Cisco BBSM 5.3 Upgrade Utility Guide

March 2004

This guide provides information for upgrading a Cisco Building Broadband Service Manager (BBSM) 5.2, 5.2a, or a Hotspot 1.0 server to software release 5.3. With this upgrade, you can use the new features provided by BBSM 5.3 without losing the current configuration of your servers. For BBSM 5.2 and 5.2a servers, this upgrade is dependent upon BBSM 5.2 Service Pack 2 (SP2). For BBSM Hotspot 1.0 servers, this upgrade is dependent upon BBSM Hotspot 1.0 Service Pack 1 (SP1).

Note The most current Cisco documentation for released products is available on Cisco Connection Online (CCO) at http://www.cisco.com. Online documents may contain updates and modifications made after the paper documents are printed.

Contents

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

Introduction

After the upgrade is installed, the software architecture on your current server is the same as the software architecture on the BBSM 5.3 and BBSM Hotspot 5.3 servers. In addition to providing new BBSM 5.3 features, this upgrade does the following:

- Performs a preinstallation check

  The upgrade removes the functionality for supporting third-party network devices. When the upgrade is launched, it checks the current network device configuration. If any third-party switches are found, a warning message appears. Installing the upgrade removes any third-party switch configurations in the database.

- Installs the following Microsoft Components:
  - Windows 2000 Service Pack 4 (SP4)
  - MSDE 2000 Service Pack 3a (SP3a)
  - MSDE updates
  - Windows 2000 Hotfixes

- Performs Security hardening

  During the upgrade procedure, security hardening is applied.

- Installs the Intel ProSet utility

  The Intel ProSet utility installs 802.1q-capable device drivers on systems that have the same type of NICs that were included in BBSM 5.2, BBSM 5.2a, or BBSM Hotspot 1.0 servers. The upgrade does not install device drivers on any other NICs, including some that are listed on the minimum spec sheet.

  The Intel ProSet utility supports these NICs:
  - BBSM 5.2—Intel(R) 82559 Fast Ethernet LAN on Motherboard
  - BBSM 5.2a—Intel(R) PRO/1000 XT Server Adapter
  - BBSM Hotspot 1.0—Intel(R) PRO/100 VM Network Connection and the Intel(R) PRO/100+ Alert on LAN* Management Adapter

  For all NICs, other than the ones listed, the following message is displayed: *The BBSM Dual VLAN feature may not be supported on the installed NIC adapters. Please check with the vendor for device driver updates.*

- Updates page sets

  After the upgrade is installed, the server contains BBSM 5.3 page sets. BBSM 5.2, 5.2a, or Hotspot 1.0 page sets that have the same name as BBSM 5.3 page sets, will be overwritten by BBSM 5.3 page sets.

Caution Before you install the upgrade, make sure that you back up any customized or modified page sets. Some page sets in the Hotspot software are not supported in BBSM 5.3. Unsupported page sets are removed from the system. Any ports that were configured to use *Free Access, Hotspot, HotspotClear,* or *BlockICSClear* will be configured to use the Access Code page set after the upgrade is applied.

These page sets are no longer supported, and the upgrade removes them from the system:

- BlockICSClear
- Free Access

  - Hotspot
  - HotspotClear
- Creates a log file

  During the upgrade, a log file (BBSM5.3UpgradeLog.txt) is created in the c:\atcom\Upgrade53 directory. This file contains installation information, such as status and error messages, and verifies that the upgrade completed successfully. A shortcut to this log file is created on the desktop.

  If an error occurs during the installation and the upgrade is not completed, the upgrade halts execution immediately, gives the user an appropriate error message to remedy the problem, and logs the error message to the log file. If an error does occur, you can run the upgrade again. After the upgrade is completed, either successfully or because of an error, the log file automatically opens in Notepad.

New and Changed Information

This section briefly describes some of the new features added to the BBSM 5.3.

System Summary web page

The BBSM System Summary web page provides status details for the BBSM server and its services.

Enhanced system event monitoring and alerts

The BBSM server now issues system events such as error, warning, and informational events to the Windows system Event Log using the standard Windows 2000 process. The server can be configured to generate Simple Network Management Protocol (SNMP) traps when an event is written into the Event Log.

Dual VLAN support

A second VLAN is now supported as an Institute of Electrical and Electronics Engineers (IEEE) protocol 802.1Q trunk to network devices so BBSM supports the separation of client traffic from management traffic.

Support for duplicate IP addresses

BBSM now supports static clients that have duplicate IP addresses. This includes multiple static clients with the same static IP address or multiple static clients with an IP address that overlaps the DHCP range on BBSM. The BBSM server automatically maps clients with duplicate static IP addresses to different network address translation (NAT) IP addresses. The client browsers are automatically redirected to the appropriate Connect page and then prompted to authenticate. This feature requires that port protection is enabled on network devices to prevent duplicate IP clients from interfering with each other.

Access codes by duration

Customers can now create an access code by duration. These access codes can be used for any amount of time within a year until no time is left for the access code.

PMS or print billing configured per server

As of this release, PMS or print billing is configured for each server, not each site.

SSL page sets disabled when SSL certificate is not installed on the BBSM server

When a secure sockets layer (SSL) certificate is not installed on a BBSM server, the page sets that require SSL cannot be chosen.

Security hardening

As of BBSM 5.3, the BBSM appliances ship with security hardening. Hardening BBSM involves disabling unnecessary services, removing and modifying registry key entries, and applying appropriate restrictive permissions to files and services to prevent exploitation. In addition to the BBSM server being hardened, other devices on the network should also be configured to ensure proper security. Examples include filtering on firewalls, access control lists, and intrusion detection systems. For additional information, see this BBSM white paper, which describes the procedure for hardening a BBSM server:

http://www.cisco.com/application/pdf/en/us/guest/products/ps533/c1244/cdccont_0900aecd80093fe0.pdf

Updated Information

The following sections provide updated information about BBSM 5.3.

Security Hardening - Terminal Services

If your server has *Terminal Services* installed, you can enhance security hardening by configuring the Terminal Services properties to limit remote access to the BBSM server from the external NIC only.

Step 1 Determine the description of the external NIC on your BBSM server:

- **a.** From the desktop, right-click **My Network Places**, then click **Properties**. The Network and Dial-up Connections window appears.
- **b.** Right-click **External**, then click **Properties**. The External Properties window appears.
- **c.** From the Connect using area, note the description of the external NIC; you need to know this information in Step 5 below.
- **d.** Close the External Properties window.
- **e.** Close the Network and Dial-up Connections window.

Step 2 Choose **Start** > **Programs** > **Administrative Tools** > **Terminal Services Configuration**. The Terminal Services Configuration window appears.

Step 3 Right-click **RDP-Tcp** and click **Properties**. The RDP-Tcp Properties window appears.

Step 4 Click the **Network Adapter** tab.

Step 5 From the Network adapter drop-down menu, choose the external NIC description.

Step 6 Verify that Maximum connections is set to **5**.

Step 7 Click **OK**.

Step 8 Close the Terminal Services Configuration window.

Single VLAN Configuration

If you are using a single VLAN configuration and Cisco Ethernet switches and want to use a non-default management VLAN ID, you must change the Ethernet switch's VLAN ID. The switch's SNMP password configured in WEBconfig must be appended with @<*management VLAN #*>, which enables BBSM to discover ports in the VLAN. For example, if the switch's SNMP read-write community string is *private* and its management VLAN # is *100*, change the switch's BBSM SNMP password to *private@100*. You can also use the Switch Discovery Wizard to specify the management VLAN when you are adding switches to BBSM.

Indexed SNMP passwords are not supported on Cisco Aironet access points. Do not append @*<VLAN ID>* to the SNMP passwords of the access points on BBSM even if the access point management VLAN ID is not 1. If a non-default management VLAN ID is used on the access points, make sure that the management VLAN is set up as a native VLAN on the access points and on the switch trunk that the access points are connected to. For more information, see CSCed74734.

Access points are not configured automatically with a default VLAN. If you add, remove, or change any VLAN configuration from an access point, you must reconfigure the access point port settings by using WEBconfig. For additional information, refer to the *Cisco BBSM 5.3 Configuration Guide*.

Dual VLAN

- For dual VLANs to be supported on the BBSM server, you must use the Intel PRO family of NICs.
- If you need to install the restore image on a BBSM 5.3 rack-mounted server, you must have the Intel PRO/1000 MT Dual Port Server Adapter, part number PWLA8492MT, installed in the lower slot or the image installation will fail. Refer to the *Cisco BBSM 5.3 Quick Start Guide* for details.
- In a multi-VLAN configuration, the VLANs associated with the trunk port should not be native because packets on a native VLAN are sent untagged to the BBSM server and the server rejects them when the internal NIC is enabled for IEEE protocol 802.1Q (specifies formatting for dual VLANs).
- If the internal NIC link speed on the BBSM 5.3 Hotspot appliance is set to auto-detect or auto-negotiate, or both, no clients can connect in the dual VLAN configuration. The internal NIC model of the D530 server is Intel Pro/1000 MT Desktop, and it does not forward packets with its link speed set to auto-negotiate after dual VLANs are configured. For it to forward packets in the dual VLAN configuration, its link speed must be set to either 100 or 1000 Mbps full duplex, depending on the speed of the switch port that it is connected to.

  Follow these steps to set the link speed of the internal NIC on the D530 server:

  1. Launch the PROset application.

     Note You can launch it from a small PROset icon in the right corner of the task bar at the bottom of the window. You can also launch it by using the executable file at this location: c:\Program Files\Intel\NCS\ProSet\Proset.exe.

  2. Click **Intel(R) Pro/1000 MT Desktop Adapter** on the left panel.
  3. Click the **Speed** tab on the right panel.
  4. Click the **100 Mbps** full-duplex or **1000 mbps** full-duplex radio button.

CyberSource

BBSM software includes a credit card accounting policy that invokes an application program interface (API) that is provided by CyberSource to interface with the CyberSource ICS credit card processing system. Included in the CyberSource API is a digital certificate, CyberSource_SJC_US.crt, which authenticates a CyberSource ICS server and a command line application, *Ecert*, to configure ICS merchant IDs from that ICS server. On January 16, 2004, the digital certificate expired and CyberSource changed its merchant ID configuration logic so that Ecert is now obsolete.

Note BBSM servers that were previously configured with CyberSource ICS merchant IDs for BBSM credit card accounting still operate correctly. It is not necessary for existing customers who are using the ICS accounting policy to make any changes on their BBSM server.

BBSM administrators who want to use the BBSM ICS credit card accounting policy must configure an ICS merchant ID on the BBSM server before end users can use any of the BBSM ICS credit card accounting page sets. One of the steps in configuring the merchant ID is to run Ecert with the merchant ID as a command line parameter. Ecert communicates with a CyberSource server, authenticated with the previously mentioned digital certificate, and generates a public/private key pair and corresponding digital certificate for the BBSM server and the specified merchant ID. The CyberSource ICS API, when invoked from BBSM, uses the generated keys and certificate to communicate credit card information with a CyberSource ICS server.

Follow these steps to obtain and use the current versions of the CyberSource server digital certificate and the Ecert application:

Step 1 From the BBSM server, go to c:\opt\ics\keys, and rename the CyberSource_SJC_US.crt file to **CyberSource_SJC_US.crt.old**.

Step 2 Go to the CyberSource website (http://www.cybersource.com/support_center/management/keyupdate).

Note You need a CyberSource account to access this page.

Step 3 Locate and download the following files to **c:\opt\ics\keys**:

- CyberSource_SJC_US.cer
- ecert-nt-3.4.10.exe

Step 4 Open a DOS window, and enter **cd c:\opt\ics\keys**.

Step 5 Press **Enter**.

Step 6 Enter **ecert-nt-3.4.10.exe <merchantID>**, where <merchantID> is your CyberSource merchant ID number, and press **Enter**.

Step 7 Enter **copy c:\opt\CyberSource\SDK\<merchantID>.*** and press **Enter**.

Step 8 Enter **copy c:\opt\CyberSource\SDK\CyberSource_SJC_US.crt** and press **Enter**.

Step 9 Close the DOS window.

Step 10 Configure BBSM to do credit card billing as described in the *Cisco BBSM 5.3 Configuration Guide* using <merchantID> as the credit card billing Merchant ID.

Site Controller

The Site Controller feature has been removed from BBSM 5.3 and is no longer supported.

Port Hopping

Configuring port hopping on a “Null: Clients connect to router” or a packet inactivity status detection type, Cisco Aironet access point, breaks packet inactivity functionality. When this happens, BBSM does not disconnect clients on time. The workaround is to disable port hopping on those network elements. If the packet inactivity status detection type is used, there is no need to turn on port hopping because packet inactivity allows clients to port hop.

IP Spoofing

As of BBSM 5.2 SP2, a new feature has been added that detects IP spoofing, which occurs when a second MAC address, such as a laptop, tries to use the same IP address. Consequently, the second MAC address is prevented from accessing the system.

Because the IP address spoofing feature blocks a DHCP client if its IP address is already associated with an existing active session, some DHCP clients cannot connect although they have IP addresses assigned through DHCP. The affected clients cannot ping BBSM’s internal NIC address. They receive “The Page Cannot Be Displayed” error message on their browsers.

This problem can occur in these situations:

1. A link status switch type is used when a hub device is connected to a switch port.
2. A hibernating client is connected to a switch that is configured as a link status switch.
3. A long packet inactivity period is used.
4. A combination of long packet inactivity and port hopping is used.

In all of these cases, BBSM maintains a session although a client is no longer in the network or is not requesting to renew the IP address. Because the DHCP server is not aware of the existing session in BBSM, it assigns the IP address to another client when the default lease time expires. When this occurs, the IP address spoofing logic in BBSM blocks packets from the IP address because packets are from a different IP and MAC combination.

IP Spoofing Workaround for Switches

For situations 1 and 2 above, the workaround is to either remove the hub or other device from the port or to change the activity detection method, which is set through WEBconfig. Otherwise, the switch type of the affected devices must be changed to the packet inactivity switch type, and the packet inactivity period must be configured to be less than 15 minutes. See the “Port Hopping” section above. Follow these steps:

Step 1 Go to the Network Elements - Switches web page in WEBconfig, and use the > button to navigate to the switch that needs modification.

Step 2 Click the **Switch Type** drop-down arrow, and change the selected switch type to the correct packet type. For example, if you are using the Cisco Catalyst 2940, you would choose Cisco Catalyst 2940 Packet. As soon as this change is made, the Packet Inactivity Period field is enabled.

Note If you need to use a long packet inactivity period or port hopping, you must increase the DHCP lease time. The minimum DHCP lease time is calculated by using the appropriate formula:

[(PIP or PHD + 15 minutes) * 2] or [(PIP + PHD + 15 minutes) * 2],
where PIP equals *Packet Inactivity Period* and PHD equals *Port Hop Delay*.

For example, if PIP equals 30 minutes and PHD equals 10 minutes, then the minimum DHCP lease time must be changed to 110 minutes [(30 + 10 + 15) * 2]. To configure the DHCP lease time, see the "Increasing the DHCP Lease Time" section on page 9.

Step 3 From the Packet Inactivity Period field, enter a value of time, in seconds, that is 15 minutes or less.

Step 4 To save the changes, click **Save**.

Step 5 Repeat for every switch needing this modification.

Only Cisco switches support Packet Inactivity switch types. If you are using other switch types, they are considered legacy devices and are not supported by TAC.

If you are using a Daily Access Policy (24 hours) and a switch that cannot support the packet inactivity detection type, another alternative is to change the DHCP lease time to 24 hours. This will guarantee that the IP address will not be given to other users within that period.

IP Spoofing Workaround for Access Points

For situations 3 and 4 above, the workaround is to reduce the packet inactivity period or the combined packet inactivity periods and port hop delay to be less than 15 minutes. See the "Port Hopping" section on page 7. To do so, follow these steps:

Step 1 Go to the Network Elements - Access Point web page in WEBconfig, and use the ">" button to navigate to the access point that needs modification.

Step 2 Under Access Point Type, change the selected access point type to the correct packet type. For example, if you are using the Cisco Aironet 1100 AP, you would choose Cisco Aironet 1100 Packet.

Note If you need to use a long packet inactivity period or port hopping, you must increase the DHCP lease time, which is calculated by using this formula:

[(PIP or PHD + 15 minutes) * 2],

where PIP equals *Packet Inactivity Period* and PHD equals *Port Hop Delay*. For example, if the PIP equals 30 minutes, then the minimum DHCP lease time would be 90 minutes [(30 + 15) * 2]. To configure the DHCP lease time, continue to the following section.

Step 3 From the Packet Inactivity Period field, enter a value of time, in seconds, that is 15 minutes or less.

Step 4 To save the changes, click **Save**.

Step 5 Repeat for every access point needing this modification.

Only Cisco access points support Packet Inactivity switch types. If you are using other access point types, they are considered legacy devices and are not supported by TAC.

Increasing the DHCP Lease Time

Follow these steps to increase the DHCP lease time:

Step 1 From the BBSM desktop, choose **Start > Programs > Administrative Tools > DHCP**. The DHCP window appears.

Step 2 Right-click the **Scope** folder and choose **Properties**. The Scope BBSM53 Properties window appears.

Note If the Properties option is not visible, wait a few seconds, and right-click the **Scope** folder again.

Step 3 In the Lease duration for DHCP clients area, enter the correct number of hours and minutes, and click **OK**.

Step 4 Close the DHCP window.

Open Caveats

This section describes caveats that have not been resolved:

- CSCee05330

  Although BBSM 5.3 SP1 enables you to configure dual VLANs with the Address Change Wizard on new BBSM 5.3 appliances, you cannot use the wizard to configure dual VLANs on most upgraded servers. This problem affects all servers that do not have this specific BBSM 5.3 internal NIC: *Intel(R) PRO/1000 MT Dual Port Server Adapter #2*. If you run the wizard with any other NIC type, the internal NIC settings are changed, and BBSM cannot communicate with the internal network. This action renders your server inoperable until you complete the manual configuration of dual VLANs.

  The workaround is to manually configure dual VLANs. For detailed steps using the Intel PROset utility, refer to the "Configuring Dual VLANs" section in the *Cisco BBSM 5.3 Configuration Guide*.

Upgrade Procedure

Please read the following important information before you begin the upgrade procedure:

- To install this upgrade, you must have Administrative rights on the BBSM 5.2 or BBSM Hotspot 1.0 servers.
- For remote upgrades, you can use *Terminal Services* or another remote access application.
- This upgrade does not require NIC connectivity.

- You cannot use WEBpatch or the Hotspot Updates tool to install this upgrade.
- Do not power down or reboot the server while the upgrade is running.

Caution After this upgrade is installed, the server contains BBSM 5.3 page sets. Before you install the upgrade, make sure that you back up any customized or modified page sets. Some page sets in the Hotspot software are not supported in BBSM 5.3. Unsupported page sets are removed from the system. Any ports that were configured to use *Free Access*, *Hotspot*, *HotspotClear*, or *BlockICSClear* will be configured to use the Access Code page set after the upgrade is applied.

Before installing this upgrade, you must replace all third-party network devices with Cisco devices and reconfigure your network. If you don't replace them, the upgrade permanently removes the configuration for all third-party network devices and renders your network inoperable. You will see a warning message before this happens.

On BBSM Hotspot 1.0 servers, the upgrade replaces the Custom Web Page Wizard with the BBSM 5.3 Page Set Wizard. After the upgrade is installed, you cannot use the BBSM 5.3 Page Set Wizard to modify any page sets that were created with the Custom Web Page Wizard. You must use the software development kit (SDK) to modify these page sets.

Follow these steps to begin the upgrade procedure:

Step 1 Insert the BBSM upgrade utility CD into the CD-ROM drive.

Step 2 Choose **Start > Run**. The Run window appears.

Step 3 Browse to **BBSM5.3Upgrade.exe** on the CD and click **Open**.

Step 4 From the Run window, click **OK**. The BBSM 5.3 Upgrade - Installation Folder window appears.

Step 5 Accept the default path, and click **Finish**. The PackageForTheWeb dialog box appears.

Caution For the upgrade to work, the files must be installed in c:\atcom\upgrade53.

Step 6 Click **Yes**, and wait while the upgrade files are extracted. The following two windows appear:

- Administrator Login
- Cisco BBSM 5.3 Upgrade

Note If you are installing the upgrade on the BBSM Hotspot 1.0 server and you are using page sets that BBSM Hotspot 5.3 no longer supports, the UpgradeInstall dialog box appears. To continue with the upgrade, click **Yes**.

If you are using a third-party network device that BBSM 5.3 does not support, the UpgradeInstall dialog box appears. To continue with the upgrade, click **Yes**.

Step 7 Enter the existing Administrator username, then enter the password twice.

Note During the upgrade, the server reboots several times. By entering an existing Administrator name and password, the upgrade automatically logs in after each reboot. If you click Cancel, the upgrade continues, but you must log in manually after each reboot.

Step 8 Click **OK**. Wait approximately 40 minutes while the upgrade automatically installs and updates the following software:

- Windows 2000 SP4
- MSDE 2000 SP3a
- Security Hardening (1)
- BBSM
- Intel PROSet
- MSDE Updates
- Windows 2000 Hotfixes
- Security Hardening (2)

Step 9 After the upgrade is installed, a log file (BBSM5.3UpgradeLog.txt) automatically opens in Notepad. Review the file, verify that the upgrade completed successfully, then close the window.

Note A shortcut to this log file is automatically created on the desktop.

Step 10 Remove the BBSM upgrade utility CD from the CD-ROM drive.

Note If you run the upgrade more than one time on the same server, the Overwrite Protection dialog box appears. To continue with the upgrade, click **Yes to All**.

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.

Related Documentation

The following documents provide information about BBSM:

- Cisco BBSM 5.3 Configuration Guide (order number DOC-7815807=)
- Cisco BBSM 5.3 Operations Guide (order number DOC-7816161=)
- Cisco BBSM 5.3 Software Installation Guide (order number DOC-7815714=)
- Cisco BBSM 5.3 Quick Start Guide (order number DOC-7816060=)
- Release Notes for Cisco BBSM 5.3 (available on Cisco.com)

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

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 submit e-mail 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, the Cisco Technical Assistance Center (TAC) provides 24-hour-a-day, 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. If you do not hold a valid Cisco service contract, please contact your reseller.

Cisco TAC Website

The Cisco TAC website 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. The Cisco TAC website is located at this URL:

http://www.cisco.com/tac

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

Using the online TAC Case Open Tool is the fastest way to open P3 and P4 cases. (P3 and P4 cases are those in which your network is minimally impaired or for which 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 the recommended resources, your case will be assigned to a Cisco TAC engineer. The online TAC Case Open Tool is located at this URL:

http://www.cisco.com/tac/caseopen

For P1 or P2 cases (P1 and P2 cases are those in which 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.

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

  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 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/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/ipj

- 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

This document is to be used in conjunction with the documents listed in the Related Documentation section.

Printed in the USA on recycled paper containing 10% postconsumer waste.