MARMARA ÜNİVERSİTESİ TEKNOLOJİ FAKÜLTESİ

BİLGİSAYAR MÜHENDİSLİĞİ

BİLGİSAYAR AĞLARINA GİRİŞ
LAB FİNAL RAPOR

HAZIRLAYAN

BERKANT ERMİŞ-170423852

FERZA ER-170423058

BUĞRA ALPASLAN-170423022

11.GRUP

OTEL AĞ ALTYAPI TASARIMI

Projenin Amacı ve Kapsamı:

Bu projenin amacı, bir otel işletmesi için güvenli, hızlı ve verimli bir ağ altyapısı tasarlamaktır. Cisco Packet Tracer uygulaması kullanarak gerçekleştirdiğimiz bu tasarımda, otelin farklı bölümleri (resepsiyon, restoran, yönetici, finans, insan kaynakları, satış-pazarlama vb.) arasında kesintisiz iletişim sağlanması hedeflenmişitir. Proje kapsamında; ağ cihazlarının konumlandırılması, IP adresleme planlaması, VLAN yapısı, kablolu ve kablosuz bağlantılar gibi temel ağ bileşenleri planlanarak, otelin hem iç hizmetleri hem de müşteri kullanımı için ideal bir ağ ortamı oluşturulmuştur.

Ağ Topolojisi ve Tasarımı:

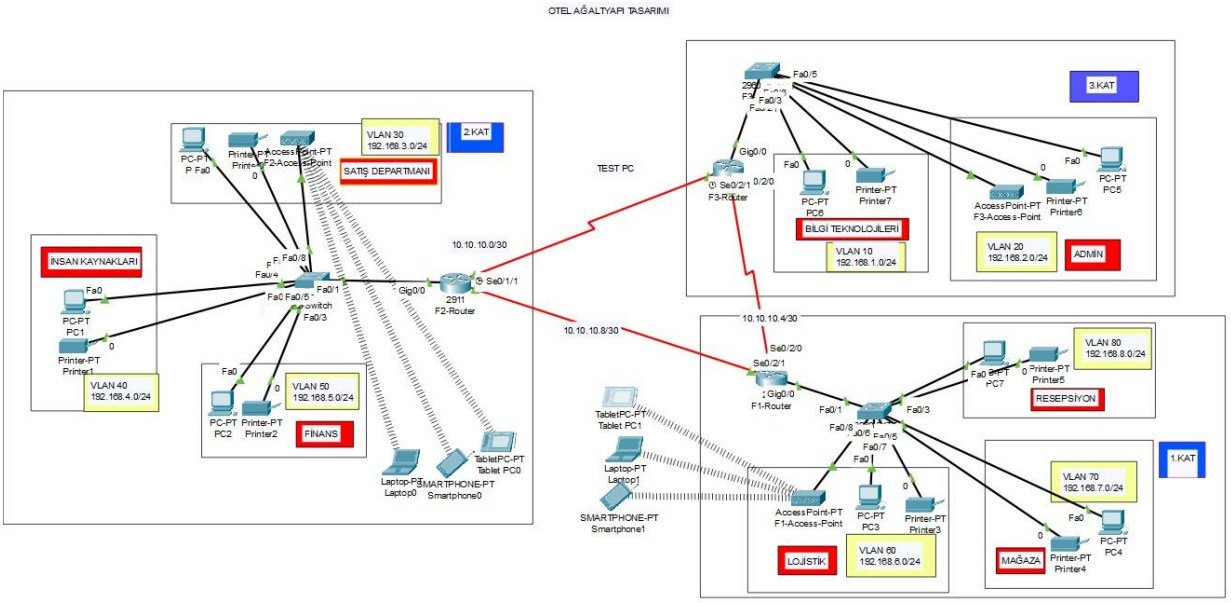
Projenin temel ağ topolojisi 3 kat ve 8 farklı departmandan oluşmaktadır. 1.katta resepsiyon, mağaza ve lojistik departmanları; 2.katta finans, insan kaynakları ve satış departmanı; 3.katta admin (yönetici) ve bilgi teknolojileri (IT) departmanları bulunmaktadır.

Kullandığımız Donanım Cihazları:

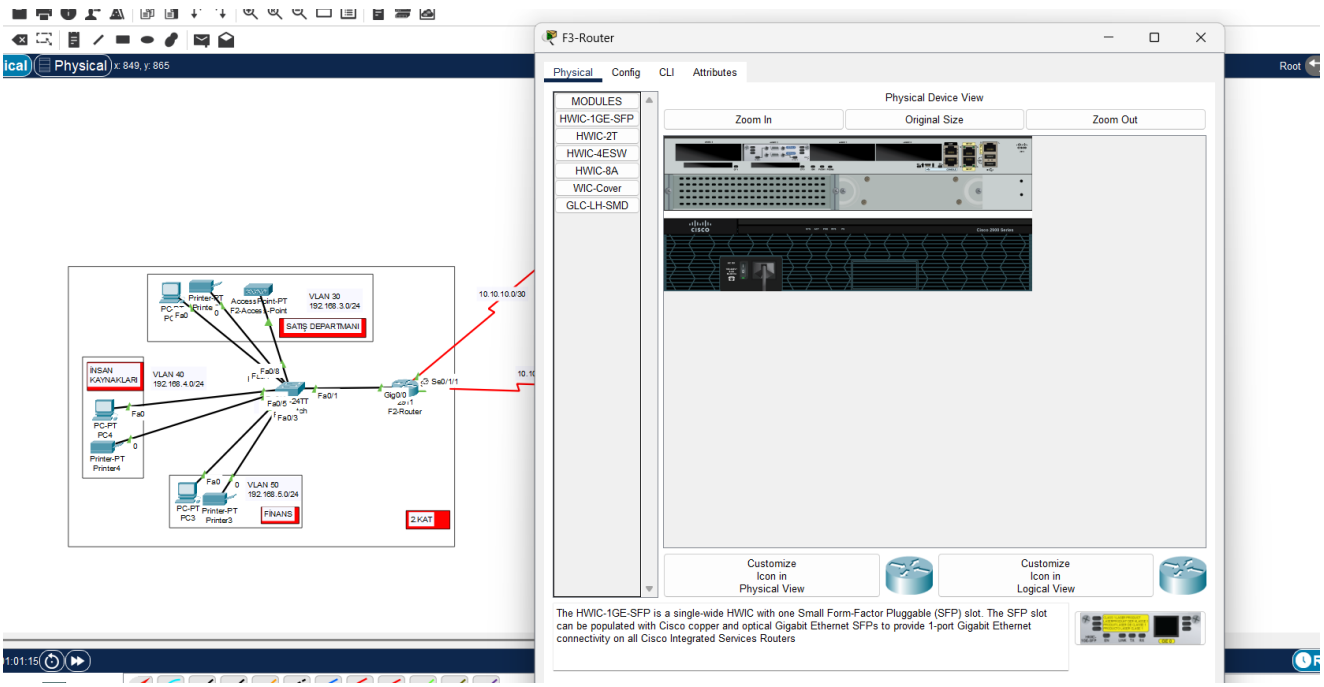
- 8 adet masaüstü (PC) ve 8 adet Yazıcı (printer) (Her departmanda bir adet PC ve bir adet Printer olacak şekilde)
- 3 adet access point (Her kat için bir tane)
- 3 adet Switch
- 3 adet Router

Gerçekleştirilen Adımlar:

- Ağ yapısnı tasarlamak ve uygulamak için Cisco Packet Tracer simülasyon programı kullanılmıştır.
- Ağkatmanında hiyerarşik model kullanılmıştır; yönlendiriciler ve anahtarlar kullanarak ağdaki trafik yönetimi ve kontrolü sağlanmıştır.
- Tüm routerlar seri DCE kabloları ile birbirine bağlanmıştır.
- Routerlar arası ağlar sırasıyla 10.10.10.0/30,10.10.10.4/30,10.10.10.8/30 olarak belirlenmiştir.
- Her katta bir adet switch ilgili kata yerleştirilerek ağa dahil edilmiştir.
- Her katta dizüstü bilgisayar, tablet ve telefonlara bağlı WIFI ağlarını oluşturulmuştur.
- Her departman için bir adet yazıcı kurulumu gerçekleştirilmiştir.
- Departmanlar arası ayrım sağlamak için VLAN yapısı uygulanmıştır.
- Yönlendiriciler üzerinde dinamik yönlendirme protokolü olarak OSPF yapılandırılmıştır.
- Ağdaki tüm cihazların, DHCP sunucusu olarak yapılandırılmış ilgili yönlendiricileri ile dinamik olarak IP adresi alması sağlanmıştır.
- Ağdaki tüm cihazların birbirleriyle iletişim kurması sağlanmıştır.
- Uzaktan erişimi mümkün kılmak için yönlendiricilere SSH yapılandırılması uygulanmıştır.
- BT departmanında bulunan Test-PC adlı bilgisayar, fa0/1 portuna bağlanarak uzaktan oturum açma testleri gerçekleştirilmiştir.
- Yalnızca Test-PC'nin bağlandığı fa0/1 portuna erişim izni verilerek, bağlantı noktası güvenliği port-security ile sağlanmıştır.
- Tüm ağ yapısı test edilerek, herhangi bir bağlantı veya erişim problemi ile karşılaşılmadığı doğrulanmıştır.



Şekil 1: Ağ topolojisi tasarımımızda, her bir katın departmanlarını birbirine bağlamak için F1-switch, F2-switch ve F3-switch olmak üzere kat başına bir adet anahtar (switch) kullanılmıştır. Katlar arası iletişimi ve yönlendirmeyi sağlamak için F1-router, F2-router ve F3-router adlandırmalarıyla her katta bir yönlendirici (router) konumlandırılmıştır. Kablosuz cihazların (dizüstü bilgisayar, tablet, telefon vb.) kablolu ağa entegrasyonu için her katta bir adet Erişim Noktası (Access Point) kullanılmıştır. Her departman için birer adet kişisel bilgisayar (PC) ve yazıcı (Printer) sisteme dahil edilmiştir. Departman içi cihazların anahtarlara ve anahtarların yönlendiricilere bağlantısı otomatik kabloları seçim özelliği kullanılarak gerçekleştirilmiştir. Yönlendiriciler arası geniş alan ağı (WAN) bağlantısı ise Seri DCE (Data Circuit-terminating Equipment) kabloları aracılığıyla sağlanmıştır.



Şekil 2: Yönlendiriciler (routerlar) arası geniş alan ağı (WAN) bağlantısını oluşturmak için, her bir yönlendiriciye HWIC-2T (High-Speed WAN Interface Card with 2 T1/E1 ports) modülleri entegre edilmiştir. Bu modüller, Şekil 2'de görüldüğü üzere, seri DCE (Data Circuit-terminating Equipment) kabloları aracılığıyla doğrudan bağlantı kurulmasını sağlamıştır. Bu yapılandırma, yönlendiriciler arasında güvenilir ve yüksek performanslı bir WAN omurgası oluşturarak, farklı katmanlardaki ağların birbirleriyle iletişim kurabilmesine olanak tanımıştır. HWIC-2T kartlarının kullanılması, seri arayüzler üzerinden veri iletiminin standartlara uygun bir şekilde gerçekleştirilmesine imkan tanımıştır.

1.KAT:

DEPARTMANLAR	NETWORK ADRES	SUBNET MASK	HOST ADRES ARALIĞI	BROADCAST ADRES
Resepsiyon	192.168.8.0	255.255.255.0	192.168.8.1-192.168.8.254	192.168.8.255
Mağaza	192.168.7.0	255.255.255.0	192.168.7.1-192.168.7.254	192.168.7.255
Lojistik	192.168.6.0	255.255.255.0	192.168.6.1-192.168.6.254	192.168.6.255

2.KAT:

DEPARTMANLAR	NETWORK ADRES	SUBNET MASK	HOST ADRES ARALIĞI	BROADCAST ADRES
Finans	192.168.5.0	255.255.255.0	192.168.5.1-192.168.5.254	192.168.5.255
İnsan Kaynakları	192.168.4.0	255.255.255.0	192.168.4.1-192.168.4.254	192.168.4.255
Satış-Pazarlama	192.168.3.0	255.255.255.0	192.168.3.1-192.168.3.254	192.168.3.255

3.KAT:

DEPARTMANLAR	NETWORK ADRES	SUBNET MASK	HOST ADRES ARALIĞI	BROADCAST ADRES
IT	192.168.2.0	255.255.255.0	192.168.2.1-192.168.2.254	192.168.2.255
Yönetici	192.168.1.0	255.255.255.0	192.168.1.1-192.168.1.254	192.168.1.255

ROUTERLAR ARASINDAKİ BAĞLANTI YOLLARININ ADRESLERİ

NAME	NETWORK ADRES	SUBNET MASK	HOST ADRES ARALIĞI	BROADCAST ADRES
1.KAT ROUTER-2.KAT ROUTER	10.10.10.8/30	255.255.255.252	10.10.10.9-10.10.10.10	10.10.10.11
2.KAT ROUTER-3.KAT ROUTER	10.10.10.0/30	255.255.255.252	10.10.10.1-10.10.10.2	10.10.10.3
3.KAT ROUTER-1.KAT ROUTER	10.10.10.4/30	255.255.255.252	10.10.10.5-10.10.10.6	10.10.10.7

Yönlendiriciler Arasındaki Bağlantı Yollarının Adreslemesi ve Verimlilik

WAN bağlantılarımızda, yönlendiriciler arası iletişimi sağlamak için 10.10.10.0/30, 10.10.10.4/30 ve 10.10.10.8/30 IP blokları belirlenmiştir. Bu seçimin temel nedeni, /30 alt ağ maskesinin (subnet mask) nokta-nokta (point-to-point) bağlantılar için sunduğu yüksek verimliliktir.

Bir /30 alt ağ maskesi, 2^{(32-30)} = 2^2 = 4 IP adresi içerir. Bu dört adresten biri ağ adresi (Network Address), diğeri yayın adresi (Broadcast Address) olarak kullanılırken, kalan iki IP adresi kullanılabilir ana bilgisayar (Host) adresleri olarak tahsis edilebilir. Bu yapı, her bir nokta-nokta bağlantı için yalnızca gerekli olan iki IP adresini sağlayarak IP adresi havuzumuzun daha verimli kullanılmasını mümkün kılmaktadır.

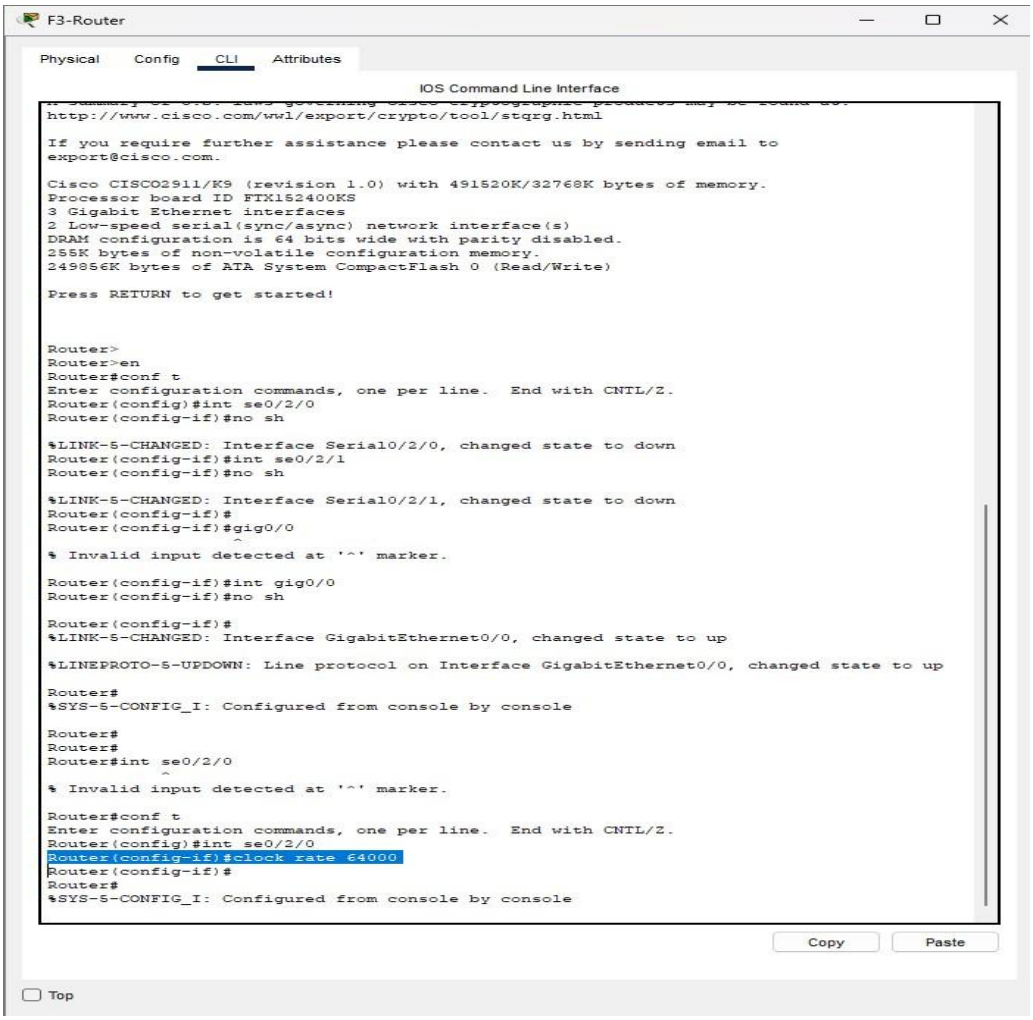
Her /30 alt ağı 4 IP adresi kapsadığından, bir sonraki alt ağın başlangıç adresi, önceki alt ağın yayın adresinden sonraki ilk kullanılabilir IP adresi olmak zorundadır. Örneğin: 10.10.10.0/30 bloğu için:

- Ağ Adresi: 10.10.10.0
- Kullanılabilir Host Adresleri: 10.10.10.1 - 10.10.10.2
- Yayın Adresi: 10.10.10.3

Bu durumda, bir sonraki alt ağ 10.10.10.4/30 ile başlar. 10.10.10.4/30 bloğu için:

- Ağ Adresi: 10.10.10.4
- Kullanılabilir Host Adresleri: 10.10.10.5 - 10.10.10.6
- Yayın Adresi: 10.10.10.7

Ve bunu takiben, 10.10.10.8/30 ile başlayan alt ağ gelir.
Bu sıralı ve düzenli IP atama prensibi, IP çakışmalarını önlerken aynı zamanda ağ yönetimini ve sorun giderme süreçlerini basitleştirmektedir. Bu yaklaşım, ağımızdaki IP adresi tüketimini optimize ederek gelecekteki genişlemeler için daha fazla esneklik sağlamaktadır.



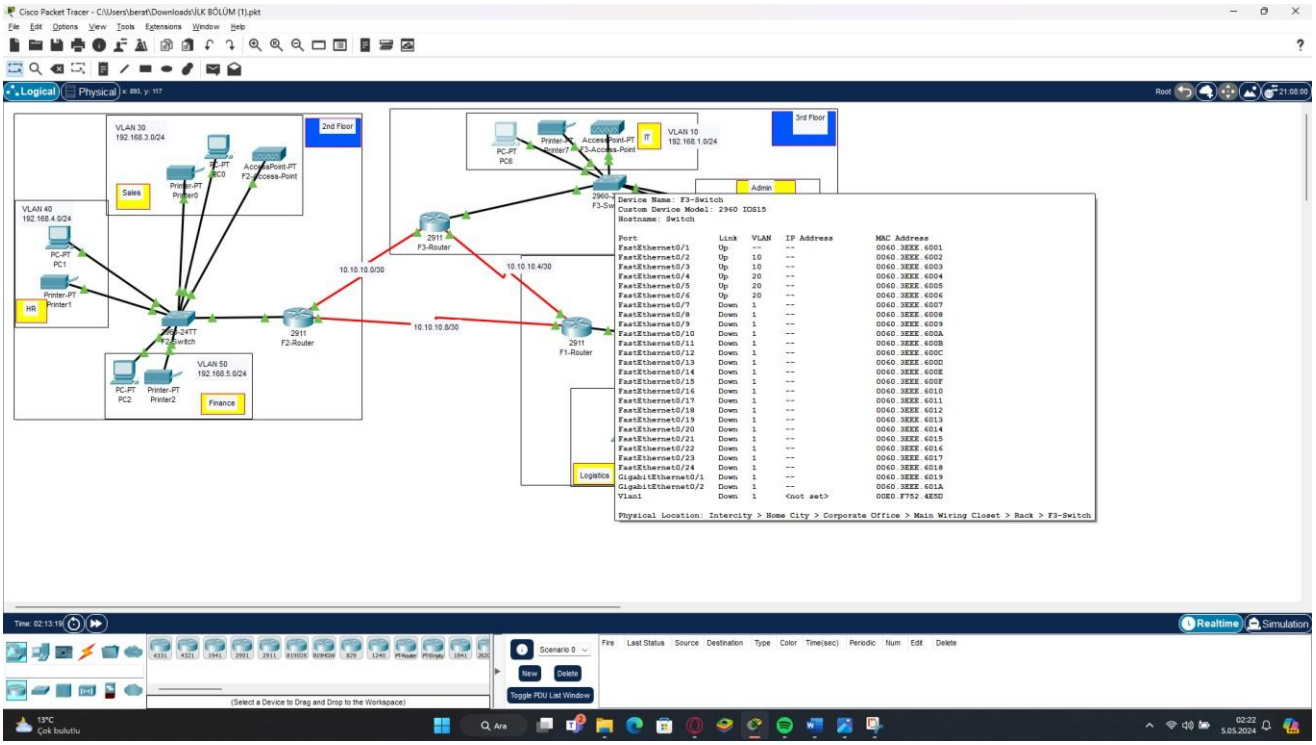
Şekil3: Router'in yapılandırma süreci gerçekleştirilmiştir. İlk olarak router'a seri ve Gigabit Ethernet arabirimleri tanıtılmış ve bu arabirimler üzerinde temel konfigürasyonlar yapılmıştır. GigabitEthernet0/0 ve Serial0/2/0 arabirimlerine ip adres komutları kullanılarak IP adresleri atanmış ve no shutdown komutu ile arabirimler aktif hale getirilmiştir. Ayrıca, seri arabirime iletişimin sağlıklı bir şekilde çalışabilmesi için clock rate 64000 komutu uygulanmıştır. Bu clock rate, DCE (Data Communication Equipment) konumundaki router'larda zamanlama sinyali sağlamak için kullanılır. Yapılandırma sonunda, show ip interface brief komutu ile arabirimlerin IP adresleri, durumları ve protokol durumları kontrol edilmiştir. Bu işlemler üç router için de aynı şekilde tekrarlanmıştır.

```
Switch>
Switch>
Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#int range fa0/2-3
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 50
% Access VLAN does not exist. Creating vlan 50
Switch(config-if-range)#int range fa0/4-5
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 40
% Access VLAN does not exist. Creating vlan 40
Switch(config-if-range)#int range fa0/6-8
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 30
% Access VLAN does not exist. Creating vlan 30
Switch(config-if-range)#do wr
Building configuration...
[OK]
Switch(config-if-range)#int range fa0/1
Switch(config-if-range)#switchport mode trunk

Switch(config-if-range)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down
```

Copy Paste

Top

Şekil4: Bu yapılandırmada, switch üzerinde çeşitli FastEthernet portları belirli VLAN'lara atanarak ağ segmentasyonu gerçekleştirilmiştir. İlk olarak interface range fa0/2-3 komutu ile seçilen portlar erişim (access) moduna alınmış ve switchport access vlan 50 komutu ile VLAN 50'ye atanmıştır. Aynı şekilde, fa0/4-5 aralığındaki portlar VLAN 40'a, fa0/6 portu ise VLAN 30'a atanmıştır. Her VLAN oluşturulmadan önce sistem tarafından otomatik olarak tanımlanmıştır. Bu işlem, ağda farklı departman veya hizmetler için sanal ağlar oluşturarak veri trafiğini izole etmeye yarar.
Son olarak, fa0/1 portu seçilerek switchport mode trunk komutu uygulanmış ve bu port trunk moduna alınmıştır. Trunk portlar, birden fazla VLAN bilgisini aynı bağlantı üzerinden taşıyabildiği için genellikle switchler arası bağlantılarda veya router bağlantılarında kullanılır. Bu yapılandırma ile switch, hem VLAN segmentasyonu hem de VLAN'lar arası geçiş için uygun hale getirilmiştir.



Şekil5: İlgili portların aktif olduğu ve VLAN'a atandığı görülmektedir.

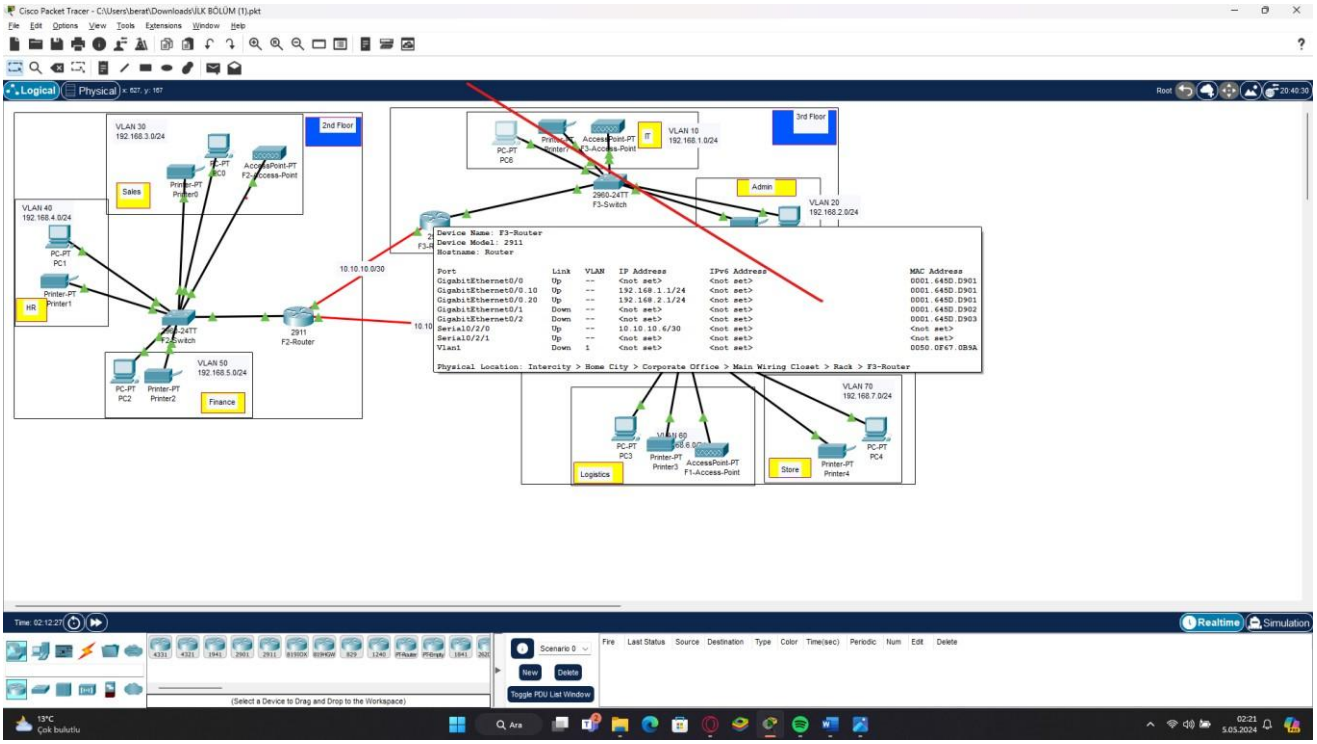
```
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#int se0/2/0
Router(config-if)#ip address 10.10.10.6 255.255.255.252
Router(config-if)#int se0/2/1
Router(config-if)#ip address 10.10.10.6 255.255.255.252
% 10.10.10.4 overlaps with Serial0/2/0
```

Şekil6: Bu yapılandırmada Router üzerinde seri arabirimlere IP adresleri atanmıştır. İlk olarak interface Serial0/2/0 komutu ile ilgili seri port seçilmiş ve ip address 10.10.10.6 255.255.255.252 komutu ile IP adresi atanmıştır. Daha sonra interface Serial0/2/1 arabirimi için de aynı IP adresi atanmak istenmiş fakat sistem tarafından % 10.10.10.4 overlaps with Serial0/2/0 şeklinde bir uyarı mesajı verilmiştir. Bu uyarı, her iki arabirime aynı IP bloğuna ait adreslerin atanmasının IP çakışmasına (overlap) neden olduğunu belirtmektedir.

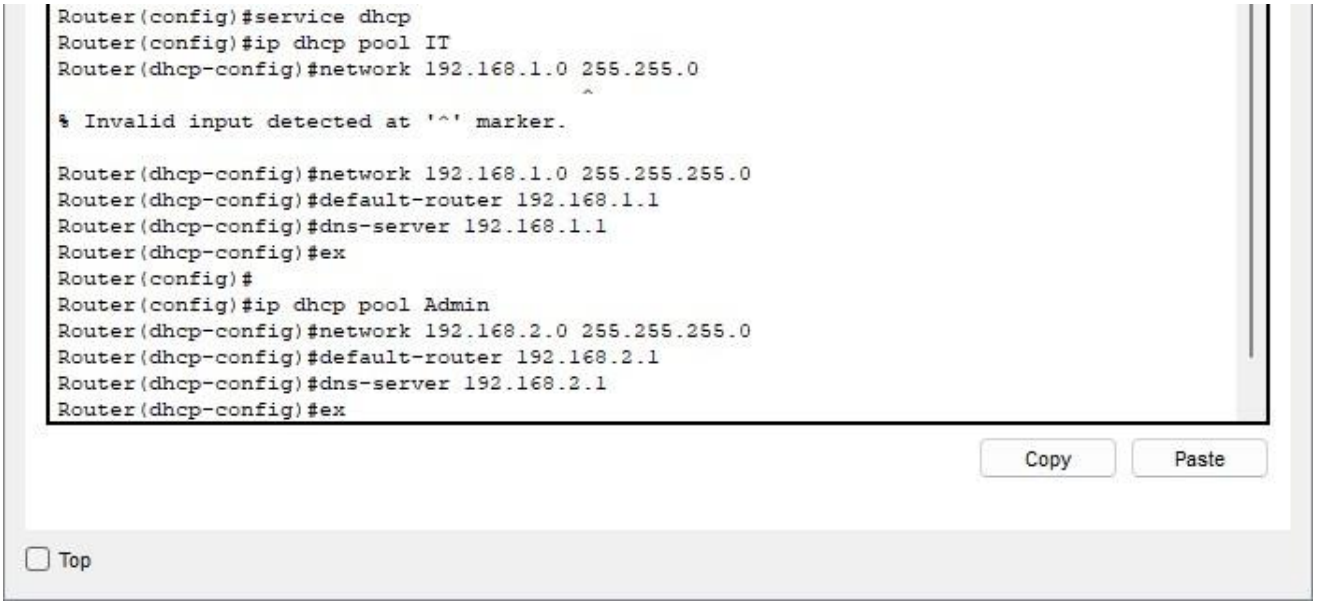
Bu durum, iki seri arayüzün aynı alt ağda yer almaması gerektiğini ya da her bir bağlantı için farklı IP blokları kullanılması gerektiğini göstermektedir. Bu hata, ağ topolojisinin doğru çalışması açısından önemli bir konfigürasyon hatasına işaret etmektedir ve düzeltilmesi gerekir.

```
Router(config)#int gig0/0.10
Router(config-subif)#encapsulation dot1Q 10
Router(config-subif)#ip address 192.168.1.1 255.255.255.0
Router(config-subif)#ex
Router(config)#
Router(config)#int gig0/0.20
Router(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0.20, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.20, changed state to
up

Router(config-subif)#encapsulation dot1Q 20
Router(config-subif)#ip address 192.168.2.1 255.255.255.0
Router(config-subif)#ex
```

Şekil 7: Bu yapılandırmada, bir router üzerinde inter-VLAN routing işlemi gerçekleştirebilmek için subinterface'ler oluşturulmuştur. Fiziksel bir GigabitEthernet arayüzü (GigabitEthernet0/0) altına sanal alt arayüzler tanımlanarak, her bir VLAN için ayrı IP yapılandırmaları yapılmıştır.
İlk olarak interface gig0/0.10 komutu ile VLAN 10'a ait bir subinterface tanımlanmış, ardından encapsulation dot1Q 10 komutu ile bu alt arayüzün 802.1Q VLAN etiketleme protokolü kullanarak VLAN 10'a ait olduğu belirtilmiştir. Bu alt arayüze ip address 192.168.1.1 255.255.255.0 komutu ile IP adresi atanmıştır.
Aynı işlemler VLAN 20 için de tekrarlanmıştır. interface gig0/0.20 komutu ile ikinci subinterface oluşturulmuş, encapsulation dot1Q 20 komutu ile bu arayüz VLAN 20'ye bağlanmıştır ve ip address 192.168.2.1 255.255.255.0 komutu ile IP adresi verilmiştir.
Bu yapılandırma sayesinde router, VLAN 10 ve VLAN 20 arasında yönlendirme (routing) işlemi yapabilecek duruma gelmiştir. Böylece farklı VLAN'larda bulunan istemciler, router üzerinden birbirleriyle iletişim kurabilir hale gelmiştir. Ayrıca alt arayüzlerin aktif hale gelmesiyle birlikte "line protocol" durumlarının "up" olduğu görülmektedir.



Şekil 8: Vlanlar için IP adreslerinin atandığı görülmektedir.



Şekil 9: Bu yapılandırmada, router üzerinde DHCP (Dynamic Host Configuration Protocol) servisi etkinleştirilmiş ve belirli VLAN'lara ait IP adreslerini otomatik olarak dağıtabilmek için DHCP havuzları (pools) tanımlanmıştır.

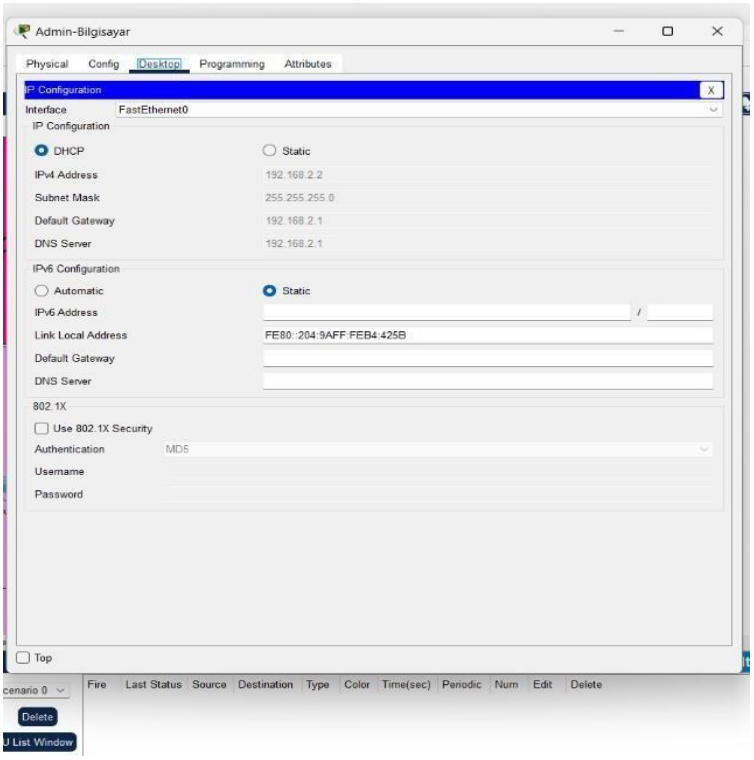
1. DHCP Servisinin Aktifleştirilmesi

Router(config)#service dhcp

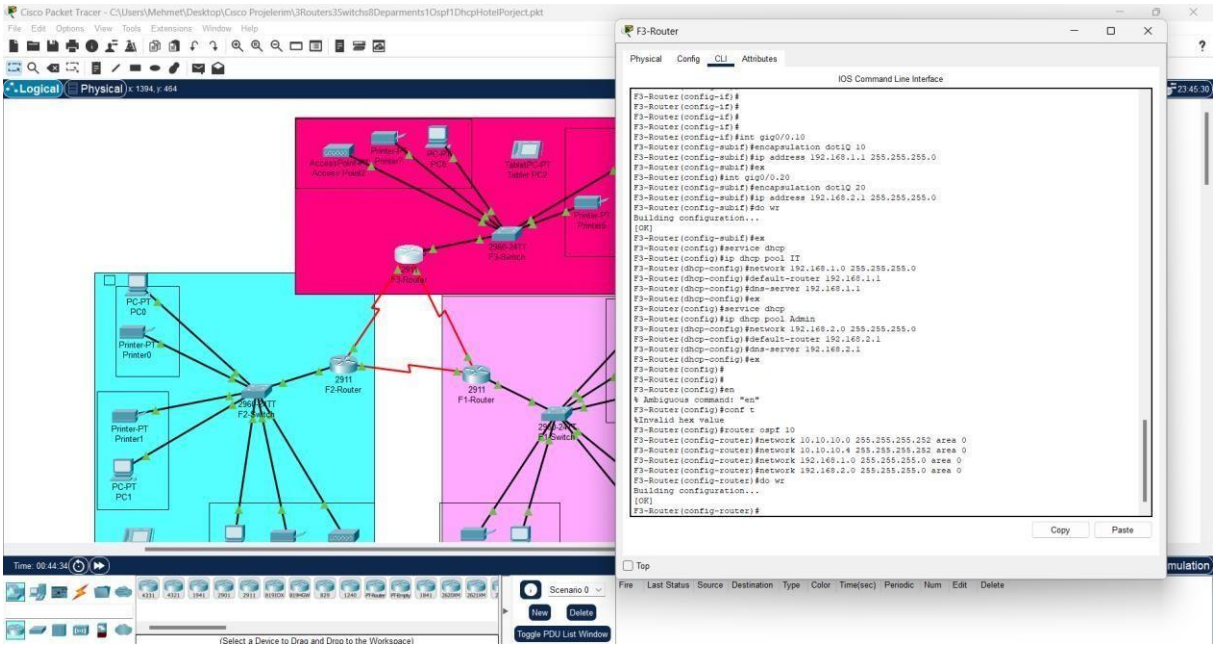
Bu komut, router üzerinde DHCP servisini aktif hale getirir. Böylece router, istemcilere otomatik IP dağıtımı yapabilecek duruma gelir.

2. DHCP Havuzu Oluşturma – İlk Havuz (VLAN 10 için)

Router(config)#ip dhcp pool V10
Router(dhcp-config)#network 192.168.10.0 255.255.255.0
Burada “V10” isimli bir DHCP havuzu oluşturulmuştur. Bu havuzdan IP almak isteyen cihazlara 192.168.10.0/24 ağına ait adresler atanacaktır.
Router(dhcp-config)#default-router 192.168.10.1
Router(dhcp-config)#dns-server 192.168.1.1
default-router: DHCP ile birlikte istemcilere verilecek varsayılan ağ geçididir.
dns-server: DHCP istemcilerine verilecek DNS sunucusunun IP adresidir.
3. İkinci DHCP Havuzu – VLAN 20 için
Router(config)#ip dhcp pool Admin
Router(dhcp-config)#network 192.168.20.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.20.1
Router(dhcp-config)#dns-server 192.168.1.1
Bu blokta da “Admin” adında ikinci bir DHCP havuzu tanımlanmıştır. Aynı yapı kullanılarak bu sefer 192.168.20.0/24 ağına ait istemcilere dinamik IP verilecektir.
DHCP hizmeti sayesinde, ağa bağlanan istemciler manuel ayar yapmadan otomatik olarak IP, gateway ve DNS bilgilerini alabilir.
Bu yapılandırma, büyük ağlarda IP yönetimini kolaylaştırır ve IP çakışmalarını önler. Ayrıca VLAN’lara özel DHCP yapılandırılması sayesinde farklı ağ segmentlerine uygun IP dağıtımı sağlanır.



Şekil 10: DHCP havuzu oluşturulduğu ve atanan dinamik IP’lerin atandığı görülmektedir.



Şekil 11: 1. Subinterface (Alt Arayüz) Tanımlama ve VLAN Atamaları

int g0/0.10

encapsulation dot1Q 10

ip address 192.168.10.1 255.255.255.0

GigabitEthernet0/0.10 adlı alt arayüz (subinterface) oluşturulmuş. Bu alt arayüz VLAN 10 ile eşleştirilmiş (encapsulation dot1Q 10 komutu ile). Bu VLAN'a ait alt ağa 192.168.10.1 IP adresi atanmış.

Benzer şekilde GigabitEthernet0/0.20 alt arayüzü oluşturulmuş. VLAN 20 ile ilişkilendirilmiş. IP adresi olarak 192.168.20.1 atanmış.

Bu işlemler sayesinde router, VLAN 10 ve VLAN 20'ye bağlı istemciler arasında yönlendirme (routing) yapabilir hale gelir. Bu, Router-on-a-Stick yöntemiyle yapılan inter-VLAN yönlendirmeye örnektir.

2. OSPF (Open Shortest Path First) Yönlendirme Protokolü Yapılandırması:

router ospf 1

network 192.168.10.0 0.0.0.255 area 0

network 192.168.20.0 0.0.0.255 area 0

router ospf 1: OSPF yönlendirme protokolü başlatılıyor (process ID 1).

network komutları ile OSPF'e dahil edilecek ağlar tanımlanıyor:

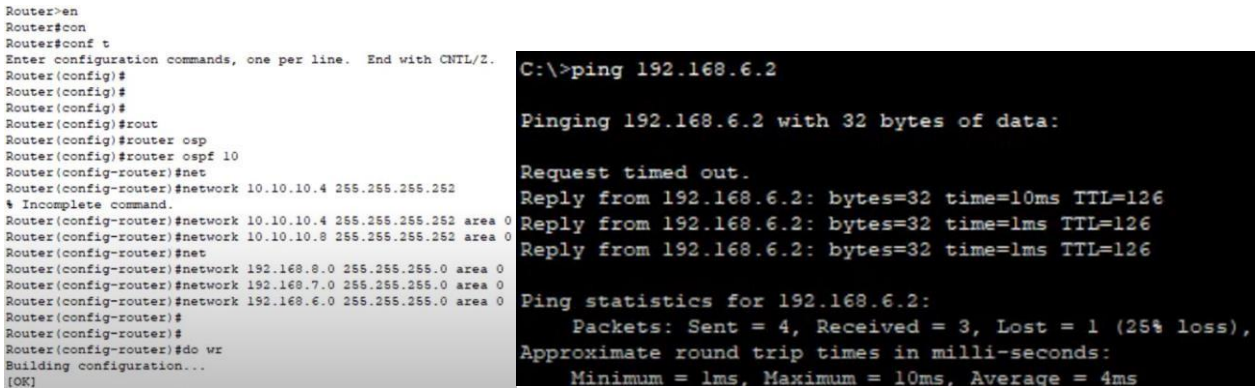
192.168.10.0/24 ve 192.168.20.0/24 ağları OSPF area 0 (backbone area) içine alınmış.

Bu yapılandırma ile router, bu ağlara bağlı diğer yönlendiricilerle dinamik yönlendirme bilgisi paylaşabilecek hale gelir. Böylece IP paketleri, OSPF protokolü kullanılarak en kısa yoldan hedefe yönlendirilir.

Özetle:

Subinterface'ler tanımlanarak VLAN'lara IP atanmış, Router, VLAN'lar arası iletişim için yapılandırılmış,

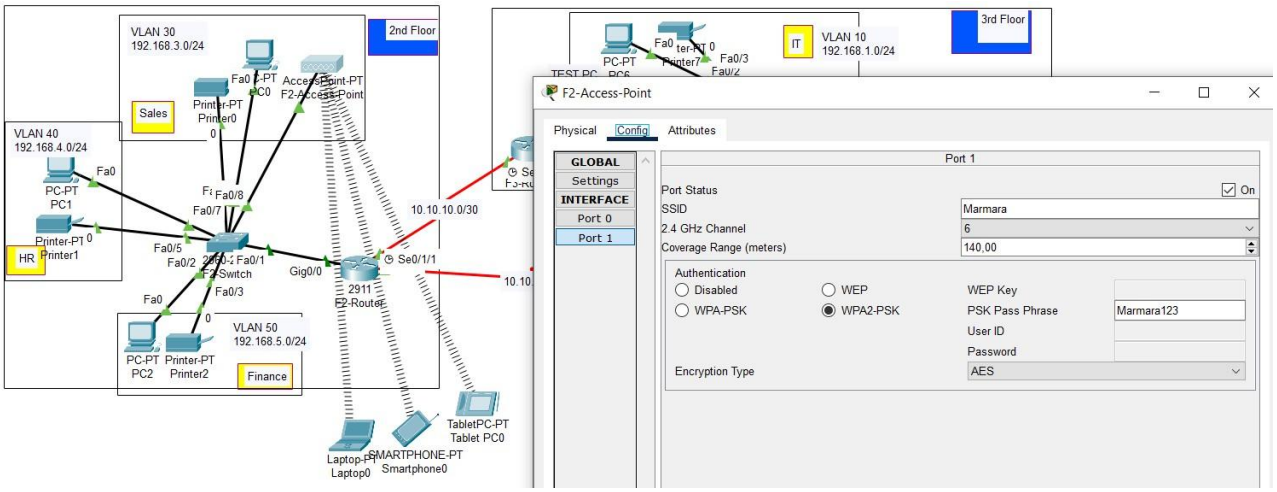
OSPF protokolü kullanılarak ağ yönlendirmesi dinamik hale getirilmiştir.



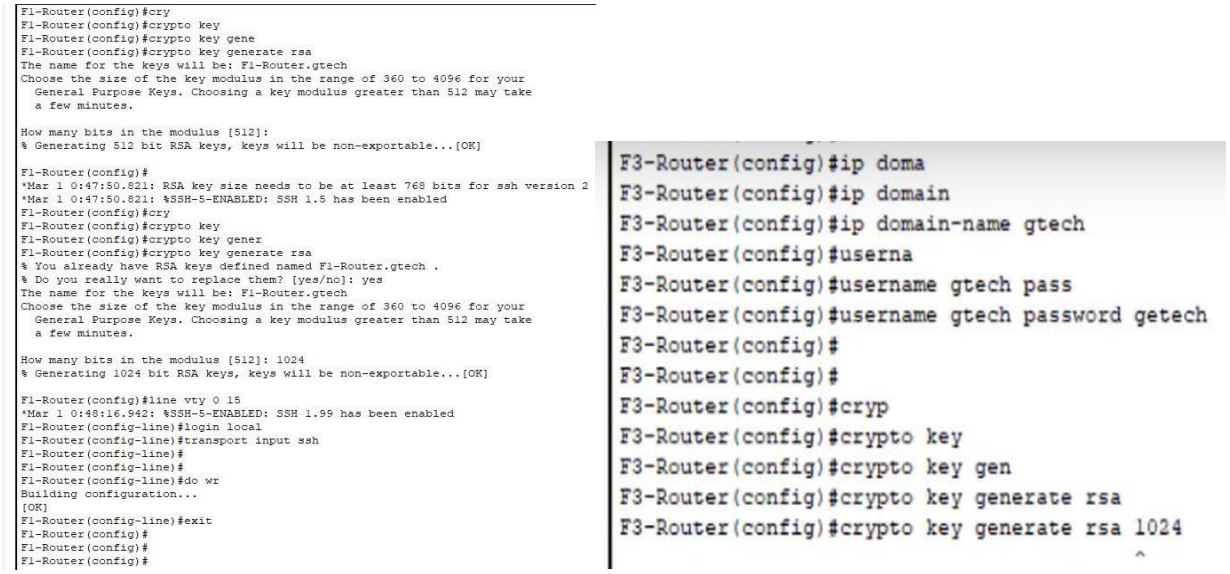
Şekil 12: Bu yapılandırmada, ağdaki tüm cihazların birbirleriyle iletişim kurabilmesi amacıyla her bir router'a bağlı olan ağlar, router üzerinde uygun komutlarla tanımlanmıştır. Görselin sol kısmında yer alan komut çıktılarında, yönlendirici (router) üzerinde OSPF (Open Shortest Path First) yönlendirme protokolü yapılandırılmıştır. OSPF yönlendirme sürecinde, router ospf 10 komutu ile sürecin başlatıldığı, ardından network komutlarıyla ilgili ağların OSPF protokolüne dahil edildiği görülmektedir. Bu işlemler sayesinde router, kendi bağlı olduğu ağları OSPF'e dahil ederek diğer router'larla yönlendirme bilgisi paylaşabilir duruma gelmiştir.

Görselin sağ tarafında yer alan komut çıktısında ise bir bilgisayardan 192.168.6.2 IP adresine yapılan ping testi gösterilmektedir. İlk denemede zaman aşımı (Request timed out) yaşanmasına rağmen, sonraki üç pakette başarılı yanıtlar alınmıştır. Bu durum, OSPF protokolü aracılığıyla yönlendirme bilgilerinin öğrenilmesinden sonra ağlar arası iletişimin başarıyla kurulduğunu göstermektedir.

Sonuç olarak, her bir router'a bağlı olan network'lerin doğru şekilde yapılandırılması ve OSPF protokolüyle dinamik yönlendirme yapılması sayesinde ağdaki tüm cihazların birbiriyle iletişim kurması sağlanmıştır.

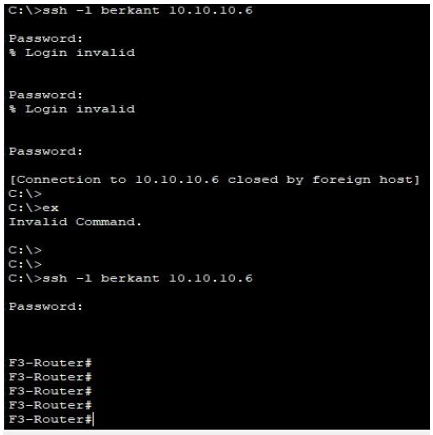


Şekil 13: Bu çalışmada, mobil cihazların da ağa kablosuz olarak erişebilmesi amacıyla "Marmara" adında bir WiFi ağı oluşturulmuştur. Access Point üzerinden yapılandırılan bu kablosuz ağda, SSID adı "Marmara" olarak belirlenmiş ve WPA2-PSK şifreleme yöntemiyle güvenli hale getirilmiştir. Şifre olarak "Marmara123" tanımlanmıştır. Daha sonra dizüstü bilgisayar, tablet ve akıllı telefon gibi cihazlar bu WiFi ağına bağlanarak internet erişimi ve ağ içi iletişimleri başarıyla gerçekleştirmiştir. Bu sayede, hem kablolu hem de kablosuz cihazlar aynı yerel ağ yapısında birleştirilmiştir..

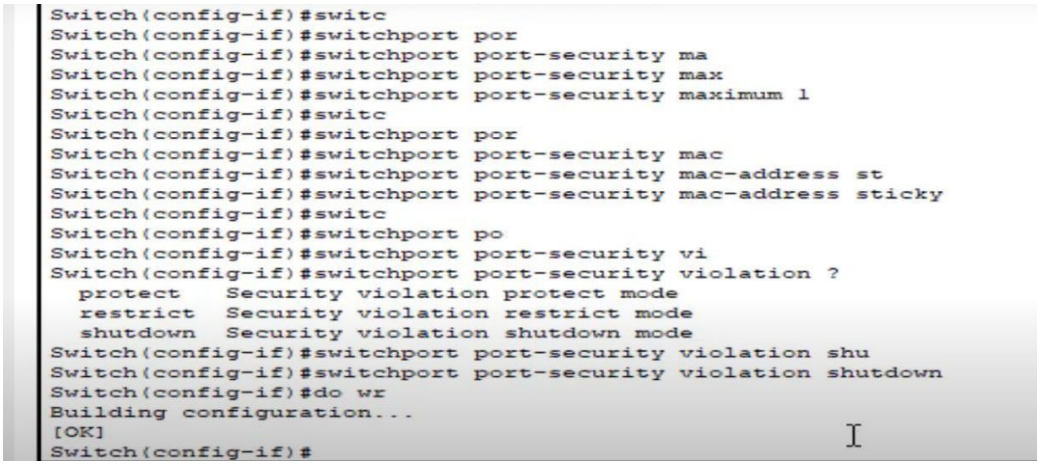


Şekil 14: Bu adımda, uzaktan güvenli erişim sağlamak amacıyla her bir router için SSH (Secure Shell) yapılandırması gerçekleştirilmiştir. SSH yapılandırması için öncelikle router üzerinde bir alan adı (domain name) tanımlanmış ve ardından kullanıcı adı ile şifre belirlenmiştir. Daha sonra RSA anahtarları oluşturularak router'ın şifreli bağlantılar için hazır hale gelmesi sağlanmıştır.

Yapılandırma işlemleri sırasında ip domain-name, username, crypto key generate rsa komutları kullanılmış ve 1024 bitlik RSA anahtarı üretilmiştir. Ayrıca VTY hatları üzerinden sadece SSH erişimine izin verilerek güvenli bağlantı sınırlandırılmıştır. Görselde görüldüğü üzere sonrasında bilgisayardan router'a SSH bağlantısı başarıyla sağlanmış ve parola ekranı görüntülenmiştir. Bu yapılandırma sayesinde ağ yöneticileri, router cihazlarına şifreli ve güvenli bir şekilde uzaktan erişebilmektedir.



Şekil 15: Yapılandırılan SSH bağlantısının doğruluğunu test etmek amacıyla bir istemci cihaz üzerinden ssh -l gtech 10.10.10.1 komutu kullanılarak hedef router'a erişim sağlanmıştır. Kullanıcı adı ve şifre doğru girildikten sonra komut satırına erişim başarılı bir şekilde gerçekleştirilmiştir. Görselde de görüldüğü üzere "F2-Router>" ifadesi, kullanıcı oturumunun router üzerinde aktif olduğunu göstermektedir. Bu test ile SSH yapılandırmasının doğru şekilde çalıştığı ve uzaktan güvenli bağlantının sağlandığı doğrulanmıştır.



Şekil 16: Güvenli ağ erişimini sağlamak amacıyla, bir switch portuna sadece belirli bir bilgisayarın bağlanabilmesi için port-security özelliği yapılandırılmıştır. Bu yapılandırmada, port güvenliği aktif hale getirilmiş, maksimum bir cihazın bağlanmasına izin verilmiş ve MAC adresi otomatik olarak öğrenilerek hafızaya alınmıştır (sticky özelliği). Ayrıca, yetkisiz bir cihaz bağlantı kurmaya çalıştığında portun kapanması için “shutdown” modu etkinleştirilmiştir. Böylece fiziksel erişim kontrolü sağlanarak ağ güvenliği artırılmıştır.