



Release Notes for Campus Manager 4.0.6 on Solaris

These release notes are for use with the Campus Manager 4.0.6, part of the CiscoWorks family of products running on a Solaris platform. Supported Solaris versions are Solaris 8 (Solaris 2.8) and Solaris 9 (Solaris 2.9).

These release notes provide:

- [New Features, page 2](#)
- [Product Documentation, page 3](#)
- [Related Documentation, page 5](#)
- [Additional Information Online, page 5](#)
- [Support Information, page 6](#)
- [Known Problems, page 6](#)
- [Resolved Problems in Campus Manager 4.0.6, page 51](#)
- [Obtaining Documentation, page 57](#)
- [Documentation Feedback, page 58](#)
- [Obtaining Technical Assistance, page 60](#)
- [Obtaining Additional Publications and Information, page 62](#)
- [Open Source License Acknowledgements, page 63](#)



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

© 2006 Cisco Systems, Inc. All rights reserved.

New Features

This section describes the new features and enhancements available in Campus Manager 4.0.6. These include:

- [Enhanced Homepage](#)
- [Setup Center](#)
- [Enhanced Device Selector](#)

Enhanced Homepage

The Campus Manager Homepage provides information on the status of Device Discovery, Data Collection, and User Tracking Acquisition.

It also provides information on the physical and logical discrepancies as well as the details of the jobs that have been completed recently. You can access the frequently used features in the application from the homepage.

For more details, see *User Guide for Campus Manager 4.0.6*.

Setup Center

The Setup Center is a centralized location that displays all the System configuration related information.

The Setup Center also allows you to configure and check the necessary server settings from a single place.

For more details, see *User Guide for Common Services 3.0.5*.

Enhanced Device Selector

The new Device Selector allows you to perform search and advanced search for devices based on specified search criteria.

For more details, see *User Guide for Common Services 3.0.5*.

Product 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 1](#) describes the product documentation that is available.

Table 1 **Product Documentation**

Document Title	Available Formats
<i>Quick Start Guide for LAN Management Solution 2.6</i>	<ul style="list-style-type: none"> Printed document that was included with the product. On Cisco.com at: http://www.cisco.com/en/US/products/sw/cscowork/ps2425/prod_installation_guides_list.html
<i>Data Migration Guide for LMS 2.6</i>	<ul style="list-style-type: none"> Printed document that was included with the product. On Cisco.com at this URL: http://www.cisco.com/en/US/products/sw/cscowork/ps2425/prod_installation_guides_list.html
<i>User Guide for Campus Manager 4.0.6</i>	<ul style="list-style-type: none"> PDF on the product CD-ROM. On Cisco.com at this URL: http://cisco.com/en/US/products/sw/cscowork/ps563/products_user_guide_list.html Printed document available by order (part number DOC-7817186=).¹
<i>Supported Devices Table for Campus Manager 4.0.6</i>	On Cisco.com at this URL: http://cisco.com/en/US/products/sw/cscowork/ps563/products_device_support_tables_list.html

Table 1 **Product Documentation (continued)**

Document Title	Available Formats
<i>Installation and Setup Guide for Campus Manager 4.0.6 on Solaris</i>	<ul style="list-style-type: none"> • Printed document that was included with the product. • PDF on the product CD-ROM. • On Cisco.com at this URL: http://cisco.com/en/US/products/sw/cscowork/ps563/prod_installation_guides_list.html • Printed document available by order (part number DOC-7817187=).¹
<i>Context-sensitive Online help</i>	<ul style="list-style-type: none"> • Select an option from the navigation tree, then click Help. • Click the Help button in the dialog box.

1. See the “Obtaining Documentation” section on page 57.

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	Description and Available Formats
<i>User Guide for CiscoWorks Common Services 3.0.5</i>	<p>Describes CiscoWorks Common Services. It gives an overview of the applications that comprise Common Services 3.0.5 and provides conceptual information about network management.</p> <p>This also describes common tasks you can accomplish with Common Services. This document is available in the following formats:</p> <ul style="list-style-type: none"> • PDF on the product CD-ROM. • On Cisco.com at: http://www.cisco.com/en/US/products/sw/cscowork/ps3996/products_user_guide_list.html • Printed document available by order (part number DOC-7817182=).¹

1. See the “Obtaining Documentation” section on page 57.

Additional Information Online

The following product specific information is available online:

Service Packs (SP) contain updated files necessary for the latest device support and fixes to known problems that are not available in Campus Manager 4.0.6. If you are a registered user, you can download SP for Campus Manager from:

<http://www.cisco.com/cgi-bin/tablebuild.pl/cw2000-campus>

Support Information

Campus Manager 4.0.6 supports only US-English and Japanese versions of Solaris Operating Systems. It does not support any other language version. Set the default locale to US-English for US-English version and Japanese for Japanese version.

Known Problems

This section describes the known problems in this release:

- [General Notes and Known Problems, page 7](#)
- [General Known Problems, page 8](#)
- [Browser Known Problems, page 17](#)
- [Path Analysis Known Problems, page 18](#)
- [User Tracking Known Problems, page 24](#)
- [Topology Services Known Problems, page 29](#)
- [ANI Server Known Problems, page 43](#)
- [VLAN Port Assignment Known Problems, page 48](#)
- [Spanning Tree Protocol Known Problems, page 50](#)

**Note**

To obtain more information about known problems, access the Cisco Software Bug Toolkit at <http://www.cisco.com/cgi-bin/Support/Bugtool/home.pl> (You will be prompted to log into Cisco.com)

General Notes and Known Problems

Note the following:

- Your browser must be properly configured. If it is not properly configured, Campus Manager might not work correctly. For more details, see the [Installation and Setup Guide for Campus Manager 4.0.6](#).
- Campus Manager requires a DNS server to function properly. Many commands operate erratically or not at all, if there is no DNS server on the network.
- You cannot run Campus Manager from a browser invoked from an X-Window System since this is not supported. Install a browser on the client from which you wish to connect.
- You can upgrade your operating system (OS) either before or after you upgrade Campus Manager. However, if you upgrade the OS after upgrading Campus Manager, you will not receive any OS-related patch warnings or service pack-related warnings.
- Verify that the latest version of all required OS patches, service packs, and third-party device drivers are installed before proceeding with an OS upgrade.
- Do not export an entire topology map to Visio. Instead, select and export particular devices or a segment of the network and export it.

General Known Problems

The table below lists the known problems that are not specific to any module in Campus Manager.

Table 3 **General Known Problems**

Bug ID	Summary	Explanation
CSCsc49501	VeriSign security certificate displays expiry warning message.	<p>The VeriSign security certificate expires in June 2006. After that date, Campus Manager will display the Certificate expiry message whenever you launch applet based pages.</p> <p>However, all modules in Campus Manager will continue to work.</p> <p>Workaround: Ignore the message.</p>
CSCsb86066	Topology and Path Analysis do not launch when NAT or firewall are configured.	<p>If Campus Manager is installed in a server with NAT or firewall, Topology and Path Analysis do not launch. The following message appears:</p> <p><code>Cant connect to ANI Sever</code></p> <p>Workaround:</p> <p>If you enable the ports supported by Common Services, Topology and Path Analysis work in a firewall setup.</p> <p>For details on these ports, see Installation and Setup Guide for CiscoWorks Common Services 3.0.5 (Includes CiscoView) on Solaris.</p>

Table 3 **General Known Problems (continued)**

Bug ID	Summary	Explanation
CSCsc24255	Improper error message while configuring IVR.	<p>This problem occurs in the following scenario:</p> <p>If you do not give proper SNMP or Telnet credentials for a device in DCR, RME does not fetch Config details from that device.</p> <p>When you try to configure IVR for that device in Campus Manager, the following error message appears:</p> <pre>Failed in export/Import config.</pre> <p>Workaround:</p> <p>Enter proper SNMP and Telnet credentials for the device in DCR.</p>
CSCsb28190	Campus Manager applications do not start in ACS mode.	<p>Topology Services, Path Analysis, VLAN Port Assignment, and Discrepancy Report tasks do not start when you login to CiscoWorks in ACS mode.</p> <p>This problem occurs if you select Assign a Ciscoworks on a per Network Device Group Basis option in ACS server, but in the selected device group, you do not add the CiscoWorks server IP address.</p> <p>Workaround:</p> <p>When you assign a user to a specific group, ensure that you add the CiscoWorks Server IP address to that device group.</p>
CSCsa80727	Sometimes, launching of Campus Manager UIs fails.	<p>Campus Manager UIs do not open when the daemon manager is not restarted for a long period of time.</p> <p>Workaround:</p> <ol style="list-style-type: none"> 1. Stop the daemon manager. 2. Wait for 10 minutes and start the daemon manager. <p>Campus Manager UIs now open properly.</p>

Table 3 **General Known Problems (continued)**

Bug ID	Summary	Explanation
CSCsa44629	Campus Manager does not restore Topology Map settings after you take a back up and restore the data in another machine, that has Campus Manager 4.0.	<p>Campus Manager does not save the changes to layout style and background colors in Topology Map settings, that were backed up in another machine.</p> <p>This occurs when you:</p> <ol style="list-style-type: none"> 1. Modify Topology Map settings on a machine with Campus Manager 3.3. 2. Back up and restore the files on another machine, which has Campus Manager 4.0. 3. Run Data Collection. 4. Start Topology Services. <p>Workaround:</p> <ol style="list-style-type: none"> 1. Run <i>NMSROOT/campus/conf/upgrade/cm/topo/2cm31maplayout.pl</i> on the machine with Campus Manager 3.3 to generate the map files. 2. Copy the map files to the location on the target system, where you have restored the data: <i>NMSROOT/campus/etc/users/username/</i> 3. Upgrade Topology Map by selecting File > Upgrade View Layouts from Topology Services.

Table 3 **General Known Problems (continued)**

Bug ID	Summary	Explanation
CSCsa22708	Campus Manager does not manage existing devices when you upgrade from higher device limit to lower device limit.	<p>This problem occurs because Campus Manager performs a fresh discovery of the network to obtain the devices and does not import them from the earlier versions.</p> <p>Workaround: None.</p>
CSCin43133	Install may fail because of improper mount of CD-ROM.	<p>Using Volume Management, vold mounts the CD-ROM as /cdrom/cdrom0. cdrom0 is a link to volume label of the CD-ROM.</p> <p>For example cm4.0, where cm4.0 is the volume label.</p> <p>In normal circumstances, the link gets cleared after the CD-ROM is ejected. However, if the link is not cleared, when you mount another CD-ROM, it is mounted as /cdrom/cdrom0, This is then linked to cm4.0#1.</p> <p>This # character causes problems during installation.</p> <p>To verify if the directory name has a # character appended to its name, navigate to the /cdrom/cdrom0 directory, and check the present working directory using <code>pwd</code> command.</p> <p>Workaround:</p> <ol style="list-style-type: none"> 1. Eject the CD-ROM. 2. Stop the vold: <ul style="list-style-type: none"> <code>/etc/volmgt stop</code> 3. Start the vold: <ul style="list-style-type: none"> <code>/etc/volmgt start</code> 4. Delete the contents of /cdrom0 directory. <p>The CD-ROM should now mount normally.</p>

Table 3 **General Known Problems (continued)**

Bug ID	Summary	Explanation
CSCin23883	Jobs created in Path Analysis or User Tracking appear in the Job Management page even after uninstalling Campus Manager.	<p>If you have scheduled Path Analysis or User Tracking jobs and then uninstall Campus Manager, the jobs are not deleted from the CiscoWorks Job Management page.</p> <p>Workaround;</p> <p>Delete the Path Analysis or User Tracking jobs from the Job Management page.</p>
CSCdu51651	You cannot select the first template from the drop-down box, when you create SPVC/SPVP/Advanced parameters.	<p>Under ATM if you create SPVC/SPVP/Advanced parameters, you cannot select the first template from the drop-down box. This is because the traffic parameter fields are not populated.</p> <p>Workarounds:</p> <ol style="list-style-type: none"> 1. Go to Select/Edit and select the template. 2. Click OK. <p>Or</p> <ol style="list-style-type: none"> 1. Select the second template 2. Select the first template.
CSCdt55303	Starting Campus Manager application with the Print dialog box open in another Campus Manager application results in an error.	<p>This problem occurs if you:</p> <ol style="list-style-type: none"> 1. Select Print from active Campus Manager application. 2. Start another Campus Manager application, with the Print dialog box open. <p>The new application window does not respond to user input.</p> <p>Workaround:</p> <p>Close the Print dialog box and restart the application.</p>

Table 3 **General Known Problems (continued)**

Bug ID	Summary	Explanation
CSCdt42318	Cannot copy and paste IP addresses from Topology Services to Path Analysis when you use keyboard shortcuts.	<p>This problem occurs if you:</p> <ul style="list-style-type: none"> • Enter Ctrl-C to copy address after selecting an IP address in Topology Services, <p>Or</p> <ul style="list-style-type: none"> • Enter Ctrl-V with the cursor active in the From field in Path Analysis. • In both cases the following is pasted in instead of the IP address: <pre>java.lang.nullPointerException</pre> <p>Ctrl-X, Ctrl-C, and Ctrl-V (keyboard shortcuts for cut, copy, and paste commands) are not supported by summary tables in the Topology Services main window.</p> <p>It is also not supported by most of the tables that are displayed by Campus Manager applications.</p> <p>Also, in applications that allow you to copy support table cells by selecting Edit > Copy, a carriage return is added to the end of the last cell copied.</p> <p>Workaround:</p> <p>None.</p>

Table 3 *General Known Problems (continued)*

Bug ID	Summary	Explanation
CSCdt22462	Download of Java applets on Windows 2000 machines may take longer than expected if virus checker application is enabled.	<p>On some Windows systems, the initial download of large Java applets (or subsequent downloads of the same applets that are not cached locally) might take longer than expected (up to six minutes in some instances).</p> <p>After the applet has been loaded and cached locally, the problem no longer occurs.</p> <p>The delay is caused by client side filtering mechanisms such as virus scanning. Some virus scanners are configured to automatically scan content downloaded by browsers. Scanning consumes a lot of memory and results in disk paging on most systems.</p> <p>Hence, downloading is significantly slower than expected. The effect is less on systems with large amounts of RAM and virtual memory.</p> <p>Workaround:</p> <p>Disable the automatic scanning of all downloaded files, and instead enable the scanning of program files only (specified by file extension).</p> <p>Exact instructions vary depending on the virus scanner installed on your system.</p>

Table 3 **General Known Problems (continued)**

Bug ID	Summary	Explanation
CSCds88388	Cannot launch CiscoView on an IGX series device.	<p>This occurs if you:</p> <ol style="list-style-type: none"> 1. Launch Topology Services. 2. Open LAN Edge view. 3. Right-click on IGX series device and select CiscoView from the Context menu. A dialog box appears. 4. Enter appropriate community strings, and CiscoView attempts to launch. An error message appears. <p>Workaround: Launch CiscoView on IGX series devices via Cisco WAN Manager.</p>
CSCdm88520	Minimized windows are not visible when you select them from a Window menu.	<p>If a window is minimized, you cannot make it visible by selecting it from a Window menu.</p> <p>Workaround: Double-click the icon of the window on the taskbar.</p>

Table 3 **General Known Problems (continued)**

Bug ID	Summary	Explanation
CSCdm8320	<p>Campus Manager applications do not work when you access CiscoWorks using <code>http://localhost:1741</code></p>	<p>If you access CiscoWorks applications using <code>http://localhost:1741</code> from a browser on the same machine that CiscoWorks server is installed on, Campus Manager suite of applications will not work.</p> <p>Workaround:</p> <p>Use full DNS name or IP address of server, even when accessing it locally.</p>
CSCdm77812	<p>In Path Analysis, Tools > Path Trace displays an error, <code>null pointer exception</code> on Microsoft Internet Explorer 5.0 with the URL of a local host.</p>	<p>If your system has a non-blank <i>CLASSPATH</i> environment variable, your browser might behave unpredictably.</p> <p>Workaround:</p> <p>Reset the <i>CLASSPATH</i> variable non-globally:</p> <ul style="list-style-type: none"> • Solaris— Reset the <i>CLASSPATH</i> variable from the terminal window from where you launch the browser. • Windows—Reset the <i>CLASSPATH</i> variable in MS-DOS prompt window and launch the browser from the prompt.

Browser Known Problems

The table below lists the browser related known problems existing in Campus Manager.

Table 4 *Browser Known Problems*

Bug ID	Summary	Explanation
CSCin39472	Problems with Campus Manager applications after logout.	<p>When you logout from CiscoWorks, Campus Manager applications will continue to function. However, the following functions will not be available:</p> <ul style="list-style-type: none"> • Launching Help. • Tasks in Campus Manager that require user action between applications. For example, highlighting a device in Topology Services using Path Analysis. <p>Workaround:</p> <ol style="list-style-type: none"> 1. Close all Campus Manager applications. 2. Login into CiscoWorks. 3. Launch Campus Manager applications.
CSCdt11838	You are not prompted to install the Java plug-in when launching an application that utilizes the plug-in for the first time.	<p>If RealJukebox Plug-in for Navigator is already installed on a Windows client before the first launch of application utilizing Java Plug-in, you are not prompted to install Java Plug-in.</p> <p>Workaround:</p> <p>Uninstall RealJukebox Plug-in.</p> <p>Another option is to rename nprjplug.dll file in Navigator Plug-ins directory with a new extension. For example, nprjplug.dll.bak.</p> <p>After Java Plug-in is installed, you can reactivate RealJukebox Plug-in by changing the renamed file back to nprjplug.dll.</p>

Table 4 *Browser Known Problems (continued)*

Bug ID	Summary	Explanation
CSCdp43999	Maps and configuration dialogs display offset menus and list boxes in Netscape on a Solaris client.	Sometimes, when you launch a map or a configuration dialog box, menus or list boxes are not displayed below the menu. This offset occurs in Navigator on a Solaris client. Workaround: Move or resize window.

Path Analysis Known Problems

The table below lists the Path Analysis related known problems in Campus Manager.

Table 5 *Path Analysis Known Problems*

Bug ID	Summary	Explanation
CSCsa22380	Layer 2 Path Trace is not seen between IPv6 End host as source and its first hop IPv6 router.	In Path Analysis, when you run a Path Trace using IPv6 address of the End host and some other IPv6 destination (say router), Layer 3 Trace is observed. However, Layer 2 Trace (switches if any) between End host and First hop router is not shown in Path Trace. Workaround: None.
CSCin37960	VLAN-to-Subnet mapping information is not available for Phone Traces.	Path Analysis does not provide VLAN-to-Subnet mapping information, when you run Path Trace between two IP phones. Workaround: None.

Table 5 **Path Analysis Known Problems (continued)**

Bug ID	Summary	Explanation
CSCin37938	Interface Type displays <code>Unknown</code> for phones in Path Analysis Table.	This problem occurs when you run Path Traces between IP Phones or between a device and IP Phone. Workaround: None.
CSCin36082	Additional hop appears when you perform a trace using HSRP virtual IP address.	An additional hop appears if you perform a trace by providing an HSRP virtual IP address as the source or destination in the path trace. Workaround: None.
CSCin35773	Map displays self loop when routing loop occurs.	Occasionally, when the potential first hop learnt by Path Analysis is not discovered successfully by Campus Manager, the map displays a self loop. Workaround: None.
CSCin30899	Path Analysis does not work when LSR Traceroute is disabled.	If you disable source route on routers, Path Analysis sometimes might not display the route occasionally. Workaround: None.
CSCin28223	CORBA related error message is logged into the log file during path trace.	Occasionally, during path trace, a CORBA related error message is logged into the <code>ani.log</code> file. Workaround: Close the client browser window and relaunch Path Analysis.
CSCin00624	Path trace involving HSRP router results in an empty If Index entry in the Path Analysis table.	This problem occurs when you run a Path trace that includes the IP address of an HSRP router in the From field of a path trace. Workaround: None.

Table 5 *Path Analysis Known Problems (continued)*

Bug ID	Summary	Explanation
CSCdw15555	Voice trace does not get Cisco CallManager cluster information if Cisco CallManager HTTPD shuts down.	<p>Path Analysis Voice Trace needs to query Call Managers known to ANI to check what the cluster membership is.</p> <p>This is done through a HTTP query.</p> <p>As a security precaution, you might disable the Web Server on all cluster members except one. This is because Cisco CallManagers use IIS, and can be badly damaged by viruses such as Code Red and NIMDA.</p> <p>However, if cluster members have Web Server shut off, Path Analysis cannot obtain information on cluster membership and cannot retrieve CDRs.</p> <p>Workaround:</p> <p>Turn the Web Server on the Cisco CallManager back on.</p>

Table 5 **Path Analysis Known Problems (continued)**

Bug ID	Summary	Explanation
CSCdw03410	Path Voice Trace does not consider transcoding points.	<p>Current Campus Manager Path Analysis Voice Trace is valid only in the case where the two endpoints are IP Phones registered with the same Cisco CallManager cluster.</p> <p>For other cases (involving transcoding), Path Analysis Voice Trace does not get correct path information.</p> <p>Examples:</p> <ul style="list-style-type: none"> • Phone call from IP phone to POTS phone off H.323 gateway (e.g. 3640) • Phone call from one Cisco CallManager cluster to another. <p>In such a case the path would be:</p> <ol style="list-style-type: none"> a. From phone 1 to Cisco CallManager 1 b. From Cisco CallManager 1 to Cisco CallManager 2 through H.323 inter-cluster trunk c. From Cisco CallManager 2 to phone 2 <ul style="list-style-type: none"> • Phone call to gateway (PSTN, analog, etc.) • Phone call to other servers (voicemail, conference, etc.) <p>This is a very complex issue, and may require new instrumentation from telephony servers, etc.</p> <p>Workaround:</p> <p>None.</p>

Table 5 Path Analysis Known Problems (continued)

Bug ID	Summary	Explanation
CSCdt42600	To and From fields may not function properly after selecting Print in Path Analysis.	<p>This problem is caused by Java Virtual Machine bug. After you select Print in Path Analysis, the To and From fields may not accept mouse focus, or focus may appear in both fields, simultaneously.</p> <p>Workaround:</p> <p>Resize the Java console window. If the problem persists, close the Path Analysis window and open another window.</p>
CSCdt42404	Trace tab displays GMT as time zone, although server is set to local time zone.	<p>A number of Java bugs involve incorrect interpretation of time zones. Usually, the correct time zone appears if you set the local time zone to the appropriate three-letter abbreviation. For example, PST for Pacific Standard Time.</p> <p>This problem is observed on Solaris clients with TZ environment variable set to American/Tijuana.</p> <p>Workaround:</p> <p>If the TZ environment variable is instead set to PST8PDT, Java interprets local time zone correctly.</p>
CSCdt23712	Path Analysis displays the Elvis module of Cisco Catalyst 6000 devices as unknown.	<p>Since Path Analysis depends on ANI for its tracing capabilities, if a device-related discovery problem occurs in ANI, it results in an unsuccessful trace.</p> <p>Workaround:</p> <p>None.</p>
CSCdt04978	Highlighted path trace in Topology Services map may be difficult to view.	<p>It may be difficult to view highlighted path trace in Topology Services map, specially if you select the Fit to Window view.</p> <p>Workaround:</p> <p>Zoom into Topology Services Map view by selecting Select All Highlighted Objects > Zoom to Selected.</p>

Table 5 **Path Analysis Known Problems (continued)**

Bug ID	Summary	Explanation
CSCds79693	Voice trace query results always appear using local time zone.	<p>Local time zone always appears in voice trace query results, even if you select GMT time zone when specifying call start time.</p> <p>Workaround: None.</p>
CSCds77461	Call Detail Records (CDR) query results are sometimes displayed after pressing Cancel .	<p>Multiple threads are launched to query every Cisco CallManager for information specified in your CDR query.</p> <p>Since all query activities can take a second or two to cancel, query results sometimes continue to appear even after you press Cancel.</p> <p>Workaround: None.</p>
CSCds77438	Path Analysis Map tab does not refresh properly.	<p>This problem occurs when running both the client and the server on the same machine. It occurs after running a large number of Path traces on the client browser.</p> <p>Workaround: Close browser and relaunch Campus Manager.</p> <p>We recommend that you run the client and server on different machines.</p> <p>Although this does not prevent this problem, it reduces its frequency because you need to run a large number of traces before the problem occurs.</p>

User Tracking Known Problems

Information displayed in a row might not reflect the most current network state. This is because User Tracking discovery takes information from routers and switches.

Since these switches collect their information at different times, the information in a row reflects the state of the network or subnet at the time displayed in the Last Seen field.

The table below lists other User Tracking related known problems existing in Campus Manager.

Table 6 *User Tracking Known Problems*

Bug ID	Summary	Explanation
CSCsb17074	User Tracking does not discover hosts connected to devices with SNMPv3 credentials.	When you manage the devices Cisco Catalyst 3750 and Cisco Catalyst 4000 with SNMPv3 Credentials in Campus Manager, and if there are end hosts connected to these devices, the end hosts are not discovered and shown by User Tracking. Workaround: None.
CSCsc49155	User Tracking report generator displays error for some Custom queries.	If you run a custom query on User Tracking reports after remote migration, an error message appears. Campus Manager 3.x allows you to create some queries that are not supported by CM 4.0.x. Hence, an error is displayed when you run the queries. Workaround: Delete the old queries created in Campus Manager 3.x, and create new queries.

Table 6 **User Tracking Known Problems (continued)**

Bug ID	Summary	Explanation
CSCsc54306	User Tracking discovery spans more than the specified subnet.	<p>When you start subnet discovery of user nodes, devices in that subnet are marked for discovery.</p> <p>Since switches support multiple VLANs, discovery could span more than the subnet that you selected. User Tracking discovers additional end host nodes that are not in the selected subnet.</p> <p>Workaround:</p> <p>Query only the required VLAN option in the subnet discovery window.</p>
CSCsa30812	Job reports are not available after upgrading to Campus Manager 4.0.	<p>Reports for the jobs that are successfully completed in Campus Manager 3.3 are not available after upgrading to Campus Manager 4.0.</p> <p>This is because of the change in format of the Reports in Campus Manager 4.0.</p> <p>In earlier versions of Campus Manager, job results were stored in plain text, whereas in Campus Manager 4.0, the results are stored in serialized objects.</p> <p>Workaround:</p> <p>None.</p>
CSCsa27118	User Tracking Report displays Port State as Static for dot1x authenticated ports.	<p>User Tracking Report displays Port State as Static when an end host is connected to the switch port, which is configured for dot1x authentication.</p> <p>This is because the device populates vmVlanType as Static for dot1x authenticated ports.</p> <p>Workaround:</p> <p>None</p>

Table 6 *User Tracking Known Problems (continued)*

Bug ID	Summary	Explanation
CSCsa20659	Purge Job is created although you delete it from User Tracking Report Jobs.	<p>In User Tracking, Purge Job is created even if you try to delete it from the User Tracking Report Jobs and Common Services JRM pages.</p> <p>It gets deleted and then recreated immediately. There is no functionality loss because of this.</p> <p>Workaround: None.</p>
CSCsa14652	NAM and IDS Modules appear as end hosts in User Tracking.	<p>Cisco Catalyst 6000 devices running native IOS service modules appear as end hosts in User Tracking.</p> <p>This is caused by a problem on the device.</p> <p>Workaround: None.</p>
CSCin00363	End host does not appear if obsolete device IP address is assigned.	<p>If you connect a CDP device to the port and then add a new end host, this new end host is not learnt. This is because ANI is not aware of such a change.</p> <p>Workaround:</p> <ol style="list-style-type: none"> 1. Delete the specific device. 2. Perform Data Collection for the neighboring devices. 3. Perform User Tracking discovery for that device.
CSCin00181	Last Seen field gets updated for disconnected IP phones.	<p>The Last Seen field in Phone Tracking corresponds only to the Last Seen field on Cisco CallManager and not to the Last Seen field on Network.</p> <p>Workaround: None.</p>

Table 6 **User Tracking Known Problems (continued)**

Bug ID	Summary	Explanation
CSCec59408	Campus Manager does not query CISCO-PORT-SECURITY-MIB to verify port security configuration.	<p>In User Tracking, configuring port security for a port makes the CAM entry static. When port security is configured, Campus Manager does not query CISCO-PORT-SECURITY-MIB.</p> <p>This is because of a device specific MIB implementation problem.</p> <p>Workaround:</p> <p>Upgrade to Cisco IOS Release 12.2(18)EW1 or 12.2(20)EW.</p>
CSCdw04499	End hosts are not discovered with Catalyst 3550 running Cisco IOS Release 12.1(6)EA1 or earlier.	<p>End hosts are not discovered with Catalyst 3550 XL running Cisco IOS release 12.1(4)EA1 and Cisco IOS release 12.1(6)EA1.</p> <p>Workaround:</p> <p>This problem has been fixed in Cisco IOS release 12.1(6)EA1a. Upgrade to this version.</p>
CSCdw04486	End hosts not discovered with Catalyst 2950 running a software release earlier than Cisco IOS Release 12.0(5)WC2.	<p>End hosts not discovered with Catalyst 2950 running a software release earlier than Cisco IOS Release 12.0(5)WC2.</p> <p>Workaround:</p> <p>This problem has been fixed in Cisco IOS Release 12.0(5)WC2. Upgrade to this version.</p>
CSCdt25525	User Tracking Main Table sometimes displays CDP-enabled devices that are outside the ANI discovery boundary.	<p>During User Tracking discovery, User Tracking reads entries from the CAM table. These entries may include MAC addresses of devices that fall outside the ANI discovery boundary.</p> <p>Workaround:</p> <p>None.</p>

Table 6 *User Tracking Known Problems (continued)*

Bug ID	Summary	Explanation
CSCdt06183	User Tracking Main Table may not display all entries that are displayed in the phone table.	<p>User Tracking entries shown in the Main Table are discovered from network. However, User Tracking entries shown in the phone table are read from Cisco CallManager.</p> <p>If User Tracking cannot discover particular phones in network, entries for such phones in the User Tracking phone table will not have device and port information.</p> <p>Workaround:</p> <p>Ensure that the switch to which the IP Phones are connected, is managed by Campus Manager.</p>
CSCdr85384	Phone entries displayed by User Tracking differ from entries displayed by Cisco CallManager.	<p>User Tracking phone entries acquired through SNMP for each Cisco CallManager may be different from entries in Cisco CallManager.</p> <p>The Cisco CallManager database displays a historical record of all phones registered to Cisco CallManager.</p> <p>The SNMP agent retains only records of phones registered since the agent was started. This accounts for any differences.</p> <p>Workaround:</p> <p>None.</p>
CSCsd58215	DNS resolution for end user entries takes inordinate amount of time.	<p>DNS resolution, which occurs for end hosts discovered in user tracking, takes a lot of time to timeout if the DNS resolution for the corresponding IP address is not available in the DNS Server. Campus does not exit without waiting for a response from the DNS Server.</p> <p>Workaround:</p> <p>Set the property Ani.resolve=false in ANIServer.properties.</p>

Table 6 **User Tracking Known Problems (continued)**

Bug ID	Summary	Explanation
CSCse79161	User Tracking does not discover endhosts using SNMPv3 if the endhosts are connected to some of the Catalyst IOS devices such as Catalyst 2900, Catalyst 4000 and Catalyst 6000.	<p>This problem is caused by insufficient support for SNMPv3 - VLAN based context names in Catalyst IOS devices.</p> <p>Workaround:</p> <p>This problem has been fixed in recent Catalyst IOS image versions 12.2 and above for some devices. So ensure that the devices are running these versions of Catalyst IOS.</p> <p>Also, check whether the image supports SNMPv3 - VLAN based indexing for those device types.</p> <p>If the device does not have support for SNMPv3 - VLAN based context names in Catalyst IOS, remove SNMPv3 credentials from DCR and manage the device using SNMPv2.</p>

Topology Services Known Problems

The table below lists the Topology Services related known problems in Campus Manager.

Table 7 **Topology Services Known Problems**

Bug ID	Summary	Explanation
CSCdr28017	Topology Services does not support clusters of devices.	<p>Clusters of devices, that is, sets of devices grouped together under the same IP management address, are not supported in Topology Services</p> <p>Workaround:</p> <p>None.</p>

Table 7 **Topology Services Known Problems (continued)**

Bug ID	Summary	Explanation
CSCsa37595	Cannot delete large number of devices from Topology Services.	<p>An error message appears when you try to delete more than 100 devices from VTP Domain View in Topology Services.</p> <p>Workaround:</p> <p>We recommend that you reinitialize the database instead of deleting large number of devices through the User Interface.</p>
CSCsa27318	Topology Services displays an <code>OutOfMemoryError</code> , while working with 3000 devices.	<p>When you save the layouts and re-start topology map after using Topology Map tools such as zoom and drag, Java console displays an error:</p> <pre>java.lang.OutOfMemoryError.</pre> <p>Workaround:</p> <ol style="list-style-type: none"> 1. In the Java Plugin Control panel, go to the Advanced tab. 2. Add <code>-mx512m</code> to the existing Java Runtime Parameters.
CSCsa25203	Campus Manager does not generate Time Domain Reflectometry (TDR) Report for Cisco 3750 and Cisco 4000 series switches.	<p>Campus Manager displays a blank report when you run TDR test on Cisco 3750 and Cisco 4000 series switches.</p> <p>This is because MIBs are not available to support TDR feature on these devices.</p> <p>Workaround:</p> <p>None.</p>

Table 7 **Topology Services Known Problems (continued)**

Bug ID	Summary	Explanation
CSCsa22699	Inter-VLAN Routing configuration user interface (UI) does not differentiate primary and secondary IP addresses.	<p>Inter-VLAN Routing configuration user interface shows multiple entries for the same interface when you configure primary and secondary IP addresses for SVI or sub-interfaces.</p> <p>The UI does not clearly differentiate the primary and secondary IP addresses.</p> <p>Workaround:</p> <p>This problem does not occur in Cisco IOS Release 12.1(20)E3 or later.</p>
CSCsa18405	In PVLAN configuration, the secondary VLAN creation and association to Primary VLAN fail on Cisco Catalyst Operating System version 8.1.	<p>In devices with Cisco Catalyst Operating System version 8.1, Secondary VLAN creation and association with Primary VLAN fail if the device is running on version VTP version 3.</p> <p>Workaround:</p> <p>Either:</p> <ul style="list-style-type: none"> • Upgrade to Cisco Catalyst Operating System version 8.2. <p>Or</p> <ul style="list-style-type: none"> • Change VTP version to 2 and VTP mode to transparent.

Table 7 **Topology Services Known Problems (continued)**

Bug ID	Summary	Explanation
CSCsa12292	VLANs are not loaded for STP Offline Computation.	<p>This problem occurs in Topology Services when you:</p> <ol style="list-style-type: none"> 1. Launch STP Offline for PVST From the Topology Map. 2. Go to Reports > VLAN STP > Recommendations > STP Offline 3. Click Select Instance. <p>No VLANs are loaded.</p> <p>Devices that do not support CISCO-STP-EXTENSIONS-MIB will not support any STP related functionality.</p> <p>Workaround: None</p>
CSCsa11888	Channel or Trunk cannot be configured because of STP recalculation.	<p>Campus Manager sets the channel mode to Desirable Non-silent on the selected devices to be channelled. However, STP state changes occur when any mode change happens.</p> <p>So, if one of the two devices of the channel is an end-device and is only reachable through the to-be-channelled links, the device cannot be reached until the spanning-tree converges.</p> <p>Workaround: None.</p>

Table 7 **Topology Services Known Problems (continued)**

Bug ID	Summary	Explanation
CSCsa10216	Incorrect VTP version displayed in VTP reports.	<p>This problem occurs in Topology Services:</p> <p>The VTP Report displays the VTP version as 1 while the actual VTP version running on the device is VTP version 2.</p> <p>This problem occurs only with some of the Cisco Catalyst platforms such as C4506, C3750G, C2900.</p> <p>Workaround: None.</p>
CSCsa04026	Link line or connection between two devices gets warped, if one device is moved.	<p>This problem is seen in Topology services display map. When there is a long line between devices and one of the device is dragged to a different location on the map, a kink in the line develops with the link line connecting these two devices getting warped.</p> <p>The line appears jagged, instead of being straight.</p> <p>Workaround: To avoid this behavior, have devices closer to each other.</p>
CSCin68983	Cannot configure Trunk between Catalyst 2900XL and Catalyst 3500XL devices.	<p>Trunk configuration fails between Catalyst 2900XL and Catalyst 3548XL series switches.</p> <p>This is caused by lack of MIB support.</p> <p>Workaround: None.</p>
CSCin48159	Cannot launch IDSM from Service Modules launch point for IDSM2 card of Cisco Catalyst 6000 device.	<p>From Topology Services, you cannot start IDSM using the Service Module launch point. This is because of a defect in SNMP agent of the device.</p> <p>Workaround: None.</p>

Table 7 **Topology Services Known Problems (continued)**

Bug ID	Summary	Explanation
CSCin46641	Campus Manager does not calculate Trunk mode related discrepancies.	<p>Topology Services does not report the following discrepancies for Cisco Catalyst 2900 series, 3500 series, and 4000 IOS devices, in Trunk mode.</p> <ul style="list-style-type: none"> • AutoTrunk • NoTrunk • TrunkNegotiationEnabled <p>This is because of the lack of MIB support in the devices.</p> <p>Workaround: None.</p>
CSCin46405	Campus Manager does not report Spanning Tree discrepancies for some devices.	<p>Campus Manager does not report the following Spanning Tree discrepancies for some devices:</p> <ul style="list-style-type: none"> • BackboneFastDisabled • UplinkFastDisabled • BPDUGuarDisabled • STPEnabledOnAccessPorts <p>This is because of lack of MIB support in the devices.</p> <p>Workaround: None.</p>
CSCin46370	Trunk Negotiation Enabled Discrepancy Report does not show the Trunk mode details of the ports of some devices.	<p>TrunkNegotiationEnabled Discrepancy Report does not show Trunk mode details of the ports on Cisco Catalyst 2950, Cisco Catalyst 3550, and Cisco Catalyst 4000 IOS devices.</p> <p>This is because of a defect in SNMP agent of the device.</p> <p>Workaround: None.</p>

Table 7 **Topology Services Known Problems (continued)**

Bug ID	Summary	Explanation
CSCin45496	Campus Manager does not report UDLD discrepancy for Cisco Catalyst 2900 series switches.	<p>Discrepancy Reports does not display UDLD disabled discrepancy for Cisco Catalyst 2900 switches.</p> <p>This is because of a defect in SNMP agent of the device.</p> <p>Workaround: None.</p>
CSCin45070	Launch points do not work if http/https ports have other than the default value.	<p>In Topology Services, the launch points for Service Modules function only if the http/https port numbers are set to their default value.</p> <p>Launch Points must function for any valid http/https port number configured on the service modules.</p> <p>Workaround: None.</p>
CSCin43965	Spanning Tree reports more than one root for a switch cloud.	<p>Spanning Tree reports more than one root for a switch cloud containing Cisco 2900XL, Cisco 3500XL, Cisco 2950, or Cisco 3550 devices, if the selected VLAN is not assigned to any of the ports in these devices.</p> <p>This is because of a defect in SNMP agent of the devices.</p> <p>Workaround: None.</p>

Table 7 *Topology Services Known Problems (continued)*

Bug ID	Summary	Explanation
CSCin36988	Cannot calculate utilization of VCs in tunnel.	<p>This problem occurs in Topology Services when you:</p> <ol style="list-style-type: none"> 1. Setup a tunnel between two ATM devices and let the devices see each other as Interim Local Management Interface (ILMI) neighbors on their tunnel interfaces (subinterfaces) only. 2. Select Fabric view. 3. Select a device and its associated VP tunnel link. 4. Select Tools > Display VCs > Per device. 5. Click Get Info. <p>An error appears:</p> <p>Failed to compute utilization for some or all rows</p> <p>Workaround:</p> <p>None.</p>

Table 7 **Topology Services Known Problems (continued)**

Bug ID	Summary	Explanation
CSCin36950	Cannot view VCs in a tunnel from Topology Services main window.	<p>This problem occurs in Topology Services when you:</p> <ol style="list-style-type: none"> 1. Setup a tunnel between two ATM devices and let the devices see each other as Interim Local Management Interface (ILMI) neighbors on their tunnel interfaces (subinterfaces) only. 2. Select Fabric view. 3. Select a device and its associated VP tunnel link. 4. Select Tools > ATM Management > Display VCs > Per device. <p>The device or port chooser does not list subinterfaces.</p> <p>Workaround: None.</p>
CSCin29281	Device Attribute of Cisco Catalyst 6000 devices does not display the IP address.	<p>Device Attribute of Cisco Catalyst 6000 devices does not display the IP address of WS-X6624-FXS module.</p> <p>Instead, Device Attribute displays the IP address of Supervisor engine.</p> <p>This is because of a defect in the SNMP agent on the device. For more details, see CSCin33075.</p> <p>Workaround: None.</p>

Table 7 **Topology Services Known Problems (continued)**

Bug ID	Summary	Explanation
CSCin27895	Topology Services does not show VLANs as active, if the switch is in NULL folder under VTP Domain.	<p>Topology Services > VTP Domains > NULL folder shows VLANs in VTP server devices as inactive, if the VTP Domain name is not configured on the device.</p> <p>Topology Services displays the VLANs as inactive although the state of the VLAN on the switch is active.</p> <p>Workaround:</p> <p>Either:</p> <ul style="list-style-type: none"> • Configure VTP domain name in the device and rediscover. <p>Or</p> <ul style="list-style-type: none"> • Configure VTP domain mode of the device as transparent and rediscover.
CSCin22459	Topology Groups membership update does not work as expected.	<p>This problem occurs in Topology Services when you:</p> <ol style="list-style-type: none"> 1. Launch Custom Views for a group by selecting Campus Manager > Topology Services. 2. With the Custom Views window open, delete a device group using Topology Group Administration. <p>Custom View does not update automatically.</p> <p>Workaround:</p> <p>Re-open the Custom View window.</p>

Table 7 **Topology Services Known Problems (continued)**

Bug ID	Summary	Explanation
CSCin01977	Position of devices connected to Switch Cloud change after upgrade.	<p>Switch clouds and fabrics represent the collection of LAN switches and ATM switches, respectively.</p> <p>These logical entities are very specific to the currently discovered network. That is, if a new switch is discovered, you cannot uniquely identify a switch cloud or fabric across ANI databases.</p> <p>Workaround: None.</p>
CSCef67937	Campus Manager does not show port as trunking if the port is part of the Channel.	<p>This problem occurs when Cisco Catalyst 3750 has a 12.1 EA software version.</p> <p>When a port is part of channel and configured as trunk, Campus Manager does not display the port as trunking for Cisco Catalyst 3750 switches.</p> <p>Workaround: Upgrade Cisco Catalyst 3750 device to 12.2(18)SE1 or later.</p>
CSCeb68819	Topology Services does not display dual links.	<p>When two devices with dual links are aligned vertically on top of each other, the co-ordinates of the vertices of both links become the same.</p> <p>If the devices are not vertical, Topology Map displays dual links.</p> <p>Workaround: Relayout the maps using hierarchical or symmetrical layout, so that the devices do not align vertically.</p>

Table 7 **Topology Services Known Problems (continued)**

Bug ID	Summary	Explanation
CSCea39271	Topology Services displays the devices connected to a UB Token-Ring Hub in the Unconnected Devices View.	<p>CiscoWorks discovers Cisco Catalyst 4700 and Catalyst 4500 devices, but displays them under Unconnected Devices View, and not in Layer 2 View.</p> <p>Campus Manager cannot draw the map for the devices, as the routers are connected through a UB hub.</p> <p>Workaround: None.</p>
CSCdw49136	Campus Manager cannot establish connection between ATM ELAN and Ethernet VLAN when you remove LEC from Cisco Catalyst 2900XL devices.	<p>Initially, VLAN and ELAN are connected in Topology Services. When you remove LEC from Cisco Catalyst 2900XL devices, the connection between VLAN and ELAN is broken for 2900XL devices.</p> <p>This is because of a bug on 2900XL agent devices, where it does not support CISCO-LEC-EXT MIB.</p> <p>Workaround: None</p>
CSCdv41860	Fetching LANE component details displays an error <code>AniSQLException</code> .	<p>In Topology Services, if you create a LANE component in an ATM switch (LS1010) and launch its view, all the Profile and Diagnosis menu items related to this component display the following error:</p> <p><code>Internal error</code></p> <p>Workaround: None.</p>

Table 7 **Topology Services Known Problems (continued)**

Bug ID	Summary	Explanation
CSCdt50619	Two devices, connected by multiple links, appear to be connected by only one link.	<p>When two devices are connected by multiple links, and you rediscover either devices or links, all of the links are stacked on one another.</p> <p>This causes the devices to appear as if they are connected by only one link.</p> <p>Workaround:</p> <p>Perform a re-layout.</p>
CSCdt27824	Entire list of ports in a VTP domain appear when you select certain Transparent VTP domains from the VLAN Assignment dialog box.	<p>When similar VLAN definitions exist on a VTP server and transparent devices, VLAN is added under the parent folder and all transparent devices.</p> <p>Thus, VLAN ports appear under all transparent devices.</p> <p>Workaround:</p> <p>Run Find Ports query and enter only device name/address to view ports for a particular device.</p>
CSCdt18293	Visio drawing does not import cleanly into Microsoft Visio.	<p>If you export a Topology map as a Visio drawing, it is not imported cleanly into Microsoft Visio.</p> <p>Links are drawn out of place, and some incorrect links appear to be drawn between devices.</p> <p>Workaround:</p> <p>Clean the Visio drawing manually after import.</p>

Table 7 **Topology Services Known Problems (continued)**

Bug ID	Summary	Explanation
CSCdr11577	Virtual Circuit (VC) error chart is blank.	<p>A blank chart could mean either a continuous polling failure or a failure caused by other problems.</p> <p>For example, a blank VC error chart might be caused by a continuous polling failure (of VC error related data).</p> <p>It could also be because these statistics may not be supported on certain image versions of the ATM switch, being polled.</p> <p>Workaround: None.</p>
CSCdp88318	Link attributes are not updated after a change is made.	<p>If you change link attributes, ANI Server does not properly discover and display the change in reports.</p> <p>Workaround: To update link attributes, close and relaunch Topology Services.</p>

ANI Server Known Problems

The table below lists the ANI Server related known problems in Campus Manager.

Table 8 **ANI Server Known Problems**

Bug ID	Summary	Explanation
CSCsc43106	Device not discovered if SysUpTime is masked.	<p>If the SysUpTime is masked in v1 default view, Device Discovery does not discover the device.</p> <p>Workaround:</p> <p>Manually add the devices to DCR.</p> <p>Or</p> <p>Remove the mask in v1 default view.</p>
CSCsa20827	Subnet based groups are not deleted from Campus Manager Topology Groups although you delete them from DCR.	<p>In DCR, if you delete all devices or all devices in a subnet, the corresponding subnet based groups in Campus Manager are not deleted immediately.</p> <p>Workaround:</p> <p>If you want the subnet groups to be deleted earlier than 20 minutes, change the property from:</p> <pre>SubnetPollerConfigTime = 1200000</pre> <p>to a lesser value in the properties file:</p> <pre>NMSROOT/MDC/tomcat/webapps/campus/WEB-INF/classes/CM_Implementation_Details.properties.</pre>

Table 8 ANI Server Known Problems (continued)

Bug ID	Summary	Explanation
CSCsa19337	ANI goes into Unknown State when you delete all devices from DCR.	<p>This problem occurs in ANI when you:</p> <ol style="list-style-type: none"> 1. Discover some devices by specifying seed devices in Campus Manager. The DCR is updated with those devices. 2. Run data collection on those devices. 3. Invoke Topology Services. Devices appear in Views. <p>Deleting all devices from DCR will show ANI state and UT state as Unknown although you specify the seed devices in Device Discovery settings.</p> <p>Workaround: None.</p>
CSCin74855	Device not managed in Campus Manager if management IP is not in ACS.	<p>If a device has multiple IP addresses, Campus Manager automatically determines the management IP address of the device.</p> <p>If the management IP address is not ACS (that is, the device is added in ACS with a different address), this device is not managed in Campus Manager. Data collection is not done for this device.</p> <p>Workaround: IP address in ACS and management IP address in DCR should be the same.</p>
CSCin33112	Cannot delete devices on a remote system in SSL mode using the command line interface.	<p>The Delete Device command fails if you use it on a remote server in the SSL mode.</p> <p>Workaround: None.</p>

Table 8 **ANI Server Known Problems (continued)**

Bug ID	Summary	Explanation
CSCdz11668	ANI Discovery causes interfaces to go down.	<p>If you install Campus Manager on Solaris 2.8, the database interfaces go down shortly after beginning discovery.</p> <p>This causes the browsers to stop communicating with the CiscoWorks server. The interfaces while being displayed as <i>UP</i> in ifconfig, do not appear when you enter <code>netstat -rn</code>.</p> <p>This problem is caused by a Solaris bug; Sun Alert ID: 48601: Solaris 8 and Solaris 9 Network Interface may Stop Responding to TCP Traffic.</p> <p>This problem occurs in the following releases:</p> <ul style="list-style-type: none"> • Solaris 8 with patch 108528-16, or • Solaris 8 with patch 108528-17 but without patch 113652-01 <p>Workaround:</p> <ul style="list-style-type: none"> • Downgrade to kernel patch 108528-15 or earlier and restart the system. <p>Or</p> <ul style="list-style-type: none"> • Disable the ANIServer process allows CiscoWorks to continue functioning without Campus Manager applications. <p>The Sun bug mentioned above is resolved in Solaris 8 with patch 108528-17 and patch 113652-01 (for use with patch 108528-17 only).</p>

Table 8 ANI Server Known Problems (continued)

Bug ID	Summary	Explanation
CSCdw67129	Topology Services cannot resolve the hostname of newly discovered devices.	<p>If you add the DNS entry for the devices after initial discovery, Topology Services cannot resolve the hostname of the newly discovered devices.</p> <p>The subsequent discoveries do not resolve the IP address to a hostname until the ANIServer reloads.</p> <p>This occurs only in devices that do not have a DNS entry before discovery. Devices that have a DNS entry before ANI discovers them, do not have this problem.</p> <p>Workaround:</p> <p>Do either of the following:</p> <ul style="list-style-type: none"> • Restart CiscoWorks Server. ANI resolves the IP address to a hostname after restart. <p>Or</p> <ol style="list-style-type: none"> 1. Display the sysName in Topology Services (does not require a restart). 2. Select Topology Services > Layer 2 View > View > Display Labels > Show Sysname <p>Alternatively, you can do any of the following:</p> <ul style="list-style-type: none"> • Run Device Discovery again. • Stop and start the ANIServer. • If you require Campus Manager to ignore the cache and always look up the DNS server, add the following variable in the Java command line of the ANIServer: <p style="margin-left: 40px;"><code>Dnetworkaddress.cache.ttl=0</code></p>

Table 8 ANI Server Known Problems (continued)

Bug ID	Summary	Explanation
CSCdt20329	ATM switches, for which Remote Monitoring (RMON) is enabled, are not highlighted when Show Enabled Devices is selected.	<p>This problem occurs when you:</p> <ol style="list-style-type: none"> 1. Select Topology Services. 2. Highlight an ATM fabric under Managed Domains/ATM Domains 3. Select Display View. 4. Select devices, and click Tools > RMON Data Collection > Show Enabled Devices <p>Workaround: None.</p>
CSCdp76410	Campus Manager client cannot connect to server using proxies.	<p>Campus Manager does not support proxies.</p> <p>Workaround: None</p>
CSCdm58624	Campus Manager reports VTP Disconnected Domain discrepancy when VTP Domain is configured across a LANE Trunk.	<p>Campus Manager reports Disconnected Domain discrepancy even when VTP domain is configured across ATM cloud and the default ATM-VLAN is configured to carry VTP advertisements across the cloud.</p> <p>Workaround: Ignore the discrepancy.</p>
CSCdm48015	An ATM trunk port is shown as belonging to a VLAN, even if there is no corresponding LANE client associated with that VLAN.	<p>In VLAN-to-port association, all ATM ports on switches (except ATM switches) belonging to VLAN appear.</p> <p>Workaround: Ignore ATM ports in VLAN-to-port association.</p>
CSCdp00593	SNMP report displays wrong HwVersion and HwVersionMinor for Cisco LS1010 devices.	<p>This is because the image has reached EOE.</p> <p>Workaround: Enter show hardware in the command line interface of Cisco LS1010 devices.</p>

Table 8 ANI Server Known Problems (continued)

Bug ID	Summary	Explanation
CSCdm91634	In Campus Manager device report, number of ports in a device's ATM module are incorrectly displayed as zero.	<p>This problem occurs in Catalyst 5000 devices running Catalyst operating system software release 4.3(1a). It is caused by missing if Entry for device ATM module.</p> <p>ANI Server depends on ifEntry to determine number of ports in a particular module.</p> <p>Workaround:</p> <p>None.</p>

VLAN Port Assignment Known Problems

The table below lists the VLAN Port Assignment related known problems in Campus Manager.

Table 9 VLAN Port Assignment Known Problems

Bug ID	Summary	Explanation
CSCsc24275	VLAN interfaces created through IVR are not shown in the existing interface list for that device.	<p>If the corresponding VLAN on which the new VLAN interface is being created does not already exist in the device, the interface is not shown in the list.</p> <p>Workaround:</p> <p>Create a VLAN in the device before you create VLAN interfaces.</p> <p>Or</p> <p>Create interfaces for existing VLANs in the device.</p>

Table 9 **VLAN Port Assignment Known Problems (continued)**

Bug ID	Summary	Explanation
CSCin67286	Topology Services cannot populate PVLAN to port association for some ports in Cisco Catalyst 4000 IOS devices.	<p>If the ports are inactive Topology services does not show PVLAN to port association in Cisco Catalyst 4000 IOS devices.</p> <p>Workaround:</p> <p>Upgrade the IOS image to 12.2(25)EWA or later.</p>
CSCdw09818	Port Attribute in VLAN Port Assignment displays incorrect information.	<p>This problem is observed only on inactive ports. The MIB values returned by the devices latch on to the previous speed and duplex properties.</p> <p>This is because of a defect in SNMP agent of the device.</p> <p>Workaround:</p> <p>None.</p>

Spanning Tree Protocol Known Problems

The table below lists the Spanning Tree Protocol related known problems in Campus Manager.

Table 10 *Spanning Tree Protocol Known Problems*

Bug ID	Summary	Explanation
CSCsa12292	VLANs not loaded for STP Offline Computation.	<p>This problem occurs in STP when you:</p> <ol style="list-style-type: none"> 1. Launch STP Offline for PVST From the Topology Map. 2. Go to Reports >VLAN STP Recommendations > STP Offline 3. Click Select Instance <p>No VLANs are loaded.</p> <p>Devices that do not support CISCO-STP-EXTENSIONS-MIB will not support any STP related functionality.</p> <p>Workaround: None.</p>
CSCsa09287	Cannot map VLANs to instance if the device runs MISTP.	<p>In STP, if the device is running STP type as MIST, configuring the instance to VLAN mapping from STPConfigurationReport > InstanceTab is not applied on the device.</p> <p>This is caused by an SNMP Agent problem.</p> <p>Workaround: None.</p>

Table 10 *Spanning Tree Protocol Known Problems (continued)*

Bug ID	Summary	Explanation
CSCin67279	Community suffix support is not available for MST on Cisco IOS switches.	In STP, community suffix support is not available for MST and MISTP on Cisco IOS switches. Workaround: None.
CSCed72194	MST device report does not report CIST root correctly.	In STP, MST device report may not report the CIST root properly. This is because the dot1dStpDesignatedRootCost object corresponds to external root path cost. Hence the value of the object is 0 for all switches in the MST region that contains the CIST root. Workaround: None.

Resolved Problems in Campus Manager 4.0.6

The following table lists the problems that have been fixed in Campus Manager 4.0.6.

Table 11 *Resolved Problems in Campus Manager 4.0.6*

Bug ID	Summary	Additional Information
CSCeg75854	Campus Manager did not support WS-X6582-2PA flexwan card.	This problem has been resolved.
CSCsa52136	Wake On LAN was not supported in User Tracking.	This problem has been resolved.
CSCsa83447	You could not delete multiple community strings at the same time. This was because you could select only one radio button.	This problem has been resolved. The Radio buttons have been replaced by check boxes. You can select multiple community strings by selecting the check boxes

Table 11 **Resolved Problems in Campus Manager 4.0.6 (continued)**

Bug ID	Summary	Additional Information
CSCsb16407	Name of the new groups created based on SystemContact and SystemLocation was case sensitive.	This problem has been resolved. Now you can specify group names which are not case sensitive.
CSCsb52555	You could not schedule quarterly jobs for User Tracking Custom Reports. Also, there was no e-mail notification.	This problem has been resolved. You can now schedule quarterly jobs for User Tracking Custom Reports. E-mail notification containing the URL of the report is also supported.
CSCsc17087	You could not perform selective Data Collection for new devices alone.	This problem has been resolved. You can now perform selective Data Collection either for All Devices or for New Devices only.
CSCsc24107	Last Seen Column filter in User Tracking Custom Reports was not working properly.	This problem has been resolved. For more details, see the section Operator Values for Last Seen Column in Campus Manager Online Help.
CSCsc51917	Although you could create group names with special characters, you could not select or edit them.	This problem has been resolved. You cannot create group names with special characters in their names.
CSCsc61310	Path Analysis could not handle switches with Multi Layer Switch Feature Card (MSFC).	This problem has been resolved.
CSCsd65038	User Tracking reports leaked database connections.	This problem has been resolved. This happened when database connection was not closed properly because of the errors while running User Tracking reports.
CSCsd73842	Campus Manager 4.0 did not support Auxiliary VLANs on Cisco Catalyst 4000 Series.	This problem has been resolved. Campus Manager now supports Auxiliary VLANs on Cisco Catalyst 4000 Series.

Table 11 **Resolved Problems in Campus Manager 4.0.6 (continued)**

Bug ID	Summary	Additional Information
CSCsd79426	When you started Campus Manager applications, the status of ANI server was always reported to be initializing.	This problem has been resolved. This happens if the LogMsg.logfile property in <i>NMSROOT/campus/etc/cwsi/ANIServer.properties</i> pointed to a directory rather than a file.
CSCsd82813	utdebug did not work with certain fixed-configuration IOS switches.	This problem has been resolved.
CSCsd89046	Campus Manager could not list the unreachable devices.	This problem has been resolved.
CSCsd99630	Campus Manager Data Collection did not complete successfully.	This problem has been resolved.
CSCsd99642	Campus Manager daemons ran out of memory while loading the ANI database.	This problem has been resolved.
CSCse03007	You could not export a Visio XML file from the Topology Map LAN Edge View.	This problem has been resolved. This problem occurred when you selected a cloud object, such as witch clouds and ATM fabric clouds for export.
CSCse09907	You had to redo Data Collection if ANIServer was restarted.	This problem has been resolved.
CSCse11889	The ani.log file did not get backed up as ani.log_backup when ANI process was restarted.	This problem has been resolved.
CSCse13232	You wanted to by-pass <code>InetAddress.getHostName()</code> and directly go for JNDI look up.	This problem has been resolved.
CSCse14478	ANI processes stopped because of some unwanted blocking calls that locked the VTP Domain and VLAN objects.	This problem has been resolved.
CSCse17014	User Tracking added duplicate entries during major acquisition.	This problem has been resolved.

Table 11 **Resolved Problems in Campus Manager 4.0.6 (continued)**

Bug ID	Summary	Additional Information
CSCse22299	Data Collection and User Tracking Acquisition ignored large SNMP timeout values.	This problem has been resolved.
CSCse29553	In the Online Help, Duplicate SysName was listed in Physical Discrepancies instead of Logical Discrepancies.	This problem has been resolved.
CSCse32030	User Tracking did not function when you migrated from SNMPv3 to SNMPv2.	This problem has been resolved.
CSCse34643	Campus Manager did not support auxiliary VLANs on Cisco Catalyst 3550 Series devices. This resulted in getting incomplete information on IP Phones connected to Cisco Catalyst 3550 Series devices with auxiliary VLANs.	This problem has been resolved.
CSCse41622	When you connected IP Phones to trunk ports, the User Tracking Phone Report showed duplicate entries for one extension.	This problem has been resolved.
CSCse43345	When you deleted a device from DCR, the event was not sent to Campus Manager. So the device existed in ANI, but not in DCR. As a result, ANI hung and User Tracking failed.	This problem has been resolved.

Table 11 **Resolved Problems in Campus Manager 4.0.6 (continued)**

Bug ID	Summary	Additional Information
CSCse47733	<p>Cisco Catalyst 6000 Series devices were displayed in Unconnected View of Campus Manager 4.0.4 Topology Services.</p> <p>This happened although CDP-MIB responded properly to SNMP queries and had corresponding entries on neighboring devices.</p>	<p>This problem has been resolved.</p>
CSCse48823	<p>Online Help did not contain information on Visio 2003 support in Campus Manager.</p>	<p>Online Help and User Guide have been updated.</p> <p>This problem has been resolved.</p>
CSCse68260	<p>User Tracking queried for suspended or otherwise non-operational VLANs. This resulted in triggering Authentication failure traps.</p>	<p>This problem occurred when:</p> <ul style="list-style-type: none"> • Any non-operational VLANs on a specified switch contained operationally up ports. • Any non-operational VLANs on a specified switch contained any port, and the UTGetVlansOnDownPorts property was not set to '0' in the ANIServer.properties file. <p>This problem has been resolved.</p>
CSCse76357	<p>You could not launch SSH from the Topology Map for MSFCs.</p>	<p>This problem has been resolved.</p>
CSCse92940	<p>Campus did not manage logical interfaces on Catalyst 6000/76xx routers.</p>	<p>Campus manages only the physical interfaces existing in the device hardware which will be populated by the entity mib.</p> <p>So the links were not displayed in the topology map if those devices were connected to neighbor devices through these logical interfaces.</p> <p>This problem has been resolved.</p>

Table 11 **Resolved Problems in Campus Manager 4.0.6 (continued)**

Bug ID	Summary	Additional Information
CSCse91697	Data Collection and User Tracking ran for a long time.	This happened when SNMPv3 was being used, and when there were corrupt cache entries in either <i>NMSROOT/campus/etc/cwsi/Snmpv3EngineParam.txt</i> or <i>UTSnmpv3EngineParam.txt</i> . This problem has been resolved.
CSCsd32162	Sorted order was not retained in User Tracking exported data.	This problem has been resolved.
CSCse95701	Layer 2 view of Topology Services showed a shared media link, when a switch was connected to a router interface of type l2vlan.	This problem has been resolved.
CSCse98258	ANIServer crashed with Java HotSpot Virtual Machine error.	This problem has been resolved.
CSCsf01061	Data collection generated Authentication failure traps while querying inactive VLANs.	This problem has been resolved.
CSCsf09634	Campus Manager applications such as Topology Services and Path Analysis did not start if the HTTP port for CiscoWorks was set to 80.	This problem has been resolved.
CSCsf00966	User Tracking reported duplicate entries for end hosts connected to uplink ports on Catalyst 4000 IOS switches.	This problem has been resolved.

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

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

<http://www.cisco.com/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

Product Documentation DVD

Cisco documentation and additional literature are available in the Product Documentation DVD package, which may have shipped with your product. The Product Documentation DVD is updated regularly and may be more current than printed documentation.

The Product Documentation DVD is a comprehensive library of technical product documentation on portable media. The DVD enables you to access multiple versions of hardware and software installation, configuration, and command guides for Cisco products and to view technical documentation in HTML. With the DVD, you have access to the same documentation that is found on the Cisco website without being connected to the Internet. Certain products also have .pdf versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD=) from Cisco Marketplace at this URL:

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

Ordering Documentation

Beginning June 30, 2005, registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

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

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at tech-doc-store-mkpl@external.cisco.com or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can send comments about Cisco 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.

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

From this site, you can perform these tasks:

- 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 and notices for Cisco products is available at this URL:

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

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:

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 might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies—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.

- Nonemergencies—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 to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.x through 8.x.

Never use a revoked 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

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

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation 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 Technical Support & Documentation Website

The Cisco Technical Support & Documentation 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/techsupport>

Access to all tools on the Cisco Technical Support & Documentation 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**

Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI 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.

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)—Your network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

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

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

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

Obtaining Additional Publications and Information

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

- Cisco Marketplace provides a variety of Cisco books, reference guides, 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>

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

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

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions.

- *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>

- Networking products offered by Cisco Systems, 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 for networking professionals to 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>

- 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>

Open Source License Acknowledgements

The following acknowledgements pertain to this software license.

OpenSSL/Open SSL Project

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>).

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

License Issues

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License:

© 1998-1999 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment: “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org/>)”
4. The names “OpenSSL Toolkit” and “OpenSSL Project” must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called “OpenSSL” nor may “OpenSSL” appear in their names without prior written permission of the OpenSSL Project.

6. Redistributions of any form whatsoever must retain the following acknowledgment:

“This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)”

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT “AS IS” AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License:

© 1995-1998 Eric Young (eay@cryptsoft.com). All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

“This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)”.

The word ‘cryptographic’ can be left out if the routines from the library being used are not cryptography-related.

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: “This product includes software written by Tim Hudson (tjh@cryptsoft.com)”.

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License].

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)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2006 Cisco Systems, Inc. All rights reserved.

