



Release Notes for Cisco BBSM 5.3

February 2004

These release notes describe features and caveats for the Cisco Building Broadband Service Manager (BBSM), version 5.3. These release notes also contain important BBSM software information.



Note

The most current Cisco documentation for released products is available at this Cisco website: http://www.cisco.com/en/US/products/sw/netmgsw/ps533/prod_release_notes_list.html.
Online documents may contain updates and modifications made after the paper documents are printed.

Contents

This release note contains the following sections:

- [Introduction, page 2](#)
- [New in Software Release 5.3, page 2](#)
- [Important Notes, page 3](#)
- [Open Caveats, page 8](#)
- [Resolved Caveats, page 10](#)
- [Obtaining Documentation, page 11](#)
- [Documentation Feedback, page 12](#)
- [Obtaining Technical Assistance, page 12](#)
- [Obtaining Additional Publications and Information, page 14](#)



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

Copyright © 2004 Cisco Systems, Inc. All rights reserved.

Introduction

Cisco Building Broadband Service Manager (BBSM) is a gateway server for public access networks that enables high-speed Internet access. BBSM enables simple “plug-and-play” access, self-provisioning of end-user services, multiple authentication and billing options, and web-based configuration, management, and reporting.

The BBSM server integrates and manages these key functions:

- **Connection**—Enables you to provide Internet access to end users regardless of the client’s network interface configurations. Network deployment options include Ethernet, Long-Reach Ethernet (LRE), wireless, and cable.
- **Authentication**—Supports multiple authentication methods, such as port-based authentication, RADIUS, and access codes.
- **Accounting**—Supports accounting and payment methods including credit cards, RADIUS, and the property management system (PMS). The PMS and credit card billing can also allow impulse charges for additional bandwidth or future value-added services.
- **Portal**—Includes a forced portal, walled garden free access, and Connect (start) pages that you can customize.
- **Bandwidth options**—Supports options such as bandwidth throttling and bandwidth reservation.
- **Network deployment and configuration**—Includes multiple features to support network installation, configuration, and testing.
- **SDK**—A comprehensive software developer’s kit (SDK) can help you develop custom access or accounting policies or a PMS module for a new PMS interface.

BBSM is available as a preloaded server appliance, or you can purchase the software separately and install it yourself. If you are installing the BBSM software, refer to the *Cisco BBSM 5.3 Installation Guide* for instructions on installing BBSM and for the minimum hardware and software requirements. For information on obtaining the installation guide and other documentation, refer to the [“Related Documentation” section on page 11](#).

New in Software Release 5.3

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 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 be 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 now configured for each server, not each site.

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

When an 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. A BBSM white paper describes the procedure for hardening a BBSM server:

http://www.cisco.com/application/pdf/en/us/guest/products/ps533/c1244/cdcont_0900aecd80093fe0.pdf

Important Notes

The following sections provide updated BBSM information.

Site Controller Note

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

Dual VLAN Note

- You must use the Intel PRO family of NICs for dual VLANs to be supported on the BBSM server.
- 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 Cisco ships the BBSM appliance with the PROset utility installed on it. You can launch it from a small PROset icon in the right-hand 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-hand panel.
3. Click the **Speed** tab on the right-hand panel.
4. Click the **100 Mbps** full-duplex or **1000 mbps** full-duplex radio button.

CyberSource Note

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 that 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.

Single-VLAN Configuration Note

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 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*.

Port Hopping Note

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 in 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 since packet inactivity allows clients to port-hop.

IP Spoofing Note

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. Since 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 Note](#)" section on page 5. 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: $[(PIP \text{ or } PHD + 15 \text{ minutes}) * 2]$ or $[(PIP + PHD + 15 \text{ minutes}) * 2]$, 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 7.

- 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 Note” section on page 5](#). 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: $[(PIP \text{ or } PHD + 15 \text{ minutes}) * 2]$ 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 for BBSM 5.2:

- CSCec52226
When there is a wrong secret (password) for the RADIUS Authentication server, the Warning message is not written to the event log.
There is no workaround.
- CSCec68543
If dual VLANs are configured on BBSM and network devices, the Switch Discovery Wizard does not properly mark uplink ports on the port maps of the network devices.
There is no workaround.
- CSCec72520
If a user forgets to unbind AtNat from the internal NIC when configuring dual VLANs, BBSM reboots continuously.

The workaround to prevent continuous reboots is to follow these steps:

1. Unplug the Ethernet cable from the internal NIC and reboot the BBSM server.
2. After the server reboots, right-click **My Network Places** and choose **Properties**. The Network and Dial-up Connections window appears.
3. Right-click **AtNatMP** and choose **Properties**. The AtNatMP Properties window appears.
4. Uncheck the **Adaptive Network Address Translation Service** check box and click **OK** to close the window.
5. Close the Network and Dial-up Connections window.
6. Plug the Ethernet cable back into the internal NIC to allow clients to use the network.



Note For additional information, see “Configuring Dual VLANs” in the *Cisco BBSM 5.3 Configuration Guide*.

- CSCec75504
Static clients (with no DNS) cannot connect when using Netscape and http proxies. Clients using Internet Explorer (IE) can connect.
The workaround is to use IE.
- CSCec79940
Clients that are configured with a specific proxy setting on their browser cannot access the Internet through BBSM. These clients can access the Start page, see the Connecting page, and ping websites, but they cannot access any web pages using the browser.

The only proxy settings that are affected by this incident are as follows:

- The proxy server is a non-dotted single word, such as *cisco*.
- The proxy port is not any of the following: 80, 8000, 8080, or 8888.

Examples:

- Client with proxy server *www.cisco.com* and port 1234 is not affected by this bug because it has a dotted proxy.
- Client with proxy server *cisco* and port 8888 is not affected by this bug because it uses proxy port 8888.
- Client with proxy server *cisco* and port 1234 is affected by this bug because it is using a non-standard port and a non-dotted proxy server.

The workaround is to disable the TCP port filtering on BBSM. To do so, follow these steps:

1. Right-click **My Network Places**, and choose **Properties**.
2. Right-click **External** and choose **Properties**. The Network and Dial-up Connections window appears.



Note Disabling the security policy on this network interface applies to both interfaces.

3. Highlight **Internet Protocol (TCP/IP)** and click **Properties**.
 4. Click **Advanced**.
 5. Click the **Options** tab.
 6. Click **IP security**.
 7. Click **Properties**. The IP Security window appears.
 8. Click the **Do not use IPSEC** radio button.
 9. Close all windows.
- CSCec87143

When the BBSM server is rebooted, the display sometimes appears at 800 x 600 and the Display Properties window shows 800 x 600 as the highest screen setting possible.

The workaround is to follow these steps:

1. From the desktop, right-click **My Computer**, and choose **Properties**. The System Properties window appears.
2. Click the **Hardware** tab.
3. Click **Device Manager**. The Device Manager window appears.
4. Expand the **Monitors** tree.
5. Right-click **Plug and Play Monitor**, and choose **Uninstall**. The Confirm Device Removal dialog box appears.
6. Click **OK**.
7. Close the Device Manager window.
8. Close the System Properties window.
9. Right-click the desktop, and choose **Properties**.
10. Click the **Settings** tab.

11. From the Screen area, choose **1024 by 768 pixels**.
 12. From the Colors area, choose **High Color (16 bit)**.
 13. Click **Apply**, and then click **OK**.
 14. Click **Yes** to accept the Monitor settings.
 15. Click **OK**.
- CSCed01326

When you use the Switch Discovery Wizard, clicking the Help button does not open any help windows and this error message appears: *The process cannot access the file because it is being used by another process.* (If you have already clicked the Help button, you do not have to close the Switch Discovery Wizard to recover.)

The workaround is to follow these steps:

1. Press **Ctrl-Alt-Delete**.
2. Click **Task Manager**.
3. Click the **Processes** tab.
4. Choose the **IEXPLORE.EXE** process, and then click **End Process**.
5. From the Task Manager Warning window, click **Yes**.
6. Close the Windows Task Manager window.

The workaround to open the Online Help instead of using the Switch Discovery Wizard Help button is to follow these steps:

1. Open the Internet Explorer browser.
2. Choose **File > Open**.
3. Click **Browse**.
4. Navigate to the `c:\atcom\www\help\wizards` folder, and choose the **SwchDiscWizOLH-Main.htm** file.
5. Click **OK**.

Resolved Caveats

This section describes caveats that have been resolved.

- CSCdz89097
The Switch Discovery Wizard no longer allows special characters in the Site Name. This prevents the WEBconfig Navigation Bar from disappearing.
- CSCdz89824
For security reasons, the default MSDE System Administrator (sa) account password is no longer accepted during the BBSM installation procedure.
- CSCea58252
When using the RADIUSClear page set, BBSM no longer posts a phantom entry in the Port_State_Radius table, which prevented customers from connecting.

- CSCea65940
Port Control now allows a user with the operator permission to make port configuration changes on a single port.
- CSCea78055
Clients can now connect if VLAN 1 is configured as a native VLAN on the 1200 access point with IOS 12.2.
- CSCeb37180
The Yahoo Messenger client with proxy enabled or the Yahoo Messenger client firewall setting enabled can no longer send and receive messages without being authenticated by BBSM.
- CSCec24304
An unauthenticated client can no longer send e-mail and download e-mail headers using Microsoft Outlook Express.
- CSCec25149
On the Subscription Home page set, the *Bandwidth Per User* field for a port in Port Control is no longer disabled, and the BBSM administrator can now set a bandwidth throttling level on a client port.
- CSCed74734
When the Switch Discovery Wizard is used to configure Cisco Aironet access points, and you specify a non-default management VLAN ID for access points, the wizard incorrectly appends @<management VLAN ID> to the access point's SNMP password on BBSM. Consequently, clients cannot connect because Cisco access points do not support indexed passwords.

The workaround is to rediscover Cisco access points with the Switch Discovery Wizard without editing the BBSM VLAN ID field (by leaving the BBSM VLAN ID as 1), or to use WEBconfig to edit and remove @<VLAN ID> from the access point's SNMP password on BBSM.

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_inpk/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Ordering tool:
<http://www.cisco.com/en/US/partner/ordering/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.

CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, *Packet*, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0705R)

Copyright © 2004 Cisco Systems, Inc. All rights reserved.

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