Secure Router 3120 and Secure Router 1000 Series

Release 9.2 Release Notes

NN47260-400

Document status: Standard
Document version: 02.07
Document date: 19 May 2008

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Nortel Networks.

The software described in this document is furnished under a license agreement and may be used only in accordance with the terms of that license. The software license agreement is included in this document.

Trademarks

*Nortel, Nortel Networks, the Nortel logo, and the Globemark are trademarks of Nortel Networks.

All other products or services may be trademarks, registered trademarks, service marks, or registered service marks of their respective owners.

The asterisk after a name denotes a trademarked item.

Restricted rights legend

Use, duplication, or disclosure by the United States Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013. Notwithstanding any other license agreement that may pertain to, or accompany the delivery of, this computer software, the rights of the United States Government regarding its use, reproduction, and disclosure are as set forth in the Commercial Computer Software-Restricted Rights clause at FAR 52.227-19.

Statement of conditions

In the interest of improving internal design, operational function, and/or reliability, Nortel Networks reserves the right to make changes to the products described in this document without notice. Nortel Networks does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein. Portions of the code in this software product may be Copyright © 1988, Regents of the University of California. All rights reserved. Redistribution and use in source and binary forms of such portions are permitted, provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that such portions of the software were developed by the University of California, Berkeley. The name of the University may not be used to endorse or promote products derived from such portions of the software without specific prior written permission. SUCH PORTIONS OF THE SOFTWARE ARE PROVIDED " AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

Nortel Secure Router Release Notes
In addition, the program and information contained herein are licensed only pursuant to a license agreement that contains restrictions on use and disclosure (that may incorporate by reference certain limitations and notices imposed by third parties).

Nortel Networks software license agreement

This Software License Agreement ("License Agreement") is between you, the end-user ("Customer") and Nortel Networks Corporation and its subsidiaries and affiliates ("Nortel Networks"). PLEASE READ THE FOLLOWING CAREFULLY. YOU MUST ACCEPT THESE LICENSE TERMS IN ORDER TO DOWNLOAD AND/OR USE THE SOFTWARE. USE OF THE SOFTWARE CONSTITUTES YOUR ACCEPTANCE OF THIS LICENSE AGREEMENT. If you do not accept these terms and conditions, return the Software, unused and in the original shipping container, within 30 days of purchase to obtain a credit for the full purchase price. "Software" is owned or licensed by Nortel Networks, its parent or one of its subsidiaries or affiliates, and is copyrighted and licensed, not sold. Software consists of machine-readable instructions, its components, data, audio-visual content (such as images, text, recordings or pictures) and related licensed materials including all whole or partial copies. Nortel Networks grants 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 nonexclusive 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 nonexclusive 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

Preface

How to get help

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

The 9.2 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.

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

New Features

The 9.2 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 9.2 provide interoperability of Secure Routers with other elements of the Nortel product and solutions families. This improves the position of Secure Routers in Nortel multi-product network and convergence deployments. Building on the existing, rich feature support, these new Secure Router capabilities will allow further pursuit of installed base opportunities by addressing interoperability and convergence feature needs. Additionally, the new features address some regional requirements in markets outside of North America. Lastly, these releases deliver feature parity across all SR1000 Series and SR3120 platforms and make feature support and deployment more consistent across the product range.

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.

Release 9.2

QoS over Frame Relay on all Secure Router

Provides additional support for Voice over IP solutions and other remote traffic needing the ability to be prioritized to ensure no delays occur.

X.21 support on Serial interface

Support for X.21 is a software only change with no changes to the serial interface hardware required on the routers. X.21 support allows the products to be positioned in many deployments outside North America that require serial interfaces.

In addition to X.21, the serial interface on 1001S and 3120 also supports RS-232, RS-449, EIA-530, and EIA-530A signaling in the 9.2 release. You need to order the cables for each serial interface type (X.21, RS-232, RS-449, EIA-530, EIA-503A) separately.

QoS over Ethernet

Provides the capability to prioritize and rate-limit traffic transmitted over outbound Ethernet interfaces. It will allow the positioning of the Secure Router 1000 Series and 3120 models in Ethernet WAN applications, projected to be a rapidly growing market in enterprise networks.

Cone NAT and NAT Hairpinning (Unistim)

NAT support is enhanced with restricted cone NAT and NAT hairpinning to allow Unistim traversal in conjunction with the STUN-like (Unistim port discovery protocol) protocol.

SIP ALG Interoperability with Nortel Call Servers

Provides enhancements to existing SIP ALG in the Secure Router NAT/Firewall stack to interoperate with MCS5100 Call Servers, allowing better positioning in converged applications.

FRF.12 Interoperability

Provides fragmentation and interleaving support to enhance quality of service in deployment scenarios using sub-T1 links.

cRTP Interoperability

Provides a reduction in serialization delay for RTP (voice media) packets by compressing the UDP/IP/RTP header.

Secure Routing Interoperability with Nortel VPN router

Provides enhanced support for site to site VPNs.

Design for Serviceability and other enhancements

- SNMP Trap Support

- Sharing IP addresses across forward & reverse NAT policies with Static NAT
- Statistics for VLAN dropped packets
- BGP Protocol source (i.e., route-map "route-type source")
- BGP ECMP
- Packet Capture Enhancement
- Extension to firewall policies for multiple ranges in a single dynamic NAT pool
- Extension to firewall policies for a single dynamic NAT pool in multiple policies
- IKE Dead Peer Detection allows the Secure Router 1000 Series and 3120 models to detect that the peer gateway is not reachable to improve network performance and availability

Release 9.3

Boot Config

There are two enhancements to the system boot facility. The changes are to the firmware image only. No update is necessary to the boot loader.

Procedure for converting a Tasman 3120 router to Nortel Software

If you are migrating a Tasman branded 3120 router running Tasman software to Nortel software, please use the following steps:

- Start the boot of the new H1000.Z and stop it at the boot prompt
- Boot the unit to [VxWorks Boot]

Note: Keep pressing any key until you see the boot prompt.

Step	Action
1	type "<ctrl>B<cr>"
2	type "P<cr>"
3	Enter model number: 1777
4	Power cycle the unit, it will boot to [VxWorks Boot] ***Note:*** Keep pressing any key until you see the boot prompt.
5	type "<ctrl>B<cr>"
6	type "P<cr>"
7	Enter model number: 3120

8	type "X"
9	reset to factory defaults: Y
10	type "@"
11	Enter new root username: admin

—End—

Procedure for converting a Tasman 1000 Series router to Nortel Software

If you are migrating a Tasman branded 1000 Series router running Tasman software to Nortel software, please use the following steps:

- Start the boot of the new 1000 series Software (JP1010.Z, T1000.Z) and stop it at the boot prompt
- Boot the unit to [VxWorks Boot]

  Note: Keep pressing any key until you see the boot prompt.

Step	Action
1	type "<ctrl>B<cr>"
2	type "P<cr>"
3	Enter model number: 1777
4	Power cycle the unit, it will boot to [VxWorks Boot] ***Note:*** Keep pressing any key until you see the boot prompt.
5	type "<ctrl>B<cr>"
6	type "P<cr>"
7	Enter model number: 1001, 1002 or 1004
8	type "X"
9	reset to factory defaults: Y
10	type "@"
11	Enter new root username: admin

—End—

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 and SR1000 Series:

USB

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

Compact Flash

You can use compact flash with the SR1001, SR1001s and SR3120. You cannot use compact flash with SR1002 and SR1004.

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

Software Upgrade Process

The Nortel Secure Router 9.2 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 (NN4760-300)* or *Secure Router 1000 Series Installation Guide (NN4762-300)* for detailed instructions on how to upgrade the software.

CAUTION

It is recommended that you install the version 9.2 software upgrade through the console port since telnet, SNMP agent and WebUI enabled settings are not retained during the upgrade process. The default settings for telnet and WebUI are now specifically disabled in version 9.2. You can enable SSH and save the configuration prior to the upgrade to version 9.2. Once the router has been upgraded to version 9.2, users must explicitly enable these settings and save the configuration.

SR3120 and SR1000 Series Routers software images

Description	File Size	Version	File Name
SR 3120 Application image	9253370	9.2 (r9.2)	H1000.Z
SR 3120 Field Upgradable BootROM image	416592	9.2 (r9.2)	3120_r9.2.bin
SR 1001 Series Application image	9649770	9.2 (r9.2)	J1100.Z
SR 1001 Field Upgradeable BootROM image	374064	9.2 (r9.2)	1001_r9.2.bin
SR 1001s Series Application image	10103064	9.2 (r9.2)	JP1010.Z
SR 1001s Field Upgradeable BootROM image	414608	9.2 (r9.2)	1001S_r9.2 .bin
SR 1002/1004 Series Application image	8532303	9.2 (r9.2)	T1000.Z
SR 1002/1004 Series Field Upgradeable BootROM image	255515	9.2 (r9.2)	1000_r9.2.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.

MIBs have been updated for release 9.2 to provide additional benefits as described in "New Features" (page 8).
The MIBs file for release 9.2 is named SR1000_3120_r9.2MIBs.zip.

Before upgrading to version 9.2, 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 key

Step Action

1

```
router > config t
```

2 `router/configure >` **`ssh_keygen`**

3 `Router/configure/ssh_keygen >` **`generate ?`**

4 `Router/configure/ssh_keygen >` **`generate rsa`**

Generate RSA host key

—End—

Enable the SSH server

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

—End—

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

Standard MIB name	RFC	File name
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
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

Proprietary MIB name	File name
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

Standard MIB	Description
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.
RFC 1724	Describes MIB objects used for RIP routing protocol.
RFC 1850	Describes MIB objects used for OSPF routing protocol.
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.

Nortel MIB	Description
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.
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 9.2

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 9.1.1 for Secure Router 3120

Reference #	Subsystem	Description
13274	MLFR	PVCs of a MFR bundle flap intermittently when traffic is sent through all the PVCs at more than CIR configured. 20 PVCs were configured on a MFR bundle with 5 T1 channels of a CT3 card
11003	BGP	Aggregate address is advertised even when there is no contributing route in bgp

Reference #	Subsystem	Description
11073	BGP	In the following scenario, Router does not install the BGP routes received over an EBGP multihop session. 1. Configure a ppp bundle between R1 R2 and between R2 R3 2. Configure IBGP between R1 and R2 and redistribute connected routes of R2 to R1 3. Configure a static route in R3 to reach R1 with R2 as the next hop 4. Configure a EBGP multi-hop session between R1 and R3 Note: R1 uses IBGP routes from R2 to establish TCP session with R3 5. Configure some static routes in R3 and redistribute them to R1
13356	Ethernet	Ethernet vlanid is not getting added to the subinterface
13365	Ethernet	The device under test is not responding to the ping request for the sub-interface,if ip address of main interface is unconfigured
13327	IGMP	TcliCo crash occurred when giving "show ip igmp groups detail" while sending group leave report from the igmpv2 host
12883	OSPF	A tag of 10 digits falling within permitted range set to external routes redistributed into ospf is not saved in the config
13261	Platform	If a large number of packets that can’t be routed arrive at the Ethernet port, it hogs the CPU and slows the system down
11149	VRRP	Telnet session on the router running VRRP and OSPF hangs when debugging of ARP packets is enabled
13328	SNMP	Wrong status display for T1s interfaces within CT3 in SNMP port information. SNMP manager is displaying status as Up for T1s within CT3 though they are actually down. CLI will show correct status
11640	Telco	LEDs are not displaying correct status when the peer link is disabled. Even if the peer is disabled the LEDs continues to maintain the green state (UP)
13257	VLAN	Links are flapping for MFR bridge vlan bundle when sending wire rate vlan traffic. MFR bundle had 10 t1 links in a ct3, while passing vlan traffic through it.
13367	SNMP	Setting the system host name thru SNMP doesn’t update the CLI host name
11413	Serial	L3_ Wrong error message is displayed when adaptive rate is configured on the serial bundle

Reference #	Subsystem	Description
13530	Radius	The display of RADIUS information does not show which type of user mapping exists.
13409	Platform	show boot_params command accepts parameters
11359	PIM-SM	PIM does not send joins after executing the command clear ip mroute even if receiver is active and is sending IGMP joins
11545	Platform	If one power supply is present, the system shows that two power supplies are OK.
11814	Serial	The link drop and restore feature is only for multilink bundles but serial PPP bundle accepts restore command
13303	CT3	Interface display for local and remote loopback line_t1/payload_t1 for T1s should be slot/port/t1_no in place of slot/t1_no
13554	MLPPP	Though the debug message shows the changing linecode is not supported still the box is accepting the linecode change command
13238	WIF	Bundle cannot span across 2 CT3 cards with all links configured on the bundle
12709	VLAN	VLAN management enable/disable command for interfaces is not present. It exists in the tunnel configuration, but for all other interfaces/bundles
12743	GRE	Add Ethernet0 Ethernet1 as unnumbered source are not able to provide the slot/port number
12787	QoS-PPP	Throughput of PPP bundle configured on serial link only has 80% bandwidth of QoS class at 1024 byte packets
14528	OSPF	PIM Crash when encountering an OSPF routing loop due to errors in updating the pim list. Fix created so when this is encountered there is no crash and log an event that there are routing loops. The log message is as follows: Warning: Check for possible routing loops.
14529	CLI	IGMP saves improperly if no interface is defined. Fix created to check if an interface is defined before allowing to fetch at the next level.
14530	IP	Arp Table corruption if the arp reply comes back from a different interface then the interface that the arp request was send on. Fix created to only update the arp table if the arp reply came from the same interface that the request was sent on.

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 9.2.

```
crypto
ike policy site64 64.1.1.1
local-address 20.1.1.10
remote-id email "me@acme.com"
```

Issues resolved since release 8.3.6 for Secure Routers 1001 and 1001S and release 8.4.5 for Secure Routers 1002 and 1004

Reference #	Subsystem	Description
Q01299095	BGP	Secure Router crashes while trying to save the local configuration in a Multi Hop BGP configuration environment
Q01298905	Boot strap	When a Secure router receives a Candidate Boot Strap Router advertisement packet with a prefix count equals to zero a crash occurs
Q01298874	IP Multicast	Secure router crashes after the sender stops sending traffic momentarily in a high throughput Multicast traffic environment
Q01300033	RIP	Secure Router will not advertise directly attached interfaces via RIP1 or RIP2 to the neighbor
Q01300027	RIP	Secure Router will not advertise non natural mask static routes over a RIP1 interface
Q01300008	MLPPP	Secure Router does not support Multicast Extensions to Multi Link PPP
Q01299998	QoS	DSCP markings for the Router Generated packets are not Compliant with Nortel Networks Service Class definitions
Q01300183	IPSec VPN	When the VPN router as an ABOT initiator tries to initiate an Ipsec Tunnel to a secure router which is the responder the tunnel never gets established
Q01298937	VRRP	Secure router fails to generate Gratuitous ARP or use Virtual Mac address in a VRRP environment
Q01314561	MLPPP	Secure router sends a default MRU value during a MLPPP negotiation
12330	MLPPP	rxPoll crash seen in PPP bundles on serial links when mru is set to boundary values

Reference #	Subsystem	Description
Q01375334	BGP	Secure Router crashes when BGP aggregate summary and PIM are configured
Q01314575	MLPPP	Secure Router ignores LCP config rejects for certain options from the peer during a MLPPP negotiation

Known Issues, Limitations, and Guidelines

The following known issues, limitations, and guidelines apply to Release 9.2:

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 #	SR	Subsystem	Description
10937	SR3120	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	SR3120	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	SR3120	PIM-SM	Assert fails in "pimsm_rpcs.c", line 222: "grp" in the particular scenario where RIP, PIM, CBSR, CRP, and IGMP were enabled
11690	SR3120	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.
11835	SR3120	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	SR3120	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	SR3120	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

Reference #	SR	Subsystem	Description
11894	SR3120	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	SR3120	QOS-PPP	Deleting class leads to decrement of packet count in previously collected samples. Save samples prior to deleting a class.
13556	SR3120	Ethernet	Sub-interface won’t display proxy arp when it is enabled on the same
13301	SR3120	RIP/RIP2	RIP compatibility feature is not according to RFC.It fails 1 and 3 combination.
13551	SR3120	CT3	Different Invalid messages are coming up while doing shut/no shut the CT3 multilink bundle while inserting errors from Cerjac
13555	SR3120	HDLC	There is no warning message indicating that HDLC bundles cannot be configured as IP unnumbered interfaces.
13578	SR3120	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	SR3120	Platform	Bundle of dissimilar interfaces not supported
14144	SR3120	Device Man ager	Cannot telnet to the router from GUI with Microsoft Internet Explorer version 7. Microsoft IE 7 is not currently support. Use an earlier version of Microsoft Internet Explorer
14284	SR3120	Device Man ager	GUI displays page expired on right click of any links in the tree. User must left click on the GUI links.
14315	SR3120	Device Man ager	NAT IP address configured for firewall policy corp for a policy priority 1024 (default) cannot be unconfigured from GUI. User must use the CLI to unconfigure the firewall policy prioirty 1024.
14046	SR3120 and SR1000 Series	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.

Reference #	SR	Subsystem	Description
14266	SR3120	IP	IP load balancing is not working in per flow mode with 2 MLPPP CT3 bundles Static routes are added on for destination network
14274	SR3120	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	SR3120 and SR1000 Series	IP	tftpGet: Error occurred while transferring the file" for upload and download operations. Current TFTP server design will support only 3 active connections
14289	SR3120	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	SR1000 Series	FireWall	MCS Instant Messaging (IM) does not work in a Secure Router trunk SIP configuration. SIP Line side is supported.
14355	SR1000 Series	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	SR1000 Series	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	SR1000 Series	RIP	Assertion failed file "rip.c", line 1345. Intermittent in nature
14456	SR1000 Series	PIM-SM	When a static RP is configured on non-CRP/non-BSR router, dynamically learnt RPS are converted to static RP
14457	SR3120 and SR1000 Series	Device Man ager	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.

Reference #	SR	Subsystem	Description
14469	SR3120 and SR1000 Series	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	SR1000 Series	ISDN	Unable to configure BGP routing on SR1001 with an ISDN Card
13297	SR1000 Series	CLI	The password command does not return the correct display on Secure Router 1001
13640	SR3120	SNMP	SR 3120 and 1000 Series do not support the following mibs when walking the mibs through mib browser: ethernetIpFilterListName ethernetIpFilterPacketDirection. These above mibs are located in the ntEnterpriseDataTasman Mgmtethernet.mib file.
13753	SR1000 Series	IP	SR1001/1001S hostname of 10 characters causes telnet instability -- Q01415185. Host names should be less than 10 characters
14296	SR1000 Series	FireWall	When removing policies from the firewall the router locked up and had to be rebooted to get back operational.
13187	SR1000 Series	SNMP	Incorrect LMI timers values are displayed in SNMP manager
13764	SR3120	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	SR1000 Series	Device Man ager	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	SR1000 Series	Device Man ager	GUI displays page expired on right click of any links in the tree. User must left click on the GUI links.

Reference #	SR	Subsystem	Description
14315	SR1000 Series	Device Man ager	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	SR1000 Series	Platform	“hdlc” command is missing in “show system” tree for SR1000 series platforms. The command is present in the SR3120 version.
13117	SR3120 and SR1000 Series	QOS-PPP	crash :tcliCo ;when interface enabled for network type broadcast and deleting the bundle.
14172	SR3120 and SR1000 Series	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	SR3120	VLAN	Creating a VLAN management interface and passing inbound management traffic through the FR bundle causes the bundle to stop transmitting.
12725	SR3120	Serial	Bundles not coming up for serial V.35 when the interface is configured as a DCE under various clock rates.
12757	SR3120	SNMP	Serial MIBs does not display proper values
12758	SR3120	MLPPP	In a couple of scenarios, MLPPP bundle configured on a DS3 links flaps.
12068	SR1000 Series	MLFR	LMI parameters values are getting retained even when Interface type or LMI type is changed
12403	SR1000 Series	MLFR	Individual PVC flap when traffic is sent at more than wire speed in FR bundle configured on serial links.
12592	SR1000 Series	MLPPP	PAP/CHAP parameters are retained when encapsulation of the bundle is removed by deletion of links of the bundle
12131	SR1000 Series	BGP	eBGP and iBGP sessions are getting established even though the router-id is same in both the peer.
12306	SR1000 Series	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	SR1000 Series	Bundle	Disabling and enabling RED feature on a bcp bundle stops transmitting traffic(able to receive traffic)

Reference #	SR	Subsystem	Description
12405	SR1000 Series	Compact Flash	Box not bootable from image in the Compact Flash -- Often Reproducible
12430	SR1000 Series	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	SR1000 Series	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	SR1000 Series	IP	With per_flow IP load balancing, it does not distribute the traffic flows among all PVCs in FR bundles.
12490	SR1000 Series	SNMP	TAIS and TRAI alarm traps are not shown in SR1001.
12640	SR1000 Series	VRRP	After shutting down an ethernet interface and enabling VRRP in the same, the state changes to MASTER and tries to send VRRP
12657	SR1000 Series	VRRP	VRRP WAN interface tracking does not detect the change when the WAN interface is deleted.
14783	SR3120 and SR1000 Series	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	SR3120 and SR1000 Series	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.
Q01557644	SR3120 and SR1000 Series	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	SR3120 and SR1000 Series	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.

Reference #	SR	Subsystem	Description
			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	SR3120 and SR1000 Series	Documentati on Errata	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.

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.
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.

Subsystem	Description
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.
VPN	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 9.2 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.
GRE	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.
GRE	The tunnel destination cannot be the peer-ip of a wan interface.
IP Multicast	Admin scoped BSR functionality is not supported.
IP Multicast	Multicast boundary and ttl-threshold cannot be configured.
IP Multicast	Multicast route limit is not supported.
QoS	CR and BR must be specified when adding a new outbound class for policing, even though they are CBQ parameters
Telco	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.
Frame Relay and OSPF	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**

<table>
<tr><th>Subsystem</th><th>Description</th></tr>
<tr><td>QoS over Frame Relay</td><td>

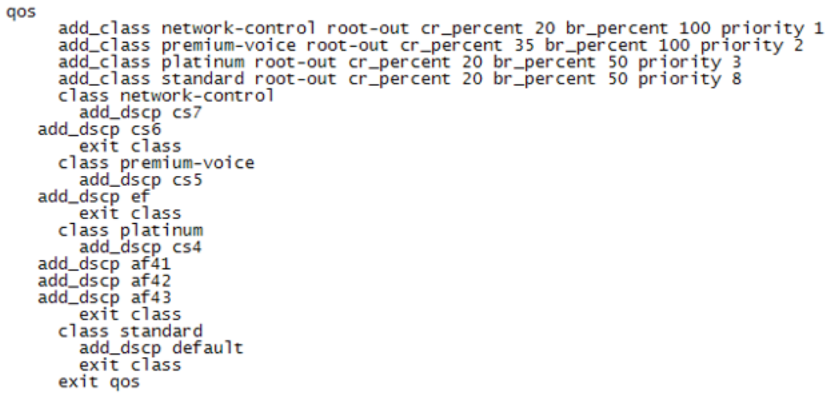
While QoS over Frame Relay & FRF.12 should not be turned on concurrently on the same interface since it will cause double queuing, you can turn on QoS over Frame Relay for classification and monitoring and use FRF.12 for queueing. QoS over Frame Relay does not allow setting up of more than 6 classes 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.

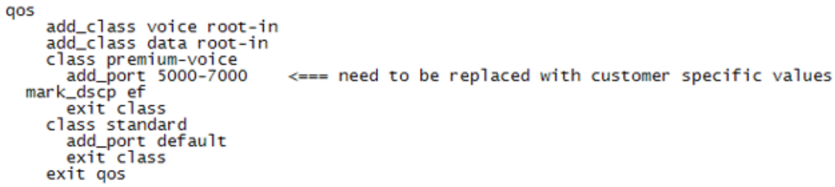
CBQ model configuration



```
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
```

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
```

</td></tr>
</table>

Subsystem	Description
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 • **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

Subsystem	Description
	— 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 9.2 Release Notes

Publication: NN47260-400
Document status: Standard
Document version: 02.07
Document date: 19 May 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.

The information in this document is subject to change without notice. Nortel Networks reserves the right to make changes in design or components as progress in engineering and manufacturing may warrant.