Release Notes for Cisco ONS 15305 Release 3.0

March 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 3.0*, 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

Changes to the Release Notes, page 2

Caveats, page 2

Resolved Caveats for Release 3.0, page 14

New Features and Functionality, page 15

Related Documentation, page 15

Obtaining Documentation, page 15

Documentation Feedback, page 16

Cisco Product Security Overview, page 17

Obtaining Technical Assistance, page 18

Obtaining Additional Publications and Information, page 19

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 3.0* since the production of the Cisco ONS 15305 System Software CD for Release 3.0. No changes have been added to the release notes for Release 3.0.

Caveats

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

Network Element Caveats

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.

Workaround:

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 a MNGT port and bridge ports connected to the same switch. STP or GVRP is enabled on the ONS 15305. The switch receives frames with the same MAC address from different ports, and therefore, only the last source port is stored in MAC address table. When the last frame is received from the bridge port the MNGT port becomes unavailable for management traffic.

Workaround:

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

Resolution:

This issue is under investigation.

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 a named VLAN. In some rare configurations this could create a loop in the topology, and a storm of replicated IGMP packets. The IGMP packets reaches VLAN even though the ingress port is not member of the VLAN. Thus VLAN-tagged IGMP packets bypass ingress filtering.

Workaround

There is usually no need for a configuration that allows this to happen. Verify that the VLAN configuration in the topology is consistent and does not contain any partially configured links.

Resolution

This issue is under investigation.

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.

Workaround:

Generally the safest alternative is to erase the configuration prior to changing the system mode. Alternatives are under investigation.

The following steps might be successful:

Step 1 Locally connect to MNGT-port and connect with Cisco Edge Craft.

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 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 Cisco Edge Craft.

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

Note This procedure cannot be performed 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 Cisco Edge Craft a lot of “DXC inlet bit error” alarms. No other type of alarms has been recorded from the Cisco Edge 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 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 is:

- 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 Cisco Edge Craft: “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 if the size is 64 byte. When the size is increased to 75 byte, the packet loss issue 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 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.

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. For example, if Port 2 module 1, port 1 module 2, and port 1 module 3 send 100Mb traffic streams to port 1 module 1, where 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 Cisco Edge Craft, 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:

This issue is under investigation.

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:

This issue is under investigation.

CSCeg11010

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

Workaround:

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

CSCeg11478

Reverting from Release 2.0.x to 1.1.1 fails.

Workaround:

The following procedure must be used to successfully revert 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.

CTC Caveats

CSCsd55970

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

Workaround:

If running IP numbered, use Cisco Edge Craft.

CSCsd53022 Alarm Profiles

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

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

Workaround:

Use Cisco Edge Craft

CSCsd53035 RS Path Trace

It is not possible to manage RS Path Trace.

Workaround:

Use Cisco Edge Craft.

CSCsd53039 HO VC Path Trace

It is not possible to manage HO VC Path Trace.

Workaround:

Use Cisco Edge Craft.

CSCsd53044 Ether/WAN Path Trace

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

Workaround:

Use Cisco Edge Craft.

CSCsd53050 PDH Path Trace

It is not possible to manage PDH Path Trace.

Workaround:

Use Cisco Edge Craft.

CSCsd53054 IPPM

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

Workaround:

Use Cisco Edge Craft.

CSCsd53059

Optical RX Level is not available.

Workaround:

Use Cisco Edge Craft.

CSCsd53065

Ethernet statistics are not available.

Workaround:

Use Cisco Edge Craft.

CSCsd08986 Create Cross-connects Only (TL-1 like)

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

Workaround:

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.

Workaround:

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.

Workaround:

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.

Workaround:

Use Synchronize Alarms.

CSCsd53093 Edit VCAT Circuit

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

Workaround:

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.

Workaround:

None

CSCsd53104 Invalid LP-UNEQ Alarms when Deleting PDH Circuits

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

Workaround:

Set the port OOS.

CSCsd53109 SNCP Protected VCAT Circuits

Working and protect paths are not shown in different colors.

Workaround:

None

CSCsd53122

Conditions are not displayed in the Conditions tab.

Workaround:

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.

Workaround:

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.

Workaround:

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.

Workaround:

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.

Workaround:

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.

Workaround:

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.

Workaround:

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.

Workaround:

Restart CTC after disabling an interface.

Security

It is not possible to edit a user.

Workaround:

Delete the user and create a new user.

Resolved Caveats for Release 3.0

This section highlights the resolved caveats for Release 3.0.

- CSCeg58260. System-up-time should be able to store up-time up to approximately 497 days. Experience shows this counters wraps around well before (approximately 40 days).
- CSCeg58295. Disabling OSPF causes device-restart if Stub area exists (IP-Numbered mode only). Device restarts when disabling OSPF if stub area exists.
- CSCeg58300. Static Unicast Table (number of entries) causes device-restart. Administratively set a value for Unicast-Global-Forwarding Table causes device restart. If configuring a value for Unicast-Global-Forwarding table "*AfterReset*" lower than the number of static entries in the table, and then select software reset for the device, a device restart will be experienced.
- CSCeg58312.When the setting for aging time is set above 650 seconds, aging still starts at 650 seconds.
- CSCeg58372. There is an RSTP and GVRP conflict.If both RSTP and GVRP run simultaneously, a device-restart may be experienced when disabling GVRP.
- 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".
- 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).
- CSCef88892. When first configuring IP numbered DCN management link between ONS15305 and ONS15454SDH, the link may not come up. For the DCN link to come up, one must toggle the mode field, on ONS15305, from "IpOverDcc" to "Not Used" then back to "IpOverDcc".
- CSCeg58364. Auto negotiation for Flow control on LANx-ports does not work (2xGE_SMAP only).The PAUSE-capable bit is not announced during auto negotiation when Flow Control is set to AutoNeg.
- CSCeg58380. SNC Protected unidirectional cross-connection not supported. When one direction of a path forms part of an SNC protected unidirectional cross-connection, the other direction can not form part of a different SNC protected unidirectional cross-connection. But the two directions can form part of two different unidirectional un-protected cross-connections. This applies to unidirectional cross-connections on all path layers.
- CSCsc16719. IS-IS multicast frames are not properly filtered. 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 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.

New Features and Functionality

This section highlights new features and functionality for Release 3.0. For an overview of features of the ONS 15305, consult the *Cisco ONS 15305 Installation and Operations Guide, Release 2.0*.

The following additional features have been added for Release 3.0.

- A CTC management application can be downloaded to the ONS15305 using the NE Maintenance interface in Cisco Edge Craft Release 2.2.

Related Documentation

This section lists any documentation related to release 3.0 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

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/techsupport

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

Product Documentation DVD

The Product Documentation DVD is a comprehensive library of technical product documentation on a portable medium. The DVD enables you to access multiple versions of installation, configuration, and command guides for Cisco hardware and software products. With the DVD, you have access to the same HTML documentation that is found on the Cisco website without being connected to the Internet. Certain products also have .PDF versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD= or DOC-DOCDVD=SUB) from Cisco Marketplace at this URL:

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

Cisco Optical Networking Product Documentation CD-ROM

Optical networking-related documentation, including Cisco ONS 15xxx product documentation, is available in a CD-ROM package that ships with your product. The Optical Networking Product Documentation CD-ROM is updated periodically and may be more current than printed documentation.

Ordering Documentation

Registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

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

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at tech-doc-store-mkpl@external.cisco.com or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can submit comments about Cisco documentation 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 will find information about how to:

- 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, security notices, and security responses for Cisco products is available at this URL:

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

To see security advisories, security notices, and security responses as they are updated in real time, you can subscribe to the Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed. Information about how to subscribe to the PSIRT RSS feed is found at 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 have identified a vulnerability in a Cisco product, contact PSIRT:

- For Emergencies only—security-alert@cisco.com

  An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- For Nonemergencies—psirt@cisco.com

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

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

Tip We encourage you to use Pretty Good Privacy (PGP) or a compatible product (for example, GnuPG) to encrypt any sensitive information that you send to Cisco. PSIRT can work with information that has been encrypted with PGP versions 2.*x* through 9.*x*.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

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

The link on this page has the current PGP key ID in use.

If you do not have or use PGP, contact PSIRT at the aforementioned e-mail addresses or phone numbers before sending any sensitive material to find other means of encrypting the data.

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation 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, at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support & Documentation 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 & Documentation 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 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 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)—An existing 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 operations 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 the network is impaired, while 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.

- The *Cisco Product Quick Reference Guide* is a handy, compact reference tool that includes brief product overviews, key features, sample part numbers, and abbreviated technical specifications for many Cisco products that are sold through channel partners. It is updated twice a year and includes the latest Cisco offerings. To order and find out more about the Cisco Product Quick Reference Guide, go to this URL:

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

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, 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

  or view the digital edition at this URL:

  http://ciscoiq.texterity.com/ciscoiq/sample/
- *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
- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:

  http://www.cisco.com/en/US/products/index.html
- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

  http://www.cisco.com/discuss/networking
- 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.