Release Notes for Cisco ONS 15302 Release 1.0.1

Release notes address closed (maintenance) issues, caveats, and new features for the Cisco ONS 15302. For detailed information regarding features, capabilities, hardware, and software introduced with this release, refer to Release 1.0 of the Cisco ONS 15302 Installation and Operations Guide. For the most current version of the Release Notes for Cisco ONS 15302 Release 1.0.1, visit the following URL:

http://www.cisco.com/en/US/products/hw/optical/ps2001/prod_release_notes_list.html

Cisco also provides Bug Toolkit, a web resource for tracking defects. To access Bug Toolkit, visit the following URL:

http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl

Contents

Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Changes to the Release Notes

This section documents supplemental changes that have been added to the *Release Notes for Cisco ONS 15302 Release 1.0.1* since the production of the Cisco ONS 15302 System Software CD for Release 1.0.1.

No changes have been added to the release notes for Release 1.0.1.

Caveats

Review the notes listed below before deploying the ONS 15302. Caveats with DDTS tracking numbers are known system limitations that are scheduled to be addressed in a subsequent release. Caveats without DDTS tracking numbers are provided to point out procedural or situational considerations when deploying the product.

DDTS # CSCdz25077

When using the ONS 15302 as a distribution switch connected to an IP multicast router, the ONS 15302 should forward IGMP join and leave packets to the router. However, when operating in basic bridge mode, IGMP join and leave messages are not forwarded to other ports in the VLAN. The ONS 15302 supports dedicated forwarding tables for MAC layer multicast traffic and IGMP snooping. By enabling these features as follows, you can ensure that the IGMP packets are forwarded correctly.

Step 1 Step 1 To reduce the maximum number of VLANs to less than 4000 and make space available for the MAC multicast tables (this is a one-to-one relation, so for every VLAN you take off, you can have another multicast group entry), enter the commands:

\Services\Device-Tuning\General Vlan=3900

The device reboots.

Step 2 Step 2 To enable the MAC multicast feature, enter the command:

\Bridge\Multicast\parameters multicast=true

Step 3 Step 3 To enable the IGMP snooping feature, enter the command:

\Bridge\IGMP-Snooping\parameters IGMP=true

Now, when IGMP join messages are received from an end user, the transaction will be registered in the bridge and forwarded to the other ports in the VLAN. The related multicast traffic will now be forwarded only to the bridge port of the received the IGMP join message. IGMP leave messages will be forwarded only, and the registered IGMP entries in the bridge will time out (default 150 seconds). This issue will be resolved in a future release.

DDTS # CSCdz37795

A LAN port may lose traffic or packets when another LAN becomes congested, or packets otherwise overload the port. For example, connect two ONS 15302s (A and B) back to back. Set up a VLAN between A1 and B1 and another VLAN between A2 and B2. Run all ports in 100 MB mode with flow control on. Offer 30 MB from A1 to B1 and 30 MB from A2 to B2. Then reduce the B1 mode to 10 MB. Packet loss will be observed. To avoid this issue, do not use different speeds on the LAN-ports. Note that if the WAN capacity is lower than the slowest LAN-port, the issue will not occur (flow control will work). This issue will be resolved in a future release.

DDTS # CSCdz22948

The ONS 15302 cannot be provisioned with the same IP subnet on its management interfaces; for example, the management port and one or more of the DCC channels. All IP interfaces must be provisioned with a dedicated IP subnet. Introducing an ONS 15302 into an ONS 15454 topology where all the ONS 15454 management interfaces are on the same subnet, only one management interface of the ONS 15302 can be provisioned on that subnet. To work around this, provision the “ONS 15454 subnet” for the “A-DCC-R” interface, and provision a different subnet to the management port of the ONS 15302. This issue will be resolved in a future release.

DDTS # CSCdz26587

There is no immediate connectivity when managing an ONS 15302 via an ONS 15454 running proxy ARP. Add static routes on the management station or PC to work around this issue. This issue will be resolved in a future release.

DDTS # CSCdz26606

During failure in an ONS 15454 ring where static routes have been provisioned over the link that fails, the ONS 15302 loses connectivity due to an inability to interoperate with OSPF. If the ONS 15454 allows more than one static route to the same destination, but through different interfaces, then “back-up” routes can be provisioned to avoid this issue. This issue will be resolved in a future release.

DDTS # CSCdz34676

AIS is not transmitted to the E1 customer side after an LOSS on the far end. This is standard behavior according to PRA specification ETS 300-233. This caveat is informational only, and no change is planned for the ONS 15302.

DDTS # CSCee44539

SYSTEM-UP-TIME is incorrect . System- up- time should be able to store up- time up to approximately 497 days. Counters reset at approximately 40 days, causing the up time to display incorrectly. This issue is under ongoing investigation.

DDTS # CSCee44556

A restart is triggered when receiving a specific frame (BOOTP). An ONS 15302 connected to a common HUB via MNGT-port reboot after having been in operation for some time. ROS is sensitive to specific frames (BOOTP) and this causes a software restart. This vulnerability applies for all IP-addressed ports (LAN/WAN/MNGT). This issue is under ongoing investigation.

Workaround:

Turn off BootP messaging from the router (in this specific case).

DDTS # CSCee44553

"Ping events"are incorrectly described. When using the "ping utility" from CiscoEdgeCraft, if the ping is not successful, abortTftp events are reported. Tftp events are not relevant in this context. This issue is under ongoing investigation.

DDTS # CSCee44582

ONSCLI commands for IP DCN configuration are missing. ONS 15302s have numerous features for advanced configuration to achieve IP connectivity from a Network operation center. Current and previous versions of ONS 15302 SW do not provide commands in ONSCLI to manage routing tables and routing protocols supported by NEs.

Workaround:

Use CiscoEdgeCraft for IP DCN configuration.

This issue will be resolved in a future release.

DDTS#CSCee27998

Mismatch between 'Running SW Revision' presented during start-up and the actual software in the equipment.

Workaround:

Verify the SW-ICS by means of VT100 or CEC. For R1.0.1, the correct SW ICS is ICS08.

This issue will be resolved in a future release.

Resolved Caveats for Release 1.0.1

- ONSCLI Priority Group command has no meaning/function and is removed
- ONSCLI traffic class table handler improved
- ONSCLI fixed bug in printing the RMON and MIB2 counters
- RIP-enable status handling (after reboot) corrected
- Too many VT100 printouts on WAN-channel disable

- PM: PLM alarm used as defect criteria by mistake
- PM: FE mistakenly counts as UAS at NE defect if RDI is present when NE defect occurs
- False WAN-sequence fail alarm when connected to older VCTE-FPGA
- PM does not count SES/UAS at VC-12 UNEQ/TIM alarms
- SW-download automatic fallback mechanism corrected/improved
- DCC-R/M disconnect/reconnect on MSP-create
- VCTE-FPGA (High latency when higher traffic rate than WAN cap is sent)
- SNMP vulnerability changes
- Delete DHCP entry causes crash
- IGMP messages not forwarded
- 30 min Telnet timeout reduced to 30 seconds
- Un-initialized STP variable (non- connected port reported as forwarding)
- RIP initially distributes 0.0.0.0 route when enabled
- RipEnable setting is ignored on CDB download
- OSPF stub area: Default summary LSA not generated
- Forwarding of STP BPDU's when STP disabled
- IS-IS Multicast packets not forwarded
- Pause packets has SA MAC = 00:00:00:00:00:00
- STP topology change timer corrected
- Problem with RMON Counters wrap-around
- Nessus Security Scan issues solved
- Initiating Ping with packet size 1500 causes a fatal error
- Ping with large packets causes hang
- Forwarding of IS-IS and IGMP does not work if STP pr. VLAN
- IS-IS and IGMP packets forwarded when STP port in blocking mode
- After setting of path-trace transmit to all 0, watchdog timeout at next restarts
- Incorrect formatted log-file events
- Full traffic stop on the WAN port when the difference in the delay between the VC-12 with shortest delay and the VC-12 with longest delay becomes longer than 200 us.
- The aggregate port Rx-level is not shown when the port's operational status is down.
- The RS-SES and RS-UAS alarms do not increment to indicate error condition when injecting B1 errors at the rate of 10E-4. Behavior is correct when LOS or LOF is injected.
- MSP DNR (Do Not Revert) is not sent out after a manual clear when the device is operating in non-revertive mode.
- It was possible to manage the autonegotiation, speed and duplex mode parameters on the WAN ports. This does not make sense, since the WAN ports always operate with autonegotiation disabled, 100 MB and full duplex mode
- Flow control on WAN ports is always in status on after a device reboot
- Protection commands available in ONSCLI even if device is unprotected

- Command type noCommand should not be presented as an available option in ONSCLI help text for PROTECTION.SWITCHING-COMMAND
- Not possible to set Ethernet port's flow control mode to autoNeg
- FATAL ERROR on Set of local terminal password if the user is not a super user
- Problem with loss of packets when flow control is active
- VC-4 DEG/EXC alarms not reported when link2 disabled

New Features and Functionality

This section highlights new features and functionality for Release 1.0.x. For an overview of features of the 15302, consult the Cisco ONS 15302 Installation and Operations Guide, Release 1.0.

- Max Ethernet frame size increased to 6k
- Change default RIP-version per interface to RIPv2
- New WAN port alarm seqFail added.

Related Documentation

Release-Specific Documents

None.

Platform-Specific Documents

- Cisco ONS 15302 Quick Installation Guide, Release 1.0
- Cisco ONS 15302 Installation and Operations Guide, Release 1.0

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

http://www.cisco.com/univercd/home/home.htm

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpck/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Ordering tool:

  http://www.cisco.com/en/US/partner/ordering/index.shtml

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

You can send comments about technical documentation to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, Cisco Technical Support provides 24-hour-a-day, award-winning technical assistance. The Cisco Technical Support Website on Cisco.com features extensive online support resources. In addition, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not hold a valid Cisco service contract, contact your reseller.

Cisco Technical Support Website

The Cisco Technical Support Website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, 365 days a year at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support Website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool automatically provides recommended solutions. If your issue is not resolved using the recommended resources, your service request will be assigned to a Cisco TAC engineer. The TAC Service Request Tool is located at this URL:

http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco TAC engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)
EMEA: +32 2 704 55 55
USA: 1 800 553 2447

For a complete list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—Your network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

  http://www.cisco.com/go/marketplace/

- The Cisco *Product Catalog* describes the networking products offered by Cisco Systems, as well as ordering and customer support services. Access the Cisco Product Catalog at this URL:

  http://cisco.com/univercd/cc/td/doc/pcat/

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

  http://www.cisco.com/packet

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

  http://www.cisco.com/go/iqmagazine

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

  http://www.cisco.com/ipj

- World-class networking training is available from Cisco. You can view current offerings at this URL:

  http://www.cisco.com/en/US/learning/index.html

This document is to be used in conjunction with the documents listed in the Related Documentation section.