Avaya Secure Router 3120 and Secure Router 1000 Series Release 9.4 Release Notes

Release 9.4
NN47260-400
Issue 04.02
March 2013

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

“Documentation” means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya generally makes available to users of its products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of documentation unless such modifications, additions, or deletions were performed by Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked websites referenced within this site or documentation provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on its hardware and Software (“Product(s)”). Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this Product while under warranty is available to Avaya customers and other parties through the Avaya Support website: http://support.avaya.com. Please note that if you acquired the Product(s) from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya. “Software” means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products or pre-installed on hardware products, and any upgrades, updates, bug fixes, or modified versions.

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; 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 materials on this site, the Documentation, Software, or hardware provided by Avaya. All content on this site, the documentation and the Product 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 unless expressly authorized by Avaya. 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

“Third Party Components” mean certain software programs or portions thereof included in the Software that may contain software (including open source software) distributed under third party agreements (“Third Party Components”), which contain terms regarding the rights to use certain portions of the Software (“Third Party Terms”). Information regarding distributed Linux OS source code (for those Products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the Documentation or on Avaya’s website at: http://support.avaya.com/Copyright. You agree to the Third Party Terms for any such Third Party Components.

Trademarks

The trademarks, logos and service marks (“Marks”) displayed in this site, the Documentation and Product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation and Product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners, and “Linux” is a registered trademark of Linus Torvalds.

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: http://support.avaya.com.

Contact Avaya Support

See the Avaya Support website: http://support.avaya.com for product notices and articles, or to report a problem with your Avaya product. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: http://support.avaya.com, scroll to the bottom of the page, and select Contact Avaya Support.

Contents

Chapter 1: Introduction

This document describes the new features, important notices, and fixed and known issues for the Avaya Secure Router 3120 and Avaya Secure Router 1000 Series release 9.4 software.

Document changes since last issue

The following change has been made to this document since the last issue:

- Added a procedure for obtaining a license for Secure Router 3120 and Secure Router 1000 series using a new E-mail address. For more information, see Obtaining a license for Secure Router 3120 and Secure Router 1000 series on page 13.

Chapter 2: New Features

The following sections describe the new features for the Avaya Secure Router 3120 and Avaya Secure Router 1000 Series Release 9.4.

Packet Capture of VLAN Packet with Filter Rules

The capturing of VLAN traffic for a specific VLAN ID is done using packet capture access-list rules and applying them to a capture buffer specifying the direction. In release 9.4, the access-list rule supports fields to filter on the MAC portion of the packet header. The MAC access-list can filter on the source and destination MAC address, Ether type, CoS user defined field, VLAN, and second VLAN.

Note:

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

See *Avaya Secure Router 3120 Configuration Guide* or *Avaya Secure Router 1000 Series Configuration Guide* for more information.

Queue in Queue VLAN Support

In previous releases, Ethernet interfaces could be configured as VLAN Tagged and Vld Tagged interfaces. Additionally, there was a limit of two levels of VLAN tagging (VLAN + Vld) allowed. In release 9.4, the Queue in Queue VLAN feature provides 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.

See *Avaya Secure Router 3120 Configuration Guide* or *Avaya Secure Router 1000 Series Configuration Guide* for more information.

Independent VLAN Learning (IVL) Support

Independent VLAN Learning allows the router to split the ARP table according to VLAN so that the ARP table lookup is based on both MAC and VLAN Id.

See *Avaya Secure Router 3120 Configuration Guide* or *Avaya Secure Router 1000 Series Configuration Guide* for more information.

TCP MSS Clamping

The TCP MSS Clamping 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 tree 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 Ethernet interfaces (including subinterfaces), bundles, GRE/IPIP Tunnels, and firewall policies.

See *Avaya Secure Router 3120 Configuration Guide* or *Avaya Secure Router 1000 Series Configuration Guide* for more information.

QOS Strict Priority Queuing (SPQ)

Release 9.4 supports Strict Priority Queuing (SPQ) to minimize latency and jitter for traffic on Main Ethernet interfaces and MLPPP, PPP, and HDLC bundle interfaces. SPQ uses the shaping and scheduling infrastructure currently used with Class Based Queuing (CBQ), so there is minimal change to QoS configuration. When SPQ is enabled, instead of queuing the classified traffic into class queues, the traffic flows through one of the interface queues based on the configuration. SPQ supports up to eight 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.

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.

See *Avaya Secure Router 3120 Configuration Guide* or *Avaya Secure Router 1000 Series Configuration Guide* for rmore information.

RADIUS Client with Vendor Specific Attribute (VSA) Support

Users can configure a RADIUS profile on the Secure Router to authenticate users centrally using a RADIUS server. In release 9.4, during the user authentication process, the RADIUS server sends the privilege level as part of vendor-specific attribute (VSA) data. The RADIUS client on the Secure Router detects the VSA data, gets the privilege level, and maps it to the appropriate access levels on the Secure Router. For example, the router User Privilege Level for the Callback Login VSA value is mapped to 3.

See *Avaya Secure Router 3120 Configuration Guide* or *Avaya Secure Router 1000 Series Configuration Guide* for more information.

Daylight Saving Time Support

In release 9.4, Daylight Saving Time is supported on the Secure Router for time zones in the U.S.A., Canada, and Australia. The command **`show dst`** displays the current settings for daylight saving.

See *Avaya Secure Router 3120 Configuration Guide* or *Avaya Secure Router 1000 Series Configuration Guide* for more information.

Chapter 3: Important information and notices

This section provides important information and notices applicable to this release.

QoS DSCP Values

There are many network related protocols that are generated by the router which in Release R9.2 did not have any DSCP values applied to them. This could cause network services to have their traffic dropped under load. The table below shows the DSCP values that will be set for packet originating from the router for the following network protocols:

Table 1: QoS DSCP Values

Protocol	QoS DSCP Value
RIP	CS6
OSPF (Keepalive)	CS7
OSPF (Other)	CS6
BGP (Keepalive)	CS7
BGP (Other)	CS6
PIM	CS6
IGRP, IGRP1	CS6
IGMP	CS6
VRRP	CS6
ICMP	CS6
DHCP	CS6
ISAKMP (IKE/IPSEC) port 500 UDP	CS6
NAT Traversal - ISAKMP (IKE/IPSEC) port 4500 UDP	CS6
Telnet	CS7

Memory requirements

The SR3120 ships with 16 MB of flash memory and 256 MB DRAM.

The SR1001 and SR1001S ships with 16MB of flash memory and 128MB of DRAM. The SR1002 ships with 16MB of flash memory and 256MB of DRAM. The SR1004 ships with 32MB of flash memory and 256MB of DRAM.

Software Upgrade Process

The Avaya Secure Router 9.4 release is supported on the Secure Router 3120 and 1000 Series models. The software is located on the CD and on the Avaya Technical Support website.

See the *Secure Router 3120 Installation Guide (NN47260–300)* or *Secure Router 1000 Series Installation Guide (NN47262–300)* for detailed instructions on how to upgrade the software.

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.

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.

Table 2: SR3120 and SR1000 Series Routers software images

Description	File Size	Version	File Name
SR 3120 Application Image	9 520 000	r9.4	H1000.Z
SR 1001 Series Application Image	9 417 947	r9.4	J1100.Z
SR 1001S Series Application image	9 869 258	r9.4	JP1010.Z
SR 1002/1004 Series Application image	8 748 478	r9.4	T1000.Z

Obtaining a license for Secure Router 3120 and Secure Router 1000 series

Perform the following procedure to obtain a license for Secure Router 3120 and Secure Router 1000 series.

Procedure

1. Send an E-mail request to datalicensing@avaya.com.
2. In your E-mail, include the following information:
   a. Type of Secure Router; for example, SR1001, SR1002, SR1004, or SR3120.
   b. Order code for the license ordered.
   c. License Authorization Codes (LAC) received with your purchase.
   d. Serial number of the router.
      - To obtain the serial number from a Secure Router 100x/3120, from the Command Line Interface (CLI), enter the following command:

        ```
        show system configuration
        ```

   Note:

   The E-mail account avaya0118@gwsmail.com is no longer active. To request a license, contact datalicensing@avaya.com.

Configuring SSH

About this task

Before upgrading to version 9.4, you can enable SSH and save the secure router configuration. You need to generate the key, then enable the SSH server, save the router configuration and then reboot the device.

To generate a key and enable SSH, use the following procedures.

Generate an RSA key

Procedure

1. `router > config t`
2. `router/configure >ssh_keygen`
3. `Router/configure/ssh_keygen > generate rsa`
   The RSA host key is generated.

Enable the SSH server with RSA key

Procedure

1. `Router/configure/ssh_server > hostfile shrsakey`
2. `Router/configure/ssh_server > enable`
   Secure shell server is enabled.
3. `Router/configure/ssh_server >`

Generate a DSA key

Procedure

1. `router > config t`
2. `router/configure > ssh_keygen`
3. `Router/configure/ssh_keygen > generate dsa`
   The DSA host key is generated.

Enable the SSH server with DSA key

Procedure

1. `Route/configure/ssh_server >enable`
   Secure shell server is enabled.

2. `Router/configure/ssh_server >`

Adding a pass phrase to the host file

Procedure

```
Router/configure/ssh_server >hostfile <filename> <phrase>
```

Variable	Value
<filename>	The host file name
<phrase>	The rsa/dsa pass phrase

SNMP MIBs

The Secure Routers SR3120 and SR1000 Series are SNMPv1/v2/v2c agents with Industry Standard MIBs, as well as private MIB extensions, which ensures compatibility with existing network management tools.

These MIBs are provided with different versions of code. Consult the Avaya website where a file named mib.zip will contain all these MIBs, and a special file named manifest for the order of the MIB compilation.

Standard MIBs

Refer to the README file for details. Be sure to compile rfc1213.mib before you compile any standard MIBs. The Standard MIB folder contains the following MIBs:

Standard MIB name	RFC	File name
IANA Interface type	n/a	iana-iftype.mib
MIB for network management of TCP/IP based Internet MIBs	RFC1213	rfc1213.mib
Manages Frame Relay DLCI parameters	RFC1315	rfc1315.mib
MIB objects for DS1 interface	RFC1406	rfc1406.mib
MIB objects for DS3 interface	RFC1407	rfc1407.mib
Definitions of Managed Objects for the Ethernet-like Interface types	RFC1643	rfc1643.mib

Standard MIB name	RFC	File name
Definitions of Managed Objects for the Fourth Version of the Border Gateway Protocol (BGP-4) using SMIv2	RFC1657	rfc1657.mib
RIP version 2 MIB extensions	RFC1724	rfc1724.mib
OSPF Version 2 Management Information Base	RFC1850	rfc1850.mib
The Interfaces Group MIB using SMIv2	RFC2233	rfc2233.mib
Objects used for managing Virtual Router Redundancy Protocol (VRRP) routers	RFC2787	rfc2787.mib

Proprietary MIBs

Proprietary MIBs were known as Enterprise MIBs in previous releases of the Secure Router documentation.

Table 3: Proprietary MIBs (formerly Enterprise MIBs)

Proprietary MIB name	File name
	nortel.mib
bundle.mib	ntEnterpriseDataTasmanMgmtbundle.mib
chassis.mib	ntEnterpriseDataTasmanMgmtchassis.mib
config.mib	ntEnterpriseDataTasmanMgmtconfig.mib
dos.mib	ntEnterpriseDataTasmanMgmtdos.mib
dsx-tc.mib	ntEnterpriseDataTasmanMgmtdsx-tc.mib
dsx-te1.mib	ntEnterpriseDataTasmanMgmtdsx-te1.mib
dsx-te3.mib	ntEnterpriseDataTasmanMgmtdsx-te3.mib
environment.mib	ntEnterpriseDataTasmanMgmtenvironment.mib
ethernet.mib	ntEnterpriseDataTasmanMgmtethernet.mib
fr.mib	ntEnterpriseDataTasmanMgmtfr.mib
ghdlc.mib	ntEnterpriseDataTasmanMgmtghdlc.mib
ip.mip	ntEnterpriseDataTasmanMgmtip.mip
ppp.mib	ntEnterpriseDataTasmanMgmtppp.mib
ntEnterpriseData.mib	ntEnterpriseData.mib
qos.mib	ntEnterpriseDataTasmanMgmtqos.mib
snAg.mib	ntEnterpriseDataTasmanMgmtsnAg.mib
snmp.mib	ntEnterpriseDataTasmanMgmtsnmp.mib

Proprietary MIB name	File name
system.mib	ntEnterpriseDataTasmanMgmtsystem.mib
serial.mib	ntEnterpriseDataTasmanMgmtMgmtserial.mib

MIBs

Secure Routers support standard and proprietary MIBs. By default, the SNMP agent is disabled on the device. You can enable and disable the SNMP agent using the CLI.

The following tables provide information about supported MIBs. All proprietary MIBs are now compliant to SNMPv2 framework as defined in RFC 1908 (coexistence between Version 1 and Version 2 of the Internet-standard Network Management Framework). The different MIBs which define these standards are: RFC 1902, RFC 1903, RFC 1904, RFC 1905, RFC 1907, and RFC 1908.

Table 4: Information about Standard MIBs

Standard MIB	Description
RFC 1213	Standard MIB-II objects. The following groups or variables are not supported for this MIB: • egp • at
RFC 1315	MIB objects for frame relay DTE interface. The following SNMP SET operation variables on frDlcmiTable are not supported for this MIB: • frDlcmiAddress • frDlcmiAddrsssLen • frDlcmiMaxSupportedVCs • frDlcmiMulticast
RFC 1406	MIB objects for DS1 interface. The following Far End tables are not supported for this MIB: • dsx1FarEndCurrentTable • dsx1FarEndIntervalTable • dsx1FarEndTotalTable
RFC 1407	MIB objects for DS3 interface.
RFC 1643	MIB objects for Ethernet-like interface. The following variables are supported for this MIB:

Standard MIB	Description
	• dot3StatsFCSErrors • dot3StatsDeferredTransmissions • dot3StatsFrameTooLongs The remainder are not supported.
RFC 1657	Describes MIB objects used for BGP4 routing protocol.
RFC 1724	Describes MIB objects used for RIP routing protocol.
RFC 1850	Describes MIB objects used for OSPF routing protocol.
RFC 2127	Describes MIB objects used for ISDN interfaces. Supported on SR1001 and SR1001s Series routers having an ISDN S/T or U interface.
RFC 2233	MIB objects for interface table extensions including StackTable and ifXTable. IfStackTable shows the sub-layer relationships of interfaces. The following groups or variables are not supported for this MIB3: • ifTestTable • ifRcvAddressTable • In the ifXTable, all High Counters (HC)(ifHC***) variables requiring 64-bit counters are not supported.
RFC 2787	Describes MIB objects used for managing Virtual Redundancy Protocol (VRRP) routers.

Table 5: Information about Avaya Proprietary MIBs

Avaya MIB	Description
bundle.mib	Defines objects related to bundle and link configuration.
chassis.mib	Defines objects related to chassis serial number and model number.
config.mib	Defines objects related to saving configurations for network and flash.
dsx-te1.mib	Defines objects for interface cards that support TE1. These include configuration and statistics for ANSI/ATT/IETF and USER. These objects only pertain to Layer 1.
environment.mib	Defines environment-related objects, e.g., temperature, fans, etc.
ethernet.mib	Defines objects related to configuration and statistics for Ethernet interfaces.
fr.mib	Defines objects related to configuration and statistics for frame relay and MFR bundles.
ghdlc.mib	Defines objects related to configuration and statistics for generic HDLC bundles.
ip.mib	Defines objects related to IP addressable interfaces and static routes.

Avaya MIB	Description
ntEnterpriseDataTasmanMgmtsyste m.mib	Defines system objects such as IP Address, hostName and DNS server.
ppp.mib	Defines objects related to PPP/MLPPP bundles for configuration and statistics.
products.mib	Defines registration objects (sysObjectID) for various Avaya products.
qos.mib	Defines objects related to QOS monitoring and configuration. This release contains only Random Early Detect (RED) objects and class-based queuing.
smi.mib	Defines the top-level object assignments for the Avaya MIB tree. This MIB should be compiled before any other Avaya MIBs are compiled. This MIB does not contain any objects that can be used for management operations.
snmp.mib	Defines objects related to SNMP community and trap_host configurations.
system.mib	Defines objects related to system information, e.g., IP address, host name, and DNS.
Serial.mib	Defines objects related to configuration and statistics for Serial interfaces.

USB and Compact Flash

USB and Compact Flash

You can use the following USB and compact flash memory with the SR3120, SR1001 and SR1001S:

USB

You can use USB only with the SR3120

- Lexar: 1G, 512M
- Sandisk: (MICRO) 2G, 1G, 512M
- (MINI) 512M

Compact Flash

- Sandisk 1G, 512M
- White electronics design: 4G, 2G, 1G, 512M

Chapter 4: Resolved Issues

The following table lists customer issues resolved in Release 9.4.

Table 6: Issues resolved in release 9.4 for Secure Router 3120 and Secure Router 1000 Series

Legacy ID	WI number	Subsystem	Description
Q01752569	wi00546713	WAN	Serial Interface can not support clock rate of 2048 Kbps
Q01830532	wi00532492	CLI	The command **`show cfg_log`** records a wrong IP address in certain cases
Q01833664	wi00547026	Reverse Telnet	Reverse telnet parameters are not set to default values
Q01974816	wi00532703	IPSEC	Unable to ping remote router if bypass-trusted-self is configured on the tunnel
Q01981504	wi00532704	GRE Tunnel	GRE Tunnel not forwarding packets that contain PPTP headers
Q01994993	wi00547243	AAA	Telnet with RADIUS does not support special characters
Q01994988	wi00532708	SYSLOG	SYSLOG with radius enable only sends logout messages and does not send any login attempts messages
Q01995002	wi00547244	SYSLOG	SYSLOG Sever sending messages using UTC instead of local time.
Q01998517	wi00532713	VRRP	ARP table not updating when transitioning between being VRRP Master and Backup
Q02003661-01	wi00547241	Firewall	The SIP ALG is not setting Maddr field in the SIP invite packet is not being modified to the NAT public address
Q02043113	wi00547256	PPP	PPP link will not come up when receiving PPP control packets which contain padding
Q0204836	wi00547259	ISDN	Saved configuration on reboot sets ISDN tei-type to point-to-point even though it was saved at multi-point
Q02080119	wi00532735	PIM	Telnet session hangs when configuring static RP under PIM
Q02084398	wi00547280	SNMP	Source address for the SNMP traps and replies are not used for a tunnel interface
Q02090931	wi00532745	ARP	ARP table not updated when gratuitous ARP received with destination MAC address of all zeros
Q02104526	wi00532739	BGP	Default route propagation of EBGP to IBGP does not work

Legacy ID	WI number	Subsystem	Description
Q02106949	wi00532748	SNMP	Ethernet sub interfaces do not appear in the SNMP Interface Table
Q02115304	wi00532753	SSH Server	Router crashed when exiting a SSH session during key exchange in a specific condition
Q02117393	wi00547279	QOS	High latency with high priority traffic when large bursts of low priority large packets
Q02117989	wi00532732	DHCP Server	Router crashes when BOOTP request is received over Ethernet sub-interface for the DHCP server
Q01901647	wi00532662	Serial Link	“Serial Link does not come up when using TELLABS modem” was resolved by using a special serial cable — Part Number N0200146 , Cable, V.35, Serial DTE Inverted Clock Signal.

Note:

Stored configurations for ike policies, prior to release 9.2, which specified a remote-id parameter will not load properly. Release 9.2 introduced a new parameter “der-encoded-dn” which requires a quoted string to allow spaces to be specified. Additionally, the email and domain-name parameters must now be quoted strings.

For example, the prior crypto configuration:

```
crypto
ike policy site64 64.1.1.1
local-address 20.1.1.10
remote-id email me@acme.com <mailto:me@acme.com>
```

Must be converted to the following to work properly in Release 9.3 and later.

```
crypto
ike policy site64 64.1.1.1
local-address 20.1.1.10
remote-id email "me@acme.com"
```

Chapter 5: Known Issues and Limitations

The following known issues and limitations apply to Release 9.4:

Table 7: Known Issues and Limitations

Legacy ID	WI number	Subsystem	Description
11690	N/A	PIM-SM	Assert fails in "mrt.c", line 1114: "!s"in the particular scenario where RIP, PIM, CBSR, CRP, and IGMP were enabled and the serial link and then ppp3 were shutdown.
Q01763585	wi00546752	BGP	1001 and 1001s support a maximum prefix threshold of up to 4000 on BGP routes
Q01825080	wi00546994	Miscellaneous	Source address obtained from a down" interface should not be used. Always use a loopback address. "
Q01773361	wi00532307	BGP	BGP routes are not sent through IP-IP tunnel.
Q01783871	wi00532363	Routing	An error message should be shown when trying to configure routing on an ethernet sub-interface.
Q01636896	wi00546939	SNMP	The ethernetDhcpRelayServerAddr MIB displays an address of 0.0.0.0 when Ethernet interface is configured.
Q01826457	wi00532480	BGP	BGP cannot be configured after configuring NAT. Configure BGP before NAT.
Q01774970	wi00546834	Ethernet	Due to a platform limitation with 1000 Series routers, MTU option is limited to 64-1500-1600 on T1/E1 interfaces.
Q01820014	wi00546977	PIM-SM	tGateDTask crashes in PIM-SM with multicast traffic if RIP is enabled on the sub-interface.
Q01767310	wi00546792	SNTP	Group needs to be implemented as MIB Table to take care of multiple SNTP Servers.
Q01805060	wi00546927	Firewall	The routed-intf" option with nat-ip in firewall policy does not work if the route is through a PPPoE interface. "
Q01826963	wi00547006	PIM-SM	When source specific joins are sent from IGMPv3, they need to be in the configured ssm-range" of PIM-SM configuration to ensure correct operation. "
Q01887561	wi00532635	Routing	There is a extremely rare occurrence of a crash when snmp client is accessing the IpCidrRouteTable with Max repeaters set to over 300;

Legacy ID	WI number	Subsystem	Description
Q01869825	wi00547144	SNMP	There is a rare occurrence where sending continuous SNMP queries with SNMP community string larger than 64 characters, may cause the router to display repeated error messages on the console.
Q01871102	wi00547149	SNMP	When a tunnel or PPOE interface is administratively shut down, the ifLastChange MIB is not updated properly

Other limitations

The following are other miscellaneous limitations in release 9.4

- SNMP SET operations are not supported.
- OSPF-P2P network type over Ethernet (broadcast) is not supported.
- An interface name of “0” and “1” are reserved for the Ethernets and should not be used on any other types of interfaces.
- When connecting to SR1002/1004 router console port set the terminal to flow control as NONE
- 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

Chapter 6: General Guidelines and Considerations

The following are general guidelines and considerations in Release 9.4:

Table 8: General Guidelines and Considerations

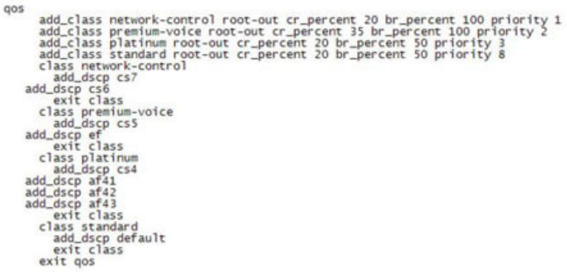
Subsystem	Description
System	It is strongly recommended that you always do execute a write memory command from the CLI after performing any configuration changes, or before doing a manual restart of the router. The configuration file that the router uses when starting up is not automatically updated. The file is only updated when the write memory command is invoked.
1001/3120 Platform	It is strongly recommended that when the removable compact and USB flash is in operation, e.g. file listing/copying/deleting etc., do not eject the flash card. Ejecting the compact or USB flash can render the system console unusable and may also corrupt the system or flash memory. If this situation ever occurs, the system needs to be rebooted to recover and if flash is corrupted, the flash needs to be formatted. Before performing a file related operation that uses USB and compact flash, format them on the device once.
VPN/Firewal	When the Secure Routers are used for VPN functionality only, they still have a stateful firewall active in the routers. The firewall policies can be wild carded to let the traffic flow through. However, the traffic flowing through the router will be subjected to stateful inspection checks i.e. the router must see both outgoing and incoming traffic corresponding to a connection.
VPN	• Remote Access VPN requires the use of a 3rd party IPSec VPN client that should be the SafeNet VPN client as it has been extensively tested. Other standards-based IPSec VPN clients should work, however many vendors restrict the use of the VPN client to only their associated hardware. The SafeNet VPN client can work with any standards-based VPN IPSec hardware. • Remote Access using user group method should not be used when remote users are using a private IP address and behind a NAT Firewall. Mode config based Remote Access can be used for that application.
AAA/FW/ACLs	Release 9.3 and later is verified to support up to 500 Firewall policies, 250 AAA lists and 750 ACLs.
GRE	• While configuring the GRE tunnel, verify that the tunnel destination is reachable through a physical interface. • A "redistribute connected" under OSPF will introduce a recursive route to the tunnel destination through the tunnel itself, which will bring down the tunnel. To

Subsystem	Description
	prevent this, configure a 32-bit route for the destination through a physical interface. • The tunnel destination cannot be the peer-ip of a wan interface.
IP Multicast	• Admin scoped BSR functionality is not supported. • Multicast boundary and ttl-threshold cannot be configured. • Multicast route limit is not supported.
QoS	CR and BR must be specified when adding a new outbound class for CBQ shaping, even though CBQ shaping feature is not enabled at the time of configuration.
Telco	Alarm RLOS is generated when BERT 'all 0s' option is chosen and executed. This happens because maximum number of zeros has been exceeded in a row. This will not happen when B8ZS (zero suppression) is turned on. When there are too many zeros in a row the receivers will not be able to stay in lock with the frame, and the entire trunk will go down. One should not use the all 0 pattern when the mode is AMI on both D4 and ESF framing. This issue doesn't affect E1 since HDB3 encoding is always on.

Frame Relay and OSPF	Configurations with Secure Router to Avaya Multiprotocol Router running Frame Relay and OSPF.
	It is recommended that you disable RFC-1490 fragmentation as shown below.
	`Router > configure t`
	`Router/configure > interface bundle fr-`
	`bn configuring existing WAN bundle interface fr-bn`
	`Router/configure/interface/bundle fr-bn > fr`
	`Router/configure/interface/bundle fr-bn/fr > no enable`
	`fragment_rfc1490`

QoS over Frame Relay	While QoS over Frame Relay & FRF.12 should not be turned on concurrently on the same interface since it will cause double queuing, you can turn on QoS over Frame Relay for classification and monitoring and use FRF.12 for queueing. QoS over Frame Relay does not allow setting up of more than 6 classes over low speed bundles. The following configuration example shows a CBQ model configuration with four classes for low speed (<512K) links. **Note:** When you use FRF.12 fragmentation on low-speed links, you must set the fragmentation size to 640 bytes. In this example, the user is standardizing on a single QoS configuration regardless of link speed. Control traffic such as routing protocol traffic, is prioritized over all other traffic. The other applications prioritized are voice, interactive applications, and best effort.

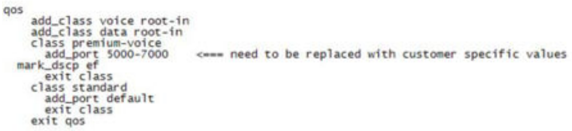
<table>
<tr><th>Subsystem</th><th>Description</th></tr>
<tr><td></td><td>



```
qos
     add_class network-control root-out cr_percent 20 br_percent 100 priority 1
     add_class premium-voice root-out cr_percent 35 br_percent 100 priority 2
     add_class platinum root-out cr_percent 20 br_percent 50 priority 3
     add_class standard root-out cr_percent 20 br_percent 50 priority 8
     class network-control
       add_dscp cs7
   add_dscp cs6
       exit class
     class premium-voice
       add_dscp cs5
   add_dscp ef
       exit class
     class platinum
       add_dscp cs4
   add_dscp af41
   add_dscp af42
   add_dscp af43
       exit class
     class standard
       add_dscp default
       exit class
     exit qos
```

Figure 1: CBQ model configuration

The following configuration example shows an example of QoS over Frame Relay classification and marking only on the egress while queuing is done by FRF.12. Port-based classification allows a user to mark dscp for voice traffic properly. The following configuration is on egress direction of the PVC. Control traffic marking is a missing item.



```
qos
    add_class voice root-in
    add_class data root-in
    class premium-voice
      add_port 5000-7000    <=== need to be replaced with customer specific values
  mark_dscp ef
      exit class
    class standard
      add_port default
      exit class
    exit qos
```

Figure 2: QoS over Frame Relay classification and marking

</td></tr>
<tr><td>ALG</td><td>

The Firewall ALG on the Secure Router supports the following configurations for trunking between Call Servers.

• SIP Trunking between MCS5100 Call Servers

The Firewall ALG on the Secure Router does NOT support the following configurations for trunking between Call Servers.

• SIP Trunking between CS1K or BCM Call Servers

• H.323 Trunking between BCM Call Servers

The workaround for an unsupported VoIP configuration (either Call Server or phone) is to turn off the respective firewall ALG and gatekeeper. For example, the syntax to disable the H.323 ALG is

```
config term
firewall global
algs
no h323
no gatekeeper
```

The following phones and protocols were tested.

• Avaya IP Phones (Unistim)

- Avaya IP Phone 2001

- Avaya IP Phone 2002

- Avaya IP Phone 2004

</td></tr>
</table>

Subsystem	Description
	- Avaya IP Phone 2007 • Avaya IP Phones (SIP) - Avaya IP Phone 1120E - Avaya IP Phone 1140E • Servers - CS1000E — for Unistim phones - MCS 3.5 — for PC clients and 1120E/1140E phones - TFTP/DHCP/FTP — for all phones and PCs • Protocols - UDP — SIP (MCS 3.5 sigma and PC clients) - TCP — SIP (LCS PC clients) - Unistim — IP phones - IP traffic in general testing
QoS- Frame Relay	The QoS feature **`enable <feature> <direction>`** should be configured at a Frame Relay bundle level QoS context. All other QoS commands such as **`add_class`**, **`class`**, **`delete_class`**, and **`delete_all`** are not applicable at the Frame Relay bundle level. These commands are valid at the PVC QoS context and should be used at that level in the CLI to create flows.