Chapter 9: Troubleshooting the Network

Connecting Networks

Cisco | Networking Academy®
Mind Wide Open™

Chapter 9

9.0 Introduction

9.1 Troubleshooting with a Systematic Approach

9.2 Network Troubleshooting

9.3 Summary

9.1 Troubleshooting with a Systematic Approach

Cisco | Networking Academy®
Mind Wide Open™

Chapter 9: Objectives

- 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.
- Describe troubleshooting tools used to gather and analyze symptoms of network problems.
- Determine the symptoms and causes of network problems using a layered model.
- Troubleshoot a network using the layered model.

Documenting the Network

Network documentation is a complete set of accurate and current network documentation. This documentation includes:

- Configuration files, including network configuration files and end-system configuration files
- Physical and logical topology diagrams
- A baseline performance level

Network Documentation

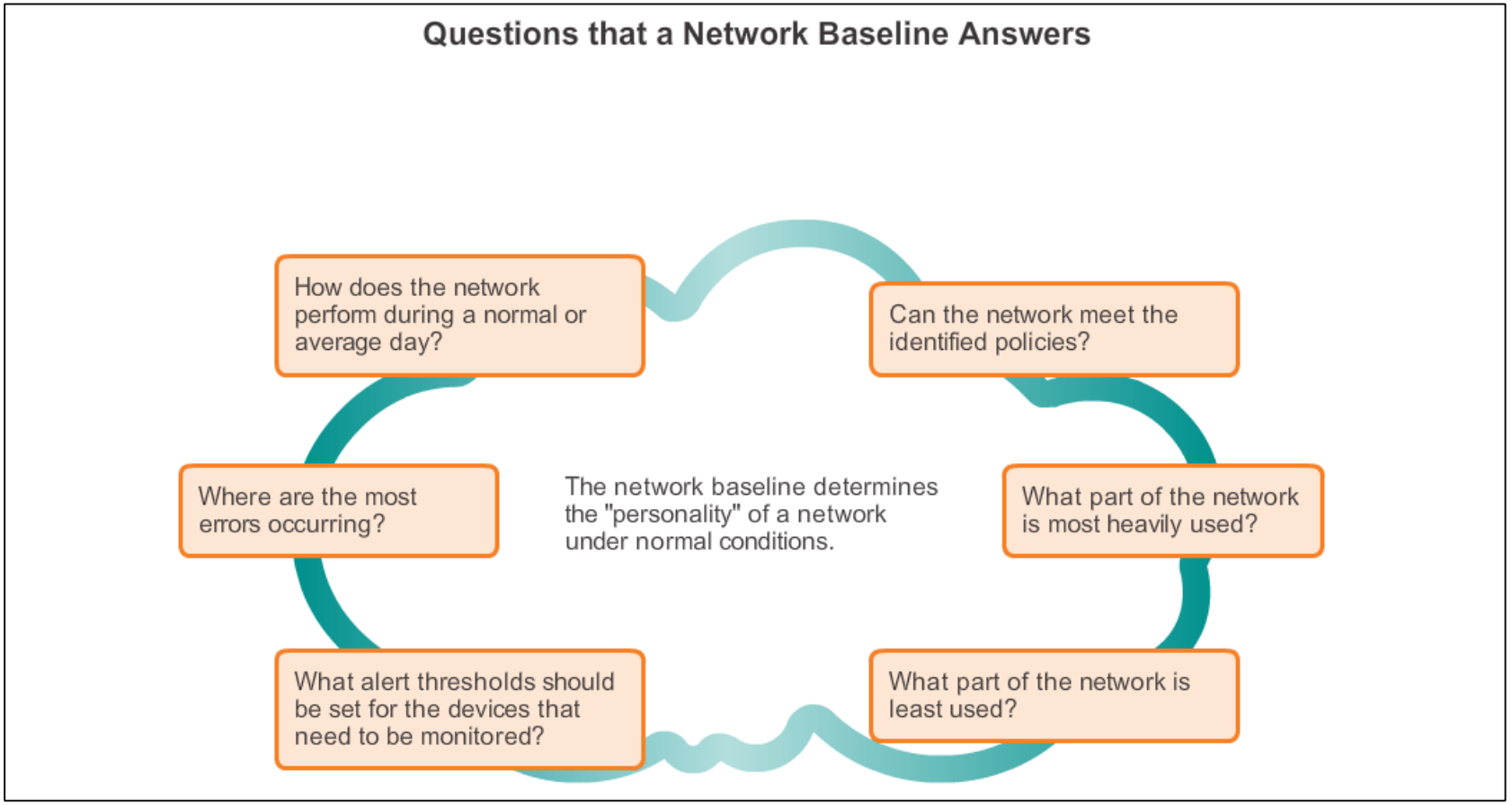
Network Topology Diagrams

- Physical Topology
  - Device type
    - Model and manufacturer
  - Operating system version
    - Cable type and identifier
  - Cable specification
    - Connector type
  - Cabling endpoints

- Logical Topology
  - Device identifiers
    - IP address and prefix lengths
  - Interface identifiers
    - Connection type
  - DLCI for virtual circuits
    - Site-to-site VPNs
  - Routing protocols
    - Static routes
  - Data-link protocols
    - WAN technologies used

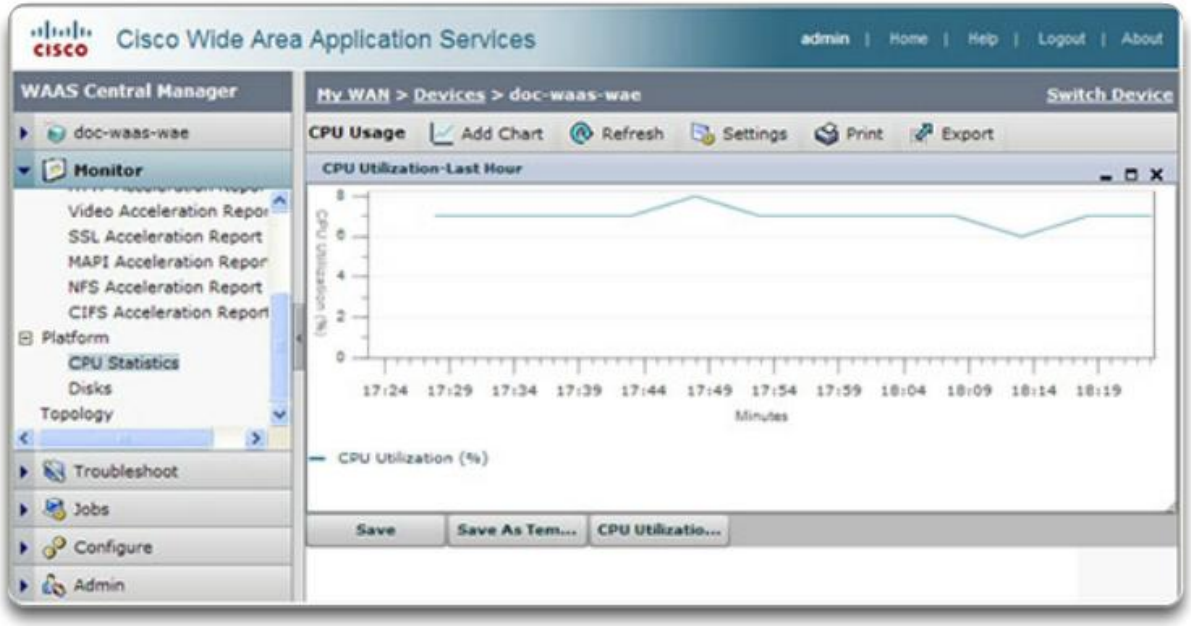
Network Documentation

Establishing a Network Baseline



Establishing a Network Baseline (cont.)

- **Step 1**. Determine what types of data to collect.
- **Step 2.** Identify devices and ports of interest.
- **Step 3.** Determine the baseline duration.



Network Documentation

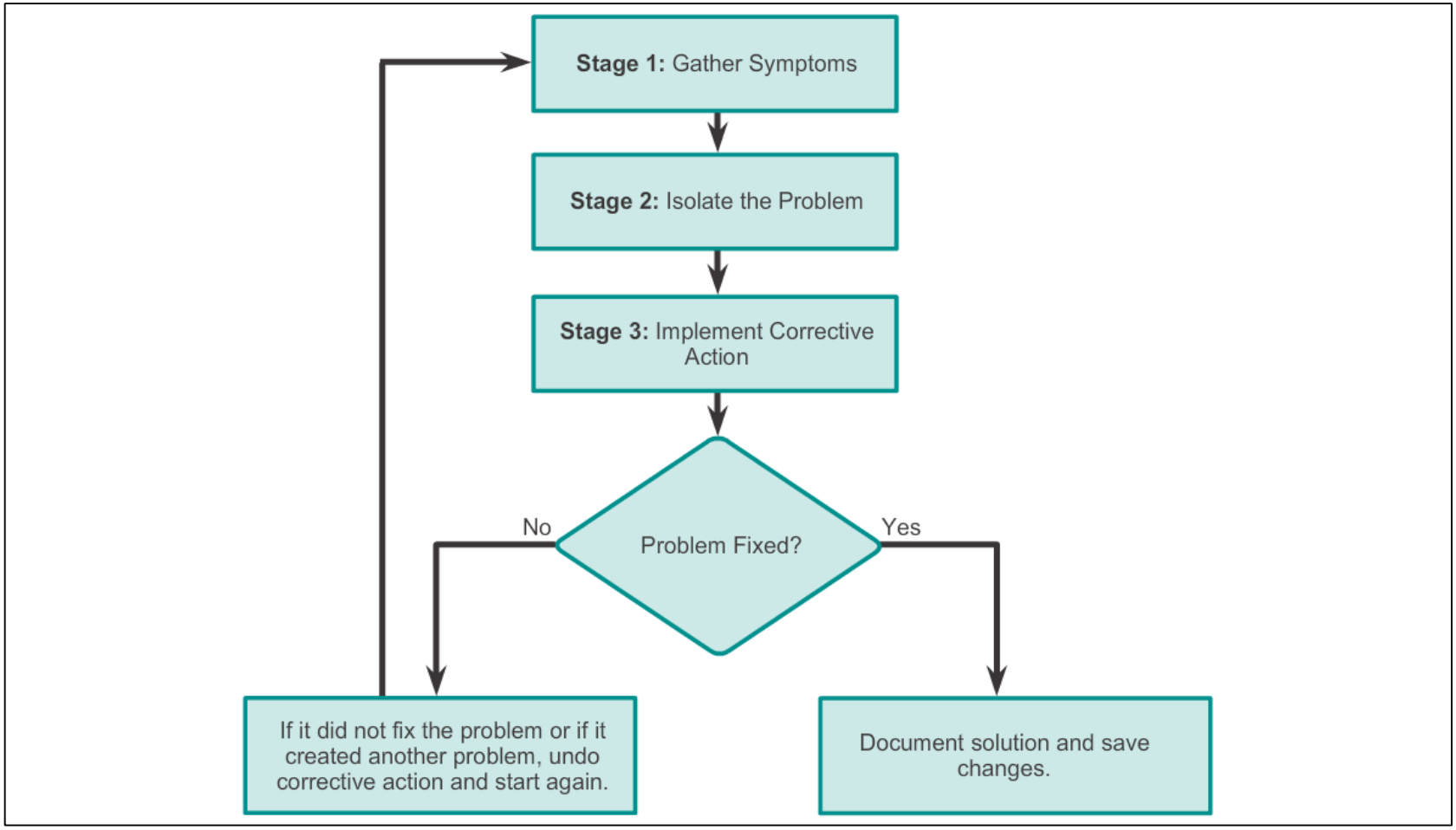
Measuring Data

Commands that are useful to the network documentation process include:

- **ping**
- **telnet**
- **show ip interface brief**
- **show ipv6 interface brief**
- **show ip route**
- **show ipv6 route**
- **show cdp neighbor detail**

Troubleshooting Process

General Troubleshooting Procedures



Troubleshooting Process

Gathering Symptoms

Commands for Gathering Symptoms

Command	Description
ping {*host* | *ip-address*}	Sends an echo request packet to an address, then waits for a reply. The *host* | *ip-address* variable is the IP alias or IP address of the target system.
traceroute {*destination*}	Identifies the path a packet takes through the 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.
show ip interface brief **show ipv6 interface brief**	Displays a summary of the status of all interfaces on a device.
show ip route **show ipv6 route**	Displays contents of currently running configuration file.
show running-config	Displays a list of options for enabling or disabling debugging events on a device.
[no] debug ?	Displays a list of options for enabling or disabling debugging events on a device.
show protocols	Displays the configured protocols and shows the global and interface-specific status of any configured Layer 3 protocol.

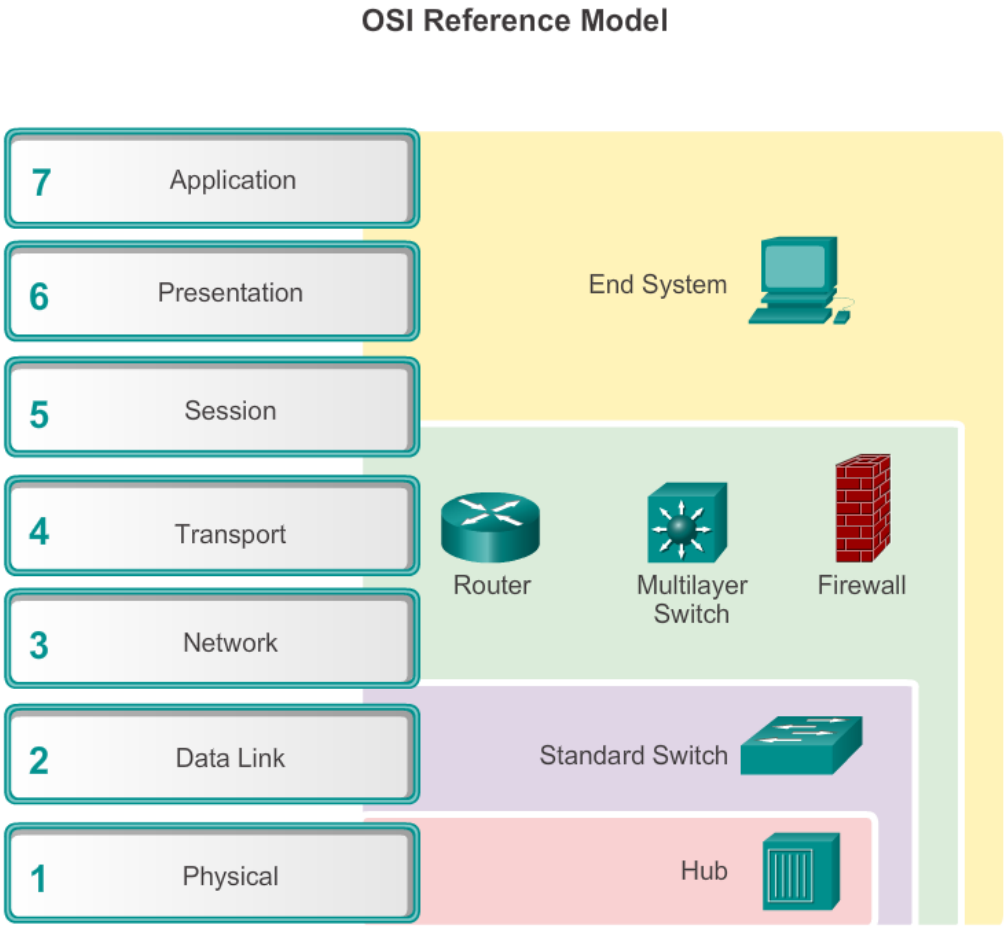
Troubleshooting Process

Questioning End 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?
Did anything unusual happen since the last time it 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?

Isolating the Issue Using Layered Models

Using Layered Models for Troubleshooting



Troubleshooting Methods

Using the layered models, there are three primary methods for troubleshooting networks:

- Bottom-up
- Top-down
- Divide-and-conquer

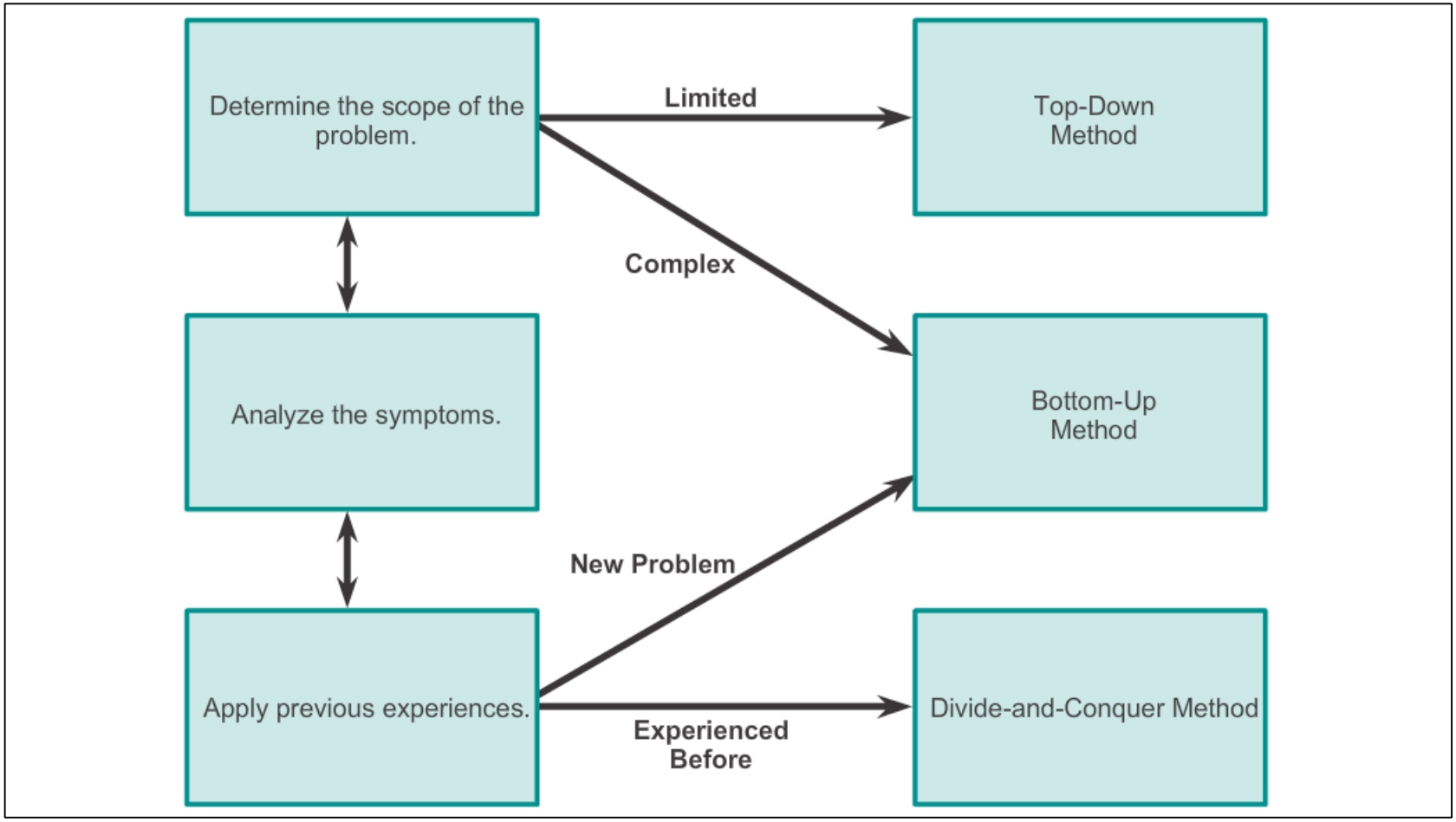
Troubleshooting Methods (cont.)

In addition to the systematic, layered approach to troubleshooting, there are also, less-structured troubleshooting approaches:

- One troubleshooting approach is based on an educated guess by the network administrator, based on the symptoms of the problem.
- Another approach involves comparing a working and nonworking situation, and spotting significant differences.
- Swapping the problematic device with a known, working one is a quick way to troubleshoot.

Isolating the Issue Using Layered Models

Guidelines for Selecting a Troubleshooting Method



9.2 Network Troubleshooting

Cisco | Networking Academy®
Mind Wide Open™

Software Troubleshooting Tools

Common software troubleshooting tools include:

- NMS tools
- Knowledge bases
- Baselining tools
- Host-based protocol analyzers
- Cisco IOS EPC

Hardware Troubleshooting Tools

Common hardware troubleshooting tools include:

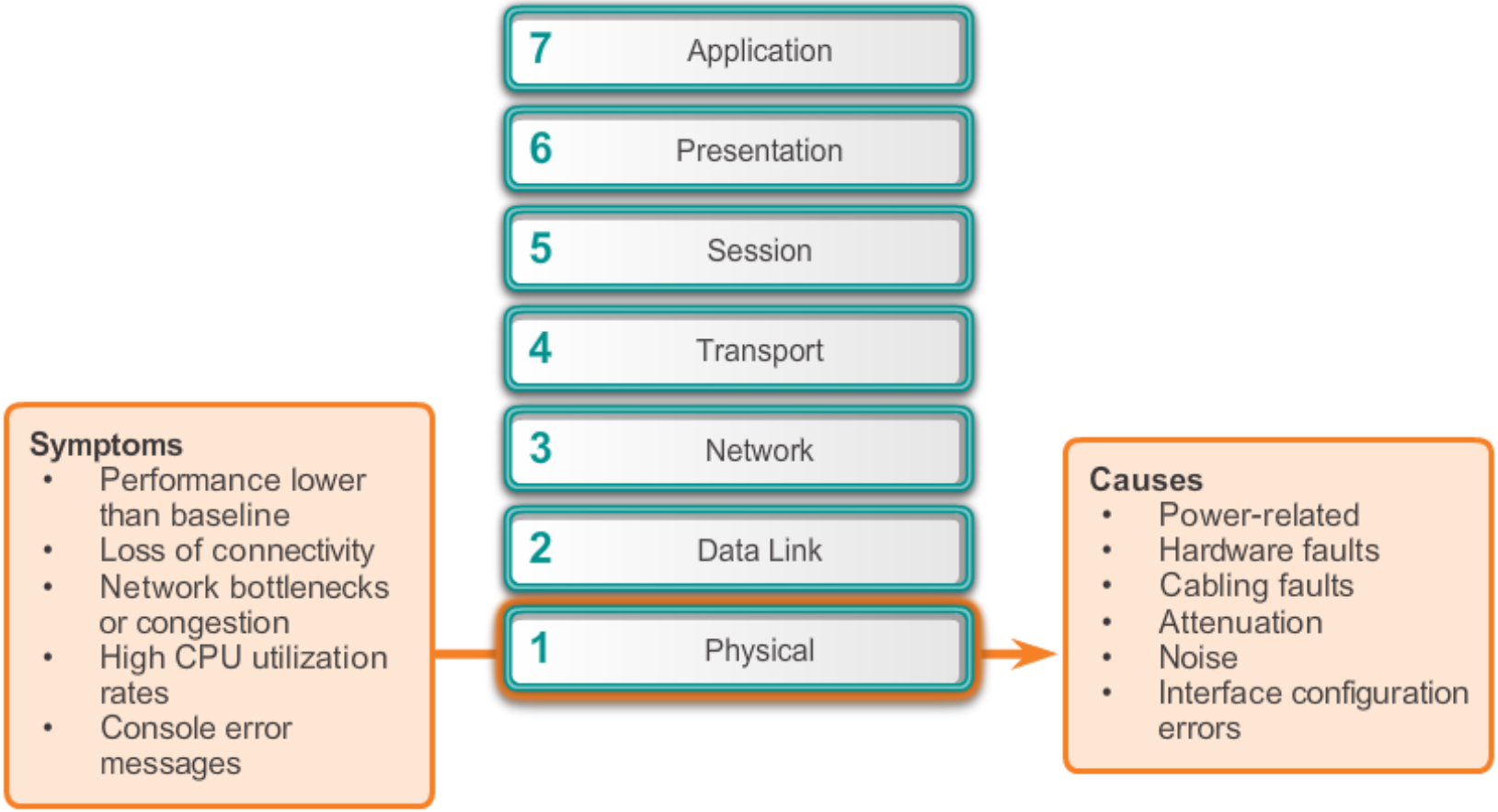
- Network analysis module
- Digital multimeters
- Cable testers
- Cable analyzers
- Portable network analyzers

Using a Syslog Server for Troubleshooting

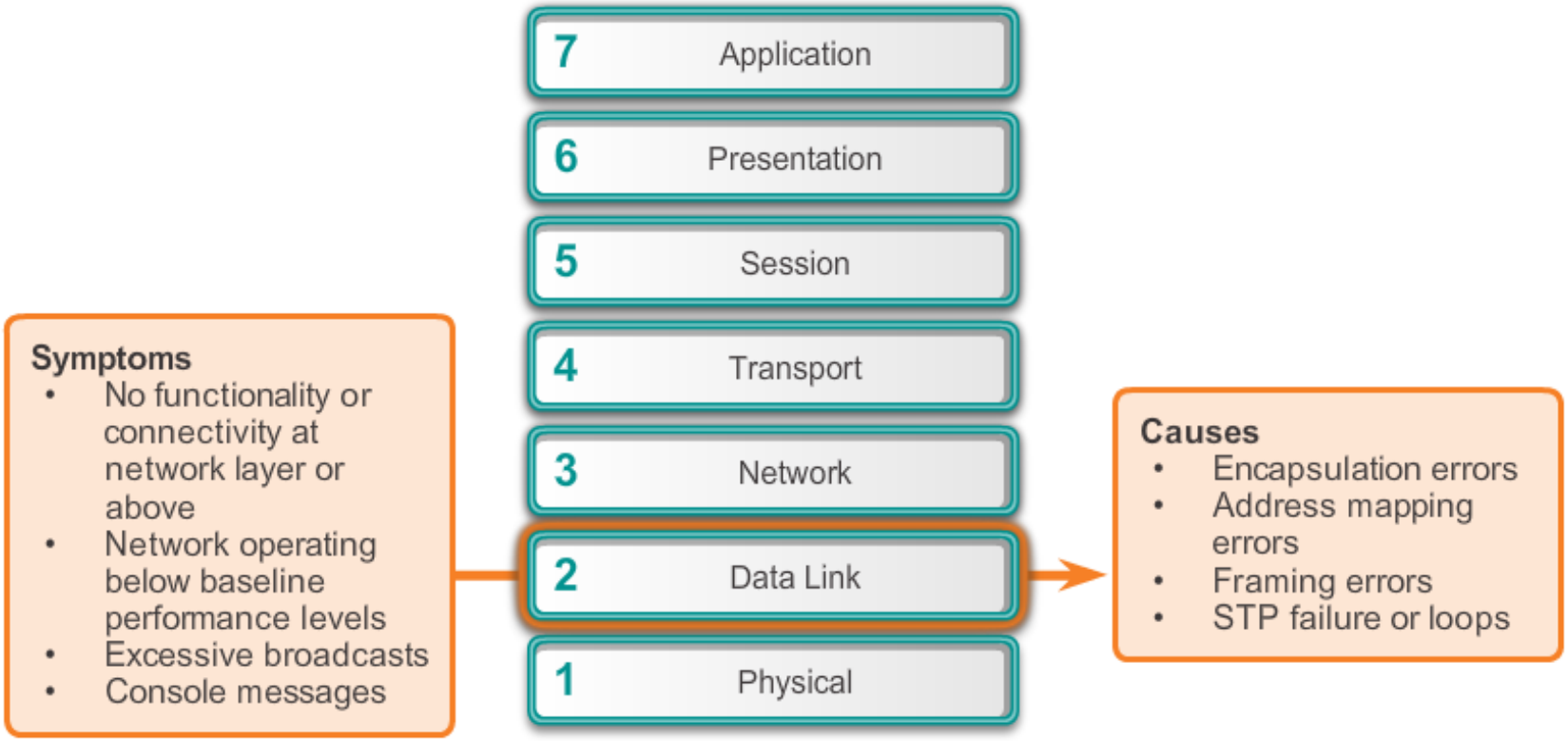
Severity Level

	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

Physical Layer Troubleshooting

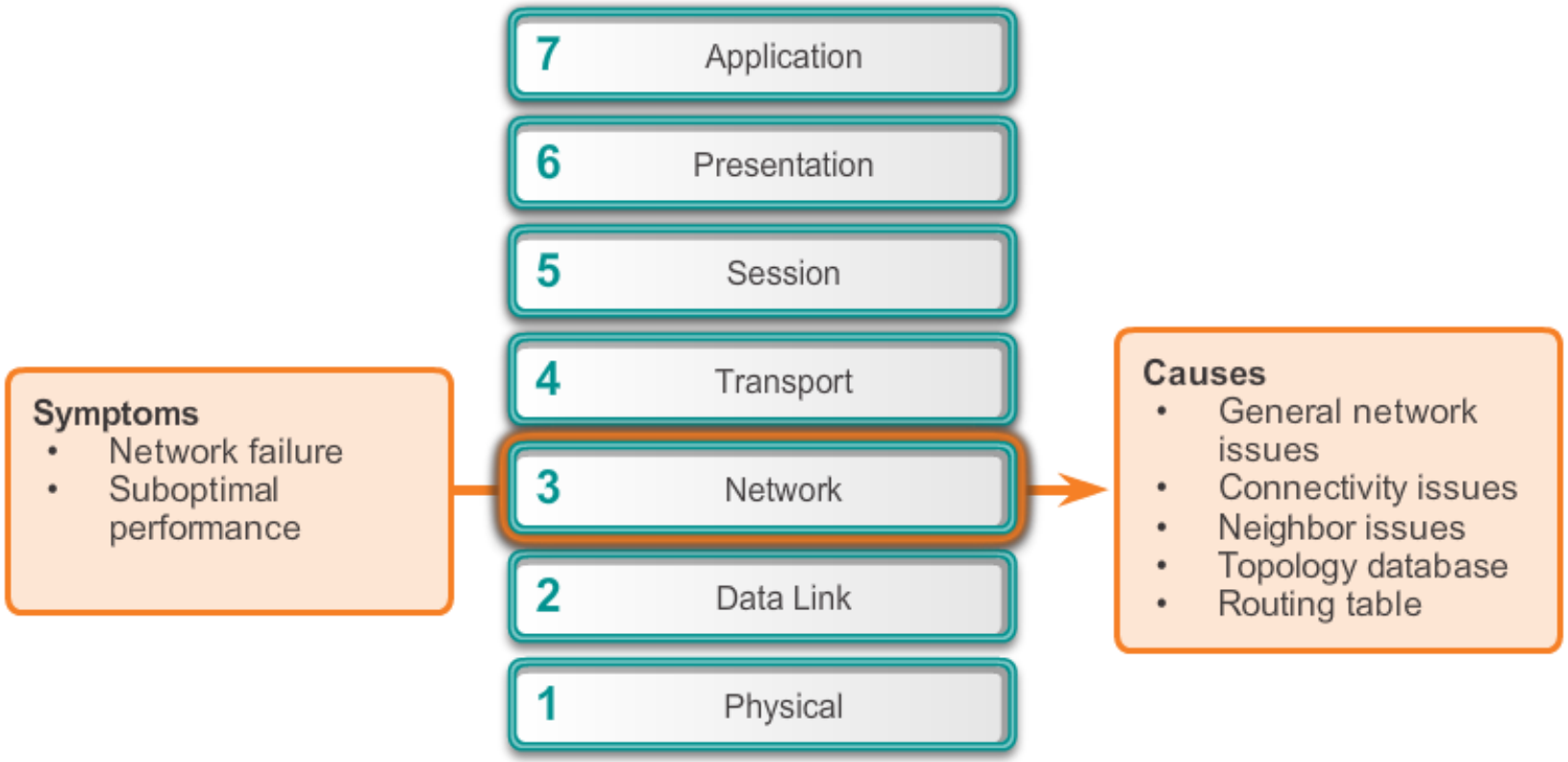


Data Link Layer Troubleshooting



Symptoms and Causes of Network Troubleshooting

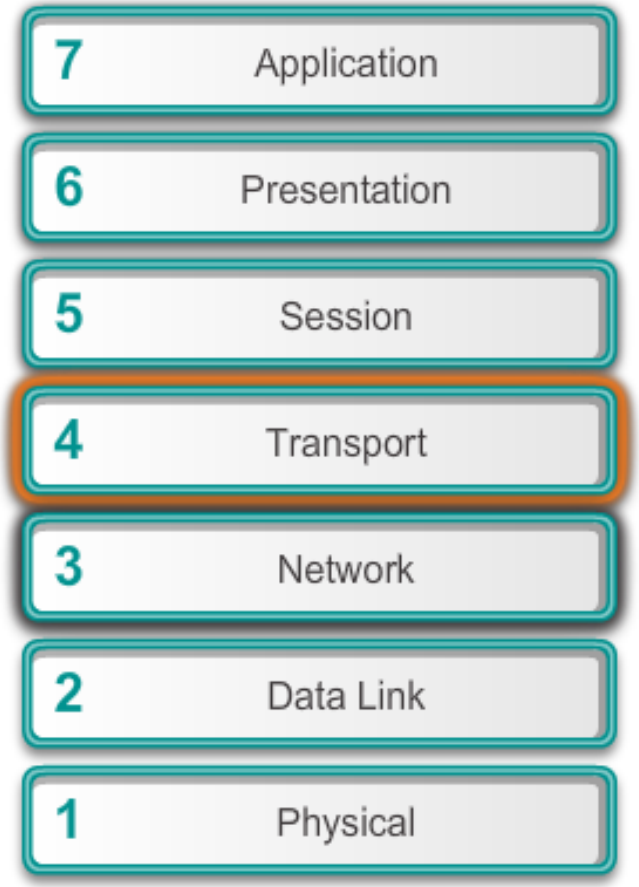
Network Layer Troubleshooting



Transport Layer Troubleshooting – ACLs

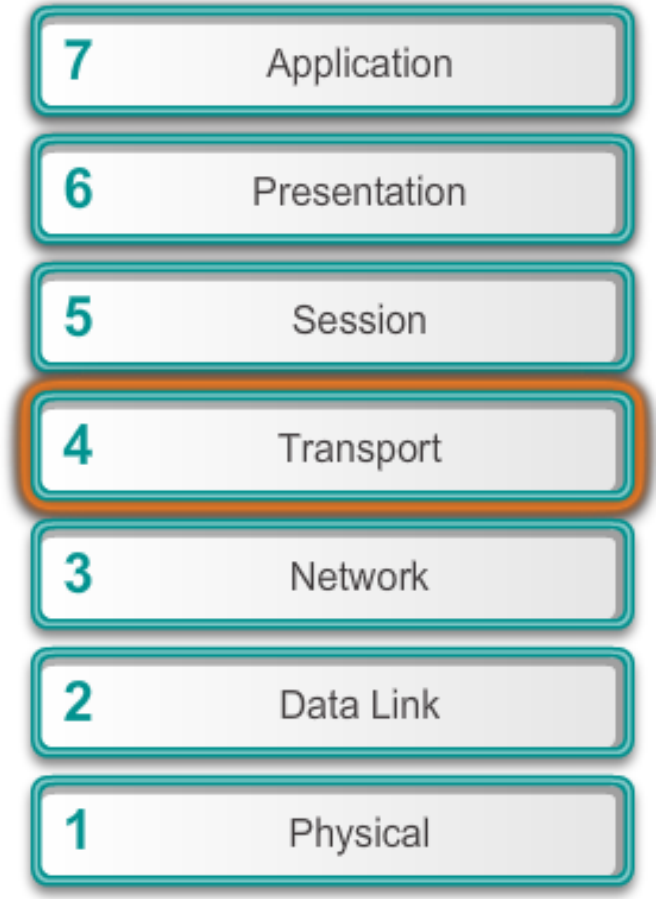
Common ACL Misconfigurations

- Selection of traffic flow
- Order of ACL entries
- Implicit deny all
- Address and IPv4 wildcard masks
- Selection of transport layer protocol
- Source and destination ports
- Use of the `established` keyword
- Uncommon protocols

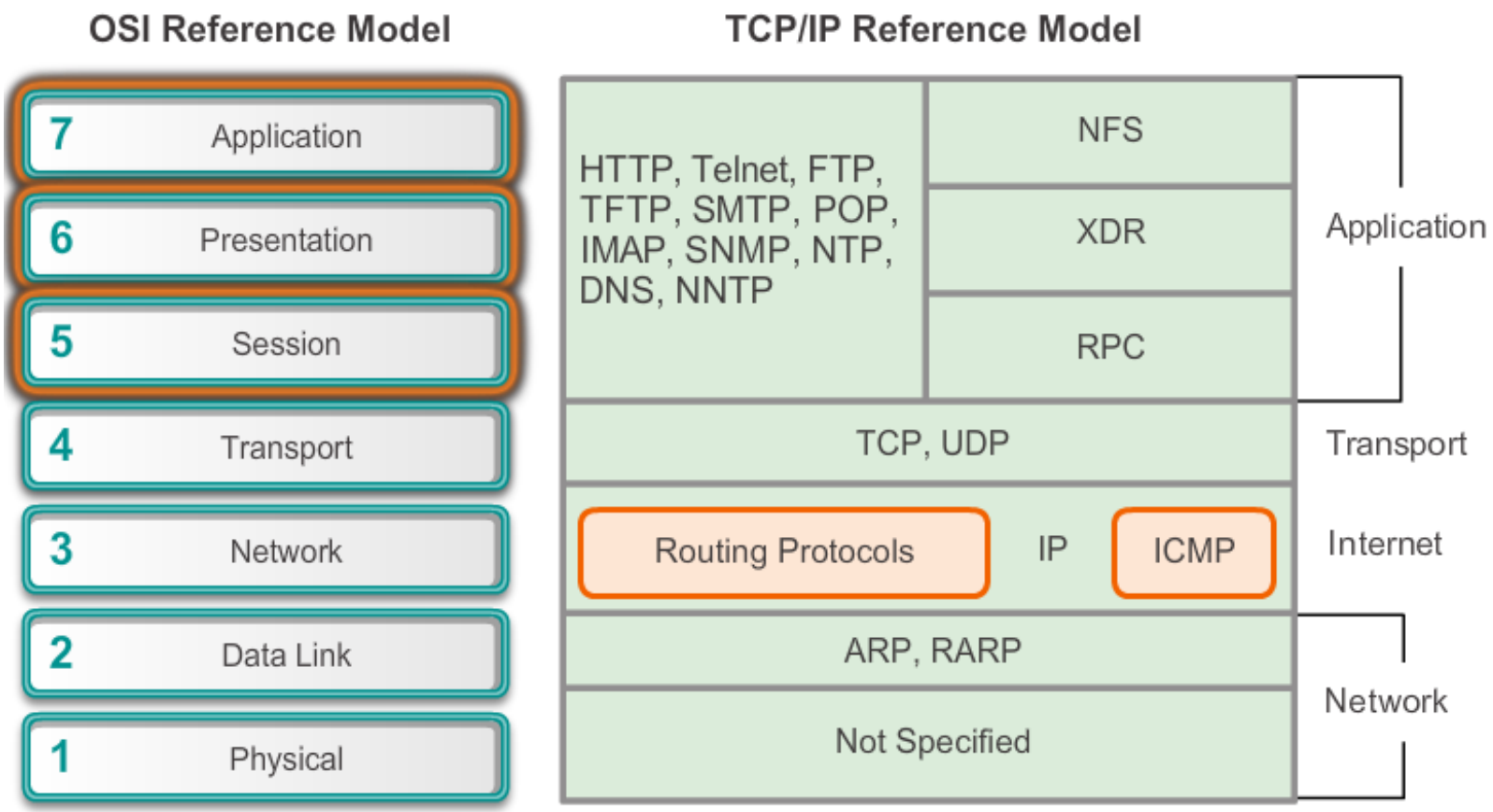


Transport Layer Troubleshooting – NAT for IPv4

Common Interoperability Areas
- BOOTP and DHCP
- DNS and WINS
- SNMP
- Tunneling and encryption protocols



Application Layer Troubleshooting



Components of Troubleshooting End-to-End Connectivity

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

Step 1. Check physical connectivity at the point where network communication stops, including 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.

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

Step 4. Verify that the default gateway is correct.

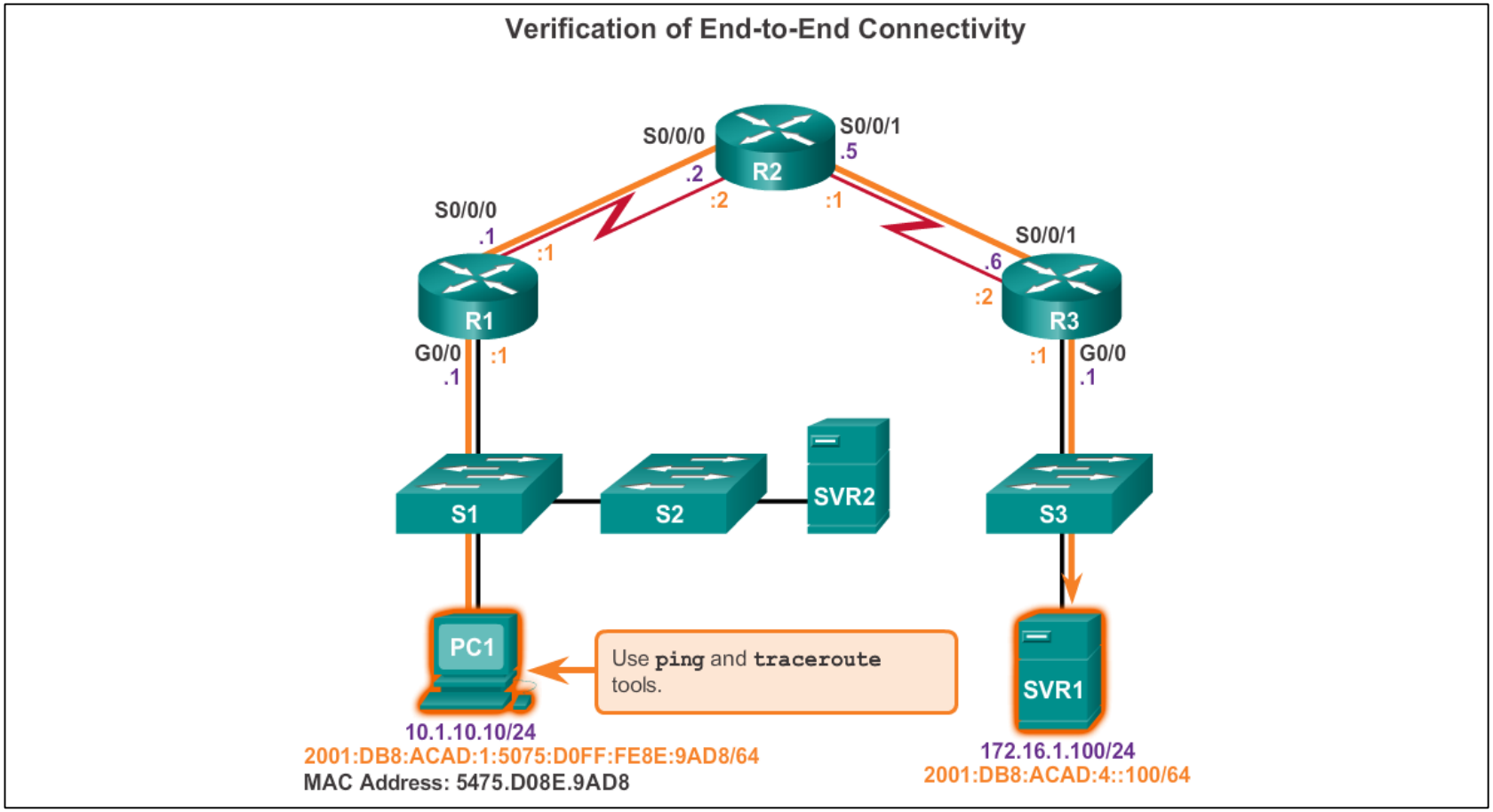
Step 5. Ensure that devices are determining the correct path from the source to the destination. Manipulate the routing information if necessary.

Step 6. Verify that the transport layer is functioning properly. Telnet can 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 an accessible DNS server.

End-to-End Connectivity Problem Initiates Troubleshooting



Step 1. Verify the Physical Layer

```
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#
```

Step 2. Check for Duplex Mismatches

Duplex configuration guidelines:

- Point-to-point Ethernet links should always run in full-duplex mode.
- Half-duplex is not common anymore and mostly encountered if hubs are used.
- Autonegotiation of speed and duplex is recommended.
- If autonegotiation does not work, manually set the speed and duplex on both ends.
- Half-duplex on both ends performs better than a duplex mismatch.

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

IPv4:

- **arp** command (PC)
- **show mac address-table** command (router)

Verify the IPv4 Default Gateway

```
R1# show ip route
<output omitted>
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
```

```
C:\Windows\system32> route print
<output omitted>

Network Destination  Netmask   Gateway     Interface     Metric
         0.0.0.0     0.0.0.0   10.1.10.2   10.1.10.100      11
```

IPv6:

- **netsh interface ipv6 show neighbor** command (PC)
- **show ipv6 neighbors**

Verify the IPv6 Default Gateway

```
PC1> ipconfig
Windows IP Configuration
 Connection-specific DNS Suffix :
 IPv6 Address. . . . . . . . . . :
2001:db8:acad:1:5075:d0ff:fe8e:9ad8
 Link-local IPv6 Address . . . . : fe80::5075:d0ff:fe8e:9ad8%13
 IPv4 Address. . . . . . . . . . : 10.1.1.100
 Subnet Mask . . . . . . . . . . : 255.255.255.0
 Default Gateway . . . . . . . . : fe80::1
                                   10.1.10.1
```

Step 4. Verify Default Gateway

Verify the IPv4 Default Gateway

```
R1# show ip route
<output omitted>
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
```

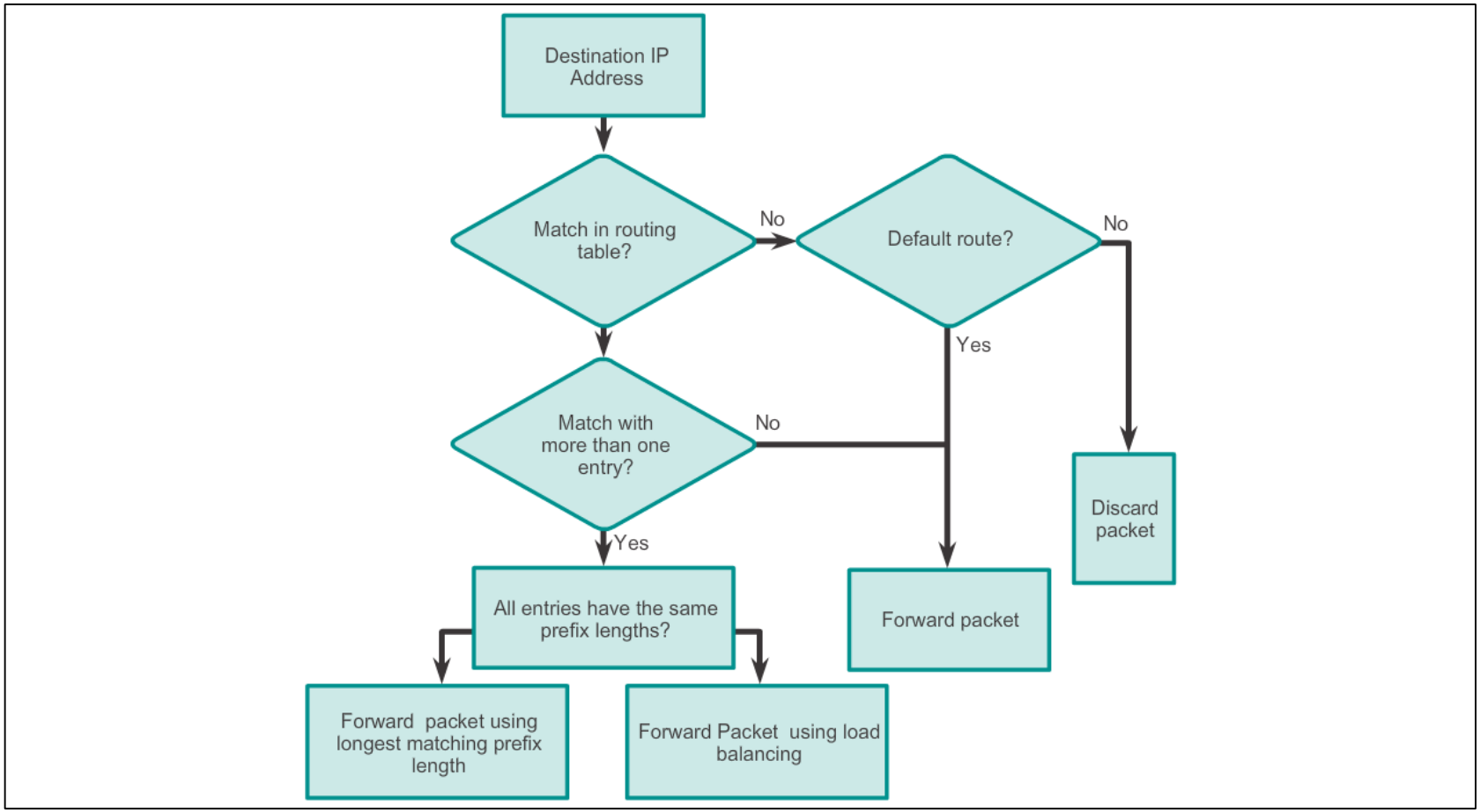
```
C:\Windows\system32> route print
<output omitted>

Network Destination  Netmask    Gateway     Interface     Metric
         0.0.0.0     0.0.0.0    10.1.10.2  10.1.10.100       11
```

Verify the IPv6 Default Gateway

```
PC1> ipconfig
Windows IP Configuration
 Connection-specific DNS Suffix :
 IPv6 Address. . . . . . . . . . :
2001:db8:acad:1:5075:d0ff:fe8e:9ad8
 Link-local IPv6 Address . . . . : fe80::5075:d0ff:fe8e:9ad8%13
 IPv4 Address. . . . . . . . . . : 10.1.1.100
 Subnet Mask . . . . . . . . . . : 255.255.255.0
 Default Gateway . . . . . . . . : fe80::1
                                   10.1.10.1
```

Step 5. Verify Correct Path



Step 6. Verify the Transport Layer

Successful Telnet Connection Over IPv4

```
PC1> telnet 2001:DB8:172:16::100
HQ#
```

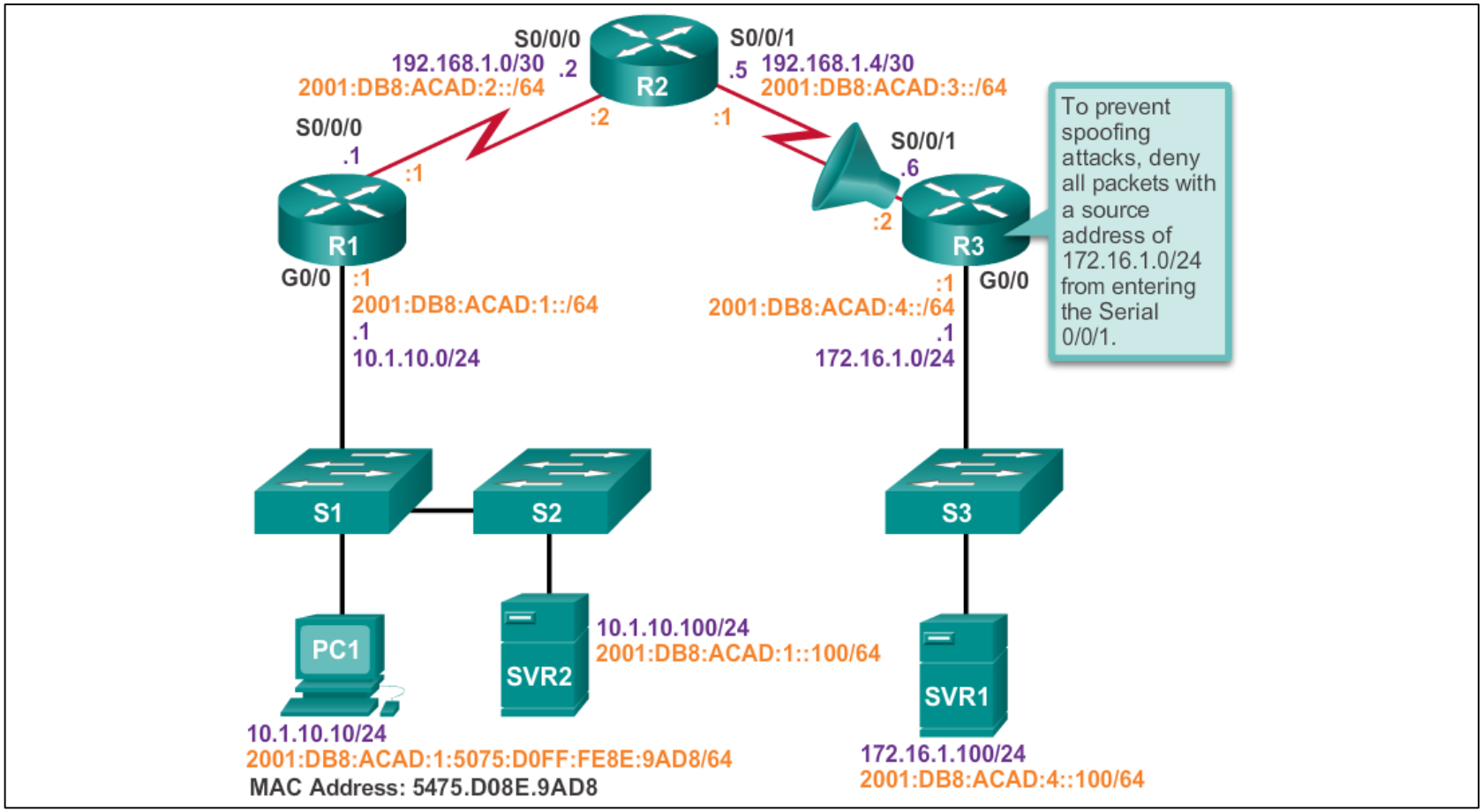
Successful Telnet Connection Over IPv6

```
R1# telnet 2001:db8:acad:3::2
Trying 2001:DB8:ACAD:3::2 ... Open

User Access Verification

Password:
R3>
```

Step 7. Verify ACLs



Step 8. Verify DNS

```
R1(config)# ip host ipv4-server 172.16.1.100
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(config)# ipv6 host ipv6-server 2001:db8:acad:4::100
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#
```

Chapter 9: Summary