Release Notes for Cisco Unified MobilityManager Release 1.2(3)

January 2, 2007

These release notes describe limitations and restrictions, important notes, caveats, and documentation updates for Cisco Unified MobilityManager Release 1.2(3).

Contents

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

Related Documentation

Cisco Unified MobilityManager Documentation

Refer to the documentation set for Cisco Unified MobilityManager for detailed configuration and use information. Navigate from the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_mobmg/1_2/index.htm

Cisco Unified IP Phone Documentation

Refer to publications that are specific to your language, phone model and Cisco Unified CallManager version. Navigate from the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_ipphon/index.htm

Cisco Unified CallManager Documentation

Refer to the Cisco Unified CallManager Documentation Guide and other publications specific to your Cisco Unified CallManager version. Navigate from the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/index.htm

Installation Notes

The following installation notes apply to Cisco Unified MobilityManager Release 1.2(3):

- Restart Cisco Unified MobilityManager whenever Cisco Unified CallManager is upgraded.

- During a new installation, you may be prompted to respond to multiple "DVD Found/Media Check" messages. At the first prompt, enter **Yes** to ensure the integrity of the DVD, and enter **No** to subsequent prompts to continue the installation.
- If you are upgrading from Cisco Unified MobilityManager Release 1.2(1), you can perform a software upgrade.
- If you are upgrading from Cisco Unified MobilityManager Release 1.1(2), you must do a new install. The new install must be on a system with the same IP address as the system used for Cisco Unified MobilityManager 1.1(1). For more information about installation, refer to the *Cisco Unified MobilityManager Installation Guide*:

  http://www.cisco.com/univercd/cc/td/doc/product/voice/c_mobmg/index.htm

Important Notes

This section provides information about Cisco IP Telephony Platform support. For more information, see the *Cisco IP Telephony Platform Guide*:

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_mobmg/1_2/admins/plat1_2/index.htm

The following Cisco IP Telephony Platform GUI options are *not* supported:

- Clusters
- Simple Mail Transfer Protocol (SMTP)
- Security: Certificate Management and IPSec Management

Note Cisco Security Agent (CSA) is supported in Cisco Unified MobilityManager Release 1.2(3).

Bulk Provisioning CLI

A new CLI utility in Platform administration allows for bulk provisioning of Cisco Unified MobilityManager users.

Before you can perform bulk insertion of users, you must create a userinfo.csv file on a Secure File Transfer Protocol (SFTP)-enabled system. The userinfo.cvs file must be in comma-separated value (CSV) format (columns that require non-blank entries are marked with *):

- Mobile_Voice_Access_User ID*
- Mobile_Unified_CallManager User ID*
- DeviceName
- Enable User Remote Access
- Maximum number of Group Allowed
- Maximum number Line Appearance Allowed
- Maximum number of Remote Destination Allowed*
- Maximum number of Allowed Caller Filters Allowed*
- Maximum number of Blocked Caller Filters Allowed*
- Group Identification*
- Description
- Line Number*
- Enable Caller ID Override
- Caller ID Override Number
- Enable Delay Before Ringing Cellular Phone
- Delay Before Ringing Cellular Phone (msec)
- Maximum wait time for desk phone pickup (msec)
- Enable Cellular Phone Pickup
- Remote Destination*
- CallerID
- Enable Mobile Connect
- Enable Maximum Cellular Phone Pickup Timer

- Maximum Cellular Phone Pickup Timer (msec)
- Enable Maximum Cellular Phone Ring Timer (msec)
- Maximum Cellular Phone Ring Timer (msec)
- Enable Minimum Cellular Phone Ring/Pickup Timer
- Minimum Cellular Phone Ring/Pickup Timer (msec)

By convention, the first line of a CSV (comma-separated format) file is reserved for comments. Therefore, enter input values starting in the second row.

For example, an input line for the userinfo.csv file might be:

1000,usera,,no,1,1,1,1,1,1,test,1681000,enable,,enable,4000,10000,enable,99023136,,yes,enable,20000,enable,19000,default,9000

After creating the CSV file, follow these steps to add the user information using bulk provisioning:

Procedure

Step 1 Enter this command to send the userinfo.csv file from the SFTP server to the Cisco Unified MobilityManager server:

```
utils get_cisco_mobile_connect_users_info
```

Step 2 Enter this command:

```
utils cisco_mobile_connect_users_insert
```

The system prompts with the following question:

```
Do you want to delete all the cisco mobile connect users from the
database (Y/N):
```

If you select **Y**, the system deletes the user information from the database and then inserts the contents of the new userinfo.csv file into the database. If you select **N**, the system skips the bulk deletion and proceeds with normal bulk insertion of userinfo.csv contents into the database.

Step 3 Log in to the Cisco Unified MobilityManager administration web interface.

Step 4 Choose **System > Data Synchronization**.

Step 5 Click **Start Now** to begin data synchronization and load the Mobile Connect users into memory.

The following information applies to bulk provisioning:

- The user data is not validated by way of an AXL request to Cisco Unified CallManager.
- If the file format is incorrect, the bulk provisioning is executed, but the information is not added to the user database.
- Each user ID is associated with only one remote destination.

Platform CLI Commands

The following CLI commands are supported:

- **file check**
- **show firewall**
- **show logins**
- **show open files**
- **show open ports**
- **show timezone config**
- **unset network dns**
- **utils cisco_mobile_connect_users_insert**
- **utils get_cisco_mobile_connect_users_info**
- **utils reset_ui_administrator_password**

Limitations and Restrictions

This section describes limitations and restrictions that apply to Cisco Unified MobilityManager Release 1.2(3).

Calling Search Space Configuration

To ensure correct Mobile Connect functionality, you must configure the calling search space for the CTI outgoing port line level in Cisco Unified CallManager. Refer to Cisco Unified CallManager caveat CSCsh13165.

Cryptographic Features

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at: http://www.cisco.com/wwl/export/crypto/tool/stqrg.html.

If you require further assistance please contact us by sending email to export@cisco.com.

Supported MCS Servers

The following MCS servers are supported for Cisco Unified MobilityManager Release 1.2(3):

- MCS-7815-I1 (3.0 GHz)
- MCS-7815-I2
- MCS-7825-H1 (3.4 GHz)
- MCS-7825-H2
- MCS-7825-I2
- MCS-7835-H1 (3.4 GHz)
- MCS-7835-H1 retrofit
- MCS-7835-H2
- MCS-7835-I1 (3.4 GHz)
- MCS-7835-I2
- MCS-7845-H2
- MCS-7835-I1 retrofit
- MCS-7845-H1 (3.4 GHz dual processor)
- MCS-7845-H1 retrofit

- MCS-7845-I1 (3.4 GHz dual processor)
- MCS-7845-I1 retrofit

Note Cisco Unified MobilityManager Release 1.2(3) does not currently support the MCS-7825-I1 server.

Caveats

This section contains these topics:

Using Bug Toolkit

Known problems (bugs) are graded according to severity level. These release notes contain descriptions of:

- All severity level 1 or 2 bugs.
- Significant severity level 3 bugs.

You can search for problems by using the Cisco Software Bug Toolkit.

To access Bug Toolkit, you need the following items:

- Internet connection
- Web browser
- Cisco.com user ID and password

To use the Software Bug Toolkit, follow these steps:

Procedure

Step 1 To access the Bug Toolkit, go to http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl.

Step 2 Log on with your Cisco.com user ID and password.

Step 3 Click the **Launch Bug Toolkit** hyperlink.

Step 4 To look for information about a specific problem, enter the bug ID number in the "Enter known bug ID" field and click **Search**.

Open Caveats

Table 1 lists Severity 1, 2 and 3 defects that are resolved for Cisco Unified MobilityManager Release 1.2(3).

For more information about an individual defect, you can access the online record for the defect by clicking the Identifier or going to the URL shown. You must be a registered Cisco.com user to access this online information.

Because defect status continually changes, be aware that Table 1 reflects a snapshot of the defects that were open at the time this report was compiled. For an updated view of open defects, access Bug Toolkit as described in the Using Bug Toolkit, page 8.

Table 1 Open Caveats

Identifier	Headline and Bug Toolkit Link
CSCsd76348	It is necessary to reboot Cisco Unified MobilityManager for restore to work after changing the network domain http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsd76348
CSCsd99095	AXL device lookup fails with special characters in password http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsd99095
CSCse34483	Upgraded from 121 to 122, CLI show hardware shows UNKNOWN http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCse34483

Table 1 Open Caveats (continued)

Identifier	Headline and Bug Toolkit Link
CSCse34538	Cannot view file using CLI file view activelog http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCse34538
CSCsh21594	File format is not checked for the **utils cisco_mobile_connect_users_insert** command http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsh13165
CSCsh13165	Need to configure the calling search space for the CTI outgoing port line level for Mobile Connect to work http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsh13165

Resolved Caveats

Table 2 lists Severity 1, 2 and 3 defects that are resolved for Cisco Unified MobilityManager Release 1.2(3).

For more information about an individual defect, you can access the online record for the defect by clicking the Identifier or going to the URL shown. You must be a registered Cisco.com user to access this online information.

Because defect status continually changes, be aware that Table 2 reflects a snapshot of the defects that were open at the time this report was compiled. For an updated view of open defects, access Bug Toolkit as described in the "Using Bug Toolkit" section on page 8.

Table 2 Resolved Caveats

Identifier	Headline and Bug Toolkit Link
CSCsc06315	System parameter default values shown in the help page are incorrect http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsc06315
CSCsc69509	The join feature does not work for mobile pickup calls with the Select option http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsc69509

Table 2 Resolved Caveats (continued)

Identifier	Headline and Bug Toolkit Link
CSCsc70192	If Cisco Unified CallManager 5.0.1 is connected to an H.323 gateway, Call Park interaction with Cisco Unified MobilityManager cell pickup does not work properly http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsc70192
CSCsc86924	Cisco Unified MobilityManager does not verify that the LDAP information that is entered works http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsc86924
CSCsd42377	Adding a user requires that AXL server settings be configured on the System page http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsd42377
CSCsd45744	Cisco Unified MobilityManager SNMP provides the wrong information for sysObjectID and sysName http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsd45744
CSCsd45760	Cisco Unified MobilityManager should provide MIB configuration information for system contact and location http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsd45760
CSCsd48604	A SQLException occurs in the log following successful login to Cisco Unified MobilityManager administration http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsd48604
CSCsd52890	MTP should be checked in the SIP trunk to have a voice path in the mobile phone http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsd52890
CSCsd55789	The show account fails after changing the IP address from the GUI right after a fresh install http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsd55789
CSCsd56373	Users should be prompted for the Directory User Setting whenever an older version of Cisco Unified MobilityManager is used http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsd56373
CSCsd56406	The CLI command show/set web-security pair should be either supported or removed http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsd56406

Table 2 Resolved Caveats (continued)

Identifier	Headline and Bug Toolkit Link
CSCsd56408	CLI command utilities network capture eth0/eth1 does not work if CSA is on http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsd56408
CSCsd56410	A CLI command set for password security should be added http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsd56410
CSCsd56639	The Backup Scheduler should give a warning if no features are selected http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsd56639
CSCsd61648	When multiple CTI links are out of service, an alarm is created only for the last out of service link http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsd61648
CSCsd68388	The **show cert trust** command is not supported in the CLI http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsd76348
CSCse31107	CTI Userids changed to all uppercase http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCse31107
CSCse31316	User cannot update the shared ports and out port users http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCse31316
CSCse36706	LDAP directory Admin password in plain text in web source file http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCse36706
CSCse51453	SNMP Description shows wrong platform type http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCse51453
CSCse55253	During fresh install, DVD found/media check shown two or three times http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCse55253
CSCse55259	No progress indication during the last 20 minutes of software upgrade http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCse55259
CSCse58976	Delete account does not work http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCse58976
CSCse97812	SNR / Mobility Manager. IOS Error “vxml version 1.0 not supported” http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCse97812

Table 2 Resolved Caveats (continued)

Identifier	Headline and Bug Toolkit Link
CSCse98352	Multiple Shared Line User Links should be used for bulk calls http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCse98352
CSCsg66392	Third prompt is not played after no user ID is given http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsg66392

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. This section explains the product documentation resources that Cisco offers.

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 library of technical product documentation on a portable medium. The DVD enables you to access installation, configuration, and command guides for Cisco hardware and software products. With the DVD, you have access to the HTML documentation and some of the PDF files found on the Cisco website at this URL:

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

The Product Documentation DVD is created and released regularly. DVDs are available singly or by subscription. Registered Cisco.com users can order a Product Documentation DVD (product number DOC-DOCDVD= or DOC-DOCDVD=SUB) from Cisco Marketplace at the Product Documentation Store at this URL:

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

Ordering Documentation

You must be a registered Cisco.com user to access Cisco Marketplace. Registered users may order Cisco documentation at the Product Documentation Store at this URL:

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

If you do not have a user ID or password, you can register at this URL:

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

Documentation Feedback

You can provide feedback about Cisco technical documentation on the Cisco Support site area by entering your comments in the feedback form available in every online document.

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 do the following:

- 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 encryption key 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 to find other means of encrypting the data before sending any sensitive material.

Product Alerts and Field Notices

Modifications to or updates about Cisco products are announced in Cisco Product Alerts and Cisco Field Notices. You can receive these announcements by using the Product Alert Tool on Cisco.com. This tool enables you to create a profile and choose those products for which you want to receive information.

To access the Product Alert Tool, you must be a registered Cisco.com user. Registered users can access the tool at this URL:

http://tools.cisco.com/Support/PAT/do/ViewMyProfiles.do?local=en

To register as a Cisco.com user, go to this URL:

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

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Support 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 Support Website

The Cisco 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 at this URL:

http://www.cisco.com/en/US/support/index.html

Access to all tools on the Cisco 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 Before you submit a request for service online or by phone, use the **Cisco Product Identification Tool** to locate your product serial number. You can access this tool from the Cisco Support website by clicking the **Get Tools & Resources** link, clicking the **All Tools (A-Z)** tab, and then choosing **Cisco Product Identification Tool** from the alphabetical list. This 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.

Tip **Displaying and Searching on Cisco.com**

If you suspect that the browser is not refreshing a web page, force the browser to update the web page by holding down the Ctrl key while pressing **F5**.

To find technical information, narrow your search to look in technical documentation, not the entire Cisco.com website. After using the Search box on the Cisco.com home page, click the **Advanced Search** link next to the Search box on the resulting page and then click the **Technical Support & Documentation** radio button.

To provide feedback about the Cisco.com website or a particular technical document, click **Contacts & Feedback** at the top of any Cisco.com web page.

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 Online Subscription Center is the website where you can sign up for a variety of Cisco e-mail newsletters and other communications. Create a profile and then select the subscriptions that you would like to receive. To visit the Cisco Online Subscription Center, go to this URL:

  http://www.cisco.com/offer/subscribe

- 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 channel product 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

- *Internet Protocol Journal* is a quarterly journal published by Cisco 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, 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 where networking professionals 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

- "What's New in Cisco Documentation" is an online publication that provides information about the latest documentation releases for Cisco products. Updated monthly, this online publication is organized by product category to direct you quickly to the documentation for your products. You can view the latest release of "What's New in Cisco Documentation" at this URL:

  http://www.cisco.com/univercd/cc/td/doc/abtunicd/136957.htm

- 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