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

Software Release 9.3.1 Readme Notes

1. Release Summary

Release Date: 07-May-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 v9.3.1 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://support.nortel.com/go/main.jsp?cscat=DOCDETAIL&id=523853&poid=15961

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

For users upgrading to v9.3.1 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 v9.3.1 release you must enter the following commands

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

2)Boot the v9.3.1 release. Enter the following commands:

```
configure t
aaa
enable
save local
```

Stored configuration is saved in the proper order.

BGP Upgrade for SR 3120

Prior to upgrading to Release r9.3.1 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	9431039	'r9.3.1'	H1000.Z
Secure Router 1002/1004	8734562	'r9.3.1'	T1000.Z
Secure Router 1001	9412296	'r9.3.1'	J1100.Z
Secure Router 1001S	9866814	'r9.3.1'	JP1010.Z

5. Version of Previous Release

Software Version 9.3

6. Compatibility

N/A

7. New Features in the 9.3.1 Release

7.1 Temperature Sensor Notes (ID: Q01846576)

Temperature Sensor Readings

The actual internal temperatures are now displayed through CLI across the Secure Router Product line. Below is a table of the temperature thresholds for each of the Secure Routers along with how the CLI temperature display has changed. The temperature is in Celsius along with it state and is viewable under Nortel ntEnterpriseDataTasmanMgmtenvironment MIB.

	Router Internal Temperature Thresholds			
		Normal Range	**Warning Range**	**Critical Range**
Model Number	**SR1001** **SR1001S**	Up to 66 degrees C	66 – 71 degrees C	Above 71 degrees C
	SR1002 **SR1002E** **SR1004** **SR1004E**	Up to 80 degrees C	81 – 90 degrees C	Above 90 degrees C
	SR3120	Up to 66 degrees C	66 - 71 degrees C	Above 71 degrees C

Hysteresis has been added (+/- 2.0 degrees C about the thresholds) to increase immunity to noise.

SR3120 CLI Display

Release r9.2 Display

```
lnb70grlr_3120a > show temperature
Temperature:
Sensor                    Permissible    Current    Status
=========================================================
Motherboard Location 1    10C - 50C      31C        OK
Motherboard Location 2    10C - 50C      31C        OK
Motherboard Location 3    10C - 50C      27C        OK
```

Release r9.3.1

```
lnb70grlr_3120a > show temperature
Temperature:
Sensor                     Permissible    Current    Status
=========================================================
Motherboard Location 1    10C - 68C       31.3C      NORMAL
Motherboard Location 2    10C - 68C       31.6C      NORMAL
Motherboard Location 3    10C - 68C       28.1C      NORMAL
lnb70grlr_3120a >
```

SR1002/1004 Cli Display

Release r9.2 Display

```
test/configure > show temperature
Internal Unit temperature is within the recommended operating range (NORMAL)
```

Release r9.3.1

```
test/configure > show temperature
Internal Unit temperature (64.0 C) is within limits (NORMAL)
```

SR1001 and SR1001S CLI Display

Release r9.2 Display

```
OJ > show temperature
Internal Unit temperature is within the recommended operating range (NORMAL)
OJ >
```

Release r9.3.1

```
OJ > show temperature
Internal Unit temperature (39.0 C) is within limits (NORMAL)
```

7.2 64 BGP Peer Support (ID Q01847300)

This feature is supported only for SR 3100. The limit on the maximum number of BGP peers was increased from 8 to 64 BGP peers.

Limitation:

BGP peer default maximum number of prefixes was reduced to 5K. Previously it was set to 150K (See Upgrade Section)
Under fully loaded condition (64 peers and maximum routes), the convergence time takes in the order of minutes.

7.3 Route Redistribution (ID Q01815191)

This feature is to support matching of tag and setting of tag in routing protocols. One particular usecase scenario is to tag the routes redistributed from BGP and RIP into OSPF so that we could later match on those tags to exclude the routes from being redistributed back into BGP.

Two new options namely “match tag” and “set tag” are added to the CLI command “policy route_map”. This provides a support to create route_map with a match condition for route-tag. This route_map can be used with redistribution command, to permit or deny the redistribution of routes, based on the tag value of the routes. The route_map can also be created with a set option for route-tag.

Some possible usage scenarios are,

1. If a route_map is created with “match tag” 500 and “set tag” 1000 and is used for redistributing routes, then all the routes with route-tag 500 will be redistributed with route-tag 1000. Other routes will not get redistributed
2. If a route_map is created with “match tag 500” and no “set tag” and is used for redistributing routes, then all the routes with tag matching 500 will be redistributed with the same tag 500.Other routes will not get redistributed.
3. If a route_map is created with no “match tag” and “set tag 1000” and is used for redistributing routes, then all the routes will be redistributed with tag 1000.

The “match tag” and “set tag” can also be used along with other match conditions and set options in the route-maps. The CLI command “show policy route-map” will display the match and set configuration for route-tags.

Please find the semantics of the commands below,

```
configure/policy/route_map rmap1 10 > match ?
      as_path
      community
      ip
      source-protocol
      tag

configure/policy/route_map rmap1 10 > set ?
      as_path
      community
      distance
      local_preference
      metric
      metric_type
      origin
      tag
```

7.4 Burst Tolerance for FR and PPP

This feature is used to configure the burst tolerance capacity on PPP and FR interfaces. User can set the burst tolerance value in terms of milliseconds ranging from 15 to 200 ms. It tunes the max and min thresholds for interface RED and class RED accordingly. Burst tolerance can be configured irrespective of CBQ status on the bundle. At present burst tolerance is supported on PPP and FR interfaces.

For PPP interface burst tolerance is always configured at the bundle command level. However for FR interfaces, burst tolerance is configured at the bundle command level, only when CBQ is enabled on the bundle. When CBQ is **NOT** enabled on FR bundle, then the burst tolerance must be configured at pvc command level.

This feature is recommended for low speed links (T1/E1) on Secure Router 1004 and Secure Router 3120 series only.

CLI Command Syntax:

As described above burst tolerance can be configured at bundle level and pvc level as well. However, the command syntax remains same. The default value of burst tolerance is 15 ms. The maximum value can be configured is 200 ms. The values can be configured only in multiples of 5 ms.

```
configure/interface/bundle wan # burst-tolerance 50
```

For FR bundle, this parameter is configured as pvc sub-command level.

```
configure/interface/bundle wan/fr/pvc 100 # burst-tolerance 50
```

This sets the burst tolerance to specified value by user. It updates the max and min threshold values of interface RED (when CBQ is not enabled) and class RED (when CBQ is enabled on the interface) accordingly.

7.5 Problems Resolved in the 9.3.1 Release

Bug Reference	Subsystem	Severity	Priority	Description
Q01846576	Mainboard	Enhancement	P4	Actual temperature needs to be displayed through both CLI and SNMP
Q01809672	QoS	Broken Feature	P2	Router does not handle large bursts of traffic which results in dropped packets
Q01841304	SSH	Broken Feature	P2	SSH Server stops working after a few days
Q01838098	DHCP	Broken Feature	P2	Show running config does not display dhcp configuration if the router fails to get an ip address from the dhcp server

Q01815334	PPP	Broken Feature	P3	A fractional PPP link failed to recover from the link being unlooped at the remote end on the SR1001
Q01830565	TELCO	Broken Feature	P3	The SR 3120 can not support the 128 bundles on a CT3 interface
Q01839472	BGP4+	Broken Feature	P4	Propagation of default routes by BGP is not working
Q01848304	Config Manager	Enhancement	P3	Warning message when configuring "sys log con informational"
Q01815191	OSPF	Enhancement	P4	OSPF redistribute limitation: support for External Route Tag
Q01847300	BGP	Enhancement	P3	Unable to configure 64 BGP peers on a SR 3120
Q01858993	VLAN	Broken Feature	P1	Unable to access the router using the VLAN management address when configure to do VLAN bridging with the r9.3 release
Q01848547	IPSec	Broken Feature	P3	IPSec NAT-Traversal is not working in transport mode
Q01858133	Serial Interface	Broken Feature	P3	Line termination resistors need to be enabled for Smart Serial.

8. Outstanding Issues

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

9. Known Limitations

Refer to the Secure Router 1000/3120 version 9.3.0 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