avaya.com

Ethernet Routing Switch 3500 Series
Software Release 5.0.2

1. Release Summary

Release Date: 26-November-2012
Purpose: Software maintenance release to introduce new features, as well as to address customer and internally found software issues.

2. Important Notes Before Upgrading to This Release

None.

3. Platforms Supported

Ethernet Routing Switch 3500 (All models).

4. Notes for Upgrade

Please see "Ethernet Routing Switch 3500 Series, Configuration – System, Software Release 5.0" (available at http://www.avaya.com/support . Click Products, select Ethernet Routing Switch 3500 Series from the A-Z list, then select Documentation > View All Documents) for details on how to upgrade your Switch.

Filenames for This Release

File Name	Module or File Type	File Size (bytes)
3500_1006_diag.bin	Diagnostic image	2,183,001
3500_502016.img	Agent code image	7,876,516
3500_502017.img	Agent code image (SSH)	8,094,420
Ethernet_Routing_Switch_35 xx_MIBs_5.0.2.zip	Software Release 5.0.2 MIB definition files	1,323,000

5. Version of Previous Release

Software Version 5.0.1.

6. Compatibility

This software release is managed with Enterprise Device Manager (EDM).

7. Changes in This Release

7.1. New Features in This Release

7.1.1. SLAMon Agent

Identifying occurrences of and isolating performance issues in a network has always been a difficult task. Embedding monitoring devices in the network infrastructure is one way to tackle this problem and this is the focus for SLA Monitor (SLAMon).

Through the use of coordinated network performance tests and efficiently distributed monitoring devices, an accurate picture of overall network health can quickly be developed. Areas in which performance is not up to expectations can then be specifically targeted for deeper analysis or troubleshooting, if necessary.

To support efficient configuration, issue detection and isolation, a centralized monitoring service is ideally suitable to coordinate monitoring agent actions and analyze tests results. The ability to easily and rapidly perform end-to-end network QoS tests and isolate issues requires distributed monitoring agents that are pervasive yet introduce minimal impact to the devices themselves. This divides the responsibilities of SLAMon into two main components of the SLAMon Server and SLAMon Agent.

The SLAMon agent support is available in the ERS 3500 switches with release 5.0.2. The agent operation will be largely transparent to the customer. The agent will be disabled by default (due to security considerations) and will require a single command to achieve minimum configuration on the switch.

The SLAMon agent also supports some local configuration capabilities as well as the ability to query the status of the SLAMon agent and server connection.

CLI Syntax:

PrivExec or global configuration Mode Commands:
show application slamon agent

Application Mode Commands:
[default] slamon agent-comm-port <0-65535>
[default] slamon agent ip address <IP address>
[default] slamon agent port <0-65535>
[no | default] slamon cli [enable]
[default] slamon cli-timeout <60-600>
[no | default] slamon cli-timeout-mode [enable]
[no | default] slamon oper-mode [enable]
[default] slamon server ip address <IP address> <secondary IP address>
[default] slamon server port <0-65535>

CLI Example:

ERS3500> ena
ERS3500# show application slamon agent
SLAMon Operational Mode: Enabled
SLAMon Agent Encryption: Not supported.
SLAMon Agent Address: 47.80.225.190
SLAMon Agent Port: 50011
SLAMon Agent Registration Status: Not Registered
SLAMon Registered Server Address: 0.0.0.0
SLAMon Registered Server Port: 0

SLAMon Server Registration Time: 0
SLAMon CLI Mode: Enabled
SLAMon CLI Timeout Mode: Disabled
SLAMon CLI Timeout: 60 seconds
SLAMon Configured Server Address: 0.0.0.0
SLAMon Configured Server Port: 0
SLAMon Configured Agent Address: 0.0.0.0
SLAMon Configured Agent Port: 0
SLAMon Agent-To-Agent Communication Port: 50012
SLAMon Configured Agent-To-Agent Communication Port: 0

ERS3500# config t
ERS3500 (config)# application
ERS3500 (config-app)# slamon agent ip address 10.30.56.100
ERS3500 (config-app)# slamon agent port 50056
ERS3500 (config-app)# slamon server ip address 135.10.100.1
ERS3500 (config-app)# slamon server port 50156
ERS3500 (config-app)# slamon agent-comm-port 50256
ERS3500 (config-app)# slamon oper-mode enable
ERS3500 (config-app)# exit

7.1.2. Show output includes UTC timestamp

Enables the user to monitor the exact time a specific configuration is invoked. Right after issuing the "show *" command, the UTC stamp is displayed.

With this feature in place, the exact time for a "show" command is displayed just before specific output. The user can enable/disable timestamp using the CLI commands:

CLI Syntax:

Enable Timestamp state
(config)#cli timestamp enable

Disabled Timestamp state changes
(config)#no cli timestamp enable

Reset the timestamp state (disable)
(config)#default cli timestamp enable

By default, the timestamp state is disabled. The current state is preserved between switch/stack reboots. The timestamp corresponds to SNTP, and the time is set using "clock *" commands.

ERS3500(config)#sh clock
THU 2012/11/12 11:38:02 GMT+00:00

Daylight saving recurring time is disabled

Daylight saving time is disabled
Time zone offset from UTC is 00:00

The output for the show clock without SNTP looks like this:

ERS3500(config)#sh clock
THU 1970/01/01 00:00:23 GMT+00:00

Daylight saving recurring time is disabled
Daylight saving time is disabled
Time zone offset from UTC is 00:00

CLI Example

(config)#cli timestamp enable
#show vlan ip
TUE 2012/11/20 10:37:39

==========

Vid ifIndex Address Mask MacAddress Offset Routing

==========

Primary Interfaces

---

1 10001 10.101.39.13 255.255.0.0 2C:F4:C5:A3:18:80 1 Enabled

Total VLAN IP entries: 1

(config)#default cli timestamp enable
#show vlan ip
==========

Vid ifIndex Address Mask MacAddress Offset Routing

==========

Primary Interfaces

---

1 10001 10.101.39.13 255.255.0.0 2C:F4:C5:A3:18:80 1 Enabled

Total VLAN IP entries: 1

7.2 Old Features Removed From This Release

None.

7.3 Problems Resolved in This Release

- Modify DDR settings to prevent intermittent switch lock up
- No error is displayed when trying to set vlan 1 as Voice Vlan
- Password for RADIUS keep alive packets was not encrypted
- Use RADIUS request packet format in RADIUS reachability packets

wi01054413 3524GT-Pwr+ units: Interface Descriptor responds back with Avaya Metro ESU1860V
wi01042622 ERS 35xx:Ports using Crossover cable goes Down after specifying the Speed/Duplex
wi01043987 Processor usage goes into 100%(and remains forever) when page is refreshed continuously from web browser
wi01046160 3524GT combo ports still In MDI mode after reset
wi01056621 AUTO: DUT becomes stuck in exception error loop when HW resetting the DUT

8. Outstanding Issues

None.

9. Known Limitations

wi01056275:
Static route remains inactive after being recursively resolved through a redundant route even after the next hop becomes accessible again. This happens because of the summary route. The workaround is to disable and re-enable IP routing.

The issue can be prevented by a proper design of the addressing plan so that the IP summarization can take effect. Figure 1 and text below illustrates the issue and a workaround.

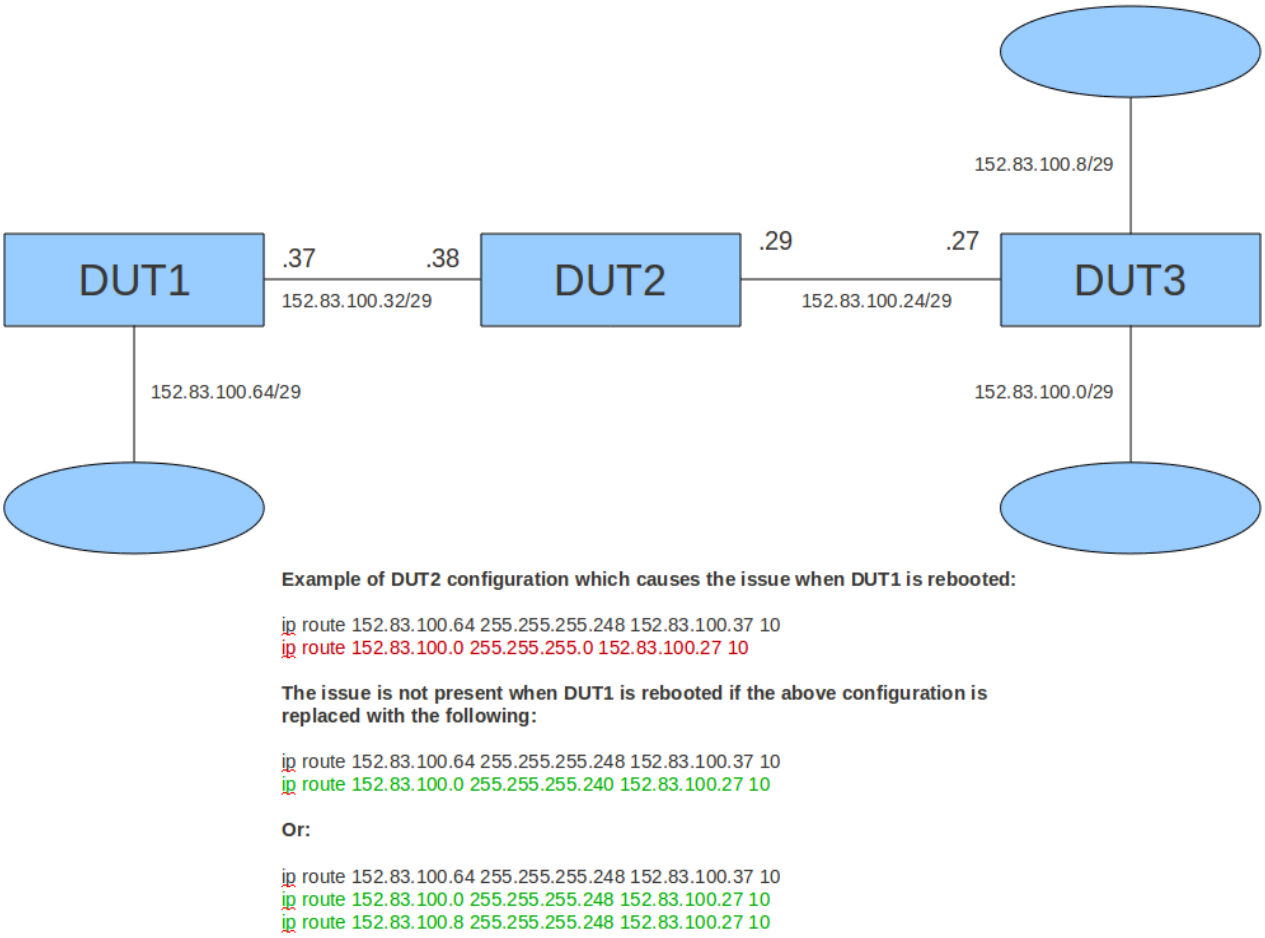

Figure 1 : Sample network

On DUT2, network 152.83.100.64/24 is reachable via DUT1 interface 152.83.100.37 (a static route is configured). Also, to achieve connectivity with 152.83.100.0/29 and 152.83.100.8/29 networks, a static route 152.83.100.0/24 with next-hop 152.83.100.27 (DUT3) is configured. This is a summary route and aggregates all the 152.83.100.x/29 networks in the setup.

When DUT1 is unavailable (rebooted), a route to 152.83.100.64/29 would become a non-local static route due to the next-hop 152.83.100.37/29 being resolved recursively through the summary route 152.83.100.0/24 next-hop 152.83.100.27/29 (DUT3). Thus, the 152.83.100.64/29 network would wrongly appear to be reachable via DUT3 interface 152.83.100.27. This happens because of the IP route summarization.

When DUT1 becomes available again, the route 152.83.100.64/29 through DUT1 (next-hop 152.83.100.37/29) does not recover.

The workaround for the above issue is to disable and re-enable IP routing on DUT2.

The issue can be prevented by a proper design of the addressing plan so that the IP summarization can take effect.

In Figure 1, we are provided with two examples that can successfully replace the initial configuration. With these configurations the issue described above will be avoided. In both examples, the summary route 152.83.100.0/24 is replaced with a more specific summary route (152.83.100.0/28) or with routes to each different subnet.

10. Documentation Corrections

For other known issues, please refer to the product release notes and technical documentation available from the Avaya Technical Support web site at: http://www.avaya.com/support .