LEARN IT CAMP

Project Title: Enterprise Network Implementation with Hierarchical Design

Objective:
Your task is to configure a hierarchical enterprise network based on the provided topology. You will implement a multi-layer architecture including Core, Distribution, and Access layers. The configuration will involve VLANs, Rapid Spanning Tree Protocol (RSTP), inter-VLAN routing, OSPF for dynamic routing, DHCP services for client IP addressing, and secure access to the Internet via NAT.

IP Addressing Scheme:

- **LAN Networks:** Use the 10.0.0.0/8 private address space.

- **Management VLAN (VLAN 99):** 10.99.0.0/24

- **Sales VLAN (VLAN 10):** 10.10.0.0/23

- **IT VLAN (VLAN 20):** 10.20.0.0/24

- **Admin VLAN (VLAN 30):** 10.30.0.0/24

- **Servers VLAN (VLAN 90):** 10.90.0.0/24

- **Point-to-Point Links (Core Switch to Core Router):** 10.255.255.0/30 and 10.255.255.4/30

- **Internet Connection (Core Router to Cloud):** Assume the ISP provides the address 203.0.113.1/30 for your router's external interface.

Part 1: Initial Device Setup and LLDP

1. **Hostname Configuration:** Assign logical hostnames to all routers and switches based on their layer and position (e.g., Core-R1, Core-SW1, Dist-SW1, Access-SW1, etc.).

2. **Enable LLDP:** Enable Link Layer Discovery Protocol (LLDP) globally on all switches and routers to facilitate network discovery and documentation.

3. **Basic Security:**

   - Set the privileged EXEC mode password to class.

   - Set the console and VTY line passwords to cisco.

   - Encrypt all plaintext passwords.

Part 2: Access Layer Configuration (VLANs and Trunks)

1. **VLAN Creation:** On all switches (Core, Access and Distribution), create the following VLANs:

   - VLAN 10 (Name: Staff)

   - VLAN 20 (Name: IT)

   - VLAN 30 (Name: Admin)

   - VLAN 90 (Name: Servers)

   - VLAN 99 (Name: Management)

2. **Access Port Assignment:**

   - On the access layer switches, assign ports connected to PCs to the Vlans i.e. **Staff VLAN (VLAN 10)**.

   - Configure these ports for switchport mode access and enable spanning-tree portfast.

3. **Trunking:**

   - Configure the links between the access layer switches, the distribution layer switches and Core Switches as 802.1Q trunks.

   - Ensure trunks only allow VLANs 10, 20, 30, 90 and 99.

Part 3: Spanning Tree Protocol (STP) Optimization

1. **Protocol Selection:** Ensure all switches are running **Rapid PVST+** (Rapid Per-VLAN Spanning Tree Protocol).

2. **Root Bridge Configuration:**

    o   Configure **Core-SW1** to be the primary root bridge for VLANs 10, 30 and 90.

    o   Configure **Core-SW2** to be the primary root bridge for VLANs 20 and 99.

    o   Configure the other Core switch to be the secondary root for each set of VLANs respectively. This ensures load balancing across the uplinks if one fails.

Part 4: Distribution Layer & Inter-VLAN Routing

1. **Enable IP Routing:** On Core-SW1 and Core-SW2 (which are multilayer switches), enable IP routing.

2. **SVI Configuration:** On both Core switches, create Switched Virtual Interfaces (SVIs) for all VLANs (10, 20, 30, 90, 99). These SVIs will serve as the default gateways for the devices in those VLANs.

    o   Assign the first usable IP address of each VLAN's subnet to the SVI on CoreSW1.

    o   Assign the second usable IP address of each VLAN's subnet to the SVI on CoreSW2.

    o   *(Note: For a real high-availability network, you would use a First Hop Redundancy Protocol like HSRP, but for this task, we will rely on OSPF to manage pathing).*

3. **Server Port:** Configure the port connecting to **Server0** on its access switch to be in the **Servers VLAN (VLAN 30)** and assign the server a static IP address: 10.30.0.10/24 with the gateway as the Core-SW1 SVI for VLAN 30.

4. Configure the necessary trunk links, VLANS and STP for high availability on the 6 Distribution switches

Part 5: Core Layer and OSPF Routing

1. **IP Addressing on Routed Links:** Configure IP addresses on the point-to-point links between the Core switches and the Core router.

2. **OSPF Configuration:**

    o   Enable OSPF using process ID 1 on the Core router and both Core switches.

    o   Configure the router OSPF process with a router-ID.

- On the Core switches, advertise the VLAN subnets into OSPF Area 0.
- On all three devices, enable OSPF on the point-to-point interfaces connecting them, placing them in Area 0.

Part 6: DHCP Services

1. **DHCP Server:** Configure Core-R1 to act as a DHCP server for the Staff, Admin and IT VLANs.

2. **DHCP Pools:**

   - Create a DHCP pool for **VLAN 10 (Staff)**. Exclude the gateway addresses used by the SVIs.

   - Create a DHCP pool for **VLAN 20 (IT)**. Exclude the gateway addresses.

   - Create a DHCP pool for **VLAN 30 (Admin)**. Exclude the gateway addresses.

   - Configure each pool to provide the correct default gateway and a DNS server address of 8.8.8.8.

3. **DHCP Relay:** On the SVIs for VLAN 10, 20 and 30 on both Core switches, configure an ip helper-address pointing to the OSPF-reachable interface of Core-R1.

4. **Client Verification:** Set all PCs to obtain their IP configuration automatically via DHCP.

Part 7: Internet Access

1. **Core Router WAN Configuration:** Configure the interface on Core-R1 that connects to the Cloud with the public IP address 203.0.113.1/30.

2. **Default Route:** Add a static default route (0.0.0.0 0.0.0.0) on Core-R1 pointing towards the ISP (e.g., 203.0.113.2).

3. **Route Redistribution:** Redistribute this static default route into the OSPF domain so that all internal devices learn how to reach the internet.

4. **Network Address Translation (NAT):**

   - Configure NAT on Core-R1.

   - Define an access list that permits all private IP ranges (10.0.0.0/8) to be translated.

   - Configure NAT overload (PAT) on the router's outside interface to translate the permitted private addresses to its public IP.

   - Apply NAT to the appropriate inside and outside interfaces.

Part 8: Verification and Testing

1. **LLDP:** Use show lldp neighbors on several devices to verify physical connections.

2. **STP:** Use show spanning-tree vlan [vlan-id] to verify root bridge roles.

3. **OSPF:** Use show ip ospf neighbor and show ip route to confirm routing tables are populated correctly on the core and distribution devices.

4. **DHCP:** Check the PCs to ensure they have received correct IP addresses from the DHCP pools.

5. **Connectivity:**

   o Ping from a PC in VLAN 10 to a PC in another part of VLAN 10.

   o Ping from a PC in VLAN 10 to Server0 in VLAN 30 (testing inter-VLAN routing).

   o Ping the internet from all PC's