**VLAN & IP Addressing Configuration on Multilayer Switch (3560)**

We will configure **VLANs, IP addresses, inter-VLAN routing, and trunking** on the **Multilayer Switch (3560)**.

**Create VLANs** (10, 20, 30, 100).  
**Assign IP addresses to VLAN interfaces (SVIs)** as default gateways.  
**Enable Inter-VLAN Routing**.  
**Configure trunk ports for VLAN communication**.  
**Set DHCP relay (IP helper) for VLANs**.

Switch> enable

Switch# configure terminal

**Create VLANs**

Switch(config)# vlan 10

Switch(config-vlan)# name Management

Switch(config-vlan)# exit

Switch(config)# vlan 20

Switch(config-vlan)# name Students

Switch(config-vlan)# exit

Switch(config)# vlan 30

Switch(config-vlan)# name Faculty

Switch(config-vlan)# exit

Switch(config)# vlan 100

Switch(config-vlan)# name Guests

Switch(config-vlan)# exit

**Assign IP Addresses to VLAN Interfaces (SVIs)**

Each VLAN needs an **interface (SVI) with an IP address** to act as a **default gateway**.

Switch(config)# interface vlan 10

Switch(config-if)# ip address 192.168.10.1 255.255.255.0

Switch(config-if)# no shutdown

Switch(config-if)# exit

Switch(config)# interface vlan 20

Switch(config-if)# ip address 172.16.20.1 255.255.255.0

Switch(config-if)# no shutdown

Switch(config-if)# exit

Switch(config)# interface vlan 30

Switch(config-if)# ip address 172.16.30.1 255.255.255.0

Switch(config-if)# no shutdown

Switch(config-if)# exit

Switch(config)# interface vlan 100

Switch(config-if)# ip address 10.10.100.1 255.255.255.0

Switch(config-if)# no shutdown

Switch(config-if)# exit

**Enable Inter-VLAN Routing**

By default, Layer 3 switching is **disabled**. We enable **IP routing** so VLANs can communicate.

Switch(config)# ip routing

**Configure Trunk Ports**

We set **GigabitEthernet 0/1 and 0/2 as trunk ports** for VLAN traffic.

Switch(config)# interface gigabitethernet 0/1

Switch(config-if)# switchport trunk encapsulation dot1q

Switch(config-if)# switchport mode trunk

Switch(config-if)# switchport trunk allowed vlan 10,20,30,100

Switch(config-if)# exit

Switch(config)# interface gigabitethernet 0/2

Switch(config-if)# switchport trunk encapsulation dot1q

Switch(config-if)# switchport mode trunk

Switch(config-if)# switchport trunk allowed vlan 10,20,30,100

Switch(config-if)# exit

**Configure DHCP Relay (IP Helper Address)**

Since **DHCP Server is on a separate device**, we need to forward DHCP requests.

Switch(config)# interface vlan 20

Switch(config-if)# ip helper-address 192.168.10.2

Switch(config-if)# exit

Switch(config)# interface vlan 30

Switch(config-if)# ip helper-address 192.168.10.2

Switch(config-if)# exit

Switch(config)# interface vlan 100

Switch(config-if)# ip helper-address 192.168.10.2

Switch(config-if)# exit

Switch(config)# exit

Switch# write memory

**Verification Commands**

Use these commands to check if everything is correct:

Switch# show vlan brief → Check VLANs

Switch# show ip interface brief → Verify SVI IPs

Switch# show interfaces trunk → Confirm trunk ports

Switch# show running-config → View full config

**Configuring the DHCP Server (On a PC or Server) in Packet Tracer**

Since **Packet Tracer does not support a dedicated Cisco DHCP server**, we will use a **Server device with the built-in DHCP service**. This will allow VLAN 20 (Students), VLAN 30 (Faculty), and VLAN 100 (Guests) to get **dynamic IP addresses**.

**Create separate DHCP pools** for VLAN 20, VLAN 30, and VLAN 100.  
**Set the correct default gateway** for each VLAN.  
**Ensure DHCP is enabled** and clients receive valid IP leases.

**Step-by-Step DHCP Server Configuration**

**Place the DHCP Server in the Topology**

1. **Go to Packet Tracer** → Open your **network topology**.
2. **Select a Server** from the **End Devices** section.
3. **Place the server** in the **Management VLAN (VLAN 10)**.
4. **Connect the Server to the Multilayer Switch (Fa0/3)**.

**Configure the DHCP Server’s Static IP (For Management VLAN)**

1. Click on the **DHCP Server**.
2. Go to the **Desktop** tab → Open **IP Configuration**.
3. Set a **Static IP Address** for the server:
   * **IP Address:** 192.168.10.2
   * **Subnet Mask:** 255.255.255.0
   * **Default Gateway:** 192.168.10.1
   * **DNS Server:** 8.8.8.8 (Google DNS)

Now, the DHCP Server is **reachable on VLAN 10**.

**Enable the DHCP Service**

1. Click on the **DHCP Server**.
2. Go to the **Services** tab → Select **DHCP**.
3. **Ensure DHCP service is turned ON** (toggle switch).

**Configure DHCP Pools for Each VLAN**

Now, we will create **three DHCP pools** for VLAN 20, VLAN 30, and VLAN 100.

**VLAN 20 (Students) – DHCP Pool Configuration**

1. In the **DHCP tab**, click on **Add Pool**.
2. Name it **STUDENT\_POOL**.
3. Configure the following settings:
   * **Default Gateway:** 172.16.20.1
   * **DNS Server:** 8.8.8.8
   * **Start IP Address:** 172.16.20.10
   * **Subnet Mask:** 255.255.255.0
   * **Maximum Number of Users:** 50 (or any limit you prefer).
4. Click **Save**.

**VLAN 30 (Faculty) – DHCP Pool Configuration**

1. Click on **Add Pool**.
2. Name it **FACULTY\_POOL**.
3. Configure the following settings:
   * **Default Gateway:** 172.16.30.1
   * **DNS Server:** 8.8.8.8
   * **Start IP Address:** 172.16.30.10
   * **Subnet Mask:** 255.255.255.0
   * **Maximum Number of Users:** 30.
4. Click **Save**.

**VLAN 100 (Guests) – DHCP Pool Configuration**

1. Click on **Add Pool**.
2. Name it **GUEST\_POOL**.
3. Configure the following settings:
   * **Default Gateway:** 10.10.100.1
   * **DNS Server:** 8.8.8.8
   * **Start IP Address:** 10.10.100.10
   * **Subnet Mask:** 255.255.255.0
   * **Maximum Number of Users:** 20.
4. Click **Save**.

**Verification via CLI**

On the **Multilayer Switch**, check the DHCP relay functionality:

Switch# show ip interface brief

Switch# show running-config

**Configure Access Layer Switches (2960) Based on Multilayer Switch Port Usage**

**Complete Configuration for Both Multilayer Core Switch (3560) and Access Switch (2960)**

This configuration **ensures all connections are properly trunked and VLANs are correctly assigned**.

**Configuration for Multilayer Core Switch (3560)**

**Configure Trunk Ports to Access Switches (Gig0/1 & Gig0/2)**

MultilayerSwitch(config)# interface gigabitethernet 0/1

MultilayerSwitch(config-if)# switchport trunk encapsulation dot1q

MultilayerSwitch(config-if)# switchport mode trunk

MultilayerSwitch(config-if)# switchport trunk allowed vlan 10,20,30,100

MultilayerSwitch(config-if)# exit

MultilayerSwitch(config)# interface gigabitethernet 0/2

MultilayerSwitch(config-if)# switchport trunk encapsulation dot1q

MultilayerSwitch(config-if)# switchport mode trunk

MultilayerSwitch(config-if)# switchport trunk allowed vlan 10,20,30,100

MultilayerSwitch(config-if)# exit

**Configure Trunk Port to WLC (Fa0/1)**

MultilayerSwitch(config)# interface fastethernet 0/1

MultilayerSwitch(config-if)# switchport trunk encapsulation dot1q

MultilayerSwitch(config-if)# switchport mode trunk

MultilayerSwitch(config-if)# switchport trunk allowed vlan 10

MultilayerSwitch(config-if)# exit

**Configure Access Port to Firewall (Fa0/2)**

MultilayerSwitch(config)# interface fastethernet 0/2

MultilayerSwitch(config-if)# switchport mode access

MultilayerSwitch(config-if)# switchport access vlan 10

MultilayerSwitch(config-if)# exit

**Configuration for Access Switch (2960)**

**Configure Trunk Ports to Multilayer Switch (Fa0/1) & AP (Fa0/2)**

AccessSwitch(config)# interface fastethernet 0/1

AccessSwitch(config-if)# switchport trunk encapsulation dot1q

AccessSwitch(config-if)# switchport mode trunk

AccessSwitch(config-if)# switchport trunk allowed vlan 10,20,30,100

AccessSwitch(config-if)# exit

AccessSwitch(config)# interface fastethernet 0/2

AccessSwitch(config-if)# switchport trunk encapsulation dot1q

AccessSwitch(config-if)# switchport mode trunk

AccessSwitch(config-if)# switchport trunk allowed vlan 10,20,30,100

AccessSwitch(config-if)# exit

**Verify Configuration**

On **Multilayer Switch**, check trunk status:

MultilayerSwitch# show interfaces trunk

On **Access Switch**, check trunk status:

AccessSwitch# show interfaces trunk

**Ensure VLANs Exist on Access Switches (2960)**

On **each Access Switch**, create VLANs:

AccessSwitch(config)# vlan 10

AccessSwitch(config-vlan)# exit

AccessSwitch(config)# vlan 20

AccessSwitch(config-vlan)# exit

AccessSwitch(config)# vlan 30

AccessSwitch(config-vlan)# exit

AccessSwitch(config)# vlan 100

AccessSwitch(config-vlan)# exit

**This will ensure VLANs are recognized by the Access Switches.**

**Set Native VLAN on Fa0/1 (Multilayer Switch to WLC)**

On **Multilayer Switch**:

MultilayerSwitch(config)# interface fastethernet 0/1

MultilayerSwitch(config-if)# switchport trunk native vlan 10

MultilayerSwitch(config-if)# exit

**Step-by-Step RADIUS Configuration on Core Switch**

**1. Enable AAA & Define RADIUS Server**

CoreSwitch# configure terminal

CoreSwitch(config)# aaa new-model

CoreSwitch(config)# aaa authentication login default group radius local

CoreSwitch(config)# radius-server host 192.168.10.6 key radiuskey123

**2. Enable SSH Authentication via RADIUS**

CoreSwitch(config)# line vty 0 4

CoreSwitch(config-line)# login authentication default

CoreSwitch(config-line)# transport input ssh

CoreSwitch(config-line)# exit

**3. Ensure SSH is Enabled**

CoreSwitch(config)# ip domain-name example.com

CoreSwitch(config)# crypto key generate rsa

(Choose a key size of at least \*\*1024 bits\*\*)

CoreSwitch(config)# ip ssh version 2

CoreSwitch(config)# exit

CoreSwitch# write memory

MULTILAYER SWITCH CONIFGURATION

**Enable PortFast for Access Ports**

Since **Fa0/2** connects to the **RADIUS Server** (end device), it should **not participate in spanning tree negotiations** to avoid delays.

**Apply this to Fa0/2:**

MultilayerSwitch# configure terminal

MultilayerSwitch(config)# interface FastEthernet0/2

MultilayerSwitch(config-if)# spanning-tree portfast

MultilayerSwitch(config-if)# end

MultilayerSwitch# write memory

**Allow VLANs on Trunk Links to Access Switches**

Currently, **Gig0/1 and Gig0/2** (trunk links to **Access Switch 1 & 2**) are **correctly configured** but **only native VLAN 10 is set**. To support **Dynamic VLAN Assignment**, make sure all VLANs (10, 20, 30, 100) are allowed.

**Apply this to G0/1 and G0/2:**

MultilayerSwitch# configure terminal

MultilayerSwitch(config)# interface GigabitEthernet0/1

MultilayerSwitch(config-if)# switchport trunk allowed vlan 10,20,30,100

MultilayerSwitch(config-if)# exit

MultilayerSwitch(config)# interface GigabitEthernet0/2

MultilayerSwitch(config-if)# switchport trunk allowed vlan 10,20,30,100

MultilayerSwitch(config-if)# end

MultilayerSwitch# write memory

MultilayerSwitch(config-if)# end

MultilayerSwitch# write memory

**Configuration for ISP Router (Cisco 1941)**

**Step-by-Step CLI Configuration for ISP Router**

**Enter Configuration Mode**

ISP\_Router# configure terminal

**Assign WAN IP Address on Gig 0/0 (Connected to Core Router)**

ISP\_Router(config)# interface GigabitEthernet0/0

ISP\_Router(config-if)# ip address 203.0.113.2 255.255.255.252

ISP\_Router(config-if)# no shutdown

ISP\_Router(config-if)# exit

**Explanation:**

* **203.0.113.2** is the ISP Router's **WAN IP**.
* **Subnet Mask /30 (255.255.255.252)** → Allows only two usable IPs:
  + 203.0.113.1 (Core Router)
  + 203.0.113.2 (ISP Router)

**Configure Static Route for Internet Access**

ISP\_Router(config)# ip route 0.0.0.0 0.0.0.0 203.0.113.1

**Explanation:**

* This tells the ISP Router: "**Forward all traffic to the Core Router (203.0.113.1) for internet access.**"

**Enable NAT (If Needed for Simulation)**

ISP\_Router(config)# access-list 1 permit any

ISP\_Router(config)# ip nat inside source list 1 interface GigabitEthernet0/0 overload

**Explanation:**

* This applies **NAT (Network Address Translation)** so multiple private IPs can **share the WAN IP**.

**Enable OSPF or Keep Static Routing**

If using **Static Routing (Simpler Approach)**:

**No extra OSPF configuration is needed**. Just keep the static route.

If you **want dynamic routing via OSPF**, configure it like this:

ISP\_Router(config)# router ospf 1

ISP\_Router(config-router)# network 203.0.113.0 0.0.0.3 area 0

ISP\_Router(config-router)# exit

ISP\_Router(config)# write memory

**Explanation:**

* **Advertises WAN network (203.0.113.0/30) to OSPF area 0**.

**CLI Configuration for Core Router (Cisco 2911)**

**Purpose:**

* Acts as the **gateway between internal VLANs and the ISP**.
* Connects to the **ISP Router (1941) via Gig 0/0**.
* Connects to the **Firewall (ASA 5506-X) via Gig 0/1**.
* **Handles routing between internal networks**.

**Assign IP Addresses to Interfaces**

**Set WAN IP (Connected to ISP Router)**

CoreRouter# configure terminal

CoreRouter(config)# interface GigabitEthernet0/0

CoreRouter(config-if)# ip address 203.0.113.1 255.255.255.252

CoreRouter(config-if)# no shutdown

CoreRouter(config-if)# exit

**Explanation:**

* Assigns **WAN IP (203.0.113.1)** for communication with the ISP Router (203.0.113.2).
* Uses **subnet mask /30 (255.255.255.252)** for point-to-point connection.

**Set LAN IP (Connected to Firewall)**

CoreRouter(config)# interface GigabitEthernet0/1

CoreRouter(config-if)# ip address 192.168.1.1 255.255.255.0

CoreRouter(config-if)# no shutdown

CoreRouter(config-if)# exit

**Explanation:**

* **LAN IP (192.168.1.1)** is used for internal network traffic.
* **Firewall (ASA 5506-X) will use 192.168.1.2** as its IP.

**Configure Static Routing to ISP**

CoreRouter(config)# ip route 0.0.0.0 0.0.0.0 203.0.113.2

**Explanation:**

* This **default route** forwards all **external traffic to the ISP Router (203.0.113.2)**.

**Enable OSPF (If Using Dynamic Routing)**

CoreRouter(config)# router ospf 10

CoreRouter(config-router)# network 192.168.1.0 0.0.0.255 area 0

CoreRouter(config-router)# network 203.0.113.0 0.0.0.3 area 0

CoreRouter(config-router)# exit

CoreRouter(config)# write memory

**Explanation:**

* Advertises the **internal LAN network (192.168.1.0/24)**.
* Advertises the **WAN network (203.0.113.0/30)**.
* OSPF **is only needed if another router will dynamically learn routes**.

**Configure NAT (If Needed)**

If **Firewall will handle NAT**, skip this step.  
If **Core Router will handle NAT**, use:

CoreRouter(config)# access-list 1 permit any

CoreRouter(config)# ip nat inside source list 1 interface GigabitEthernet0/0 overload

**Explanation:**

* Allows **internal clients to share the WAN IP** for internet access.

**CLI Configuration for Firewall (Cisco ASA 5506-X)**

**Purpose:**

* **Secure network traffic between internal VLANs and the ISP**.
* **Control traffic flow between Core Router, Multilayer Switch, and external networks**.
* **Provide NAT (if not handled by Core Router)**.
* **Apply ACLs to filter unwanted traffic**.

**Assign IP Addresses to Firewall Interfaces**

**Set WAN IP (Outside - Connected to Core Router)**

Firewall# configure terminal

Firewall(config)# interface GigabitEthernet1/1

Firewall(config-if)# nameif OUTSIDE

Firewall(config-if)# security-level 0

Firewall(config-if)# ip address 192.168.1.2 255.255.255.0

Firewall(config-if)# no shutdown

Firewall(config-if)# exit

**Explanation:**

* **WAN interface (192.168.1.2/24) is connected to Core Router (192.168.1.1)**.
* **Security level 0** → Represents **untrusted external traffic**.

**Set LAN IP (Inside - Connected to Multilayer Switch)**

Firewall(config)# interface GigabitEthernet1/2

Firewall(config-if)# nameif INSIDE

Firewall(config-if)# security-level 100

Firewall(config-if)# ip address 192.168.10.254 255.255.255.0

Firewall(config-if)# no shutdown

Firewall(config-if)# exit

**Explanation:**

* **LAN interface (192.168.10.254/24) is connected to the Multilayer Switch (Fa0/4)**.
* **Security level 100** → Represents **trusted internal traffic**.

**Configure Default Route to Core Router**

Firewall(config)# route OUTSIDE 0.0.0.0 0.0.0.0 192.168.1.1

**Explanation:**

* Sends **all unknown (internet) traffic to the Core Router (192.168.1.1)**.

**Configure Basic ACL Rules**

**Allow Essential Traffic (ICMP, DHCP, DNS, RADIUS, HTTP, etc.):**

Firewall(config)# access-list OUTSIDE-IN permit icmp any any

Firewall(config)# access-list OUTSIDE-IN permit udp any any eq 67

Firewall(config)# access-list OUTSIDE-IN permit udp any any eq 53

Firewall(config)# access-list OUTSIDE-IN permit tcp any any eq 80

Firewall(config)# access-group OUTSIDE-IN in interface OUTSIDE

**Explanation:**

* Allows **ICMP (Ping), DHCP, DNS, and HTTP traffic**.
* Applies rules to the **OUTSIDE (WAN) interface**.