enabled on the sub-interface.
Q01767310	SNTP	Group needs to be implemented as MIB Table to take care of multiple SNTP Servers.
Q01805060	Firewall	The "routed-intf" option with nat-ip in firewall policy does not work if the route is through a PPPoE interface.
Q01773908	VRRP	Unable to track ethernet interfaces in VRRP.
Q01826963	PIM-SM	When source specific joins are sent from IGMPv3, they need to be in the configured "ssm-range" of PIM-SM configuration to ensure correct operation.

General Guidelines and Considerations

General Guidelines and Considerations

Subsystem	Description
System	It is strongly recommended that you always do execute a write memory command from the CLI after performing any configuration changes, or before doing a manual restart of the router. The configuration file that the router uses when starting up is not automatically updated. The file is only updated when the write memory command is invoked.

Subsystem	Description
1001/3120 Platform	It is strongly recommended that when the removable compact and USB flash is in operation, e.g. file listing/copying/deleting etc., do not eject the flash card. Ejecting the compact or USB flash can render the system console unusable and may also corrupt the system or flash memory. If this situation ever occurs, the system needs to be rebooted to recover and if flash is corrupted, the flash needs to be formatted. Before performing a file related operation that uses USB and compact flash, format them on the device under test once
VPN / Firewall	When the Secure Routers are used for VPN functionality only, they still have a stateful firewall active in the routers. The firewall policies can be wild carded to let the traffic flow through. However, the traffic flowing through the router will be subjected to stateful inspection checks i.e. the router must see both outgoing and incoming traffic corresponding to a connection.
VPN	• Remote Access VPN requires the use of a 3rd party IPSec VPN client that should be the SafeNet VPN client as it has been extensively tested. Other standards-based IPSec VPN clients should work, however many vendors restrict the use of the VPN client to only their associated hardware. The SafeNet VPN client can work with any standards-based VPN IPSec hardware. • Remote Access using user group method should not be used when remote users are using a private IP address and behind a NAT Firewall. Mode config based Remote Access can be used for that application.
AAA/FW/ ACLs	Release 9.3 is verified to support up to 500 Firewall policies, 250 AAA lists and 750 ACLs.
GRE	• While configuring the GRE tunnel, verify that the tunnel destination is reachable through a physical interface. • A "redistribute connected" under OSPF will introduce a recursive route to the tunnel destination through the tunnel itself, which will bring down the tunnel. To prevent this, configure a 32-bit route for the destination through a physical interface. • The tunnel destination cannot be the peer-ip of a wan interface.
IP Multicast	• Admin scoped BSR functionality is not supported. • Multicast boundary and ttl-threshold cannot be configured. • Multicast route limit is not supported.
QoS	CR and BR must be specified when adding a new outbound class for CBQ shaping, even though CBQ shaping feature is not enabled at the time of configuration.

<table>
<tr><th>Subsystem</th><th>Description</th></tr>
<tr><td>Telco</td><td>Alarm RLOS is generated when BERT 'all 0s' option is chosen and executed. This happens because maximum number of zeros has been exceeded in a row. This will not happen when B8ZS (zero suppression) is turned on. When there are too many zeros in a row the receivers will not be able to stay in lock with the frame, and the entire trunk will go down. One should not use the all 0 pattern when the mode is AMI on both D4 and ESF framing. This issue doesn't affect E1 since HDB3 encoding is always on.</td></tr>
<tr><td>Frame Relay and OSPF</td><td>Configurations with Secure Router to Nortel Multiprotocol Router running Frame Relay and OSPF.
It is recommended that you disable RFC-1490 fragmentation as shown below.

Router > configure t
Router/configure > interface bundle fr-bn
configuring existing WAN bundle interface fr-bn
Router/configure/interface/bundle fr-bn > fr
Router/configure/interface/bundle fr-bn/fr > no enable fragment_rfc1490</td></tr>
<tr><td>QoS over Frame Relay</td><td>While QoS over Frame Relay & FRF.12 should not be turned on concurrently on the same interface since it will cause double queuing, you can turn on QoS over Frame Relay for classification and monitoring and use FRF.12 for queueing. QoS over Frame Relay does not allow setting up of more than 6 classes over low speed bundles.

The following configuration example shows a CBQ model configuration with four classes for low speed (<512K) links.

Note: When you use FRF.12 fragmentation on low-speed links, you must set the fragmentation size to 640 bytes.

In this example, the user is standardizing on a single QoS configuration regardless of link speed. Control traffic such as routing protocol traffic, is prioritized over all other traffic. The other applications prioritized are voice, interactive applications, and best effort.

CBQ model configuration
qos
add_class network-control root-out cr_percent 20 br_percent 100 priority 1
add_class premium-voice root-out cr_percent 35 br_percent 100 priority 2
add_class platinum root-out cr_percent 20 br_percent 50 priority 3
add_class standard root-out cr_percent 20 br_percent 50 priority 8
class network-control
add_dscp cs7
add_dscp cs6
exit class
class premium-voice
add_dscp cs5
add_dscp ef
exit class
class platinum
add_dscp cs4
add_dscp af41
add_dscp af42
add_dscp af43
exit class
class standard
add_dscp default
exit class
exit qos</td></tr>
</table>

Subsystem	Description

	The following configuration example shows an example of QoS over Frame Relay classification and marking only on the egress while queuing is done by FRF.12. Port-based classification allows a user to mark dscp for voice traffic properly. The following configuration is on egress direction of the PVC. Control traffic marking is a missing item.
	QoS over Frame Relay classification and marking
	`qos`
	`add_class voice root-in`
	`add_class data root-in`
	`class premium-voice`
	`add_port 5000-7000 <=== need to be replaced with customer specific values`
	`mark_dscp ef`
	`exit class`
	`class standard`
	`add_port default`
	`exit class`
	`exit qos`

ALG	The Firewall ALG on the Secure Router supports the following configurations for trunking between Call Servers. • SIP Trunking between MCS5100 Call Servers The Firewall ALG on the Secure Router does NOT support the following configurations for trunking between Call Servers. • SIP Trunking between CS1K or BCM Call Servers • H.323 Trunking between BCM Call Servers The workaround for an unsupported VoIP configuration (either Call Server or phone) is to turn off the respective firewall ALG and gatekeeper. For example, the syntax to disable the H.323 ALG is **`config term`** **`firewall global`** **`algs`** **`no h323`** **`no gatekeeper`** The following phones and protocols were tested. • **Nortel IP Phones (Unistim)** — Nortel IP Phone 2001 — Nortel IP Phone 2002 — Nortel IP Phone 2004 — Nortel IP Phone 2007 • **Nortel IP Phones (SIP)** — Nortel IP Phone 1120E — Nortel IP Phone 1140E

Subsystem	Description
	• **Servers** — CS1000E - for Unistim phones — MCS 3.5 - for PC clients and 1120E/1140E phones — TFTP/DHCP/FTP - for all phones and PC's • **Protocols** — UDP - SIP (MCS 3.5 sigma and pc clients) — TCP - SIP (LCS pc clients) — Unistim - IP phones — IP traffic in general testing
QoS- Frame Relay	The QoS feature **`enable <feature> <direction>`** should be configured at a Frame Relay bundle level QoS context. All other QoS commands such as **`add_class`**, **`class`**, **`delete_class`**, **`delete_all`** are not applicable at the Frame Relay bundle level. These commands are valid at the PVC QoS context and should be used at that level in the CLI to create flows.

Secure Router 3120 and Secure Router 1000 Series

Release 9.3 Release Notes

Publication: NN47260-400
Document status: Standard
Document version: 03.01
Document date: 28 March 2008

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

Sourced in Canada and the United States of America.