Network+ CompTIA (N10-009) — Day 3

Spanning Tree Protocol (STP) and Layer 2 Loops

Command:
```
show mac address-table dynamic
```

MAC Address Tables

- Dynamically populated by learning (snooping) the source MAC addresses of frames.
- MAC addresses are paired with the ingress (receiving) port.
- **Note:** Duplicate MAC addresses are disallowed. If the same MAC address is learned on different ports, it will *flap* (move between ports).

Frame Forwarding Types

- **Flood:** Frames are sent (flooded) out all ports except the ingress port (broadcast).
  - Broadcast destination MAC address is all F's in hexadecimal (`FF:FF:FF:FF:FF:FF`).
- **Forward:** Frames are forwarded out a single port based on the destination MAC address if known (unicast).
  - If the destination MAC is unknown, the frame is flooded out all ports.
- **Multicast:** Frames are flooded by default.
  - May be controlled with IGMP snooping (beyond Network+ scope).

Layer 2 Loops

- Occur due to redundancy in the network.
- Broadcast frames flood out all ports except the ingress port; redundant cables can loop broadcasts back into devices that already sent them, causing a loop.
- Uncontrolled Layer 2 loops cause:
  - Broadcast storms
  - MAC table instability
  - Extreme latency
  - Effectively make an entire VLAN unusable

Spanning Tree Protocol (STP)

- Enabled by default on most switches.
- Purpose: Identify and block ports to eliminate loops.
- Communicates via Bridge Protocol Data Units (BPDUs).

STP Process:

1. **Determine Root Bridge**
   - Lowest Bridge ID (BID) is elected Root Bridge.
   - BID = Priority + MAC Address.
   - Priority defaults to 32768.
   - Tie-breaker: lowest MAC address wins.
2. **Determine Root Ports**
   - Port on each switch with the lowest total path cost to Root Bridge.
   - Lower cost is better.
   - Path cost example values (won't be on the exam):
     - 100 Mbps = 19
     - 1 Gbps = 4
     - 10 Gbps = 2
   - If cost ties, compare BIDs, then port IDs.
3. **Determine Designated Ports**
   - Ports on links with the lowest cost path to Root Bridge.
   - All ports on Root Bridge are designated.
   - If one port is a Root Port, the other side must be designated.
   - Remaining ports decided by lowest cost path.
4. **Block all other ports** to prevent loops.

STP Standards

- **IEEE 802.1D** — Original STP, slow (30–50 seconds convergence).
  - When a root port link goes down, it takes 30–50 seconds to unblock ports and reconverge.
- **IEEE 802.1W** — Rapid STP (2 seconds or less convergence).
- **MSTP (IEEE 802.1s)** — Multiple Spanning Tree Protocol, supports multiple VLANs and is ideal for mixed vendor environments.
- Cisco proprietary STP versions:
  - **PVST+** and **RPVST+** allow separate spanning trees per VLAN.

Layer 2 Risks

- Devices not running STP cause loop risks:
  - Unmanaged switches
  - Hubs
- **Note:** Redundant cabling connected to non-STP devices WILL cause layer 2 loops.

Port Status Colors on Switches

- **Orange:** Port blocked by STP
- **Green:** Port forwarding normally

VLAN Operation and Essentials

What is a VLAN?

- A VLAN (Virtual Local Area Network) is a logical segmentation of a network into separate broadcast domains.
- By default, all ports are on VLAN 1.
- Each VLAN corresponds to its own subnet.
- VLANs are separated by routers (router ends the VLAN).

Useful Commands:

- `show vlan brief` — Displays VLAN configuration.
- `switchport access vlan 10` — Assigns port to VLAN 10.

Voice VLANs

- IP phones (VoIP phones) are often deployed in a separate VLAN.
- IP phones operate as 2-port switches (one port to the phone, one for the PC).
- The extra port on the IP phone is typically assigned to a different VLAN (usually the data VLAN).
- **Exam notes:**
    - If an IP phone is not in the correct VLAN, it may fail to get its configuration.
    - The "access VLAN" config may also be called the **native VLAN**, which is the untagged VLAN for an 802.1Q trunk.

Switchport Configuration Example

```
interface gigabitEthernet 0/10
 switchport mode access
 switchport access vlan 12
 switchport voice vlan 21
end
```

- Assigning a VLAN to a port changes the subnet of any connected device.
- If a host is on the wrong VLAN, connectivity issues may occur.
- Devices with DHCP static reservations must be placed in the VLAN matching the reservation's subnet.
- IP phones are often placed in a separate VLAN for voice traffic.

802.1Q Trunking and VLANs

- 802.1Q is the IEEE standard for VLAN tagging on trunk links.
- Allows multiple VLANs to share a single physical link.
- Tags frames with a VLAN ID in the Ethernet frame header.
- The **native VLAN** traffic is sent untagged.

Trunk Links Can Be Used For:

- Layer 2 switch to Layer 3 switch
- Layer 2 switch to Layer 2 switch
- Switch to router (using router subinterfaces)
- Switch to firewall
- Multiple SSIDs on an Access Point (AP)

CLI Example — Configuring a Trunk Port

```
enable
configure terminal
interface gigabitEthernet 0/49-0/50
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport trunk native vlan 999
interface gigabitEthernet 0/10
 switchport mode access
 switchport access vlan 20
end
```

Securing Individual Switch Ports

- **Important:** If a switch port is not in use (unattended/unused), you **MUST disable it** to prevent unauthorized access.

Exploit: Rogue 802.1Q Trunks

- **VLAN Hopping:** A rogue switch can form an unauthorized 802.1Q trunk, gaining access to VLANs that should be isolated.
- **VLAN Hopping via Double Tagging:** Attackers place multiple 802.1Q headers in a frame, with the inner VLAN being one normally segmented and unreachable without a router.
- **Solution:** Disable dynamic trunk formation on unused ports.

CLI Example — Disable Dynamic Trunking on Ports

```
interface range gigabitEthernet 1/1 - 16
 switchport mode access
end
```

Securing Against MAC Flooding Attacks

- **Definition:** MAC flooding is an attack where an attacker sends many packets with fake MAC addresses to overload a switch's MAC address table.
- **Objective:** Overflow the MAC address table, causing the switch to flood frames to all ports, potentially exposing sensitive data.
- **Tool:** `dsniff` suite includes `macof`, which can perform MAC flooding.
  - Command example: `macof -i <interface>`

Switch MAC Address Storage Capacity

- Typically ranges from 8,000 to 64,000 MAC addresses, depending on the switch model.

Display Learned MAC Address Count

```
show mac address-table
```

- **Exam notes:**
  - MAC Address Table is also called the **CAM Table**.
  - Easy to spot if one port has thousands of different MAC addresses.

Port Security — Enabling Protection on Switch Ports

- **Port Security** limits the number of MAC addresses that can be learned on a port.
- If more MAC addresses are detected than allowed, the port will shut down.
- The switch logs the MAC address and VLAN causing the security violation.

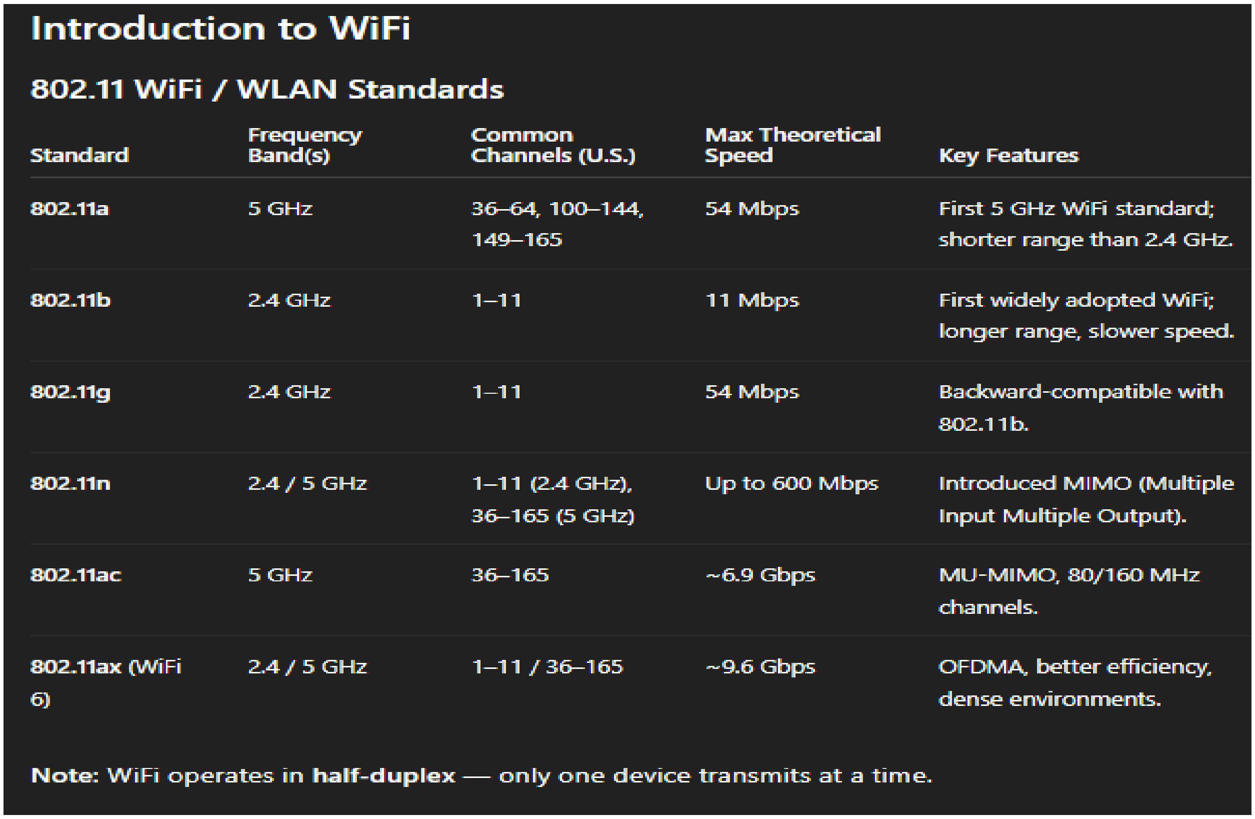
Port Security Types

- **Static:** Manually enter allowed MAC addresses.
- **Dynamic:** Automatically learn MAC addresses.
- **Sticky:** Automatically learn MACs and save them to running configuration.

CLI Example — Enable Port Security on an Interface

```
interface gigabitEthernet 0/10
 switchport mode access
 switchport port-security
 switchport port-security maximum 2
 switchport port-security violation shutdown
 switchport port-security mac-address sticky
end
```

Chapter 5: WiFi Technologies



Introduction to WiFi

802.11 WiFi / WLAN Standards

Standard	Frequency Band(s)	Common Channels (U.S.)	Max Theoretical Speed	Key Features
802.11a	5 GHz	36–64, 100–144, 149–165	54 Mbps	First 5 GHz WiFi standard; shorter range than 2.4 GHz.
802.11b	2.4 GHz	1–11	11 Mbps	First widely adopted WiFi; longer range, slower speed.
802.11g	2.4 GHz	1–11	54 Mbps	Backward-compatible with 802.11b.
802.11n	2.4 / 5 GHz	1–11 (2.4 GHz), 36–165 (5 GHz)	Up to 600 Mbps	Introduced MIMO (Multiple Input Multiple Output).
802.11ac	5 GHz	36–165	~6.9 Gbps	MU-MIMO, 80/160 MHz channels.
802.11ax (WiFi 6)	2.4 / 5 GHz	1–11 / 36–165	~9.6 Gbps	OFDMA, better efficiency, dense environments.

Note: WiFi operates in **half-duplex** — only one device transmits at a time.

Infrastructure WLANs

- **Wireless Access Points (AP or WAP)** create the WLAN.
- **Shared Bandwidth** — all clients on the same channel share the available bandwidth.
- **CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance)** is used in all 802.11 standards to reduce collisions.

Channel Selection for WiFi

2.4 GHz

- Total channels (U.S.): **1–11**
- Recommended non-overlapping channels: **1, 6, 11**
- **Exam Note:** Microwave ovens and Bluetooth devices can cause interference in the 2.4 GHz band.

5 GHz

- Non-overlapping channels: e.g., **36–48**, 52–64, 100–144, 149–165
- Shorter range, higher throughput.

Key Terms & Definitions

- **Spectrum Analyzer**
  A tool (hardware or software) that visually displays RF signal strength across frequency ranges, helping identify interference sources.
- **WiFi Analyzer**
  A software tool that detects nearby WiFi networks, their SSIDs, channels, and signal strengths to assist in channel planning.
- **802.11h**
  Amendment to 802.11 for 5 GHz operation.
  Includes:
  - **DFS (Dynamic Frequency Selection):** Detects radar signals and moves APs to different channels to avoid interference.
  - **TPC (Transmit Power Control):** Adjusts power levels to reduce interference and comply with regulations.

Deploying WLANs

- **SSID (Service Set Identifier)**
  - Network name (max 32 characters, case-sensitive).
  - Broadcast in **beacon frames**.
  - Must match exactly for connection.
  - **Hiding the SSID** is **not** a security feature — SSIDs can be detected in captured packets.

Common SSID Practices

1. **Internal SSID**
   - WPA2/WPA3 Enterprise mode
   - For employees only
2. **IoT SSID**
   - For devices like cameras, printers
   - WPA2-PSK or WPA3-SAE

3. **Guest SSID** (if required)
    - Isolated from internal resources
    - Internet-only access
    - Use Captive Portal authentication

Performance Recommendations

- Limit to **3 or fewer SSIDs** to reduce management overhead and airtime consumption.
- Avoid hidden SSIDs (slows roaming).
- Consider **Wireless Client Isolation** for guest networks.

Captive Portals

- Enforce Acceptable Use Policy (AUP) via web redirection.
- Common for guest WiFi.
- Misconfiguration can cause intermittent connectivity.
- Not suitable for IoT devices.
- CLI for enabling guest VLAN (Cisco example):

```
bash
CopyEdit
Switch(config)# vlan 50
Switch(config-vlan)# name Guest
Switch(config-vlan)# exit
Switch(config)# interface g0/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 50
```

Wireless Modes

- **Ad Hoc Mode (IBSS – Independent Basic Service Set)**
  Devices connect directly to each other without a central AP.
  Peer-to-peer, decentralized, temporary connections.
- **Infrastructure Mode (ESS – Extended Service Set)**
  Multiple APs connected to a wired LAN; enables roaming with one set of credentials.

Wireless Mesh Networks

- Mesh APs create a **backhaul** link between each other and to the wired network.
- Common for city-wide WiFi or first responder networks.
- Mounted on streetlights, traffic poles, etc.

WLAN Controllers

- **Definition:** Centralized device that manages multiple APs, controlling configuration, firmware updates, security, and monitoring.
- **CAPWAP (Control and Provisioning of Wireless Access Points)**
  Tunneling protocol used by WLAN controllers to communicate with APs for management and data forwarding.