Release Notes for Cisco ONS 15310-CL Release 8.5

OL-14422-01
September 18, 2007

Release notes address closed (maintenance) issues, caveats, and new features for the Cisco ONS 15310-CL. For detailed information regarding features, capabilities, hardware, and software introduced with this release, refer to Release 8.5 of the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Procedure Guide, Cisco ONS 15310-CL and Cisco ONS 15310-MA Reference Guide, and Cisco ONS 15310-CL and Cisco ONS 15310-MA Troubleshooting Guide* and Release 8.5 of the *Cisco ONS SONET TL1 Command Guide*. For the most current version of the Release Notes for Cisco ONS 15310-CL Release 8.5, 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

Americas 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 15310-CL Release 8.5* since the production of the Cisco ONS 15310-CL System Software CD for Release 8.5.

Caveats

Review the notes listed below before deploying the Cisco ONS 15310-CL. Caveats with tracking numbers are known system limitations that are scheduled to be addressed in a subsequent release. Caveats without tracking numbers are provided to point out procedural or situational considerations when deploying the product.

Maintenance and Administration

Caution VxWorks is intended for qualified Cisco personnel only. Customer use of VxWorks is not recommended, nor is it supported by Cisco's Technical Assistance Center. Inappropriate use of VxWorks commands can have a negative and service affecting impact on your network. Please consult the troubleshooting guide for your release and platform for appropriate troubleshooting procedures. To exit without logging in, enter a Control-D (hold down the Control and D keys at the same time) at the Username prompt. To exit after logging in, type “logout” at the VxWorks shell prompt.

Note CTC does not support adding/creating more than 5 circuits in auto-ranged provisioning. This is as designed.

Note In releases prior to 4.6 you could independently set proxy server gateway settings; however, with Release 4.6.x and forward, this is no longer the case. To retain the integrity of existing network configurations, settings made in a pre-4.6 release are not changed on an upgrade to Release 7.x. Current settings are displayed in CTC (whether they were inherited from an upgrade, or they were set using the current GUI).

CSCse04103

Applying the forced switch/manual switch on protect facility when no protection switch in operation, FRCDWKSWBK-NO-TRFSW/MANWKSWBK-NO-TRFSW is not raised for 1+1. There is no workaround for this issue. This issue will be fixed in a future release.

CSCse87943

RFI-P is raised on both Working and Protect path in a 1+1 topology on an Cisco ONS 15310-MA. This occurs with an ML card with an STS cross connection with another ML card in another chassis and when the POS port on the Cisco ONS 15310-MA side is shut down. There is no workaround for this issue. This issue will be fixed in a future release.

CSCse90514

The soak timer on POS port reduces which is not an expected behavior after creating a circuit on a POS port that is kept in OOS state. There is no workaround for this issue.

CSCsd84638

Sometimes IP connectivity to an Cisco ONS 15310-MA is lost and pinging the node fails. Also, as a result, CTC fails to come up. This can occur if both the Ethernet port on the CTXMA card and the Ethernet port on the backplane are accidentally connected to the same network, resulting in loops in the switching network. In normal operation the backport should be used to connect to the network and the frontport should only be used for onsite maintenance. If this issue occurs detach the Ethernet cables from both the frontport and the backport and connect via the backport (or frontport) only, rather than via both at the same time. This issue will not be resolved.

TL1

Note To be compatible with TL1 and DNS, all nodes must have valid names. Node names should contain alphanumeric characters or hyphens, but no special characters or spaces.

Resolved Caveats for Release 8.5

This section documents caveats resolved in Release 8.5.

Alarms

CSCse67377

AIS-L Alarm is not visible against EC1 port, if LOS or LOF is injected onto the port. EC1 port is in service and there is no circuit present. This is a hardware limitation which detects AIS-L received from line side, but it cannot raise AIS-L when it receives LOS or LOF from the line.

Data I/O Cards

CSCsf13376

CRC treshold is not triggered when there are excessive CRC errors reported on ML-100 card. This issue is resolved in Release 8.5.

Maintenance and Administration

CSCse58159

MEA alarm is not raised when the port rate is changed to a rate that is not supported by the pluggable port module (PPM). This issue is resolved in Release 8.5.

CSCsg57065

When a non-traffic bearing SFP is removed, it causes a path protection switch in the other PPM that has active circuits. This issue is resolved in Release 8.5.

CSCse96077

When either you remove and then reinsert an I/O card, or a small burst of defects occurs for a very short period (less than 1 sec), false TCAs can be triggered that indicate line or traffic problems on an I/O port. Once triggered, the TCAs will be raised every 15 mins, after the 15 min PM report. There are no alarms for the associated ports. Traffic is not affected.

The cards affected are:

ONS 15454 DS1, DS1_E1_56, DS3 (including DS3, DS3N, DS3E, DS3NE), DS3_EC1, DS3XM, DWDM, E1, E1_42, OC3-8, OC12-4, MRC-12, OC192XFP; and ONS 15310-CL and ONS 15310-MA IO ports.

There are two workarounds:

- Place the affected ports in OOS-DSBLD and then back to IS. This clears the problem for the specific port on the card, but the traffic will be down during the period of OOS-DSBLD.
- Soft reset the card with problem ports. This clears the problem on all ports on the card. Soft reset might cause a protection switch if any port on that card or the card itself is in a protection group.

You can switch all protected ports away from the card that is to be soft-reset. In this case you can do manual switches away from the ports on that card, or in the case of an equipment switch, away from the equipment to be reset.

You can also perform a soft reset without any pre-action. This might result in protection switches of all active protected ports on that card. In the case of an equipment protection group resetting, the active equipment might incur a protection switch. The switch time will not exceed 60 ms.

For unprotected ports or card equipment, traffic will not be affected.

This issue is resolved in Release 8.5.

CSCse75851

Tracebacks are seen in "**show tech**" or "**show ons alarm defect**" command output for ML100T-8 on the Cisco ONS 15310-CL after logging in through the CTC by way of the Cisco IOS CLI. This issue does not occur when these commands are issued through the console. The workaround is to ignore these tracebacks because they do not impact the functioning of the data card.

New Features and Functionality

This section highlights new features and functionality for Release 8.5. For detailed documentation of each of these features, consult the user documentation.

New Software Features and Functionality

The following new software features are added for Release 8.5.

CTC Cache Installer

The CTC Cache Installer is an executable file, SetupCtc-<version>.exe, that is provided on Software Release 8.5 CDs for Cisco ONS products. The CTC cache installer is also available on Cisco.com. You can use CTC Cache Installer to install or reinstall the CTC JAR files into the CTC cache directory on your PC. This is useful when you are using a new CTC version and want to install or reinstall the CTC JAR files without logging into a node or using the StartCTC application (StartCTC.exe).

Disable Inactive User Privileges for Superuser

Users with superuser security privileges can provision security policies on the Cisco ONS 15310-MA. If the superuser privileges are enabled in the NE defaults, superusers can be configured to override the inactive user timeout interval.

Microsoft Vista Support on CTC

The Microsoft Vista operating systems is supported on the Cisco Transport Controller (CTC) in Release 8.5.

Open-Ended VCAT

An open-ended Virtual Concatenated (VCAT) circuit can have a data card at one end and one or more unique non-data card (OC-N/STM-N) destinations at the other end (that is, the open end). The open-ended VCAT circuits can originate or terminate on any pair of OC-N ports and you can route open-ended VCAT circuits using any of the cards and ports supported by VCAT.

Selective Autonegotiation

The selective autonegotiation feature enables autonegotiation for a specific speed and duplex type. If selective autonegotiation is enabled, the port attempts to autonegotiate only to a specific speed and duplex. The link comes up if both the speed and duplex of the attached autonegotiating device matches that of the port. You cannot enable selective autonegotiation if either the speed or duplex of the port is set to auto.

Software Download/Database Backup

The Software Download/Database Backup feature allows database backup restore and software download to an end user network element (ENE) when proxy firewall is enabled by provisioning of a list of legal FTP hosts and enabling them for a specified interval of time.

STS Around the Ring

You can provision synchronous transport signal (STS) circuits with a source endpoint and a destination endpoint on the same node, and route the traffic around a ring. The circuit source and destination can be on the same card, but you must use two different ports on the card.

Manual routing is required for STS around the ring circuits and "Route Automatically" must be unchecked in the CTC circuit provisioning pane. STS around the ring circuits created using Transaction Language 1 (TL1) are discovered by CTC and the status "COMPLETE" is displayed. STS around the ring supports circuit sizes; STS-1, 3c, 6c, 9c, 12c, 24c, 36c, 48c, and 192cs. Both unidirectional and bidirectional circuits are supported, and STS around the ring circuits are CCAT only, VCAT is not supported. STS around ring circuits are linear circuits.

User Defined Alarm Types

User Defined Alarm Types allows you to dynamically add and delete the alarm types. In addition to the existing hard coded alarm type attributes, you can define up to 50 alarm types. These dynamically added alarm types can be associated, or disassociated, to any external alarm input and the added alarm type can use the same behavior as hard coded alarm type attributes.

TL1

TL1 Command Changes

New Commands

The following new TL1 commands are added:

- ENT-FTPSERVER
- RTRV-FTPSERVER
- DLT-FTPSERVER
- ED-FTPSERVER
- ENT-ALMTYPE
- DLT-ALMTYPE
- RTRV-ALMTYPE
- TST-INSERRBITS-MOD2

Command Syntax Changes

The syntax of the following commands is change:

- **ED-DS1** syntax changed from:

  ED-DS1:[<TID>]:<aid>:<CTAG>:::[TACC=<tacc>],[TAPTYPE=<taptype>],[AISONLPBK=<aisonlpbk>],[MODE=<mode>],[FMT=<fmt>];

  To:

  ED-DS1:[<TID>]:<aid>:<CTAG>:::[TACC=<tacc>],[TAPTYPE=<taptype>],[AISONLPBK=<aisonlpbk>],[MODE=<mode>],[FMT=<fmt>],[BERTMODE=<bertmode>],[BERTPATTERN=<bertpattern>],[BERTERRCOUNT=<berterrcount>];

- **ED-ETH** syntax changed from:

  ED-ETH:[<TID>]:<src>:<CTAG>:::[FLOW=<flow>],[EXPDUPLEX=<expduplex>],[EXPSPEED=<expspeed>],[VLANCOS=<vlancosthreshold>],[IPTOS=<iptosthreshold>],[NAME=<name>],[CMDMDE=<cmdmde>],[SOAK=<soak>]:[<pst>[,<sst>]];

  To:

  ED-ETH:[<TID>]:<src>:<CTAG>:::[FLOW=<flow>],[EXPDUPLEX=<expduplex>],[SELECTIVEAUTO=<selectiveauto>],[EXPSPEED=<expspeed>],[VLANCOS=<vlancos>],[IPTOS=<iptos>],[NAME=<name>],[CMDMDE=<cmdmde>],[SOAK=<soak>]:[<pst>[,<sst>]];

- **ED-FSTE** syntax changed from:

  ED-FSTE:[<TID>]:<src>:<CTAG>:::[FLOW=<flow>],[EXPDUPLEX=<expduplex>],[EXPSPEED=<expspeed>],[VLANCOS=<vlancosthreshold>],[IPTOS=<iptosthreshold>],[NAME=<name>],[CMDMDE=<cmdmde>],[SUPPRESS=<suppress>],[SOAK=<soak>]:[<pst>[,<sst>]];

  To:

  ED-FSTE:[<TID>]:<src>:<CTAG>:::[FLOW=<flow>],[EXPDUPLEX=<expduplex>],[EXPSPEED=<expspeed>],[SELECTIVEAUTO=<selectiveauto>],[VLANCOS=<vlancos>],[IPTOS=<iptos>],[NAME=<name>],[CMDMDE=<cmdmde>],[SUPPRESS=<suppress>],[SOAK=<soak>]:[<pst>[,<sst>]];

- **ED-T1** syntax changed from:

  ED-T1:[<TID>]:<aid>:<CTAG>:::[LINECDE=<linecde>],[FMT=<fmt>],[LBO=<lbo>],[TACC=<tacc>],[TAPTYPE=<taptype>],[SOAK=<soak>],[SFBER=<sfber>],[SDBER=<sdber>],[SYNCMSG=<syncmsg>],[SENDDUS=<senddus>],[NAME=<name>],[CMDMDE=<cmdmde>],[AISONLPBK=<aisonlpbk>],[MODE=<mode>],[SYNCMAP=<syncmap>],[ADMSSM=<admssm>],[VTMAP=<vtmap>],[AISVONAIS=<aisvonais>],[AISONLOF=<aisonlof>],[INHFELPBK=<inhfelpbk>]:[<pst>[,<sst>]];

  To:

  ED-T1:[<TID>]:<aid>:<CTAG>:::[LINECDE=<linecde>],[FMT=<fmt>],[LBO=<lbo>],[TACC=<tacc>],[TAPTYPE=<taptype>],[SOAK=<soak>],[SFBER=<sfber>],[SDBER=<sdber>],[SYNCMSG=<syncmsg>],[SENDDUS=<senddus>],[NAME=<name>],[CMDMDE=<cmdmde>],[AISONLPBK=<aisonlpbk>],[MODE=<mode>],[SYNCMAP=<syncmap>],[ADMSSM=<admssm>],[VTMAP=<vtmap>],[AISVONAIS=<aisvonais>],[AISONLOF=<aisonlof>],[INHFELPBK=<inhfelpbk>],[BERTMODE=<bertmode>],[BERTPATTERN=<bertpattern>],[BERTERRCOUNT=<berterrcount>]:[<pst>[,<sst>]];

- **ED-T3** syntax changed from:

  ED-T3:[<TID>]:<aid>:<CTAG>:::[FMT=<fmt>],[LINECDE=<linecde>],[LBO=<lbo>],[INHFELPBK=<inhfelpbk>],[TACC=<tacc>],[TAPTYPE=<taptype>],[SOAK=<soak>],[SFBER=<sfber>],[SDBER=<sdber>],[NAME=<name>],[AISONLPBK=<aisonlpbk>],[CMDMDE=<cmdmde>]:[<pst>[,<sst>]];

  To:

  ED-T3:[<TID>]:<aid>:<CTAG>:::[FMT=<fmt>],[LINECDE=<linecde>],[LBO=<lbo>],[INHFELPBK=<inhfelpbk>],[TACC=<tacc>],[TAPTYPE=<taptype>],[SOAK=<soak>],[SFBER=<sfber>],[SDBER=<sdber>],[NAME=<name>],[AISONLPBK=<aisonlpbk>],[CMDMDE=<cmdmde>],[BERTMODE=<bertmode>],[BERTPATTERN=<bertpattern>],[BERTERRCOUNT=<berterrcount>]:[<pst>[,<sst>]];

- **ED-WDMANS** syntax changed from:

ED-WDMANS:[<TID>]:<aid>:<CTAG>:::[POWERIN=<powerIn>],[POWEROUT=<powerOut>],[POWEREXP=<powerExp>],[NTWTYPE=<ringType>],[PPMESH=<ppmesh>],[DITHER=<dither>];

To:

ED-WDMANS:[<TID>]:<aid>:<CTAG>:::[POWERIN=<powerIn>],[POWEROUT=<powerOut>],[POWEREXP=<powerExp>],[POWEROSC=<powerOSC>],[NTWTYPE=<ringType>],[PPMESH=<ppmesh>],[DITHER=<dither>];

Command Response Changes

The following TL1 command responses have changed:

- **RTRV-DS1** response changed from:

  <AID>::[TACC=<tacc>],[TAPTYPE=<taptype>],[AISONLPBK=<aisonlpbk>],[MODE=<mode>],[FMT=<fmt>

  To:

  <AID>::[TACC=<tacc>],[TAPTYPE=<taptype>],[AISONLPBK=<aisonlpbk>],[MODE=<mode>],[FMT=<fmt>],[BERTMODE=<bertmode>],[BERTPATTERN=<bertpattern>],[BERTERRCOUNT=<berterrcount>],[BERTERRRATE=<berterrrate>],[BERTSYNCSTATUS=<bertsyncstatus>];

- **RTRV-ETH** response changed from:

  <aid>::[<adminstate>],[<linkstate>],[<mtu>],[<flowctrl>],[<optics>],[<duplex>],[<speed>],[<flow>],[<expduplex>],[<expspeed>],[<vlancosthreshold>],[<iptosthreshold>],[<name>],[<soak>],[<soakleft>]:<pst>,[<sst>]

  To:

  <aid>::[<adminstate>],[<linkstate>],[<mtu>],[<flowctrl>],[<optics>],[<duplex>],[<speed>],[<flow>],[<expduplex>],[<expspeed>],[<selectiveauto>],[<vlancosthreshold>],[<iptosthreshold>],[<name>],[<soak>],[<soakleft>]:<pst>,[<sst>]

- **RTRV-FSTE** response changed from:

  <aid>::[<adminstate>],[<linkstate>],[<mtu>],[<flowctrl>],[<optics>],[<duplex>],[<speed>],[<flow>],[<expduplex>],[<expspeed>],[<vlancosthreshold>],[<iptosthreshold>],[<name>],[<suppress>],[<soak>],[<soakleft>]:<pst>,[<sst>]

  To:

  <aid>::[<adminstate>],[<linkstate>],[<mtu>],[<flowctrl>],[<optics>],[<duplex>],[<speed>],[<flow>],[<expduplex>],[<expspeed>],[<selectiveauto>],[<vlancosthreshold>],[<iptosthreshold>],[<name>],[<suppress>],[<soak>],[<soakleft>]:<pst>,[<sst>]

- **RTRV-T1** response changed from:

  <AID>::[LINECDE=<linecde>],[FMT=<fmt>],[LBO=<lbo>],[TACC=<tap>],[TAPTYPE=<taptype>],[SOAK=<soak>],[SOAKLEFT=<soakleft>],[SFBER=<sfber>],[SDBER=<sdber>],[NAME=<name>],[SYNCMSG=<syncmsg>],[SENDDUS=<senddus>],[RETIME=<retime>],[AISONLPBK=<aisonlpbk>],[AISVONAIS=<aisvonais>],[AISONLOF=<aisonlof>],[MODE=<mode>],[SYNCMAP=<syncmap>],[ADMSSM=<admssm>],[PROVIDESYNC=<providesync>],[VTMAP=<vtmap>],[INHFELPBK=<inhfelpbk>]:<PST>,[<SST>]

  To:

<AID>::[LINECDE=<linecde>],[FMT=<fmt>],[LBO=<lbo>],[TACC=<tap>],[TAPTYPE=<taptype>],[SOAK=<soak>],[SOAKLEFT=<soakleft>],[SFBER=<sfber>],[SDBER=<sdber>],[NAME=<name>],[SYNCMSG=<syncmsg>],[SENDDUS=<senddus>],[RETIME=<retime>],[AISONLPBK=<aisonlpbk>],[AISVONAIS=<aisvonais>],[AISONLOF=<aisonlof>],[MODE=<mode>],[SYNCMAP=<syncmap>],[ADMSSM=<admssm>],[PROVIDESYNC=<providesync>],[VTMAP=<vtmap>],[INHFELPBK=<inhfelpbk>]:,[BERTMODE=<bertmode>],[BERTPATTERN=<bertpattern>],[BERTERRCOUNT=<berterrcount>],[BERTERRRATE=<berterrrate>],[BERTSYNCSTATUS=<bertsyncstatus>]:<PST>,[<SST>]

- **RTRV-T3** response changed from:

  <AID>::[FMT=<fmt>],[LINECDE=<linecde>],[LBO=<lbo>],[INHFELPBK=<inhfelpbk>],[TACC=<tap>],[TAPTYPE=<taptype>],[SOAK=<soak>],[SOAKLEFT=<soakleft>],[SFBER=<sfber>],[SDBER=<sdber>],[NAME=<name>],[AISONLPBK=<aisonlpbk>]:<PST>,[<SST>]

  To:

  <AID>::[FMT=<fmt>],[LINECDE=<linecde>],[LBO=<lbo>],[INHFELPBK=<inhfelpbk>],[TACC=<tap>],[TAPTYPE=<taptype>],[SOAK=<soak>],[SOAKLEFT=<soakleft>],[SFBER=<sfber>],[SDBER=<sdber>],[NAME=<name>],[AISONLPBK=<aisonlpbk>][BERTMODE=<bertmode>],[BERTPATTERN=<bertpattern>],[BERTERRCOUNT=<berterrcount>],[BERTERRRATE=<berterrrate>],[BERTSYNCSTATUS=<bertsyncstatus>]:<PST>,[<SST>]

TL1 ENUM Changes

The following sections highlight ENUM items changed (added or removed), by ENUM type.

BERT_ERR_RATE

The following BERT_ERR_RATE enums are added:

- BERT_ERR_RATE_NONE => “STOP”
- BERT_ERR_RATE_SINGLE => “SINGLE”
- BERT_ERR_RATE_TEN_POWER_MINUS_3 => “1E-3”
- BERT_ERR_RATE_TEN_POWER_MINUS_4 => “1E-4”
- BERT_ERR_RATE_TEN_POWER_MINUS_5 => “1E-5”
- BERT_ERR_RATE_TEN_POWER_MINUS_6 => “1E-6”

BERT_ERR_RATE is used in the following command:

- **TST-INSERRBITS-<MOD2>**

BERT_MODE

The following BERT_MODE enums are added:

- BERT_MODE_NONE => “NONE”
- BERT_MODE_TPGM_B => “TPGM-B”
- BERT_MODE_TPGM_L => “TPGM-L”
- BERT_MODE_TPG_B => “TPG-B”
- BERT_MODE_TPG_L => “TPG-L”

- BERT_MODE_TPM_B => “TPM-B”
- BERT_MODE_TPM_L => “TPM-L”

BERT_MODE is used in the following commands:

- **ED-DS1**
- **ED-T1**
- **ED-T3**

BERT_PATTERN

The following BERT_PATTERN enums are added:

- BERT_PATTERN_ALT_ONE_ALT_ZERO => “ALT-ONE-ALT-ZERO”
- BERT_PATTERN_NONE => “NONE”
- BERT_PATTERN_PRBS15 => “PRBS15”
- BERT_PATTERN_PRBS20 => “PRBS20”
- BERT_PATTERN_PRBS23 => “PRBS23”
- BERT_PATTERN_QRSS => “QRSS”

BERT_PATTERN is used in the following commands:

- **ED-DS1**
- **ED-T1**
- **ED-T3**

ENV_ALMTYPE

The following ENV_ALMTYPE enums are added:

- ENV_ALMTYPE_ALMTYPE_SYSTEMDEFINED => “SYSTEMDEFINED”
- ENV_ALMTYPE_ALMTYPE_USERDEFINED => “USERDEFINED”

ENV_ALMTYPE is used in the following command:

- **RTRV-ALMTYPE**

EQPT_TYPE

The following EQPT_TYPE enum is removed:

- EQPT_TYPE_EQPT_ID_CXC_STS => “SSXC”

The following EQPT_TYPE enum is added:

- EQPT_TYPE_EQPT_ID_CXC_STS => “CXC”

EQUIPMENT_TYPE

The following EQUIPMENT_TYPE enum is removed:

- EQUIPMENT_TYPE_ET_CXC => “SSXC”

The following EQUIPMENT_TYPE enum is added:

- EQUIPMENT_TYPE_ET_CXC => “CXC”

EQUIPMENT_TYPE is used in the following command:

- **CHG-EQPT**

OPTICAL_LINK_TYPE

The following OPTICAL_LINK_TYPE enum is added:

- OPTICAL_LINK_TYPE_OL_INTERLEAVER => “OTS-INTLEAV”

OPTICAL_LINK_TYPE is used in the following commands:

- **ED-LNK**
- **RTRV-LNK**

STM1E_MODE

The following STM1E_MODE enums are added:

- PAYLOAD_PT_DS3 => “DS3”
- PAYLOAD_PT_EC1 => “EC1”

STM1E_MODE is used in the following commands:

- **ED-FAC**

TL1 Error Code Changes

New Error Codes

The following new error codes are added:

- ICNV
  - Cannot set Timer value if FTP server is not enabled
- IDNV
  - Alarm Type Exceeds Maximum Length Allowed
  - Invalid Enable Value
  - Invalid Timer Value
- IDRG
  - Invalid Trap Destination
- IIDT
  - Non-IP Hostname or Invalid TID In FTP URL
- IIFM
  - Invalid Alarm Type - Must Conform To TL1 Rules
- IPNC
  - Selective auto Negotiate Cannot be enabled
- NO
  - No Applicable PM Data
- SAIS

  - Connection In Service
- SROF
  - Alarm Type Not Found
  - Alarm type In Use
  - Cannot Delete System Defined Alarm Type
  - Duplicate Alarm Type Create Attempted
  - Duplicate FTP Server Create Attempted
  - FTP Server Not Found
  - Facility Not Part Of Appropriate BLSR
  - Facility Not Part Of Appropriate MSSPR
  - Maximum FTP server Creation Limit Exceeded
  - Maximum UserDefined Alarm Type Limit
  - OCH Client Connection Does Not Exist

Related Documentation

Release-Specific Documents

- *Release Notes for the Cisco ONS 15310-MA Release 7.2*
- *Release Notes for the Cisco ONS 15310-CL Release 8.5*
- *Release Notes for the Cisco ONS 15454 SDH Release 8.5*
- *Release Notes for the Cisco ONS 15454 Release 8.5*

Platform-Specific Documents

- *Cisco ONS 15310-CL and Cisco ONS 15310-MA Procedure Guide*
  Provides installation, turn up, test, and maintenance procedures
- *Cisco ONS 15310-CL and Cisco ONS 15310-MA Reference Manual*
  Provides technical reference information for cards, nodes, and networks
- *Cisco ONS 15310-CL and Cisco ONS 15310-MA Troubleshooting Guide*
  Provides a list of SONET alarms and troubleshooting procedures, general troubleshooting information, transient conditions, and error messages
- *Cisco ONS SONET TL1 Command Guide*
  Provides a comprehensive list of TL1 commands
- *Cisco ONS SONET TL1 Reference Guide*
  Provides general information, procedures, and errors for TL1
- *Cisco ONS 15310-CL and Cisco ONS 15310-MA Ethernet Card Software Feature and Configuration Guide*
  Provides software feature and operation information for Ethernet cards

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

Service and Support

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.