CCNA: Switching, Routing, and Wireless Essentials

**Module 3 – VLANs (Virtual Local Area Networks)**

*I. Definition of VLANs*

- VLANs are logical groupings of network devices that function as if they were on the same physical network segment, even though they may be physically located on different segments. They are defined by software, not by physical connections.

- **Key Importance:**

+ **Broadcast Domain Reduction:** VLANs break down large broadcast domains into smaller ones, significantly improving network performance and reducing network congestion.

**+ Enhanced Security:** By segmenting the network, VLANs enhance security by restricting communication between different groups of users or devices.

**+ Improved Network Management:** VLANs make network management easier by allowing administrators to group devices based on function, team, or application, simplifying network configuration and troubleshooting.

**+ Flexibility and Scalability:** VLANs provide flexibility in network design and allow for easier network expansion and changes as business needs evolve.

**=> In essence, VLANs offer a powerful mechanism for creating a more efficient, secure, and manageable network environment**

*I. Benefits of VLANs*

- **Improved Network Security:** By segmenting the network into smaller broadcast domains, VLANs limit the impact of security breaches. If a malicious attack occurs on one VLAN, it's less likely to spread to other parts of the network.

- **Enhanced Network Performance:** VLANs reduce network congestion by limiting the number of devices that share the same broadcast domain. This leads to faster data transmission and improved overall network performance.

- **Simplified Network Management:** VLANs make it easier to manage and troubleshoot network issues. By isolating different departments or workgroups into separate VLANs, network administrators can quickly identify and resolve problems within specific segments.

- **Flexible Network Design:** VLANs provide flexibility in network design by allowing network administrators to logically group devices based on function or department, regardless of their physical location.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

*III. Types of VLANS*

- Default VLAN:

- Data VLAN: Data VLANs are the workhorses of network segmentation, designed to isolate user-generated traffic within specific groups. These groups can be defined by various criteria, such as department, role, or project. By separating users into distinct VLANs, organizations can enhance network security, improve performance, and simplify network management.

- Native VLAN:

+ **Untagged Traffic Carrier:** The native VLAN carries untagged traffic on trunk ports.

+ **Default VLAN:** On Cisco devices, VLAN 1 is often the default native VLAN.

+ **Security Risk:** Using VLAN 1 as the native VLAN can create security vulnerabilities.

- Management VLAN: A management VLAN is a data VLAN configured specifically for network management traffic including SSH, Telnet, HTTPS, HTTP, and SNMP. By default, VLAN 1 is configured as the management VLAN on a Layer 2 switch.

- Voice VLAN: A separate VLAN is needed to support Voice over IP (VoIP). VoIP traffic requires the following:

+ Assured bandwidth to ensure voice quality

+ Transmission priority over other types of network traffic

+ Ability to be routed around congested areas on the network

+ Delay of less than 150 ms across the network

*IV. VLAN Trunks:*

- **Purpose:** Allow communication between devices in the same VLAN that are connected to different switches without the need for a router.

- **How they work:**

+ Carry traffic from multiple VLANs on a single link.

+ Utilize IEEE 802.1Q standard for coordination.

+ Operate on various Ethernet speeds (Fast Ethernet, Gigabit Ethernet, 10-Gigabit Ethernet).

- **Key Characteristics:**

+ Not assigned to a specific VLAN.

+ Can be used between switches, routers, servers, and other 802.1Q-capable devices.

+ By default, on Cisco Catalyst switches, all VLANs are supported on trunk ports.

A diagram of a computer network

Description automatically generated

*V. Network without VLAN:*

In a network without VLANs, each subnet forms a single broadcast domain. This means that any broadcast sent within a subnet will be received by all devices within that subnet. While this can be useful for some applications, it also has drawbacks:

* **Increased Network Traffic:** Unnecessary broadcasts can significantly increase network traffic, potentially impacting performance for other devices.
* **Security Risks:** Broadcasts can be exploited by attackers to scan the network or spread malware.
* **Scalability Issues:** As the number of devices in a broadcast domain grows, broadcast traffic can become overwhelming, leading to performance degradation.

*VI. Network with VLAN:*

- When VLANs are implemented, a network is logically divided into multiple broadcast domains. In this scenario, faculty devices are in VLAN 10, and student devices are in VLAN 20. When PC1 (in VLAN 10) sends a broadcast, switch S2 only forwards that broadcast to ports assigned to VLAN 10. This prevents the broadcast from reaching devices in VLAN 20.

- VLANs offer several key advantages:

* **Reduced Broadcast Traffic:** By segmenting the network, VLANs confine broadcasts to specific groups of devices, significantly reducing unnecessary traffic within the network.
* **Enhanced Security:** VLANs provide a layer of security by isolating different groups of users and devices. This helps prevent unauthorized access and limits the impact of security breaches.
* **Improved Network Performance:** Reduced broadcast traffic leads to improved network performance for all devices.
* **Simplified Network Management:** VLANs make it easier to manage and troubleshoot network issues by isolating problems to specific segments.