



Release Notes for Cisco ONS 15600 Release 7.2

August 2007



Note

The terms "Unidirectional Path Switched Ring" and "UPSR" may appear in Cisco literature. These terms do not refer to using Cisco ONS 15xxx products in a unidirectional path switched ring configuration. Rather, these terms, as well as "Path Protected Mesh Network" and "PPMN," refer generally to Cisco's path protection feature, which may be used in any topological network configuration. Cisco does not recommend using its path protection feature in any particular topological network configuration.

Release notes address closed (maintenance) issues, caveats, and new features for the Cisco ONS 15600. For detailed information regarding features, capabilities, hardware, and software introduced with this release, refer to Release 7.2 of the *Cisco ONS 15600 Procedure Guide*, *Cisco ONS 15600 Reference Manual*, *Cisco ONS SONET TLI Command Guide*, and *Cisco ONS 15600 Troubleshooting Guide*. For the most current version of the Release Notes for Cisco ONS 15600 Release 7.2, visit the following URL:

<http://www.cisco.com/univercd/cc/td/doc/product/ong/15600/600relnt/index.htm>

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



Corporate Headquarters:

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

Copyright © 2007 Cisco Systems, Inc. All rights reserved.

Contents

- [Changes to the Release Notes, page 2](#)
- [Caveats, page 2](#)
- [Resolved Caveats for Release 7.2, page 8](#)
- [New Features and Functionality, page 8](#)
- [Related Documentation, page 10](#)
- [Obtaining Documentation, page 11](#)
- [Documentation Feedback, page 12](#)
- [Cisco Product Security Overview, page 12](#)
- [Obtaining Technical Assistance, page 13](#)
- [Obtaining Additional Publications and Information, page 14](#)

Changes to the Release Notes

This section documents supplemental changes that have been added to the *Release Notes for Cisco ONS 15600 Release 7.2* since the production of the Cisco ONS 15600 System Software CD for Release 7.2.

No changes have been added to the release notes for Release 7.2.

Caveats

Review the notes listed below before deploying the ONS 15600. 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.

Hardware

ONS-SE-2G-xx.x

The ONS-SE-2G-xx.x complies with performance criteria for all intra-facility fiber cables and connectors per Telcordia GR-326-CORE, Issue 3 Sept. 1999. Cisco recommends the following approved suppliers for intrafacility fiber cables to use with this product:

- Volex
- Fitel
- Sumitomo
- Fujikura
- Tyco

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.

CSCsd45025

PPM hardware part numbers are displayed incorrectly in the inventory column. This issue will be resolved in Release 8.0.

CSCsd84932

When an ASAP card IPIO that has STS1 circuits on it is removed, the downstream NE will see UNEQ-P on the STS1 circuits instead of AIS-P, as expected. Concatenated circuits will see AIS-P, as expected. This issue does not occur with 4PIO removals, or with concatenated circuits. This issue will be resolved in a future release.

CSCsb96697

When you perform a Manual Switch To Protect and then an SD-L condition is raised on the Protect port that preempts the Manual Switch To Protect, the CTC Maintenance > Protection tab shows "APS_CLEAR." When you click Clear in that tab while the SD-L is still present on the protect port, the K bytes will change to "No Request" for about 400-1000 frames before redeclaring the SD-L condition. This issue can occur on ONS 15600 ASAP cards with 1+1 protection. It does not affect other cards or protection schemes. This issue does not affect traffic. This issue can only occur when using the CTC Maintenance > Protection tab under the aforementioned conditions. To avoid this issue, do not click Clear when the CTC Maintenance > Protection tab shows "APS_CLEAR" and SD-L is present on the protect port. This issue will be resolved in a future release.

CSCeh84908

A CTC client session can disconnect from an ONS node during simultaneous deletion of large numbers of VT level circuits (3000+). Connectivity to the node will recover without any user action. If the condition persists, restart the CTC session to reconnect. This issue is under investigation.

CSCeg57163

ONS platforms support only a single OSPF virtual link. This issue will be resolved in a future release.

CSCdy58342

Network connectivity could be lost if a backbone area becomes segmented into multiple GNEs. This occurs only if multiple ONS 15600 nodes and routers are connected to the same LAN in OSPF area 0. If a link between two routers breaks, the CTC session connected to Router 1 will not be able to communicate with the ONS 15600 connected to Router 2. To resolve, you must repair the link between the routers or provide another form of redundancy in the network. This is as designed.

CSCdz07098

If OSPF on LAN is enabled with an area ID that is the same as the area ID of any of the DCC Links, CTC will not be able to discover any of the DCC Connected Nodes. To avoid this issue, set the OSPF on LAN area ID to an area other than any of those already occupied by a DCC link. This is as designed.

CSCdy25142

Equipment alarms are always reported based on the activity of the particular card, without taking card redundancy into consideration. Thus, an equipment alarm such as CTNEQPT-PB-0 may be raised against a line card as CR(SA) even though the traffic is protected. This issue will not be resolved.

CSCeb49407

Choosing certain qualities of RES settings in the CTC Provisioning tab, Timing subtab, may trigger a reference failure. Specifically, this can occur if you select the quality of RES level such that any of the following are true.

- $ST3 < RES < ST3E$
- $ST4 < RES < SMC$
- $RES < ST4$

When you then input an actual reference signal lower than ST3E quality, the failure is triggered. This issue will not be resolved.

Optical IO Cards

CSCsd88186

A MFGMEM alarm might be incorrectly raised when using an ASAP card with the PIO4 with one SFP, then replacing that with a PIO1 and an XFP, then returning to the original configuration. When the alarm is mistakenly raised, it does not clear. You must remove and reinsert the SFP to clear the alarm. This issue will be resolved in a future release.

CSCse08282

When the Active XC is removed, the traffic from the line card might be lost. If the line card is an ASAP card, the lack of traffic will cause a low transition signal density to enter the ASAP line card ASIC on the backplane egress interface. The downstream FPGA on the ASAP IPIO daughter card will begin detecting B1 errors. These B1 errors will cause unexpected path protection switches. These errors will also be reported as equipment failures.

To avoid this issue ensure that the Active XC is in OOS-MT state before removing it. If this issue does occur, reset the IPIO ASAP daughter card to clear the errored state. Resetting the ASAP carrier card will also clear the errored state. This issue will be resolved in a future release.

CSCsc51518

In ASAP card view, the PIM graphic might not update with the correct color after an alarm is cleared. This can occur anytime there is an alarm raised against the PIM or any of its subcomponents (PPM or port). To recover from this state, you must either click the Synchronize button, or change to node view and then back to card view. This issue will be resolved in a future release.

CSCef20813

No graphical representations of LEDs for ASAP ports are displayed in the CTC card view. SD and SF LED representations are also absent from the CTC node view for some legacy OCn cards. There are no plans to resolve this issue.

BLSR Functionality

CSCsd62731

When you create a circuit in IS,AINS state while a BLSR is in the switch state the circuit will not transition from IS/AINS to IS. To avoid this ensure that the BLSR is in a stable state before creating a circuit. This issue will be resolved in a future release.

CSCeh49665

Connections might still exist after circuit deletions on BLSR DRI rings for which the primary node is isolated. For BLSR DRI rings with several types of DRI circuits, if you isolate the primary node by deleting the database, reseal the I/O cards, then delete all BLSR DRI circuits, the SSXCs still show connections. To avoid this issue, do not delete or create BLSR DRI circuits when a node on the BLSR DRI ring is isolated. This issue will not be resolved.

Interoperability

CSCdx61916 and CSCeg20536

If, using CTC, you attempt to create a protected VT1.5 circuit that originates on one ONS 15327/454 that is connected to the ONS 15600 via path protection to another ONS 15327/454 that is connected to the ONS 15600 via 1+1 or BLSR, the circuit creation request will be denied because of mixed protection domains. CTC is currently incapable of routing VT circuits across the ONS 15600 when mixed protection schemes are involved. VT traffic can be routed across the ONS 15600 when mixed protection schemes are involved by performing the following:

-
- Step 1** On the ONS 15600, create an STS level cross connect with the requisite path selectors.
 - Step 2** Use CTC to create a VT circuit from the source node to the trunk ports that interface to the 15600.

- Step 3** Use CTC to create a VT circuit between the destination node and the trunk ports that interface with the 15600.
-

**Note**

While this workaround provides the ability to route VT traffic across the ONS 15600 when mixed protection domains exist, the traffic must be managed as three separate circuits instead of one single end-to-end circuit.

This issue will be resolved in a future release.

CSCdy68110

When you attempt to configure VT circuits on a test configuration consisting of two ONS 15454 nodes and one ONS 15600 node, when both ONS 15454s are connected to the ONS 15600 node using a dual path protection connection configuration, and when the ONS 15600 node serves as an intermediate node between the two ONS 15454 nodes, you may be unable to create a VT circuit from one ONS 15454 to the ONS 15600 and then to the other ONS 15454. VT Tunnels are created, but the VT circuit is not created. A mixed protection domain error message is raised when this occurs. To avoid this issue, create the VT tunnels manually, so that the two tunnels do not create a topology where the working and protect tunnels share the same I/O card. After the tunnels have been created, the VT circuit can be successfully added. This issue will be resolved in future release.

CSCdx94969

Physical PM parameters can not be retrieved through the SNMP interface. MIBs released with the ONS 15600 do not have entries for the following physical PM parameters.

- LBC
- OPR
- OPT

The standard SONET Generic MIB does not have entries for these. To work around this issue, use CTC to retrieve the values. SNMP support for these parameters may be considered for a future release.

CSCdy54737

The following PM parameters can not be retrieved through SNMP.

- **Line:**
 - FC-L
- **Path:**
 - FC-P
 - PPJC-Pdet
 - NPJC-Pdet
 - PPJC-Pgen
 - NPJC-Pgen
- **Protection groups:**

- PSC
- PSD
- **Far End counts for line and path**
- **1-Day PM counts**

To retrieve these counts, use CTC. SNMP support for these parameters may be considered for a future release.

Bridge and Roll

CSCdy14265

The manual bridge and roll feature allows you to perform the END command once the roll operation transitions from a ROLL PENDING to ROLL condition, even if the roll to port has an invalid signal. To avoid traffic impact, ensure that the roll-to line is alarm-free. If an alarm exists, you can choose to do nothing and wait for the alarm to clear, to delete the roll, or to proceed in spite of the alarm. This issue will not be resolved.

Alarms

CSCsd52527

The AS-MT and the AS-CMD alarms do not show up on the alarm profile in CTC, so you cannot change the severity of these alarm using CTC. This issue will be resolved in a future release.

TL1

CSCsd52415

You cannot set the GIGE admin state to IS,AINS using the TL1 ED-GIGE command for the ONS 15600 ASAP card. The TL1 ED-GIGE command denies attempts to change the ADMIN state to IS,AINS this card. CTC, however, can execute the state change. This issue will be resolved in a future release.

CSCsd59138

The wrong SSMs for additional references are displayed in the TL1 RTRV-SYCN command response for a 1+1 working line when that line is used as the primary reference for a node. References including SYNC-NE 2 and 3, and SYNC-BITS are incorrectly reported. To avoid confusion, use CTC to view the correct SSMs. This issue will be resolved in a future release.

CSCsd95331

The status field incorrectly displays IS-NR when performing a RTRV-EQPT TL1 command where the AID is of type PIM (Pluggable I/O Module) or PPM (Pluggable Port Module). Since PIMs and PPMs do not support equipment protection, the status field should display NA. This issue will be resolved in a future release.

CSCsb72582

You cannot perform an ENT-EQPT for a valid card type when the current equipment state is OOS-AUMA,MEA&UAS. When the fault PPM comes up as OOS-AUMA,MEA&UAS and then the ENT-EQPT command is entered using TL1, the command is rejected. This issue will be resolved in a future release.

CSCeb46234

A TL1 user cannot preprovision IO cards when a filler card is in the slot. Removal of the filler card will clear the slot and allow the TL1 user to preprovision the IO card. This is by design.

Resolved Caveats for Release 7.2

The following caveats were resolved in Release 7.2.

Maintenance and Administration

CSCsb82218

When a PPM or PIM is physically removed from a node yet remains provisioned, the CTC display shows as blue, as though it was only preprovisioned. Because the PPM or PIM is physically removed, and thus raises an improper removal alarm, CTC should display the alarmed entity as yellow. This issue is resolved in Release 7.2.

New Features and Functionality

This section highlights new features and functionality for Release 7.2. For detailed documentation of each feature, consult the user documentation.

New Hardware Features

One-Port I/O Module for OC-192 Support on ASAP Cards

Release 7.2 supports a new 1-Port I/O (1PIO) module, also called a Pluggable Input/Output Module (PIM), which plugs into the ASAP carrier card. With the Release 7.2 1PIO module the ASAP card provides up to four OC-192 ports per card. The ports operate at up to 2488.320 Mbps over a single-mode

fiber. The ASAP card, when used with the new IPIO module, supports up to four physical connector adapters (known as Small Form-factor Pluggables [SFPs or XFPs]), with two fibers per connector adapter (transmit [Tx] and receive [Rx]), for use with OC-192 line rates.

New ASAP Connectors

The following XFPs are new for Release 7.2, and work with the IPIO only:

- ONS-XC-10G-S1
- ONS-XC-10G-L2

An ASAP carrier card supports up to four IPIO/PIMs for OC192 line rates. Each IPIO supports one SFP/XFP. The maximum configuration for an ASAP card using IPIOs is 4 SFP/XFP ports. These ports can each be provisioned as OC192 line rate.

New Software Features

Network Circuit Automatic Routing Overridable NE Default

The Network Circuit Automatic Routing Overridable NE default makes it possible to set by default whether or not a user creating circuits can change (override) the automatic circuit routing setting (also provisionable as a default).

The new NE default supporting this feature is:

```
CTC.circuits.RouteAutomaticallyDefaultOverridable
```

This default works in combination with the existing circuit routing default:

```
CTC.circuits.RouteAutomatically
```

The overridable option enables network administrators to manage how circuits are created on a network-wide basis. For example, if the Automatic Circuit Routing default is set to FALSE (the check box is unchecked by default), then setting the Network Circuit Automatic Routing Overridable default to FALSE ensures that manual circuit routing is enforced for all users creating circuits (the default is not overridable by the user). When the Network Circuit Automatic Routing Overridable default is set to TRUE (the factory configured setting) users can click in the Automatic Routing check box to change the automatic routing setting if they wish.

When the Route Automatically check box is not selectable during circuit creation, the following automatic routing sub-options will also be unavailable:

- Using Required Nodes/Spans
- Review Route Before Creation

Like the Automatic Circuit Routing default, the Network Circuit Automatic Routing Overridable default applies to all nodes in the network. The Route Automatically check box is either overridable or not depending on how the default is set for the node you are logged into through CTC. To ensure correct behavior after setting the default, propagate the chosen default setting to all nodes through which users might log into the network to perform provisioning. For more information on NE defaults and their provisioning consult the user documentation.

TL1

TL1 ENUM Changes

TL1 ENUM Items Added or Removed

Table 1 highlights ENUM items changed (added or removed) for Release 7.2, by ENUM type.

Table 1 *EQUIPMENT_TYPE enum items added to Release 7.2*

Enum Name	Enum Value
EQUIPMENT_TYPE_ET_PIM_1	"PIM-1"

EQUIPMENT_TYPE is used in the following commands:

- ENT-EQPT
- CHG-EQPT
- RTRV-EQPT
- DLT-EQPT
- RTRV-INV

Related Documentation

Release-Specific Documents

- *Release Notes for the Cisco ONS 15600, Release 7.0*
- *Release Notes for the Cisco ONS 15454 SDH, Release 7.2*
- *Release Notes for the Cisco ONS 15327, Release 7.2*
- *Release Notes for the Cisco ONS 15454, Release 7.2*
- *Release Notes for the Cisco ONS 15310-CL, Release 7.2*
- *Cisco ONS 15600 Software Upgrade Guide, Release 7.2*

Platform-Specific Documents

- *Cisco ONS 15600 Procedure Guide*
Provides installation, turn up, test, and maintenance procedures
- *Cisco ONS 15600 Reference Manual*
Provides technical reference information for SONET/SDH cards, nodes, and networks
- *Cisco ONS 15600 Troubleshooting Guide*
Provides a list of SONET alarms and troubleshooting procedures, general troubleshooting information, and hardware replacement procedures

- *Cisco ONS SONET TL1 Command Guide*
Provides a comprehensive list of TL1 commands

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

<http://www.cisco.com/univercd/home/home.htm>

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Documentation DVD

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

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

Cisco Ordering tool:

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

Cisco Marketplace:

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

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpck/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Ordering tool:
<http://www.cisco.com/en/US/partner/ordering/>
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 1 800 553-NETS (6387).

Documentation Feedback

You can send comments about technical documentation to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Cisco Product Security Overview

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

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

From this site, you can perform these tasks:

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

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

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

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

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

Reporting Security Problems in Cisco Products

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

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



Tip

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

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

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

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

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

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, Cisco Technical Support provides 24-hour-a-day, award-winning technical assistance. The Cisco Technical Support Website on Cisco.com features extensive online support resources. In addition, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not hold a valid Cisco service contract, contact your reseller.

Cisco Technical Support Website

The Cisco Technical Support Website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, 365 days a year, at this URL:

<http://www.cisco.com/techsupport>

Access to all tools on the Cisco Technical Support Website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

<http://tools.cisco.com/RPF/register/register.do>



Note

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

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco TAC engineer. The TAC Service Request Tool is located at this URL:

<http://www.cisco.com/techsupport/servicerequest>

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco TAC engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

<http://www.cisco.com/techsupport/contacts>

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—Your network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

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

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

<http://www.ciscopress.com>

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

<http://www.cisco.com/packet>

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

<http://www.cisco.com/go/iqmagazine>

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

<http://www.cisco.com/ipj>

- World-class networking training is available from Cisco. You can view current offerings at this URL:

<http://www.cisco.com/en/US/learning/index.html>

This document is to be used in conjunction with the documents listed in the “[Related Documentation](#)” section.

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

Copyright © 2007, Cisco Systems, Inc.
All rights reserved.