enable

configure terminal

hostname Ankara-Router

enable secret cisco

ip routing

! Interface configurations for VLANs

interface GigabitEthernet0/0

no shutdown

description Trunk to Switch

exit

interface GigabitEthernet0/0.10

encapsulation dot1Q 10

ip address 192.168.1.1 255.255.255.0

description Management VLAN

no shutdown

exit

interface GigabitEthernet0/0.20

encapsulation dot1Q 20

ip address 192.168.2.1 255.255.255.0

description Workers VLAN

no shutdown

exit

interface GigabitEthernet0/0.30

encapsulation dot1Q 30

ip address 192.168.4.1 255.255.255.0

description Servers VLAN

no shutdown

exit

! Serial interface configurations

interface Serial0/0/0

ip address 10.10.10.1 255.255.255.252

clock rate 128000

no shutdown

description Link to Istanbul

exit

interface Serial0/0/1

ip address 10.10.11.1 255.255.255.252

clock rate 128000

no shutdown

description Link to Izmir

exit

! OSPF Configuration

router ospf 1

router-id 1.1.1.1

network 192.168.1.0 0.0.0.255 area 0

network 192.168.2.0 0.0.0.255 area 0

network 192.168.4.0 0.0.0.255 area 0

network 10.10.10.0 0.0.0.3 area 0

network 10.10.11.0 0.0.0.3 area 0

exit

write memory

**Ankara Switch**

plaintext

Copy code

enable

configure terminal

hostname Ankara-SW

enable secret cisco

! VLAN Configuration

vlan 10

name Management

exit

vlan 20

name Workers

exit

vlan 30

name Servers

exit

! Assign VLANs to Access Ports

interface range FastEthernet0/1-8

switchport mode access

switchport access vlan 10

exit

interface range FastEthernet0/9-16

switchport mode access

switchport access vlan 20

exit

interface range FastEthernet0/17-24

switchport mode access

switchport access vlan 30

exit

! Configure Trunk Port to Router

interface GigabitEthernet0/1

switchport mode trunk

switchport trunk allowed vlan 10,20,30

exit

write memory

**Istanbul Router**

plaintext

Copy code

enable

configure terminal

hostname Istanbul-Router

enable secret cisco

ip routing

! Interface configurations for VLANs

interface GigabitEthernet0/0

no shutdown

description Trunk to Switch

exit

interface GigabitEthernet0/0.10

encapsulation dot1Q 10

ip address 192.168.1.2 255.255.255.0

ip helper-address 192.168.1.11

description Management VLAN

no shutdown

exit

interface GigabitEthernet0/0.20

encapsulation dot1Q 20

ip address 192.168.2.2 255.255.255.0

ip helper-address 192.168.1.11

description Workers VLAN

no shutdown

exit

interface GigabitEthernet0/0.30

encapsulation dot1Q 30

ip address 192.168.3.2 255.255.255.0

ip helper-address 192.168.1.11

description Guests VLAN

no shutdown

exit

! Serial interface configurations

interface Serial0/0/0

ip address 10.10.10.2 255.255.255.252

no shutdown

description Link to Ankara

exit

interface Serial0/0/1

ip address 10.10.12.1 255.255.255.252

clock rate 128000

no shutdown

description Link to Izmir

exit

! OSPF Configuration

router ospf 1

router-id 2.2.2.2

network 192.168.1.0 0.0.0.255 area 0

network 192.168.2.0 0.0.0.255 area 0

network 192.168.3.0 0.0.0.255 area 0

network 10.10.10.0 0.0.0.3 area 0

network 10.10.12.0 0.0.0.3 area 0

exit

write memory

**Istanbul Switch**

plaintext

Copy code

enable

configure terminal

hostname Istanbul-SW

enable secret cisco

! VLAN Configuration

vlan 10

name Management

exit

vlan 20

name Workers

exit

vlan 30

name Guests

exit

! Assign VLANs to Access Ports

interface range FastEthernet0/1-8

switchport mode access

switchport access vlan 10

exit

interface range FastEthernet0/9-16

switchport mode access

switchport access vlan 20

exit

interface range FastEthernet0/17-24

switchport mode access

switchport access vlan 30

exit

! Configure Trunk Port to Router

interface GigabitEthernet0/1

switchport mode trunk

switchport trunk allowed vlan 10,20,30

exit

write memory

**Izmir Router**

plaintext

Copy code

enable

configure terminal

hostname Izmir-Router

enable secret cisco

ip routing

! Interface configurations for VLANs

interface GigabitEthernet0/0

no shutdown

description Trunk to Switch

exit

interface GigabitEthernet0/0.10

encapsulation dot1Q 10

ip address 192.168.1.3 255.255.255.0

ip helper-address 192.168.1.11

description Management VLAN

no shutdown

exit

interface GigabitEthernet0/0.20

encapsulation dot1Q 20

ip address 192.168.2.3 255.255.255.0

ip helper-address 192.168.1.11

description Workers VLAN

no shutdown

exit

interface GigabitEthernet0/0.30

encapsulation dot1Q 30

ip address 192.168.3.3 255.255.255.0

ip helper-address 192.168.1.11

description Guests VLAN

no shutdown

exit

! Serial interface configurations

interface Serial0/0/0

ip address 10.10.11.2 255.255.255.252

no shutdown

description Link to Ankara

exit

interface Serial0/0/1

ip address 10.10.12.2 255.255.255.252

no shutdown

description Link to Istanbul

exit

! OSPF Configuration

router ospf 1

router-id 3.3.3.3

network 192.168.1.0 0.0.0.255 area 0

network 192.168.2.0 0.0.0.255 area 0

network 192.168.3.0 0.0.0.255 area 0

network 10.10.11.0 0.0.0.3 area 0

network 10.10.12.0 0.0.0.3 area 0

exit

write memory

**Izmir Switch**

plaintext

Copy code

enable

configure terminal

hostname Izmir-SW

enable secret cisco

! VLAN Configuration

vlan 10

name Management

exit

vlan 20

name Workers

exit

vlan 30

name Guests

exit

! Assign VLANs to Access Ports

interface range FastEthernet0/1-8

switchport mode access

switchport access vlan 10

exit

interface range FastEthernet0/9-16

switchport mode access

switchport access vlan 20

exit

interface range FastEthernet0/17-24

switchport mode access

switchport access vlan 30

exit

! Configure Trunk Port to Router

interface GigabitEthernet0/1

switchport mode trunk

switchport trunk allowed vlan 10,20,30

exit

write memory

This configuration ensures:

1. **Ankara's Server** acts as the centralized DHCP server.
2. All VLANs in Istanbul and Izmir can relay DHCP requests to Ankara via ip helper-address.
3. OSPF dynamically routes traffic across the network.

Test connectivity and let me know if you need further clarifications!

4o

**You said:**

xp Cihcp poo p network 192.168.1.0 2SS.2SS.2SS.O default—router 192.168.1.2 ip dhcp pool p2 network 192.1€8.2.0 255.255.255.0 default—route: 192.168.2.2 what about something like this

**ChatGPT said:**

ChatGPT

The configuration you provided looks similar to a **router-based DHCP server setup**, but it seems incomplete and slightly misformatted. Here’s the correct structure and explanation for using **router-based DHCP pools** if you want to set up DHCP on the **router itself** instead of using a dedicated DHCP server.

**Router DHCP Pool Configuration**

You can configure **DHCP pools** directly on a router by following this structure:

**Example for VLAN 10 (Management):**

plaintext

Copy code

ip dhcp pool Management

network 192.168.1.0 255.255.255.0

default-router 192.168.1.1

dns-server 192.168.1.11

**Example for VLAN 20 (Workers):**

plaintext

Copy code

ip dhcp pool Workers

network 192.168.2.0 255.255.255.0

default-router 192.168.2.1

dns-server 192.168.1.11

**Example for VLAN 30 (Guests):**

plaintext

Copy code

ip dhcp pool Guests

network 192.168.3.0 255.255.255.0

default-router 192.168.3.1

dns-server 192.168.1.11

**Example for VLAN 30 (Servers in Ankara):**

plaintext

Copy code

ip dhcp pool Servers

network 192.168.4.0 255.255.255.0

default-router 192.168.4.1

dns-server 192.168.1.11

**Complete DHCP Setup on a Router**

1. **Exclude Reserved Addresses**: Reserve IP addresses for router interfaces, switches, and servers:

plaintext

Copy code

ip dhcp excluded-address 192.168.1.1 192.168.1.10

ip dhcp excluded-address 192.168.2.1 192.168.2.10

ip dhcp excluded-address 192.168.3.1 192.168.3.10

ip dhcp excluded-address 192.168.4.1 192.168.4.10

1. **Create DHCP Pools**: Define the DHCP pools for each VLAN as shown above.

**DHCP Configuration for Each Router**

If **each router provides DHCP for its own VLANs**, configure the pools as follows:

**Ankara Router:**

plaintext

Copy code

enable

configure terminal

ip dhcp excluded-address 192.168.1.1 192.168.1.10

ip dhcp excluded-address 192.168.2.1 192.168.2.10

ip dhcp excluded-address 192.168.4.1 192.168.4.10

ip dhcp pool Management

network 192.168.1.0 255.255.255.0

default-router 192.168.1.1

dns-server 192.168.1.11

ip dhcp pool Workers

network 192.168.2.0 255.255.255.0

default-router 192.168.2.1

dns-server 192.168.1.11

ip dhcp pool Servers

network 192.168.4.0 255.255.255.0

default-router 192.168.4.1

dns-server 192.168.1.11

exit

**Istanbul Router:**

plaintext

Copy code

enable

configure terminal

ip dhcp excluded-address 192.168.1.2 192.168.1.10

ip dhcp excluded-address 192.168.2.2 192.168.2.10

ip dhcp excluded-address 192.168.3.2 192.168.3.10

ip dhcp pool Management

network 192.168.1.0 255.255.255.0

default-router 192.168.1.2

dns-server 192.168.1.11

ip dhcp pool Workers

network 192.168.2.0 255.255.255.0

default-router 192.168.2.2

dns-server 192.168.1.11

ip dhcp pool Guests

network 192.168.3.0 255.255.255.0

default-router 192.168.3.2

dns-server 192.168.1.11

exit

**Izmir Router:**

plaintext

Copy code

enable

configure terminal

ip dhcp excluded-address 192.168.1.3 192.168.1.10

ip dhcp excluded-address 192.168.2.3 192.168.2.10

ip dhcp excluded-address 192.168.3.3 192.168.3.10

ip dhcp pool Management

network 192.168.1.0 255.255.255.0

default-router 192.168.1.3

dns-server 192.168.1.11

ip dhcp pool Workers

network 192.168.2.0 255.255.255.0

default-router 192.168.2.3

dns-server 192.168.1.11

ip dhcp pool Guests

network 192.168.3.0 255.255.255.0

default-router 192.168.3.3

dns-server 192.168.1.11

exit

**Verification Commands**

1. **Check DHCP Pools**:

plaintext

Copy code

show ip dhcp pool

1. **Check Assigned IPs (DHCP Bindings)**:

plaintext

Copy code

show ip dhcp binding

1. **Test from a PC**:
   * Set the PC to **Obtain IP Address Automatically** in the IP Configuration.
   * Verify the PC gets the correct IP address, default gateway, and DNS server.

**Notes**

* The DHCP configuration you provided can be applied on **each router**. However, using a centralized DHCP server is more efficient for large networks like this. If you decide to use router-based DHCP, ensure OSPF is correctly set up for routing traffic across the network.

Let me know if you need additional guidance!

4o

**You said:**

but the dns server is 192.168.4.2

**ChatGPT said:**

ChatGPT

Thank you for pointing that out! If the **DNS Server** IP address is 192.168.4.2, you need to update the **DNS Server** field in all DHCP pool configurations to reflect this. Here’s the corrected configuration:

**Updated DHCP Configuration for Each Router**

**Ankara Router:**

plaintext

Copy code

enable

configure terminal

ip dhcp excluded-address 192.168.1.1 192.168.1.10

ip dhcp excluded-address 192.168.2.1 192.168.2.10

ip dhcp excluded-address 192.168.4.1 192.168.4.10

ip dhcp pool Management

network 192.168.1.0 255.255.255.0

default-router 192.168.1.1

dns-server 192.168.4.2

ip dhcp pool Workers

network 192.168.2.0 255.255.255.0

default-router 192.168.2.1

dns-server 192.168.4.2

ip dhcp pool Servers

network 192.168.4.0 255.255.255.0

default-router 192.168.4.1

dns-server 192.168.4.2

exit

**Istanbul Router:**

plaintext

Copy code

enable

configure terminal

ip dhcp excluded-address 192.168.1.2 192.168.1.10

ip dhcp excluded-address 192.168.2.2 192.168.2.10

ip dhcp excluded-address 192.168.3.2 192.168.3.10

ip dhcp pool Management

network 192.168.1.0 255.255.255.0

default-router 192.168.1.2

dns-server 192.168.4.2

ip dhcp pool Workers

network 192.168.2.0 255.255.255.0

default-router 192.168.2.2

dns-server 192.168.4.2

ip dhcp pool Guests

network 192.168.3.0 255.255.255.0

default-router 192.168.3.2

dns-server 192.168.4.2

exit

**Izmir Router:**

plaintext

Copy code

enable

configure terminal

ip dhcp excluded-address 192.168.1.3 192.168.1.10

ip dhcp excluded-address 192.168.2.3 192.168.2.10

ip dhcp excluded-address 192.168.3.3 192.168.3.10

ip dhcp pool Management

network 192.168.1.0 255.255.255.0

default-router 192.168.1.3

dns-server 192.168.4.2

ip dhcp pool Workers

network 192.168.2.0 255.255.255.0

default-router 192.168.2.3

dns-server 192.168.4.2

ip dhcp pool Guests

network 192.168.3.0 255.255.255.0

default-router 192.168.3.3

dns-server 192.168.4.2

exit

**Centralized DHCP Configuration (if using Ankara Server)**

If DHCP is centralized on the **Ankara Server**, then all other routers just need the **IP Helper Address** to forward DHCP requests. Here's an example of updated IP Helper configuration:

**For Istanbul Router:**

plaintext

Copy code

interface GigabitEthernet0/0.10

encapsulation dot1Q 10

ip address 192.168.1.2 255.255.255.0

ip helper-address 192.168.4.2

no shutdown

interface GigabitEthernet0/0.20

encapsulation dot1Q 20

ip address 192.168.2.2 255.255.255.0

ip helper-address 192.168.4.2

no shutdown

interface GigabitEthernet0/0.30

encapsulation dot1Q 30

ip address 192.168.3.2 255.255.255.0

ip helper-address 192.168.4.2

no shutdown

**For Izmir Router:**

plaintext

Copy code

interface GigabitEthernet0/0.10

encapsulation dot1Q 10

ip address 192.168.1.3 255.255.255.0

ip helper-address 192.168.4.2

no shutdown

interface GigabitEthernet0/0.20

encapsulation dot1Q 20

ip address 192.168.2.3 255.255.255.0

ip helper-address 192.168.4.2

no shutdown

interface GigabitEthernet0/0.30

encapsulation dot1Q 30

ip address 192.168.3.3 255.255.255.0

ip helper-address 192.168.4.2

no shutdown

**Summary**

* **DNS Server** is updated to 192.168.4.2.
* Each router's DHCP pool uses the new DNS server IP.
* If you're using **centralized DHCP** (on the Ankara server), configure the ip helper-address on all routers to forward DHCP requests to 192.168.4.2.

Let me know if you need further clarifications!

4o

**You said:**

but if I want the devices in same vlan can send ping to each other just like the pc in the management of istabul can send to the pcs in each managment department in each city, but the workers can not send to the managment because they can just send to the workers and so and so

**ChatGPT said:**

ChatGPT

To allow **devices in the same VLAN across all cities** to communicate but prevent inter-VLAN communication (e.g., Workers VLAN cannot communicate with Management VLAN), you need to configure the following:

1. **Inter-VLAN Routing for the Same VLANs Across Cities**:
   * Use **OSPF** to route traffic between VLANs with the same IDs (e.g., VLAN 10 for Management across cities).
2. **Access Control Lists (ACLs)**:
   * Apply **ACLs** to restrict communication between different VLANs.

**Step 1: Configure OSPF for Routing Between Same VLANs**

Ensure OSPF is configured to advertise the networks for each VLAN. This allows devices in the **same VLAN ID** (e.g., VLAN 10 for Management) to communicate across different cities.

**Example: OSPF Configuration for Each Router**

**Ankara Router:**

plaintext

Copy code

router ospf 1

router-id 1.1.1.1

network 192.168.1.0 0.0.0.255 area 0 ! Management VLAN

network 192.168.2.0 0.0.0.255 area 0 ! Workers VLAN

network 192.168.4.0 0.0.0.255 area 0 ! Servers VLAN

network 10.10.10.0 0.0.0.3 area 0 ! Link to Istanbul

network 10.10.11.0 0.0.0.3 area 0 ! Link to Izmir

exit

**Istanbul Router:**

plaintext

Copy code

router ospf 1

router-id 2.2.2.2

network 192.168.1.0 0.0.0.255 area 0 ! Management VLAN

network 192.168.2.0 0.0.0.255 area 0 ! Workers VLAN

network 192.168.3.0 0.0.0.255 area 0 ! Guests VLAN

network 10.10.10.0 0.0.0.3 area 0 ! Link to Ankara

network 10.10.12.0 0.0.0.3 area 0 ! Link to Izmir

exit

**Izmir Router:**

plaintext

Copy code

router ospf 1

router-id 3.3.3.3

network 192.168.1.0 0.0.0.255 area 0 ! Management VLAN

network 192.168.2.0 0.0.0.255 area 0 ! Workers VLAN

network 192.168.3.0 0.0.0.255 area 0 ! Guests VLAN

network 10.10.11.0 0.0.0.3 area 0 ! Link to Ankara

network 10.10.12.0 0.0.0.3 area 0 ! Link to Istanbul

exit

**Step 2: Use ACLs to Block Inter-VLAN Communication**

Access Control Lists (ACLs) will be used to **allow VLAN communication only between devices with the same VLAN ID** and block traffic between different VLANs.

**Example ACL Configuration**

1. **Allow Communication for VLAN 10 (Management)**:
   * Allow VLAN 10 devices in any subnet to communicate with each other.
   * Block traffic to other VLANs.

plaintext

Copy code

access-list 101 permit ip 192.168.1.0 0.0.0.255 192.168.1.0 0.0.0.255

access-list 101 deny ip 192.168.1.0 0.0.0.255 any

1. **Allow Communication for VLAN 20 (Workers)**:
   * Allow VLAN 20 devices to communicate only with other VLAN 20 devices.
   * Block traffic to other VLANs.

plaintext

Copy code

access-list 102 permit ip 192.168.2.0 0.0.0.255 192.168.2.0 0.0.0.255

access-list 102 deny ip 192.168.2.0 0.0.0.255 any

1. **Allow Communication for VLAN 30 (Guests)**:
   * Allow VLAN 30 devices to communicate only with other VLAN 30 devices.
   * Block traffic to other VLANs.

plaintext

Copy code

access-list 103 permit ip 192.168.3.0 0.0.0.255 192.168.3.0 0.0.0.255

access-list 103 deny ip 192.168.3.0 0.0.0.255 any

**Step 3: Apply ACLs to Router Interfaces**

Apply these ACLs to the **router interfaces** for each VLAN to enforce the restrictions.

**Ankara Router:**

plaintext

Copy code

interface GigabitEthernet0/0.10

ip access-group 101 in

exit

interface GigabitEthernet0/0.20

ip access-group 102 in

exit

interface GigabitEthernet0/0.30

ip access-group 103 in

exit

**Istanbul Router:**

plaintext

Copy code

interface GigabitEthernet0/0.10

ip access-group 101 in

exit

interface GigabitEthernet0/0.20

ip access-group 102 in

exit

interface GigabitEthernet0/0.30

ip access-group 103 in

exit

**Izmir Router:**

plaintext

Copy code

interface GigabitEthernet0/0.10

ip access-group 101 in

exit

interface GigabitEthernet0/0.20

ip access-group 102 in

exit

interface GigabitEthernet0/0.30

ip access-group 103 in

exit

**Step 4: Verify Configuration**

1. **Test Communication Between Same VLANs Across Cities**:
   * From a PC in VLAN 10 in Istanbul, ping a PC in VLAN 10 in Ankara or Izmir.
   * Ensure the ping succeeds.
2. **Test Inter-VLAN Restrictions**:
   * From a PC in VLAN 20 (Workers), ping a PC in VLAN 10 (Management).
   * Ensure the ping is blocked.
3. **Check ACL Counters**:
   * Verify ACL hits using the following command:

plaintext

Copy code

show access-lists

1. **Verify Routing**:
   * Check the OSPF neighbors and routing table to ensure correct connectivity:

plaintext

Copy code

show ip ospf neighbor

show ip route

**Explanation**

* **OSPF** ensures devices in the same VLAN (but different cities) can route their traffic.
* **ACLs** block traffic between VLANs to enforce segmentation.

This configuration ensures that:

1. **Devices in the same VLAN (e.g., Management VLAN) across cities** can communicate.
2. **Devices in different VLANs** cannot communicate with each other.

Let me know if you need further clarification!

4o

**You said:**

you did a great job, now can you write all of the codes for each device, starting with the Routers, switches, and the DHCP, write a complete codes

**ChatGPT said:**

ChatGPT

Here’s the **complete configuration** for each device (routers, switches, and DHCP server) in your network, incorporating **OSPF routing**, **VLAN setup**, **ACLs**, and the **DHCP server**. This configuration ensures devices in the same VLAN across cities can communicate, but inter-VLAN communication is restricted.

**1. Ankara Router**

plaintext

Copy code

enable

configure terminal

hostname Ankara-Router

enable secret cisco

ip routing

! Interface configurations for VLANs

interface GigabitEthernet0/0

no shutdown

description Trunk to Switch

exit

interface GigabitEthernet0/0.10

encapsulation dot1Q 10

ip address 192.168.1.1 255.255.255.0

description Management VLAN

ip access-group 101 in

no shutdown

exit

interface GigabitEthernet0/0.20

encapsulation dot1Q 20

ip address 192.168.2.1 255.255.255.0

description Workers VLAN

ip access-group 102 in

no shutdown

exit

interface GigabitEthernet0/0.30

encapsulation dot1Q 30

ip address 192.168.4.1 255.255.255.0

description Servers VLAN

ip access-group 103 in

no shutdown

exit

! Serial interfaces

interface Serial0/0/0

ip address 10.10.10.1 255.255.255.252

clock rate 128000

no shutdown

description Link to Istanbul

exit

interface Serial0/0/1

ip address 10.10.11.1 255.255.255.252

clock rate 128000

no shutdown

description Link to Izmir

exit

! OSPF Configuration

router ospf 1

router-id 1.1.1.1

network 192.168.1.0 0.0.0.255 area 0

network 192.168.2.0 0.0.0.255 area 0

network 192.168.4.0 0.0.0.255 area 0

network 10.10.10.0 0.0.0.3 area 0

network 10.10.11.0 0.0.0.3 area 0

exit

! ACLs to restrict inter-VLAN communication

access-list 101 permit ip 192.168.1.0 0.0.0.255 192.168.1.0 0.0.0.255

access-list 101 deny ip any any

access-list 102 permit ip 192.168.2.0 0.0.0.255 192.168.2.0 0.0.0.255

access-list 102 deny ip any any

access-list 103 permit ip 192.168.4.0 0.0.0.255 192.168.4.0 0.0.0.255

access-list 103 deny ip any any

write memory

**2. Ankara Switch**

plaintext

Copy code

enable

configure terminal

hostname Ankara-SW

enable secret cisco

! VLAN Configuration

vlan 10

name Management

exit

vlan 20

name Workers

exit

vlan 30

name Servers

exit

! Assign VLANs to Access Ports

interface range FastEthernet0/1-8

switchport mode access

switchport access vlan 10

exit

interface range FastEthernet0/9-16

switchport mode access

switchport access vlan 20

exit

interface range FastEthernet0/17-24

switchport mode access

switchport access vlan 30

exit

! Configure Trunk Port to Router

interface GigabitEthernet0/1

switchport mode trunk

switchport trunk allowed vlan 10,20,30

exit

write memory

**3. Istanbul Router**

plaintext

Copy code

enable

configure terminal

hostname Istanbul-Router

enable secret cisco

ip routing

! Interface configurations for VLANs

interface GigabitEthernet0/0

no shutdown

description Trunk to Switch

exit

interface GigabitEthernet0/0.10

encapsulation dot1Q 10

ip address 192.168.1.2 255.255.255.0

description Management VLAN

ip access-group 101 in

no shutdown

exit

interface GigabitEthernet0/0.20

encapsulation dot1Q 20

ip address 192.168.2.2 255.255.255.0

description Workers VLAN

ip access-group 102 in

no shutdown

exit

interface GigabitEthernet0/0.30

encapsulation dot1Q 30

ip address 192.168.3.2 255.255.255.0

description Guests VLAN

ip access-group 103 in

no shutdown

exit

! Serial interfaces

interface Serial0/0/0

ip address 10.10.10.2 255.255.255.252

no shutdown

description Link to Ankara

exit

interface Serial0/0/1

ip address 10.10.12.1 255.255.255.252

clock rate 128000

no shutdown

description Link to Izmir

exit

! OSPF Configuration

router ospf 1

router-id 2.2.2.2

network 192.168.1.0 0.0.0.255 area 0

network 192.168.2.0 0.0.0.255 area 0

network 192.168.3.0 0.0.0.255 area 0

network 10.10.10.0 0.0.0.3 area 0

network 10.10.12.0 0.0.0.3 area 0

exit

! ACLs to restrict inter-VLAN communication

access-list 101 permit ip 192.168.1.0 0.0.0.255 192.168.1.0 0.0.0.255

access-list 101 deny ip any any

access-list 102 permit ip 192.168.2.0 0.0.0.255 192.168.2.0 0.0.0.255

access-list 102 deny ip any any

access-list 103 permit ip 192.168.3.0 0.0.0.255 192.168.3.0 0.0.0.255

access-list 103 deny ip any any

write memory

**4. Istanbul Switch**

plaintext

Copy code

enable

configure terminal

hostname Istanbul-SW

enable secret cisco

! VLAN Configuration

vlan 10

name Management

exit

vlan 20

name Workers

exit

vlan 30

name Guests

exit

! Assign VLANs to Access Ports

interface range FastEthernet0/1-8

switchport mode access

switchport access vlan 10

exit

interface range FastEthernet0/9-16

switchport mode access

switchport access vlan 20

exit

interface range FastEthernet0/17-24

switchport mode access

switchport access vlan 30

exit

! Configure Trunk Port to Router

interface GigabitEthernet0/1

switchport mode trunk

switchport trunk allowed vlan 10,20,30

exit

write memory

**5. Izmir Router**

plaintext

Copy code

enable

configure terminal

hostname Izmir-Router

enable secret cisco

ip routing

! Interface configurations for VLANs

interface GigabitEthernet0/0

no shutdown

description Trunk to Switch

exit

interface GigabitEthernet0/0.10

encapsulation dot1Q 10

ip address 192.168.1.3 255.255.255.0

description Management VLAN

ip access-group 101 in

no shutdown

exit

interface GigabitEthernet0/0.20

encapsulation dot1Q 20

ip address 192.168.2.3 255.255.255.0

description Workers VLAN

ip access-group 102 in

no shutdown

exit

interface GigabitEthernet0/0.30

encapsulation dot1Q 30

ip address 192.168.3.3 255.255.255.0

description Guests VLAN

ip access-group 103 in

no shutdown

exit

! Serial interfaces

interface Serial0/0/0

ip address 10.10.11.2 255.255.255.252

no shutdown

description Link to Ankara

exit

interface Serial0/0/1

ip address 10.10.12.2 255.255.255.252

no shutdown

description Link to Istanbul

exit

! OSPF Configuration

router ospf 1

router-id 3.3.3.3

network 192.168.1.0 0.0.0.255 area 0

network 192.168.2.0 0.0.0.255 area 0

network 192.168.3.0 0.0.0.255 area 0

network 10.10.11.0 0.0.0.3 area 0

network 10.10.12.0 0.0.0.3 area 0

exit

! ACLs to restrict inter-VLAN communication

access-list 101 permit ip 192.168.1.0 0.0.0.255 192.168.1.0 0.0.0.255

access-list 101 deny ip any any

access-list 102 permit ip 192.168.2.0 0.0.0.255 192.168.2.0 0.0.0.255

access-list 102 deny ip any any

access-list 103 permit ip 192.168.3.0 0.0.0.255 192.168.3.0 0.0.0.255

access-list 103 deny ip any any

write memory

**6. Izmir Switch**

plaintext

Copy code

enable

configure terminal

hostname Izmir-SW

enable secret cisco

! VLAN Configuration

vlan 10

name Management

exit

vlan 20

name Workers

exit

vlan 30

name Guests

exit

! Assign VLANs to Access Ports

interface range FastEthernet0/1-8

switchport mode access

switchport access vlan 10

exit

interface range FastEthernet0/9-16

switchport mode access

switchport access vlan 20

exit

interface range FastEthernet0/17-24

switchport mode access

switchport access vlan 30

exit

! Configure Trunk Port to Router

interface GigabitEthernet0/1

switchport mode trunk

switchport trunk allowed vlan 10,20,30

exit

write memory

**7. DHCP Server**

1. Open the **Server** in Packet Tracer.
2. Go to the **Services** tab.
3. In the **DHCP section**, create the following pools:
   * **ManagementPool**: 192.168.1.0/24, Gateway: 192.168.1.1
   * **WorkersPool**: 192.168.2.0/24, Gateway: 192.168.2.1
   * **GuestsPool**: 192.168.3.0/24, Gateway: 192.168.3.1
   * **ServersPool**: 192.168.4.0/24, Gateway: 192.168.4.1