CCNA 3 v7.0 Curriculum: Module 12 – Network Troubleshooting

itexamanswers.net/ccna-3-v7-0-curriculum-module-12-network-troubleshooting.html

April 16, 2020

Contents

12.0. Introduction

12.0.1. Why should I take this module?

Welcome to Network Troubleshooting!

Who is the best network administrator that you have ever seen? Why do you think this person is so good at it? Likely, it is because this person is really good at troubleshooting network problems. They are probably experienced administrators, but that is not the whole story. Good network troubleshooters generally go about this in a methodical fashion, and they use all of the tools available to them.

The truth is that the only way to become a good network troubleshooter is to always be troubleshooting. It takes time to get good at this. But luckily for you, there are many, many tips and tools that you can use. This module covers the different methods for network troubleshooting and all of the tips and tools you need to get started. This module also has two really good Packet Tracer activities to test your new skills and knowledge. Maybe your goal should be to become the best network administrator that someone else has ever seen!

12.0.2. What will I learn to do in this module?

Module Title: Network Troubleshooting

Module Objective: Troubleshoot enterprise networks.

Topic Title	Topic Objective
Network Documentation	Explain how network documentation is developed and used to troubleshoot network issues.
Troubleshooting Process	Compare troubleshooting methods that use a systematic, layered approach.
Troubleshooting Tools	Describe different networking troubleshooting tools.

Topic Title	Topic Objective
Symptoms and Causes of Network Problems	Determine the symptoms and causes of network problems using a layered model.
Troubleshooting IP Connectivity	Troubleshoot a network using the layered model.

12.1. Network Documentation

12.1.1. Documentation Overview

As with any complex activity like network troubleshooting, you will need to start with good documentation. Accurate and complete network documentation is required to effectively monitor and troubleshoot networks.

Common network documentation includes the following:

- Physical and logical network topology diagrams
- Network device documentation that records all pertinent device information
- Network performance baseline documentation

All network documentation should be kept in a single location, either as hard copy or on the network on a protected server. Backup documentation should be maintained and kept in a separate location.

12.1.2. Network Topology Diagrams

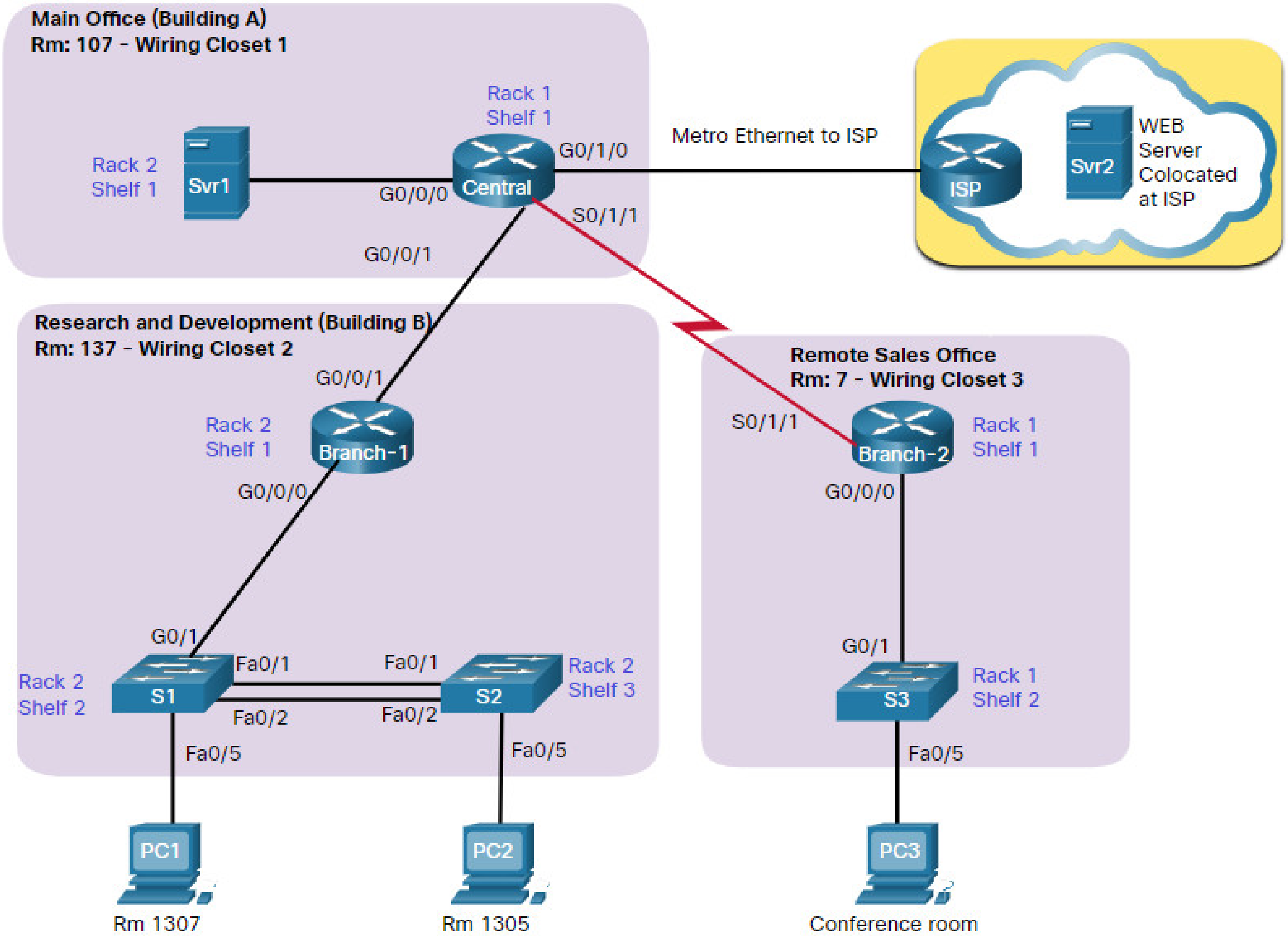
Network topology diagrams keep track of the location, function, and status of devices on the network. There are two types of network topology diagrams: the physical topology and the logical topology.

Click each button for an example and explanation of physical and logical topologies.

Physical Topology
A physical network topology shows the physical layout of the devices connected to the network. You need to know how devices are physically connected to troubleshoot physical layer problems. Information recorded on the physical topology typically includes the following:

- Device name
- Device location (address, room number, rack location)
- Interface and ports used
- Cable type

The figure shows a sample physical network topology diagram.



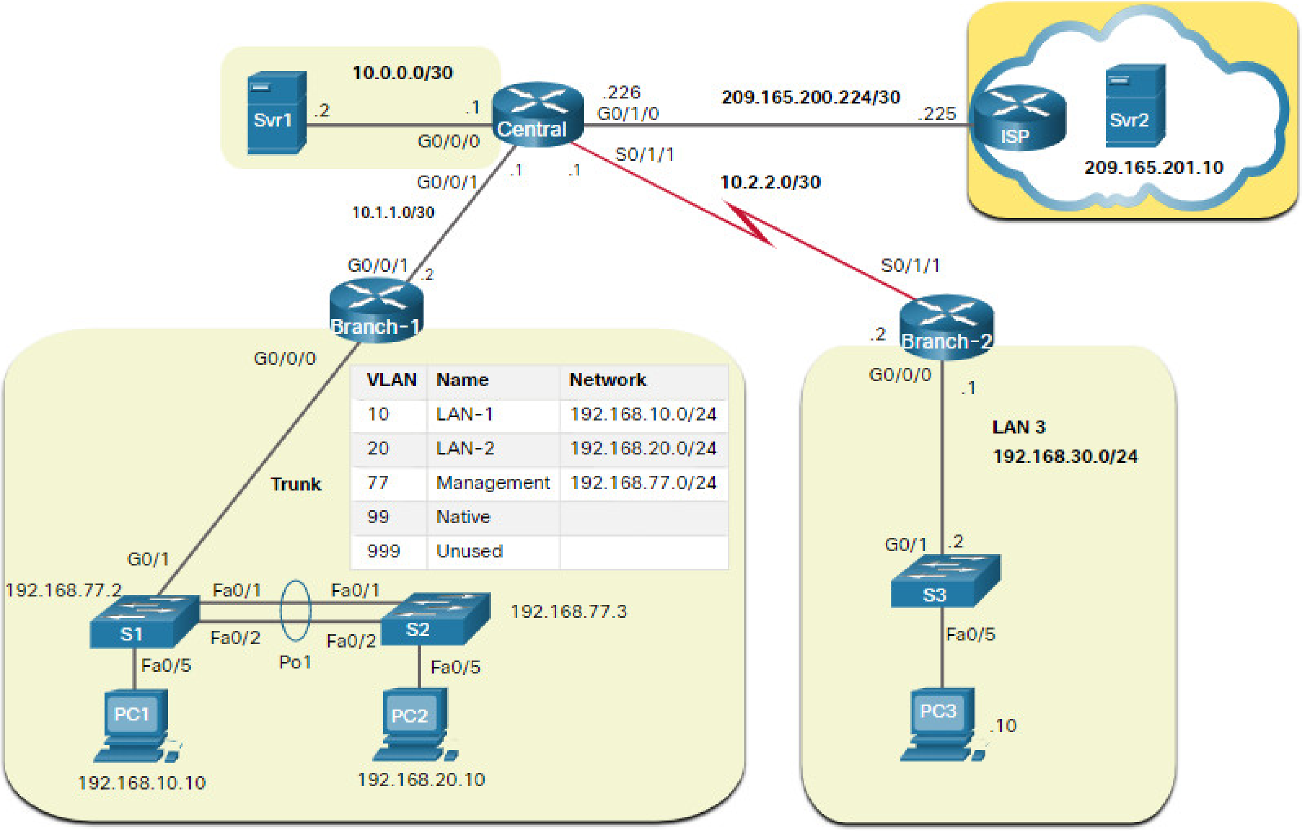
Logical IPv4 Topology

A logical network topology illustrates how devices are logically connected to the network. This refers to how devices transfer data across the network when communicating with other devices. Symbols are used to represent network components, such as routers, switches, servers, and hosts. Additionally, connections between multiple sites may be shown, but do not represent actual physical locations.

Information recorded on a logical network topology may include the following:

- Device identifiers
- IP addresses and prefix lengths
- Interface identifiers
- Routing protocols / static routes
- Layer 2 information (i.e., VLANs, trunks, EtherChannels)

The figure displays a sample logical IPv4 network topology.

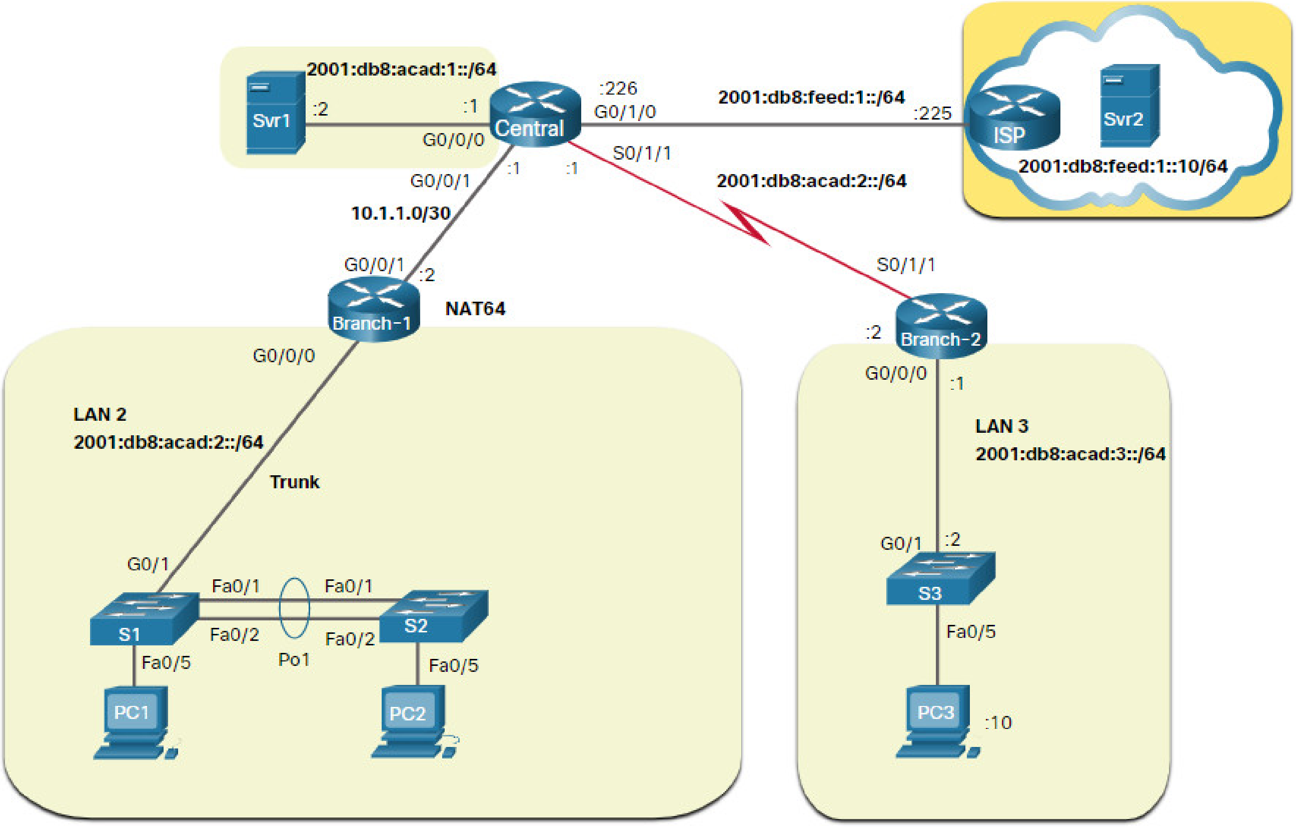


VLAN	Name	Network
10	LAN-1	192.168.10.0/24
20	LAN-2	192.168.20.0/24
77	Management	192.168.77.0/24
99	Native	
999	Unused	

Logical IPv6 Topology

Although IPv6 addresses could also be displayed in the same IPv4 logical topology, for the sake of clarity, we have created a separate logical IPv6 network topology.

The figure displays a sample IPv6 logical topology.



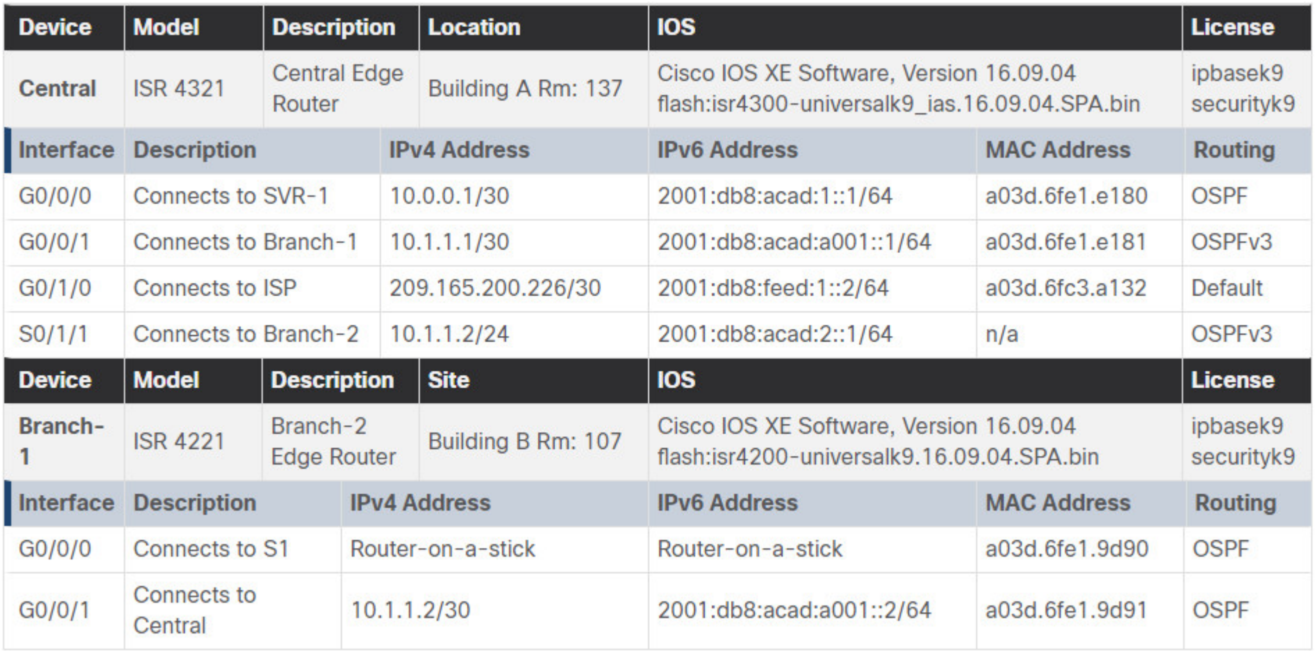
12.1.3. Network Device Documentation

Network device documentation should contain accurate, up-to-date records of the network hardware and software. Documentation should include all pertinent information about the network devices.

Many organizations create documents with tables or spreadsheets to capture relevant device information.

Click each button for examples of router, switch, and end device documentation.

Router Device Documentation
The table displays sample network device documentation for two interconnecting routers.

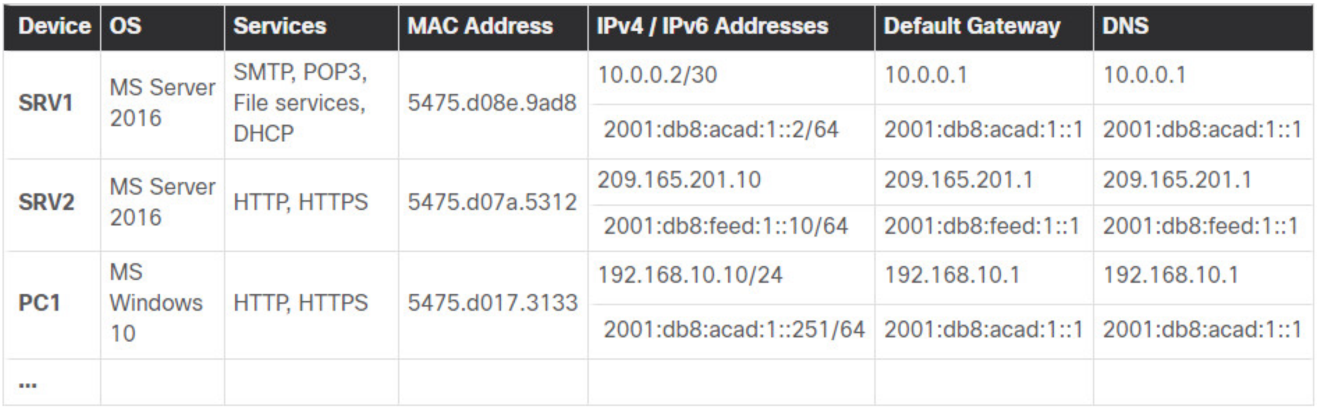


Device	Model	Description	Location	IOS	License
Central	ISR 4321	Central Edge Router	Building A Rm: 137	Cisco IOS XE Software, Version 16.09.04 flash:isr4300-universalk9_ias.16.09.04.SPA.bin	ipbasek9 securityk9
Interface	**Description**	**IPv4 Address**	**IPv6 Address**	**MAC Address**	**Routing**
G0/0/0	Connects to SVR-1	10.0.0.1/30	2001:db8:acad:1::1/64	a03d.6fe1.e180	OSPF
G0/0/1	Connects to Branch-1	10.1.1.1/30	2001:db8:acad:a001::1/64	a03d.6fe1.e181	OSPFv3
G0/1/0	Connects to ISP	209.165.200.226/30	2001:db8:feed:1::2/64	a03d.6fc3.a132	Default
S0/1/1	Connects to Branch-2	10.1.1.2/24	2001:db8:acad:2::1/64	n/a	OSPFv3
Device	**Model**	**Description**	**Site**	**IOS**	**License**
Branch-1	ISR 4221	Branch-2 Edge Router	Building B Rm: 107	Cisco IOS XE Software, Version 16.09.04 flash:isr4200-universalk9.16.09.04.SPA.bin	ipbasek9 securityk9
Interface	**Description**	**IPv4 Address**	**IPv6 Address**	**MAC Address**	**Routing**
G0/0/0	Connects to S1	Router-on-a-stick	Router-on-a-stick	a03d.6fe1.9d90	OSPF
G0/0/1	Connects to Central	10.1.1.2/30	2001:db8:acad:a001::2/64	a03d.6fe1.9d91	OSPF

End-system Documentation Files

End-system documentation focuses on the hardware and software used in servers, network management consoles, and user workstations. An incorrectly configured end-system can have a negative impact on the overall performance of a network. For this reason, having access to end-system device documentation can be very useful when troubleshooting.

This table displays a sample of information that could be recorded in an end-system device document.



Device	OS	Services	MAC Address	IPv4 / IPv6 Addresses	Default Gateway	DNS
SRV1	MS Server 2016	SMTP, POP3, File services, DHCP	5475.d08e.9ad8	10.0.0.2/30 2001:db8:acad:1::2/64	10.0.0.1 2001:db8:acad:1::1	10.0.0.1 2001:db8:acad:1::1
SRV2	MS Server 2016	HTTP, HTTPS	5475.d07a.5312	209.165.201.10 2001:db8:feed:1::10/64	209.165.201.1 2001:db8:feed:1::1	209.165.201.1 2001:db8:feed:1::1
PC1	MS Windows 10	HTTP, HTTPS	5475.d017.3133	192.168.10.10/24 2001:db8:acad:1::251/64	192.168.10.1 2001:db8:acad:1::1	192.168.10.1 2001:db8:acad:1::1
...						

12.1.4. Establish a Network Baseline

The purpose of network monitoring is to watch network performance in comparison to a predetermined baseline. A baseline is used to establish normal network or system performance to determine the “personality” of a network under normal conditions.

Establishing a network performance baseline requires collecting performance data from the ports and devices that are essential to network operation.

A network baseline should answer the following questions:

- How does the network perform during a normal or average day?
- Where are the most errors occurring?
- What part of the network is most heavily used?
- What part of the network is least used?
- Which devices should be monitored and what alert thresholds should be set?
- Can the network meet the identified policies?

Measuring the initial performance and availability of critical network devices and links allows a network administrator to determine the difference between abnormal behavior and proper network performance, as the network grows, or traffic patterns change. The baseline also provides insight into whether the current network design can meet business requirements. Without a baseline, no standard exists to measure the optimum nature of network traffic and congestion levels.

Analysis after an initial baseline also tends to reveal hidden problems. The collected data shows the true nature of congestion or potential congestion in a network. It may also reveal areas in the network that are underutilized, and quite often can lead to network redesign efforts, based on quality and capacity observations.

The initial network performance baseline sets the stage for measuring the effects of network changes and subsequent troubleshooting efforts. Therefore, it is important to plan for it carefully.

12.1.5. Step 1 – Determine What Types of Data to Collect

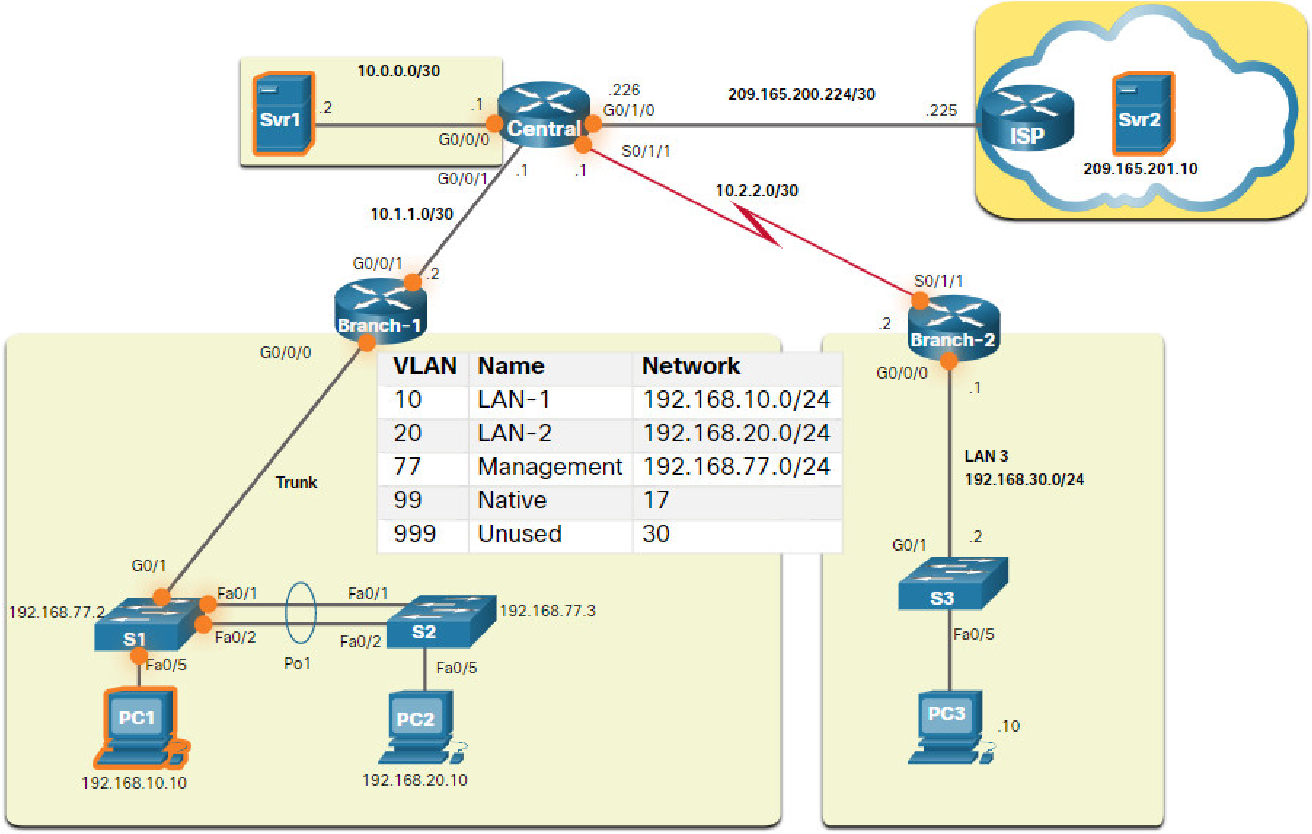
When conducting the initial baseline, start by selecting a few variables that represent the defined policies. If too many data points are selected, the amount of data can be overwhelming, making analysis of the collected data difficult. Start out simply and fine-tune along the way. Some good starting variables are interface utilization and CPU utilization.

12.1.6. Step 2 – Identify Devices and Ports of Interest

Use the network topology to identify those devices and ports for which performance data should be measured. Devices and ports of interest include the following:

- Network device ports that connect to other network devices
- Servers
- Key users
- Anything else considered critical to operations

A logical network topology can be useful in identifying key devices and ports to monitor. In the figure, the network administrator has highlighted the devices and ports of interest to monitor during the baseline test.



VLAN	Name	Network
10	LAN-1	192.168.10.0/24
20	LAN-2	192.168.20.0/24
77	Management	192.168.77.0/24
99	Native	17
999	Unused	30

The devices of interest include PC1 (the Admin terminal), and the two servers (i.e., Srv1 and Svr2). The ports of interest typically include router interfaces and key ports on switches.

By shortening the list of ports that are polled, the results are concise, and the network management load is minimized. Remember that an interface on a router or switch can be a virtual interface, such as a switch virtual interface (SVI).

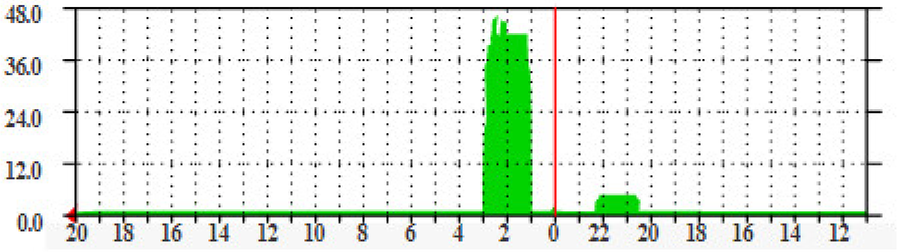
12.1.7. Step 3 – Determine the Baseline Duration

The length of time and the baseline information being gathered must be long enough to determine a “normal” picture of the network. It is important that daily trends of network traffic are monitored. It is also important to monitor for trends that occur over a longer period, such as weekly or monthly. For this reason, when capturing data for analysis, the period specified should be, at a minimum, seven days long.

The figure displays examples of several screenshots of CPU utilization trends captured over a daily, weekly, monthly, and yearly period.

CPU Utilization

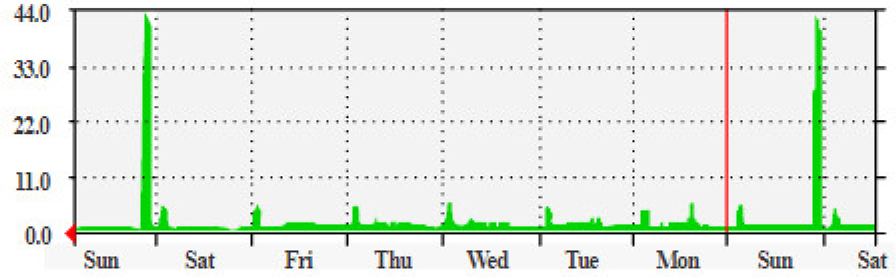
Daily Graph (5 minute Average)



Max Load: **46%** Average Load: **3%** Current Load: **1%**

CPU Utilization

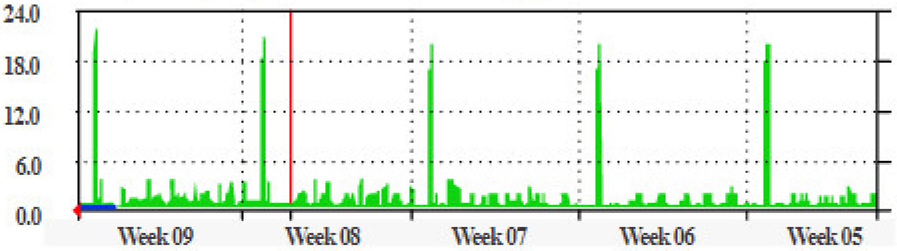
Weekly Graph (2 Hour Average)



Max Load: **43%** Average Load: **2%** Current Load: **1%**

CPU Utilization

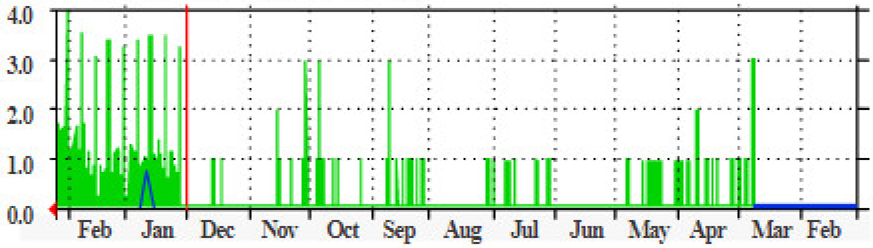
Monthly Graph (30 Minute Average)



Max Load: **43%** Average Load: **2%** Current Load: **1%**

CPU Utilization

Yearly Graph (1 day Average)



Max Load: **43%** Average Load: **0%** Current Load: **1%**

In this example, notice that the work week trends are too short to reveal the recurring utilization surge every weekend on Saturday evening, when a database backup operation consumes network bandwidth. This recurring pattern is revealed in the monthly trend. A yearly trend as shown in the example may be too long of a duration to provide meaningful baseline performance details. However, it may help identify long term patterns which should be analyzed further.

Typically, a baseline needs to last no more than six weeks, unless specific long-term trends need to be measured. Generally, a two-to-four-week baseline is adequate.

Baseline measurements should not be performed during times of unique traffic patterns, because the data would provide an inaccurate picture of normal network operations. Conduct an annual analysis of the entire network, or baseline different sections of the network on a rotating basis. Analysis must be conducted regularly to understand how the network is affected by growth and other changes.

12.1.8. Data Measurement

When documenting the network, it is often necessary to gather information directly from routers and switches. Obvious useful network documentation commands include **ping**, **traceroute**, and **telnet,** as well as **show** commands.

The table lists some of the most common Cisco IOS commands used for data collection.

Command	Description
`show version`	Displays uptime, version information for device software and hardware.

`show ip interface [brief]`
`show ipv6 interface [brief]`
	• Displays all the configuration options that are set on an interface.
	• Use the **brief** keyword to only display up/down status of IP interfaces and the IP address of each interface.

`show interfaces`	• Displays detailed output for each interface. • To display detailed output for only a single interface, include the interface type and number in the command (e.g. Gigabit Ethernet 0/0/0).

`show ip route`
`show ipv6 route`
	• Displays the routing table content listing directly connected networks and learned remote networks.
	• Append **static**, **eigrp**, or **ospf** to display those routes only.

Command	Description
`show cdp neighbors detail`	Displays detailed information about directly connected Cisco neighbor devices.

`show arp`
`show ipv6 neighbors`
	Displays the contents of the ARP table (IPv4) and the neighbor table (IPv6).

`show running-config`	Displays current configuration.
`show vlan`	Displays the status of VLANs on a switch.
`show port`	Displays the status of ports on a switch.
`show tech-support`	• This command is useful for collecting a large amount of information about the device for troubleshooting purposes. • It executes multiple show commands which can be provided to technical support representatives when reporting a problem

Manual data collection using **show** commands on individual network devices is extremely time consuming and is not a scalable solution. Manual collection of data should be reserved for smaller networks or limited to mission-critical network devices. For simpler network designs, baseline tasks typically use a combination of manual data collection and simple network protocol inspectors.

Sophisticated network management software is typically used to baseline large and complex networks. These software packages enable administrators to automatically create and review reports, compare current performance levels with historical observations, automatically identify performance problems, and create alerts for applications that do not provide expected levels of service.

Establishing an initial baseline or conducting a performance-monitoring analysis may require many hours or days to accurately reflect network performance. Network management software or protocol inspectors and sniffers often run continuously over the course of the data collection process.

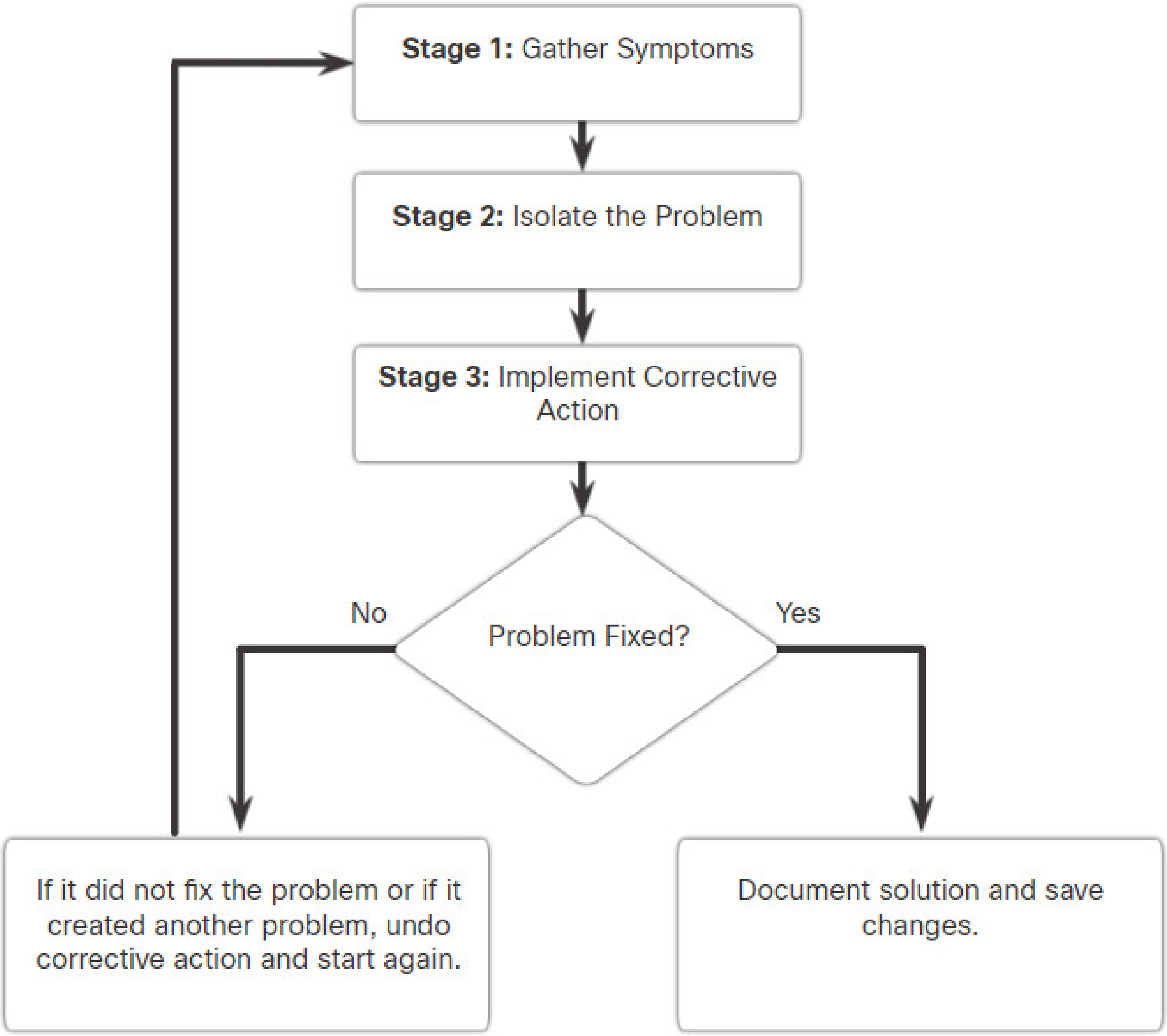
12.2. Troubleshooting Process

12.2.1. General Troubleshooting Procedures

Troubleshooting can be time consuming because networks differ, problems differ, and troubleshooting experience varies. However, experienced administrators know that using a structured troubleshooting method will shorten overall troubleshooting time.

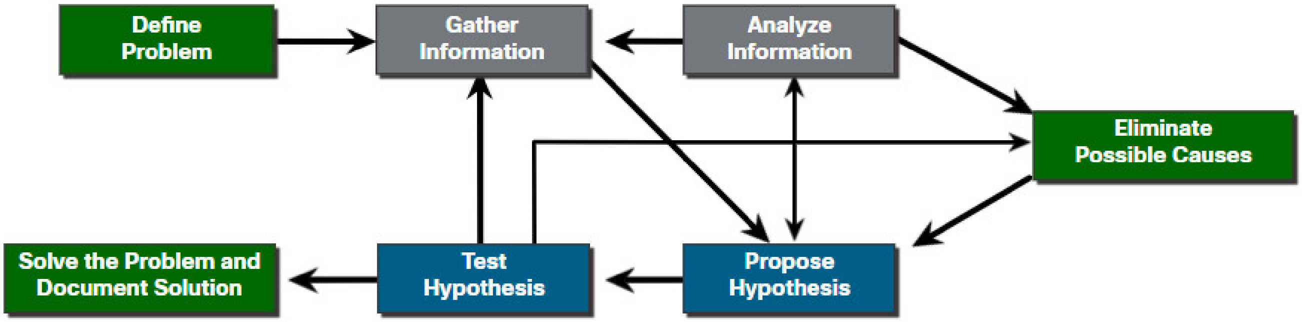
Therefore, the troubleshooting process should be guided by structured methods. This requires well defined and documented troubleshooting procedures to minimize wasted time associated with erratic hit-and-miss troubleshooting. However, these methods are not static. The troubleshooting steps taken to solve a problem are not always the same or executed in the exact same order.

There are several troubleshooting processes that can be used to solve a problem. The figure displays the logic flowchart of a simplified three-stage troubleshooting process. However, a more detailed process may be more helpful to solve a network problem.


Stage 1: Gather Symptoms
Stage 2: Isolate the Problem
Stage 3: Implement Corrective Action
Problem Fixed?
No
Yes
If it did not fix the problem or if it created another problem, undo corrective action and start again.
Document solution and save changes.

12.2.2. Seven-Step Troubleshooting Process

The figure displays a more detailed seven-step troubleshooting process. Notice how some steps interconnect. This is because, some technicians may be able to jump between steps based on their level of experience.



Click each button for a detailed description of the steps to solve a network problem.

Define the Problem
The goal of this stage is to verify that there is a problem and then properly define what the problem is. Problems are usually identified by a symptom (e.g., the network is slow or has stopped working). Network symptoms may appear in many different forms, including alerts from the network management system, console messages, and user complaints.

While gathering symptoms, it is important to ask questions and investigate the issue in order to localize the problem to a smaller range of possibilities. For example, is the problem restricted to a single device, a group of devices, or an entire subnet or network of devices?

In an organization, problems are typically assigned to network technicians as trouble tickets. These tickets are created using trouble ticketing software that tracks the progress of each ticket. Trouble ticketing software may also include a self-service user portal to submit tickets, access to a searchable trouble tickets knowledge base, remote control capabilities to solve end-user issues, and more.

Gather Information
In this step, targets (i.e., hosts, devices) to be investigated must be identified, access to the target devices must be obtained, and information gathered. During this step, the technician may gather and document more symptoms, depending on the characteristics that are identified.

If the problem is outside the boundary of the organization’s control (e.g., lost internet connectivity outside of the autonomous system), contact an administrator for the external system before gathering additional network symptoms.

Eliminate Possible Causes

If multiple causes are identified, then the list must be reduced by progressively eliminating possible causes to eventually identify the most probable cause. Troubleshooting experience is extremely valuable to quickly eliminate causes and identify the most probable cause.

Test Hypothesis
Before testing the solution, it is important to assess the impact and urgency of the problem. For instance, could the solution have an adverse effect on other systems or processes? The severity of the problem should be weighed against the impact of the solution. For example, if a critical server or router must be offline for a significant amount of time, it may be better to wait until the end of the workday to implement the fix. Sometimes, a workaround can be created until the actual problem is resolved.

Create a rollback plan identifying how to quickly reverse a solution. This may prove to be necessary if the solution fails.

Implement the solution and verify that it has solved the problem. Sometimes a solution introduces an unexpected problem. Therefore, it is important that a solution be thoroughly verified before proceeding to the next step.

If the solution fails, the attempted solution is documented and the changes are removed. The technician must now go back to the Gathering Information step and isolate the issue.

Solve the problem
When the problem is solved, inform the users and anyone involved in the troubleshooting process that the problem has been resolved. Other IT team members should be informed of the solution. Appropriate documentation of the cause and the fix will assist other support technicians in preventing and solving similar problems in the future.

12.2.3. Question End Users

Many network problems are initially reported by an end user. However, the information provided is often vague or misleading. For example, users often report problems such as “the network is down”, “I cannot access my email”, or “my computer is slow”.

In most cases, additional information is required to fully understand a problem. This usually involves interacting with the affected user to discover the “who”, “what”, and “when” of the problem.

The following recommendations should be employed when communicate with user:

- Speak at a technical level they can understand and avoid using complex terminology.
- Always listen or read carefully what the user is saying. Taking notes can be helpful when documenting a complex problem.

- Always be considerate and empathize with users while letting them know you will help them solve their problem. Users reporting a problem may be under stress and anxious to resolve the problem as quickly as possible.

When interviewing the user, guide the conversation and use effective questioning techniques to quickly ascertain the problem. For instance, use open questions (i.e., requires detailed response) and closed questions (i.e., yes, no, or single word answers) to discover important facts about the network problem.

The table provides some questioning guidelines and sample open ended end-user questions.

When done interviewing the user, repeat your understanding of the problem to the user to ensure that you both agree on the problem being reported.

Guidelines	Example Open Ended End-User Questions
Ask pertinent questions.	• What does not work? • What exactly is the problem? • What are you trying to accomplish?
Determine the scope of the problem.	• Who does this issue affect? Is it just you or others? • What device is this happening on?
Determine when the problem occurred / occurs.	• When exactly does the problem occur? • When was the problem first noticed? • Were there any error message(s) displayed?
Determine if the problem is constant or intermittent.	• Can you reproduce the problem? • Can you send me a screenshot or video of the problem?
Determine if anything has changed.	What has changed since the last time it did work?
Use questions to eliminate or discover possible problems.	• What works? • What does not work?

12.2.4. Gather Information

To gather symptoms from suspected networking device, use Cisco IOS commands and other tools such as packet captures and device logs.

The table describes common Cisco IOS commands used to gather the symptoms of a network problem.

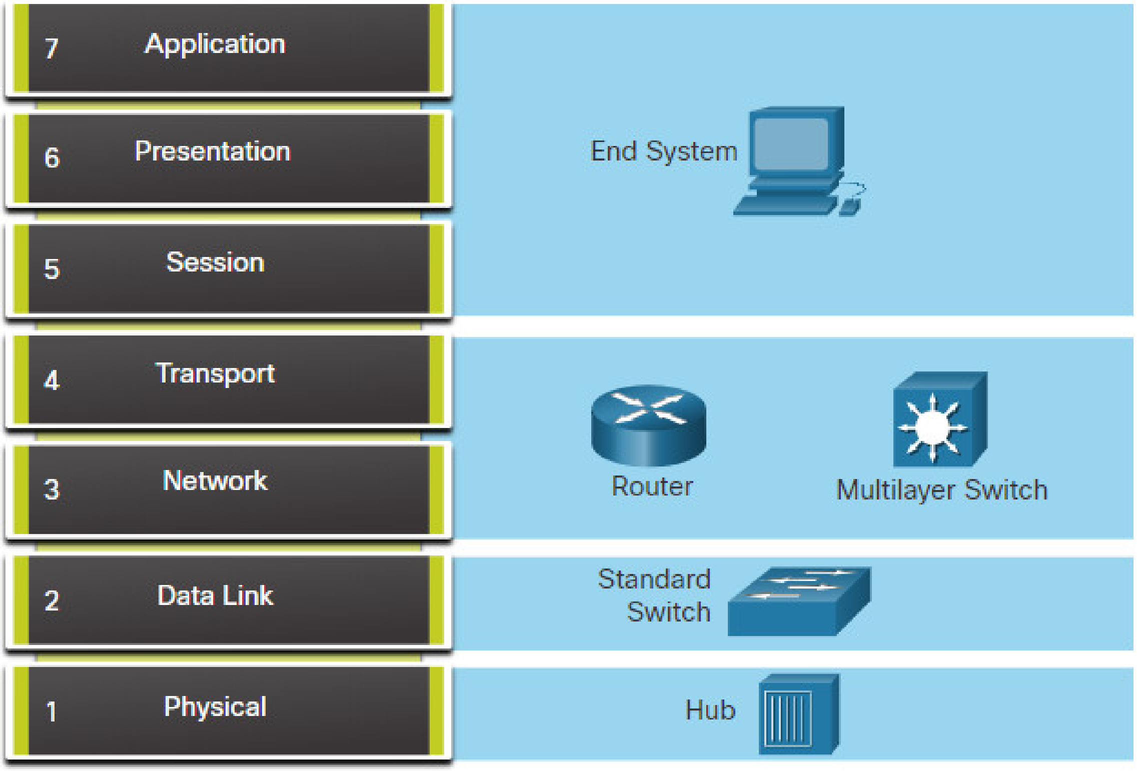
Command	Description
ping {*host* | *ip-address*}	• Sends an echo request packet to an address, then waits for a reply • The *host* or *ip-address* variable is the IP alias or IP address of the target system
traceroute *destination*	• Identifies the path a packet takes through the networks • The *destination* variable is the hostname or IP address of the target system
telnet {*host* | *ip-address*}	• Connects to an IP address using the Telnet application • Use SSH whenever possible instead of Telnet
ssh -l *user-id ip-address*	• Connects to an IP address using SSH • SSH is more secure than Telnet
show ip interface brief **show ipv6 interface brief**	• Displays a summary status of all interfaces on a device • Useful for quickly identifying IP addressing on all interfaces.
show ip route **show ipv6 route**	Displays the current IPv4 and IPv6 routing tables, which contains the routes to all known network destinations
show protocols	Displays the configured protocols and shows the global and interface-specific status of any configured Layer 3 protocol
debug	Displays a list of options for enabling or disabling debugging events

Note: Although the **debug** command is an important tool for gathering symptoms, it generates a large amount of console message traffic and the performance of a network device can be noticeably affected. If the **debug** must be performed during normal working hours, warn network users that a troubleshooting effort is underway, and that network performance may be affected. Remember to disable debugging when you are done.

12.2.5. Troubleshooting with Layered Models

The OSI and TCP/IP models can be applied to isolate network problems when troubleshooting. For example, if the symptoms suggest a physical connection problem, the network technician can focus on troubleshooting the circuit that operates at the physical layer.

The figure shows some common devices and the OSI layers that must be examined during the troubleshooting process for that device.



Notice that routers and multilayer switches are shown at Layer 4, the transport layer. Although routers and multilayer switches usually make forwarding decisions at Layer 3, ACLs on these devices can be used to make filtering decisions using Layer 4 information.

12.2.6. Structured Troubleshooting Methods

There are several structured troubleshooting approaches that can be used. Which one to use will depend on the situation. Each approach has its advantages and disadvantages. This topic describes methods and provides guidelines for choosing the best method for a specific situation.

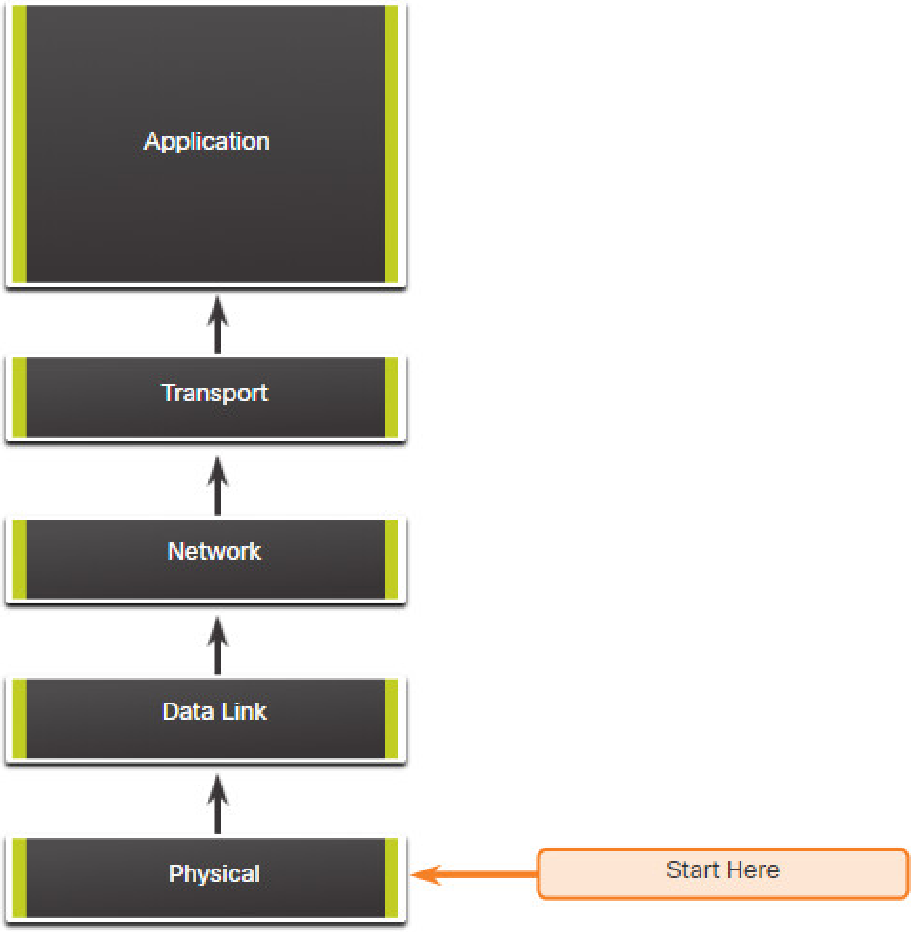
Click each button for a description of the different troubleshooting approaches that can be used.

Bottom-Up

In bottom-up troubleshooting, you start with the physical components of the network and move up through the layers of the OSI model until the cause of the problem is identified, as shown in the figure.

Bottom-up troubleshooting is a good approach to use when the problem is suspected to be a physical one. Most networking problems reside at the lower levels, so implementing the bottom-up approach is often effective.

The disadvantage with the bottom-up troubleshooting approach is it requires that you check every device and interface on the network until the possible cause of the problem is found. Remember that each conclusion and possibility must be documented so there can be a lot of paper work associated with this approach. A further challenge is to determine which devices to start examining first.



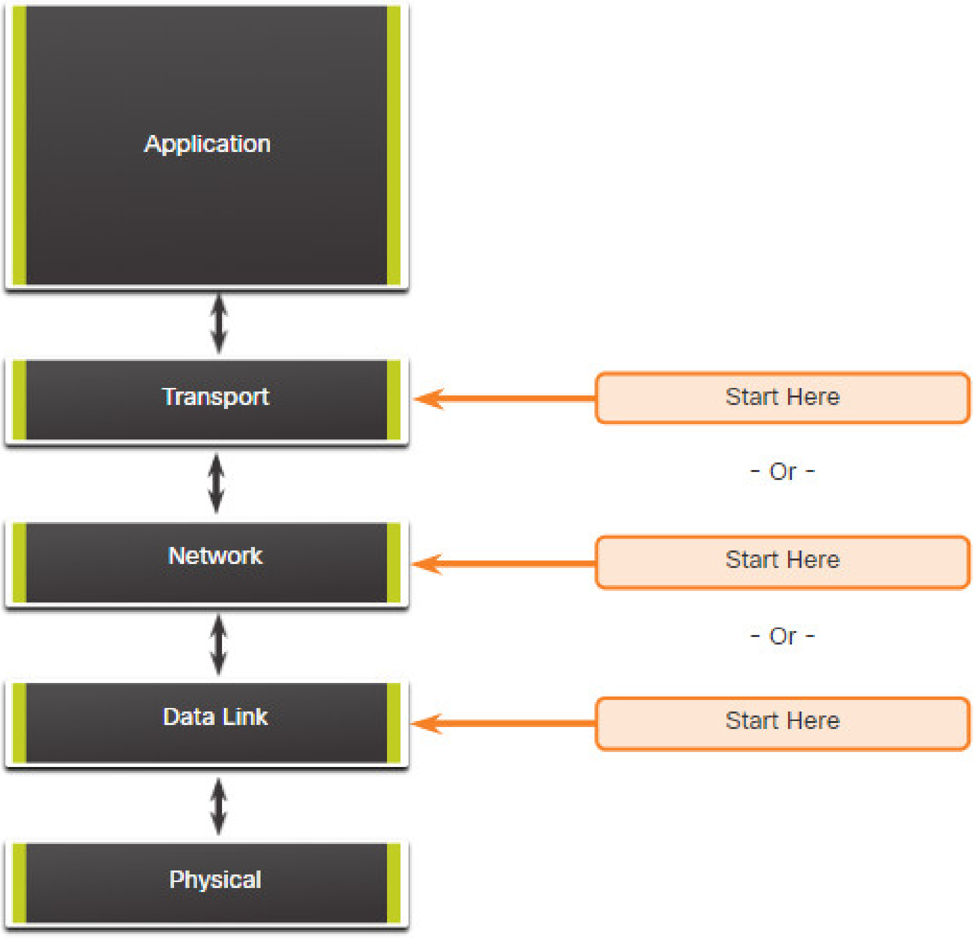
Divide-and-Conquer

The figure shows the divide-and-conquer approach to troubleshooting a networking problem.

The network administrator selects a layer and tests in both directions from that layer.

In divide-and-conquer troubleshooting, you start by collecting user experiences of the problem, document the symptoms and then, using that information, make an informed guess as to which OSI layer to start your investigation. When a layer is verified to be functioning properly, it can be assumed that the layers below it are functioning. The administrator can work up the OSI layers. If an OSI layer is not functioning properly, the administrator can work down the OSI layer model.

For example, if users cannot access the web server, but they can ping the server, then the problem is above Layer 3. If pinging the server is unsuccessful, then the problem is likely at a lower OSI layer.



Follow-the-Path

This is one of the most basic troubleshooting techniques. The approach first discovers the actual traffic path all the way from source to destination. The scope of troubleshooting is reduced to just the links and devices that are in the forwarding path. The objective is to eliminate the links and devices that are irrelevant to the troubleshooting task at hand. This approach usually complements one of the other approaches.

Comparison

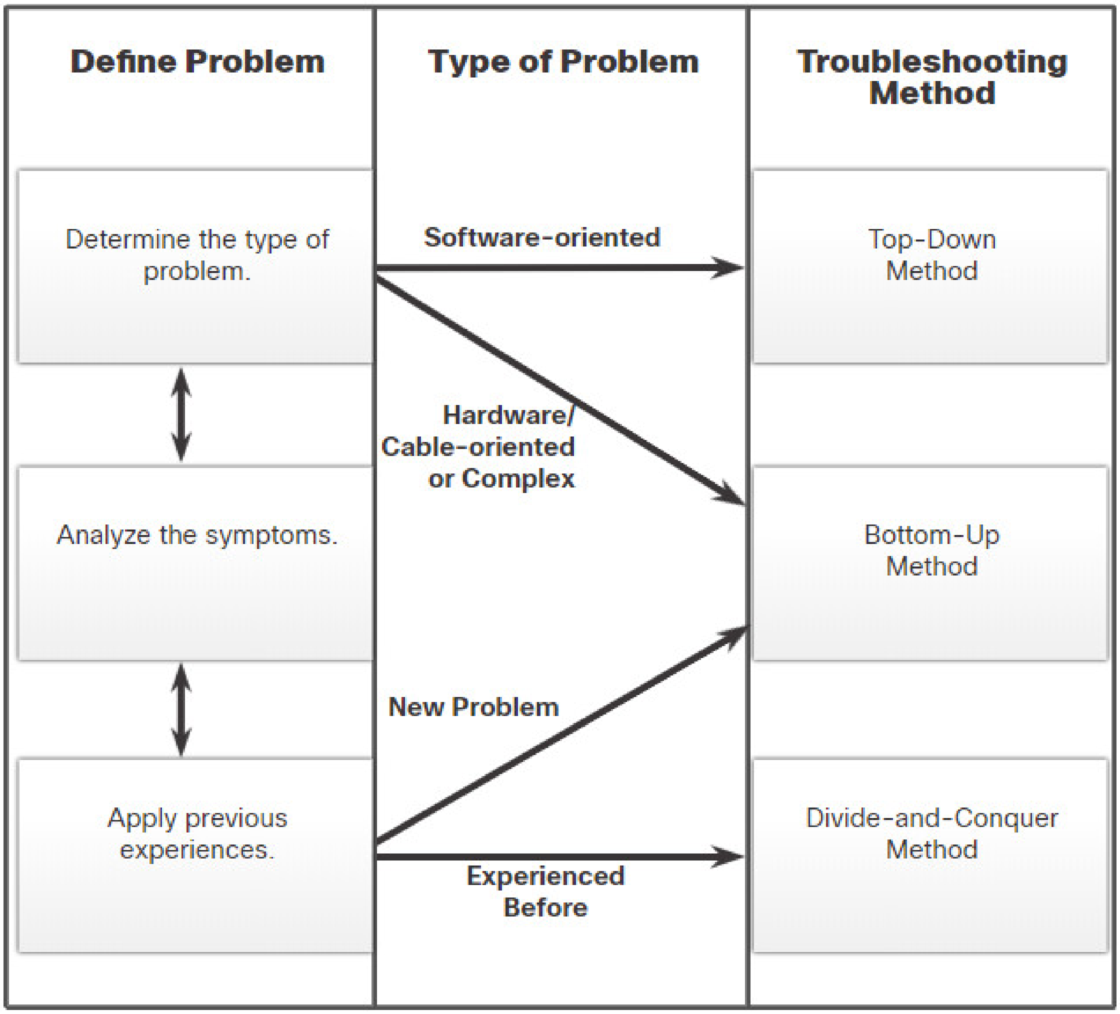
This approach is also called the spot-the-differences approach and attempts to resolve the problem by changing the nonoperational elements to be consistent with the working ones. You compare configurations, software versions, hardware, or other device properties, links, or processes between working and nonworking situations and spot significant differences between them.

The weakness of this method is that it might lead to a working solution, without clearly revealing the root cause of the problem.

12.2.7. Guidelines for Selecting a Troubleshooting Method

To quickly resolve network problems, take the time to select the most effective network troubleshooting method.

The figure illustrates which method could be used when a certain type of problem is discovered.



For instance, software problems are often solved using a top-down approach while hardware-based problem are solved using the bottom-up approach. New problems may be solved by an experienced technician using the divide-and-conquer method. Otherwise, the bottom-up approach may be used.

Troubleshooting is a skill that is developed by doing it. Every network problem you identify and solve gets added to your skill set.

12.3. Troubleshooting Tools

12.3.1. Software Troubleshooting Tools

As you know, networks are made up of software and hardware. Therefore, both software and hardware have their respective tools for troubleshooting. This topic discusses the troubleshooting tools available for both.

A wide variety of software and hardware tools are available to make troubleshooting easier. These tools may be used to gather and analyze symptoms of network problems. They often provide monitoring and reporting functions that can be used to establish the network baseline.

Click each button for a detailed description of common software troubleshooting tools.

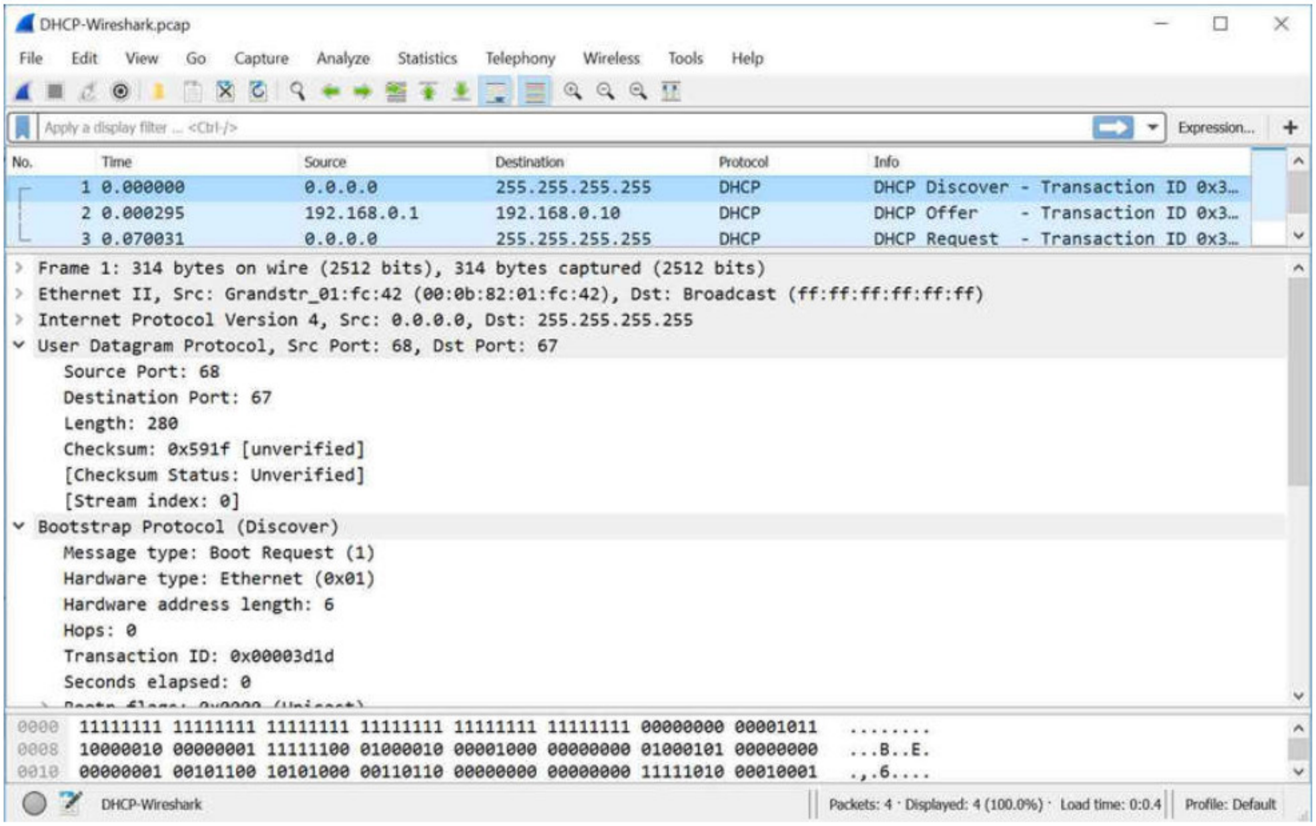
Network Management System Tools
Network management system (NMS) tools include device-level monitoring, configuration, and fault-management tools. These tools can be used to investigate and correct network problems. Network monitoring software graphically displays a physical view of network devices, allowing network managers to monitor remote devices continuously and automatically. Device management software provides dynamic device status, statistics, and configuration information for key network devices. Search the internet for “NMS Tools” for more information.

Knowledge Bases
Online network device vendor knowledge bases have become indispensable sources of information. When vendor-based knowledge bases are combined with internet search engines, a network administrator has access to a vast pool of experience-based information.

For example, the **Cisco Tools & Resources** page can be found at http://www.cisco.com under the **Support** menu. This page provides tools that can be used for Cisco hardware and software.

12.3.2. Protocol Analyzers

Protocol analyzers can investigate packet content while flowing through the network. A protocol analyzer decodes the various protocol layers in a recorded frame and presents this information in a relatively easy to use format. The figure shows a screen capture of the Wireshark protocol analyzer.



```
No.  Time        Source        Destination       Protocol  Info
  1 0.000000    0.0.0.0       255.255.255.255   DHCP      DHCP Discover - Transaction ID 0x3…
  2 0.000295    192.168.0.1   192.168.0.10      DHCP      DHCP Offer    - Transaction ID 0x3…
  3 0.070031    0.0.0.0       255.255.255.255   DHCP      DHCP Request  - Transaction ID 0x3…
```

```
> Frame 1: 314 bytes on wire (2512 bits), 314 bytes captured (2512 bits)
> Ethernet II, Src: Grandstr_01:fc:42 (00:0b:82:01:fc:42), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
v User Datagram Protocol, Src Port: 68, Dst Port: 67
    Source Port: 68
    Destination Port: 67
    Length: 280
    Checksum: 0x591f [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
v Bootstrap Protocol (Discover)
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x00003d1d
    Seconds elapsed: 0
  > Bootp flags: 0x0000 (Unicast)
```

```
0000  11111111 11111111 11111111 11111111 11111111 11111111 00000000 00001011   ........
0008  10000010 00000001 11111100 01000010 00001000 00000000 01000101 00000000   ...B..E.
0010  00000001 00101100 10101000 00110110 00000000 00000000 11111010 00010001   .,.6....
```

The information displayed by a protocol analyzer includes the physical layer bit data, data link layer information, protocols, and descriptions for each frame. Most protocol analyzers can filter traffic that meets certain criteria so that all traffic to and from a device can be captured. Protocol analyzers such as Wireshark can help troubleshoot network performance problems. It is important to have both a good understanding of TCP/IP and how to use a protocol analyzer to inspect information at each TCP/IP layer.

12.3.3. Hardware Troubleshooting Tools

There are multiple types of hardware troubleshooting tools.

Click each button for a detailed description of common hardware troubleshooting tools.

Digital Multimeters
Digital multimeters (DMMs), such as the Fluke 179 shown in the figure, are test instruments that are used to directly measure electrical values of voltage, current, and resistance.

In network troubleshooting, most tests that would need a multimeter involve checking power supply voltage levels and verifying that network devices are receiving power.

Cable Testers

Cable testers are specialized, handheld devices designed for testing the various types of data communication cabling. The figure displays the Fluke LinkRunner AT Network Auto-Tester.

Cable testers can be used to detect broken wires, crossed-over wiring, shorted connections, and improperly paired connections. These devices can be inexpensive continuity testers, moderately priced data cabling testers, or expensive time-domain reflectometers (TDRs). TDRs are used to pinpoint the distance to a break in a cable. These devices send signals along the cable and wait for them to be reflected. The time between sending the signal and receiving it back is converted into a distance measurement. The TDR function is normally packaged with data cabling testers. TDRs used to test fiber-optic cables are known as optical time-domain reflectometers (OTDRs).

Portable Network Analyzers

Portable devices like the Fluke OptiView, shown in the figure, are used for troubleshooting switched networks and VLANs.

By plugging the network analyzer in anywhere on the network, a network engineer can see the switch port to which the device is connected, and the average and peak utilization. The analyzer can also be used to discover VLAN configuration, identify top network talkers (hosts generating the most traffic), analyze network traffic, and view interface details. The device can typically output to a PC that has network monitoring software installed for further analysis and troubleshooting.

12.3.4. Syslog Server as a Troubleshooting Tool

Syslog is a simple protocol used by an IP device known as a syslog client, to send text-based log messages to another IP device, the syslog server. Syslog is currently defined in RFC 5424.

Implementing a logging facility is an important part of network security and for network troubleshooting. Cisco devices can log information regarding configuration changes, ACL violations, interface status, and many other types of events. Cisco devices can send log messages to several different facilities. Event messages can be sent to one or more of the following:

- **Console** – Console logging is on by default. Messages log to the console and can be viewed when modifying or testing the router or switch using terminal emulation software while connected to the console port of the network device.
- **Terminal lines** – Enabled EXEC sessions can be configured to receive log messages on any terminal lines. Like console logging, this type of logging is not stored by the network device and, therefore, is only valuable to the user on that line.
- **Buffered logging** – Buffered logging is a little more useful as a troubleshooting tool because log messages are stored in memory for a time. However, log messages are cleared when the device is rebooted.

- **SNMP traps** – Certain thresholds can be preconfigured on routers and other devices. Router events, such as exceeding a threshold, can be processed by the router and forwarded as SNMP traps to an external SNMP network management station. SNMP traps are a viable security logging facility but require the configuration and maintenance of an SNMP system.
- **Syslog** – Cisco routers and switches can be configured to forward log messages to an external syslog service. This service can reside on any number of servers or workstations, including Microsoft Windows and Linux-based systems. Syslog is the most popular message logging facility, because it provides long-term log storage capabilities and a central location for all router messages.

Cisco IOS log messages fall into one of eight levels, as shown in the table.

	Level	Keyword	Description	Definition
Highest Level	0	Emergencies	System is unusable	LOG_EMERG
	1	Alerts	Immediate action is needed	LOG_ALERT
	2	Critical	Critical conditions exist	LOG_CRIT
	3	Errors	Error conditions exist	LOG_ERR
	4	Warnings	Warning conditions exist	LOG_WARNING
Lowest Level	5	Notifications	Normal (but significant) condition	LOG_NOTICE
	6	Informational	Informational messages only	LOG_NFO
	7	Debugging	Debugging messages	LOG_DEBUG

The lower the level number, the higher the severity level. By default, all messages from level 0 to 7 are logged to the console. While the ability to view logs on a central syslog server is helpful in troubleshooting, sifting through a large amount of data can be an overwhelming task. The **logging trap** *level* command limits messages logged to the syslog server based on severity. The level is the name or number of the severity level. Only messages equal to or numerically lower than the specified level are logged.

In the command output, system messages from level 0 (emergencies) to 5 (notifications) are sent to the syslog server at 209.165.200.225.

```
R1(config)# logging host 209.165.200.225
R1(config)# logging trap notifications
R1(config)# logging on
R1(config)#
```

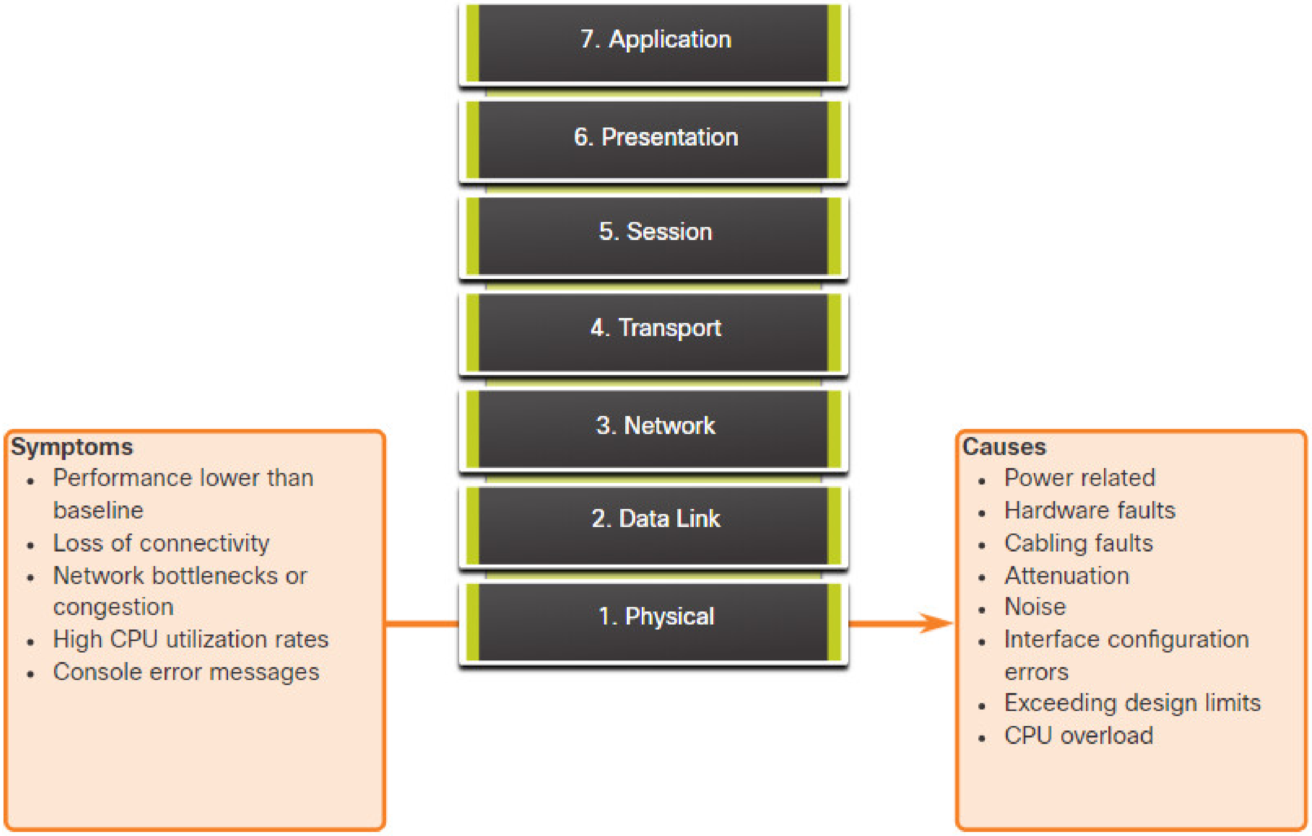
12.4. Symptoms and Causes of Network Problems

12.4.1. Physical Layer Troubleshooting

Now that you have your documentation, some knowledge of troubleshooting methods and the software and hardware tools to use to diagnose problems, you are ready to start troubleshooting! This topic covers the most common issues that you will find when troubleshooting a network.

Issues on a network often present as performance problems. Performance problems mean that there is a difference between the expected behavior and the observed behavior, and the system is not functioning as could be reasonably expected. Failures and suboptimal conditions at the physical layer not only inconvenience users but can impact the productivity of the entire company. Networks that experience these kinds of conditions usually shut down. Because the upper layers of the OSI model depend on the physical layer to function, a network administrator must have the ability to effectively isolate and correct problems at this layer.

The figure summarizes the symptoms and causes of physical layer network problems.



Symptoms

- Performance lower than baseline
- Loss of connectivity
- Network bottlenecks or congestion
- High CPU utilization rates
- Console error messages

Causes

- Power related
- Hardware faults
- Cabling faults
- Attenuation
- Noise
- Interface configuration errors
- Exceeding design limits
- CPU overload

The table lists common symptoms of physical layer network problems.

Symptom	Description

Symptom	Description
Performance lower than baseline	• Requires previous baselines for comparison. • The most common reasons for slow or poor performance include overloaded or underpowered servers, unsuitable switch or router configurations, traffic congestion on a low-capacity link, and chronic frame loss.
Loss of connectivity	• Loss of connectivity could be due to a failed or disconnected cable. • Can be verified using a simple ping test. • Intermittent connectivity loss can indicate a loose or oxidized connection.
Network bottlenecks or congestion	• If a router, interface, or cable fails, routing protocols may redirect traffic to other routes that are not designed to carry the extra capacity. • This can result in congestion or bottlenecks in parts of the network.
High CPU utilization rates	• High CPU utilization rates are a symptom that a device, such as a router, switch, or server, is operating at or exceeding its design limits. • If not addressed quickly, CPU overloading can cause a device to shut down or fail.
Console error messages	• Error messages reported on the device console could indicate a physical layer problem. • Console messages should be logged to a central syslog server.

The next table lists issues that commonly cause network problems at the physical layer.

Problem Cause	Description
Power-related	• This is the most fundamental reason for network failure. • Check the operation of the fans and ensure that the chassis intake and exhaust vents are clear. • If other nearby units have also powered down, suspect a power failure at the main power supply.

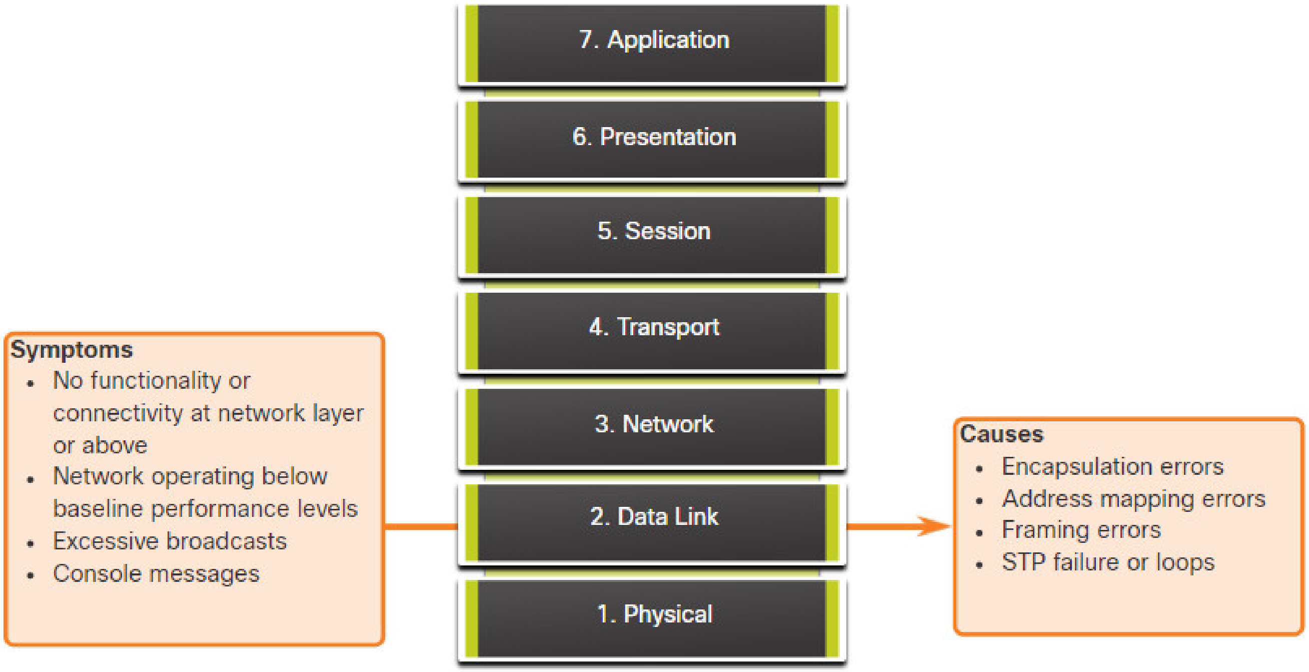
Problem Cause	Description
Hardware faults	• Faulty network interface cards (NICs) can be the cause of network transmission errors due to late collisions, short frames, and jabber. • Jabber is often defined as the condition in which a network device continually transmits random, meaningless data onto the network. • Other likely causes of jabber are faulty or corrupt NIC driver files, bad cabling, or grounding problems.
Cabling faults	• Many problems can be corrected by simply reseating cables that have become partially disconnected. • When performing a physical inspection, look for damaged cables, improper cable types, and poorly crimped RJ-45 connectors. • Suspect cables should be tested or exchanged with a known functioning cable.
Attenuation	• Attenuation can be caused if a cable length exceeds the design limit for the media, or when there is a poor connection resulting from a loose cable, or dirty or oxidized contacts. • If attenuation is severe, the receiving device cannot always successfully distinguish one bit in the data stream from another bit.
Noise	• Local electromagnetic interference (EMI) is commonly known as noise. • Noise can be generated by many sources, such as FM radio stations, police radio, building security, and avionics for automated landing, crosstalk (noise induced by other cables in the same pathway or adjacent cables), nearby electric cables, devices with large electric motors, or anything that includes a transmitter more powerful than a cell phone.
Interface configuration errors	• Many things can be misconfigured on an interface to cause it to go down, such as incorrect clock rate, incorrect clock source, and interface not being turned on. • This causes a loss of connectivity with attached network segments.
Exceeding design limits	• A component may be operating sub-optimally at the physical layer because it is being utilized beyond specifications or configured capacity. • When troubleshooting this type of problem, it becomes evident that resources for the device are operating at or near the maximum capacity and there is an increase in the number of interface errors.

Problem Cause	Description
CPU overload	• Symptoms include processes with high CPU utilization percentages, input queue drops, slow performance, SNMP timeouts, no remote access, or services such as DHCP, Telnet, and ping are slow or fail to respond. • On a switch the following could occur: spanning tree reconvergence, EtherChannel links bounce, UDLD flapping, IP SLAs failures. • For routers, there could be no routing updates, route flapping, or HSRP flapping. • One of the causes of CPU overload in a router or switch is high traffic. • If one or more interfaces are regularly overloaded with traffic, consider redesigning the traffic flow in the network or upgrading the hardware.

12.4.2. Data Link Layer Troubleshooting

Troubleshooting Layer 2 problems can be a challenging process. The configuration and operation of these protocols are critical to creating a functional, well-tuned network. Layer 2 problems cause specific symptoms that, when recognized, will help identify the problem quickly.

The figure summarizes the symptoms and causes of data link layer network problems.



The table lists common symptoms of data link layer network problems.

Symptom	Description
No functionality or connectivity at the network layer or above	Some Layer 2 problems can stop the exchange of frames across a link, while others only cause network performance to degrade.
Network is operating below baseline performance levels	• There are two distinct types of suboptimal Layer 2 operation that can occur in a network. • First, the frames take a suboptimal path to their destination but do arrive causing the network to experience unexpected high-bandwidth usage on links. • Second, some frames are dropped as identified through error counter statistics and console error messages that appear on the switch or router. • An extended or continuous ping can help reveal if frames are being dropped.
Excessive broadcasts	• Operating systems use broadcasts and multicasts extensively to discover network services and other hosts. • Generally, excessive broadcasts are the result of a poorly programmed or configured applications, a large Layer 2 broadcast domain, or an underlying network problem (e.g., STP loops or route flapping).
Console messages	• A router recognizes that a Layer 2 problem has occurred and sends alert messages to the console. • Typically, a router does this when it detects a problem with interpreting incoming frames (encapsulation or framing problems) or when keepalives are expected but do not arrive. • The most common console message that indicates a Layer 2 problem is a line protocol down message

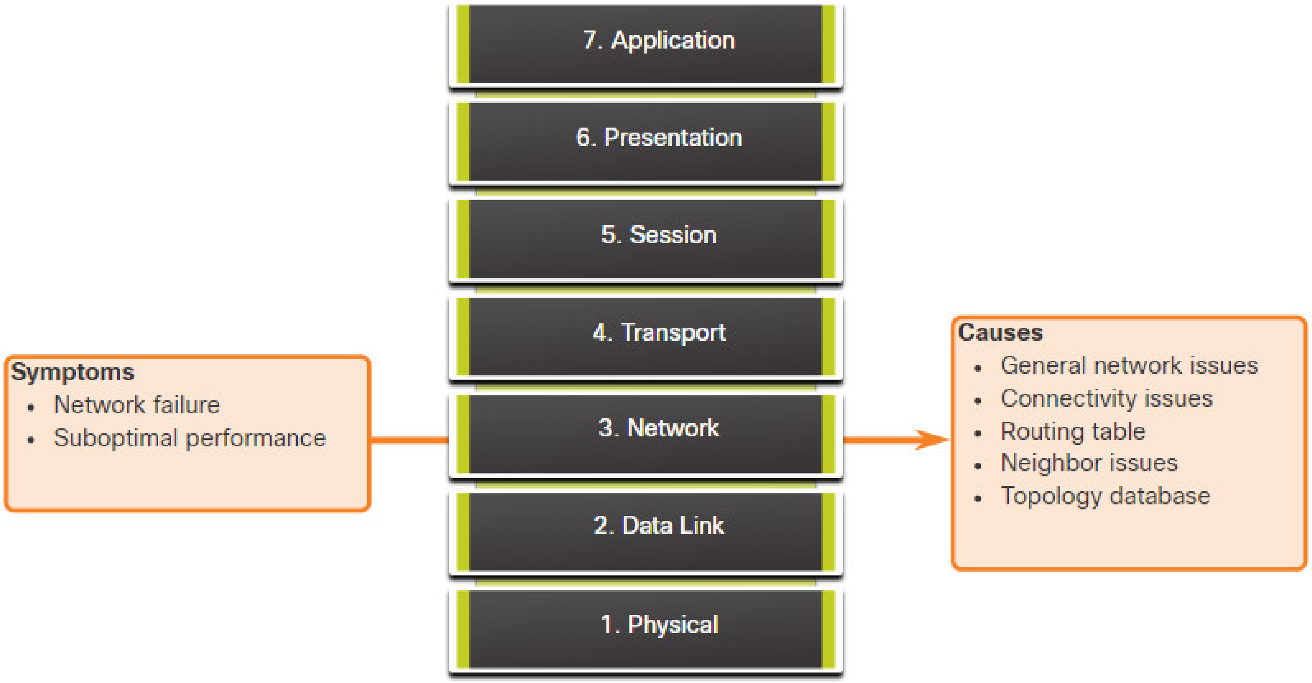
The table lists issues that commonly cause network problems at the data link layer.

Problem Cause	Description
Encapsulation errors	• An encapsulation error occurs because the bits placed in a field by the sender are not what the receiver expects to see. • This condition occurs when the encapsulation at one end of a WAN link is configured differently from the encapsulation used at the other end.

Problem Cause	Description
Address mapping errors	• In topologies, such as point-to-multipoint or broadcast Ethernet, it is essential that an appropriate Layer 2 destination address be given to the frame. This ensures its arrival at the correct destination. • To achieve this, the network device must match a destination Layer 3 address with the correct Layer 2 address using either static or dynamic maps. • In a dynamic environment, the mapping of Layer 2 and Layer 3 information can fail because devices may have been specifically configured not to respond to ARP requests, the Layer 2 or Layer 3 information that is cached may have physically changed, or invalid ARP replies are received because of a misconfiguration or a security attack.
Framing errors	• Frames usually work in groups of 8-bit bytes. • A framing error occurs when a frame does not end on an 8-bit byte boundary. • When this happens, the receiver may have problems determining where one frame ends, and another frame starts. • Too many invalid frames may prevent valid keepalives from being exchanged. • Framing errors can be caused by a noisy serial line, an improperly designed cable (too long or not properly shielded), faulty NIC, duplex mismatch, or an incorrectly configured channel service unit (CSU) line clock.
STP failures or loops	• The purpose of the Spanning Tree Protocol (STP) is to resolve a redundant physical topology into a tree-like topology by blocking redundant ports. • Most STP problems are related to forwarding loops that occur when no ports in a redundant topology are blocked and traffic is forwarded in circles indefinitely. This causes excessive flooding because of a high rate of STP topology changes. • A topology change should be a rare event in a well-configured network. • When a link between two switches goes up or down, there is eventually a topology change when the STP state of the port is changing to or from forwarding. • However, when a port is flapping (oscillating between up and down states), this causes repetitive topology changes and flooding, or slow STP convergence or re-convergence. • This can be caused by a mismatch between the real and documented topology, a configuration error, such as an inconsistent configuration of STP timers, an overloaded switch CPU during convergence, or a software defect.

12.4.3. Network Layer Troubleshooting

Network layer problems include any problem that involves a Layer 3 protocol, such as IPv4, IPv6, EIGRP, OSPF, etc. The figure summarizes the symptoms and causes of network layer network problems.



The table lists common symptoms of network layer network problems.

Symptom	Description
Network failure	• Network failure is when the network is nearly or completely non-functional, affecting all users and applications on the network. • These failures are usually noticed quickly by users and network administrators and are obviously critical to the productivity of a company.
Suboptimal performance	• Network optimization problems usually involve a subset of users, applications, destinations, or a type of traffic. • Optimization issues can be difficult to detect and even harder to isolate and diagnose. • This is because they usually involve multiple layers, or even a single host computer. • Determining that the problem is a network layer problem can take time.

In most networks, static routes are used in combination with dynamic routing protocols. Improper configuration of static routes can lead to less than optimal routing. In some cases, improperly configured static routes can create routing loops which make parts of the network unreachable.

Troubleshooting dynamic routing protocols requires a thorough understanding of how the specific routing protocol functions. Some problems are common to all routing protocols, while other problems are particular to the individual routing protocol.

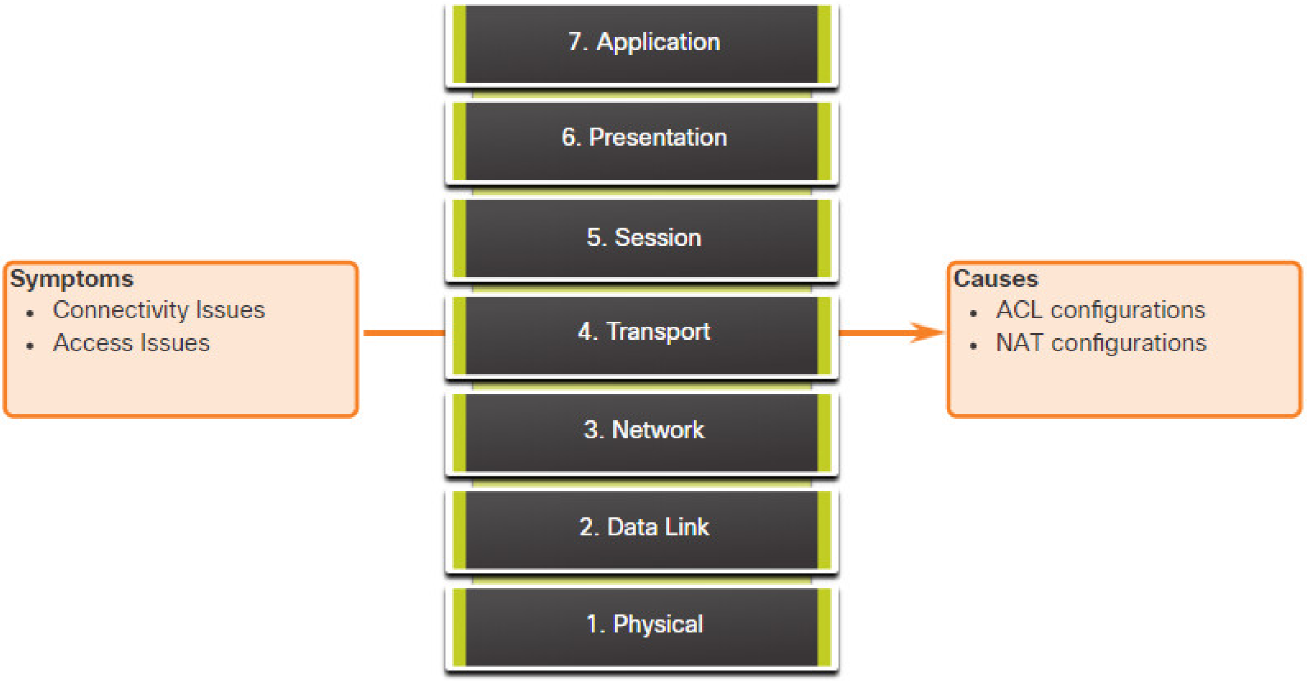
There is no single template for solving Layer 3 problems. Routing problems are solved with a methodical process, using a series of commands to isolate and diagnose the problem.

The table lists areas to explore when diagnosing a possible problem involving routing protocols.

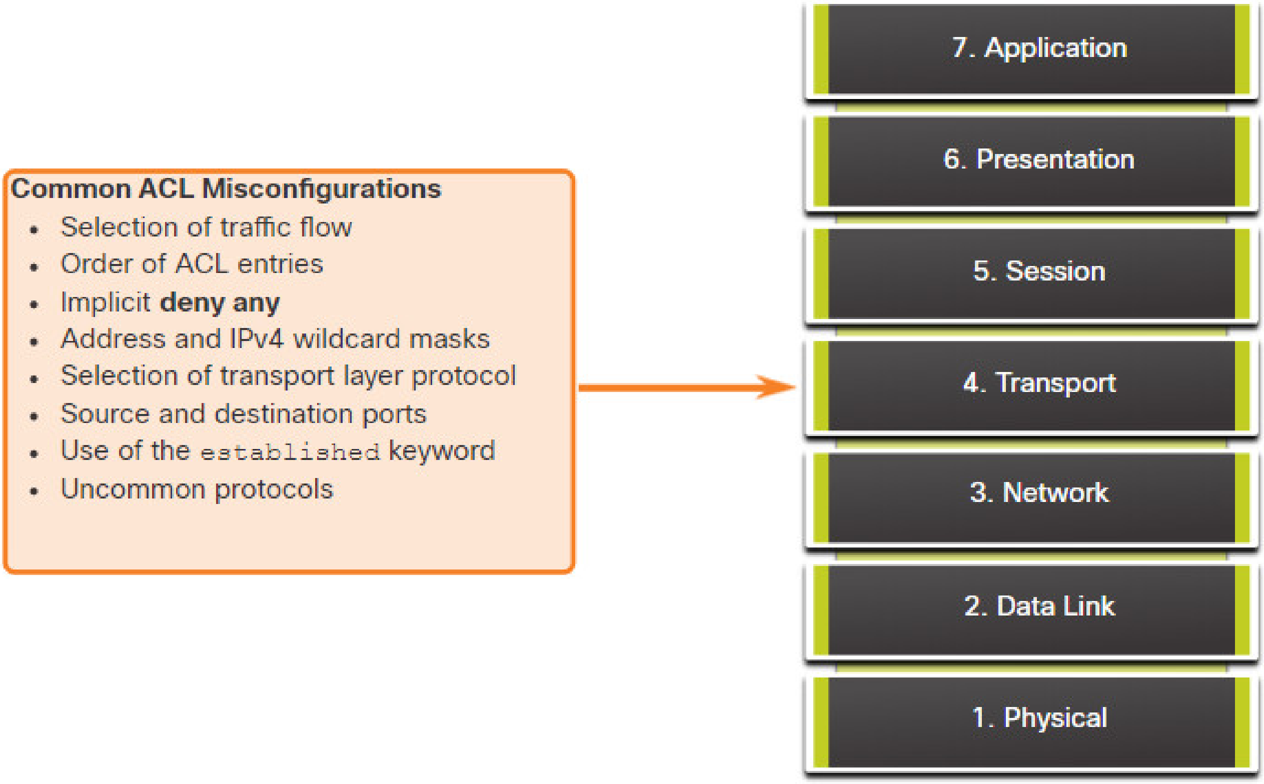
Problem Cause	Description
General network issues	• Often a change in the topology, such as a down link, may have effects on other areas of the network that might not be obvious at the time. • This may include the installation of new routes, static or dynamic, or removal of other routes. • Determine whether anything in the network has recently changed, and if there is anyone currently working on the network infrastructure.
Connectivity issues	• Check for any equipment and connectivity problems, including power problems such as outages and environmental problems (for example, overheating). • Also check for Layer 1 problems, such as cabling problems, bad ports, and ISP problems.
Routing table	• Check the routing table for anything unexpected, such as missing routes or unexpected routes. • Use **debug** commands to view routing updates and routing table maintenance.
Neighbor issues	If the routing protocol establishes an adjacency with a neighbor, check to see if there are any problems with the routers forming neighbor adjacencies.
Topology database	If the routing protocol uses a topology table or database, check the table for anything unexpected, such as missing entries or unexpected entries.

12.4.4. Transport Layer Troubleshooting – ACLs

Network problems can arise from transport layer problems on the router, particularly at the edge of the network where traffic is examined and modified. For instance, both access control lists (ACLs) and Network Address Translation (NAT) operate at the network layer and may involve operations at the transport layer, as shown in the figure.



The most common issues with ACLs are caused by improper configuration, as shown in the figure.


7. Application
6. Presentation
5. Session
4. Transport
3. Network
2. Data Link
1. Physical
Common ACL Misconfigurations
Selection of traffic flow
Order of ACL entries
Implicit deny any
Address and IPv4 wildcard masks
Selection of transport layer protocol
Source and destination ports
Use of the established keyword
Uncommon protocols

Problems with ACLs may cause otherwise working systems to fail. The table lists areas where misconfigurations commonly occur.

Misconfigurations	Description
Selection of traffic flow	• Traffic is defined by both the router interface through which the traffic is traveling and the direction in which this traffic is traveling. • An ACL must be applied to the correct interface, and the correct traffic direction must be selected to function properly.
Order of access control entries	• The entries in an ACL should be from specific to general. • Although an ACL may have an entry to specifically permit a type of traffic flow, packets never match that entry if they are being denied by another entry earlier in the list. • If the router is running both ACLs and NAT, the order in which each of these technologies is applied to a traffic flow is important. • Inbound traffic is processed by the inbound ACL before being processed by outside-to-inside NAT. • Outbound traffic is processed by the outbound ACL after being processed by inside-to-outside NAT.
Implicit deny any	When high security is not required on the ACL, this implicit access control element can be the cause of an ACL misconfiguration.
Addresses and IPv4 wildcard masks	• Complex IPv4 wildcard masks provide significant improvements in efficiency but are more subject to configuration errors. • An example of a complex wildcard mask is using the IPv4 address 10.0.32.0 and wildcard mask 0.0.32.15 to select the first 15 host addresses in either the 10.0.0.0 network or the 10.0.32.0 network.
Selection of transport layer protocol	• When configuring ACLs, it is important that only the correct transport layer protocols be specified. • Many network administrators, when unsure whether a type of traffic flow uses a TCP port or a UDP port, configure both. • Specifying both opens a hole through the firewall, possibly giving intruders an avenue into the network. • It also introduces an extra element into the ACL, so the ACL takes longer to process, introducing more latency into network communications.

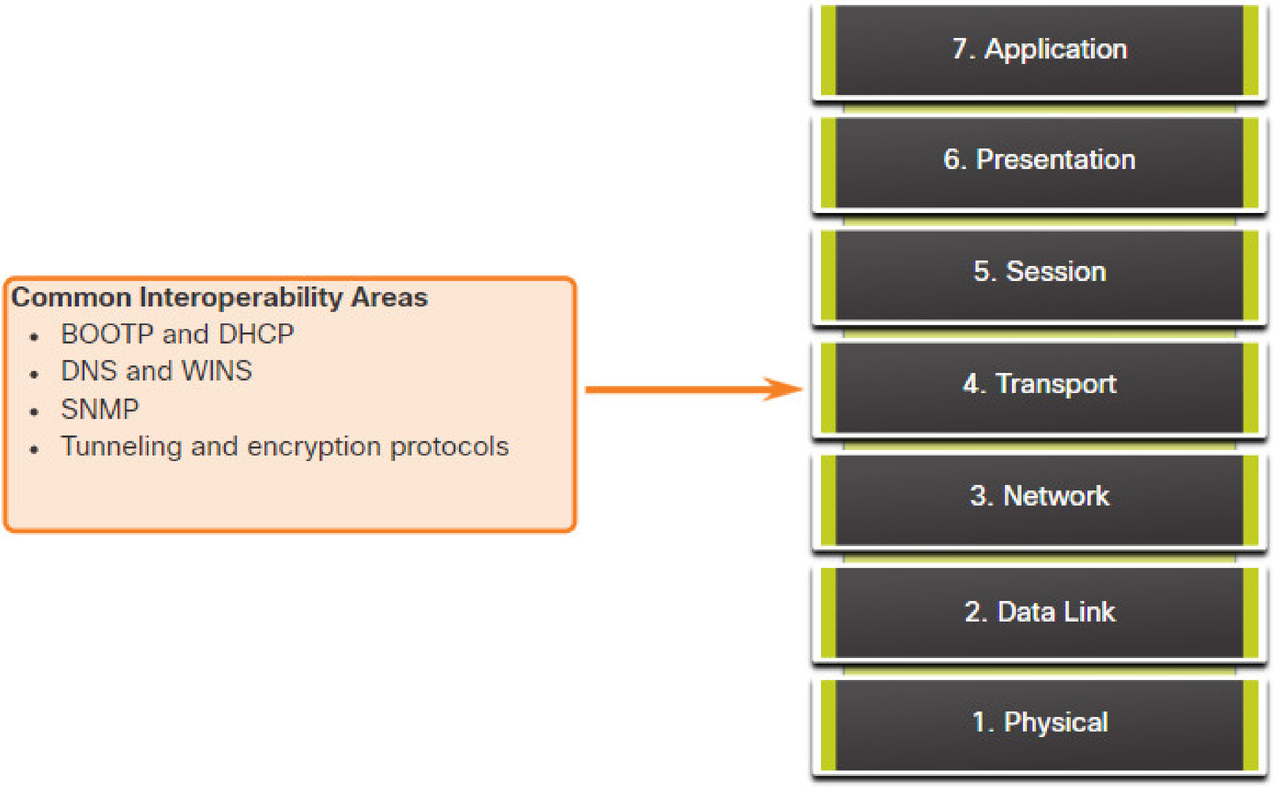
Misconfigurations	Description
Source and destination ports	• Properly controlling the traffic between two hosts requires symmetric access control elements for inbound and outbound ACLs. • Address and port information for traffic generated by a replying host is the mirror image of address and port information for traffic generated by the initiating host.
Use of the established keyword	• The **established** keyword increases the security provided by an ACL. • However, if the keyword is applied incorrectly, unexpected results may occur.
Uncommon protocols	• Misconfigured ACLs often cause problems for protocols other than TCP and UDP. • Uncommon protocols that are gaining popularity are VPN and encryption protocols.

The **log** keyword is a useful command for viewing ACL operation on ACL entries. This keyword instructs the router to place an entry in the system log whenever that entry condition is matched. The logged event includes details of the packet that matched the ACL element. The **log** keyword is especially useful for troubleshooting and provides information on intrusion attempts being blocked by the ACL.

12.4.5. Transport Layer Troubleshooting – NAT for IPv4

There are several problems with NAT, such as not interacting with services like DHCP and tunneling. These can include misconfigured NAT inside, NAT outside, or ACLs. Other issues include interoperability with other network technologies, especially those that contain or derive information from host network addressing in the packet.

The figure summarizes common interoperability areas with NAT.



Common Interoperability Areas

- BOOTP and DHCP
- DNS and WINS
- SNMP
- Tunneling and encryption protocols

The table lists common interoperability areas with NAT.

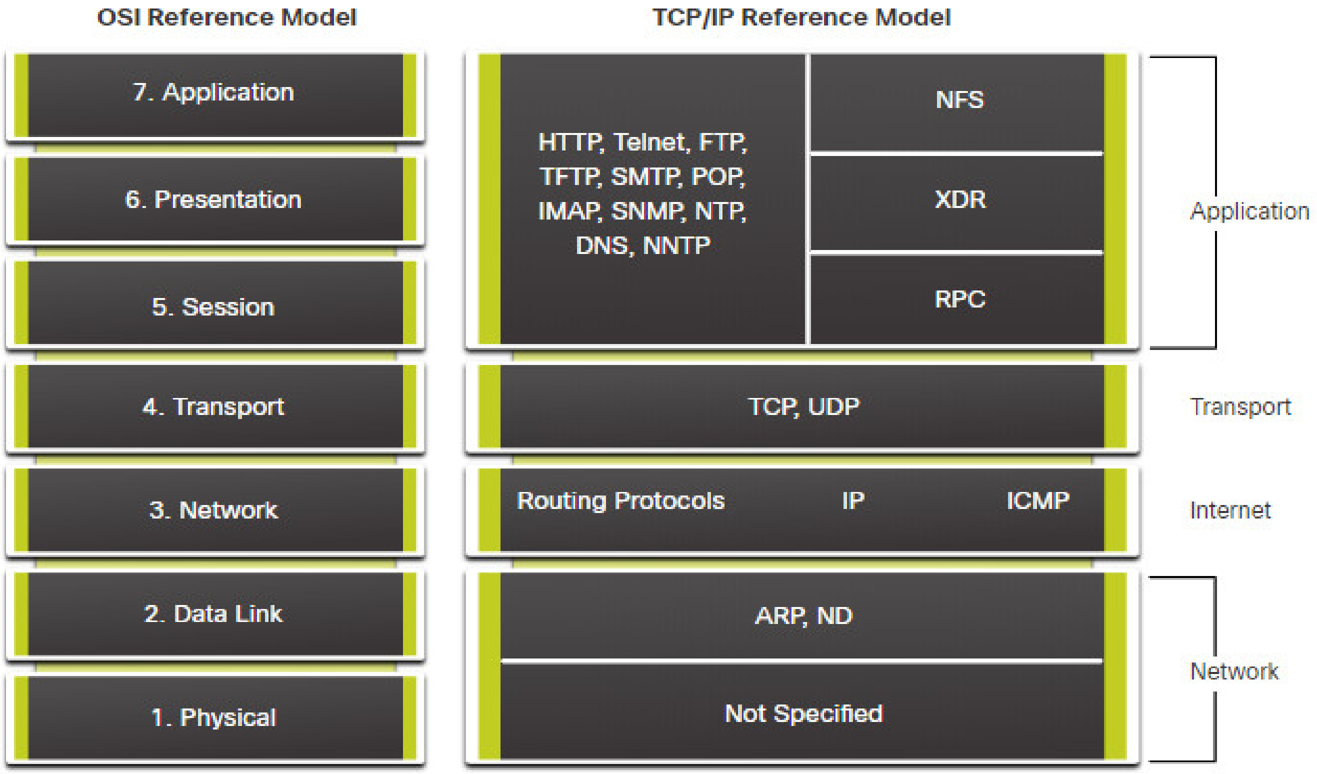
Symptom	Description
BOOTP and DHCP	• Both protocols manage the automatic assignment of IPv4 addresses to clients. • Recall that the first packet that a new client sends is a DHCP-Request broadcast IPv4 packet. • The DHCP-Request packet has a source IPv4 address of 0.0.0.0. • Because NAT requires both a valid destination and source IPv4 address, BOOTP and DHCP can have difficulty operating over a router running either static or dynamic NAT. • Configuring the IPv4 helper feature can help solve this problem.
DNS	• Because a router running dynamic NAT is changing the relationship between inside and outside addresses regularly as table entries expire and are recreated, a DNS server outside the NAT router does not have an accurate representation of the network inside the router. • Configuring the IPv4 helper feature can help solve this problem.

Symptom	Description
SNMP	• Like DNS packets, NAT is unable to alter the addressing information stored in the data payload of the packet. • Because of this, an SNMP management station on one side of a NAT router may not be able to contact SNMP agents on the other side of the NAT router. • Configuring the IPv4 helper feature can help solve this problem.
Tunneling and encryption protocols	• Encryption and tunneling protocols often require that traffic be sourced from a specific UDP or TCP port, or use a protocol at the transport layer that cannot be processed by NAT. • For example, IPsec tunneling protocols and generic routing encapsulation protocols used by VPN implementations cannot be processed by NAT.

12.4.6. Application Layer Troubleshooting

Most of the application layer protocols provide user services. Application layer protocols are typically used for network management, file transfer, distributed file services, terminal emulation, and email. New user services are often added, such as VPNs and VoIP.

The figure shows the most widely known and implemented TCP/IP application layer protocols.



The table provides a short description of these application layer protocols.

Applications	Description
SSH/Telnet	Enables users to establish terminal session connections with remote hosts.
HTTP	Supports the exchanging of text, graphic images, sound, video, and other multimedia files on the web.
FTP	Performs interactive file transfers between hosts.
TFTP	Performs basic interactive file transfers typically between hosts and networking devices.
SMTP	Supports basic message delivery services.
POP	Connects to mail servers and downloads email.
SNMP	Collects management information from network devices.
DNS	Maps IP addresses to the names assigned to network devices.
Network File System (NFS)	Enables computers to mount drives on remote hosts and operate them as if they were local drives. Originally developed by Sun Microsystems, it combines with two other application layer protocols, external data representation (XDR) and remote-procedure call (RPC), to allow transparent access to remote network resources.

The types of symptoms and causes depend upon the actual application itself.

Application layer problems prevent services from being provided to application programs. A problem at the application layer can result in unreachable or unusable resources when the physical, data link, network, and transport layers are functional. 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.

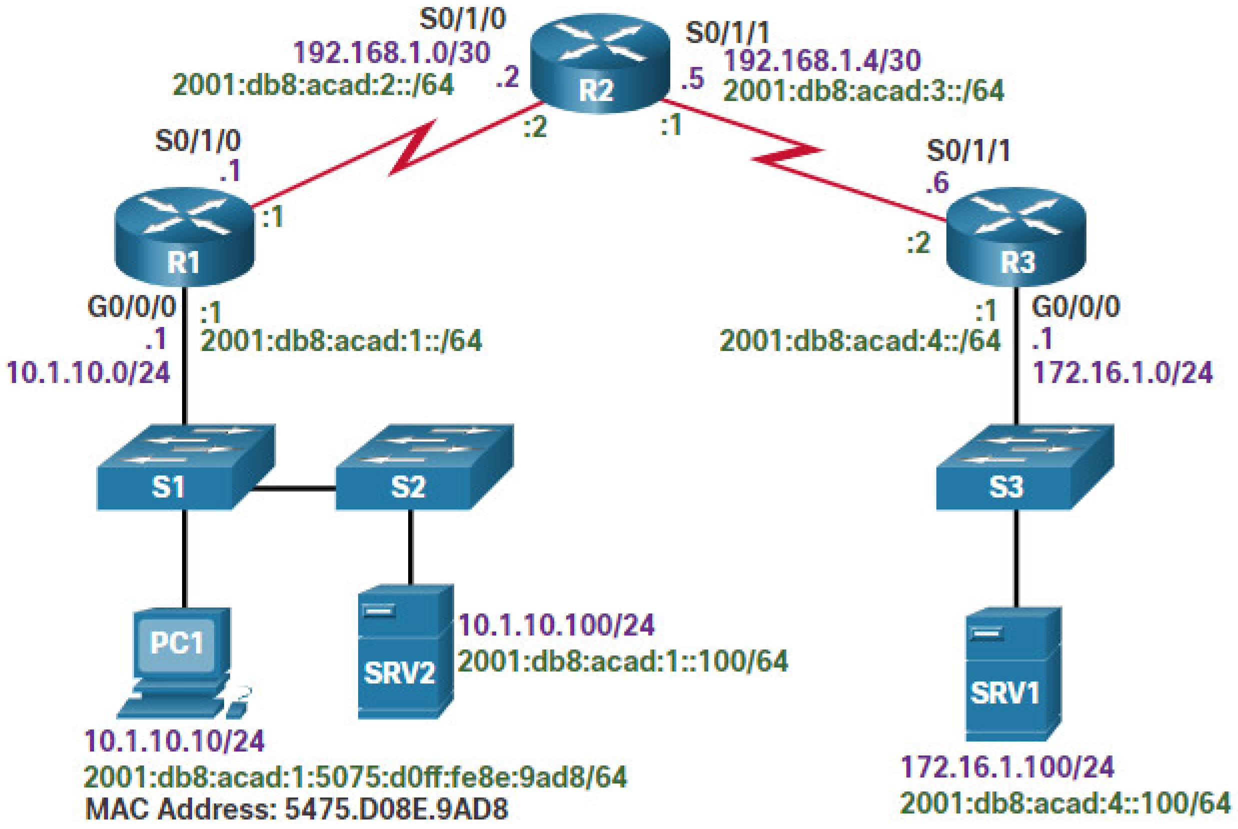
A problem at the application layer may cause users to complain that the network or an application that they are working with is sluggish or slower than usual when transferring data or requesting network services.

12.5. Troubleshooting IP Connectivity

12.5.1. Components of Troubleshooting End-to-End Connectivity

This topic presents a single topology and the tools to diagnose, and in some cases solve, an end-to-end connectivity problem. Diagnosing and solving problems is an essential skill for network administrators. There is no single recipe for troubleshooting, and a problem can be diagnosed in many ways. However, by employing a structured approach to the troubleshooting process, an administrator can reduce the time it takes to diagnose and solve a problem.

Throughout this topic, the following scenario is used. The client host PC1 is unable to access applications on Server SRV1 or Server SRV2. The figure shows the topology of this network. PC1 uses SLAAC with EUI-64 to create its IPv6 global unicast address. EUI-64 creates the Interface ID using the Ethernet MAC address, inserting FFFE in the middle, and flipping the seventh bit.



When there is no end-to-end connectivity, and the administrator chooses to troubleshoot with a bottom-up approach, the following are common steps the administrator can take:

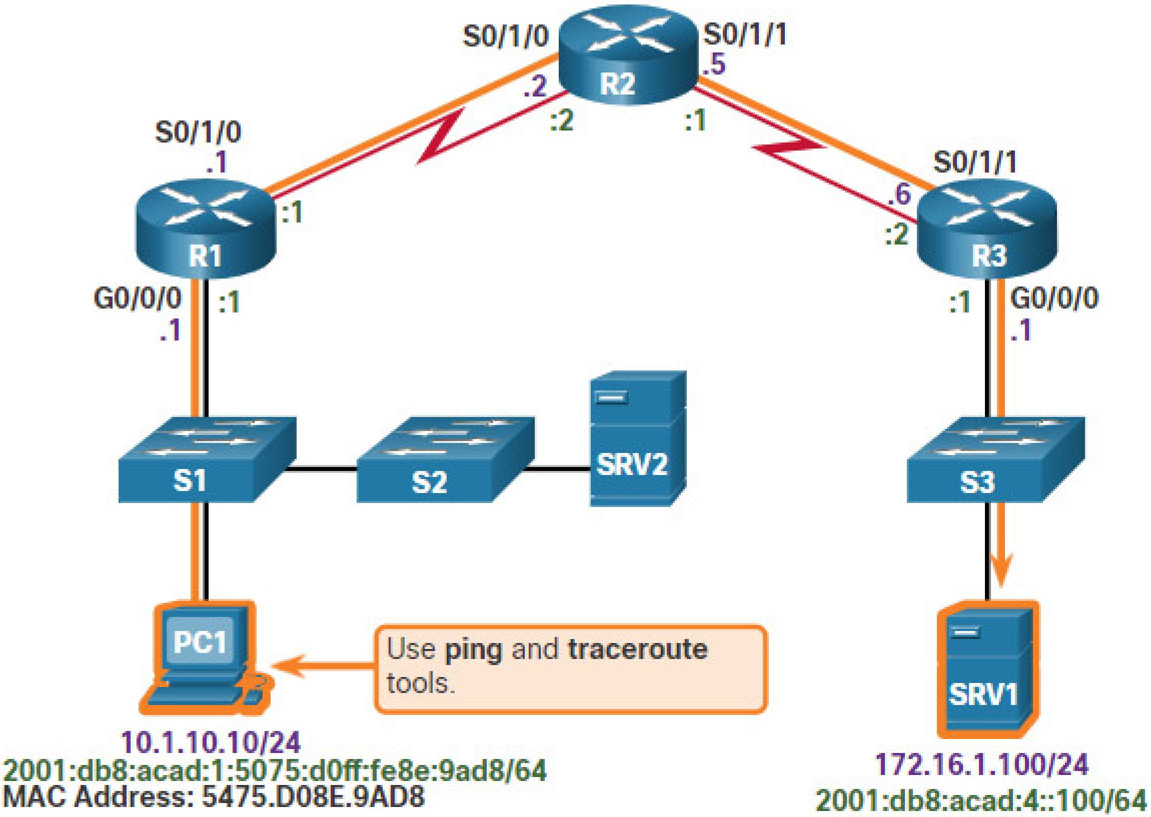
Step 1. Check physical connectivity at the point where network communication stops. This includes cables and hardware. The problem might be with a faulty cable or interface, or involve misconfigured or faulty hardware.
Step 2. Check for duplex mismatches.
Step 3. Check data link and network layer addressing on the local network. This includes IPv4 ARP tables, IPv6 neighbor tables, MAC address tables, and VLAN assignments.

Step 4. Verify that the default gateway is correct.
Step 5. Ensure that devices are determining the correct path from the source to the destination. Manipulate the routing information if necessary.
Step 6. Verify the transport layer is functioning properly. Telnet can also be used to test transport layer connections from the command line.
Step 7. Verify that there are no ACLs blocking traffic.
Step 8. Ensure that DNS settings are correct. There should be a DNS server that is accessible.

The outcome of this process is operational, end-to-end connectivity. If all the steps have been performed without any resolution, the network administrator may either want to repeat the previous steps or escalate the problem to a senior administrator.

12.5.2. End-to-End Connectivity Problem Initiates Troubleshooting

Usually what initiates a troubleshooting effort is the discovery that there is a problem with end-to-end connectivity. Two of the most common utilities used to verify a problem with end-to-end connectivity are **ping** and **traceroute**, as shown in the figure.



Click each button to review the ping, traceroute, and tracert utilities.

- IPv4 ping
- IPv4 traceroute
- IPv6 ping and traceroute

IPv4 ping

Ping is probably the most widely-known connectivity-testing utility in networking and has always been part of Cisco IOS Software. It sends out requests for responses from a specified host address. The **ping** command uses a Layer 3 protocol that is a part of the TCP/IP suite called ICMP. Ping uses the ICMP echo request and ICMP echo reply packets. If the host at the specified address receives the ICMP echo request, it responds with an ICMP echo reply packet. Ping can be used to verify end-to-end connectivity for both IPv4 and IPv6. The command output shows a successful ping from PC1 to SRV1, at address 172.16.1.100.

```
C:\> ping 172.16.1.100
Pinging 172.16.1.100 with 32 bytes of data:
Reply from 172.16.1.100: bytes=32 time=199ms TTL=128
Reply from 172.16.1.100: bytes=32 time=193ms TTL=128
Reply from 172.16.1.100: bytes=32 time=194ms TTL=128
Reply from 172.16.1.100: bytes=32 time=196ms TTL=128
Ping statistics for 172.16.1.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 193ms, Maximum = 199ms, Average = 195ms
C:\>
```

Note: The **traceroute** command is commonly performed when the **ping** command fails. If the **ping** succeeds, the **traceroute** command is commonly not needed because the technician knows that connectivity exists.

12.5.3. Step 1 – Verify the Physical Layer

All network devices are specialized computer systems. At a minimum, these devices consist of a CPU, RAM, and storage space, allowing the device to boot and run the operating system and interfaces. This allows for the reception and transmission of network traffic. When a network administrator determines that a problem exists on a given device, and that problem might be hardware-related, it is worthwhile to verify the operation of these generic components. The most commonly used Cisco IOS commands for this purpose are **show processes cpu**, **show memory**, and **show interfaces**. This topic discusses the **show interfaces** command.

When troubleshooting performance-related issues and hardware is suspected to be at fault, the **show interfaces** command can be used to verify the interfaces through which the traffic passes.

Refer to the command output of the **show interfaces** command.

```
R1# show interfaces GigabitEthernet 0/0/0
GigabitEthernet0/0/0 is up, line protocol is up
Hardware is CN Gigabit Ethernet, address is d48c.b5ce.a0c0(bia d48c.b5ce.a0c0)
Internet address is 10.1.10.1/24
(Output omitted)
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
85 packets input, 7711 bytes, 0 no buffer
Received 25 broadcasts (0 IP multicasts)
0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
0 watchdog, 5 multicast, 0 pause input
10112 packets output, 922864 bytes, 0 underruns
0 output errors, 0 collisions, l interface resets
11 unknown protocol drops
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
R1#
```

Click each button for an explanation of the highlighted output.

- Input queue drops
- Output queue drops
- Input errors
- Output errors

Input queue drops
Input queue drops (and the related ignored and throttle counters) signify that at some point, more traffic was delivered to the router than it could process. This does not necessarily indicate a problem. That could be normal traffic during peak periods. However, it could be an indication that the CPU cannot process packets in time, so if this number is consistently high, it is worth trying to spot at which moments these counters are increasing and how this relates to CPU usage.

12.5.4. Step 2 – Check for Duplex Mismatches

Another common cause for interface errors is a mismatched duplex mode between two ends of an Ethernet link. In many Ethernet-based networks, point-to-point connections are now the norm, and the use of hubs and the associated half-duplex operation is becoming less common. This means that most Ethernet links today operate in full-duplex mode, and while collisions were normal for an Ethernet link, collisions today often indicate that duplex negotiation has failed, or the link is not operating in the correct duplex mode.

The IEEE 802.3ab Gigabit Ethernet standard mandates the use of autonegotiation for speed and duplex. In addition, although it is not strictly mandatory, practically all Fast Ethernet NICs also use autonegotiation by default. The use of autonegotiation for speed and duplex is the current recommended practice.

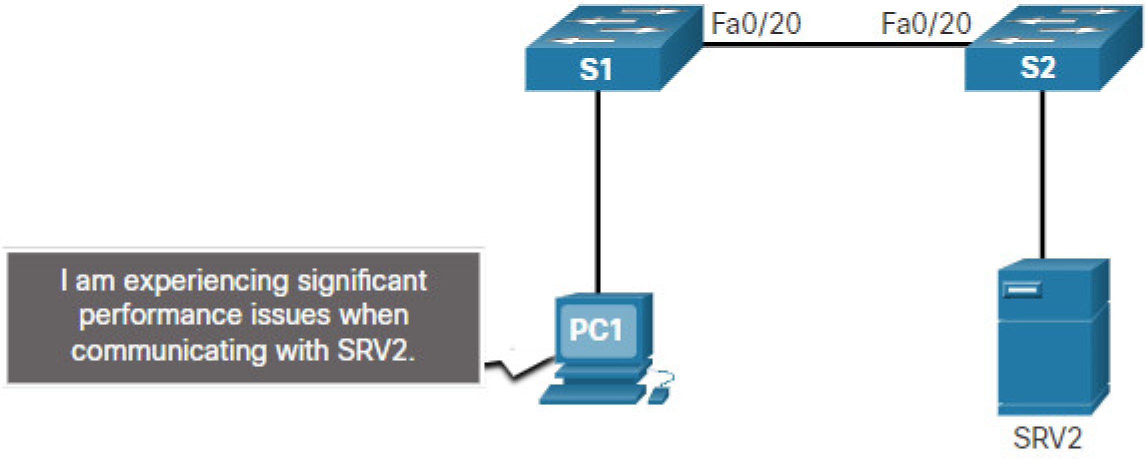
However, if duplex negotiation fails for some reason, it might be necessary to set the speed and duplex manually on both ends. Typically, this would mean setting the duplex mode to full-duplex on both ends of the connection. If this does not work, running half-duplex on both ends is preferred over a duplex mismatch.

Duplex configuration guidelines include the following:

- Autonegotiation of speed and duplex is recommended.
- If autonegotiation fails, manually set the speed and duplex on interconnecting ends.
- Point-to-point Ethernet links should always run in full-duplex mode.
- Half-duplex is uncommon and typically encountered only when legacy hubs are used.

Troubleshooting Example

In the previous scenario, the network administrator needed to add additional users to the network. To incorporate these new users, the network administrator installed a second switch and connected it to the first. Soon after S2 was added to the network, users on both switches began experiencing significant performance problems connecting with devices on the other switch, as shown in the figure.


Fa0/20
Fa0/20
S1
S2
I am experiencing significant performance issues when communicating with SRV2.
PC1
SRV2

The network administrator notices a console message on switch S2:

```
*Mar 1 00:45:08.756: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on FastEthernet0/20 (not half duplex), with Switch FastEthernet0/20 (half duplex).
```

Using the **show interfaces fa 0/20** command, the network administrator examines the interface on S1 that is used to connect to S2 and notices it is set to full-duplex, as shown the command output.

```
S1# show interface fa 0/20
FastEthernet0/20 is up, line protocol is up (connected)
Hardware is Fast Ethernet, address is 0cd9.96e8.8a01 (bia 0cd9.96e8.8a01)
MTU 1500 bytes, BW 10000 Kbit/sec, DLY 1000 usec, reliability 255/255, txload 1/255,
rxload 1/255
Encapsulation ARPA, loopback not set Keepalive set (10 sec)
Full-duplex, Auto-speed, media type is 10/100BaseTX

(Output omitted)

S1#
```

The network administrator now examines the other side of the connection, the port on S2. The command out shows that this side of the connection has been configured for half-duplex.

```
S2# show interface fa 0/20
FastEthernet0/20 is up, line protocol is up (connected)
Hardware is Fast Ethernet, address is 0cd9.96d2.4001 (bia 0cd9.96d2.4001)
MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec, reliability 255/255, txload 1/255,
rxload 1/255
Encapsulation ARPA, loopback not set Keepalive set (10 sec)
Half-duplex, Auto-speed, media type is 10/100BaseTX

(Output omitted)

S2(config)# interface fa 0/20
S2(config-if)# duplex auto
S2(config-if)#
```

The network administrator corrects the setting to **duplex auto** to automatically negotiate the duplex. Because the port on S1 is set to full-duplex, S2 also uses full-duplex.

The users report that there are no longer any performance problems.

12.5.5. Step 3 – Verify Addressing on the Local Network

When troubleshooting end-to-end connectivity, it is useful to verify mappings between destination IP addresses and Layer 2 Ethernet addresses on individual segments. In IPv4, this functionality is provided by ARP. In IPv6, the ARP functionality is replaced by the neighbor discovery process and ICMPv6. The neighbor table caches IPv6 addresses and their resolved Ethernet physical (MAC) addresses.

Click each button for an example and explanation of the command to verify Layer 2 and Layer 3 addressing.

- Windows IPv4 ARP Table
- Windows IPv6 Neighbor Table
- IOS IPv6 Neighbor Table
- Switch MAC Address Table

Windows IPv4 ARP Table
The **arp** Windows command displays and modifies entries in the ARP cache that are used to store IPv4 addresses and their resolved Ethernet physical (MAC) addresses. As shown in the command output, the **arp** Windows command lists all devices that are currently in the ARP cache.

The information that is displayed for each device includes the IPv4 address, physical (MAC) address, and the type of addressing (static or dynamic).

The cache can be cleared by using the **arp -d** Windows command if the network administrator wants to repopulate the cache with updated information.

Note: The **arp** commands in Linux and MAC OS X have a similar syntax.

```
C:\> arp -a
Interface: 10.1.10.100 --- 0xd
  Internet Address      Physical Address      Type
  10.1.10.1             d4-8c-b5-ce-a0-c0    dynamic
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
C:\>
```

12.5.6. Troubleshoot VLAN Assignment Example

Another issue to consider when troubleshooting end-to-end connectivity is VLAN assignment. In the switched network, each port in a switch belongs to a VLAN. Each VLAN is considered a separate logical network, and packets destined for stations that do not belong to the VLAN must be forwarded through a device that supports routing. If a host in one VLAN sends a broadcast Ethernet frame, such as an ARP request, all hosts in the same VLAN receive the frame; hosts in other VLANs do not. Even if two hosts are in the same IP network, they will not be able to communicate if they are connected to ports assigned to two separate VLANs. Additionally, if the VLAN to which the port belongs is deleted, the port becomes inactive. All hosts attached to ports belonging to the VLAN that was deleted are unable to communicate with the rest of the network. Commands such as show vlan can be used to validate VLAN assignments on a switch.

Assume for example, that in an effort to improve the wire management in the wiring closet, your company has reorganized the cables connecting to switch S1. Almost immediately afterward, users started calling the support desk stating that they could no longer reach devices outside their own network.

Click each button for an explanation of the process used to troubleshoot this issue.

- Check the ARP Table

- Check the Switch MAC Table
- Correct the VLAN Assignment

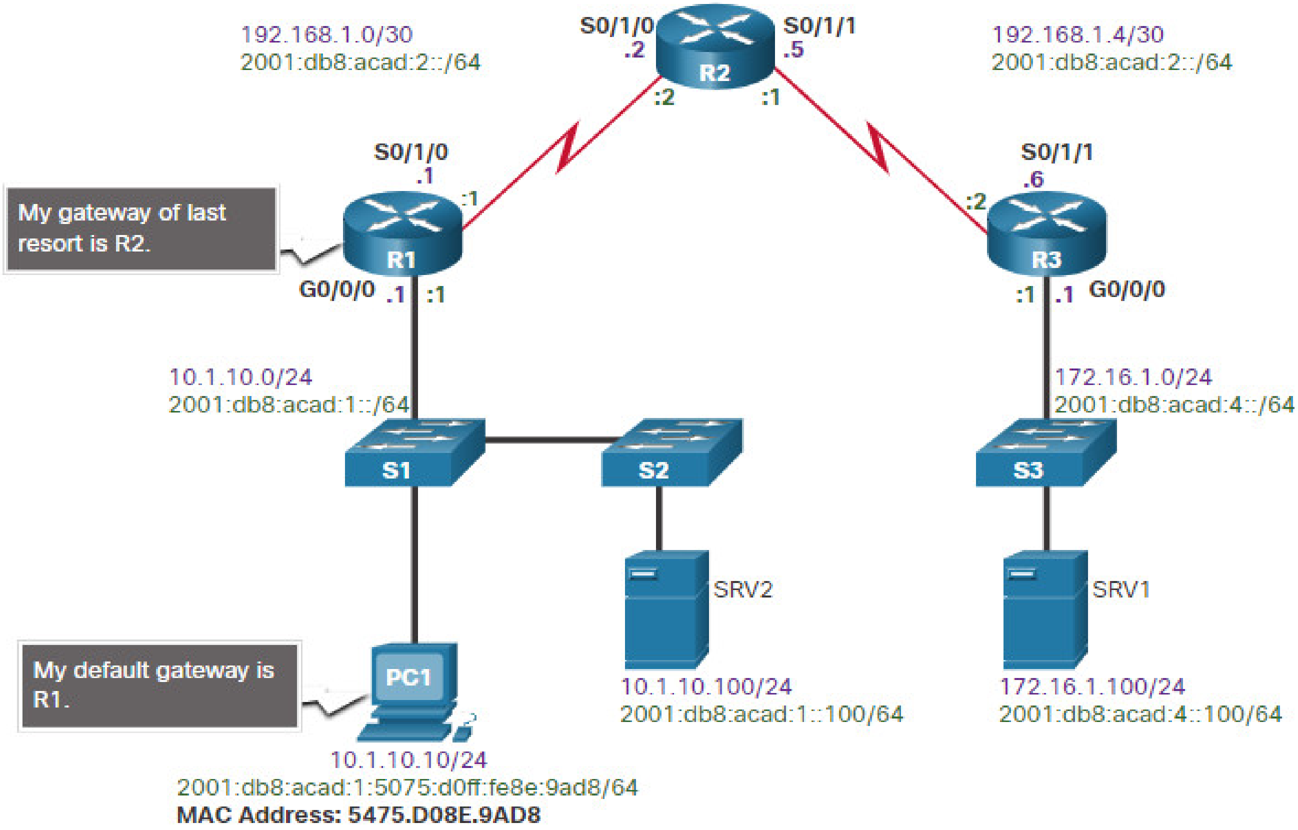
Check the ARP Table
An examination of PC1 ARP table using the **arp** Windows command shows that the ARP table no longer contains an entry for the default gateway 10.1.10.1, as shown in the command output.

```
C:\> arp -a
Interface: 10.1.10.100 --- 0xd
  Internet Address      Physical Address      Type
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
C:\>
```

12.5.7. Step 4 – Verify Default Gateway

If there is no detailed route on the router, or if the host is configured with the wrong default gateway, then communication between two endpoints in different networks does not work.

The figure illustrates how PC1 uses R1 as its default gateway. Similarly, R1 uses R2 as its default gateway or gateway of last resort. If a host needs access to resources beyond the local network, the default gateway must be configured. The default gateway is the first router on the path to destinations beyond the local network.



Troubleshooting IPv4 Default Gateway Example

In this example, R1 has the correct default gateway, which is the IPv4 address of R2. However, PC1 has the wrong default gateway. PC1 should have the default gateway of R1 10.1.10.1. This must be configured manually if the IPv4 addressing information was manually configured on PC1. If the IPv4 addressing information was obtained automatically from a DHCPv4 server, then the configuration on the DHCP server must be examined. A configuration problem on a DHCP server usually affects multiple clients.

Click each button to view the command output for R1 and PC1.

- R1 Routing Table
- PC1 Routing Table

R1 Routing Table

The command output of the **show ip route** Cisco IOS command is used to verify the default gateway of R1

```
R1# show ip route | include Gateway|0.0.0.0

Gateway of last resort is 192.168.1.2 to network 0.0.0.0
S* 0.0.0.0/0 [1/0] via 192.168.1.2

R1#
```

12.5.8. Troubleshoot IPv6 Default Gateway Example

In IPv6, the default gateway can be configured manually, using stateless autoconfiguration (SLAAC), or by using DHCPv6. With SLAAC, the default gateway is advertised by the router to hosts using ICMPv6 Router Advertisement (RA) messages. The default gateway in the RA message is the link-local IPv6 address of a router interface. If the default gateway is configured manually on the host, which is very unlikely, the default gateway can be set to either the global IPv6 address, or to the link-local IPv6 address.

Click each button for an example and explanation of troubleshooting an IPv6 default gateway issue.

- R1 Routing Table
- PC1 Addressing
- Check R1 Interface Settings
- Correct R1 IPv6 Routing
- Verify PC1 Has an IPv6 Default Gateway

R1 Routing Table
As shown in the command output, the **show ipv6 route** Cisco IOS command is used to check for the IPv6 default route on R1. R1 has a default route via R2.

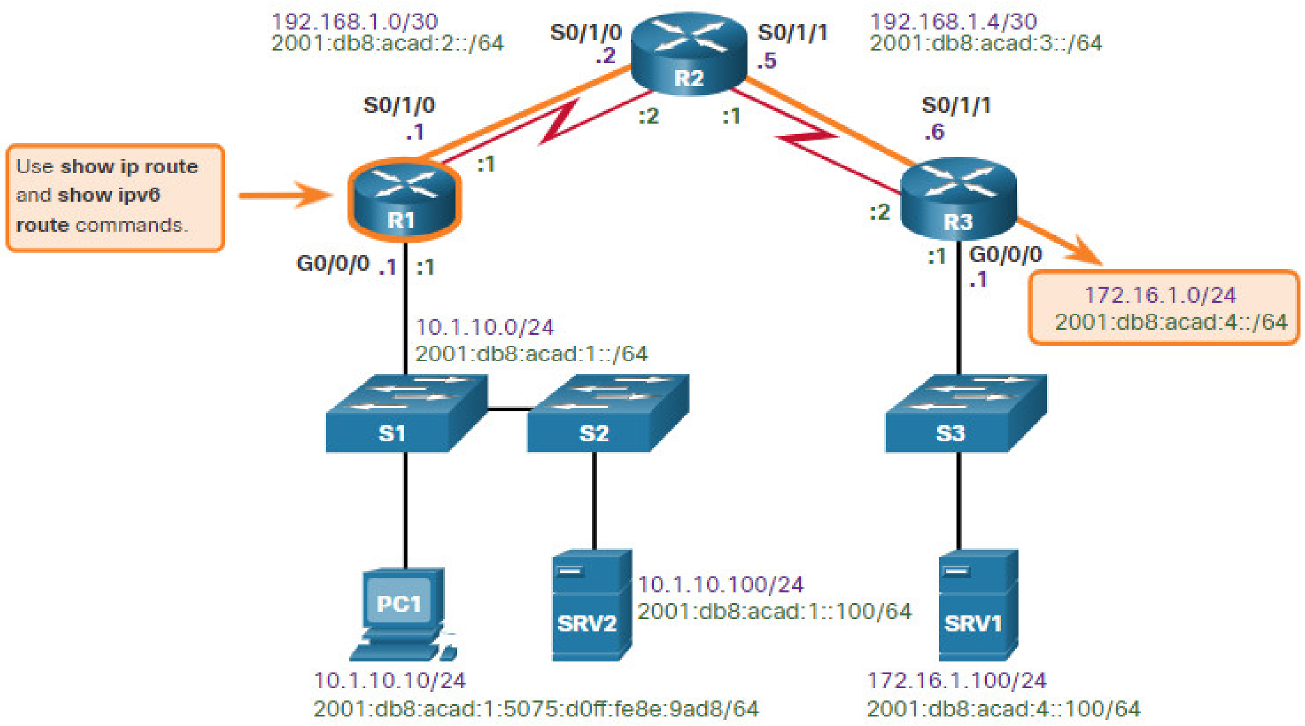
```
R1# show ipv6 route

(Output omitted)

S ::/0 [1/0]
via 2001:DB8:ACAD:2::2
R1#
```

12.5.9. Step 5 – Verify Correct Path

When troubleshooting, it is often necessary to verify the path to the destination network. The figure shows the reference topology indicating the intended path for packets from PC1 to SRV1.



Use **show ip route** and **show ipv6 route** commands.

The routers in the path make the routing decision based on information in the routing tables. Click each button to view the IPv4 and IPv6 routing tables for R1.

- R1 IPv4 Routing Table
- R1 IPv6 Routing Table

R1 IPv4 Routing Table

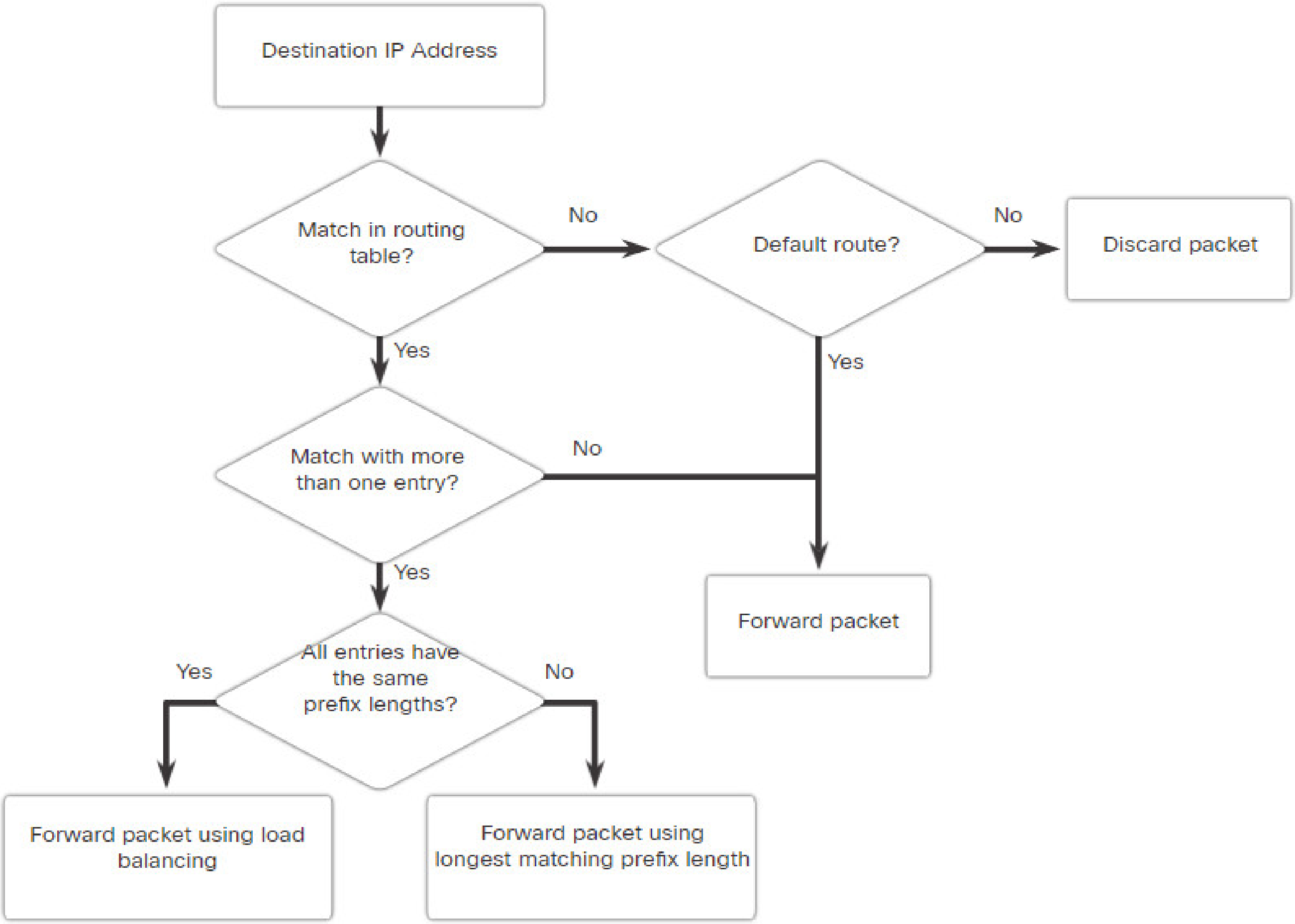
```
R1# show ip route | begin Gateway
Gateway of last resort is 192.168.1.2 to network 0.0.0.0
O*E2  0.0.0.0/0 [110/1] via 192.168.1.2, 00:00:13, Serial0/1/0
      10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        10.1.10.0/24 is directly connected, GigabitEthernet0/0/0
L        10.1.10.1/32 is directly connected, GigabitEthernet0/0/0
      172.16.0.0/24 is subnetted, 1 subnets
O        172.16.1.0 [110/100] via 192.168.1.2, 00:01:59, Serial0/1/0
      192.168.1.0/24 is variably subnetted, 3 subnets, 2 masks
C        192.168.1.0/30 is directly connected, Serial0/1/0
L        192.168.1.1/32 is directly connected, Serial0/1/0
O        192.168.1.4/30 [110/99] via 192.168.1.2, 00:06:25, Serial0/1/0
R1#
```

The IPv4 and IPv6 routing tables can be populated by the following methods:

- Directly connected networks
- Local host or local routes
- Static routes
- Dynamic routes
- Default routes

The process of forwarding IPv4 and IPv6 packets is based on the longest bit match or longest prefix match. The routing table process will attempt to forward the packet using an entry in the routing table with the greatest number of leftmost matching bits. The number of matching bits is indicated by the prefix length of the route.

The figure describes the process for both the IPv4 and IPv6 routing tables.


Destination IP Address
Match in routing table?
No
Default route?
No
Discard packet
Yes
Yes
Match with more than one entry?
No
Yes
Forward packet
Yes
All entries have the same prefix lengths?
No
Forward packet using load balancing
Forward packet using longest matching prefix length

Examine the following scenarios based on the flow chart above. If the destination address in a packet:

- Does not match an entry in the routing table, then the default route is used. If there is not a default route that is configured, the packet is discarded.
- Matches a single entry in the routing table, then the packet is forwarded through the interface that is defined in this route.
- Matches more than one entry in the routing table and the routing entries have the same prefix length, then the packets for this destination can be distributed among the routes that are defined in the routing table.
- Matches more than one entry in the routing table and the routing entries have different prefix lengths, then the packets for this destination are forwarded out of the interface that is associated with the route that has the longer prefix match.

Troubleshooting Example

Devices are unable to connect to the server SRV1 at 172.16.1.100. Using the **show ip route** command, the administrator should check to see if a routing entry exists to network 172.16.1.0/24. If the routing table does not have a specific route to the SRV1 network, the network administrator must then check for the existence of a default or summary route entry in the direction of the 172.16.1.0/24 network. If none exists, then the problem may be with routing and the administrator must verify that the network is included within the dynamic routing protocol configuration or add a static route.

12.5.10. Step 6 – Verify the Transport Layer

If the network layer appears to be functioning as expected, but users are still unable to access resources, then the network administrator must begin troubleshooting the upper layers. Two of the most common issues that affect transport layer connectivity include ACL configurations and NAT configurations. A common tool for testing transport layer functionality is the Telnet utility.

Caution: While Telnet can be used to test the transport layer, for security reasons, SSH should be used to remotely manage and configure devices.

Troubleshooting Example

A network administrator is troubleshooting a problem where they cannot connect to a router using HTTP. The administrator pings R2 as shown in the command output.

```
R1# ping 2001:db8:acad:2::2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:2::2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/2/3 ms
R1#
```

R2 responds and confirms that the network layer, and all layers below the network layer are operational. The administrator knows the issue is with Layer 4 or up and must start troubleshooting those layers.

Next, the administrator verifies that they can Telnet to R2 as shown in the command output.

```
R1# telnet 2001:db8:acad:2::2
Trying 2001:DB8:ACAD:2::2 ... Open
User Access Verification
Password:
R2> exit
[Connection to 2001:db8:acad:2::2 closed by foreign host]
R1#
```

The administrator has confirmed that Telnet services is running on R2. Although the Telnet server application runs on its own well-known port number 23 and Telnet clients connect to this port by default, a different port number can be specified on the client to connect to any TCP port that must be tested. Using a different port other than TCP port 23 indicates whether the connection is accepted (as indicated by the word “Open” in the output), refused, or times out. From any of those responses, further conclusions can be made concerning the connectivity. Certain applications, if they use an ASCII-based session protocol, might even display an application banner, it may be possible to trigger some responses from the server by typing in certain keywords, such as with SMTP, FTP, and HTTP.

For example, the administrator attempts to Telnet to R2 using port 80.

```
R1# telnet 2001:db8:acad:2::2 80
Trying 2001:DB8:ACAD:2::2, 80 ... Open
^C
HTTP/1.1 400 Bad Request
Date: Mon, 04 Nov 2019 12:34:23 GMT
Server: cisco-IOS
Accept-Ranges: none
400 Bad Request
[Connection to 2001:db8:acad:2::2 closed by foreign host]
R1#
```

The output verifies a successful transport layer connection, but R2 is refusing the connection using port 80.

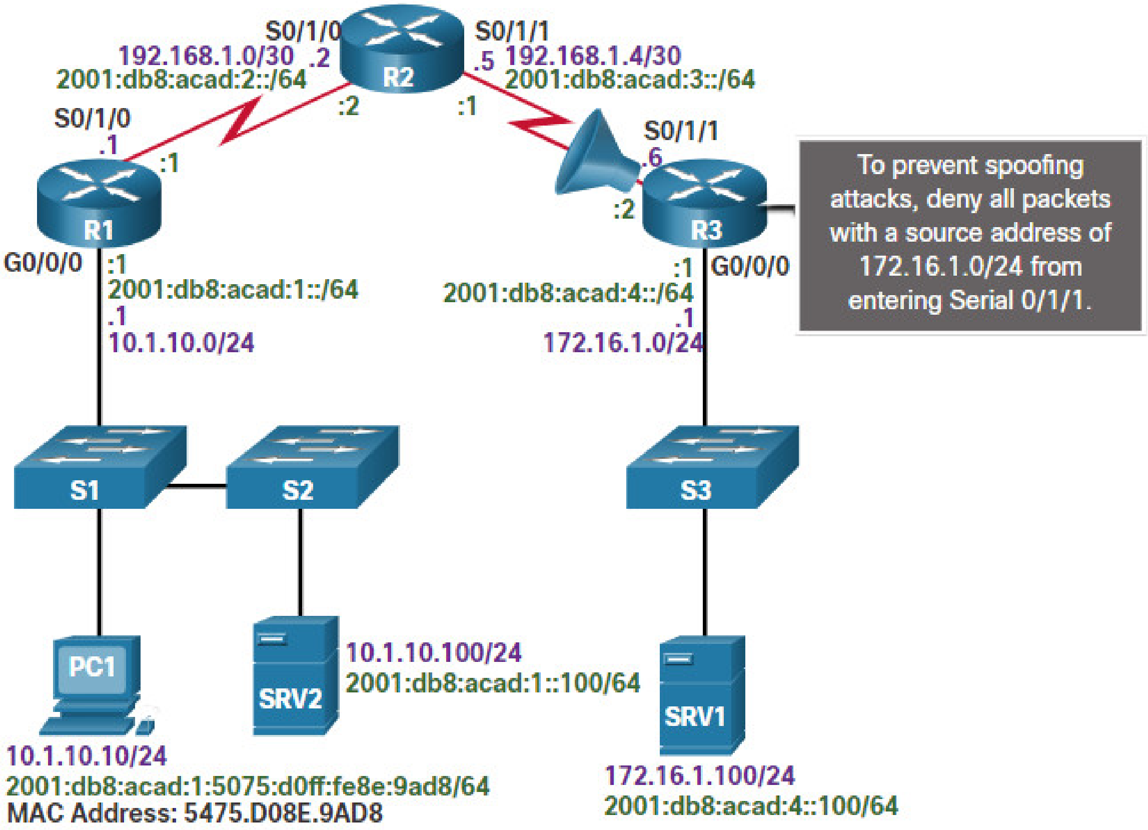
12.5.11. Step 7 – Verify ACLs

On routers, there may be ACLs that prohibit protocols from passing through the interface in the inbound or outbound direction.

Use the **show ip access-lists** command to display the contents of all IPv4 ACLs and the **show ipv6 access-list** command to display the contents of all IPv6 ACLs configured on a router. The specific ACL can be displayed by entering the ACL name or number as an option for this command. The **show ip interfaces** and **show ipv6 interfaces** commands display IPv4 and IPv6 interface information that indicates whether any IP ACLs are set on the interface.

Troubleshooting Example

To prevent spoofing attacks, the network administrator decided to implement an ACL that is preventing devices with a source network address of 172.16.1.0/24 from entering the inbound S0/0/1 interface on R3, as shown in the figure. All other IP traffic should be allowed.



To prevent spoofing attacks, deny all packets with a source address of 172.16.1.0/24 from entering Serial 0/1/1.

However, shortly after implementing the ACL, users on the 10.1.10.0/24 network were unable to connect to devices on the 172.16.1.0/24 network, including SRV1.

Click each button for an example of how to troubleshoot this issue.

show ip access-lists
The **show ip access-lists** command displays that the ACL is configured correctly, as shown in the command output.

```
R3# show ip access-lists
Extended IP access list 100
    10 deny ip 172.16.1.0 0.0.0.255 any (108 matches)
    20 permit ip any any (28 matches)
R3#
```

12.5.12. Step 8 – Verify DNS

The DNS protocol controls the DNS, a distributed database with which you can map hostnames to IP addresses. When you configure DNS on the device, you can substitute the hostname for the IP address with all IP commands, such as **ping** or **telnet**.

To display the DNS configuration information on the switch or router, use the **show running-config** command. When there is no DNS server installed, it is possible to enter names to IP mappings directly into the switch or router configuration. Use the **ip**

host command to enter a name to be used instead of the IPv4 address of the switch or router, as shown in the command output.

```
R1(config)# ip host ipv4-server 172.16.1.100
R1(config)# exit
R1#
```

Now the assigned name can be used instead of using the IP address, as shown in the command output.

```
R1# ping ipv4-server
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.100, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/5/7 ms
R1#
```

To display the name-to-IP-address mapping information on a Windows-based PC, use the **nslookup** command.

12.5.13. Packet Tracer – Troubleshoot Enterprise Networks

This activity uses a variety of technologies you have encountered during your CCNA studies, including routing, port security, EtherChannel, DHCP, and NAT. Your task is to review the requirements, isolate and resolve any issues, and then document the steps you took to verify the requirements.

12.5.13 Packet Tracer – Troubleshoot Enterprise Networks

12.6. Module Practice and Quiz

12.6.1. Packet Tracer – Troubleshooting Challenge – Document the Network

In this Packet Tracer activity, you will document a network that is unknown to you.

- Test network connectivity.
- Compile host addressing information.
- Remotely access default gateway devices.
- Document default gateway device configurations.
- Discover devices on the network.
- Draw the network topology.

12.6.1 Packet Tracer – Troubleshooting Challenge – Document the Network

12.6.2. Packet Tracer – Troubleshooting Challenge – Use Documentation to Solve Issues

In this Packet Tracer activity, you use network documentation to identify and fix network communications problems.

- Use various techniques and tools to identify connectivity issues.
- Use documentation to guide troubleshooting efforts.
- Identify specific network problems.
- Implement solutions to network communication problems.
- Verify network operation.

12.6.2 Packet Tracer – Troubleshooting Challenge – Use Documentation to Solve Issues

12.6.3. What did I learn in this module?

Network Documentation

Common network documentation includes: physical and logical network topologies, network device documentation recording all pertinent device information, and network performance baseline documentation. Information found on a physical topology typically includes the device name, device location (address, room number, rack location, etc.), interface and ports used, and cable type. Network device documentation for a router may include the interface, IPv4 address, IPv6 address, MAC address and routing protocol. Network device documentation for a switch may include the port, access, VLAN, trunk, EtherChannel, native, and enabled. Network device documentation for end-systems may include device name, OS, services, MAC address, IPv4 and IPv6 addresses, default gateway, and DNS. A network baseline should answer the following questions:

- How does the network perform during a normal or average day?
- Where are the most errors occurring?
- What part of the network is most heavily used?
- What part of the network is least used?
- Which devices should be monitored and what alert thresholds should be set?
- Can the network meet the identified policies?

When conducting the initial baseline, start by selecting a few variables that represent the defined policies, such as interface utilization and CPU utilization. A logical network topology diagram can be useful in identifying key devices and ports to monitor. The length of time and the baseline information being gathered must be long enough to determine a “normal” picture of the network. When documenting the network, gather information directly from routers and switches using the **show**, **ping**, **traceroute**, and **telnet** commands.

Troubleshooting Process

The troubleshooting process should be guided by structured methods. One method is the seven-step troubleshooting process: 1. Define the problem, 2. Gather information, 3. Analyze information, 4. Eliminate possible causes, 5. Propose hypothesis, 6. Test hypothesis, and 7. Solve the problem. When talking to end users about their network problems, ask both open and closed-ended questions. Use the **show**, **ping**, **traceroute**, and **telnet** commands to gather information from devices. Use the layered models to perform bottom-up, top-down, or divide-and-conquer troubleshooting. Other models include follow-the-path, substitution, comparison, and educated guess. Software problems are often solved using a top-down approach while hardware-based problems are solved using the bottom-up approach. New problems may be solved by an experienced technician using the divide-and-conquer method.

Troubleshooting Tools

Common software troubleshooting tools include NMS tools, knowledge bases, and baselining tools. A protocol analyzer, such as Wireshark, decodes the various protocol layers in a recorded frame and presents this information in an easy to use format. Hardware troubleshooting tools include digital multimeters, cable testers, cable analyzers, portable network analyzers, and Cisco Prime NAM. Syslog server can also be used as a troubleshooting tool. Implementing a logging facility for network troubleshooting. Cisco devices can log information regarding configuration changes, ACL violations, interface status, and many other types of events. Event messages can be sent to one or more of the following: console, terminal lines, buffered logging, SNMP traps, and syslog. The lower the level number, the higher the severity level. The **logging trap** *level* command limits messages logged to the syslog server based on severity. The level is the name or number of the severity level. Only messages equal to or numerically lower than the specified level are logged.

Symptoms and Causes of Network Problems

Failures and suboptimal conditions at the physical layer usually cause networks to shut down. Network administrators must have the ability to effectively isolate and correct problems at this layer. Symptoms include performance lower than baseline, loss of connectivity, congestion, high CPU utilization, and console error messages. The causes are usually power-related, hardware faults, cabling faults, attenuation, noise, interface configuration errors, exceeding component design limits, and CPU overload.

Data link layer problems cause specific symptoms that, when recognized, will help identify the problem quickly. Symptoms include no functionality/connectivity at Layer 2 or above, network operating below baseline levels, excessive broadcasts, and console messages. The causes are usually encapsulation errors, address mapping errors, framing errors, and STP failures or loops.

Network layer problems include any problem that involves a Layer 3 protocol, both routed protocols (such as IPv4 or IPv6) and routing protocols (such as EIGRP, OSPF, etc.). Symptoms include network failure and suboptimal performance. The causes are usually general network issues, connectivity issues, routing table problems, neighbor issues, and the topology database.

Transport layer problems can arise from transport layer problems on the router, particularly at the edge of the network where traffic is examined and modified. Symptoms include connectivity and access issues. Causes are likely to be misconfigured NAT or ACLs. ACL misconfigurations commonly occur at the selection of traffic flow, order of access control entries, implicit deny any, addresses and IPv4 wildcard masks, selection of transport layer protocol, source and destination ports, use of the established keyword, and uncommon protocols. There are several problems with NAT including misconfigured NAT inside, NAT outside, or ACL. Common interoperability areas with NAT include BOOTP and DHCP, DNS, SNMP, and tunneling and encryption protocols.

Application layer problems can result in unreachable or unusable resources when the physical, data link, network, and transport layers are functional. 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.

Troubleshooting IP Connectivity

Diagnosing and solving problems is an essential skill for network administrators. There is no single recipe for troubleshooting, and a problem can be diagnosed in many ways. However, by employing a structured approach to the troubleshooting process, an administrator can reduce the time it takes to diagnose and solve a problem.

End-to-end connectivity problems are usually what initiates a troubleshooting effort. Two of the most common utilities used to verify a problem with end-to-end connectivity are **ping** and **traceroute.** The **ping** command uses a Layer 3 protocol that is a part of the TCP/IP suite called ICMP. The **traceroute** command is commonly performed when the **ping** command fails.

Step 1. Verify the physical layer. The most commonly used Cisco IOS commands for this purpose are **show processes cpu**, **show memory**, and **show interfaces**.

Step 2. Check for duplex mismatches. Another common cause for interface errors is a mismatched duplex mode between two ends of an Ethernet link. In many Ethernet-based networks, point-to-point connections are now the norm, and the use of hubs and the associated half-duplex operation is becoming less common. Use the **show interfaces** *interface* command to diagnose this problem.

Step 3. Verify addressing on the local network. When troubleshooting end-to-end connectivity, it is useful to verify mappings between destination IP addresses and Layer 2 Ethernet addresses on individual segments. The **arp** Windows command displays and modifies entries in the ARP cache that are used to store IPv4 addresses and their resolved Ethernet physical (MAC) addresses. The **netsh interface ipv6 show neighbor** Windows command output lists all devices that are currently in the neighbor table. The **show ipv6 neighbors** command output displays an example of the neighbor table on the Cisco IOS router. Use the **show mac address-table** command to display the MAC address table on the switch.

VLAN assignment is another issue to consider when troubleshooting end-to-end connectivity. Use the **arp** Windows command to see the entry for a default gateway. Use the **show mac address-table** command to check the switch MAC table. This may show that not a VLAN assignments are correct.

Step 4. Verify the default gateway. The command output of the **show ip route** Cisco IOS command is used to verify the default gateway of a router. On a Windows host, the **route print** Windows command is used to verify the presence of the IPv4 default gateway.

In IPv6, the default gateway can be configured manually, using stateless autoconfiguration (SLAAC), or by using DHCPv6. The **show ipv6 route** Cisco IOS command is used to check for the IPv6 default route on a router. The **ipconfig** Windows command is used to verify if a PC1 has an IPv6 default gateway. The command output of the **show ipv6 interface** *interface* will tell you if a router is or is not enabled as an IPv6 router. Enable a router as an IPv6 router using the **ipv6 unicast-routing** command. To verify that a host has the default gateway set, use the **ipconfig** command on the Microsoft Windows PC or the **ifconfig** command on Linux and Mac OS X.

Step 5. Verify correct path. The routers in the path make the routing decision based on information in the routing tables. Use the **show ip route | begin Gateway** command for an IPv4 routing table. Use the **show ipv6 route** command for an IPv6 routing table.

Step 6. Verify the transport layer. Two of the most common issues that affect transport layer connectivity include ACL configurations and NAT configurations. A common tool for testing transport layer functionality is the Telnet utility.

Step 7. Verify ACLs. Use the **show ip access-lists** command to display the contents of all IPv4 ACLs and the **show ipv6 access-list** command to show the contents of all IPv6 ACLs configured on a router. Verify which interface has the ACL applied using the **show ip interfaces** command.

Step 8. Verify DNS. To display the DNS configuration information on the switch or router, use the **show running-config** command. Use the **ip host** command to enter name to IPv4 mapping to the switch or router as shown in the command output.

12.6.4 Module Quiz – Network Troubleshooting

Download Slide Powerpoint (PPT)

CCNA 3 v7.0 Curriculum: Module 12 - Network Troubleshooting.pptx

1 file(s) 1.74 MB

Download

Tags:ccna 3 v7 modules