Release Notes for Cisco ONS 15302 Release 2.0.2

June 2005

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 2.0 of the Cisco ONS 15302 Installation and Operations Guide. For the most current version of the Release Notes for Cisco ONS 15302 Release 2.0.2, 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 2.0.2* since the production of the Cisco ONS 15302 System Software CD for Release 2.0.2.

No changes have been added to the release notes for Release 2.0.2.

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 # CSCei15120

Incoming IGMP packets are VLAN-tagged, and hold the VID of a VLAN that is configured on the device. The ingress port is not a member of a named VLAN. In some rare configurations this could create a loop in the topology, and a storm of replicated IGMP packets. The IGMP packets reach the VLAN even though the ingress port is not member of the VLAN. Thus VLAN-tagged IGMP packets bypass ingress filtering.

Workaround

There is usually no need for a configuration that allows this to happen.

Verify that the VLAN configuration in the topology is consistent and does not contain any partially configured links. This issue is under investigation.

DDTS # CSCei15125

Changing the system mode from IP (default) to IP unnumbered can result in problems.

Release 2.0 software is limited with respect to changing the system mode from IP (default) to IP unnumbered.

Even though there are IP addresses and routing protocols configured on an NE the operator does not receive any notification. Notification could enable the operator to forestall the change until necessary configuration changes have been made.

From a software design point of view, the configuration of system mode for DCN routing is seen as a strategic choice, which the operator should configure prior to configuring the IP address and protocols on the device. The reason for this is that the network design is different for each of the system modes.

The consequence for changing the system mode from IP to IP unnumbered is complicated and severe problems can result if handled incorrectly. In the worst case, you might not be able to regain IP connectivity to the NE.

Workaround

Generally, the safest alternative is to erase the configuration prior to changing the system mode. If you do not wish to lose your configuration, however, the following steps have proved successful.

Step 1 Locally connect to a MNGT-port and connect with CiscoEdgeCraft.

Step 2 Remove all IP addresses in the IP interface table except for the MNGT-port address (IF=1000).

Step 3 Remove all static configured routes (even the 0.0.0.0 route).

Step 4 Disable active routing protocols (RIP and/or OSPF).

Step 5 Locally connect to the device via ONSCLI (VT100).

Step 6 Remove the IP address assigned to the management port (ONSCLI>ip ip=0.0.0.0 sub=0.0.0.0).

Step 7 Set the system mode to IP unnumbered (IPUN) and reset the device.

Step 8 Change the IP address (MNGT-port) to fit your new network design and reconfigure the SNMP community.

Step 9 Reconnect to the device with CiscoEdgeCraft.

Step 10 Commission IP unnumbered configuration; IP over PPP (DCC), OSPF, etc.

Note This procedure cannot be obtained via remote access to the network element.

Resolution

N/A

DDTS # CSCeg59263

When operating in L2 mode, Ethernet frames with MAC destination address in the range 01:80:C2:00:00:10 to 01:80:C2:00:00:FF are not correctly filtered due to limitations in the switch ASIC. Special steps are taken to forward 01:80:C2:00:00:14 and:15 (IS hello), but 01:80:C2:00:00:14 and:15 are not forwarded if one is employing Provider VLAN by using Ethertype 0xFFFF (legacy provider VLAN). The condition for this issue is to have legacy VLAN tunneling in use.

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 # CSCeg59341

Incorrect SYSTEM-UP-TIME. System-up-time should be able to store up-time up to approximately 497 days. Experience shows this counters wraps around well before (appr. 40 days). Ongoing investigation.

DDTS # CSCeg59350

Incorrect description of “Ping events”. When using “ping utility” from CiscoEdgeCraft, and the ping is not successful, abortTftp events are reported. Tftp events are not relevant in this context. Ongoing investigation.

DDTS # CSCeg59356

In some cases the different priority tags of frames going out on WAN ports are ignored. This will be the case when the number of VC-12s allocated to a WAN port is less than 47 (i.e. the capacity of the WAN link is less than 100Mbit/s). The switch sees the wan port as an FE port, and will not see the need for prioritizing between the frames. Thus adapting the traffic to the actual bandwidth is handed over to the FPGA mapping the frames into SDH.

Workaround

Solved for 2xGE + SMAP and 8xFE + SMAP modules.

DDTS # CSCeg59367

The device restarts when disabling OSPF if stub area exists.

DDTS # CSCeg59373

Administratively set a value for Unicast-Global-Forwarding Table causes device restart.

If configuring a value for Unicast-Global-Forwarding table “AfterReset” lower than the number of static entries in the table, and then select software reset for the device, a device restart will be experienced.

Workaround

Avoid configuring a lower number than statically configured in the Unicast-Global-Forwarding table.

DDTS # CSCeg59382

When aging time is set above 650 seconds, it will still start at 650 seconds. This issue is observed when the following are executed:

- Fill the forwarding table using SmartBits to generate different source addresses (default forwarding table size is 8192).
- The default aging time is 3600, but still the number of entries in the table starts to reduce at approximately 650 sec.

DDTS # CSCeg59390

If both RSTP and GVRP run simultaneously, a device-restart may be experienced when disabling GVRP.

Workaround

RSTP must be disabled before disabling GVRP.

DDTS # CSCeg59396

The protocol tunneling works for VTP, CDP and RSTP protocols, but is not able to tunnel normal STP packages. This issue will be resolved in an upcoming release.

DDTS # CSCef88892

When first configuring IP numbered DCN management link between ONS15302 and ONS15454SDH, the link may not come up.

Workaround

For the DCN link to come up, toggle the mode field on ONS 15302, from “IpOverDcc” to “Not Used” then back to “IpOverDcc.”

Resolved Caveats for Release 2.0.2

The following issues are resolved as of Release 2.0.2

- DDTS # CSCeg59396; STP protocol packages are not tunneled through an ONS 15302. Other protocols, such as VTP, CDP and RSTP are tunnelled properly through the ONS 15302.
- Packet buffer hang. No traffic is running on WAN port in the receiver direction, towards the switch port. There are no alarms or other symptoms on a failure. The error is not present on WANx ports.
- Flow control enable/disable. Flow control is not disabled on the SDH side of the WAN port when flow control is disabled on the Switch side of the WAN port. The flow control packets will be dropped in the switch, and therefore the user will see no difference in the behavior.
- Pause packet detection. Packets with multicast address 01-80-C2-00-00-01 but with length/type field different from 8808 and control opcode field different from 00-01 may be misinterpreted as pause packets, and therefore lead to reduced link capacity on links where flow control is enabled
- PM data collection. False G.826 performance errors may be reported on VC-channels in a VCG connected to a WANx port. The error was only present on the WANx port on the new R2.0 GFP-WAN module.
- RDI generation. When the optical input signal is removed RDI shall be generated on the outgoing VC-12 containers on the WAN port, the RDI generation was not stable, resulting in a fluctuating operational WAN capacity in the remote end. The error is not present on WANx ports.
- Priority to queue mapping. 802.1p did not work properly for WANx ports.
- Don't allow selecting SDH Port2 as sync source on unprotected device.
- GALNET diagnostics incorrectly report error.
- Receiving OSPF LSA-update on the MNGT-port lead to reboot. (IPUN only).
- Configuring path-trace for a WANx-port could not be issued from ONSCLI.
- Invert alarm-output port driving (align with ONS 15305).
- Correct Temp-Serial-Buffer usage, possible device reboot when VT100/Mngt-port is connected.
- The metric displayed in routing table is 110 independent of hop count to destination address for routes learned via the OSPF algorithm. (IPUN only).
- Protocol tunneling correction. (CiscoEdgeCraft R2.0 or newer is required for this feature).

- There was a possibility for generation of CRC-errors when flow control is disabled on WAN-port.
- There was a possibility that a WANx- port could stop forwarding traffic, and continuously send pause frames out on the link.
- When sending Ethernet frames over 46 or more VC-12s, there was a drastic reduction in throughput when flow control was enabled (WANx-port).
- When sending Ethernet frames over proprietary mapping (WANx-port), the performance was lower than on WAN-port due to the fact that 8 HDLC flags were inserted between frames instead of 1 HDLC flag.
- The GFP FCS error counters did not count correct.
- Extended Signal Label not presented correctly (CiscoEdgeCraft R2.0 or newer is required for this feature).
- Correct Trail Signal Label decoding (VCAT-VC12) in ONSCLI.
- Certain types of LSAs entering a ring of NEs running OSPF over IPUN interfaces provoked restart of the NEs (due to endless circulation).

The following issues are resolved as of Release 2.0.

- Cannot provision same IP subnet on common PPP link.
- Proxy ARP on the ONS 15454 is not supported by ONS 15302.
- ONS 15302 does not interoperate with OSPF causing DCC failure.
- POS, ATM, and gigE is broken in 11/11 GSR conn_isp image.
- Bridge blocks IGMP message.
- Other Lan port loss traffic when another Lan get congestion.
- Cosmetic code refinement suggested by code review.
- cnfvifccprof fails for rep more than 32 due to indexing problem.

New Features and Functionality

This section highlights new features and functionality for Release 2.0. For an overview of features of the 15302, consult the Cisco ONS 15302 Installation and Operations Guide, Release 2.0.

The following new module types have been added for Release 2.0.

- New WAN mapper module to support standard Ethernet over SDH (EoS).

The following additional features have been added for Release 2.0.

- VCAT on VC-12 and VC-3 for ports on new module (WAN module GFP).
- GFP-F for ports on new module (WAN module GFP).
- Soft LCAS bidirectional for ports on new module (WAN module GFP).
- Standard LCAS for ports on new module (WAN module GFP).
- IP unnumbered for management connectivity. Introduced as System mode for MCN configuration. Needs to be set in ONSCLI since:
  - It is a strategic choice for IP configuration
  - Planning of MCN.

- Provider VLAN (QinQ), Ether type 8100, is supported for ports on new module (WAN module GFP).
- Protocol Tunnelling.
- IP In-band solution for management connectivity when L1 mode is used for Ethernet transport. Configurable modes: 192kbit/s or 512kbit/s.
- OSPF interoperate with ONS15454SDH on DCN architectures.

The following miscellaneous features have added for Release 2.0.0.

- NE “running status” commands added in ONSCLI.
- Correlated status of LAN and WAN-ports (When WAN-port “down” LAN-port is “down”).
- WAN Port “down” alarm
- DCC Termination Failure. CSF alarm is now supported for all DCC encapsulations supported.
- Telmon debug counter visibility in ONSCLI.
- Configurable CRC 16/32 in DCC for PPP encapsulation.
- Support for PPP encapsulation also in DCC-M.
- PDH PM counters for E1 ports (in PRA mode)
- Support of S1 byte in SDH, (do-not-use command).

General improvements/enhancements

- Improved optical level presentation when LOS. Displays now ---
- Optimized buffer handling in NE for sending traps to manager.
- Rx-sequence number added per VC-12 on WAN-port (Troubleshooting in case of Seq-fail alarm)
- Revert option for software introduced as switch-bank selection when restarting NE.

Related Documentation

Release-Specific Documents

- *Release Notes for Cisco ONS 15302 Release 2.0*
- *Release Notes for Cisco ONS 15305 Release 2.0.2*
- *Release Notes for Cisco Edge Craft Release 2.0.1*

Platform-Specific Documents

- *Cisco ONS 15302 Quick Installation Guide, Release 2.0*
- *Cisco ONS 15302 Installation and Operations Guide, Release 2.0*

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

Documentation DVD

Cisco documentation and additional literature are available in a Documentation DVD package, which may have shipped with your product. The Documentation DVD is updated regularly and may be more current than printed documentation. The Documentation DVD package is available as a single unit.

Registered Cisco.com users (Cisco direct customers) can order a Cisco Documentation DVD (product number DOC-DOCDVD=) from the Ordering tool or Cisco Marketplace.

Cisco Ordering tool:

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

Cisco Marketplace:

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

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/

- 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 1 800 553-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.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you can perform these tasks:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL:

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

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies—security-alert@cisco.com
- Nonemergencies—psirt@cisco.com

Tip We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.*x* through 8.*x*.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one that has the most recent creation date in this public key server list:

http://pgp.mit.edu:11371/pks/lookup?search=psirt%40cisco.com&op=index&exact=on

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

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

Note Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support Website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

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 provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is 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/

- *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.