



Release Notes for *Cisco ONS 15310-CL* *Release 7.0.5*

June 2008



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 15310-CL. For detailed information regarding features, capabilities, hardware, and software introduced with this release, refer to Release 7.0 of the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Procedure Guide*, *Cisco ONS 15310-CL and Cisco ONS 15310-CL and Cisco ONS 15310-MA Reference Guide*, *Cisco ONS SONET TL1 Command Guide*, and *Cisco ONS 15310-CL and Cisco ONS 15310-MA Troubleshooting Guide*.

For the most current version of the Release Notes for Cisco ONS 15310-CL Release 7.0.5, 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

- [Changes to the Release Notes, page 2](#)
- [Caveats, page 2](#)
- [Resolved Caveats for Release 7.0.x, page 4](#)
- [New Features and Functionality, page 5](#)



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

© 2007 Cisco Systems, Inc. All rights reserved.

- [Related Documentation, page 9](#)
- [Obtaining Documentation, page 9](#)
- [Documentation Feedback, page 10](#)
- [Cisco Product Security Overview, page 10](#)
- [Obtaining Technical Assistance, page 11](#)
- [Obtaining Additional Publications and Information, page 13](#)

Changes to the Release Notes

This section documents supplemental changes that have been added to the *Release Notes for Cisco ONS 15310-CL Release 7.0.5* since the production of the Cisco ONS 15310-CL System Software CD for Release 7.0.5.

No changes have been added to the release notes for Release 7.0.5.

Caveats

Review the notes listed below before deploying the 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



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.

CSCsc56694

IPPM enabled by CTC for an OCn trunk card is disabled automatically after two hours. This issue will be resolved in Release 8.0.

Alarms

CSCse85355

The NE should report alarms or conditions on ingress port not on any internal ports. Alarm detected at the internal ports (TERM) side will be ingress map to the MON side. So the NE raises the STS-MON/VT-MON and STS-TERM/VT-TERM alarms or conditions on the STS-MON/VT-MON

ports, irrespective of the actual detection port (MON or TERM). If the user wants the customized severity to be reflected for a specific STS/VT alarms, the alarm profile entities of both STS-MON and STS-TERM, if available, should be changed to the same severity.

CSCsd52665

The NE should report alarms or conditions on ingress port not on any internal ports. Alarm detected at the internal ports (TERM) side will be ingress map to the MON side. So the NE raises the STS-MON/VT-MON and STS-TERM/VT-TERM alarms or conditions on the STS-MON/VT-MON ports, irrespective of the actual detection port (MON or TERM). If the user wants the customized severity to be reflected for a specific STS/VT alarms, the alarm profile entities of both STS-MON and STS-TERM, if available, should be changed to the same severity.

CSCsd56328

The NE should report alarms or conditions on ingress port not on any internal ports. Alarm detected at the internal ports (TERM) side will be ingress map to the MON side. So the NE raises the STS-MON/VT-MON and STS-TERM/VT-TERM alarms or conditions on the STS-MON/VT-MON ports, irrespective of the actual detection port (MON or TERM). If the user wants the customized severity to be reflected for a specific STS/VT alarms, the alarm profile entities of both STS-MON and STS-TERM, if available, should be changed to the same severity.

CSCsg74976

With a hook a test set on OC-3/OC-12, when REI-P is injected, the far-end PM counts on OC-3/OC-12 do not increment. A workaround is to view the far-end PM counts for CV-P which is equal to the near-end CV-P (B3) count of upstream node. This issue is resolved in release 8.0.1.

Path Protection Functionality

CSCee53579

Traffic hits can occur in an unprotected to path protection topology upgrade in unidirectional routing. If you create an unprotected circuit, then upgrade the unprotected circuit to a path protection circuit using Unprotected to path protection wizard, selecting unidirectional routing in the wizard, the circuit will be upgraded to a path protection circuit. However, during the conversion, traffic hits on the order of 300 ms should be expected. 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 7.0.x

The following items are resolved in Release 7.0.x.

Maintenance and Administration

CSCsi04127

When you upgrade nodes from R6.22 to R7.0.4, BITS-1 IN, BITS-2 IN, BITS-1 OUT, and BITS-2 OUT go into In-Service (IS), although the R6.2.2 line-timed nodes have all the BITS facilities set to Out-of-service (OOS), before the upgrade. This issue is resolved in Release 7.05 and 7.23.

Path Protection

CSCsh77496

If path protection/SNCP circuits are created while path defects are present on path protection/SNCP trunks, then sometimes path protection/SNCP circuits may not switch and traffic outage is observed

Workaround: Avoid creating path protection circuits while faults are present on either of the path protection trunks ports. This issue is resolved in 6.03, 7.05 and 7.2.3

Bridge and Roll

CSCei37364

When a rollTo leg is not receiving a good signal, and because of this the rollPending alarm is not cleared, there is no alarm indicating the reason that the RollPending alarm fails to clear. This issue is resolved in Release 7.0.

Data I/O Cards

CSCsb40206

In Asymmetric configuration, with autonegotiation enabled and flow control selected, an ML-series card might fail to synchronize with, or to recognize the asymmetric flow control. This issue is resolved in Release 7.0.

Electrical IO Cards

CSCsd59042

When upgrading the software from Release 6.x.x to Release 7.x.x, the DS3 and EC1-12 cards fail to load if the node name begins with the letters FL. Changing the node name resolves this issue.

New Features and Functionality

This section highlights new features and functionality for Release 7.0.x. For complete documentation of each of the features of the ONS 15310-CL, consult the user documentation.

New Software Features and Functionality

The following feature has been added for Release 7.0.2.

Daylight Savings Time Support

With Release 7.0.2 CTC and TL1 display daylight savings time (DST) in keeping with the new DST rules applicable from 2007 forward. As described in the change in energy policy for the United States of America (USA), the DST start date will be the 2nd Sunday of March and the DST end date will be 1st Sunday of November.

The following features were added for Release 7.0.

Server Trails

Release 7.0.x adds support for server trails. A server trail is a non-DCC link across a third-party network that connects two CTC network domains. A server trail allows circuit provisioning when no DCC is available. You can create server trails between any two optical or DS-3 ports. The end ports on a server trail can be different types. Server trails are not allowed on DCC-enabled ports.

The server trail link is bidirectional and can be VT1.5, VT2, STS1, STS-3c, STS-6c, STS-12c, or STS-48c, depending on the port; you cannot upgrade an existing server trail to another size. A server trail link can be one of the following protection types: Preemptible, Unprotected, and Fully Protected. The server trail protection type determines the protection type for any circuits that traverse it. PCA circuits will use server trails with the Preemptible attribute.

When creating circuits or VCATs, you can choose a server trail link during manual circuit routing. CTC can also route circuits over server trail links during automatic routing. VCAT common-fiber automatic routing is not supported.

Link Consolidation

CTC provides the ability to consolidate the DCC, general communications channel (GCC), optical transport section (OTS), server trail, and provisionable patchcord (PPC) links shown in the network view into a more streamlined view. Link consolidation allows you to condense multiple internodal links into

a singular link. The link consolidation sorts links by class, meaning that all DCC links are consolidated together, for example. You can access individual links within consolidated links using the right-click shortcut menu. Each link has an associated icon.

Link consolidation is only available on non-detailed maps. Non-detailed maps display nodes in icon form instead of detailed form, meaning the nodes appear as rectangles with ports on the sides. Refer to the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Procedure Guide* for more information about consolidated links.

Data Communications Network Tool

Release 7.0.x CTC includes a data communications network (DCN) tool that assists with network troubleshooting for Open Shortest Path First (OSPF) networks. This tool, located in network view, executes an internal dump command to retrieve information about all nodes accessible from the entry point. The retrieved information is the same as you would get if you were to execute a dump using special networking commands. The contents of the dump file can be saved or printed and furnished to Cisco Technical Support for use in OSPF network support.

Advanced Circuit Filtering and Export

Release 7.0.x adds an Advanced tab to the Circuit Filter dialog. With advanced circuit filtering you can filter on selected rings, nodes, links, or source/drop combinations.

Also, you can export the active Circuit window data in HTML, comma-separated values (CSV), or tab-separated values (TSV) format using the Export command from the File menu.

Superuser Privileges for Provisioning Users

With Release 7.0.x Superusers can grant permission to Provisioning users to perform a set of tasks, including retrieving the audit log, restoring a database, clearing performance monitoring (PM) parameters, activating a software load, and reverting a software load. These privileges can only be set using the node-level network element (NE) defaults, with the exception of the PM clearing privilege, which can be granted to a Provisioning user from the CTC Provisioning > Security > Access tabs. For more information about setting up Superuser privileges, refer to the *Cisco ONS 15454 Procedure Guide*.

CTC Download Highest Level NET JAR File

As of Release 7.0.x CTC, during network topology discovery, polls each node in the network to determine which one contains the most recent version of the CTC software. If CTC discovers a node in the network that has a more recent version of the CTC software than the version you are currently running, CTC generates a message stating that a later version of CTC has been found in the network, and offers to install the CTC software upgrade JAR files. If you have network discovery disabled, CTC will not seek more recent versions of the software. Unreachable nodes are not included in the upgrade discovery.

Local Domain Creation and Viewing

With Release 7.0.x a Superuser can control whether domains that any future users create and view persist globally (for all CTC sessions), or only locally (within the current CTC session in which they are created), as well as who can create domains (all users, or just Superusers). This control is given to Superusers by means of the NE default, CTC.network.LocalDomainCreationAndViewing. The factory

pre-set default value is FALSE, meaning domain information is applied to all CTC sessions and only Superusers can create a domain or add a node to a domain. Setting the default to TRUE enables the option for local domain creation by any user.

Enhanced Fault Management

Release 7.0.x adds increased flexibility for fault management. When an entity is put in the OOS,MT administrative state, the node suppresses all standing alarms on that entity. All alarms and events appear on the Conditions tab. You can change this behavior for the LPBKFACILITY and LPBKTERMINAL alarms. To display these alarms on the Alarms tab, you can set the NODE.general.ReportLoopbackConditionsOnOOS-MTPorts to TRUE in the NE Defaults editor.

Rx and Tx Indication for TCAs

For electrical card or port PMs for which a direction, either Receive (Rx) or Transmit (Tx), can be detected, Release 7.0.x CTC and TL1 display the Rx or Tx value with the associated threshold crossing alert (TCA) description. For specific cards, port types, and PMs supported consult the Performance Monitoring chapter of the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Reference Manual*.

TL1

TL1 Command Changes

Command Syntax Changes

The syntax of the following commands is changed in Release 7.0.x.

ENT-TADRMAP syntax:

```
ENT-TADRMAP[:<TID>]::<CTAG>:::TIDNAME=<name>,[IPADDR=<ipAddr>],[PORT=<p
ort>],[ENCODING=<encoding>],[NSAP=<nsapAddr>];
```

Is changed to:

```
ENT-TADRMAP[:<TID>]::<CTAG>:::TIDNAME=<tidname>,[IPADDR=<ipaddr>],[PORT=
<port>],[ENCODING=<encoding>],[NSAP=<nsap>];
```

OPR-SYNCNSW syntax:

```
OPR-SYNCNSW[:<TID>]::<CTAG>;
```

Is changed to:

```
OPR-SYNCNSW[:<TID>][[:<aid>]:<CTAG>;
```

RTRV-NE-SYNCN syntax:

```
RTRV-NE-SYNCN[:<TID>]::<CTAG>[:::];
```

Is changed to:

```
RTRV-NE-SYNCN[:<TID>][[:<aid>]:<CTAG>[:::];
```

RTRV-SYNCN syntax:

```
RTRV-SYNCN[:<TID>]:<aid>:<CTAG>[:::];
```

Is changed to:

RTRV-SYNCN[:<TID>][:<aid>]:<CTAG>[:::];

RTRV-TADRMAP syntax:

RTRV-TADRMAP[:<TID>][:<AID>]:<CTAG>:::MODE=<modeType>

Is changed to:

RTRV-TADRMAP[:<TID>][:<AID>]:<CTAG>[:::MODE=<modeType>]

ED-NE-GEN syntax:

ED-NE-GEN[:<TID>]:<CTAG>[:::NAME=<name>],[[IPADDR=<ipaddr>],[[IPMASK=<ipmask>],[[DEFRTR=<defrtr>],[[IIOPORT=<iioport>],[[NTP=<ntp>],[[SUPPRESSIP=<mode>];

Is changed to:

ED-NE-GEN[:<TID>]:<CTAG>[:::NAME=<name>],[[IPADDR=<ipaddr>],[[IPMASK=<ipmask>],[[DEFRTR=<defrtr>],[[IIOPORT=<iioport>],[[NTP=<ntp>],[[PROXYSRV=<isProxyServer>],[[FIREWALL=<isFireWall>];

Command Response Changes

The following TL1 response has changed in Release 7.0.x.

RTRV-INV response:

<aid>,<aidtype>::[<pn>],[<hwrev>],[<fwrev>],[<sn>],[<clei>],[<twl1=nwl in code>],[<pluginvendorid>],[<pluginpn>],[<pluginhwrev>],[<pluginfwrev>],[<pluginsn>],[<ilossref>],[<productId>],[<versionId>],[<fpgaVersion>]

Is changed to:

<aid>,<aidtype>::[<pn>],[<hwrev>],[<fwrev>],[<sn>],[<clei>],[<twl1=nwl in code>],[<pluginvendorid>],[<pluginpn>],[<pluginhwrev>],[<pluginfwrev>],[<pluginsn>],[<ilossref>],[<productId>],[<versionId>],[<fpgaVersion>],[<vendorId>]

TL1 ENUM Items Added

Table 1 and Table 2 highlight ENUM items added for Release 7.0.x, by ENUM type.

Table 1 *EQUIPMENT_TYPE enum items added to Release 7.0.x*

| Enum Name | Enum Value |
|---------------------------------|-----------------|
| EQUIPMENT_TYPE_ET_UNKNOWN | "UNKNOWN" |
| EQUIPMENT_TYPE_ET_UNPROVISIONED | "UNPROVISIONED" |

EQUIPMENT_TYPE is used in the following commands:

- CHG-EQPT
- ENT-EQPT

Table 2 *MTU_TYPE enum items added to Release 7.0.x*

| Enum Name | Enum Value |
|-----------|------------|
| MTU_1500 | "1500" |

MTU_TYPE is used in the following commands:

- ED-GIGE
- ED-POS

Related Documentation

Release-Specific Documents

- Release Notes for the Cisco ONS 15310-CL, Release 7.0
- Release Notes for the Cisco ONS 15310-MA, Release 7.0.x
- Release Notes for the Cisco ONS 15454 SDH, Release 7.0.x
- Release Notes for the Cisco ONS 15327, Release 7.0.x
- Release Notes for the Cisco ONS 15600, Release 7.0.x
- Release Notes for the Cisco ONS 15454, Release 7.0.x

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 SONET/SDH 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, 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_inpk/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 © 2006 - 2007, Cisco Systems, Inc.
All rights reserved.