Release Notes for Cisco ONS 15305 Release 3.0.6

OL-16677-01
June 20, 2008

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 3.0.6, 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/pcgi-bin/Support/Bugtool/launch_bugtool.pl

Contents

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

Changes to Release Note

This section documents supplemental changes that have been added to the Release Notes for Cisco ONS 15305 Release 3.0.6 since the production of the Cisco ONS 15305 System Software CD for Release 3.0.6.

No changes have been added to the release notes for Release 3.0.6.

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.

CSCsh50098

VLAN Fatal Error deadlock situation.

Symptom:

The device is caught in an endless boot-crash loop if the parameter "VLAN Max Entries After Reset" is set to lower than 100. The following reason for boot may be captured from VT100 during the restart:

FATAL ERROR: ROOT: Bad parameters in HSG_init_hash

Conditions:

Initializing the CDB when the parameter "VLAN Max Entries After Reset" is too low causes a crash without removing the problematic entry from the CDB. This causes the device to keep rebooting and crashing forever.

Work-around:

The first 100 VLANs need to be available as system resources, and therefore the number of VLANs should never be set to less than number of needed VLANs + 100.

Resolution:

Under investigation.

CSCsh50102

The MNGT-port is reported "Up" even though not physically connected.

Symptom:

The operational condition for the management-port is reported "up" even though not physically connected.

Conditions:

The node is configured for IP unnumbered routing and connectivity is obtained through point-to-point link(s). The Management port is disconnected.

Operational condition for the management-port is reported "up" as a result of the design for IP unnumbered routing. The management-port IF index is "borrowed" by point-to-point links in order to obtain unnumbered routing support.

Work-around:

None.

Reproducibility:

100%

Resolution:

Not applicable.

CSCsh38125

Improper behavior when deleting MSP PG with far end Manual switch.

Symptom:

ONS15305 CTC behave improperly while deleting a MSP Protection Group whit a remote manual switch to protection in place.

Conditions:

MSP bidirectional Protection Group in place between an ONS15305 and a ONS15454E; Traffic is manually switched on the protect path on the ONS15454E side, when the user try to delete the MSP Protection Group on the ONS15305 side:

- CTC display a warning message "Protect port is Active. You might lose traffic. Really want to continue?"
- On pressing "Yes", the error message "EID - 3182 - The topology element is in use and cannot be deleted as requested" is displayed if the node is DCC connected on the protection group (as the node is DCC connected and deleting the protection group may result in connection loss between CTC and node)
- Despite the error message CTC goes ahead and deletes the protection group, if the node is connected only via DCC the connection to the node is lost.

Work-around:

Always verify that traffic is in the working patch before deleting a protection group. In case a DCC connection is present and node connection is lost, is possible to recover the connection by issuing a manual switch on the ONS15454E side to move back the traffic (and DCC) to the working path.

Resolution:

Under investigation.

CSCsh38260

Force switch command not cleared in case of SF in protect line

Symptom:

Force switch command is not cleared in case of Signal Fail on protect line; traffic correctly switches to working port.

Conditions:

On a network with a MSP bidirectional, non revertive Protection Group between a ONS15305 and an ONS15454E:

- The user issue a Force to protection command on the ONS15305 side to switch the traffic on the protection path for maintenance reason.
- While the Force command is active an external event (e.g. a fiber cut) cause a Signal Failure on the protect path; the traffic switch back correctly to the working path but the Force switch command is not automatically cleared
- When the signal recover on the protected path, the Force command still in place cause the traffic to switch again on the protect path.

Work-around:

None.

Resolution:

Under investigation.

CSCsh43868

Timing report issues - able to add same timing source as reference more than once.

Symptom:

It is possible to add the same timing source more that once in the timing provisioning panel.

Work-around:

None.

Resolution:

None.

CSCsh45166

VC12-VCT Circuit state goes to partial state after fiber pull and restore.

Symptom:

After a fiber failure (e.g. fiber cut) on the MSP Protection Group connection between a ONS15305 and an ONS15454E that carry VC12-VCTunnel circuits, this kind of circuits are reported by CTC as PARTIAL and do not revert back to DISCOVERED also after the fiber failure has been cleared

Despite the wrong indication on CTC the traffic is flowing error free over the circuit.

Conditions:

The problem is present on VC12 circuits passing over MSP protection group connection between OSN15305 and ONS15454E, when the circuits is using VC-Tunnel feature on the ONS15454 network.

Work-around:

None.

Resolution:

Under investigation.

CSCsh47996

No indication in timing report for timing ref failures.

Symptom:

If one of the configured timing source fails, the current system timing switch to a working one, but In CTC timing report (under Maintenance->Timing tab) there is no indication of the source failure.

Work-around:

None.

Resolution:

Under investigation.

CSCsh48050

Current value in MS performance monitoring never reset.

Symptom:

The current value for MS performance monitoring counters does not reset on time interval shift. Previous time interval report the correct counters value for that intervals, while the current values are absolute counters that only increment on specific events and do not reset to zero on interval ends.

Work-around:

None.

Resolution:

Under investigation.

CSCsd47988

OSPF routing on the MNGT-port is only supported when node operates as IPUN GW.

Symptom:

Enabling OSPF routing on MNGT-port will only be successful for NE's configured as IP unnumbered gateway. This is a limitation in the IP unnumbered router design.

Work-around:

Enable IPUN gateway. Be aware that several IPUN gateways in one IP segment may cause suboptimal routing. Consider assigning unique IP segments to each IP unnumbered router in the topology. This will provide an expandable network configuration.

Resolution:

N/A

CSCsd47998

MNGT port stops responding because of MAC addresses conflict.

Symptom:

MNGT port not responding.

Condition:

The ONS 15305 has MNGT port and bridge ports connected to the same switch. STP or GVRP is enabled on the ONS 15305. Switch receives frames with the same MAC address from different ports, and therefore, only last the source port is stored in MAC address table. In case last frame received from bridge port - MNGT port became not available for management traffic.

Work-around:

Disable STP and GVRP on ONS 15305. or enable STP on switch, or connect MNGT port and bridge port to different switches.

Resolution:

To be clarified

CSCei15125

Changing system mode from IP (default) to IP un-numbered implies problems.

Experiences from field (labs) tell us that current implementation have limitations in software for changing system mode from IP (default) to IP un-numbered.

Even though there are IP addresses and routing protocols configured on NE the operator does not receive any notification, which could have prevented the change until necessary configuration changes have been maintained.

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

The consequence for changing the system mode from IP to IP un-numbered is complicated and you may experience severe problems. Worst-case scenario is not being able to re-obtain IP connectivity to NE.

Work-around:

Generally the safest alternative is to erase the configuration prior to change the system mode. We are aware that this is an unpopular alternative, and have performed some testing to find a more proper work-around.

Up to now we have tested some different configurations, and the following steps were successful:

Step 1 Locally connect to 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 device via ONSCLI (VT100).

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

Step 7 Set 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 re-configure the SNMP community.

Step 9 Re-connect to device with CiscoEdgeCraft.

Step 10 Commission IP un-numbered configuration. IP over PPP (DCC), OSPF, etc.

NoteThis 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 STM1-8 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 CiscoEdgeCraft a lot of "DXC inlet bit error" alarms. No other type of alarms has been recorded from the CiscoEdgeCraft. All these 3 event happens at the same time, so the root cause should be the same.

CSCea71600

The fail is related on module STM1-8. 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 are:

- C5:board_3 module STM1-8 SN0307008095, 2 times / 10 tests
- C7:board_3 module STM1-8 SN0307008095, 1 time / 10 tests
- C7:board_4 module STM1-8 SN0303006397, 1 time / 10 tests

When this fail happens, record the following alarm from the CiscoEdgeCraft: "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

Work-around:

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.

Work-around:

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.

Work-around:

Use protocol tunneling supported by GE-2+MAP and E100-8+MAP 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.

Work-around:

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 inter modular 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 \ping utility\ from CiscoEdgeCraft, and the ping is not successful, abortTftp events are reported. Tftp events are not relevant in this context.

Work-around:

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.

Work-around:

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

Resolution:

Ongoing investigation.

CSCeg11010

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

Work-around:

Mode fields for all pre-provisioned dccR and dccM must be revisited and re configured for "Poverty".

CSCeg11478

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

Work-around:

The following procedure must be used to successfully revert back to Release 1.1.1, after upgrading to release 2.0.0:

Step 1 Main card firmware, 45004-70AA_PM_ ED05.bin, must be uploaded first.

Step 2 Software file, 45004-77AB_PM_ED06.bin, must be uploaded.

Step 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.

CTC Caveats

CSCsd55970

CTC is only available when running in system mode IP unnumbered.

Work-around:
If running IP numbered, use Cisco Edge Craft.

CSCsd53022

It is not possible to view or modify severity of alarms in the Alarm Profile Editor.

Note If CTC is used for storing a new Alarm Profile all severities are set to critical.

Work-around:
Use Cisco Edge Craft

CSCsd53035

It is not possible to manage RS Path Trace.

Work-around:
Use Cisco Edge Craft.

CSCsd53039

It is not possible to manage HO VC Path Trace.

Work-around:
Use Cisco Edge Craft.

CSCsd53044

It is not possible to manage Ether/WAN Path Trace.

Work-around:
Use Cisco Edge Craft.

CSCsd53050

It is not possible to manage PDH Path Trace.

Work-around:
Use Cisco Edge Craft.

CSCsd53054

It is not possible to provision or maintain IPPM. IPPM Performance Monitoring is not available.

Work-around:
Use Cisco Edge Craft.

CSCsd53059

Optical RX Level is not available.

Work-around:
Use Cisco Edge Craft.

CSCsd53065

Ethernet statistics are not available.

Work-around:
Use Cisco Edge Craft.

CSCsd08986

The circuit creation wizard gives the option of creating cross-connects only (TL-1 like). This is not supported

Work-around:
Use Cisco Edge Craft.

CSCsd53068 Alarms Indicating Structuring Mismatch

If there are alarms indicating structuring mismatch, and no partial circuits, there might be stranded structuring/cross-connects.

Work-around:

Use Cisco Edge Craft to clean up manually.

CSCsd53070 SNCP Switching

When switching to the Circuit > Edit pane it occasionally appears that not all members are switched. The switch is actually performed on all members, but there is a display issue.

Work-around:

Perform a Synchronize with the node from the Provisioning > General tab.

CSCsd53083 Shelf View Alarm Color

When an alarm state changes, the alarm color in shelf view occasionally is not updated accordingly.

Work-around:

Use Synchronize Alarms.

CSCsd53093 Edit VCAT Circuit

It is not possible to add VCAT members after a VCAT circuit has been created.

Work-around:

Delete the circuit and recreate with the correct number of members.

CSCsd53101 Alarm Display

The LOM alarm and TIM alarm are displayed with different IDs in network view and shelf view.

Work-around:

None

CSCsd53104 Invalid LP-UNEQ Alarms when Deleting PDH Circuits

When PDH circuits are deleted, LP-UNEQ alarms are raised.

Work-around:

Set the port OOS.

CSCsd53109 SNCP Protected VCAT Circuits

Working and protect paths are not shown in different colors.

Work-around:

None

CSCsd53122

Conditions are not displayed in the Conditions tab.

Work-around:

Use Cisco Edge Craft.

CSCsd53124

Other clients are not updated when Ether bridge parameters are edited.

Modifications in the three tabs under shelf view > Provisioning > Ether Bridge are not reflected on other clients.

Work-around:

Use the Reset button to refresh models.

CSCsc54466 Modify VLAN Tagging from CTM

When a modification is performed from CTM, other clients are not updated accordingly, while if the modification is performed from CTC, other clients are updated.

Work-around:

In CTC, use “Synchronize with Node” in the shelf view > Provisioning > General tab.

In CTM, move the NE OOS and move it back IS.

Firewall Considerations

Firewall Considerations for CTC vs. NEs. The following settings and values apply to firewalls when using CTC with the ONS 15305.

- Security—Use 17476.
- SNMP SET/GET—Use UDP 161.
- SNMP traps—Use UDP 162, 10162, or 13000 (Solaris 1099).
- Bulk Transfer— The default TCP range is 4500-4510.
- TFTP (software download and config upload)—Use UDP 69.
- Time protocol (RFC868)—Use UDP 37.
- Telnet (ONSCLI)—Use TCP 23.

Circuits Shown as Partial

Circuits occasionally show status “Partial.” This can be due to network element discovery that is incomplete, or to incomplete circuit definition.

Work-around:

Network element discovery/rediscovery must be complete before the circuits are fully discovered. If network element discovery is complete, but still the circuits show as “Partial,” delete and recreate the affected circuits.

Transient Alarms During Circuit Creation

During circuit creation or circuit deletion transient alarms might occur. This is expected behavior.

Work-around:

None

Transient Loss of Connection

Transient loss of CTC connection to the network element can occur. This is related to the timeout of SNMP requests, or the number of simultaneous TCP connections.

Work-around:

None, the network element is rediscovered when connectivity is recovered.

Deleting VCAT Circuits

Transient loss of CTC connection to the network element can occur if the network element or DCN network is heavily loaded and SNMP requests time out. Deleting VCAT circuits can typically result in this behavior. If a VCAT delete operation fails and CTC reconnects to the NE, remaining alarm conditions will be present. You can continue deleting any partial circuits still remaining, and all alarms related to the partial circuit(s) should be cleared. If alarms remain, navigate to the card view of the circuit end points and apply the Reset BW (reset bandwidth) check button. This will set the administrative bandwidth of the port to 0 and clear all alarm conditions associated with the port.

Deleting VCAT members from VCAT Circuits

The CTC Network Circuit Provisioning wizard allows CTC users to delete VCAT members from VCAT circuits in any order, without issuing any warning message; however, the following rules governing deletion of VCAT members that start, terminate, or end on an ONS 15305 NE apply:

1. You can only delete 1 circuit member at a time.
2. You can only delete the LAST VCAT member of any VCAT circuit.

If these rules are not followed, deletion of VCAT circuits will result in erroneous circuits and critical alarms from the ONS 15305 NE. The only way to amend the situation caused by deleting wrong VCAT member(s) is to delete the entire VCAT circuit and create a new one.

Software Download

Due to the design of the core CTC software download mechanism, it is not possible to initiate or monitor software download jobs in network view for ONS 15305 nodes. Navigate to the shelf view on each node to perform these tasks. Avoid software download from two CTC instances on the same PC. TFTP port contention might result. The same might occur if you are running Cisco Edge Craft on the same PC as the CTC session. If a download in CTC fails, shut down CEC and try again.

SNMP Trap Port Management

CTC for the ONS 15305 SDH requires listening access to the UDP port 162. For standard SNMP traps, a CTC instance starting up will first try to access port 162. It will then start an RMI-based service that allows other CTC instances on the same computer to receive traps as well. If the CTC instance fails to acquire use of port 162, it will try to connect to an available RMI-based trap distribution service.

Usage in the Solaris Operating System

When using the ONS 15305 SDH in a Solaris environment without required privileges to access port 162, a separate process must be present for forwarding port 162 traps to port 10162.

Concurrent Operation of Cisco Edge Craft and CTC Reserved Ports

The reserved SNMP port can only be held by one application at the time, so concurrent operation of Cisco Edge Craft and CTC should be avoided. For example, software download uses TFTP as the transport protocol. The TFTP port must be available, and with required privileges, to the management interface in order for the download to succeed without incident.

Number of Simultaneous Clients

There is a limit of 4 concurrent TCP connections to an ONS 15305 network element. The consequence is that no more than two CTC instances (including CTM) should be run on an NE simultaneously. If a Network Element is responding to a ping, and to Cisco Edge Craft, but not to CTC, this is most likely the issue.

Web Server Content Corrupt

The software for the management application (CTC) downloads directly to the NE Compact Flash. If the download fails it might corrupt the content of the Compact Flash.

Work-around:

If CTC is available, perform a software download of the management application.

If CTC is not available use Cisco Edge Craft to perform software download of the management application.

Note Always perform a manual reboot of the NE after the download of management application is complete.

CTC on PCs with Two IP Interfaces

If CTC is running on a PC with two or more IP interfaces, the operation of CTC can be affected by disabling one of them.

Work-around:

Restart CTC after disabling an interface.

Security

It is not possible to edit a user.

Work-around:

Delete the user and create a new user.

Resolved Caveats for Release 3.0.6

CSCsk69196: Database Restore Fails

Restoring the CDB file failed in NEs with unnumbered IP. Restoring the database failed when the CDB contained route entries, like static default gateway route, that exist in the working configuration.

CSCsi84125: Synchronization Issues for SSM Enabled T0 Candidates

Problems were noticed for synchronization schemes with SSM enabled and two or more T0 candidates. Symptoms included incorrect re-selection of sync-source, random selection of T0 reference after boot up, absence of switch-over to higher quality T0 reference and so on.

DCN (IP/IPUN) - PPP improvements

Miscellaneous improvements are implemented for PPP. In previous versions the PPP link was vulnerable to ending up in a lock state (no CSF alarm). Additionally the Echo Request counter was not reinitialized when a PPP channel was started. This caused a link to go down and come up repeatedly after the first keep-alive failure.

DCN (IPUN) - Interoperability issue OSPF (ML-HC / ML-TN)

The interoperability issue of OSPF (ML-HC/ML-TN) is fixed in this release.

DCN (IPUN) - Insertion of Illegal Host Routes

When the MNGT-port was connected to a LAN, and the gateway feature set to false, routes to hosts that were outside the locally connected broadcast segment were incorrectly inserted in the routing table.

DCN (IPUN) - Multicast and Broadcast Filtering on PPP/DCC

Processing of MAC multicast packets arriving on the DCC is improved in this release.

Packets with unsupported MAC multicast destinations are discarded instead of forwarded to the routing process.

In rare cases excessive amount of multicast traffic results in a DCC stuck condition. The DCC is temporarily recovered by setting to *NotUsed* mode and then back to *IPoverDCC* mode.

DCN (PPP) - Test of Peer IP Address when IPCP is Notified as UP

In some cases the IPCP presents illegal peer address (like 0.0.0.0) before it finally presents the correct peer address. If an illegal address is presented the OSPF is not notified.

This validity test prevents illegal peer addresses being advertised into OSPF.

CSCsl02062: Support for Repair Circuits after MAC Address Change

Function is available from **CTC->Tools->Circuits->Repair Circuit Wizard.**

Network layer of CTC calculates which nodes are involved with a given node id (MAC address) change and issues an *updateCircuitIds*(oldId,newId) call on those nodes.

This is now implemented for ONS15305.

Note It is recommended that the management software (CTC) be restarted for the changes to take effect. Resynchronize all the affected nodes in a CTM environment.

CSCsl39659: Editing circuit name does not persist CTC reboot

This issue was observed when using circuit names with special meaning in regular expression. This is fixed in this release.

Timing Report Issues

The following issues concerning the timing report are addressed:

Clock status

The clock status (NE or BITS) reflects free run (NE) or squelched (BITS) status.

Synchronization source state

The synchronization source state column reflects the administrative line state (in service or out of service).

Synchronization source condition

The sync source condition column reflects the current alarm state for the line. It shows OOB if there are active alarms preventing the line to be a valid sync source. (LOS, AIS, TIM or LOF alarms)

Condition changed

The timestamp displays the timestamp of the affecting alarm if the port is out of service.

SSM quality

The SSM quality received by the synchronization source is mapped correctly.

New Features and Functionality

There are no new feature for this release.

Related Documentation

This section lists any documentation related to release 3.0.6 of Cisco ONS 15305.

Release-Specific Documents

- Release Notes for Cisco ONS 15302 Release 2.0
- Release Notes for Cisco ONS 15305 Release 2.0
- Release Notes for Cisco Edge Craft Release 2.2

Platform-Specific Documents

- Cisco ONS 15305 Quick Installation Guide, Release 2.0
- Cisco ONS 15305 Installation and Operations Guide, Release 2.0
- Cisco ONS 15305 Cisco Transport Controller Operations Guide, R3.0

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation,* which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

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