Advanced Gateway 2330
Secure Router 4134/2330

Software Release 10.3.4
Release Notes

1. Release Summary

Release Date: Nov 9, 2012
Purpose: Software maintenance release to address customer found software issues.

2. Notes for Upgrade

2.1 General Upgrade Information

Please see the technical documentation for the Secure Router 4134 and 2330 version 10.3 available at: http://www.avaya.com/support for details on how to upgrade your Secure Router unit.

File Names for This Release

Description	File Size	Version	File Name	BootRom Version
Secure Router 4134 Application Image	29 469 747	10.3.4	SR4134.Z	62
Secure Router 2330 Application Image	30 5280 18	10.3.4	SR2330.Z	52
Advanced Gateway 2330 Application Image	30 5280 18	10.3.4	AG2330.Z	52

2.2 SNMP Server

WARNING

After the upgrade to 10.3.4, the SNMP Server will not interoperate with the SNMP clients without updating the stored configuration if upgrading from 10.3 or before. Two SNMP commands do not exist that were in previous releases which are "trap-host" and "trap-version" which are replace with the "target-address" command.

The SNMP Server with this new release supports SNMP version 3. There are two parts of the SNMP Server configuration that must be changed to restore the full functionality of SNMP Server. The first part is enabling SNMP clients to access the SNMP Server and the second part is setting up the SNMP trap host.

The following sections showing the upgrade procedures for SNMP Server are using the following SNMP stored configuration generated under 10.3 Release.

```
snmp-server
  community public rw
  chassis-id SR
  enable traps
    exit traps
  trap-host 10.1.1.1 public
  snmp-enable
  exit snmp-server
```

Updated SNMP Server section after following the upgrade procedures:

```
snmp-server
  engine-id
    local 0000000c000000007f000001
    exit engine-id
  community public public-sec
  chassis-id SR
  enable traps
    exit traps
  group public-group public-sec v1
  access-group public-group v1 noAuth read-view mgmt notify-view all-mibs
  target-address v1addr 10.1.1.1 group-params group-tag timeout 1500 retry-count 3 remote-port 162
  target-params group-params public-sec v1 noAuth
  target-params group-parms public-sec v1 noAuth
  notify group-tag group-tag trap
  notify-filter group-profile 1.3 included
  notify-profile group-params group-profile
  view mgmt 1.3.6.1 included
  view all-mibs 1 included
  snmp-enable
  exit snmp-server
```

2.2.1 Configuring SNMP for version 1 access to the SNMP Server

The SNMP community command has changed under this new release and requires a series of commands to enable an equivalent access for SNMP client to access SNMP Server.

Procedure Steps

Step Action

----

1 To enter the configuration mode, enter:

```
configure terminal
```

2 To enter the SNMP Server configuration, enter:

```
snmp-server
```

3 Delete the previous community command, enter:

```
no community public rw
```

4 Specify the community string with security level, enter:

```
community public public-sec
```

5 Specify the group with the same security level and version 1, enter:

```
group public-group public-sec v1
```

6 Specify the access to the group, enter:

```
access-group public-group v1 noAuth read mgmt notify all-mibs
```

7 To specify the read access, enter:

```
view mgmt 1.3.6.1 included
```

8 To specify the notify access, enter:

```
view all-mibs 1 included
```

9 To exit the SNMP Server configuration mode, enter:

```
exit
```

2.2.2 SNMP Server Configuration changes needed to support SNMP Trap Host

Procedure Steps

Step Action

----

1 To enter the configuration mode, enter:

```
configure terminal
```

2 To enter the SNMP Server configuration, enter:

```
snmp-server
```

3 Specify target parameters security, enter:

```
target-params group-params public-sec v1 noAuth
```

4 Specify the trap host address, enter:

```
target-address v1addr 10.1.1.1 group-params group-tag
```

5 Specify the trap notification, enter:

```
notify group-tag group-tag trap
```

6 Specify the notify profile, enter:

```
notify-profile group-params group-profile
```

7 To specify the notify filter, enter:

```
notify-filter group-profile 1.3 included
```

8 To exit the SNMP Server configuration mode, enter:

```
exit
```

2.3 SSM Upgrade procedure if upgrading from Release before 10.3

Note:

1. These steps are applicable and need to be executed only when upgrading from 10.2.x to 10.3.x. These steps from not needed when upgrading from 10.3.x to 10.3.x
2. When SSM is disabled and enabled, then SSM configuration goes away, so make sure to note down previous SSM configuration.

Here are steps –

1. Disable the ssm if running.
   a. Use command “SR# show ssm sip-server status” to confirm if SSM is running or not.
   b. Use command “SR/configure/voice/service/voip/ssm# no enable” to disable SSM if it is running.
2. Remove SSM database using CLI “SR# clear ssm database”
3. Enable SSM using CLI “SR/configure/voice/service/voip/ssm# enable”
4. Perform SSM configuration as needed.

2.4 Converting between Advanced Gateway and Secure Router

Both the Secure Router 2330 and Advanced Gateway 2330 hardware support the Secure Router and Advanced Gateway Product with the appropiate licensing and software support.

The "file version" command now shows both the version of the image and whether the image is for the Secure Router 2330 or Advanced Gateway 2330 product. The output of the command looks at follows:

```
host# file version

WARNING :
Do not remove the Compact Flash during this process
Do not reboot this device during this process

Versions of files in /cf0/:
Filename:           Version:
--------------------    ----------
found compressed file - skipping file body checksum
SR2330.Z                10.3.4     Image Type = Secure Router
found compressed file - skipping file body checksum
AG2330.Z                10.3.4    Image Type = Advance Gateway
```

The show system licenses display in /cf0/:

2.4.1 Converting an Advanced Gateway to Secure Router

Converting the Advanced Gateway to Secure Router involves the following steps:

- Acquire an Advanced Gateway Upgrade License for Secure Router through Avaya Customer Support
- Install the Secure Router Software (SR2330.Z) on the 2330
- Set Boot Image to SR2330.Z
- Verify Boot Image with "file version" command
- configure system license to Secure Router
- system reboots as a Secure Router 2300

For acquiring the Advanced Gateway license to convert to the Secure Router product you will need the serial number of the Advanced Gateway. This is the Serial Number of slot 0 not the Chassis Serial Number. To determine the serial number of slot 0 use the ***show chassis*** command. The following page shows the output of the command and the actual serial number of slot 0 of this Advanced Gateway is highlighted:

```
host# show chassis

Chassis Model: AG2330
Chassis Operational Status: NORMAL

Chassis Serial number: LBNNTMJX9600GP
Chassis Rev: 11

Slot/SubSlot   Card-Type     Status      Serial#
-------------------------------------------------------
  0        MPU_A        NORMAL      LBNNTMJX960080  ← Serial Number Needed for Licenses
 INT        SCIM_A        NORMAL      LBNNTMJX97001H
 INT        PVIM_A        NORMAL      LBNNTMJX98001P
 0/7        SFP          Present     ---
 0/8        SFP          Present     ---

INT - Mainboard internal module.
```

After acquiring the conversion license number for your Advanced Gateway you will need to download the Secure Router Application Image (SR2330.Z) and Secure Router MIB file (SR2330_10.2.2MIBs.zip) from: http://www.avaya.com/support. Install SR2330.Z file on either /cf0 or cf1. For the conversion process described in these release notes it will be showing the install related to /cf0. Also install the Secure Router MIB files to management console which is being used to monitor the Advanced Gateway.

Below shows the sequence of converting to the Secure Router product:

```
HOST# show version
 Runtime: 10.2.2.0
 Created: Jun 18 2010, 18:44:48
 Type   : AG Image ← current Active Product – Advanced Gateway
    Boot: 0.0.0.42 (NORMAL Boot)
 NorBoot: 0.0.0.40
 GolBoot: 0.0.0.42


Slot/SubSlot  Card-Type  Status   CPLD-Exp CPLD-Main
--------------------------------------------------
  0/-       MPU_A     NORMAL   ---     0x16

host# show system licenses
```

```
Licensed for advance gateway
Licensed PVIM channels = 8
Licensed SSM user capacity = 25

host# file ls

CONTENTS OF /cf0:

  size        date       time      name
--------      ------     ------    --------
30524235   NOV-08-2012   12:06:10 SR2330.Z
      1427    JUN-23-2010  17:51:34  system.cfg
30524235    NOV-08-2012  12:06:10  AG2330.Z

Total bytes: 90188426
Bytes Free on /cf0:  36118528
host# file version

WARNING :
Do not remove the Compact Flash during this process
Do not reboot this device during this process


Versions of files in /cf0/:
Filename:              Version:
--------------------    ----------
found compressed file - skipping file body checksum
SR2330.Z                10.3.4.0        Image Type = Secure Router ← Secure Router Image Type
found compressed file - skipping file body checksum
AG2330.Z                10.3.4.0        Image Type = Advance Gateway ← Advanced Gateway Image Type
HOST#


host# configure term
host/configure# boot_params
Boot dev  [ftp,cf0,cf1]   : cf0
Boot Ethernet Port  [1-8] : 0
Boot file name            : AG2330.Z SR2330.Z ← Changing Boot Image to Secure Router
Server name               : host
Server IP address         : 192.168.24.1
My IP address             : 192.168.24.10
My subnet mask            : 255.255.0.0
Gateway IP address        :
User name                 : demo
Password                  :
Checksum enable     [0:Disable,1:Enable]: 1
Show header enable  [0:Disable,1:Enable]: 0
Save bootrom image  [0:AutoUpdate,1:NormalBTupd,2:GoldenBTupd,3:NoUpd]: 0
display mode  [0:minimum 1:maximum]: 0

BOOT PARAMETERS HAVE BEEN SAVED.

DO YOU WANT TO REBOOT: (Y/N) ?  n ← Do NOT reboot at this point

host/configure# system licenses convertToRouter
Warning: Prior to converting the system to the Advance Gateway functionality.
Warning: Do the following steps
Warning: Download the Secure Router Image SR2330.Z to the boot device, either /cf0 or /cf1
Warning: Set the boot device and boot file name under the boot_params command to SR2330.Z
```

```
Warning: If you proceed, system reboots upon successful conversion
Continue with conversion ? (y/n) : y
Enter License key: xxxxxx ← Enter your license key
Completed...
Conversion Completed...
system reboots in 5 seconds
Warning: If Boot failed, you need reprogram boot menu under boot process


<Mini-Twister Micro POST>
BTS: NORMAL
DDR2: READ MEM   1GB
I2C: PASS
<Mini-Twister Micro POST Completed>
<Mini-Twister Micro POST>
BTS: GOLDEN
DDR2: READ MEM   1GB
I2C: PASS
** Boot stage: M
<Mini-Twister Micro POST Completed>



                   VxWorks System Boot

Copyright (c) 2010 Avaya

PROCESSOR     : MPC8347 TBG
SYSTEM MEMORY : 1G
VxWorks       : VxWorks5.5.1
BSP version   : 1.1/0
Boot version  : 0.0.0.42 (GOLDEN Boot)
Creation date : Nov  8 2012, 11:54:14
NORMAL Bt ver : 0.0.0.52
GOLDEN Bt ver : 0.0.0.52
Baseline ver  : 0.0.0.52 (Internal version for checking)
System name   : SR 2330




Press any key to stop auto-boot...
Compact Flash Device: CF0, Filename: /cf0/SR2330.Z
MODEL: SR -- allow SR image
MODEL: SR -- allow SR image
[SYSTEM] Runtime image loading done
[SYSTEM] Bootrom image loading done
[SYSTEM] Runtime image uncompressing
[SYSTEM] Preparing to transfer control (loader)...


Starting runtime image...



Chassis Model: SR2330
Chassis Operational Status: BOOT

Chassis Serial number: LBNNTMJX9600GP
Chassis Rev: 11

Slot/SubSlot    Card-Type      Status       Serial#
-------------------------------------------------------
  0          MPU_A         NORMAL       LBNNTMJX960080
 INT          SCIM_A        NORMAL       LBNNTMJX97001H
 INT          PVIM_A        NORMAL       LBNNTMJX98001P
 0/7         SFP           Present      ---
 0/8         SFP           Present      ---

Safenet VPN option installed.
PVDM Link set at 100M/FD

Avaya, Inc. and its Licensors
Copyright 1998-2011 All rights reserved
AVAYA (Secure Router SR2330)
Version: 10.3.4.0
Built: Nov  8 2012, 11:54:14 PST
login: admin
password:

admin logged in on Thu Apr 24 18:17:50 2010 from CONSOLE
In system.cfg, Total commands executed: 44, Total errors: 0

host# show version
 Runtime: 10.3.4.0
 Created:   Nov  8 2012, 11:54:14
 Type   : SR Image ← current Active Product – Secure Router
    Boot: 0.0.0.52 (NORMAL Boot)
 NorBoot: 0.0.0.52
 GolBoot: 0.0.0.52


Slot/SubSlot  Card-Type  Status   CPLD-Exp CPLD-Main
---------------------------------------------------
   0/-       MPU_A      NORMAL   ---      0x16
   1/-       ADSL_ANX_A NORMAL   ---      0x3

host# show system licenses
Licensed for router
Licensed PVIM channels = 8
Licensed SSM user capacity = 25
HOST#
```

The conversion to Secure Router is complete

2.4.2 Converting Secure Router to Advanced Gateway

WARNING

All the Advanced Gateway functionality already exists in the Secure Router Product. Converting a Secure Router to the Advanced Gateway product does not require a license but to restore it back to a Secure Router after converting it to an Advanced Gateway will require a license.

Converting the Secure Router to Advanced Gateway involves the following steps:

- Install the Advance Gateway Software (AG2330.Z) on the 2330
- Set Boot Image to AG2330.Z
- Verify Boot Image with “file version” command
- Configure system license to Advanced Gateway
- System reboots as an Advanced Gateway 2330

Below shows the sequence of converting to the Advanced Gateway product:

```
host# show version
Version: 10.3.4.0
Built: Nov  8 2012, 11:54:14 PST
Type   : SR Image ← current Active Product – Secure Router
   Boot: 0.0.0.52 (NORMAL Boot)
 NorBoot: 0.0.0.52
 GolBoot: 0.0.0.52


Slot/SubSlot  Card-Type  Status   CPLD-Exp CPLD-Main
---------------------------------------------------
   0/-       MPU_A      NORMAL   ---      0x16
   1/-       ADSL_ANX_A NORMAL   ---      0x3


host# configure term
host/configure# boot_params

WARNING : Configuration changeBoot dev  [ftp,cf0,cf1]   : cf0
Boot Ethernet Port  [1-8] : 0
Boot file name          : SR2330.Z AG2330.Z ← Changing Boot Image to Advanced Gateway
Server name             : host
Server IP address       : 192.168.24.1
My IP address           : 192.168.24.10
My subnet mask          : 255.255.0.0
Gateway IP address      :
User name               : demo
Password                :
Checksum enable     [0:Disable,1:Enable]: 1
Show header enable  [0:Disable,1:Enable]: 0
Save bootrom image  [0:AutoUpdate,1:NormalBTupd,2:GoldenBTupd,3:NoUpd]: 0
display mode  [0:minimum 1:maximum]: 1 0


BOOT PARAMETERS HAVE BEEN SAVED.
```

```
DO YOU WANT TO REBOOT: (Y/N) ?  n ← Do NOT reboot at this point


HOST/configure# system licenses convertToGateway
Warning: Prior to converting the system to the Advance Gateway functionality.
Warning: Do the following steps
Warning: Download the Advance Gateway Image AG2330.Z to the boot device, either /cf0 or /cf1
Warning: Set the boot device and boot file name under the boot_params command to AG2330.Z
Warning: If you proceed, system reboots upon successful conversion
Continue with conversion ? (y/n) : y
Completed...
Conversion Completed...
system reboots in 5 seconds
Warning: If Boot failed, you need reprogram boot menu under boot process


<Mini-Twister Micro POST>
BTS: NORMAL
DDR2: READ MEM   1GB
I2C: PASS
<Mini-Twister Micro POST Completed>

<Mini-Twister Micro POST>
BTS: GOLDEN
DDR2: READ MEM   1GB
I2C: PASS
** Boot stage: Three
<Mini-Twister Micro POST Completed>

                VxWorks System Boot

Copyright (c) 2010 Avaya

PROCESSOR     : MPC8347 TBG
SYSTEM MEMORY : 1G
VxWorks       : VxWorks5.5.1
BSP version   : 1.1/0
Boot version  : 0.0.0.52 (GOLDEN Boot)
Creation date : Jun 10 2011, 11:09:20
NORMAL Bt ver : 0.0.0.52
GOLDEN Bt ver : 0.0.0.52
Baseline ver  : 0.0.0.52 (Internal version for checking)
System name   : AG 2330


Press any key to stop auto-boot...
Compact Flash Device: CF0, Filename: /cf0/AG2330.Z
MODEL: AG -- allow AG image
MODEL: AG -- allow AG image
[SYSTEM] Runtime image loading done
[SYSTEM] Bootrom image loading done
[SYSTEM] Runtime image uncompressing
[SYSTEM] Preparing to transfer control (loader)...


Starting runtime image...


Chassis Model: AG2330
Chassis Operational Status: BOOT

Chassis Serial number: LBNNTMJX9600GP
Chassis Rev: 11

Slot/SubSlot    Card-Type      Status       Serial#
------------------------------------------------------
   0          MPU_A         NORMAL       LBNNTMJX960080
  INT          SCIM_A        NORMAL       LBNNTMJX97001H
  INT          PVIM_A        NORMAL       LBNNTMJX98001P
  0/7         SFP          Present      ---
  0/8         SFP          Present      ---

Avaya, Inc. and its Licensors
Copyright 1998-2010 All rights reserved
AVAYA (Advanced Gateway AG2330)
Version: 10.3.4.0
Built: Nov  8 2012, 11:54:14 PST

login:
In system.cfg, Total commands executed: 44, Total errors: 0
admin
password:

admin logged in on Wed Jul 27 21:27:32 2011 from CONSOLE
host# show system licenses
Licensed for advance gateway
Licensed PVIM channels = 8
Licensed SSM user capacity = 25

host## show version
Version: 10.3.4.0
Built: Nov  8 2012, 11:54:14 PST
Type   : AG Image ← current Active Product – Advanced Gateway
    Boot: 0.0.0.52 (NORMAL Boot)
 NorBoot: 0.0.0.52
 GolBoot: 0.0.0.52


Slot/SubSlot  Card-Type  Status   CPLD-Exp CPLD-Main
---------------------------------------------------
   0/-       MPU_A     NORMAL   ---      0x16
host#
```

The conversion to Advanced Gateway is complete.

3. Version of Previous Release

Software Version 10.3.3

4. Compatibility

N/A

5. New Features since 10.3 Release

5.1 Tunnel support using dynamically acquired IP Address

> **WARNING**
>
> **This feature only works with tunnel protection and can support only one remote dynamic IP address peer per tunnel. Only one tunnel can be setup to accept an unknown IP Address as its destination IP Address.**

This feature enables a tunnel between the branch router and head office where the branch office acquires it IP Address through the provider by DHCP. This tunnel can be setup as either an IPIP or GRE Tunnel with tunnel protection. The head office can have multipleVPN Site to Site and GRE/IPIP tunnels along with this new feature.

To show how to setup this feature on the Secure Router this section will give the procedure to update both the branch and head office as shown in Figure 1 to use a GRE tunnel with tunnel protection and OSPF to synchronize the routing between the head and branch office.

5.1.1 Configuring Tunnel for Branch Office using DHCP acquired IP Address

In this example the branch office is using SR 2330 with Ethernet 0/5 as its public DHCP acquired IP address and Ethernet 0/6 as its trusted side. The default route will be provided by DHCP and OSPF will be configured over the tunnel and redistributing static routes.

The tunnel source is set to the Ethernet name that is acquiring the DHCP address. The tunnel destination is set to the head office IP Address.

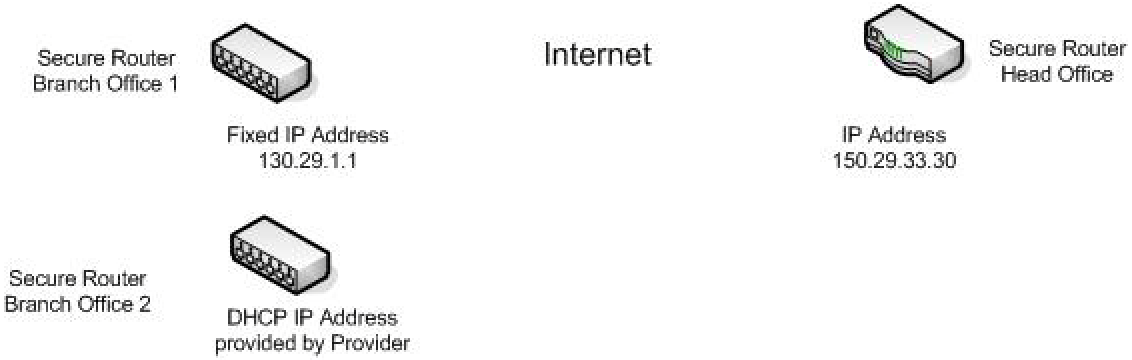

Figure 1 Network Topology with each Branch Office using a IPSec Protected Tunnel to the Head Office

Procedure Steps

Step Action

----

1 To enter the configuration mode, enter:

```
configure terminal
```

2 Configure the Ethernet for DHCP, enter:

```
interface ethernet 0/5
```

3 Specify to request default route, enter:

```
dhcp-client request-default-router
```

4 Specify to enable dhcp, enter:

```
dhcp-client enable
```

5 To exit the Ethernet configuration, enter:

```
exit
```

6 Specify tunnel configuration, enter:

```
interface tunnel main
```

7 Specify the tunnel IP Address , enter:

```
ip address 20.1.1.2 24
```

8 Specify tunnel source address, enter:

```
tunnel source ethernet0/5
```

9 Specify tunnel destination address, enter:

```
tunnel destination 150.29.30.30
```

10 Specify tunnel type as GRE, enter:

```
tunnel mode gre
```

11 Specify tunnel protection, enter:

```
tunnel protection main key123
```

12 Specify tunnel as untrusted firewall interface, enter:

```
crypto untrusted
```

13 To exit the tunnel configuration, enter:

```
exit
```

14 Configure firewall internet zone, enter:

```
firewall internet
```

15 Specify Ethernet 0/ 5 on the untrusted side, enter:

```
interface ethernet0/5
```

16 Specify tunnel on the untrusted side, enter:

```
interface main
```

17 Specify policy to allow icmp, enter:

```
policy 10 in permit protocol icmp self
```

18 To exit the policy, enter:

```
exit
```

19 Specify policy to allow ike, enter:

```
policy 11 in permit service ike self
```

20 To exit the policy, enter:

```
exit
```

21 To exit the firewall internet, enter:

```
exit
```

22 Configure firewall corp zone, enter:

```
firewall corp
```

23 Specify Ethernet 0/ 6 on the trusted side, enter:

```
interface ethernet0/6
```

24 To exit the firewall corp, enter:

```
exit
```

25 Specify router-id for ospf, enter:

```
router-id 2.2.2.2
```

26 Specify OSPF configuration, enter:
```
router ospf 1
```
27 Specify the tunnel network, enter:
```
network 20.1.1.0 0.0.0.255 area 0
```
28 Specify redistribute static, enter:
```
redistribute static
```
29 To exit the OSPF configuration, enter:
```
exit
```
30 To exit the configuration mode, enter:
```
exit
```

5.1.2 Configuring Tunnel for Head Office

In this example the head office is using SR 4134 with Ethernet 0/1 as its untrusted interface that the tunnel is configured on and Ethernet 0/2 is the interface that OSPF interfaces with the head office OSPF network. The default route is 150.29.30.1 which is over Ethernet 0/1.

The tunnel destination is set 0.0.0.0 (allow any to connect) and the tunnel source is set to the IP Address of Ethernet 0/1.

Procedure Steps

Step Action

----

1 To enter the configuration mode, enter:
```
configure terminal
```
2 Configure the untrusted Ethernet, enter:
```
interface ethernet 0/1
```
3 Specify to request default route, enter:
```
ip address 150.29.30.30 29
```
4 To exit the Ethernet configuration, enter:
```
exit
```
5 Configure the trusted Ethernet, enter:
```
interface ethernet 0/2
```
6 Specify to request default route, enter:
```
ip address 130.20.1.1 24
```
7 To exit the Ethernet configuration, enter:
```
exit
```
8 Specify the default static route, enter:
```
ip route 0.0.0.0/0 150.29.30.1
```
9 Specify tunnel configuration, enter:
```
interface tunnel branch2
```
10 Specify the tunnel IP Address , enter:
```
ip address 20.1.1.1 24
```
11 Specify tunnel source address, enter:
```
tunnel source 150.29.30.31
```
12 Specify tunnel destination address, enter:
```
tunnel destination 0.0.0.0
```
13 Specify tunnel type as GRE, enter:
```
tunnel mode gre
```
14 Specify tunnel protection, enter:
```
tunnel protection br2 key123
```
15 Specify tunnel as untrusted firewall interface, enter:

```
crypto untrusted
```

16 To exit the tunnel configuration, enter:

```
exit
```

17 Configure firewall internet zone, enter:

```
firewall internet
```

18 Specify Ethernet 0/1 on the untrusted side, enter:

```
interface ethernet0/1
```

19 Specify tunnel on the untrusted side, enter:

```
interface branch2
```

20 Specify policy to allow icmp, enter:

```
policy 10 in permit protocol icmp self
```

21 To exit the policy, enter:

```
exit
```

22 Specify policy to allow ike, enter:

```
policy 11 in permit service ike self
```

23 To exit the policy, enter:

```
exit
```

24 To exit the firewall internet, enter:

```
exit
```

25 Configure firewall internet zone, enter:

```
firewall corp
```

26 Specify Ethernet 0/ 2 on the trusted side, enter:

```
interface ethernet0/2
```

27 To exit the firewall corp, enter:

```
exit
```

28 Specify router-id for ospf, enter:

```
router-id 1.1.1.1
```

29 Specify OSPF configuration, enter:

```
router ospf 1
```

30 Specify the tunnel network, enter:

```
network 20.1.1.0 0.0.0.255 area 0
```

31 Specify the corp network, enter:

```
network 130.20.1.0 0.0.0.255 area 0
```

32 To exit the OSPF configuration, enter:

```
exit
```

33 To exit the configuration mode, enter:

```
exit
```

5.2 OSPF Inbound Filtering using Route Maps with Distribution List

OSPF supports route maps to filter outgoing routes that are sent by the redistribute command under the ospf section in the prior releases. This release enables the administrator to filter incoming OSPF routes received and block them from being set into the routing table. The new command distribution-list under the ospf section accepts a route map to specify what routes to accept. Both commands accept route-map which consists of access list entries of routes to permit and deny.

In this example the head office is using SR 4134 with Ethernet 0/1 as its untrusted interface that have a number of site to site VPN tunnels are configured on and Ethernet 0/2 is the interface that OSPF interfaces with the head office OSPF network. The remote networks on the VPN site to site tunnels need to be blocked so that the VPN site to site tunnels work.

Procedure Steps

Step Action

----

1 To enter the configuration mode, enter:

```
configure terminal
```

2 Configure the untrusted Ethernet, enter:

```
interface ethernet 0/1
```

3 Specify to request default route, enter:

```
ip address 150.29.30.30 29
```

4 To exit the Ethernet configuration, enter:

```
exit
```

5 Configure the trusted Ethernet, enter:

```
interface ethernet 0/2
```

6 Specify to request default route, enter:

```
ip address 130.20.1.1 24
```

7 To exit the Ethernet configuration, enter:

```
exit
```

8 Specify the default static route, enter:

```
ip route 0.0.0.0/0 150.29.30.1
```

9 Specify a network to block in the access list, enter:

```
access-list ospf-list-in deny 133.22.1.0/24
```

10 Specify a different network to block in the access list, enter:

```
access-list ospf-list-in deny 133.23.1.0/24
```

11 Specify a different network to block in the access list, enter:

```
access-list ospf-list-in deny 133.24.1.0/24
```

12 Specify allowing the rest through in the access list, enter:

```
access-list ospf-list-in permit any
```

13 Specify the route map, enter:

```
route-map ospf-filter-in permit 1
```

14 Specify the access list to match against, enter:

```
match ip address ospf-list-in
```

15 To exit the route map configuration, enter:

```
exit
```

16 Specify router-id for ospf, enter:

```
router-id 1.1.1.1
```

17 Specify OSPF configuration, enter:

```
router ospf 1
```

18 Specify the corp network, enter:

```
network 130.20.1.0 0.0.0.255 area 0
```

19 Specify the routes to block, enter:

```
distribution-list route-map ospf-filter-in in
```

20 To exit the OSPF configuration, enter:

```
exit
```

21 To exit the configuration mode, enter:

5.3 Secure FTP client (SFTP)

A Secure FTP client is able under the new command sftp. There is support for only one SFTP client at a time and it does not support ipv6 addresses. The sftp command is at the root of the command tree. The syntax is as follows:

sftp hostname <cipher> <mac> <port>

Keyword Parameter	Value	Type	Default Value
hostname	IP Address or username@IP Address If only IP Address is specified assumes logged in username.	Required	none
cipher	none des blowfish blowfish-cbc 3des-cbc aes128-cbc aes192-cbc aes256-cbc	Optional	aes128-cbc
mac	hmac-sha1 hmac-sha1-96 hmac-md5 hmac-md5-96 hmac-ripemd160	Optional	hmac-sha1
port	1 - 65535	Optional	22

5.4 SNMP Version 3

The SNMP Version 3 has the following restrictions:

- To configure SNMP Server requires the administrator to be Level -1 User.
- SNMP sets are not supported
- ACLv6 views are not supported
- The maximum recommend number of SNMP communities, users, groups, target addresses, and views are:

1.	Community	16
2.	Users	16
3.	Groups	32
4.	Target Addresses	10
5.	Views	512

SNMP configuration commands have many common parameters that specify a profile for both accessing and sending traps to a client. The commands are the same for all versions of SNMP except the community command for version 1 and 2c replaces the user command.

The common parameters are as follows and used in the sample configurations following:

SECURITY_NAME - defined in the user command for snmp version 3 and in the community command in both version 1 and 2c. This name is used in the group and target_params commands.

GROUP_NAME is defined in the group command. This value is used in the access-group command.

SNMP_VERSION is defined in the group command. This value is used in the access-group and target-params. The possible values are v1, 2c or v3.

SECURITY_LEVEL is defined in the access-group command. This value is used in the target-params command. The possible values are NoAuth, AuthNoPriv, or AuthPriv. SNMP versions 1 and 2c only support NoAuth. The auth and priv configuration is specified in the user command.

TARGET_PARAM_NAME is specified in the target-params command. This value is used in the target-address and notify-profile command.

NOTIFY_TAG is defined in the notify command. This value is used in the target-address command.

PROFILE_NAME is defined in the notify-profile command. This value is used in notify-filter.

VIEW_NAME is defined in the access-group command. This value is used in the view command. The VIEW_NAME values can be different in the read, write_view(not supported), and notify_view parameter of the access-group command and define separate read and notify view inclusions and exclusions depending on the VIEW_NAME.

Sample SNMP Version 1 or 2c configuration

```
community  community_name SECURITY_NAME
group GROUP_NAME SECURITY_NAME SNMP_VERSION
access-group GROUP_NAME SNMP_VERSION SECURITY_LEVEL  read VIEW_NAME write-view VIEW_NAME notify-view
VIEW_NAME
target-params TARGET_PARAM_NAME SECURITY_NAME SNMP_VERSION SECURITY_LEVEL
target-address user1addr 47.152.227.120 TARGET_PARAM_NAME NOTIFY_TAG timeout 1500 retry-count 3
notify user1tag NOTIFY_TAG traps
notify-profile TARGET_PARAM_NAME PROFILE_NAME
notify-filter PROFILE_NAME 1.3.6.1 included
view VIEW_NAME 1.3 include
view VIEW_NAME  1.3.6.1.3.5 exclude
enable traps enable-all
```

Sample SNMP Version 3 configuration

```
user SECURITY_NAME
group GROUP_NAME SECURITY_NAME SNMP_VERSION
access-group GROUP_NAME SNMP_VERSION SECURITY_LEVEL  read VIEW_NAME write-view VIEW_NAME notify-view
VIEW_NAME
target-params TARGET_PARAM_NAME SECURITY_NAME SNMP_VERSION SECURITY_LEVEL
target-address user1addr 47.152.227.120 TARGET_PARAM_NAME NOTIFY_TAG timeout 1500 retry-count 3
notify user1tag NOTIFY_TAG traps
notify-profile TARGET_PARAM_NAME PROFILE_NAME
notify-filter PROFILE_NAME 1.3.6.1 included
view VIEW_NAME 1.3 include
view VIEW_NAME  1.3.6.1.3.5 exclude
enable traps enable-all
```

Under SNMP version 3 the SNMP user accounts can be setup with different security and authentication methods. The following type of users can be setup:

- User with noAuth (used for v1 and 2vC)
- User with sha1authNoPriv
- User with md5authNoPriv
- User with sha1authdesPriv
- User with md5authdesPriv
- User with sha1auth3desPriv
- User with md5auth3desPriv
- User with sha1authaes128Priv
- User with md5authaes128Priv

Below show sample configuration for a SNMP user setup for each of these modes:

```
Community  community_name USER_NAME
group GROUP_NAME USER_NAME SNMP_VERSION
access-group GROUP_NAME SNMP_VERSION SECURITY_LEVEL  read VIEW_NAME write-view VIEW_NAME notify-view
VIEW_NAME
target-params TARGET_PARAM_NAME USER_NAME SNMP_VERSION SECURITY_LEVEL
target-address user1addr 47.152.227.120 TARGET_PARAM_NAME NOTIFY_TAG timeout 1500 retry-count 3
notify user1tag NOTIFY_TAG traps
notify-profile TARGET_PARAM_NAME PROFILE_NAME
notify-filter PROFILE_NAME 1.3.6.1 included
view VIEW_NAME 1.3 in
enable traps enable-all
```

```
user USER_NAME
group GROUP_NAME USER_NAME SNMP_VERSION
access-group GROUP_NAME SNMP_VERSION SECURITY_LEVEL  read VIEW_NAME write-view VIEW_NAME notify-view
VIEW_NAME
target-params TARGET_PARAM_NAME USER_NAME SNMP_VERSION SECURITY_LEVEL
target-address user1addr 47.152.227.120 TARGET_PARAM_NAME NOTIFY_TAG timeout 1500 retry-count 3
notify user1tag NOTIFY_TAG traps
notify-profile TARGET_PARAM_NAME PROFILE_NAME
notify-filter PROFILE_NAME 1.3.6.1 included
view VIEW_NAME 1.3 in
enable traps enable-all
```

```
User with noAuth:
-------------------
user user1
group guser1 user1 v3
access-group guser1 v3 noAuth read two write-view two notify-view two
target-params user1params user1 v3 noAuth
target-address user1addr 47.152.227.120 user1params user1tag timeout 1500 retry-count 3
notify user1tag user1tag traps
notify-profile  user1params user1profile
notify-filter user1profile 1.3.6.1 included
view two 1.3 in
enable traps enable-all
```

```
User with sha1authNoPriv:
--------------------------
user usersha1 auth-type sha1 auth-password shapassword
group gusersha1 usersha1 v3
access-group gusersha1 v3 authNoPriv read two write-view two notify-view two
target-params usersha1params usersha1 v3 authNoPriv
```

```
target-address usersha1addr 47.152.227.120 usersha1params usersha1tag timeout 1500 retry-count 3
notify usersha1tag usersha1tag traps
notify-profile  usersha1params usersha1profile
notify-filter usersha1profile 1.3.6.1 included
enable traps enable-all
```

```
User with md5authNoPriv:
---------------------------
user usermd5 auth-type md5 auth-password md5password
group gusermd5 usermd5 v3
access-group gusermd5 v3 authNoPriv read two write-view two notify-view two
target-params usermd5params usermd5 v3 authNoPriv
target-address usermd5addr 47.152.227.120 usermd5params usermd5tag timeout 1500 retry-count 3
notify usermd5tag usermd5tag traps
notify-profile  usermd5params usermd5profile
notify-filter usermd5profile 1.3.6.1 included
enable traps enable-all
```

```
User with sha1authdesPriv:
---------------------------
user usersha1des auth-type sha1 auth-password shapassword encrypt-type des encrypt-password despassword
group gusersha1des usersha1des v3
access-group gusersha1des v3 authPriv read two write-view two notify-view two
target-params usersha1desparams usersha1des v3 authPriv
target-address usersha1desaddr 47.152.227.120 usersha1desparams usersha1destag timeout 1500 retry-count 3
notify usersha1destag usersha1destag traps
notify-profile  usersha1desparams usersha1desprofile
notify-filter usersha1desprofile 1.3.6.1 included
enable traps enable-all
```

```
User with md5authdesPriv:
---------------------------
user usermd5des auth-type md5 auth-password md5password encrypt-type des encrypt-password despassword
group gusermd5des usermd5des v3
access-group gusermd5des v3 authPriv read two write-view two notify-view two
target-params usermd5desparams usermd5des v3 authPriv
target-address usermd5desaddr 47.152.227.120 usermd5desparams usermd5destag timeout 1500 retry-count 3
notify usermd5destag usermd5destag traps
notify-profile  usermd5desparams usermd5desprofile
notify-filter usermd5desprofile 1.3.6.1 included
enable traps enable-all
```

```
User with sha1auth3desPriv:
---------------------------
user usersha13des auth-type sha1 auth-password shapassword encrypt-type 3des encrypt-password 3despassword
group gusersha13des usersha13des v3
access-group gusersha13des v3 authPriv read two write-view two notify-view two
target-params usersha13desparams usersha13des v3 authPriv
target-address usersha13desaddr 47.152.227.120 usersha13desparams usersha13destag timeout 1500 retry-count 3
notify usersha13destag usersha13destag traps
notify-profile usersha13desparams usersha13desprofile
notify-filter usersha13desprofile 1.3.6.1 included
enable traps enable-all
```

```
User with md5auth3desPriv:
---------------------------
user usermd53des auth-type md5 auth-password md5password encrypt-type 3des encrypt-password 3despassword
group gusermd53des usermd53des v3
access-group gusermd53des v3 authPriv read two write-view two notify-view two
target-params usermd53desparams usermd53des v3 authPriv
target-address usermd53desaddr 47.152.227.120 usermd53desparams usermd53destag timeout 1500 retry-count 3
notify usermd53destag usermd53destag traps
notify-profile usermd53desparams usermd53desprofile
notify-filter usermd53desprofile 1.3.6.1 included
enable traps enable-all
```

```
User with sha1authaes128Priv:
---------------------------
user usersha1aes128 auth-type sha1 auth-password shapassword encrypt-type aes128 encrypt-password aes128password
group gusersha1aes128 usersha1aes128 v3
access-group gusersha1aes128 v3 authPriv read two write-view two notify-view two
target-params usersha1aes128params usersha1aes128 v3 authPriv
target-address usersha1aes128addr 47.152.227.120 usersha1aes128params usersha1aes128tag timeout 1500 retry-count 3
notify usersha1aes128tag usersha1aes128tag traps
notify-profile  usersha1aes128params usersha1aes128profile
notify-filter usersha1aes128profile 1.3.6.1 included
enable traps enable-all

User with md5authaes128Priv:
---------------------------
user usermd5aes128 auth-type md5 auth-password md5password encrypt-type aes128 encrypt-password aes128password
group gusermd5aes128 usermd5aes128 v3
access-group gusermd5aes128 v3 authPriv read two write-view two notify-view two
target-params usermd5aes128params usermd5aes128 v3 authPriv
target-address usermd5aes128addr 47.152.227.120 usermd5aes128params usermd5aes128tag timeout 1500 retry-count 3
notify usermd5aes128tag usermd5aes128tag traps
notify-profile  usermd5aes128params usermd5aes128profile
notify-filter usermd5aes128profile 1.3.6.1 included
enable traps enable-all
```

5.4.1 New CLI SNMP Configuration Commands

The SNMP configuration for version v1, 2c does not specify any user configuration. But must still setup the group access and

5.4.1.1 community

This command configures a v1/v2 community string and aligns it to a security name

Syntax
[no] community [community-name] [security- name]

Keyword Parameter	Value	Type	Default Value
community-name	String max 32 characters	Required	none
security-name	String max 32 characters	Required	none

Example:
SR/configure/snmp-server#community public publicsec-name

5.4.1.2 engine-id

This command configures a local or a remote engine id. The remote engine id are used to allow SNMP v3 informs to be set up to a remote NMS

Syntax
[no] engine-id [local [id]] | *[remote [id] [remote host ipAddr]]*

Keyword Parameter	Value	Type	Default Value
Type	Local remote	Required	none
id	String min 5 characters max 32 characters	Required	none
Ip Addresss	Ip address in dot format (a.b.c.d)	Required for remote type	none
remote-port	min 1024 max 65535	Optional for remote type	162

Example:

```
SR/configure/snmp-server#engine-id local 000c0a0a0ac8
SR/configure/snmp-server#engine-id remote 000c0a0a0a2f 10.4.4.3
```

5.4.1.3 user

Add a v3 user

Syntax:
[no] user [user name] <auth-type {md5 **|** *sha1} [auth-pass] [password] < encrypt-type {aes128* **|** *des* **|** *3des} [encrypt-pass] [password]> <engineid [remote id]>*

Keyword Parameter	Value	Type	Default Value
security-name	String max 32 characters	Required	none
auth-type	md5 sha1	Optional	none
auth-password	String max 32 characters	Optional	none Requires auth-type to be specified if used
encrypt-type	des 3des aes128	Optional	none
encrypt-password	String max 32 characters	Optional	none Requires encrypt-type to be specified if used
engineid	String max 64 characters	Optional	none

Example:

```
SR/configure/snmp-server#user bill
SR/configure/snmp-server#user nancy auth-type md5 auth-pass 456pass1
SR/configure/snmp-server#user tasman engineid 000c0a0a0a98
```

5.4.1.4 group

Assign a v1/v2 security name or a v3 user to a group

Syntax:
[no] group [group name] [security name **|** *user name] [version]*

Keyword Parameter	Value	Type	Default Value
groupname	String max 32 characters	Required	none
username	String Max 32 characters	Required	none
snmp version	v1 v2c v3	Required	none

Example:
```
SR/configure/snmp-server#group v1group publicsec-name v1
SR/configure/snmp-server#group v3group  v3
```

5.4.1.5 access-group

Define access level to a group

Syntax:
[no] access-group [group name] [version] [security-level] <read-view [viewname] > <write-view [viewname]> <notify-view [viewname]> <acl-view [IP rule set name]>

Keyword Parameter	Value	Type	Default Value
groupname	String max 32 characters	Required	none
snmp version	v1 v2c v3	Required	none
security level	noAuth authNoPriv authPriv	Required	none
read-view	String max 32 characters	Optional	none
write-view	String max 32 characters	Optional	none
notify-view	String max 32 characters	Optional	none
acl-view	String max 20 characters	Optional	none

Example:
```
SR/configure/snmp-server#access-group v1group v1 noAuth read-view test notify-view testnotify
SR/configure/snmp-server#access-group v3group v3 authNoPriv read-view v3view notify-view v3view
acl-view ipv4acl
```

5.4.1.6 view

Configure a view subtree

Syntax:
[no] view [view-name] [OID or the sub-tree] [option]

Keyword Parameter	Value	Type	Default Value
viewname	String max 32 characters	Required	none
sub-tree	OID or SNMP sub-tree	Required	none
action	excluded included	Required	none

Example:

```
SR/configure/snmp-server#view test iso included
SR/configure/snmp-server#view test ipAddrTable excluded
SR/configure/snmp-server#view test system excluded
SR/configure/snmp-server#view test 1.3.6.1.2.1.1.0 included
```

5.4.1.7 target-address

Configure target address attributes for traps/notifications and informs

Syntax:
[no] target-address [target addr name] [NMS ip] [target params name] [target tag name] <retry-count> <timeout> <NMS port>

Keyword Parameter	Value	Type	Default Value
groupname	String max 32 characters	Required	none
Address-name	String Max 32 characters	Required	none
IP Addresss	IP address in dot format (a.b.c.d)	Required	none
param-name	String max 32 characters	Required	none
tag-list	String max 32 characters	Required	none
timeout	String max 32 characters	Optional	1500
retry-count	String max 20 characters	Optional	3
remote-port	min 1024 max 65535	Optional	162

Example:

```
SR/configure/snmp-server#target-address Addr1 10.1.1.1 Param1 BranchDevice
```

5.4.1.8 target-params

Configure target parameters

Syntax:
[no] target-params [target params name] [v1/v2 security name / v3 username] [version] [security-level]

Keyword Parameter	Value	Type	Default Value
param-name	String max 32 characters	Required	none
security-name	String		
snmp version	v1 v2c v3	Required	none
security-level	noAuth authNoPriv authPriv	Required	none

Example:
SR/configure/snmp-server#target-params Param1 nortel v3 authNoPriv

5.4.1.9 notify

Define notify parameters

Syntax:
[no] notify [notify name] [target tag] [traps | *informs]*

Keyword Parameter	Value	Type	Default Value
notify-name	String max 32 characters	Required	none
notify-tag	String max 32 characters	Required	none
type-value	traps inform	Required	none

Example:
SR/configure/snmp-server#notify Notification BranchDevice traps

5.4.1.10 notify-profile

Define profiles for a notify

Syntax:
[no] notify-profile [target params name] [profile name]

Keyword Parameter	Value	Type	Default Value

params-name	String max 32 characters	Required	none
profile-name	String max 32 characters	Required	none

Example:

SR/configure/snmp-server#notify-profile Param1 Profile1

5.4.1.11 notify-filter

Filter rules for notify

Syntax:
[no] notify-filter [profile name] [OID / subtree] [option]

Keyword Parameter	Value	Type	Default Value
Profile-name	String max 32 characters	Required	none
sub-tree	OID or SNMP sub-tree	Required	none
action	excluded included	Required	none

Example:
SR/configure/snmp-server#notify-filter Profile1 1.3.6.1 included

5.4.2 CLI Display Commands

show snmp communities	Displays the communities and associated security name
show snmp target-address	Displays the Target address attributes
show snmp views	Displays all the views configured
show snmp view [view name]	Displays the specified view configured
show snmp target-params	Displays info about the target parameters
show snmp users	Displays the information of all users configured with type of authentication / encryption if any.
show snmp access-group	Displays access-privilege of groups configured
show snmp user-groups	Display the association between groups and v1/v2 communities or v3 usernames.

show snmp engine-id	Display the identification of the local SNMP engine and all remote engines that have been configured on the router.
show snmp notify	List of notify tables
show snmp notify-filter	Notify table filters configured
show snmp notify-profile	Profiles of notify table

5.5 Proxy ARP support over Vlans

Proxy ARP is now configurable for Vlans and is configured under the ip sub-tree of vlan configuration. A new cli command "show ip proxy-arp" will display the interfaces configured with proxy-arp.

5.5.1 Cli Commands

5.5.1.1 ip proxy-arp

This command configures proxy arp under both Ethernet and vlan interfaces. The ip proxy_arp command under the Ethernet interface has been deprecated. The ip proxy_arp command will still be accepted and work properly in existing configuration files but the new command ip proxy-arp command will be stored in new configuration files generated with this and future releases.

Syntax
[no] ip proxy-arp

Example:

```
host/configure/vlan vlan200##ip proxy-arp
```

5.5.1.2 show ip proxy-arp

This command shows the interfaces that are configured to support proxy-arp

Syntax
show ip proxy-arp

Example:

```
host #show ip proxy-arp
Proxy Arp Interfaces
  ethernet6
  vlan202
host#
```

5.6 Support for multiple Contivity VPN clients behind NAT to use the same user profile

The previous release had a restriction that if multiple Contivity VPN clients were behind NAT they each needed a separate user profile if there was concurrent access. This restriction does no longer apply and all clients can use the same user profile. There are two separate keep alive parameters that must be enabled for this support to work under the crypto contivity-ira section. Both the client keepalive and nat keepalive parameter must be enabled. Refer to the sample crypto contivity-ira section below.

```
contivity-iras
 ike policy cvc_1
   local-address 10.1.1.1
   remote-id user-name "user1" xxxx
   proposal 1
    exit proposal
   client configuration
     address-pool 1 20.1.1.2 20.1.1.30
     private-side-address 20.1.1.1
     keepalive
      enable
      exit keepalive
     split-tunnel
      exit split-tunnel
     nat-keepalive 20
     exit configuration
   exit policy
 ipsec policy cvc_1
   proposal 1
    lifetime seconds 65000
    exit proposal
   exit policy
 exit contivity-iras
```

Sample crypto contivity-ira section of the Secure Router Configuration File

6. Problems Resolved in the 10.3.4 Release

Bug Reference	Subsystem	Description
wi00965041	Firewall	Telnet and SSH sessions terminating to the router are not cleaned up properly when the session is closed by the Secure Router Firewall
wi00989703	VPN	VPN Phones failed to connect after the following error message was displayed on the console “0x376833a8 (IKES): memPartAlloc: block too big - 293200 in partition 0x50cedb8”
wi00954235	VOIP	Caller continues to hear ring back after call originating on FXS phone is answered on EC500
wi00997596	VPN	Packets sent with TTL of 1 across VPN site-to-site tunnel cause tunnel to fail
wi00998038	Firewall	Router crashed when SIP alg was enabled on the firewall
wi00998467	VRRP	Unable to ping a VRRP address on the router over site-to-site tunnel
wi00998484	VRRP	Unable to ping a VRRP address of an interface configure on the firewall
wi01000293	ARP	ARP entry not updating when a gratuitous ARP is received on different interface over VLAN
wi01001461	Platform	Router crashes after executing “show module test serial 1/1” command on a serial interface that is not configured
wi01001687	VLAN	show arp does not display the physical port where mac address was learned on a vlan interface
wi01003165	VOIP	e1PRI to e1PRI calls are broken
wi01003891	VOIP	FXS-e1PRI call with PESQ is dropping after 3 mins in Normal Mode with Aura
wi01005075	Firewall	SIP alg functionality problems
wi01006229	VOIP	FXS to FXO & FXO to FXS calls are failing with " No path confirm (first)" error in Normal Mode with Aura
wi01006946	VOIP	TDM Hairpin failures
wi01007256	GRE	Fragmentation fails when using a VLAN over GRE tunnel
wi01012465	RIP	Router hangs when Ethernet bounces and is running RIP where multiple RIP peers are advising the same route but different next hop
wi01014247	Platform	AAA authentication not using the configured source address
wi01024192	VRRP	Unable to ping a VRRP address of an interface configured with crypto in VPN-only mode
wi01027437	Platform	Router uses local credentials even when TACACS server reachable and sent authentication failure
wi01027486	Contivity	Ungraceful client disconnects can result in duplicate tunnels
wi01029686	Routing	Incorrect routing with GRE tunnel and ECMP
wi01030915	Tunnel VPN	IPIP tunnel with tunnel protection fails when large windows copy is done across tunnel
wi01049544	Routing	Advanced Gateway 2330 has system max-route-limit is set to large by default
wi01049551	Platform	On factory reset of Advanced Gateway 2330, the platform fails to boot up due to incorrect default image file name

7. Outstanding Issues

N/A

8. Known Limitations

- The secure_passwords command uses nvram to store the key for encrypting/decrypting that has secured passwords in the configuration file. To transfer the system.cfg to another router that has secure_passwords, the administrator needs first to disable secure passwords by executing a no secure_password command and resave the configuration file. This new configuration file can then be loaded on another router and then execute the secure_password command and save local to protect the passwords on the new router.
- Wild charater '%' keeps getting added on the CLI command "dial-per voice pots-destination pattern" on a save local and reboot.

9. Documentation Corrections

- Document Name: Troubleshooting Avaya Secure Router 2330/4134 10.3
  Document Number: NN47263-700_04_01
  Document Release: 10.3

  On page 88 it states "Link Aggregation is supported on the non-CPU Ethernet ports only." However, LACP is supported on all Ethernet ports.

10. Notes

- ICMP rate limiting is enabled by default. If trace route intermittently fails at the router it might be caused by ICMP rate limiting dropping the ICMP error response. The CLI command "ip icmp rate-limit" can change the interval in which ICMP error responses are dropped. Setting the ICMP rate limiting interval to zero disables this feature.
- A new cli command "tcp-seq-except-bgp-self-port" under the dos-protect section of the firewall global settings allows BPG to use MD5 signatures through when tcp-seq-number-predict and tcp-seq-number-range command are set under the dos protect section. It allows for any TCP connection with the BGP destination port of 179 not to have the tcp connection resequenced which causes the MD5 digest to fail.
- ISDN BRI voice bundle with default TE1 mode value of Point to Multipoint will not come up until the bundle is manually changed to point-to point.
- Syntax of rule under "voice translation-rule" was allowing "\+".The backslash (\) was used as an escape character to support "+". Since "+" can be used without the support of "\", use of backslash in the translation rules is redundant and no longer required. Hence backslash (\) is removed from the syntax of rule.

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

Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya. End User agree 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 Web sites referenced within this site or documentation(s) 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 this product. 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 Web site: http://www.avaya.com/support
Please note that if you acquired the product from an authorized reseller, the warranty is provided to you by said reseller and not by Avaya.

Licenses

Copyright

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