



Secure Router 3120

Software Release 9.1.1

1. Release Summary

Release Date: 02-November-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 3120

4. Notes for Upgrade

Please see the technical documentation for the Secure Router 3120 version 9.1 available at: <http://www.nortel.com/support> (select Categories and then Routers & Routing Switches) for details on how to upgrade your Secure Router 3120. Customers may also refer to the Secure Router 3120 v9.1.0 read-me file for a list of previously fixed issues and enhancements.

File Names for This Release

Description	Date	File Size	Version	File Name
Secure Router 3120 Application Image	Nov 1, 2006	7,589,297	r9.1.1	H1000.Z

5. Version of Previous Release

Software Version 9.1.0

6. Compatibility

N/A

7. Changes in the 9.1.1 Release

PMTU Support for IPSEC tunnels

Support PMTU as a configurable option. – if enabled and fragmentation is required and DF bit s set, will send an ICMP error to the packet originator. The DF bit from the inner IP header will be copied to the outer IP header; this will allow intermediate routers to fragment or not depending on the value of the DF bit. IP fragmentation will be supported for IP packets that exceed the MTU after insertion of GRE/IPIP header. IP fragmentation if applicable is based on the MTU of the outbound physical interface.

The cli commands are the following

```
configure
|-- crypto
|   |-- pmtu
|       |-- dfbitval
|       |-- threshold-mtu
|       |-- unsecured-icmp-processing
|
|   |-- interface
|       |-- tunnel
|           |-- ip
|               |-- mtu
|
show
|-- crypto
|   |-- pmtu
|       |-- config
|       |-- df-bit
```

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 a 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	<p>NAME altvlan – Alternate vlan id for IP Phones</p> <p>SYNTAX R1/configure/ip/dhcps/pool x # altvlan vlanid <cr></p> <p>DESCRIPTION. vlanid -- vlan id (enter a integer 0 - 65535)</p> <p>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.</p>

Name	Description
callserver	<p>NAME callserver – Call Server for IP Phones</p> <p>SYNTAX R1/configure/ip/dhcps/pool x # callserver ip1 port port_val appserver ip2 svpsserver ip3 <cr></p> <p>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 address of the XAS application server svpsserver -- SpectraLink Voice Priority (SVP) server ip3 -- ip address of the SVP server</p> <p>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 svpsserver option configures dhcp option 151.</p>
wireless	<p>NAME wireless – Wireless AP Series IP Phones</p> <p>SYNTAX R1/configure/ip/dhcps/pool x # wireless ip1 <cr></p> <p>DESCRIPTION ip1 -- ip address wireless server</p> <p>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.</p>

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

R1/configure/firewall global/algs >

Old Features Removed From This Release

None.

Problems Resolved in the 9.1.1 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
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

8. Outstanding Issues

Refer to the Secure Router 3120 version 9.1.0 Release notes

9. Known Limitations

Refer to the Secure Router 3120 version 9.1.0 Release notes

10. Documentation Corrections

None

Copyright © 2006 Nortel Networks Limited - All Rights Reserved. Nortel, Nortel Networks, the Nortel logo, Globe mark, and Passport 8100/8300/8600 are trademarks of Nortel Networks Limited.

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>