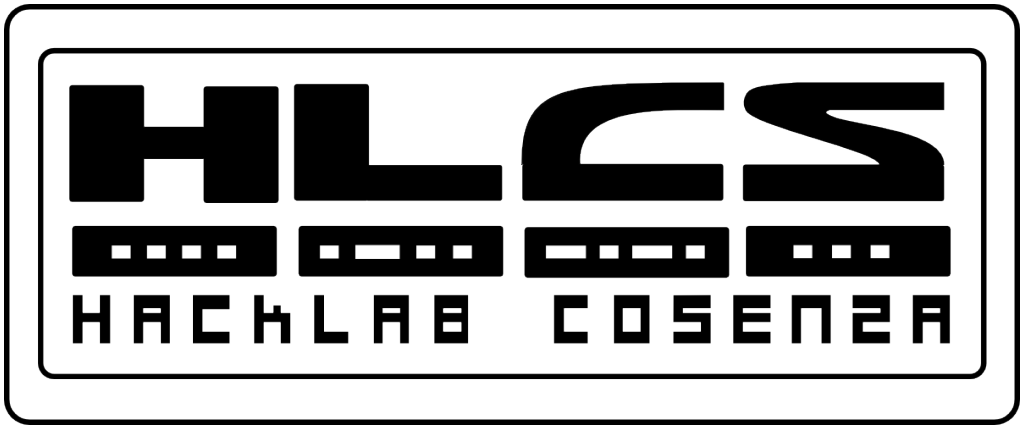


Troubleshooting

Working at a Small-to-Medium Business or ISP – Chapter 9

Overview

After completion of this chapter, you should be able to:

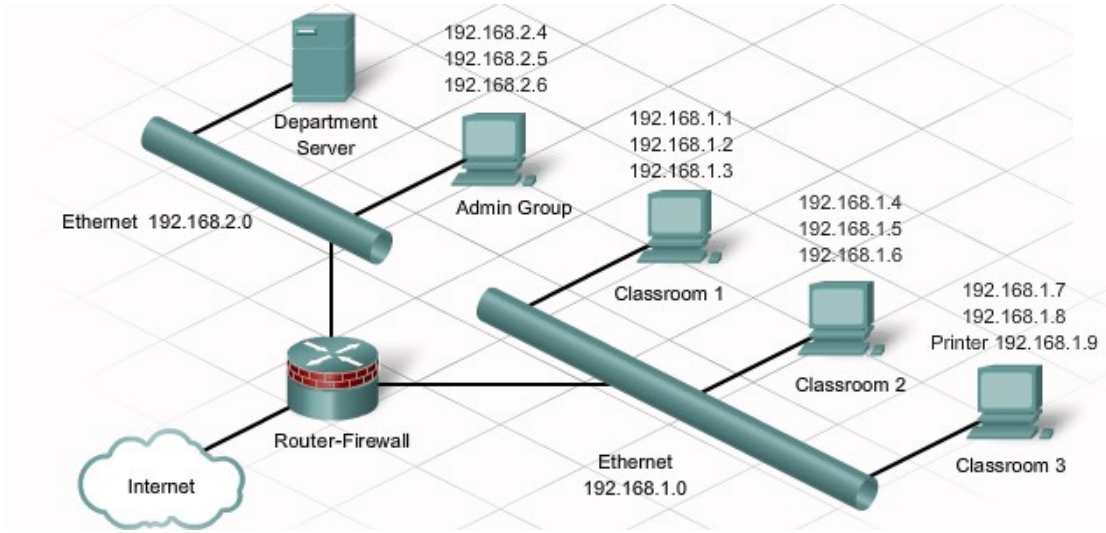
- Use the OSI model as a framework for troubleshooting network problems.
- Identify and correct problems with hardware and operation at Layer 1 and Layer 2.
- Troubleshoot IP addressing problems, including subnet mask, host range errors, DHCP and NAT issues.
- Identify and correct problems with RIPv2 configuration and implementation.
- Explain possible causes of problems occurring with user applications and how to recognize symptoms of DNS failures.
- Create a plan to prepare to take the ICND1 examination in order to obtain a CCENT certification.

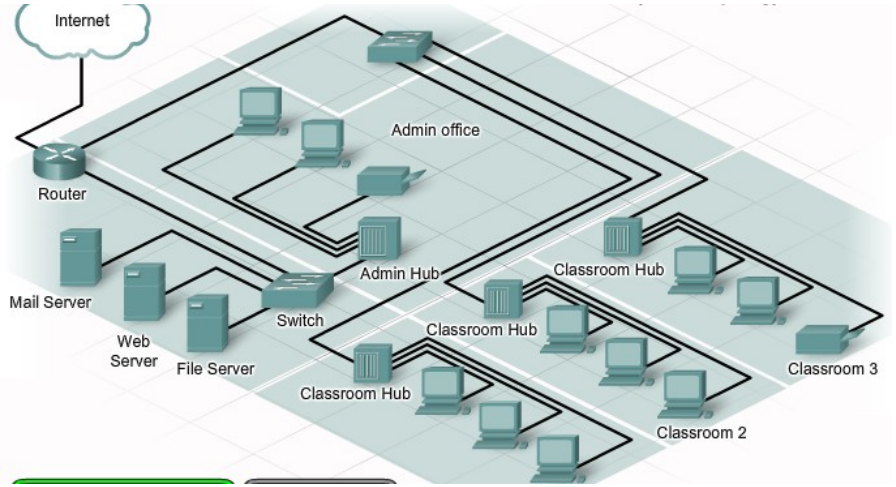
Troubleshooting approaches

- **Top-down** - Starts with the Application Layer and works down.
  - It looks at the problem from the point of view of the user and the application.
  - Is it just one application that is not functioning, or do all applications fail?
  - Do other workstations have similar issues?
- **Bottom-up** - Starts with the Physical Layer and works up.
  - The Physical Layer is concerned with hardware and wire connections.
  - Are cables securely connected?
  - If the equipment has indicator lights, are those lights on or off?
- **Divide-and-Conquer**
  - Typically troubleshooting begins at one of the middle layers and works up or down from there.
  - For example, the troubleshooter may begin at the Network Layer by verifying IP configuration information.

Network Topologies

It is very difficult to troubleshoot any type of network connectivity issue without a network diagram that depicts the IP addresses, IP routes, and devices, such as firewalls and switches. Logical and physical topologies are extremely useful in troubleshooting.

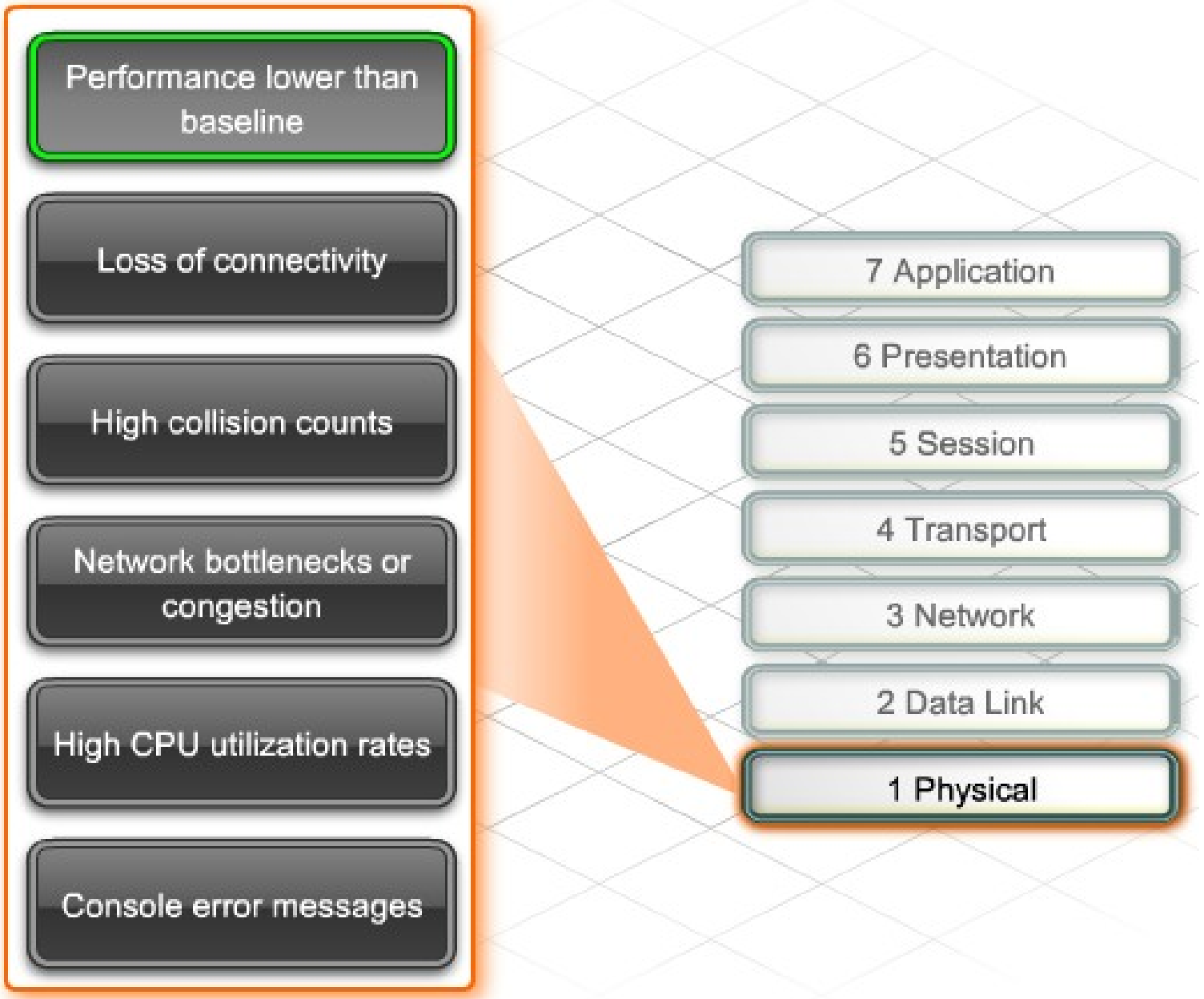




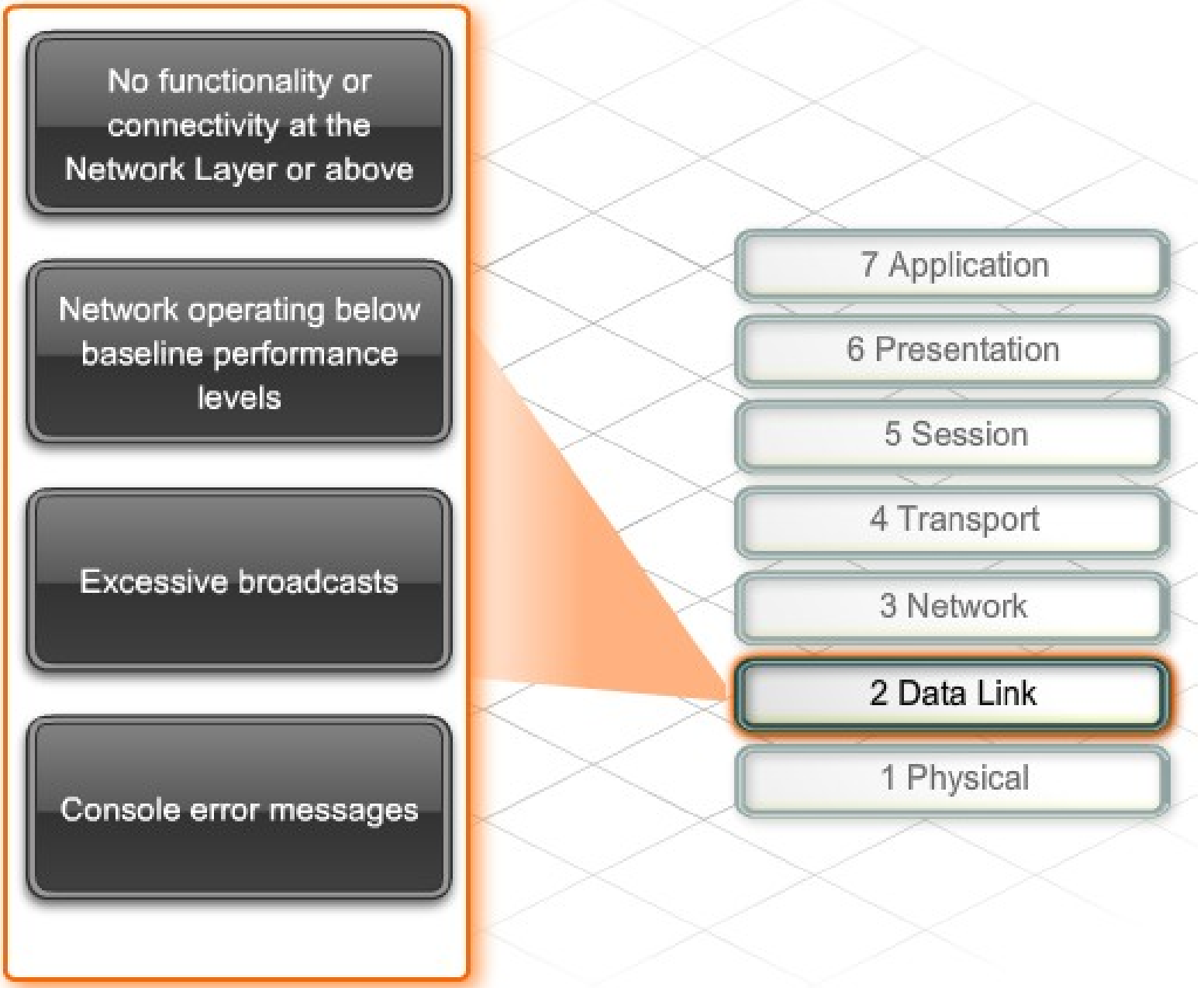
Troubleshooting Tools

- Network Documentation and Baseline Tools
  - can be used to draw network diagrams, keep network software and hardware documentation up to date, and help to cost-effectively measure baseline network bandwidth use. These software tools often provide monitoring and reporting functions for establishing the network baseline
- Network Management System Tools
  - They graphically display a physical view of the network devices. If a failure occurs, the tool can locate the source of the failure and determine whether it was caused by malware, malicious activity, or a failed device
- Knowledge Bases
- Protocol (or Packet) Analyzers
  - decodes the various protocol layers in a recorded frame and presents this information in a relatively easy-to-use format.
  - Protocol analyzers can capture network traffic for analysis. The captured output can be filtered to view specific traffic or types of traffic based on certain criteria

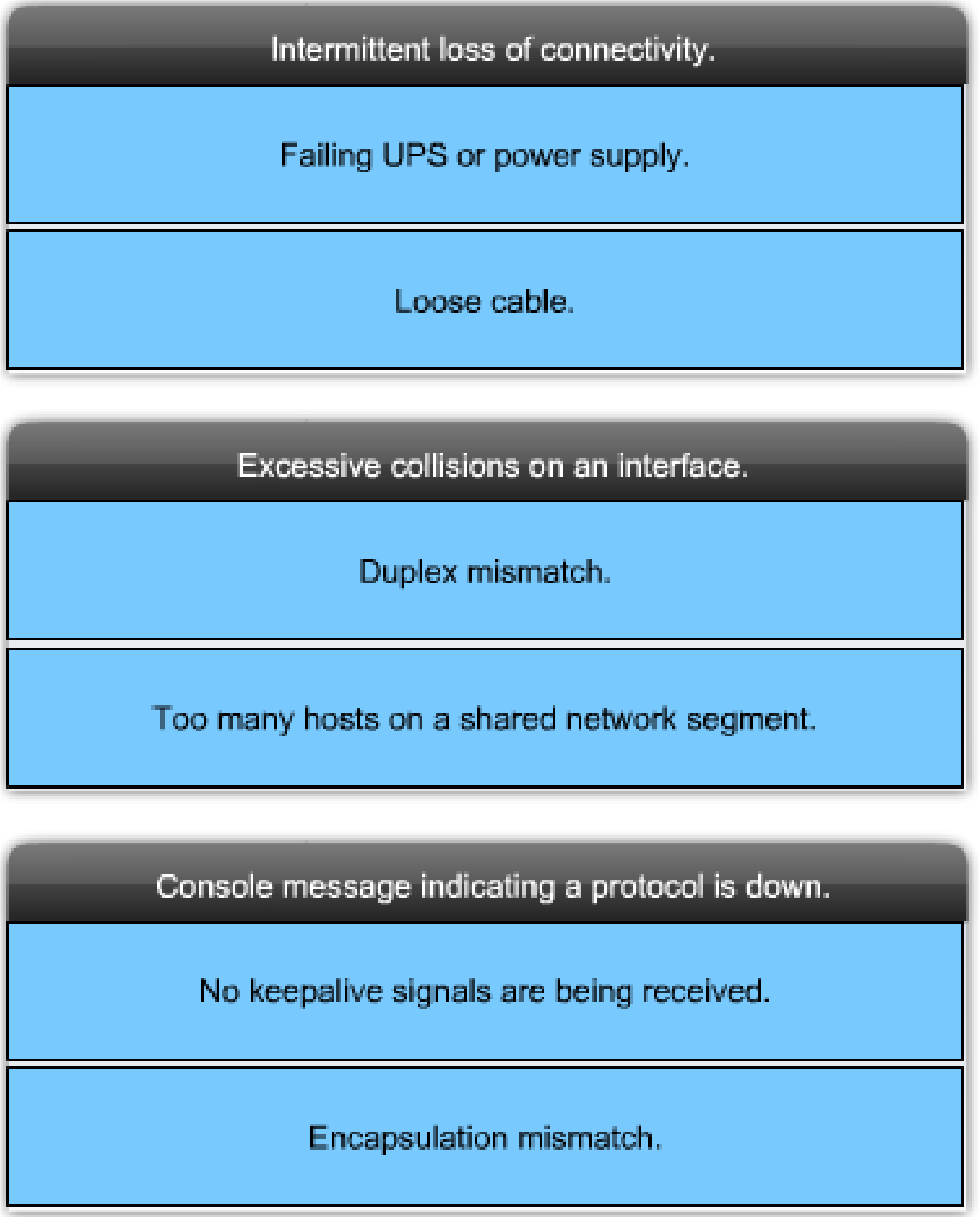
Layer 1 Symptomes



Layer 2 Symptomes



Layer 1 & 2 Symptomes



Troubleshooting Network Devices

When booting any Cisco networking device, it is helpful to observe the **console messages** that appear during the boot sequence.

After the Cisco IOS software is loaded, the technician can use commands to verify that the hardware and software are fully operational.

- The ***show version*** command displays the version of the operating system and whether all interface hardware is recognized.
- The ***show flash*** command displays the contents of the Flash memory, including the Cisco IOS image file. It also displays the amount of Flash memory currently being used and the amount of memory available.
- The ***show ip interfaces brief*** command shows the operational status of the device interfaces and IP addresses assigned.
- The ***show running-configuration*** and ***show startup-configuration*** commands verify whether all the configuration commands were recognized during the reload.

Troubleshooting Hardware

1841 LED Indicators on successful boot		
LED	Color	Status
SYS PWR	Green	Router has successfully booted up and the software is functional. Slow, steady blinking when system is booting or in the ROM monitor.
SYS ACT	Green	Blinking when packets are transmitted or received on any WAN or LAN interface, or when monitoring system activity.
CF	Blinking Green	Flash memory is busy. Do not remove the CompactFlash memory card when this light is on.

Startup problems

- If there is **not enough memory** to decompress the image, the device scrolls error messages rapidly or constantly reboots.
  - The device may be able to boot into **ROMmon mode** by issuing a **Ctrl-Break** command during startup
- If a valid **startup configuration file cannot be found**, some Cisco devices execute an **autoinstall** utility.
  - This utility broadcasts a **TFTP request** for a configuration file.
  - Other devices immediately enter an initial configuration dialog, known as the **setup utility** or **setup mode**

Interfaces Status

The output for the ***show ip interface brief*** command includes a summary of the device interfaces, including the IP address and interface **status/protocol:**

- **Up/up status** - indicates normal operation and that both the media and the Layer 2 protocol are functional.
- **Down/down status** - indicates that a connectivity or media problem exists.
- **Up/down status** - indicates that the media is connected properly, but that the Layer 2 protocol is not functioning or is misconfigured

Common **Layer 2 issues** that can cause an **up/down output** include:

- **Encapsulation** is improperly configured.
- No **keepalives** are received on the interface.

Media errors

Occasionally, **media errors are not severe enough** to cause the circuit to fail, but do cause network performance issues. The *show interfaces* command provides additional troubleshooting information to help identify these media errors.

- **Excessive Noise** - On Ethernet and serial interfaces, the presence of **many CRC errors** but not many collisions is an indication of excessive noise. CRC errors usually indicate a media or cable error. Common causes include electrical interference, loose or damaged connections, or using the incorrect cabling type.
- **Excessive collisions** - Collisions usually occur only on **half-duplex or shared-media** Ethernet connections. Damaged cables can cause excessive collisions.
- **Excessive runt frames** - Malfunctioning NICs are the usual cause of runt frames, but they can be caused by the same issues as excessive collisions.
- **Late collisions** - A properly designed and configured network should never have late collisions. Excessive cable lengths are the most common cause. Duplex mismatches can also be responsible.

(A **runt frame** is an Ethernet frame that is less than the IEEE 802.3 minimum length of 64 octets,

a **late collision** is one that happens further into the packet than is allowed for by the protocol standard)

Troubleshooting WAN

- Typically, WAN connectivity relies on equipment and media that is **owned and managed by a telecommunications service provider** (TSP). Because of this, it is important for technicians to know how to troubleshoot the **customer premises equipment** and to communicate the results to the TSP.
- To successfully troubleshoot serial WAN connectivity problems, it is important to **know the type of modem or CSU/DSU** that is installed and how to place the device in a loopback state for testing.

A CSU/DSU (Channel Service Unit/Data Service Unit) is a digital-interface device used to connect a Data Terminal Equipment device or DTE, such as a router, to a digital circuit, such as a T1 line

Troubleshooting WAN (1/2)

The interface status line of the show interfaces serial command can display **six possible problem states**:

- **Serial x is down, line protocol is down (DTE mode)** - When the router serial interface cannot detect **any signal** on the line, it reports both the line and the Layer 2 protocol down.
- **Serial x is up, line protocol is down (DTE mode)** - If the serial interface does not receive **keepalives** or if there is an **encapsulation** error, the Layer 2 protocol is reported down.
- **Serial x is up, line protocol is down (DCE mode)** - In cases where the router is providing the clock signal and a DCE cable is attached, but **no clock rate is configured**, the Layer 2 protocol is reported down.
- **Serial x is up, line protocol is up (looped)** - It is common practice to place a circuit in a loopback condition to **test connectivity**. If the serial interface receives its own signals back on the circuit, it reports the line as looped.

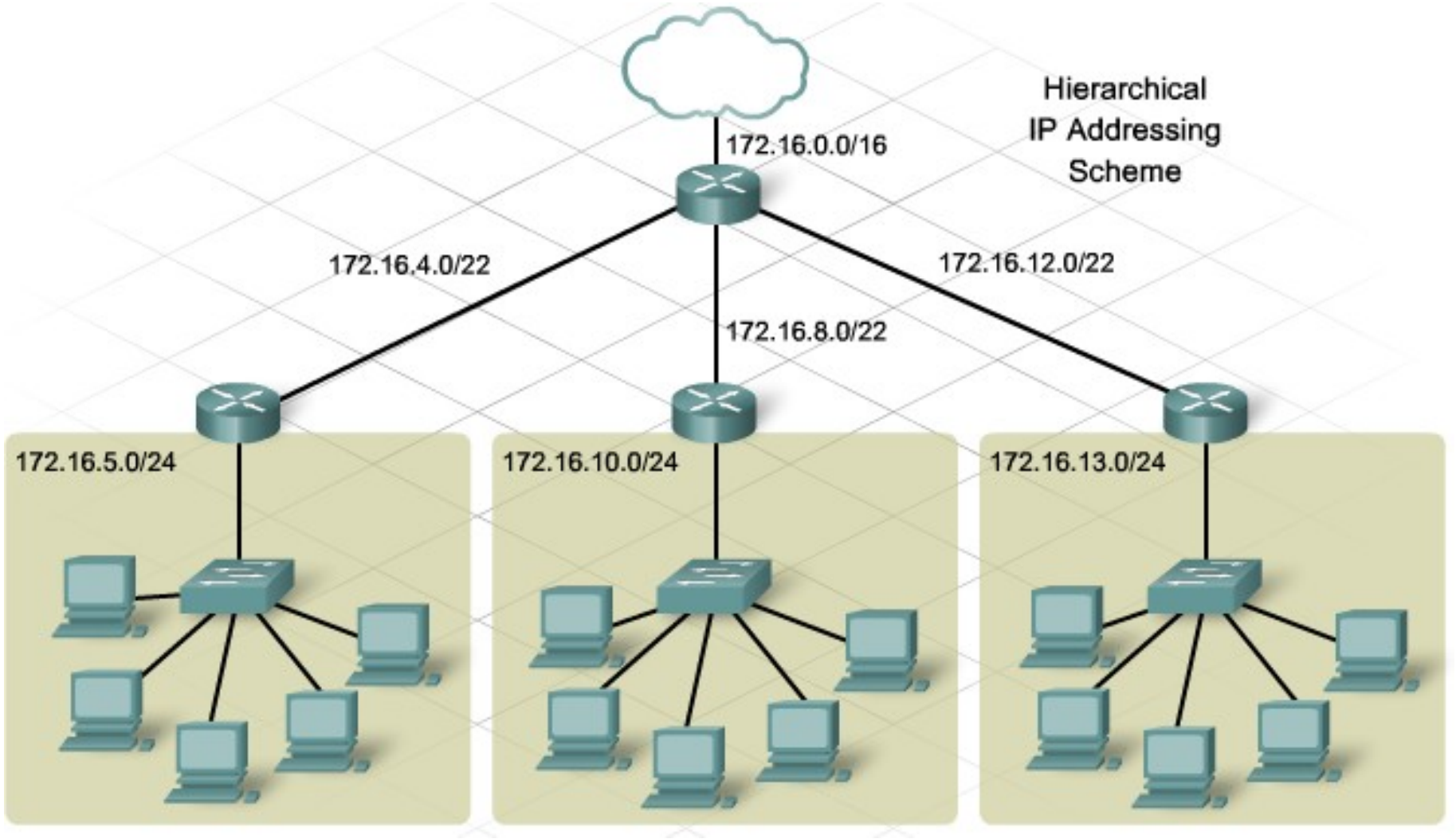
Troubleshooting WAN (2/2)

- **Serial x is administratively down, line protocol is down** - An administratively down interface is one that is configured with the *shutdown* **command**.
  - Usually all that is needed to fix this condition is to enter the ***no shutdown*** command on the interface.
  - If the interface does not come up using the no shutdown command, check the **console messages** for a duplicate IP address message.
  - If a **duplicate IP** address exists, correct the problem and issue the *no shutdown* command again.
- **Serial x is up, line protocol is up** - The interface is operating as expected.

Subnetting Review

	192.168.1.0 (/24)	Address:	11000000.10101000.00000001.00000000
	255.255.255.0	Mask:	11111111.11111111.11111111.00000000
0	192.168.1.0 (/27)	Address:	11000000.10101000.00000001.00000000
	255.255.255.224	Mask:	11111111.11111111.11111111.11100000
1	192.168.1.32 (/27)	Address:	11000000.10101000.00000001.00100000
	255.255.255.224	Mask:	11111111.11111111.11111111.11100000
2	192.168.1.64 (/27)	Address:	11000000.10101000.00000001.01000000
	255.255.255.224	Mask:	11111111.11111111.11111111.11100000
3	192.168.1.96 (/27)	Address:	11000000.10101000.00000001.01100000
	255.255.255.224	Mask:	11111111.11111111.11111111.11100000
4	192.168.1.128 (/27)	Address:	11000000.10101000.00000001.10000000
	255.255.255.224	Mask:	11111111.11111111.11111111.11100000
5	192.168.1.160 (/27)	Address:	11000000.10101000.00000001.10100000
	255.255.255.224	Mask:	11111111.11111111.11111111.11100000
6	192.168.1.192 (/27)	Address:	11000000.10101000.00000001.11000000
	255.255.255.224	Mask:	11111111.11111111.11111111.11100000
7	192.168.1.224 (/27)	Address:	11000000.10101000.00000001.11100000
	255.255.255.224	Mask:	11111111.11111111.11111111.11100000

Hierarchical IP addressing scheme



Hierarchical IP addressing scheme

- If IP addressing is assigned in a r**andom manner**, it is difficult to determine where a source or destination address is located
- Hierarchical IP addressing schemes offer many advantages, including **smaller routing tables** that require less processing power
- However, a **poorly planned hierarchical network**, or a badly documented plan, can create problems, such as overlapping subnets or incorrectly configured subnet masks on devices
- An **overlapping subnet** occurs when the address range of two separate subnets include some of the same host or broadcast addresses.
- Overlapping subnets **do not always cause** a complete network **outage**

Dhcp Issues

- Subnet having **too many hosts** is when some hosts are unable to receive an IP address from the DHCP server.
- Use the ***show ip dhcp binding*** command to check whether the DHCP server has available addresses
- Use the ***show ip dhcp conflict*** command to display all address conflicts recorded by the DHCP server.
- If an **address conflict is detected**, the address is **removed** from the pool and not assigned until an administrator resolves the conflict.

DHCP Broadcast Forward

- Because routers normally do not forward broadcasts, either the DHCP server must be on **the same local network** as the hosts or the router must be configured to relay the broadcast messages.
- A router can be configured to **forward all broadcast packets,** including DHCP requests, to a specific server using the ***ip helper-address*** command. This command allows a router to change the destination broadcast addresses within a packet to a specified unicast address:
  - ***Router(config-if)# ip helper-address x.x.x.x***
- Once this command is configured, all **broadcast packets will be forwarded** to the server IP address specified in the command, including DHCP requests.

Troubleshooting NAT

- It is critical that the correct interfaces are designated as the **inside** or **outside** interface for NAT.
- In most NAT implementations, the inside interface connects to the local network, which uses private IP address space.
- The outside interface connects to the public network, usually the ISP.
- **Verify** this configuration using the ***show running-config interface*** command.
- Use **traceroute** to determine the path the translated packets are taking and verify that the route is correct

Troubleshooting Layer 3 routing

- The primary tool to use when troubleshooting Layer 3 routing problems is the ***show ip route*** command. This command displays all the routes the router uses to forward traffic.
- The **routing table consists of route entries** from the following sources:
  - Directly connected networks
  - Static routes
  - Dynamic routing protocols
- Any time a **routing problem is suspected**, use the ***show ip route*** command to ensure that all the expected routes are installed in the routing table.

Dynamic routing issues


```
R1#show ip protocols
Routing Protocol is "rip"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Sending updates every 30 seconds, next due in 26 seconds
  Invalid after 180 seconds, hold down 180, flushed after 240
  Redistributing: rip
  Default version control: send version 2, receive version 2
    Interface              Send  Recv  Triggered RIP  Key-chain
    Serial0/0/0            2     2
  Automatic network summarization is in effect
```

Layer 4 Issues

- A common indication of Layer 4 problems is users reporting that **some web services**, especially video or audio, are not reachable.
- Verify that the **ports being permitted and denied by the firewall** are the correct ones for the applications.
- For a better understanding of which ports correspond to specific applications, review the information on TCP, UDP, and ports

Troubleshooting Upper Layers

- It can be **difficult to isolate problems** to the upper layers, especially if the client configuration does not reveal any obvious problems.
- To determine that a network problem is with an upper layer function, start by eliminating basic connectivity as the source of the problem.
- Using the "divide and conquer" method of troubleshooting, begin with verifying Layer 3 connectivity.
  - Step 1. Ping the host default gateway.
  - Step 2. Verify end-to-end connectivity.
  - Step 3. Verify the routing configuration.
  - Step 4. Ensure that NAT is working correctly.
  - Step 5. Check for firewall filter rules.

End of lesson