



Module 12: Network Troubleshooting

Enterprise Networking, Security, and Automation v7.0
(ENSA)



Module Objectives

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.
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

Network Documentation

Documentation Overview

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

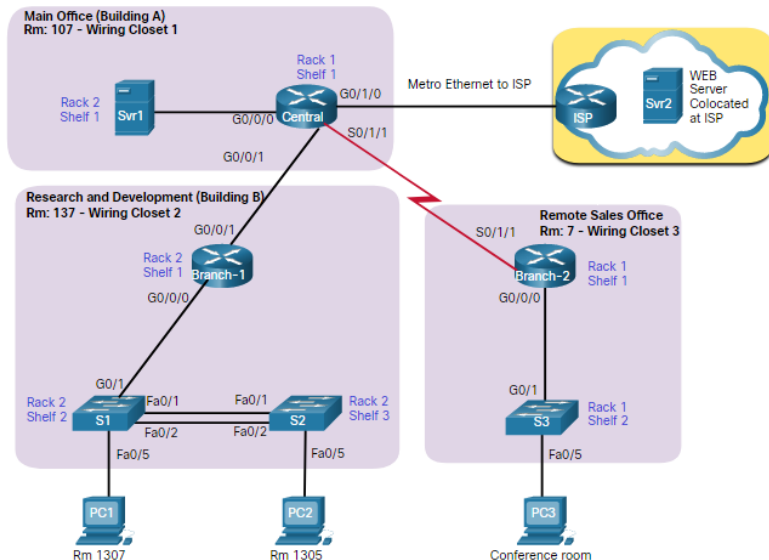
All network documentation should be kept in a single location and backup documentation should be maintained and kept in a separate location.

Network Documentation

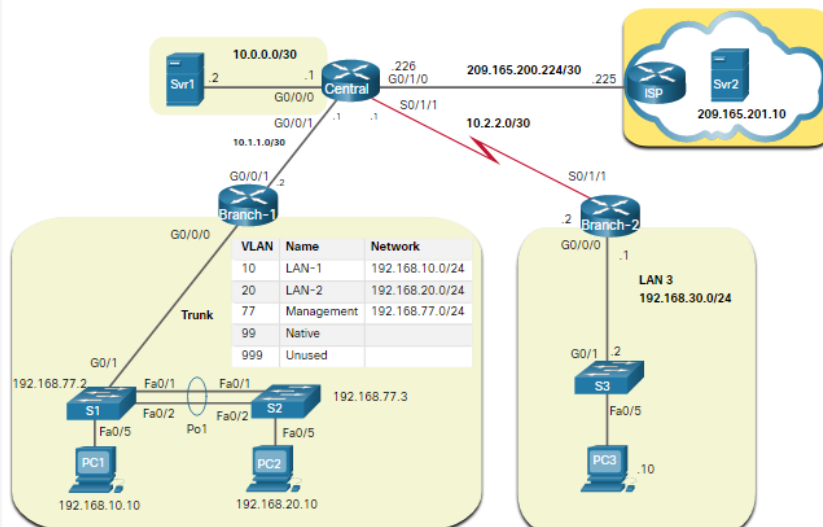
Network Topology Diagrams

There are two types of network topology diagrams: physical and logical.

Physical Topology



Logical Topology



Network Documentation

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.

Router Device Documentation

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

Switch Device Documentation

Device	Model	Description	Mgt. IP Address	IOS			VTP	
S1	Cisco Catalyst WS-C2960-24TC-L	Branch-1 LAN1 switch	192.168.77.2/24	IOS: 15.0(2)SE7 Image: C2960-LANBASEK9-M			Domain: CCNA Mode: Server	
Port	Description		Access	VLAN	Trunk	EtherChannel	Native	Enabled
Fa0/1	Port Channel 1 trunk to S2 Fa0/1		-	-	Yes	Port-Channel 1	99	Yes
Fa0/2	Port Channel 1 trunk to S2 Fa0/2		-	-	Yes	Port-Channel 1	99	Yes
Fa0/3	*** Not in use ***		Yes	999	-	-		Shut
Fa0/4	*** Not in use ***		Yes	999	-	-		Shut
Fa0/5	Access port to user		Yes	10	-	-		Yes

End-System Documentation

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	10.0.0.1	10.0.0.1
				2001:db8:acad:1::2/64	2001:db8:acad:1::1	2001:db8:acad:1::1
SRV2	MS Server 2016	HTTP, HTTPS	5475.d07a.5312	209.165.201.10	209.165.201.1	209.165.201.1
				2001:db8:feed:1::10/64	2001:db8:feed:1::1	2001:db8:feed:1::1
PC1	MS Windows 10	HTTP, HTTPS	5475.d017.3133	192.168.10.10/24	192.168.10.1	192.168.10.1
				2001:db8:acad:1::251/64	2001:db8:acad:1::1	2001:db8:acad:1::1

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.

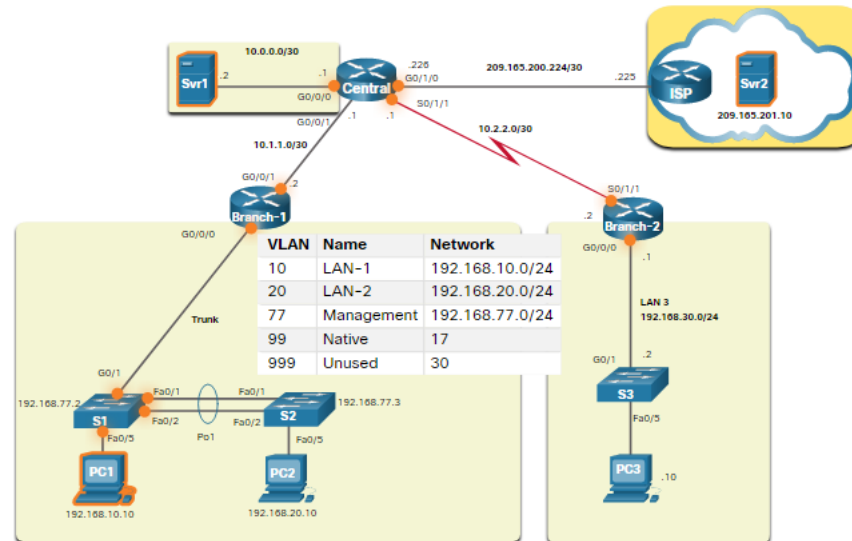
Some good starting variables are interface utilization and CPU utilization.

Step 2 - Identify Devices and Ports of Interest

A logical network topology can be useful in identifying key devices and ports to monitor.

As shown in the sample topology, the devices and ports of interest include:

- PC1 (the Admin terminal)
- Two servers (i.e., Srv1 and Svr2)
- Router interfaces
- Key ports on switches



Step 3 - Determine the Baseline Duration

When capturing data for analysis, the period specified should be:

- At a minimum, seven days long.
- Last no more than six weeks, unless specific long-term trends need to be measured.
- Generally, a two-to-four-week baseline is adequate.

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.

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

Command	Description
<code>show version</code>	• Displays uptime, version information for device software and hardware
<code>show ip interface [brief]</code> <code>show ipv6 interface [brief]</code>	• Displays all the configuration options that are set on an interface.
<code>show interfaces</code>	• Displays detailed output for each interface.
<code>show ip route [static eigrp ospf bgp]</code> <code>show ipv6 route [static eigrp ospf bgp]</code>	• Displays the routing table content listing directly connected networks and learned remote networks.
<code>show cdp neighbors detail</code>	• Displays detailed information about directly connected Cisco devices.
<code>show arp</code> <code>show ipv6 neighbors</code>	• Displays the contents of the ARP table (IPv4) and the neighbor table (IPv6).
<code>show running-config</code>	• Displays current configuration.
<code>show vlan</code>	• Displays the status of VLANs on a switch.
<code>show port</code>	• Displays the status of ports on a switch.
<code>show tech-support</code>	• Used to collect a large amount of information using multiple show commands for technical support reporting purposes.

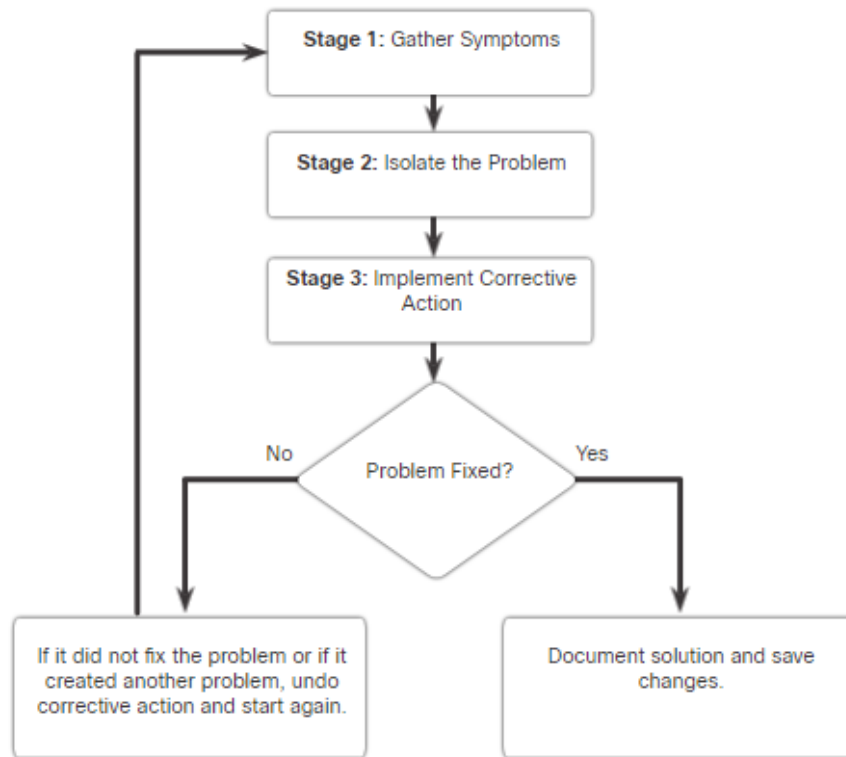
12.2 Troubleshooting Process

Troubleshooting Process

General Troubleshooting Procedures

Troubleshooting can be time consuming because networks differ, problems differ, and troubleshooting experience varies.

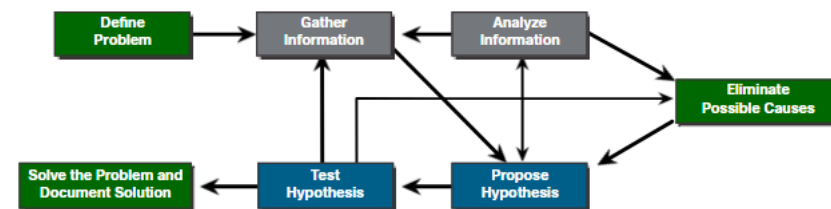
- Using a structured troubleshooting method will shorten overall troubleshooting time.
- There are several troubleshooting processes that can be used to solve a problem.
- The figure displays the logic flowchart of a simplified three-stage troubleshooting process.



Troubleshooting Process

Seven-Step Troubleshooting Process

The figure displays a more detailed seven-step troubleshooting process.



Steps	Description
Define the Problem	<ul style="list-style-type: none">• Verify that there is a problem and then properly define what the problem is.
Gather Information	<ul style="list-style-type: none">• Targets (i.e., hosts, devices) are identified, accessed, and information gathered.
Analyze Information	<ul style="list-style-type: none">• Identify possible causes using network documentation, network baselines, knowledge bases, and peers.
Eliminate Possible Causes	<ul style="list-style-type: none">• Progressively eliminate possible causes to eventually identify the most probable cause.
Propose Hypothesis	<ul style="list-style-type: none">• When the most probable cause has been identified, a solution must be formulated.
Test Hypothesis	<ul style="list-style-type: none">• Assess the urgency of the problem, create a rollback plan, implement the solution, and verify outcome.
Solve the Problem	<ul style="list-style-type: none">• When solved, inform all involved and document the cause and solution to help solve future problems.

(1) Question End Users

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

Guidelines	Example Open Ended End-User Questions
Ask pertinent questions.	<ul style="list-style-type: none"> • What does not work? • What exactly is the problem? • What are you trying to accomplish?
Determine the scope of the problem.	<ul style="list-style-type: none"> • Who does this issue affect? Is it just you or others? • What device is this happening on?
Determine when the problem occurred / occurs.	<ul style="list-style-type: none"> • 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.	<ul style="list-style-type: none"> • Can you reproduce the problem? • Can you send me a screenshot or video of the problem?
Determine if anything has changed.	<ul style="list-style-type: none"> • What has changed since the last time it did work?
Use questions to eliminate or discover possible problems.	<ul style="list-style-type: none"> • What works? • What does not work?

(2) Gather Information

Common Cisco IOS commands used to gather network problem symptoms.

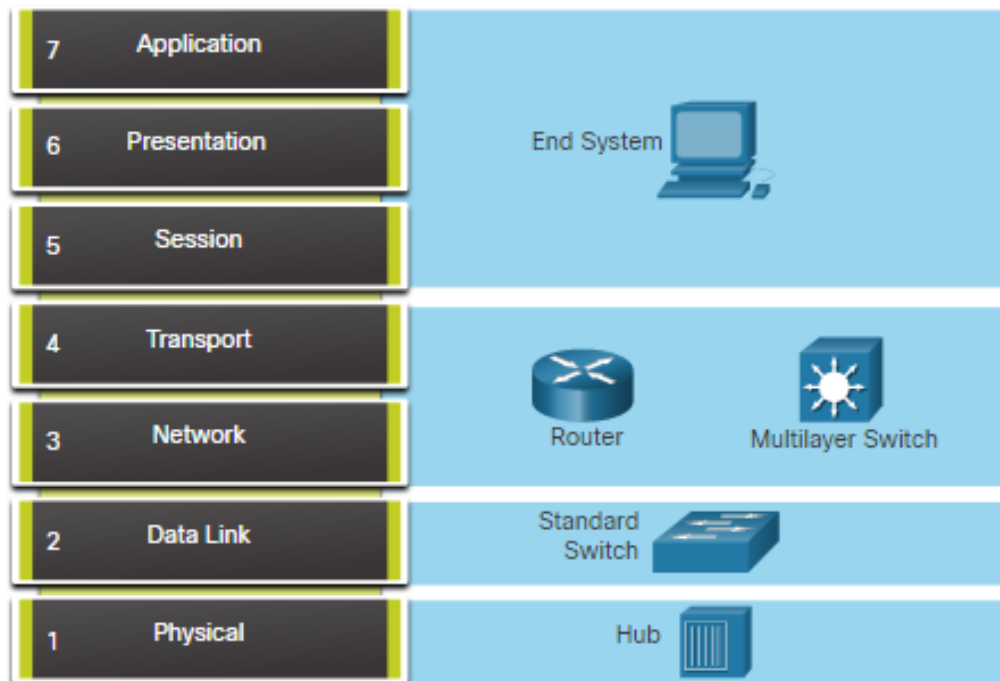
Command	Description
<code>ping {host ip-address}</code>	• Sends an echo request packet to an address, then waits for a reply.
<code>traceroute destination</code>	• Identifies the path a packet takes through the networks.
<code>telnet {host ip-address}</code>	• Connects to an IP address using the Telnet application (Note: Use SSH whenever possible).
<code>ssh -l user-id ip-address</code>	• Connects to an IP address using SSH.
<code>show ip interface brief</code> <code>show ipv6 interface brief</code>	• Displays a summary status of all interfaces on a device.
<code>show ip route</code> <code>show ipv6 route</code>	• Displays the current IPv4 and IPv6 routing tables.
<code>show protocols</code>	• Displays the global and interface-specific status of any configured Layer 3 protocol.
<code>debug</code>	• Displays a list of options for enabling or disabling debugging events.

Troubleshooting Process

Troubleshooting with Layered Models

The OSI and TCP/IP models can be applied to isolate network problems when troubleshooting.

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



12.3 Troubleshooting Process

Troubleshooting Tools

Software Troubleshooting Tools

Common software troubleshooting tools include the following:

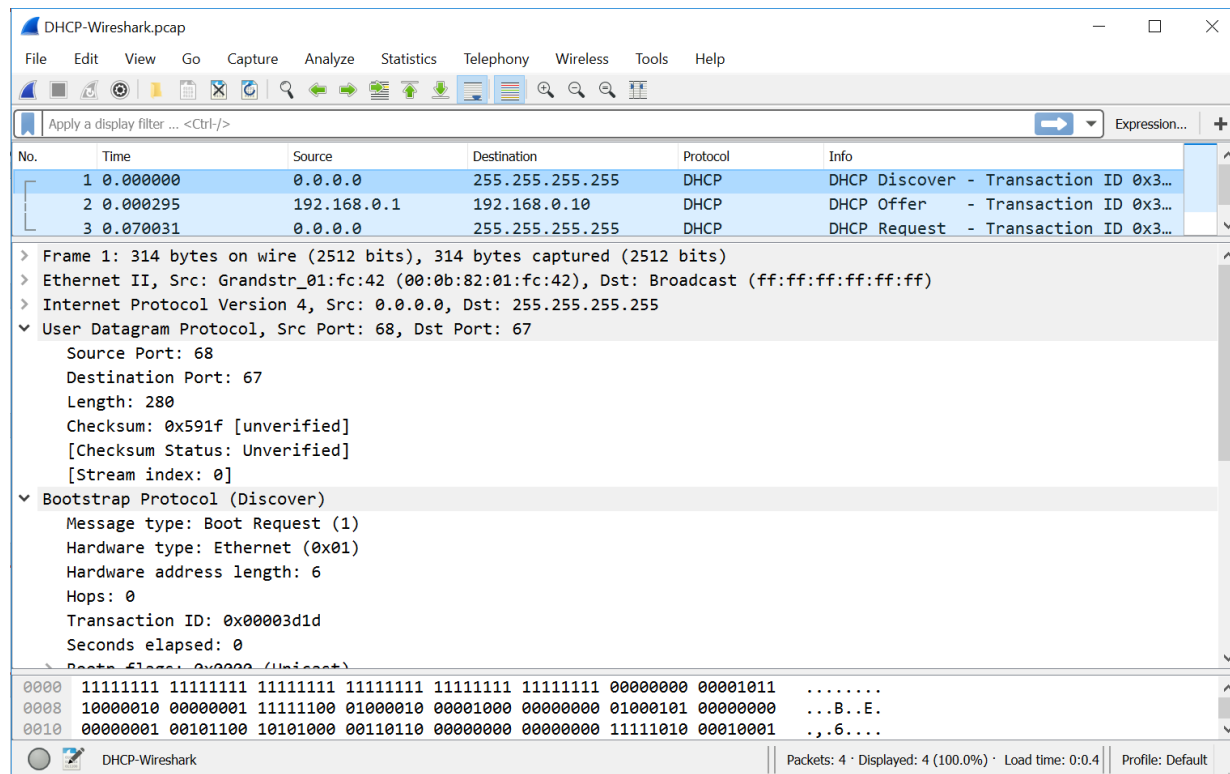
Software Tool	Description
Network Management System Tools	<ul style="list-style-type: none">• Network software include device-level monitoring, configuration, and fault-management tools.• Tools can be used to investigate and correct network problems.
Knowledge Bases	<ul style="list-style-type: none">• 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.
Baselining Tools	<ul style="list-style-type: none">• Many tools for automating the network documentation and baselining process are available.• Baselining tools help with common documentation tasks such as network diagrams, update network software and hardware documentation, and cost-effectively measure baseline network bandwidth use.

Troubleshooting Tools

Protocol Analyzers

A protocol analyzer can capture and display the physical layer to the application layer information contained in a packet.

Protocol analyzers, such as Wireshark, can help troubleshoot network performance problems.



Troubleshooting Tools

Hardware Troubleshooting Tools

There are multiple types of hardware troubleshooting tools.

Hardware Tools	Description
Digital Multimeters	Devices measure electrical values of voltage, current, and resistance.
Cable Testers	Handheld devices are designed for testing the various types of data communication cabling.
Cable Analyzers	Multifunctional handheld devices used to test and certify copper and fiber cables.
Portable Network Analyzers	Specialized device used for troubleshooting switched networks and VLANs.
Cisco Prime NAM	Browser-based interface that displays device performance analysis in a switched and routed environment.

Syslog Server as a Troubleshooting Tool

Syslog is used by syslog clients to send text-based log messages to a syslog server.

- Log messages can be sent to the console, VTY lines, memory buffer, or syslog server.
- Cisco IOS log messages fall into one of eight levels.
- The lower the level number, the higher the severity level.
- By default, the console displays level 6 (debugging) messages.
- In the command output, level 0 (emergencies) to 5 (notifications) are sent to the syslog server at 209.165.200.225.

Level	Keyword
0	Emergencies
1	Alerts
2	Critical
3	Errors
4	Warnings
5	Notifications
6	Informational
7	Debugging

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

12.5 Troubleshooting IP Connectivity

Components of Troubleshooting End-to-End Connectivity

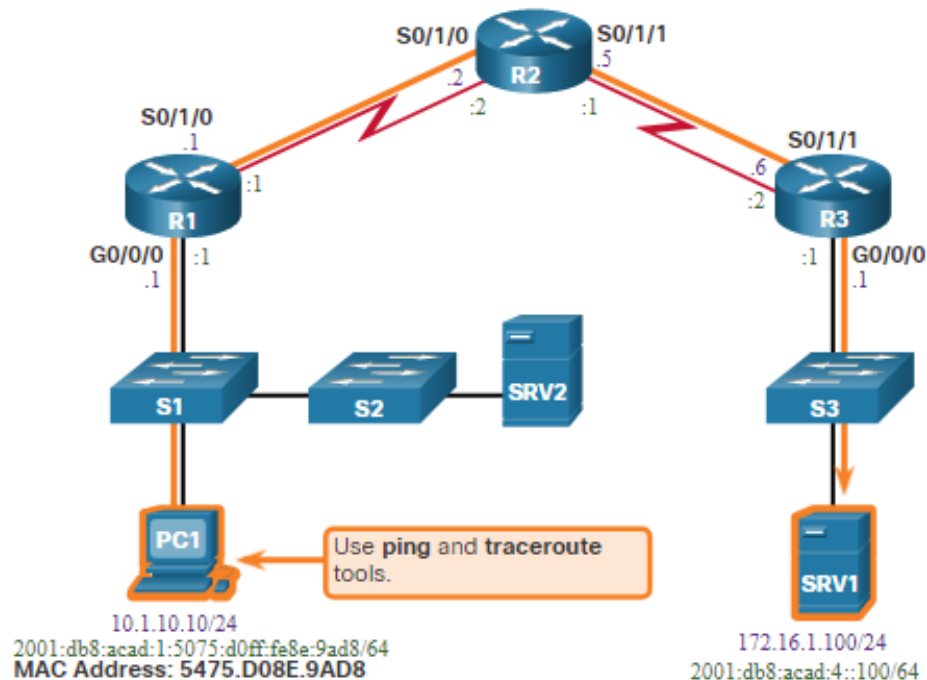
Bottom-up approach steps when there is no end-to-end connectivity are as follows:

1. Check physical connectivity at the point where network communication stops.
2. Check for duplex mismatches.
3. Check data link and network layer addressing on the local network.
4. Verify that the default gateway is correct.
5. Ensure that devices are determining the correct path from the source to the destination.
6. Verify the transport layer is functioning properly.
7. Verify that there are no ACLs blocking traffic.
8. Ensure that DNS settings are correct.

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**.



Troubleshooting IP Connectivity

Step 1 - Verify the Physical Layer

The **show interfaces** command is useful when troubleshooting performance-related issues and hardware is suspected to be at fault.

Of interest in the output are the:

- Interface status
- Input queue drops
- Output queue drops
- Input errors
- Output errors

```
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 runs, 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#
```

Troubleshooting IP Connectivity

Step 2 - Check for Duplex Mismatches

The IEEE 802.3ab Gigabit Ethernet standard mandates the use of autonegotiation for speed and duplex and practically all Fast Ethernet NICs also use autonegotiation by default.

Problems can occur when there is a duplex mismatch.

```
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#
```

```
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)#
```

Step 3 - Verify Addressing on the Local Network

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.

```
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:\>
```

Troubleshooting IP Connectivity

Troubleshoot VLAN Assignment Example

Another issue to consider when troubleshooting end-to-end connectivity is VLAN assignment.

For example, the MAC address on Fa0/1 should be in VLAN 10 instead of VLAN 1.

```
S1# show mac address-table
      Mac Address Table
-----
Vlan    Mac Address      Type    Ports
---
All     0100.0ccc.cccc    STATIC  CPU
All     0100.0ccc.cccd    STATIC  CPU
1       d48c.b5ce.a0c0    DYNAMIC Fa0/1
10      000f.34f9.9201    DYNAMIC Fa0/5
10      5475.d08e.9ad8    DYNAMIC Fa0/13
Total Mac Addresses for this criterion: 5
S1#
```

The following configuration changes Fa0/1 to VLAN 10 and verifies the change.

```
S1(config)# interface fa0/1
S1(config-if)# switchport mode access
S1(config-if)# switchport access vlan 10
S1(config-if)# exit
S1#
S1# show mac address-table
      Mac Address Table
-----
Vlan    Mac Address      Type    Ports
---
All     0100.0ccc.cccc    STATIC  CPU
All     0100.0ccc.cccd    STATIC  CPU
10      d48c.b5ce.a0c0    DYNAMIC Fa0/1
10      000f.34f9.9201    DYNAMIC Fa0/5
10      5475.d08e.9ad8    DYNAMIC Fa0/13
Total Mac Addresses for this criterion: 5
S1#
```

Troubleshooting IP Connectivity

Step 4 - Verify Default Gateway

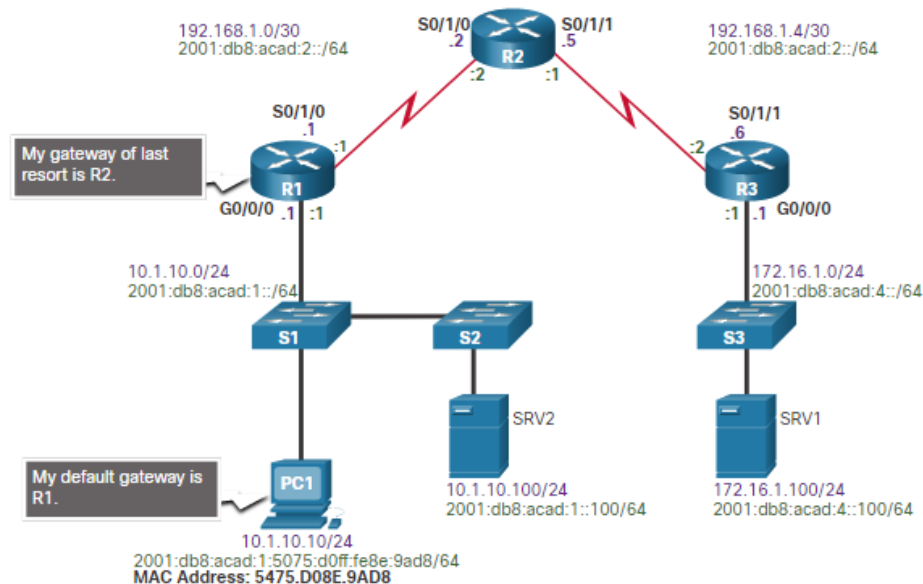
Misconfigured or missing default gateways can cause connectivity problems.

In the figure for example, the default gateways for:

- R1 is 192.168.1.2 (R2)
- PC1 is 10.1.10.1 (R1 G0/0/0)

Useful commands to verify the default gateway on:

- R1: **show ip route**
- PC1: **route print** (or **netstat -r**)



Troubleshoot IPv6 Default Gateway Example

An IPv6 default gateway can be configured manually, using SLAAC, or by using DHCPv6.

For example, a PC is unable to acquire its IPv6 configuration using SLAAC. The command output is missing the all IPv6-router multicast group (FF02::2).

```
R1# show ipv6 interface GigabitEthernet 0/0/0
GigabitEthernet0/0/0 is up, line protocol is up
IPv6 is enabled, link-local address is FE80::1
No Virtual link-local address(es):
Global unicast address(es):
  2001:DB8:ACAD:1::1, subnet is 2001:DB8:ACAD:1::/64
Joined group address(es):
  FF02:: 1
  FF02::1:FF00:1

(Output omitted)
R1#
```

R1 is enabled as an IPv6 router and now the output verifies that R1 is a member of ff02::2, the All-IPv6-Routers multicast group.

```
R1(config)# ipv6 unicast-routing
R1(config)# exit
R1# show ipv6 interface GigabitEthernet 0/0/0
GigabitEthernet0/0/0 is up, line protocol is up
IPv6 is enabled, link-local address is FE80::1
No Virtual link-local address(es):
Global unicast address(es):
  2001:DB8:ACAD:1::1, subnet is 2001:DB8:ACAD:1::/64
Joined group address(es):
  FF02:: 1
  FF02:: 2
  FF02::1:FF00:1

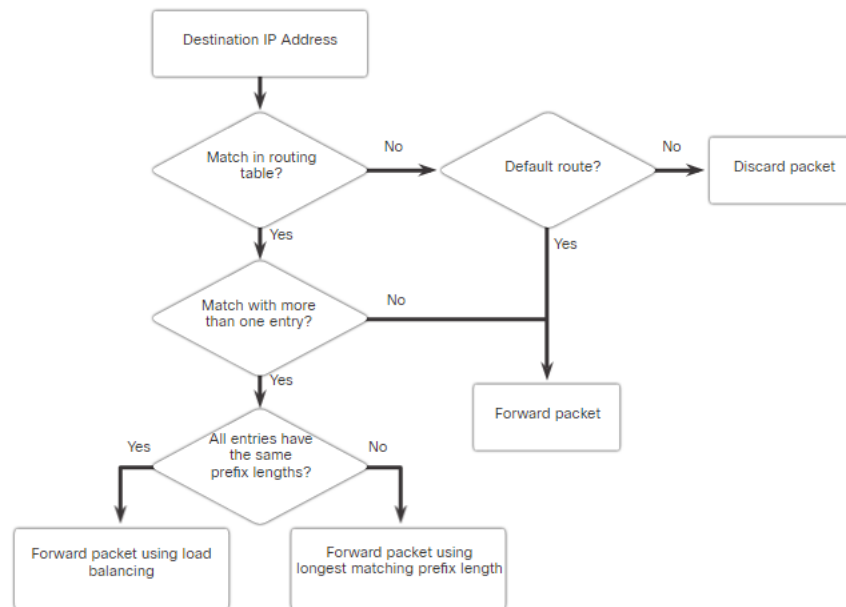
(Output omitted)
R1#
```

Troubleshooting IP Connectivity

Step 5 - Verify Correct Path

When troubleshooting, it is often necessary to verify the path to the destination network.

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



Troubleshooting IP Connectivity

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.
- 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#
```


Troubleshooting IP Connectivity

Step 7 - Verify ACLs

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

In this example, ACL 100 has been incorrectly configured inbound on the G0/0/0 instead of inbound on S0/1/1.

```
R3# show ip interface serial 0/1/1 | include access list
Outgoing Common access list is not set
Outgoing access list is not set
Inbound Common access list is not set
Inbound access list is not set
R3#
R3# show ip interface gig 0/0/0 | include access list
Outgoing Common access list is not set
Outgoing access list is not set
Inbound Common access list is not set
Inbound access list is 100
R3#
```

The ACL is removed from G0/0/0 and configured inbound on S0/1/1.

```
R3(config)# interface GigabitEthernet 0/0/0
R3(config-if)# no ip access-group 100 in
R3(config-if)# exit
R3(config)#
R3(config)# interface serial 0/1/1
R3(config-if)# ip access-group 100 in
R3(config-if)# end
R3#
```

Troubleshooting IP Connectivity

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. command output.
- Use the **ip host** global configuration command to enter a name to be used instead of the IPv4 address of the switch or router, as shown in the command output.
- Use the **nslookup** Windows command to display the name-to-IP-address mapping information.

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

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#
```

Packet Tracer - Troubleshoot Enterprise Networks

In this Packet Tracer activity, you complete the following objectives:

- Part 1: Verify Switching Technologies
- Part 2: Verify DHCP
- Part 3: Verify Routing
- Part 4: Verify WAN Technologies
- Part 5: Verify Connectivity

12.6 Module Practice and Quiz