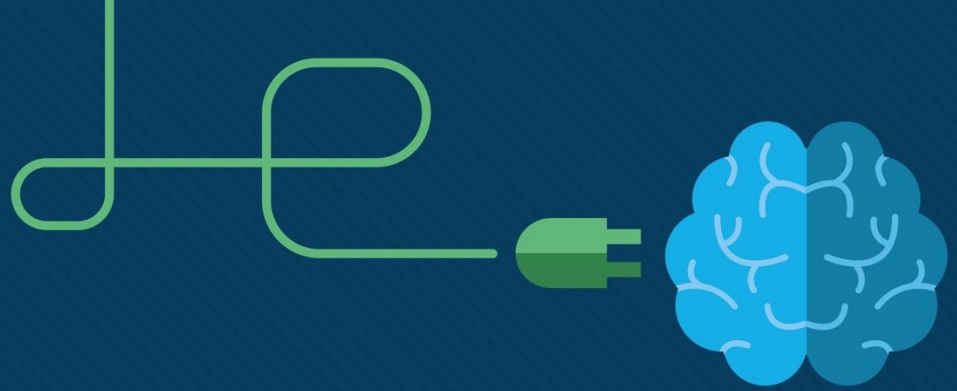


Chapter 8: Network Troubleshooting

CCNA Routing and Switching

Connecting Networks v6.0

Chapter 8 - Sections & Objectives

- 8.1 Troubleshooting Methodology
  - Explain troubleshooting approaches for various network problems.
    - Explain how network documentation is developed and used to troubleshoot network issues.
    - Describe the general troubleshooting process.
    - Compare troubleshooting methods that use a systematic, layered approach.
- 8.2 Troubleshooting Scenarios
  - Troubleshoot end-to-end connectivity in a small to medium-sized business network, using a systematic approach.
    - Use an ICMP echo-based IP SLA to troubleshoot network connectivity issues.
    - Describe different networking troubleshooting tools.
    - Determine the symptoms and causes of network problems using a layered model.
    - Troubleshoot a network using the layered model.

8.1 Troubleshooting Methodology

Documenting the Network

Router Documentation

Device Name, Model	Interface Name	MAC Address	IPv4 Address	IPv6 Addresses	IP Routing Protocols
R1, Cisco 1941, c1900-universalk9-mz.SPA.154-3.M2.bin	G0/0	0007.8580.a159	192.168.10.1 /24	2001:db8:cafe:10::1/64 fe80::1	EIGRPv4 10 EIGRPv6 20
	G0/1	0007.8580.a160	192.168.11.1 /24	2001:db8:cafe:11::1/64 fe80::1	EIGRPv4 10 EIGRPv6 20
	S0/0/0	N/A	10.1.1.1/30	2001:db8:acad:20::1/64 fe80::	EIGRPv4 10 EIGRPv6 20
R2, Cisco 1941, c1900-universalk9-mz.SPA.152-4.M1	S0/0/0	N/A	10.1.1.2/30	2001:db8:acad:20::2/64 fe80::2	EIGRPv4 10 EIGRPv6 20

- For troubleshooting purposes, network administrators must have a complete set of accurate and current network documentation which includes:
  - Configuration files, including network configure files and end-system configuration files
  - Physical and logical topology diagrams
  - Baseline performance levels
- Network Configuration files should contain all relevant information about any devices including:
  - Type of device, model designation
  - IOS image name
  - Device network hostname
  - Location of the device
  - If modular, include module/slot info

Documenting the Network (Cont.)

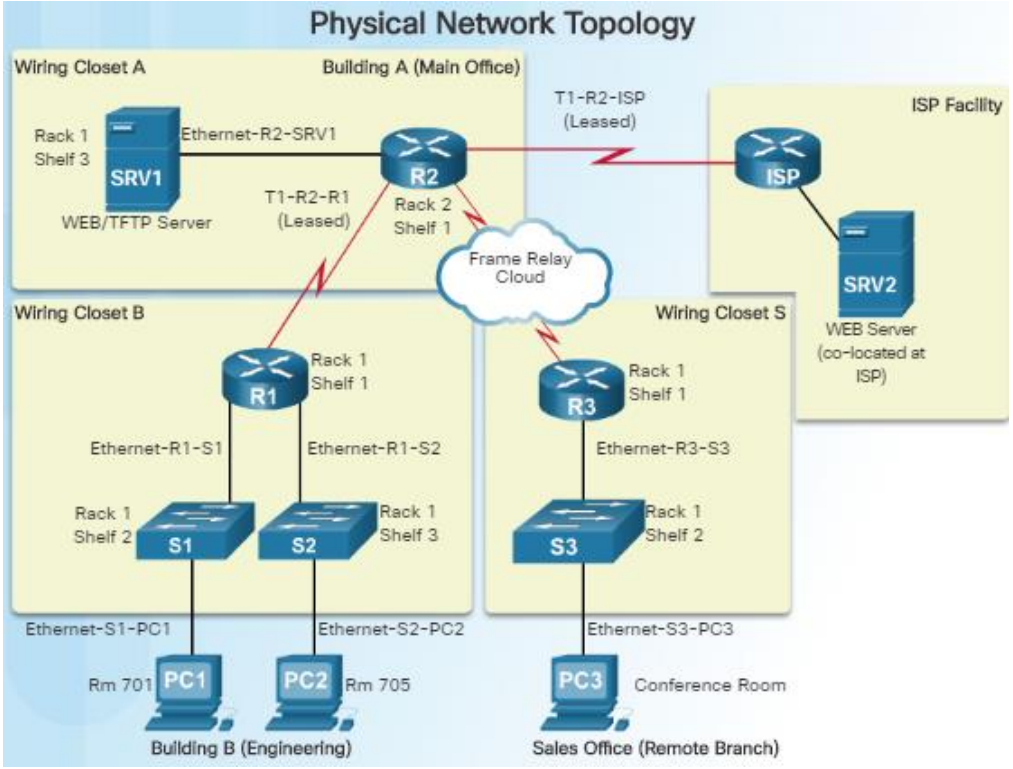
Router Documentation

Device Name, Model	Interface Name	MAC Address	IPv4 Address	IPv6 Addresses	IP Routing Protocols
R1, Cisco 1941, c1900-universalk9-mz.SPA.154-3.M2.bin	G0/0	0007.8580.a159	192.168.10.1 /24	2001:db8:cafe:10::1/64 fe80::1	EIGRPv4 10 EIGRPv6 20
	G0/1	0007.8580.a160	192.168.11.1 /24	2001:db8:cafe:11::1/64 fe80::1	EIGRPv4 10 EIGRPv6 20
	S0/0/0	N/A	10.1.1.1/30	2001:db8:acad:20::1/64 fe80::	EIGRPv4 10 EIGRPv6 20
R2, Cisco 1941, c1900-universalk9-mz.SPA.152-4.M1	S0/0/0	N/A	10.1.1.2/30	2001:db8:acad:20::2/64 fe80::2	EIGRPv4 10 EIGRPv6 20

- If modular, include module/slot info
- Data link and network layer addresses
- Any additional important information about physical aspects of the device

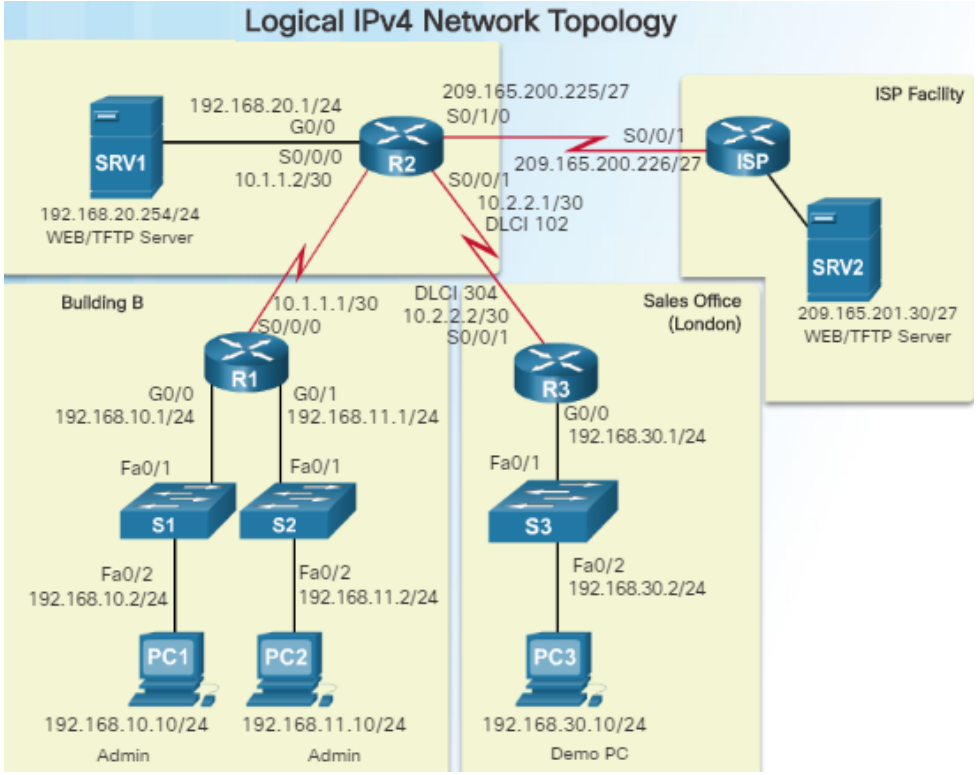
- End-system configuration files focus on the hardware and software used on end-system devices such as servers, network management consoles, and user workstations. Documentation should include:
  - Device name (purpose)
  - Operating system and version
  - IPv4 and IPv6 addresses
  - Subnet mask and prefix length
  - Default gateway and DNS server
  - Any high-bandwidth network applications used on the end system

Network Topology Diagrams



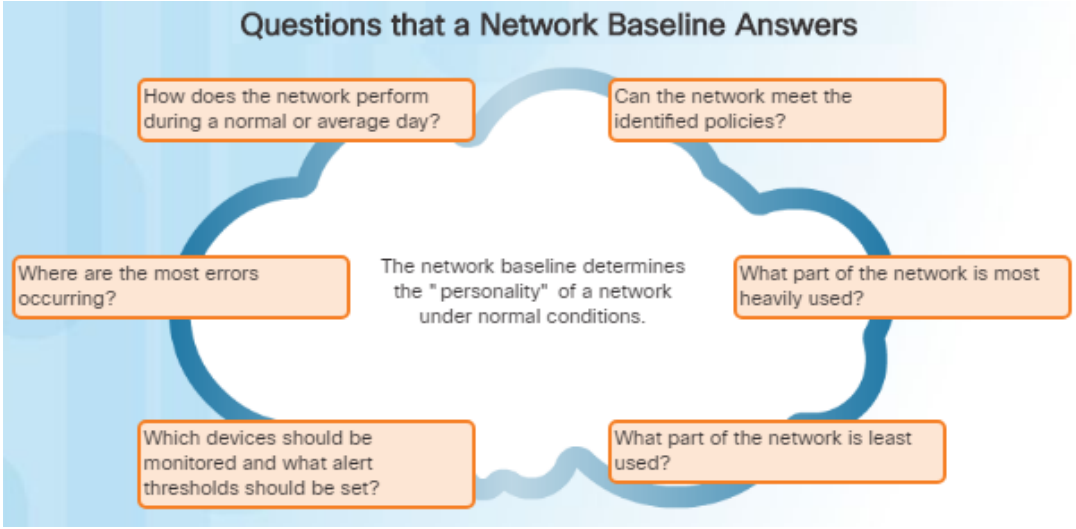
- Network topology diagrams keep track of the location, function, and status of devices on the network. There are two types of topology diagrams:
  - Physical topology
  - Logical topology
- Physical Topology network diagrams show the physical layout of the devices connected to the network and typically include:
  - Device type
  - Model and manufacturer
  - Operating System version
  - Cable type and identifier
  - Cable specification
  - Connector type
  - Cabling endpoints

Network Topology Diagrams (Cont.)



- Logical network topology diagrams illustrate how devices are logically connected to the network
- Symbols are used to represent network elements, such as routers, servers, hosts, VPN concentrators, and security devices.
- Documented information might include:
  - Device identifiers
  - IP address and prefix lengths
  - Interface identifiers
  - Connection type
  - Frame Relay DLCI for virtual circuits (if applicable)
  - Site-to-site VPNs
  - Routing protocols and static routes
  - WAN technologies used
  - Data-link protocols

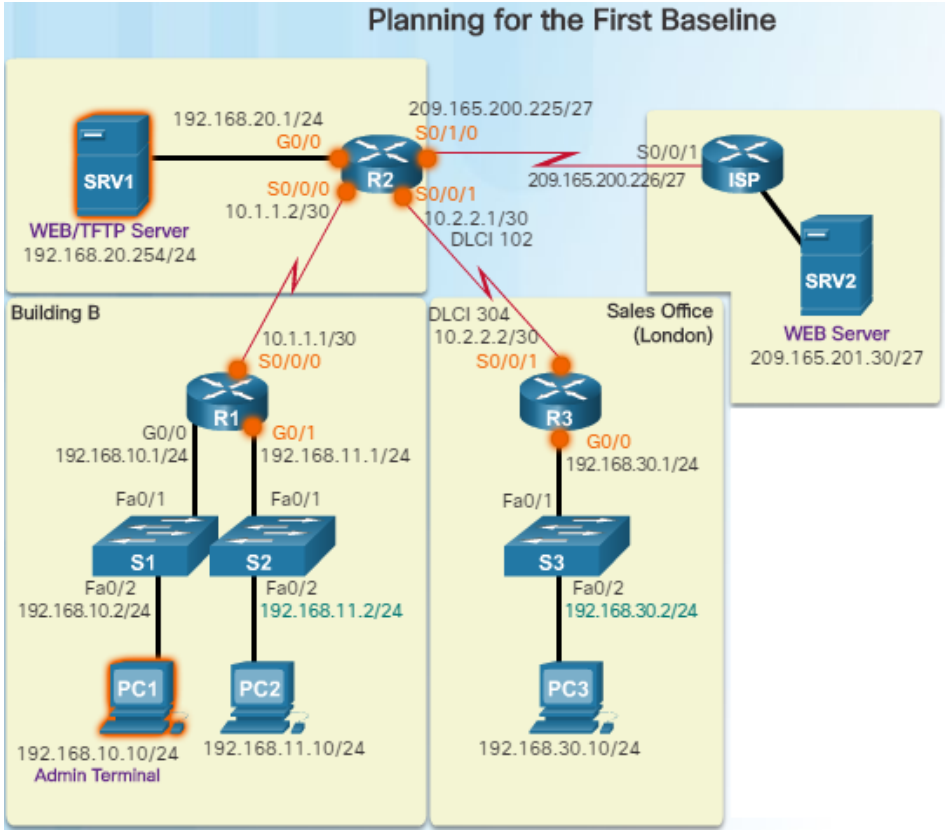
Establishing a Network Baseline



- The purpose of network monitoring is to watch network performance in comparison to a predetermined baseline.
- A network performance baseline
  - Is used to establish normal network or system performance
  - Requires collecting performance data from the ports and devices that are essential to operation
  - Allows the network administrator to determine the difference between abnormal behavior and proper network performance

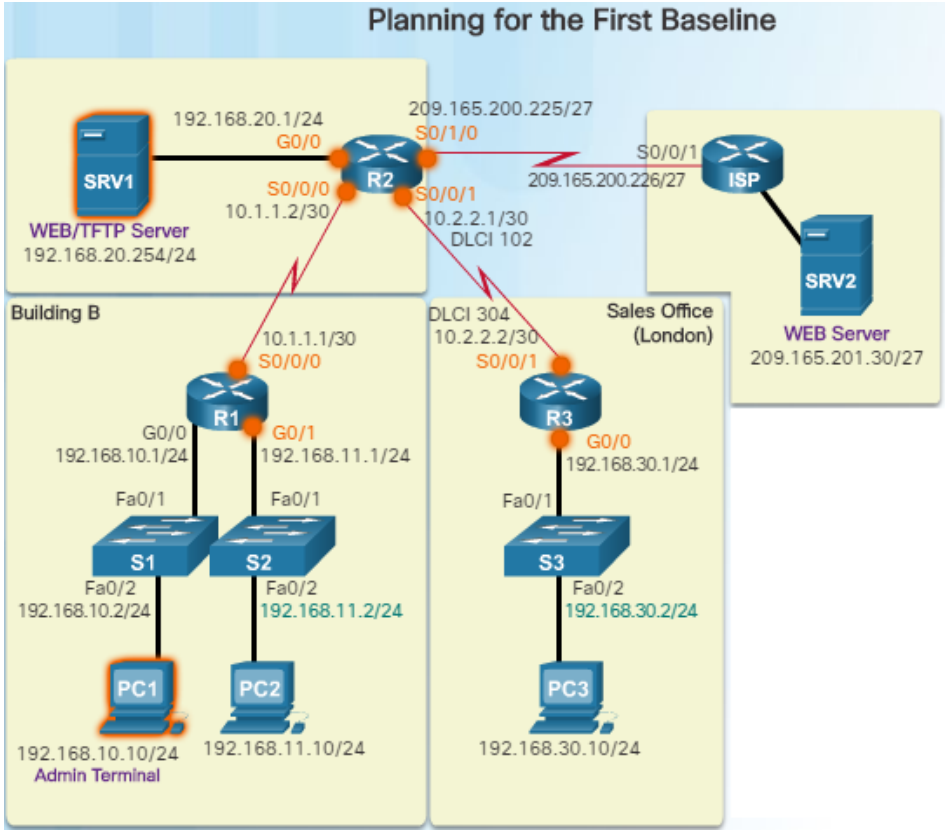
Analysis after an initial baseline also tends to reveal hidden problems. The collected data can show the true nature of congestion or potential congestion in a network.

Steps to Establish a Network Baseline



- Step 1: Determine what types of data to collect.
  - Start out with a few variables that represent the defined policy.
  - Not that capturing too many data points can be overwhelming making analysis difficult.
  - Start out simply, and fine-tune along the way.
- Step 2: Identify devices and ports of interest.
  - Use the network topology to identify key devices for which performance data should be measured.
  - Devices and ports of interest include network device ports that connect to other network devices, servers, and key users.

Steps to Establish a Network Baseline (Cont.)



- Step 3: Determine the baseline duration
  - The length of time and baseline information being gathered must be sufficient for establishing a typical picture of the network.
  - Daily trends of network traffic should be measured.
  - Monitor for trends that occur over a longer period of time such as weekly or monthly.
- Capture data trends and include:
  - Screenshots of CPU utilization trends captured over a daily, weekly, monthly, and yearly period
- Note: Baseline measurements should not be performed during times of unique traffic patterns.

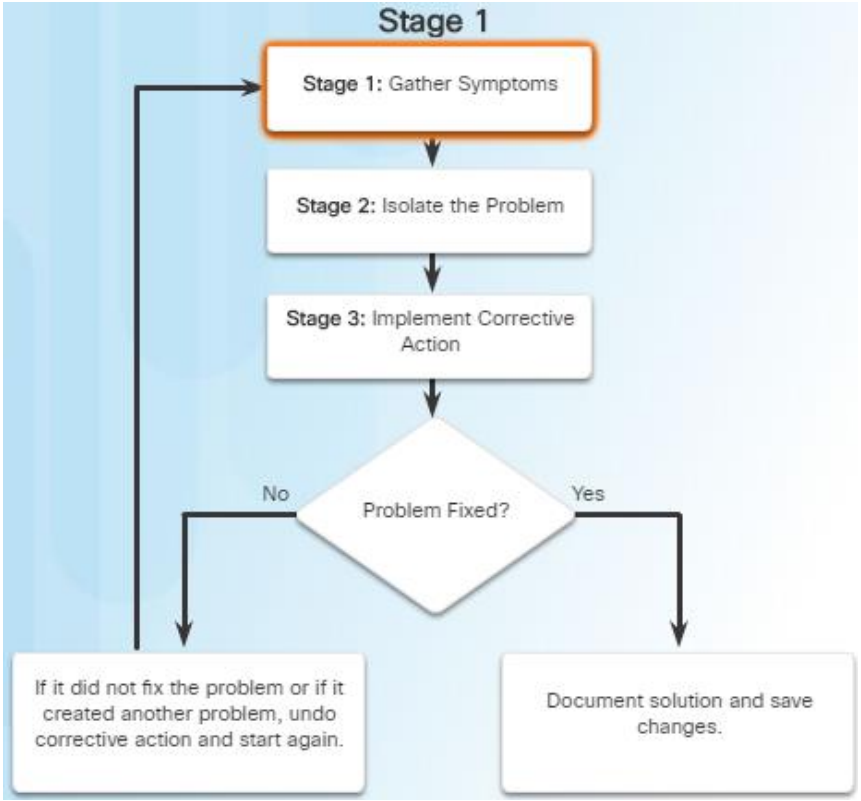
Measuring Data

Commands for Data Collection

Command	Description
`show version`	Shows uptime, version information for device software and hardware.
`show ip interface [brief]` `show ipv6 interface [brief]`	Shows all the configuration options that are set on an interface. Use the `brief` keyword to only show up/down status of IP interfaces and the IP address is of each interface.
`show interfaces [interface_type interface_num]`	Shows detailed output for each interface. To show detailed output for only a single interface, include the interface type and number in the command (e.g. gigabitethernet 0/0).
`show ip route` `show ipv6 route`	Shows the contents of the routing table.
`show arp` `show ipv6 neighbors`	Shows the contents of the ARP table (IPv4) and the neighbor table (IPv6).
`show running-config`	Shows current configuration.
`show port`	Shows the status of ports on a switch.
`show vlan`	Shows the status of VLANs 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.
`show ip cache flow`	Displays a summary of the NetFlow accounting statistics.

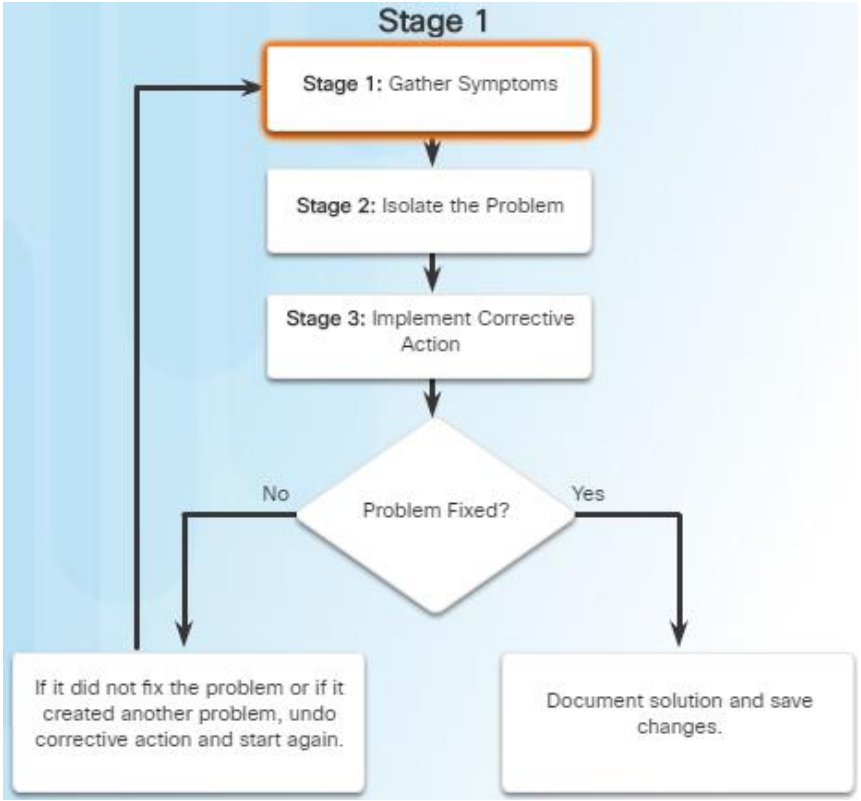
- When documenting the network, it is necessary to gather information directly from routers and switches.
- **Ping**, **traceroute**, and **telnet** are useful commands to document.
- The figure to the left lists some of the most common Cisco IOS **show** commands used for data collection.
- Manual data collection using **show** commands on individual network devices is very time consuming and is not a scalable solution. This should be reserved for smaller networks or mission critical devices.
- Sophisticated network management software is typically used to baseline large and complex networks.

General Troubleshooting Procedures



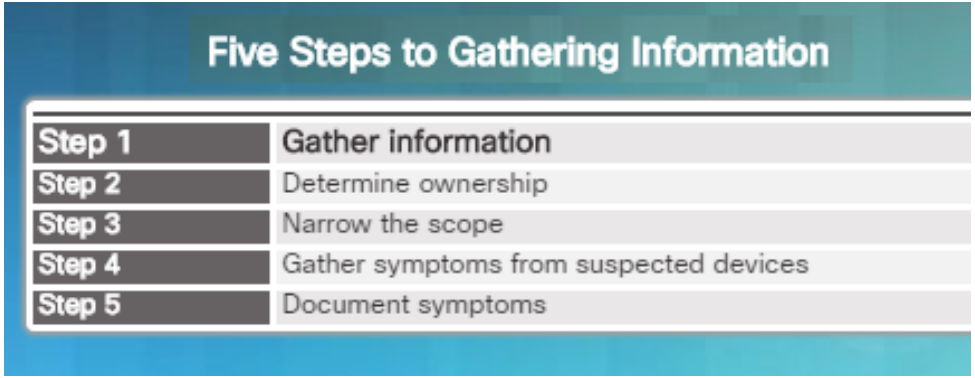
- Using efficient troubleshooting techniques shortens overall troubleshooting time.
- There are three major stages to the troubleshooting process:
- Stage 1. Gather symptoms –
  - Gather and document symptoms from the network, end systems, and users.
  - The network administrator determines which network components have been affected and how the functionality of the network has changed in comparison to the baseline.
  - Symptoms may come from the network management system, console messages, and user complaints.
  - Ask questions and investigate the issue in order to localize the problem to a smaller range of possibilities.

General Troubleshooting Procedures (Cont.)



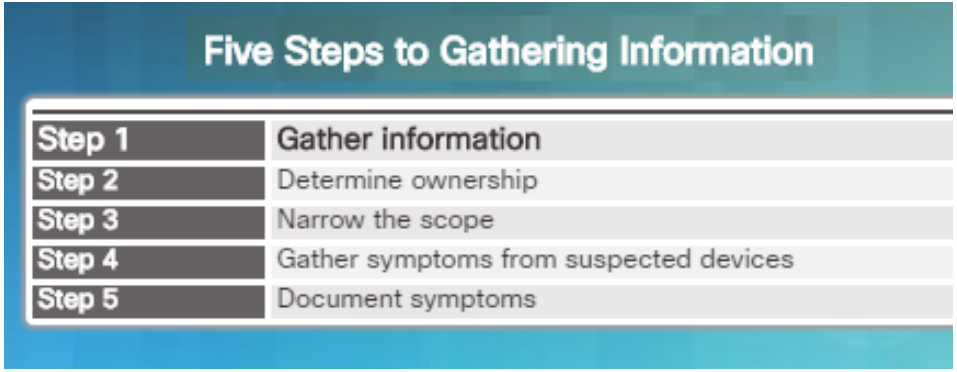
- Stage 2. Isolate the problem –
  - Isolating is the process of eliminating variables until a single problem, or a set of related problems has been identified as the cause.
  - The network administrator should examine the problems at the logical layer of the network so that the most likely cause can be detected.
- Stage 3. Implement corrective action –
  - After identifying the cause of the problem, the network administrator works to correct the problem by implementing, testing, and documenting possible solutions.
  - Can the solution be implemented immediately, or does it need to be postponed?
  - The severity of the problem should be weighed against the impact of the solution.

Gathering Symptoms



- It is important to gather facts and evidence that will allow you to progressively eliminate possible causes, and eventually identify the root cause of the issue.
- There are five information gathering steps:
- Step 1. Gather Information
  - Gather information from the trouble ticket, users, or end systems affected by the problem to form a definition of the problem.
- Step 2. Determine ownership
  - If the problem is within the control of the organization, move onto the next stage. If it is outside of the boundary of organizational control, contact an administrator for the external system.
- Step 3. Narrow the scope

Gathering Symptoms (Cont.)



- Determine if the problem is at the core, distribution, or access layer.
- At the identified layer, analyze the existing symptoms and try to determine which piece of equipment is most likely the cause.

- Step 4. Gather symptoms from suspect devices
  - Using a layered troubleshooting approach, gather hardware and software symptoms from the suspect devices.
  - Is it a hardware of software configuration problem?
- Step 5. Document symptoms
  - If the problem cannot be solved using the documented symptoms, begin the isolating stage of the general troubleshooting process.
  - Gather symptoms from devices using commands/tools including: **ping**, **traceroute**, **telnet**, **show**, **debug**, device logs and packet captures.

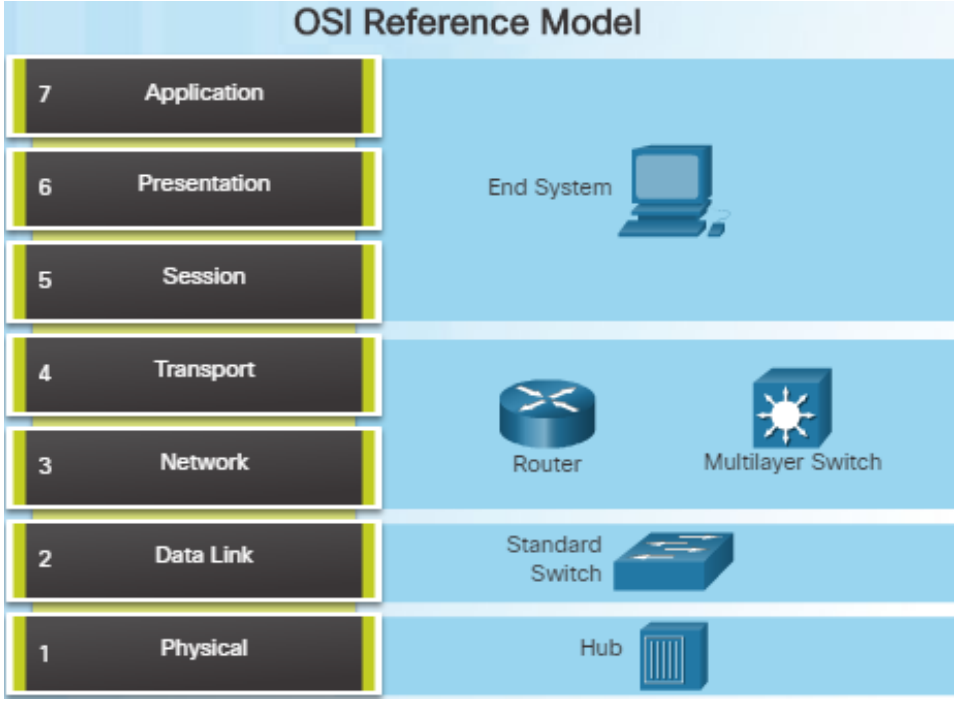
Questioning End Users

Guidelines When Questioning Users

Guidelines	Example End-user Questions
Ask questions that are pertinent to the problem.	What does not work?
Use each question as a means to either eliminate or discover possible problems.	Are the things that do work and the things that do not work related?
Speak at a technical level that the user can understand.	Has the thing that does not work ever worked?
Ask the user when the problem was first noticed.	When was the problem first noticed?
Determine if anything happened since the last time the device worked.	What has changed since the last time it did work?
Ask the user to recreate the problem, if possible.	Can you reproduce the problem?
Determine the sequence of events that took place before the problem happened.	When exactly does the problem occur?

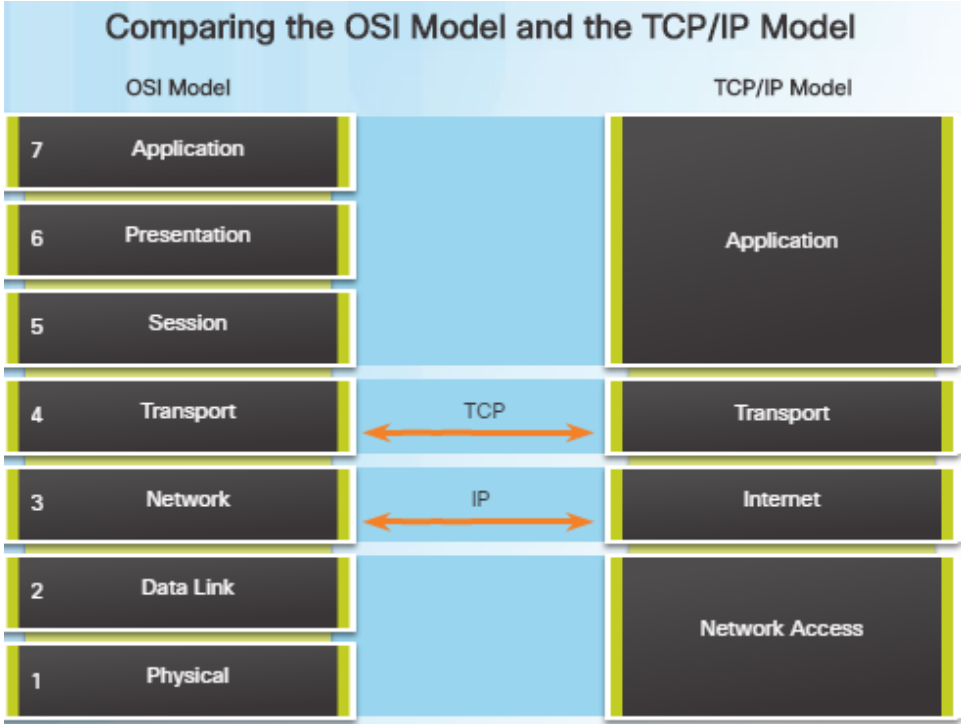
- In many cases, the problem is reported by an end user. This information may often be misleading or vague.
- This may require asking questions of end users to better help determine what the problem is.
- Use effective questioning techniques when asking the end users about a network problem they may be experiencing.
- The table to the left provides some guidelines and sample end-user questions.

Using Layered Models for Troubleshooting



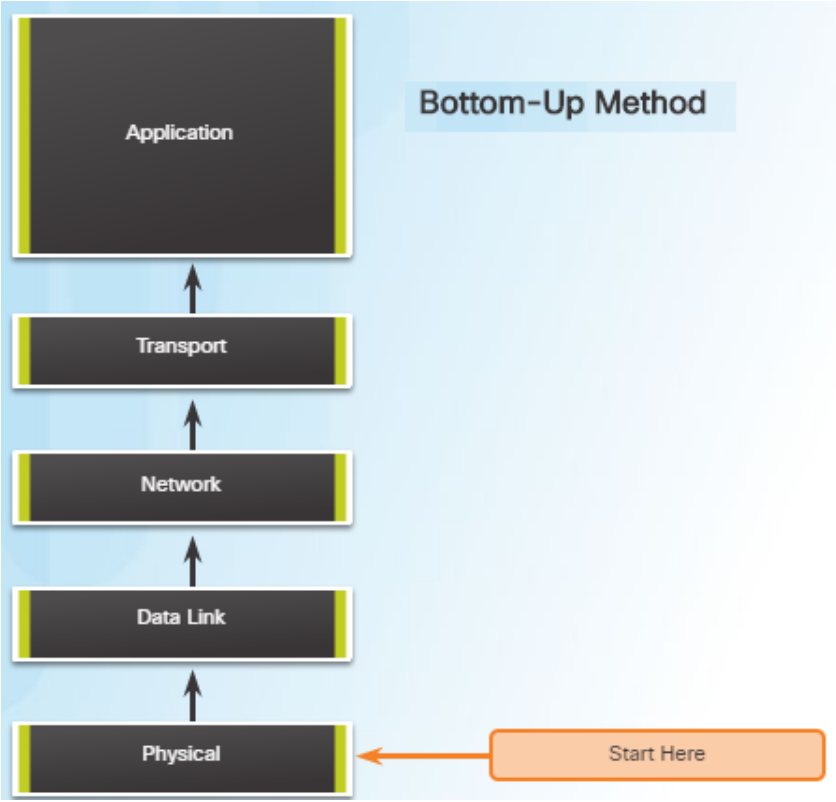
- If no solution is identified, the network administrator compares the characteristics of the problem to the logical layers of the network to isolate and solve the issue.
- The OSI reference model provides a common language for network administrators and is commonly used in troubleshooting networks.
- Problems are typically described in terms of a given OSI model layer.
- The OSI reference model describes how information from a software application in one computer moves through a network to a software application in another computer.

Using Layered Models for Troubleshooting (Cont.)



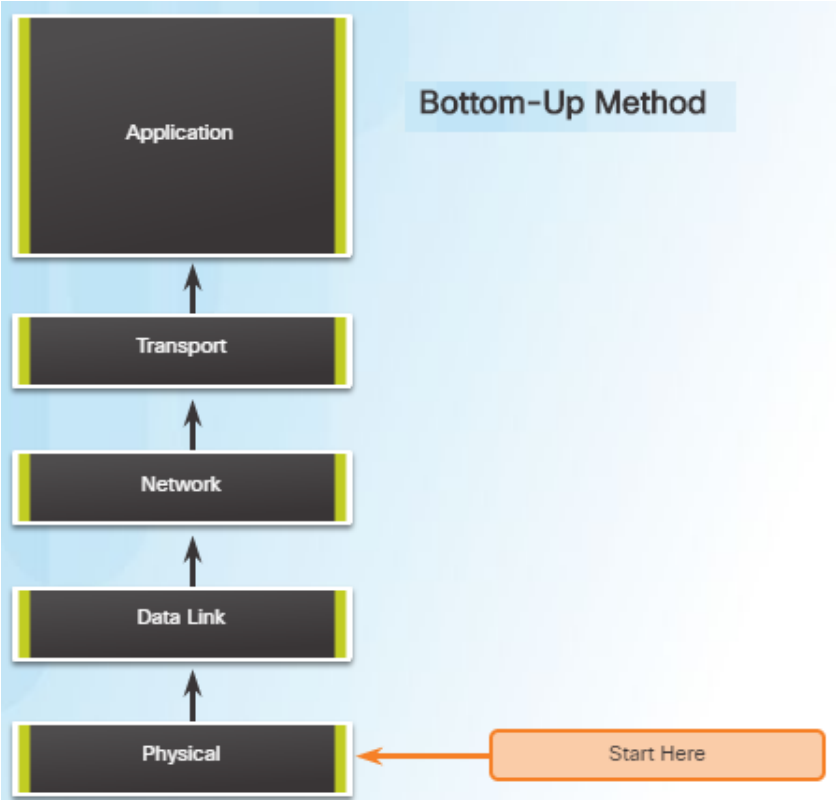
- Similar to the OSI networking model, the TCP/IP networking model also divides networking architecture into modular layers.
- The figure to the left shows how the two models map to each other.
- The application layer in the TCP/IP suite combines the functions of the three OSI model layers: session, presentation, and application.
- The TCP/IP network access layer corresponds to the OSI physical and data link layers.

Troubleshooting Methods



- Using the layered models, there are three primary methods for troubleshooting networks and each has its advantages and disadvantages:
  - Bottom-up
  - Top-down
  - Divide-and-conquer
- Bottom-up Troubleshooting Method
  - 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
  - This 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 using this method is often effective
  - The disadvantage with this method is it requires that you check every device and interface on the network until the cause of the problem is found.

Troubleshooting Methods (Cont.)

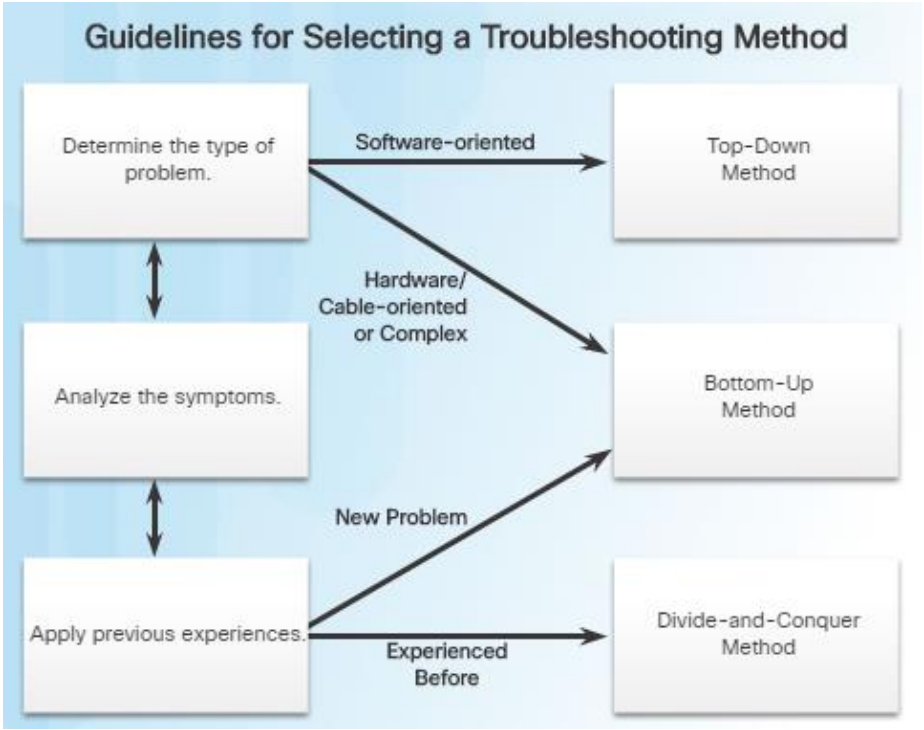


- Top-Down Troubleshooting Method
  - This method starts with troubleshooting the end-user applications and moves down through the layers of the OSI model until the cause of the problem has been identified.
  - End-user applications are tested before tackling the more specific networking pieces.
  - Use this approach for simpler problems.
  - The disadvantage is that it requires checking every network application until the problem is found.
- Divide-and-Conquer Troubleshooting Method
  - The network administrator selects a layer and tests in both directions from that layer.
  - 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.
  - If a layer is functioning properly, all layers below can be assumed to be functioning.

Other Troubleshooting Methods

- In addition to the systematic, layered approach to troubleshooting, there are also, less-structured approaches.
  - Educated guess by the network administrator
    - Guess is based on the symptoms of the problem
    - This is more successful when implemented by seasoned network administrators who can rely on their extensive knowledge and experience
  - Comparing a working and non-working situation
    - Look for differences between configurations, software versions, and hardware and other device properties.
    - This method can be helpful when the network administrator is lacking an area of expertise or when the problem needs to be resolved quickly.
  - Substitution
    - Involves swapping the problematic devices with known, working ones.
    - If the problem remains, the network administrator knows to look elsewhere.

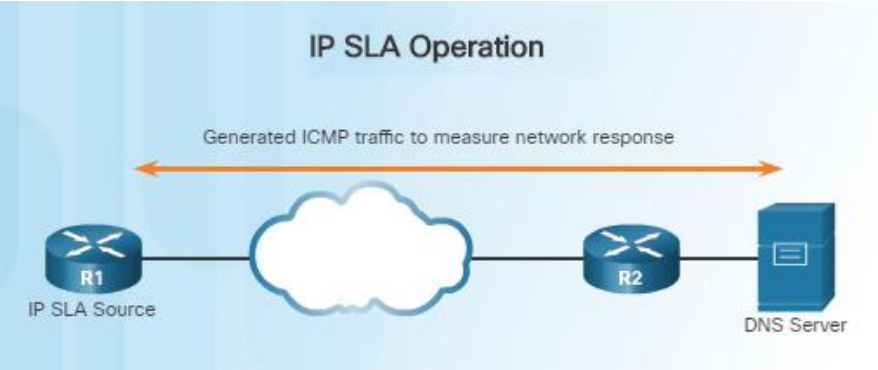
Guidelines for Selecting a Troubleshooting Method



- To quickly resolve network problems, take the time to select the most effective network troubleshooting method. An example:
  - Two IP routers are not exchanging routing information.
  - The last time this type of problem occurred, it was a protocol issue.
  - Therefore, choose the divide-and-conquer troubleshooting method.
  - Analysis reveals that there is connectivity between the routers.
  - Start the troubleshooting process at the physical or data link layer.
  - Confirm connectivity and begin testing the TCP/IP-related functions at the next layer up in the OSI model, the network layer.

8.2 Troubleshooting Scenarios

IP SLA Concepts



- In the figure above, R1 is the IP SLA source that monitors the connection to the DNS server by periodically sending ICMP requests to the server.

- Network administrators must discover network failures as early as possible.
  - A useful tool for this task is the Cisco IOS IP Service Level Agreement (SLA).
  - IP SLAs use generated traffic to measure network performance between two networking devices, multiple network locations, or across multiple network paths.
- Network engineers use IP SLAs to simulate network data and IP services to collect network performance information in real time.
- Additional benefits for using IP SLA's include:
  - SLA monitoring, measurement, and verification
  - Monitoring to provide continuous, reliable, and predictable measurements (jitter, latency, packet loss)
  - IP service network health assessment to verify that the existing QoS is sufficient for new IP services.

IP SLA Configuration

Available IP SLA Operations

```
R1# show ip sla application
        IP Service Level Agreements
Version: Round Trip Time MIB 2.2.0, Infrastructure Engine-III

Supported Operation Types:
        icmpEcho, path-echo, path-jitter, udpEcho, tcpConnect, http
        dns, udpJitter, dhcp, ftp, VoIP, icmpJitter
        802.1agEcho VLAN, Port, 802.1agJitter VLAN, Port, y1731Delay
        y1731Loss, udpApp, wspApp, mcast, generic

Supported Features:
        IPSLAs Event Publisher

IP SLAs low memory water mark: 61167610
Estimated system max number of entries: 44800

Estimated number of configurable operations: 44641
Number of Entries configured  : 0
Number of active Entries      : 0
Number of pending Entries     : 0
Number of inactive Entries    : 0
Time of last change in whole IP SLAs: *20:27:15.935 UTC Wed Jan 27 2016
```

- Instead of using **ping** manually, a network engineer can use IP SLA ICMP Echo operation to test the availability of network devices.
- The IP SLA ICMP Echo operation provides the following measurements:
  - Availability monitoring (packet loss statistics)
  - Performance monitoring (latency and response time)
  - Network operation (end-to-end connectivity)
- **show ip sla application** – this privileged EXEC mode command verifies that the desired IP SLA operation is supported on the source device.
  - The output in the figure confirms that R1 is capable of supporting IP SLA. However, there are no sessions configured.

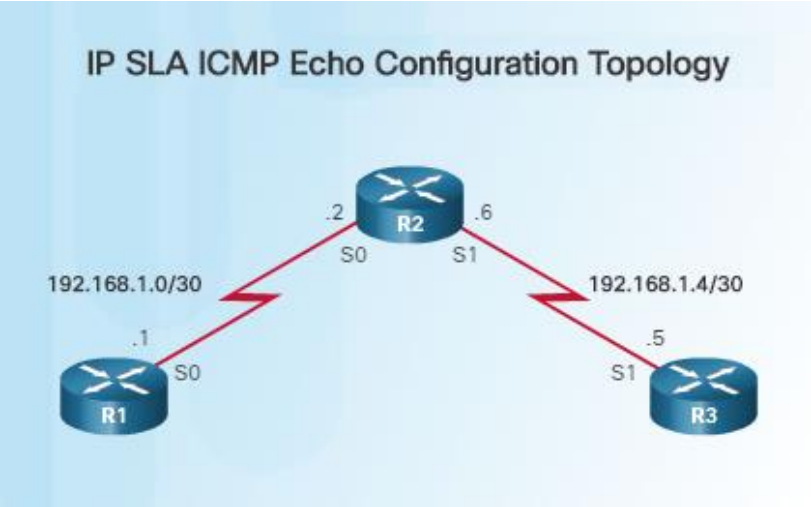
IP SLA Configuration (Cont.)

Available IP SLA Operations

```
R1# show ip sla application
       IP Service Level Agreements
Version: Round Trip Time MIB 2.2.0, Infrastructure Engine-III

Supported Operation Types:
       icmpEcho, path-echo, path-jitter, udpEcho, tcpConnect, http
       dns, udpJitter, dhcp, ftp, VoIP, icmpJitter
       802.1agEcho VLAN, Port, 802.1agJitter VLAN, Port, y1731Delay
       y1731Loss, udpApp, wspApp, mcast, generic

Supported Features:
       IPSLAs Event Publisher

IP SLAs low memory water mark: 61167610
Estimated system max number of entries: 44800

Estimated number of configurable operations: 44641
Number of Entries configured  : 0
Number of active Entries      : 0
Number of pending Entries     : 0
Number of inactive Entries    : 0
Time of last change in whole IP SLAs: *20:27:15.935 UTC Wed Jan 27 2016
```

- To create an IP SLA operation and enter IP SLA configuration mode, use the **ip sla operation-number** global configuration command.
  - The operation number is a unique number that is used to identify the operation being configured.
- From IP SLA config mode, you can configure the IP SLA operation as an ICMP Echo operation and set the frequency rate:
  - Router(config-ip-sla)# **icmp-echo** { *dest-ip-address* | *dest-hostname* } [**source-ip** { *ip-address* | *hostname* } | **source-interface** *interface-id*]
  - Router(config)# **ip sla schedule** *operation-number* [**life** { **forever** | *seconds* }] [**start-time** { *hh* : *mm* [: *ss*] [*month day* | *day month*] | **pending** | **now** | **after** *hh:mm:ss*] [**ageout** *seconds*] [**recurring**]

Sample IP SLA Configuration




```
R1# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)# ip sla 1
R1(config-ip-sla)# icmp-echo 192.168.1.5
R1(config-ip-sla-echo)# frequency 30
R1(config-ip-sla-echo)# exit
R1(config)# ip sla schedule 1 start-time now life forever
R1(config)# end
R1#
```

- To help understand how to configure a simple IP SLA, refer to the figure and configuration commands to the left.
- The configuration commands demonstrate how to configure an IP SLA operation with an operation number of 1.
  - Multiple IP SLA operations may be configured on a device. Each operation can be referred to by its operation number.
  - The **icmp-echo** command identifies the destination address to be monitored.
  - The **frequency** command is setting the IP SLA rate to 30 second intervals.
- The **ip sla schedule** command is scheduling the IP SLA operation number 1 to start immediately and continue until manually cancelled.

Verifying an IP SLA Configuration

Verifying IP SLA Configuration

```
R1# show ip sla configuration
IP SLAs Infrastructure Engine-III
Entry number: 1
Owner:
Tag:
Operation timeout (milliseconds): 5000
Type of operation to perform: icmp-echo
Target address/Source address: 192.168.1.5/0.0.0.0
Type Of Service parameter: 0x0
Request size (ARR data portion): 28
Verify data: No
Vrf Name:
Schedule:
  Operation frequency (seconds): 30 (not considered if randomly scheduled)
  Next Scheduled Start Time: Start Time already passed
  Group Scheduled : FALSE
  Randomly Scheduled : FALSE
  Life (seconds): Forever
  Entry Ageout (seconds): never
  Recurring (Starting Everyday): FALSE
  Status of entry (SNMP RowStatus): Active
Threshold (milliseconds): 5000
Distribution Statistics:
  Number of statistic hours kept: 2
  Number of statistic distribution buckets kept: 1
  Statistic distribution interval (milliseconds): 20
Enhanced History:
```

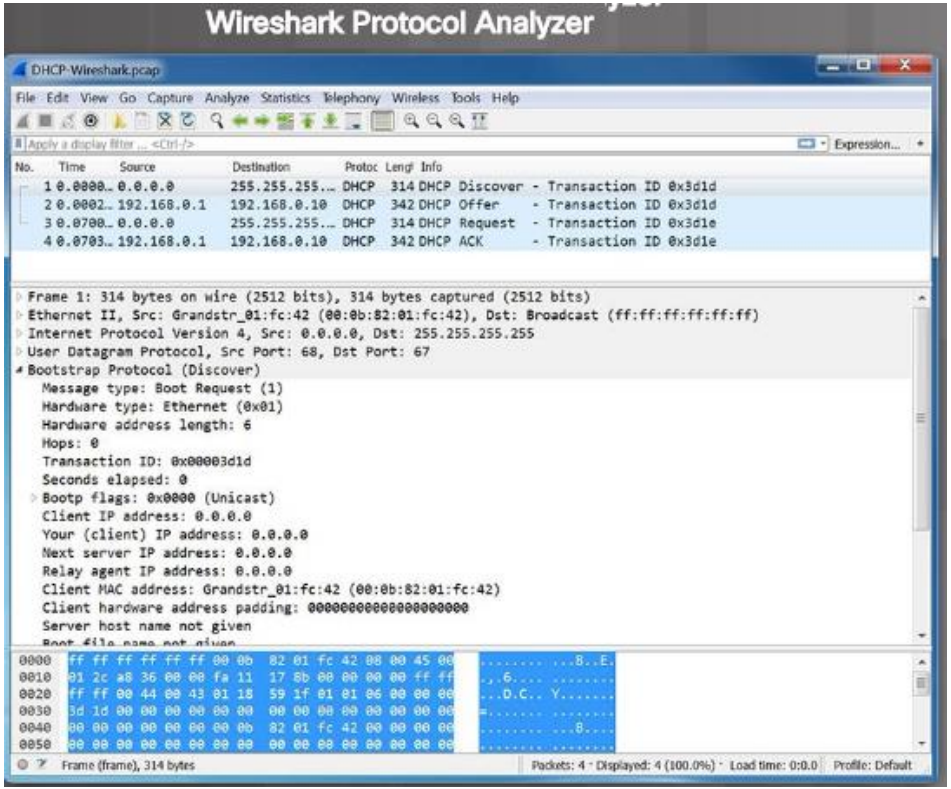
- Use the **show ip sla configuration** *operation-number* command to display configuration values
- In the figure to the left, the **show ip sla configuration** command displays the IP SLA ICMP Echo configuration.
- Use the **show ip sla statistics** [*operation-number*] command to display the IP SLA operation monitoring statistics.

```
R1# show ip sla statistics
IPSLAs Latest Operation Statistics

IPSLA operation id: 1
       Latest RTT: 12 milliseconds
Latest operation start time: 00:12:31 UTC Wed Jan 27 2016
Latest operation return code: OK
Number of successes: 57
Number of failures: 0
Operation time to live: Forever
```

Software Troubleshooting Tools

- Common software troubleshooting tools include these:
  - Network Management System Tools
    - NMS tools include device-level monitoring, configuration, and fault-management tools.
    - These graphical tools can be used to investigate and correct network problems.
  - Knowledge Bases
    - On-line network device vendor knowledge bases are very useful.
    - When vendor-based knowledge bases are combined with Internet search engines, a network administrator has access to a vast pool of experience-based information.
  - Baselining Tools
    - Many tools for automating the network documentation and baselining process are available. For example:
    - SolarWinds Network Performance Monitor

Protocol Analyzers



- Protocol analyzers are useful to investigate packet content while the content is flowing through the network.
- A protocol analyzer decodes the various protocol layers in a recorded frame and presents it in an easy to use format.
- The figure to the left shows a screen capture of the Wireshark protocol analyzer.
- Most protocol analyzers can filter traffic that meets certain criteria. For example, all traffic to and from a particular device can be captured.
- Protocol analyzers are very helpful in troubleshooting network performance problems.

Hardware Troubleshooting Tools

- There are multiple types of hardware troubleshooting tools including:
  - Digital Multimeters are test instruments that are used to directly measure electrical values of voltage, current, and resistance.
  - Cable Testers are specialized handheld devices designed for testing the various types of data communication cabling. They can be used to detect broken wires, crossed-over wiring, shorted connections, and improperly paired connections. More expensive time-domain reflectometers (TDRs) are used to pinpoint the distance to a break in a cable.
  - Cable Analyzers are multifunctional handheld devices that are used to test and certify copper and fiber cables for different services and standards.

Hardware Troubleshooting Tools (Cont.)

- Portable Network Analyzers 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 devices is connected.
  - They can also see the average and peak utilization as well as the VLAN configuration.
- Network Analysis Module – The Cisco NAM is a device or software.
  - It provides an embedded browser-based interface that generates reports on the traffic that consumes critical network resources.
  - The NAM can capture and decode packets and track response times to pinpoint an application problem to a particular network or server.

Troubleshooting Tools
Using a Syslog Server for Troubleshooting

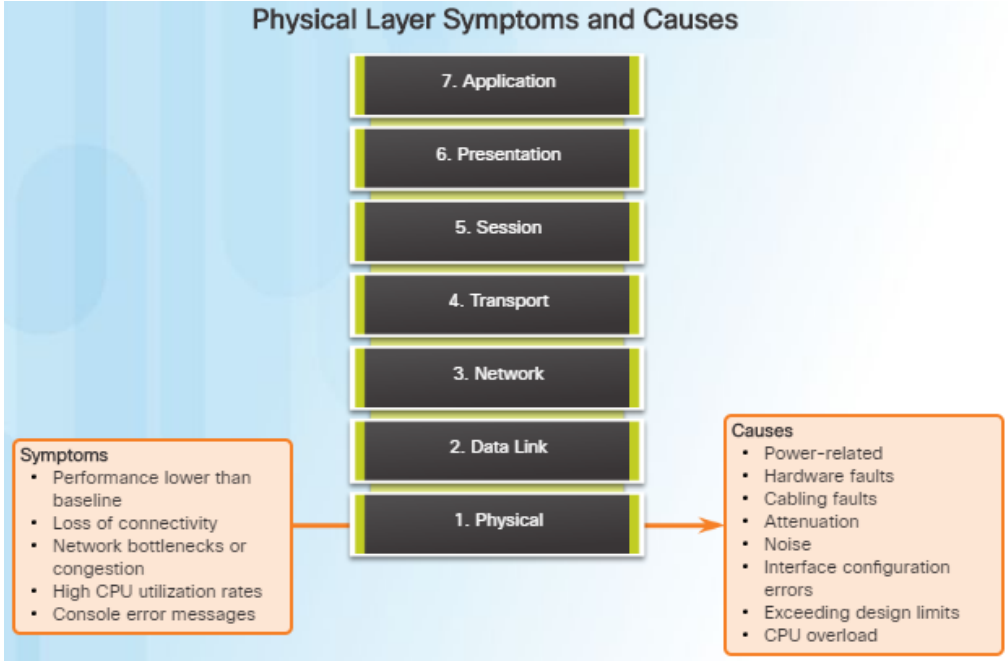
Severity Levels

	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
	5	notifications	Normal (but significant) condition	LOG_NOTICE
	6	informational	Informational messages only	LOG_INFO
Lowest Level	7	debugging	Debugging messages	LOG_DEBUG

- Cisco devices can send log messages to several different facilities including:
  - Console
  - Terminal lines
  - Buffered logging
  - SNMP traps
  - External Syslog service

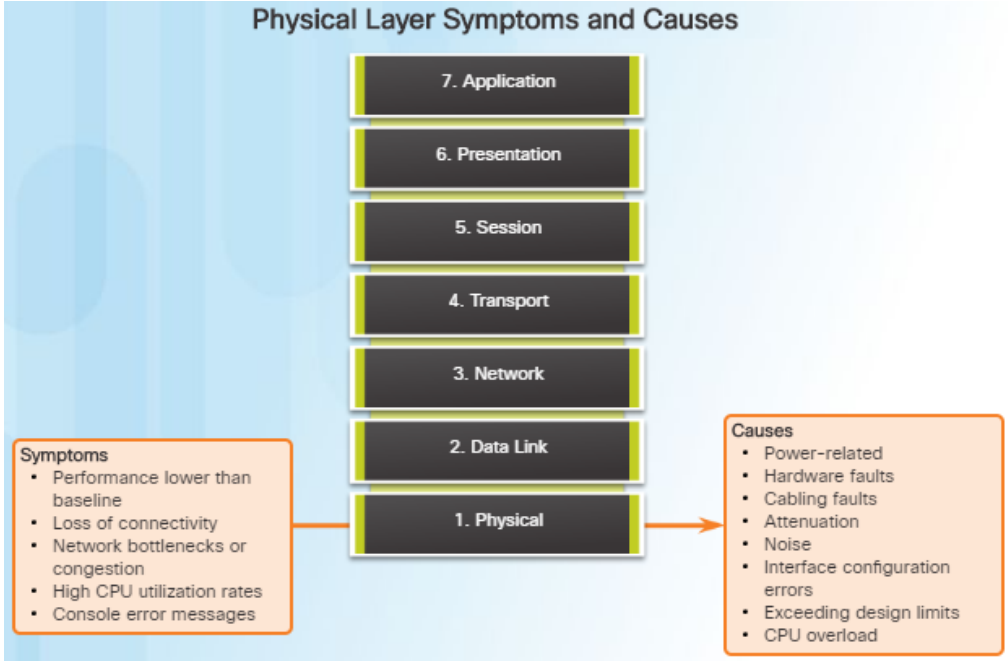
- Syslog is a simple protocol used by an IP device known as a syslog client to send text-based log messages to another IP device known as the syslog server.
- Implementing a logging facility is a very important part of network security and also for network troubleshooting.
- Cisco devices can log various types of information including configuration changes, ACL violations, interface status, and many other types of events.
- Cisco IOS log messages fall into one of eight levels as shown in the figure to the left. The lower the level number, the higher the severity level.

Physical Layer Troubleshooting



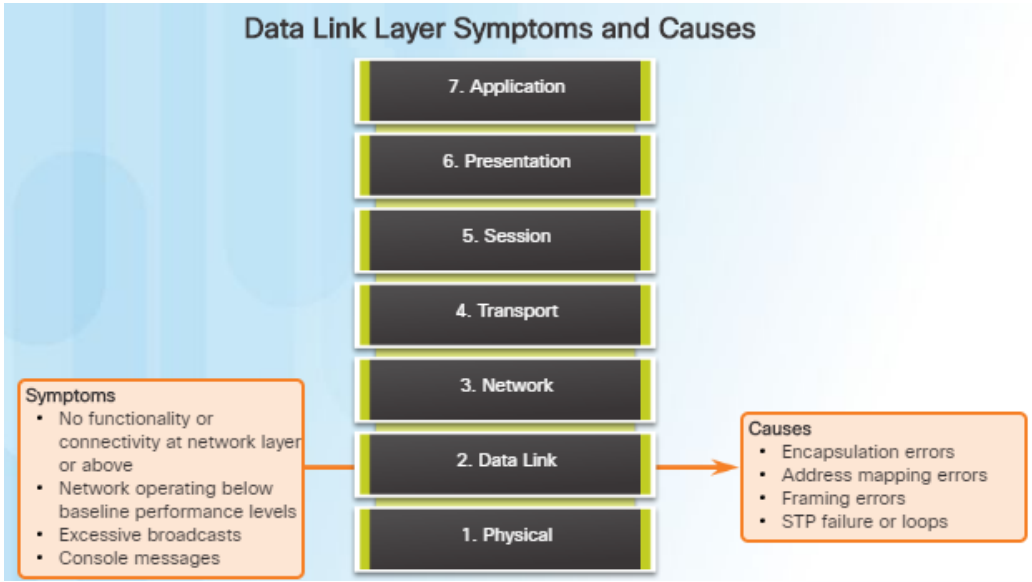
- The physical layer is the only layer with physically tangible properties, such as wires, cards, and antennas.
- Issues on a network often present as performance problems.
- Because the upper layers of the OSI model depend on the physical layer to function, a network administrator must have the ability to effectively isolate and correct problems at this layer.
- Common symptoms of network problems at the physical layer include:
  - Performance lower than baseline
  - Loss of connectivity
  - Network bottlenecks or congestion
  - High CPU utilization rates
  - Console error messages

Physical Layer Troubleshooting (Cont.)



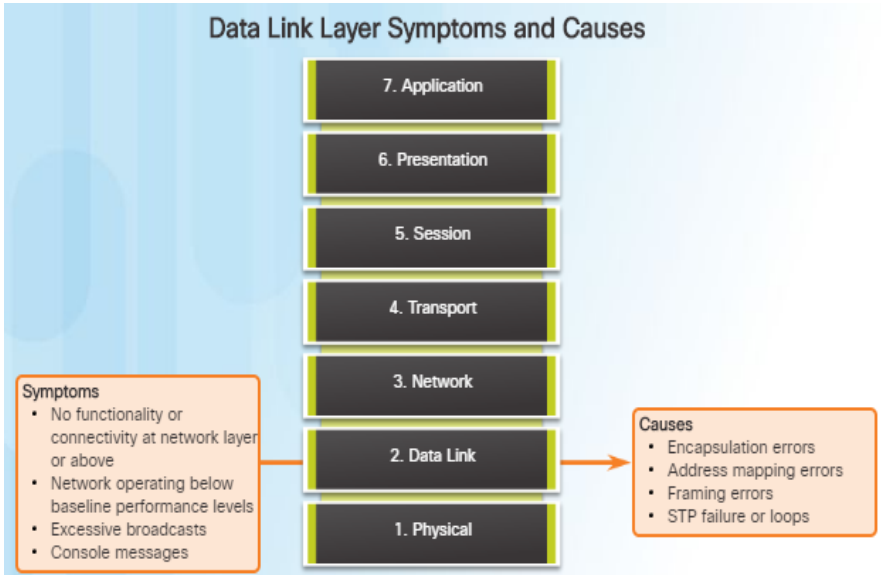
- Issues that commonly cause network problems at the physical layer include:
  - Power-related
  - Hardware faults
  - Cabling faults
  - Attenuation
  - Noise
  - Interface-configuration errors
  - Exceeding design limits
  - CPU overload

Data Link Layer Troubleshooting



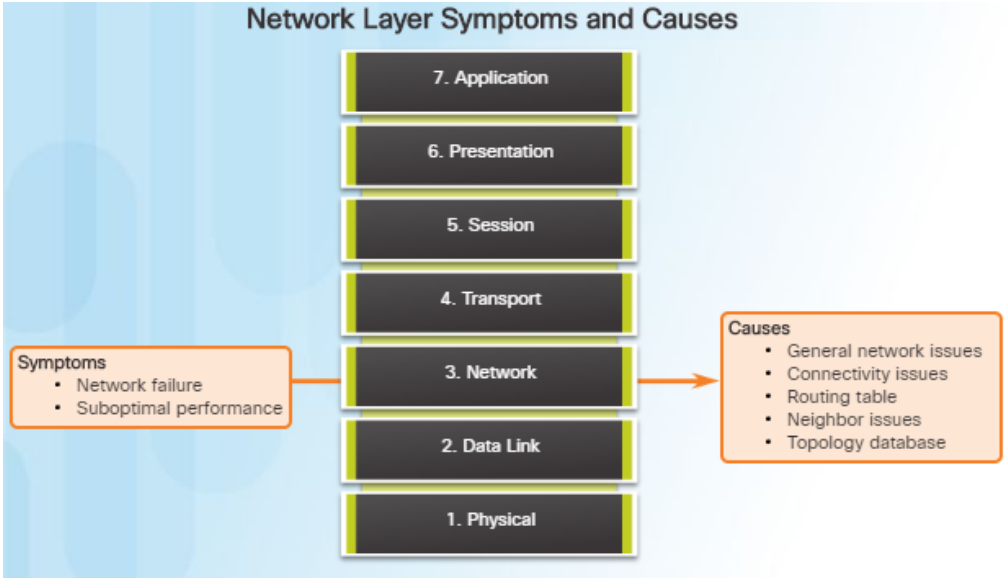
- Troubleshooting Layer 2 problems can be a challenging process.
- Layer 2 problems cause specific symptoms that, when recognized, will help identify the problem quickly:
  - No functionality or connectivity at the network layer or above
  - Network is operating below baseline performance levels
  - Excessive broadcasts
  - Most common Layer 2 console message is: “line protocol down”

Data Link Layer Troubleshooting (Cont.)



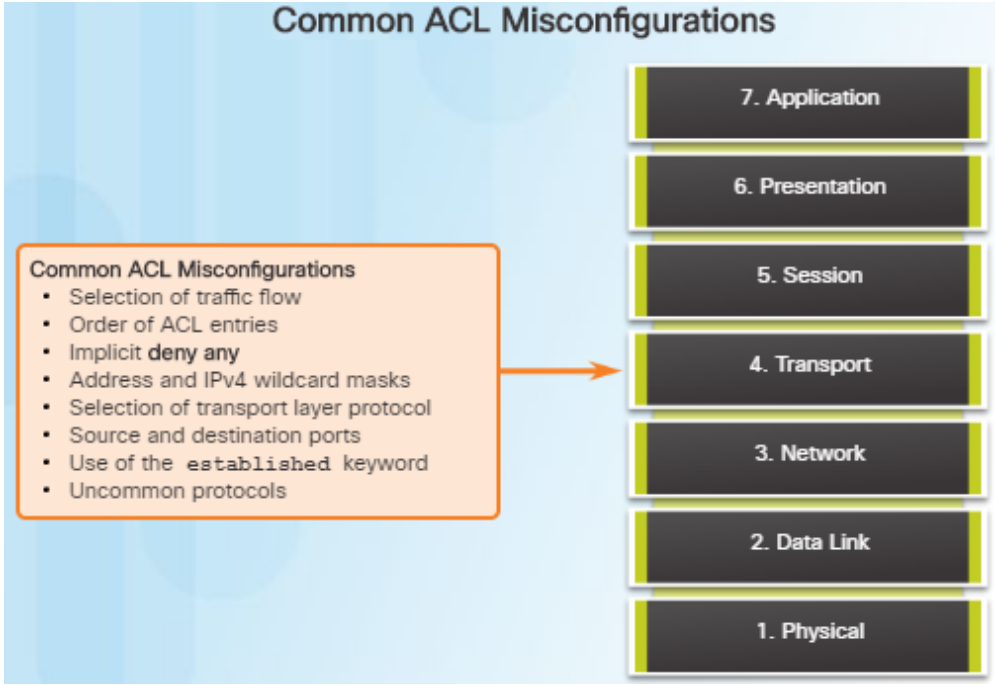
- Issues at the data link layer that commonly result in network connectivity or performance problems include these:
  - Encapsulation errors
    - Encapsulation at one end of a WAN link is configured differently from that on the other end.
  - Address mapping errors
    - In a point-to-multipoint or broadcast Ethernet topology, it is essential that an appropriate Layer 2 destination address be given to the frame.
  - Framing errors
    - A framing error occurs when a frame does not end on an 8-bit byte boundary.
  - Spanning Tree Protocol (STP) failures or loops.
    - 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.

Network Layer Troubleshooting



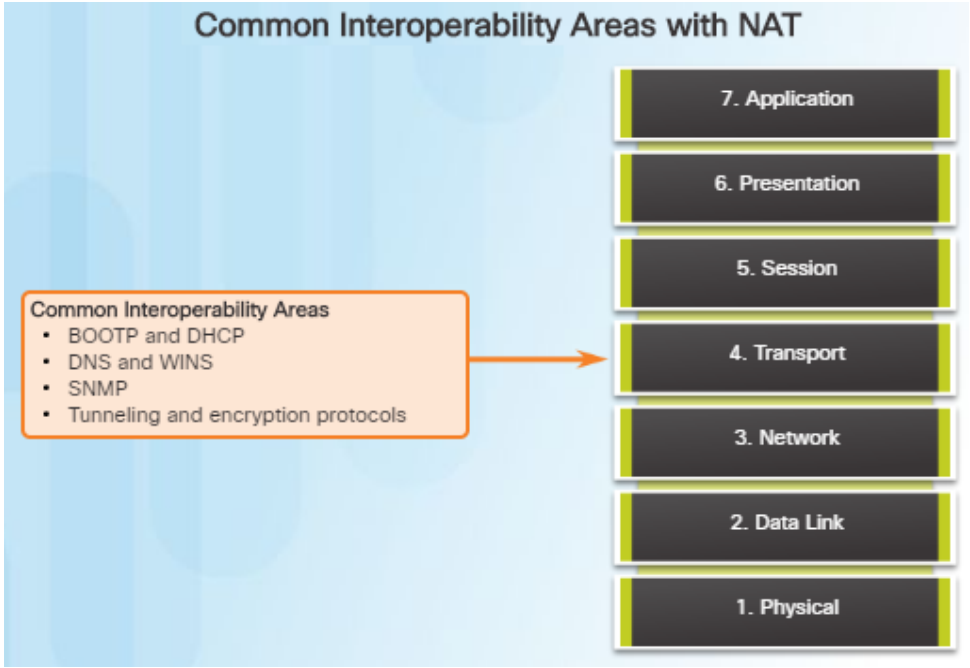
- Network layer problems include any problem that involves a Layer 3 protocol (routed or routing protocols)
- Common symptoms of network layer problems:
  - Network failure
  - Suboptimal performance
- Areas to explore when diagnosing a possible problem involving routing protocols:
  - General network issues
  - Connectivity issues – Also check for Layer 1 or power issues
  - Routing table issues – use **debug**
  - Neighbor issues – check for adjacencies if used
  - Check the routing table topology database

Transport Layer Troubleshooting - ACLs



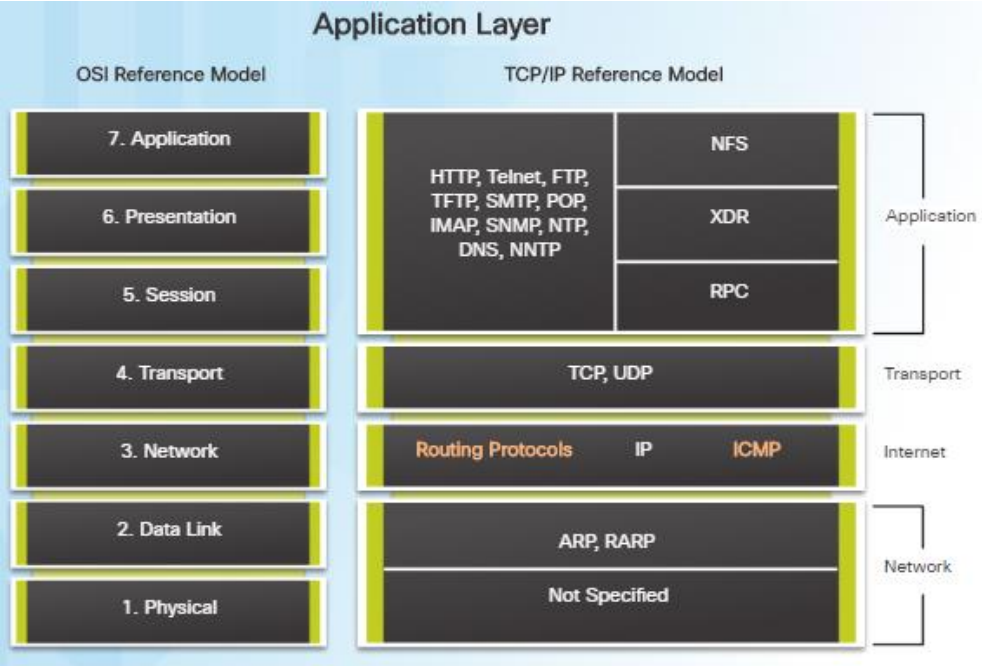
- Network problems can arise from transport layer problems on the router. Improper ACL configuration issues might include:
  - Wrong selection of traffic flow (inbound/outbound)
  - Incorrect order of access control entries
  - Implicit **deny any**
  - Misconfiguration of addresses and IPv4 wildcard masks
  - Selecting both UDP and TCP protocols when unsure
  - Incorrect source and destination ports
  - Incorrect use of the **established** keyword
  - Misconfiguration of uncommon protocols such as VPN and encryption protocols

Transport Layer Troubleshooting – NAT for IPv4



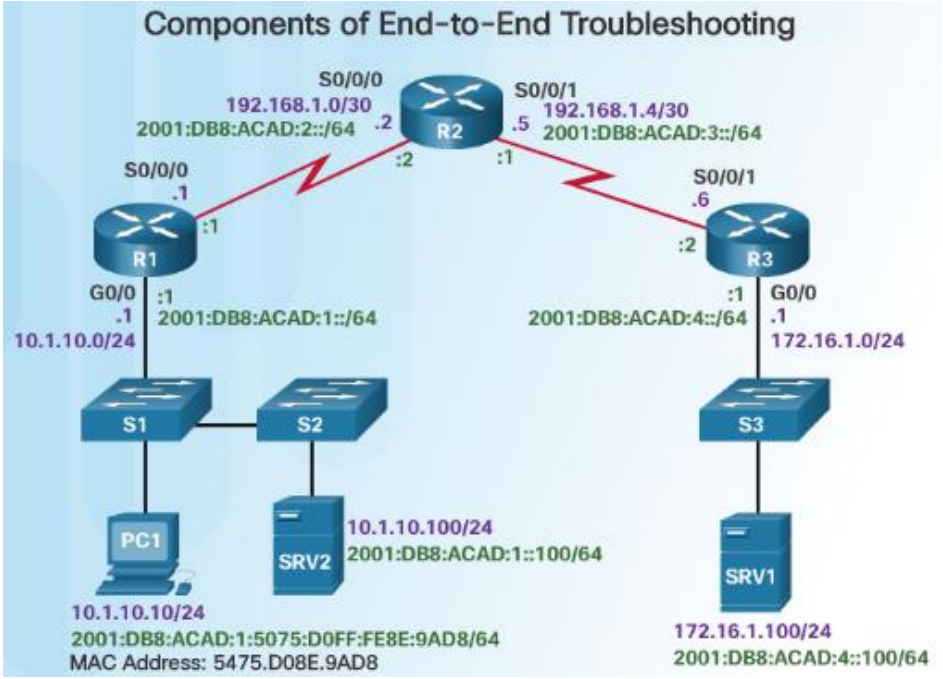
- There are a number of problems with NAT such as not interacting with services like DHCP and tunneling.
- These can include misconfigured NAT inside, NAT outside, or a misconfigured ACL.
- Other issues include interoperability with other network technologies including:
  - BOOTP and DHCP
  - DNS
  - SNMP
  - Tunneling and encryption protocols

Application Layer Troubleshooting



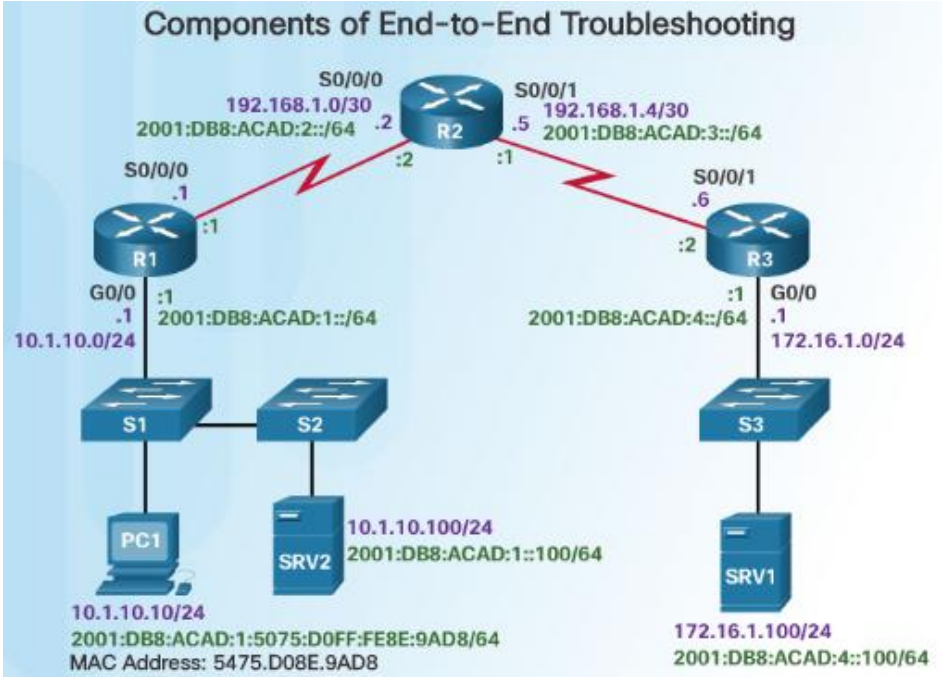
- Most of the application layer protocols provide user services for network management, file transfer, distributed file services, terminal emulation, and email.
- The most widely known and implemented TCP/IP application layer protocols include:
  - SSH/Telnet, HTTP, FTP, TFTP
  - SMTP, POP, SNMP, DNS, NFS
- 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.

Components of Troubleshooting End-to-End Connectivity



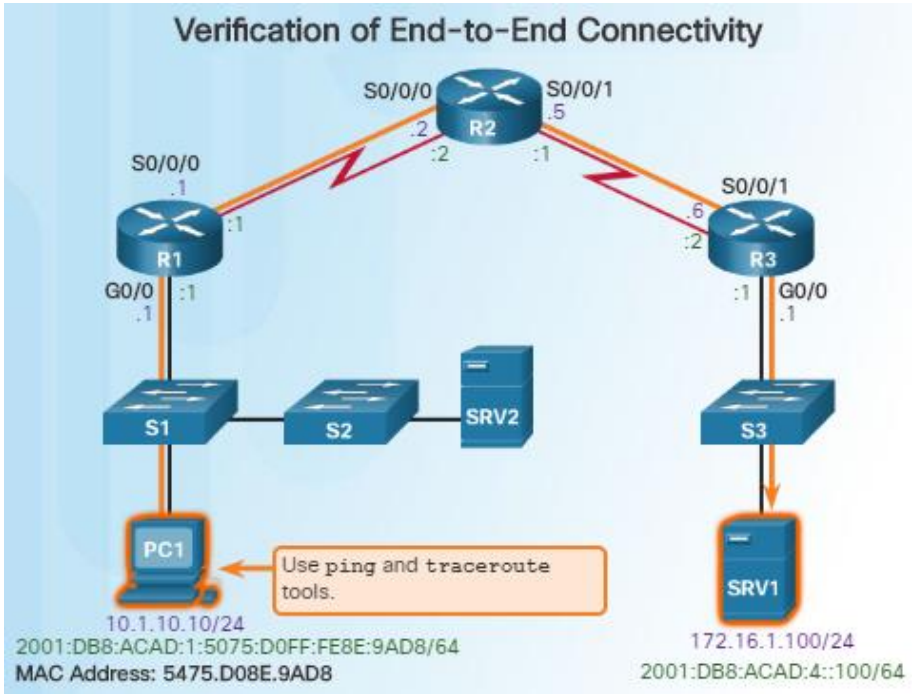
- By employing a structured approach to the troubleshooting process, an administrator can reduce the time it takes to diagnose and solve a problem.
- Throughout this topic, the following scenario (see figure) is used. The client host PC1 is unable to access applications on server SRV1 or server SRV2.
- 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.
- Here are the steps an administrator can take when troubleshooting with the bottom-up approach:

Components of Troubleshooting End-to-End Connectivity (Cont.)



- **Step 1.** Check physical connectivity at the point where network communication stops.
- **Step 2.** Check for duplex mismatches.
- **Step 3.** Check data link and network layer addressing on the local network.
- **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 that the transport layer is functioning properly (Telnet can be used).
- **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.

End-to-End Connectivity Problem Initiates Troubleshooting



- **Ping** and **traceroute** are the two most common utilities to test end-to-end connectivity.
- 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.
  - **ping** can be used for IPv4 and IPv6
- The **traceroute** command illustrates the path the IPv4 packets take to reach their destination.
  - The Cisco IOS **traceroute** command can be used for both IPv4 and IPv6
  - The **tracert** command can be used on Windows
- The **traceroute** command is commonly performed when the **ping** command fails.

Step 1 – Verify the Physical Layer

Examining Input and Output Statistics

```
R1# show interfaces GigabitEthernet 0/0
GigabitEthernet0/0 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, 1 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#
```

- When a network administrator determines that a problem exists on a given device, and that problem might be hardware-related, it is useful to verify its operation using the following IOS commands:
  - **show processes cpu**
  - **show memory**
  - **show interfaces**
- When troubleshooting performance-related issues and hardware is suspected to be at fault, use the **show interfaces** command. The output will show the following:
  - Input queue drops
  - Output queue drops
  - Input errors
  - Output errors

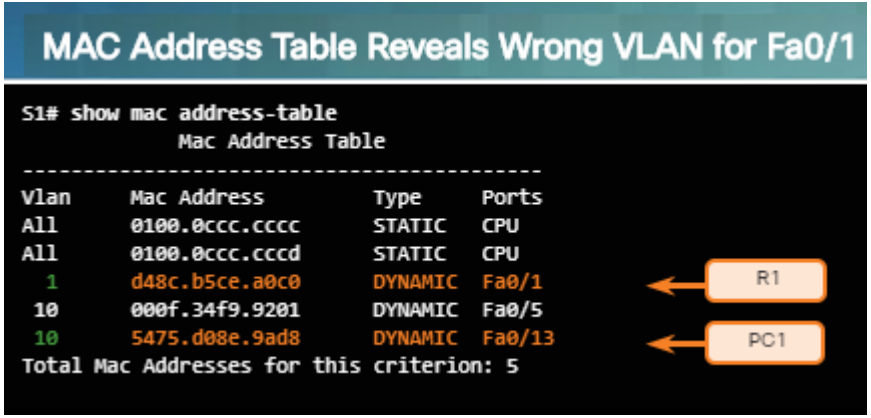
Step 2 – Check for Duplex Mismatches

```
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>
```

```
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)#
```

- Duplex mismatch between two ends of an Ethernet link is another common cause for interface errors.
- The IEEE 802.3ab Gigabit Ethernet standard mandates the use of autonegotiation for speed and duplex. Most Fast Ethernet NICs also use autonegotiation by default.
- However, if duplex negotiation fails for some reason, it might be necessary to set the speed and duplex manually on both ends.
- Point-to-point Ethernet links should always run in full-duplex mode.
- The use of autonegotiation for speed and duplex is the current recommended practice.

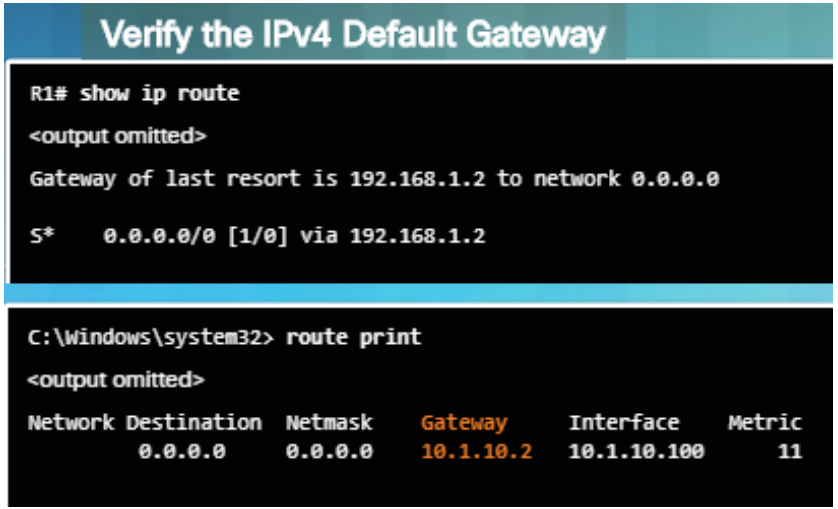
Step 3 – Verify Layer 2 and 3 Addressing on the Local Network



- Look for VLAN assignment issues when troubleshooting end-to-end connectivity issues using the **show vlan** command on a switch.
- The output of the **show mac address-table** command can also be helpful when looking for VLAN assignment issues. This command is used to display the MAC address table on the switch, but also includes VLAN information.

- The **arp** Windows command can be used to help verify mappings between destination IP addresses and Layer 2 Ethernet addresses.
  - The **arp –d** command can be used to clear the arp cache and allow it to repopulate with updated info.
- The **netsh interface ipv6 show neighbor** Windows command will list all devices that are currently in the neighbor table.
  - By examining the neighbor table, the network administrator can verify that the destination IPv6 addresses map to correct Ethernet addresses.
- The **show ipv6 neighbors** command can be used on a Cisco IOS router.

Step 4 – Verify Default Gateway



- These commands will help verify the presence of the IPv4 default gateway.

- If there is no default route on the router or if the host is configured with the wrong default gateway, then communication between two endpoints on different networks will not work.
- In addition to the commands in the figure, the following can be useful when troubleshooting:
  - Use the **show ipv6 route** Cisco IOS command to check for the IPv6 default route on R1 and use the **ipconfig** Windows command to verify if a PC has an IPv6 default gateway
  - The **show ipv6 interface GigabitEthernet 0/0** command can verify if it is a member of the correct multicast group.
  - Use the **ipconfig** command on Windows PCs to verify if the correct default gateway is set.

Step 5 – Verify Correct Path

Examining the IPv6 Routing Table on R1

```
R1# show ipv6 route
IPv6 Routing Table - default - 7 entries
Codes: C - Connected, L - Local, S - Static
       U - Per-user Static route, B - BGP, R - RIP
       I1 - ISIS L1, I2 - ISIS L2, A - ISIS interarea
       IS - ISIS summary, D - EIGRP, EX - EIGRP external
       ND - ND Default, NDp - ND Prefix, DCE - Destination
       NDr - Redirect, O - OSPF Intra, OI - OSPF Inter
       OE1 - OSPF ext 1, OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1
       ON2 - OSPF NSSA ext 2
S   ::/0 [1/0]
     via 2001:DB8:ACAD:2::2
C   2001:DB8:ACAD:1::/64 [0/0]
     via GigabitEthernet0/0, directly connected
L   2001:DB8:ACAD:1::1/128 [0/0]
     via GigabitEthernet0/0, receive
C   2001:DB8:ACAD:2::/64 [0/0]
     via Serial0/0/0, directly connected
L   2001:DB8:ACAD:2::1/128 [0/0]
     via Serial0/0/0, receive
D   2001:DB8:ACAD:3::/64 [90/41024000]
     via FE80::2, Serial0/0/0
D   2001:DB8:ACAD:4::/64 [90/41024256]
     via FE80::2, Serial0/0/0
L   FF00::/8 [0/0]
     via Null0, receive
R1#
```

- When troubleshooting a connectivity issue, it is often necessary to verify the path to the destination network.
- Use either the **show ip route or show ipv6 route** command to verify that the route exists to the destination device/network.
- The process of forwarding IPv4 and IPv6 packets is based on the longest bit match or longest prefix match. If the destination address in a packet:
  - Does not match an entry in the routing table, then the default route is used. If there's no default route, 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.

Step 6 – Verify the Transport Layer

Testing the HTTP Transport Layer over IPv6 from R1

```
R1# telnet 2001:db8:acad:3::2 80
Trying 2001:DB8:ACAD:3::2, 80 ...
% Connection refused by remote host

R1#
```

- The output above shows a successful Telnet connection from R1 to R3, over IPv6 using port 80.
- The output verifies a successful transport layer connection.

- 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.
- The two most common issues that affect transport layer connectivity are ACL and NAT configuration problems.
- A common tool for testing transport layer functionality is the Telnet utility.
- If a ping is successful to a server, then the network administrator knows that all layers below the network layer, between the user and the server are operational.
  - The administrator knows the issue is with Layer 4 or up.
- For example: R1# **telnet 2001:db8:acad:3::2**

Step 7 – Verify ACLs

Display ACLs and ACL Placement on R1

```
R3# show ip access-lists
Extended IP access list 100
    deny ip 172.16.1.0 0.0.0.255 any (3 match(es))
    permit ip any any

R3# show ip interface Serial 0/0/1 | include access list
   Outgoing access list is not set
   Inbound access list is not set

R3# show ip interface gigabitethernet 0/0 | include access list
   Outgoing access list is not set
   Inbound  access list is 100
```

- On routers, there may be ACLs configured that prohibit protocols from passing through the interface in the inbound or outbound direction. Use the following commands to display the contents of all ACLs:
  - **show ip access-lists**
  - **show ipv6 access-list**
- Use the following commands to see if there are ACLs set on a particular interface:
  - **show ip interfaces**
  - **show ipv6 interfaces**

Step 7 – Verify DNS

Creating Name to IP Mappings

```
R1(config)# ip host ipv4-server 172.16.1.100
R1(config)# exit
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 = 52/56/64 ms
R1#
R1# conf t
R1(config)# ipv6 host ipv6-server 2001:db8:acad:4::100
R1(config)# exit
R1# ping ipv6-server
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:4::100,
timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5),
round-trip min/avg/max = 52/54/56 ms
R1#
```

- The DNS protocol controls the DNS, a distributed database with which you can map hostnames to IP addresses.
- When DNS is configured on a device, you can substitute the hostname for the IP address for all IP commands including **ping** and **telnet**.
- If there is no DNS server configured on a device, you can use the **ip host** command to enter name to IPv4 mappings on a switch or router.
- The **ipv6 host** command is used for IPv6.
- The figure to the left demonstrates the use of these commands.

8.3 Summary

Summary

Conclusion

- Explain troubleshooting approaches for various network problems.
- Troubleshoot end-to-end connectivity in a small to medium-sized business network, using a systematic approach.


CISCO