Multilayer Core Switch Configuration

What?

The **core switch** is the backbone of the network. It provides **VLAN segmentation**, **inter-VLAN routing**, and **redundancy** while connecting distribution switches, firewall, WLC, and servers.

Why?

A **multilayer switch** is required to handle both **Layer 2 switching (VLANs)** and **Layer 3 routing** for inter-VLAN communication. Without it, traffic between different VLANs wouldn't be possible.

How?

- **VLANs were created** to segment network traffic for different departments (**IT, HR, Finance, Server, Guest, and Management VLANs**). This isolates traffic, reducing broadcast domain congestion.
- **SVI (Switch Virtual Interfaces) were configured** for each VLAN, allowing the switch to route between them.
- **Trunk ports were set up** to pass VLAN traffic between the core switch and distribution switches.
- **IP routing was enabled** so that inter-VLAN traffic could be handled internally by the switch.
- **A default route was added** to send any unknown traffic towards the firewall for further security checks.
- **Unused ports were disabled** (moved to VLAN 999) to prevent unauthorized device connections.

Distribution Switches (IT, HR, Finance) Configuration

What?

Each department has a **dedicated distribution switch** to manage local devices, laptops, and APs while maintaining **trunk links to the core switch for connectivity**.

Why?

The use of **distribution switches** improves network segmentation, preventing congestion on the core switch. It also simplifies network management and enhances security.

How?

- **VLANs were assigned** based on department needs to ensure each group has its own isolated network.

- **Trunk links were configured** to connect the distribution switches to the core switch, allowing them to pass multiple VLANs.
- **Access ports were assigned** to devices such as department laptops and APs.
- **Security features were applied**, including:
    - **Port security** (to block unauthorized devices).
    - **BPDU Guard** (to prevent rogue switches from affecting the network).
    - **DHCP Snooping** (to protect against rogue DHCP servers).

Wireless LAN Controller (WLC) Configuration

What?

The **WLC** manages wireless connectivity, ensuring **SSID segmentation** for different user groups (employees vs. guests).

Why?

A **centralized WLC** is needed to control **access points, enforce security policies, and manage wireless traffic** efficiently.

How?

- **Trunk connections were established** between the WLC and core switch to allow all necessary VLANs for wireless traffic.
- **RADIUS authentication was enabled** to ensure only authorized users can access secure WiFi.
- **A guest network was configured** with strict ACLs to allow internet-only access while blocking internal resources.

DHCP and DNS Server Configuration

What?

The **DHCP server automatically assigns IP addresses**, while the **DNS server translates domain names into IP addresses**.

Why?

Instead of manually assigning IP addresses to devices, **DHCP ensures dynamic allocation**. DNS is required for domain name resolution.

How?

- **DHCP scopes were defined** for each VLAN to ensure proper IP allocation.

- **IP helper addresses were added** to allow DHCP requests to pass through VLANs and reach the DHCP server.
- **DNS settings were configured** so that clients could resolve domain names correctly.

Firewall (ASA) Configuration

What?

The **Cisco ASA firewall** is responsible for **network security, filtering traffic, and connecting the internal network to the outside world**.

Why?

The firewall ensures **unauthorized traffic is blocked**, internal resources are protected, and only approved data flows between networks.

How?

- **Interfaces were assigned:**
  - **INSIDE (192.168.99.11)** – Connected to the core switch.
  - **OUTSIDE (192.168.200.2)** – Connected to the core router (simulating ISP access).
- **ACLs (Access Control Lists) were applied** to restrict unauthorized inter-VLAN communication.
- **NAT (Network Address Translation) was configured** to allow internal users to access external resources.
- **Static routes were added** to send outbound traffic to the core router.

Core Router Configuration

What?

The **core router** is the **final network component before traffic reaches the external network (ISP or BGP attack simulation)**.

Why?

A core router is necessary to **handle external routing, provide BGP testing, and connect to the outside network**.

How?

- **BGP (Border Gateway Protocol) was configured** to simulate an external attack scenario.
- **OSPF (Open Shortest Path First) routing was enabled** to dynamically exchange routes with the firewall.

- **A static route was added** to ensure default traffic is forwarded correctly.

Redundant Core Switch Configuration (CoreSwitch-2)

What?

To ensure **high availability**, a **redundant core switch** was added.

Why?

If the primary core switch fails, the **secondary core switch takes over automatically**, ensuring no downtime.

How?

- **VLANs were mirrored from CoreSwitch-1** to maintain consistency.
- **HSRP (Hot Standby Router Protocol) was configured** to provide failover capability.
- **Trunk links were established** with the distribution switches for redundancy.
- **Firewall redundant interface was connected** using VLAN 100.
- **STP (Spanning Tree Protocol) was adjusted** to prevent loops in the network.

Testing and Verification

What?

Before finalizing, **multiple tests were conducted** to verify reliability and security.

Why?

Testing ensures that **all configurations work as expected**, preventing network failures after deployment.

How?

User Connectivity Test: Verified that all VLANs can communicate correctly.
Failover Testing: Simulated a **core switch failure** to check if HSRP activates backup switch.
Firewall Security Test: Ensured **NAT, ACLs, and outside internet access work**.
Guest WiFi Restrictions: Confirmed that **guest users cannot access internal resources**.
BGP Attack Simulation: Tested firewall blocking **external BGP advertisements**.

Final Summary

This network **implements enterprise-grade security, redundancy, and scalability**, ensuring a **high-performance, secure, and resilient infrastructure**.

✓ **Highly Secure:** Implemented **firewall ACLs, RADIUS authentication, port security, and DHCP snooping**.
✓ **Scalable:** Designed to **support more VLANs, new departments, and branch office expansions**.
✓ **Redundant:** Configured with **HSRP, STP, and dual distribution switch connections to prevent downtime**.
✓ **Future-Ready: Supports external BGP integration for enterprise growth**.

Multilayer Core Switch Configuration

This configuration will set up VLANs, assign IP addresses, configure trunk/access ports, and prepare the core switch for inter-VLAN routing. The **multilayer core switch** will act as the **default gateway** for all VLANs and handle inter-VLAN routing.

VLAN Creation and IP Address Assignment

These commands create VLANs for each department and assign IP addresses for inter-VLAN routing.

CoreSwitch# configure terminal

! Create VLANs

CoreSwitch(config)# vlan 10

CoreSwitch(config-vlan)# name IT_Department

CoreSwitch(config-vlan)# exit

CoreSwitch(config)# vlan 20

CoreSwitch(config-vlan)# name HR_Department

CoreSwitch(config-vlan)# exit

```
CoreSwitch(config)# vlan 30
CoreSwitch(config-vlan)# name Finance_Department
CoreSwitch(config-vlan)# exit

CoreSwitch(config)# vlan 50
CoreSwitch(config-vlan)# name Server_VLAN
CoreSwitch(config-vlan)# exit

CoreSwitch(config)# vlan 70
CoreSwitch(config-vlan)# name IT_Guest_VLAN
CoreSwitch(config-vlan)# exit

CoreSwitch(config)# vlan 80
CoreSwitch(config-vlan)# name HR_Guest_VLAN
CoreSwitch(config-vlan)# exit

CoreSwitch(config)# vlan 90
CoreSwitch(config-vlan)# name Finance_Guest_VLAN
CoreSwitch(config-vlan)# exit

CoreSwitch(config)# vlan 99
CoreSwitch(config-vlan)# name Management_VLAN
CoreSwitch(config-vlan)# exit
```

Assigning IP Addresses for VLANs (SVI Configuration)

Assign IP addresses to the VLAN interfaces. These IP addresses will act as **default gateways** for devices in their respective VLANs.

```
CoreSwitch(config)# interface vlan 10
CoreSwitch(config-if)# ip address 192.168.10.1 255.255.255.0
CoreSwitch(config-if)# no shutdown
CoreSwitch(config-if)# exit

CoreSwitch(config)# interface vlan 20
CoreSwitch(config-if)# ip address 192.168.20.1 255.255.255.0
CoreSwitch(config-if)# no shutdown
CoreSwitch(config-if)# exit

CoreSwitch(config)# interface vlan 30
CoreSwitch(config-if)# ip address 192.168.30.1 255.255.255.0
CoreSwitch(config-if)# no shutdown
CoreSwitch(config-if)# exit

CoreSwitch(config)# interface vlan 50
CoreSwitch(config-if)# ip address 192.168.50.1 255.255.255.0
CoreSwitch(config-if)# no shutdown
CoreSwitch(config-if)# exit

CoreSwitch(config)# interface vlan 70
CoreSwitch(config-if)# ip address 192.168.70.1 255.255.255.0
CoreSwitch(config-if)# no shutdown
CoreSwitch(config-if)# exit

CoreSwitch(config)# interface vlan 80
CoreSwitch(config-if)# ip address 192.168.80.1 255.255.255.0
CoreSwitch(config-if)# no shutdown
CoreSwitch(config-if)# exit
```

CoreSwitch(config)# interface vlan 90

CoreSwitch(config-if)# ip address 192.168.90.1 255.255.255.0

CoreSwitch(config-if)# no shutdown

CoreSwitch(config-if)# exit

CoreSwitch(config)# interface vlan 99

CoreSwitch(config-if)# ip address 192.168.99.3 255.255.255.0

CoreSwitch(config-if)# no shutdown

CoreSwitch(config-if)# exit

Trunk and Access Port Configuration

Configure ports based on their connections and ensure **VLANs are allowed on trunks** for proper VLAN propagation.

Ports Connected to Servers (Access Ports)

#DHCP Server (Fa0/5) in Server VLAN (VLAN 50)

CoreSwitch(config)# interface fastEthernet 0/5

CoreSwitch(config-if)# switchport mode access

CoreSwitch(config-if)# switchport access vlan 50

CoreSwitch(config-if)# no shutdown

CoreSwitch(config-if)# exit

#DNS Server (Fa0/6) in Server VLAN (VLAN 50)

CoreSwitch(config)# interface fastEthernet 0/6

CoreSwitch(config-if)# switchport mode access

CoreSwitch(config-if)# switchport access vlan 50

CoreSwitch(config-if)# no shutdown

CoreSwitch(config-if)# exit

Ports Connected to Distribution Switches (Trunk Ports)

Allow relevant VLANs for each department on the trunk ports.

#HR Distribution Switch (Fa0/9)

CoreSwitch(config)# interface fastEthernet 0/9

CoreSwitch(config-if)# switchport trunk encapsulation dot1q

CoreSwitch(config-if)# switchport mode trunk

CoreSwitch(config-if)# switchport trunk allowed vlan 10,20,30,50,80,99

CoreSwitch(config-if)# switchport trunk native vlan 99

CoreSwitch(config-if)# no shutdown

CoreSwitch(config-if)# exit

IT Distribution Switch (Fa0/10)

CoreSwitch(config)# interface fastEthernet 0/10

CoreSwitch(config-if)# switchport trunk encapsulation dot1q

CoreSwitch(config-if)# switchport mode trunk

CoreSwitch(config-if)# switchport trunk allowed vlan 10,20,30,50,70,99

CoreSwitch(config-if)# switchport trunk native vlan 99

CoreSwitch(config-if)# no shutdown

CoreSwitch(config-if)# exit

#Finance Distribution Switch (Fa0/12)

CoreSwitch(config)# interface fastEthernet 0/12

CoreSwitch(config-if)# switchport trunk encapsulation dot1q

CoreSwitch(config-if)# switchport mode trunk

CoreSwitch(config-if)# switchport trunk allowed vlan 10,20,30,50,90,99

CoreSwitch(config-if)# switchport trunk native vlan 99

CoreSwitch(config-if)# no shutdown

CoreSwitch(config-if)# exit

Ports Connected to WLC and Router

Wireless LAN Controller (Fa0/24)

CoreSwitch(config)# interface fastEthernet 0/24

CoreSwitch(config-if)# switchport trunk encapsulation dot1q

CoreSwitch(config-if)# switchport mode trunk

CoreSwitch(config-if)# switchport trunk allowed vlan 10,20,30,50,70,80,90,99

CoreSwitch(config-if)# switchport trunk native vlan 99

CoreSwitch(config-if)# no shutdown

CoreSwitch(config-if)# exit

Router for Internet (Gig0/1)

CoreSwitch(config)# interface gigabitEthernet 0/1

CoreSwitch(config-if)# switchport trunk encapsulation dot1q

CoreSwitch(config-if)# switchport mode trunk

CoreSwitch(config-if)# switchport trunk allowed vlan 10,20,30,99

CoreSwitch(config-if)# switchport trunk native vlan 99

CoreSwitch(config-if)# no shutdown

CoreSwitch(config-if)# exit

Enabling Routing on the Core Switch

Since this is a multilayer switch, we need to enable **IP routing** for inter-VLAN communication.

CoreSwitch(config)# ip routing

CoreSwitch(config)# exit

Static Route for Internet Access (Optional)

If the **router (192.168.99.1)** is handling internet access, add a **default route** pointing to it.

CoreSwitch(config)# ip route 0.0.0.0 0.0.0.0 192.168.99.1

CoreSwitch(config)# exit

Saving the Configuration

Make sure to save your configuration to avoid losing settings after a reboot.

CoreSwitch# write memory

Final Check

1. **Verify VLANs:**

   CoreSwitch# show vlan brief
2. **Verify Trunk Ports:**

   CoreSwitch# show interfaces trunk
3. **Verify Routing:**

   CoreSwitch# show ip route

Summary of Actions:

- **VLANs Created:** IT, HR, Finance, Server, Management, IT Guest, HR Guest, Finance Guest.
- **IP Addresses Assigned:** Default gateways for each VLAN.
- **Trunk Ports Configured:** To distribution switches, WLC, and router.
- **Access Ports Configured:** For DHCP and DNS servers.
- **IP Routing Enabled:** For inter-VLAN communication.

- **Default Route Configured:** For internet access via the router.

Distribution Switch Configuration for IT, HR, and Finance Departments

Each distribution switch connects the department's end devices (laptops, APs) and uplinks to the multilayer core switch. We'll configure:

1. **VLAN Assignments**
2. **Trunk Ports (to Core Switch)**
3. **Access Ports (to End Devices like Laptops, APs, Laptops)**
4. **Management IP (VLAN 99)**

A. IT Distribution Switch Configuration

IT_DistSwitch> enable

IT_DistSwitch# configure terminal

IT_DistSwitch(config)# vlan 10

IT_DistSwitch(config-vlan)# name IT_Department

IT_DistSwitch(config-vlan)# exit

IT_DistSwitch(config)# vlan 70

IT_DistSwitch(config-vlan)# name IT_Guest

IT_DistSwitch(config-vlan)# exit

IT_DistSwitch(config)# vlan 99

IT_DistSwitch(config-vlan)# name Management

IT_DistSwitch(config-vlan)# exit

Configure the Trunk Port to Core Switch (Fa0/24)

IT_DistSwitch(config)# interface FastEthernet0/24

IT_DistSwitch(config-if)# description Link_to_CoreSwitch

IT_DistSwitch(config-if)# switchport mode trunk

IT_DistSwitch(config-if)# switchport trunk native vlan 99

IT_DistSwitch(config-if)# switchport trunk allowed vlan 10,70,99

IT_DistSwitch(config-if)# exit

Assign Access Ports to Devices

- **IT Laptop (Fa0/1)**

IT_DistSwitch(config)# interface FastEthernet0/1

IT_DistSwitch(config-if)# description IT_Laptop

IT_DistSwitch(config-if)# switchport mode access

IT_DistSwitch(config-if)# switchport access vlan 10

IT_DistSwitch(config-if)# exit

- **IT Laptop (Fa0/2)**

IT_DistSwitch(config)# interface FastEthernet0/2

IT_DistSwitch(config-if)# description IT_Laptop

IT_DistSwitch(config-if)# switchport mode access

IT_DistSwitch(config-if)# switchport access vlan 10

IT_DistSwitch(config-if)# exit

- **IT Access Point (Fa0/3)**

IT_DistSwitch(config)# interface FastEthernet0/3

IT_DistSwitch(config-if)# description IT_AP

IT_DistSwitch(config-if)# switchport mode access

IT_DistSwitch(config-if)# switchport access vlan 10

IT_DistSwitch(config-if)# exit

- **IT Guest AP (Fa0/4)**

IT_DistSwitch(config)# interface FastEthernet0/4

IT_DistSwitch(config-if)# description IT_Guest_AP

IT_DistSwitch(config-if)# switchport mode access

IT_DistSwitch(config-if)# switchport access vlan 70

IT_DistSwitch(config-if)# exit

Assign Management IP for Switch (VLAN 99)

IT_DistSwitch(config)# interface vlan 99

IT_DistSwitch(config-if)# ip address 192.168.99.4 255.255.255.0

IT_DistSwitch(config-if)# no shutdown

IT_DistSwitch(config-if)# exit

IT_DistSwitch# write memory

B. HR Distribution Switch Configuration

HR_DistSwitch> enable

HR_DistSwitch# configure terminal

HR_DistSwitch(config)# vlan 20

HR_DistSwitch(config-vlan)# name HR_Department

HR_DistSwitch(config-vlan)# exit

HR_DistSwitch(config)# vlan 80

HR_DistSwitch(config-vlan)# name HR_Guest

HR_DistSwitch(config-vlan)# exit

HR_DistSwitch(config)# vlan 99

HR_DistSwitch(config-vlan)# name Management

HR_DistSwitch(config-vlan)# exit

Configure the Trunk Port to Core Switch (Fa0/24)

HR_DistSwitch(config)# interface FastEthernet0/24

HR_DistSwitch(config-if)# description Link_to_CoreSwitch

HR_DistSwitch(config-if)# switchport mode trunk

HR_DistSwitch(config-if)# switchport trunk native vlan 99

HR_DistSwitch(config-if)# switchport trunk allowed vlan 20,80,99

HR_DistSwitch(config-if)# exit

Assign Access Ports to Devices

- **HR Laptop (Fa0/1)**

HR_DistSwitch(config)# interface FastEthernet0/1

HR_DistSwitch(config-if)# description HR_Laptop

HR_DistSwitch(config-if)# switchport mode access

HR_DistSwitch(config-if)# switchport access vlan 20

HR_DistSwitch(config-if)# exit

- **HR Laptop (Fa0/2)**

HR_DistSwitch(config)# interface FastEthernet0/2

HR_DistSwitch(config-if)# description HR_Laptop

HR_DistSwitch(config-if)# switchport mode access

HR_DistSwitch(config-if)# switchport access vlan 20

HR_DistSwitch(config-if)# exit

- **HR Access Point (Fa0/3)**

HR_DistSwitch(config)# interface FastEthernet0/3

HR_DistSwitch(config-if)# description HR_AP

HR_DistSwitch(config-if)# switchport mode access

HR_DistSwitch(config-if)# switchport access vlan 20

HR_DistSwitch(config-if)# exit

- **HR Guest AP (Fa0/4)**

HR_DistSwitch(config)# interface FastEthernet0/4

HR_DistSwitch(config-if)# description HR_Guest_AP

HR_DistSwitch(config-if)# switchport mode access

HR_DistSwitch(config-if)# switchport access vlan 80

HR_DistSwitch(config-if)# exit

Assign Management IP for Switch (VLAN 99)

HR_DistSwitch(config)# interface vlan 99

HR_DistSwitch(config-if)# ip address 192.168.99.5 255.255.255.0

HR_DistSwitch(config-if)# no shutdown

HR_DistSwitch(config-if)# exit

HR_DistSwitch# write memory

C. Finance Distribution Switch Configuration

Finance_DistSwitch> enable

Finance_DistSwitch# configure terminal

Finance_DistSwitch(config)# vlan 30

Finance_DistSwitch(config-vlan)# name Finance_Department

Finance_DistSwitch(config-vlan)# exit

Finance_DistSwitch(config)# vlan 90

Finance_DistSwitch(config-vlan)# name Finance_Guest

Finance_DistSwitch(config-vlan)# exit

Finance_DistSwitch(config)# vlan 99

Finance_DistSwitch(config-vlan)# name Management

Finance_DistSwitch(config-vlan)# exit

Configure the Trunk Port to Core Switch (Fa0/24)

Finance_DistSwitch(config)# interface FastEthernet0/24

Finance_DistSwitch(config-if)# description Link_to_CoreSwitch

Finance_DistSwitch(config-if)# switchport mode trunk

Finance_DistSwitch(config-if)# switchport trunk native vlan 99

Finance_DistSwitch(config-if)# switchport trunk allowed vlan 30,90,99

Finance_DistSwitch(config-if)# exit

Assign Access Ports to Devices

- **Finance Laptop (Fa0/1)**

Finance_DistSwitch(config)# interface FastEthernet0/1

Finance_DistSwitch(config-if)# description Finance_Laptop

Finance_DistSwitch(config-if)# switchport mode access

Finance_DistSwitch(config-if)# switchport access vlan 30

Finance_DistSwitch(config-if)# exit

- **Finance Laptop (Fa0/2)**

Finance_DistSwitch(config)# interface FastEthernet0/2

Finance_DistSwitch(config-if)# description Finance_Laptop

Finance_DistSwitch(config-if)# switchport mode access

Finance_DistSwitch(config-if)# switchport access vlan 30

Finance_DistSwitch(config-if)# exit

- **Finance Access Point (Fa0/3)**

Finance_DistSwitch(config)# interface FastEthernet0/3

Finance_DistSwitch(config-if)# description Finance_AP

Finance_DistSwitch(config-if)# switchport mode access

Finance_DistSwitch(config-if)# switchport access vlan 30

Finance_DistSwitch(config-if)# exit

- **Finance Guest AP (Fa0/4)**

Finance_DistSwitch(config)# interface FastEthernet0/4

Finance_DistSwitch(config-if)# description Finance_Guest_AP

Finance_DistSwitch(config-if)# switchport mode access

Finance_DistSwitch(config-if)# switchport access vlan 90

Finance_DistSwitch(config-if)# exit

Assign Management IP for Switch (VLAN 99)

Finance_DistSwitch(config)# interface vlan 99

Finance_DistSwitch(config-if)# ip address 192.168.99.6 255.255.255.0

Finance_DistSwitch(config-if)# no shutdown

Finance_DistSwitch(config-if)# exit

Finance_DistSwitch# write memory

Verification Commands for All Distribution Switches

- **Check VLANs**

show vlan brief

- **Check Trunking**

show interfaces trunk

- **Check IP Interfaces**

show ip interface brief

Detailed CLI for WLC, DNS, and DHCP Configuration on Multilayer Core Switch

Connecting to the DHCP Server (VLAN 50)

Purpose: Ensure devices in all VLANs can obtain IP addresses from the centralized DHCP server.

Step-by-Step Configuration:

1. **Assign VLAN 50 to the DHCP server port:**

   interface FastEthernet0/5

   description DHCP_Server

   switchport mode access

   switchport access vlan 50

   no shutdown

   exit

2. **Configure DHCP Helper Address on VLAN Interfaces (To Relay DHCP Requests):** This is essential for VLANs that don't directly reside in VLAN 50.

   interface vlan 10

   ip helper-address 192.168.50.100

```
exit

interface vlan 20
ip helper-address 192.168.50.100
exit

interface vlan 30
ip helper-address 192.168.50.100
exit

interface vlan 70
ip helper-address 192.168.50.100
exit

interface vlan 80
ip helper-address 192.168.50.100
exit

interface vlan 90
ip helper-address 192.168.50.100
exit
```

Connecting to the DNS Server (VLAN 50)

Purpose: Allow all VLANs to resolve domain names via the centralized DNS server.

Step-by-Step Configuration:

1. **Assign VLAN 50 to the DNS server port:**

```
interface FastEthernet0/6
description DNS_Server
```

switchport mode access

switchport access vlan 50

no shutdown

exit

Connecting to the WLC (Wireless LAN Controller)

Purpose: Ensure wireless clients across different VLANs (especially Guest VLANs) can connect to the WLC and access the appropriate networks.

Step-by-Step Configuration:

1. **Configure Trunk Port for the WLC Connection (Allowing Guest VLANs):**

   interface FastEthernet0/24

   description Link_to_WLC

   switchport trunk encapsulation dot1q

   switchport mode trunk

   switchport trunk native vlan 99

   switchport trunk allowed vlan 10,20,30,50,70,80,90,99

   no shutdown

   exit

2. **Ensure Management VLAN 99 is used for managing the WLC:**

   interface vlan 99

   ip address 192.168.99.3 255.255.255.0

   no shutdown

   exit

Security for Unused Ports (VLAN 999)

Purpose: Secure unused ports by placing them in an isolated VLAN and shutting them down.

Step-by-Step Configuration:

1. **Assign Unused Ports to VLAN 999 and Shutdown:**

   interface range FastEthernet0/1 - 4, FastEthernet0/8, FastEthernet0/11, FastEthernet0/13 - 23, GigabitEthernet0/2

   switchport mode access

   switchport access vlan 999

   shutdown

   exit

Final Verification Commands

After configuring, verify that everything is working as expected:

1. **Check VLAN Assignment:**
2. show vlan brief
3. **Verify Trunk Ports:**
4. show interfaces trunk
5. **Verify DHCP Relay (Helper) Addresses:**
6. show run | include helper-address
7. **Test DNS and DHCP Functionality from Client Devices (Ping Tests):**

ACL Configuration for VLAN Isolation & Essential Access

Goals:

1. **Isolate VLANs but Allow Essential Services (DNS & DHCP)**
2. **Guest VLANs (70, 80, 90) Have Internet Access Only**
3. **IT (VLAN 10) Has Limited Access to HR (VLAN 20) & Finance (VLAN 30)**
4. **Future-Proof ACLs for RADIUS & Firewall Integration**
5. **Multilayer Core Switch Handles Inter-VLAN Routing; Core Router (2901) Reserved for Internet Routing**

1. ACL for Guest VLANs (VLAN 70, 80, 90)

Objective:

- Block **internal VLAN access** (IT, HR, Finance) but **allow Internet** access through the **Core Router (192.168.99.1)**.
- Allow access to **DNS** and **DHCP servers**.

ACL 100:

access-list 100 permit udp any host 192.168.50.100 eq bootps ! Allow DHCP

access-list 100 permit udp any host 192.168.50.2 eq domain ! Allow DNS

access-list 100 deny ip 192.168.70.0 0.0.0.255 192.168.10.0 0.0.0.255 ! Block IT

access-list 100 deny ip 192.168.70.0 0.0.0.255 192.168.20.0 0.0.0.255 ! Block HR

access-list 100 deny ip 192.168.70.0 0.0.0.255 192.168.30.0 0.0.0.255 ! Block Finance

access-list 100 permit ip any host 192.168.99.1 ! Allow Internet (via Core Router)

access-list 100 deny ip any any ! Deny All Other Traffic

2. ACL for IT Department (VLAN 10)

Objective:

- Allow **limited access** to **HR (VLAN 20)** and **Finance (VLAN 30)** for specific services.
- Allow **full access** to **DNS** and **DHCP**.

ACL 101:

access-list 101 permit udp any host 192.168.50.100 eq bootps ! Allow DHCP

access-list 101 permit udp any host 192.168.50.2 eq domain ! Allow DNS

access-list 101 permit tcp 192.168.10.0 0.0.0.255 192.168.20.0 0.0.0.255 eq 445 ! SMB Access to HR

access-list 101 permit tcp 192.168.10.0 0.0.0.255 192.168.30.0 0.0.0.255 eq 445 ! SMB Access to Finance

access-list 101 permit tcp 192.168.10.0 0.0.0.255 192.168.20.0 0.0.0.255 eq smtp ! Email to HR

access-list 101 deny ip 192.168.10.0 0.0.0.255 192.168.20.0 0.0.0.255 ! Block Other HR Access

access-list 101 deny ip 192.168.10.0 0.0.0.255 192.168.30.0 0.0.0.255 ! Block Other Finance Access

access-list 101 permit ip any any ! Allow All Other Traffic

3. ACL for Management VLAN (VLAN 99)

Objective:

- Allow **management devices** to access **all VLANs** for network administration.
- This includes **WLC**, **Admin PCs**, and **future RADIUS** configurations.

ACL 102:

access-list 102 permit ip 192.168.99.0 0.0.0.255 any ! Allow Management Devices Full Access

4. Apply ACLs to VLAN Interfaces

Guest VLANs (70, 80, 90):

interface vlan 70

ip access-group 100 in

interface vlan 80

ip access-group 100 in

interface vlan 90

ip access-group 100 in

IT Department (VLAN 10):

interface vlan 10

ip access-group 101 in

Management VLAN (VLAN 99):

interface vlan 99

ip access-group 102 in

5. Verification Commands

1. **Check ACL Application:**

show run interface vlan 70

show run interface vlan 10

show run interface vlan 99

2. **Test Connectivity:**

- **From Guest VLAN:** Try to ping **internal VLANs (IT, HR, Finance)** – should **fail**. Test **Internet access** – should **work**.
- **From IT VLAN:** Test **SMB access** to HR and Finance – should **work**. Any other access – should **fail**.
- **From Management VLAN:** Should have **full access** across all VLANs.

Disable Unused Ports

Since **Fa0/2 and Fa0/3** are used for **APs**, and **Fa0/24** is the **trunk port** to the core switch, **disable all other ports (Fa0/4 - Fa0/23)**:

DistSwitch(config)# interface range Fa0/4-23

DistSwitch(config-if-range)# switchport mode access

DistSwitch(config-if-range)# switchport access vlan 999

DistSwitch(config-if-range)# shutdown

DistSwitch(config-if-range)# spanning-tree bpduguard enable

DistSwitch(config-if-range)# exit

VLAN 999 (Blackhole VLAN) must be created first

DistSwitch(config)# vlan 999

DistSwitch(config-vlan)# name Unused_Ports

DistSwitch(config-vlan)# exit

Enable Port Security on Active Ports

Apply **Port Security** to AP and Guest AP connections:

DistSwitch(config)# interface Fa0/2

DistSwitch(config-if)# switchport mode access

DistSwitch(config-if)# switchport access vlan 10 # Change for HR/Finance

DistSwitch(config-if)# switchport port-security

DistSwitch(config-if)# switchport port-security maximum 10

DistSwitch(config-if)# switchport port-security violation shutdown

DistSwitch(config-if)# exit

DistSwitch(config)# interface Fa0/3

DistSwitch(config-if)# switchport mode access

DistSwitch(config-if)# switchport access vlan 70 # Change for HR/Finance

DistSwitch(config-if)# switchport port-security

DistSwitch(config-if)# switchport port-security maximum 10

DistSwitch(config-if)# switchport port-security violation restrict

DistSwitch(config-if)# exit

Explanation:

- **Fa0/2 (AP port)** → Allows **10 MAC addresses**, if exceeded, it **shuts down the port**.
- **Fa0/3 (Guest AP port)** → Allows **10 MAC addresses**, if exceeded, it **only restricts access** (not shutdown).

Enable BPDU Guard on Access Ports

BPDU Guard prevents **unauthorized switches** from connecting.

DistSwitch(config)# interface range Fa0/2-3

DistSwitch(config-if-range)# spanning-tree portfast

DistSwitch(config-if-range)# spanning-tree bpduguard enable

DistSwitch(config-if-range)# exit

Trunk ports (Fa0/24) should NOT have BPDU Guard enabled.

Enable DHCP Snooping

Enable DHCP Snooping on the Switch

DistSwitch(config)# ip dhcp snooping

DistSwitch(config)# ip dhcp snooping vlan 10 70 # Include VLANs for other departments

DistSwitch(config)# exit

Set Trusted Interfaces:

- **Fa0/2 (AP Port) & Fa0/3 (Guest AP Port) → Trusted**
- **Fa0/24 (Trunk to Core Switch) → Trusted**

DistSwitch(config)# interface Fa0/2

DistSwitch(config-if)# ip dhcp snooping trust

DistSwitch(config-if)# exit

DistSwitch(config)# interface Fa0/3

DistSwitch(config-if)# ip dhcp snooping trust

DistSwitch(config-if)# exit

DistSwitch(config)# interface Fa0/24

DistSwitch(config-if)# ip dhcp snooping trust

DistSwitch(config-if)# exit

Access ports (unused ports) should NOT be trusted to prevent **Rogue DHCP attacks**.

Configure ASA Firewall

Step 1: Configure the Inside Interface

ciscoasa(config)# interface GigabitEthernet1/1

ciscoasa(config-if)# nameif INSIDE

ciscoasa(config-if)# security-level 100

ciscoasa(config-if)# ip address 192.168.99.11 255.255.255.0

ciscoasa(config-if)# no shutdown

ciscoasa(config-if)# exit

Connects firewall to the Multilayer Core Switch.

Step 2: Configure the Outside Interface

ciscoasa(config)# interface GigabitEthernet1/2

ciscoasa(config-if)# nameif OUTSIDE

ciscoasa(config-if)# security-level 0

ciscoasa(config-if)# ip address 192.168.200.2 255.255.255.252

ciscoasa(config-if)# no shutdown

ciscoasa(config-if)# exit

Connects firewall to the Core Router.

Configure Core Router

Since the **Core Router** connects to the firewall, it must have a matching subnet.

CoreRouter(config)# interface GigabitEthernet0/0

CoreRouter(config-if)# ip address 192.168.200.1 255.255.255.252

CoreRouter(config-if)# no shutdown

CoreRouter(config-if)# exit

Step 3: Add a Default Route on ASA to the Core Router

ciscoasa(config)# route OUTSIDE 0.0.0.0 0.0.0.0 192.168.200.1

Allows ASA to forward internet-bound traffic to the Core Router.

Configure Multilayer Core Switch

Since **all VLANs are configured here**, update its default route to point to the ASA firewall:

CoreSwitch(config)# ip route 0.0.0.0 0.0.0.0 192.168.99.11

This ensures that traffic flows through the firewall before reaching the Core Router.

Configure Firewall Access Control Policies

Now, configure the ASA firewall policies for **Inter-VLAN Blocking, Guest VLAN Restrictions, and Management Access.**

Step 1: Block Inter-VLAN Communication

ciscoasa(config)# access-list BLOCK_INTERVLAN extended deny ip 192.168.10.0 255.255.255.0 192.168.20.0 255.255.255.0

ciscoasa(config)# access-list BLOCK_INTERVLAN extended deny ip 192.168.10.0 255.255.255.0 192.168.30.0 255.255.255.0

ciscoasa(config)# access-list BLOCK_INTERVLAN extended deny ip 192.168.20.0 255.255.255.0 192.168.30.0 255.255.255.0

ciscoasa(config)# access-list BLOCK_INTERVLAN extended permit ip any any

ciscoasa(config)# access-group BLOCK_INTERVLAN in interface INSIDE

Prevents departments from communicating with each other.

Step 2: Restrict Guest VLANs

ciscoasa(config)# access-list GUEST_POLICY extended deny ip 192.168.70.0 255.255.255.0 any

ciscoasa(config)# access-list GUEST_POLICY extended deny ip 192.168.80.0 255.255.255.0 any

ciscoasa(config)# access-list GUEST_POLICY extended deny ip 192.168.90.0 255.255.255.0 any

ciscoasa(config)# access-list GUEST_POLICY extended permit ip any any

ciscoasa(config)# access-group GUEST_POLICY in interface INSIDE

Guests can only access the internet, not internal VLANs.

Step 3: Restrict Management Access

ciscoasa(config)# access-list ALLOW_MGMT extended permit ip 192.168.10.0 255.255.255.0 192.168.99.0 255.255.255.0

ciscoasa(config)# access-list ALLOW_MGMT extended deny ip any 192.168.99.0 255.255.255.0

ciscoasa(config)# access-group ALLOW_MGMT in interface INSIDE

Only IT VLAN can access the Management VLAN (99).

Step 4: Block Unwanted Traffic (P2P, Torrents, etc.)

ciscoasa(config)# access-list BLOCK_BAD_TRAFFIC extended deny tcp any any eq 6881

ciscoasa(config)# access-list BLOCK_BAD_TRAFFIC extended deny tcp any any eq 135

ciscoasa(config)# access-list BLOCK_BAD_TRAFFIC extended deny tcp any any eq 137

ciscoasa(config)# access-list BLOCK_BAD_TRAFFIC extended permit ip any any

ciscoasa(config)# access-group BLOCK_BAD_TRAFFIC in interface INSIDE

Prevents malicious traffic like P2P file sharing.

Enable NAT for Internet Access

Configure NAT so internal devices can access external networks:

ciscoasa(config)# object network INTERNAL-NETWORK

ciscoasa(config-network-object)# subnet 192.168.10.0 255.255.255.0

ciscoasa(config-network-object)# nat (INSIDE,OUTSIDE) dynamic interface

ciscoasa(config-network-object)# exit

This allows VLANs to communicate with the internet via NAT.

Verify Configuration

Check Routing

ciscoasa# show route

CoreRouter# show ip route

Check Access Control

ciscoasa# show access-list

Check NAT

ciscoasa# show nat

Check Interface Status

ciscoasa# show interface ip brief

Summary

1. **Firewall Placement:**
    - **Gi1/1 (INSIDE) → Multilayer Core Switch (192.168.99.11)**
    - **Gi1/2 (OUTSIDE) → Core Router (192.168.200.2)**
2. **Routing:**
    - **Multilayer Core Switch** → Default route to 192.168.99.11
    - **ASA Firewall** → Default route to 192.168.200.1
    - **Core Router** → Default route to ISP
3. **Access Control:**
    - **Inter-VLAN restrictions**
    - **Guest VLAN isolation**
    - **Management VLAN access only for IT**
    - **Blocking of malicious traffic**
4. **NAT & Internet Access:**
    - Internal network translated for internet access.

Your **next-hop IP address** should be the IP of the **ISP router** that connects your core router to the Internet.

Step 1: Identify the ISP Router's IP

- Your **core router (Gig0/0) has IP: 192.168.200.1/30**.
- A **/30 subnet** has **only two usable IPs**:
    - **192.168.200.1** (Assigned to your core router)
    - **192.168.200.2** (Should be the ISP router's IP)

So, your **ISP router's next-hop IP should be 192.168.200.2**.

Step 2: Set the Default Route on the Core Router

Run this command on your **core router**:

Router(config)# ip route 0.0.0.0 0.0.0.0 192.168.200.2

This tells the router: **"Send all unknown traffic to 192.168.200.2"** (ISP router).

Step 3: Verify the Default Route

Run:R

Router# show ip route

You should see something like:

S* 0.0.0.0/0 [1/0] via 192.168.200.2

This confirms the default route is correctly set.

Step 4: Test External Connectivity

1**Ping the ISP router** (If it's up and responding):

Router# ping 192.168.200.2

- If **successful**, move to the next step.
- If **failing**, check if the ISP router interface is up.

2**Try pinging a public IP** (like Google's 8.8.8.8):

Router# ping 8.8.8.8

- If **this fails**, check if NAT is configured on your **firewall**.
- You may also need to **allow ICMP traffic on your firewall**.

Radius

RADIUS Configuration (Packet Tracer-Compatible)

Since **Packet Tracer has limited AAA and RADIUS support**, I have **revised all CLI commands** to ensure they work within **Packet Tracer's capabilities** while securing the topology.

Step 1: Configure Core Switch (Remove Port 4 from VLAN 999 & Assign to VLAN 50)

CoreSwitch# configure terminal

CoreSwitch(config)# interface Fa0/4

CoreSwitch(config-if)# no shutdown

CoreSwitch(config-if)# switchport mode access

CoreSwitch(config-if)# switchport access vlan 99

Use the VLAN where RADIUS server is located

CoreSwitch(config-if)# description RADIUS Server Connection

CoreSwitch(config-if)# exit

CoreSwitch(config)# write memory

Port 4 is now assigned to VLAN 50 (Server VLAN) instead of VLAN 999 (Blackhole VLAN).

Step 2: Configure RADIUS Server (192.168.50.3)

On Server PT in Packet Tracer

1. **Go to Server PT → Click "Services" Tab → Select "AAA (RADIUS)"**

2. **Enable RADIUS Service.**
3. **Add a New User:**
    - **Username:** admin
    - **Password:** password123
    - **User Type:** Administrator
    - **Click "Add" and Save Changes.**
4. **Add RADIUS Clients (Switches, WLC, Firewall):**
    - **Client Name:** CoreSwitch
    - **Client IP:** 192.168.99.3
    - **Secret:** radiuspass
    - **Click "Add" and Save Changes.**
    - **Repeat for:**
        - **IT Distribution Switch** (192.168.99.4)
        - **HR Distribution Switch** (192.168.99.5)
        - **Finance Distribution Switch** (192.168.99.6)
        - **Wireless LAN Controller** (192.168.50.10)
        - **Firewall ASA** (192.168.99.11)
5. **Save Configuration.**

The RADIUS Server is now configured and ready to authenticate network devices.

Step 3: Configure Core Switch for RADIUS Authentication

```
CoreSwitch(config)# aaa new-model
CoreSwitch(config)# aaa authentication login default group radius local
CoreSwitch(config)# aaa authorization exec default group radius local
CoreSwitch(config)# radius-server host 192.168.99.19 auth-port 1645 key radiuspass
CoreSwitch(config)# radius-server timeout 5
CoreSwitch(config)# radius-server retransmit 3
CoreSwitch(config)# exit
```

CoreSwitch(config)# write memory

Core Switch now uses RADIUS for SSH authentication and falls back to local authentication if RADIUS fails.

Step 4: Configure IT, HR, Finance Distribution Switches

(192.168.99.4, 192.168.99.5, 192.168.99.6)

IT-DistSwitch# configure terminal

IT-DistSwitch(config)# aaa new-model

IT-DistSwitch(config)# radius-server host 192.168.50.3 key radiuspass

IT-DistSwitch(config)# aaa authentication login default group radius local

IT-DistSwitch(config)# line vty 0 4

IT-DistSwitch(config-line)# login authentication default

IT-DistSwitch(config-line)# transport input ssh

IT-DistSwitch(config-line)# exit

IT-DistSwitch(config)# write memory

Repeat the same for HR-DistSwitch & Finance-DistSwitch.

Step 5: Configure RADIUS on Firewall (ASA)

ciscoasa# configure terminal

ciscoasa(config)# aaa authentication ssh console LOCAL

ciscoasa(config)# aaa authentication telnet console LOCAL

ciscoasa(config)# write memory

Firewall will now authenticate SSH logins using RADIUS first.

Configure RADIUS on Wireless LAN Controller (WLC)

Configuring RADIUS on Wireless LAN Controller (WLC) via Web Interface in Packet Tracer

Since Packet Tracer does not provide direct CLI access to the **Wireless LAN Controller (WLC)**, we need to **configure RADIUS authentication via the Web GUI**.

Step 1: Access WLC Web Interface

1. **Connect a PC to the WLC** via a wired connection.
2. Open a web browser (on the connected PC).
3. **Enter the IP address of the WLC** in the browser's address bar.
    - Example: If the **WLC IP address is 192.168.50.10**, type:
    - http://192.168.50.10
4. **Login to the WLC Web Interface** using:
    - **Username:** admin
    - **Password:** admin

Step 2: Configure RADIUS Authentication

Step 1: Fill in the RADIUS Server Details

- **Server Index (Priority): 1** ***(Keep as default if this is the primary RADIUS server)***

- **Server IP Address: 192.168.50.3** ***(This is the IP of your RADIUS Server)***
- **Shared Secret Format: ASCII** ***(Keep as default)***
- **Shared Secret: radiuspass** ***(Enter the same secret key configured on the RADIUS server)***
- **Confirm Shared Secret: radiuspass** ***(Re-enter the same key)***
- **Port Number: 1812** ***(Default RADIUS authentication port)***
- **Server Status: Enabled**
- **Support for CoA: Disabled** ***(No need for Change of Authorization in this setup)***
- **Server Timeout: 2** ***(Keep as default, but can be increased if authentication issues occur)***
- **Network User: ✅ Check this option** ***(This allows wireless clients to authenticate using RADIUS)***
- **Management: ❌ Leave unchecked** ***(This is for WLC management authentication via RADIUS, not needed now)***
- **Management Retransmit Timeout: 2** ***(Keep as default)***
- **IPSec: ❌ Leave unchecked** ***(Not required in Packet Tracer setup)***

Step 2: Apply and Save

1. **Click the Apply button.**
2. **Click Save Configuration at the top-right to make the changes persistent.**

Step 3: Verify RADIUS Authentication

1. **Go to the "WLANs" tab and edit your Wi-Fi SSID (e.g., SecureWiFi).**
2. **Navigate to Security Settings and enable RADIUS Authentication.**
3. **Select the RADIUS Server (192.168.50.3) from the list.**
4. **Click Apply and Save Configuration.**
5. **Test by connecting a wireless laptop to Wi-Fi:**
    - **When prompted, enter the RADIUS username & password from the RADIUS server.**
    - **If authentication succeeds, RADIUS is working correctly.**

Step 7: Testing RADIUS Authentication

Verify SSH Authentication via RADIUS

On a PC:

ssh -l admin 192.168.99.3

- **Enter password123 → Should authenticate via RADIUS.**
- **If RADIUS fails, it should fall back to the local password.**

Verify RADIUS Logs

show aaa sessions

show radius statistics

Verify Wireless Authentication

1. **Connect a Laptop to Wi-Fi.**
2. **Enter the username admin and password password123.**
3. **If it connects successfully, RADIUS authentication is working.**

BGP

Simulating an External Attack Using BGP

1. **Connect a new router to the Core Router** (simulating an ISP or attacker).
2. **Enable BGP on both routers**.
3. **Attach a PC to the new router** (simulating an external attacker).
4. **Test attacks** (Ping, SSH, and Packet Capture).

Step 1: Add the External Router & Laptop

1. **Drag & Drop**:
    - **1 New Router** (AttackerRouter)
    - **1 Laptop** (AttackerPC)
2. **Connections**:
    - **Core Router [Gig0/1] ⟷ [Gig0/0] New External Router**
    - **New External Router [Gig0/1] ⟷ Attacker Laptop (FastEthernet0)**

Step 2: Configure BGP on the New External Router

On AttackerRouter

Router(config)# hostname AttackerRouter

AttackerRouter(config)# interface GigabitEthernet0/0

AttackerRouter(config-if)# ip address 192.168.201.2 255.255.255.252

AttackerRouter(config-if)# no shutdown

AttackerRouter(config-if)# exit

AttackerRouter(config)# interface GigabitEthernet0/1

AttackerRouter(config-if)# ip address 203.0.113.1 255.255.255.0

AttackerRouter(config-if)# no shutdown

AttackerRouter(config-if)# exit

AttackerRouter(config)# router bgp 65002

AttackerRouter(config-router)# neighbor 192.168.201.1 remote-as 65001

AttackerRouter(config-router)# network 203.0.113.0 mask 255.255.255.0

AttackerRouter(config-router)# exit

AttackerRouter(config)# ip route 0.0.0.0 0.0.0.0 192.168.201.1

AttackerRouter(config)# write memory

Step 3: Configure BGP on Core Router

On Core Router

Router(config)# interface GigabitEthernet0/1

Router(config-if)# ip address 192.168.201.1 255.255.255.252

Router(config-if)# no shutdown

Router(config-if)# exit

Router(config)# router bgp 65001

Router(config-router)# neighbor 192.168.201.2 remote-as 65002

Router(config-router)# network 192.168.99.0 mask 255.255.255.0

Router(config-router)# exit

Router(config)# write memory

Step 4: Configure the Attacker Laptop

1. **Click on the Laptop → Desktop → IP Configuration**
    - **IP Address:** 203.0.113.2
    - **Subnet Mask:** 255.255.255.0
    - **Default Gateway:** 203.0.113.1

Step 5: Verify BGP Configuration

Check BGP Neighbor Relationship

On **Core Router**:

Router# show ip bgp summary

Expected Output:

- Should show **BGP neighbor** (192.168.201.2) in **Established state**.

On **AttackerRouter**:

AttackerRouter# show ip bgp summary

Expected Output:

- Should show **BGP neighbor** (192.168.201.1) in **Established state**.

Step 6: Simulating an Attack

Ping Internal Network

From the **attacker's laptop**, open the command prompt and try:

ping 192.168.99.3 (Multilayer Core Switch)

ping 192.168.50.3 (RADIUS Server)

- **Expected:** If firewall & ACLs are working, pings should fail.
- **If pings succeed:** Your firewall **is not blocking** external traffic.

Attempt SSH Attack

ssh -l admin 192.168.99.3

- **Expected:** Should be blocked unless **RADIUS misconfiguration exists**.

Packet Capture (Simulation Mode)

1. **Switch to Simulation Mode in Packet Tracer**.
2. **Capture traffic** between the external router and your internal network.
3. **Look for unauthorized packets**.

Updated BGP Security Configuration for Packet Tracer

Since **distribute-list is not supported**, we will use **static routing and ACLs on the firewall** to block unauthorized traffic.

Step 1: Configure Basic BGP on Core Router

Router(config)# router bgp 65001

Router(config-router)# neighbor 192.168.201.2 remote-as 65002

Router(config-router)# exit

Router(config)# write memory

This ensures BGP peering is established **without filtering** (since Packet Tracer does not support filtering).

Step 2: Block Outbound Internal Network Advertisement (Using ACL on the Firewall)

Since BGP filtering is **not available in Packet Tracer**, we **block advertisements using the firewall ACL**.

ciscoasa(config)# access-list BLOCK_BGP_TRAFFIC extended deny ip 192.168.99.0 255.255.255.0 any

ciscoasa(config)# access-group BLOCK_BGP_TRAFFIC in interface OUTSIDE

ciscoasa(config)# write memory

This prevents internal routes (192.168.99.0/24) from being advertised to the attacker router.

Step 3: Block Unauthorized BGP Traffic

To prevent an **attacker router from injecting fake routes**, block **all BGP (TCP 179) traffic from the attacker**:

ciscoasa(config)# access-list BLOCK_ATTACK extended deny tcp 192.168.201.0 255.255.255.252 any eq 179

ciscoasa(config)# access-group BLOCK_ATTACK in interface OUTSIDE

ciscoasa(config)# write memory

This **blocks all BGP advertisements from the attacker router**, preventing route hijacking.

Security Outcome

✓ The attacker router will NOT learn the internal network (192.168.99.0/24).
✓ Fake BGP advertisements from the attacker are blocked by the firewall.
✓ Your core router does NOT leak internal routes due to the firewall ACL.

OSPF

Step-by-Step Guide to Implement OSPF in Your Packet Tracer Topology

OSPF (Open Shortest Path First) is the best choice for dynamic routing in topology. Since **Packet Tracer does not support EIGRP on all devices**, we will use **OSPF** as the **Interior Gateway Protocol (IGP)** to dynamically route traffic between your **Multilayer Core Switch, Firewall, and Core Router**.

Why Use OSPF Instead of EIGRP?

1. **Packet Tracer Limitation** – EIGRP is Cisco proprietary, and Packet Tracer does not support it on **ASA Firewalls** or some other devices.
2. **Scalability** – OSPF is an open standard, works in large networks, and supports **multi-area configurations**.
3. **Link-State Protocol** – Provides faster convergence and better routing decisions than EIGRP in mixed-vendor environments.

Overview of OSPF in Network

Device	OSPF Area	Interfaces	Network Advertised
Multilayer Core Switch	Area 0 (Backbone)	VLAN Interfaces	192.168.10.0/24, 192.168.20.0/24, 192.168.30.0/24, 192.168.50.0/24, 192.168.99.0/24
Firewall (ASA)	Area 0	Inside (192.168.99.11) & Outside (192.168.200.2)	192.168.99.0/24, 192.168.200.0/30

Device	OSPF Area	Interfaces	Network Advertised
Core Router	Area 0	Gi0/0 (192.168.200.1)	Default Route (0.0.0.0/0)

Step 1: Enable OSPF on the Multilayer Core Switch

Assign OSPF to VLAN Interfaces (Backbone Area 0)

CoreSwitch(config)# router ospf 1

CoreSwitch(config-router)# router-id 2.1.2.1

CoreSwitch(config-router)# network 192.168.10.0 0.0.0.255 area 0

CoreSwitch(config-router)# network 192.168.20.0 0.0.0.255 area 0

CoreSwitch(config-router)# network 192.168.30.0 0.0.0.255 area 0

CoreSwitch(config-router)# network 192.168.50.0 0.0.0.255 area 0

CoreSwitch(config-router)# network 192.168.99.0 0.0.0.255 area 0

CoreSwitch(config-router)# exit

CoreSwitch(config)# write memory

This ensures OSPF is enabled and advertising all VLANs for inter-VLAN routing.

Step 2: Enable OSPF on the Firewall (ASA)

Since **Packet Tracer's ASA Firewall does not support advanced OSPF features**, we will configure it in a **basic setup**.

ciscoasa(config)# router ospf 1

ciscoasa(config-router)# network 192.168.99.0 255.255.255.0 area 0

ciscoasa(config-router)# network 192.168.200.0 255.255.255.252 area 0

ciscoasa(config-router)# exit

ciscoasa(config)# write memory

Now the firewall participates in OSPF and advertises its networks.

Step 3: Enable OSPF on the Core Router

CoreRouter(config)# router ospf 1

CoreRouter(config-router)# router-id 3.3.3.3

CoreRouter(config-router)# network 192.168.200.0 0.0.0.3 area 0

CoreRouter(config-router)# default-information originate

CoreRouter(config-router)# exit

CoreRouter(config)# write memory

This advertises the default route (0.0.0.0/0) to the internal OSPF network, allowing all internal devices to access the internet.

Step 4: Verify OSPF Configuration

On Multilayer Core Switch

CoreSwitch# show ip ospf neighbor

CoreSwitch# show ip route ospf

This ensures OSPF neighbors are established and routes are learned.

On ASA Firewall

ciscoasa# show ospf neighbor

ciscoasa# show route ospf

This verifies that OSPF is working on the firewall.

On Core Router

CoreRouter# show ip ospf neighbor

CoreRouter# show ip route ospf

Ensures the router is advertising the default route via OSPF.

Step 5: Test OSPF Connectivity

1. **Ping from IT Department PC (VLAN 10) to Finance PC (VLAN 30)**
    - **Expected:** Success (OSPF enables inter-VLAN routing)
2. ping 192.168.30.10
3. **Ping from IT Department PC (VLAN 10) to the Internet (e.g., 8.8.8.8)**
    - **Expected:** Success if NAT is properly configured on the firewall
4. ping 8.8.8.8
5. **Check Routing Table on Any PC in VLAN 10**
6. tracert 8.8.8.8
    - **Expected Path:**
        - PC → Core Switch → Firewall → Core Router → ISP

Summary of OSPF Implementation

Device	OSPF Configuration	Purpose
Multilayer Core Switch	OSPF Area 0, advertises VLAN networks	Enables inter-VLAN routing
ASA Firewall	OSPF Area 0, advertises 192.168.99.0/24 and 192.168.200.0/30	Connects LAN to Core Router
Core Router	OSPF Area 0, advertises 192.168.200.0/30, distributes default route	Provides internet access

---

Step-by-Step Guide to Adding & Configuring a Redundant Core Switch with HSRP for High Availability

Objective

✓ Add a new redundant Core Switch (CoreSwitch-2)
✓ Configure HSRP for failover & redundancy
✓ Ensure proper VLAN trunking & communication
✓ Test & verify automatic failover between CoreSwitch-1 & CoreSwitch-2

Physical Setup in Packet Tracer

Drag and place a new Multilayer Switch (3650 or 3560)

- Name it CoreSwitch-2
  Connect Gig0/2 of CoreSwitch-1 to Gig0/2 of CoreSwitch-2
- Use a Crossover Cable
- This trunk link will be used for HSRP communication & VLAN trunking

Why Use Gig0/2?
✓ High-speed Gigabit link
✓ Ensures VLAN traffic is properly passed between switches
✓ Supports HSRP failover communication

Configure VLANs on CoreSwitch-2

Before enabling HSRP, ensure CoreSwitch-2 has the same VLANs as CoreSwitch-1.

Step 1: Create VLANs on CoreSwitch-2

Run the following commands on CoreSwitch-2:

```
CoreSwitch-2# configure terminal
CoreSwitch-2(config)# vlan 10
CoreSwitch-2(config-vlan)# name IT_Department
CoreSwitch-2(config-vlan)# exit

CoreSwitch-2(config)# vlan 20
CoreSwitch-2(config-vlan)# name HR_Department
CoreSwitch-2(config-vlan)# exit

CoreSwitch-2(config)# vlan 30
CoreSwitch-2(config-vlan)# name Finance_Department
CoreSwitch-2(config-vlan)# exit

CoreSwitch-2(config)# vlan 50
CoreSwitch-2(config-vlan)# name Server_VLAN
CoreSwitch-2(config-vlan)# exit

CoreSwitch-2(config)# vlan 70
CoreSwitch-2(config-vlan)# name IT_Guest_VLAN
CoreSwitch-2(config-vlan)# exit

CoreSwitch-2(config)# vlan 80
CoreSwitch-2(config-vlan)# name HR_Guest_VLAN
CoreSwitch-2(config-vlan)# exit

CoreSwitch-2(config)# vlan 90
CoreSwitch-2(config-vlan)# name Finance_Guest_VLAN
```

CoreSwitch-2(config-vlan)# exit

CoreSwitch-2(config)# vlan 99

CoreSwitch-2(config-vlan)# name Management_VLAN

CoreSwitch-2(config-vlan)# exit

CoreSwitch-2(config)# write memory

Now, VLANs match between CoreSwitch-1 & CoreSwitch-2.

Configure Trunking on Gig0/2

Ensure VLAN traffic is properly passed between both switches.

Step 2: Configure Trunk on CoreSwitch-1

CoreSwitch-1# configure terminal

CoreSwitch-1(config)# interface gigabitEthernet 0/2

CoreSwitch-1(config-if)# switchport trunk encapsulation dot1q

CoreSwitch-1(config-if)# switchport mode trunk

CoreSwitch-1(config-if)# switchport trunk native vlan 99

CoreSwitch-1(config-if)# switchport trunk allowed vlan 10,20,30,50,70,80,90,99

CoreSwitch-1(config-if)# no shutdown

CoreSwitch-1(config-if)# exit

CoreSwitch-1(config)# write memory

Step 3: Configure Trunk on CoreSwitch-2

CoreSwitch-2# configure terminal

CoreSwitch-2(config)# interface gigabitEthernet 0/2

CoreSwitch-2(config-if)# switchport trunk encapsulation dot1q

CoreSwitch-2(config-if)# switchport mode trunk

CoreSwitch-2(config-if)# switchport trunk native vlan 99

CoreSwitch-2(config-if)# switchport trunk allowed vlan 10,20,30,50,70,80,90,99

CoreSwitch-2(config-if)# no shutdown

CoreSwitch-2(config-if)# exit

CoreSwitch-2(config)# write memory

Now both switches can properly communicate using VLAN trunking.

Configure HSRP for Redundancy

Step 4: Configure HSRP on CoreSwitch-1 (Primary)

Run the following for each VLAN:

CoreSwitch-1# configure terminal

CoreSwitch-1(config)# interface vlan 10

CoreSwitch-1(config-if)# ip address 192.168.10.3 255.255.255.0

CoreSwitch-1(config-if)# standby 10 ip 192.168.10.1

CoreSwitch-1(config-if)# standby 10 priority 110

CoreSwitch-1(config-if)# standby 10 preempt

CoreSwitch-1(config-if)# exit

CoreSwitch-1(config)# interface vlan 20

CoreSwitch-1(config-if)# ip address 192.168.20.3 255.255.255.0

CoreSwitch-1(config-if)# standby 20 ip 192.168.20.1

CoreSwitch-1(config-if)# standby 20 priority 110

CoreSwitch-1(config-if)# standby 20 preempt

CoreSwitch-1(config-if)# exit

CoreSwitch-1(config)# interface vlan 30

CoreSwitch-1(config-if)# ip address 192.168.30.3 255.255.255.0

CoreSwitch-1(config-if)# standby 30 ip 192.168.30.1

CoreSwitch-1(config-if)# standby 30 priority 110

CoreSwitch-1(config-if)# standby 30 preempt

CoreSwitch-1(config-if)# exit

CoreSwitch-1(config)# interface vlan 50

CoreSwitch-1(config-if)# ip address 192.168.50.5 255.255.255.0

CoreSwitch-1(config-if)# standby 50 ip 192.168.50.1

CoreSwitch-1(config-if)# standby 50 priority 110

CoreSwitch-1(config-if)# standby 50 preempt

CoreSwitch-1(config-if)# exit

CoreSwitch-1(config)# interface vlan 99

CoreSwitch-1(config-if)# ip address 192.168.99.8 255.255.255.0

CoreSwitch-1(config-if)# standby 99 ip 192.168.99.1

CoreSwitch-1(config-if)# standby 99 priority 110

CoreSwitch-1(config-if)# standby 99 preempt

CoreSwitch-1(config-if)# exit

CoreSwitch-1(config)# write memory

Now CoreSwitch-1 is the Active HSRP router for all VLANs.

Step 5: Configure HSRP on CoreSwitch-2 (Standby)

CoreSwitch-2# configure terminal

CoreSwitch-2(config)# interface vlan 10

CoreSwitch-2(config-if)# ip address 192.168.10.4 255.255.255.0

CoreSwitch-2(config-if)# standby 10 ip 192.168.10.1

CoreSwitch-2(config-if)# standby 10 priority 90

CoreSwitch-2(config-if)# standby 10 preempt

```
CoreSwitch-2(config-if)# exit

CoreSwitch-2(config)# interface vlan 20
CoreSwitch-2(config-if)# ip address 192.168.20.4 255.255.255.0
CoreSwitch-2(config-if)# standby 20 ip 192.168.20.1
CoreSwitch-2(config-if)# standby 20 priority 90
CoreSwitch-2(config-if)# standby 20 preempt
CoreSwitch-2(config-if)# exit

CoreSwitch-2(config)# interface vlan 30
CoreSwitch-2(config-if)# ip address 192.168.30.4 255.255.255.0
CoreSwitch-2(config-if)# standby 30 ip 192.168.30.1
CoreSwitch-2(config-if)# standby 30 priority 90
CoreSwitch-2(config-if)# standby 30 preempt
CoreSwitch-2(config-if)# exit

CoreSwitch-2(config)# interface vlan 50
CoreSwitch-2(config-if)# ip address 192.168.50.6 255.255.255.0
CoreSwitch-2(config-if)# standby 50 ip 192.168.50.1
CoreSwitch-2(config-if)# standby 50 priority 90
CoreSwitch-2(config-if)# standby 50 preempt
CoreSwitch-2(config-if)# exit

CoreSwitch-2(config)# interface vlan 99
CoreSwitch-2(config-if)# ip address 192.168.99.9 255.255.255.0
CoreSwitch-2(config-if)# standby 99 ip 192.168.99.1
CoreSwitch-2(config-if)# standby 99 priority 90
CoreSwitch-2(config-if)# standby 99 preempt
CoreSwitch-2(config-if)# exit
```

CoreSwitch-2(config)# write memory

Now CoreSwitch-2 is the Standby HSRP router for all VLANs.

Verification & Testing

Step 6: Verify HSRP Status

Run on both switches:

show standby brief

Expected Output:

- CoreSwitch-1 = Active
- CoreSwitch-2 = Standby

Step 7: Simulate a Failure

On CoreSwitch-1, shut down Gig0/2:

CoreSwitch-1(config)# interface gigabitEthernet 0/2

CoreSwitch-1(config-if)# shutdown

CoreSwitch-2 should now become Active.

Config of redundant switch on other components

1. Connecting Distribution Switches to Redundant Core Switch

Each **distribution switch** (IT, HR, Finance) must be connected to **both Core Switches** for redundancy.

IT Distribution Switch

IT_Distribution# configure terminal

interface FastEthernet0/4 # New uplink to Redundant Core Switch

switchport mode trunk

switchport trunk allowed vlan 10,70,99

spanning-tree portfast trunk

exit

write memory

HR Distribution Switch

HR_Distribution# configure terminal

interface FastEthernet0/4 # New uplink to Redundant Core Switch

switchport mode trunk

switchport trunk allowed vlan 20,80,99

spanning-tree portfast trunk

exit

write memory

Finance Distribution Switch

Finance_Distribution# configure terminal

interface FastEthernet0/4 # New uplink to Redundant Core Switch

switchport mode trunk

switchport trunk allowed vlan 30,90,99

spanning-tree portfast trunk

exit

write memory

Now, all Distribution Switches are connected to both Core Switches.

2. Configure Firewall Connection to Redundant Core Switch

Since the firewall needs a connection to **both Core Switches**, we configure **a second uplink to the Redundant Core Switch**.

Assign VLAN 100 and Configure Its IP on CoreSwitch2

CoreSwitch2# configure terminal

vlan 100

name Firewall_VLAN

exit

interface vlan 100

ip address 192.168.100.3 255.255.255.0

no shutdown

exit

write memory

Assign Correct IP to Firewall Redundant Interface

ciscoasa# configure terminal

interface GigabitEthernet1/3

nameif INSIDE2

security-level 100

ip address 192.168.100.1 255.255.255.0

no shutdown

exit

write memory

Update Static Routes

ciscoasa# configure terminal

route INSIDE 192.168.0.0 255.255.0.0 192.168.99.3 # Primary Core Switch

route INSIDE2 192.168.0.0 255.255.0.0 192.168.100.3 # Redundant Core Switch

exit

write memory

Now, the firewall is connected to both core switches properly.

3. Configure WLC Redundant Connection via Core Switch

Redundant_Core# configure terminal

interface fa 0/24 # Connection to WLC

CoreSwitch2(config)# interface FastEthernet0/24

CoreSwitch2(config-if)# switchport trunk encapsulation dot1q

CoreSwitch2(config-if)# switchport mode trunk

CoreSwitch2(config-if)# switchport trunk allowed vlan 1,10,20,30,50,70,80,90,99

CoreSwitch2(config-if)# no shutdown

CoreSwitch2(config-if)# exit

Now, WLC has an alternate path through the Redundant Core Switch.

4. Connecting Servers to Redundant Core Switch

Since servers are in **VLAN 50 (Server VLAN)**, they need **dual connections** to both core switches.

Configure Server VLAN on the Redundant Core Switch

Redundant_Core# configure terminal

interface Vlan50

ip address 192.168.50.6 255.255.255.0

standby 50 ip 192.168.50.1

standby 50 priority 90

standby 50 preempt

no shutdown

exit

write memory

Now, the redundant core switch can handle Server VLAN traffic.

5. Enable Spanning Tree Protocol (STP) to Prevent Loops

Since we connected **both Core Switches to all components**, we must enable **STP (Spanning Tree Protocol)** to avoid network loops.

Configure STP on Both Core Switches

On **both core switches**, configure **Rapid PVST+**:

CoreSwitch-1# configure terminal

spanning-tree mode rapid-pvst

spanning-tree vlan 1-4094 root primary

exit

write memory

On **Redundant Core Switch**:

Redundant_Core# configure terminal

spanning-tree mode rapid-pvst

spanning-tree vlan 1-4094 root secondary

exit

write memory

Now, STP will block redundant links when both switches are up and re-enable them when one fails.

6. Update DHCP & DNS Server Configuration

Configure Server VLAN on Redundant Core Switch

Redundant_Core# configure terminal

interface FastEthernet0/5 # DHCP Server Port

switchport mode access

switchport access vlan 50

no shutdown

exit

interface FastEthernet0/6 # DNS Server Port

switchport mode access

switchport access vlan 50

no shutdown

exit

write memory

Enable DHCP Relay (IP Helper) for VLANs on Redundant Core Switch

interface vlan 10

ip helper-address 192.168.50.100

exit

interface vlan 20

ip helper-address 192.168.50.100

exit

interface vlan 30

ip helper-address 192.168.50.100

exit

write memory

Now, DHCP requests will be relayed correctly to the server.

7. Testing & Verification

Run the following commands to ensure redundancy works:

show standby brief ! Verify HSRP failover

show spanning-tree summary ! Ensure STP is working

show ip route ! Verify routing updates

show interfaces trunk ! Check trunk connections

1. Configuring Ports on Redundant Core Switch for Distribution Switches

Redundant Core Switch Port Configuration for Distribution Switches

CoreSwitch-2# configure terminal

! IT Distribution Switch Link

interface FastEthernet0/11

switchport mode trunk

switchport trunk allowed vlan 10,70,99

no shutdown

exit

! HR Distribution Switch Link

interface FastEthernet0/12

switchport mode trunk

switchport trunk allowed vlan 20,80,99

no shutdown

exit

! Finance Distribution Switch Link

interface FastEthernet0/13

switchport mode trunk

switchport trunk allowed vlan 30,90,99

no shutdown

exit

write memory

Now, all Distribution Switches are properly connected to the Redundant Core Switch.

---

2. Configuring Firewall Connection on Redundant Core Switch

Firewall Port Configuration on Redundant Core Switch

CoreSwitch-2# configure terminal

interface GigabitEthernet0/1

switchport mode trunk

switchport trunk allowed vlan 10,20,30,50,99

switchport trunk native vlan 99

no shutdown

exit

write memory

Now, the firewall can communicate properly with both Core Switches.

4. Servers - No Extra Ports Available for Redundant Core Switch

Issue: No Ports Available on Servers for Connection

- In **Packet Tracer**, servers typically **only have one Ethernet port** (FastEthernet0).
- This means **we cannot physically connect a server to both Core Switches**.
- **Redundancy cannot be implemented at the hardware level**.

Workaround (Possible in Real Networks, but NOT in Packet Tracer)

🔸 In a real-world scenario, **servers would have multiple NICs** (Network Interface Cards), allowing a connection to **both Core Switches**.

🔸 **Link Aggregation (LACP)** or **NIC Teaming** would be used for failover.

🔸 **In Packet Tracer, this is not possible**.

Conclusion: Servers will remain connected only to CoreSwitch-1, and redundancy for servers **CANNOT** be configured in Packet Tracer.

Since **you implemented port security** on **distribution switches**, connecting new redundant links **triggers a security violation**, causing the ports to **shut down (err-disabled)** or **block communication** (blinking red).

Remove Port Security for Specific Ports

Since **we only want to remove port security from Fa0/4**, use the following CLI on **each distribution switch**:

- **IT Distribution Switch**

IT_Distribution# configure terminal

interface FastEthernet0/4

no switchport port-security

no switchport port-security maximum

no switchport port-security violation restrict

no switchport port-security mac-address sticky

exit

write memory

- **HR Distribution Switch**

HR_Distribution# configure terminal

interface FastEthernet0/4

no switchport port-security

no switchport port-security maximum

no switchport port-security violation restrict

no switchport port-security mac-address sticky

exit

write memory

- **Finance Distribution Switch**

Finance_Distribution# configure terminal

interface FastEthernet0/4

no switchport port-security

no switchport port-security maximum

no switchport port-security violation restrict

no switchport port-security mac-address sticky

exit

write memory

Reactivate the Ports

After removing port security, re-enable the ports if they were **err-disabled**:

IT_Distribution# configure terminal

interface FastEthernet0/4

shutdown

no shutdown

exit

write memory

Repeat the **shutdown & no shutdown** steps for **HR** and **Finance** distribution switches.

Now, the ports should turn green and work properly.

Fixing BPDU Guard Error on Fa0/4 (Err-Disable Due to BPDU Guard)

Your **FastEthernet0/4 port** is being **shut down due to BPDU Guard** detecting a BPDU packet. This happens because the port was previously configured as an **edge/access port** and is now receiving BPDU messages from the Redundant Core Switch (which is a trunk link).

Remove BPDU Guard from FastEthernet0/4

Since **FastEthernet0/4 is now a trunk port**, **BPDU Guard must be removed**:

Dist1Switch# configure terminal

interface FastEthernet0/4

no spanning-tree bpduguard enable

exit

write memory

This will prevent the port from going into err-disable due to BPDU messages.

Reactivate the Port

Now that BPDU Guard is removed, reactivate the port:

Dist1Switch# configure terminal

interface FastEthernet0/4

shutdown

no shutdown

exit

write memory

The port should now remain active and turn green without getting disabled.