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

Software Release 9.4 Release Notes

1. Release Summary

Release Date: April 9, 2010
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 v9.4 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:
https://support.nortel.com/go/main.jsp?cscat=DOCDETAIL&id=523853&poid=15961

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

For users upgrading to v9.4 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 disabling prior to setting the key.

1)Before loading the v9.4 release you must enter the following commands
configure terminal
aaa
no enable
save local
2)Boot the v9.4 release. Enter the following commands:
configure terminal
aaa
enable
save local

Stored configuration is saved in the proper order.

Firewall Upgrade

Prior to upgrading to Release r9.4 (from releases earlier than r9.3) you need to disable the IKE ALG and save the configuration prior to loading the r9.4 Release.

Firewall Upgrade Procedure

Procedure Steps

Step	Action
1	To enter the configuration mode, enter: **`configure terminal`**
2	To firewall global, enter: **`firewall global`**
3	To firewall alg, enter: **`algs`**
4	Disable IKE alg, enter: **`no ike`**
5	To exit alg section, enter: **`exit`**
6	To exit firewall, enter: **`exit`**
7	To exit configuration mode, enter: **`exit`**
8	Save configuration, enter: **`save local`**

BGP Upgrade for SR 3120

Prior to upgrading to Release r9.4 (from 9.3 or earlier release) 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	9,520,000	r9.4	H1000.Z
Secure Router 1002/1004	8,748,478	r9.4	T1000.Z
Secure Router 1001	9,417,947	r9.4	J1100.Z
Secure Router 1001S	9,869,258	r9.4	JP1010.Z

5. Version of Previous Release

Software Version 9.3.3

6. Compatibility

N/A

7. New Features in the 9.4 Release

7.1 Packet Capture of Vlan Packet with Filter Rules

The capturing of vlan traffic for a specific vlan id is done thru packet capture access-list rules and applying them to a capture buffer specifying the direction. The access-list rule now supports new fields to filter on according to mac portion of the packet header. The mac accesss-list can filter on the source and destination mac address, ether type, CoS user defined field, vlan , second vlan. Only the mac source address and mac destination address require the proto field to be of mac type. All other mac fields can be applied to any proto type of the access-list rule.

The syntax of the *mac* access-list rule is:

```
add permit mac <src-mac> <dest-mac> <ethertype> <cos> <vlan> <vlan2>
```

Of which *ethertype*, *cos*, *vlan*, *vlan2* are optional parameters.
cos (802.1p) & *vlan* are for outer vlan tag.
vlan2 is for the inner vlan tag for a double tagged frame.

Warning
Packet capture for vlan packets does not work on the Ethernet sub-interfaces

As an example, to capture all the TCP traffic over vlan id 10 with an ether type of 0x8100 on Ethernet 0/1 you would do the following procedure:

```
Host/debug/pcap > show-config
Packet capture global configurations:
=====================================
Maximum size reserved for packet capture : 5120KB
Alloted for packet capture sessions : 0KB
Available for packet capture sessions : 5120KB
Maximum number of sessions allowed : 5

capture     configuration  session     interface:    buffer size  total pkts
name :      committed :    active :                  (Kb) :       captured :
================================================================================
================================================================================
Host/debug/pcap > access-list invlan10
Host/debug/pcap/access-list invlan10 > add permit tcp any any ethertype 0x8100 vlan 10
Host/debug/pcap/access-list invlan10 > exit
Host/debug/pcap > access-list outvlan10
Host/debug/pcap/access-list outvlan10 > add permit tcp any any ethertype 0x8100 vlan 10
Host/debug/pcap/access-list outvlan10 > exit
Host/debug/pcap > capture vlan10
Host/debug/pcap/capture vlan10 > attach ethernet 0/1
Host/debug/pcap/capture vlan10 > filter invlan10 in
Host/debug/pcap/capture vlan10 > filter outvlan10 out
Host/debug/pcap/capture vlan10 > wrap
Host/debug/pcap/capture vlan10 > direction both
Host/debug/pcap/capture vlan10 > commit
Host/debug/pcap/capture vlan10 > show-config

Packet Capture : vlan10
=====================================
Interface attached : ethernet0/1
State : Disabled.
Configurations committed
Duration of session : 0 secs
Direction : IN, OUT
Buffer Wrap : ON
Capture all packets
Capture entire contents of each packet
Capture non-IP packets : ON
packets captured in this session : 0
Buffer size for this session : 1024KB
Inbound Filter : invlan10

Pcap Filter Rule List : invlan10
1. permit tcp any any
Outbound Filter : outvlan10

Pcap Filter Rule List : outvlan10
1. permit tcp any any
Host/debug/pcap/capture vlan10 > exit
```

```
Host/debug/pcap > show-config

Packet capture global configurations :
=====================================
Maximum size reserved for packet capture : 5120KB
Alloted for packet capture sessions : 1024KB
Available for packet capture sessions : 4096KB
Maximum number of sessions allowed : 5

capture     configuration  session     interface:    buffer size  total pkts
name :      committed :    active :                  (Kb) :       captured :
================================================================================
vlan10         yes            no       ethernet0/1         1024         0
================================================================================
Host/debug/pcap > enable
Enabled session vlan10
Host/debug/pcap > show-config

Packet capture global configurations :
=====================================
Maximum size reserved for packet capture : 5120KB
Alloted for packet capture sessions : 1024KB
Available for packet capture sessions : 4096KB
Maximum number of sessions allowed : 5

capture     configuration  session     interface:    buffer size  total pkts
name :      committed :    active :                  (Kb) :       captured :
================================================================================
vlan10         yes            yes      ethernet0/1         1024        128
================================================================================
Host/debug/pcap > no enable
Disabled session vlan10
Host/debug/pcap > show int ethernet 0/1


ethernet 0/1
ipaddr       60.1.1.1
netmask      255.255.255.0
description  -
status       up
configured   auto
  speed      -
  mode       -
actual
  speed      100
  mode       full_duplex
mss          600
mtu          1500

ethernet0/1 (vlan:10) (unit number 0)
Type: ETHERNET (802.1q)
Flags: (0x880fc343)  Up, RUNNING, MULTICAST-ROUTE
Internet Address: 60.1.1.1
Internet Netmask: 255.255.255.0
Internet Broadcast: 60.1.1.255
Maximum Transfer Unit: 1500 bytes
Mac Address:  00:50:52:02:02:01

port counters since last boot/clear
  Bytes Rx                    71244  Bytes Tx                    54498
  Packets Rx                    842  Packets Tx                    625
  Runts Rx                       40  Collisions                      0
  Babbels Rx                      0  Late Collisions                 0
  Err Packets Rx                  0  Up/Down States (Phys)          13
  Up/Down States (Admin)          5

port counters for the last five minutes
  Bytes Rx                    5463  Bytes Tx                    4521
  Packets Rx                    64  Packets Tx                    64
  Runts Rx                       0  Collisions                      0
  Babbels Rx                     0  Late Collisions                 0
  Err Packets Rx                 0  Up/Down States (Phys)           0
  Up/Down States (Admin)         0
```

7.2 Queue in Queue VLAN Support

The Queue in Queue VLAN feature has backwards compatibility with previous commands and there are no new CLI commands to support it.

In previous releases, Ethernet interfaces could be configured as Vlan Tagged and Vld Tagged interfaces. When untagged packets (eg. IP packets) are to be switched using a vlan, the interface has to be configured as Vlan Tagged. When a vlan tagged packet is to be switched with another level of Vlan, the interface has to be configured as Vld Tagged. The Vlan & Vld interfaces have their own configuration and forwarding tables. Additionally, there was a limit of 2 levels of Vlan tagging (Vlan + Vld) allowed.

Using the Queue in Queue Vlan feature, there is a single type of tagged interface which allows packets to be switched with any number of Vlan tags. Packets are then switched on the outermost level of Vlan tags. However, the Vlan for management can only accept single tagged packets.

7.3 Independent VLAN Learning (IVL) Support

Independent Vlan Learning allows the router to split the ARP table according to VLAN so that ARP table lookup is based on both MAC and VLAN Id. The default mode for ARP for backward functionality is Shared VLAN learning mode.

When vlan forwarding and macbridging is enable to show whether IVL is set issue the
Show vlanfwd macbridge config command . The output will look like the following if it is
Enabled:

```
host/configure/vlanfwd > show vlanfwd macbridge config
Macbridge:              Enabled
MacAge(in minutes):     5
MAC Learning Type:      Independent VLAN learning (ivl)
```

When vlan forwarding and macbridging is enable but configured for Shared Vlan Learning the
Output will look like the following:

```
host/configure/vlanfwd/macbridge > show vlanfwd macbridge config
Macbridge:              Enabled
MacAge(in minutes):     5
MAC Learning Type:      Shared VLAN learning (svl)
```

When macbridge is disabled:

```
host/configure/vlanfwd > show vlanfwd macbridge config
Macbridge:              Disabled
MacAge(in minutes):     5
```

7.4 TCP MSS Clamping

The TCP MSS feature enables the configuration of the maximum segment size (MSS) for transient packets that traverse the router, The **ip tcp-mss** command under the interface section specifies the MSS value on the intermediate router of the TCP SYN packets to avoid truncation. When a TCP SYN packet traverses the router the MSS option is lowered to the specified value in the TCP packet.

The ability to set the TCP MSS value is supported on Ethernets (including subinterfaces), Bundles and GRE/IPIP Tunnels and firewall policy. Firewall policy level MSS clamping gives greater granularity by allowing the clamping to be performed only for certain hosts. When setting the TCP MSS value it is recommended that the MSS value is at least 40 bytes less than the MTU of the interface. The TCP header takes up 20 bytes of data (or more if options are used); the IP header also uses 20 or more bytes. This means that between them a minimum of 40 bytes are needed for headers, all of which is non-data “overhead”.

7.4.1 Configuring TCP MSS on a GRE/IPIP Tunnel Interface

Procedure Steps

Step	Action
1	To enter the configuration mode, enter: **configure terminal**
2	To select the tunnel, enter: **interface tunnel <tunnel-name>**
3	Specify the IP address for the tunnel, enter: **[ip address <ip address> <subnet-mask>]**
4	Specify the source address of the tunnel, enter: **tunnel source <A.B.C.D>**
5	Specify the destination address of the tunnel, enter: **tunnel destination <A.B.C.D>**
6	Specify the tcp-mtu of the tunnel, enter: **ip tcp-mss <value>**
7	To exit the tunnel configuration mode, enter: **exit**

7.4.2 Configuring Ethernet Interface

Procedure Steps

Step	Action
1	To enter the configuration mode, enter: **configure terminal**
2	To select the Ethernet, enter: **interface ethernet <port number>**
3	Specify the tcp-mtu of the Ethernet, enter: **ip tcp-mss <value>**
4	To exit the Ethernet configuration mode, enter: **exit**

7.4.3 Configuring TCP MSS on Existing PPP Bundle Interface

Procedure Steps

Step	Action
1	To enter the configuration mode, enter: **configure terminal**
2	To select the Ethernet, enter: **interface bundle <name>**
3	Specify the tcp-mtu of the bundle, enter: **ip tcp-mss <value>**
4	To exit the bundle configuration mode, enter: **exit**

7.4.4 Configuring TCP MSS on an Existing Frame Relay Bundle PVC Interface

Procedure Steps

Step	Action
1	To enter the configuration mode, enter: **configure terminal**
2	To select the Ethernet, enter: **interface bundle <name>**
3	Specify frame relay section, enter: **fr**
4	To select the Ethernet, enter: **frpvc <pvc-number>**
5	Specify the tcp-mtu of the bundle, enter: **ip tcp-mss <value>**
6	To exit the frame relay pvc configuration mode, enter: **exit**
7	To exit the frame relay configuration mode, enter: **exit**
8	To exit the bundle configuration mode, enter: **exit**

7.4.5 Configuring TCP MSS on Firewall Policy

Procedure Steps

Step	Action
1	To enter the configuration mode, enter: **configure terminal**
2	To select the firewall map, enter: **firewall <zone>**
3	Specify the tcp-mtu of the Ethernet, enter: **Policy <priority> <direction values [in,out}>**
4	Specify the tcp-mtu for the policy, enter: **ip tcp-mss <value>**
5	To exit the firewall policy, enter: **exit**
6	To exit the firewall configuration mode, enter: **exit**

7.5 QOS Strict Priority Queuing (SPQ)

Secure Router supports Strict Priority Queuing (SPQ) feature to minimize latency and jitter for traffic on Main Ethernets, MLPPP,PPP, and HDLC bundle interfaces. SPQ uses the shaping/scheduling infrastructure currently used with Class Based Queuing (CBQ), so there is minimal change to QoS configuration. Traffic is classified and marked as before. When SPQ is enabled, instead of queuing the classified traffic into class queues, the traffic will flow through one of the interface queues based on the configuration. SPQ supports up to 8 different queues per physical interface in which each queue has a separate priority. This means that multiple flows can be queued into a single queue if their priority values are the same. SPQ can be enabled or disabled at the interface level for outbound flows. just like CBQ. Only CBQ or SPQ can be active on any interface yet both can be active at the same time on different interfaces. The SPQ queues are named 1 through 8 where queue 1 is the highest priority and the lowest priority is 8. All unclassified flows will be dropped unless a default class is configured and mapped to the lowest priority queue (queue 8).

Unlike CBQ where the committed rate percentage and peak rate percentage are specified globally in the class map with SPQ the committed rate percentage is specified for each queue at the interface level with the shape command. The peak rate percentage is 100% for all SPQ interface queues. After the committed rate percentage for all the queues has been observed the remaining bandwidth is serviced by priority. By default the committed rate for any SPQ interface queue is zero. The latency for traffic for a SPQ queue can increase once it exceeds the committed rate percentage for that queue.

7.5.1 CLI QOS Commands

To configure SPQ you must configure traffic classes for each traffic flow under the interface section and assign an SPQ queue number for each class with the assign_queue command. When SPQ is enabled on an interface, the committed rate (cr_percent) and peak rate (br_percent) values defined for the class are ignored. For SPQ, the committed rate is specified using the queue command under QoS section of the interface. All the clear and show commands are equivalent for SPQ as for CBQ.

7.5.2 Mapping a traffic class to an SPQ queue on Ethernet interface

Procedure Steps

Step	Action
1	To enter the configuration mode, enter: **`configure terminal`**
2	To select the Ethernet, enter: **`interface ethernet <port number,0 or 1>`**
3	To enter QoS section, enter: **`qos`**
4	To create a traffic class, enter: **`add_class <class-name> <parent-name> <cr_percent> <br_percent>`**
5	To configure the traffic class, enter: **`class <class_name>`**
6	To classify traffic, use the "add" commands. For example, to classify traffic according to diffServ code point, use: **`add_dscp <value>`**
7	Specify which SPQ queue, enter: **`assign-queue <queue number, range 1 - 8>`**
8	To exit class configuration mode, enter: **`exit`**
9	To configure committed rate for the queue: **`queue <queue number, range 1 - 8> <cr_percent>`**
10	To exit QoS configuration mode, enter: **`exit`**

7.5.3 Enable SPQ for Ethernet Interface

Procedure Steps

Step Action

----

1 To enter the configuration mode, enter:
```
configure terminal
```
2 To select the ethernet, enter:
```
interface ethernet  <port number, 0 or 1>
```
3 Specify qos chassis section, enter:
```
qos
```
4 Enable SPQ, enter:
```
enable spq output
```

7.6 RADIUS Client with Vendor Specific Attribute (VSA) Support

During the user authentication process, in response to the access-request, radius server will send the privilege level as part of the vendor-specific attribute (26) in access-accept packet.

Radius client on secure router will detect vendor-specific attribute data; get the privilege level and map it to the appropriate access level(s) on secure router.

If for a user both Service-Type attribute and Vendor-Specific attribute are configured, access privilege level for that user will be based on Service-Type. The following table shows the mapping of the VSA value to router user privilege level.

Radius Vendor Specific Attribute Value		Secure Router Privilege Level
1	Login	4
2	Framed	2
3	Callback Login	3
4	Callback Framed	4
5	Outbound	4
6	Administrative	1
7	NAS Prompt	4
8	Authenticate Only	4
9	Callback NAS Prompt	4
10	Call Check	4
11	Callback Administrative	4

7.7 Daylight Saving Time Support

Daylight Saving Time is now supported on the Secure Router for time zones for in US, Canada, and Australia. The command ***show dst*** displays the current settings for daylight savings.

Enable Daylight Saving Time

Procedure Steps

Step Action

----

1 To enter the configuration mode, enter:

```
configure terminal
```

2 To enable daylight saving time, enter:

```
dst enable
```

```
host > show dst
Current TimeZone     : -8:0
Current date and time: TUE APR 06 10:46:03 2010
DST mode             : Enabled
DST                  : in effect
DST start            : SUN MAR 14 02:00:00 2010 Local
```

8. Problems Resolved in the 9.4 Release

Bug Reference	Subsystem	Description
Q01752569	WAN	Serial Interface can not support clock rate of 2048 Kbps
Q01830532	CLI	The command show cfg_log records a wrong IP address in certain cases
Q01833664	Reverse Telnet	Reverse telnet parameters are not set to default values
Q01974816	IPSEC	Unable to ping remote router if bypass-trusted-self is configured on the tunnel
Q01981504	GRE Tunnel	GRE Tunnel not forwarding packets that contain PPTP headers
Q01994993	AAA	Telnet with RADIUS does not support special characters
Q01994988	SYSLOG	SYSLOG with radius enable only sends logout messages and does not send any login attempts messages
Q01995002	SYSLOG	SYSLOG Sever sending messages using UTC instead of local time.
Q01998517	VRRP	Arp table not updating when transitioning between being VRRP Master and Backup
Q02003661-01	Firewall	The SIP ALG is not setting Maddr field in the SIP invite packet is not being modified to the NAT public address
Q02043113	PPP	PPP link will not come up when receiving PPP control packets which contain padding
Q02048369	ISDN	Saved configuration on reboot sets ISDN tei-type to point-to-point even though it was saved as multi-point
Q02080119	PIM	Telnet session hangs when configuring static RP under PIM
Q02084398	SNMP	Source address for the SNMP traps and replies are not used for a tunnel interface
Q02090931	ARP	ARP table not updated when gratuitous ARP received with destination MAC address of all zeros
Q02104526	BGP	Default route propagation of EBGP to IBGP does not work
Q02106949	SNMP	Ethernet sub interfaces do not appear in the SNMP Interface Table
Q02115304	SSH Server	Router crashed when exiting a SSH session during key exchange in a specific condition
Q02117393	QOS	High latency with high priority traffic when large bursts of low priority large packets
Q02117989	DHCP Server	Router crashes when BOOTP request is received over Ethernet sub-interface for the DHCP server

9. Outstanding Issues

Refer to the Secure Router 1000/3120 version 9.3.0, 9.3.1, 9.3.2,9.3.3 Release notes

10. Notes

Problem Q01901647 "Serial Link does not come up when using TELLABS modem" was resolved by using a special serial cable which is Part Number listed below:

N0200146 Cable, V.35, Serial DTE Inverted Clock Signal.

11. Known Limitations

Refer to the Secure Router 1000/3120 version 9.3.0, 9.3.1, 9.3.2,9.3.3 Release notes
Avoid configuring an admin distance of 130 for dynamic routing protocols(RIP,OSPF,and BGP). Admin distance of 130 is internally used by BGP.
Frame Relay Bundles do not support QOS SPQ

12. Documentation Corrections

None.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO/ ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA RESELLER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA RESELLER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA AUTHORIZED RESELLER, AND AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE (“AVAYA”).

Copyright

Except where expressly stated otherwise, no use should be made of the Documentation(s) and Product(s) provided by Avaya. All content in this documentation(s) and the product(s) provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Third Party Components

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Product ("Third Party Terms"). Information regarding distributed Linux OS source code (for those Products that have distributed the Linux OS source code), and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site: http://support.avaya.com/Copyright