Installing Cisco Security Agent 4.0.1.539-1.1.3 for Cisco CallManager Releases 3.2(3), 3.3, and 4.0

This document provides installation instructions and information about Cisco Security Agent for Cisco CallManager 3.2(3), 3.3, and 4.0. If Cisco CallManager resides on the same server with Cisco Customer Response Applications (CRA), you can use this document or the *Installing Cisco Security Agent 4.0.1.539-1.1(3) for Cisco Customer Response Applications Releases 2.2(5), 3.0(3), and 3.1(2)* document to install the agent on that co-resident server, because both products use identical security policies.

Contents

This document contains information on the following topics:

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

Introduction

The Cisco Security Agent (CSA) provides intrusion detection and protection for the Cisco CallManager 3.2(3), 3.3, and 4.0 cluster. The agent provides Windows platform security based on a tested security rules set (policy). The policy has rigorous levels of host intrusion detection and prevention. The agent controls system operations by using policies that allow or deny specific system actions before system resources are accessed. This process occurs transparently and does not hinder overall system performance.

Note In addition to being specifically tuned for the Cisco CallManager and Cisco CRA software, Cisco Security Agent for Cisco CallManager provides support for many Cisco-approved third-party applications. The agent also provides security for web and database services. In addition, CSA provides security checks for TCP/IP if you install the Network Shim, which serves as a host-based intrusion detection system. When a later version of the agent becomes available, Cisco strongly recommends that you install the later version.

Cisco strongly recommends that you run this agent in conjunction with the latest Cisco-provided operating system service releases and upgrades. To obtain the Cisco-provided operating system service releases and upgrades, see Table 1.

Follow the installation instructions in this document to install CSA on all servers within the voice cluster, including Cisco CallManager, Cisco CRA, Remote Database, voice, and speech servers. Do not install the agent on client machines.

The policy included with Cisco Security Agent for Cisco CallManager provides support for many Cisco-approved, third-party monitoring tools, including the following applications:

- Concord eHealth Monitor
- HP OpenView Operations Agent 7.1
- HP OpenView Performance Manager 3.3
- Integrated Research Prognosis
- McAfee VirusScan 7.0
- Micromuse Netcool
- NetIQ Vivinet Manager
- RealVNC
- Symantec Corporate Edition 8.0
- Trend Anti-Virus
- Windows Terminal Services

If you use a third-party software tool that is not Cisco-approved, you must purchase and install the fully managed console product, Management Center for Cisco Security Agents (CSA MC), and contact the Cisco Technical Assistance Center (TAC) for information on customizing the policy to support your Cisco-approved, third-party applications. See the "Obtaining Technical Assistance" section on page 12 for information on contacting TAC. See the "Migrating to the Management Center for Cisco Security Agents" section on page 7 for more information on migrating to CSA MC.

Before You Begin the Installation

Before you install the Cisco Security Agent for Cisco CallManager, review the following information:

- The Cisco Security Agent supports any Cisco Media Convergence Server (MCS) or customer-provided, Cisco-approved server where Cisco CallManager Releases 3.2(3), 3.3(x), or 4.0 and Cisco-provided operating system version 2000.2.4 (or later) are installed, unless the *Cisco CallManager Compatibility Matrix* indicates otherwise. To obtain the *Cisco CallManager Compatibility Matrix*, see Table 1.
- Install this security agent on every server in the Cisco CallManager cluster, including coresident servers where Cisco CallManager and Cisco Customer Response Solutions/Cisco Customer Response Applications run.
- Install the agent first on the publisher database server and verify that the installation completed successfully; then, install the agent on all subscriber servers serially, that is, on one server at a time.
- Do not install the agent between the operating system and Cisco CallManager installation.
- Before each Cisco CallManager upgrade, you must disable the Cisco Security Agent service using the procedure shown in the "Disabling and Reenabling the Cisco Security Agent Service" section on page 6. You must also ensure that the service does not get reenabled at any time during the Cisco CallManager installation.

Caution You must disable the Cisco Security Agent service before installing, uninstalling, or upgrading any software, including the operating system, Cisco CallManager, maintenance releases, service releases, support patches and plugins.

You must disable the agent using the method described in the "Disabling and Reenabling the Cisco Security Agent Service" section on page 6. Ensure that the service does not get reenabled at any time during the installation or upgrade. Failure to do so may cause problems with the installation or upgrade.

After the software installation, or upgrade, you must reenable the Cisco Security Agent service.

When you disable the service, the agent no longer provides intrusion detection for the server.

- If you plan to upgrade from Cisco CallManager 3.2(3) to Cisco CallManager 3.3 and you run the agent on the server, you must disable the Cisco Security Agent service before the upgrade. After the upgrade, you must reinstall the Cisco Security Agent on all servers in the cluster because the upgrade to Cisco CallManager 3.3 deletes the agent.
- If you plan to upgrade from Cisco CallManager 3.3(2) to Cisco CallManager 3.3(3) or 4.0 and you run the agent on the server, you must disable the Cisco Security Agent service before the upgrade; however, you do not need to reinstall the agent after the upgrade. Remember to enable the Cisco Security Agent service after the upgrade.
- Before you install or upgrade the agent, back up your Cisco CallManager data. For more information on how to perform this task, refer to the appropriate version of the Cisco CallManager backup documentation. To obtain the Cisco CallManager backup documentation, see Table 1.
- Before you install or upgrade the agent, back up all applications that run in the cluster. Refer to the appropriate backup documentation for more information.

- Do not use Terminal Services to install or upgrade the agent. Cisco installs Terminal Services, so Cisco Technical Assistance Center can perform remote management and configuration tasks. Do not use Integrated Lights Out to install or upgrade the agent.

  If you want to do so, you can use Virtual Network Computing (VNC) to install or upgrade the agent. To obtain VNC documentation, see Table 1.

Caution If you currently run Cisco HIDS Agent (Entercept) on the server, you must uninstall the software from Add/Remove Programs before you install the Cisco Security Agent. If you fail to uninstall the Cisco HIDS Agent before the Cisco Security Agent installation, the installation deletes the TCP stack, and the Cisco Security Agent does not install the firewall component that is necessary for security.

- The agent installation causes a brief spike in CPU usage. To minimize call-processing interruptions, Cisco recommends that you install the agent during a time when call processing is minimal. The agent protects the server as soon as you install the software, but the agent does not provide complete functionality until you reboot the server.

Note Rebooting the server may cause call-processing interruptions. Cisco recommends that you reboot the server at the end of the business day or during a time when call processing is minimal.

- Before you upgrade the agent or reinstall the agent on the server, you must uninstall the agent and then reinstall the software.

  When you uninstall the agent by using Add/Remove Programs or Start > Programs > Cisco Systems > Cisco Security Agent > Uninstall Security Agent, a prompt asks whether you want to uninstall the agent. You have limited time to click Yes to disable the protection. If you choose No or wait to disable the protection, the security mode automatically enables.

Caution After you uninstall the software, reboot the server immediately. If you do not reboot the server immediately, the flag continues to display in the Windows 2000 system tray, and the Message tab in the graphical user interface (GUI) displays errors, but the software does not provide protection.

- After the installation, you do not need to perform any agent configuration tasks. The software immediately begins to work as designed. Security logs display in the Message tab of the agent GUI, in Microsoft Event Viewer, and in the security.txt file (C:\Program Files\Cisco\CSAgent\log).
- The Cisco IP Telephony Applications Backup Utility does not back up the log files or text file that the agent generates.

  If you need to restore the Cisco CallManager data to the server for any reason, you must reinstall the agent after you restore the Cisco CallManager data.

Tip If you encounter problems with installing or uninstalling the agent, see the "Troubleshooting" section on page 9.

Installing the Cisco Security Agent

Item Needed: Executable from the web

Review the "Before You Begin the Installation" section on page 3, which provides information that ensures a successful installation. To install the Cisco Security Agent for Cisco CallManager, perform the following procedure:

Procedure

Step 1 From the CallManager server, go to the Voice Software Download URL at http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml.

Note The Cisco Security Agent and policies post on the voice products cryptographic software site. You can navigate to the site from the voice application (Cisco CallManager, CRS, and so on) software window.

Step 2 Download the latest version of the Cisco Security Agent file: **CiscoCM-CSA-<version>-K9.exe**.

For example, download the file, CiscoCM-CSA-4.0.1.nnn-1.n-K9.exe, where 4.0.1.nnn-1.n specifies the version of the agent and policy.m

Step 3 Note the location where you saved the downloaded file.

Step 4 Double-click the downloaded file to begin the installation.

Step 5 When the Welcome window displays, click **Next**.

Step 6 To accept the license agreement, click **Yes**.

Step 7 Choose a location where the software will install; click **Next**.

Step 8 Click **Next** to install the Network Shim.

Caution You must install the Network Shim for the agent to have full functionality.

Step 9 The status window displays the options that you chose. To accept the current settings, click **Next**.

Step 10 Continue to wait while the installation completes; do not click Cancel.

Step 11 Click **Yes** to reboot the server.

Caution If you want to do so, you can reboot the server at the end of the business day. Rebooting the server may cause call-processing interruptions. The agent protects the server as soon as you install the software, but the agent does not provide complete functionality until you reboot the server.

Step 12 Click **Finish**.

Tip When the installation completes, a red flag displays in the Windows 2000 system tray. You can also verify that the software installed by locating the Cisco Security Agent in the Add/Remove Programs window.

Step 13 Perform this procedure on every server in the cluster.

Disabling and Reenabling the Cisco Security Agent Service

You must disable the CSA service whenever you want to perform a task that requires the server to be restarted, such as installing, upgrading, or uninstalling software. If you disable the CSA service, you must reenable it before it starts monitoring the Cisco CallManager server again.

Caution You must disable the Cisco Security Agent service using this method before installing, uninstalling, or upgrading any software, including the operating system, Cisco CallManager, maintenance releases, service releases, support patches and plugins. Ensure that the service does not get reenabled at any time during the installation/upgrade. Failure to do so may cause problems with the installation or upgrade.

After installing, upgrading, or uninstalling the software, you must reenable the Cisco Security Agent service.

When you disable the service, the agent no longer provides intrusion detection for the server.

Caution Cisco recommends that you perform the following procedure serially, that is, on one server at a time. After you complete installing, upgrading, or uninstalling the software, you can reenable the service on the server; then, you can disable the service on the next server where you plan to perform the same software operation.

Perform the following steps to disable the CSA service.

Procedure

Step 1 Choose **Start > Settings > Control Panel > Administrative Tools > Services**.

Step 2 From the Services window, right-click **Cisco Security Agent** and choose **Properties**.

Step 3 In the Properties window, verify that the General tab displays.

Step 4 In the Service Status area, click **Stop**.

Step 5 From the Startup type drop-down list box, choose **Disabled**.

Step 6 Click **OK**.

Caution In the Service window, verify that the Startup Type of the CSA service is disabled.

Step 7 Perform this procedure on every server where you plan to install or upgrade Cisco CallManager.

Caution You must reenable the Cisco Security Agent service after installing, upgrading, or uninstalling software by performing the preceding procedure and clicking **Start**.

Suspending and Resuming the Cisco Security Agent Service

Suspending a service places the service in a state of suspended animation. When you reboot the server, the service automatically resumes. You should suspend the CSA service only if you want to perform a task that does not require restarting the server. To suspend the CSA service, you can use the *net stop* command from a command prompt or the Suspend Security menu option from the CSA icon in the Windows task bar.

Caution Do not use the suspend service method to stop the CSA service before installing, uninstalling, or upgrading software on the server. For these tasks, always use the procedure in the preceding section to disable the agent.

Verifying the Agent Version on the Server

To verify the agent version on the server, locate and run the file **C:\utils\MCSver.exe**.

Upgrading the Cisco Security Agent

Before you upgrade the Cisco Security Agent, perform the following tasks:

1. Uninstall the existing version that is installed on the server.

   See the "Uninstalling the Cisco Security Agent" section on page 9.

2. Install the new version that you plan to run on the server.

   See the "Installing the Cisco Security Agent" section on page 5.

Migrating to the Management Center for Cisco Security Agents

The security agent that is included with Cisco CallManager uses a static policy that cannot be changed or viewed. To add, change, delete, or view rules and policies that Cisco Security Agent for Cisco CallManager includes, or to add support for non-Cisco approved, third-party applications, you must purchase and install the fully managed console product, Management Center for Cisco Security Agents (CSA MC).

CSA MC contains two components:

- The Management Center installs on a secured server and includes a web server, a configuration database, and a web-based interface. The Management Center allows you to define rules and policies and create agent kits that are then distributed to agents that are installed on other network systems and servers.
- The Cisco Security Agent (the managed agent) installs on all Cisco CallManager servers in the cluster and enforces security policies. The managed agent registers with the Management Center and can receive policy and rule updates. It also sends event log reports back to its Management Center.

Before you begin, you should obtain the latest version of the following CSA MC documents:

- *Installing Management Center for Cisco Security Agents*
- *Using Management Center for Cisco Security Agents*

- *Release Notes for Management Center for Cisco Security Agents*

You can download these documents at http://www.cisco.com/en/US/customer/products/sw/cscowork/ps5212/prod_technical_documentation.html

In a Cisco CallManager environment, ensure that the Management Center component is installed on a separate, secured server and the managed agent component is installed on all Cisco CallManager servers in the cluster. Make sure that the server that is intended for the Management Center meets the system requirements that are listed in *Installing Management Center for Cisco Security Agents.*

Caution Do not install the Management Center on servers where you have installed Cisco CallManager. If you attempt to do so and the CSA MC installation detects that a version of Microsoft SQL Server runs on the server, the managed console installation automatically aborts.

After you have obtained the CSA MC package and documentation, perform the following procedure:

Step 1 On a separate (non-Cisco CallManager) server, uninstall the Cisco Security Agent, if it exists, by following the instructions in the Uninstalling the Cisco Security Agent section.

Step 2 Download the latest version of the Cisco CallManager policy XML file. You can obtain the policy on the Voice Software Download URL at http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml.

Note The Cisco Security Agent and policies post on the voice products cryptographic software site. You can navigate to the site from the voice application (Cisco CallManager, CRS, and so on) software window.

Step 3 Note the location where you saved the downloaded file.

Step 4 Install the CSA MC by following the instructions in the MC installation section of *Installing Management Center for Cisco Security Agents.*

Step 5 Follow the instructions in *Using Management Center for Cisco Security Agents* for importing the policy that you downloaded in Step 2.

Step 6 Use the Quick Start Configuration section of *Installing Management Center for Cisco Security Agents* to perform the following tasks:

- Configure a group
- Attach the policy to the group
- Build an agent kit

Step 7 Distribute and install the new managed agent that was created in Step 6 by following the instructions in the Cisco Security Agent Installation and Overview section of *Installing Management Center for Cisco Security Agents.*

Uninstalling the Cisco Security Agent

Caution You cannot install the same version of the agent on top of the version that is installed. You must uninstall the agent and then reinstall the software. When you uninstall the agent, a prompt asks whether you want to uninstall the agent. You have limited time to click Yes to disable the protection. If you choose No or wait to disable the protection, the security mode automatically enables.

After you uninstall the software, reboot the server immediately. If you do not reboot the server immediately, the flag continues to display in the Windows 2000 system tray, the Message tab in the graphical user interface (GUI) displays errors, and the software does not provide protection.

To uninstall the security agent, perform the following procedure:

Procedure

Step 1 Perform one of the following tasks:

- Choose **Start > Control Panel > Add/Remove Programs**; click **Remove** for the Cisco Security Agent; go to Step 2.
- Choose **Start > Programs > Cisco Systems > Cisco Security Agent > Uninstall Cisco Security Agent**; go to Step 2.

Step 2 To stop the agent, click **Yes**.

Step 3 To uninstall the agent, click **Yes**.

Step 4 Reboot the server.

Caution After you uninstall the software, reboot the server immediately. If you do not reboot the server immediately, the flag continues to display in the Windows 2000 system tray, the Message tab in the graphical user interface (GUI) displays errors, but the software does not provide protection.

Troubleshooting

If you encounter problems with installing or uninstalling the agent, perform the following tasks:

- Verify that you rebooted the server.
- Verify that you did not use Terminal Services to install/upgrade the software.
- Verify that you uninstalled Cisco HIDS Agent (Entercept) before the installation.
- Obtain the installation logs from C:\Program Files\Cisco\CSAgent\log. Inspect the Cisco Security AgentInstallInfo.txt and driver_install.log files.
- For installations, verify that you installed the Network Shim. The driver_install.log should state that the csanet2k.inf installed. If the Network Shim is not installed, uninstall the agent and then install the agent again.

Obtaining Additional Information About the Cisco Security Agent

For additional information on the Cisco Security Agent, perform the following procedure:

Procedure

Step 1 Perform one of the following tasks:

- In the Windows 2000 system tray, right-click the flag and choose **Open Control Panel**; go to Step 2.
- Choose **Start > Programs > Cisco Systems > Cisco Security Agent > Cisco Security Agent**; go to Step 2.

Step 2 In the upper, right corner of the window, click the **?** icon.

The Cisco Security Agent documentation displays.

Tip To obtain the Cisco Security Agent 4.0 documentation, click the following URL:

http://www.cisco.com/en/US/partner/products/sw/secursw/ps5057/index.html

Obtaining Related Cisco CallManager Documentation

Click the URLs in Table 1 to navigate to related Cisco CallManager documentation.

Table 1 Quick Reference for URLs

Related Information and Software	URL and Additional Information
Operating system documentation and Virtual Network Computing (VNC) documentation (not readme documentation)	http://www.cisco.com/univercd/cc/td/doc/product/voice/iptel_os/index.htm
Cisco MCS data sheets	http://www.cisco.com/en/US/products/hw/voiceapp/ps378/index.html
Software-only servers (IBM, HP, Compaq, Aquarius)	http://www.cisco.com/en/US/products/hw/voiceapp/ps378/prod_brochure_list.html
Cisco CallManager Compatibility Matrix	http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/index.htm
Cisco CallManager documentation	http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/index.htm
Cisco CallManager backup and restore documentation	http://www.cisco.com/univercd/cc/td/doc/product/voice/backup/index.htm

Table 1 Quick Reference for URLs (Continued)

Related Information and Software	URL and Additional Information
Cisco CallManager, SQL Server, and operating system service releases, upgrades, and readme documentation	http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml **Note** The operating system and SQL Server 2000 service releases post on the voice products operating system cryptographic software page. You can navigate to the site from the Cisco CallManager software page.
Related Cisco IP telephony application documentation	http://www.cisco.com/univercd/cc/td/doc/product/voice/index.htm
Cisco Integrated Communications System (ICS) 7750	http://www.cisco.com/univercd/cc/td/doc/product/voice/ics/index.htm

Obtaining Documentation

Cisco provides several ways to obtain documentation, 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 on the World Wide Web at this URL:

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

You can access the Cisco website at this URL:

http://www.cisco.com

International Cisco websites can be accessed from this URL:

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

Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which may have shipped with your product. The Documentation CD-ROM is updated regularly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual or quarterly subscription.

Registered Cisco.com users can order a single Documentation CD-ROM (product number DOC-CONDOCCD=) through the Cisco Ordering tool:

http://www.cisco.com/en/US/partner/ordering/ordering_place_order_ordering_tool_launch.html

All users can order annual or quarterly subscriptions through the online Subscription Store:

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

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 Networking Products MarketPlace:

  http://www.cisco.com/en/US/partner/ordering/index.shtml

- 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 800 553-NETS (6387).

Documentation Feedback

You can submit comments electronically on Cisco.com. On the Cisco Documentation home page, click **Feedback** at the top of the page.

You can send your comments in e-mail 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, Inc.
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, the Cisco Technical Assistance Center (TAC) provides 24-hour, award-winning technical support services, online and over the phone. Cisco.com features the Cisco TAC website as an online starting point for technical assistance.

Cisco TAC Website

The Cisco TAC website (http://www.cisco.com/tac) provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The Cisco TAC website is available 24 hours a day, 365 days a year.

Accessing all the tools on the Cisco TAC website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a login ID or password, register at this URL:

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

Opening a TAC Case

The online TAC Case Open Tool (http://www.cisco.com/tac/caseopen) is the fastest way to open P3 and P4 cases. (Your network is minimally impaired or you require product information). After you describe your situation, the TAC Case Open Tool automatically recommends resources for an immediate solution. If your issue is not resolved using these recommendations, your case will be assigned to a Cisco TAC engineer.

For P1 or P2 cases (your production network is down or severely degraded) or if you do not have Internet access, contact Cisco TAC by telephone. Cisco TAC engineers are assigned immediately to P1 and P2 cases to help keep your business operations running smoothly.

To open a case 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 listing of Cisco TAC contacts, go to this URL:

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

TAC Case Priority Definitions

To ensure that all cases are reported in a standard format, Cisco has established case priority definitions.

Priority 1 (P1)—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.

Priority 2 (P2)—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.

Priority 3 (P3)—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.

Priority 4 (P4)—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 Catalog* describes the networking products offered by Cisco Systems, as well as ordering and customer support services. Access the *Cisco Product Catalog* at this URL:

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

- Cisco Press publishes a wide range of networking publications. Cisco suggests these titles for new and experienced users: Internetworking Terms and Acronyms Dictionary, Internetworking Technology Handbook, Internetworking Troubleshooting Guide, and the Internetworking Design Guide. For current Cisco Press titles and other information, go to Cisco Press online at this URL:

  http://www.ciscopress.com

- Packet magazine is the Cisco quarterly publication that provides the latest networking trends, technology breakthroughs, and Cisco products and solutions to help industry professionals get the most from their networking investment. Included are networking deployment and troubleshooting tips, configuration examples, customer case studies, tutorials and training, certification information, and links to numerous in-depth online resources. You can access Packet magazine at this URL:

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

- iQ Magazine is the Cisco bimonthly publication that delivers the latest information about Internet business strategies for executives. 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/en/US/about/ac123/ac147/about_cisco_the_internet_protocol_journal.html

- Training—Cisco offers world-class networking training. Current offerings in network training are listed at this URL:

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