# Exploring Wireless Standards and Technologies

### Chapter-10

- Wireless routers are common networking devices used in **Small Office Home Office (SOHO)** environments. A wireless router combines **three devices in one**: a **router**, a **network switch**, and a **wireless access point**. This makes it ideal for small networks such as homes and small offices.
- A typical wireless router has **five Ethernet interfaces**. One of these is the **Internet port**, also known as the **Wide Area Network (WAN) port**. This port connects the wireless router to an internet modem, allowing internet access for all connected devices. Without an active internet connection, devices connected to the wireless router can still communicate with each other locally but cannot access internet resources.
- A wireless router can create a **local network** even without an internet connection. Devices connected to the router—either wired or wireless—can still communicate with each other, share files, or use local services because they are on the same network. However, without an active connection to an internet service provider, the router cannot forward traffic to the internet, so devices are unable to access websites, online services, or cloud-based resources.
- The remaining Ethernet ports function as a **built-in network switch**. These ports allow devices to connect using wired Ethernet connections. The switch forwards data frames between wired devices and also between wired and wireless devices, enabling full communication across the entire network.
- In addition, the wireless router includes a **built-in access point** that broadcasts radio signals in the **2.4 GHz and/or 5 GHz frequency bands**. This allows wireless clients such as laptops and smartphones to connect to the network.
- The router functionality enables communication between wired and wireless networks and also supports advanced services such as a **Dynamic Host Configuration Protocol (DHCP) server**. DHCP automatically assigns network settings—including IP address, subnet mask, default gateway, and DNS server addresses—to all connected devices.

- The **Service Set Identifier (SSID)** is the **name of a wireless network**. It allows wireless devices to distinguish one wireless network from another. Without SSIDs, users would find it difficult to identify which network they should connect to.
- Home users and organizations usually **change the default SSID** provided by the device manufacturer to a more recognizable name. However, as a **security best practice**, organizations should avoid using SSIDs that clearly identify the organization or attract attackers.

- For example, many IT professionals configure SSIDs using their company name. While this makes it easy for employees to find the network, it also makes it easier for hackers to identify a potential target.
- When a wireless router or access point is powered on, it loads its configuration and begins broadcasting its presence. These devices continuously transmit **beacon frames** that include information such as:
    - ➢ SSID
    - ➢ Wireless encryption standard
    - ➢ Operating channel
    - ➢ Media Access Control (MAC) address
- Any device with a compatible wireless adapter—such as laptops, smartphones, tablets, or IoT devices—can detect these beacon frames. This allows users to view and select available wireless networks within range.
- *When a wireless router or access point is powered on, it loads its configuration and begins transmitting* ***beacon frames****. Beacon frames are broadcast regularly to advertise the wireless network's presence and include information such as the* ***SSID, channel, and security settings****.*
- ***Example:***
  *A router broadcasting the SSID Home_WiFi sends beacon frames, allowing nearby devices to detect and display the network in their available Wi-Fi list.*

- When a wireless client (also called a **station**) connects to a wireless router or access point, the process is known as an **association**.
- When a client successfully joins a wireless network, it stores the network's **SSID and password** in a **Preferred Network List (PNL)**. This list allows the device to automatically reconnect to the same wireless network in the future without requiring the user to re-enter the credentials.
- The wireless network adapter then sends out **probe requests** for each SSID stored in the PNL. These probes are used to search for known wireless networks within range.
- When a wireless network matching one of the stored SSIDs is detected, the client attempts to establish an **association** with that wireless network, completing the connection process
- When a wireless client connects to a wireless router or access point, the connection is called an **association**. The client saves the network's **SSID and password** in a **Preferred Network List (PNL)** so it can reconnect automatically in the future. The device sends **probe requests** to search for these saved networks, and when a matching network is found within range, the client attempts to associate and connect to it.

# Assuring Network Availability

## Network Device Performance Metrics

Network professionals use **performance metrics** to determine whether a networking device is operating normally or experiencing potential issues.

### Common Performance Metrics

- **Temperature**
- **CPU utilization**
- **Memory utilization**
- **Bandwidth**
- **Latency**
- **Jitter**

## Temperature

- Networking devices operate continuously and generate heat while processing network traffic.
- During peak usage, higher workload increases device temperature.
- **Sensors** (internal/external) are used to monitor temperature.
- **High temperature** may indicate:
  - Excessive utilization
  - Hardware failure
- Devices may **automatically shut down** to prevent damage.
- **Low temperature** can cause condensation on electronic components.

## CPU Utilization

- The **CPU** performs all computational and forwarding tasks.
- High traffic increases CPU usage.
- As CPU utilization approaches **100%**:

    - Device performance degrades
    - New processes may be rejected
- High CPU usage can cause:
    - Slow packet forwarding
    - Network delays
- Checking CPU utilization helps diagnose performance issues.

## Memory Utilization

- Networking devices use **RAM** to run processes and store packets temporarily.
- Incoming messages are stored in **buffers** before forwarding.
- Adequate memory improves:
    - Processing speed
    - Forwarding efficiency
- **Low available memory** may indicate:
    - Critical system failure
    - Need for immediate troubleshooting

## Network Bandwidth

**Network bandwidth** refers to the **maximum amount of data (packets)** that can be transmitted from a source device to a destination device within a given period of time.

### Bandwidth Utilization and Monitoring

- Monitoring bandwidth usage helps network professionals:
    - Evaluate overall network performance
    - Detect **congestion**
    - Identify **latency issues**
    - Discover **physical layer problems**
    - Detect possible **security threats**

## Latency

**Latency** is the **time delay between a request being sent and a response being received** over a network.

### Causes of High Latency

- Network congestion

- Faulty network devices or links
- Packet loss and retransmissions
- Physical or configuration issues

### Latency Troubleshooting Process

- Network professionals **capture network traffic** between:
  - The source (user's device)
  - The destination (server)
- **Packet analysis** is performed to:
  - Measure response times
  - Compare latency across different network segments
- This helps **isolate the affected part of the network**

## Jitter

**Jitter** is the **variation in packet delay** as packets travel across a network.

### Key Points

- In an ideal network, packets from the same sender arrive with **consistent latency**.
- Jitter occurs when packets arrive at **different time intervals**.
- Jitter increases when:
  - Network traffic is high
  - The network becomes saturated or congested

### Impact of Jitter

- Most noticeable in **real-time applications** such as:
  - **Voice over IP (VoIP)**
  - **Video conferencing**
- High jitter can cause:
  - Choppy or distorted audio
  - Freezing or delayed video
  - Poor user experience

## Jitter

**Jitter** is the **variation in delay (latency) between received packets** on a network.

**Key Points**

- In an ideal network, packets from the same source arrive with **consistent latency**.
- Jitter increases when:
  - Network traffic is high
  - The network becomes congested
- Jitter mainly affects **real-time applications** such as:
  - **VoIP (Voice over IP)**
  - **Video conferencing**

**Impact of High Jitter**

- Choppy or distorted audio
- Delayed or frozen video
- Poor user experience in real-time communication

**Exam Tip**

**Low latency with high jitter** can still cause poor VoIP and video performance.

## SNMP (Simple Network Management Protocol)

Techniques are commonly used to collect and analyze network traffic

**SNMP** is a network protocol used to **monitor, manage, and configure network devices**.

**Purpose of SNMP**

- Monitor device performance
- Collect statistics
- Retrieve device status
- Apply configuration changes remotely

**SNMP Versions**

**SNMPv1:** Does not support any security such as data encryption or authentication, hence it's not recommended for use.

**SNMPv2:** This version of SNMP is an improvement on how SNMP handles communication between the SNMP Manager and SNMP Agent, but this version does not support data encryption
or authentication. Hence, it's not recommended for use.

**SNMPv3:** This version of SNMP is an improvement on prior versions and supports data

- encryption, integrity checking, and authentication.

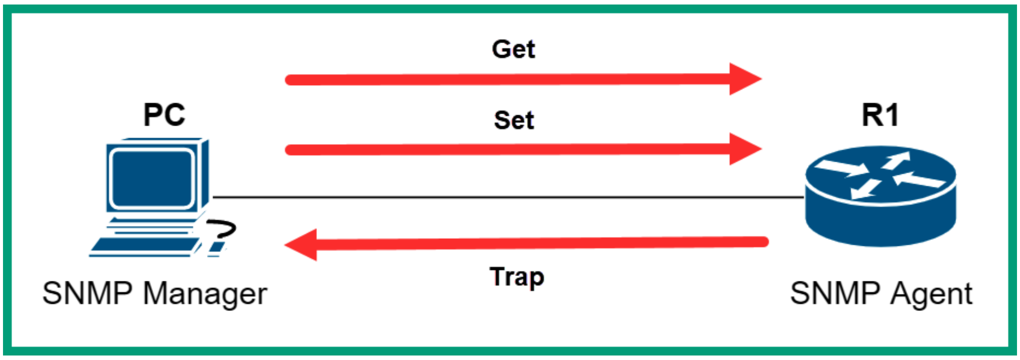
## SNMP Components (NMS)

A **Network Management System (NMS)** consists of:

□ **SNMP Manager:**
A centralized system (software) that **monitors, manages, and controls network devices**. It sends **Get and Set requests** and receives **Trap messages**.

□ **SNMP Agent:**
Software running on network devices (routers, switches, servers) that **collects device information** and responds to the manager's requests.

□ **Management Information Base (MIB):**
A **structured database** that defines and organizes the information managed by SNMP. It contains objects (variables) that the agent maintains and the manager queries.



**Explanation of the SNMP diagram:**

- **SNMP Manager (PC):**
  The management system that monitors and controls network devices.
- **SNMP Agent (R1 – Router):**
  Software running on the network device that collects and provides device information.

**Message flow shown:**

1. **Get (Manager → Agent):**
   The SNMP manager requests information from the device
   *Example:* asking for interface status or bandwidth usage.
2. **Set (Manager → Agent):**
   The SNMP manager changes a configuration value on the device
   *Example:* enabling or disabling an interface.
3. **Trap (Agent → Manager):**
   The SNMP agent sends an Event-driven notification to the manager when an important event occurs
   *Example:* interface down, high CPU usage.

# Network Device Logs

Network devices, security appliances, servers, and end devices generate **logs**, which are records of events that occur on the device. These logs include details such as **time stamps, event type, and descriptions**.

Network professionals use logs to **monitor network activity, troubleshoot problems, and identify the cause of issues** like outages or security incidents.

By analyzing logs before, during, and after an event, they can determine what happened and why.

Logs also help maintain **accountability, auditing, and security** on a network. Without logs, identifying the cause of network problems becomes very difficult.

**Logs** are records of events generated by networking devices, servers, security appliances, and end devices.

In networking, an **event** is **any action or occurrence on a device or network** that the system recognizes and records.

**Examples of events:**

- A device powering on or shutting down
- A user logging in or logging out
- A link going up or down
- A configuration change
- A security alert or failed login attempt
- A network outage or error

Each event is usually **recorded in a log with a timestamp and description**, so network administrators can monitor, troubleshoot, and audit network activity.

- ***Timestamp tells** when **the event happened***
- ***Description tells** what **happened***

## Types of Logs

### Traffic logs

- **Traffic logs** record information about the **data traffic flowing between devices** on a network. They provide a **summary of network traffic over a specific time period** and include detailed information such as source, destination, protocol, and data usage.
- Network professionals use traffic logs mainly for **monitoring, troubleshooting, and post-event analysis**.
- By reviewing past traffic patterns and comparing them with current activity, they can identify **abnormal behavior, performance issues, or security incidents**.

## Audit logs

- **Audit logs** record detailed information about **who performed an action, what action was performed, and when it occurred** on a network or system.
- They help network professionals track **user activities and resource access**, including source and destination addresses, timestamps, and user details.
- Audit logs are mainly used for **accountability, security monitoring, and compliance**, making it easier to investigate unauthorized access or policy violations.

Example

- This audit log shows **who** (admin) accessed the network device, **what** action was performed (login), **when** it happened (timestamp), and **from where** (source IP), helping administrators track and verify user activity.

## Syslog

Syslog allows networking devices (routers, switches, servers, firewalls) to **send their log messages to a centralized syslog server** over the network.

**Why Syslog is used:**

- Avoids logging in to each device separately
- Makes **monitoring and troubleshooting easier**
- Helps in **security auditing and event analysis**

**Example:**
If a router interface goes down, the router automatically sends a **syslog message** to the syslog server describing the event with time and severity details.

**Default Syslog message format (Cisco devices):**

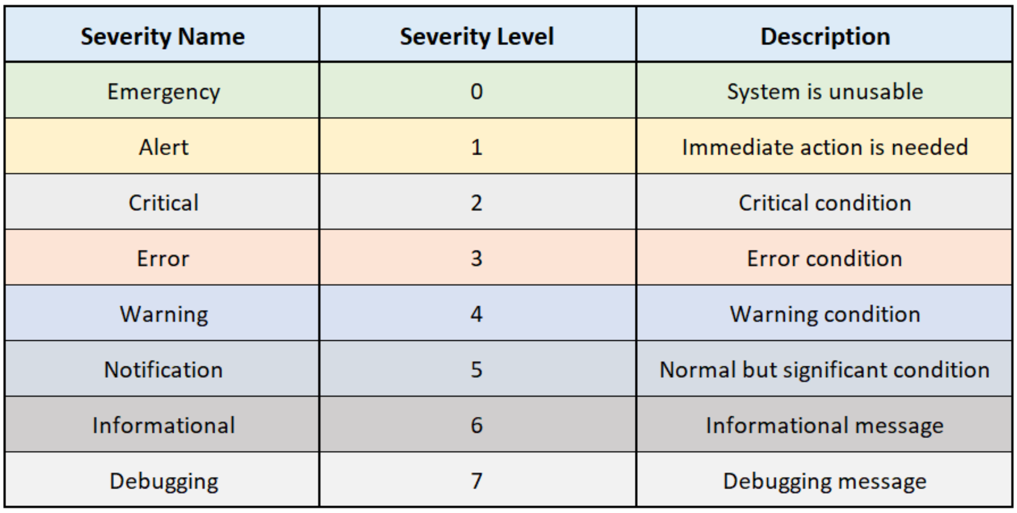
```
seq no: timestamp: %facility-severity-MNEMONIC: description
```

**Components explained briefly:**

- **Seq no:** Unique sequence number of the log message
- **Timestamp:** Date and time when the event occurred
- **Facility:** Indicates the source or type of event (Facility tells where the log message came from (system, protocol, authentication, etc.))
- **Severity:** Shows how critical the event is
- **Mnemonic:** Short, unique code identifying the event
- **Description:** Brief explanation of what happened

Syslog helps network professionals **centrally collect, analyze, and respond to network events** effectively.

The following table contains the Syslog severity levels, their names, and descriptions:



| Severity Name | Severity Level | Description |
|---|---|---|
| Emergency | 0 | System is unusable |
| Alert | 1 | Immediate action is needed |
| Critical | 2 | Critical condition |
| Error | 3 | Error condition |
| Warning | 4 | Warning condition |
| Notification | 5 | Normal but significant condition |
| Informational | 6 | Informational message |
| Debugging | 7 | Debugging message |