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

Software Release 9.2.5
Readme Notes

1. Release Summary

Release Date: 21-September-2007
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 v9.2.5 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 v9.2.5 from a release earlier than v9.2.0, it is recommended that you install the v9.2.5 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 v9.2.5.

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 r9.2.5 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 v9.2.5 release you must enter the following commands
```
configure t
aaa
no enable
save local
```
2)Boot the v9.2.5 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	9,304,863	'r9.2.5'	H1000.Z
Secure Router 1002/1004	8,555,366	'r9.2.5'	T1000.Z
Secure Router 1001	9,672,802	'r9.2.5'	J1100.Z
Secure Router 1001S	10,125,436	'r9.2.5'	JP1010.Z

5. Version of Previous Release

Software Version 9.2.4

6. Compatibility

N/A

7. New Features in the 9.2.5 Release

IP Filtering on VLAN Ethernet sub-interfaces

The same IP filtering rules that could be set on the Main Ethernet interface can now also be applied to any VLAN Ethernet sub-interface.

Increased the capacity of QOS over Ethernet

SR 3120, 1004 and 1002 have increase the QOS Buffering up to 50000 Kbs
SR 1001and SR1001S have increase the QOS Buffering up to 20000 Kbs

Bert tests able to run over configured bundles

Ability to run telco tests without deleting the bundle prior to running the telco tests. When entering a telco test, you will be prompt whether to continue if the wan interface is configured in a bundle. If you enter yes then the link will show that it is under test in the bundle display**.**

New parameter "smartjack" on the loopback command under test

This enables setting the remote smart jack device into loopback mode or not.

test t1 x > [no] loopback remote smartjack

New parameter "defaults" under the enable-all command under firewall algs

The r9.2.5 release selected algs are disabled by default (see Firewall ALG Notes section of this document). This new option "defaults" restores the firewall to the set of algs which are enabled by default.

Multiple IP Helper over VLAN

This enhancement is documented under ER Q01465479 in Clarify. IP-Helper addresses are supported on physical ethernet interfaces. The customer is requesting support for IP-Helper addresses on VLAN based sub-interfaces

At Startup reading system.cfg from an alternate drive

When rebooting the router if it is boot from an alternate drive (/cf0 or /usb0) then if a system.cfg resides on the same drive it will execute it when the router boots.

Problems Resolved in the 9.2.5 Release

Bug Reference	Subsystem	Severity	Priority	Description
Q01465479	Platform	Enhancement	P5	Multiple IP Helper over VLAN
Q01465468	Platform	Broken Feature	P3	IP filtering on vlan Ethernet sub-interfaces
Q01612873	QOS	Broken Feature	P3	Increased QOS RED thresholds to support more bursty traffic in Frame Relay
Q01577851	Telco	Broken Feature	P3	Support for setting up a remote smartjack for telco test
Q01577852 Q01587199	Telco	Broken Feature	P3	Ability to run a Bert test without having to delete the bundle to run the test
Q01617254	SSH	Broken Feature	P2	Inability to login to router under SSH when configured for Radius and the initial user name specified in the login session does not exist in Radius. Future attempts with the correct user and password fail for that session.
Q01623399	Firewall	Crash	P1	Router crashes when customer uses Microsoft Communicator 2005 client and tries to connect to their internal Live Communicator server.
Q01637079	Firewall	Broken Feature	P3	Firewall NAT using TCP, while accessing an single server with repeated use may occasionally lock the up the client workstation for a long period of time
Q01657691	Crypto	Broken Feature	P3	SSH sever does not work with keys generated with RSA

Bug Reference	Subsystem	Severity	Priority	Description
Q01681635	SSH	Crash	P1	Crash with the lastest version of Secure CRT when disconnecting found on r9.2.4
Q01716188	SNMP	Crash	P3	Router occasionally crashes when retrieving the routing table with SNMP
Q01729897	Platform	Broken Feature	P3	Cannot set the ToS field on a ping command
Q01730755	VRRP	Broken Feature	P3	VRRP does not full initialize on boot up if snmp is enabled and the router is set to display the running configuration on boot up
Q01731388	VRRP	Crash	P1	VRRP crashes when disabling the VRRP group if the VRRP group is not in backup or master state
Q01738866	SNMP	Broken Feature	P3	snAuthenticationLoginMethod mib displays wrong values for auth methods
Q01743040	DHCP Server	Broken Feature	P3	Dhcp server offers wrong ip address if dhcp client requests the same address which belong to another dhcp pool
Q01744158	SNMP	Broken Feature	P3	Router when it boots does not send out start trap
Q01744357	SNMP	Broken Feature	P3	Bundle total bandwidth and link bandwidth under the bundle mib is not showing in the correct value
Q01745096	SNMP	Broken Feature	P2	SR 1001,SR1002/1004 are not sending snmp trap for Frame Relay PVC state changes with the frDLCIStatusChange (active/inactive) trap

Firewall ALG Notes

Firewall ALG Name	Protocol and Port Number	Default Factory Setting	Notes
sip Session initiation protocol	UDP Port 5060	Enabled	
sip-tcp Session initiation protocol	TCP Port 5060	Enabled	
msn Microsoft Networs Messenger	TCP Port 1863	Enabled	Works with MSN client to version 7.0
gatekeeper Micosoft NetMeeting H323-Gatekeep(server to server)	UDP Port 1719	Disabled	Unusual use case for H323 trunking through NAT
msgudp Microsoft Gaming Zone	UDP Port 47624	Disabled	
tftp Trivial file transfer protocol	UDP Port 69	Enabled	
rpc Remote Procedure call	UDP Port 111	Enabled	
dns Domain Name Service	UDP Port 53	Disabled	Unusual use case – DNS Server on the private side missing needed cli configuration
n2p Net2Phone private protocol	UDP Port 6801	Disabled	Old version, n2p protocol mostly repaced by sip even in n2p clients

Firewall ALG Name	Protocol and Port Number	Default Factory Setting	Notes
pcanywhere Norton/Symantec's pcanywhere protocol	UDP Port 5632	Disabled	Rare use case version 5.0.0
l2tp Layer 2 Tunneling protocol	UDP Port 1701	Enabled	
sql Structured Query Language Oracle's port	UDP Port 1521	Disabled	Port not really registered wth IANA, rare use case
rtsp554 Real Time Streaming Protocol	UDP Port 554	Enabled	
Rtsp7070 Real Time Streaming Protocol Apple's quicktime port	UDP Port 7070	Enabled	
h323 H323 Protocol	UDP Port 1720	Enabled	
irc Internet Relay Chat	UDP Port 6667	Disabled	
aim AOL Instant Messager	TCP Port 5190	Disabled	Only compatiable with older versions that do not encrypt
pptp point to point tunneling protocol (management session)	TCP Port 1723	Enabled	
ftp File Transfer Protocol	TCP Port 21	Enabled	
web Hyper Text Protocol	UDP Port 80	Enabled	
smtp Simple Mail Transfer Protocol	TCP Port 25	Enabled	
n2pe Net2Phone Private Protocol	TCP Port 81	Disabled	
ils Micosoft NetMeeting over LDAP Internet Location Server	TCP Port 389	Disabled	
cuseeme CU-SeeMe	TCP Port 7648	Disabled	Rare use case
mszone Microsoft Gaming Zone	TCP Port 28801	Disabled	
nntp Network New Transfer Protocol	TCP Port 119	Disabled	Proxy transport system may not be reliable or stable
netbios	TCP Port 139	Disabled	Rare use case
aimudp AOL Instant Messager	UDP Port 5190	Enabled	
ike Internet Key Exchange Protocol	UDP Port 500	Disabled	
ils2 Microsoft NetMeeting over LDAP Internet Location Server	TCP Port 1002	Disabled	

A new parameter on the enable-all command "default" sets all the algs to the factory-defaults (as above).

The help strings under firewall:global:algs:? are expanded.

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.

Name	Description
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> **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.

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