Version 8.4.2

Part No. 322008-A
March 2006

600 Technology Park Drive
Billerica, MA 08121-4130

Secure Router 1002, 1004 Release Notes

NORTEL

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 EGLIGENCE) ARISING OUT OF YOUR USE OF THE SOFTWARE, EVEN IF NORTEL NETWORKS, ITS AGENTS OR SUPPLIERS HAVE BEEN ADVISED OF THEIR POSSIBILITY. The forgoing 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.

Table of Contents

1 Introduction

In 2006, Nortel had acquired Tasman Network. From the acquisition the Nortel Secure Routers emerged. Bug fixes and enhancements were provided from feedback from field and customers.

The Nortel Secure Router 8.4.2 release is for general use and is supported on the Secure Router 1002/1004 platforms only. The 8.4.2 release will be downloadable from the Customer Service Portal site; www.nortel.com/support; select "Product Categories" and then select "Routers and Routing Switches". Scroll down to the Secure Router family.

These release notes are for Nortel Secure Router OS version 8.4.2. With the release of the 8.4.2 software, all SR routers will be shipping with this version of software installed on the listed platforms. This release includes new functionality and bug fixes, as well providing support for all of the features found in prior versions 8.4, 8.0.x, 7.x and 6.0.x of software. Please refer to the New Features section of this document for further details.

Topics covered in these release notes are:

- **New Features, Improvements and Changes**
- **Supported Features**
- **Memory Requirements**
- **Feature Documentation**
- **Software Deliverables**
- **Resolved Problems**
- **Known Issues and Limitations**
- **Contacting Nortel Technical Support**

2 New Features, Improvements and Changes

The 8.4.2 release is follow-on to all 7.x, 8.0.x and 8.4 software releases and contains all of the features included in those versions.

8.4.2 New Features and Improvement Summary

8.4.2 is built on 8.4.1 and includes changes to productize Tasman routers into Nortel's Secure Router product line following the acquisition. The changes enhance the already available features from 8.4.1 by adding Nortel CLI, GUI and SNMP related changes for better integration, manageability, and sustenance within the Nortel product family of Secure Routers. Such integration enhancements will be a continuous effort and it is expected that future releases will include changes in this regard.

8.4.1 New Features and Improvement Summary

8.4.1 is built on 8.4 (and further sub-releases) and includes important customer enhancements and bug fixes which are listed in section '7'.

8.4 New Features and Improvement Summary

8.4 is built on 8.2 (and further sub-releases) and includes important bug fixes and enhancements. Customer requested enhancements are listed in Section '3' and bug fixes are listed in section '7'.

2.2 Class based Queuing (CBQ) QoS for FR and MFR Interfaces

Until this release, SR Frame Relay (and MFR) interfaces provided the traditional PVC based rate limiting quality (shaping and policing) of service that is defined in the frame relay standards. Queuing of packets was only allowed when congestion was noticed in the outbound direction.

With the implementation of CBQ based QoS on FR and MFR interfaces, now both options exist for administrators to configure their QoS requirements over the FR/MFR interface.

Here are some important facts to remember:

- Both CBQ based QoS and traditional rate limiting QoS cannot be enabled on the same FR/MFR interface
- Classes are created at the PVC level, QoS is enabled at the Interface level
- The FR CBQ QoS functionality, behavior and configuration is identical to the CBQ QoS available on PPP and HDLC Interfaces today
- CBQ QoS can be enabled to be merely a 'monitoring' of the flows, same as the CBQ monitoring feature available on the PPP/HDLC interfaces
- CBQ option is available on the WAN outbound (egress) direction and policing (rate limiting) option is available in both WAN outbound (egress) and WAN inbound (ingress) direction. Please note that both CBQ based QoS and policing (rate limiting) cannot be enabled on the egress direction, at the same time.

Below CLI tree show new commands introduced into the frame relay sub-CLI level. For detailed command description, please refer to the Command Line Reference Guide online or the Documentation CD accompanying the product.

```
bundle
|-- fr
|    |-- pvc
|    |    |-- qos
|    |    |    |-- add_class
|    |    |    |-- class
|    |    |    |    |-- committed_rate
|    |    |    |    |-- committed_rate_percent
|    |    |    |    |-- burst_rate
|    |    |    |    |-- burst_rate_percent
|    |    |    |    |-- police
|    |    |    |    |-- priority
|    |    |    |    |-- queue_buffers
|    |    |    |    |-- add_src_ip
|    |    |    |    |-- add_dst_ip
|    |    |    |    |-- add_port
|    |    |    |    |-- add_vlan_id
|    |    |    |    |-- add_dscp
|    |    |    |    |-- add_dot1p
|    |    |    |    |-- delete_ip_address
|    |    |    |    |-- delete_port
```

```
|    |    |    |    |-- delete_vlan_id
|    |    |    |    |-- delete_dscp
|    |    |    |    |-- delete_dot1p
|    |    |    |    |-- nat_ip
|    |    |    |    |-- mark_dscp
|    |    |    |    |-- mark_dot1p
|    |    |    |    |-- mark_vlan
|    |    |    |    |-- ewf
|    |    |    |    |-- red
|    |    |    |    |-- enable
|    |    |    |-- delete_class
|    |    |    |-- delete_all
|-- qos
|    |-- enable
```

2.3 Adaptive QoS - Dynamic QoS Class parameter adjustment based on Bandwidth Availability

This feature only applies to Multilink PPP interfaces. If the QoS class parameters are created with '%' values assigned, if individual links within the 'bundle' interface go in and out of service, then the 'dynamic QoS class parameter adjustment' will recalculate the new parameters and enforce traffic accordingly.

The previous release (8.2) '%' parameter assignment provided static link addition/deletion (administratively adding/deleting links to/from bundle) related calculations. The dynamic recalculation of the parameters upon detection of individual link status changes was not available until this release. Please note that the '%' parameter assignment is only available on the PPP/MLPPP interfaces, not on the FR/MFR interfaces.
Following link status conditions cause the bandwidth calculation to be updated dynamically:

- Administratively shutting down/enabling physical links
- Links down due to alarms (LOF, LOS etc.)
- Links down due to excessive errors

Please note the following conditions that cause the link to go down/up, do not trigger dynamic class bandwidth calculations:

- Excessive Zeros Received (REXZ)
- Receive Far End Block Error (RFBE)
- Loss of Receive Clock (LORC)
- Link loopbacks
- Transmit Pulse Density (TPDE)
- Transmit Remote Alarm Indication (TRAI)
- Threshold alarms (1-10)

2.4 VLAN Encapsulation over GRE

This feature enables transport of Ethernet frames over IP. It combines VLAN Forwarding with GRE encapsulation. IPSec can be enabled on the GRE tunnel, protecting the Ethernet Frame data.
Below is a list of features supported:

- Can interconnect remote-sites using
  - 802.1Q Tagged frames
  - Untagged Ethernet II frames
- Jumbo frame (4K)
- VLAN tagging & forwarding

- VLAN Management
- GRE
  - IP Fragmentation
  - Tunnel protection using IPSec
  - 100 tunnels
- Point to Multipoint

Please note that the following features cannot be supported:
- Outbound QoS using inner IP flow
- VLAN flooding over GRE Tunnels

2.5 Timed Reboot

New CLI parameter is added to 'reload' command to allow the administrator to assign a delay to the reboot process so that reboot can be executed at a certain time convenient to the administrator.

At the top level tree	router# reload ?
Name	**reload –** restart the system
Syntax	**reload [cancel/in]** <cr>
Description	**[cancel]** – Cancel a current scheduled reload of the system **[in]** – delay in minutes before reloading the system

2.6 Serial Console Timeout

CLI command is added to configure the Console timeout duration (auto logging off the user). The default is the same as the Telnet console timeout. The CLI command also enables turning off the timeout feature wherein the console screen doesn't logout.

2.7 Large Telnet Banner

The CLI command previously allowed a maximum of 255 character long Telnet banners. With this new addition, the telnet banner could be many more than 1000 characters.

2.8 Suppress configuration during Boot-up

When the system boots and configures its previous stored state, for security purposes, Secure Routers will not show the last saved configuration as the system is being configured. Prior to this release, each line in the last saved configuration file (system.cfg) was displayed and configuration status was displayed.

At the 'configure/system' level tree	Router/configure/system# display-boot-config ?
Name	**display-boot-config –** whether to dump last saved configuration when system boots
Syntax	**Display-boot-config [yes/no]** <cr>
Description	**[yes]** – old behavior, dump system.cfg content when system boots up **[no]** – the new 'default behavior': do not display system.cfg content when system boots up

2.9 NxT1 MLPPP Compatibility with Juniper M-Series when LFI is auto-enabled

This was primarily a customer reported issue regarding Secure Routers connected using NxT1 MLPPP configuration to Juniper M-40 routers which had LFI enabled (by default) couldn't pass some of the traffic. This was because M-40 was transmitting some high priority traffic without MLPPP headers and also without a full IP header (some header compression was auto-enabled without negotiation with the SR). SR patch was to receive these packets without dropping them.

2.10 Other Bug fixes and enhancements

8.4 also includes important enhancements and bug fixes that are listed in sections below.

8.2 Features and Improvement Summary:

- Secure Router Device Manager Web User Interface for SR 100X product lines (1001, 1002, 1002E, 1004 and 1004E products)
- Enhanced MIB to support SNMP based router management using any third party SNMP v1/v2 based management software like HP OpenView.
- Stateful Firewall is now included with 'VPN for management only' license
- Source Address for SNMP response packets is now configurable.
- A VLD enabled Ethernet interface can now accept both 802.1q and 802.3 frames and will add VLD encapsulations before forwarding them.
- Excessive HDLC error handling within the system

2.11 Web based Graphical User Interface (for SR 100X products only)

This is the first release of the web based graphical user interface Device Manager feature that is designed for SR 1001, 1002, 1002E, 1004 and 1004E routers. SR extends a giant leap ahead in the ease of configuration and management by providing both novice and experienced users the ability to configure and maintain the above routers using the HTTP based device manager. The device manager is embedded in the router and uses your Internet browser as the client. The recommended browser is the Microsoft™ Internet Explorer version 5.5 or higher. The recommended resolution is 1024x768.

There are top three tabs at the top of the screen, which represent three distinct personalities and feature set for different users.

Status Tab

The first page after the successful login screen shows the status of the overall system, which includes serial number of product, s/w version, power supply and other information. In addition, the status/health page also displays brief information about all the interfaces currently configured and also VPN and Stateful Firewall statistics. Links on this page take the user to detailed status and statistics display for each of the individual areas.

Guided Setup Tab

The second important aspect of the Web based GUI is the Guided Setup page. This page focuses on those users unfamiliar with any router CLI to easily configure the basic interfaces, VPN and Stateful Firewall in a stepwise and network diagram assisted manner.

Configuration Tab

The third part of the Web GUI provides CLI level flexibilities for creating/modifying/deleting detailed configurations of the router. This section is more useful for advanced users.

The first release of the Device Manager focuses primarily on the configuration and monitoring of VPN and Stateful Firewall feature set. In addition, configuration of basic LAN and WAN interfaces and some system management options are enabled in this release.

Some important considerations about the first version of Device Manager

- The Device Manager allows basic configuration of LAN interfaces. VLAN, VLD etc. configurations are not included in this release.
- WAN interface configuration is limited to PPP/MLPPP IP-terminated bundle configurations.
- Dynamic routing parameters cannot be configured in this release; only static routes can be configured.
- Most advanced VPN and Firewall features can be configured in this release.
- ACLs, QoS etc. advanced features are planned for support in future Device Manager releases.

Nortel will be continuously improving its SR Web GUI based configuration feature and will release more features in upcoming releases.

2.12 SNMP MIB support for Advanced Management functions

8.2 includes many enhancements to the existing standard and enhanced MIBs to provide better management of the system through third party management software like HP OV. These modified MIBs now allow configuration of:

- Global Passwords
- Telnet banners
- RADIUS and TACACS+
- Firmware upload and download
- Configuration files upload and download
- Syslog settings
- IFNET table to enable or disable the status of the interfaces
- Reboot/reload router
- SNMP traps
- DNS settings

2.13 Stateful Firewall enabled for “VPN for management only” License

In the previous releases, out of the three VPN feature license options, the VPN for management only license feature didn't work with stateful firewall. With 8.2, the complete stateful firewall is enabled by default on all VPN license options.

2.14 Source IP address configurable on SNMP response packets

As per RFC 1098 and 1901, the user should have the option to change the SNMP response packet's source IP address in the IP header. Until this release, the SNMP chose internally the interface on which the response packet was going as the source IP address and it was not user configurable.
A new CLI command was added in the snmp-server section to provide the flexibility to the user. The default behavior (no user configuration) is same as before, the source IP address is the outgoing interface's address. If configured, all outgoing SNMP packets originated from the router will carry the user configured ip address as the source address.

New Command:

Under 'snmp-server' tree	`router/configure/snmp-server# snmp-source ?`
Name	**`snmp-source -`** `Configure the SNMP Source IP Address.`
Syntax	**`snmp-source [address]`** `<cr>`
Description	**`[address]`** `- SNMP Source IP Address`

2.15 VLD Interface accepts both 802.1q and 802.3 frames

In the previous releases, if an Ethernet interface was configured for VLD tagging (Queue in queue/ double tagging), the router only processed incoming 802.1q packets and discarded 802.3 packets. This caused some upstream routers to lose periodic update/hello packets, which were untagged. With 8.4, the router will tag the untagged (802.3) incoming packets with VLD tag and proceed with the packet forwarding.

2.16 Excess HDLC error handling

In certain rare scenarios, faults in single T1/E1 link could create in excess of 1,000 consecutive HDLC link errors, which could cause the system to be temporarily unresponsive to other inputs. If there are other WAN interfaces configured in the system, they might loose some keep alive packets resulting in link status flaps. When the link generates so many errors, the link is immediately brought down and system generates SNMP link down trap messages and will try to recover the link after certain time gap. If the link is still in error, the system will generate more SNMP traps and continue to monitor the link for errors. The 'show interface bundle <bundle name>' will show the error status of the link(s) within the bundle.

To recover from such flapping status situation, use the 'hdlc_error' command to set the error count threshold for bringing the link down. Use the 'hdlc_link_deactivate' command to define the action the system should take if error threshold is reached. The third new command 'hdlc_link_activate' allows the user to bring those links up that were brought down by the deactivate command. Once the link has been brought down due to excessive HDLC errors, the user has to bring the link back up manually by using 'hdlc_link_deactive' command. The default behavior is that the system will behave as in the pre-8.2 version, that is, the system will continue to try and recover the link.

New Command 1:

Under 'system' tree	host/configure# system hdlc_error ?
Name	**hdlc_error –** Sets the threshold for consecutive hdlc errors (default: 1000)
Syntax	**hdlc_error [error_limit]** <cr>
Description	**[error_limit]** – Number of consecutive hdlc errors on a link (default: 1000). Valid Range(s): 100 – 12000.

New Command 2:

Under 'system' tree	host/configure# system hdlc_link_deactivate ?
Name	**hdlc_link_deactivate –** System wide setting for whether to deactivate links after excessive HDLC errors threshold is exceeded
Syntax	**hdlc_link_deactivate <cr>**

New Command 3:

Under 'bundle' tree	Host configure interface bundle *xxx*# hdlc_link_activate ?
Name	**hdlc_link_activate –** Setting to allow link to be brought up without having to shutdown the bundle (if link has automatically deactivated due to excessive HDLC errors)
Syntax	**hdlc_link_activate <cr>**

3 Customer Requested Enhancements

The following lists represent software enhancements that were specifically requested by customers and resolved in prior Tasman Networks TiOS releases.

NOTE: Reference numbers in numeric format were reported and logged in the Tasman bug tracking database. Reference numbers starting with "Q" were reported and logged in the Nortel bug tracking database.

These following enhancements were added to **r8.4**.

Reference #	Subsystem	Description
10153	Bootrom	Allows the 'boot prompt' to be customizable to help customer write scripts to auto-configure Secure Routers.
12337	MLPPP	NxT1 MLPPP LFI Compatibility with Juniper M40
8853	Management	Would like to see Console timeout option as a security feature.

The following represents software enhancements that were specifically requested by customers. These enhancements were added to **r8.2.1**.

Reference #	Subsystem	Description
9927	System Recovery	The administrator now has the option to choose what action the boot-prompt command 'X' can perform on the SR 100X products. For more information, refer to section 2.1 – system recovery enhancements.

The following represents software enhancements that were specifically requested by customers. These enhancements were added to **r8.2**.

Reference #	Subsystem	Description
9203	SNMP	To be compliant with RFC 1098 and 1901, the source IP address of the SNMP response packets should be allowed to be set by the user. New CLI command added under 'snmp-server' allows user configurable snmp-source ip address.
9279	VLAN	Previously, the Ethernet interface could be set up to access only 802.1q packets for VLD (Queue in Queue) tagging. 802.3 packets if received were dropped. With r8.2, the OS will tag the 802.3 packets with VLD header and process as per VLAN/VLD forwarding table.
9658	Platform	Excessive link errors on one bundle cause all bundles in the system to go down momentarily.
9659	VPN/Firewall	'VPN for management only' license previously didn't allow stateful firewall to be configured.
9675	RADIUS	The service-type value '6' is now recognized as an admin-user (level 1). If the user specifies the service-type as login-user (level 1) or administrator-user (also level 1), RADIUS authentication now treats them as administrator (level 1) user login for the router.

4 Supported Features from Previous Releases

Secure Router OS version 8.4.2 supports all of the features from previous software releases, plus the new features available only in 8.4 and 8.0.x. All features are available on the SR 1002, 1004 routers.

5 Memory Requirements

SR 1002, 1004 products currently come equipped with 16(1002/1002E) or 32 (1004/1004E) Mbytes of Flash memory and 256 Mbytes of SDRAM memory. With this configuration customers can run the Dynamic routing software including RIP v1 & v2, OSPF and BGP4 as well as advanced features such as VPN and Firewall. VPN is an optionally licensed feature and not included in the base 8.0 release. Please contact Nortel for information on VPN licensing.

6 Software Deliverables

The release 8.4.2 is supported on SR 1002/1002E and 1004/1004E models only.

SR 1002(E) and 1004(E) Routers

Description	Date	File Size	Version	File Name
SR 1002/1004 Application image	03/01/2006	7,567,760	r8.4.2	T1000.Z
SR 1002/1004 Field Upgradeable BootROM image	03/16/2005	255,544	T1k031605	T1000_r8_2_1a.bin

NOTE: All existing SR 1002 and 1004 units must upgrade to the new BootROM images to run r7.0.2 or later software. All new SR 1002 and 1004 units will be shipped with both the updated EPROM and will the downloadable BootROM image.

SNMP MIBs

Both standard and enterprise MIBs have been updated to provide additional benefits as described in section 2.2 above.

7 Resolved Problems

The following list identifies problems that **have been resolved** in release 8.4.1.

Reference #	Subsystem	Description
12070	System	The display of tunnel MTU reflects the outbound interface's MTU less the needed header size of the tunnel.
12337	MLPPP	Juniper M Series router interoperability fix: LFI is auto-enabled on MLPPP bundles in the Juniper M Series and Secure Router doesn't expect LFI processed packets in an MLPPP bundle.
12492	RIP	RIPv1 port scan crash
12591	GRE	Tunnel flaps when only the default route exists in the routing table for the destination address
12621	CLI	The CLI prompt is not stored properly on rare occasions
12759	NAT	Port command in NAT is not stored in the system configuration file
12801	Syslog	Syslog with VPN debug enabled does not log full debug entries.
12809	System	'display-boot-config' option should not be stored in the system configuration file
12857	MLFR	System occasionally crashes when clearing LMI stats on a Multilink Frame Relay bundle when LMI is disabled ('no lmi').

The following list identifies problems that **have been resolved** in release 8.4.

Reference #	Subsystem	Description
10841	T1	Under extremely rare circumstances, unknown T1 errors cause T1 to go down temporarily.
12337	MLPPP LFI	When Juniper M40 is used to LFI auto-enabled, Juniper doesn't negotiate PPP header compression before transmitting certain packets.
11773	VLAN	VLAN Management MAC table doesn't timeout or refresh under certain circumstances.

The following list identifies problems that **have been resolved** in release 8.2.1.

Reference #	Subsystem	Description
10019	Platform	In rare occasions, a SR 1002/1004 router might register a negative environment temperature number and generate large number of event logs.

10184	Platform	In very rare cases, a 1200-7030 series router might not recover after a reset because of invalid model number recognition.
10321	DHCP Server	DHCP Server would not respond if certain DHCP relay requests are received.

The following list identifies problems that **have been resolved** in release 8.2.

Reference #	Subsystem	Description
8377	CLI	After creating 126 WAN interface bundles, the administrator could only partially create the 127th bundle and then system used to reject further configuration. With r8.2, the system provides message in time to the administrator and prevents the system from being partially configured.
8787	Firewall	Couldn't assign same public IP address for forward and reverse firewall policies.
9174	Web GUI	Outgoing byte counters for ESP are not updated in 'show firewall connections all.
9252	Ethernet	Runt/Bubble counters are not getting updated in the system.
9479	Platform (1001)	Interfaces used to go down when files were copied from system flash to compact flash.
9556	Web GUI	User cannot save the configuration over the Web GUI.
9556	Web GUI	The Web bundle display cannels does not show any channels in use when all 24 DS0s are allocated to it.
9568	Platform	Under certain circumstances, excessive T1 line errors on a single WAN interface bundle can cause the other bundles to go down.
9594	Web GUI	Web UI screen field values are not getting updated after deleting the T1 settings in the Web.
9597	Web GUI	When configuring remote access VPN under mode-config, incorrect validation of match-address is observed.
9615	Telco	Bit error counter under 'module test' shows negative number.
9619	Firewall	The administrator could not clear firewall counters in the previous release. A new CLI command was introduced 'clear firewall statistics' to resolve this.
9626	DHCPServer	When DHCP relay is configured within dhcp server and box is rebooted, the system may come up with errors.
9836	Telco	Command to remove loopback by executing "no loopback inward" used to fail.

The following list identifies problems that **have been resolved** in release 8.0.1:

Reference #	Subsystem	Description
7916	Telco	When remote line loopback is removed and BERT 0s/1s command is used, the system locks up temporarily for a few seconds.
8522	Ethernet	IXIA throughput tests sometimes yield errors on the Ethernet side of the 4100 (DS3) routers.
8628	System	System reboots under certain conditions and “taskmon low not active” message is stored in the event log.
8682	SNTP	SNTP gets incorrect hour value.
8799	System	Turning off the telnet or the ftp server and saving the config. file to default file causes the system to reboot after a system restart.
8945	CLI	User level 2 cannot execute the show config running command
8847	Telco	It is confusing which clock source is used in the case of ADM configuration, mostly a documentation issue. Clear explanation needed.
8972	Telco	When BERT test on unframed E1 is stopped, the link continues to stay in test mode and down for data traffic.
9162	Platform	False temperature error on SR 1002 and 1004 platform caused by problem on communications bus.
9583	BGP4	6200 reboots with 5 bridge customer setup
9643	Bundle	Task: 0x8c28a640 "tcli0" when link is unconfigured form the mlppp or for the mfr bundle.
9160	CLI	TelnetClientCliMainFunction: TELNET_CLIENT_ERROR' error message is displayed when telnet command is executed
9294	CLI	prompt/file> invalidate_boot Cmd is missing for 1400,4100,6200,6300 and 7030. Added the invalidate_boot command for 1400,4100,6200,6300 and 7030.
9274	Firewall	Create a dmz map on firewall and change the default max-connections for dmz to say 2000. Save local and reboot the box, the configuration is not restored back.
9370	FireWall	Stealth mode is not able to configure for "self"
9444	FireWall	TCP Sequence No. range in Firewall goes out of range quite fast
9371	FireWall	Firewall debug messages could not be seen in Syslog
9463	FireWall	No of active connections in show firewall connections & in show firewall policy detail are not matching when connection rate is set.

9417	Firewall	"no debug disable-firewall" is not working after creating a firewall map. Shows the message "Error in disabling access policy by pass firewall feature on this box is enabled".
9418	Firewall	Improper error messages displayed in firewall when max number of schedule and address objects are reached.
9174	Firewall	Outgoing byte counters for ESP packets do not get updated in "show firewall connections all"
9623	Firewall	When the RTSP Alg kicks in, it causes a buffer leak in the firewall module
9655	Firewall	TCP reset generated by the firewall is not going back to originator when VPN is not used
9173	GRE	Ping executed for an IP address (in the tunnel's subnet) not present and debug enabled shows debug information indefinitely.
9387	GRE	Does not drop a packet with Routing present bit in the GRE header but ignores it
9194	IPSec	Configuration saving in a specific scenario can differ. If a default policy (Ex: 1024) is modified for the number of max connections the router can handle it is not getting saved. If the number of connections is the same as the number of max connections of the given map (or snet). This bug is valid if the snet defaults. Otherwise, policy always inherits the snet defaults and hence, the bug is irrelevant.
9657	IPSec	Mempartfree occurs SR 1002 and 1004 when 2 IKE SAs are present for the same policy and "clear crypto IKE sa all" command is executed.
9638	QoS	The router will not allow enabling of policing on Ethernet interface. Giving invalid error message for valid operation.
9061	TCLSH	"tclsh" command has a memory leak of 466KB and system runs out of memory if tclsh executed too many times.
9678	VLAN	Un-configuring the sub-interface in IPMUX mode will hang / crash the box in a particular scenario
9428	VPN	GRE keepalives is not working properly with IPSec protection
9175	VPN	Site-to-Site VPN between two sites has problems as the box one site side hangs frequently
9293	VPN	TCP Reset sent over a VPN Tunnel from built in firewall causes box to reboot.

8 Known Issues, Limitations & Guidelines

This section details known Issues, limitations, and Guidelines for version 8.4.2 software. For further information on specific issues, contact Nortel Technical Support.

Known Issues

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
Q01299080	BGP	Secure router crashes while trying to update the downstream BGP peer with several thousand routes learned from an upstream BGP peer
Q01300037	QoS	Class Based Queuing or Shaping not available on Ethernet interfaces
Q01298874	IP Multicast	Secure router crashes after the sender stops sending traffic momentarily in a high throughput Multicast traffic environment
Q01299086	BGP	Secure router crashes when BGP is deleted dynamically while a peer connection exists
Q01307112	MLPPP	Unable to ping with sizes over 1500 bytes between Secure Router and Nortel Multi Protocol Router over a MLPPP connection
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 Multiclass Extensions to Multi Link PPP
Q01299998	QoS	DSCP markings for the Router Generated packets are not Compliant with Nortel Networks Service Class definitions
Q01300001	Frame Relay	Unable to configure FRF.12 over single Frame Relay Links
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

Q01314575	MLPPP	Secure router ignores LCP config rejects for certain options from the peer during a MLPPP negotiation
7530	System	Passing 44.21 Mbps traffic with 64 bytes packet size over FR or PPP DS3 Bundle causes the bundle to go down after an extended period of time. Larger byte size data or mixed data packet sizes do not exhibit this issue
7566	Drop & Insert	Voice quality is poor with non-contiguous channels configured on the PBX port. Configuring contiguous channels resolves this issue
7874	System	On a 6200, when 1-8 T1's are in use (LED status green), and T1's 9-16 are "no enabled" the WAN status LEDs on both IC's are green, the summary LED is remains red
7804	VPN	In site-to-site VPN, clearing an IKE SA by the specific policy name does not send a delete notification to the peer. However, it clears the local IKE SA. Workaround is to clear all the IKE SAs in the router.
8402	VPN	In mode configuration based VPN remote access, clearing the IPSec SA by the specific policy name does not clear it. The workaround is to clear all the IPSec SAs on the router.
8850	GRE	RIP routes are not established through the GRE Tunnel. Work around is to configure the tunnel IP address and the tunnel source addresses to the same address.
8929	IP Multicast	PIM generates a misleading Syslog gated error message. This is an erroneous message.
9102	GRE	Crypto command does not get removed from tunnel after the tunnel is removed from the firewall configuration. Deleting the crypto command from the tunnel interface configuration works around this issue.
9145	GRE	A tunnel is not reducing the length of packet after discovering the Path-MTU. Disabling path MTU in this scenario will fragment packets and workaround this issue.
9239	IP Multicast	Multicast protocols (IGMP, PIM-SM or PIM-SSM) not supported on unnumbered interfaces.
9240	IP Multicast	PIM-SM cannot operate in static RP and BSR mode simultaneously (i.e. if static RP is configured for router then all BSR messages will be ignored).
9241	IP Multicast	Static routes with interface name rather than a gateway IP address are not supported with Multicast protocols in this release.
9243	QoS	Policing is not supported for outbound traffic on Ethernet interfaces.
9244	QoS	Multi-level policing currently not supported. Policing is done only for leaf classes. Any policing configuration on non-leaf classes is ignored.
----	QoS	CR and BR must be specified when adding a new outbound class for policing, even though they are CBQ parameters they are required.
9376	1001 Compact Flash	Removing the compact flash when ‘file ls’ or ‘dir’ file listing commands are in progress can cause the system to become unstable.

9377	1001 Compact Flash	At boot prompt, when using the boot command to format the flash, if the compact flash is ejected, the system can become unusable.
9895 (9876)	1001 Platform	1001 router has been observed to be rather slow during either system flash or compact flash operations. Copying an image from removable compact flash to system flash can take up to 30 minutes.
9920	Firewall	Enabling MIME flood protection by-passes URL key filter.

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 Platform	It is strongly recommended that when the removable compact flash is in operation, e.g. file listing/copying/deleting etc., do not eject the flash card. Ejecting the compact flash can render the system console unusable and may also corrupt the system or compact 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.
VPN / Firewall	When the SR 1002 & 1004 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.
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	R8.2 is verified to support up to 500 Firewall policies, 250 AAA lists and 750 ACLs.
GRE	Only IPv4 is supported as the passenger protocol for GRE.
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 they are required.

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.

9 How to Get Support

Accessing Technical Assistance

If a service contract has been purchased with this Nortel product from a distributor or authorized reseller, contact the technical support for that distributor or reseller for technical assistance.

If a Nortel service program was purchased with this product, contact Nortel Technical Support for technical assistance. To obtain contact information for Nortel Technical Support, go to http://www.nortel.com/support and click the **Contact Technical Support** link found on the left-hand side of the page. From this page a Customer Service Request can be initiated online or the phone number of the nearest Technical Solutions Center can be obtained. If Internet access is not readily available, call 1-800-4NORTEL (1-800-466-7835) to obtain the telephone number of the nearest Technical Solutions Center.

An Express Routing Code (ERC) is available for many Nortel products. When used, an ERC allows a technical assistance call to be routed to a technical support representative who specializes in that product. To locate product Express Routing Codes, go to http://www.nortel.com/erc.