Chapter 8: Network Troubleshooting

Connecting Networks

Cisco | Networking Academy®
Mind Wide Open™

8.1 Troubleshooting Methodology

Cisco | Networking Academy®
Mind Wide Open™

1 Network Documentation

- Documentation is critical to being able to monitor and troubleshoot a network.
- Documentation includes:
  - Configuration files
    - Network configuration files
    - End-system configuration files
  - Topology diagrams
    - Physical topology
    - Logical topology
  - A baseline performance levels

Network Configuration Tables

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

Router documentation

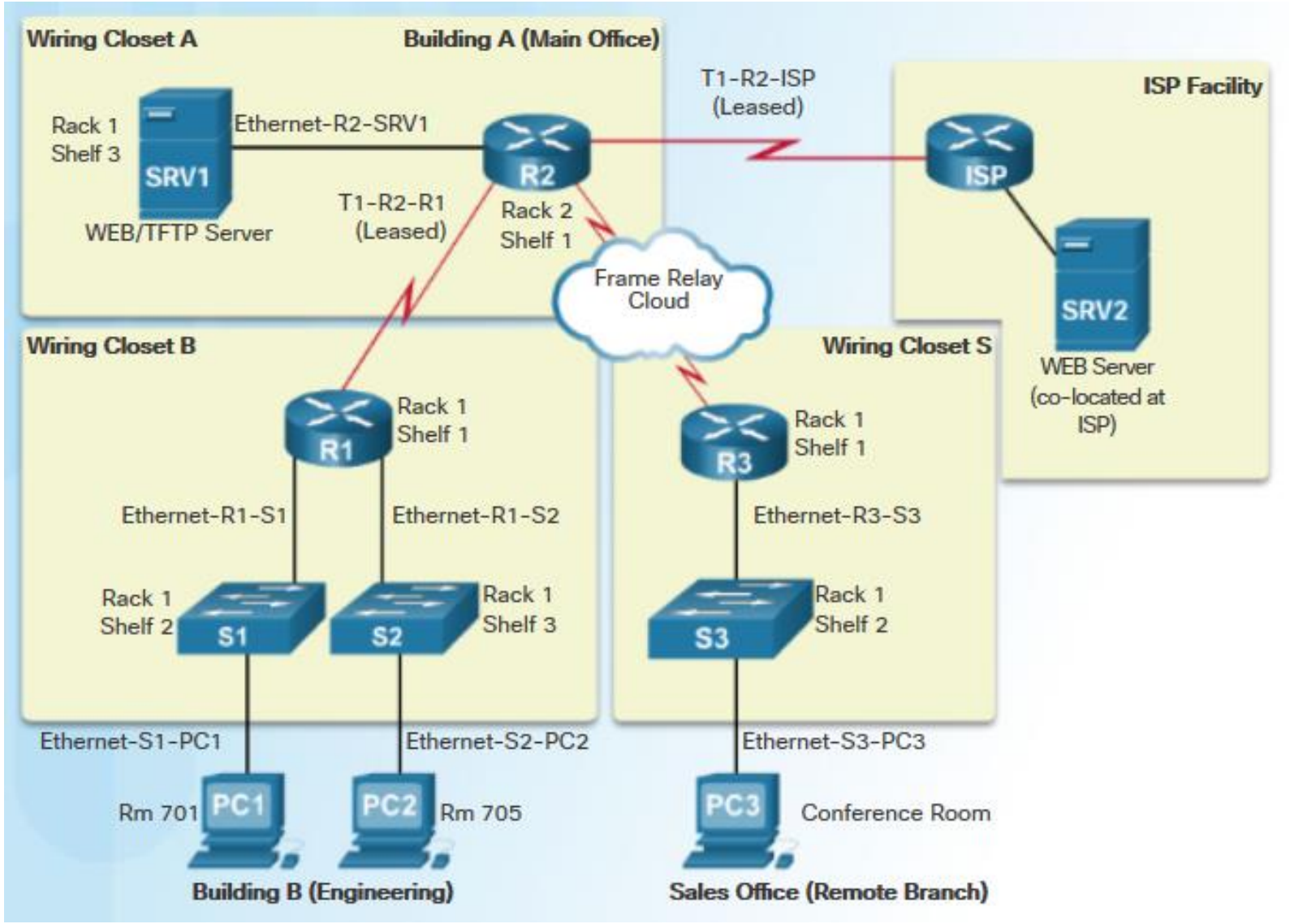
Switch Information	Port	Speed	Duplex	STP	Port Fast	Trunk Status	Ether Channel L2 or L3	VLANs	Key
S1, Cisco WS-2960-24TT, 192.168.10.2/24, 2001:db6:acad:99::2, c2960-lanbasek9-mz.150-2.SE7.bin	G0/1	100 Gb/s	Auto	Fwd	No	On	None	1	Connects to R1
	F0/2	100 Mb/s	Auto	Fwd	Yes	No	None	1	Connects to PC1

Switch documentation

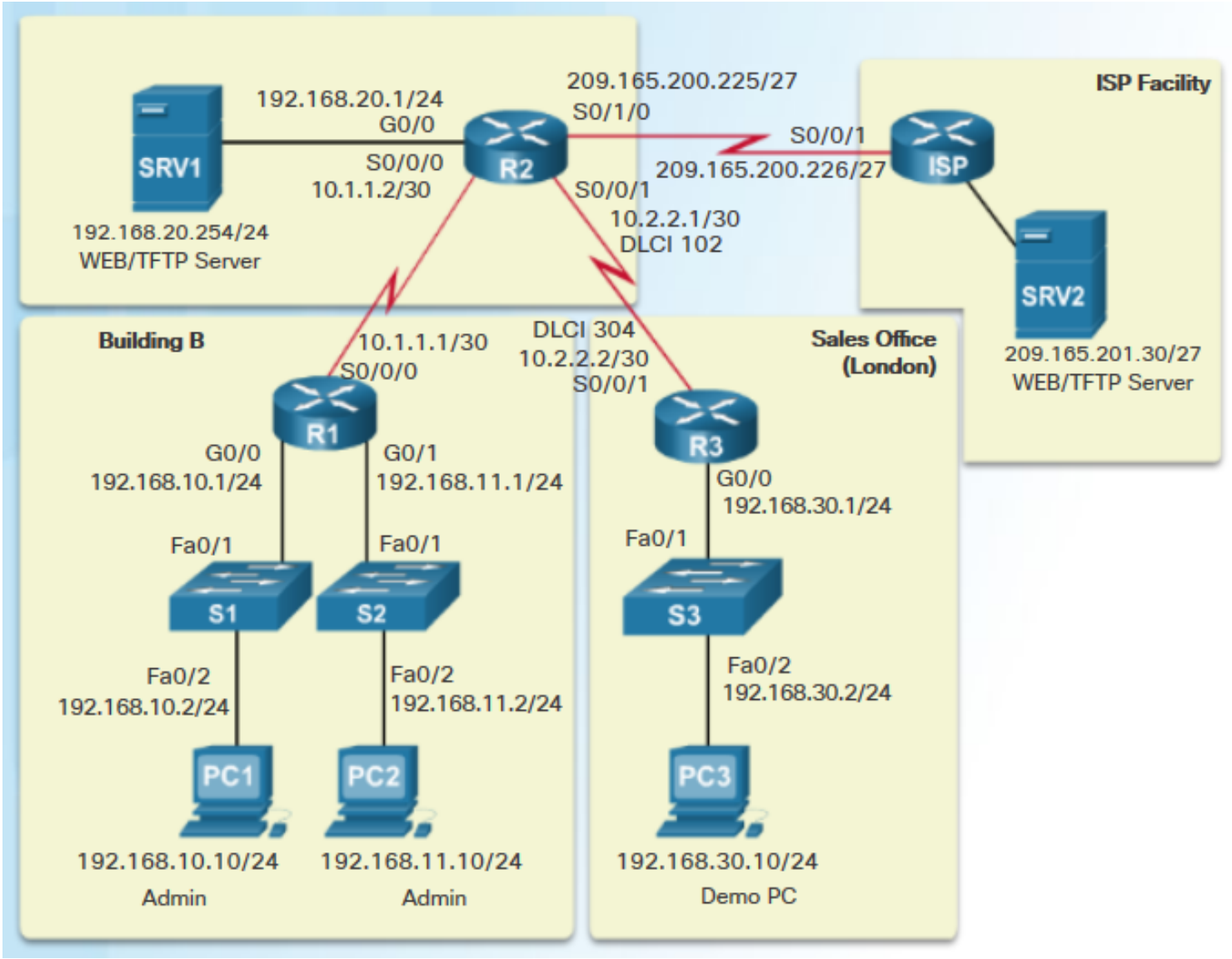
End-System Configuration Tables

Device Name (Purpose)	Operating System / Version	IP Address / Subnet Mask	Default Gateway Address	DNS Server Address	WINS Server Address	Network Applications	High Bandwidth Applications
SRV1 (Web/TFTP Server)	UNIX	192.168.20.254 /24	192.168.20.1 /24	192.168.20.1 /24		HTTP FTP	-
SRV2 (Web Server) co-located at ISP	UNIX	209.165.201.30 /27	209.165.201.1 /27	209.165.201.1 /27		HTTP	-
PC1 (Admin Term)	UNIX	192.168.10.10 /24	192.168.10.1 /24	192.168.10.1 /24		FTP Telnet	VoIP
PC2 (User PC – Engineering)	Windows XP Pro SP2	192.168.11.10 /24	192.168.11.1 /24	192.168.11.1 /24		HTTP FTP	VoIP
PC3 (Demo PC – Marketing)	Windows XP Pro SP2	192.168.30.10 /24	192.168.30.1 /24	192.168.30.1 /24		HTTP	Streaming Video VoIP

Physical Network Topology

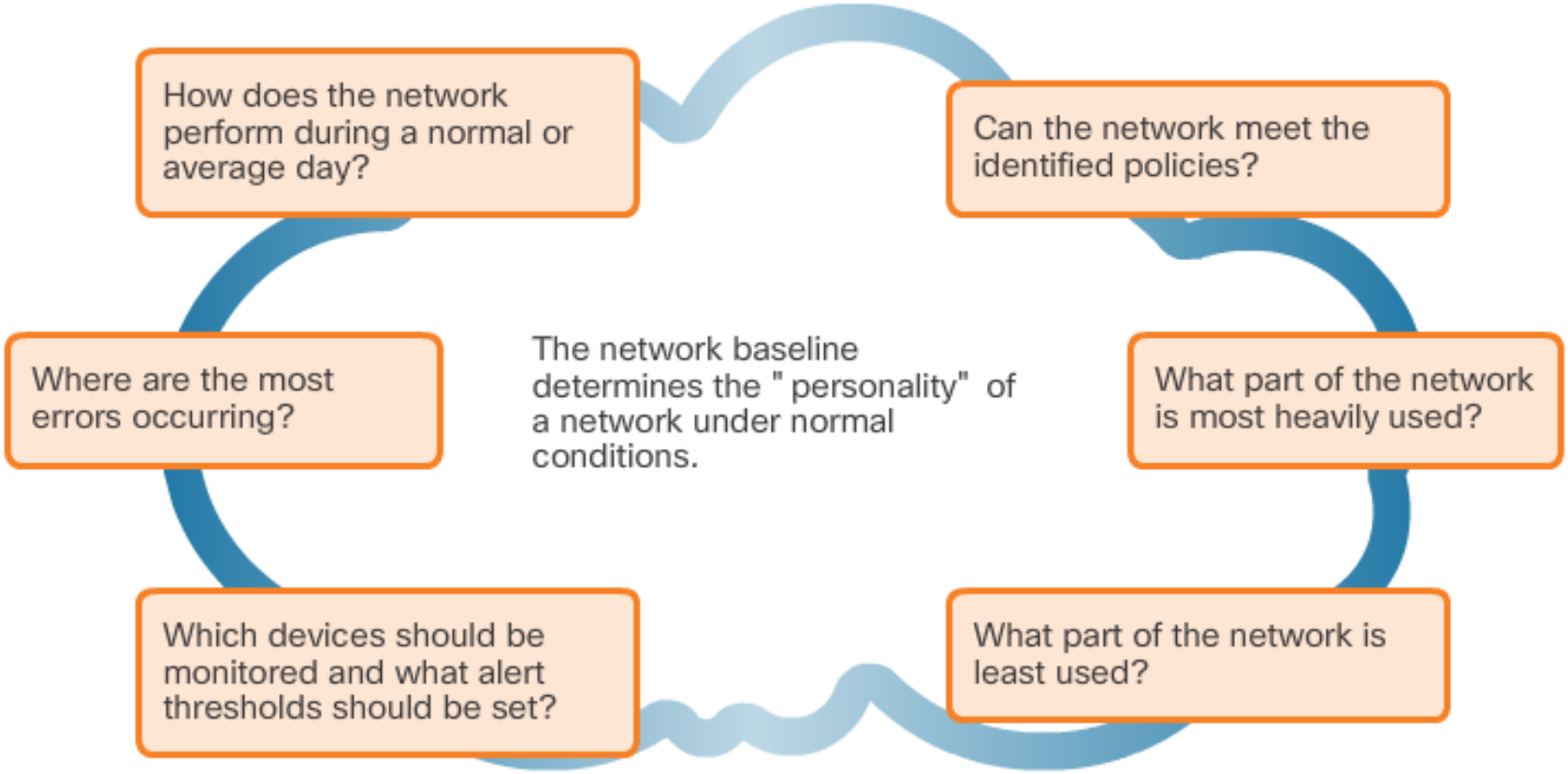


Logical Network Topology

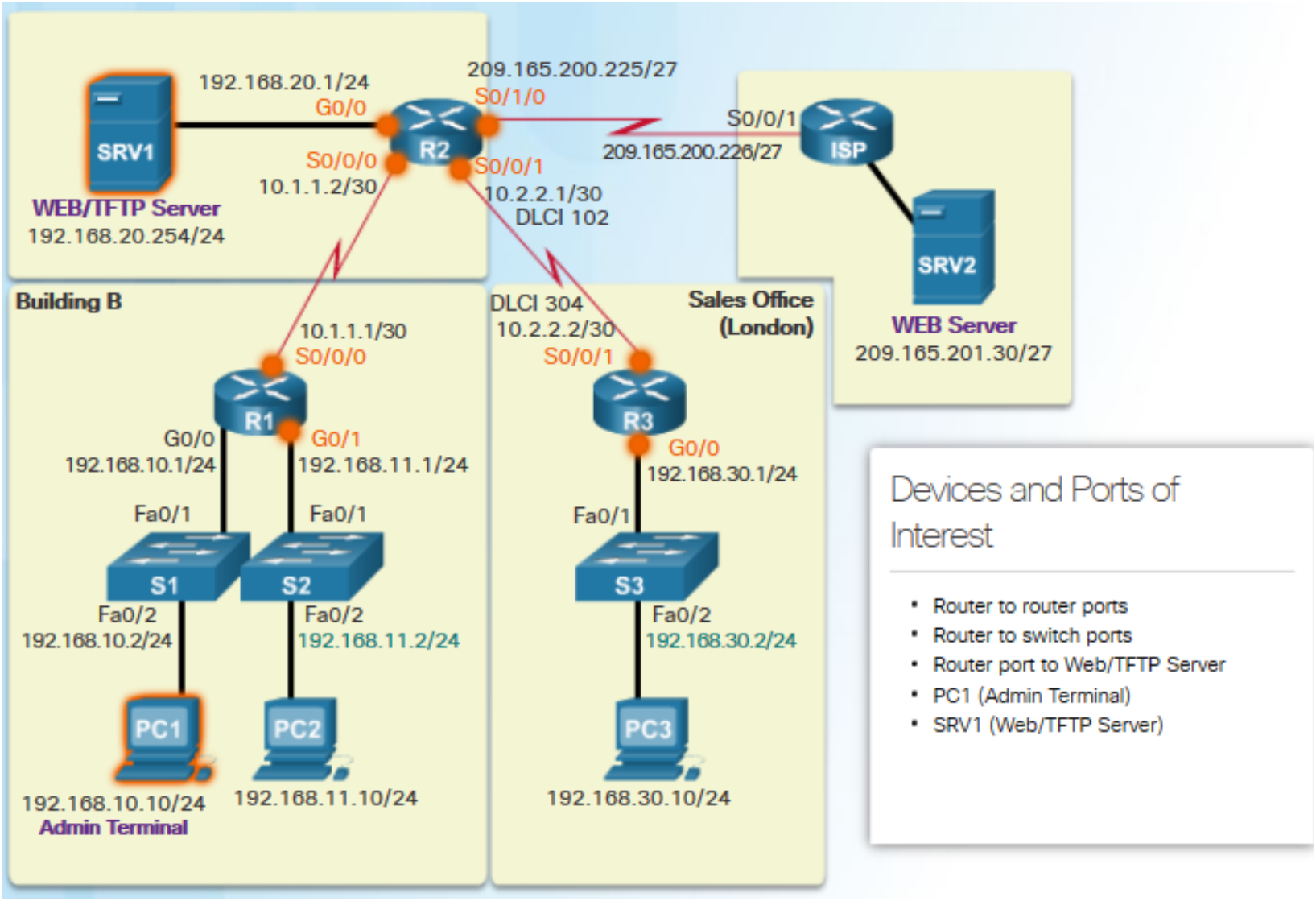


Establishing a Network Baseline

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



Identifying devices and ports of interest



Devices and Ports of Interest

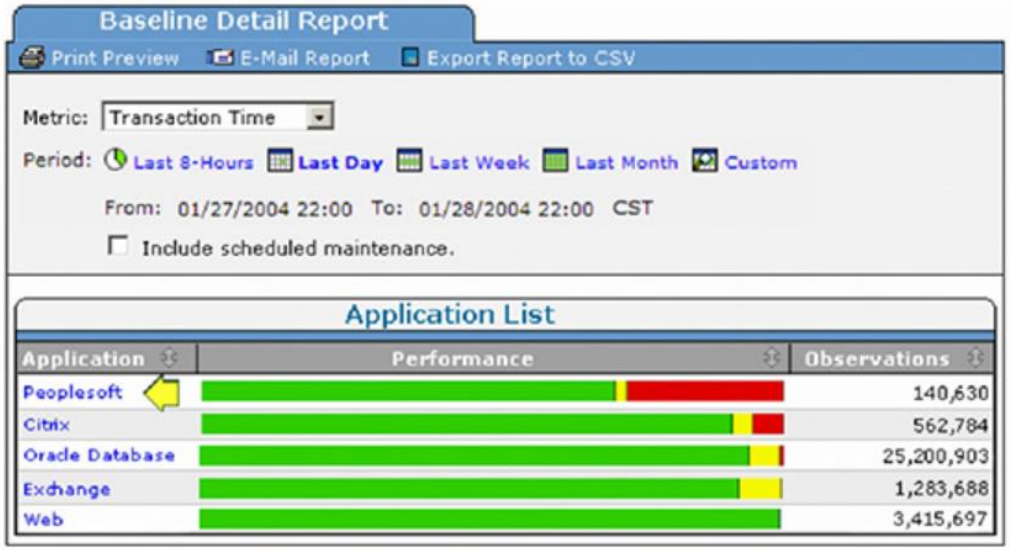
- Router to router ports
- Router to switch ports
- Router port to Web/TFTP Server
- PC1 (Admin Terminal)
- SRV1 (Web/TFTP Server)

Measuring Data

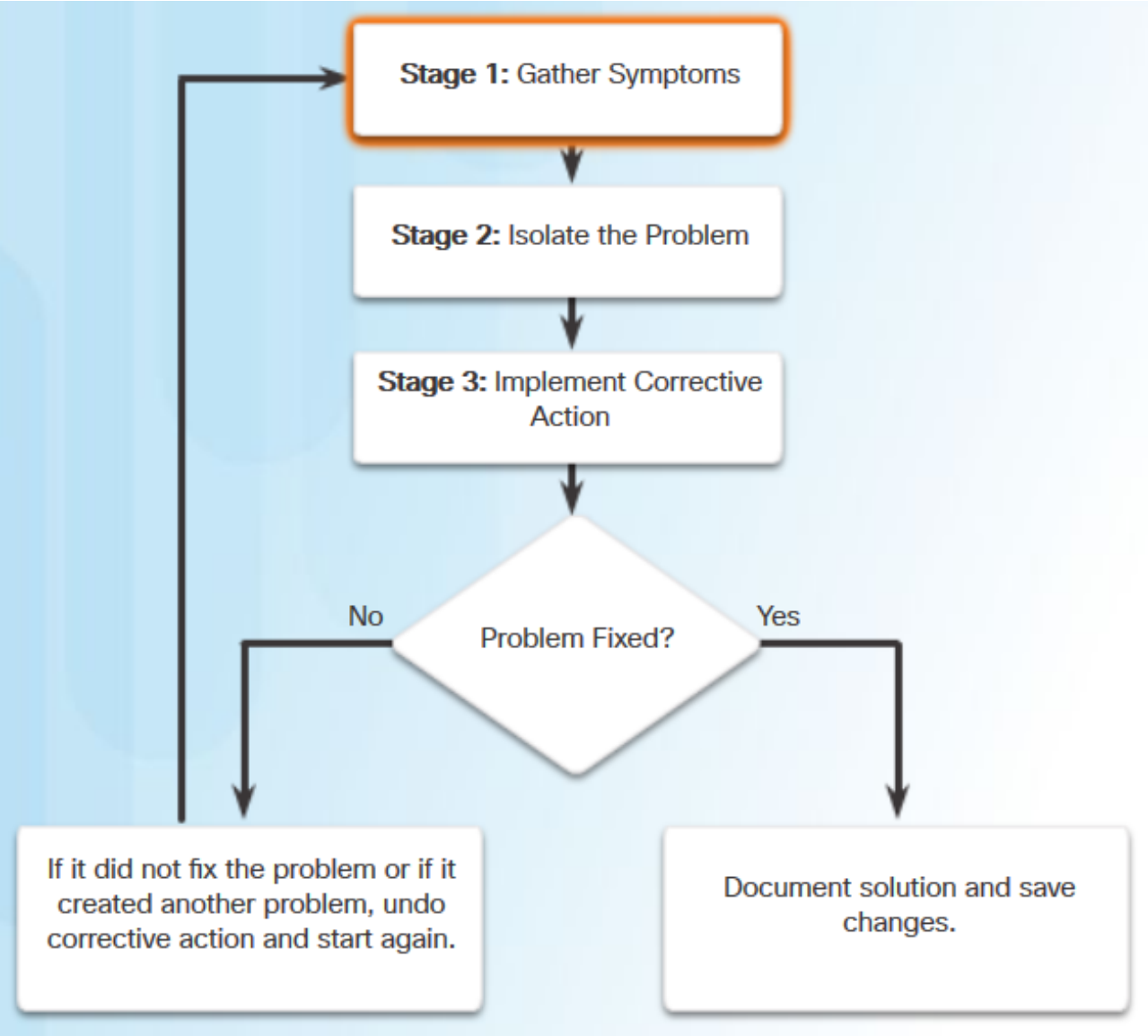
Command	Description
`show version`	Shows uptime, version information for device software and hardware.
`show ip interface [brief]` `show ipv6 interface [brief]`	Shows all the configuration options that are set on an interface. Use the **brief** keyword to only show up/down status of IP interfaces and 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.

Manual collection of data

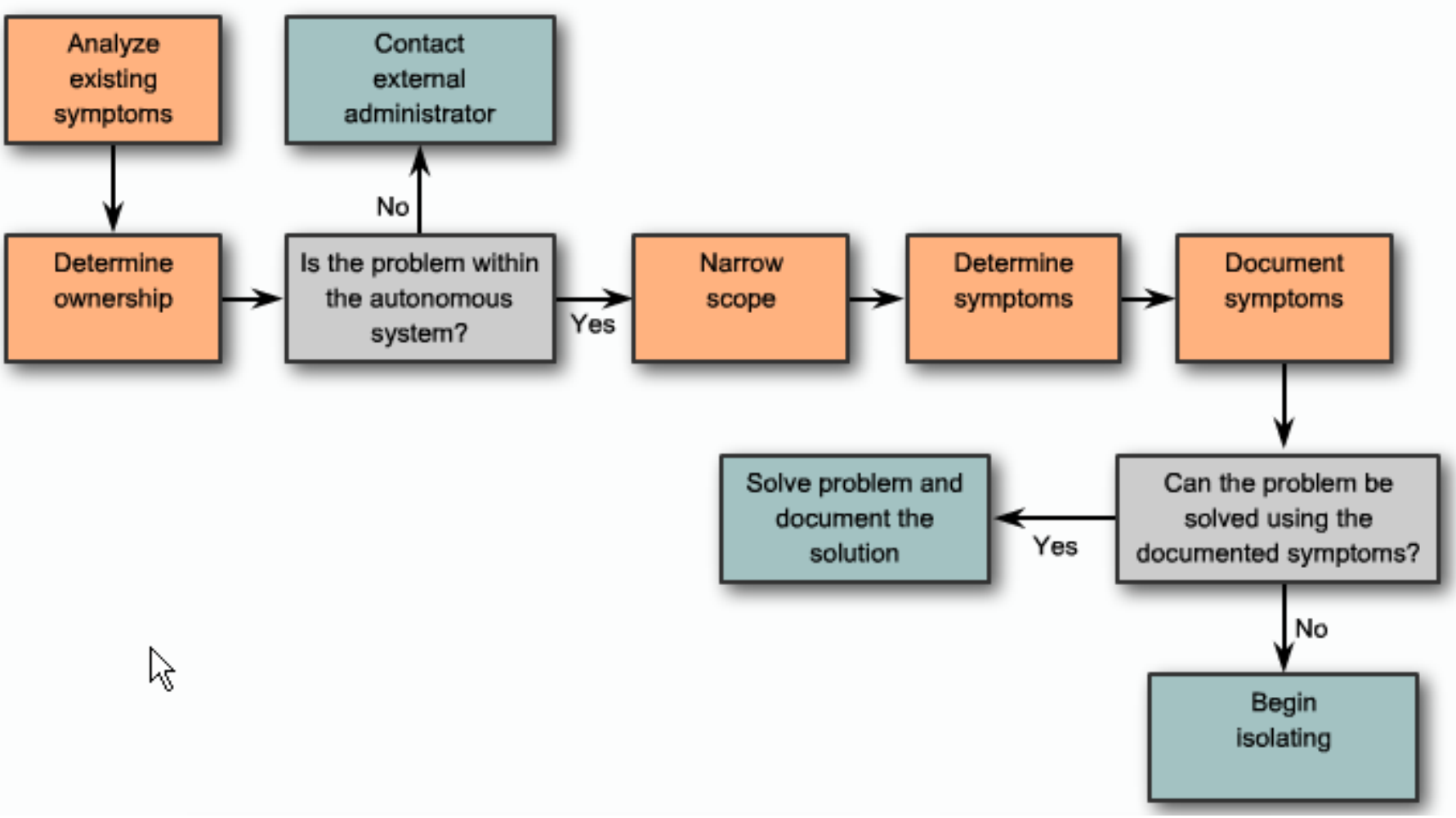
Automated tools



2 Troubleshooting Process



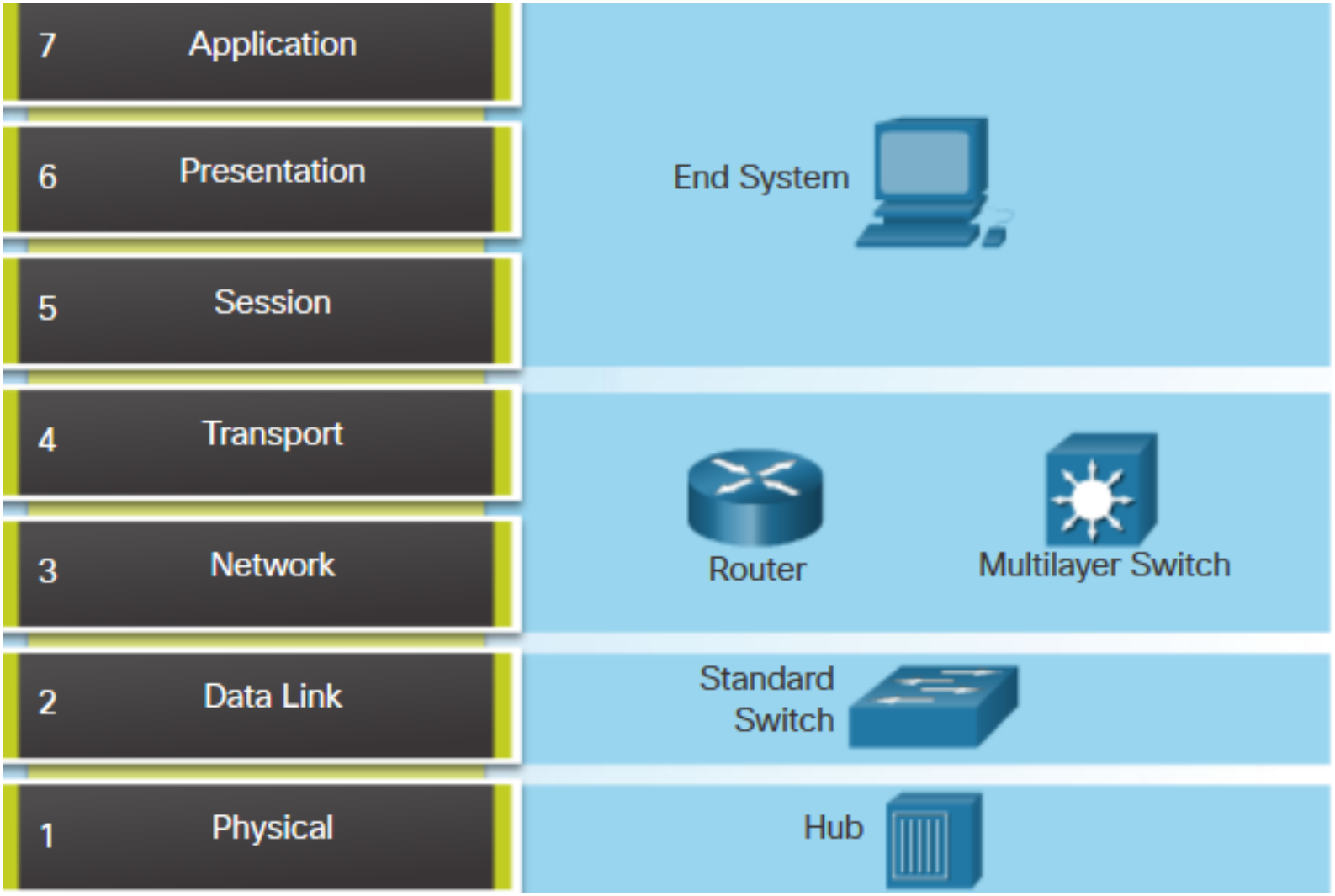
Gathering Symptoms



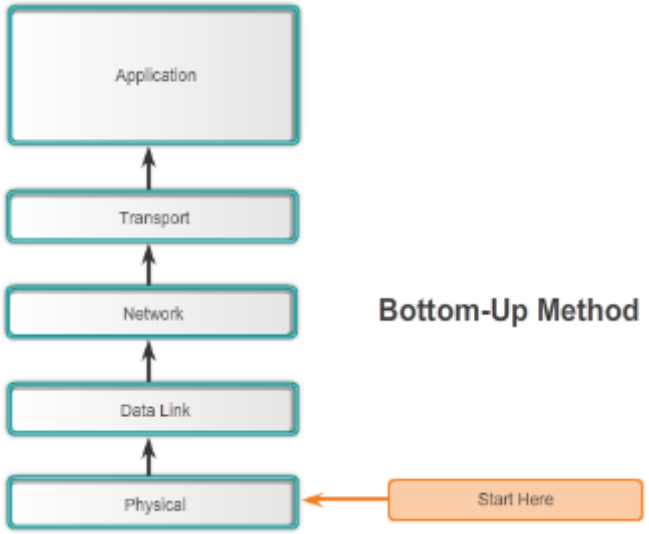
Gathering Symptoms

Command	Description
ping {*host*|*ip-address*}	Sends an echo request packet to an address, then waits for a reply. The *host* or *ip-address* variable is the IP alias or IP address of the target system.
traceroute {*destination*}	Identifies the path a packet takes through the networks. The *destination* variable is the hostname or IP address of the target system.
telnet {*host*|*ip-address*}	Connects to an IP address using the Telnet application.
ssh -l *userid ip-address*	Connects to an IP address using SSH.
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 the current IPv4 and IPv6 routing tables, which contains the routes to all known network destinations.
show running-config	Displays contents of currently running configuration file.
[no] debug ?	Displays a list of options for enabling or disabling debugging events.
show protocols	Displays the configured protocols and shows the global and interface-specific status of any configured Layer 3 protocol.

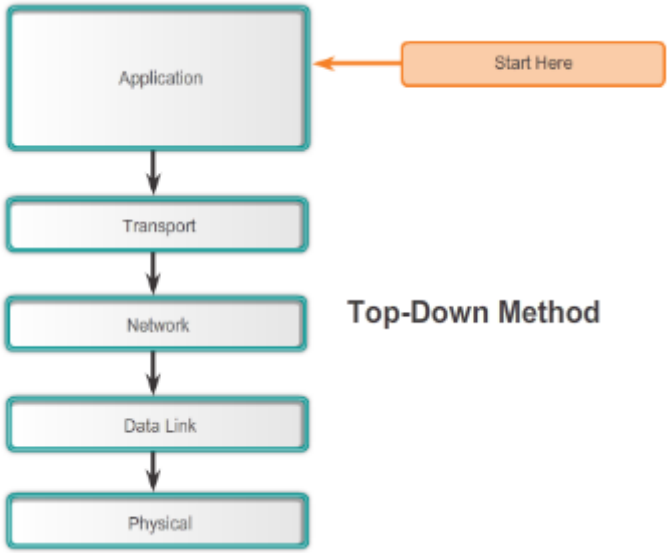
Using Layered Models for Troubleshooting



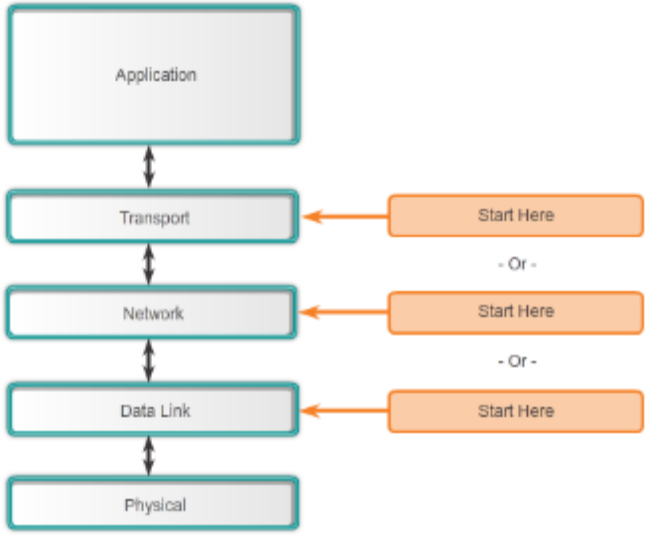
Troubleshooting Methods



Bottom-Up Method



Top-Down Method

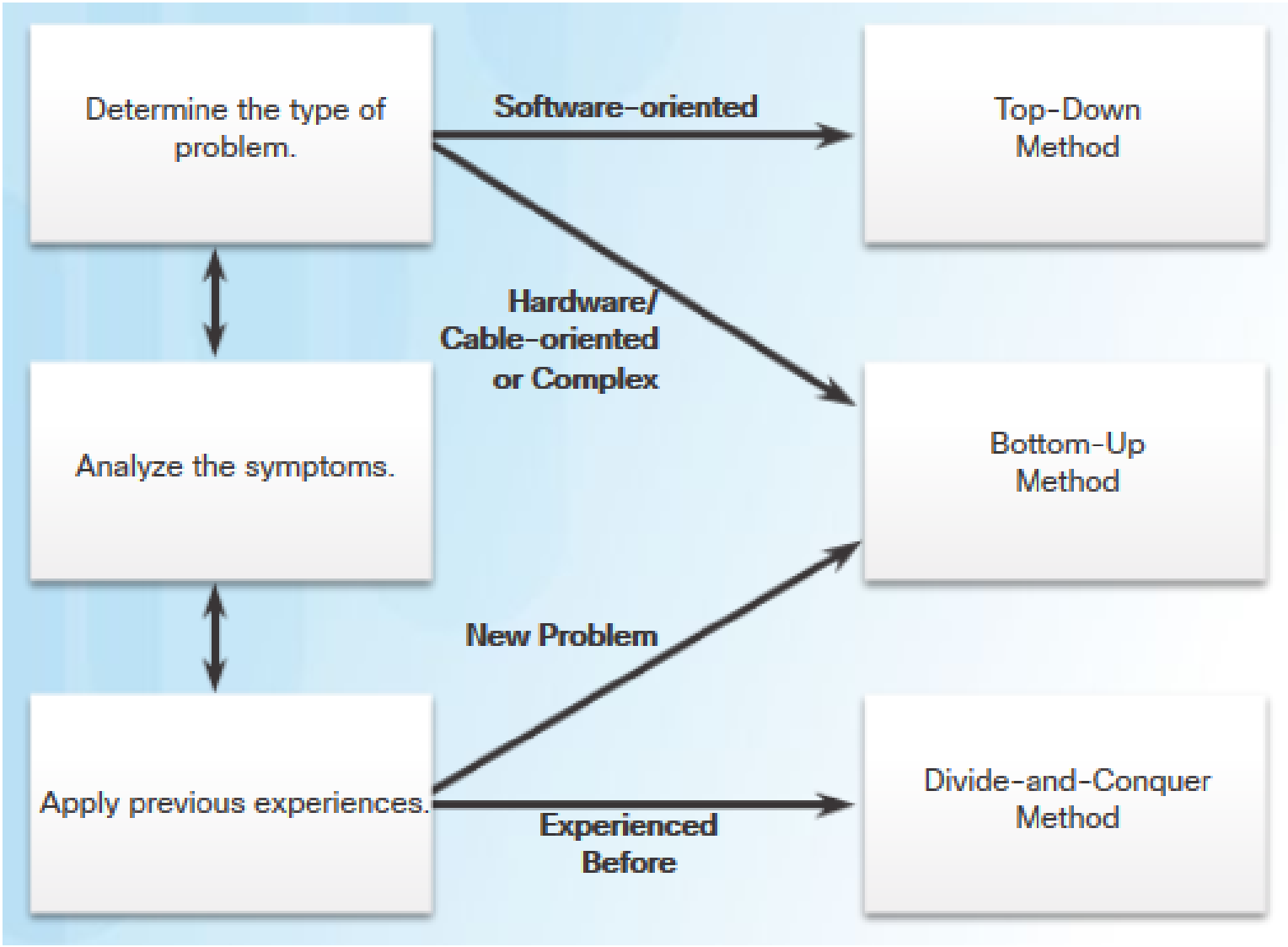


Divide-And-Conquer Method

Another Troubleshooting Methods

- Educated guess
  - By an expert network administrator.
  - Based on the symptoms of the problem.
- Comparison
  - Comparing a working and non-working situation and spotting significant differences.
- Substitution
  - Swapping the problematic device with a known, working one.

Guidelines for Selecting a Troubleshooting Method

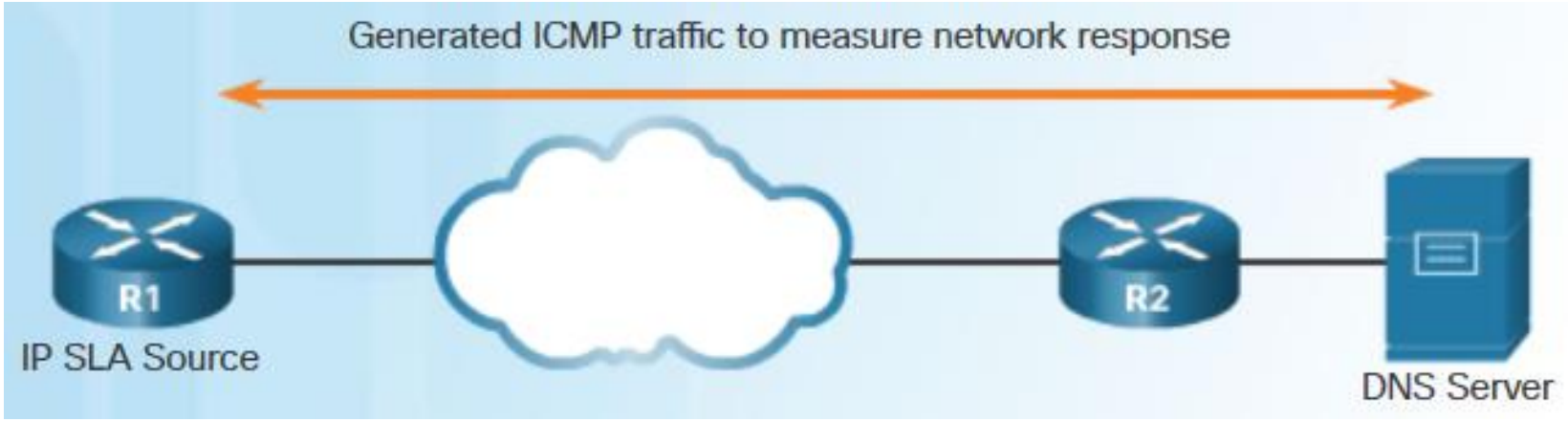


8.2 Troubleshooting Scenarios

Cisco | Networking Academy®
Mind Wide Open™

1 IP SLA Concept

- Cisco IP Service Level Agreement (IP SLA) generates traffic to measure network performance.
  - SLA monitoring, measurement, and verification
  - Measure the jitter, latency, or packet loss in the network
  - IP service network health assessment
  - Edge-to-edge network availability



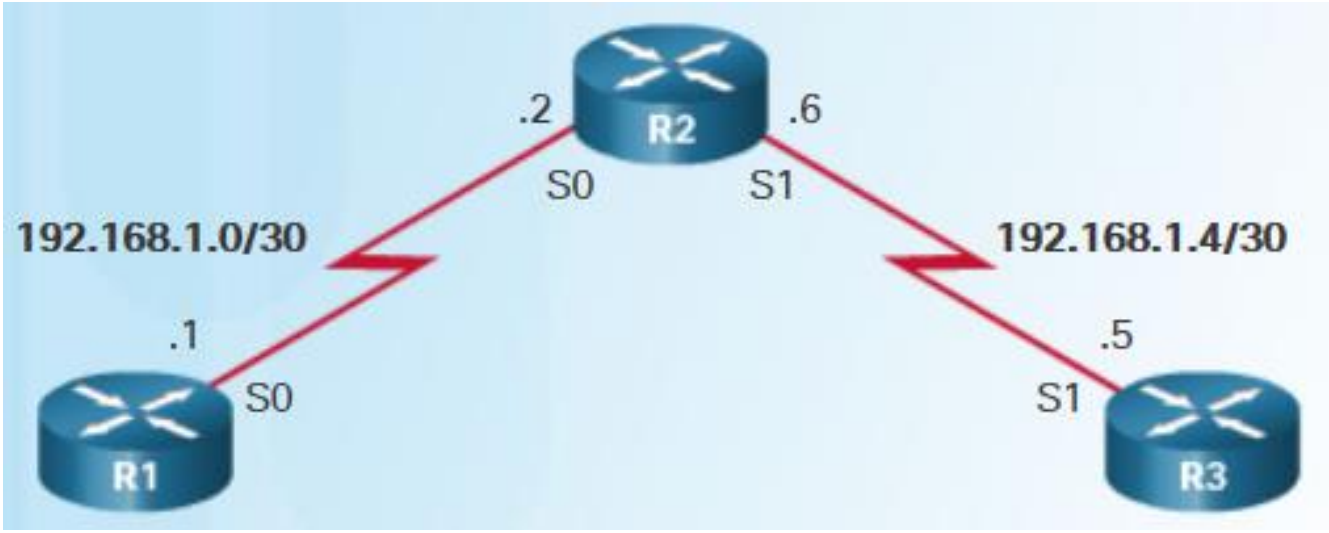
IP SLA Configuration

Router #show ip sla application

```
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
```

IP SLA Configuration

IP SLA ICMP Echo 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#
```

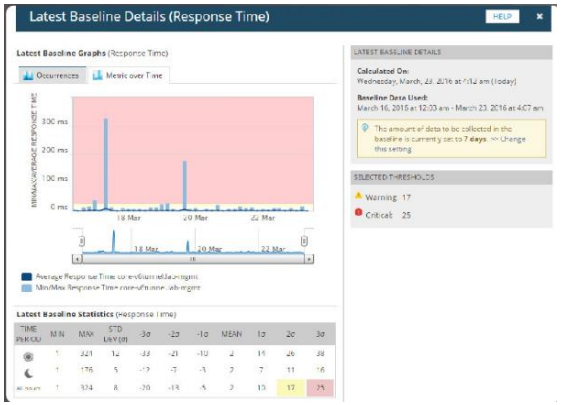
Verifying IP SLA configuration

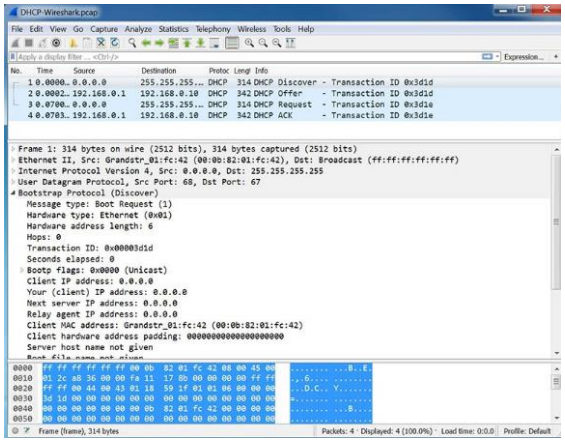
```
R1# show ip sla configuration
IP SLAs Infrastructure Engine-III
Entry number: 1
Owner:
Tag:
Operation timeout (milliseconds): 5000
Type of operation to perform: icmp-echo
Target address/Source address: 192.168.1.5/0.0.0.0
Type Of Service parameter: 0x0
Request size (ARR data portion): 28
Verify data: 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:
History Statistics:
   Number of history Lives kept: 0
   Number of history Buckets kept: 15
   History Filter Type: None
```

```
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
```

2 Software Troubleshooting Tools

- Network Management System Tools
  - IBM QRadar, SolarWinds Log & Event Management, HP Arcsight
  - Zabbix, Nagios, PRTG
- Knowledge Bases
  - Cisco Tools & Resources, Fluke Knowledge Base, Google
- Baselining Tools
  - create network diagrams, measure network baseline
  - help keep network software and hardware documentation up-to-date
- Protocol Analyzers
  - investigate packet content while flowing through the network





HardwareTroubleshooting Tools

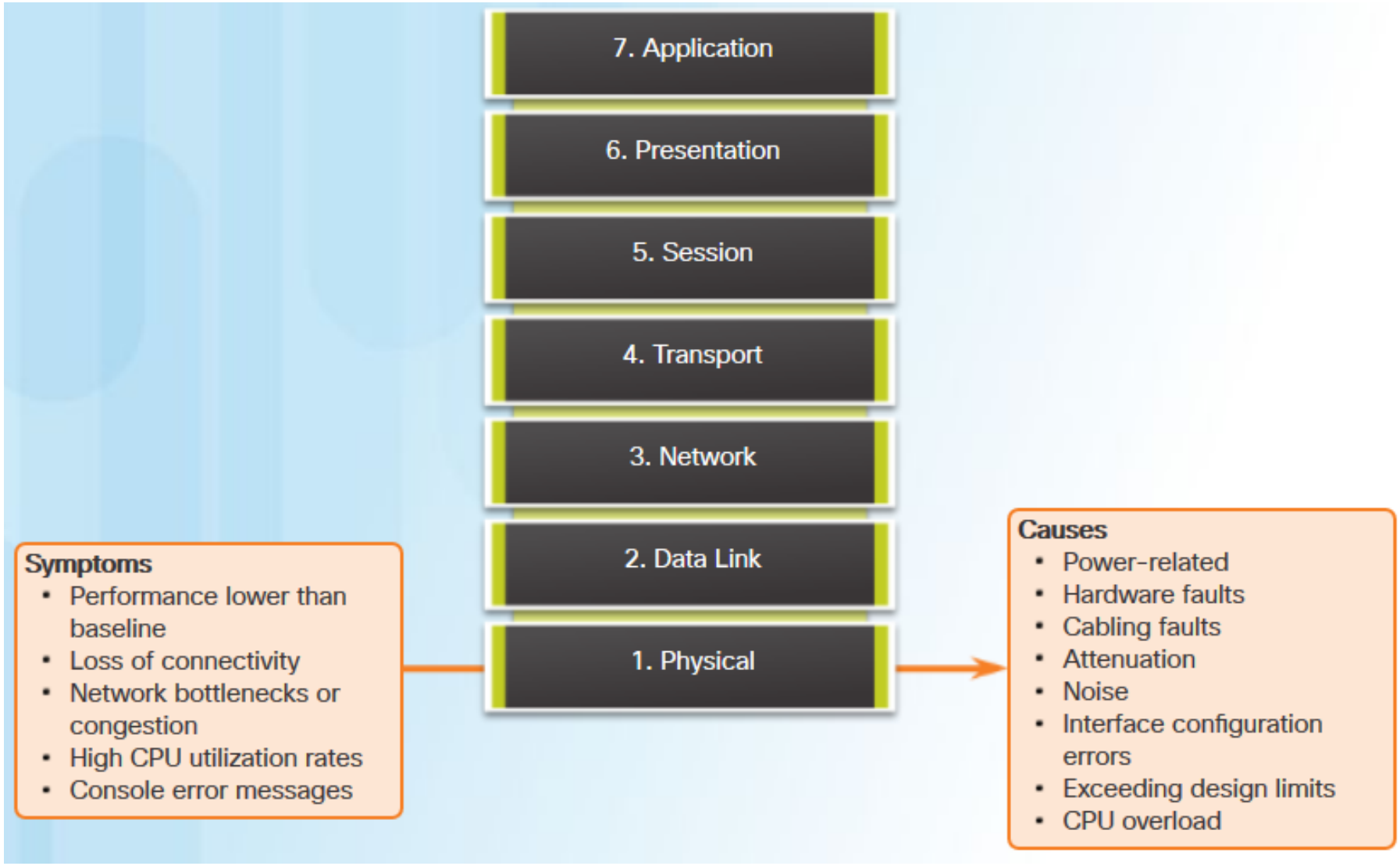
- Network analysis module (NAM)
- Digital multimeters
- Cable testers
  - Fluke MicroMapper, MicroScanner, IntelliTone
- Cable analyzers
  - Fluke CableIQ, DTX Cable Analyzer
- Portable network analyzers
  - Fluke OptiView, Bluelight BL400A

Using a Syslog Server for Troubleshooting

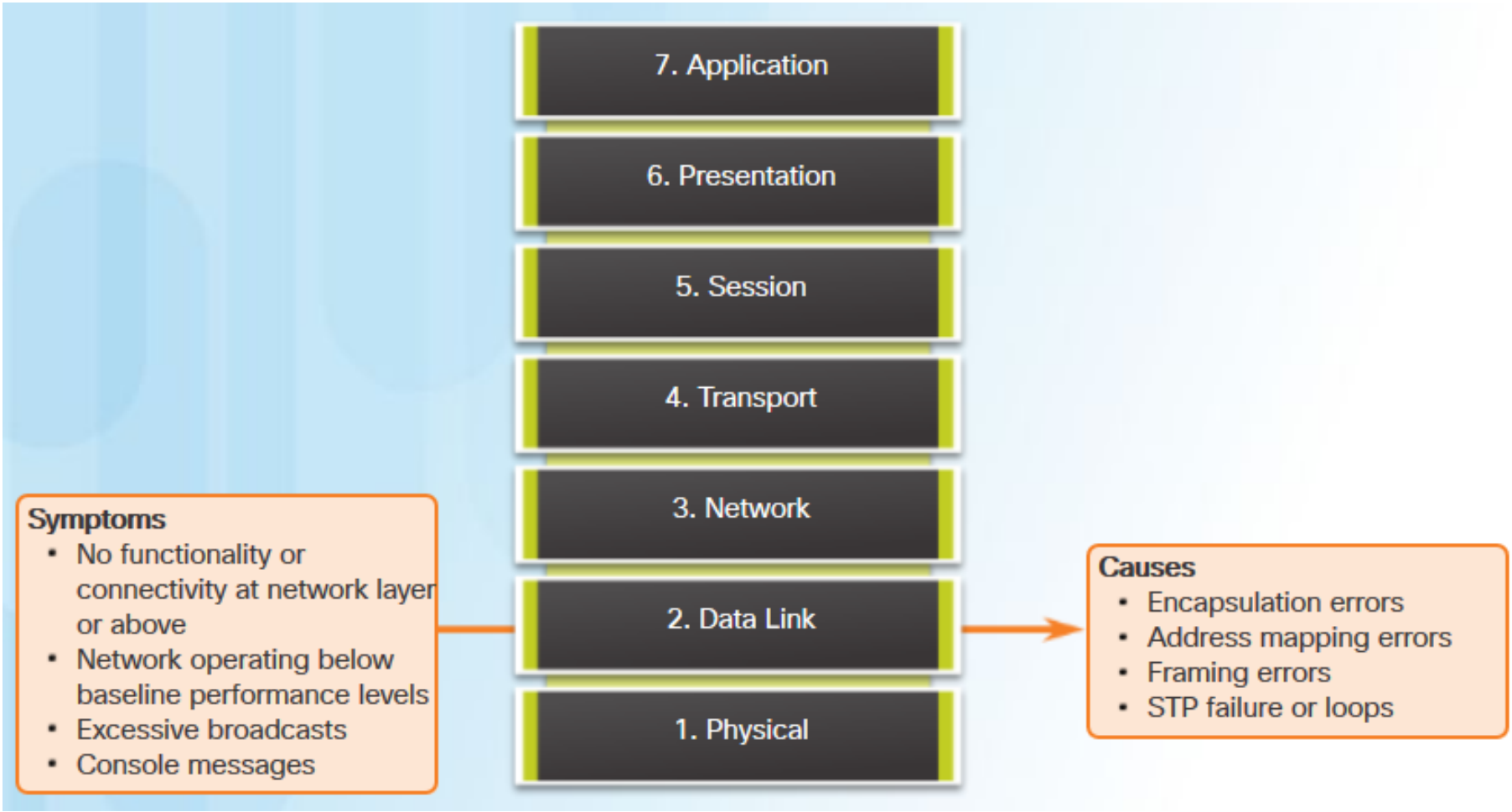
	Level	Keyword	Description	Definition
Highest Level	0	emergencies	System is unusable	LOG_EMERG
	1	alerts	Immediate action is needed	LOG_ALERT
	2	critical	Critical conditions exist	LOG_CRIT
	3	errors	Error conditions exist	LOG_ERR
	4	warnings	Warning conditions exist	LOG_WARNING
	5	notifications	Normal (but significant) condition	LOG_NOTICE
	6	informational	Informational messages only	LOG_INFO
Lowest Level	7	debugging	Debugging messages	LOG_DEBUG

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

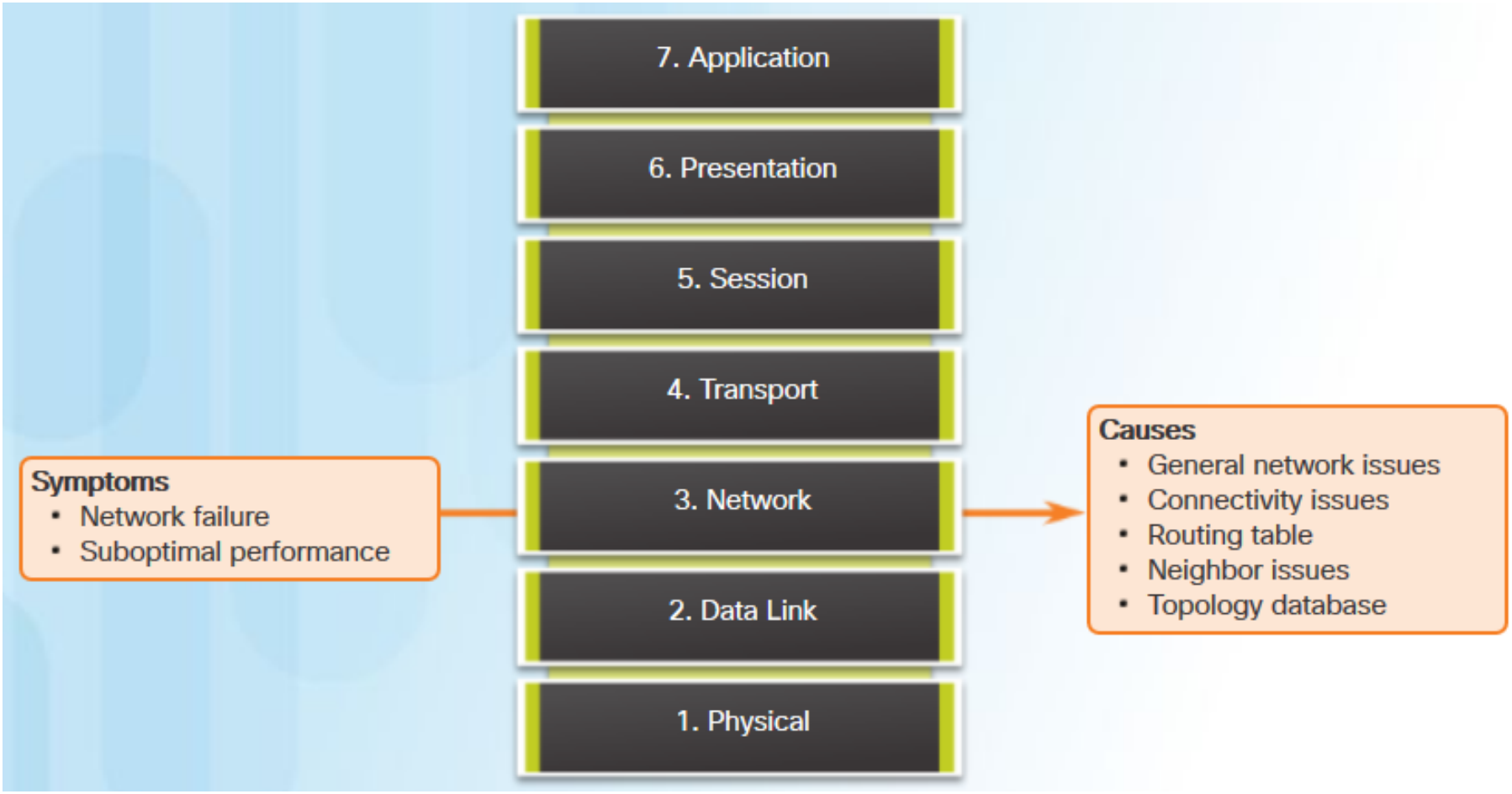
3 Network Troubleshooting: Physical Layer



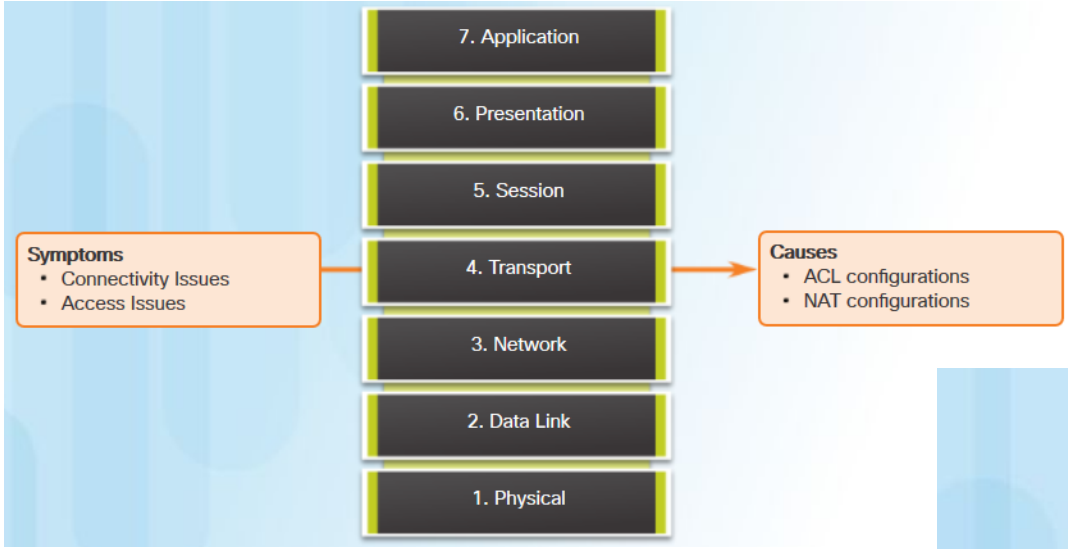
Data Link Layer Troubleshooting

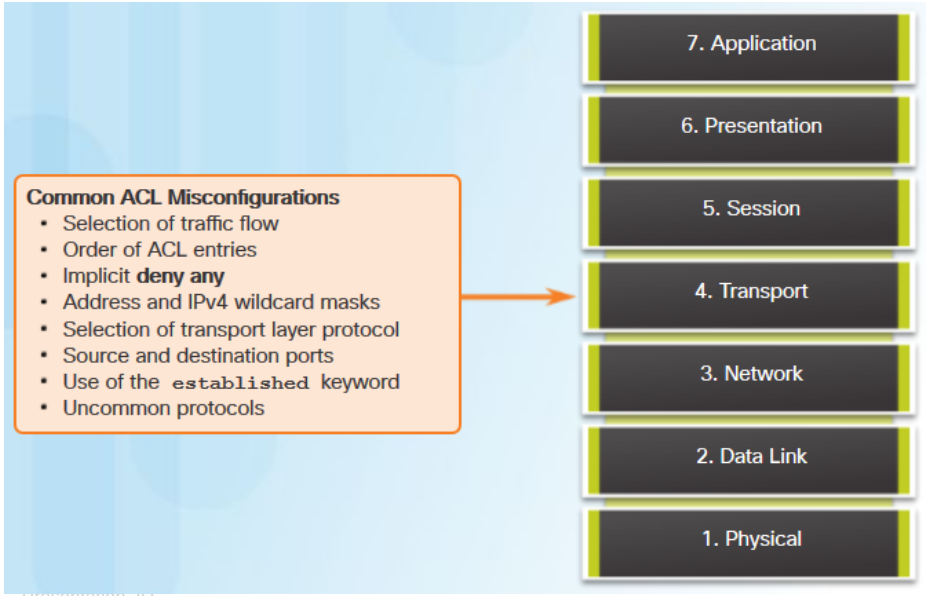


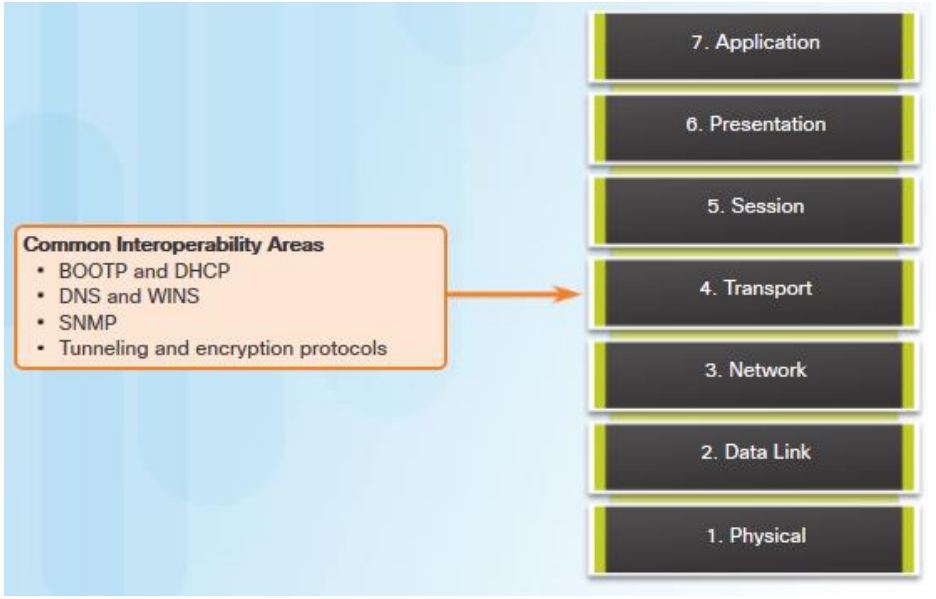
Network Layer Troubleshooting



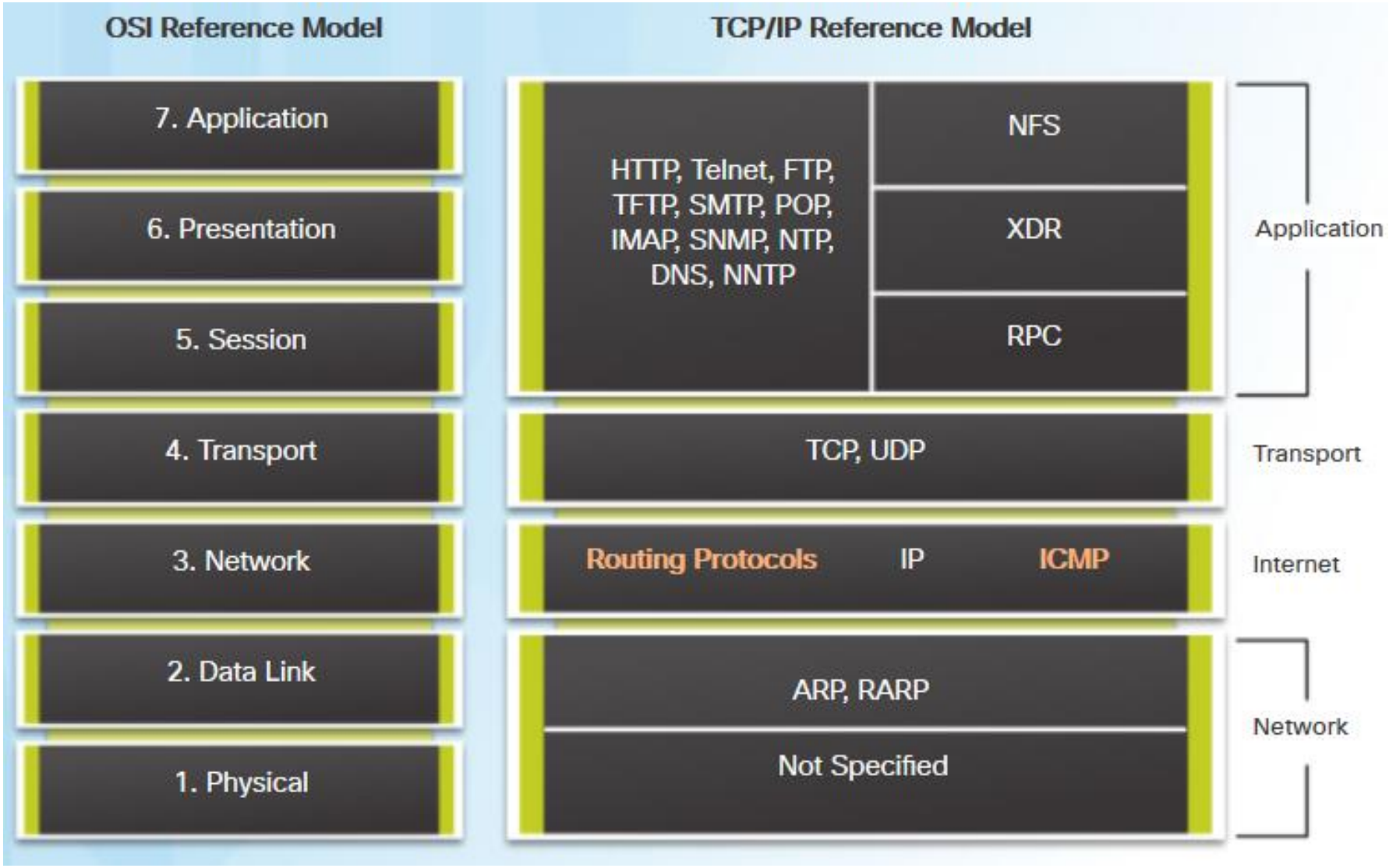
Transport Layer Troubleshooting





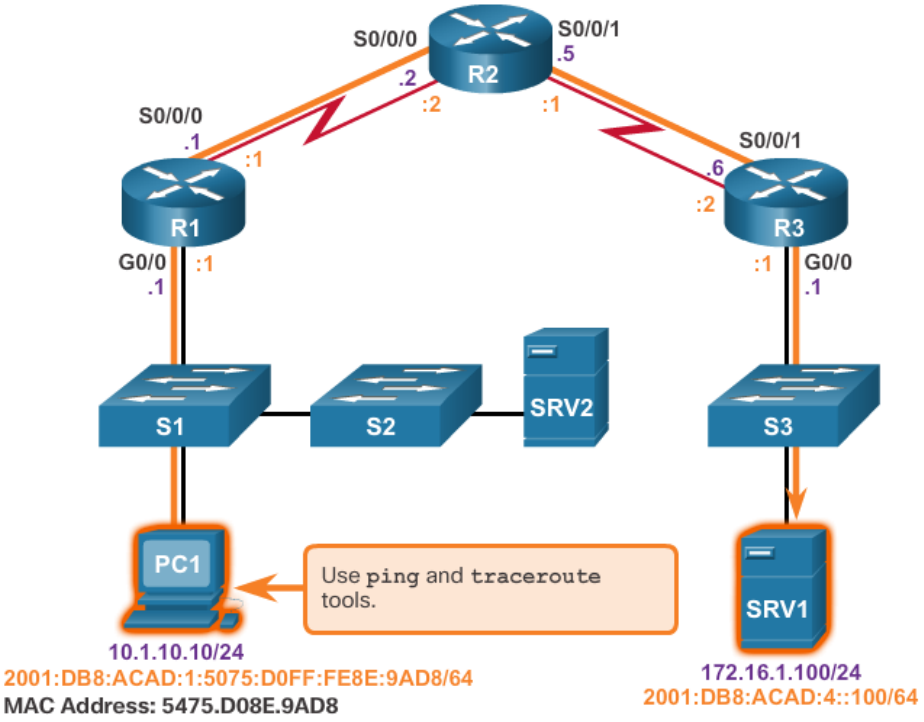


Application Layer Troubleshooting



Troubleshooting IP Connectivity

- **Step 1.** Check physical connectivity
- **Step 2.** Check for duplex mismatches.
- **Step 3.** Check data link and network layer addressing.
- **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.
- **Step 6.** Verify the transport layer is functioning properly.
- **Step 7.** Verify that there are no ACLs blocking traffic.
- **Step 8.** Ensure that DNS settings are correct.



Troubleshooting IP Connectivity

- **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#
```

Troubleshooting IP Connectivity

- **Step 2.** Check for duplex mismatches

Duplex configuration guidelines:

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

```
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>
```

Troubleshooting IP Connectivity

- **Step 3.** Verify L2 and L3 addressing on the LAN

L2 addressing

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

```
PC1> 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
224.0.0.252      01-00-5e-00-00-fc   static
255.255.255.255  ff-ff-ff-ff-ff-ff   static
```

```
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  Fa0/4
 10     000f.34f9.9201      DYNAMIC  Fa0/5
 10     5475.d08e.9ad8      DYNAMIC  Fa0/13
Total Mac Addresses for this criterion: 5
```

L3 addressing

- **netsh interface ipv6 show neighbor**
- **show ipv6 neighbors**

```
PC1> netsh interface ipv6 show neighbor
Interface 13: LAB
Internet Address                Physical Address    Type
------------------------------  ----------------    -------
fe80::9c5a:e957:a865:bde9       00-0c-29-36-fd-f7   Stale
fe80::1                         d4-8c-b5-ce-a0-c0   Reachable (Router)
ff02::2                         33-33-00-00-00-02   Permanent
ff02::16                        33-33-00-00-00-16   Permanent
ff02::1:2                       33-33-00-01-00-02   Permanent
ff02::1:3                       33-33-00-01-00-03   Permanent
ff02::1:ff05:f9fb               33-33-ff-05-f9-fb   Permanent
ff02::1:ffce:a0c0               33-33-ff-ce-a0-c0   Permanent
ff02::1:ff65:bde9               33-33-ff-65-bd-e9   Permanent
ff02::1:ff67:bae4               33-33-ff-67-ba-e4   Permanent
```

```
R1# show ipv6 neighbors
IPv6 Address                              Age  Link-layer Addr  State  Interface
FE80::21E:7AFF:FE79:7A81                    8  001e.7a79.7a81   STALE  Gi0/0
2001:DB8:ACAD:1:5075:D0FF:FE8E:9AD8         0  5475.d08e.9ad8   REACH  Gi0/0
```

Troubleshooting IP Connectivity

- **Step 4.** Verify default gateway

```
C:\Windows\system32> ipconfig
Windows IP Configuration
   Connection-specific DNS Suffix . :
   Link-local IPv6 Address . . . . . : fe80::5075:d0ff:fe8e:9ad8%13
   IPv4 Address. . . . . . . . . . . : 10.1.1.100
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.1.10.1
```

```
R1# show ipv6 route

<output omitted>

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

```
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
```

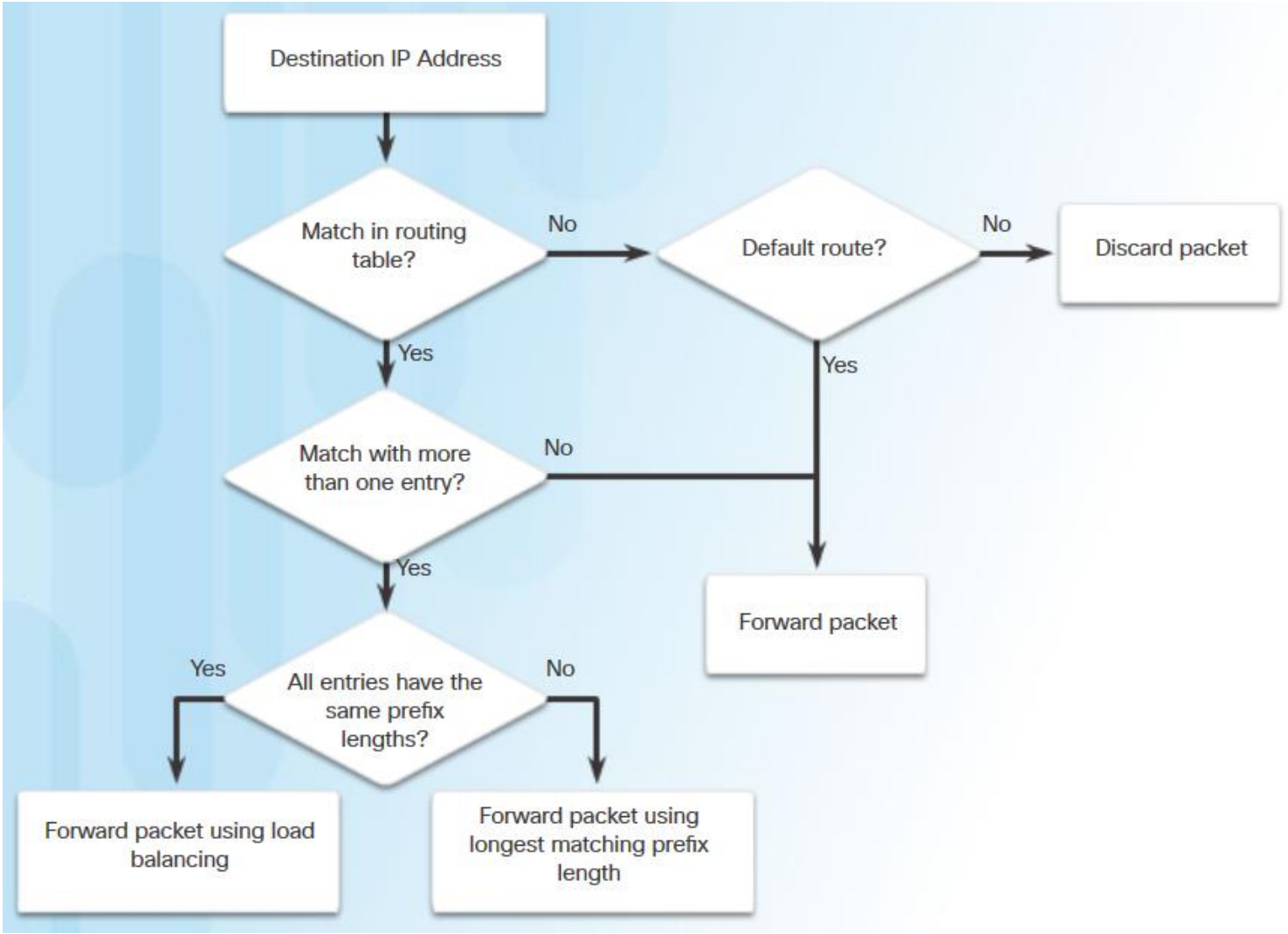
```
R1# show ip route

<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
```

```
R1# show ipv6 interface GigabitEthernet 0/0
GigabitEthernet0/0 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>
```

Troubleshooting IP Connectivity

- **Step 5.** Verify correct path



Troubleshooting IP Connectivity

- **Step 6.** Verify the transport layer

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

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

R1#
```

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

User Access Verification

Password:
R3>
```

```
PC1> telnet 2001:DB8:172:16::100 80
HTTP/1.1 400 Bad Request
Date: Wed, 26 Sep 2012 07:27:10 GMT
Server: cisco-IOS
Accept-Ranges: none
400 Bad Request
Connection to host lost.
```

Troubleshooting IP Connectivity

- **Step 7.** Verify ACLs

```
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
```

Troubleshooting IP Connectivity

- **Step 7.** Verify DNS

```
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#
```