



Managing Physical and Logical Network Services with Topology Services

Topology Services is an application that enables you to view, monitor, and configure the physical and logical services on your network:

- View detailed network information about all devices, links, and ports in your network.
- View a display of the physical and logical services in your network. Open network management tools from the network views.
- Configure, manage, and monitor the ATM devices in your network.
- Logically segment your network and manage workgroups that use VLANs.
- Create and manage the LANE services in your network to extend VLANs across ATM devices
- View port, device, and trunk attributes; view and find port information in a VTP domain; and configure VLANs on a trunk.
- Display reports about inconsistencies or misconfigurations in your physical and logical network setups.

The following topics give an overview of Topology Services. For more detailed information, refer to the Topology Services online help.

- Starting and Navigating in Topology Services, page 2-2
- Using Topology Services, page 2-6
- Topology Services Concepts, page 2-13
- Troubleshooting Topology Services, page 2-33

Starting and Navigating in Topology Services

From the CiscoWorks2000 desktop, select **Campus Manager > Topology Services**. The Topology Services main window appears.

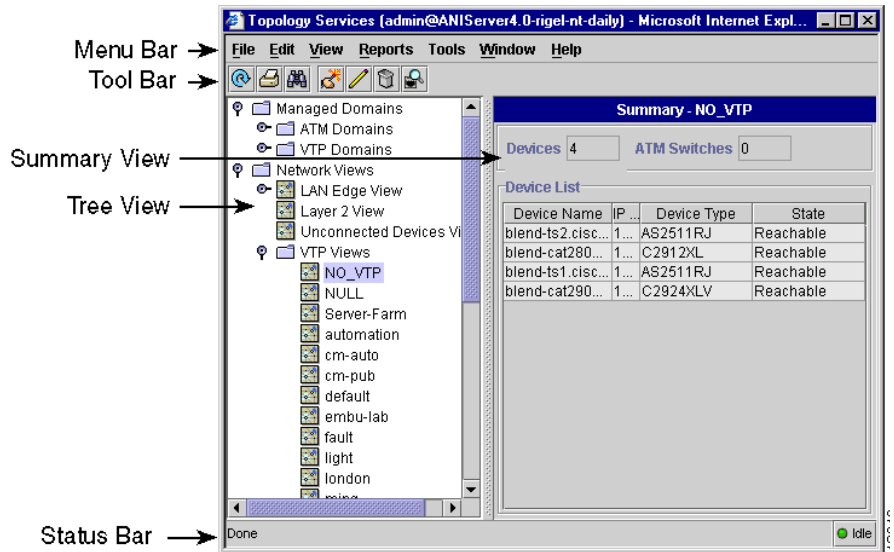
Topology Services provides multiple windows for performing tasks. Refer to the following sections for a description of the elements in the windows:

- Using the Topology Services Main Window, page 2-2
- Using Network Topology Views, page 2-5

Using the Topology Services Main Window

The Topology Services main window displays VTP domains, VLANs, ATM domains, and ATM-VLANs discovered in your network. The main window is divided into five components: Menu Bar, Tool Bar, Tree View, Summary View, and Status Bar (see Figure 2-1).

Figure 2-1 Topology Services Main Window



Topology Services provides several methods for accessing network information or status, as shown in Table 2-1.

Table 2-1 Topology Services Main Window Components

Item	Description	Usage Notes
Menu Bar	Contains Topology Services commands.	None.
Toolbar	Provides quick access to frequently used menu options.	To show or hide the toolbar, select View > Show Toolbar .
Tree View	Displays discovered VTP domains, VLANs, ATM domains, and ATM-VLANs. You can access the LAN Edge, Layer 2, and Unconnected Devices network views of managed domains.	<ul style="list-style-type: none"> Right-click items and select Display View to display network topology views. Single-click icons or links to display summary information.
Summary View	Displays configuration information about the items displayed in the Tree View.	Click and drag column headings to change the order in which they appear.

Table 2-1 Topology Services Main Window Components (continued)

Item	Description	Usage Notes
Status Bar	Displays Topology Services system messages on the left and the Discovery Status button on the right.	Double-clicking on the status light displays the Discovery Information dialog box, which tells you your ANI Server and User Tracking login status and the completion time of the last ANI and User Tracking discoveries.

You can access all network and domain summary information from Topology Services by clicking on the corresponding folder in the tree view of the main Topology Services window:

Managed Domains—Displays the ATM and VTP domain configuration.

Network Views—Displays the following:

- **LAN Edge View**—Shows network connectivity between Layer 3 devices that have routing characteristics. Devices without Layer 3 connectivity are placed in ATM Domain or Switch Cloud network views.
 - **ATM Domain View**—Displays the ATM switches and ATM end-hosts in your network.
 - **Switch Cloud View**—Displays the Layer 2 devices between two Layer 3 devices in your network.
- **Layer 2 View**—Displays the Layer 2 information about your network, including ATM and LAN switches, routers, MLS devices, hubs, and switch probes.
- **Unconnected Devices View**—Displays devices for which connectivity information could not be obtained, including devices that are not supported by Topology Services. This can include non-Cisco ATM devices discovered through Integrated Local Management Interface (ILMI), since it is an industry standard.
- **VTP Views**—Displays devices that are participating in VTP domains. Also displays the non-VTP devices and ATM domain connected directly to the VTP domain.

Using Network Topology Views

A network topology view is a graphical representation of the devices in your network. You can use network topology views to see different aspects of your network. Only devices and links discovered in your network are displayed. As you use Topology Services, listed devices and links change dynamically to display what the ANI Server discovers in your network.

Network Topology views provide various abstract views of your network (see Figure 2-2). Table 2-2 describes the Network Topology window components.

Figure 2-2 Network Topology Windows

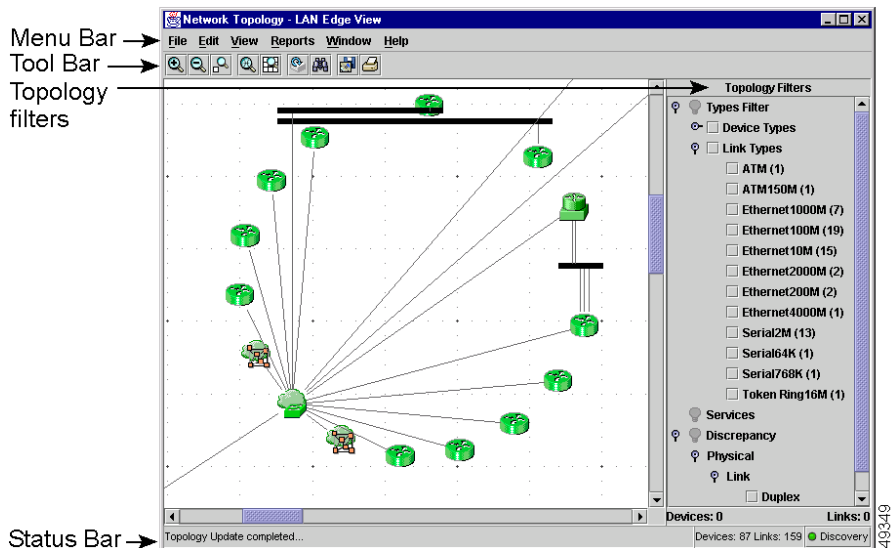


Table 2-2 Network Topology View Components

Item	Description	Usage Notes
Menu Bar	Contains Topology Services commands.	None.
Toolbar	Provides quick access to frequently used menu options.	To show or hide the toolbar, select View > Show Toolbar .

Table 2-2 Network Topology View Components (continued)

Item	Description	Usage Notes
Topology Filters	Allows you to filter and display devices and links.	Filter device types, link types, network discrepancies, LANE components, and ATM components.
Status Bar	Displays Topology Services system messages on the left and the Discovery Status button on the right.	Click the color-coded Discovery Status button to view the Discovery Information window for ANI Server and User Tracking status.

Using Topology Services

Table 2-3 describes the main tasks you can perform with Topology Services. For more information about each task, refer to Topology Services online help.

Table 2-3 Topology Services Tasks

Task	Purpose	Action
View summary information.	Displays detailed information about the managed domains in your network.	From the tree view, click on a managed domain or a network view from the tree view. The summary information about the domain appears in the right pane.
Open a network topology view.	Displays a graphical representation of the devices in your network. You can customize the network views and use Find to find elements in the network views.	<ol style="list-style-type: none"> 1. Right-click on an item in the tree view. 2. Click Display View. The Network Topology window opens. <p>To change the view layout:</p> <ol style="list-style-type: none"> 1. Select View > Relayout. 2. Choose a layout style.

Table 2-3 Topology Services Tasks (continued)

Task	Purpose	Action
Display Device Labels.	Displays device information labels in network topology views.	<ol style="list-style-type: none"> 1. From a network topology view, select View > Display Labels > For All Nodes. 2. Select the type of label you want displayed: <ul style="list-style-type: none"> – DNS Name – IP Address – SysName <p>To clear labels, select View > Display Labels > Clear Labels.</p>
Download a Cisco Visio stencil.	Downloads the cm_cisco.vss stencil file. After the stencil is downloaded once, you can export a network topology view to Visio.	<ol style="list-style-type: none"> 1. From a network topology view, select File > Download Visio Stencil. 2. Navigate to a directory where you want to save the file. Do not change the default filename. 3. Click Save.
Export a network topology view to Visio.	Exports a network topology view as a text file that can be used in Visio to create a drawing.	<ol style="list-style-type: none"> 1. From a network topology view, select File > Export to Visio... The Enter the CISCO stencil file window appears. 2. Navigate to the directory where you saved the Cisco stencil file (cm_cisco.vss). 3. Select the file and click Open. 4. Accept the default name or enter a filename. 5. Select Save.

Table 2-3 Topology Services Tasks (continued)

Task	Purpose	Action
Display Device, Port, Link, Aggregate Link, or Trunk Attributes.	Displays information about devices, ports, links, aggregate links, or trunks on your network.	<ol style="list-style-type: none"> 1. From a network topology view, select a managed domain or network view. 2. Select a device, port, link, or trunk that you want information on. 3. Select Reports, then the type of report you want to view: <ul style="list-style-type: none"> • Device Attributes • Port Attributes • Link Attributes • Aggregate Link Attributes • Trunk Attributes
Display Service Attributes.	Displays information about the available services in your network.	From a network topology view, right-click an application server icon and select Service Attributes .
Access ICS Devices.	Starts the Cisco ICS System Manager.	From a network topology view, right-click an ICS device icon and select Cisco ICS System Manager .
Access Application Servers and start Cisco CallManager.	Gives access to an applications server.	<ol style="list-style-type: none"> 1. From a network topology view, right-click an application server icon and select Service Attributes. 2. Click the Launch button in the Launch column of the Service Attributes window.

Table 2-3 Topology Services Tasks (continued)

Task	Purpose	Action
Display Multi-Layer Switching (MLS) Reports.	Displays information about devices in your network that participate in multi-layer switching.	<ol style="list-style-type: none"> 1. From a network topology view, click two or more MLS devices. 2. To display relationships between: <ul style="list-style-type: none"> • Layer 3 route processing devices, select Reports > Multi-Layer Switching > Route Processors. • Layer 3 switching and forwarding devices, select Reports > Multi-Layer Switching > Switch Engines.
View ANI Server Discovery Metrics.	Displays a report containing statistics for the last <i>n</i> discovery cycles.	From the Topology Services main window, select Reports > Discovery Report .
View Discrepancy Reports.	Displays a report of physical or logical discrepancies on your network.	<ol style="list-style-type: none"> 1. From the CiscoWorks2000 desktop, select Campus Manager > Discrepancy Reports. 2. Select the type of discrepancies you would like to view: <ul style="list-style-type: none"> • Physical Discrepancies—potential misconfigurations in the physical layout of your network. • Logical Discrepancies—potential misconfigurations in the logical setup of the VTP Domains, VLANs, and LANE components of your network.
Customize Discrepancy Reports.	Allows you to choose which discrepancies you want reported.	<ol style="list-style-type: none"> 1. From the CiscoWorks2000 desktop, select Campus Manager > Administration > Network Discrepancies. 2. Select the discrepancies you would like displayed and click Apply to save your changes.

Table 2-3 Topology Services Tasks (continued)

Task	Purpose	Action
View the Color and Icon Legend.	Displays a legend of icons and colors used in the network views.	Select Help > Legend...
Create an Ethernet VLAN.	Provides a visual method of creating, modifying, and deleting an Ethernet VLAN in your network.	<ol style="list-style-type: none"> 1. From the tree view, select a VTP domain 2. Select Tools > VLAN Management > Create > Ethernet... and enter the required information in the fields. 3. Click Apply.
Create a Token Ring VLAN.	Provides a visual method of creating, modifying, and deleting a Token Ring VLAN in your network.	<ol style="list-style-type: none"> 1. Create the Token Ring BRF: <ol style="list-style-type: none"> a. From the tree view, select a VTP domain. b. Select Tools > VLAN Management > Create > Token Ring BRF... and enter the required information in the fields. c. Click Apply. 2. Create the Token Ring CRF: <ol style="list-style-type: none"> a. Select the same VTP domain you selected in Step 1. b. Select Tools > VLAN Management > Create > Token Ring CRF... and enter the required information in the fields. c. Click Apply.

Table 2-3 Topology Services Tasks (continued)

Task	Purpose	Action
View Spanning Tree definitions.	Allows you to view the spanning tree definitions on your network.	<ol style="list-style-type: none"> 1. From the Topology Services main window, select Managed Domains > VTP Domains. 2. Double-click a VTP Domain. 3. Select a VLAN. 4. Select View > Display View. The Network Topology window appears. 5. Double-click VLAN in the Topology Filters list. 6. Select the Spanning Tree check box.
Add a LAN Emulation Server (LES) to an existing VLAN.	Allows you to extend VLANs across ATM networks.	<ol style="list-style-type: none"> 1. From the tree view, select a VLAN. 2. Select Tools > LANE Management > Add/Modify LANE Services... 3. Select a device to use as the LE server from the drop-down list box.
Configure an LE Config Server (LECS).	Allows you to configure an LE Config Server (LECS) on each ATM domain.	<ol style="list-style-type: none"> 1. From the tree view, select a VLAN. 2. Select Tools > LANE Management > Configure Config Server. The Config Servers for each ATM domain are shown. 3. Select a device to use as the LECS from the drop-down list box.
Create an SPVC or SPVP.	Allows you to create an SPVC or SPVP between two devices.	<ol style="list-style-type: none"> 1. From the tree view, select an ATM domain. 2. Select Tools > ATM Management > Create SPVC/SPVP.

Table 2-3 Topology Services Tasks (continued)

Task	Purpose	Action
Display a Virtual Connection.	<p>Displays information about a virtual connection (VC).</p> <p>You can focus on particular VC types in your ATM domain, and you can determine the amount of bandwidth used on a link by a VC.</p>	<ol style="list-style-type: none"> From the Topology Services main window, select Tools > ATM Management > Display VCs. Select either: <ul style="list-style-type: none"> Per Device—displays all the active connections on the selected link. Between Devices—select two links and display a list of virtual connections between them. This selection is valid only for SVCs and links connecting ATM hosts.
Perform a Virtual Connection (VC) Trace.	Displays information about your virtual connection (VC) in tabular and graphical formats.	<ol style="list-style-type: none"> Display the desired virtual connections in your ATM network. From the VC List window, select a virtual connection. Click Trace Report. For a graphical display, click Highlight view. This trace may require substantial system resources. To clear trace reports, select the highlighted trace display in the Network Topology window and select Edit > Clear Highlighted.
Set the ATM interface configuration.	Allows you to set the interface configuration on ATM devices, without the CLI.	<ol style="list-style-type: none"> From the tree view, select an ATM domain. Select Tools > ATM Management > Interface Configuration.

Topology Services Concepts

You should understand these concepts when using Topology Services:

- ANI Server, page 2-13
- Supported Protocols, page 2-13
- Virtual LANs (VLANs), page 2-16
- LAN Emulation (LANE) Configuration, page 2-22
- VTP Domains, page 2-29
- ATM Domains, page 2-32
- Application Servers, page 2-33

ANI Server

Campus Manager uses the CiscoWorks2000 Server's Asynchronous Network Interface (ANI) Server to automatically discover devices in your network. This service must be set before you can use Campus Manager. Refer to *Getting Started with the CiscoWorks2000 Server* or the ANI Server online help for details about this service.

Supported Protocols

The following concepts are important for understanding how to use Topology Services:

- Virtual Trunk Protocol (VTP), page 2-14
- Spanning-Tree Protocol, page 2-14
- Inter-Switch Link (ISL) Protocol, page 2-15
- IEEE 802.1Q, page 2-15
- LAN Emulation (LANE), page 2-15
- Token Ring Bridging Protocols, page 2-16

You must make sure that the applicable protocols are implemented correctly in your network; otherwise, the information gathered might be incomplete.

Virtual Trunk Protocol (VTP)

To implement VLANs in your network, you must activate Virtual Trunk Protocol (VTP) on all switches that will participate in the VLAN-segmented network. Using VTP, each switch in server mode advertises its management domain on its trunk ports, its configuration revision number, and its known VLANs and their specific parameters. A VTP domain is made up of one or more interconnected devices that share the same VTP domain name. A switch can be configured for only one VTP domain.

VTP servers and clients maintain all VLANs everywhere within the VTP domain. A VTP domain defines the boundary of the specified VLAN. Servers also transmit information through trunks to other attached switches and receive updates from those trunks.

For more information on:

- VLANs—refer to the “Virtual LANs (VLANs)” section on page 2-16.
- VTP—refer to the “VTP Domains” section on page 2-29.

Spanning-Tree Protocol

Spanning-Tree Protocol is a link management protocol that provides path redundancy while preventing undesirable loops in the network. For an Ethernet network to function properly, only one active path can exist between two stations.

Multiple active paths between stations cause loops in the network. If a loop exists in the network, hosts might receive duplicate messages. In addition, switches might learn host Media Access Control (MAC) addresses on multiple switch ports. These conditions result in an unstable network.

The spanning tree algorithm calculates the best loop-free path throughout a switched network. This is necessary for the creation of fault-tolerant internetworks.

Spanning tree defines a tree with a root switch and a loop-free path from the root to all switches in the extended Layer 2 network. Spanning Tree Protocol (STP) forces redundant data paths into a standby (blocked) state. If a network segment in the spanning tree fails and a redundant path exists, the spanning tree algorithm recalculates the spanning tree topology and activates the standby path.

Inter-Switch Link (ISL) Protocol

Inter-Switch Link (ISL) is a Cisco-proprietary protocol that allows VLAN trunking by maintaining VLAN information as traffic flows between switches and routers.

You can pass VLAN information between devices by configuring links between the switches. If you want a link to carry more than one VLAN, you must use ISL. To use ISL, you must configure the ports on both sides of the link as trunk ports.

When two VTP domains are interconnected using an ISL trunk between two LAN switches, by default, no VLAN traffic is forwarded. However, you can configure the ports on each switch to receive and forward specific VLANs. To configure the ports, the VLANs on either side of the ISL trunk must be identical and share the same VLAN characteristics such as VLAN names, VLAN indexes, and so on.

IEEE 802.1Q

IEEE 802.1Q is the industry-standard encapsulation protocol to carry traffic for multiple VLANs over a single link.

LAN Emulation (LANE)

LANE services are commonly required to provide Ethernet connectivity across ATM backbones. LANE emulates the layer-2 logical services of Ethernet networks across ATM devices, such as the LightStream 1010 ATM switches and the LANE modules in the Catalyst 5000 series switches. Specifically, LANE provides the broadcast and multicast functions of Ethernet networks across these ATM backbones.

For more information on LANE, refer to the “LAN Emulation (LANE) Configuration” section on page 2-22.

Token Ring Bridging Protocols

Two Token Ring bridging protocols are supported:

- **Source-Route Bridging (SRB)**—A source-route bridge makes all forwarding decisions based upon data in the routing information field (RIF). It does not learn or look up Media Access Control (MAC) addresses. Therefore, SRB frames without a RIF are not forwarded.

If the trCRF is configured for SRB, ports configured in the trCRF are members of the broadcast domain for the non-source route (NSR) broadcast issued by stations seeking their designation station. Stations belonging to a different trCRF do not receive these broadcasts.

When the NSR broadcast fails to find the destination station, the station sends an All Routes Explorer (ARE) frame. The ARE propagates to all trCRFs belonging to the trBRF. This broadcast frame is not propagated to trCRFs belonging to other trBRFs unless there is an external connection between the trBRFs.

- **Source-Route Transparent Bridging (SRT)**—SRT bridging is an IEEE standard that combines source-route bridging and transparent bridging. An SRT bridge forwards frames that do not contain a RIF based on the destination MAC address. Frames that contain a RIF are forwarded based on source routing.

If the trCRF is configured for SRT, non-source route (NSR) broadcasts are forwarded to other trCRFs (within the same parent trBRF). The trBRF transparently bridges these NSR broadcasts to other trCRFs configured for SRT. All NSR- and NSR-configured trCRF children view the trBRF as a traditional transparent bridge.

Refer to the “Token Ring VLANs” section on page 2-21 for information about Token Ring VLANs.

Virtual LANs (VLANs)

A Virtual LAN (VLAN) is a group of devices on one or more LANs on different network segments that are configured so they can communicate as if they were all on the same network segment. VLANs are based on logical connections instead of physical connections, so they are extremely flexible.

VLANs allow you to group ports on a switch to limit unicast, multicast, and broadcast traffic flooding. Flooded traffic originating from a particular VLAN is only flooded out other ports belonging to that VLAN.

The following topics provide you with information about:

- Differences Between Traditional and Virtual LANs (VLANs), page 2-17
- Advantages of VLANs, page 2-17
- VLAN Components, page 2-19
- Types of VLANs Supported, page 2-20

Differences Between Traditional and Virtual LANs (VLANs)

A traditional LAN is configured according to the physical infrastructure it is connecting. Users are grouped based on their location in relation to the hub they are connected to and how the cable is run to the wiring closet. Segmentation is typically provided by the routers that connect each shared hub.

A virtual LAN (VLAN) is a switched network that is logically segmented by functions, project teams, or applications regardless of the physical location of users. Each switch port can be assigned to a different VLAN. Ports in a VLAN share broadcasts; ports that do not belong to that VLAN do not share these broadcasts.

Switches remove the physical constraints imposed by a shared-hub architecture because they logically group users and ports across the enterprise. As a replacement for shared hubs, switches remove the physical barriers imposed in each wiring closet.

Advantages of VLANs

VLANs provide the following advantages:

- Simplification of Moves, Adds, and Changes, page 2-18
- Controlled Broadcast Activity, page 2-18
- Workgroup and Network Security, page 2-18

Simplification of Moves, Adds, and Changes

Adds, moves, and changes are some of the greatest expenses in managing a network. Many moves require recabling and almost all moves require new station addressing and hub and router reconfiguration.

VLANs simplify adds, moves, and changes. VLAN users can share the same network address space regardless of their location. If a group of VLAN users move but remain in the same VLAN connected to a switch port, their network addresses do not change. If a user moves from one location to another but stays in the same VLAN, the router configuration does not need to be modified.

Controlled Broadcast Activity

Broadcast traffic occurs in every network. If incorrectly managed, broadcasts can seriously degrade network performance or even bring down an entire network. Broadcast traffic in one VLAN is not transmitted outside that VLAN, which substantially reduces overall broadcast traffic, frees bandwidth for real user traffic, and lowers the vulnerability of the network to broadcast storms.

You can control the size of broadcast domains by regulating the size of their associated VLANs and by restricting both the number of switch ports in a VLAN and the number of people using these ports.

You can also assign VLANs based on the application type and the amount of application broadcasts. You can place users sharing a broadcast-intensive application in the same VLAN group and distribute the application across the campus.

Workgroup and Network Security

You can use VLANs to provide security firewalls, restrict individual user access, flag any unwanted network intrusion, and control the size and composition of the broadcast domain.

You can increase security by segmenting the network into distinct broadcast groups. VLANs provide the following advantages:

- Restricts number of users in a VLAN
- Configures all unused ports to a default low-service VLAN

VLAN Components

VLAN components are:

- Switches that logically segment connected end stations

Switches are the entry point for end-station devices into the switched domain and provide the intelligence to group users, ports, or logical addresses into common communities of interest. LAN switches also increase performance and dedicated bandwidth across the network.

You can group ports and users into communities using a single switch or connected switches. By grouping ports and users across multiple switches, VLANs can span single-building infrastructures, interconnected buildings, or campus networks. Each switch can make filtering and forwarding decisions by packet and communicate this information to other switches and routers within the network.

- Routers that extend VLAN communications between workgroups

Routers provide policy-based control, broadcast management, and route processing and distribution. They also provide the communication between VLANs and VLAN access to shared resources such as servers and hosts. Routers connect to other parts of the network that are either logically segmented into subnets or require access to remote sites across wide area links.

- Transport protocols that carry VLAN traffic across shared LAN and ATM backbones

The VLAN transport enables information exchange between interconnected switches and routers on the corporate backbone. The backbone acts as the aggregation point for large volumes of traffic. It also carries end-user VLAN information and identification between switches, routers, and directly attached servers. Within the backbone, high-bandwidth, high-capacity links carry the traffic throughout the enterprise.

Types of VLANs Supported

Topology Services supports four types of VLANs:

- Ethernet VLANs, page 2-20
- ATM-VLANs, page 2-20
- Token Ring VLANs, page 2-21

Ethernet VLANs

An Ethernet VLAN is the typical VLAN design, which consists of a logical group of end-stations, independent of physical location on an Ethernet network. Catalyst switches support a port-centric, or static, VLAN configuration. All end stations connected to ports belonging to the same VLAN are assigned to the same Ethernet VLAN.

ATM-VLANs

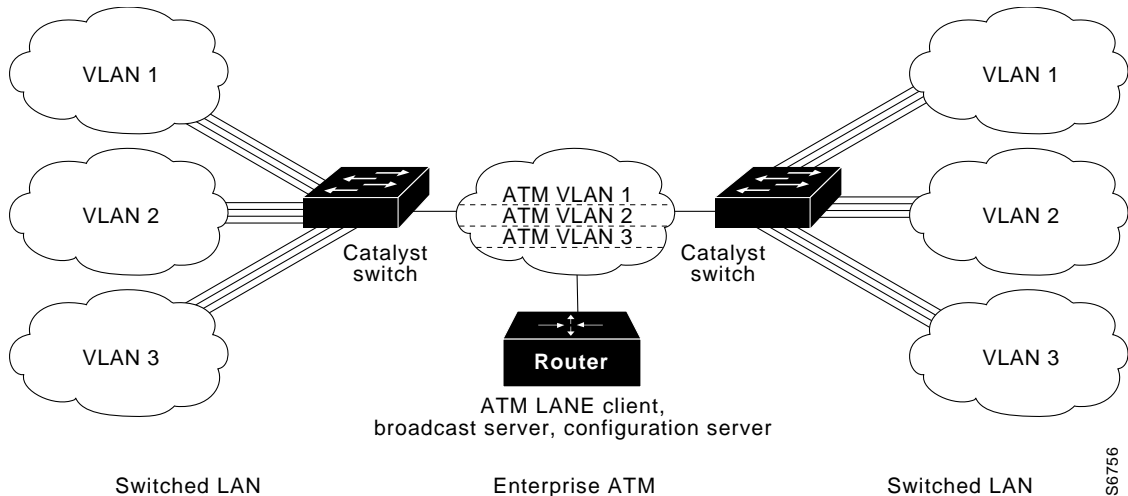
An ATM-VLAN spans an ATM network bridging two or more Ethernet VLANs using LAN Emulation (LANE). LANE provides connectivity between ATM-attached devices by emulating a LAN over an ATM cloud, including the following:

- Connectivity between ATM-attached stations and LAN-attached stations
- Connectivity between LAN-attached stations across an ATM network

Because LANE connectivity is defined at the MAC layer, upper protocol layer functions of LAN applications can continue unchanged when the devices join ATM-VLANs.

An ATM network can support multiple independent ATM-VLANs. End-system membership in any of the ATM-VLANs is independent of the physical location of the end system, which simplifies hardware moves and changes. In addition, end-stations can move easily from one ATM-VLAN to another, whether or not the hardware moves.

Figure 2-3 ATM LANE to Extend VLANs Example



S6756

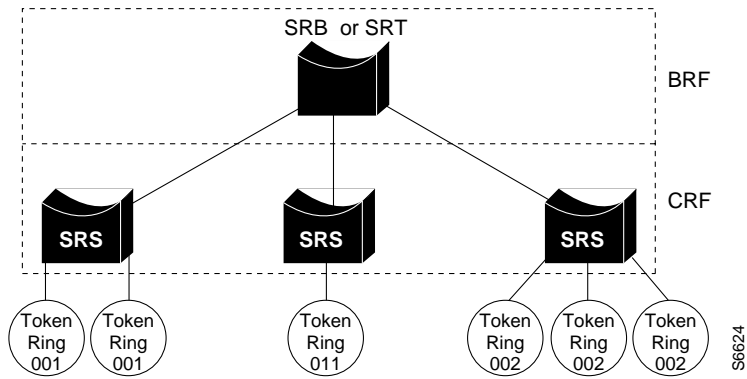
Token Ring VLANs

A Token Ring VLAN is a set of rings interconnected through a bridging function. You must use VTP version 2 to deploy Token Ring VLANs using Campus Manager.

Two Token Ring VLAN types are defined in VTP version 2:

- Token Ring Concentrator Relay Function (trCRF)—A trCRF is a logical grouping of ports. Each trCRF is contained in only one trBRF, which is referred to as its parent.
- Token Ring Bridge Relay Function (trBRF)—A trBRF is a logical grouping of trCRFs. The trBRF is used to join different trCRFs. In addition, the trBRF can be extended across a network of switches through high-speed uplinks between the switches to join trCRFs contained in different switches.

Figure 2-4 Token Ring VLANs



LAN Emulation (LANE) Configuration

LAN Emulation (LANE) enables existing applications to access an ATM network as if they were operating over traditional LANs, such as Ethernet or Token Ring. LANE allows LAN users to benefit from ATM without modifying end-system hardware or software. End-user hosts on LANs can connect to other end-user hosts on LANs, as well as to ATM-attached servers, routers, and switches.

LANE reconciles the differences between ATM and LAN protocols by masking the connection setup and handshaking functions required by the ATM switch. LANE basically bridges LAN traffic across ATM. LANE has specific hardware requirements. For details, refer to your switch or router documentation.

The following topics provide you with information about:

- LANE Components, page 2-23
- How LANE Works, page 2-25
- ATM LANE Configuration Guidelines, page 2-27

LANE Components

LANE is defined on a client-server LAN model, and the following LANE components must be configured for LANE services to be fully functional:

- LE Configuration Server (LECS)—Acts as the registration point for each emulated LAN within the ATM backbone.
- LE Server/Broadcast Server (LES)—Provides the broadcast and multicast forwarding functions.
- LE Clients (LECs)—Provides the connection points within the ATM backbone for each emulated Layer 2 logical network.

These LANE components and the requirements for using them in an ATM network are described in Table 2-4.

Table 2-4 LANE Component Descriptions



Component	Description	Requirements
LE Configuration Server (LECS)	Contains the database that determines to which master LECS an ATM-VLAN client belongs. Clients consult the LE configuration server to determine which ATM-VLAN it should join. The LECS returns the ATM address of the LES for that ATM-VLAN, and also maintains the LES redundancy information.	Cisco recommends having one master LECS per ATM domain. Campus Manager does not support more than one master LECS, but you can have additional backup LECSs.
Broadcast Server ¹ (BUS)	Sequences and distributes multicast and broadcast packets and handles unicast flooding.  Note Cisco's implementation combines the LE and Broadcast servers (LE/Broadcast servers); however, the functions remain separate.	Cisco recommends having one active master combined LE/Broadcast server per ATM-VLAN. You can have additional backup LE/Broadcast servers.

Table 2-4 LANE Component Descriptions (continued)

Component	Description	Requirements
LE Server (LES) ¹	<p>The LE server acts as the control center. Provides joining, address resolution, and address registration services to the LE clients in that ATM-VLAN. Clients can register destination unicast and multicast MAC addresses with the LE server. The LE server also handles LANE Address Resolution Protocol (LE_ARP) requests and responses.</p> <p>Clients can communicate directly with one another only when they are connected to the same LE server.</p> <p> Note Cisco's implementation combines the LE and Broadcast servers (LE/Broadcast servers); however, the functions remain separate.</p>	Cisco recommends having one active master combined LE/Broadcast server per ATM-VLAN. Multiple LE/Broadcast servers can exist on the same physical ATM network where each server supports a different ATM-VLAN. You can have additional backup LE/Broadcast servers.
LE Client (LEC)	The LE Client emulates a LAN interface to higher-layer protocols and applications. It forwards data to other LANE clients and performs LANE address-resolution functions.	Can be a member of only one ATM-VLAN. An ATM device can have several LE clients—one client for each ATM-VLAN of which it is a member.

1. In Cisco's implementation of LANE, the LE server and broadcast server are one entity. In this document, references to an LE server include the broadcast server.

How LANE Works

ATM is a connection-oriented service, while LAN is a broadcast medium. ATM uses connection-oriented service with point-to-point signaling or multipoint signaling between source and destination devices. LAN-based protocol suites use connectionless service and broadcasts to enable source devices to find one or more destination devices.

Using LANE, LAN broadcasts are emulated as ATM unicasts. LANE emulates a broadcast environment such as IEEE 802.3 Ethernet or 802.5 Token Ring on top of an ATM network that is a point-to-point environment. Client devices, such as routers, ATM workstations, and LAN switches use LES functions to emulate a LAN across ATM.

LANE defines a service interface for network layer protocols that is identical to existing MAC layers. No changes are required to existing upper layer protocols and applications. Data sent across the ATM network is encapsulated in the appropriate LAN MAC packets. LANE essentially bridges LAN traffic across ATM and defines the operation of an emulated LAN.

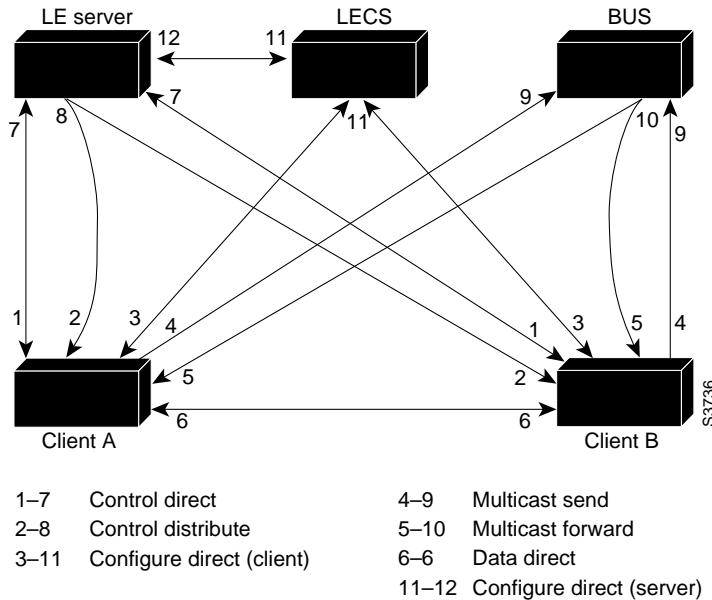
LANE does not emulate every particular physical or data-link characteristic. For example, it does not support carrier sense multiple access collision detect (CSMA/CD) for either Ethernet or Token Ring. LANE on the ATM switch router supports only the IP protocol.

LANE can be implemented on these devices:

- Directly attached ATM hosts
- Layer 2 devices, such as the Catalyst switches or ATM switch routers
- Layer 3 devices, such as routers

Communication among LANE components is ordinarily handled by several types of switched virtual channel circuits (VCCs). Some VCCs are unidirectional; others are bidirectional. Some are point-to-point; others are point-to-multipoint. (See Figure 2-5.)

Figure 2-5 LANE Virtual Circuit Types



The elements in Figure 2-5 function as follows:

- **Control direct VCC**—The LEC, as part of its initialization, sets up a bi-directional point-to-point VCC to the LES for sending or receiving control traffic. The LEC is required to accept control traffic from the LES through this VCC and must maintain the VCC while participating as a member of the emulated LAN.
- **Control distribute VCC**—The LES may optionally establish a unidirectional VCC back to the LEC for distributing control traffic. Whenever an LES cannot resolve a LAN Emulation Address Resolution Protocol (LE_ARP) request from an LEC, it forwards the request out the control distribute VCC to all of the clients in the LAN. The control distribute VCC enables information from the LES to be received whenever a new MAC address joins the LAN or whenever the LES cannot resolve an LE_ARP request.
- **Data direct VCC**—Once an ATM address has been resolved by a LEC, this bidirectional point-to-point VCC is set up between clients that exchange unicast data traffic. Most client traffic travels via these VCCs.

- Multicast send VCC—The LEC sets up a unidirectional point-to-point VCC to a multicast server. This VCC is used by the LEC to send multicast traffic to the BUS for forwarding out the multicast forward VCC. The LEC also sends out unicast data on this VCC until it resolves the ATM address of a destination.
- Multicast forward VCC—The BUS sets up a unidirectional VCC to the LECs for distributing data from the BUS. This can either be a unidirectional point-to-point or unidirectional point-to-multipoint VCC. Data sent by an LEC over the multicast send VCC is forwarded to all LECs via the multicast forward VCC.
- Configure direct VCC—This is a transient VCC that is established by the LEC to the LECS to obtain the LES ATM address which controls a particular LAN that the LEC must join.

ATM LANE Configuration Guidelines

Use these guidelines when configuring LANE:

- The LECS is always assigned to the major interface. Assigning any other component to the major interface is identical to assigning that component to the 0 subinterface.
- The LES/BUS and the LEC of the *same* ELAN can be configured on the same subinterface.
- LECs of two *different* ELANs cannot be configured on the same subinterface.
- The LES/BUS for *different* ELANs cannot be configured on the same subinterface.
- All ATM switches have identical lists of the global LECS addresses with the identical priorities.
- The operating LECSs must use exactly the same configuration database. Create and maintain a configuration file containing the LECS database and load it onto devices using the **config net** command. This method minimizes errors and allows you to maintain the database centrally.
- The LANE subsystem supports up to 16 LECS addresses.
- The number of LES/BUSs that can be defined per ELAN is unlimited.
- When a LECS switchover occurs, no previously joined clients are affected.

- In a LES/BUS switchover, there is a momentary loss of clients until all clients are transferred to the new LES/BUS.
- LECSs come up as masters automatically until a higher level LECS tells them otherwise.
- You can configure redundant LES/BUSs and LECSs to reduce the likelihood of a server failure resulting in loss of communication on the LANE network. With redundant LES/BUSs and LECSs, LANE components can switch to the backup LES/BUS or LECS automatically if the primary server fails.



Note LES/BUS/LECS redundancy works only with LECS and LES/BUS combinations on Cisco devices. Third-party LANE components interoperate with the LECS and LES/BUS functions of Cisco devices but cannot take advantage of the redundancy features.

- With multiple LES/BUSs configured for a single ELAN, the priority of a given LES/BUS is established by the order in which it was entered in the LECS database. When a higher priority LES/BUS comes online, it takes over the functions of the current LES/BUS on the ELAN. For a short time after a power on, some LECs might change from one LES/BUS to another, depending upon the order in which the LES/BUSs come online.
- If no specified LES/BUS is up or connected to the master LECS, and more than one LES/BUS is defined for an ELAN, the LECS rejects any configuration request for that specific ELAN.
- Changes made to the list of LECS addresses on ATM switches can take up to one minute to propagate through the network. Changes made to the configuration database regarding LES/BUS addresses take effect almost immediately.
- If no designated LECS is operational or reachable, the ATM Forum-defined *well-known* LECS address is used.

In the event of an ATM network failure, there can be multiple master LECs and multiple active LES/BUSs for the same ELAN, resulting in a partitioned network. Clients continue to operate normally, but transmission between different partitions of the network is not possible. The system recovers when the network break is repaired.

VTP Domains

Before using Topology Services to monitor the VLANs in your network, consider your VTP domain design.

A VTP domain is made up of one or more interconnected devices that share the same VTP domain name. A switch can be configured to be in only one VTP domain, and each VLAN has a name that is unique within a management domain.

Typically, you use a VTP domain to ease administrative control of your network or to account for physical boundaries within your network. However, you can set up as many or as few VTP domains as are appropriate for your administrative needs. Consider that VTP is transmitted on all trunk connections, including ISL, IEEE 802.1Q, 802.10, and LANE.

The following topics provide you with information about:

- Virtual Trunk Protocol (VTP), page 2-29
- Components of VTP Domains, page 2-30

Virtual Trunk Protocol (VTP)

Using Virtual Trunk Protocol (VTP), each switch in server mode advertises its management domain on its trunk ports, its configuration revision number, and its known VLANs and their specific parameters. Therefore, a new VLAN must be configured on only one device in the management domain, and the information is automatically learned by all the other devices (not in VTP transparent mode) in the same management domain. Once a device learns about a VLAN, it receives all frames on that VLAN from any trunk port and, if appropriate, forwards them to each of its other trunk ports.

Two versions of VTP are supported—VTP 1 and VTP 2. Every switch in the VTP domain must use the same VTP version. The VTP version is important if you use Campus Manager in a Token Ring environment because you must use version 2 with Token Ring devices. Verify the software image version of all of the devices in your network to make sure they support VTP 2.

Components of VTP Domains

Within a VTP domain, you can configure switches as follows:

- **Server**—VTP servers advertise their VLAN configuration to other switches in the same VTP domain and synchronize their VLAN configuration with other switches based on advertisements received over trunk links. VTP server is the default mode.
- **Client**—VTP clients operate the same way as VTP servers, but you cannot create, change, or delete VLANs on a VTP client. VTP clients also do not broadcast VTP advertisements like the VTP servers do.
- **Transparent**—VTP transparent switches do not participate in VTP. A VTP transparent switch does not advertise its VLAN configuration and does not synchronize its VLAN configuration based on received advertisements.

Your VTP domain structure influences the behavior of Topology Services. Use these guidelines to ensure that your network is set up correctly for Topology Services:

- One VTP Server—Multiple VTP Clients, page 2-30
- Multiple VTP Servers, page 2-30
- VTP Server—VTP Transparent, page 2-31
- VTP Not Transparent Only, page 2-31

One VTP Server—Multiple VTP Clients

In this scenario, at least one VTP server for each VTP domain is required. Cisco recommends that you configure the other devices as VTP clients, especially if you have a large network. Having only one VTP server maintains VLAN consistency across the network.

Multiple VTP Servers

For multiple VTP servers, consider that the device with the most recent configuration revision number controls VTP advertisements. The configuration revision number associated with a device's known set of VLANs (in one management domain). This revision number can be compared to another device's configuration revision number (for the same management domain) to determine

which is more recent. This revision number is incremented when a device is reconfigured to define a new VLAN, delete an existing VLAN, suspend or resume an existing VLAN, or modify the parameters of an existing VLAN.

If a network has two or more VTP servers that are not connected by Inter-Switch Link (ISL), the VLAN configuration on those servers may not be synchronized. In this case, Topology Services reads the VLAN information from the VTP server with the latest revision number. You must ensure that the most recent changes to VLANs are made on the VTP server with the highest configuration revision number.

VTP Server—VTP Transparent

To prevent your devices from participating in VTP, configure them as VTP transparent. When you create a VLAN on a VTP transparent switch, the VLAN is local to that switch, and is not known to other devices in the network.

Topology Services reads VLAN information from the VTP servers and transparent switches in your network. Topology Services attempts to correlate VLAN information between transparent switches and those known to the VTP Server. If a transparent switch is participating in a VLAN identical to the VLAN known to the VTP Server, the VLAN is shown belonging to each.

Provided that you have at least one VTP server in your network, you can create local VLANs on transparent switches. However, you lose a verifiable consolidated view of the VLAN states of your switches. A switch in transparent mode does not communicate its VLAN state to a server nor does it accept changes to its VLAN state from the server.

VTP Not Transparent Only

Even if you use Topology Services in a VTP domain that contains VTP transparent switches and no VTP servers, Topology Services will discover the VLANs in your network. You are not required to have a VTP Server in each VTP domain for Topology Services to discover VLANs.

ATM Domains

You can view and monitor ATM domain status, including standalone ELANs, in your network. You can also use the ATM Domain network views to obtain detail about devices in each ATM domain.

The ANI Server discovers the ATM switches and end hosts, and all physical and logical links among those switches and hosts. These components comprise the ATM domain.

An ATM domain is a group of interconnected ATM switches and ATM end-hosts that can be discovered with the Interim Local Management Interface (ILMI) neighbor discovery mechanism. Switches within the ATM network must support AToM MIB (RFC 1695).

ATM End host contains an ATM network interface adapter. Examples of ATM endpoints are workstations, routers, data service units (DSUs), LAN switches, and video coder-decoder (CODEC).

ATM switches:

1. Accept the incoming cell from an ATM endpoint or another ATM switch.
2. Read and update the cell header information.
3. Switch the cell to an output interface toward its destination.

ICS Devices

Integrated Communication System (ICS) devices provide a complete voice and data network solution. They have all the elements needed to deliver data, voice, and video in a single chassis. Refer to the documentation included with the ICS device for more information.

ICS device components are discovered as separate IP addresses, but are shown as one device icon in the network topology view.

See Table 2-3 on page 2-6 on how to access an ICS device from Topology Services.

Application Servers

Application servers are high-availability workflow systems that provide categories of service on a network, such as Cisco AVVID (architecture for Voice, Video and Integrated Data) services. For example, a Media Convergence Server (MCS) is an application server providing such AVVID-related applications as Cisco CallManager.

Cisco CallManager provides signaling and call control services to Cisco integrated multimedia applications as well as third-party applications. Cisco CallManager services can be distributed and clustered over an IP network, thereby allowing scale to 10,000 users and triple call-processing redundancy. The ANI Server component of CiscoWorks2000 discovers application servers and Topology Services displays them in the Layer 2 View.

**Note**

Topology Services cannot distinguish a Windows NT server from an application server running Cisco CallManager. Topology Services always displays a Windows NT server or a Media Convergence Server as an application server.

Troubleshooting Topology Services

Use the information in the following topics to help you troubleshoot Topology Services:

- Frequently Asked Questions, page 2-33
- Troubleshooting Suggestions, page 2-36

Frequently Asked Questions

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

- Does VTP need to be enabled?, page 2-34
- If there are multiple VTP servers in a VTP domain, which VTP server receives VLAN configuration changes?, page 2-34

- Can VLANs in a VTP server domain have the same name as a VLAN on a VTP transparent switch?, page 2-35
- Can you move ports from a transparent switch into a VLAN in the parent VTP domain?, page 2-35
- Will Topology Services display VLAN information for a switch that is in VTP transparent mode?, page 2-35
- In the LAN edge network view, how can I tell which switches in a switch cloud are connected to a router?, page 2-35
- Why is there is no information about the LE Config Server in the summary of an ATM-VLAN?, page 2-36
- Why does a Windows NT server appear as an application server?, page 2-36

Does VTP need to be enabled?

Topology Services requires Virtual Trunk Protocol (VTP) to be enabled in order to create VLANs. For most predictable results, Cisco recommends having at least one switch configured as a VTP server and the remaining switches configured as VTP clients.

If there are multiple VTP servers in a VTP domain, which VTP server receives VLAN configuration changes?

If the two VTP servers are in the same domain and are connected by VTP trunks, it does not matter which switch the changes are made on. VTP ensures that the information on all VTP servers and clients in a single VTP domain are coordinated and share the same configuration.

If the servers are in different VTP domains, then they do not share VLAN states, but they are both known to Topology Services. You must select the VTP domain in which you want to make the VLAN changes, and the corresponding VTP servers will reflect those changes.

If there are two servers with the same VTP domain that are not connected by trunks the configurations managed by the two servers may diverge. This configuration is not supported by Topology Services, and is reported as a discrepancy.

Can VLANs in a VTP server domain have the same name as a VLAN on a VTP transparent switch?

You can have VLANs with the same name provided that other characteristics, such as VLAN index and SAID value, are also identical. Discrepancies occur when there are identically named VLANs with other attributes that are different (such as index, and so on). Topology Services does not consider it a discrepancy if two VLANs share identical definitions.

It is usually best to use the default names that Topology Services creates for each VLAN.

Can you move ports from a transparent switch into a VLAN in the parent VTP domain?

Yes, but you must first create the VLAN (with identical attributes) on the transparent switch. To create a VLAN that exists on both the VTP server and all the transparent switches in a VTP domain, you can select the **Create VLAN on all Transparent Switches** check box when creating the VLAN.

Will Topology Services display VLAN information for a switch that is in VTP transparent mode?

Topology Services will attempt to correlate information from VTP transparent switches with VTP servers in the same domain. It will check the ISL index, VLAN name, and VLAN type for each VLAN, if the VLANs are identical, then they will be displayed

In the LAN edge network view, how can I tell which switches in a switch cloud are connected to a router?

The **Aggregate Link Attributes** option is available when you right-click on a link in the LAN Edge network view. The Aggregate Link Attributes window shows the list of links between a switch cloud and a router. This cannot be indicated in the view itself because individual links are not shown, there can be more than one link between a router and the devices in a switch cloud.

Why is there is no information about the LE Config Server in the summary of an ATM-VLAN?

LE Config Servers do not belong to a specific ATM-VLAN. Different LANE components could be going to different LE Config Servers (based on neighboring LS1010 registry information) to join the same ATM-VLAN.

Why does a Windows NT server appear as an application server?

If a Windows NT server is used as a seed device for ANI Server discovery, it will appear in Topology Services as an application server. Because an application server is installed on Windows NT, Topology Services discovers both of these device types as one device.



Note

It is not recommended to use an end-station as a seed device. See ANI online help for more information about choosing a seed device.

Troubleshooting Suggestions

Use the information in the Troubleshooting Topology Services table to troubleshoot the Topology Services application.

Table 2-5 *Troubleshooting Topology Services*

Symptom	Probable Cause	Possible Solution
Links that appeared correctly earlier now show as dashed lines.	If you move a port, ANI cannot determine by looking at the CDP cache if a link has been removed or the link is inactive. It marks the link notInNetwork instead of removing it.	If you have changed the port for this link, and the link should no longer appear, delete the link. At the next discovery, it should no longer appear.
After initial discovery, not all of the devices are discovered, and many devices are unreachable.	If devices are not discovered by Topology Services, it is likely that community strings are not entered correctly in the ANI Server.	Check the community strings on the devices and in the ANI Server Admin application. Then verify that the devices appear in the network view.

Table 2-5 Troubleshooting Topology Services (continued)

Symptom	Probable Cause	Possible Solution
Topology Services will not start. When attempts are made to start Topology Services, an error message states that Topology Services is already running.	If you close the windows that appear when the application is loading, and then try to restart the application, you will receive this error.	Wait for a reasonable amount of time, and then attempt to start the application. Do not close the message windows that appear when the application is loading
After creating an ATM-VLAN, it does not appear in the summary information for the VLAN with which it was associated.	After creating a new LE Broadcast Server, an entry for a standalone ATM-VLAN will immediately appear in the Standalone ATM-VLANs folder inside the appropriate ATM domain in the ATM Domains folder.	In order to see the appropriate hybrid ATM-VLAN entry for the VLAN (under the appropriate VTP domain) for which the LE Broadcast Server was created, you must first create a LAN Emulation Client for the new ATM-VLAN and rediscover your network.
An unknown device type appears under the network view filters. For example: 1.3.6.14.1.326.2.2.(7)	This string is the raw SNMP OID from the device. This will occur when the ANI Server discovers a non-Cisco device. This is a device that is responding to SNMP but is from another vendor. The number in parentheses indicates the number of these devices that appear in the network view.	To determine the vendor for a non-Cisco device, refer to the following URL: http://www.isi.edu/in-notes/iana/assignments/enterprise-numbers

