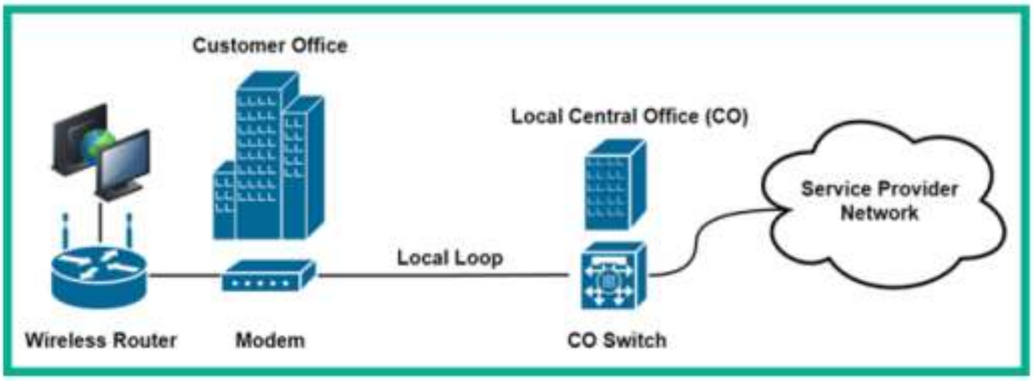
Chapter 10: Exploring Wireless Standards and Technologies

- Wireless networking has evolved over the years to enhance mobility and efficiency, enabling seamless communication for devices like laptops, smartphones, and tablets.
- It bridges wired and wireless networks using access points and routers, allowing users to connect and move freely within a network's range.

Exploring wireless networking

- When designing a wireless network for an organization, it’s important to consider:
  - The components needed
  - The number of wireless clients that need access to the wireless network,
  - The location of these clients within an organization.
- The components needed are access points, switch, modems or wireless routers.
- Wireless routers are common wireless networking devices that are commonly found within **Small Office Home Office** (**SOHO**) networks.

The following diagram shows the connection between an internet modem and a wireless router:



Wireless Router:

- The router functionality allows devices that are connected to the wired and wireless network types to intercommunicate with each other.

In a wireless router, different interfaces are:

The internet port or WAN port:

- Used to establish a wired connection from the internet modem to the wireless router for the purpose of providing internet access to devices that are connected to the wireless router.

Ethernet ports:

- Operate like a typical network switch, allow to interconnect clients with each other using a wired connection.
- The built-in switch within the wireless routers functions like a typical network switch that forwards frames between devices on the wired and wireless networks.

Access point feature:

- The wireless router has built-in access point feature to generate radio frequencies within the 2.4 GHz and/or 5 GHz band to create a wireless network, allowing wireless clients to connect to the device.
- In medium-sized to large organizations, access points are commonly implemented to provide wireless coverage to all areas within a building.

Dynamic Host Configuration Protocol (DHCP) server

- The router feature allows network professionals to create a **DHCP** server within the wireless router to provide IP addresses, subnet mask, default gateway, and **Domain Name System** (**DNS**) server addresses to all connected clients.

Beacons, probes, stations, and SSIDs

SSIDs

- The **Service Set Identifier** (**SSID**) is simply the name of the wireless network that allows wireless clients to identify one wireless network from another.
- Without **SSID**, it'll be quite challenging for users to identify their wireless network from another network.
- Many IT professionals usually configure their wireless networks with SSIDs that are easily identifiable such as using their company's name.
- However, as a good security practice, organizations should not set an SSID that can easily identify the organization's network.

Beacons

- When a wireless router or access point is powered on, the firmware and configurations are loaded in memory and the device begins to broadcast its presence within the surrounding.
- Wireless routers and access points continuously broadcast **beacons** that contain specific information about themselves such as: **the SSID, wireless encryption standard, operating channel, and even their Media Access Control (MAC) address.**
- The beacons are detected and inspected by any device that has a supported wireless network adapter such as smartphones, tablets, **Internet of Things** (**IoT**) devices, and laptops, therefore allowing a user to identify wireless networks within the surrounding.

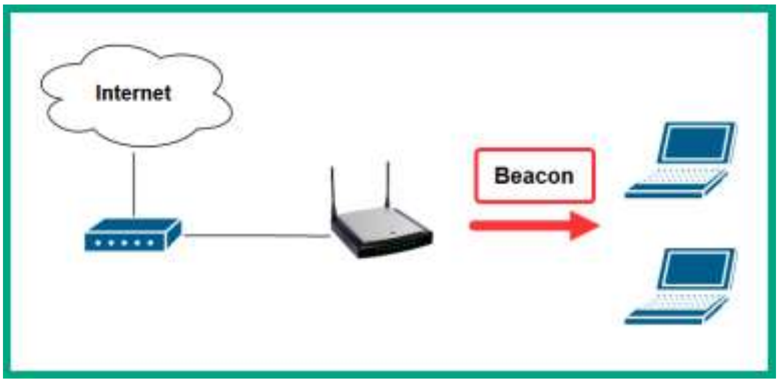


Figure 10.4 – Wireless beacons

- Wireless routers and access points provide the capability of disabling the SSID broadcast as a technique of hiding your wireless network from wireless clients. However, hacker or cybersecurity professional can discover a hidden wireless network and security configurations from beacons and probes using very specialized skills

Probes

- Probe requests are a type of WiFi management frame. They are used simply for network discovery. The probe request will contain the SSID of a known network.

Stations

- Wireless clients, such as laptops, smart TVs, and IoT devices, are examples of stations on a wireless network.
- When a wireless client (station) establishes a connection to a wireless router or access point, it's referred to as an **association**.
- When a client joins a wireless network, the client saves both the SSID and password into a **Preferred Network List** (**PNL**) that allows the user to easily re-join the same wireless network in the future.
- This enables the wireless network adapter on a client to begin sending probes for each entry within the PNL on the device.
- The **probes** allow the client to seek any of the wireless networks via their SSIDs that are stored within the PNL. Once a wireless network is found within the signal range, the client will attempt to create an association with the wireless network.
- Hacker or cybersecurity professional can capture the probes to determine the wireless networks that are stored on a client and attempt to perform an *AP-less attack* to retrieve the password/ passphrase of an organization's wireless network.
- However, many newer devices are now allowing IT professionals to prevent the client from automatically connecting to a saved wireless network that's within range.

Chapter 11: Assuring Network Availability

Network performance metrics

- Performance metrics help network professionals within the industry to determine whether their network is operating as expected or the delivery of network resources is affected.
- Network professionals use various tools and processes to collect data about the network. This data is then used for analysis and to generate reports that indicate the actual performance of the network.
- Some common performance metrics that are used to determine whether a networking device is operating as expected or whether there's a potential issue:
- **Temperature:** Network professionals commonly implement internal and/or external sensors with devices to closely monitor temperature changes. If the temperature is too hot or above normal, it can be an early warning of excessive utilization or a possible hardware issue on the device.
- **Central processing unit (CPU) utilization**: CPU utilization increases closer to 100%, the device will not be able to handle newer processes or perform additional computation tasks and networking device is not forwarding traffic as quickly as expected.
- **Memory utilization:** Whenever messages are received on a networking device, they are stored within a buffer before processing and forwarding them to their destinations. The available memory on a networking device affects the performance of how quickly messages are processed and forwarded to their destination.
- **Bandwidth:** The network bandwidth is simply the total amount of packets that can be transferred from a source device to a destination device within a given time. Observing the bandwidth utilization network professionals collect and analyze the overall performance of the actual network.
- Various techniques are commonly used to collect and analyze network traffic, such as: **Simple Network Management Protocol** (**SNMP**) and NetFlow
- **Latency:** Latency is simply the measurement of time between a request and response over a network. From the response time the network professionals collect and analyze the overall performance of the actual network.
- **Jitter:** Jitter measures the variation of delay times of incoming packets on a network. Inconsistency between a source and destination can create a bad experience for the end user who is using a VoIP phone or video-conferencing application.

Simple Network Management Protocol (SNMP)

- SNMP is a common network protocol that allows network professionals to easily monitor devices within their organization.
- The SNMP Manager allows the network professional to easily collect statistical data from devices on the network, retrieve device statuses, and push configuration changes to network devices.

- There are different versions of SNMP, as follows: **SNMPv1, SNMPv2, SNMPv3**
  - **SNMPv1 and SNMPv2**: Does not support any security such as data encryption or authentication, hence it's not recommended for use.
  - **SNMPv3**: Supports data encryption, integrity checking, and authentication.
- When working with SNMP, three main components need to work together to create a **Network Management System** (**NMS**):
  - SNMP Manager
  - SNMP Agent
  - **Management Information Based** (**MIB**)

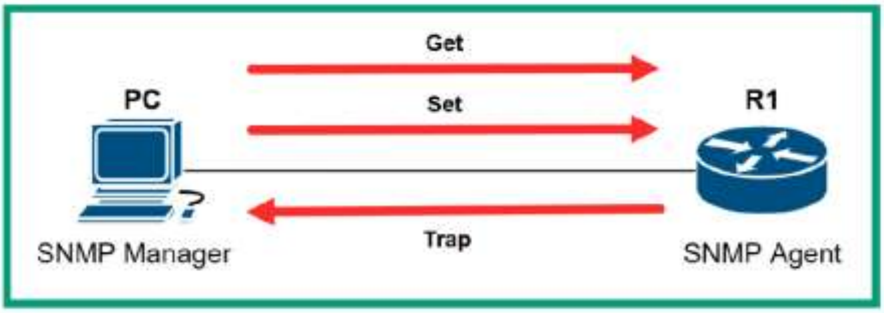


Figure 11.4 – SNMP messages

- The Manager is an application that's installed on the network professional's computer or centrally on a server. The Manager must collect information and make configurations on devices that are running the agent.
- The manager can retrieve information from agents on the network by sending an SNMP GET message, which instructs the agent to respond with the requested information. Additionally, the manager sends SNMP SET messages to an agent when configuration changes are needed.
- The Trap data units are sent from the Agent to the Manager as they contain data about changes or events that occurred on the device and only send information when a threshold has been met.

Network device logs

- Networking devices, security appliances, servers, and end devices commonly generate logs, which are records of every event that has occurred on the device.
- Network professionals depend on the logs created by a device to determine the reason for an event.
- **Example:** Imagine if an organization experienced a network outage for a few minutes during the night. The networking devices will generate log messages for each event that occurred, including the timestamps and a description of the event. Network professionals can observe the logs before, during, and after the event from various devices within the affected area of the network to determine the reason for the outage and probable causes.
- Without network device logs, it's quite challenging to determine the reasons for events that occurred on a network.

- **Traffic logs** contain information and details about the traffic that flows between devices on a network. They allow network professionals to see a summary of all the traffic for a given time.
- **Audit logs** help network professionals determine who and what resources were accessed on the network, the source and destination addresses, the timestamp of the event, and user information.
- **Syslog:** Protocol allows devices to generate logs for events that occur on a device forward their log messages over a network to a centralized logging server.