Scalable Network Design & NOC Webinar

# Network Troubleshooting

Ashaba Nebert
nashaba@renu.ac.ug

# Network Troubleshooting

4th October 2023



## Outline

- Network Documentation
- Troubleshooting Process
- Troubleshooting Tools
- Symptoms and Causes of Network Problems
- Troubleshooting IP Connectivity
- Q & A

# Network Documentation: Overview

Accurate and complete network documentation is required to effectively monitor and troubleshoot networks.

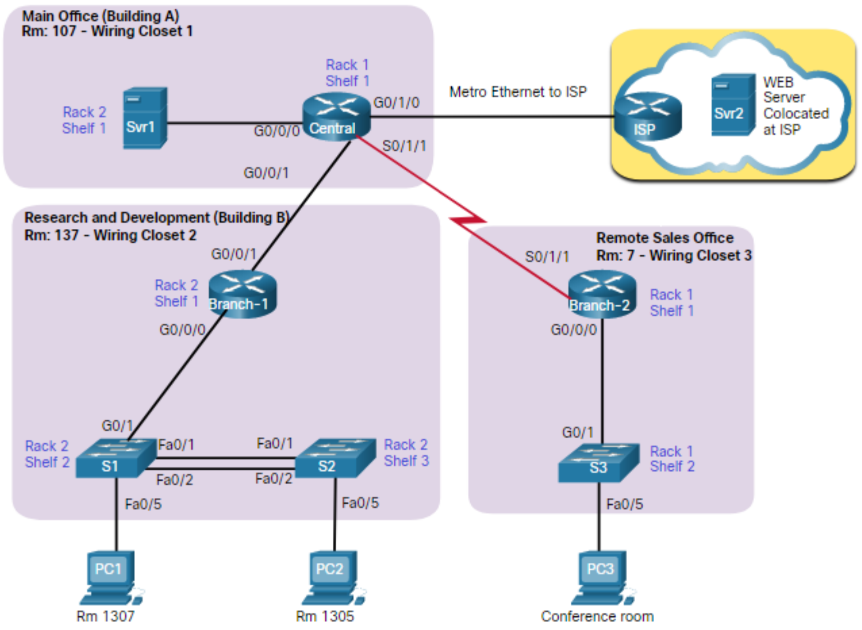
Common network documentation:

- Physical and logical network topology diagrams
- Network device documentation that records all pertinent device information
- Network performance baseline documentation

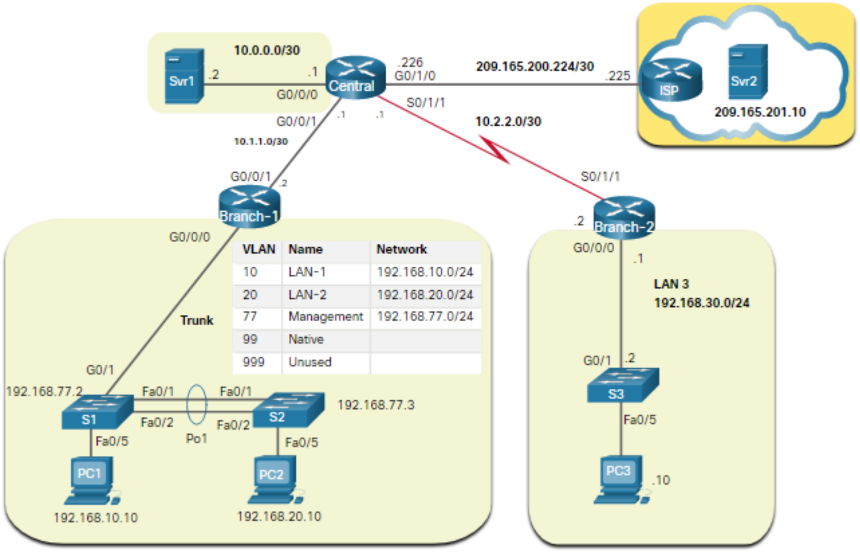
All network documentation should be kept in a single location and backup documentation should be maintained and kept in a separate location.

# Network Documentation: Network Topology Diagrams

## Physical Topology




## Logical Topology




| VLAN | Name | Network |
|---|---|---|
| 10 | LAN-1 | 192.168.10.0/24 |
| 20 | LAN-2 | 192.168.20.0/24 |
| 77 | Management | 192.168.77.0/24 |
| 99 | Native | |
| 999 | Unused | |

# Network Documentation: Device Documentation

Network device documentation should contain;

- accurate, up-to-date network hardware and software records.
- 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 |

# Network Documentation: Network Baseline

A network baseline is used to establish normal network performance to determine the “personality” of a network under normal conditions.

Establishing a network performance baseline requires collecting performance data from the ports and devices that are essential to network operation.

The baseline data is as follows:

- Provides insight into whether the current network design can meet business requirements.
- Can reveal areas of congestion or areas in the network that are underutilized

# Network Documentation: Network Baseline

## Step 1 - Determine What Types of Data to Collect

When conducting the initial baseline, select a few variables representing 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.

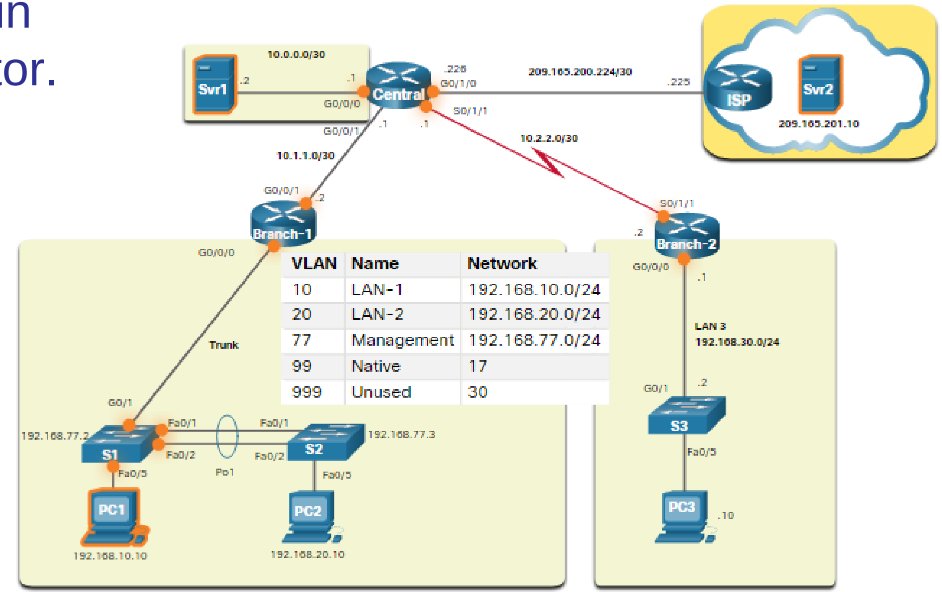
# Network Documentation: Network Baseline

## 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



# Network Documentation: Network Baseline

## 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.

# Network Documentation: Data Measurement

## Common commands used for data collection

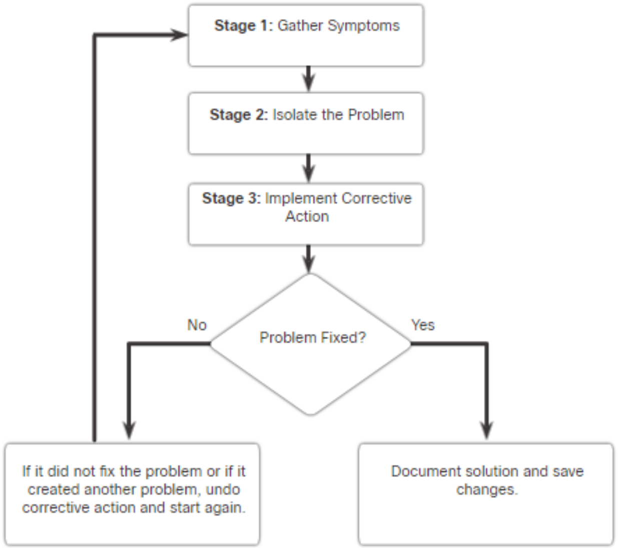
| Command | Description |
|---|---|
| `show version` | • Displays uptime, version information for device software and hardware |
| `show ip interface [brief]`<br>`show ipv6 interface [brief]` | • Displays all the configuration options that are set on an interface. |
| `show interfaces` | • Displays detailed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

# Troubleshooting Process

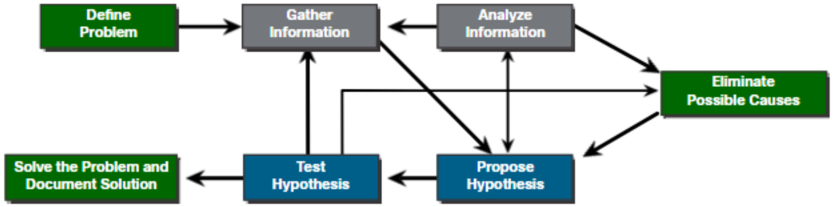
## General Troubleshooting Procedures

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.



# Seven Step Troubleshooting Process




| Steps | Description |
|---|---|
| **Define the Problem** | • Verify that there is a problem and then properly define what the problem is. |
| **Gather Information** | • Targets (i.e., hosts, devices) are identified, accessed, and information gathered. |
| **Analyze Information** | • Identify possible causes using network documentation, network baselines, knowledge bases, and peers. |
| **Eliminate Possible Causes** | • Progressively eliminate possible causes to eventually identify the most probable cause. |
| **Propose Hypothesis** | • When the most probable cause has been identified, a solution must be formulated. |
| **Test Hypothesis** | • Assess the urgency of the problem, create a rollback plan, implement the solution, and verify outcome. |
| **Solve the Problem** | • When solved, inform all involved and document the cause and solution to help solve future problems. |

# Troubleshooting Process

## Question Users

| Guidelines | Example Open Ended End-User Questions |
|---|---|
| Ask pertinent questions. | • What does not work?<br>• What exactly is the problem?<br>• What are you trying to accomplish? |
| Determine the scope of the problem. | • Who does this issue affect? Is it just you or others?<br>• What device is this happening on? |
| Determine when the problem occurred / occurs. | • When exactly does the problem occur?<br>• When was the problem first noticed?<br>• Were there any error message(s) displayed? |
| Determine if the problem is constant or intermittent. | • Can you reproduce the problem?<br>• Can you send me a screenshot or video of the problem? |
| Determine if anything has changed. | • What has changed since the last time it did work? |
| Use questions to eliminate or discover possible problems. | • What works?<br>• What does not work? |

# Troubleshooting Process

## Gather Information

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

| Layer and PDU | Function |
|---|---|
| **7. Application** {Data} | • High-level protocols such as for resource sharing or remote file access, e.g. HTTP |
| **6. Presentation** {Data} | • Translation of data between a networking service and an application; including character encoding, data compression and encryption/decryption |
| **5. Session** {Data} | • Managing communication sessions, i.e., continuous exchange of information in the form of multiple back-and-forth transmissions between two nodes. |
| **4. Transport** *{Segment\|Datagram}* | • Transmission of data segments between points on a network, including segmentation, acknowledgement and multiplexing. |
| **3. Network** *{Packet}* | • Structuring and managing a multi-node network, including addressing, routing and traffic control |
| **2. Data link** *{Frame}* | • Transmission of data frames between two nodes connected by a physical layer |
| **1. Physical** *{Bit\|Symbol}* | • Transmission and reception of raw bit streams over a physical medium |

# Troubleshooting Process

## Structured Troubleshooting Methods

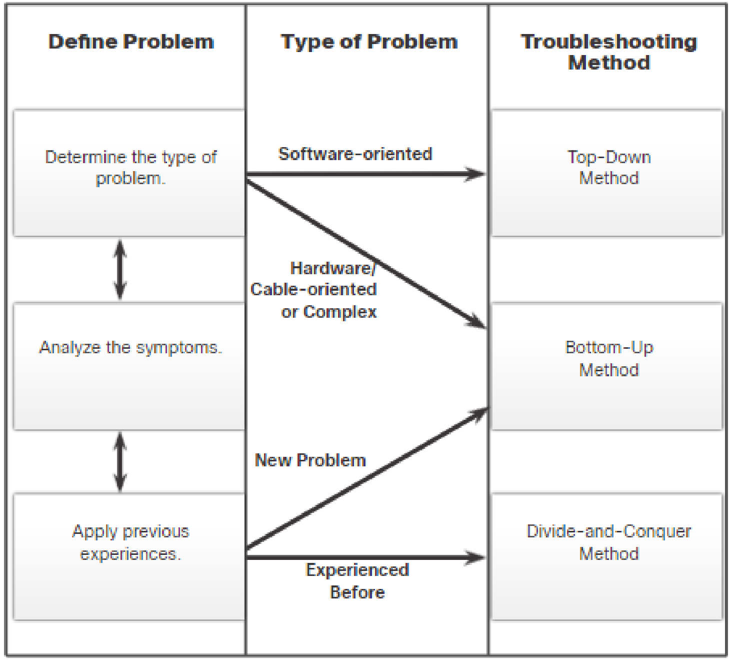
| Troubleshooting Approach | Description |
|---|---|
| **Bottom-Up** | • Good approach to use when the problem is suspected to be a physical one. |
| **Top-Down** | • Use this approach for simpler problems, or when you think the problem is with a piece of software. |
| **Divide-and-Conquer** | • Start at a middle layer (i.e, Layer 3) and tests in both directions from that layer. |
| **Follow-the-Path** | • Used to discover the actual traffic path from source to destination to reduce the scope of troubleshooting. |
| **Substitution** | • You physically swap a suspected problematic device with a known, working one. |
| **Comparison** | • Attempts to resolve the problem by comparing a nonoperational element with the working one. |
| **Educated guess** | • Success of this method varies based on your troubleshooting experience and ability. |

# Troubleshooting Process

## Guidelines for Selecting a Troubleshooting Method

To quickly resolve network problems, take the time to select the most effective network troubleshooting method.

- The figure illustrates which method could be used when a certain type of problem is discovered.
- Troubleshooting is a skill that is developed by doing it.
- Every network problem you identify and solve gets added to your skill set.

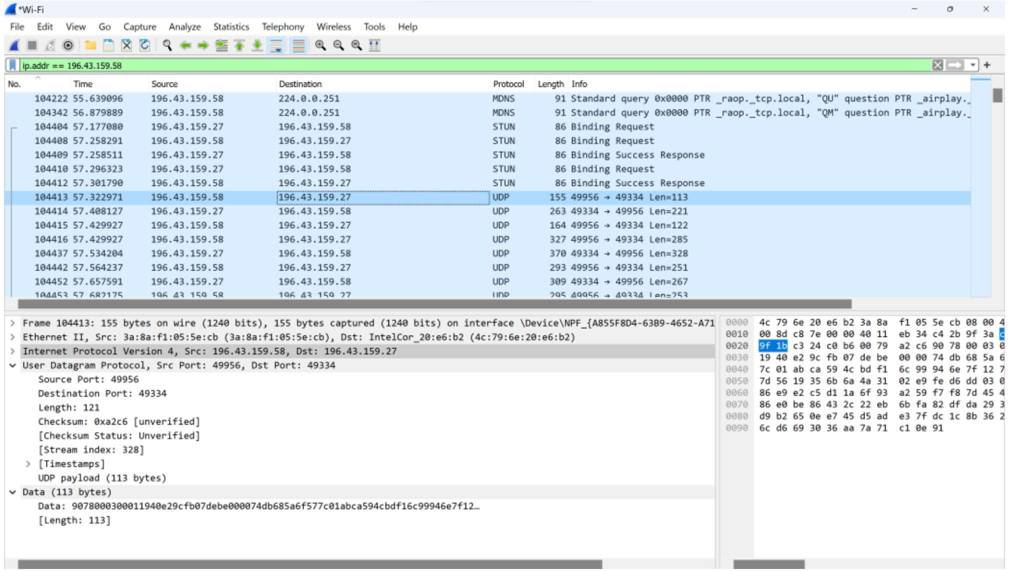


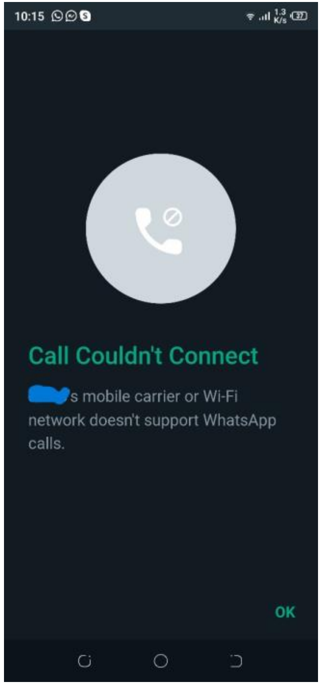
# Troubleshooting Tools: Software

| Software Tool | Description |
|---|---|
| **Network Management System Tools** | • Network software include device-level monitoring, configuration, and fault-management tools.<br>• Tools can be used to investigate and correct network problems. |
| **Knowledge Bases** | • Online network device vendor knowledge bases have become indispensable sources of information.<br>• 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.<br>• 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

- These investigate packet content while flowing through the network. Various protocol layers are decoded in a recorded frame and this information is presented in a relatively easy-to-use format.
- Protocol analyzers, such as Wireshark, can help troubleshoot network performance problems.




# Troubleshooting Tools: Hardware

| 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. |

# Troubleshooting Tools

## 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)#
```

# Symptoms and Causes of Network Problems

## Physical Layer Troubleshooting

| Symptom | Description |
|---|---|
| **Performance lower than baseline** | • Requires previous baselines for comparison.<br>• The most common reasons include overloaded or underpowered servers, unsuitable switch or router configurations, traffic congestion on a low-capacity link, and chronic frame loss. |
| **Loss of connectivity** | • Loss of connectivity could be due to a failed or disconnected cable.<br>• Can be verified using a simple **ping** test.<br>• Intermittent connectivity loss can indicate a loose or oxidized connection. |
| **Network bottlenecks or congestion** | • If a route fails, routing protocols could redirect traffic to sub-optimal routes.<br>• This can result in congestion or bottlenecks in parts of the network. |
| **High CPU utilization rates** | • High CPU utilization rates indicates that a device is operating at or exceeding its design limits.<br>• If not addressed quickly, CPU overloading can cause a device to shut down or fail. |
| **Console error messages** | • Error messages reported on the device console could indicate a physical layer problem.<br>• Console messages should be logged to a central syslog server. |

# Symptoms and Causes of Network Problems

## Physical Layer Troubleshooting

| Problem Cause | Description |
|---|---|
| **Power-related** | Check the operation of the fans and ensure that the chassis intake and exhaust vents are clear. |
| **Hardware faults** | Faulty or corrupt NIC driver files, bad cabling, or grounding problems can cause network transmission errors such as late collisions, short frames, and jabber. |
| **Cabling faults** | Look for damaged cables, improper cable, and poorly crimped connectors. Suspect cables should be tested or exchanged with a known functioning cable. |
| **Attenuation** | Attenuation can be caused if a cable length exceeds the design limit for the media, or when there is a poor connection resulting from a loose cable, or dirty or oxidized contacts. |
| **Noise** | Local electromagnetic interference (EMI) can be generated by many sources, such as crosstalk, nearby electric cables, large electric motors, FM radio stations, police radio, and more. |
| **Interface configuration errors** | Causes can include incorrect clock rate, incorrect clock source, and interface not being turned on. This causes a loss of connectivity with attached network segments. |
| **Exceeding design limits** | A component could operate sub-optimally if it is being utilized beyond specifications. |
| **CPU overload** | Symptoms include processes with high CPU utilization percentages, input queue drops, slow performance, SNMP timeouts, no remote access, no DHCP services, Telnet, and pings are slow or fail to respond. |

# Symptoms and Causes of Network Problems

## Data Link Layer Troubleshooting

| Symptom | Description |
|---|---|
| **No functionality or connectivity at the network layer or above** | Some Layer 2 problems can stop the exchange of frames across a link, while others only cause network performance to degrade. |
| **Network is operating below baseline performance levels** | • Frames can take a suboptimal path to their destination but still arrive causing the network to experience unexpected high-bandwidth usage on links.<br>• An extended or continuous ping can help reveal if frames are being dropped. |
| **Excessive broadcasts** | • Operating systems use broadcasts and multicasts extensively.<br>• Generally, excessive broadcasts are the result of a poorly programmed or configured applications, a large Layer 2 broadcast domains, or an underlying network problems . |
| **Console messages** | • Routers send messages when it detects a problem with interpreting incoming frames (encapsulation or framing problems) or when keepalives are expected but do not arrive.<br>• The most common console message that indicates a Layer 2 problem is a line protocol down message |

# Symptoms and Causes of Network Problems

## Data Link Layer Troubleshooting

| Problem Cause | Description |
|---|---|
| **Encapsulation errors** | Occurs when bits placed in a field by the sender are not what the receiver expects to see. |
| **Address mapping errors** | Occurs when Layer 2 and Layer 3 addressing is not available. |
| **Framing errors** | Framing errors can be caused by a noisy serial line, an improperly designed cable, faulty NIC, duplex mismatch, or an incorrectly configured channel service unit (CSU) line clock. |
| **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, excessive flooding because of a high rate of STP topology changes. |

# Symptoms and Causes of Network Problems

## Network Layer Troubleshooting

| Symptom | Description |
|---|---|
| **Network failure** | • Occurs when the network is nearly or completely non-functional, affecting all users and applications on the network.<br>• These failures are usually noticed quickly by users and network administrators and are obviously critical to the productivity of a company. |
| **Suboptimal performance** | • These involve a subset of users, applications, destinations, or a type of traffic.<br>• Optimization issues can be difficult to detect and even harder to isolate and diagnose.<br>• This is because they usually involve multiple layers, or even a single host computer.<br>• Determining that the problem is a network layer problem can take time. |

# Symptoms and Causes of Network Problems

## Network Layer Troubleshooting

| Problem Cause | Description |
|---|---|
| **General network issues** | • Often a change in the topology may unknowingly have effects on other areas of the network.<br>• Determine whether anything in the network has recently changed, and if there is anyone currently working on the network infrastructure. |
| **Connectivity issues** | Check for any equipment and connectivity problems, including power problems, environmental problems, and Layer 1 problems, such as cabling problems, bad ports, and ISP problems. |
| **Routing table** | Check the routing table for anything unexpected, such as missing routes or unexpected routes. |
| **Neighbor issues** | Check to see if there are any problems with the routers forming neighbor adjacencies. |
| **Topology database** | Check the table for anything unexpected, such as missing entries or unexpected entries. |

# Symptoms and Causes of Network Problems

## Transport Layer Troubleshooting - ACLs

| Misconfigurations | Description |
|---|---|
| **Selection of traffic flow** | An ACL must be applied to the correct interface in the correct traffic direction. |
| **Order of access control entries** | The entries in an ACL should be from specific to general. |
| **Implicit deny any** | The implicit ACE can be the cause of an ACL misconfiguration. |
| **Addresses and IPv4 wildcard masks** | Complex IPv4 wildcard masks are more efficient, but are more subject to configuration errors. |
| **Selection of transport layer protocol** | It is important that only the correct transport layer protocol be specified in an ACE. |
| **Source and destination ports** | Ensuring that the correct inbound and outbound ports are specified in an ACE |
| **Use of the established keyword** | The **established** keyword applied incorrectly, can provide unexpected results. |
| **Uncommon protocols** | Misconfigured ACLs often cause problems for protocols other than TCP and UDP. |

# Symptoms and Causes of Network Problems

## Transport Layer Troubleshooting - NAT for IPv4

| Symptom | Description |
|---|---|
| **BOOTP and DHCP** | • The DHCP-Request packet has a source IPv4 address of 0.0.0.0.<br>• However, NAT requires both a valid destination and source IPv4 address, therefore, BOOTP and DHCP can have difficulty operating over a router running either static or dynamic NAT.<br>• Configuring the IPv4 helper feature can help solve this problem. |
| **DNS** | • A DNS server outside the NAT router does not have an accurate representation of the network inside the router.<br>• Configuring the IPv4 helper feature can help solve this problem. |
| **SNMP** | • An SNMP management station on one side of a NAT router may not be able to contact SNMP agents on the other side of the NAT router.<br>• Configuring the IPv4 helper feature can help solve this problem. |
| **Tunneling and encryption protocols** | Encryption and tunneling protocols often require that traffic be sourced from a specific UDP or TCP port, or use a protocol at the transport layer that cannot be processed by NAT. |

# Symptoms and Causes of Network Problems

## Application Layer Troubleshooting

| Applications | Description |
|---|---|
| **SSH/Telnet** | Enables users to establish terminal session connections with remote hosts. |
| **HTTP** | Supports the exchanging of text, graphic images, sound, video, and other multimedia files on the web. |
| **FTP** | Performs interactive file transfers between hosts. |
| **TFTP** | Performs basic interactive file transfers typically between hosts and networking devices. |
| **SMTP** | Supports basic message delivery services. |
| **POP** | Connects to mail servers and downloads email. |
| **SNMP** | Collects management information from network devices. |
| **DNS** | Maps IP addresses to the names assigned to network devices. |
| **NFS** | Network File System (NFS) enables computers to mount and use drives on remote hosts. |

# Troubleshooting IP Connectivity

The bottom-up approach to test end to end connectivity;

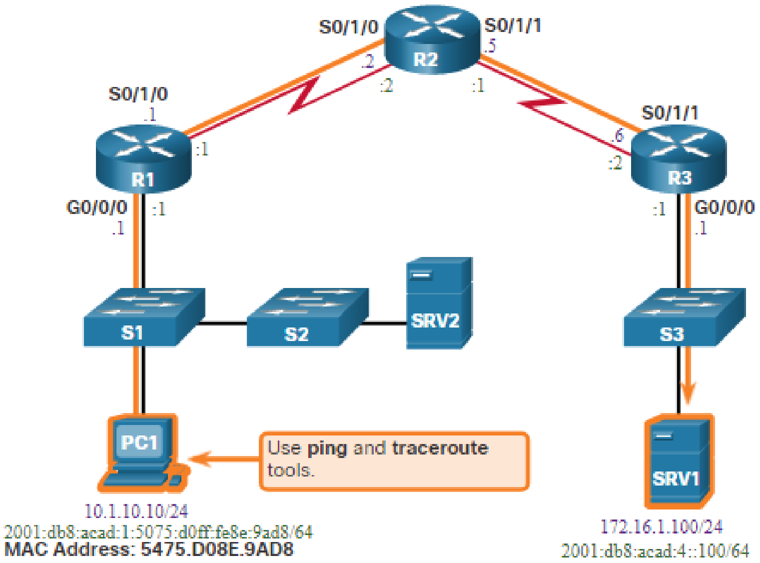
- Check physical connectivity at the point where network communication stops.
- Check for duplex mismatches.
- Check data link and network layer addressing on the local network.
- Verify that the default gateway is correct.
- Ensure that devices are determining the correct path from the source to the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

# Troubleshooting IP Connectivity

## 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 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

The IEEE 802.3ab Gigabit Ethernet standard mandates the use of auto-negotiation for speed and duplex and practically all Fast Ethernet NICs also use auto-negotiation 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)#
```

# Troubleshooting IP Connectivity

## 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#
```

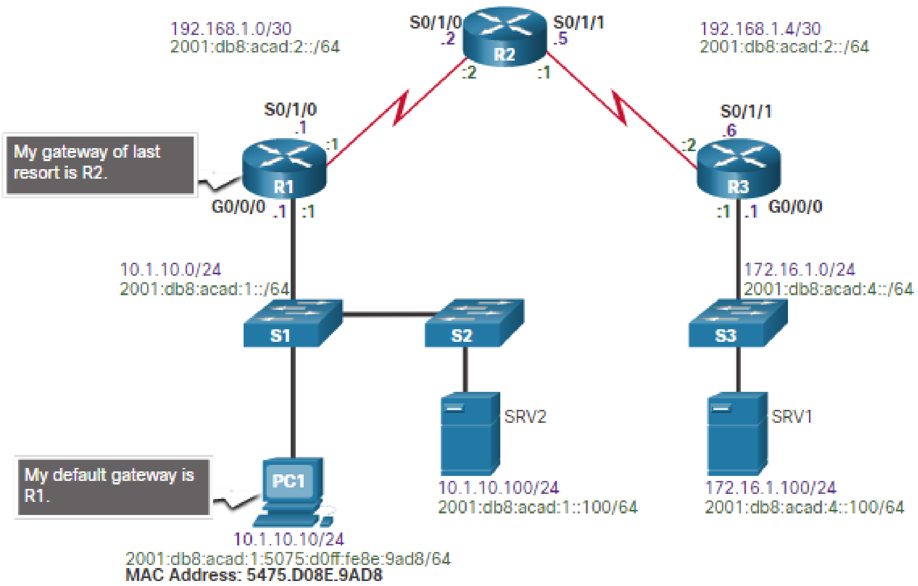
# Troubleshooting IP Connectivity

## 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)



# Troubleshooting IP Connectivity

## Troubleshoot IPv6 Default Gateway Example

An IPv6default 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.

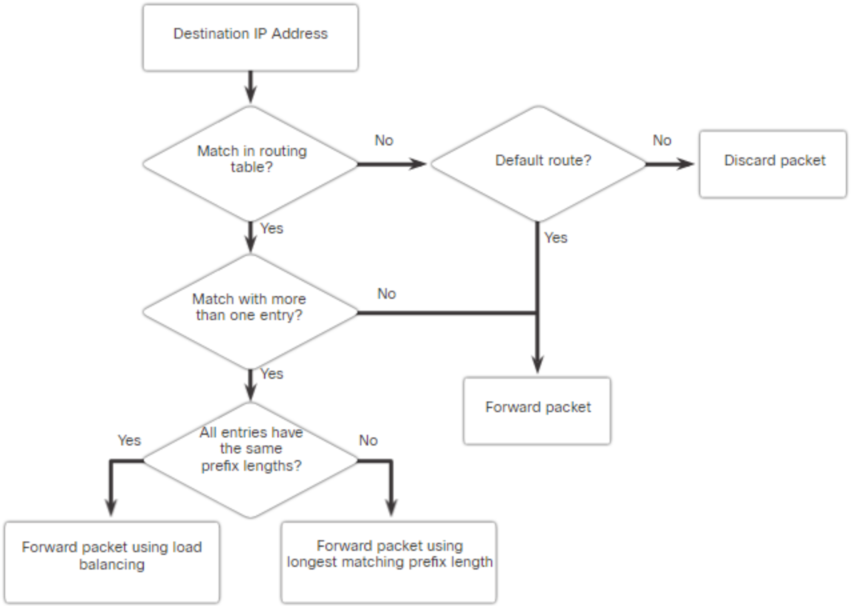
```
R1(config)# ipv6 unicast-routing
R1(config)# exit
R1# show ipv6 interface GigabitEthernet 0/0/0
GigabitEthernet0/0/0 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::1
  No Virtual link-local address(es):
  Global unicast address(es):
    2001:DB8:ACAD:1::1, subnet is 2001:DB8:ACAD:1::/64
  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 to test TCP (handshake).

```
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 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#
```

# Q & A

# THE END

Thank you for your time