# Secure Router 1001,1001S, 1002, 1004, and 3120

## Software Release 9.3.3
## Readme Notes

## 1. Release Summary

Release Date: 11-Nov-2008
Purpose: Software maintenance release to address customer found software issues.

## 2. Important Notes before Upgrading to This Release

For Secure Router customers who are upgrading to v9.3.3 from a Secure Router version earlier than v9.3.0, it is highly recommended to refer to the v9.2.0 and v9.3.0 release notes for details on upgrading, converting units running Tasman branded code, and changes to the default settings. The Secure Router 1000/3120 v9.2.0 release notes can be found here:

v9.2.0 Release Notes:
http://www130.nortelnetworks.com/go/main.jsp?cscat=DOCDETAIL&DocumentOID=523853&RenditionID=REND832949&poid=15961

v9.3.0 Release Notes:
https://support.nortel.com/go/main.jsp?cscat=DOCDETAIL&id=681775&poid=15961

For users upgrading to v9.3.3 from a release earlier than v9.2.0, it is recommended that you install the v9.3.1 software upgrade through the console port since telnet, SNMP agent and WebUI enabled settings are not retained during the upgrade process. Starting with v9.2.0, the default settings for telnet and WebUI are now specifically disabled. Another option would be to enable SSH and save the configuration prior to the upgrade. Once the router has been upgraded to v9.2.0 or higher, users must explicitly enable these settings and save the configuration. Please refer to the v9.2.0 release notes for additional details.

Note: **IMPORTANT -** If your Secure Router unit is configured for RADIUS or TACACS Service, you must follow these upgrade procedures when upgrading from an earlier release to v9.3.1.

To make the handling of RADIUS and TACACS work properly when changing the shared key it requires that the RADIUS/TACACS are disabled when setting it. In the previous release the enabling aaa facility came prior to the RADIUS settings. Under the r9.2.6 release the AAA service enable command is stored after both the TACACS and RADIUS sections to insure that the service is disable prior to setting the key.

1)Before loading the v9.3.3 release you must enter the following commands

```
configure terminal
aaa
no enable
save local
```

2)Boot the v9.3.3 release. Enter the following commands:

```
configure terminal
aaa
```

```
enable
save local
```

Stored configuration is saved in the proper order.

### BGP Upgrade for SR 3120

Prior to upgrading to Release r9.3.3 (from 9.3 or earlier release) check that the each of your BGP peers does not send more than 5K prefixes. If so set the maximum_prefix parameter under the BGP peer section to the proper amount and store the configuration prior to upgrading.

## 3. Platforms Supported

Nortel Secure Router 3120
Nortel Secure Router 1001
Nortel Secure Router 1001S
Nortel Secure Router 1002
Nortel Secure Router 1004

## 4. Notes for Upgrade

Please see the technical documentation for the Secure Router 1000 and 3120 version 9.3 available at: http://www.nortel.com/support for details on how to upgrade your Secure Router unit.

**File Names for This Release**

| Description | File Size | Version | File Name |
|---|---|---|---|
| Secure Router 3120 Application Image | 9484497 | r9.3.3 | H1000.Z |
| Secure Router 1002/1004 | 8799726 | r9.3.3 | T1000.Z |
| Secure Router 1001 | 9492841 | r9.3.3 | J1100.Z |
| Secure Router 1001S | 9946386 | r9.3.3 | JP1010.Z |

## 5. Version of Previous Release

Software Version 9.3.2

## 6. Compatibility

N/A

# 7. New Features in the 9.3.3 Release

## 7. 1 Multicast over GRE

### Multicast Routing Support for GRE Tunnels

The Multicast Routing protocol (PIM-SM) support over GRE tunnels has been added to the secure routers. Typically, multicast routing protocol control traffic and multicast data traffic will be sent over GRE tunnels when there has to be a data exchange between two multicast enabled routers that are separated by a IP cloud which does not have multicast capabilities. In such scenarios, ability to configure PIM over GRE tunnels helps in transporting multicast packets (both control and data) across a non-Multicast aware IP cloud.

**Configuration Guide:**

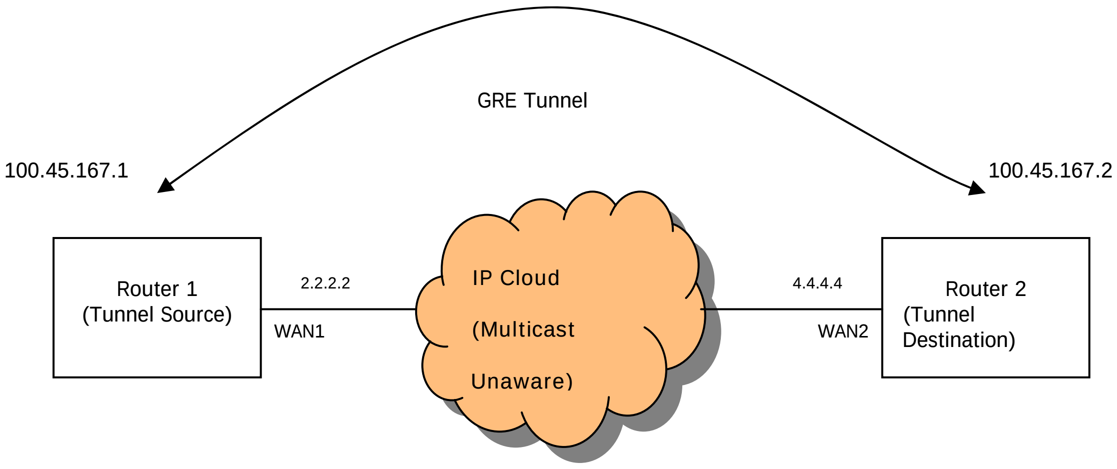
When configuring PIM over GRE tunnels the following points need to be adhered.

1. When PIM is to be run over GRE tunnels, the GRE tunnels are to be configured with tunnel IP addresses at both the tunnel end-points should be configured in the same subnet. Also, it is mandatory to ensure the reachability to the tunnel destination either via IGP or static route.

2. When configuring PIM over GRE tunnels (Tunnel source configured same as the IP address of the tunnel) configuring the tunnel interface as the CBSR or CRP is not allowed, as the RPF check will fail at the tunnel end point routers (as result of having the 32-bit static route to the tunnel destination).

3. If the BSR/ RP/ Multicast Source networks reside on the other side of the tunnel, the reachability towards the BSR/ RP/ Multicast Source *should be* ensured with the next-hop as tunnel's other end, either by IGP or static routes.

The following snapshots illustrate an example configuration:



Nortel Secure Router 1000/3120 version 9.3.2

Below is the sample configuration.

**Snapshot at Router 1:**

```
Router 1/configure> interface tunnel t1
Router 1/configure/interface t1> ip address 100.45.167.1 255.255.255.0
Router 1/configure/interface t1> tunnel source 2.2.2.2
Router 1/configure/interface t1> tunnel destination 4.4.4.4
Router 1/configure/interface t1> exit tunnel


Router 2/configure> interface tunnel t2
Router 2/configure/interface t2> ip address 100.45.167.2 255.255.255.0
Router 2/configure/interface t2> tunnel source 4.4.4.4
Router 2/configure/interface t2> tunnel destination 2.2.2.2
Router 2/configure/interface t2> exit tunnel
```

There are no new CLI commands added for the purpose of supporting multicast over GRE tunnels. The PIM related configurations have the same syntax as they do for Ethernet or WAN interfaces.

## 7.2 VPN-Only Mode

Earlier releases of Secure Router products required that firewall to be configured to use the IPSec VPN features. This release overcomes the limitation and introduces VPN-Only mode. Enabling this mode would allow the traffic to skip firewall related checks and IPSec services would be provided based on the policies configured.

To switch to VPN-Only mode, it requires the router to be rebooted to take effect. After the router is rebooted in VPN-Only mode all the commands under the firewall section will not exist.

### CLI

To Display IPSec VPN configuration without Firewall

```
    Host > show system security
```

### Conversion procedure to VPN-Only Mode

```
Host> file
Host/file > copy system.cfg firewall.cfg
 Host/file > exit
Host> conf t
Host/configure > system security firewall-disable
Host/configure> write mem
Host/configure> exit
Host> reboot
```

### Converting back procedure to Firewall Mode

```
Host> file
Host/file > copy system.cfg vpnonly.cfg
Host/file > copy firewall.cfg system.cfg
Host/file > exit
Host> conf t
Host/configure > no system security firewall-disable
Host/configure> exit
Host> reboot
```

## 7.3 Problems Resolved in the 9.3.3 Release

| Bug Reference | Subsystem | Description |
|---|---|---|
| Q01773908 | VRRP | VRRP tracking of an Ethernet interface was not working properly |
| Q01811646 | PIM-SM | Assertion failed gated[-2042573744]: file "pimsm_sg_assert.c", line 957: ". This assertion shows up when the connectivity to the peer BSR is lost abruptly. |
| Q01823264 | PIM-SM | tGateDTask crashes – Pump multicast traffic across ethernet interface to wan; modifying the IP-Address of ethernet interface results in tGateDTask crash. This crash is intermittent in nature |
| Q01872419-01 | SNMP | ifInOctets, ifOutOctets, ifInUcastPkts, ifOutUcastPkts MIB objects not updated for Tunnel, PPPoE interfaces |
| Q01893980 | PIM-SM | PIM Assert - Assertion failed gated[-1940797664]: file "pimsm_jpxmit.c", line 727: "0". Observed when doing multicast and ospf routing failover. This crash is intermittent in nature and no specific sequence associated with it. |
| Q01904190 | PPP | SR3120 serial links do not retry PPP after T1 outage |
| Q01906180 | Routing | A change in the routing table (RIB) does not produce the change in the route cache and causes the packets to be routed in the wrong direction. |
| Q01909753 | Routing | tGateDTask crash in rt_change_aspath_ieng. Observed when there is a spurt of external LSA (Type 5) received on the box. Notes: This issue seen only when external LSAs are flooded by the remote peer. |
| Q01910382 | RIP | RIP Packets sent by the remote are not being accepted by Secure Router 3120. This issue crops up intermittently when T1 connection goes down and up. |
| Q01911292 | Multicast | tGateDTask crash in MulticastTimer pimsm_sg_ppending_job. Observed when the source mask length received in the JOIN message is *not* 32. |
| Q01912461 | PIM-SM | Assertion failed gated[tGateDTask] pimsm_sg_assert.c", line 963 |
| Q01912466 | OSPF | tGateDTask crash in ospf_spf_external. Observed when there is a spurt of external LSA (Type 5) received on the box. |
| Q01915093 | VLAN | Adding Vldid to fwd table on newly created BCP bundle does not save to configuration if the bundle has not come up prior to saving the configuration |
| Q01917083 | IGMP-SNOOPING | IGMP Snooping - Forward all IP Multicast Traffic to "**mrouter**" port regardless of any IGMP JOIN registration on the port. |
| Q01918535 | PIM-SM | Assertion "pimsm_utils.c", line 976. |
| Q01921848 | SSH | SSH does not timeout unauthenticated users |
| Q01922216 | SSH | Error message displayed on console (memPartFree: invalid block) after invalid login attempt |
| Q01922302 | SNMP | SNMP trap message length greater than 255 bytes gets corrupted |
| Q01925553 | Routing | An infrequent crash when receiving a route update |
| Q01926182 | PIM-SM | tGateDTask "assertion pimsm.c, line 6244" |
| Q01927573 | HDLC | HDLC bundle with release after r9.3 are not compatiable with release prior to r9.3 and the bundle will not come up |
| Q01930592 | CLI | CLI crash occurs with the command "show ip mroute pim-sm gp X gmask 255.255.25.0" |
| Q01930611 | PIM-SM | PIM-SM Assertion failed in a particular scenario. Observed when route to RP gets changed. |
| Q01936123 | DHCP | Unable to remove dhcp-client retry interval from config |

## 8. Outstanding Issues

Refer to the Secure Router 1000/3120 version 9.3.0, 9.3.1, 9.3.2 Release notes

## 9. Known Limitations

Refer to the Secure Router 1000/3120 version 9.3.0, 9.3.1, 9.3.2 Release notes
SNMP SET operations are not supported
OSPF – P2P network type over Ethernet interface (broadcast) is not supported.
An interface name of “0” and “1” are reserved for the Ethernets and should not be used on any other types of interfaces.
When connecting to SR1002/1004 router console port set the terminal to flow control as NONE

## 10. Documentation Corrections

The pin out RJ45 console port are as follows:

Pin 1: RTS
Pin 2: DTR
Pin 3: TD
Pin 4: GROUND
Pin 5: GROUND
Pin 6: RD
Pin 7: DSR
Pin 8: CTS

When connecting to console port set the terminal to flow control as NONE.

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.

To access more technical documentation, search our knowledge base, or open a service request online, please visit Nortel Technical Support on the web at: http://www.nortel.com/support