Version 8.3.5

Part No. 322001-B
May 2006

600 Technology Park Drive
Billerica, MA 08121-4130

Secure Router 1001/1001S Release Notes

Copyright © 2006 Nortel Networks. All rights reserved.

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 Inc.

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 Networks, the Nortel Networks logo, Secure Router and Contivity are trademarks of Nortel Networks.
Adobe and Acrobat Reader are trademarks of Adobe Systems Incorporated.
America Online and AOL are trademarks of America Online, Inc.
iPlanet, Java, and Sun Microsystems are trademarks of Sun Microsystems.
Microsoft, Windows, and Windows NT are trademarks of Microsoft Corporation.
Netscape, Netscape Communicator, Netscape Directory Server, and Netscape Navigator are trademarks of Netscape
Communications Corporation.
Steel-Belted Radius is a trademark of Funk Software, Inc.
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 Inc. reserves the right to make changes to the products described in this document without notice. Nortel Networks Inc. 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 Inc. 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 Networks 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 Networks 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 Networks 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 Networks 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 NETWORKS 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 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 8.3.5 release is for general use and is supported on the Secure Router 1001 platform only. The 8.3.5 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.

2 New Features

2.1 8.3 Features

2.1.1 E1 Support for SR 1001

8.3 adds E1 support on SR 1001 product line. All SR1001 products that ship with 8.3 (and higher) will have the software selectable T1/E1 port option. The SR 1001 hardware supports both T1 and E1 signaling. This is unlike 1002 and 1004 products where T1 and E1 routers are manufactured and ordered separately. Hence, the software selectable option will only work on the SR 1001 product. The customer can use one CLI command to convert the T1 port into an E1 port. The procedure to convert T1 to E1 is as follows:

Step 1: configure the ‘carrier-type’ of the port to convert from T1(default) to E1

```
Host> configure term
Host/configure> module t1 1
Host/configure/module/t1 1> carrier-type e1
```

Step 2: Reboot the system

```
Host> configure/module/t1 1> [Ctrl-Z]
Host> reload
```

The procedure is the same to convert an E1 port into a T1 port. If you have a system configuration file that expected a particular port type, after the port change and system reboot, port specific commands will fail. So it is important to first rename the existing system.cfg configuration file into another file, say ‘sysold.cfg’. Transfer the file into an editable system (e.g. Windows System with Notepad), and then either cut-paste the configuration within the ‘Host/configure>’ mode or TFTP the new configuration file into the system and execute ‘Host> configure flash’ or save the file as system.cfg and then reboot again.

2.1.2 ISDN BRI Backup Interface

With the 8.3 release, the optional ‘backup’ port on the 1001 can be ordered to support ISDN-BRI-ST interface or an ISDN-BRI-U interface. This option can only be chosen when ordering for the first time and is not field-upgradeable. Only 1001s with 8.3.5 or higher can be ordered to be shipped with the optional ISDN backup option.

8.3 is a largely controlled release of the ISDN interface with some limitations as described in the itemized list below. Care should be taken when selecting ISDN deployments by filtering the customer requirements with the feature availability.

When the primary connectivity (T1/E1) links go down, ISDN can be used as a secondary connection. ISDN can be used as dial up connection to connect to Internet or remote server for certain amount of time until the primary T1/E1 links are restored. ISDN is a good solution for the small or medium size businesses that want to connect their Local Area Network to the Internet with an ISDN router.

The ISDN backup port is designed to work in a “primary”-“backup” environment where the primary link can be a T1 or an E1 interface. The backup ISDN interface will become active and dial and establish a connection when the primary T1/E1 interface fails due to either a ‘physical link failure’ or a ‘logical routing protocol peer failure’.

ISDN interface is created as an IP interface with a low priority default route. The primary interface’s default route has higher priority and hence, the low priority route is never installed in the routing forwarding table as long as the primary interface’s default route is active. When for any reason the primary’s default route is pulled out of the routing table (physical link failure or dynamic routing peer non-response), the ISDN interface’s routing entry becomes active and the ISDN interface then dials the number pre-configured in the CLI.

When the primary link recovers and the primary route is re-added into the forwarding table, all data traffic is automatically diverted back to the primary. This causes an idle timer to start on the ISDN interface as there is no more traffic flowing through the ISDN interface. The ISDN interface disconnects the call after a certain idle timeout. This idle timeout parameter is configurable on the CLI.

Currently supported Features:

- ISDN BRI Option
  - S/T Interface
  - U Interface

  These are two separate hardware configurations and hence correct part-number must be used when ordering. ISDN option is only available as factory-installed; field upgradeability of existing 1001 routers is not possible.

- ISDN Switch variants

basic-ni (default)	- National ISDN switch type
basic-dms	- NT DMS-100 switch type
basic-5ess	- AT&T basic rate switch type
basic-1tr6	- German 1tr6 switch type
ntt	- NTT (Japan) switch type
vn3	- French VN3 switch type
basic-etsi	- ETSI (**EuroISDN**) switch type
basic-ccitt	- CCITT (worldwide) switch type

  Note: After changing switch-type in the CLI, a system reboot is necessary for the change to take effect.

- Bandwidth
  - 64Kbps
  - 128Kbps

Note: ISDN Interface bandwidth is statically configured for either 64 or 128Kbps connectivity. The 128Kbps connectivity is supported using MLPPP protocol. Dynamic bandwidth on demand (BAP/BACP) is planned for a future release.

- Connectivity
  - Point to Point

  Note: Point to Multipoint ISDN connectivity is planned for a future release.

- Authentication Options
  - PAP
  - CHAP
  - None

- Layer 2 Encapsulation
  - PPP (for 64Kbps)
  - MLPPP (for 128Kbps)

- Layer 3
  - IP

  Note: The ISDN interface must be IP configured. VLAN forwarding over ISDN interface is not available in this release.

- Dial on Demand
  - To dial out using the backup ISDN-BRI interface, the primary interface failure is first detected. Once the ISDN-BRI interface is up and running, there is an idle timeout available that disconnects the line when no traffic is observed for a user-configurable duration. The call is re-established when data traffic is detected on the ISDN interface and the timer is reset.

- ISDN as backup Interface
  - Supported. As described above. Physical failures and logical layer 3 failures related to dynamic route peer connectivity loss will be detected and ISDN backup interface will be activated.

  Note: If no dynamic routing is configured on the primary interface, then logical primary link failures cannot be detected.

- ISDN as the only Interface (ISDN as primary interface)
  - This is supported where the T1/E1 port is not used.

- Other Layer 3 applications
  - IPSec VPN and Stateful Inspection FW supported (NAT based on FW is supported)
  - ACL (Packet Filters) supported
  - QoS over ISDN is not supported in this release.
  - VLAN based forwarding not supported over ISDN interfaces
  - IPMUX mode not supported on the 1001 platform.

- Configuration
  - CLI

  Note: GUI and SNMP configuration/status for ISDN is not supported in this release.

This is the first controlled release of the feature to accommodate customer acceptance cycle and proceed with a comprehensive GA in the next release.

2.1.3 PPPoE Support for SR 1001

8.3 provides PPPoE software support to help connect the on-board Ethernet ports to external DSL modems to provide DSL connectivity to the router. The main purpose of this feature on the Tasman Opal Jr is a back-up/fail-over solution.
When the primary connectivity goes down, traffic will switchover to the back up interface, in this case a virtual PPPoE interface. A PPPoE client session will get established with a PPPoE server and traffic will be routed through this path until the primary connectivity is restored.

The following features and limitations exist in this first release of PPPoE.

- Connectivity
  - Primary
    - Can be used to make the Ethernet port connected to an external DSL modem as the primary WAN connectivity (and not use the T1/E1 port).
  - Backup
    - The T1/E1 port can be used as a primary interface while the PPPoE interface (over an existing Ethernet interface) can be used as the backup/failover link when the primary fails. The primary failure could be due to physical link issues or a logical layer 3 routing peer failure.

    Note: If a default static route is used for the primary link, logical layer 3 failures of the primary (remote layer 3 dead) cannot be detected and switch over to DSL may not happen.

  Note: In this release, the PPPoE interface cannot be used as a load balancing interface where the primary and the PPPoE interface are active at the same time and load balancing the outbound traffic.

- Security
  - PAP
  - CHAP
  - Either
  - None

- PPPoE Client Software only
  - This software release is for the PPPoE client to connect to an external DSL modem to either learn its IP address or use the configured IP address to communicate with the DSL aggregation device.

- Keepalive supported to monitor the status of the peer.

- Access Concentrator can be specified to pick a particular PPPoE server

- Only one PPPoE client per Ethernet Interface will be supported. There is no PPPoE support over logical IP/VLAN sub-interfaces.

- Management

  - CLI

  Note: SNMP and GUI support for PPPoE is not available in this release.

- PPPoE assumes that the netmask for IP address to be 32bits wide when the address is supplied by the remote PPPoE Server.

- PPPoE virtual interface will be automatically configured with Stateful Firewall and put in the 'Internet' Zone. To activate data traffic, the local interface (the other Ethernet port in most cases) must be configured as a trusted interface in the firewall configuration.
- Other Features supported on PPPoE Interface
  - Stateful FW (and Firewall NAT) are supported in this release
- Features not Supported over PPPoE virtual interface in this release
  - The two Ethernet ports cannot be connected to two external DSL modems (using PPPoE) for load sharing. Only one active PPPoE session will be available for data transfer.
  - Dynamic unicast and Multicast routing protocols are not supported on PPPoE interface in this release. Only static routes can be configured on this interface.
  - IPSec Tunneling over PPPoE is not supported in this release.
  - QoS, ACL and VLAN (tag/forward) over PPPoE interfaces are not supported in this release
  - IPMUX And VLAN forward/tag mode not supported

2.2 8.3.5 Features

- **ISDN BRI Point to Multipoint**
  - On an ISDN BRI interface, as many as eight devices can be attached to a single line. Note: Though there could be up to eight devices connected to the ISDN line, at any given time a maximum of only 2 calls can be active). The ISDN network identifies each of these devices uniquely with the help of an address called a Terminal Endpoint Identifier or TEI (Note: This address is not the telephone number).

  - The addresses of the device may be pre-configured or dynamically allocated.

  - In **dynamic addressing**, each device has to request an address from the network before it can perform any signaling activity. The value range of the TEI which will be assigned by the network, as specified by the standards, is from 64 to 126. This topology of connecting multiple devices on a single ISDN line is also known as **point-to-multipoint.**

  - With **fixed addressing**, the address of each device has to be configured to match the addresses pre-configured for that line. TEI values in this case can be anywhere from 0 to 63. This topology of only having a single device connected is known as **point-to-point.**

  - The Nortel Secure Router 1001/1001S with S/T interface can be connected as one of the TEs on to the passive S/T bus. And using the answer1 and answer2 configuration, the user can configure the box to answer calls coming only to these numbers.

- **QoS/RED over ISDN interface**
  - QoS is now available over ISDN interface also.

- **VLAN Encapsulation over GRE**

  - Enables transport of Ethernet over IP
  - Combines Nortel VLAN Forwarding with GRE
  - Provides protection using standard IPSec
  - Can interconnect remote-sites using
    - 802.1Q Tagged frames
    - Untagged Ethernet II frames

    - Supported
        - Jumbo frame (4K)
        - VLAN tagging & forwarding
        - VLAN Management
        - GRE
            - IP Fragmentation
            - Tunnel protection using IPSec
            - 100 tunnels
        - Point to Multipoint
        -
    - Not supported
        - Outbound QoS using inner IP flow
- Re-branding from Tasman to Nortel SR 1001/1001S
- Introduction of the Secure Router 1001S
    - 1 port universal serial V.35, DCE/DTE
    - 2 integrated 10/100 auto-sensing Ethernet ports
    - Dedicated management console
        - 1xRJ-45 console
        - External compact flash support
    - VPN SafeNet Chip
    - ISDN BRI Back-up available

3 Supported Features from Previous Release

The 8.3.5 release is based on the 8.3. The subsequent features from this branch have been merged with 8.3.5.

4 Memory Requirements

The SR 1001/1001S has a fixed memory. It consists of 16MB of flash memory and 128MB of DRAM.

5 Software Deliverables

The Nortel Secure Router 8.3.5 release is supported on the Nortel Secure Router 1001 and 1001S. The software is located on the CD and on the Nortel support site.

SR 1001/1001S Routers

Description	File Size	Version	File Name
SR 1001 Series Application image	9295313	8.3.5 (r8.3.5)	J1100.Z
SR 1001 Series Field Upgradeable BootROM image	373984	8.3.5 (J1100_031805)	T1001_r8_3.bin
SR 1001 Series MIBs	78791	8.3.5	Mibs.zip

NOTE: All existing SR 1001 units must upgrade to the new BootROM images to run r7.0.2 or later software. All new SR 1001/1001S units will be shipped with both the updated EPROM and with the downloadable BootROM image.

NOTE: Files ending with ".Z" are Boot ROM images; Files ending with ".bin" is the executable image.

SNMP MIBs

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

6 Resolved Problems

This chapter describes issues and considerations that apply to version 8.3.5 release of the Secure Router 1001/1001S.

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.

Customer issued fixed in this release

Reference #	Description
12735	During interoperation testing with Juniper M-40 series, PPP drops the frames for certain classes of traffic.
10932	The crypto type configured as trusted for PPPoE interface is not retained after save and reboot
11988	Ethernet hangs with large number of collisions
12110	Destination-based NAT
12269	Management command needs to be added in VLAN-GRE.
12213	Call fails on SBC NI1 BRI U interface
11844	Scheduled Reload
10968	If traffic is not passed through PPPoE interface for a while then, PPPoE session has to come down automatically.
11167	Task: 0x86556c60 rxpoll crash in PPPoE client when following parameters are unconfigured in pppoe server
10634	PPPoE session comes down when a sub-interface is configured for the ethernet interface over which PPPoE is configured.
10974	Task: 0x83f6ec90 "want" crash while clearing the pppoe session continuously from sever side
10966	Configuring pppoe authentication method as PAP-CHAP, the authentication method works for none also
10972	PPPoE Debug IN message display incorrect debug information
10986	Debug message for pppoe control packet (PADO packet) displays incorrect destination MAC address
11194	PPPoE client does not send PADT packet to Access concentrator, in the following test scenarios.
11195	The Debug PPPoE events and PPPoE packets can still be displayed in the following test scenario.
11232	PPPoE session get established, when Auth protocol configured as chap in pppoe client and ms-chap in pppoe server
11233	Task: 0x83f71d90 wan2 crash when wrong chap auth protocol is configured, with max string for username and password.

12004	In a particular scenario packets are dropped by QoS scheduler even though the Average Inbound rate is less than CR.
12007	Policing rate can be configured to be more than wire bandwidth on a MLPPP bundle in a particular scenario.
12009	In a particular scenario buffer pool counters indicates negative value
11957	In DCE Mode Can not Set Clock Rate above 2000000
11958	Show mod conf all there are no serial shown.
11810	Value of Mib 'ifSpeed' for bundle intf for bundle configured using serial link displayed incorrectly as 48000000
11772	Method to authenticate the user login process is represented by wrong octets for the mib 'snAuthenticationLoginMethod'
11300	cable type command is missing in SR 1002/1004 E boxes.
12328	BPV Counters none-Functional

7 Known Issues, Limitations, & Guidelines

Reference #	Subsystem	Description
Q01299095	BGP	Secure Router crashes while trying to save the local configuration in a Multi Hop BGP configuration environment
Q01375334	BGP	Secure Router crashes when BGP aggregate summary and PIM are configured
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

Reference #	**Description**
12068	LMI parameters values are getting retained even when Interface type or LMI type is changed
12403	Individual PVC flap when traffic is sent at more than wire speed in FR bundle configured on serial links.
12330	rxPoll crash seen in PPP bundles on serial links when mru is set to boundary values
12592	PAP/CHAP parameters are retained when encapsulation of the bundle is removed by deletion of links of the bundle
12131	eBGP and iBGP sessions are getting established even though the router-id is same in both the peer.
12306	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	Disabling and enabling RED feature on a bcp bundle stops transmitting traffic(able to receive traffic)
12405	Box not bootable from image in the Compact Flash -- Often Reproducible
12430	DHCP Server is not getting unconfigured using command "no ip dhcp" if the remote database is not reachable in a particular scenario.
12485	DHCP Server assigns ip-address to dhcp-client which is being used by some other host in the network in a particular scenario.
12620	With per_flow IP load balancing, it does not distribute the traffic flows among all PVCs in FR bundles.
12490	TAIS and TRAI alarm traps are not shown in SR1001.
12640	After shutting down an ethernet interface and enabling VRRP in the same, the state changes to MASTER and tries to send VRRP
12657	VRRP WAN interface tracking does not detect the change when the WAN interface is deleted.

8 General Guidelines and Considers

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.