Campus Network Portfolio

Project Overview

This Campus Network Portfolio involves the design and configuration of a comprehensive campus network that includes core, distribution, and access layers with the Cisco iOS command line. In this project, I implement various protocols and technologies to ensure network segmentation, redundancy, security, and efficient traffic management. Key protocols and technologies include virtual local area networks (VLANs), trunking, spanning tree protocol (STP), EtherChannel, first hop redundancy protocols (FHRP), layer 3 switching, switch virtual interfaces (SVIs), DHCP relay, DHCP snooping, dynamic ARP inspection (DAI), and port security.

Protocols and Technologies

Virtual Local Area Networks (VLANs):

Using VLANs, I segment network traffic, improving security and performance by isolating different types of traffic. Each VLAN represents a distinct broadcast domain.

Configuration:

> **vlan 10:** Creates VLAN 10 on the switch.
> **name VLAN10**: Assigns the name "VLAN10" to VLAN 10.
>
> **vlan 20**: Creates VLAN 20 on the switch.
> **name VLAN20**: Assigns the name "VLAN20" to VLAN 20.

Trunking (IEEE 802.1q):

Trunking is configured to carry multiple VLANs over a single link between switches, allowing VLAN traffic to be passed through the network.

Configuration:

> **interface range GigabitEthernet0/1-2**: Selects the interface range GigabitEthernet0/1 to GigabitEthernet0/2.
>
> **switchport mode trunk**: Sets the interfaces to trunk mode, allowing them to carry multiple VLANs.
>
> **switchport trunk native vlan 254**: Specifies VLAN 254 as the native VLAN for untagged traffic on the trunk links.

switchport trunk allowed vlan 1,10,20,30,40,90,100,180,254: Allows the specified VLANs to pass through the trunk links.

Notes:
These commands configure trunk links on the GigabitEthernet0/1 and GigabitEthernet0/2 ports of the given switch, allowing them to carry traffic for multiple VLANs. They designate VLAN 254 as the native VLAN for untagged traffic and specify the allowed VLANs that can pass through these trunk links.

Spanning Tree Protocol (STP):

I add STP to prevent network loops and ensure redundancy by electing root bridges and blocking redundant paths. I include Portfast so that new end devices I add are immediately connected to the switch. Since I added Portfast, I make sure to enable BPDU (Bridge Protocol Data Unit) Guard so that any untrusted end devices cannot act like a switch and gain information about the network.

Configuration:

spanning-tree vlan 10,20,90,100,254 root primary: Configures the switch as the primary root bridge for VLANs 10, 20, 90, 100, and 254.

spanning-tree vlan 30,40,180 root secondary: Configures the switch as the secondary root bridge for VLANs 30, 40, and 180.

spanning-tree portfast: Enables Portfast on the switch to immediately transition ports to the forwarding state for connected end devices.

spanning-tree bpduguard enable: Enables BPDU Guard.

Notes:
This configuration is on one of the two distribution switches of the network. It sets the given switch as the primary root bridge for STP in VLANs 10, 20, 90, 100, and 254, making it the central point for these VLANs to prevent loops. As the central point, it will make the spanning tree calculations and traffic forwarding decisions for these VLANs. The switch is also configured as the secondary root bridge for VLANs 30, 40, and 180, which means it will take over as the root bridge if the primary root bridge fails. BPDU Guard protects against potential BPDU attacks by disabling Portfast-enabled ports that receive BPDU packets, ensuring untrusted devices cannot participate in STP.

EtherChannel:

EtherChannel is used to bundle multiple physical links into a single logical link, increasing bandwidth and providing redundancy. By aggregating multiple interfaces, EtherChannel can balance traffic loads across the links and ensure that the network remains functional in case one of the links fails.

Configuration:

interface Port-channel1: Creates Port-channel 1.

switchport mode trunk: Sets Port-channel 1 to trunk mode.

switchport trunk native vlan 254: Specifies VLAN 254 as the native VLAN for Port-channel 1.

switchport trunk allowed vlan 1,10,20,30,40,90,100,180,254: Allows the specified VLANs on Port-channel 1.

interface range GigabitEthernet0/1-2: Selects the interface range GigabitEthernet0/1 to GigabitEthernet0/2.

channel-group 1 mode active: Adds the interfaces to channel group 1 with LACP (Link Aggregation Control Protocol) in active mode.

Notes:
For the port channel to work properly, it needs to have the same attributes as the physical interfaces that it aggregates. This means configuring the port channel interface with the same trunk settings as the physical interfaces. In this configuration, the port channel is set as a trunk link separately. Then, ports GigabitEthernet0/1 and GigabitEthernet0/2 are added to the port channel. Activating LACP allows the switch to automatically form an EtherChannel by exchanging LACP packets between the connected devices, ensuring dynamic link aggregation and improved redundancy and load balancing.

First Hop Redundancy Protocol (FHRP):
With a FHRP, I provide default gateway redundancy, ensuring high availability to the network. My implementation uses HSRP (Hot Standby Router Protocol).

Configuration:

interface Vlan10: Selects the interface for VLAN 10.

ip address 192.168.10.2 255.255.255.0: Assigns the IP address 192.168.10.2 with a subnet mask of 255.255.255.0 to VLAN 10.

standby 1 ip 192.168.10.1: Configures the HSRP virtual IP address 192.168.10.1.

standby 1 priority 110: Sets the HSRP priority to 110 (higher priority means more likely to become the active router).

standby 1 preempt: Enables preemption, allowing the router to take over as active if it has a higher priority.

Notes:

This implementation ensures that the network continues to run smoothly if the primary gateway router for VLAN 10 goes down. Using HSRP, redundancy is provided by creating a virtual router shared between multiple physical routers. If the primary router fails to send 'Hello' messages, the standby router will become the new active router, and traffic will be routed through the virtual IP address.

Layer 3 Switching:

Layer 3 switches are configured to perform routing between VLANs, enabling inter-VLAN communication and improving routing efficiency within the campus network.

Configuration:

> **interface Vlan10**: Selects the interface for VLAN 10.
>
> **ip address 192.168.10.1 255.255.255.0**: Assigns the IP address 192.168.10.1 with a subnet mask of 255.255.255.0 to VLAN 10.
>
> **interface Vlan20**: Selects the interface for VLAN 20.
>
> **ip address 192.168.20.1 255.255.255.0**: Assigns the IP address 192.168.20.1 with a subnet mask of 255.255.255.0 to VLAN 20.

Notes:
This configuration creates Switched Virtual Interfaces (SVIs) on the Layer 3 switch by providing distinct IP addresses for each VLAN. With these SVIs, the Layer 3 switch can route traffic between the VLANs efficiently, enabling inter-VLAN communication and improving overall routing efficiency within the campus network.

DHCP Relay:

I configure DHCP Relay to forward DHCP requests from clients in different VLANs to a centralized DHCP server, ensuring proper IP address allocation.

Configuration:

> **interface Vlan10**: Selects the interface for VLAN 10.
>
> **ip helper-address 192.168.1.1**: Configures the DHCP relay agent to forward DHCP requests to the DHCP server at IP address 192.168.1.1.

Notes:
DHCP Relay is essential in this network because DHCP clients are located in different VLANs from the DHCP server. Without DHCP relay, DHCP requests (broadcast messages) from other VLANs would not reach the DHCP server because routers typically do not forward broadcast traffic. In this configuration, DHCP Relay uses a helper address 192.168.1.1 to act as the intermediary, sending unicast packets between the DHCP server and the end devices on other VLANs.

DHCP Snooping:

By enabling DHCP Snooping, I filter untrusted DHCP messages from the network, preventing rogue DHCP servers from distributing incorrect IP addresses.

Configuration:

ip dhcp snooping: Enables DHCP snooping globally on the switch.

interface range GigabitEthernet0/1-2: Selects the interface range of the trunk ports to be trusted.

ip dhcp snooping trust: Configures the selected interface as trusted for DHCP snooping, allowing DHCP messages from this interface.

Notes:
With these commands, DHCP snooping inspects the DHCP messages being sent to ensure that only trusted DHCP servers are allowed to send DHCP messages. When specifying the interface range, it is important to ensure that the interface connected to the DHCP server is configured as trusted. Otherwise, DHCP packets from the server would be blocked, preventing DHCP clients from receiving their IP addresses and causing network communication issues.

Dynamic Arp Inspection (DAI):

DAI is enabled to prevent ARP spoofing attacks by verifying ARP packets against the DHCP snooping database, ensuring the integrity of IP-to-MAC address mappings.

Configuration:

ip arp inspection validate src-mac dst-mac ip: Configures DAI to validate the source MAC, destination MAC, and IP address in ARP packets.

interface range GigabitEthernet0/1-2: Selects the interface range of the trunk ports to be trusted.

ip arp inspection trust: Configures the selected interface as trusted for ARP inspection.

Notes:
After adding these commands, the network is protected against malicious devices sending false ARP messages to associate their MAC address with the IP address of another device. These false messages could be used to intercept or disrupt traffic.

Port Security:
I add port security to limit the number of MAC addresses on a port, protecting against MAC flooding attacks and ensuring that only authorized devices can connect.

Configuration:

interface range FastEthernet0/1-24: Selects the interface range FastEthernet0/1 to FastEthernet0/24.

switchport mode access: Sets the interfaces to access mode.

switchport port-security: Enables port security on the interfaces.

switchport port-security maximum 3: Limits the number of MAC addresses allowed on each port to 3.

switchport port-security violation restrict: Configures the action to take when a security violation occurs (restrict the port).

switchport port-security mac-address sticky: Enables sticky MAC addresses.

Notes:
Port security is configured to limit the number of MAC addresses on each port, protecting against MAC flooding attacks and unauthorized devices. By default, port security shuts down a port when a violation occurs, which is a safe option for protecting against attacks. In this network, I set the maximum number of devices on each port to 3, allowing for the connection of two devices per switch with room for an additional device. Enabling sticky MAC addresses allows the switch to dynamically learn and retain MAC addresses, providing flexibility while maintaining security.

SSH (Secure Shell):
For secure remote access for network administration from the connected end devices, I add SSH to the network. This provides encrypted communication between the administrator and the other network devices, ensuring that sensitive information, such as login credentials and configuration commands, is not exposed to unauthorized parties.

Configuration:

ip domain-name SSH-KEY.com: Sets the domain name for the network device. This is required for generating the RSA key pair.

crypto key generate rsa modulus 2048: Generates an RSA key pair, which is necessary for SSH encryption.

username admin privilege 15 secret password: Creates a user with administrative privileges and a secret password for authentication.

line vty 0 4: Selects the VTY (virtual terminal) lines for configuration, allowing up to 5 simultaneous remote sessions.

transport input ssh: Restricts the transport input to SSH only, disabling other protocols like Telnet.

login local: Uses the local user database for authentication.

Notes:
Adding a domain name is required for the RSA key generation process. This network configuration uses a 2048-bit RSA key pair, which provides strong encryption for SSH sessions. In this network, RSA ensures substantial security by using a private key (kept by the administrator who generated the key) and a public key (shared with those the administrator grants access to). This allows for secure key exchange and digital signatures, preventing man-in-the-middle attacks.