Release Notes for Cisco IP Telephony Backup and Restore System (BARS), Version 4.0 (7)

This Release Note contains information about this release of BARS:

- Important Information, page 1
- Checking the Compatibility Matrix, page 2
- Setting the Trace Directory Path to Default C: Drive, page 2
- Backing Up and Restoring Security for Cisco CallManager, page 3
- Resolved Issues, page 11
- Known Issues, page 11
- Obtaining Information about Additional Issues, page 11
- Obtaining Documentation, page 11
- Documentation Feedback, page 12
- Obtaining Technical Assistance, page 12
- Obtaining Additional Publications and Information, page 14

Use this document in conjunction with *Cisco IP Telephony Backup and Restore System (BARS), Version 4.0 (2),* which provides information on utility installation, configuration, and restoration procedures. To obtain this document, click the following URL:

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

Important Information

All-third party applications, including Cisco-provided and Cisco-approved applications that are co-resident on the Cisco CallManager server, must be stopped and disabled before you use the restore process.

Note Be sure to stop and disable all intrusion-detection applications, such as Cisco Security Agent and any virus-protection software, before using the restore process.

CISCO SYSTEMS

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

> **Tip** After using BARS to perform a restore, be sure to reinstall Cisco IP telephony applications/products/plugins/service releases/locales/add-on devices to versions that are compatible with the restored version of Cisco CallManager. If this is not done, you may lose data during the next upgrade of Cisco CallManager as well as losing all locales and add-on devices.

Checking the Compatibility Matrix

Be sure to check the Cisco CallManager Compatibility matrix at the following URL for information about which components have been tested with various BARS releases:

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

> **Note** If you receive a warning while using BARS that indicates an incompatibility issue, double-check the matrix. If the matrix indicates that BARS has been tested with the component that the warning specifies, you can ignore the warning.

Setting the Trace Directory Path to Default C: Drive

If you are replacing a server with four drives, Cisco recommends that you set the trace directory path on the server to the default C: drive before you back up your server. After you install Cisco CallManager on the new server, you can configure the trace drive to collect trace files.

Use the following procedure to set the trace directory path to the default:

Procedure

Step 1 In Cisco CallManager Administration, choose **Application > Cisco CallManager Serviceability**.

The Cisco CallManager Serviceability window displays.

Step 2 Choose **Trace > Configuration**.

Step 3 From the Server pane on the left side of the Trace Configuration window, click the server name or IP address of the four-disk drive server.

Step 4 Click the Cisco CallManager service.

The Trace Configuration window for the service and server displays.

Step 5 In the upper-right corner of the window, click the **SDL Configuration** link.

Step 6 In the Trace Directory Path field under Trace Output Settings, change the drive letter to **C:**.

Step 7 Click Update.

Backing Up and Restoring Security for Cisco CallManager

If you configured security in your Cisco CallManager 4.0 or 4.1 cluster, the following information applies for backups and restorations:

- Use the latest version of the Cisco IP Telephony Backup and Restore System (BARS) utility to back up data.

- BARS 4.0(7) backs up the CTL file and security-related configuration that exists in the database.

- Unless stated in this release note, all guidelines in the *Cisco IP Telephony Backup and Restore System (BARS) Administration Guide* apply.

- For a list of Cisco CallManager data that get backed up and restored, refer to the *Cisco IP Telephony Backup and Restore System (BARS) Administration Guide.*

- All CTL operations depend on the Cisco CTL Provider service in Cisco CallManager Serviceability. Ensure that the service is activated and running when you use the CTL client after restorations complete.

- Any time that you update the CTL file, always run BARS, as described in the *Cisco IP Telephony Backup and Restore System (BARS) Administration Guide*.

This section contains the following topics:

Backing Up and Restoring Security for Cisco CallManager 4.0

If you implemented the CTL client and CAPF functionality in Cisco CallManager 4.0, use the following procedures for backups and restorations:

Backing Up CAPF 1.0(1) Files For Cisco CallManager 4.0

If you use CAPF utility 1.0(1) with Cisco CallManager 4.0, perform the following procedure to back up the CAPF files.

Procedure

Step 1   Use the latest version of BARS to back up the Cisco CallManager data on the publisher database server.

Step 2   Locate the server in the cluster where you installed CAPF utility 1.0(1). Copy **capf.phone** and all **.0 files** from the CAPF installation directory to a directory on a remote computer.

The default location for the CAPF installation specifies C:\Program Files\Cisco\capf.

Restoring Data Only When Security Exists in the Cisco CallManager 4.0 Cluster

To restore 4.0 data when security exists in your Cisco CallManager 4.0 cluster, perform the following procedure:

Procedure

Step 1   Restore the data, as described in the BARS administration guide.

Step 2   Update the CTL file; sign the CTL file with a token that exists in the file and that the phone trusts.

Step 3   In Cisco CallManager Serviceability, restart the Cisco CallManager and Cisco TFTP services.

Step 4   Reset the devices.

Replacing a Secure 4.0 Publisher Database Server Where CAPF Utility 1.0(1) Was Installed

To replace a secure Cisco CallManager 4.0 publisher database server where CAPF Utility 1.0(1) was installed, perform the following procedure:

Procedure

Step 1   Obtain at least one token that exists in the current CTL file and that the phone trusts. You must use the token later in this procedure.

Step 2   On the new or rebuilt server, perform the following operating system tasks:

    a.   Use the Cisco-provided disks to install the Windows 2000 operating system.

    b.   Upgrade the operating system to match the version that currently runs in the cluster.

    c.   Apply operating system service releases to match the version that runs in the cluster.

Step 3 On the new or rebuilt server, perform the following Cisco CallManager installation tasks:

    a. Use Cisco-provided disks to install Cisco CallManager.

    b. Upgrade Cisco CallManager to match the version that runs in the cluster.

    c. Apply Cisco CallManager service releases and engineering specials to match the version that runs in the cluster.

    d. Identify the location where you previously installed CAPF on the publisher database server. Reinstall CAPF utility 1.0(1) to the same location on the new or rebuilt server, as described in *Cisco IP Phone Authentication and Encryption for Cisco CallManager 4.0*.

    e. If the CTL client previously existed on the publisher database server, go to Cisco CallManager Administration and install the CTL client.

    f. On the new or rebuilt server, install the version of BARS that created the BARS backup file in the "Backing Up CAPF 1.0(1) Files For Cisco CallManager 4.0" section on page 4.

Step 4 Use BARS to restore the data on the new or rebuilt publisher database server; verify that the restored data exists on the publisher database server.

Step 5 Copy the files that were backed up in Step 2 in the "Backing Up CAPF 1.0(1) Files For Cisco CallManager 4.0" section on page 4 to the CAPF installation directory on the new or rebuilt publisher database server.

Step 6 Run the CTL client to update the CTL file; make sure that you click the **Update CTL file** radio button and sign the file with a token that exists in the file and that the phone trusts.

    Tip Because the CTL file gets restored, do not choose the Mixed Mode or Non-Secure Mode options after you launch and run the CTL client.

Step 7 In Cisco CallManager Serviceability, restart the Cisco TFTP and Cisco CallManager services.

Step 8 Reset all devices.

Replacing a Secure 4.0 Subscriber Server Where CAPF Utility 1.0(1) Was Installed

To replace a secure Cisco CallManager 4.0 subscriber server where CAPF utility 1.0(1) was installed, performed the following procedure:

Procedure

Step 1 Obtain at least one token that exists in the current CTL file and that the phone trusts. You must use the token later in this procedure.

Step 2 Verify that you performed the tasks in the "Backing Up CAPF 1.0(1) Files For Cisco CallManager 4.0" section on page 4.

Step 3 On the new or rebuilt server, perform the following operating system tasks:

    a. Use the Cisco-provided disks to install the Windows 2000 operating system.

    b. Upgrade the operating system to match the version that currently runs in the cluster.

    c. Apply operating system service releases to match the version that runs in the cluster.

Step 4   On the new or rebuilt server, perform the following Cisco CallManager installation tasks:

    a.   Use Cisco-provided disks to install Cisco CallManager.

    b.   Upgrade Cisco CallManager to match the version that runs in the cluster.

    c.   Apply Cisco CallManager service releases and engineering specials to match the version that runs in the cluster.

    d.   Identify the location where you previously installed CAPF on the subscriber server. Reinstall CAPF utility 1.0(1) to the same location on the new or rebuilt server, as described in *Cisco IP Phone Authentication and Encryption for Cisco CallManager 4.0*.

    e.   If the CTL client previously existed on the subscriber server, go to Cisco CallManager Administration and install the CTL client.

Step 5   Copy all **.0 files** from C:\Program Files\Cisco\Certificates on the publisher database server to the C:\Program Files\Cisco\Certificates on the new or rebuilt subscriber server.

Step 6   Copy the files that were backed up in Step 2 in the "Backing Up CAPF 1.0(1) Files For Cisco CallManager 4.0" section on page 4 to the CAPF installation directory on the new or rebuilt subscriber server.

Step 7   Run the CTL client to update the CTL file; make sure that you click the **Update CTL file** radio button and sign the file with a token that exists in the file and that the phone trusts.

        🔍

    Tip   Because the CTL file gets restored, do not choose the Mixed Mode or Non-Secure Mode options after you launch and run the CTL client.

Step 8   In Cisco CallManager Serviceability, restart the Cisco CallManager and Cisco TFTP services.

Step 9   Reset all devices.

Replacing a Secure 4.0 Publisher Database Server Where CAPF Was Not Installed

To replace a secure Cisco CallManager 4.0 publisher database where CAPF utility 1.0(1) was not installed, perform the following procedure:

Procedure

Step 1   Obtain at least one token that exists in the current CTL file and that the phone trusts. You must use the token later in this procedure.

Step 2   On the new or rebuilt server, perform the following operating system tasks:

    a.   Use the Cisco-provided disks to install the Windows 2000 operating system.

    b.   Upgrade the operating system to match the version that currently runs in the cluster.

    c.   Apply operating system service releases to match the version that runs in the cluster.

Step 3   On the new or rebuilt server, perform the following Cisco CallManager installation tasks:

    a.   Use Cisco-provided disks to install Cisco CallManager.

    b.   Upgrade Cisco CallManager to match the version that runs in the cluster.

    c.   Apply Cisco CallManager service releases and engineering specials to match the version that runs in the cluster.

Step 4   If the CTL client previously existed on the publisher database server, go to Cisco CallManager Administration and install the CTL client on the new or rebuilt server.

Step 5   On the new or rebuilt server, install the version of BARS that created the BARS backup file in the "Backing Up CAPF 1.0(1) Files For Cisco CallManager 4.0" section on page 4.

Step 6   Use BARS to restore the data on the new or rebuilt publisher database server; verify that the restored data exists on the publisher database server.

Step 7   Run the CTL client to update the CTL file; make sure that you click the **Update CTL file** radio button and sign the file with a token that exists in the file and that the phone trusts.

Tip   Because the CTL file gets restored, do not choose the Mixed Mode or Non-Secure Mode options after you launch and run the CTL client.

Step 8   In Cisco CallManager Serviceability, restart the Cisco TFTP and Cisco CallManager services.

Step 9   Reset all devices.

Replacing a Secure 4.0 Subscriber Server Where CAPF Was Not Installed

To replace a secure Cisco CallManager 4.0 subscriber server where CAPF utility 1.0(1) was not installed, perform the following procedure:

Procedure

Step 1   Obtain at least one token that exists in the current CTL file and that the phone trusts. You must use the token later in this procedure.

Step 2   On the new or rebuilt server, perform the following operating system tasks:

    a. Use the Cisco-provided disks to install the Windows 2000 operating system.

    b. Upgrade the operating system to match the version that currently runs in the cluster.

    c. Apply operating system service releases to match the version that runs in the cluster.

Step 3   On the new or rebuilt server, perform the following Cisco CallManager installation tasks:

    a. Use Cisco-provided disks to install Cisco CallManager.

    b. Upgrade Cisco CallManager to match the version that runs in the cluster.

    c. If the CTL client previously existed on the subscriber server, go to Cisco CallManager Administration and install the CTL client on the new or rebuilt server.

    d. Apply Cisco CallManager service releases and engineering specials to match the version that runs in the cluster.

Step 4   Copy all **.0 files** from C:\Program Files\Cisco\Certificates on the publisher database server to C:\Program Files\Cisco\Certificates on the new or rebuilt subscriber server.

Step 5 Run the CTL client to update the CTL file; make sure that you click the **Update CTL file** radio button and sign the file with a token that exists in the file and that the phone trusts.

> ⌕
>
> **Tip** Because the CTL file gets restored, do not choose the Mixed Mode or Non-Secure Mode options after you launch and run the CTL client.

Step 6 In Cisco CallManager Serviceability, restart the Cisco CallManager and Cisco TFTP services on the subscriber server.

Step 7 Reset all devices.

Backing Up and Restoring Security for Cisco CallManager 4.1

If you implemented the CTL client and CAPF functionality in Cisco CallManager 4.1, use the following procedures for backups and restorations:

Restoring Data Only

If you implemented security, you must update the CTL file after you restore the data; sign the CTL file with a token that exists in the file and that the phone trusts.

For data restorations, you do not need to re-create the Cisco CallManager self-signed certificate/keys or the CAPF certificate/keys. If you copied the Cisco Unity certificate to all servers in the cluster prior to the data restoration, you do not need to copy the certificate again.

Replacing an Existing or Failed Secure 4.1 Publisher Database Server

When you replace an existing/failed publisher database server, the Cisco CallManager installation automatically installs the Cisco CallManager self-signed certificate/keys and the CAPF certificate/keys on the server.

If you need to replace or rebuild an existing/failed publisher database server and you configured security prior to the replacement/rebuild, perform the following procedure:

Procedure

Step 1 Obtain at least one token that exists in the current CTL file and that the phone trusts. You must use the token in Step 9.

Step 2 Use the latest version of BARS to back up the Cisco CallManager data on the existing publisher database server.

Step 3 On the new or rebuilt server, perform the following operating system tasks:

    a. Use the Cisco-provided disks to install the Windows 2000 operating system.

    b. Upgrade the operating system to match the version that currently runs in the cluster.

    c. Apply operating system service releases to match the version that runs in the cluster.

Step 4 On the new or rebuilt server, perform the following Cisco CallManager installation tasks:

    a. Use Cisco-provided disks to install Cisco CallManager.

    b. Upgrade Cisco CallManager to match the version that runs in the cluster.

    c. Apply Cisco CallManager service releases and engineering specials to match the version that runs in the cluster.

Step 5 On the new or rebuilt server, install the version of BARS that created the backup file in Step 2.

Step 6 Use BARS to restore the data on the new or rebuilt publisher database server.

Step 7 Verify that the restored data exists on the publisher database server.

Step 8 If the CTL client exists on a subscriber server or a PC/workstation, go to Step 9. If the CTL client existed on the failed publisher database server, go to Cisco CallManager Administration and install the CTL client.

> 🔎
>
> **Tip** Because the CTL file gets restored, do not choose the Mixed Mode or Non-secure cluster security option after you launch and run the CTL client.

Step 9 Run the CTL client to update the CTL file; make sure that you click the **Update CTL file** radio button and sign the file with a token that exists in the file and that the phone trusts.

Step 10 Restart the Cisco TFTP and Cisco CallManager services.

Step 11 Reset all devices.

Replacing an Existing/Failed Secure 4.1 Subscriber Server

If you are replacing an existing/failed secure subscriber server and you configured security prior to the replacement/rebuild, perform the following tasks:

Procedure

Step 1 Obtain at least one token that exists in the current CTL file and that the phone trusts. You must use the token in Step 5.

Step 2 On the new or rebuilt subscriber server, perform the following operating system tasks:

    a. Use the Cisco-provided disks to install the Windows 2000 operating system.

    b. Upgrade the operating system to match the version that currently runs in the cluster.

    c. Apply operating system service releases to match the version that currently runs in the cluster.

Step 3 On the new or rebuilt subscriber server, perform the following Cisco CallManager installation tasks:

   a. Use Cisco-provided disks to install Cisco CallManager.

   b. Upgrade Cisco CallManager to match the version that runs in the cluster.

   c. Apply Cisco CallManager service releases and engineering specials to match the version that runs in the cluster.

Step 4 If the CTL client exists on the publisher database server or a PC/workstation, go to Step 5. If the CTL client existed on the failed subscriber server, browse to Cisco CallManager Administration and install the CTL client.

> $\mathcal{Q}$
> **Tip** Because the CTL file gets restored, do not choose the Mixed Mode or Non-secure cluster security option after you launch and run the CTL client.

Step 5 Run the CTL client to update the CTL file; click the **Update CTL File** radio button and sign the file with a token that existed in the file and is trusted by the phones.

Step 6 Restart the Cisco CallManager and Cisco TFTP services.

Step 7 Reset all devices.

Restoring the 4.1 Cisco CallManager Cluster That Uses Security

The *Cisco IP Telephony Backup and Restore System (BARS) Administration Guide* describes how to restore the entire Cisco CallManager cluster in the unlikely event that every server in the cluster crashes. Before you restore a secure cluster, ensure that your situation meets all of the following criteria:

- Every server in the cluster crashed.
- You configured security prior to the restoration.
- The phones and the backup file contain a valid CTL file.

If your situation meets the preceding criteria, perform the following tasks:

1. Obtain at least one token that exists in the current CTL file and that the phone trusts.

2. Restore the entire cluster, as described in the BARS documentation. Start with the publisher database server. After you complete the restoration on the publisher database server, restore the subscriber servers one at a time.

3. If the CTL client existed on a failed server in the cluster, reinstall the CTL client on the new or rebuilt server.

4. Run the CTL client. Click the **Update CTL file** radio button and make sure that you sign the file with a token that exists in the CTL file and that the phone trusts.

> $\mathcal{Q}$
> **Tip** Because the CTL file gets restored, do not choose the Mixed Mode or Non-secure cluster security option after you launch and run the CTL client.

5. Restart the Cisco TFTP and Cisco CallManager services.

6. Reset all devices.

Resolved Issues

Table 1 describes the resolved issues (severity 1, 2 or 3) for BARS release 4.0(7):

Table 1   *Resolved Issues for BARS Release 4.0(7)*

Identifier	Headline and URL
CSCeh07856	BARS appends data to Cdr.dmp, causing disk space to get depleted.
CSCsa60945	BARS needs to back up security files. For complete procedures on how to back up and restore security files for Cisco CallManager 4.0 and Cisco CallManager 4.1, see the "Backing Up and Restoring Security for Cisco CallManager" section on page 3.
CSCsa62356	BARS 4.0.6 SR1 issues incorrect warning about wrong CAR version.

Known Issues

There are no known Sev 1, 2 or 3 issues in this release of BARS.

Obtaining Information about Additional Issues

If you have an account with Cisco.com (Cisco Connection Online), you can use the Bug Toolkit to find caveats for this product.

To use the Bug Toolkit, click the following URL:

http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl

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

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/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 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.

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

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 automatically provides recommended solutions. If your issue is not resolved using the recommended resources, your service request will be 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/

- 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://cisco.com/univercd/cc/td/doc/pcat/

- *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