



# Release Notes for Cisco Unified Operations Manager 2.0

---

These release notes are for use with Cisco Unified Operations Manager (Operations Manager).

These release notes provide:

- [New Features, page 1](#)
- [Product Documentation, page 2](#)
- [Related Documentation, page 3](#)
- [Circumstances that Can Affect Data, page 3](#)
- [Known Problems, page 4](#)
- [Resolved Problems, page 19](#)
- [Obtaining Documentation, page 20](#)
- [Documentation Feedback, page 20](#)
- [Cisco Product Security Overview, page 21](#)
- [Product Alerts and Field Notices, page 22](#)
- [Obtaining Technical Assistance, page 22](#)
- [Obtaining Additional Publications and Information, page 24](#)

## New Features

Cisco Unified Operations Manager adds the following:

- Trunk group modeling; performance, capacity, and availability monitoring.
- Support for video endpoint discovery, monitoring, and reporting.
- Acceptance testing, phone-feature testing, dial-plan validation, and phone-to-phone testing.
- New device support:
  - Cisco Unified CallManager 5.1
  - Cisco Unified Presence Server



---

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

© 2006 Cisco Systems, Inc. All rights reserved.

- Cisco SIP Proxy Server
- Cisco Unity Express 2.3
- Feature-based licensing. You can purchase two levels of functionality for Operations Manager: Premium Edition and Standard Edition.
- Enhancements to:
  - Device monitoring.
  - Synthetic testing.
  - Phone reporting.
  - Performance graphing.

## Product Documentation



### Note

The originally published printed and electronic documentation is included with your product. Any changes after original publication are reflected on Cisco.com, where you will find the most up-to-date documentation.

Table 1 describes the product documentation that is available.

**Table 1**      **Product Documentation**

Document Title	Available Formats
<i>Release Notes for Cisco Unified Operations Manager 2.0</i>	<ul style="list-style-type: none"> <li>• Printed document that was included with the product.</li> <li>• PDF on the product CD-ROM.</li> <li>• On Cisco.com at the following URL: <a href="http://www.cisco.com/en/US/products/ps6535/prod_release_notes_list.html">http://www.cisco.com/en/US/products/ps6535/prod_release_notes_list.html</a></li> </ul>
<i>Quick Start Guide for Cisco Unified Operations Manager 2.0</i>	<ul style="list-style-type: none"> <li>• Printed document that was included with the product.</li> <li>• PDF on the product CD-ROM.</li> <li>• On Cisco.com at the following URL: <a href="http://www.cisco.com/en/US/products/ps6535/prod_installation_guides_list.html">http://www.cisco.com/en/US/products/ps6535/prod_installation_guides_list.html</a></li> </ul>
<i>Installation Guide for Cisco Unified Operations Manager (Includes Service Monitor) 2.0</i>	<ul style="list-style-type: none"> <li>• PDF on the product CD-ROM.</li> <li>• On Cisco.com at the following URL: <a href="http://www.cisco.com/en/US/products/ps6535/prod_installation_guides_list.html">http://www.cisco.com/en/US/products/ps6535/prod_installation_guides_list.html</a></li> </ul>
<i>User Guide for Cisco Unified Operations Manager 2.0</i>	<ul style="list-style-type: none"> <li>• PDF on the product CD-ROM.</li> <li>• On Cisco.com at the following URL: <a href="http://www.cisco.com/en/US/products/ps6535/products_user_guide_list.html">http://www.cisco.com/en/US/products/ps6535/products_user_guide_list.html</a></li> </ul>
<i>Supported Devices Table for Cisco Unified Operations Manager 2.0</i>	On Cisco.com at the following URL: <a href="http://www.cisco.com/en/US/products/ps6535/products_device_support_tables_list.html">http://www.cisco.com/en/US/products/ps6535/products_device_support_tables_list.html</a>
Context-sensitive online help	<ul style="list-style-type: none"> <li>• Select an option from the navigation tree, then click <b>Help</b>.</li> <li>• Click the Help button in the page.</li> </ul>

## Related Documentation


**Note**

We sometimes update the printed and electronic documentation after original publication. Therefore, you should also review the documentation on Cisco.com for any updates.

[Table 2](#) describes the additional documentation that is available.

**Table 2**      **Related Documentation**

Document Title	Available Formats
<i>Release Notes for Cisco Unified Service Monitor 2.0</i>	<ul style="list-style-type: none"> <li>PDF on the product CD-ROM</li> <li>On Cisco.com at the following URL: <a href="http://www.cisco.com/en/US/products/ps6536/prod_release_notes_list.html">http://www.cisco.com/en/US/products/ps6536/prod_release_notes_list.html</a></li> </ul>
<i>User Guide for Cisco Unified Service Monitor 2.0</i>	<ul style="list-style-type: none"> <li>PDF on the product CD-ROM.</li> <li>On Cisco.com at the following URL: <a href="http://www.cisco.com/en/US/docs/net_mgmt/cisco_unified_service_monitor/2.0/user/guide/usrgd.html">http://www.cisco.com/en/US/docs/net_mgmt/cisco_unified_service_monitor/2.0/user/guide/usrgd.html</a></li> </ul>
<i>Release Notes for CiscoWorks Common Services 3.0.3 (Includes CiscoView 6.1.2) on Windows</i>	<ul style="list-style-type: none"> <li>PDF on the product CD-ROM.</li> <li>On Cisco.com at the following URL: <a href="http://www.cisco.com/en/US/docs/net_mgmt/cisoworks_common_services_software/3.0.5/release/windows/notes/CWCS_RNW_305.html">http://www.cisco.com/en/US/docs/net_mgmt/cisoworks_common_services_software/3.0.5/release/windows/notes/CWCS_RNW_305.html</a></li> </ul>
<i>Installation and Setup Guide for CiscoWorks Common Services (Includes CiscoView) on Windows</i>	<ul style="list-style-type: none"> <li>PDF on the product CD-ROM.</li> <li>On Cisco.com at the following URL: <a href="http://www.cisco.com/en/US/docs/net_mgmt/cisoworks_common_services_software/3.0.5/installation/windows/guide/cs305igw_1.html">http://www.cisco.com/en/US/docs/net_mgmt/cisoworks_common_services_software/3.0.5/installation/windows/guide/cs305igw_1.html</a></li> </ul>
<i>User Guide for CiscoWorks Common Services</i>	<ul style="list-style-type: none"> <li>PDF on the product CD-ROM.</li> <li>On Cisco.com at the following URL: <a href="http://www.cisco.com/en/US/docs/net_mgmt/cisoworks_common_services_software/3.0.5/installation/windows/guide/cs305igw_1.html">http://www.cisco.com/en/US/docs/net_mgmt/cisoworks_common_services_software/3.0.5/installation/windows/guide/cs305igw_1.html</a></li> </ul>

## Circumstances that Can Affect Data

[Table 3](#) documents problems you may encounter.

**Table 3** *Circumstances that Can Affect Data*

Description	Circumstances
<p>No DSP records for Voice Interface Cards (VICs) that are supported by the following network modules:</p> <ul style="list-style-type: none"> <li>NM-1V</li> <li>NM-2V</li> <li>NM-HDA</li> </ul> <p>Affected record type: 109</p>	<p>CISCO-DSP-MGMT-MIB is not supported on the listed network modules. This bug applies to all devices that support them.</p> <p>Bug ID: CSCeb62542</p>
<p>Number of CAS ports is incorrect and CAS channel status is missing for all supported network devices that run Cisco IOS except for Cisco Universal Gateways. GSU always reports the number of CAS ports as follows:</p> <ul style="list-style-type: none"> <li>24 ports for each T1</li> <li>31 ports for each E1</li> </ul> <p>For example, if a device has two T1 ports, Operations Manager reports the total number of T1 CAS ports as 48, no matter how many CAS ports are configured on the device.</p> <p>Affected record types: 102, 112, 113</p>	<p>Except for Cisco Universal Gateways, the network devices that run Cisco IOS do not support CISCO-POP-MGMT-MIB.</p> <p>Bug IDs: CSCdm87395, CSCdx04678</p>

## Known Problems

Table 4 describes problems known to exist in this release.

**Table 4** *Known Problems in Operations Manager*

Bug ID	Summary	Explanation
CSCsb60614	Cluster name changes are not reflected in Operations Manager.	<p>If you change the name of a cluster in Cisco Unified CallManager after the devices have been added to Operations Manager, the name change does not occur in Operations Manager. This is the case even after performing inventory collection.</p> <p>Workaround:</p> <p>Delete the devices in the cluster from Operations Manager and then re-add the devices.</p>
CSCsb63311	In the Service Quality Alerts display, filtering does not work when using multiple criteria.	<p>Using multiple filtering options at one time to customize the Service Quality Alerts display does not work correctly.</p> <p>Workaround:</p> <p>Filter the Service Quality Alerts display based on a single criterion.</p>

**Table 4**      **Known Problems in Operations Manager (continued)**

Bug ID	Summary	Explanation
CSCsb66977	Voice application software (for example, Cisco Conference Connection, Cisco Unified CallManager, or Cisco Emergency Responder) goes to the Unsupported state.	<p>On some servers that have voice application software installed, rebooting causes the server to go to the Unsupported state in Operations Manager.</p> <p>The problem occurs on servers that have the Windows operating system version upgraded to 2000.2.7sr3 or 2000.4.1.</p> <p>The problem is caused by incompatibility between the CDP driver installed by the voice application and Microsoft Security hotfix MS05-019. For more information regarding the hotfix, see the Microsoft website for more details.</p> <p>Workaround:</p> <p>Upgrade the CDP driver on the voice application server.</p> <ol style="list-style-type: none"> <li>1. Uninstall the CDP driver from the voice application server. Run the following command: <pre>C:\Program Files\Cisco\Bin&gt; cdpinstaller -v -u CISCO_CDP</pre> </li> <li>2. Log on to any Cisco Unified CallManager 4.1 server and copy the following files to the voice application server. <ul style="list-style-type: none"> <li>• CDP.SYS (C:\Program Files\Cisco\Bin)</li> <li>• CDPintf.dll (C:\WINNT\system32)</li> <li>• CDPInstaller.exe</li> <li>• CDP.inf</li> </ul> </li> <li>3. Install the new CDP driver by running the following command: <pre>C:\program files\Cisco\Bin&gt; cdpinstaller -v -l "C:\Program Files\Cisco\Bin\cdp.inf" -c p -i CISCO_CDP</pre> </li> </ol>
CSCsb73004	An error occurs when you launch a trending graph for a device when the time of the graph is configured for more than 48 minutes in the past.	<p>The error states that there is not any data available for the last 48 minutes. This error occurs due to an incorrect system uptime in the device.</p> <p>This error occurs in specific Cisco IOS versions. Refer to the Cisco IOS IP SLA bugs, CSCin66315 and CSCeb46870.</p> <p>Workaround:</p> <p>Upgrade the Cisco IOS version, or reboot the source device. For details, see CSCin66315 and CSCeb46870.</p>

Table 4 Known Problems in Operations Manager (continued)

Bug ID	Summary	Explanation
CSCsb83202	OperationallyDown events for voice ports are being cleared automatically, even though the port is still down in the router.	<p>The operationallyDown event for voice ports in routers are being cleared even though the port continues to be down.</p> <p>Operations Manager only sends an operationallyDown alarm if the operating status (the OperStatus for this router) is in one of the following states:</p> <ul style="list-style-type: none"> <li>• Down (2).</li> <li>• Testing (3) (If not suppressing testing-related alarms).</li> </ul> <p>If, during a polling cycle, the <i>ifOperStatus</i> is Down (2), the alarm is generated. If, during the next polling cycle, the <i>ifOperStatus</i> is Dormant (5), the operationallyDown alarm is cleared because it is not Down (2) or Testing (3).</p> <p>Related bug: CSCsb87389.</p> <p>Workaround: None.</p>
CSCsc07502	Some screens in Operations Manager are not sized correctly when opened.	<p>Several popup screens open with the status bar covering the bottom of the screen. Some popups are not resizable, and the buttons located at the bottom right are covered by the status bar.</p> <p>This occurs only with Windows XP Service Pack 2 using Microsoft Internet Explorer, and with certain security settings configured. The security settings are applied when the Operations Manager server is put in a security zone where the sizing of popups opened by scripts is disabled.</p> <p>Workaround:</p> <p>For detailed instructions, access this bug through Cisco Software Bug Toolkit at <a href="http://www.cisco.com/cgi-bin/Support/Bugtool/home.pl">http://www.cisco.com/cgi-bin/Support/Bugtool/home.pl</a>. (You will be prompted to log into Cisco.com.)</p> <p>To fix the problem, the Allow script-initiated windows without size or position constraints option should be enabled for the security zone that the Operations Manager server is in.</p> <p>Do one of the following:</p> <ul style="list-style-type: none"> <li>• Enable the setting, Allow script-initiated windows without size or position constraints, for the security zone that the Operations Manager server is in.</li> <li>• Add the IPCOM server site to the local intranet or trusted security zone.</li> </ul> <p><b>Note</b> In many cases, using the server name instead of the IP address in the browser will fix the problem. But the Operations Manager server must be in the same domain as the client, and DNS must be configured correctly. Alternatively, you can add the IP address to the Local Intranet or Trusted security zone.</p>

Table 4 Known Problems in Operations Manager (continued)

Bug ID	Summary	Explanation																								
CSCsc10167	On the Alert Details page, once a tool is launched, you cannot relaunch it.	In the Alert Details page, once you select a tool from the Launch Tools menu you cannot launch the selected tool again until you choose another tool.  Workaround:  After launching a tool, to launch the same tool again, you must either select a different tool or select the Launch Tools option in the menu.  After doing either of these actions, you can relaunch your original choice.																								
CSCsc12967	Exchange services are displayed as stopped when Cisco Unity is configured for failover.	When Cisco Unity is configured for failover mode, Operations Manager shows Microsoft Exchange Services as being stopped.  Workaround: None.																								
CSCsc44538	The DFMServer and VHMServer processes are not registering with the broker.  Devices that are added to Operations Manager when it is in this condition exhibit the following behavior: <ul style="list-style-type: none"> <li>• ALL devices become stuck in the Inventory Collection in Progress state.</li> <li>• All devices move to the unreachable state.</li> </ul>	After installing Operations Manager and rebooting the server, either the DFMServer, or the VHMServer, or both processes do not start. There is no sm_server.exe instance (or there are only two sm_server.exe instances) in the Windows task manager.  Workaround:  Perform the following: <ol style="list-style-type: none"> <li>1. Run <code>net stop crmdmgt.</code></li> <li>2. Wait 15 minutes.</li> <li>3. Run <code>net start crmdmgt.</code></li> </ol> After the CPU cools down, check the Windows task manager. There should be four instances of sm_server.exe.  The output of the <b>brcontrol</b> command should show both DFM and VHM.  For example:  C:\Program Files\CSCOp\objects\smarts\bin>brcontrol  Broker is located at: IPCOM-daily:9002 Started: Jan 06 10:21:09 2006 <table border="1"> <thead> <tr> <th>Domain</th> <th>Host Name</th> <th>Port</th> <th>Proc ID</th> <th>State</th> <th>Last Chg Time</th> </tr> </thead> <tbody> <tr> <td>-----</td> <td>-----</td> <td>-----</td> <td>-----</td> <td>-----</td> <td>-----</td> </tr> <tr> <td>DFM</td> <td>IPCOM-daily.cisco.com</td> <td>2163</td> <td>14120</td> <td>RUNNING</td> <td>Jan 06 16:18:03 2006</td> </tr> <tr> <td>VHM</td> <td>IPCOM-daily.cisco.com</td> <td>2206</td> <td>8856</td> <td>RUNNING</td> <td>Jan 06 16:18:04 2006</td> </tr> </tbody> </table>	Domain	Host Name	Port	Proc ID	State	Last Chg Time	-----	-----	-----	-----	-----	-----	DFM	IPCOM-daily.cisco.com	2163	14120	RUNNING	Jan 06 16:18:03 2006	VHM	IPCOM-daily.cisco.com	2206	8856	RUNNING	Jan 06 16:18:04 2006
Domain	Host Name	Port	Proc ID	State	Last Chg Time																					
-----	-----	-----	-----	-----	-----																					
DFM	IPCOM-daily.cisco.com	2163	14120	RUNNING	Jan 06 16:18:03 2006																					
VHM	IPCOM-daily.cisco.com	2206	8856	RUNNING	Jan 06 16:18:04 2006																					
CSCsc61752	In the Service Level View, when Cisco IP Contact Center (IPCC) is part of a user-defined view, it only appears in the tree view (view pane).	User-defined views in the Service Level View do not show Cisco IP Contact Centers in the map display pane. They only appear in the view pane.  Workaround: None.																								

Table 4 Known Problems in Operations Manager (continued)

Bug ID	Summary	Explanation
CSCsc87486	In the Personalized report, not all the graphs are shown for the node-to-node test violations.	<p>In the Personalized report for node-to-node tests, 24-Hour History shows the graph for only the following metrics:</p> <ul style="list-style-type: none"> <li>• Source-to-Destination Packet Jitter.</li> <li>• Destination-to-Source Packet Jitter.</li> <li>• Average Latency.</li> </ul> <p>No other graphs are displayed.</p> <p>Workaround: None.</p>
CSCsc91915	When creating node-to-node tests, errors are displayed when the test limit is exceeded.	<p>When creating more node-to-node tests than allowed (the limit is 250), the following errors are displayed:</p> <ul style="list-style-type: none"> <li>• Exceeding the test limit.</li> <li>• No selected studies. Please check field(s) for invalid entries.</li> </ul> <p>Workaround: None.</p> <p>You can ignore the error messages.</p>
CSCsd21804	Learning appears in the Device Type column of the Alerts and Events display.	<p>On the Alerts and Events display and the Alert Details page, you may see <i>Learning</i> in the Device Type column. Learning indicates that Operations Manager was discovering the device when the alert occurred. The following events can trigger an alert during discovery:</p> <ul style="list-style-type: none"> <li>• Duplicate IP (might be generated for any type of device)</li> <li>• Events for media servers only: <ul style="list-style-type: none"> <li>– FanDown</li> <li>– FanDegraded</li> <li>– TemperatureSensorDown</li> <li>– TemperatureSensorDegraded</li> </ul> </li> </ul> <p>Workaround:</p> <ul style="list-style-type: none"> <li>• Simply wait; the actual device type is reflected in the Device Type column when new events occur.</li> <li>• Look up the current state of a device from the Detailed Device View, which always displays the current state.</li> </ul>

**Table 4**      **Known Problems in Operations Manager (continued)**

Bug ID	Summary	Explanation
CSCsc26996	Next Discovery, in the Device Management: Summary page, displays the incorrect time.	<p>The problem is due to a registry setting in Windows that appears for certain time zones for which Daylight Saving Time changes are applicable. If the check box for Daylight Saving Time is not checked, problems occur when converting valid date strings to a Date object. This registry key remains even if the time zone of the machine is switched to another time zone for which Daylight Saving Time is not applicable.</p> <p>Following is the registry information:</p> <p>HKEY_LOCAL_MACHINE\CurrentControlSet\Control\TimeZoneInformation</p> <p>DisableAutoDaylightTimeSet REG_DWORD 0x00000001(1)</p> <p>Workaround:</p> <p>If the system is in a time zone that has Daylight Saving Time, check the Automatically adjust for Daylight Saving Time changes check box.</p> <p>If the system is in a time zone for which Daylight Saving Time is not applicable, but the registry key is present and set to 1, do the following:</p> <ol style="list-style-type: none"> <li>1. Change to a time zone for which Daylight Saving Time is applicable.</li> <li>2. Check the Automatically adjust for Daylight Saving Time changes check box, and click <b>Apply</b>.</li> </ol> <p>This will cause the registry key to disappear. Now switch the machine to its present time zone.</p>
CSCsd22730	Automatic discovery does not discover Cisco Unity Express devices.	<p>During automatic discovery, using either ping sweep or CDP, Cisco Unity Express devices are discovered. These devices go into the Unreachable state.</p> <p>Workaround:</p> <p>Manually add Cisco Unity Express devices into Operations Manager.</p>
CSCsd58055	The Devices report may show a device's capability as UnknownMDFType.	<p>The Devices report displays a device's capability as UnknownMDFType when the device is not supported by Operations Manager.</p> <p>Workaround: None.</p>
CSCsd69455	The right-click menu in the Service Level View does not display some of the options for Cisco Unified CallManagers.	<p>When you right-click on a Cisco Unified CallManager in the Service Level View, not all the menu items are available in the list. Also, in the Detailed Device View for a Cisco Unified CallManager's device capabilities, Media Server and Host are not displayed.</p> <p>Workaround:</p> <p>Rediscover the Cisco Unified CallManager.</p>

Table 4 Known Problems in Operations Manager (continued)

Bug ID	Summary	Explanation
CSCsd71626	The Service Level View does not display a Cisco Unified CallManager cloud that was previously displayed.	<p>During initial discovery or when the Operations Manager server boots up, if the Cisco Unified CallManager Service is down on all members of the cluster, this cluster will not show up in the Service Level View.</p> <p>Workaround:</p> <p>Rediscover the device once the Cisco Unified CallManager is reachable and the Cisco Unified CallManager Service is running on the Cisco Unified CallManagers.</p>
CSCsd81030	Error in attaching to the DfmBroker.	<p>After installing Operations Manager, rebooting, and importing devices for discovery, all devices go to the unreachable state. An error occurs when trying to attach to the DFMBroker.</p> <p>To verify this, do the following:</p> <ol style="list-style-type: none"> <li>1. Open a command prompt and go to: &lt;NMSROOT&gt;\objects\smarts\bin.</li> </ol> <p><b>Note</b> NMSROOT is the directory where Operations Manager is installed on your system. If you selected the default directory during installation, it is C:\Program Files\CSCOpX.</p> <ol style="list-style-type: none"> <li>2. Run <code>brcontrol1</code>. You will see the following message:  Error attaching to broker: IPCOM-PERF4GBL:9002</li> </ol> <p>Workaround:</p> <p>Do the following:</p> <ol style="list-style-type: none"> <li>1. Open a command prompt.</li> <li>2. Run <code>net stop crmdmgt.d</code>.</li> <li>3. Wait 15 minutes.</li> <li>4. Run <code>net start crmdmgt.d</code>.</li> </ol> <p>After the CPU cools down, check the Windows task manager. There should be four instances of <code>sm_server.exe</code> and two instances of <code>brstart.exe</code>.</p>
CSCse75607	Unreachable devices are displayed in Operations Manager device management.	<p>If the SNMP agent on a device is working intermittently, Operations Manager may discover the device, but may move it to the unreachable state during inventory collection.</p> <p>This occurs because the device was responding to SNMP queries during automatic discovery, then did not respond to SNMP queries during inventory collection.</p> <p>Workaround: None.</p>


**Table 4** Known Problems in Operations Manager (continued)

Bug ID	Summary	Explanation
CSCse78310	Detailed Device View for Cisco Unity devices displays incorrect information	<p>For Cisco Unity releases prior to 4.2, the Detailed Device View shows the following:</p> <ul style="list-style-type: none"> <li>• Current Number Of Licensed Subscribers as Not Available.</li> <li>• Maximum Number of Licensed Subscribers as Not Available.</li> <li>• Current Number of Inbox Licenses as Not Available.</li> <li>• Maximum Number of Inbox Licenses as Not Available.</li> <li>• Even though Cisco Unity 4.0(4) is upgraded to 4.0(5), the version on all services is still shown as 4.0(4).</li> </ul> <p>Workaround: Upgrade to Cisco Unity 4.2, then run RSK Configuration Wizard.</p> <p><b>Note</b> This workaround applies only to the Cisco Unity service version issue. The workaround does not fix the first four counter issues mentioned above. There is no workaround for those issues.</p>
CSCsf05654	Some PRI channels are showing as active, even though they are inactive.	<p>For PRI channels, D channels are always shown as active. Therefore, the four T1 ports on the Cisco Unified CallManager record (record 100) appear active. As a result, four out of a total of 96 channels appear active.</p> <p>This also applies to the MGCP gateway data record (record 101); two D channels are active on the two T1 ports.</p> <p>D channels are always shown as active in the case of PRI channels.</p> <p>Workaround: None.</p>
CSCsf06360	The Service Impact Report displays incorrect information for a gateway's unresponsive event, if it is part of a route list or route group.	<p>The Service Impact Report may display incorrect information (all routes lost) when the following occurs:</p> <ul style="list-style-type: none"> <li>• A gateway is part of a route list or route group.</li> <li>• Another device (switch) also forms a route group that is part of the same route list.</li> <li>• Gateway becomes unresponsive.</li> </ul> <p>The Service Impact Report is incorrect, because the other route group is still active. Calls will continue to go through the other route group.</p> <p>This problem affects the number of calls that can pass through the route list.</p> <p>Workaround: None.</p>
CSCsf15041	The device MCS7825I (with the sysObjectID 1.3.6.1.4.1.9.1.746) is listed as UnKnownMDFType.	<p>Operations Manager displays Cisco 7800 Series Media Convergence Server MCS7825I (with the sysObjectID 1.3.6.1.4.1.9.1.746) capabilities as UnKnownMDFType.</p> <p>The sysObjectID 1.3.6.1.4.1.9.1.746 is not supported. See bug ID CSCsf15027.</p> <p>Workaround: None.</p>

**Table 4** *Known Problems in Operations Manager (continued)*

<b>Bug ID</b>	<b>Summary</b>	<b>Explanation</b>
CSCsf18921	Threshold settings appear incorrectly in performance graphs.	Configured thresholds for route list and route group are displayed incorrectly in performance graphs. Only one threshold setting appears in the graph.  Workaround: None.
CSCsf19029	Message-Waiting Indicator synthetic tests on Cisco Unity and Cisco Unity Express fail periodically.	Message-Waiting Indicator synthetic tests created on Cisco Unity and Cisco Unity Express may fail.  Workaround: None.
CSCsf27034	Route group and route list calculation limitations for MGCP and H323 gateway.	For MGCP gateways, route group, and route list, utilization is calculated for all channels of the T1/E1 ports even though partial T1/E1 circuits are configured. Operations Manager gets the data from Cisco Unified CallManager, and the data does not contain the MGCP port configuration information.  For H323 gateways, all ports which are part of the device are included in the route group and route list calculation even though not all of the ports are configured for call routing. This limitation is also caused by Cisco Unified CallManager not having the required information.  Workaround: None.
CSCsf98008	In the Detailed Device View for negative synthetic tests, the success criterion for end-to-end calls and phone registration always shows availability as 100 percent.	In the Detailed Device View for negative tests, the availability is displayed as 100 percent and failure as 0 percent. These two settings are not applicable to the negative synthetic tests. The Detailed Device View should display N/A for this field.  Workaround:  None.


Table 4 Known Problems in Operations Manager (continued)

Bug ID	Summary	Explanation
CSCsg25738	Unable to collect performance data on Cisco IP Contact Center devices.	<p>If the Windows services are not started correctly on the Cisco IP Contact Center system, you will not be able to collect performance data.</p> <p>You must enable the extension.</p> <p>Workaround:</p> <p>Use Regedit.exe to enable the extension.</p> <hr/> <p> <b>Caution</b> If you use Registry Editor incorrectly, you may cause serious problems that may require you to reinstall your operating system. Microsoft cannot guarantee that you can solve problems that result from using Registry Editor incorrectly. Use Registry Editor at your own risk.</p> <hr/> <ol style="list-style-type: none"> <li>1. Start Regedit.exe. (You cannot use Regedt32.exe because it does not allow searching for registry values.)</li> <li>2. Select the following key: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services</li> <li>3. Click the <b>Edit</b> menu and select <b>Find</b>.</li> <li>4. In the Find What field, type <b>Disable Performance Counters</b>.</li> <li>5. Click <b>Find Next</b>. This will locate a performance key that may have the registry value set to 1.</li> <li>6. If the registry value is set to 1, set the value to 0 or delete the registry value.</li> <li>7. Press <b>F3</b> to find the next occurrence of this registry value.</li> <li>8. Repeat the previous two steps until there are no performance keys that have the Disable Performance Counters value set to 1.</li> </ol> <p><b>Note</b> The Disable Performance Counters value may not appear in the registry. The value can be created and given a DWORD value of 1 to disable counters.</p>
CSCsg63640	The More Tools option in the right-click menu of the Service Level View does not work for some devices.	<p>For some devices, when you click the More Tools option in the right-click menu of the Service Level View, nothing appears. This occurs if the version of Macromedia Flash on the client system is lower than 8.0.</p> <p>Workaround:</p> <p>Upgrade to Macromedia Flash 8.0.</p>

**Table 4**      **Known Problems in Operations Manager (continued)**

<b>Bug ID</b>	<b>Summary</b>	<b>Explanation</b>
CSCsg63657	The data files 147 and 148 are not updated when a Cisco Unified CallManager becomes unresponsive.	When a Cisco Unified CallManager fails to respond to Operations Manager requests, route group and route list information is not obtained. Therefore, no error logs are generated for the route group and route list data files in the performance collection folder (%NMSROOT%\data\gsu\_#GSUDATA#_).  Workaround: None.

**Table 4**      **Known Problems in Operations Manager (continued)**

Bug ID	Summary	Explanation
CSCsg62467	Operations Manager does not discover IP phones if the number of ports in the network is greater than 30,000.	<p>If the number of ports in your network is greater than 30,000, Operations Manager does not discover the IP phones in your network. This occurs because the PIFServer runs out of memory.</p> <p>The maximum memory setting for the PIFServer process must be increased. The default maximum memory value is 300 MB, which supports 30,000 phones and 30,000 ports.</p> <p>If the number of phones and ports is greater than these numbers, the PIFServer's maximum memory setting must be increased.</p> <p>Use the following guidelines for determining the maximum memory setting:</p> <ul style="list-style-type: none"> <li>• 300 MB—30,000 phones and 30,000 ports</li> <li>• 350 MB—30,000 phones and 50,000 ports</li> <li>• 400 MB—30,000 phones and 80,000 ports</li> <li>• 500 MB—30,000 phones and more than 1,00,000 ports</li> </ul> <p>Workaround:</p> <p>To update the maximum memory:</p> <ol style="list-style-type: none"> <li>1. On the Operations Manager system, open the Registry Editor by entering <b>regedit</b> in the Run window.</li> </ol> <div style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <p> <b>Caution</b> If you use Registry Editor incorrectly, you may cause serious problems that may require you to reinstall your operating system. Microsoft cannot guarantee that you can solve problems that result from using Registry Editor incorrectly. Use Registry Editor at your own risk.</p> </div> <ol style="list-style-type: none"> <li>2. Select the following key: HKEY_LOCAL_MACHINE\SOFTWARE\Cisco\Resource Manager\CurrentVersion\Daemons\PIFServer</li> <li>3. Edit the value for Args and replace the sub-string <i>-Xmx300m</i> with the appropriate value. For example, if you need to set the maximum memory setting to 400 MB change <i>-Xmx300m</i> to <i>-Xmx400m</i>.</li> <li>4. Click <b>OK</b> to save the changes.</li> <li>5. Close the Registry Editor window.</li> <li>6. Restart the daemon manager by entering the following commands in a command prompt: <pre>net stop crmdmgt net start crmdmgt</pre> </li> </ol>

**Table 4** *Known Problems in Operations Manager (continued)*

<b>Bug ID</b>	<b>Summary</b>	<b>Explanation</b>
CSCsg96469	Cisco Unified CallManager related service outages are not properly identified in Operations Manager.	When a Cisco Unified CallManager service outage occurs the event generated by Operations Manager indicates that a HeartBeatThreshold has been exceeded. This is the same event that occurs when the HeartBeat falls below the configured threshold of 24 ticks per minute. The event details do not indicate that the HeartBeat actually went to zero.  Workaround: None
CSCsh07060	InsufficientFreeMemory is reported incorrectly for Cisco Unified CallManager 5.0 clusters.	Events for InsufficientFreeMemory are being generated for Cisco Unified CallManager clusters 5.0 and higher. Operations Manager is not determining the correct InsufficientFreeMemory.  Workaround: None
CSCsh15251	Alerts and events are not always cleared from the Alerts and Events Display.	In the Alerts and Events Display, for a device that has multiple alerts or events, you can only clear alerts or events one time. If you try to clear additional alerts or events after already clearing an alert or event on the device, an error occurs and the event or alert does not get cleared.  Workaround:  Refresh the page (press F5 or relaunch the page) and clear the additional events or alerts.

Table 4 Known Problems in Operations Manager (continued)

Bug ID	Summary	Explanation
CSCsh19219	Operations Manager fails to import the HTTPS Security Certificate from the Cisco Unified CallManager cluster.	<p>When encryption is enable on the Cisco Unified CallManager cluster, Operations Manager fails to import the HTTPS Security Certificate from the Cisco Unified CallManager cluster.</p> <p>Workaround:</p> <p><b>Note</b> If after completing this procedure the Cisco Unified CallManagers are still partially monitored due to insufficient credentials, the Cisco Unified CallManagers must be deleted and manually readded.</p> <p>Do the following:</p> <ol style="list-style-type: none"> <li>1. Open the Cisco Unified CallManager Admin Page (<a href="http://&lt;ccmip&gt;/ccmadmin">http://&lt;ccmip&gt;/ccmadmin</a>) in Internet Explorer. A Security Alert Window appears.</li> <li>2. Click <b>View Certificate</b>. You would see a line similar to the following: <i>Issued To: &lt;Name&gt;</i>.</li> <li>3. Write down the name.</li> <li>4. Click the <b>Details</b> tab.</li> <li>5. Click the <b>Copy To File...</b> A wizard appears.</li> <li>6. Click <b>Next</b>.</li> <li>7. Select the <b>DER Encoded Binary X.509 (.CER)</b> radio button.</li> <li>8. Click <b>Next</b>.</li> <li>9. Provide a valid filename (for example: c:\mycert.cer).</li> <li>10. Click <b>Next</b>.</li> <li>11. Click <b>Finish</b>.</li> <li>12. Click <b>OK</b>. This completes the certificate download. Next you must import the certificate manually into the cacerts file.</li> <li>13. In a command prompt <i>cd</i> to the cscopx\lib\jre\lib\security directory.</li> <li>14. Run the following command: <pre>keytool -import -alias "File Name" -file c:\mycert.cer -keystore cacerts -storepass "changeit"</pre> <ul style="list-style-type: none"> <li>- "File Name" is the name obtained in Step 3.</li> <li>- C:\mycert.cer is the file name provided in Step 11.</li> </ul> </li> </ol>

Table 4 Known Problems in Operations Manager (continued)

Bug ID	Summary	Explanation
CSCsh19219 (continued)		<p><b>15.</b> Repeat Steps 1 through 13 for the required Cisco Unified CallManagers.</p> <p><b>16.</b> Rediscover all the Cisco Unified CallManagers that you performed this procedure for.</p> <p><b>Note</b> Even if the certificate is not valid, it is still possible to insert it into the cacerts. The Cisco Unified CallManager will go into the Monitored state, but the performance graphing will not work. In the case of manual import, you must manually validate the certificate.</p>
CSCsh94025	After upgrading from Operations Manager 1.1, only nine phones are displayed in the CiscoWorks Common Services Licensing page.	<p>When you upgrade from Operations Manager 1.1 using an upgrade license, only nine phones are displayed in the CiscoWorks Common Services Licensing page.</p> <p>Operations Manager 2.0 is actually licensed to support any existing Operations Manager 1.1 licensing limits plus nine additional phones. The system status report displays the correct supported phone limit.</p> <p>Workaround:</p> <p>To fix the CiscoWorks Common Services Licensing page:</p> <ol style="list-style-type: none"> <li><b>1.</b> On the Operations Manager system, go to CSCOpX\etc\licenses.</li> <li><b>2.</b> Delete the ipcom.lic file.</li> <li><b>3.</b> Delete any licenses that contain keyword <i>Evaluation</i>.</li> <li><b>4.</b> Restart the daemon manager.</li> </ol>

# Resolved Problems

Table 5 describes problems that were fixed in this release.

**Table 5** Problems Resolved in Operations Manager 2.0

Bug ID	Summary	Explanation
CSCsc30250	The Service Level View would display the following message:  A script in this movie is causing Macromedia Flash Player 8 to run slowly. If it continues to run, your computer may become unresponsive. Do you want to abort the script?	This message appeared when there was an update to the Service Level View and that update contained a large amount of content (100 KBs or more), or if the client system was under a load due to other processes using CPU memory. This no longer occurs.
CSCsd38707 CSCsd45913	During discovery, ping sweep did not consider domain names or syslocation.	During discovery, the domain name filter did not work correctly. The domain name filter has been changed, and now works correctly.
CSCsd65399	After upgrading, IP Communications Operations Manager 1.0 still appeared under Start > Programs.	Now after upgrade you will only see one option, Cisco Unified Operations Manager 2.0.
CSCsd78140	Wrong IP SLA results were displayed for the Phone Status Test Results report.	When you ran a Phone Status Test and scheduled it to run once, the resulting report displayed wrong information in the IP SLA column. Now the correct information is displayed.
CSCsd80619	The SRST cloud would disappear when changes in the cluster were made.	In the Service Level View, the SRST clouds (to indicate that the cluster has SRST connections) disappeared from the first-level map-display pane. This has been fixed.
CSCsd80651	During physical discovery, Cisco Unified CallManager's HTTP credentials were not getting picked up.	Cisco Unified CallManager 5.0 would go into the Partially Monitored state because its HTTP credentials were not getting picked up during physical discovery. Cisco Call Manager 5.0 HTTP credentials are now getting picked up correctly.
CSCsd80704	Sometimes automatic discovery did not stop.	Automatic discovery did not progress if any Cisco Unified CallManager 5.0 devices were used as seed devices. Also, the discovery process did not terminate on its own. This no longer occurs.
CSCsd80731	Discovery Credentials did not have a provision to enter the Windows Management Instrumentation (WMI) credentials.	WMI credentials can now be entered through the Add Devices page ( <b>Devices &gt; Device Management &gt; Add Devices</b> ).
CSCsd84401	Device discovery would sometimes take a very long time to complete.	The default SNMP timeout used to validate device credentials is 3 seconds with 2 retries. This caused discovery time to increase under the following conditions: <ul style="list-style-type: none"> <li>• There were many SNMP unreachable devices in the network.</li> <li>• Multiple credentials were supplied.</li> </ul> Now you can choose the SNMP timeout for different networks based on the network characteristics.

## Obtaining Documentation

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

### Cisco.com

You can access the most current Cisco documentation at this URL:

<http://www.cisco.com/techsupport>

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

[http://www.cisco.com/public/countries\\_languages.shtml](http://www.cisco.com/public/countries_languages.shtml)

### Product Documentation DVD

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

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

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

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

### Ordering Documentation

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

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

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

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

### Documentation Feedback

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

# Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

[http://www.cisco.com/en/US/products/products\\_security\\_vulnerability\\_policy.html](http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html)

From this site, you will find information about how to do the following:

- Report security vulnerabilities in Cisco products
- Obtain assistance with security incidents that involve Cisco products
- Register to receive security information from Cisco

A current list of security advisories, security notices, and security responses for Cisco products is available at this URL:

<http://www.cisco.com/go/psirt>

To see security advisories, security notices, and security responses as they are updated in real time, you can subscribe to the Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed. Information about how to subscribe to the PSIRT RSS feed is found at this URL:

[http://www.cisco.com/en/US/products/products\\_psirt\\_rss\\_feed.html](http://www.cisco.com/en/US/products/products_psirt_rss_feed.html)

## Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you have identified a vulnerability in a Cisco product, contact PSIRT:

- For emergencies only—[security-alert@cisco.com](mailto:security-alert@cisco.com)

An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- For nonemergencies—[psirt@cisco.com](mailto:psirt@cisco.com)

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532



**Tip**

We encourage you to use Pretty Good Privacy (PGP) or a compatible product (for example, GnuPG) to encrypt any sensitive information that you send to Cisco. PSIRT can work with information that has been encrypted with PGP versions 2.x through 9.x.

Never use a revoked encryption key or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

[http://www.cisco.com/en/US/products/products\\_security\\_vulnerability\\_policy.html](http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html)

The link on this page has the current PGP key ID in use.

If you do not have or use PGP, contact PSIRT to find other means of encrypting the data before sending any sensitive material.

## Product Alerts and Field Notices

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

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

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

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

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

## Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Support website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

## Cisco Support Website

The Cisco Support website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day at this URL:

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

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

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



### Note

Before you submit a request for service online or by phone, use the **Cisco Product Identification Tool** to locate your product serial number. You can access this tool from the Cisco Support website by clicking the **Get Tools & Resources** link, clicking the **All Tools (A-Z)** tab, and then choosing **Cisco Product Identification Tool** from the alphabetical list. This tool offers three search options: by product ID or model name; by tree view; or, for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.



### Tip

#### Displaying and Searching on Cisco.com

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

To find technical information, narrow your search to look in technical documentation, not the entire Cisco.com website. After using the Search box on the Cisco.com home page, click the

**Advanced Search** link next to the Search box on the resulting page and then click the **Technical Support & Documentation** radio button.

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

## Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

<http://www.cisco.com/techsupport/servicerequest>

For S1 or S2 service requests, or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411

Australia: 1 800 805 227

EMEA: +32 2 704 55 55

USA: 1 800 553 2447

For a complete list of Cisco TAC contacts, go to this URL:

<http://www.cisco.com/techsupport/contacts>

## Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

**Severity 1 (S1)**—An existing network is “down” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

**Severity 2 (S2)**—Operation of an existing network is severely degraded, or significant aspects of your business operations are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

**Severity 3 (S3)**—Operational performance of the network is impaired while most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

**Severity 4 (S4)**—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

# Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

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

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

- The *Cisco Product Quick Reference Guide* is a handy, compact reference tool that includes brief product overviews, key features, sample part numbers, and abbreviated technical specifications for many Cisco products that are sold through channel partners. It is updated twice a year and includes the latest Cisco channel product offerings. To order and find out more about the *Cisco Product Quick Reference Guide*, go to this URL:

<http://www.cisco.com/go/guide>

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

<http://www.cisco.com/go/marketplace/>

- Cisco Press publishes a wide range of general networking, training, and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

<http://www.ciscopress.com>

- *Internet Protocol Journal* is a quarterly journal published by Cisco for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the *Internet Protocol Journal* at this URL:

<http://www.cisco.com/ipj>

- Networking products offered by Cisco, as well as customer support services, can be obtained at this URL:

<http://www.cisco.com/en/US/products/index.html>

- Networking Professionals Connection is an interactive website where networking professionals share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

<http://www.cisco.com/discuss/networking>

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

<http://www.cisco.com/univercd/cc/td/doc/abtnicd/136957.htm>

- World-class networking training is available from Cisco. You can view current offerings at this URL:

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

This document is to be used in conjunction with the documents listed in the [“Product Documentation”](#) section.

CCVP, the Cisco logo, and Welcome to the Human Network 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, 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, Networkers, Networking Academy, Network Registrar, 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. (0711R)

Copyright © 2006 Cisco Systems, Inc. All rights reserved.

