Release Notes for Cisco ONS 15305 Release 2.0.3

August 2006

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 2.0 of the Cisco ONS 15305 Installation and Operations Guide. For the most current version of the Release Notes for Cisco ONS 15305 Release 2.0.3, 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 2.0.3* since the production of the Cisco ONS 15305 System Software CD for Release 2.0.3.

No changes have been added to the release notes for Release 2.0.3.

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.

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

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.

CSCeb22543

The failure is present in different corners and at different temperatures. We have Errors (#14 B3 errors in 24 hour of test, #1 Loss of Pattern) on a STM-1 link with #3 8xSTM-1 modules. We records also packet lost on a FE link mapped into STM-1 optical path. When these errors / packet lost happens, we record from Cisco Craft a lot of “DXC inlet bit error” alarms. No other type of alarms has been recorded from the Cisco-Craft. All these 3 event happens at the same time, so the root cause should be the same.

CSCea71600

The fail is related on module 8xSTM-1. During EDVT corner 5 & corner 7:

Corner 5: power supplies on the modules at -5% except power supply DC-DC module at +5%, Temperature= +50˚C

Corner 7: each power supplies at -5%, Temperature= +50˚C this module does not starts. This cause fail on the traffic path related to this modules.

The number of fails is:

- C5:board_3 module 8xSTM-1 SN0307008095, 2 times / 10 tests
- C7:board_3 module 8xSTM-1 SN0307008095, 1 time / 10 tests
- C7:board_4 module 8xSTM-1 SN0303006397, 1 time / 10 tests

When this fail happens, record the following alarm from the Cisco EdgeCraft:

“slot3 inlet Fail DXC inlet failure”.

64 byte packets are lost when testing flow control

CSCea31245

Conditions:

When sending 100 Mb from two ports to a single port, the packets are lost when the size is 64 byte. When the size is increased to 75 byte, the packet loss goes away

Workaround:

This type of traffic is not typical for a device in normal operation but it can occur in a lab test setup

Resolution:

None

CSCea33354

No pause packets received on ports sending traffic to a congested mirrored port.

Conditions:

If a mirrored port becomes congested and flow control is enabled, no pause packets are generated toward ports belonging to other modules. Flow control is not working properly if ports used for mirroring become congested. If traffic to a mirrored port is sent from a LAN port situated in a different module than the mirrored port pause packets are not received and mirrored packets are lost. The real traffic flow is not disturbed by the mirrored port flow control problem, and the copy port traffic handling is working fine.

Workaround:

None

CSCeg58254

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 0 1:80:C2:00:00:14 and:15 (IS hello).

01:80:C2:00:00:14 and:15 are not forwarded if one is employing Provider VLAN by using Ethertype 0xFFFF (legacy provider VLAN).

Conditions:

Legacy VLAN tunneling in use.

Workaround:

Use protocol tunneling supported by 2xGE + SMAP and 8xFE + SMAP to provide transparent Ethernet (with or without provider VLAN).

CSCea33042

Same priority and same packet size yields different traffic flows.

Conditions:

There are 4 streams setup each has the same packet size (64 byte) going across 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, sometimes the traffic can be equally distributed. However, using random packet sizes, the distribution seems to be more equal.

Workaround:

This type of traffic in not typical for a device in normal operation, but it can occur in a lab test setup.

Resolution:

None

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.

CSCeg58273

AbortTftp events reported on unsuccessful ping.

Conditions:

When using \223ping utility\224 from AXXCRAFT, and the ping is not successful, abortTftp events are reported. Tftp events are not relevant in this context.

Workaround:

None.

CSCeg58278

802.1p does not work satisfactorily for WAN ports on 4xFE+4xMAP, 8xSTM-1+8xMAP and 8xMAP modules.

Symptom:

In some cases the different priority tags of frames going out on WAN ports are ignored.

Conditions:

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 100M it/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.

Resolution:

Ongoing investigation.

CSCeg58312

Max aging time is 650 sec.

Symptom:

When the setting for aging time is set above 650 seconds, aging still starts at 650 seconds.

Conditions:

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

Workaround:

None.

CSCeg58361

Unnecessary LINK_DOWN events reported in history after boot/restart.

Symptom:

DCC Link “down” events reported in “notification history” after boot.

Conditions:

All DCC channels, even if not represented by DCC applicable HW, reports LINK “DOWN” in notification history after device power up (restart).

Workaround:

None

Resolution:

Ongoing investigation.

CSCeg58388

Device reboots if switching OSPF InterfaceType from “point-to-point” to “broadcast,” or if disabling OSPF while InterfaceType is “point-to-point”. This issue is observed when OSPF is enabled, the OSPF Interface table is populated and the InterfaceType of an entry in the OSPF Interface table is changed to “point-to-point.”

Workaround

Restore a CDB-backup without the incorrect interface type configured. If you don't have such a CDB-backup, SUPPORT can assist in modifying the CDB-backup of your current configuration.

CSCeg58398

Device initiates an additional boot sequence when restarted after CDB-restoration, to clean up invalid configuration data, after which the ProviderTags parameter is set to “disabled.”

VLAN membership or tag status of an Ethernet port has been changed after the parameter ProviderTags has been enabled, and the device has been rebooted (due to software/firmware upgrade, or restore of configuration database).

Workaround:

Disable ProviderTags parameter when removing the port from the VLAN or changing its tag status.

CSCef88892

When first configuring IP numbered DCN management link between ONS 15305 and ONS15454SDH, the link may not come up.

Workaround:

For the DCN link to come up, one must toggle the mode field, on ONS 15305, from “IpOverDcc” to “Not Used” then back to “IpOverDcc”.

CSCeg11010

Some dccR and dccM Mode field may reset to “Not Used” after upgrade to R2.0 in IP numbered mode.

Workaround:

Mode fields for all pre-provisioned dccR and dccM must be revisited and reconfigured for “Poverty”.

CSCeg11478

Reverting from R2.0 back to R1.1.1 will fail.

Workaround:

The following procedure must be used to successfully revert back to Release 1.1.1, after upgrading to release 2.0:

1. Main card firmware, 45004-70AA_PM_ ED05.bin, must be uploaded first.
2. Software file, 45004-77AB_PM_ED06.bin, must be uploaded.
3. Definition file, 55004-01AB_PM_ED06.def, must be uploaded.

CSCeg45943

The Mac table overflow “Duration Timer” does not increment.

After overloading the forwarding database a “bridge table overflow” occurs, but the duration of the condition stays at 0h 0m 0s.

Resolved Caveats for Release 2.0.3

The following caveats are resolved as of Release 2.0.3.

- CSCsd46155—The maximum value of the Time Protocol interval is 1080 minutes, rather than 1440 minutes.
- CSCse88569—Ethernet management port block issues.
- CSCse44755—In a 2 by 14 configuration some FE10/100 WAN ports remain in the down state.
- CSCei15120—The incoming IGMP packets are VLAN-tagged, and holding the VID of a VLAN that is configured on the device. The ingress port is not a member of named VLAN. In some rare configurations this could create a loop in the topology, and a storm of replicated IGMP packets. The IGMP packets reaches VLAN even though the ingress port is not member of the VLAN. Thus VLAN-tagged IGMP packets bypass ingress filtering.
- CSCeg58260—System-up-time value rolls after approximately 40 days, rather than 497 days.
- CSCeg58295—Disabling OSPF caused device-restart if Stub area existed. (IP-Numbered mode only).
- CSCeg58300—Static Unicast Table (number of entries) caused device-restart. Administratively set a value for Unicast-Global-Forwarding Table caused device restart.
- CSCeg58361—Unnecessary LINK_DOWN events reported in history after boot/restart.All DCC channels, even if not represented by DCC applicable HW, reports LINK “DOWN” in notification history after device power up (restart).
- CSCeg58372—If both RSTP and GVRP ran simultaneously, a device-restart could be experienced when disabling GVRP.
- DCN (IP/IPUN): Code error for the HDLC driver caused loss of management connectivity. An error was introduced in March 2006, which could cause loss of management connectivity (IP and CLI). The problem was detected in a setup, which combined MSP (1+1), PPP/DCC and OSPF.
- DCN (IP/IPUN): Interop issue for PPP over DCC. The PPP stack in previous releases had an error in the processing of unsupported PPP LCP options in the PPP stack. The error caused that the PPP link would never come up (persistent CSF alarm) because of peer support PPP LCP options that the ONS 15305 does not support.
- Intermittent power module out alarm(s). Power module out alarms were raised and cleared after a NE restart.When power alarms are enabled for the power module(s) equipped in ONS 15305, a raised and cleared power module out alarm occurred after software reset.
- Software download flash failure. To prevent SWDL-lockup, downloading processes have been improved, by a time-supervision mechanism.
- RMON probes on Ethernet ports could cause restarts.Adding RMON probes on LANX-ports, that are not yet physically equipped and known by the system, will provoke a device-restart. The RMON-probe validation process is now extended with additional check to verify whether the port is physically equipped and known by the system.
- Ethernet: Correlation of WANx- and WAN alarms. In previous releases WANX specific alarms were reported against WAN-port, this mapping is now corrected (ref. source-field in the alarm-list view).

- Ethernet over SDH: Persistent WrongSeqChannel alarm for Proprietary mapping (MAJOR). There was a chance that a full stop of traffic could occur for the proprietary mapping. The situation was triggered by an SDH error present for a very short period of time on one or more of the involved channels, e.g. incidents on intermediate nodes or SNCP switching. The condition was recognized by a persistent WrongSeqChannel alarm reported for one of the VC's in the group. In addition the port was reported “down” and the operational bandwidth reflected the administratively set bandwidth (1-50 VC-12s). The remedy was to set bandwidth to 0 and return it to desirable bandwidth again (on opposite WAN(x)-port).
- SDH: T0 Holdover was reported after a software reset. Previous software versions have implied a T0 holdover stage for a period after software reset. From this version and onward this will not occur.
- SDH: T0-sync entries (E12/EXT) had default SSM-enabled setting. When adding E12/EXT sync references in the T0-table, the SSM field was always set to ENABLED. Since this field has no meaning for these selected ports (E12/EXT), the default value is now changed to DISABLED.
- SDH: Change of threshold for pointer justification alarm reporting. In previous releases the Epj alarm was reported for a threshold 100 justifications within a 15 minutes interval. This low threshold caused that alarms was present for links even though the SDH traffic did not suffer severely. The threshold for this release and onward introduce now a greater threshold (30000). If it's desirable to keep a low threshold for raising Epj alarm the operator may configure this from CiscoEdgeCraft.
- SDH: Software restart could cause a short interrupt of SDH traffic being transported by STM-4 and/or STM-16 aggregates. (MAJOR). A software error could cause a short traffic interruption (milliseconds) for SDH traffic (VC's).
- SWDL: Improved Swdl triggering. (MAJOR). The SNMP set swdlTrigger operation made faster, reducing re-entrance / conflict possibilities.
- Improved process prioritizing to avoid conflicts causing software restart. (CRITICAL). All priority 3 processes moved up to priority 4. Now WatchDog and ONSCLI processes can run when other priority 4 tasks are heavily loaded. Enabled 'time-slice' on ONSCLI process, so that WatchDog handler can run during ONSCLI 'running-config' execution. Refine UpdCDB handling (flow control parameter setting), not putting extra background load onto the system.
- Improved diagnostics in ONSCLI to determine fault conditions and configuration issues.Minor corrections for status reports in running-config. Minor corrections in the logging of boot-up sequence stored as a part display-debug-info command (added ReasonForBoot).Minor corrections for RIP parameters display. Reduce information dumping in running-config command (MAC-addr. table / Alarm log).
- Correct MNGT-port disable/enable handling. Management port recovers (without the need of removing/reinserting the cable) when disabled and enabled again from ONSCLI.
- DCN (IP/IPUN): Added O-bit in Hello (similar to DD-packets). Interoperability issue.
- Ethernet: Spontaneous restart triggered when receiving a specific frame (BootP). (MAJOR). An ONS 15305 connected to a DCN via any IP addressed Ethernet port rebooted after have been in operation for some time. The root cause was vulnerability for a specific BootP frame. The following reason for boot could be captured from VT100 during the restart:
  `FATAL ERROR: DHCP: Excm-CommonExceptionHandler - dump call-stack (?)`
- Ethernet: IS-IS multicast frames are not properly filtered. (MAJOR). The Ethernet switch discarded large IS-IS multicast frames. Originally frames with destination MAC address 01:80:C2:00:00:14 and :15 have to be forwarded by the CPU due to ASIC limitations. A software fix introduced in March 2005 for a MTU issue to resolve problems with IP connectivity in a large scaled DCN introduced the problem. This fix caused IS-IS multi-cast frames of sizes above 1500 was not properly forwarded anymore.

- Software default parameter changes: AlarmReporting for traffic modules changed from disabled to enabled [1]. EgressSSM for S1 byte changed from DoNotUse to T0 [2]. Default ageing time for bridge changed from 3600 sec to 300 sec (recommended by 802.1D)
- Change for default severity of Epj alarm condition(s). Release 2.0 for ONS 15305 introduced an alarm to identify frequent pointer adjustments per configured AU-4 and/or AU-4-4c. The alarm is identified as Excessive Pointer Justification (Epj) in CiscoEdgeCraft, and is by default raised if number of justifications per 15 minutes interval is greater than 100. In order to clear Epj alarm(s) the operator may increase the threshold for alarm reporting or make sure that the network is properly synchronized. The default severity for this alarm was “Major” even though the traffic seldom is affected. This alarm will from now on have the severity “Warning”. If desirable by operator to keep “Major” as severity for this alarm, it is possible to change this in the alarm config-table available from the device menu in CiscoEdgeCraft.
- Improved diagnostics in ONSCLI to determine fault conditions and configuration issues. More information in running-config command (optical Rx, PM, SDH-port status, etc.). Miscellaneous corrections for status reports in running-config. Log of boot-up sequence is now stored as a part display-debug-info command.Extended diagnostics for HW (SPI bus, VBAT, SETS FPGA)
- Interrupt avalanche when Optical loop on selected sync-source.When an optical loop was in place for a SDH-port, which was a preferred sync-source, the operator could experience reduced system performance. The CPU could be kept busy and no response from CLI and no IP connectivity could be the result from this vulnerability. The problem could be experienced for the following conditions:
  - STM-n port defined as T0 sync source (SSM enabled)
  - STM-n port Egress SSM = T0
  - STM-n port looped optically
- Hanging power-alarms when changing power-modules.When changing from the 230VAC power module type to the 48VDC kind, the operator would observe “hanging” alarms (-input low) referred for the previous module type (230VAC).
- Changing IpmFftMaxEntriesAfterReset did not prompt operator to software restart the node to activate configuration. CiscoEdgeCraft will prompt user that restart is required to apply change in configuration.
- CDB-restore provokes FATAL-ERROR (provider-tag enabled). (MAJOR) Latest CiscoEdgeCraft release resolves this issue by enhanced logic and sequence control.
- DCN (IPUN): Lost IP connectivity in multiple OSPF areas. (MAJOR). When the IP unnumbered network running OSPF with multiple areas, the operator could experience randomly that the IP connectivity to NE's in other areas is lost.
- DCN (IPUN): Incorrect ospf -> areaInterface table content. If changing the IP address on a node running IP unnumbered mode, the OSPF interface table incorrectly displayed the old IP address for the active instances listed in the table.
- DCN (IPUN): Change of IP (in ONSCLI) was not possible when OSPF were enabled In previous releases for an ONS 15305 running system mode IP unnumbered it was not allowed to change the IP interface of the node without temporarily disabling OSPF.

1. The default changes for alarm reporting may highlight formerly suppressed conditions for your installation. I.e. if you for previous software level(s) have not changed these parameters, you may recognize alarms after the upgrade, which you suppressed before.
2. In previous releases DoNotUse has been the default configuration for the S1 byte (active when SSM is enabled). Feedback from customers has triggered a change for this, and from this release and onward, T0 will be the default value. If your network synchronization scheme requires DoNotUse for any SDH-ports, make sure to set the parameter in configuration file prior to upgrade to this release level

- DCN (IPUN): NE reboots when adding OSPF area number 8. (MAJOR). The maximum areas to be configured for IP unnumbered are 8. A software code error caused a spontaneous restart when adding the 8th area.
- DCN (IPUN): Removed the gateway owner command for nodes without L3 lic.
- DCN (IPUN): Loss of management connectivity. Routing cease to work. (MAJOR). One or more OSPF topology changes will trigger the problem, and may cause loss of management connectivity to one or more NE's. The “lost nodes” are random and may occur on any node running OSPF in the topology. This is a severe DCN problem and all nodes running IP unnumbered with OSPF enabled should be upgraded.
- DCN (IPUN): Node not reachable after software reset. When the node is running in IP unnumbered mode and IPUN gateway is disabled, the operator could experience that the node was not reachable after software reset when connected to the MNGT-port. A manual flush (arp -d) of ARP table on the connected computer recovered connectivity. The manual flush of arp table in PC is no longer required since a solution is implemented in this release.
- DCN (IPUN): “IP address already in use” is reported on PC. This may be experienced for a NE, which is configured to system mode IP unnumbered and “IPUN Gateway” is disabled. If the PC was connected to the MNGT-port and a change was applied for the IP configuration of the PC, e.g. change of IP address, the operator could experience “IP address already in use”. An improvement in the ARP proxy software improves this and makes the IP addressing more convenient.
- DCN (IPUN): The IPUN router could cause severe IP problems in a LAN. (MAJOR). The ONS 15305 management port is connected to the LAN. System mode is IP unnumbered and “IPUN Gateway” is disabled.After some while the IP unnumbered configured node takes ownership for all potential IP addresses in the LAN. The network could not be recovered before the MNGT-port was disconnected from the LAN and other router ARP tables was flushed and/or aged out. An improvement is added in the ARP proxy software to avoid this for the future.
- DCN (IP/IPUN): L1CC (inband) ports now support CSF alarm condition (CiscoEdgeCraft) No alarms were reported for L1CC in previous releases for R.2.0 of ONS 15305. This made troubleshooting difficult.
- DCN (IP/IPUN): IP Inband (L1CC) did not work for 2xGE_SMAP in mode 192 kbit/s.The L1CC (L1 Ethernet Communication Channel) configured in 192kbit/s mode (DCC-R equivalent) did not work properly.
- DCN (IP/IPUN): PPP/DCC problem with SDH loop-back Looping a SDH interface with a DCC channel configured in PPP mode will as expected cause the link to go down. When the loop is removed, and the SDH link re-established, it is expected that the PPP connection will be re-established, but it was not. The PPP link remained in down state, hence no communication over the link was possible.
- DCN (IP/IPUN): Change of DCN system mode should raise a warning to the user. Even though a known issue describing the design limitations for changing router system mode in CSCei15125, page 2, we have in addition added the procedure for this in the help options for the system mode attribute in ONSCLI. If you write ONSCLI>Management-Modes\sys ? a list will be presented with recommended procedure.
- DCN (IP): PPP link on DCC was not taken down/up when configuring the IP address. When configuring DCC channels the channel should have been taken down and then up again every time the operator configure an IP address on a DCC interface. Without a routine in place, IP connectivity cannot be obtained. In order to resolve this issue CiscoEdgeCraft handles this during configuration. Latest release of CiscoEdgeCraft must be used for successful operation.

- DCN (IP): Disabling OSPF generates Fatal Error if stub area exists. (MAJOR) Fatal error occurred when disabling OSPF if stub area exists.The following call-stack could be read when monitoring the spontaneous boot via ONSCLI and/or in display-debug-info log in ONSCLI:

```
000e98c4 HOSTP_copy_dump_info
000e9d54 HOSTG_fatal_error
0024cf3c OSSYSG_fatal_error
0024fdb0 OSMEMG_rn_free
00141d24 OSPFC_memory_free
0011ec28 OSPFP_free_lsa
00120fd8 OSPFC_deactivate_area
0011f93c OSPFP_deactivate_general
00121238 OSPFC_update_general
0013cae4 OSPFP_snmpGenSet
001d162c SNMPC_itc_call
001c0450 SNMPG_call
0011fdf4 OSPFP_task_receive
00236e78 CMNTSKP_task
0038bf40 task_wrapper_exit
```

- Ethernet: Static Unicast Fatal Error. (MAJOR). 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 would be experienced.The following message could be read when monitoring the spontaneous boot via CLI and/or in display-debug-info log in ONSCLI:

```
FATAL ERROR: ROOT: OSBUFG_buf_alloc: Invalid pool_id
```

- Ethernet: RSTP and GVRP conflict caused FATAL-ERROR. (MAJOR). When both RSTP and GVRP run simultaneously, a device-restart could be experienced when disabling GVRP. The following message could be read when monitoring the spontaneous boot via CLI and/or in display-debug-info log in ONSCLI:

```
FATAL ERROR: BRMN: OSTIMG_timer_delete: timer not stopped
```

- Ethernet: VLAN-tagged IGMP packets bypass ingress filtering. (MAJOR). IGMP packets reached the VLAN even though the ingress port was not member of the VLAN. The incoming IGMP packets were VLAN-tagged, and obtained the VID of a VLAN that is configured on the device.The ingress port was not a member of named VLAN.In some rare configurations this could create a loop in the topology, and a storm of replicated IGMP packets.
- Ethernet: Modifying or adding a description on a LANx- or WANx-port may cause interrupt of Ethernet traffic. (MAJOR). The description field, typically used for customer identification, was modified.The event history showed a LAN-port down and up event. The traffic was interrupted for approximately 3 seconds for plain Ethernet bridge connections. If e.g. STP is activated in the network, then traffic interruption will be longer.Applied for LANx- and WANx-ports on the 8xFE+SMAP and 2xGE+SMAP modules.
- Ethernet: LED status for Ethernet ports on 2xGE+SMAP module did not properly display link and status for traffic.
- Ethernet: Max aging time is from now on 630 sec. Due to a limitation in ASIC (Ethernet switch) it is not possible to configure more than 630 sec for aging of MAC addresses in the Unicast Global Forwarding Table. Previous provided range for this parameter has been ageing up to 3600 seconds, but the automatic ageing overruled this and MAC addresses were aged out after approximately 630 seconds.
- Ethernet over SDH: VCAT-VC4 (LCAS) WithinCapacityUpStream NOK.The WithinCapacityUpStream flag was not set for VCAT-VC4 (LCAS).

- Ethernet over SDH: WAN-delay alarm for WANx- and LANx-ports (in L1) with proprietary EoS mapping missing.
- Ethernet over SDH: Ethernet over SDH cross-connections on VC-4 level with SNC/n may leave NIM hanging.The code error applied for LANx- and WANx-ports with VC-4 and soft-lcas mapping, and cross-connections with SNC/n protection. Delete of cross-connections, or removal of the protection leg, will leave the NIM-objects behind.
- SDH/TDM: G.826/829 counters did not properly report historical performance data. The table for history of PM counters for a VC-4 mapped with GE traffic incorrectly stated no BER conditions for previous interval. E.g. when reading PM counters for a VC-4 transporting Ethernet over SDH traffic it was recognized that history of BBE and ES counters was not properly listed.
- SDH: Synergy between EgressSSM and selected SYNC-source. When the Current Sync Source is a SDH port with SSM enabled, the EgressSSM (outward signalling on S1 byte) should state DNU (DoNotUse). Normally this will be the case whether the EgressSSM on the STM-1 port is (default) configured as 'DoNotUse' or 'T0' (T0 to reflect the current sync quality).A bug caused that if the EgressSSM of the STM-1 port was reconfigured from 'DoNotUse' to 'T0', while the port was the active/current Sync Source, the outward signalling, egressSSM/S1, would change from DNU to e.g. PRC (whatever is the current Sync Quality). Instead, the outwardsignalling should state DNU, since the STM-1 port is still synchronized upon.
- The CPU on System Controller seems to run on half speed. (CRITICAL). A software error sometimes caused the SDRAM bus to perform at only 50% of the speed. Problems such as reduced performance of traffic (DCN/Ethernet L2) and MNGT-port block could be typical symptoms of this bug. For some nodes being affected by this bug we've recognized GUN/GOV for MCC1 and MCC2 reported in CLI and in display-debug-info log available from ONSCLI.(The SDRAM refresh rate could be incorrect on the System Controller boards due to an undefined value in one of the SDRAM refresh rate configuration registers. This caused the refresh to appear many times faster then necessary on some boards, slowing down SDRAM access up to 50%.)

The following caveats are resolved as of Release 2.0.2.

- 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. Can be experienced on the 8xSTM-1 modules.
- 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 operator 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. Can be experienced on the following modules: STM1-8, GE-2+MAP and E100-8+MAP.
- Operational Wan-capacity calculation when Admin=0.When EoS proprietary mapping is used and the Administrative capacity is set to 0Mbit/s, the operational capacity may be reported different from 0Mbit/s. Can be experienced on the following modules: E100-8+MAP.
- PM data collection. False G.826 performance errors may be reported on VC-channels in a VCG connected to a LANx or WANx port. Can be experienced on the following modules: E100-8+MAP.
- MNGT-port blocked. The mngt-port occasionally locks-up, resulting in loss of management connectivity to the device. A recovery mechanism is now in place (re-initializing the transmitter).
- OH-byte map-table entry is cleared (slot/port) when UNMAPPING an OH-byte configuration.
- DCC-transparency corrected.
- Reduce MTU on management interfaces (DCC channels) to 1500.

- Fixed bug in handling of IP packets larger than 1500 bytes sent and received by CPU.
- Improved System Controller diagnostics.
- Remove “clear” command from terminal-prompt.
- Relocation of application-code in CompactFlash, according R2.0 mapping, is corrected.
- Fixed - device reboots if switching OSPF InterfaceType from “point-to-point” to “broadcast”. CEC R.2.0.2 and onwards does not allow changing this parameter.
- Add timer supervision on deteriorating external clock reference (2MHz sync input port).
- FE port blocks when port configuration is changed (L1-L2 transition), CSCeg61386.
- Receiving OSPF LSA-update on the MNGT-port lead to reboot. (IPUN only).
- Correct Temp-Serial-Buffer usage, possible device reboot when VT100/Mngt-port connected.
- Extended Signal Label not presented correctly (CEC R.2.0.2 or newer is required for this feature).
- The metric displayed in routing table was110 independent of hop count to destination address for routes learned via the OSPF algorithm. (IPUN only).
- ONSCLI Running-configuration command improvements (alarm data / IP-data / module HW-inventory).
- ONSCLI Merge debug-counters and log-file commands to “display-debug-info” and “clear-debug-info.”
- SNC Protected unidirectional Cross-connection are now supported. CSCeg58380
- 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 tags were inserted, the default port priority was always used for selecting forwarding queue on FE-LANx ports.
- When sending Ethernet frames over proprietary EoS 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 throughput was too low when using half duplex on FE-LANx ports.
- When flow-control was enabled and the traffic consisted of frames with length 9k bytes or slightly less, some frames were dropped on FE-LANx (L1) ports.
- DDTS CSCeg58364; auto negotiation for Flow control on LANx-ports now works (GE-2+MAP only).
- The GFP FCS error counters did not count correct.
- Certain types of LSAs entering a ring of NEs running OSPF over IPUN interfaces provoked restart of the NEs (due to endless circulation).
- Enabling PRIORITY is now possible if FlowControl has ever been enabled (applied only for Ethernet ports on GE-2+MAP).
- Jumbo frames are now dropped if Jumbo-frames are disabled (GE-2+MAP only). Read correct port speed (GE-2+MAP only).

The following caveats are resolved as of Release 2.0.

- Back pressure with 64 bytes packets causes loss and uneven distribution

- GigE port does not handle traffic in fiber w/auto Gen enabled
- Restart triggered when receiving a specific frame (Bootp)
- GigE port/Incorrect media/connection
- Mismatch between “Running SW Revision” presented during start-up and the actual software in the equipment.

New Features and Functionality

This section highlights new features and functionality for Release 2.0. For an overview of features of the 15305, consult the Cisco ONS 15305 Installation and Operations Guide, Release 2.0.

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

- 2-port Gigabit Ethernet module with WAN mapper (Configurable modes; 2xLANx+0xWANx or 2xLANx+2xWANx).
- 8-port Fast Ethernet module with WAN mapper (Configurable modes; 14xLANx+2xWANx or 8xLANx+8xWANx).

The following additional features have been added for Release 2.0.

- Contiguous concatenation according to G.707, for STM-4 and STM-16: VC-4-4c.
- SNC/n (Sub Network Connection Protection with non-intrusive monitoring).
- IPPM (Intermediate path performance monitoring) for up to 63 paths'.
- VCAT on VC-12, VC-3 and VC-4.
- GFP-F on new Ethernet modules.
- Soft LCAS bidirectional on new Ethernet modules.
- Standard LCAS on new Ethernet modules.
- IP In-band solution for management connectivity when L1 mode is used for Ethernet transport. Configurable modes: 192kbit/s or 512kbit/s.
- Rapid Spanning Tree Protocol (RSTP) per device.
- 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.
- OSPF interoperable with ONS15454 SDH on DCN architectures.
- L1 Ethernet transport on new Ethernet modules.
- Support for frame size up to 9,216 octets for L1 services
- Provider VLAN (QinQ), Ether type 8100, is supported on new Ethernet modules.
- Protocol Tunnelling. All MAC addresses in range; 0180C2000000 to 0180C20000FF, except for 0180C2000001, is transported transparently, including the following protocols:
  - RSTP, MSTP, STP, GVRP, GMRP, LACP and 802.1x

The following miscellaneous features have been added for Release 2.0.

- Bulk transfer - CXC tables, Alarm history and PM data (PM data just applicable for higher level management solution).

- Complete Network Release Download including “update policy”.
- E1 Performance Monitoring
- E1 Fixed pointer support for synchronization of e.g. base stations
- DCC transparency (Cisco Edge Craft will now handle this feature).
- NE “running status” commands added in ONSCLI.
- SNCP Switch Event.
- WAN Port “down” alarm
- DCC Termination Failure. CSF alarm is now supported for all DCC encapsulations supported.
- SNCP Performance parameters (Non-intrusive monitors).
- Telmon debug counter visibility in ONSCLI.
- Configurable CRC 16/32 in DCC for PPP encapsulation.
- Pointer adjustment notification (Excessive Pointer justification alarm). Configurable threshold levels Introduced to discover synchronization problems in network.

General improvements/enhancements

- Improved Password Recovery routine, generated based upon the overall serial number of NE.
- Feature licenses will from now on be generated based upon the overall serial number of NE.
- Improved optical level presentation when LOS. Displays now ---
- Optimized buffer handling in NE for sending traps to manager.
- Alarm log increased from 1000 to 500.

Related Documentation

Release-Specific Documents

- *Release Notes for Cisco ONS 15302 Release 2.0.2*
- *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 15305 Quick Installation Guide, Release 2.0*
- *Cisco ONS 15305 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.