CHAPTER 5

Tracking Packet Flow Using Path Analysis

Path Analysis is an operations and diagnostic application that traces the connectivity between two specified points on your network, including the physical and logical paths taken by packets flowing between those points.

Use Path Analysis to:

- Analyze paths between two Layer 2 or Layer 3 devices using device hostnames or IP addresses and show results visually in a network map, table, or textual “trace” display
- Highlight Layer 2 and Layer 3 paths on the Topology Services network view
- Display Layer 3 paths between two specified devices in the managed domain and, where possible, display the Layer 2 path between two specified end-user hosts known to User Tracking
- Display information about interface properties such as Maximum Transmission Unit (MTU) size, speed, MAC address, and media type
- Trace the paths that Voice over IP (VoIP) traffic takes on data networks
- Display information about device properties such as node name, device type, chassis type, up-time, and one alias
- Invoke CiscoView, Telnet, and Cisco CallManager from devices displayed on the Path Analysis map
- Invoke Visual Switch Manager from Cisco 1900, 2900XL, and 3500XL devices displayed on the Path Analysis map

The following topics provide you with information about:

- Starting and Navigating in Path Analysis, page 5-2
- Using Path Analysis, page 5-5
- Path Analysis Concepts, page 5-7
- Troubleshooting Path Analysis, page 5-17

Starting and Navigating in Path Analysis

From the CiscoWorks2000 desktop, select **Campus Manager >Path Analysis**. The Path Analysis main window appears (see Figure 5-1). Refer to Table 5-1 for a description of the elements of the Path Analysis main window.

Figure 5-1 Path Analysis Main Window

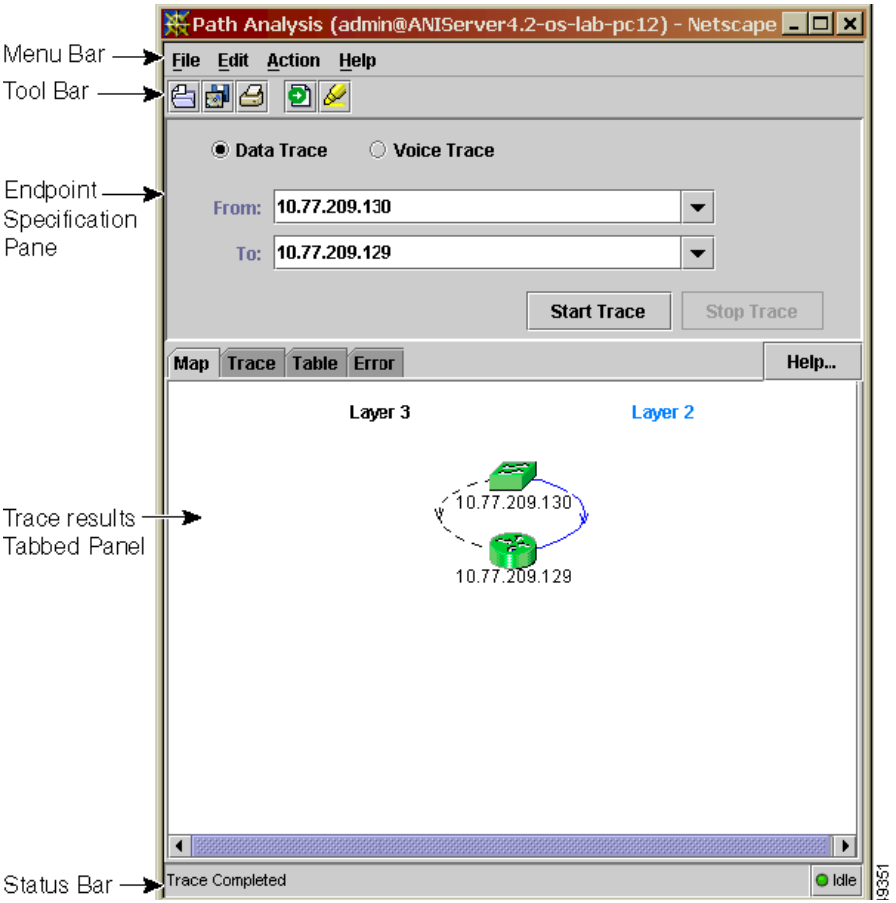


Table 5-1 Path Analysis Main Window Elements

Item	Description	Usage Notes
Menu Bar	Contains Path Analysis Commands	None.
Tool Bar	Provides quick access to frequently used menu options	None.
Endpoint Specification Panel	Contains fields for specifying the start and end-points for a trace	You can specify Cisco devices, end-user stations, or IP phones.
Trace Results Tabbed Panel	Displays the results of the trace in Map, Trace, and Table format	Click on the desired tab to display the results in each format.
Status Bar	Displays informational, diagnostic, and warning messages.	For a complete list of status bar messages, see Table 5-3 on page 5-19. Click the color-coded Discovery Status button to view the Discovery Information window.

Using Path Analysis

Table 5-2 lists the main tasks that you can perform using Path Analysis. All actions begin from the Path Analysis main window, unless otherwise noted. For more information about each task, refer to the Path Analysis online help.

Table 5-2 Main Path Analysis Tasks

Task	Purpose	Action
Discover the network for Path Analysis.	To start ANI discovery and user and node acquisition, to provide the information Path Analysis uses to perform Layer 3 and Layer 2 traces.	Select **Action > Discover All**.
Modify the subnet mapping table.	To ensure that the VLAN and ELAN mapping information is correct. Review previously supplied information and update it if necessary.	1. Select **Edit > Subnet Mapping...**. 2. Click **Discover**. 3. Modify desired information. 4. Click **Apply**.
Perform a data trace between two end-points.	Determines the path packets take from one device to another, including Layer 2 and Layer 3 devices.	1. Select **Data Trace**. 2. Enter DNS names or IP addresses in the **From** and **To** fields. 3. Select **Action > Start Trace**.
Perform a VoIP trace on a completed call.	Traces the paths that VoIP traffic follows on your data network. You can do a voice trace only on a call with a Call Detail Record (CDR).	1. Select **Voice Trace**. 2. Click **Find Call...**. 3. Enter one or more search criteria. 4. Click **Get Records**. 5. Select the desired CDR. 6. Click **Start Trace**.

Table 5-2 Main Path Analysis Tasks (continued)

Task	Purpose	Action
Reverse a data trace.	Checks the reverse direction connectivity between two end-points.	1. Select **Action > Reverse Trace Direction**. The IP addresses in the From and To fields are automatically reversed. 2. Select **Action > Start Trace**.
View the trace in a graphical map format.	Displays a graphical representation of the path trace.	1. Perform a path trace. 2. Click the **Map** tab.
View the trace in a command line output format.	Displays the trace information as it would be shown on the device command line interface.	1. Perform a path trace. 2. Click the **Trace** tab.
View the trace in a table format.	Displays the trace information in tabular columns.	1. Perform a path trace. 2. Click the **Table** tab.
Save a trace.	Saves a trace, allowing you to view it later.	Select **File > Save Trace As...**.
View the path in Topology Services.	Displays the path in the Topology Services network view.	Select **Action > Highlight Devices in Network View.**
Start CiscoView from Path Analysis.	Starts CiscoView, a GUI-based device management application, to obtain dynamic status, statistics, and comprehensive configuration for Cisco internetworking devices.	Right-click a device icon in Map view and select **CiscoView**.

Path Analysis Concepts

You should understand these concepts when using Path Analysis:

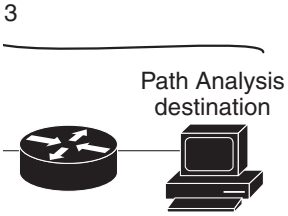
- Path Analysis Requirements, page 5-7
- Valid Data Path Trace End-Points, page 5-10
- Valid VoIP Trace End-Points, page 5-11
- Call Detail Records and VoIP Tracing, page 5-12
- Layer 3 Paths, page 5-13
- Layer 2 Paths, page 5-13
- Shortcuts, page 5-14
- Subnet to VLAN/ELAN Mapping, page 5-14
- VLAN/ELAN Subnet Mapping Table and Layer 2 Tracing, page 5-16
- VLAN/ELAN Subnet Mapping Table and Layer 3 Tracing, page 5-17

Path Analysis Requirements

There are four main components in Path Analysis as shown in Figure 5-2:

- CiscoWorks2000 Client running Path Analysis
- CiscoWorks2000 Server
- Source of the path
- Destination of the path

Figure 5-2 Path Analysis Components



Path Analysis investigates and reports on Layer 3 and Layer 2 paths between a source and destination (Leg 3 in Figure 5-2). For Path Analysis to be able to perform this analysis on Leg 3, Legs 1 and 2 must be functional.

For the path between the client and server (Leg 1) to be functional, there must be problem-free communication between server and client. (For example, problematic communication results when a firewall exists between the client and server.)

For the path between the server and the source (Leg 2) to be functional, the following requirements must be met:

- IP connectivity
- SNMP communication
- No routers configured to block source-routed IP packets. Make sure the router configuration does not contain the following statement:

```
no ip source-route
```

Note By default, Cisco routers are configured to **not** block source-routed IP packets.

For Layer 2 analysis to take place between the source and destination (Leg 3), the following conditions must be met:

- Both ends of a Layer 3 hop are managed Cisco devices known to the Topology Services application (device is a green icon on the topology view) or end-user stations known to the User Tracking application. A question mark icon (unknown or inaccessible device) on either end of the Layer 3 hop indicates that the previously mentioned prerequisites are not met.
- All Cisco devices are running CDP.
- Path Analysis supports Layer 2 tracing on Ethernet, Fast Ethernet, Gigabit Ethernet, and LAN Emulation networks. LAN Emulation support includes tracing on the path inside an ATM cloud. For this release, Path Analysis Layer 2 tracing does not support FDDI, Token Ring, and WAN interfaces or router bridge groups.
- Subnet to VLAN/ELAN mappings (automatically discovered or manually provided through the editor) are correct and complete. Refer to the “Subnet to VLAN/ELAN Mapping” section on page 5-14.
- Connectivity information for the subnet in question is known to Topology Services.
- The VLAN/ELAN information is known to Topology Services.
- The Layer 2 path does not involve router bridging (bridge groups).
- All Layer 2 devices are SNMP accessible.

- Install and configure DNS.
- For Voice over IP (VoIP) tracing, CDR logging must be enabled on all Media Convergence Servers.

Note As a general rule, do not expect to see a Layer 2 path for every Layer 3 hop.

Valid Data Path Trace End-Points

You can select source and destination end-points for a data path trace by doing one of the following:

- Entering a Domain Name System (DNS) name or IP address
- Copying and pasting node names or IP addresses selected from Topology Services
- Copying and pasting node names or IP addresses highlighted in User Tracking

A trace source end-point must be inside the managed organization for accurate Path Analysis results, and can be either:

- A device known to the ANI Server or User Tracking, such as a LAN switch, an ATM switch, a router, or a fast hub that supports Cisco Discovery Protocol (CDP)
- An end-user host discovered by User Tracking

For Layer 2 tracing, trace source end-points must be Cisco devices. Layer 3 tracing supports any trace source end-point inside the managed organization.

A trace source end-point must be reachable from the CiscoWorks2000 server. If it is not reachable, an alert message appears. See Table 5-3 on page 5-19 for definitions of the status bar messages and alert box messages.

A trace destination end-point can be any IP address or DNS name on the Internet, including addresses outside the managed organization. But firewalls and devices along the path that do not support source-routed IP packets can prevent Path Analysis from completing a trace to its intended destination. Layer 2 tracing, where possible, occurs only inside the managed organization.

Note Layer 3 tracing does not support PCs or workstations with more than one network adapter. In this release, Path Analysis does not support devices using the AppleTalk or IPX protocols.

It is possible to specify a source end-point outside of the managed domain, but trace results from this usage might not be completely accurate. Therefore, Cisco Systems recommends against this usage.

Valid VoIP Trace End-Points

You can determine the data paths and troubleshoot the signaling paths that Voice over IP (VoIP) traffic uses on your network.

Additionally, you can trace the flow of packets for three types of VoIP telephone calls on your data network.

Type of Call	Description	Trace Methods
Completed call	Telephone call that has occurred and completed. Call Detail Records (CDRs) exist only for completed calls.	Trace as voice data, using the telephone number of the called (destination end-point) telephone.
Call in progress	Telephone call that has begun, but has not concluded.	• Obtain IP addresses in User Tracking for the voice-enabled devices and gateways in your network. • Trace the packets as standard data (select **Data Trace**), using end-point IP addresses. Do not use telephone numbers. (No CDRs exist for a call in progress.)

Type of Call	Description	Trace Methods
Potential call	Telephone call that has not occurred, but might occur in the future.	• Obtain IP addresses in User Tracking for the voice-enabled devices and gateways in your network. • Trace the packets as standard data (select **Data Trace**), using end-point IP addresses. Do not use telephone numbers. (No CDRs exist for a call in progress.)

Call Detail Records and VoIP Tracing

Call Detail Records (CDRs) exist only for completed calls (calls that have occurred and have been successfully completed). CDRs contain the called and calling telephone numbers, which are required to perform a voice trace.

To find the required CDRs, you can filter your search criteria by any combination on the following three filters available in the Voice Trace Query window:

- Called Time—the approximate time at which the call began and time zone. When you enable Called Time filtering, you include among your CDR search the time at which you have specified that the call occurred.
- Called Number—all or part of the telephone number for which the call was intended (destination end-point). Complete telephone numbers narrow the search; incomplete telephone numbers broaden it. When you enable Called Number Filtering, you include among your CDR search criteria the destination end-point to which the call was directed.
- Calling Number—all or part of the telephone number from which the call took place. The Calling Number value might be an unreliable source of information and might not provide valid matches to your query. Therefore, data entry in the Calling Number field is disabled by default.

  If your search query proves too broad to produce the desired results, you can narrow your search by providing a Calling Number value. When you enable Calling Number Filtering, you include among your CDR search criteria the source end-point to which the call was directed.

CDR results appear in the large white space within the Voice Trace Query window. This area contains a collapsible tree display of CDRs received from the server.

You can expand a CDR to display additional information about the segment, such as the date and time of the call, the IP address of the VoIP device, the port, and the cause of termination. Information in the tree view allows you to confirm that you found the correct CDR before you start to trace the path between the end-points.

Layer 3 Paths

The Layer 3 path is the logical path on the network that packets follow through Cisco devices such as routers. Layer 3, known also as the network layer, represents the logical network, the network at the Internet Protocol (IP) level. Layer 3 path displays the end-points and routers on the network.

Layer 3 output from Path Analysis is similar to the output of the UNIX and Windows NT traceroute command, but is more detailed.

Path Analysis supports only the IP protocol at this time. AppleTalk and IPX are not supported. Layer 3 tracing does not support PCs or workstations with more than one network adapter.

Layer 2 Paths

The Layer 2 path is the physical path on the network that packets follow through Cisco devices.

The Layer 2 path includes devices that are either Simple Network Management Protocol (SNMP) accessible and known through Topology Services, or are SNMP inaccessible but have been discovered by User Tracking (for example, end-user hosts).

The Layer 2 path provides further resolution of the Layer 3 path, but is not necessarily a complete representation of all Layer 2 devices. For example, hubs or other devices that do not support the Cisco Discovery Protocol (CDP) do appear in the Layer 2 traces.

Path Analysis uses information from the ANI Server to build Layer 2 paths, combining:

- Network topology information.
- Virtual LAN (VLAN) and Emulated LAN (ELAN) information. Refer to the “Virtual LANs (VLANs)” section on page 2-16.

- User and host information.
- Current LAN spanning tree configuration.

Path Analysis supports Layer 2 tracing on Ethernet, Fast Ethernet, Gigabit Ethernet, and LAN Emulation (LANE) networks. LANE support includes tracing on the path inside an ATM cloud. For this release, Path Analysis Layer 2 tracing does not support FDDI, Token Ring, and WAN interfaces or router bridge groups.

Note As a general rule, do not expect to see a Layer 2 path for every Layer 3 hop.

Shortcuts

Shortcut connections occur in the Layer 2 path where packets are IP-switched after the router has determined the next-hop destination.

Shortcuts appear in the Layer 2 path as connections between switch ports, which bypass intervening routers. Currently, the only shortcuts reported are those provided by the Cisco Catalyst 5000 switches.

You can recognize shortcuts in the Map display in one of two ways:

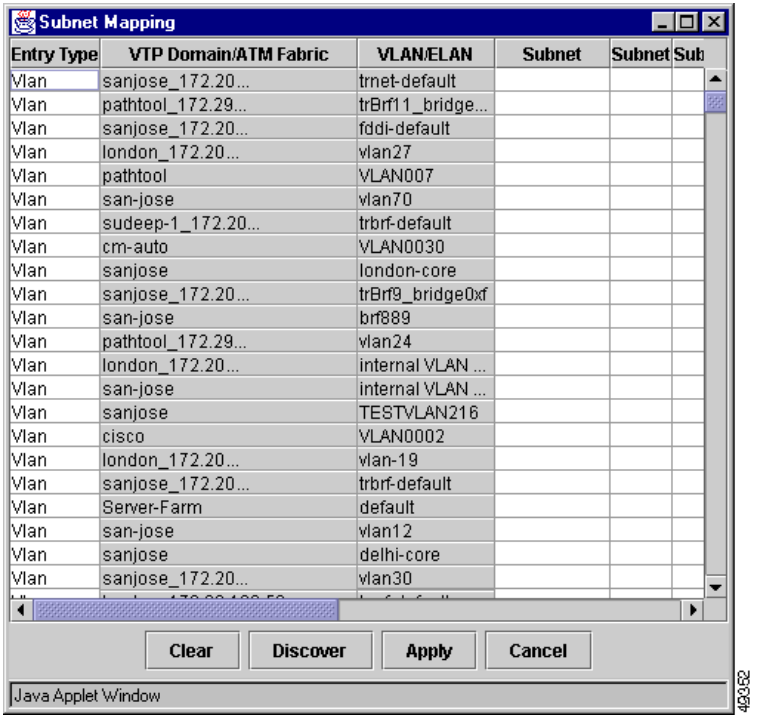
- Where shortcutting exists and the Layer 2 path is known, the shortcutting switches are highlighted in blue and connected by an arrow.
- Where shortcutting exists but the complete Layer 2 path is unknown, the recognized shortcutting switch is highlighted in blue.

Subnet to VLAN/ELAN Mapping

The VLAN/ELAN Subnet Mapping Table displays VLAN, ELAN, and associated subnet mappings. This information can be useful when performing Layer 3 traces and is required in order to perform Layer 2 traces.

You should view the VLAN/ELAN Subnet Mapping Table during the initial setup of Path Analysis and whenever your subnet mapping changes. To view the table, select **Edit >Subnet Mapping...**. The VLAN/ELAN Subnet Mapping Table window appears, similar to the one shown in Figure 5-3. If you need to, you can add or delete entries in the table, or discover a fresh set of information.

Figure 5-3 VLAN/ELAN Subnet Mapping Table



On a typical network, information displayed in the table is discovered automatically by the Path Analysis application. It is therefore unlikely that you would need to insert additional entries manually.

The first three columns in the VLAN/ELAN Subnet Mapping Table contain text that cannot be edited. The column headings are **Entry Type**, **VTP Domain/ATM Domain**, and **VLAN/ELAN**. You can edit the text in any **Subnet** column.

One of three font styles is used to render information in a cell. The use of a particular font conveys information about the source and validity of a mapping:

- Black, plain text indicates an automatically discovered mapping that is known to the system.
- Blue, italic text indicates a manually provided mapping that is unknown to the system.
- Red, bold type indicates invalid information (for example, bad syntax).

Note You must click **Apply** for any changes to take affect on the server. No changes take affect on the server until you click **Apply**.

To verify whether you must enter information manually, click **Clear**, and then **Discover** to see the automatically discovered mapping of subnets to VLANs or ELANs, as well as subnets that do not map to any VLAN or ELAN. If you know the information is incomplete, you must enter the missing information manually.

The results of automatic discovery might vary slightly over time, even if the structure of your network is unchanged. If you obtain a complete set of information using discovery, you might want to apply that information to the server, in case subsequent discoveries are incomplete.

Note If you remove a VLAN/ELAN from your network, you must remove the corresponding information from the table.

VLAN/ELAN Subnet Mapping Table and Layer 2 Tracing

You can specify three types of entries in this table: VLAN, ELAN, and Subnet. For each VLAN or ELAN entry in the table, you can specify the subnets that reside on that VLAN/ELAN. If this information is not provided manually and cannot be discovered automatically, Layer 2 tracing cannot occur on that subnet.

Therefore, you should check the automatically discovered values following an installation, and enter any needed information. If information is missing from the VLAN/ELAN mapping table, no Layer 2 traces are performed on those subnets with missing mapping information.

The following conditions are acceptable mappings:

- A VLAN/ELAN is not mapped to a subnet if that is the actual case in the network. This can occur, for example, when a VLAN or ELAN is used for non-IP traffic.
- A VLAN/ELAN is mapped to more than one IP subnet. This is not a common configuration, but does occur occasionally in some networks.
- A single subnet is mapped to multiple VLAN/ELAN entries. This occurs when you have multiple VLANs and ELANs bound together to form a larger LAN that corresponds to a subnet.

VLAN/ELAN Subnet Mapping Table and Layer 3 Tracing

Successful Layer 3 tracing requires that all subnets within the managed domain are listed in one of the table rows.

Use this information to identify non-Cisco or non-Cisco Discovery Protocol (CDP) devices. These are devices that are not discovered or displayed in Topology Services views.

Layer 3 traces would generally access these devices through SNMP unless they reside on a known, managed subnet within the organization. Layer 3 path traces make this determination by referencing these devices to the VLAN/ELAN Mapping Table.

If a subnet has no entry in the table, there will be no SNMP information in the table view or outgoing interface information for the non-Cisco or non-CDP devices on that subnet. Layer 3 path traces will function properly in all other respects, however.

The Entry Type column shows three types of entries: Vlan, Elan, and Subnet.

If the Entry Type column shows Vlan or Elan, subnets for corresponding VLANs or ELANs are listed in the Subnet column(s) for that row.

If the Entry Type column shows Subnet, the stand-alone subnet (one that does not map to a VLAN or ELAN) appears in the first Subnet column for that row. Do not add entries in the Subnet column for stand-alone subnets.

Troubleshooting Path Analysis

Use the information in the following topics to help you troubleshoot Path Analysis:

- Frequently Asked Questions, page 5-18
- Troubleshooting Suggestions, page 5-25

Frequently Asked Questions

Use the information in these sections to answer some of your common questions:

- What are the most common operator errors?, page 5-19
- What do the status bar and alert box messages mean?, page 5-19
- What do the different kinds of lines and icons represent in Map Display?, page 5-21
- Can I have more than one Path Analysis window open and working at one time?, page 5-21
- What are valid source and destination end-points?, page 5-21
- Does Layer 2 Path Analysis support tracing virtual connections inside ATM clouds?, page 5-21
- Why do I have a Layer 2 path with some Layer 2 devices missing?, page 5-21
- How can I troubleshoot a failed Layer 3 path trace?, page 5-22
- If a previously discovered end-user station becomes unreachable, how do I determine which switch port it is connected to?, page 5-22
- Do I need to configure anything to enable voice traces to function?, page 5-22
- Am I required to use the Voice tab for voice traces?, page 5-23
- Should I use parentheses or hyphens when specifying a telephone number for voice tracing?, page 5-23
- Should I specify a calling number for voice tracing?, page 5-23
- Should I specify the called number for voice tracing?, page 5-23
- Should I specify the time and time range for voice tracing?, page 5-23
- What is the best time range to specify for voice tracing?, page 5-24
- How do I trace calls over a PSTN?, page 5-24
- Can I perform a trace on busy or unanswered calls?, page 5-24

What are the most common operator errors?

These are two of the more common errors:

- Incomplete subnet to VLAN/ELAN mapping information. See the "Subnet to VLAN/ELAN Mapping" section on page 5-14 section for information about providing subnet mappings for VLANs.
- Invalid community strings (SNMP passwords) for managed devices. Refer to *Getting Started with the CiscoWorks2000 Server* for information about setting community strings for managed devices.

What do the status bar and alert box messages mean?

The following are informational status messages:

- "Trace Completed" means that the trace succeeded.
- "Trace Stopped" means that you intervened to stop the trace prematurely.
- "Trace Running" means that the trace is still in progress and has not yet encountered any problems.

All other status bar or alert box messages indicate that an error has occurred. See Table 5-3 for definitions of the status bar messages and alert box messages.

Table 5-3 Status Bar Messages

Message	Probable Cause	Severity	Possible Solution
'From' field contains bad source endpoint	Invalid string entered for path trace source.	Low	Confirm that the **From** field entry is a valid IP address or DNS name.
'To' field contains bad destination endpoint	Invalid string entered for path trace destination.	Low	Confirm that the **To** field entry is a valid IP address or DNS name.
Source and Destination Endpoints are on same device	Not possible to trace path between two IP addresses on one device.	Low	Make sure the **To** and **From** entries are not for the same device.
Trace Running	Trace has not yet completed.	N/A	—

Table 5-3 Status Bar Messages (continued)

Message	Probable Cause	Severity	Possible Solution
Trace Aborted	Error or anomalous situation prevented successful path trace.	Variable	—
Trace Timed Out	Trace attempt exceeded the timeout value (default 4 minutes). Path traces can take up to several minutes to complete.	Variable	Select **Edit > Options...** and increase the default trace timeout value.
Trace Stopped	User stopped trace.	N/A	—
Trace Completed	Trace completed successfully.	N/A	—

Table 5-4 Alert Box Messages

Message	Definition	Severity	Possible Solution
Could not reach source	No IP connectivity between the CiscoWorks2000 Server and source.	High	Run a path trace between the CiscoWorks2000 Server and the source to analyze IP connectivity. Ping the device to determine if it is reachable.
Could not complete trace	One or more Layer 3 hops determined, but trace did not reach destination. Typically results from firewall rules, access lists, or blocked source-routed packets.	Variable	1. Choose a destination on the same side of the firewall as the source. 2. Verify access lists along the path and correct any problems. 3. Confirm that no routers along the path block source-routed IP packets.
Could not determine first hop	No known hops. Information to determine first hop is incomplete or inconsistent.	High	1. Confirm that source is in managed domain and SNMP-accessible. 2. Verify community strings. 3. Confirm end-user stations are not multihomed (containing multiple NICs). Path Analysis does not support this configuration.

What do the different kinds of lines and icons represent in Map Display?

The different kinds of lines and shapes in Map View are visual clues, and each has a specific meaning. See the Path Analysis online help for detailed information about interpreting these lines and shapes.

Can I have more than one Path Analysis window open and working at one time?

Yes. Path Analysis supports multiple, concurrent path traces from a single computer. You can start additional instances of a running Campus Manager application only after the first running instance of that application is loaded and functional.

What are valid source and destination end-points?

Path Analysis uses strict selection criteria for source and destination end-points. See the "Valid Data Path Trace End-Points" section on page 5-10 section for more details.

Does Layer 2 Path Analysis support tracing virtual connections inside ATM clouds?

Yes, but only for LAN Emulation (LANE).

Why do I have a Layer 2 path with some Layer 2 devices missing?

Two common reasons a Layer 2 path exists with some Layer 2 devices missing are:

- On a Layer 2 path, only Cisco Discovery Protocol (CDP) devices that are known to Topology Services are shown. Hubs or non-Cisco devices are not shown.
- If there has not been a successful Virtual Connection (VC) trace, the Layer 2 path only includes the LANE devices on the edges of the ATM cloud, not ATM switches inside the ATM cloud.

How can I troubleshoot a failed Layer 3 path trace?

Do the following:

- Determine the meaning of the status bar message. See Table 5-3.
- Ping the source and/or destination.
- Perform a traceroute on the source and/or destination.

If a previously discovered end-user station becomes unreachable, how do I determine which switch port it is connected to?

View the User Tracking entries for the unreachable end-user station.

Alternatively, you can run a path trace from anywhere else on the network to this end-user station. The last hop appears in Map view as a dotted line (best guess).

Why does an end-user station that is known to User Tracking show as an unmanaged device in Path Analysis?

Path Analysis relies on User Tracking entries that have been discovered in the last 48 hours. If you want to use an end-user station as a source or destination end-point for a path trace, you must perform a User and Host Acquisition in User Tracking or run Discover All in Path Analysis.

Do I need to configure anything to enable voice traces to function?

Yes, you need to:

Step 1 Enable Call Detail Record (CDR) logging on Cisco CallManager.

Step 2 Enable Simple Network Management Protocol (SNMP) on Cisco CallManager.

Step 3 Provide community strings for all Media Convergence Servers to the ANI Server.

Step 4 Provide IP addresses for discovery of Media Convergence Servers.

Am I required to use the Voice tab for voice traces?

In most cases, you must select the Voice Trace button in the Path Analysis main window to trace completed Voice over IP (VoIP) calls. However, there are two exceptions.

Do not select the Voice Trace button if you are looking at the signaling path by either:

- Tracing calls between an IP phone and a Media Convergence Server
- Tracing calls between a gateway and a Media Convergence Server

In these two cases, select the Data Trace button instead.

Should I use parentheses or hyphens when specifying a telephone number for voice tracing?

Any parentheses, hyphens, spaces, or other non-numeric characters that you enter when specifying a telephone number for voice tracing are automatically deleted from your query.

Should I specify a calling number for voice tracing?

The Calling Number value might not provide valid Call Detail Record (CDR) matches to your query, so in most cases you should not specify a calling number.

However, if you do not specify a calling number, and if your query results in too many CDRs found, then you can narrow your search criteria by specifying a calling number.

Should I specify the called number for voice tracing?

Yes, it is best to specify the called number.

Should I specify the time and time range for voice tracing?

Yes. It is best to specify the start time and time range for voice tracing.

What is the best time range to specify for voice tracing?

In many cases, a 15-minute range before and after the specified time is sufficient to locate a call without exceeding the limit of 100 Call Detail Records (CDRs).

If your query matches more than 100 CDRs, no records are shown. Instead, an error message appears.

If you specify a time range that is too brief, the search might not find your desired CDR.

How do I trace calls over a PSTN?

IP phone calls routed over a Public Switched Telephone Network (PSTN) follow a uniform path:

1. The source IP phone sends Voice over IP (VoIP) packets to the source gateway.
2. Packets flow from the source gateway through the PSTN on their way to the destination gateway.
3. The destination gateway routes packets to the destination IP phone.

Calls following this path produce one Call Detail Record (CDR) for the first leg of the call and another CDR for the final leg of the call. Each CDR contains a start and end-point for its leg of the call. No CDR exists for the PSTN path.

When you search for this kind of call, both CDRs should appear in the Voice Trace Query Results window. You must then select each CDR independently to perform a trace on that leg of the call.

You cannot perform a voice trace on the PSTN leg of the call.

Can I perform a trace on busy or unanswered calls?

Yes, however you must perform a *data* trace using the *IP addresses* of the IP phones. You cannot perform a voice trace using the calling and called numbers because busy or unanswered calls do not generate CDR records.

Troubleshooting Suggestions

Use the information in Table 5-5 to troubleshoot the Path Analysis application.

Table 5-5 Troubleshooting Path Analysis

Symptom	Probable Cause	Possible Solution
Data Traces		
Path Analysis client does not start.	Path Analysis could take up to several minutes to start because there are many files that must be loaded and processed from the server. There is a problem with the server.	1. Make sure you allow enough time for Path Analysis to load and process the files from the server. 2. Make sure you have specified the correct URL. 3. Make sure the server is up and running. 4. Select **Server Configuration > Administration > Process Management > Process Status** to confirm that all required services on the server are up and running. If any required services are not running, start them. Refer to *Getting Started with the CiscoWorks2000 Server*. 5. Reboot the server.

Table 5-5 Troubleshooting Path Analysis (continued)

Symptom	Probable Cause	Possible Solution
Path Analysis client starts, but error message displays.	Server processes are not running normally.	Select **Server Configuration > Administration > Process Management > Process Status** to confirm that the ANI server, ANI DB engine, Gatekeeper, EDS-TR, and EDS services are running on the server. If any processes are not running, start them.
Start a path trace and get "undefined seed" error message.	Seed device was not specified in ANI.	Select **Server Configuration > Setup > ANI Server Admin > Discovery Settings** to define a seed device.
Start a path trace and get "Initial discovery in progress" error.	After the ANI server process has begun network discovery, it takes several minutes (or hours depending on the size of the network) to complete the discovery. When ANI discovery concludes, then user and host acquisition begins. No path trace is possible until both of these processes are complete.	Wait until ANI discovery, User Tracking ping sweeps, and user and host acquisition have completed before starting a path trace. You can monitor the progress of the discovery process in Path Analysis, which gives an indication of all three processes.
Intermittent or recurring Path Analysis performance lag.	You have a misconfigured or non-functional DNS server. Your network is congested. One or more of your devices is too busy to respond to SNMP queries.	Confirm that your DNS servers are operational and properly configured.

Table 5-5 Troubleshooting Path Analysis (continued)

Symptom	Probable Cause	Possible Solution
Path is discovered, but does not seem to function as shown.	An ACL (access control list) is allowing traffic from your CiscoWorks2000 server to the destination end-point, but is blocking traffic between your source and destination end-points.	None.
No Layer 2 path for a given Layer 3 hop.	Layer 2 analysis is possible only when both ends of the Layer 3 hop are managed Cisco devices known to Topology Services or end-user stations known to User Tracking. A question mark icon on either end of the Layer 3 hop indicates that these prerequisites have not been met. Refer to the "Path Analysis Concepts" section on page 5-7 for more information about prerequisites for performing Layer 2 path analysis.	1. Enable CDP for all Cisco devices. 2. In Topology Services, verify that all devices on this subnet are discovered and SNMP-accessible. If they are not, then verify their community strings and run ANI Discovery again. 3. Verify that end-user stations are listed by User Tracking. If they are not, then run user and node acquisition again, preferably with ping sweeps enabled. 4. If there are VLANs or ELANs associated with this subnet, verify that the subnet mappings are correct for each Layer 3 hop and confirm that Topology Services has complete and accurate VLAN/ELAN information for all interfaces.

Table 5-5 Troubleshooting Path Analysis (continued)

Symptom	Probable Cause	Possible Solution
Not all Layer 2 devices in the physical path are shown.	Path Analysis displays only those Layer 2 Cisco devices known to Topology Services and end-user stations known to User Tracking. It does not include intervening hubs or non-Cisco or non-CDP devices.	No action required.
No Layer 2 shortcutting (multilayer switching) is shown on the Map view.	Layer 2 shortcuts are supported on Catalyst 5000 switches (including the RSM module). Shortcut information only appears if you have specified the correct write community string. The Catalyst 5000 creates shortcuts on the first few packets in a flow, but they can be aged out. It is possible that a shortcut might not be present when you run a path trace. You can create a shortcut by having the source generate a few packets towards the destination before running a path trace.	If you do not see shortcut information on a Catalyst 5000 device, it might be because a shortcut does not exist or you do not have the correct write community string specified. Select **CiscoWorks2000 > Setup > ANI Server Admin > SNMP Settings** to confirm that you have the correct write community string specified. (The write community string is used to query the MLS MIB; not to configure the device.)
A LANE segment appears in the Layer 2 trace, and shows connectivity between two LANE clients on either side of an ATM cloud, but does not show the intervening ATM switches.	There was no data-direct virtual channel between the two LANE clients during the trace. There are unsuppored software revisions on ATM switches and LANE cards in the ATM cloud.	See the Cisco documentation available on CCO. Select **Cisco Product Documentation > Network Management > CiscoWorks2000 > Campus Manager/ CWSI Campus > Supported Devices**.
Path Analysis did not find a complete Layer 3 path between the source and the destination devices.	There could be many possible causes.	Check the status bar for messages and check for alert box messages. See Table 5-3 and Table 5-4.

Table 5-5 Troubleshooting Path Analysis (continued)

Symptom	Probable Cause	Possible Solution
Table view does not contain the full set of information on Layer 3 interfaces.	Path Analysis collects this information about Cisco devices that are SNMP-reachable and on non-Cisco routers as long as they are SNMP-reachable and are within a subnet that is known to be within the organizational domain. The organizational domain comprises the subnets listed in the Subnet to VLAN/ELAN mapping table.	1. Check the community strings and correct them if necessary. 2. Select **Topology Services > View > Display View** and confirm Cisco devices are SNMP-accessible (green icon). 3. Check the Subnet to VLAN/ELAN mapping table and make sure that the subnet of the device is listed. Refer to the "VLAN/ELAN Subnet Mapping Table and Layer 2 Tracing" section on page 5-16.
Voice Traces		
No records found in query.	Records might not be found because: • The Media Convergence Server might not have been discovered. • The search criteria are too narrow. • Call Detail Record (CDR) logging is disabled on the Media Convergence server, or on one or more Media Convergence Servers in a cluster.	1. Select **Topology Services > Layer 2 View** and check whether the Media Convergence Server was discovered. The Media Convergence Server icon should be green. 2. Enter a less restrictive time range, exclude the Calling Number value, and/or enter a less specific called number. 3. Enable CDR logging on Cisco CallManager.

Table 5-5 Troubleshooting Path Analysis (continued)

Symptom	Probable Cause	Possible Solution
Too many matches found.	The search criteria are too broad.	Enter a more restrictive time range or a more specific calling or called number.
Call Detail Record (CDR) query takes too long.	CDR query might take too long because: • Your search criteria are too broad. In organizations with high call volume, a longer time range (outside the 15-minute recommended range) might be too broad, causing the Media Convergence Server to have to search through too many records. • Path Analysis cannot access the Media Convergence Server.	1. Narrow your search criteria by reducing the time range or providing a calling number. 2. Make sure that all Media Convergence Servers that have been discovered in Topology Services are running and accessible.