Secure Router 1001/1001S

Software Release 8.3.6

1. Release Summary

Release Date: 22-September-2006
Purpose: Software maintenance release to address customer found software issues and minor enhancements.

2. Important Notes before Upgrading to This Release

None.

3. Platforms Supported

Nortel Secure Router 1001 models
Nortel Secure Router 1001S models

4. Notes for Upgrade

Please see the technical documentation for the Secure Router 1001/1001S version 8.3.5 available at: http://www.nortel.com/support (select Categories and then Routers & Routing Switches) for details on how to upgrade your Secure Router 1001/1001S units.

File Names for This Release

Description	Date	File Size	Version	File Name
Secure Router 1001 Application image	September 20,2006	9,273,787	'r8.3.6'	J11000.Z
Secure Router 1001S Application Image	September 21, 2006	9,737,488	'r8.3.6'	JP1010.Z

5. Version of Previous Release

Software Version **8.3.5**

6. Compatibility

N/A

7. Changes in This Release

Redundant DHCP Relay

The ability of DHCP Relay to support up to 4 DHCP Servers per Ethernet interface to forward packets to. The dhcp_relay command has been deprecated and replaced by the dhcp-relay command. To configure multiple DHCP Servers for DHCP Relay to use enter a separate dhcp-relay command for each dhcp server ip address. The order in which the dhcp servers are entered in the same order that the dhcp requests are forwarded in.

Disabling the IPSEC Anti-replay service

The ability to disable the anti-replay service is useful when using Diff-serv marking on an ipsec tunnel where you want to support voice traffic at a higher priority then data traffic. As the voice call level (high priority) increases then the data traffic is delayed sufficiently where the anti-replay service starts affecting the amount of (lower priority) data traffic that is delivered properly. By disabling the anti-replay service more data traffic can get through.

There is a new configuration command under crypto command tree which can enable/disable the anti-replay service. By default the anti-replay service is enabled. Also a new show crypto configuration command was added. Below is an example of toggling the service on and off.

```
R1/configure > crypto
R1/configure/crypto > antireplay-service
R1/configure/crypto > show crypto configuration

Crypto Configuration
------------------------
Anti-Replay Service: ON

R1/configure/crypto > no antireplay-service
R1/configure/crypto > show crypto configuration

Crypto Configuration
------------------------
Anti-Replay Service: OFF
```

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 cli commands are the following

```
configure
|-- ip
```

```
|    |-- dhcps
|    |    |-- pool
|    |    |    |- altvlan
|    |    |    |- call server
|    |    |    |- wireless
```

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> **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 configures 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.

Name	Description
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.

Ability to Enable/Disable Firewall ALGs

All the firewall algs are enabled by default when the firewall is configured. It can become necessary to selectively disable ALGs in the firewall when applications fail due to incompatibility with the Firewall ALG. When a configuration is saved on the router if a firewall alg is disabled the disabling of that alg will be saved. The configuration of the algs is under the firewall/global/algs subtree.

The following example show how to disable the SIP ALG in the firewall and how to
Display the current enabled firewall ALGs.

```
R1/configure/firewall global/algs > show firewall algs
Firewall Algs     Status
---------------   ---------
aim               Enabled
cuseeme           Enabled
dns               Enabled
ftp               Enabled
gatekeeper        Enabled
h323              Enabled
icq               Enabled
ils               Enabled
irc               Enabled
l2tp              Enabled
msgtcp            Enabled
msgudp            Enabled
msn               Enabled
mszone            Enabled
n2p               Enabled
n2pe              Enabled
nntp              Enabled
pcanywhere        Enabled
pptp              Enabled
rpc               Enabled
rtsp554           Enabled
rtsp7070          Enabled
```

```
sip             Enabled
smtp            Enabled
sql             Enabled
tftp            Enabled
web             Enabled
R1/configure/firewall global/algs > no ftp
Firewall FTP Alg disabled
R1/configure/firewall global/algs > no sip
Firewall SIP Alg disabled
R1y/configure/firewall global/algs > show firewall algs
Firewall Algs    Status
---------------  ---------
aim              Enabled
cuseeme          Enabled
dns              Enabled
ftp              Disabled
gatekeeper       Enabled
h323             Enabled
icq              Enabled
ils              Enabled
irc              Enabled
l2tp             Enabled
msgtcp           Enabled
msgudp           Enabled
msn              Enabled
mszone           Enabled
n2p              Enabled
n2pe             Enabled
nntp             Enabled
pcanywhere       Enabled
pptp             Enabled
rpc              Enabled
rtsp554          Enabled
rtsp7070         Enabled
sip              Disabled
smtp             Enabled
sql              Enabled
tftp             Enabled
web              Enabled

R1/configure/firewall global/algs > sip
Firewall SIP Alg enabled
R1/configure/firewall global/algs > show firewall algs
Firewall Algs    Status
---------------  ---------
aim              Enabled
cuseeme          Enabled
dns              Enabled
ftp              Disabled
gatekeeper       Enabled
h323             Enabled
icq              Enabled
ils              Enabled
irc              Enabled
l2tp             Enabled
msgtcp           Enabled
msgudp           Enabled
msn              Enabled
mszone           Enabled
```

n2p	Enabled
n2pe	Enabled
nntp	Enabled
pcanywhere	Enabled
pptp	Enabled
rpc	Enabled
rtsp554	Enabled
rtsp7070	Enabled
sip	Enabled
smtp	Enabled
sql	Enabled
tftp	Enabled
web	Enabled

Ethernet supports MTU of 1600 bytes

This feature was added so that a GRE tunnel could be configured over the Ethernet that supports 1500 bytes of user data without having to fragment the packet over the tunnel.

Clear Firewall connections

Added cli commands

Added cli commands to be able to clear firewall connections.

```
clear
|-- firewall
|    |-- connection
|    |-- connections
```

Clear Commands

Name	Description
connection	**NAME** Clear firewall connections related to ip address **SYNTAX** R1#clear firewall connection ip_address <cr> **DESCRIPTION**. ip_address -- ip address related to the firewall connection to be cleared .
connections	**NAME** Clear all firewall connections **SYNTAX** R1#clear firewall connection ip_address <c

R1/configure/firewall global/algs >

Old Features Removed From This Release

None.

Problems Resolved in the 8.3.6 Release

CQ#	Subsystem	Severity	Priority	Description
11072	BGP	Crash	P2	Crash when executing show ip bgp table
13185	DHCP SERVER	Broken Feature	P3	Firewall not handling vlan packets originating from the dhcp server
13226	QOS	Broken Feature	P3	Percent QOS recalculation issue between Cisco router
13315	DHCP RELAY	Broken Feature	P3	DHCP Relay does not work over sub interfaces
13365	Ethernet	Broken Feature	P3	Subinterface is brought down when the main interface is unconfigured
13540	CLI	Broken Feature	P3	Did not execute the command after receiving the CR from the console
13624	MLPPP	Broken Feature	P3	MLPPP failed to negotiate with the other side if it rejected an MRU of 1500.
13671	Ethernet	Broken Feature	P3	When Tasman box reboots, Ethernet interfaces not coming up in certain scenarios
13781	VLAN	Broken Feature	P3	VLD tagging of untagged packets not working properly
13795	IPSEC	Broken Feature	P3	VPN Tunnel does not return ICMP unreachable (must fragment) message back to the sender
13796	Firewall	Broken Feature	P3	Firewall connection not cleared if arp entry for an ip address of the firewall connection was removed
13913	Ethernet	Broken Feature	P3	Ethernet remains down with bundle tracking if the bundle goes down and then comes back up.
------	SNMP	Broken Feature	P3	SNMPv2c (get bulk) doesn't work

Additional Notes:

Workaround for Bug 13540: When doing cut and paste buffer from the console to insure that the commands complete fully set the console to not time out. This is done by setting the telnet_timeout to zero.

8. Outstanding Issues

Refer to the Secure Router 1001/1001S version 8.3.6 Release notes

9. Known Limitations

Refer to the Secure Router 1001/1001S version 8.3.6 Release notes

10. Documentation Corrections

None