NORTEL

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

Software Release 9.2.6
Readme Notes

1. Release Summary

Release Date: 4-January -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 v9.2.6 from a Secure Router version earlier than v9.2.0, it is highly recommended to refer to the v9.2.0 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:

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

For users upgrading to v9.2.6 from a release earlier than v9.2.0, it is recommended that you install the v9.2.6 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 v9.2.6.

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 v9.2.6 release you must enter the following commands

```
configure t
aaa
no enable
save local
```

2)Boot the v9.2.6 release. Enter the following commands:

```
Configure t
aaa
enable
save local
```

Stored configuration is saved in the proper order.

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 9.2 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	9,305,731	‘r9.2.6’	H1000.Z
Secure Router 1002/1004	8,555,355	‘r9.2.6’	T1000.Z
Secure Router 1001	9,676,633	‘r9.2.6’	J1100.Z
Secure Router 1001S	10,129,110	‘r9.2.6’	JP1010.Z

5. Version of Previous Release

Software Version 9.2.5

6. Compatibility

N/A

7. New Features in the 9.2.5 Release

N/A

Problems Resolved in the 9.2.6 Release

Bug Reference	Subsystem	Severity	Priority	Description
Q01612873	Frame Relay QOS	Broken Feature	P3	Frame Relay CBQ does not operate properly when frame size is larger than 1400. Also the DE bit was being set for all QOS classes after the committed Rate (CR) for their class was exhausted. This caused the upstream routers to drop the burst traffic for high priority classes.
Q01727508	OSPF	Broken Feature	P3	Received redistributed static route was not being added to the routing table even though it was added to the OSPF Link State Database.
Q01764968	OSPF	Crash	P1	OSPF was not handling an LSI update which contained multiple router LSAs to delete and would cause the router to reboot.
Q01767679	SSH Server	Crash	P1	In a peculiar scenario with 5 concurrent SSH sessions are running a ping the SSH server causes a crash.
Q01768453	TACACS	Broken Feature	P3	Tacacs does not support space in the shared key
Q01792195	SSH Server	Broken Feature	P2	SSH session is not terminating on the router if closed from client while a ping is executing.
Q01792201	Telnet Server	Crash	P1	In a peculiar scenario, the router would crash with 10 telnet sessions continually logging in and out over time.
Q01800762	SSH Server	Broken Feature	P3	Unable to establish an SSH session with public key authentication method when SSH Server is using a DSA key.
Q01805785	SSH Server	Broken Feature	P3	Unable to clear the SSH session when a user is executing a CLI command.

SSH Server Notes

The **generate** CLI command under the ssh-keygen command sub-tree has been changed. It no longer has the optional **passphrase** option. This was removed since a key generated with this option was unable to be used by the SSH Server after the router was rebooted.

DHCP Server Notes

IP Phone Support for Full mode with DHCP Server

The dhcp server has been changed to understand Nortel specific dhcp options used to configure Nortel IP Phones in Full mode. The ip phones when configured for full mode will make a dhcp discover broadcast on the network that they are attached to. The secure router will match it to the corresponding dhcp pool and return all the dhcp options configured for that dhcp pool. All the Nortel specific dhcp options are defined under the ip dhcps pool subtree.

The dhcp options 66 and 150 are configured by setting the tftpserver option under the dhcp pool. The option 66 will return the primary tftp server ip address (first entry) as a text field. The dhcp option 150 will return multiple tftp server ip address as a length encoded binary field where each address is 4 bytes.

The dhcp option 150 is defined by Cisco for the use of SIP phones so that they can have redundant backup for downloading the images on the SIP phones.

The cli commands are the following

```
configure
|-- ip
|    |-- dhcps
|    |    |-- pool
|    |    |    |- altvlan
|    |    |    |- call server
|    |    |    |- wireless
|    |    |    |- tftpserver
```

Configuration Commands

Name	Description
altvlan	**NAME** altvlan – Alternate vlan id for IP Phones **SYNTAX** R1/configure/ip/dhcps/pool x # altvlan vlanid <cr> **DESCRIPTION**. vlanid -- vlan id (enter a integer 0 - 65535) **NOTES** This command configures dhcp option 191 which configures the alternate vlan id that the IP phone is to use. This command will configure a dummy dhcp option 128 so that the IP phones accept this option.
callserver	**NAME** callserver – Call Server for IP Phones **SYNTAX** R1/configure/ip/dhcps/pool x # callserver ip1 port port_val appserver ip2 svpserver ip3 <cr>

Name	Description
	DESCRIPTION ip1 -- ip address of call server port -- parameter to configure the call server port number port_val -- port number that the call server is listening on range 1024 – 65535 (default 4100) appserver -- parameter to configure the XAS application server ip2 -- ip addres of the XAS application server svpserver -- SpectraLink Voice Priority (SVP) server ip3 -- ip address of the SVP server **NOTES** This command configure dhcp option 128. There can be up to 2 call servers per dhcp pool. The first call server entered is the primary call server. The svpserver option configures dhcp option 151.
wireless	**NAME** wireless – Wireless AP Series IP Phones **SYNTAX** R1/configure/ip/dhcps/pool x # **wireless** ip1 <cr> **DESCRIPTION** ip1 -- ip address wireless server **NOTES** This command can not be present with any of the other IP Phone options. The maximum number of wireless servers is 3. This option configures dhcp option 43.
tftpserver	**NAME** tftpserver – ip address of tftpserver **SYNTAX** R1/configure/ip/dhcps/pool x # **tftpserver** ip1 <cr> **DESCRIPTION** ip1 -- ip address tftp server **NOTES** The maximum number of tftp servers is 8. This option configures dhcp option 66 and option 150(multiple tftp severs).

8. Outstanding Issues

Refer to the Secure Router 1000/3120 version 9.2.0 Release notes

9. Known Limitations

Refer to the Secure Router 1000/3120 version 9.2.0 Release notes

10. Documentation Corrections

Earlier versions of the Secure Router 1000 and 3120 documentation set 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.

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