CIT

Cisco Internetwork Troublshooting

Version 5.1

Student Guide

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the Cisco Web site at www.cisco.com/go/offices.

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan • Thailand • Turkey Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Table of Contents

Module 1

Establishing a Baseline

Overview

Some of the biggest challenges facing the information technology (IT) world are the expenses that are incurred as a result of network outages. The negative impact of these expenses should make it a high priority of network professionals to be able to diagnose and correct a network problem as efficiently as possible. To help accomplish this, a baseline should be established to provide a snapshot of the configuration of a network while it is performing at an acceptable level. Using baseline information as a standard reduces the time that troubleshooters need to spend learning about the structure and configuration of a network and helps them know when they have reached the goal of returning the network to its baseline operation. Without a baseline, troubleshooters are left with having to make guesses and estimates about whether they have reached their goal, and their efforts will most likely occur in a haphazard and inefficient manner.

Module Objectives

Upon completing this module, you will be able to:

- Create a network configuration table and topology diagram
- Create an end-system configuration table and end-to-end topology diagram

Module Outline

The module contains these components:

- Creating Network Configuration Documentation
- Creating End-System Network Configuration Documentation

Creating Network Configuration Documentation

Overview

When troubleshooting a network, a troubleshooter uses a baseline to efficiently diagnose and correct network problems. The baseline information for a network is captured on documentation such as network configuration tables and topology diagrams. This lesson discusses the creation of relevant and accurate network documentation as a troubleshooting tool for returning a suboptimal or failing network back to an acceptable condition. The information contained in this lesson assumes a worst-case scenario in which you are almost completely unfamiliar with a network and need to create documentation from scratch.

Relevance

Useful network documentation will make you a more effective troubleshooter by saving you time and effort. When the configuration of your network is failing or performing suboptimally, a network configuration table will provide you with a saved configuration that should perform at an acceptable level. Network documentation will also prevent you from performing the time-consuming and error-prone process of creating a network configuration from scratch.

Objectives

Upon completing this lesson, you will be able to:

- Identify the components of a network configuration table
- Identify the components of a topology diagram
- Discover network configuration information
- Describe the process of creating network documentation
- Create network documentation

Learner Skills and Knowledge

To benefit fully from this lesson, you must have these prerequisite skills and knowledge:

- Advanced knowledge of IP addressing and routing concepts
- Advanced understanding of network topologies
- Advanced knowledge of Cisco IOS command syntax

The skills and knowledge can be based on experience, but should be equivalent to topics covered in the *Building Scalable Cisco Internetworks* (BSCI), *Building Cisco Multilayer Switched Networks* (BCMSN), and *Building Cisco Remote Access Networks* (BCRAN) courses.

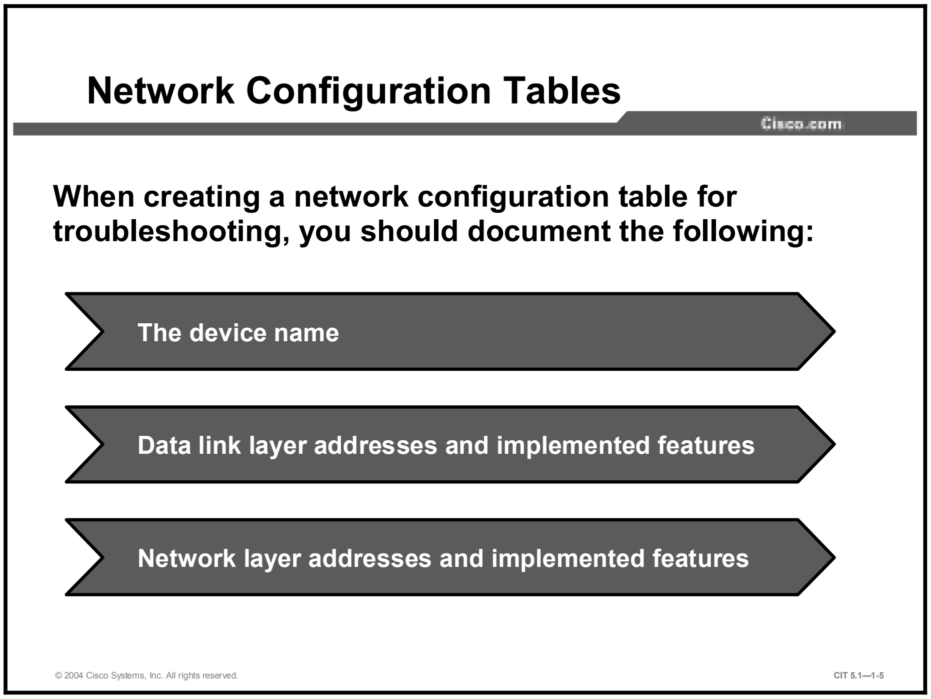
Outline

This lesson includes these topics:

- Overview
- Identifying the Components of a Network Configuration Table
- Identifying the Components of a Topology Diagram
- Discovering Network Configuration Information
- Describing the Process of Creating Network Documentation
- Creating Network Documentation
- Summary
- Quiz

Identifying the Components of a Network Configuration Table

This topic identifies the components that troubleshooters should include in a network configuration table created for the purpose of troubleshooting a network.



Network Configuration Tables

Cisco.com

When creating a network configuration table for troubleshooting, you should document the following:

- The device name
- Data link layer addresses and implemented features
- Network layer addresses and implemented features

© 2004 Cisco Systems, Inc. All rights reserved.

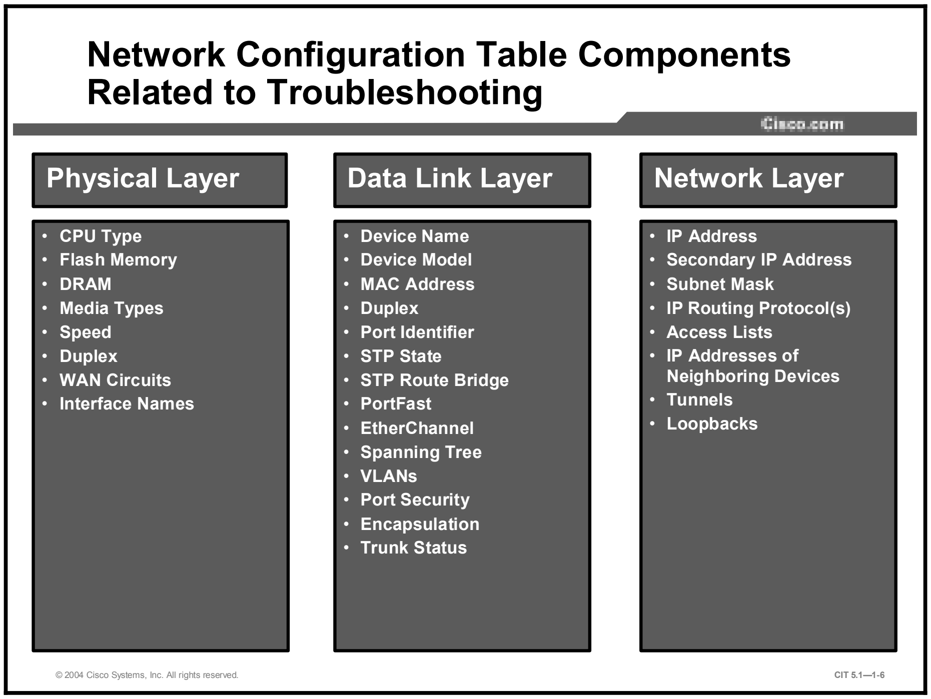
CIT 5.1—1-5

A network configuration table shows accurate records of the hardware and software used in a network. The components of a network configuration table are the different types of data that will comprehensively document the hardware and software components of a network.

When creating a network configuration table for troubleshooting, you should document the following:

- The device name
- Data link layer addresses and implemented features
- Network layer addresses and implemented features
- Any important information about the physical aspects of the device

Note The decision of what specific components to include on network documentation should be made by someone who has knowledge of the network being documented and has some previous experience troubleshooting that network.



Network Configuration Table Components Related to Troubleshooting

Physical Layer

- CPU Type
- Flash Memory
- DRAM
- Media Types
- Speed
- Duplex
- WAN Circuits
- Interface Names

Data Link Layer

- Device Name
- Device Model
- MAC Address
- Duplex
- Port Identifier
- STP State
- STP Route Bridge
- PortFast
- EtherChannel
- Spanning Tree
- VLANs
- Port Security
- Encapsulation
- Trunk Status

Network Layer

- IP Address
- Secondary IP Address
- Subnet Mask
- IP Routing Protocol(s)
- Access Lists
- IP Addresses of Neighboring Devices
- Tunnels
- Loopbacks

CIT 5.1—1-6

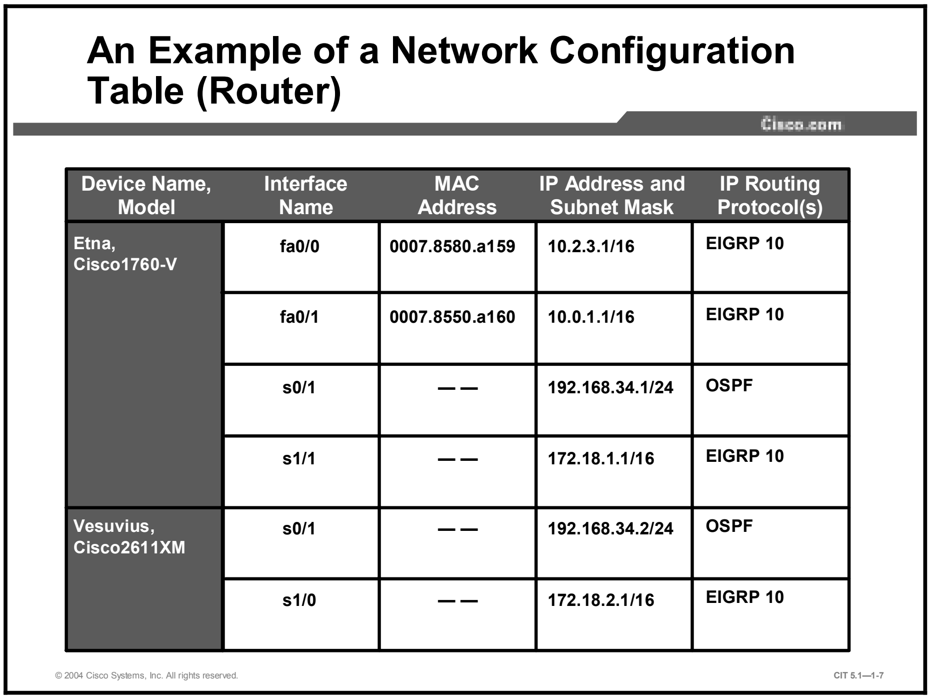
Because of the complex nature of most networks, there is a great deal of information that you could possibly record. To simplify things, troubleshooters can separate the components of a network configuration table related to troubleshooting into categories based on their relationship to the layers of the commonly referenced TCP/IP networking model.

Network documentation can vary, depending on the purpose of the documentation and the types of devices that are being documented. A comprehensive configuration table constructed for the purpose of troubleshooting will contain different components than one that is constructed for budgetary tracking or maintenance purposes. Some data components, such as speed, are not useful for a device, such as a router; however, these components are crucial pieces of information to record for a switch. A multilayered switch would require components pertaining to both routers and switches. Because similar types of information are contained within each device, it would be possible to combine network configuration tables for routers and switches; however, it usually makes sense to use separate tables.

Components will also vary depending on the features implemented on the devices. The Router ID (RID) number would be an important piece of information to record about a router running Open Shortest Path First (OSPF). However, if you were running only Enhanced Interior Gateway Routing Protocol (EIGRP), you would not document the RID number.

Example: Router Network Configuration Table

This example of a network configuration table contains information that can be used to describe a router.



An Example of a Network Configuration Table (Router)

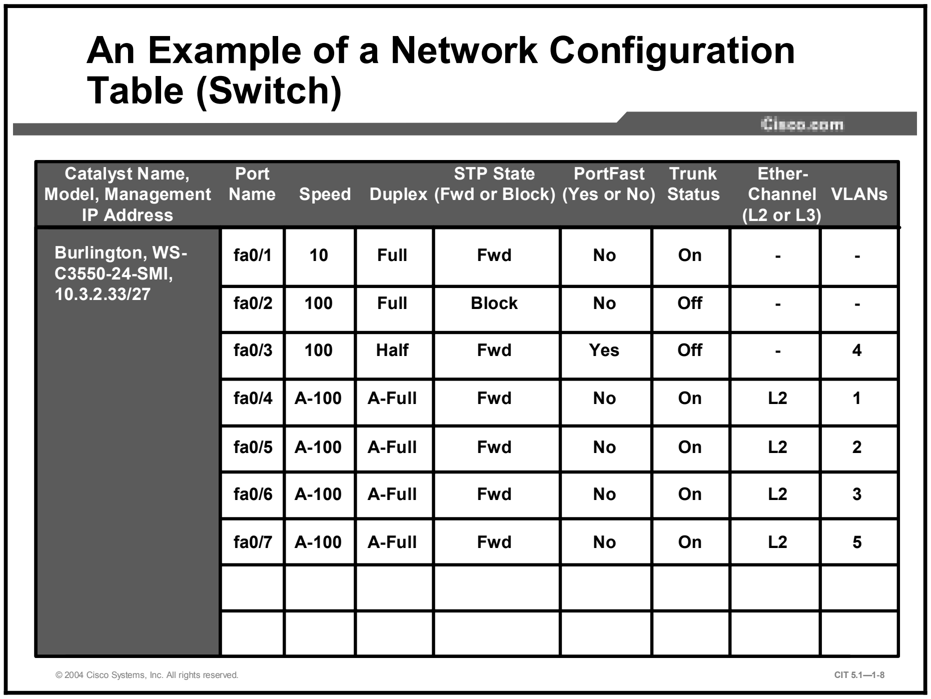
Device Name, Model	Interface Name	MAC Address	IP Address and Subnet Mask	IP Routing Protocol(s)
Etna, Cisco1760-V	fa0/0	0007.8580.a159	10.2.3.1/16	EIGRP 10
	fa0/1	0007.8550.a160	10.0.1.1/16	EIGRP 10
	s0/1	— —	192.168.34.1/24	OSPF
	s1/1	— —	172.18.1.1/16	EIGRP 10
Vesuvius, Cisco2611XM	s0/1	— —	192.168.34.2/24	OSPF
	s1/0	— —	172.18.2.1/16	EIGRP 10

CIT 5.1—1-7

In this example, the following categories are used to document the properties of the devices:

- Device name, model
- Interface name
- MAC address
- IP address and subnet mask
- IP routing protocol(s)

This is an example of a network configuration table that would be used to document the characteristics of a standard switch.



An Example of a Network Configuration Table (Switch)

Catalyst Name, Model, Management IP Address	Port Name	Speed	Duplex	STP State (Fwd or Block)	PortFast (Yes or No)	Trunk Status	Ether-Channel (L2 or L3)	VLANs
Burlington, WS-C3550-24-SMI, 10.3.2.33/27	fa0/1	10	Full	Fwd	No	On	-	-
	fa0/2	100	Full	Block	No	Off	-	-
	fa0/3	100	Half	Fwd	Yes	Off	-	4
	fa0/4	A-100	A-Full	Fwd	No	On	L2	1
	fa0/5	A-100	A-Full	Fwd	No	On	L2	2
	fa0/6	A-100	A-Full	Fwd	No	On	L2	3
	fa0/7	A-100	A-Full	Fwd	No	On	L2	5

CIT 5.1—1-8

In this example, the following categories have been used to document the properties of the switch:

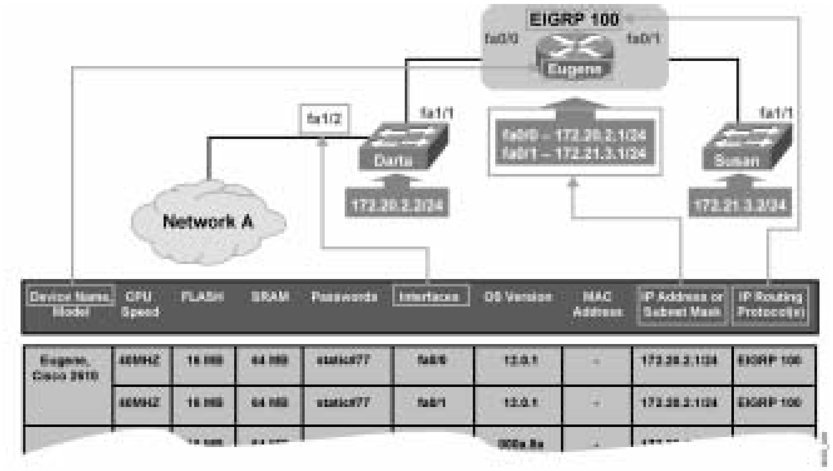
- Device name and model
- Management IP address
- Port name
- Speed
- Duplex
- STP state
- PortFast
- Trunk status
- EtherChannel
- VLANs

Identifying the Components of a Topology Diagram

This topic identifies the components that make up a network topology diagram.

The Components of a Network Topology Diagram

Cisco.com



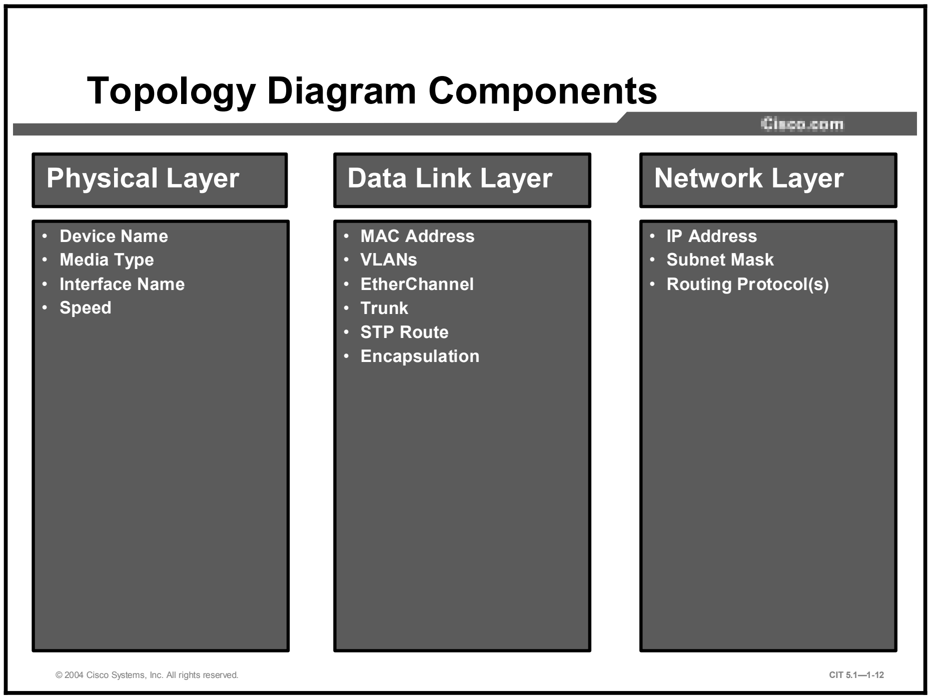
Device Name, Model	CPU Speed	FLASH	SRAM	Passwords	Interfaces	OS Version	MAC Address	IP Address or Subnet Mask	IP Routing Protocol(s)
Eugene, Cisco 2610	40MHZ	16 MB	64 MB	static#77	fa0/0	12.0.1	-	172.20.2.1/24	EIGRP 100
	40MHZ	16 MB	64 MB	static#77	fa0/1	12.0.1	-	172.20.2.1/24	EIGRP 100
		16 MB	64 MB			000a.8a	-	172.2	

CIT 5.1—1-11

A topology diagram is a graphical representation of a network. The topology diagram illustrates how each device in a network is connected, while also detailing the aspects of its logical architecture. Topology diagrams share many of the same components as their network configuration table counterparts.

Each network device should be represented on the diagram with consistent notation or a graphical symbol, and each logical and physical connection should be represented using a simple line or some other appropriate symbol. At a minimum, most topology diagrams include illustrations of all devices and how those devices are connected.

Many topologies also include network cloud symbols. A labeled cloud symbol is often employed to represent entities that are either outside of the autonomous control of your network or outside the scope of the topology diagram. Put simply, labeled cloud symbols are placeholders signifying that a network, or collection of networks, exists; however, knowing anything about those networks other than their existence is not particularly relevant to the diagram.



Topology Diagram Components

Cisco.com

Physical Layer

- Device Name
- Media Type
- Interface Name
- Speed

Data Link Layer

- MAC Address
- VLANs
- EtherChannel
- Trunk
- STP Route
- Encapsulation

Network Layer

- IP Address
- Subnet Mask
- Routing Protocol(s)

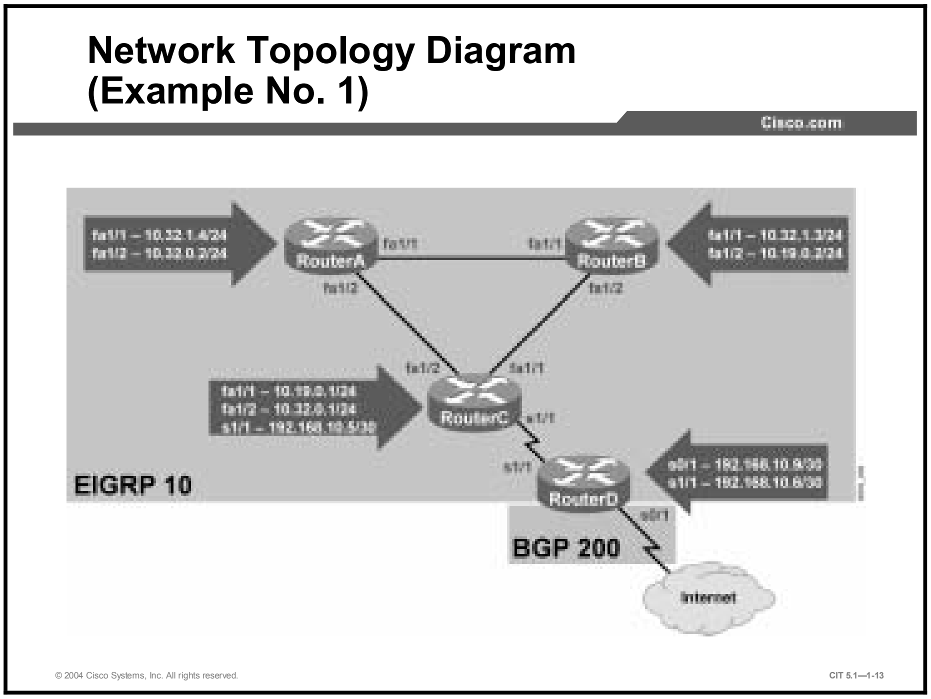
CIT 5.1—1-12

Although the components of a topology diagram can be restricted to a particular layer of the TCP/IP model, most often they are a combination of the most important components of several logical layers. To illustrate the important components of a network at the Internet TCP/IP layer, you might include IP addresses, subnet masks, and routing protocols.

Some topologies are informal hand-drawn sketches, while others are more elaborate, using detailed symbols, multiple colors, and different ways to view them. The latter are typically created using graphics applications that vary in functionality. While some applications can be used as a solution to manually create a network diagram, others can automatically create and maintain a topology of an existing network.

Example: Network Topology Diagram

This is an example of a topology diagram.



Network Topology Diagram (Example No. 1)

Cisco.com

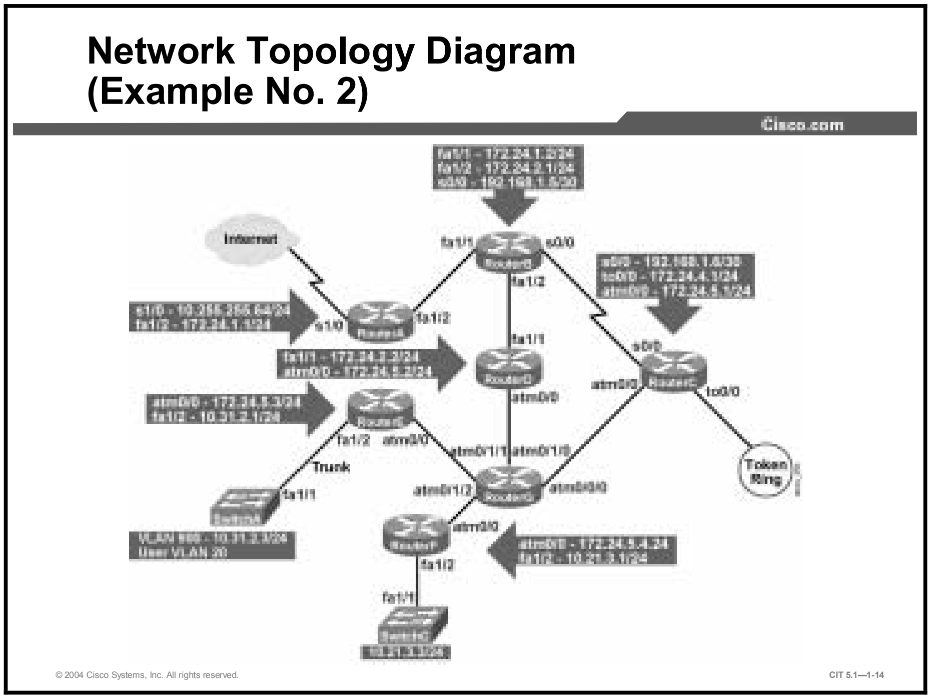
© 2004 Cisco Systems, Inc. All rights reserved.

CIT 5.1—1-13

This topology diagram includes the following components:

- Device name
- Interface or port name
- IP address
- Routing protocol(s)

This is a second example of a topology diagram.



Network Topology Diagram (Example No. 2)

Cisco.com

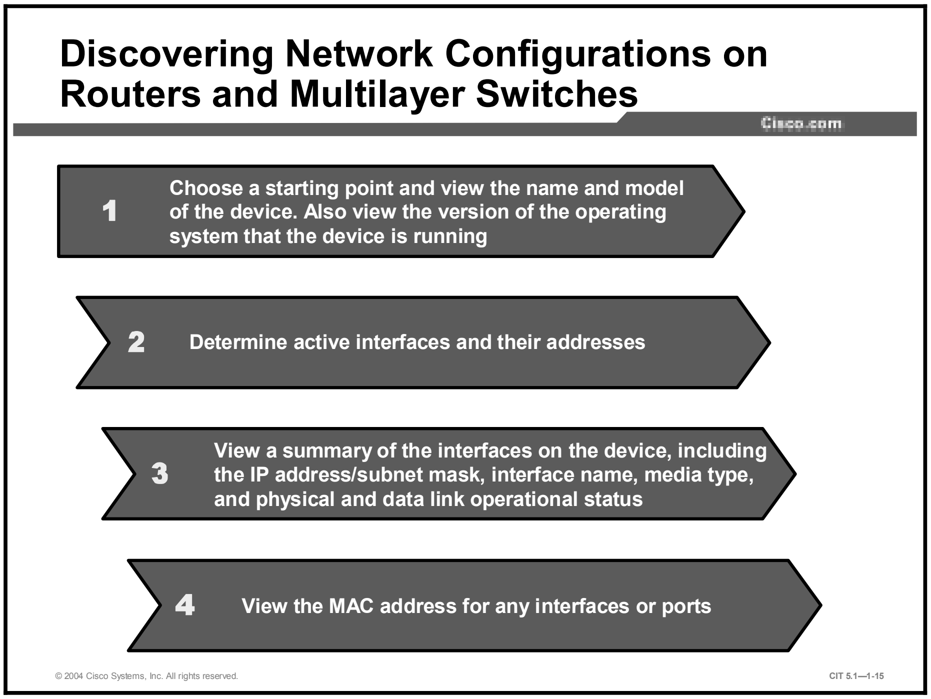
CIT 5.1—1-14

This example shows the following components of a network topology diagram:

- Device name
- Interface or port name
- IP address
- VLANs
- Trunks

Discovering Network Configuration Information

This topic describes the procedure for discovering network configuration information.



Discovering Network Configurations on Routers and Multilayer Switches

Cisco.com

1 Choose a starting point and view the name and model of the device. Also view the version of the operating system that the device is running

2 Determine active interfaces and their addresses

3 View a summary of the interfaces on the device, including the IP address/subnet mask, interface name, media type, and physical and data link operational status

4 View the MAC address for any interfaces or ports

© 2004 Cisco Systems, Inc. All rights reserved.

CIT 5.1—1-15

Procedure: Discovering Network Configuration of a Router

The following steps outline the procedure for discovering the network configuration of a router or multilayer switch:

Step 1 Choose a starting point and view the name and model of the device. Also view the version of the operating system that the device is running.

- Enter **show version**.

Step 2 Determine active interfaces and their addresses.

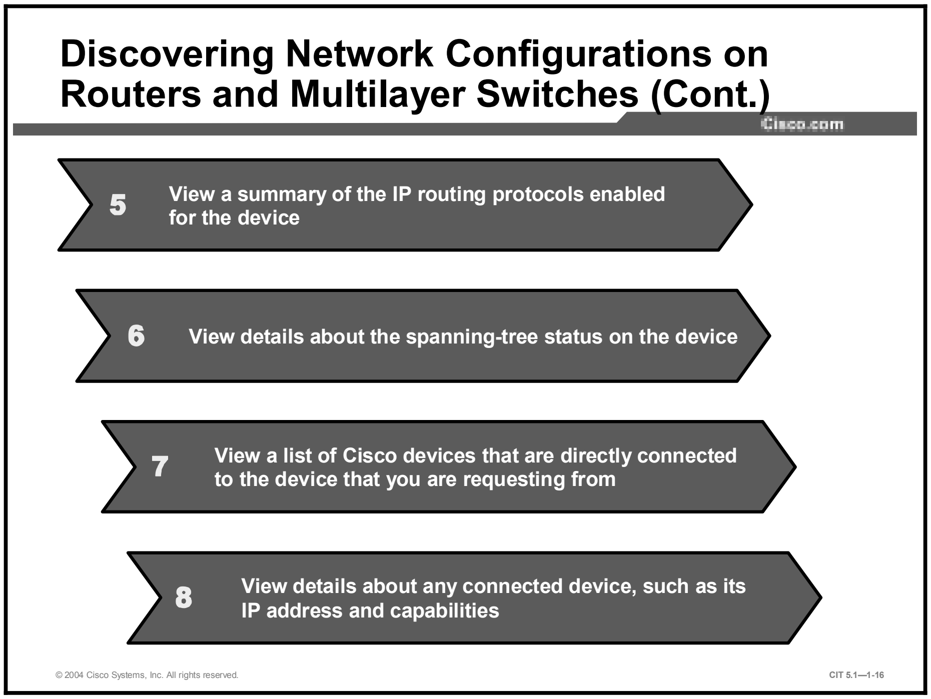
- Enter **show ip interfaces**.

Step 3 View a summary of the interfaces on the device, including the IP address or subnet mask, interface name, media type, and physical and data link operational status.

- Enter **show ip interfaces brief**.

Step 4 View the MAC address for any interfaces or ports.

- Enter **show interface** {*interface-name*} for each interface or enter **show interfaces** to see a list of all interfaces at once.



Discovering Network Configurations on Routers and Multilayer Switches (Cont.)

5 View a summary of the IP routing protocols enabled for the device

6 View details about the spanning-tree status on the device

7 View a list of Cisco devices that are directly connected to the device that you are requesting from

8 View details about any connected device, such as its IP address and capabilities

CIT 5.1—1-16

Step 5 View a summary of the IP routing protocols enabled for the device.

- Enter **show ip protocols**.

Step 6 View details about the spanning-tree status on the device.

- Enter **show spanning-tree summary**
  or **show spanning-tree vlan** {*vlan-number*}.

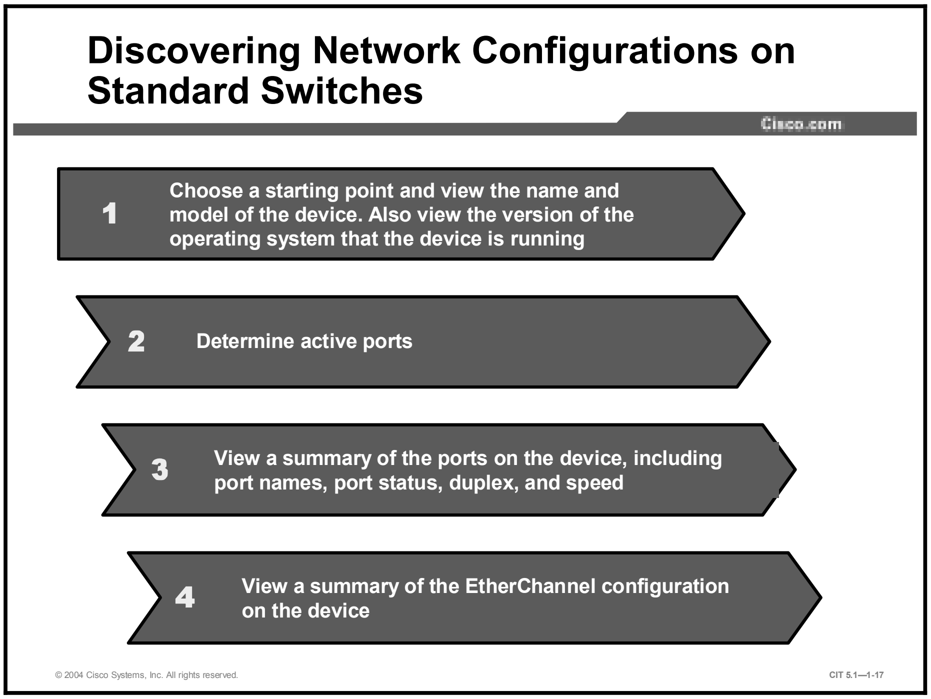
Step 7 View a list of Cisco devices that are directly connected to the device that you are requesting from.

- Enter **show cdp neighbors [detail]** or, if cdp is disabled, enter **ping**.

Step 8 View details about any connected device, such as its IP address and capabilities.

- Enter **show cdp entry** {*device id*}**, show ip eigrp neighbors,** or **show ip ospf neighbor**.

Note If CDP is disabled, you may want to enable CDP temporarily to make it easier to discover information about neighboring devices. However, enabling CDP on your devices does not guarantee that the neighboring devices will have CDP enabled.



Discovering Network Configurations on Standard Switches

Cisco.com

1 Choose a starting point and view the name and model of the device. Also view the version of the operating system that the device is running

2 Determine active ports

3 View a summary of the ports on the device, including port names, port status, duplex, and speed

4 View a summary of the EtherChannel configuration on the device

CIT 5.1—1-17

Procedure: Discovering Network Configuration of a Standard Switch

The following steps outline the procedure for discovering the network configuration of a standard switch:

Step 1 Choose a starting point and view the name and model of the device. Also view the version of the operating system that the device is running.

- Enter **show version**.

Step 2 Determine active ports.

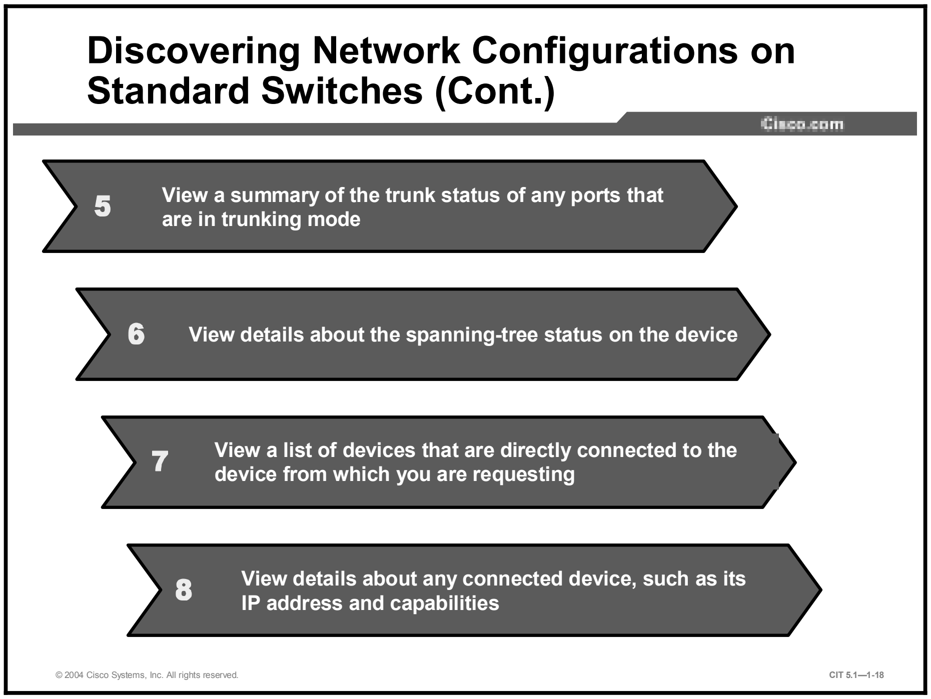
- Enter **show interfaces description**.

Step 3 View a summary of the ports on the device, including port names, port status, duplex, and speed.

- Enter **show interfaces status**.

Step 4 View a summary of the EtherChannel configuration on the device.

- Enter **show etherchannel summary**.



Discovering Network Configurations on Standard Switches (Cont.)

5 View a summary of the trunk status of any ports that are in trunking mode

6 View details about the spanning-tree status on the device

7 View a list of devices that are directly connected to the device from which you are requesting

8 View details about any connected device, such as its IP address and capabilities

CIT 5.1—1-18

Step 5 View a summary of the trunk status of any ports that are in trunking mode.

- Enter **show interfaces trunk**.

Step 6 View details about the spanning-tree status on the device.

- Depending on the IOS version, enter either **show spanning-tree** or **show spantree**.

Step 7 View a list of devices that are directly connected to the device from which you are requesting.

- Enter **show cdp neighbors** or, if CDP is disabled, enter **ping**.

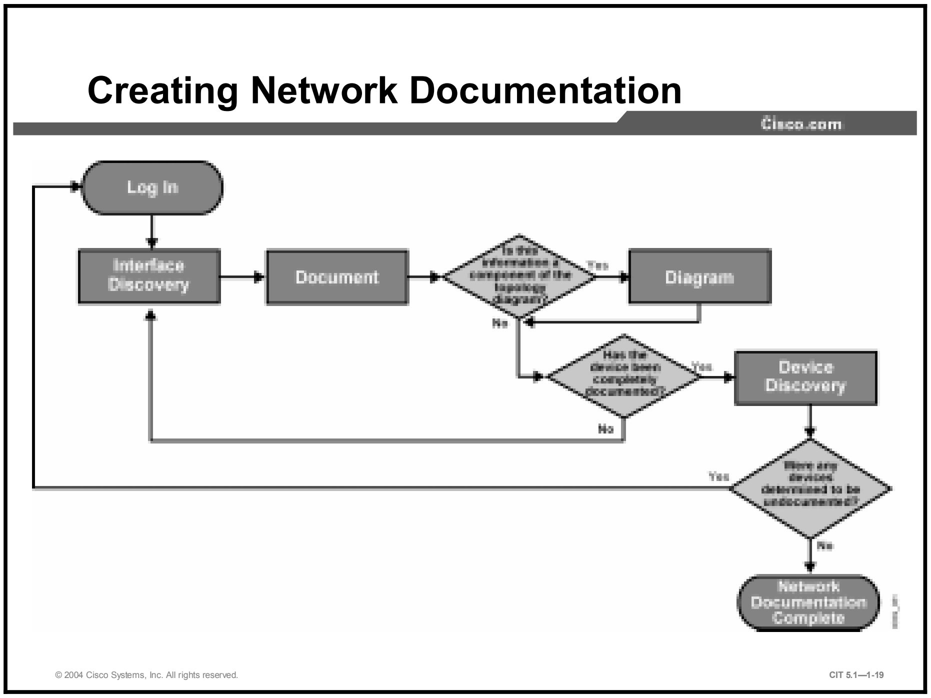
Step 8 View details about any connected device, such as its IP address and capabilities.

- Enter **show cdp entry** {*entry name*} or, if cdp is disabled, enter **show mac-address table**.

Note You can get all of this information by entering the **show tech-support** command, but be aware that the output from this command will give you a lot more information than you actually need.

Describing the Process of Creating Network Documentation

This topic describes the process of creating network documentation.



Creating Network Documentation

Cisco.com

Log In
Interface Discovery
Document
Is this information a component of the topology diagram?
Yes
No
Diagram
Has the device been completely documented?
Yes
No
Device Discovery
Were any devices determined to be undocumented?
Yes
No
Network Documentation Complete

© 2004 Cisco Systems, Inc. All rights reserved.

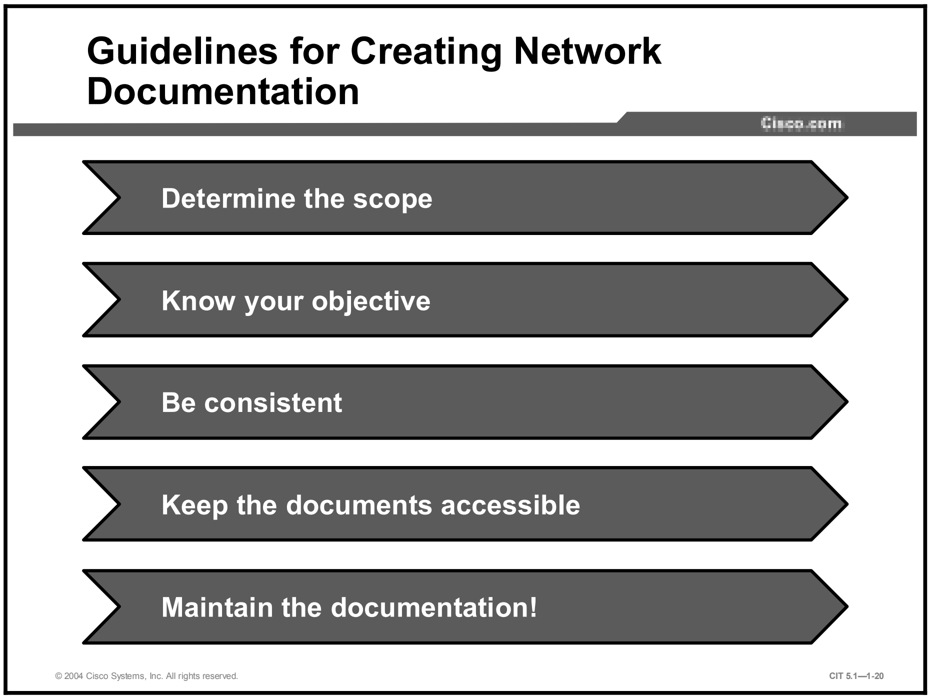
CIT 5.1—1-19

Stage	Description
Stage 1: Log In	To start, log in to a device. If you are already in the middle of the process, log in to an undocumented neighboring device.
Stage 2: Interface Discovery	Discover relevant information about the device. Relevant information is determined by the components of your network configuration table.
Stage 3: Document	Document the information that you discover about the device on the network configuration table. If the information that you document is also a component of the topology diagram, proceed to Stage 4. If all of the relevant information about the device has been documented, skip Stage 4 and move on to Stage 5.
Stage 4: Diagram	Transfer any information about the device from the network configuration table that corresponds with the components of your topology diagram. Once the information has been transferred, if all relevant information about the device has been documented, move on to Stage 5. Otherwise, return to Stage 2.
Stage 5: Device Discovery	Determine if any devices that neighbor the device to which you are logged into are undocumented. If you determine that new neighboring devices exist, return to Stage 1. Otherwise, if there are no new neighboring devices, the network documentation is complete.

Note The process recommends that the network configuration table and topology diagram be created in concert. However, it may benefit you to create one type of document first depending on your specific needs and the amount of documentation that is already available.

Creating Network Documentation

This topic supplies guidelines for creating network documentation.



Guidelines for Creating Network Documentation

Cisco.com

- Determine the scope
- Know your objective
- Be consistent
- Keep the documents accessible
- Maintain the documentation!

© 2004 Cisco Systems, Inc. All rights reserved. CIT 5.1—1-20

Good network configuration documentation allows you to quickly learn specific information about network devices.

Guidelines for creating effective network documentation are as follows:

- **Determine the scope:** To determine the scope of your network documentation, it is important to know which network devices are included in your domain of responsibility.
- **Know your objective:** Only collect data that is relevant to your objective and provide sufficient detail for those relative pieces. Extra layers of information will only make the documentation more difficult to use.
- **Be consistent:** Use consistent terminology, abbreviations, and style. Try to make the documents orderly and easy to understand. When possible, use templates and keep a library of symbols and graphic icons that you can re-use.
- **Keep the documents accessible:** Store the network documentation in a location where it is readily available on the job. It is also suggested that a copy of the documentation be kept in a secure location offsite.
- **Maintain the documentation:** Modify your network documentation as conditions and devices in the network change. *This is especially important.*

Note You may want to implement a process for handling changes to the network documentation. Factors in this process that need to be accounted for are reporting network changes, maintaining version control, and assigning responsibility for modifying and distributing updated documents.

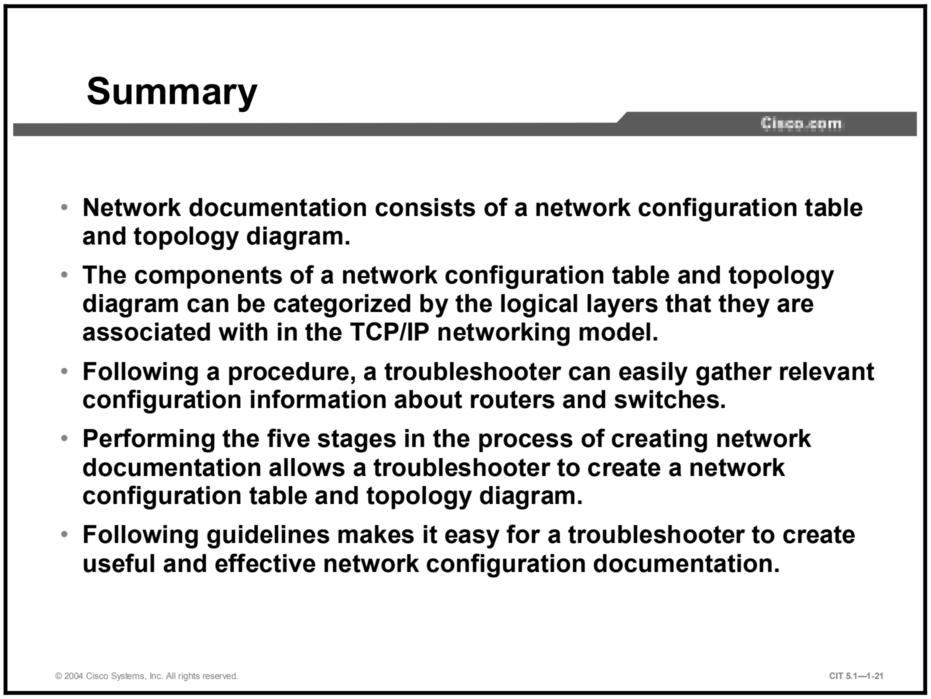
Example: Creating Successful Network Documentation

Last year, you were handed the task of documenting the network for your branch of the corporation. You completed this task on time and with compliments from your boss. One year later, troubleshooters still use the network documentation to successfully troubleshoot network problems. The following is a list of reasons why your documentation was a success:

- You asked questions to find out exactly which network segments and devices were in your domain of responsibility.
- You inquired about why the documentation was being created and what its uses would be. You then queried two of the most experienced network employees to learn which information would be most useful to meet those needs. As a result, you knew exactly what information to record and did not waste any time with unnecessary research.
- You used a consistent symbology and terminology to represent the data in both graphical and tabular form.
- You designated logical locations to store copies of the documentation and posted signage at those locations so that the networking employees could easily find them. You also employed a sign-out sheet so that the copies of the network documentation could be accounted for.
- You implemented a reporting and system so that employees could relay information about changing conditions in the network to a central location. When a change in network conditions took place, employees knew whom to notify and that person promptly modified, dated, and distributed the updated versions to the designated locations.

Summary

This topic summarizes the key points discussed in this lesson.



Summary

- Network documentation consists of a network configuration table and topology diagram.
- The components of a network configuration table and topology diagram can be categorized by the logical layers that they are associated with in the TCP/IP networking model.
- Following a procedure, a troubleshooter can easily gather relevant configuration information about routers and switches.
- Performing the five stages in the process of creating network documentation allows a troubleshooter to create a network configuration table and topology diagram.
- Following guidelines makes it easy for a troubleshooter to create useful and effective network configuration documentation.

CIT 5.1—1-21

References

For additional information, refer to these resources:

- http://www.cisco.com
- Cisco IOS command reference guides

Next Steps

For the associated lab exercise, refer to the following section of the course Lab Guide:

- Lab Exercise 1-1: Network Baseline Discovery

Quiz

Use the practice items here to review what you have learned in this lesson. The correct answers are found in the Quiz Answer Key.

Q1) Which list only includes components of a network configuration table?

A) IP address, controller event, multipoint DLCI, map statement, interface name

B) bridge-zone, OSPF area, checksum, router ID, subnet mask

C) device name, interface name, MAC address, duplex, access lists

D) IP address, subnet mask, checksum, bytes, data flow status

Q2) At a minimum, a network topology diagram will include which components? (Choose two.)

A) devices

B) contact information

C) module firmware loaded

D) connections between devices

E) interface spanning-tree configuration

Q3) Which IOS command would you use to view a list of devices that are directly connected to the device from which you are making the request?

A) **show ip interfaces**

B) **show spanning-tree**

C) **show cdp neighbors**

D) **show connected devices**

Q4) What should be the first step when performing a network discovery?

A) determine active interfaces

B) choose a starting point

C) view interface summaries

D) view summary of IP routing protocols

Q5) Which are guidelines for creating useful network configuration documentation? (Choose three.)

A) use consistent symbols, terminology, and styles

B) know the scope of the documentation

C) update the documentation exactly once a year

D) store the documents in a logical location

E) gather all possible information

Quiz Answer Key

Q1) C

Relates to: Identifying the Components of a Network Configuration Table

Q2) A, D

Relates to: Identifying the Components of a Topology Diagram

Q3) C

Relates to: Discovering Network Configuration Information

Q4) B

Relates to: Describing the Process of Creating Network Documentation

Q5) A, B, D

Relates to: Creating Network Documentation

Creating End-System Network Configuration Documentation

Overview

Network documentation can be a valuable tool for troubleshooting. However, a network is not complete without end systems, and a misconfigured end system can have a negative impact on the overall performance of a network. This lesson discusses the creation of configuration documentation for the purposes of troubleshooting end systems connected to a network. The information contained in this lesson assumes a scenario in which network devices have already been documented and you are unfamiliar with the configuration. Therefore, you will need to create the end-system portion of the network documentation from scratch.

Relevance

End-system devices, such as servers, network management consoles, and desktop workstations, play a large role in the way that a network operates; therefore, end-system devices should not be ignored. Maintaining relevant documentation about the configuration of end systems gives you a complete picture of the network and allows you to make intelligent decisions about any modifications or upgrades that end systems may require. The inclusion of end-system network configuration information in the baseline will enable you to troubleshoot problems in a timely and efficient manner.

Objectives

Upon completing this lesson, you will be able to:

- Identify the components of an end-system network configuration table
- Identify the components of an end-system network topology diagram
- Identify commands and applications used to discover information about end-system network configurations
- Discover end-system network configuration information
- Create an end-system network configuration table and end-to-end topology diagram

Learner Skills and Knowledge

To benefit fully from this lesson, you must have these prerequisite skills and knowledge:

- Basic knowledge of IP addressing and routing concepts on Windows 2000 devices
- Advanced understanding of network topologies

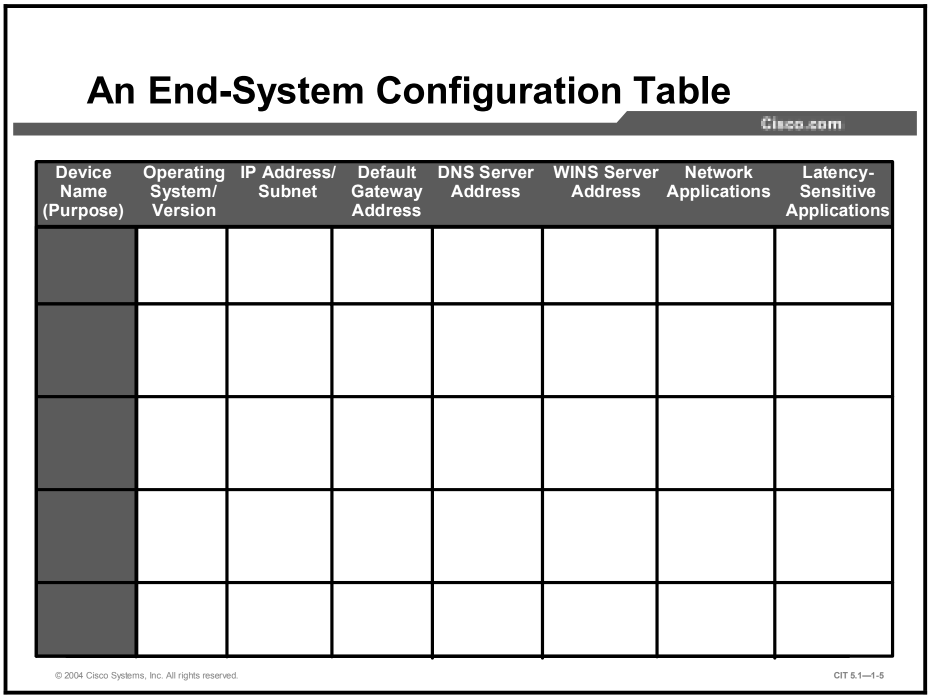
Outline

This lesson contains these topics:

- Overview
- Identifying the Components of an End-System Network Configuration Table
- Identifying the Components of an End-System Network Topology Diagram
- Identifying Commands and Applications Used to Gather Information About End-System Network Configurations
- Discovering End-System Network Configuration Information
- Creating End-System Network Configuration Documentation
- Summary
- Quiz

Identifying the Components of an End-System Network Configuration Table

This topic identifies the components that troubleshooters should include in a network configuration table used to troubleshoot end systems.



An End-System Configuration Table

Cisco.com

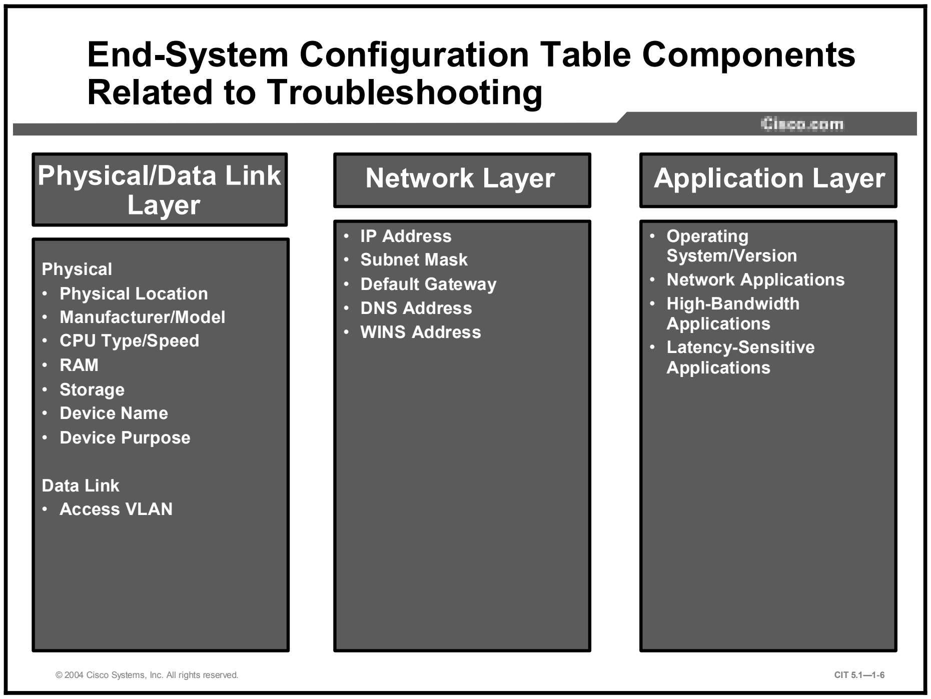
Device Name (Purpose)	Operating System/ Version	IP Address/ Subnet	Default Gateway Address	DNS Server Address	WINS Server Address	Network Applications	Latency-Sensitive Applications

CIT 5.1—1-5

An end-system network configuration table is baseline documentation that shows accurate records of the hardware and software used in end systems.

When creating an end-system network configuration table for troubleshooting, you should document the following:

- Device name (purpose)
- Operating system and version
- IP address
- Subnet mask
- Default gateway, DNS server, and WINS server addresses
- Any latency-sensitive network applications that the end system runs



End-System Configuration Table Components Related to Troubleshooting

Physical/Data Link Layer

Physical
- Physical Location
- Manufacturer/Model
- CPU Type/Speed
- RAM
- Storage
- Device Name
- Device Purpose

Data Link
- Access VLAN

Network Layer

- IP Address
- Subnet Mask
- Default Gateway
- DNS Address
- WINS Address

Application Layer

- Operating System/Version
- Network Applications
- High-Bandwidth Applications
- Latency-Sensitive Applications

CIT 5.1—1-6

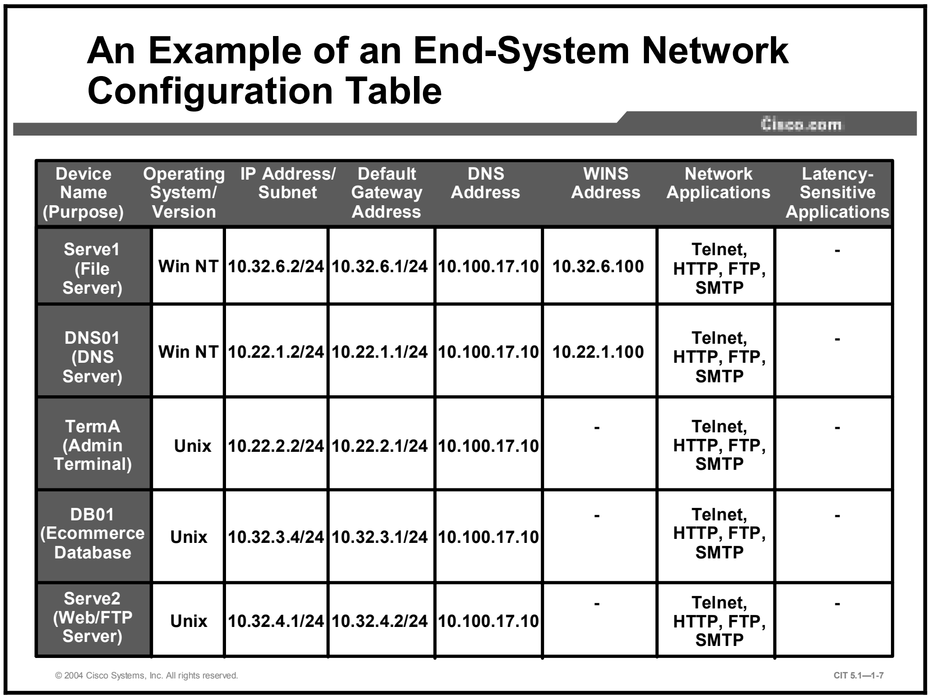
An end-system network configuration table will contain different components based on its use. Some tables are used administratively for inventory. Some simply list the physical location of the device and perhaps a note about when it needs to be backed up, while others are used as a tool for troubleshooting.

An end-system network configuration table used for troubleshooting typically varies, depending on the device being recorded. There are many different types of end systems and, therefore, there is quite a bit of information that you can record. To simplify things, it can be helpful to divide the information that you record into categories based on the relationship the component has with the layers of the TCP/IP networking model. It is important to find out which pieces of information are the most useful for troubleshooting your particular end systems.

Recording network applications that are available on an end system is useful information to include on an end-system network configuration table. It is also a good idea to record any high-bandwidth and latency-sensitive network applications that are running on the end-system, because they are likely to be a target of a troubleshooter. This is because these network applications can have a large impact on network performance. Examples of high-bandwidth applications are streaming video, such as QuickTime, and multicast applications, such as IP/TV.

Example: End-System Network Configuration Table

This example of a network configuration table contains information that troubleshooters can use to describe most end systems.



An Example of an End-System Network Configuration Table

Device Name (Purpose)	Operating System/ Version	IP Address/ Subnet	Default Gateway Address	DNS Address	WINS Address	Network Applications	Latency-Sensitive Applications
Serve1 (File Server)	Win NT	10.32.6.2/24	10.32.6.1/24	10.100.17.10	10.32.6.100	Telnet, HTTP, FTP, SMTP	-
DNS01 (DNS Server)	Win NT	10.22.1.2/24	10.22.1.1/24	10.100.17.10	10.22.1.100	Telnet, HTTP, FTP, SMTP	-
TermA (Admin Terminal)	Unix	10.22.2.2/24	10.22.2.1/24	10.100.17.10	-	Telnet, HTTP, FTP, SMTP	-
DB01 (Ecommerce Database	Unix	10.32.3.4/24	10.32.3.1/24	10.100.17.10	-	Telnet, HTTP, FTP, SMTP	-
Serve2 (Web/FTP Server)	Unix	10.32.4.1/24	10.32.4.2/24	10.100.17.10	-	Telnet, HTTP, FTP, SMTP	-

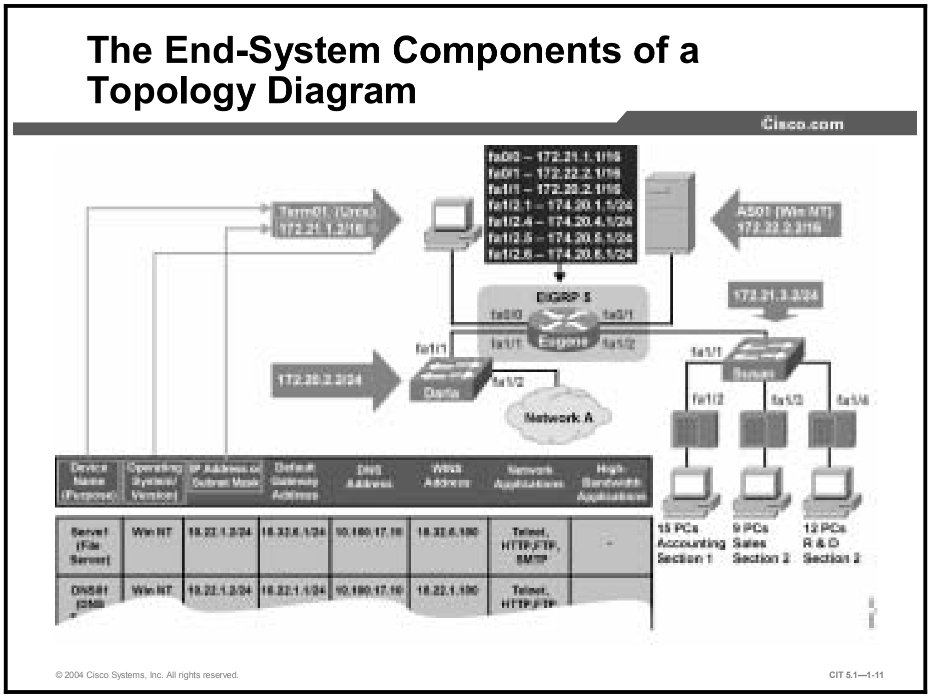
CIT 5.1—1-7

In this example, the following categories are used to document the network-related properties of a device:

- Device name (purpose)
- Operating system and version
- IP address or subnet mask
- Default gateway address
- DNS server address
- WINS server address
- Network applications
- Latency-sensitive applications

Identifying the Components of an End-System Network Topology Diagram

This topic identifies the components of a network topology diagram that pertain to end systems.



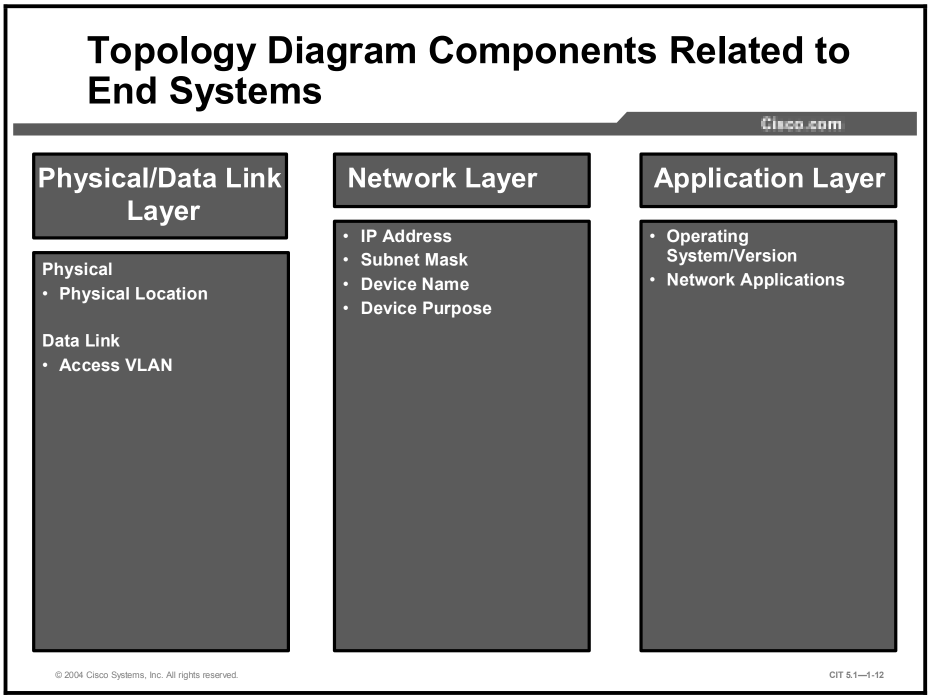
The End-System Components of a Topology Diagram

Device Name (Purpose)	Operating System/ Version	IP Address or Subnet Mask	Default Gateway Address	DNS Address	WINS Address	Network Applications	High-Bandwidth Applications
Serve1 (File Server)	Win NT	10.22.1.2/24	10.32.6.1/24	10.180.17.10	10.32.6.100	Telnet, HTTP,FTP, SMTP	-
DNS01 (DNS	Win NT	10.22.1.2/24	10.22.1.1/24	10.180.17.10	10.22.1.100	Telnet, HTTP,FTP	

CIT 5.1—1-11

An end-system network topology is a graphical representation of the tabular data gathered in the end-system network configuration table. Topologies should illustrate how end systems are both physically and logically connected to the network. Since end systems are frequently added to existing network diagrams, topology diagrams that include end systems often also include components of network device configurations.

Like the network devices in a topology diagram, end systems in a network topology do not typically include every component of the end-system network configuration table. Minimally, the end systems on a topology diagram should include the name, and an illustration, of the device and how it is connected to the network.



Topology Diagram Components Related to End Systems

Physical/Data Link Layer

Physical
- Physical Location

Data Link
- Access VLAN

Network Layer

- IP Address
- Subnet Mask
- Device Name
- Device Purpose

Application Layer

- Operating System/Version
- Network Applications

CIT 5.1—1-12

Like an end-system network configuration table, the components of a topology diagram that include end systems can have different components, depending on the types of end systems in the network. These components can also be categorized according to logical TCP/IP layers.

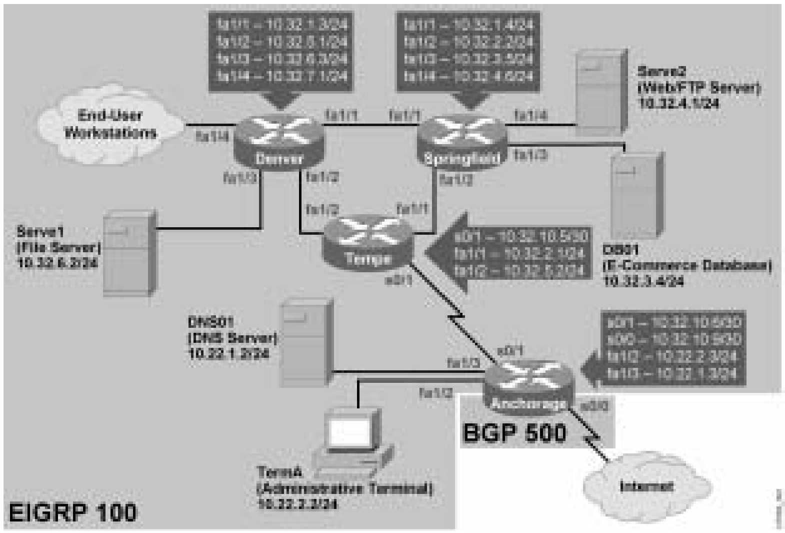
A topology diagram that includes end systems will differ, depending on its focus. A topology that is focused on the end systems rather than the configuration of network devices may represent the network components as a network cloud symbol with the details of the end systems connected to it. On the other hand, all the details of the network device configuration may be included on the same diagram that includes the end systems.

Example: Topology Diagram with Both Network Devices and End Systems

This is an example of a topology diagram that includes both network devices and end systems.

A Network Topology Diagram That Includes End-Systems

Cisco.com



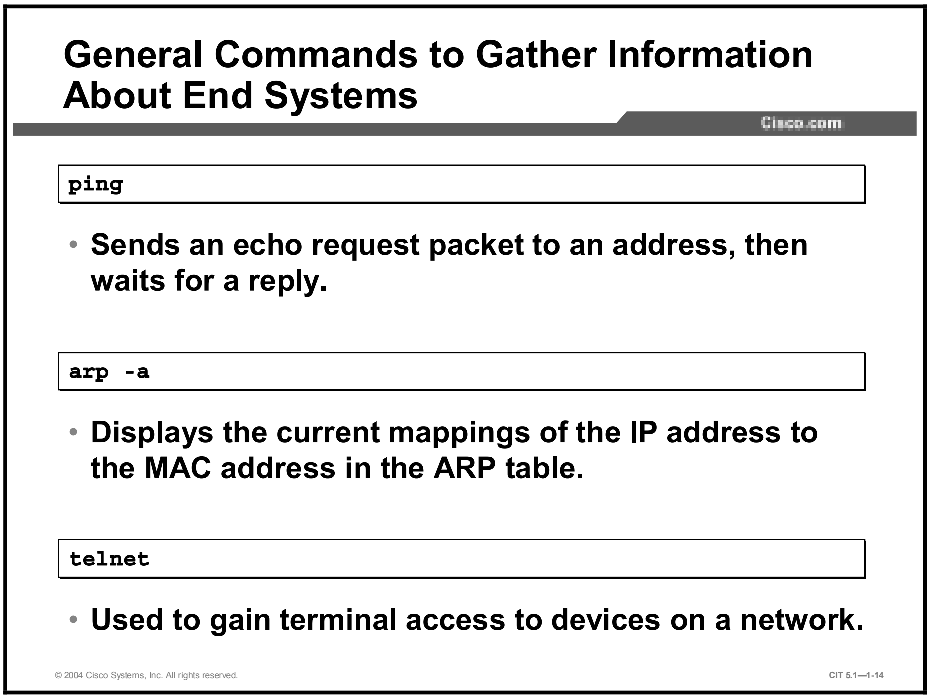
CIT 5.1—1-13

This example includes the following components related to end systems:

- Device name and purpose
- Operating system
- IP address

Identifying Commands and Applications Used to Gather Information About End-System Network Configurations

This topic identifies commands and applications that troubleshooters use to gather information about the network configuration of end systems.



General Commands to Gather Information About End Systems

```
ping
```

- Sends an echo request packet to an address, then waits for a reply.

```
arp -a
```

- Displays the current mappings of the IP address to the MAC address in the ARP table.

```
telnet
```

- Used to gain terminal access to devices on a network.

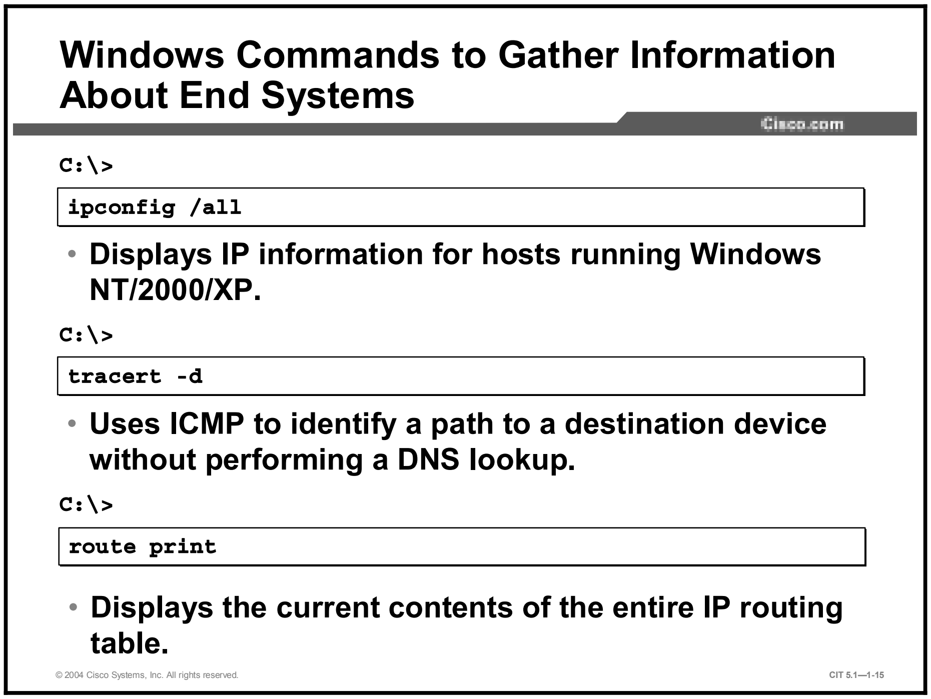
© 2004 Cisco Systems, Inc. All rights reserved.

CIT 5.1—1-14

The table shows general commands that a troubleshooter uses to gather information about the network configuration of an end system. These commands are considered general because they can be applied on end systems running the most common operating systems.

General Commands to Gather Information About End Systems

Command	Description
ping {*host* | *ip-address*}	Sends an echo request packet to an address, then waits for a reply. The *host* | *ip-address* variable is the IP alias or IP address of the target system.
arp –a	Displays the current mappings of the IP address to the MAC address in the Address Resolution Protocol (ARP) table.
telnet	Used to gain terminal access to devices on a network. A successful connection is also an indication that the end system supports the TCP protocol.



Windows Commands to Gather Information About End Systems

```
C:\>
ipconfig /all
```

- Displays IP information for hosts running Windows NT/2000/XP.

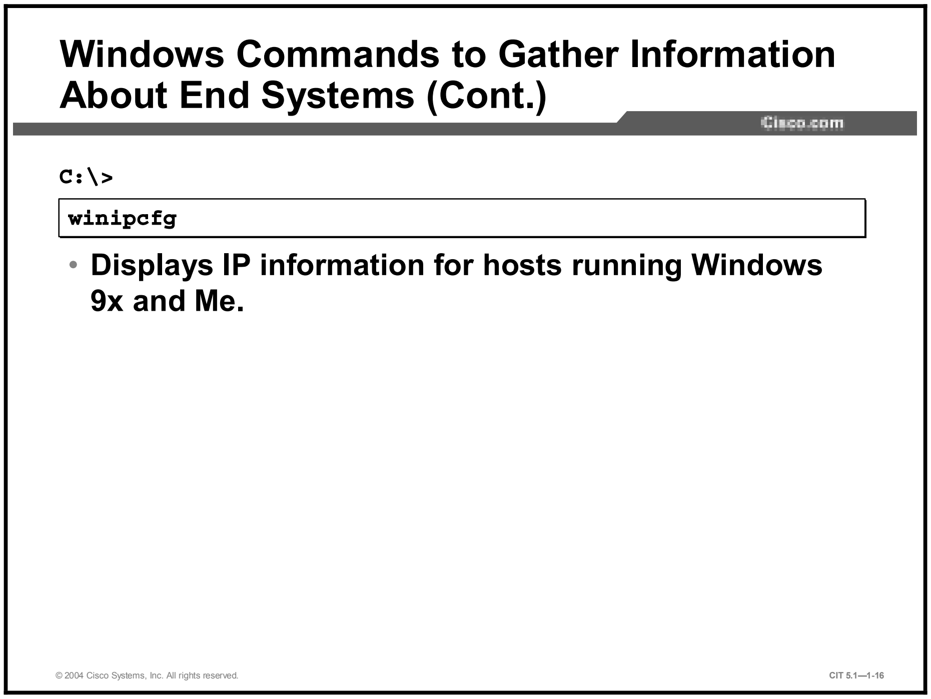
```
C:\>
tracert -d
```

- Uses ICMP to identify a path to a destination device without performing a DNS lookup.

```
C:\>
route print
```

- Displays the current contents of the entire IP routing table.

CIT 5.1—1-15



Windows Commands to Gather Information About End Systems (Cont.)

```
C:\>
winipcfg
```

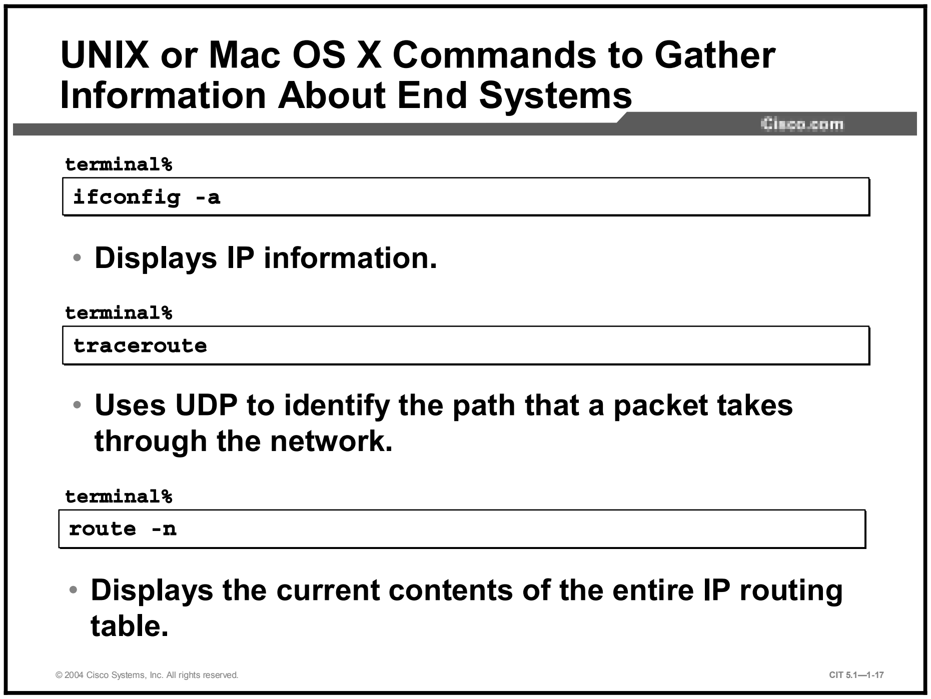
- Displays IP information for hosts running Windows 9x and Me.

CIT 5.1—1-16

The table shows commands that a troubleshooter uses on an end system running a Windows operating system to gather information about the network configuration of an end system.

Windows Commands to Gather Information About End Systems

Command	Description
ipconfig /all	Displays IP information for hosts running Windows NT/2000/XP.
tracert *-d* [*destination*]	Uses Internet Control Message Protocol (ICMP) to identify a path to a destination device for Windows hosts without performing a Domain Name System (DNS) lookup.
route print	Displays the current contents of the entire IP routing table.
winipcfg	Displays IP information for hosts running Windows 9x and Me.



UNIX or Mac OS X Commands to Gather Information About End Systems

```
terminal%
ifconfig -a
```

- **Displays IP information.**

```
terminal%
traceroute
```

- **Uses UDP to identify the path that a packet takes through the network.**

```
terminal%
route -n
```

- **Displays the current contents of the entire IP routing table.**

© 2004 Cisco Systems, Inc. All rights reserved. CIT 5.1—1-17

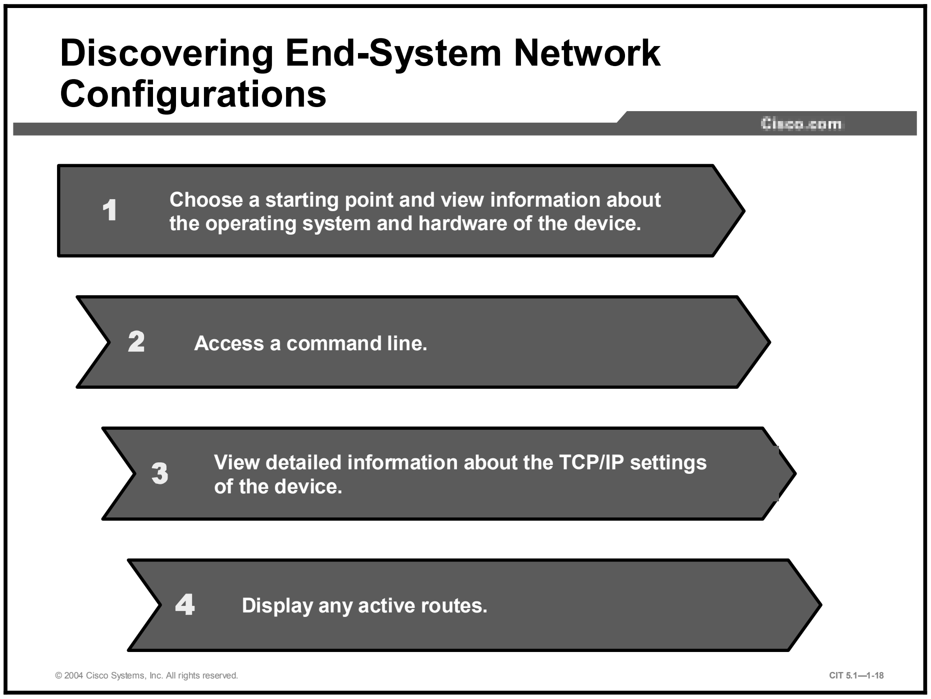
The table shows commands that a troubleshooter uses on an end system running the UNIX or Mac OS X operating systems to gather information about the network configuration of an end system.

UNIX or Mac OS X Commands to Gather Information About End Systems

Command	Description
ifconfig -a	Displays IP information for UNIX and Mac OS X hosts.
traceroute [*destination*]	Uses User Datagram Protocol (UDP) to identify the path a packet takes through the network. The *destination* variable is the host name or IP address of the target system.
route -n	Displays the current contents of the entire IP routing table.

Discovering End-System Network Configuration Information

This topic describes the procedure of discovering end-system network configuration information.



Discovering End-System Network Configurations

Cisco.com

1 Choose a starting point and view information about the operating system and hardware of the device.

2 Access a command line.

3 View detailed information about the TCP/IP settings of the device.

4 Display any active routes.

© 2004 Cisco Systems, Inc. All rights reserved.

CIT 5.1—1-18

Procedure: Discovering End-System Network Configurations

The following steps outline the procedure for discovering the network configuration of an end system:

Step 1 Choose a starting point and view information about the operating system and hardware of the device.

Note On a Windows end system, information about the operating system and hardware can be accessed by choosing **Start>Settings>Control Panel** and then double-clicking the **Systems** icon. On a Mac running Mac OS X, click the **Apple** icon and choose **About This Mac**.

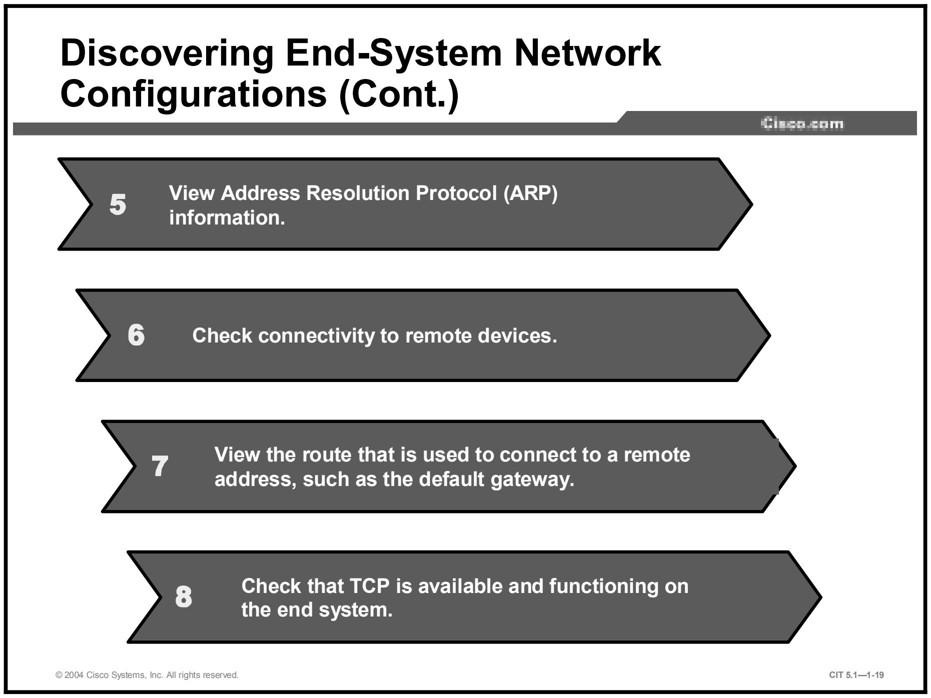
Step 2 Access a command line.

Note To access a command line on a Windows end system, choose **MS-DOS** or the command prompt from the Start menu. The command line terminal utility on Mac OS X can be found in the Utilities folder located in the Applications directory.

Step 3 View detailed information about the TCP/IP settings of a device. This is accomplished by entering the **ipconfig /all** or **winipcfg** commands in a Windows command prompt or entering **ifconfig -a** in a UNIX or Mac OS X command line. The important information to record includes the following: IP address/subnet mask, default gateway address, and any DNS or WINS server addresses.

Note When viewing the information returned from **ipconfig /all**, it is helpful to note if the IP address of a device is static or if it has been temporarily assigned through DHCP.

Step 4 Display any active routes by entering the **route print** command in a Windows command prompt or entering **route –n** in a UNIX or Mac OS X command line.



Discovering End-System Network Configurations (Cont.)

5 View Address Resolution Protocol (ARP) information.

6 Check connectivity to remote devices.

7 View the route that is used to connect to a remote address, such as the default gateway.

8 Check that TCP is available and functioning on the end system.

© 2004 Cisco Systems, Inc. All rights reserved. CIT 5.1—1-19

Step 5 View ARP information by entering the **arp -a** command.

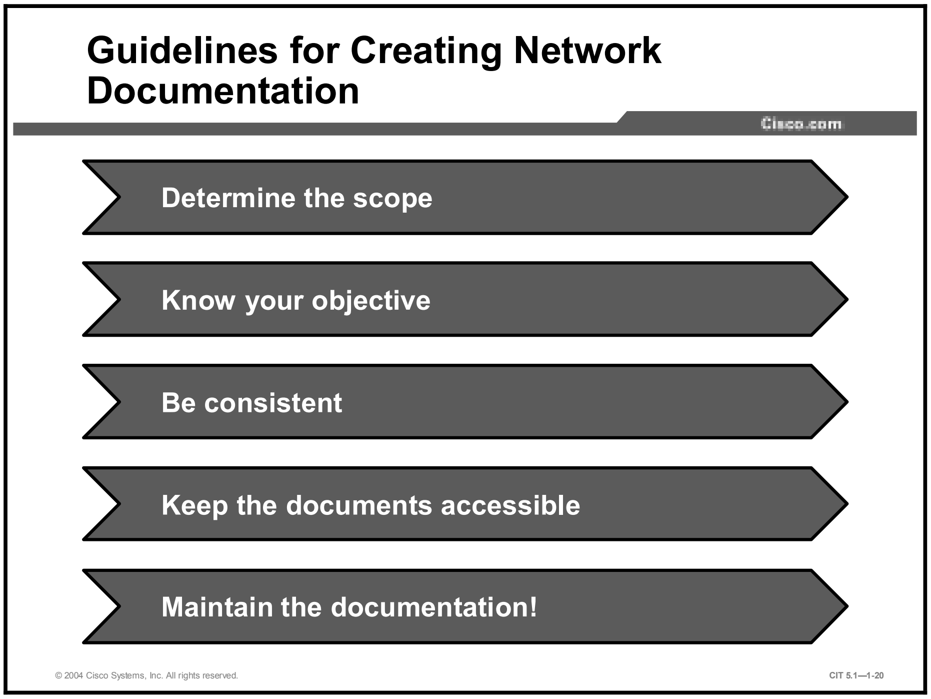
Step 6 Check connectivity to remote devices by attempting to ping a device across a link.

Step 7 View the route that is used to connect to a remote address, such as the default gateway. To accomplish this, enter **tracert** {*ip-address* | *hostname*} in a Windows command prompt or enter **traceroute** {*ip-address* | *hostname*} in a UNIX or Mac OS X command line.

Step 8 Check that TCP is available and functioning on the end system by entering the **telnet** {*ip-address* | *hostname*} command.

Creating End-System Network Configuration Documentation

This topic identifies guidelines for troubleshooters to create end-system network configuration documentation.



Guidelines for Creating Network Documentation

Cisco.com

- Determine the scope
- Know your objective
- Be consistent
- Keep the documents accessible
- Maintain the documentation!

CIT 5.1—1-20

Good end-system network configuration documentation allows you to quickly learn specific information about end systems.

Guidelines for creating effective end-system network documentation are as follows:

- **Determine the scope:** To determine the scope of your end-system network documentation, it is important to know which end systems are included in your domain of responsibility.
- **Know your objective:** Only collect data that is relevant to your objective and provide sufficient detail for those relative pieces. Extra layers of information will only make the documentation more difficult to use.
- **Be consistent:** Use consistent terminology, abbreviations, and style. Try to make the documents orderly and easy to understand. When possible, use templates and keep a library of symbols and graphic icons that you can re-use.
- **Keep the documents accessible:** Store the network documentation in a location where it is readily available on the job. It is also suggested that a copy of the documentation be kept in a secure location offsite.
- **Maintain the documentation:** Modify your network documentation as conditions and devices in the network change. *This is especially important.*

Note You may want to implement a process for handling changes to the network documentation. Factors in this process that need to be accounted for are reporting network changes, maintaining version control, and assigning responsibility for modifying and distributing updated documents.

Example: Creating Successful End-System Network Configuration Documentation

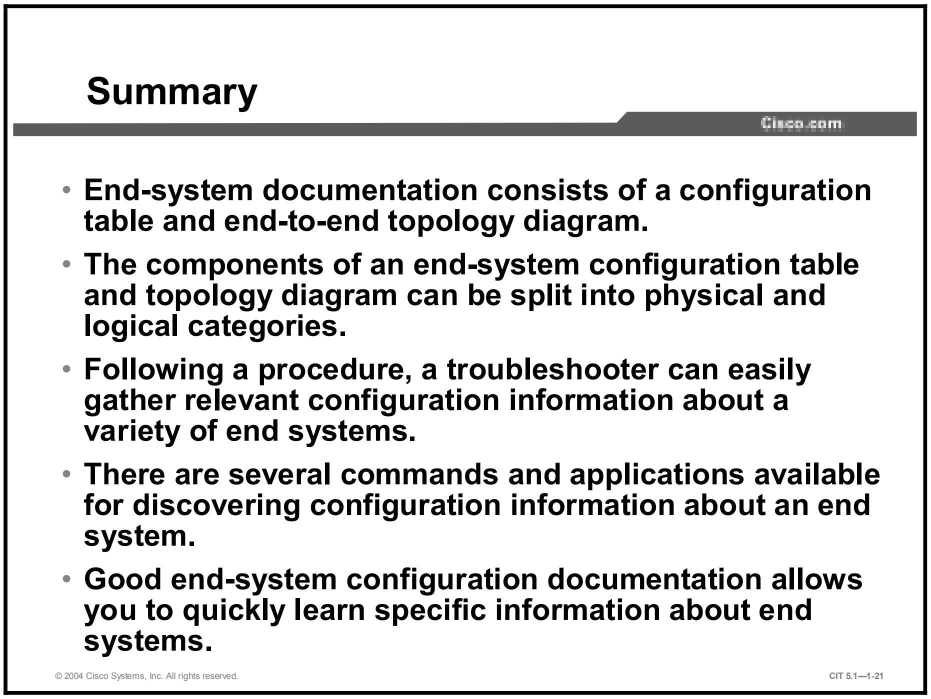
At your company, your primary job function is to maintain and troubleshoot network servers and desktops. You and your team already do a respectable job of fixing problems, but you have been asked to create documentation of the network end systems to expedite troubleshooting efforts and cut down on costs. Your company currently has configuration tables and topology diagrams of your network configuration without end systems.

A month later, the network support staff has been using the end-system documentation for troubleshooting. Estimates have determined that the time that your department spends troubleshooting end systems in the past month has dropped considerably. Your documentation was a success for the following reasons:

- You had a good idea of what the scope of the documentation should be because you were already familiar with the end systems on your network.
- You recorded the appropriate types and amounts of information for each documented end system.
- You used symbols and terminology consistent with the existing network documentation that your co-workers were already familiar with.
- You kept the documentation current by implementing a system for employees to report changes, and updating the documentation in a timely manner has been added to your job description.
- You stored the documentation in convenient and clearly marked locations close to each administrative terminal.

Summary

This topic summarizes the key points discussed in this lesson.



Summary

- End-system documentation consists of a configuration table and end-to-end topology diagram.
- The components of an end-system configuration table and topology diagram can be split into physical and logical categories.
- Following a procedure, a troubleshooter can easily gather relevant configuration information about a variety of end systems.
- There are several commands and applications available for discovering configuration information about an end system.
- Good end-system configuration documentation allows you to quickly learn specific information about end systems.

CIT 5.1—1-21

References

For additional information, refer to this resource:

- http://www.cisco.com/

Next Steps

For the associated lab exercise, refer to the following section of the course Lab Guide:

- Lab Exercise 1-2: Creating End-System Baseline Discovery

Quiz

Use the practice items here to review what you have learned in this lesson. The correct answers are found in the Quiz Answer Key.

Q1) Which list includes only components of an end-system network configuration table?

A) PortFast, IP address, network applications, trunk status

B) IOS type/version, subnet mask, default gateway address, STP state

C) IP address, subnet mask, routing protocol, duplex, access list

D) IP address, default gateway, WINS address, networked applications

Q2) Which list includes only components of a topology diagram that are related to end systems?

A) trunk status, PortFast, subnet mask

B) MAC address, network applications, IP address

C) duplex, interface name, routing protocol

D) IP address, subnet mask, STP state

Q3) Which end-system command would be used to view the address that a host dynamically obtains from DHCP?

A) **ping**

B) **route print**

C) **show ip resolve**

D) **ipconfig /all**

Q4) Which step in the process of discovering end-system network configurations will give you a list of the active routes for a host?

A) entering the **ipconfig/all** command

B) entering the **tracert** command

C) entering the **route print** command

D) using Telnet to connect to a device

Q5) To reduce the amount of paperwork generated by documenting end systems, which guideline should you follow?

A) document all possible aspects of the hardware and network configuration of an end system

B) create separate end-system topology diagrams instead of adding end systems to existing network diagrams

C) determine an objective for the documentation and collect data that meets that objective

D) document desktops and laptops along with infrastructure devices such as servers and databases

Quiz Answer Key

Q1) D

Relates to: Identifying the Components of an End-System Network Configuration Table

Q2) B

Relates to: Identifying the Components of an End-System Network Topology Diagram

Q3) D

Relates to: Identifying Commands and Applications Used to Gather Information About End-System Network Configurations

Q4) C

Relates to: Discovering End-System Network Configuration Information

Q5) C

Relates to: Creating End-System Network Configuration Documentation

Module 2

Determining an Effective Troubleshooting Strategy

Overview

An organization depends on its users being able to access network resources to conduct its daily business. When you determine an effective troubleshooting strategy, you can isolate problems and implement solutions quicker and more cost-effectively than without a strategy. Thus, you can quickly restore the vital network functionality on which your organization relies. If you do not have an effective troubleshooting strategy, you can lose business opportunities, profits, and end-user confidence in the competence of your organization. In this module, you will take what you already know about logical layered models and apply that knowledge to a physical network. You will then use your understanding of those layers to select a troubleshooting approach and gather symptoms from network devices, users, and end systems.

Module Objectives

Upon completing this module, you will be able to:

- Identify the layer or layers in the OSI and TCP/IP models that encapsulated data flow maps to at each component of a logical network
- Describe a general network troubleshooting process
- Gather information about the symptoms of a network problem
- Select an approach for troubleshooting network problems

Module Outline

The module contains these components:

- Applying a Layered Model to a Network
- Describing a General Troubleshooting Process
- Gathering Symptoms
- Selecting a Troubleshooting Approach
- Lesson Assessments

Applying a Layered Model to a Network

Overview

In the previous module, you focused on the physical aspects of a network. You determined which equipment was being used in your network and how those devices were connected to establish a baseline. In this lesson, you will learn how to apply a layered networking model to your network to help you troubleshoot variances off your baseline. When you apply a layered model to a network, you divide the complexity of the problem into more manageable and understandable parts. This allows you to resolve problems quickly.

Relevance

Logical networking models separate network functionality into modular layers. You apply these modular layers to your network to isolate problems and even create divisions of labor. For example, if the symptoms of a communications problem suggest a physical connection problem, the telephone company service person can focus on troubleshooting the T1 circuit (operating at the physical layer). The repairperson does not have to know anything about TCP/IP (operating at the network layer) or attempt to make changes to devices operating outside of the realm of the suspected logical layer. The repairperson concentrates on the physical circuit. If the circuit checks out OK, either the repairperson or a different specialist looks at areas in another layer that could be causing the problem.

Objectives

Upon completing this lesson, you will be able to:

- Match the layers of the TCP/IP model to the layers of the OSI model
- Identify the stages of data flow through a fully functioning network with interconnecting end systems using Cisco routers and switches
- Identify the logical layer or layers that encapsulated data is at as it flows through a logical network end-to-end

Learner Skills and Knowledge

To benefit fully from this lesson, you must have these prerequisite skills and knowledge:

- Familiarity with the Cisco IOS commands covered in the Cisco *Building Scalable Cisco Internetworks* (BSCI), *Building Cisco Multilayer Switched Networks* (BCMSN), and *Building Cisco Remote Access Networks* (BCRAN) courses
- An understanding of basic encapsulated data concepts
- The ability to analyze debug information

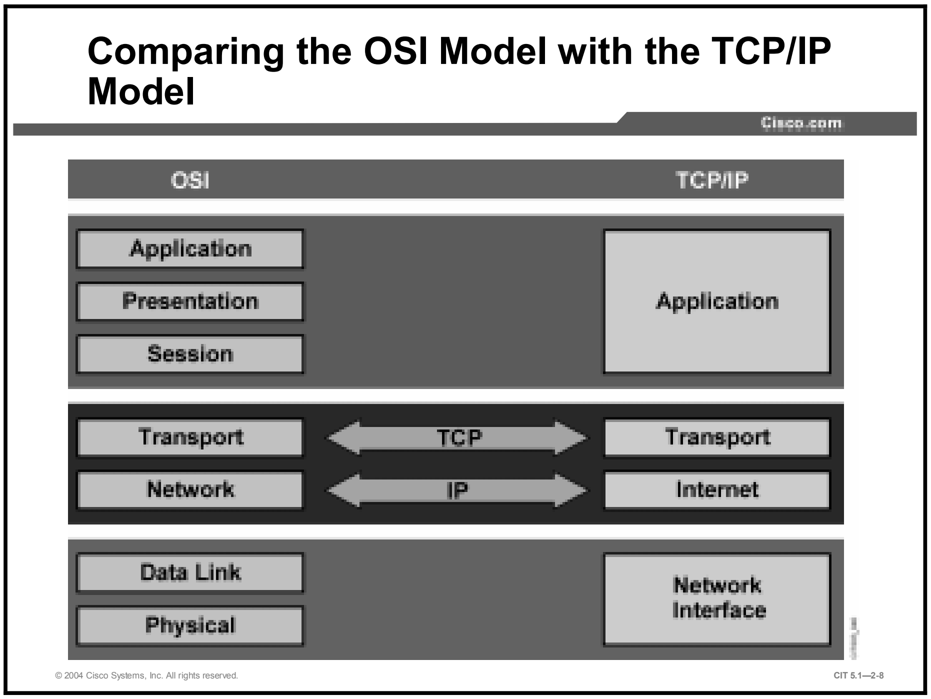
Outline

This lesson includes these topics:

- Overview
- Comparing Layered Networking Models
- Identifying the Encapsulated Data Flow Process
- Identifying the Layers of a Logical Model
- Summary
- Quiz

Comparing Layered Networking Models

This topic matches the logical layers of the Open Systems Interconnection (OSI) networking model to the TCP/IP networking model.



Comparing the OSI Model with the TCP/IP Model

Cisco.com

OSI		TCP/IP
Application Presentation Session		Application
Transport	TCP	Transport
Network	IP	Internet
Data Link Physical		Network Interface

© 2004 Cisco Systems, Inc. All rights reserved. CIT 5.1—2-8

Similar to the OSI networking model, the TCP/IP networking model divides networking architecture into modular layers. The figure and the table show how the TCP/IP networking model maps to the layers of the OSI networking model. It is this close mapping that allows the TCP/IP suite of protocols to successfully communicate with so many networking technologies.

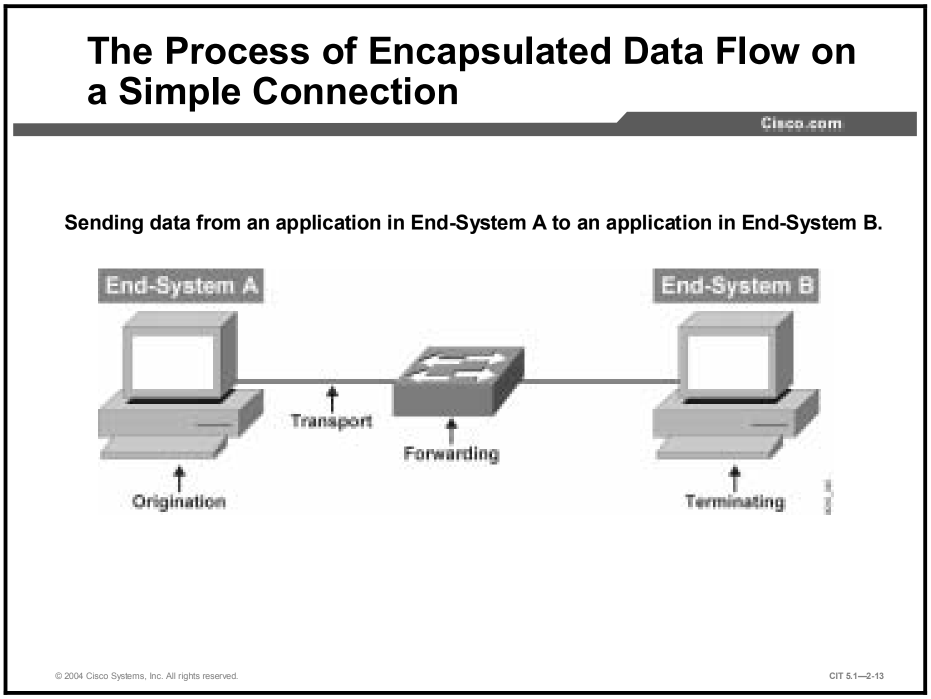
Describing the TCP/IP Layers and Their Relationship to the OSI Model

TCP/IP Layer	In the OSI Model, Maps to	Description
Network Interface	Physical Data Link	The network interface layer frames and encapsulates data and transmits the encapsulated data to the physical interface.
Internet	Network	This Internet layer of the TCP/IP protocol provides connectivity and path selection between two end systems. This is the layer at which routing occurs.
Transport	Transport	The transport layer is responsible for exchanging segments between devices on a TCP/IP network.
Application	Session Presentation Application	The application layer provides communication between applications, such as FTP, HTTP, and Simple Mail Transfer Protocol (SMTP) on separate hosts.

Note The TCP/IP model illustrates the close relationship between the session, presentation, and application OSI layers by combining them into a single layer. Given this close relationship, this course will refer to a component of any of these three layers as part of the application layer.

Identifying the Encapsulated Data Flow Process

This topic identifies the process of encapsulated data flow through an end-to-end network.



The Process of Encapsulated Data Flow on a Simple Connection

Cisco.com

Sending data from an application in End-System A to an application in End-System B.

© 2004 Cisco Systems, Inc. All rights reserved.

CIT 5.1—2-13

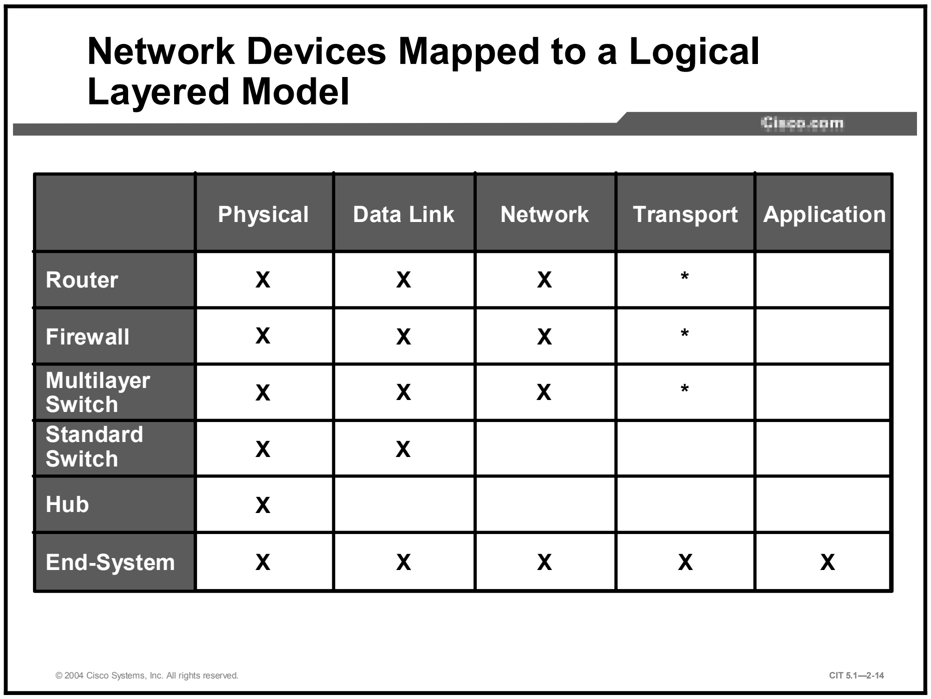
The table describes the stages in the process of sending encapsulated data between end systems.

Sending Encapsulated Data Between Two End Systems

Stage	Description
Origination	End-System A takes data from an application and converts it as needed for transmission over a physical network. This involves the following: ■ Converting data into segments ■ Encapsulating segments with a header that includes network addressing information and converting segments into packets ■ Encapsulating packets with a header that includes physical addressing information and converting packets into frames ■ Converting frames into bits
Transport	Data passes over physical medium as bits.
Forwarding	When data reaches a network device, the device removes data control information as needed. Standard switches read physical addressing information and forward frames to an interface. Routers, firewalls, and multilayer switches read network addressing information and forward packets to an interface. The transport and forwarding stages alternate until the data flows through all devices that are necessary to reach the interface of the target end system.
Terminating	The interface of End-System B receives the data from the physical medium, removes the data control information, and converts the data as needed for use with the target application.

Identifying the Layers of a Logical Model

This topic identifies the logical layers that a troubleshooter should focus on when troubleshooting specific networking devices.



Network Devices Mapped to a Logical Layered Model

	Physical	Data Link	Network	Transport	Application
Router	X	X	X	*	
Firewall	X	X	X	*	
Multilayer Switch	X	X	X	*	
Standard Switch	X	X			
Hub	X				
End-System	X	X	X	X	X

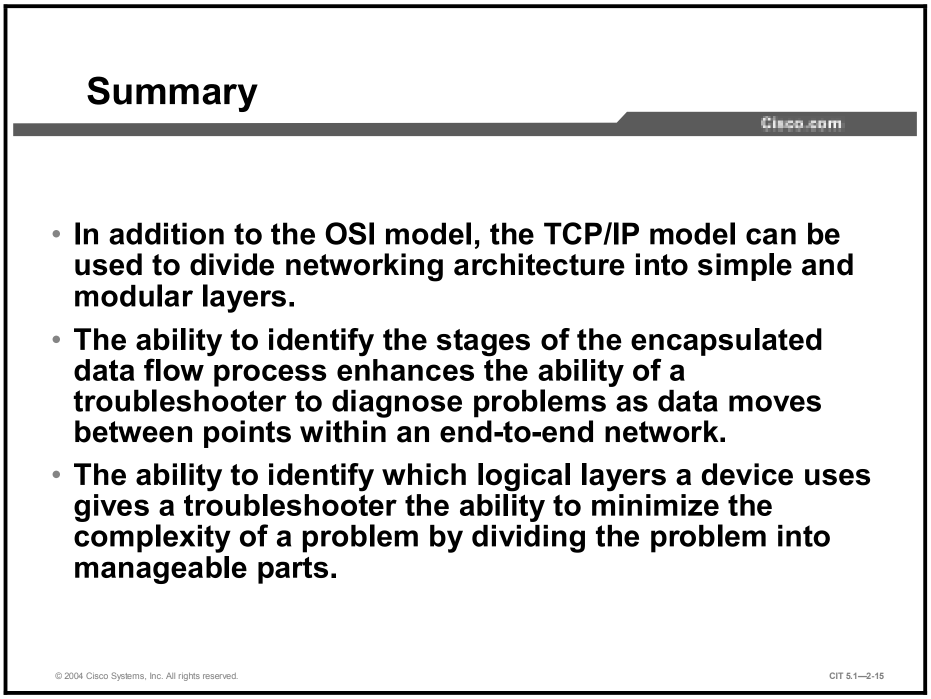
CIT 5.1—2-14

Note Devices marked with an asterisk (*) can have some involvement with the indicated layer, but do not perform primary functions at that layer.

The ability to identify which layers pertain to a networking device gives a troubleshooter the ability to minimize the complexity of a problem by dividing the problem into manageable parts. For instance, knowing that network layer issues are of no importance to a switch (aside from multilayer switches) defines the boundaries of your task to the physical and data link layers. Given that there is still plenty to consider at only these two layers, this simple knowledge can prevent you from troubleshooting irrelevant possibilities and will significantly reduce the amount of time that you spend attempting to correct a problem. However, it is still important to note that there are network applications that are part of these devices that move into the session, presentation, and application layers.

Summary

This topic summarizes the key points discussed in this lesson.



Summary

- In addition to the OSI model, the TCP/IP model can be used to divide networking architecture into simple and modular layers.
- The ability to identify the stages of the encapsulated data flow process enhances the ability of a troubleshooter to diagnose problems as data moves between points within an end-to-end network.
- The ability to identify which logical layers a device uses gives a troubleshooter the ability to minimize the complexity of a problem by dividing the problem into manageable parts.

CIT 5.1—2-15

References

For additional information, refer to this resource:

- http://www.cisco.com/tac/

Next Steps

For the associated lab exercise, refer to the following section of the course Lab Guide:

- Lab Exercise 2-1: Applying a Layered Model to a Network

Quiz

Use the practice items here to review what you have learned in this lesson. The correct answers are found in the Quiz Answer Key.

Q1) Which is the correct mapping of the TCP/IP model layers with the OSI model layers?

A) network interface and data link layers map to physical layer
Internet layer maps to network layer
transport layer maps to transport and session layers
application layer maps to presentation and application layers

B) network interface layer maps to physical layer
Internet layer maps to data link and network layers
transport layer maps to transport and session layers
application layer maps to presentation and application layers

C) physical layer maps to transport and application layers
network interface layer maps to physical layers
transport layer maps to data link layers
network maps to Internet, session, and presentation

D) network interface layer maps to physical and data link layers
Internet layer maps to network layer
transport layer maps to transport layer
application layer maps to session, presentation, and application layers

Q2) During which stage of the encapsulated data flow process does an end system receive data from a network and begin the process of removing data control information to make it usable with an application?

A) origination

B) transport

C) forwarding

D) terminating

Q3) A multilayer switch is considered a _____ device.

A) Layer 1

B) Layer 2

C) Layer 3

D) Layer 4

Quiz Answer Key

Q1) D

Relates to: Comparing Layered Networking Models

Q2) D

Relates to: Identifying the Encapsulated Data Flow Process

Q3) C

Relates to: Identifying the Layers of a Logical Model

Describing a General Troubleshooting Process

Overview

You must have a specific methodology to follow to effectively solve a problem. In this lesson, you will learn a general troubleshooting process that can be applied to any network troubleshooting situation.

Relevance

Having a general troubleshooting process gives you a method to follow for any troubleshooting situation. Applying this general process helps a troubleshooter resolve problems quicker and more cost-effectively because it reduces the possibility that a troubleshooter will waste time or get confused.

Objectives

Upon completing this lesson, you will be able to:

- Describe the general troubleshooting process
- Describe the Gathering Symptoms stage of the general troubleshooting process
- Describe the Isolate the Problem stage of the general troubleshooting process
- Describe the Correct the Problem stage of the general troubleshooting process

Learner Skills and Knowledge

To benefit fully from this lesson, you must have these prerequisite skills and knowledge:

- Familiarity with the OSI and TCP/IP networking model concepts

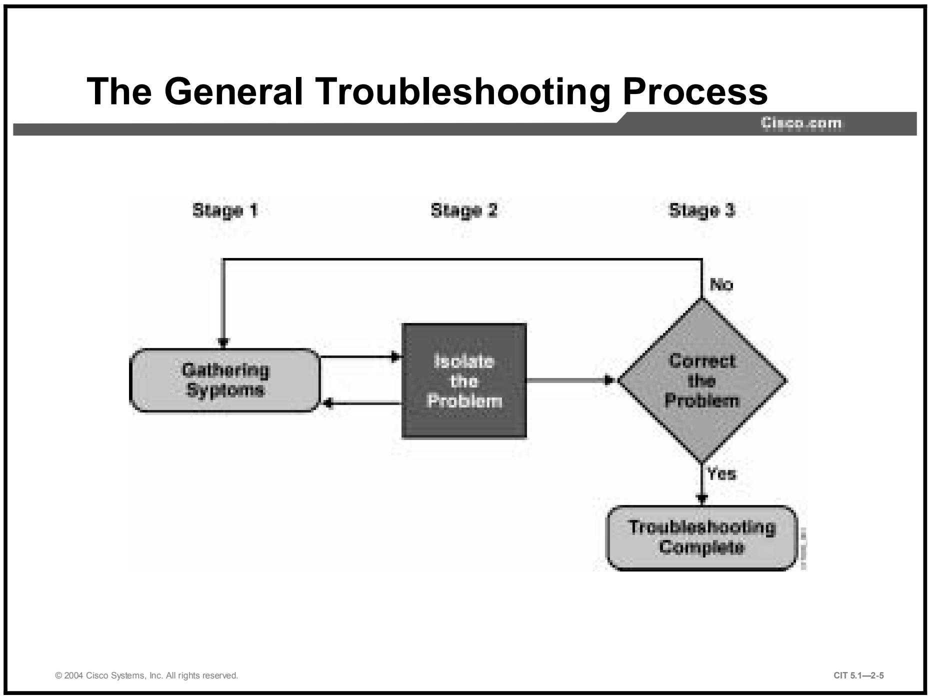
Outline

This lesson includes these topics:

- Overview
- Describing the General Troubleshooting Process
- Describing the Gathering Symptoms Stage
- Describing the Isolate the Problem Stage
- Describing the Correct the Problem Stage
- Summary
- Quiz

Describing the General Troubleshooting Process

This topic describes the general process that a troubleshooter should use when faced with a networking problem.



The General Troubleshooting Process

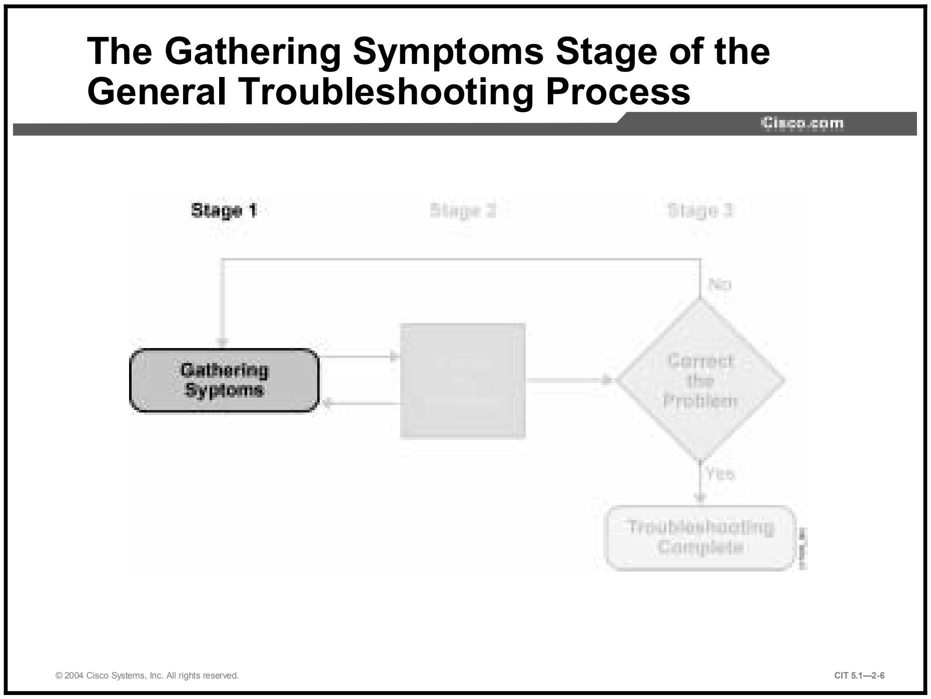
CIT 5.1—2-5

The stages of the general troubleshooting process are Gather Symptoms, Isolate the Problem, and Correct the Problem. The stages are not mutually exclusive. At any point in the process, you may retrace your steps. For instance, while you are isolating a problem, you may need to gather more symptoms. Or, perhaps when you attempt to correct a problem, you cause another unidentified problem. As a result, you need to gather the symptoms, isolate, and correct the new problem.

You should establish a policy for each stage. A policy will give you a consistent manner in which to perform each stage. Part of your policy should include documenting every important piece of information.

Describing the Gathering Symptoms Stage

This topic describes the Gathering Symptoms stage of the general troubleshooting process of which troubleshooters should be aware.



The Gathering Symptoms Stage of the General Troubleshooting Process

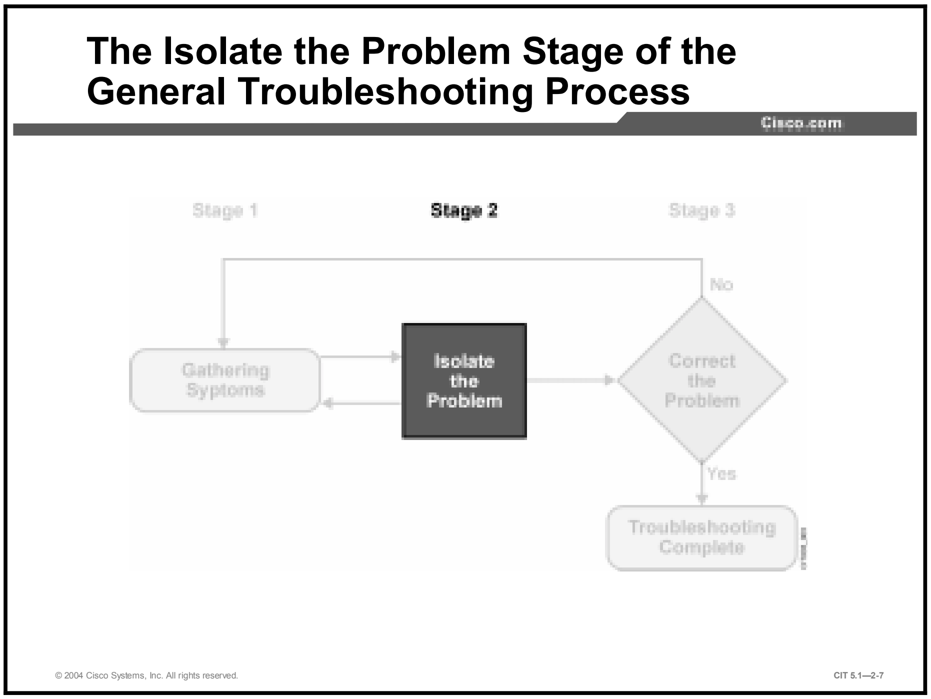
CIT 5.1—2-6

To perform the Gathering Symptoms stage of the general troubleshooting process, the troubleshooter gathers and documents symptoms from the network, end systems, or users. In addition, the troubleshooter determines what network components have been affected and how the functionality of the network has changed compared to the baseline. Symptoms may appear in many different forms. These forms include alerts from the network management system, console messages, and user complaints.

While you gather symptoms, you will use questions as a method of localizing the problem to a smaller range of possibilities. However, you have not truly isolated the problem until you have identified a single problem or a set of related problems.

Describing the Isolate the Problem Stage

This topic describes the Isolate the Problem stage of the general troubleshooting process of which troubleshooters should be aware.



The Isolate the Problem Stage of the General Troubleshooting Process

CIT 5.1—2-7

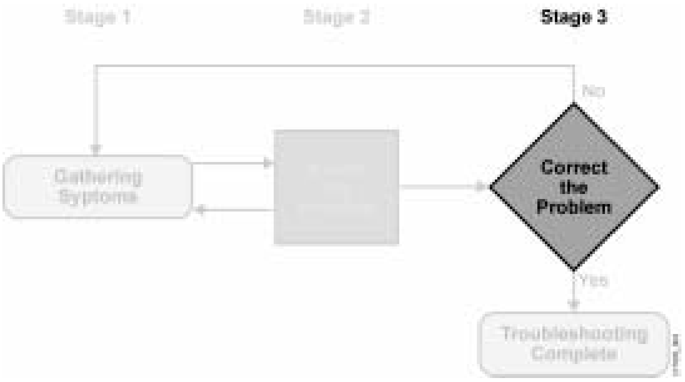
To perform the Isolate the Problem stage of the general troubleshooting process, the troubleshooter identifies the characteristics of problems at the logical layers of the network so that the most likely cause can be selected. At this stage, the troubleshooter may gather and document more symptoms depending on the problem characteristics that are identified.

Describing the Correct the Problem Stage

This topic describes the Correct the Problem stage of the general troubleshooting process of which troubleshooters should be aware.

The Correct the Problem Stage of the General Troubleshooting Process

Cisco.com

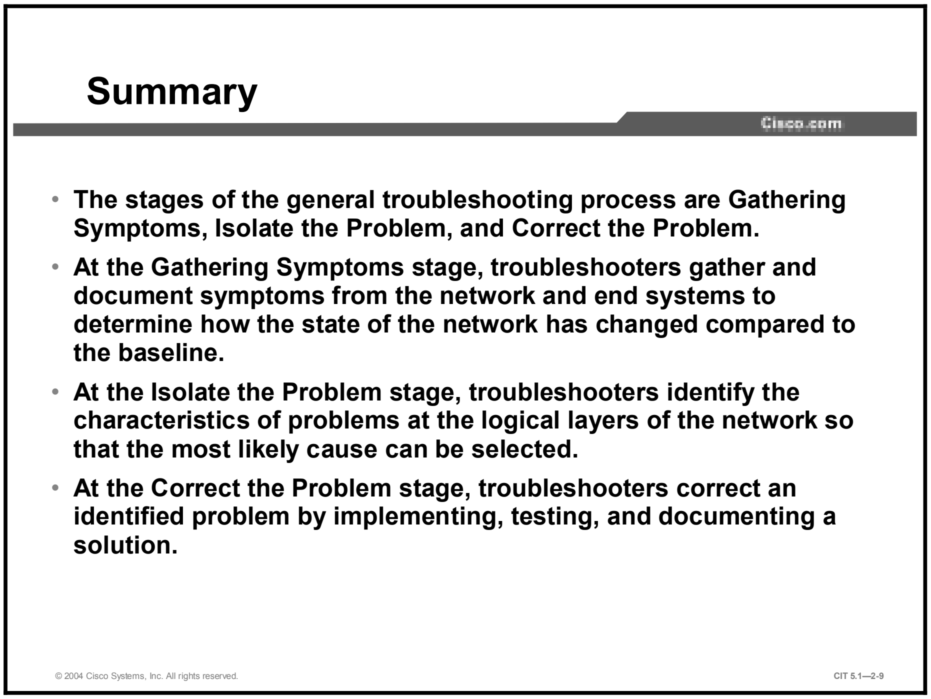


CIT 5.1—2-8

To perform the Correct the Problem stage of the general troubleshooting process, the troubleshooter corrects an identified problem by implementing, testing, and documenting a solution. If corrective actions do not fix the problem, it is important that a troubleshooter reverses any changes that were made that did not create a positive result toward the solution. If, when testing the correction results, the troubleshooter determines that another problem has been created, the attempted solution is documented and the troubleshooter returns to gathering symptoms and isolating the problem.

Summary

This topic summarizes the key points discussed in this lesson.



Summary

- **The stages of the general troubleshooting process are Gathering Symptoms, Isolate the Problem, and Correct the Problem.**
- **At the Gathering Symptoms stage, troubleshooters gather and document symptoms from the network and end systems to determine how the state of the network has changed compared to the baseline.**
- **At the Isolate the Problem stage, troubleshooters identify the characteristics of problems at the logical layers of the network so that the most likely cause can be selected.**
- **At the Correct the Problem stage, troubleshooters correct an identified problem by implementing, testing, and documenting a solution.**

CIT 5.1—2-9

References

For additional information, refer to this resource:

- http://www.cisco.com/univercd/home/home.htm

Quiz

Use the practice items here to review what you have learned in this lesson. The correct answers are found in the Quiz Answer Key.

Q1) Which statements are true about the stages of the general troubleshooting process? (Choose two.)

A) The stages are mutually exclusive.

B) The steps must be followed closely to avoid retracing.

C) At any stage, more symptoms may need to be collected.

D) You must establish a blanket policy that covers all stages.

E) any policy made should include documenting every important piece of information.

Q2) Which describes the Gathering Symptoms stage of the general troubleshooting process?

A) determining what network components have been affected

B) implementing, testing, and documenting a solution

C) selecting the most likely cause

D) making configuration changes to the routing table

Q3) Which describes the Isolate the Problem stage of the general troubleshooting process?

A) implementing, testing, and documenting a solution

B) backing up the current configuration

C) determining what network components have been affected

D) selecting the most likely cause

Q4) Which describes the Correct the Problem stage of the general troubleshooting process?

A) determining what network components have been affected

B) implementing, testing, and documenting a solution

C) interviewing an end user

D) selecting the most likely cause

Quiz Answer Key

Q1) C, E

Relates to: Describing the General Troubleshooting Process

Q2) A

Relates to: Describing the Gathering Symptoms Stage

Q3) D

Relates to: Describing the Isolate the Problem Stage

Q4) B

Relates to: Describing the Correct the Problem Stage

Gathering Symptoms

Overview

In the lesson "Describing a General Troubleshooting Process," you learned the general troubleshooting process. The first stage of the process is where the troubleshooter gathers symptoms of the problem. By gathering symptoms, a troubleshooter builds a knowledge base about potential reasons for a problem. In this lesson, you will learn how to gather symptoms from network devices, end users, and end systems.

Relevance

When troubleshooters jump to conclusions, their assumptions can be their worst enemy. When you gather symptoms, you create a complete description of a problem. With an incomplete view of the problem, you can jump to erroneous conclusions and spend wasted time and resources on things that have nothing to do with the problem at hand. The time you spend gathering symptoms allows you to spend less time randomly trying solutions. When you diagnose and fix problems in your network, you must gather a complete list of symptoms before attempting a correction.

Objectives

Upon completing this lesson, you will be able to:

- Gather symptoms from network devices to complete a list of network symptoms
- Gather hardware and software symptoms from user feedback to complete a list of symptoms at the end system
- Gather data at the end system to complete a list of hardware and software symptoms displayed at the end system

Learner Skills and Knowledge

To benefit fully from this lesson, you must have these prerequisite skills and knowledge:

- Familiarity with layered model troubleshooting approaches
- Familiarity with the Cisco IOS commands covered in the Cisco *Building Scalable Cisco Internetworks* (BSCI), *Building Cisco Multilayer Switched Networks* (BCMSN), and *Building Cisco Remote Access Networks* (BCRAN) courses

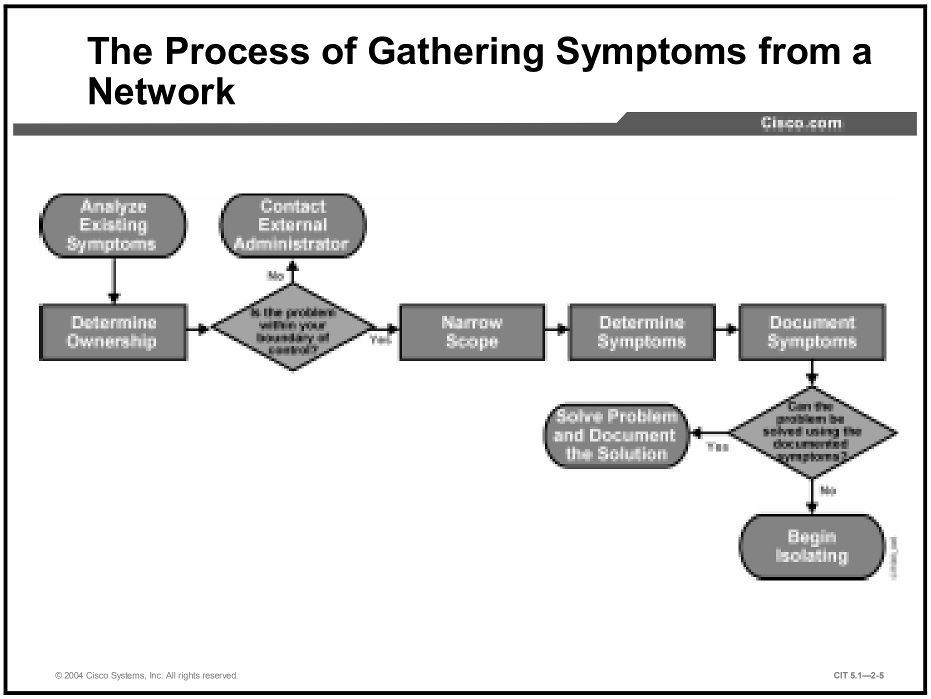
Outline

This lesson includes these topics:

- Overview
- Gathering Network Symptoms
- Gathering User Symptoms
- Gathering End-System Symptoms
- Summary
- Quiz

Gathering Network Symptoms

This topic describes the process that troubleshooters use to gather symptoms from network devices.



The Process of Gathering Symptoms from a Network

Cisco.com
Analyze Existing Symptoms
Contact External Administrator
No
Determine Ownership
Is the problem within your boundary of control?
Yes
Narrow Scope
Determine Symptoms
Document Symptoms
Can the problem be solved using the documented symptoms?
Yes
Solve Problem and Document the Solution
No
Begin Isolating

CIT 5.1—2-5

The table describes each of the stages in the process of gathering network symptoms that troubleshooters can use.

The Process of Gathering Network Symptoms

Stage	Description
Stage 1: Analyze Existing Symptoms	To get a description of the problem, troubleshooters analyze any gathered symptoms from the trouble ticket or from any users or end systems affected by the problem.
Stage 2: Determine Ownership	If the problem is in the system that troubleshooters are responsible for, they move on to Stage 3. If the problem is outside their boundary of control, troubleshooter should stop gathering network symptoms and contact an administrator for the external system.
Stage 3: Narrow Scope	Troubleshooters determine if the problem is at the core, distribution, or access layer of their network. At the identified layer, troubleshooters use their analysis of existing symptoms and knowledge of the network topology to determine which piece or pieces of equipment are the most likely culprits.
Stage 4: Determine Symptoms	Using a layered troubleshooting approach, troubleshooters gather hardware and software symptoms from the suspect devices. Troubleshooters start with the most likely culprit and use knowledge and experience to determine if the problem is more likely a hardware or software configuration problem. ■ When gathering symptoms for perceived hardware problems, troubleshooters should physically inspect the devices using their sense of hearing, sight, smell, and touch. ■ When gathering symptoms for perceived software configuration problems, troubleshooters should use Cisco IOS commands to check the status of various aspects of the problem devices. Troubleshooters should use what they have learned about the problem to determine which aspects of the configuration to inspect.
Stage 5: Document Symptoms	Troubleshooters should document any hardware or software symptoms. If the problem can be solved using the documented symptoms, a troubleshooter will solve the problem and document the solution. If the problem cannot be solved, the troubleshooter begins the isolating phase of the general troubleshooting process.

The table lists Cisco IOS commands that a troubleshooter uses to gather symptoms about a network.

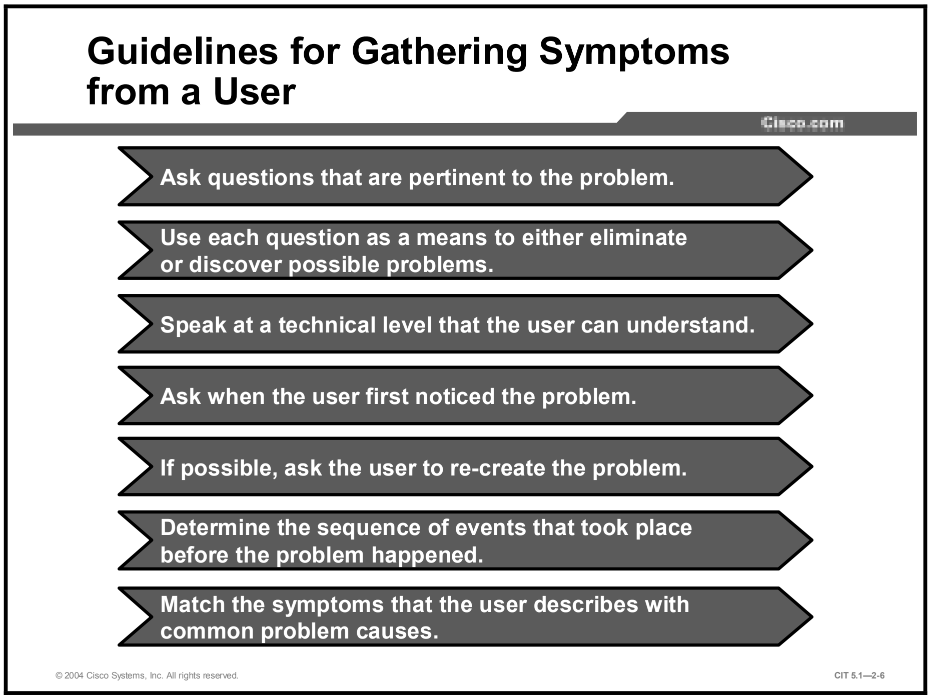
Cisco IOS Commands for Gathering Network Symptoms

Command	Description
ping *{host | ip-address}*	Sends an echo request packet to an address, then waits for a reply. The *host* | *ip-address* variable is the IP alias or IP address of the target system.
traceroute *[destination]*	Identifies the path a packet takes through the network. The *destination* variable is the hostname or IP address of the target system.
telnet *{host | ip-address}*	Connects to an IP address using the Telnet application.
show interface status	Displays the status of all interfaces on a device.
show ip interface brief	Displays a summary of the status of all interfaces on a device.
show ip route	Displays the current state of the IP routing table.
show running-config interface	Displays the contents of the current running configuration file.
[no] debug ?	Displays a list of options for enabling or disabling debugging events on a device.

Note Be prudent with your use of the **debug** command on a network. It may increase CPU utilization to a level at which the performance of a network device can be noticeably affected. Be sure to disable debugging when you no longer need its capabilities.

Gathering User Symptoms

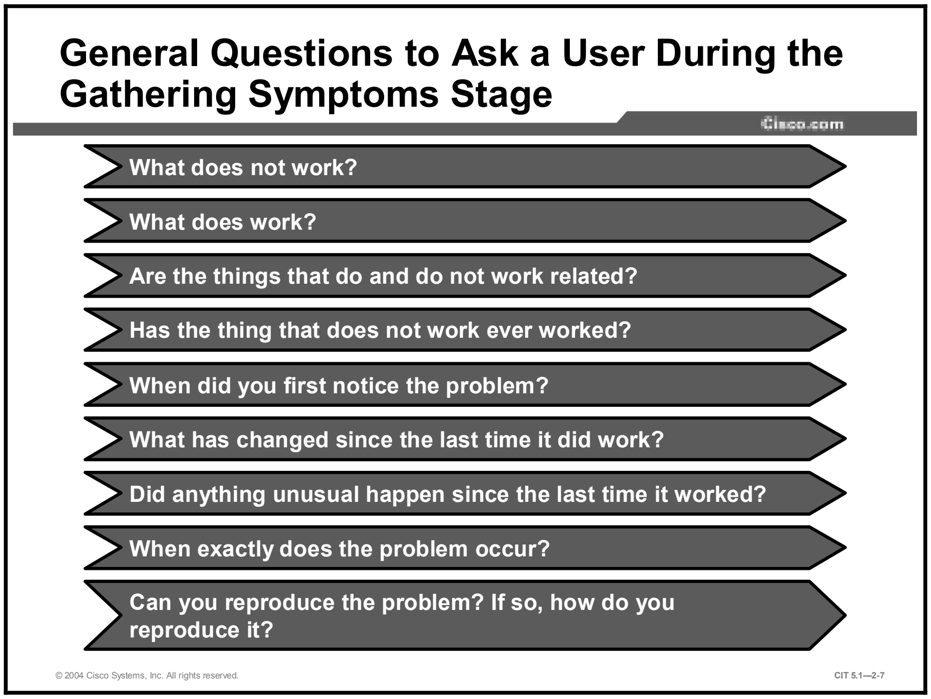
This topic discusses guidelines that troubleshooters use for effectively gathering symptoms from users.



Guidelines for Gathering Symptoms from a User

- Ask questions that are pertinent to the problem.
- Use each question as a means to either eliminate or discover possible problems.
- Speak at a technical level that the user can understand.
- Ask when the user first noticed the problem.
- If possible, ask the user to re-create the problem.
- Determine the sequence of events that took place before the problem happened.
- Match the symptoms that the user describes with common problem causes.

CIT 5.1—2-6



General Questions to Ask a User During the Gathering Symptoms Stage

- What does not work?
- What does work?
- Are the things that do and do not work related?
- Has the thing that does not work ever worked?
- When did you first notice the problem?
- What has changed since the last time it did work?
- Did anything unusual happen since the last time it worked?
- When exactly does the problem occur?
- Can you reproduce the problem? If so, how do you reproduce it?

CIT 5.1—2-7

Example: Gathering Network Symptoms from the End User

A user calls you claiming inability in "getting to the Internet." Through asking questions, you learn that the user first noticed the problem within the last 20 minutes. You ask the user to try to re-create the problem by opening a browser and attempting to reach an Internet site. The connection cannot be made and the user gets a "Cannot Reach Server or DNS Error" message. The user states that this was already tried and the only site that the user can successfully reach is the site run by the department in which the user works.

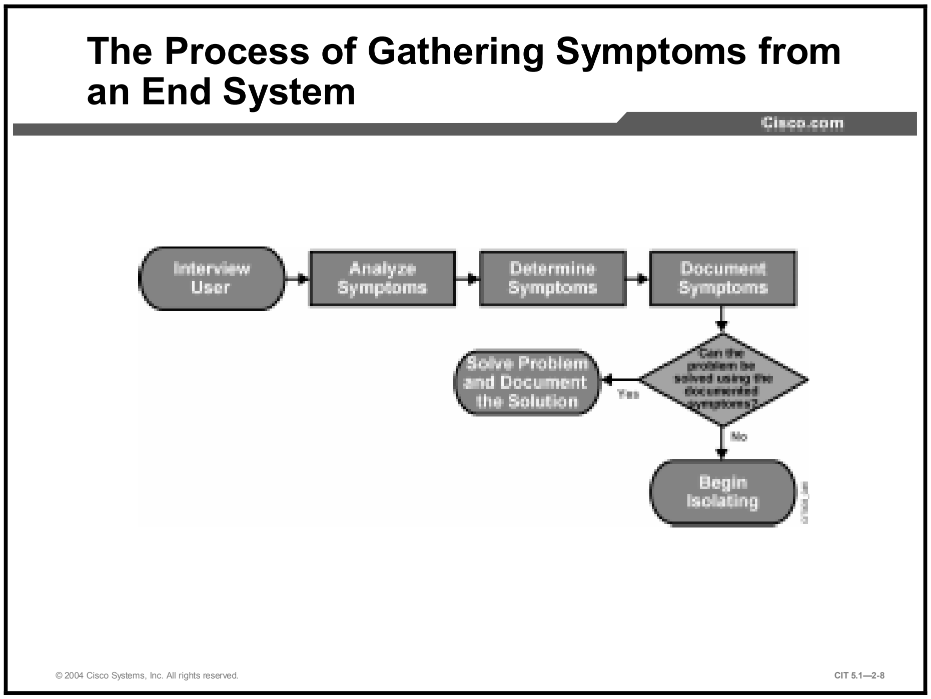
Considering this a key fact, you ask if the site is on the company LAN. The user becomes confused because the user does not know what a LAN is. Trying a different approach, you ask if it is an intranet site. The user says, "Yes, at least that is what my boss calls it." Knowing that the user can reach local servers, but not anything outside of the company network, you suspect that routing may be the issue.

Feeling confident that the gateway router is operating correctly, you try to determine the sequence of events that took place before the problem arose by asking if the user has recently accessed the network settings in the Control Panel. This is something the user, stating to you, does not know, but a little while ago was checking out the preferences for the browser and "clicked on some stuff." The user does not think anything important was changed, though. Hearing this, you make a visit to the user and discover that the address for the default gateway has indeed been removed.

Your use of an effective interviewing technique allowed you to come up with a clear description of the problem. The next step will either be to use the gathered symptoms to correct the problem or to begin the isolating phase.

Gathering End-System Symptoms

This topic describes the process that troubleshooters use for gathering symptoms from end systems.



The Process of Gathering Symptoms from an End System

Cisco.com

Interview User

Analyze Symptoms

Determine Symptoms

Document Symptoms

Can the problem be solved using the documented symptoms?

Yes

Solve Problem and Document the Solution

No

Begin Isolating

© 2004 Cisco Systems, Inc. All rights reserved.

CIT 5.1—2-8

Note This course focuses on troubleshooting network connectivity. You may need to seek help from external vendors or workstation and server administrators to effectively troubleshoot problems at end systems.

The table describes each of the stages in the process of gathering network symptoms.

The Process of Gathering Symptoms from End Systems

Stage	Description
Stage 1: Interview User	If possible, troubleshooters gather initial symptoms from the user and use those symptoms as a platform to gather at the end system.
Stage 2: Analyze Symptoms	Troubleshooters will get a description of the problem by analyzing any gathered symptoms from the user.
Stage 3: Determine Symptoms	Using a layered troubleshooting approach, troubleshooters gather hardware and software symptoms from the end system, starting with the most likely culprit. Troubleshooters should rely on experience to decide if the problem is more likely a hardware or software problem. ■ When gathering symptoms for perceived hardware problems, troubleshooters should perform a physical inspection of the end system using their sense of hearing, sight, smell, and touch, starting with the most obvious symptom. Information gathered from the user will help determine the most obvious places to begin. ■ When gathering symptoms for perceived software problems, troubleshooters test the network applications on the end system. Information gathered from the user helps determine the most obvious applications to test.
Stage 4: Document Symptoms	Troubleshooters should document any hardware and software symptoms. If the problem can be solved using the documented symptoms, the troubleshooter solves the problem and documents the solution. If the problem cannot be solved at this point, the troubleshooter begins the isolating phase of the general troubleshooting process.

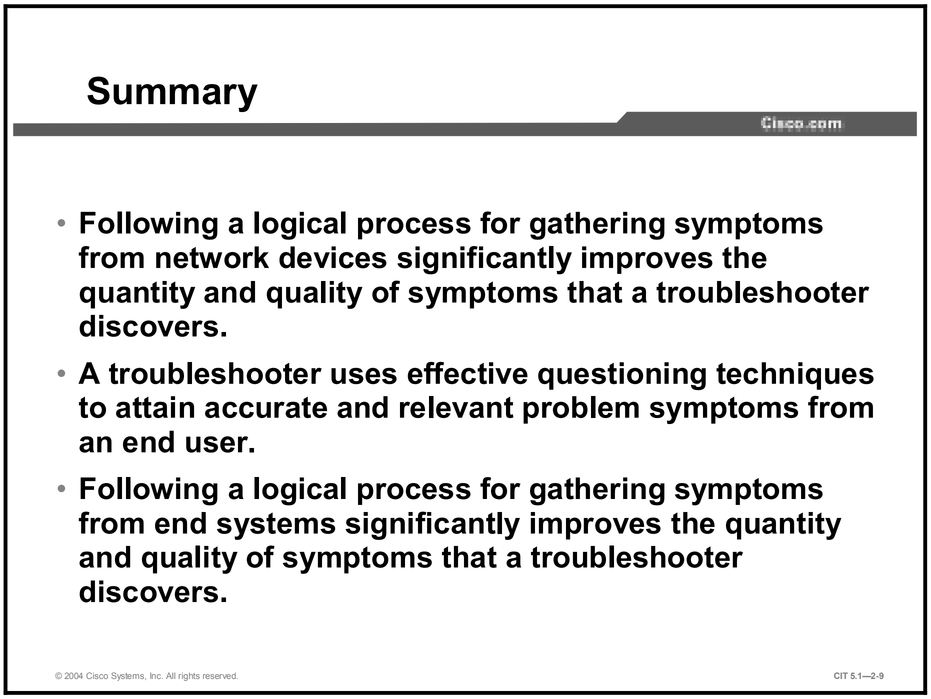
The table lists the commands that a troubleshooter uses on end systems to gather symptoms about a network.

Commands for Gathering Symptoms on End Systems

Command	Description
ping {*host* | *ip-address*}	Sends an echo request packet to an address, then waits for a reply. The *host* | *ip-address* variable is the IP alias or IP address of the target system.
telnet {*host* | *ip-address*}	Connects to an IP address or host name using the Telnet application.
Windows: **tracert** [*destination*] Mac/UNIX: **traceroute** [*destination*]	Identifies the path a packet takes through the network. The *destination* variable is the host name or IP address of the target system.
Windows: **ipconfig /all** Mac/UNIX: **ifconfig -a**	Displays information relating to the IP configuration of an end system.
arp -a	Verifies that the declared IP address for the end system is correct.
Windows: **route print** Mac/UNIX: **route -n**	Displays the contents of the entire IP routing table.
netstat -rn	Displays the status of all connected devices and links without querying a DNS server.

Summary

This topic summarizes the key points discussed in this lesson.



Summary

- Following a logical process for gathering symptoms from network devices significantly improves the quantity and quality of symptoms that a troubleshooter discovers.
- A troubleshooter uses effective questioning techniques to attain accurate and relevant problem symptoms from an end user.
- Following a logical process for gathering symptoms from end systems significantly improves the quantity and quality of symptoms that a troubleshooter discovers.

CIT 5.1—2-9

References

For additional information, refer to this resource:

- http://www.cisco.com/univercd/home/home.htm

Next Steps

For the associated case study, refer to the following section of the course Lab Guide:

- Case Study (Trouble Ticket A) 2-1: Gathering Symptoms

Quiz

Use the practice items here to review what you have learned in this lesson. The correct answers are found in the Quiz Answer Key.

Q1) Match the stage in the process of gathering network symptoms with the correct description.

A) Analyze existing symptoms

B) Determine ownership

C) Narrow scope

D) Determine symptoms

E) Document symptoms

_____ 1. Identifying whether a problem is inside or outside the boundary of control for a troubleshooter

_____ 2. Problem is either solved at this stage or troubleshooter moves on to the isolating phase

_____ 3. Determining if the problem is with the hardware or the software configuration

_____ 4. Getting a description of the problem

_____ 5. Identifying if the problem is at the core, distribution, or access layer of their network

Q2) If a user in your company network tells you that e-mail cannot be sent. What would be the most pertinent question to ask?

A) Are you using a laptop or a desktop computer?

B) Is the SMTP server correctly configured?

C) When did you first notice the problem?

D) Can you open a word processing application?

Q3) Once all of the symptoms have been gathered at an end system and the problem cannot be solved, what is the next event that should take place?

A) get a new IP address for the end system

B) replace the end system

C) begin isolating the symptoms to identify a single problem

D) reboot the end system

Quiz Answer Key

Q1) 1=B, 2=E, 3=D, 4=A, 5=C

Relates to: Gathering Network Symptoms

Q2) C

Relates to: Gathering User Symptoms

Q3) C

Relates to: Gathering End-System Symptoms

Selecting a Troubleshooting Approach

Overview

To effectively solve a problem, you must have a specific methodology to follow. In this lesson, you will learn the three main approaches to troubleshooting. You will also learn to select a suitable troubleshooting approach for the specific problem that needs to be solved based on your skill level and temperament.

Relevance

Troubleshooting is both a science and an art. There are a number of ways that you can approach a networking problem. If you have a method to follow, you will resolve the problem more quickly and cost-effectively than if you approach the problem haphazardly. It is important for you to pick an approach and stay with it; otherwise, there may be confusion, wasted time, and wasted effort, resulting in a slower, less-efficient resolution of a problem.

Objectives

Upon completing this lesson, you will be able to:

- Describe the bottom-up approach to troubleshooting using a logical layered model
- Describe the top-down approach to troubleshooting using a logical layered model
- Describe the divide-and-conquer approach to troubleshooting using a logical layered model
- Select an approach for troubleshooting network problems

Learner Skills and Knowledge

To benefit fully from this lesson, you must have these prerequisite skills and knowledge:

- Familiarity with the OSI and TCP/IP networking model concepts

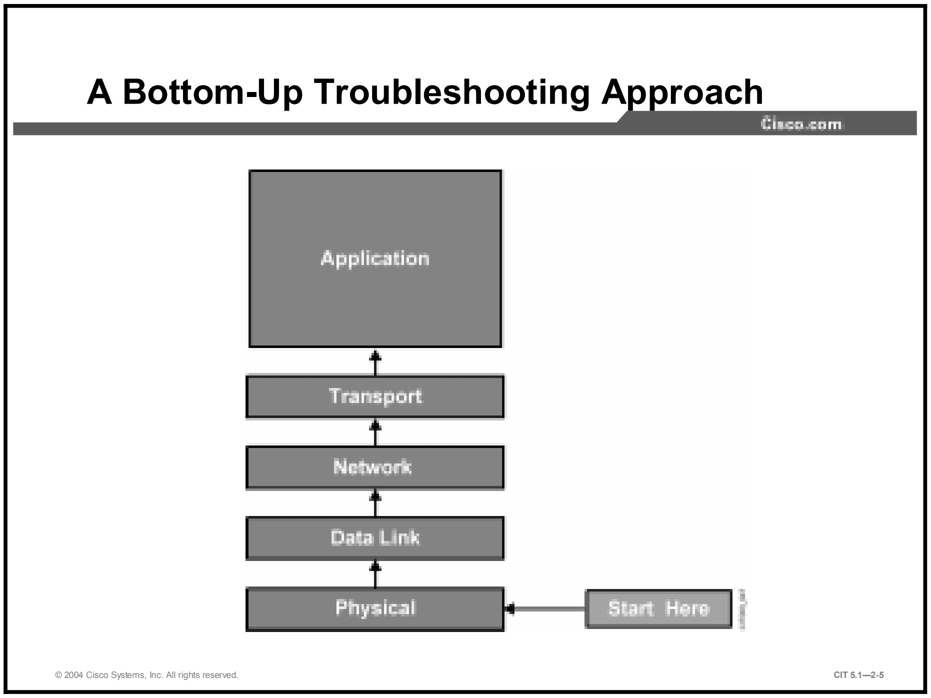
Outline

This lesson includes these topics:

- Overview
- Describing a Bottom-Up Troubleshooting Approach
- Describing a Top-Down Troubleshooting Approach
- Describing a Divide-and-Conquer Troubleshooting Approach
- Selecting a Troubleshooting Approach
- Summary
- Quiz

Describing a Bottom-Up Troubleshooting Approach

This topic describes the bottom-up approach to troubleshooting a network problem.



A Bottom-Up Troubleshooting Approach

Cisco.com

Application

Transport

Network

Data Link

Physical

Start Here

© 2004 Cisco Systems, Inc. All rights reserved.

CIT 5.1—2-5

When you apply a bottom-up approach toward troubleshooting a networking problem, you start with the physical components of the network and work your way up the layers of the OSI model until you identify the cause of the problem. It is a good approach for a troubleshooter to use when the problem is suspected to be physical. Most networking problems reside at the lower levels, so implementing the bottom-up approach will often result in effective results. This approach is also appropriate when you are troubleshooting more complex problems because you are looking at the problems from a detailed view.

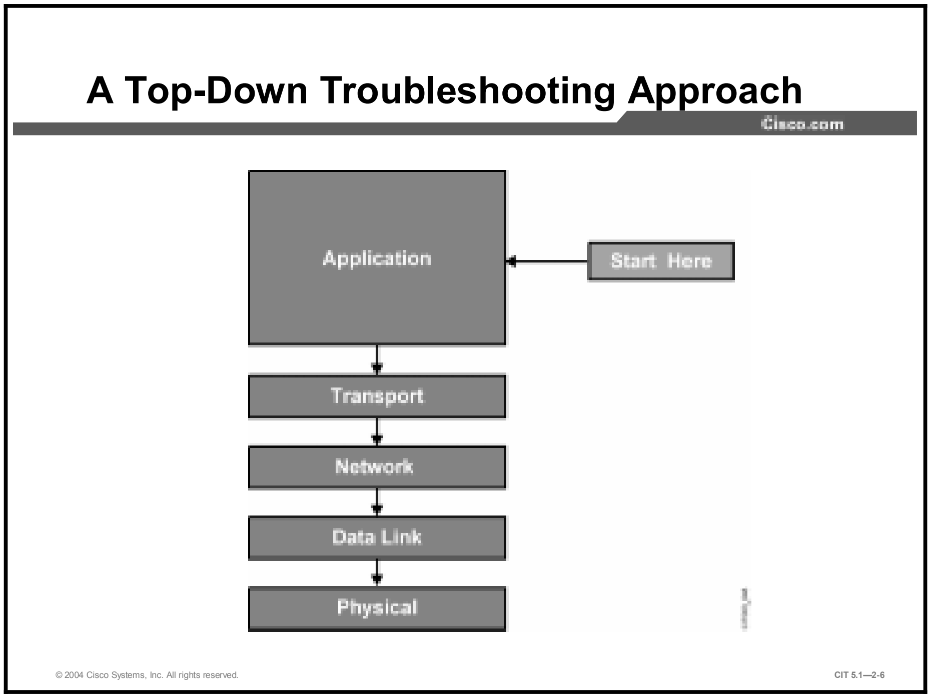
The downside to selecting this approach is that it requires you to check every device, interface, and so forth on the network until you find the possible cause of the problem and to document each conclusion and possibility. The challenge is to determine which devices to start with.

In many cases, you can determine if the problem lies within the first four layers by entering a simple **traceroute** command. If the connection is successful, the cause is likely at the application level. Otherwise, you will need to take a closer look at the lower levels to locate the problem.

Note	Be sure that Internet Control Message Protocol (ICMP) is enabled on your network for commands such as **ping** and **traceroute** to work. If ICMP is not permitted, a **ping** or **traceroute** command can easily be mistaken for a loss of connectivity.

Describing a Top-Down Troubleshooting Approach

This topic describes the top-down approach to troubleshooting a network problem.



A Top-Down Troubleshooting Approach

Cisco.com

Application

Start Here

Transport

Network

Data Link

Physical

© 2004 Cisco Systems, Inc. All rights reserved.

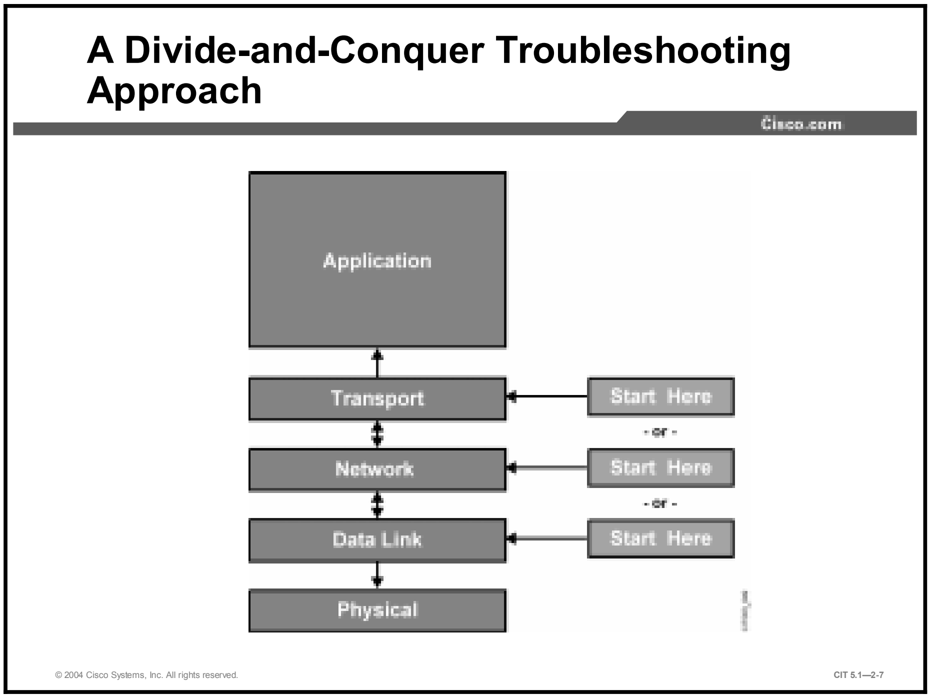
CIT 5.1—2-6

When you apply a top-down approach toward troubleshooting a networking problem, you start with the end-user application and work your way down from the upper layers of the OSI model until you have identified the cause of the problem. When you select this approach, you are directed to test the applications of an end system before tackling the more specific networking pieces. A troubleshooter would most likely select this approach for simpler problems or when the troubleshooter thinks that the problem is with a piece of software.

The disadvantage of selecting this approach is that it requires you to check and document every network application until you find the possible cause of the problem each conclusion and possibility. Like the bottom-up approach, the challenge is to determine which application to start with.

Describing a Divide-and-Conquer Troubleshooting Approach

This topic describes the divide-and-conquer approach to troubleshooting a network problem.



A Divide-and-Conquer Troubleshooting Approach

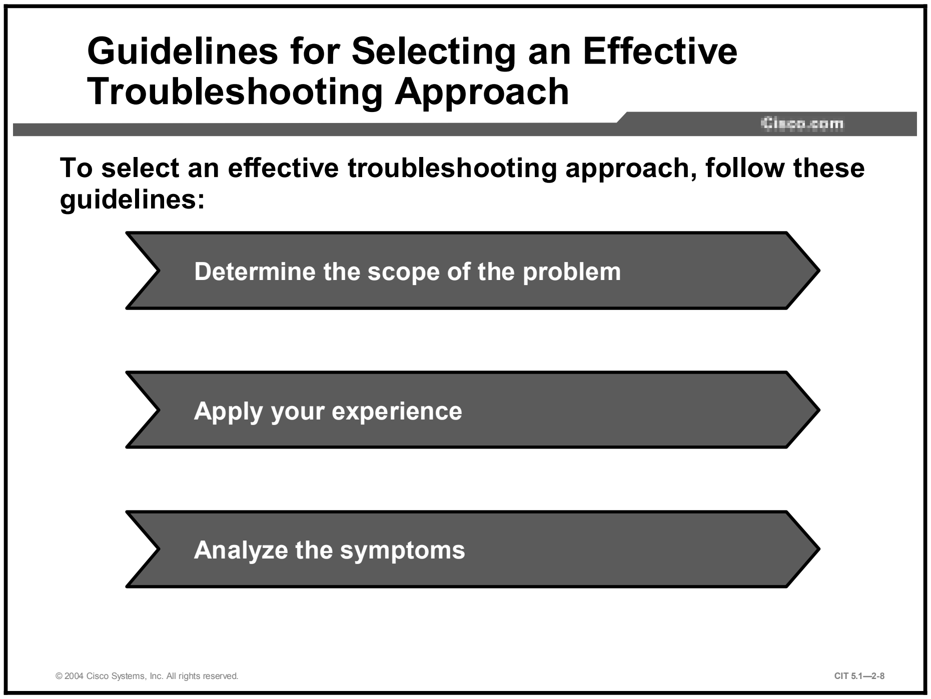
CIT 5.1—2-7

When you apply the divide-and-conquer approach toward troubleshooting a networking problem, you select a layer and test in both directions from the starting layer. You begin the divide-and-conquer approach at a particular layer based on your experience level and the symptoms that you have gathered about the problem. The Cisco IOS command set excels at allowing you to choose an intermediate level to begin troubleshooting and at identifying a direction to work toward. Once you have identified the direction of the problem, you work in that direction until you can identify the cause of the problem.

If you can verify that a layer is functioning, it is typically a safe assumption that the layers below it are functioning, as well. If a layer is not functioning properly, you should gather symptoms of the problem at that layer and work your way down.

Selecting a Troubleshooting Approach

This topic discusses guidelines for effectively selecting a troubleshooting approach.



Guidelines for Selecting an Effective Troubleshooting Approach

To select an effective troubleshooting approach, follow these guidelines:

- Determine the scope of the problem
- Apply your experience
- Analyze the symptoms

© 2004 Cisco Systems, Inc. All rights reserved. CIT 5.1—2-8

When you select an effective troubleshooting approach to solve a network problem, you resolve the problem in a quicker, more cost-effective manner.

To select an effective troubleshooting approach, follow these guidelines:

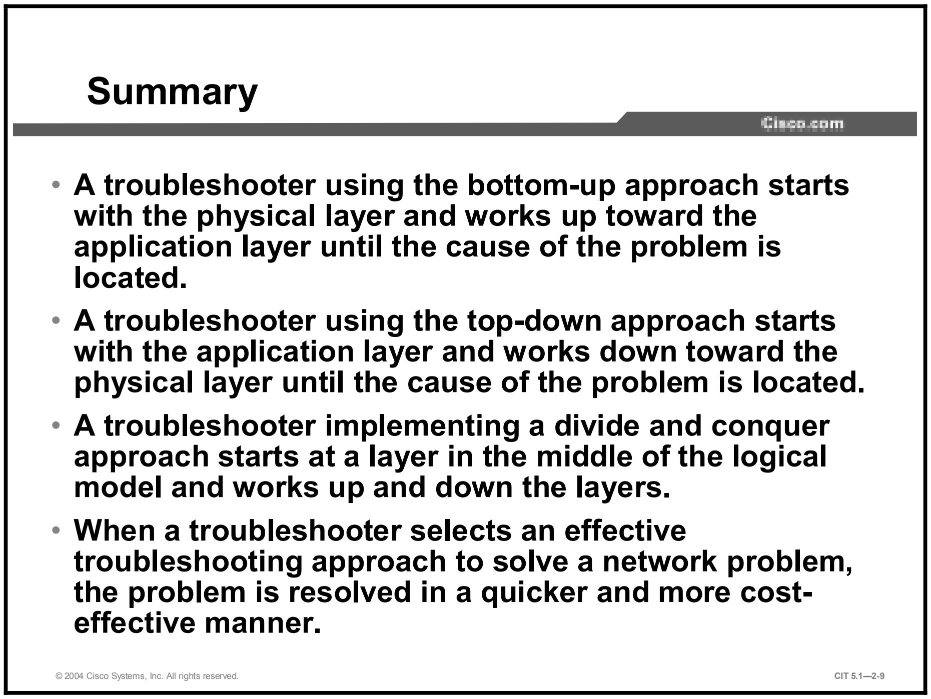
- **Determine the scope of the problem:** A troubleshooting approach is often selected based on its complexity. A bottom-up approach typically works better for complex problems. A top-down approach typically works for simple problems. Using a bottom-up approach for a simple problem may be overkill and inefficient. Typically, if symptoms come from users, you will use a top-down approach. If symptoms come from the network, a bottom-up approach will likely be more effective.
- **Apply your experience:** If you have troubleshot a particular problem previously, you may know of a way to shorten the troubleshooting process. A less-experienced troubleshooter will likely implement a bottom-up approach, while a skilled troubleshooter may be able to jump into a problem at a different layer using the divide-and-conquer approach.
- **Analyze the symptoms:** The more that you know about a problem, the better chance you have to solve it. You may find that you can immediately correct a problem simply by analyzing the symptoms.

Example: Selecting a Troubleshooting Approach

Before attempting to solve a problem, you need to select a troubleshooting approach. You are having issues with inconsistent routing behavior on your network. The symptoms are similar to those that you have seen previously and point to a likely protocol issue. Because there is connectivity between the routers, you know that it is not likely a problem at the physical or data link layer. Based on this knowledge and your past experience, you decide to use the divide-and-conquer approach, and you begin testing the TCP/IP-related functions at the network layer.

Summary

This topic summarizes the key points discussed in this lesson.



Summary

- A troubleshooter using the bottom-up approach starts with the physical layer and works up toward the application layer until the cause of the problem is located.
- A troubleshooter using the top-down approach starts with the application layer and works down toward the physical layer until the cause of the problem is located.
- A troubleshooter implementing a divide and conquer approach starts at a layer in the middle of the logical model and works up and down the layers.
- When a troubleshooter selects an effective troubleshooting approach to solve a network problem, the problem is resolved in a quicker and more cost-effective manner.

CIT 5.1—2-9

References

For additional information, refer to this resource:

- http://www.cisco.com/univercd/home/home.htm

Quiz

Use the practice items here to review what you have learned in this lesson. The correct answers are found in the Quiz Answer Key.

Q1) What is an example of a problem that would take place at the network level of the bottom-up approach to troubleshooting?

A) An interface malfunctions.

B) A routing loop occurred.

C) A router heat sink needed to be replaced.

D) The duplex setting of a port is incorrectly set.

Q2) If you have exhausted the possibility of the problem occurring in all but the final level of the top-down troubleshooting approach, which layer are you concerned with?

A) physical

B) data link

C) transport

D) application

Q3) Using a divide-and-conquer approach, which layer would you begin with if you isolated the problem to an access list on a router?

A) physical

B) data link

C) network

D) application

Q4) The power of the Cisco IOS command set encourages which troubleshooting approach?

A) bottom-up

B) top-down

C) divide-and-conquer

Quiz Answer Key

Q1) B

Relates to: Describing a Bottom-Up Troubleshooting Approach

Q2) A

Relates to: Describing a Top-Down Troubleshooting Approach

Q3) C

Relates to: Describing a Divide and Conquer Troubleshooting Approach

Q4) C

Relates to: Selecting a Troubleshooting Approach

Lesson Assessments

Overview

Use the lesson assessments here to test what you have learned in this module. The correct answers and solutions are found in the Lesson Assessment Answer Key.

Outline

This section includes these assessments:

- Quiz 2-1: Describing a General Troubleshooting Process
- Quiz 2-2: Selecting a Troubleshooting Approach

Quiz 2-1: Describing a General Troubleshooting Process

Complete this quiz to assess what you learned in the lesson.

Objectives

This assessment tests your knowledge of how to:

- Describe the general troubleshooting process
- Describe the Gathering Symptoms stage of the general troubleshooting process
- Describe the Isolate the Problem stage of the general troubleshooting process
- Describe the Correct the Problem stage of the general troubleshooting process

Quiz

Answer these questions:

Q1) Which stage of the general troubleshooting process are you in if you are testing the network to ensure that you have not introduced an additional problem?

A) Gathering Symptoms
B) Isolating the Problem
C) Correcting the Problem

Q2) Which step in the general troubleshooting process involves interviewing a user?

A) Gathering Symptoms
B) Isolating the Problem
C) Correcting the Problem

Q3) Given three possible causes of a network problem, you enter commands that help you decide which one is most likely the cause of the problem. Which step in the general troubleshooting process are you performing?

A) Gathering Symptoms
B) Isolating the Problem
C) Correcting the Problem

Scoring

You have successfully completed the quiz for this lesson when you earn a score of 100 percent.

Quiz 2-2: Selecting a Troubleshooting Approach

Complete this quiz to assess what you learned in the lesson.

Objectives

This assessment tests your knowledge of how to:

- Describe the bottom-up approach to troubleshooting using a logical layered model
- Describe the top-down approach to troubleshooting using a logical layered model
- Describe the divide and conquer approach to troubleshooting using a logical layered model
- Select an approach to troubleshooting network problems

Quiz

Answer these questions:

Q1) At which layer of the OSI model does the bottom-up approach to troubleshooting begin?

A) application

B) data link

C) network

D) physical

Q2) Using the divide and conquer troubleshooting approach, you decide to begin troubleshooting a TCP/IP problem at the network layer. You determine that the network layer is working properly. Based on this knowledge, which of the following layers is not assumed to be working properly?

A) physical layer

B) data link layer

C) transport layer

Q3) You have isolated a problem to be an encapsulation type mismatch between point-to-point serial interfaces (data link layer). Given this problem, which troubleshooting approach would be the least effective?

A) bottom-up

B) top-down

C) divide-and-conquer

Q4) A user has reported that a certain application does not run from the user's end system. You know that there are no filters applied that would prevent the application from working. Running a **traceroute** command verifies that a connection exists between the end system of the user and the application server. Applying a layered approach to troubleshooting, which layer should you troubleshoot next?

A) physical

B) network

C) data link

D) application

Q5) If you know that a user can access some resources, but not others, which layer is the least likely culprit?

A) physical

B) network

C) transport

D) application

Q6) Which troubleshooting approach is most appropriate to implement if the problem is located at the network interface?

A) bottom-up

B) top-down

C) divide-and-conquer

Q7) Which one of the following is a problem that would occur at the first level of the top-down troubleshooting approach?

A) The PortFast setting on a port is incorrectly set to OFF

B) The STP state on an interface was incorrectly set to FORWARD.

C) A jabbering port was identified.

D) An FTP client application was found to be corrupt.

Scoring

You have successfully completed the quiz for this lesson when you earn a score of 80 percent or better.

Lesson Assessment Answer Key

Quiz 2-1: The General Troubleshooting Process

Q1) C

Q2) A

Q3) B

Quiz 2-2: Selecting a Troubleshooting Approach

Q1) D

Q2) C

Q3) B

Q4) D

Q5) A

Q6) A

Q7) D

Module 3

Resolving Problems at the Physical and Data Link Layers

Overview

Once you have gathered the symptoms of a problem and selected a troubleshooting approach, the next step is to use those symptoms to isolate the problems and perform the necessary steps to correct them. In this module, you will perform the isolation and correction phases of the general troubleshooting process to resolve network optimization and failure problems at the physical and data link layers of the Open Systems Interconnection (OSI) model.

Module Objectives

Upon completing this module, you will be able to:

- Isolate problems occurring at the physical and data link layers
- Correct problems occurring at the physical and data link layers

Module Outline

The module contains these components:

- Isolating the Problem
- Correcting the Problem

Isolating the Problem

Overview

As a troubleshooter, you use symptoms to narrow problems to a single problem or to a small set of related problems. These symptoms help you to direct your troubleshooting efforts.

The physical and data link layers are very closely related. This close relationship often makes isolating a problem difficult for a troubleshooter. In this lesson, you will use specific characteristics and commands to isolate failures of media, devices, and software at the physical and data link layers of networks.

Relevance

All of the upper layers of the OSI model depend on the media, devices, and software operating at the physical and data link layers to function. Effectively isolating and correcting failures and suboptimal conditions at these lower layers is vital.

Objectives

Upon completing this lesson, you will be able to:

- Identify the symptoms of problems occurring at the physical layer
- Identify the symptoms of problems occurring at the data link layer
- Analyze command and application output to isolate problems occurring at the physical and data link layers
- Isolate problems occurring at the physical and data link layers

Learner Skills and Knowledge

To benefit fully from this lesson, you must have these prerequisite skills and knowledge:

- The ability to apply layered model troubleshooting approaches
- Familiarity with Cisco command syntax and technologies covered in the Cisco *Building Scalable Cisco Internetworks* (BSCI), *Building Cisco Multilayer Switched Networks* (BCMSN), and *Building Cisco Remote Access Networks* (BCRAN) courses

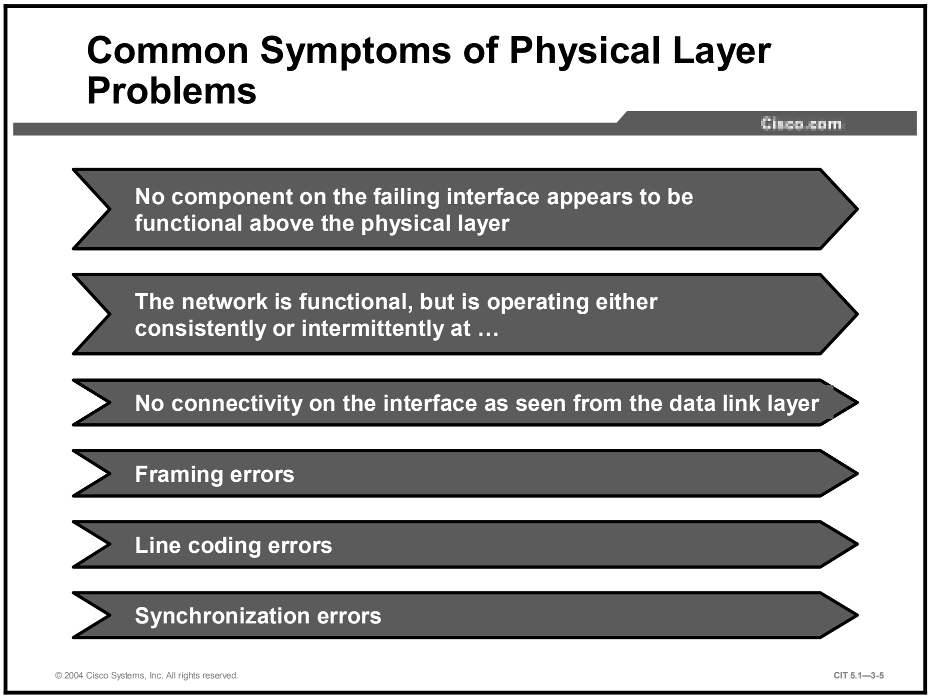
Outline

This lesson includes these topics:

- Overview
- Identifying the Symptoms of Problems Occurring at the Physical Layer
- Identifying the Symptoms of Problems Occurring at the Data Link Layer
- Analyzing Commands and Applications Used to Isolate Problems Occurring at the Physical and Data Link Layers
- Isolating Problems Occurring at the Physical and Data Link Layers
- Summary
- Quiz

Identifying the Symptoms of Problems Occurring at the Physical Layer

This topic identifies symptoms of problems that occur at the physical layer that troubleshooters should be able to identify.



Common Symptoms of Physical Layer Problems

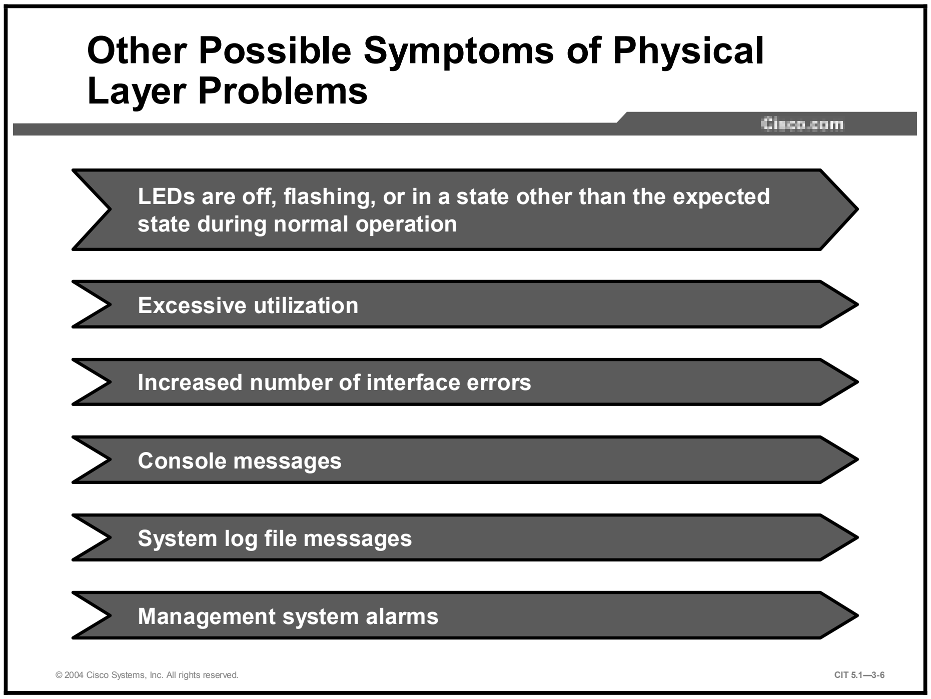
- No component on the failing interface appears to be functional above the physical layer
- The network is functional, but is operating either consistently or intermittently at …
- No connectivity on the interface as seen from the data link layer
- Framing errors
- Line coding errors
- Synchronization errors

© 2004 Cisco Systems, Inc. All rights reserved. CIT 5.1—3-5

Troubleshooting problems at the physical layer is distinctly different from troubleshooting problems at higher layers. This is because the physical layer is the only layer with physically tangible components, such as cables, interfaces, and antennas.

When you have a physical layer failure, you experience either an intermittent or consistent loss of connectivity across that link. This condition will cause data to transfer at less than the expected data rate. After you log in to the device where the link terminates and start gathering symptoms, you will see that no network component above the physical layer is communicating with peer components on systems connected through the failed interface or media.

Other common symptoms of physical layer problems include the appearance of errors relating to framing, line coding, and synchronization.



Other Possible Symptoms of Physical Layer Problems

- LEDs are off, flashing, or in a state other than the expected state during normal operation
- Excessive utilization
- Increased number of interface errors
- Console messages
- System log file messages
- Management system alarms

CIT 5.1—3-6

Symptoms of a physical layer problem that you may encounter include console and management messages and system log files. Perhaps the first time you know that you have a problem is when a device shows console messages indicating that an area of the network is not functioning. For example, a console message for a failing interface may display the following:

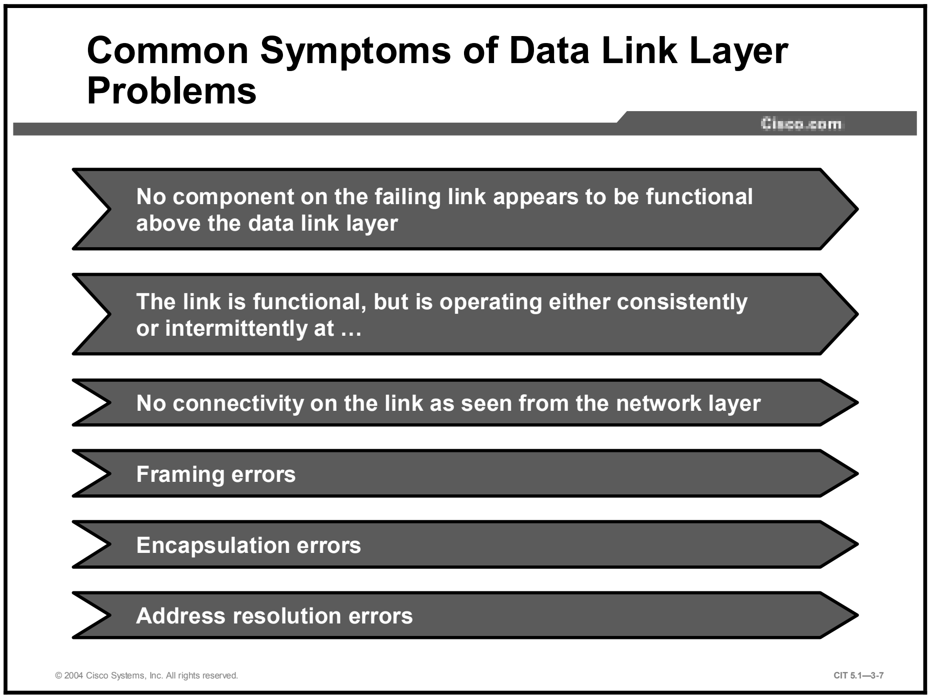
```
Feb 12 9:22:37: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Serial1/0, changed state to down
```

Viewing the LEDs of a device usually gives you reliable feedback for diagnosing the operational status of a device. When troubleshooting the physical status of a device, you will find that the LEDs of a failing device are in a state other than the state that you are supposed to see during normal operation. The changed state of the LED could be off, flashing, or some variation in color.

A device may have a problem at the physical layer because more traffic is being directed to the interface than it can serve. When troubleshooting this type of problem, you may find that the interface is operating at or near the maximum capacity, and you may have an increase in the number of interface errors. As you gather information, the problematic interface reveals excessive runts, late collisions, loss of framing, or an increase in the number of buffer failures. The output from a **ping** or **traceroute** command reports excessive packet loss or latency.

Identifying the Symptoms of Problems Occurring at the Data Link Layer

This topic identifies the symptoms of problems a troubleshooter would look for at the data link layer.



Common Symptoms of Data Link Layer Problems

Cisco.com

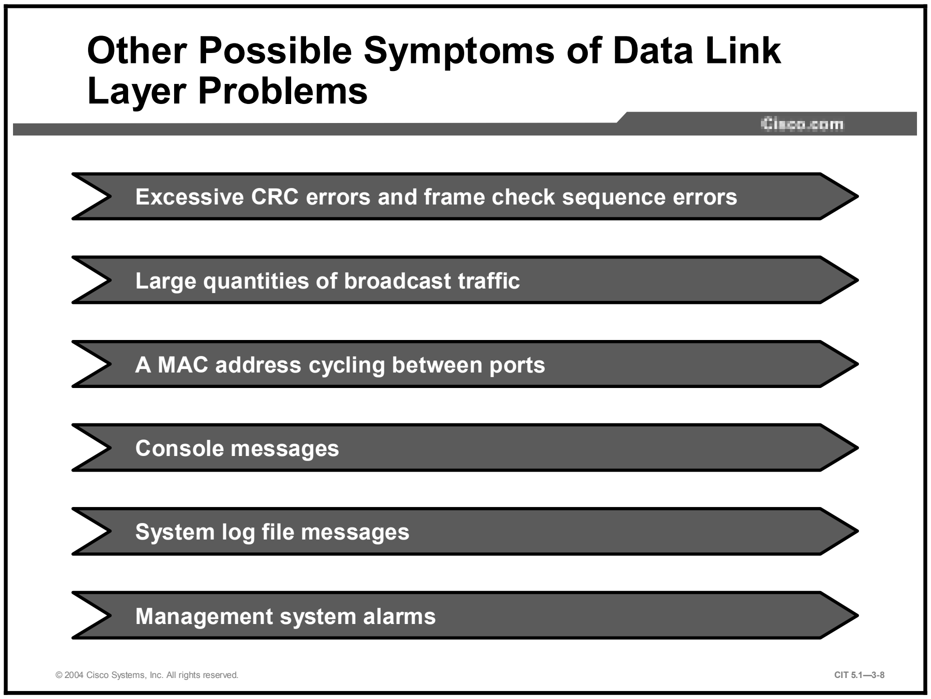
- No component on the failing link appears to be functional above the data link layer
- The link is functional, but is operating either consistently or intermittently at …
- No connectivity on the link as seen from the network layer
- Framing errors
- Encapsulation errors
- Address resolution errors

© 2004 Cisco Systems, Inc. All rights reserved. CIT 5.1—3-7

A data link problem occurs when the data link layer fails to manage data transfer, to correct the transmission errors of bits across a physical connection, or to properly encapsulate or de-encapsulate packets for the network layer. Troubleshooting a data link failure problem requires you to verify the operation and accuracy of hardware addresses, address resolution protocol (ARP) caches, repeaters, bridges, and switches.

Devices experiencing a problem at the data link layer have physical connectivity, but will not transfer data through the failed interface. Troubleshooting with a **ping** or **traceroute** command may produce packet loss, and no keepalives will be sent or received on the interface. No protocol operating at a layer above the data link layer will communicate with peers on systems connected only through the failed interface.

Data link optimization problems are arguably the least likely to be seen by a troubleshooter. Data link layer optimization problems occur when the physical aspects of a data connection are functioning; however, the rate of data flow is substandard because of the improper configuration or failure of data link layer components. Like suboptimal problems at the physical layer, data layer optimization issues result in either consistent or intermittent periods of degraded data flow.



Other Possible Symptoms of Data Link Layer Problems

- Excessive CRC errors and frame check sequence errors
- Large quantities of broadcast traffic
- A MAC address cycling between ports
- Console messages
- System log file messages
- Management system alarms

CIT 5.1—3-8

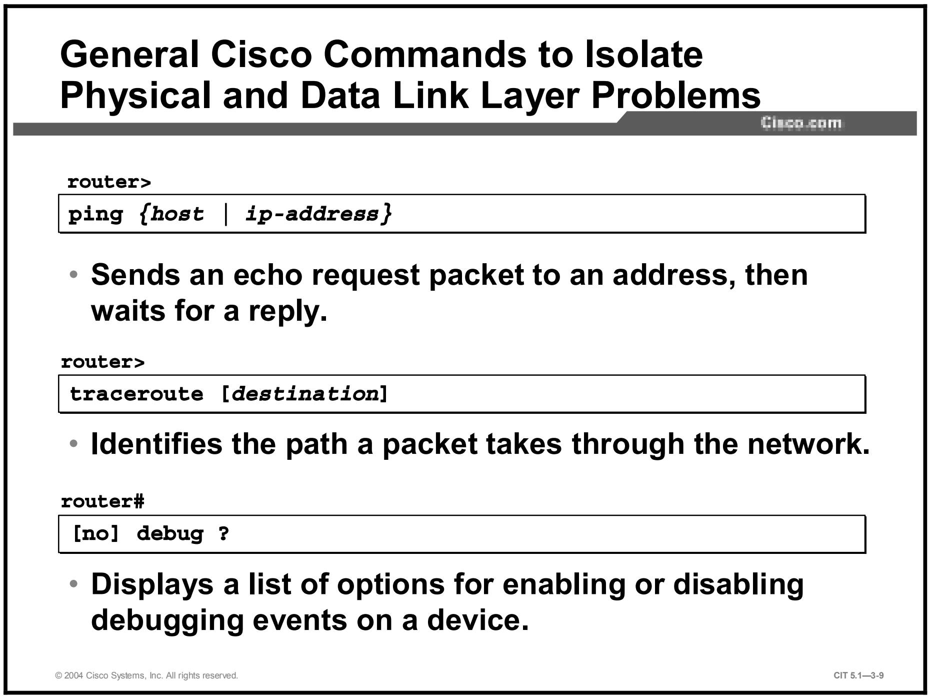
If the problem is at the data link layer, console messages on the affected device may indicate that Cisco Discovery Protocol (CDP) messages are not being sent between neighboring Cisco equipment. Also, if the problem is at the data link layer and not the physical layer, entering the **show interfaces** command will indicate that the interface is “up,” but the line protocol is “down.” For example, a **show interfaces** command for a failing interface may display one of these messages:

```
router1>show interfaces
Ethernet0/0 is up, line protocol is down


router2>show interfaces
Serial0/0 is up, line protocol is down
```

Symptoms that may be present during the suboptimal performance of data link layer components include excessive cyclic redundancy check (CRC) errors and frame check sequence (FCS) errors. Through console messages, you may also discover large quantities of broadcast traffic that indicate this type of problem.

Analyzing Commands and Applications Used to Isolate Problems Occurring at the Physical and Data Link Layers

This topic analyzes the output of commands and applications to help troubleshooters isolate a problem at the physical or data link layer.



General Cisco Commands to Isolate Physical and Data Link Layer Problems

Cisco.com

```
router>
ping {host | ip-address}
```

- **Sends an echo request packet to an address, then waits for a reply.**

```
router>
traceroute [destination]
```

- **Identifies the path a packet takes through the network.**

```
router#
[no] debug ?
```

- **Displays a list of options for enabling or disabling debugging events on a device.**

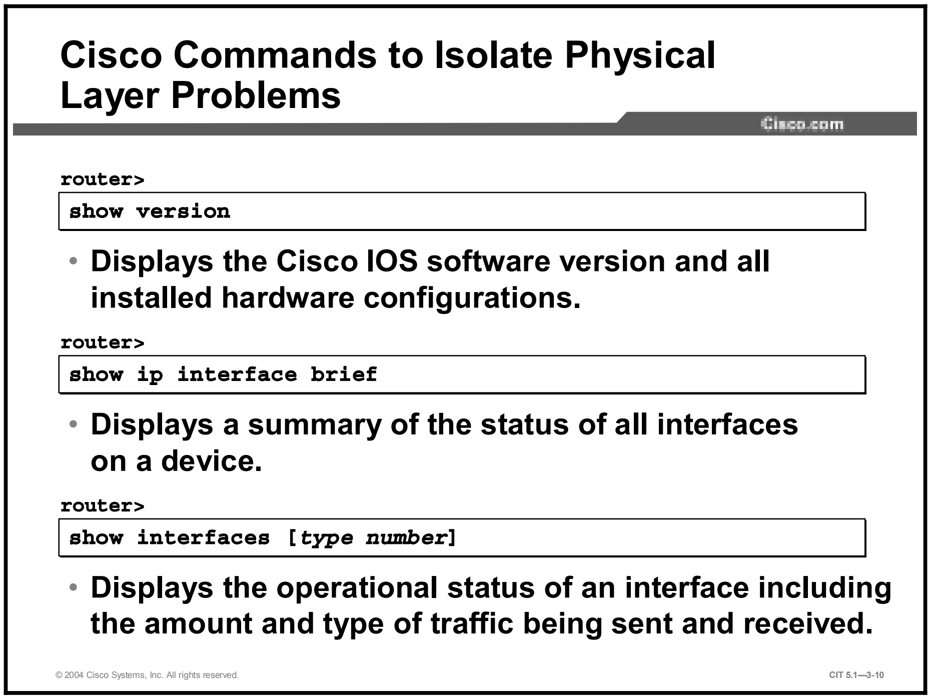
© 2004 Cisco Systems, Inc. All rights reserved.

CIT 5.1—3-9

The Cisco commands listed in the table display information about several networking layers. A troubleshooter uses the information from these commands to isolate problems at the physical and data link layers.

Cisco IOS Commands to Isolate General Physical and Data Link Layer Problems

Command	Description
ping *{host | ip-address}*	(User or Privileged) Sends an echo request packet to an address, then waits for a reply. The *host|ip-address* variable is the IP alias or IP address of the target system.
traceroute [*protocol*] [*destination*]	(User or Privileged) Identifies the path a packet takes through the network. The default protocol is IP, and the default *destination* variable is the IP alias or IP address of the target system. Protocols that can be used are **appletalk**, **clns**, **ip** and **vines**. Based on the destination address or host name on the command line, the default parameters for the appropriate protocol are assumed and the tracing action begins.
[**no**] **debug ?**	Displays a list of options for enabling or disabling debugging events on a device.



Cisco Commands to Isolate Physical Layer Problems

```
router>
show version
```

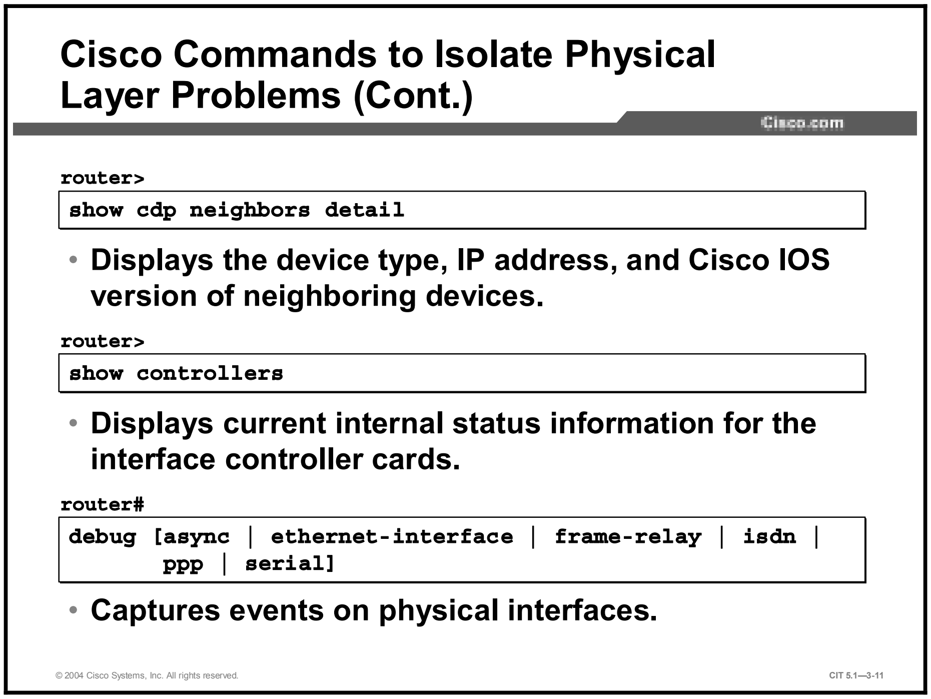
- Displays the Cisco IOS software version and all installed hardware configurations.

```
router>
show ip interface brief
```

- Displays a summary of the status of all interfaces on a device.

```
router>
show interfaces [type number]
```

- Displays the operational status of an interface including the amount and type of traffic being sent and received.



Cisco Commands to Isolate Physical Layer Problems (Cont.)

```
router>
show cdp neighbors detail
```

- Displays the device type, IP address, and Cisco IOS version of neighboring devices.

```
router>
show controllers
```

- Displays current internal status information for the interface controller cards.

```
router#
debug [async | ethernet-interface | frame-relay | isdn |
       ppp | serial]
```

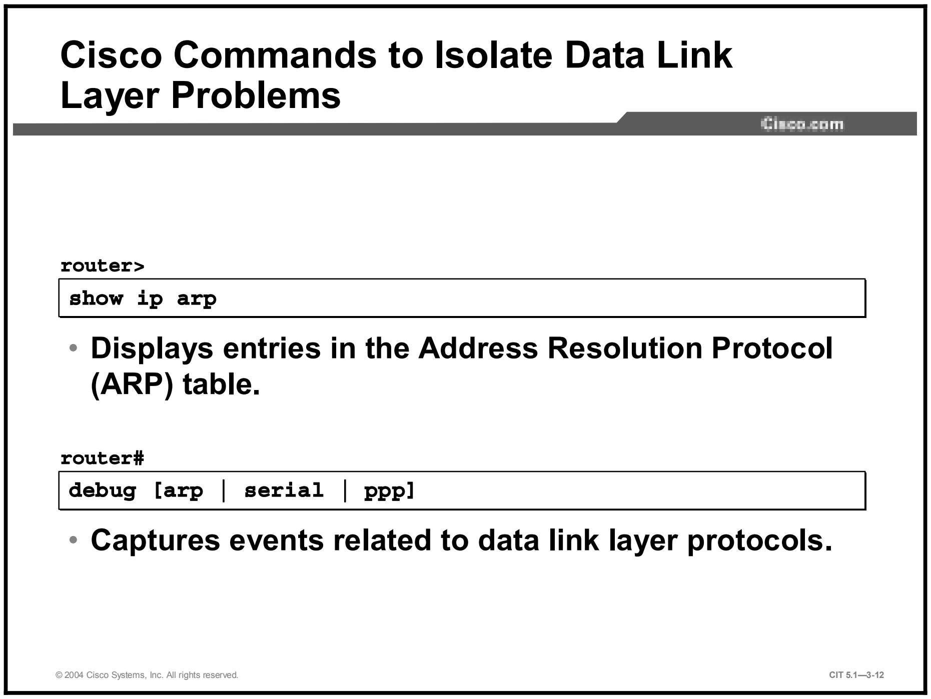
- Captures events on physical interfaces.

The table lists several Cisco IOS commands that a troubleshooter uses to display information about several networking layers; however, are important for isolating problems at the physical layer.

Cisco Commands to Isolate Physical Layer Problems

Command	Description
show version	Displays the Cisco IOS software version and all installed hardware configurations.
show ip interface brief	Displays a summary of the status of all interfaces on a device.
show interfaces [*type number*]	Displays the operational status of an interface and also the amount and type of traffic being sent and received.
show cdp neighbors detail	Displays the device type and Cisco IOS version of neighboring devices.
show controllers	Displays current internal status information for the interface controller cards.
debug [**async** | **ethernet-interface** | **frame-relay** | **isdn** | **ppp** | **serial**]	Captures events on physical interfaces.

Note The **show** command displays a snapshot of the current characteristics of the network device interface or protocol. The **debug** command displays the events taking place from the time the command is entered until reporting is disabled. Using **debug** commands places more of a negative impact on the performance of a networking device than isolating a problem with **show** commands. Therefore, it is a good idea to isolate a problem using only **show** commands when possible. If the information returned from entering **show** commands does not help you isolate a problem, use **debug** commands that target what you feel is the most likely cause of the problem.



Cisco Commands to Isolate Data Link Layer Problems

```
router>
show ip arp
```

- Displays entries in the Address Resolution Protocol (ARP) table.

```
router#
debug [arp | serial | ppp]
```

- Captures events related to data link layer protocols.

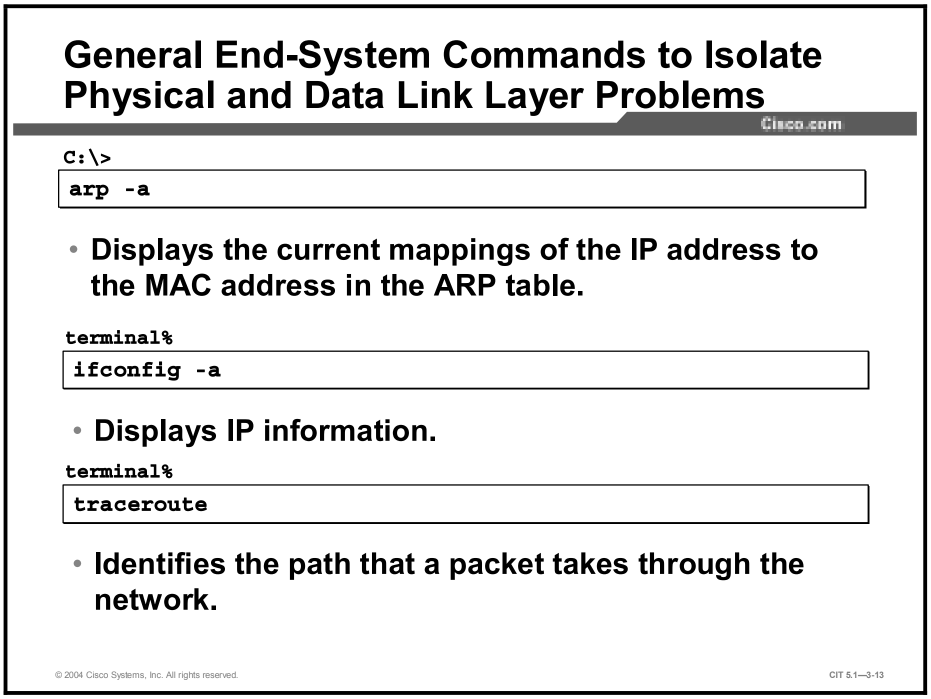
CIT 5.1—3-12

The table list several Cisco IOS commands that a troubleshooter uses to display information about several networking layers; however, are important for isolating problems at the data link layer.

Cisco Commands to Isolate Data Link Layer Problems

Command	Description
show ip arp	Displays entries in the ARP table.
debug [**arp** | **serial** | **ppp**]	Captures events related to data link layer protocols.

Note Not all of the commands listed are available on some versions of Cisco operating systems. To determine which commands are available for use with your devices, consult the online documentation for Cisco devices at http://www.cisco.com/univercd/home/home.htm.



General End-System Commands to Isolate Physical and Data Link Layer Problems

```
C:\>
arp -a
```

- Displays the current mappings of the IP address to the MAC address in the ARP table.

```
terminal%
ifconfig -a
```

- Displays IP information.

```
terminal%
traceroute
```

- Identifies the path that a packet takes through the network.

© 2004 Cisco Systems, Inc. All rights reserved. CIT 5.1—3-13

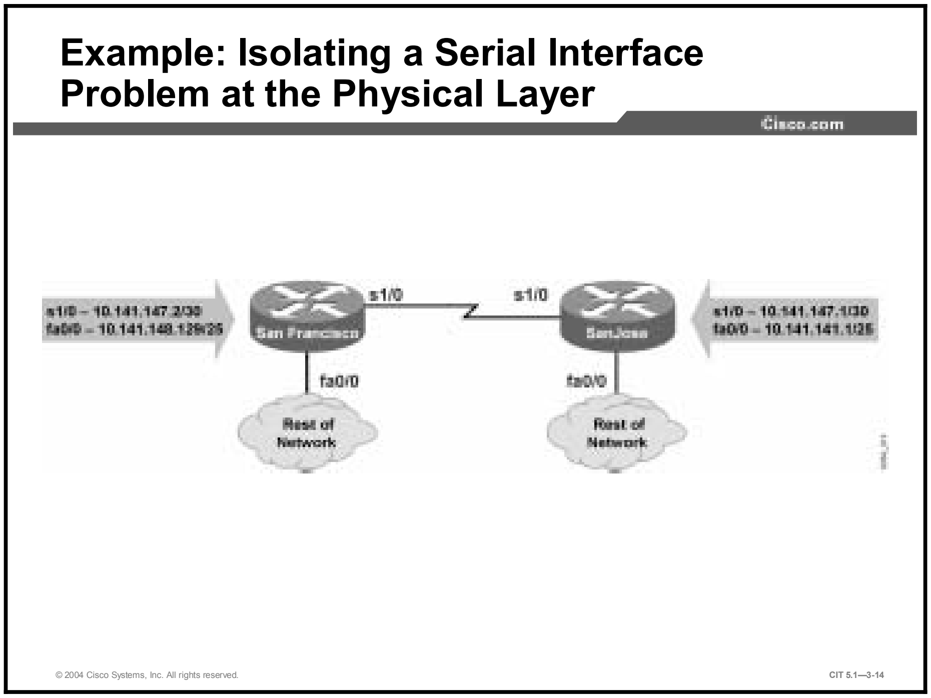
The table shows commands that a troubleshooter uses to isolate problems at the physical and data link layers. Although many of these commands display information that concerns the network layer, the commands are noteworthy at the physical and data link layers because they highlight problems in the interface between the data link and network layers. Note that the commands covered previously in the course appear in this table, but not in the related slides.

General End-System Commands to Isolate Physical and Data Link Layer Problems

Command	Description
ping *{host* | *ip-address}*	Sends an echo request packet to an address, then waits for a reply. The *host* | *ip-address* variable is the IP alias or IP address of the target system.
arp –a	Displays the current mappings of the IP address to the MAC address in the ARP table for hosts running Windows NT/2000/XP.
netstat -rn	Displays the routing table in numeric form without querying a Domain Name System (DNS) server for hosts running Windows NT/2000/XP.
ipconfig [**/all**]	Displays IP information for hosts running Windows NT/2000/XP.
tracert [**-d**] [*destination*]	Determines a path to a destination device for Windows hosts. The *destination* variable is the IP alias or IP address of the target system.
winipcfg	Displays IP information for hosts running Windows 9x and Me.
ifconfig -a	Displays IP information for UNIX and Mac OS X hosts.
traceroute [*destination*]	Identifies the path a packet takes through the network for UNIX and Mac OS X hosts. The destination variable is the hostname or IP address of the target system.

Example: Isolating Serial Interface Problems at the Physical Layer

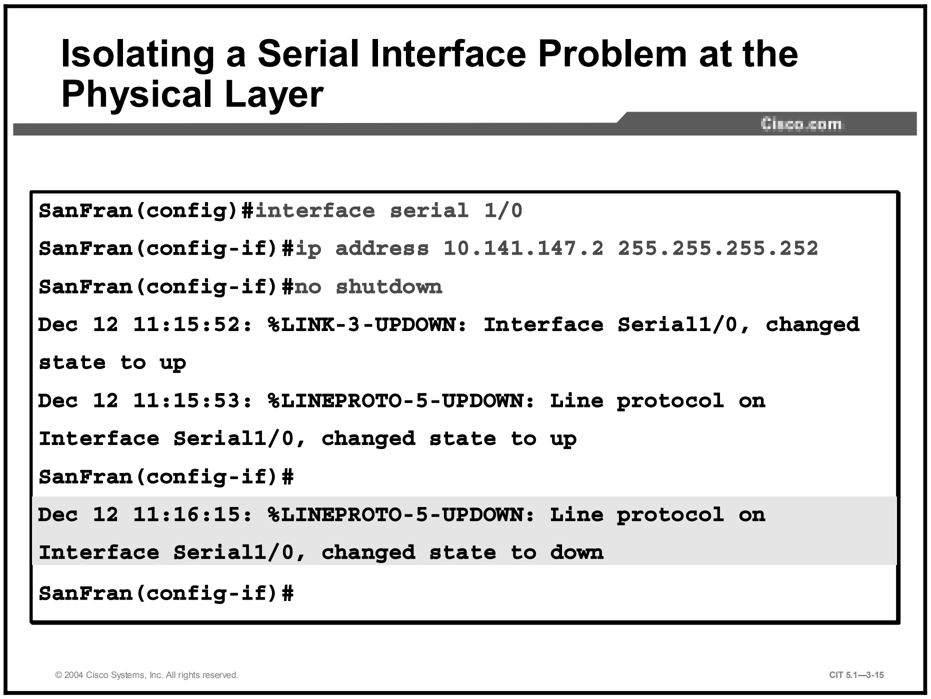
You and an associate are connecting a router named SanFran to a router named SanJose across a serial link. You have connectivity to the console port on SanFran through your PC, and to the console port on SanJose through a dial-up modem.



Example: Isolating a Serial Interface Problem at the Physical Layer

CIT 5.1—3-14

Your associate recently configured the Serial 1/0 interface on SanJose with the IP address 10.141.147.1 / 30. You need to configure the Serial 1/0 interface on SanFran with IP address 10.141.147.2 / 30. While configuring SanFran, you observe the console message in the figure.



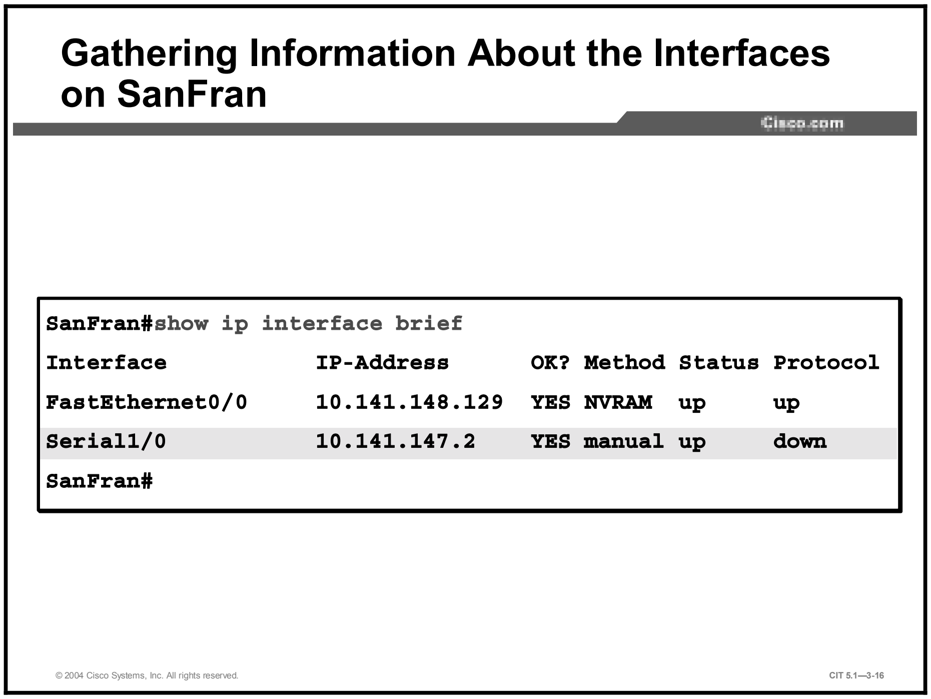
Isolating a Serial Interface Problem at the Physical Layer

```
SanFran(config)#interface serial 1/0
SanFran(config-if)#ip address 10.141.147.2 255.255.255.252
SanFran(config-if)#no shutdown
Dec 12 11:15:52: %LINK-3-UPDOWN: Interface Serial1/0, changed
state to up
Dec 12 11:15:53: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Serial1/0, changed state to up
SanFran(config-if)#
Dec 12 11:16:15: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Serial1/0, changed state to down
SanFran(config-if)#
```

CIT 5.1—3-15

The "line protocol down" message indicates that there is a problem with the interface preventing it from functioning properly.

To isolate the problem and confirm that the system message is not a transient message, you decide to use a Cisco **show** command that will display a summary of the status of the interface. Entering the **show ip interface brief** command shows that the interface named Serial 1/0 is "up," but that the line protocol is "down."

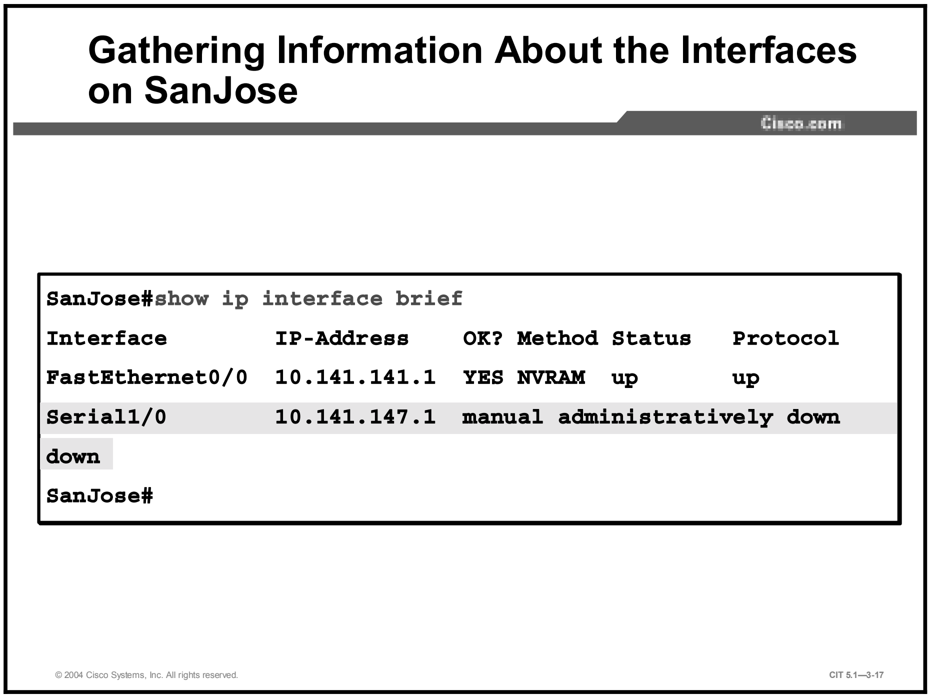


Gathering Information About the Interfaces on SanFran

```
SanFran#show ip interface brief
Interface          IP-Address      OK? Method Status Protocol
FastEthernet0/0    10.141.148.129  YES NVRAM  up     up
Serial1/0          10.141.147.2    YES manual up     down
SanFran#
```

CIT 5.1—3-16

To continue isolating the problem, you use your dial-up modem to connect to the console session on SanJose. There you use the **show ip interface brief** command.



Gathering Information About the Interfaces on SanJose

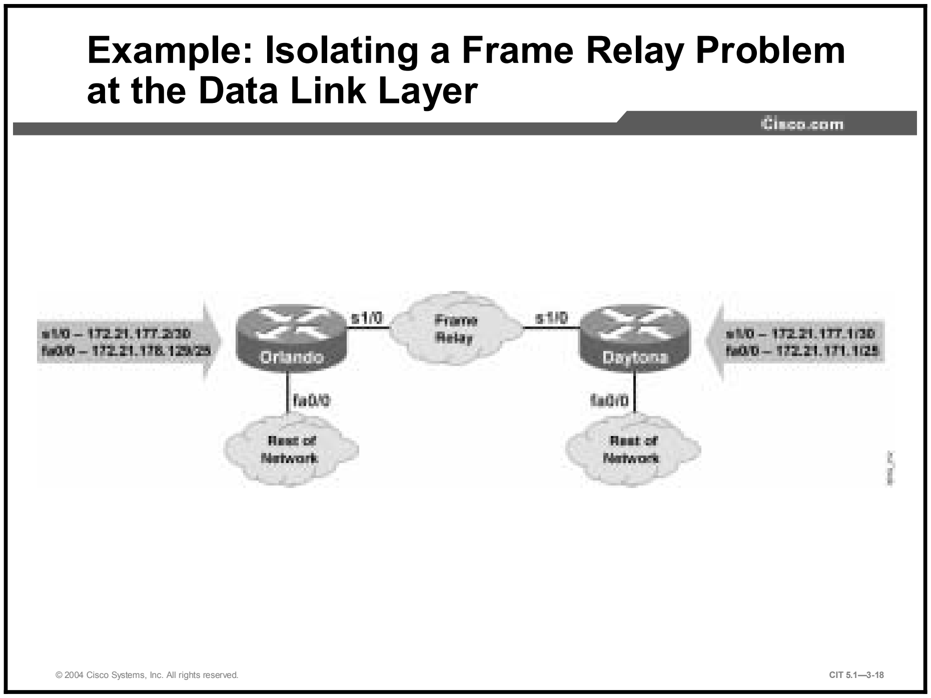
```
SanJose#show ip interface brief
Interface        IP-Address    OK? Method Status   Protocol
FastEthernet0/0  10.141.141.1  YES NVRAM  up       up
Serial1/0        10.141.147.1  manual administratively down
down
SanJose#
```

CIT 5.1—3-17

The output of this command shows that interface Serial 1/0 on SanJose is “administratively down,” or that the interface is not configured to be active. The line protocol is also in a “down” state. For Cisco routers, the default interface state of a router with no configuration information is “shutdown.” Your associate forgot to activate the interface when it was configured. To fix this problem, you will need to activate the interface.

Example: Isolating Frame Relay Problems at the Data Link Layer

You are the network engineer for a router named Orlando. Orlando uses Frame Relay to connect to a router named Daytona. You have connectivity to the console port on Orlando through a terminal server and a dial-up modem on your PC.

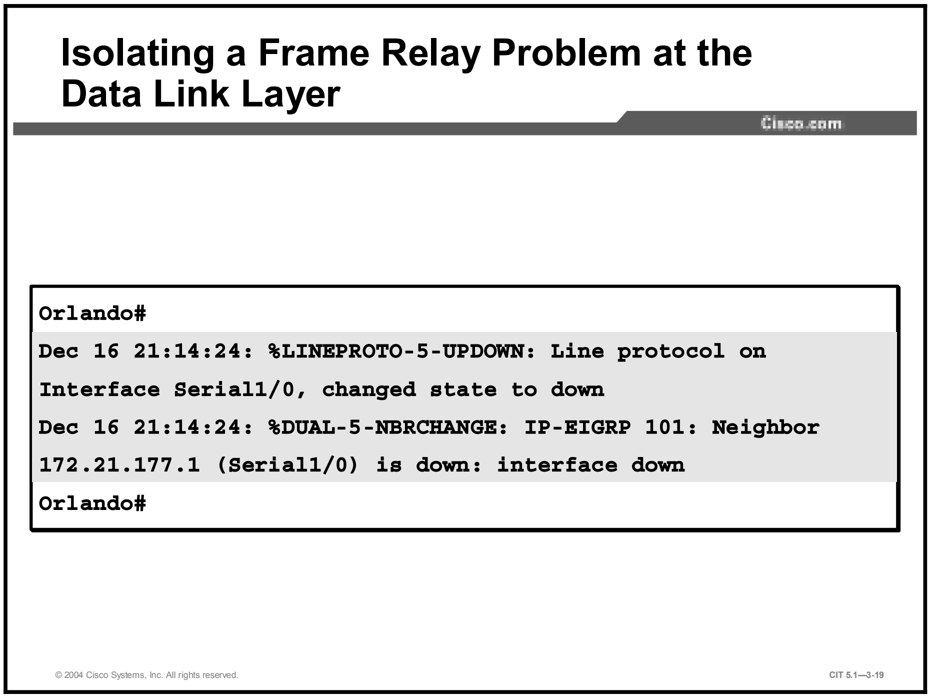


Example: Isolating a Frame Relay Problem at the Data Link Layer

CIT 5.1—3-18

Your network is stable, and you have not made any changes. One night, Network Operations calls you to tell you that the link to Daytona is down. You ask if anyone had made changes to the configuration of Orlando. Network Operations says that it made no changes. Your contact also tells you that the users in Daytona are complaining that they cannot connect to anyone in Orlando.

Network Operations says that it saw the following console message on Orlando during a check of the logs.



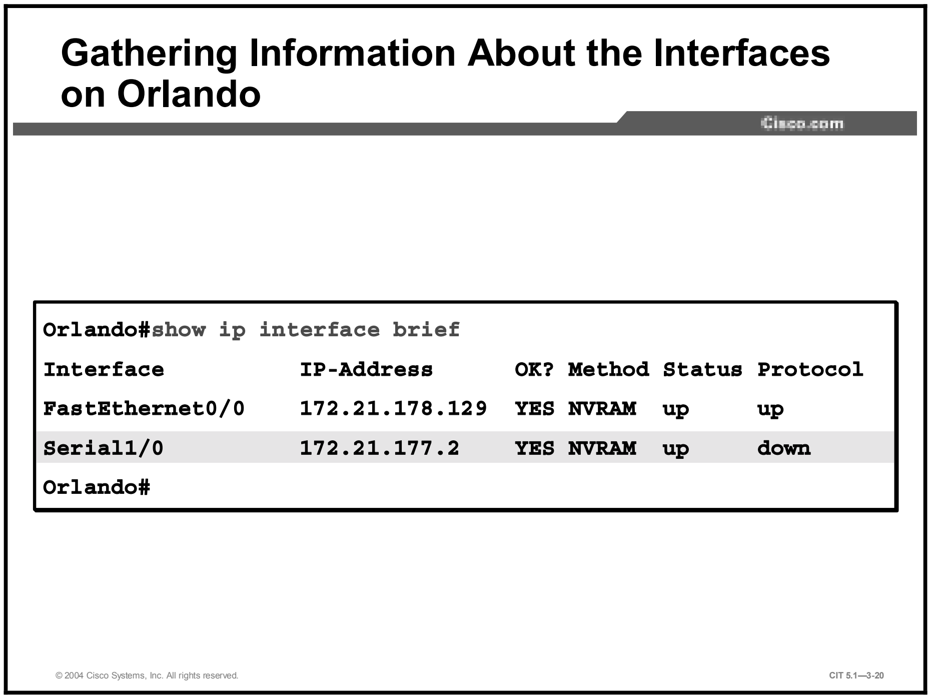
Isolating a Frame Relay Problem at the Data Link Layer

```
Orlando#
Dec 16 21:14:24: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Serial1/0, changed state to down
Dec 16 21:14:24: %DUAL-5-NBRCHANGE: IP-EIGRP 101: Neighbor
172.21.177.1 (Serial1/0) is down: interface down
Orlando#
```

CIT 5.1—3-19

The "line protocol down" message is an indication that there is a problem with the interface at the data link layer preventing it from functioning properly. When the line protocol goes down, Enhanced Interior Gateway Routing Protocol (EIGRP) neighbor adjacencies will become inoperable on that interface.

To start problem isolation, you connect to the console port on Orlando and use the **show ip interface brief** command to look for interface status. The output of this command shows that interface Serial 1/0 on Orlando is “up,” but the line protocol is “down.”



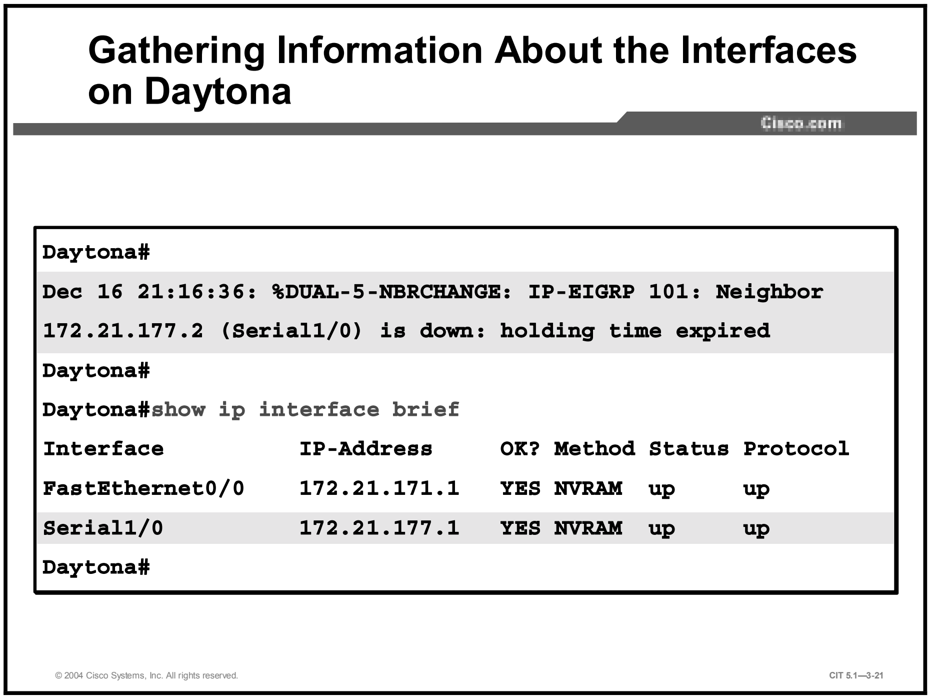
Gathering Information About the Interfaces on Orlando

```
Orlando#show ip interface brief
Interface          IP-Address      OK? Method Status Protocol
FastEthernet0/0    172.21.178.129  YES NVRAM  up     up
Serial1/0          172.21.177.2    YES NVRAM  up     down
Orlando#
```

CIT 5.1—3-20

You call Network Operations in Daytona and ask your contact to use the **show ip interface brief** command to display the interface status and any recent console messages. Your contact at Network Operations reads a recent console message stating that the hold time for the EIGRP neighbor has expired.

Your contact at Network Operations tells you that the output of the **show ip interface brief** command on Daytona shows that interface Serial 1/0 on Daytona is “up” and the line protocol is “up.”

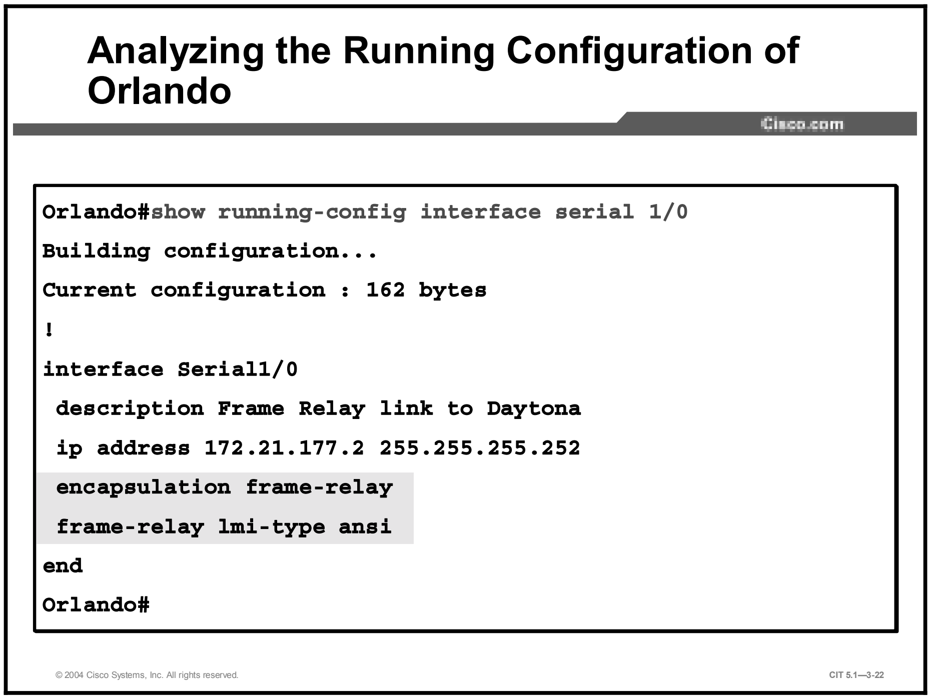


Gathering Information About the Interfaces on Daytona

```
Daytona#
Dec 16 21:16:36: %DUAL-5-NBRCHANGE: IP-EIGRP 101: Neighbor
172.21.177.2 (Serial1/0) is down: holding time expired
Daytona#
Daytona#show ip interface brief
Interface          IP-Address     OK? Method Status Protocol
FastEthernet0/0    172.21.171.1   YES NVRAM  up     up
Serial1/0          172.21.177.1   YES NVRAM  up     up
Daytona#
```

CIT 5.1—3-21

The problem appears to be on your device, so you return to your console session on Orlando for further problem isolation. You display specific interface configuration information with the **show running-config interface serial 1/0** command.



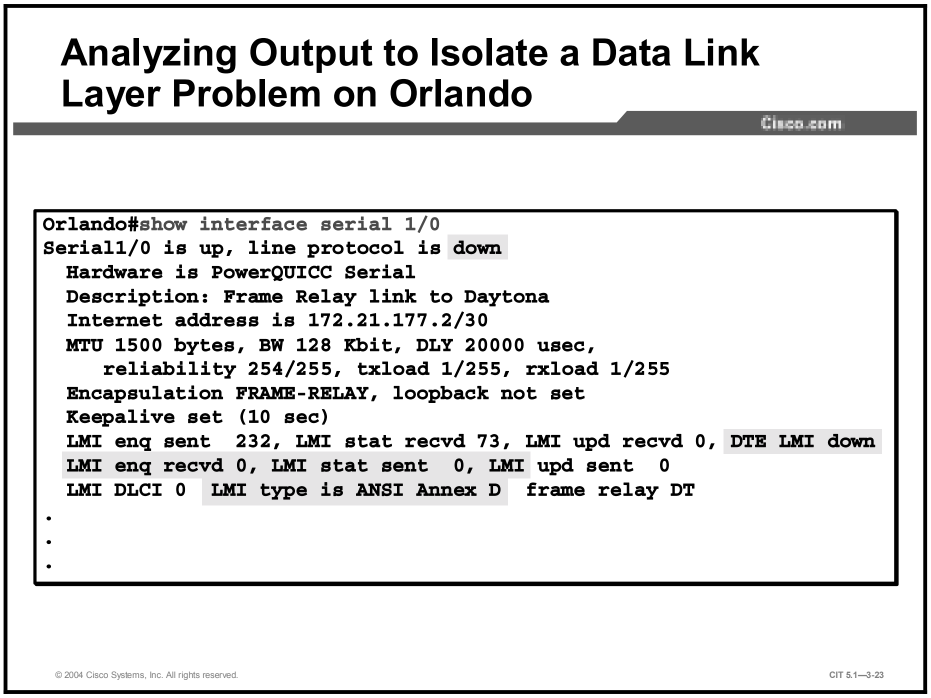
Analyzing the Running Configuration of Orlando

```
Orlando#show running-config interface serial 1/0
Building configuration...
Current configuration : 162 bytes
!
interface Serial1/0
 description Frame Relay link to Daytona
 ip address 172.21.177.2 255.255.255.252
 encapsulation frame-relay
 frame-relay lmi-type ansi
end
Orlando#
```

CIT 5.1—3-22

The configuration indicates that the interface has Frame Relay encapsulation and is expecting an American National Standards Institute (ANSI) Local Management Interface (LMI) type. This output matches your baseline configuration information.

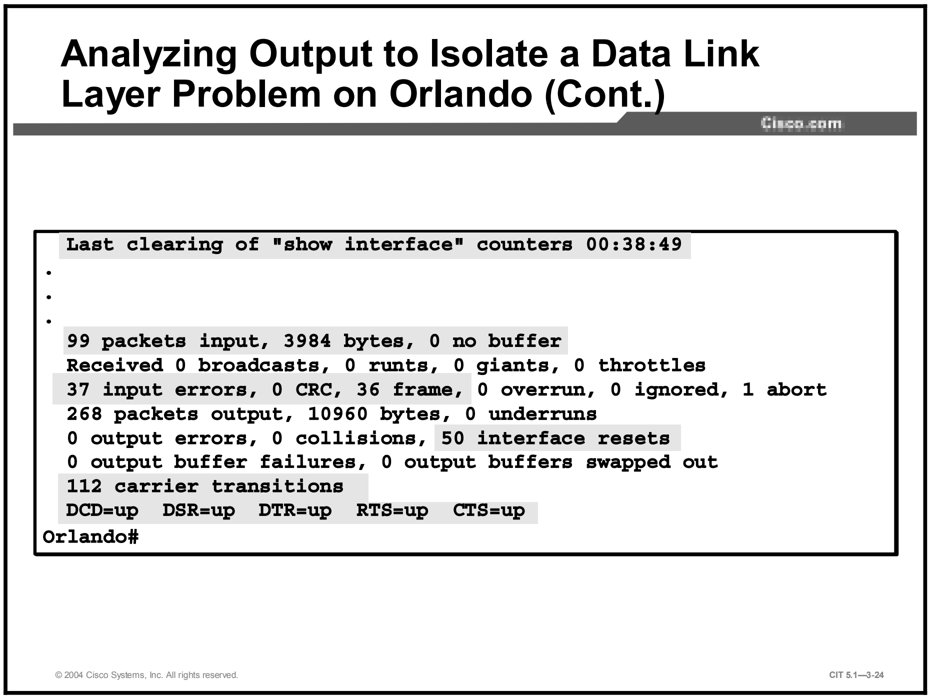
You decide to look for more information on the interface with the **show interface serial 1/0** command.



Analyzing Output to Isolate a Data Link Layer Problem on Orlando

```
Orlando#show interface serial 1/0
Serial1/0 is up, line protocol is down
  Hardware is PowerQUICC Serial
  Description: Frame Relay link to Daytona
  Internet address is 172.21.177.2/30
  MTU 1500 bytes, BW 128 Kbit, DLY 20000 usec,
     reliability 254/255, txload 1/255, rxload 1/255
  Encapsulation FRAME-RELAY, loopback not set
  Keepalive set (10 sec)
  LMI enq sent  232, LMI stat recvd 73, LMI upd recvd 0, DTE LMI down
  LMI enq recvd 0, LMI stat sent  0, LMI upd sent  0
  LMI DLCI 0  LMI type is ANSI Annex D  frame relay DT
.
.
.
```

CIT 5.1—3-23



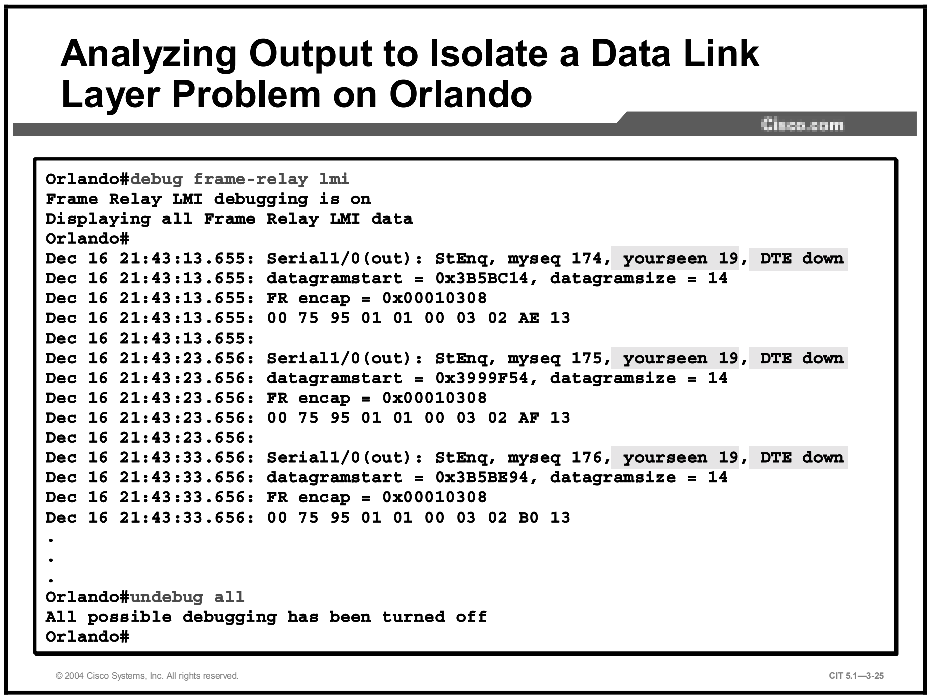
Analyzing Output to Isolate a Data Link Layer Problem on Orlando (Cont.)

```
  Last clearing of "show interface" counters 00:38:49
.
.
.
  99 packets input, 3984 bytes, 0 no buffer
  Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
  37 input errors, 0 CRC, 36 frame, 0 overrun, 0 ignored, 1 abort
  268 packets output, 10960 bytes, 0 underruns
  0 output errors, 0 collisions, 50 interface resets
  0 output buffer failures, 0 output buffers swapped out
  112 carrier transitions
  DCD=up  DSR=up  DTR=up  RTS=up  CTS=up
Orlando#
```

CIT 5.1—3-24

Orlando is sending LMI inquiries but not receiving the same number of LMI status packets back from the Frame Relay service provider. You also notice a large number of input errors and carrier transitions. You begin to question what your Frame Relay carrier has done.

You decide to enter the **debug frame-relay lmi** command to gather some additional details.



Analyzing Output to Isolate a Data Link Layer Problem on Orlando

```
Orlando#debug frame-relay lmi
Frame Relay LMI debugging is on
Displaying all Frame Relay LMI data
Orlando#
Dec 16 21:43:13.655: Serial1/0(out): StEnq, myseq 174, yourseen 19, DTE down
Dec 16 21:43:13.655: datagramstart = 0x3B5BC14, datagramsize = 14
Dec 16 21:43:13.655: FR encap = 0x00010308
Dec 16 21:43:13.655: 00 75 95 01 01 00 03 02 AE 13
Dec 16 21:43:13.655:
Dec 16 21:43:23.656: Serial1/0(out): StEnq, myseq 175, yourseen 19, DTE down
Dec 16 21:43:23.656: datagramstart = 0x3999F54, datagramsize = 14
Dec 16 21:43:23.656: FR encap = 0x00010308
Dec 16 21:43:23.656: 00 75 95 01 01 00 03 02 AF 13
Dec 16 21:43:23.656:
Dec 16 21:43:33.656: Serial1/0(out): StEnq, myseq 176, yourseen 19, DTE down
Dec 16 21:43:33.656: datagramstart = 0x3B5BE94, datagramsize = 14
Dec 16 21:43:33.656: FR encap = 0x00010308
Dec 16 21:43:33.656: 00 75 95 01 01 00 03 02 B0 13
.
.
.
Orlando#undebug all
All possible debugging has been turned off
Orlando#
```

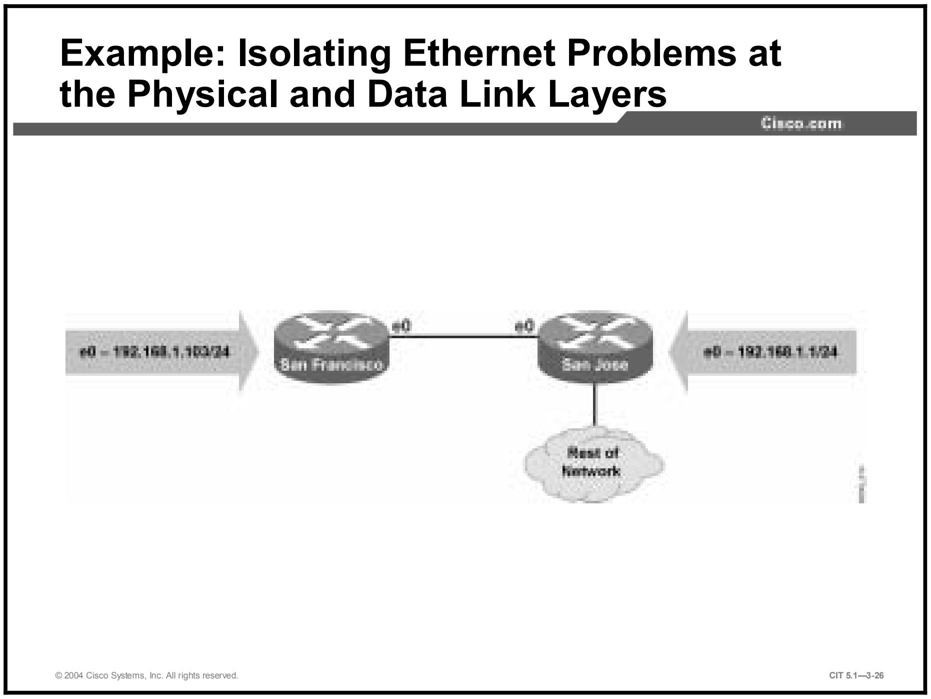
© 2004 Cisco Systems, Inc. All rights reserved. CIT 5.1—3-25

The result of the **debug frame-relay lmi** command helps you isolate the issue. If the Frame Relay service were working correctly, you would see an LMI reply from the switch for every LMI request the router sends to the switch. In addition, you should periodically see a full LMI status message from the switch that includes a description of the permanent virtual circuits (PVCs). This full LMI status message is sent in response to a status enquiry message that the router transmits after every six LMI keepalives. With the default keepalive of 10 seconds, you should see the full LMI status every minute. You would also see an incrementing counter in the Yourseen field and the data terminal equipment (DTE) status would be “up.”

Because everything used to work and no one changed anything on Orlando, you can pinpoint the issue to the Frame Relay carrier and the LMI encapsulation type. You have a defined LMI type in your interface configuration. If your service provider changed the LMI type that was offered to you, the line protocol would fail because of mismatched LMI types.

Example: Isolating Ethernet Problems at the Physical and Data Link Layers

You have just activated an Ethernet interface named Ethernet 0 on a router named SanFran.

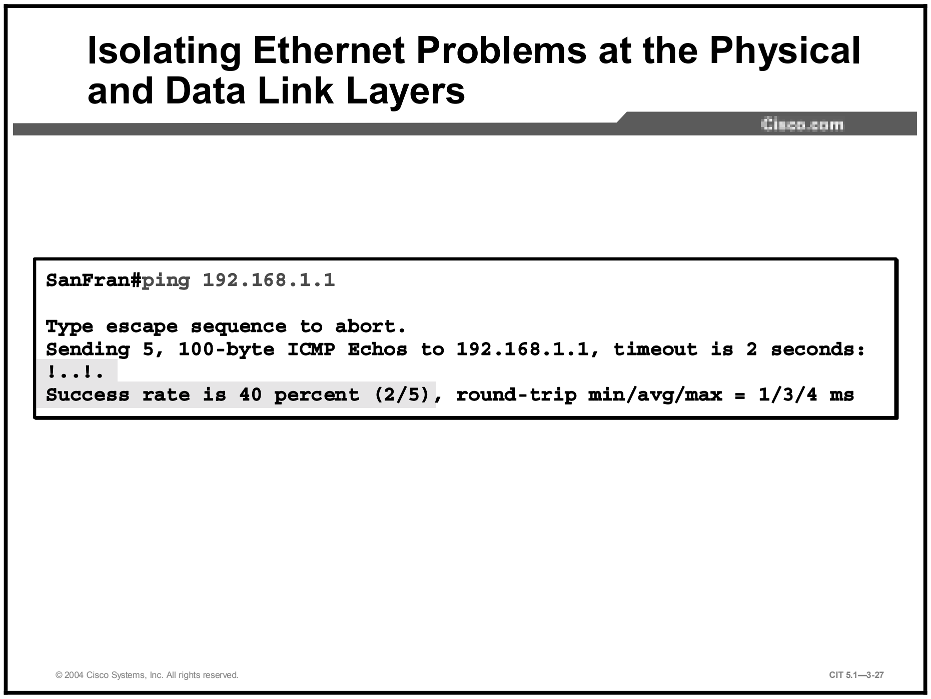


Example: Isolating Ethernet Problems at the Physical and Data Link Layers

Cisco.com

CIT 5.1—3-26

To verify the operation of the interface, you ping your default gateway through Ethernet 0 and notice that there is a 60 percent packet loss.



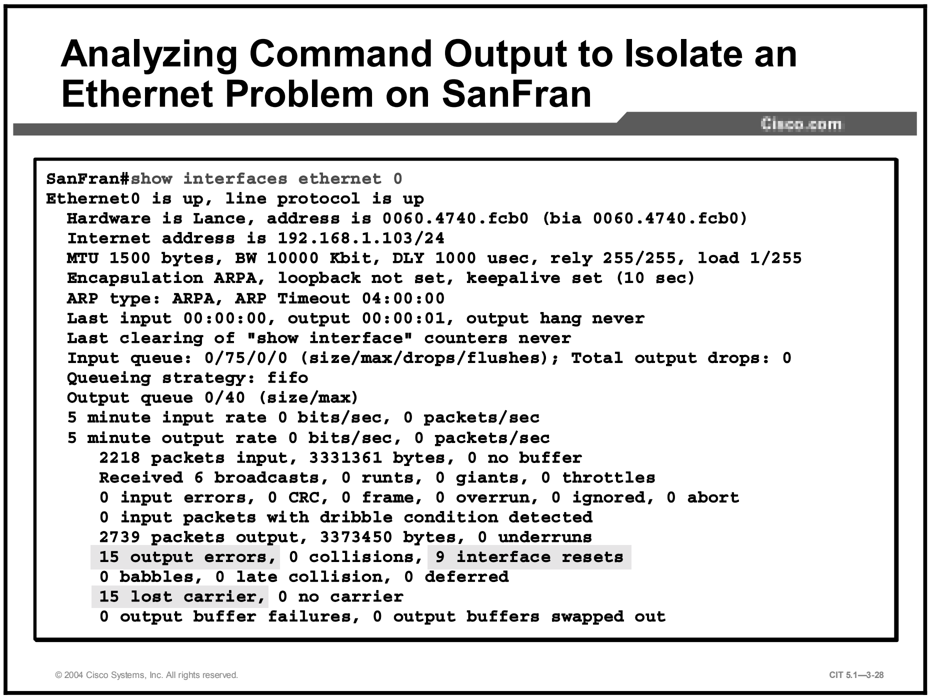
Isolating Ethernet Problems at the Physical and Data Link Layers

```
SanFran#ping 192.168.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
!..!.
Success rate is 40 percent (2/5), round-trip min/avg/max = 1/3/4 ms
```

CIT 5.1—3-27

The packet loss is an indication that there is a problem with the interface preventing it from functioning properly.

To isolate the problem to a particular interface, you enter the Cisco IOS **show interface ethernet0** command to display the status of the interface. The command output shows that interface Ethernet 0 is “up,” but other information on the screen indicates a problem.



Analyzing Command Output to Isolate an Ethernet Problem on SanFran

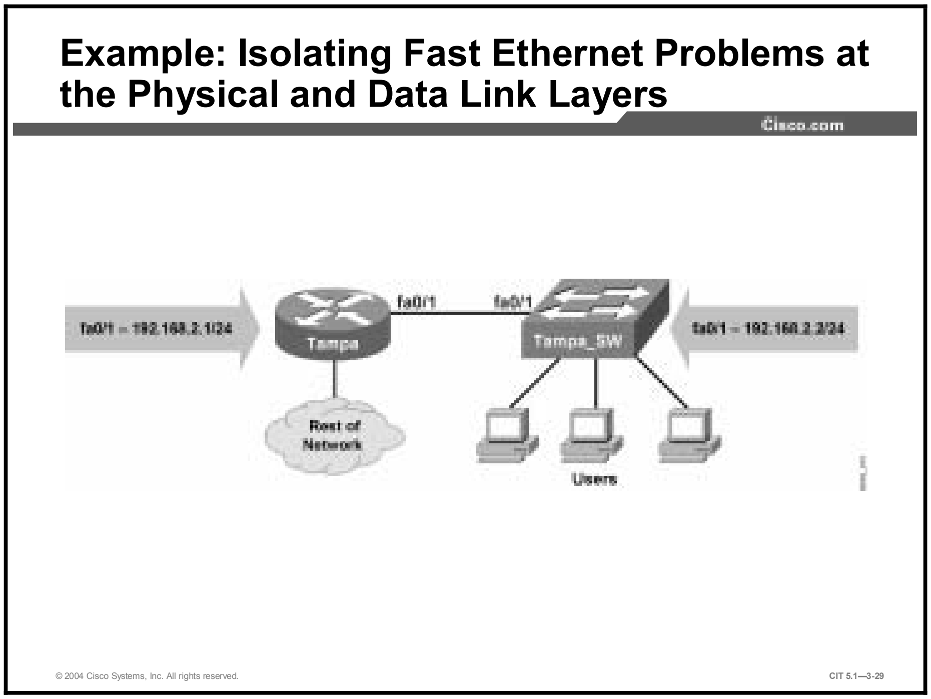
```
SanFran#show interfaces ethernet 0
Ethernet0 is up, line protocol is up
  Hardware is Lance, address is 0060.4740.fcb0 (bia 0060.4740.fcb0)
  Internet address is 192.168.1.103/24
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec, rely 255/255, load 1/255
  Encapsulation ARPA, loopback not set, keepalive set (10 sec)
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:00, output 00:00:01, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     2218 packets input, 3331361 bytes, 0 no buffer
     Received 6 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 input packets with dribble condition detected
     2739 packets output, 3373450 bytes, 0 underruns
     15 output errors, 0 collisions, 9 interface resets
     0 babbles, 0 late collision, 0 deferred
     15 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
```

CIT 5.1—3-28

Note that the display shows that there were 15 output errors, 9 interface resets, and 15 instances of lost carrier. These are all indications that there might be a physical layer problem with the interface connection. Lost carrier indicates that the Ethernet interface lost its connection to the device on the other end of the Ethernet cable. The interface resets indicate that the interface has restarted itself after an error condition. One possible cause of this problem is a cable not properly seated in the router interface connector.

Example: Isolating Fast Ethernet Problems at the Physical and Data Link Layers

You have just connected the Fast Ethernet interface of a router named Tampa to the Fast Ethernet port of an Ethernet switch.

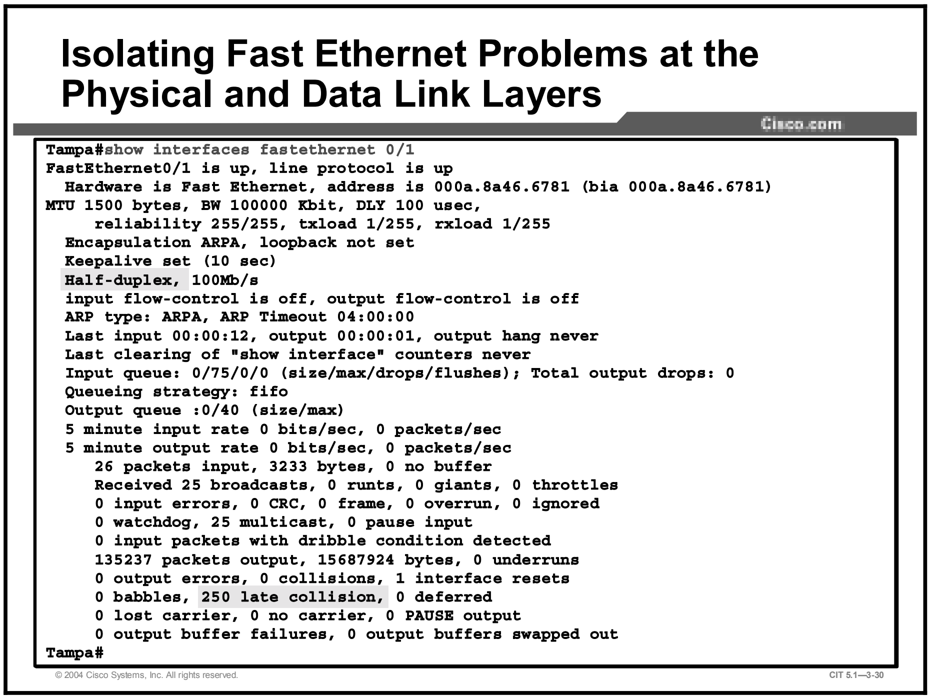


Example: Isolating Fast Ethernet Problems at the Physical and Data Link Layers

CIT 5.1—3-29

The link appeared to be opening properly; however, the applications group complained that it was performing poorly under load.

To diagnose the problem, you enter the **show interfaces** command to observe the rate of the interface.



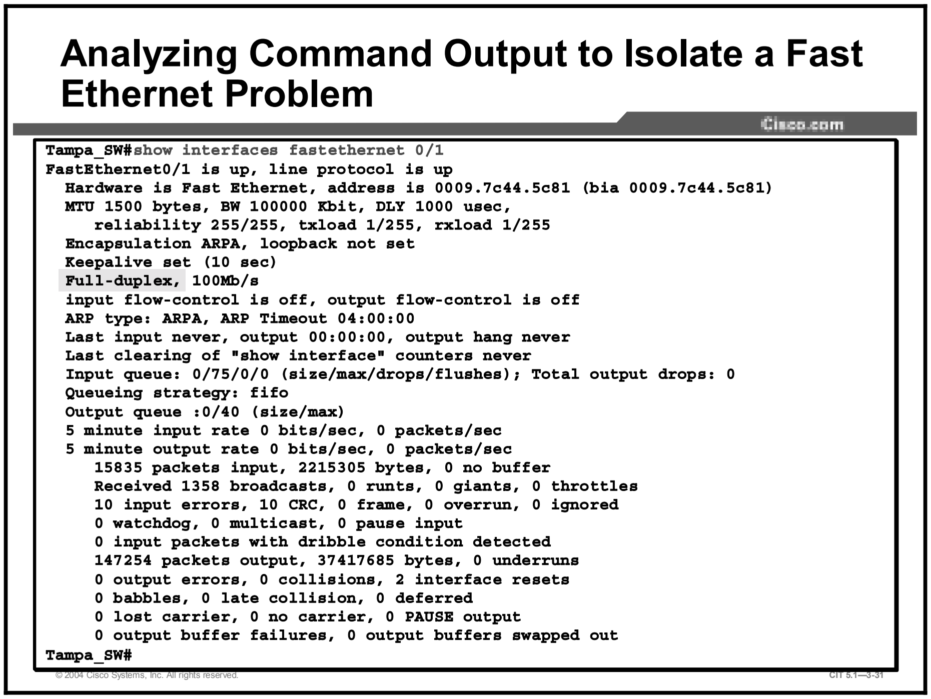
Isolating Fast Ethernet Problems at the Physical and Data Link Layers

```
Tampa#show interfaces fastethernet 0/1
FastEthernet0/1 is up, line protocol is up
  Hardware is Fast Ethernet, address is 000a.8a46.6781 (bia 000a.8a46.6781)
MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Half-duplex, 100Mb/s
  input flow-control is off, output flow-control is off
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:12, output 00:00:01, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue :0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     26 packets input, 3233 bytes, 0 no buffer
     Received 25 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 25 multicast, 0 pause input
     0 input packets with dribble condition detected
     135237 packets output, 15687924 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface resets
     0 babbles, 250 late collision, 0 deferred
     0 lost carrier, 0 no carrier, 0 PAUSE output
     0 output buffer failures, 0 output buffers swapped out
Tampa#
```

CIT 5.1—3-30

You note that the interface is configured in half-duplex mode and that the late collision counter is incrementing. Late collisions are an indication that there may be a mismatch in the duplex configurations of the interfaces on this connection.

To isolate the problem further, you move to the switch on the other end of the link; you issue a **show interface** command and observe the status of the port on the other end of the link.



Analyzing Command Output to Isolate a Fast Ethernet Problem

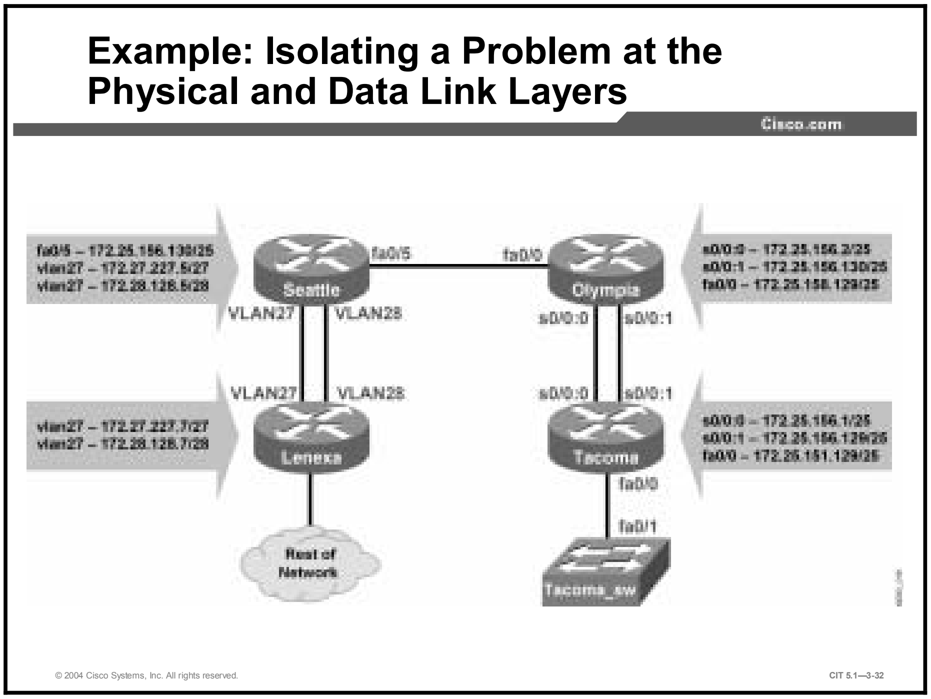
```
Tampa_SW#show interfaces fastethernet 0/1
FastEthernet0/1 is up, line protocol is up
  Hardware is Fast Ethernet, address is 0009.7c44.5c81 (bia 0009.7c44.5c81)
  MTU 1500 bytes, BW 100000 Kbit, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s
  input flow-control is off, output flow-control is off
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue :0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     15835 packets input, 2215305 bytes, 0 no buffer
     Received 1358 broadcasts, 0 runts, 0 giants, 0 throttles
     10 input errors, 10 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 0 multicast, 0 pause input
     0 input packets with dribble condition detected
     147254 packets output, 37417685 bytes, 0 underruns
     0 output errors, 0 collisions, 2 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier, 0 PAUSE output
     0 output buffer failures, 0 output buffers swapped out
Tampa_SW#
```

CIT 5.1—3-31

You note that the interface at this end of the connection is set in full-duplex mode. The duplex misconfiguration is the cause of the problem.

Example: Isolating a Problem at the Physical and Data Link Layers

You are the network engineer for the northeast division of Acme. Your site in Seattle (with a router named Seattle) runs a Layer 3 switch that connects the division's resources to the corporate core in Lenexa and Elmhurst. (Note that Elmhurst is not show in the diagram.)



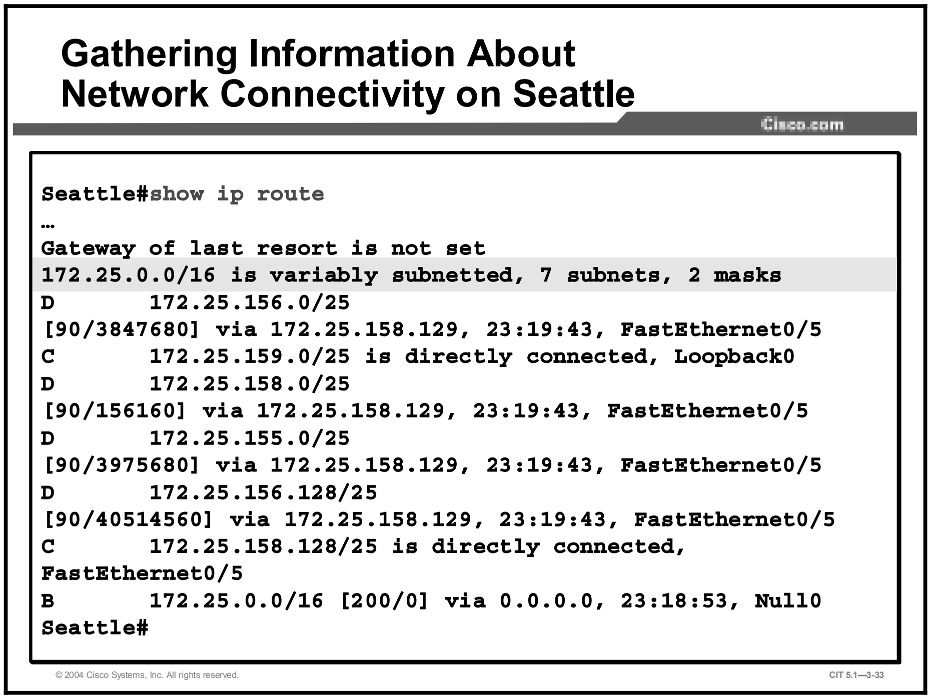
Example: Isolating a Problem at the Physical and Data Link Layers

© 2004 Cisco Systems, Inc. All rights reserved.

CIT 5.1—3-32

One morning, Network Operations calls to tell you that Seattle no longer has connectivity outside of the division. You ask if anyone in Seattle Operations has made changes. Network Operations says that no changes were made to the production network. The users throughout the division are complaining that they cannot connect to anywhere.

To verify network connectivity, you look at the routing table with the **show ip route** command. You confirm that there are no routes outside of the division.

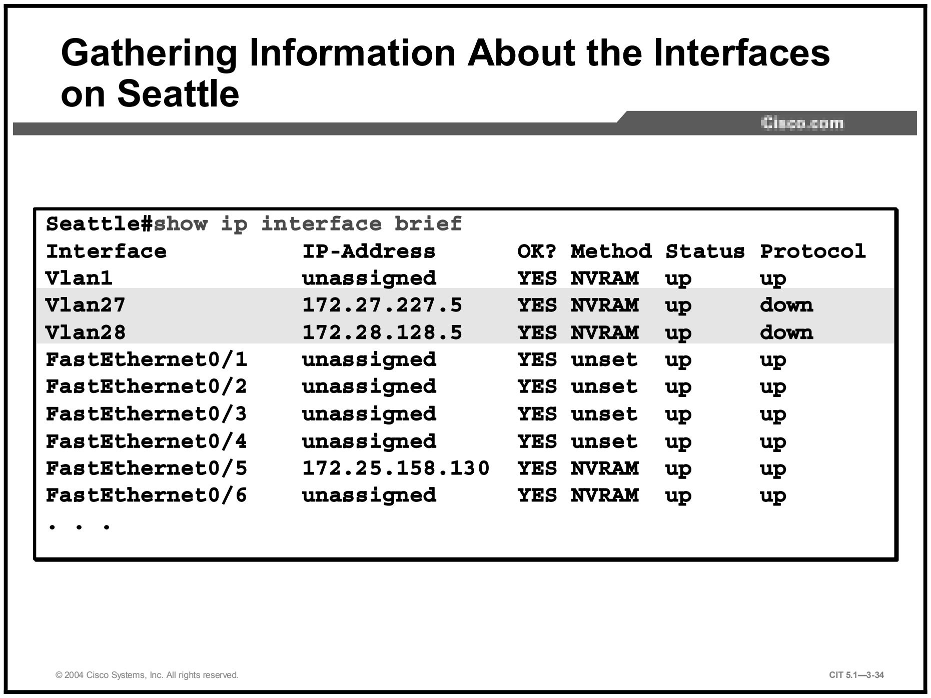


Gathering Information About Network Connectivity on Seattle

```
Seattle#show ip route
…
Gateway of last resort is not set
172.25.0.0/16 is variably subnetted, 7 subnets, 2 masks
D       172.25.156.0/25
[90/3847680] via 172.25.158.129, 23:19:43, FastEthernet0/5
C       172.25.159.0/25 is directly connected, Loopback0
D       172.25.158.0/25
[90/156160] via 172.25.158.129, 23:19:43, FastEthernet0/5
D       172.25.155.0/25
[90/3975680] via 172.25.158.129, 23:19:43, FastEthernet0/5
D       172.25.156.128/25
[90/40514560] via 172.25.158.129, 23:19:43, FastEthernet0/5
C       172.25.158.128/25 is directly connected,
FastEthernet0/5
B       172.25.0.0/16 [200/0] via 0.0.0.0, 23:18:53, Null0
Seattle#
```

CIT 5.1—3-33

Next, you look at the interface status on Seattle using the **show ip interface brief** command.



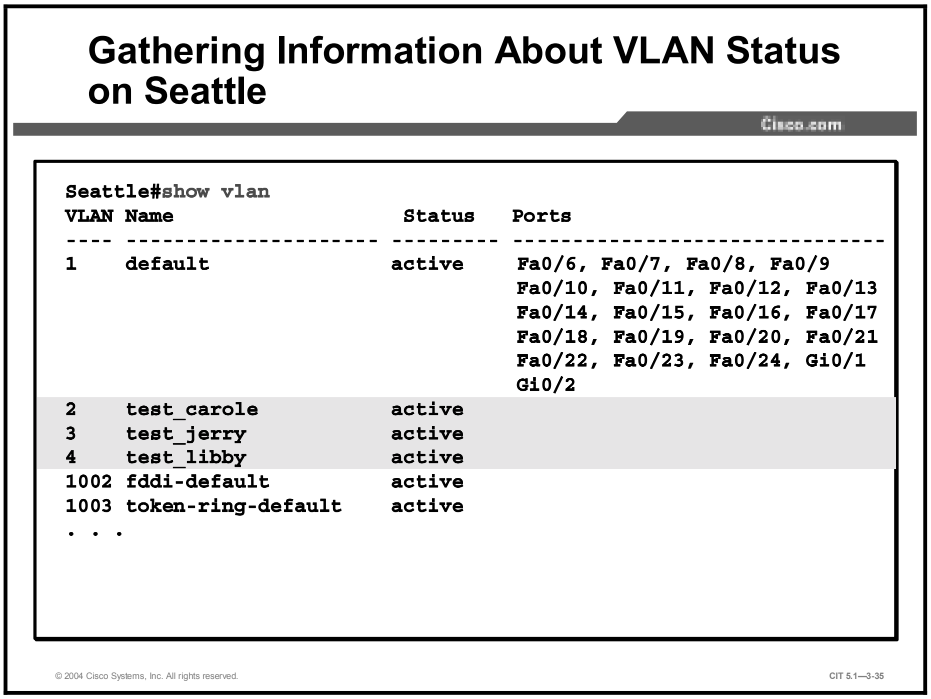
Gathering Information About the Interfaces on Seattle

```
Seattle#show ip interface brief
Interface          IP-Address      OK? Method Status Protocol
Vlan1              unassigned      YES NVRAM  up     up
Vlan27             172.27.227.5    YES NVRAM  up     down
Vlan28             172.28.128.5    YES NVRAM  up     down
FastEthernet0/1    unassigned      YES unset  up     up
FastEthernet0/2    unassigned      YES unset  up     up
FastEthernet0/3    unassigned      YES unset  up     up
FastEthernet0/4    unassigned      YES unset  up     up
FastEthernet0/5    172.25.158.130  YES NVRAM  up     up
FastEthernet0/6    unassigned      YES NVRAM  up     up
. . .
```

CIT 5.1—3-34

You see that interfaces VLAN27 and VLAN28 have an “up” status, but the protocol is “down.”

Using the **show vlan** command, you review the VLAN status on Seattle.



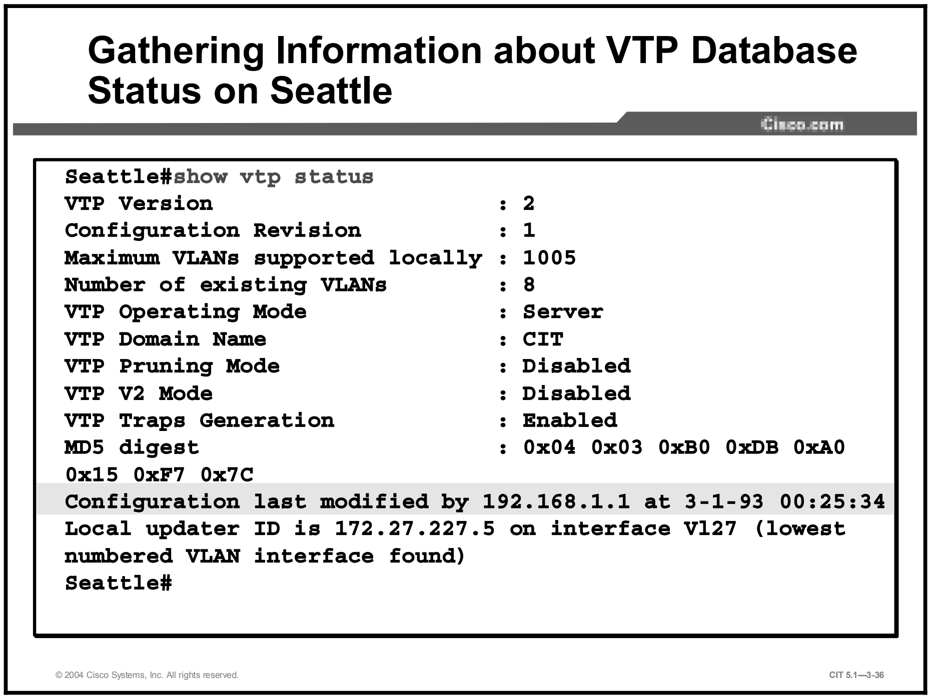
Gathering Information About VLAN Status on Seattle

```
Seattle#show vlan
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                                Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                                Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                                Fa0/22, Fa0/23, Fa0/24, Gi0/1
                                                Gi0/2
2    test_carole                      active
3    test_jerry                       active
4    test_libby                       active
1002 fddi-default                     active
1003 token-ring-default               active
. . .
```

CIT 5.1—3-35

You see that VLAN27 and VLAN28 are missing, and some self-described "test" VLANs are present. You realize that if the VLAN27 and VLAN28 are not in the VLAN table, the protocol on the associated interfaces would indeed be shutdown. However, you need to determine why the VLANs are now missing.

You review the VLAN Trunking Protocol (VTP) database status on Seattle with the **show vtp status** command.



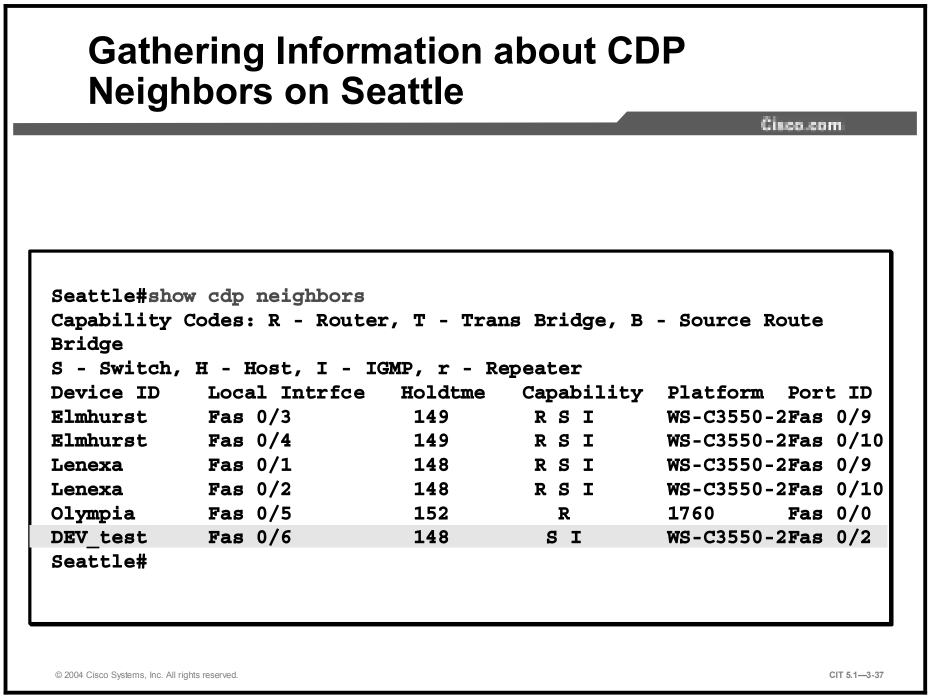
Gathering Information about VTP Database Status on Seattle

```
Seattle#show vtp status
VTP Version                     : 2
Configuration Revision          : 1
Maximum VLANs supported locally : 1005
Number of existing VLANs        : 8
VTP Operating Mode              : Server
VTP Domain Name                 : CIT
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Enabled
MD5 digest                      : 0x04 0x03 0xB0 0xDB 0xA0
0x15 0xF7 0x7C
Configuration last modified by 192.168.1.1 at 3-1-93 00:25:34
Local updater ID is 172.27.227.5 on interface Vl27 (lowest
numbered VLAN interface found)
Seattle#
```

CIT 5.1—3-36

You notice two significant items—that the VTP database was last updated by the switch with IP address 192.168.1.1, and that your switch is configured for VTP server mode. You know that 192.168.1.1 should not be changing your database, and if you were properly in VTP transparent mode, it would not. Just for fun, you will try to determine who has IP address 192.168.1.1 and how they got to your switch.

You look for local switches with the **show cdp neighbors** command.



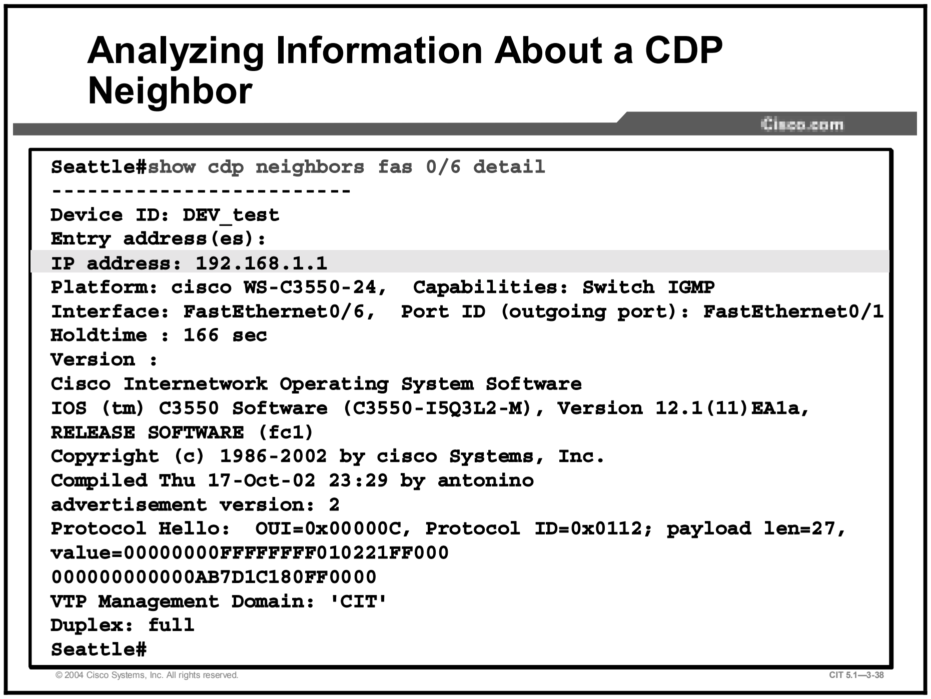
Gathering Information about CDP Neighbors on Seattle

```
Seattle#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route
Bridge
S - Switch, H - Host, I - IGMP, r - Repeater
Device ID    Local Intrfce   Holdtme   Capability  Platform  Port ID
Elmhurst     Fas 0/3          149       R S I      WS-C3550-2Fas 0/9
Elmhurst     Fas 0/4          149       R S I      WS-C3550-2Fas 0/10
Lenexa       Fas 0/1          148       R S I      WS-C3550-2Fas 0/9
Lenexa       Fas 0/2          148       R S I      WS-C3550-2Fas 0/10
Olympia      Fas 0/5          152         R        1760      Fas 0/0
DEV_test     Fas 0/6          148        S I       WS-C3550-2Fas 0/2
Seattle#
```

CIT 5.1—3-37

You do not recognize the DEV_test switch, so you will need to investigate.

With the **show cdp neighbors fastethernet 0/6 detail** command, you can review more information about the DEV_test switch.



Analyzing Information About a CDP Neighbor

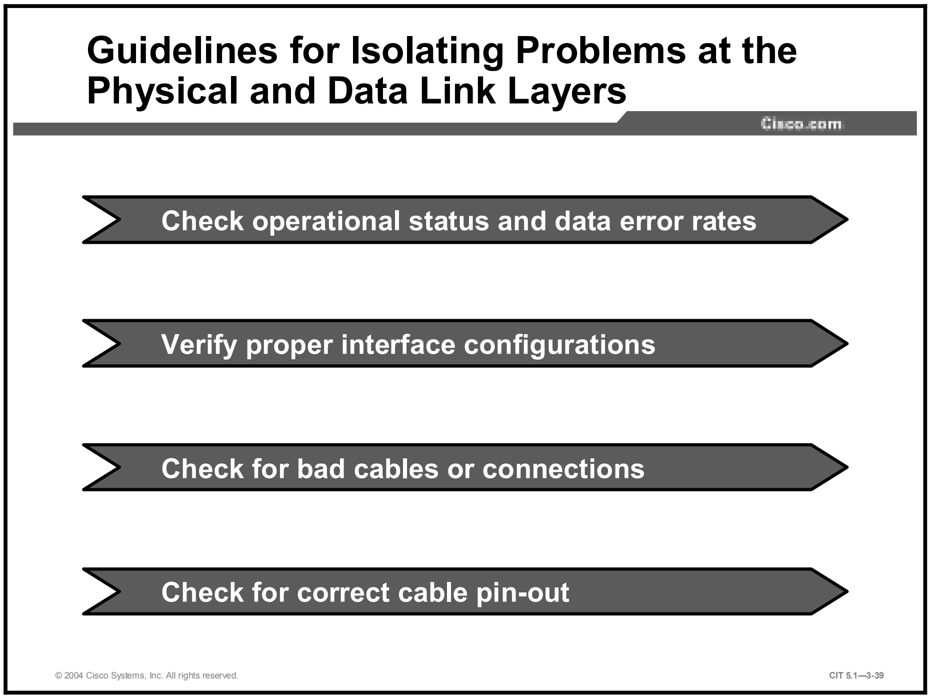
```
Seattle#show cdp neighbors fas 0/6 detail
-------------------------
Device ID: DEV_test
Entry address(es):
IP address: 192.168.1.1
Platform: cisco WS-C3550-24,  Capabilities: Switch IGMP
Interface: FastEthernet0/6,  Port ID (outgoing port): FastEthernet0/1
Holdtime : 166 sec
Version :
Cisco Internetwork Operating System Software
IOS (tm) C3550 Software (C3550-I5Q3L2-M), Version 12.1(11)EA1a,
RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2002 by cisco Systems, Inc.
Compiled Thu 17-Oct-02 23:29 by antonino
advertisement version: 2
Protocol Hello:  OUI=0x00000C, Protocol ID=0x0112; payload len=27,
value=00000000FFFFFFFF010221FF000
000000000000AB7D1C180FF0000
VTP Management Domain: 'CIT'
Duplex: full
Seattle#
```

CIT 5.1—3-38

You determine that DEV_test has IP address 192.168.1.1 and that the switch broke your network. You have isolated the problem to a new switch overwriting your VTP database when your switch was in VTP server mode. (When you call Operations, they do admit to putting on a test switch for some experimentation.)

Isolating Problems Occurring at the Physical and Data Link Layers

This topic uses guidelines to help troubleshooters isolate problems at the physical and data link layers.



Guidelines for Isolating Problems at the Physical and Data Link Layers

Cisco.com

- Check operational status and data error rates
- Verify proper interface configurations
- Check for bad cables or connections
- Check for correct cable pin-out

© 2004 Cisco Systems, Inc. All rights reserved.

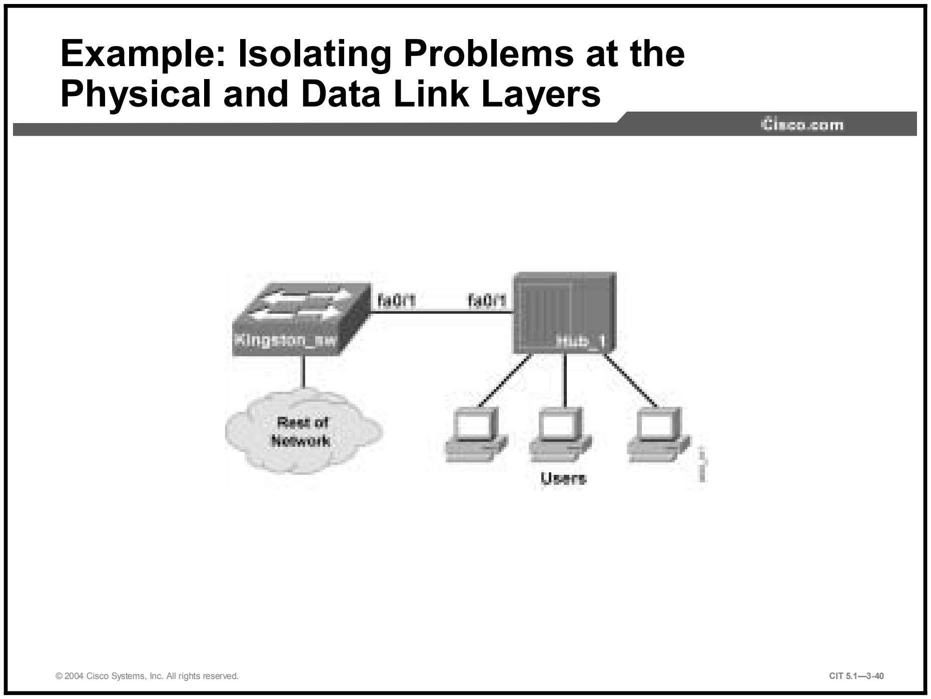
CIT 5.1—3-39

Use an effective and systematic technique to isolate a problem successfully at the physical or data link layer. Use the following guidelines to isolate problems at the physical and data link layers:

- **Check operational status and data error rates:** Use Cisco **show** commands to check for statistics such as collisions, input, and output errors. The characteristics of these statistics will vary, depending on the technologies used on the network. Use **debug** commands for additional details when you cannot get enough information to isolate the problem using **show** commands.
- **Verify proper interface configurations:** Check that all switch or hub ports are configured for the correct VLAN or collision domain, and that spanning tree, speed, and duplex settings are correctly configured. Confirm that any active ports or interfaces are not shut down.
- **Check for bad cables or connections:** Verify that the cable from the source interface is properly connected and that it is in good condition. If you doubt the integrity of a cable, exchange the cable with a known working cable. If you doubt the connection is good, remove the cable, perform a physical inspection of both the cable and the interface, and then reconnect the cable. If a suspect cable is connected to a wall jack, use a cable tester to ensure that the jack is properly wired. A link light that is lit and displays the color indicating proper operation will also be evidence that the connection is successful.
- **Check for correct cable pin-out:** Verify that the proper cable is used. A crossover or rollover cable may be required for direct connections between some devices.

Example: Isolating Problems at the Physical and Data Link Layers

A group of users has reported that their connection to the network has gone down. You examine the end-system topology diagram for the network and realize that all of the users affected are connected to the same switch and hub combination.



Example: Isolating Problems at the Physical and Data Link Layers

Cisco.com

© 2004 Cisco Systems, Inc. All rights reserved.

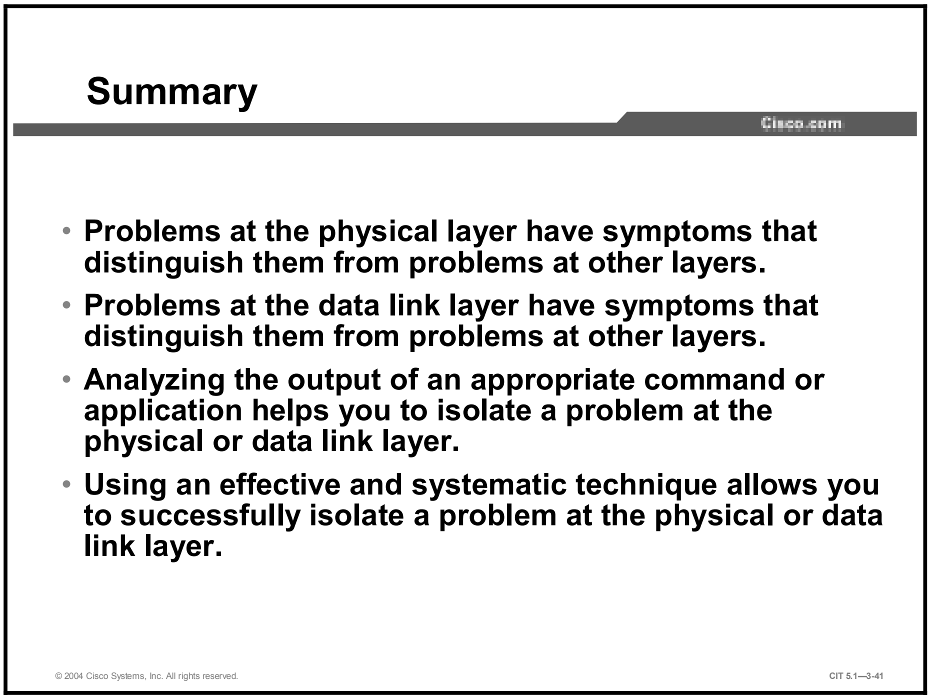
CIT 5.1—3-40

This situation leads you to continue isolating the problem at the common connection. You perform an onsite inspection of the physical connection of the switch and the hub, and you note that all of the link lights are lit and are showing a color indicating correct operation. All cables appear to be of the correct type and pin-out.

After verifying that the physical connections are working, you decide to connect to the switch to check the port configurations. You note that the speed setting for one of the ports is set to 10 Mbps; however, the port speed should be set to 100 Mbps. This mismatch in speed is the likely source of your connection problem.

Summary

This topic summarizes the key points discussed in this lesson.



Summary

- Problems at the physical layer have symptoms that distinguish them from problems at other layers.
- Problems at the data link layer have symptoms that distinguish them from problems at other layers.
- Analyzing the output of an appropriate command or application helps you to isolate a problem at the physical or data link layer.
- Using an effective and systematic technique allows you to successfully isolate a problem at the physical or data link layer.

CIT 5.1—3-41

References

For additional information, refer to these resources:

- Cisco online documentation: http://www.cisco.com/univercd/home/home.htm
- Cisco Technical Assistance Center (TAC): http://www.cisco.com/tac

Quiz

Use the practice items here to review what you have learned in this lesson. The correct answers are found in the Quiz Answer Key.

Q1) Which command output would you most likely see if you had a problem at the physical layer?

A) neighbor 172.10.160.2 (Serial 1/1) is down: holding time expired

B) Ethernet 0/0 is down, line protocol is down

C) Serial 1/0 is up, line protocol is administratively down

D) invalid command, no available connection

Q2) Which command output would you most likely see if you had a problem at the data link layer?

A) Serial 0/1 is down, line protocol is down

B) Ethernet 0/1 is down, line protocol is down

C) interface Serial 1/0, changed state to up

D) Serial 0/1 is up, line protocol is down

Q3) Which Cisco IOS command would you enter to view details about the Cisco IOS software and all installed hardware modules?

A) **show protocols**

B) **show version**

C) **debug controllers**

D) **show ip interface brief**

Q4) A group of users reports that their connection to the network has gone down. You suspect it to be a problem in either the physical or data link layer. You check the operational status, errors, and configuration of the affected interfaces. You still have not found the cause of the problem.

Which guideline for isolating a problem at the physical and data link layers have you omitted?

A) verifying the IP address of the default gateway

B) checking cable configuration

C) disabling spanning tree

D) viewing TCP information on a host

Quiz Answer Key

Q1) B

Relates to: Identifying the Symptoms of Problems Occurring at the Physical Layer

Q2) D

Relates to: Identifying the Symptoms of Problems Occurring at the Data Link Layer

Q3) B

Relates to: Analyzing Commands and Applications Used to Isolate Problems Occurring at the Physical and Data Link Layers

Q4) B

Relates to: Isolating Problems Occurring at the Physical and Data Link Layers

Correcting the Problem

Overview

Once a troubleshooter has determined the most likely cause of a problem, the next phase that needs to be considered involves correcting the problem. In this lesson, you will correct isolated problems using identified commands to configure physical and data link layer components.

Relevance

A doctor is not successful unless there is a follow-up to the diagnosis of your problem with a successful solution. The same idea applies to network troubleshooters. Isolating a problem is a big step in troubleshooting. However, the process is not complete until you have solved the problem and returned the network to its baseline state.

Objectives

Upon completing this lesson, you will be able to:

- Identify commands and applications used to correct problems occurring at the physical and data link layers
- Identify physical and data link layer support resources
- Correct a problem occurring at the physical or data link layer

Learner Skills and Knowledge

To benefit fully from this lesson, you must have these prerequisite skills and knowledge:

- Ability to apply layered model troubleshooting approaches
- Familiarity with Cisco command syntax covered in the Cisco *Building Scalable Cisco Internetworks* (BSCI), *Building Cisco Multilayer Switched Networks* (BCMSN), and *Building Cisco Remote Access Networks* (BCRAN) courses

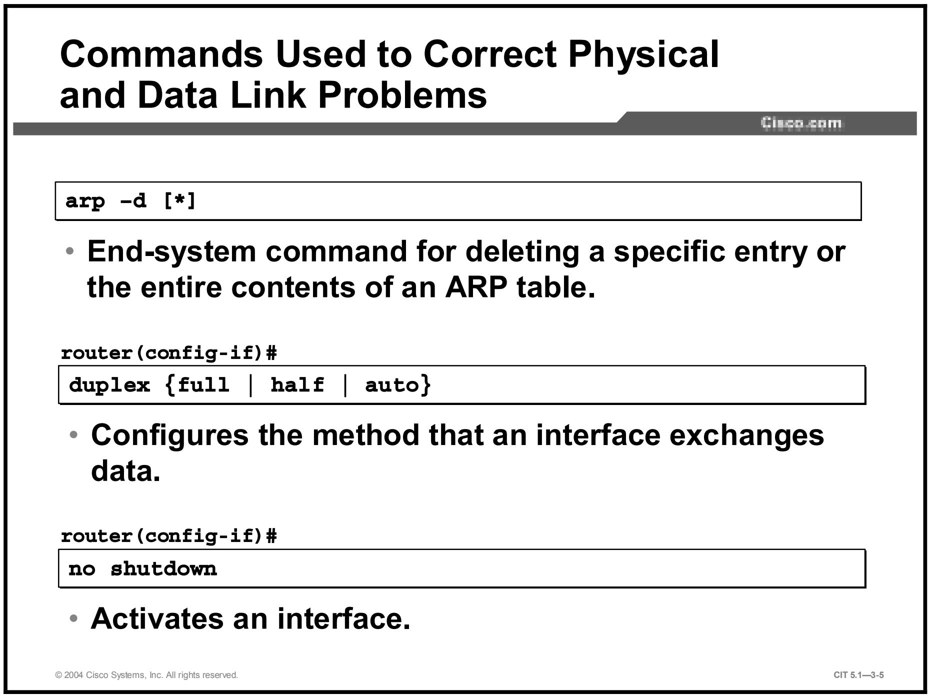
Outline

This lesson includes these topics:

- Overview
- Identifying Commands and Applications to Correct Problems Occurring at the Physical and Data Link Layers
- Identifying Physical and Data Link Layer Support Resources
- Correcting Problems Occurring at the Physical and Data Link Layers
- Summary
- Quiz

Identifying Commands and Applications to Correct Problems Occurring at the Physical and Data Link Layers

This topic lists selected commands and applications used by troubleshooters to correct problems at the physical and data link layers.



Commands Used to Correct Physical and Data Link Problems

Cisco.com

```
arp -d [*]
```

- End-system command for deleting a specific entry or the entire contents of an ARP table.

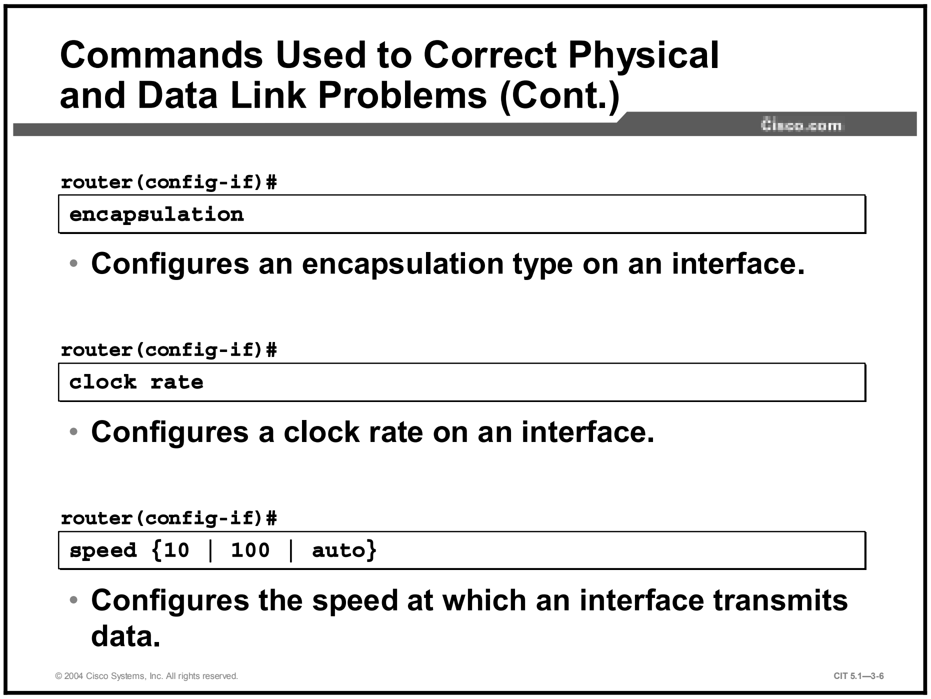
```
router(config-if)#
duplex {full | half | auto}
```

- Configures the method that an interface exchanges data.

```
router(config-if)#
no shutdown
```

- Activates an interface.

CIT 5.1—3-5



Commands Used to Correct Physical and Data Link Problems (Cont.)

Cisco.com

```
router(config-if)#
encapsulation
```

- Configures an encapsulation type on an interface.

```
router(config-if)#
clock rate
```

- Configures a clock rate on an interface.

```
router(config-if)#
speed {10 | 100 | auto}
```

- Configures the speed at which an interface transmits data.

CIT 5.1—3-6

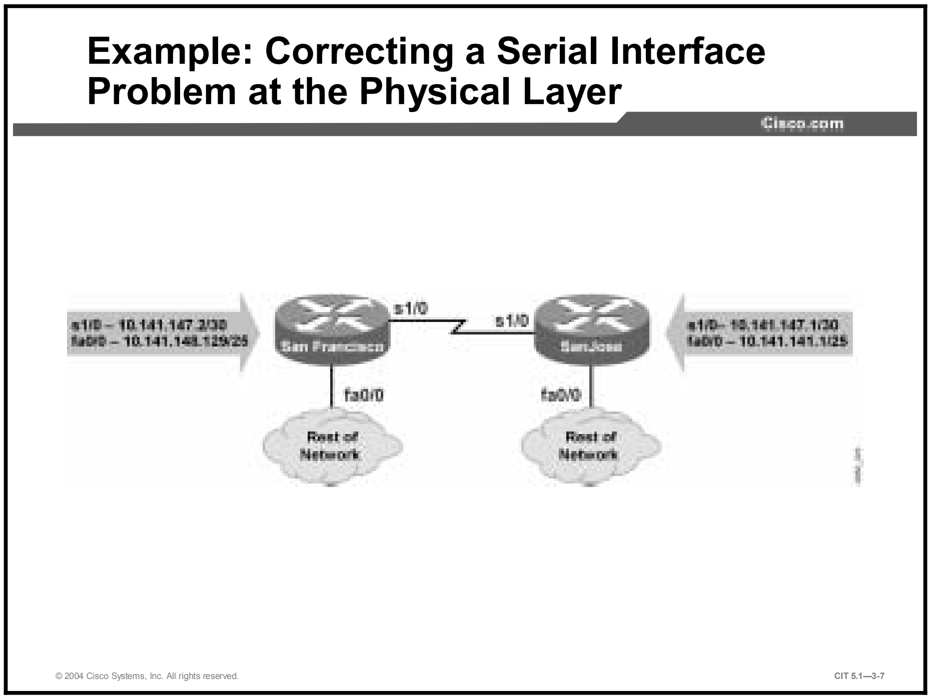
The table shows selected commands that a troubleshooter uses to correct problems that occur at the physical and data link layers.

Commands Used to Correct Physical and Data Link Problems

Command	Description
arp -d *ip-address*	End-system command for deleting a specific entry or the entire contents of an Address Resolution Protocol (ARP) table.
duplex {**full** | **half** | **auto**}	Configures the method that an interface exchanges data.
no shutdown	Activates an interface.
encapsulation	Configures an encapsulation type on an interface.
clock rate	Configures a clock rate on an interface.
speed {**10** | **100** | **auto**}	Configures the speed at which an interface transmits data.

Example: Correcting a Serial Interface Problem at the Physical Layer

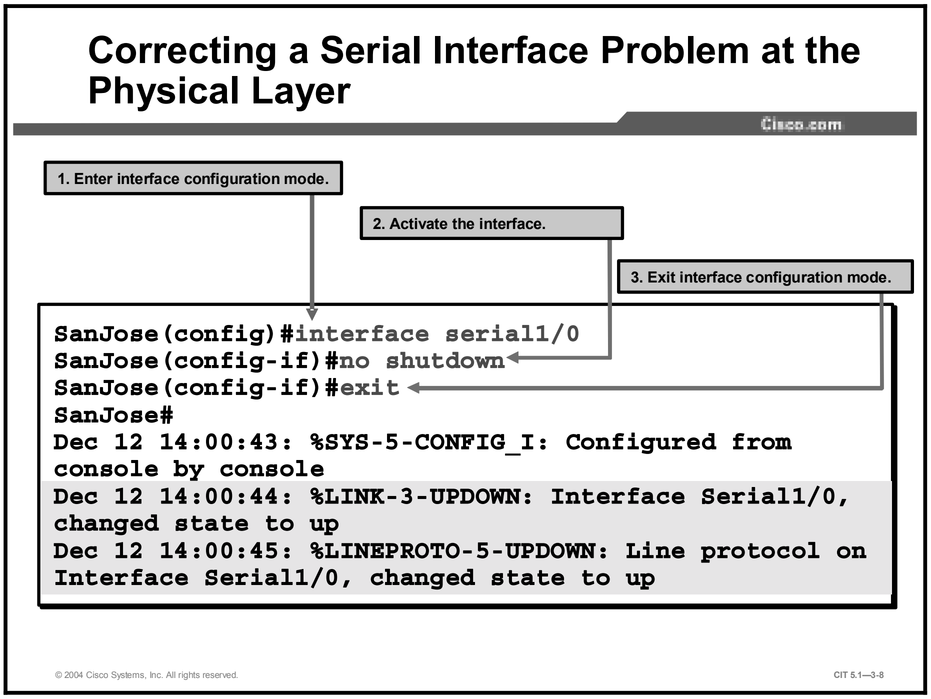
You find a problem with an inactive interface on a router named SanJose. You need to enter a Cisco IOS command that will activate the interface named Serial1/0.



Example: Correcting a Serial Interface Problem at the Physical Layer

CIT 5.1—3-7

To accomplish this, you enter interface configuration mode and apply the **no shutdown** command. The console messages show interface Serial1/0 going to an active state.



Correcting a Serial Interface Problem at the Physical Layer

Cisco.com

1. Enter interface configuration mode.

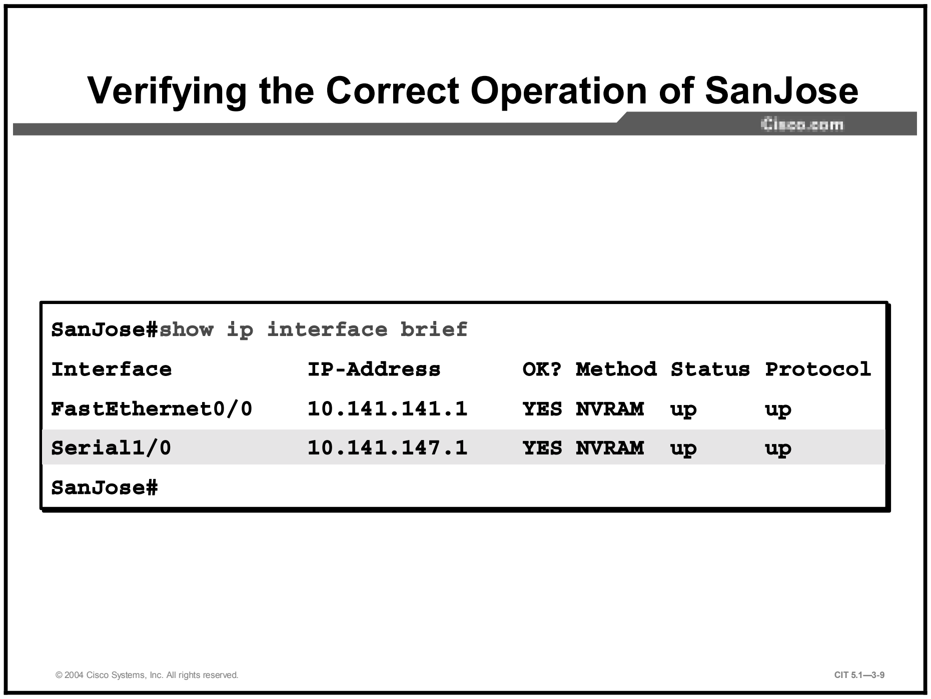
2. Activate the interface.

3. Exit interface configuration mode.

```
SanJose(config)#interface serial1/0
SanJose(config-if)#no shutdown
SanJose(config-if)#exit
SanJose#
Dec 12 14:00:43: %SYS-5-CONFIG_I: Configured from
console by console
Dec 12 14:00:44: %LINK-3-UPDOWN: Interface Serial1/0,
changed state to up
Dec 12 14:00:45: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Serial1/0, changed state to up
```

CIT 5.1—3-8

Next, you enter the **show ip interface brief** command on the SanJose router to verify the interface status.

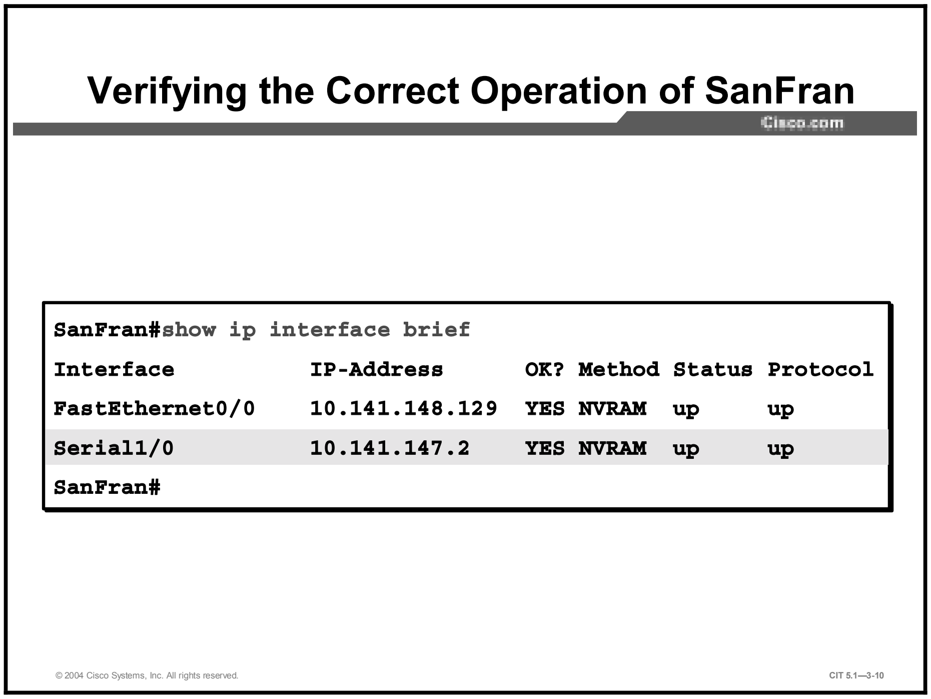


Verifying the Correct Operation of SanJose

```
SanJose#show ip interface brief
Interface           IP-Address      OK? Method Status  Protocol
FastEthernet0/0     10.141.141.1    YES NVRAM  up      up
Serial1/0           10.141.147.1    YES NVRAM  up      up
SanJose#
```

© 2004 Cisco Systems, Inc. All rights reserved. CIT 5.1—3-9

The line status is up and this side of the link looks operational. You return to the console session on the SanFran router to verify the interface status there.

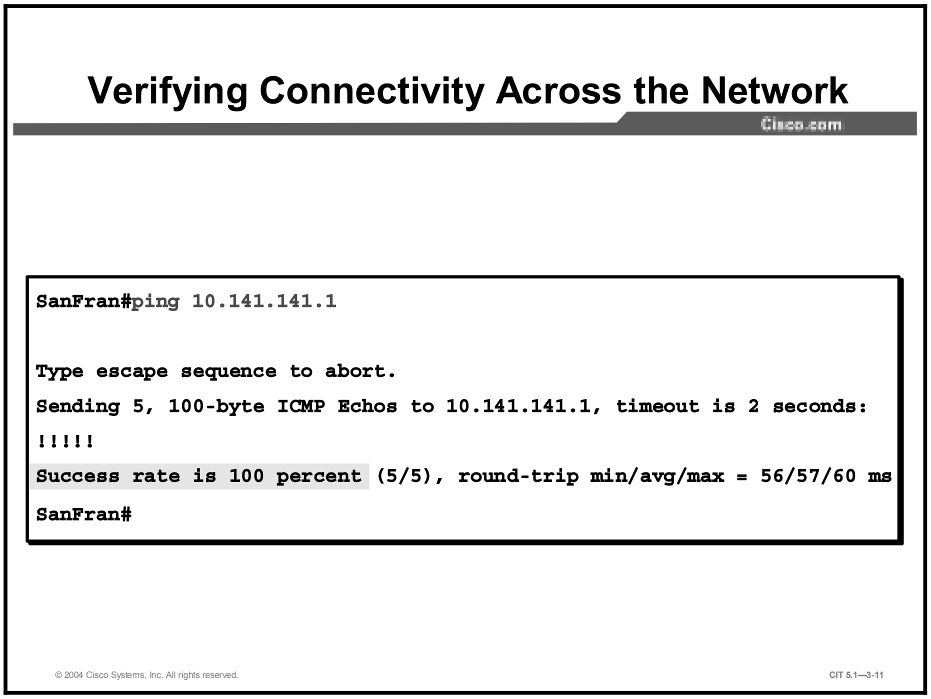


Verifying the Correct Operation of SanFran

```
SanFran#show ip interface brief
Interface           IP-Address      OK? Method Status  Protocol
FastEthernet0/0     10.141.148.129  YES NVRAM  up      up
Serial1/0           10.141.147.2    YES NVRAM  up      up
SanFran#
```

© 2004 Cisco Systems, Inc. All rights reserved. CIT 5.1—3-10

The line status is “up” here, as well. As a final validation, you use the **ping** command across the link to verify connectivity across the network, data link, and physical layers.



Verifying Connectivity Across the Network

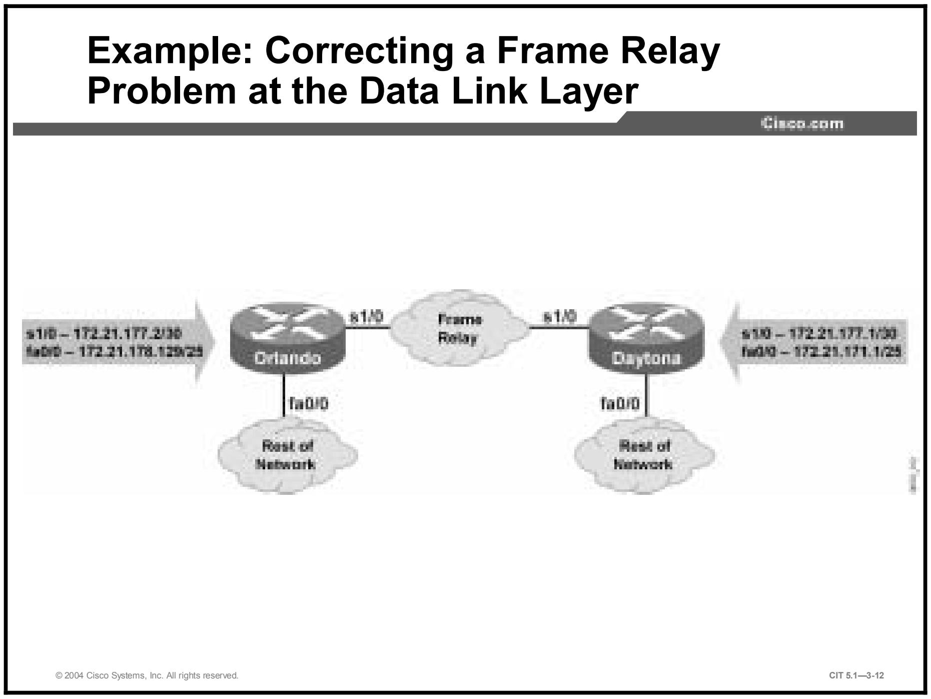
```
SanFran#ping 10.141.141.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.141.141.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 56/57/60 ms
SanFran#
```

CIT 5.1—3-11

The ping test is successful. You have resolved the physical layer issue.

Example: Correcting a Frame Relay Problem at the Data Link Layer

You have isolated a problem believed to be an incorrect LMI type on a Frame Relay interface.

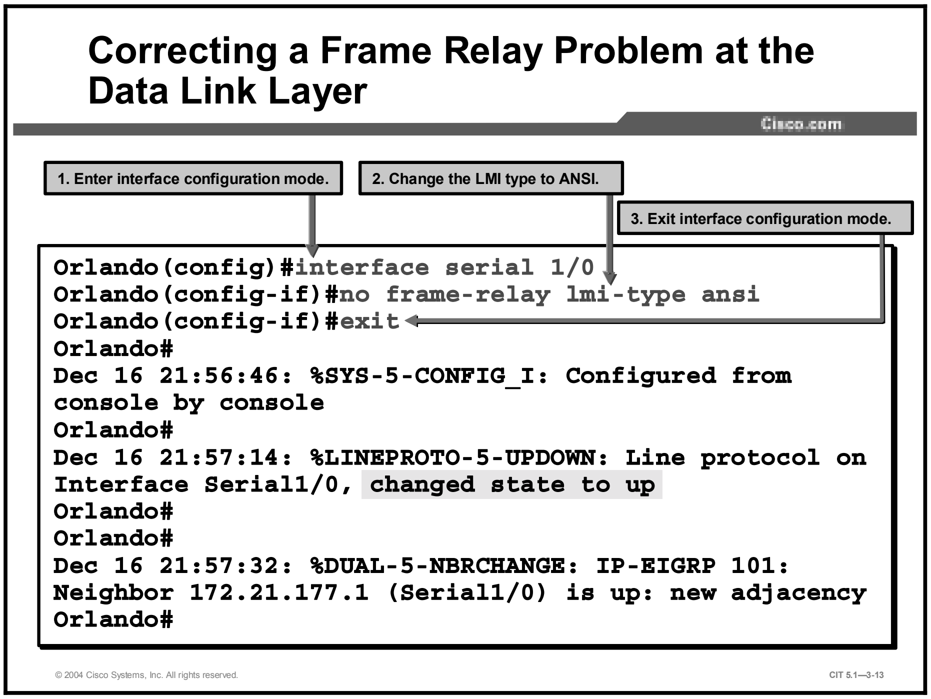


Example: Correcting a Frame Relay Problem at the Data Link Layer

Cisco.com

CIT 5.1—3-12

To verify the issue, you need to enter a Cisco IOS command that will allow the Cisco IOS software to auto-sense the LMI type on interface Serial1/0. You enter interface configuration mode on the Orlando router and apply the **no frame-relay lmi-type ansi** command.



Correcting a Frame Relay Problem at the Data Link Layer

1. Enter interface configuration mode.

2. Change the LMI type to ANSI.

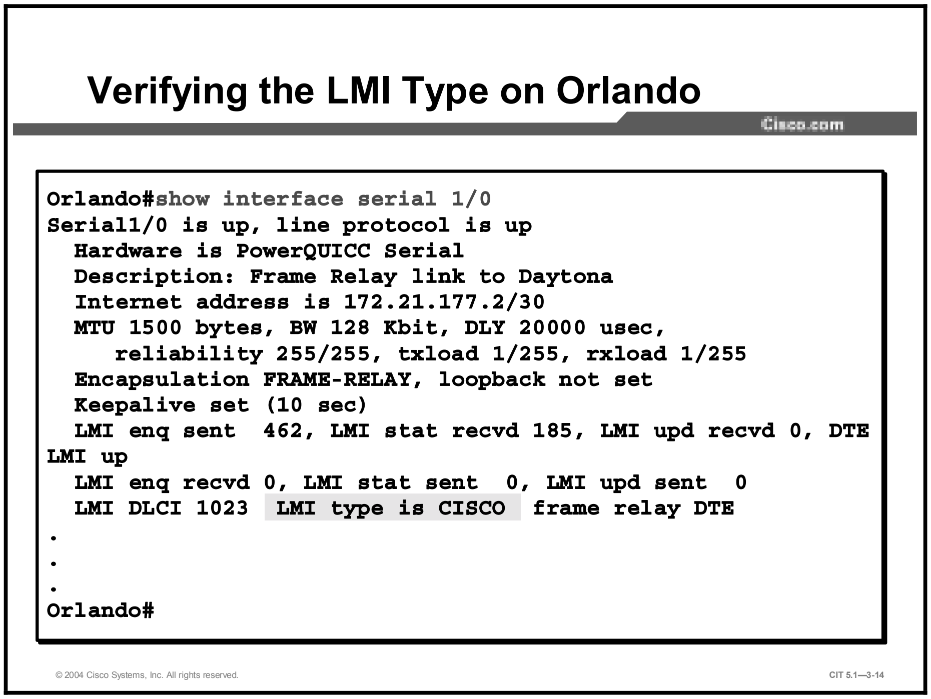
3. Exit interface configuration mode.

```
Orlando(config)#interface serial 1/0
Orlando(config-if)#no frame-relay lmi-type ansi
Orlando(config-if)#exit
Orlando#
Dec 16 21:56:46: %SYS-5-CONFIG_I: Configured from
console by console
Orlando#
Dec 16 21:57:14: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Serial1/0, changed state to up
Orlando#
Orlando#
Dec 16 21:57:32: %DUAL-5-NBRCHANGE: IP-EIGRP 101:
Neighbor 172.21.177.1 (Serial1/0) is up: new adjacency
Orlando#
```

CIT 5.1—3-13

The console messages show interface Serial1/0 changing to an active state. Therefore, the messages validate your assumption. The line protocol comes up, and an EIGRP neighbor adjacency re-establishes with the Daytona router.

Although you know that the line protocol is up if you have an EIGRP neighbor, you verify the current interface status.



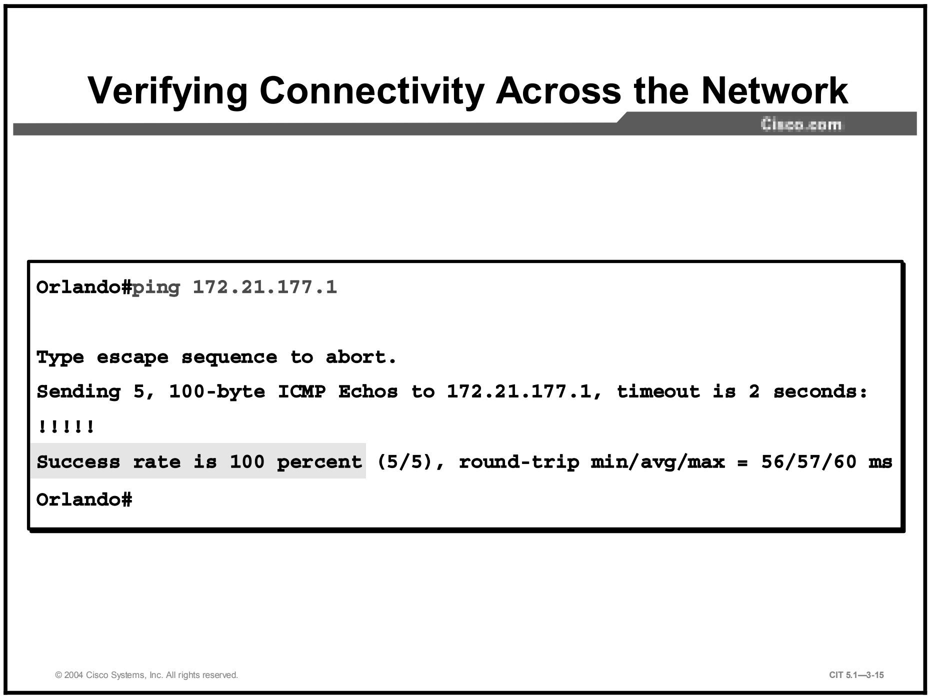
Verifying the LMI Type on Orlando

```
Orlando#show interface serial 1/0
Serial1/0 is up, line protocol is up
  Hardware is PowerQUICC Serial
  Description: Frame Relay link to Daytona
  Internet address is 172.21.177.2/30
  MTU 1500 bytes, BW 128 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation FRAME-RELAY, loopback not set
  Keepalive set (10 sec)
  LMI enq sent  462, LMI stat recvd 185, LMI upd recvd 0, DTE
LMI up
  LMI enq recvd 0, LMI stat sent  0, LMI upd sent  0
  LMI DLCI 1023  LMI type is CISCO  frame relay DTE
.
.
.
Orlando#
```

CIT 5.1—3-14

You see that the Cisco IOS software has auto-sensed a Cisco LMI type. The Frame Relay provider changed the LMI type, which caused your link to go down.

As a final validation that the data link issue has been resolved, you use the **ping** command across the link to verify connectivity across the network, data link, and physical layers.



Verifying Connectivity Across the Network

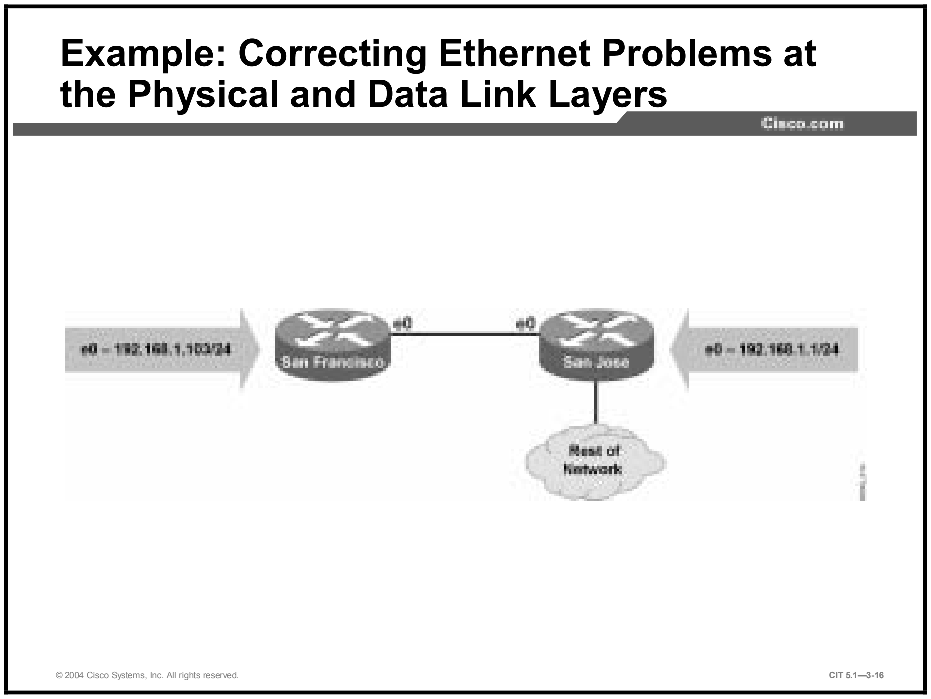
```
Orlando#ping 172.21.177.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.21.177.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 56/57/60 ms
Orlando#
```

CIT 5.1—3-15

The ping test is successful. You have resolved the data link layer issue, and your network is running again. You *will* need to discuss unscheduled changes with your Frame Relay carrier in the morning.

Example: Correcting an Ethernet Problem at the Physical and Data Link Layers

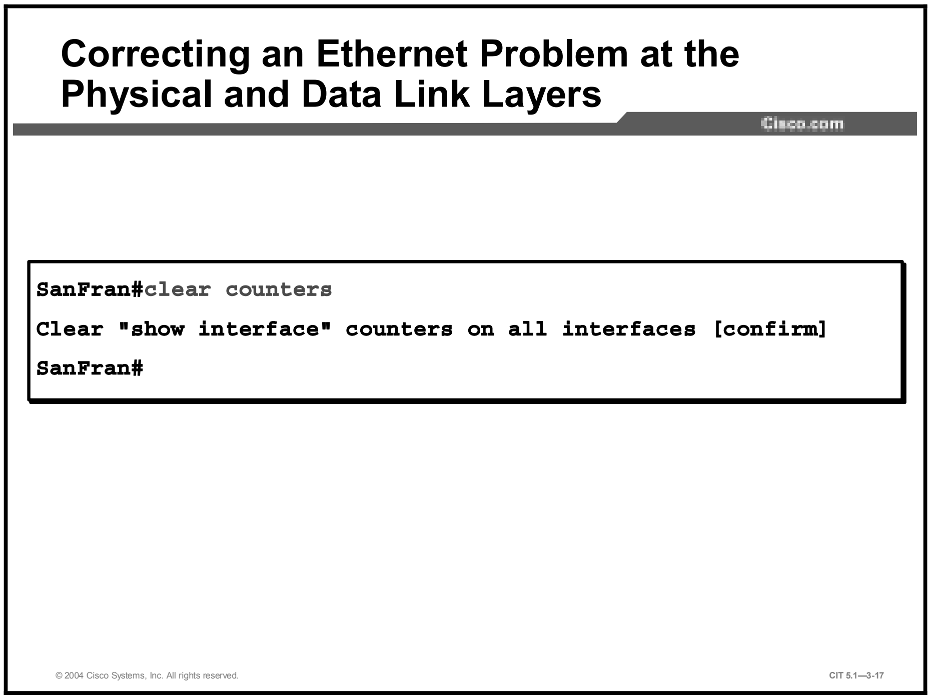
You have isolated a problem believed to be an incorrectly seated cable in an Ethernet interface.



Example: Correcting Ethernet Problems at the Physical and Data Link Layers

CIT 5.1—3-16

Given this condition, you disconnect and reconnect both ends of the Ethernet cable, connecting to the interface named Ethernet 0 on the SanFran router. This will ensure that the cable is properly seated. Once that is done, you enter the **clear counters** command to reset all of the data and error counters on the interface to zero.

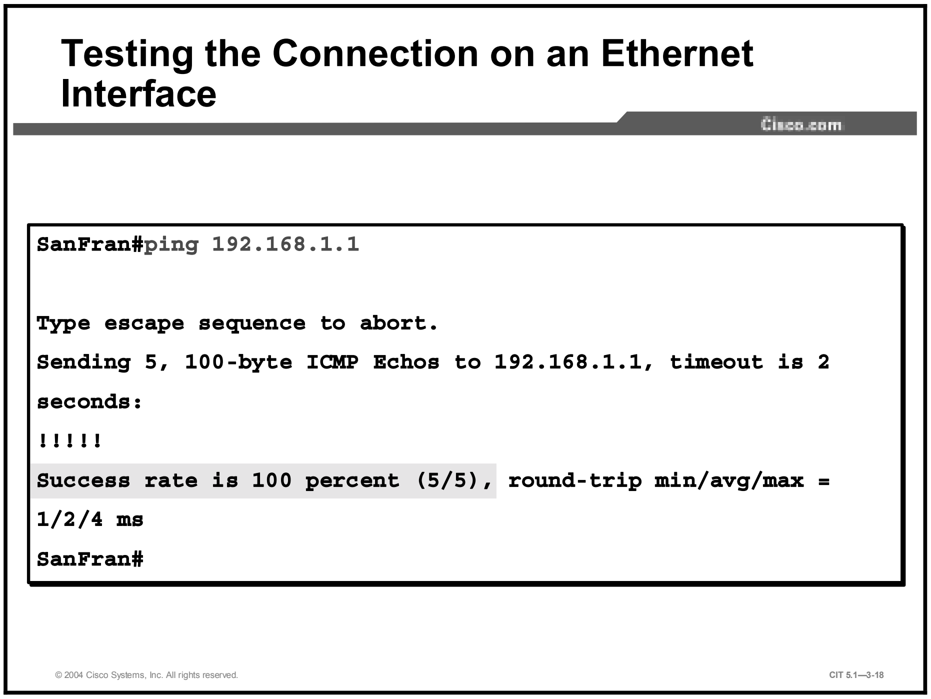


Correcting an Ethernet Problem at the Physical and Data Link Layers

```
SanFran#clear counters
Clear "show interface" counters on all interfaces [confirm]
SanFran#
```

CIT 5.1—3-17

You ping the interface to test if it is operating properly.



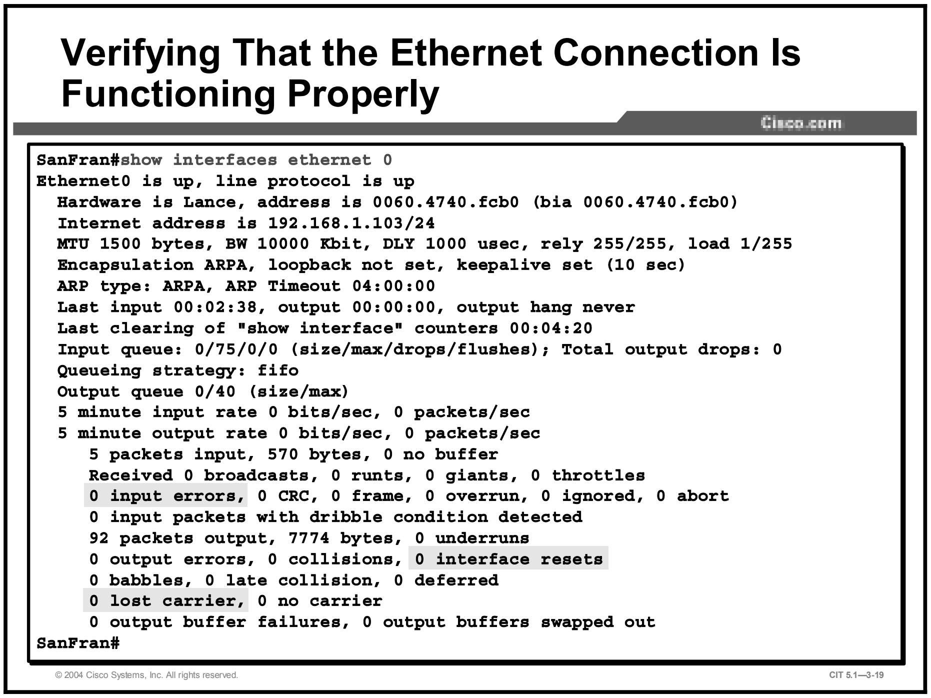
Testing the Connection on an Ethernet Interface

```
SanFran#ping 192.168.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2
seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
1/2/4 ms
SanFran#
```

© 2004 Cisco Systems, Inc. All rights reserved.

CIT 5.1—3-18

The connection is made successfully. You enter the **show interface** command to verify that you are no longer receiving any errors on the interface.



Verifying That the Ethernet Connection Is Functioning Properly

```
SanFran#show interfaces ethernet 0
Ethernet0 is up, line protocol is up
  Hardware is Lance, address is 0060.4740.fcb0 (bia 0060.4740.fcb0)
  Internet address is 192.168.1.103/24
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec, rely 255/255, load 1/255
  Encapsulation ARPA, loopback not set, keepalive set (10 sec)
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:02:38, output 00:00:00, output hang never
  Last clearing of "show interface" counters 00:04:20
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     5 packets input, 570 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 input packets with dribble condition detected
     92 packets output, 7774 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
SanFran#
```

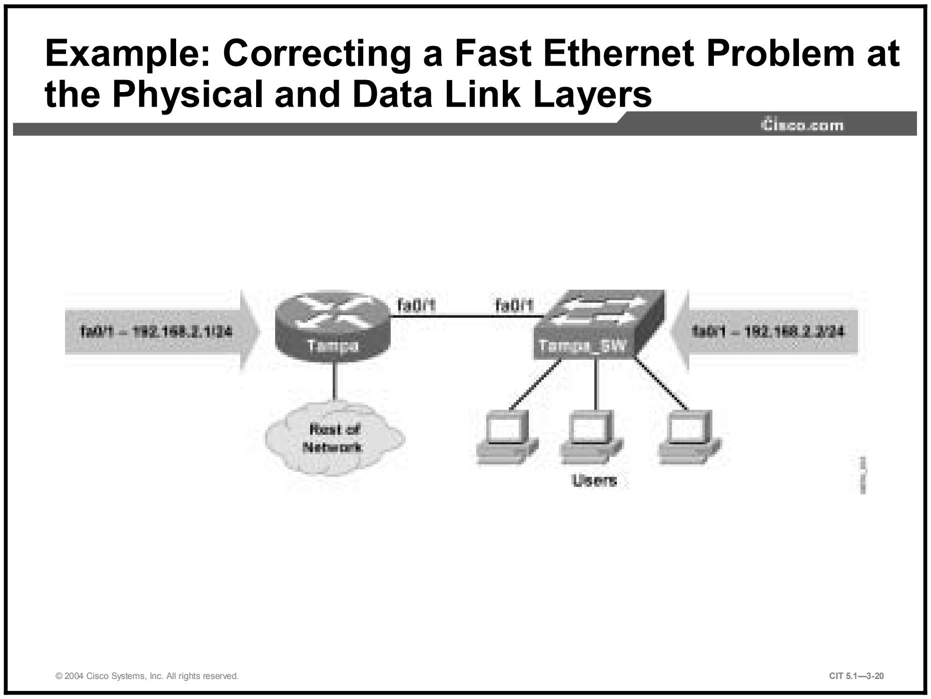
© 2004 Cisco Systems, Inc. All rights reserved.

CIT 5.1—3-19

Note that the error counters remain at zero. The problem with the incorrectly seated cable has been corrected, and the interface is functioning properly.

Example: Correcting Fast Ethernet Problems at the Physical and Data Link Layers

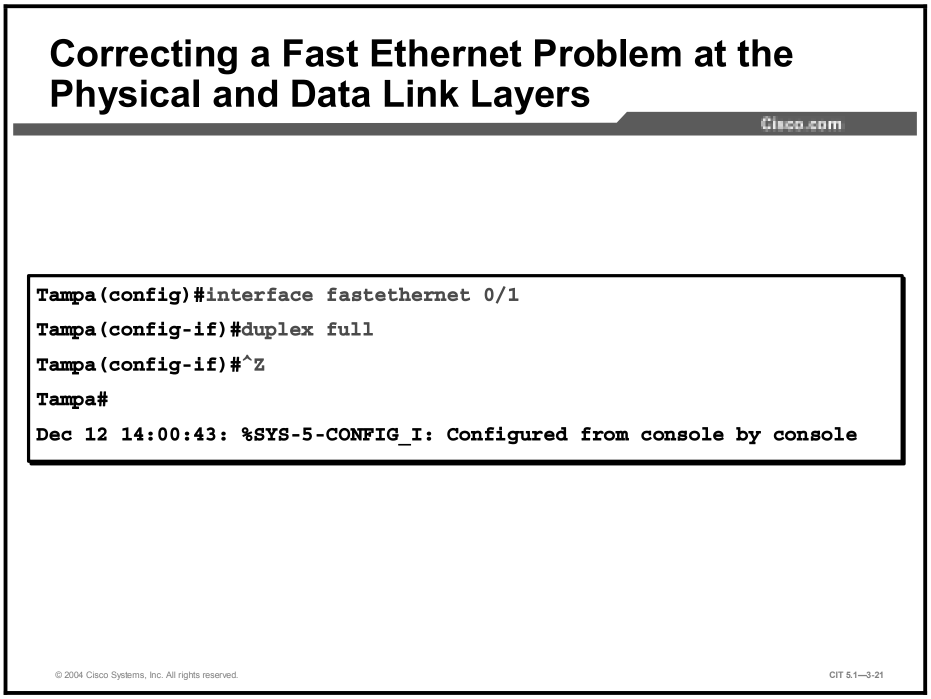
Given a problem with a duplex mismatch on Fast Ethernet interfaces, you will change the configuration so that the duplex configurations match.



Example: Correcting a Fast Ethernet Problem at the Physical and Data Link Layers

CIT 5.1—3-20

Both of these devices are capable of communicating at full-duplex mode; therefore, you must change the duplex configuration of the Tampa router to match the switch.

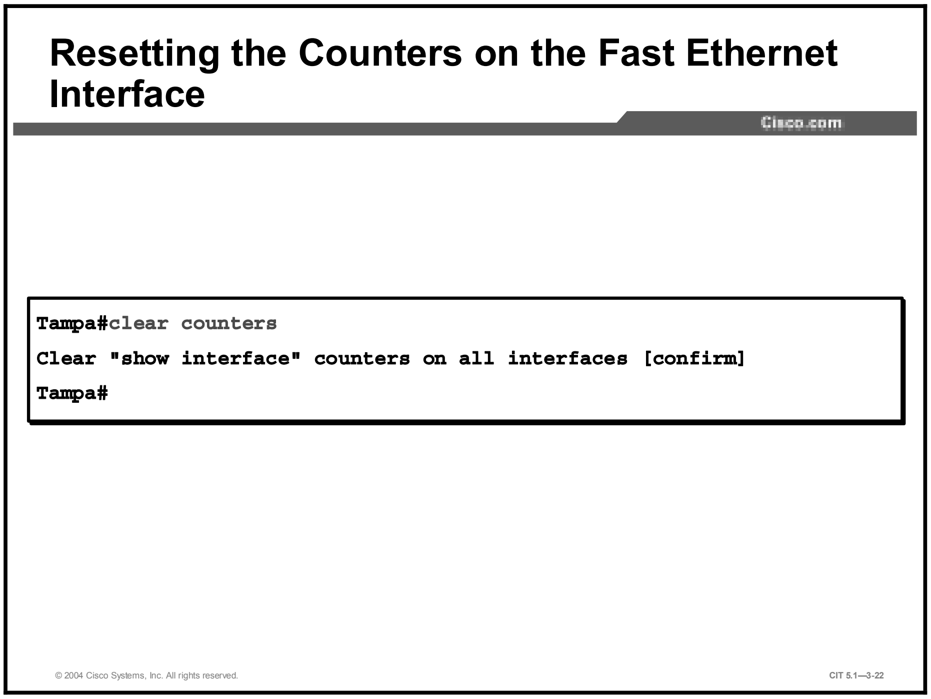


Correcting a Fast Ethernet Problem at the Physical and Data Link Layers

```
Tampa(config)#interface fastethernet 0/1
Tampa(config-if)#duplex full
Tampa(config-if)#^Z
Tampa#
Dec 12 14:00:43: %SYS-5-CONFIG_I: Configured from console by console
```

CIT 5.1—3-21

Use the **clear counters** command to reset the interface counters.

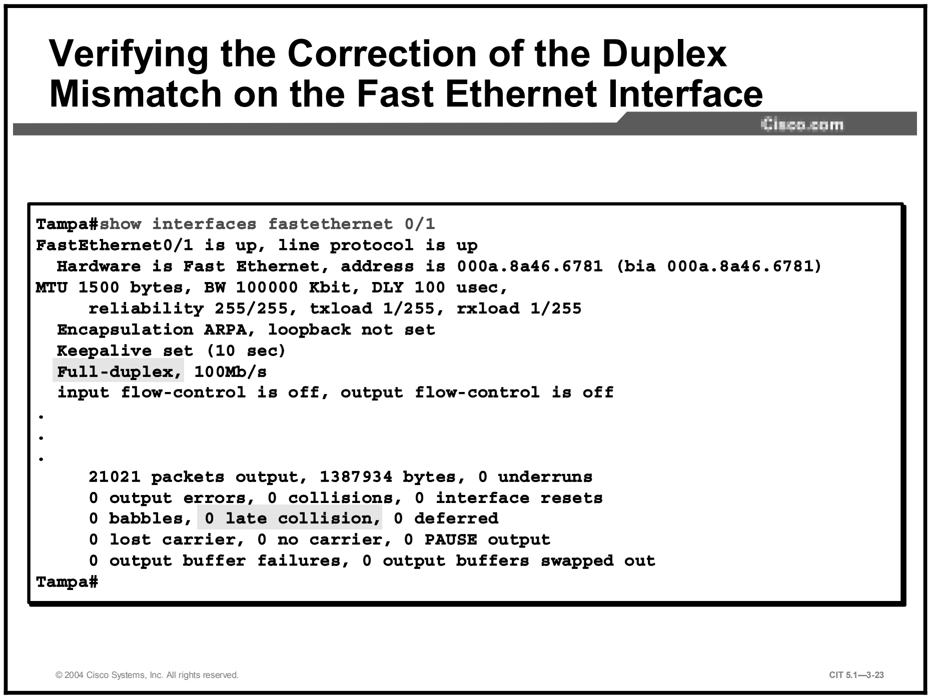


Resetting the Counters on the Fast Ethernet Interface

```
Tampa#clear counters
Clear "show interface" counters on all interfaces [confirm]
Tampa#
```

CIT 5.1—3-22

You ask the operations group to test its application, and then you enter the **show interface** command to verify that the interface is configured properly and no longer indicating any errors.



Verifying the Correction of the Duplex Mismatch on the Fast Ethernet Interface

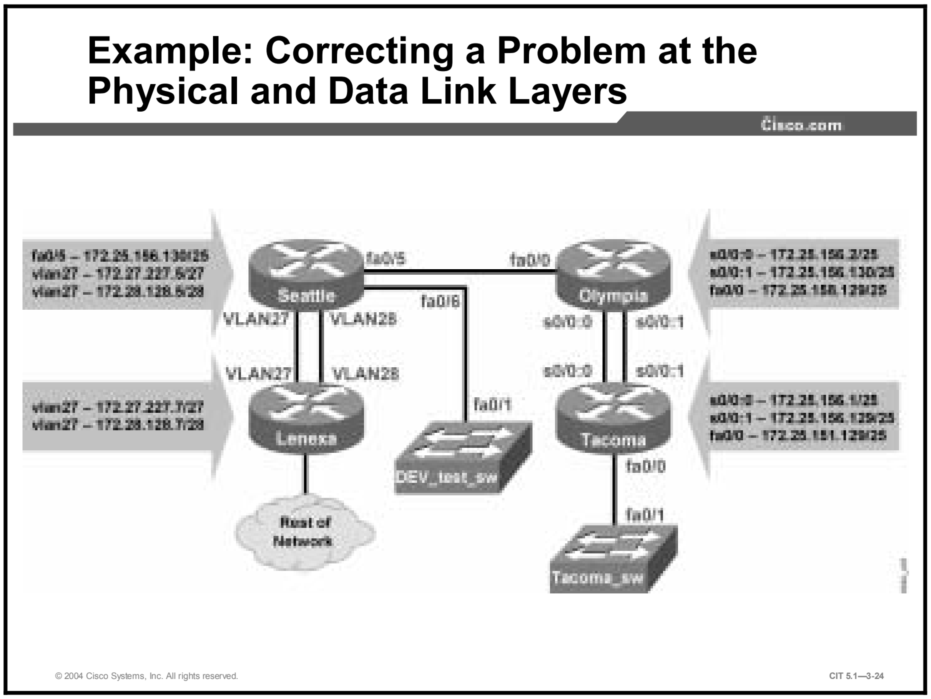
```
Tampa#show interfaces fastethernet 0/1
FastEthernet0/1 is up, line protocol is up
  Hardware is Fast Ethernet, address is 000a.8a46.6781 (bia 000a.8a46.6781)
MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s
  input flow-control is off, output flow-control is off
.
.
.
     21021 packets output, 1387934 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier, 0 PAUSE output
     0 output buffer failures, 0 output buffers swapped out
Tampa#
```

CIT 5.1—3-23

The command output indicates that the interface is operating in full-duplex mode and that there are zero late collisions. The duplex mismatch on the Fast Ethernet interface has been corrected.

Example: Correcting a Problem at the Physical and Data Link Layers

You have isolated a problem where a new switch was overwriting the VTP database on the Seattle Layer 3 switch because Seattle was in VTP server mode.

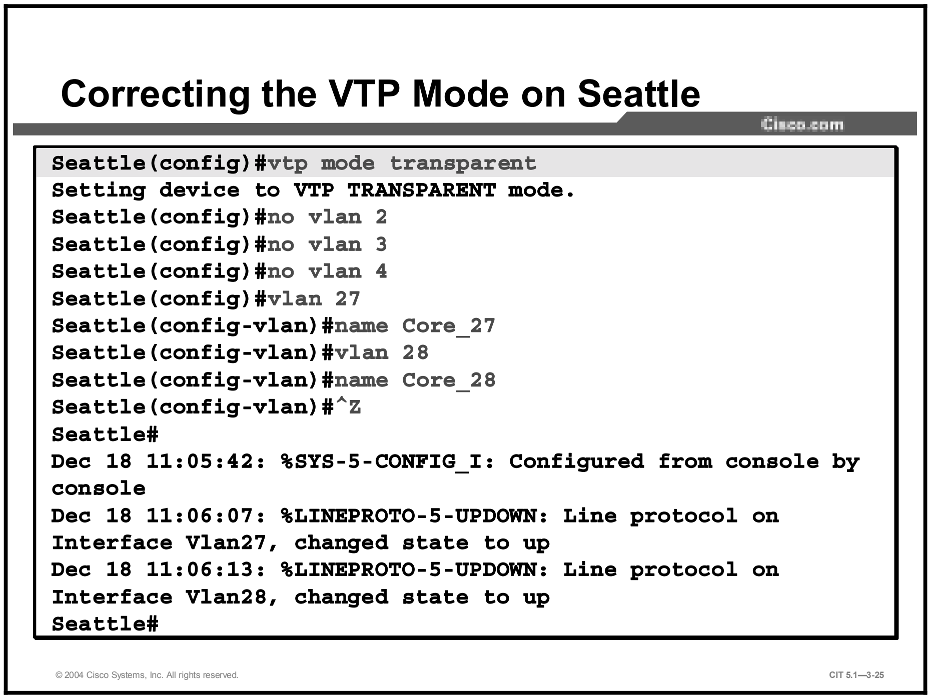


Example: Correcting a Problem at the Physical and Data Link Layers

CIT 5.1—3-24

Given this condition, you go into configuration mode on the Seattle router to resolve the issue.

As a first step, you configure the **vtp mode transparent** command to set the VTP mode of the switch to transparent.



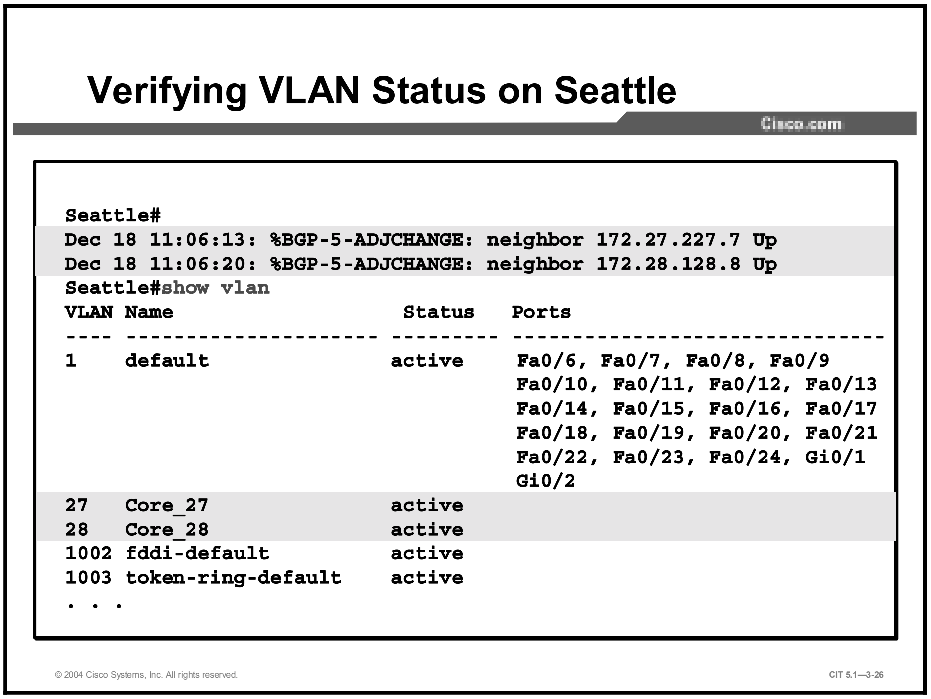
Correcting the VTP Mode on Seattle

```
Seattle(config)#vtp mode transparent
Setting device to VTP TRANSPARENT mode.
Seattle(config)#no vlan 2
Seattle(config)#no vlan 3
Seattle(config)#no vlan 4
Seattle(config)#vlan 27
Seattle(config-vlan)#name Core_27
Seattle(config-vlan)#vlan 28
Seattle(config-vlan)#name Core_28
Seattle(config-vlan)#^Z
Seattle#
Dec 18 11:05:42: %SYS-5-CONFIG_I: Configured from console by
console
Dec 18 11:06:07: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Vlan27, changed state to up
Dec 18 11:06:13: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Vlan28, changed state to up
Seattle#
```

CIT 5.1—3-25

You also remove the nonproduction VLANs, and configure VLAN27 and VLAN28. The console messages show the line protocol on interface VLAN27 and VLAN28 changing to an active state.

You also notice console messages showing that the Border Gateway Protocol (BGP) neighbor adjacencies are up. Although the neighbors would not be present without active VLANs, you use the **show vlan** command to verify the VLAN status.



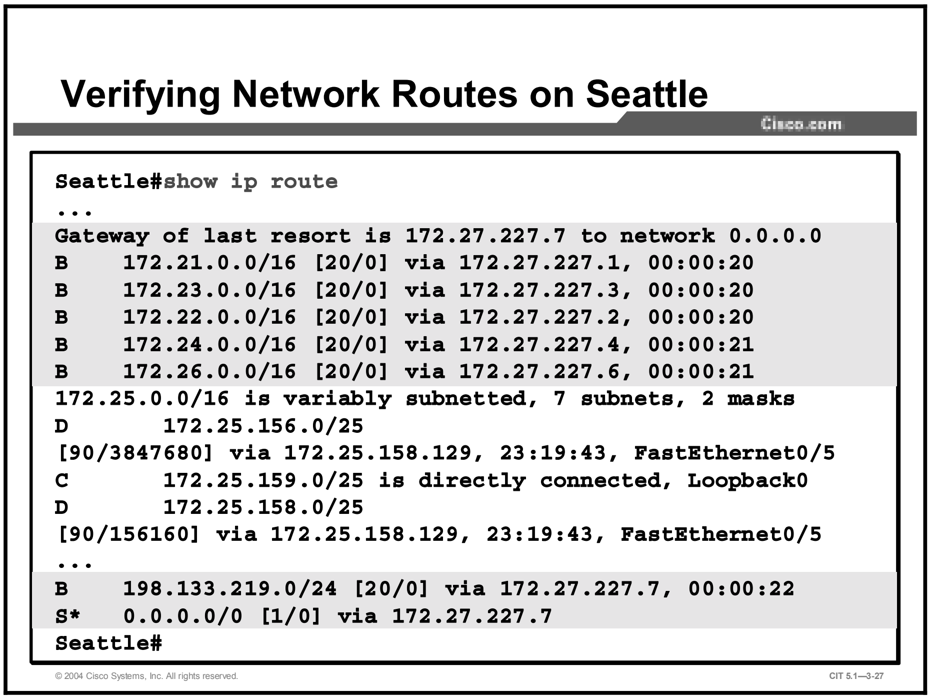
Verifying VLAN Status on Seattle

```
Seattle#
Dec 18 11:06:13: %BGP-5-ADJCHANGE: neighbor 172.27.227.7 Up
Dec 18 11:06:20: %BGP-5-ADJCHANGE: neighbor 172.28.128.8 Up
Seattle#show vlan
VLAN Name                  Status    Ports
---- -------------------- --------- ------------------------------
1    default              active     Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                     Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                     Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                     Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                     Fa0/22, Fa0/23, Fa0/24, Gi0/1
                                     Gi0/2
27   Core_27              active
28   Core_28              active
1002 fddi-default         active
1003 token-ring-default   active
. . .
```

© 2004 Cisco Systems, Inc. All rights reserved. CIT 5.1—3-26

You see that VLAN27 and VLAN28 are active.

You use the **show ip route** command to verify network connectivity out of the division.



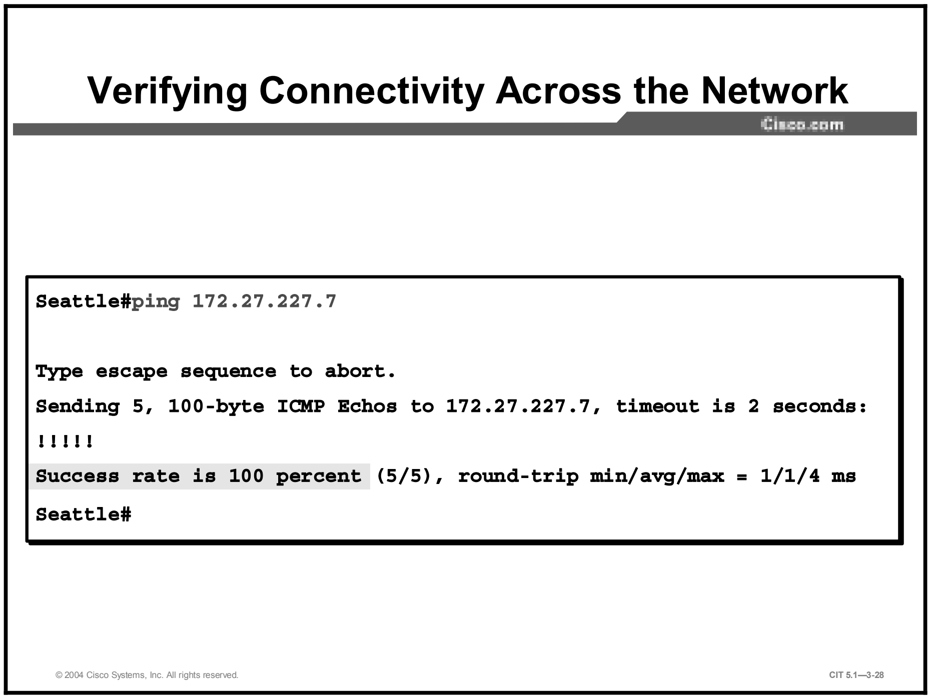
Verifying Network Routes on Seattle

```
Seattle#show ip route
...
Gateway of last resort is 172.27.227.7 to network 0.0.0.0
B    172.21.0.0/16 [20/0] via 172.27.227.1, 00:00:20
B    172.23.0.0/16 [20/0] via 172.27.227.3, 00:00:20
B    172.22.0.0/16 [20/0] via 172.27.227.2, 00:00:20
B    172.24.0.0/16 [20/0] via 172.27.227.4, 00:00:21
B    172.26.0.0/16 [20/0] via 172.27.227.6, 00:00:21
172.25.0.0/16 is variably subnetted, 7 subnets, 2 masks
D       172.25.156.0/25
[90/3847680] via 172.25.158.129, 23:19:43, FastEthernet0/5
C       172.25.159.0/25 is directly connected, Loopback0
D       172.25.158.0/25
[90/156160] via 172.25.158.129, 23:19:43, FastEthernet0/5
...
B    198.133.219.0/24 [20/0] via 172.27.227.7, 00:00:22
S*   0.0.0.0/0 [1/0] via 172.27.227.7
Seattle#
```

© 2004 Cisco Systems, Inc. All rights reserved. CIT 5.1—3-27

You see that BGP routes from the other divisions have reappeared in the routing table.

As a final validation, you use the **ping** command to verify connectivity across the network, data link, and physical layers.



Verifying Connectivity Across the Network

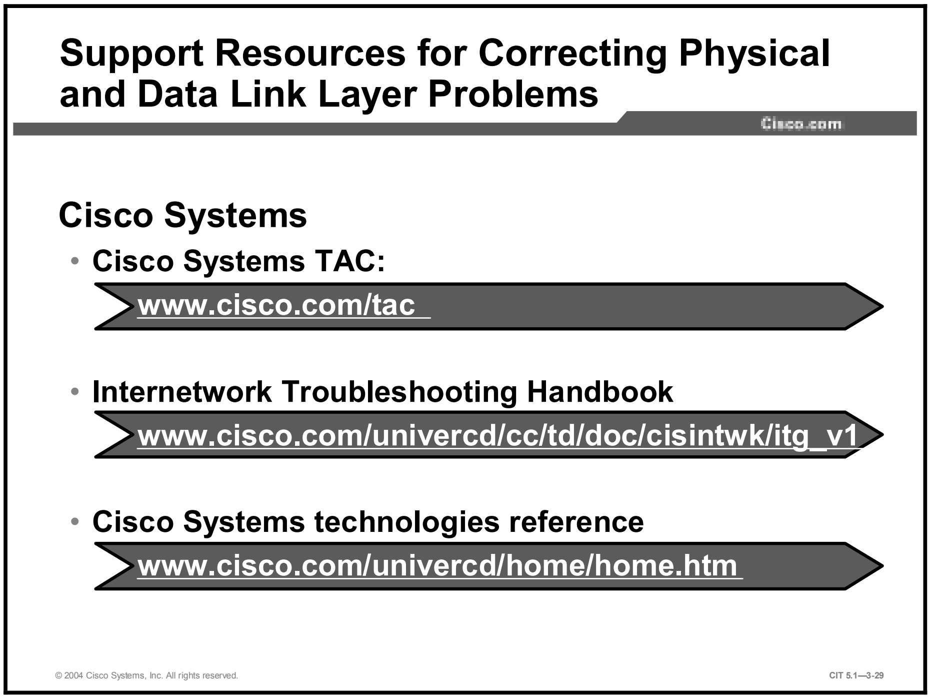
```
Seattle#ping 172.27.227.7

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.27.227.7, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
Seattle#
```

CIT 5.1—3-28

The successful ping test verifies that network connectivity has been restored. You will now discuss with Operations adding test devices to production networks.

Identifying Physical and Data Link Layer Support Resources

This topic lists support resources to assist you in correcting problems at the physical and data link layers.

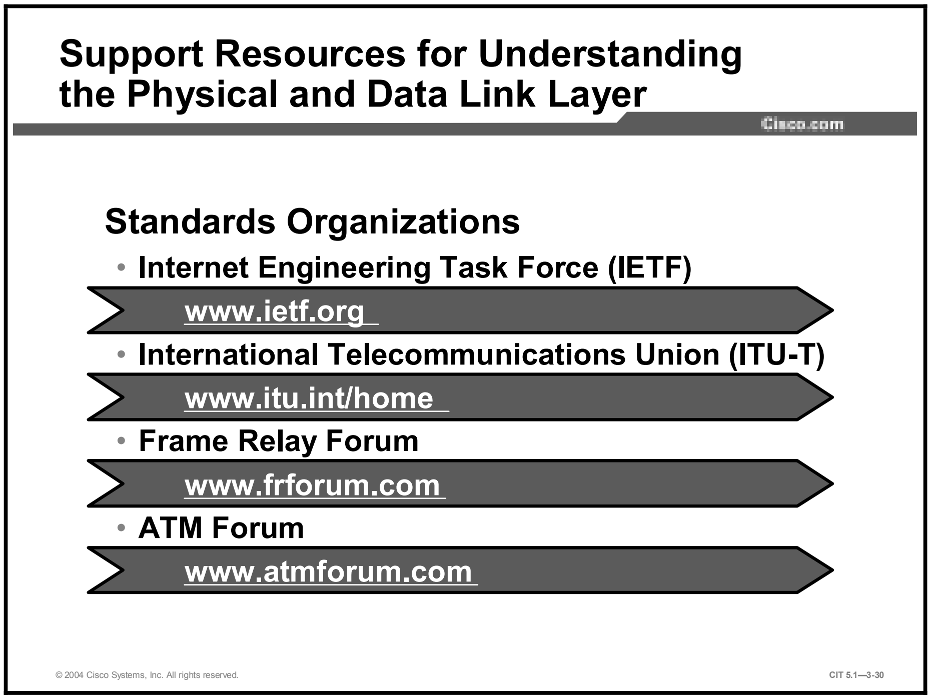


Support Resources for Correcting Physical and Data Link Layer Problems

Cisco Systems

- **Cisco Systems TAC:**
  - www.cisco.com/tac
- **Internetwork Troubleshooting Handbook**
  - www.cisco.com/univercd/cc/td/doc/cisintwk/itg_v1
- **Cisco Systems technologies reference**
  - www.cisco.com/univercd/home/home.htm

CIT 5.1—3-29



Support Resources for Understanding the Physical and Data Link Layer

Standards Organizations

- Internet Engineering Task Force (IETF)
  - www.ietf.org
- International Telecommunications Union (ITU-T)
  - www.itu.int/home
- Frame Relay Forum
  - www.frforum.com
- ATM Forum
  - www.atmforum.com

CIT 5.1—3-30

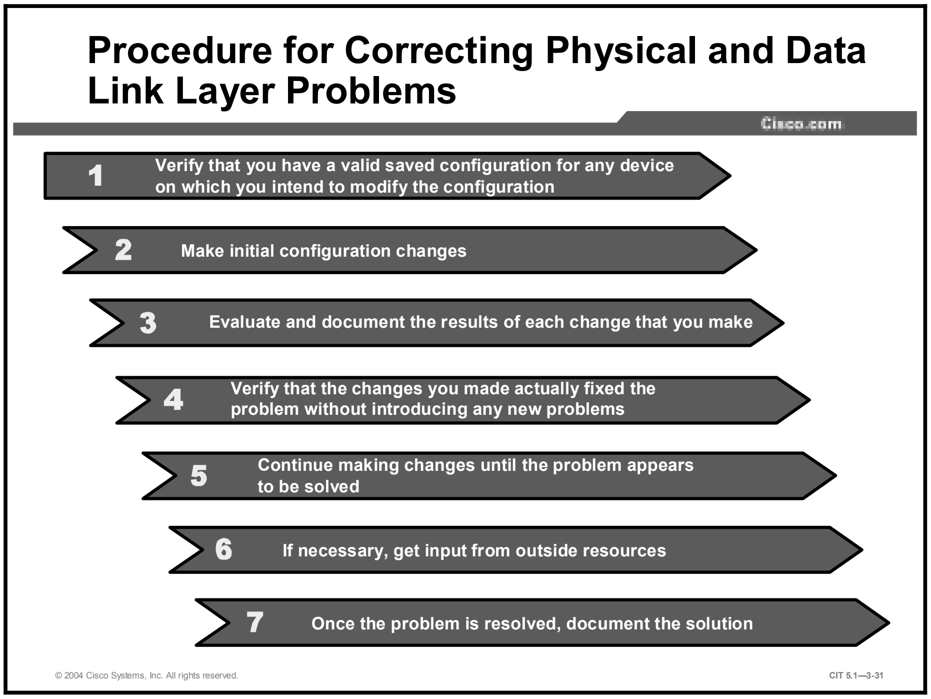
Despite your knowledge and experience about networking, there will still be times when you will need to consult an outside resource. These support resources are commonly used as reference materials for commands and configuration procedures and research for technology-specific information and industry standards. Given the ability to use online support resources to do effective research, you save time that you may have otherwise spent on the phone with a support professional. You also save the money that you would have committed to hiring a consultant.

For command and configuration references, the Cisco Systems website has one of the largest collections of networking information on the Internet. Visit the Technical Assistance Center (TAC), Cisco.com, and technology reference pages to find information for troubleshooting Cisco Systems products. From these locations, you can search on a specific technology, such as Ethernet, Frame Relay, serial line, or ATM. It is often helpful to narrow your search by including phrases such as “configuration examples” or “troubleshooting.”

To learn more about industry standards, visit the Internet Engineering Task Force (IETF), International Telecommunication Union Telecommunication Standardization Sector (ITU-T), Frame Relay Forum, and ATM Forum. These sites contain detailed documentation about a wide array of networking technologies.

Correcting Problems Occurring at the Physical and Data Link Layers

This topic lists the steps troubleshooters should take to correct problems at the physical and data link layers.



Procedure for Correcting Physical and Data Link Layer Problems

Cisco.com

1. Verify that you have a valid saved configuration for any device on which you intend to modify the configuration
2. Make initial configuration changes
3. Evaluate and document the results of each change that you make
4. Verify that the changes you made actually fixed the problem without introducing any new problems
5. Continue making changes until the problem appears to be solved
6. If necessary, get input from outside resources
7. Once the problem is resolved, document the solution

© 2004 Cisco Systems, Inc. All rights reserved.

CIT 5.1—3-31

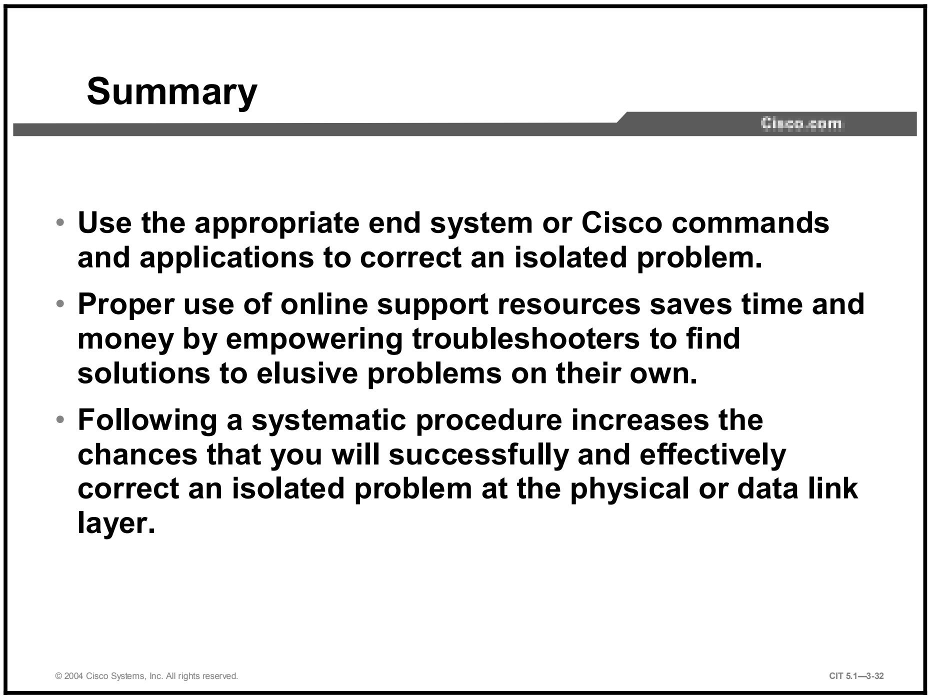
The table lists the suggested steps for correcting an isolated problem at the physical and data link layers.

Procedure for Correcting Problems Occurring at the Physical and Data Link Layers

Step	Description
1	Verify that you have a valid saved configuration for any device on which you intend to modify the configuration. This provides for eventual recovery to a known initial state.
2	Make initial hardware and software configuration changes. If the correction requires more than one change, make only one change at a time.
3	Evaluate and document the changes and the results of each change that you make. If you perform your problem-solving steps and the results are unsuccessful, immediately undo the changes. If the problem is intermittent, you may need to wait to see if the problem occurs again before you can evaluate the effect of your changes.
4	Verify that the changes you made actually fixed the problem without introducing any new problems. The network should be returned to the baseline operation, and no new or old symptoms should be present. If the problem is not solved, undo all the changes that you made. If you discover new or additional problems while you are making corrections, step back and modify your correction plan.
5	Continue making changes until the original problem appears to be solved.
6	If necessary, get input from outside resources. If none of your attempts to correct the problem are successful, take the problem to another person. This may be a coworker, consultant, or Cisco TAC. On some occasions, you may need to generate various crash files. This creates output that a specialist at Cisco Systems can analyze.
7	Once the problem is resolved, document the solution.

Summary

This topic summarizes the key points discussed in this lesson.



Summary

- Use the appropriate end system or Cisco commands and applications to correct an isolated problem.
- Proper use of online support resources saves time and money by empowering troubleshooters to find solutions to elusive problems on their own.
- Following a systematic procedure increases the chances that you will successfully and effectively correct an isolated problem at the physical or data link layer.

CIT 5.1—3-32

References

For additional information, refer to these resources:

- Cisco online documentation: http://www.cisco.com/univercd/home/home.htm
- Cisco Technical Assistance Center (TAC): http://www.cisco.com/tac/

Next Steps

For the associated case study and lab exercises, refer to the following sections of the course Lab Guide:

- Case Study (Trouble Ticket B) 3-1: Isolating Physical and Data Link Layer Problems
- Lab Exercise (Trouble Ticket B) 3-1: Correcting Problems at the Physical and Data Link Layers
- Lab Exercise (Trouble Ticket C) 3-2: Troubleshooting Problems at the Physical and Data Link Layers

Quiz

Use the practice items here to review what you have learned in this lesson. The correct answers are found in the Quiz Answer Key.

Q1) Which command is used at an end system to correct problems at the data link layer related to resolving network and data link layer addresses?

A) **shutdown**

B) **interface**

C) **clock rate**

D) **arp -d**

Q2) Which website would you most likely use to find the latest detailed technical documentation about the PPP protocol?

A) www.apple.com

B) www.linux.org

C) www.sniffers.com

D) www.ietf.org

Q3) List the steps for correcting an isolated problem at the physical or data link layer in the recommended order.

_____ 1. Evaluate and document the results of each change that you make.

_____ 2. Document the solution.

_____ 3. Get input from outside resources.

_____ 4. Continue making changes until the original problem appears to be solved.

_____ 5. Verify that the changes you made actually fixed the problem without introducing any new problems.

_____ 6. Make initial changes to the configuration.

Quiz Answer Key

Q1) D

Relates to: Identifying Commands and Applications to Correct Problems Occurring at the Physical and Data Link Layers

Q2) D

Relates to: Identifying Physical and Data Link Layer Support Resources

Q3) Correct order: 2, 6, 5, 4, 3, 1

Relates to: Correcting Problems Occurring at the Physical and Data Link Layers

Module 4

Resolving Problems at the Network Layer

Overview

Now that you have used the symptoms you gathered to isolate and correct problems at the physical and data link layers, you will find that the process is the same for correcting problems at the network layer. However, the symptoms of the problem differ as do the commands and applications that you use to successfully resolve problems. In this module, you will perform the isolation and correction phases of the general troubleshooting process to resolve failure and optimization problems at the network layer of the Open Systems Interconnection (OSI) model.

Module Objectives

Upon completing this module, you will be able to:

- Isolate problems occurring at the network layer
- Correct problems occurring at the network layer

Module Outline

The module contains these components:

- Isolating the Problem
- Correcting the Problem

Isolating the Problem

Overview

A troubleshooter applies the general troubleshooting process of gathering and analyzing symptoms, and then isolating and correcting problems at the network layer. The process is the same regardless of the logical layers to which the process is applied; however, the focus of this lesson is logical addressing, subnet masks, and routing protocols. In this lesson, you will analyze symptoms and use commands and applications to isolate problems at the network layer.

Relevance

The primary responsibility of the network layer is to manage the movement of data between networks and to find the best path for data to travel toward a destination. If a problem arises at this layer, the data will not delivered to the destination, the data will not delivered as quickly as it should be, or the data will be delivered in deference to other higher priority traffic. This information will make you a better troubleshooter to effectively isolate problems at the network layer, thus avoiding extended or periodic loss of packet delivery and suboptimal delivery performance.

Objectives

Upon completing this lesson, you will be able to:

- Identify the symptoms of problems occurring at the network layer
- Analyze Cisco command and application output to isolate problems occurring at the network layer
- Identify end-system commands and applications used to isolate problems occurring at the network layer
- Isolate problems occurring at the network layer

Learner Skills and Knowledge

To benefit fully from this lesson, you must have these prerequisite skills and knowledge:

- The ability to apply layered model troubleshooting approaches
- Familiarity with Cisco command syntax and technologies covered in the Cisco *Building Scalable Cisco Internetworks* (BSCI), *Building Cisco Multilayer Switched Networks* (BCMSN), and *Building Cisco Remote Access Networks* (BCRAN) courses

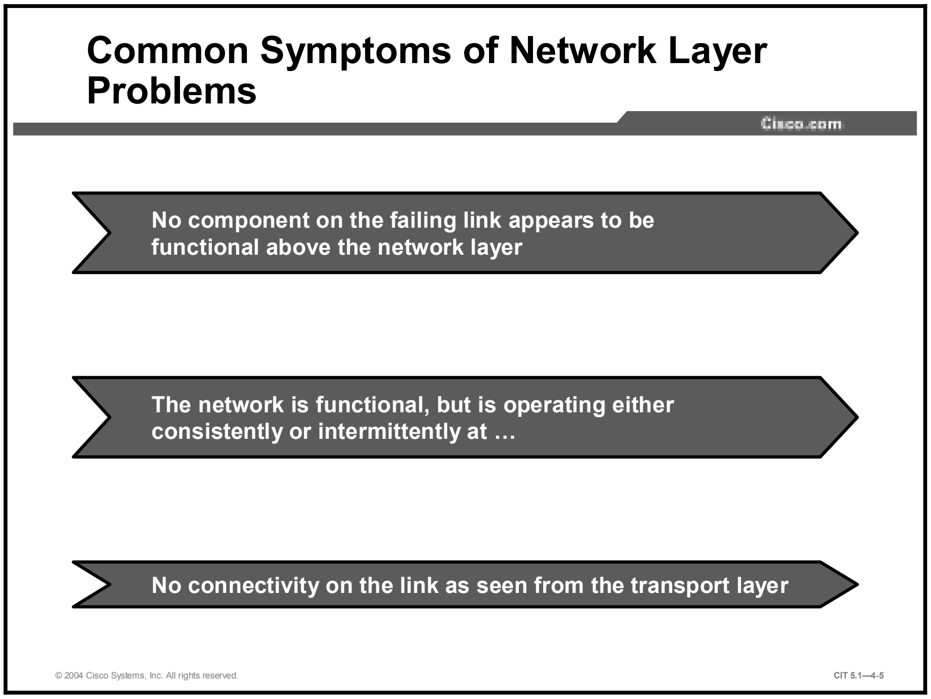
Outline

This lesson includes these topics:

- Overview
- Identifying the Symptoms of Problems Occurring at the Network Layer
- Analyzing Cisco Commands and Applications Used to Isolate Problems Occurring at the Network Layer
- Identifying End-System Commands and Applications Used to Isolate Problems Occurring at the Network Layer
- Isolating Problems Occurring at the Network Layer
- Summary
- Quiz

Identifying the Symptoms of Problems Occurring at the Network Layer

This topic identifies the symptoms of problems occurring at the network layer that troubleshooters should be able to identify.



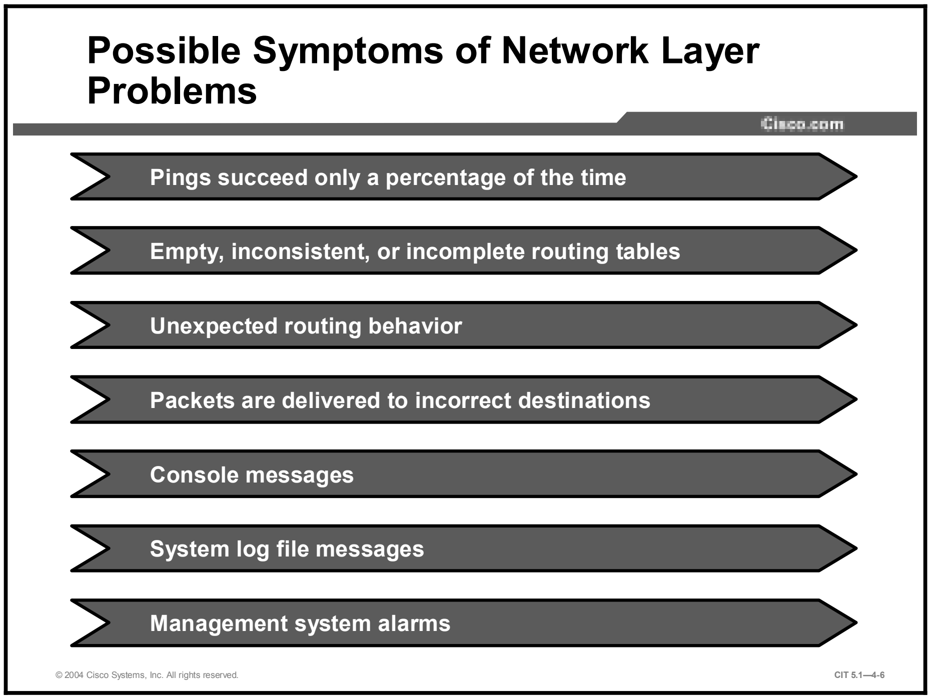
Common Symptoms of Network Layer Problems

- No component on the failing link appears to be functional above the network layer
- The network is functional, but is operating either consistently or intermittently at …
- No connectivity on the link as seen from the transport layer

CIT 5.1—4-5

The failure of a network component at the network layer has the potential to cause a loss of connectivity with peers on other devices. It may be difficult for a troubleshooter to determine the layer in which a problem is located. This is because a symptom of that problem may also be shared with physical and data link layer failure problems. If your troubleshooting efforts show that there are no problems at the physical and data link layers, you have a concrete indication that your problem resides at the network layer or higher.

You can identify a possible optimization problem on a link at the network layer because data will be transferred in a slow, sporadic, or unexpected manner compared to the data transfer rate documented in your baseline. Symptoms short of a complete failure to route packets may include misrouted packets that are ultimately lost or excessive transit delays.



Possible Symptoms of Network Layer Problems

- Pings succeed only a percentage of the time
- Empty, inconsistent, or incomplete routing tables
- Unexpected routing behavior
- Packets are delivered to incorrect destinations
- Console messages
- System log file messages
- Management system alarms

CIT 5.1—4-6

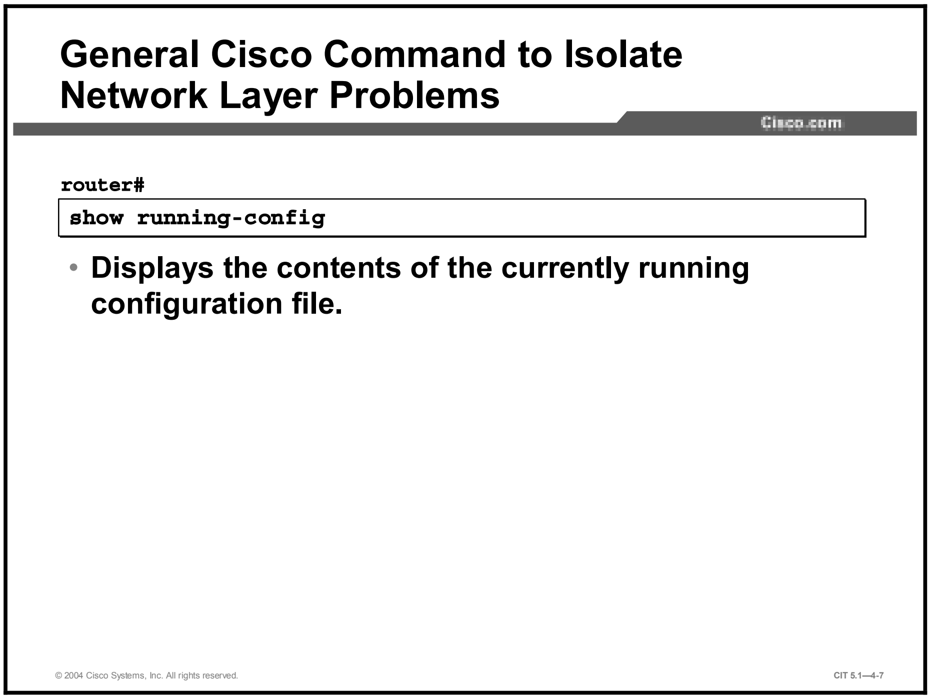
Not all network layer problems present the same symptoms. These symptoms can include such things as misrouted packets and console messages being displayed by the system. The following example shows a console message that a troubleshooter may see if duplicate IP addresses exist on a network:

```
Feb 17 11:21:47: %IP-4-DUPADDR: Duplicate address 172.44.118.1
on FastEthernet0/1, sourced by 000a.8a44.de40
```

Other messages, such as ping failures or Internet Control Message Protocol (ICMP) unreachable messages, may be present. You may also receive an alarm from the network management system or see evidence of a problem in a system log file.

Analyzing Cisco Commands and Applications Used to Isolate Problems Occurring at the Network Layer

This topic analyzes the output of Cisco commands and applications with the purpose of helping troubleshooters isolate a problem occurring at the network layer.



General Cisco Command to Isolate Network Layer Problems

```
router#
show running-config
```

- **Displays the contents of the currently running configuration file.**

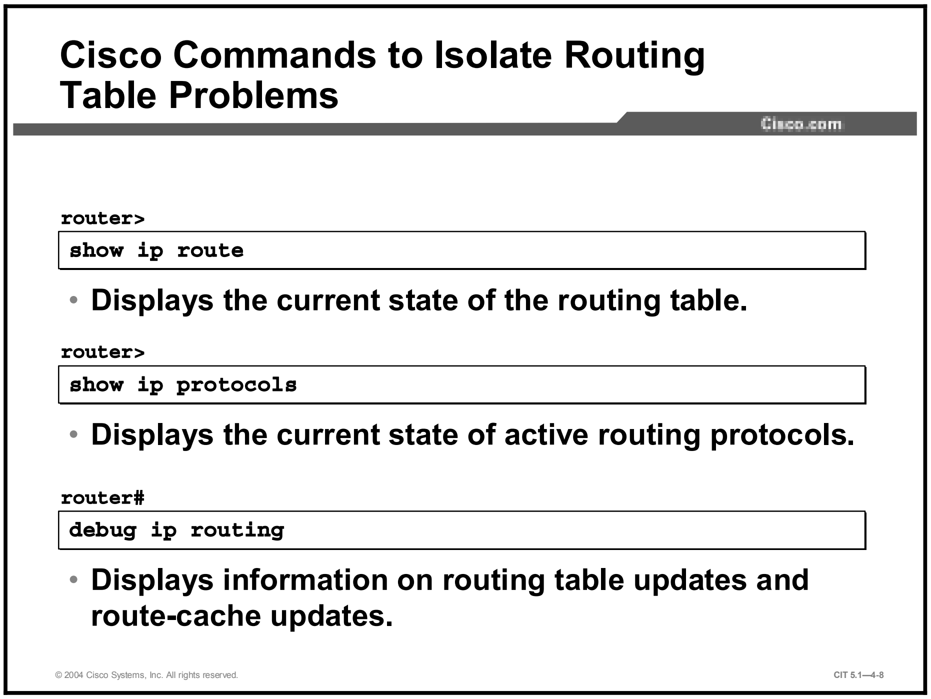
CIT 5.1—4-7

The Cisco commands listed in the table display information about several networking layers. A troubleshooter uses the information from these commands to isolate problems at the network layer. Note that the commands covered previously in the course are shown in the command tables, but not in the slides.

General Cisco Commands to Isolate Network Layer Problems

Command	Description
ping {*host* | *ip-address*}	Sends an echo request packet to an address, then waits for a reply. The *host* | *ip-address* variable is the IP alias or IP address of the target system.
traceroute [**destination**]	Identifies a path to a destination device.
[**no**] **debug ?**	Displays a list of options for enabling or disabling debugging events on a device.
show running-config	Displays the contents of the currently running configuration file.
show ip arp	Displays all Address Resolution Protocol (ARP) table entries in cache.
debug arp	Displays information about ARP transactions.
show ip interface [**brief**]	Displays a summary of the status of an IP interface.

Note Use packet debugging with extreme caution; otherwise, you might cause the router to lock up and stop routing traffic. As a general rule, do not use packet debugging on a production router unless you have physical access to the router and are willing to risk it going down.



Cisco Commands to Isolate Routing Table Problems

```
router>
show ip route
```

- Displays the current state of the routing table.

```
router>
show ip protocols
```

- Displays the current state of active routing protocols.

```
router#
debug ip routing
```

- Displays information on routing table updates and route-cache updates.

CIT 5.1—4-8

The Cisco commands listed in the table display information about routing tables. A troubleshooter uses the information from these commands to isolate problems related to routing tables at the network layer.

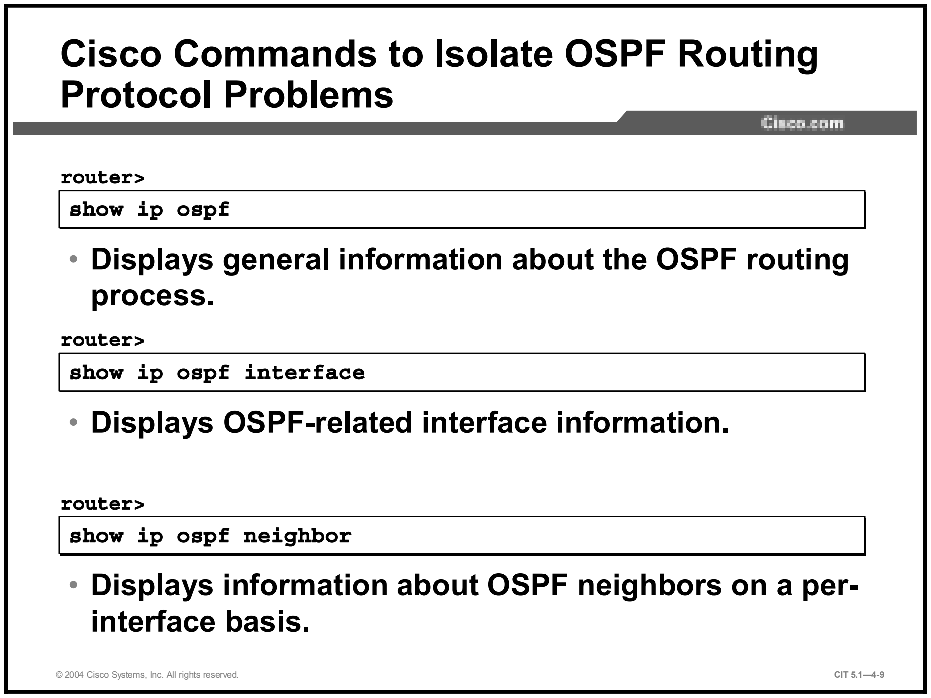
Note Troubleshooters can use the **clear** and **show** commands in combination to view the most current data about a device.

Cisco Commands to Isolate Routing Table Problems

Command	Description
`show ip route`	Displays the current state of the routing table.
`show ip protocols`	Displays the current state of the active routing protocols.
`debug ip routing`	Displays information on routing table updates and route-cache updates.

Note When debugging, have a vty window separate from the console window open in which an appropriate command (for instance, **no debug all**) is pretyped and only requires a quick hit of the Enter key. This can sometimes allow you to escape quickly from a debugging session that is providing overwhelming output.

Multiple commands can be used to troubleshoot routing protocols such as Open Shortest Path First (OSPF).



Cisco Commands to Isolate OSPF Routing Protocol Problems

```
router>
show ip ospf
```

- Displays general information about the OSPF routing process.

```
router>
show ip ospf interface
```

- Displays OSPF-related interface information.

```
router>
show ip ospf neighbor
```

- Displays information about OSPF neighbors on a per-interface basis.

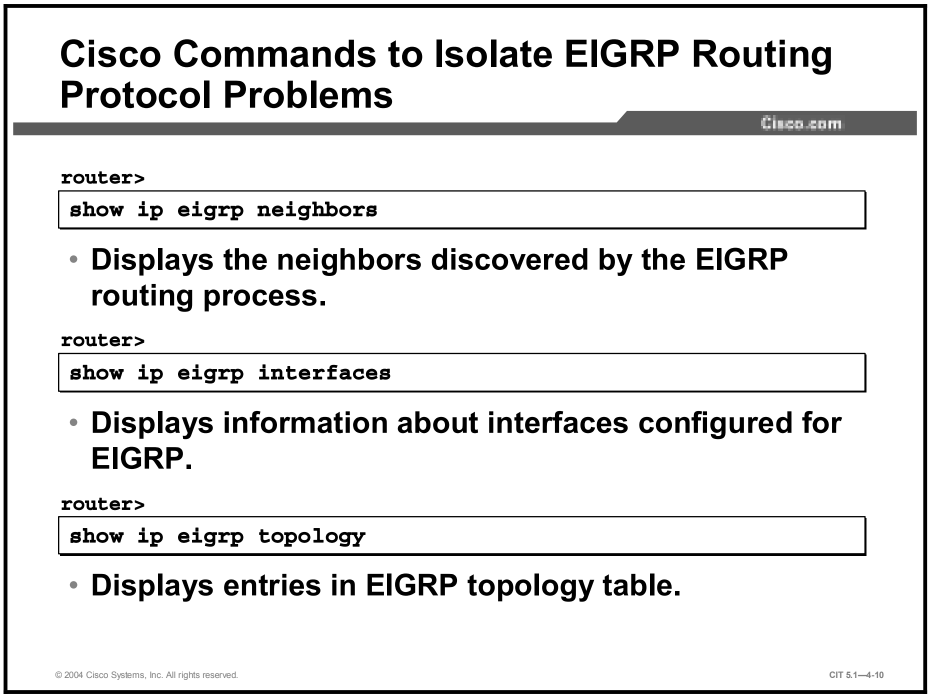
© 2004 Cisco Systems, Inc. All rights reserved. CIT 5.1—4-9

The Cisco commands listed in the table display information about the OSPF routing protocol. A troubleshooter can use information from these and other commands to isolate problems related to the OSPF routing protocol at the network layer.

Cisco Commands to Isolate OSPF Routing Protocol Problems

Command	Description
show ip ospf	Displays general information about the OSPF routing process.
show ip ospf interface	Displays OSPF-related interface information.
show ip ospf neighbor	Displays information about OSPF neighbors on a per-interface basis.

Additional commands can be used to support Enhanced Interior Gateway Routing Protocol (EIGRP).



Cisco Commands to Isolate EIGRP Routing Protocol Problems

```
router>
show ip eigrp neighbors
```

- Displays the neighbors discovered by the EIGRP routing process.

```
router>
show ip eigrp interfaces
```

- Displays information about interfaces configured for EIGRP.

```
router>
show ip eigrp topology
```

- Displays entries in EIGRP topology table.

© 2004 Cisco Systems, Inc. All rights reserved.

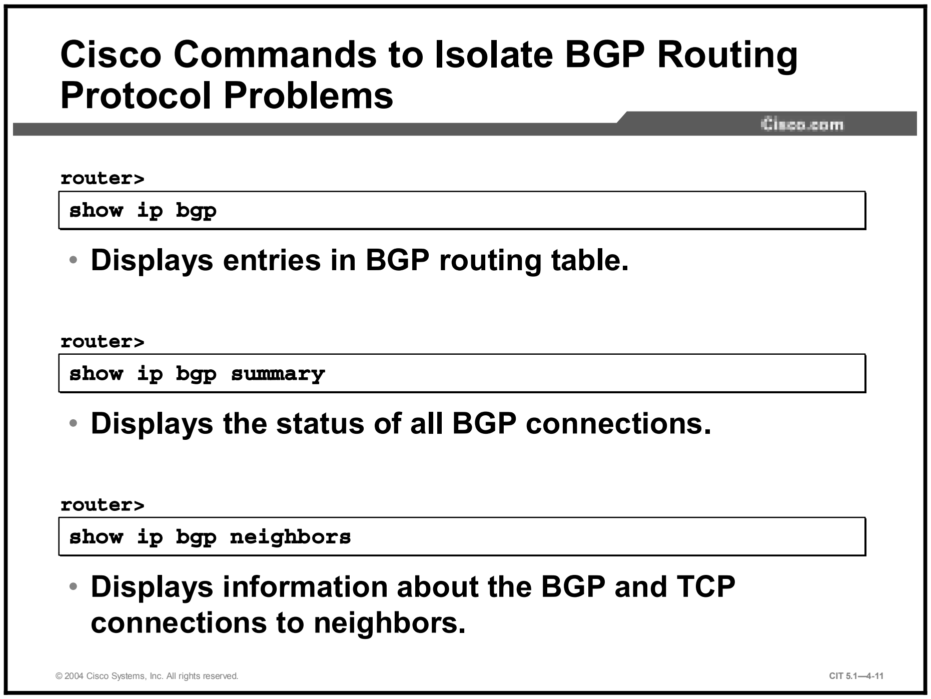
CIT 5.1—4-10

The Cisco commands listed in the table display information about the EIGRP routing protocol. A troubleshooter can use information from these and other commands to isolate problems related to the EIGRP routing protocol at the network layer.

Cisco Commands to Isolate EIGRP Routing Protocol Problems

Command	Description
show ip eigrp neighbors	Displays information about the neighbors discovered by the EIGRP routing process.
show ip eigrp interface	Displays information about interfaces configured for EIGRP.
show ip eigrp topology	Displays entries in the EIGRP topology table.

Multiple commands can be used to manage Border Gateway Protocol (BGP) routing processes.



Cisco Commands to Isolate BGP Routing Protocol Problems

```
router>
show ip bgp
```

- Displays entries in BGP routing table.

```
router>
show ip bgp summary
```

- Displays the status of all BGP connections.

```
router>
show ip bgp neighbors
```

- Displays information about the BGP and TCP connections to neighbors.

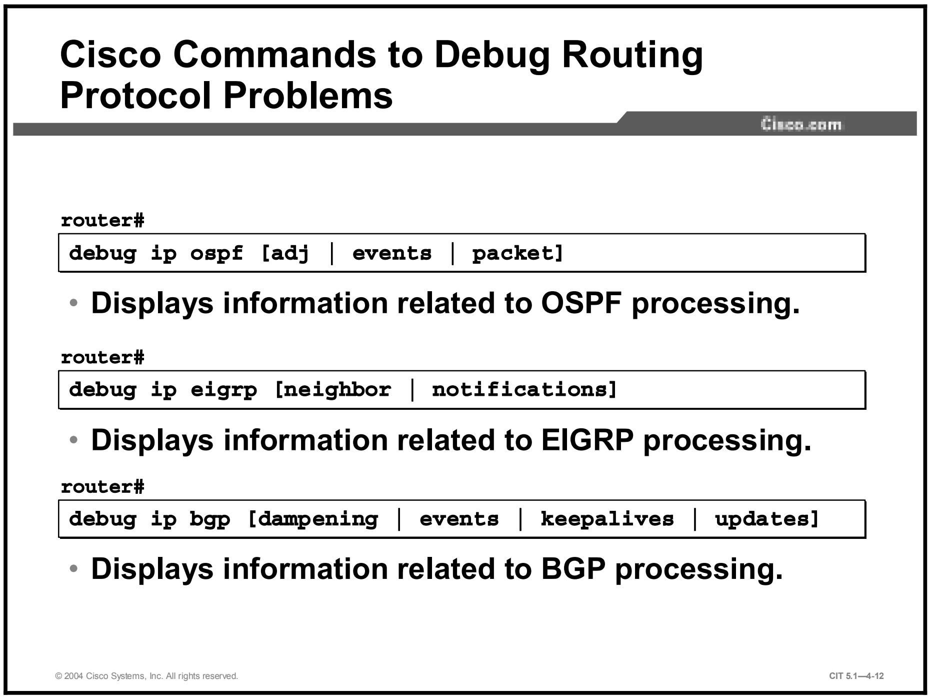
CIT 5.1—4-11

A troubleshooter uses the information from these commands to isolate problems related to the BGP routing protocol at the network layer.

Cisco Commands to Isolate BGP Routing Protocol Problems

Command	Description
`show ip bgp`	Displays entries in BGP routing table.
`show ip bgp summary`	Displays the status of all BGP connections.
`show ip bgp neighbors`	Displays information about the TCP and BGP connections to neighbors.

Debugging commands can be used to isolate problems on routing protocols.



Cisco Commands to Debug Routing Protocol Problems

Cisco.com

```
router#
debug ip ospf [adj | events | packet]
```

- **Displays information related to OSPF processing.**

```
router#
debug ip eigrp [neighbor | notifications]
```

- **Displays information related to EIGRP processing.**

```
router#
debug ip bgp [dampening | events | keepalives | updates]
```

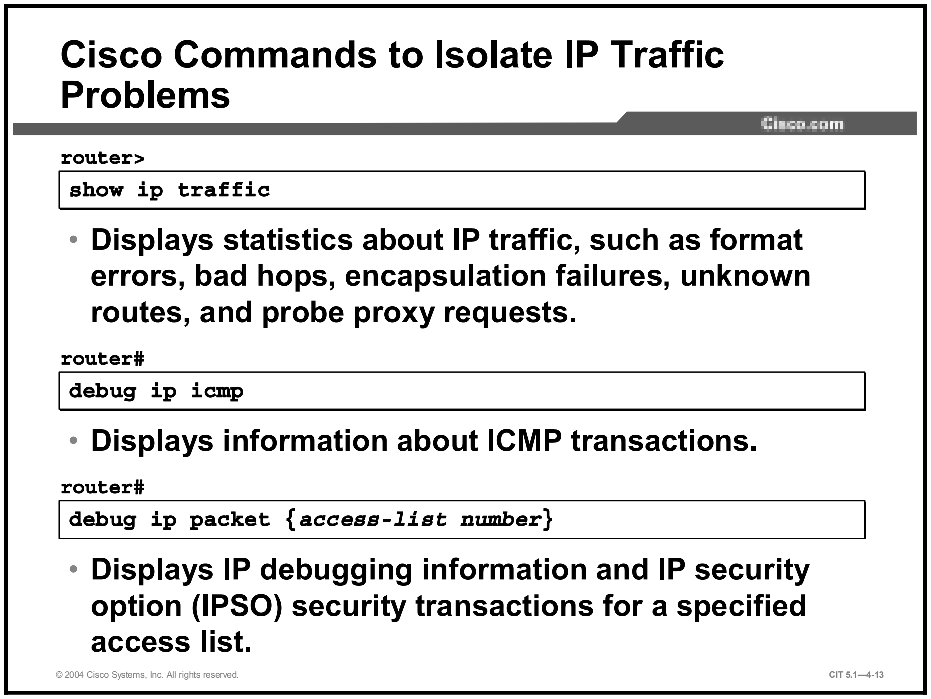
- **Displays information related to BGP processing.**

CIT 5.1—4-12

The debugging commands listed in the table can be used to provide information about routing protocol processes. A troubleshooter can use information from these and other commands to isolate problems related to network layer routing protocols.

Cisco Commands to Debug OSPF and EIGRP Routing Protocol Problems

Command	Description
debug ip ospf [adj | events | packet]	Displays information related to OSPF processing.
debug ip eigrp [neighbor | notifications]	Displays information related to EIGRP processing.
debug ip bgp [dampening | events | keepalives | updates]	Displays information related to BGP processing.



Cisco Commands to Isolate IP Traffic Problems

```
router>
show ip traffic
```

- Displays statistics about IP traffic, such as format errors, bad hops, encapsulation failures, unknown routes, and probe proxy requests.

```
router#
debug ip icmp
```

- Displays information about ICMP transactions.

```
router#
debug ip packet {access-list number}
```

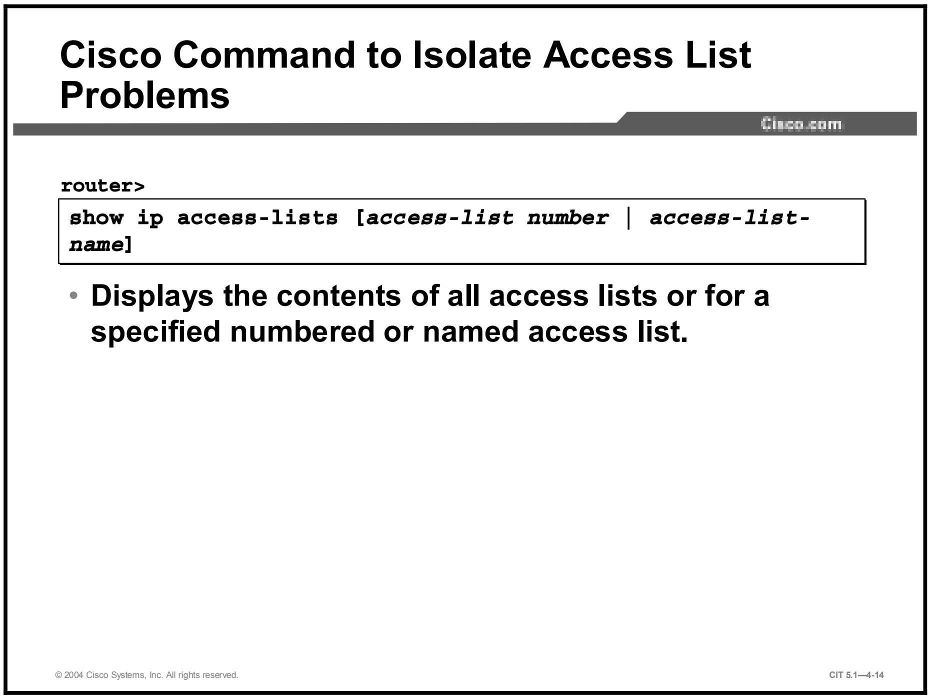
- Displays IP debugging information and IP security option (IPSO) security transactions for a specified access list.

CIT 5.1—4-13

The Cisco commands listed in the table display information about IP traffic. A troubleshooter uses the information from these commands to isolate problems related to IP traffic at the network layer.

Cisco Commands for Gathering Information About IP Traffic

Command	Description
show ip traffic	Displays statistics about IP traffic, such as format errors, bad hops, encapsulation failures, unknown routes, and probe proxy requests.
debug ip icmp	Displays information about ICMP transactions.
debug ip packet {*access-list name*}	Displays IP debugging information and IP security option (IPSO) security transactions for a specified access list.



Cisco Command to Isolate Access List Problems

```
router>
show ip access-lists [access-list number | access-list-
name]
```

- **Displays the contents of all access lists or for a specified numbered or named access list.**

CIT 5.1—4-14

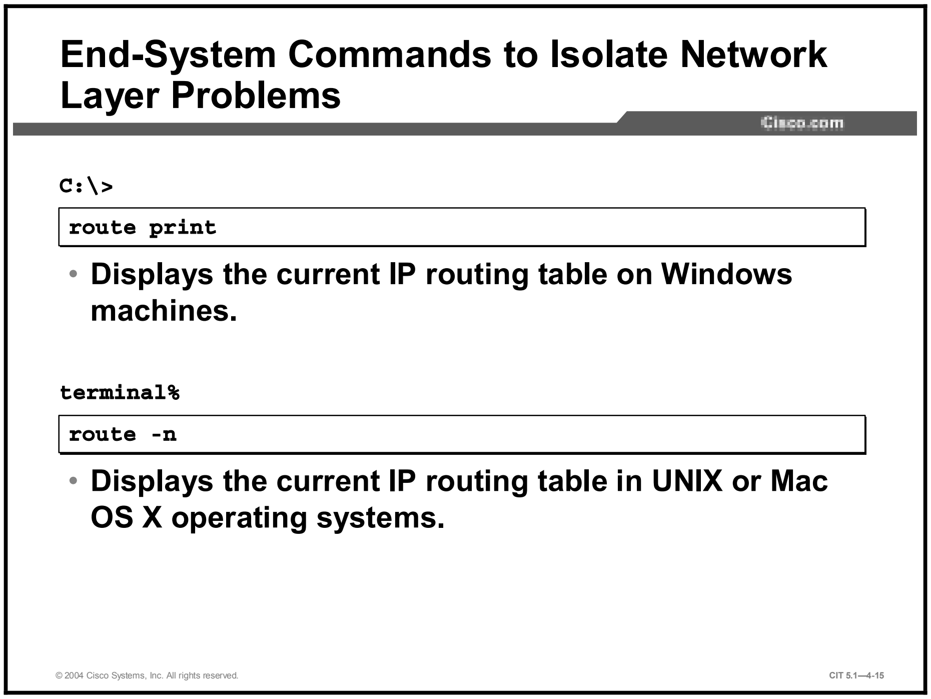
The command listed in the table is the Cisco command that displays information about access control lists (ACLs). A troubleshooter uses the information from this command to isolate problems related to ACLs at the network layer.

Cisco Command for Isolating Access Control List Problems

Command	Description
show ip access-lists [*access-list-number* | *access-list-name*]	Displays the contents of all access lists or for a specified numbered or named access list.

Identifying End-System Commands and Applications Used to Isolate Problems Occurring at the Network Layer

This topic identifies commands and applications that a troubleshooter enters at the end system to isolate problems occurring at the network layer.



End-System Commands to Isolate Network Layer Problems

```
C:\>
route print
```

- **Displays the current IP routing table on Windows machines.**

```
terminal%
route -n
```

- **Displays the current IP routing table in UNIX or Mac OS X operating systems.**

CIT 5.1—4-15

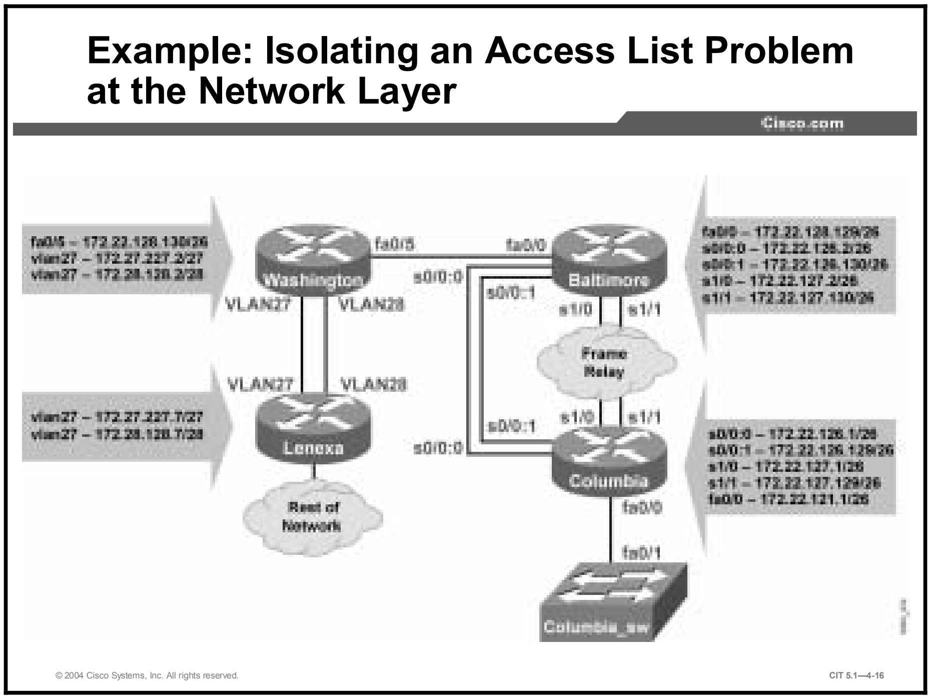
The table shows commands that a troubleshooter may use to isolate problems at the network layer. Although many of the commands also display information that concerns the data link layer, these commands are noteworthy at the network layer because they highlight problems in the interface between the data link and network layers.

End-System Commands to Isolate Network Layer Problems

Command	Description
ping *{host* | *ip-address}*	Sends an echo request packet to an address, then waits for a reply. The *host* | *ip-address* variable is the IP alias or IP address of the target system.
arp –a	Displays the current mappings of the IP address to the MAC address in the ARP table.
netstat -rn	Displays the status of all connected devices and links without querying a Domain Name System (DNS) server on Windows hosts.
ipconfig [**/all**]	Displays IP information for hosts running Windows NT, 2000, or XP.
tracert [**-d**] [*destination*]	Identifies a path to a destination device for Windows hosts without querying a DNS server. The *destination* variable is the IP alias or IP address of the target system.
route print	Displays the current IP routing table fro Windows hosts.
winipcfg	Displays IP information for hosts running Windows 9x and Me.
ifconfig –a	Displays IP information for UNIX and Mac OS X hosts.
traceroute -d [*destination*]	Identifies the path a packet takes through the network without querying a DNS server for Mac OS X or UNIX hosts. The *destination* variable is the host name or IP address of the target system.
route -n	Displays the current IP routing table for Mac OS X or UNIX hosts.

Example: Isolating an Access List Problem at the Network Layer

You are the second-level network engineer for a division with locations in Washington, Baltimore, and Columbia. The networking devices at each location are named after the names of the city in which they reside. You have console access to the router named Washington, which gives you IP connectivity to all devices in your network. Your span of responsibility in the corporate network includes the 172.22.0.0/16 network.



Example: Isolating an Access List Problem at the Network Layer

fa0/5 – 172.22.128.130/26
vlan27 – 172.27.227.2/27
vlan27 – 172.28.128.2/28

fa0/0 – 172.22.128.129/26
s0/0:0 – 172.22.126.2/26
s0/0:1 – 172.22.126.130/26
s1/0 – 172.22.127.2/26
s1/1 – 172.22.127.130/26

vlan27 – 172.27.227.7/27
vlan27 – 172.28.128.7/28

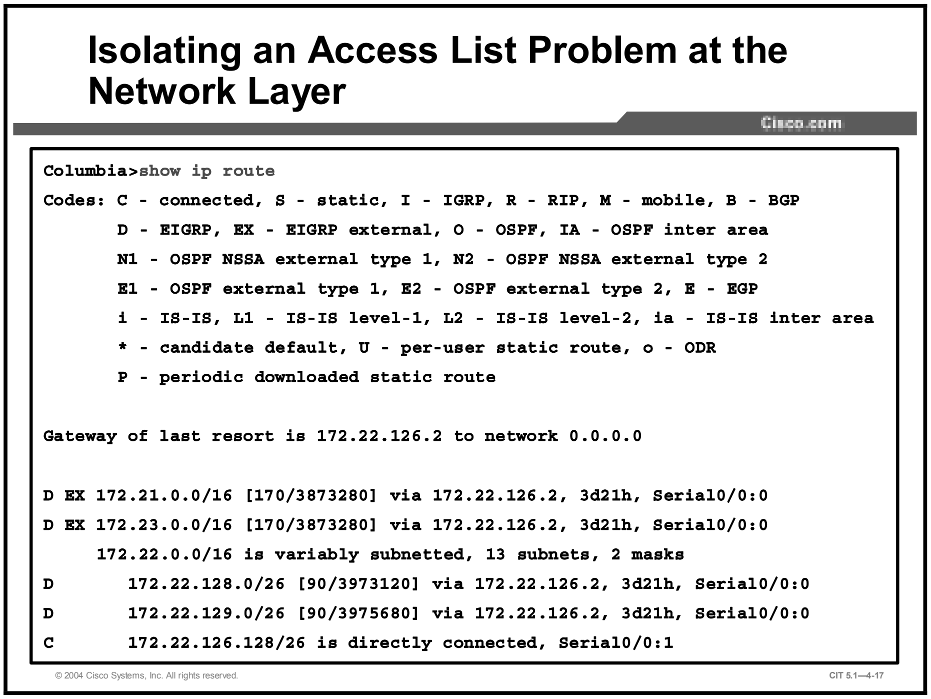
s0/0:0 – 172.22.126.1/26
s0/0:1 – 172.22.126.129/26
s1/0 – 172.22.127.1/26
s1/1 – 172.22.127.129/26
fa0/0 – 172.22.121.1/26

© 2004 Cisco Systems, Inc. All rights reserved.

CIT 5.1—4-16

One day, a new IT manager is transferred from a division that supports Daytona to the Columbia offices. The new manager calls you to mention that a route to Cisco Systems cannot be seen in the network table on Columbia. This manager used to be able to see the route in the network table on Daytona. Apparently, connectivity to Cisco Systems still exists.

You check your base configuration files. Although the route is not needed for connectivity, management policy dictates that the route 198.133.219.0/24 for Cisco Systems is supposed to be in the routing tables for all devices. You check the routing table on Columbia and confirm that the route is not on the access router.

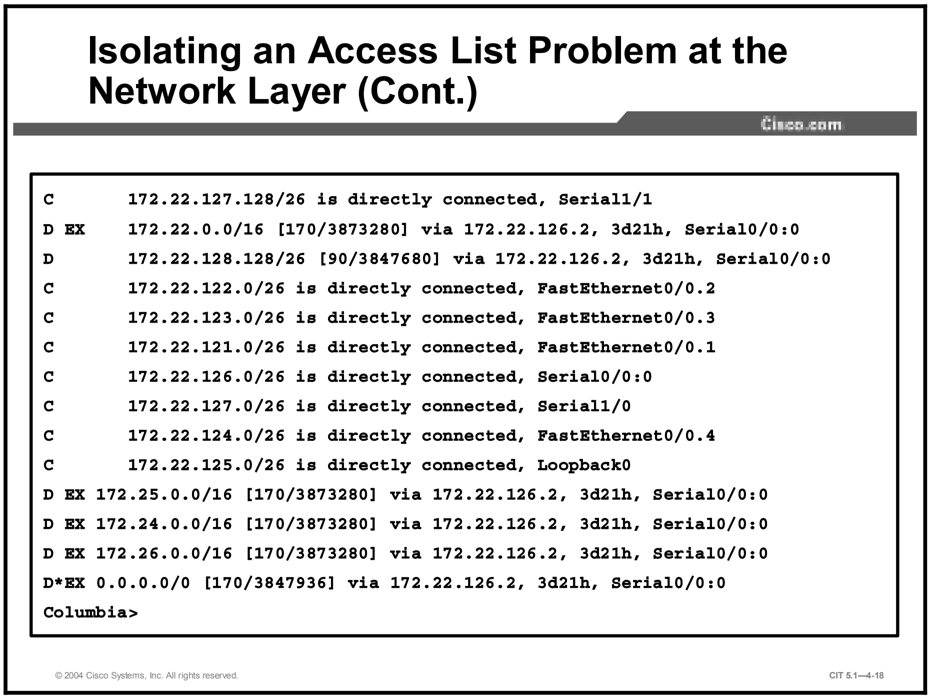


Isolating an Access List Problem at the Network Layer

```
Columbia>show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 172.22.126.2 to network 0.0.0.0

D EX 172.21.0.0/16 [170/3873280] via 172.22.126.2, 3d21h, Serial0/0:0
D EX 172.23.0.0/16 [170/3873280] via 172.22.126.2, 3d21h, Serial0/0:0
     172.22.0.0/16 is variably subnetted, 13 subnets, 2 masks
D       172.22.128.0/26 [90/3973120] via 172.22.126.2, 3d21h, Serial0/0:0
D       172.22.129.0/26 [90/3975680] via 172.22.126.2, 3d21h, Serial0/0:0
C       172.22.126.128/26 is directly connected, Serial0/0:1
```

© 2004 Cisco Systems, Inc. All rights reserved.

CIT 5.1—4-17



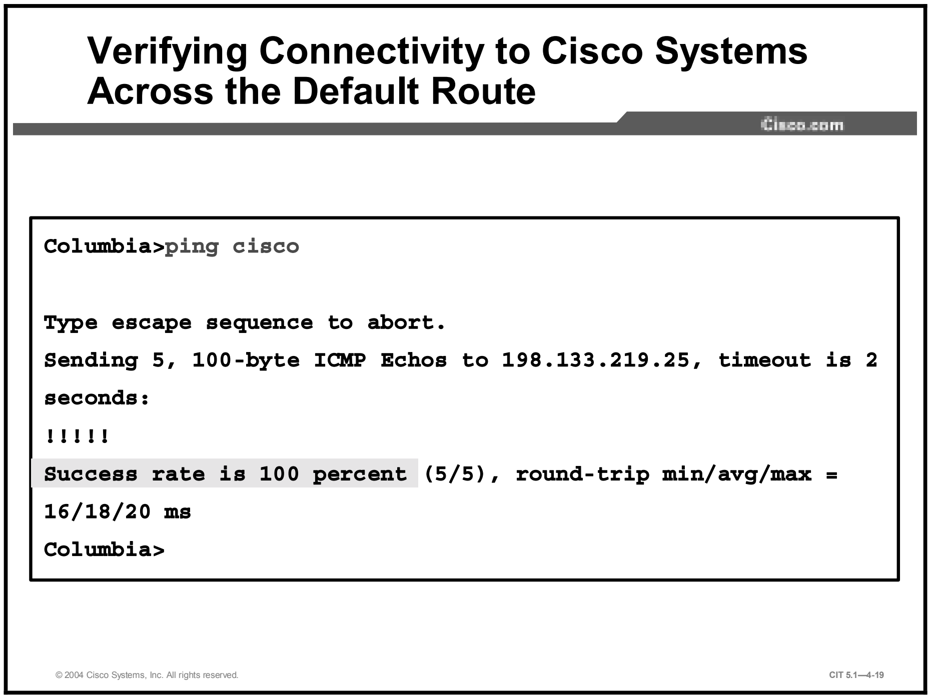
Isolating an Access List Problem at the Network Layer (Cont.)

```
C       172.22.127.128/26 is directly connected, Serial1/1
D EX    172.22.0.0/16 [170/3873280] via 172.22.126.2, 3d21h, Serial0/0:0
D       172.22.128.128/26 [90/3847680] via 172.22.126.2, 3d21h, Serial0/0:0
C       172.22.122.0/26 is directly connected, FastEthernet0/0.2
C       172.22.123.0/26 is directly connected, FastEthernet0/0.3
C       172.22.121.0/26 is directly connected, FastEthernet0/0.1
C       172.22.126.0/26 is directly connected, Serial0/0:0
C       172.22.127.0/26 is directly connected, Serial1/0
C       172.22.124.0/26 is directly connected, FastEthernet0/0.4
C       172.22.125.0/26 is directly connected, Loopback0
D EX 172.25.0.0/16 [170/3873280] via 172.22.126.2, 3d21h, Serial0/0:0
D EX 172.24.0.0/16 [170/3873280] via 172.22.126.2, 3d21h, Serial0/0:0
D EX 172.26.0.0/16 [170/3873280] via 172.22.126.2, 3d21h, Serial0/0:0
D*EX 0.0.0.0/0 [170/3847936] via 172.22.126.2, 3d21h, Serial0/0:0
Columbia>
```

© 2004 Cisco Systems, Inc. All rights reserved.

CIT 5.1—4-18

Not seeing the route, you ping Cisco Systems across the default route to verify connectivity.



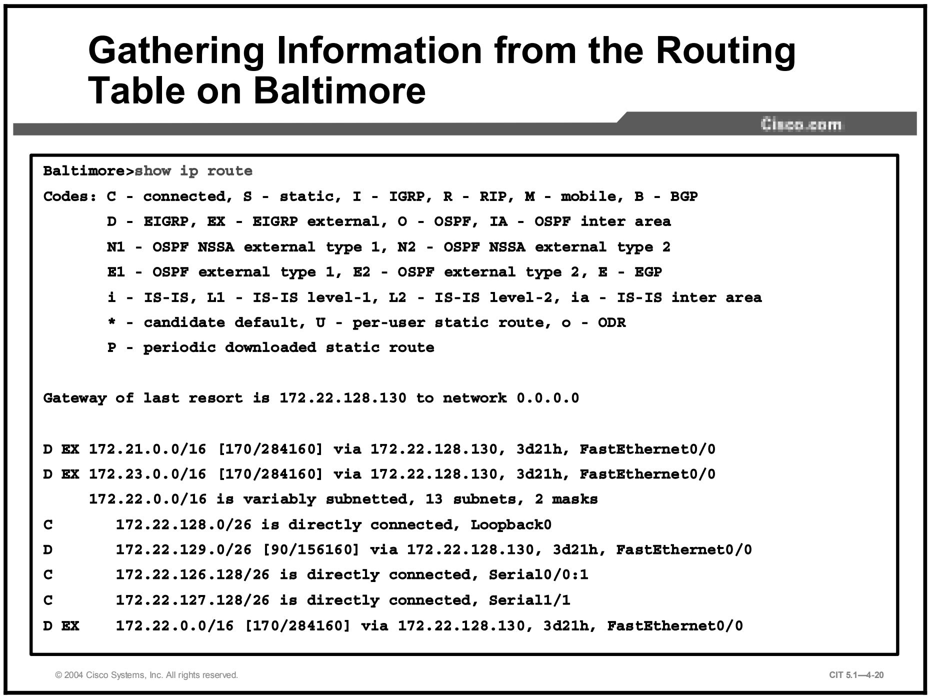
Verifying Connectivity to Cisco Systems Across the Default Route

```
Columbia>ping cisco

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 198.133.219.25, timeout is 2
seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
16/18/20 ms
Columbia>
```

CIT 5.1—4-19

The ping is successful.

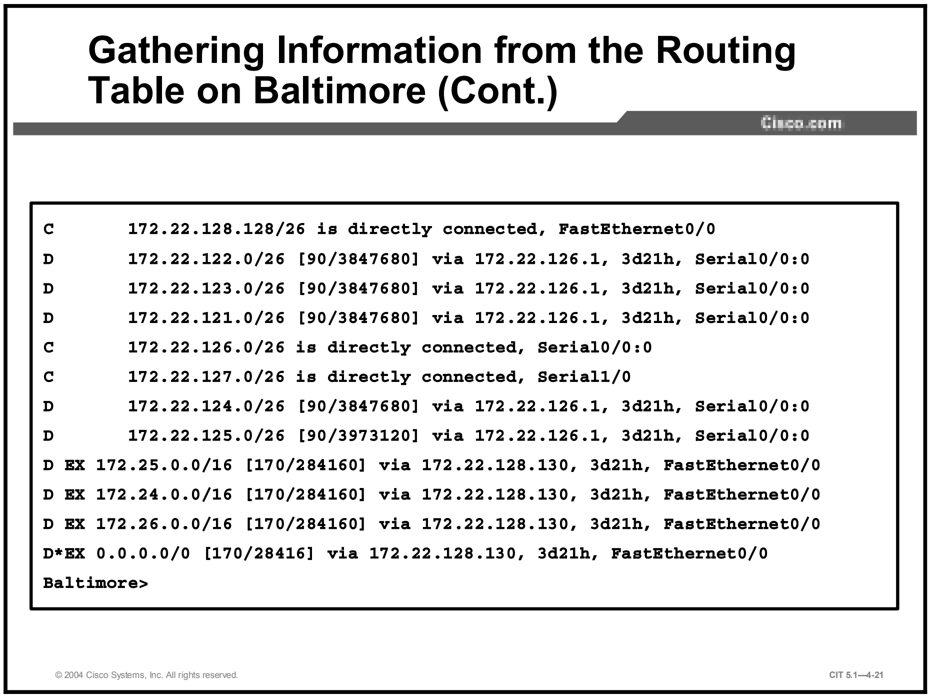
You check the routing table on Baltimore and confirm that the route is not on the distribution router.



Gathering Information from the Routing Table on Baltimore

```
Baltimore>show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 172.22.128.130 to network 0.0.0.0

D EX 172.21.0.0/16 [170/284160] via 172.22.128.130, 3d21h, FastEthernet0/0
D EX 172.23.0.0/16 [170/284160] via 172.22.128.130, 3d21h, FastEthernet0/0
     172.22.0.0/16 is variably subnetted, 13 subnets, 2 masks
C       172.22.128.0/26 is directly connected, Loopback0
D       172.22.129.0/26 [90/156160] via 172.22.128.130, 3d21h, FastEthernet0/0
C       172.22.126.128/26 is directly connected, Serial0/0:1
C       172.22.127.128/26 is directly connected, Serial1/1
D EX    172.22.0.0/16 [170/284160] via 172.22.128.130, 3d21h, FastEthernet0/0
```

© 2004 Cisco Systems, Inc. All rights reserved. CIT 5.1—4-20

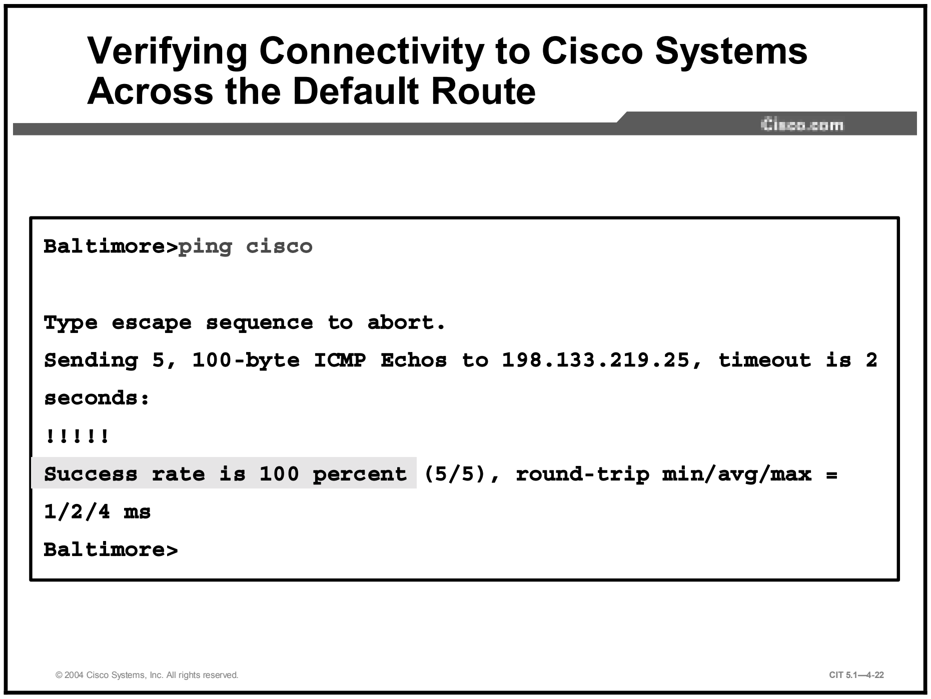


Gathering Information from the Routing Table on Baltimore (Cont.)

```
C       172.22.128.128/26 is directly connected, FastEthernet0/0
D       172.22.122.0/26 [90/3847680] via 172.22.126.1, 3d21h, Serial0/0:0
D       172.22.123.0/26 [90/3847680] via 172.22.126.1, 3d21h, Serial0/0:0
D       172.22.121.0/26 [90/3847680] via 172.22.126.1, 3d21h, Serial0/0:0
C       172.22.126.0/26 is directly connected, Serial0/0:0
C       172.22.127.0/26 is directly connected, Serial1/0
D       172.22.124.0/26 [90/3847680] via 172.22.126.1, 3d21h, Serial0/0:0
D       172.22.125.0/26 [90/3973120] via 172.22.126.1, 3d21h, Serial0/0:0
D EX 172.25.0.0/16 [170/284160] via 172.22.128.130, 3d21h, FastEthernet0/0
D EX 172.24.0.0/16 [170/284160] via 172.22.128.130, 3d21h, FastEthernet0/0
D EX 172.26.0.0/16 [170/284160] via 172.22.128.130, 3d21h, FastEthernet0/0
D*EX 0.0.0.0/0 [170/28416] via 172.22.128.130, 3d21h, FastEthernet0/0
Baltimore>
```

© 2004 Cisco Systems, Inc. All rights reserved. CIT 5.1—4-21

Again, you verify that you are able to use the default route on Baltimore to ping Cisco Systems.

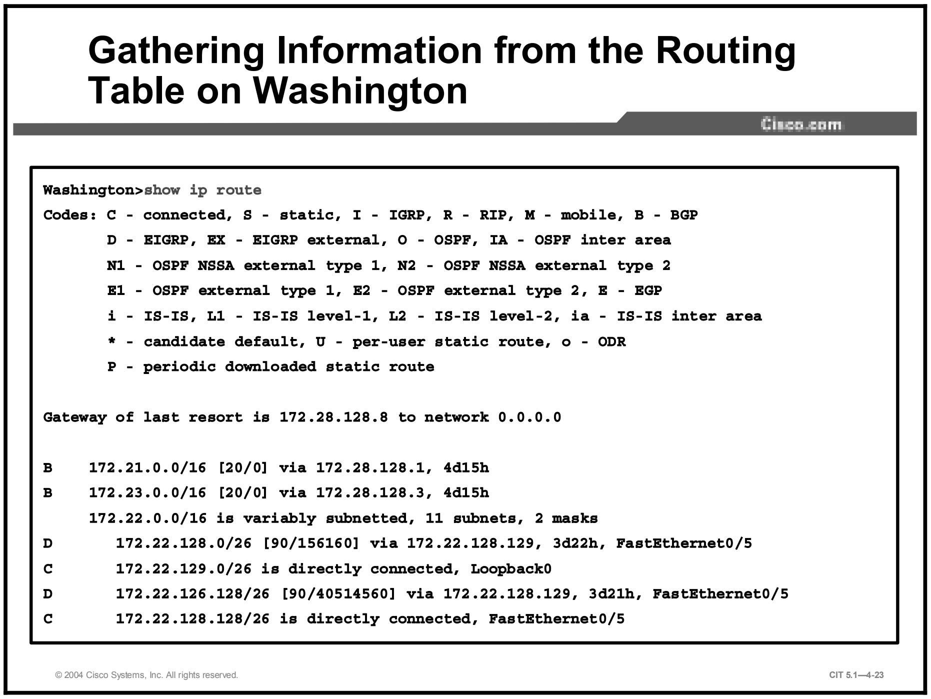


Verifying Connectivity to Cisco Systems Across the Default Route

```
Baltimore>ping cisco

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 198.133.219.25, timeout is 2
seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
1/2/4 ms
Baltimore>
```

CIT 5.1—4-22

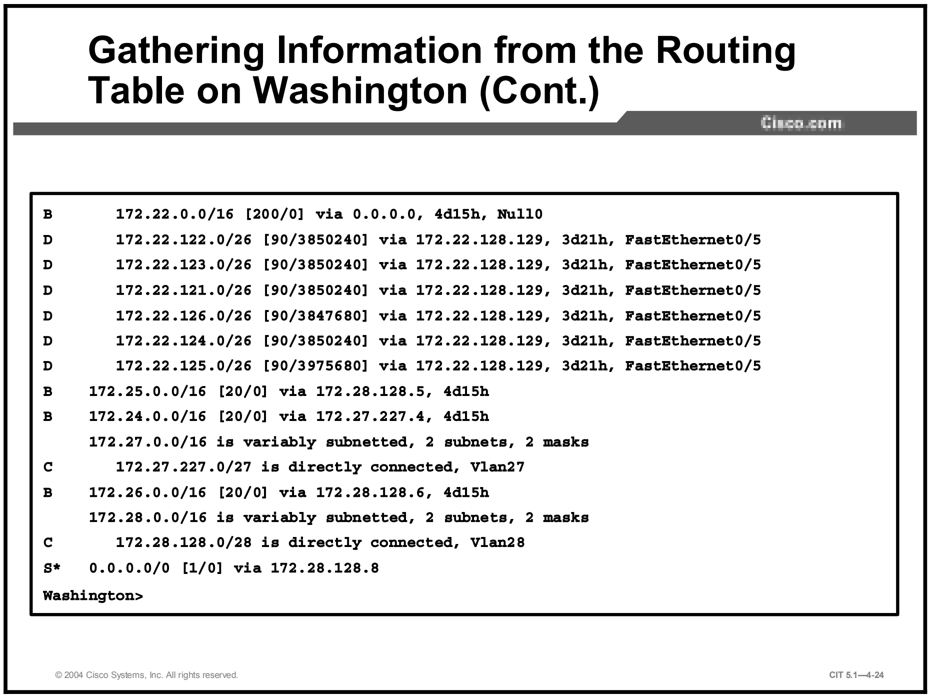
Finally, you check the routing table on Washington and confirm that the 198.133.219.0/24 route is not on the core router.



Gathering Information from the Routing Table on Washington

```
Washington>show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 172.28.128.8 to network 0.0.0.0

B    172.21.0.0/16 [20/0] via 172.28.128.1, 4d15h
B    172.23.0.0/16 [20/0] via 172.28.128.3, 4d15h
     172.22.0.0/16 is variably subnetted, 11 subnets, 2 masks
D       172.22.128.0/26 [90/156160] via 172.22.128.129, 3d22h, FastEthernet0/5
C       172.22.129.0/26 is directly connected, Loopback0
D       172.22.126.128/26 [90/40514560] via 172.22.128.129, 3d21h, FastEthernet0/5
C       172.22.128.128/26 is directly connected, FastEthernet0/5
```

© 2004 Cisco Systems, Inc. All rights reserved. CIT 5.1—4-23

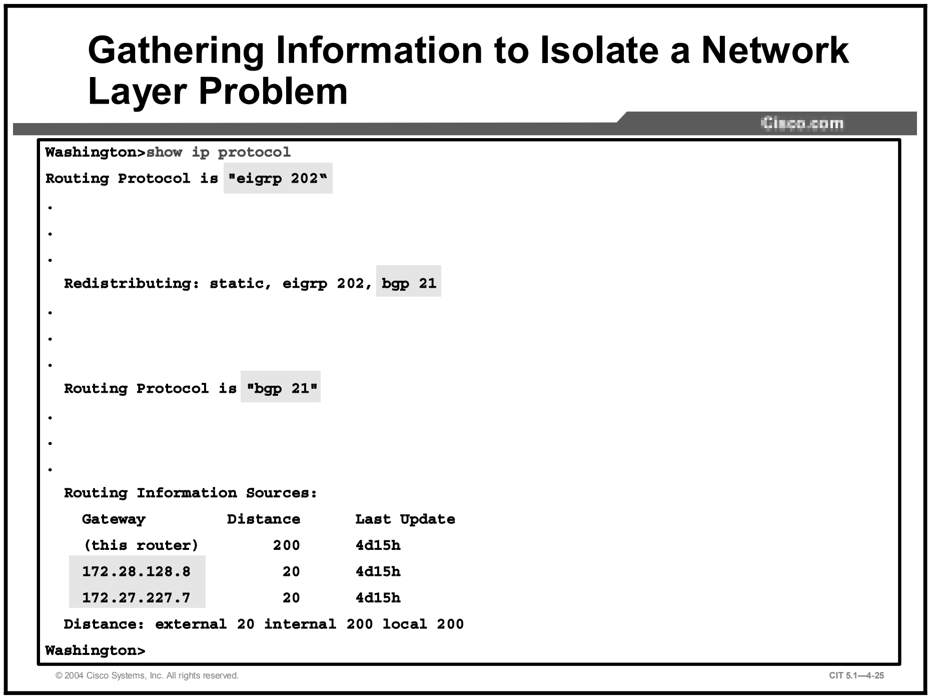


Gathering Information from the Routing Table on Washington (Cont.)

```
B       172.22.0.0/16 [200/0] via 0.0.0.0, 4d15h, Null0
D       172.22.122.0/26 [90/3850240] via 172.22.128.129, 3d21h, FastEthernet0/5
D       172.22.123.0/26 [90/3850240] via 172.22.128.129, 3d21h, FastEthernet0/5
D       172.22.121.0/26 [90/3850240] via 172.22.128.129, 3d21h, FastEthernet0/5
D       172.22.126.0/26 [90/3847680] via 172.22.128.129, 3d21h, FastEthernet0/5
D       172.22.124.0/26 [90/3850240] via 172.22.128.129, 3d21h, FastEthernet0/5
D       172.22.125.0/26 [90/3975680] via 172.22.128.129, 3d21h, FastEthernet0/5
B    172.25.0.0/16 [20/0] via 172.28.128.5, 4d15h
B    172.24.0.0/16 [20/0] via 172.27.227.4, 4d15h
     172.27.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       172.27.227.0/27 is directly connected, Vlan27
B    172.26.0.0/16 [20/0] via 172.28.128.6, 4d15h
     172.28.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       172.28.128.0/28 is directly connected, Vlan28
S*   0.0.0.0/0 [1/0] via 172.28.128.8
Washington>
```

© 2004 Cisco Systems, Inc. All rights reserved. CIT 5.1—4-24

You have determined that the route 198.133.219.0/24 for Cisco Systems, which is supposed to be in the routing table for all devices, is not in the routing tables for any of the devices that you manage. To help isolate the problem, you review the status of the current routing protocols on Washington.



Gathering Information to Isolate a Network Layer Problem

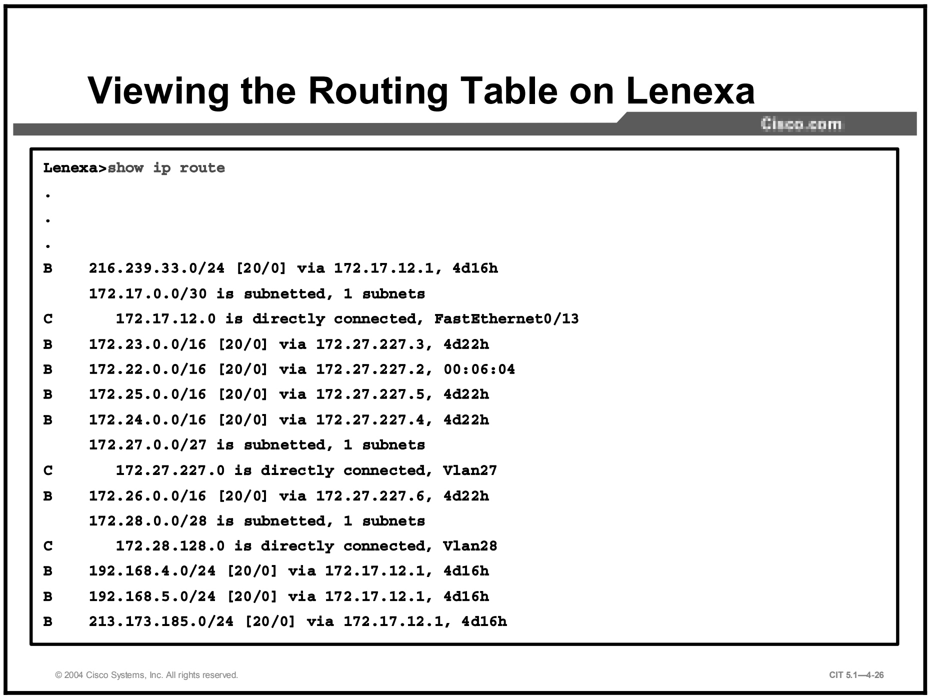
```
Washington>show ip protocol
Routing Protocol is "eigrp 202"
.
.
.
  Redistributing: static, eigrp 202, bgp 21
.
.
.
  Routing Protocol is "bgp 21"
.
.
.
  Routing Information Sources:
    Gateway         Distance      Last Update
    (this router)        200      4d15h
    172.28.128.8          20      4d15h
    172.27.227.7          20      4d15h
  Distance: external 20 internal 200 local 200
Washington>
```

© 2004 Cisco Systems, Inc. All rights reserved.

CIT 5.1—4-25

You see that Enhanced Interior Gateway Routing Protocol (EIGRP) 202 is running and is redistributing BGP 21. You also see that BGP 21 is running and has neighbor relationships with 172.27.227.7 and 172.28.128.8.

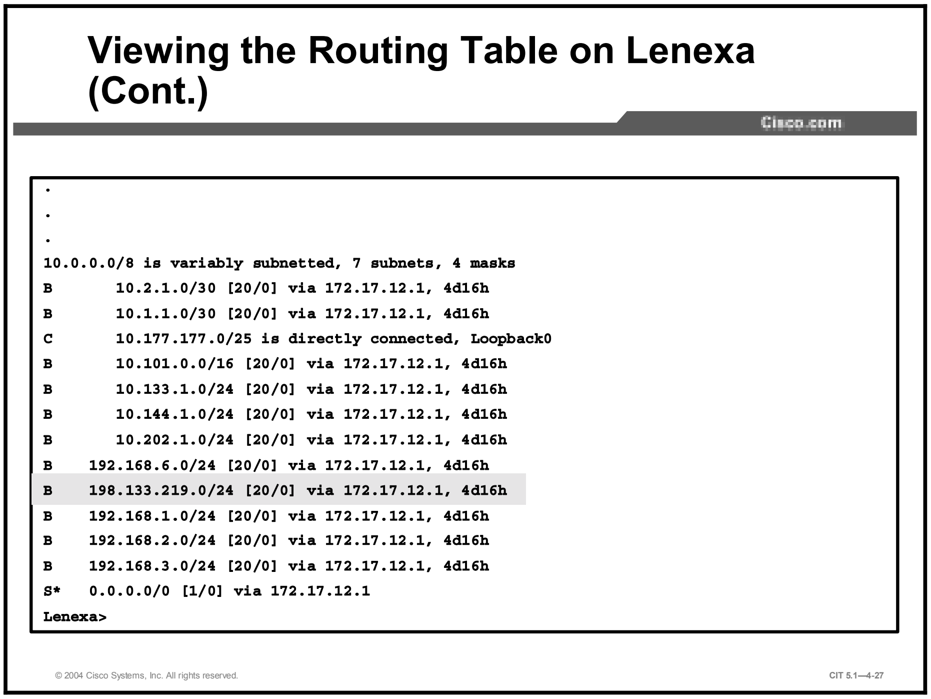
You connect to Lenexa, a corporate core device, at 172.27.227.7 and check for the presence of the 198.133.219.0/24 route. Again, you use the **show ip route** command to look at the current routing table.



Viewing the Routing Table on Lenexa

```
Lenexa>show ip route
.
.
.
B    216.239.33.0/24 [20/0] via 172.17.12.1, 4d16h
     172.17.0.0/30 is subnetted, 1 subnets
C       172.17.12.0 is directly connected, FastEthernet0/13
B    172.23.0.0/16 [20/0] via 172.27.227.3, 4d22h
B    172.22.0.0/16 [20/0] via 172.27.227.2, 00:06:04
B    172.25.0.0/16 [20/0] via 172.27.227.5, 4d22h
B    172.24.0.0/16 [20/0] via 172.27.227.4, 4d22h
     172.27.0.0/27 is subnetted, 1 subnets
C       172.27.227.0 is directly connected, Vlan27
B    172.26.0.0/16 [20/0] via 172.27.227.6, 4d22h
     172.28.0.0/28 is subnetted, 1 subnets
C       172.28.128.0 is directly connected, Vlan28
B    192.168.4.0/24 [20/0] via 172.17.12.1, 4d16h
B    192.168.5.0/24 [20/0] via 172.17.12.1, 4d16h
B    213.173.185.0/24 [20/0] via 172.17.12.1, 4d16h
```

© 2004 Cisco Systems, Inc. All rights reserved. CIT 5.1—4-26



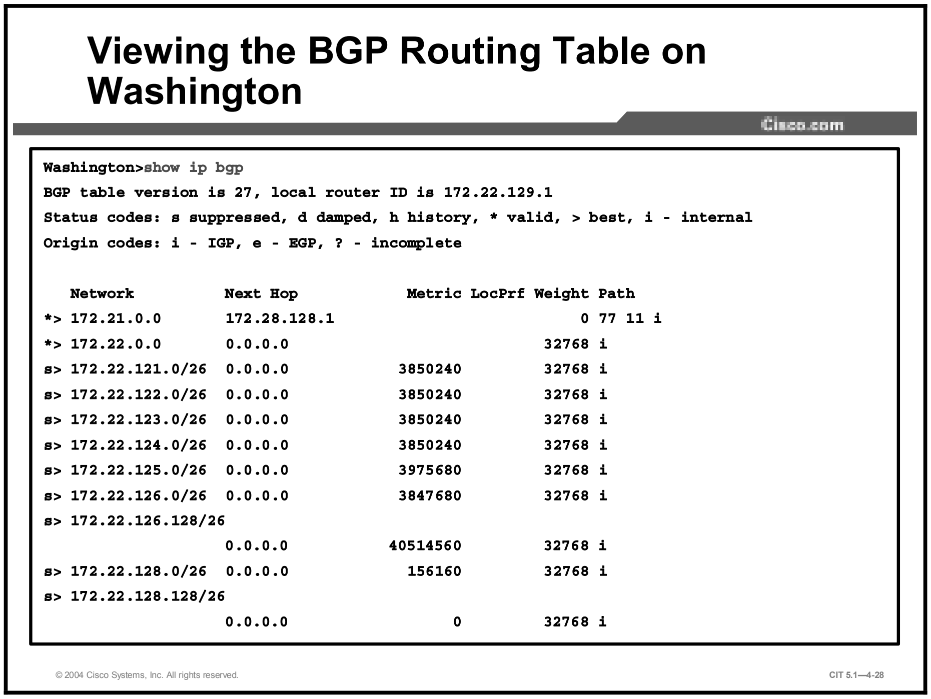
Viewing the Routing Table on Lenexa (Cont.)

```
.
.
.
10.0.0.0/8 is variably subnetted, 7 subnets, 4 masks
B       10.2.1.0/30 [20/0] via 172.17.12.1, 4d16h
B       10.1.1.0/30 [20/0] via 172.17.12.1, 4d16h
C       10.177.177.0/25 is directly connected, Loopback0
B       10.101.0.0/16 [20/0] via 172.17.12.1, 4d16h
B       10.133.1.0/24 [20/0] via 172.17.12.1, 4d16h
B       10.144.1.0/24 [20/0] via 172.17.12.1, 4d16h
B       10.202.1.0/24 [20/0] via 172.17.12.1, 4d16h
B    192.168.6.0/24 [20/0] via 172.17.12.1, 4d16h
B    198.133.219.0/24 [20/0] via 172.17.12.1, 4d16h
B    192.168.1.0/24 [20/0] via 172.17.12.1, 4d16h
B    192.168.2.0/24 [20/0] via 172.17.12.1, 4d16h
B    192.168.3.0/24 [20/0] via 172.17.12.1, 4d16h
S*   0.0.0.0/0 [1/0] via 172.17.12.1
Lenexa>
```

© 2004 Cisco Systems, Inc. All rights reserved. CIT 5.1—4-27

You have verified that the 198.133.219.0/24 route is on at least one of the corporate core devices.

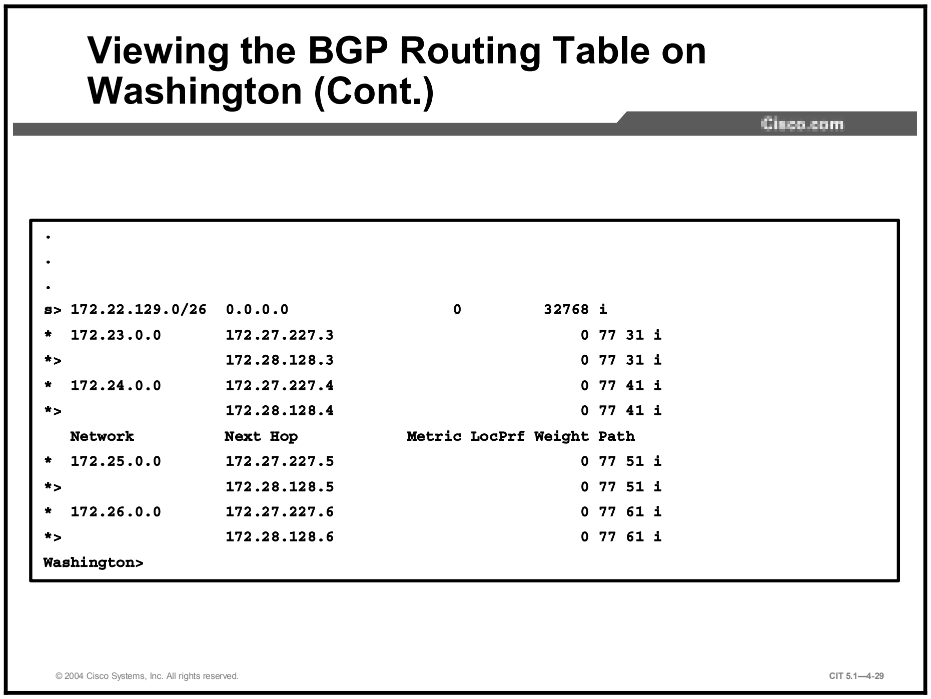
You now return to the console on Washington and examine the BGP routing table.



Viewing the BGP Routing Table on Washington

```
Washington>show ip bgp
BGP table version is 27, local router ID is 172.22.129.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 172.21.0.0       172.28.128.1                           0 77 11 i
*> 172.22.0.0       0.0.0.0                            32768 i
s> 172.22.121.0/26  0.0.0.0            3850240         32768 i
s> 172.22.122.0/26  0.0.0.0            3850240         32768 i
s> 172.22.123.0/26  0.0.0.0            3850240         32768 i
s> 172.22.124.0/26  0.0.0.0            3850240         32768 i
s> 172.22.125.0/26  0.0.0.0            3975680         32768 i
s> 172.22.126.0/26  0.0.0.0            3847680         32768 i
s> 172.22.126.128/26
                    0.0.0.0           40514560         32768 i
s> 172.22.128.0/26  0.0.0.0             156160         32768 i
s> 172.22.128.128/26
                    0.0.0.0                  0         32768 i
```

CIT 5.1—4-28



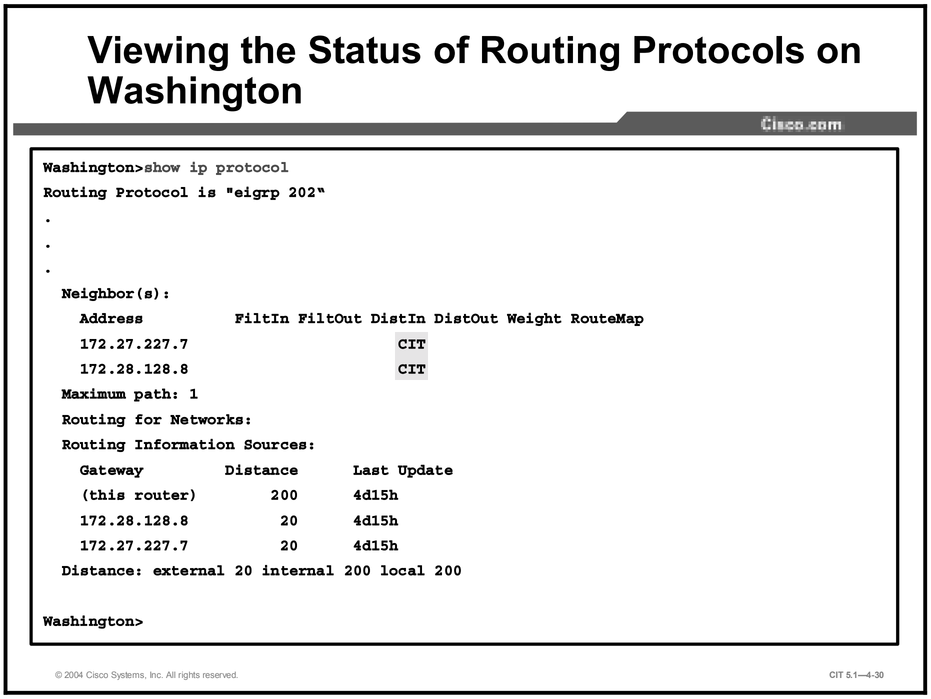
Viewing the BGP Routing Table on Washington (Cont.)

```
.
.
.
s> 172.22.129.0/26  0.0.0.0                  0         32768 i
*  172.23.0.0       172.27.227.3                           0 77 31 i
*>                  172.28.128.3                           0 77 31 i
*  172.24.0.0       172.27.227.4                           0 77 41 i
*>                  172.28.128.4                           0 77 41 i
   Network          Next Hop            Metric LocPrf Weight Path
*  172.25.0.0       172.27.227.5                           0 77 51 i
*>                  172.28.128.5                           0 77 51 i
*  172.26.0.0       172.27.227.6                           0 77 61 i
*>                  172.28.128.6                           0 77 61 i
Washington>
```

CIT 5.1—4-29

You determine that the 198.133.219.0/24 route is not in the BGP table on Washington.

For further problem isolation, you again review the status of the routing protocols on Washington.



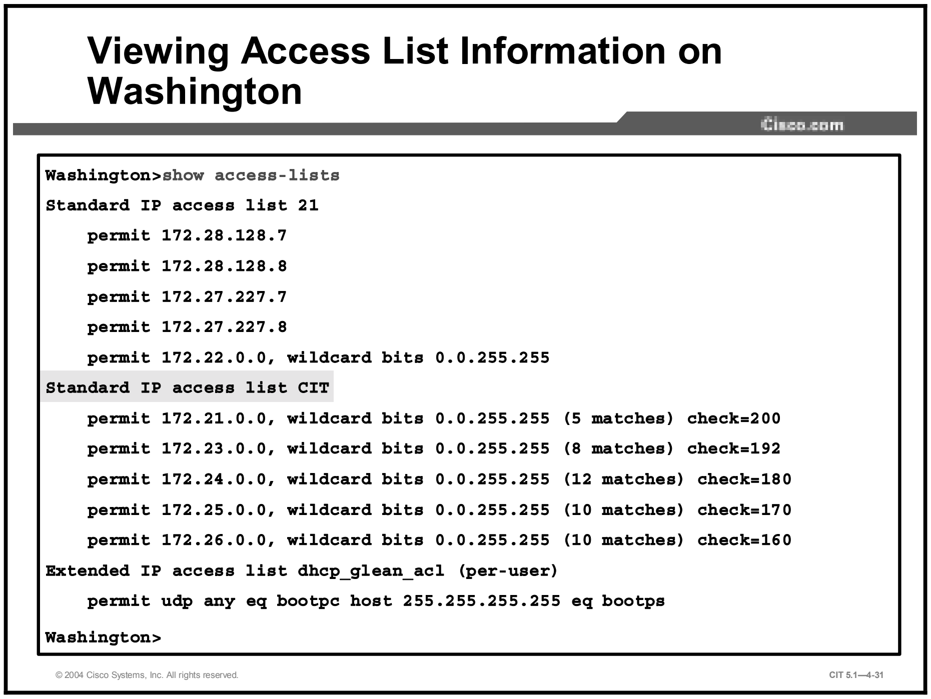
Viewing the Status of Routing Protocols on Washington

```
Washington>show ip protocol
Routing Protocol is "eigrp 202"
.
.
.
  Neighbor(s):
    Address          FiltIn FiltOut DistIn DistOut Weight RouteMap
    172.27.227.7                       CIT
    172.28.128.8                       CIT
  Maximum path: 1
  Routing for Networks:
  Routing Information Sources:
    Gateway         Distance      Last Update
    (this router)        200      4d15h
    172.28.128.8          20      4d15h
    172.27.227.7          20      4d15h
  Distance: external 20 internal 200 local 200

Washington>
```

© 2004 Cisco Systems, Inc. All rights reserved. CIT 5.1—4-30

You notice that a distribution list named CIT is applied to inbound routes from the BGP neighbors. You realize that you probably should have been more observant and noticed the distribution list earlier. In this case, BGP is using the distribution list named CIT to choose what routes it will accept from a neighbor.

You then use the **show access-lists** command to review the access list information.



Viewing Access List Information on Washington

```
Washington>show access-lists
Standard IP access list 21
    permit 172.28.128.7
    permit 172.28.128.8
    permit 172.27.227.7
    permit 172.27.227.8
    permit 172.22.0.0, wildcard bits 0.0.255.255
Standard IP access list CIT
    permit 172.21.0.0, wildcard bits 0.0.255.255 (5 matches) check=200
    permit 172.23.0.0, wildcard bits 0.0.255.255 (8 matches) check=192
    permit 172.24.0.0, wildcard bits 0.0.255.255 (12 matches) check=180
    permit 172.25.0.0, wildcard bits 0.0.255.255 (10 matches) check=170
    permit 172.26.0.0, wildcard bits 0.0.255.255 (10 matches) check=160
Extended IP access list dhcp_glean_acl (per-user)
    permit udp any eq bootpc host 255.255.255.255 eq bootps
Washington>
```

CIT 5.1—4-31

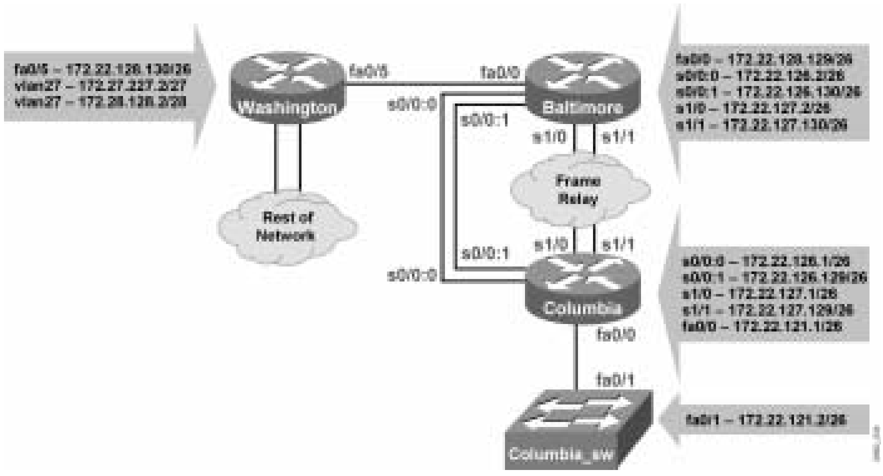
You know that you need to permit all networks that are to be passed by a distribution list. You see that the Cisco Systems network 198.133.219.0/24 is not permitted with the existing access list named CIT. The issue has been isolated to the missing network address in this access list.

Example: Isolating an IP Addressing Problem at the Network Layer

You are the second-level network engineer for a division with locations in Washington, Baltimore, and Columbia. The networking devices at each location are named after the names of the city in which they reside. You have console access to the router named Washington, which gives you IP connectivity to all devices in your network. Your span of responsibility in the corporate network includes the 172.22.0.0/16 subnet.

Example: Isolating an IP Addressing Problem at the Network Layer

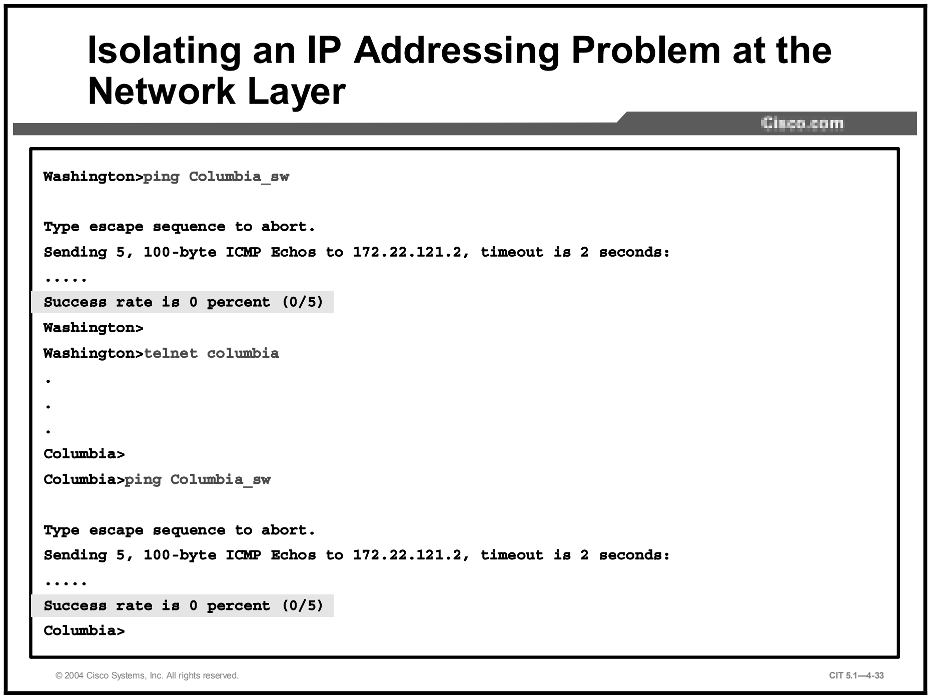
Cisco.com



CIT 5.1—4-32

One day, Network Operations in Columbia calls to report that it cannot ping the switch named Columbia_SW. Network Operations does not recall changing any of the configurations, and they cannot ping Columbia_SW from Washington, either.

You check on the base configuration information and note that the Columbia router and Columbia_SW switch are connected over a 100 Mbps Fast Ethernet link. You try to ping Columbia_SW from Washington and have a 0 percent success rate. You then use Telnet to connect to the Columbia router and try to ping Columbia_SW from there.



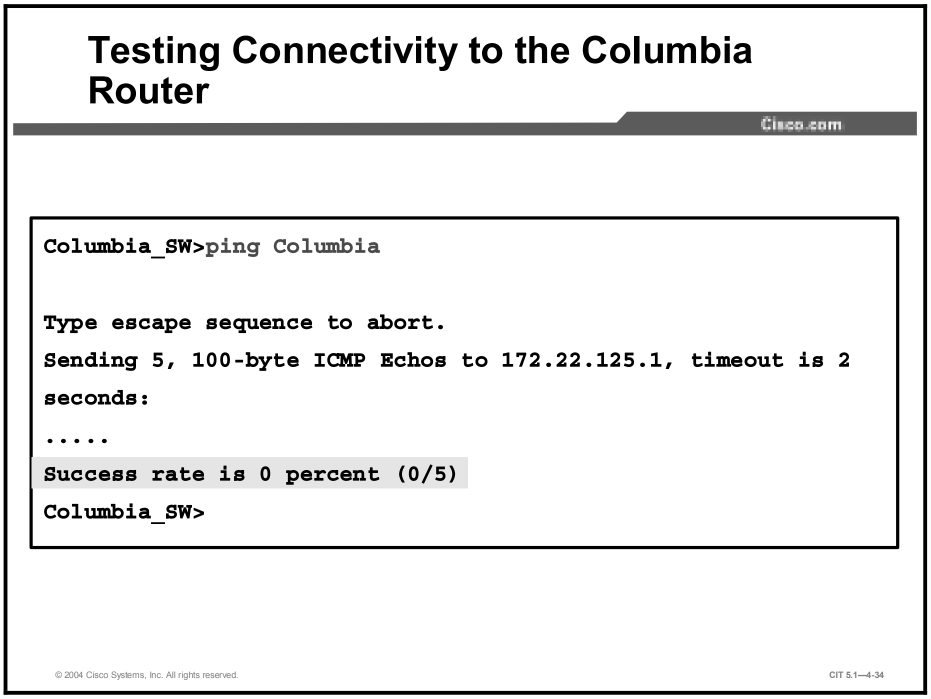
Isolating an IP Addressing Problem at the Network Layer

```
Washington>ping Columbia_sw

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.22.121.2, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
Washington>
Washington>telnet columbia
.
.
.
Columbia>
Columbia>ping Columbia_sw

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.22.121.2, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
Columbia>
```

CIT 5.1—4-33

You note that neither the Washington nor Columbia routers can reach the Columbia_SW switch.

You ask Network Operations in Columbia to try to ping the Columbia router from Columbia_SW.



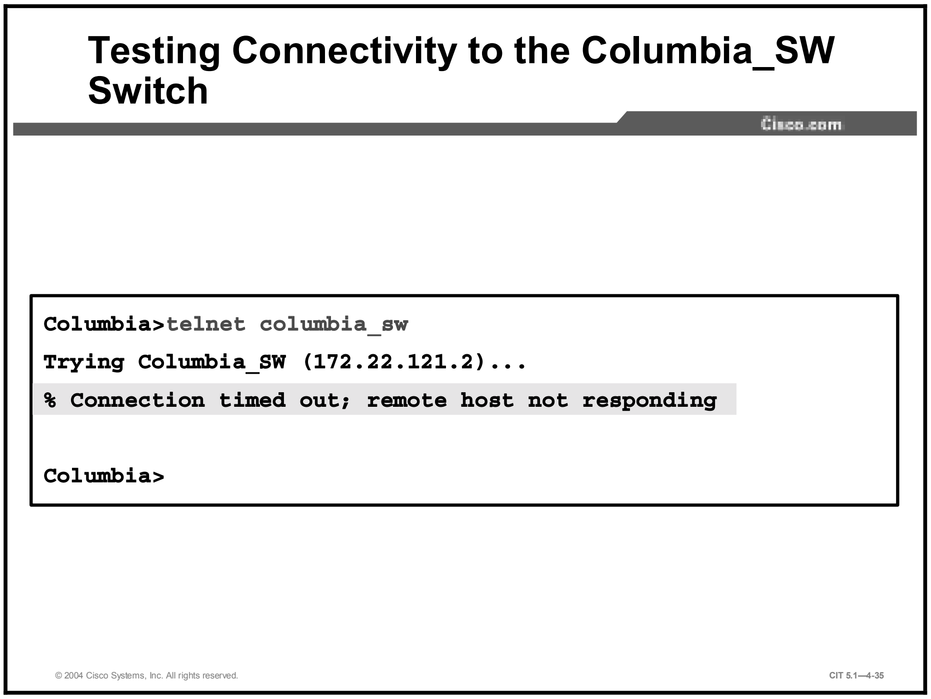
Testing Connectivity to the Columbia Router

```
Columbia_SW>ping Columbia

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.22.125.1, timeout is 2
seconds:
.....
Success rate is 0 percent (0/5)
Columbia_SW>
```

© 2004 Cisco Systems, Inc. All rights reserved. CIT 5.1—4-34

Pinging the Columbia router from Columbia_SW fails.

From the Columbia router, you try using Telnet to connect to the Columbia_SW switch.



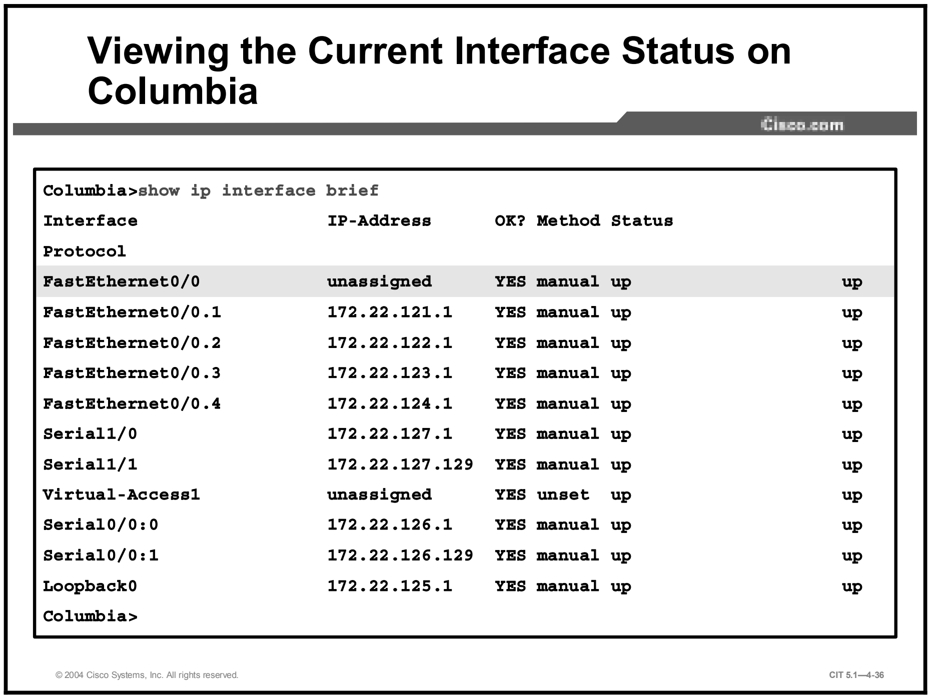
Testing Connectivity to the Columbia_SW Switch

```
Columbia>telnet columbia_sw
Trying Columbia_SW (172.22.121.2)...
% Connection timed out; remote host not responding

Columbia>
```

© 2004 Cisco Systems, Inc. All rights reserved. CIT 5.1—4-35

You note that Telnet and ping traffic to the Columbia_SW switch is not being transferred.

To help isolate the problem, you review the current interface status on Columbia.



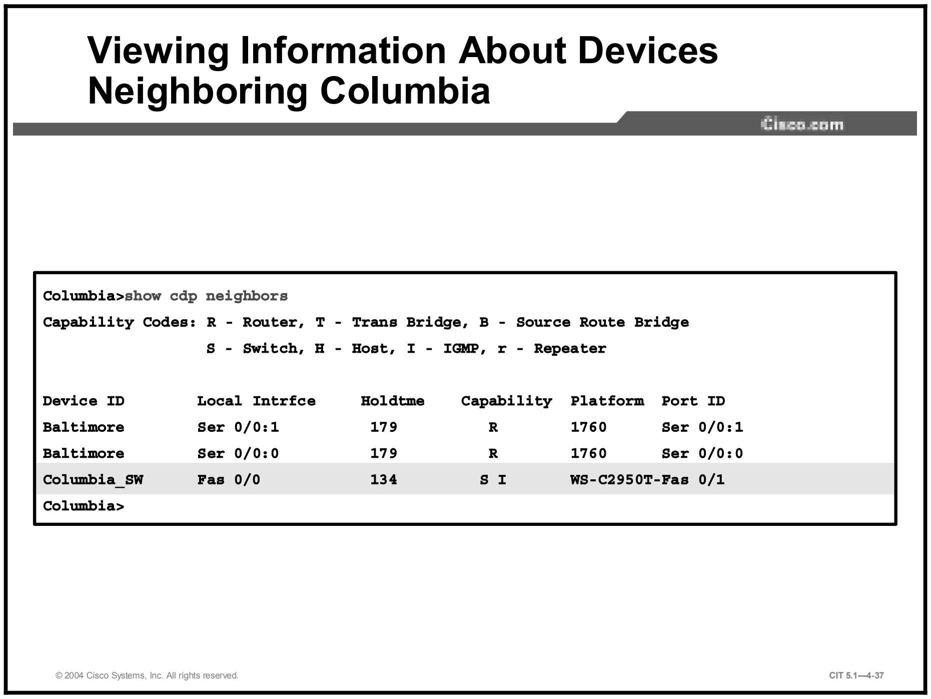
Viewing the Current Interface Status on Columbia

```
Columbia>show ip interface brief
Interface                  IP-Address      OK? Method Status
Protocol
FastEthernet0/0            unassigned      YES manual up                    up
FastEthernet0/0.1          172.22.121.1    YES manual up                    up
FastEthernet0/0.2          172.22.122.1    YES manual up                    up
FastEthernet0/0.3          172.22.123.1    YES manual up                    up
FastEthernet0/0.4          172.22.124.1    YES manual up                    up
Serial1/0                  172.22.127.1    YES manual up                    up
Serial1/1                  172.22.127.129  YES manual up                    up
Virtual-Access1            unassigned      YES unset  up                    up
Serial0/0:0                172.22.126.1    YES manual up                    up
Serial0/0:1                172.22.126.129  YES manual up                    up
Loopback0                  172.22.125.1    YES manual up                    up
Columbia>
```

© 2004 Cisco Systems, Inc. All rights reserved. CIT 5.1—4-36

You see that the physical link to Columbia_SW on Fast Ethernet 0/0 is up.

You then check for Cisco Discovery Protocol (CDP) neighbors with the **show cdp neighbors** command.



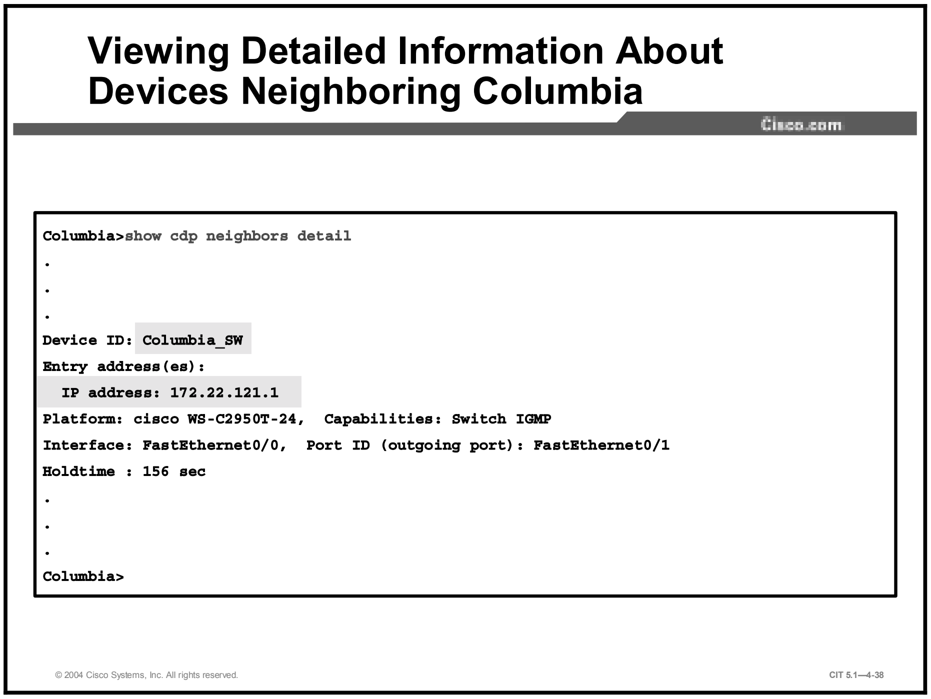
Viewing Information About Devices Neighboring Columbia

```
Columbia>show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
Baltimore        Ser 0/0:1          179          R        1760      Ser 0/0:1
Baltimore        Ser 0/0:0          179          R        1760      Ser 0/0:0
Columbia_SW      Fas 0/0            134         S I       WS-C2950T-Fas 0/1
Columbia>
```

© 2004 Cisco Systems, Inc. All rights reserved. CIT 5.1—4-37

You see that CDP packets are being received from Columbia_SW.

You look for additional information with the **show cdp neighbors detail** command.



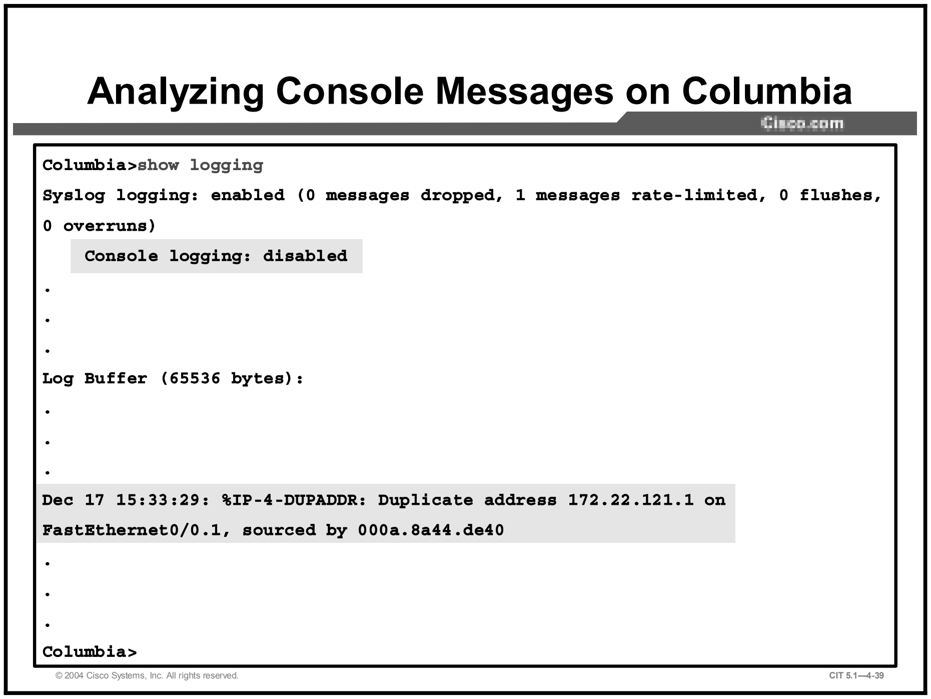
Viewing Detailed Information About Devices Neighboring Columbia

```
Columbia>show cdp neighbors detail
.
.
.
Device ID: Columbia_SW
Entry address(es):
  IP address: 172.22.121.1
Platform: cisco WS-C2950T-24,  Capabilities: Switch IGMP
Interface: FastEthernet0/0,  Port ID (outgoing port): FastEthernet0/1
Holdtime : 156 sec
.
.
.
Columbia>
```

CIT 5.1—4-38

You see the issue. Now it is time to illustrate the issue for Network Operations.

You call back Network Operations in Columbia to see if there are any error messages on the console of Columbia or Columbia_SW. No one at Network Operations has seen any. You ask their team to input the command **show logging** on Columbia to help isolate the issue. (You enter the **show logging** command on Columbia, as well.)



Analyzing Console Messages on Columbia

```
Columbia>show logging
Syslog logging: enabled (0 messages dropped, 1 messages rate-limited, 0 flushes,
0 overruns)
    Console logging: disabled
.
.
.
Log Buffer (65536 bytes):
.
.
.
Dec 17 15:33:29: %IP-4-DUPADDR: Duplicate address 172.22.121.1 on
FastEthernet0/0.1, sourced by 000a.8a44.de40
.
.
.
Columbia>
```

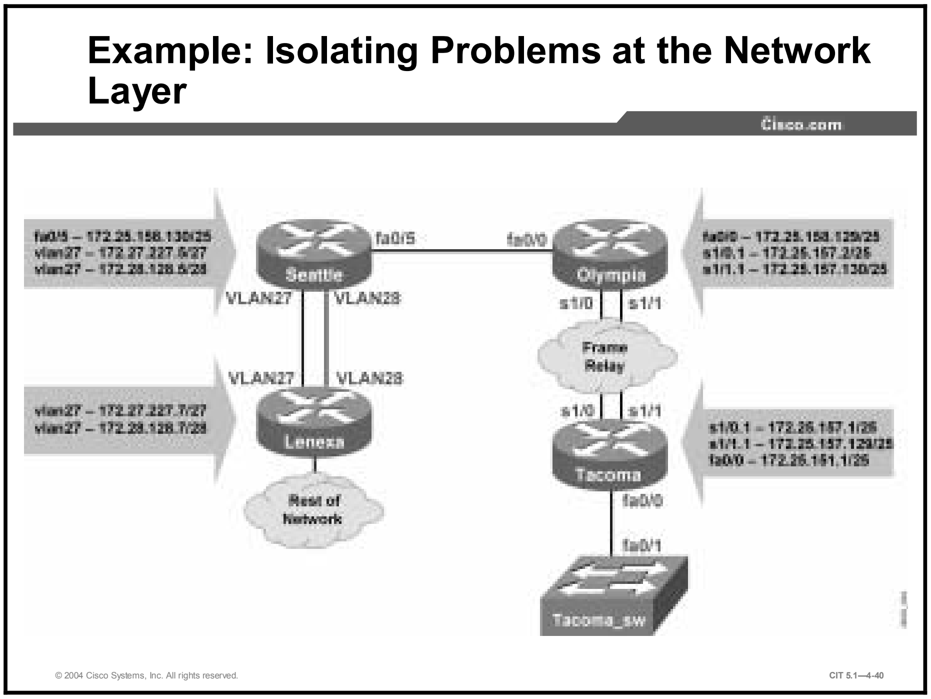
© 2004 Cisco Systems, Inc. All rights reserved. CIT 5.1—4-39

You ask Network Operations to check if console logging is disabled. Your default practice is to have console logging enabled, because console messages can provide useful information. You then suggest that Network Operations scan the error messages for reoccurring messages. Network Operations notices that there is a duplicate IP address (172.22.121.1) on FastEthernet0/0.1. This is indeed a network layer issue.

You know from the baseline that Columbia should have IP address 172.22.121.1 on Fast Ethernet 0/0.1. However, Columbia_SW should use 172.22.121.2. If logging had been enabled, the isolation problem would have been trivial.

Example: Isolating Problems at the Network Layer

You are the second-level network engineer for a division with locations in Seattle, Olympia, and Tacoma. The networking devices at each location are named after the names of the city in which they reside. You have console access to the router named Seattle, which gives you IP connectivity to all devices in your network. Your span of responsibility in the corporate network includes the 172.25.0.0/16 subnet.



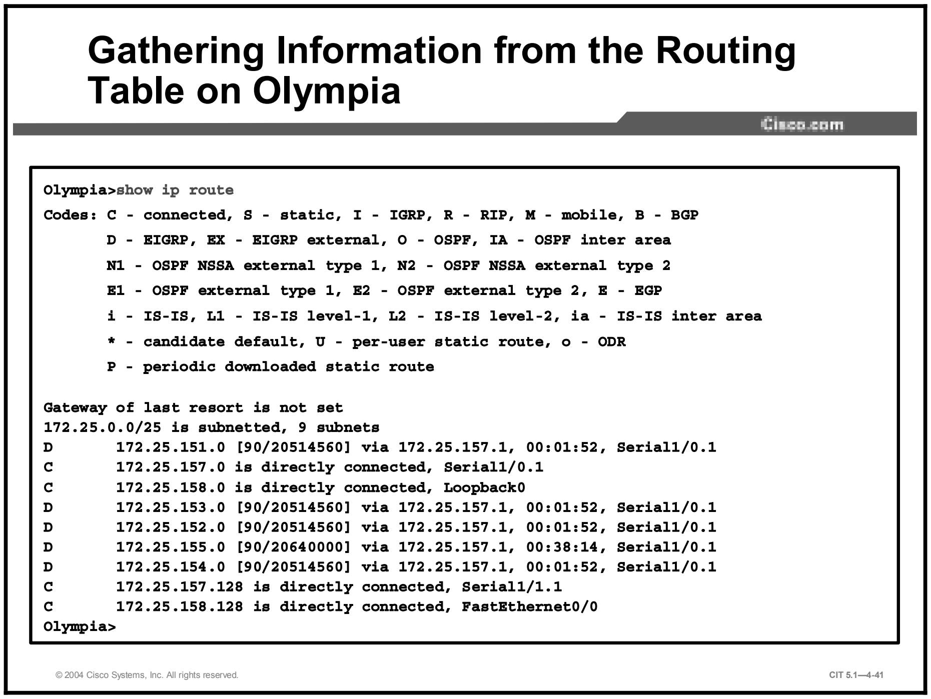
Example: Isolating Problems at the Network Layer

© 2004 Cisco Systems, Inc. All rights reserved.

CIT 5.1—4-40

One day, Network Operations from Olympia calls to say that it has lost all routes from the Seattle core router.

You ask the network operations team what they see in their routing table. They list only their connected routes and the routes from the access router Tacoma.

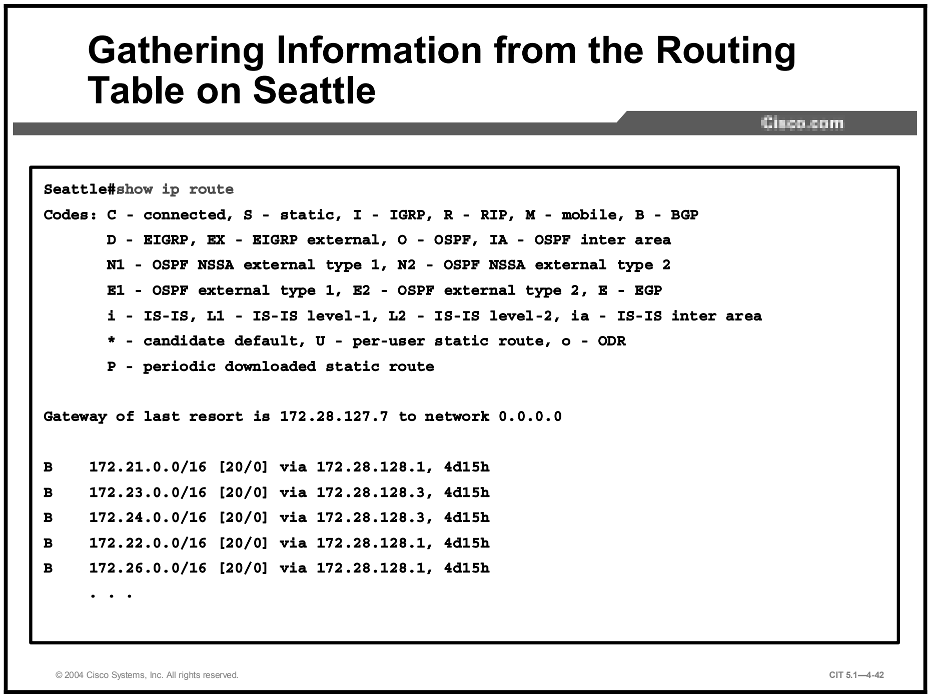


Gathering Information from the Routing Table on Olympia

```
Olympia>show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set
172.25.0.0/25 is subnetted, 9 subnets
D       172.25.151.0 [90/20514560] via 172.25.157.1, 00:01:52, Serial1/0.1
C       172.25.157.0 is directly connected, Serial1/0.1
C       172.25.158.0 is directly connected, Loopback0
D       172.25.153.0 [90/20514560] via 172.25.157.1, 00:01:52, Serial1/0.1
D       172.25.152.0 [90/20514560] via 172.25.157.1, 00:01:52, Serial1/0.1
D       172.25.155.0 [90/20640000] via 172.25.157.1, 00:38:14, Serial1/0.1
D       172.25.154.0 [90/20514560] via 172.25.157.1, 00:01:52, Serial1/0.1
C       172.25.157.128 is directly connected, Serial1/1.1
C       172.25.158.128 is directly connected, FastEthernet0/0
Olympia>
```

CIT 5.1—4-41

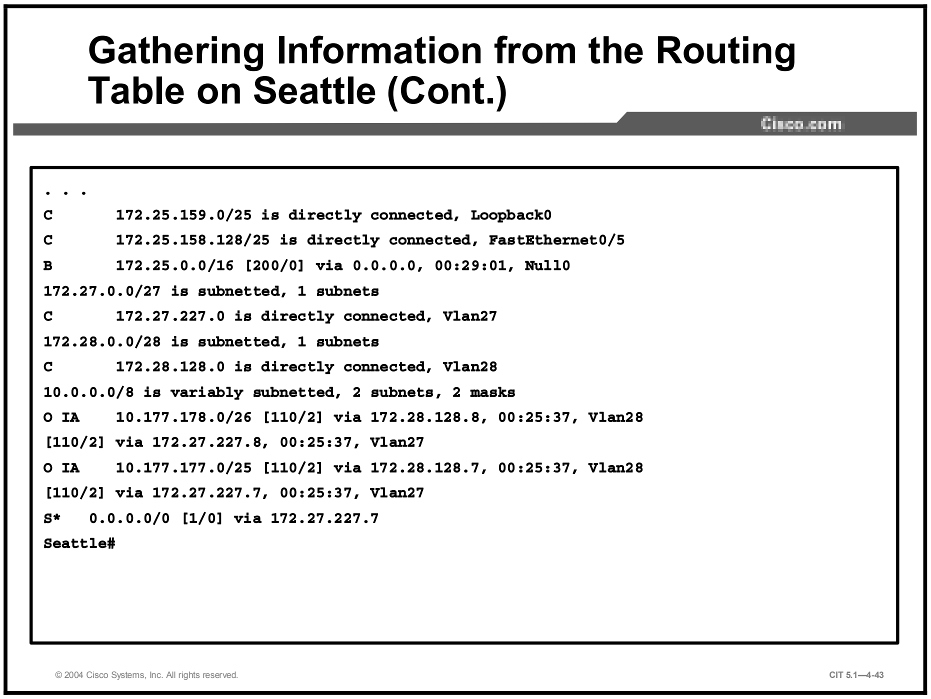
You check the status of routes on Seattle.



Gathering Information from the Routing Table on Seattle

```
Seattle#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 172.28.127.7 to network 0.0.0.0

B    172.21.0.0/16 [20/0] via 172.28.128.1, 4d15h
B    172.23.0.0/16 [20/0] via 172.28.128.3, 4d15h
B    172.24.0.0/16 [20/0] via 172.28.128.3, 4d15h
B    172.22.0.0/16 [20/0] via 172.28.128.1, 4d15h
B    172.26.0.0/16 [20/0] via 172.28.128.1, 4d15h
     . . .
```

CIT 5.1—4-42



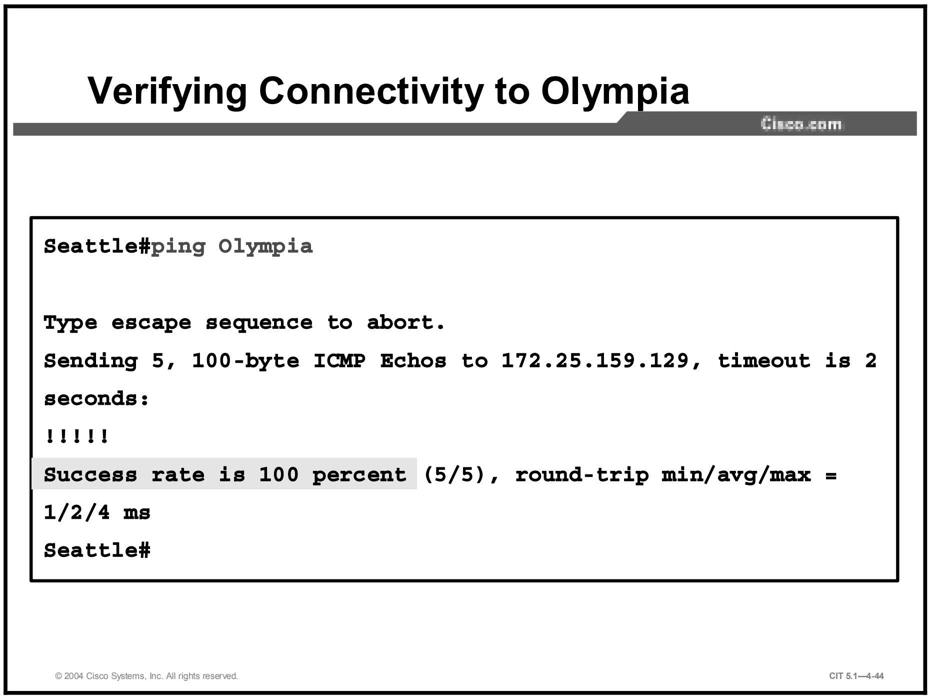
Gathering Information from the Routing Table on Seattle (Cont.)

```
. . .
C       172.25.159.0/25 is directly connected, Loopback0
C       172.25.158.128/25 is directly connected, FastEthernet0/5
B       172.25.0.0/16 [200/0] via 0.0.0.0, 00:29:01, Null0
172.27.0.0/27 is subnetted, 1 subnets
C       172.27.227.0 is directly connected, Vlan27
172.28.0.0/28 is subnetted, 1 subnets
C       172.28.128.0 is directly connected, Vlan28
10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
O IA    10.177.178.0/26 [110/2] via 172.28.128.8, 00:25:37, Vlan28
[110/2] via 172.27.227.8, 00:25:37, Vlan27
O IA    10.177.177.0/25 [110/2] via 172.28.128.7, 00:25:37, Vlan28
[110/2] via 172.27.227.7, 00:25:37, Vlan27
S*   0.0.0.0/0 [1/0] via 172.27.227.7
Seattle#
```

CIT 5.1—4-43

You notice that you are missing the routes from the Olympia distribution router.

You verify connectivity to Olympia.



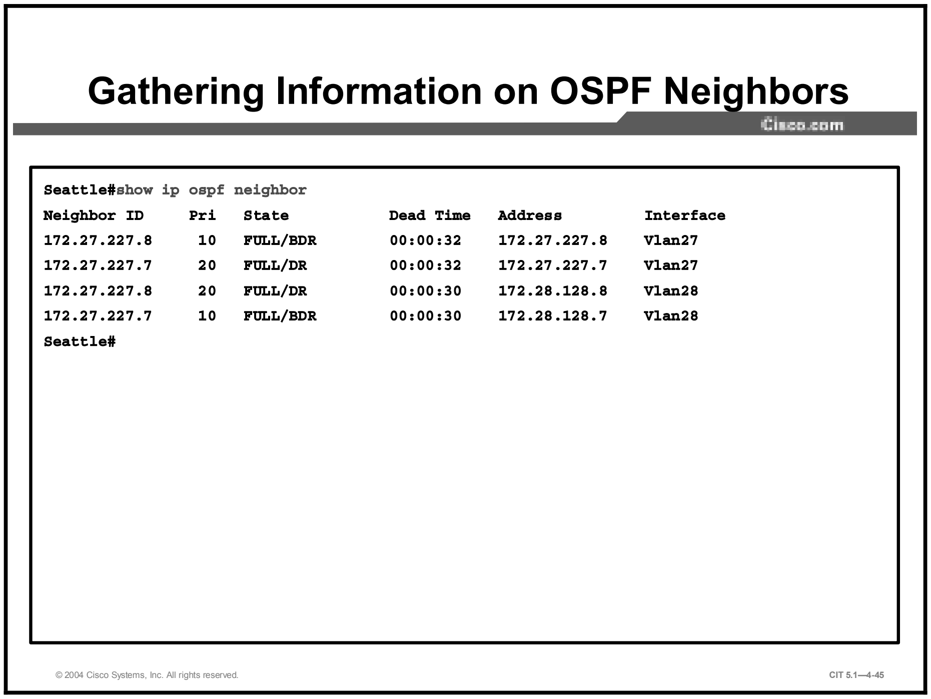
Verifying Connectivity to Olympia

```
Seattle#ping Olympia

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.25.159.129, timeout is 2
seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
1/2/4 ms
Seattle#
```

CIT 5.1—4-44

This command confirms that you have network layer connectivity to Olympia.

You check the status of OSPF neighbors on Seattle.



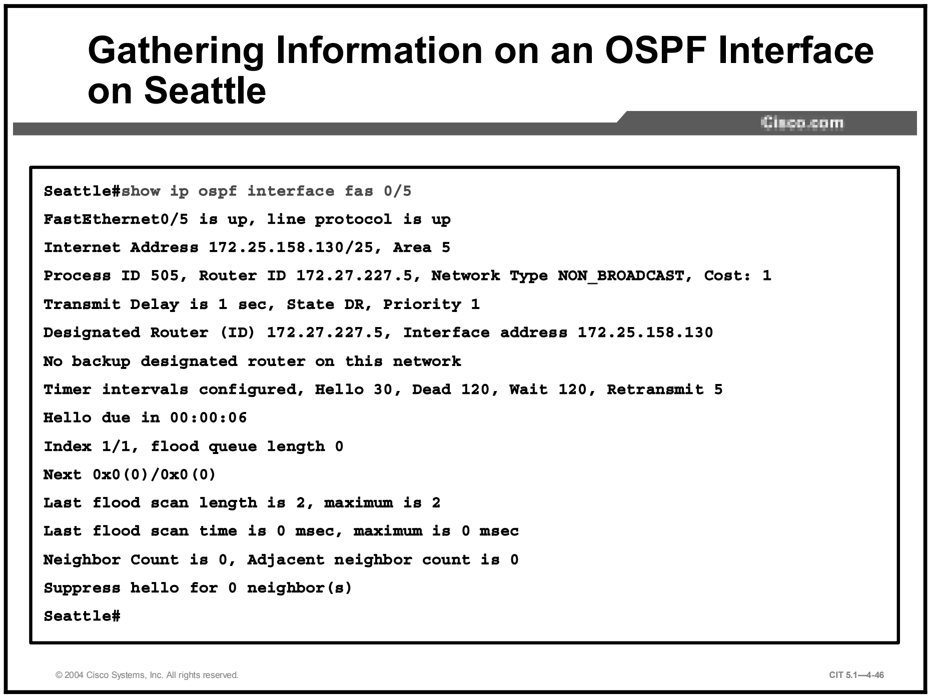
Gathering Information on OSPF Neighbors

```
Seattle#show ip ospf neighbor
Neighbor ID     Pri   State           Dead Time   Address         Interface
172.27.227.8     10   FULL/BDR        00:00:32    172.27.227.8    Vlan27
172.27.227.7     20   FULL/DR         00:00:32    172.27.227.7    Vlan27
172.27.227.8     20   FULL/DR         00:00:30    172.28.128.8    Vlan28
172.27.227.7     10   FULL/BDR        00:00:30    172.28.128.7    Vlan28
Seattle#
```

CIT 5.1—4-45

You see that there is no neighbor relationship with Olympia.

You verify that the interfaces between Seattle and Olympia have been configured for OSPF.

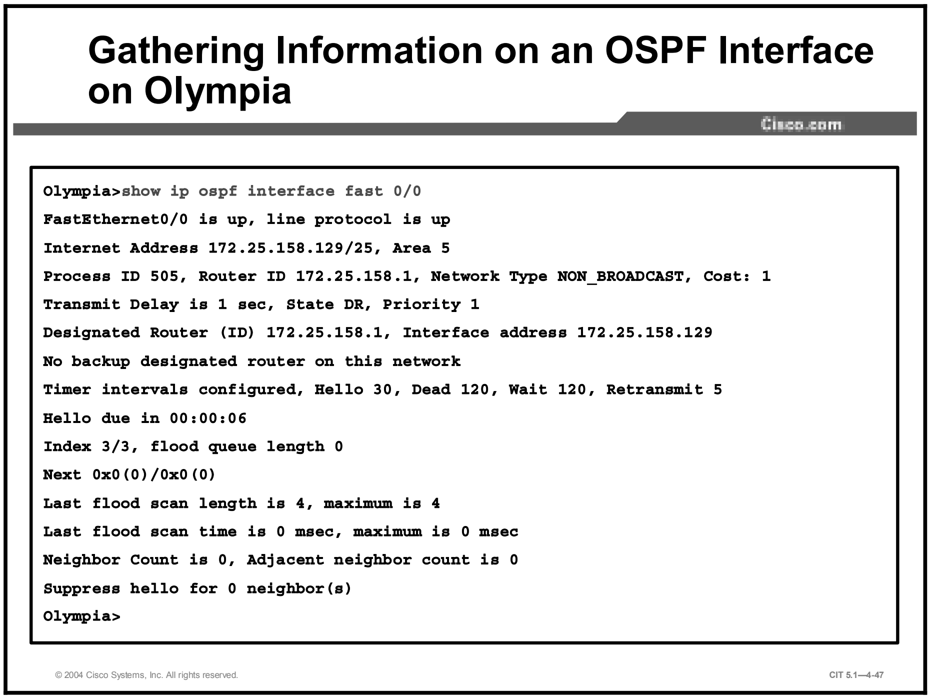


Gathering Information on an OSPF Interface on Seattle

```
Seattle#show ip ospf interface fas 0/5
FastEthernet0/5 is up, line protocol is up
Internet Address 172.25.158.130/25, Area 5
Process ID 505, Router ID 172.27.227.5, Network Type NON_BROADCAST, Cost: 1
Transmit Delay is 1 sec, State DR, Priority 1
Designated Router (ID) 172.27.227.5, Interface address 172.25.158.130
No backup designated router on this network
Timer intervals configured, Hello 30, Dead 120, Wait 120, Retransmit 5
Hello due in 00:00:06
Index 1/1, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 2, maximum is 2
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 0, Adjacent neighbor count is 0
Suppress hello for 0 neighbor(s)
Seattle#
```

CIT 5.1—4-46

You see that the Fast Ethernet interfaces between Seattle and Olympia are OSPF interfaces without any neighbors.

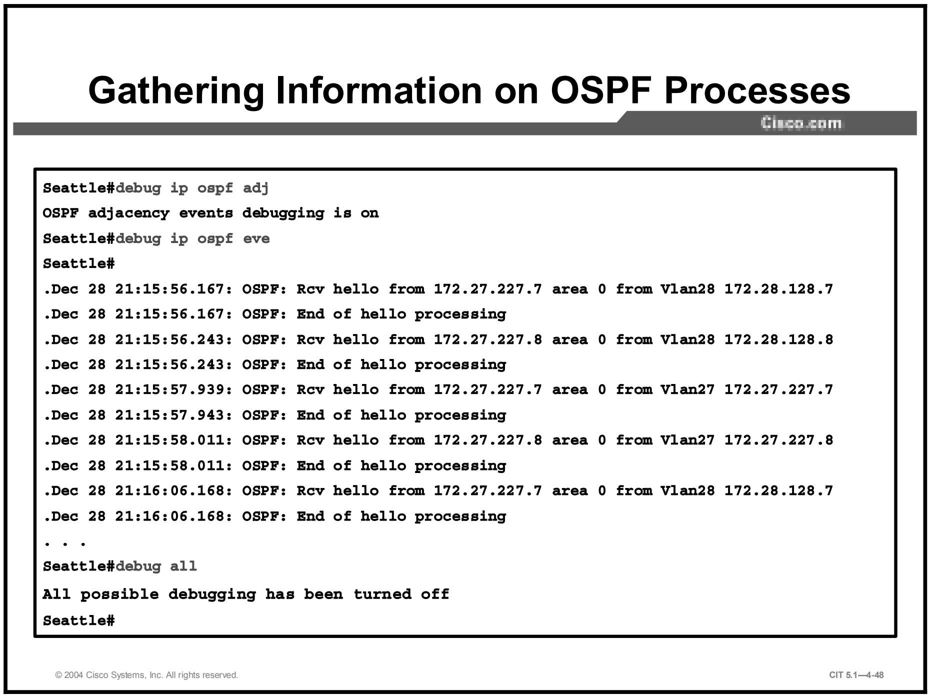


Gathering Information on an OSPF Interface on Olympia

```
Olympia>show ip ospf interface fast 0/0
FastEthernet0/0 is up, line protocol is up
Internet Address 172.25.158.129/25, Area 5
Process ID 505, Router ID 172.25.158.1, Network Type NON_BROADCAST, Cost: 1
Transmit Delay is 1 sec, State DR, Priority 1
Designated Router (ID) 172.25.158.1, Interface address 172.25.158.129
No backup designated router on this network
Timer intervals configured, Hello 30, Dead 120, Wait 120, Retransmit 5
Hello due in 00:00:06
Index 3/3, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 4, maximum is 4
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 0, Adjacent neighbor count is 0
Suppress hello for 0 neighbor(s)
Olympia>
```

CIT 5.1—4-47

You may run some debugging commands on Seattle, as needed.



Gathering Information on OSPF Processes

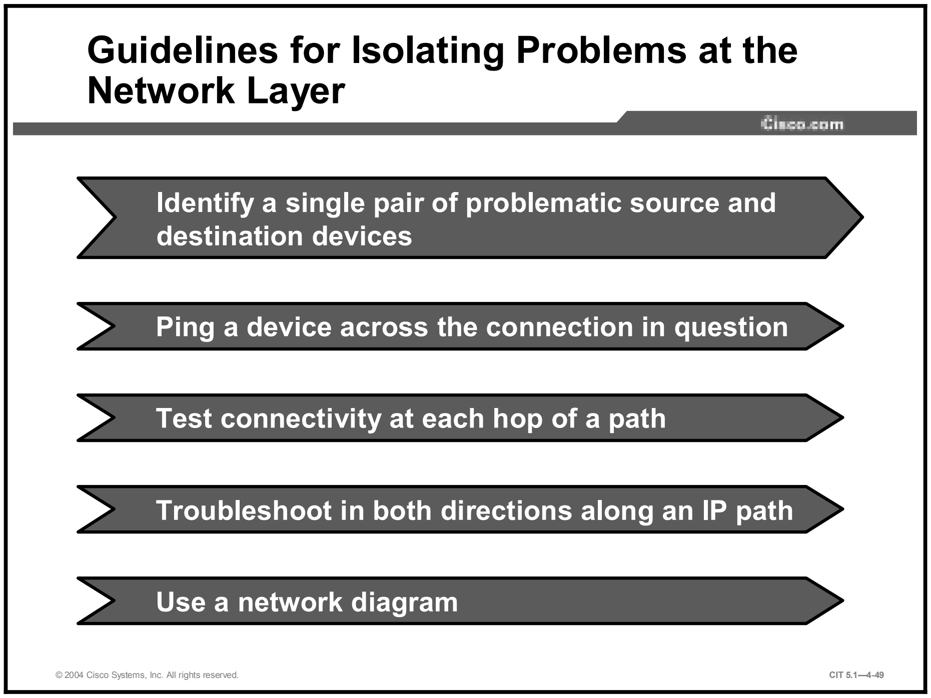
```
Seattle#debug ip ospf adj
OSPF adjacency events debugging is on
Seattle#debug ip ospf eve
Seattle#
.Dec 28 21:15:56.167: OSPF: Rcv hello from 172.27.227.7 area 0 from Vlan28 172.28.128.7
.Dec 28 21:15:56.167: OSPF: End of hello processing
.Dec 28 21:15:56.243: OSPF: Rcv hello from 172.27.227.8 area 0 from Vlan28 172.28.128.8
.Dec 28 21:15:56.243: OSPF: End of hello processing
.Dec 28 21:15:57.939: OSPF: Rcv hello from 172.27.227.7 area 0 from Vlan27 172.27.227.7
.Dec 28 21:15:57.943: OSPF: End of hello processing
.Dec 28 21:15:58.011: OSPF: Rcv hello from 172.27.227.8 area 0 from Vlan27 172.27.227.8
.Dec 28 21:15:58.011: OSPF: End of hello processing
.Dec 28 21:16:06.168: OSPF: Rcv hello from 172.27.227.7 area 0 from Vlan28 172.28.128.7
.Dec 28 21:16:06.168: OSPF: End of hello processing
. . .
Seattle#debug all
All possible debugging has been turned off
Seattle#
```

CIT 5.1—4-48

You should see the issue. (If not, this issue will be illustrated in the Isolating Problems Occurring at the Network Layer topic).

Isolating Problems Occurring at the Network Layer

This topic identifies guidelines for isolating problems at the network layer.



Guidelines for Isolating Problems at the Network Layer

- Identify a single pair of problematic source and destination devices
- Ping a device across the connection in question
- Test connectivity at each hop of a path
- Troubleshoot in both directions along an IP path
- Use a network diagram

CIT 5.1—4-49

Use an effective and systematic technique to successfully isolate a problem at the network layer. To isolate problems at the network layer, use the following guidelines:

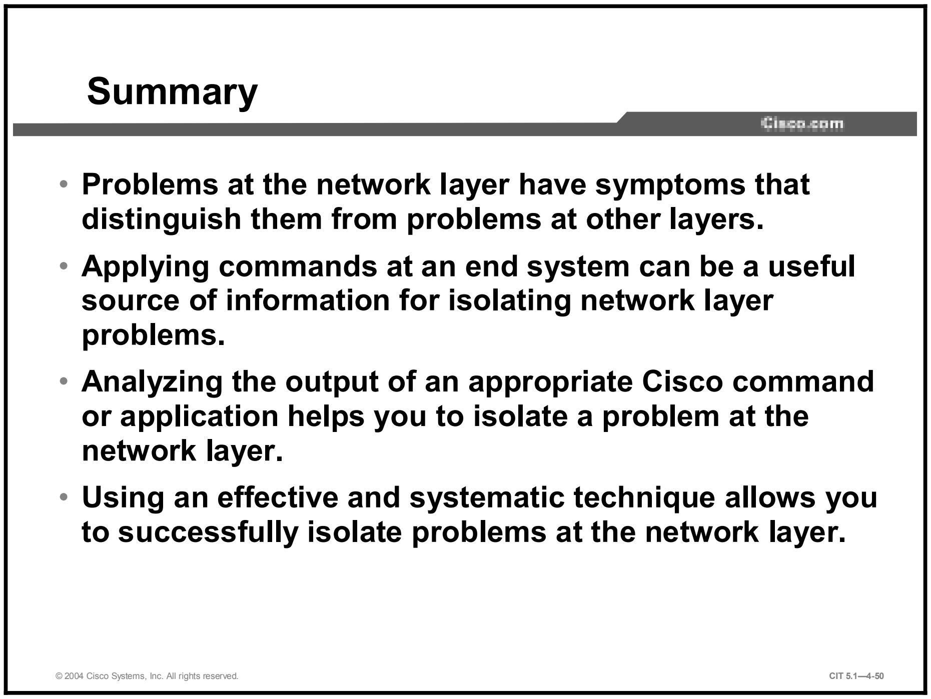
- **Identify a single pair of problematic source and destination devices:** When you have identified the two devices that are the most likely sources of the connectivity problem, test the connectivity between the two devices.
- **Ping a device across the connection:** Pinging a device verifies that the problem is at the network layer. If the ping fails, check both the physical and data link layers. If the **ping** command is successful, the physical and data link layers are functioning properly and the problem resides in the upper layers.
- **Test connectivity at each hop of a connection:** There is a potential for problems at every hop between the source and destination. Therefore, it is important that you test connectivity at each hop to determine where a problem exists.
- **Troubleshoot in both directions along an IP path:** A packet can have a working path in one direction, such as from the source to the destination, but not have a working path in the opposite direction. This situation happens because IP does not store path information in its packets. To prevent overlooking an error, perform all troubleshooting steps in both directions of an IP path.
- **Use a network diagram:** Use a network diagram to understand the path that the traffic should take. Compare the path that the traffic should have taken to the path that it is actually taking. This task is especially important if you are troubleshooting a problem across large networks.

Example: Isolating Problems Occurring at the Network Layer

Users on an Ethernet LAN have reported that their connection to the Internet has gone down. Examining the topology diagram for the network, you determine which networking devices are the possible problem. You use Cisco diagnostic commands to narrow down the problem to a particular path involving multiple routers. You enter the **ping** command from the source router that the users had been attempting to connect through to the destination router. As you expected, this test fails. You then enter the **ping** command from the destination router to the source router. The ping works. You test the connectivity between the source and destination routers at the physical and data link layers and determine that both layers are functioning correctly. The results indicate that you have a problem at the network layer. You execute **show** and **debug** commands on the path and discover a misconfigured static address in the routing table of one of the routers in the path.

Summary

This topic summarizes the key points discussed in this lesson.



Summary

- Problems at the network layer have symptoms that distinguish them from problems at other layers.
- Applying commands at an end system can be a useful source of information for isolating network layer problems.
- Analyzing the output of an appropriate Cisco command or application helps you to isolate a problem at the network layer.
- Using an effective and systematic technique allows you to successfully isolate problems at the network layer.

CIT 5.1—4-50

References

For additional information, refer to these resources:

- Cisco online documentation:
  http://www.cisco.com/univercd/home/home.htm
- Cisco Technical Assistance Center (TAC):
  http://www.cisco.com/tac
- Troubleshooting TCP/IP:
  http://www.cisco.com/univercd/cc/td/doc/cisintwk/itg_v1/tr1907.htm

Quiz

Use the practice items here to review what you have learned in this lesson. The correct answers are found in the Quiz Answer Key.

Q1) Users in a segment of your company LAN are complaining that access to devices on the network is much slower than usual. You check the network topology diagram to determine which devices are routing packets to that segment.

What symptom(s) would be present if this problem is located at the network layer?

A) A particular application consistently crashes; there are large amounts of broadcast traffic.

B) No devices are reachable; Layer 3 is consistently not operational.

C) There are excessive CRC/FCS errors; default routes are missing from the routing table.

D) Traffic is taking a path other than the expected path recorded in the baseline.

Q2) A NIC on an end system was faulty and replaced. However, the end system still cannot connect beyond the local network. Examine this snippet of the configuration for the default gateway for the end system and then choose a command that might solve the problem using the information given.

```
interface Ethernet0
ip address 192.168.1.254 255.255.255.0
no ip directed-broadcast
```

A) **clear interface Ethernet0**

B) **clear arp-cache**

C) **ip directed-broadcasts**

D) **debug ip packet detail**

Q3) What command would you enter at a Windows NT end system to display the current IP routing table for a device?

A) **ipconfig /all**

B) **ifconfig –a**

C) **route print**

D) **arp –a**

Q4) Users on a large Ethernet LAN report that their connection to the network is much slower than usual. You determine which two routers are the source and destination devices for the users of that network. You know that there is connectivity, so you run a trace instead of pinging between the devices. Running a trace from the source to the destination indicates that there is significant latency at a few of the hops along the path. You reverse the trace and verify that there is latency from the destination to the source, as well. You recognize that this latency is the cause of the problem but you are not sure why it is happening. Which guideline for isolating problems at the network layer should you practice next?

A) perform a loopback test to verify that the TCP/IP stack is loaded and functional

B) disable spanning tree on the destination device, but not the source device.

C) refer to the network diagram to verify that the devices are connecting across the expected path

D) visually inspect the serial connection between the devices

Quiz Answer Key

Q1) D

Relates to: Identifying the Symptoms of Problems Occurring at the Network Layer

Q2) B

Relates to: Analyzing Cisco Commands and Applications to Isolate Problems Occurring at the Network Layer

Q3) C

Relates to: Identifying End-System Commands and Applications Used to Isolate Problems Occurring at the Network Layer

Q4) C

Relates to: Isolating Problems Occurring at the Network Layer

Correcting the Problem

Overview

Once a troubleshooter has determined the most likely cause of the problem, the next stage of the general troubleshooting process is to correct the problem. In this lesson, you will correct network layer problems using commands and applications that configure network layer components.

Relevance

Isolating a network problem is a vital step for you to perform to successfully troubleshoot a problem. However, merely isolating the problem will not bring about the types of changes that you need to make so that the network functions at the documented network baseline. To resolve the problem, you must use the tools and resources provided by Cisco and your end systems to configure the properties of your network.

Objectives

Upon completing this lesson, you will be able to:

- Identify Cisco commands that are used to correct problems occurring at the network layer
- Identify end-system commands and applications that are used to correct problems occurring at the network layer
- Identify network layer support resources
- Correct a problem occurring at the network layer

Learner Skills and Knowledge

To benefit fully from this lesson, you must have these prerequisite skills and knowledge:

- The ability to apply layered model troubleshooting approaches
- Familiarity with Cisco command syntax covered in the Cisco *Building Scalable Cisco Internetworks* (BSCI), *Building Cisco Multilayer Switched Networks* (BCMSN), and *Building Cisco Remote Access Networks* (BCRAN) courses

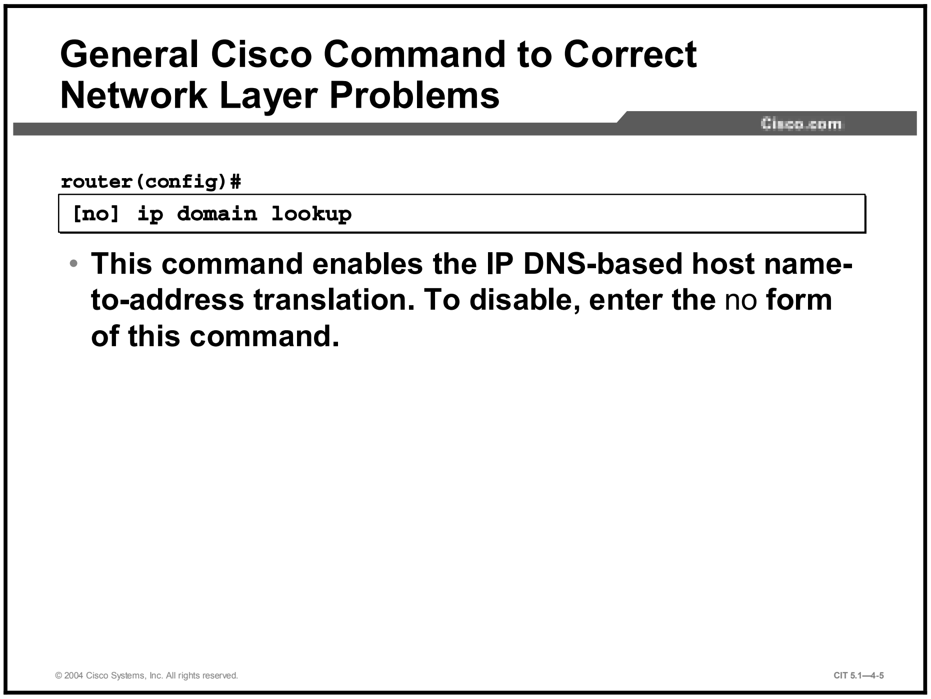
Outline

This lesson includes these topics:

- Overview
- Identifying Cisco Commands Used to Correct Problems Occurring at the Network Layer
- Identifying End-System Commands and Applications Used to Correct Problems Occurring at the Network Layer
- Identifying Network Layer Support Resources
- Correcting Problems Occurring at the Network Layer
- Summary
- Quiz

Identifying Cisco Commands Used to Correct Problems Occurring at the Network Layer

This topic identifies Cisco commands that troubleshooters use to correct problems at the network layer.



General Cisco Command to Correct Network Layer Problems

```
router(config)#
[no] ip domain lookup
```

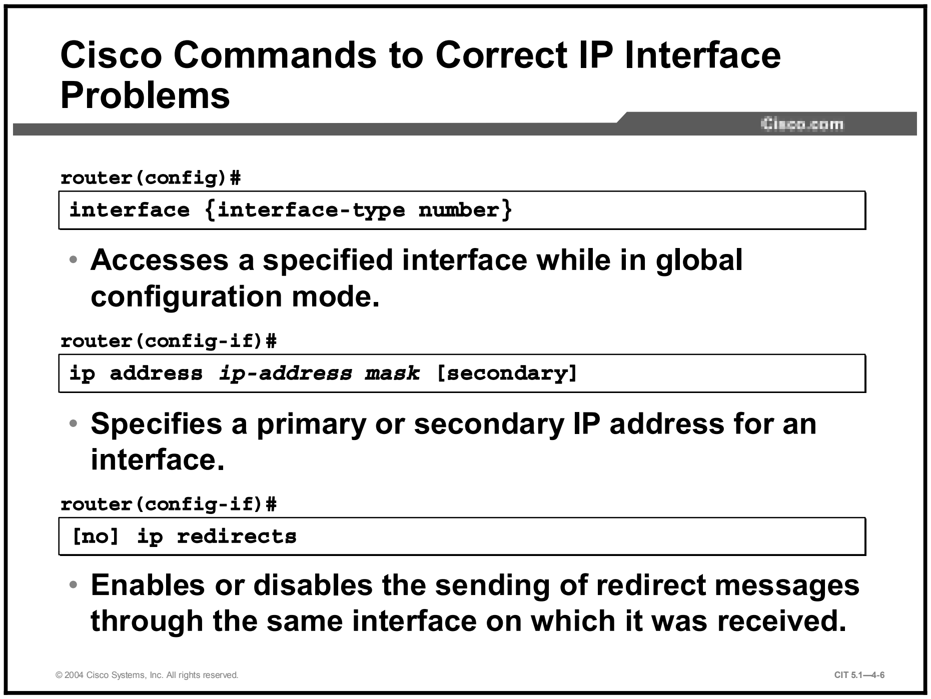
- **This command enables the IP DNS-based host name-to-address translation. To disable, enter the** no **form of this command.**

CIT 5.1—4-5

The general Cisco command listed in the table makes configuration changes that can be used by troubleshooters to correct problems at the network layer.

General Cisco Command to Correct Network Layer Problems

Command	Description
`[no] ip domain lookup`	Enables the IP DNS-based host name-to-address translation. To disable, enter the **no** form of this command.



Cisco Commands to Correct IP Interface Problems

```
router(config)#
interface {interface-type number}
```

- Accesses a specified interface while in global configuration mode.

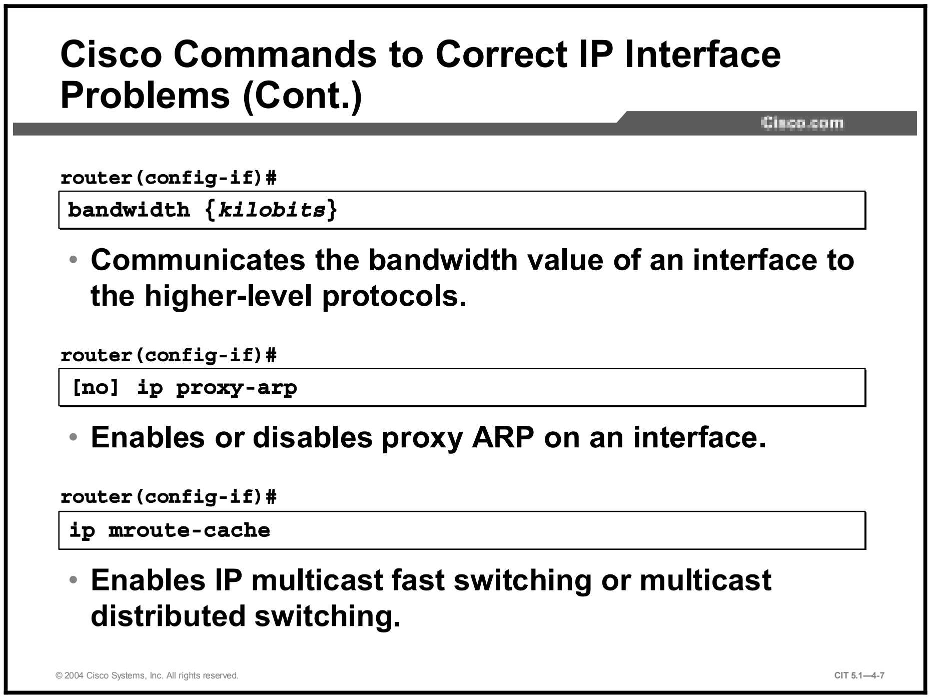
```
router(config-if)#
ip address ip-address mask [secondary]
```

- Specifies a primary or secondary IP address for an interface.

```
router(config-if)#
[no] ip redirects
```

- Enables or disables the sending of redirect messages through the same interface on which it was received.

CIT 5.1—4-6



Cisco Commands to Correct IP Interface Problems (Cont.)

```
router(config-if)#
bandwidth {kilobits}
```

- Communicates the bandwidth value of an interface to the higher-level protocols.

```
router(config-if)#
[no] ip proxy-arp
```

- Enables or disables proxy ARP on an interface.

```
router(config-if)#
ip mroute-cache
```

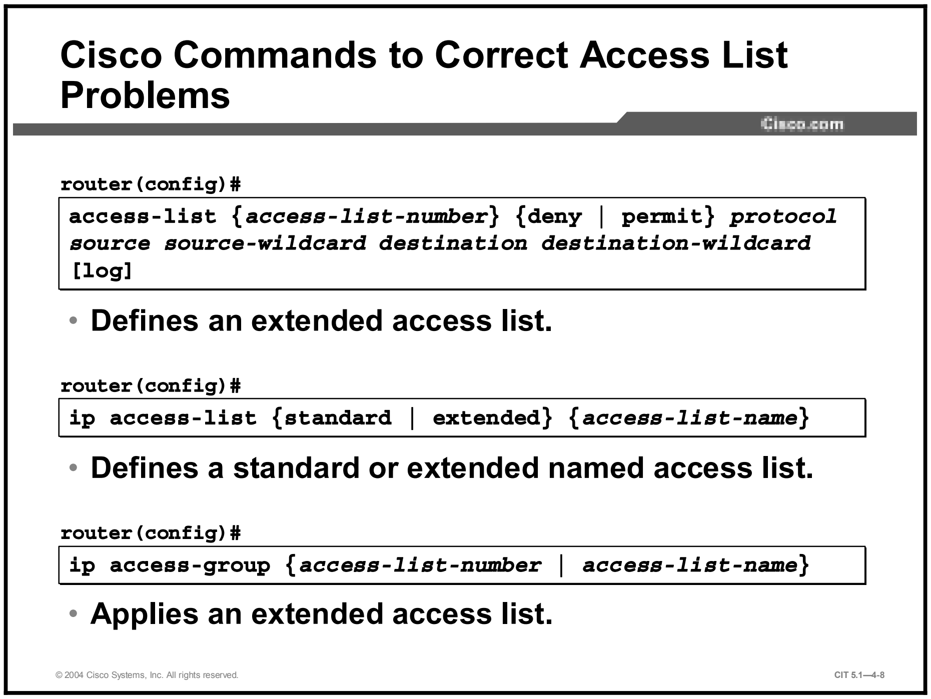
- Enables IP multicast fast switching or multicast distributed switching.

CIT 5.1—4-7

Troubleshooters can use the Cisco commands listed in the table to make configuration changes to correct problems with IP interfaces that occur at the network layer.

Cisco Commands to Correct IP Interface Problems

Command	Description
interface {**interface-type number**}	Accesses a specified interface while in global configuration mode.
ip address ***ip-address mask*** [**secondary**]	Specifies a primary or secondary IP address for an interface.
[**no**] **ip redirects**	Enables or disables the sending of redirect messages through the same interface on which it was received.
bandwidth *kilobits*	Communicates the bandwidth value of an interface to the higher-level protocols.
[**no**] **ip proxy-arp**	Enables or disables proxy ARP on an interface.
ip mroute-cache	Enables IP multicast fast switching or multicast distributed switching.



Cisco Commands to Correct Access List Problems

```
router(config)#
access-list {access-list-number} {deny | permit} protocol
source source-wildcard destination destination-wildcard
[log]
```

- Defines an extended access list.

```
router(config)#
ip access-list {standard | extended} {access-list-name}
```

- Defines a standard or extended named access list.

```
router(config)#
ip access-group {access-list-number | access-list-name}
```

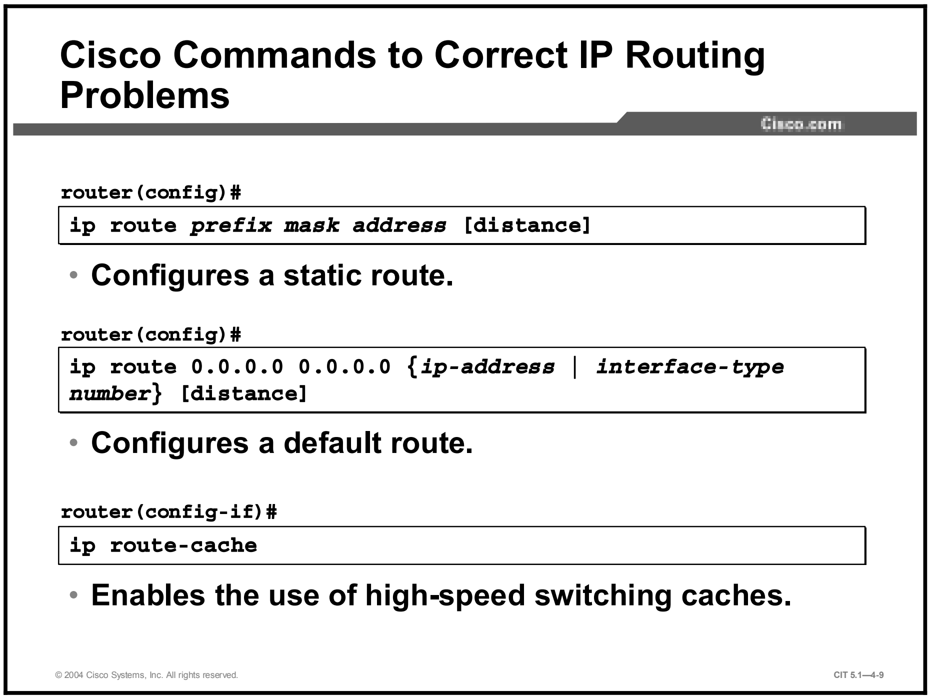
- Applies an extended access list.

Troubleshooters can use the Cisco commands listed in the table to make configuration changes to correct problems with access lists that occur at the network layer.

Cisco Commands to Correct Access List Problems

Command	Description
access-list {*access-list-number*} {**deny** | **permit**} *protocol source source-wildcard destination destination-wildcard* [**log**]	Defines an extended access list.
ip access-list {**standard** | **extended**} {*access-list-name*}	Defines a standard or extended named access list.
ip access-group {*access-list-number* | *access-list-name*}	Applies an extended access list.

Note Not all of the commands listed are available on some versions of Cisco operating systems. To determine which commands are available for use with your devices, consult the online documentation for Cisco devices at http://www.cisco.com/univercd/home/home.htm.



Cisco Commands to Correct IP Routing Problems

router(config)#

```
ip route prefix mask address [distance]
```

- Configures a static route.

router(config)#

```
ip route 0.0.0.0 0.0.0.0 {ip-address | interface-type
number} [distance]
```

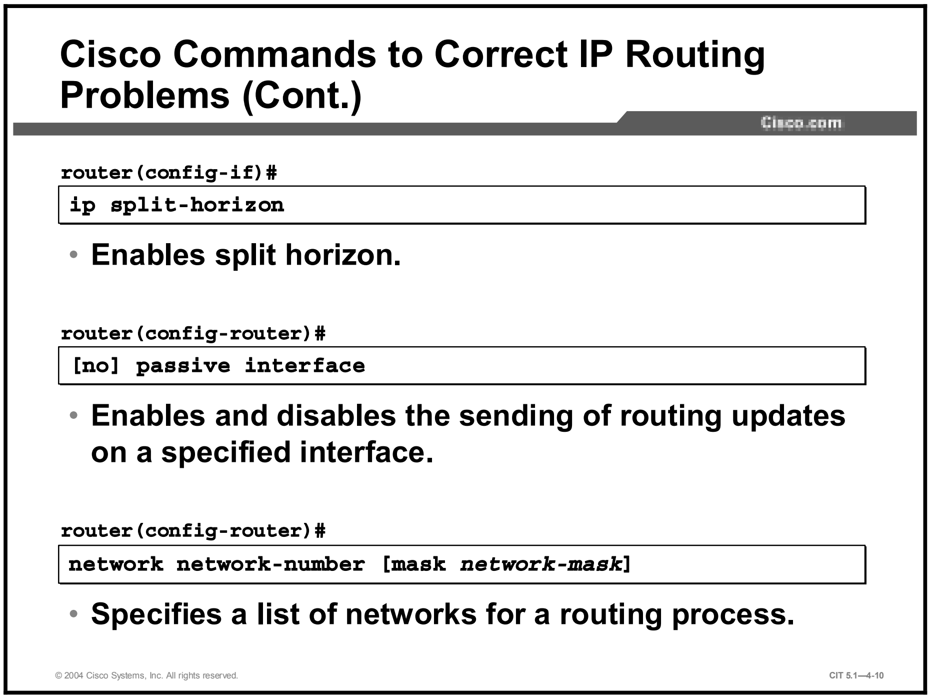
- Configures a default route.

router(config-if)#

```
ip route-cache
```

- Enables the use of high-speed switching caches.

CIT 5.1—4-9



Cisco Commands to Correct IP Routing Problems (Cont.)

router(config-if)#

```
ip split-horizon
```

- Enables split horizon.

router(config-router)#

```
[no] passive interface
```

- Enables and disables the sending of routing updates on a specified interface.

router(config-router)#

```
network network-number [mask network-mask]
```

- Specifies a list of networks for a routing process.

CIT 5.1—4-10

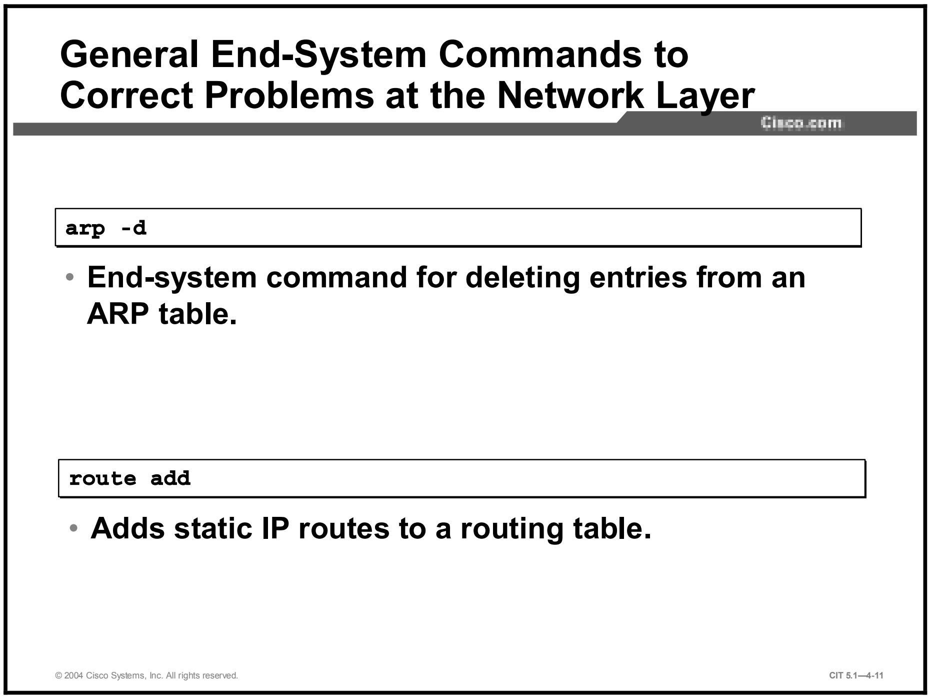
Troubleshooters can use the Cisco commands listed in the table to make configuration changes to correct problems with IP routing that occur at the network layer.

Cisco Commands for Correcting IP Routing Problems

Command	Description
ip route *prefix mask address* [**distance**]	Configures a static route.
ip route 0.0.0.0 0.0.0.0 {*ip-address* | *interface-type number*} [**distance**]	Configures a default route.
ip route-cache	Enables the use of high-speed switching caches.
ip split-horizon	Enables split horizon.
[**no**] **passive-interface**	Enables and disables the sending of routing updates on a specified interface.
network network-number [**mask** *network-mask*]	Specifies a list of networks for a routing process.

Identifying End-System Commands and Applications Used to Correct Problems Occurring at the Network Layer

This topic identifies commands and applications applied at the end system that troubleshooters use to correct problems at the network layer.



General End-System Commands to Correct Problems at the Network Layer

```
arp -d
```

- End-system command for deleting entries from an ARP table.

```
route add
```

- Adds static IP routes to a routing table.

CIT 5.1—4-11

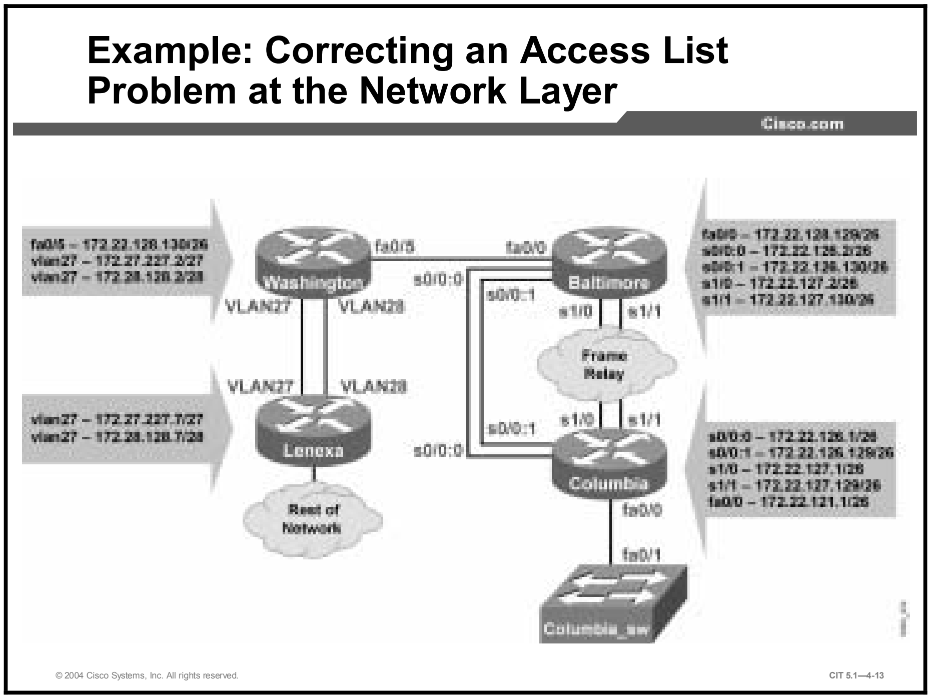
Troubleshooters can use the end-system commands listed in the table to make configuration changes to correct problems at the network layer.

End-System Commands to Correct Problems at the Network Layer

Command	Description
`arp -d`	Deletes entries from an ARP table. This command can be wildcarded with an asterisk (*) to delete all ARP entries.
`route add`	Adds static IP routes to a routing table.
`ipconfig`	Releases and renews IP address leases on hosts running Windows NT, 2000, or XP.
`winipcfg`	Releases and renews IP address leases on hosts running Windows 98 and Me.
`ifconfig`	Configures IP information on hosts running Mac OS X and UNIX.

Example: Correcting an Access List Problem at the Network Layer

You are the second-level network engineer for sites in Washington, Baltimore, and Columbia. The devices are named after the city names. You have console access to the router named Washington, and, through it, IP connectivity to all devices in your network. Your span of network responsibility in the corporation includes the 172.22.0.0/16 subnet.



Example: Correcting an Access List Problem at the Network Layer

Cisco.com

fa0/5 – 172.22.128.130/26
vlan27 – 172.27.227.2/27
vlan27 – 172.28.128.2/28

vlan27 – 172.27.227.7/27
vlan27 – 172.28.128.7/28

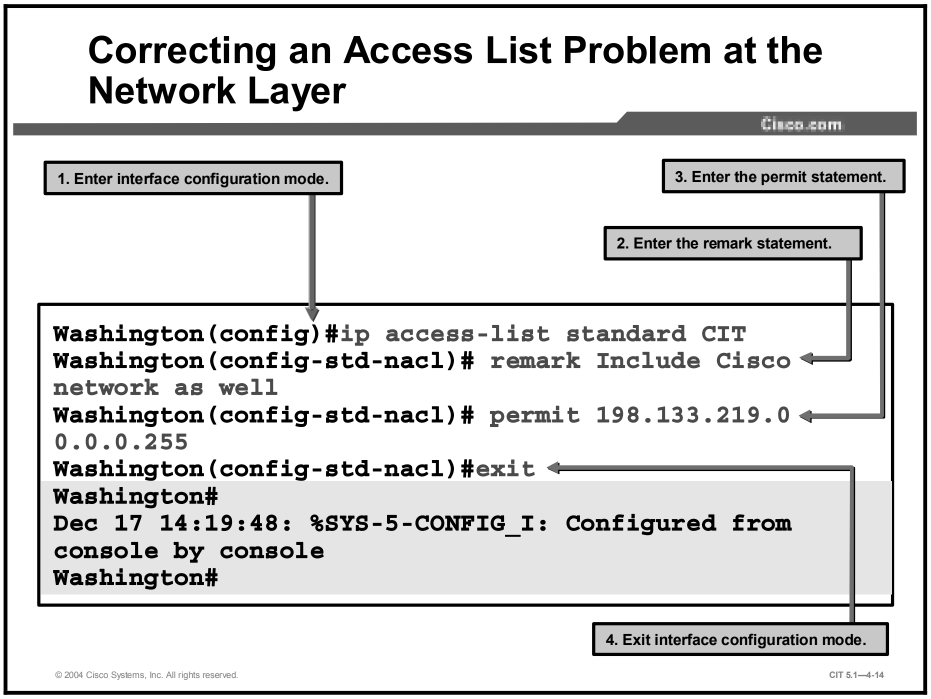
fa0/0 – 172.22.128.129/26
s0/0:0 – 172.22.126.2/26
s0/0:1 – 172.22.126.130/26
s1/0 – 172.22.127.2/26
s1/1 – 172.22.127.130/26

s0/0:0 – 172.22.126.1/26
s0/0:1 – 172.22.126.129/26
s1/0 – 172.22.127.1/26
s1/1 – 172.22.127.129/26
fa0/0 – 172.22.121.1/26

CIT 5.1—4-13

You have determined that route 198.133.219.0/24 for Cisco Systems, which is supposed to be in the table for all devices, is not in the routing tables for any of your devices. You know from reviewing the access lists on Washington that Cisco Systems network 198.133.219.0/24 is not permitted by the distribution list in effect with your BGP neighbors.

To correct the problem, you need to expand the access list to permit route 198.133.219.0/24. You go into configuration mode and update the access list.



Correcting an Access List Problem at the Network Layer

1. Enter interface configuration mode.

2. Enter the remark statement.

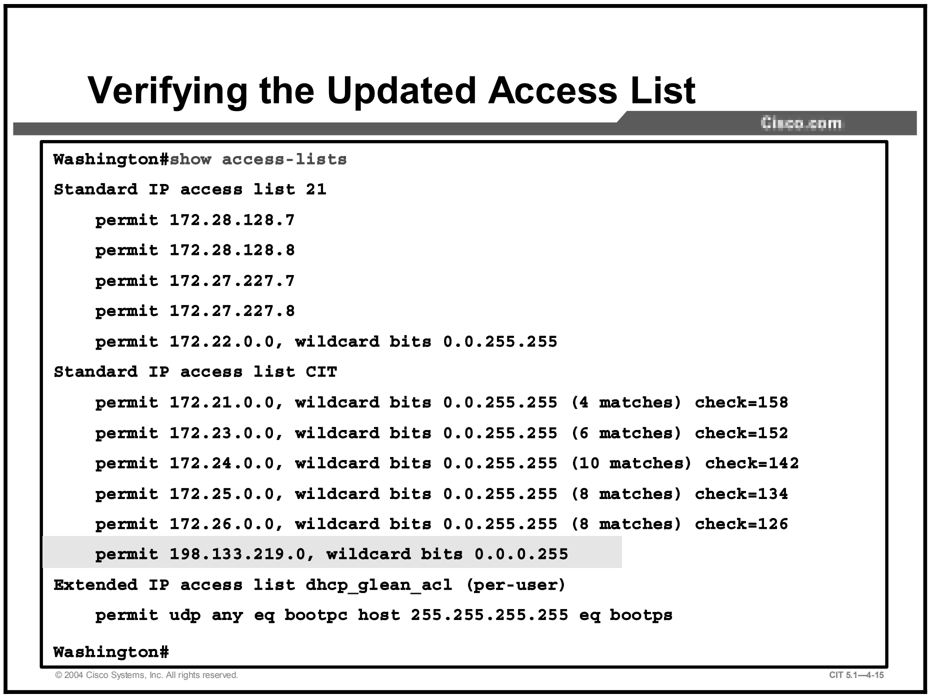
3. Enter the permit statement.

4. Exit interface configuration mode.

```
Washington(config)#ip access-list standard CIT
Washington(config-std-nacl)# remark Include Cisco
network as well
Washington(config-std-nacl)# permit 198.133.219.0
0.0.0.255
Washington(config-std-nacl)#exit
Washington#
Dec 17 14:19:48: %SYS-5-CONFIG_I: Configured from
console by console
Washington#
```

© 2004 Cisco Systems, Inc. All rights reserved. CIT 5.1—4-14

You then verify that the access list was updated.

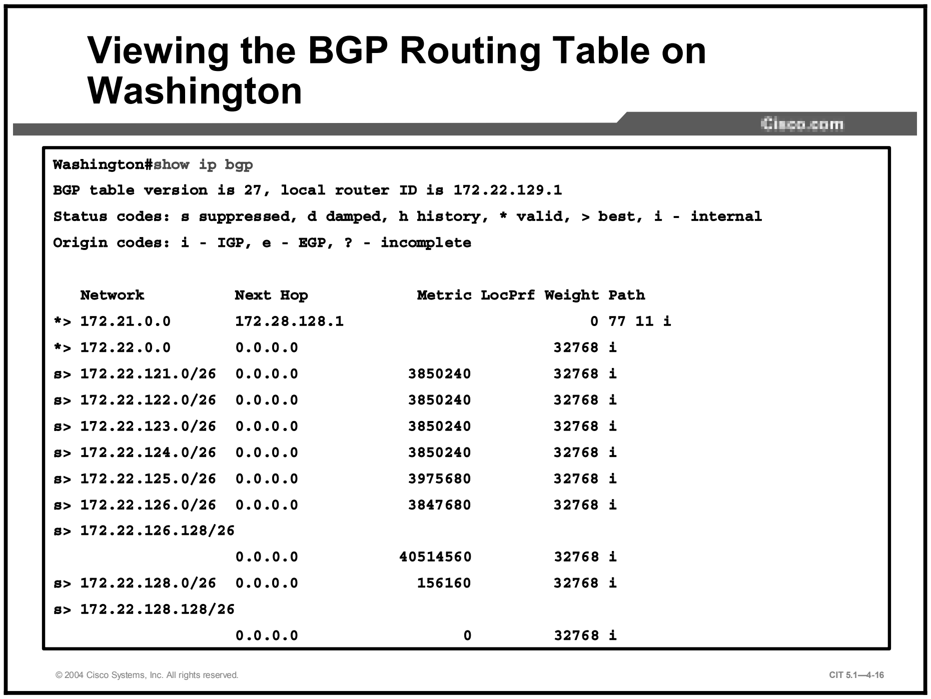


Verifying the Updated Access List

```
Washington#show access-lists
Standard IP access list 21
    permit 172.28.128.7
    permit 172.28.128.8
    permit 172.27.227.7
    permit 172.27.227.8
    permit 172.22.0.0, wildcard bits 0.0.255.255
Standard IP access list CIT
    permit 172.21.0.0, wildcard bits 0.0.255.255 (4 matches) check=158
    permit 172.23.0.0, wildcard bits 0.0.255.255 (6 matches) check=152
    permit 172.24.0.0, wildcard bits 0.0.255.255 (10 matches) check=142
    permit 172.25.0.0, wildcard bits 0.0.255.255 (8 matches) check=134
    permit 172.26.0.0, wildcard bits 0.0.255.255 (8 matches) check=126
    permit 198.133.219.0, wildcard bits 0.0.0.255
Extended IP access list dhcp_glean_acl (per-user)
    permit udp any eq bootpc host 255.255.255.255 eq bootps
Washington#
```

© 2004 Cisco Systems, Inc. All rights reserved. CIT 5.1—4-15

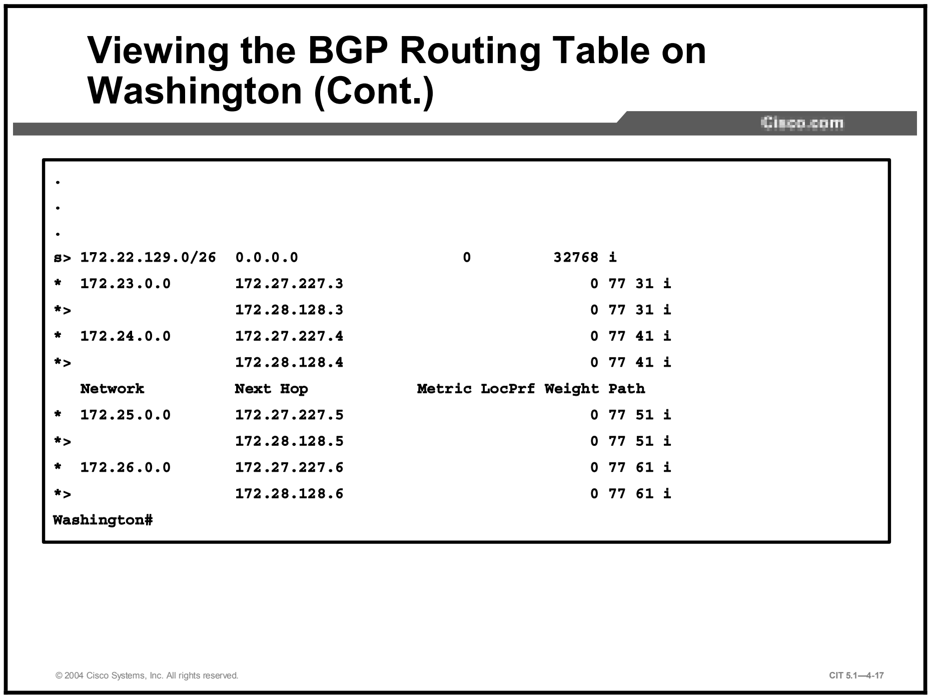
You now check to see if the Cisco Systems route is in the BGP table on Washington.



Viewing the BGP Routing Table on Washington

```
Washington#show ip bgp
BGP table version is 27, local router ID is 172.22.129.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 172.21.0.0       172.28.128.1                             0 77 11 i
*> 172.22.0.0       0.0.0.0                              32768 i
s> 172.22.121.0/26  0.0.0.0            3850240           32768 i
s> 172.22.122.0/26  0.0.0.0            3850240           32768 i
s> 172.22.123.0/26  0.0.0.0            3850240           32768 i
s> 172.22.124.0/26  0.0.0.0            3850240           32768 i
s> 172.22.125.0/26  0.0.0.0            3975680           32768 i
s> 172.22.126.0/26  0.0.0.0            3847680           32768 i
s> 172.22.126.128/26
                    0.0.0.0           40514560           32768 i
s> 172.22.128.0/26  0.0.0.0             156160           32768 i
s> 172.22.128.128/26
                    0.0.0.0                  0           32768 i
```

© 2004 Cisco Systems, Inc. All rights reserved. CIT 5.1—4-16



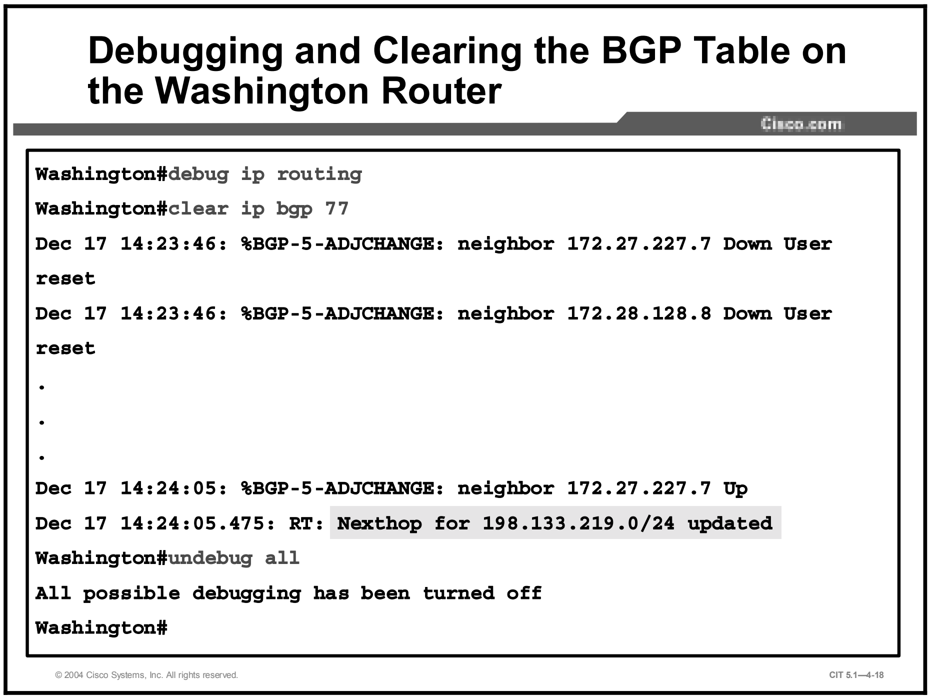
Viewing the BGP Routing Table on Washington (Cont.)

```
.
.
.
s> 172.22.129.0/26  0.0.0.0                  0           32768 i
*  172.23.0.0       172.27.227.3                             0 77 31 i
*>                  172.28.128.3                             0 77 31 i
*  172.24.0.0       172.27.227.4                             0 77 41 i
*>                  172.28.128.4                             0 77 41 i
   Network          Next Hop            Metric LocPrf Weight Path
*  172.25.0.0       172.27.227.5                             0 77 51 i
*>                  172.28.128.5                             0 77 51 i
*  172.26.0.0       172.27.227.6                             0 77 61 i
*>                  172.28.128.6                             0 77 61 i
Washington#
```

© 2004 Cisco Systems, Inc. All rights reserved. CIT 5.1—4-17

The network 198.133.219.0/24 is not yet present. You need to clear a BGP session when you change the inbound or outbound policy for the session. Changing the inbound access list will change the inbound policy for a BGP session.

You use the **debug ip routing** command to watch for routing updates and then clear the BGP session with the corporate core neighbors in AS 77.



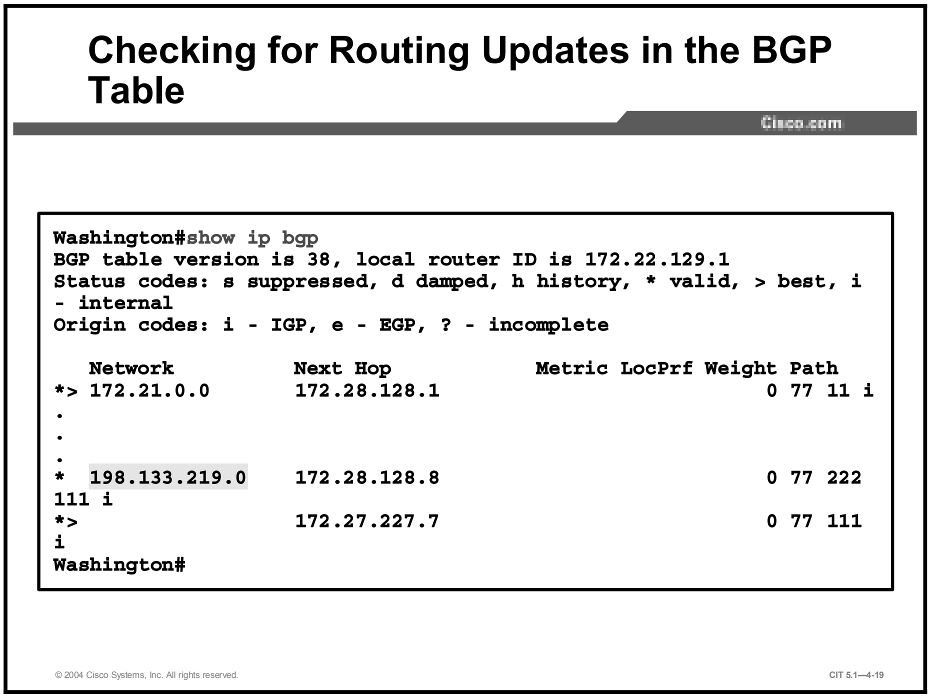
Debugging and Clearing the BGP Table on the Washington Router

```
Washington#debug ip routing
Washington#clear ip bgp 77
Dec 17 14:23:46: %BGP-5-ADJCHANGE: neighbor 172.27.227.7 Down User
reset
Dec 17 14:23:46: %BGP-5-ADJCHANGE: neighbor 172.28.128.8 Down User
reset
.
.
.
Dec 17 14:24:05: %BGP-5-ADJCHANGE: neighbor 172.27.227.7 Up
Dec 17 14:24:05.475: RT: Nexthop for 198.133.219.0/24 updated
Washington#undebug all
All possible debugging has been turned off
Washington#
```

CIT 5.1—4-18

You know that the 198.133.219.0/24 route has been added when you see the following line: "RT: Nexthop for 198.133.219.0/24 updated".

Now you verify that the Cisco Systems route is in the BGP table on Washington.



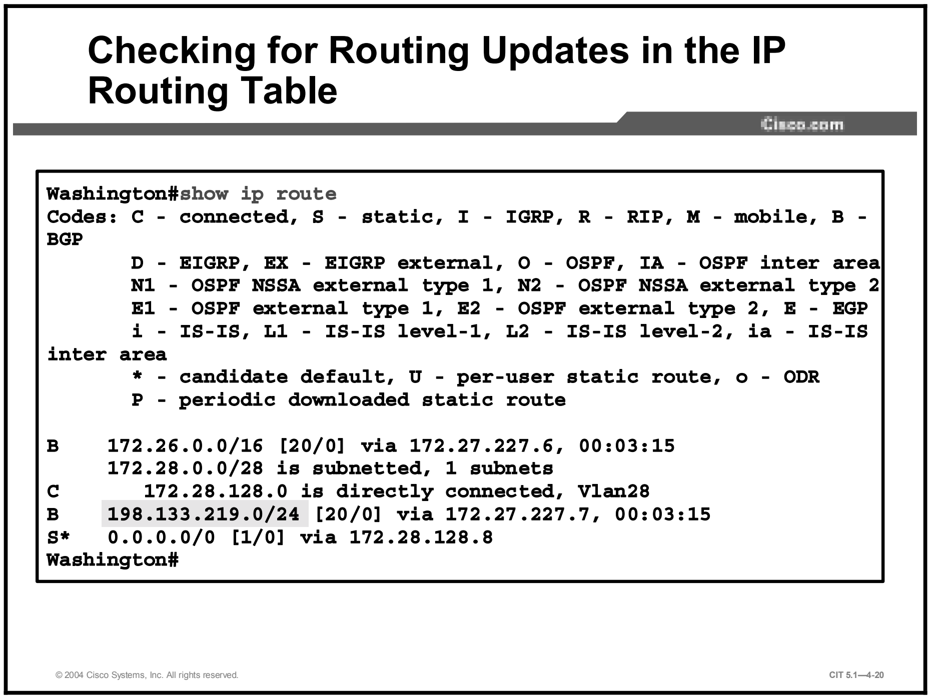
Checking for Routing Updates in the BGP Table

```
Washington#show ip bgp
BGP table version is 38, local router ID is 172.22.129.1
Status codes: s suppressed, d damped, h history, * valid, > best, i
- internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 172.21.0.0       172.28.128.1                           0 77 11 i
.
.
.
*  198.133.219.0    172.28.128.8                           0 77 222
111 i
*>                  172.27.227.7                           0 77 111
i
Washington#
```

CIT 5.1—4-19

The table has been updated and the Cisco Systems address is displayed.

You verify that the Cisco Systems address is also in the IP routing table by entering the **show ip route** command.



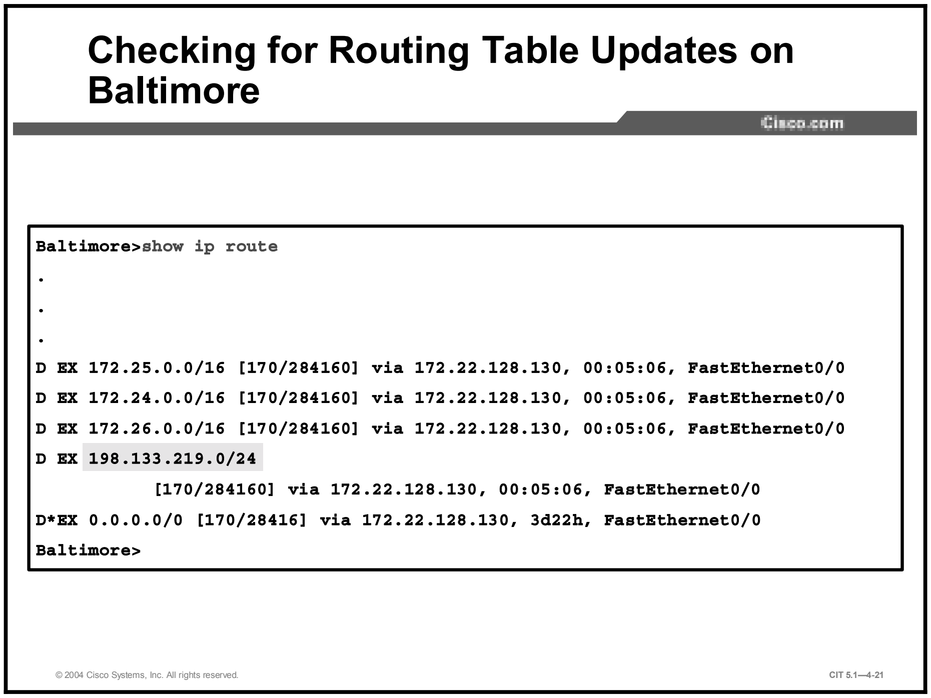
Checking for Routing Updates in the IP Routing Table

```
Washington#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B -
BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

B    172.26.0.0/16 [20/0] via 172.27.227.6, 00:03:15
     172.28.0.0/28 is subnetted, 1 subnets
C       172.28.128.0 is directly connected, Vlan28
B    198.133.219.0/24 [20/0] via 172.27.227.7, 00:03:15
S*   0.0.0.0/0 [1/0] via 172.28.128.8
Washington#
```

CIT 5.1—4-20

The 198.133.219.0/24 route is now present in the routing table on Washington.

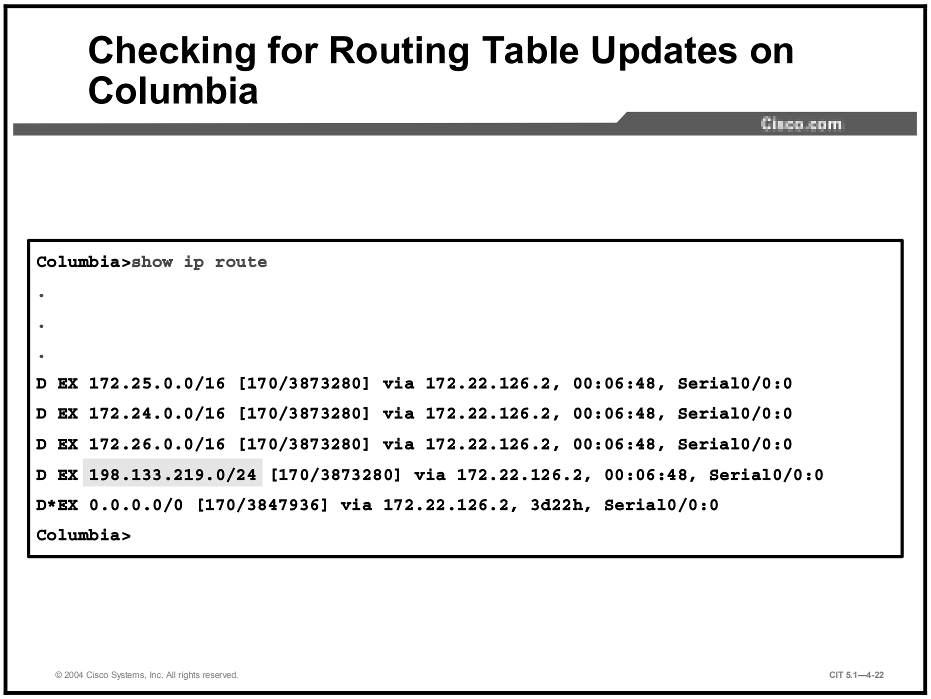
As a final validation that the network layer issue has been resolved, you use the **show ip route command** on Baltimore and Columbia to verify that those routers also see the 198.133.219.0/24 route.



Checking for Routing Table Updates on Baltimore

```
Baltimore>show ip route
.
.
.
D EX 172.25.0.0/16 [170/284160] via 172.22.128.130, 00:05:06, FastEthernet0/0
D EX 172.24.0.0/16 [170/284160] via 172.22.128.130, 00:05:06, FastEthernet0/0
D EX 172.26.0.0/16 [170/284160] via 172.22.128.130, 00:05:06, FastEthernet0/0
D EX 198.133.219.0/24
          [170/284160] via 172.22.128.130, 00:05:06, FastEthernet0/0
D*EX 0.0.0.0/0 [170/28416] via 172.22.128.130, 3d22h, FastEthernet0/0
Baltimore>
```

CIT 5.1—4-21



Checking for Routing Table Updates on Columbia

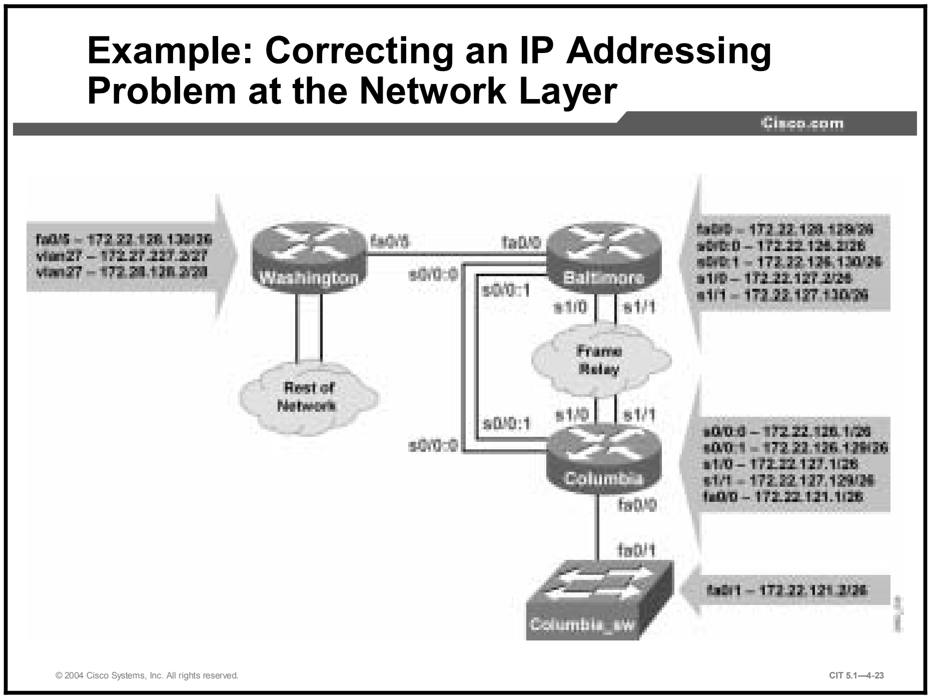
```
Columbia>show ip route
.
.
.
D EX 172.25.0.0/16 [170/3873280] via 172.22.126.2, 00:06:48, Serial0/0:0
D EX 172.24.0.0/16 [170/3873280] via 172.22.126.2, 00:06:48, Serial0/0:0
D EX 172.26.0.0/16 [170/3873280] via 172.22.126.2, 00:06:48, Serial0/0:0
D EX 198.133.219.0/24 [170/3873280] via 172.22.126.2, 00:06:48, Serial0/0:0
D*EX 0.0.0.0/0 [170/3847936] via 172.22.126.2, 3d22h, Serial0/0:0
Columbia>
```

CIT 5.1—4-22

The Cisco Systems route has been restored to all of your devices. You have resolved the network layer issue and restored your baseline configuration.

Example: Correcting an IP Addressing Problem at the Network Layer

You are the second-level network engineer for a division with locations in Washington, Baltimore, and Columbia. The networking devices at each location are named after the names of the city in which they reside. You have console access to the router named Washington, which gives you IP connectivity to all devices in your network. Your span of responsibility in the corporate network includes the 172.22.0.0/16 subnet.



Example: Correcting an IP Addressing Problem at the Network Layer

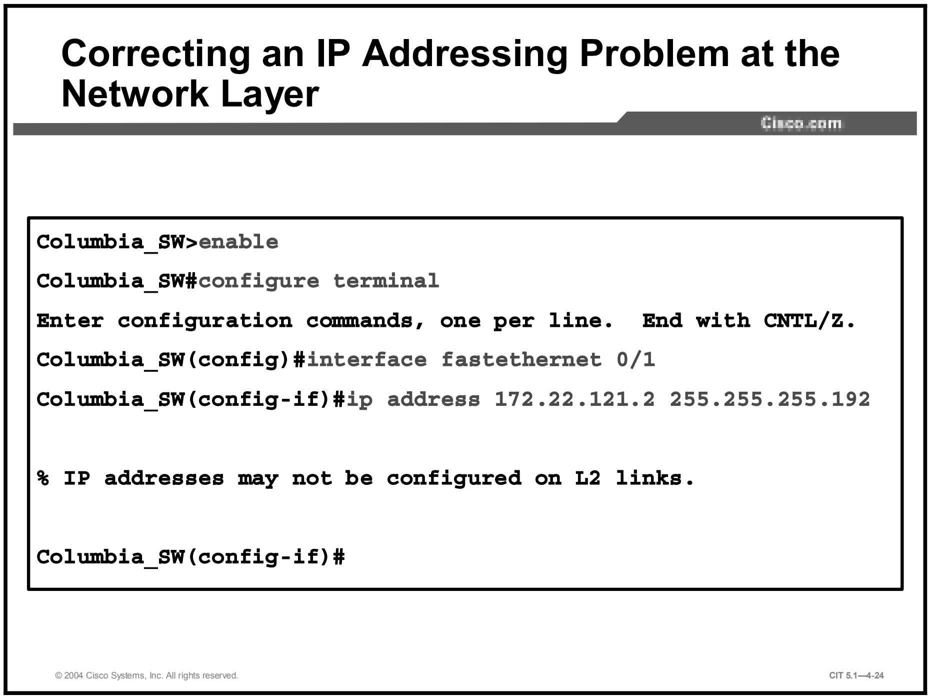
© 2004 Cisco Systems, Inc. All rights reserved.

CIT 5.1—4-23

One day, Network Operations calls to report that it cannot ping the switch named Columbia_SW. Network Operations does not recall changing any of the configurations and cannot ping Columbia_SW from Washington, either.

You have determined that there is a duplicate IP address 172.22.121.1 on the Fast Ethernet between Columbia and Columbia_SW. You know from the baseline that Columbia should have IP address 172.22.121.1/26 on Fast Ethernet 0/0.1 and that Columbia_SW should use IP address 172.22.121.2/26.

To correct the problem, Network Operations needs to modify the IP address on Columbia_SW. As a good practice, Network Operations should also restore console logging. Network Operations goes into configuration mode and tries to update the IP address on Fast Ethernet 0/1 on Columbia_SW.



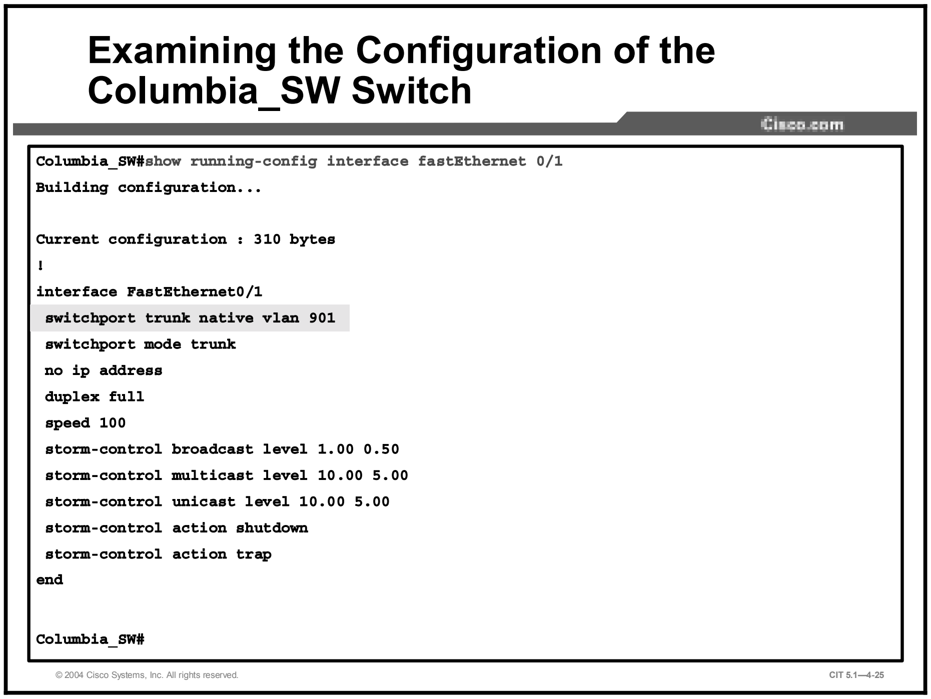
Correcting an IP Addressing Problem at the Network Layer

```
Columbia_SW>enable
Columbia_SW#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Columbia_SW(config)#interface fastethernet 0/1
Columbia_SW(config-if)#ip address 172.22.121.2 255.255.255.192

% IP addresses may not be configured on L2 links.

Columbia_SW(config-if)#
```

CIT 5.1—4-24

Network Operations calls you back, stating that the IP address on Fast Ethernet 0/1 cannot be configured because it is a switched interface.

You agree and ask Network Operations to enter the **show running-config interface FastEthernet 0/1** command from the privileged EXEC mode. After Network Operations does this, you ask your contact there to look for the native VLAN for the 2950 switch.



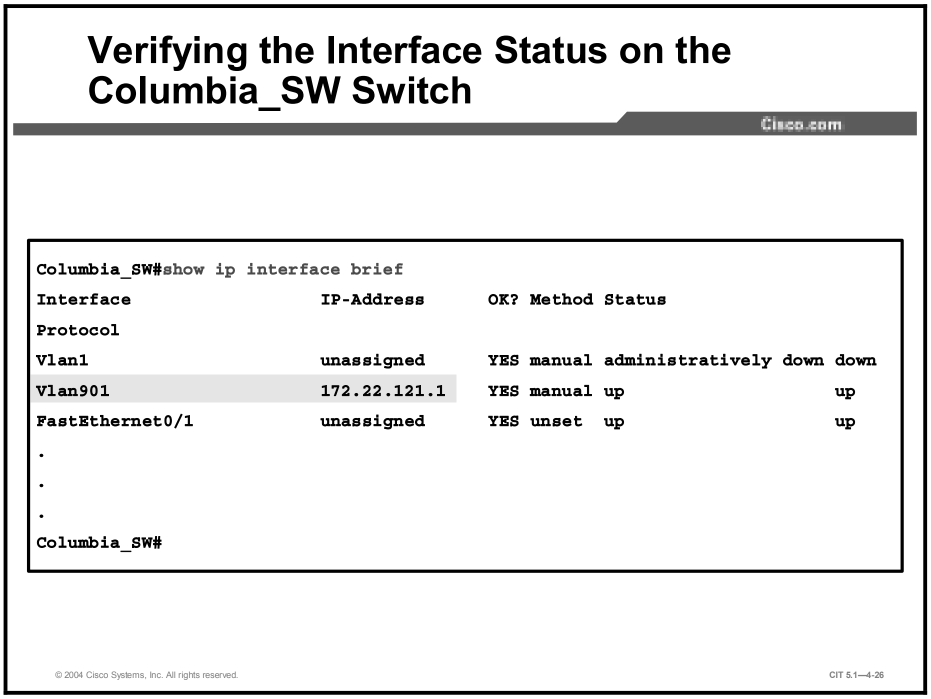
Examining the Configuration of the Columbia_SW Switch

```
Columbia_SW#show running-config interface fastEthernet 0/1
Building configuration...

Current configuration : 310 bytes
!
interface FastEthernet0/1
 switchport trunk native vlan 901
 switchport mode trunk
 no ip address
 duplex full
 speed 100
 storm-control broadcast level 1.00 0.50
 storm-control multicast level 10.00 5.00
 storm-control unicast level 10.00 5.00
 storm-control action shutdown
 storm-control action trap
end


Columbia_SW#
```

CIT 5.1—4-25

The native VLAN is VLAN901.

You ask Network Operations to enter the **show ip interface brief** command to confirm that this interface is active.

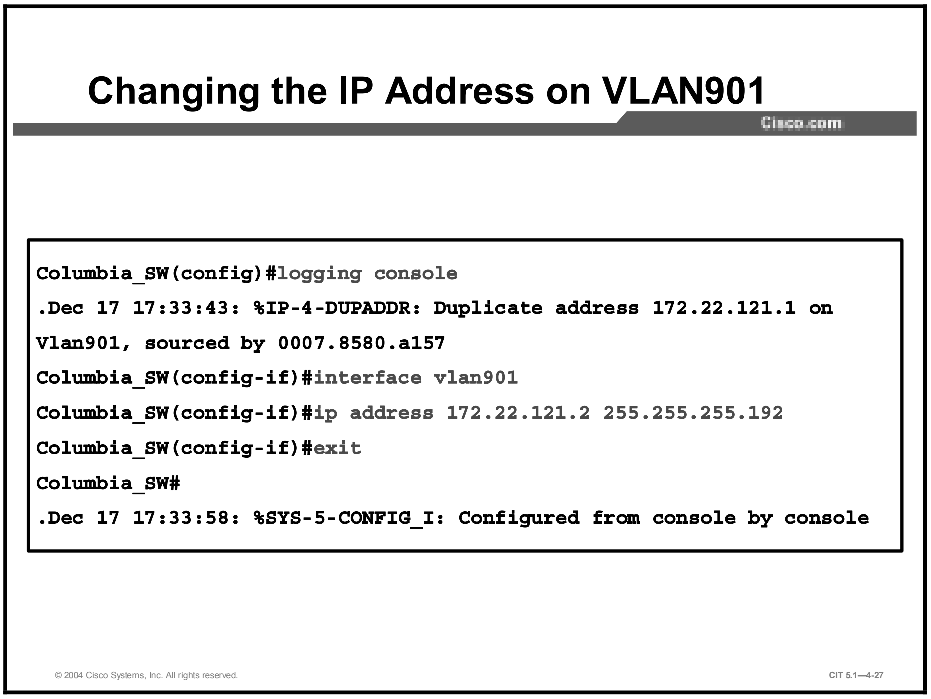


Verifying the Interface Status on the Columbia_SW Switch

```
Columbia_SW#show ip interface brief
Interface                 IP-Address      OK? Method Status
Protocol
Vlan1                     unassigned      YES manual administratively down down
Vlan901                   172.22.121.1    YES manual up                    up
FastEthernet0/1           unassigned      YES unset  up                    up
.
.
.
Columbia_SW#
```

© 2004 Cisco Systems, Inc. All rights reserved. CIT 5.1—4-26

Interface VLAN901 is active, so you direct Network Operations to change the IP address on the VLAN901 interface.

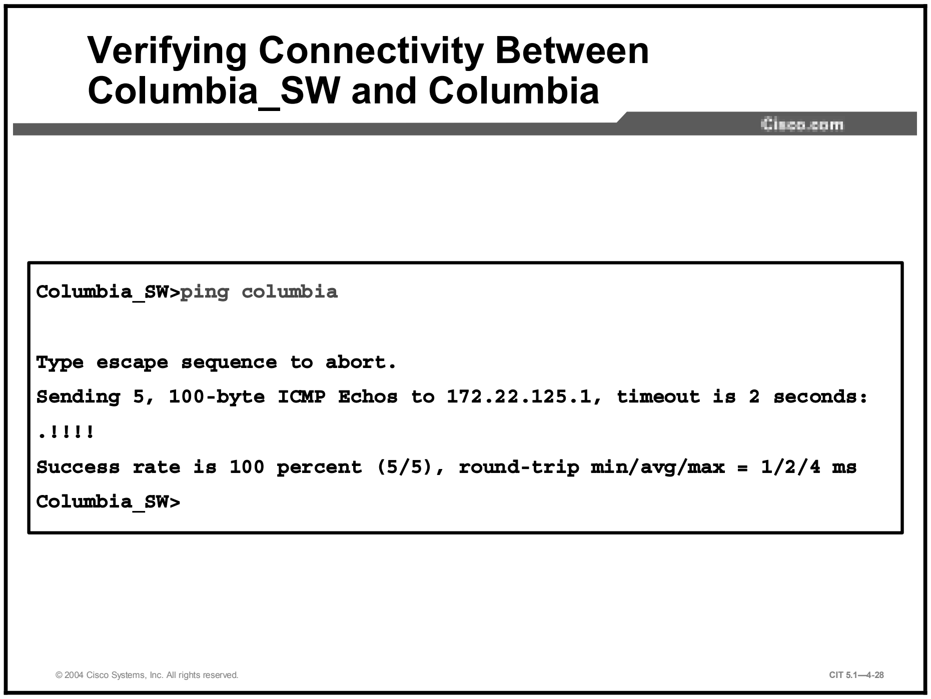


Changing the IP Address on VLAN901

```
Columbia_SW(config)#logging console
.Dec 17 17:33:43: %IP-4-DUPADDR: Duplicate address 172.22.121.1 on
Vlan901, sourced by 0007.8580.a157
Columbia_SW(config-if)#interface vlan901
Columbia_SW(config-if)#ip address 172.22.121.2 255.255.255.192
Columbia_SW(config-if)#exit
Columbia_SW#
.Dec 17 17:33:58: %SYS-5-CONFIG_I: Configured from console by console
```

© 2004 Cisco Systems, Inc. All rights reserved. CIT 5.1—4-27

To test that the new configuration will work, Network Operations verifies that Columbia_SW can reach Columbia.

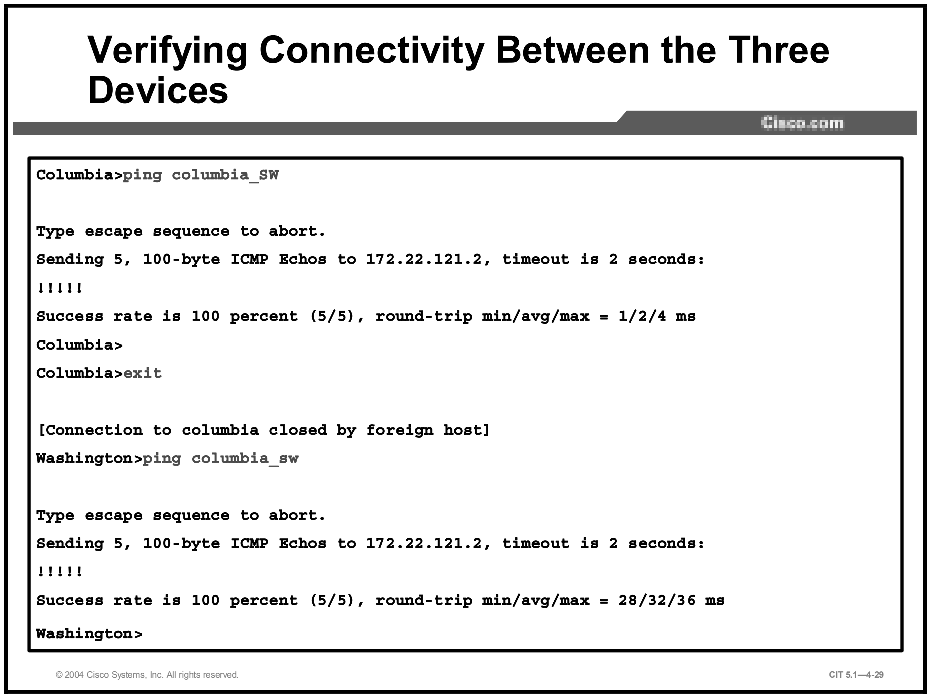


Verifying Connectivity Between Columbia_SW and Columbia

```
Columbia_SW>ping columbia

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.22.125.1, timeout is 2 seconds:
.!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
Columbia_SW>
```

CIT 5.1—4-28

You then verify that Columbia and Washington can reach Columbia_SW.



Verifying Connectivity Between the Three Devices

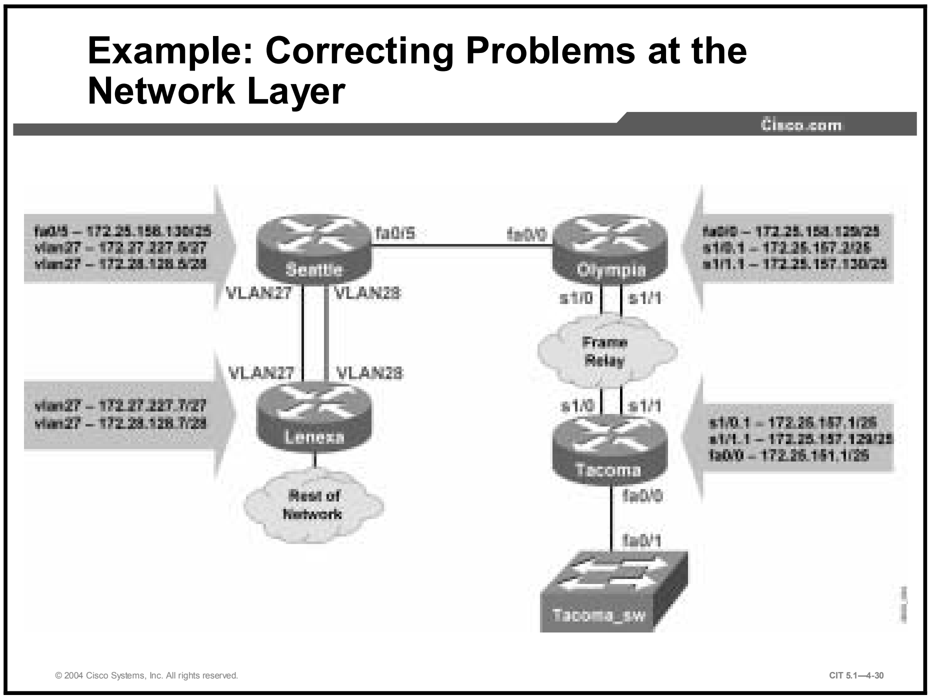
```
Columbia>ping columbia_SW

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.22.121.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
Columbia>
Columbia>exit

[Connection to columbia closed by foreign host]
Washington>ping columbia_sw

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.22.121.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/32/36 ms
Washington>
```

CIT 5.1—4-29

The duplicate IP address has been replaced with the proper IP address. You have resolved the network layer issue and restored your baseline configuration.

Example: Correcting Problems at the Network Layer

You are the second-level network engineer for a division with locations in Seattle, Olympia, and Tacoma. The networking devices at each location are named after the names of the city in which they reside. You have console access to the router named Seattle, which gives you IP connectivity to all devices in your network. Your span of responsibility in the corporate network includes the 172.25.0.0/16 subnet.



Example: Correcting Problems at the Network Layer

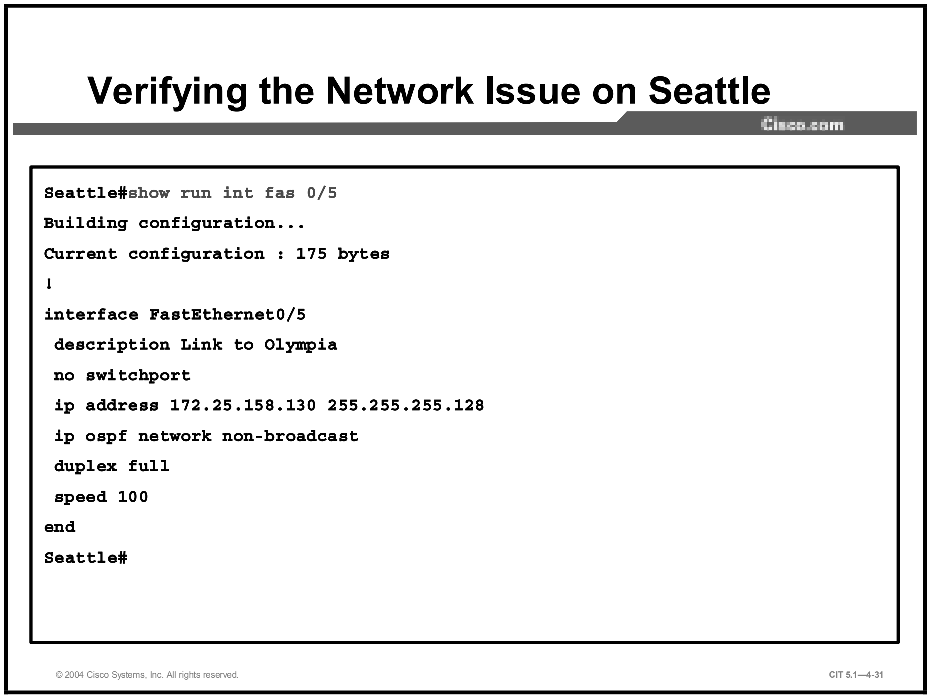
Cisco.com

© 2004 Cisco Systems, Inc. All rights reserved.

CIT 5.1—4-30

You previously determined that there was an issue forming OSPF neighbor adjacencies between Seattle and Olympia.

You can verify the issue by looking at the interface configuration.

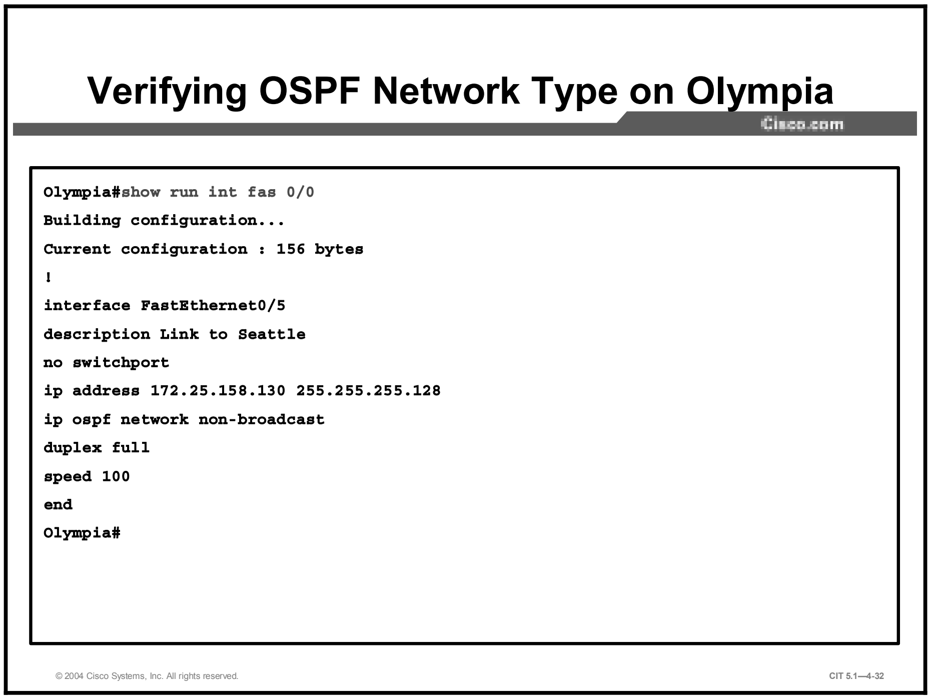


Verifying the Network Issue on Seattle

```
Seattle#show run int fas 0/5
Building configuration...
Current configuration : 175 bytes
!
interface FastEthernet0/5
 description Link to Olympia
 no switchport
 ip address 172.25.158.130 255.255.255.128
 ip ospf network non-broadcast
 duplex full
 speed 100
end
Seattle#
```

© 2004 Cisco Systems, Inc. All rights reserved. CIT 5.1—4-31

You should also verify the OSPF network type on Olympia.



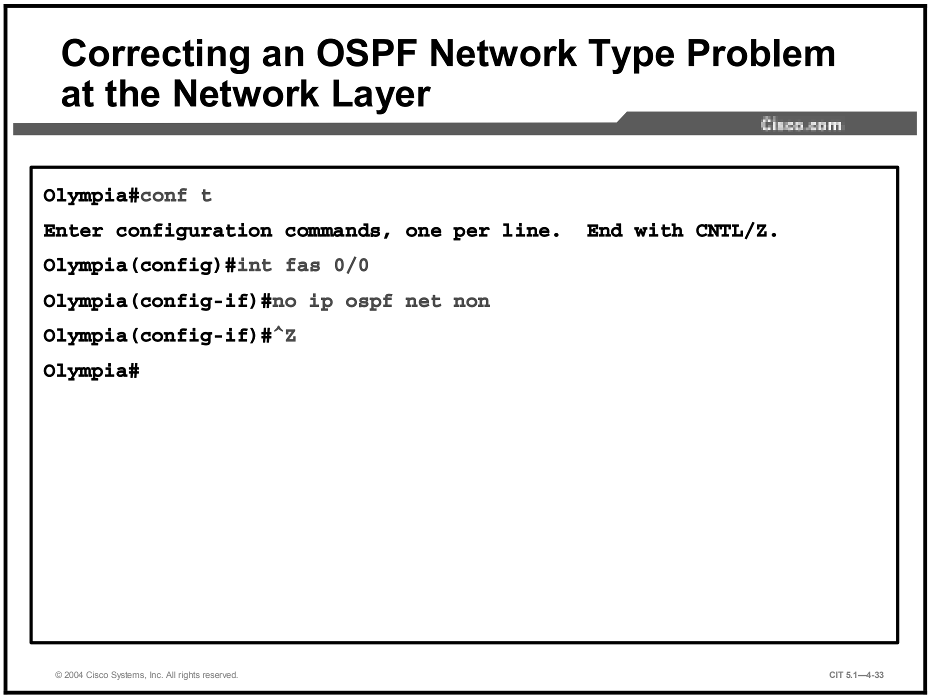
Verifying OSPF Network Type on Olympia

```
Olympia#show run int fas 0/0
Building configuration...
Current configuration : 156 bytes
!
interface FastEthernet0/5
description Link to Seattle
no switchport
ip address 172.25.158.130 255.255.255.128
ip ospf network non-broadcast
duplex full
speed 100
end
Olympia#
```

© 2004 Cisco Systems, Inc. All rights reserved. CIT 5.1—4-32

You should notice that an OSPF network type of “non-broadcast” has been configured on both interfaces. If the Ethernet default OSPF network type of “broadcast” was in place, the OSPF adjacencies should occur.

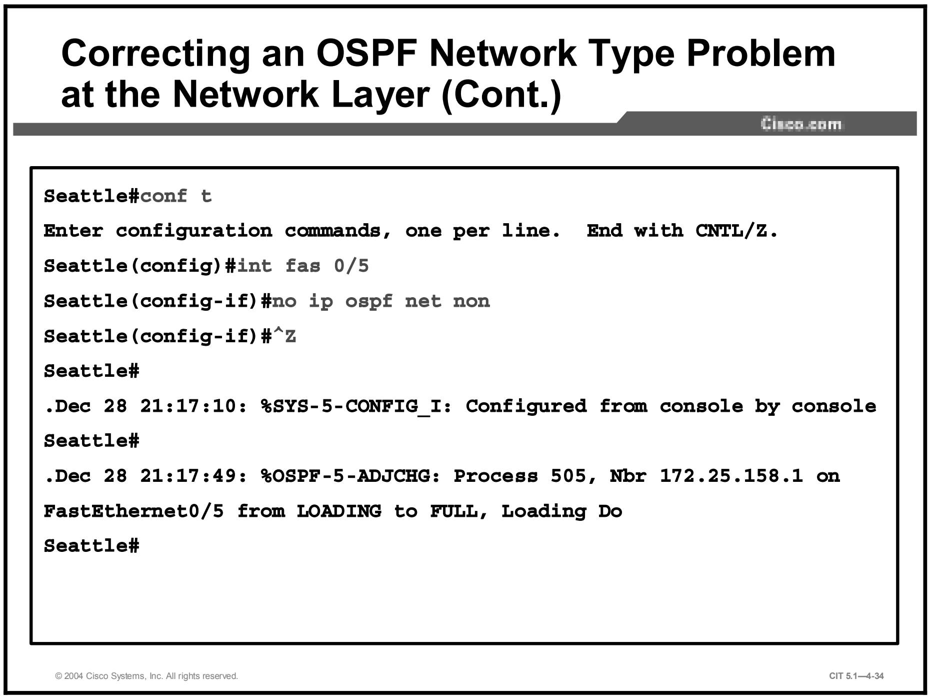
You quickly resolve the issue.



Correcting an OSPF Network Type Problem at the Network Layer

```
Olympia#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Olympia(config)#int fas 0/0
Olympia(config-if)#no ip ospf net non
Olympia(config-if)#^Z
Olympia#
```

CIT 5.1—4-33



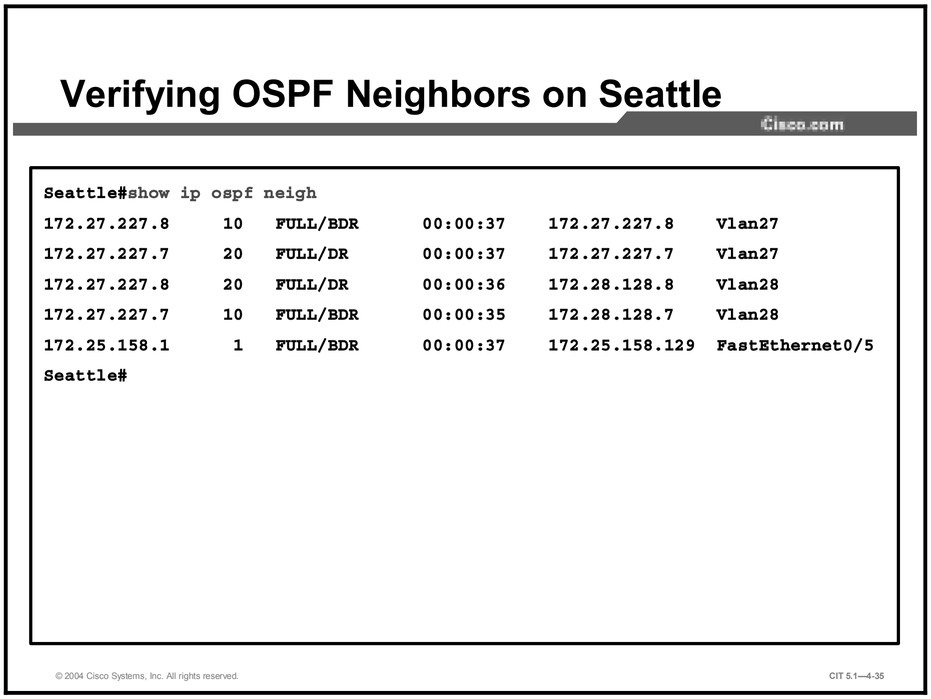
Correcting an OSPF Network Type Problem at the Network Layer (Cont.)

```
Seattle#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Seattle(config)#int fas 0/5
Seattle(config-if)#no ip ospf net non
Seattle(config-if)#^Z
Seattle#
.Dec 28 21:17:10: %SYS-5-CONFIG_I: Configured from console by console
Seattle#
.Dec 28 21:17:49: %OSPF-5-ADJCHG: Process 505, Nbr 172.25.158.1 on
FastEthernet0/5 from LOADING to FULL, Loading Do
Seattle#
```

CIT 5.1—4-34

The OSPF adjacency message on the console indicates that the neighbor adjacencies have been established.

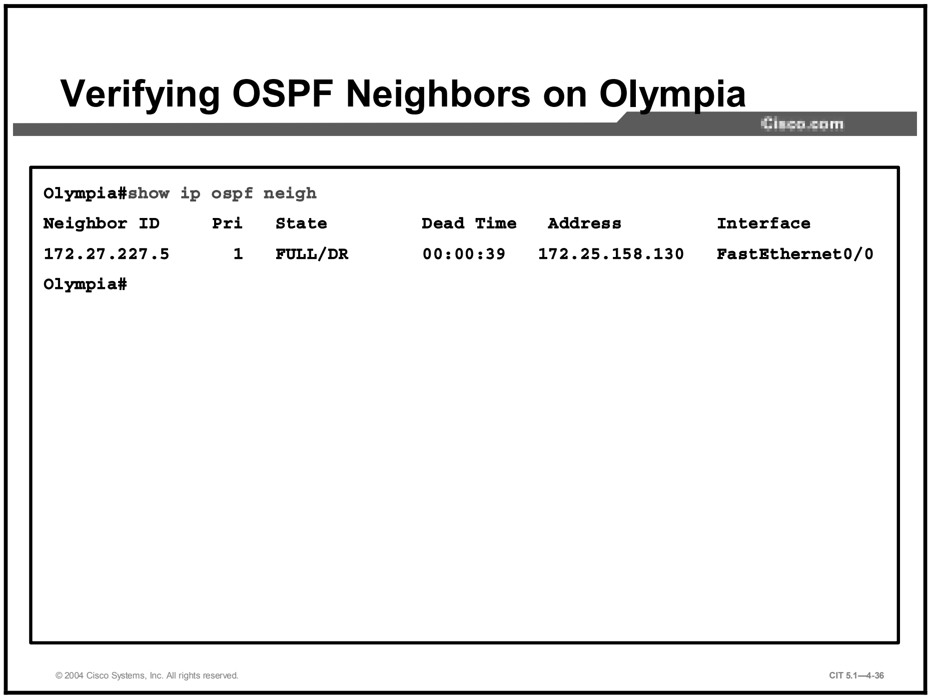
You verify the OSPF neighbors in the network.



Verifying OSPF Neighbors on Seattle

```
Seattle#show ip ospf neigh
172.27.227.8     10   FULL/BDR      00:00:37    172.27.227.8     Vlan27
172.27.227.7     20   FULL/DR       00:00:37    172.27.227.7     Vlan27
172.27.227.8     20   FULL/DR       00:00:36    172.28.128.8     Vlan28
172.27.227.7     10   FULL/BDR      00:00:35    172.28.128.7     Vlan28
172.25.158.1      1   FULL/BDR      00:00:37    172.25.158.129   FastEthernet0/5
Seattle#
```

CIT 5.1—4-35



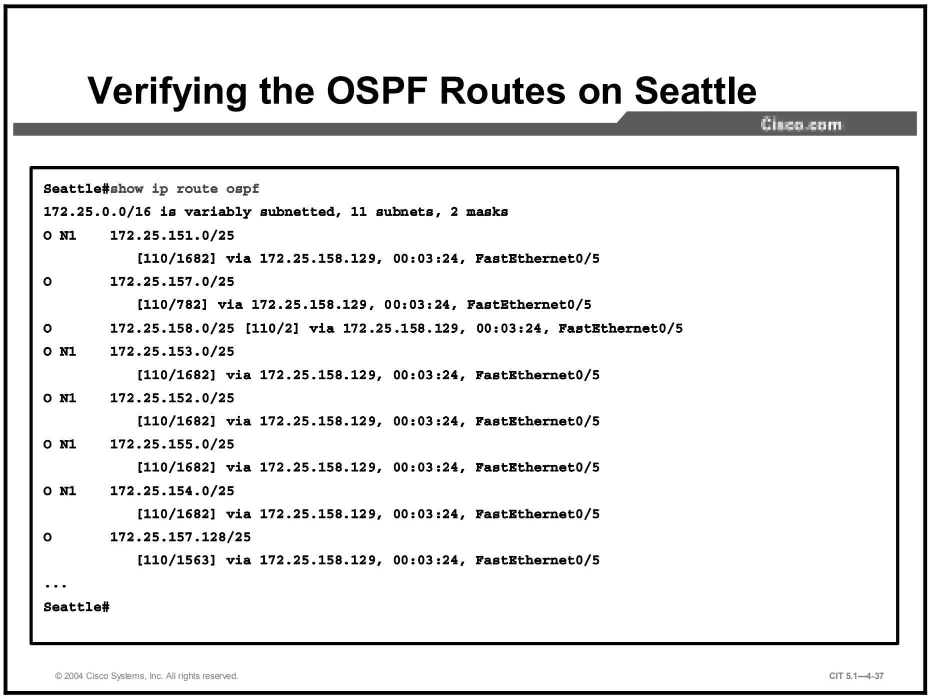
Verifying OSPF Neighbors on Olympia

```
Olympia#show ip ospf neigh
Neighbor ID     Pri   State         Dead Time   Address         Interface
172.27.227.5      1   FULL/DR       00:00:39   172.25.158.130   FastEthernet0/0
Olympia#
```

CIT 5.1—4-36

The OSPF adjacencies are established between Seattle and Olympia.

Finally, you can verify that OSPF routes are being exchanged between Seattle and Olympia.



Verifying the OSPF Routes on Seattle

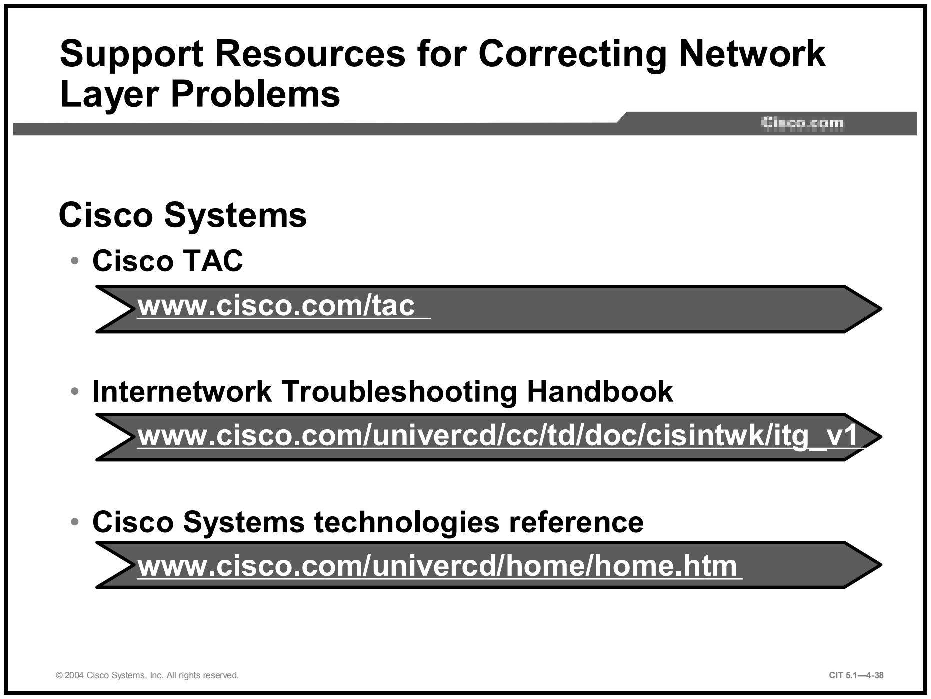
```
Seattle#show ip route ospf
172.25.0.0/16 is variably subnetted, 11 subnets, 2 masks
O N1    172.25.151.0/25
           [110/1682] via 172.25.158.129, 00:03:24, FastEthernet0/5
O       172.25.157.0/25
           [110/782] via 172.25.158.129, 00:03:24, FastEthernet0/5
O       172.25.158.0/25 [110/2] via 172.25.158.129, 00:03:24, FastEthernet0/5
O N1    172.25.153.0/25
           [110/1682] via 172.25.158.129, 00:03:24, FastEthernet0/5
O N1    172.25.152.0/25
           [110/1682] via 172.25.158.129, 00:03:24, FastEthernet0/5
O N1    172.25.155.0/25
           [110/1682] via 172.25.158.129, 00:03:24, FastEthernet0/5
O N1    172.25.154.0/25
           [110/1682] via 172.25.158.129, 00:03:24, FastEthernet0/5
O       172.25.157.128/25
           [110/1563] via 172.25.158.129, 00:03:24, FastEthernet0/5
...
Seattle#
```

CIT 5.1—4-37

The problem has been resolved.

Identifying Network Layer Support Resources

This topic identifies support resources to assist troubleshooters in correcting problems at the network layer.



Support Resources for Correcting Network Layer Problems

Cisco Systems

- **Cisco TAC**
  - www.cisco.com/tac
- **Internetwork Troubleshooting Handbook**
  - www.cisco.com/univercd/cc/td/doc/cisintwk/itg_v1
- **Cisco Systems technologies reference**
  - www.cisco.com/univercd/home/home.htm

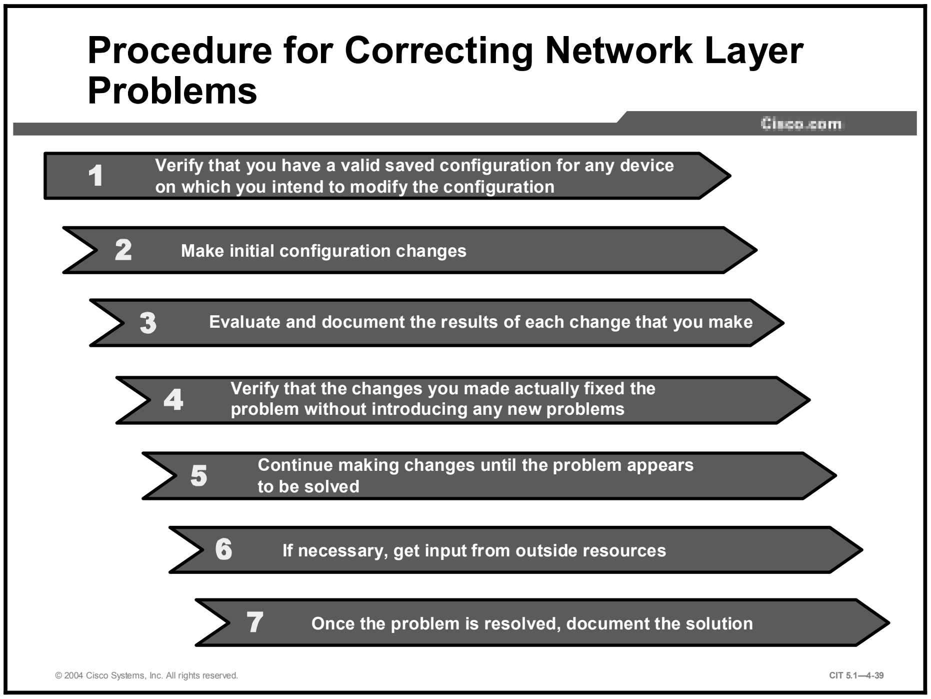
CIT 5.1—4-38

Despite your knowledge and experience about networking, there will still be times when you will need to consult an outside resource. These support resources are commonly used as reference materials for commands and configuration procedures and as research for technology-specific information and industry standards. Given the ability to use online support resources to do effective research, you save time that you may have otherwise spent on the phone with a support professional, and you save money that you would have committed to hiring a consultant.

For command and configuration references, go to the source. The Cisco Systems website has one of the largest collections of networking information on the Internet. Visit Cisco.com to use the Technical Assistance Center (TAC), Internetwork Troubleshooting Handbook, and technology reference pages to find information for troubleshooting Cisco Systems products. From these locations, you can search on a specific topic, such as access list, routing protocol, EIGRP, OSPF, or BGP. It is often helpful to narrow your search by including phrases such as “configuration examples” or “troubleshooting.”

Correcting Problems Occurring at the Network Layer

This topic identifies the steps to assist troubleshooters in correcting problems at the network layer.



Procedure for Correcting Network Layer Problems

1. Verify that you have a valid saved configuration for any device on which you intend to modify the configuration
2. Make initial configuration changes
3. Evaluate and document the results of each change that you make
4. Verify that the changes you made actually fixed the problem without introducing any new problems
5. Continue making changes until the problem appears to be solved
6. If necessary, get input from outside resources
7. Once the problem is resolved, document the solution

CIT 5.1—4-39

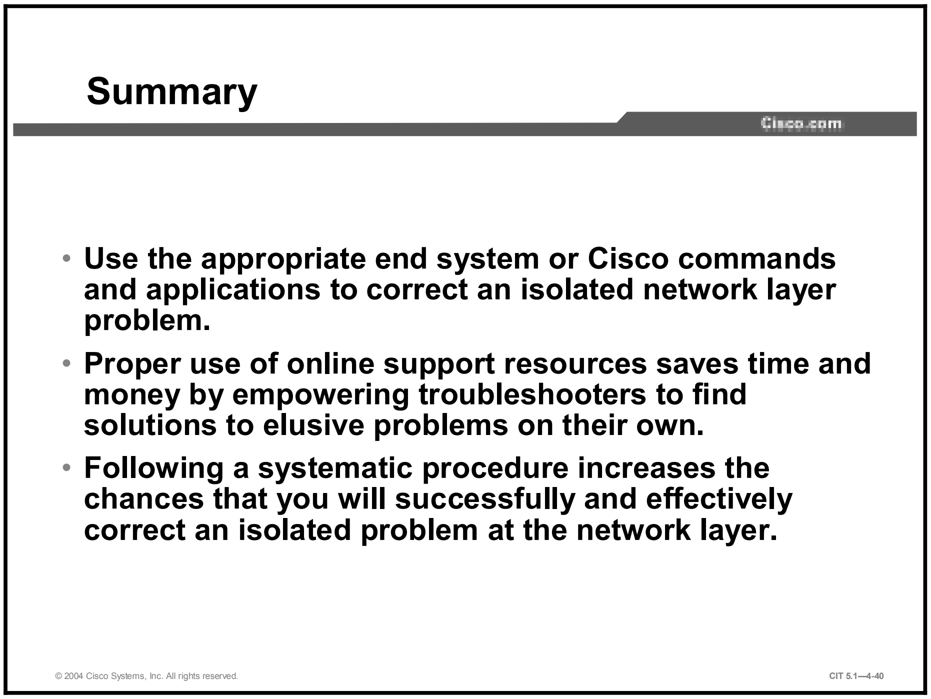
The table lists suggested steps for troubleshooters to correct isolated problems at the physical and data link layers.

Correcting Network Layer Problems

Step	Description
1	Ensure that you have a valid saved configuration for any device on which you intend to modify the configuration. This provides for eventual recovery to a known initial state.
2	Make initial hardware and software configuration changes. If the correction requires more than one change, make only one change at a time.
3	Evaluate and document the changes and the results of each change that you make. If you perform your problem-solving steps and the results are unsuccessful, immediately undo the changes. If the problem is intermittent, you may need to wait to see if the problem occurs again before you can evaluate the effect of your changes.
4	Verify that the changes you made actually fixed the problem without introducing any new problems. The network should be returned to the baseline operation, and no new or old symptoms should be present. If the problem is not solved, undo all the changes that you made. If you discover new or additional problems while you are making corrections, step back and modify your correction plan.
5	Stop making changes when the original problem appears to be solved.
6	If necessary, get input from outside resources. If none of your attempts to correct the problem are successful, take the problem to another person. This may be a coworker, consultant, or Cisco TAC. On rare occasions, you may need to perform a core dump, which creates output that a specialist at Cisco Systems can analyze.
7	Once the problem is resolved, document the solution.

Summary

This topic summarizes the key points discussed in this lesson.



Summary

- Use the appropriate end system or Cisco commands and applications to correct an isolated network layer problem.
- Proper use of online support resources saves time and money by empowering troubleshooters to find solutions to elusive problems on their own.
- Following a systematic procedure increases the chances that you will successfully and effectively correct an isolated problem at the network layer.

CIT 5.1—4-40

References

For additional information, refer to these resources:

- Cisco online documentation: http://www.cisco.com/univercd/home/home.htm
- Cisco Technical Assistance Center (TAC): http://www.cisco.com/tac
- Troubleshooting TCP/IP: http://www.cisco.com/univercd/cc/td/doc/cisintwk/itg_v1/tr1907.htm

Next Steps

For the associated case study and lab exercises, refer to the following sections of the course Lab Guide:

- Case Study (Trouble Ticket D) 4-1: Isolating Network Layer Problems
- Lab Exercise (Trouble Ticket D) 4-1: Correcting Problems at the Network Layer
- Lab Exercise (Trouble Ticket E) 4-2: Troubleshooting Problems at the Physical, Data Link, and Network Layers
- Lab Exercise (Trouble Ticket F) 4-3: Troubleshooting Problems at the Physical, Data Link, and Network Layers

Quiz

Use the practice items here to review what you have learned in this lesson. The correct answers are found in the Quiz Answer Key.

Q1) Which Cisco command is used to correct a problem with the BGP exterior routing protocol?

A) **passive-interface {interface-type number}**

B) **neighbor {*ip-address* | *peer-group-name*} update-source interface**

C) **ip route *prefix mask address* [*distance*]**

D) **ip mroute-cache**

Q2) Which end-system command do you use to renew or release an IP address lease on a Windows 98 machine?

A) **ipconfig**

B) **arp**

C) **winipcfg**

D) **route delete**

Q3) Which website would you most likely use to read the latest detailed technical documentation about the EIGRP protocol?

A) http://www.itu.int/home

B) http://www.atmforum.com

C) http://www.frforum.com

D) http://www.cisco.com

Q4) While correcting a problem with a misconfigured access list, you notice that the problem is not solved despite the numerous changes you have made. Instead of making additional configuration changes, you wisely undo all of the changes that you made previously. Which step of the recommended procedure for correcting problems at the network layer are you performing?

A) make initial configuration changes

B) stop making changes when the original problem appears to be solved

C) once the problem is solved, document the solution

D) verify that the changes you made actually fixed the problem without introducing any new problems

Quiz Answer Key

Q1) B

Relates to: Identifying Cisco Commands Used to Correct Problems Occurring at the Network Layer

Q2) C

Relates to: Identifying End-System Commands and Applications Used to Correct Problems Occurring at the Network Layer

Q3) D

Relates to: Identifying Network Layer Support Resources

Q4) D

Relates to: Correcting Problems Occurring at the Network Layer

Module 5

Resolving Problems at the Transport and Application Layers

Overview

The process that troubleshooters use for isolating and correcting problems at the transport and application layers is the same as the process for isolating and correcting problems at the lower layers. What differentiates these problems are the symptoms they present and the commands, applications, and steps that you use to successfully resolve these problems. In this module, you will perform the isolation and correction phases of the general troubleshooting process to resolve failure and optimization problems at the transport and application layers of the Open Systems Interconnection (OSI) model.

Module Objectives

Upon completing this module, you will be able to:

- Isolate problems occurring at the transport and application layers
- Correct problems occurring at the transport and application layers

Module Outline

The module contains these components:

- Isolating the Problem
- Correcting the Problem

Isolating the Problem

Overview

Troubleshooters can apply the same general troubleshooting process for analyzing gathered symptoms to isolate problems at the transport and application layers that they would apply to isolate problems at the lower layers. The ideas stay the same, but the technological focus shifts to involve things such as refused or timed out connections, access lists, and Domain Name System (DNS) issues. In this lesson, you will analyze defined symptoms and use commands and applications to isolate problems at the transport and application layers.

Relevance

The primary responsibility of the upper layers of the OSI model is providing services such as email and file transfer, and handling the transportation of the data used by those applications to the lower layers. If a problem arises at these layers, the data is not delivered to the destination or the performance is so slow that it affects productivity. You will likely hear complaints from those users who are accessing services such as email and file transfer. To avoid extended or periodic losses in the ability to transmit data and users who complain that the network is too slow, it is important for a troubleshooter to effectively isolate problems at the transport and application layers.

Objectives

Upon completing this lesson, you will be able to:

- Identify the symptoms of problems occurring at the transport layer
- Identify the symptoms of problems occurring at the application layer
- Analyze command and application output to isolate problems occurring at the transport layer
- Analyze command and application output to isolate problems occurring at the application layer
- Isolate problems occurring at the transport and application layers

Learner Skills and Knowledge

To benefit fully from this lesson, you must have these prerequisite skills and knowledge:

- The ability to apply layered model troubleshooting approaches
- Familiarity with the Cisco command syntax and technologies covered in the Cisco *Building Scalable Cisco Internetworks* (BSCI), *Building Cisco Multilayer Switched Networks* (BCMSN), and *Building Cisco Remote Access Networks* (BCRAN) courses
- Basic TCP and User Datagram Protocol (UDP) concepts

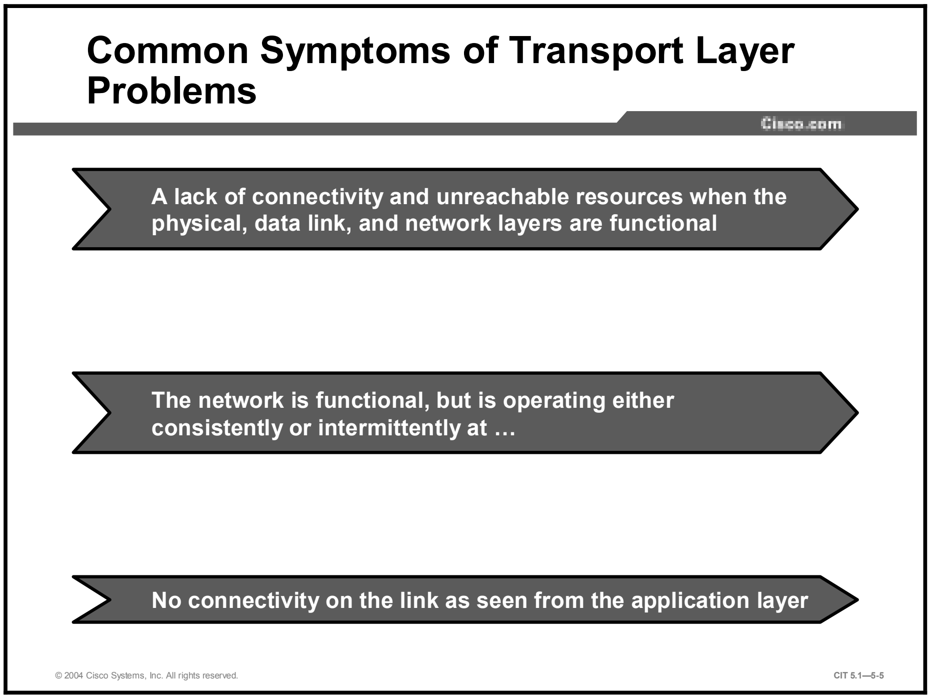
Outline

This lesson includes these topics:

- Overview
- Identifying the Symptoms of Problems Occurring at the Transport Layer
- Identifying the Symptoms of Problems Occurring at the Application Layer
- Analyzing Commands and Applications Used to Isolate Problems Occurring at the Transport Layer
- Analyzing Commands and Applications Used to Isolate Problems Occurring at the Application Layer
- Isolating Problems Occurring at the Transport and Application Layers
- Summary
- Quiz

Identifying the Symptoms of Problems Occurring at the Transport Layer

This topic identifies the symptoms of transport layer problems that troubleshooters should be able to identify.



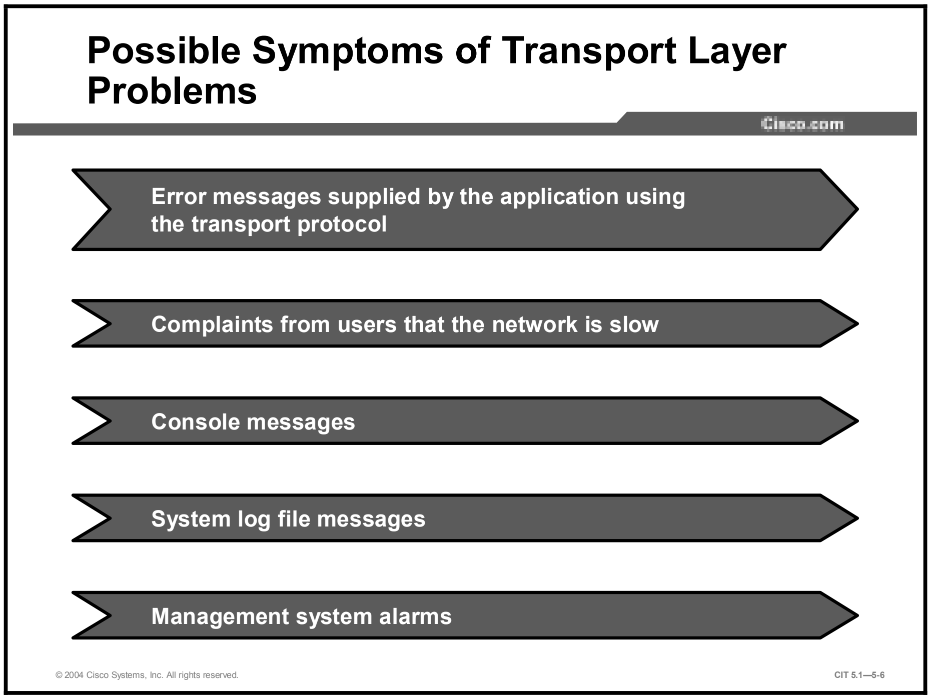
Common Symptoms of Transport Layer Problems

- A lack of connectivity and unreachable resources when the physical, data link, and network layers are functional
- The network is functional, but is operating either consistently or intermittently at …
- No connectivity on the link as seen from the application layer

CIT 5.1—5-5

A transport layer failure problem is a network problem that occurs at the transport layer of the OSI model when data from the upper layers is not transported to the lower layer services of a receiver. A problem at the transport layer results in a lack of connectivity and unreachable resources when the physical, data link, and network layers are functional.

Another problem at the transport layer occurs when the physical, data link, and network layers are functional, but data from the applications using the transport layer protocols does not transfer at the rate established in the baseline. For the TCP/IP protocol suite, a failure problem at the transport layer will involve either the TCP or the UDP, which moves data from a source port to a destination port.



Possible Symptoms of Transport Layer Problems

- Error messages supplied by the application using the transport protocol
- Complaints from users that the network is slow
- Console messages
- System log file messages
- Management system alarms

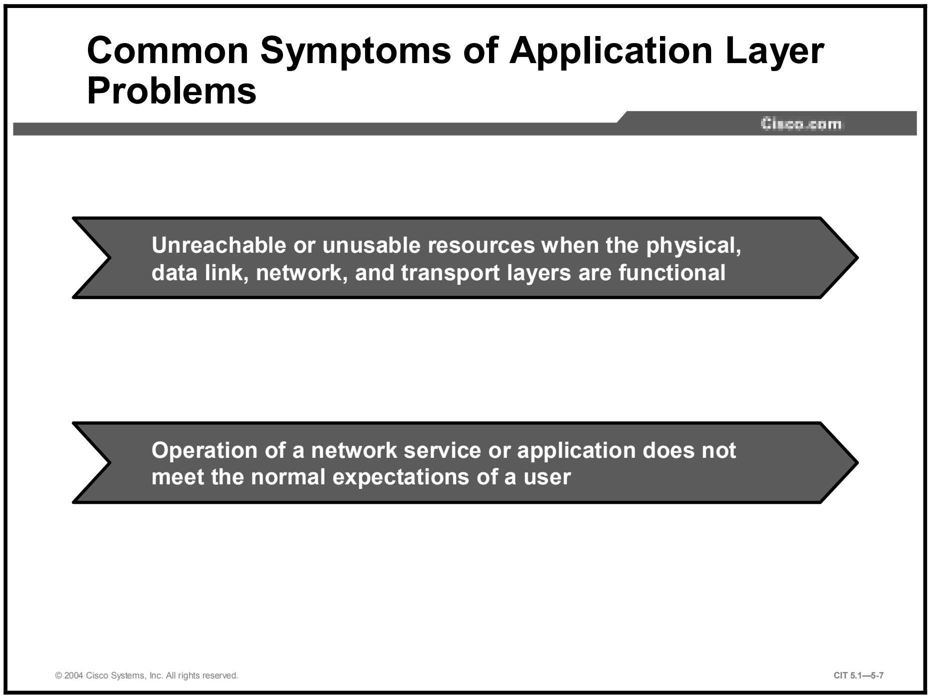
CIT 5.1—5-6

The symptoms that a troubleshooter may encounter for a failure problem at the transport layer include console messages, system log file messages, management system alarms, or error messages supplied by the application using the transport protocol.

Other symptoms of a transport layer problem may be identified as complaints from users that the network is slow, or that there is partial or intermittent connectivity or erratic performance. This erratic performance could be due to windowing problems, long round-trip times (RTTs), retransmissions, fragmentation, or duplicates.

Identifying the Symptoms of Problems Occurring at the Application Layer

This topic identifies the symptoms of application layer problems that troubleshooters should be able to identify.



Common Symptoms of Application Layer Problems

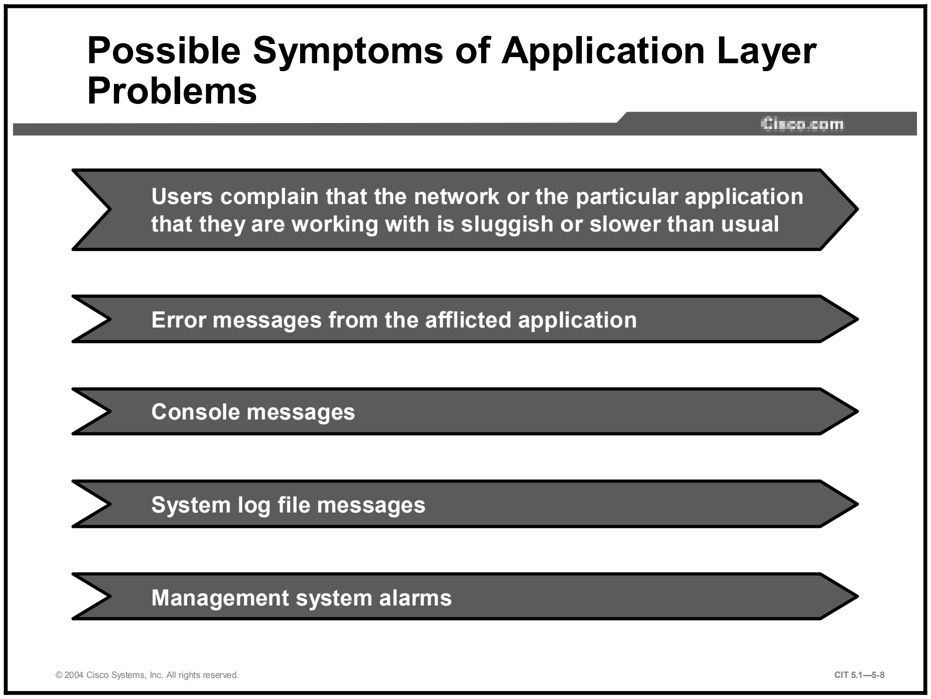
Unreachable or unusable resources when the physical, data link, network, and transport layers are functional

Operation of a network service or application does not meet the normal expectations of a user

CIT 5.1—5-7

An application layer problem is a network problem that occurs at the session layer (Layer 5), the presentation layer (Layer 6), or the application layer (Layer 7) of the OSI model that prevents services from being provided to application programs. The application layer is the interface between an application and the transport layer. This layer deals with high-level protocols rather than segments, bytes, packets, or bits. A problem at the application layer results in unreachable or unusable resources when the physical, data link, network, and transport layers are functional. With application layer problems, it is possible to have full network connectivity, but the application simply cannot provide data.

Another type of problem at the application layer occurs when the physical, data link, network, and transport layers are functional, but the data transfer and requests for network services from a single network service or application do not meet the normal expectations of a user.



Possible Symptoms of Application Layer Problems

Cisco.com

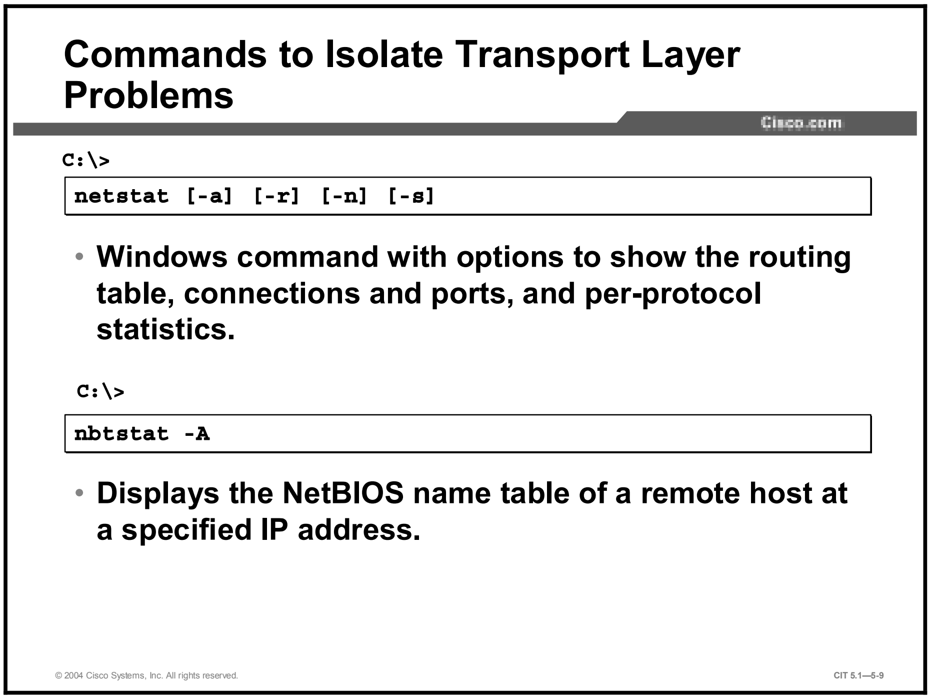
- Users complain that the network or the particular application that they are working with is sluggish or slower than usual
- Error messages from the afflicted application
- Console messages
- System log file messages
- Management system alarms

CIT 5.1—5-8

A problem at the application layer may cause users to complain that the network or the particular application that they are working with is sluggish or slower than usual when transferring data or requesting network services. A failing application may supply various error messages that are sometimes informative and will help you isolate the problem to a particular component in the transport layer.

Analyzing Commands and Applications Used to Isolate Problems Occurring at the Transport Layer

This topic identifies the output of commands and applications with the purpose of helping troubleshooters isolate a problem at the transport layer.



Commands to Isolate Transport Layer Problems

```
C:\>
netstat [-a] [-r] [-n] [-s]
```

- **Windows command with options to show the routing table, connections and ports, and per-protocol statistics.**

```
C:\>
nbtstat -A
```

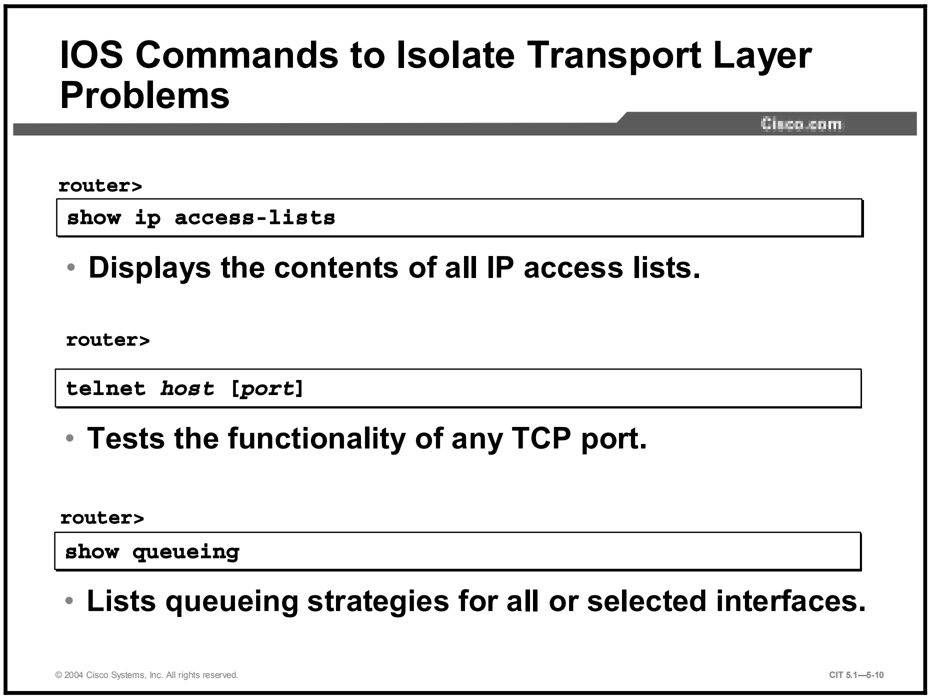
- **Displays the NetBIOS name table of a remote host at a specified IP address.**

CIT 5.1—5-9

The table shows commands that a troubleshooter may use to isolate problems at the transport layer. Although many of these commands also display information that concerns other layers, the commands are noteworthy at the transport layer because they highlight problems in the interface between the network and transport layers.

General Commands to Isolate Transport Layer Problems

Command	Description
ping *{host | ip-address}*	Sends an echo request packet to an address, then waits for a reply. The *host* | *ip-address* variable is the host name or IP address of the target system.
traceroute *[destination]*	Identifies the path a packet takes through the network. The *destination* variable is the host name or IP address of the target system. This command is used with Cisco IOS, UNIX, and Mac OS X.
tracert *[destination]*	Verifies connectivity to a destination device for Windows hosts. The *destination* variable is the IP alias or IP address of the target system.
netstat –[**-a**] [**-r**] [**-n**] [**-s**]	(Windows command) Has options to show the routing table, connections and ports, and per-protocol statistics.
nbtstat –A	Displays the NetBIOS name table of a remote host at a specified IP address.
show running-config	Shows access list rules being applied in the current configuration.



IOS Commands to Isolate Transport Layer Problems

```
router>
show ip access-lists
```

- Displays the contents of all IP access lists.

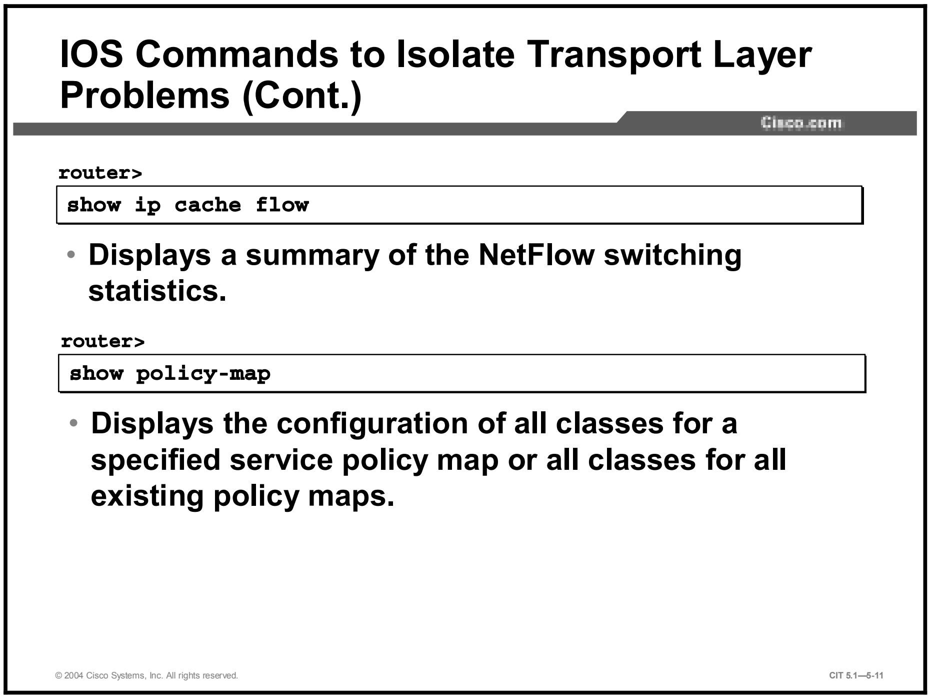
```
router>
telnet host [port]
```

- Tests the functionality of any TCP port.

```
router>
show queueing
```

- Lists queueing strategies for all or selected interfaces.

CIT 5.1—5-10



IOS Commands to Isolate Transport Layer Problems (Cont.)

```
router>
show ip cache flow
```

- Displays a summary of the NetFlow switching statistics.

```
router>
show policy-map
```

- Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps.

CIT 5.1—5-11

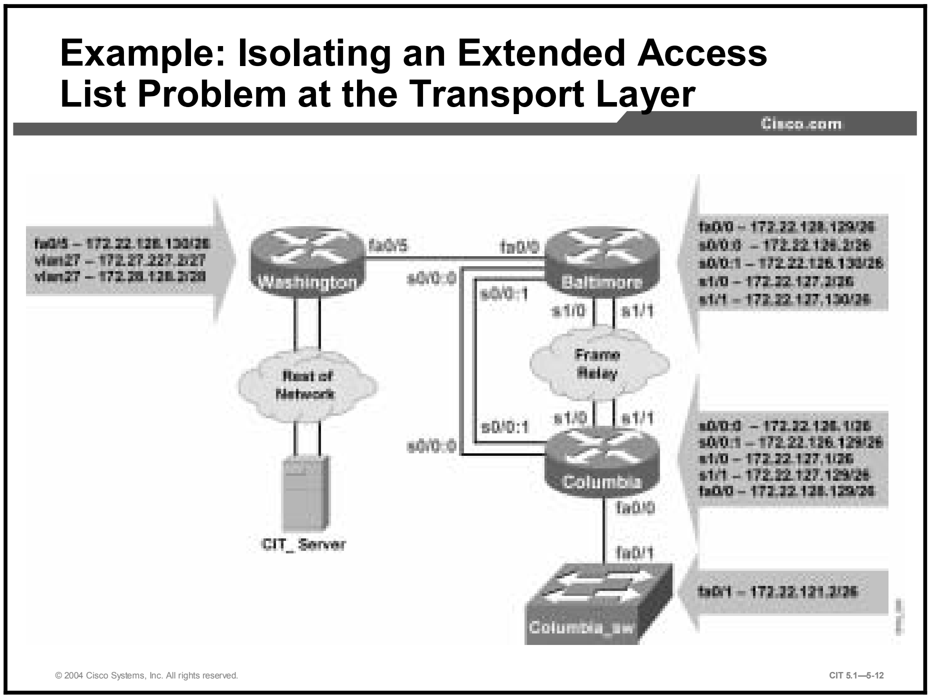
The Cisco commands listed in the table display information about transport layer issues. A troubleshooter uses the information from these commands to isolate problems at the transport layer that are related to TCP and UDP.

Commands Used to Isolate Transport Layer Problems

Command	Description
show ip access-lists	Displays the contents of all IP access lists.
show ip traffic	Displays statistics about IP traffic, such as format errors, bad hops, encapsulation failures, unknown routes, and probe proxy requests.
telnet *host* [*port*]	Tests the functionality of any TCP port.
show queueing [custom **|** fair **|** priority **|** random-detect [interface *atm-subinterface* [vc [[*vpi*/] *vci*]]]]	Lists queueing strategies for all or selected interfaces.
show ip cache flow	Displays a summary of the NetFlow switching statistics.
show policy-map	Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps.

Example: Isolating an Extended Access List Problem at the Transport Layer

You are the second-level network engineer for Columbia. You have console access to both the access router named Columbia and the access switch named Columbia_SW. You also have IP connectivity to all other devices in your division. Your division supports the 172.22.0.0/16 subnet.



Example: Isolating an Extended Access List Problem at the Transport Layer

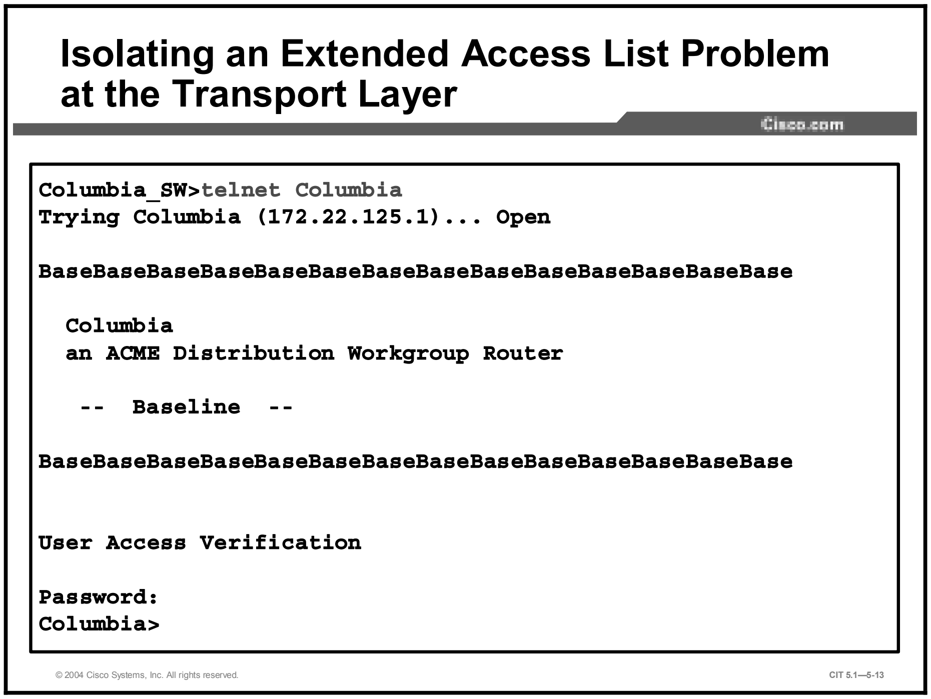
© 2004 Cisco Systems, Inc. All rights reserved.

CIT 5.1—5-12

The MIS department calls to report that none of the PC end users can use Telnet to connect to a server named CIT_Server. MIS reports that the end users cannot even connect to the distribution router named Baltimore from their PCs.

You know from your base configuration information that the end users connect over Columbia_SW to Columbia. Columbia and Columbia_SW are connected via a 100 Mbs Fast Ethernet link.

You connect to the console port on Columbia_SW and attempt to use Telnet to connect to Columbia.



Isolating an Extended Access List Problem at the Transport Layer

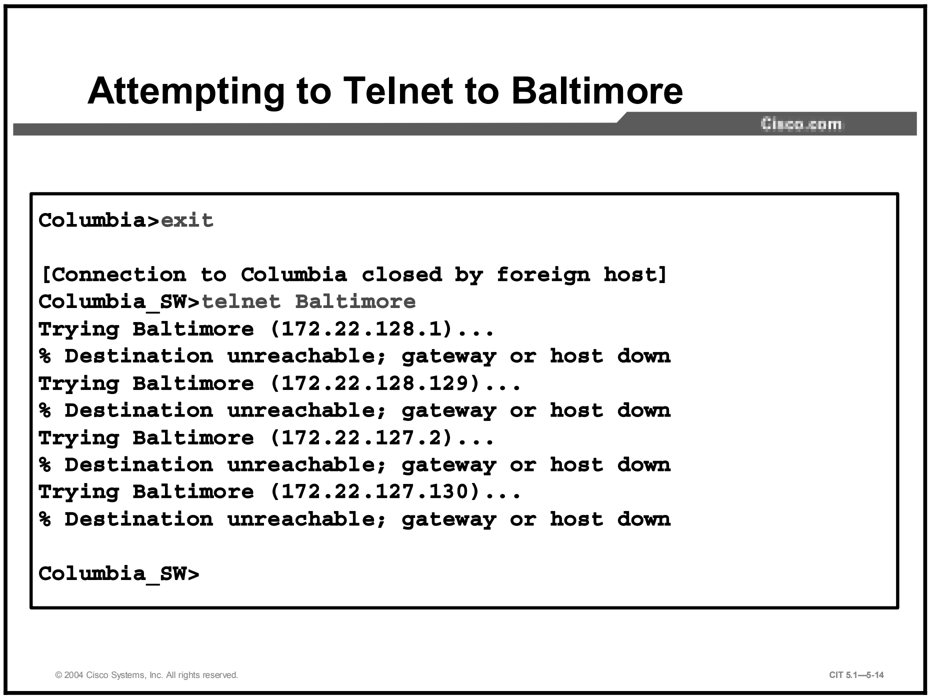
```
Columbia_SW>telnet Columbia
Trying Columbia (172.22.125.1)... Open

BaseBaseBaseBaseBaseBaseBaseBaseBaseBaseBaseBaseBaseBase

  Columbia
  an ACME Distribution Workgroup Router

   --  Baseline  --

BaseBaseBaseBaseBaseBaseBaseBaseBaseBaseBaseBaseBaseBase


User Access Verification

Password:
Columbia>
```

CIT 5.1—5-13

Because you can connect to Columbia from Columbia_SW, there appears to be no issues between these two devices.

Note This example uses the host names that have been configured in the standard host table mappings for the *Cisco Internetwork Troubleshooting* (CIT) labs.

You close the Telnet session to Columbia and try to connect to Baltimore from Columbia_SW.



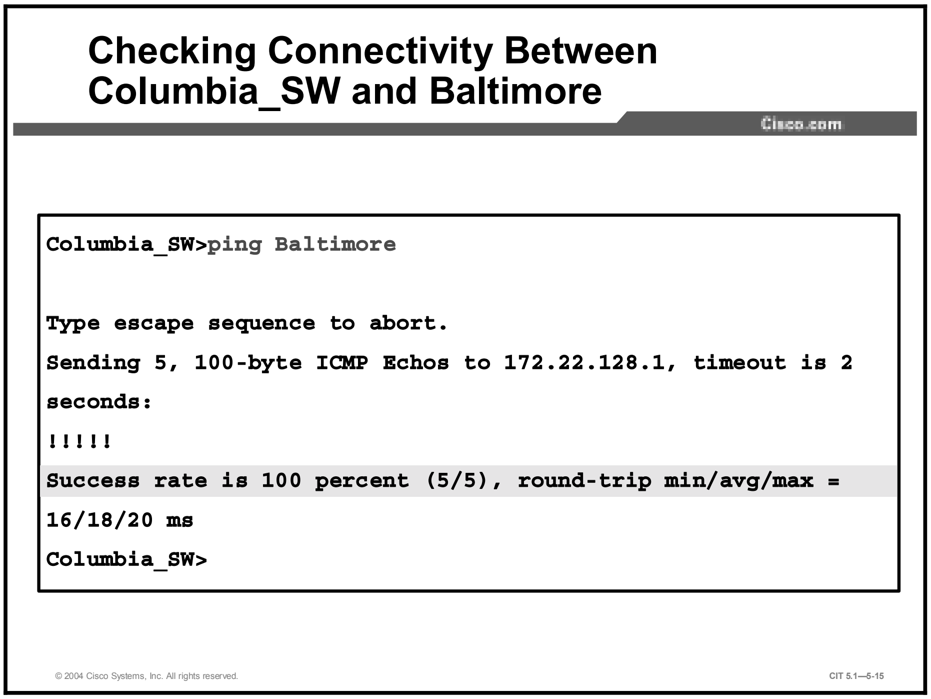
Attempting to Telnet to Baltimore

```
Columbia>exit

[Connection to Columbia closed by foreign host]
Columbia_SW>telnet Baltimore
Trying Baltimore (172.22.128.1)...
% Destination unreachable; gateway or host down
Trying Baltimore (172.22.128.129)...
% Destination unreachable; gateway or host down
Trying Baltimore (172.22.127.2)...
% Destination unreachable; gateway or host down
Trying Baltimore (172.22.127.130)...
% Destination unreachable; gateway or host down

Columbia_SW>
```

CIT 5.1—5-14

You note that the Telnet session from Columbia_SW cannot be opened on Baltimore.

To help isolate the problem, you check to see if Columbia_SW can ping Baltimore.



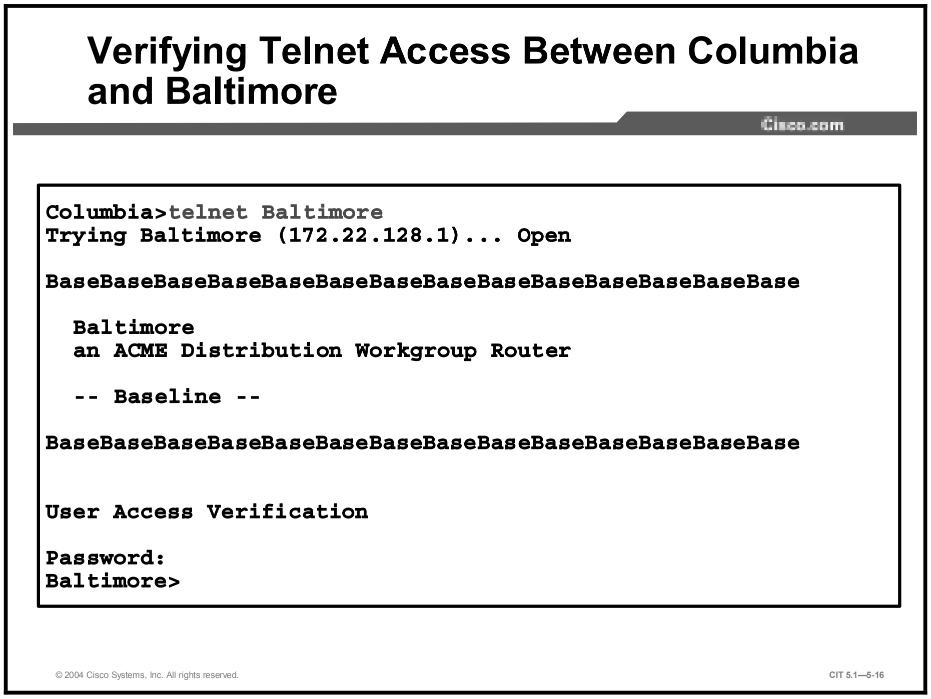
Checking Connectivity Between Columbia_SW and Baltimore

```
Columbia_SW>ping Baltimore


Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.22.128.1, timeout is 2
seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
16/18/20 ms
Columbia_SW>
```

CIT 5.1—5-15

You see that Columbia_SW can ping Baltimore, so it appears that the physical, data link, and network layers between these devices are working. This makes you suspect that the issue is with an access list.

Next, you try to open a Telnet session from Columbia to Baltimore.



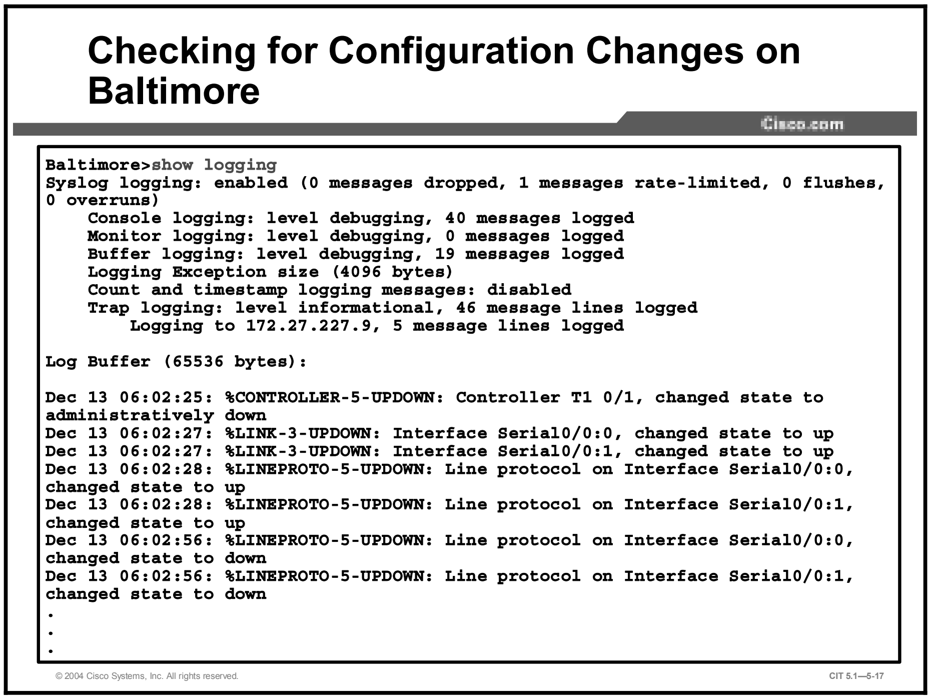
Verifying Telnet Access Between Columbia and Baltimore

```
Columbia>telnet Baltimore
Trying Baltimore (172.22.128.1)... Open

BaseBaseBaseBaseBaseBaseBaseBaseBaseBaseBaseBaseBaseBase

  Baltimore
  an ACME Distribution Workgroup Router

  -- Baseline --

BaseBaseBaseBaseBaseBaseBaseBaseBaseBaseBaseBaseBaseBase


User Access Verification

Password:
Baltimore>
```

CIT 5.1—5-16

You see that Columbia can open a Telnet session to Baltimore, so this tells you that Baltimore is not blocking all inbound Telnet traffic.

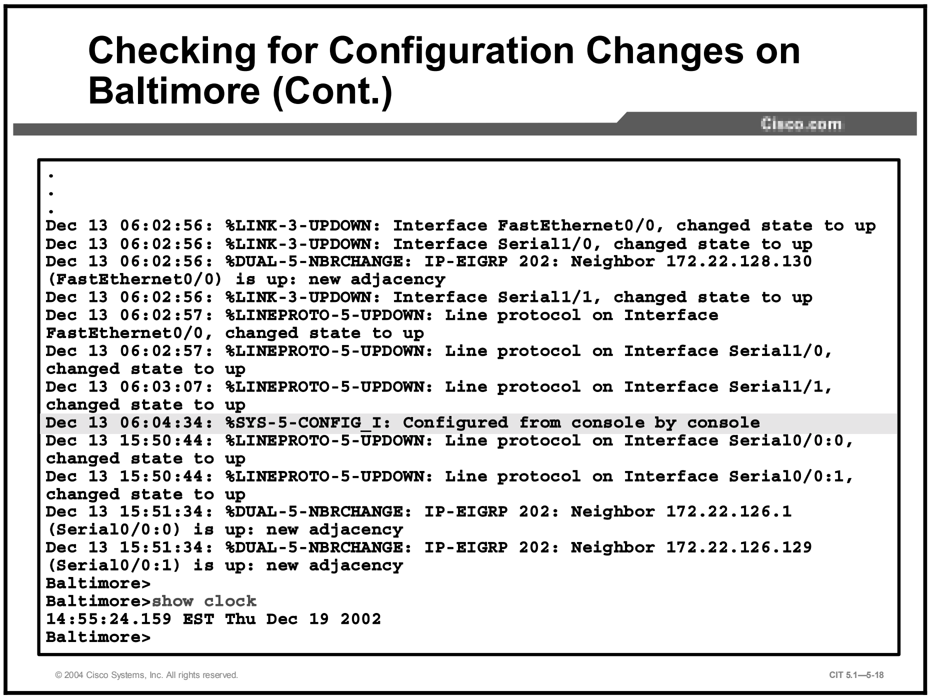
You look for signs of recent configuration changes on Baltimore by entering the **show logging** and **show clock** commands.



Checking for Configuration Changes on Baltimore

```
Baltimore>show logging
Syslog logging: enabled (0 messages dropped, 1 messages rate-limited, 0 flushes,
0 overruns)
    Console logging: level debugging, 40 messages logged
    Monitor logging: level debugging, 0 messages logged
    Buffer logging: level debugging, 19 messages logged
    Logging Exception size (4096 bytes)
    Count and timestamp logging messages: disabled
    Trap logging: level informational, 46 message lines logged
        Logging to 172.27.227.9, 5 message lines logged

Log Buffer (65536 bytes):

Dec 13 06:02:25: %CONTROLLER-5-UPDOWN: Controller T1 0/1, changed state to
administratively down
Dec 13 06:02:27: %LINK-3-UPDOWN: Interface Serial0/0:0, changed state to up
Dec 13 06:02:27: %LINK-3-UPDOWN: Interface Serial0/0:1, changed state to up
Dec 13 06:02:28: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0:0,
changed state to up
Dec 13 06:02:28: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0:1,
changed state to up
Dec 13 06:02:56: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0:0,
changed state to down
Dec 13 06:02:56: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0:1,
changed state to down
.
.
.
```

CIT 5.1—5-17



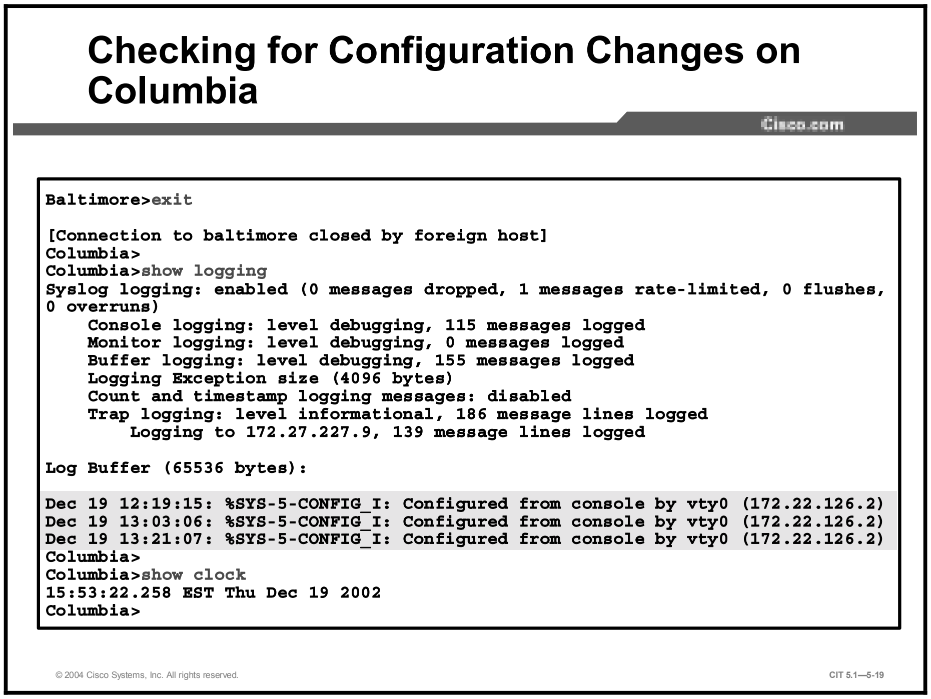
Checking for Configuration Changes on Baltimore (Cont.)

```
.
.
.
Dec 13 06:02:56: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
Dec 13 06:02:56: %LINK-3-UPDOWN: Interface Serial1/0, changed state to up
Dec 13 06:02:56: %DUAL-5-NBRCHANGE: IP-EIGRP 202: Neighbor 172.22.128.130
(FastEthernet0/0) is up: new adjacency
Dec 13 06:02:56: %LINK-3-UPDOWN: Interface Serial1/1, changed state to up
Dec 13 06:02:57: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/0, changed state to up
Dec 13 06:02:57: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1/0,
changed state to up
Dec 13 06:03:07: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1/1,
changed state to up
Dec 13 06:04:34: %SYS-5-CONFIG_I: Configured from console by console
Dec 13 15:50:44: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0:0,
changed state to up
Dec 13 15:50:44: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0:1,
changed state to up
Dec 13 15:51:34: %DUAL-5-NBRCHANGE: IP-EIGRP 202: Neighbor 172.22.126.1
(Serial0/0:0) is up: new adjacency
Dec 13 15:51:34: %DUAL-5-NBRCHANGE: IP-EIGRP 202: Neighbor 172.22.126.129
(Serial0/0:1) is up: new adjacency
Baltimore>
Baltimore>show clock
14:55:24.159 EST Thu Dec 19 2002
Baltimore>
```

CIT 5.1—5-18

You see that no configuration changes have been made on Baltimore for several days. Therefore, you return to the console session on Columbia.

You look for signs of recent configuration changes on Columbia with the **show logging** and **show clock** commands.



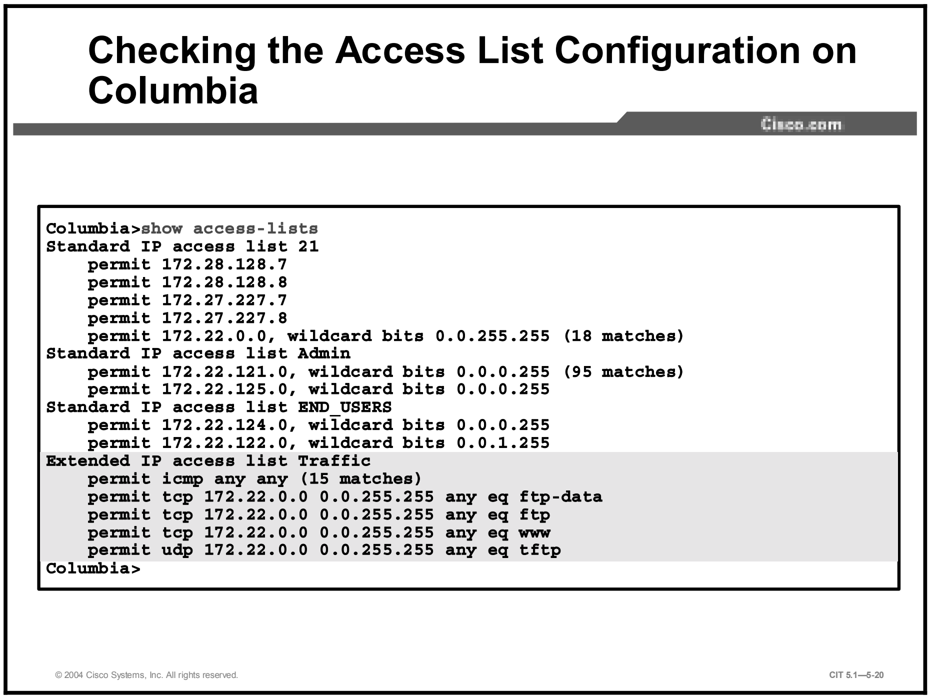
Checking for Configuration Changes on Columbia

```
Baltimore>exit

[Connection to baltimore closed by foreign host]
Columbia>
Columbia>show logging
Syslog logging: enabled (0 messages dropped, 1 messages rate-limited, 0 flushes,
0 overruns)
    Console logging: level debugging, 115 messages logged
    Monitor logging: level debugging, 0 messages logged
    Buffer logging: level debugging, 155 messages logged
    Logging Exception size (4096 bytes)
    Count and timestamp logging messages: disabled
    Trap logging: level informational, 186 message lines logged
        Logging to 172.27.227.9, 139 message lines logged

Log Buffer (65536 bytes):

Dec 19 12:19:15: %SYS-5-CONFIG_I: Configured from console by vty0 (172.22.126.2)
Dec 19 13:03:06: %SYS-5-CONFIG_I: Configured from console by vty0 (172.22.126.2)
Dec 19 13:21:07: %SYS-5-CONFIG_I: Configured from console by vty0 (172.22.126.2)
Columbia>
Columbia>show clock
15:53:22.258 EST Thu Dec 19 2002
Columbia>
```

CIT 5.1—5-19

You notice that someone was at least in configuration mode on Columbia in the last few hours. You did not have any upgrades planned, but you need to review the details of the access lists on Columbia. Because pings to Baltimore from Columbia_SW are successful, you suspect that the problem is probably with an extended access list filtering too much traffic.

You use the **show access-lists** commands to review the current access lists configured on Columbia.



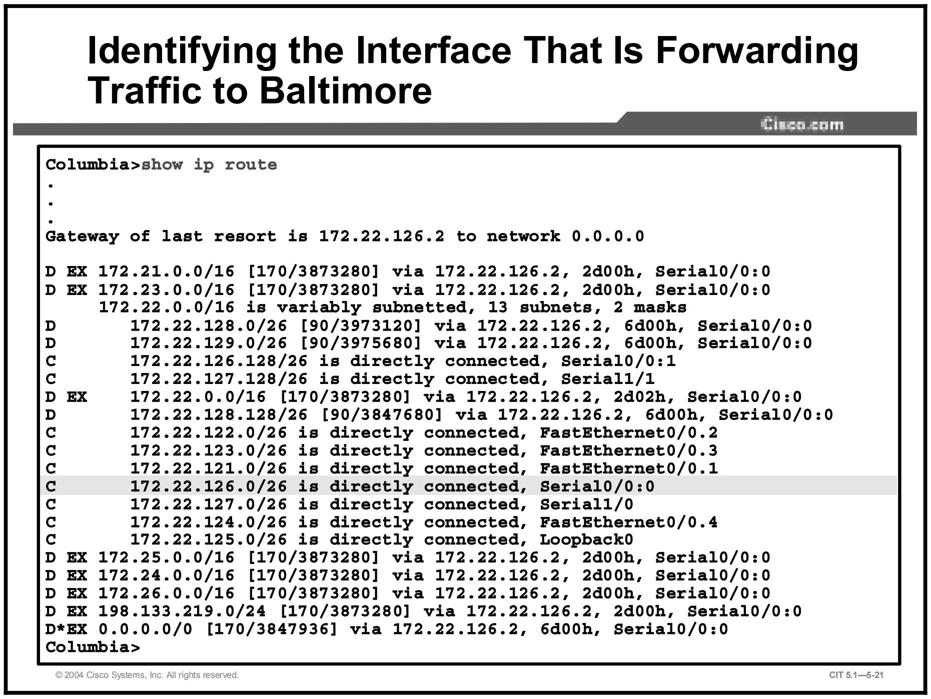
Checking the Access List Configuration on Columbia

```
Columbia>show access-lists
Standard IP access list 21
    permit 172.28.128.7
    permit 172.28.128.8
    permit 172.27.227.7
    permit 172.27.227.8
    permit 172.22.0.0, wildcard bits 0.0.255.255 (18 matches)
Standard IP access list Admin
    permit 172.22.121.0, wildcard bits 0.0.0.255 (95 matches)
    permit 172.22.125.0, wildcard bits 0.0.0.255
Standard IP access list END_USERS
    permit 172.22.124.0, wildcard bits 0.0.0.255
    permit 172.22.122.0, wildcard bits 0.0.1.255
Extended IP access list Traffic
    permit icmp any any (15 matches)
    permit tcp 172.22.0.0 0.0.255.255 any eq ftp-data
    permit tcp 172.22.0.0 0.0.255.255 any eq ftp
    permit tcp 172.22.0.0 0.0.255.255 any eq www
    permit udp 172.22.0.0 0.0.255.255 any eq tftp
Columbia>
```

CIT 5.1—5-20

The only extended access list is called “Traffic.” This access list explicitly permits Internet Control Message Protocol (ICMP), FTP, web, and TFTP traffic. However, the implicit deny at the end of the list would block Telnet traffic that came from Columbia_SW from being forwarded to Baltimore.

You also use the **show ip route command** to determine which interface is being used to forward traffic to Baltimore.

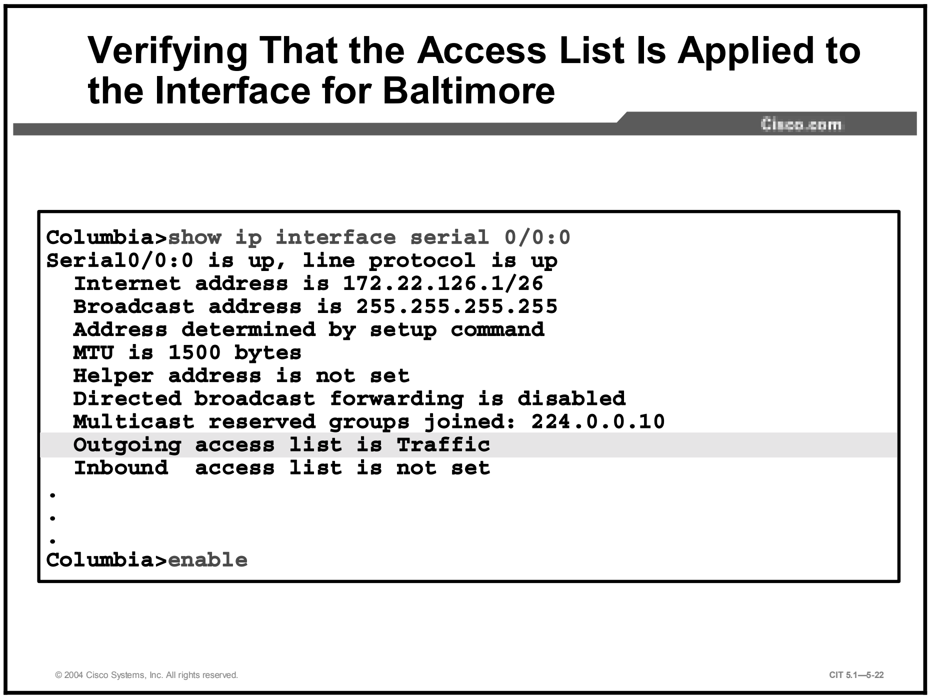


Identifying the Interface That Is Forwarding Traffic to Baltimore

```
Columbia>show ip route
.
.
.
Gateway of last resort is 172.22.126.2 to network 0.0.0.0

D EX 172.21.0.0/16 [170/3873280] via 172.22.126.2, 2d00h, Serial0/0:0
D EX 172.23.0.0/16 [170/3873280] via 172.22.126.2, 2d00h, Serial0/0:0
     172.22.0.0/16 is variably subnetted, 13 subnets, 2 masks
D       172.22.128.0/26 [90/3973120] via 172.22.126.2, 6d00h, Serial0/0:0
D       172.22.129.0/26 [90/3975680] via 172.22.126.2, 6d00h, Serial0/0:0
C       172.22.126.128/26 is directly connected, Serial0/0:1
C       172.22.127.128/26 is directly connected, Serial1/1
D EX    172.22.0.0/16 [170/3873280] via 172.22.126.2, 2d02h, Serial0/0:0
D       172.22.128.128/26 [90/3847680] via 172.22.126.2, 6d00h, Serial0/0:0
C       172.22.122.0/26 is directly connected, FastEthernet0/0.2
C       172.22.123.0/26 is directly connected, FastEthernet0/0.3
C       172.22.121.0/26 is directly connected, FastEthernet0/0.1
C       172.22.126.0/26 is directly connected, Serial0/0:0
C       172.22.127.0/26 is directly connected, Serial1/0
C       172.22.124.0/26 is directly connected, FastEthernet0/0.4
C       172.22.125.0/26 is directly connected, Loopback0
D EX 172.25.0.0/16 [170/3873280] via 172.22.126.2, 2d00h, Serial0/0:0
D EX 172.24.0.0/16 [170/3873280] via 172.22.126.2, 2d00h, Serial0/0:0
D EX 172.26.0.0/16 [170/3873280] via 172.22.126.2, 2d00h, Serial0/0:0
D EX 198.133.219.0/24 [170/3873280] via 172.22.126.2, 2d00h, Serial0/0:0
D*EX 0.0.0.0/0 [170/3847936] via 172.22.126.2, 6d00h, Serial0/0:0
Columbia>
```

You see that traffic for Baltimore is sent across the interface named Serial0/0:0.

Finally, you check that the access list named Traffic is applied to Serial 0/0:0 with the **show ip interface serial 0/0:0** command.

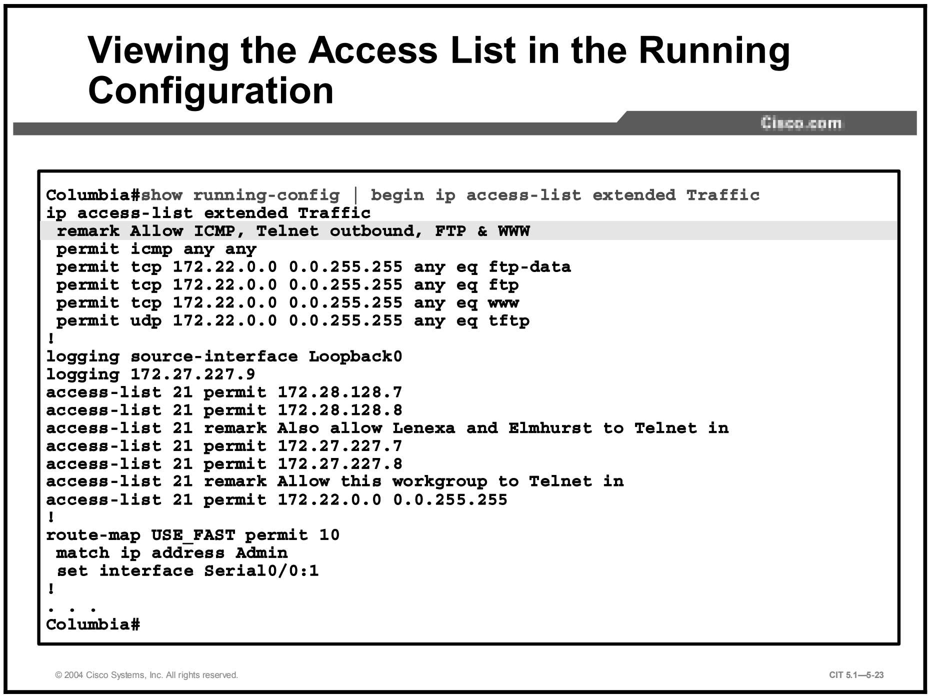


Verifying That the Access List Is Applied to the Interface for Baltimore

```
Columbia>show ip interface serial 0/0:0
Serial0/0:0 is up, line protocol is up
  Internet address is 172.22.126.1/26
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Multicast reserved groups joined: 224.0.0.10
  Outgoing access list is Traffic
  Inbound  access list is not set
.
.
.
Columbia>enable
```

© 2004 Cisco Systems, Inc. All rights reserved. CIT 5.1—5-22

You also review the access list in the running configuration.



Viewing the Access List in the Running Configuration

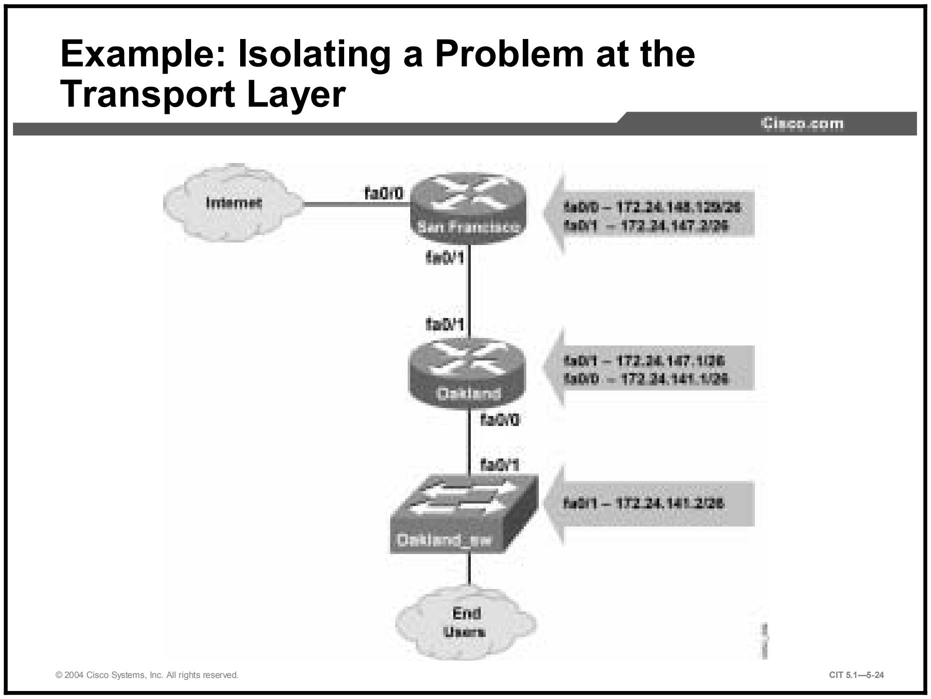
```
Columbia#show running-config | begin ip access-list extended Traffic
ip access-list extended Traffic
 remark Allow ICMP, Telnet outbound, FTP & WWW
 permit icmp any any
 permit tcp 172.22.0.0 0.0.255.255 any eq ftp-data
 permit tcp 172.22.0.0 0.0.255.255 any eq ftp
 permit tcp 172.22.0.0 0.0.255.255 any eq www
 permit udp 172.22.0.0 0.0.255.255 any eq tftp
!
logging source-interface Loopback0
logging 172.27.227.9
access-list 21 permit 172.28.128.7
access-list 21 permit 172.28.128.8
access-list 21 remark Also allow Lenexa and Elmhurst to Telnet in
access-list 21 permit 172.27.227.7
access-list 21 permit 172.27.227.8
access-list 21 remark Allow this workgroup to Telnet in
access-list 21 permit 172.22.0.0 0.0.255.255
!
route-map USE_FAST permit 10
 match ip address Admin
 set interface Serial0/0:1
!
. . .
Columbia#
```

© 2004 Cisco Systems, Inc. All rights reserved. CIT 5.1—5-23

You have isolated the issue. The outbound access list named Traffic does not include a permit statement for Telnet. All Telnet traffic from the access switch and end users is being filtered. The remark statement for the access list Traffic states that it should support TCP outbound.

Example: Isolating a Problem at the Transport Layer

You are the second-level network engineer for Oakland. You have console access to both the access router named Oakland and the access switch named Oakland_SW. You also have IP connectivity to all other devices in your division. Your division supports the 172.24.0.0/16 subnet.



Example: Isolating a Problem at the Transport Layer

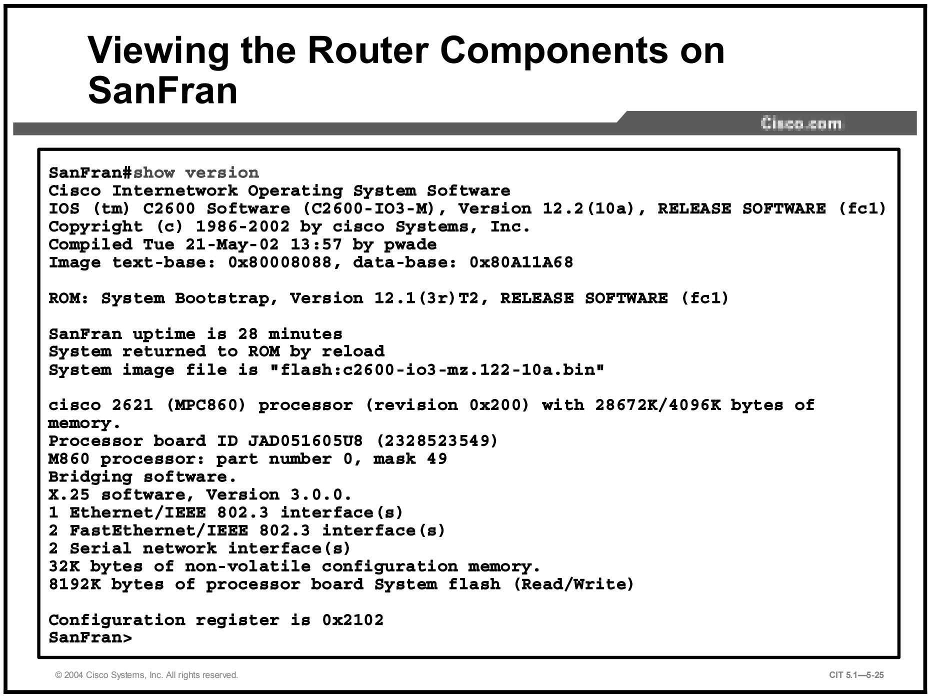
CIT 5.1—5-24

You receive a message that SanFran crashed last night, and that Network Operations had to reload SanFran this morning. Network Operations asks you to determine why the router crashed, indicating that no configuration changes have been made in weeks.

You know that SanFran is running the firewall feature set and that it is acting as the firewall to the Internet for the rest of the division.

Note This example topology does not follow the CIT lab configuration.

First, you decide to check out the software and hardware on SanFran. You log onto SanFran and use the **show version** command to review the basic router components.



Viewing the Router Components on SanFran

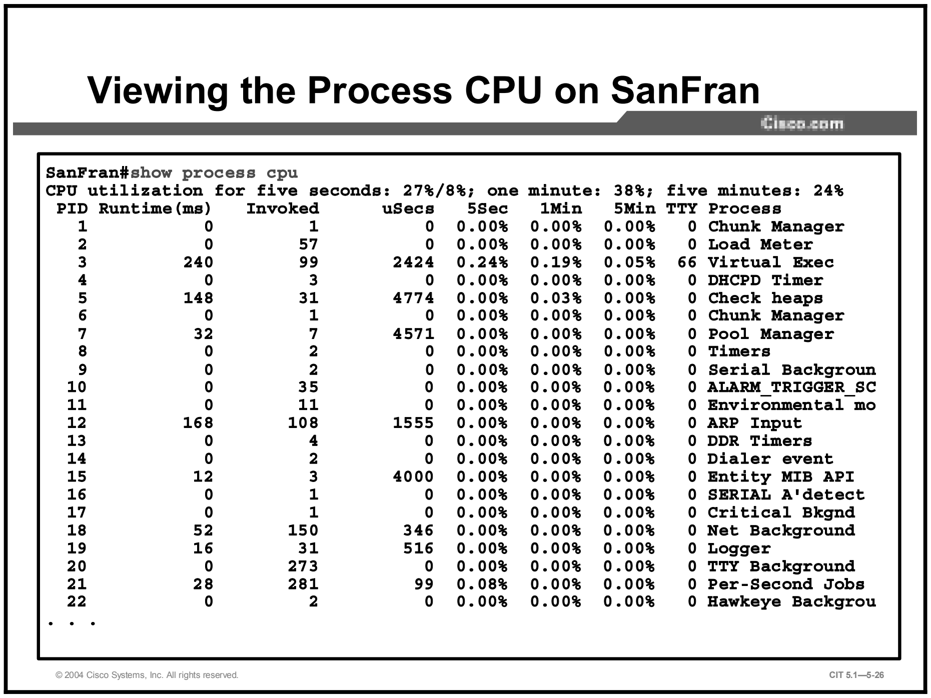
```
SanFran#show version
Cisco Internetwork Operating System Software
IOS (tm) C2600 Software (C2600-IO3-M), Version 12.2(10a), RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2002 by cisco Systems, Inc.
Compiled Tue 21-May-02 13:57 by pwade
Image text-base: 0x80008088, data-base: 0x80A11A68

ROM: System Bootstrap, Version 12.1(3r)T2, RELEASE SOFTWARE (fc1)

SanFran uptime is 28 minutes
System returned to ROM by reload
System image file is "flash:c2600-io3-mz.122-10a.bin"

cisco 2621 (MPC860) processor (revision 0x200) with 28672K/4096K bytes of
memory.
Processor board ID JAD051605U8 (2328523549)
M860 processor: part number 0, mask 49
Bridging software.
X.25 software, Version 3.0.0.
1 Ethernet/IEEE 802.3 interface(s)
2 FastEthernet/IEEE 802.3 interface(s)
2 Serial network interface(s)
32K bytes of non-volatile configuration memory.
8192K bytes of processor board System flash (Read/Write)

Configuration register is 0x2102
SanFran>
```

© 2004 Cisco Systems, Inc. All rights reserved.

CIT 5.1—5-25

You see that SanFran is a 2600 series router running the “io3-ms.122-10a” image. SanFran has two Fast Ethernet ports, two serial ports, and an Ethernet port. The router has been up for 28 minutes and was reloaded. This all seems reasonable given what you heard from Network Operations and what you know about the network.

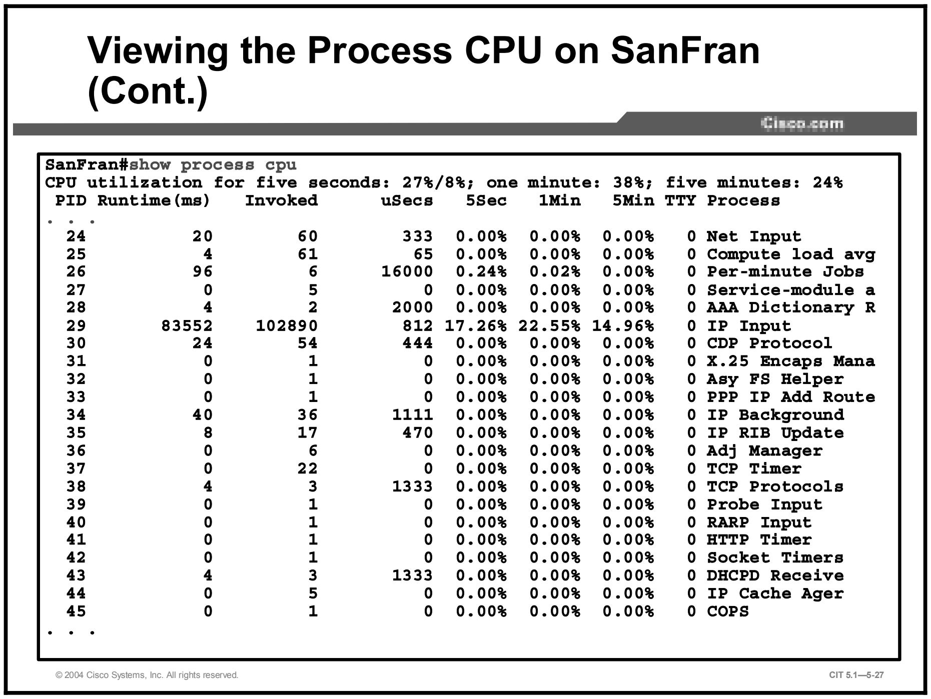
You decide to use the **show process CPU** command to review the process CPU utilization on SanFran.



Viewing the Process CPU on SanFran

```
SanFran#show process cpu
CPU utilization for five seconds: 27%/8%; one minute: 38%; five minutes: 24%
 PID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min TTY Process
   1           0         1          0  0.00%  0.00%  0.00%   0 Chunk Manager
   2           0        57          0  0.00%  0.00%  0.00%   0 Load Meter
   3         240        99       2424  0.24%  0.19%  0.05%  66 Virtual Exec
   4           0         3          0  0.00%  0.00%  0.00%   0 DHCPD Timer
   5         148        31       4774  0.00%  0.03%  0.00%   0 Check heaps
   6           0         1          0  0.00%  0.00%  0.00%   0 Chunk Manager
   7          32         7       4571  0.00%  0.00%  0.00%   0 Pool Manager
   8           0         2          0  0.00%  0.00%  0.00%   0 Timers
   9           0         2          0  0.00%  0.00%  0.00%   0 Serial Backgroun
  10           0        35          0  0.00%  0.00%  0.00%   0 ALARM_TRIGGER_SC
  11           0        11          0  0.00%  0.00%  0.00%   0 Environmental mo
  12         168       108       1555  0.00%  0.00%  0.00%   0 ARP Input
  13           0         4          0  0.00%  0.00%  0.00%   0 DDR Timers
  14           0         2          0  0.00%  0.00%  0.00%   0 Dialer event
  15          12         3       4000  0.00%  0.00%  0.00%   0 Entity MIB API
  16           0         1          0  0.00%  0.00%  0.00%   0 SERIAL A'detect
  17           0         1          0  0.00%  0.00%  0.00%   0 Critical Bkgnd
  18          52       150        346  0.00%  0.00%  0.00%   0 Net Background
  19          16        31        516  0.00%  0.00%  0.00%   0 Logger
  20           0       273          0  0.00%  0.00%  0.00%   0 TTY Background
  21          28       281         99  0.08%  0.00%  0.00%   0 Per-Second Jobs
  22           0         2          0  0.00%  0.00%  0.00%   0 Hawkeye Backgrou
. . .
```

© 2004 Cisco Systems, Inc. All rights reserved. CIT 5.1—5-26



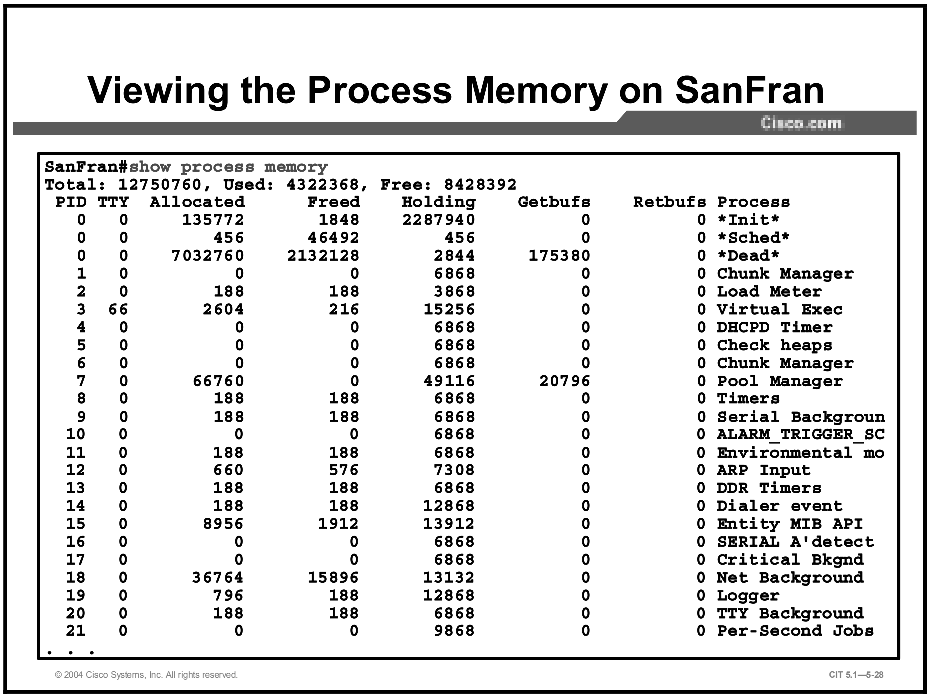
Viewing the Process CPU on SanFran (Cont.)

```
SanFran#show process cpu
CPU utilization for five seconds: 27%/8%; one minute: 38%; five minutes: 24%
 PID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min TTY Process
. . .
  24          20        60        333  0.00%  0.00%  0.00%   0 Net Input
  25           4        61         65  0.00%  0.00%  0.00%   0 Compute load avg
  26          96         6      16000  0.24%  0.02%  0.00%   0 Per-minute Jobs
  27           0         5          0  0.00%  0.00%  0.00%   0 Service-module a
  28           4         2       2000  0.00%  0.00%  0.00%   0 AAA Dictionary R
  29       83552    102890        812 17.26% 22.55% 14.96%   0 IP Input
  30          24        54        444  0.00%  0.00%  0.00%   0 CDP Protocol
  31           0         1          0  0.00%  0.00%  0.00%   0 X.25 Encaps Mana
  32           0         1          0  0.00%  0.00%  0.00%   0 Asy FS Helper
  33           0         1          0  0.00%  0.00%  0.00%   0 PPP IP Add Route
  34          40        36       1111  0.00%  0.00%  0.00%   0 IP Background
  35           8        17        470  0.00%  0.00%  0.00%   0 IP RIB Update
  36           0         6          0  0.00%  0.00%  0.00%   0 Adj Manager
  37           0        22          0  0.00%  0.00%  0.00%   0 TCP Timer
  38           4         3       1333  0.00%  0.00%  0.00%   0 TCP Protocols
  39           0         1          0  0.00%  0.00%  0.00%   0 Probe Input
  40           0         1          0  0.00%  0.00%  0.00%   0 RARP Input
  41           0         1          0  0.00%  0.00%  0.00%   0 HTTP Timer
  42           0         1          0  0.00%  0.00%  0.00%   0 Socket Timers
  43           4         3       1333  0.00%  0.00%  0.00%   0 DHCPD Receive
  44           0         5          0  0.00%  0.00%  0.00%   0 IP Cache Ager
  45           0         1          0  0.00%  0.00%  0.00%   0 COPS
. . .
```

© 2004 Cisco Systems, Inc. All rights reserved. CIT 5.1—5-27

The 5-second CPU utilization is currently 27 percent. This seems reasonable.

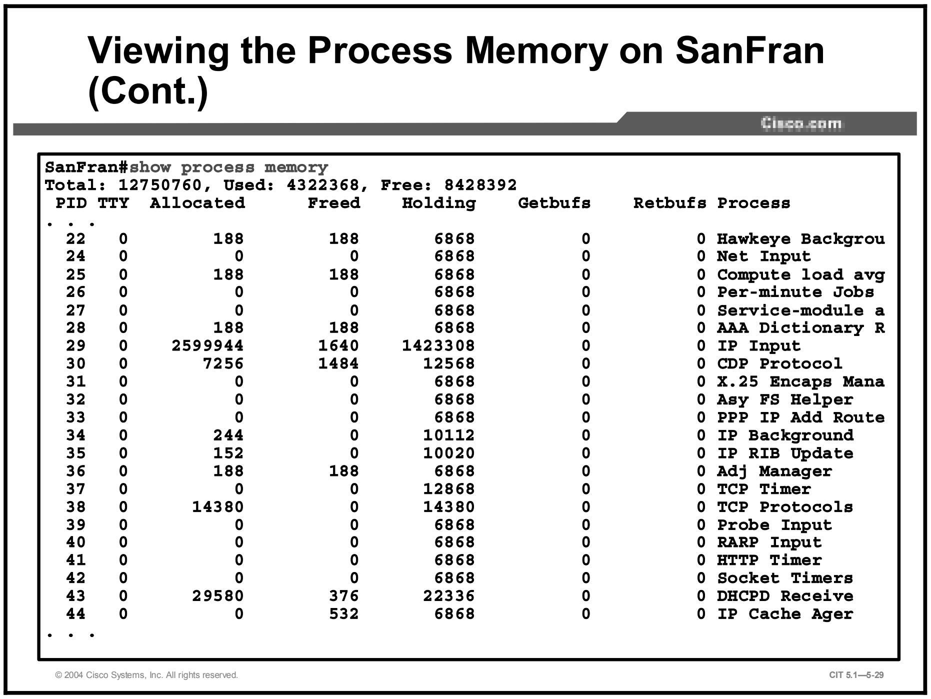
You then use the **show process memory** command to review the process memory utilization on SanFran.



Viewing the Process Memory on SanFran

```
SanFran#show process memory
Total: 12750760, Used: 4322368, Free: 8428392
 PID TTY  Allocated      Freed    Holding    Getbufs    Retbufs Process
   0   0     135772       1848    2287940          0          0 *Init*
   0   0        456      46492        456          0          0 *Sched*
   0   0    7032760    2132128       2844     175380          0 *Dead*
   1   0          0          0       6868          0          0 Chunk Manager
   2   0        188        188       3868          0          0 Load Meter
   3  66       2604        216      15256          0          0 Virtual Exec
   4   0          0          0       6868          0          0 DHCPD Timer
   5   0          0          0       6868          0          0 Check heaps
   6   0          0          0       6868          0          0 Chunk Manager
   7   0      66760          0      49116      20796          0 Pool Manager
   8   0        188        188       6868          0          0 Timers
   9   0        188        188       6868          0          0 Serial Backgroun
  10   0          0          0       6868          0          0 ALARM_TRIGGER_SC
  11   0        188        188       6868          0          0 Environmental mo
  12   0        660        576       7308          0          0 ARP Input
  13   0        188        188       6868          0          0 DDR Timers
  14   0        188        188      12868          0          0 Dialer event
  15   0       8956       1912      13912          0          0 Entity MIB API
  16   0          0          0       6868          0          0 SERIAL A'detect
  17   0          0          0       6868          0          0 Critical Bkgnd
  18   0      36764      15896      13132          0          0 Net Background
  19   0        796        188      12868          0          0 Logger
  20   0        188        188       6868          0          0 TTY Background
  21   0          0          0       9868          0          0 Per-Second Jobs
. . .
```

© 2004 Cisco Systems, Inc. All rights reserved. CIT 5.1—5-28



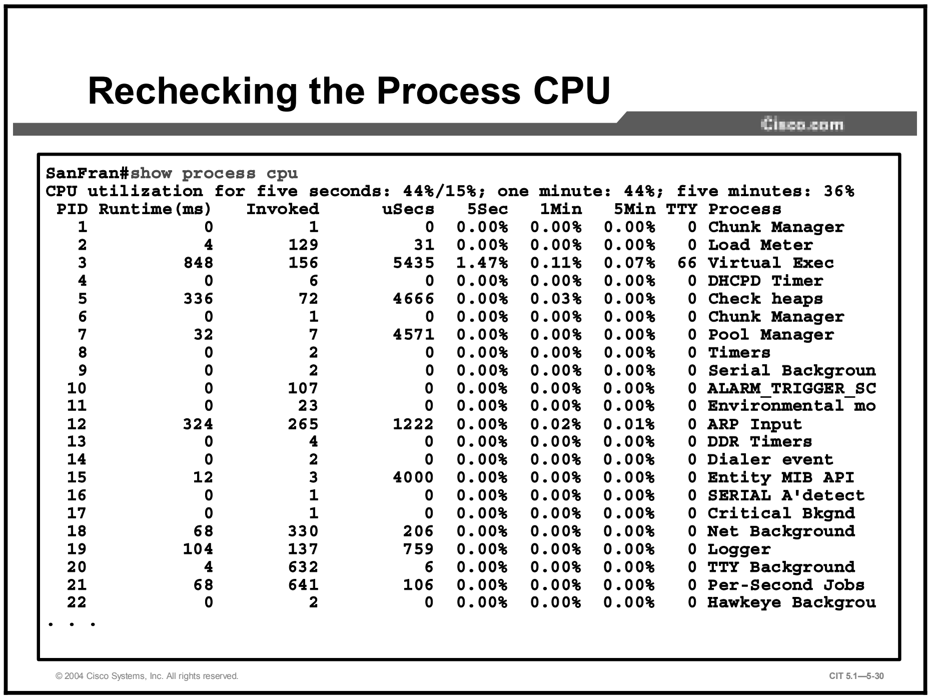
Viewing the Process Memory on SanFran (Cont.)

```
SanFran#show process memory
Total: 12750760, Used: 4322368, Free: 8428392
 PID TTY  Allocated      Freed    Holding    Getbufs    Retbufs Process
. . .
  22   0        188        188       6868          0          0 Hawkeye Backgrou
  24   0          0          0       6868          0          0 Net Input
  25   0        188        188       6868          0          0 Compute load avg
  26   0          0          0       6868          0          0 Per-minute Jobs
  27   0          0          0       6868          0          0 Service-module a
  28   0        188        188       6868          0          0 AAA Dictionary R
  29   0    2599944       1640    1423308          0          0 IP Input
  30   0       7256       1484      12568          0          0 CDP Protocol
  31   0          0          0       6868          0          0 X.25 Encaps Mana
  32   0          0          0       6868          0          0 Asy FS Helper
  33   0          0          0       6868          0          0 PPP IP Add Route
  34   0        244          0      10112          0          0 IP Background
  35   0        152          0      10020          0          0 IP RIB Update
  36   0        188        188       6868          0          0 Adj Manager
  37   0          0          0      12868          0          0 TCP Timer
  38   0      14380          0      14380          0          0 TCP Protocols
  39   0          0          0       6868          0          0 Probe Input
  40   0          0          0       6868          0          0 RARP Input
  41   0          0          0       6868          0          0 HTTP Timer
  42   0          0          0       6868          0          0 Socket Timers
  43   0      29580        376      22336          0          0 DHCPD Receive
  44   0          0        532       6868          0          0 IP Cache Ager
. . .
```

© 2004 Cisco Systems, Inc. All rights reserved. CIT 5.1—5-29

SanFran is using about one-third of its memory, which is workable, as well. You consider the issues.

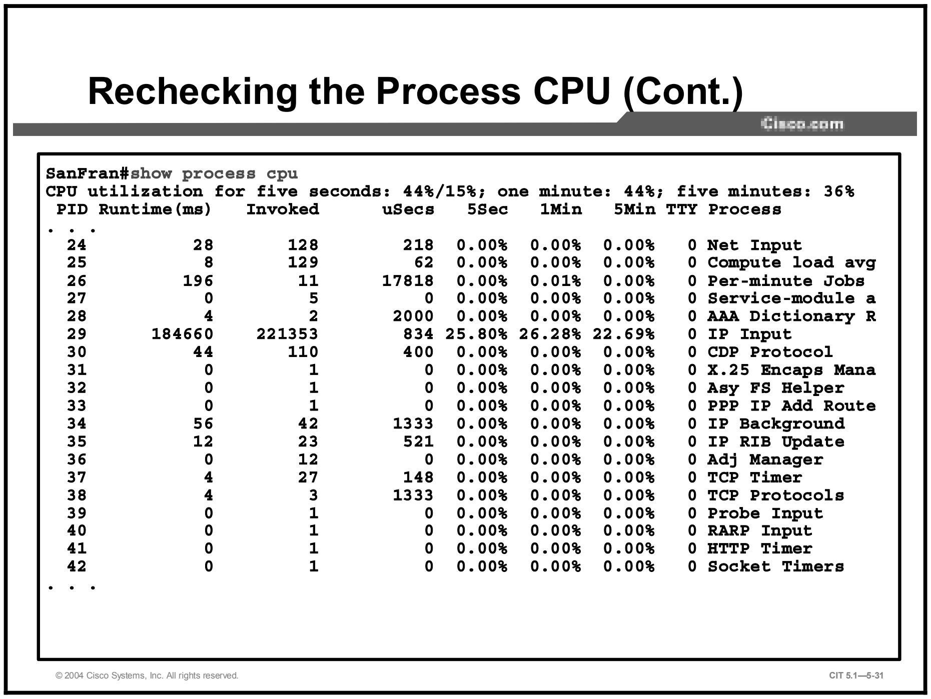
After a few minutes, you review the current process CPU utilization on SanFran.



Rechecking the Process CPU

```
SanFran#show process cpu
CPU utilization for five seconds: 44%/15%; one minute: 44%; five minutes: 36%
 PID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min TTY Process
   1           0         1          0  0.00%  0.00%  0.00%   0 Chunk Manager
   2           4       129         31  0.00%  0.00%  0.00%   0 Load Meter
   3         848       156       5435  1.47%  0.11%  0.07%  66 Virtual Exec
   4           0         6          0  0.00%  0.00%  0.00%   0 DHCPD Timer
   5         336        72       4666  0.00%  0.03%  0.00%   0 Check heaps
   6           0         1          0  0.00%  0.00%  0.00%   0 Chunk Manager
   7          32         7       4571  0.00%  0.00%  0.00%   0 Pool Manager
   8           0         2          0  0.00%  0.00%  0.00%   0 Timers
   9           0         2          0  0.00%  0.00%  0.00%   0 Serial Backgroun
  10           0       107          0  0.00%  0.00%  0.00%   0 ALARM_TRIGGER_SC
  11           0        23          0  0.00%  0.00%  0.00%   0 Environmental mo
  12         324       265       1222  0.00%  0.02%  0.01%   0 ARP Input
  13           0         4          0  0.00%  0.00%  0.00%   0 DDR Timers
  14           0         2          0  0.00%  0.00%  0.00%   0 Dialer event
  15          12         3       4000  0.00%  0.00%  0.00%   0 Entity MIB API
  16           0         1          0  0.00%  0.00%  0.00%   0 SERIAL A'detect
  17           0         1          0  0.00%  0.00%  0.00%   0 Critical Bkgnd
  18          68       330        206  0.00%  0.00%  0.00%   0 Net Background
  19         104       137        759  0.00%  0.00%  0.00%   0 Logger
  20           4       632          6  0.00%  0.00%  0.00%   0 TTY Background
  21          68       641        106  0.00%  0.00%  0.00%   0 Per-Second Jobs
  22           0         2          0  0.00%  0.00%  0.00%   0 Hawkeye Backgrou
. . .
```

CIT 5.1—5-30



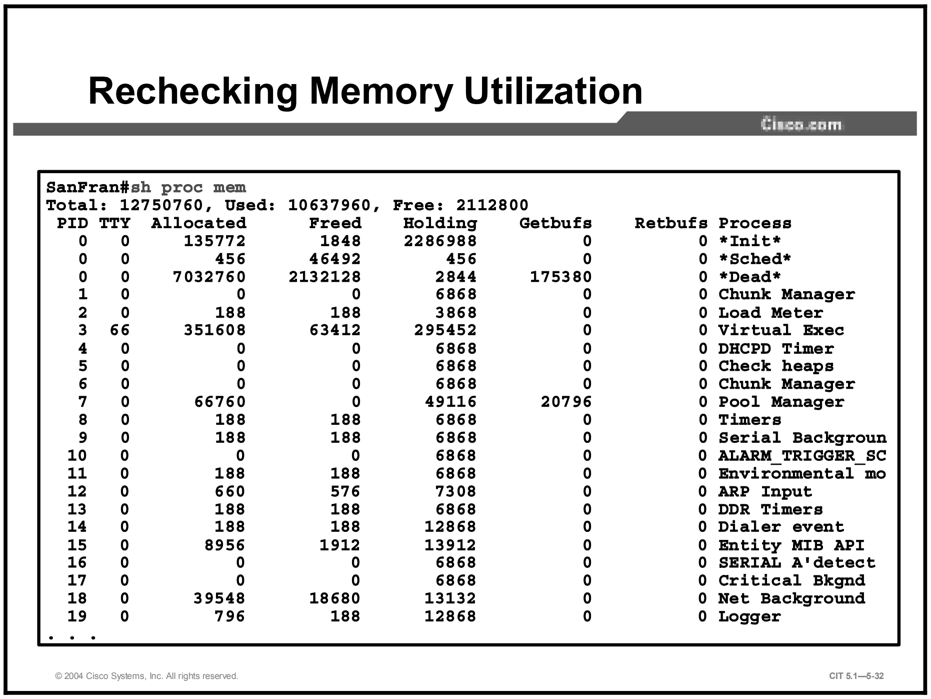
Rechecking the Process CPU (Cont.)

```
SanFran#show process cpu
CPU utilization for five seconds: 44%/15%; one minute: 44%; five minutes: 36%
 PID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min TTY Process
. . .
  24          28       128        218  0.00%  0.00%  0.00%   0 Net Input
  25           8       129         62  0.00%  0.00%  0.00%   0 Compute load avg
  26         196        11      17818  0.00%  0.01%  0.00%   0 Per-minute Jobs
  27           0         5          0  0.00%  0.00%  0.00%   0 Service-module a
  28           4         2       2000  0.00%  0.00%  0.00%   0 AAA Dictionary R
  29      184660    221353        834 25.80% 26.28% 22.69%   0 IP Input
  30          44       110        400  0.00%  0.00%  0.00%   0 CDP Protocol
  31           0         1          0  0.00%  0.00%  0.00%   0 X.25 Encaps Mana
  32           0         1          0  0.00%  0.00%  0.00%   0 Asy FS Helper
  33           0         1          0  0.00%  0.00%  0.00%   0 PPP IP Add Route
  34          56        42       1333  0.00%  0.00%  0.00%   0 IP Background
  35          12        23        521  0.00%  0.00%  0.00%   0 IP RIB Update
  36           0        12          0  0.00%  0.00%  0.00%   0 Adj Manager
  37           4        27        148  0.00%  0.00%  0.00%   0 TCP Timer
  38           4         3       1333  0.00%  0.00%  0.00%   0 TCP Protocols
  39           0         1          0  0.00%  0.00%  0.00%   0 Probe Input
  40           0         1          0  0.00%  0.00%  0.00%   0 RARP Input
  41           0         1          0  0.00%  0.00%  0.00%   0 HTTP Timer
  42           0         1          0  0.00%  0.00%  0.00%   0 Socket Timers
. . .
```

CIT 5.1—5-31

You start to look closer. Your process CPU utilization has jumped to 44 percent for 5 seconds.

You review the current process memory utilization.

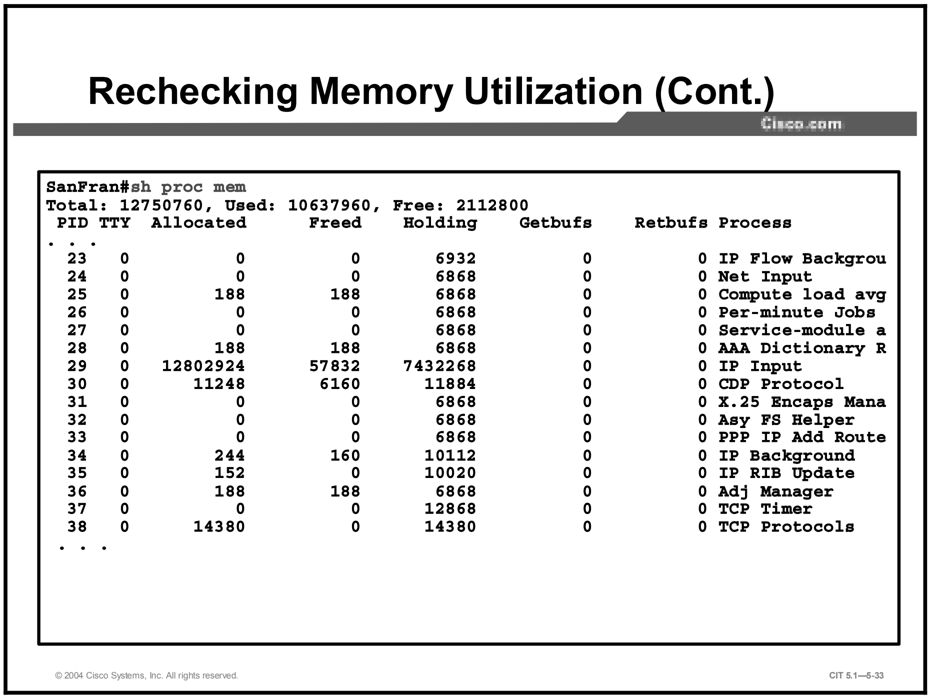


Rechecking Memory Utilization

```
SanFran#sh proc mem
Total: 12750760, Used: 10637960, Free: 2112800
 PID TTY  Allocated      Freed    Holding    Getbufs    Retbufs Process
   0   0     135772       1848    2286988          0          0 *Init*
   0   0        456      46492        456          0          0 *Sched*
   0   0    7032760    2132128       2844     175380          0 *Dead*
   1   0          0          0       6868          0          0 Chunk Manager
   2   0        188        188       3868          0          0 Load Meter
   3  66     351608      63412     295452          0          0 Virtual Exec
   4   0          0          0       6868          0          0 DHCPD Timer
   5   0          0          0       6868          0          0 Check heaps
   6   0          0          0       6868          0          0 Chunk Manager
   7   0      66760          0      49116      20796          0 Pool Manager
   8   0        188        188       6868          0          0 Timers
   9   0        188        188       6868          0          0 Serial Backgroun
  10   0          0          0       6868          0          0 ALARM_TRIGGER_SC
  11   0        188        188       6868          0          0 Environmental mo
  12   0        660        576       7308          0          0 ARP Input
  13   0        188        188       6868          0          0 DDR Timers
  14   0        188        188      12868          0          0 Dialer event
  15   0       8956       1912      13912          0          0 Entity MIB API
  16   0          0          0       6868          0          0 SERIAL A'detect
  17   0          0          0       6868          0          0 Critical Bkgnd
  18   0      39548      18680      13132          0          0 Net Background
  19   0        796        188      12868          0          0 Logger
. . .
```

© 2004 Cisco Systems, Inc. All rights reserved.

CIT 5.1—5-32



Rechecking Memory Utilization (Cont.)

```
SanFran#sh proc mem
Total: 12750760, Used: 10637960, Free: 2112800
 PID TTY  Allocated      Freed    Holding    Getbufs    Retbufs Process
. . .
  23   0          0          0       6932          0          0 IP Flow Backgrou
  24   0          0          0       6868          0          0 Net Input
  25   0        188        188       6868          0          0 Compute load avg
  26   0          0          0       6868          0          0 Per-minute Jobs
  27   0          0          0       6868          0          0 Service-module a
  28   0        188        188       6868          0          0 AAA Dictionary R
  29   0   12802924      57832    7432268          0          0 IP Input
  30   0      11248       6160      11884          0          0 CDP Protocol
  31   0          0          0       6868          0          0 X.25 Encaps Mana
  32   0          0          0       6868          0          0 Asy FS Helper
  33   0          0          0       6868          0          0 PPP IP Add Route
  34   0        244        160      10112          0          0 IP Background
  35   0        152          0      10020          0          0 IP RIB Update
  36   0        188        188       6868          0          0 Adj Manager
  37   0          0          0      12868          0          0 TCP Timer
  38   0      14380          0      14380          0          0 TCP Protocols
 . . .
```

© 2004 Cisco Systems, Inc. All rights reserved.

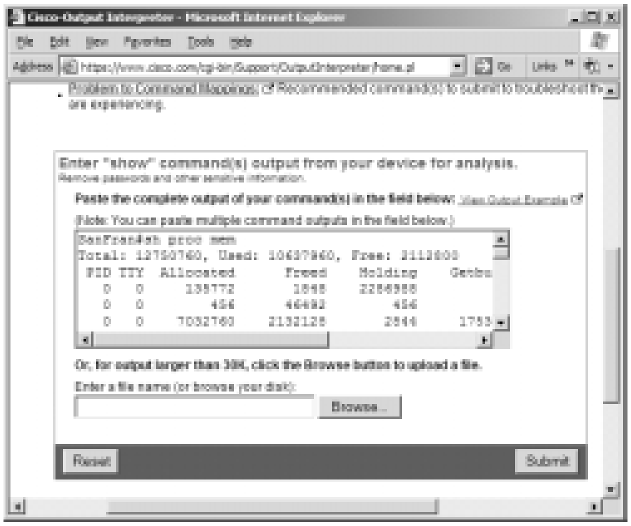
CIT 5.1—5-33

SanFran is rapidly consuming its free memory. Could this indicate a serious issue?

You decide to capture the latest command output and go to Cisco.com to run it through the Output Interpreter.

Sending Results to Cisco Systems Output Interpreter

Cisco.com



Cisco-Output Interpreter - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address https://www.cisco.com/cgi-bin/Support/OutputInterpreter/home.pl
Go
Links

- Problem to Command Mappings: Recommended command(s) to submit to troubleshoot th... are experiencing.

Enter "show" command(s) output from your device for analysis.
Remove passwords and other sensitive information.

Paste the complete output of your command(s) in the field below: View Output Example

(Note: You can paste multiple command outputs in the field below.)

```
SanFran4sh proc mem
Total: 12750760, Used: 10637960, Free: 2112800
 PID TTY  Allocated      Freed    Holding    Getbu
   0   0     135772       1848    2286588
   0   0        456      46492        456
   0   0    7032760    2132128       2544      1753
```

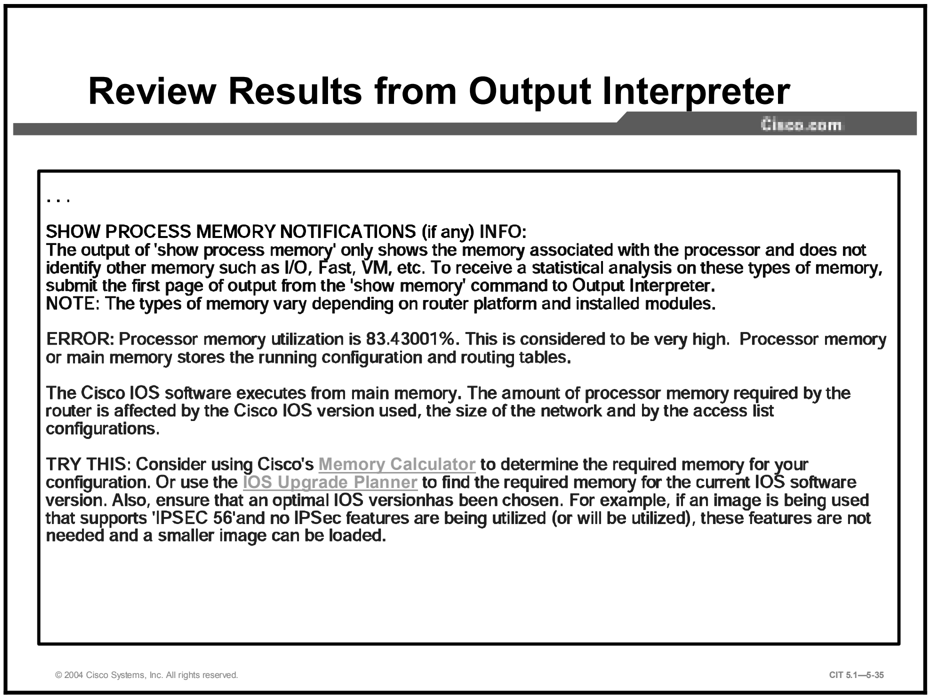
Or, for output larger than 30K, click the Browse button to upload a file.

Enter a file name (or browse your disk):

CIT 5.1—5-34

Note The actual navigation steps to get to this screen are not shown. You need to go to http://www.cisco.com and then go to the Output Interpreter tool under Support.

You review the results.



Review Results from Output Interpreter

. . .

SHOW PROCESS MEMORY NOTIFICATIONS (if any) INFO:
The output of 'show process memory' only shows the memory associated with the processor and does not identify other memory such as I/O, Fast, VM, etc. To receive a statistical analysis on these types of memory, submit the first page of output from the 'show memory' command to Output Interpreter.
NOTE: The types of memory vary depending on router platform and installed modules.

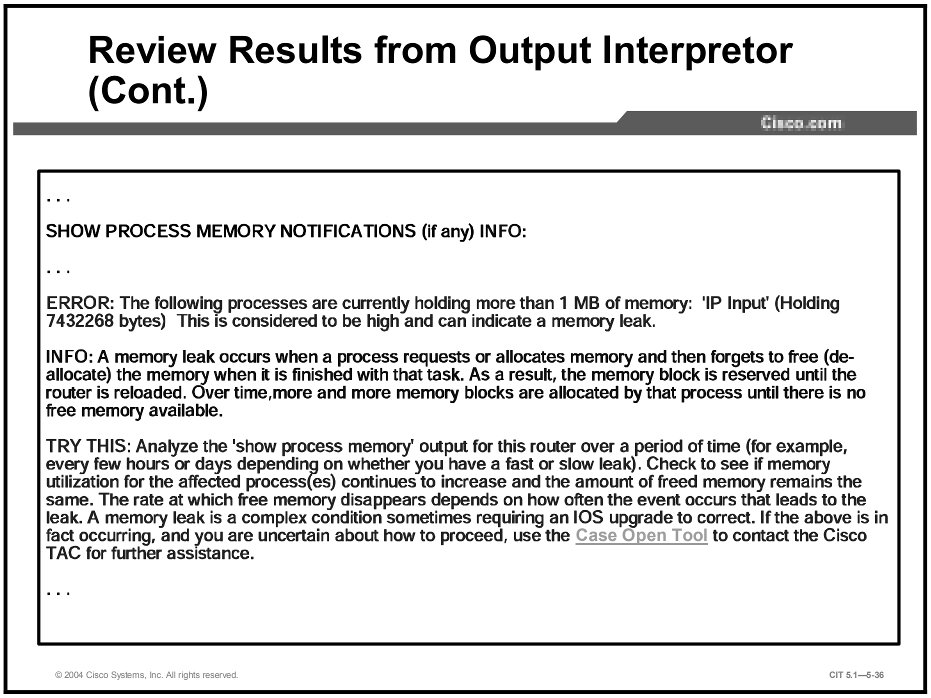
ERROR: Processor memory utilization is 83.43001%. This is considered to be very high. Processor memory or main memory stores the running configuration and routing tables.

The Cisco IOS software executes from main memory. The amount of processor memory required by the router is affected by the Cisco IOS version used, the size of the network and by the access list configurations.

TRY THIS: Consider using Cisco's Memory Calculator to determine the required memory for your configuration. Or use the IOS Upgrade Planner to find the required memory for the current IOS software version. Also, ensure that an optimal IOS versionhas been chosen. For example, if an image is being used that supports 'IPSEC 56'and no IPSec features are being utilized (or will be utilized), these features are not needed and a smaller image can be loaded.

CIT 5.1—5-35

The Output Interpreter agrees that the memory utilization on SanFran is very high. You scroll down for additional results.



Review Results from Output Interpretor (Cont.)

. . .

SHOW PROCESS MEMORY NOTIFICATIONS (if any) INFO:

. . .

ERROR: The following processes are currently holding more than 1 MB of memory: 'IP Input' (Holding 7432268 bytes) This is considered to be high and can indicate a memory leak.

INFO: A memory leak occurs when a process requests or allocates memory and then forgets to free (de-allocate) the memory when it is finished with that task. As a result, the memory block is reserved until the router is reloaded. Over time,more and more memory blocks are allocated by that process until there is no free memory available.

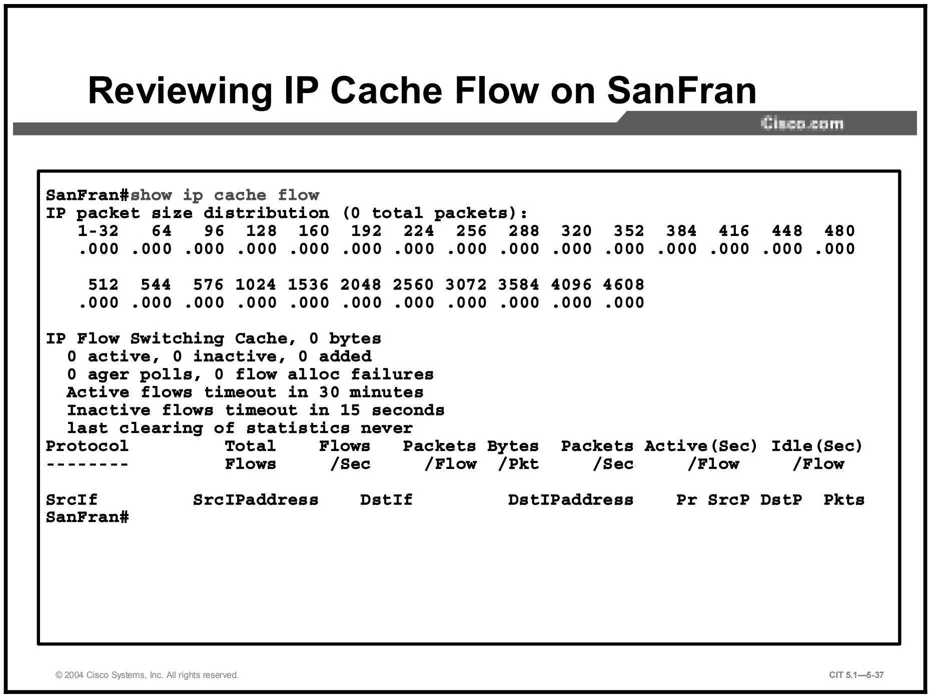
TRY THIS: Analyze the 'show process memory' output for this router over a period of time (for example, every few hours or days depending on whether you have a fast or slow leak). Check to see if memory utilization for the affected process(es) continues to increase and the amount of freed memory remains the same. The rate at which free memory disappears depends on how often the event occurs that leads to the leak. A memory leak is a complex condition sometimes requiring an IOS upgrade to correct. If the above is in fact occurring, and you are uncertain about how to proceed, use the Case Open Tool to contact the Cisco TAC for further assistance.

. . .

CIT 5.1—5-36

The Output Interpreter notes that IP input is consuming a lot of resources. The Output Interpreter also suggests that SanFran might have a memory leak. You know that SanFran has a fast leak, because memory is being quickly consumed.

You go back to your console screen and try the **show ip cache flow** command to review IP traffic flows on SanFran.



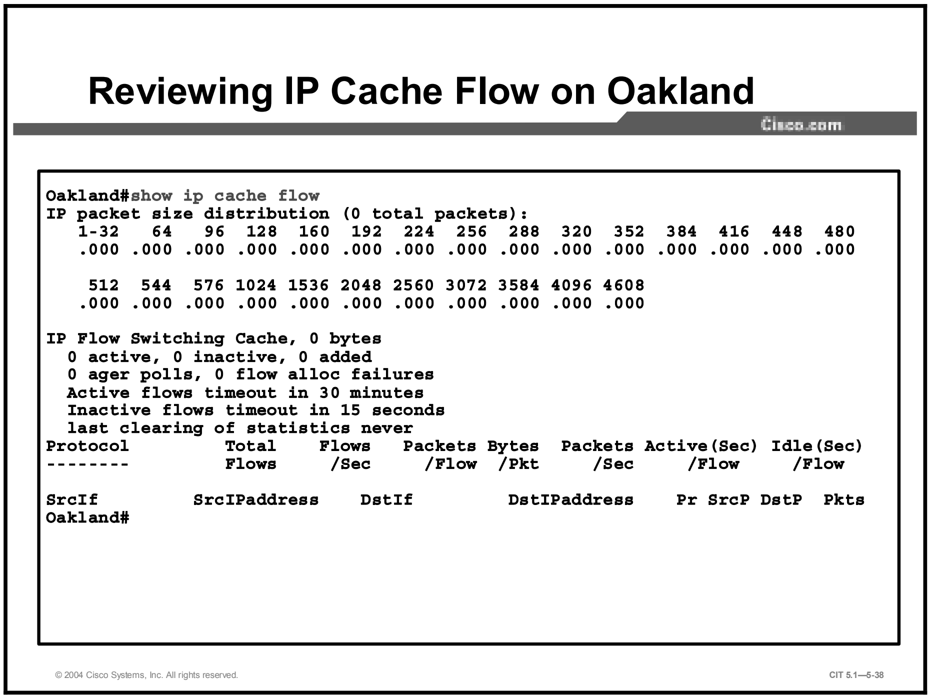
Reviewing IP Cache Flow on SanFran

```
SanFran#show ip cache flow
IP packet size distribution (0 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000

    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 0 bytes
  0 active, 0 inactive, 0 added
  0 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
  last clearing of statistics never
Protocol         Total    Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------         Flows     /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
SanFran#
```

© 2004 Cisco Systems, Inc. All rights reserved. CIT 5.1—5-37

Because the output does not show any packets in the packet size distribution, you realize that cache flow switching has not been configured on any interfaces.

You try to review IP traffic flows on Oakland.



Reviewing IP Cache Flow on Oakland

```
Oakland#show ip cache flow
IP packet size distribution (0 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000

    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 0 bytes
  0 active, 0 inactive, 0 added
  0 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
  last clearing of statistics never
Protocol         Total    Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------         Flows     /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Oakland#
```

© 2004 Cisco Systems, Inc. All rights reserved.

CIT 5.1—5-38

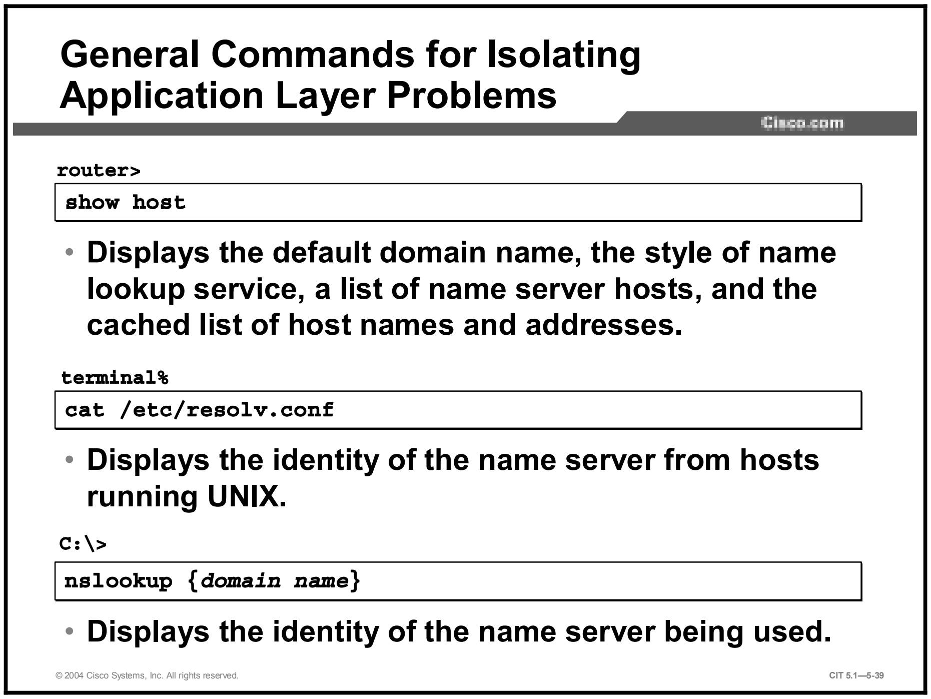
Cache flow switching has not been configured on Oakland either.

You know that you have a fast memory leak on SanFran; therefore, in the longer term, you need to upgrade the IOS image. In the very short term, you want to determine what is causing the leak.

Note	A misconfigured network device does not cause this issue. This example will be continued in the next module.

Analyzing Commands and Applications Used to Isolate Problems Occurring at the Application Layer

This topic identifies the output of commands and applications with the purpose of helping troubleshooters isolate a problem at the application layer.



General Commands for Isolating Application Layer Problems

router>

```
show host
```

- **Displays the default domain name, the style of name lookup service, a list of name server hosts, and the cached list of host names and addresses.**

terminal%

```
cat /etc/resolv.conf
```

- **Displays the identity of the name server from hosts running UNIX.**

C:\>

```
nslookup {domain name}
```

- **Displays the identity of the name server being used.**

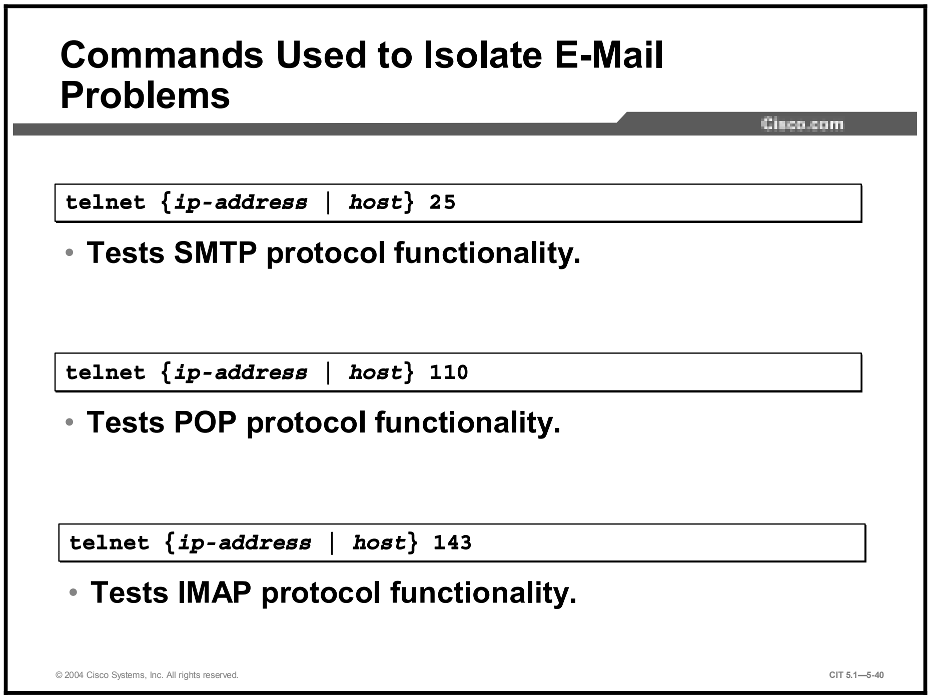
CIT 5.1—5-39

The table shows commands that a troubleshooter uses to isolate problems at the application layer. Although many of the commands also display information that concerns other layers, these commands are noteworthy at the application layer because they highlight problems in the interface between the transport and application layers.

General Commands for Isolating Application Layer Problems

Command	Description
show host	Displays the default domain name, the style of name lookup service, a list of name server hosts, and the cached list of host names and addresses.
cat /etc/resolv.conf	Displays the identity of the name server from hosts running UNIX.
ifconfig -a	Displays IP information for UNIX and Mac OS X hosts.
ipconfig /all	Displays IP information for hosts running Windows NT, 2000, or XP.
traceroute *[destination]*	Identifies the path that a packet takes through the network. The *destination* variable is the host name or IP address of the target system. This command is used with Cisco IOS, UNIX, and Mac OS X.
tracert *[destination]*	Verifies connectivity to a destination device for Windows hosts. The *destination* variable is the IP alias or IP address of the target system.
winipcfg	Displays IP information for hosts running Windows 9x and Me.
nslookup {*domain name*}	Displays the identity of the name server being used.
ping {*ip-address* | *domain name*}	Verifies connectivity and tests the functionality of address resolution services.

Note Not all of the commands listed are available on some versions of Cisco operating systems. To determine which commands are available for use with your devices, consult the online documentation for Cisco devices at http://www.cisco.com/univercd/home/home.htm.



Commands Used to Isolate E-Mail Problems

```
telnet {ip-address | host} 25
```

- **Tests SMTP protocol functionality.**

```
telnet {ip-address | host} 110
```

- **Tests POP protocol functionality.**

```
telnet {ip-address | host} 143
```

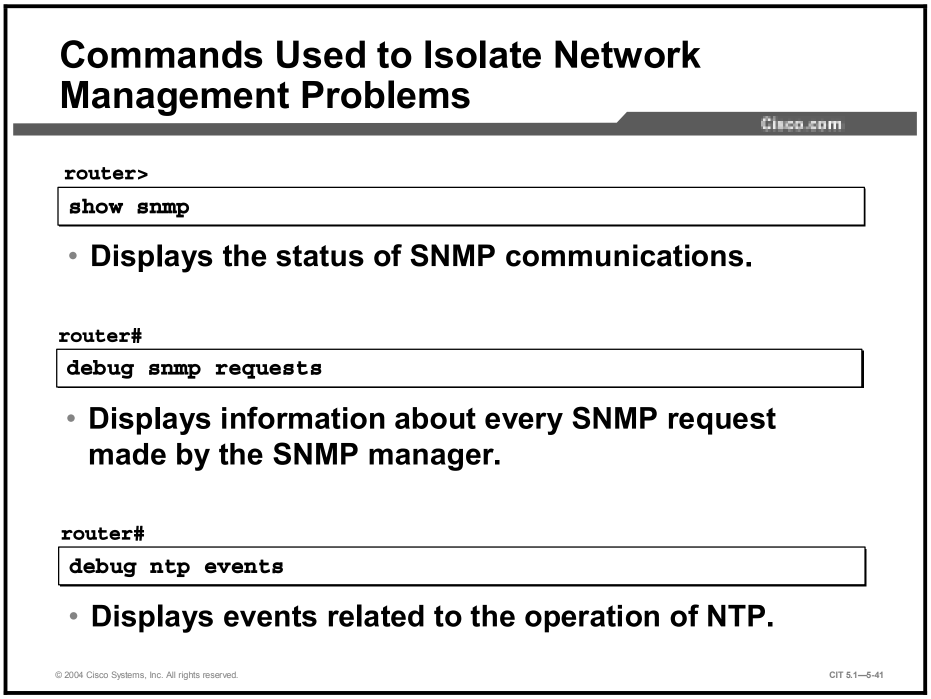
- **Tests IMAP protocol functionality.**

CIT 5.1—5-40

The commands listed in the table display information about the e-mail network application. A troubleshooter uses the information from these commands to isolate problems at the application layer that are related to e-mail and the Post Office Protocol – Version 3 (POP3), Simple Mail Transfer Protocol (SMTP), and Internet Message Access Protocol (IMAP) protocols.

Commands Used to Isolate E-Mail Problems

Command	Description
telnet {*ip-address* | *host*} **25**	Tests SMTP protocol functionality.
telnet {*ip-address* | *host*} **110**	Tests POP protocol functionality.
telnet {*ip-address* | *host*} **143**	Tests IMAP protocol functionality.



Commands Used to Isolate Network Management Problems

```
router>
show snmp
```

- Displays the status of SNMP communications.

```
router#
debug snmp requests
```

- Displays information about every SNMP request made by the SNMP manager.

```
router#
debug ntp events
```

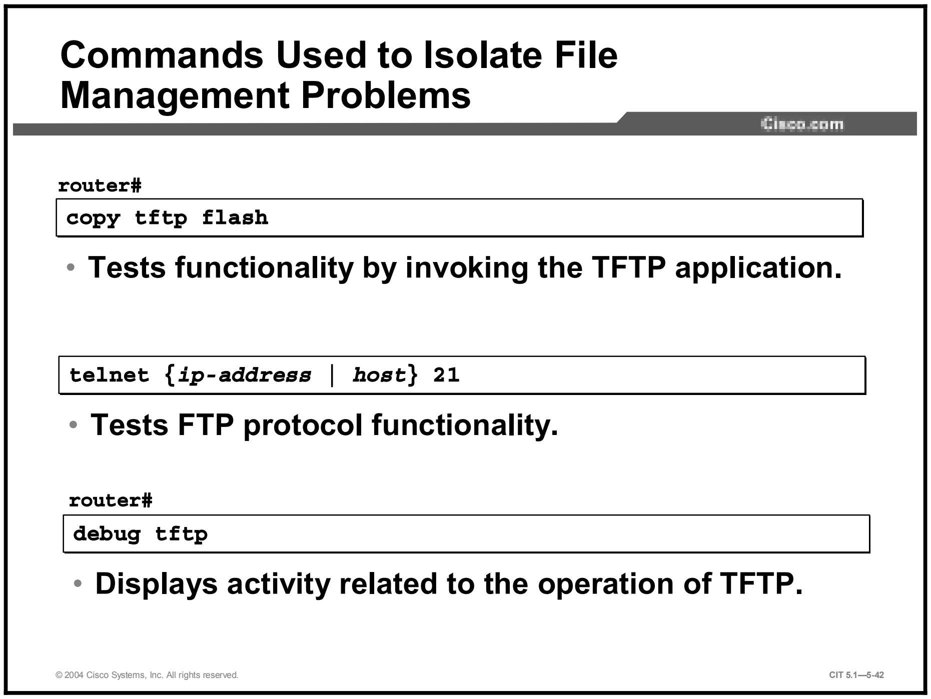
- Displays events related to the operation of NTP.

CIT 5.1—5-41

The commands listed in the table display information about network management applications. A troubleshooter uses the information from these commands to isolate problems at the application layer that are related to the Simple Network Management Protocol (SNMP) and Network Time Protocol (NTP).

Commands Used to Isolate Network Management Problems

Command	Description
show snmp	Displays the status of SNMP communications.
debug snmp requests	Displays information about every SNMP request made by the SNMP manager.
debug ntp events	Displays events related to the operation of NTP.



Commands Used to Isolate File Management Problems

```
router#
copy tftp flash
```

- **Tests functionality by invoking the TFTP application.**

```
telnet {ip-address | host} 21
```

- **Tests FTP protocol functionality.**

```
router#
debug tftp
```

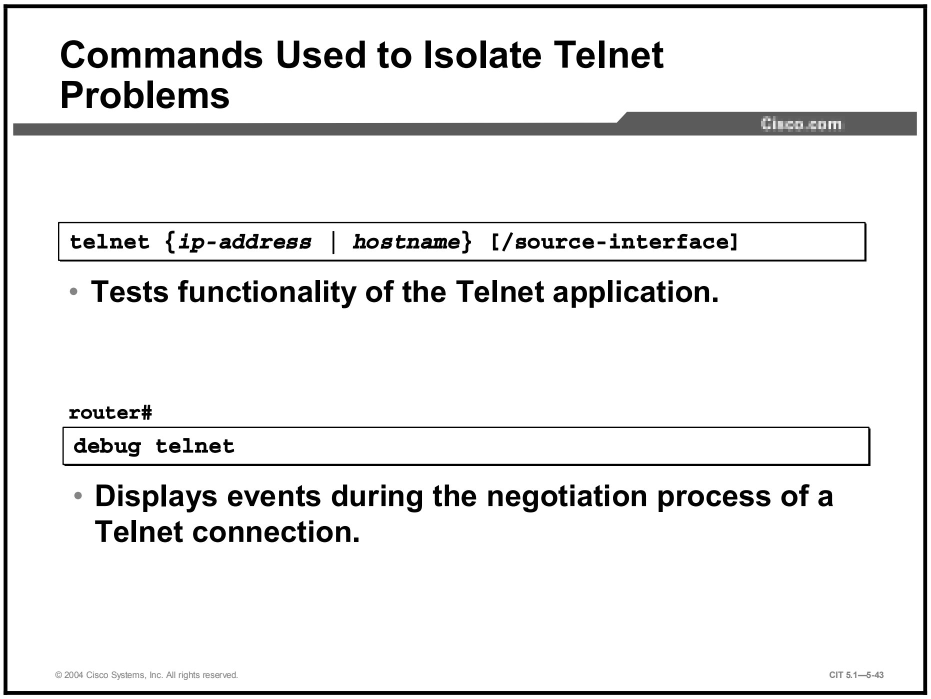
- **Displays activity related to the operation of TFTP.**

CIT 5.1—5-42

The commands listed in the table display information about file management applications. A troubleshooter uses the information from these commands to isolate problems at the application layer that are related to FTP and TFTP.

Commands Used to Isolate File Management Problems

Command	Description
copy tftp flash	Tests functionality by invoking the TFTP application.
telnet {*ip-address* | *host*} **21**	Tests FTP protocol functionality.
debug tftp	Displays activity related to the operation of TFTP.



Commands Used to Isolate Telnet Problems

```
telnet {ip-address | hostname} [/source-interface]
```

- **Tests functionality of the Telnet application.**

```
router#
debug telnet
```

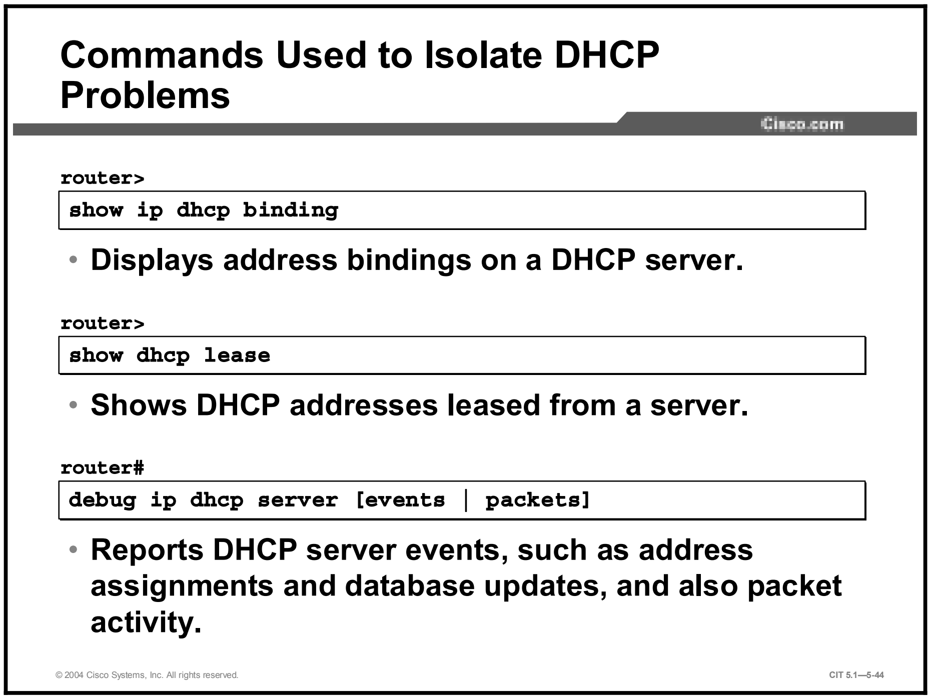
- **Displays events during the negotiation process of a Telnet connection.**

CIT 5.1—5-43

The commands listed in the table display information about the Telnet application. A troubleshooter uses the information from these commands to isolate problems at the application layer that are related to the Telnet application.

Commands Used to Isolate Telnet Problems

Command	Description
telnet {*ip-address* | *hostname*} [/source-interface]	Tests functionality of the Telnet application.
debug telnet	Displays events during the negotiation process of a Telnet connection.



Commands Used to Isolate DHCP Problems

Cisco.com

router>

```
show ip dhcp binding
```

- **Displays address bindings on a DHCP server.**

router>

```
show dhcp lease
```

- **Shows DHCP addresses leased from a server.**

router#

```
debug ip dhcp server [events | packets]
```

- **Reports DHCP server events, such as address assignments and database updates, and also packet activity.**

CIT 5.1—5-44

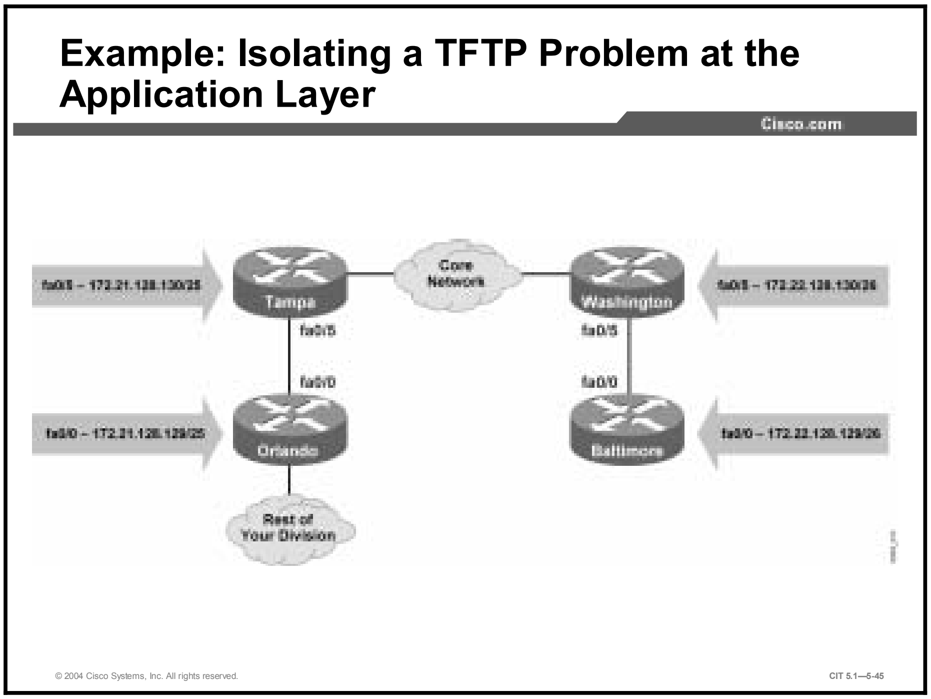
The commands listed in the table display information about the DHCP application. A troubleshooter uses the information from these commands to isolate problems at the application layer that are related to the Telnet application.

Commands Used to Isolate DHCP Problems

Command	Description
show ip dhcp binding	Displays address bindings on a DHCP server.
show dhcp lease	Shows DHCP addresses leased from a server.
debug ip dhcp server [events | packets]	Reports DHCP server events, such as address assignments and database updates, and also packet activity.

Example: Isolating a TFTP Problem at the Application Layer

You are the second-level network engineer for Orlando. You have console access to the distribution router named Orlando and IP connectivity to all other devices in your division. Your division supports the 172.21.0.0/16 subnet.



Example: Isolating a TFTP Problem at the Application Layer

Cisco.com
fa0/5 – 172.21.128.130/25
Tampa
Core Network
Washington
fa0/5 – 172.22.128.130/26
fa0/5
fa0/0
fa0/5
fa0/0
fa0/0 – 172.21.128.129/25
Orlando
Baltimore
fa0/0 – 172.22.128.129/26
Rest of Your Division

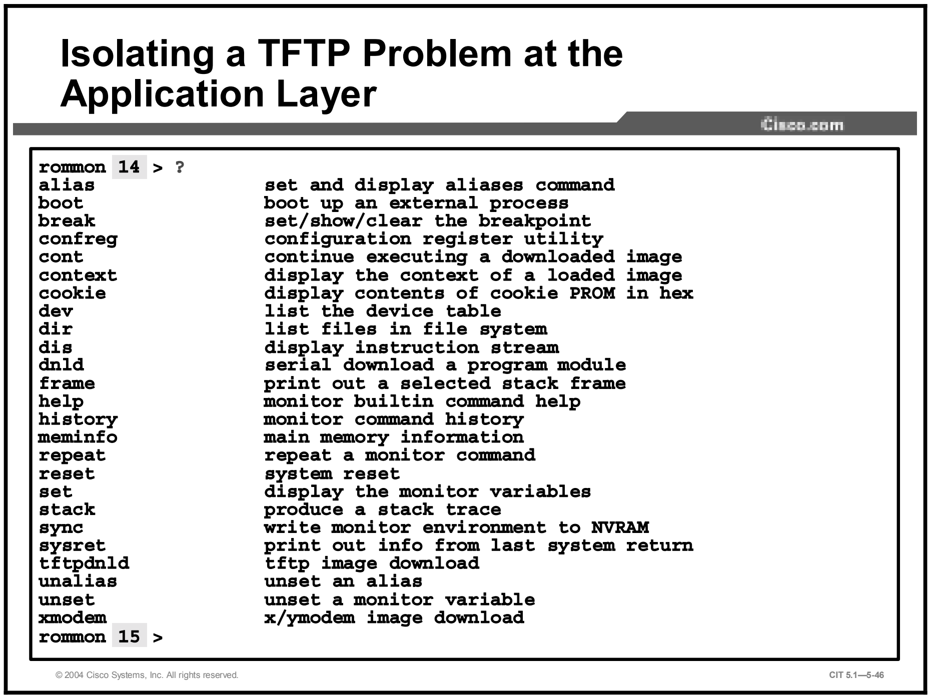
© 2004 Cisco Systems, Inc. All rights reserved.

CIT 5.1—5-45

Juan from Network Operations stops by your office to tell you that, somehow, the Cisco IOS image has been erased from the Orlando router. He was trying to retrieve the image from Baltimore but cannot get TFTP to work.

You know from your base configuration information that there is at least a 100 Mbs Fast Ethernet link between Orlando and Baltimore. Therefore, this would be a good source to use for downloading the Cisco IOS image. You connect to the console port on Orlando to assess the situation.

First, you look at available commands from within ROMMON mode.



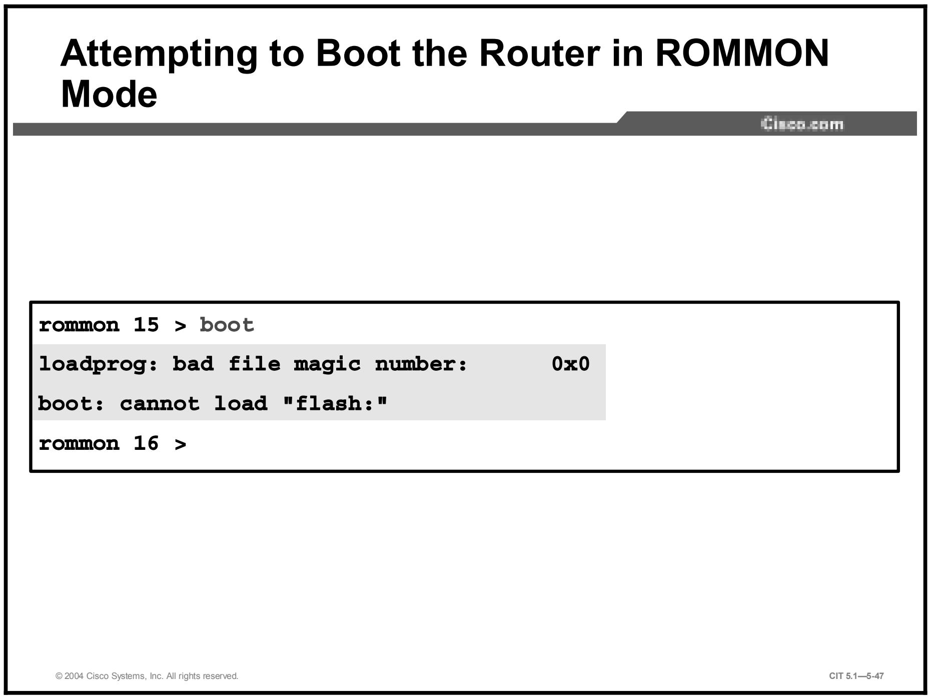
Isolating a TFTP Problem at the Application Layer

```
rommon 14 > ?
alias               set and display aliases command
boot                boot up an external process
break               set/show/clear the breakpoint
confreg             configuration register utility
cont                continue executing a downloaded image
context             display the context of a loaded image
cookie              display contents of cookie PROM in hex
dev                 list the device table
dir                 list files in file system
dis                 display instruction stream
dnld                serial download a program module
frame               print out a selected stack frame
help                monitor builtin command help
history             monitor command history
meminfo             main memory information
repeat              repeat a monitor command
reset               system reset
set                 display the monitor variables
stack               produce a stack trace
sync                write monitor environment to NVRAM
sysret              print out info from last system return
tftpdnld            tftp image download
unalias             unset an alias
unset               unset a monitor variable
xmodem              x/ymodem image download
rommon 15 >
```

CIT 5.1—5-46

You note that the ROMMON prompt is on 14 and 15, which indicates that several commands have already been issued.

Next, you enter the ROMMON **boot** command to try to boot the router in case the Cisco IOS image is not really missing.

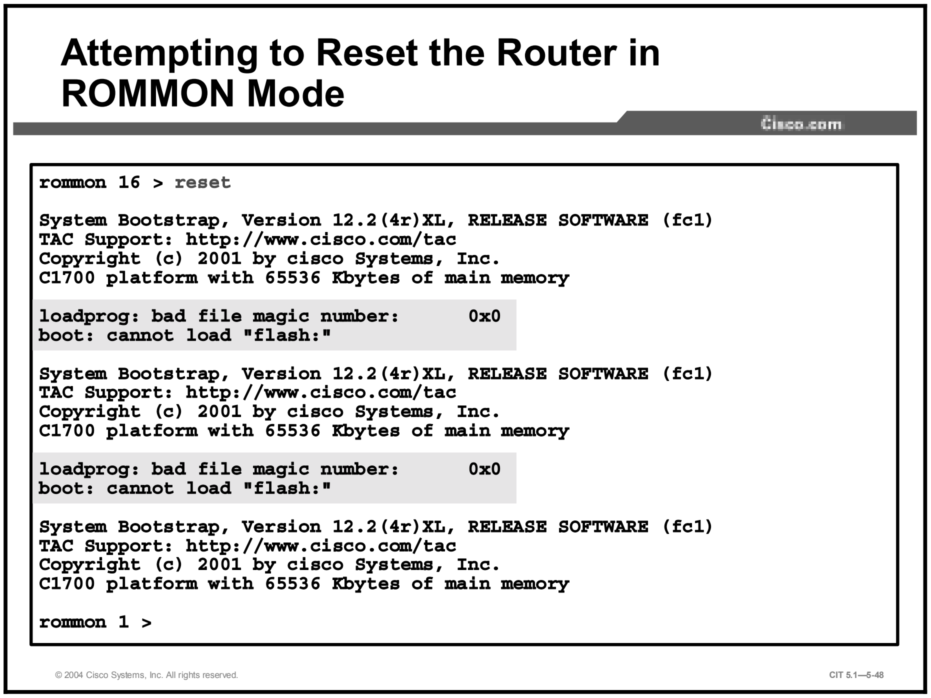


Attempting to Boot the Router in ROMMON Mode

```
rommon 15 > boot
loadprog: bad file magic number:      0x0
boot: cannot load "flash:"
rommon 16 >
```

CIT 5.1—5-47

Entering the **boot** command did not work. You try to **reset t**he router to see if that will restore the IOS image.



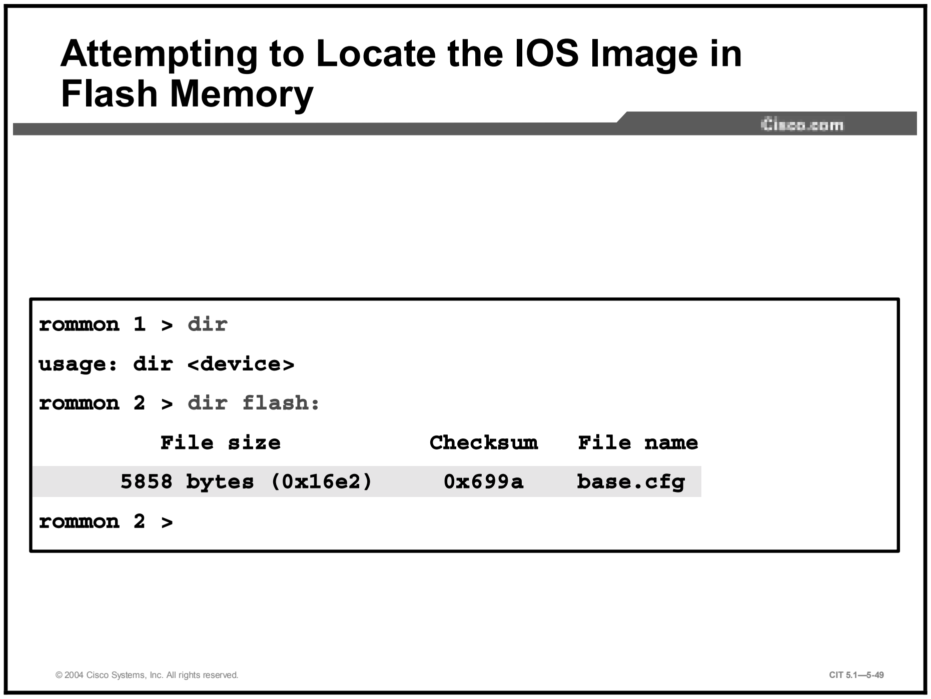
Attempting to Reset the Router in ROMMON Mode

```
rommon 16 > reset

System Bootstrap, Version 12.2(4r)XL, RELEASE SOFTWARE (fc1)
TAC Support: http://www.cisco.com/tac
Copyright (c) 2001 by cisco Systems, Inc.
C1700 platform with 65536 Kbytes of main memory

loadprog: bad file magic number:      0x0
boot: cannot load "flash:"

System Bootstrap, Version 12.2(4r)XL, RELEASE SOFTWARE (fc1)
TAC Support: http://www.cisco.com/tac
Copyright (c) 2001 by cisco Systems, Inc.
C1700 platform with 65536 Kbytes of main memory

loadprog: bad file magic number:      0x0
boot: cannot load "flash:"

System Bootstrap, Version 12.2(4r)XL, RELEASE SOFTWARE (fc1)
TAC Support: http://www.cisco.com/tac
Copyright (c) 2001 by cisco Systems, Inc.
C1700 platform with 65536 Kbytes of main memory

rommon 1 >
```

CIT 5.1—5-48

Entering the **reset** command did not restore the image.

You decide to look for the IOS image in the file system.



Attempting to Locate the IOS Image in Flash Memory

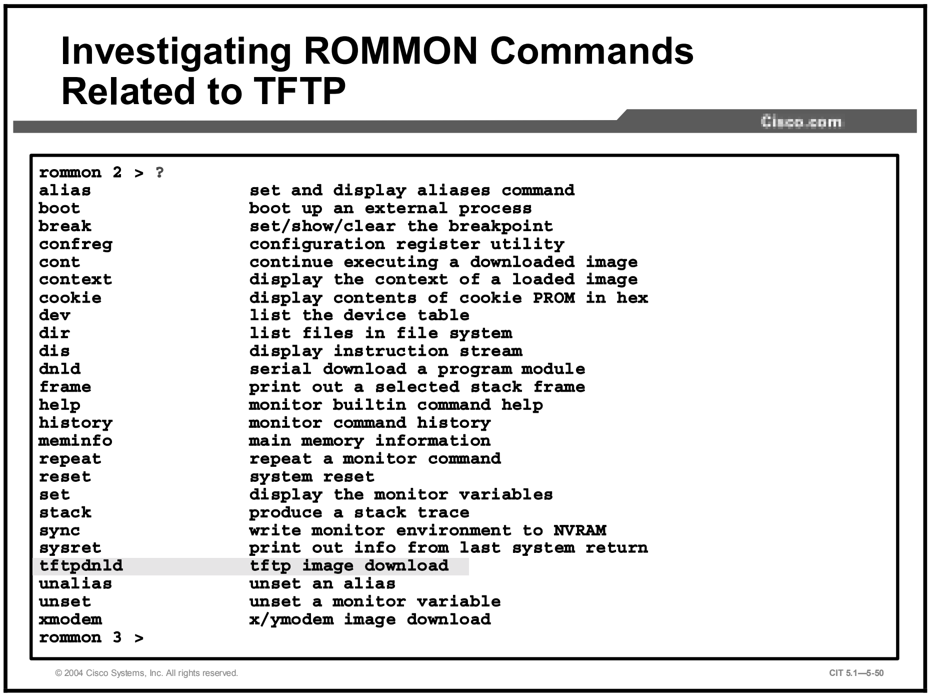
```
rommon 1 > dir
usage: dir <device>
rommon 2 > dir flash:
         File size           Checksum   File name
      5858 bytes (0x16e2)     0x699a    base.cfg
rommon 2 >
```

© 2004 Cisco Systems, Inc. All rights reserved.

CIT 5.1—5-49

Juan is correct; there is no IOS image in Flash memory. At 5858 bytes, base.cfg is not big enough to be an IOS image. You learn from Juan that the image was erased while someone was saving a backup configuration file.

You decide that you really will need to use TFTP to recover the image. You check out the commands available from the ROMMON level.



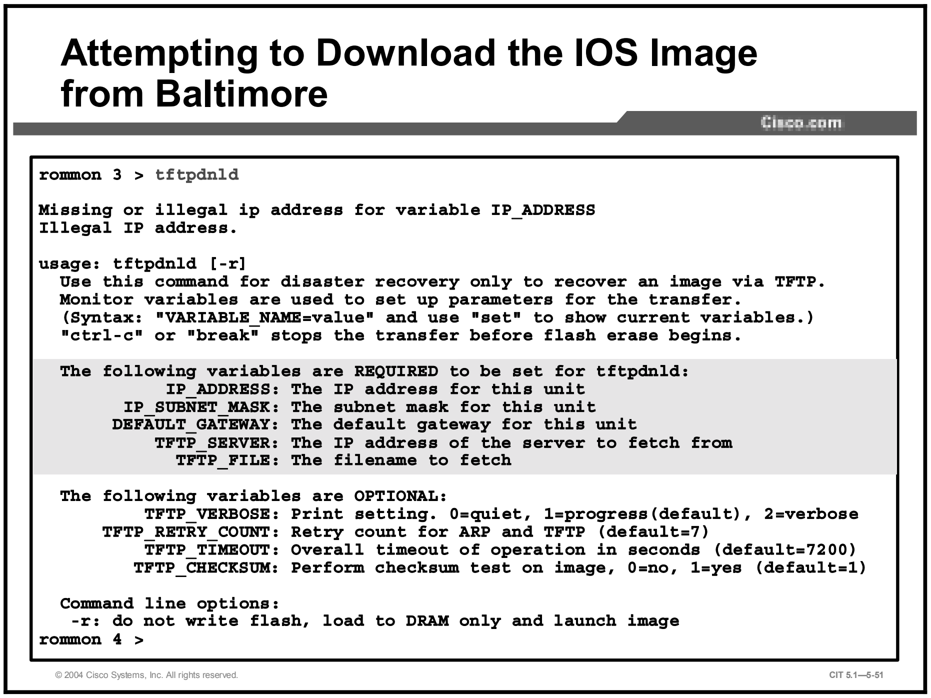
Investigating ROMMON Commands Related to TFTP

```
rommon 2 > ?
alias               set and display aliases command
boot                boot up an external process
break               set/show/clear the breakpoint
confreg             configuration register utility
cont                continue executing a downloaded image
context             display the context of a loaded image
cookie              display contents of cookie PROM in hex
dev                 list the device table
dir                 list files in file system
dis                 display instruction stream
dnld                serial download a program module
frame               print out a selected stack frame
help                monitor builtin command help
history             monitor command history
meminfo             main memory information
repeat              repeat a monitor command
reset               system reset
set                 display the monitor variables
stack               produce a stack trace
sync                write monitor environment to NVRAM
sysret              print out info from last system return
tftpdnld            tftp image download
unalias             unset an alias
unset               unset a monitor variable
xmodem              x/ymodem image download
rommon 3 >
```

© 2004 Cisco Systems, Inc. All rights reserved.

CIT 5.1—5-50

You decide that **tftpdnld** is the command that you will need to download the image from Baltimore. You enter the **tftpdnld** command.



Attempting to Download the IOS Image from Baltimore

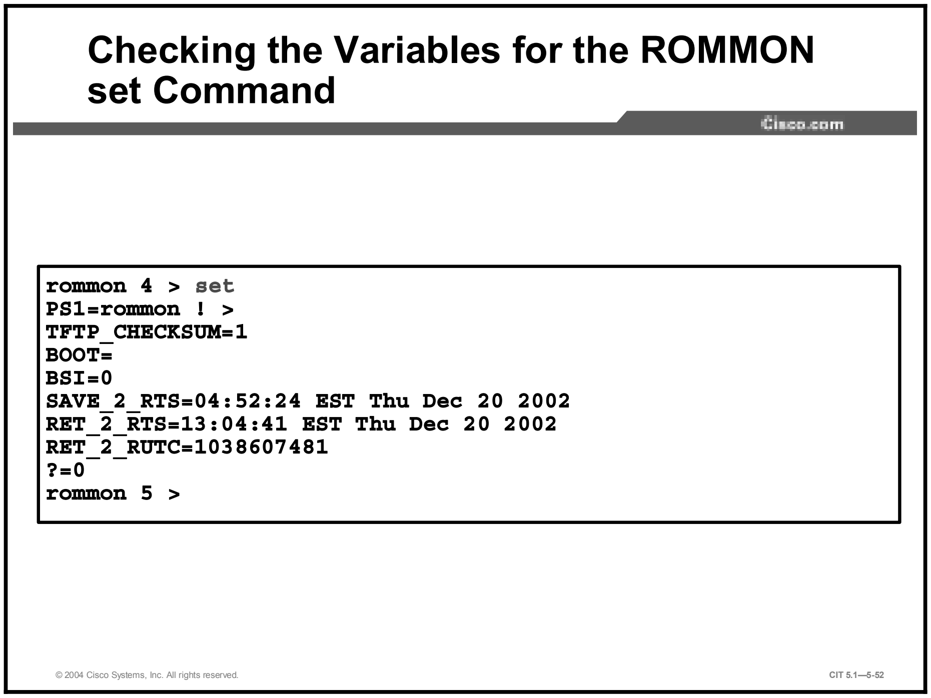
```
rommon 3 > tftpdnld

Missing or illegal ip address for variable IP_ADDRESS
Illegal IP address.

usage: tftpdnld [-r]
  Use this command for disaster recovery only to recover an image via TFTP.
  Monitor variables are used to set up parameters for the transfer.
  (Syntax: "VARIABLE_NAME=value" and use "set" to show current variables.)
  "ctrl-c" or "break" stops the transfer before flash erase begins.

  The following variables are REQUIRED to be set for tftpdnld:
            IP_ADDRESS: The IP address for this unit
        IP_SUBNET_MASK: The subnet mask for this unit
       DEFAULT_GATEWAY: The default gateway for this unit
           TFTP_SERVER: The IP address of the server to fetch from
             TFTP_FILE: The filename to fetch

  The following variables are OPTIONAL:
          TFTP_VERBOSE: Print setting. 0=quiet, 1=progress(default), 2=verbose
      TFTP_RETRY_COUNT: Retry count for ARP and TFTP (default=7)
          TFTP_TIMEOUT: Overall timeout of operation in seconds (default=7200)
         TFTP_CHECKSUM: Perform checksum test on image, 0=no, 1=yes (default=1)

  Command line options:
   -r: do not write flash, load to DRAM only and launch image
rommon 4 >
```

© 2004 Cisco Systems, Inc. All rights reserved.

CIT 5.1—5-51

The attempt fails, and the command output displays messages that are symptoms of an issue with the TFTP application layer protocol.

To help isolate these issues, you first check for current variables with the **set** command on the Orlando router.

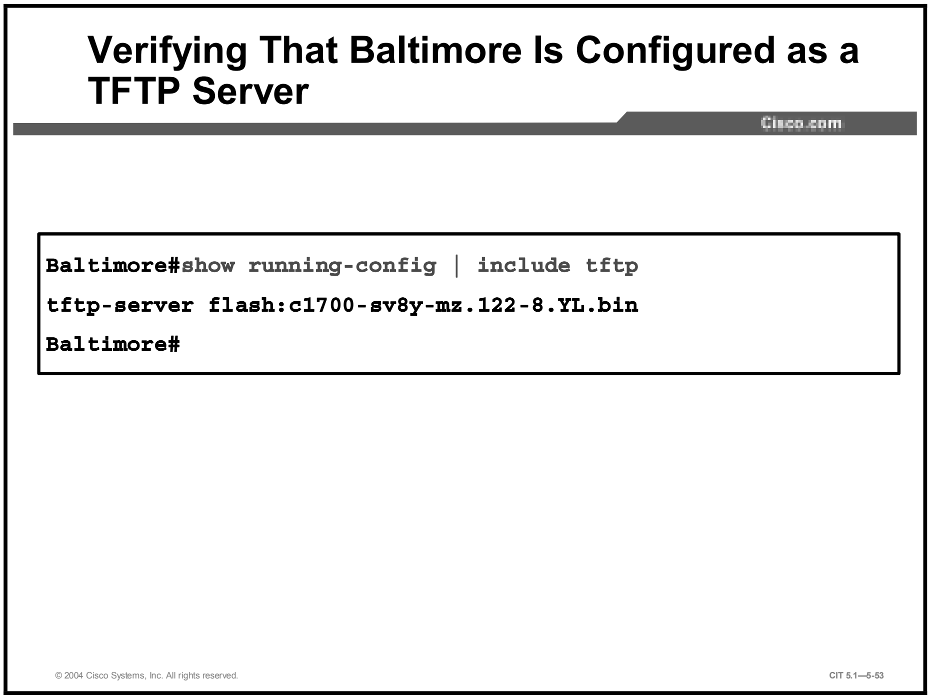


Checking the Variables for the ROMMON set Command

```
rommon 4 > set
PS1=rommon ! >
TFTP_CHECKSUM=1
BOOT=
BSI=0
SAVE_2_RTS=04:52:24 EST Thu Dec 20 2002
RET_2_RTS=13:04:41 EST Thu Dec 20 2002
RET_2_RUTC=1038607481
?=0
rommon 5 >
```

CIT 5.1—5-52

It looks as though none of the required variables are set on the Orlando router. You call Network Operations in Baltimore and ask for verification that Baltimore has been configured as a TFTP server. You ask Network Operations to use the **show running-config | include tftp** command to verify that the TFTP server is running and has the image for the 1760 router.



Verifying That Baltimore Is Configured as a TFTP Server

```
Baltimore#show running-config | include tftp
tftp-server flash:c1700-sv8y-mz.122-8.YL.bin
Baltimore#
```

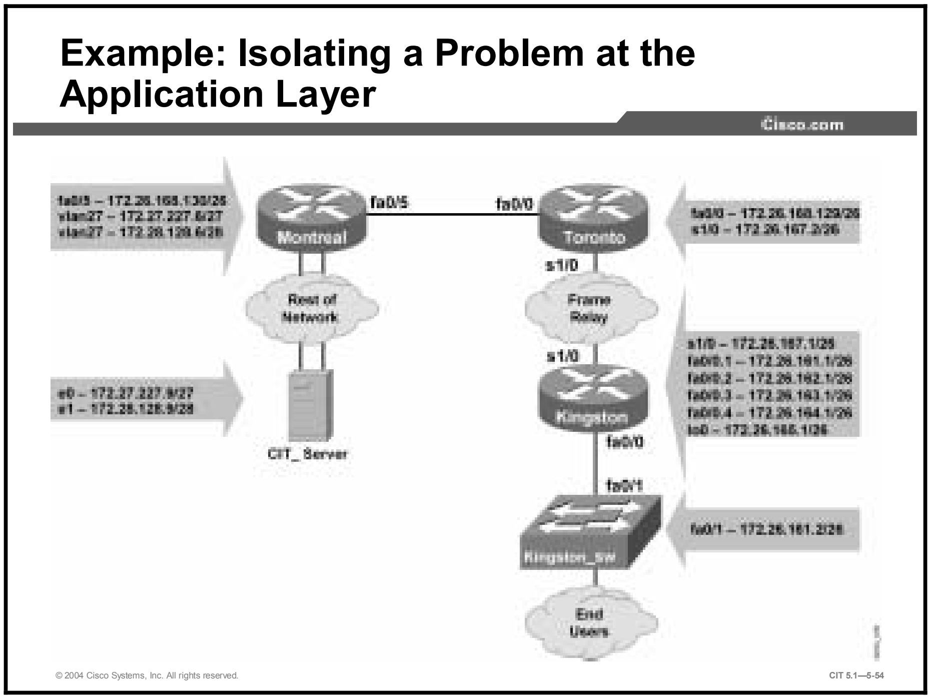
CIT 5.1—5-53

Network Operations in Baltimore reports that the TFTP server is running and offers **flash:c1700-sv8y-mz.122-8.YL.bin** for your use.

You have isolated the issue: the **tftpdnld** command needs the IP address and mask for the local router, the default gateway for the local router, the IP address of the TFTP server, and the name of the file to be transferred.

Example: Isolating a Problem at the Application Layer

You are the second-level network engineer in Kingston. You have console access to the access router named Kingston and IP connectivity to all other devices in your division. Your division supports the 172.26.0.0/16 subnet. Early this morning, network interns Bill and Jerry configured IPSec between Kingston and Toronto to encrypt corporate traffic on the frame relay link.



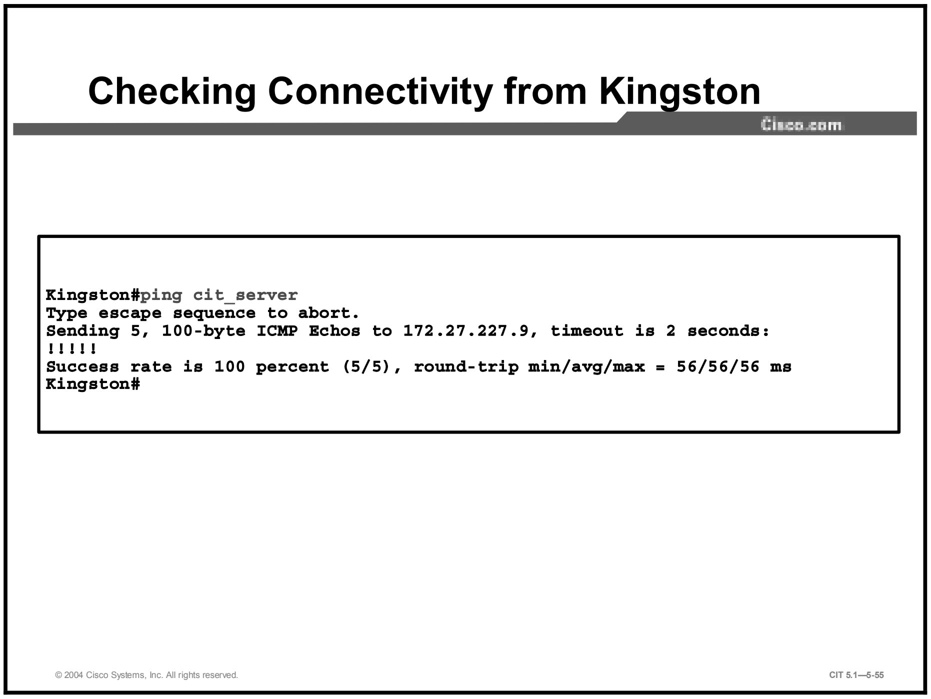
Example: Isolating a Problem at the Application Layer

© 2004 Cisco Systems, Inc. All rights reserved.

CIT 5.1—5-54

Now the Kingston end users are complaining that they cannot get access to devices in the corporate network, such as the CIT_Server.

You test connectivity from Kingston.



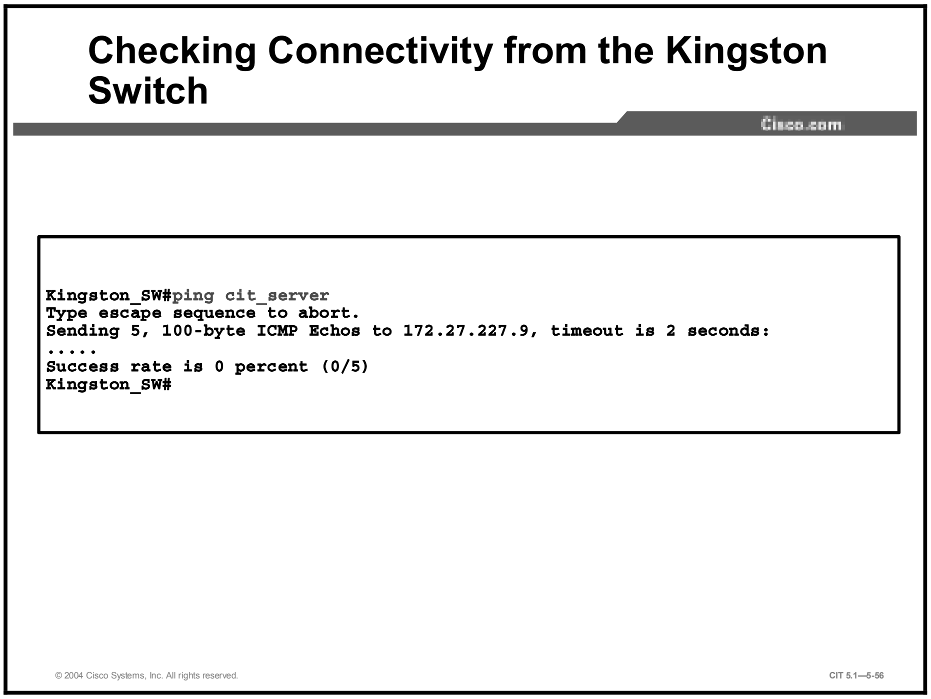
Checking Connectivity from Kingston

```
Kingston#ping cit_server
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.27.227.9, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 56/56/56 ms
Kingston#
```

CIT 5.1—5-55

Kingston has connectivity to the CIT_Server.

You open another terminal emulation window, connect to the Kingston switch, and try to connect to the CIT_Server.



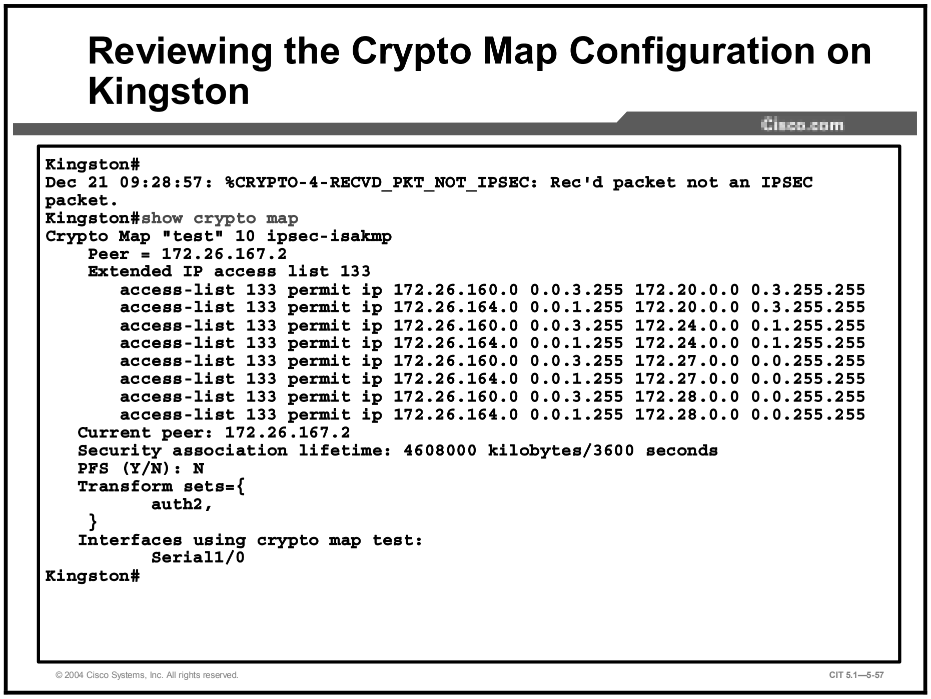
Checking Connectivity from the Kingston Switch

```
Kingston_SW#ping cit_server
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.27.227.9, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
Kingston_SW#
```

CIT 5.1—5-56

As reported, Kingston_SW cannot reach the CIT_Server. Because the IPSec configurations are new, it is time to look at them.

You return to your console session and review the crypto map on Kingston.



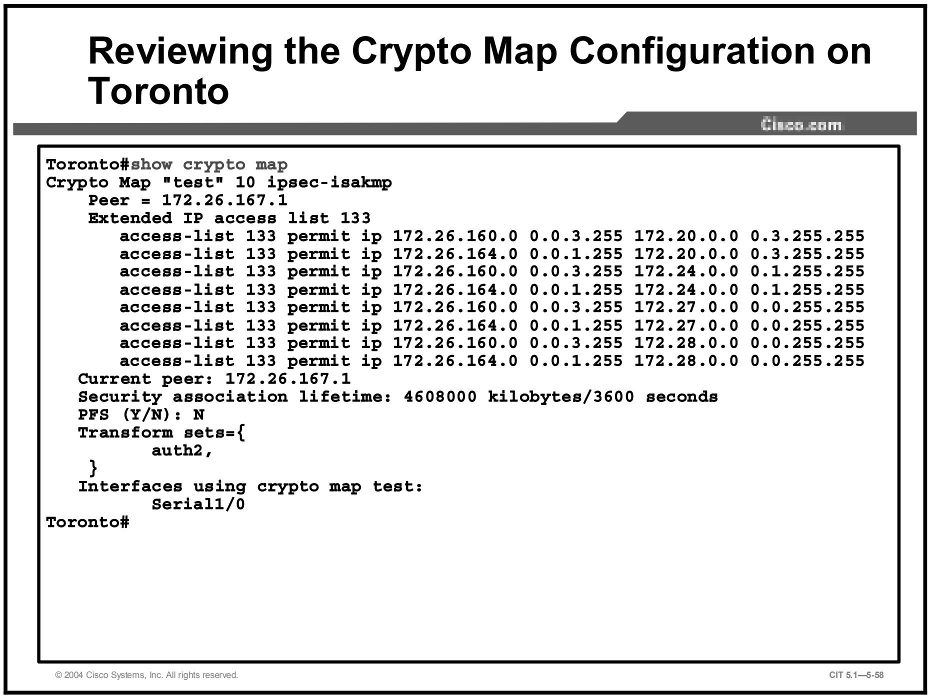
Reviewing the Crypto Map Configuration on Kingston

```
Kingston#
Dec 21 09:28:57: %CRYPTO-4-RECVD_PKT_NOT_IPSEC: Rec'd packet not an IPSEC
packet.
Kingston#show crypto map
Crypto Map "test" 10 ipsec-isakmp
    Peer = 172.26.167.2
    Extended IP access list 133
       access-list 133 permit ip 172.26.160.0 0.0.3.255 172.20.0.0 0.3.255.255
       access-list 133 permit ip 172.26.164.0 0.0.1.255 172.20.0.0 0.3.255.255
       access-list 133 permit ip 172.26.160.0 0.0.3.255 172.24.0.0 0.1.255.255
       access-list 133 permit ip 172.26.164.0 0.0.1.255 172.24.0.0 0.1.255.255
       access-list 133 permit ip 172.26.160.0 0.0.3.255 172.27.0.0 0.0.255.255
       access-list 133 permit ip 172.26.164.0 0.0.1.255 172.27.0.0 0.0.255.255
       access-list 133 permit ip 172.26.160.0 0.0.3.255 172.28.0.0 0.0.255.255
       access-list 133 permit ip 172.26.164.0 0.0.1.255 172.28.0.0 0.0.255.255
   Current peer: 172.26.167.2
   Security association lifetime: 4608000 kilobytes/3600 seconds
   PFS (Y/N): N
   Transform sets={
          auth2,
    }
   Interfaces using crypto map test:
          Serial1/0
Kingston#
```

CIT 5.1—5-57

The configuration looks pretty reasonable. The map is applied to interface Serial 1/0, and the current peer is 172.26.167.2. The access list picks up the local subnets on Kingston and on the corporate subnets.

You open another window for a console session to review the crypto map on Toronto.



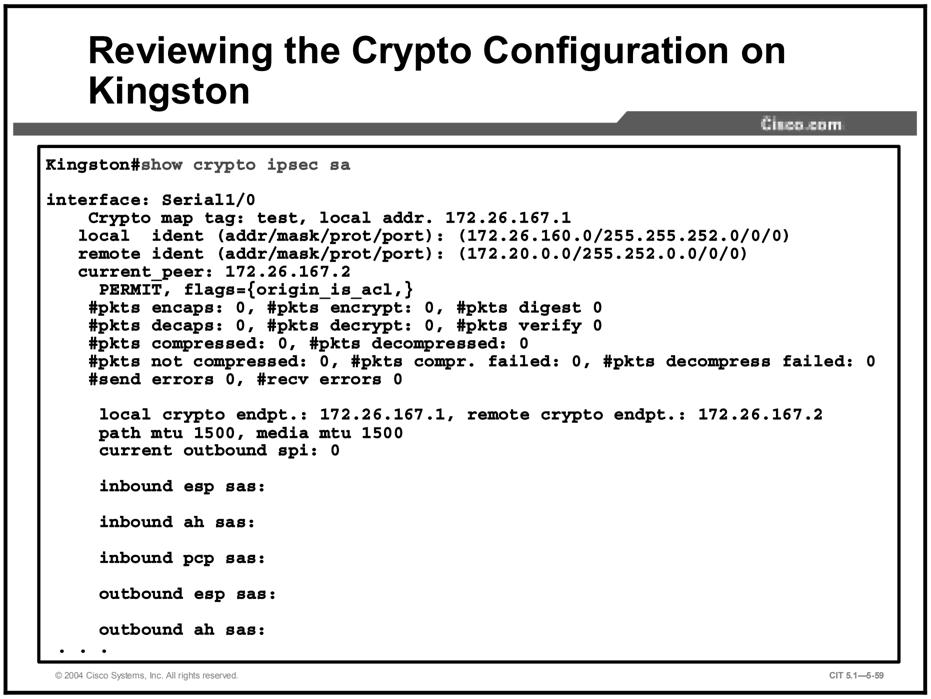
Reviewing the Crypto Map Configuration on Toronto

```
Toronto#show crypto map
Crypto Map "test" 10 ipsec-isakmp
    Peer = 172.26.167.1
    Extended IP access list 133
       access-list 133 permit ip 172.26.160.0 0.0.3.255 172.20.0.0 0.3.255.255
       access-list 133 permit ip 172.26.164.0 0.0.1.255 172.20.0.0 0.3.255.255
       access-list 133 permit ip 172.26.160.0 0.0.3.255 172.24.0.0 0.1.255.255
       access-list 133 permit ip 172.26.164.0 0.0.1.255 172.24.0.0 0.1.255.255
       access-list 133 permit ip 172.26.160.0 0.0.3.255 172.27.0.0 0.0.255.255
       access-list 133 permit ip 172.26.164.0 0.0.1.255 172.27.0.0 0.0.255.255
       access-list 133 permit ip 172.26.160.0 0.0.3.255 172.28.0.0 0.0.255.255
       access-list 133 permit ip 172.26.164.0 0.0.1.255 172.28.0.0 0.0.255.255
   Current peer: 172.26.167.1
   Security association lifetime: 4608000 kilobytes/3600 seconds
   PFS (Y/N): N
   Transform sets={
          auth2,
    }
   Interfaces using crypto map test:
          Serial1/0
Toronto#
```

CIT 5.1—5-58

The peer is correct; the map is applied to the appropriate interface. You see the Kingston and the corporate subnets.

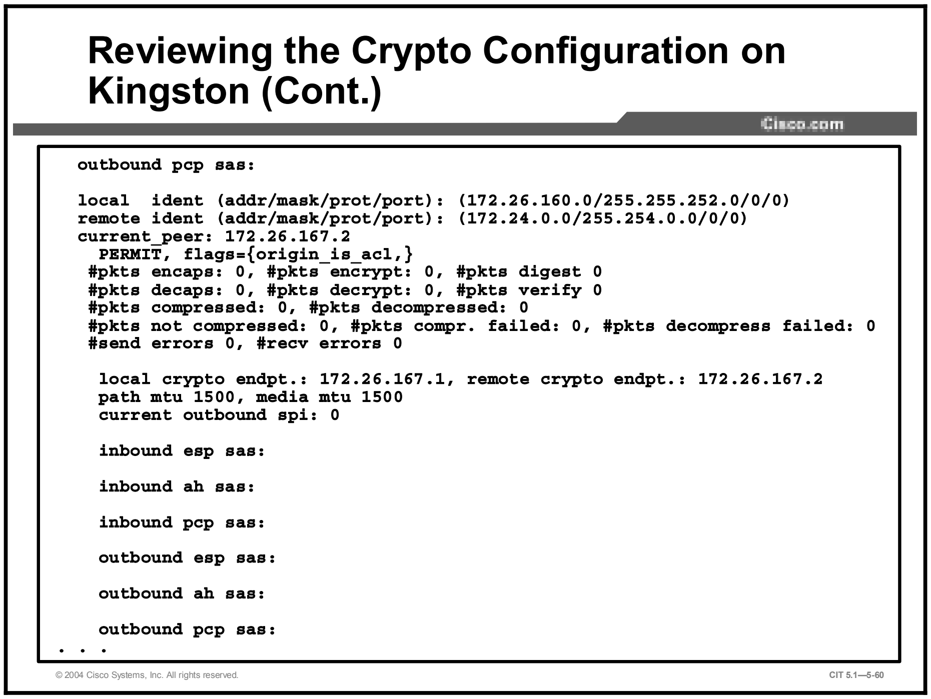
You try reviewing the crypto IPSec security associations.



Reviewing the Crypto Configuration on Kingston

```
Kingston#show crypto ipsec sa

interface: Serial1/0
    Crypto map tag: test, local addr. 172.26.167.1
   local  ident (addr/mask/prot/port): (172.26.160.0/255.255.252.0/0/0)
   remote ident (addr/mask/prot/port): (172.20.0.0/255.252.0.0/0/0)
   current_peer: 172.26.167.2
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 0, #pkts encrypt: 0, #pkts digest 0
    #pkts decaps: 0, #pkts decrypt: 0, #pkts verify 0
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 172.26.167.1, remote crypto endpt.: 172.26.167.2
     path mtu 1500, media mtu 1500
     current outbound spi: 0

     inbound esp sas:

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:

     outbound ah sas:
 . . .
```

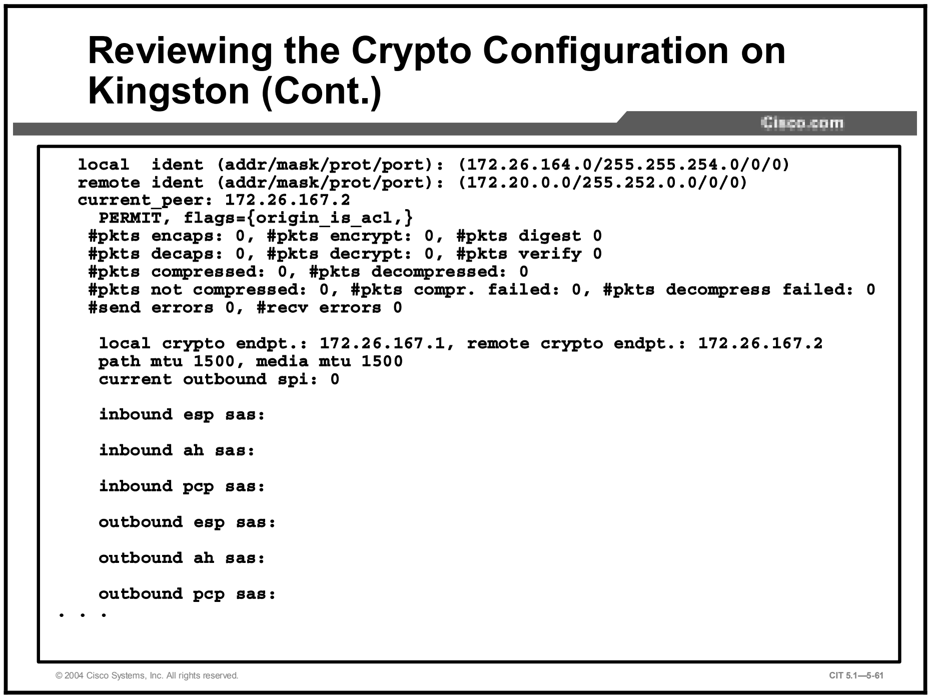
CIT 5.1—5-59



Reviewing the Crypto Configuration on Kingston (Cont.)

```
  outbound pcp sas:

  local  ident (addr/mask/prot/port): (172.26.160.0/255.255.252.0/0/0)
  remote ident (addr/mask/prot/port): (172.24.0.0/255.254.0.0/0/0)
  current_peer: 172.26.167.2
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 0, #pkts encrypt: 0, #pkts digest 0
   #pkts decaps: 0, #pkts decrypt: 0, #pkts verify 0
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0
   #send errors 0, #recv errors 0

    local crypto endpt.: 172.26.167.1, remote crypto endpt.: 172.26.167.2
    path mtu 1500, media mtu 1500
    current outbound spi: 0

    inbound esp sas:

    inbound ah sas:

    inbound pcp sas:

    outbound esp sas:

    outbound ah sas:

    outbound pcp sas:
. . .
```

CIT 5.1—5-60



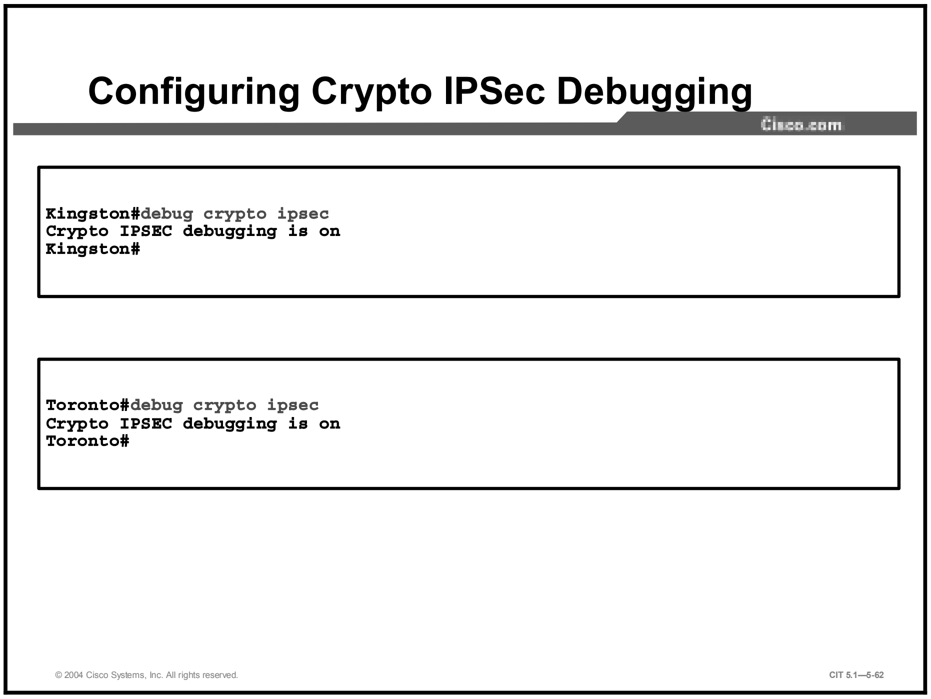
Reviewing the Crypto Configuration on Kingston (Cont.)

```
  local  ident (addr/mask/prot/port): (172.26.164.0/255.255.254.0/0/0)
  remote ident (addr/mask/prot/port): (172.20.0.0/255.252.0.0/0/0)
  current_peer: 172.26.167.2
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 0, #pkts encrypt: 0, #pkts digest 0
   #pkts decaps: 0, #pkts decrypt: 0, #pkts verify 0
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0
   #send errors 0, #recv errors 0

    local crypto endpt.: 172.26.167.1, remote crypto endpt.: 172.26.167.2
    path mtu 1500, media mtu 1500
    current outbound spi: 0

    inbound esp sas:

    inbound ah sas:

    inbound pcp sas:

    outbound esp sas:

    outbound ah sas:

    outbound pcp sas:
. . .
```

CIT 5.1—5-61

There are certainly a lot of screens to review. You may notice that no security associations have been established. Perhaps it is time to try some **debug** commands.

You set up debugging on both Kingston and Toronto.



Configuring Crypto IPSec Debugging

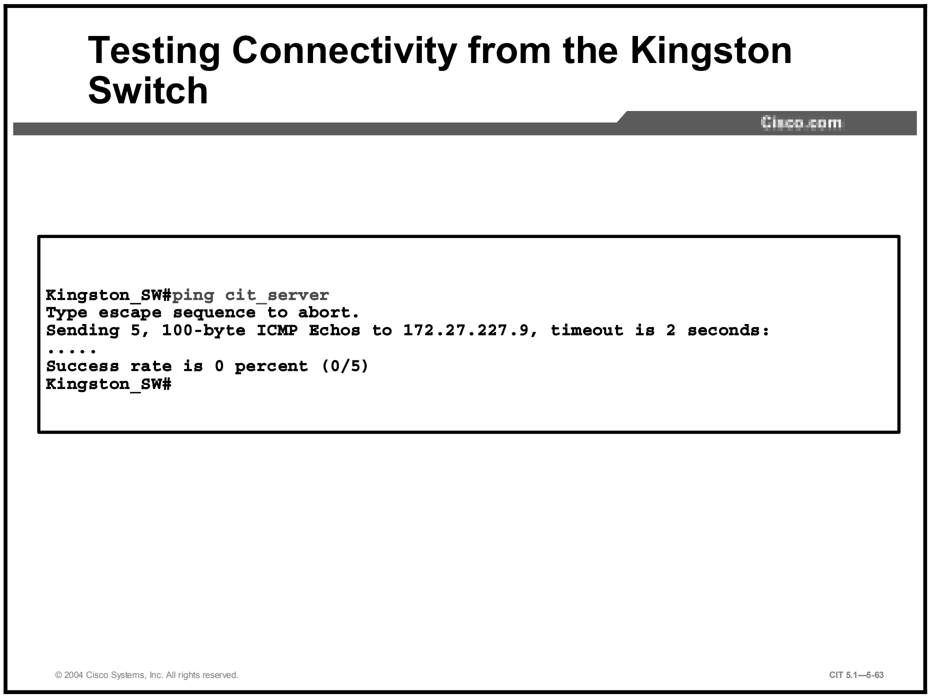
```
Kingston#debug crypto ipsec
Crypto IPSEC debugging is on
Kingston#
```

```
Toronto#debug crypto ipsec
Crypto IPSEC debugging is on
Toronto#
```

CIT 5.1—5-62

Then you try again to connect to the CIT_server from Kingston_SW.

You start another ping test from Kingston_SW.



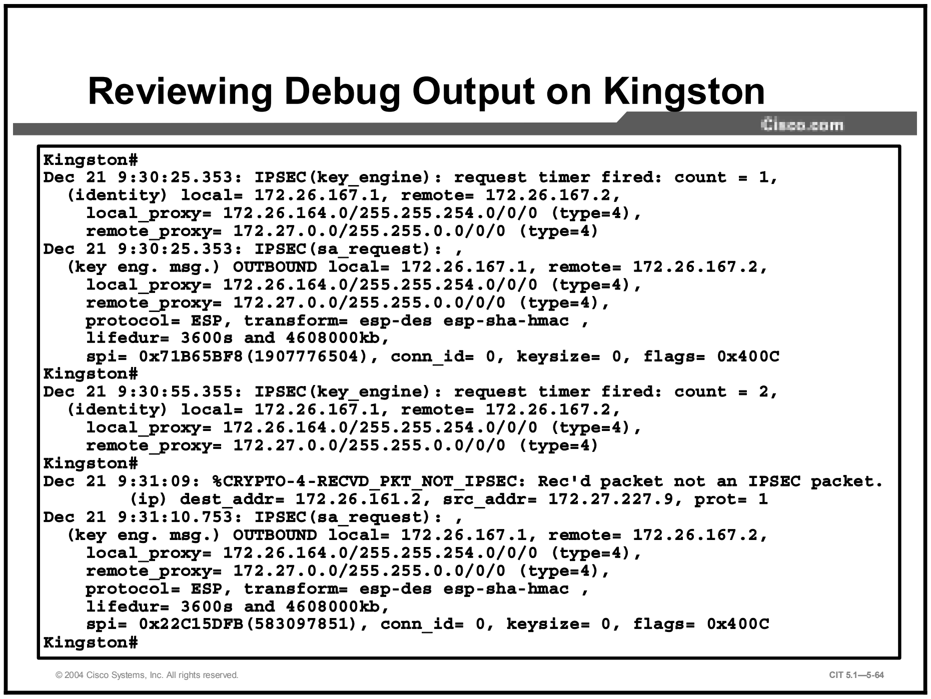
Testing Connectivity from the Kingston Switch

```
Kingston_SW#ping cit_server
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.27.227.9, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
Kingston_SW#
```

CIT 5.1—5-63

As expected, the ping test fails. Did the debugging process show anything?

You review the console output on Kingston.



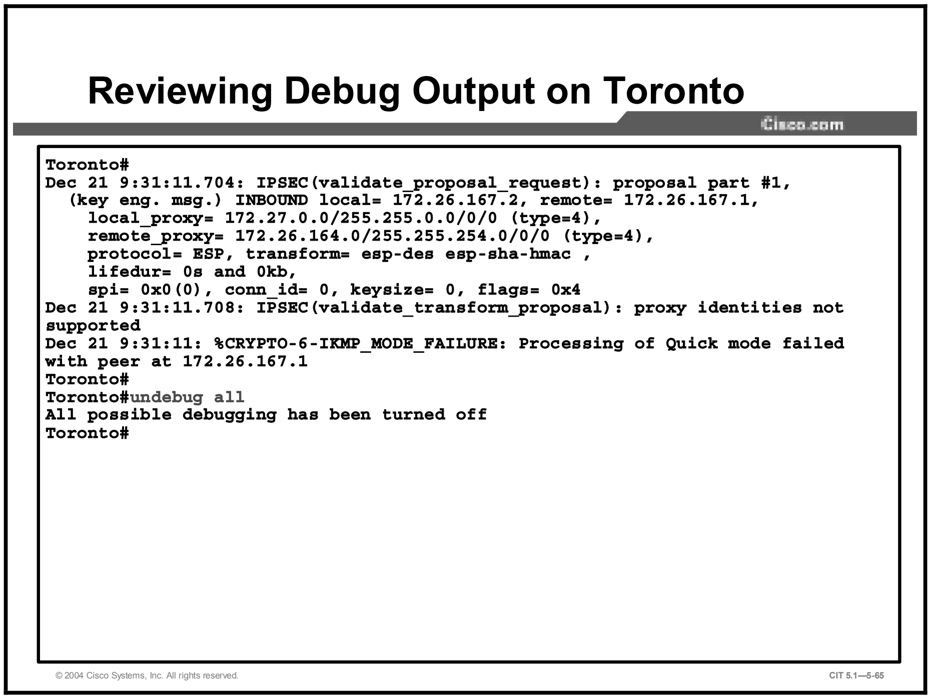
Reviewing Debug Output on Kingston

```
Kingston#
Dec 21 9:30:25.353: IPSEC(key_engine): request timer fired: count = 1,
  (identity) local= 172.26.167.1, remote= 172.26.167.2,
    local_proxy= 172.26.164.0/255.255.254.0/0/0 (type=4),
    remote_proxy= 172.27.0.0/255.255.0.0/0/0 (type=4)
Dec 21 9:30:25.353: IPSEC(sa_request): ,
  (key eng. msg.) OUTBOUND local= 172.26.167.1, remote= 172.26.167.2,
    local_proxy= 172.26.164.0/255.255.254.0/0/0 (type=4),
    remote_proxy= 172.27.0.0/255.255.0.0/0/0 (type=4),
    protocol= ESP, transform= esp-des esp-sha-hmac ,
    lifedur= 3600s and 4608000kb,
    spi= 0x71B65BF8(1907776504), conn_id= 0, keysize= 0, flags= 0x400C
Kingston#
Dec 21 9:30:55.355: IPSEC(key_engine): request timer fired: count = 2,
  (identity) local= 172.26.167.1, remote= 172.26.167.2,
    local_proxy= 172.26.164.0/255.255.254.0/0/0 (type=4),
    remote_proxy= 172.27.0.0/255.255.0.0/0/0 (type=4)
Kingston#
Dec 21 9:31:09: %CRYPTO-4-RECVD_PKT_NOT_IPSEC: Rec'd packet not an IPSEC packet.
         (ip) dest_addr= 172.26.161.2, src_addr= 172.27.227.9, prot= 1
Dec 21 9:31:10.753: IPSEC(sa_request): ,
  (key eng. msg.) OUTBOUND local= 172.26.167.1, remote= 172.26.167.2,
    local_proxy= 172.26.164.0/255.255.254.0/0/0 (type=4),
    remote_proxy= 172.27.0.0/255.255.0.0/0/0 (type=4),
    protocol= ESP, transform= esp-des esp-sha-hmac ,
    lifedur= 3600s and 4608000kb,
    spi= 0x22C15DFB(583097851), conn_id= 0, keysize= 0, flags= 0x400C
Kingston#
```

CIT 5.1—5-64

You may notice that because the received packet is not encapsulated, there may be a policy setup error in the IPSec peers.

You review the console output on Toronto.



Reviewing Debug Output on Toronto

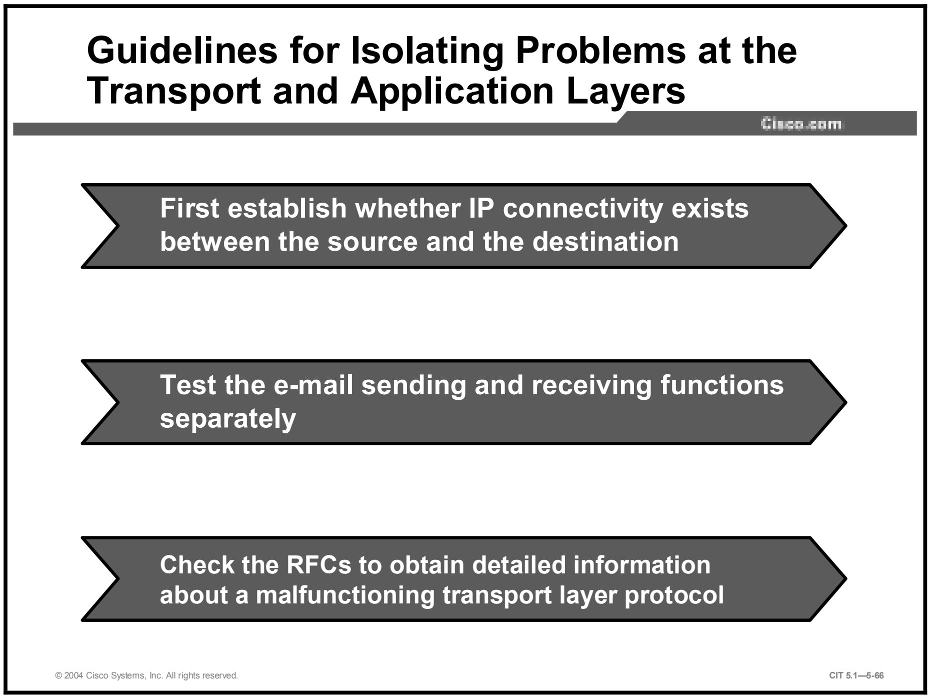
```
Toronto#
Dec 21 9:31:11.704: IPSEC(validate_proposal_request): proposal part #1,
  (key eng. msg.) INBOUND local= 172.26.167.2, remote= 172.26.167.1,
    local_proxy= 172.27.0.0/255.255.0.0/0/0 (type=4),
    remote_proxy= 172.26.164.0/255.255.254.0/0/0 (type=4),
    protocol= ESP, transform= esp-des esp-sha-hmac ,
    lifedur= 0s and 0kb,
    spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
Dec 21 9:31:11.708: IPSEC(validate_transform_proposal): proxy identities not
supported
Dec 21 9:31:11: %CRYPTO-6-IKMP_MODE_FAILURE: Processing of Quick mode failed
with peer at 172.26.167.1
Toronto#
Toronto#undebug all
All possible debugging has been turned off
Toronto#
```

CIT 5.1—5-65

From Toronto, you see that the negotiation with the remote peer failed. You should be able to isolate the problem with the information provided up to now.

Isolating Problems Occurring at the Transport and Application Layers

This topic identifies guidelines to help troubleshooters isolate problems at the transport and application layers.



Guidelines for Isolating Problems at the Transport and Application Layers

First establish whether IP connectivity exists between the source and the destination

Test the e-mail sending and receiving functions separately

Check the RFCs to obtain detailed information about a malfunctioning transport layer protocol

CIT 5.1—5-66

Guidelines for isolating problems at the transport and applications layers are as follows:

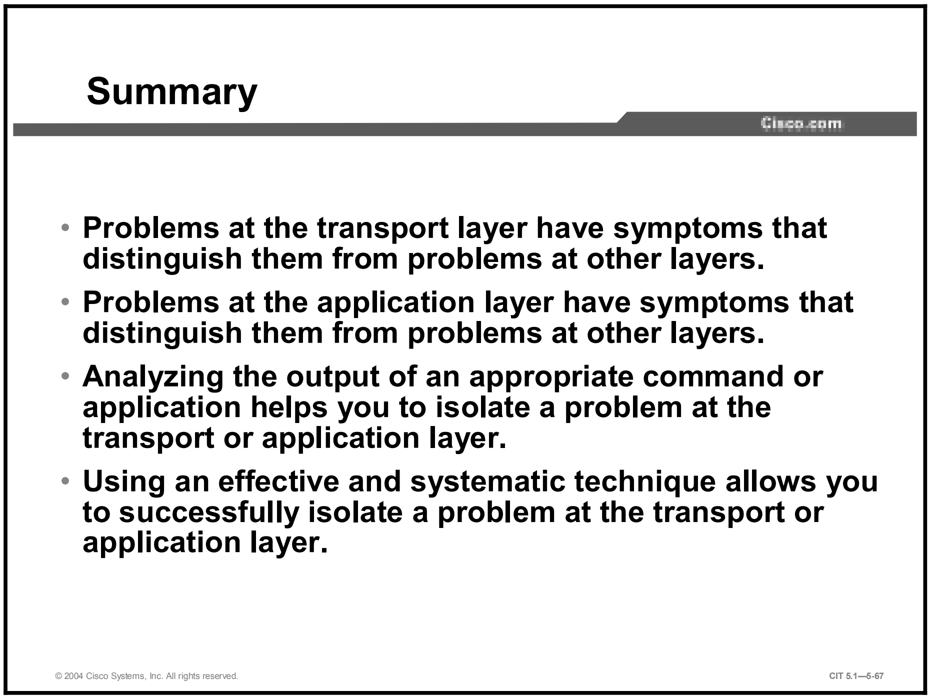
- First, establish whether IP connectivity exists between the source and the destination. If IP connectivity exists, the issue must be at the transport layer or above.
- Test the e-mail sending and receiving functions separately. E-mail uses different protocols to send and receive mail.
- Check the RFCs to obtain detailed information about a malfunctioning transport layer protocol. Depending on the problem, you can check the RFCs to determine information such as the IP protocols in use, the TCP or UDP port numbers that are used by the protocol, any inbound TCP connections or UDP packets that are required, whether the protocol embeds IP addresses in the data portion of the packet, and whether the protocol runs as a client or a server.

Example: Isolating a Problem Occurring at the Transport or Application Layer

In a fairly short period of time, a large number of network users call to report that they cannot send e-mail, but they can receive it. Your network has separate servers for sending and receiving e-mail. (An SMTP server is used to send e-mail, and a POP3 server is used to receive and save e-mail.) Because the users are receiving e-mail, you doubt that the POP3 server is malfunctioning. The problem sending e-mail can be isolated to the server running the SMTP protocol. Testing the physical, data link, and network layers shows no problems. To test the transport layer, you attempt to use Telnet to connect into the SMTP server through the port number for the SMTP protocol (25). You do not receive a hello message from the server. This isolates the problem to either the transport or application layer.

Summary

This topic summarizes the key points discussed in this lesson.



Summary

- Problems at the transport layer have symptoms that distinguish them from problems at other layers.
- Problems at the application layer have symptoms that distinguish them from problems at other layers.
- Analyzing the output of an appropriate command or application helps you to isolate a problem at the transport or application layer.
- Using an effective and systematic technique allows you to successfully isolate a problem at the transport or application layer.

CIT 5.1—5-67

References

For additional information, refer to these resources:

- Cisco online documentation:
  http://www.cisco.com/univercd/home/home.htm
- Cisco Technical Assistance Center (TAC):
  http://www.cisco.com/tac
- Troubleshooting TCP/IP:
  http://www.cisco.com/univercd/cc/td/doc/cisintwk/itg_v1/tr1907.htm
- Using Test TCP (TTCP) to Test Throughput:
  http://www.cisco.com/warp/public/471/ttcp.html

Quiz

Use the practice items here to review what you have learned in this lesson. The correct answers are found in the Quiz Answer Key.

Q1) Which of the following choices describes symptoms of failure problems at the transport layer?

A) Nothing at or above Layer 4 is operational; an application consistently displays error messages.

B) Pings across the connection consistently fail; there is no connectivity at Layer 1 and Layer 2; upper layers are functioning properly.

C) Pings across the connection consistently work; an excessive number of CRC errors are reported.

D) Running a trace shows latency at two out of three hops across a connection.

Q2) The help desk receives a call from a user who states that e-mail cannot be sent. The user is unsure whether e-mail can be received. Testing shows that the end system has connectivity to the network. You narrow the source of the problem down to the e-mail application, which has been corrupted. Which symptom helps you to determine that this is a problem at the application layer?

A) Layers 5, 6, and 7 are all functioning; all layers below are not functioning.

B) All applications are running slower than normal; there is a loss of connectivity at Layer 3.

C) Layers 5, 6, and 7 are not operational; all layers below are functioning.

D) Layer 4 is not operational; all layers above Layer 4 are operational.

Q3) Which command do you enter at a UNIX end system to most quickly find the identity of the name server?

A) **ttcp**

B) **nslookup**

C) **winipcfg**

D) **tcptrace**

Q4) Which command should a troubleshooter use to test the functionality of the SMTP protocol?

A) **debug ip dhcp server**

B) **telnet** {*ip-address* | *host*} **80**

C) **copy tftp**

D) **telnet** {*ip-address* | *host*} **25**

Q5) A group of users on the same segment of a large Ethernet LAN report that they can connect to an FTP server, but they cannot transfer any files. No other segments appear to have this problem. You are not sure what the issue is. What should you do next?

A) ping the default gateway

B) ask the users to continue attempting to transfer files

C) check the RFC for information about the FTP protocol

D) apply the **debug telnet** command to determine the cause of the problem

Quiz Answer Key

Q1) A

Relates to: Identifying the Symptoms of Problems Occurring at the Transport Layer

Q2) C

Relates to: Identifying the Symptoms of Problems Occurring at the Application Layer

Q3) B

Relates to: Analyzing Commands and Applications Used to Isolate Problems Occurring at the Transport Layer

Q4) D

Relates to: Analyzing Commands and Applications Used to Isolate Problems Occurring at the Application Layer

Q5) C

Relates to: Isolating Problems Occurring at the Transport and Application Layers

Correcting the Problem

Overview

Once you have performed isolating techniques to determine the most likely cause of a problem, the next stage of the general troubleshooting process is to correct the problem. In this lesson, you will correct isolated transport and application layer problems using commands and applications that optimize transport and application layer components.

Relevance

Isolation is a vital step for a troubleshooter to perform to successfully troubleshoot a problem. However, merely isolating the problem will not bring on the types of changes that you need to make so that the network functions at the documented baseline. To resolve the problem, you must use the tools and resources that Cisco and your end systems provide to configure the properties of your network.

Objectives

Upon completing this lesson, you will be able to:

- Identify commands and applications used to correct problems occurring at the transport layer
- Identify commands and applications used to correct problems occurring at the application layer
- Identify transport and application layer support resources
- Correct problems occurring at the transport and application layers

Learner Skills and Knowledge

To benefit fully from this lesson, you must have these prerequisite skills and knowledge:

- The ability to apply layered model troubleshooting approaches
- Familiarity with Cisco command syntax covered in the Cisco *Building Scalable Cisco Internetworks* (BSCI), *Building Cisco Multilayer Switched Networks* (BCMSN), and *Building Cisco Remote Access Networks* (BCRAN) courses
- Basic TCP and UDP concepts

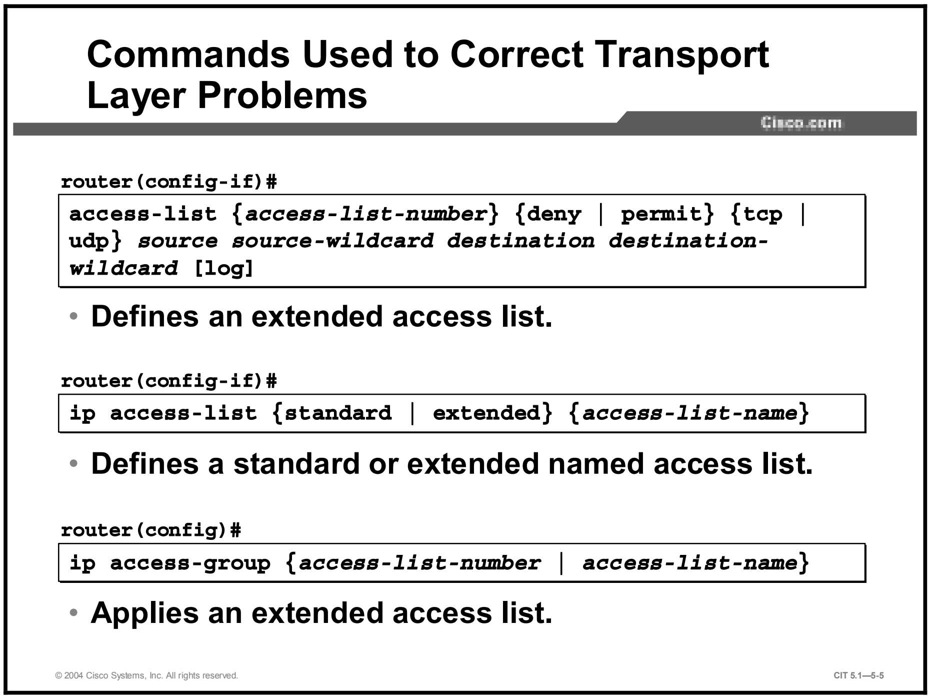
Outline

This lesson includes these topics:

- Overview
- Identifying Commands and Applications Used to Correct Problems Occurring at the Transport Layer
- Identifying Commands and Applications Used to Correct Problems Occurring at the Application Layer
- Identifying Transport and Application Layer Support Resources
- Correcting Problems Occurring at the Transport and Application Layers
- Summary
- Quiz

Identifying Commands and Applications Used to Correct Problems Occurring at the Transport Layer

This topic identifies selected commands and applications used by troubleshooters to correct problems occurring at the transport layer.



Commands Used to Correct Transport Layer Problems

Cisco.com

router(config-if)#

```
access-list {access-list-number} {deny | permit} {tcp |
udp} source source-wildcard destination destination-
wildcard [log]
```

- Defines an extended access list.

router(config-if)#

```
ip access-list {standard | extended} {access-list-name}
```

- Defines a standard or extended named access list.

router(config)#

```
ip access-group {access-list-number | access-list-name}
```

- Applies an extended access list.

CIT 5.1—5-5

Troubleshooters can use the commands listed in the table to make configuration changes to correct problems with TCP and UDP at the transport layer.

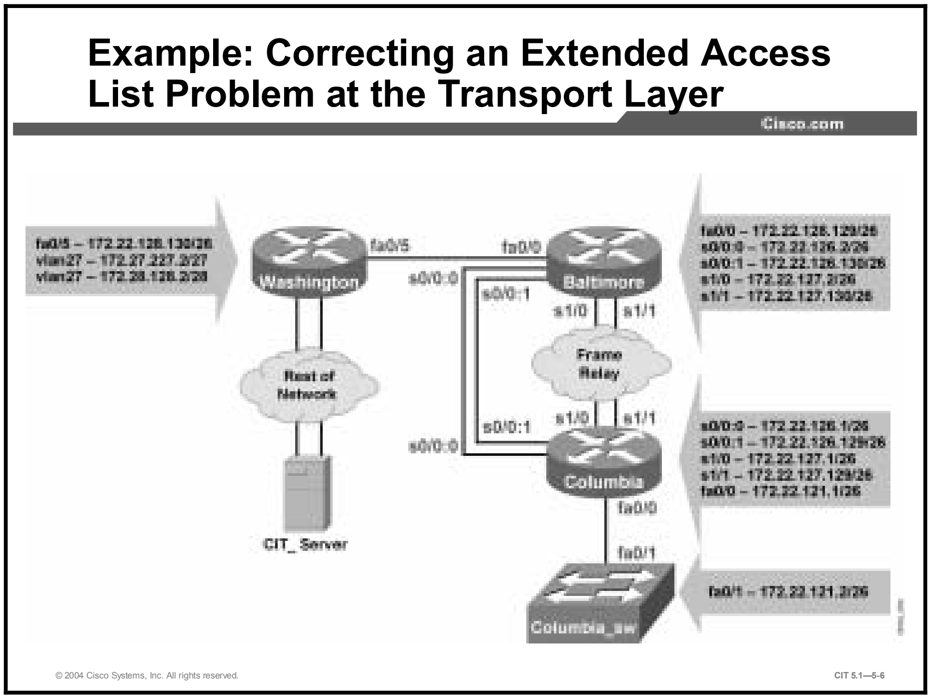
Commands Used to Correct Transport Layer Problems

Command	Description
Access-list {*access-list-number*} {**deny** | **permit**} {**tcp** | **udp**} *source source-wildcard destination destination-wildcard* [**log**]	Defines an extended access list.
ip access-list {**standard** | **extended**} {*access-list-name*}	Defines a standard or extended named access list.
ip access-group {*access-list-number* | *access-list-name*}	Applies an extended access list.

Note Not all of the commands listed are available on some versions of Cisco operating systems. To determine which commands are available for use with your devices, consult the online documentation for Cisco devices at http://www.cisco.com/univercd/home/home.htm.

Example: Correcting an Extended Access List Problem at the Transport Layer

You are the second-level network engineer for Columbia. You have console access to both the console router named Columbia and the access switch named Columbia_SW. You also have IP connectivity to all other devices in your division. Your division supports the 172.22.0.0/16 subnet.



Example: Correcting an Extended Access List Problem at the Transport Layer

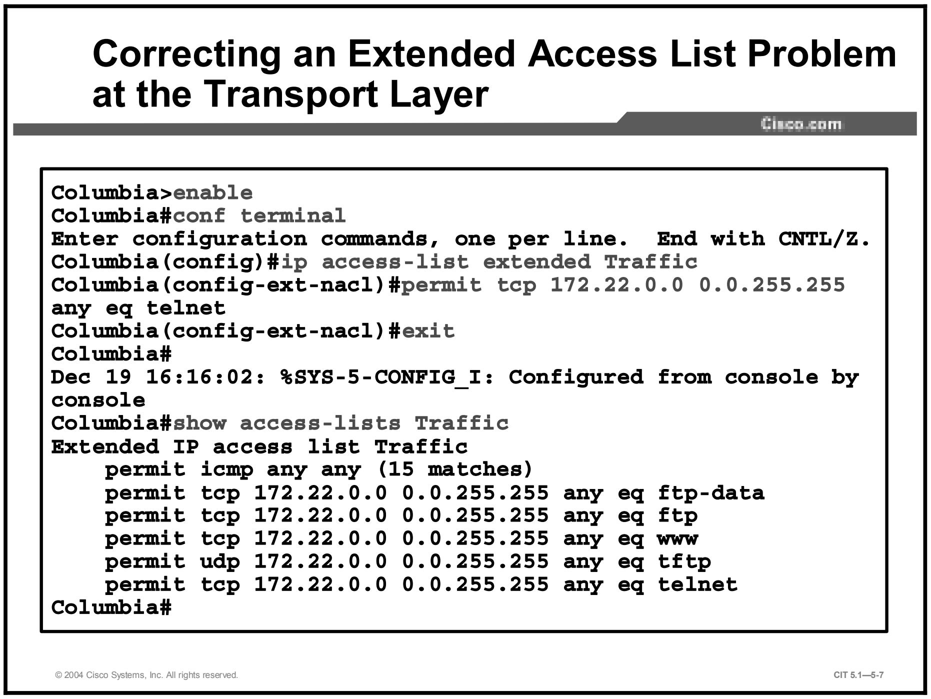
© 2004 Cisco Systems, Inc. All rights reserved.

CIT 5.1—5-6

You know from your base configuration information that the end users connect to Columbia through Columbia_SW. Columbia and Columbia_SW are connected over a 100 MB Fast Ethernet link. You have verified that you cannot use Telnet to connect to Baltimore from Columbia_SW, but you can connect from Columbia.

You have determined that there is an incomplete extended access list that is filtering Telnet traffic from the access switch and all end users.

You need to correct the extended access list named Traffic, which is located on Columbia.



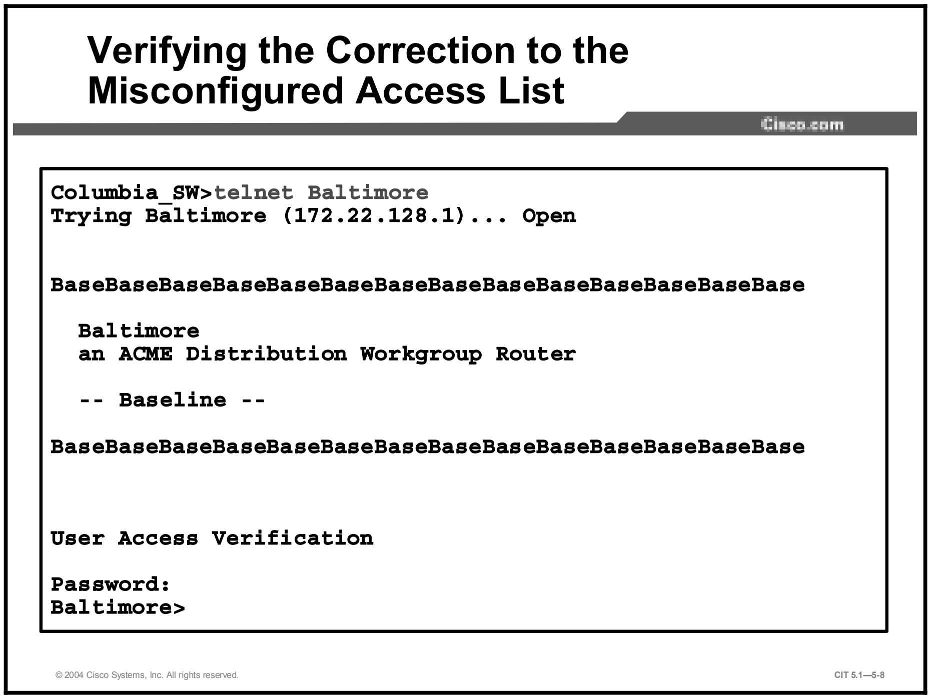
Correcting an Extended Access List Problem at the Transport Layer

```
Columbia>enable
Columbia#conf terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Columbia(config)#ip access-list extended Traffic
Columbia(config-ext-nacl)#permit tcp 172.22.0.0 0.0.255.255
any eq telnet
Columbia(config-ext-nacl)#exit
Columbia#
Dec 19 16:16:02: %SYS-5-CONFIG_I: Configured from console by
console
Columbia#show access-lists Traffic
Extended IP access list Traffic
    permit icmp any any (15 matches)
    permit tcp 172.22.0.0 0.0.255.255 any eq ftp-data
    permit tcp 172.22.0.0 0.0.255.255 any eq ftp
    permit tcp 172.22.0.0 0.0.255.255 any eq www
    permit udp 172.22.0.0 0.0.255.255 any eq tftp
    permit tcp 172.22.0.0 0.0.255.255 any eq telnet
Columbia#
```

CIT 5.1—5-7

You include a line to support Telnet in the access list named Traffic.

Finally, you return to the console session on Columbia_SW to verify that the change worked and that you can use Telnet to connect to Baltimore.



Verifying the Correction to the Misconfigured Access List

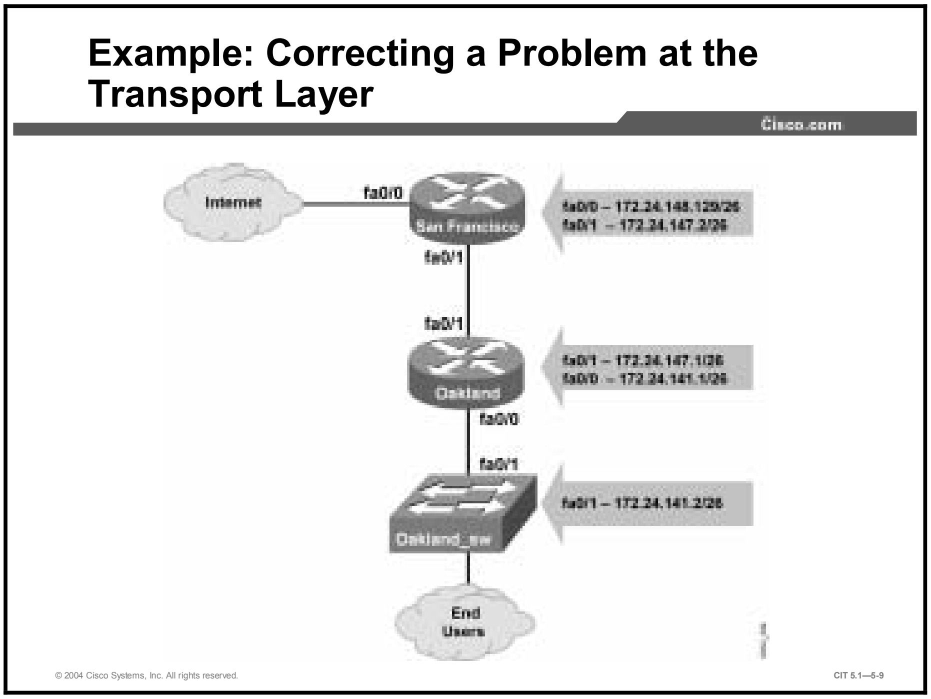
```
Columbia_SW>telnet Baltimore
Trying Baltimore (172.22.128.1)... Open


BaseBaseBaseBaseBaseBaseBaseBaseBaseBaseBaseBaseBaseBase

  Baltimore
  an ACME Distribution Workgroup Router

  -- Baseline --

BaseBaseBaseBaseBaseBaseBaseBaseBaseBaseBaseBaseBaseBase



User Access Verification

Password:
Baltimore>
```

CIT 5.1—5-8

The incomplete extended access list has been updated to support Telnet. You have resolved the transport layer issue and restored your baseline configuration.

Example: Correcting a Problem at the Transport Layer

You are the second-level network engineer for Oakland. You have console access to both the access router named Oakland and the access switch named Oakland_SW. You also have IP connectivity to all other devices in your division. Your division supports the 172.24.0.0/16 subnet. The router SanFran is running the firewall feature set and is acting as the firewall to the Internet for the rest of the division.



Example: Correcting a Problem at the Transport Layer

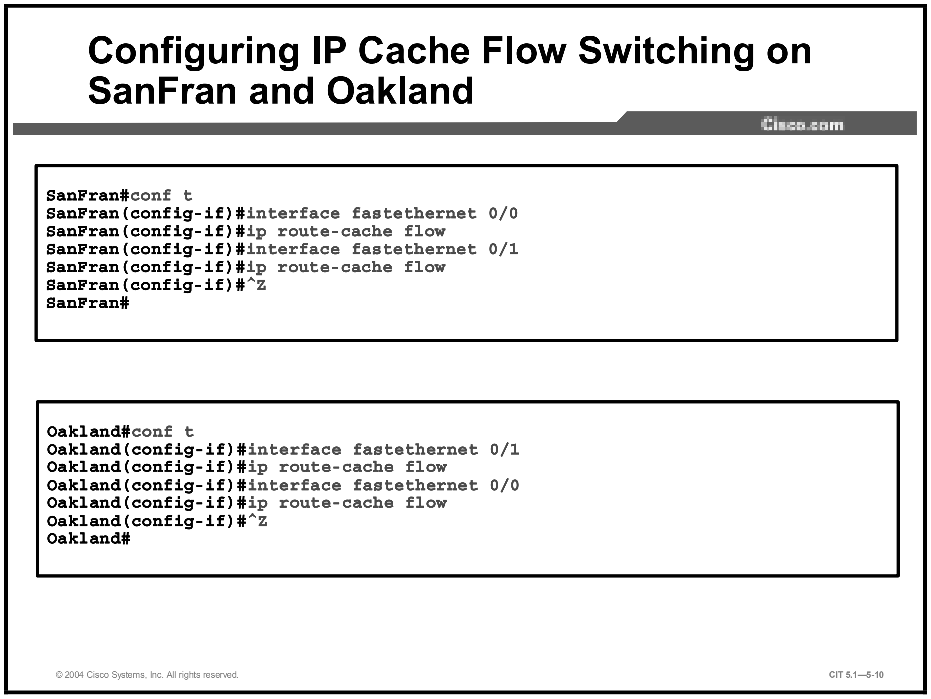
© 2004 Cisco Systems, Inc. All rights reserved.

CIT 5.1—5-9

There are some issues in the network. After SanFran crashed last night, you determined that it has a fast memory leak. You have noted that the IP input process on SanFran is consuming a lot of resources. In the short term, you would like to understand what current traffic flows are causing high IP input processing. In the longer term, you need to decide if an IOS upgrade is needed on SanFran.

Note	This example topology does not follow the CIT lab configuration.

First you configure IP cache flow routing on both SanFran and Oakland.



Configuring IP Cache Flow Switching on SanFran and Oakland

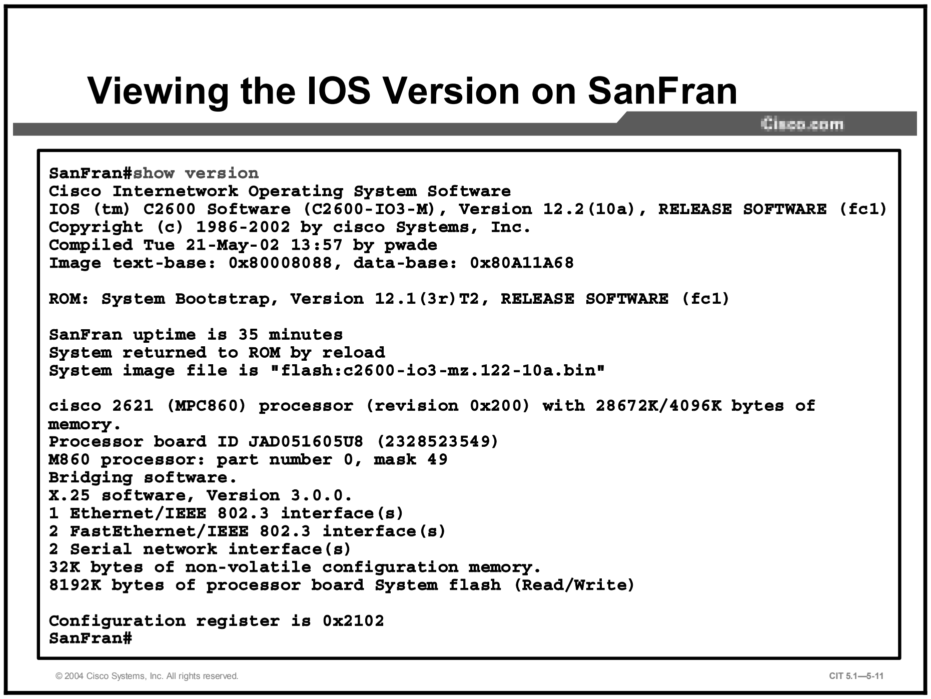
```
SanFran#conf t
SanFran(config-if)#interface fastethernet 0/0
SanFran(config-if)#ip route-cache flow
SanFran(config-if)#interface fastethernet 0/1
SanFran(config-if)#ip route-cache flow
SanFran(config-if)#^Z
SanFran#
```

```
Oakland#conf t
Oakland(config-if)#interface fastethernet 0/1
Oakland(config-if)#ip route-cache flow
Oakland(config-if)#interface fastethernet 0/0
Oakland(config-if)#ip route-cache flow
Oakland(config-if)#^Z
Oakland#
```

CIT 5.1—5-10

After configuring IP cache flow, you decide you want to wait a few minutes for the routers to process some packets.

You decide to look for issues with the current IOS image on SanFran. First you review what image SanFran is running.



Viewing the IOS Version on SanFran

```
SanFran#show version
Cisco Internetwork Operating System Software
IOS (tm) C2600 Software (C2600-IO3-M), Version 12.2(10a), RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2002 by cisco Systems, Inc.
Compiled Tue 21-May-02 13:57 by pwade
Image text-base: 0x80008088, data-base: 0x80A11A68

ROM: System Bootstrap, Version 12.1(3r)T2, RELEASE SOFTWARE (fc1)

SanFran uptime is 35 minutes
System returned to ROM by reload
System image file is "flash:c2600-io3-mz.122-10a.bin"

cisco 2621 (MPC860) processor (revision 0x200) with 28672K/4096K bytes of
memory.
Processor board ID JAD051605U8 (2328523549)
M860 processor: part number 0, mask 49
Bridging software.
X.25 software, Version 3.0.0.
1 Ethernet/IEEE 802.3 interface(s)
2 FastEthernet/IEEE 802.3 interface(s)
2 Serial network interface(s)
32K bytes of non-volatile configuration memory.
8192K bytes of processor board System flash (Read/Write)

Configuration register is 0x2102
SanFran#
```

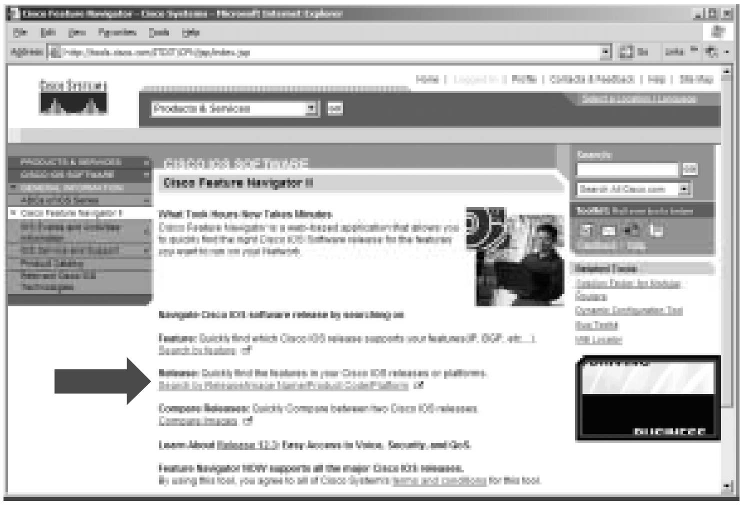
CIT 5.1—5-11

SanFran is running the IOS image c2600-io3-mz.122-10a.

Next, you go to Cisco.com to review the IOS Release status.

Reviewing IOS Release Status on the Cisco Feature Navigator

Cisco.com



Cisco Feature Navigator - Cisco Systems - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address
Home | Logged In | Profile | Contacts & Feedback | Help | Site Map
Products & Services
PRODUCTS & SERVICES
CISCO IOS SOFTWARE
GENERAL INFORMATION
Cisco Feature Navigator II
Search
Search All Cisco.com
Related Tools

CISCO IOS SOFTWARE

Cisco Feature Navigator II

What Took Hours Now Takes Minutes

Cisco Feature Navigator is a web-based application that allows you to quickly find the right Cisco IOS Software release for the features you want to run on your Network.

Navigate Cisco IOS software release by searching on

Feature: Quickly find which Cisco IOS release supports your features(IP, OSPF, etc...). Search by feature

Release: Quickly find the features in your Cisco IOS releases or platforms. Search by Release/Image Name/Product Code/Platform

Compare Releases: Quickly Compare between two Cisco IOS releases. Compare Images

Learn About Release 12.3: Easy Access to Voice, Security, and QoS.

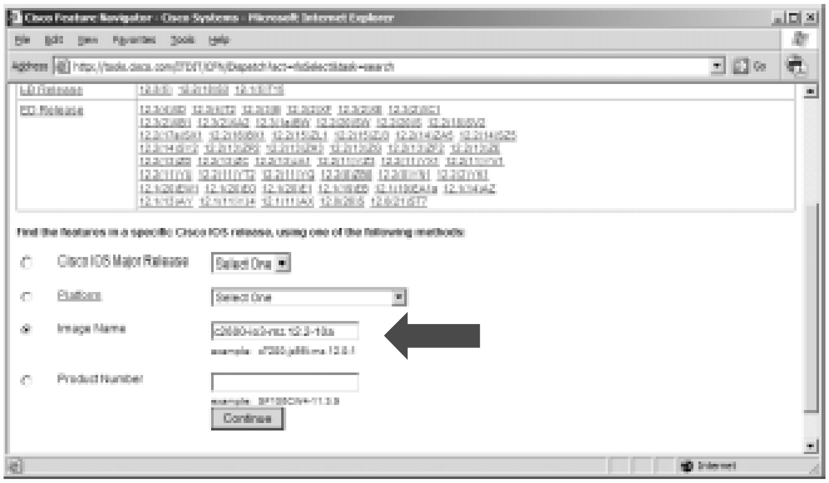
Feature Navigator NOW supports all the major Cisco IOS releases. By using this tool, you agree to all of Cisco Systems's terms and conditions for this tool.

CIT 5.1—5-12

Note The actual navigation steps to get to this screen are not shown. You needed to log onto http://www.cisco.com and go to the Cisco Feature Navigator under Products and Services.

Finding Features by IOS Image Name on the Cisco Feature Navigator

Cisco.com



Find the features in a specific Cisco IOS release, using one of the following methods:

○ Cisco IOS Major Release — Select One

○ Platform — Select One

● Image Name — c2600-io3-mz.12.2-10a
example: c7200-js56i-mz.12.0.1

○ Product Number —
example: [illegible]

Continue

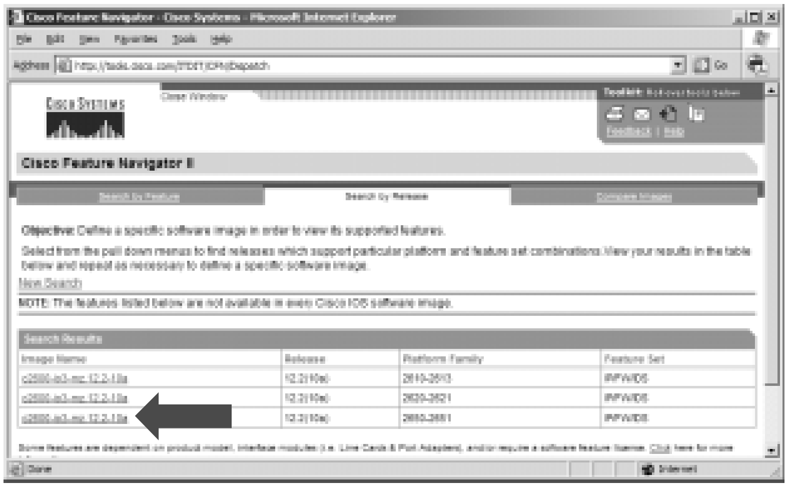
CIT 5.1—5-13

You enter the image name used by SanFran.

You work through the Feature Navigator screens.

Reviewing IOS Release Status on the Cisco Feature Navigator

Cisco.com



Cisco Feature Navigator II

Objective: Define a specific software image in order to view its supported features.

Select from the pull down menus to find releases which support particular platform and feature set combinations. View your results in the table below and repeat as necessary to define a specific software image.

NOTE: The features listed below are not available in every Cisco IOS software image.

Search Results

Image Name	Release	Platform Family	Feature Set
c2600-io3-mz.12.2-10a	12.2(10a)	2610-2613	IP/FW/IDS
c2600-io3-mz.12.2-10a	12.2(10a)	2620-2621	IP/FW/IDS
c2600-io3-mz.12.2-10a	12.2(10a)	2650-2651	IP/FW/IDS

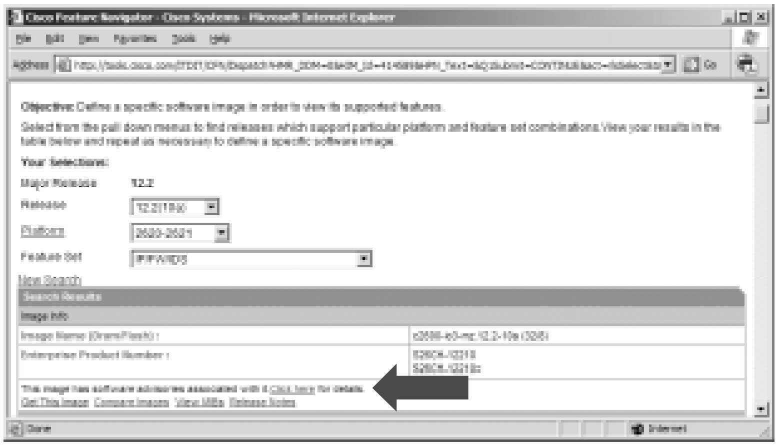
Some features are dependent on product model, interface modules (i.e. Line Cards & Port Adapters), and/or require a software feature license. Click here for more

CIT 5.1—5-14

You select one of the images.

Looking for Software Advisories for a Specific Image

Cisco.com


Cisco Feature Navigator - Cisco Systems - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address
Go
Done
Internet

Objective: Define a specific software image in order to view its supported features.

Select from the pull down menus to find releases which support particular platform and feature set combinations. View your results in the table below and repeat as necessary to define a specific software image.

Your Selections:

Major Release	12.2
Release	12.2(10a)
Platform	2620-2621
Feature Set	IP/FW/IDS

New Search

Search Results

Image Info

Image Name (Dram/Flash) :	c2600-io3-mz.12.2-10a (32/8)
Enterprise Product Number :	S26CH-12210 S26CH-12210c

This image has software advisories associated with it. Click here for details.

Get This Image Compare Images View MIBs Release Notes

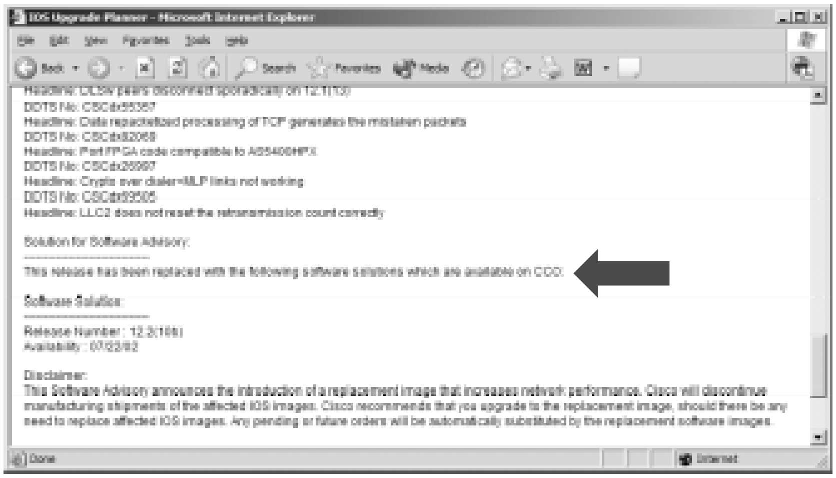
CIT 5.1—5-15

You see that the image has software advisories associated with it, so you go review them.

You review the advisories and note that the release has been replaced by a new image.

Reviewing the Software Advisories for a Specific Image (Cont.)

Cisco.com


IOS Upgrade Planner - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Media
Done
Internet

Headline: DLSw peers disconnect sporadically on 12.1(13)
DDTS No: CSCdx55357
Headline: Data repacketized processing of TCP generates the mistaken packets
DDTS No: CSCdx82069
Headline: Port FPGA code compatible to AS5400HPX
DDTS No: CSCdx26997
Headline: Crypto over dialer+MLP links not working
DDTS No: CSCdx93505
Headline: LLC2 does not reset the retransmission count correctly

Solution for Software Advisory:

This release has been replaced with the following software solutions which are available on CCO:

Software Solution:

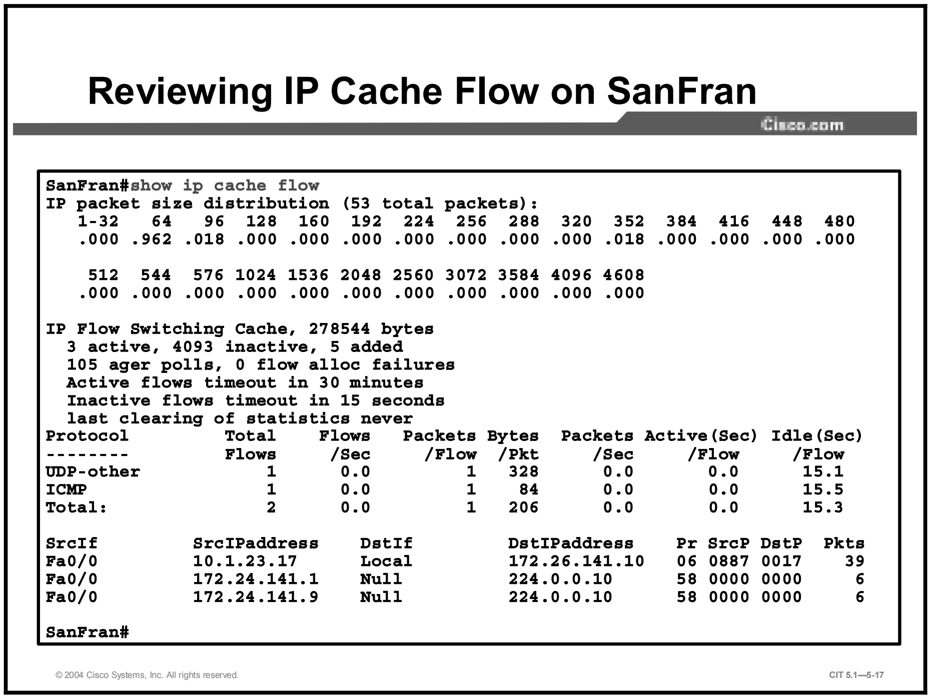
Release Number : 12.2(10b)
Availability : 07/22/02

Disclaimer:
This Software Advisory announces the introduction of a replacement image that increases network performance. Cisco will discontinue manufacturing shipments of the affected IOS images. Cisco recommends that you upgrade to the replacement image, should there be any need to replace affected IOS images. Any pending or future orders will be automatically substituted by the replacement software images.

CIT 5.1—5-16

You decide that you will need to upgrade the image. Because this image is several releases back, you will need to determine which most recent version supports your requirements and hardware.

Now you want to check the status of IP traffic flows in your network.



Reviewing IP Cache Flow on SanFran

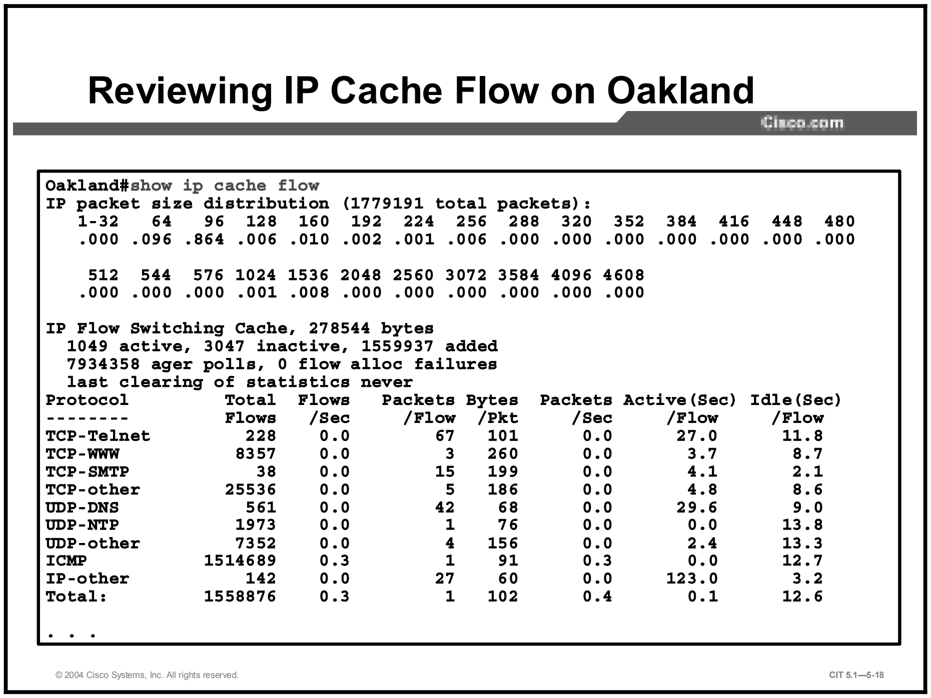
```
SanFran#show ip cache flow
IP packet size distribution (53 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .000 .962 .018 .000 .000 .000 .000 .000 .000 .000 .018 .000 .000 .000 .000

    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 278544 bytes
  3 active, 4093 inactive, 5 added
  105 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
  last clearing of statistics never
Protocol         Total    Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------         Flows     /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow
UDP-other            1      0.0         1   328      0.0       0.0      15.1
ICMP                 1      0.0         1    84      0.0       0.0      15.5
Total:               2      0.0         1   206      0.0       0.0      15.3

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Fa0/0         10.1.23.17      Local         172.26.141.10   06 0887 0017    39
Fa0/0         172.24.141.1    Null          224.0.0.10      58 0000 0000     6
Fa0/0         172.24.141.9    Null          224.0.0.10      58 0000 0000     6

SanFran#
```

© 2004 Cisco Systems, Inc. All rights reserved.

CIT 5.1—5-17

There are not any suspicious flows on SanFran.

You look at the traffic flows on Oakland.



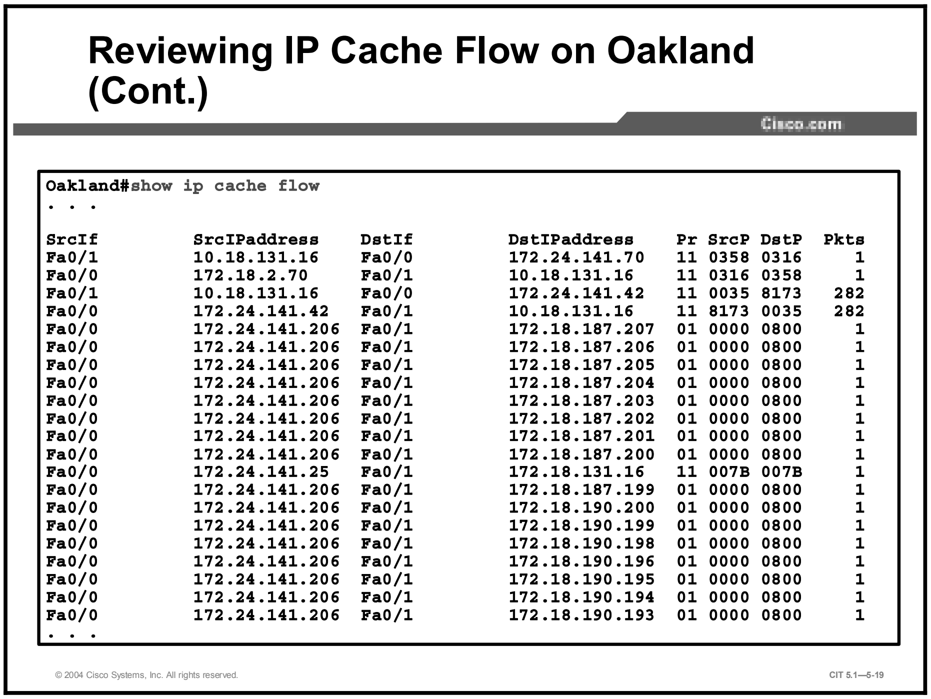
Reviewing IP Cache Flow on Oakland

```
Oakland#show ip cache flow
IP packet size distribution (1779191 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .000 .096 .864 .006 .010 .002 .001 .006 .000 .000 .000 .000 .000 .000 .000

    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .000 .000 .000 .001 .008 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 278544 bytes
  1049 active, 3047 inactive, 1559937 added
  7934358 ager polls, 0 flow alloc failures
  last clearing of statistics never
Protocol         Total  Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------         Flows   /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow
TCP-Telnet         228    0.0        67   101      0.0      27.0      11.8
TCP-WWW           8357    0.0         3   260      0.0       3.7       8.7
TCP-SMTP            38    0.0        15   199      0.0       4.1       2.1
TCP-other        25536    0.0         5   186      0.0       4.8       8.6
UDP-DNS            561    0.0        42    68      0.0      29.6       9.0
UDP-NTP           1973    0.0         1    76      0.0       0.0      13.8
UDP-other         7352    0.0         4   156      0.0       2.4      13.3
ICMP           1514689    0.3         1    91      0.3       0.0      12.7
IP-other           142    0.0        27    60      0.0     123.0       3.2
Total:         1558876    0.3         1   102      0.4       0.1      12.6

. . .
```

© 2004 Cisco Systems, Inc. All rights reserved.

CIT 5.1—5-18

You notice that ICMP traffic constitutes the major percentage of the total flows and that the majority of packets are between 64 and 96 bytes. This is a very unusual traffic pattern.



Reviewing IP Cache Flow on Oakland (Cont.)

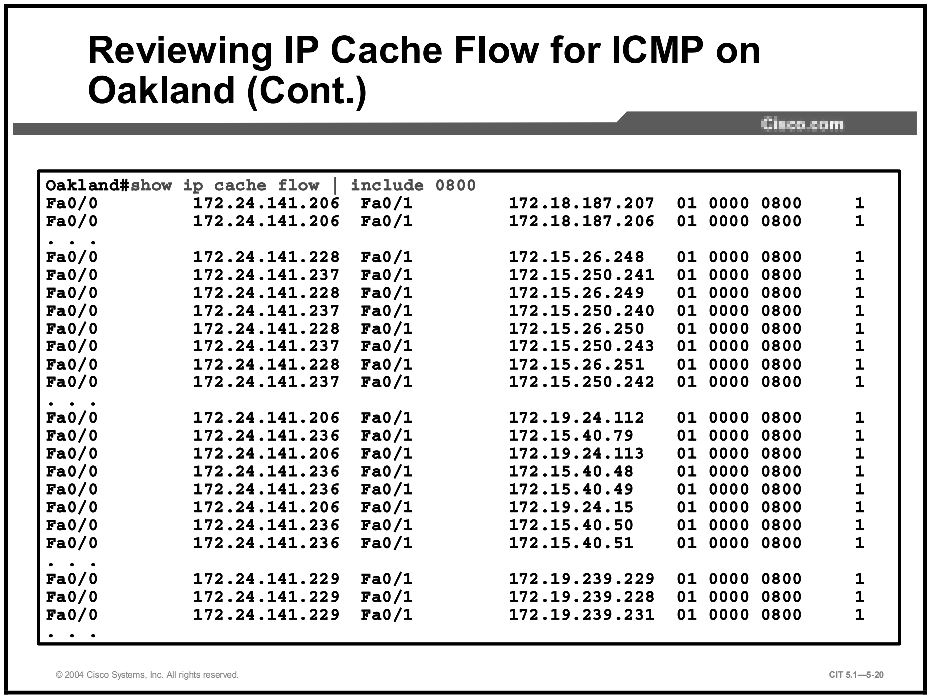
```
Oakland#show ip cache flow
. . .
SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Fa0/1         10.18.131.16    Fa0/0         172.24.141.70   11 0358 0316     1
Fa0/0         172.18.2.70     Fa0/1         10.18.131.16    11 0316 0358     1
Fa0/1         10.18.131.16    Fa0/0         172.24.141.42   11 0035 8173   282
Fa0/0         172.24.141.42   Fa0/1         10.18.131.16    11 8173 0035   282
Fa0/0         172.24.141.206  Fa0/1         172.18.187.207  01 0000 0800     1
Fa0/0         172.24.141.206  Fa0/1         172.18.187.206  01 0000 0800     1
Fa0/0         172.24.141.206  Fa0/1         172.18.187.205  01 0000 0800     1
Fa0/0         172.24.141.206  Fa0/1         172.18.187.204  01 0000 0800     1
Fa0/0         172.24.141.206  Fa0/1         172.18.187.203  01 0000 0800     1
Fa0/0         172.24.141.206  Fa0/1         172.18.187.202  01 0000 0800     1
Fa0/0         172.24.141.206  Fa0/1         172.18.187.201  01 0000 0800     1
Fa0/0         172.24.141.206  Fa0/1         172.18.187.200  01 0000 0800     1
Fa0/0         172.24.141.25   Fa0/1         172.18.131.16   11 007B 007B     1
Fa0/0         172.24.141.206  Fa0/1         172.18.187.199  01 0000 0800     1
Fa0/0         172.24.141.206  Fa0/1         172.18.190.200  01 0000 0800     1
Fa0/0         172.24.141.206  Fa0/1         172.18.190.199  01 0000 0800     1
Fa0/0         172.24.141.206  Fa0/1         172.18.190.198  01 0000 0800     1
Fa0/0         172.24.141.206  Fa0/1         172.18.190.196  01 0000 0800     1
Fa0/0         172.24.141.206  Fa0/1         172.18.190.195  01 0000 0800     1
Fa0/0         172.24.141.206  Fa0/1         172.18.190.194  01 0000 0800     1
Fa0/0         172.24.141.206  Fa0/1         172.18.190.193  01 0000 0800     1
. . .
```

CIT 5.1—5-19

As you scroll through the output, you notice that many sequential flows have been attempted from device 172.24.141.206 to devices in the 172.18.190.0 network. Oakland routes this traffic to SanFran. Although you are using private addressing inside your network, SanFran has no route via the Internet to any device in the 172.18.190.0 network.

You believe that there is a virus in your network. You surmise that the IP input process on SanFran is using up a lot of resources handling traffic to which SanFran does not have a valid route.

You look for other devices with the same destination port using the **show ip cache flow | include 0800** command.



Reviewing IP Cache Flow for ICMP on Oakland (Cont.)

Cisco.com

```
Oakland#show ip cache flow | include 0800
Fa0/0         172.24.141.206  Fa0/1         172.18.187.207  01 0000 0800     1
Fa0/0         172.24.141.206  Fa0/1         172.18.187.206  01 0000 0800     1
. . .
Fa0/0         172.24.141.228  Fa0/1         172.15.26.248   01 0000 0800     1
Fa0/0         172.24.141.237  Fa0/1         172.15.250.241  01 0000 0800     1
Fa0/0         172.24.141.228  Fa0/1         172.15.26.249   01 0000 0800     1
Fa0/0         172.24.141.237  Fa0/1         172.15.250.240  01 0000 0800     1
Fa0/0         172.24.141.228  Fa0/1         172.15.26.250   01 0000 0800     1
Fa0/0         172.24.141.237  Fa0/1         172.15.250.243  01 0000 0800     1
Fa0/0         172.24.141.228  Fa0/1         172.15.26.251   01 0000 0800     1
Fa0/0         172.24.141.237  Fa0/1         172.15.250.242  01 0000 0800     1
. . .
Fa0/0         172.24.141.206  Fa0/1         172.19.24.112   01 0000 0800     1
Fa0/0         172.24.141.236  Fa0/1         172.15.40.79    01 0000 0800     1
Fa0/0         172.24.141.206  Fa0/1         172.19.24.113   01 0000 0800     1
Fa0/0         172.24.141.236  Fa0/1         172.15.40.48    01 0000 0800     1
Fa0/0         172.24.141.236  Fa0/1         172.15.40.49    01 0000 0800     1
Fa0/0         172.24.141.206  Fa0/1         172.19.24.15    01 0000 0800     1
Fa0/0         172.24.141.236  Fa0/1         172.15.40.50    01 0000 0800     1
Fa0/0         172.24.141.236  Fa0/1         172.15.40.51    01 0000 0800     1
. . .
Fa0/0         172.24.141.229  Fa0/1         172.19.239.229  01 0000 0800     1
Fa0/0         172.24.141.229  Fa0/1         172.19.239.228  01 0000 0800     1
Fa0/0         172.24.141.229  Fa0/1         172.19.239.231  01 0000 0800     1
. . .
```

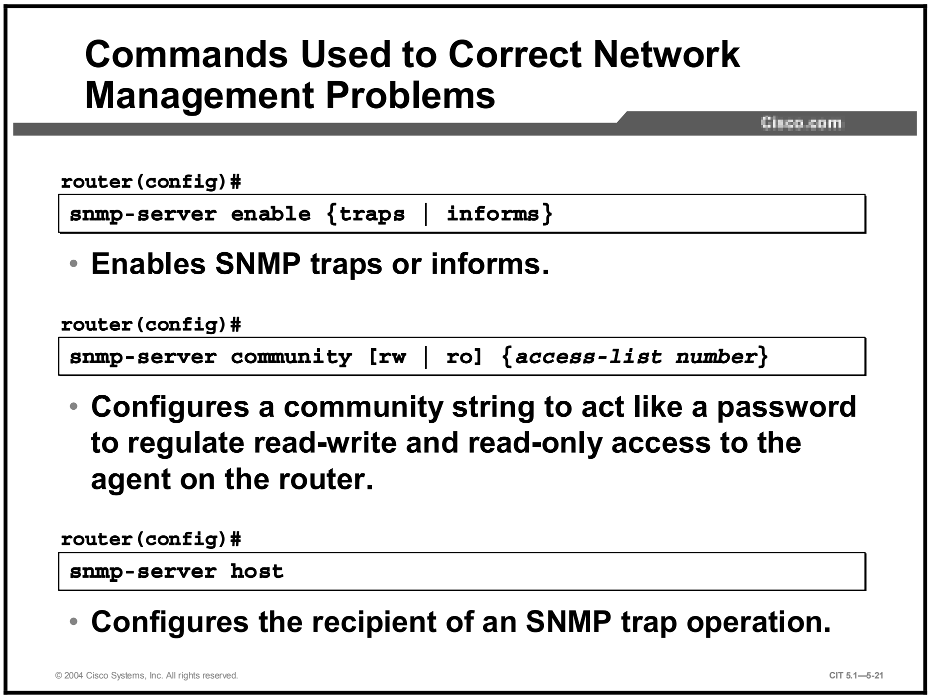
CIT 5.1—5-20

You see several internal devices that appear to be infected, perhaps with some variant of the Nachi virus.

Now it is time to tell the MIS department the IP addresses of devices that you suspect to be infected. You will work with MIS to clean up the device and network issues.

Identifying Commands and Applications Used to Correct Problems Occurring at the Application Layer

This topic identifies selected commands and applications used by troubleshooters to correct problems occurring at the application layer.



Commands Used to Correct Network Management Problems

```
router(config)#
snmp-server enable {traps | informs}
```

- Enables SNMP traps or informs.

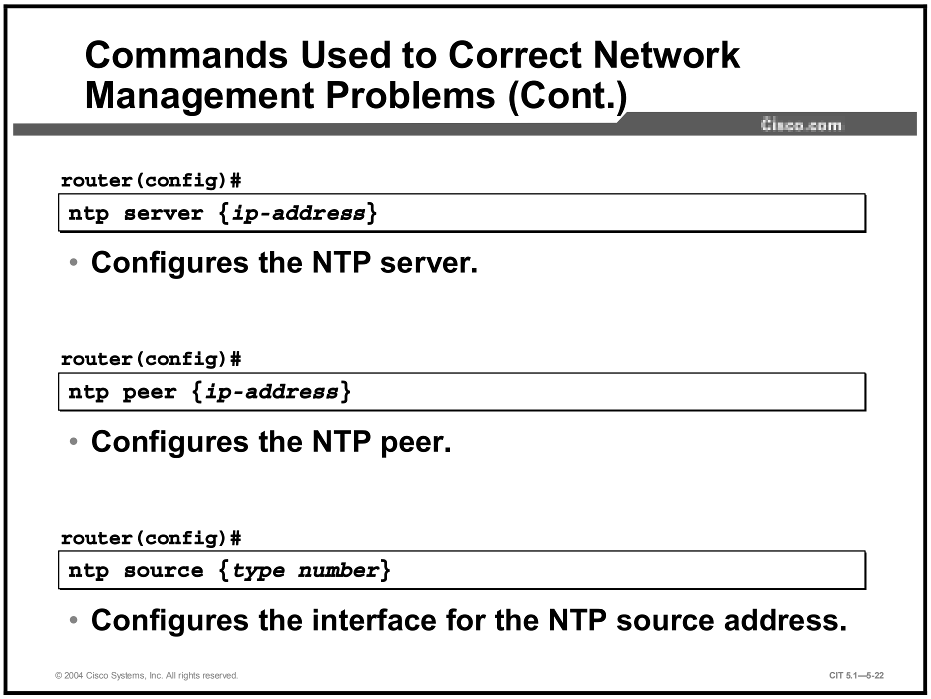
```
router(config)#
snmp-server community [rw | ro] {access-list number}
```

- Configures a community string to act like a password to regulate read-write and read-only access to the agent on the router.

```
router(config)#
snmp-server host
```

- Configures the recipient of an SNMP trap operation.

CIT 5.1—6-21



Commands Used to Correct Network Management Problems (Cont.)

```
router(config)#
ntp server {ip-address}
```

- Configures the NTP server.

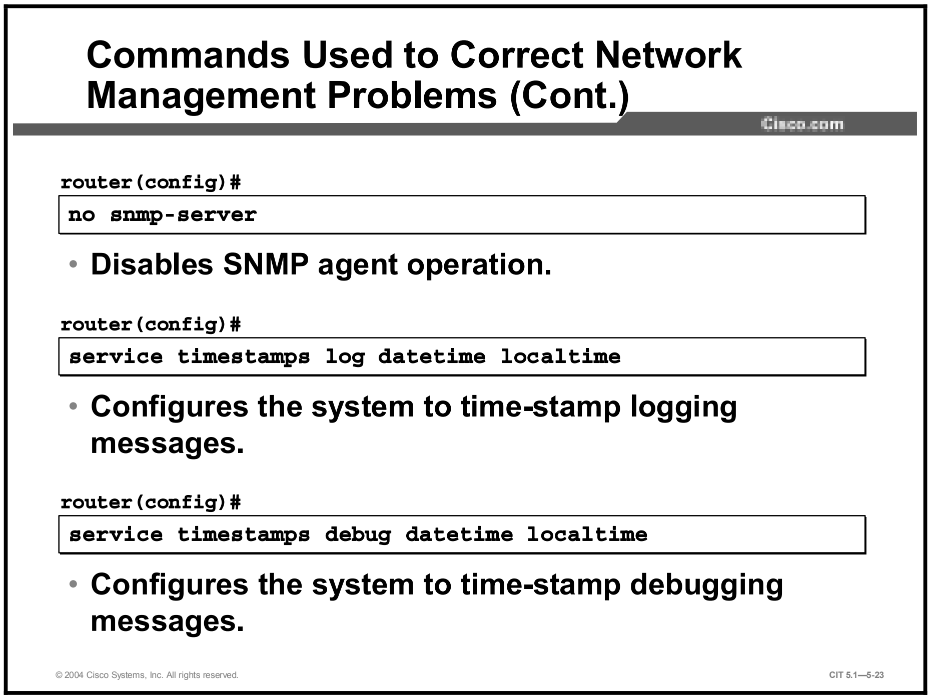
```
router(config)#
ntp peer {ip-address}
```

- Configures the NTP peer.

```
router(config)#
ntp source {type number}
```

- Configures the interface for the NTP source address.

CIT 5.1—6-22



Commands Used to Correct Network Management Problems (Cont.)

router(config)#

```
no snmp-server
```

- **Disables SNMP agent operation.**

router(config)#

```
service timestamps log datetime localtime
```

- **Configures the system to time-stamp logging messages.**

router(config)#

```
service timestamps debug datetime localtime
```

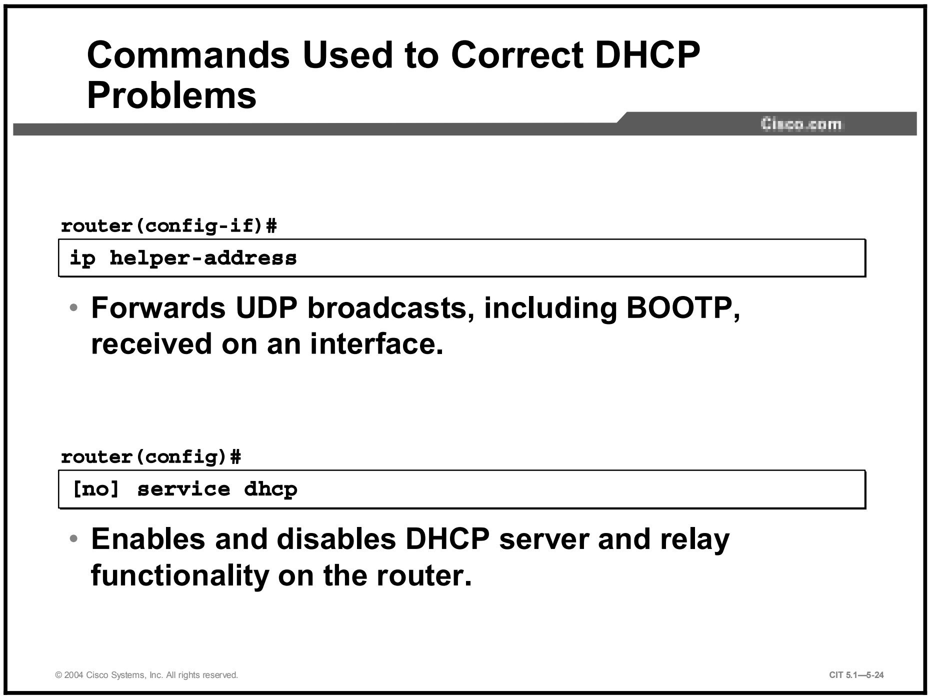
- **Configures the system to time-stamp debugging messages.**

CIT 5.1—5-23

Troubleshooters can use the commands listed in the table to make configuration changes to correct problems with network management protocols at the application layer.

Commands Used to Correct Network Management Problems

Command	Description
snmp-server enable {**traps** | **informs**}	Enables SNMP traps or informs.
snmp-server community [**rw** | **ro**] {*access-list number*}	Configures a community string to act like a password to regulate read-write and read-only access to the agent on the router.
snmp-server host	Configures the recipient of an SNMP trap operation.
ntp server {*ip-address*}	Configures the NTP server.
ntp peer {*ip-address*}	Configures the NTP peer.
ntp source {*type number*}	Configures the interface for the NTP source address.
no snmp-server	Disables SNMP agent operation.
service timestamps log datetime localtime	Configures the system to time-stamp logging messages.
service timestamps debug datetime localtime	Configures the system to time-stamp debugging messages.



Commands Used to Correct DHCP Problems

```
router(config-if)#
ip helper-address
```

- Forwards UDP broadcasts, including BOOTP, received on an interface.

```
router(config)#
[no] service dhcp
```

- Enables and disables DHCP server and relay functionality on the router.

CIT 5.1—5-24

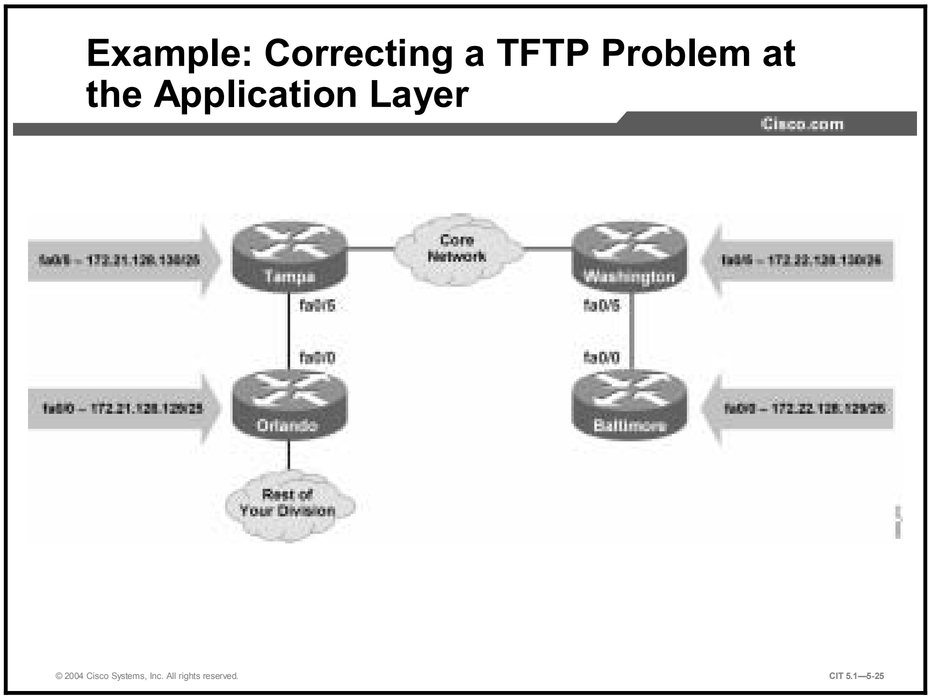
Troubleshooters can use the commands listed in the table to make configuration changes to correct problems with DHCP at the application layer.

Commands Used to Correct DHCP Problems

Command	Description
ip helper-address	Forwards UDP broadcasts, including Bootstrap Protocol (BOOTP), received on an interface.
[**no**] **service dhcp**	Enables and disables DHCP server and relay functionality on the router.

Example: Correcting a TFTP Problem at the Application Layer

You are the second-level network engineer for Orlando. You have console access to the distribution router named Orlando and IP connectivity to all other devices in your division. Your division supports the 172.21.0.0/16 subnet.



Example: Correcting a TFTP Problem at the Application Layer

Cisco.com
fa0/5 – 172.21.128.130/25
Tampa
Core Network
Washington
fa0/5 – 172.22.128.130/25
fa0/5
fa0/0
fa0/5
fa0/0
fa0/0 – 172.21.128.129/25
Orlando
Baltimore
fa0/0 – 172.22.128.129/25
Rest of Your Division

CIT 5.1—5-25

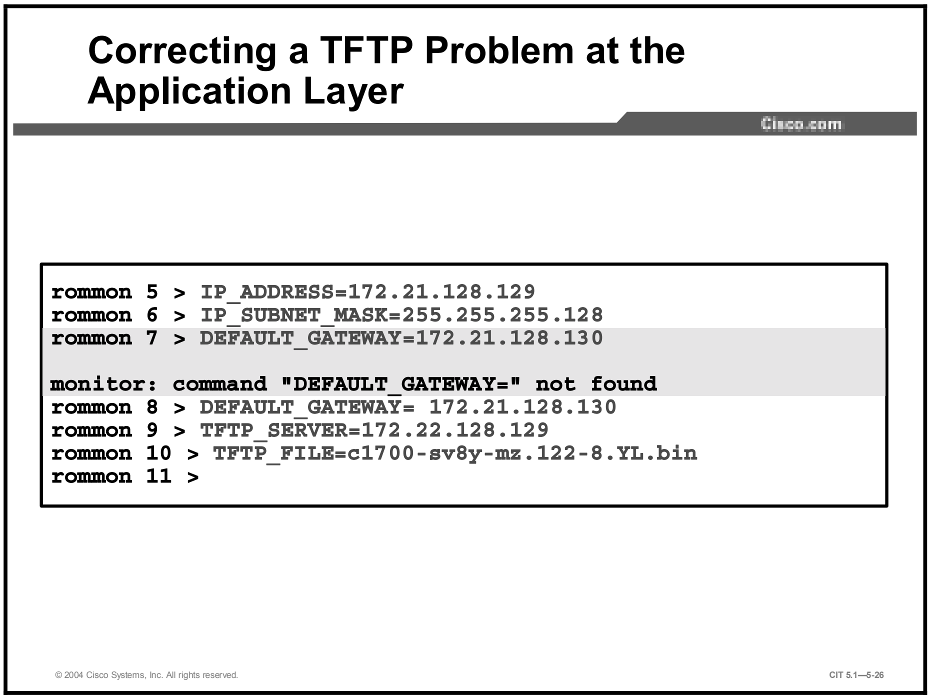
The IOS image has been accidentally erased from Orlando. Baltimore has a TFTP server running that offers an image with the file name “flash:c1700-sv8y-mz.122-8.YL.bin” for your use. You isolated the TFTP issues: the **tftpdnld rommon** command needs the IP address and mask for the local router, the default gateway for the local router, the IP address of the TFTP server, and the name of the file to be transferred.

You make a list of these values:

```
Local IP address = 172.21.128.129

Local Mask = 255.255.255.128

Local Default Gateway = 172.21.128.130

TFTP Server = 172.22.128.129

File = c1700-sv8y-mz.122-8.YL.bin
```

You review the relevant information on Cisco.com and know that you need to enter the following command to set these variables: **variable_name=***variable*.

Now you need to configure the TFTP variables on Orlando.



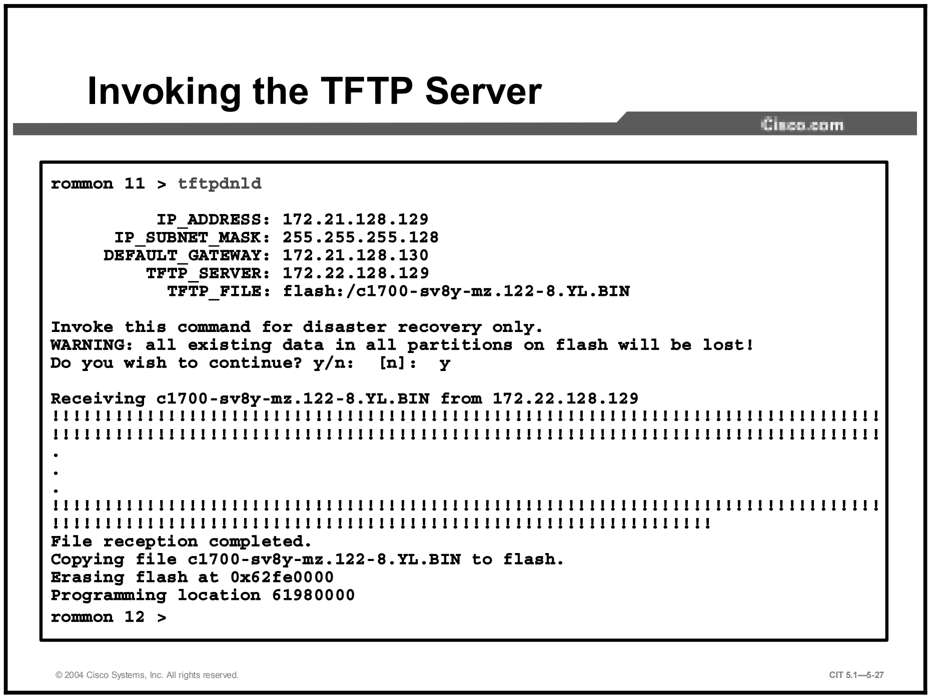
Correcting a TFTP Problem at the Application Layer

```
rommon 5 > IP_ADDRESS=172.21.128.129
rommon 6 > IP_SUBNET_MASK=255.255.255.128
rommon 7 > DEFAULT_GATEWAY=172.21.128.130

monitor: command "DEFAULT_GATEWAY=" not found
rommon 8 > DEFAULT_GATEWAY= 172.21.128.130
rommon 9 > TFTP_SERVER=172.22.128.129
rommon 10 > TFTP_FILE=c1700-sv8y-mz.122-8.YL.bin
rommon 11 >
```

CIT 5.1—5-26

The variables have been configured after you remove an extra space.

You now invoke the TFTP program.



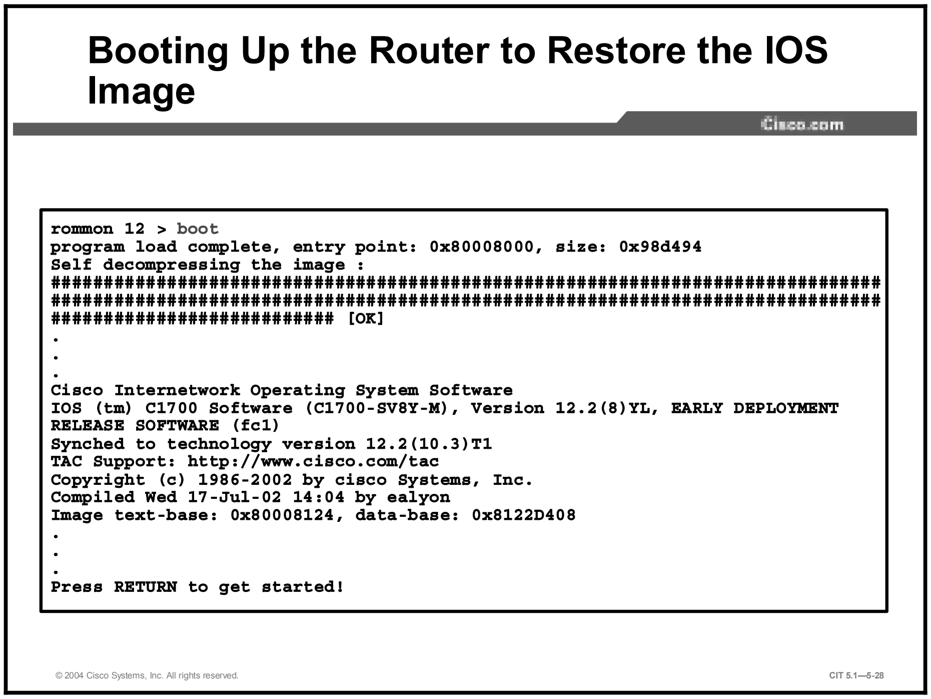
Invoking the TFTP Server

```
rommon 11 > tftpdnld

          IP_ADDRESS: 172.21.128.129
      IP_SUBNET_MASK: 255.255.255.128
     DEFAULT_GATEWAY: 172.21.128.130
         TFTP_SERVER: 172.22.128.129
           TFTP_FILE: flash:/c1700-sv8y-mz.122-8.YL.BIN

Invoke this command for disaster recovery only.
WARNING: all existing data in all partitions on flash will be lost!
Do you wish to continue? y/n:  [n]:  y

Receiving c1700-sv8y-mz.122-8.YL.BIN from 172.22.128.129
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
.
.
.
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
File reception completed.
Copying file c1700-sv8y-mz.122-8.YL.BIN to flash.
Erasing flash at 0x62fe0000
Programming location 61980000
rommon 12 >
```

© 2004 Cisco Systems, Inc. All rights reserved. CIT 5.1—5-27

After configuring the parameters to support TFTP, the TFTP download process appears to work. You have resolved the application layer issue of missing TFTP parameters.

You now need to boot up the router using the new image.



Booting Up the Router to Restore the IOS Image

```
rommon 12 > boot
program load complete, entry point: 0x80008000, size: 0x98d494
Self decompressing the image :
###############################################################################
###############################################################################
############################ [OK]
.
.
.
Cisco Internetwork Operating System Software
IOS (tm) C1700 Software (C1700-SV8Y-M), Version 12.2(8)YL, EARLY DEPLOYMENT
RELEASE SOFTWARE (fc1)
Synched to technology version 12.2(10.3)T1
TAC Support: http://www.cisco.com/tac
Copyright (c) 1986-2002 by cisco Systems, Inc.
Compiled Wed 17-Jul-02 14:04 by ealyon
Image text-base: 0x80008124, data-base: 0x8122D408
.
.
.
Press RETURN to get started!
```

© 2004 Cisco Systems, Inc. All rights reserved. CIT 5.1—5-28

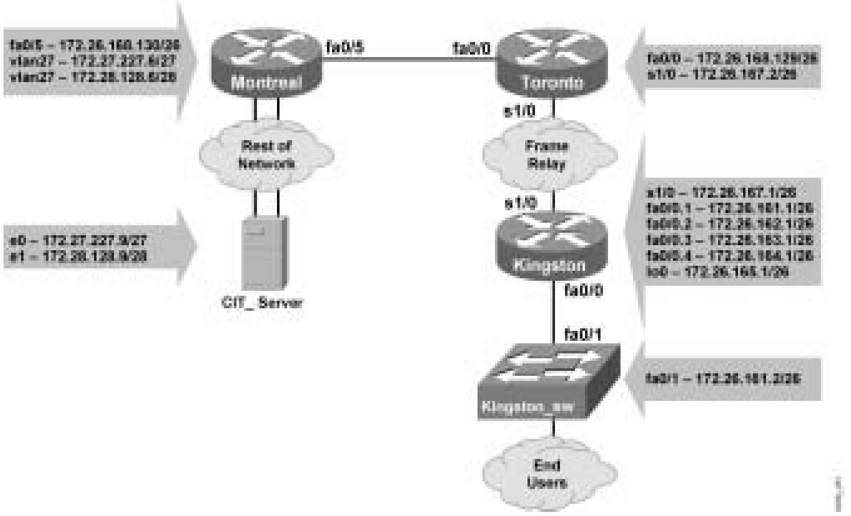
The IOS image has been restored. You finish by restoring the baseline configuration files.

Example: Correcting a Problem at the Application Layer

You are the second-level network engineer in Kingston. You have console access to the access router named Kingston and IP connectivity to all other devices in your division. Your division supports the 172.26.0.0/16 subnet.

Example: Correcting a Problem at the Application Layer

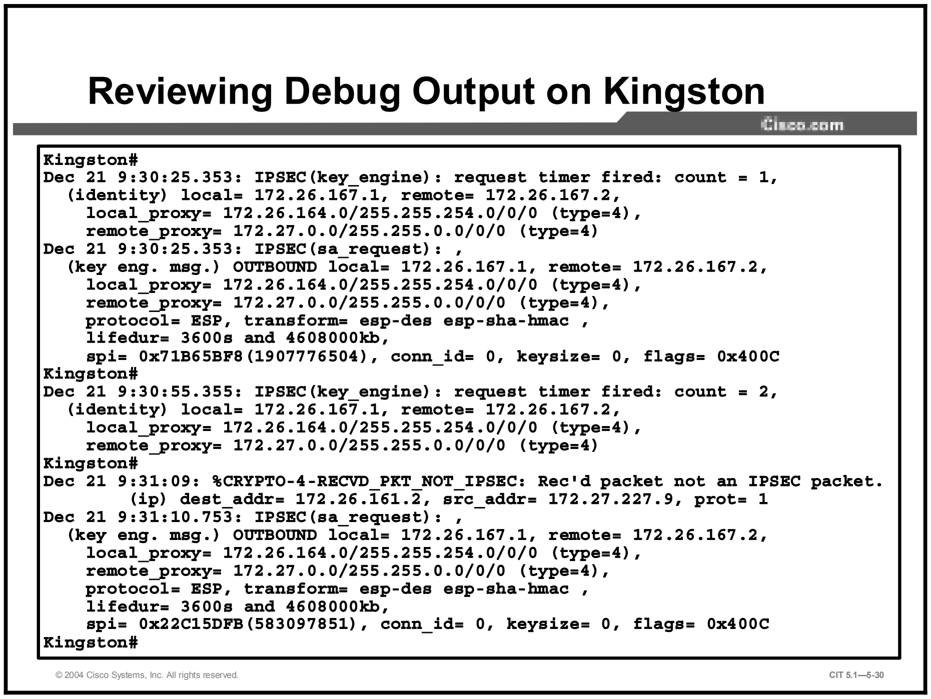
Cisco.com



CIT 5.1—5-29

You have determined that a recent IPSec configuration between Toronto and Kingston is broken. You believe there is a policy setup error in the IPSec peers. IPSec negotiation between the remote peers fails. You should have already isolated the issue.

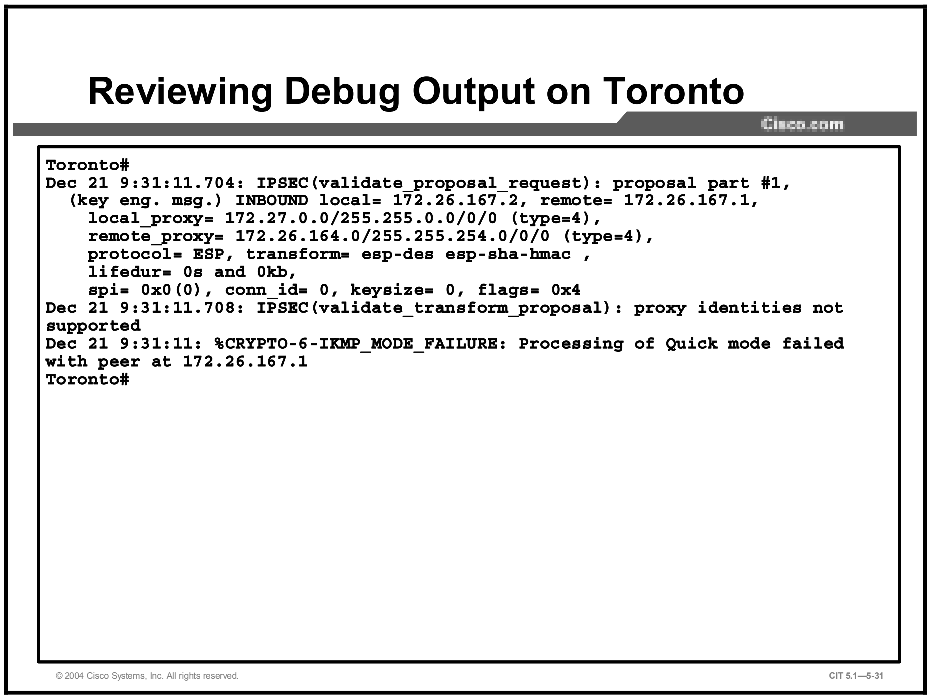
As needed, review the previous **debug crypto ipsec** command output.



Reviewing Debug Output on Kingston

```
Kingston#
Dec 21 9:30:25.353: IPSEC(key_engine): request timer fired: count = 1,
  (identity) local= 172.26.167.1, remote= 172.26.167.2,
    local_proxy= 172.26.164.0/255.255.254.0/0/0 (type=4),
    remote_proxy= 172.27.0.0/255.255.0.0/0/0 (type=4)
Dec 21 9:30:25.353: IPSEC(sa_request): ,
  (key eng. msg.) OUTBOUND local= 172.26.167.1, remote= 172.26.167.2,
    local_proxy= 172.26.164.0/255.255.254.0/0/0 (type=4),
    remote_proxy= 172.27.0.0/255.255.0.0/0/0 (type=4),
    protocol= ESP, transform= esp-des esp-sha-hmac ,
    lifedur= 3600s and 4608000kb,
    spi= 0x71B65BF8(1907776504), conn_id= 0, keysize= 0, flags= 0x400C
Kingston#
Dec 21 9:30:55.355: IPSEC(key_engine): request timer fired: count = 2,
  (identity) local= 172.26.167.1, remote= 172.26.167.2,
    local_proxy= 172.26.164.0/255.255.254.0/0/0 (type=4),
    remote_proxy= 172.27.0.0/255.255.0.0/0/0 (type=4)
Kingston#
Dec 21 9:31:09: %CRYPTO-4-RECVD_PKT_NOT_IPSEC: Rec'd packet not an IPSEC packet.
        (ip) dest_addr= 172.26.161.2, src_addr= 172.27.227.9, prot= 1
Dec 21 9:31:10.753: IPSEC(sa_request): ,
  (key eng. msg.) OUTBOUND local= 172.26.167.1, remote= 172.26.167.2,
    local_proxy= 172.26.164.0/255.255.254.0/0/0 (type=4),
    remote_proxy= 172.27.0.0/255.255.0.0/0/0 (type=4),
    protocol= ESP, transform= esp-des esp-sha-hmac ,
    lifedur= 3600s and 4608000kb,
    spi= 0x22C15DFB(583097851), conn_id= 0, keysize= 0, flags= 0x400C
Kingston#
```

© 2004 Cisco Systems, Inc. All rights reserved. CIT 5.1—5-30



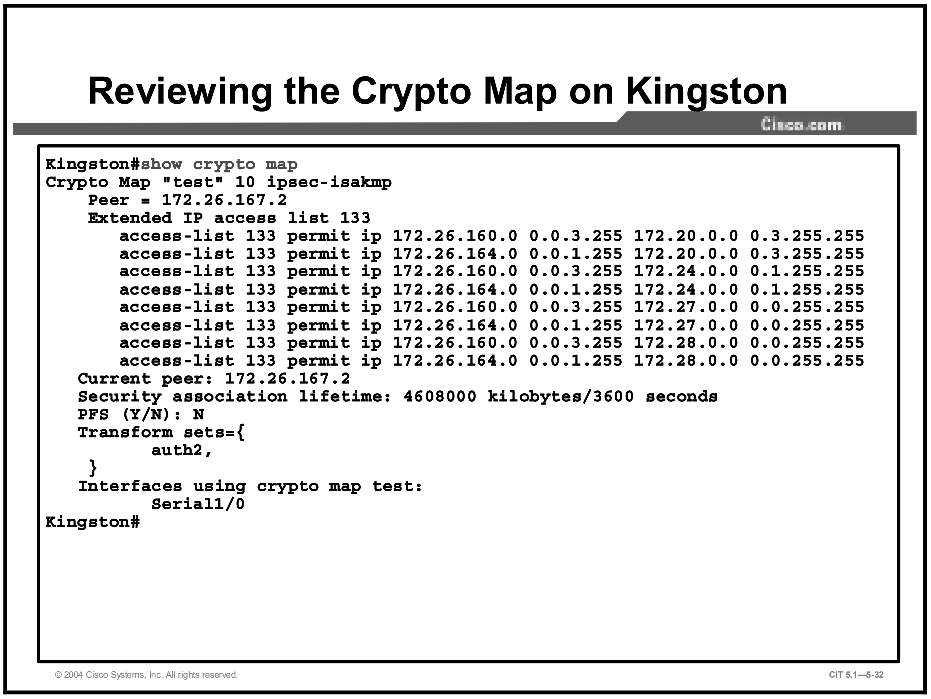
Reviewing Debug Output on Toronto

```
Toronto#
Dec 21 9:31:11.704: IPSEC(validate_proposal_request): proposal part #1,
  (key eng. msg.) INBOUND local= 172.26.167.2, remote= 172.26.167.1,
    local_proxy= 172.27.0.0/255.255.0.0/0/0 (type=4),
    remote_proxy= 172.26.164.0/255.255.254.0/0/0 (type=4),
    protocol= ESP, transform= esp-des esp-sha-hmac ,
    lifedur= 0s and 0kb,
    spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
Dec 21 9:31:11.708: IPSEC(validate_transform_proposal): proxy identities not
supported
Dec 21 9:31:11: %CRYPTO-6-IKMP_MODE_FAILURE: Processing of Quick mode failed
with peer at 172.26.167.1
Toronto#
```

© 2004 Cisco Systems, Inc. All rights reserved. CIT 5.1—5-31

This output should help you identify the problem.

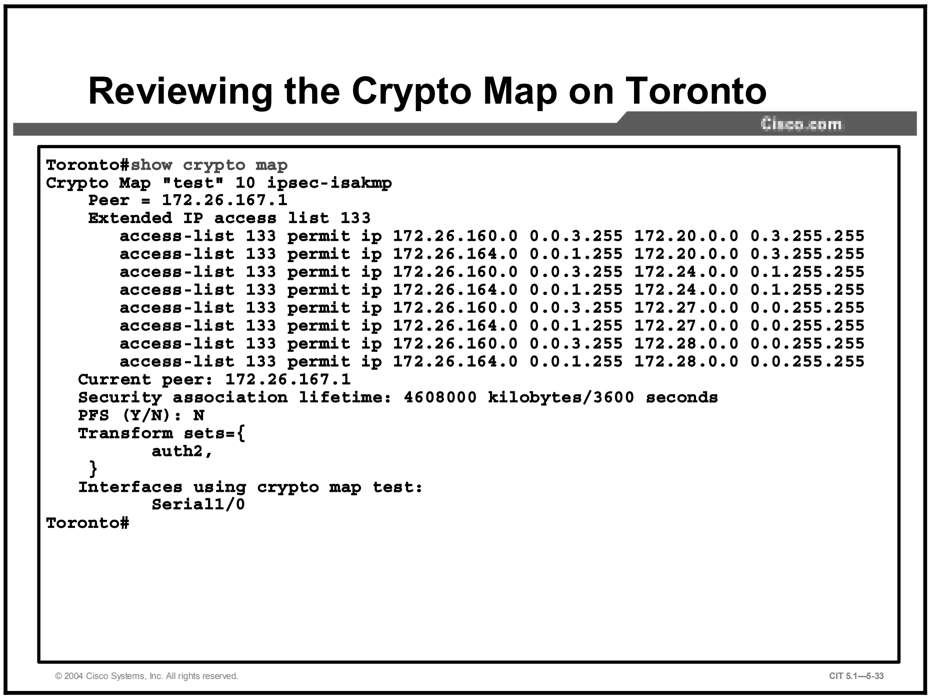
Verify the exact problem with the **show crypto map** command.



Reviewing the Crypto Map on Kingston

```
Kingston#show crypto map
Crypto Map "test" 10 ipsec-isakmp
    Peer = 172.26.167.2
    Extended IP access list 133
       access-list 133 permit ip 172.26.160.0 0.0.3.255 172.20.0.0 0.3.255.255
       access-list 133 permit ip 172.26.164.0 0.0.1.255 172.20.0.0 0.3.255.255
       access-list 133 permit ip 172.26.160.0 0.0.3.255 172.24.0.0 0.1.255.255
       access-list 133 permit ip 172.26.164.0 0.0.1.255 172.24.0.0 0.1.255.255
       access-list 133 permit ip 172.26.160.0 0.0.3.255 172.27.0.0 0.0.255.255
       access-list 133 permit ip 172.26.164.0 0.0.1.255 172.27.0.0 0.0.255.255
       access-list 133 permit ip 172.26.160.0 0.0.3.255 172.28.0.0 0.0.255.255
       access-list 133 permit ip 172.26.164.0 0.0.1.255 172.28.0.0 0.0.255.255
   Current peer: 172.26.167.2
   Security association lifetime: 4608000 kilobytes/3600 seconds
   PFS (Y/N): N
   Transform sets={
          auth2,
    }
   Interfaces using crypto map test:
          Serial1/0
Kingston#
```

© 2004 Cisco Systems, Inc. All rights reserved. CIT 5.1—5-32



Reviewing the Crypto Map on Toronto

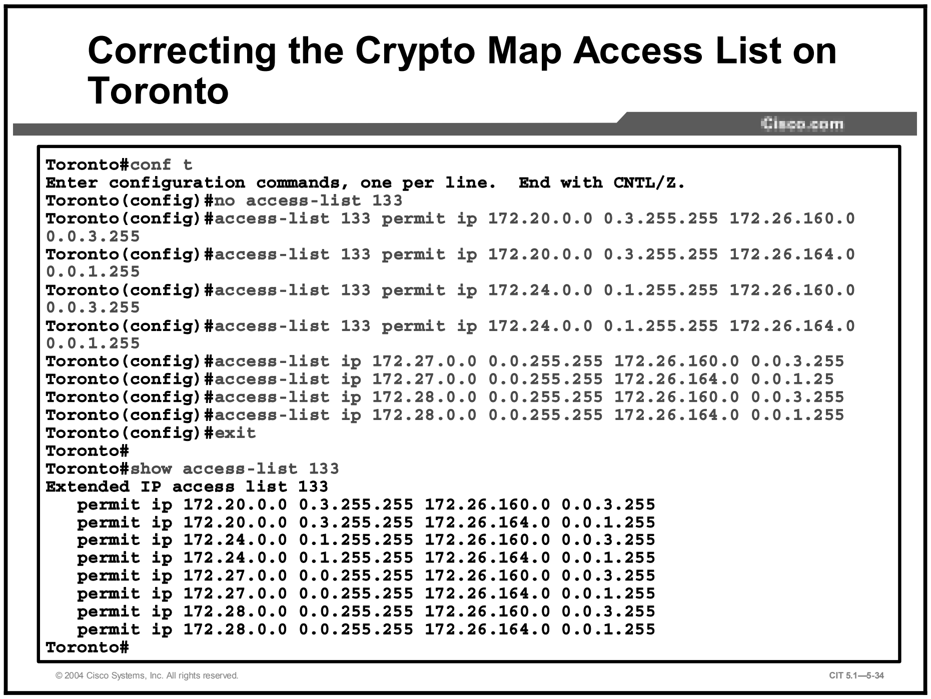
```
Toronto#show crypto map
Crypto Map "test" 10 ipsec-isakmp
    Peer = 172.26.167.1
    Extended IP access list 133
       access-list 133 permit ip 172.26.160.0 0.0.3.255 172.20.0.0 0.3.255.255
       access-list 133 permit ip 172.26.164.0 0.0.1.255 172.20.0.0 0.3.255.255
       access-list 133 permit ip 172.26.160.0 0.0.3.255 172.24.0.0 0.1.255.255
       access-list 133 permit ip 172.26.164.0 0.0.1.255 172.24.0.0 0.1.255.255
       access-list 133 permit ip 172.26.160.0 0.0.3.255 172.27.0.0 0.0.255.255
       access-list 133 permit ip 172.26.164.0 0.0.1.255 172.27.0.0 0.0.255.255
       access-list 133 permit ip 172.26.160.0 0.0.3.255 172.28.0.0 0.0.255.255
       access-list 133 permit ip 172.26.164.0 0.0.1.255 172.28.0.0 0.0.255.255
   Current peer: 172.26.167.1
   Security association lifetime: 4608000 kilobytes/3600 seconds
   PFS (Y/N): N
   Transform sets={
          auth2,
    }
   Interfaces using crypto map test:
          Serial1/0
Toronto#
```

© 2004 Cisco Systems, Inc. All rights reserved. CIT 5.1—5-33

These screens should clarify the issue. The access list is duplicated on the two peers, but it should be a mirror image on one router. Which one should be replaced?

Toronto has an incorrect access list. The access list on Toronto needs to identify the subnets reachable via Fast Ethernet 0/0 (or from Montreal) as being the source of traffic to encapsulate. Based on the current network, these subnets include 172.21.0.0, 172.22.0.0, 172.23.0.0, 172.240.0, 172.25.0.0, 172.27.227.0, and 172.28.128.0. The destinations for this traffic are the remote subnets reachable via Kingston, or 172.26.161.0, 172.26.162.0, 172.26.163.0, 172.26.164.0, and 172.26.165.0. Currently, access list 133 has been misconfigured and is a duplicate of the access list on Kingston. The misconfiguration reverses the proper sources and destinations for traffic.

You remove the old access list and configure the correct one to mirror the access list on Kingston.



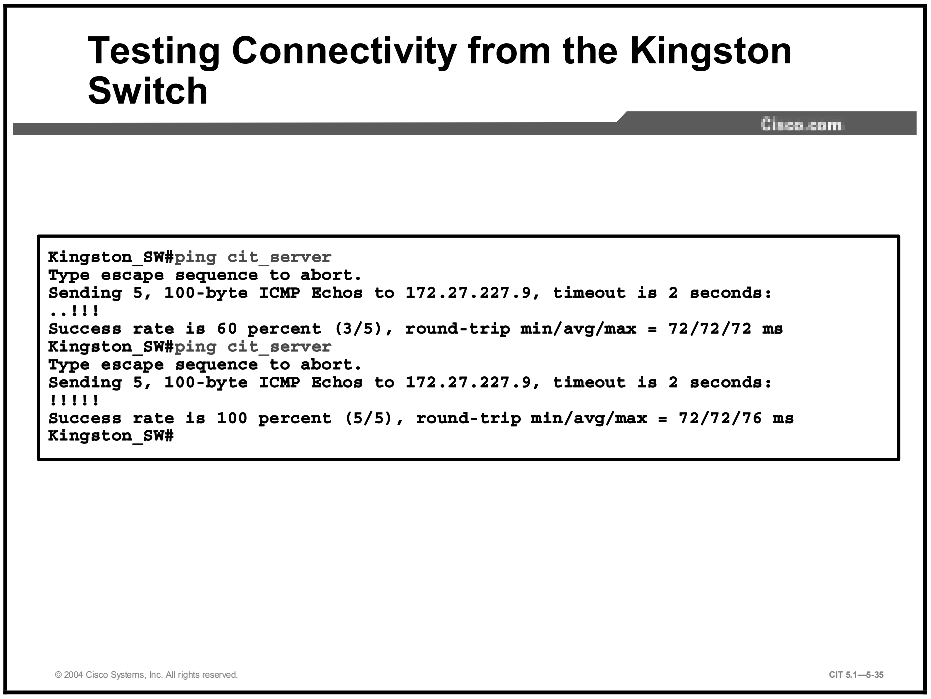
Correcting the Crypto Map Access List on Toronto

```
Toronto#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Toronto(config)#no access-list 133
Toronto(config)#access-list 133 permit ip 172.20.0.0 0.3.255.255 172.26.160.0
0.0.3.255
Toronto(config)#access-list 133 permit ip 172.20.0.0 0.3.255.255 172.26.164.0
0.0.1.255
Toronto(config)#access-list 133 permit ip 172.24.0.0 0.1.255.255 172.26.160.0
0.0.3.255
Toronto(config)#access-list 133 permit ip 172.24.0.0 0.1.255.255 172.26.164.0
0.0.1.255
Toronto(config)#access-list ip 172.27.0.0 0.0.255.255 172.26.160.0 0.0.3.255
Toronto(config)#access-list ip 172.27.0.0 0.0.255.255 172.26.164.0 0.0.1.25
Toronto(config)#access-list ip 172.28.0.0 0.0.255.255 172.26.160.0 0.0.3.255
Toronto(config)#access-list ip 172.28.0.0 0.0.255.255 172.26.164.0 0.0.1.255
Toronto(config)#exit
Toronto#
Toronto#show access-list 133
Extended IP access list 133
   permit ip 172.20.0.0 0.3.255.255 172.26.160.0 0.0.3.255
   permit ip 172.20.0.0 0.3.255.255 172.26.164.0 0.0.1.255
   permit ip 172.24.0.0 0.1.255.255 172.26.160.0 0.0.3.255
   permit ip 172.24.0.0 0.1.255.255 172.26.164.0 0.0.1.255
   permit ip 172.27.0.0 0.0.255.255 172.26.160.0 0.0.3.255
   permit ip 172.27.0.0 0.0.255.255 172.26.164.0 0.0.1.255
   permit ip 172.28.0.0 0.0.255.255 172.26.160.0 0.0.3.255
   permit ip 172.28.0.0 0.0.255.255 172.26.164.0 0.0.1.255
Toronto#
```

CIT 5.1—5-34

You check the new access list with the **show access-list 133** command and see that the new access list now properly mirrors the access list on Kingston.

Finally, you verify that Kingston_SW has access to the CIT_Server.



Testing Connectivity from the Kingston Switch

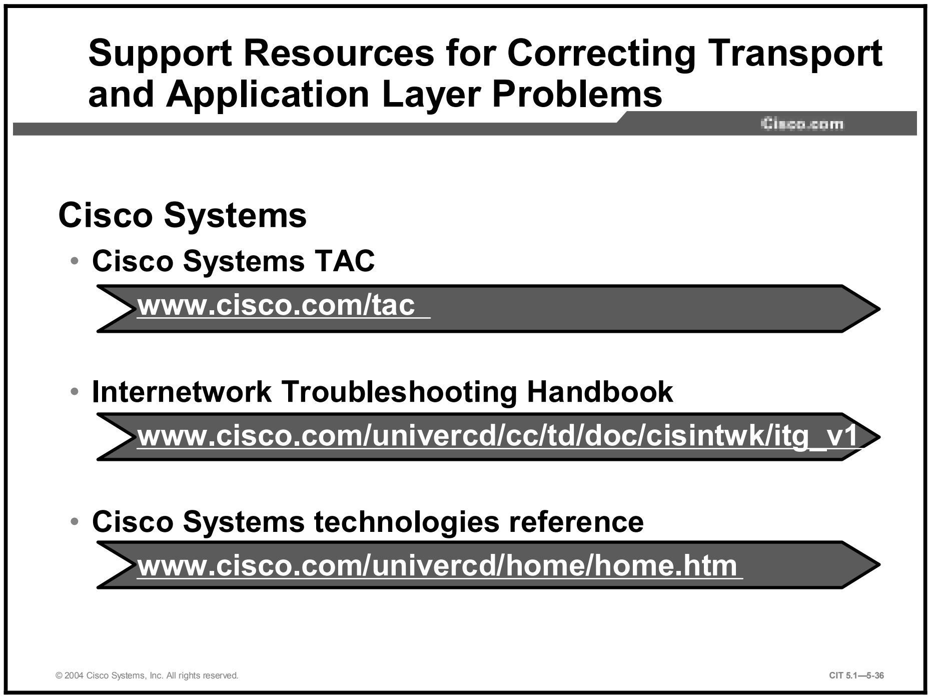
```
Kingston_SW#ping cit_server
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.27.227.9, timeout is 2 seconds:
..!!!
Success rate is 60 percent (3/5), round-trip min/avg/max = 72/72/72 ms
Kingston_SW#ping cit_server
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.27.227.9, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 72/72/76 ms
Kingston_SW#
```

You may notice that the first two packets did not receive a reply on the initial ping test. This is due to time delays in establishing IKE and IPsec security associations. The second ping test was 100 percent successful.

You have resolved the issue.

Identifying Transport and Application Layer Support Resources

This topic identifies support resources used to assist troubleshooters to correct problems occurring at the transport and application layers.



Support Resources for Correcting Transport and Application Layer Problems

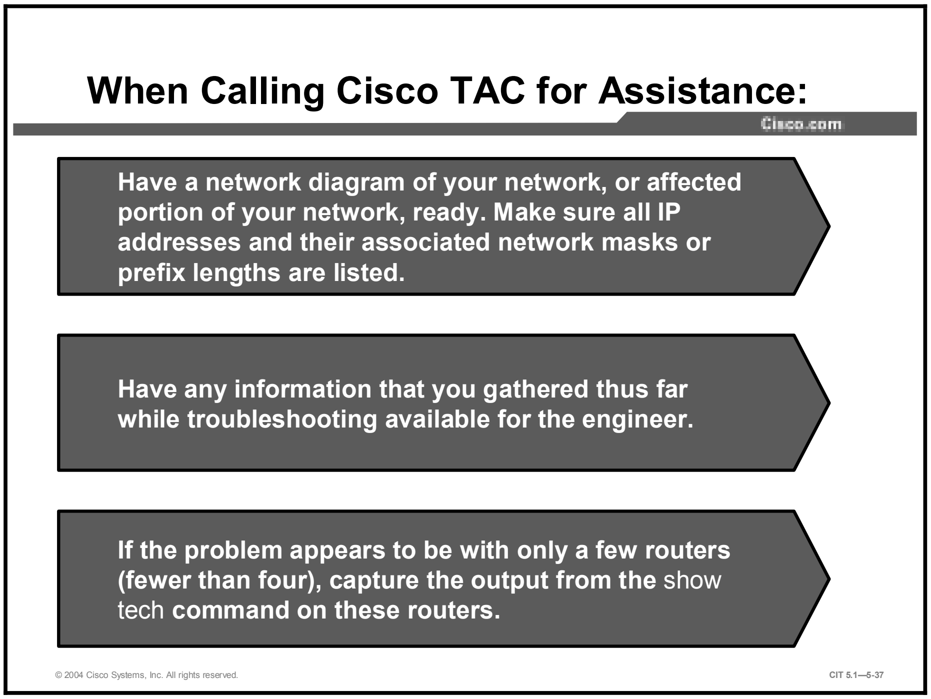
Cisco Systems

- **Cisco Systems TAC**
  - www.cisco.com/tac
- **Internetwork Troubleshooting Handbook**
  - www.cisco.com/univercd/cc/td/doc/cisintwk/itg_v1
- **Cisco Systems technologies reference**
  - www.cisco.com/univercd/home/home.htm

CIT 5.1—5-36

Even as you develop knowledge and experience in networking, there may be times when you will need to consult additional resources. These support resources are commonly used as reference materials for commands and configuration procedures and for research on technology-specific information and industry standards.

The Cisco Systems website has one of the largest collections of networking information on the Internet. Visit Cisco.com to use the Technical Assistance Center (TAC), Internetwork Troubleshooting Handbook, and technology reference pages to find information for troubleshooting Cisco Systems products. From these locations, you can search on a specific topic, such as extended access list and IPSec. It is often helpful to narrow searches by including phrases such as “configuration examples” or “troubleshooting.” You can also use the various tools on the site, such as the Output Interpreter, which will analyze command output from your network devices.



When Calling Cisco TAC for Assistance:

- Have a network diagram of your network, or affected portion of your network, ready. Make sure all IP addresses and their associated network masks or prefix lengths are listed.
- Have any information that you gathered thus far while troubleshooting available for the engineer.
- If the problem appears to be with only a few routers (fewer than four), capture the output from the show tech command on these routers.

CIT 5.1—5-37

Before calling Cisco TAC, do the following and document the results so that you can be easily assisted:

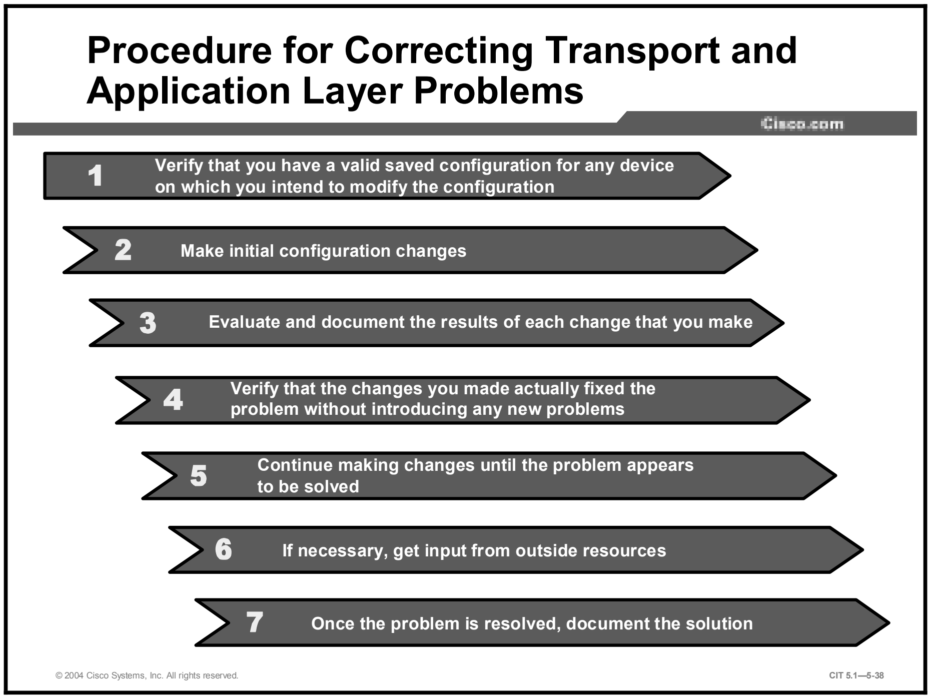
- Have a network diagram of your network, or affected portion of your network, ready. Make sure that all IP addresses and their associated network masks or prefix lengths are listed.
- Have any information that you gathered thus far while troubleshooting available for the engineer.
- If the problem appears to be with only a few routers (fewer than four), capture the output from the **show tech** command on these routers.

Dial-in or Telnet access also helps considerably in effective problem resolution.

Note Many problems with applications can be resolved by reading technical documentation at the website of the software vendor or developer. These sites also have patches and version updates that a troubleshooter can download to repair bugs or incompatibilities.

Correcting Problems Occurring at the Transport and Application Layers

This topic identifies the steps that troubleshooters use for correcting problems occurring at the transport and application layers.



Procedure for Correcting Transport and Application Layer Problems

Cisco.com

1 Verify that you have a valid saved configuration for any device on which you intend to modify the configuration

2 Make initial configuration changes

3 Evaluate and document the results of each change that you make

4 Verify that the changes you made actually fixed the problem without introducing any new problems

5 Continue making changes until the problem appears to be solved

6 If necessary, get input from outside resources

7 Once the problem is resolved, document the solution

CIT 5.1—5-38

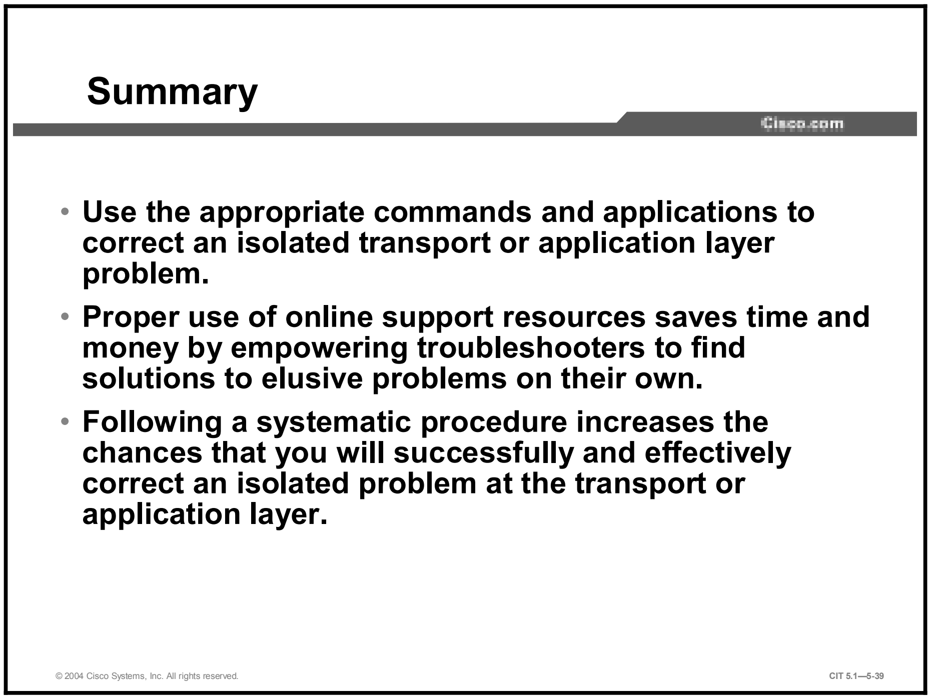
The table lists the suggested steps that a troubleshooter uses for correcting an isolated problem at the physical and data link layers.

Table for Correcting Problems Occurring at the Transport and Application Layers

Step	Description
1	Ensure that you have a valid saved configuration for any device on which you intend to modify the configuration. This provides for eventual recovery to a known initial state.
2	Make initial hardware and software configuration changes. If the correction requires more than one change, make only one change at a time.
3	Evaluate and document the changes and the results of each change that you make. If you perform your problem-solving steps and the results are unsuccessful, immediately undo the changes. If the problem is intermittent, you may need to wait to see if the problem occurs again before you can evaluate the effect of your changes.
4	Verify that the changes you made actually fixed the problem without introducing any new problems. The network should be returned to the baseline operation, and no new or old symptoms should be present. If the problem is not solved, undo all the changes that you made. If you discover new or additional problems while you are making corrections, step back and modify your correction plan.
5	Stop making changes when the original problem appears to be solved.
6	If necessary, get input from outside resources. If none of your attempts to correct the problem are successful, take the problem to another person. This may be a coworker, consultant, or Cisco TAC. On rare occasions, you may need to perform a core dump, which creates output that a specialist at Cisco Systems can analyze.
7	Once the problem is resolved, document the solution.

Summary

This topic summarizes the key points discussed in this lesson.



Summary

Cisco.com

- Use the appropriate commands and applications to correct an isolated transport or application layer problem.
- Proper use of online support resources saves time and money by empowering troubleshooters to find solutions to elusive problems on their own.
- Following a systematic procedure increases the chances that you will successfully and effectively correct an isolated problem at the transport or application layer.

© 2004 Cisco Systems, Inc. All rights reserved.

CIT 5.1—5-39

References

For additional information, refer to these resources:

- Cisco online documentation: http://www.cisco.com/univercd/home/home.htm
- Cisco Technical Assistance Center (TAC): http://www.cisco.com/tac
- Troubleshooting TCP/IP: http://www.cisco.com/univercd/cc/td/doc/cisintwk/itg_v1/tr1907.htm
- Enabling High Performance Data Transfers: http://www.psc.edu/networking/perf_tune.html

Next Steps

For the associated case study and lab exercises, refer to the following sections of the course Lab Guide:

- Case Study (Trouble Ticket G) 5-1: Isolating Problems at the Transport and Application Layers
- Lab Exercise (Trouble Ticket G) 5-1: Correcting Problems at the Transport and Application Layers
- Lab Exercise (Trouble Ticket H) 5-2: Troubleshooting Problems at All Logical Layers

Quiz

Use the practice items here to review what you have learned in this lesson. The correct answers are found in the Quiz Answer Key.

Q1) Which command would you enter to restrict TCP traffic on a particular host?

A) **outbound 3 deny tcp netmask 1**

B) **access-list 102 permit tcp any host 10.1.1.1 eq smtp**

C) **access-list 106 deny tcp any host 10.1.1.1 eq telnet**

D) **ip tcp window-size 2**

Q2) Which Cisco configuration command does a troubleshooter enter to activate unsolicited network management alarm messages when a threshold is exceeded?

A) **ip http accounting**

B) **snmp-server enable traps**

C) **ip helper-address**

D) **service dhcp**

Q3) Which website would you most likely visit to read the latest detailed technical documentation about the SMTP protocol?

A) http://www.ietf.com

B) http://www.itu.int/home

C) http://www.cisco.com

D) http://www.sniffers.com

Q4) Your satellite link traffic is experiencing the negative effects of drastically incorrect TCP windowing. To attempt to fix the problem, you initially examine the running configuration and make a few configuration changes. Which step of the procedure for correcting problems at the transport and application layers will you perform next?

A) Make initial configuration changes.

B) Stop making changes when the original problem appears to be solved.

C) Document the solution, once the problem is solved.

D) Evaluate and document the results of each change that you make.

Quiz Answer Key

Q1) C

Relates to: Identifying Commands and Applications Used to Correct Problems Occurring at the Transport Layer

Q2) B

Relates to: Identifying Commands and Applications Used to Correct Problems Occurring at the Application Layer

Q3) A

Relates to: Identifying Transport and Application Layer Support Resources

Q4) D

Relates to: Correcting Problems Occurring at the Transport and Application Layers

CIT

Course Glossary

The Course Glossary for *Cisco Internetwork Troubleshooting* (CIT) v5.1 highlights and defines key terms and acronyms used throughout this course. Many of these terms are also described in the Cisco Internetworking Terms and Acronyms resources, available via http://www.cisco.com.

Acronym or Term	Expansion of Acronym	Definition of Acronym or Term
ACL	access control list	Access lists filter network traffic by controlling whether routed packets are forwarded or blocked at the interface of the router. Your router examines each packet to determine whether to forward or drop the packet, based on the criteria you specified within the access lists. Access list criteria could be the source address of the traffic, the destination address of the traffic, the upper-layer protocol, or other information. Note that sophisticated users can sometimes successfully evade or fool basic access lists because no authentication is required
ANSI	American National Standards Institute	A voluntary organization composed of corporate, government, and other members that coordinates standards-related activities, approves U.S. national standards, and develops positions for the United States in international standards organizations. ANSI helps develop international and U.S. standards relating to, among other things, communications and networking. ANSI is a member of the IEC and the ISO.
application layer		Layer 7 of the OSI reference model. This layer provides services to application processes (such as e-mail, file transfer, and terminal emulation) that are outside the OSI model. The application layer identifies and establishes the availability of intended communication partners (and the resources required to connect with them), synchronizes cooperating applications, and establishes an agreement on the procedures for error recovery and the control of data integrity. Corresponds roughly with the transaction services layer in the SNA model.
ARP	Address Resolution Protocol	Internet protocol used to map an IP address to a MAC address. IETF Standard 37, it is defined in IETF RFC 826.
AS	autonomous system	A collection of networks under a common administration sharing a common routing strategy. Areas subdivide autonomous systems. An autonomous system must be assigned a unique 16-bit number by the IANA.
availability		The amount of time that a system or device is operational—that is, how long it is performing its intended function. Availability is represented as the ratio of the total time a device is operational during a given time interval to the length of that interval.
bandwidth		A term used to describe the capacity or throughput of a given network medium, interface, or protocol. In digital networks, bandwidth is usually stated in bits per second (bps). In analog media, it is the difference between the highest and lowest frequencies available for network signals. The frequency range necessary to convey a signal measured in units of hertz (Hz). For example, voice signals typically require approximately 3 kHz of bandwidth.

Acronym or Term	Expansion of Acronym	Definition of Acronym or Term
baseline		Documents network or system performance, configuration, and deployment at some defined point in time. Baselines taken at different points in time are useful in identifying changes in system load, performance degradation, and undocumented modifications to system configurations or topology.
BGP	Border Gateway Protocol	Interdomain exterior routing protocol that replaces EGP. BGP exchanges reachability information with other BGP systems. BGP-4 is most recently defined by RFC 1771.
CDP	Cisco Discovery Protocol	Media- and protocol-independent device-discovery protocol that runs on equipment manufactured by Cisco, including routers, access servers, bridges, and switches. Using CDP, a device can advertise its existence to other devices and receive information about other devices on the same LAN or on the remote side of a WAN. Runs on all media that support SNAP, including LANs, Frame Relay, and ATM media.
collision		In Ethernet, the result of two nodes transmitting simultaneously. The frames from each device impact and are damaged when they meet on the physical media.
congestion		A system or network condition that results when one or more network elements cannot serve the arriving traffic in a timely manner. Congestion is characterized by increased delay (latency), delay variation (jitter), and persistent queued traffic.
CRC	cyclic redundancy check	An error-checking technique in which the recipient calculates a value based on the frame or message content and compares the calculated value to a value stored in the frame or message of the sending node.
data flow		Grouping of traffic, identified in IP by a combination of source address/mask, destination address/mask, IP protocol field, and source and destination ports, where the protocol and port fields can have any of these. In effect, all traffic matching a specific combination of these values is grouped logically into a data flow. A data flow can represent a single TCP connection between two hosts, or it can represent all of the traffic between two subnets. IPSec protection applies to data flows.
data link layer		Layer 2 of the OSI reference model. Provides transit of data across a physical link. The data link layer is concerned with physical addressing and line discipline. The IEEE divided this layer into two sublayers: the MAC sublayer and the LLC sublayer. Sometimes, the data link layer is simply called the link layer. The data link layer roughly corresponds to the data link control layer of the SNA model.
DHCP	Dynamic Host Configuration Protocol	Provides a mechanism for allocating IP addresses dynamically so that addresses can be reused when hosts no longer need them. Defined in IETF RFC 2131 and updated by RFC 3396.

Acronym or Term	Expansion of Acronym	Definition of Acronym or Term
DNS	Domain Name System	System used on the Internet for translating names of network nodes into addresses. DNS (IETF Standard 13) is defined in IETF RFCs 1034 and 1035. The standard has been updated by a number of additional RFCs.
DTE	data terminal equipment	Device at the user end of a User-Network Interface that serves as a data source, destination, or both. DTE connects to a data network through a DCE device (for example, a modem) and typically uses clocking signals generated by the DCE. DTE includes devices such as computers, protocol translators, and multiplexers.
EIGRP	Enhanced Interior Gateway Routing Protocol	Advanced version of IGRP developed by Cisco Systems. Provides superior convergence properties and operating efficiency, and combines the advantages of link state protocols with those of distance vector protocols.
EMI	electromagnetic interference	Interference by electromagnetic signals that can cause reduced data integrity and increased error rates on transmission channels.
encapsulation		Wrapping of data in a particular protocol header. For example, Ethernet data is wrapped in a specific Ethernet header before data link transit. In addition, when bridging dissimilar networks, the entire frame from one network is placed in the header used by the data link layer protocol of the other network.
EtherChannel		Developed by Cisco Systems. Logical aggregation of multiple Ethernet interfaces used to form a single higher bandwidth routing or bridging endpoint.
FCS	frame check sequence	The standard 16-bit cyclic redundancy check used for HDLC and Frame Relay frames. The FCS detects bit errors occurring in the bits of the frame between the opening flag and the FCS and is only effective in detecting errors in frames no larger than 4096 octets. See also Cyclic Redundancy Check (CRC) above.
FTP	File Transfer Protocol	Application protocol, part of the TCP/IP protocol stack, used for transferring files between network nodes. FTP (IETF Standard 9) is defined in RFC 959.
flapping		A system condition characterized by oscillation between two or more states.
HTTP	Hypertext Transfer Protocol	The protocol used by web browsers and web servers to transfer files, such as text and graphic files.
IANA	Internet Assigned Numbers Authority	Organization responsible for assigning the parameter and protocol values necessary for operation and future development of the Internet.
ICMP	Internet Control Message Protocol	Network layer Internet protocol that reports errors and provides other information relevant to IP packet processing. Defined in IETF RFC 2131 and updated by RFC 3396.

Acronym or Term	Expansion of Acronym	Definition of Acronym or Term
IETF	Internet Engineering Task Force	Task force consisting of over 80 working groups responsible for developing Internet standards. The IETF operates under the auspices of ISOC.
IGP	Interior Gateway Protocol	Routing protocol used within an autonomous system in IP networks. Examples include RIP, EIGRP, OSPF, and IS-IS.
IP/TV	Internet Protocol TV	Protocol for viewing live streaming video over an IP network.
IS-IS Protocol	Intermediate System-to-Intermediate System Protocol	OSI link-state hierarchical routing protocol based on DECnet Phase V routing, whereby ISs (routers) exchange routing information based on a single metric to determine network topology.
ISOC	Internet Society	The main umbrella organization for Internet governance. It is an international membership organization.
ITU-T	International Telecommunication Union Telecommunication Standardization Sector	International body that develops worldwide standards for telecommunications technologies. The ITU-T carries out the functions of the former CCITT and is an organization within the United Nations System.
jabber		Error condition in which a network device continually transmits random, meaningless data onto the network.
jitter		The interpacket delay variance; that is, the difference between interpacket arrival and departure. Jitter is an important QoS metric for voice and video applications.
keepalive interval		Period between each keepalive message sent by a network device.
keepalive message		Message sent by a protocol instance on a network device to inform another protocol instance in the network that the virtual circuit between the two is still active.
latency		Delay. Common uses of the term include the time between when a device requests access to a network and the time permission is granted to transmit, and the time from transmission at the source to reception at the destination.
LMI	Local Management Interface	Set of enhancements to the basic Frame Relay and ATM specifications. In Frame Relay, LMI includes support for a keepalive mechanism, which verifies that data is flowing; a multicast mechanism, which provides the network server with its local DLCI and the multicast DLCI; global addressing, which gives DLCIs global rather than local significance in Frame Relay networks; and a status mechanism, which provides an ongoing status report on the DLCIs known to the switch. Known as LMT in ANSI terminology.
multiplexing		Scheme that allows multiple logical signals to transmit simultaneously across a single physical channel.

Acronym or Term	Expansion of Acronym	Definition of Acronym or Term
network layer		Layer 3 of the OSI reference model. This layer provides connectivity and path selection between two end systems. The network layer is the layer at which routing occurs. Corresponds roughly with the path control layer of the SNA model.
NMS	network management system	System responsible for managing at least part of a network. A NMS host system is generally a reasonably powerful and well-equipped computer, such as an engineering workstation. NMSs communicate with agents to help keep track of network statistics and resources.
noise		Undesirable communications channel signals.
OSI reference model	Open System Interconnection reference model	Network architectural model developed by ISO and ITU-T. The model consists of seven layers, each of which specifies particular network functions, such as addressing, flow control, error control, encapsulation, and reliable message transfer. The lowest layer (the physical layer) is closest to the media technology. The lower two layers are usually implemented in hardware and firmware, whereas the upper three layers are implemented only in software. The highest layer (the application layer) is closest to the user. The OSI reference model is used universally as a method for teaching and understanding network functionality.
OSPF	Open Shortest Path First	Link-state, hierarchical IGP routing algorithm proposed as a successor to RIP in the Internet community. OSPF features include least-cost routing, multipath routing, and load balancing. OSPF was derived from an early version of the IS-IS protocol.
peak rate		Maximum rate, in kilobits per second, at which a virtual circuit will transmit. Specified in a Service Level Specification, it is enforced at transport network ingress.
physical layer		Layer 1 of the OSI reference model. The physical layer defines the electrical, mechanical, procedural, and functional specifications for activating, maintaining, and deactivating the physical link between end systems. Corresponds with the physical control layer in the SNA model.
POP	Post Office Protocol or Point of Presence	Protocol that client e-mail applications use to retrieve mail from a mail server. The access point to a service providers transport network.
PVC	permanent virtual circuit (or connection)	Virtual circuit that is permanently established. PVCs save bandwidth and CPU usage associated with circuit establishment and tear down in situations where certain virtual circuits must exist all the time. In ATM terminology, called a permanent virtual connection.
redundancy		In internetworking, the duplication of devices, services, or connections so that, in the event of a failure, the redundant devices, services, or connections can perform the work of those that failed.

Acronym or Term	Expansion of Acronym	Definition of Acronym or Term
reliability		Performance within a design specification over time. Reliability is often measured by availability, mean time between failure (MTBF), and mean time to repair (MTTR).
RID	Router ID	Parameter used by routing protocol to identify a router. May be such things as an IP address, priority number, and so on. Varies per protocol.
RMON	Remote Monitoring	MIB agent specification, originally described in RFC 1271, that defines functions for the remote monitoring of networked devices. The RMON specification (IETF Standard 59) provides numerous monitoring, problem detection, and reporting capabilities. The RMON specification is defined in RFC 2819.
RTT	round-trip time	Time required for a network packet to travel from the source to the destination and back. RTT includes the time required for the destination to process the message from the source and generate a reply. The latency measurements taken by IPM and SAA are round-trip time latency measurements.
SMTP	Simple Mail Transfer Protocol	Internet protocol providing e-mail services. SMTP (IETF Standard 10) is defined in RFC 821.
SNMP	Simple Network Management Protocol	Network management protocol used almost exclusively in TCP/IP networks. SNMP provides a means to monitor and control network devices, and to manage configurations, statistics collection, performance, and security. SNMP (IETF Standard 62) is defined in RFC 3418.
spanning tree		Loop-free subset of a network topology that provides a path to every node.
STP	Spanning Tree Protocol	Bridge protocol that uses a spanning-tree algorithm, enabling a learning bridge to dynamically remove loops in a network topology by creating a spanning tree. Bridges exchange BPDU messages with other bridges to detect loops, and then remove the loops by shutting down selected bridge interfaces. Refers to both the IEEE 802.1 Spanning Tree Protocol standard and the earlier Digital Equipment Corporation Spanning Tree Protocol upon which it is based. The IEEE version supports bridge domains and allows the bridge to construct a loop-free topology across an extended LAN. The IEEE version generally is preferred over the Digital Equipment version.
TCP	Transmission Control Protocol	Connection-oriented transport layer protocol that provides reliable full-duplex data transmission. TCP (IETF Standard 7) is part of the TCP/IP protocol stack and is defined in RFC 793 and extended by other RFCs.
TDM	time-division multiplexing	Technique in which information from multiple channels allocates bandwidth on a single wire based on preassigned time slots. Bandwidth is allocated to each channel regardless of whether the station has data to transmit.

Acronym or Term	Expansion of Acronym	Definition of Acronym or Term
TFTP	Trivial File Transfer Protocol	Simplified version of FTP that allows files to be transferred from one computer to another over a network, usually without the use of client authentication (for example, username and password). TFTP (IETF Standard 33) is defined in RFC 1350 and has been updated by other RFCs.
throughput		Rate of information arriving at, and possibly passing through, a particular point in a network system.
topology		Physical or logical arrangement of network nodes and media within an enterprise networking structure.
transport layer		Layer 4 of the OSI reference model. This layer is responsible for reliable network communication between end nodes. The transport layer provides mechanisms for the establishment, maintenance, and termination of virtual circuits, transport fault detection and recovery, and information flow control. Corresponds to the transmission control layer of the SNA model.
UDP	User Datagram Protocol	Connectionless transport layer protocol in the TCP/IP protocol stack. UDP is a simple protocol that exchanges datagrams without acknowledgments or guaranteed delivery, requiring that error processing and retransmission be handled by other protocols. UDP (IETF Standard 6) is defined in RFC 768.

Troubleshooting Logs

Use this guide to complete the lab exercises for this course. The solutions information is found in the Lab Exercise Answer Key.

Troubleshooting Log—Trouble Ticket B

Problem	Solution

Core Router/Switch
a) Users cannot get to server or Internet.
	`interface Port-channel11`
	`no shut`
	`interface Port-channel12`
	`no shut`
	`!`

Distribution Router No issues.	`Nothing needed`

Access Router
Serial interfaces 0/0:1 and 0/0:0 are down.
	`controller T1 0/0`
	`linecode b8zs`
	`!`

Access Switch
Some PCs cannot connect to anything.
	`interface FastEthernet0/2`
	`switchport access vlan 2`
	`!`
	`interface FastEthernet0/4`
	`switchport access vlan 4`
	`!`

Troubleshooting Log—Trouble Ticket C

Problem	Solution

Core Router/Switch
a) Users cannot get to server or Internet.
b) No connectivity to dstr rtr
	`vlan 27`
	` name Core_27`
	`!`
	`vlan 28`
	` name Core_28`
	`!`
	`int fas 0/5`
	` duplex full`
	` speed 100`
	`!`
	`!`

Distribution Router
Serial interfaces 0/0:0 and 0/0:1 are down (wrong channel group configured on ser 0/0:0); fixing channel group deletes “no passive interface” in EIGRP.
	`!`
	`controller T1 0/0`
	` no channel-group 0 timeslots 1-2`
	` channel-group 0 timeslots 1-12`
	`!`
	`interface Serial0/0:0`
	` description Fast Link to Daytona`
	` ip address 172.21.176.2 255.255.255.128`
	` no shut`
	`!`
	`router eigrp 101`
	` no passive-interface Serial0/0:0`
	`!`

Access Router
a) Fa 0/0 is down because of speed mismatch; users cannot get to anywhere.
b) Serial interfaces 0/0:1 and 0/0:0 are down.
	`!`
	`a)`
	`interface FastEthernet0/0`
	` speed 100`
	`b)`
	`controller T1 0/0`
	`framing esf`
	`!`

Access Switch No issues.	`- -`

Troubleshooting Log—Trouble Ticket D

Problem	Solution

Core Router/Switch
a) Users cannot get to server (work group network not defined in RIP).
b) Users cannot get to the Internet (EIGRP not redistributing static route).
	a) router rip
	    network 172.21.0.0
	
	b) router eigrp 101
	    redistribute static

Distribution Router a) Does not form EIGRP adjacencies because of wrong AS number. b) No neighbor with Access rtr on Serial interface 0/0:0 (has IP address of ser 0/0:1).	a) **no router eigrp 11** **router eigrp 101** ! had wrong AS number passive-interface default no passive-interface Serial0/0:0 no passive-interface Serial0/0:1 no passive-interface Serial1/0.1 no passive-interface Serial1/1.1 no passive-interface FastEthernet0/0 network 172.21.176.0 0.0.0.127 network 172.21.176.128 0.0.0.127 network 172.21.177.0 0.0.0.127 network 172.21.177.128 0.0.0.127 network 172.21.178.0 0.0.0.127 network 172.21.178.128 0.0.0.127 auto-summary eigrp log-neighbor-changes ! b) interface Serial0/0:0 **ip address 172.2x.1x6.2 255.255.255.128**

Problem	Solution

Access Router
a) doesn't form EIGRP adjacencies (passive interfaces, wrong prefixes—even pods are /36, odd pods are /25).
	`router eigrp x0x`
	`no passive-interface Serial1/0.1`
	`no passive-interface Serial1/1.1`
	`passive-interface Serial1/0`
	`passive-interface Serial1/1`
	`!`
	`interface Serial1/0.1 point-to-point`
	`ip address 172.2x.1x7.1 255.255.255.[`**`128`**`|`**`192`**`]`
	`!`
	`interface Serial1/1.1 point-to-point`
	`ip address 172.2x.1x7.129 255.255.255.[`**`128`**`|`**`192`**`]`
	`!`

Access Switch
a) PCs cannot connect to anywhere.
b) PCs are getting network error messages when trying to ping.
	`a) interface FastEthernet0/1`
	`no shutdown`
	
	`b) pc's have static IP overlapping w/ DHCP server -` **`enable DHCP on PCs`**

Troubleshooting Log—Trouble Ticket E

Problem	Solution

Core Router/Switch
a) No one can connect to the Internet or CIT core (or Elmhurst or Lenexa—VLANs have swapped IP addresses).
b) Trunk is on wrong interface.
c) No BGP neighbors (wrong AS for core).
	`! a)`
	`interface Vlan27`
	`no ip address`
	`!`
	`interface Vlan28`
	`  ip address 172.28.128.1 255.255.255.240`
	
	`interface Vlan27`
	`  ip address 172.27.227.1 255.255.255.224`
	`!`
	`! b)`
	`interface FastEthernet0/15`
	`  no description Link to Orlando`
	`  no ip address 172.21.178.130 255.255.255.128`
	`  no speed 100`
	`  no duplex full`
	`  switch`
	`  shut`
	`!`
	`interface FastEthernet0/5`
	`  description Link to Orlando`
	`  no switchport`
	`  ip address 172.21.178.130 255.255.255.128`
	`  speed 100`
	`  duplex full`
	`  no shut`
	`!`
	`! c)`
	`router bgp 11`
	`  neighbor 172.27.227.7 remote-as 77`
	`  neighbor 172.28.128.8 remote-as 77`
	`  neighbor 172.27.227.7 distribute-list CIT in`
	`  neighbor 172.28.128.8 distribute-list CIT in`
	`!`
	`logging console`
	`!`

Problem	Solution

Distribution Router
a) Missing EIGRP routes (network statement issues).
b) Frame Relay links are not forming EIGRP neighbors (missing broadcasts, wrong DLCI).
	`! a)`
	`router eigrp 101`
	`  network 172.21.176.0 0.0.0.127`
	`  network 172.21.176.128 0.0.0.127`
	`  network 172.21.177.0 0.0.0.127`
	`  network 172.21.177.128 0.0.0.127`
	`  network 172.21.178.0 0.0.0.127`
	`  network 172.21.178.128 0.0.0.127`
	` no network 172.21.76.0 0.0.0.127`
	` no network 172.21.76.128 0.0.0.127`
	` no network 172.21.77.0 0.0.0.127`
	` no network 172.21.77.128 0.0.0.127`
	` no network 172.21.78.0 0.0.0.127`
	` no network 172.21.78.128 0.0.0.127`
	`! mistyped network statements`
	`!`
	`! b)`
	`interface Serial1/0.1`
	` frame-relay map ip 172.21.177.1 111 broadcast`
	`!`
	`interface Serial1/1.1`
	` frame-relay map ip 172.21.177.129 121 broadcast`
	`no frame-relay map ip 172.21.177.129 112`
	`!`

Access Router
a) No connectivity to access switch (IP address on wrong port).
b) No connectivity to distribution router (controller running loopback mode).
c) Traffic flows over wrong links (bandwidth mistyped).
	`! a)`
	`interface FastEthernet0/0`
	` no ip address`
	`!`
	`interface FastEthernet0/0.1`
	` ip address 172.21.171.1 255.255.255.128`
	`! b)`
	`controller t1 0/0`
	` no loopback local line`
	`! c)`
	`interface Serial1/0`
	` bandwidth 128`
	`!`
	`interface Serial1/1`
	` bandwidth 64`

Problem	Solution

Access Switch
Users cannot connect to anything (trunk on wrong port).
	`!`
	`interface FastEthernet0/1`
	` switchport trunk native vlan 901`
	` switchport mode trunk`
	` duplex full`
	` speed 100`
	` no shutdown`
	`!`
	`interface FastEthernet0/10`
	` no switchport mode trunk`
	` switchport trunk native vlan 901`
	` no ip address`
	` shut`
	`!`

Troubleshooting Log—Trouble Ticket F

Problem	Solution

Core Router/Switch
a) EtherChannels are down because of trunk encapsulation mismatch.
b) VTP mode is server; VLANs are getting overwritten. (Instructor can do this a few times so that all pods have the issue at least once.)
c) Duplicate OSPF RID with core (even pods with Elmhurst, odd pods with Lenexa).
	`! a) examples shown for pod 4`
	`!`
	`interface range FastEthernet0/1 - 2`
	` switchport trunk encapsulation isl`
	`!`
	`interface range FastEthernet0/3 - 4`
	` switchport trunk encapsulation dot`
	` shutdown`
	` no shutdown`
	`!`
	`! b)`
	`vtp mode transparent`
	`no vlan 10-18`
	`vlan 27`
	`vlan 28`
	`!`
	`! c)`
	`router ospf 404`
	` router-id 172.27.227.4`
	`!`
	`do clear ip ospf process`
	`y`

Distribution Router
a) Area 4 is missing NSSA statement.
b) OSPF routes are not redistributed because of wrong AS number.
c) No EIGRP neighbors because frame subinterfaces are passive for EIGRP.
	`! a) examples shown for pod 4`
	`router ospf 404`
	` area 4 nssa`
	`!`
	`! b)`
	`router eigrp 404`
	` redistribute ospf 404 metric 10000 100 255 1 1500`
	` no redistribute ospf 44 metric 10000 100 255 1 1500`
	`!`
	`! c)`
	`router eigrp 404`
	` no passive-interface Serial1/0.1`
	` no passive-interface Serial1/1.1`
	` passive-interface Serial1/0`
	` passive-interface Serial1/1`
	`!`

Problem	Solution

Access Router
a) Missing routes for two end user VLANs.
b) Frame links are down; no keepalives.
c) IP addresses on frame links are swapped.
	`! a)`
	`router eigrp 404`
	` network 172.24.141.0 0.0.0.63`
	` network 172.24.144.0 0.0.0.63`
	`! b)`
	`interface Serial1/0`
	` keepalive`
	`!`
	`interface Serial1/1`
	` keepalive`
	`!`
	`! c)`
	`interface Serial1/0.1`
	` no ip add`
	
	`interface Serial1/1.1`
	` ip address 172.24.147.129 255.255.255.192`
	
	`interface Serial1/0.1`
	` ip address 172.24.147.1 255.255.255.192`
	`!`

Access Switch No issues here.	`! no issues`

Troubleshooting Log—Trouble Ticket G

Problem	Solution
Core Router/Switch a) Wrong area is running authentication. b) Bogus access list CIT. c) Mistyped access list in distribute list (CIT for CIT).	! a) **example shown for POD2** ! router ospf 202 area 0 authentication message-digest no area 2 authentication message-digest ! ! b) **example shown for POD2** no ip access-list extended CIT ip access-list standard CIT remark Include the other pods as /16 networks permit 172.21.0.0 0.0.255.255 permit 172.23.0.0 0.0.255.255 permit 172.24.0.0 0.0.255.255 permit 172.25.0.0 0.0.255.255 permit 172.26.0.0 0.0.255.255 ! ! c) ! router bgp 65021 neighbor 10.177.177.7 distribute-list CIT in neighbor 10.177.178.8 distribute-list CIT in
Distribution Router a) Cannot connect to console (no EXEC). b) Missing ICMP; Telnet goes slow path. c) Use of physical interface on route map.	! a) line con 0 EXEC ! ! b) route-map USE_FAST permit 20 set ip next-hop 172.22.127.129 no set interface Serial1/1 ! !c) no ip access-list extended END_USERS ip access-list extended END_USERS remark Allow PC End Users permit ip any 172.22.124.0 0.0.0.255 permit ip any 172.22.122.0 0.0.1.255 !

Problem	Solution
Access Router a) Cannot connect to console (line speed). b) Missing www statement; ICMP denies end users. c) DHCP does not provide addresses.	! a) line con 0 speed 9600 ! need to connect via Telnet to fix ! b) no ip access-list extended Traffic ip access-list extended Traffic remark Allow ICMP, TCP outbound, FTP & WWW permit icmp 172.22.0.0 0.0.255.255 any permit tcp 172.22.0.0 0.0.255.255 any eq telnet permit tcp 172.22.0.0 0.0.255.255 any eq ftp-data permit tcp 172.22.0.0 0.0.255.255 any eq ftp **permit tcp 172.22.0.0 0.0.255.255 any eq www** permit udp 172.22.0.0 0.0.255.255 any eq tftp ! c) ip dhcp excluded-address 172.22.122.1 ip dhcp excluded-address 172.22.123.1 ip dhcp excluded-address 172.22.124.1 no ip dhcp excluded-address 172.22.122.2 no ip dhcp excluded-address 172.22.123.2 no ip dhcp excluded-address 172.22.124.2 !
Access Switch No issues.	! no issues

Troubleshooting Log—Ticket H

Problem	Solution

Core Router/Switch
a) Wrong banner/host name; missing service prompt.
b) No console messages.
c) Reload in xxx.
d) Cannot reach BGP neighbors.
e) MD5 keys are messed up (extra space, wrong places).
	`! a)`
	`no banner motd`
	`hostname Tampa`
	`service prompt config`
	`! b)`
	`logging console`
	`! c)`
	` reload cancel`
	`! d)`
	`router bgp 65011`
	` neighbor 10.177.177.7 update-source Loopback0`
	` neighbor 10.177.178.8 update-source Loopback0`
	`vlan 27`
	` no shut`
	`vlan 28`
	` no shut`
	`!`
	`! e)`
	` interface Vlan27`
	` no ip ospf message-digest-key 27 md5 acme`
	` ip ospf message-digest-key 27 md5 acme`
	`!`
	`interface Vlan28`
	` no ip ospf message-digest-key 27 md5 acme`
	` ip ospf message-digest-key 28 md5 ACME`
	`!`

Problem	Solution

Distribution Router
a) Wrong banner and host name.
b) Wrong prompt.
c) No need for EIGRP stub.
d) distribute list in OSPF is going wrong way.
e) Small MTU breaks serial links for EIGRP.
	`! a)`
	`no banner motd`
	`hostname Orlando`
	`!`
	`! b)`
	`no prompt %%%sInvalid%sinput%sdetected%s`
	`!`
	`! c)`
	`router eigrp 101`
	` no eigrp stub`
	`!`
	`! d)`
	`router ospf 101`
	` no distribute-list Access_Routes in`
	` distribute-list Access_Routes out`
	`!`
	`! e)`
	`interface serial 1/0`
	` no mtu 64`
	`!`
	`interface serial 1/1`
	` no mtu 64`
	`!`

Problem	Solution
Access Router a) Wrong banner and host name. b) route map permit / deny swapped, sends ARP from 0.0.0.0 out ser 1/1.1 c) Wrong ANSI type on Frame Relay. d) Access group applied wrong way on serial links.	! a) hostname Daytona ! b) no route-map USE_FAST ! route-map USE_FAST permit 10 match ip address Admin set interface Serial1/1.1 ! route-map USE_FAST deny 20 match ip address End_Users ! ! c) interface serial 1/0 no frame-relay lmi-type ansi ! interface serial 1/1 no frame-relay lmi-type ansi ! ! d) interface serial 1/1.1 ip access-group Traffic out no ip access-group Traffic in ! interface serial 1/0.1 ip access-group Traffic out no ip access-group Traffic in !
Access Switch a) SVI shutdown. b) No trunk on VLAN1.	! a) interface Vlan901 no shut ! ! b) interface FastEthernet0/1 no switchport access vlan 2 switchport trunk native vlan 901 switchport mode trunk !

Lab Guide

Overview

Use this guide to complete the lab exercises for this course. The solutions information is found in the Lab Exercise Answer Key.

Outline

This Lab Guide includes these exercises:

- Lab Exercise 1-1: Network Baseline Discovery
- Lab Exercise 1-2: Creating End-System Baseline Discovery
- Lab Exercise 2-1: Applying a Layered Model to a Network
- Case Study (Trouble Ticket A) 2-1: Gathering Symptoms
- Case Study (Trouble Ticket B) 3-1: Isolating Physical and Data Link Layer Problems
- Lab Exercise (Trouble Ticket B) 3-1: Correcting Problems at the Physical and Data Link Layers
- Lab Exercise (Trouble Ticket C) 3-2: Troubleshooting Problems at the Physical and Data Link Layers
- Case Study (Trouble Ticket D) 4-1: Isolating Network Layer Problems
- Lab Exercise (Trouble Ticket D) 4-1: Correcting Problems at the Network Layer
- Lab Exercise (Trouble Ticket E) 4-2: Troubleshooting Problems at the Physical, Data Link, and Network Layers
- Lab Exercise (Trouble Ticket F) 4-3: Troubleshooting Problems at the Physical, Data Link, and Network Layers
- Case Study (Trouble Ticket G) 5-1: Isolating Problems at the Transport and Application Layers
- Lab Exercise (Trouble Ticket G) 5-1: Correcting Problems at the Transport and Application Layers
- Lab Exercise (Trouble Ticket H) 5-2: Troubleshooting Problems at All Logical Layers

Lab Exercise 1-1: Network Baseline Discovery

Complete this lab exercise to practice what you learned in the related lesson.

Exercise Objective

In this exercise, you will establish the baseline for the configuration and operation of the CIT (Cisco Internetwork Troubleshooting) network. You will complete the following tasks:

- Determine network topology and device configurations
- Complete network configuration tables
- Update the base network diagram for your workgroup to include data link layer switch features and network layer addressing

After completing this exercise, you will be able to meet these objectives:

- Document the topology of a network
- Identify data link layer addresses and implemented features in a network
- Identify network layer addresses and implemented features, including routing protocols used in a network

Required Resources

These are the resources and equipment required to complete this exercise:

- Access to the workgroup PCs and Cisco devices in the lab network
- Familiarity with Cisco router and switch commands covered in the Cisco *Building Scalable Cisco Internetworks* (BSCI), *Building Cisco Multilayer Switched Networks* (BCMSN), and *Building Cisco Remote Access Networks* (BCRAN) courses

Command List

The commands used in this exercise are described in the table here.

Helpful Network Discovery Commands

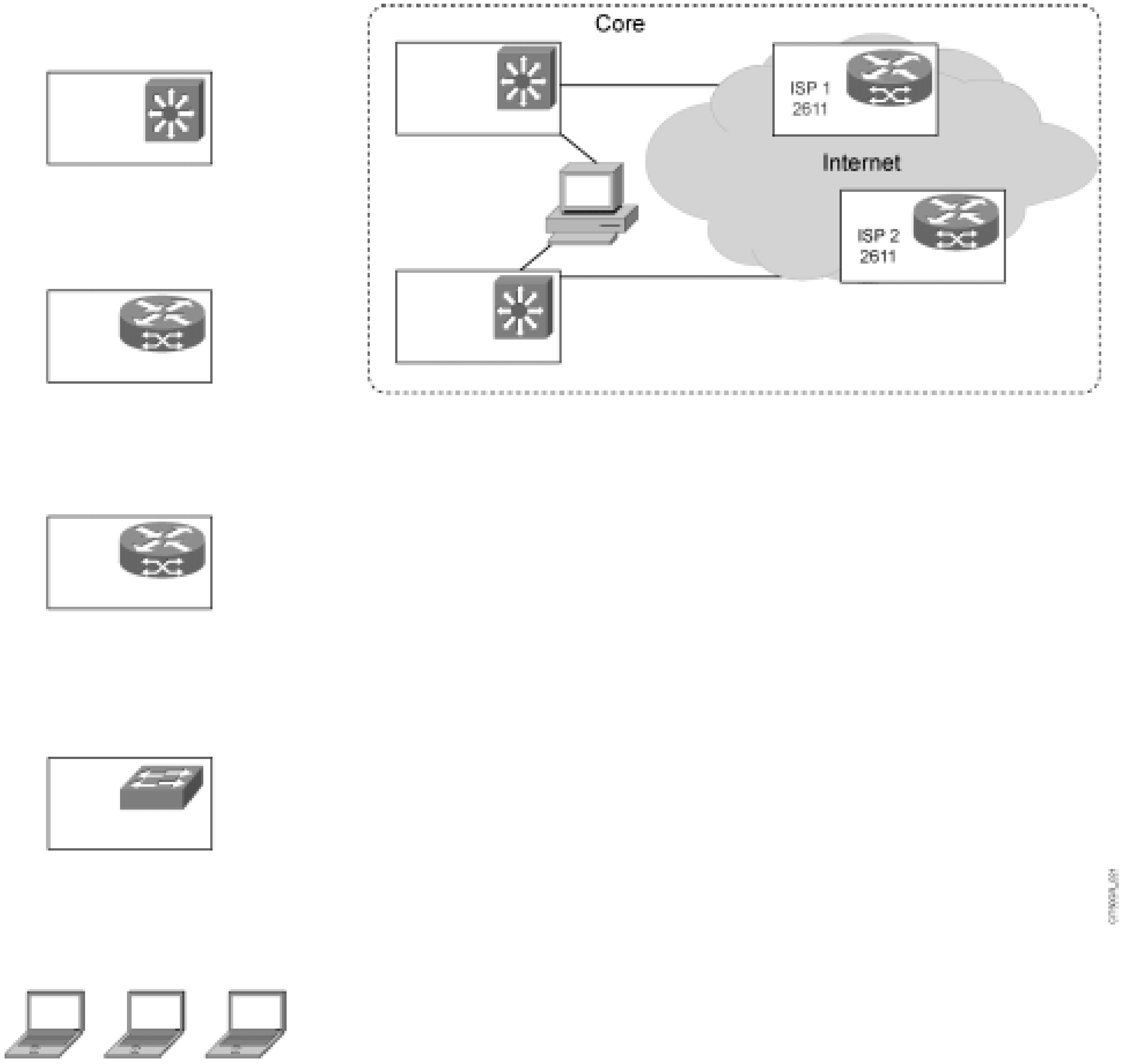
Command	Description
show access-lists	Shows configured access lists.
show cdp neighbors [detail]	Displays Cisco Discovery Protocol (CDP) neighbor information.
show controllers <type number>	Displays controller information and status.
show etherchannel summary	Displays EtherChannel port-channel summary status, including data link and network layer port and interface information.
show frame-relay map	Displays Frame Relay mapping status.
show frame-relay pvc	Displays Frame Relay permanent virtual circuit (PVC) information and status.
show interfaces status	Displays a tabular status report of the ports on a switch.
show interfaces trunk	Shows trunking interfaces.
show ip bgp summary	Shows summary Border Gateway Protocol (BGP) status.
show ip protocols	Displays routing protocol status.
show ip <protocol> interface	Displays interface information for a protocol.
show ip <protocol> neighbor	Displays information about neighbors for a specific routing protocol.
show ip route	Displays IP routing table information.
show protocols	Displays network layer addresses and interface status.
show running-config	Displays device configuration information.
show spanning-tree	Displays Spanning Tree Protocol (STP) information, including port status.
show tdm clock	Shows time-division multiplexing (TDM)-related information.
show version	Displays general hardware and software information.
show vlan	Displays VLAN information.
show vtp status	Displays VLAN Trunking Protocol (VTP) status, including domain name and revision number.
telnet {*ip-address*}	Uses Telnet to connect to an IP address.
traceroute {*ip-address*}	Runs traceroute to an IP address.

Job Aids

These job aids are available to help you complete the lab exercise:

- A base network diagram
- Blank network configuration tables

Baseline Network Diagram



Network Configuration Table (Access Router)

Device Name, Model	Interface	MAC Address	IP Address/ Subnet Mask	IP Routing Protocol(s)	Notes/Comments

Network Configuration Table (Access Router)

Notes:

Network Configuration Table (Distribution Router)

Device Name, Model	Interface	MAC Address	IP Address/ Subnet Mask	IP Routing Protocol(s)	Notes/Comments

Network Configuration Table (Distribution Router)

Notes:

Network Configuration Table (Access Switch)

Catalyst Name, Model. Management IP Address	Port	Speed	Duplex	STP State Fwd/Block	PortFast/ Trunk	Ether Channel (L2 or L3)	VLAN	IP Address

Network Configuration Table (Access Switch)

Notes:

Network Configuration Table (Core Router/Switch)

Catalyst Name, Model. Management IP Address	Port	Speed	Duplex	STP State Fwd/Block	PortFast/ Trunk	Ether Channel (L2 or L3)	VLAN	IP Address

Network Configuration Table (Core Router/Switch)

Notes:

Task 1: Create a Network Configuration Table and Network Topology Diagram

Coordinate with others in your workgroup to gather detailed information about all the devices within your workgroup. Complete the network configuration tables and transfer details to your topology diagram.

Exercise Procedure

Complete these steps:

Step 1 Connect to the console port of one device. Note that the console password and vty password for all devices is “cisco”. No privileged passwords are configured on the work group devices. The privileged password for the corporate core devices is intentionally not provided.

Step 2 Enter the router and switch commands as needed to determine baseline information.

Step 3 Document only the active interfaces of the device in the network configuration tables, sharing the information with your workgroup.

Step 4 Connect to additional devices as needed.

Step 5 Add details to your network diagram documenting the physical connections, device names, and network layer addressing of your workgroup.

Step 6 Verify connectivity across the workgroup network to the core devices.

Step 7 Ask the instructor to verify that your documentation is complete and accurate.

Exercise Verification

You have completed this exercise when you attain these results:

- You have completed the baseline network configuration tables for your workgroup.
- You have created a detailed network topology diagram for your workgroup.
- Each PC in the workgroup has used Telnet to open a session on the CIT_Server at 172.27.227.9.

Lab Exercise 1-2: Creating End-System Baseline Discovery

Complete this lab exercise to practice what you learned in the related lesson.

Exercise Objective

In this exercise, you will establish the baseline for the configuration and operation of the end systems in the CIT network. You will complete the following tasks:

- Determine end-system network configuration
- Determine end-system connectivity
- Complete end-system network configuration tables

After completing this exercise, you will be able to meet these objectives:

- Identify network layer addresses on PC end systems
- Demonstrate connectivity between end systems and network devices

Required Resources

These are the resources and equipment required to complete this exercise:

- Access to the workgroup PCs and Cisco devices in the lab network
- Familiarity with PC networking commands
- Your previously completed network topology diagram

Command List

The commands used in this exercise are described in the table here.

Helpful PC Discovery Commands

Command	Description
arp -a	Displays Address Resolution Protocol (ARP) information.
ipconfig /all	Displays IP information.
ping <ip-address>	Pings an IP address.
route print	Displays active routes.
telnet <ip-address>	Uses Telnet to connect to an IP address.
tracert -d <ip-address>	Runs tracert to an IP address.
CIT_server	Connect via HTTP to a web host.

Job Aids

These job aids are available to help you complete the lab exercise:

- A blank end-system network configuration table

End-System Network Configuration Table

Device Name, Operating System	Interface	IP Address/ Subnet Mask	Static or DHCP (with lease time)	Default Gateway	DNS Server

End-System Network Configuration Table

Notes:

Task 1: Create an End-System Network Configuration Table

Gather detailed information about each PC within your workgroup (coordinate with others in your workgroup) and complete the end-system network configuration table.

Exercise Procedure

Complete these steps:

Step 1 Enter PC commands as needed to determine baseline information about a single device.

Step 2 Document the device on the end-system network configuration table, sharing the information with your workgroup.

Step 3 Connect to additional PCs as needed.

Step 4 Add details to your workgroup network topology diagram documenting the physical connections, device names, and network layer addressing of the PCs in your workgroup.

Step 5 Verify connectivity across the workgroup network to the core devices.

Step 6 Ask your instructor to verify that your documentation is complete and accurate.

Exercise Verification

You have completed this exercise when you attain these results:

- You have completed the baseline end-system network configuration table for the PCs in your workgroup.
- You have updated the base topology diagram to include information about the end systems in your workgroup.
- Each PC in the workgroup has used Telnet to open a session on the CIT_Server at 172.28.128.9 (the server has network interface cards).
- Each PC in the workgroup has used HTTP to open a session on the CIT_Server at 172.27.227.9.

Lab Exercise 2-1: Applying a Layered Model to a Network

Complete this lab exercise to practice what you learned in the related lesson.

Exercise Objective

In this exercise, you will use various Cisco IOS commands and a protocol analyzer to map the layers in the Open Systems Interconnection (OSI) model to the encapsulated data flow in the classroom network. You will complete the following tasks:

- Develop a logical diagram for data link layer and network layer functionality in the core
- Map traffic flows for ping, Telnet, and HTTP traffic from the workgroup PCs
- Capture and analyze background traffic

After completing this exercise, you will be able to meet these objectives:

- Understand the data flow in the classroom network based on the logical network model
- Use a protocol analyzer to review background traffic
- Use Cisco IOS commands to analyze traffic flows in the network and correlate debug messages

Required Resources

These are the resources and equipment required to complete this exercise:

- Access to the workgroup PCs and Cisco devices in the lab network
- Familiarity with Cisco router and switch commands covered in the Cisco *Building Scalable Cisco Internetworks* (BSCI), *Building Cisco Multilayer Switched Networks* (BCMSN), and *Building Cisco Remote Access Networks* (BCRAN) courses
- Access to a protocol analyzer (either software or hardware)
- The network diagram from a previous exercise

Command List

The commands used in this exercise are described in the table here.

Helpful Commands

Command	Description
debug ip eigrp	Captures Enhanced Interior Gateway Routing Protocol (EIGRP) event information.
debug ip policy	Captures IP policy information.
debug ip routing	Displays information on routing table updates and route-cache updates.
debug serial interface	Captures serial interface information.
ping {*host* | *ip-address*}	Sends an echo request packet to an address, then waits for a reply. The *host* | *ip-address* variable is the IP alias or IP address of the target system.
show access-lists	Displays the contents of all access lists.
show clock	Displays current date and time information for the device.
show etherchannel summary	Displays EtherChannel port-channel summary status, including data link and network layer port and interface information.
show interface status	Displays a tabular status report of the ports on a switch.
show interfaces trunk	Shows information about trunking interfaces.
show ntp associations	Displays Network Time Protocol (NTP) associations.
show ntp status	Displays NTP status.
show route-map	Displays information about all configured route maps.
show spanning-tree vlan *vlan-id*	Displays STP information, including port status for a specific VLAN.
show vlan	Displays default and defined VLAN information.
telnet {*host* | *ip-address*}	Connects to an IP address using the Telnet application.
terminal monitor	Displays debug command output and system error messages for the current terminal and session.
traceroute [*destination*]	Identifies the path that a packet takes through the network. The *destination* variable is the host name or IP address of the target system.

Job Aids

These job aids are available to help you complete the lab exercises:

- VLAN port status chart

VLAN Port Status Chart

Device	Port	VLAN ____ Status (Forwarding or Blocked)	VLAN _____ Status (Forwarding or Blocked)	VLAN _____ Status (Forwarding or Blocked)

Task 1: Develop a Logical Diagram for Data Link and Network Layer Functionality in the Core

The Cisco Catalyst 3550 switches in the lab support both data link and network layer functionality. For this task, gather information about the VLANs and subnets in the core. Complete the VLAN port status chart.

Exercise Procedure

Complete these steps:

Step 1 Connect to the workgroup 3550. (host name _______________________________)

Step 2 Use the **show vlan** and **show spanning-tree vlan vlan-id** commands to determine which VLANs are active on the workgroup 3550. Use the **show spanning-tree vlan vlan-id** command to determine the VLAN port status (forwarding or blocked) for all switched ports. Document these results on the VLAN port status chart.

Step 3 Connect to core switches (Lenexa and Elmhurst).

Step 4 Document VLAN port status for all interfaces on the core switches.

Step 5 Sketch out the VLAN status, or add details to your network diagram documenting the logical preference for the VLANs for your workgroup.

Exercise Verification

You have completed this exercise when you attain these results:

- You have documented the VLAN status for all ports on your workgroup 3550.

Task 2: Capturing and Analyzing Background LAN Traffic

Use a protocol analyzer to capture and review background LAN traffic.

Exercise Procedure

Complete these steps:

Step 1 Start the protocol analyzer software on your PC. (This example will describe using Ethereal. If applicable, follow the directions from your instructor for a hardware protocol analyzer.)

Step 2 From the command row, choose **Display>Options**.

Step 3 Under Display Options, click **Time Of Day**. The button will appear pushed-in when it is enabled.

Step 4 From the command row, choose **Capture>Start**.

Step 5 Under Display Options, click **Update List Of Packets In Real Time**. The button will appear pushed-in when it is enabled.

Step 6 Capture a few minutes of background traffic without running any additional applications.

What kinds of traffic do you see?

____

____

____

____

____

____

Step 7 At the command prompt for the PC, enter **arp –a** to look for current ARP mappings.

What do you see? ____

____

Step 8 Enter **show arp** to look at the ARP table on the access router and the access switch. Enter **show mac-address-table** to look at the MAC addresses and VLANs on the access switch. Enable the **debug ip icmp** and **debug arp** commands on the access router and the access switch.

Step 9 Coordinate with your workgroup and ping the other PCs in the workgroup. Look for ARPs in the protocol analysis stream. Again check for ARP mappings on your PC.

What do you see? ____

____

Is this what you expected? ____

Does the access switch generate any debug messages? If so, why? ______________

____

Does the access router generate any debug messages? If so, why? ______________

____

Step 10 At the command prompt for the PC, ping your default gateway. Look for ARPs in the protocol analysis stream. Check your current ARP mappings.

What do you see? ____

____

Step 11 Using Telnet, generate some additional traffic by connecting to a workgroup device.

What do you see in terms of data flow? ______________________________

____

Is this what you expected? ____

Close this Telnet session.

Step 12 Open a browser window and connect to 172.28.128.9.

What do you see? ____

____

Is this what you expected? ____

Step 13 Exit the browser session.

Step 14 Have the learner with the console session to the 2950 switch adjust the global spanning-tree properties by entering the **no spanning-tree portfast bpdufilter default** global configuration command. Look for differences in the background traffic.

What do you see? ____

Step 15 Restore the **spanning tree** command.

Step 16 Have the learner with the console session on the access router remove the passive interfaces under EIGRP. Look for differences in the background traffic.

What do you see? ____

Step 17 Restore the EIGRP passive interfaces removed in the Step 16.

Step 18 In the second Ethereal window, click **Stop** to halt the Ethereal application.

Step 19 As needed, continue your review of the captured traffic by scrolling through the list. Choose **File>Save As** to save the capture file for future reference. Save the file as a baseline to the default location within the Ethereal directory. Be sure to select the Ethereal file extension.

Step 20 List all data flows you saw. ____

____

____

____

____

Step 21 Exit the Ethereal protocol analyzer software.

Exercise Verification

You have completed this exercise when you attain these results:

- You have used a protocol analyzer to review background traffic in the workgroup.
- You have saved a baseline traffic file.

Task 3: Analyzing Background WAN Traffic

Use Cisco IOS commands to review background WAN traffic.

Exercise Procedure

Complete these steps:

Step 1 Return to the console sessions on the workgroup routers.

Step 2 Enable the **debug ip eigrp** command on both routers and the core switch. Wait for a minute or so.

Do you see any debug messages? ____

____

Why or why not? ____

Step 3 Leave the **debug ip eigrp** event process running.

Step 4 If you are not connected to a router with active WAN interfaces, connect to the distribution router via Telnet. Configure your session so that you can also see the debug messages from the distribution router. (Coordinate entering the commands in this task with the other learners in your workgroup.)

Step 5 Enable the **debug serial interface** command on the distribution and access routers.

Examine the output for a minute or so.

What do you see? ____

____

Compare these messages on the distribution and access routers. Do they have matching time stamps? ____

Could NTP be useful in debugging? ______________________________________

Step 6 Shut down the S1/0 interface on the access router.

What and when did the access router notice?

____

____

What and when did the distribution router notice?

____

____

Step 7 Activate the S1/0 interface. To halt EIGRP event debugging, enter the **no debug ip eigrp** command**.** To activate IP routing debugging, enter the **debug ip routing** command**.**

Step 8 On the distribution router, enter the **no keepalive** interface command on S1/1.

What and when does the distribution router see?

____

____

What and when does the access router see?

____

____

Step 9 Wait at least a minute and then restore the default keepalive with the **keepalive** interface command on S1/1.

Step 10 On the distribution router, enter the **keepalive 30** interface command on the S1/1 interface.

What does the distribution router see?

____

____

What does the access router see?

____

____

Step 11 Restore the default keepalive with the **keepalive** interface command on S1/1. Halt the IP routing debug with the **no debug ip routing** command.

Step 12 On the distribution router, enter the **no keepalive** interface command on S0/0:0 on the T1.

What does the distribution router see?

____

____

What does the access router see?

____

____

Step 13 Apply the default keepalive with the **keepalive** interface command on the S0/0:0 interface.

Step 14 On the access router, enter the **linecode ami** controller command on the T1 0 controller.

What does the distribution router see?

____

____

What does the access router see?

____

____

Step 15 Restore the previous line coding with the **linecode b8zs** controller command.

Step 16 On the distribution router, enter the **framing sf** controller command on the T1 0 controller.

What does the distribution router see?

____

____

What does the access router see?

____

____

Step 17 Restore the previous framing with the **framing esf** controller command.

Step 18 On all routers and the core switch, halt all the debugging processes with the **undebug all** command.

Step 19 List all data flows that you saw. ____

____

____

____

____

Exercise Verification

You have completed this exercise when you attain these results:

- You have used Cisco IOS commands to review background WAN traffic.
- You can state what will happen if you change or remove keepalives on a serial interface.
- You can state what will happen if you change framing or line codes on a T1 controller.

Task 4: Mapping Traffic Flows

Use Cisco commands to map traffic flows in the network.

Exercise Procedure

Complete these steps:

Step 1 Enable the **debug ip icmp command** on all workgroup routers and switches.

Step 2 A learner in each workgroup should connect to the console session on the access router while the other learners in each workgroup observe. (Coordinate entering the commands in this task with the other learners in your workgroup.)

Step 3 Use the **ping** command from the access router to verify connectivity to the CIT_Server at 172.27.227.9.

Step 4 Use an extended **ping** command to verify connectivity from the Fast Ethernet 0/1.2 subinterface to the CIT_Server at 172.27.227.9.

Do you notice any differences? ____

____

Step 5 Use the **traceroute** command to verify connectivity to the core 3550 from the access router.

Step 6 Use an extended **traceroute** command to verify connectivity from the Fast Ethernet 0/1.2 subinterface to the core 3550.

Do you notice any differences? ____

____

Step 7 Use the **show ip route** command to review the routes to the core 3550.

Step 8 Use the **show ip policy**, **show route-map**, and **show access-list** commands to review policy routing on the access router.

What do you notice? ____

____

Step 9 Enable the **debug ip policy** command on the access router.

Step 10 At a PC command line, ping an address on the core 3550. Review the policy routing debug output.

What do you notice? ____

____

Step 11 From the access router, ping an address on the core 3550. Review the policy routing debug output.

What do you notice? ____

____

Step 12 On all routers and switches, halt all the debugging processes with the **undebug all** command.

Step 13 List all data flows that you saw. ____

____

____

Exercise Verification

You have completed this exercise when you attain these results:

- You have used Cisco IOS commands to map traffic flows in the network.
- You can state how policy routing on the access router will affect the traffic flows in the physical and data link layers.

Case Study (Trouble Ticket A) 2-1: Gathering Symptoms

Complete this case study to practice what you learned in the related lesson. You will be given a simple problem situation reported by the user. You must decide which questions to ask the user and which tools to use to completely document the symptoms of the problem.

Exercise Objective

In this exercise, you will use the troubleshooting checklist and Cisco IOS commands to work through a troubleshooting case study. You will complete the following step:

- Define the problem by questioning users and using Cisco IOS tools

After completing this exercise, you will be able to meet this objective:

- Decide which questions to ask and which troubleshooting tools to use to completely document the symptoms of a network problem

Required Resources

These are the resources and equipment required to complete this exercise:

- Access to the workgroup PCs and Cisco devices in the lab network
- Familiarity with Cisco router and switch commands covered in the Cisco *Building Scalable Cisco Internetworks* (BSCI), *Building Cisco Multilayer Switched Networks* (BCMSN), and *Building Cisco Remote Access Networks* (BCRAN) courses
- The network diagram from the previous exercises

Command List

The commands used in this exercise are described in the table here.

Helpful Commands

Command	Description
ping {**host** | **ip-address**}	Sends an echo request packet to an address, then waits for a reply. The *host* | *ip-address* variable is the IP alias or IP address of the target system.
show interface status	
show ip interface brief	Displays a summary of the status of all interfaces on a device.
show ip route	Displays the current state of the IP routing table.
show running-config interface	Displays the contents of the currently running configuration file.
telnet {**host** | **ip-address**}	Connects to an IP address or host name using the Telnet application.
traceroute [**destination**]	Identifies the path that a packet takes through the network. The *destination* variable is the host name or IP address of the target system..

Exercise Setup

Complete these steps, coordinating with the other learners in your workgroup:

Step 1 Connect to workgroup access router.
(host name ______________________________)

Step 2 Shut down the link to the access switch with the **shutdown** interface configuration command.

Job Aids

This job aid is available to help you complete the lab exercises:

- Information on Trouble Ticket A

Trouble Ticket A

The end users report that they can no longer reach any devices in the network. All the end users say that this issue came up suddenly, in the last five minutes or so. According to them, the network was working fine previously.

Exercise Procedure

Complete these steps, coordinating with the other learners in your workgroup.

Step 1 What additional questions would you ask the users?

____

____

____

Step 2 What commands should the users try from their PCs?

____

What information do the users discover?

____

____

____

Step 3 Where should you look first to isolate the problem?

____

What commands might you use to look for issues?

____

Try the commands. What information do you discover?

____

____

____

Step 4 Where should you look next to isolate the problem?

____

What commands might you use to look for issues?

____

Try the commands. What information do you discover?

____

____

____

Step 5 Repeat Step 4 as needed to isolate the problem.

Exercise Verification

You have completed this exercise when you attain this result:

- You have documented the symptoms of the network problem completely by questioning the user and using troubleshooting tools.

Exercise Wrap-Up

Activate the link to the access switch with the **no shutdown** interface configuration command on the access router.

Case Study (Trouble Ticket B) 3-1: Isolating Physical and Data Link Layer Problems

Complete this case study to practice what you learned in the related lesson. You will be given a problem situation escalated to Level 2 Support. You will analyze user feedback and end-system data, and use Cisco commands and applications to isolate the specific cause of any problems.

Exercise Objective

In this exercise, you will use a troubleshooting methodology and Cisco commands to isolate the specific causes of any network problems.

After completing this exercise, you will be able to meet these objectives:

- Analyze user feedback and end-system data to decide at which OSI layer to begin isolating problems
- Select the troubleshooting tools to use to isolate the specific causes of any network problems
- Develop a troubleshooting implementation plan for resolving any identified problems

Required Resources

These are the resources and equipment required to complete this exercise:

- Access to the workgroup PCs and Cisco devices in the lab network
- Familiarity with Cisco router and switch commands covered in the Cisco *Building Scalable Cisco Internetworks* (BSCI), *Building Cisco Multilayer Switched Networks* (BCMSN), and *Building Cisco Remote Access Networks* (BCRAN) courses
- A completed baseline topology diagram documenting the lab installation
- Network documentation recording the configuration of the lab installation

Command List

As you work through the case study, you may find the following list of commands helpful. The list includes router, switch, and PC commands. The commands used in this exercise should be familiar to you from previous experience or from the Cisco BSCI, BCMSN, and BCRAN courses.

Helpful Commands

Command	Description
ping *{host | ip-address}*	(User or Extended) Sends an echo request packet to an address, then waits for a reply. The *host|ip-address* variable is the IP alias or IP address of the target system.
show cdp neighbors [detail]	Displays the device type, IP address, and Cisco IOS version of neighboring devices.
show controllers *{type number}*	Displays current internal status information for the interface controller cards.
show etherchannel summary	Displays EtherChannel port-channel summary status, including data link (Layer 2) or network (Layer 3) layer port and interface information.
show frame-relay map	Displays Frame Relay mapping status.
show frame-relay pvc	Displays Frame Relay PVC information and status.
show interfaces port-channel *{interface-number}*	Displays port-channel status, including Layer 2 or Layer 3 port and interface information.
show interface status	Displays a tabular status report of the ports on a switch.
show interfaces trunk	Shows trunking interfaces.
show ip interface brief	Displays a summary of the status of all interfaces on a device.
show ip route	Displays IP routing table information.
show protocols	Displays network layer addresses and interface status.
show running-config	Displays device configuration information.
show running-config interface *{type number}*	Displays configuration information for one interface.
show spanning-tree	Displays STP information, including port status.
show tdm clock	Shows TDM-related information.
show version	Displays the Cisco IOS software version and all installed hardware configurations.
show vlan	Displays VLAN configurations on a device.
show vtp status	Displays VTP status, including domain name and revision number.
telnet *{host | ip-address}*	Uses Telnet to connect to an IP address.
trace *[destination]*	(User or Privileged) Identifies the path that a packet takes through the network. The *destination* variable is the IP alias or IP address of the target system.

Job Aids

These job aids are available to help you complete the lab exercises:

- Information on Trouble Ticket B
- Troubleshooting Log

Trouble Ticket B

You recently joined the second-level network support team for Acme. This evening you are on call for network outages. You read this report during your review of the activity log.

Network Support Activity Log

Time	Log Entry
5:30 p.m.	One Acme user reported that access to the server seemed to be slower than usual. – Help Desk – [Assigned to Network Operations]
6:01 p.m.	We checked and could ping the server. We scanned the configs on all the network devices. They look fine. – 2nd shift ops –
6:15 p.m.	Multiple users started reporting that they can no longer reach anything. – Help Desk –
6:37 p.m.	We can ping the core devices, but also noticed some network latency from the access router. Escalated to Level 1 Network Support. – 2nd shift ops – [Assigned to Mike]
6:52 p.m.	I asked the network operations team if anyone changed anything. They do not think that anyone changed anything important. Not sure what they changed. – Mike –
7:23 p.m.	I tried to fix up the configs to resolve the user access and resolve the network latency issues. I am not sure what to back out, but the issues are worse. The serial link on distribution router is flapping. I can no longer reach the CIT_Server from anywhere. – Mike –
7:33 p.m.	Escalated to Level 2 Network Support.

Troubleshooting Log: Isolating Physical and Data Link Layer Problems

Problem	Solution
Core Router/Switch	
Distribution Router	
Access Router	
Access Switch	

Exercise Procedure

Complete these steps, coordinating with the other learners in your workgroup.

Step 1 Where should you look to isolate the specific causes of any problems?

____

What commands might you use to look for issues?

____

____

Step 2 Coordinate with your workgroup to isolate the specific causes of any network problems that you identified.

Step 3 On the troubleshooting log, document each identified network problem on a specific device. The troubleshooting log is divided into four possible areas of concern: core routing and switching, distribution routing, access routing, and access switching.

Step 4 Repeat Step 1 and Step 2 as needed to isolate the specific causes of all problems.

Step 5 Develop a plan to correct the identified problems and document the plan in the space provided below.

____

____

____

____

____

Step 6 Assign the documented problems to members of your workgroup.

Step 7 Have the instructor review your troubleshooting log and correction plan.

Exercise Verification

You have completed this exercise when you attain these results:

- The problems that you discovered are documented in the troubleshooting log.
- You have isolated the specific causes of all network problems.
- Your workgroup has an implementation plan for correcting the isolated problems.

Lab Exercise (Trouble Ticket B) 3-1: Correcting Problems at the Physical and Data Link Layers

Complete this lab exercise by correcting the problems that you isolated in Case Study (Trouble Ticket B) 3-1: Isolating Physical and Data Link Layer Problems.

Exercise Objective

In this exercise, you will use various Cisco commands to correct network problems.

You will complete the following steps:

- Implement a troubleshooting implementation plan
- Verify that the data flow in the network matches your network baseline

Required Resources

These are the resources and equipment required to complete this exercise:

- Access to the workgroup PCs and Cisco devices in the lab network
- Familiarity with Cisco router and switch commands covered in the Cisco *Building Scalable Cisco Internetworks* (BSCI), *Building Cisco Multilayer Switched Networks* (BCMSN), and *Building Cisco Remote Access Networks* (BCRAN) courses
- Access to a protocol analyzer (either software or hardware)
- A network baseline documenting the lab installation
- A troubleshooting log listing isolated physical or data link problems
- An implementation plan for correcting documented physical and data link layer problems

Job Aids

This job aid is available to help you complete the lab exercise:

- Information on Trouble Ticket B

Trouble Ticket B

You recently joined the second-level network support team for Acme. This evening you are on call for network outages. You read this report during your review of the activity log.

Network Support Activity Log

Time	Log Entry
5:30 p.m.	One Acme user reported that access to the server seemed to be slower than usual. – Help Desk – [Assigned to Network Operations]
6:01 p.m.	We checked and could ping the server. We scanned the configs on all the network devices. They look fine. – 2nd shift ops –
6:15 p.m.	Multiple users started reporting that they are can no longer reach anything. –Help Desk –
6:37 p.m.	We can ping the core devices, but also noticed some network latency from the access router. Escalated to Level 1 Network Support. – 2nd shift ops – [Assigned to Mike]
6:52 p.m.	I asked the network operations team if anyone changed anything. They do not think that anyone changed anything important. Not sure what they changed. – Mike –
7:23 p.m.	I tried to fix up the configs to resolve the user access and resolve the network latency issues. I am not sure what to back out, but the issues are worse. The serial link on distribution router is flapping. I can no longer reach the CIT_Server from anywhere. – Mike –
7:33 p.m.	Escalated to Level 2 Network Support.

Task 1: Implement the Troubleshooting Plan

Coordinate activities within your workgroup.

Exercise Procedure

Complete these steps:

Step 1 Connect to the workgroup devices as needed.

Step 2 Carry out your troubleshooting implementation plan to correct all network problems.

Step 3 Verify that the network data flows match the network baseline and that you have not introduced any new problems onto the network.

Exercise Verification

You have completed this exercise when you attain these results:

- Your network data flows match the network baseline.
- You can use Telnet from the pod PC to connect to the host named Cisco (simulated on ISP1).
- You can ping the host named ISP2.
- You can browse the web files on the CIT_Server.
- You can use Telnet to connect to the CIT_Server from your pod PC.
- You can use FTP to send a file from the CIT_Server to your pod PC.

Lab Exercise (Trouble Ticket C) 3-2: Troubleshooting Problems at the Physical and Data Link Layers

Complete this lab exercise by defining, isolating, and correcting the problems outlined in Trouble Ticket C to restore the network to baseline specifications.

Exercise Objective

In this exercise, each workgroup will use a troubleshooting methodology and Cisco commands to start isolating issues.

After completing this exercise, you will be able to meet these objectives:

- Follow a logical troubleshooting process to define, isolate, and correct problems outlined in a trouble ticket
- Verify that the trouble ticket has been resolved
- Verify that the data flow in the network matches your network baseline

Required Resources

These are the resources and equipment required to complete this exercise:

- Access to the workgroup PCs and Cisco devices in the lab network
- Familiarity with Cisco router and switch commands covered in the Cisco *Building Scalable Cisco Internetworks* (BSCI), *Building Cisco Multilayer Switched Networks* (BCMSN), and *Building Cisco Remote Access Networks* (BCRAN) courses
- Access to a protocol analyzer (either software or hardware)
- A network baseline documenting the lab installation

Command List

The commands used in this exercise are described in the table here.

Helpful Commands

Command	Description
ping *{host | ip-address}*	Pings an IP address.
show cdp neighbors [detail]	Displays CDP neighbor information.
show controllers *{type number}*	Displays controller information and status.
show etherchannel summary	Displays EtherChannel port-channel summary status, including data link (Layer 2) or network (Layer 3) layer port and interface information.
show frame-relay map	Displays Frame Relay mapping status.
show frame-relay pvc	Displays Frame Relay PVC information and status.
show interface status	Displays a tabular status report of the ports on a switch.
show interfaces port-channel *{interface-number}*	Displays port-channel status, including Layer 2 or Layer 3 port and interface information.
show interfaces trunk	Shows trunking interfaces.
show ip interface brief	Displays brief form of interface information.
show ip route	Displays IP routing table information.
show protocols	Displays network layer addresses and interface status.
show running-config	Displays device configuration information.
show running-config interface *{type number}*	Displays configuration information for one interface.
show spanning-tree	Displays STP information, including port status.
show tdm clock	Shows TDM-related information.
show version	Displays general hardware and software information.
show vlan	Displays VLAN information.
show vtp status	Displays VTP status, including domain name and revision number.
telnet *{ip-address}*	Uses Telnet to connect to an IP address.
traceroute *{ip-address}*	Runs traceroute to an IP address.

Job Aids

These job aids are available to help you complete the lab exercises:

- Information on Trouble Ticket C
- Troubleshooting Log Table

Trouble Ticket C

You recently joined the second-level network support team for Acme. You know from baseline information you previously gathered that Acme has a hierarchy of routing and switching in the core, routing in the distribution layer, and switched LANs connecting its end users at the access layer. Last night, a contractor was supposed to perform a minor upgrade to the network core in Kansas. This morning, your team is reviewing a network outage.

Network Support Activity Log

Time	Log Entry
`6:46 a.m.`	Network errors are reported by the network management system. Not sure what the contractor was doing.
`6:51 a.m.`	The network is not functioning. The contractor really made a mess of things. It appears that this person had no Cisco experience and does not understand WANs, either.
`6:54 a.m.`	The network is not functioning. Using our common passwords, the contractor seems to have been logging into devices all over the network. Wish we had more details.
`7:03 a.m.`	Record whatever configuration problems you fix—we will need those when we discuss the situation with the person from accounting who insisted on selecting the lowest-price contractor.

Troubleshooting Log: Troubleshooting Physical and Data Link Layer Problems

Problem	Solution
Core Router/Switch	
Distribution Router	
Access Router	
Access Switch	

Task 1: Resolving the Trouble Ticket

Coordinate activities within your workgroup.

Exercise Procedure

Complete these steps, coordinating with the other learners in your workgroup.

Step 1 What questions should you ask the users?

____

____

What commands should the users try from their PC?

____

____

Step 2 Document the symptoms of the problem on the troubleshooting log. The troubleshooting log is divided into four possible areas of concern: core routing and switching, distribution routing, access routing, and access switching.

Step 3 Where should you look first in the network to isolate the problems?

____

What commands might you use to look for issues?

____

____

Step 4 Where should you look next to isolate the problems?

____

What commands might you use to look for issues?

____

____

Step 5 Coordinate with your workgroup to isolate the problems.

Step 6 Repeat Step 1 through Step 5 as needed to isolate all the problems.

Step 7 Develop a plan to correct the identified problems and document the plan in the space provided below.

____

____

____

____

____

Step 8 Execute the plan you developed to correct the identified problems.

Step 9 Verify that the network data flows match the network baseline and that you have not introduced any new problems into the network.

Exercise Verification

You have completed this exercise when you attain these results:

- Your network data flows match the network baseline.
- You can use Telnet to connect to the host named Cisco (simulated on ISP1).
- You can ping the host named ISP2.
- You can browse the web files on the CIT_Server.
- You can use Telnet to connect to the CIT_Server from your pod PC.
- You can use FTP to send a file from CIT_Server to your pod PC.

Case Study (Trouble Ticket D) 4-1: Isolating Network Layer Problems

Complete this case study to practice what you learned in the related lesson. You will be given a problem situation that has been escalated to Level 2 Engineering. You will analyze user feedback and end-system data, and you will use Cisco commands and applications to isolate the specific cause of any problems.

Exercise Objective

In this exercise, you will use a troubleshooting methodology and Cisco commands to isolate the specific causes of any network problems. Complete these steps, coordinating with the other learners in your workgroup:

- Implement a troubleshooting methodology to analyze user feedback and end-system data to determine at which OSI layer to begin isolating a problem
- Isolate the specific cause of any problems using Cisco tools
- Develop a plan for resolving problems

After completing this exercise, you will be able to meet these objectives:

- Analyze user feedback and end-system data to decide at which OSI layer to begin isolating problems
- Identify troubleshooting tools to use to isolate the specific causes of any network problems
- Develop a troubleshooting implementation plan for resolving any identified problems

Required Resources

These are the resources and equipment required to complete this exercise:

- Access to the workgroup PCs and Cisco devices in the lab network
- Familiarity with Cisco router and switch commands covered in the Cisco *Building Scalable Cisco Internetworks* (BSCI), *Building Cisco Multilayer Switched Network* (BCMSN), and *Building Cisco Remote Access Networks* (BCRAN) courses
- A completed baseline topology diagram documenting the lab installation
- Network documentation recording the configuration of the lab installation

Command List

The commands used in this exercise are described in the table here.

Helpful Commands

Command	Description
ping {*host* | ip-*address*}	Pings an IP address.
show ip bgp	Displays entries in the BGP routing table.
show ip bgp summary	Shows summary BGP status.
show ip interface brief	Displays brief form of interface information.
show ip *protocol* interface	Displays the status and parameters of the interfaces configured for a specific protocol. The variable *protocol* specifies the protocol.
show ip *protocol* neighbor	Displays information about neighbors for a specific routing protocol.
show ip protocols	Displays values about routing timers and network information associated with the entire router. Use this information to identify a router that is suspected of delivering bad router information.
show ip route	Displays IP routing table information.
show protocols	Displays Layer 3 addresses and interface status.

Job Aids

These job aids are available to help you complete the lab exercise:

- Information on Trouble Ticket D
- Troubleshooting Log

Trouble Ticket D

You are part of the second-level network support team for Acme. This morning, the network support team for Acme implemented multipoint subinterfaces for the distribution layer routers in preparation for the eventual connection of additional access routers. Network Support also implemented point-to-point subinterfaces on the access routers. You just received a page to check your e-mail for details on a network outage that was escalated to Level 2 Support. Your e-mail shows the following activity log.

Network Support Activity Log

Time	Log Entry
9:17 a.m.	Acme sales department can no longer connect to anything. HTTP and ping are not working.
9:44 a.m.	We updated some group parameters on the server for the sales department. We believe we have resolved the issue. [MIS]
9:53 a.m.	The sales department at Acme is complaining about receiving network error messages about address conflicts. Other users are reporting that they can no longer reach anything via their browsers or Telnet sessions. [Terry is working on the problem.]
10:03 a.m.	Network connectivity errors are reported by the network management system on the distribution router. [Robin is working on the problem.]
10:04 a.m.	Network connectivity issues are reported between the core devices and the access router. [Lynn is working on the problem.]
10:09 a.m.	Request escalation of this ticket to Level 2 Support. The network is not functioning. In retrospect, it was probably a bad idea to have Terry, Robin, and Lynn simultaneously changing the configurations. We would look at it some more, but we need to leave for a team meeting. [From Tracy, Level 1 team lead]

Troubleshooting Log: Isolating Network Layer Problems

Problem	Solution
Core Router/Switch	
Distribution Router	
Access Router	
Access Switch	

Exercise Procedure

Complete these steps, coordinating with the other learners in your workgroup.

Step 1 Add the Frame Relay interfaces to your existing network diagram.

Step 2 Where should you look to isolate the specific causes of any problems?

____

What Cisco commands would you use to look for issues?

____

____

____

____

Step 3 On the troubleshooting log, document each identified network problem on a specific device. The troubleshooting log is divided into four possible areas of concern: core routing and switching, distribution routing, access routing, and access switching. Include the problems discovered by other members of your workgroup.

Step 4 Repeat Step 1 and Step 2 as needed to isolate the specific causes of all problems.

Step 5 Develop a plan to correct the identified problems and document the plan in the space provided below.

____

____

____

____

____

Step 6 Assign the documented problems to members of your workgroup.

Step 7 Have the instructor review your troubleshooting log and correction plan.

Exercise Verification

You have completed this exercise when you attain these results:

- You have recorded the Frame Relay subinterface and DLCI numbers on your network diagram.
- The instructor has verified that you have documented all the problems in your workgroup on your troubleshooting log.
- Every member in your workgroup has been assigned one or more problems for resolution from the troubleshooting log.

Lab Exercise (Trouble Ticket D) 4-1: Correcting Problems at the Network Layer

Complete this lab exercise by correcting the problems that you isolated in Case Study (Trouble Ticket D) 4-1: Isolating Network Layer Problems, and to practice what you learned in the related lesson.

Exercise Objective

In this exercise, you will use various Cisco commands to correct network layer problems.

You will complete the following steps:

- Implement the plan you developed during the case study
- Verify that the data flow in the network matches your network baseline

Required Resources

These are the resources and equipment required to complete this exercise:

- Access to the workgroup PCs and Cisco devices in the lab network
- Familiarity with Cisco router and switch commands covered in *Building Scalable Cisco Internetworks* (BSCI), *Building Cisco Multilayer Switched Networks* (BCMSN), and *Building Cisco Remote Access Networks* (BCRAN)
- Access to a protocol analyzer (either software or hardware)
- A network baseline documenting the lab installation
- A troubleshooting log listing isolated physical or data link problems
- An implementation plan for correcting documented physical and data link layer problems

Job Aids

This job aid is available to help you complete the lab exercise:

- Information on Trouble Ticket D

Trouble Ticket D

You are part of the second-level network support team for Acme. This morning, Acme implemented multipoint subinterfaces for its distribution layer routers in preparation for the eventual connection of additional access routers. Acme also implemented point-to-point subinterfaces on the access routers. You just received a page to check your e-mail for details on a network outage that was escalated to Level 2 Support. Your e-mail shows the activity log.

Network Support Activity Log

Time	Log Entry
9:17 a.m.	Acme sales department can no longer connect to anything. HTTP and ping are not working.
9:44 a.m.	We updated some group parameters on the server for the sales department. We believe that we have resolved the issue. [MIS]
9:53 a.m.	The sales department at Acme is complaining about receiving network error messages about address conflicts. Other users are reporting that they are can no longer reach anything via their browsers or Telnet sessions. [Terry is working on the problem.]
10:03 a.m.	Network connectivity errors are reported by the network management system on the distribution router. [Robin is working on the problem.]
10:04 a.m.	Network connectivity issues are reported between the core devices and the access router. [Lynn is working on the problem.]
10:09 a.m.	Request escalation of this ticket to Level 2 Support. The network is not functioning. In retrospect, it was probably a bad idea to have Terry, Robin, and Lynn simultaneously changing the configurations. We would look at it some more, but we need to leave for a team meeting. [From Tracy, Level 1 team lead]

Task 1: Implement the Troubleshooting Plan

Coordinate activities within your workgroup.

Exercise Procedure

Complete these steps:

(Connect to the workgroup devices as needed.)

Step 1 Carry out your troubleshooting implementation plan to correct all network problems.

Step 2 Verify that the network data flows match the network baseline and that you have not introduced any new problems into the network.

Exercise Verification

You have completed this exercise when you attain these results:

- Your network data flows match the network baseline.
- You can use Telnet from the pod PC to connect to the host named Cisco (simulated on ISP1).
- You can ping the host named ISP2.
- You can browse web files on the CIT_Server.
- You can use Telnet to connect to the CIT_Server from your pod PC.
- You can use FTP to send a file from the CIT_Server to your pod PC.

Lab Exercise (Trouble Ticket E) 4-2: Troubleshooting Problems at the Physical, Data Link, and Network Layers

Complete this lab exercise by defining, isolating, and correcting the problems outlined in Trouble Ticket E to restore the network to baseline specifications.

Exercise Objective

In this exercise, each workgroup will use a troubleshooting methodology and Cisco commands to define, isolate, and correct issues. You will complete the following steps:

- Define the problem by questioning users and by using end-system tools
- Isolate the problem by analyzing documented symptoms and using Cisco commands
- Consider options for solving the problem
- Develop a troubleshooting implementation plan for correcting the problems that you identified
- Execute your troubleshooting implementation plan
- Verify that the network is restored to baseline specifications and that you have not introduced any new problems into the network

After completing this exercise, you will be able to meet these objectives:

- Follow a logical troubleshooting process to define, isolate, and correct problems outlined in a trouble ticket
- Verify that the trouble ticket has been resolved
- Verify that the data flow in the network matches your network baseline

Required Resources

These are the resources and equipment required to complete this exercise:

- Access to the workgroup PCs and Cisco devices in the lab network
- Familiarity with Cisco router and switch commands covered in *Building Scalable Cisco Internetworks* (BSCI), *Building Cisco Multilayer Switched Networks* (BCMSN), and *Building Cisco Remote Access Networks* (BCRAN)
- Access to a protocol analyzer (either software or hardware)
- A network baseline documenting the lab installation
- A troubleshooting log listing isolated physical or data link problems
- An implementation plan for correcting documented physical and data link layer problems

Command List

The commands used in this exercise are described in the table here.

Helpful Commands

Command	Description
ping {***host*** | ***address***}	Pings an IP address.
show cdp neighbors [detail]	Displays CDP neighbor information.
show controllers {***type number***}	Displays controller information and status.
show etherchannel summary	Displays EtherChannel port-channel summary status, including Layer 2 or Layer 3 port and interface information.
show frame-relay map	Displays Frame Relay mapping status.
show frame-relay pvc	Displays Frame Relay PVC information and status.
show interface port-channel {*channel*}	Displays port-channel status, including Layer 2 or Layer 3 port and interface information.
show interfaces trunk	Shows trunking interfaces.
show ip bgp	Displays entries in the BGP routing table.
show ip bgp summary	Shows summary BGP status.
show ip interface brief	Displays brief form of interface information.
show ip *protocol* **interface**	Displays interface information for a protocol.
show ip *protocol* **neighbor**	Displays information about neighbors for a specific routing protocol.
show ip protocols	Displays routing protocol status.
show ip route	Displays IP routing table information.
Show protocols	Displays Layer 3 addresses and interface status.
show running-config interface {*type number*}	Displays configuration information for one interface.
show spanning-tree	Displays STP information, including port status.
show tdm clock	Shows TDM-related information.
show vlan	Displays VLAN information.
show vtp status	Displays VTP status, including domain name and revision number.
telnet *{ip-address}*	Uses Telnet to connect to an IP address.
traceroute *{ip-address}*	Runs traceroute to an IP address.

Job Aids

These job aids are available to help you complete the lab exercise:

- Information on Trouble Ticket E

Trouble Ticket E

A huge lightning strike startles you on a day off from work. A few moments later, your cell phone rings. You recognize the phone number—it is for Level 1 Network Support at Acme.

"The lightning has been wild over by the office for the last hour," Lynn tells you. "We lost power twice and also lost a router. But when we powered up our spare and loaded our backup configuration, we could not get connectivity to the core. We called around, and several of our sites have also had power interruptions. It is probably some simple issue, but we have not been able to restore operations. We need to get this resolved quickly so payroll can be run at 7:00 a.m. So we decided to call you."

You tell Lynn that you will connect in from home and figure out what is going on.

Troubleshooting Log: Troubleshooting Physical, Data Link, and Network Layer Problems

Problem	Solution
Core Router/Switch	
Distribution Router	
Access Router	
Access Switch	

Task 1: Resolving the Trouble Ticket

Coordinate activities within your workgroup.

Exercise Procedure

Complete these steps, coordinating with the other learners in your workgroup.

Step 1 What questions should you ask the users?

____

____

What commands should the users try from their PCs?

____

____

Step 2 Document the symptoms of the problem on the troubleshooting log. The troubleshooting log is divided into four possible areas of concern: core routing and switching, distribution routing, access routing, and access switching.

Step 3 Where should you look first in the network to isolate the problems?

____

What commands might you use to look for issues?

____

____

Step 4 Where should you look next to isolate the problems?

____

What commands might you use to look for issues?

____

____

Step 5 Coordinate with your workgroup to isolate the problems.

Step 6 Repeat Step 1 through Step 5 as needed to isolate all the problems.

Step 7 Develop a plan to correct the identified problems and document the plan in the space provided below.

____

____

____

____

____

Step 8 Carry out your troubleshooting implementation plan to correct all network errors.

Step 9 Verify that the network data flows match the network baseline and that you have not introduced any new problems into the network.

Exercise Verification

You have completed this exercise when you attain these results:

- Your network data flows match the network baseline.
- You can use Telnet from the pod PC to connect to the host named Cisco (simulated on ISP1).
- You can ping the host named ISP2.
- You can browse the web files on the CIT_Server.
- You can use Telnet to connect to the CIT_Server from your pod PC.
- You can use FTP to send a file from the CIT_Server to your pod PC.

Lab Exercise (Trouble Ticket F) 4-3: Troubleshooting Problems at the Physical, Data Link, and Network Layers

Complete this lab exercise by defining, isolating, and correcting the problems outlined in Trouble Ticket F to restore the network to baseline specifications.

Exercise Objective

In this exercise, each workgroup will use a troubleshooting methodology and Cisco commands to define, isolate, and correct issues. You will complete the following steps:

- Define the problem by questioning users and using end-system tools
- Isolate the problem by analyzing documented symptoms and using Cisco commands
- Consider options for solving the problem
- Develop a troubleshooting implementation plan for correcting the problems that you identified
- Execute your troubleshooting implementation plan
- Verify that the network is restored to baseline specifications and that you have not introduced any new problems into the network

After completing this exercise, you will be able to meet these objectives:

- Follow a logical troubleshooting process to define, isolate, and correct problems outlined in a trouble ticket
- Verify that the trouble ticket has been resolved
- Verify that the data flow in the network matches your network baseline

Required Resources

These are the resources and equipment required to complete this exercise:

- Access to the workgroup PCs and Cisco devices in the lab network
- Familiarity with Cisco router and switch commands covered in *Building Scalable Cisco Internetworks* (BSCI), *Building Cisco Multilayer Switched Networks* (BCMSN), and *Building Cisco Remote Access Networks* (BCRAN)
- Access to a protocol analyzer (either software or hardware)
- A network baseline documenting the lab installation
- A troubleshooting log listing isolated physical or data link problems
- An implementation plan for correcting documented physical and data link layer problems

Command List

The commands used in this exercise are described in the table here.

Helpful Commands

Command	Description
ping {host | address}	Pings an IP address.
show cdp neighbors [detail]	Displays CDP neighbor information.
show etherchannel summary	Displays EtherChannel port-channel summary status, including Layer 2 or Layer 3 port and interface information.
show frame-relay map	Displays Frame Relay mapping status.
show frame-relay pvc	Displays Frame Relay PVC information and status.
show interface port-channel {*channel*}	Displays port-channel status, including Layer 2 or Layer 3 port and interface information.
show interfaces trunk	Shows trunking interfaces.
show ip bgp	Displays entries in the BGP routing table.
show ip bgp summary	Shows summary BGP status.
show ip interface brief	Displays brief form of interface information.
show ip *protocol* **interface**	Displays interface information for a protocol.
show ip *protocol* **neighbor**	Displays information about neighbors for a specific routing protocol.
show ip protocols	Displays routing protocol status.
show ip route	Displays IP routing table information.
show protocols	Displays Layer 3 addresses and interface status.
show running-config interface {*type number*}	Displays configuration information for one interface.
show spanning-tree	Displays STP information, including port status.
show vlan	Displays VLAN information.
show vtp status	Displays VTP status, including domain name and revision number.
telnet {*ip-address*}	Uses Telnet to connect to an IP address.
traceroute {*ip-address*}	Runs traceroute to an IP address.

Job Aids

These job aids are available to help you complete the lab exercise:

- Information on Trouble Ticket F
- Sketch of planned implementation

Trouble Ticket F

You made it through your first few days as a second-level network support engineer for Acme. Nothing too striking happened; you spent most of your time documenting what was in place in the Acme backbone and troubleshooting some network issues.

Yesterday, you went to a new employee orientation class. Unfortunately, you left your new cell phone at the office to charge.

When you return to your office, you see that users and Level 1 Support have been calling. Your phone reports 27 messages since lunch yesterday. Robin, a Level 1 engineer, has appeared in person at your office door.

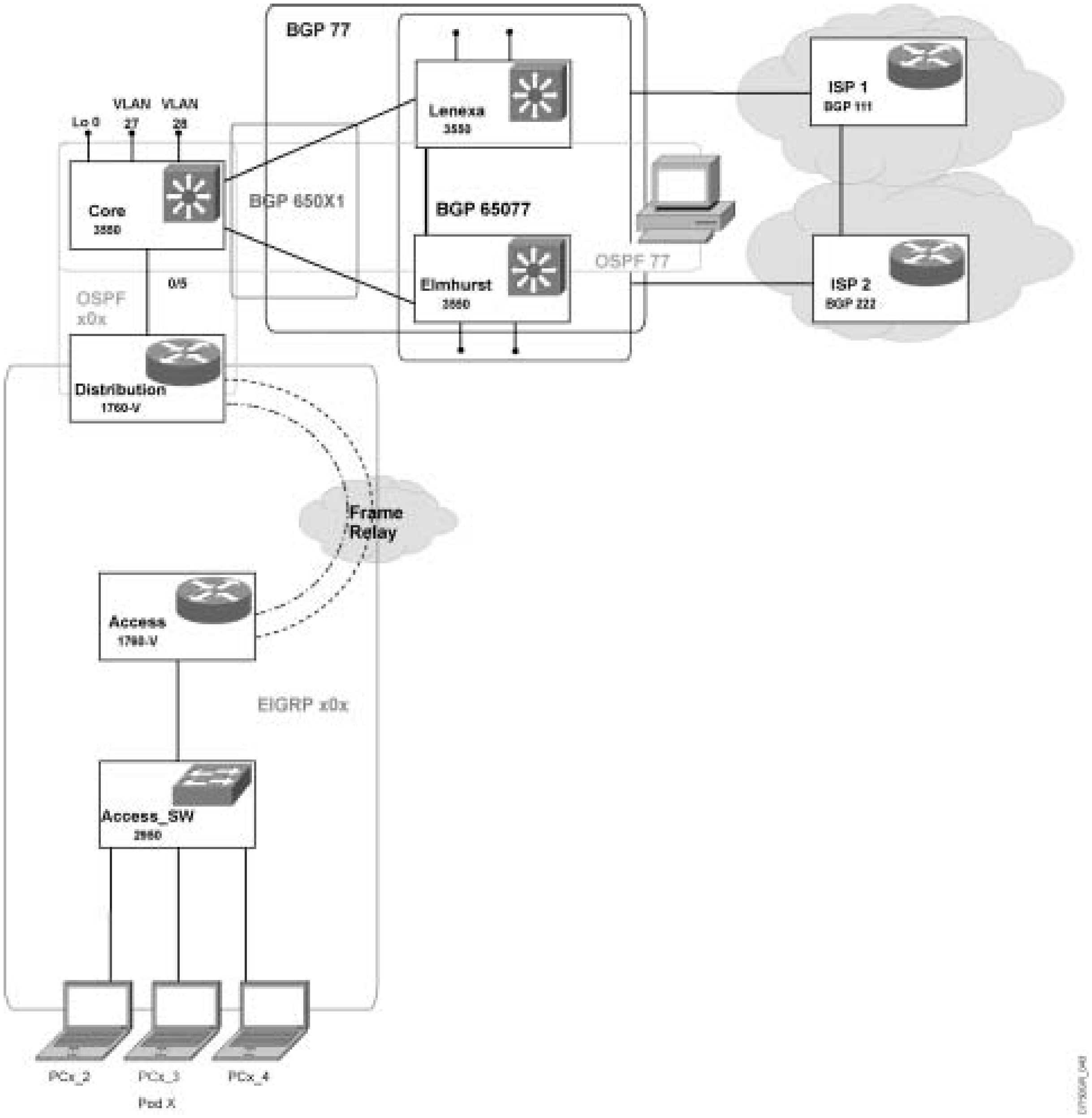
This engineer summarizes the situation. “We received a new management edict—no proprietary protocols in the core or distribution layer. EIGRP has to be scrapped and replaced with OSPF. And both of our ISPs complained about our ‘borrowing’ of AS numbers and recommended that we implement BGP confederations.”

You tell the engineer that you will come up with a conversion plan this morning.

“Well, management insisted that we perform the conversion yesterday,” the engineer says. “We did try calling you. When we could not reach you, Terry joined the conversion. EIGRP was left on the access routers, because Terry could not get an OK from those locations for an upgrade. Terry took out RIP in the core and completed the cutover to the frame links between the distribution and access routers. When Terry left for vacation, it was almost working.”

You realize that the users have a different opinion about whether the network is working. Robin hands you a rough sketch of the planned implementation.

Planned Implementation



Troubleshooting Log: Troubleshooting Physical, Data Link, and Network Layer Problems

Problem	Solution
Core Router/Switch	
Distribution Router	
Access Router	
Access Switch	

Task 1: Resolving the Trouble Ticket

Coordinate activities within your workgroup.

Exercise Procedure

Complete these steps:

Step 1 What questions should you ask the users?

____

____

What commands should they try from their PCs?

____

____

Step 2 Document the symptoms of the problem on the troubleshooting log. The troubleshooting log is divided into four possible areas of concern: core routing and switching, distribution routing, access routing, and access switching.

Step 3 Where should you look first in the network to isolate the problems?

____

What commands might you use to look for issues?

____

____

Step 4 Where should you look next to isolate the problems?

____

What commands might you use to look for issues?

____

____

Step 5 Coordinate with your workgroup to isolate the problems.

Step 6 Repeat Step 1 through Step 5 as needed to isolate all the problems.

Step 7 Develop a plan to correct the identified problems and document the plan in the space provided below.

____

____

____

____

____

Step 8 Update your network diagram to remove the old serial links and include the new routing protocols.

Step 9 Carry out your troubleshooting implementation plan to correct all network problems.

Step 10 Verify that the network data flows match the network baseline and that you have not introduced any new problems into the network.

Exercise Verification

You have completed this exercise when you attain these results:

- Your network data flows match the network baseline.
- You can use Telnet from the pod PC to connect to the host named Cisco (simulated on ISP1).
- You can ping the host named ISP2.
- You can browse the web files on the CIT_Server.
- You can use Telnet to connect to the CIT_Server from your pod PC.
- You can use FTP to send a file from the CIT_Server to your pod PC.
- Your baseline topology diagram is updated to show the current WAN links and routing protocols.

Case Study (Trouble Ticket G) 5-1: Isolating Problems at the Transport and Application Layers

Complete this case study to practice what you learned in the related lesson. You will be given a problem situation escalated to Level 2 Engineering. You will analyze user feedback and end-system data and use Cisco commands and applications to isolate the specific cause of any problems.

Required Resources

These are the resources and equipment required to complete this exercise:

- Access to the workgroup PCs and Cisco devices in the lab network
- Familiarity with Cisco router and switch commands covered in the Cisco *Building Scalable Cisco Internetworks* (BSCI), *Building Cisco Multilayer Switched Networks* (BCMSN), and *Building Cisco Remote Access Networks* (BCRAN) courses
- A completed baseline topology diagram documenting the lab installation
- Network documentation recording the configuration of the lab installation

Exercise Objective

In this exercise, you will use a troubleshooting methodology and Cisco commands to isolate the specific causes of network problems. Complete these steps, coordinating with the other learners in your workgroup:

- Analyze user feedback and end-system data to decide at which OSI layer to begin isolating a problem
- Isolate the specific cause of any problems using Cisco tools
- Develop a plan for resolving problems

After completing this exercise, you will be able to meet these objectives:

- Analyze user feedback and end-system data to decide at which OSI layer to begin isolating problems
- Select the troubleshooting tools to use to isolate the specific causes of any network problems
- Develop a troubleshooting implementation plan for resolving any identified problems

Command List

The commands used in this exercise are described in the table here.

Helpful Commands

Command	Description
arp -a	Displays ARP information.
debug ip dhcp server	Displays DHCP server debugging.
debug ip eigrp	Enables debugging of EIGRP events.
debug ip ospf adj	Enables debugging of Open Shortest Path First (OSPF) adjacencies.
debug ip policy	Enables debugging of the IP policy.
debug ip routing	Enables debugging of IP routing events.
ipconfig /all	Displays IP information for the PC.
ping {*host* | *address*}	Pings an IP address.
route print	Displays active routes for the PC.
show access-lists	Displays access list information.
show ip bgp	Displays entries in the BGP routing table.
show ip bgp summary	Shows summary BGP status.
show ip dhcp binding	Displays address bindings on the DHCP server.
show ip dhcp server statistics	Displays DHCP server statistics.
show ip interface brief	Displays brief form of interface information.
show ip policy	Displays which route map is associated with which interface.
show ip protocol interface	Displays interface information for a protocol.
show ip protocol neighbor	Displays information about neighbors for a specific routing protocol.
show ip protocols	Displays routing protocol status.
show ip route	Displays IP routing table information.
show route-map	Displays route map information.
show spanning-tree vlan *vlan-id*	Displays STP information, including port status for a specific VLAN.
show vlan *vlan-id*	Displays default and defined VLAN information.
telnet {*host* | *ip-address*}	Connects to an IP address via the Telnet application.
traceroute [*destination*]	Runs traceroute to an IP address.
tracert {*ip-address*}	Runs tracert from a PC to an IP address.

Job Aids

These job aids are available to help you complete the lab exercises:

- Information on Trouble Ticket G
- Troubleshooting Log

Trouble Ticket G

After you cleaned up the migration mess from this morning, you thought that the network was stable. Terry, the co-op student, wants to make a baseline of the Acme network for a networking class. Your boss, Lynn, tells Terry that this is OK, as long as the passwords are removed from the configurations before Terry brings them to class.

While you are out at lunch, you receive a call on your cell phone from Terry, who says that the network is down.

You ask what Terry did.

"Well, I was just running some **show** commands to get a baseline for my class," Terry starts, "and I was starting to disguise the corporate passwords. Then Lynn stopped by and asked me to implement OSPF authentication in the core."

"OK, then what?" you ask.

"I jumped right into the OSPF authentication implementation. While I was configuring OSPF, I tested a way to optimize the traffic throughout the network with our routing policy. But then I found I could not reach the Internet from the core switch, so I backed out the optimizations. Then Robin from MIS called and said that the users could not use TFTP to connect to the CIT server. Robin asked me to check the DHCP configuration. It looked OK to me. Do we have a TFTP application running on the CIT server?"

"No," you say, "we do not."

"So then I tried to connect to the access router," Terry continues. "But I could not get in. I asked the network administrators to reboot the network devices. They did, but I think they first saved my changes. Then MIS and Network Operations really started calling because the users could not access anything on the Internet or on our corporate server. I did try to back out my changes, but it was hard to concentrate with a lot of people yelling at me. I could not even log into most of the network devices. That is when I called you."

You need to isolate the cause of the problems and develop a plan to resolve them.

Troubleshooting Log: Isolating Transport and Application Layer Problems

Problem	Solution
Core Router/Switch	
Distribution Router	
Access Router	
Access Switch	

Exercise Procedure

Complete these steps, coordinating with the other learners in your workgroup.

Step 1 Where should you look to isolate the specific causes of any problems?

____

What commands might you use to look for issues?

____

____

Step 2 Coordinate with your workgroup to isolate the specific causes of any network problems that you identified.

Step 3 On the troubleshooting log, document each identified network problem on a specific device. The troubleshooting log is divided into four possible areas of concern: core routing and switching, distribution routing, access routing, and access switching.

Step 4 Repeat Step 1 and Step 2 as needed to isolate the specific causes of all problems.

Step 5 Develop a plan to correct the identified problems and document the plan in the space provided below.

____

____

____

____

____

Step 6 Assign the documented problems to members of your workgroup.

Step 7 Have the instructor review your troubleshooting log and correction plan.

Exercise Verification

You have completed this exercise when you attain these results:

- The problems that you discovered are documented in the troubleshooting log.
- You have isolated the specific causes of all network problems.
- Your workgroup has an implementation plan for correcting the isolated problems.

Lab Exercise (Trouble Ticket G) 5-1: Correcting Problems at the Transport and Application Layers

Complete this lab exercise by correcting the problems that you isolated in Case Study (Trouble Ticket G) 5-1: Isolating Problems at the Transport and Application Layers.

Exercise Objective

In this exercise, you will use various Cisco commands to correct network problems.

You will complete the following steps:

- Implement the plan you developed during the related case study
- Verify that the data flow in the network matches your network baseline

Required Resources

These are the resources and equipment required to complete this exercise:

- Access to the workgroup PCs and Cisco devices in the lab network
- Familiarity with Cisco router and switch commands covered in the Cisco *Building Scalable Cisco Internetworks* (BSCI), *Building Cisco Multilayer Switched Networks* (BCMSN), and *Building Cisco Remote Access Networks* (BCRAN) courses
- A network baseline documenting the lab installation
- A troubleshooting log listing isolated physical or data link problems
- An implementation plan for correcting documented physical and data link layer problems

Command List

The commands used in this exercise are described in the table here.

Helpful Commands

Command	Description
arp -a	Displays ARP information.
debug ip dhcp server	Displays DHCP server debugging.
debug ip eigrp	Enables debugging of EIGRP events.
debug ip ospf adj	Enables debugging of OSPF adjacencies.
debug ip policy	Enables debugging of the IP policy.
debug ip routing	Enables debugging of IP routing events.
ipconfig /all	Displays IP information for the PC.
ping {*host* | *address*}	Pings an IP address.
route print	Displays active routes for the PC.
show access-lists	Displays access list information.
show ip bgp	Displays entries in the BGP routing table.
show ip bgp summary	Shows summary BGP status.
show ip dhcp binding	Displays address bindings on the DHCP server.
show ip dhcp server statistics	Displays DHCP server statistics.
show ip interface brief	Displays brief form of interface information.
show ip policy	Displays which route map is associated with which interface.
show ip *protocol* **interface**	Displays interface information for a protocol.
show ip *protocol* **neighbor**	Displays information about neighbors for a specific routing protocol.
show ip protocols	Displays routing protocol status.
show ip route	Displays IP routing table information.
show route-map	Displays route map information.
show spanning-tree vlan *vlan-id*	Displays STP information, including port status for a specific VLAN.
show vlan *vlan-id*	Displays default and defined VLAN information.
telnet {*host* | *ip-address*}	Connects to an IP address via the Telnet application.
traceroute [*destination*]	Runs trace to an IP address.
tracert [*ip-address*]	Runs trace from a PC to an IP address.

Job Aids

This job aid is available to help you complete the lab exercise:

- Information on Trouble Ticket G

Trouble Ticket G

After you cleaned up the migration mess from this morning, you thought that the network was stable. Terry, the co-op student, wants to make a baseline of the Acme network for a networking class. Your boss, Lynn, tells Terry that this is OK, as long as the passwords are removed from the configs before Terry brings them to class.

While you are out at lunch, you receive a call on your cell phone from Terry, who says that the network is down. You ask what Terry did.

“Well, I was just running some **show** commands to get a baseline for my class,” Terry starts, “and I was starting to disguise the corporate passwords. Then Lynn stopped by and asked me to implement OSPF authentication in the core.”

“OK, then what?” you ask.

“I jumped right into the OSPF authentication implementation. While I was configuring OSPF, I tested a way to optimize the traffic throughout the network with our routing policy. But then I found I could not reach the Internet from the core switch, so I backed out the optimizations. Then Robin from MIS called and said that the users could not use TFTP to connect to the CIT server. Robin asked me to check the DHCP configuration. It looked OK to me. Do we have a TFTP application running on the CIT server?”

“No,” you say, “we do not.”

“So then I tried to connect to the access router,” Terry continues, “but I could not get in. I asked the network administrators to reboot the network devices. They did, but I think they first saved my changes. Then MIS and Network Operations really started calling because the users could not access anything on the Internet or on our corporate server. I did try to back out my changes, but it was hard to concentrate with a lot of people yelling at me. I could not even log into most of the network devices. That is when I called you.”

Task 1: Implement the Troubleshooting Plan

Coordinate activities within your workgroup.

Exercise Procedure

Complete these steps:

Step 1 Connect to the workgroup devices as needed.

Step 2 Carry out your troubleshooting implementation plan to correct all network problems.

Step 3 Verify that the network data flows match the network baseline and that you have not introduced any new problems into the network.

Exercise Verification

You have completed this exercise when you attain these results:

- Your network data flows match the network baseline.
- You can use Telnet from the pod PC to connect to the host named Cisco (simulated on ISP1).
- You can ping the host named ISP2.
- You can browse the web files on the CIT_Server.
- You can use Telnet to connect to the CIT_Server from your pod PC.
- You can use FTP to send a file from the CIT_Server to your pod PC.

Lab Exercise (Trouble Ticket H) 5-2: Troubleshooting Problems at All Logical Layers

Complete this lab exercise by defining, isolating, and correcting the problems outlined in Trouble Ticket H to restore the network to baseline specifications.

Exercise Objective

In this exercise, each workgroup will use a troubleshooting methodology and Cisco commands to define, isolate, and correct issues. You will complete the following steps:

- Define the problem by questioning users and using end-system tools
- Isolate the problem by analyzing documented symptoms and using Cisco tools
- Consider options for solving the problem
- Develop a troubleshooting implementation plan for correcting the problems that you identified
- Implement your troubleshooting implementation plan
- Verify that the network is restored to baseline specifications and that you have not introduced any new problems into the network

Required Resources

These are the resources and equipment required to complete this exercise:

- Access to the workgroup PCs and Cisco devices in the lab network
- Familiarity with Cisco router and switch commands covered in the Cisco *Building Scalable Cisco Internetworks* (BSCI), *Building Cisco Multilayer Switched Networks* (BCMSN), and *Building Cisco Remote Access Networks* (BCRAN) courses
- A network baseline documenting the lab installation

Command List

The commands used in this exercise are described in the table here.

Helpful Commands

Command	Description
arp -a	Displays ARP information.
debug ip dhcp server	Displays DHCP server debugging.
debug ip eigrp	Enables debugging of EIGRP events.
debug ip ospf adj	Enables debugging of OSPF adjacencies.
debug ip policy	Enables debugging of the IP policy.
debug ip routing	Enables debugging of IP routing events.
ipconfig /all	Displays IP information for the PC.
ping {*host* | *address*}	Pings an IP address.
route print	Displays active routes for the PC.
show access-lists	Displays access list information.
show ip bgp	Displays entries in the BGP routing table.
show ip bgp summary	Shows summary BGP status.
show ip dhcp binding	Displays address bindings on the DHCP server.
show ip dhcp server statistics	Displays DHCP server statistics.
show ip interface brief	Displays brief form of interface information.
show ip policy	Displays which route map is associated with which interface.
show ip *protocol* **interface**	Displays interface information for a protocol.
show ip *protocol* **neighbor**	Displays information about neighbors for a specific routing protocol.
show ip protocols	Displays routing protocol status.
show ip route	Displays IP routing table information.
show route-map	Displays route map information.
show spanning-tree vlan *vlan-id*	Displays STPI information, including port status for a specific VLAN.
show vlan *vlan-id*	Displays default and defined VLAN information.
telnet {*host* | *ip-address*}	Connects to an IP address via the Telnet application.
traceroute [*destination*]	Runs trace to an IP address.
tracert {ip-address}	Runs trace from a PC to an IP address.

Job Aids

These job aids are available to help you complete the lab exercise:

- Information on Trouble Ticket H
- Troubleshooting Log Table

Trouble Ticket H

When you arrive at work on Friday, Tracy is standing outside your office.

"You know how HR promised to inform us about employee terminations for personnel with network access before they occur?" Tracy asks.

"Yes, why?" you ask.

"Well, last night they escorted Lynn from MIS out of the building. They did not get word to us until well after everyone up here had gone home," Tracy says.

"So no one was here to turn off access to the devices?" you ask.

"Unfortunately, no," Tracy says. "It appears that Lynn has been in the network making some changes, but we are not sure exactly where. We shut down access for Lynn; however, the network is not working correctly. MIS first reported that the users could not get to any host on the Internet. Now, MIS reports that the end users appear to be getting network errors when they try to connect to anything. And Network Operations is reporting issues logging into the access and distribution routers, and problems reaching the Internet. To make matters worse, we cannot connect between the divisions."

Troubleshooting Log: Troubleshooting Problems at All Logical Layers

Problem	Solution
Core Router/Switch	
Distribution Router	
Access Router	
Access Switch	

Task 1: Implement the Troubleshooting Plan

Coordinate activities within your workgroup.

Exercise Procedure

Complete these steps, coordinating with the other learners in your workgroup.

Step 1 What questions should you ask the users?

____

____

What commands should the users try from their PC?

____

____

Step 2 Document the symptoms of the problem on the troubleshooting log. The troubleshooting log is divided into four possible areas of concern: core routing and switching, distribution routing, access routing, and access switching.

Step 3 Where should you look first in the network to isolate the problems?

____

What commands might you use to look for issues?

____

____

Step 4 Where should you look next to isolate the problems?

____

What commands might you use to look for issues?

____

____

Step 5 Coordinate with your workgroup to isolate the problems.

Step 6 Repeat Step 1 through Step 5 as needed to isolate all the problems.

Step 7 Develop a plan to correct the identified problems and document the plan in the space provided below.

____

____

____

____

____

Step 8 Execute the plan that you developed to correct the identified network problems.

Step 9 Verify that the network data flows match the network baseline and that you have not introduced any new problems into the network.

Exercise Verification

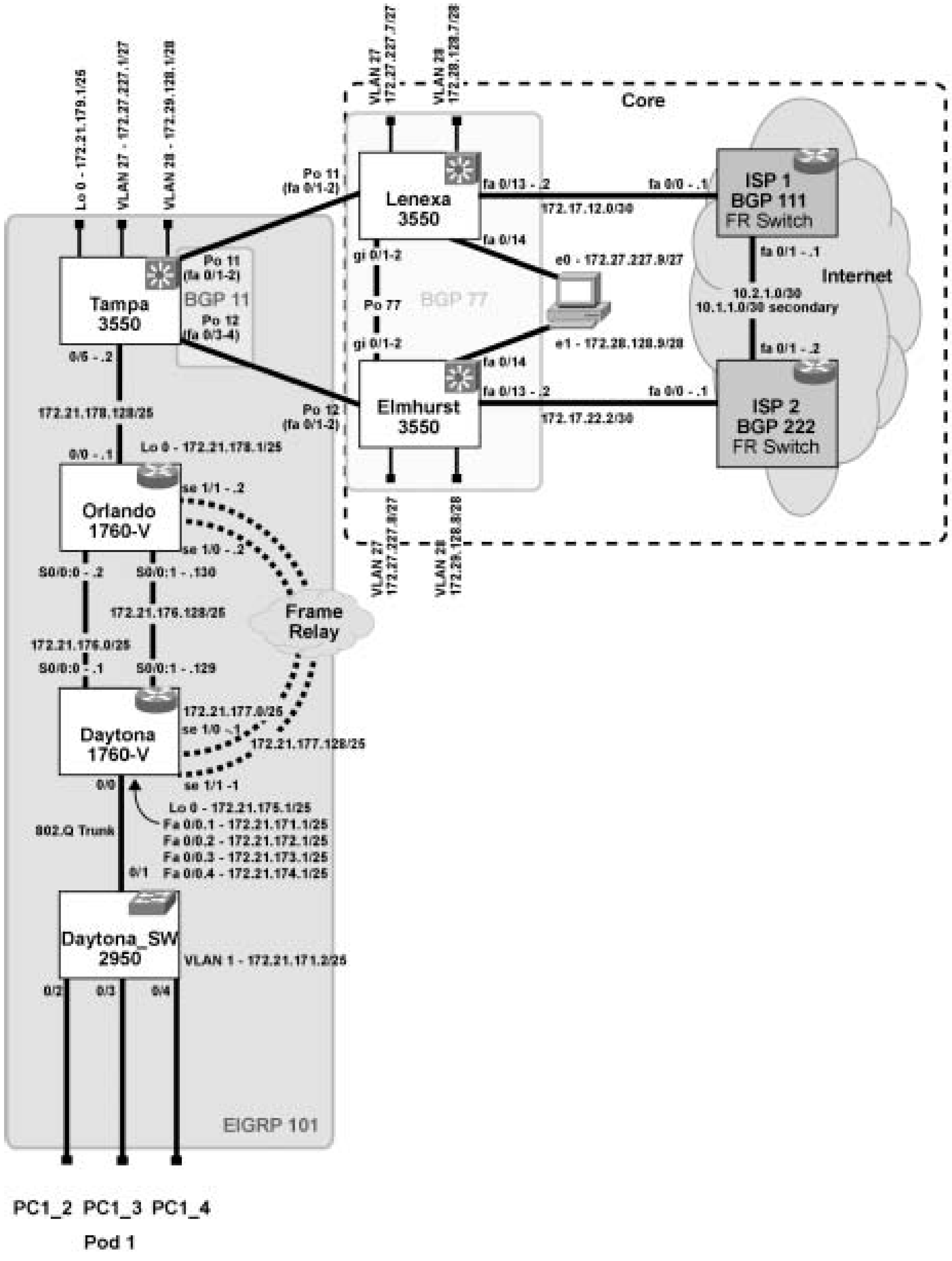
You have completed this exercise when you attain these results:

- Your network data flows match the network baseline.
- You can use Telnet from the pod PC to connect to the host named Cisco (simulated on ISP1).
- You can ping the host named ISP2.
- You can browse the web files on the CIT_Server.
- You can use Telnet to connect to the CIT_Server from your pod PC.
- You can use FTP to send a file from the CIT_Server to your pod PC.

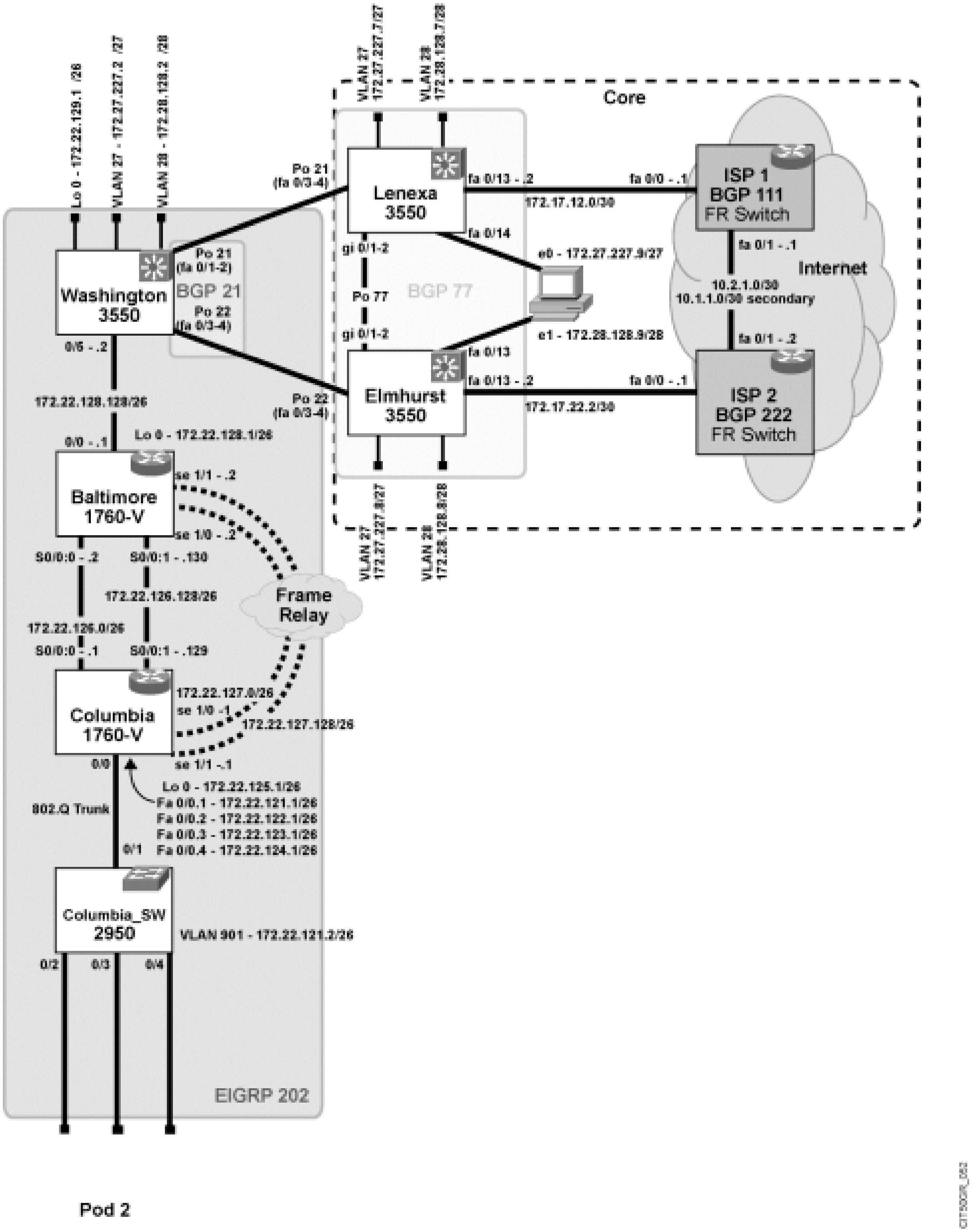
Lab Exercise Answer Key

Lab Exercise 1-1: Network Baseline Discovery

Baseline Network Diagram—Pod 1

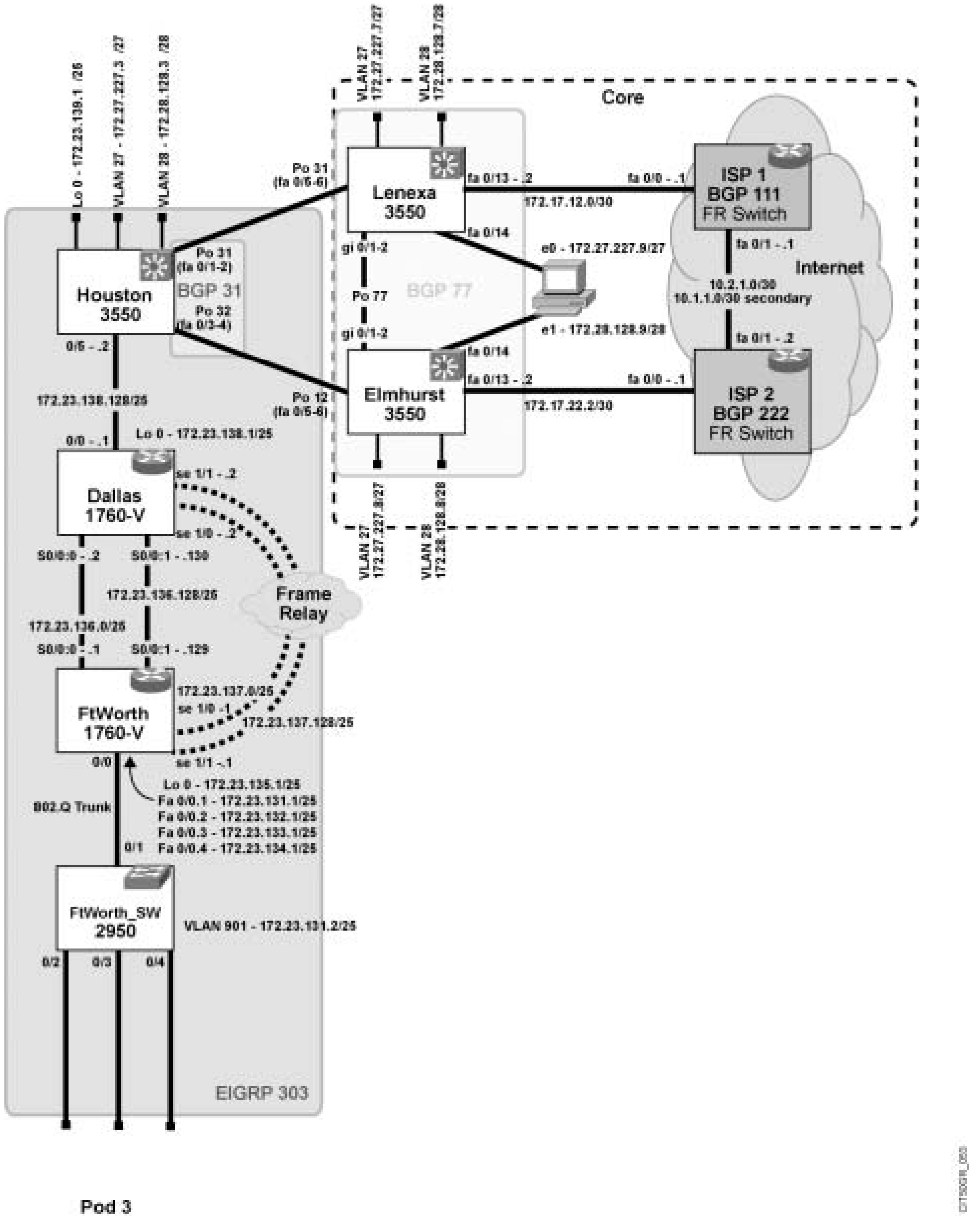


Baseline Network Diagram—Pod 2

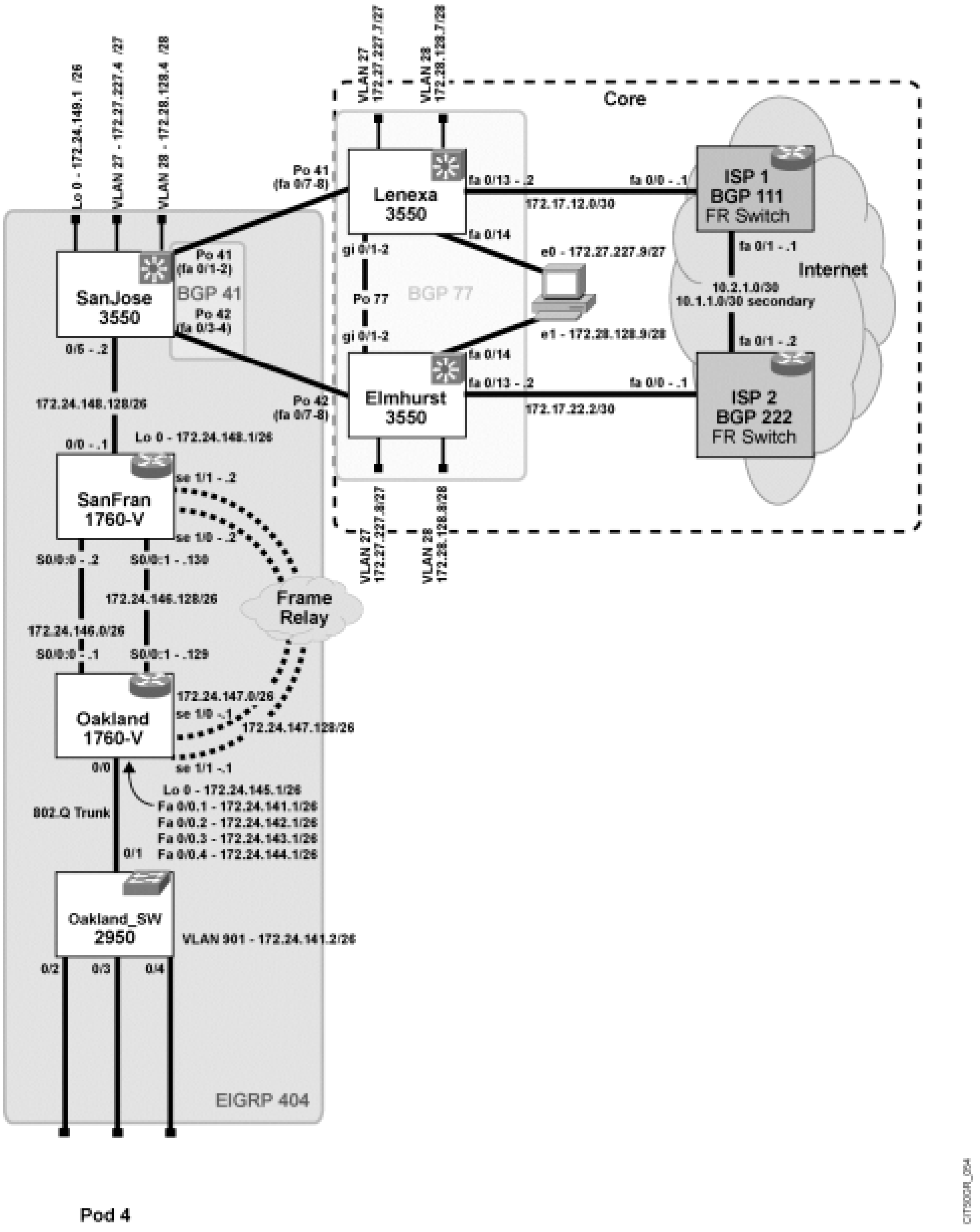


Pod 2

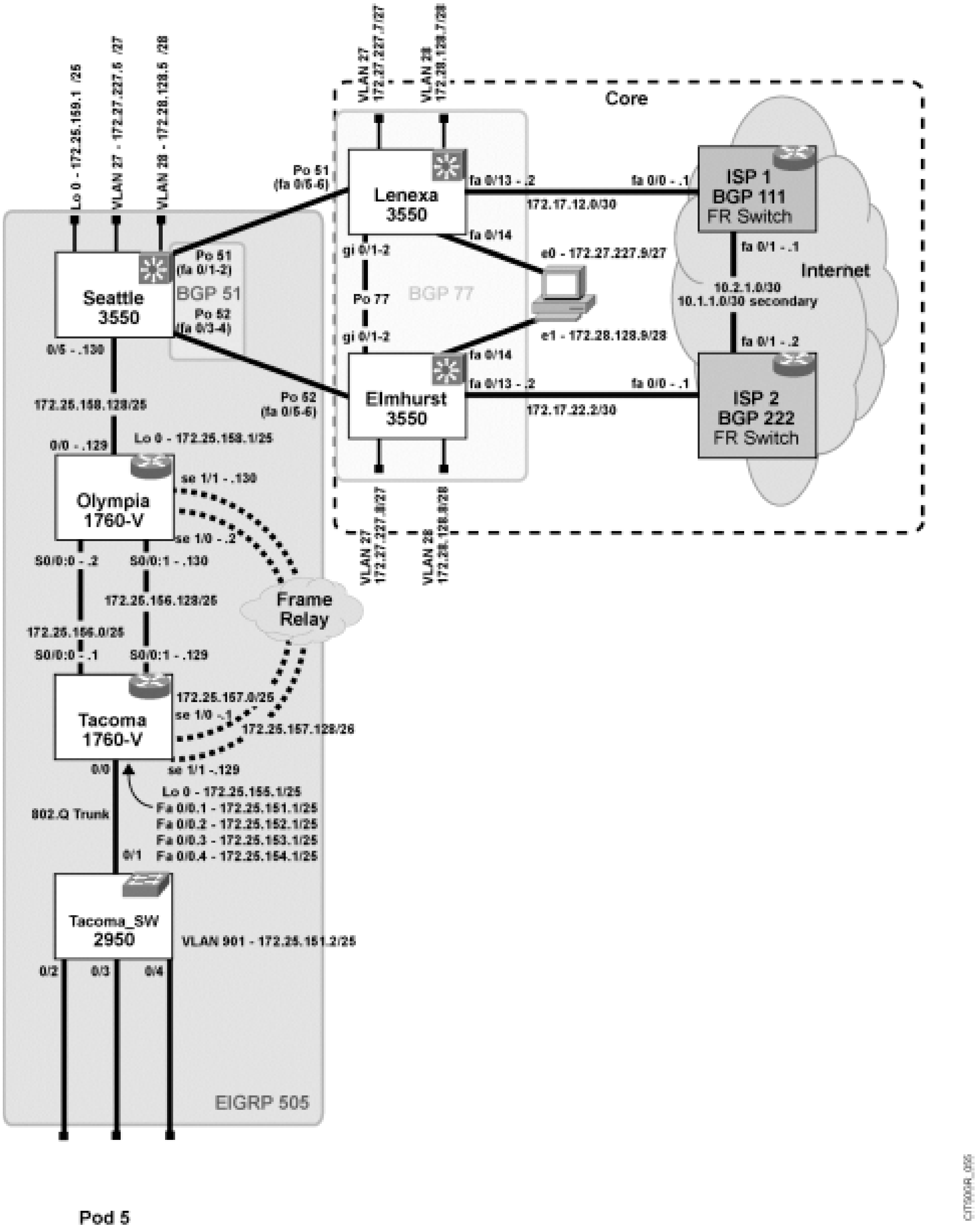
Baseline Network Diagram—Pod 3



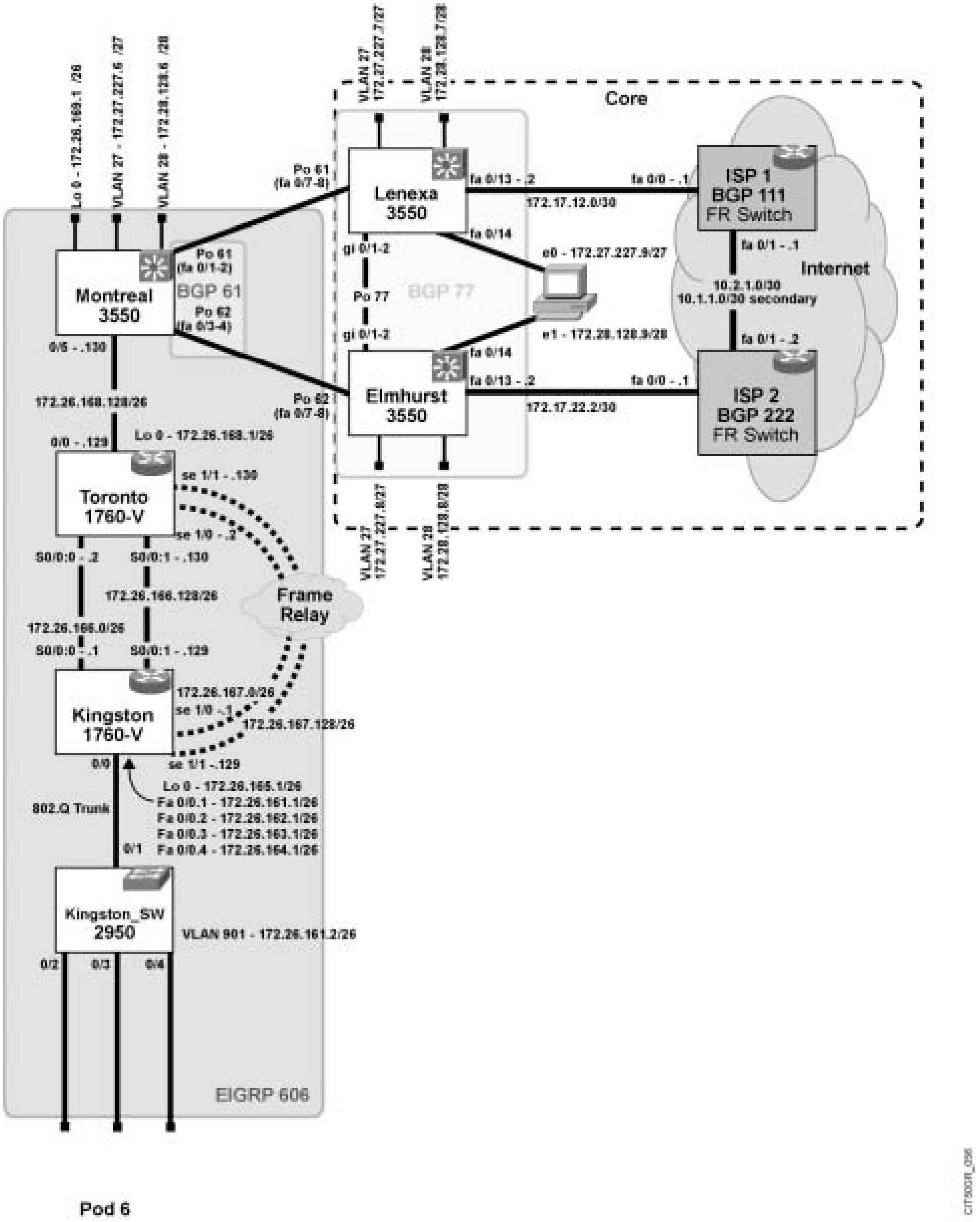
Baseline Network Diagram—Pod 4



Baseline Network Diagram—Pod 5



Baseline Network Diagram—Pod 6



Base Network Configuration Tables (All Pods)

Access Router

Device Name, Model	Interface	MAC Address	IP Address/ Subnet Mask	IP Routing Protocol(s)	Notes/Comments
Access Router Name 1760-V	Loopback 0		172.2x.1x5.1 /2x	EIGRP x0x	
Access Router Name 1760-V	Serial 0/0:0		172.2x.1x5.1 /2x	EIGRP x0x	768 K
Access Router Name 1760-V	Serial 0/0:1		172.2x.1x6.129 /2x	EIGRP x0x	64 K
Access Router Name 1760-V	Serial 1/0		172.2x.1x7.1 /2x	-----	Frame Relay
Access Router Name 1760-V	Serial 1/1		172.2x.1x7.129 /2x	-----	Frame Relay
Access Router Name 1760-V	Fast Ethernet 0/0.1		172.2x.1x1.1 /25	EIGRP x0x	VLAN 901
Access Router Name 1760-V	Fast Ethernet 0/0.2		172.2x.1x1.2 /25	EIGRP x0x	VLAN 2
Access Router Name 1760-V	Fast Ethernet 0/0.3		172.2x.1x1.3 /25	EIGRP x0x	VLAN 3
Access Router Name 1760-V	Fast Ethernet 0/0.4		172.2x.1x1.4 /25	EIGRP x0x	VLAN 4

Distribution Router

Device Name, Model	Interface	MAC Address	IP Address/ Subnet Mask	IP Routing Protocol(s)	Notes/Comments
Distribution Router Name 1760-V	Fast Ethernet 0/0		172.2x.1x8.129 /2x	EIGRP x0x	
Distribution Router Name 1760-V	Loopback 0		172.2x.1x8.1 /2x	EIGRP x0x	
Distribution Router Name 1760-V	Serial 0/0:0		172.2x.1x6.2 /2x	EIGRP x0x	768 K
Distribution Router Name 1760-V	Serial 0/0:1		172.2x.1x6.130 /2x	EIGRP x0x	64 K
Distribution Router Name 1760-V	Serial 1/0		172.2x.1x7.2 /2x	-----	Frame Relay
Distribution Router Name 1760-V	Serial 1/1		172.2x.1x7.130 /2x	-----	Frame Relay

Access Switch

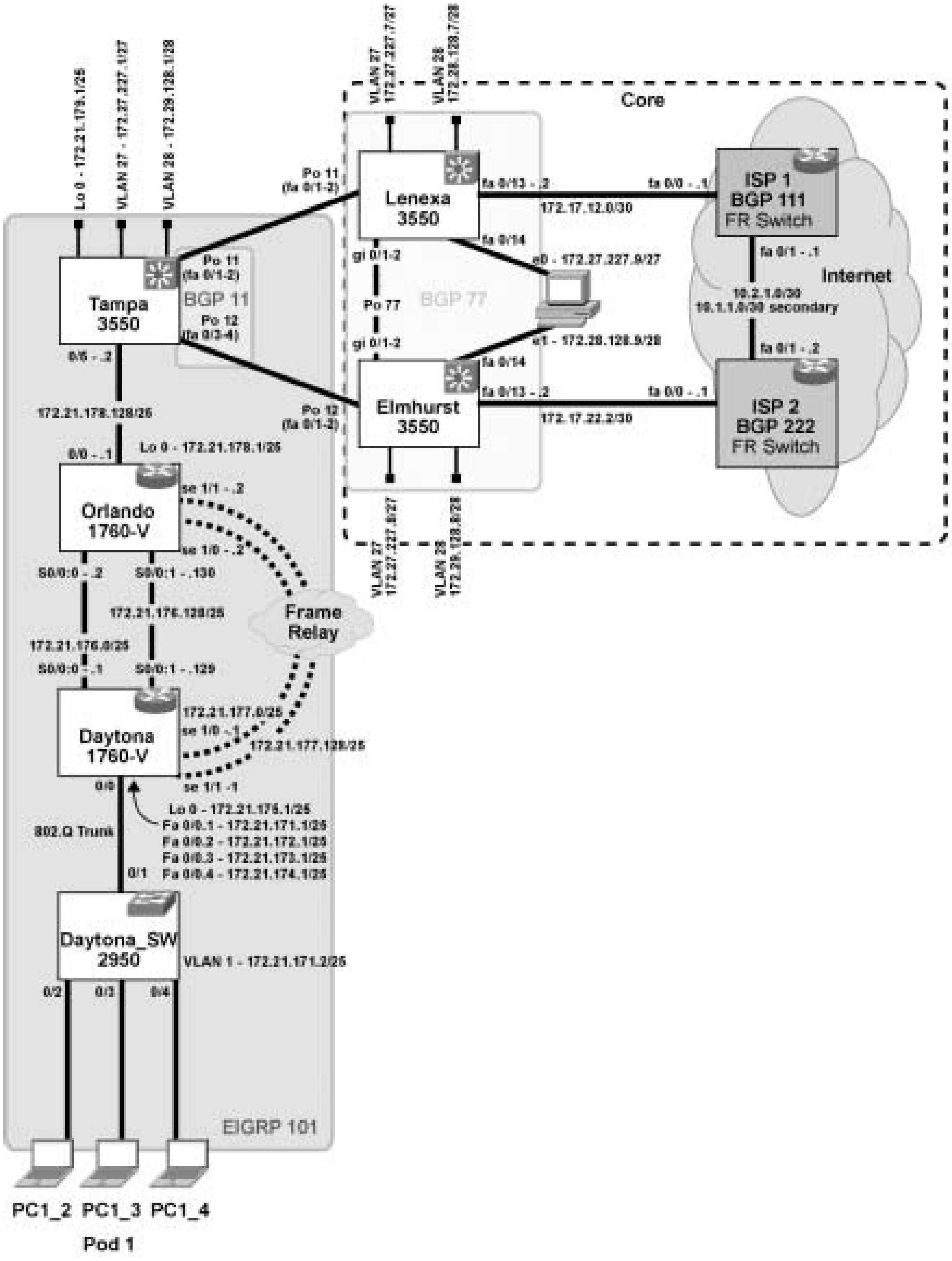
Catalyst Name, Model Management IP Address	Port	Speed	Duplex	STP State Fwd/Block	PortFast/ Trunk	Ether Channel (L2 or L3)	VLAN	IP Address
Access Switch Name Catalyst 3550 172.2x.1x1.2 /2x	Fa 0/1	100	Full	Fwd VLAN 901, 2, 3, 4	Trunk	-----	901, 2, 3, 4	172.2x.1x1.2 /2x
	Fa 0/2	100	Full	Fwd	PortFast	-----	2	
	Fa 0/3	100	Full	Fwd	PortFast	-----	3	
	Fa 0/4	100	Full	Fwd	PortFast	-----	4	

Core Router/Switch

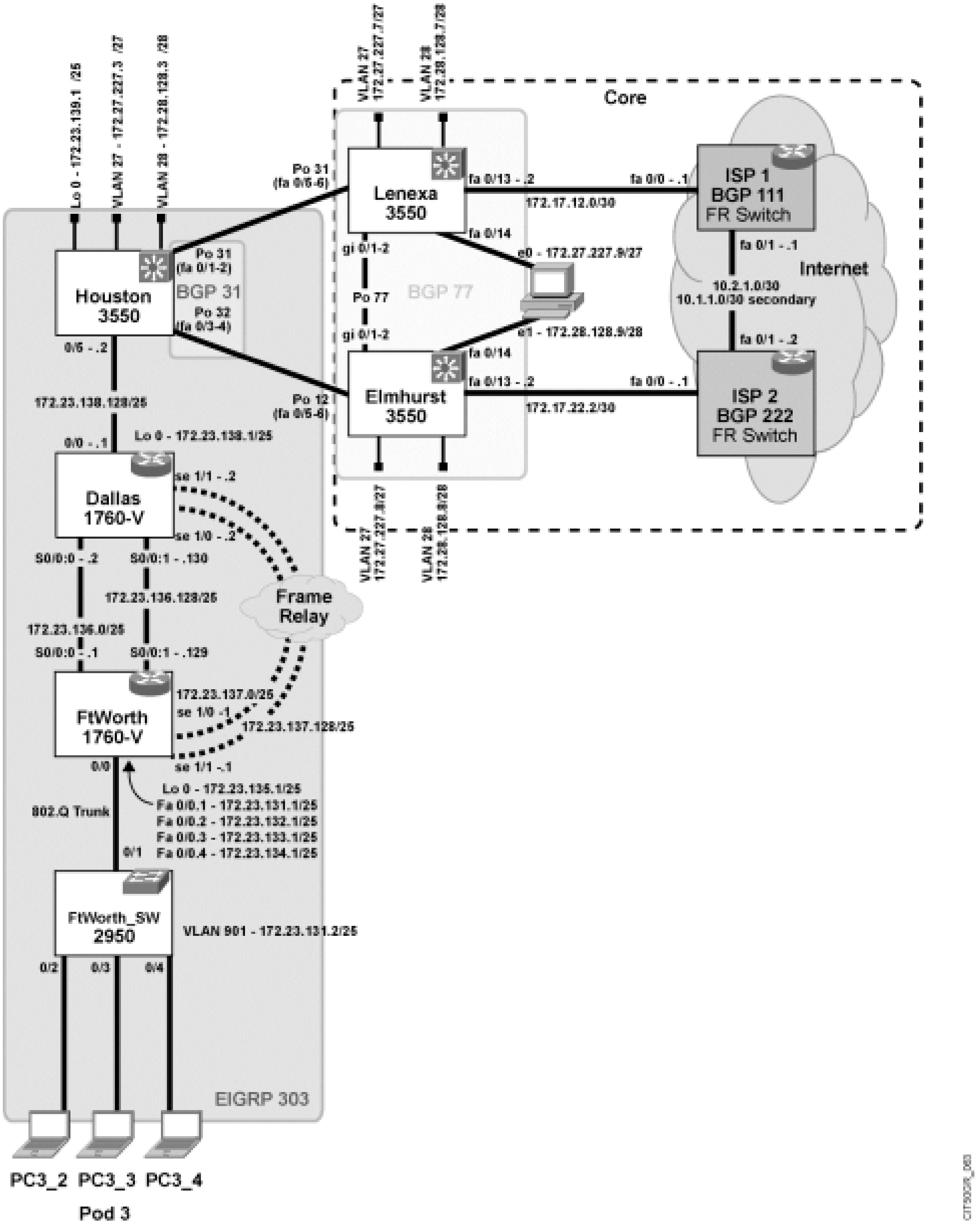
Catalyst Name, Model. Management IP Address	Port	Speed	Duplex	STP State Fwd/Block	PortFast/ Trunk	Ether Channel (L2 or L3)	VLAN	IP Address
Core Router/Switch Name Catalyst 3550	Fa 0/1	100	Full	Fwd VLAN 27 Bk VLAN 28	Trunk	Port 11 (L2)	1, 27, 28	
	Fa 0/2	100	Full	Fwd VLAN 27 Bk VLAN 28	Trunk	Port 11 (L2)	1, 27, 28	
	Fa 0/3	100	Full	Fwd VLAN 27 Bk VLAN 28	Trunk	Port 12 (L2)	1, 27, 28	
	Fa 0/4	100	Full	Fwd VLAN 27 Bk VLAN 28	Trunk	Port 12 (L2)	1, 27, 28	

Lab Exercise 1-2: Creating End-System Baseline Discovery

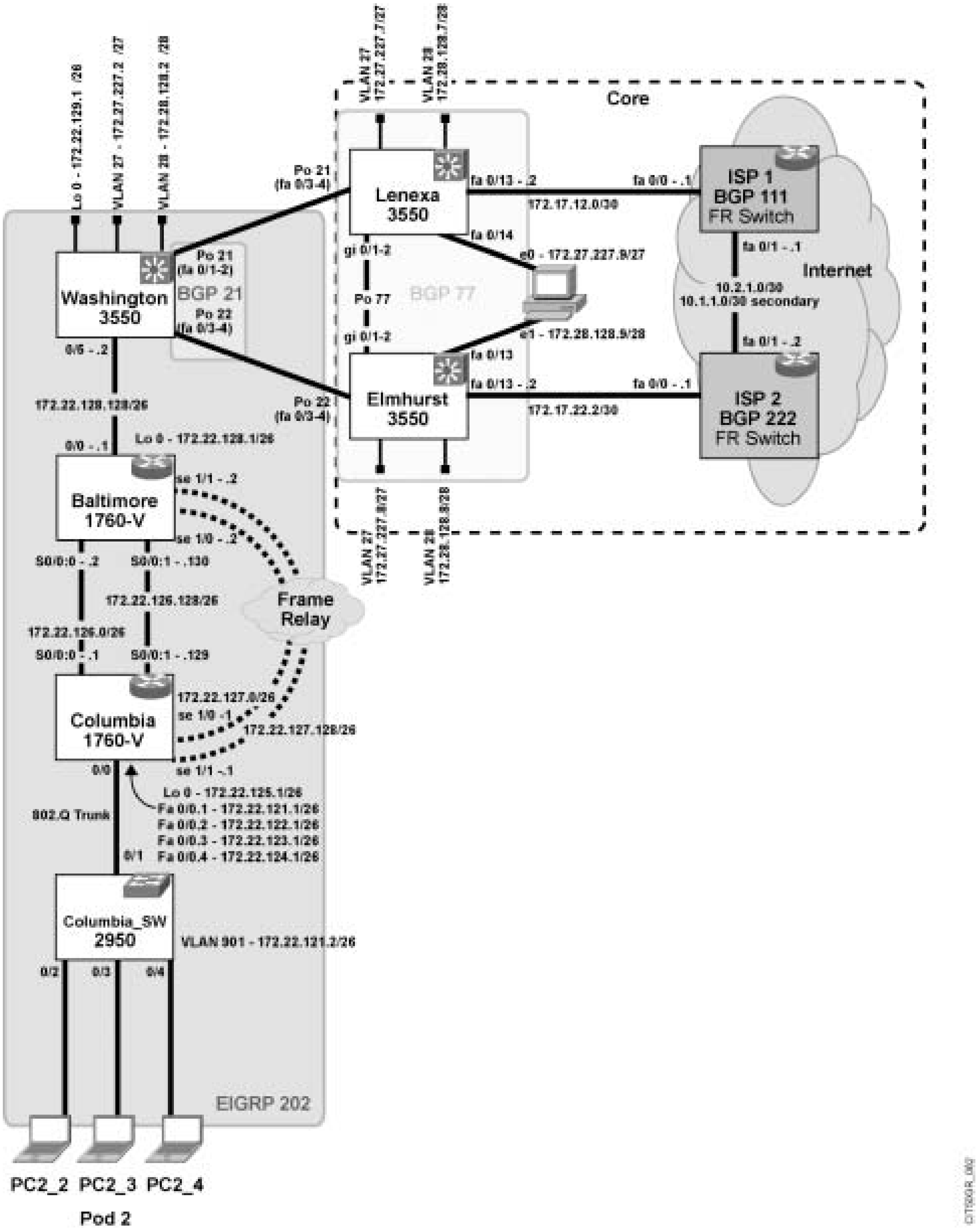
Baseline Network Diagram—Pod 1



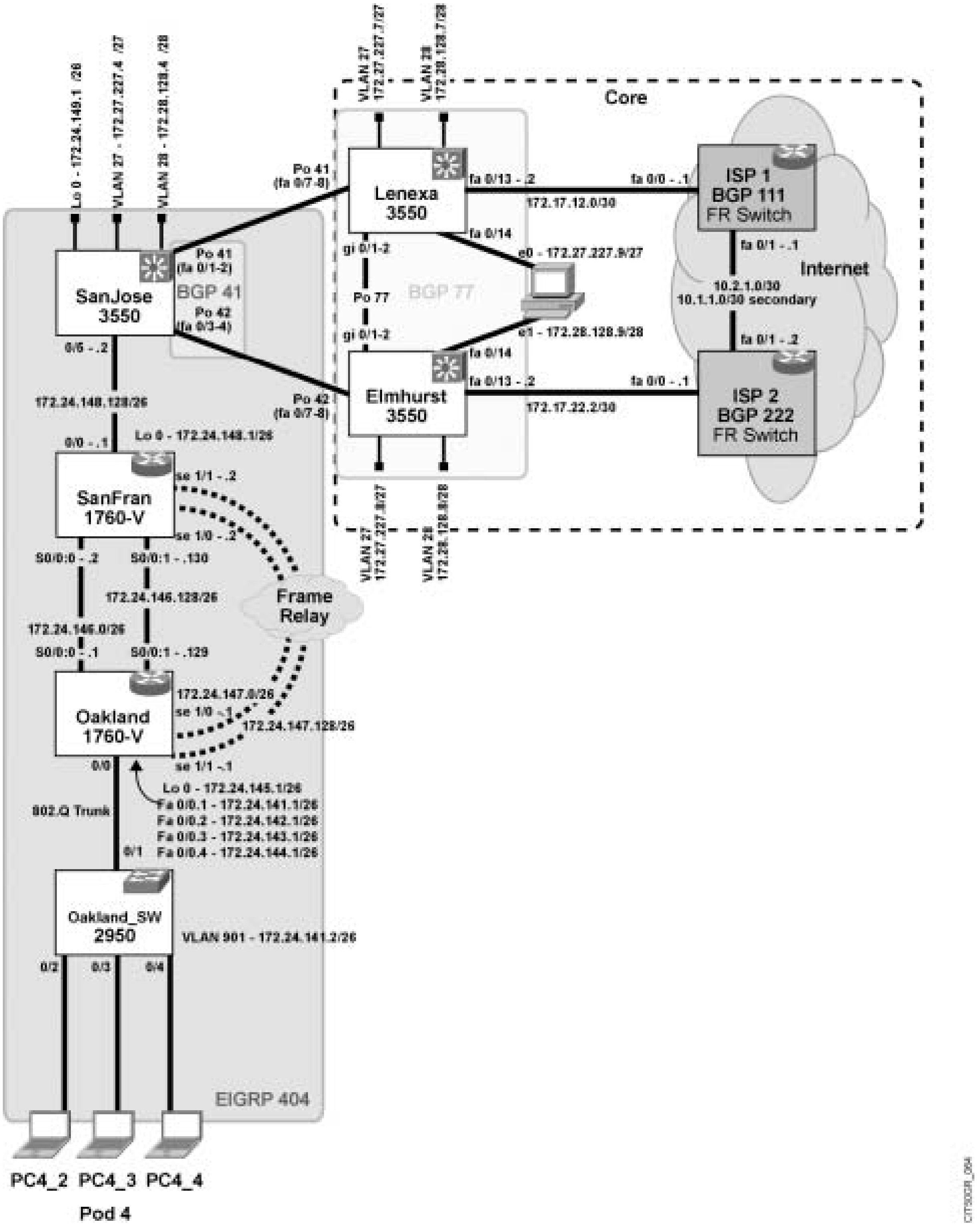
Baseline Network Diagram—Pod 2



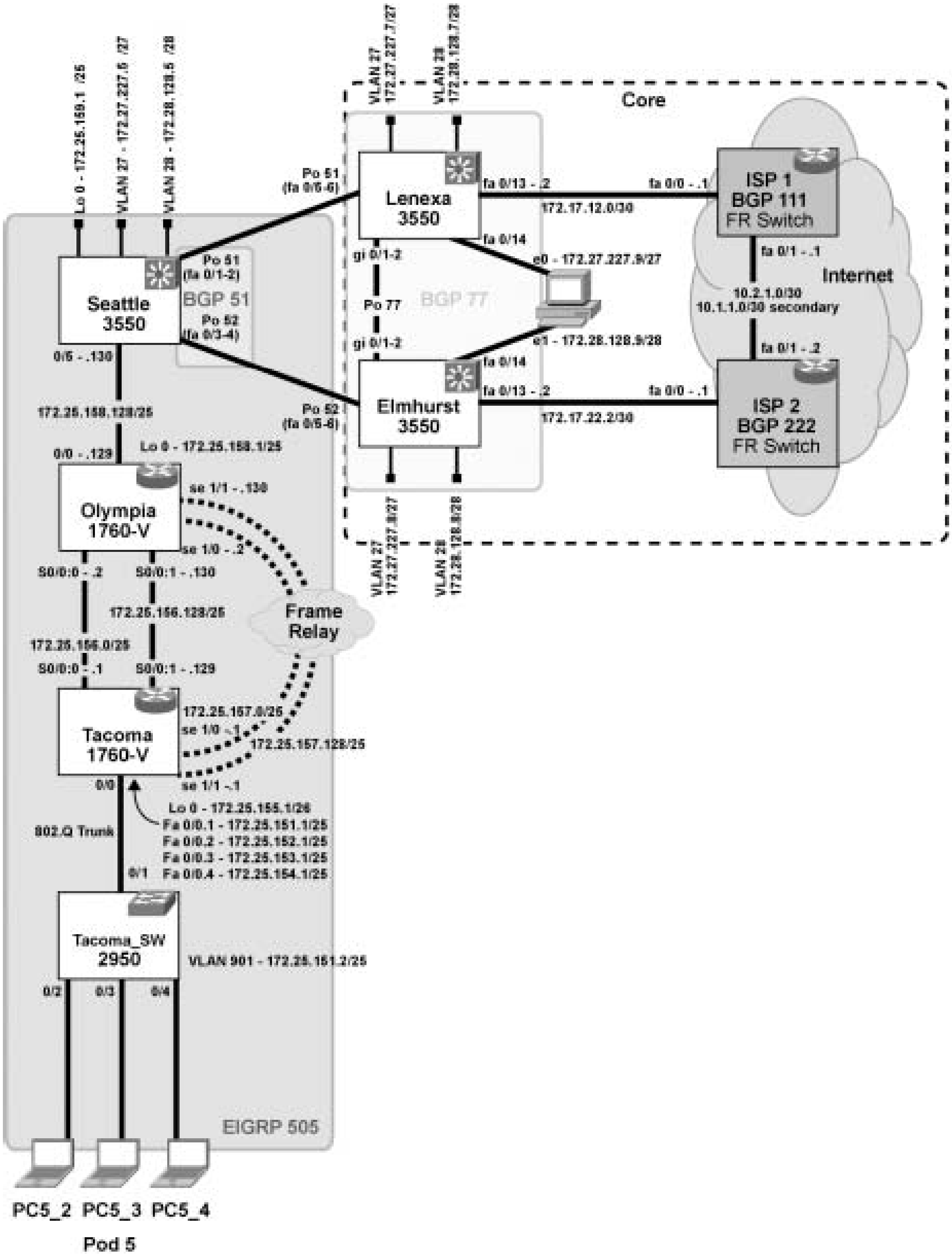
Baseline Network Diagram—Pod 3



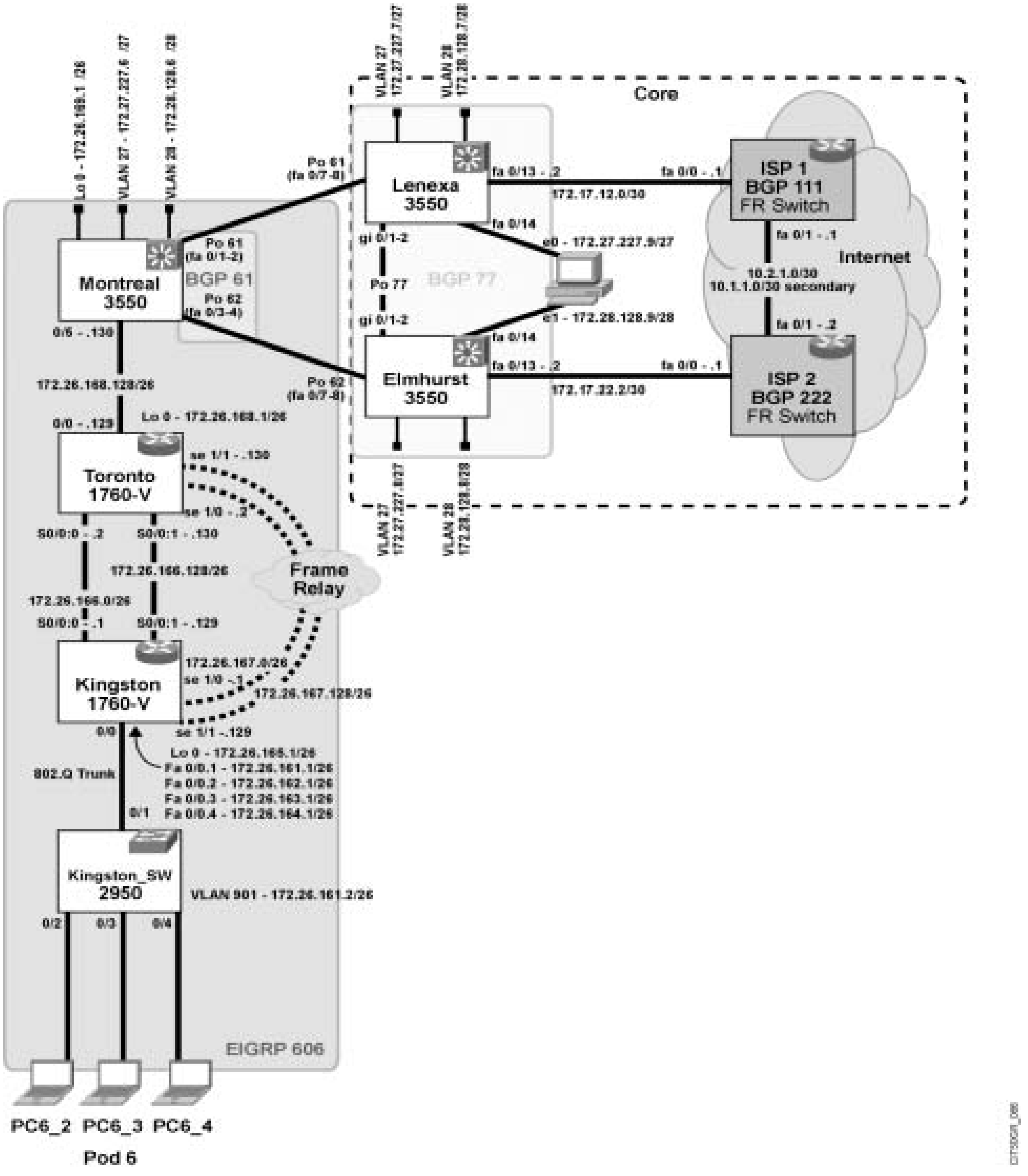
Baseline Network Diagram—Pod 4



Baseline Network Diagram—Pod 5



Baseline Network Diagram—Pod 6



Lab Exercise Answer Key (Cont.)

Your instructor will present solutions to the following exercises:

- Lab Exercise 2-1: Applying a Layered Model to a Network
- Case Study (Trouble Ticket A) 2-1: Gathering Symptoms
- Case Study (Trouble Ticket B) 3-1: Isolating Physical and Data Link Layer Problems
- Lab Exercise (Trouble Ticket B) 3-1: Correcting Problems at the Physical and Data Link Layers
- Lab Exercise (Trouble Ticket C) 3-2: Troubleshooting Problems at the Physical and Data Link Layers
- Case Study (Trouble Ticket D) 4-1: Isolating Network Layer Problems
- Lab Exercise (Trouble Ticket D) 4-1: Correcting Problems at the Network Layer
- Lab Exercise (Trouble Ticket E) 4-2: Troubleshooting Problems at the Physical, Data Link, and Network Layers
- Lab Exercise (Trouble Ticket F) 4-3: Troubleshooting Problems at the Physical, Data Link, and Network Layers
- Case Study (Trouble Ticket G) 5-1: Isolating Problems at the Transport and Application Layers
- Lab Exercise (Trouble Ticket G) 5-1: Correcting Problems at the Transport and Application Layers
- Lab Exercise (Trouble Ticket H) 5-2: Troubleshooting Problems at All Logical Layers