Release Notes for CISCO ONS 15305 Release 1.1.1

April 2004

Release notes address closed (maintenance) issues, caveats, and new features for the Cisco ONS 15305. For detailed information regarding features, capabilities, hardware, and software introduced with this release, refer to Release 1.1 of the Cisco ONS 15305 Installation and Operations Guide. For the most current version of the Release Notes for Cisco ONS 15305 Release 1.1.1, 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 15305 Release 1.1.1* since the production of the Cisco ONS 15305 System Software CD for Release 1.1.1.

No changes have been added to the release notes for Release 1.1.1.

Caveats

Review the notes listed below before deploying the ONS 15305. 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 # CSCea33196

Unfair distribution of intermodular traffic with flow control can occur. If traffic is sent from several ports in different modules and flow control is active, traffic throughput is less for ports belonging to same module as the congested.

Typical scenario:

Port 2 module 1, port 1 module 2 and port 1 module 3 send 100Mb traffic streams to port 1 module 1. All ports have flow control enabled. The result is that more traffic is sent from the ports in module 2 and 3 compared to what is sent from the port in module 1. No packet loss from any module occurs. This issue will be resolved in a future release.

DDTS # CSCea33337

Port priority is not strictly enforced when flow control is on. This can occur under the following

conditions.

The four input ports are set for 100 MB (64 bytes).

- Port 1 priority is set for 6
- Port 2 priority is set for 4
- Port 3 priority is set for 0
- Port 4 priority is set for 1

VLAN tagging is turned off for all of the FE ports while VLAN tagging is turned on for the STM1 trunk port. (This adds an additional 4 bytes to each stream.) Flow control is turned on for all the FE ports When all the ports are turned on, only Port 1 should have priority. Instead, traffic is received on both Ports 1 and 2 at almost 60/40% on each port (81,168 versus 60,876). This issue will be resolved in a future release.

DDTS # CSCeb22543

On 8xSTM1 cards there may be packet losses for LAN traffic mapped on STM1, and "DXC inlet bit error alarm" conditions may be raised, when 8xSTM1 cards are exposed to extreme temperature cycles (-5 to 50˚C with 2 hours dwell at each extreme temperature, and 1˚C/min gradients). The packet losses and raised condition can occur on the 8xSTM1 card. This only occurs under temperature stress. The frequence with which the issue has been observed is an average of 10 packets lost, and less than 100 alarms recorded in a 12 hours cycle. No failures have been detected in nominal conditions.

DDTS # CSCea71600

When power cycling (power on/off at different termperatures) the 8xSTM1 card, the card may fail to recover operation after the power on/off, and may remain in an alarmed state without carrying traffic. In this case the card indicates "DXC inlet failure alarm." The card's LED will also be red. The card recovers normal operation after a software reset. This issue occurs approximately one out of every 20 power on/offs.

DDTS # CSCea31245

If you send 100 MB from two ports to a single port (for example, to test flow control), 64 byte packets are lost. If you increase the size to 75 bytes, packets are no longer lost. This type of traffic is not, however, typical for a device in normal operation. This issue will be resolved in a future release.

DDTS # CSCea33042

Same priority and same packet size may yield different traffic flows. When four streams are set up and each has the same packet size (64 byte) going across a 100 MB STM-1 path to another ONS 15305, each of the streams can be off as much as 50%. This is not always the case, however. Sometimes the traffic can be equally distributed. Using random packet sizes, the distribution tends to be more equal. This type of traffic in not typical for a device in normal operation; however, the issue can occur in a lab test. This issue will be resolved in a future release.

DDTS # CSCea33354

If a mirrored port becomes congested and flow control is enabled, no pause packets are generated toward ports belonging to other modules. Flow control fails when ports used for mirroring become congested. If traffic to a mirrored port is sent from a LAN port situated in a different module from that of the mirrored port, pause packets are not received and mirrored packets are lost. Actual traffic flow is not disturbed by the mirrored port flow control problem, and the copy port traffic is handled correctly. This issue will be resolved in a future release.

DDTS # CSCee44527

GE-port does not handle traffic in FIBER mode when AUTONEG is ENABLED. The gigabit Ethernet port does not handle traffic when media type fiber is used and autonegotiation is enabled.

Workaround:

Set the administrative speed to 1000 MB and disable autonegotiation on the gigabit Ethernet port if fiber link is used.

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 # 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 # CSCee44556

A restart is triggered when receiving a specific frame (BOOTP). ONS 15305-s 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 # CSCee44563

A GE-port reports incorrect media/connection-type.Under certain circumstances, the media type and connector type reported for a GE-port might be wrong if the GE-module is put in traffic while the cable is in and the peer is ready to bring the link up. The issue is not traffic-affecting, and the port's Operational Status is "up." Inconsistency might occur if the link comes up very fast, and after that the module is put in traffic. The inconsistency has been observed if autonegotiation is disabled and the media type is fiber (speed is set to 1000 MB). If the module is put in traffic while the fiber is plugged in and the peer is ready to bring the link up, the media type might be reported to be copper and the connector type to be RJ45 (instead of the correct values of fiber and fiberLC respectively). This issue is under ongoing investigation.

Workaround:

Provoke a link-down link-up transition (remove and reinsert the cable force wrong port-speed and reset back to the correct port-speed). When the link comes up again after having been down for a few seconds, the reported media/connection-type will be correct.

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 either VT100 or CEC. For R1.1.1, the correct SW-ICS is ICS06.

This issue will be resolved in a future release.

Resolved Caveats for Release 1.1.1

The following caveats were resolved in Release 1.1.1

- Restore CDB does not complete successfully when the CDB backup is taken on a device running R1.0 the CDB contains "DccChannelMode" settings.
- Optical link on GE port does not come up if autonegotiation disabled and speed 1000
- STM16 module - OOF/LOF when setup as VC-4-4C (new STM16 module-file)
- Memory corruption (sDxcTu12Connections table in DXCT.c)
- Too short GALNET reset

New Features and Functionality

This section highlights new features and functionality for Release 1.1.x. For an overview of features of the 15305, consult the Cisco ONS 15305 Installation and Operations Guide, Release 1.1.

The following new module types have been added for Release 1.1.

- Single optical L-16.1 module (L16.2-1-LC) (Long Haul)
- Dual optical L4.2 module (L4.2-2-LC) (Long Haul)
- Dual Optical S1.1 + 21xE1 module (S1.1-2-LC/E1-21)
- Power Module, AC 230V

The following additional features have been added for Release 1.1.

- New MIB-variables for 230VAC Power Module Alarms
- Remove VLANs before Module Disable (as with XC etc.)
- Improved module diagnostics
- Updated SETS fpga and software support (synchronization)
- Transparent DCC

Related Documentation

Release-Specific Documents

None.

Platform-Specific Documents

- Cisco ONS 15305 Quick Installation Guide, Release 1.1
- Cisco ONS 15305 Installation and Operations Guide, Release 1.1
- Cisco Edge Craft, Software Guide

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.