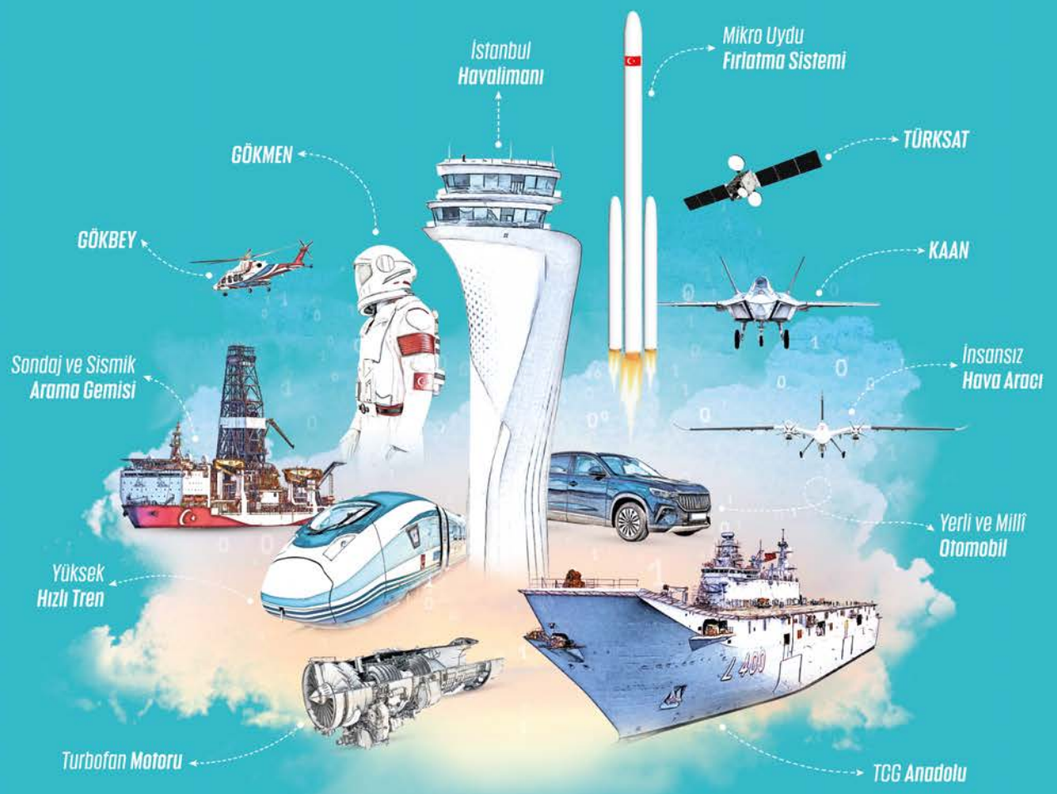
Bu kitaba sığmayan daha neler var!

eba
www.eba.gov.tr

Karekodu okut, bu kitapla ilgili EBA içeriklerine ulaş!

Teknoloji Yolculuğumuz



BU DERS KİTABI MİLLÎ EĞİTİM BAKANLIĞINCA
ÜCRETSİZ OLARAK VERİLMİŞTİR.
PARA İLE SATILAMAZ.

ISBN: 978-975-11-8790-1

Bandrol Uygulamasına İlişkin Usul ve Esaslar Hakkında Yönetmeliğin Beşinci Maddesinin İkinci Fıkrası Çerçevesinde Bandrol Taşıması Zorunlu Değildir.

SİBER GÜVENLİK ALANI

AĞ TEKNOLOJİLERİ

10 DERS MATERYALİ

MESLEKİ VE TEKNİK ANADOLU LİSESİ

SİBER GÜVENLİK ALANI



AĞ TEKNOLOJİLERİ

10

DERS MATERYALİ

MESLEKİ VE TEKNİK ANADOLU LİSESİ

SİBER GÜVENLİK ALANI

AĞ TEKNOLOJİLERİ

10

DERS MATERYALİ

YAZARLAR

Gönül ATEŞ YILDIZ
Mustafa ALGÜL
Özgü ASKER

MİLLÎ EĞİTİM BAKANLIĞI YAYINLARI 9859
YARDIMCI VE KAYNAK KİTAPLAR DİZİSİ 3311

Her hakkı saklıdır ve Millî Eğitim Bakanlığına aittir. Ders materyalinin metin, soru ve şekilleri kısmen de olsa hiçbir surette alınıp yayımlanamaz.

HAZIRLAYANLAR

Dil Uzmanı
Erman Erşan YORGANCILAR

Program Geliştirme Uzmanı
Ali DOĞAN

Rehberlik Uzmanı
Yeliz GENÇTAV

Ölçme ve Değerlendirme Uzmanı
Mustafa ÇELİK

Görsel Tasarım Uzmanı
Mehmet YILMAZ

ISBN: 978-975-11-8790-1

Millî Eğitim Bakanlığının 24.12.2020 gün ve 18433886 sayılı oluru ile Meslekî ve Teknik Eğitim Genel Müdürlüğünce ders materyali olarak hazırlanmıştır.



İSTİKLÂL MARŞI

Korkma, sönmez bu şafaklarda yüzen al sancak;
Sönmeden yurdumun üstünde tüten en son ocak.
O benim milletimin yıldızıdır, parlayacak;
O benimdir, o benim milletimindir ancak.

Çatma, kurban olayım, çehreni ey nazlı hilâl!
Kahraman ırkıma bir gül! Ne bu şiddet, bu celâl?
Sana olmaz dökülen kanlarımız sonra helâl.
Hakkıdır Hakk'a tapan milletimin istiklâl.

Ben ezelden beridir hür yaşadım, hür yaşarım.
Hangi çılgın bana zincir vuracakmış? Şaşarım!
Kükremiş sel gibiyim, bendimi çiğner, aşarım.
Yırtarım dağları, enginlere sığmam, taşarım.

Garbın âfâkını sarmışsa çelik zırhlı duvar,
Benim iman dolu göğsüm gibi serhaddim var.
Ulusun, korkma! Nasıl böyle bir imanı boğar,
Medeniyyet dediğin tek dişi kalmış canavar?

Arkadaş, yurduma alçakları uğratma sakın;
Siper et gövdeni, dursun bu hayâsızca akın.
Doğacaktır sana va'dettiği günler Hakk'ın;
Kim bilir, belki yarın, belki yarından da yakın.

Bastığın yerleri toprak diyerek geçme, tanı:
Düşün altındaki binlerce kefensiz yatanı.
Sen şehit oğlusun, incitme, yazıktır, atanı:
Verme, dünyaları alsan da bu cennet vatanı.

Kim bu cennet vatanın uğruna olmaz ki feda?
Şüheda fışkıracak toprağı sıksan, şüheda!
Cânı, cânânı, bütün varımı alsın da Huda,
Etmesin tek vatanımdan beni dünyada cüda.

Ruhumun senden İlâhî, şudur ancak emeli:
Değmesin mabedimin göğsüne nâmahrem eli.
Bu ezanlar -ki şehadetleri dinin temeli-
Ebedî yurdumun üstünde benim inlemeli.

O zaman vecd ile bin secde eder -varsa- taşım,
Her cerîhamdan İlâhî, boşanıp kanlı yaşım,
Fışkırır ruh-ı mücerret gibi yerden na'şım;
O zaman yükselerek arşa değer belki başım.

Dalgalan sen de şafaklar gibi ey şanlı hilâl!
Olsun artık dökülen kanlarımın hepsi helâl.
Ebediyyen sana yok, ırkıma yok izmihlâl;
Hakkıdır hür yaşamış bayrağımın hürriyyet;
Hakkıdır Hakk'a tapan milletimin istiklâl!

Mehmet Âkif Ersoy

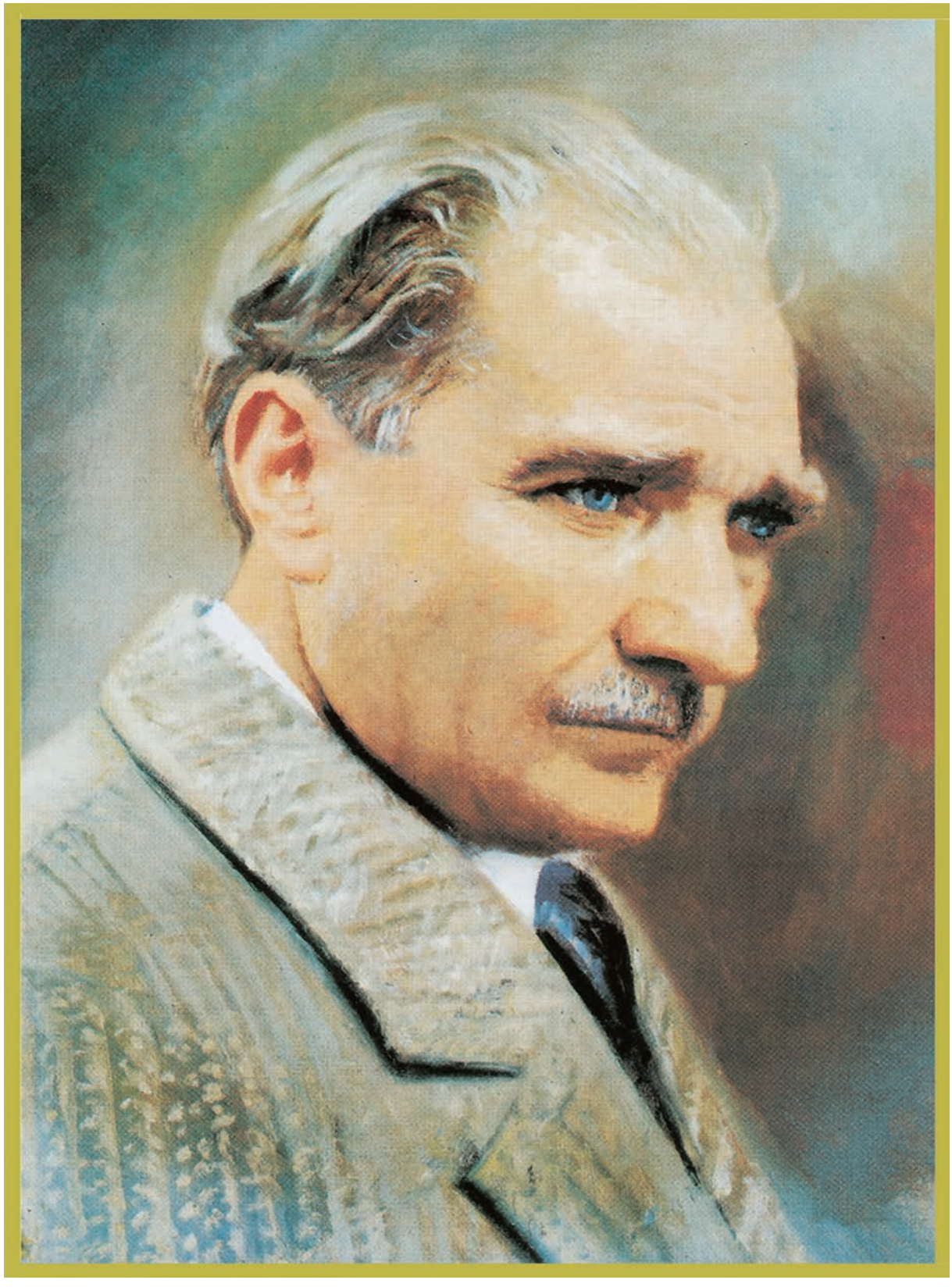
GENÇLİĞE HİTABE

Ey Türk gençliği! Birinci vazifen, Türk istiklâlini, Türk Cumhuriyetini, ilelebet muhafaza ve müdafaa etmektir.

Mevcudiyetinin ve istikbalinin yegâne temeli budur. Bu temel, senin en kıymetli hazinendir. İstikbalde dahi, seni bu hazineden mahrum etmek isteyecek dâhilî ve hâricî bedhahların olacaktır. Bir gün, istiklâl ve cumhuriyeti müdafaa mecburiyetine düşersen, vazifeye atılmak için, içinde bulunacağın vaziyetin imkân ve şeraitini düşünmeyeceksin! Bu imkân ve şerait, çok namüsait bir mahiyette tezahür edebilir. İstiklâl ve cumhuriyetine kastedecek düşmanlar, bütün dünyada emsali görülmemiş bir galibiyetin mümessili olabilirler. Cebren ve hile ile aziz vatanın bütün kaleleri zapt edilmiş, bütün tersanelerine girilmiş, bütün orduları dağıtılmış ve memleketin her köşesi bilfiil işgal edilmiş olabilir. Bütün bu şeraitten daha elîm ve daha vahim olmak üzere, memleketin dâhilinde iktidara sahip olanlar gaflet ve dalâlet ve hattâ hıyanet içinde bulunabilirler. Hattâ bu iktidar sahipleri şahsî menfaatlerini, müstevlîlerin siyasî emelleriyle tevhit edebilirler. Millet, fakr u zaruret içinde harap ve bîtap düşmüş olabilir.

Ey Türk istikbalinin evlâdı! İşte, bu ahval ve şerait içinde dahi vazifen, Türk istiklâl ve cumhuriyetini kurtarmaktır. Muhtaç olduğun kudret, damarlarındaki asil kanda mevcuttur.

Mustafa Kemal Atatürk



MUSTAFA KEMAL ATATÜRK

İÇİNDEKİLER

DERS MATERYALİNİN TANITIMI 12

1. ÖĞRENME BİRİMİ : AĞ ANAHTARLAMA 15

1.1. ANAHTARLAMA SÜRECİ 16

1.1.1. Ethernet Çerçevesinin (Ethernet Frame) İletim Süreci ve MAC Adresi Tablosunun Oluşması 17

1.1.2. Genel Yayın Alanı (Broadcast Domain) 20

1.1.3. Çarpışma Alanı (Collision Domain) 21

1.2. SANAL YEREL ALAN AĞLARI [VLAN (VIRTUAL LOCAL AREA NETWORK)] 23

1.2.1. Anahtar Portunun Operasyon Modları 24

1.2.2. VLAN Türleri 26

1.2.3. Sanal Yerel Alan Ağları Arası Yönlendirme [IVR (Inter VLAN Routing)] 35

1.3. LAN YEDEKLİLİĞİ (LOCAL AREA NETWORK REDUNDANCY) 47

1.3.1. Kapsayan Ağaç Protokolü [STP (Spanning Tree Protocol)] 47

1.3.1.1. Kapsayan Ağaç Protokolünün Çalışma Süreci 48

1.3.1.2. İki Ağ Anahtarının İki Fiziksel Portla Bağlanması 51

1.3.1.3. STP Sürecinde Port Durumları 52

1.3.1.4. Kapsayan Ağaç Protokolü Türleri 52

1.3.2. Port Kümeleme (Link Aggregation) 57

1.3.2.1. Port Kümelemenin Avantajları 58

1.3.2.2. Port Kümeleme Uygulamasında Dikkat Edilmesi Gereken Hususlar 58

1.3.2.3. Port Kümeleme Yöntemleri 58

ÖLÇME VE DEĞERLENDİRME 65

2. ÖĞRENME BİRİMİ : AĞ YÖNLENDİRME 67

2.1. STATİK YÖNLENDİRME 68

2.1.1. Komutlar ve Yapılandırma 68

2.1.2. Yönlendirme Tablosu 69

2.1.3. Statik Yönlendirme Türleri 70

2.1.3.1. Standart Statik Rota 70

2.1.3.2. Tamamen Tanımlı Statik Rota 73

2.1.3.3. Varsayılan Statik Rota 75

2.1.3.4. Özet Statik Rota 77

2.1.3.5. Kayan Statik Rota 81

2.2. DİNAMİK YÖNLENDİRME 84
2.2.1. Dinamik Yönlendirmede Karar Verme ve Yönlendirme Kararı 86
2.2.2. RIP ve RIPv2 Protokolü 87
2.2.3. EIGRP Protokolü 91
2.2.4. OSPF 95
2.2.4.1. OSPF Paketleri 96
2.2.4.2. OSPF İşleyiş Durumları 99
2.2.4.3. DR ve BDR Cihaz Seçim Süreci 100
2.2.4.4. OSPF'de Ağ Topolojisi 101
2.2.4.5. OSPF'de Maliyet Hesaplama 102
2.2.4.6. OSPF Ağlarında Yapılandırma 106
2.2.5. BGP 112
2.2.5.1. BGP Mesaj Türleri 113
2.2.5.2. BGP'de Komşuluk 113
2.2.5.3. BGP Karar Verme Süreci 115
2.2.5.4. BGP Yapılandırma Ayarları 115
ÖLÇME VE DEĞERLENDİRME 123

3. ÖĞRENME BİRİMİ : KABLOSUZ AĞ TEKNOLOJİLERİ 125
3.1. KABLOSUZ AĞLAR 126
3.1.1. Kablosuz Ağ Türleri 131
3.1.2. Kablosuz Ağ Cihazları 133
3.1.3. WLAN (IEEE 802.11) Standartları 136
3.1.4. WLAN (IEEE 802.11) Topoloji Modları 137
3.1.5. WLAN (IEEE 802.11) Çerçeve Yapisi 139
3.1.6. CSMA/CA (Carrier Sense Multiple Access With Collision Avoidance) 141
3.1.7. Kablosuz İstemcilerin Kablosuz Ağa Bağlanma Süreci 142
3.1.8. 2.4 GHz VE 5 GHz Frekanslarının Kanal Yapısı 146
3.2. KABLOSUZ AĞ YAPILANDIRMASI 150
ÖLÇME VE DEĞERLENDİRME 163

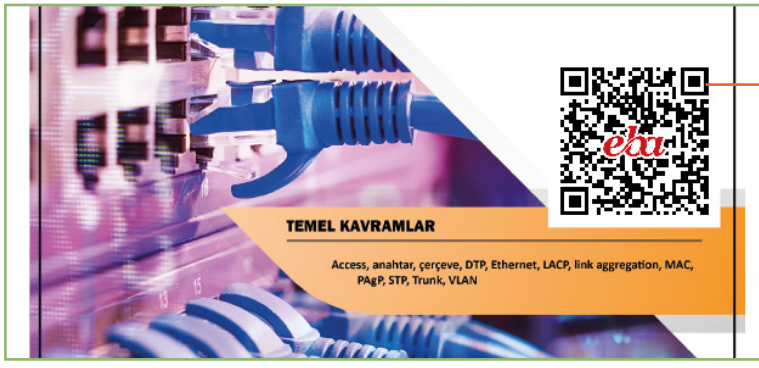
4. ÖĞRENME BİRİMİ : SANAL ÖZEL AĞLAR 165
4.1. SANAL ÖZEL AĞLAR [VPN (VIRTUAL PRIVATE NETWORK)] VE TÜRLERİ 166
4.1.1. Uzaktan Erişim VPN (REMOTE ACCESS VPN) 167
4.1.1.1. İstemcili (Client Based) VPN 167
4.1.1.2. İstemcisiz (Clientless) VPN 167
4.1.1.3. SSL/TLS (Secure Sockets Layers/Transport Layer Security) Protokolleri 167
4.1.2. Siteden Siteye VPN 168
4.1.2.1. GRE IP Tünelleme Protokolü 168

4.1.2.2. IPsec VPN 169
4.1.2.3. IPsec Framework (IPsec Çerçevesi) 169
4.1.2.4. IPsec VPN Üzerinden GRE IP Tüneli 174
4.1.3. MPLS Sanal Özel Ağlar 175
4.2. SANAL ÖZEL AĞ [VPN (VIRTUAL PRIVATE NETWORK)] UYGULAMALARI 176
ÖLÇME VE DEĞERLENDİRME 199

5. ÖĞRENME BİRİMİ : YAZILIM TABANLI AĞ (SDN) TEKNOLOJİSİ 201
5.1. YAZILIM TABANLI AĞLAR 202
5.1.1. Ağ Otomasyonu 202
5.1.2. Yazılım Tabanlı Ağ Mimarisi Bileşenleri 207
5.1.3. Yazılım Tabanlı Ağlarda Denetleyiciler 207
5.1.4. Kuzey ve Güney Yönlü Arayüzler 209
5.1.5. OpenFlow Protokolü 210
5.2. SPİNE-LEAF TEKNOLOJİSİ 216
5.2.1. Üç Katmanlı Ağ Mimarisi 217
5.2.2. Omurga-Yaprak Mimarisi 218
ÖLÇME VE DEĞERLENDİRME 220

CEVAP ANAHTARLARI 221
KAYNAKÇA 223

DERS MATERYALİNİN TANITIMI



Öğrenme birimi içinde yer alan uygulamara erişim sağlamak için kullanılan karekodu gösterir.

İÇİNDEKİLER

DERS MATERYALİNİN TANITIMI.....12
1. ÖĞRENME BİRİMİ : AĞ ANAHTARLAMA.....15
1.1. ANAHTARLAMA SÜRECİ.....16

Konuları ve konuların bulunduğu sayfa numaralarını gösterir.

1. ÖĞRENME BİRİMİ

Öğrenme biriminin numarasını gösterir.

AĞ ANAHTARLAMA

Öğrenme biriminin adını gösterir.

Farklı ağları statik yönlendirme protokolü kullanarak yapılandırma işlemini verilen adımlar doğrultusunda gerçekleştiriniz.

1. UYGULAMA

Öğrenme birimi içindeki uygulama faaliyetlerini gösterir.

HAZIRLIK ÇALIŞMALARI

1. MAC adresleriyle anahtarlama süreci nasıl gerçekleşir? Düşüncelerinizi arkadaşlarınızla paylaşınız.

2. Yerel ağ bağlantısı içindeki ağ anahtar cihazlarının veri iletme kapasitesini artırarak darboğaz oluşmasını engellemek için neler yapılabilir? Düşüncelerinizi arkadaşlarınızla paylaşınız.



Konulara ön hazırlık yapmak, öğrenme birimine öğrenciyi hazırlamak amacıyla yapılacak çalışmaları gösterir.

ARAŞTIRMA Ağ Otomasyonu

Ağ otomasyonunda kullanılan araçlar ve programlama dilleri hakkında araştırma yapınız. Ağ otomasyonu için kullanılan araçlar ve kullanımları hakkında bir rapor hazırlayınız. Ağ otomasyonu araçlarını kullanarak cihaz yapılandırma uygulamalarını gerçekleştiriniz ve uygulamaların ekran görüntülerine raporunuzda yer veriniz.

Öğrenme birimi ile ilgili araştırma etkinliğini gösterir.

ÖLÇÜTLER	EVET	HAYIR
1. Ağ topolojisinin çizimini gerçekleştirdi.		
2. Ağ anahtarlarında uygun olan VLAN oluşturma işlemini gerçekleştirdi.		
3. Ağ anahtarlarında portları ilgili VLAN'a tanımladı.		
4. Geleneksel IVR yöntemini gerçekleştirdi.		
5. Router On A Stick yöntemiyle IVR işlemini gerçekleştirdi.		

Ders materyali içeriğinde yer alan kontrol listesini gösterir.

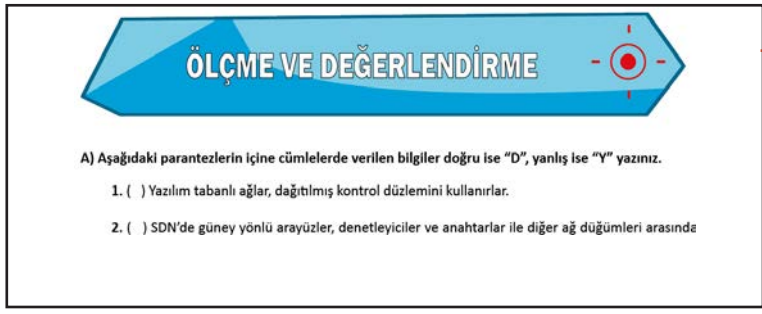
NOT: Ağ anahtarında **show interfaces trunk** komutu kullanılarak Trunk portlarla ilgili bilgiler görüntülenir.

Konuları, uygulamaları pekiştirici ve destekleyici ek bilgileri gösterir.

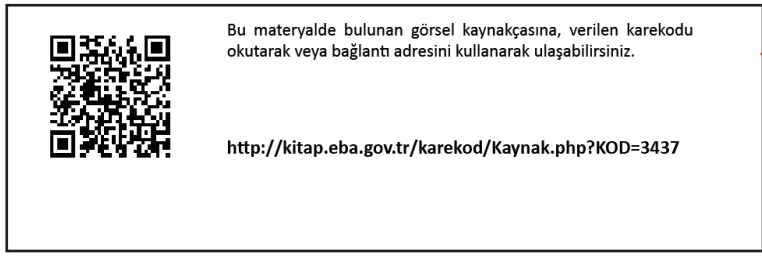
SIRA SİZDE

Görsel 2.116'daki topolojiye göre OSPF, RIP ve EIGRP ile yapılandırılan ağların BGP protokolü ile iletişim kurmasını sağlayınız.

Öğrenme birimi içindeki sıra sizde çalışmalarını gösterir.



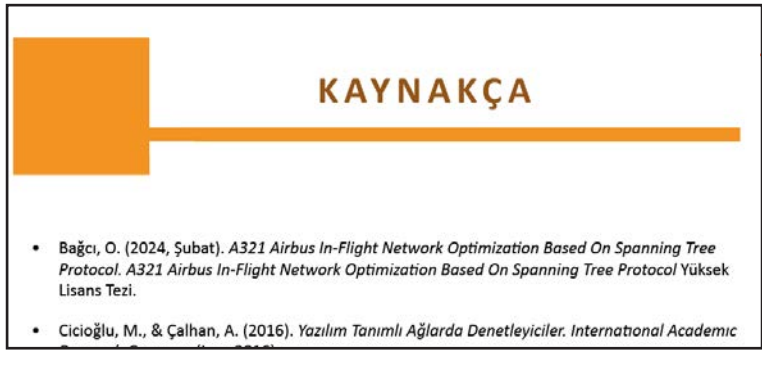
Öğrenme birimi ile ilgili ölçme ve değerlendirme çalışmalarını gösterir.



Kitapta yer alan görsellerin ve bağlantı adreslerinin kaynakçasını gösterir.



Öğrenme birimi ile ilgili ölçme ve değerlendirme sorularının cevaplarını gösterir.



Ders materyali içeriğinde yer alan alıntıların yapıldığı kaynakçaları gösterir.

1. ÖĞRENME BİRİMİ

AĞ ANAHTARLAMA

KONULAR

1.1. ANAHTARLAMA SÜRECİ

1.2. SANAL YEREL ALAN AĞLARI [VLAN (VIRTUAL LOCAL AREA NETWORK)]

1.3. LAN YEDEKLİLİĞİ (LOCAL AREA NETWORK REDUNDANCY)

NELER ÖĞRENECEKSİNİZ?

- Ethernet çerçevesinin iletim işlemlerini açıklama
- Sanal yerel alan ağları (VLAN) oluşturarak yönlendirme işlemleri yapma
- Anahtarlamada yerel alan ağlarının yedekliliğini yapma



TEMEL KAVRAMLAR

Access, anahtar, çerçeve, DTP, Ethernet, LACP, link aggregation, MAC, PAgP, STP, Trunk, VLAN

HAZIRLIK ÇALIŞMALARI

1. MAC adresleriyle anahtarlama süreci nasıl gerçekleşir? Düşüncelerinizi arkadaşlarınızla paylaşınız.

2. Yerel ağ bağlantısı içindeki ağ anahtar cihazlarının veri iletme kapasitesini artırarak darboğaz oluşmasını engellemek için neler yapılabilir? Düşüncelerinizi arkadaşlarınızla paylaşınız.

1.1. ANAHTARLAMA SÜRECİ

Yerel alan ağı [LAN (Local Area Network)] haberleşmesinde yaygın olarak Ethernet protokolü kullanılır. Ethernet protokolü, IEEE 802.3 [IEEE (Institute of Electrical and Electronics Engineers)] standardıyla tarif edilir ancak aralarında küçük değişiklikler bulunur. Ethernet anahtarlaması, OSI (Open Systems Interconnection) referans modeli ikinci katmandaki süreci ele alır ve yerel alan ağına bağlı cihazlar arasındaki veri akışını yönetir. Bu süreçte Ethernet ağ anahtarları (switch) kullanılır (Görsel 1.1).



Görsel 1.1: Ethernet ağ anahtarı

Anahtarlama işleminde, bir uç cihazdan (bilgisayar, sunucu, ağ yazıcısı vb.) gelen çerçevenin (frame) hedefe anahtarlanması sağlanır. Anahtarlamada kullanılan iki iletim yöntemi şöyledir:

1. **Depola ve İlet Anahtarlama (Store and Forward Switching):** Bu yöntemde, Ethernet çerçevesinin tamamı anahtara alınır ve tampon belleğe kaydedilir. Çerçevenin sonunda bulunan **çerçeve kontrol dizisi [FCS (Frame Check Sequence)] alanı**nda, **döngüsel artıklık denetimi [CRC (Cyclic Redundancy Check)]** yapılır. Daha sonra hedef MAC adresi ve çıkış portu tespit edilerek çerçeve hedef cihaza iletilir.

2. **Kesmeli Anahtarlama (Cut Trough Switching):** Bu yöntem, düşük gecikme süresine ihtiyaç duyulan yüksek performanslı ağlarda tercih edilir. Ethernet çerçevesi anahtara giriş yaptığında çerçevenin hedef MAC adresi ve çıkış portu tespit edildikten sonra iletim süreci başlatılır. Kesmeli anahtarlama yönteminin en büyük avantajı, veri paketlerinin hedefe çok hızlı bir şekilde iletilmesidir.



Görsel 1.2: Ethernet kartı

Uç cihazlar, **ağ arayüz kartı [NIC (Network Interface Card)]** ile ağa bağlanır. Ethernet anahtarlamasında kullanılan **NIC kartı**na **Ethernet kartı** denir (Görsel 1.2).

Yerel alan ağı haberleşmesinde cihazlar, NIC kartı üzerinde bulunan 48 bitlik benzersiz bir adresi kullanır. Bu adrese **MAC (Media Access Control)** adresi denir. MAC adresi, ağ arayüz kartına üretim aşamasında kodlanır ve **fiziksel adres** olarak da isimlendirilir. Uç cihazlar, ağ anahtarına uçları RJ-45 konnektörle sonlandırılmış ağ kablosuyla bağlanır (Görsel 1.3).



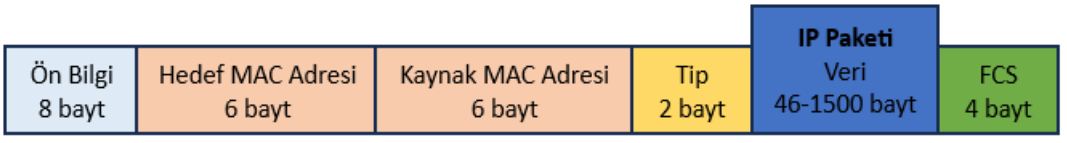
Görsel 1.3: Ağ kablosu

1.1.1. Ethernet Çerçevesinin (Ethernet Frame) İletim Süreci ve MAC Adresi Tablosunun Oluşması

Ethernet çerçevesinin iletim süreci dört aşamada gerçekleşir.

1. Çerçevenin Oluşturulması

Kaynak cihaz, OSI referans modeli üçüncü katmanından kapsüllenerek gelen IP paketini alır ve bunu Ethernet çerçevesi olarak yeniden kapsüller (Görsel 1.4).

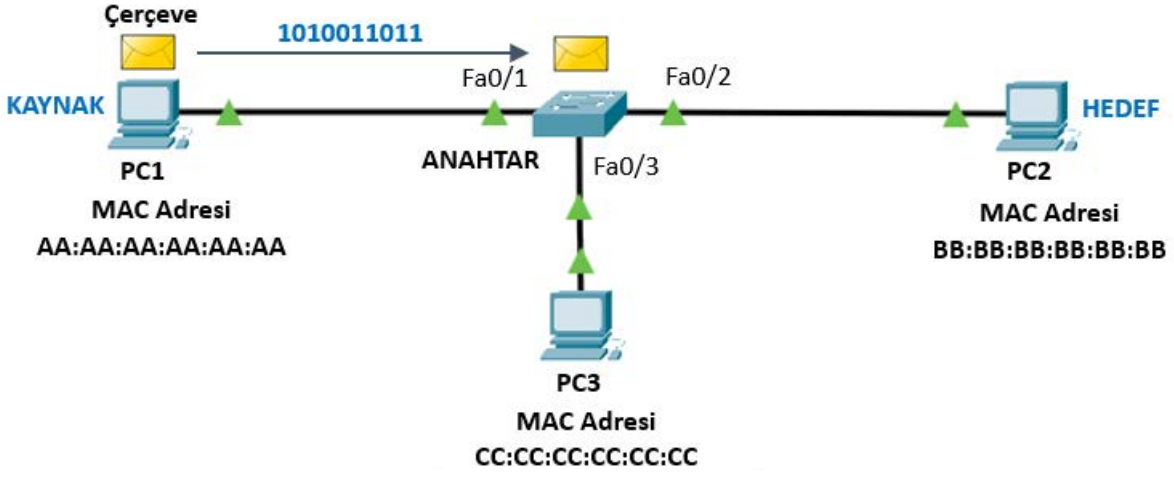


Görsel 1.4: Ethernet çerçevesi

Çerçevenin başlığında (header) ön bilgi, hedef MAC adresi, kaynak MAC adresi ve tip alanı yer alır. Bu bilgiler, ağ anahtarı tarafından okunarak çerçevenin doğru cihaza anahtarlanmasını sağlar. Taşınacak veri, çerçevenin veri (payload) kısmında yer alır. Çerçevenin sonlandırma kısmında ise çerçeve kontrol dizisi (FCS) yer alır. Hata tespiti için bir CRC kodu hesaplanır ve bu kod çerçevenin FCS alanına eklenir. Alıcı cihaz, çerçeveyi aldıktan sonra tekrar bir CRC kodu oluşturur. İki CRC kodunun eşleşmesi çerçevenin bozulmadan hedefe ulaştığını gösterir.

2. Çerçevenin Ağ Ortamına Gönderilmesi

Kaynak cihaz, oluşturulan çerçeveyi fiziksel katman (1. katman) üzerinden iletir. Çerçeve, ağda elektriksel sinyallere dönüştürülerek hedefe doğru yol alır. Çerçeve, ilk olarak kaynak cihazın bağlı olduğu ağ anahtarına ulaşır (Görsel 1.5).



Görsel 1.5: PC1'den fiziksel katmana gönderilen çerçevenin anahtara ulaşması

Çerçevenin ağ anahtarına giriş yaptığı porta **giriş noktası (ingress)** denir. Çerçeve anahtara giriş yaptıktan sonra anahtar, çerçeve başlığındaki kaynak cihazın MAC adresini okur ve öğrenir. Anahtar öğrendiği MAC adresini, MAC adres tablosunda çerçevenin giriş yaptığı porta kaydeder (Tablo 1.1).

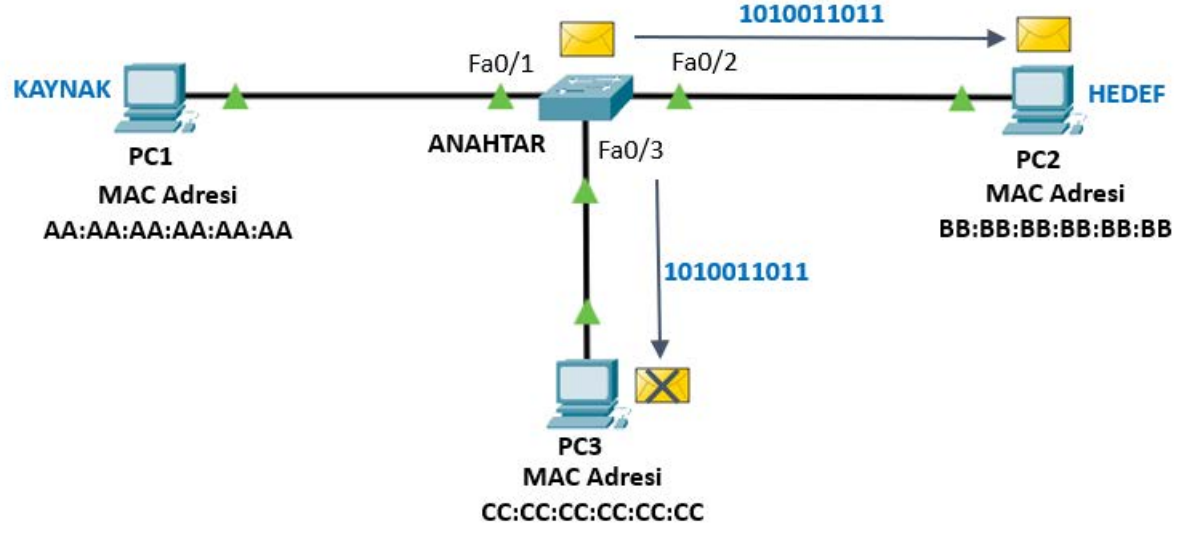
Tablo 1.1: PC1'in MAC Adresinin Anahtarın MAC Adresi Tablosuna Kaydedilmesi

MAC Adresi Tablosu			
Vlan Numarası	**Mac Adresi**	**Tip**	**Portlar**
1	AA:AA:AA:AA:AA:AA	Dinamik	Fa0/1

Anahtar tarafından öğrenilen MAC adresleri, sınırsız süreyle bellekte tutulmaz. Çoğu ağ anahtarında bu süre yaklaşık 300 saniyedir. Bu süre boyunca MAC adresinin kayıtlı olduğu porttan herhangi bir ağ trafiği geçmezse anahtar, bu MAC adresini tablosundan siler. Bu işlem, anahtarın sınırlı bellek kapasitesine sahip olması nedeniyle yapılır. Ağda yeniden trafik oluştuğunda anahtar, MAC adresini tekrar öğrenme sürecine girer.

3. Çerçevenin Hedef Cihaza Anahtarlanması

Çerçevenin ağ anahtarından çıkış yaptığı porta **çıkış noktası (egress)** denir. Çerçeveyi alan anahtar, hedef cihazın MAC adresine karşılık gelen portu MAC adresi tablosunu kontrol ederek belirledikten sonra çerçeveyi bu port üzerinden iletir. Çerçeve, yine fiziksel katman aracılığıyla hedef cihaza doğru yönlendirilir. Hedef cihazın MAC adresi, anahtarın MAC adresi tablosunda kayıtlı değilse anahtar, çerçeveyi çerçevenin geldiği port haricindeki aktif tüm portlara iletir. Bu sürece **tekil yayın seli (unicast flooding)** denir. Çerçevenin kendisine ait olmadığını doğrulayan cihazlar, çerçeveyi çöpe atar (Görsel 1.6).

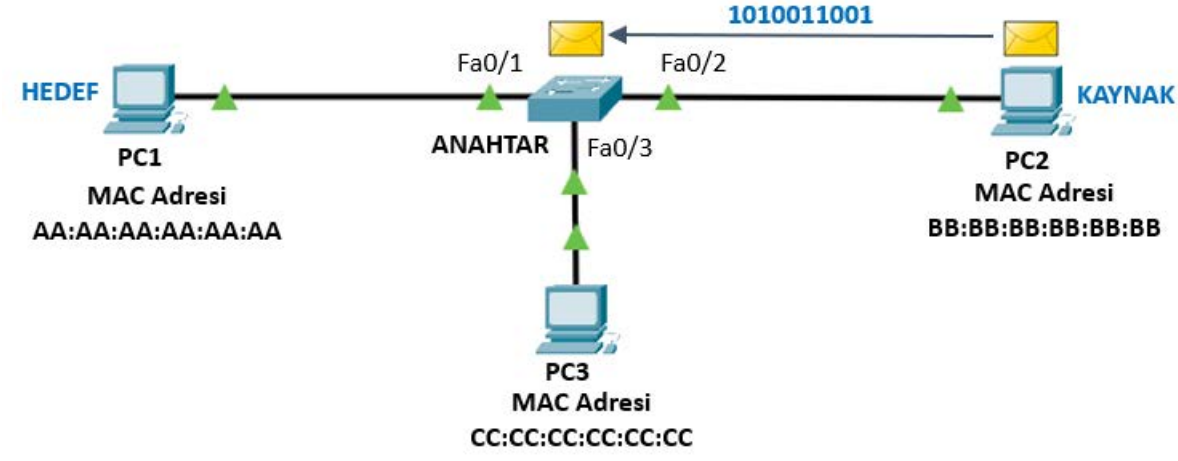


Görsel 1.6: Çerçevenin tekil yayın seli şeklinde hedef cihaza ulaştırılması

MAC adresleri anahtar tarafından öğrenildiğinde **tekil yayın seli paket iletimi** gerçekleşmez. Çerçeve, sadece hedef cihaza tekil yayın şeklinde iletilir.

4. Çerçevenin Hedef Cihaza Ulaşması

Hedef cihaz, kendisine ulaşan çerçeveyi aldıktan sonra çerçevenin başlığındaki hedef MAC adresini kontrol ederek kendisine ait olup olmadığını doğrular. Eğer çerçeve, hedef cihaza aitse cihaz çerçeveyi işler ve veri kısmını üst katmanlara iletir. Hedef cihaz veriyi işledikten sonra kaynak cihaza veri iletecekse yeniden bir çerçeve oluşturur ve fiziksel katmana iletir. Yeni oluşturulan çerçevede kendisi, kaynak ve diğer cihaz hedef olur (Görsel 1.7).



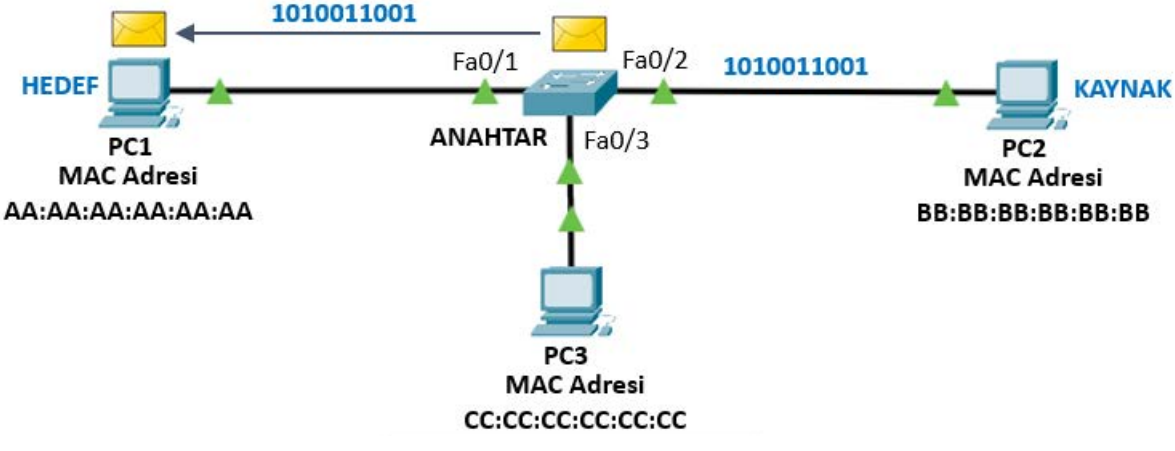
Görsel 1.7: PC2'den fiziksel katmana gönderilen çerçevenin anahtara ulaşması

Çerçeve, anahtar portuna ilk kez giriş yaptığında kaynak cihazın MAC adresi, çerçeve başlığından okunarak ilgili port ile birlikte MAC adresi tablosuna kaydedilir (Tablo 1.2).

Tablo 1.2: PC2'in MAC Adresinin Anahtarın MAC Adresi Tablosuna Kaydedilmesi

MAC Adresi Tablosu			
Vlan Numarası	**Mac Adresi**	**Tip**	**Portlar**
1	AA:AA:AA:AA:AA:AA	Dinamik	Fa0/1
1	BB:BB:BB:BB:BB:BB	Dinamik	Fa0/2

Çerçeveyi alan anahtar, çerçeve başlığından hedef cihazın MAC adresini okur. Bu adresi MAC adresi tablosundan kontrol eder ve çerçeveyi çıkartacağı portu tespit eder. Son olarak, çerçeveyi belirlenen çıkış portundan fiziksel katmana ileterek hedef cihaza ulaştırır (Görsel 1.8).



Görsel 1.8: Anahtarın çerçeveyi hedefe tekil yayın olarak iletmesi

Bir Ethernet anahtarının MAC adresi tablosu Görsel 1.9'daki biçimde görülür.

```
Switch#show mac-address-table
          Mac Address Table
-------------------------------------------

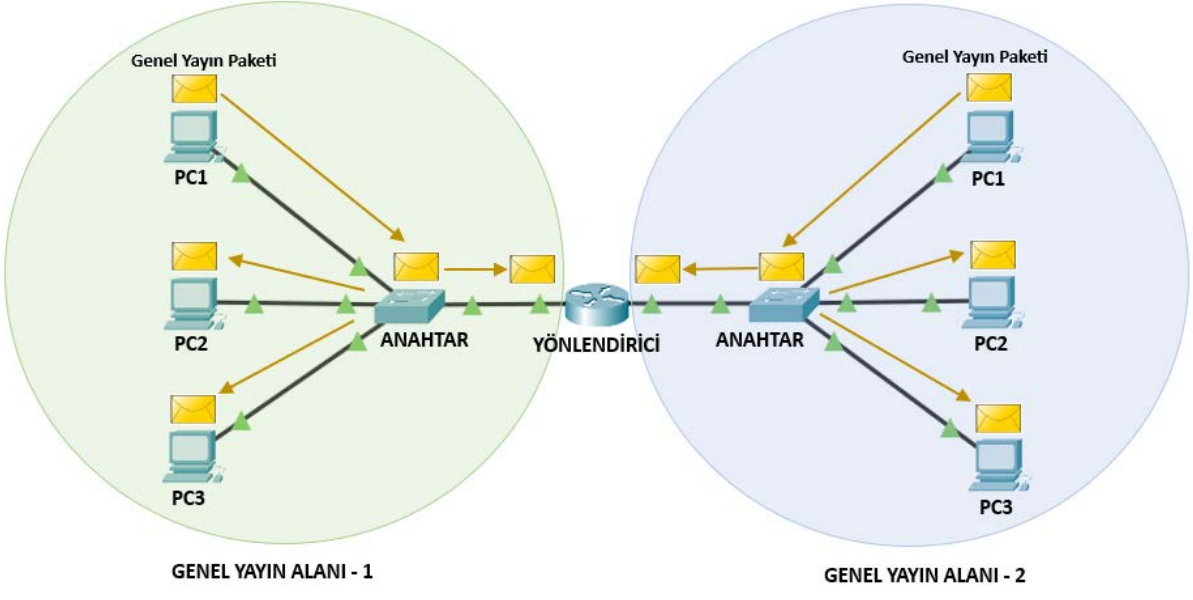
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    0001.634d.5546    DYNAMIC     Fa0/1
   1    0003.e4b2.50ac    DYNAMIC     Fa0/3
   1    0060.2f35.55ea    DYNAMIC     Fa0/4
   1    0060.477d.19b8    DYNAMIC     Fa0/2
```

Görsel 1.9: Ethernet anahtarının MAC adresi tablosunu görüntüleme

1.1.2. Genel Yayın Alanı (Broadcast Domain)

Genel yayın alanı, bir yerel alan ağı içinde genel yayın paketlerinin o yerel alan ağında bulunan tüm cihazlara iletildiği ve bu alandaki cihazların genel yayın paketlerini alabileceği bölgeyi ifade eder. Bir ağda birden fazla genel yayın alanı bulunabilir. Genel yayın alanları, üçüncü katman bir cihazla (yönlendirici, çok katmanlı anahtar vb.) birbirinden ayrılır. Bir genel yayın alanı içinde bulunan cihazlar sadece kendi genel yayın alanı içindeki cihazlara genel yayın paketlerini iletebilir (Görsel 1.10). Ayrıca yerel alan ağında VLAN'lar [Virtual Local Area Network (Sanal Yerel Alan Ağı)] oluşturarak da genel yayın alanları ayrılır.



Görsel 1.10: Birden fazla genel yayın alanının yönlendiriciyle ayrılması

Genel yayın alanının büyüklüğü, yerel alan ağının performansını etkiler. Çok büyük bir genel yayın alanında aşırı genel yayın trafiği oluşacağı için ağın bant genişliği etkilenir ve ağın performansı düşer. Ayrıca cihazlara gelen her genel yayın paketi, işlemciye yük oluşturur ve bu da enerji tüketimini artırır. Bu nedenle ağ tasarımında genel yayın alanı boyutunun iyi planlanması oldukça önemlidir.

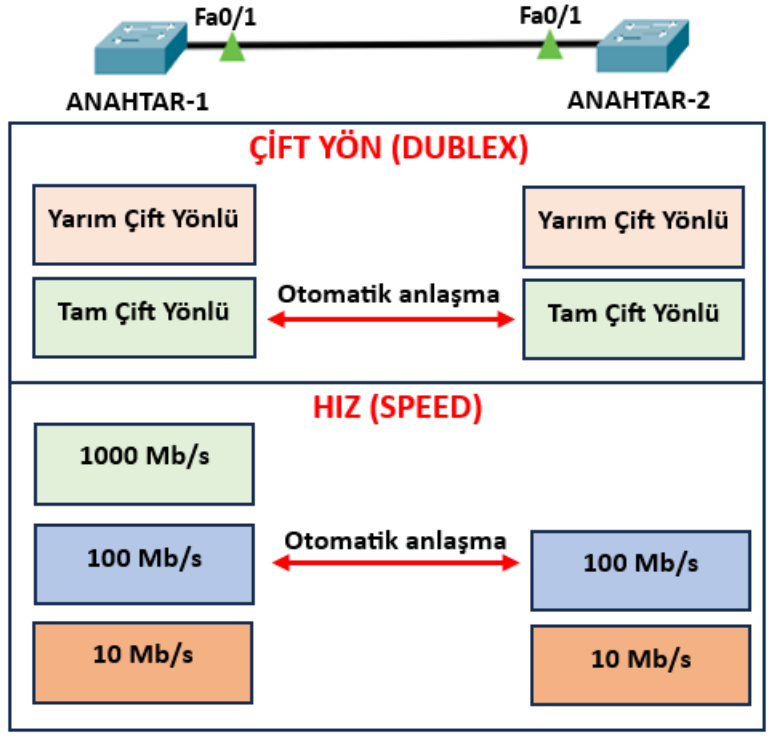
1.1.3. Çarpışma Alanı (Collision Domain)

Çarpışma alanı, ağ iletişiminde iki veya daha fazla cihazın aynı anda veri göndermesiyle çarpışmanın (collision) gerçekleşebileceği bir ağ segmentini ifade eder. Ağ haberleşmesinde çarpışma, istenen bir durum değildir. Anahtarlama cihazlarının arayüzleri **yarım çift yönlü (half dublex)** ve **tam çift yönlü (full dublex)** olmak üzere iki modda çalışır.

1. **Yarım Çift Yönlü:** Bu haberleşme modunda paylaşılmış bir iletim ortamı kullanılır. Bir cihaz, veri alırken gönderme veya veri gönderirken alma işlemi gerçekleştiremez. Veri alma ve gönderme işlemi aynı anda gerçekleşirse bu durumda çarpışma meydana gelir.

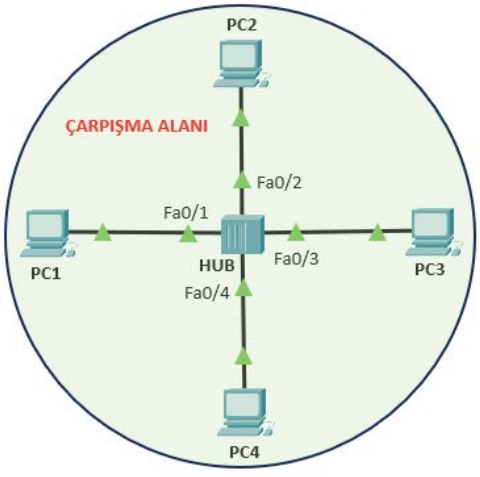
2. **Tam Çift Yönlü:** Bu haberleşme modunda cihazlar, veri alma ve gönderme işlemini aynı anda gerçekleştirebilir.

Ağ anahtarlamasında cihazlar arası çift yön modunun ve port hızlarının eşit olması gereklidir. Çift yön modu ve hız, cihazlar arası **otomatik anlaşma (autonegotiation)** gerçekleştirilerek eşleştirilir (Görsel 1.11). Aksi takdirde cihazlar arası portlar, kapalı duruma geçer ve ağ trafiği durur.

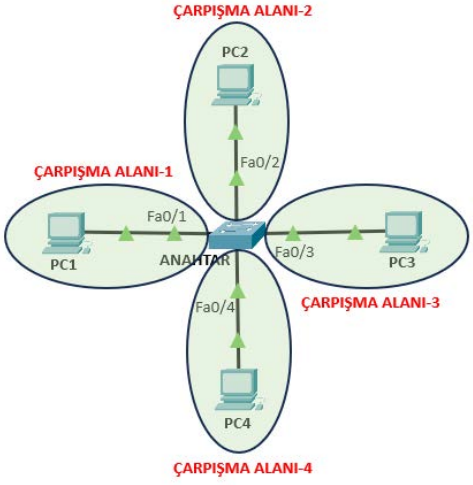


Görsel 1.11: Çift yön modunun ve port hızlarının eşleştirilmesi

Ethernet anahtarları geliştirilmeden önce anahtarlamada hub cihazları yaygın olarak kullanılırdı. **Hub**, OSI referans modeli birinci katmanında (fiziksel katman) çalışan bir cihazdır. Bu nedenle veri, hedefi bulmak için hub cihazının bir portundan giriş yaptıktan sonra herhangi bir kaynak ve hedef adresine bakılmadan gelen port haricindeki aktif tüm portlara gönderilir. Hub, yarım çift yönlü çalışan bir cihaz olduğu için çarpışmaların olması kaçınılmazdır. Hub cihazı kullanılarak gerçekleştirilen Ethernet anahtarlamasında ağ segmenti, **çarpışma alanı** olarak isimlendirilir (Görsel 1.12).



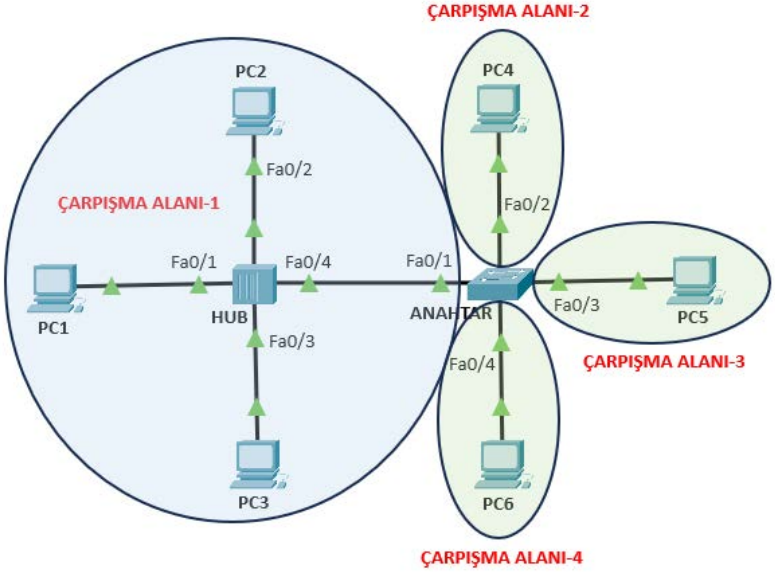
Görsel 1.12: Hub cihazı çarpışma alanı



Görsel 1.13: Anahtar portları çarpışma alanı

Ethernet anahtarlarının portları, varsayılan ayarlarda tam çift yönlü çalışır ancak istenirse port ayarları değiştirilerek yarım çift yönlü yapılandırılabilir. Bu durumda anahtara bağlı ağ segmenti, çarpışma etki alanındadır. Portlar tam çift yönlü çalıştığında her port, kendi çarpışma etki alanındadır (Görsel 1.13).

Tam çift yönlü çalışan portlar, kendi çarpışma etki alanında oldukları için ağ segmentinde çarpışma meydana gelmez. Anahtar portlarından biri hub cihazına bağlandığında o port, hub cihazının çarpışma etki alanına girer (Görsel 1.14).



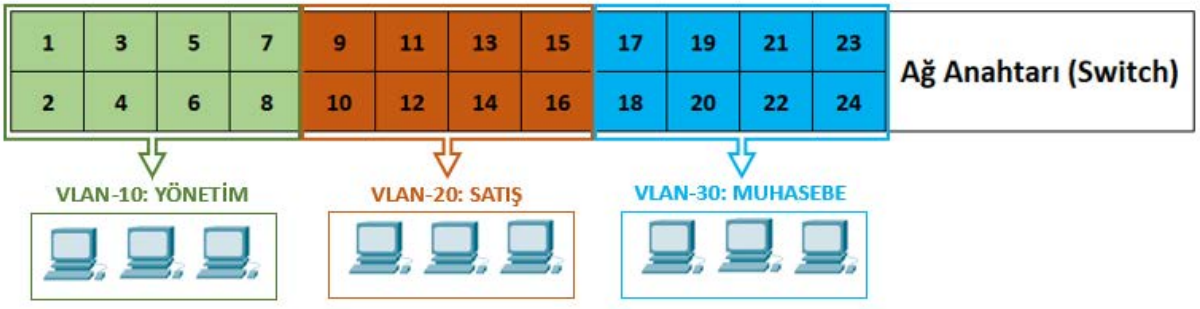
Görsel 1.14: Hub ve anahtar birlikte kullanıldığında oluşan çarpışma alanları

ARAŞTIRMA MAC adresi

MAC adresi tablosu ile ARP tablosu arasındaki farkları araştırınız. Edindiğiniz bilgileri sınıfta arkadaşlarınızla paylaşınız.

1.2. SANAL YEREL ALAN AĞLARI [VLAN (VIRTUAL LOCAL AREA NETWORK)]

Sanal yerel alan ağları, ağ anahtarı üzerindeki fiziksel portları sanal olarak gruplandırarak birbirinden izole edilmiş ağlar oluşturmak için kullanılan OSI referans modeli ikinci katman teknolojisidir (Görsel 1.15).

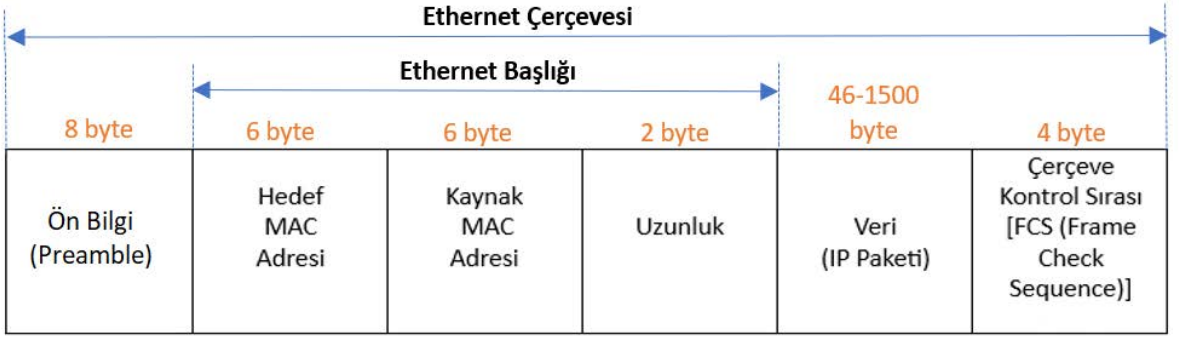


Görsel 1.15: Anahtar üzerinde oluşturulan VLAN grupları

Özellikle büyük ağ topolojilerinde VLAN yapısını kullanmak birçok fayda sağlar. Örneğin büyük bir kurum, kuruluş veya şirkette farklı idari birimler (insan kaynakları, muhasebe, satış, pazarlama, yönetim vb.) için VLAN'lar oluşturularak ve bu idari birimlerdeki kullanıcılar, ilgili VLAN'lara taşınarak hiyerarşik bir yapı oluşturulur. VLAN yapılandırma bilgileri flash hafıza ünitesinde **vlan.dat** dosyasında tutulur. VLAN'ları kullanmanın faydaları şunlardır:

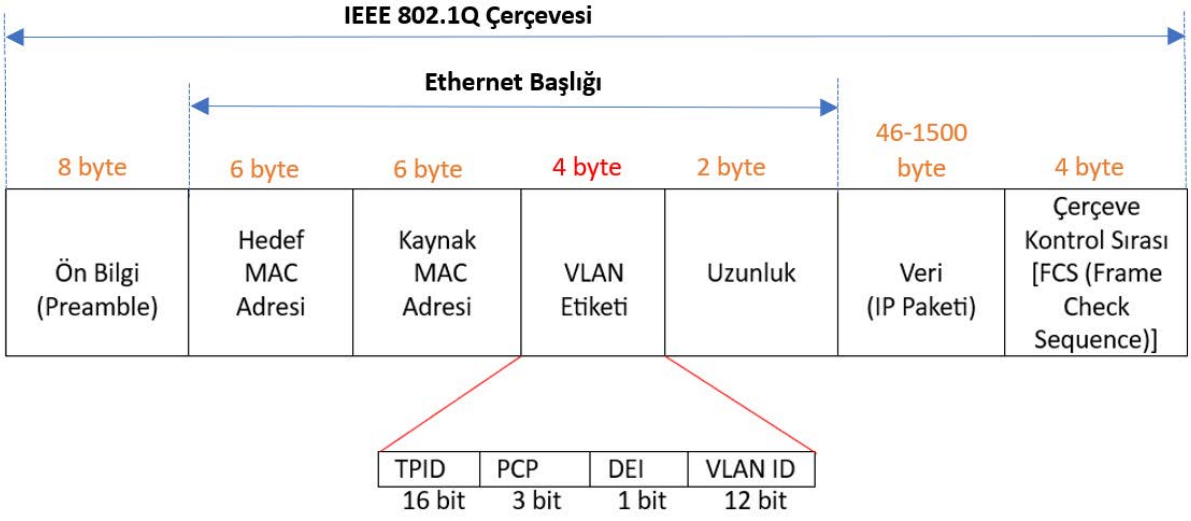
- Ağ, segmentlere ayrıldığı için oluşturulan sanal yerel ağların boyutu küçülür.
- Sanal yerel ağların boyutu küçüldüğü için ağ trafiği azalır.
- Her sanal yerel ağın trafiği birbirinden izole edilir.
- Ağ trafiği azaldığı için aygıtların **işlemci [CPU (Central Processing Unit)]** yükleri de azalır.
- Aygıtların işlemci yükleri azaldığı için enerji tasarrufu sağlanır.
- Sanal yerel ağlar birbirinden izole edildiği ve farklı sanal yerel ağlar, bir yönlendirici cihaz üzerinden kontrollü bir şekilde haberleştirileceği için güvenlik artar.
- Bir ağ kullanıcısını bulunduğu ağdan farklı bir ağa taşımak çok kolaydır.
- Hiyerarşik bir yapı oluşturulduğu için ağı yönetmek kolaydır ve ağ kaynakları daha iyi optimize edilir.

Ethernet çerçevesi (Ethernet frame), ikinci katman haberleşmesinde verinin Ethernet protokolüyle kapsüllenmiş hâline denir (Görsel 1.16).



Görsel 1.16: Ethernet çerçevesi

Ethernet çerçevesinin toplam boyutu 1.518 bayttır. Farklı VLAN'ların ağ trafiği, bir yönlendiriciyle haberleştirileceğinde trafik; ağ anahtarından çıkış yaparken Ethernet çerçevesinin ikinci katman başlığındaki **kaynak MAC adresi** ve **uzunluk** alanları arasına 4 baytlık **VLAN etiketi (VLAN Tag)** eklenir. Bu nedenle çerçevenin boyutu 1.522 bayt olur. Çerçevenin VLAN etiketi eklenmiş hâli, IEEE 802.1Q standardı ile tanımlanır (Görsel 1.17).



Görsel 1.17: VLAN etiketinin Ethernet çerçevesine eklenmesi

VLAN etiketindeki alanlar şunlardır:

Etiket Protocol Tanımlayıcısı [TPID (Tag Protocol Identifier)]: VLAN etiketinin başlangıcını gösterir. Değeri, **0 x 8.100** olarak belirlenir ve çerçevenin VLAN etiketli olduğunu ağ cihazlarına belirtir.

Öncelik Kod Noktası [PCP (Priority Code Point)]: Ethernet ağlarında **hizmet kalitesi [QoS (Quality of Service)]** sağlayabilmek için 0 ile 7 arasında değişen 8 farklı öncelik seviyesi sağlar. Ses trafiği gibi yüksek önceliğe sahip trafiklerin hizmet kalitesini artırabilmek için önceliklendirilmesi bu alanla gerçekleştirilir.

Bırakılabilirlik Göstergesi [DEI (Drop Eligible Indicator)]: Bir bitlik bu alan, ağda tıkanıklık olduğunda düşük öncelikli çerçevelerin bırakılabileceğini belirtir.

VLAN Numarası [VID (VLAN Identifier)]: Ethernet çerçevesinin hangi numaralı VLAN'a ait olduğunu belirtir. 12 bit uzunluğundaki bu alanla 0-4.095 arasında toplam 4.096 faklı VLAN tanımlanabilir ancak 0 ve 4.095 numaralı VLAN'lar, özel amaçlar sebebiyle ayrıldığından 1-4.094 arasında toplam 4.094 farklı VLAN oluşturulabilir.

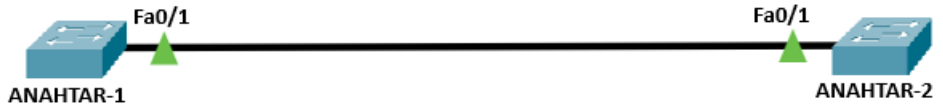
1.2.1. Anahtar Portunun Operasyon Modları

Anahtar portlarının operasyonel modları, anahtar portlarının ağ üzerindeki işlevlerini belirleyen yapılandırma türleridir. Bu modlar, portların hangi trafiği yöneteceğini belirler.

1. **Access Mode (Erişim Modu):** Anahtar portunun yalnızca bir VLAN segmentine bağlı olduğu ve bu VLAN segmentinden gelen trafiği yönettiği moddur. Bir port, erişim modunda çalıştığında sadece tek bir VLAN segmentine ait cihazlarla iletişim kurabilir ve yalnızca o VLAN segmentine ait etiketlenmemiş trafiği alır veya iletir. Access modu genellikle uç cihazlar (bilgisayarlar, yazıcılar vb.) için kullanılır.
2. **Trunk Mode (Gövde Modu):** Ağ anahtarları arasında birden fazla VLAN segmentinin ağ trafiğini aynı fiziksel port üzerinden iletmek için kullanılan bir yapılandırma modudur. Trunk olarak yapılandırılan port, birden fazla VLAN segmentinden gelen trafiği VLAN numarasıyla etiketleyerek birbirinden ayırır.

3. **Dynamic Mode (Dinamik Mod): Dinamik Gövdeleme Protokolü [DTP (Dynamic Trunkig Protocol)]** ile çalışan moda denir. Dinamik mod, iki anahtar arası bağlantının anahtarların birbiriyle paylaştıkları DTP mesajlarıyla Trunk bağlantısı olup olmayacağını belirler.

Anahtar portları, yönetici tarafından Access, Trunk veya dinamik olarak tanımlanabilir. Bu üç anahtar portu modundan dinamik mod, kendi içinde **dynamic auto (dinamik otomatik)** ve **dynamic desirable (dinamik istekli)** olarak ikiye ayrılır. Dynamic auto ve dynamic desirable portun otomatik olarak Trunk moduna geçip geçmeyeceğini dinamik mod belirler. Görsel 1.18'de iki anahtar arası bağlantı arayüzlerinin DTP mesajlarına göre ortaya çıkacak uzlaşma sonuçları görülür.



ANAHTAR-2 \ ANAHTAR-1	Dinamik Otomatik (Dynamic Auto)	Dinamik İstekli (Dynamic Desirable)	Gövde (Trunk)	Erişim (Access)
Dinamik Otomatik (Dynamic Auto)	Access	Trunk	Trunk	Access
Dinamik İstekli (Dynamic Desirable)	Trunk	Trunk	Trunk	Access
Gövde (Trunk)	Trunk	Trunk	Trunk	Sınırlı Bağlantı
Erişim (Access)	Access	Access	Sınırlı Bağlantı	Access

Görsel 1.18: İki anahtar arası bağlantı portlarının DTP uzlaşmaları

Anahtar portlarının yapılandırmasına bakılarak, DTP protokolünün etkin olup olmadığı görüntülenebilir (Görsel 1.19).

```
Switch#show interfaces fastEthernet 0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: static access
```

Görsel 1.19: DTP protokolünün etkinlik durumu

Görse 1.20'de anahtar portunun statik erişim modu olarak yapılandırılması görülür.

```
Switch(config)#interface fastEthernet 0/1
Switch(config-if)#switchport mode access
```

Görsel 1.20: Anahtar portunun statik erişim modu olarak yapılandırılması

Görsel 1.21'de anahtar portunun statik erişim modu yapılandırmasından sonraki durumu görülür.

```
Switch#show interfaces fastEthernet 0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
```

Görsel 1.21: Anahtar portunun statik erişim modu yapılandırmasından sonraki durumu

Anahtar portlarının modu, Access veya Trunk olarak tanımlansa bile portlarından DTP mesajı almaya devam eder. Dolayısıyla DTP, mesajın türüne göre çalışma modunu değiştirebilir. Bu durumun önlenmesi için arayüzlerde DTP protokolünün devre dışı bırakılması gerekir. Arayüz yapılandırmasında **switchport nonegotiate** komutu işletilerek DTP protokolü devre dışı bırakılır (Görsel 1.22).

```
Switch(config)#interface fastEthernet 0/2
Switch(config-if)#switchport mode access
Switch(config-if)#switchport nonegotiate
```

Görsel 1.22: DTP protokolünün devre dışı bırakılması

Trunk port yapılandırılırken **switchport trunk allowed vlan** komutu kullanılarak Trunk portu üzerinden istenilen VLAN'ların iletilmesi sağlanır.

NOT: Ağ anahtarında **show interfaces trunk** komutu kullanılarak Trunk portlarla ilgili bilgiler görüntülenir.

1.2.2. VLAN Türleri

VLAN'lar farklı ağ ihtiyaçlarına göre çeşitli türlere ayrılır. VLAN türleri şunlardır:

Varsayılan VLAN (Default VLAN): Bir anahtarın varsayılan olarak tüm portlarının başlangıçta üye olduğu VLAN'dır. Ağ anahtarlarında varsayılan olarak genellikle VLAN-1 biçiminde tanımlanır ancak güvenlik endişeleri nedeniyle varsayılan VLAN'ın kullanımı tercih edilmez.

Veri VLAN (Data VLAN): Büyük ağlarda farklı kullanıcı gruplarını veya cihaz gruplarını ayırmak ve birbirinden izole etmek için kullanılır. Veri VLAN'ları ağ uzmanı tarafından oluşturulur ve istenen portlar, bu VLAN'lara tanımlanır (Görsel 1.23).

```
Switch(config)#vlan 10
Switch(config-vlan)#name TEST
Switch(config-vlan)#exit
Switch(config)#interface fastEthernet 0/5
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
```

Görsel 1.23: Anahtar cihazında veri VLAN'ı oluşturma ve VLAN'a port tanımlama

Bir veri VLAN'ına tanımlanan port, varsayılan VLAN havuzundan çıkartılır.

Yönetim VLAN'ı (Management VLAN): Ağ cihazlarını (anahtar, yönlendirici) SSH ve Telnet protokolüyle uzaktan yönetebilmek ve mevcut veri VLAN'larından ayrı bir VLAN segmenti oluşturmak için yapılandırılır. Oluşturulan yönetim VLAN'ı için anahtar sanal arayüzü [SVI (Switch Virtual Inteface)] oluşturularak IP adresi yapılandırılır (Görsel 1.24).

```
Switch(config)#vlan 100
Switch(config-vlan)#name YONETIM
Switch(config-vlan)#exit
Switch(config)#interface vlan 100
Switch(config-if)#ip address 10.0.0.100 255.255.255.0
Switch(config-if)#no shutdown
```

Görsel 1.24: Yönetim VLAN'ı ve SVI oluşturma

Yerel VLAN (Native VLAN): Ağ anahtarları arasında tanımlanan Trunk portlarında VLAN etiketlemesi yapılmadan ağ trafiğini taşıyan VLAN'dır. Varsayılan ayarlarda genellikle VLAN-1 yerel VLAN olarak tanımlıdır ancak güvenlik sebebiyle genellikle değiştirilir (Görsel 1.25).

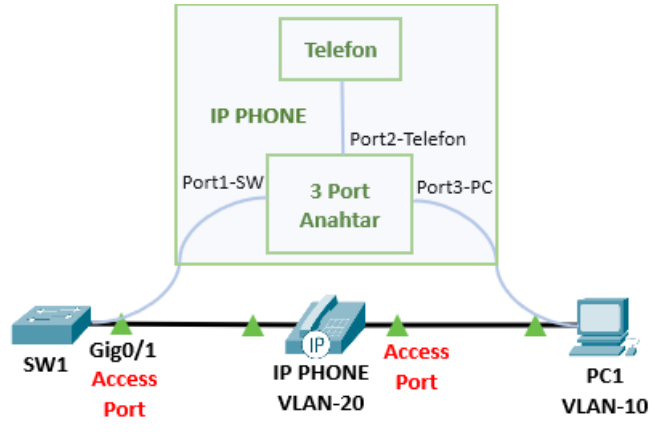
```
Switch(config)#interface gigabitEthernet 0/1
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk native vlan 100
```

Görsel 1.25: Yerel VLAN'ın değiştirilmesi

Yerel VLAN değişikliği yapılacaksa anahtarlar arası bağlantıyı gerçekleştiren her iki Trunk portta da değişiklik yapılmalıdır. Aksi takdirde yerel VLAN'ların eşleşmemesi nedeniyle sorun ortaya çıkar.

Ses VLAN (Voice VLAN): IP trafiği üzerinden sesi iletmek için kullanılan VLAN'dır. Ses trafiğini veri trafiğinden izole ederek ağ üzerinden iletir. Ağ üzerinden ses haberleşmesi, IP telefon cihazlarıyla gerçekleştirilir. Telefon haberleşmesi, ağ üzerinde herhangi bir gecikme olmadan iletilmesi gereken bir trafiktir. Bu sebeple ağ üzerinden telefon haberleşmesi yapılmak isteniyorsa anahtar cihazının IEEE 802.1p standardını desteklemesi önemlidir. IEEE 802.1p standardı, ağ üzerinde QoS'u [Quality of Service (Hizmet Kalitesi)] destekleyerek ses trafiğinin ağ üzerinde önceliklendirilmesini sağlar.

IP telefonun içinde üç adet portu bulunan bir anahtar bulunur. Görsel 1.26'da IP telefonun bağlantı şeması görülür.



Görsel 1.26: IP telefon bağlantı şeması

Ağ anahtarındaki port, Access olarak yapılandırılmasına rağmen veri ve ses farklı VLAN trafikleri olarak bu arayüzden iletilir.

Konsol bağlantısıyla bir ağ anahtarına bağlanarak VLAN oluşturma işlemini verilen adımlar doğrultusunda gerçekleştiriniz.

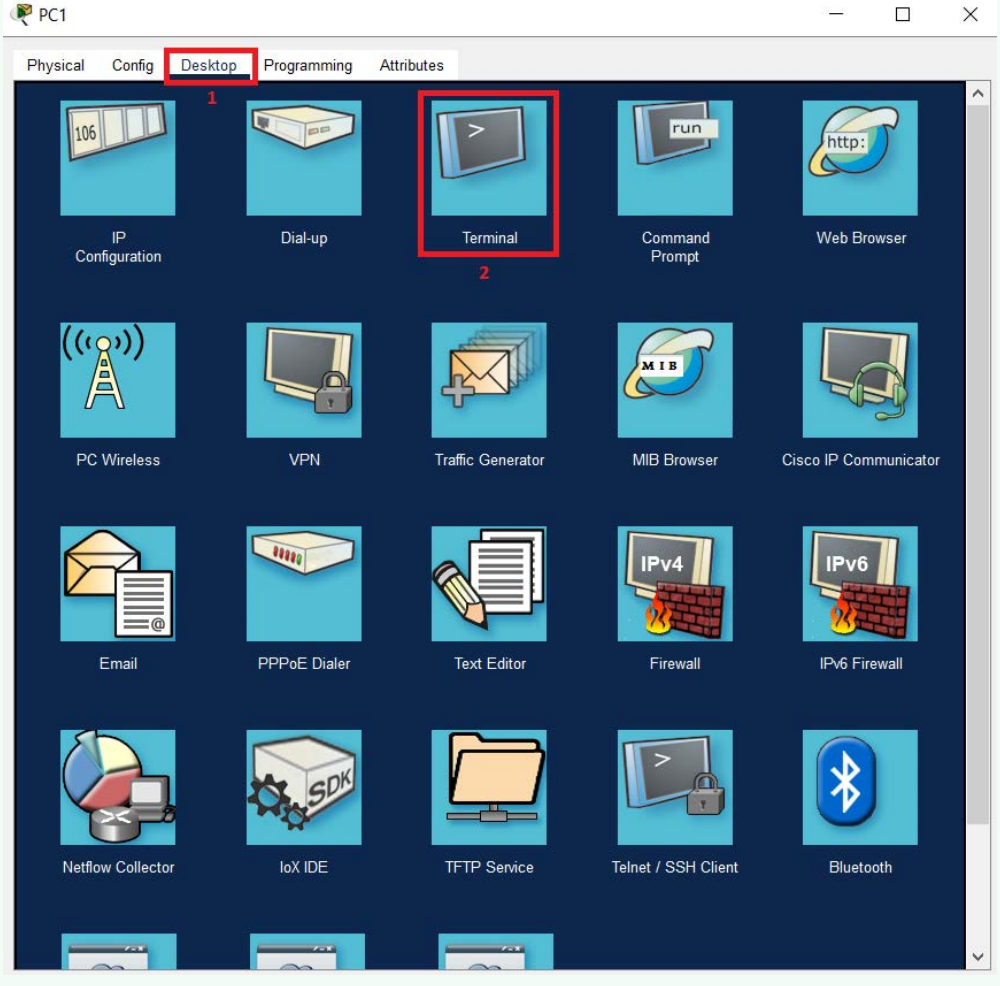
1. UYGULAMA

1. Adım: Ağ simülasyon programında Görsel 1.27'deki ağ topolojisini oluşturunuz.



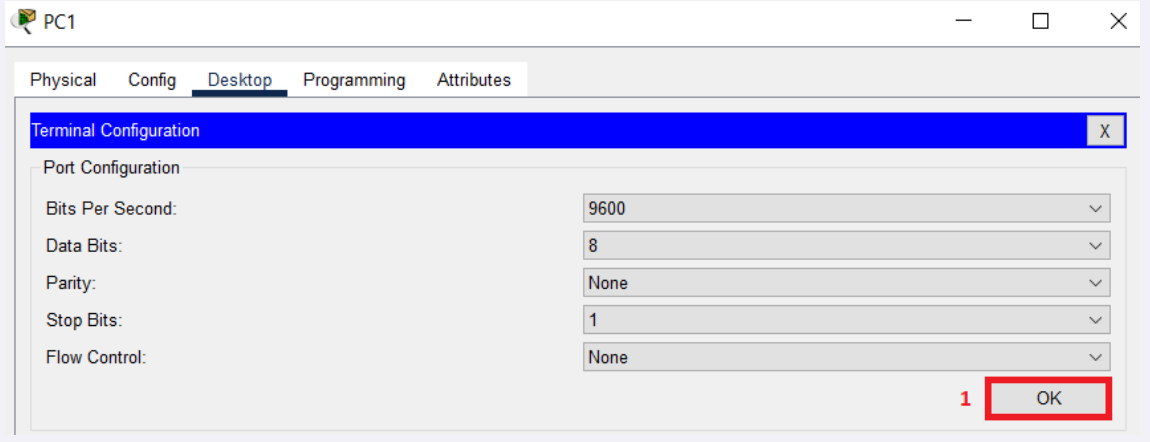
Görsel 1.27: Bilgisayardan ağ anahtarına konsol bağlantısı oluşturma

2. Adım: Topoloji üzerindeki PC1'e farenin sol tuşuyla tıklayınız ve açılan pencerede önce Desktop sekmesine sonra da Terminal öğesine tıklayarak ağ anahtarına konsol bağlantısı gerçekleştiriniz (Görsel 1.28).



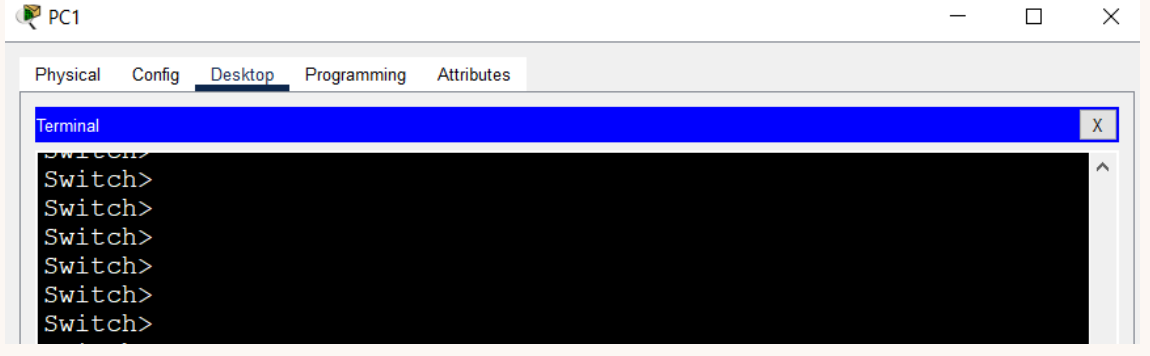
Görsel 1.28: Ağ anahtarına konsol bağlantısıyla erişim

3. Adım: Görsel 1.29'daki **OK** butonuna basınız.



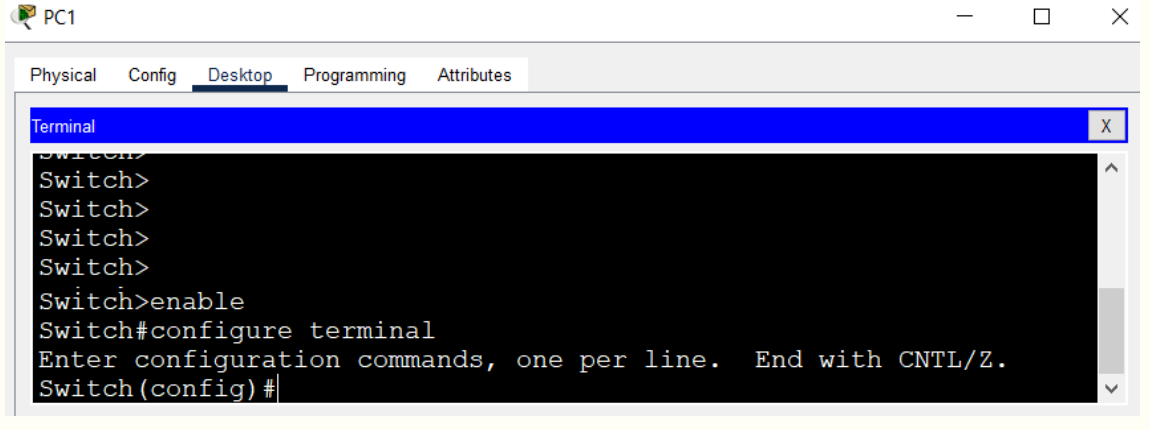
Görsel 1.29: Ağ anahtarının konsol ekranını açma

4. Adım: Konsol ekranının açıldığını gözlemleyiniz (Görsel 1.30).



Görsel 1.30: Ağ anahtarı konsol ekranı

5. Adım: **enable** komutunu kullanarak **yetkili moda**, sonrasında **configure terminal** komutunu kullanarak **konfigürasyon moduna** geçiş yapınız (Görsel 1.31).



Görsel 1.31: Yetkili moda ve konfigürasyon moduna geçiş yapma

6. Adım: Ağ anahtarında **10 IDARE**, **20 OGRETMEN**, **30 OGRENCI** şeklinde numarası ve isimleri verilen VLAN'ları aşağıdaki gibi oluşturunuz.

```
Switch(config)#vlan 10
Switch(config-vlan)#name IDARE
Switch(config-vlan)#exit
Switch(config)#vlan 20
Switch(config-vlan)#name OGRETMEN
Switch(config-vlan)#exit
Switch(config)#vlan 30
Switch(config-vlan)#name OGRENCI
Switch(config-vlan)#exit
```

7. Adım: Yetkili modda **show vlan** komutunu kullanarak VLAN veri tabanını görüntüleyiniz (Görsel 1.32).

```
Switch#show vlan 1

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                 Fa0/21, Fa0/22, Fa0/23, Fa0/24
10   IDARE                             active
20   OGRETMEN                          active    2
30   OGRENCI                           active    Gig0/1, Gig0/2
```

Görsel 1.32: VLAN veri tabanının görüntülenmesi

8. Adım: Ağ anahtarındaki 1-5 arası portları 10 numaralı IDARE VLAN'ına, 6-10 arası portları 20 numaralı OGRETMEN VLAN'ına ve 11-15 arası portları 30 numaralı OGRENCI VLAN'ına tanımlama işlemini aşağıdaki şekilde gerçekleştiriniz.

```
Switch(config)#interface range fastEthernet 0/1-5
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 10
Switch(config-if-range)#exit
Switch(config)#interface range fastEthernet 0/6-10
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 20
Switch(config-if-range)#exit
Switch(config)#interface range fastEthernet 0/11-15
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 30
```

9. Adım: Yetkili modda **show vlan** komutunu tekrar kullanarak belirlenen portların ilgili VLAN'lara tanımlandığını teyit ediniz (Görsel 1.33).

```
Switch#show vlan 1

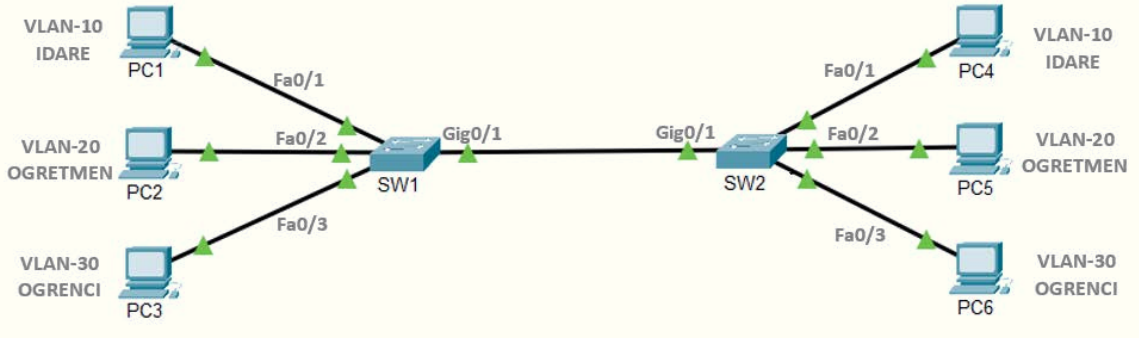
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                                 Fa0/20, Fa0/21, Fa0/22, Fa0/23
                                                 Fa0/24, Gig0/1, Gig0/2
10   IDARE                             active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5
20   OGRETMEN                          active    Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                 Fa0/10
30   OGRENCI                           active    Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                 Fa0/15
1002 fddi-default                      active    2
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
```

Görsel 1.33: Güncel VLAN veri tabanının görüntülenmesi

Farklı ağ anahtarlarında aynı VLAN'ların oluşturulup, Trunk port üzerinden aynı VLAN'ların haberleştirilmesi ve son aygıtların bağlı bulunduğu Access portlarda DTP'nin (Dynamic Trunking Protocol) devre dışı bırakılarak Layer-2 güvenliğin arttırılması işlemini verilen adımlar doğrultusunda gerçekleştiriniz.

2. UYGULAMA

1. Adım: Ağ simülasyon programında Görsel 1.34'teki ağ topolojisini oluşturunuz.



Görsel 1.34: VLAN'lar arası haberleşme ağ topolojisi

2. Adım: SW1 ve SW2 ağ anahtarlarında Görsel 1.34'te belirtilen VLAN'ları CLI arayüzüne girerek aşağıda belirtilen şekilde oluşturunuz.

SW1(config)#vlan 10	SW2(config)#vlan 10
SW1(config-vlan)#name IDARE	SW2(config-vlan)#name IDARE
SW1(config-vlan)#exit	SW2(config-vlan)#exit
SW1(config)#vlan 20	SW2(config)#vlan 20
SW1(config-vlan)#name OGRETMEN	SW2(config-vlan)#name OGRETMEN
SW1(config-vlan)#exit	SW2(config-vlan)#exit
SW1(config)#vlan 30	SW2(config)#vlan 30
SW1(config-vlan)#name OGRENCI	SW2(config-vlan)#name OGRENCI

3. Adım: SW1 ve SW2 ağ anahtarlarında Görsel 1.34'te belirtilen son aygıtların bağlı bulunduğu portların modunun **Access** olarak yapılandırılıp, **DTP** protokolünün devre dışı bırakılması ve ilgili VLAN'a taşınması işlemini CLI arayüzüne girerek aşağıda belirtilen şekilde konfigüre ediniz.

SW1(config)#interface fastEthernet 0/1	SW2(config)#interface fastEthernet 0/1
SW1(config-if)#switchport mode access	SW2(config-if)#switchport mode access
SW1(config-if)#switchport nonegotiate	SW2(config-if)#switchport nonegotiate
SW1(config-if)#switchport access vlan 10	SW2(config-if)#switchport access vlan 10
SW1(config-if)#exit	SW2(config-if)#exit
SW1(config)#interface fastEthernet 0/2	SW2(config)#interface fastEthernet 0/2
SW1(config-if)#switchport mode access	SW2(config-if)#switchport mode access
SW1(config-if)#switchport nonegotiate	SW2(config-if)#switchport nonegotiate
SW1(config-if)#switchport access vlan 20	SW2(config-if)#switchport access vlan 20
SW1(config-if)#exit	SW2(config-if)#exit
SW1(config)#interface fastEthernet 0/3	SW2(config)#interface fastEthernet 0/3
SW1(config-if)#switchport mode access	SW2(config-if)#switchport mode access
SW1(config-if)#switchport nonegotiate	SW2(config-if)#switchport nonegotiate
SW1(config-if)#switchport access vlan 30	SW2(config-if)#switchport access vlan 30

4. Adım: SW1 ve SW2 ağ anahtarında CLI arayüzüne girip, yetkili modda **show vlan** komutunu kullanarak VLAN veri tabanlarını görüntüleyiniz ve her ikisinin de aynı olduğunu teyit ediniz (Görsel 1.35).

```
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/4, Fa0/5, Fa0/6, Fa0/7
                                                 Fa0/8, Fa0/9, Fa0/10, Fa0/11
                                                 Fa0/12, Fa0/13, Fa0/14, Fa0/15
                                                 Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                                 Fa0/20, Fa0/21, Fa0/22, Fa0/23
                                                 Fa0/24, Gig0/1, Gig0/2
10   IDARE                             active    Fa0/1
20   OGRETMEN                          active    Fa0/2
30   OGRENCI                           active    Fa0/3
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
```

Görsel 1.35: SW1 ve SW2 VLAN veri tabanlarının görüntüsü

5. Adım: SW1 ve SW2 ağ anahtarlarını bağlayan portları CLI arayüzüne girip, modunu aşağıda belirtildiği gibi **Trunk** olarak yapılandırınız.

```
SW1(config)#interface gigabitEthernet 0/1
SW1(config-if)#switchport mode trunk

SW2(config)#interface gigabitEthernet 0/1
SW2(config-if)#switchport mode trunk
```

6. Adım: Son aygıtların IP yapılandırmasını aşağıda belirtilen şekilde gerçekleştiriniz.

PC1: 10.0.0.1/24 **PC4:** 10.0.0.2/24

PC2: 20.0.0.1/24 **PC5:** 20.0.0.2/24

PC3: 30.0.0.1/24 **PC6:** 30.0.0.2/24

7. Adım: PC1-PC4, PC2-PC5 ve PC3-PC6 arasında **ping** komutuyla bağlantı testi gerçekleştirerek haberleştiklerini teyit ediniz.

PC1: C:/>ping 10.0.0.2 **PC2:** C:/> ping 20.0.0.2 **PC3:** C:/> ping 30.0.0.2

NOT: Farklı VLAN'larda bulunan aygıtlar, ağ anahtarı üzerinden haberleşemez. Haberleşebilmeleri için bir yönlendirici cihazla bulundukları ağların birbirine yönlendirilmesi gerekir.

Ağ anahtarında anahtar sanal arayüzü [SVI (Switch Virtual Interface)] oluşturup Telnet protokolüyle anahtara uzaktan erişim sağlama işlemini verilen adımlar doğrultusunda gerçekleştiriniz.

3. UYGULAMA

1. Adım: Ağ simülasyon programında Görsel 1.36'daki ağ topolojisini oluşturunuz.



Görsel 1.36: Konsol bağlantısıyla Telnet yapılandırması

2. Adım: PC1'den konsol bağlantısıyla ağ anahtarının CLI arayüzüne girerek SVI oluşturunuz.

```
ANAHTAR(config)#interface vlan 1
```

3. Adım: Oluşturulan anahtar sanal arayüzü IP yapılandırmasını aşağıdaki şekilde gerçekleştiriniz.

```
ANAHTAR(config-if)#ip address 192.168.1.1 255.255.255.0
```

4. Adım: Kapalı durumda olan anahtar sanal arayüzünü aşağıda belirtilen şekilde açınız.

```
ANAHTAR(config-if)#no shutdown
```

5. Adım: Anahtar sanal arayüzü durumunu aşağıdaki şekilde görüntüleyiniz (Görsel 1.37).

```
ANAHTAR#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/1        unassigned      YES manual down                  down
FastEthernet0/2        unassigned      YES manual down                  down
FastEthernet0/3        unassigned      YES manual down                  down
FastEthernet0/4        unassigned      YES manual down                  down
FastEthernet0/5        unassigned      YES manual down                  down
FastEthernet0/6        unassigned      YES manual down                  down
FastEthernet0/7        unassigned      YES manual down                  down
FastEthernet0/8        unassigned      YES manual down                  down
FastEthernet0/9        unassigned      YES manual down                  down
FastEthernet0/10       unassigned      YES manual down                  down
FastEthernet0/11       unassigned      YES manual down                  down
FastEthernet0/12       unassigned      YES manual down                  down
FastEthernet0/13       unassigned      YES manual down                  down
FastEthernet0/14       unassigned      YES manual down                  down
FastEthernet0/15       unassigned      YES manual down                  down
GigabitEthernet0/1     unassigned      YES manual up                    up
GigabitEthernet0/2     unassigned      YES manual down                  down
Vlan1                  192.168.1.1     YES manual up                    up
ANAHTAR#
```

Görsel 1.37: Ağ anahtarının arayüz durumları

6. Adım: Ağ anahtarında yetkili moda geçiş için bir şifre tanımlayınız.

ANAHTAR(config)#enable secret Telnet123

7. Adım: Telnet yapılandırmasını aşağıda belirtilen şekilde gerçekleştiriniz.

ANAHTAR(config)#line vty 0 15

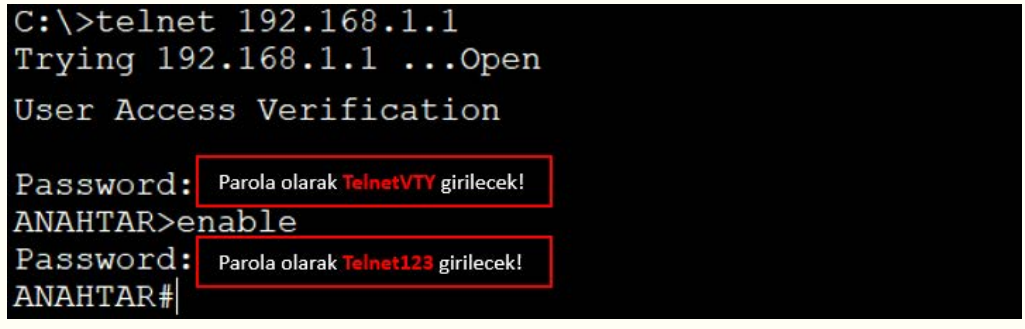
ANAHTAR(config-line)#password TelnetVTY

ANAHTAR(config-line)#login

8. Adım: PC1'in IP yapılandırmasını aşağıda belirtilen şekilde gerçekleştiriniz.

PC1: 192.168.1.2/24

9. Adım: PC1'in komut sisteminden Telnet protokolüyle ağ anahtarına bağlantı gerçekleştiriniz (Görsel 1.38).



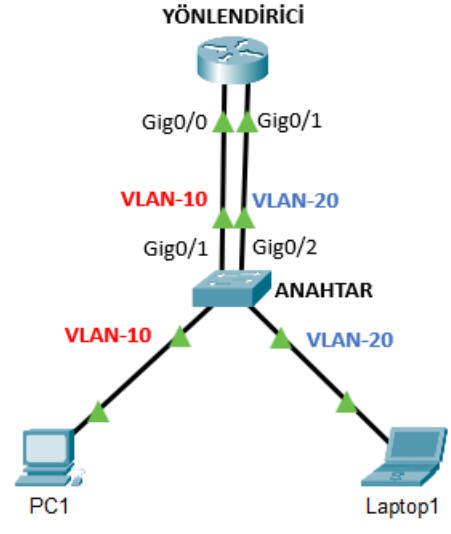
Görsel 1.38: Telnet protokolüyle ağ anahtarına bağlanma

1.2.3. Sanal Yerel Alan Ağları Arası Yönlendirme [IVR (Inter VLAN Routing)]

VLAN'lar, farklı ağ segmentleri olduğundan yönlendirme işlemi ile haberleştirilirler. VLAN'lar genellikle üç farklı yöntemle haberleştirilir. VLAN'ları haberleştirme yöntemleri şunlardır:

1. Geleneksel IVR

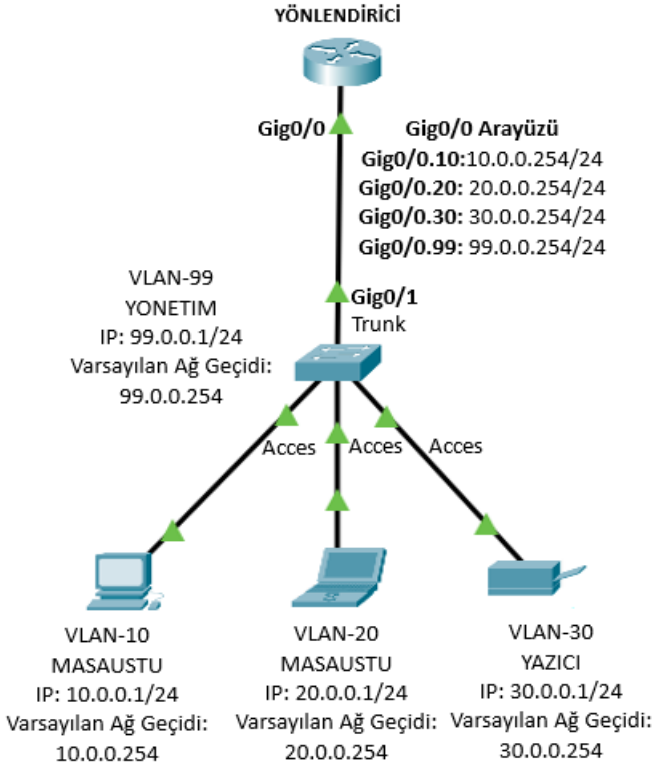
Geleneksel IVR yönteminde her VLAN segmentine yönlendirici cihaz üzerinde fiziksel bir arayüz, varsayılan ağ geçidi olarak tanımlanır (Görsel 1.39). Bu yöntem birkaç tane VLAN segmentini haberleştirmek için ideal bir çözümdür ancak çok fazla VLAN segmenti mevcutsa yönlendirici cihaz üzerindeki fiziksel arayüzler yeterli gelmeyeceği için bu yöntem kullanılamaz.



Görsel 1.39: Geleneksel IVR yöntemi

2. Router On A Stick yöntemiyle IVR

Router On A Stick yönteminde yönlendiricinin fiziksel arayüzü birden fazla sanal arayüze bölünerek her bir sanal arayüz, farklı VLAN segmenti için varsayılan ağ geçidi olarak yapılandırılır (Görsel 1.40).

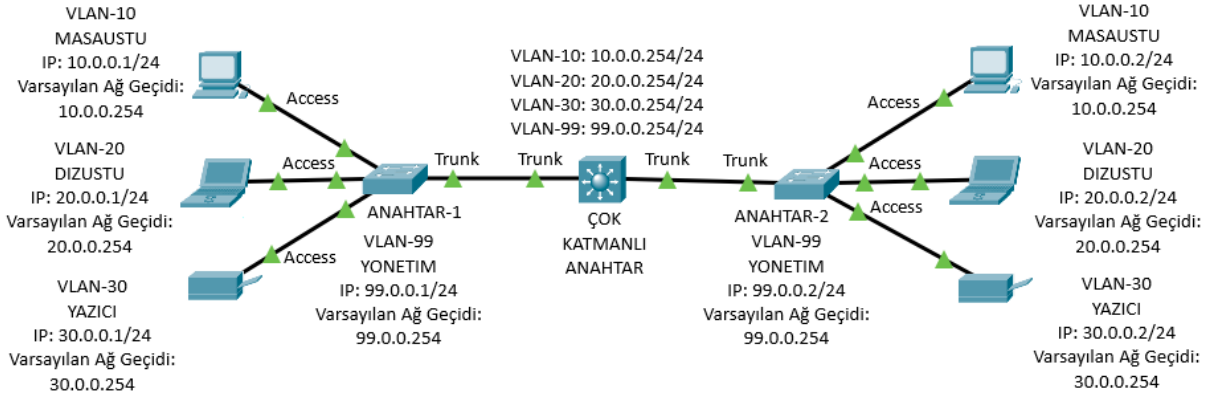


Görsel 1.40: Router On A Stick IVR yöntemi

Router On A Stick yöntemi, düşük bütçeli küçük ağ topolojilerinde tercih edilebilir ancak bütün VLAN segmentlerinin trafiği tek fiziksel arayüz üzerinden geçeceği için bant genişliği sıkıntısı yaşanabilir. Bu tek fiziksel arayüzün arızalanması durumunda yedeklilik olmadığından ağ trafiği durur.

3. Çok Katmanlı Ağ Anahtarıyla (Multilayer Switch) IVR

Çok katmanlı ağ anahtarı, **katman 3 ağ anahtarı (layer 3 switch)** olarak da anılır. Çok katmanlı ağ anahtarıyla IVR yönteminde her VLAN segmenti için katman 3 anahtar üzerinde sanal arayüz oluşturulur. Oluşturulan sanal arayüzler, ilgili VLAN segmentine varsayılan ağ geçidi olarak tanımlanır (Görsel 1.41).



Görsel 1.41: Çok katmanlı ağ anahtarıyla IVR yöntemi

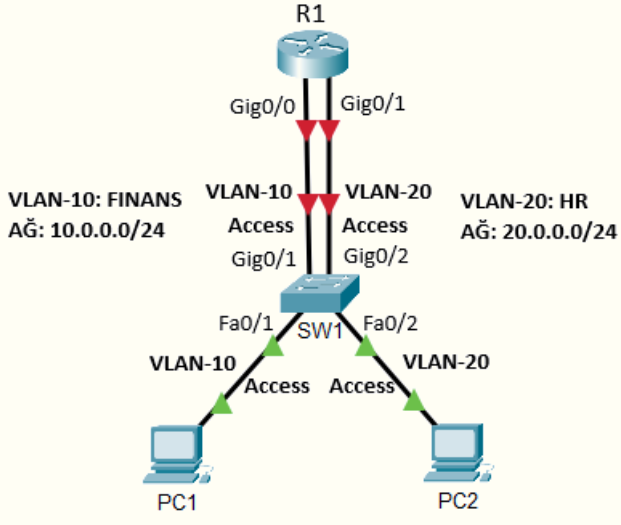
Çok katmanlı anahtarın VLAN segmentine varsayılan ağ geçidi olarak atanabilmesinin bir diğer yöntemi de fiziksel portları IP adresiyle yapılandırmaktır ancak varsayılan ayarlarda portlar, OSI referans modeli ikinci katman portu olarak çalışır. Arayüz yapılandırma modunda **no switchport** komutu çalıştırıldığında üçüncü katman arayüzü olarak çalışmaya başlar ve IP adresi yapılandırılır. Esnek olması ve kullanım kolaylığı nedeniyle genellikle sanal arayüzler yapılandırılarak kullanılır.

Çok katmanlı ağ anahtarı OSI referans modeli ikinci katman [Data Link Layer (Veri Bağı Katmanı)] ve üçüncü katman [Network Layer (Ağ Katmanı)] işlevlerini gerçekleştirebilir ancak bu cihazlar standart ayarlarında genellikle katman 2 olarak çalışır. Dolayısıyla katman 3 ağ anahtarına yönlendirme yaptırılacaksa yönlendirme özelliği aktif edilmelidir. Çok katmanlı ağ anahtarı, yüksek performanslı yönlendirme sağlar. Bu nedenle genellikle büyük ağ topolojilerinde sanal yerel alan ağları arası yönlendirme de tercih edilir.

4. UYGULAMA

Geleneksel IVR yöntemi uygulama işlemini verilen adımlar doğrultusunda gerçekleştiriniz.

1. Adım: Ağ simülasyon programında Görsel 1.42'deki ağ topolojisini oluşturunuz.



Görsel 1.42: Geleneksel IVR uygulama topolojisi

2. Adım: SW1 ağ anahtarı üzerinde **FINANS** ve **HR** VLAN'larını, CLI moduna girerek aşağıdaki gibi oluşturunuz.

```
SW1(config)#vlan 10

SW1(config-vlan)#name FINANS

SW1(config-vlan)#exit

SW1(config)#vlan 20

SW1(config-vlan)#name HR
```

3. Adım: İlgili portların modunu **Access** olarak tanımlayıp belirtilen VLAN'lara atanması ve portlarda **DTP** protokolünün devre dışı bırakılması işlemlerini gerçekleştiriniz.

```
SW1(config)#interface range gigabitEthernet 0/1, fastEthernet 0/1
SW1(config-if-range)#switchport mode access
SW1(config-if-range)#switchport access vlan 10
SW1(config-if-range)#switchport nonegotiate
SW1(config-if-range)#exit
SW1(config)#interface range gigabitEthernet 0/2, fastEthernet 0/2
SW1(config-if-range)#switchport mode access
SW1(config-if-range)#switchport access vlan 20
SW1(config-if-range)#switchport nonegotiate
```

4. Adım: R1 yönlendiricisinin arayüzlerini belirtilen ağ adresi bilgilerine göre aşağıdaki gibi konfigüre ediniz.

```
R1(config)#interface gigabitEthernet 0/0
R1(config-if)#ip address 10.0.0.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface gigabitEthernet 0/1
R1(config-if)#ip address 20.0.0.1 255.255.255.0
R1(config-if)#no shutdown
```

5. Adım: PC1 ve PC2'nin IP adres yapılandırmalarını aşağıda belirtilen şekilde konfigüre ediniz.

PC1		**PC2**	
IP Adresi	: 10.0.0.10	IP Adresi	: 20.0.0.20
Alt Ağ Maskesi	: 255.255.255.0	Alt Ağ Maskesi	: 255.255.255.0
V. Ağ Geçidi	: 10.0.0.1	V. Ağ Geçidi	: 20.0.0.1

6. Adım: PC1'de komut sistemine girerek ping komutuyla PC2'ye bağlantı testi gerçekleştiriniz (Görsel 1.43).

```
C:\>ping 20.0.0.20

Pinging 20.0.0.20 with 32 bytes of data:

Reply from 20.0.0.20: bytes=32 time<1ms TTL=127
Reply from 20.0.0.20: bytes=32 time<1ms TTL=127
Reply from 20.0.0.20: bytes=32 time<1ms TTL=127
Reply from 20.0.0.20: bytes=32 time<1ms TTL=127

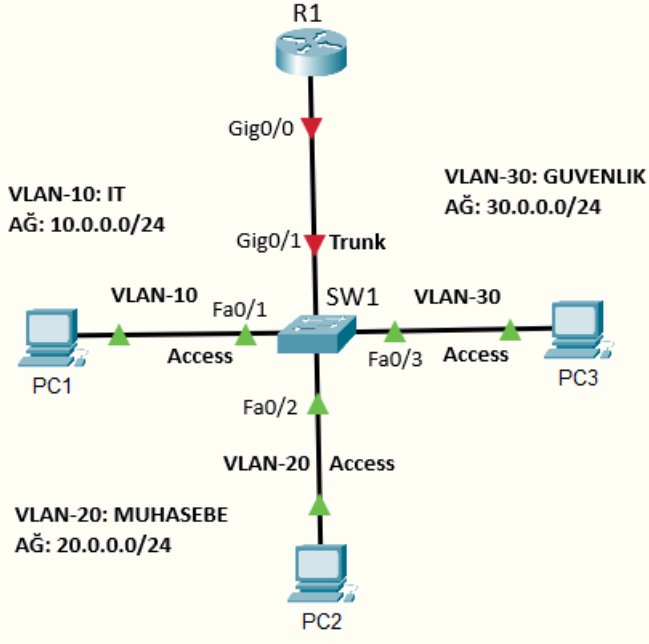
Ping statistics for 20.0.0.20:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Görsel 1.43: PC1'den PC2'ye ping komutuyla bağlantı testi

5. UYGULAMA

Router On A Stick IVR yöntemi uygulama işlemini verilen adımlar doğrultusunda gerçekleştiriniz.

1. Adım: Ağ simülasyon programında Görsel 1.44'teki ağ topolojisini oluşturunuz.



Görsel 1.44: Router On A Stick IVR uygulama topolojisi

2. Adım: SW1 ağ anahtarı üzerinde **IT**, **MUHASEBE** ve **GUVENLIK** VLAN'larını CLI moduna girerek aşağıdaki gibi oluşturunuz.

```
SW1(config)#vlan 10
SW1(config-vlan)#name IT
SW1(config-vlan)#exit
SW1(config)#vlan 20
SW1(config-vlan)#name MUHASEBE
SW1(config-vlan)#exit
SW1(config)#vlan 30
SW1(config-vlan)#name GUVENLIK
```

3. Adım: İlgili portların modunu **Access** olarak tanımlayıp belirtilen VLAN'lara atanması ve portlarda **DTP** protokolünün devre dışı bırakılması işlemlerini gerçekleştiriniz.

```
SW1(config)#interface fastEthernet 0/1
SW1(config-if)#switchport mode access
SW1(config-if)#switchport access vlan 10
SW1(config-if)#switchport nonegotiate
SW1(config)#interface fastEthernet 0/2
SW1(config-if)#switchport mode access
SW1(config-if)#switchport access vlan 20
SW1(config-if)#switchport nonegotiate
SW1(config-if)#exit
SW1(config)#interface fastEthernet 0/3
SW1(config-if)#switchport mode access
SW1(config-if)#switchport access vlan 30
SW1(config-if)#switchport nonegotiate
```

4. Adım: SW1 ağ anahtarından R1 yönlendiricisine giden **Gig0/1** portunun modunu **Trunk** olarak yapılandırınız ve DTP protokolünü devre dışı bırakınız.

```
SW1(config)#interface gigabitEthernet 0/1
SW1(config-if)#switchport mode trunk
SW1(config-if)#switchport nonegotiate
```

5. Adım: R1 yönlendiricisinin **Gig0/0** arayüzünde, her VLAN'a varsayılan ağ geçidi olarak tanımlamak için bir, alt arayüz (sub interface) oluşturunuz ve çerçeve ağ anahtarı üzerinden etiketli geleceği için ağ iletişim protokolünü, 802.1Q biçiminde değiştirerek IP adres yapılandırmasını gerçekleştiriniz.

```
R1(config)#interface gigabitEthernet 0/0
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface gigabitEthernet 0/0.10
R1(config-subif)#encapsulation dot1Q 10
R1(config-subif)#ip address 10.0.0.1 255.255.255.0
R1(config-subif)#exit
R1(config)#interface gigabitEthernet 0/0.20
R1(config-subif)#encapsulation dot1Q 20
R1(config-subif)#ip address 20.0.0.1 255.255.255.0
R1(config-subif)#exit
R1(config)#interface gigabitEthernet 0/0.30
R1(config-subif)#encapsulation dot1Q 30
R1(config-subif)#ip address 30.0.0.1 255.255.255.0
```

6. Adım: PC1, PC2 ve PC3'ün IP adres yapılandırmalarını aşağıda belirtilen şekilde konfigüre ediniz.

PC1		**PC2**		**PC3**	
IP Adresi	: 10.0.0.254	IP Adresi	: 20.0.0.254	IP Adresi	: 30.0.0.254
Alt Ağ Maskesi	: 255.255.255.0	Alt Ağ Maskesi	: 255.255.255.0	Alt Ağ Maskesi	: 255.255.255.0
V. Ağ Geçidi	: 10.0.0.1	V. Ağ Geçidi	: 20.0.0.1	V. Ağ Geçidi	: 30.0.0.1

7. Adım: PC1'de komut sistemine girerek ping komutuyla PC2'ye bağlantı testi gerçekleştiriniz (Görsel 1.45).

```
C:\>ping 20.0.0.254

Pinging 20.0.0.254 with 32 bytes of data:

Reply from 20.0.0.254: bytes=32 time<1ms TTL=127
Reply from 20.0.0.254: bytes=32 time<1ms TTL=127
Reply from 20.0.0.254: bytes=32 time=1ms TTL=127
Reply from 20.0.0.254: bytes=32 time=1ms TTL=127

Ping statistics for 20.0.0.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Görsel 1.45: PC1'den PC2'ye ping komutuyla bağlantı testi

8. Adım: PC1'de komut sistemine girerek ping komutuyla PC3'e bağlantı testi gerçekleştiriniz (Görsel 1.46).

```
C:\>ping 30.0.0.254

Pinging 30.0.0.254 with 32 bytes of data:

Reply from 30.0.0.254: bytes=32 time<1ms TTL=127
Reply from 30.0.0.254: bytes=32 time<1ms TTL=127
Reply from 30.0.0.254: bytes=32 time=1ms TTL=127
Reply from 30.0.0.254: bytes=32 time<1ms TTL=127

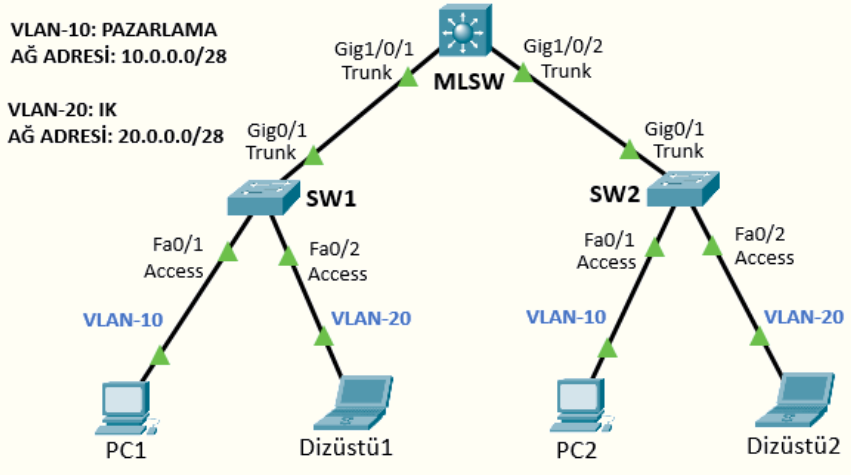
Ping statistics for 30.0.0.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Görsel 1.46: PC1'den PC3'e ping komutuyla bağlantı testi

6. UYGULAMA

Katman 3 ağ anahtarıyla IVR yöntemi uygulama işlemini verilen adımlar doğrultusunda gerçekleştiriniz.

1. Adım: Ağ simülasyon programında Görsel 1.47'deki ağ topolojisini oluşturunuz.



Görsel 1.47: Çok katmanlı ağ anahtarıyla IVR uygulama topolojisi

2. Adım: CLI moduna girerek SW1, SW2 ve MLSW ağ anahtarları üzerinde **PAZARLAMA** ve **IK** VLAN'larını aşağıdaki gibi oluşturunuz.

```
SW1(config)#vlan 10
SW1(config-vlan)#name PAZARLAMA
SW1(config-vlan)#exit
SW1(config)#vlan 20
SW1(config-vlan)#name IK
```

```
SW2(config)#vlan 10
SW2(config-vlan)#name PAZARLAMA
SW2(config-vlan)#exit
SW2(config)#vlan 20
SW2(config-vlan)#name IK
```

```
MLSW(config)#vlan 10
MLSW(config-vlan)#name PAZARLAMA
MLSW(config-vlan)#exit
MLSW(config)#vlan 20
MLSW(config-vlan)#name IK
```

3. Adım: SW1 ve SW2 ağ anahtarlarında ilgili portların modunu **Access** olarak tanımlayıp belirtilen VLAN'lara atanması ve portlarda **DTP** protokolünün devre dışı bırakılması işlemlerini gerçekleştiriniz.

```
SW1(config)#interface fastEthernet 0/1
SW1(config-if)#switchport mode access
SW1(config-if)#switchport access vlan 10
SW1(config-if)#switchport nonegotiate
SW1(config-if)#exit
SW1(config)#interface fastEthernet 0/2
SW1(config-if)#switchport mode access
SW1(config-if)#switchport access vlan 20
SW1(config-if)#switchport nonegotiate
```

```
SW2(config)#interface fastEthernet 0/1
SW2(config-if)#switchport mode access
SW2(config-if)#switchport access vlan 10
SW2(config-if)#switchport nonegotiate
SW2(config-if)#exit
SW2(config)#interface fastEthernet 0/2
SW2(config-if)#switchport mode access
SW2(config-if)#switchport access vlan 20
SW2(config-if)#switchport nonegotiate
```

4. Adım: SW1 ve SW2 ağ anahtarlarından MLSW ağ anahtarına giden portların modunu **Trunk** olarak yapılandırınız ve DTP protokolünü devre dışı bırakınız.

```
SW1(config)#interface gigabitEthernet 0/1
SW1(config-if)#switchport mode trunk
SW1(config-if)#switchport nonegotiate

SW2(config)#interface gigabitEthernet 0/1
SW2(config-if)#switchport mode trunk
SW2(config-if)#switchport nonegotiate
```

5. Adım: MLSW ağ anahtarından SW1 ve SW2 ağ anahtarlarına giden portların modunu **Trunk** olarak yapılandırınız ve DTP protokolünü devre dışı bırakınız.

```
MLSW(config)#interface range gigabitEthernet 1/0/1-2
MLSW(config-if-range)#switchport mode trunk
MLSW(config-if-range)#switchport nonegotiate
```

6. Adım: MLSW ağ anahtarında VLAN'lara varsayılan ağ geçidi görevi yapması için sanal arayüzler oluşturunuz ve ağ adresi bilgilerine göre IP adreslerini konfigüre ediniz.

```
MLSW(config)#interface vlan 10
MLSW(config-if)#ip address 10.0.0.1 255.255.255.240
MLSW(config-if)#no shutdown
MLSW(config-if)#exit
MLSW(config)#interface vlan 20
MLSW(config-if)#ip address 20.0.0.1 255.255.255.240
MLSW(config-if)#no shutdown
```

7. Adım: MLSW ağ anahtarında yönlendirme özelliğini açınız.

```
MLSW(config)#ip routing
```

8. Adım: PC1, PC2, Dizüstü1 ve Dizüstü2'nin IP adres yapılandırmalarını aşağıda belirtilen şekilde konfigüre ediniz.

PC1		**PC2**	
IP Adresi	: 10.0.0.2	IP Adresi	: 10.0.0.3
Alt Ağ Maskesi	: 255.255.255.240	Alt Ağ Maskesi	: 255.255.255.240
V. Ağ Geçidi	: 10.0.0.1	V. Ağ Geçidi	: 10.0.0.1
Dizüstü1		**Dizüstü2**	
IP Adresi	: 20.0.0.2	IP Adresi	: 20.0.0.3
Alt Ağ Maskesi	: 255.255.255.240	Alt Ağ Maskesi	: 255.255.255.240
V. Ağ Geçidi	: 20.0.0.1	V. Ağ Geçidi	: 20.0.0.1

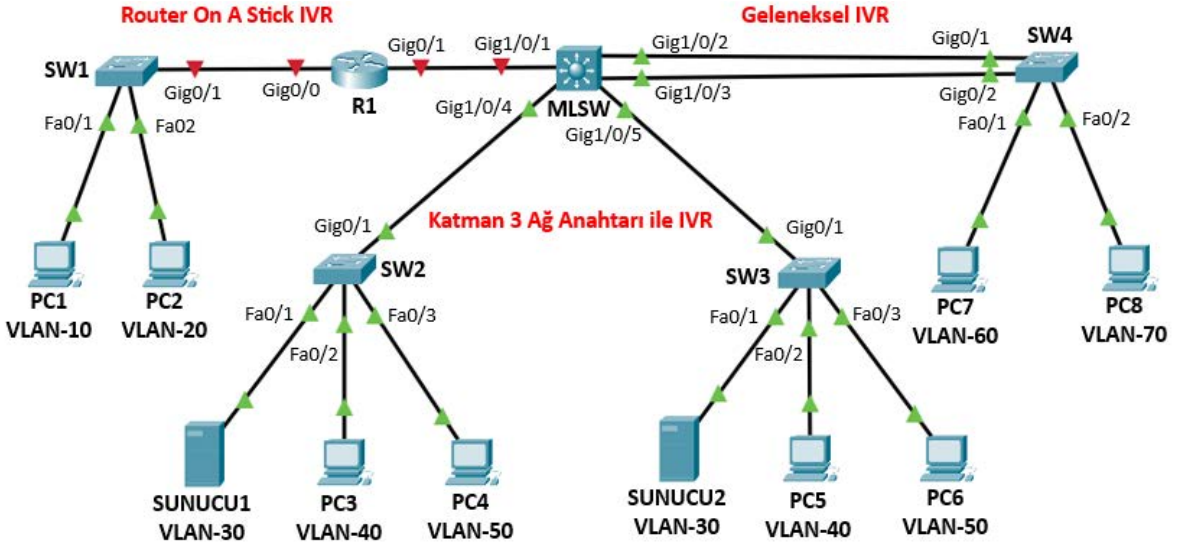
9. Adım: PC1'de komut sistemine girerek ping komutuyla PC2, Dizüstü1 ve Dizüstü2'ye aşağıda belirtilen şekilde bağlantı testi gerçekleştiriniz.

```
C:/> ping 10.0.0.3
C:/> ping 20.0.0.2
C:/> ping 20.0.0.3
```

SIRA SİZDE

Maddelerde belirtilen uygulamaları gerçekleştiriniz.

- Ağ simülasyon programında Görsel 1.48'deki ağ topolojisini çiziniz.



Görsel 1.48: VLAN'lar arası yönlendirme uygulama topolojisi

- Ağ anahtarlarında belirtilen uygun VLAN'ları oluşturunuz.

VLAN-10: SATIS	Ağ Adresi: 10.0.0.0/24
VLAN-20: DESTEK	Ağ Adresi: 20.0.0.0/24
VLAN-30: SUNUCU	Ağ Adresi: 30.0.0.0/24
VLAN-40: IK	Ağ Adresi: 40.0.0.0/24
VLAN-50: IT	Ağ Adresi: 50.0.0.0/24
VLAN-60: MUHASEBE	Ağ Adresi: 60.0.0.0/24
VLAN-70: MISAFIR	Ağ Adresi: 70.0.0.0/24
VLAN-80: YONETIM	Ağ Adresi: 80.0.0.0/28

- **R1-MLSW** arasına **90.0.0.0/30** ağ adresine göre IP adresi atayınız.
- R1 yönlendiricisine, **R1(config)#ip route 0.0.0.0 0.0.0.0 gigabitEthernet 0/1** varsayılan rota bilgisini giriniz.
- MLSW çok katmanlı ağ anahtarında **MLSW(config)#ip routing** komutunu çalıştırarak yönlendirici özelliğini aktif ediniz.
- MLSW çok katmanlı ağ anahtarına **MLSW(config)#ip route 0.0.0.0 0.0.0.0 gigabitEthernet 1/0/1** varsayılan rota bilgisini giriniz.

- R1 yönlendiricisine bağlı **10** ve **20** numaralı VLAN'ları geleneksel IVR yöntemiyle haberleştiriniz.
- **30**, **40** ve **50** numaralı VLAN'ları, MLSW çok katmanlı anahtarında sanal arayüzler oluşturarak haberleştiriniz.
- **60** ve **70** numaralı VLAN'ları, MLSW'de geleneksel IVR yöntemini uygulayarak haberleştiriniz.
- İlgili portları **Trunk** olarak yapılandırınız.
- İlgili portları **Access** olarak yapılandırınız.
- Tüm **Access** portlarında DTP protokolünü devre dışı bırakınız.
- SW2 ağ anahtarında **VLAN-80: YONETIM** VLAN'ını oluşturunuz ve VLAN-80 sanal arayüzüne **80.0.0.0/28** ağ adresinden IP adresi atayınız.
- MLSW çok katmanlı anahtarında VLAN-80 için sanal arayüz oluşturup uygun IP adresi ile yapılandırınız.
- SW2'ye varsayılan ağ geçidi olarak MLSW ağ anahtarının VLAN-80 arayüzünün IP adresini giriniz.
- SW2'ye **Telnet** ile erişebilmek için gerekli konfigürasyonu yapınız.
- Ağ anahtarlarında **99** numaralı VLAN oluşturunuz ve kullanılmayan tüm portları bu VLAN'a taşıyıp **shutdown** komutu ile kapatınız.
- Uç cihazları uygun IP adresi ile yapılandırınız.
- Tüm uç cihazlar arasında ping komutu ile bağlantı testi gerçekleştiriniz.

DEĞERLENDİRME

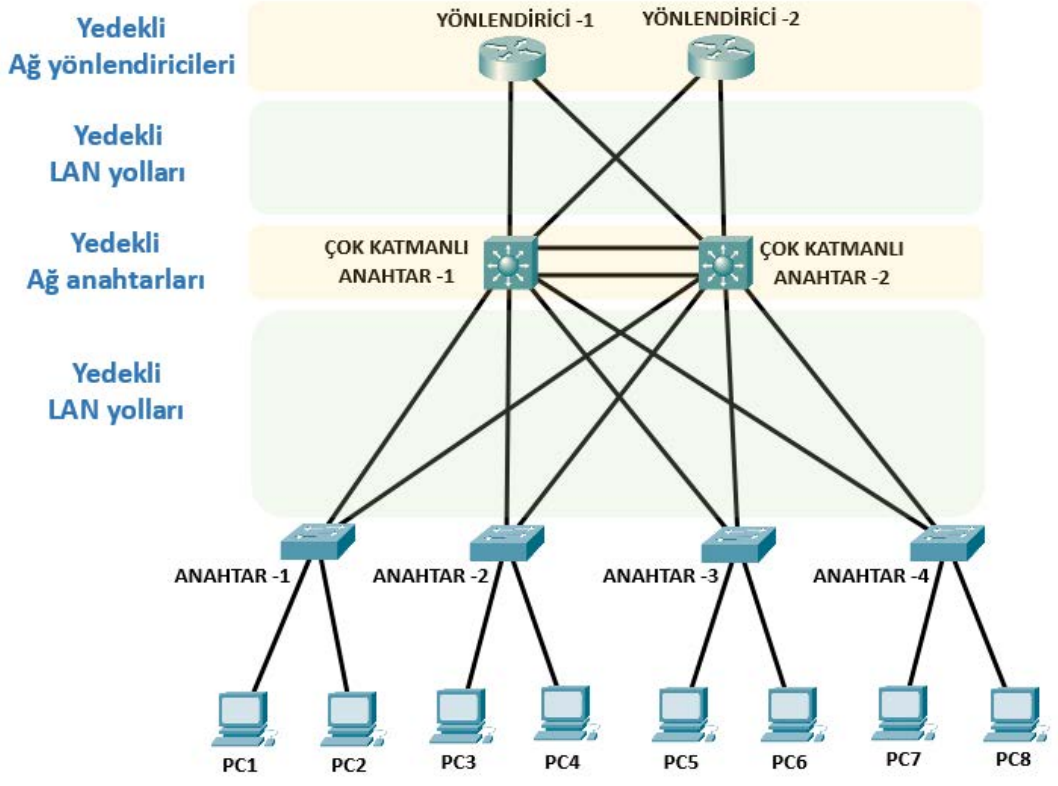
Çalışmanız aşağıda yer alan kontrol listesi kullanılarak değerlendirilecektir. Çalışmanızı yaparken değerlendirme ölçütlerini dikkate alınız.

KONTROL LİSTESİ

ÖLÇÜTLER	EVET	HAYIR
1. Ağ topolojisinin çizimini gerçekleştirdi.		
2. Ağ anahtarlarında uygun olan VLAN oluşturma işlemini gerçekleştirdi.		
3. Ağ anahtarlarında portları ilgili VLAN'a tanımladı.		
4. Geleneksel IVR yöntemini gerçekleştirdi.		
5. Router On A Stick yöntemiyle IVR işlemini gerçekleştirdi.		
6. Katman 3 ağ anahtarı yöntemiyle IVR işlemini gerçekleştirdi.		
7. Telnet protokolüyle ağ anahtarına uzaktan erişimi gerçekleştirdi.		
8. Uç cihazlar arasında bağlantı testi gerçekleştirdi.		

1.3. LAN YEDEKLİLİĞİ (LOCAL AREA NETWORK REDUNDANCY)

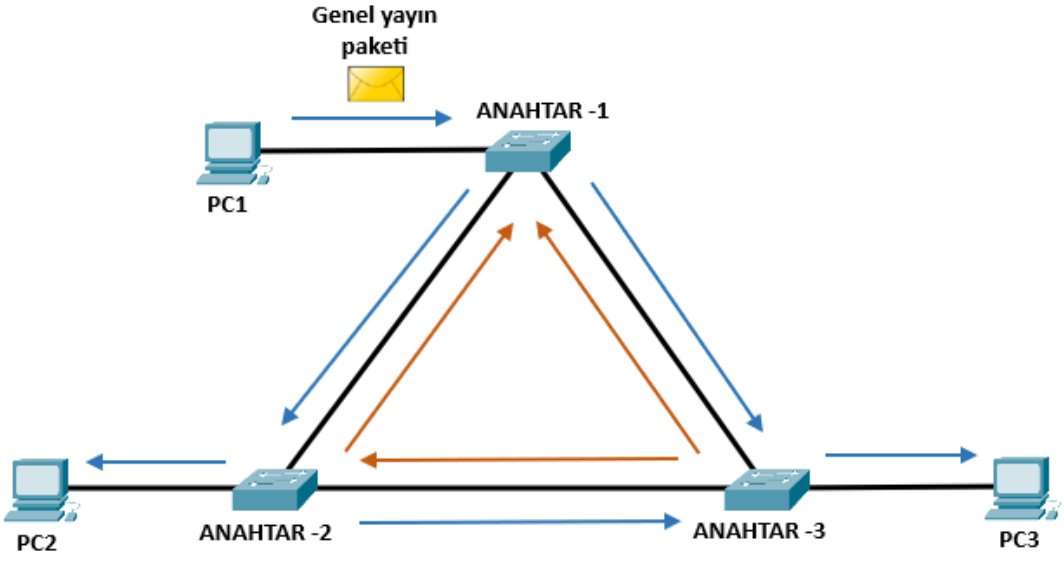
Ağa bağlı cihazların ve hizmetlerin kesintiye uğramaması kritik öneme sahiptir. Bu nedenle ağda yedeklilik sağlanması önemlidir. Yerel alan ağı yedekliliği, ağın sürekli erişilebilirliğini sağlamak için olası arızalar karşısında minimum kesintiyle çalışmasını sağlar. Yedekli bir yerel alan ağı mimarisi; birden fazla ağ bağlantısı, yönlendirici veya anahtar kullanarak oluşturulur (Görsel 1.49). Bu sayede bir ağ kablosu veya ağ cihazında meydana gelebilecek arıza durumunda ağ trafiği, diğer yedek ağ yollarını ve ağ cihazlarını kullanarak çalışmaya devam eder. Böylece ağ kesintisi ve veri kaybı en aza indirilir.



Görsel 1.49: Yedekli yerel alan ağı topolojisi

1.3.1. Kapsayan Ağaç Protokolü [STP (Spanning Tree Protocol)]

STP protokolü, 1985 yılında **Radia Perlman** isimli bilim insanı tarafından geliştirilir. Daha sonra IEEE tarafından 802.1D olarak standart hâline getirilir. Bu protokol özellikle Ethernet tabanlı ağlarda yaygın olarak kullanılır. STP protokolünün amacı, **katman 2 (layer 2)** trafiğinde **ağ döngülerini (loop)** önleyerek ve ağda yedekliliği sağlayarak veri iletiminin güvenli bir şekilde devam ettirilmesidir. Bir ağda kullanılan katman 2 anahtarların STP desteği olmaması durumunda yedeklilik sağlaması amacıyla yapılan kablolama, ağda döngü oluşmasına neden olabilir. Ağda oluşan bir döngü, bir başka deyişle verinin sürekli aynı yollar üzerinde dönmesi **genel yayın fırtınası (broadcast storm)** adı verilen ve ağ trafiğinin tıkanmasına neden olan bir soruna yol açar. Uç cihazlardan biri, bir genel yayın paketi gönderdiğinde bu paket, anahtar cihazları tarafından tüm cihazlara iletilir ve döngü nedeniyle bu genel yayın trafiği sürekli tekrar ederek çoğalır. Böylece ağ, kısa süre içinde çalışmaz hâle gelir (Görsel 1.50).



Görsel 1.50: Genel yayın fırtınası

Genel yayın fırtınası sonucu ayrıca şu sorunlar ortaya çıkar:

- Genel yayın paketlerinin sürekli artması sonucu ağ cihazlarının ve uç cihazların CPU yükü artar.
- Ağ anahtarlarının MAC adresi tablolarının stabilizasyonu bozulur.

STP protokolü, belirtilen sorunların oluşmasını engellemek için ağda döngü olup olmadığını kontrol eder. STP mesajları, anahtar cihazlarının birbirine gönderdiği **BPDU [Bridge Protocol Data Unit (Köprü Protokol Veri Birimi)]** paketleriyle iletilir. Ağda bir döngü mevcutsa anahtarlar üzerindeki bazı yolların trafiği engellenerek döngü önlenir.

1.3.1.1. Kapsayan Ağaç Protokolünün Çalışma Süreci

STP protokolü, döngüsüz bir ağ topolojisi oluşturmak için şu adımları gerçekleştirir:

1. Kök Köprü (Root Bridge) Seçme

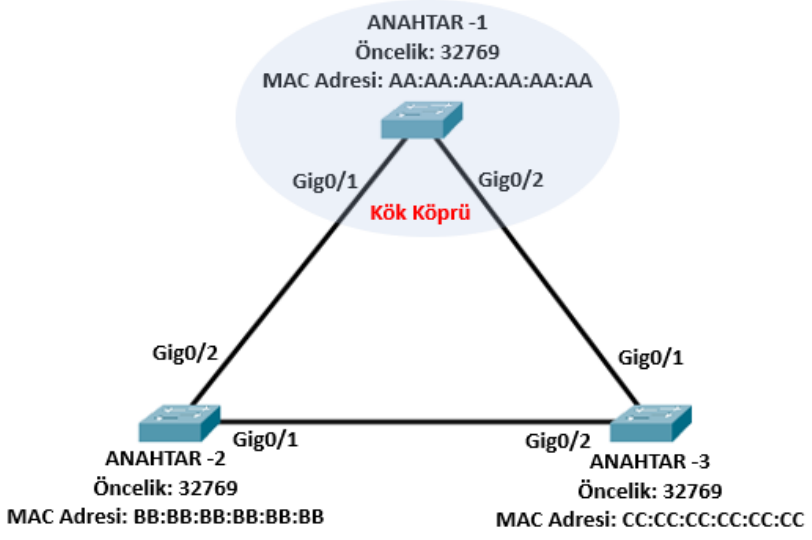
Anahtarlar ilk çalışmaya başladığında her biri kendini kök köprü ilan eder ancak BPDU paketlerini paylaşmaya başladıklarında birbiri hakkında bilgi edinmeye başlar. Bu bilgiler, kök anahtar seçiminde kullanılır. Kök köprü seçmek için öncelikle her anahtarın **BID**'si **[Bridge ID (Köprü Kimliği)]** belirlenir. BID; köprü önceliği, genişletilmiş sistem ID ve MAC adresi alanlarının birleşiminden oluşur (Görsel 1.51).

Köprü Öncelik Değeri	Genişletilmiş Sistem Kimliği	MAC Adresi
4 Bit	12 Bit	48 Bit

Görsel 1.51: Köprü kimliği

Köprü öncelik değeri (Bridge Priority), anahtar cihazlarında varsayılan olarak genellikle 32.768'dir. Genişletilmiş sistem kimliği ise varsayılanda **1**'dir. 1 değeri, varsayılan VLAN numarasının değeridir ve bu değer, köprü öncelik değeri ile toplanır. Sadece köprü öncelik değerine bakılarak kök köprü seçilebilir. Köprü öncelik değeri küçük olan anahtar, kök köprü seçilir. Köprü öncelik değerlerinin eşit olması duru-

munda MAC adresi belirleyici olur. MAC adresi küçük olan anahtar, kök köprü seçilir (Görsel 1.52). Kök köprü önceliği küçültülerek de istenen anahtarın kök köprü olması sağlanır.



Görsel 1.52: Kök köprü seçimi

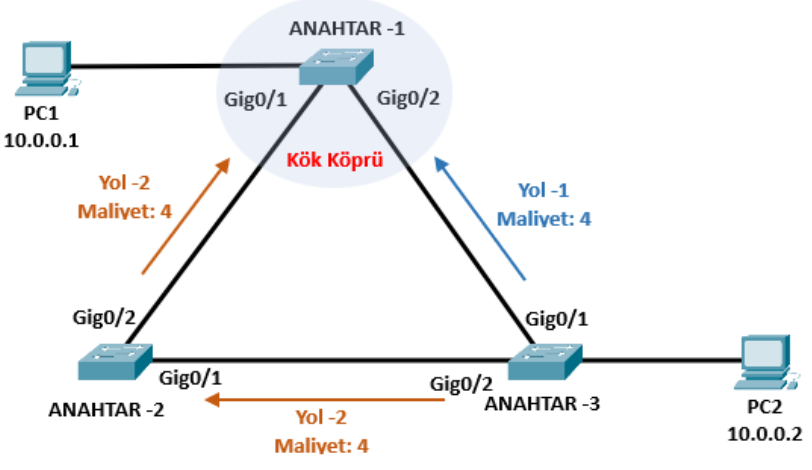
2. Kök Yol (Root Path) Maliyetini Hesaplama

Kök yol maliyetini hesaplama, genel yayın alanı içinde kök köprüye olan en iyi yolu bulmak için gerçekleştirilen işlemdir. Maliyet, ağdaki her anahtardan kök köprüye giden yol boyunca ortaya çıkan maliyetlerin toplanmasıyla elde edilir. Maliyet değerleri, anahtar portlarının bağlantı hızlarına göre değişiklik gösterir (Tablo 1.3).

Tablo 1.3: STP Kök Yol Maliyet Tablosu

Arayüz Bağlantı Hızı	STP 802.1D Maliyeti
10 Gbps	2
1 Gbps	4
100 Mbps	19
10 Mbps	100

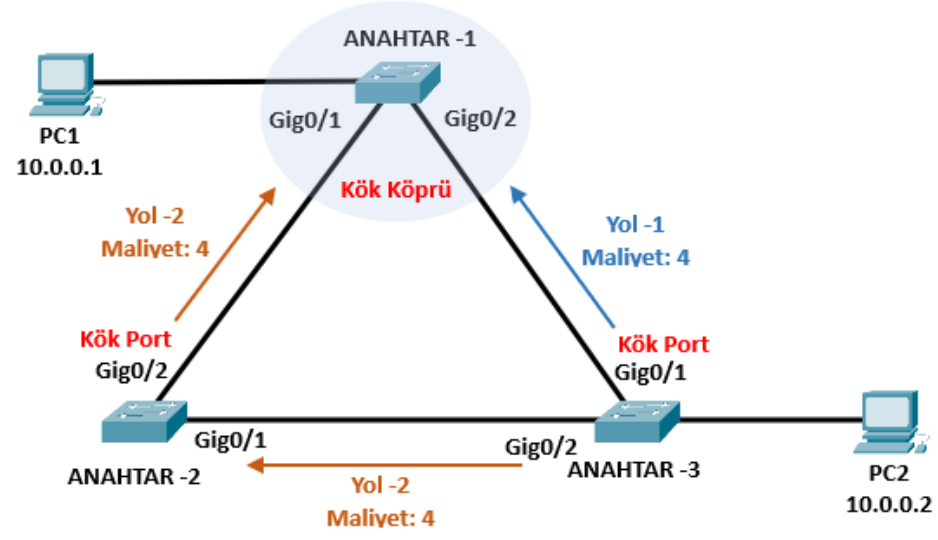
Görsel 1.53'te PC2'den PC1'e giden en iyi yolun kök yol maliyet hesaplaması görülür. Buna göre Yol-1'in toplam maliyeti 4, Yol-2'nin toplam maliyeti ise 8'dir. Bu nedenle trafik, maliyeti düşük olan 1 numaralı yoldan gider.



Görsel 1.53: STP kök yol hesaplaması

3. Kök Portları (Root Port) Belirleme

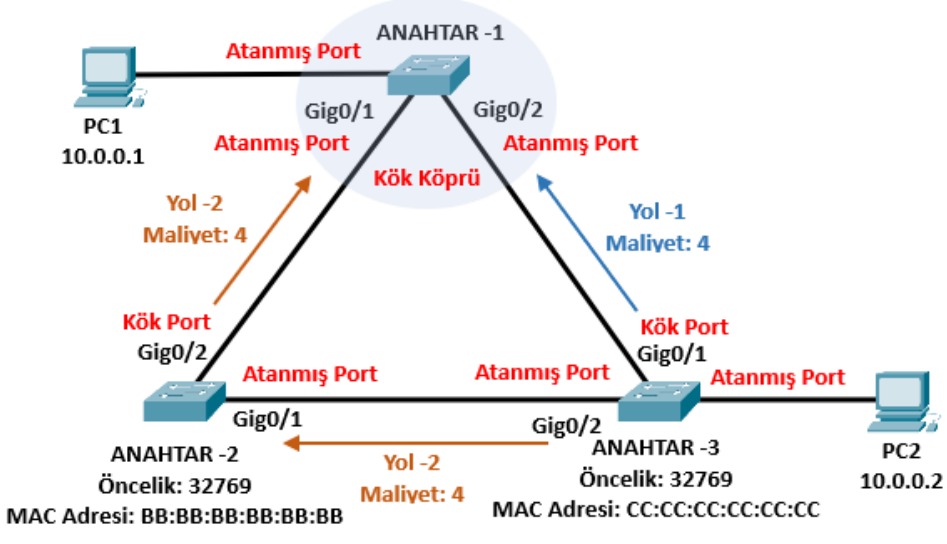
Kök portları, kök köprü olmayan anahtarların üzerinde bulunur ve kök köprüye ulaşmak için bir anahtarın kullandığı en düşük maliyetli bağlantıdır (Görsel 1.54). Kök portların anahtar üzerindeki ağ trafiğini gösteren kısmında **yeşil** LED ışığı yanar.



Görsel 1.54: STP kök port belirleme

4. Atanmış Portları (Designated Port) Belirleme

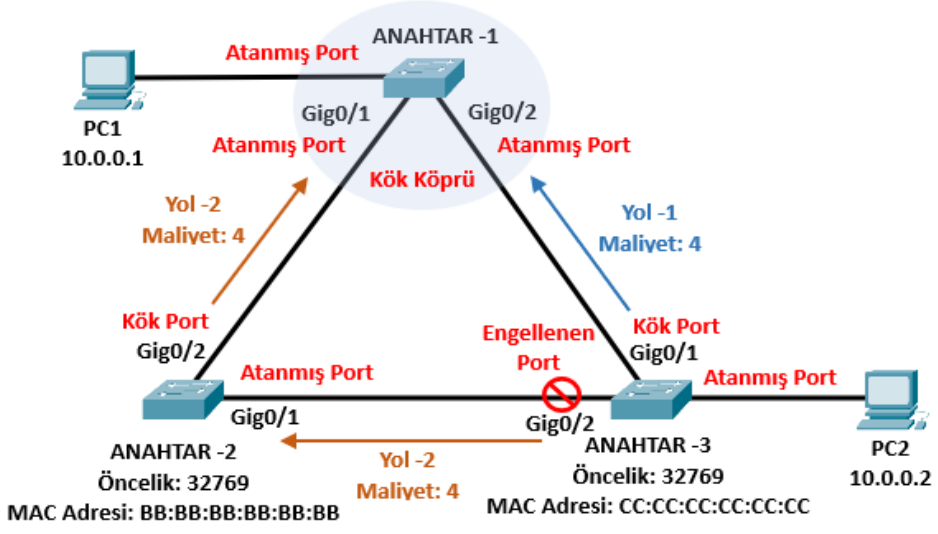
Anahtarlar arası her bağlantıda yalnızca bir atanmış port bulunur. Kök köprü üzerindeki tüm portlar, atanmış porttur. Kök köprü olmayan anahtarlar üzerinde kök port olarak tanımlanmayan portlar, atanmış port olarak belirlenir (Görsel 1.55). Atanmış portların anahtar üzerindeki ağ trafiğini gösteren kısmında **yeşil** LED ışığı yanar.



Görsel 1.55: STP atanmış port belirleme

5. Engellenen Portu (Blocked Port veya Alternate Port) Belirleme

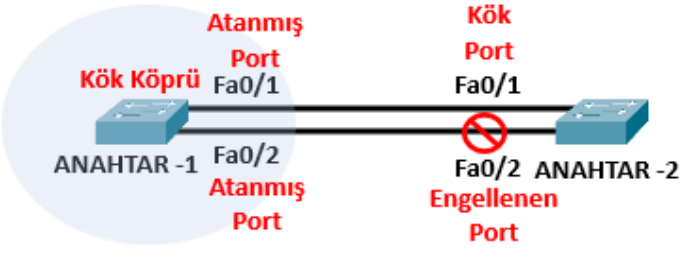
Kök köprü olmayan anahtarlar arasındaki atanmış portlardan biri engellenen port olarak belirlenir (Görsel 1.56). Engellenen portu belirlemek için atanmış portların kök yol maliyetleri hesaplanır. Kök yol maliyeti düşük olan port, atanmış port olarak kalır. Diğer atanmış port ise engellenen port olarak belirlenir. Her iki atanmış portun kök yol maliyetinin eşit olması durumunda BID değeri küçük olan anahtar üzerindeki port, atanmış port diğer anahtar üzerindeki port ise engellen port olur. Engellenen portun bulunduğu yolda anahtarlar arası veri trafiği olmaz ancak BPDU paketleri iletilmeye devam eder. Aktif olan yollardan birinde problem meydana geldiğinde anahtarlar bu durumu yine BPDU mesajlarıyla anlar ve engellenen port, döngü oluşturmuyorsa ağ trafiğine açılır. Engellenen portun anahtar üzerinde ağ trafiğini gösteren kısmında **turuncu** LED ışığı yanar.



Görsel 1.56: STP engellenen portu belirleme

1.3.1.2. İki Ağ Anahtarının İki Fiziksel Portla Bağlanması

İki ağ anahtarın birbirine birden fazla fiziksel portla bağlanması durumunda döngü oluşur. Döngü oluşmasını engellemek için STP protokolü, tekrar kök köprü seçimi gerçekleştirir. BID değeri küçük olan anahtar, kök köprü olarak seçilir. Kök köprü üzerindeki portlar, atanmış port olarak tanımlanır. Diğer anahtar üzerindeki portlar, kök port olarak tanımlanmak istenir ancak bir anahtar üzerinde birden fazla kök port olamaz. Bu durumda öncelikle kök yol maliyetleri karşılaştırılır. Maliyeti düşük olan port, kök port olur. Diğeri ise engellenen port olur. Kök yol maliyetlerinin eşit olması durumunda **port önceliği (port priority)** değerleri karşılaştırılır. Port öncelik değeri, **128. Port Numarası** şeklinde bir ifadedir. Port öncelik değeri küçük olan port, **kök port**; diğeriyse **engellenen port** olarak tanımlanır (Görsel 1.57).



Görsel 1.57: İki anahtar arasında STP süreci

1.3.1.3. STP Sürecinde Port Durumları

STP protokolünün ağ döngülerini önlemek amacıyla anahtar portları için beş farklı durumu vardır (Tablo 1.4).

Tablo 1.4: STP Protokolünün Anahtar Port Durumları

Port Durumu	BPDU Alma/Gönderme	MAC Adresi Öğrenme	Çerçeve İletimi
Engelleme	Evet / Hayır	Hayır	Hayır
Dinleme	Evet / Evet	Hayır	Hayır
Öğrenme	Evet / Evet	Evet	Hayır
İletim	Evet / Evet	Evet	Evet
Kapalı Arayüz	Hayır / Hayır	Hayır	Hayır

Engelleme (Blocking): Ağa dâhil olan portun ilk durumu, engellenen port durumudur. Bu durumda kök anahtarın belirlenmesi için BPDU paketleri alır. Veri çerçevelerini iletmez. Durum süresi 20 saniyedir.

Dinleme (Listening): Port kök anahtar yolunu belirlemek için BPDU paketlerini alır. Ayrıca komşu anahtarlar, BPDU paketlerini ileterek portun ağa dâhil olmaya hazırlandığını belirtir. Herhangi bir döngü durumu söz konusu ise port tekrar engelleme durumuna geçer. MAC adresi öğrenme süreci başlamadığı için MAC adresi tablosu güncellenmez. Dinleme süresi 15 saniyedir.

Öğrenme (Learning): Komşu anahtar MAC adreslerinin porttan öğrenilmeye başlandığı durumdur. Veri iletimi henüz başlamamıştır. Öğrenme süresi 15 saniyedir.

İletim (Forwarding): Port, tüm ağ trafiğine açıktır.

Kapalı Port (Disabled): Anahtar portu kapalıdır ve herhangi bir veri iletimi gerçekleştirmez. Port, bu durumda STP sürecine dâhil değildir.

1.3.1.4. Kapsayan Ağaç Protokolü Türleri

STP protokolünün IEEE 802.1D sürümünden itibaren farklı türleri geliştirilir. STP protokolünün farklı sürümleri Tablo 1.5'te görülür.

Tablo 1.5: STP Protokolünün Türleri

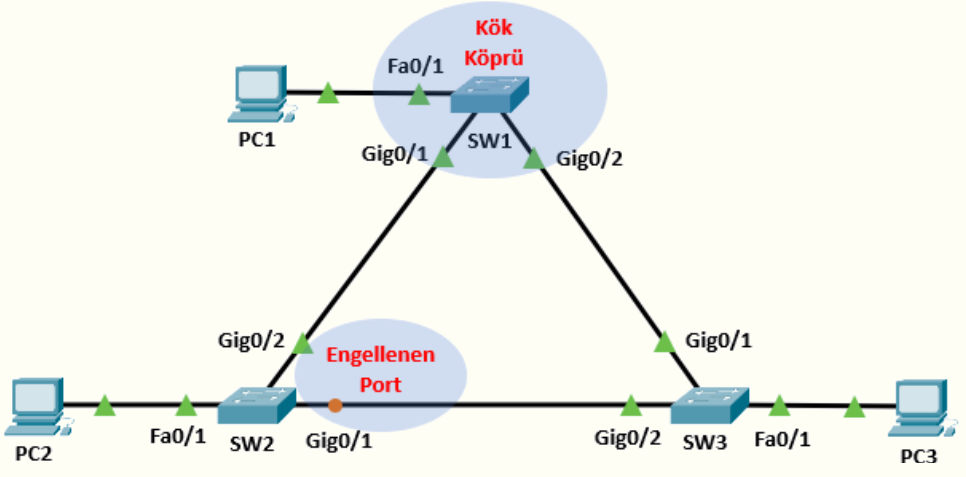
STP Türü	Açıklama
STP (Spanning Tree Protocol)	IEEE 802.1D standardıyla standartlaşmış ve ağda döngüleri önlemek için kullanılan temel protokoldür.
PVST+ (Per Vlan Spanning Tree Plus)	Her VLAN için ayrı bir STP ağacı oluşturarak VLAN bazında döngüleri önler.
RSTP (Rapid Spanning Tree Protocol)	IEEE 802.1w standardıyla standart hâle gelen bu protokol, STP'nin yakınsama süresini hızlandırarak ağdaki değişikliklere hızla yanıt verir.
Rapid PVST+ (Rapid Per Vlan Spanning Tree Plus)	Her VLAN için ayrı bir STP ağacı oluşturur ve yakınsama süresi hızlıdır.
MST (Multiple Spanning Tree)	VLAN'ları gruplandırarak örnek (instance) oluşturulur ve her örnek için bir STP ağacı oluşturulur.

NOT: Bir ağ topolojisinde STP türü değiştirilmek isteniyorsa ağda bulunan tüm ağ anahtarlarında STP türü değiştirilerek aynı duruma getirilmelidir. Aksi takdirde STP hesaplamalarında hata oluşabilir.

7. UYGULAMA

STP uygulama işlemini verilen adımlar doğrultusunda gerçekleştiriniz.

1. Adım: Ağ simülasyon programında Görsel 1.58'deki ağ topolojisini oluşturunuz.



Görsel 1.58: STP protokolü uygulama topolojisi

2. Adım: SW1 anahtarında CLI moduna girip, **show spanning tree** komutunu çalıştırarak STP durumlarını görüntüleyiniz (Görsel 1.59).

```
SW1#show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    32769
              Address     0090.0C54.37D4
              This bridge is the root
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32769  (priority 32768 sys-id-ext 1)
              Address     0090.0C54.37D4
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------
Fa0/1            Desg FWD 19        128.1    P2p
Gi0/1            Desg FWD 4         128.25   P2p
Gi0/2            Desg FWD 4         128.26   P2p
```

Görsel 1.59: SW1 anahtarına ait STP durum çıktısı

3. Adım: SW2 anahtarında CLI moduna girip, **show spanning tree** komutunu çalıştırarak STP durumlarını görüntüleyiniz (Görsel 1.60).

```
SW2#show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    32769
              Address     0090.0C54.37D4
              Cost        4
              Port        26(GigabitEthernet0/2)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32769  (priority 32768 sys-id-ext 1)
              Address     00E0.A3AE.51C1
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------
Fa0/1            Desg FWD 19        128.1    P2p
Gi0/1            Altn BLK 4         128.25   P2p
Gi0/2            Root FWD 4         128.26   P2p
```

Görsel 1.60: SW2 anahtarına ait STP durum çıktısı

4. Adım: SW3 anahtarında CLI moduna girip, **show spanning tree** komutunu çalıştırarak STP durumlarını görüntüleyiniz (Görsel 1.61).

```
SW3#show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    32769
              Address     0090.0C54.37D4
              Cost        4
              Port        25(GigabitEthernet0/1)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32769  (priority 32768 sys-id-ext 1)
              Address     00D0.BC37.0C60
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------
Fa0/1            Desg FWD 19        128.1    P2p
Gi0/1            Root FWD 4         128.25   P2p
Gi0/2            Desg FWD 4         128.26   P2p
```

Görsel 1.61: SW3 anahtarına ait STP durum çıktısı

5. Adım: PC1, PC2 ve PC3 uç cihazlarının bağlı olduğu anahtar portlarında STP protokolünü devre dışı bırakarak portların hızlı bir şekilde iletim durumuna geçmesini sağlayınız.

```
SW1(config)#interface fastEthernet 0/1

SW1(config-if)#spanning-tree portfast
```

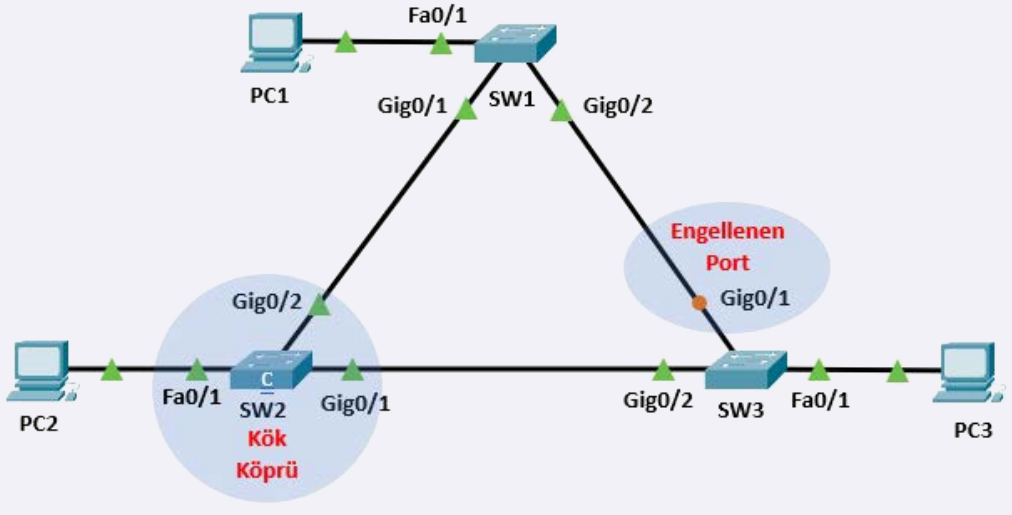
```
SW2(config)#interface fastEthernet 0/1
SW2(config-if)#spanning-tree portfast
SW3(config)#interface fastEthernet 0/1
SW3(config-if)#spanning-tree portfast
```

6. Adım: PC1, PC2 ve PC3 uç cihazlarının bağlı olduğu anahtar portlarından BPDU paketlerinin alınmasını engelleyiniz.

```
SW1(config)#interface fastEthernet 0/1
SW1(config-if)#spanning-tree bpduguard enable
SW2(config)#interface fastEthernet 0/1
SW2(config-if)#spanning-tree bpduguard enable
SW3(config)#interface fastEthernet 0/1
SW3(config-if)#spanning-tree bpduguard enable
```

7. Adım: SW2 anahtarında CLI moduna girip, VLAN-1 için öncelik değerini (BID Priority) **0** tanımlayarak kök köprü olmasını sağlayınız (Görsel 1.62).

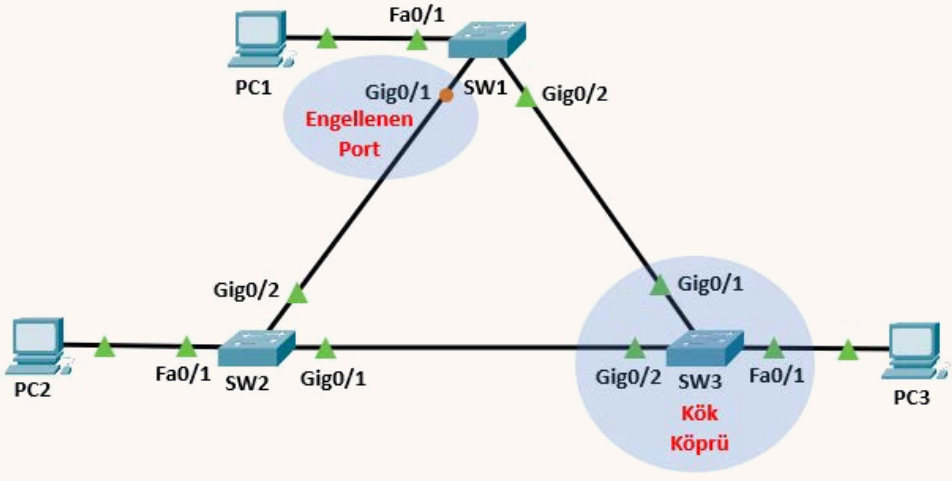
```
SW2(config)#spanning-tree vlan 1 priority 0
```



Görsel 1.62: SW2'nin kök köprü olmasının sağlanması

8. Adım: SW3 anahtarının CLI moduna girip, VLAN-1 için herhangi bir ölçüte bakmadan kök köprü olmasını sağlayacak konfigürasyonu yapınız (Görsel 1.63).

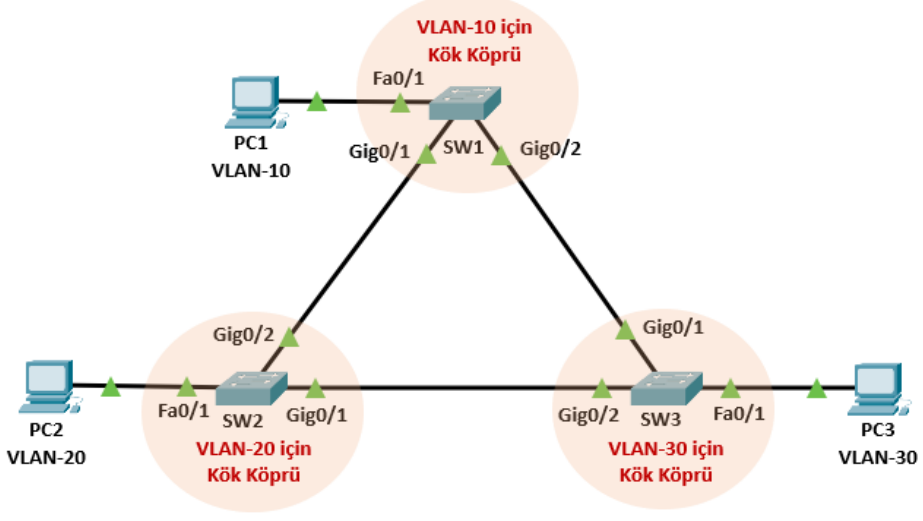
```
SW3(config)#spanning-tree vlan 1 root primary
```



Görsel 1.63: SW3'ün kök köprü olmasının sağlanması

SIRA SİZDE

Ağ simülasyon programında Görsel 1.64'teki ağ topolojisini çiziniz. Topoloji üzerinde belirtilen VLAN'lar için ilgili ağ anahtarının kök köprü olmasını sağlayacak ve uç cihazlarda STP protokolünü devre dışı bırakıp BPDU paketi alınmasını engelleyecek konfigürasyonları gerçekleştiriniz.



Görsel 1.64: Her VLAN için ayrı kök köprü belirleme ağ topolojisi

DEĞERLENDİRME

Çalışmanız aşağıda yer alan kontrol listesi kullanılarak değerlendirilecektir. Çalışmanızı yaparken değerlendirme ölçütlerini dikkate alınız.

KONTROL LİSTESİ

ÖLÇÜTLER	EVET	HAYIR
1. Ağ topolojisinin çizimini gerçekleştirdi.		
2. Anahtarlarda ilgili VLAN'ları oluşturdu.		
3. Anahtarlarda ilgili portları ilgili VLAN'a tanımladı.		
4. Anahtarlarda ilgili portları Trunk olarak yapılandırdı.		
5. Anahtarlarda STP türünü Rapid PVST olarak değiştirdi.		
6. VLAN 10 için SW1'in kök köprü olmasını sağladı.		
5. VLAN-20 için SW2'nin kök köprü olmasını sağladı.		
6. VLAN-30 için SW3'ün kök köprü olmasını sağladı.		
7. Uç cihazların bağlı olduğu portlarda STP protokolünü devre dışı bıraktı.		
8. Uç cihazların bağlı olduğu portlardan BPDU paketi alınmasını engelledi.		

1.3.2. Port Kümeleme (Link Aggregation)

Port kümeleme; ağ ortamında ağ anahtarları, yönlendiriciler ve sunucular arasında bağlantı bant genişliğini (bandwidth) artırmak; hata toleransı (fault tolerance), yük dengeleme (load balancing) ve yedeklilik sağlamak amacıyla STP engeline takılmadan birden fazla fiziksel portu tek bir mantıksal arayüz altında birleştiren teknolojidir (Görsel 1.65). Örneğin 1 Gbps bant genişliğine sahip iki fiziksel portun kümeleme işlemi sonunda oluşan mantıksal arayüz, 2 x 1 Gbps = 2 Gbps bant genişliğine sahip olur. Bu sayede cihazlar arasında daha yüksek veri transfer hızları da mümkündür.



Görsel 1.65: Port kümeleme işlemi

Fiziksel portlar bir mantıksal arayüz altında kümelendikten sonra ayrı ayrı fiziksel portları yönetmek yerine mantıksal arayüzü yönetmek yeterli olur.

1.3.2.1. Port Kümelemenin Avantajları

Ağ ortamında port kümelemenin başlıca avantajları şunlardır:

- Tek bir mantıksal arayüzü yönetmek, birden fazla fiziksel portu tek tek yönetmekten daha kolaydır.
- Fiziksel portlardan herhangi birinde veya birkaçında sorun ortaya çıktığında trafik, kesintiye uğramadan diğer port yahut portlar üzerinden devam eder. Bu sayede ağ kesintileri önlenir.
- Maliyeti sıfırdır. Port kümeleme işlemi sayesinde bant genişliği artırılabilir. Bu nedenle ekstra cihaz yatırımı yapmaya gerek kalmaz.
- STP protokolüyle uyumlu çalışır ve döngü oluşma riskini ortadan kaldırır.
- Birden fazla portun kümeleme işlemiyle birleştirilmesi tek bir porta bağımlı kalmadan yedeklilik sağlar. Bu sayede tek nokta hatalarına [SPoF (Single Point of Failure)] karşı dayanıklılık kazanılır.
- Trafik, birden fazla fiziksel port üzerinden dağıtılarak yük dengelemesi sağlanır.
- Port kümeleme hem katman 2 (Layer 2) hem de katman 3'te (Layer 3) çalışabilir. Böylece farklı seviyelerdeki bağlantı ihtiyaçları karşılanabilir.

1.3.2.2. Port Kümeleme Uygulamasında Dikkat Edilmesi Gereken Hususlar

Port kümeleme uygulamasında dikkat edilmesi gereken hususlar şunlardır:

- Kümelenecek port türleri aynı olmalıdır. Örneğin GigabitEthernet ve FastEthernet portları aynı küme içinde kullanılamaz.
- Kümelenecek tüm portların dublex modları aynı olmalıdır.
- Port kümeleme işlemi, her iki cihazda da aynı yöntemle yapılmalıdır. Statik olarak veya aynı protokol kullanılarak işlem gerçekleştirilmelidir.
- Bir ağ anahtarının port kümeleme işlemi yapılan fiziksel portları, Trunk olarak yapılandırılmışsa diğer ağ anahtarında da port kümeleme işlemi yapılacak fiziksel portların Trunk olarak yapılandırılması gerekir.
- Her iki ağ anahtarında da port kümelemeye dâhil olacak Trunk olarak yapılandırılan fiziksel portların yerel VLAN'ı aynı olmalıdır.
- Bir ağ anahtarında oluşturulacak port kümeleme işlemi, cihazın özelliklerine bağlı olarak sınırlıdır. Bu nedenle bir ağ anahtarında birden fazla port kümeleme işlemi yapılacaksa cihazın desteklediği maksimum port kümeleme sınırını bilmek faydalı olur.

1.3.2.3. Port Kümeleme Yöntemleri

Port kümeleme işlemi, iki şekilde gerçekleştirilir.

1. Statik Olarak Port Kümeleme

Statik port kümeleme yönteminde herhangi bir protokol veya otomatik bir yapılandırma kullanılmaz. Ağ anahtarları arasında otomatik anlaşma süreci yoktur. Anahtarlarda port kümeleme işlemine dâhil olacak portlar, **channel-group <Grup Numarası> mode on** şeklinde yapılandırılmalıdır (Tablo 1.6). Yapılandırma sonucunda anahtarlar arasında kanal oluşturulur.

Tablo 1.6: Statik Port Kümeleme İşlemiyle Kanal Kurulum Durumu

Statik Port Kümeleme		
Anahtar-1	**Anahtar-2**	**Kanal Kurulumu**
On	On	Evet

2. Protokolleri Kullanarak Port Kümeleme

PAgP (Port Aggregation Protocol) Protokolüyle Port Kümeleme: Özel bir üretici tarafından geliştirilmiş bir port kümeleme protokolüdür. Özel üreticiye ait ağ anahtarları arasında otomatik anlaşma yöntemiyle kanal oluşturulur. Anahtarlarda port kümeleme işlemine dâhil olacak portlar, **channel-group <Grup Numarası> mode <Desirable/Auto>** şeklinde yapılandırılmalıdır. PAgP protokolü kullanılarak yapılan port kümeleme işlemi sonucunda kanal kurulum durumu Tablo 1.7'de görülür.

Tablo 1.7: PAgP Protokolüyle Port Kümeleme İşlemi Kanal Kurulum Durumu

PAgP Protokolü ile Port Kümeleme		
Anahtar-1	**Anahtar-2**	**Kanal Kurulumu**
Desirable	Desirable	Evet
Auto	Desirable	Evet
Desirable	Auto	Evet
Auto	Auto	Hayır

LACP (Link Aggregation Control Protocol) Protokolüyle Port Kümeleme: LACP protokolü, IEEE 802.3ad standardıyla tanımlanmıştır. Tüm markaların desteklediği bir port kümeleme protokolüdür. PAgP protokolünde olduğu gibi LACP protokolünde de anahtarlar arasında otomatik anlaşma yöntemiyle kanal oluşturulur. Anahtarlarda port kümeleme işlemine dâhil olacak portlar, **channel-group <Grup Numarası> mode <Active/Passive>** şeklinde yapılandırılmalıdır. LACP protokolü kullanılarak yapılan port kümeleme işlemi sonucunda kanal kurulum durumu Tablo 1.8'de görülür.

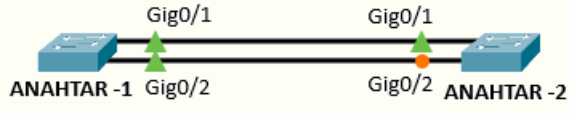
Tablo 1.8: LACP Protokolüyle Port Kümeleme İşlemi Kanal Kurulum Durumu

LACP Protokolü ile Port Kümeleme		
Anahtar-1	**Anahtar-2**	**Kanal Kurulumu**
Active	Active	Evet
Passive	Active	Evet
Active	Passive	Evet
Passive	Passive	Hayır

LACP protokolünü kullanarak port kümeleme işlemini verilen adımlar doğrultusunda gerçekleştiriniz.

8. UYGULAMA

1. Adım: Ağ simülasyon yazılımında Görsel 1.66'daki ağ topolojisini oluşturunuz.



Görsel 1.66: Arayüz kümeleme uygulama topolojisi

2. Adım: ANAHTAR-1 cihazında CLI moduna girerek LACP protokolüyle port kümeleme konfigürasyonunu gerçekleştiriniz.

ANAHTAR-1(config)#interface range gigabitEthernet 0/1-2

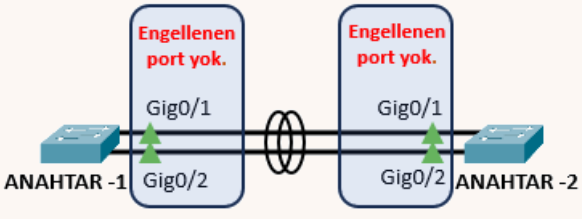
ANAHTAR-1(config-if-range)#channel-group 1 mode active

3. Adım: ANAHTAR-2 cihazında CLI moduna girerek LACP protokolüyle port kümeleme konfigürasyonunu gerçekleştiriniz.

ANAHTAR-2(config)#interface range gigabitEthernet 0/1-2

ANAHTAR-2(config-if-range)#channel-group 1 mode active

4. Adım: Anahtar cihazlarında engellenen bir port ve döngü oluşmadan port kümeleme işleminin gerçekleştiğini gözlemleyiniz (Görsel 1.67).



Görsel 1.67: Port kümeleme

5. Adım: Anahtar cihazlarında CLI moduna girip, **show etherchannel summary** komutunu çalıştırarak port kümelemeyle ilgili özet bilgilere ulaşınız (Görsel 1.68).

```
ANAHTAR-1#show etherchannel summary
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port

Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------

1      Po1(SU)         LACP      Gig0/1(P) Gig0/2(P)
```

Görsel 1.68: Port kümeleme durumunu görüntüleme

6. Adım: Anahtar cihazlarında CLI moduna girerek **show running-config** komutunu çalıştırınız ve oluşturulan kümelenmiş sanal arayüzü çalışan konfigürasyon dosyasında görüntüleyiniz (Görsel 1.69).

```
hostname ANAHTAR-1
!
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface Port-channel1
```

→ Kümelenmiş sanal arayüz

Görsel 1.69: Kümelenmiş sanal arayüzü çalışan konfigürasyon dosyasında görüntüleme

7. Adım: Anahtar cihazlarında CLI moduna girerek **show ip interface brief** komutunu çalıştırınız ve port kümeleyerek oluşturulan **Port-channel1** sanal arayüzünün aktif olduğunu görüntüleyiniz (Görsel 1.70).

```
ANAHTAR-1#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
Port-channel1          unassigned      YES manual up                    up
FastEthernet0/1        unassigned      YES manual down                  down
FastEthernet0/2        unassigned      YES manual down                  down
FastEthernet0/3        unassigned      YES manual down                  down
FastEthernet0/4        unassigned      YES manual down                  down
FastEthernet0/5        unassigned      YES manual down                  down
```

Görsel 1.70: Arayüz tablosunda Port-Channel1 sanal arayüzünü görüntüleme

8. Adım: Anahtar cihazlarında **show interfaces port-channel 1** komutunu çalıştırınız ve sanal arayüzün bant genişliğinin iki fiziksel portun bant genişliği toplamlarına eşit olduğunu görüntüleyiniz (Görsel 1.71).

```
ANAHTAR-1#show interfaces port-channel 1
Port-channel1 is up, line protocol is up (connected)
  Hardware is EtherChannel, address is 000c.8570.7ee8 (bia 000c.8570.7ee8)
  MTU 1500 bytes, BW 2000000 Kbit, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Half-duplex, 2000Mb/s
```

Görsel 1.71: Kümelenmiş sanal arayüzün bant genişliğini görüntüleme

9. Adım: Anahtar cihazlarında CLI moduna girip, kümelenmiş sanal arayüzleri **Trunk** olarak yapılandırınız.

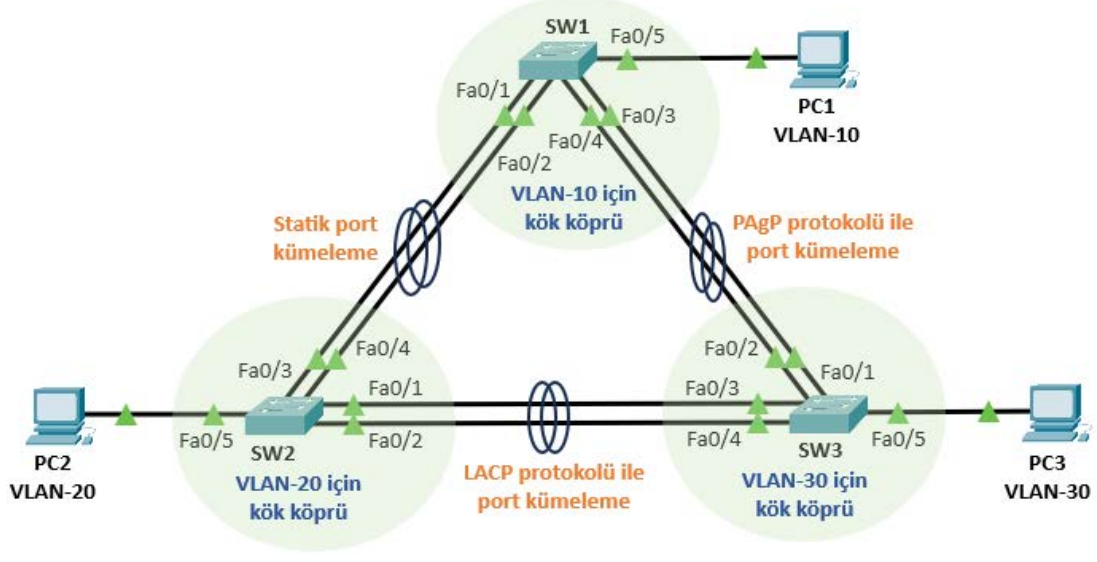
```
ANAHTAR-1(config)#interface port-channel 1
ANAHTAR-1(config-if)#switchport mode trunk
ANAHTAR-2(config)#interface port-channel 1
ANAHTAR-2(config-if)#switchport mode Trunk
```

10. Adım: Anahtar cihazlarında CLI moduna girerek kümelenmiş sanal arayüzlerde DTP protokolünü devre dışı bırakınız.

```
ANAHTAR-1(config)#interface port-channel 1
ANAHTAR-1(config-if)#switchport nonegotiate
ANAHTAR-2(config)#interface port-channel 1
ANAHTAR-2(config-if)#switchport nonegotiate
```

SIRA SİZDE

Ağ simülasyon programında Görsel 1.72'deki ağ topolojisini çiziniz. Anahtarlar arası port kümeleme işlemlerini gerçekleştirip topoloji üzerinde belirtilen VLAN'lar için ilgili ağ anahtarının, kök köprü olmasını sağlayınız.



Görsel 1.72: Üç anahtar arası döngüsüz port kümeleme uygulama topolojisi

DEĞERLENDİRME

Çalışmanız aşağıda yer alan kontrol listesi kullanılarak değerlendirilecektir. Çalışmanızı yaparken değerlendirme ölçütlerini dikkate alınız.

KONTROL LİSTESİ

ÖLÇÜTLER	EVET	HAYIR
1. Ağ topolojisinin çizimini gerçekleştirdi.		
2. Anahtarlarda ilgili VLAN'ları oluşturdu.		
3. Anahtarlarda ilgili portları ilgili VLAN'a tanımladı.		
4. Anahtarlar arası port kümeleme işlemini gerçekleştirdi.		
5. Anahtarlarda kümelenmiş sanal arayüzleri Trunk olarak yapılandırdı.		
6. Anahtarlarda STP türünü Rapid PVST olarak değiştirdi.		
7. VLAN 10 için SW1'in kök köprü olmasını sağladı.		
8. VLAN-20 için SW2'nin kök köprü olmasını sağladı.		
9. VLAN-30 için SW3'ün kök köprü olmasını sağladı.		



İnsanlığın Hayali: Yapay Genel Zekâ Nedir? Yapay Zekâdan Farkları Neler?

Dr. Elif Ebren Kaya **14/06/2024**

Makinelerin yalnızca önceden programlandıkları görevlerle sınırlı olmadığını, insana özgü yetenekler ve kendine yeterlilikle çalıştığını hayal edin. Bu, mevcut yapay zekânın geliştirilmiş bir versiyonu olarak da düşünülebilecek genel yapay zekâ çalışmaları ile gerçeğe dönüşebilir.

Yapay Genel Zekâ Nedir?

Yapay genel zekâ (AGI), kısaca insan beyninin tüm bilişsel yeteneklerine sahip bir yapay zekâ çalışma alanıdır. Henüz mevcut bir uygulaması olmayan bu çalışma alanında araştırmalar ve denemeler devam ediyor. Bu çalışma alanının temel hedefi, kendi kendine öğrenme yeteneğiyle insan benzeri bir zekâ üretebilmektir. Yapay genel zekânın günümüzdeki yapay zekâ (AI) uygulamalarından farkı ise bilinç ve

öz farkındalıktır. Günümüzde mevcut yapay zekâ teknolojilerinin tümü önceden belirlenmiş bir dizi parametreye göre çalışıyor. Örneğin metin çevirileri konusunda eğitilen bir yapay zekâ modeli sesli komutlarla isteneni anlayıp bir görüntü oluşturamaz. Ancak yapay genel zekâ teknolojisine sahip makinelerin bilgileri çok hızlı bir şekilde işlemesi ve karmaşık sorunları öğrenip çözüm geliştirebileceği öngörülüyor. Bu özellikleri sayesinde endüstride ve diğer alanlarda birçok görevi üstleneceği düşünülüyor.

Hâlihazırda etkileyici yetenekleriyle yollarda kendi kendine giden sürücüsüz otomobiller veya çok büyük miktarda veriyi analiz edebilen süper bilgisayarlar belirli görevleri mükemmel bir şekilde gerçekleştirmek için tasarlanan makinelerdir. Ancak bilgi ve becerilerini bir alandan diğerine aktarma yetenekleri yoktur. Bundan dolayı aslında dar kapsamlı birer yapay zekâ örnekleridir. Çalışmaları süren yapay genel zekânın ise insan zekâsına benzer şekilde çok çeşitli görev ve alanlarda bilgi anlama, öğrenme ve uygulama yeteneğine sahip olacağı düşünüldüğünde hayallerimizin ötesinde işler yapabileceğini söyleyebiliriz.

Peki Yapay Genel Zekâ Ne Zaman Gerçekleşecek?

Yapay genel zekâ, genelleme yapabilmeyi, bir alanda öğrenileni diğer alanlarda kullanabilmeyi gerektirir. Belirli bir veri alanında çalışabilen bir yapay zekânın aksine genel yapay zekâ, farklı alanlardaki bilgi kümelerinin birbirleriyle nasıl ilişkili olduğunu kavrayabilmeyi gerektiren karmaşık bir yapay zekâ modelidir. Bu alandaki ilerlemeler heyecan verici olsa da gerçek bir yapay genel zekânın oluşturulabilmesi için gereken, sağlam veri odaklı bir teknolojik altyapıya ne zaman ulaşabileceğimiz şimdilik belirsiz görünüyor.



Kaynak: https://bilimgenc.tubitak.gov.tr/makale/insanligin-hayali-yapay-genel-zeka-nedir-yapay-zekadan-farklari-neler

ÖLÇME VE DEĞERLENDİRME

A) Aşağıdaki parantezlerin içine cümlelerde verilen bilgiler doğru ise "D", yanlış ise "Y" yazınız.

1. ( ) Ethernet anahtarlaması OSI referans modeli ikinci katmanında gerçekleşir.

2. ( ) Fiziksel adres olarak da isimlendirilen MAC adresi 32 bittir.

3. ( ) Anahtar cihazına bağlı uç cihazlar genellikle Trunk olarak yapılandırılır.

4. ( ) STP protokolü, ikinci katmanda döngü oluşmasını engeller.

5. ( ) Port kümeleme, ikinci katmanda döngü oluşturmadan hem yedeklilik hem bant genişliğinin artmasını sağlar.

B) Aşağıdaki cümlelerde boş bırakılan yerlere doğru sözcükleri yazınız.

1. Anahtarlamada, ... ve kesmeli anahtarlama olmak üzere iki iletim yöntemi vardır.

2. Ağ anahtarlamasında, veri gönderimi yapılırken aynı anda veri almanın mümkün olduğu haberleşme yöntemine ..... iletişim denir.

3. Birden fazla fiziksel portun tek bir sanal arayüz olarak çalışmasını sağlayan teknolojiye ..... denir.

4. Ağ anahtarının fiziksel portlarını mantıksal olarak gruplandırarak birden fazla bağımsız ağ segmenti oluşturma işlemi ..... yapılandırılarak gerçekleştirilir.

5. Router On A Stick IVR yöntemi, bir ..... arayüzün birden fazla mantıksal arayüze bölünerek VLAN'lara hizmet vermesini sağlar.

C) Aşağıdaki soruları dikkatlice okuyarak doğru cevabı işaretleyiniz.

1. VLAN etiketsiz Ethernet çerçevesinin maksimum boyut değeri aşağıdakilerden hangisidir?

A) 46 bayt B) 1518 bayt C) 1522 bayt D) 4094 bayt E) 4096 bayt

2. Genel yayın alanının tanımı ile ilgili aşağıdaki ifadelerden hangisi doğrudur?

A) Genel yayın paketinin ağ segmenti içinde bulunan tüm cihazlara ulaştığı alandır.

B) Aynı IP adresine sahip olan cihazların bulunduğu ağ segmentidir.

C) Aynı ağ anahtarı üzerinde veri çerçevelerinin saklandığı bellek alanıdır.

D) Farklı VLAN'lar arasında veri iletimini sağlayan bir ağ protokolüdür.

E) Yalnızca veri iletimi için kullanılan ve ağın fiziksel bağlantı noktalarını temsil eden alandır.

3. Ağ çarpışmasıyla (collision) ilgili aşağıdaki yargılardan hangisi doğrudur?

A) İki cihazın aynı IP adresini kullanmaya çalışması durumunda meydana gelir.

B) Birden fazla genel yayın alanının çakışması durumunda ortaya çıkar.

C) Bir ağ anahtarında yerel VLAN'ın değiştirilmesi durumunda gerçekleşir.

D) Yarım çift yönlü haberleşmede, aynı ağ ortamındaki iki veya daha fazla cihazın aynı anda veri iletmeye çalışmasıyla meydana gelir.

E) Yalnızca kablosuz ağ haberleşmesinde meydana gelen bir durumdur.

4. Aşağıdakilerden hangisi port kümeleme protokolüdür?

A) FTP B) HTTP C) LACP D) SMTP E) STP

5. STP ile ilgili aşağıdaki yargılardan hangisi doğrudur?

A) Fiziksel portların bant genişliğini artırmak için kullanılan bir protokoldür.

B) VLAN'lar arası haberleşmeyi yönetmek için kullanılan bir protokoldür.

C) İkinci katman döngülerini engellemek amacıyla kullanılan bir protokoldür.

D) Dinamik yönlendirme protokolüdür.

E) Ağ trafiğini şifrelemek için kullanılan bir protokoldür.

2. ÖĞRENME BİRİMİ

AĞ YÖNLENDİRME

KONULAR

2.1. STATİK YÖNLENDİRME
2.2. DİNAMİK YÖNLENDİRME

NELER ÖĞRENECEKSİNİZ?

- Ağlar arası statik yönlendirme yapma
- Ağlar arası dinamik yönlendirme yapma



TEMEL KAVRAMLAR

BGP, dinamik yönlendirme, EIGRP, kayan statik rota, OSPF, özet rota, RIP, statik yönlendirme, tamamen tanımlı rota, varsayılan rota

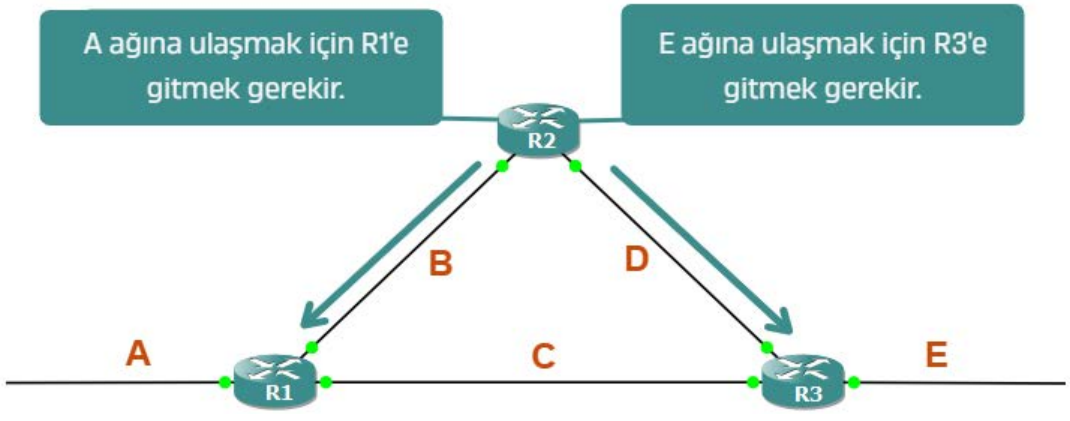
HAZIRLIK ÇALIŞMALARI

1. Yönlendirme kavramının zihninizde canlandırdıklarını sınıfta arkadaşlarınızla paylaşınız.
2. Ağ ortamlarında veri güvenliği konusunda yaşanabilecek sorunlar nelerdir? Düşüncelerinizi sınıfta arkadaşlarınızla paylaşınız.

2.1. STATİK YÖNLENDİRME

Yönlendirme, uzak mesafedeki cihazlar arasında verilerin en hızlı, en güvenli ve en kısa mesafeden iletimini sağlama işlemidir. Yönlendirme işlemi, yönlendiricinin hafızasında kaydedilen yönlendirme tabloları ile gerçekleştirir. Yönlendiriciler ağ üzerinde birçok yönlendirici ile birlikte çalışır. Bulundukları ağda gelen-giden veri paketlerini okuyarak iletimin hangi arayüzden yapılacağına karar verir.

Statik yönlendirme işleminde, ağ trafiğinde gelen verinin hangi rotadan gideceği önceden belirlenir (Görsel 2.1).



Görsel 2.1: Statik yönlendirme işleminde verinin rotası

Statik yönlendirmede yönlendirme bilgileri manuel olarak yapılandırılır. Yönlendirme tabloları ağda paylaşılmadığı için daha güvenlidir. Statik yönlendirme işleminde daha az kaynak kullanımına ihtiyaç duyulur. Bu sebeple çalışma performansı yüksektir. Çok büyük olmayan ağlar için yönetilebilir bir yöntem olmasına rağmen büyük ağlarda veya genişleyen ağ yapısında kullanımı ve yönetimi zor olabilir.

2.1.1. Komutlar ve Yapılandırma

Statik yönlendirme işlemi, yönlendirici **global yapılandırma** modundayken **ip route** komutuyla uygulanır. Komutun kullanımı şu şekildedir:

Router(config)# ip route [hedef ağ adresi] [hedef ağ maskesi] [sıçrama noktası/çıkış arayüzü] [yönetimsel uzaklık]

Hedef Ağ Adresi (Destination Network ID): Yönlendiriciye doğrudan bağlı olmayan ağın adresidir.

Hedef Ağ Maskesi (Destination Subnetmask): Yönlendiriciye doğrudan bağlı olmayan ağın ağ maskesi adresidir.

Sıçrama Noktası (Next Hop): Veri paketinin iletileceği yönlendiricinin arayüz adresidir.

Çıkış Arayüzü (Exit Interface): Veri paketini gönderecek olan yönlendiricinin çıkış yaptığı arayüzüdür.

Yönetimsel Uzaklık (Administrative Distance): Yönlendirme işleminde güvenilirliği ve tercih edilme önceliğini gösteren sayısal bir değerdir. Statik yönlendirmede yönetimsel uzaklık değeri, varsayılan olarak 1'dir. Yönlendiriciye doğrudan bağlı rotalarda ise bu değer **0**'dır.

Görsel 2.2'de Router-A ve Router-B cihazlarına yapılan statik yönlendirme komutları görülür. **ip route** komutu uygulanırken hedef ağ adresi yazıldıktan sonra bir sonraki sıçrama noktası olan yönlendirici cihazın IP adresi veya bir sonraki sıçrama için çıkış yapılacak arayüz ismi yazılır. Router-A yapılandırmasında 10.0.0.2 ile ifade edilen adres, Router-B'nin arayüz adresidir. se0/0/0 ise Router-A'nın çıkış yapılan arayüz ismidir.




```
Router-A(config)# ip route 172.16.0.0 255.255.0.0 10.0.0.2
veya
Router-A(config)# ip route 172.16.0.0 255.255.0.0 se0/0/0

Router-B(config)# ip route 192.168.1.0 255.255.255.0 10.0.0.1
veya
Router-B(config)# ip route 192.168.1.0 255.255.255.0 se0/0/1
```

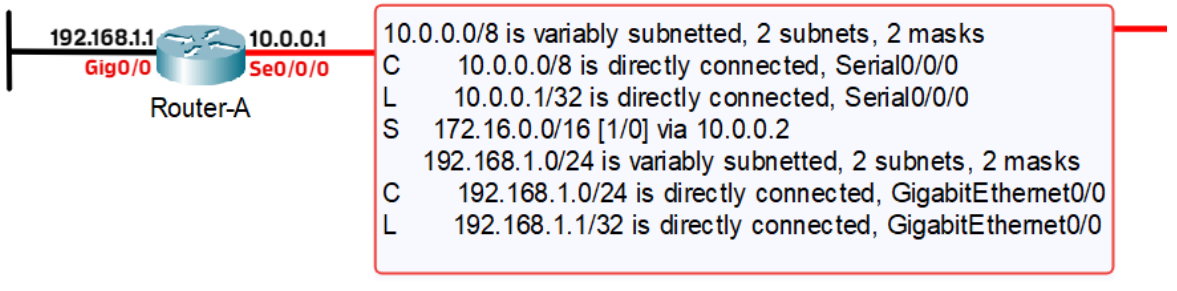
Görsel 2.2: Statik yönlendirme komutları

2.1.2. Yönlendirme Tablosu

Yönlendirme tablosunda, hedef ağ adreslerine hangi arayüz veya sıçrama noktası üzerinden gidileceği bilgisi yer alır. Yönlendirme tablosu yönlendiricinin RAM belleğinde tutulur. Yapılan yönlendirme türüne göre bu bilgiler ağ üzerinde paylaşılır ve yönlendirme rotaları oluşturulur.

Yönlendirme tablosunu görüntülemek için yönlendirici yetkili moddayken **show ip route** komutu uygulanır. Statik yönlendirme bilgisi, yönlendirme tablosunda **S** öneki ile gösterilir. Yönlendiriciye doğrudan bağlı olan yerel ağlar ise **C** öneki ile gösterilir.

Görsel 2.3'te Router-A cihazında oluşturulan yönlendirme tablosu bilgileri görülür. Yönlendiriciye doğrudan bağlı olan 10.0.0.0/8 ve 192.168.1.0/24 ağları, C öneki ile gösterilir. 172.16.0.0/16 hedef ağa ulaşmak için 10.0.0.2 sıçrama noktası üzerinden yönlendirme sağlanır. Yönlendirme, S öneki ile gösterilir. **L** öneki ile gösterilen IP adresleri ise yönlendiricinin arayüzlerine verilen yerel adreslerdir.



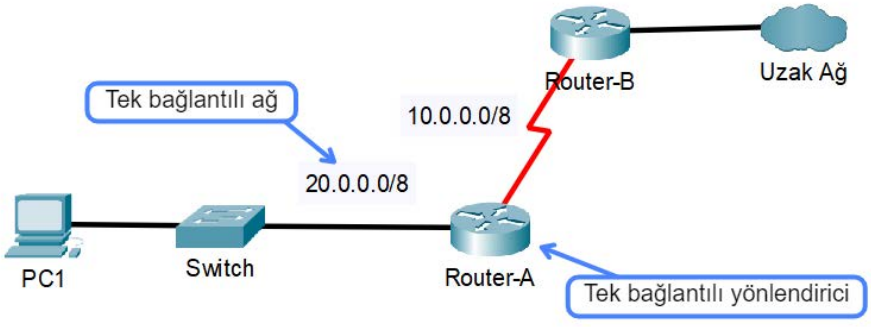
Görsel 2.3: Yönlendirme tablosu

2.1.3. Statik Yönlendirme Türleri

Statik yönlendirme türleri beş başlık altında sıralanabilir.

2.1.3.1. Standart Statik Rota

Standart statik rota, hedef adresi bilinen belirli bir ağa yapılan yönlendirme türüdür. Görsel 2.4'te Router-B cihazından 20.0.0.0/8 ağına ulaşmak için Router-A'da tanımlı olan ağa, doğrudan statik yönlendirme yapılır.



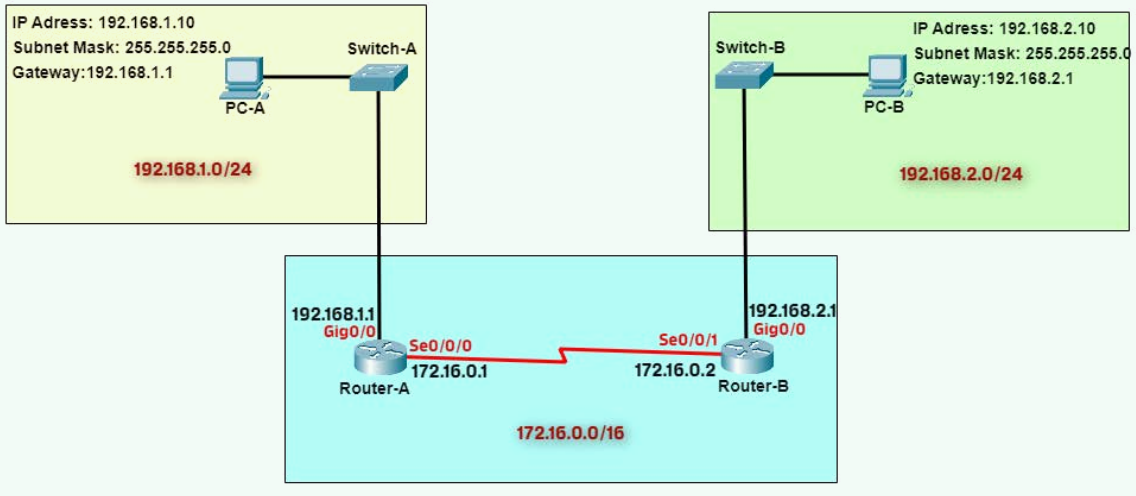
Görsel 2.4: Standart statik rota

Farklı ağları statik yönlendirme protokolü kullanarak yapılandırma işlemini verilen adımlar doğrultusunda gerçekleştiriniz.

1. UYGULAMA

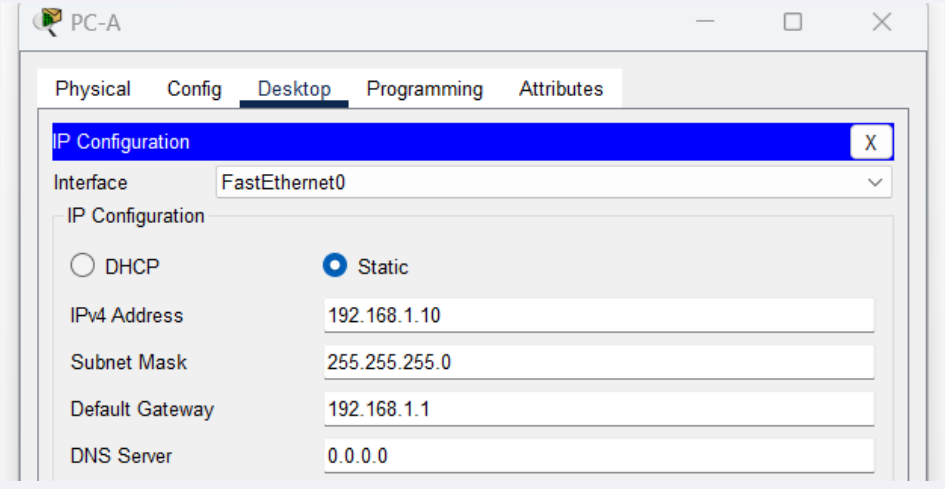
1. Adım: Ağ simülasyon programını çalıştırınız.

2. Adım: Görsel 2.5'teki ağ topolojisini oluşturunuz.



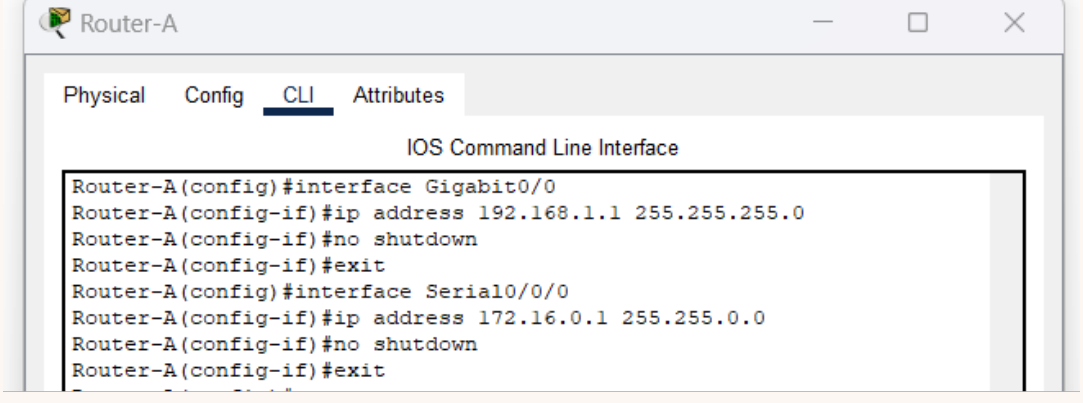
Görsel 2.5: 1. uygulamanın ağ topolojisi

3. Adım: Görsel 2.6'da PC-A cihazının IP yapılandırması görülür. Siz de PC-B cihazının IP yapılandırmasını tamamlayınız.



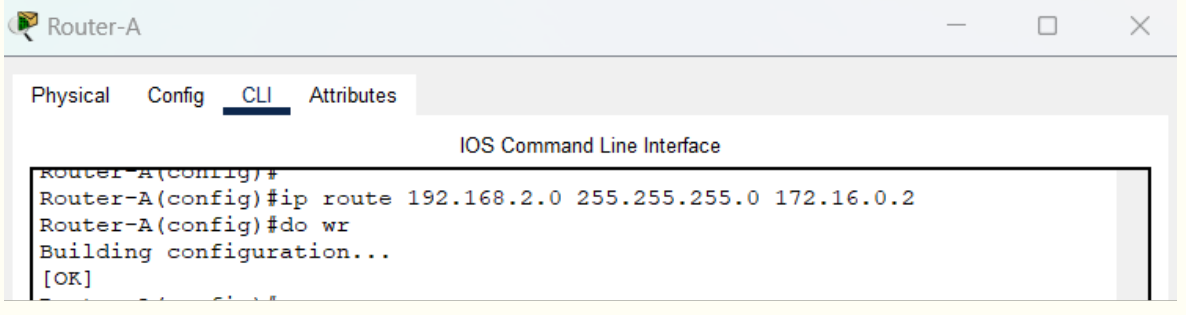
Görsel 2.6: PC-A yapılandırma bilgisi

4. Adım: Görsel 2.7'de Router-A cihazının IP yapılandırması görülür. Siz de Router-B cihazının IP yapılandırmasını tamamlayınız.



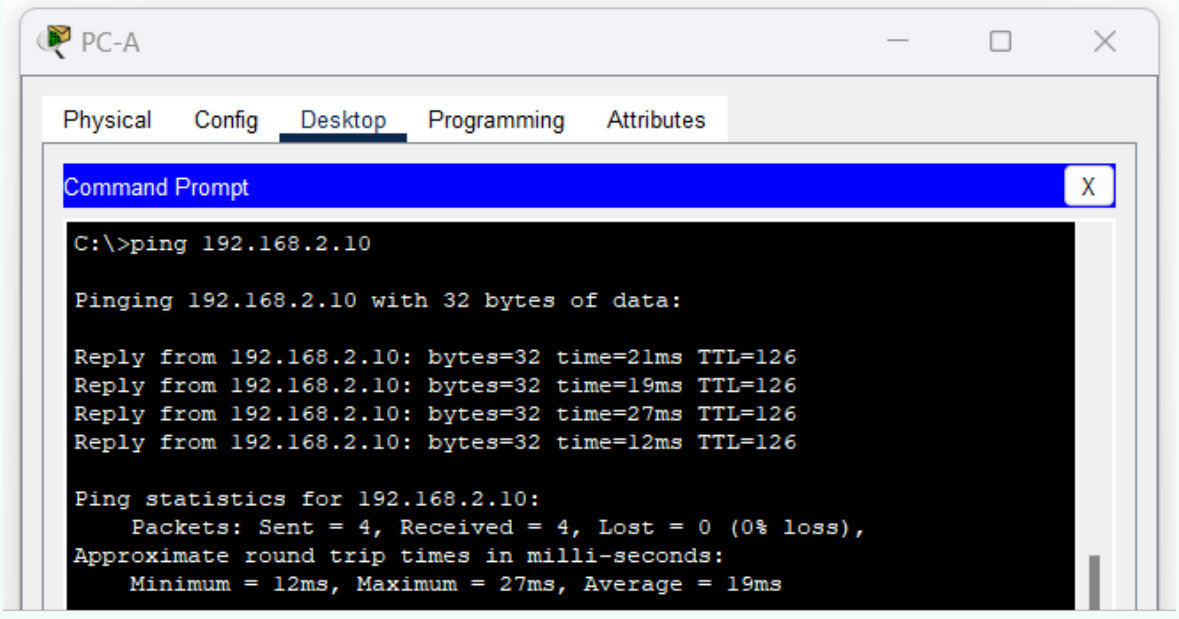
Görsel 2.7: Router-A cihazının IP yapılandırması

5. Adım: Görsel 2.8'de Router-A cihazının statik yönlendirme yapıladırması görülür. Siz de Router-B cihazının statik yönlendirme yapılandırmasını tamamlayınız.



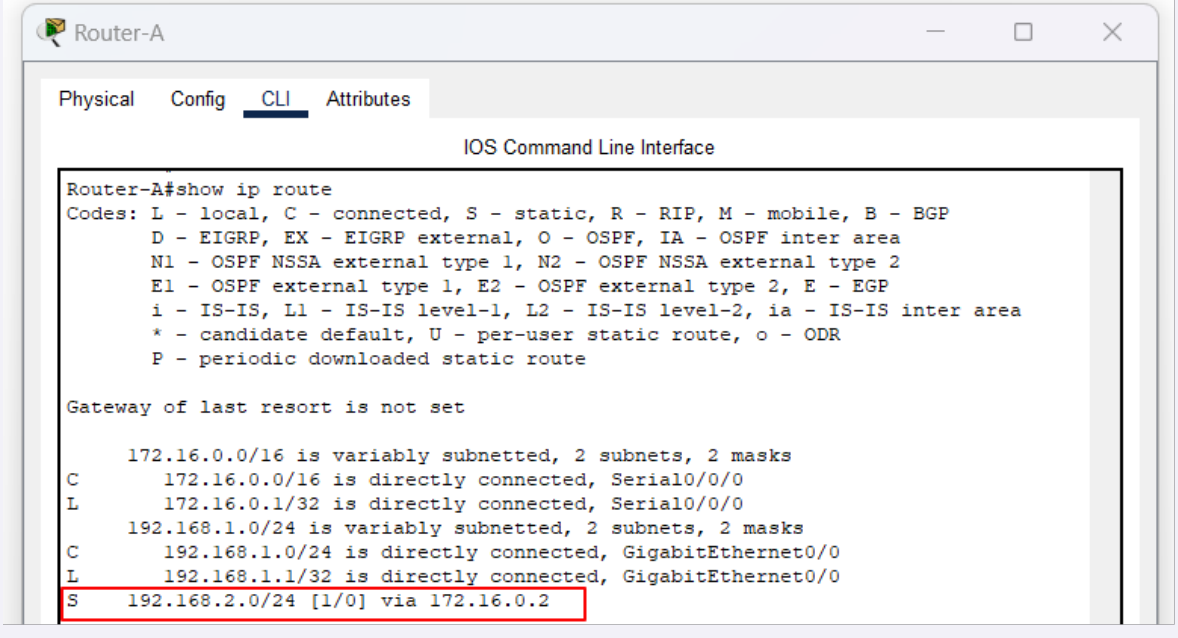
Görsel 2.8: Router-A cihazının statik yönlendirme yapılandırması

6. Adım: PC-A cihazına giriş yapıp Desktop/Command Prompt seçenekleri ile komut arayüzüne erişim sağlayınız ve bilgisayarlar arasındaki iletişimi **ping** komutuyla test ediniz (Görsel 2.9).



Görsel 2.9: ping komutu ile iletişimi test etme

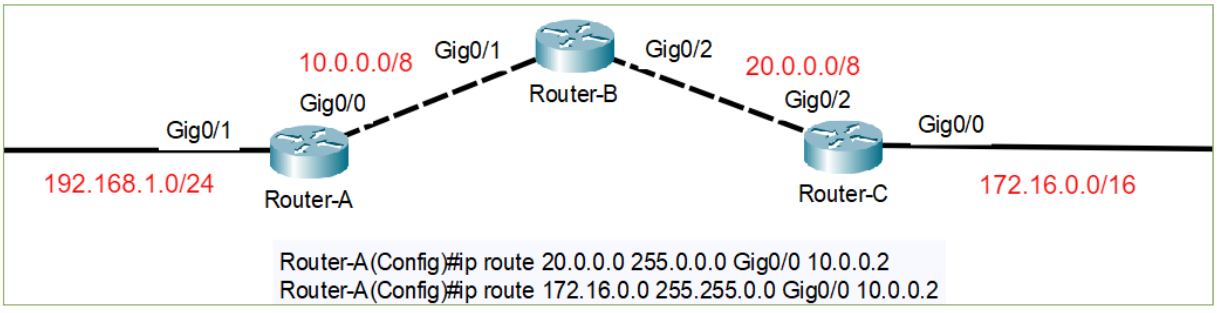
7. Adım: Router-A cihazında kaydedilen yönlendirme tablolarını görüntüleyiniz (Görsel 2.10).



Görsel 2.10: Router-A cihazında kaydedilen yönlendirme tablosunu görüntüleme

2.1.3.2. Tamamen Tanımlı Statik Rota

Statik rota tanımlaması yapılırken hem çıkış arayüzü hem de sonraki sıçrama noktası belirtilerek yapılan yönlendirme türüdür. Çıkış arayüzünün çoklu erişim arayüzü olduğu durumlarda kullanılır. Sonraki sıçrama noktası ile çıkış arayüzü doğrudan birbirine bağlı olmalıdır. Görsel 2.11'de Router-A cihazında yapılandırılan tamamen tanımlı statik rota bilgisi görülür. Hedef ağlara ulaşmak için Gig0/0 çıkış arayüzü ve 10.0.0.2 sonraki sıçrama noktası bilgisi kullanılır.



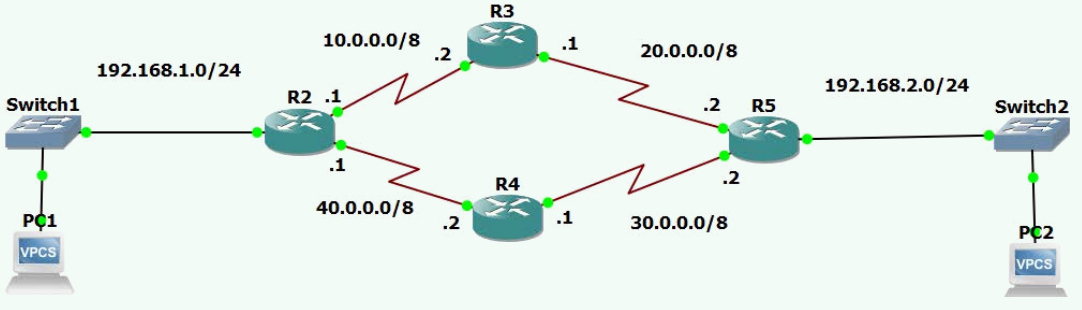
Görsel 2.11: Tamamen tanımlı statik rota

Birbirine uzak farklı ağları tamamen tanımlı statik rota yapılandırması ile yönlendirme işlemini verilen adımlar doğrultusunda gerçekleştiriniz.

2. UYGULAMA

1. Adım: Ağ simülasyon programını çalıştırınız.

2. Adım: Görsel 2.12'deki ağ topolojisini oluşturunuz.



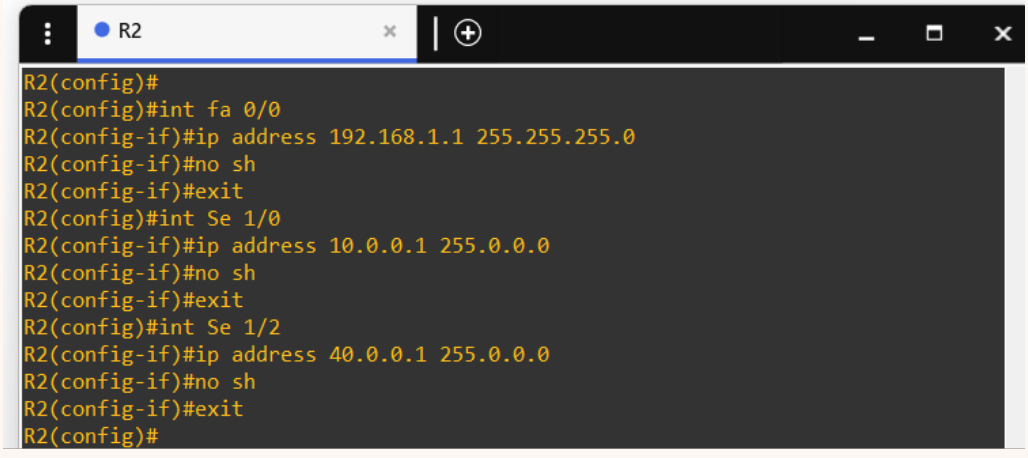
Görsel 2.12: 2. uygulamanın ağ topolojisi

3. Adım: Görsel 2.13'te PC1 cihazının IP yapılandırması görülür. Siz de PC2 cihazının IP yapılandırmasını tamamlayınız.



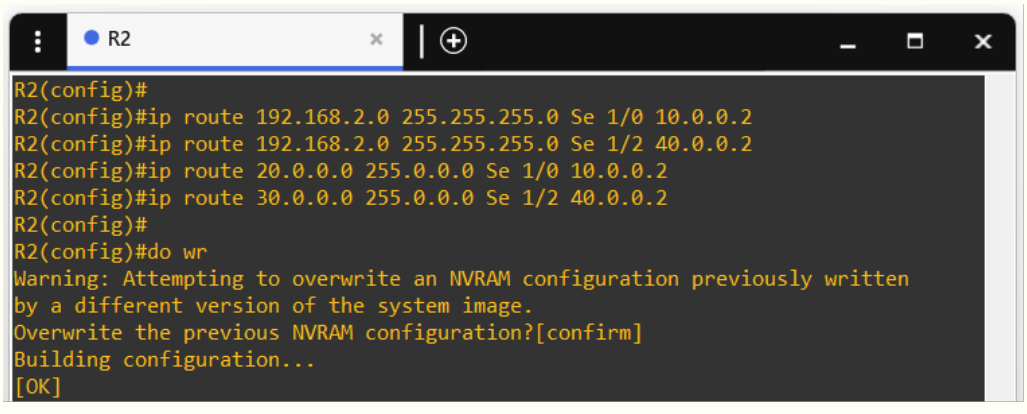
Görsel 2.13: Bilgisayar IP yapılandırması

4. Adım: Görsel 2.14'te R2 cihazının arayüzlerinde yapılandırılan IP bilgileri görülür. Siz de diğer yönlendirici cihazların IP yapılandırmalarını tamamlayınız.



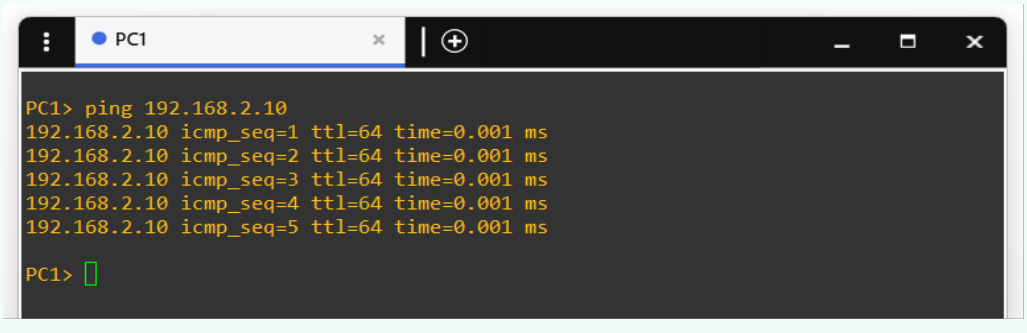
Görsel 2.14: Yönlendirici IP yapılandırması

5. Adım: R2 cihazını tamamen tanımlı statik yönlendirme protokolüyle yapılandırıp (Görsel 2.15) tüm değişiklikleri kaydediniz ve aynı işlemleri diğer yönlendirici cihazlar için de gerçekleştiriniz.



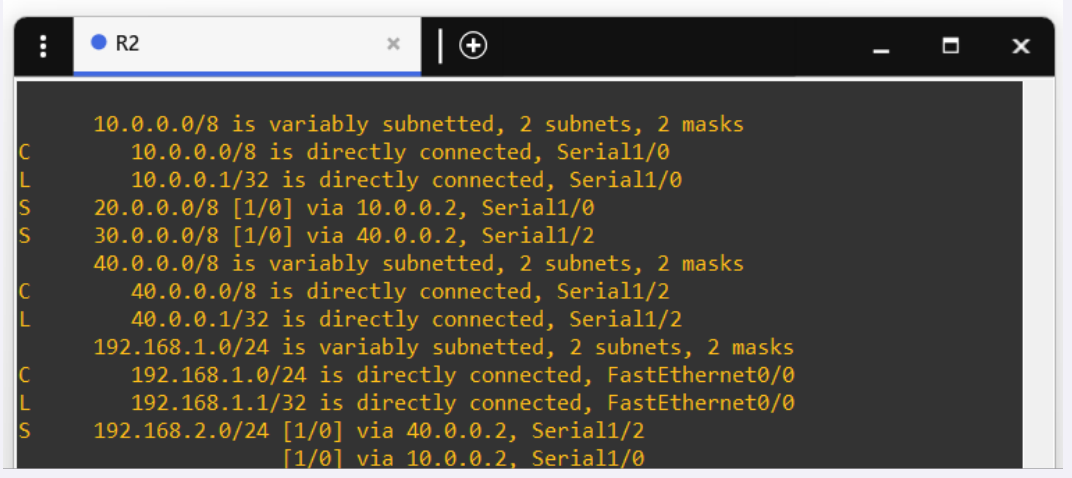
Görsel 2.15: Tamamen tanımlı statik yönlendirme işlemi

6. Adım: PC1 cihazının komut arayüzüne erişim sağlayıp PC2 cihazına erişimi, **ping** komutu ile test ediniz (Görsel 2.16).



Görsel 2.16: ping komutu ile erişimi test etme

7. Adım: R2 cihazındaki yönlendirme tablosunu görüntüleyiniz (Görsel 2.17).



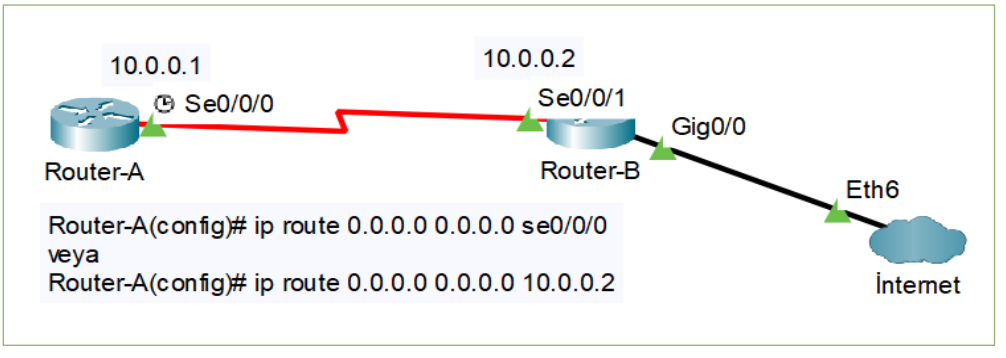
Görsel 2.17: R2 cihazındaki yönlendirme tablosunun görüntülenmesi

2.1.3.3. Varsayılan Statik Rota

Varsayılan statik rota, yönlendirme tablosunda tanımlı olmayan ağ adresleri için yapılan yönlendirme türüdür. Statik yönlendirmenin tamamını kontrol etmek mümkün olmayabilir. Tanımlı olmayan ağ adresleri için yedek bir yol gösterilir. Varsayılan rota için hedef ağ adresi ve hedef ağ maskesi bilgisi, **0.0.0.0** olarak tanımlanır. Bu, tanımlı olmayan herhangi bir adres anlamına gelir. Yönlendirme tablosunda S* öneki ile gösterilir. Varsayılan rota şu şekilde oluşturulur:

Router(config)# ip route [0.0.0.0] [0.0.0.0] [sıçrama noktası/çıkış arayüzü] [yönetimsel uzaklık]

Görsel 2.18'de Router-A cihazında oluşturulan varsayılan rota komutu görülür. Bu topolojide Router-A cihazının yönlendirme tablosunda yer almayan ağ adresi ile karşılaşılan durumda veriler, Router-A'nın **se0/0/0** portuna veya Router-B'nin **10.0.0.2** arayüzüne yönlendirilir.



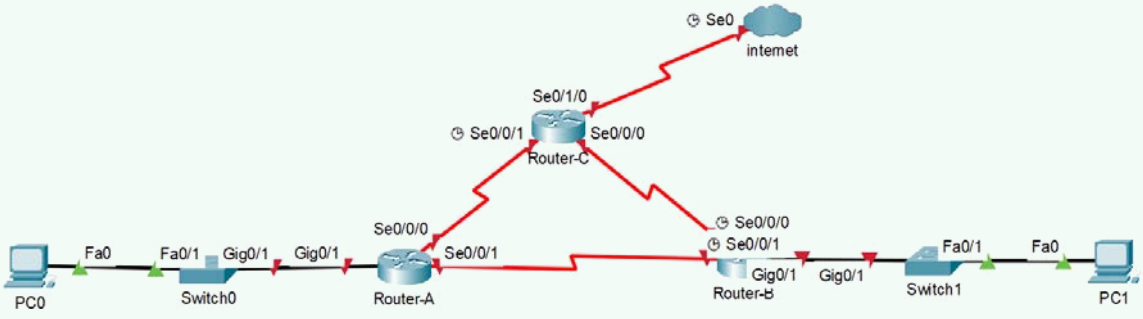
Görsel 2.18: Varsayılan rota ile yönlendirme

Statik yönlendirme işlemini varsayılan rota ile birlikte oluşturma işlemini verilen adımlar doğrultusunda gerçekleştiriniz.

3. UYGULAMA

1. Adım: Ağ simülasyon programını çalıştırınız.

2. Adım: Görsel 2.19'daki ağ topolojisini oluşturunuz.



Görsel 2.19: 3. uygulamanın ağ topolojisi

3. Adım: Bilgisayarların ve yönlendiricilerin IP adreslerini Tablo 2.1'e göre yapılandırınız.

Tablo 2.1: Bilgisayarların IP Yapılandırma Bilgileri

CİHAZ	IP ADRES	AĞ MASKESİ	DEFAULT GATEWAY
PC0	192.168.1.10	255.255.255.0	192.168.1.1
PC1	192.168.2.20	255.255.255.0	192.168.2.1

4. Adım: Router-A yönlendiricisinin komut arayüzü üzerinden IP yapılandırması Görsel 2.20'de görülür.

IOS Command Line Interface

```
Router-A(config)#interface gigabitethernet 0/1
Router-A(config-if)#ip address 192.168.1.1 255.255.255.0
Router-A(config-if)#no shutdown
Router-A(config-if)#exit
Router-A(config)#interface serial 0/0/0
Router-A(config-if)#ip address 10.0.0.1 255.0.0.0
Router-A(config-if)#no shutdown
Router-A(config-if)#exit
Router-A(config)#interface se0/0/1
Router-A(config-if)#ip address 20.0.0.1 255.0.0.0
Router-A(config-if)#no shutdown
Router-A(config-if)#exit
```

Görsel 2.20: Router-A cihazının IP yapılandırması

Tablo 2.2'ye göre yönlendiricilerin yapılandırma işlemlerini tamamlayınız.

Tablo 2.2: Yönlendiricilerin IP Yapılandırma Bilgileri

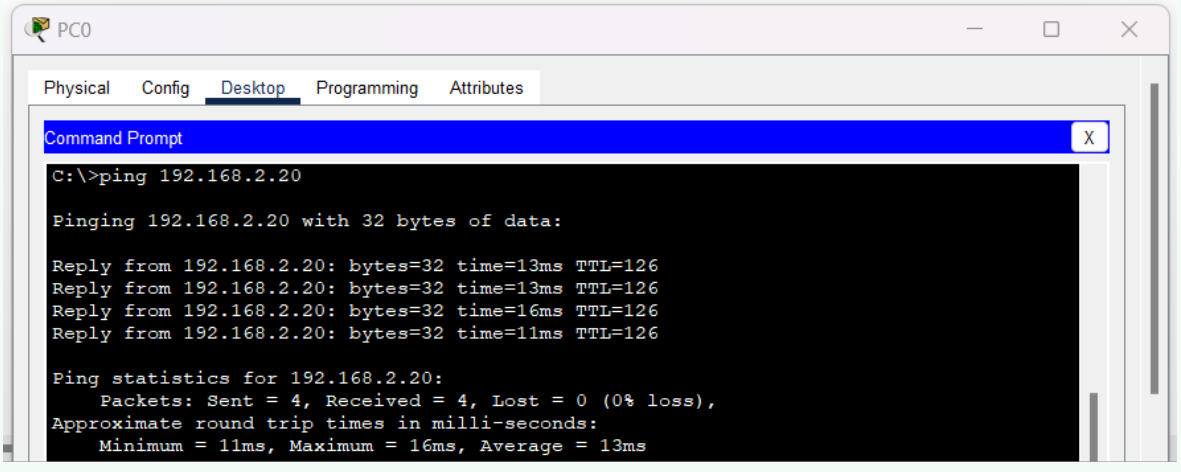
	ARAYÜZLER			
CİHAZ	Serial0/0/0	Serial0/0/1	Serial0/1/0	Gig0/1
Router-A	10.0.0.1/8	20.0.0.1/8	----	192.168.1.1/24
Router-B	30.0.0.2/8	20.0.0.2/8		192.168.2.1/24
Router-C	30.0.0.1/8	10.0.0.2/8	50.0.0.50/8	----

5. Adım: Yönlendirici cihazların statik yönlendirme ve varsayılan rota oluşturma işlemlerini her bir yönlendirici için ayrı ayrı uygulayınız (Görsel 2.21).

```
Router-A(config)#ip route 30.0.0.0 255.0.0.0 se0/0/0
%Default route without gateway, if not a point-to-point interface, may impact performance
Router-A(config)#ip route 30.0.0.0 255.0.0.0 se0/0/1
%Default route without gateway, if not a point-to-point interface, may impact performance
Router-A(config)#ip route 0.0.0.0 0.0.0.0 se0/0/0
%Default route without gateway, if not a point-to-point interface, may impact performance
```

Görsel 2.21: Varsayılan rota ve statik rota ile yönlendirme işlemi

6. Adım: Bilgisayarlar arasındaki ağ iletişimini **ping** komutu ile test ediniz (Görsel 2.22).



Görsel 2.22: Bilgisayarlar arasındaki iletişimin test edilmesi

7. Adım: Yönlendirme tablolarını görüntüleyiniz (Router-A cihazının yönlendirme tablosu Görsel 2.23'te görülür.).

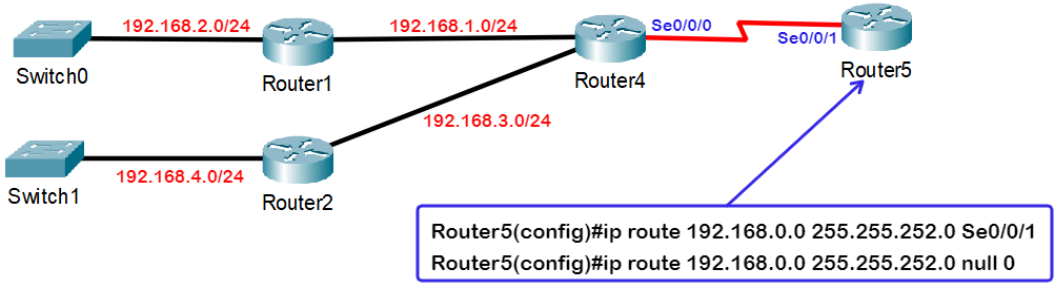
```
C       10.0.0.0/8 is directly connected, Serial0/0/0
L       10.0.0.1/32 is directly connected, Serial0/0/0
     20.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       20.0.0.0/8 is directly connected, Serial0/0/1
L       20.0.0.1/32 is directly connected, Serial0/0/1
S    30.0.0.0/8 is directly connected, Serial0/0/0
                is directly connected, Serial0/0/1
     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, GigabitEthernet0/1
L       192.168.1.1/32 is directly connected, GigabitEthernet0/1
S*   0.0.0.0/0 is directly connected, Serial0/0/0
```

Görsel 2.23: Yönlendirme tablosu bilgileri

2.1.3.4. Özet Statik Rota

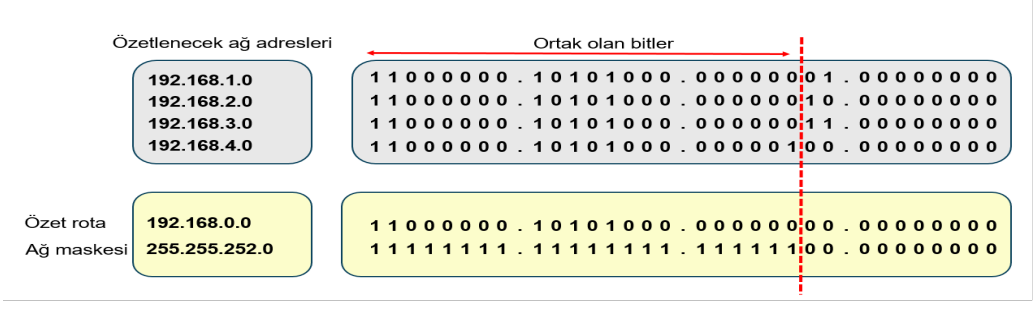
Özet statik rota, tanımlı olan birden çok statik rotanın özetlenerek tek bir rota tanımlanmasıyla yapılan yönlendirme işlemidir. Yönlendirme tablolarını sadeleştirmek ve trafik yükünü hafifletmek için kullanılır. Özet statik rotalar, aynı zamanda ağın genişletilmesi ve yönetimi için kullanım kolaylığı sağlar. Görsel 2.24'te dört farklı ağ adresinin özetlenerek tek bir ağ adresi ile yönlendirilmesi görülür. Özet statik rotada, özetlenecek ağ adreslerini kapsayacak ortak bir ağ adresi hesaplanır ve yeni bir ağ maskesi oluşturulur.

Yönlendirme döngüleri özet rota kullanımında dikkat edilmesi gereken konudur. Özet ağlar, birden fazla alt ağı kapsadığından özetlenmeyen ve yönlendirme tablosunda bulunmayan ağ adresleri, yönlendirme döngüleri oluşturabilir. Bu durum, veri paketlerinin TTL (Time To Live) değeri 0'a ulaşana kadar devam eder ve ağ verimliliğini düşürebilir. Özetlenen ağların dışında kalan paketlerin düşürülmesi amacıyla null 0 yönlendirmesi, yönlendirme döngülerini önlemek için yapılır. Null 0 yönlendirmesi, özetlenen ağ adreslerine giden geçersiz trafiğin yönlendirilmemesini sağlar. Böylece gereksiz yönlendirme döngüleri engellenir ve ağın genel verimliliği artırılır.



Görsel 2.24: Özet statik rota

Görsel 2.25'te özet rota hesaplama işlemi görülür. Özetlenecek ağ adresleri ikili sayı formatına dönüştürülür ve ortak olan bitler gruplanır. Ortak bitler özet rota için kullanılacak olan ağ adresidir. Ortak olan bitlerin tamamı **1**, farklı olan bitlerin tamamı **0** olarak hesaplanarak yeni ağ maskesi oluşturulur.



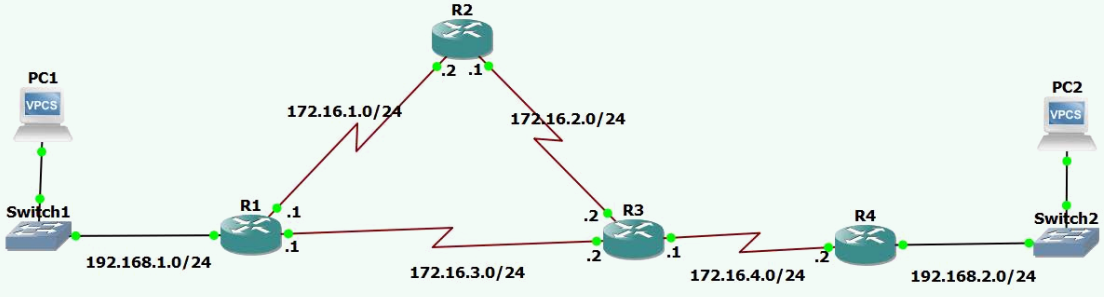
Görsel 2.25: Özet rota hesaplama

4. UYGULAMA

Özet statik rota ile yönlendirme yapma işlemini verilen adımlar doğrultusunda gerçekleştiriniz.

1. Adım: Ağ simülasyon programını çalıştırınız.

2. Adım: Görsel 2.26'daki ağ topolojisini oluşturunuz.



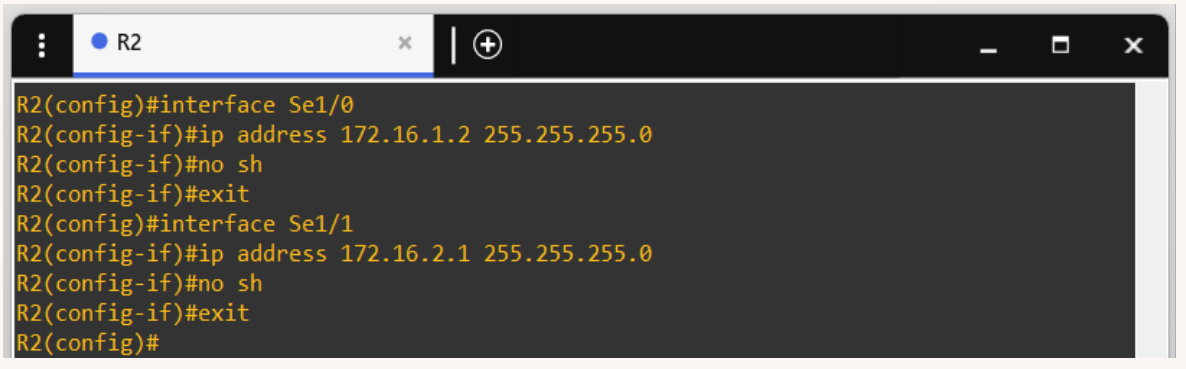
Görsel 2.26: 4. uygulamanın ağ topolojisi

3. Adım: PC1 cihazının IP yapılandırmasını Görsel 2.27'deki şekilde yapınız (PC2 cihazının da IP yapılandırmasını yapınız.).



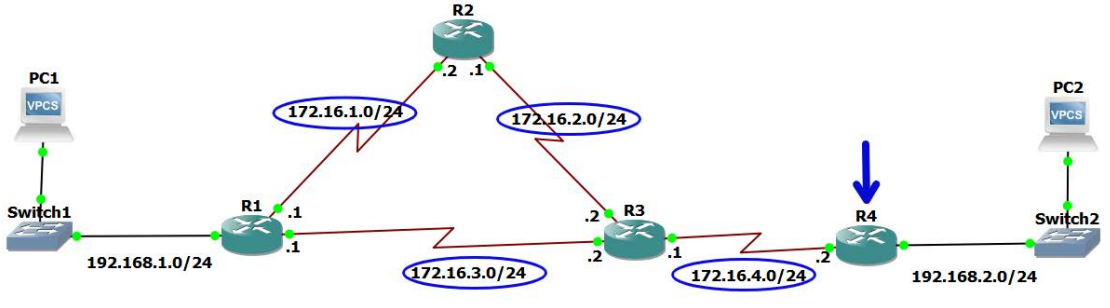
Görsel 2.27: PC1 IP yapılandırması

4. Adım: R2 cihazının IP yapılandırması, Görsel 2.28'de görüldüğü gibidir. Buna göre diğer yönlendirici cihazları da uygun IP adreslerini kullanarak yapılandırınız.



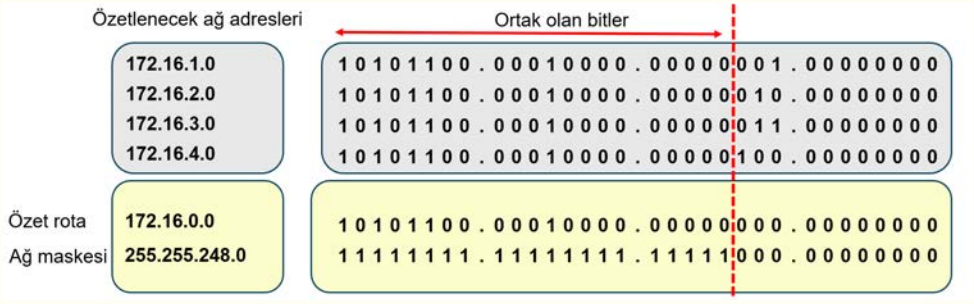
Görsel 2.28: R2 IP yapılandırması

NOT: Görsel 2.29'da özetlenecek ağ adresleri ve özet statik yönlendirmenin tanımlanacağı cihaz görülür.



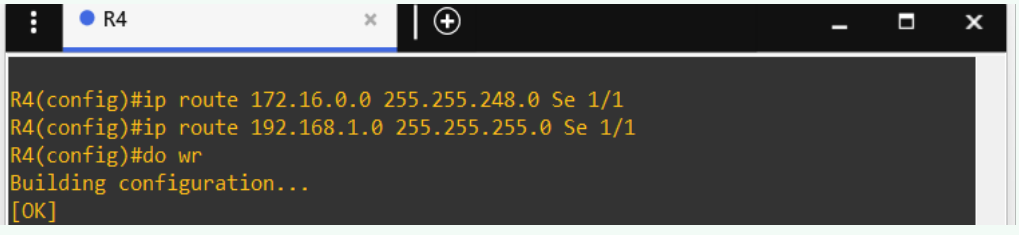
Görsel 2.29: Özet statik rotanın uygulanacağı cihazın belirlenmesi

5. Adım: Ortak ağ adresini ve ağ maskesini hesaplamak için ağ adreslerini ikili sayı sisteminde göstererek hesaplayınız (Görsel 2.30).



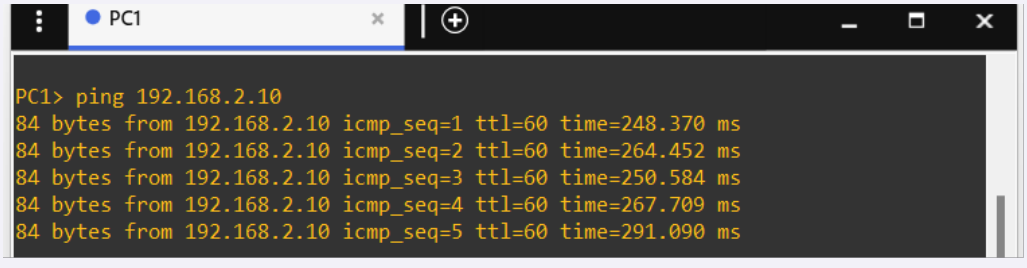
Görsel 2.30: Özet rotanın hesaplanması

6. Adım: Özet rota bilgisi ile R4 cihazında statik yönlendirme işlemini Görsel 2.31'deki gibi gerçekleştiriniz (Diğer yönlendirici cihazlar için de yönlendirme işlemlerini gerçekleştiriniz.).



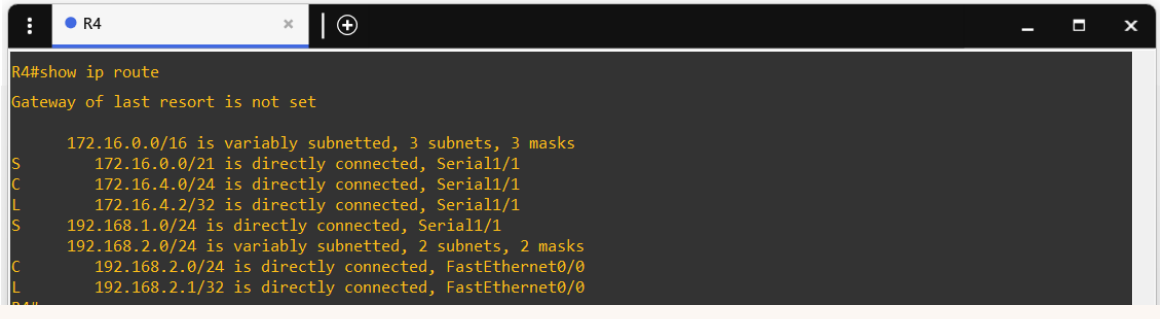
Görsel 2.31: Özet rotanın tanımlanması

7. Adım: PC1 ve PC2 cihazları arasındaki iletişimi, **ping** komutu ile test ediniz (Görsel 2.32).



Görsel 2.32: ping komutu ile iletişimin test edilmesi

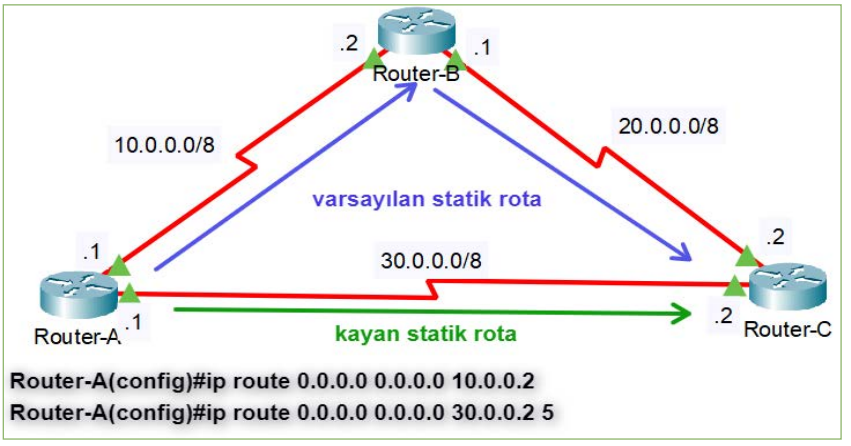
8. Adım: R4 cihazındaki yönlendirme tablosunu görüntüleyiniz (Görsel 2.33).



Görsel 2.33: Yönlendirme tablosunun görüntülenmesi

2.1.3.5. Kayan Statik Rota

Kayan statik rota, ağ üzerinde gerçekleşebilecek olası hata durumunda ana statik veya dinamik rotaya yedek bir yolun tanımlanması ile yapılan yönlendirme türüdür. Bu rota sadece ana rota kullanılamadığı durumlarda kullanır. Kayan statik rotanın yönetimsel mesafe değeri, ana rotadan daha yüksek olmalıdır. Görsel 2.34'te Router-A cihazında yapılandırılan varsayılan statik rota ve kayan statik rota bilgileri görülür. Statik yapılandırmada yönetimsel mesafe değeri 1'dir. Kayan statik rotada ise yönetimsel mesafe değeri 5 olarak verildiği görülür. Router-B cihazında herhangi bir aksaklık oluşursa kayan statik rota devreye girerek veri iletiminin devamlılığı sağlanır. Ağ iletişiminin sürekliliğini sağlamak için birden fazla kayan statik rota tanımlanabilir. Bu öncelik, yönetimsel mesafe değerlerine göre belirlenir. Ağ üzerinde oluşan aksaklık düzeldiğinde ise yeniden ana rota devreye girerek ağ iletişimi devam eder.



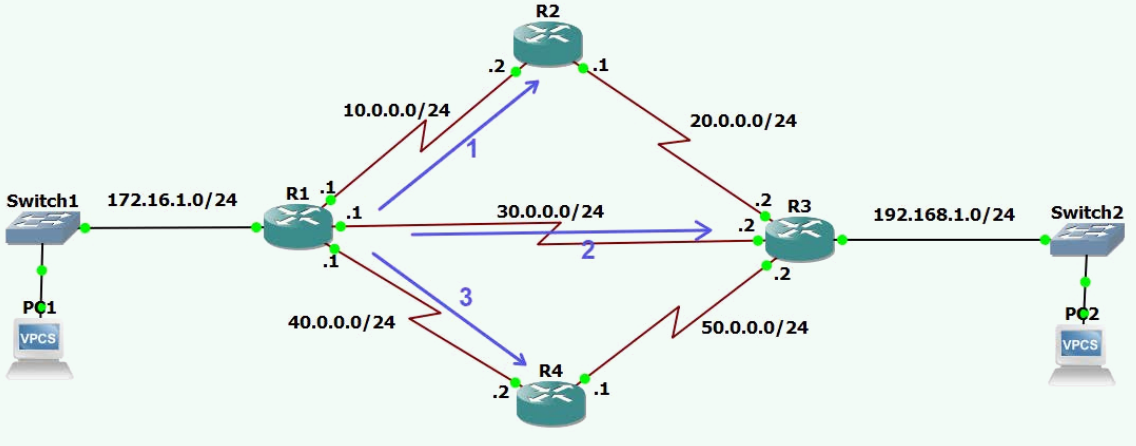
Görsel 2.34: Kayan statik rota

Kayan statik rota ile ağ yönlendirme işlemini verilen adımlar doğrultusunda gerçekleştiriniz.

5. UYGULAMA

1. Adım: Ağ simülasyon programını çalıştırınız.

2. Adım: Görsel 2.35'teki ağ topolojisini hazırlayınız (1 numaralı yolu ana rota, 2 ve 3 numaralı yolları ise kayan statik rota olarak tasarlayınız.).



Görsel 2.35: 5. uygulamanın ağ topolojisi

3. Adım: PC1 cihazının IP yapılandırmasını Görsel 2.36'daki gibi yapınız (PC2 cihazının da IP yapılandırmasını yapınız.).

```
PC1> ip 172.16.1.10 255.255.255.0 172.16.1.1
Checking for duplicate address...
PC1 : 172.16.1.10 255.255.255.0 gateway 172.16.1.1
```

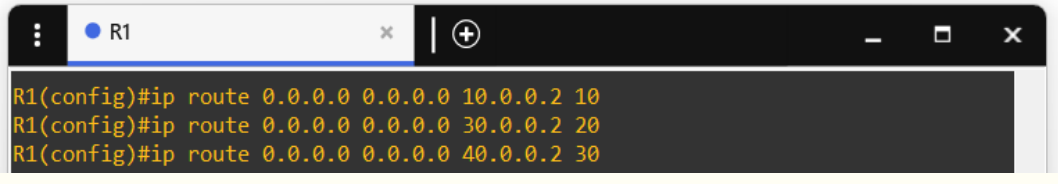
Görsel 2.36: PC1'in IP yapılandırması

4. Adım: R1 cihazının IP yapılandırmasını Görsel 2.37'deki gibi yapınız (Diğer yönlendirici cihazların da IP yapılandırmasını yapınız.).

```
R1(config)#int fa 0/0
R1(config-if)#ip address 172.16.1.1 255.255.255.0
R1(config-if)#no sh
R1(config-if)#exit
R1(config)#int se 1/0
R1(config-if)#ip address 10.0.0.1 255.255.255.0
R1(config-if)#no sh
R1(config-if)#exit
R1(config)#int se 2/2
R1(config-if)#ip address 30.0.0.1 255.255.255.0
R1(config-if)#no sh
R1(config-if)#exit
R1(config)#int se 2/0
R1(config-if)#ip address 40.0.0.1 255.255.255.0
R1(config-if)#no sh
R1(config-if)#exit
```

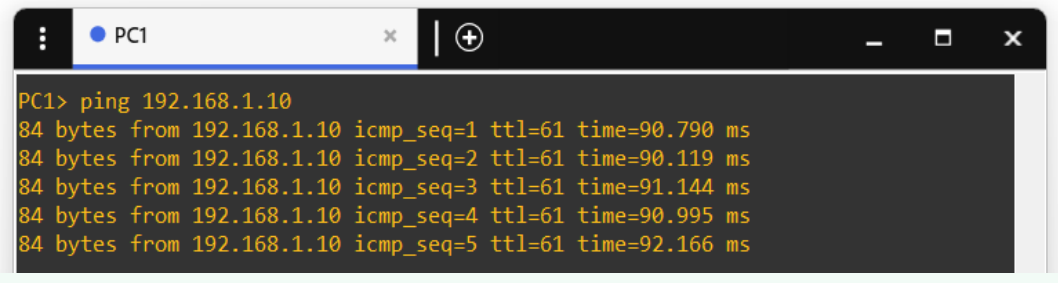
Görsel 2.37: R1'in IP yapılandırması

5. Adım: R1 cihazının varsayılan statik ve kayan statik yönlendirme işlemini Görsel 2.38'deki gibi yapınız (Diğer yönlendirici cihazların da yönlendirme işlemlerini yapınız.).



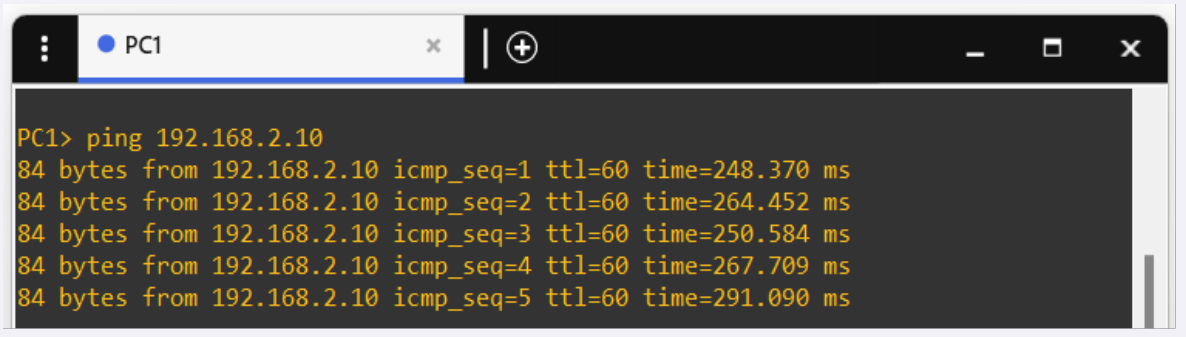
Görsel 2.38: Varsayılan ve kayan statik yönlendirme işlemi

6. Adım: PC1 ve PC2 cihazlarının iletişimini **ping** komutu ile test ediniz (Görsel 2.39).



Görsel 2.39: PC1 ve PC2 bilgisayarları arasındaki iletişimin test edilmesi

7. Adım: PC1 ve PC2 cihazları arasındaki iletişimi, **ping** komutu ile test ediniz (Görsel 2.40).

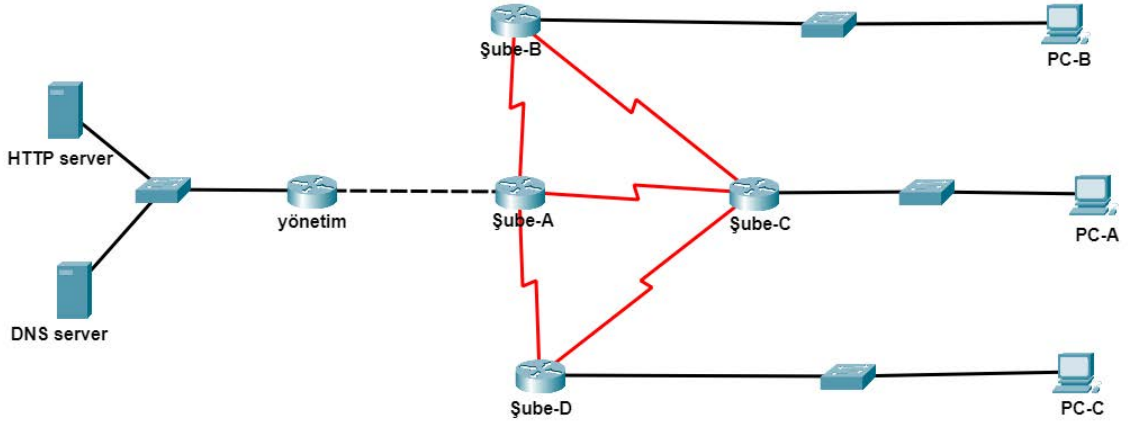


Görsel 2.40: ping komutu ile iletişimin test edilmesi

NOT: OSPF protokolü yüksek bant genişliğine sahip rotaları tercih etse de eğer bir statik yönlendirme, düşük bant genişliğine sahip rota tanımlıyorsa yönlendirici bu statik rotayı seçer. Bunun nedeni ise statik yönlendirmenin AD değerinin OSPF'nin AD değerinden daha düşük olmasıdır. Bu durumda yönlendirici, daha düşük AD değerine sahip statik rotayı tercih ederek veri iletimini bu yol üzerinden gerçekleştirir.

SIRA SİZDE

Küçük bir ofis ortamında planlanan ağ topolojisi Görsel 2.41'deki gibidir. Tüm ağı statik yönlendirme ile yapılandırınız. Ayrıca ağda varsayılan statik rota ve kayan statik rota oluşturunuz. Bilgisayarların web sunucuya erişimini sağlayınız ve birbirleriyle iletişimini test ediniz.



Görsel 2.41: Sıra sizde etkinliğinin ağ topolojisi

DEĞERLENDİRME

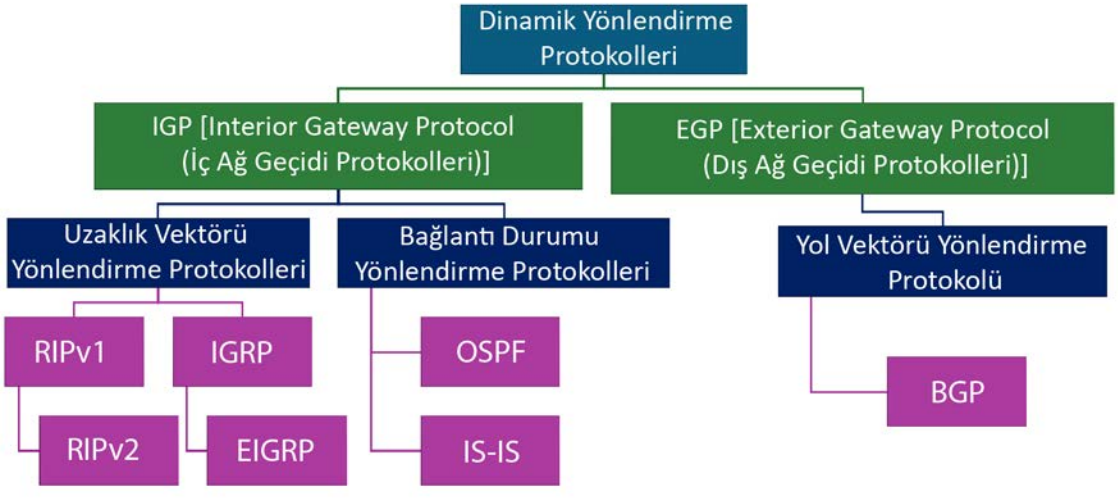
Çalışmanız aşağıda yer alan kontrol listesi kullanılarak değerlendirilecektir. Çalışmanızı yaparken değerlendirme ölçütlerini dikkate alınız.

KONTROL LİSTESİ

ÖLÇÜTLER	EVET	HAYIR
1. Ağ simülasyon programıyla ağ topolojisini tasarladı.		
2. Tüm ağı statik yönlendirmeyle yapılandırdı.		
3. Varsayılan statik rotayı oluşturdu.		
4. Kayan statik rotayı oluşturdu.		
5. Bilgisayarların web sunucuya erişimini sağladı.		
6. Bilgisayarların birbirleriyle iletişimini test etti.		

2.2. DİNAMİK YÖNLENDİRME

Dinamik yönlendirme, statik yönlendirmenin yetersiz kaldığı büyük ve bağımsız ağların iletişiminde kullanılan yöntemdir. Dinamik yönlendirmede cihazlar, yönlendirme tablolarını belirli aralıklarla ağdaki diğer cihazlarla paylaşır. Her cihaz, aldığı yeni yönlendirme tablo bilgilerini kendi yönlendirme tablosuna ekler. Bu bilgiler yönlendirme işlemi için en hızlı ve en güvenilir rotanın bulunmasında kullanılır. Genişleyen ağ yapısında bir cihazın eklenmesi ya da çıkarılması durumunda değişiklikler, otomatik olarak işlemeye devam eder. Doğru yapılandırma sağlandığında işleyişi statik yapılandırmaya göre daha kolaydır fakat yönlendirme tablolarının paylaşılması güvenlik açığına sebep olabilir. Bunun için ek güvenlik yapılandırma ayarları yapılması gereklidir. Dinamik yönlendirmede kullanılan protokollerin sınıflandırılması Görsel 2.42'de görülür.



Görsel 2.42: Dinamik yönlendirme protokolleri

1. **İç Ağ Geçidi Protokolleri:** Otonom bir iç ağ yapısındaki cihazların kullandığı dinamik protokolleri içerir.

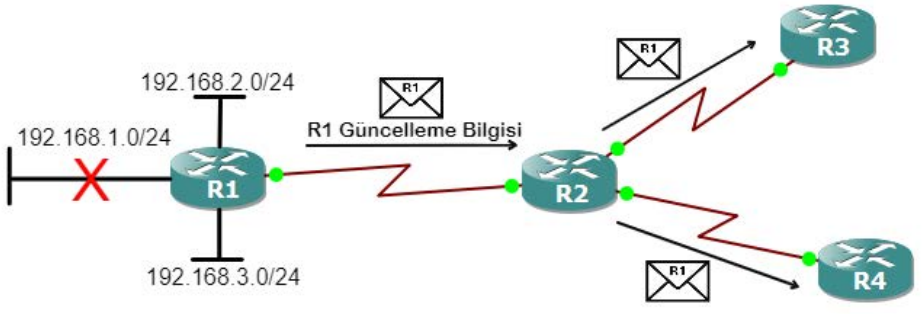
   Uzaklık Vektörü Yönlendirme: Yönlendiriciler arasındaki mesafeye göre yapılan yönlendirme işlemidir. Bu mesafede uzaklık; hedef ağa giderken yapılan sıçrama sayısı, maliyet, bant genişliği, gecikme gibi değerlere göre hesaplanır. Hedef ağa ulaşmak için sonraki yönlendiricinin yönü veya çıkış arayüzü de vektör bilgisidir. Görsel 2.43'te R1 yönlendiricisinin 172.16.1.0/24 ağına giderken bir sıçrama yapacağı ve çıkış yönünün Se0/0/0 arayüzü olduğu görülür.



Görsel 2.43: Uzaklık vektörü ile yönlendirme

Uzaklık vektörü ile yönlendirmede, hedef ağın tam yol bilgisi bilinmez. Sadece hedef ağa ulaşmak için gerekli toplam uzaklık veya metrik bilgisi kullanılır.

Bağlantı Durumu Yönlendirme: Yönlendiricilerin bağlantı durumu bilgilerini paylaşarak bir ağın tamamı hakkında bilgi sahibi olduğu yönlendirme işlemidir. Bağlantı durumunu paylaşan yönlendiriciler, ağ topoloji haritasını oluşturur. Kaynaktan hedefe giderken ağdaki en hızlı rotanın belirlenmesini sağlar. Görsel 2.44'te R1 cihazının güncel bağlantı durumu paylaşımı görülür. R1 yönlendiricisine doğrudan bağlı ağlardan 192.168.1.0/24'ün bağlantıda olmadığı, diğer ağların ise bağlantıda olduğu güncelleme bilgisi ağdaki diğer yönlendiricilerle paylaşılır. Bağlantı durumunda değişiklik olan her yönlendirici, bu paylaşımı yapar ve böylelikle topoloji haritasının güncel kalması sağlanır.

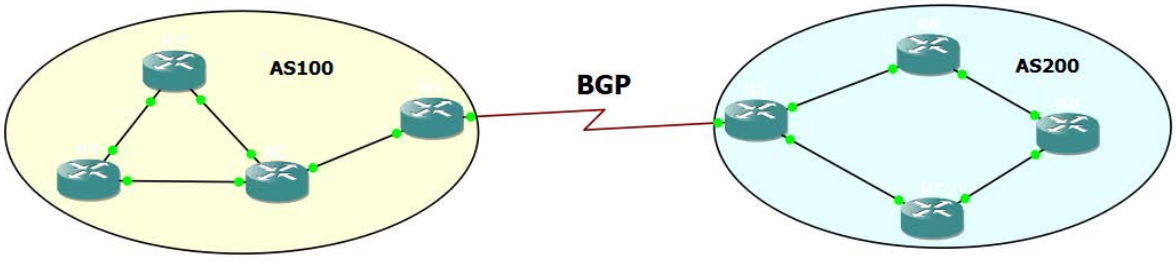


Görsel 2.44: Güncelleme bilgisi paylaşımı

2. **Dış Ağ Geçidi Protokolleri:** Birbirinden bağımsız otonom ağ yapılarının kullandığı dinamik protokolleri içerir. Birbirinden farklı otonom sistemlerde sınır ağ geçidi olarak adlandırılan yönlendiriciler, bu protokoller aracılığıyla farklı ağlar arasında veri iletişimini sağlar.

   Yol Vektörü Yönlendirme: Farklı otonom sistemler arasında yönlendiricilerin durum bilgilerini paylaşarak en iyi yolun bulunmasını sağlayan protokoldür.

Görsel 2.45'te otonom numaraları 100 ve 200 olan farklı sistemler arasında BGP protokolü ile yönlendirme görülür.



Görsel 2.45: Yol vektörü ile yönlendirme

Dinamik ağ protokollerinin özelliklerine göre karşılaştırması Tablo 2.3'te görülür.

Tablo 2.3: Dinamik Ağ Protokollerinin Karşılaştırması

Özellikleri	Uzaklık Vektörü				Bağlantı Durumu	
	RIPv1	RIPv2	IGRP	EIGRP	OSPF	IS-IS
Birleştirme Hızı	Yavaş	Yavaş	Yavaş	Hızlı	Hızlı	Hızlı
Ölçeklenebilirlik	Küçük	Küçük	Küçük	Büyük	Büyük	Büyük
VLSM	Hayır	Evet	Hayır	Evet	Evet	Evet
Kaynak Kullanımı	Düşük	Düşük	Düşük	Orta	Yüksek	Yüksek
Uygulama	Basit	Basit	Basit	Karmaşık	Karmaşık	Karmaşık

2.2.1. Dinamik Yönlendirmede Karar Verme ve Yönlendirme Kararı

Yönlendirme kararı, veri paketlerinin kaynaktan hedefe gönderilme sürecinde en verimli ve en güvenli yolun seçilmesini sağlar. Bu karar mekanizmaları birbiriyle iletişim kurar ve ağ trafiğinin yönetimini sağlar. Gerçek zamanlı verilerle en uygun rotalar belirlenir.

1. **Administrative Distance (Yönetimsel Mesafe):** Yönlendirme protokollerinin güvenirliğini ifade eden 0 ile 255 arasında sayısal bir değerdir. AD değerinin küçük olması tercih sebebidir. Tablo 2.4'te protokollerin AD değerleri görülür.

Tablo 2.4: Protokollerin AD Değerleri

Protokol	AD Değeri
Directly Connected Interface	0
Static Route	1
RIP	120
IGRP	100
EIGRP (Internal)	90
EIGRP (External)	170
OSPF	110
EGP	140
BGP (Internal)	200
BGP (External)	20
IS -IS	115

2. **Metrik Hesaplama:** Yönlendirme kararı verilirken bir rotanın tercih edilebilirliğini hesaplamak için kullanılan değerdir. Bu hesaplamada aynı protokolü kullanan ağlarda hangi rotanın daha iyi olduğu belirlenir. Metrik hesaplama için her protokol farklı ölçütleri kullanır. Protokollerin metrik hesapları Tablo 2.5'te görülür.

Tablo 2.5: Protokollerin Metrik Hesapları

Protokol	Metrik Ölçütü	Hesaplama Yöntemi
RIP	Hop Count (Geçilen yönlendirici sayısı)	Geçilen her yönlendirici değeri 1 olarak hesaplanır.
OSPF	Cost (Maliyet)	$Cost = \frac{\text{Referans Bant Genişliği}}{\text{Arayüz Bant Genişliği}}$
EIGRP	Bandwidth (Bant genişliği), Delay (Bekleme), Load (Yük), Reliability (Güvenirlik)	*Metric=256 x (K1×Bandwidth+K3×Delay)*
BGP	Path Attributes (Yol öznitelikleri)	AS Path length, Local Preference, MED gibi öznitelikler kullanılır.
IS-IS	Cost (Maliyet)	Manuel atanır veya varsayılan değeri kullanılır.

2.2.2. RIP ve RIPv2 Protokolü

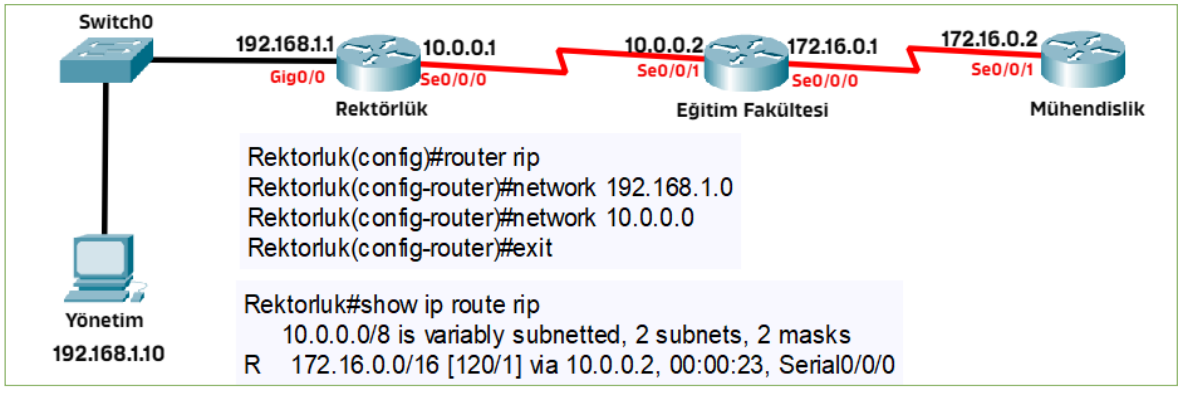
RIP (Routing Information Protocol), Bellman-Ford algoritmasını kullanan ve iki hedef arasında en kısa yolu uzaklık vektörüne göre seçen protokoldür. Yol hesaplamasında kaç adet cihaz üzerinden sıçrama yaparak ilerleyeceğini hesaplar. En fazla on beş sıçrama hesabı yapabildiği için küçük ağlarda tercih edilen bir protokoldür. Yönetimsel uzaklık değeri 120'dir. RIP yapılandırmasında her yönlendirici, kendi arayüzüne doğrudan bağlı ağ adreslerini kaydeder. Ağdaki her yönlendirici, 30 saniye aralıklarla güncellemeleri kontrol eder. Komşu yönlendiricileri arasında yapılan değişiklikler ise bekleme süresi olmadan güncellenir. RIP yapılandırmasında kullanılan komutlar şunlardır:

Router(config)#**router rip**

Router(config-router)#**network x.x.x.x**

Yönlendirme tablolarını görüntülemek için yönlendirici yetkili moddayken **show ip route rip** komutu uygulanır. Yönlendirme bilgisi **R** harfi ile görülür.

Görsel 2.46'da **Rektörlük** ismindeki yönlendiricinin RIP protokolü ile yönlendirme komutları görülür.



Görsel 2.46: RIP ile yönlendirme

Cihaz, kendisine doğrudan bağlı ağları yönlendirme tablosuna ekler. Yönlendirme tablosunda yer alan bilgiler şunlardır:

R: RIP protokolü ile yapılan yönlendirme bilgisidir.

172.16.0.0/16: Hedef ağ adresi bilgisidir.

[120/1]: Yönetimsel uzaklık ve hedef ağa giderken sıçrama yapılan cihaz sayısı bilgisidir.

10.0.0.2: Hedef ağa giderken sıçrama yapılan cihazın adres bilgisidir.

Serial 0/0/0: Hedef ağa gitmek için kullanılan arayüz bilgisidir.

RIPv2 (Routing Information Protocol Version 2), RIP protokolünün eksikliklerini ve zayıf yönlerini tamamlayan bir protokoldür. Ağ performansını ve veri güvenliğini arttıran bazı özellikler eklenmiştir.

RIP ve RIPv2'nin karşılaştırması Tablo 2.6'da görülür.

Tablo 2.6: RIP ve RIPv2'nin Karşılaştırması

RIP	RIPv2
Güncellemeler için yayın adresi kullanır.	Güncellemeler için çoklu yayın adresi kullanır.
Yayın adresi 255.255.255.255'tir.	Çoklu yayın adresi 224.0.0.9'dur.
Tetikleyici güncelleme kullanmaz.	Tetikleyici güncelleme kullanır.
Sınıfsız etki alanları arası yönlendirmeyi (CIDR) desteklemez.	Sınıfsız etki alanları arası yönlendirmeyi (CIDR) destekler.
Değişken uzuluklu ağ maskesini (VLSM) desteklemez.	Değişken uzuluklu ağ maskesini (VLSM) destekler.
Kimlik doğrulamayı desteklemez.	Kimlik doğrulamayı destekler.
Otomatik özetleme yapar.	Otomatik özetleme iptal edilebilir.

RIPv2 yapılandırmasında kullanılan komutlar şunlardır:

Router(config)#**router rip**

Router(config-router)#**version 2**

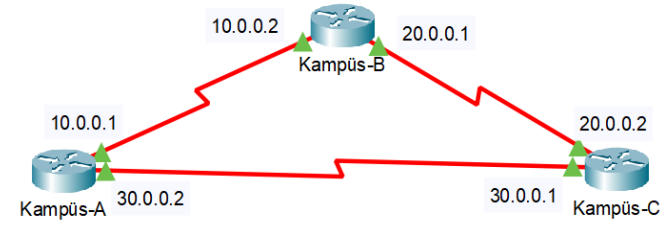
Router(config-router)#**network x.x.x.x**

Otomatik özetleme, belirli ağların veya alt ağların genel bir ağ adresiyle ifade edilerek özetlenmesi işlemidir. Ağ adreslerinin detaylandırılarak alt adreslere bölünmesi hem adres verimliliğini hem de yönlendirmenin daha detaylı olarak ifade edilmesini sağlar. Örneğin C sınıfı bir adres olan 192.168.1.0/24 ağı; 192.168.1.0/26, 192.168.2.64/26, 192.168.1.128/26 ve 192.168.1.192/26 olarak dört farklı alt ağa bölünebilir. Otomatik özetleme işlemi aktif olduğunda bu ağlar, 192.168.0.0/16 ağ adresi ile ifade edilir. Bu özellik, devre dışı bırakılmadığı durumlarda alt ağlar arası iletişimde sorunlara yol açabilir. Otomatik özetleme işlemi **no auto summary** komutuyla iptal edilir.

Görsel 2.47'de Kampüs-A cihazında RIPv2 ile yapılan yönlendirme komutları görülür. Yönlendirme tablosunda ise 20.0.0.0 ağına hangi arayüzler ve adresler üzerinden ulaşabileceği görülür.

```
Kampus-A(config)#router rip
Kampus-A(config-router)#version 2
Kampus-A(config-router)#network 10.0.0.0
Kampus-A(config-router)#network 30.0.0.0
```

```
Kampus-A#show ip route rip
     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
R    20.0.0.0/8 [120/1] via 10.0.0.2, 00:00:11, Serial0/0/0
                [120/1] via 30.0.0.1, 00:00:23, Serial0/0/1
```



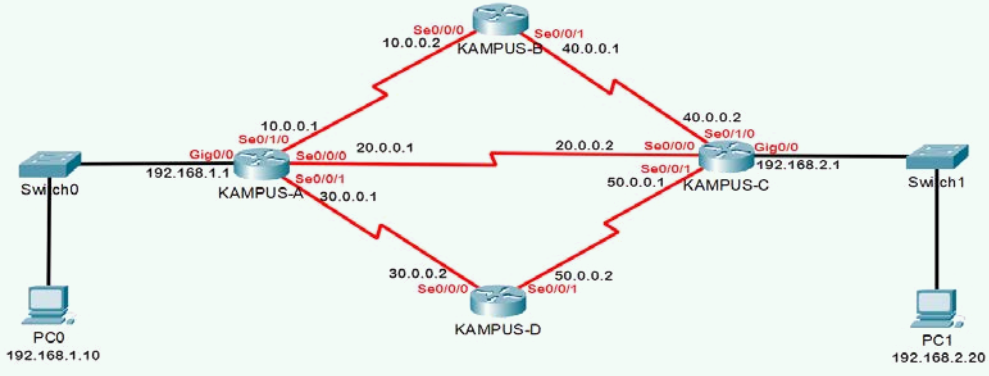
Görsel 2.47: RIPv2 ile yönlendirme

6. UYGULAMA

RIPv2 protokolünü kullanarak farklı ağların iletişim kurabilmesi işlemini verilen adımlar doğrultusunda gerçekleştiriniz.

1. Adım: Ağ simülasyon programını çalıştırınız.

2. Adım: Görsel 2.48'deki ağ topolojisini oluşturunuz.



Görsel 2.48: 6. uygulamanın ağ topolojisi

3. Adım: Görsel 2.49'da KAMPUS-A cihazının IP yapılandırması görülür. Siz de tüm cihazların yapılandırmalarını uygun arayüzlere göre oluşturunuz.

```
KAMPUS-A(config)#int gig0/0
KAMPUS-A(config-if)#ip address 192.168.1.1 255.255.255.0
KAMPUS-A(config-if)#no sh
KAMPUS-A(config-if)#int se0/1/0
KAMPUS-A(config-if)#ip address 10.0.0.1 255.0.0.0
KAMPUS-A(config-if)#no sh
KAMPUS-A(config-if)#int se0/0/0
KAMPUS-A(config-if)#ip address 20.0.0.1 255.0.0.0
KAMPUS-A(config-if)#no sh
KAMPUS-A(config-if)#int se0/0/1
KAMPUS-A(config-if)#ip address 30.0.0.1 255.0.0.0
KAMPUS-A(config-if)#no sh
```

Görsel 2.49: KAMPUS-A cihazının IP yapılandırması

4. Adım: Görsel 2.50'de KAMPUS-A cihazının RIPv2 ile yapılandırması görülür. Siz de tüm yönlendiricileri RIPv2 ile yapılandırınız.

```
KAMPUS-A(config)#router rip
KAMPUS-A(config-router)#version 2
KAMPUS-A(config-router)#network 192.168.1.0
KAMPUS-A(config-router)#network 10.0.0.0
KAMPUS-A(config-router)#network 20.0.0.0
KAMPUS-A(config-router)#network 30.0.0.0
KAMPUS-A(config-router)#no auto summary
```

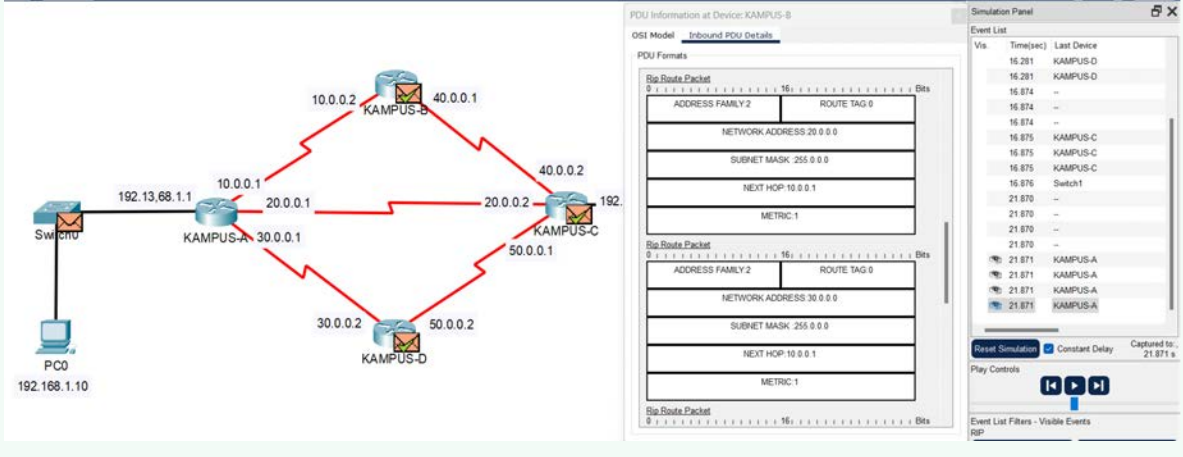
Görsel 2.50: KAMPUS-A cihazının RIPv2 ile yapılandırması

5. Adım: KAMPUS-A cihazında kaydedilen yönlendirme tablosunu görüntüleyiniz (Görsel 2.51).

```
KAMPUS-A#show ip route rip
     30.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
R    40.0.0.0/8 [120/1] via 10.0.0.2, 00:00:17, Serial0/1/0
R    50.0.0.0/8 [120/1] via 20.0.0.2, 00:00:06, Serial0/0/0
                [120/1] via 30.0.0.2, 00:00:14, Serial0/0/1
     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
R    192.168.2.0/24 [120/1] via 20.0.0.2, 00:00:06, Serial0/0/0
```

Görsel 2.51: KAMPUS-A cihazının yönlendirme tablosu

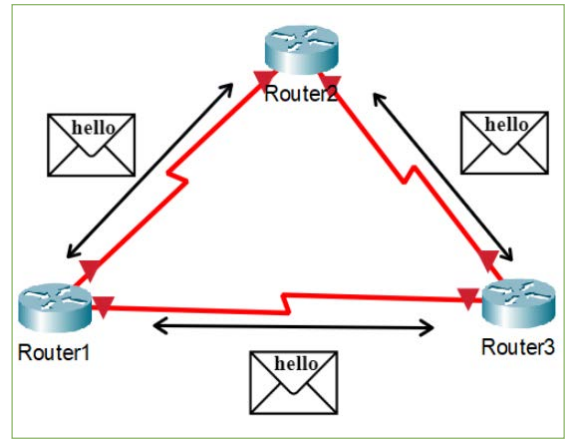
6. Adım: Simülasyon modunda veri paketini RIP olarak seçip, bilgisayarlar arasında ağ iletişimini test ederek RIP veri paketinin bilgilerini görüntüleyiniz (Görsel 2.52).



Görsel 2.52: RIP veri paketinin görüntülenmesi

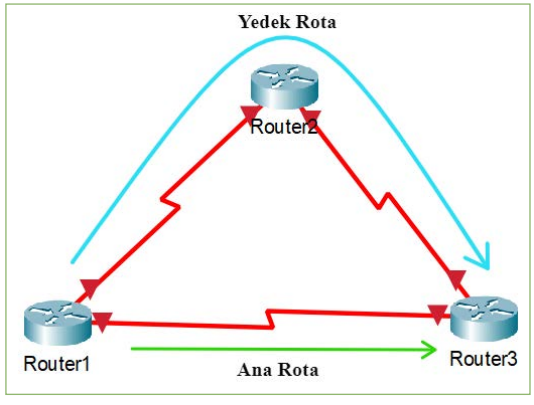
2.2.3. EIGRP Protokolü

EIGRP (Enhanced Interior Gateway Protocol), IGRP'nin (Interior Gateway Protocol) geliştirilmiş versiyonudur. EIGRP hem uzaklık hem de bağlantı durumu kontrolü yapabilen hibrit bir protokoldür. Uzaklık vektörü ile komşu cihazlardan ağın tamamı hakkında bilgi alabilir. Bağlantı durumu ile de bant genişliği, veri iletim hızı gibi değişkenlerle ilgili bilgi alır. Yönlendirme tablolarını komşu cihazlarla paylaşır ve yapılan değişiklikleri günceller. En fazla **255** cihaza kadar sıçrama yapabilir. Bu yönüyle daha büyük ağlarda kullanıma uygundur. İç ağlarda yönetimsel uzaklık değeri **90**, dış ağlarda ise **170**'tir. VLSM ve CIDR'yi destekler. EIGRP protokolünü kullanan cihazlar arasında **beş saniye** aralıklarla **hello** paketleri gönderilir. Bu paketi alan cihazlar **acknowledgement** paketi ile komşuluğu onaylar. Komşu cihazdan on **beş saniye** içinde cevap alınamazsa komşuluk bilgileri silinir. EIGRP'de kullanılan **hello** paketleri Görsel 2.53'te görülür.



Görsel 2.53: EIGRP'de kullanılan hello paketleri

EIGRP, yönlendiricilerin güncelleme tablolarını paylaşırken ve verilerin iletimini sağlarken güvenli iletim için **RTP**'yi **(Realiable Transport Protocol)** kullanır.



Görsel 2.54: Ana rota ve yedek rota gösterimi

Yönlendirme işleminde en iyi rotayı belirlemek için **DUAL (Diffusing Update Algorithm)** algoritmasını kullanır. DUAL algoritmasında ana rotaya alternatif olarak yedek rota da belirlenir. Ana rotada herhangi bir aksaklık meydana gelirse yedek rota üzerinden iletim devam eder (Görsel 2.54). DUAL algoritmasında **komşuluk tablosu** ve **topoloji tablosu** olmak üzere iki çeşit tablo bulunur. Komşuluk tablosunda komşu cihazların bağlantı bilgileri yer alırken topoloji tablosunda ağdaki tüm rotalar ve metrik değerler yer alır.

EIGRP protokolü tanımlanırken **1** ile **65.565** arasında bir otonom sistem numarası (AS) belirlenir. Otonom sistem numarası, protokolün tanımlı olduğu tüm cihazlarda aynı olmalıdır. EIGRP yapılandırmasında kullanılan komutlar şunlardır:

Router(config)#router eigrp [otonom sistem numarası]

Router(config-router)#network [ağ adresi] [ağ maskesi / genel arama maskesi (wildcard)]

Yönlendiricinin belirli bir ağa veya alt ağa yayın yapması isteniyorsa genel arama maskesi kullanılır. Genel arama maskesi, IP adresinin belirli bitlerinin ağ adresleri ile eşleştirilmesiyle hesaplanır. Genel arama maskesini hesaplamanın en pratik yolu ağ maskesinin 255.255.255.255'ten çıkarılmasıdır. Görsel 2.55'te bu işlemin iki sayı sisteminde hesaplaması görülür.

	11111111.11111111.11111111.11111111	255.255.255.255
Alt Ağ Maskesi →	- 11111111.11111111.11111111.00000000	255.255.255.000
Genel Arama Maskesi →	00000000.00000000.00000000.11111111	000.000.000.255

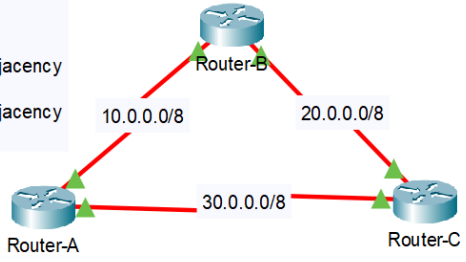
Görsel 2.55: Genel arama maskesinin hesaplanması

Yönlendirme tablosundaki EIGRP rotalarını görüntülemek için **show ip route eigrp** komutu kullanılır. Görsel 2.56'da Router-A cihazında yapılandırılan EIGRP ile yönlendirme komutları görülür.

```
Router-A(config)#router eigrp 100
Router-A(config-router)#network 10.0.0.0 0.255.255.255
Router-A(config-router)#network 30.0.0.0 0.255.255.255
Router-A(config-router)#
%DUAL-5-NBRCHANGE: IP-EIGRP 100: Neighbor 10.0.0.2 (Serial0/0/0) is up: new adjacency

%DUAL-5-NBRCHANGE: IP-EIGRP 100: Neighbor 30.0.0.2 (Serial0/0/1) is up: new adjacency
```

```
Router-A#show ip route eigrp
     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
D    20.0.0.0/8 [90/2681856] via 10.0.0.2, 00:02:10, Serial0/0/0
                [90/2681856] via 30.0.0.2, 00:01:44, Serial0/0/1
```



Görsel 2.56: EIGRP ile yönlendirme

A sınıfı bir ağ adresinin genel arama adresi 0.255.255.255 olarak hesaplanır. Yönlendirme işlemi tüm cihazlarda tamamlandığında **new adjacency** bilgisi bir arayüz üzerinden komşuluk eklendiğini gösterir. Router-A cihazındaki yönlendirme tablosunda, 20.0.0.0 ağına erişim bilgileri görülür. Yönlendirme tablosunda yer alan bilgiler şunlardır:

D: EIGRP ile yönlendirme bilgisidir.

20.0.0.0/8: Hedef ağ adres bilgisidir.

[90-2681856]: EIGRP yönetimsel uzaklık değeri ile hedef ağ için toplam maliyet metrik değeridir.

10.0.0.2: Hedef ağa gitmek için sıçrama yapılacak olan yönlendiricinin arayüz adres bilgisidir.

00:02:10: EIGRP ile komşuluk sağlandığı andan itibaren geçen süre bilgisidir.

Serial0/0/0: Hedef ağa gitmek için çıkış yapılan arayüz bilgisidir.

Görsel 2.57'de **show ip eigrp neighbors** komutuyla komşuluk bilgisi görülür.

```
Router-A#show ip eigrp neighbors
IP-EIGRP neighbors for process 100
H   Address         Interface       Hold Uptime   SRTT   RTO  Q  Seq
                                    (sec)         (ms)       Cnt Num
0   10.0.0.2        Se0/0/0          13 00:16:35  40     1000 0  4
1   30.0.0.2        Se0/0/1          12 00:15:59  40     1000 0  8
```

Görsel 2.57: Komşuluk bilgisinin görüntülenmesi

Komşuluk tablosunda yer alan bilgiler şunlardır:

H (Handle/Instance): EIGRP komşuluğuna atanan indeks numarasıdır. Komşulukların sıralanmasını sağlar.

Address: EIGRP komşusunun IP adresidir.

Interface: EIGRP komşuluğunun kurulduğu arayüz bilgisidir. Mesajlar bu arayüzden iletilir.

Hold: EIGRP komşuluğunun durumunu beklemek için geçen süredir. Eğer bu süre içinde komşuluk mesajı iletilmezse komşuluk düşer.

Uptime: EIGRP komşuluğunun kurulduğu süredir.

SRTT (Smooth Round-Trip Time): EIGRP mesajlarının komşu cihaza ulaşma süresidir.

RTO (Retransmit Timeout): EIRP mesajlarının yeniden gönderilmesi için beklenen süredir.

Q (Queue): EIGRP mesajların gönderim kuyruğunda bekleyen mesaj sayısıdır.

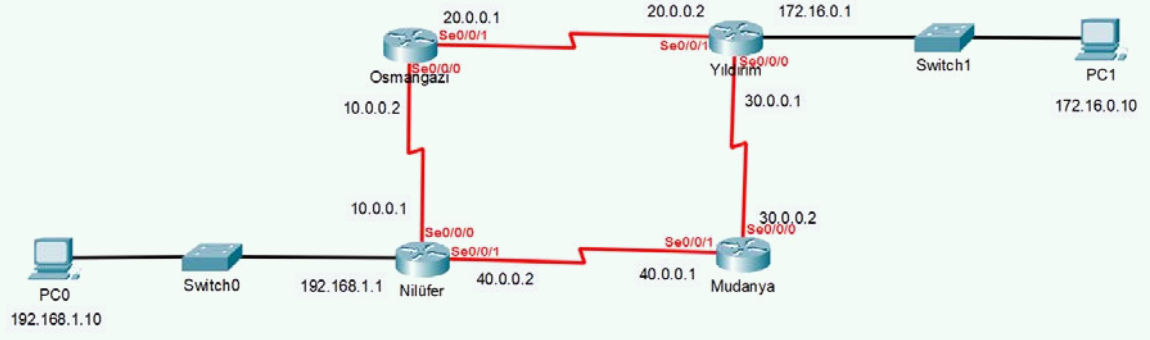
Seq (Sequence Number): EIGRP komşuluğu için kullanılan sıra numarasıdır.

7. UYGULAMA

EIGRP ile yönlendirme işlemini verilen adımlar doğrultusunda gerçekleştiriniz.

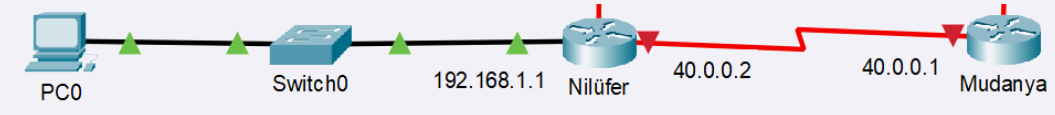
1. Adım: Ağ simülasyon programını çalıştırınız.

2. Adım: Görsel 2.58'deki ağ topolojisini oluşturunuz.



Görsel 2.58: 7. uygulamanın ağ topolojisi

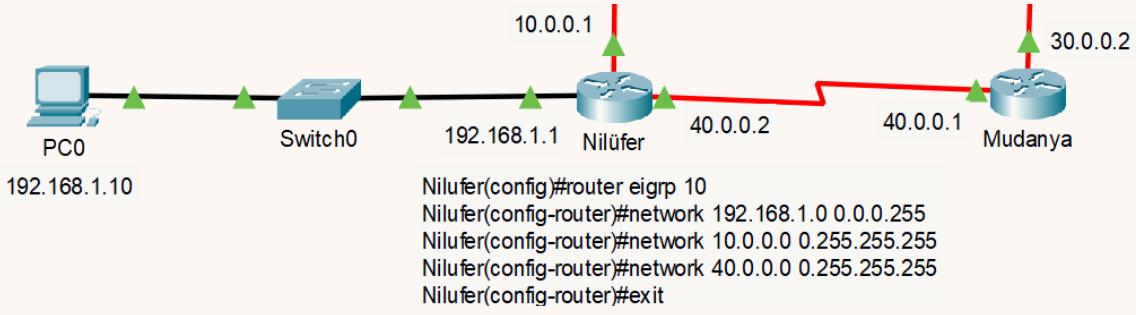
3. Adım: Görsel 2.59'da Nilüfer isimli yönlendiricinin arayüzüne ait IP yapılandırılması görülür. Siz de tüm yönlendirici cihazları ve bilgisayarları uygun IP adresleriyle yapılandırınız.




```
Nilufer(config)#int gig0/1
Nilufer(config-if)#ip address 192.168.1.1 255.255.255.0
Nilufer(config-if)#no sh
Nilufer(config-if)#int se0/0/0
Nilufer(config-if)#ip address 10.0.0.1 255.0.0.0
Nilufer(config-if)#no sh
Nilufer(config-if)#int se0/0/1
Nilufer(config-if)#ip address 40.0.0.2 255.0.0.0
Nilufer(config-if)#no sh
Nilufer(config-if)#do write
Building configuration...
```

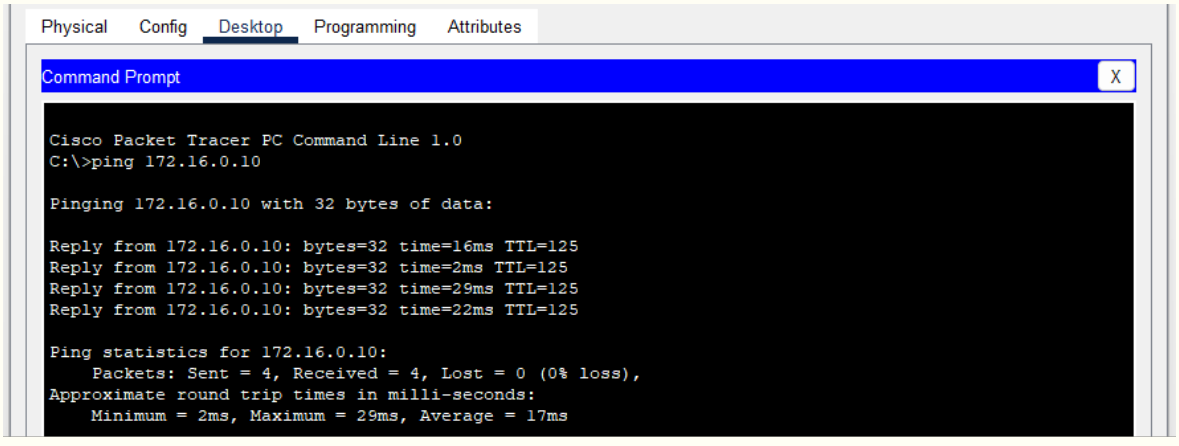
Görsel 2.59: Nilüfer cihazının IP yapılandırması

4. Adım: Görsel 2.60'ta Nilüfer isimli yönlendiricinin EIGRP ile yönlendirme komutları görülür. Siz de tüm yönlendiricilerin yönlendirme işlemlerini tamamlayınız.



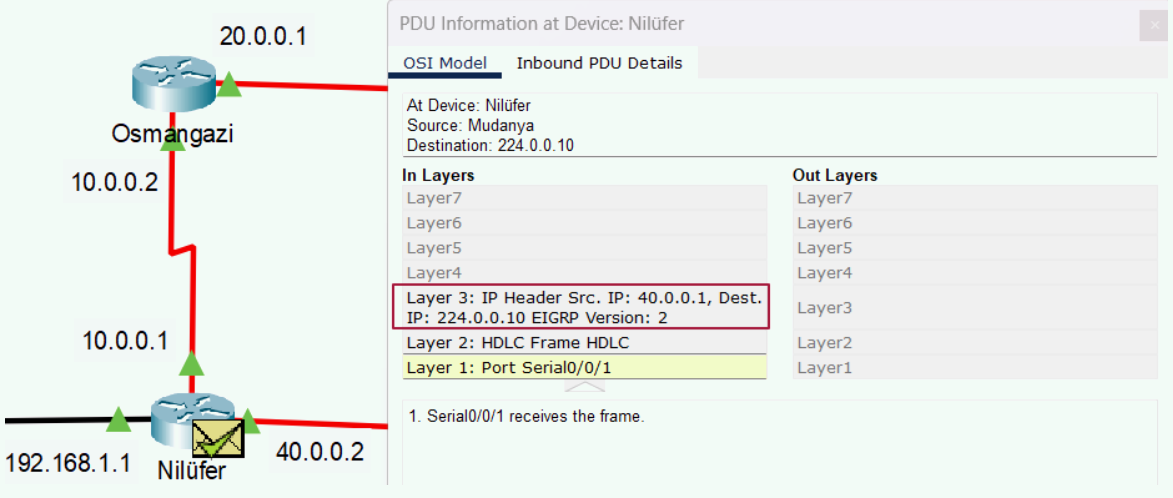
Görsel 2.60: EIGRP ile yönlendirme

5. Adım: PC0 cihazının arayüzüne giriş yapıp, Desktop/Command Prompt seçeneğinden komut arayüzüne girerek **ping** komutu ile PC0 ve PC1 cihazlarının ağ iletişimini test ediniz (Görsel 2.61).



Görsel 2.61: Bilgisayarlar arası iletişimin test edilmesi

6. Adım: Simülasyon modda ARP ve EIGRP paketlerini seçerek yönlendiriciler arasında gönderilen paketleri görüntüleyiniz (Görsel 2.62).



Görsel 2.62: EIGRP paketlerinin görüntülenmesi

7. Adım: Nilüfer cihazının EIGRP ile yapılan yönlendirme bilgilerini görüntüleyiniz (Görsel 2.63).

```
Nilufer#show ip route eigrp
     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
D    20.0.0.0/8 [90/2681856] via 10.0.0.2, 00:07:25, Serial0/0/0
D    30.0.0.0/8 [90/2681856] via 40.0.0.1, 00:06:04, Serial0/0/1
     40.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
D    172.16.0.0/16 [90/2682112] via 10.0.0.2, 00:06:39, Serial0/0/0
                   [90/2682112] via 40.0.0.1, 00:06:04, Serial0/0/1
```

Görsel 2.63: Yönlendirme bilgisinin görüntülenmesi

8. Adım: Nilüfer cihazının EIGRP ile oluşturulan komşuluk bilgilerini görüntüleyiniz (Görsel 2.64).

```
Nilufer#show ip eigrp neighbors
IP-EIGRP neighbors for process 10
H  Address         Interface     Hold Uptime    SRTT  RTO  Q  Seq
                                 (sec)  (ms)    Cnt  Num
0  10.0.0.2        Se0/0/0       13   00:08:25  40   1000 0  11
1  40.0.0.1        Se0/0/1       13   00:06:54  40   1000 0  18
```

Görsel 2.64: Komşuluk bilgilerinin görüntülenmesi

2.2.4. OSPF

OSPF (Open Shortest Path First), bağlantı durumu yönlendirme protokollerinden biri olup **ilk önce en kısa yolun hesaplaması** mantığıyla çalışır. Uzaklık vektörü protokollerine göre biraz daha karmaşık bir yapıdadır. Bağlantı durumu kontrolü ile ağın tamamı hakkında bilgiye sahip olur. Ağda meydana gelen değişiklikler veya arızalar sonucu hatların değişmesi bilgisini, tetiklenmiş güncellemeler ile günceller.

En iyi kısa yolu hesaplamak ve ağın tamamı hakkında bilgi sahibi olmak için **Dijkstra Algoritmasını** kullanır. Dijsktra algoritması SPF (Short Path First) hesaplaması yaparak SPF ağacı oluşturur. Buna göre her yönlendirici, ağdaki diğer komşu yönlendiricilerle aralarındaki maliyeti hesaplayan veri tabanı kayıtları oluşturur. Daha sonra bu bilgiler, belirli aralıklarla güncellenerek paylaşılır. OSPF'de yönlendirici cihazlarda kaydedilen tablolar şunlardır:

Komşu Tablosu (Neighbor Table): Yönlendiricinin doğrudan bağlı olduğu komşu cihazların bilgilerinin kaydedildiği tablodur. Her yönlendiricide bu tablo farklıdır. Komşu tablosu **show ip ospf neighbor** komutu ile görüntülenir.

Topoloji Tablosu (Topology Table): Dijkstra Algoritması ile hesaplanan bu tabloda, ağdaki tüm yönlendiricilerin bağlantı durumunu kaydeder. Yönlendiriciler, komşu cihazlara **LSA (Link State Advertisement)** paketleri gönderir. Bu paketlerde, kendi bağlantı durumu bilgisini paylaşır. LSA paketlerini alan her yönlendirici, bu bilgileri **LSDB (Link State Database)** tablosuna kaydeder. Yönlendirici cihazlar belirli aralıklarla kaydettiği bilgileri ağdaki diğer yönlendirici cihazlarla paylaşır. Böylelikle ağın tamamı hakkında bilgi sahibi olur. Topoloji bilgisi **show ip ospf database** komutu ile görüntülenir.

Yönlendirme Tablosu (Routing Table): LSDB'den elde edilen verilerle en iyi yol için yapılacak yönlendirme bilgileri bu tabloda kaydedilir. Bu tabloda, hedef ağ adreslerine ulaşmak için kullanılacak çıkış arayüzleri ve komşu yönlendirici bilgileri yer alır. Yönlendirme tablosundaki OSPF rotaları **show ip route ospf** komutu ile görüntülenir.

Her yönlendirici kendi bağlantı noktalarını ve kendine bağlı ağları doğrudan öğrenir. Bağlantıda olduğu diğer cihazların bilgilerini ise bağlantı durumu kontrol mesajlarıyla öğrenir. Ağa katılan bir cihazın diğer cihazlarla ilk tanışması sırasında ve normal çalışma süresince cihazlar arasında bilgi mesajları iletilir. Bu mesajlar; cihazların kendini tanıtması, bağlantı ve yönlendirme bilgilerini paylaşması ile ilgilidir. Belirli aralıklarla yapılan bu işlem, ağın güncel bilgilerle sorunsuz çalışmasını hedefler.

2.2.4.1. OSPF Paketleri

OSPF ağlarında yönlendiriciler arasında ağ bilgilerini paylaşmak ve en iyi rotayı hesaplamak için bazı paketler kullanılır. Bu paketler; yeni bir komşu cihazla tanışma, veri tabanı bilgilerini güncelleme ve ağ durumlarını paylaşma ile ilgili birçok süreci sağlar. OSPF yönlendiriciler arasında gönderilen bilgilerin bütünlüğü ve doğruluğunun sağlanması açısından önemlidir. OSPF veri paketleri şunlardır:

1. **Hello Paketi:** Komşu yönlendiricileri keşfetmek, komşuluk oluşturmak ve komşulukları sürdürmek için kullanılır.

2. **DBD (Database Description) Paketi:** Yönlendiriciler arasındaki bağlantı durumu, veri tabanı (LSDB) bilgilerinin senkronize edilmesini sağlar. Her yönlendirici kendi LSDB bilgisini kaydeder. DBD paketleri, bir yönlendiricinin veri tabanındaki LSA bilgilerinin özet başlıklarını gönderir. LSA'lar hakkında özet bilgi sağlayarak hangi LSA'nın talep edilmesi gerektiğine karar verir. Bu bilgiler, ağda belirli aralıklarla paylaşılarak tüm LSDB'lerin aynı anda güncel olması sağlanır. LSDB'ler doğru SPF'lerin oluşturulmasında önemli rol oynar.

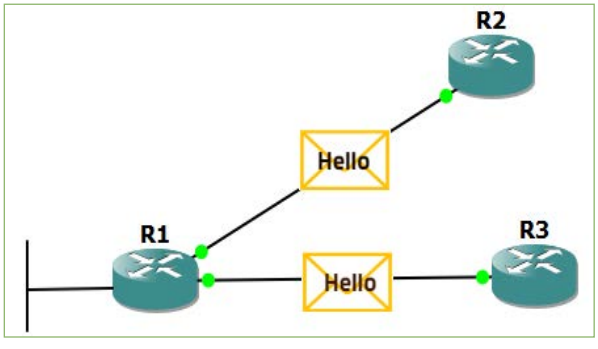
3. **LSR (Link-State Request) Paketi:** Yönlendiriciler arasında özel bağlantı durum kayıtlarının istenmesini sağlar. Eksik olan veya güncellenmesi gereken LSA talepleri için LSR'ler kullanılır.

4. **LSU (Link-State Update) Paketi:** Yönlendiriciler arasında güncellenmiş LSA'ları iletmek için kullanılır.

5. **LSAck (Link-State Acknowledgment) Paketi:** Gönderilen LSA paketlerinin başarılı bir şekilde alındığını onaylamak için kullanılır.

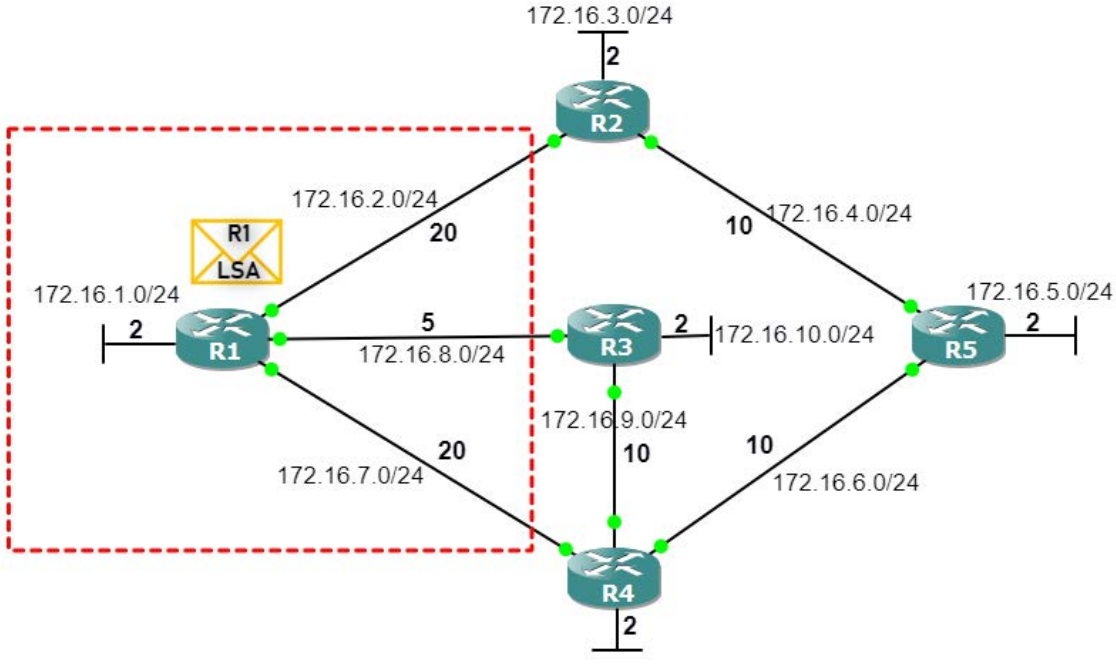
Bağlantı durumu kontrolü ile komşuluk kurulması süreci şu şekildedir:

1. **Hello Paketi:** Yönlendiriciler, ağdaki komşu cihazlarla tanışmak için **hello** paketleri gönderir. Bu tanışma paketinde yönlendirici, kendini tanıtır. Bu mesajı alan diğer yönlendiriciler, mesajdaki bilgiyi kaydedip kendi bilgilerini gönderir. Bu şekilde komşuluk bağlantısı sağlanır. Komşuluk sağlandıktan sonra da belirli aralıklarla **hello** paketleri gönderilir ve bağlantının devam edip etmediği kontrol edilir. Bu paketler iletilmediğinde ise bağlantı bilgisi komşu tablosundan silinir. OSPF'de noktadan noktaya bağlantılarda **on** saniye aralıklarla **hello** paketleri gönderilir. Yönlendiriciler belirli bir süre boyunca **hello** paketi almadığında **ölü aralık zamanı (dead interval)** devreye girer. Ölü aralık zamanı, hello paketi gönderim süresinin dört katı olup **kırk** saniyedir. Bu süre sonunda cevap alınamazsa komşuluk LSDB'den silinir. Görsel 2.65'te R1 yönlendiricisinden R2 ve R3 yönlendiricilerine gönderilen **hello** paketleri görülür.



Görsel 2.65: Hello paketi gönderimi

2. LSA Paketleri: Yönlendiriciler hem kendileri hem de bağlantıda oldukları diğer yönlendirici cihazlar hakkında bağlantı durum bilgisini üretir. Bu paketlere **LSA** adı verilir. Görsel 2.66'da R1 yönlendiricisinden diğer yönlendiricilerine kendi LSA paketlerinin paylaşımı görülür.



Görsel 2.66: LSA paketinin gönderimi

3. LSDB Güncellemesi: LSA paketleri alındığında yönlendirici, bu bilgileri bağlantı durum veri tabanına kaydeder. LSDB'ler ile tüm ağın topolojisi hakkında bilgi sahibi olunur. Yönlendiriciler belirli aralıklarla kendi LSDB'lerini paylaşır ve ağın en güncel durumu yansıtılmış olur. Görsel 2.66'daki ağ topolojine göre yönlendiricilerin bağlantı durumu veri tabanı bilgileri Tablo 2.7'de görülür.

Tablo 2.7: Bağlantı Durumu Veri Tabanı Bilgileri

Bağlantı Durumu Veri Tabanı	
R1 Bağlantı Durumu: 172.16.1.0/24 ağına bağlı maliyet = 2 172.16.2.0/24 ağına bağlı maliyet = 20 172.16.8.0/24 ağına bağlı maliyet = 5 172.16.7.0/24 ağına bağlı maliyet = 20	**R3 Bağlantı Durumu:** 172.16.8.0/24 ağına bağlı maliyet = 5 172.16.9.0/24 ağına bağlı maliyet = 10 172.16.10.0/24 ağına bağlı maliyet = 2
R2 Bağlantı Durumu: 172.16.2.0/24 ağına bağlı maliyet = 20 172.16.3.0/24 ağına bağlı maliyet = 2 172.16.4.0/24 ağına bağlı maliyet = 10	**R4 Bağlantı Durumu:** 172.16.6.0/24 ağına bağlı maliyet = 10 172.16.7.0/24 ağına bağlı maliyet = 20 172.16.9.0/24 ağına bağlı maliyet = 10

R5 Bağlantı Durumu:

172.16.4.0/24 ağına bağlı maliyet = 10

172.16.5.0/24 ağına bağlı maliyet = 2

172.16.6.0/24 ağına bağlı maliyet = 10

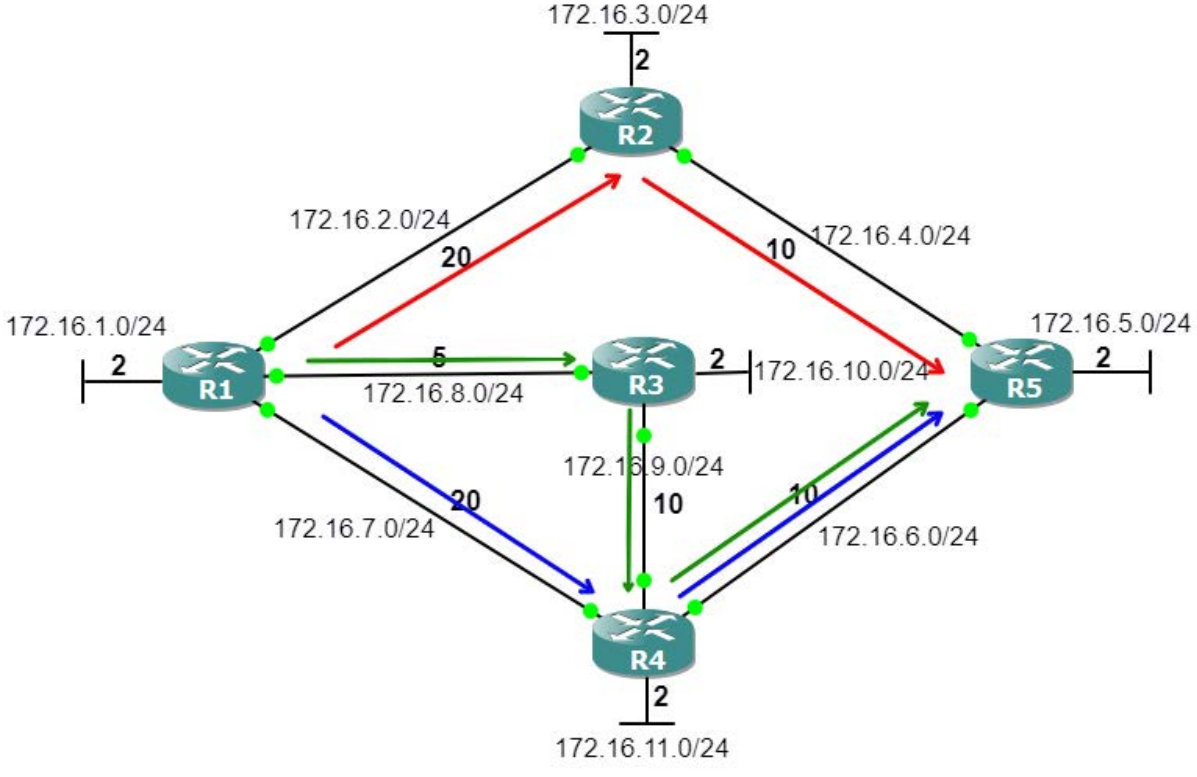
4. **SPF Hesaplama:** Yönlendiricilerde kaydedilen LSDB bilgilerine dayanarak en kısa yol bilgisinin hesaplanmasıdır. Görsel 2.66'da R1 cihazından R5 cihazına bağlı 172.16.5.0 ağına erişim için rotalar görülür. En kısa yol maliyeti şu şekilde hesaplanır:

   R1 --> R2 --> R5 rotasına göre toplam maliyet 20 + 10 + 2 = 32

   R1 --> R3 --> R4 --> R5 rotasına göre toplam maliyet 5 + 10 + 10 + 2 = 27

   R1 --> R4 --> R5 rotasına göre toplam maliyet 20 + 10 + 2 = 32

Verilen hesaplamaya göre en kısa yol maliyet değeri, **27** ile **R1 --> R3 --> R4 --> R5** rotası olduğundan bu rota tercih edilir (Görsel 2.67).



Görsel 2.67: En iyi yolun seçilmesi

5. **Yönlendirme Tablosunun Güncellenmesi:** SPF hesaplamasından sonra hedef ağlar ile ilgili en iyi yol bilgileri oluşturulur ve tabloya kaydedilir. R1 cihazında kaydedilen yönlendirme tablosu bilgileri şöyledir:

Doğrudan Bağlı Ağlar

172.16.1.0/24 Fastethernet 0/0

172.16.2.0/24 Serial 0/0/0

172.16.8.0/24 Serial 0/0/1

172.16.7.0/24 Serial 0/0/2

Uzak Ağlar

172.16.3.0/24, R2 Serial 0/0/0 üzerinden, maliyet = 22

172.16.10.0/24, R3 Serial 0/0/1 üzerinden, maliyet = 7

172.16.9.0/24, R3 Serial 0/0/1 üzerinden, maliyet = 15

172.16.11.0/24, R3 Serial 0/0/1 üzerinden, maliyet = 17

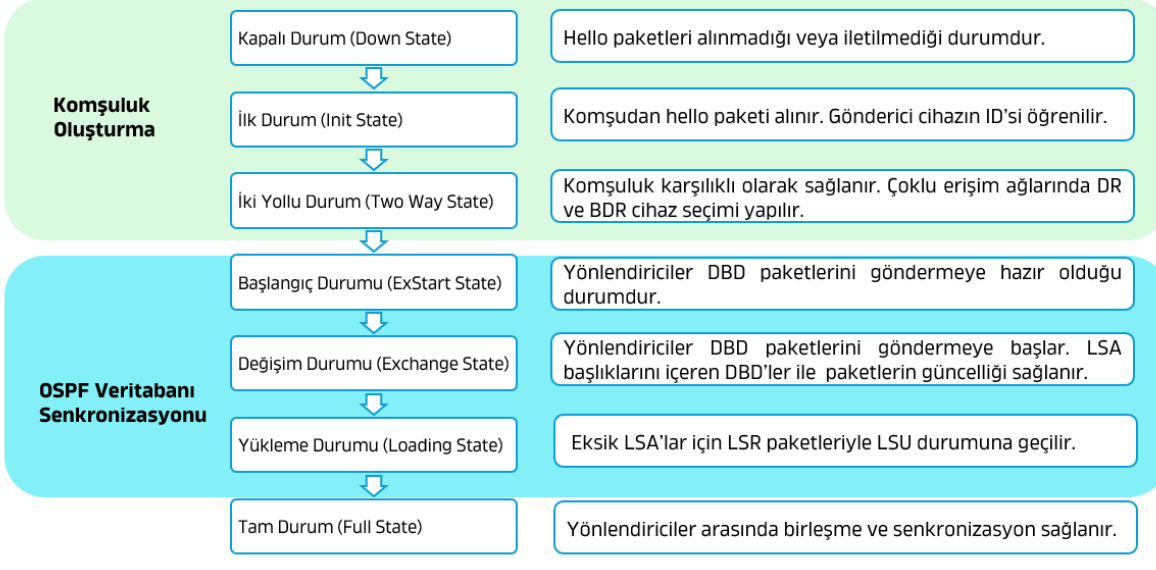
172.16.4.0/24, R2 Serial 0/0/0 üzerinden, maliyet = 30

172.16.6.0/24, R3 Serial 0/0/1 üzerinden, maliyet = 25

172.16.5.0/24, R3 Serial 0/0/1 üzerinden, maliyet = 27

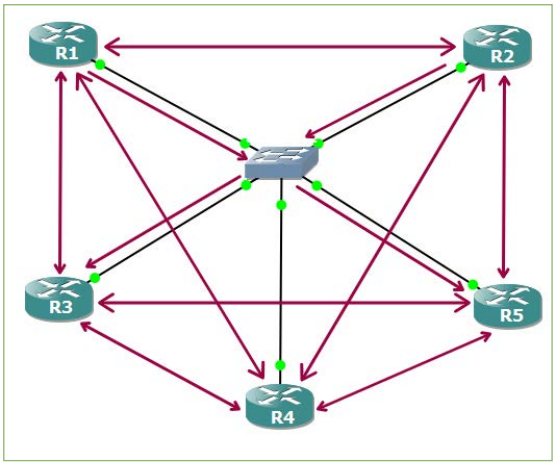
2.2.4.2. OSPF İşleyiş Durumları

OSPF'de ağa yeni katılan bir yönlendiricinin komşuluk kurduktan sonra en iyi rotaları hesaplayıp diğer yönlendiricilerle birleştirmeyi tamamlaması gerekir. Yönlendiricinin kapalı durumdan tam birleşme durumuna geçmesi için gereken süreçler Görsel 2.68'de görülür.



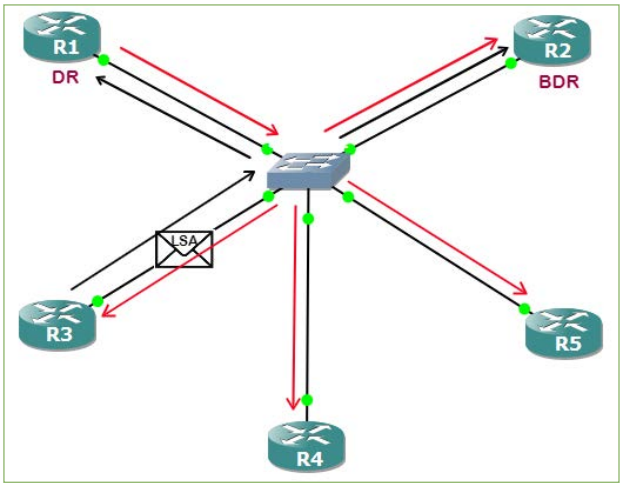
Görsel 2.68: OSPF işleyiş durumları

Birden fazla yönlendiricinin etkin olduğu çoklu erişim ağlarında her bir yönlendiricinin LSA paketleri göndermesi gereksiz ağ trafiğine sebep olur. Görsel 2.69'da beş adet yönlendirici cihaz arasındaki komşuluk bağlantısı görülür. Hem komşuluk oluşturulmasında hem de veri tabanı senkronizasyon süreçlerinde LSA paketlerinin iletimi çok fazla trafiğe neden olur.



Görsel 2.69: Cihazlar arasında komşuluk bağlantısı

LSA paketlerinin gönderiminde gereksiz ağ trafiğini önlemek için yönlendiriciler arasında **DR (Designated Router)** ve **BDR (Backup Designated Router)** seçimi gerçekleştirilir. Ağda DR ve BDR rolünde olmayan yönlendiriciler, doğrudan birbirleri ile değil DR cihazı aracılığıyla LSA bilgilerini paylaşır ve bu bilgilerin bir kopyasını da BDR cihazına iletir. DR cihaz ise ağdaki tüm yönlendiricilerden aldığı LSA paketlerini yeniden BDR ve diğer tüm yönlendiricilere gönderir. DR cihazın devre dışı kalması durumunda BDR cihazı, DR görevini üstlenir. Sistemde BDR cihazı kalmadığı için yeni bir BDR cihazı seçilir. DR ve BDR ile iletişim kuran diğer standart cihazlar ise **DROTHER** olarak adlandırılır. Devre dışı kalan DR cihazı geri döndüğünde yeniden DR görevini üstlenemez ve DROTHER olarak devam eder. Görsel 2.70'te R3 cihazından gönderilen LSA paketini DR ve BDR cihazları teslim alır ve görevi DR olan R1 cihazı tarafından BDR ve diğer tüm cihazlara gönderilir.



Görsel 2.70: DR ve BDR cihaz seçimi

2.2.4.3. DR ve BDR Cihaz Seçim Süreci

OSPF ağlarında verimliliği sağlamak ve denetlemek için tüm yönlendiricilerde DR ve BDR cihazlar kullanır. BDR, DR cihazın yedeğidir. DR ve BDR cihaz seçiminde OSPF öncelik değeri dikkate alınır. En yüksek öncelik değerine sahip yönlendirici DR, ikinci en yüksek öncelik değerine sahip yönlendirici ise BDR seçilir. Öncelik değeri varsayılan olarak 1'dir. Öncelik değeri 0 olan yönlendiriciler DR-BDR cihaz seçim sürecine dâhil edilmez. Eğer tüm yönlendiricilerin öncelik değeri 1 ise Router ID değerine göre DR-BDR seçimi yapılır. En yüksek Router ID, DR; ikinci en yüksek Router ID, BDR olarak seçilir. Bu cihazların seçimi, yönetici tarafından manuel veya OSPF protokolünün işleyişi sırasında otomatik olarak yapılır. DR-BDR seçim süreci çoklu erişim (multiaccess) ağlarında gerçekleşir. Noktadan noktaya (point-to-point) ağlarda gerçekleşmez. DR ve BDR cihaz seçim süreci şu şekildedir:

1. **Öncelik Değerleri (Priority):** OSPF ağlarında yönlendiricilerin DR ve BDR cihaz olabilmesi için sahip olması gereken ve 0 ila 255 arasındaki sayısal bir değerdir. Ağ iletişiminde komşuluk kurulması sürecinde her yönlendirici, kendi öncelik değerini ve yönlendirici kimlik bilgisini diğer cihazlarla paylaşır. Ağ yöneticileri, belirlenen yönlendiricilerin DR ve BDR olarak seçilmesi için öncelik değerini manuel olarak ayarlayabilir. Öncelik değerini belirlemek için yönlendirici, arayüz yapılandırma modundayken şu komutlar uygulanır:

   Router(config)#**interface <arayüz_ismi>**

   Router(config-if)#**ip ospf priority <değer>**

2. Yönlendirici Kimliği (Router ID): Her yönlendiricinin benzersiz olarak tanımlanmasını sağlayan değerdir. Yönlendirici kimliği manuel olarak veya arayüz değerlerine göre belirlenir.

Manuel Tanımlama: Yönlendirici kimliğinin doğrudan yapılandırılmasıdır. Yönlendirici, yönlendirme protokolü yapılandırma modundayken şu komutlar ile uygulanır:

Router(config)**#router ospf <ospf işlem numarası>**

Router(config-router)**#router-id <router-id>**

Manuel tanımlama, ağ yöneticisi tarafından yapılır. Genellikle en tercih edilen yöntemdir.

Loopback Arayüzü: Yönlendirici kimliğinin manuel olarak tanımlanmadığı durumlarda varsa loopback arayüzlerden en yüksek IP adresine sahip değer, yönlendirici kimliği olarak seçilir.

Router(config)**#interface loopback0**

Router(config-if)**#ip address 192.168.1.1 255.255.255.255**

Router(config)**#interface loopback1**

Router(config-if)**#ip address 10.0.0.1 255.255.255.255**

Verilen yapılandırmaya göre loopback0 arayüzünde tanımlı olan 192.168.1.1 adresi, en yüksek değer olduğu için Router-ID olarak seçilir.

Fiziksel Arayüz: Yönlendirici kimliğinin hem manuel olarak tanımlanmadığı hem de loopback arayüzü yapılandırılmadığı durumlarda fiziksel arayüzlerin IP adresine bakılır. Aktif arayüzlerde yapılandırılan en yüksek IP adresi o yönlendiricinin kimliği olarak belirlenir.

Router(config)**#interface GigabitEthernet0/0**

Router(config-if)**#ip address 172.16.0.2 255.255.255.0**

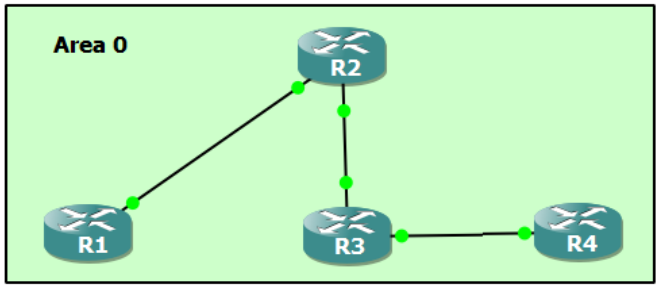
Router(config)**#interface GigabitEthernet0/1**

Router(config-if)**#ip address 192.168.0.1 255.255.255.0**

Verilen yapılandırmaya göre GigabitEthernet0/1 arayüzünde tanımlı olan 192.168.0.1 adresi en yüksek değer olduğu için Router-ID olarak seçilir.

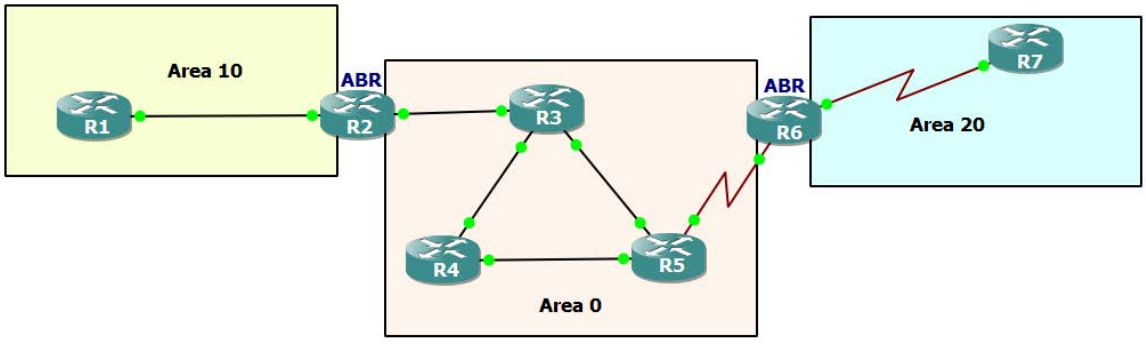
2.2.4.4. OSPF'de Ağ Topolojisi

OSPF ağlarında yönlendirmenin daha etkili ve ölçeklenebilir olması için alanlar kullanılır. Hiyerarşik yapı tasarlanırken tüm yönlendiricilerin bağlı olduğu omurga alanı, **Area 0** olarak adlandırılır. OSPF alanları LSA ve LSDB bilgilerini paylaşan yönlendiricilerden oluşur. OSPF ile yönlendirme **tek alanlı** veya **çok alanlı** olarak yapılabilir. Görsel 2.71'de tek alanlı OSPF yapılandırması görülür. Tek alanlı OSPF'de tüm yönlendiriciler, **omurga alanı** olarak adlandırılan **Area 0**'da yer alır.



Görsel 2.71: Tek alanlı OSPF

Çok alanlı OSPF ağlarında ise hiyerarşik yapı tasarlanırken tüm alanlar omurga alanı olan Area 0'a bağlanır. Alanları birbirine bağlayan sınır yönlendiricileri, **ABR (Area Border Router)** olarak adlandırılır. Görsel 2.72'de R2 ve R6 cihazları ABR'dir. OSPF alanlarında ağ topolojisi ve kullanılan cihaz sayıları birbirinden farklı olabilir. Aynı alandaki cihazlar, aynı işlem numarası ile gruplanır. Her bir alanın bağlantı durumu veya ağ güncellemeleri, kendi içinde değerlendirilir. Büyük ağların işleyişinde bellek yükünü hafifleten bir yöntemdir.



Görsel 2.72: Çok alanlı OSPF

2.2.4.5. OSPF'de Maliyet Hesaplama

OSPF ağlarında maliyet hesabı ile bir yolun tercih edilme önceliği belirlenir. Veri paketlerinin bir arayüzden gönderilmesi daha düşük maliyetli yolun seçilmesi ile olur. Bir yolun düşük maliyetli olması verilerin en hızlı şekilde gönderilmesini ifade eder. Bu sebeple maliyet hesabı arayüzlerin bant genişliği ile ters orantılıdır. OSPF maliyet hesabı şu formülle yapılır:

$$\text{Maliyet} = \frac{\text{referans bant genişliği}}{\text{arayüz bant genişliği}}$$

Varsayılan bant genişliği 100.000.000 bps'dir. Arayüzlerin bant genişliklerine göre maliyet hesapları Tablo 2.8'de görülür.

Tablo 2.8: Arayüzlerin Maliyet Hesabı

Arayüz	Referans Bant Genişliği / Arayüz Bant Genişliği	Maliyet
10 Gigabit Ethernet 10 Gb/sn	100.000.000 / 10.000.000.000	1
Gigabit Ethernet 1Gb/sn	100.000.000 / 1.000.000.000	1
Fast Ethernet 100 Mb/sn	100.000.000 / 100.000.000	1
Ethernet 10 Mb/sn	100.000.000 / 10.000.000	10
Seri 1.544 Mb/sn	100.000.000 / 1.544.000	64
Seri 128 Kb/sn	100.000.000 / 128.000	781
Seri 64 Kb/sn	100.000.000 / 64.000	1562

OSPF ağlarında maliyet hesaplanırken tam sayılar kullanıldığı için referans bant genişliği 100 Mbps'den hızlı bağlantılarda sorunlara sebep olabilir. Bu sebeple 100 Mbps'den daha hızlı bağlantılarda, referans bant genişliği daha yüksek bir değer olarak ayarlanmalıdır. Referans bant genişliğini değiştirmek bağlantı kapasitesini etkilemez. Sadece metrik hesabı yapmak için kullanılır. Referans bant genişliğini değiştirmek için **auto-cost reference-bandwidth** komutu kullanılır. Gigabit Ethernet bağlantılarda komut, şu şekilde uygulanır:

Router(config)#**router ospf <ospf işlem numarası>**

Router(config-router)# **auto-cost reference-bandwidth 1000**

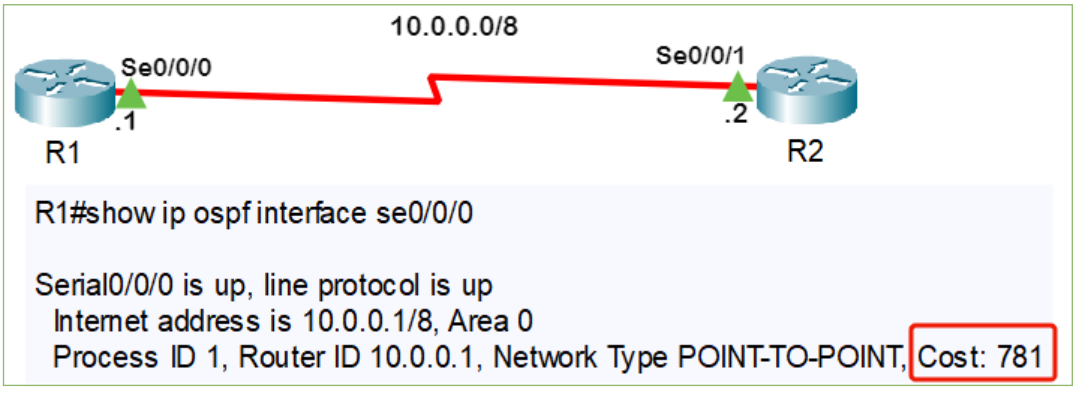
Arayüz bant genişliği ise **bandwidth [bant_genişliği]** komutu ile değiştirilir. Bant genişliği değeri **Kbps** olarak kabul edilir. Bir arayüzü varsayılan bant genişliğine döndürmek için **no bandwidth** komutu uygulanır. Gigabit Ethernet arayüzünün bant genişliğini 1 Gbps olarak değiştirmek ve bu değişikliği iptal etmek için uygulanan komutlar şunlardır:

Router(config)#**interface gigabitEthernet 0/1**

Router(config-if)# **bandwidth 1000000**

Router(config-if)# **no bandwidth**

Bir arayüzün maliyetini görüntülemek için **show ip ospf interface [arayüz]** komutu kullanılır. Görsel 2.73'te R1 yönlendiricinin se0/0/0 arayüzünün maliyeti görülür.



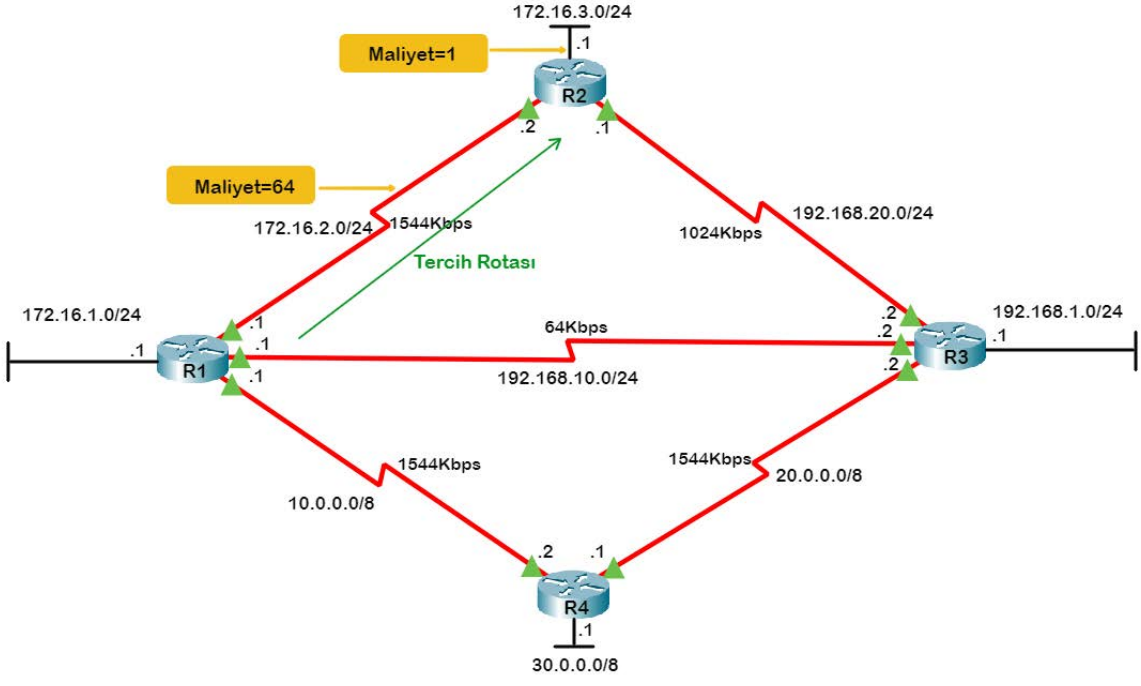
Görsel 2.73: Arayüz maliyetinin görüntülenmesi

ARAŞTIRMA OSPF Maliyeti

OSPF maliyetinin hesabının manuel olarak yapılandırılmasının sebebini araştırınız. Elde ettiğiniz bilgileri sınıfta arkadaşlarınızla paylaşınız.

NOT: Arayüz bant genişliği düşük olan rotanın OSPF maliyeti, bant genişliği yüksek olan rotaya göre daha yüksektir.

OSPF ağlarında maliyet hesabı yapılırken, kaynaktan hedefe giderken bir rotanın toplam maliyeti hesaplanır. Hedef ağa ulaşırken birden fazla rota olabilir. Maliyeti en düşük rota, öncelikli olarak tercih edilir. Maliyeti en düşük rotada cihazlardan biri başarısız olursa maliyet hesaplamasıyla ikinci en düşük maliyetli rota, yeni rota olarak belirlenir. Görsel 2.74'te R1, R2, R3 ve R4 yönlendiricilerinin bulunduğu ağda, bağlantı arayüzlerinin bant genişliği görülür. 172.16.1.0/24 ağı ile 172.16.3.0/24 ağının arasındaki en düşük maliyet, R1 ve R2 cihazlarının kullandığı yol olarak hesaplanır. İki yerel ağ arasındaki en düşük toplam maliyet, 65 olarak hesaplanır. Bu rota tercih rotası olarak belirlenir.



Görsel 2.74: En düşük maliyetli rotanın belirlenmesi

Görsel 2.75'te R1 cihazının yönlendirme bilgileri görülür.

```
R1#show ip route ospf
O    20.0.0.0 [110/128] via 10.0.0.1, 00:14:46, Serial0/1/0
O    30.0.0.0 [110/65] via 10.0.0.1, 00:08:23, Serial0/1/0
     172.16.0.0/16 is variably subnetted, 5 subnets, 2 masks
O       172.16.3.0 [110/65] via 172.16.2.2, 00:03:12, Serial0/0/0
O    192.168.1.0 [110/129] via 10.0.0.1, 00:08:03, Serial0/1/0
O    192.168.20.0 [110/161] via 172.16.2.2, 00:03:12, Serial0/0/0
```

Görsel 2.75: R1 cihazının yönlendirme bilgisi

Yönlendirme bilgilerinin açıklaması şöyledir:

O: OSPF ile yapılan yönlendirme bilgisidir.

172.16.3.0: Hedef ağ adres bilgisidir.

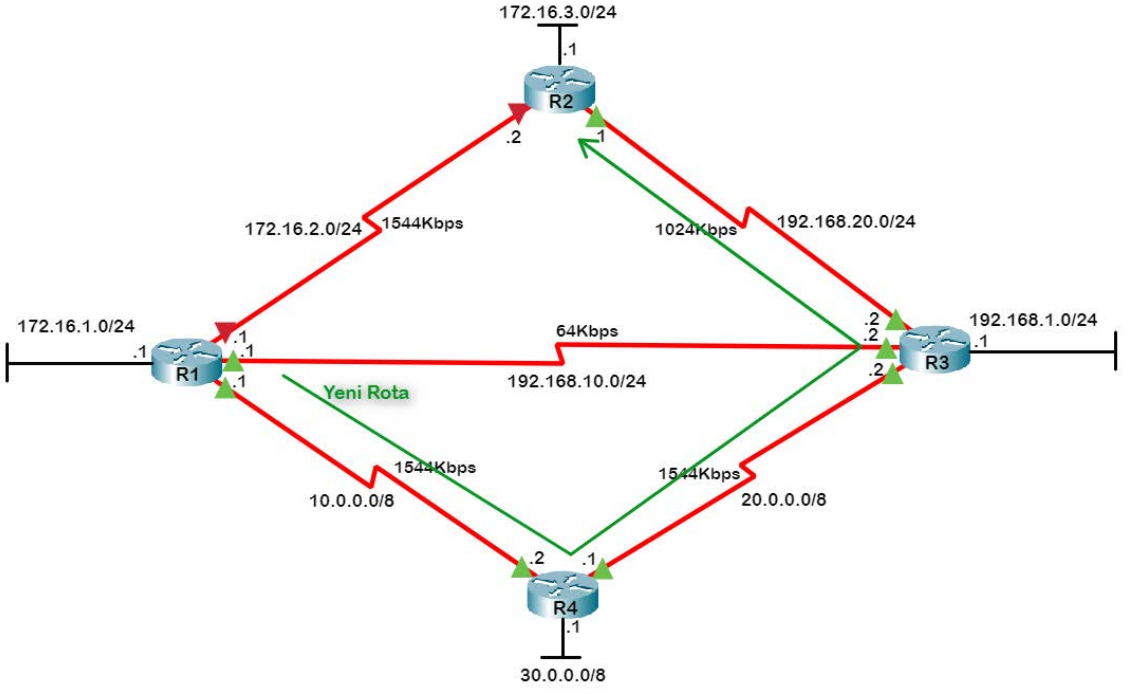
[110/65]: 110, OSPF'in yönetimsel değeri; 65, toplam maliyet değeridir.

via 172.16.2.2: Hedef ağa gitmek için sıçrama yapılacak cihazın adres bilgisidir.

00:03:12: Komşuluk kurulduğu andan itibaren geçen süredir.

Serial0/0/0: Hedef ağa gitmek için çıkış yapılan arayüz bilgisidir.

Görsel 2.76'da R2 cihazının serial0/0/1 arayüzü kapatıldığında 172.16.1.0/24 ile 172.16.3.0/24 ağları arasında en düşük maliyetli yeni rota bilgisi görülür.



Görsel 2.76: Yeni rota bilgisi

R1 cihazının yeni yönlendirme tablosu Görsel 2.77'de görülür. Yeni rotaya göre maliyet değeri 226 olan yol seçilmiştir.

```
R1#show ip route ospf
O    20.0.0.0 [110/128] via 10.0.0.1, 00:11:09, Serial0/1/0
O    30.0.0.0 [110/65] via 10.0.0.1, 00:04:46, Serial0/1/0
     172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
O       172.16.3.0 [110/226] via 10.0.0.1, 00:00:25, Serial0/1/0
O    192.168.1.0 [110/129] via 10.0.0.1, 00:04:26, Serial0/1/0
O    192.168.20.0 [110/225] via 10.0.0.1, 00:00:25, Serial0/1/0
```

Görsel 2.77: R1 cihazının yönlendirme tablosundaki OSPF rotalarının görüntülenmesi

OSPF ağlarında en iyi yol maliyetini manuel olarak hesaplamak için arayüzlerin bant genişliği **bandwidth** komutuyla değiştirilir. Bu yapılandırmanın aynı ağdaki her arayüz için aynı olması gerekir. Bir arayüzün maliyet değerini görüntülemek için **show ip ospf interface [arayüz]** komutu kullanılır. Görsel 2.78'de R1 cihazına ait arayüzlerin maliyet değerleri görülür.

```
R1#show ip ospf interface br
R1#show ip ospf interface brief
Interface     PID   Area                  IP Address/Mask      Cost  State  Nbrs
F/C
Gig0/0          1   0                   172.16.1.1/255.255.255.0   1       DR  0/0
Se0/0/0         1   0                   172.16.2.1/255.255.255.0   64    POINT  0/0
Se0/0/1         1   0                 192.168.10.1/255.255.255.0   1562  POINT  0/0
Se0/1/0         1   0                       10.0.0.1/255.0.0.0     64    POINT  0/0
```

Görsel 2.78: Arayüz maliyetinin görüntülenmesi

2.2.4.6. OSPF Ağlarında Yapılandırma

OSPF yapılandırması, yönlendirici cihazın komut arayüzünde yapılandırma modunda yapılır.

OSPF ile yönlendirmenin temel yapılandırması şu şekilde yapılır:

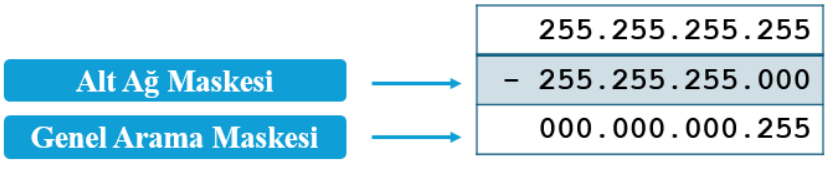
1. **OSPF'i Tanımlama:** Yönlendirici, global yapılandırma modundayken 1-65.535 arasında belirlenen OSPF işlem numarası ile OSPF tanımlanır. Komut şu şekildedir:

   Router(config)#router ospf <area-id>

2. **Yönlendirme Bölgesini Belirleme:** Yönlendirici, yapılandırma modundayken hangi arayüzlerin hangi alanlara dâhil edileceği belirlenir. Yönlendirme bölgesini belirleme komutu şu şekildedir:

   network [ağ_adresi] [genel arama maskesi] area [bölge_ID]

   OSPF, sınıfsız bir yönlendirme olduğu için genel arama maskesi her zaman kullanılır. Genel arama maskesiyle IP adreslerinin belirli kısımlarının eşleşmesi sağlanır. Genel arama maskesinde bit 0 ise adrese karşılık gelen bit değeriyle eşleşir, bit 1 ise adrese karşılık gelen bit değerini yok sayar. Genel arama maskesini hesaplamak için kolay metot, alt ağ maskesini 255.255.255.255'ten çıkarmaktır (Görsel 2.79).



Görsel 2.79: Genel arama maskesini hesaplama

3. **Arayüzleri OSPF'ye Ekleme:** Yönlendiricinin arayüzlerinin hangi OSPF alanına dâhil olduğunu belirleme işlemidir. OSPF mesajları tüm etkin arayüzlerden iletilir. Bu durum bant genişliğinin verimsiz kullanımına ve bazı güvenlik açıklarına sebep olur. Bu sebeple OSPF mesajlarının gerekli olmayan arayüzlerden iletilmesini önlemek için pasif arayüz yapılandırması yapılır. Arayüzleri OSPF'ye dâhil etmek için şu komutlar kullanılır:

   Router(config)#**interface [arayüz_ismi]**

   Router(config-if)#**ip ospf [OSPF_işlem_numarası] area [bölge_ID]**

   OSPF mesajlarının iletilmesi istenmeyen arayüzleri, pasif arayüz olarak yapılandırmak için şu komutlar kullanılır:

   Router(config)#**Router ospf [OSPF_işlem_numarası]**

   Router(config-router)#**Passive-interface [arayüz ismi]**

4. **Yönlendirici Kimliğini Belirleme:** Yönlendirici kimliği ile her yönlendirici benzersiz bir şekilde tanımlanır. Yönlendirici kimliğini manuel olarak belirlemek için şu komutlar kullanılır:

   Router(config)#**router ospf [OSPF_işlem_numarası]**

   Router(config-router)#**router-id [Router_ID]**

5. **Yönlendirici Öncelik Değerini Belirleme:** DR ve BDR cihaz seçimi için yönlendiricilerin öncelik değeri yapılandırılır. Öncelik değerini belirlemek için şu komutlar uygulanır:

   Router(config)#**interface [arayüz_ismi]**

   Router(config-if)#**ip ospf priority [değer]**

6. **OSPF Zamanlayıcı ve Hız Ayarlarını Yapılandırma:** OSPF veri paketlerinin gönderim hızının ve sıklığının ayarlanmasını sağlar. Zamanlayıcı ve hız ayarını belirlemek için şu komutlar uygulanır:

   Router(config)#**interface [arayüz_ismi]**

   Router(config-if)#**ip ospf hello-interval [saniye]**

   Router(config-if)#**ip ospf dead-interval [saniye]**

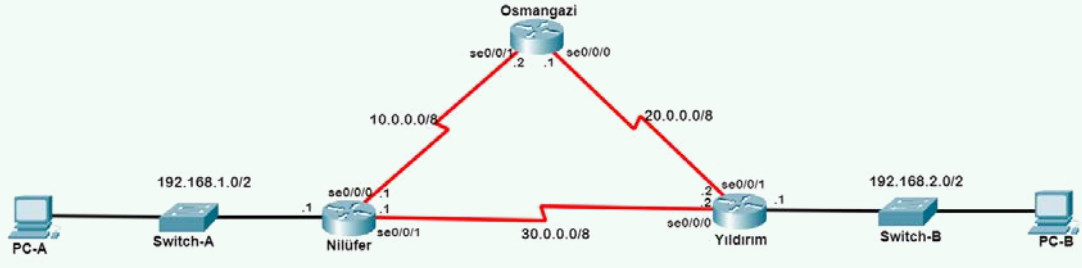
7. **Yapılandırmayı Kontrol Etme:** Yapılan değişiklikleri kaydettikten sonra komşuluk bilgilerini görüntülemek için **show ip ospf neighbor** komutu kullanılır. OSPF yapılandırması hakkında genel bilgi görüntülemek için **show ip ospf** komutu kullanılır. Bu komutlar yönlendiricinin yetkili modda uygulanır.

8. UYGULAMA

OSPF ile yönlendirme işlemini verilen adımlar doğrultusunda gerçekleştiriniz.

1. Adım: Ağ simülasyon programını çalıştırınız.

2. Adım: Görsel 2.80'deki ağ topolojisini hazırlayınız.



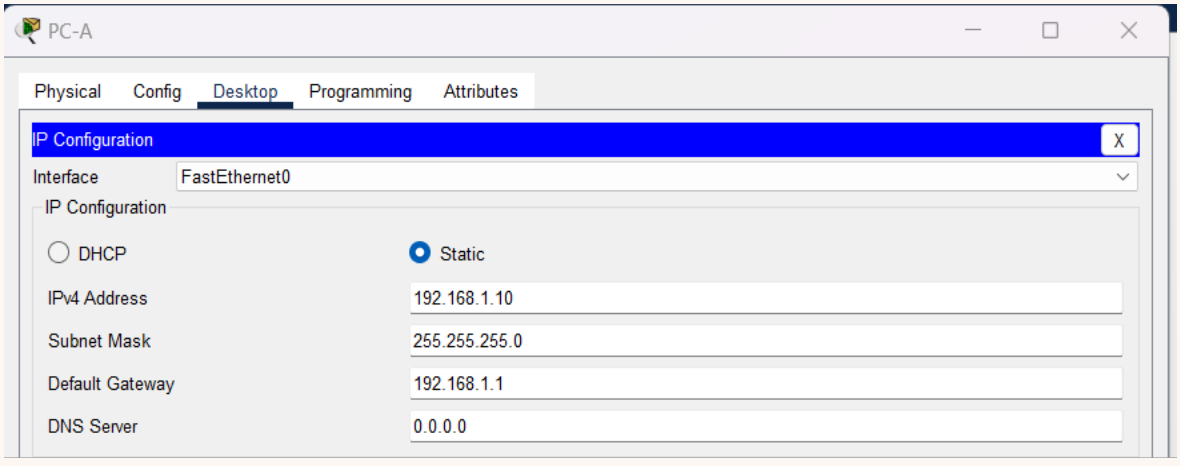
Görsel 2.80: 8. uygulamanın ağ topolojisi

3. Adım: Nilüfer isimli cihazın yapılandırma ayarları Görsel 2.81'de görülür. Siz de tüm yönlendiricileri yapılandırınız.

```
Nilufer(config)#interface serial0/0/0
Nilufer(config-if)#ip address 10.0.0.1 255.0.0.0
Nilufer(config-if)#no sh
Nilufer(config-if)#exit
Nilufer(config)#interface serial0/0/1
Nilufer(config-if)#ip address 30.0.0.1 255.0.0.0
Nilufer(config-if)#no sh
Nilufer(config-if)#exit
Nilufer(config)#interface gigabitethernet 0/1
Nilufer(config-if)#ip address 192.168.1.1 255.255.255.0
Nilufer(config-if)#no sh
Nilufer(config-if)#exit
```

Görsel 2.81: Nilüfer cihazının IP yapılandırması

4. Adım: PC-A cihazının yapılandırması Görsel 2.82'de görülür. Siz de PC-B cihazını yapılandırınız.



Görsel 2.82: PC-A IP yapılandırması

5. Adım: Nilüfer isimli cihazın OSPF ile yapılandırması Görsel 2.83'te görülür. Siz de tüm yönlendiricilerde OSPF yapılandırmasını tamamlayınız.

```
Nilufer(config)#router ospf 1
Nilufer(config-router)#network 10.0.0.0 0.255.255.255 area 0
Nilufer(config-router)#network 20.0.0.0 0.255.255.255 area 0
Nilufer(config-router)#network 192.168.1.0 0.0.0.255 area 0
Nilufer(config-router)#exit
Nilufer(config)#
```

Görsel 2.83: OSPF yapılandırması

6. Adım: Nilüfer isimli cihazın komşu tablosu Görsel 2.84'te görülür. Siz de diğer cihazların komşu tablolarını görüntüleyiniz.

```
Nilufer#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
192.168.2.1       0   FULL/  -        00:00:34    30.0.0.2        Serial0/0/1
20.0.0.1          0   FULL/  -        00:00:31    10.0.0.2        Serial0/0/0
Nilufer#
```

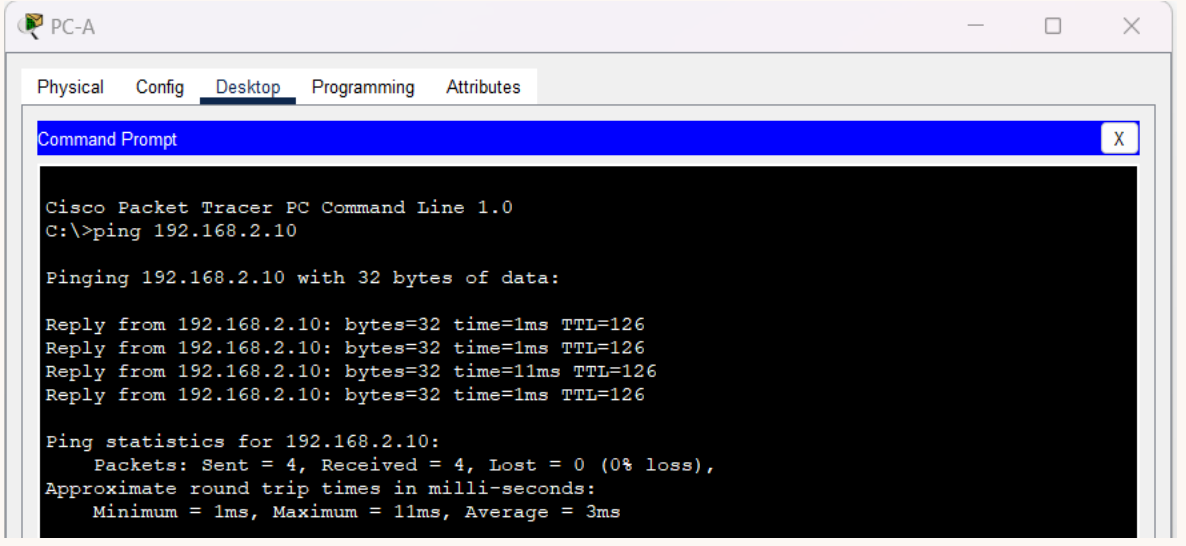
Görsel 2.84: Komşu tablosunun görüntülenmesi

7. Adım: Nilüfer isimli cihazın yönlendirme tablosu Görsel 2.85'te görülür. Siz de cihazların yönlendirme tablolarını görüntüleyiniz.

```
Nilufer#show ip route ospf
O    20.0.0.0 [110/128] via 30.0.0.2, 00:15:43, Serial0/0/1
              [110/128] via 10.0.0.2, 00:15:43, Serial0/0/0
O    192.168.2.0 [110/65] via 30.0.0.2, 00:15:18, Serial0/0/1
```

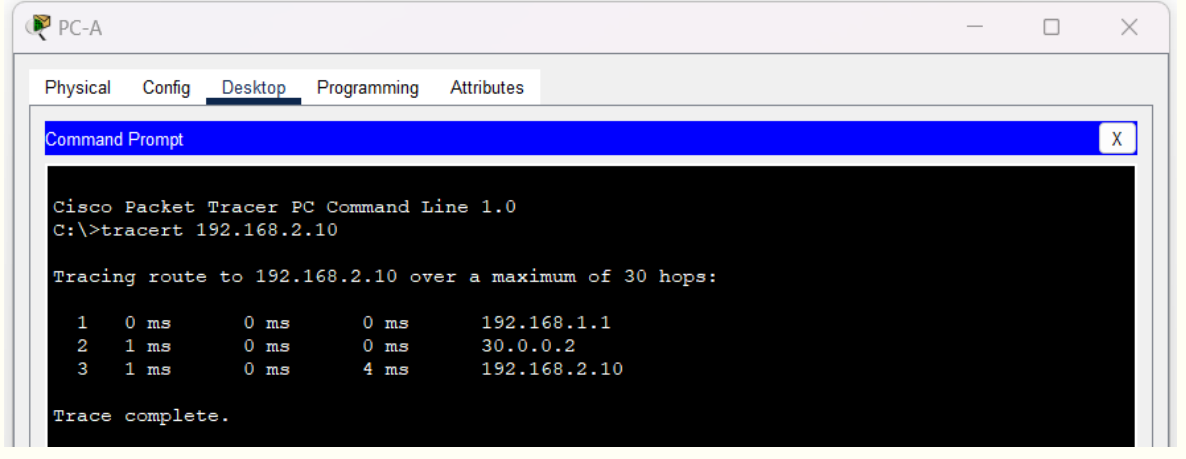
Görsel 2.85: Yönlendirme tablosunda OSPF rotalarının görüntülenmesi

8. Adım: PC-A ve PC-B cihazları arasındaki iletişimi **ping** komutuyla test ediniz (Görsel 2.86).



Görsel 2.86: PC-A ve PC-B bilgisayarları arasındaki iletişimin test edilmesi

9. Adım: PC-A'dan PC-B'ye rota görüntüleme işlemini **tracert** komutu ile yapınız (Görsel 2.87).



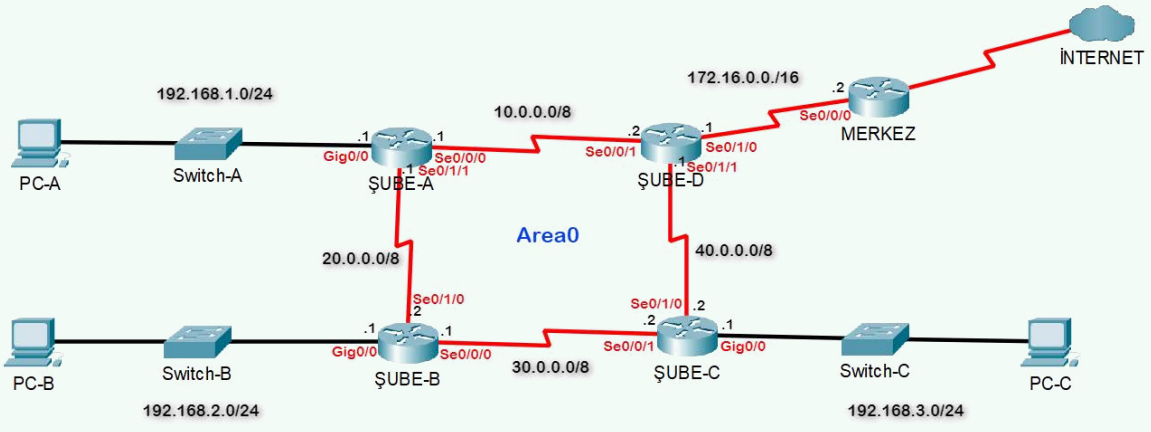
Görsel 2.87: tracert komutu ile rota görüntüleme

9. UYGULAMA

Varsayılan rotayı OSPF ile diğer yönlendiricinin öğrenmesini sağlama işlemini verilen adımlar doğrultusunda gerçekleştiriniz.

1. Adım: Ağ simülasyon programını çalıştırınız.

2. Adım: Görsel 2.88'deki ağ topolojisini hazırlayınız.



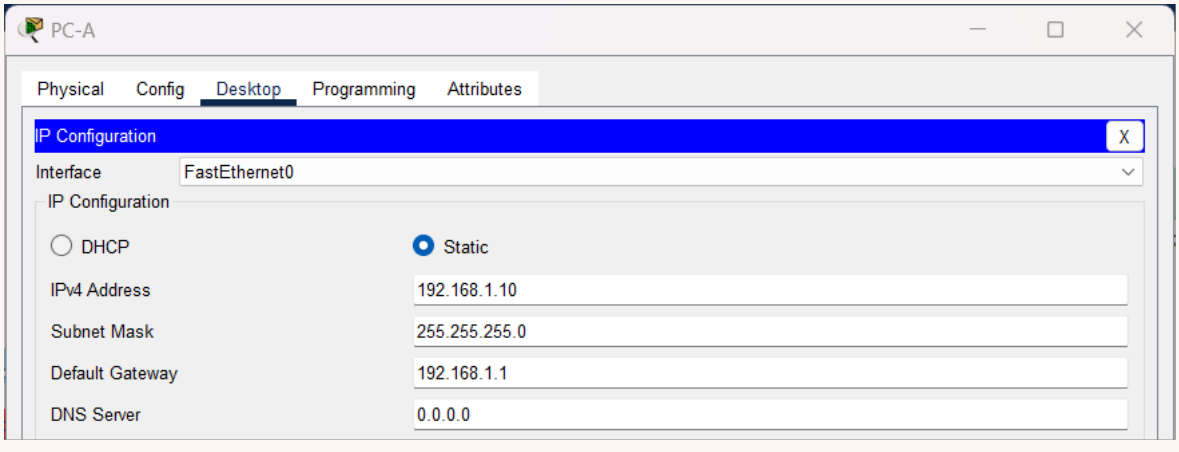
Görsel 2.88: 9. uygulamanın ağ topolojisi

3. Adım: ŞUBE-D yönlendiricisinin arayüz yapılandırması Görsel 2.89'da görülür. Siz de ağdaki tüm yönlendiricilerin yapılandırmasını yapınız.

```
SUBE-D(config)#interface se0/0/1
SUBE-D(config-if)#ip address 10.0.0.2 255.0.0.0
SUBE-D(config-if)#exit
SUBE-D(config)#interface se0/1/1
SUBE-D(config-if)#ip address 40.0.0.1 255.0.0.0
SUBE-D(config-if)#exit
SUBE-D(config)#interface se0/1/0
SUBE-D(config-if)#ip address 172.16.0.1 255.255.0.0
SUBE-D(config-if)#exit
```

Görsel 2.89: ŞUBE-D yönlendiricisinin IP yapılandırması

4. Adım: PC-A bilgisayarının yapılandırması Görsel 2.90'da görülür. Siz de ağdaki diğer bilgisayarların yapılandırmasını yapınız.



Görsel 2.90: PC-A cihazının IP yapılandırması

5. Adım: ŞUBE-D yönlendiricisinde se0/1/0 arayüzünde varsayılan rotayı yapılandırınız (Görsel 2.91).

```
SUBE-D(config)#
SUBE-D(config)#ip route 0.0.0.0 0.0.0.0 se0/1/0
SUBE-D(config)#
```

Görsel 2.91: ŞUBE-D yönlendiricisinde statik rota tanımlama

6. Adım: ŞUBE-D yönlendiricisindeki OSPF yapılandırması Görsel 2.92'de görülür. Siz de ağdaki diğer yönlendiricilerin OSPF yapılandırmasını yapınız.

```
SUBE-D(config)#router ospf 10
SUBE-D(config-router)#network 10.0.0.0 0.255.255.255 area 0
SUBE-D(config-router)#network 40.0.0.0 0.255.255.255 area 0
SUBE-D(config-router)#network 172.16.0.0 0.0.255.255 area 0
SUBE-D(config-router)#exit
```

Görsel 2.92: ŞUBE-D yönlendiricisinin OSPF yapılandırması

7. Adım: ŞUBE-D yönlendiricisindeki varsayılan rotanın diğer yönlendiricilere öğretilmesini **default-information originate** komutu ile sağlayınız (Görsel 2.93).

```
SUBE-D(config)#router ospf 10
SUBE-D(config-router)#default-information originate
SUBE-D(config-router)#
```

Görsel 2.93: Varsayılan rotanın öğretilmesi

8. Adım: PC-A'dan PC-C'ye iletişimi **ping** komutu ile test ediniz (Görsel 2.94).

```
C:\>ping 192.168.3.10

Pinging 192.168.3.10 with 32 bytes of data:

Reply from 192.168.3.10: bytes=32 time=2ms TTL=125
Reply from 192.168.3.10: bytes=32 time=2ms TTL=125
Reply from 192.168.3.10: bytes=32 time=2ms TTL=125
Reply from 192.168.3.10: bytes=32 time=18ms TTL=125

Ping statistics for 192.168.3.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 18ms, Average = 6ms
```

Görsel 2.94: PC-A ve PC-D bilgisayarları arasındaki iletişimin test edilmesi

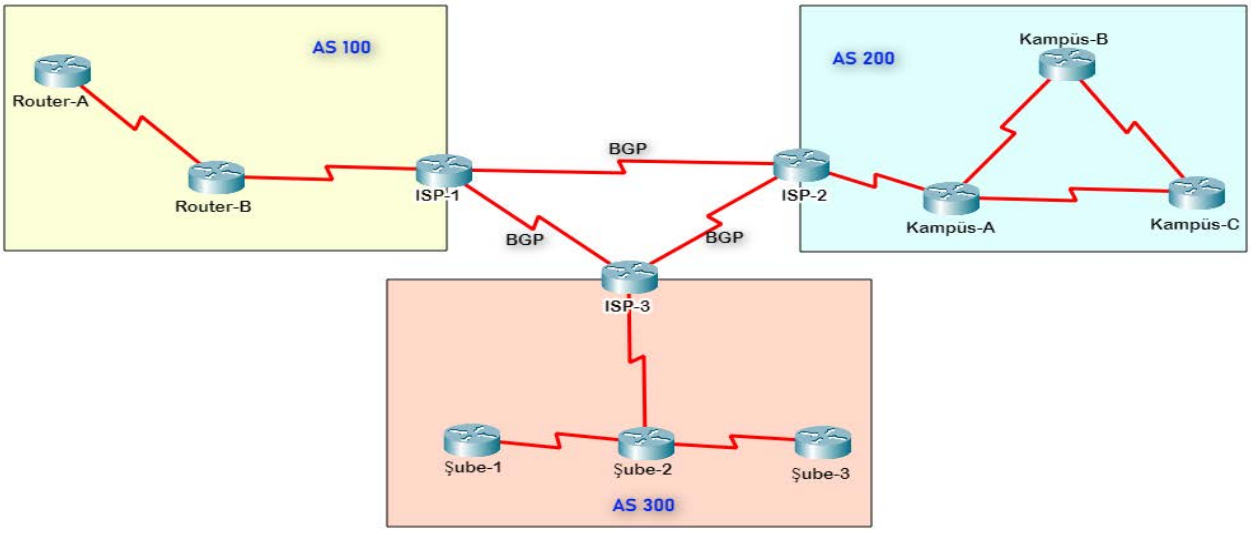
9. Adım: ŞUBE-B cihazınında yönlendirme tablosunda OSPF rotalarını görüntüleyiniz (Görsel 2.95).

```
Router#show ip route ospf
O     10.0.0.0 [110/128] via 20.0.0.1, 00:22:07, Serial0/1/0
O     40.0.0.0 [110/128] via 30.0.0.2, 00:21:57, Serial0/0/0
O     192.168.1.0 [110/65] via 20.0.0.1, 00:22:07, Serial0/1/0
O     192.168.3.0 [110/65] via 30.0.0.2, 00:21:57, Serial0/0/0
O*E2 0.0.0.0/0 [110/1] via 30.0.0.2, 00:21:57, Serial0/0/0
O*E2 0.0.0.0/0 [110/1] via 20.0.0.1, 00:21:57, Serial0/1/0
```

Görsel 2.95: Yönlendirme tablosunda OSPF rotalarının görüntülenmesi

2.2.5. BGP

BGP (Border Gateway Protocol), internet servis sağlayıcıları tarafından kullanılan ve farklı otonom sistem numarasına sahip ağlar arasında yönlendirme yapan sınır ağ geçidi protokolüdür. İnternetin temel yapısını oluşturan otonom sistemler arasında yaygın olarak kullanılır. **Otonom sistemler**, tek bir elden yönetilen büyük ağlar topluluğudur. Her sistem kendi yönlendirme kurallarına sahiptir. Otonom numaraları, 1-65.535 arasındaki bir sayı değeriyle ifade edilir. 0 ve 65.535 numaraları rezerve olarak ayrılmıştır. 1-64.495 arasındaki sayılar genel otonom sistem numaralarıdır. 64.496-64.511 dokümantasyonda kullanılmak üzere ayrılmıştır. 64.512-65.534 ise özel otonom sistem numaralarıdır. BGP protokolü ise bu otonom sistemlerin birbirini tanımasını ve yönlendirme bilgilerinin paylaşılmasını sağlar. BGP, diğer protokollerden farklı olarak durum bilgisi paylaşmaz. Sınır geçidi olarak adlandırılan ağ cihazlarının diğer yönlendiricilerden aldığı güncel bilgiye göre yönlendirme kararı vermesini sağlar. Görsel 2.96'da farklı otonom numaralarına sahip ağların internet servis sağlayıcısı üzerinden BGP ile yönlendirilmesi görülür.



Görsel 2.96: BGP protokolü

BGP'nin özellikleri şunlardır:

- 1 ile 65.535 arasında otonom sistem numarası kullanır.
- Hedefe giderken üzerinden geçilen otonom sistem sayısına göre metrik hesaplama yapar.
- CIDR'yi destekler.
- TCP protokolü ile iletişim sağlanır. Kimlik doğrulama TCP seviyesinde yapıldığı için BGP kimlik doğrulamaya ihtiyaç duymaz.
- MD5 algoritması ile kimlik doğrulama yapılarak BGP eşleri arasındaki TCP oturumunun güvenliği sağlanır.
- Komşuluk mesajları 60 saniye aralıklarla kontrol edilir.
- Yönetimsel uzaklık değeri; aynı otonom sistemler arasında 200, farklı otonom sistemler arasında 20'dir.
- Farklı otonom sistemlerdeki yönlendiriciler, EBGP (Dış Sınır Ağ Geçidi Protokolü); aynı otonom sisteminin içindeki yönlendiriciler, IBGP (İç Sınır Ağ Geçidi Protokolü) kullanır.

2.2.5.1. BGP Mesaj Türleri

BGP sistemlerde komşu yönlendiriciler arasında bilgi alışverişi mesaj paketleri ile sağlanır. BGP mesaj paketleri şunlardır:

OPEN: Komşuluk kurulumunda BGP oturumunu başlatmak için kullanılan paketlerdir. Bu mesaj paketinde versiyon bilgisi, otonom sistem numarası, yönlendirici kimliği, oturum süresi gibi bilgiler yer alır.

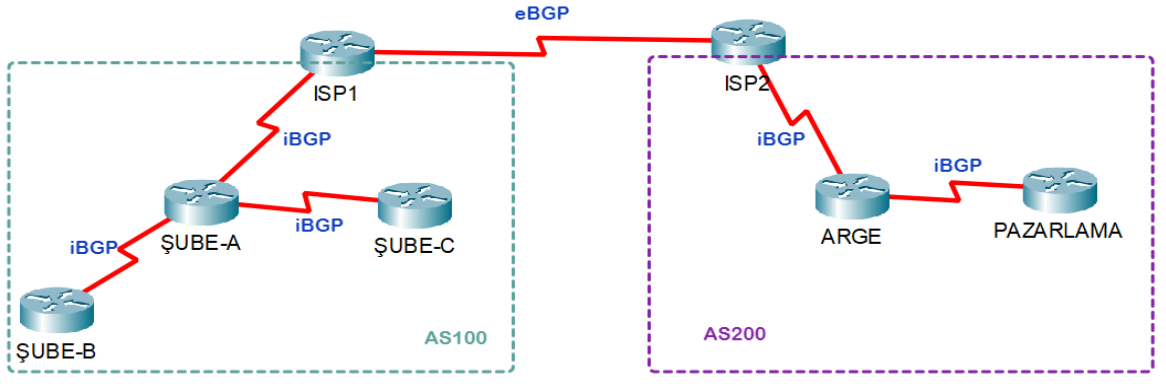
KEEPALIVE: BGP oturumunun aktif olarak devam etmesini sağlar.

UPDATE: Yönlendiriciler arasındaki yönlendirme bilgilerinin güncellenmesini sağlar. Güncelleme mesajları ile yeni rotaların eklenmesi veya mevcut rotanın silinmesi gibi işlemler sağlanır.

NOTIFICATION: BGP, oturumlar arasında hata tespit edildiğinde oturumun kapatılmasını sağlar.

2.2.5.2. BGP'de Komşuluk

Komşuluk, BGP sistemlerde yer alan cihazların TCP bağlantısı ile iletişim kurması ve birbirini tanıması sürecidir. BGP sistemlerde de cihazların bulunduğu konuma göre **iBGP (interior Border Gateway)** ve **eBGP (exterior Border Gateway)** olmak üzere iki farklı komşuluk türü vardır. iBGP, aynı otonom sistemlerdeki cihazlar arasında; eBGP, farklı otonom sistemlerdeki cihazlar arasında kurulan komşuluğu ifade eder. Görsel 2.97'de BGP komşuluk türleri görülür.



Görsel 2.97: BGP'de komşuluk türleri

BGP iletişiminde komşuluk durumları şu şekildedir:

Idle State (Boşta Durumu): BGP'nin ilk çalışmaya başlama aşamasıdır. TCP bağlantısı sağlanması için beklenir. TCP oturumu kurulamadığı durumlarda BGP başarısız olur ve **idle** durumuna geçilir.

Connect State (Bağlantı Durumu): Komşu yönlendirici ile TCP bağlantısının tam olarak sağlandığı durumdur. Üçlü el sıkışma olarak bilinen **three-way-handshake** ile TCP oturumu başlatılır ve **OpenSent State** durumuna geçilir. TCP bağlantısı sağlanamazsa yine idlle durumuna geçer.

Active State (Aktif Durum): Komşu yönlendirici ile TCP bağlantısının sağlanamadığı ve bağlantının kurulmaya çalışıldığı aşamadır. Bağlantı sağlanırsa OpenSent, sağlanamazsa **idle** durumuna geçer.

OpenSent State (Açık Gönderim Durumu): Komşu yönlendiriciden Open mesajı alınır ve doğruluğu kontrol edilir. Paket doğrulanırsa **KeepAlive**, doğrulanmazsa **Notification** mesajı gönderilir.

OpenConfirm State (Açık Onay Durumu): Komşu yönlendiriciden Keepalive mesajının beklendiği durumdur. Mesaj alınırsa **Established** durumuna geçer. Mesaj alınamazsa yine **idle** durumuna geçer.

Established State (Bağlantı Kuruldu Durumu): BGP komşuluğu başarılı bir şekilde sağlanmıştır. Yönlendiriciler arasında bilgi alışverişi devam eder.

BGP komşuluk süreci tamamlandığında komşuluk özet bilgisi **show ip bgp summary** komutu ile görüntülenir. Komşuluk özet bilgisi, Görsel 2.98'de görülür. Bu özette; BGP yönlendiricisi olan R1'in ID'si, otonom sistem numarası, yönlendirme tablosunda bulunan toplam yol sayısı ve kullanılan bellek miktarı bilgileri yer alır. Komşu 10.10.10.1 ile BGP oturumu kurulurken gönderilen ve alınan mesaj sayısı ve komşuluk kurulumundan sonra geçen süre bilgisi de gösterilir.

```
R1#show ip bgp summary
BGP router identifier 1.1.1.1, local AS number 20
BGP table version is 6, main routing table version 6
5 network entries using 660 bytes of memory
5 path entries using 260 bytes of memory
3/2 BGP path/bestpath attribute entries using 460 bytes of memory
3 BGP AS-PATH entries using 72 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
Bitfield cache entries: current 1 (at peak 1) using 32 bytes of memory
BGP using 1484 total bytes of memory
BGP activity 4/0 prefixes, 5/0 paths, scan interval 60 secs

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
10.10.10.1      4    35       9       4        6    0    0 00:02:52        4
```

Görsel 2.98: Komşuluk özet bilgisinin görüntülenmesi

Kurulan komşuluk hakkında bilgi almak için **show ip bgp neighbors** komutu kullanılır. Görsel 2.99'da bu komutun kullanımı görülür.

```
R1#show ip bgp neighbors
BGP neighbor is 10.10.10.1,  remote AS 35, external link
  BGP version 4, remote router ID 3.3.3.3
  BGP state = Established, up for 00:00:51
  Last read 00:00:51, last write 00:00:51, hold time is 180, keepalive interval is 60
seconds
  Neighbor capabilities:
    Route refresh: advertised and received(new)
    Address family IPv4 Unicast: advertised and received
  Message statistics:
    InQ depth is 0
    OutQ depth is 0

                         Sent       Rcvd
    Opens:                  1          1
    Notifications:          0          0
    Updates:                3          6
    Keepalives:             1          1
    Route Refresh:          0          3
    Total:                  5         11
  Default minimum time between advertisements runs is 30 seconds
```

Görsel 2.99: Komşuluk bilgisinin görüntülenmesi

BGP yönlendirme tablosunu görüntülemek için **show ip bgp** komutu kullanılır. Bu komut hedef ağlara ulaşmak için kullanılan yolları ve detaylarını gösterir. Aynı zamanda metrikler hakkında detaylı bilgi içerir. Görsel 2.100'de komutun kullanımı görülür.

```
R1#show ip bgp
BGP table version is 6, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 10.10.10.0/30    0.0.0.0                  0      0 32768 i
*                   10.10.10.1               0      0      0 35 i
*> 20.20.20.0/30    10.10.10.1               0      0      0 35 i
*> 192.168.2.0/24   10.10.10.1               0      0      0 35 50 i
*> 192.168.10.0/24  0.0.0.0                  0      0 32768 i
```

Görsel 2.100: BGP yönlendirme tablosunun görüntülenmesi

Yönlendirme tablosunda yer alan yönlendirme metrikleri şunlardır:

Network: BGP ile yönlendirmeye dâhil olan ağların bilgisini gösterir.

Next Hop: Hedef ağa giderken bir sonraki sıçrama yapılacak olan arayüz adresini gösterir.

Metric: Yolun tercih sırasını belirtir. Rota metrik değeri BGP'de genellikle 0'dır.

LocPrf: Rotaların tercih sırasını belirtir. LocPrf değeri yüksek olan rotanın tercih edilme olasılığı daha yüksektir.

Weight: Yerel yönlendiricilere özgü ağırlık değeridir. Ağırlık değeri yüksek olan rotalar yüksek önceliğe sahiptir.

Path: BGP rotalarının üzerinden geçtiği otonom sistem numaralarını gösterir.

Status: Bir rotanın geçerli ve en iyi yol olup olmadığının bilgisini gösterir. * geçerli, > en iyi yol anlamına gelir.

2.2.5.3. BGP Karar Verme Süreci

BGP'de bir yönlendiricinin bir rotayı tercih etmesi sürecinde bazı işlem adımları takip edilir. Hedef ağa giderken kullanılabilecek rotaların kalitesi ve uygunluğuna göre en iyi yol seçimi yapılır. Karar verme süreci adımları şunlardır:

- Yeni yönlendirme bilgilerinin alınması ve BGP tablosuna eklenmesi
- Yeni alınan rotaların geçerli/geçersiz olarak yönlendirme tablosuna eklenmesi ve güncellenmesi
- En iyi rotanın seçimi
- En iyi rotanın yönlendirme tablosuna eklenmesi
- Yeni rotaların komşulara iletilmesi

2.2.5.4. BGP Yapılandırma Ayarları

BGP yapılandırmasıyla yönlendiriciler arasında bilgi paylaşımı sağlanır. Yönlendiricilerin bulunduğu konuma göre iBGP veya eBGP yapılandırılması yapılır. BGP farklı otonom sistemler arasında yönlendirme

yapar. Bu sebeple aynı sistemdeki yönlendiricilerin aynı otonom sistem numarası ile yapılandırılması gerekir. BGP yapılandırmasında komşuluk tanımlanır ve yönlendirme bilgileri iletilir. BGP yapılandırmasında kullanılan komutlar şunlardır:

Router(config)#**router bgp [otonom_sistem_numarası]**

Router(config-router)#**bgp router-id [router_ID]**

Router(config-router)# **neighbor [komşu_IP] remote-as [komşu_otonom_sistem_numarası]**

Router(config-router)#**network [network_id] mask [alt_ağ_maskesi]**

Router(config-router)#**redistribute connected**

Otonom sistemler içinde OSPF, EIGRP gibi farklı yönlendirme protokolleri kullanıldığı zaman protokoller arasında rotaların dâhil edilmesi gerekir. Bunun için kullanılan komut şudur:

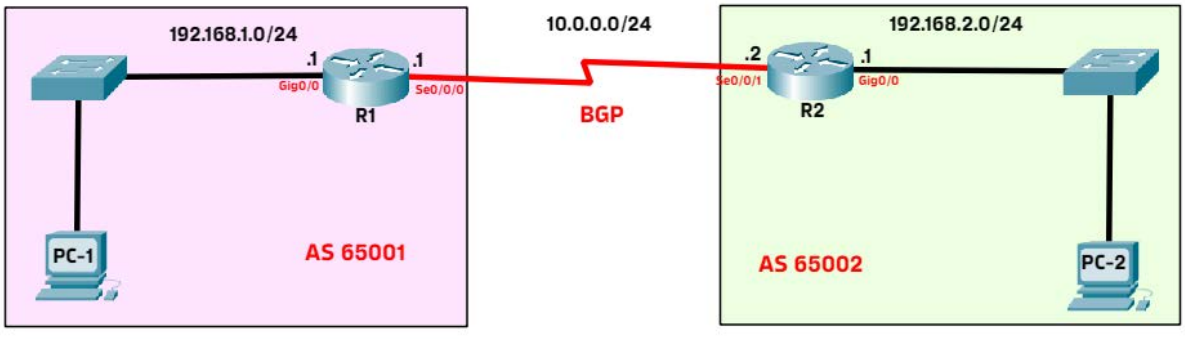
Router(config)#**redistribute [protocol] [process_id]**

Örneğin otonom sistem numarası 65001 olan BGP ağına OSPF ile öğrenilen rotaları dâhil etmek için şu komutlar uygulanır:

Router(config-router)#**router bgp 65001**

Router(config-router)#**redistribute ospf 1**

Görsel 2.101'de otonom sistem numaraları 65001 ve 65002 olan ağlar görülür.



Görsel 2.101: BGP ile yönlendirme

BGP yapılandırması için R1 ve R2 cihazlarında şu komutlar uygulanır:

R1(config)#router bgp 65001

R1(config-router)#bgp router-id 1.1.1.1

R1(config-router)#neighbor 10.0.0.2 remote-as 65002

R1(config-router)#network 10.0.0.0 mask 0.0.0.255

R1(config-router)#network 192.168.1.0 mask 0.0.0.255

R1(config-router)#redisribute connected

```
R2(config)#router bgp 65002
R2(config-router)#bgp router-id 2.2.2.2
R2(config-router)#neighbor 10.0.0.1 remote-as 65001
R2(config-router)#network 10.0.0.0 mask 0.0.0.255
R2(config-router)#network 192.168.2.0 mask 0.0.0.255
R2(config-router)#redisribute connected
```

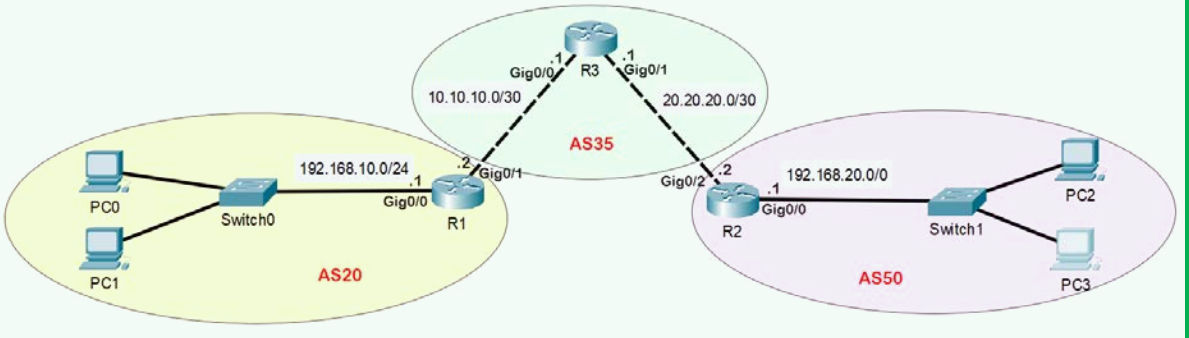
Bu komutlar uygulandığı zaman komşuluk kurulur ve bildirim olarak gözükür.

10. UYGULAMA

Farklı otonom sistem numarasına sahip ağları BGP ile yapılandırma işlemini verilen adımlar doğrultusunda gerçekleştiriniz.

1. Adım: Ağ simülasyon programını çalıştırınız.

2. Adım: Görsel 2.102'deki ağ topolojisini hazırlayınız.



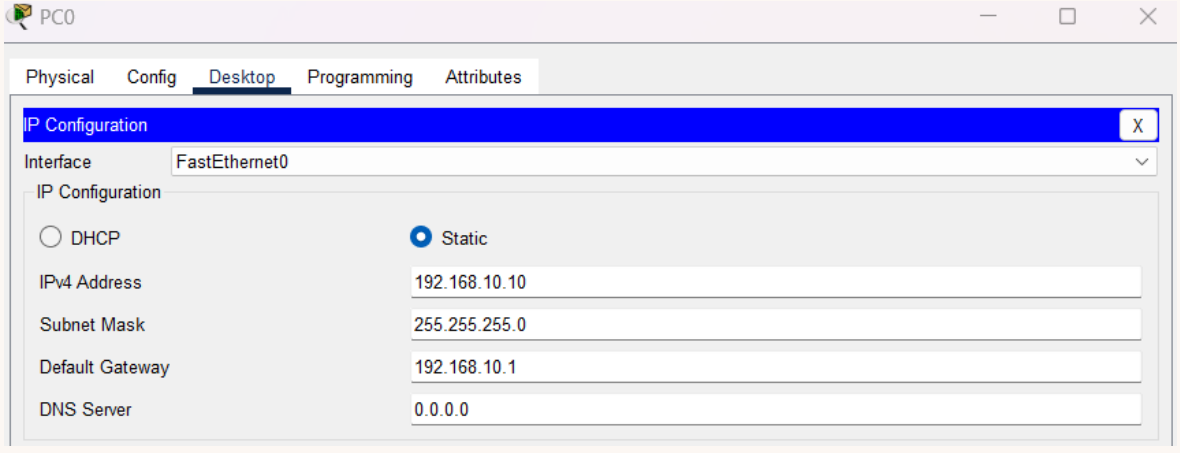
Görsel 2.102: 10. uygulamanın ağ topolojisi

3. Adım: R1 yönlendiricisinin arayüz yapılandırması Görsel 2.103'te görülür. Siz de ağdaki diğer yönlendiricilerin yapılandırmalarını tamamlayınız.

```
R1(config)#int gig0/0
R1(config-if)#ip address 192.168.10.1 255.255.255.0
R1(config-if)#no sh
R1(config-if)#exit
R1(config)#int gig0/1
R1(config-if)#ip address 10.10.10.2 255.255.255.252
R1(config-if)#no sh
R1(config-if)#exit
```

Görsel 2.103: R1 yönlendiricinin arayüz yapılandırması

4. Adım: PC0 bilgisayarının yapılandırması Görsel 2.104'te görülür. Siz de ağdaki diğer bilgisayarların yapılandırmalarını tamamlayınız.



Görsel 2.104: PC0'ın IP yapılandırması

5. Adım: R1 yönlendiricisinin BGP yapılandırması Görsel 2.105'te görülür. Siz de ağdaki diğer yönlendiricilerin BGP yapılandırmalarını tamamlayınız.

```
R1(config)#router bgp 20
R1(config-router)#bgp router-id 1.1.1.1
R1(config-router)#neighbor 10.10.10.1 remote-as 35
R1(config-router)#network 10.10.10.0 mask 255.255.255.252
R1(config-router)#network 192.168.10.0 mask 255.255.255.0
R1(config-router)#do wr
Building configuration...
[OK]
```

Görsel 2.105: R1 BGP yapılandırması

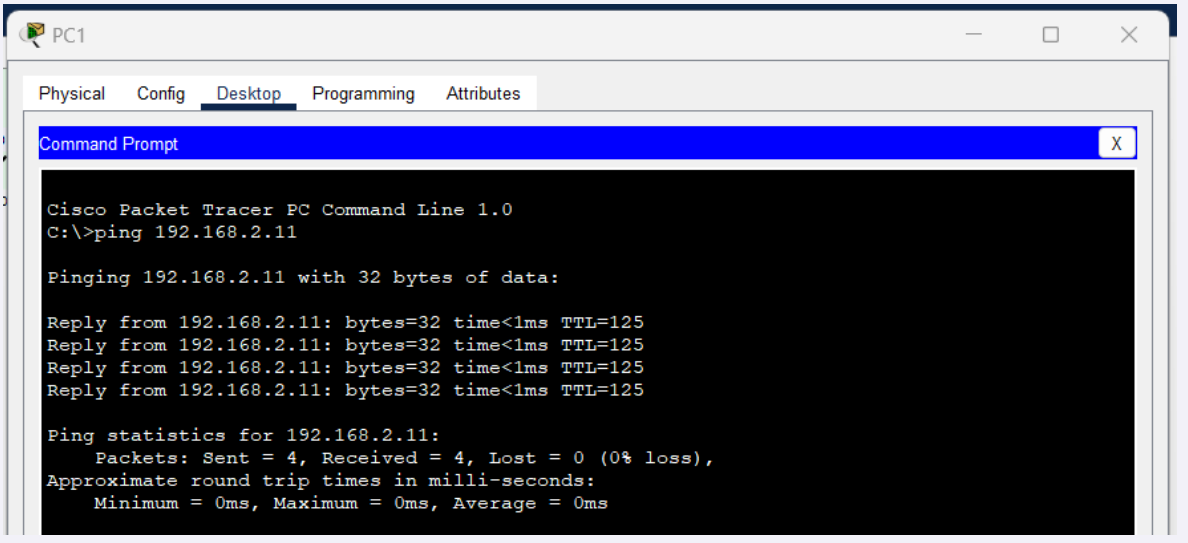
6. Adım: R1 yönlendiricinin BGP yönlendirme bilgisi Görsel 2.106'da görülür. Siz de ağdaki diğer yönlendiricilerin BGP yönlendirme bilgilerini görüntüleyiniz.

```
R1#show ip bgp
BGP table version is 10, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 10.10.10.0/30    0.0.0.0                  0      0 32768 i
*                   10.10.10.1               0      0      0 35 i
*> 20.20.20.0/30    10.10.10.1               0      0      0 35 50 i
*> 192.168.2.0/24   10.10.10.1               0      0      0 35 50 i
*> 192.168.10.0/24  0.0.0.0                  0      0 32768 i
```

Görsel 2.106: BGP yönlendirme tablosunun görüntülenmesi

7. Adım: PC1'den PC4'e iletişimi **ping** komutu ile test ediniz (Görsel 2.107).



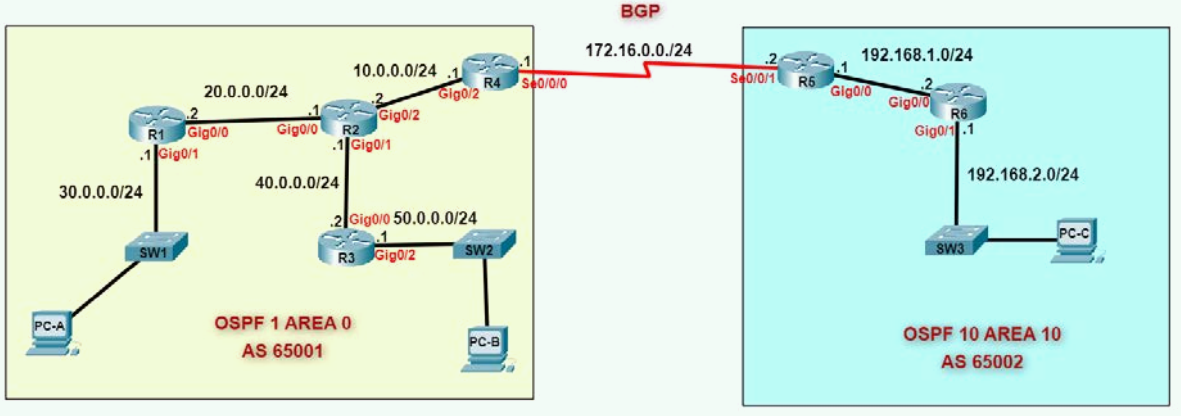
Görsel 2.107: PC1 ve PC4 bilgisayarları arasındaki iletişimin test edilmesi

11. UYGULAMA

İki farklı OSPF alanını BGP ile yönlendirme işlemini verilen adımlar doğrultusunda gerçekleştiriniz.

1. Adım: Ağ simülasyon programını çalıştırınız.

2. Adım: Görsel 2.108'deki ağ topolojisini hazırlayınız.



Görsel 2.108: 11. uygulamanın ağ topolojisi

3. Adım: R4 cihazının arayüz yapılandırmaları Görsel 2.109'da görülür. Siz de diğer yönlendiricilerin arayüz yapılandırmalarını tamamlayınız.

```
R4(config)#interface gig0/2
R4(config-if)#ip address 10.0.0.1 255.255.255.0
R4(config-if)#no sh
R4(config-if)#interface se0/0/0
R4(config-if)#ip address 172.16.0.1 255.255.255.0
R4(config-if)#no sh
R4(config-if)#exit
```

Görsel 2.109: R4 yönlendiricisinin IP yapılandırması

4. Adım: R4 cihazında uygulanan OSPF yapılandırması Görsel 2.110'da görülür. Siz de OSPF işlem numaraları ve alan numaralarını dikkate alarak tüm yönlendiricilerde OSPF yapılandırmasını gerçekleştiriniz.

```
R4(config)#router ospf 1
R4(config-router)#network 172.16.0.0 0.0.0.255 area 0
R4(config-router)#network 10.0.0.0 0.0.0.255 area 0
R4(config-router)#
```

Görsel 2.110: R4 yönlendiricisinde OSPF tanımı

5. Adım: R4 cihazında uygulanan BGP yapılandırması Görsel 2.111'de görülür. Siz de R5 cihazında BGP yapılandırmasını gerçekleştiriniz.

```
R4(config)#router bgp 65001
R4(config-router)#neighbor 172.16.0.2 remote-as 65002
R4(config-router)#neighbor 172.16.0.2 next-hop-self
R4(config-router)#
```

Görsel 2.111: R4 yönlendiricisinde BGP yapılandırması

6. Adım: R4 cihazında OSPF ve BGP rotalarının yeniden dağıtılmasını sağlayınız (Görsel 2.112).

```
R4(config)#router ospf 1
R4(config-router)#redistribute bgp 65001 subnets
R4(config-router)#exit
R4(config)#
R4(config)#router bgp 65001
R4(config-router)#redistribute ospf 1
R4(config-router)#exit
```

Görsel 2.112: R4 yönlendiricisinde OSPF ve BGP rotalarının dağıtılması

7. Adım: R5 cihazında OSPF ve BGP rotalarının yeniden dağıtılmasını sağlayınız (Görsel 2.113).

```
R5(config)#router ospf 10
R5(config-router)#redistribute bgp 65002 subnets
R5(config-router)#exit
R5(config)#router bgp 65002
R5(config-router)#router ospf 10
R5(config-router)#exit
```

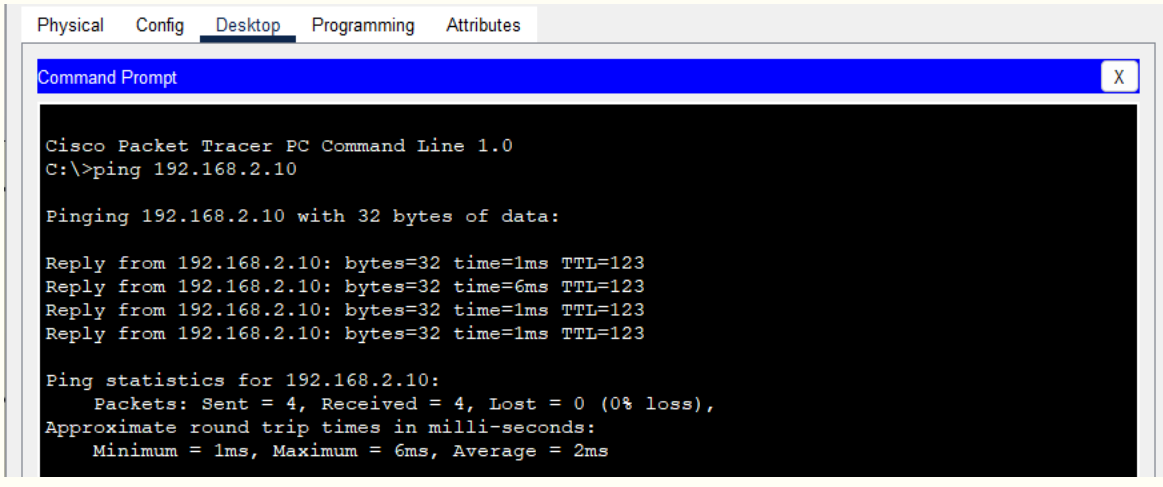
Görsel 2.113: R5 yönlendiricisinde OSPF ve BGP rotalarının dağıtılması

8. Adım: R4 cihazında BGP yol bilgisini görüntüleyiniz (Görsel 2.114).

```
R4(config)#router ospf 1
R4(config-router)#redistribute bgp 65001 subnets
R4(config-router)#exit
R4(config)#
R4(config)#router bgp 65001
R4(config-router)#redistribute ospf 1
R4(config-router)#exit
```

Görsel 2.114: R4 yönlendiricisinde OSPF rotalarının dağıtılması

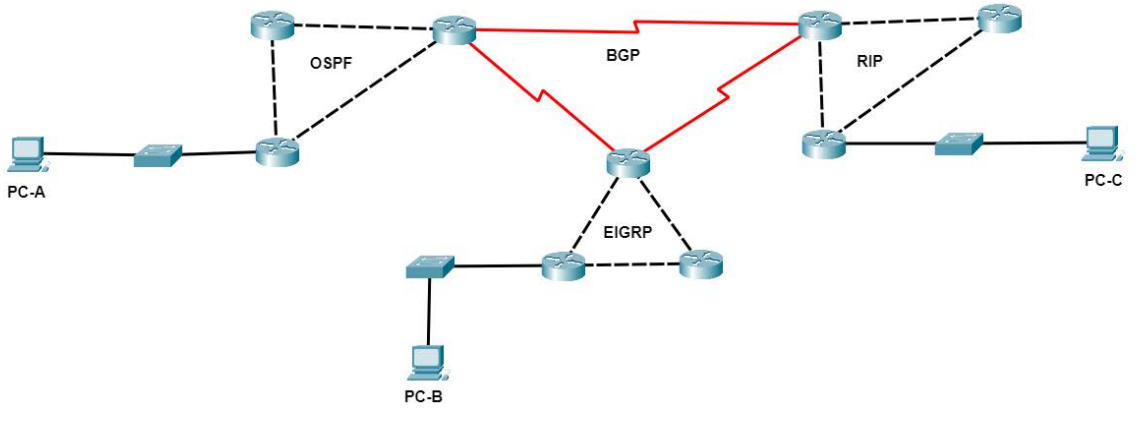
9. Adım: PC-A'dan PC-C'ye iletişimi **ping** komutuyla test ediniz (Görsel 2.115).



Görsel 2.115: PC-A ve PC-C bilgisayarları arasındaki iletişimin test edilmesi

SIRA SİZDE

Görsel 2.116'daki topolojiye göre OSPF, RIP ve EIGRP ile yapılandırılan ağların BGP protokolü ile iletişim kurmasını sağlayınız.



Görsel 2.116: Sıra sizde etkinliğinin ağ topolojisi

DEĞERLENDİRME

Çalışmanız aşağıda yer alan kontrol listesi kullanılarak değerlendirilecektir. Çalışmanızı yaparken değerlendirme ölçütlerini dikkate alınız.

KONTROL LİSTESİ

ÖLÇÜTLER	EVET	HAYIR
1. Ağ simülasyon programıyla ağ topolojisini tasarladı.		
2. OSPF alanındaki cihazların yapılandırmasını tamamladı.		
3. EIGRP alanındaki cihazların yapılandırmasını tamamladı.		
4. RIP alanındaki cihazların yapılandırmasını tamamladı.		
5. BGP yapılandırmasını tamamladı.		
6. Bilgisayarların birbirleriyle iletişimini test etti.		



SearchGPT: Arama Motorlarının Geleceği mi?

Gürkan Caner Birer

OpenAI, arama motorlarının işleyişini kökten değiştirmeyi amaçlayan SearchGPT'nin prototipini duyurdu. Bu model, geleneksel arama motorlarından farklı olarak, kullanıcıların sorularına doğrudan ve özlü yanıtlar veriyor.

SearchGPT, geniş bir bilgi tabanını analiz ederek kullanıcıların sorgularına en uygun yanıtları üretiyor. Sistem, karmaşık soruları anlayıp, ilgili bilgileri sentezleyerek kullanıcıya sunuyor. OpenAI'nin yaptığı ilk testlerde, SearchGPT'nin kullanıcı sorularına verdiği yanıtların doğruluk oranının %80'in üzerinde olduğu görüldü. Prototip şu anda sınırlı bir kullanıcı grubuyla test ediliyor. Kullanıcıların %92'si SearchGPT'nin geleneksel arama motorlarına göre daha verimli olduğunu belirtti. Öte yandan SearchGPT Perplexity.AI gibi yapay zekâ arama motorlarından çok da farklı görünmüyor. Sesli arama gibi vadedilen özelliklerin henüz etkin olmaması ve olmayan bilgilerin varmış gibi sunulması anlamına gelen "halüsinasyon" probleminin devam ediyor olması lansmanın biraz abartılı olabileceği izlenimi oluşturdu.

Ayrıca bilginin sunulduğu orijinal kaynaklara atıf verme konusundaki zayıflık da web sitesi sahiplerini endişelendiriyor. SearchGPT bir web sitesindeki bilgileri sunarken, çoğunlukla kullanıcıları orijinal kaynağa yönlendirmiyor. Bu durumda kullanıcılara ulaşamayan web site sahiplerinin gelirleri ve içerik üretmeye yönelik motivasyonları azalabilir. Bu hâliyle SearchGPT Google'ın önemli bir rakibi olabilecek düzeyde olmasa da gelecek için umut vadediyor.

Kaynak: https://bilimteknik.tubitak.gov.tr/makale/searchgpt-arama-motorlarinin-gelecegi-mi

ÖLÇME VE DEĞERLENDİRME

A) Aşağıdaki cümlelerde parantez içine yargılar doğru ise "D", yanlış ise "Y" yazınız.

1. ( ) Statik yönlendirmede rotalar, manuel olarak yapılandırılır.

2. ( ) Yönlendirme tablosunda yer almayan adresler, varsayılan statik rotaya yönlendirilir.

3. ( ) Dinamik yönlendirme bilgisi ağda hiçbir cihazla paylaşılmaz.

4. ( ) OSPF paketleri DR cihaz üzerinden yönetilir.

5. ( ) BGP komşuluk bilgileri show ip route static komutu ile öğrenilir.

B) Aşağıdaki cümlelerde boş bırakılan yerlere doğru kelimeleri yazınız.

1. Ana statik veya dinamik rotaya ek olarak tanımlanan yedek rotaya ..... denir.

2. Yönlendiriciler arasındaki mesafeye göre yapılan yönlendirme işlemine ..... ile yönlendirme denir.

3. OSPF'de yönlendiricinin doğrudan bağlı olduğu komşu cihazların bilgisinin kaydedildiği tabloya ..... tablosu denir.

4. OSPF ağlarında komşuluk bilgisini öğrenmek için ..... komutu kullanılır.

5. Farklı otonom sistem numarasına sahip ağlar arasında yönlendirme yapan protokole ..... denir.

C) Aşağıdaki soruları dikkatlice okuyarak doğru cevabı işaretleyiniz.

1. Yönlendirme tablosunda statik yönlendirme bilgisini gösteren önek aşağıdakilerden hangisidir?

A) C B) L C) O D) R E) S

2. Statik yönlendirmede hem çıkış arayüzü hem de sonraki sıçrama noktası belirtilerek yapılan yönlendirme türü aşağıdakilerden hangisidir?

A) Kayan statik rota B) Özet statik rota C) Standart statik rota

D) Tamamen tanımlı statik rota E) Varsayılan statik rota

3. Aşağıdakilerden hangisi dış ağ geçidi protokolüdür?

A) BGP B) EIGRP C) RIP D) RIPv2 E) OSPF

4. OSPF'nin yönetimsel mesafe değeri aşağıdakilerden hangisidir?

A) 1 B) 110 C) 120 D) 200 E) 220

5. Dinamik yönlendirmede komşu yönlendiricileri keşfetmek, yeni komşuluk kurmak ve kurulan komşulukları sürdürmek için kullanılan veri paketi aşağıdakilerden hangisidir?

A) DBD B) Hello C) LSA D) LSR E) LSU

6. Aşağıdakilerden hangisi OSPF'de yönlendiricilerin tam iletişime geçmesi için gerekli süreçlerden biri değildir?

A) Down State B) ExStart State C) Init State

D) Loading State E) Real State

7. OSPF'de bir arayüzün maliyetini görüntülemek için aşağıdaki komutlardan hangisi kullanılır?

A) show ip ospf bandwidth B) show ip ospf interface

C) show ip ospf neighbor D) show ip ospf route

E) show ip ospf table

8. Farklı otonom sistemlerdeki yönlendiriciler arasında kullanılan dış ağ geçidi yönlendirici aşağıdakilerden hangisidir?

A) EBGP B) IBGP C) IGRP D) RIP E) OSPF

9. BGP oturumlarında hata tespit edildiğinde oturumların kapatılmasını sağlayan mesaj paketi aşağıdakilerden hangisidir?

A) KEEPALIVE B) NOTIFICATION C) OPEN

D) PROCESS E) UPDATE

10. Komşuluğun başarılı bir şekilde sağlandığını ifade eden BGP komşuluk durumu aşağıdakilerden hangisidir?

A) Active State B) Connecting C) Established

D) Open Confirm E) Open Sent

3. ÖĞRENME BİRİMİ

KABLOSUZ AĞ TEKNOLOJİLERİ

KONULAR

3.1. KABLOSUZ AĞLAR

3.2. KABLOSUZ AĞ YAPILANDIRMASI

NELER ÖĞRENECEKSİNİZ?

- Kablosuz ağ teknolojilerini açıklama
- Kablosuz LAN yapılandırması yapma



TEMEL KAVRAMLAR

Ad-Hoc mod, Bluetooth, erişim noktası, IEEE802.11, LoRa, modem, Wi-Fi, WPAN, WWAN, ZigBee, 4-Way Handshake

HAZIRLIK ÇALIŞMALARI

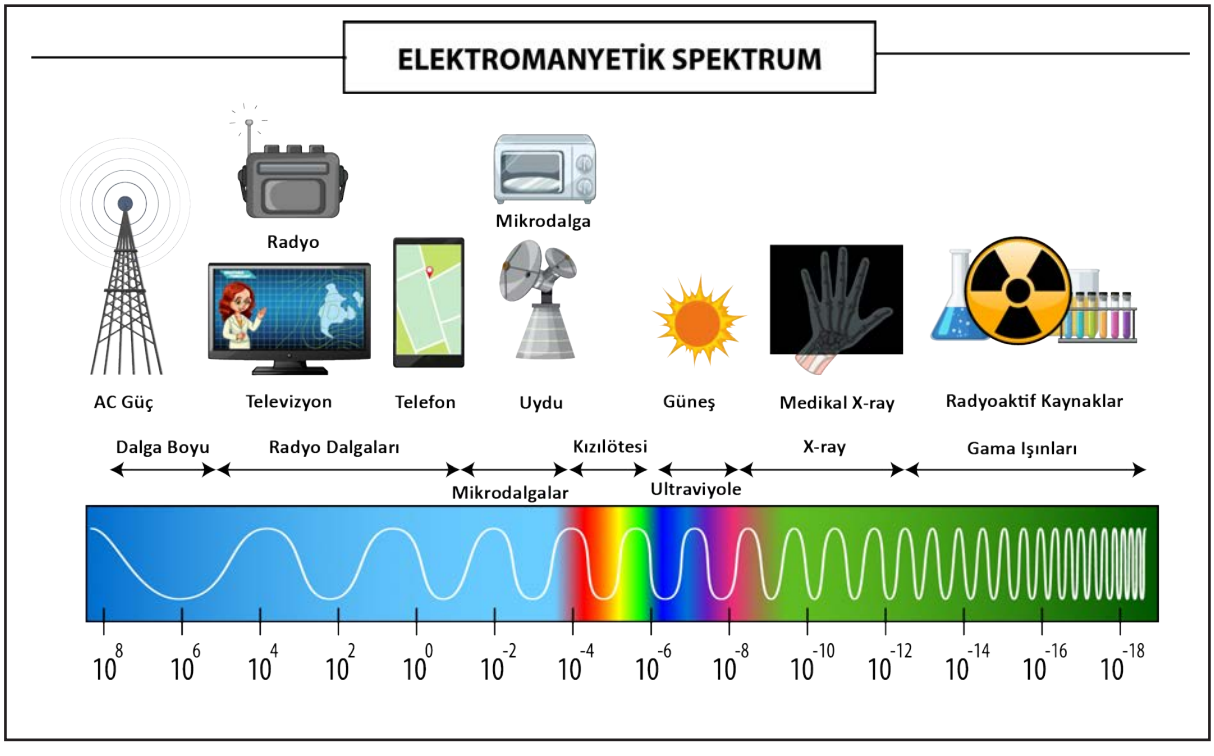
1. Cep telefonu, dizüstü bilgisayar, tablet gibi kablosuz cihazlar birbiriyle nasıl iletişim kurar? Düşüncelerinizi arkadaşlarınızla paylaşınız.

2. Akıllı ev, akıllı şehir gibi sistemlerin zihninizde canlandırdıklarını sınıfta arkadaşlarınızla paylaşınız.

3.1. KABLOSUZ AĞLAR

Kablosuz ağ teknolojileri, veri iletiminin kablosuz olarak radyo dalgaları, kızıl ötesi, mikro dalga gibi elektromanyetik dalgalarla yapıldığı sistemlerdir. Kablosuz ağlar kullanıcılara erişim kolaylığı, hareket serbestliği, çoklu cihaz desteği ve kurulum kolaylığı sağlar. Kablolu ağlara göre kurulumu daha kolaydır. Kullanılan ağ teknolojilerinin türüne göre belirli bir mesafede ve hızda veri iletimi sağlanır. Kablosuz iletişimde veriler, hava ortamında yayılarak ilerlediği için olumsuz ortam koşulları sinyalin kalitesini ve kapsama alanını etkileyebilir.

Kablosuz ağ teknolojilerinin yer aldığı frekans aralıkları, elektromanyetik spekturum üzerinde görülür (Görsel 3.1). Elektromanyetik spektrumda, farklı frekans aralıkları ve dalga boylarında çalışan kablosuz teknolojiler görülür. Her bir kablosuz ağ teknolojisi kendine uygun frekans aralığında faaliyet gösterir.



Görsel 3.1: Elektromanyetik spektrum

Kablosuz ağ teknolojilerinden bazıları şu şekildedir:

NFC (Near Field Communication)

NFC, genellikle birkaç santimetreye kadar çok yakın mesafelerde kablosuz cihazlar arasında veri iletişimini sağlayan kablosuz ağ teknolojisidir. Lisanssız olan ISM (Industrial, Scientific and Medical) radyo frekans bandında 13,56 MHz'te çalışır. Veri aktarım hızı 106 ile 424 Kbps arasındadır. Bu teknolojiye sahip iki cihaz birbiriyle eşler arası bağlantı kurabilir ve veri paylaşabilir. Yine NFC teknolojine sahip akıllı telefonlar veya akıllı kartlarla temassız ödeme yapılabilir (Görsel 3.2). Güvenlik sistemlerinde NFC kartlar veya anahtarlarla erişim kontrolü sağlanabilir.



Görsel 3.2: NFC ile temassız ödeme sistemi

Bluetooth

Bluetooth; akıllı ev cihazları, ses bağlantıları, otomobil içi bağlantılar, kulaklık, klavye, fare gibi kısa mesafedeki kablosuz iletişim araçlarının radyo dalgaları ile iletişim kurmasını sağlayan IEEE 802.15 WPAN teknolojisidir (Görsel 3.3). 100 metreye kadar mesafede iletişim sağlanır. Bluetooth teknolojisini kullanan cihazlar, düşük güç tüketimi ve hızlı bağlantı özelliklerine sahiptir. Bluetooth teknolojisinin iki farklı çalışma modu şu şekildedir:

BLE (Bluetooth Low Energy): Düşük enerji tüketimi gerektiren uygulamalar ve cihazlar için kullanılır [akıllı saatler, sağlık verilerini izleyen cihazlar, IoT (Internet of Things) cihazlar, sensörler vb.].

BR/EDR (Basic Rate/Enhanced Data Rate): Daha yüksek veri iletim hızı ve sürekli bağlantı gerektiren uygulamalar için kullanılır (kulaklıklar, fareler, cihazlar arası veri transferi, ses sistemleri, araç içi ses ve telefon bağlantıları).



Görsel 3.3: Blueetooth teknolojisi

ZigBee

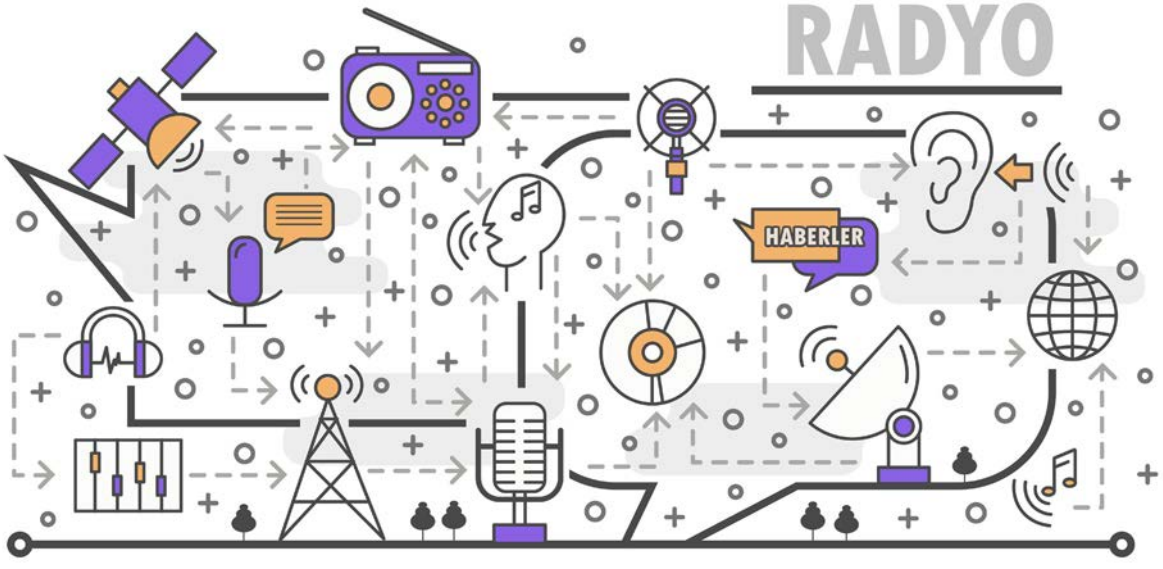
ZigBee, düşük güç tüketimi ve düşük maliyetli kablosuz veya sensör ağlar oluşturmak için kullanılan teknolojidir. Akıllı ev sistemleri, endüstriyel otomasyon ve sağlık uygulamaları, akıllı şehir uygulamaları gibi birçok alanda kullanılır. IEEE 802.15.4 standardını kullanan kablosuz ağ teknolojisidir. ZigBee ile birkaç yüz metreye kadar iletişim sağlanabilir (Görsel 3.4).



Görsel 3.4: ZigBee ile akıllı ev uygulaması

RF (Radio Frequency)

RF, elektromanyetik spektrumda 3 KHz ile 300 GHz arasında yer alan bir frekans bandıdır. **RF modülü**, bir cihazdan başka bir cihaza gerçek zamanlı verileri radyo dalgalarıyla yaymak için kullanılan elektronik devredir. RF modülünün veri iletim hızı, 1 Kbps ile 10 Kbps arasında değişir. Radyo dalgaları, farklı frekanslarda farklı hizmetleri sağlamak için geniş bir uygulama alanında çeşitli teknolojilere de entegre edilerek çalışır. Geniş bir kapsama alanında hizmet sunar fakat elektromanyetik gürültüden, olumsuz hava koşullarından veya fiziksel engellerden de etkilenebilir. Radyo dalgaları, frekans ve güce bağlı olarak farklı mesafelerde iletim sağlayabilir. RF teknolojileri radyo, televizyon, radar, mobil iletişim, uydu, tıbbi cihazlar, yangın koruma sistemleri gibi birçok alanda kullanılır (Görsel 3.5).



Görsel 3.5: RF teknolojisi

LoRa (Long Range)

LoRa, radyo frekanslarının daha uzun mesafelerde düşük güç tüketimiyle kullanılmasını sağlayan teknolojilerdir. IoT uygulamalarının yaygınlaşmasıyla birlikte verilerin daha uzun mesafelerde ve düşük güç tüketimiyle iletilmesi ihtiyaç hâline gelir. LoRa, Chirp Spread Spectrum (CSS) teknolojisinden türetilen bir modülasyon tekniği olup radyo frekanslarının uzun mesafelerde kullanımını sağlar. CSS radyo dalgalarının bir frekans aralığı boyunca yayılarak ilerlemesini sağlar. LoRa, kullanıldığı bölgeye bağlı olarak 433, 868 veya 915 MHz frekans bandında çalışır. Kentsel alanlarda birkaç kilometreye kadar iletim

sağlanırken açık alanlarda 15 kilometreye kadar iletim sağlanabilir. LoRa teknolojisini kullanan uç cihazların ağ geçitleri ve uygulama sunucuları ile iletişim sağladığı geniş alan ağına **LoRaWAN** adı verilir. LoRa IoT uygulamalar; akıllı tarım uygulamaları, akıllı şehir sistemleri, çevre izleme araçları ve enerji yönetimi gibi birçok alanda kullanılır (Görsel 3.6).



Görsel 3.6: LoRa teknolojisi

Wi-Fi (Wireless Fidelity)

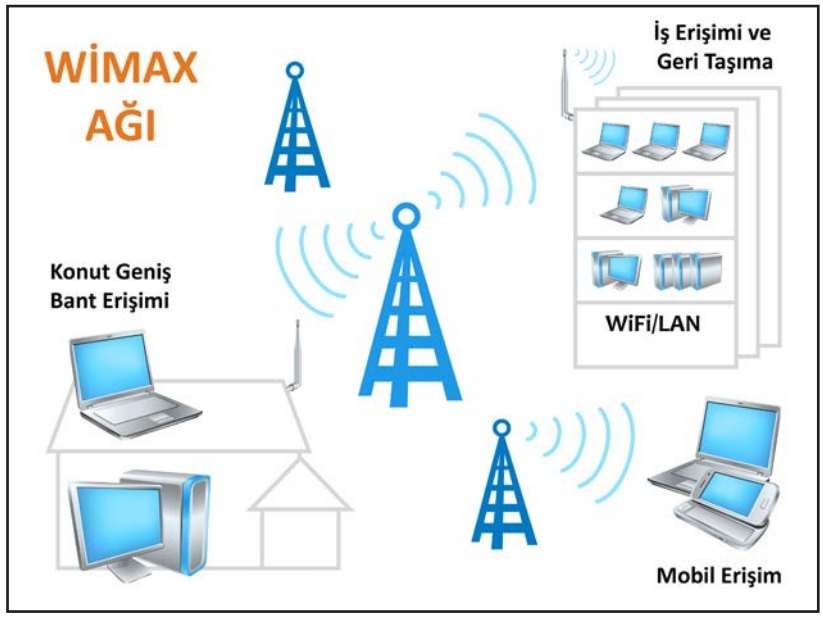


Görsel 3.7: Wi-Fi

Wi-Fi, IEEE 802.11 standartlarıyla çalışan belirli bir mesafede yüksek veri iletim hızı sağlayan kablosuz alan ağı teknolojisidir. Wi-Fi protokolü 2.4 GHz ile 5 GHz frekans bandında çalışır. Genellikle birkaç yüz metreye kadar veri iletimi yapabilir. Veri iletim mesafesi ve kalitesi, ortam koşullarına bağlı olarak değişkenlik gösterebilir. Erişim noktaları ile kablosuz ağ sinyalleri daha uzak mesafelere taşınarak ağ genişletilebilir. Yönlendiriciyle ağ trafiği yönetilebilir ve ağda internet hizmeti sağlanabilir. Wi-Fi ağlar; konutlar, restoranlar, mağazalar, iş yerleri, okullar, hastaneler gibi çeşitli alanlarda kullanıma uygundur (Görsel 3.7).

WiMAX (Worldwide Interoperability for Microwave Access)

WİMAX, sabit ve mobil istasyonlarla birlikte çalışan ve çok geniş kapsama alanında kablosuz iletişimi sağlayan ağ teknolojisidir. Sabit istasyonlar yaklaşık 50 km, mobil istasyonlar ise yaklaşık 15 km mesafede veri iletimi sağlar. WİMAX, IEEE 802.16 standardını kullanır ve çeşitli frekans bantlarında çalışabilir (Görsel 3.8).



Görsel 3.8: WİMAX

Hücresel Ağlar (Cellular)



Görsel 3.9: Hücresel (Cellular)

Hücresel ağlar, karasal alanlarda konumlandırılmış genellikle baz istasyonları ile oluşturulan hücreler aracılığıyla veri iletişiminin sağlandığı teknolojilerdir (Görsel 3.9). Mobil iletişimle en çok ilişkilendirilen ağ teknolojisidir. Hücreler belirli bir mesafedeki alanı ifade eder. Geniş bir coğrafya üzerinde yer alan hücreler, baz istasyonlarının kapsama alanları ile ifade edilir. Cihazlar, birbirine komşu hücreler arasında genellikle sinyalin daha güçlü olduğu hücreye geçiş yapar. Bu geçiş işlemine **handoff** denir. Hücrenin merkezinde yer alan baz istasyonları, mobil cihazlarla iletişimi sağlar. Hareket hâlindeki mobil cihazlar, en yakın kapsama alanındaki baz istasyonuna bağlanarak iletişimin devamlılığını sağlar. Hücresel teknolojiler 1 G, 2 G, 3 G gibi isimlerle ifade edilir. G harfi, Generation (nesil) anlamına gelir. İlk hücresel teknolojiler yalnızca ses iletimi sağlarken sonraki nesillerde veri iletim kapasitesi ve hızlarının artmasıyla birlikte ses, görüntü, mobil oyunlar ve IoT teknolojileri gibi çeşitli uygulamaların kullanılmasını sağlar. Yüksek veri hızı ve internet iletişimi için en çok tercih edilen teknolojilerden biridir.

Uydu Sistemleri (Satellite)

Uydular, yeryüzünden belirli bir yükseklikte dünya yörüngesinde dönen cihazlardır (Görsel 3.10). Bu cihazlar, dünya üzerinde yer alan istasyonlardan sinyal alır ve bu istasyonlara sinyal gönderir. Karasal ağ iletişiminin zor olduğu yerlerde bile uydu aracılığıyla çok geniş kapsama alanında veri iletimi sağlanır. Uydu sistemleri; iletişim yayınları, hava durumu tespiti, navigasyon sistemleri, gözlem-izleme sistemleri gibi birçok amaçla kullanılır.



Görsel 3.10: Uydu Sistemleri

ARAŞTIRMA Kablosuz ağ

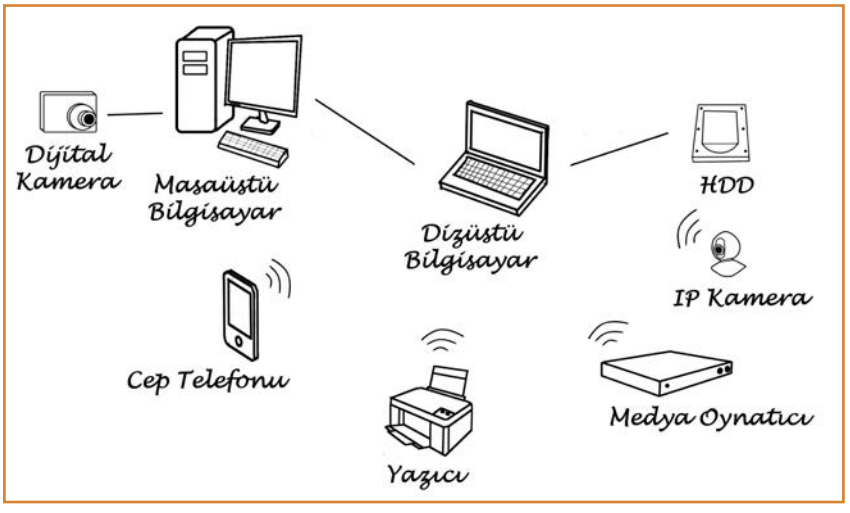
Kablosuz ağ teknolojilerinin tarihsel gelişimini araştırınız. Edindiğiniz bilgileri sınıfta arkadaşlarınızla paylaşınız.

3.1.1. Kablosuz Ağ Türleri

Kablosuz ağ türleri, kablosuz ağların kullanıldığı mesafe ve kullanım alanlarına göre sınıflandırılmasını ifade eder. Bunlar küçük bir alandan büyük bir coğrafya üzerine kadar kullanılabilen ağ çeşitleridir. Kablosuz ağ türleri şunlardır:

WPAN [Wireless Personal Area Network (Kablosuz Kişisel Alan Ağı)]

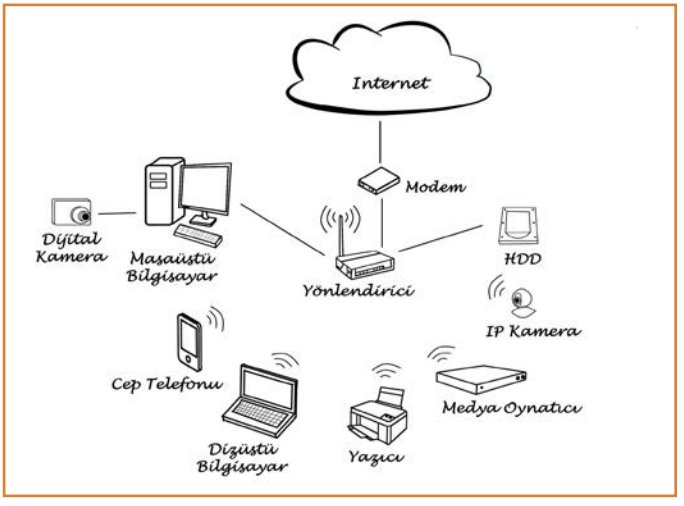
WPAN, kısa mesafedeki cihazlar arasında sağlanan kablosuz ağ türüdür. Genellikle 10 metreye kadar iletişim sağlanır. Bluetooth ve ZigBee tabanlı teknolojilerin desteklediği elektronik cihazlar tarafından kullanılır. WPAN teknolojileri 802.15 standardını ve 2.4 GHz radyo frekansını kullanır. Görsel 3.11'de kısa mesafede oluşturulan WPAN görülür.



Görsel 3.11: WPAN

WLAN [Wireless Local Area Network (Kablosuz Yerel Alan Ağı)]

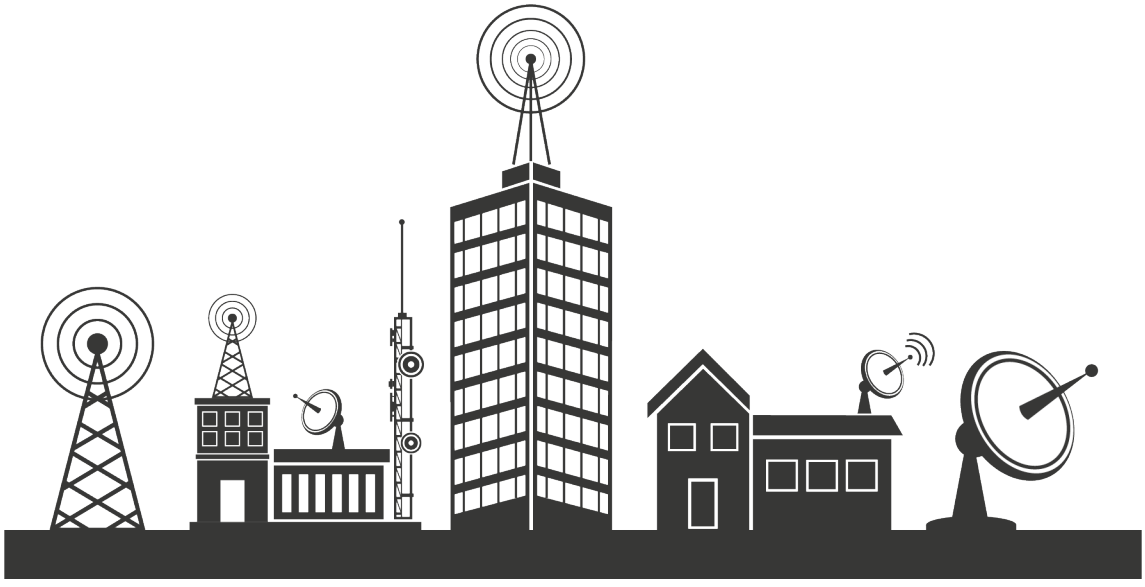
WLAN, genellikle 100 metreye kadar iletişimin sağlandığı küçük ölçekli kablosuz ağlardır. Ev, ofis, kampüs gibi sınırlı alanlarda kullanıma uygundur. WLAN teknolojileri 802.11 standardını ve 2.4-5 GHz radyo frekansını kullanır. Görsel 3.12'de kablosuz ağ cihazları ve merkezî bir yönlendiriciyle oluşturulan WLAN görülür.



Görsel 3.12: Kablosuz ağ cihazları ve merkezî bir yönlendiriciyle oluşturulan WLAN

WMAN [Wireless Metropolitan Area Network (Kablosuz Metropol Alan Ağı)]

WMAN, büyük şehirler veya bölgeler üzerinde kablosuz iletişimin sağlandığı orta büyüklükteki kablosuz alan ağlarıdır. Bir kuruluşun uzak mesafedeki farklı şubeleri, kampüsler, hastaneler gibi birçok geniş alanda kullanılır (Görsel 3.13).



Görsel 3.13: WMAN

WWAN [Wireless Wide Area Network (Kablosuz Geniş Alan Ağı)]

WWAN, geniş coğrafi alanlar üzerinde kablosuz iletişimin sağlandığı çok büyük geniş alan ağıdır (Görsel 3.14). Ulusal ve küresel iletişim için uygundur. Hücresel ağlar ve uydu teknolojileri kullanılır.



Görsel 3.14: WWAN

SIRA SİZDE

Ağ simülasyon programı ile küçük bir ofis kullanımına uygun WLAN topolojisi tasarlayınız.

DEĞERLENDİRME

Çalışmanız aşağıda yer alan kontrol listesi kullanılarak değerlendirilecektir. Çalışmanızı yaparken değerlendirme ölçütlerini dikkate alınız.

KONTROL LİSTESİ

ÖLÇÜTLER	EVET	HAYIR
1. Ağ simülasyon programını çalıştırdı.		
2. Ağ ortamında kullanılacak uygun ağ cihazlarını seçti.		
3. Ofis ortamına uygun olarak ağ cihazlarının yerleşimini yaptı.		

3.1.2. Kablosuz Ağ Cihazları

Kablosuz ağ cihazları, kablosuz ağ iletişiminin sağlanması ve veri iletiminin sorunsuz olarak tamamlanmasını sağlar. Kablosuz iletişimde veri akışının yönetimi, sinyalin güçlendirilmesi ve iletimi, kapsama alanının belirlenmesi ve veri güvenliği bu cihazlarla sağlanır. Kablosuz ağ cihazları ve bunlarda kullanılan bileşenler şu şekildedir:

Kablosuz Ağ Kartı

Kablosuz ağ kartları; masaüstü veya dizüstü bilgisayar, tablet, telefon gibi uç cihazların kablosuz bir ağa bağlanabilmesi için kullanılan donanımlardır. Yeni nesil teknolojilerde genellikle dâhilî kablosuz ağ kartı bulunur. Dâhilî kablosuz ağ kartının bulunmadığı durumlarda ise PCI genişleme yuvasına veya USB bağlantı noktasına ağ kartı takılabilir (Görsel 3.15).



Görsel 3.15: Kablosuz ağ kartı

Kablosuz Modem

Modemler, internet servis sağlayıcısından [ISP (Internet Service Provider)] gelen sinyalleri işleyerek ağ cihazlarının anlayacağı formata dönüştüren cihazlardır. Modem; dijital sinyalleri analog sinyallere dönüştürürken **modülasyon**, analog sinyalleri dijital sinyallere dönüştürürken **demodülasyon** işlemini gerçekleştirir. Modemler farklı bağlantı türlerine göre sınıflandırılabilir. DSL modem, telefon hattı üzerinden; kablo modem, kablo TV hattı üzerinden; fiber modem, fiber optik kablolar üzerinden; 4G/5G modem, mobil veri ağları üzerinden internet bağlantısı sağlar.

Kablosuz modemler ise kablosuz cihazlara, kablosuz bir ağ üzerinden internet hizmeti sağlar. Kablosuz modemler aynı zamanda yönlendirici işlevini yürütür (Görsel 3.16).



Görsel 3.16: Kablosuz modem

Kablosuz modemin bileşenleri şu şekildedir:

WAN Portu: İnternet servis sağlayıcısına bağlanan porttur.

LAN Portu: Kablolu yerel ağ oluşturmak için kullanılan pottur. Bilgisayar, yazıcı veya diğer kablolu ağ cihazları bu porta bağlanarak ağa dâhil edilir.

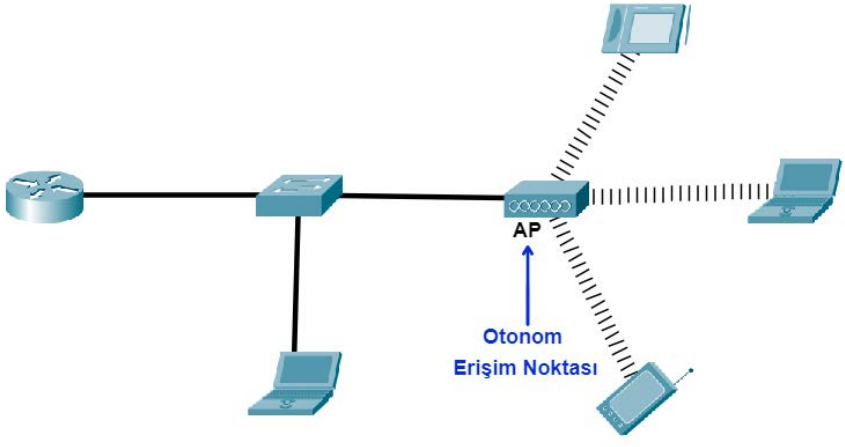
Wi-Fi Antenleri: Kablosuz sinyalleri hem alır hem de iletir.

Yönetim Araçları: Modemin yapılandırma ayarlarının yapıldığı ve yönetiminin sağlandığı yazılım arayüzüdür.

Kablosuz Erişim Noktası

Kablosuz erişim noktası, kablolu bir ağın kablosuz ağ olarak genişletilerek kullanılmasını sağlayan cihazdır. Kablosuz erişim noktalarıyla mobil cihazlar, tablet, dizüstü bilgisayar gibi kablosuz cihazlar, kablolu bir ağa bağlanabilir. Kullanıldığı ağın ihtiyacına ve amacına göre kontrol yöntemi farklı olan iki tür erişim noktası vardır. Erişim noktası türleri şu şekildedir:

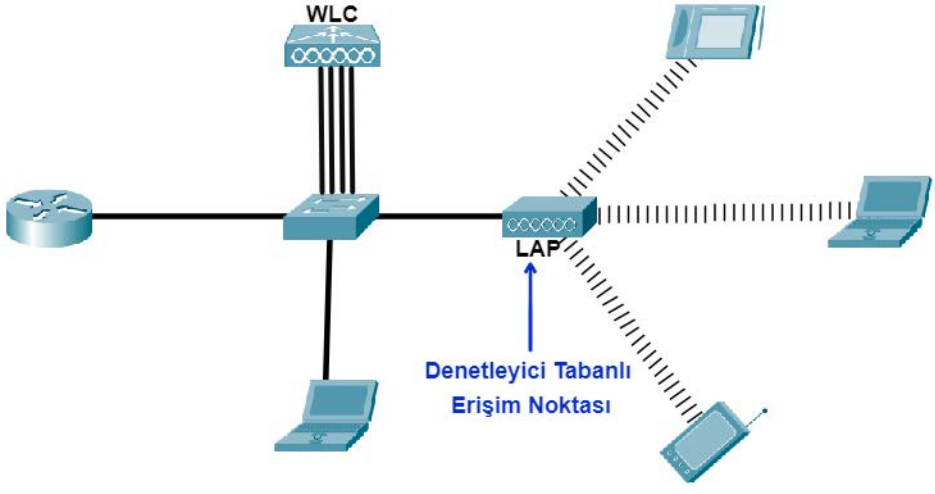
1. **Otonom Erişim Noktası:** Kullanıcı sayısının az olduğu küçük veya orta ölçekli ağlarda tercih edilen erişim noktalarıdır. Bu cihazların yapılandırması ilk kurulumda yapılır. Kablosuz cihazın yapılandırması, sayının çok arttığı veya ağın genişletilmesi gerektiği durumlarda yeni erişim noktaları eklenerek manuel yapılır. Görsel 3.17'de manuel olarak yapılandırılan erişim noktası görülür.



Görsel 3.17: Otonom erişim noktası

2. **Denetleyici Tabanlı Erişim Noktası:** Kullanıcı sayısının çok fazla olduğu büyük ofis, fabrika, hastane, alışveriş merkezi gibi alanlarda tercih edilen erişim noktalarıdır. Bu alanlarda veri iletişimi birden çok erişim noktasıyla sağlanır. **LAP (Lightweight Access Point)** olarak adlandırılan bu cihazlar, özel bir yapılandırma gerektirmez. LAP'lerin yapılandırması, **WLC (WLAN Controller)** adı verilen merkezî cihaz tarafından sağlanır. Ağa dâhil olan her erişim noktası, otomatik olarak WLC tarafından yapılandırılır

ve yönetilir. LAP'ler WLC ile iletişim kurmak için **LWAPP (Lightweight Access Point Protocol)** protokolünü kullanır. WLC'lerin kullanımında bant genişliğini arttırmak, ağ trafiğini dengelemek ve yedeklilik sağlamak amacıyla **LAG (Link Aggregation Group)** bağlantısı kullanılır. LAG teknolojisinde birden fazla bağlantı olduğu için bant genişliği artar. Aynı zamanda ağ trafiği, tüm bağlantılar üzerinden sağlanarak yük dengelenir. Bir bağlantıda arıza olması durumunda diğer bağlantılar üzerinden veri iletimi devam ettiği için yedeklilik de sağlanmış olur. Görsel 3.18'de denetleyici tabanlı erişim noktasıyla kablosuz ağ erişimi görülür.



Görsel 3.18: Denetleyici tabanlı erişim noktası

Antenler

Antenler, elektromanyetik sinyalleri alan ve yayan cihazlardır. Aldıkları sinyalleri, elektrik sinyallerine dönüştürerek verinin işlenmesini sağlar. Wi-Fi, Bluetooth gibi kablosuz iletişimde kullanılır. Antenlerin kapsama alanı ve gücü, kablosuz ağ iletiminin kalitesini belirler. Kablosuz ağın ihtiyacına göre kullanılan anten türlerinden bazıları şunlardır:

Çok Yönlü Anten (Omnidirectional Antenna): Kablosuz sinyalin her yöne (360 derece) yayılmasını sağlayan antenlerdir (Görsel 3.19). Ev, küçük ofis, kafeterya gibi genel Wi-Fi erişiminin yapıldığı alanlarda kullanıma uygundur.



Görsel 3.19: Çok yönlü anten



Görsel 3.20: Yönlü anten

Yönlü Anten (Directional Antenna): Kablosuz sinyali, belirli bir yönde yoğunlaştırarak yayar (Görsel 3.20). Sinyalin yönünde kapsama alanı daha yüksekken diğer yönlerde düşüktür. Sinyalin gücü, belirli bir hedefe doğru artırılarak uzak mesafelere taşınabilir. TV ve radyo iletişiminde kullanılır.

Çok Giriş Çıkışlı Anten [MIMO (Multiple Input Multiple Output) Antenna]: Birden fazla antenle çoklu sinyal alışverişini kabul eden ve yöneten sistemdir (Görsel 3.21). Kablosuz ağların bant genişliğini attırmak için kullanılır. Kapsama alanı oldukça büyük ve etkilidir. Bazı Wi-Fi yönlendiricilerde, mobil iletişimde, kurumsal ve endüstriyel uygulamalarda kullanılır.



Görsel 3.21: Çok giriş çıkışlı anten

3.1.3. WLAN (IEEE 802.11) Standartları

Kablosuz ağ standartları, kablosuz iletişimin sağlıklı bir şekilde yapılmasını sağlayan kurallar ve protokoller bütünüdür. Kablosuz ağ iletişiminin keşfinden bugüne kadar birçok teknoloji hayata dâhil olur. Bu teknolojilerin geliştirilmesi, birbiriyle uyumlu çalışması ve entegre edilmesi standartlarla sağlanır. Bu standartları oluşturan kurum ve kuruluşlardan biri de **Elektrik ve Elektronik Mühendisleri Enstitüsüdür (IEEE)**. Kablosuz ağ iletişiminde IEEE 802.11 standartları kullanılır. Bu standartlarla kablosuz cihazların hangi frekansta çalışacağı, veri taşıma kapasitesi, veri iletim hızı, veri iletim mesafesi, modülasyon yöntemleri gibi birçok özelliği belirlenir. Kablosuz ağ standartlarının isimleri ve özellikleri Tablo 3.1'de görülür.

Tablo 3.1: IEEE 802.11 Standartları

Standart	Frekans	Bant Genişliği	Veri Hızı	Mesafe	Modülasyon
802.11	2.4 GHz	20 MHz	2 Mbps	20-100 m	DSSS/FHSS
802.11b	2.4 GHz	20 MHz	11 Mbps	38-140 m	DSSS
802.11a	5 GHz	20 MHz	54 Mbps	38-140 m	OFDM
802.11g	2.4 GHz	20 MHz	54 Mbps	38-140 m	DSSS, OFDM
802.11n	2.4-5 GHz	20-40 MHz	600 Mbps	70-250 m	OFDM, MIMO
802.11ac	5 GHz	20-40-80-160 MHz	3.5 Gbps	35-160 m	OFDM, MIMO
802.11ax	2.4-5-6 GHz	40-80-160 MHz	9.6 Mbps	30-120 m	MIMO, OFDMA

IEEE 802.11: Wi-Fi Alliance tarafından geliştirilen ve kablosuz ağ iletişiminin kurallarını belirleyen ilk standarttır. Daha sonradan geliştirilen kablosuz ağların temelini oluşturur. 2.4 GHz frekans bandında çalışır ve 2 Mbps veri hızında 100 metreye kadar iletim sağlayabilir.

IEEE 802.11b: Wi-Fi1 olarak da adlandırılan bu standart, 1999 yılında kullanıma sunulur. 2.4 GHz frekans bandında çalışırken daha yüksek hızda veri iletimi yapabilir. Aynı zamanda diğer kablosuz cihazlardan gelen paraziti azaltmak için DSSS/CCK modülasyon tekniğini kullanır. İç mekânlarda 38, dış mekânlarda 140 metreye kadar veri iletimi sağlayabilir.

IEEE 802.11a: Wi-Fi2 olarak da adlandırılan bu standart, 1999 yılında kullanıma sunuldu. Wi-Fi1'e göre daha yüksek hızda veri iletimini desteklemek için OFDM modülasyonunu kullanır. Bu standart, 802.11b ve 802.11g standartlarıyla uyumlu çalışmaz.

IEEE 802.11g: Wi-Fi3 olarak da adlandırılan bu standart, 2003 yılında kullanıma sunuldu. 2.4 GHz frekans bandında çalışır ve 54 Mbps'ye kadar veri iletimi sağlayabilir. Azaltılmış bant genişliği kapasitesiyle 802.11b ile geriye dönük uyumluluk sağlar.

IEEE 802.11n: Wi-Fi4 olarak da adlandırılan bu standart, 2009 yılında kullanıma sunuldu. Hem 2.4 GHz hem de 5 GHz frekans bandında çalışan bu standart, 600 Mbps'ye kadar da veri iletimini destekler. Sınırlı veri hızına sahip 802.11a/b/g cihazlarıyla geriye dönük uyumluluk sağlar.

IEEE 802.11ac: Wi-Fi5 olarak da adlandırılan bu standart, 2013 yılında kullanıma sunuldu. Daha yüksek bant genişliği ile 3.5 Gbps'ye kadar veri iletimi sağlar. Gönderici ve alıcı cihazlarda çoklu anten (MIMO) teknolojisini kullanan ilk Wi-Fi standardıdır. Sınırlı veri hızına sahip 802.11 a/n cihazlarıyla geriye dönük uyumluluk sağlar.

IEEE 802.11ax: Wi-Fi6 olarak adlandırılan bu standart, 2021 yılında kullanıma sunuldu. 2.4 GHz, 5 GHz ve 6 GHz frekans bantlarında çalışır. Teorik olarak 9.6 Gbps veri iletim hızını destekler fakat bu veri iletim hızı; Wi-Fi hızının arttırılması ile ilgili değildir, artan cihaz sayılarının arasında bu hızın paylaştırılması ile ilgilidir. Bu standart, veri hızını birden fazla cihaza bölme ve yönlendiricilerin tek bir yayın çerçevesinde birden fazla cihaza veri göndermesine olanak sağlar. Ayrıca uzun menzil desteğiyle dış mekân operasyonlarını da destekler. Bu özellikler; yüksek çözünürlüklü video, bulut erişimi gibi veri yoğunluğu fazla uygulamalarda daha iyi performans sağlar.

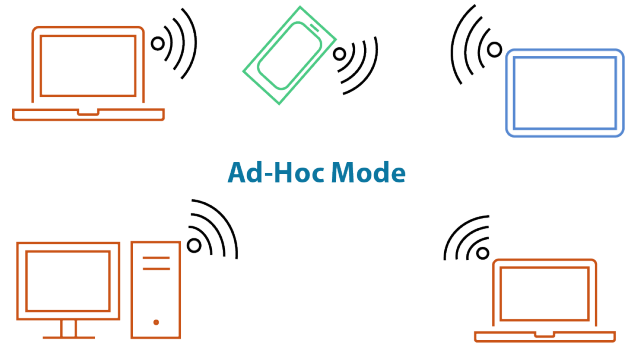
IEEE P802.11be: Wi-Fi7 olarak adlandırılan bu standardın 2024 yılında tamamlanması beklenmektedir. Yaklaşık 40 Gbit/s veri hızı ve 320 MHz bant genişliği sunarak Wi-Fi teknolojisinde önemli bir ilerleme kaydedilir. Ayrıca daha düşük gecikme süresi ve yoğun Wi-Fi alanlarında daha iyi performans sağlamak üzere mevcut Wi-Fi yeteneklerini geliştiren birçok yenilik içerir.

3.1.4. WLAN (IEEE 802.11) Topoloji Modları

Kablosuz yerel alan ağlarında kullanılan topoloji modları şu şekildedir:

Ad-Hoc Mode (Anlık Mod)

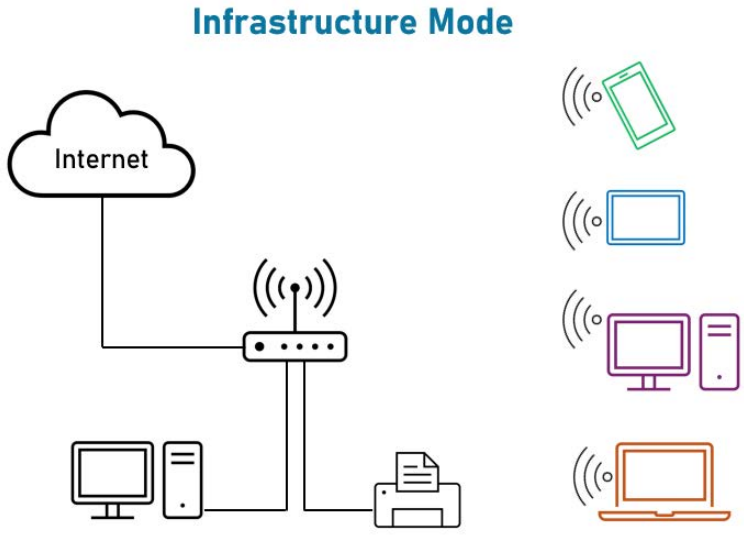
Ad-Hoc, kablosuz cihazlar arasında kurulan eşten eşe bağlantı modudur. Bu bağlantı şeklinde erişim noktası veya yönlendirici gibi ara bir cihaza ihtiyaç duyulmadan cihazlar doğrudan bağlantı kurar (Görsel 3.22). Bluetooth veya Wi-Fi Direct ile yapılan bağlantı, bu türün örnekleridir. Ad-Hoc modu ile yapılan bağlantı, bağımsız temel servis kümesi **IBSS (Independent Basic Service Set)** olarak ifade edilir.



Görsel 3.22: Ad-Hoc mod

Infrastructure Mode (Altyapı Modu)

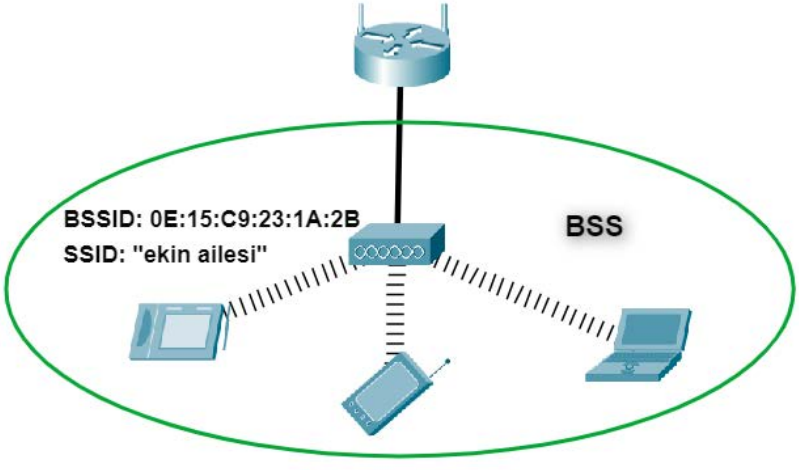
Infrastructure, kablosuz ağ cihazlarının erişim noktası veya yönlendirici aracılığıyla birbirine bağlanarak oluşturulan ağ topolojisi modudur. Alt yapı modunda istemciler merkezî bir cihaza bağlıdır. İstemcilerin yapılandırması ve birbirleriyle iletişimi, merkezî cihaz tarafından sağlanır (Görsel 3.23).



Görsel 3.23: Infrastructure Modu

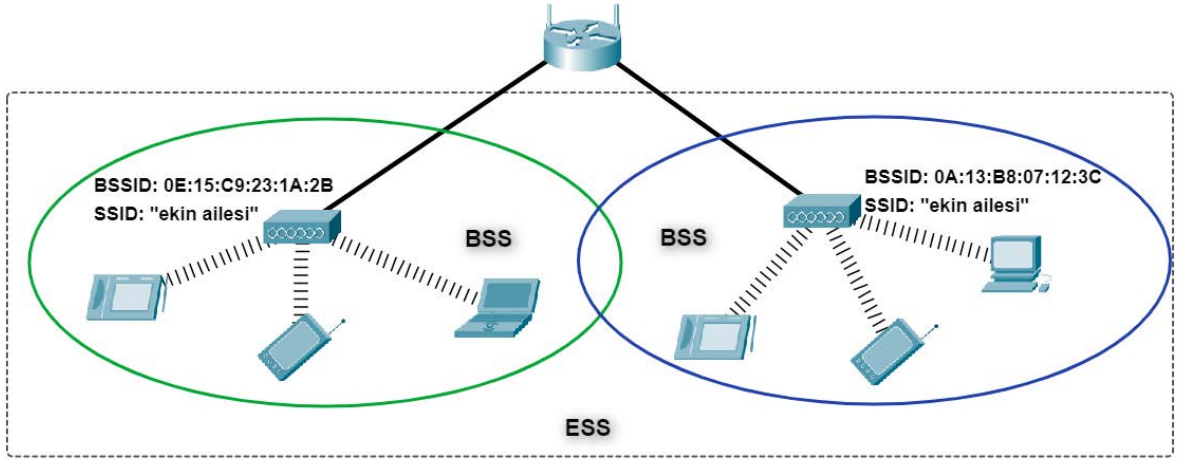
Kablosuz ağ yapıları ve uygulamaları şu şekildedir:

BSS [Basic Service Set (Temel Servis Kümesi)]: Temel servis kümesinde kablosuz istemcilerin tek bir merkezî cihaza bağlanarak oluşturduğu topolojidir (Görsel 3.24). Her BSS kendine ait ağ adını kullanır. Ev, küçük ofis, kafeterya gibi alanlarda kullanıma uygundur.



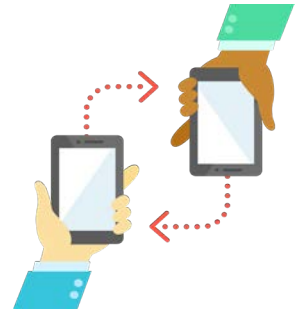
Görsel 3.24: BSS

ESS [Extended Service Set (Genişletilmiş Servis Kümesi)]: Birden fazla BSS'nin bir araya getirilmesiyle oluşturulan ve daha geniş kapsama alanına sahip topolojidir (Görsel 3.25).



Görsel 3.25: ESS

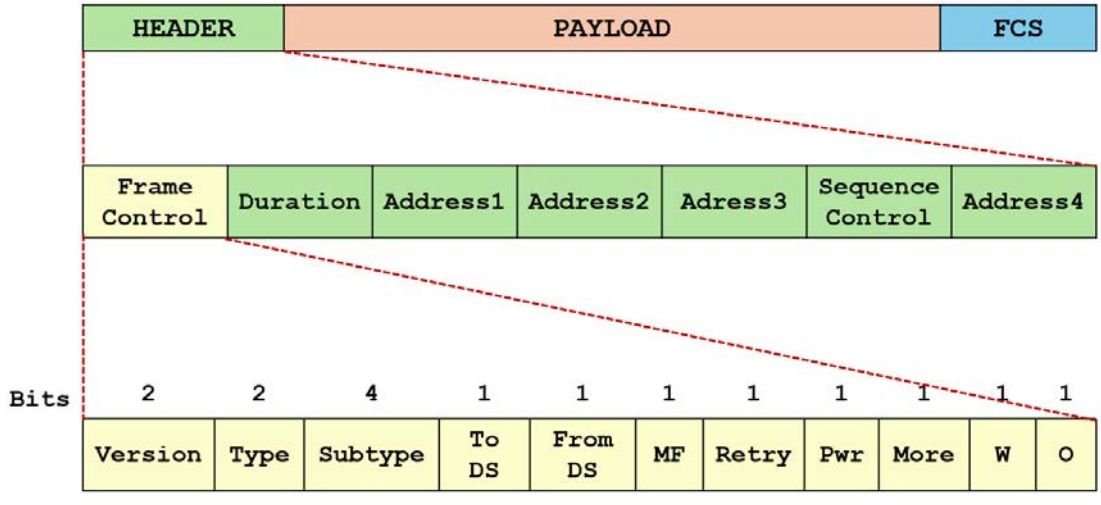
Tethering Mode (Paylaşım Modu): Hücresel veri erişimi olan akıllı telefon veya tabletin, etkin bağlantı noktası ile internet paylaşımı yaptığı topolojidir (Görsel 3.26). İnternet paylaşım modu; Wi-Fi, USB veya Blouetooth bağlantısı ile sağlanabilir.



Görsel 3.26: Tethering

3.1.5. WLAN (IEEE 802.11) Çerçeve Yapısı

Çerçeve yapısı, bir verinin nasıl iletileceğini ve nasıl kontrol edileceğini belirleyen veri paketleridir. 802.11 çerçeve yapısı da kablosuz ağlarda veri iletiminin gerçekleştirilmesini sağlar. Görsel 3.27'de 802.11 çerçeve yapısı görülür.



Görsel 3.27: 802.11 çerçeve yapısı

802.11 çerçeve yapısındaki bilgiler şu şekildedir:

Header (Başlık): Verilerin iletimi, işlenmesi ve kontrolü ile ilgili temel bilgileri içerir.

Payload (Yük): Çerçeve ile iletilen veri bölümüdür. Veri çerçevelerinde veriler, kontrol çerçevelerinde kontrol bilgileri, yönetim çerçevelerinde yönetim bilgileri taşınır. Yük boyutu, gönderilen verinin miktarına göre değişiklik gösterir.

FCS [Frame Check Sequence (Çerçeve Kontrol Dizisi)]: Gönderilen verinin kontrolünün yapılmasını sağlayan alandır. Gönderici ve alıcı arasında verinin eksiksiz olarak gönderilmesini kontrol eder.

Frame Control (Çerçeve Kontrol): Çerçeve türünün ve özelliklerinin yer aldığı 16 bitlik alandır. Çerçeve kontrolünde yer alan alt alanlar şu şekildedir:

- **Version (Sürüm):** Kullanılan IEEE 802.11 protokolünün sürüm bilgisini gösterir.
- **Type (Tür):** Gönderilen çerçevenin türünü gösterir. **Veri**, **kontrol** ve **yönetim** olmak üzere üç farklı çerçeve türü vardır. 00, yönetim çerçevesi; 01, kontrol çerçevesi; 10, veri çerçevesi olarak işlenir.
- **Subtype (Alt Tür):** Gönderilen çerçevenin alt türünü gösterir. Örneğin yönetim çerçevelerinde Beacon, Probe Request/Response; kontrol çerçevelerinde RTS, CTS; veri çerçevelerinde ACK işlemleri alt tür olarak belirtilir.
- **To DS [To Distribution System (Dağıtım Sistemine)]:** Çerçevenin bir erişim noktasına yönlendirilmesi bilgisinin gösterildiği alandır. Bu değer **1** ise çerçeve bir erişim noktasına yönlendirilir, **0** ise yönlendirilmez.
- **From DS [From Distribution System (Dağıtım Sisteminden)]:** Çerçevenin bir erişim noktasından gönderilme bilgisinin gösterildiği alandır. Bu değer **1** ise çerçeve, erişim noktasından gelir. **0** ise çerçeve, erişim noktasından gelmez.
- **MF [More Fragment (Daha Fazla Parça)]:** Çerçevenin birden fazla parçadan oluşma bilgisinin gösterildiği alandır. Bu değer **0** ise çerçeve, tek parçadan oluşuyor demektir. **1** ise çerçeve, birden fazla parçadan oluşuyor demektir.
- **Retry (Tekrar Deneme):** Çerçevenin yeniden gönderilme bilgisinin gösterildiği alandır. Bu değer **1** ise çerçeve yeniden gönderim tekrarıdır. **0** ise çerçeve ilk defa iletiliyordur.
- **Pwr [Power Management (Güç Yönetimi)]:** Çerçevenin düşük güç modunda olup olmadığını gösterir. Bu değer **1** ise çerçeve, düşük güç modunda bir cihazdan gönderilmiştir. **0** ise cihaz, aktif veri iletimi yapıyordur.
- **More (Daha Fazla):** Gönderilen verinin daha fazla ek veriye sahip olup olmadığını gösterir. Bu değer **1** ise çerçeve ek veri gönderir. **0** ise ek veri göndermez.
- **W [WEP Encryption (WEP Şifreleme)]:** Şifreleme türünü gösterir. Bu değer **1** ise WEP şifreleme tekniği kullanılıyordur. **0** ise bu teknik kullanılmıyor anlamına gelir.
- **O [Order (Sıralama)]:** Sıralı veri iletim bilgisinin gösterildiği alandır. Bu değer **1** ise sıralı iletim yapılır. **0** ise sıralı iletim yapılmaz.

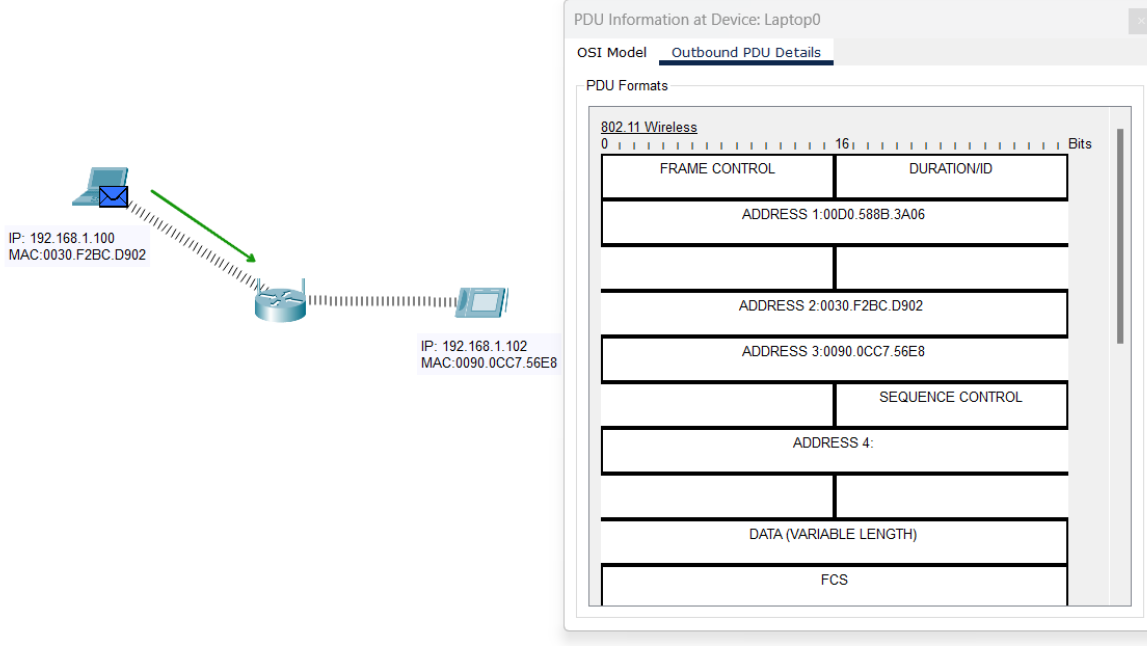
Duration (Süre): Çerçevenin ağ kaynaklarını kullanacağı süreyi gösteren alan veya çerçevenin tanımlayıcı ID'sidir.

Address (Adres): Adres alanı bilgileri, paketin hangi cihazdan gönderildiğine bağlı olarak değişiklik gösterir. Çerçeve kontrolünün altında bulunan To DS ve From DS değerlerine göre çerçevenin hangi cihazdan geldiği veya hangi cihaza gideceği belirlenir. İlk üç adres alanı, tüm kontrollerde yer alıyorken **Adres 4** alanı opsiyoneldir. Adres 4 alanı, köprü veya tekrarlayıcı gibi cihazlara çerçevenin yönlendirildiği durumlarda kullanılır. Adres bilgileri şu şekildedir:

- **To DS=0, From DS=0:** Çerçeve, doğrudan iki kablosuz istemci arasında iletilir. Adres 1 hedef cihazın MAC adresini, Adres 2 kaynak cihazın MAC adresini, Adres 3 erişim noktasının BSS bilgisini gösterir.
- **To DS=0, From DS=1:** Çerçevenin bir erişim noktasından bir istemciye yönlendirildiğini gösterir. Adres 1 hedef cihazın MAC adresi, Adres 2 erişim noktasının MAC adresi, Adres 3 kaynak cihazın adres bilgisini gösterir.
- **To DS=1, From DS=0:** Çerçevenin bir istemciden bir erişim noktasına yönlendirildiğini gösterir. Adres 1 hedef erişim noktasının MAC adresi, Adres 2 kaynak cihazın MAC adresi, Adres 3 hedef cihazın MAC adresi bilgisini gösterir.
- **To DS=1, From DS=1:** Çerçevenin bir erişim noktasından bir erişim noktasına yönlendirildiğini gösterir. Adres 1 hedef erişim noktasının MAC adresi, Adres 2 kaynak erişim noktasının MAC adresi, Adres 3 hedef erişim noktasının MAC adresi, Adres 4 köprü cihazının MAC adres bilgisini gösterir.

Sequence Control (Sıra Kontrol): Parçalanmış çerçevelerin doğru sırayla yeniden birleştirilmesini kontrol eden alandır.

Görsel 3.28'de kablosuz iki istemci arasında yapılan iletişim sırasında kablosuz istemciden kablosuz erişim noktasına yönlendirilen 802.11 Wireless çerçeve yapısı görülür.

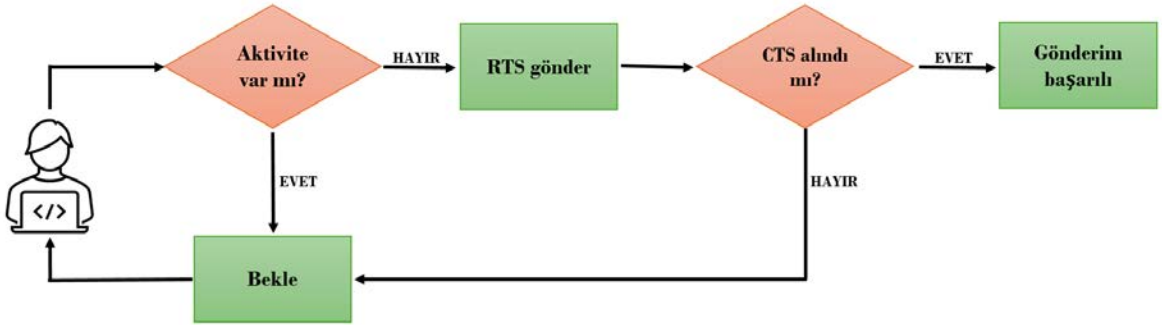


Görsel 3.28: 802.11 çerçeve yapısı

3.1.6. CSMA/CA (Carrier Sense Multiple Access With Collision Avoidance)

Bilgisayar ağlarında cihazların aynı anda veri gönderme isteği, ağda çarpışmaya sebep olur. Çarpışma algılandığında tüm cihazlar, çarpışma sinyalini alır ve veri gönderimini durdurur. Her cihaz, rastgele belirlediği bekleme süresinden sonra yeniden veri gönderimini dener. Kablolu ağlarda çarpışmayı tespit

etmek için CSMA/CD protokolü kullanılır. Kablolu ağlarda veriler kablo üzerinden aktarıldığı için veri hattının kontrol edilmesi mümkündür. Kablosuz ağlarda ise veriler hava ortamında yayılarak ilerlediği için çarpışmanın tespiti zordur. Bu sebeple kablosuz ağlarda çarpışmadan kaçınmayı sağlamak için CSMA/CA protokolü kullanılır (Görsel 3.29).

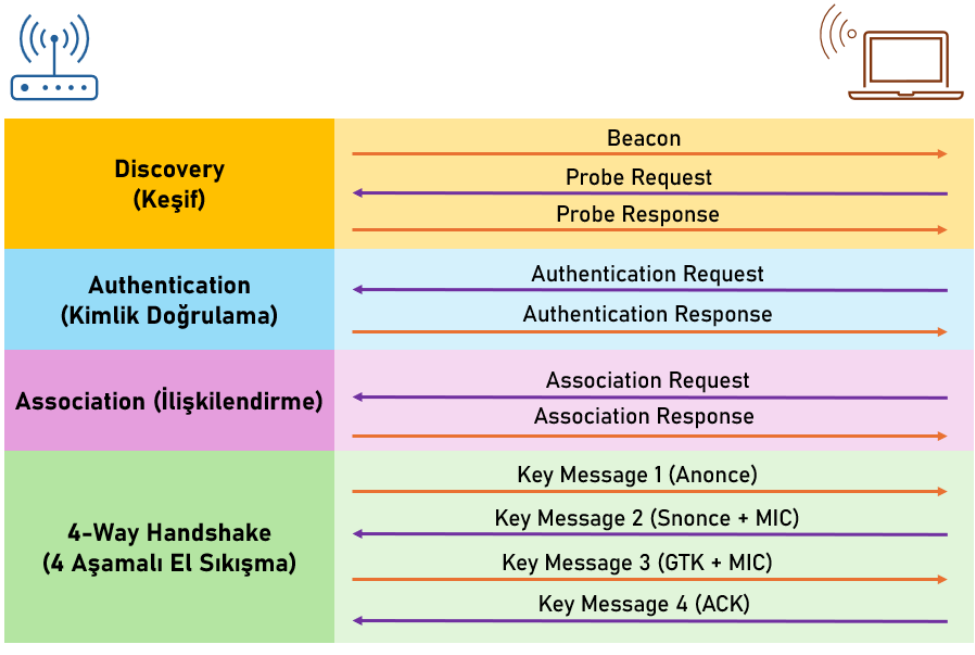


Görsel 3.29: CSMA/CA

CSMA/CA'da kullanıcının veri iletme isteğinden önce, devam eden bir veri akışının var olup olmadığı kontrol edilir. Eğer devam eden bir veri akışı varsa gönderici bekleme süresine girer. Eğer veri akışı yoksa kablosuz erişim noktasına RTS [Request to Send (Veri Gönderim İsteği)] gönderilir. Kablosuz erişim noktası meşgulse RTS reddedilir ve gönderici bekleme süresine girer. Meşgul değilse göndericiye CTS [Clear to Send (Gönderim Onayı)] gönderir. CTS onayından sonra kablosuz erişim noktası, göndericinin veri iletimi tamamlanana kadar diğer istekleri beklemeye alır.

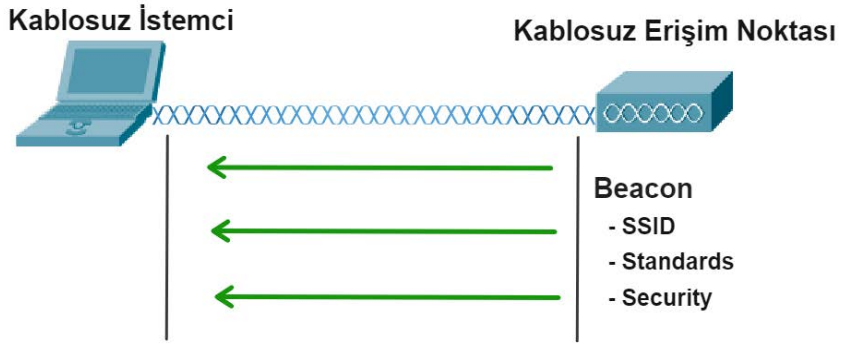
3.1.7. Kablosuz İstemcilerin Kablosuz Ağa Bağlanma Süreci

Kablosuz istemcilerin kablosuz bir ağa dâhil olabilmeleri için bir erişim noktası veya kablosuz yönlendiriciyle ilişkilendirilmesi gerekir. Bu süreçte kablosuz ağ keşfedilir, gerekli anlaşmalar sağlanır ve ağa bağlanma süreci tamamlanır. Kablosuz cihazlar arasında gerçekleşen sürecin aşamaları Görsel 3.30'da görülür.



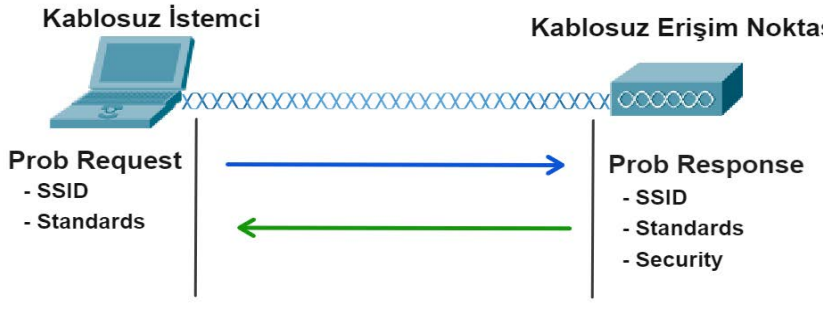
Görsel 3.30: Kablosuz bağlantı süreci

Discovery: Kablosuz cihazların birbirini keşfetmesi süreci aktif ve pasif olarak iki şekilde gerçekleşir. Pasif keşif sürecinde kablosuz erişim noktası veya yönlendiriciler, periyodik aralıklarla Beacon mesajı yayınlar. **Beacon** mesajında kablosuz erişim noktasının SSID bilgisi, desteklenen standartları ve güvenlik ayarları yer alır. Bu mesajlar, kablosuz istemcilerin ağ ve cihaz seçmesine yardımcı olur. Görsel 3.31'de kablosuz erişim noktasından yayınlanan **Beacon** mesajları görülür.



Görsel 3.31: Beacon mesajı

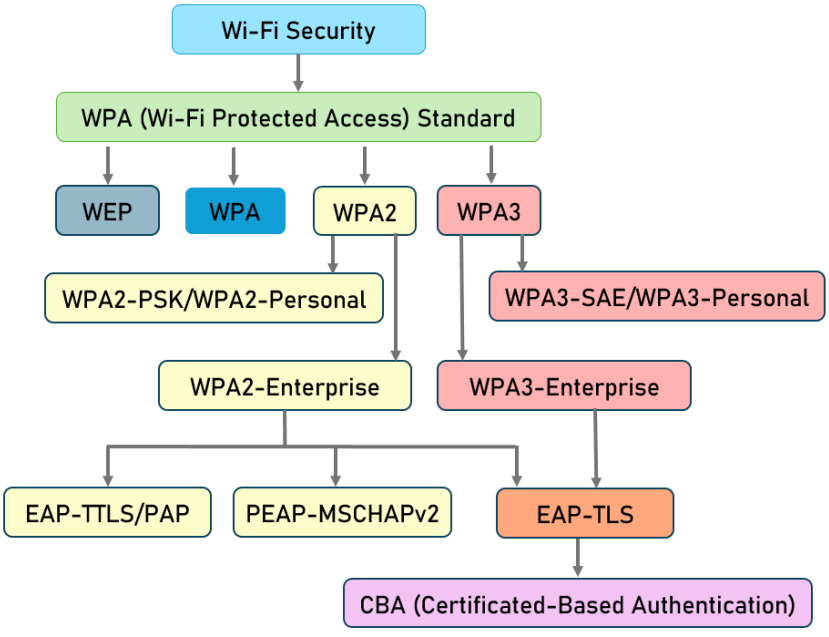
Aktif keşif sürecinde ise kablosuz istemciler, ağda aktif olan erişim noktalarını tespit etmek için **Prob Request** mesajı yayınlar. Bu mesajla SSID'si bilinen veya bilinmeyen bir ağın yapılandırma bilgileri talep edilir. Yapılandırma talebini alan kablosuz erişim noktaları, kendilerine ait yapılandırma bilgilerini içeren **Prob Response** mesajı yayınlar. Yanıt mesajları kablosuz istemcilerin uygun ağı seçmesine yardımcı olur. Görsel 3.32'de **Prob Request** ve **Prob Response** mesajları görülür.



Görsel 3.32: Prob mesajları

Authentication: Kimlik doğrulama süreci güvenli iletişimin sağlanmasında önemli bir aşamadır. Bu süreçte kullanıcılar veya cihaz kimlikleri doğrulanır. Ağa yetkisiz erişimin engellenmesi ve ağ güvenliğinin sağlanması açısından kimlik doğrulama kritik öneme sahiptir.

Kimlik doğrulama sürecinde kablosuz istemci, keşif aşamasında aldığı yanıtları kontrol eder. İletişim kurmak istediği ağın SSID ve şifreleme uyumluluğunu dikkate alarak düşük seviyeli 802.11 kimlik doğrulama çerçevesi gönderir. Kablosuz erişim noktası bu çerçeveyle kimlik doğrulama talebini alır ve kablosuz istemciye doğrulama çerçevesini yanıt olarak iletir. Görsel 3.33'te kimlik doğrulama protokollerinin hiyerarşisi görülür.



Görsel 3.33: Kimlik doğrulama protokolleri

Kimlik doğrulama sürecinde kullanılan yöntem ve protokoller şu şekildedir:

1. **Open Authentication:** Açık kimlik doğrulama yönteminde istemci cihaz, herhangi bir kimlik bilgisi olmadan ağa direkt katılır. Ağa erişim basittir fakat ağ güvenliği açısından zayıf bir yöntemdir. Herkese açık alanlardaki ağlarda tercih edilir.

2. **Wired Equivalent Privacy (WEP):** 802.11 kablosuz ağ standartlarında uygulanan ilk güvenlik protokolüdür. Paylaşılan gizli bir anahtar veya SSID ile veri şifreleme ve şifre çözme yöntemini kullanır.

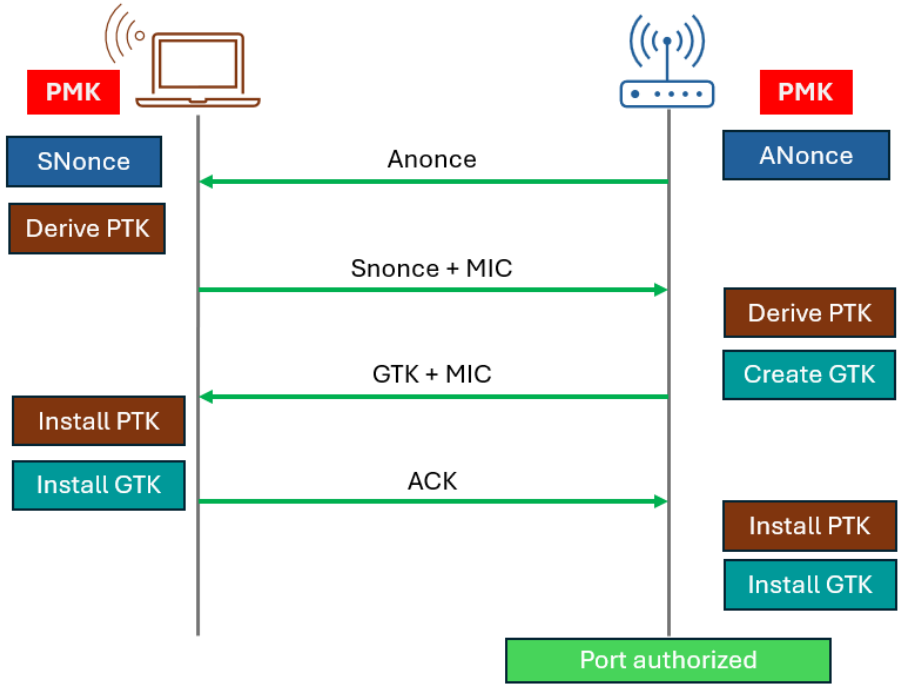
3. **Wi-Fi Protected Access (WPA):** WPA protokolü, daha güçlü şifreleme ve kimlik doğrulama yöntemiyle öne çıkar. 128 bitlik şifreleme yöntemi ile daha güçlü bir koruma sağlayarak kötü niyetli şifre çözme saldırılarının önüne geçer.

4. **Wi-Fi Protected Access2 (WPA2):** WPA'ya göre daha güvenli bir kimlik doğrulama protokolüdür. **AES (Advanced Encryption Standard)** şifreleme tekniğiyle güçlü parolalar oluşturur. **WPA2-PSK**, ev veya ofis gibi yönetilebilir küçük ağ ortamlarında tercih edilen bir yöntemdir. İstemciler, önceden belirlenen SSID ve parolayla ağa katılır. **WPA2-Enterprise** ise büyük ölçekli ağlarda merkezî bir **RADIUS** sunucu üzerinden kimlik doğrulama yapar. Her cihaz, şifrelenmiş özel bir tünel üzerinden kimlik doğrulamasının ardından ağa bağlanır.

5. **Wi-Fi Protected Access3 (WPA3):** 2018 yılında kullanılmaya başlanılan en güncel protokoldür. WPA2'ye kıyasla güvenlik açısından iyileştirmelerle öne çıkar. 192 bitlik şifrelemeyle daha yüksek güvenlik sağlarken kaba kuvvet saldırılarına karşı ek savunma yöntemlerini de kullanır. **WPA3-PSK** da ev veya ofis gibi yönetilebilir küçük ağ ortamlarında tercih edilir. **SAE (Simultaneous Authentication of Equals)** protokolüyle eş zamanlı kimlik koruması sağlar. Özellikle şifre kırma saldırıları için SAE daha güçlü bir koruma sunar. WPA3-Enterprise, daha büyük ve kurumsal ağlarda tercih edilir. Merkezî sunucu ve istemcilerin kimlik doğrulama sürecinde ek sertifika doğrulamaları da ister.

Association: Kimlik doğrulama sürecinden sonra ağ kaynaklarına erişim sağlamak için ilişkilendirme süreci gerçekleşir. Kablosuz istemci, kablosuz erişim noktasına bağlandıktan sonra **Association Request** isteği gönderir. Bu talebi alan kablosuz erişim noktası, **Association Response** ile ilişkilendirme cevabını iletir.

4-Way Handshake: Kablosuz istemci ve erişim noktası arasında ilişkilendirme süreci tamamlandıktan sonra veri aktarımı için güvenli bir bağlantı kurulur. Bu bağlantı, **EAPOL (Extensible Authentication Protocol Over LAN)** çerçeveleriyle sağlanır. EAPOL mesajlarıyla kablosuz ağda güvenli anahtar paylaşımı ve doğrulama işlemleri sağlanır. Kablosuz istemci ve erişim noktası arasında güvenli oturumun başlatılması sürecinde **PMK (Pairwise Master Key)** ortak anahtarı oluşturulur. Daha sonra istemci ve erişim noktası arasındaki bireysel oturum için PMK'den türetilen **PTK (Pairwise Transient Key)** geçici anahtarı oluşturulur. PTK, veri şifreleme ve kimlik doğrulama için kullanılan anahtardır. **GTK (Group Temporal Key)** ise çoklu istemciler için oluşturulan grup anahtarıdır. Grup seviyesinde şifreleme ve doğrulama yapar. Görsel 3.34'te EAPOL çerçevelerinin iletimi ile gerçekleşen 4-Way Handshake aşamaları görülür.



Görsel 3.34: 4-Way Handshake aşamaları

4-Way Handshake mesajları şu şekildedir:

1. **Anonce:** Erişim noktası tarafından oturumu başlatmak için kullanılan rastgele oluşturulmuş bir sayı değeridir.

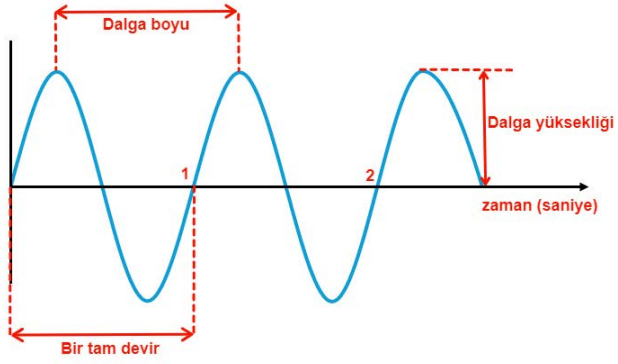
2. **Snonce + MIC:** İlk mesajı aldıktan sonra oturum açmak için kablosuz istemcinin oluşturduğu sayı değeridir. Bu mesajla birlikte mesajın bütünlüğünü kontrol eden **MIC (Message Integrity Code)** kodu gönderilir.

3. **GTK + MIC:** İstemciden gelen ikinci mesaja yanıt olarak kendi şifreleme anahtarını ve doğrulama bilgilerini ekler.

4. **ACK:** Erişim noktasından gelen mesajın doğruluğu onaylanır ve oturum başlatılır.

3.1.8. 2.4 GHz ve 5 GHz Frekanslarının Kanal Yapısı

Frekans, bir sinyalin bir saniyede yaptığı tam devir sayısıdır. Frekans ölçü birimi **Hertz (Hz)** ile ifade edilir. Dalga boyu, sinyalin iki tepe noktası arasındaki uzaklıktır. **Dalga boyu**, frekansla ters orantılıdır. Frekans arttıkça dalga boyu kısalır. **Dalga yüksekliği** ise sinyalin gücünü ifade eder. Görsel 3.35'te bir frekansın zaman çizelgesinde yaptığı dalgalar görülür.

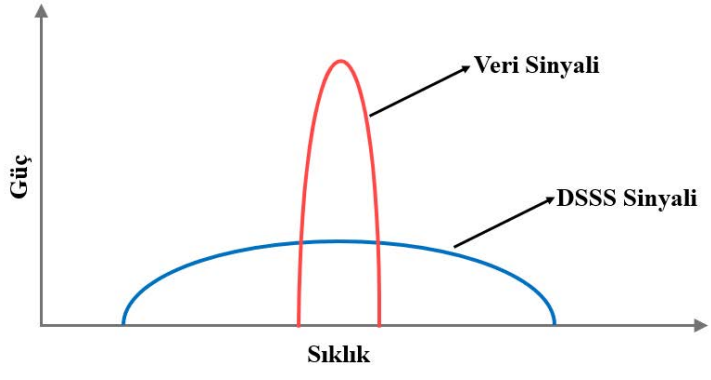


Görsel 3.35: Frekans

Kablosuz iletişimde frekans, veri iletim hızını ve sinyalin kapsama alanını doğrudan etkiler. **Kanal** ise belirli bir frekans bandının aralıklara bölünerek ifade edilmesidir. Frekans bandında oluşan parazitleri en aza indirmek, veri iletim hızını optimize etmek ve kapsama alanını genişletmek için kanallar kullanılır. Kablosuz ağ ortamında, bir kanala talebin çok artması kanalın doygunluğuna sebep olur ve iletişimin kalitesi düşer. Kanal doygunluğunu azaltmak ve kanalı daha verimli hâle getirmek için kullanılan modülasyon tekniklerinden bazıları şunlardır:

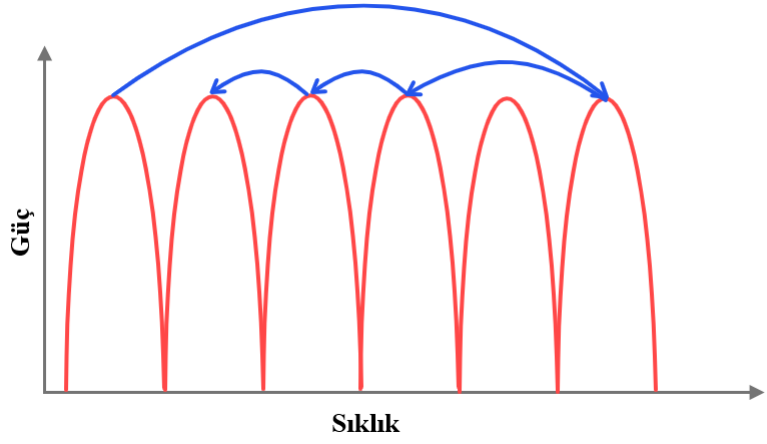
DSSS [Direct-Sequence Spread Spectrum (Doğrudan Sıralı Yayılmış Spektrum)]: Bir sinyalin daha geniş bir frekans bandına yayılarak iletilmesini sağlar. Bu tekniğin amacı, sinyalin diğer sinyallerle karışmasını önlemek ve parazitlere karşı daha dayanıklı olmasını sağlamaktır.

DSSS, 802.11b cihazları tarafından kullanılan bir tekniktir. Bu yöntemde veri sinyali, yayılma kodlarıyla modüle edilir. Böylece aynı frekansta birden fazla veri sinyali, farklı yayılma kodları kullanılarak birbirinden ayırt edilebilir. DSSS sinyalinin veri sinyalini geniş bir frekans bandına yayarak iletmesi Görsel 3.36'da görülür.



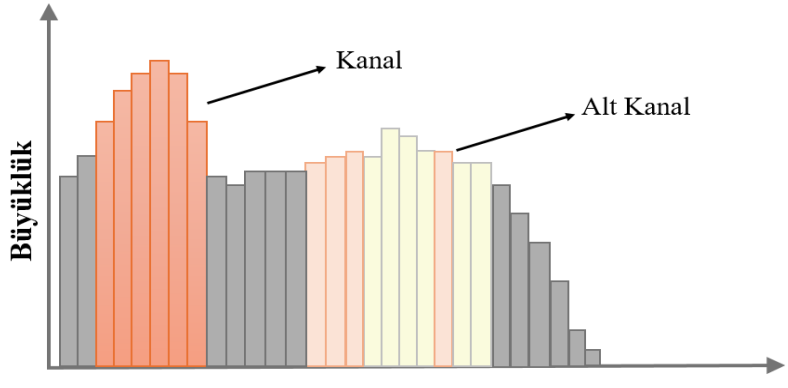
Görsel 3.36: DSSS

FHSS [Frequency Hopping Spread Spectrum (Frekans Atlamalı Yayılmış Spektrum)]: Bir sinyalin belirli aralıklarla frekans atlayarak iletilmesini sağlar. Bu teknikte, FHSS sinyali ile gönderici ve alıcı cihaz arasında eş zamanlı sıçrama bilgisi kullanılır. Çok kısa aralıklarla yapılan bu işlemle veri sinyalleri, parazit oluşumuna karşı korunur fakat veri iletim hızı daha düşüktür. Bu, 802.11 standartlarında kullanılan tekniktir. FHSS sinyali ile frekans atlaması Görsel 3.37'de görülür.



Görsel 3.37: FHSS

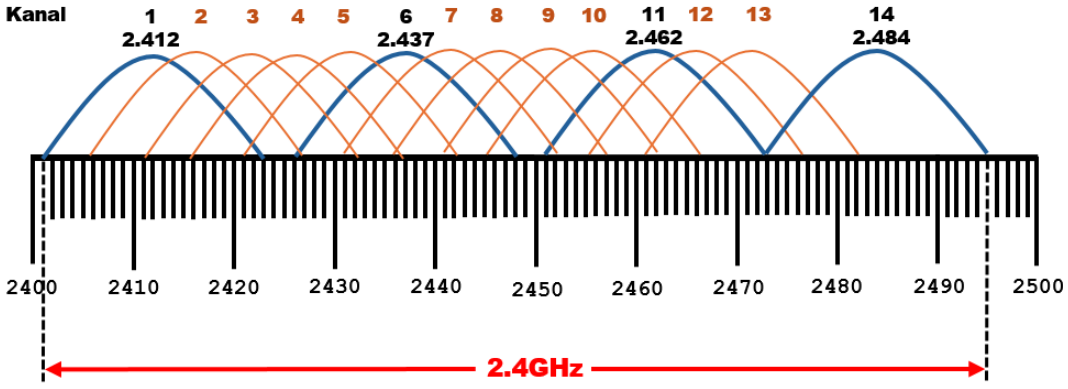
OFDM [Orthogonal Frequency-Division Multiplexing (Ortagonal Frekans Bölmeli Çoklama)]: Bir sinyalin frekans bandını birden fazla alt banda bölerek iletilmesini sağlar. Bu teknikte frekanslar birbirine ortagonaldir. **Frekansların ortagonal olması**, frekansların birbirine dik olarak üst üste gelmesini ifade eder. Alt frekans bandında sinyaller, eş zamanlı olarak iletilir ve birbirini etkilemez. Bu sebeple veri iletim hızı yüksektir ve parazit oluşumuna karşı güvenlidir. 802.11 a/g/n/ac tarafından kullanılan tekniktir. 802.11ax ise OFDMA'yı (Ortogonal Frekans Bölmeli Çoklu Erişim) kullanır. Görsel 3.38'de OFDM ile kanalların alt kanallara bölünmesiyle yapılan veri iletimi görülür.



Görsel 3.38: OFDM

Kablosuz erişim ortamında, birden çok erişim noktası kullanıldığında kanallar çakışabilir. Doğru bir yapılandırma ve kanal seçimi ile bu sorunun önüne geçilir. IEEE 802.11 standardında kullanılan kanallar şu şekildedir:

2.4 GHz Kanal Yapısı: 2.4 GHz frekans bandında yer alan kanallar ve frekansları Görsel 3.39'da görülür. Her bir kanal 5 MHz'lik aralıklarla ayrılır. Bu aralıklar, birbiri içine geçmiş örtük frekans aralıklarıdır.



Görsel 3.39: 2.4 GHz kanal yapısı

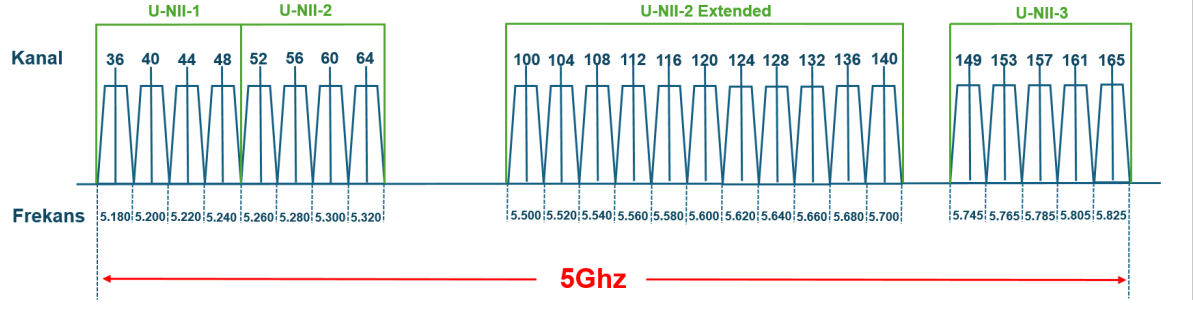
Görsel 3.39'a göre **1** numaralı kanal 2.401 GHz ile 2.423 GHz aralığında çalışır. **2** numaralı kanalın ise 2.406 GHz'ten başladığı görülür. Birbirine yakın kanallar, örtük frekans bandında yer aldıkları için parazit ve çakışma sorunları yaşanabilir. Bu sorunu önlemek için birden fazla erişim noktasının bulunduğu ağlarda birbirinden uzak ve örtük olmayan kanallar tercih edilmelidir. 2.4 frekans bandında 1, 6 ve 11 numaralı kanallar çakışmaz.

Tablo 3.2'de 2.4 GHz frekans bandında yer alan kanallar, numaraları ve frekansları görülür. Bu kanalların kullanımı bulunulan ülkeye göre değişiklik gösterebilir. Kuzey Amerika'daki ülkeler 11. kanala kadar kullanırken diğer ülkelerde 12 ve 13. kanallar kullanılır. 14 numaralı kanal ise sadece Japonya'da kullanılır.

Tablo 3.2: 2.4 GHz Kanalları ve Frekansları

Kanal	1	2	3	4	5	6	7	8	9	10	11	12	13	14
Frekans (MHz)	2412	2417	2422	2427	2432	2437	2442	2447	2452	2457	2462	2467	2472	2484

5 GHz Kanal Yapısı: 5 GHz frekans bandında yer alan kanallar (Görsel 3.40), 20 GHz'lik frekanslarla birbirinden ayrılır. Kanallar arasında örtük bir frekans aralığı yoktur. Dolayısıyla herhangi bir çakışma söz konusu değildir. 5 GHz frekans bandı, **U-NII (Unlicenced National Information Infrastructure)** olarak ifade edilen alt frekans bantlarına ayrılır. Kablosuz istemcilerin çok fazla olduğu ağlarda hızlı veri iletimi sağlar. Ayrıca bant genişliğini ve veri hızını arttırmak için kanal birleştirme yapılabilir. 20 Mhz'lik kanallar 40 Mhz, 80 Mhz veya 160 Mhz'lik kanallara birleştirilir. Yüksek performanslı uygulamalar ve geniş ağ kapasitesi için kullanışlı bir yöntemdir.



Görsel 3.40: 5 GHz kanal yapısı

Tablo 3.3'te 5 GHz frekans bandında yer alan kanallar ve frekansları görülür.

Tablo 3.3: 5 GHz Kanalları ve Frekansları

Kanal Numarası	Frekans	Bant Tanımı
36	5180	U-NII-1
40	5200	U-NII-1
44	5220	U-NII-1
48	5240	U-NII-1
52	5260	U-NII-2
56	5280	U-NII-2
60	5300	U-NII-2
64	5320	U-NII-2
100	5500	U-NII-2 Extended
104	5520	U-NII-2 Extended
108	5540	U-NII-2 Extended
112	5560	U-NII-2 Extended
116	5580	U-NII-2 Extended
120	5600	U-NII-2 Extended
124	5620	U-NII-2 Extended
128	5640	U-NII-2 Extended
132	5660	U-NII-2 Extended
136	5680	U-NII-2 Extended
140	5700	U-NII-2 Extended
149	5745	U-NII-3
153	5765	U-NII-3
157	5785	U-NII-3
161	5805	U-NII-3
165	5825	U-NII-3

3.2. KABLOSUZ AĞ YAPILANDIRMASI

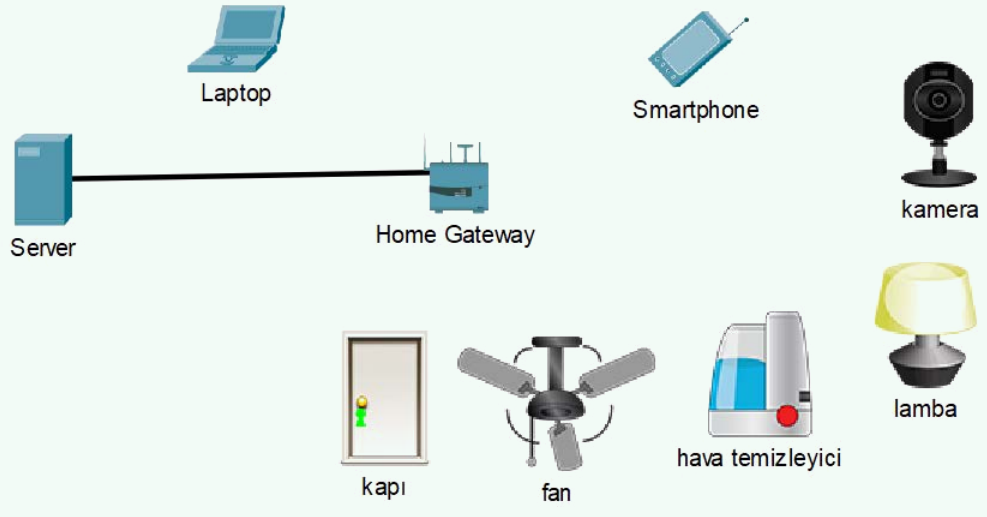
Kablosuz ağ yapılandırmasında ilk adım, kablosuz ağ cihazının yönetim arayüzü üzerinden yapılandırma yapılmasıdır. Bu aşamada kablosuz ağ adı (SSID), erişim şifresi, güvenlik protokolü gibi temel bilgiler belirlenir. Kablosuz ağın ihtiyacına göre gelişmiş yapılandırma seçenekleri ile kablosuz ağın özelleştirilmesi de mümkündür. Dış kullanıcılar için misafir ağının oluşturulması, belirli cihazların ağa bağlanabilmesi için MAC filtreleme işlemi, ağ yoğunluğuna göre frekans seçimi, kapsama alanı için frekans bandı seçimi, frekans seçimi vb. yapılabilecek özelleştirmelerden bazılarıdır.

1. UYGULAMA

Ad-Hoc modu ile akıllı ev sistemi oluşturma işlemini verilen adımlar doğrultusunda gerçekleştiriniz.

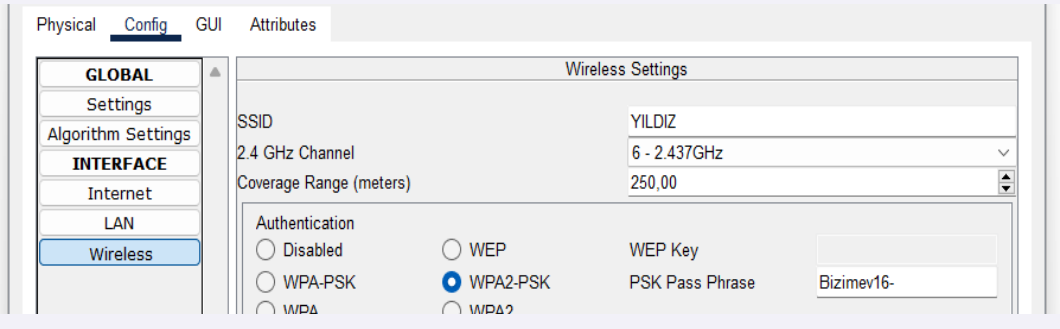
1. Adım: Ağ simülasyon programını çalıştırınız.

2. Adım: Görsel 3.41'deki ağ topolojisini hazırlayınız.



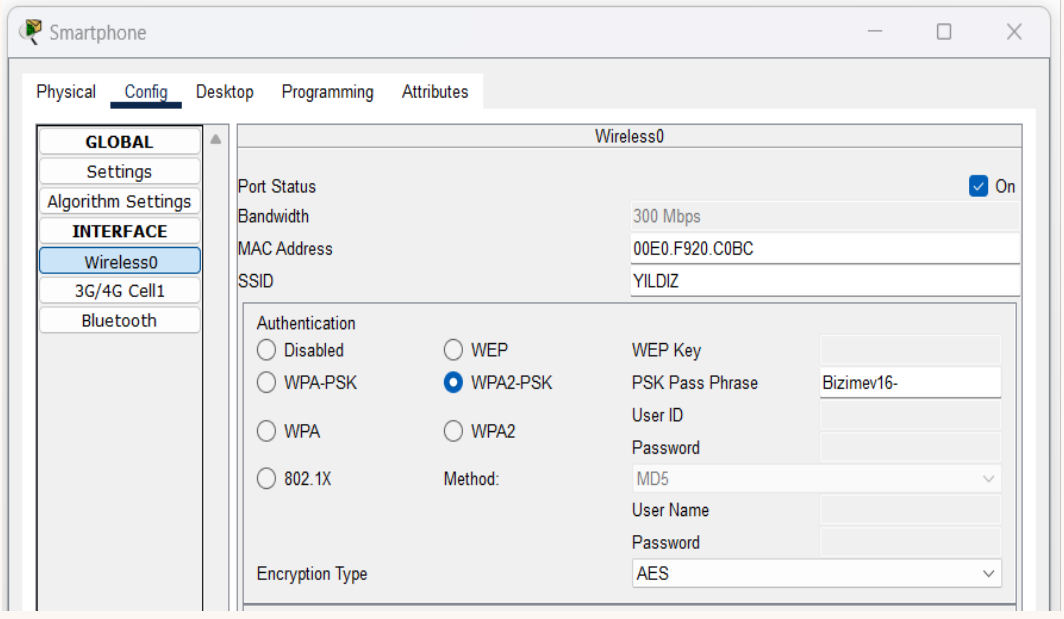
Görsel 3.41: 1. uygulama için ağ topolojisi

3. Adım: Home Gateway cihazının kablosuz ağ ayarlarından ağın görünür adını **YILDIZ** ve şifresini **Bizimev16-** olarak değiştiriniz (Görsel 3.42).



Görsel 3.42: Kablosuz ağ ayarları

4. Adım: Görsel 3.43'te **Smartphone** cihazının Home Gateway cihazına kablosuz bağlantısı görülür. Siz de **Laptop** ve **IoT** cihazlarının kablosuz ağ bağlantısını sağlayınız.



Görsel 3.43: SSID ve şifre ile bağlantı sağlanması

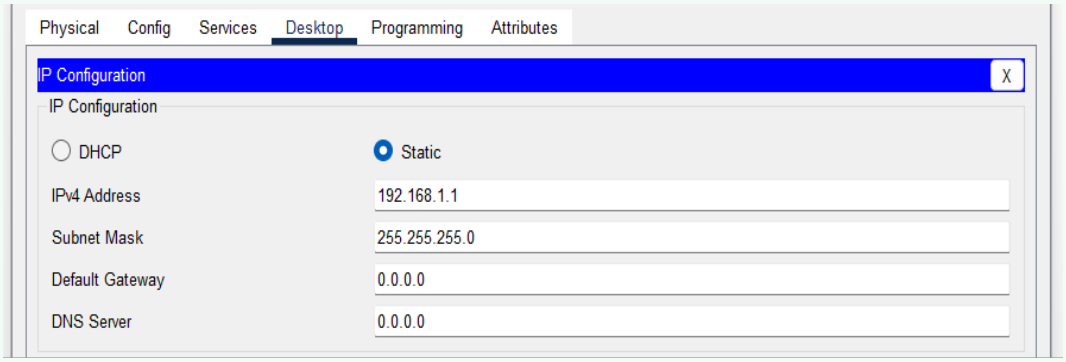
NOT: Laptop cihazının kablosuz bağlantısı için wireless modülünün eklenmesi gerekir.

5. Adım: Tablo 3.4'teki yapılandırma bilgilerine göre ağ cihazlarının IP yapılandırmalarını yapınız.

Tablo 3.4: IP Yapılandırması

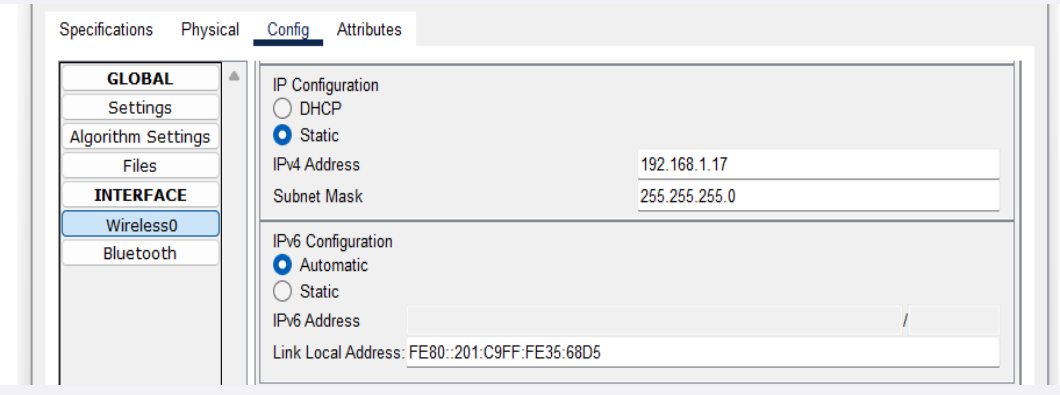
CİHAZ ADI	IP ADRESİ
Server	192.168.1.1
Laptop	192.168.1.11
Smartphone	192.168.1.12
kamera	192.168.1.13
lamba	192.168.1.14
hava temizleyici	192.168.1.15
fan	192.168.1.16
kapı	192.168.1.17

6. Adım: Görsel 3.44'te **Server** cihazının IP yapılandırma bilgisi görülür. Siz de **Laptop** ve **Smartphone** cihazlarının IP yapılandırmasını yapınız.



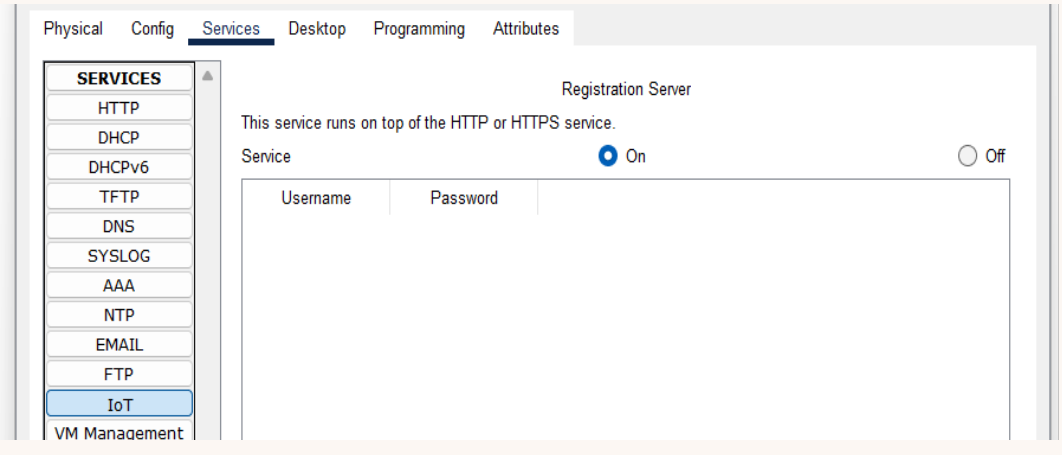
Görsel 3.44: Server IP yapılandırması

7. Adım: Görsel 3.45'te **kapı** cihazının IP yapılandırması görülür. Siz de diğer IoT cihazlarının IP yapılandırmasını yapınız.



Görsel 3.45: Kapı cihazı IP yapılandırması

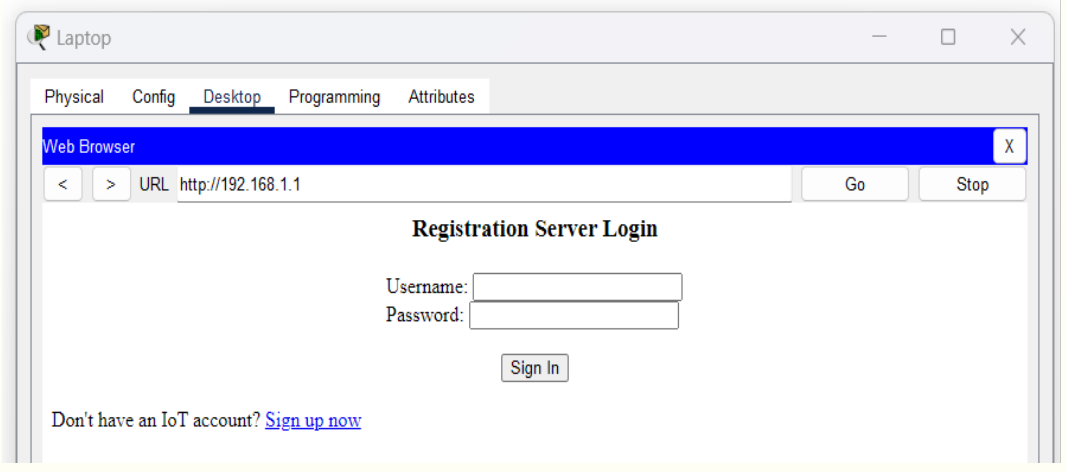
8. Adım: Server cihazında IoT hizmetini aktif ediniz (Görsel 3.46).



Görsel 3.46: IoT hizmetini aktif yapma

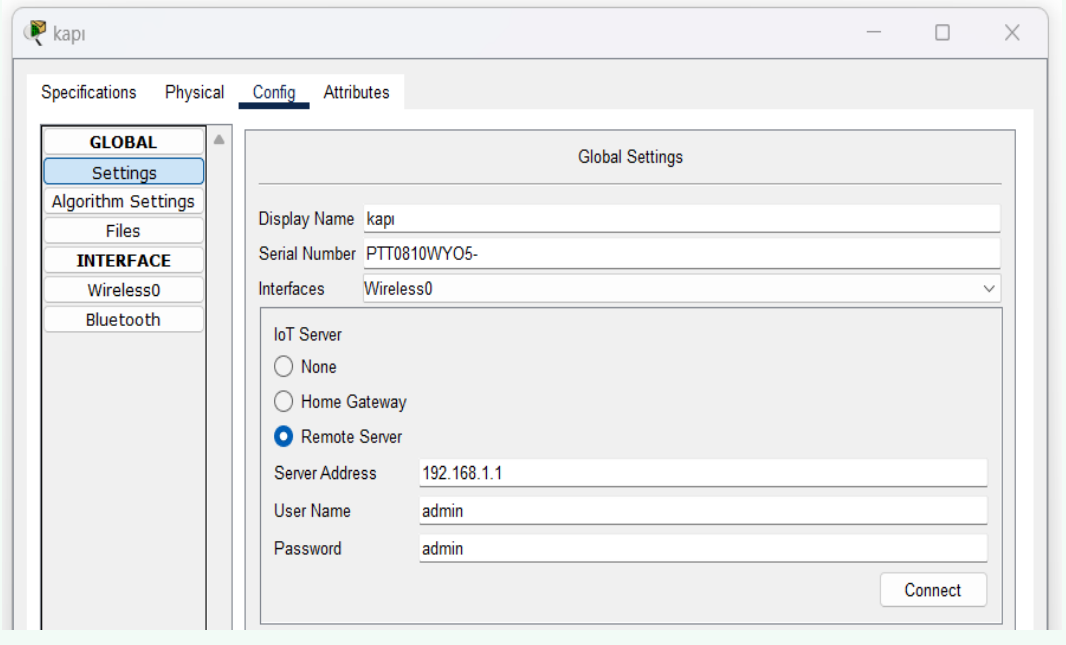
9. Adım: IoT cihazlarının uzaktan kontrolü için Laptop veya Smartphone cihazından sunucuya bağlanarak kullanıcı adı ve şifre ile erişim sağlayınız (Görsel 3.47).

NOT: Sunucu ile kurulan ilk bağlantıda **Sign up now** seçeneğiyle yeni bir kullanıcı adı ve şifre belirlenir. Daha sonraki erişimlerde web sayfası üzerinden sunucunun IP adresi ile bağlantı, belirlenen kullanıcı adı ve şifreyle sağlanır.



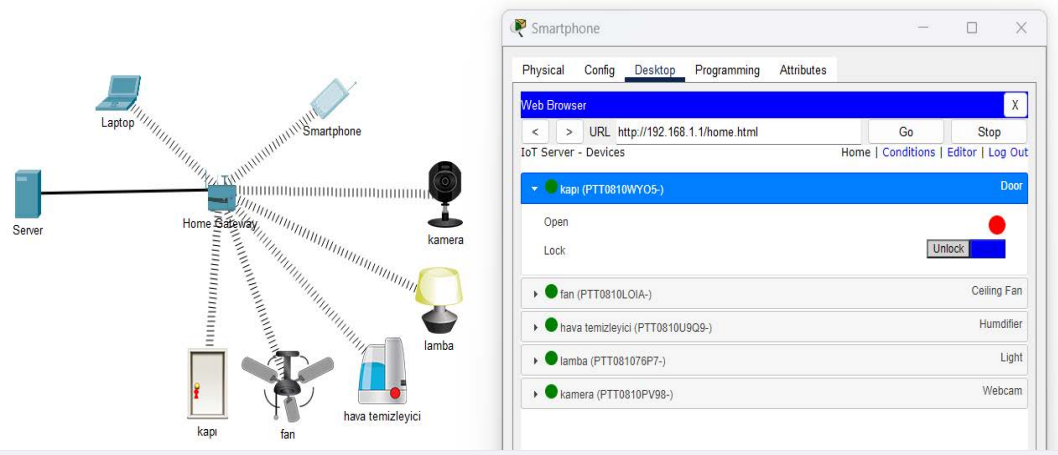
Görsel 3.47: IoT cihaz yönetimi için bağlantı

10. Adım: Görsel 3.48'de kapı cihazının uzaktan kontrolü için sunucu bağlantısı görülür. Siz de diğer IoT cihazlarının sunucu bağlantısını yapınız.



Görsel 3.48: IoT cihazında sunucu bağlantısı oluşturma

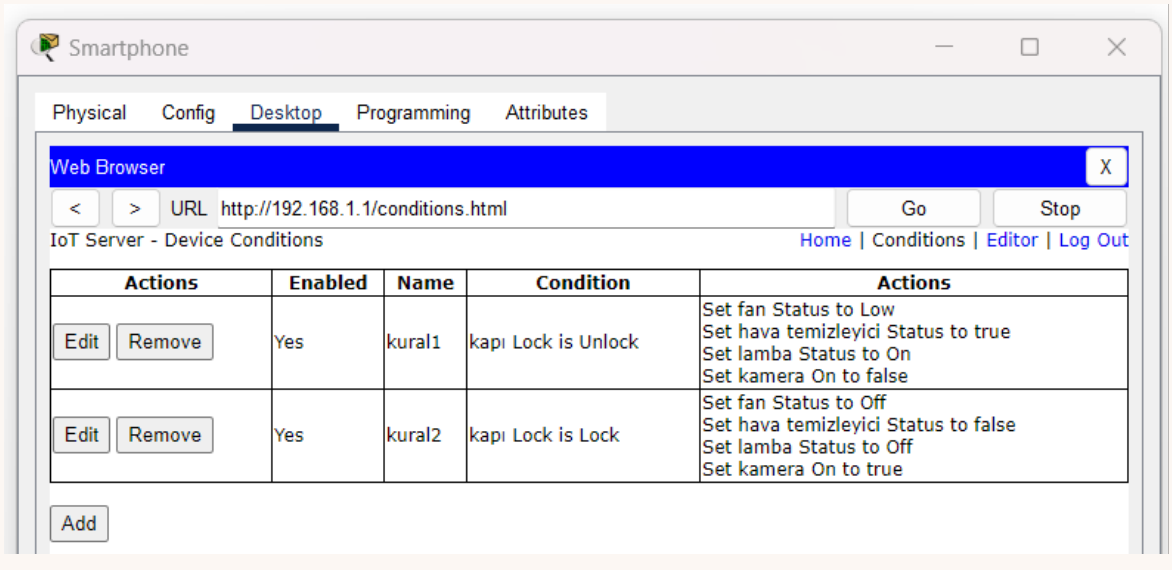
11. Adım: Smartphone cihazından kontrol edilebilir IoT cihazlarını görüntüleyiniz (Görsel 3.49).



Görsel 3.49: IoT cihazlarını görüntüleme

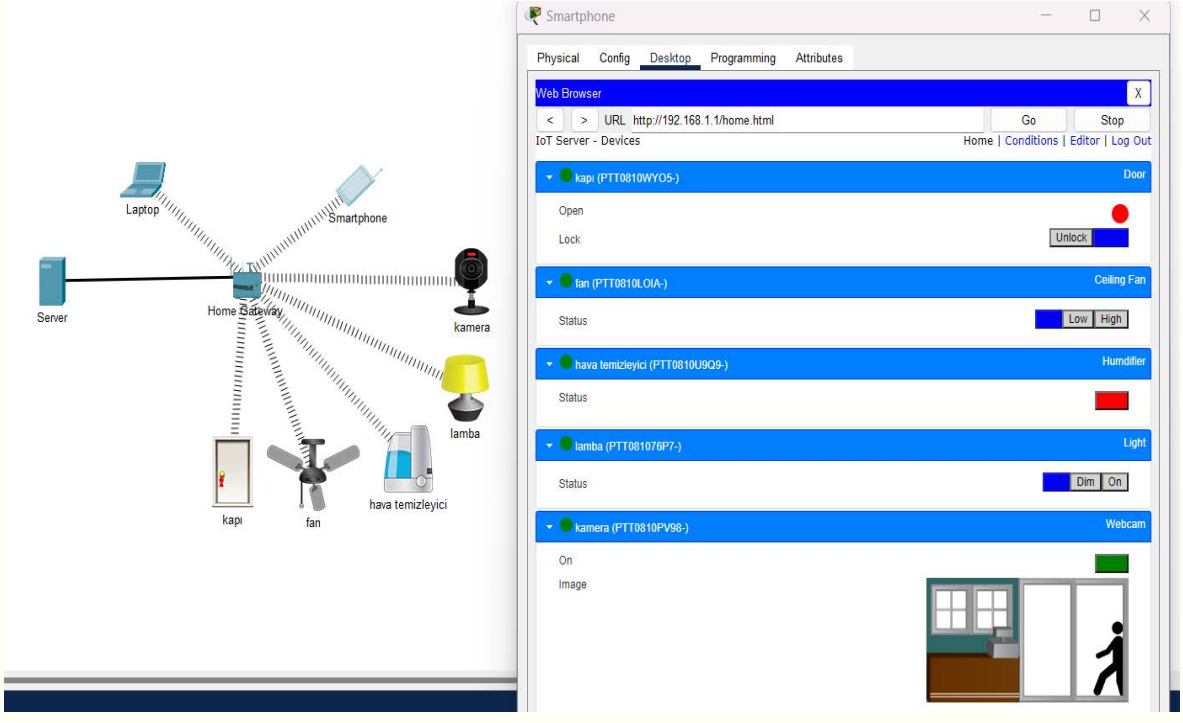
12. Adım: Kapı kilidi açıldığında lamba, fan ve hava temizleyicinin çalışmasını ve kameranın kapanmasını sağlayan kontrolü ekleyiniz [Kapı kilitlendiğinde kamera çalışmalı; lamba, fan ve hava temizleyici kapanmalıdır (Görsel 3.50).].

NOT: IoT cihazları için koşullar, kontrol penceresinden **Conditions** sekmesiyle yönetilir.



Görsel 3.50: IoT yönetiminde koşul oluşturma

13. Adım: Akıllı ev sisteminden kapının kilitlenip açılmasının kontrolünü yapınız (Görsel 3.51).



Görsel 3.51: IoT cihazların çalışması

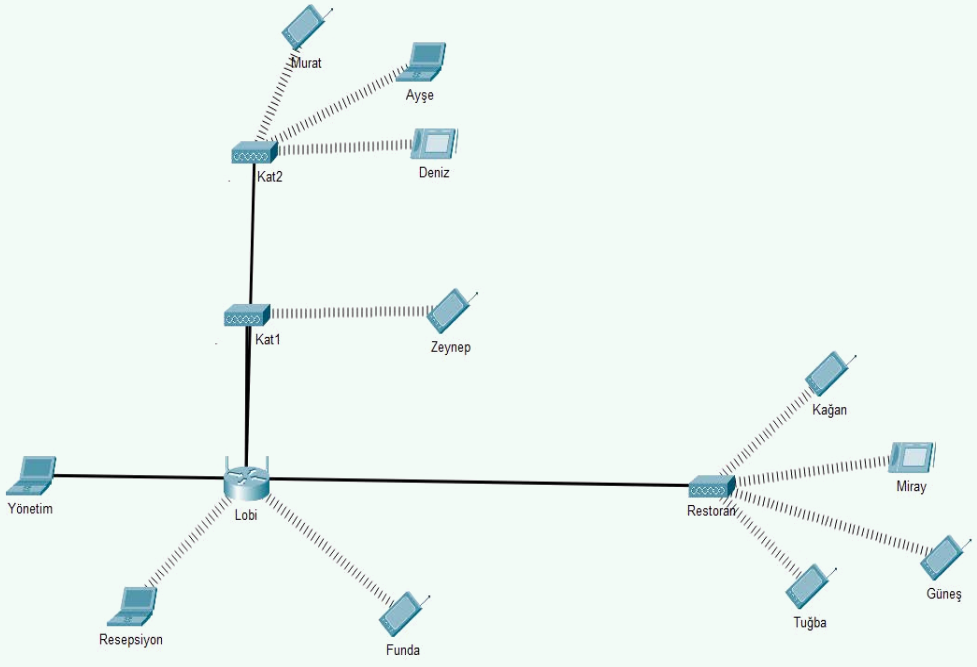
Bir otelde kablosuz cihazlarla Infrastructure Modu ile yerel alan ağı oluşturulmak istenir. Kablosuz yönlendiricinin yapılandırması **Yönetim** bilgisayarı tarafından kontrol edilir. Hem **Lobi** ve **Restoran** katında hem de diğer katlarda (Kat1 ve Kat2) kablosuz ağ erişimini sağlama işlemini verilen adımlar doğrultusunda gerçekleştiriniz.

2. UYGULAMA

NOT: Lobi cihazıyla sadece **Resepsiyon** bilgisayarı 5 GHz bağlantı kuracaktır. Aynı zamanda misafir kullanıcılar için ayrı bir erişim sağlanmalıdır. **Lobi** cihazı ile aynı şifre ve SSID bilgisine sahip **Restoran** erişim noktası da ağın genişletilmesini sağlayacaktır.

1. Adım: Ağ simülasyon programını çalıştırınız.

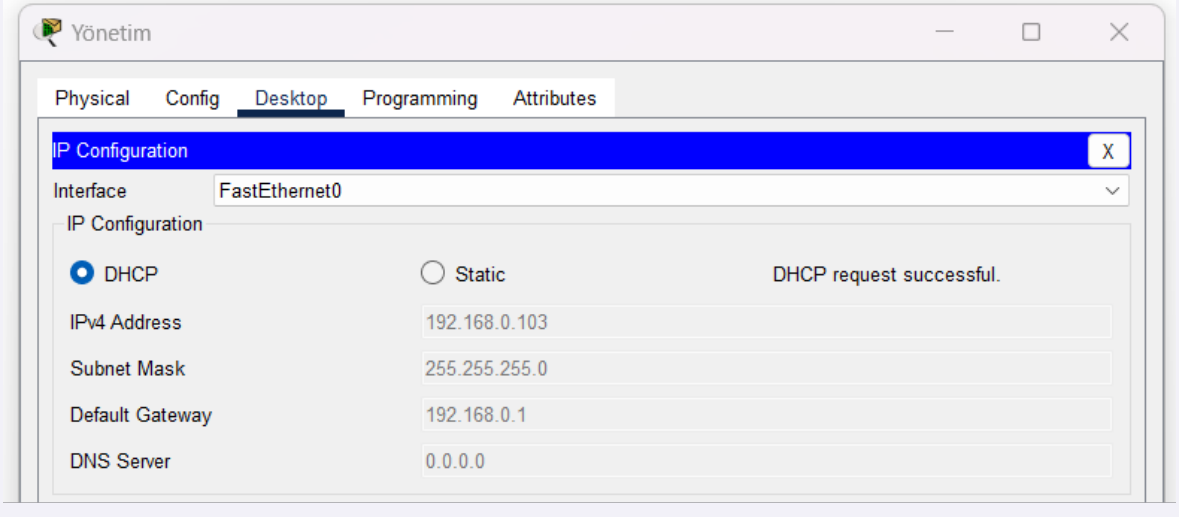
2. Adım: Görsel 3.52'deki ağ topolojisini hazırlayınız.



Görsel 3.52: 2. uygulamanın ağ topolojisi

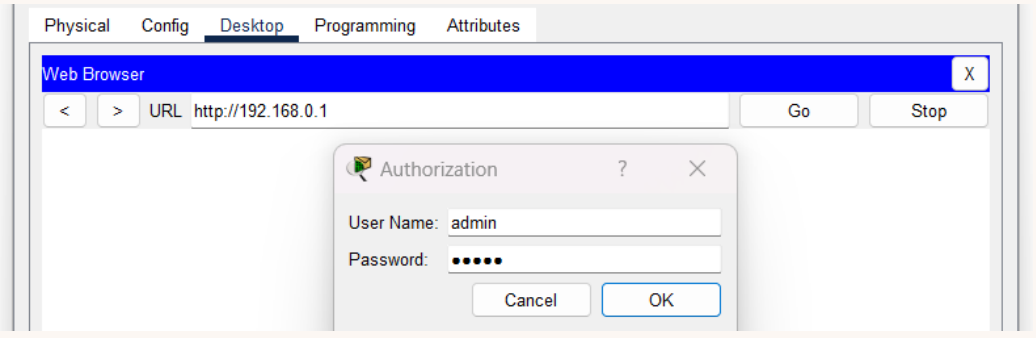
NOT: Kablosuz bağlantı için dizüstü bilgisayarlara wireless modülü eklenmelidir.

3. Adım: Yönetim bilgisayarının otomatik IP almasını sağlayınız (Görsel 3.53).



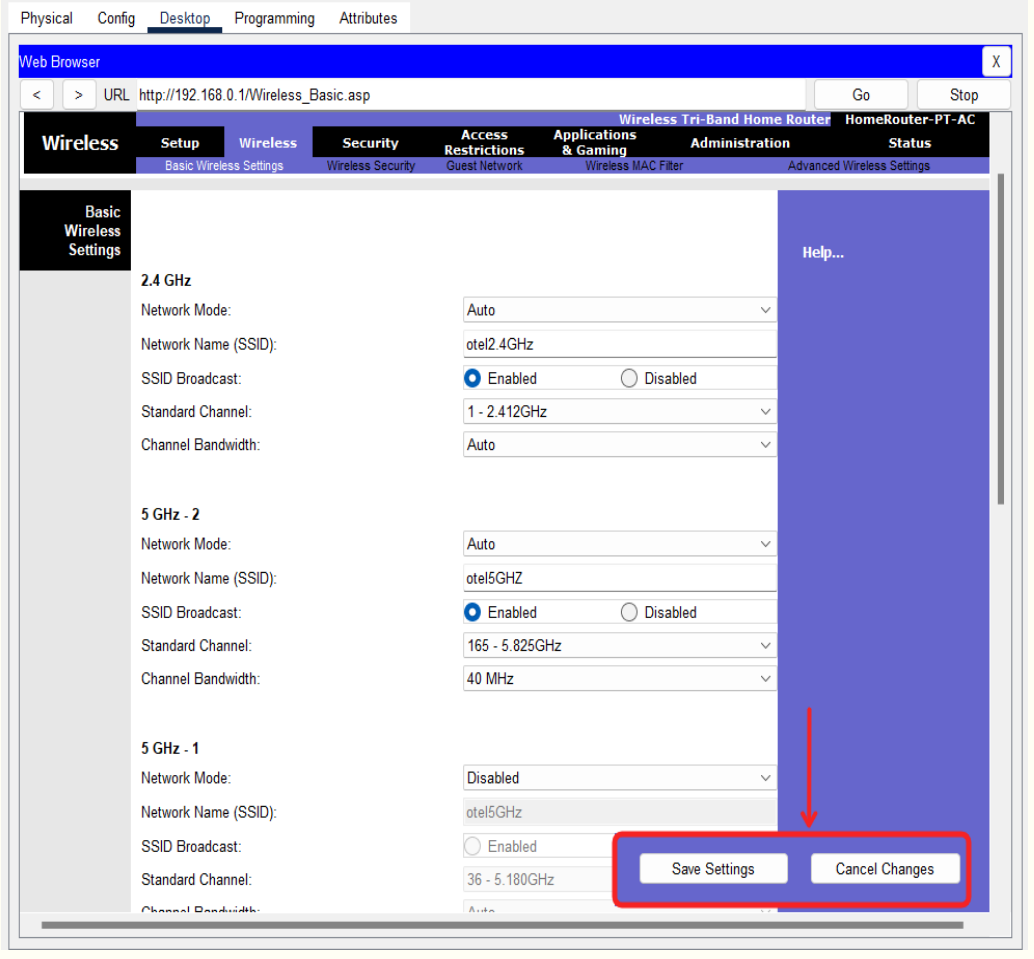
Görsel 3.53: Yönetim bilgisayarının IP yapılandırması

4. Adım: Yönetim bilgisayarından kablosuz yönlendiricinin yapılandırma arayüzüne erişim sağlayınız (Görsel 3.54).



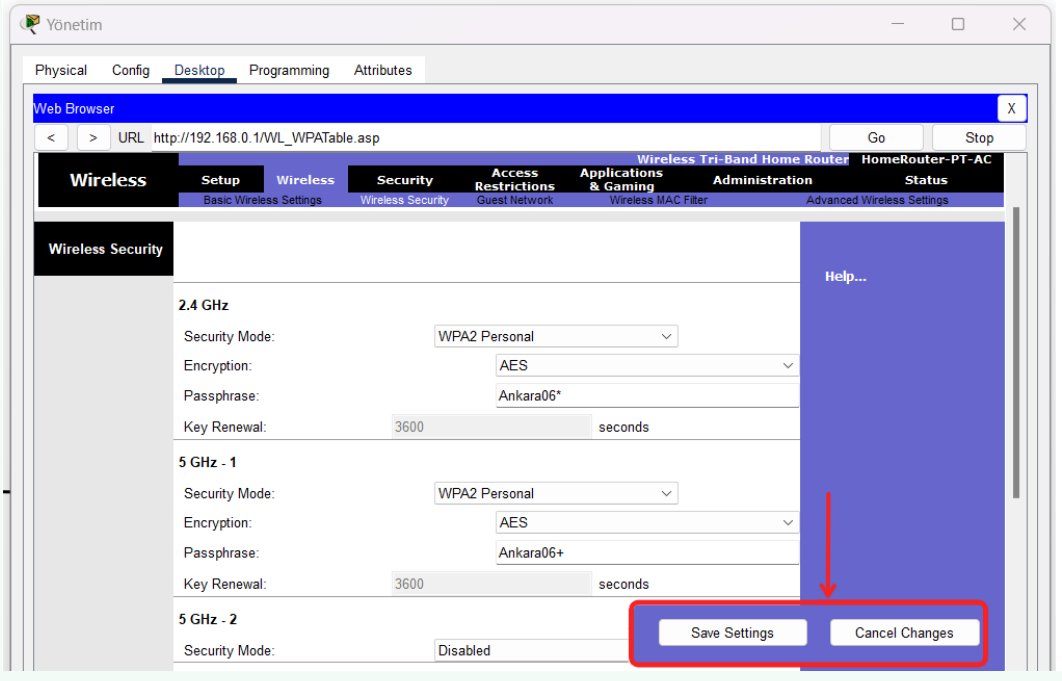
Görsel 3.54: Kablosuz erişim cihazının yapılandırma arayüzüne giriş

5. Adım: Kablosuz yönlendiricinin temel kablosuz ağ ayarlarından 2.4 GHz ve 5 GHz frekanslarının görünür adını, kanal bilgisini ve bant genişliğini değiştirip kaydediniz (Görsel 3.55).



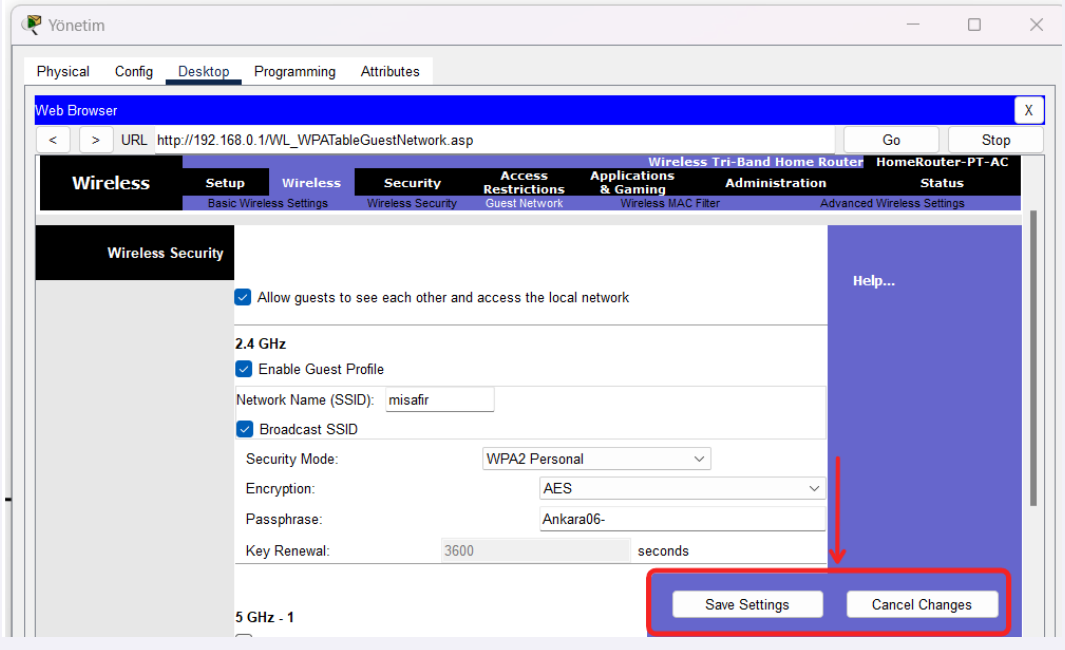
Görsel 3.55: Temel kablosuz ağ ayarları

6. Adım: Kablosuz yönlendiricinin kablosuz güvenlik seçeneklerinden 2.4 GHz ve 5 GHz frekansları için şifre oluşturunuz (Görsel 3.56).



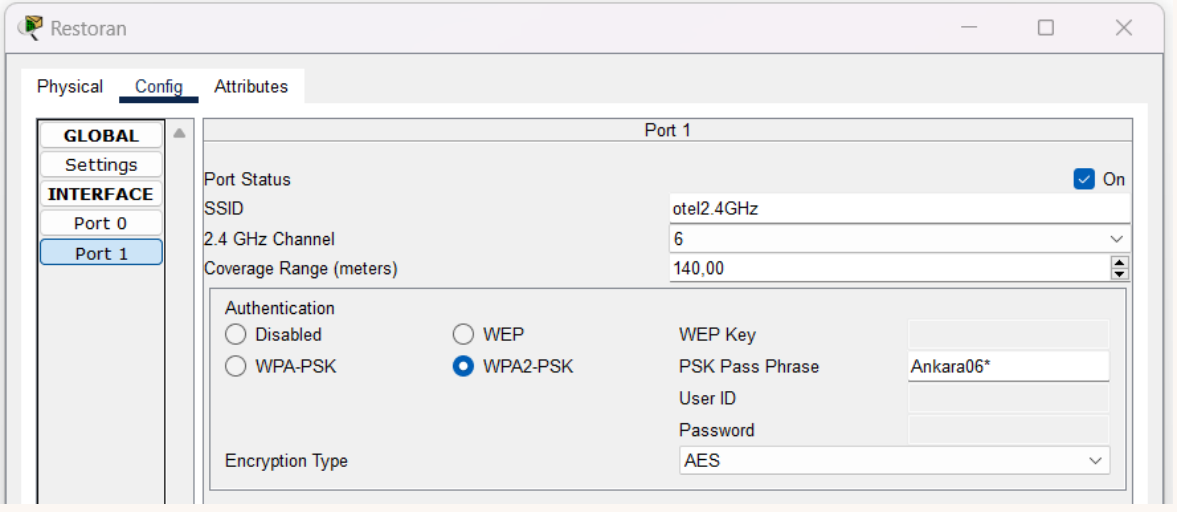
Görsel 3.56: Frekans bantları için şifre belirleme

7. Adım: Misafir kullanıcılar için 2.4 GHz frekansında profil oluşturunuz (Görsel 3.57).



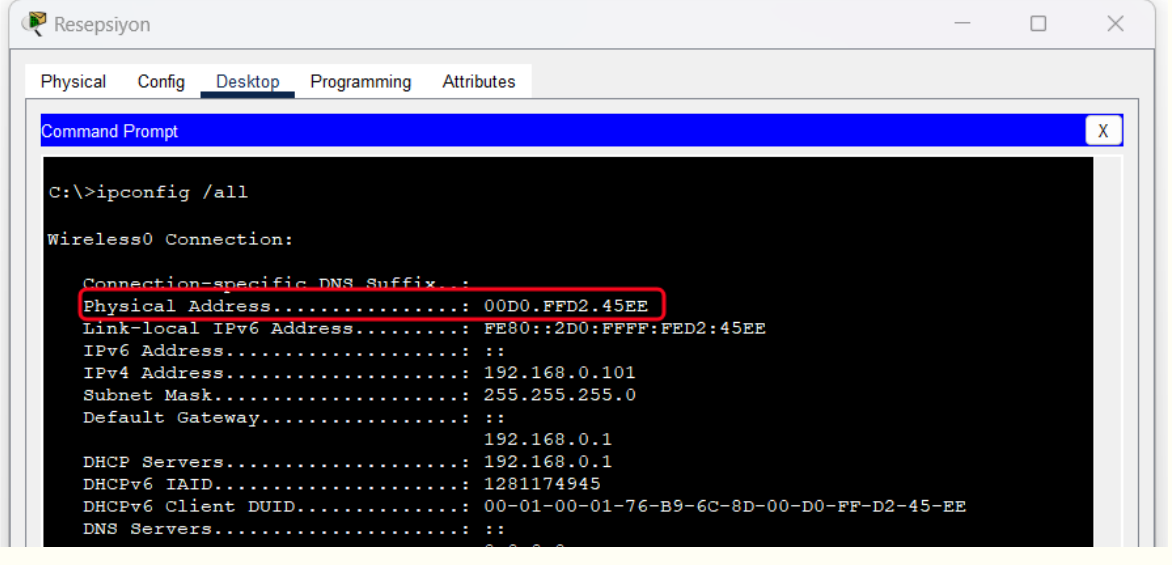
Görsel 3.57: Kablosuz ağda misafir kullanıcı profili oluşturma

8. Adım: **Restoran** isimli erişim noktasının görünür adını ve şifresini **Lobi** cihazıyla aynı olacak şekilde uygulayınız (Görsel 3.58).



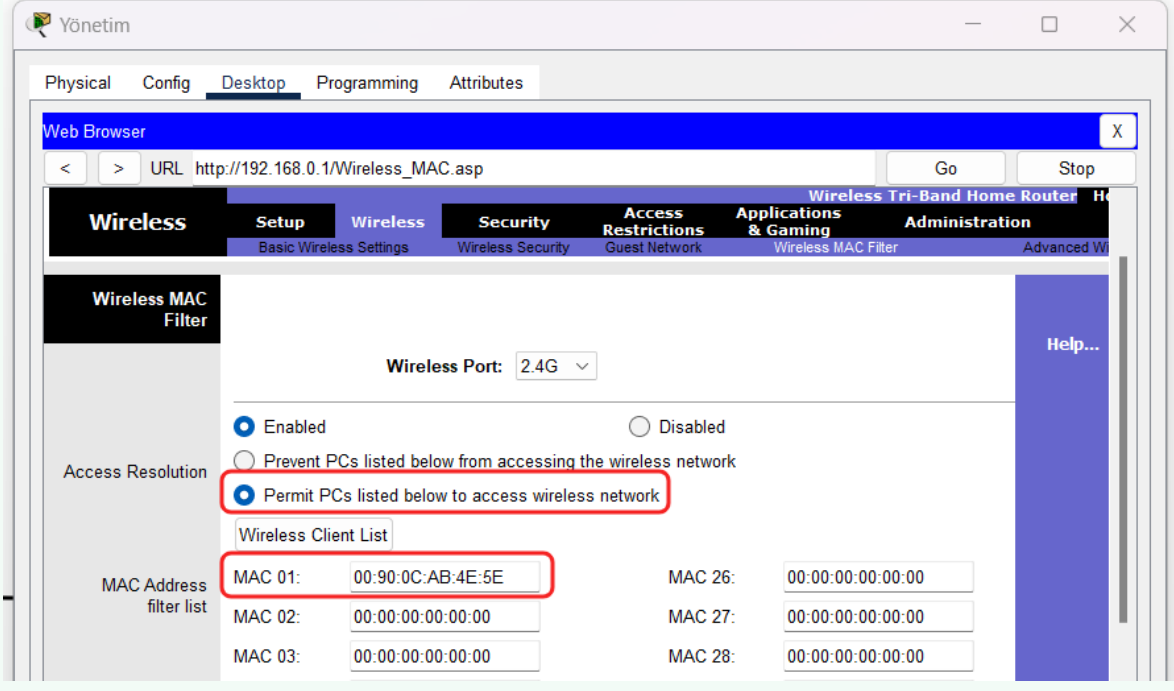
Görsel 3.58: Restoran cihazının kablosuz ayarları

9. Adım: **Resepsiyon** bilgisayarının kablosuz ağ kartının MAC adresini öğreniniz (Görsel 3.59).



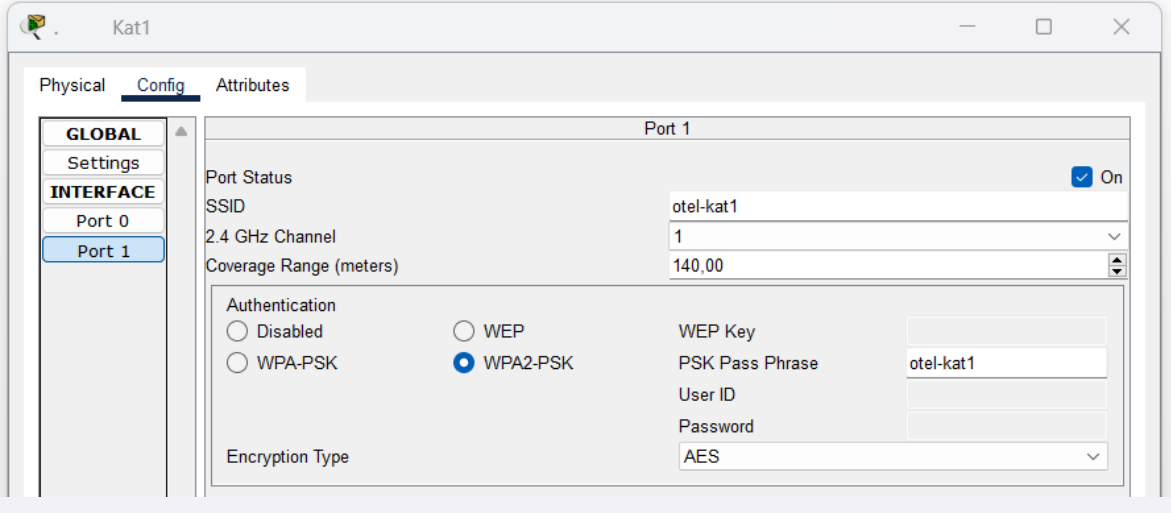
Görsel 3.59: Resepsiyon bilgisayarının MAC adresini öğrenme

10. Adım: Kablosuz yönlendiricinin MAC filtreleme seçeneği ile 5 GHZ frekans bandının sadece **Resepsiyon** bilgisayarı tarafından kullanımına izin veriniz (Görsel 3.60).



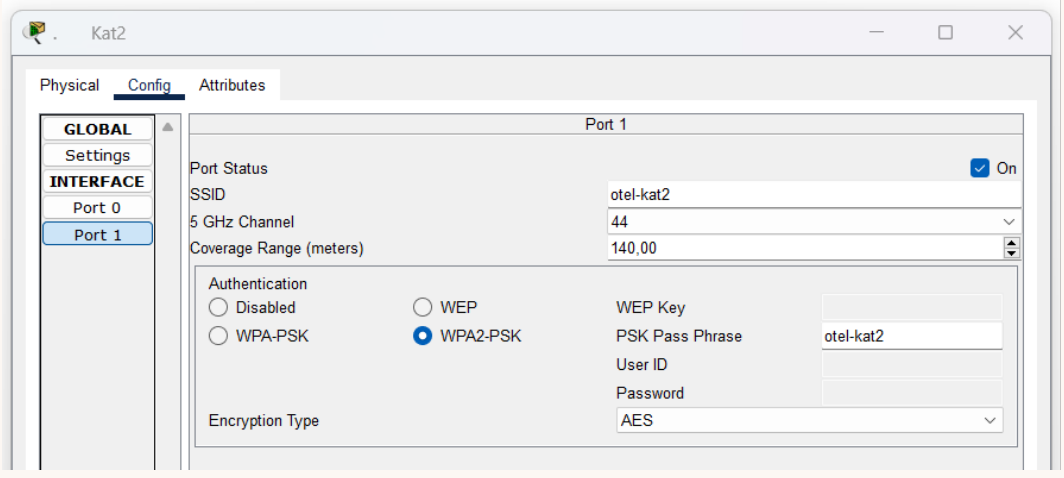
Görsel 3.60: MAC filtreleme

11. Adım: **Kat1** erişim noktasının görünür adını ve şifresini düzenleyiniz (Görsel 3.61).



Görsel 3.61: Kat1 cihazının SSID ve şifresini belirleme

12. Adım: **Kat2** erişim noktasının görünür adını ve şifresini düzenleyiniz (Görsel 3.62).



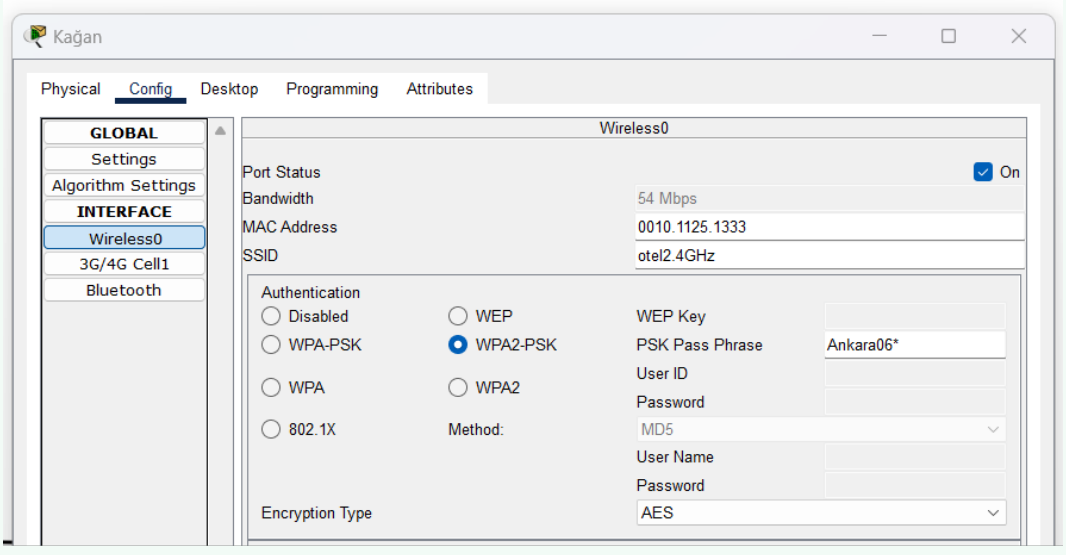
Görsel 3.62: Kat2 cihazının SSID ve şifresini belirleme

13. Adım: **Ayşe** isimli dizüstü bilgisayarı kablosuz ağa dâhil ediniz (Görsel 3.63).



Görsel 3.63: Kablosuz ağ seçimi ile ağa katılma

14. Adım: Görsel 3.64'te **Kağan** isimli akıllı telefonun kablosuz ağa dâhil edilmesi görülür. Siz de diğer tablet ve telefonları uygun ağlara dâhil ediniz.



Görsel 3.64: Kablosuz istemcinin ağa dâhil olması

SIRA SİZDE

Ağ simülasyon programı ile hastane ortamında kullanılacak kablosuz ağ topolojisi tasarlayınız. Ağdaki tüm cihazların merkezî bir yönlendirici üzerinden IP yapılandırması almasını sağlayınız. Yönlendiriciden uzak mesafedeki iletişimi erişim noktaları ile destekleyiniz.

DEĞERLENDİRME

Çalışmanız aşağıda yer alan kontrol listesi kullanılarak değerlendirilecektir. Çalışmanızı yaparken değerlendirme ölçütlerini dikkate alınız.

KONTROL LİSTESİ

ÖLÇÜTLER	EVET	HAYIR
1. Ağ simülasyon programını çalıştırdı.		
2. Ağ ortamında kullanılacak uygun ağ cihazlarını seçti.		
3. Ağ cihazlarının yerleşimini yaptı.		
4. Ağ cihazlarının yapılandırmasını yaptı.		
5. Ağ iletişimini test etti.		

ÖLÇME VE DEĞERLENDİRME

A) Aşağıdaki cümlelerde parantez içine yargılar doğru ise "D", yanlış ise "Y" yazınız.

1. ( ) Veri iletiminin kablosuz olarak radyo dalgaları, kızıl ötesi, mikro dalga gibi elektromanyetik dalgalarla yapıldığı sistemlere kablosuz ağ teknolojileri denir.

2. ( ) Radyo frekansları elektromanyetik spektrumda gözle görünür ışık aralığında yer alır.

3. ( ) Karasal ağ iletişiminin zor olduğu alanlarda uydu sistemleri ile veri iletimi sağlanır.

4. ( ) Erişim noktası, kablolu bir ağın kablosuz olarak genişletilmesini sağlar.

5. ( ) Kablosuz ağlarda çarpışmayı tespit etmek için CSMA/CD protokolü kullanılır.

B) Aşağıdaki cümlelerde boş bırakılan yerlere doğru kelimeleri yazınız.

1. Büyük şehirler veya bölgeler üzerinde kablosuz iletişimin sağlandığı orta büyüklükteki kablosuz alan ağına ..... denir.

2. Kablosuz sinyalin her yöne (360 derece) yayılmasını sağlayan antenlere ..... denir.

3. Hücresel veri erişimi olan akıllı telefon veya tabletin etkin bağlantı noktası ile internet paylaşımına ..... modu denir.

4. Kablosuz istemcilerin ağa bağlanma sürecinde pasif keşif ..... mesajlarıyla yapılır.

5. 4-Way Handshake sürecinde veri aktarımı için güvenli bağlantının sağlanması ..... çerçeveleri ile gerçekleşir.

C) Aşağıdaki soruları dikkatlice okuyarak doğru cevabı işaretleyiniz.

1. Uzaktan kumanda, kamera, bilgisayar gibi cihazların kısa mesafede kablosuz iletişimini sağlayan ağ türü aşağıdakilerden hangisidir?

A) WLAN B) WMAN C) WPAN D) WWAN E) WWW

2. Kablosuz ağda yer alan LAP'lerin yapılandırmasını ve denetlenmesini sağlayan erişim noktası türü aşağıdakilerden hangisidir?

A) Ağ kartı B) Anten C) Bluetooth D) Modem E) WLC

3. Kablosuz ağ iletişiminde kullanılan standart aşağıdakilerden hangisidir?

A) IEEE 800.11 B) IEEE 802.11 C) IEEE 803.11

D) IEEE 804.11 E) IEEE 805.11

4. WLAN çerçeve yapısında çerçeve türünün ve özelliklerinin yer aldığı 16 bitlik alan aşağıdakilerden hangisidir?

A) Address B) Duration C) Frame Control

D) Header E) Sequence Control

5. Kablosuz istemcilerin ağa bağlanma sürecinde veri iletimi için güvenli bağlantının oluşturulduğu dört aşamalı el sıkışma süreci aşağıdakilerden hangisidir?

A) Association B) Authenticaiton C) Connecting

D) Discovery E) 4-Way Handshake

6. Kimlik doğrulama sürecinde, paylaşılan gizli bir anahtar veya SSID ile veri şifreleme-veri çözme yöntemini uygulayan güvenlik protokolü aşağıdakilerden hangisidir?

A) Open Authentication B) WEP C) WPA

D) WPA2 E) WPA3

7. Bir sinyalin bir saniyede yaptığı devir sayısına verilen ad aşağıdakilerden hangisidir?

A) Akım B) Dalga C) Direnç D) Frekans E) Güç

8. Belirli bir frekans bandının aralıklara bölünmesiyle oluşturulan kullanım alanlarına verilen ad aşağıdakilerden hangisidir?

A) Alan B) Bölüm C) Frekans D) Kanal E) SSID

4. ÖĞRENME BİRİMİ

SANAL ÖZEL AĞLAR

KONULAR

4.1. SANAL ÖZEL AĞLAR [VPN (VIRTUAL PRIVATE NETWORK)] VE TÜRLERİ

4.2. SANAL ÖZEL AĞ [VPN (VIRTUAL PRIVATE NETWORK)] UYGULAMALARI

NELER ÖĞRENECEKSİNİZ?

- Sanal özel ağları açıklama
- Sanal özel ağ uygulamaları yapma



TEMEL KAVRAMLAR

Anahtar, bütünlük, gizlilik, Gre, IPsec, Mpls, SSL, şifreleme, TLS, Tunnel, VPN

HAZIRLIK ÇALIŞMALARI

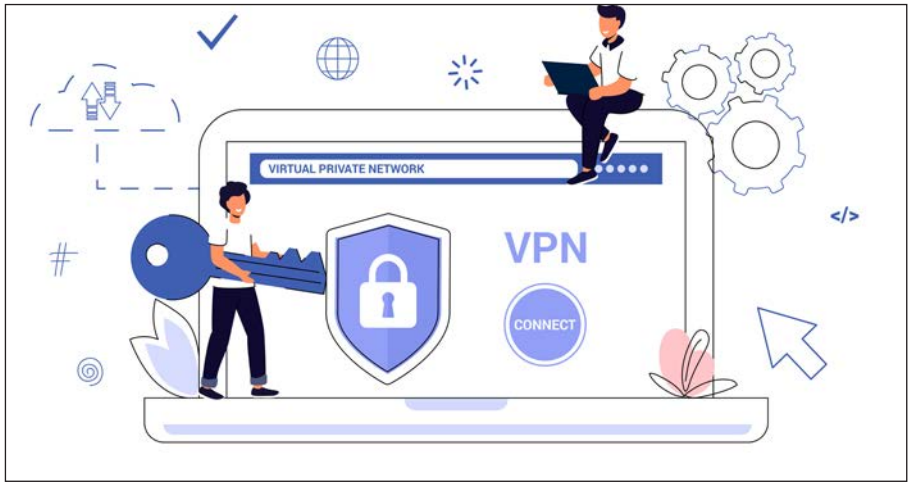
1. VPN kullanmadan güvenli ağ çözümleri neler olabilir? Düşüncelerinizi arkadaşlarınızla paylaşınız.

2. Mobil bankacılık uygulamaları, banka sunucularıyla internet üzerinden güvenli iletişime nasıl geçiyor olabilir? Düşüncelerinizi arkadaşlarınızla tartışınız.

4.1. SANAL ÖZEL AĞLAR [VPN (VIRTUAL PRIVATE NETWORK)] VE TÜRLERİ

Kurum ve kuruluşlar için özel bir ağ kullanmanın maliyeti yüksek olabilir. Özel ağlar, özellikle geniş bir coğrafi alana yayılan ve çok sayıda kullanıcının bağlanması gereken durumlarda gereklidir. Kurulumu için pahalı donanıma ihtiyaç duyulur, yüksek bakım ve yönetim maliyetleri gerektirir. VPN teknolojisi, bu maliyetleri önemli ölçüde azaltan bir çözümdür.

VPN, internet üzerinden gönderilen ağ trafiğini güvenli hâle getirmek için uçtan uca bağlantı oluşturan bir ağ teknolojisidir. VPN teknolojisi (Görsel 4.1), internet üzerinde güvenli bir tünelleme tekniği kullanır.

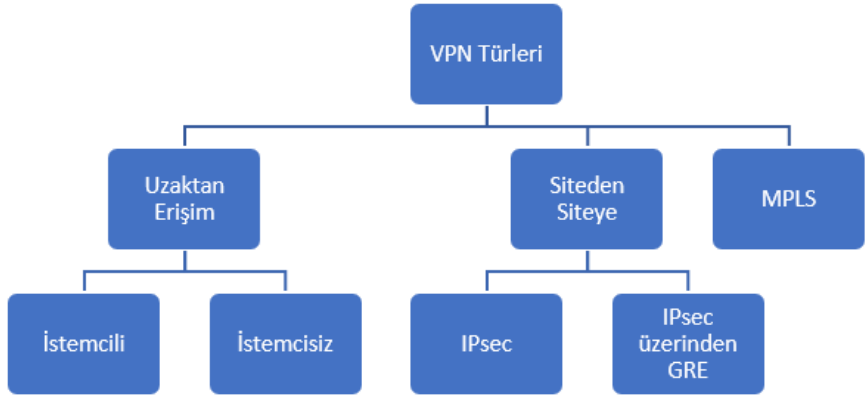


Görsel 4.1: VPN teknolojisi

VPN teknolojisi, ilk geliştirildiği yıllarda sadece internet üzerinde tünel oluşturarak, şifreleme ve kimlik doğrulma yapmadan uçtan uca iletim sağlardı ancak verilerin güvenliğini sağlamak için bugün bu yöntem, güçlü bir koruma sağlayamaz. Dolayısıyla güncel VPN teknolojilerinde kimlik doğrulama ve şifreleme teknolojileri gibi verilerin güvenliğini sağlayacak yöntemler kullanılır.

VPN teknolojisi, genel bir ağ olan internet üzerinden güvenli bağlantı oluşturmayı sağlar. Böylece kullanıcıların, kurum veya kuruluşların özel sanal ağlarına internet üzerinden güvenli bir şekilde erişmelerini mümkün kılar. VPN teknolojisi, verileri şifreleyerek ve kullanıcıların IP adreslerini gizleyerek genel ağın güvenlik risklerini önemli ölçüde ortadan kaldırır. Böylece yüksek maliyetli özel ağlara ihtiyaç duymadan, internetin mevcut altyapısını kullanarak güvenli ve düşük maliyetli bir ağ çözümü elde edilir. Yüksek maliyetli donanım ve bakım gerektirmeyen bu teknoloji, özellikle küçük ve orta ölçekli işletmelerin güvenli ağ bağlantıları oluşturabilmeleri için büyük bir avantajdır.

VPN teknolojisi genellikle **uzaktan erişim (remote access), siteden siteye (site-to-site) ve MPLS [Multi Protocol Label Switching (Çok Protokollü Etiket Anahtarlama)]** olmak üzere üç ana kategoride değerlendirilir. VPN türleri Görsel 4.2'de görülür.



Görsel 4.2: VPN türleri

4.1.1. Uzaktan Erişim VPN (Remote Access VPN)

Uzaktan erişim VPN'leri, bireylerin herhangi bir yerden şirket ağlarına güvenli bir şekilde bağlanmalarına olanak tanır. Bu tür VPN'ler, genellikle seyahat eden çalışanlar veya evden çalışanlar tarafından kullanılır. Kullanıcılar, VPN istemcisi yazılımını kullanarak internet üzerinden şirketin VPN sunucusuna bağlanır ve bu bağlantı şifrelenerek güvence altına alınır. Bu sayede kullanıcılar, şirketin dâhilî kaynaklarına (dosya, veri tabanı, uygulama vb.) sanki fiziksel olarak ofisteymiş gibi erişebilir.

4.1.1.1. İstemcili (Client Based) VPN

İstemcili uzaktan erişim VPN türünde, kullanıcıların kişisel cihazlarından (bilgisayar, tablet, akıllı telefon vb.) özel bir ağa güvenli şekilde bağlanması için özel bir istemci yazılımına ihtiyaç duyulur. Kullanıcı, cihazında yüklü istemci yazılımı çalıştırdığında, hedef özel ağa kimlik doğrulaması yapılarak bağlanır. Sanal özel ağ bağlantısı kurulduğunda istemciyle hedef sunucu arasındaki veri trafiği şifrelenir.

4.1.1.2. İstemcisiz (Clientless) VPN

İstemcisiz uzaktan erişim VPN türünde, kullanıcıların kişisel cihazlarında ek bir yazılım yüklemeye ihtiyaç yoktur. Sadece web tarayıcısı kullanılarak özel bir ağa güvenli bir şekilde bağlanılmasını sağlayan bir teknolojidir. İstemcisiz VPN'ler, SSL/TLS protokollerini kullanarak web tabanlı bir arayüz üzerinden hedef sunucuyla güvenli bir bağlantı kurar. Kullanıcılar, tarayıcıları aracılığıyla kendilerine erişim yetkisi verilen uygulamalara ve hizmetlere erişebilir hâle gelir. Bu özelliklerinden dolayı kullanımı oldukça basittir.

4.1.1.3. SSL/TLS (Secure Sockets Layers/Transport Layer Security) Protokolleri

SSL ve **TLS**, internet gibi milyarlarca kullanıcının bulunduğu güvensiz bir ağ ortamında, web tarayıcısıyla web siteleri arasında gerçekleşen veri trafiğinin güvenliğini sağlamak için geliştirilmiş protokollerdir.

SSL Protokolü: Web üzerinden istemci ve sunucu arasındaki iletişimin güvenliğini sağlamak için geliştirilmiş bir şifreleme protokolüdür. Netscape tarafından geliştirilen SSL protokolünün v1, v2 ve v3 olmak üzere üç versiyonu vardır. 1994 yılında kullanıma sunulan SSLv1'in birçok güvenlik açığı olması nedeniyle 1995 yılında SSLv2 kullanıma sunulur. Son olarak 1996 yılında, SSLv2'de tespit edilen kimlik doğrulama ve veri bütünlüğüyle ilgili güvenlik açıklarından dolayı SSLv3 versiyonu kullanıma sunulur. SSLv3, 2014 yılında kendisine gerçekleştirilen **POODLE** gibi siber saldırılara maruz kalması nedeniyle artık güvenli kabul edilmemektedir.

TLS Protokolü: SSL protokolü, güvenli kabul edilmediği için yerini çok daha güvenli olan TLS protokolüne bırakır. TLS protokolünün versiyonları şunlardır:

- **TLS 1.0:** 1999 yılında yayımlanan ilk versiyon, SSLv3 ile çok benzerdir. SSLv3'te tespit edilen bazı güvenlik açıklıkları bu versiyonda ortadan kaldırılır. Özellikle POODLE saldırısına karşı güçlendirme yapılır ancak TLS 1.0 versiyonunun BEAST (Browser Exploit Against SSL/TLS) saldırılarına karşı güvenlik önlemi yoktur.
- **TLS 1.1:** 2006 yılında yayımlanan bu versiyonda çeşitli güvenlik iyileştirmeleri yapılır. BEAST saldırılarına önlem olarak şifreli verilerin işlenme şekli değiştirilir.
- **TLS 1.2:** 2008 yılında yayımlanan versiyon, daha güçlü şifreleme (AES) algoritmalarını destekler. Özetleme fonksiyonu olarak MD5 ve SHA1'in yerine SHA-256 kullanır. Kullanıcıya özel şifreleme yöntemleri belirleme esnekliği sunar.
- **TLS 1.3:** 2018 yılında yayımlanan son versiyon, en güvenilir ve en hızlı versiyondur. Diğer versiyonlarda bulunan birçok zayıf şifreleme teknikleri kaldırılarak sade, hızlı ve güvenilir bir protokol hâline getirilir.

ARAŞTIRMA İstemcili/İstemcisiz VPN

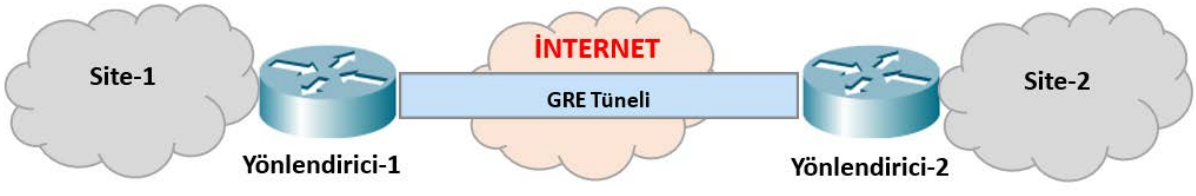
İstemcili/İstemcisiz VPN'lerin nerelerde kullanıldığını araştırınız. Edindiğiniz bilgileri sınıfta arkadaşlarınızla paylaşınız.

4.1.2. Siteden Siteye VPN

Siteden siteye VPN'ler, farklı coğrafi konumlarda bulunan iki veya daha fazla ağın internet üzerinden güvenli bir şekilde haberleşmesini sağlar. Genellikle büyük şirketler, kurum ve kuruluşlar, merkez ağları ile şube ağları arasında veri iletişimini güvenli hâle getirmek için kullanır. Her iki uçta da VPN ağ geçidi bulunur ve bu cihazlar, veriyi şifreleyip karşı tarafa iletir. Karşı taraftaki VPN ağ geçidi, şifreli gelen verinin şifresini çözer ve hedef ağa ulaştırır.

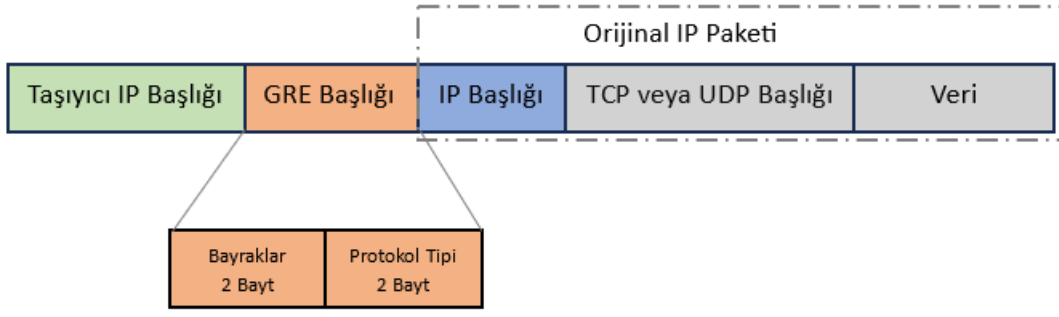
4.1.2.1. GRE IP Tünel Protokolü

GRE (Generic Routing Encapsulation), Cisco firması tarafından geliştirilmiş bir tünel protokolüdür. İki farklı ağ arasındaki haberleşme, GRE protokolüyle oluşturulan tünel sayesinde internet üzerinden veya geniş alan ağı üzerinden siteden siteye sanal özel ağ haberleşmesi gibi noktadan noktaya gerçekleşir (Görsel 4.3).



Görsel 4.3: GRE tünel yapısı

GRE protokolü, farklı türlerdeki ağ katmanı (OSI Referans Modeli Üçüncü Katmanı) protokollerini (IPv4, IPv6, IPX, AppleTalk vb.) bir GRE başlığı ve taşıyıcı bir IP başlığıyla kapsülleyerek (encapsulation) paketin yönlendirilmesini sağlar (Görsel 4.4). GRE tüneli her türlü ağ trafiğini (tekil yayın, çok noktaya yayın ve genel yayın) taşır.

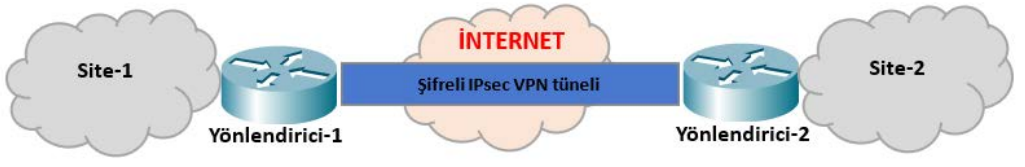


Görsel 4.4: GRE protokolü paket yapısı

GRE kapsüllemesi gerçekleştirilirken orijinal IP paketine 4 bayt GRE başlığı ve 20 bayt taşıyıcı IP başlığı olmak üzere toplam 24 bayt eklenir. Eklenen bu 24 bayt, 1.500 bayt olan MTU [Maximum Transmission Unit (Maksimum İletim Miktarı)] boyutundan düşer. Böylece MTU boyutu 1.476 olarak güncellenir. GRE protokolü, kimlik doğrulaması ve ağ trafiğini şifreleme işlemini gerçekleştirmez. Bu nedenle güvenlikten söz edilemez.

4.1.2.2. IPsec VPN

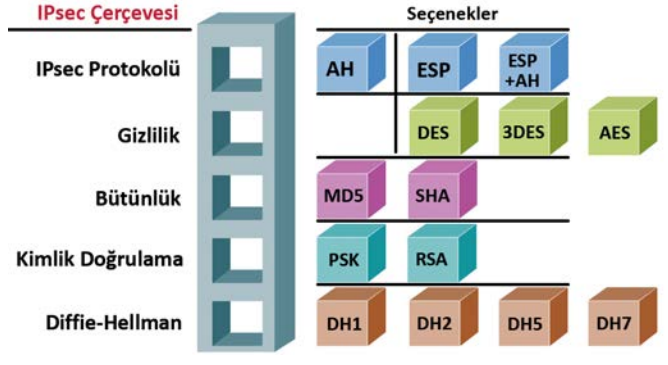
IPsec VPN, internet gibi genel ağ ortamlarında altyapı yatırımı gerektirmeden verilerin güvenli bir şekilde iletilmesini sağlayan sanal özel ağdır. IPsec (Internet Protocol Security); verilerin gizliliğini, bütünlüğünü ve kimlik doğrulamasını sağlamak için IPsec çerçevesinde tanımlanan teknolojiler kullanır. IPsec sanal özel ağında veriler, siteden siteye oluşturulan şifreli bir tünel üzerinden güvenli bir şekilde iletilir (Görsel 4.5). IPsec tünelinden yalnızca tekil yayın (unicast) paketleri iletilir. Çok noktaya yayın (multicast) ve genel yayın (broadcast) paketleri iletilemez.



Görsel 4.5: IPsec VPN tünel yapısı

4.1.2.3. IPsec Framework (IPsec Çerçevesi)

IPsec çerçevesi, internet protokolü (IP) üzerinden güvenli veri iletimi sağlamak için kullanılan protokoller çerçevesidir (Görsel 4.6). IPsec, ağlar arası veri aktarımında güvenliği sağlamak için bir dizi protokol ve algoritma kullanır. Bu çerçeve; veri bütünlüğü, gizlilik, kimlik doğrulama ve tekrarlama saldırılarına karşı koruma sağlar.



Görsel 4.6: IPsec çerçevesi

ARAŞTIRMA Tekrarlama saldırısı

Tekrarlama saldırısıyla ilgili araştırma yapınız. Araştırma sonuçlarını öğretmeniniz ve arkadaşlarınızla paylaşınız.

IPsec özellikle VPN'lerde ve diğer güvenli iletişim gerektiren uygulamalarda yaygın olarak kullanılır.

A) IPsec Protokolleri

Verilerin internet ağı üzerinden güvenli bir şekilde gönderilmesi için VPN teknolojileri kullanılır. VPN teknolojilerinde IPsec protokolü yaygın olarak tercih edilir. IPsec, **taşıma (transport)** ve **tünel (tunnel)** olmak üzere iki ana modda çalışır.

Taşıma (Transport) Modu: Uçtan uca güvenlik sağlamak için kullanılır. Bu modda, OSI (Open System Interconnection) referans modeli üçüncü katman PDU'su (Protocol Data Unit) olan IP paketinin (packet) yalnızca veri (payload) kısmı şifrelenir. IP başlığı ise şifrelenmez.

Tünel (Tunnel) Modu: Ağlar arası güvenli tüneller oluşturmak için kullanılır. Bu modda, OSI (Open System Interconnection) referans modeli üçüncü katman PDU'su olan IP paketinin tamamı (hem IP başlığı hem de veri kısmı) şifrelenir ve şifreli IP paketinin başına yeni bir IP başlığı eklenir.

IPsec protokol kümesinin iki ana üyesi **AH [Authentication Header (Kimlik Doğrulama Başlığı)]** ve **ESP [Encapsulation Security Protocol (Kapsülleme Güvenlik Protokolü)]** protokolleridir. AH ve ESP protokolleri IP paketi kapsüllemesinde üç faklı şekilde kullanılır. Bu kullanım şekilleri şunlardır:

1. AH Protokolüyle Kapsülleme

AH protokolü, IPsec çerçevesinde veri paketlerinin kimlik doğrulamasını ve bütünlüğünü sağlamak için kullanılır ancak bu protokolde şifreleme yapılmadığı için verilerin gizliliği sağlanamaz ve bu durumda güvenlik açığı oluşabilir. AH protokolüyle hem taşıma modu hem de tünel modu kullanılabilir.

a) AH Protokolüyle Taşıma Modu Kapsüllemesi

Görsel 4.7'de orijinal IP paketi kapsüllemesi görülür.



Görsel 4.7: Orijinal IP paketi

AH protokolü taşıma modunda kullanıldığında IP başlığı ile TCP başlığı arasına AH başlığı eklenerek kapsülleme yapılır (Görsel 4.8). Yeni IP paketinin tamamı için AH protokolüyle kimlik doğrulaması yapılır.



Görsel 4.8: IPsec AH taşıma modu

b) AH Protokolüyle Tünel Modu Kapsüllemesi

Görsel 4.9'da orijinal IP paketi kapsüllemesi görülür.



Görsel 4.9: Orijinal IP paketi

AH protokolü tünel modunda kullanıldığında IP başlığının önüne önce AH başlığı sonra yeni IP başlığı eklenerek kapsülleme yapılır (Görsel 4.10). Yeni IP paketinin tamamı için AH protokolüyle kimlik doğrulaması yapılır.



Görsel 4.10: IPsec AH tünel modu

2. ESP Protokolüyle Kapsülleme

ESP protokolü; ağ üzerinde güvenli iletim için verinin gizliliğini, bütünlüğünü, kimlik doğrulamasını sağlar ve veri paketlerini şifreler. IP paketlerine eklenerek ağ üzerinde iletilen verinin üçüncü kişiler tarafından okunmasını veya değiştirilmesini önler. ESP başlığı (ESP header), ESP kuyruğu (ESP trailer) ve ESP kimlik doğrulama verisi (ESP auth) olmak üzere üç kısımdan oluşur. ESP protokolü hem taşıma hem de tünel modunda kullanılabilir.

a) ESP Protokolüyle Taşıma Modu Kapsüllemesi

Görsel 4.11'de orijinal IP paketi kapsüllemesi görülür.



Görsel 4.11: Orijinal IP paketi

ESP protokolü taşıma modunda kullanıldığında IP başlığı ile TCP başlığı arasına ESP başlığı, verinin sonuna ESP kuyruğu ve ESP doğrulama verisi eklenerek kapsülleme yapılır (Görsel 4.12). Bu yöntemde verinin şifrelenmesi ve kimlik doğrulaması, ESP protokolü tarafından yapılır.



Görsel 4.12: IPsec ESP taşıma modu

b) ESP Protokolüyle Tünel Modu Kapsüllemesi

Görsel 4.13'te orijinal IP paketi kapsüllemesi görülür.



Görsel 4.13: Orijinal IP paketi

ESP protokolü tünel modunda kullanıldığında IP başlığının önüne önce ESP başlığı sonra yeni IP başlığı, verinin sonuna ESP kuyruğu ve ESP doğrulama verisi eklenerek kapsülleme yapılır (Görsel 4.14). Bu yöntemde orijinal IP paketi ESP protokolüyle şifrelenir ve kimlik doğrulaması yapılır.



Görsel 4.14: IPsec ESP tünel modu

3. ESP+AH Protokolleriyle Kapsülleme

ESP+AH protokolleriyle kapsülleme, IP paketlerinin ESP ve AH protokollerinin birlikte kullanılarak kapsüllendiği yöntemdir. Bu yöntem; veri paketlerinin bütünlüğünü, kimlik doğrulamasını ve gizliliğini daha güçlü şekilde sağlamayı amaçlar.

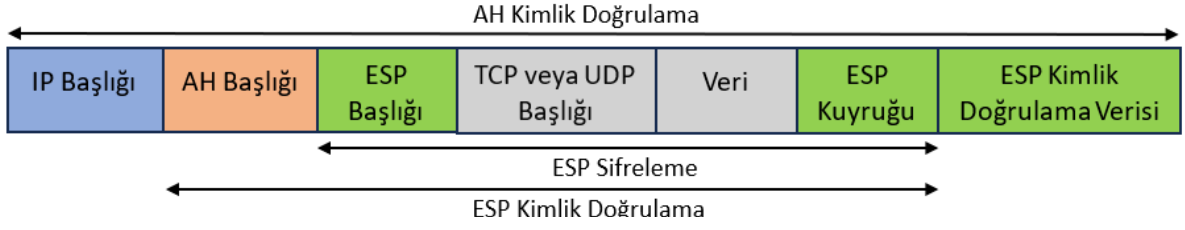
a) ESP+AH Protokolleriyle Taşıma Modu Kapsüllemesi

Görsel 4.15'te orijinal IP paketi kapsüllemesi görülür.



Görsel 4.15: Orijinal IP paketi

ESP+AH kombinasyonu taşıma modunda kullanıldığında IP başlığı ile TCP başlığı arasına önce ESP başlığı sonra AH başlığı, verinin sonuna ESP kuyruğu ve ESP doğrulama verisi eklenerek kapsülleme yapılır (Görsel 4.16). Bu yöntemde veri, ESP protokolü tarafından şifrelenir ve kimlik doğrulaması yapılır. Daha sonra IP paketi için AHS protokolüyle kimlik doğrulaması yapılır.



Görsel 4.16: IPsec ESP+AH taşıma modu

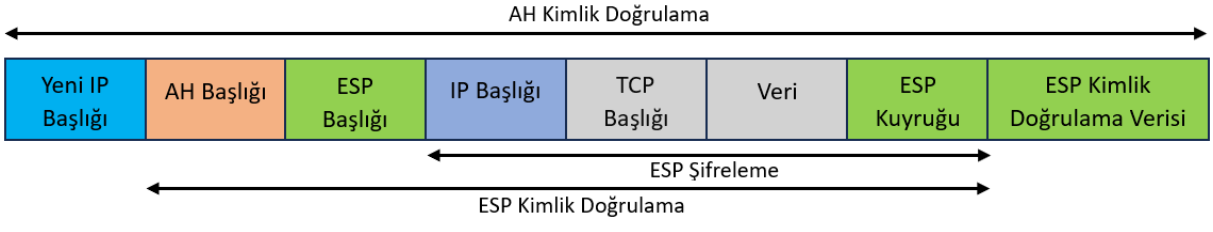
b) ESP+AH Protokolleriyle Tünel Modu Kapsüllemesi

Görsel 4.17'de orijinal IP paketi kapsüllemesi görülür.



Görsel 4.17: Orijinal IP paketi

ESP+AH kombinasyonu tünel modunda kullanıldığında önce IP başlığının önüne ESP başlığı sonra AH başlığı son olarak yeni IP başlığı eklenir. Verinin sonuna ESP kuyruğu ve ESP doğrulama verisi eklenerek kapsülleme yapılır (Görsel 4.18). Bu yöntemde orijinal IP paketi, ESP protokolü tarafından şifrelenir ve kimlik doğrulaması yapılır. Daha sonra yeni IP paketinin tamamı için AH protokolüyle kimlik doğrulaması yapılır.



Görsel 4.18: IPsec ESP+AH tünel modu

B) IPsec Şifreleme Algoritmaları

IPsec; veri güvenliğini sağlamak için **DES (Data Encryption Standard), 3DES (Triple Data Encryption Standard), AES (Advanced Encryption Standard)** ve **SEAL (Simple Encrypted Arithmetic Library)** si-

metrik kripto algoritmalarını kullanır ancak DES ve 3DES algoritmaları, daha eski ve güvenlik zafiyetleri barındırdığı için yüksek güvenlik ve performans sunan AES algoritması yaygın olarak tercih edilir. AES algoritması 128, 192 veya 256 bit uzunluğunda şifreleme anahtarı kullanarak verileri 128 bitlik bloklar hâlinde şifreler.

C) IPsec Bütünlük (Integrity) Algoritmaları

IPsec, veri bütünlüğünü kontrol etmek için **MD5 (Message-Digest Algorithm 5)** ve **SHA (Secure Hash Algorithm)** algoritmalarını kullanır ancak bugün güncel ve güvenilir olması sebebiyle SHA algoritması tercih edilir.

Ç) IPsec Kimlik Doğrulama Algoritmaları

IPsec'te kimlik doğrulama işlemi iki farklı yöntemle gerçekleştirilir. Bunlar, **PSK [Pre-Shared Key (Önceden Paylaşılmış Anahtar)]** yöntemi ve **RSA (Rivest-Shamir-Adleman)** asimetrik kripto algoritmasıyla kimlik doğrulamadır.

1. **PSK Yöntemiyle Kimlik Doğrulama:** Bu yöntemde, iki tarafın önceden belirlenmiş bir anahtarı paylaşması ile kimlik doğrulama gerçekleştirilir.
2. **RSA Yöntemiyle Kimlik Doğrulama:** RSA kripto algoritmasıyla kimlik doğrulama yönteminde, her iki taraf da özel ve genel anahtar olmak üzere bir çift anahtar kullanır. Genel anahtar herkesle paylaşılırken özel anahtar sadece sahibi tarafından bilinir. Bağlantı kurulduğunda taraflardan biri diğerine, kendi özel anahtarına sahip olduğunu kanıtlamak için bir dijital imza gönderir. RSA, daha yüksek güvenlik sağlar çünkü kimlik doğrulama, özel anahtarın gizliliği korunduğu sürece güvenilirdir.

D) IPsec Güvenli Anahtar Değişimi

Güvenli anahtar değişimi, IPsec çerçevesinin temel bileşenlerinden biridir. Güvenli anahtar değişimi gerçekleştirilirken **Diffie-Hellman asimetrik kriptografi algoritması** kullanılır. Güvenli anahtar değişimi sürecine **IKE (Internet Key Exchange)** denir. IKE, IPsec için gerekli olan güvenlik ilişkilerini [Security Association (SA)] kurmak için kullanılır. IKE, iki taraf arasında güvenli bir anahtar değişimi gerçekleştirerek şifreleme, kimlik doğrulama ve veri bütünlüğü için kullanılacak algoritmaları belirler. Güvenli anahtar değişimi gerçekleştirildiğinde IPsec VPN tüneli kurulmuş olur. IPsec VPN tüneli oluşturmanın IKE Faz 1 ve IKE Faz 2 olmak üzere iki aşaması vardır.

IKE Faz 1: Faz 1'in amacı, Faz 2 sürecinde kullanılacak güvenli bir tünel oluşturmaktır. Faz 2 sürecine hazırlıktır. Bu aşamada, VPN tüneli kurulacak iki taraf arasında ISAKMP SA (Internet Security Association and Key Management Protocol Security Association) oluşturulur. IKE Faz 1 sürecinde ISAKMP SA oluşturma adımları şunlardır:

1. Adım: Müzakere (Negotiation)

VPN tüneli kurulacak iki eş arasında şu konular müzakere edilir:

- Veri bütünlüğünü sağlamak için karma oluşturma (hashing) algoritması (MD5, SHA)
- Kimlik doğrulama (authentication) yöntemi (Ön paylaşımlı anahtar, RSA dijital sertifika)
- Anahtar değişiminde kullanılacak Diffie-Hellman asimetrik kriptografi algoritmasının grubu (DH1, DH2 ve DH5)
- Faz 1 tünelinin yaşam süresi [lifetime (86.400 saniye)]
- Kullanılacak şifreleme algoritmasını (DES, 3DES ve AES) belirleme

NOT: Müzakere sürecinde tünel yaşam ömrünün 86.400 saniye olarak belirlenmesi, tünelin 1 gün boyunca hayatta kalacağı anlamına gelir. Bu sürenin sonunda Faz 1 süreci yeniden başlatılır.

2. Adım: DH (Diffie-Hellman) Anahtar Değişimi

Başarılı bir müzakere sürecinin sonunda, belirlenen DH grubu kullanılarak anahtar değişimi gerçekleştirilir.

3. Adım: Kimlik Doğrulama

İki eş arasında, üzerinde anlaşılan yöntemle kimlik doğrulama işlemi gerçekleştirilir. Kimlik doğrulama işlemi, ön paylaşımlı anahtar veya RSA dijital sertifika yöntemiyle gerçekleştirilir. Kimlik doğrulama iki modda gerçekleştirilir.

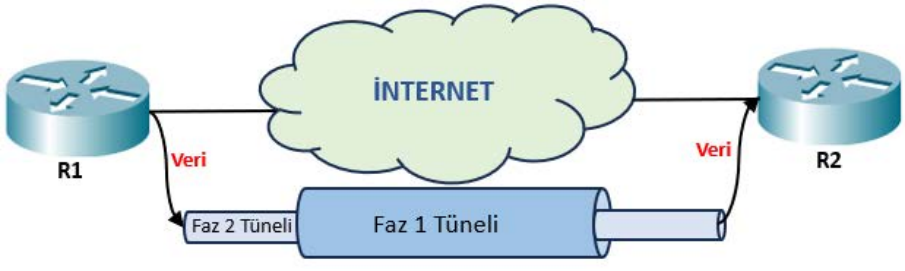
- **Ana Mod (Main Mode):** Daha güvenli ve yavaştır.
- **Agresif Mod (Aggressive Mode):** Hızlı ancak güvenlik seviyesi bakımından daha düşüktür.

Kimlik doğrulama işleminden sonra ISAKMP tüneli veya Faz 1 tüneli kurulur.

IKE Faz 2: Faz 2 sürecinde IPsec güvenlik ilişkileri [IPsec SA (IPsec Security Association)] oluşturulur. Faz 2 sürecinde IPsec SA oluşturulurken şu konular müzakere edilir:

- Kullanılacak IPsec protokolü (AH ve ESP)
- Kapsülleme modu (taşıma ve tünel)
- Kimlik doğrulama algoritması (MD5 ve SHA)
- Kullanılacak şifreleme algoritması (DES, 3DES ve AES)
- Tünelin yaşam süresini belirleme

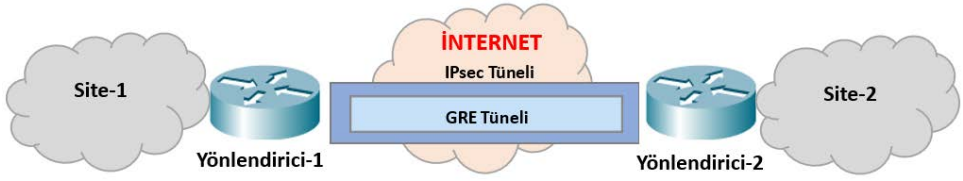
Faz 2 tüneli, hızlı mod (quick mode) yöntemiyle Faz 1'de oluşturulan tünelin içinde oluşturulur. Faz 1 ve Faz 2 tünelleri oluşturulup, IPsec tüneli tamamlanınca iki eş arasındaki ağ trafiği iç içe oluşturulan iki tünel içerisinden güvenli bir şekilde iletilir (Görsel 4.19).



Görsel 4.19: IPsec tüneli

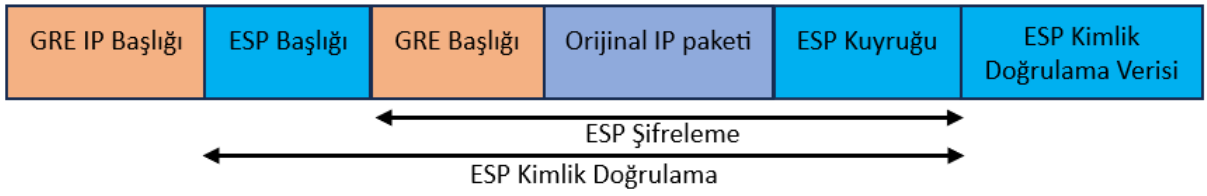
4.1.2.4. IPsec VPN Üzerinden GRE IP Tüneli

GRE protokolü, güvenlik kaygılarının olmadığı bir dönemde geliştirilir. Bu nedenle GRE tünel trafiğinde kimlik doğrulaması ve şifreleme yapılmaz. Bugün sürekli artan siber tehdit ve saldırılardan dolayı veri güvenliğinin sağlanması zorunluluktur. IPsec VPN, internet gibi genel bir ağ ortamından güvenli veri trafiği oluşturmak için kullanılır. IPsec, ilk geliştirildiği yıllarda sadece tekil yayın (unicast) IP paketlerini iletir. Bu durum özellikle EIGRP, OSPF gibi dinamik yönlendirme protokollerinin komşuluk oluşturmak için kullandığı çoklu yayın (multicast) paketlerin iletilmesini engeller. IPsec VPN üzerinden GRE IP tüneli, bu sorunu çözmek için kullanılır (Görsel 4.20).



Görsel 4.20: IPsec VPN üzerinden GRE IP tüneli yapısı

IPsec VPN üzerinden GRE IP tüneli yönteminde, orijinal IP paketi öncelikle GRE protokolüyle kapsüllenir. Tekil, çoklu veya genel yayın trafiği GRE protokolüyle kapsüllendiğinde yeni IP paketi, tekil yayın paketi hâline gelir. GRE protokolüyle kapsüllenen yeni IP paketi, IPsec tarafından kapsüllenir. Böylece GRE tüneli kullanılarak IPsec tünelinden her türlü ağ trafiği geçmiş olur. IPsec VPN üzerinden GRE IP tüneli taşıma modu paket yapısı Görsel 4.21'de, tünel modu paket yapısı ise Görsel 4.22'de görülür. Bu yöntem kullanılarak her türlü ağ trafiği siteden siteye şifrelenmiş şekilde iletilir.



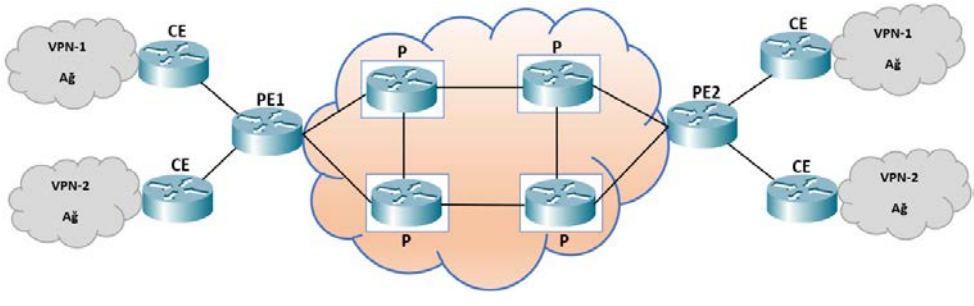
Görsel 4.21: Taşıma modu IPsec VPN üzerinden GRE IP tüneli paket yapısı



Görsel 4.22: Tünel modu IPsec VPN üzerinden GRE IP tüneli paket yapısı

4.1.3. MPLS Sanal Özel Ağlar

MPLS sanal özel ağlar, veri paketlerini yönlendirirken hız ve verimliliği artırmak için etiketleme tekniğini kullanan bir ağ teknolojisidir. Özellikle büyük kurumsal ağlarda, farklı tür ağların birbirinden izole edilmesini sağlar. MPLS sanal özel ağı, noktadan noktaya VPN'lerin aksine çok noktadan çok noktaya iletim gerçekleştirir. MPLS tünellerinden çok noktaya yayın (multicast) paketleri iletilir. Maliyeti oldukça yüksektir. OSI referans modelinin ikinci ve üçüncü katmanları arasında çalışır. MPLS, ağ trafiğini iletirken doğrudan şifreleme gerçekleştirilmez ancak şifreleme ihtiyacı olduğu durumlarda IPsec gibi protokollerle entegre edilerek şifreleme gerçekleştirilir. MPLS sanal özel ağlarında yönlendirme sürecinin yürütülmesi işlemi, servis sağlayıcılar tarafından gerçekleştirilir. Ayrıca QoS [Quality of Service (Hizmet Kalitesi)] sunarak belirli trafik türlerine öncelik verilmesini sağlar. Görsel 4.23'te gösterilen VPN-1 ağları ve VPN-2 ağları, MPLS üzerinden birbirinden izole edilmiş bir şekilde kendi aralarında haberleşir.



Görsel 4.23: MPLS ağ mimarisi

Topolojide yer alan her ağın MPLS'ye çıkış yapacağı bir sınır noktası vardır. Bu sınır noktasına **CE [Customer Edge (Müşteri Sınırı)]** denir. MPLS'nin sınır noktası ise **PE [Provider Edge (Servis Sağlayıcı Sınırı)]** olarak isimlendirilir. MPLS bulutu içindeki yönlendiriciler ise **P [(Provider Router (Servis Sağlayıcı Yönlendiricisi)]** olarak isimlendirilir. Ağ trafiklerini birbirinden izole etmek için PE yönlendiricilerinde **VRF**'ler **[Virtual Routing Forwarding (Sanal Yönlendirme İletme)]** oluşturulur.

MPLS, paketleri yönlendirirken IP adresi yerine etiketleri kullanır. PE yönlendiricilerinde paketler etiketlenerek ilgili VRF üzerinden MPLS bulutuna ve tüm ağ içine gönderilir. Her bir P yönlendirici, paketin etiketine bakarak hızlı bir şekilde hangi yöne gitmesi gerektiğini belirler ve paketi bir sonraki sıçrama noktasına (hop) yönlendirir. Süreç, paket hedefine ulaşana kadar devam eder.

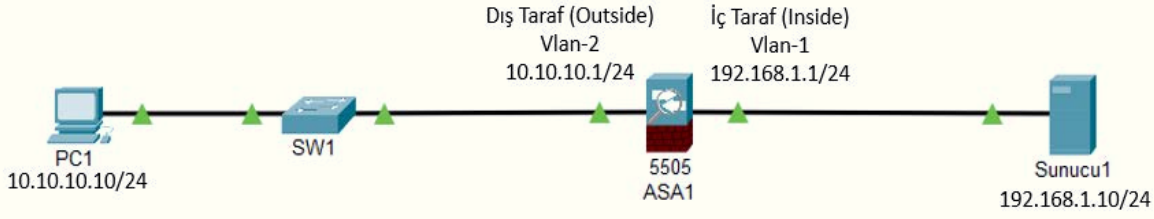
4.2. SANAL ÖZEL AĞ [VPN (VIRTUAL PRIVATE NETWORK)] UYGULAMALARI

Verilerin gizliliğini ve güvenliğini artırmak için sanal özel ağ uygulamaları kullanılır.

Güvenlik duvarı ile istemcisiz SSL VPN uygulama işlemini verilen adımlar doğrultusunda gerçekleştiriniz.

1. UYGULAMA

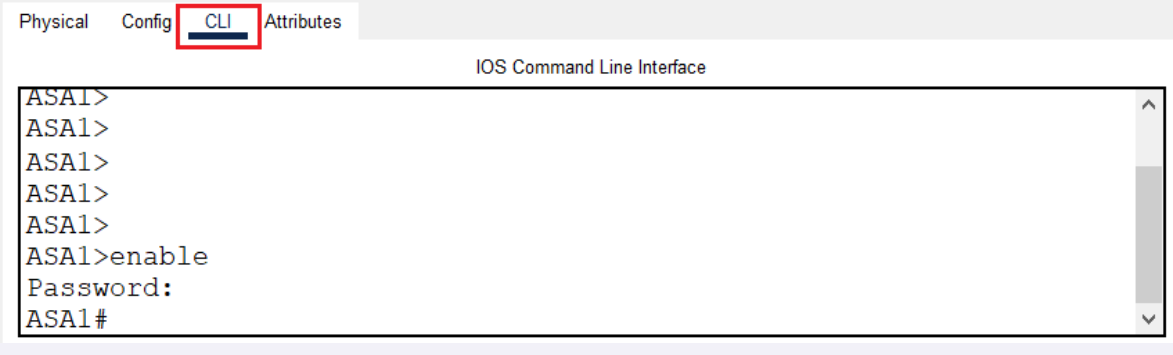
1. Adım: Ağ simülasyon programında Görsel 4.24'teki ağ topolojisini oluşturunuz.



Görsel 4.24: İstemcisiz SSL web VPN ağ topolojisi

2. Adım: Güvenlik duvarının üzerine farenin sol tuşuyla tıklayınız ve CLI [Command Line Interface (Komut Satırı Arayüzü)] sekmesini seçiniz.

3. Adım: **enable** komutu kullanarak ve parola (Password) kısmını boş bırakarak yetkili moda geçiş yapınız (Görsel 4.25).



Görsel 4.25: Ağ cihazlarının CLI modunun açılması

4. Adım: Güvenlik duvarının sanal arayüz IP adreslerini CLI moduna girerek aşağıdaki şekilde konfigüre ediniz.

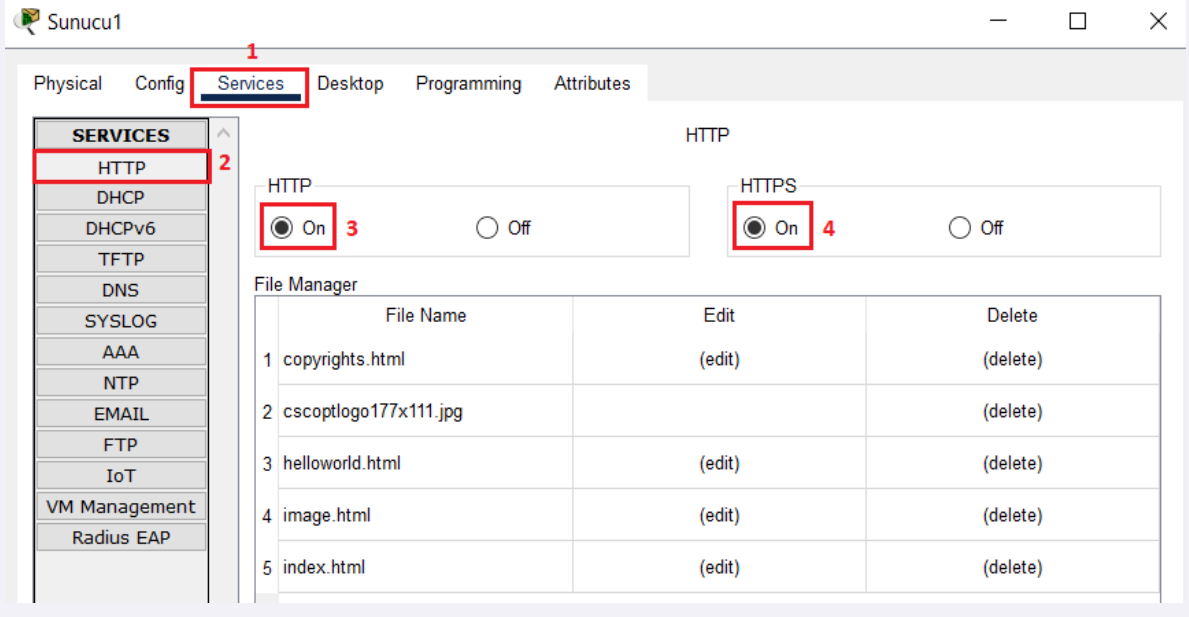
```
ASA1#configure terminal
ASA1(config)#interface vlan 1
ASA1(config-if)#ip address 192.168.1.1 255.255.255.0
ASA1(config-if)#no shutdown
ASA1(config-if)#exit
ASA1(config)#interface vlan 2
ASA1(config-if)#ip address 10.10.10.1 255.255.255.0
ASA1(config-if)#no shutdown
```

5. Adım: PC1 ve Sunucu1'in IP adres yapılandırmasını aşağıdaki şekilde konfigüre ediniz.

PC1		**Sunucu1**	
IP Adresi	: 10.10.10.10	**IP Adresi**	: 192.168.1.10
Alt Ağ Maskesi	: 255.255.255.0	**Alt Ağ Maskesi**	: 255.255.255.0
Varsayılan Ağ Geçidi	: ----------	**Varsayılan Ağ Geçidi**	: ----------

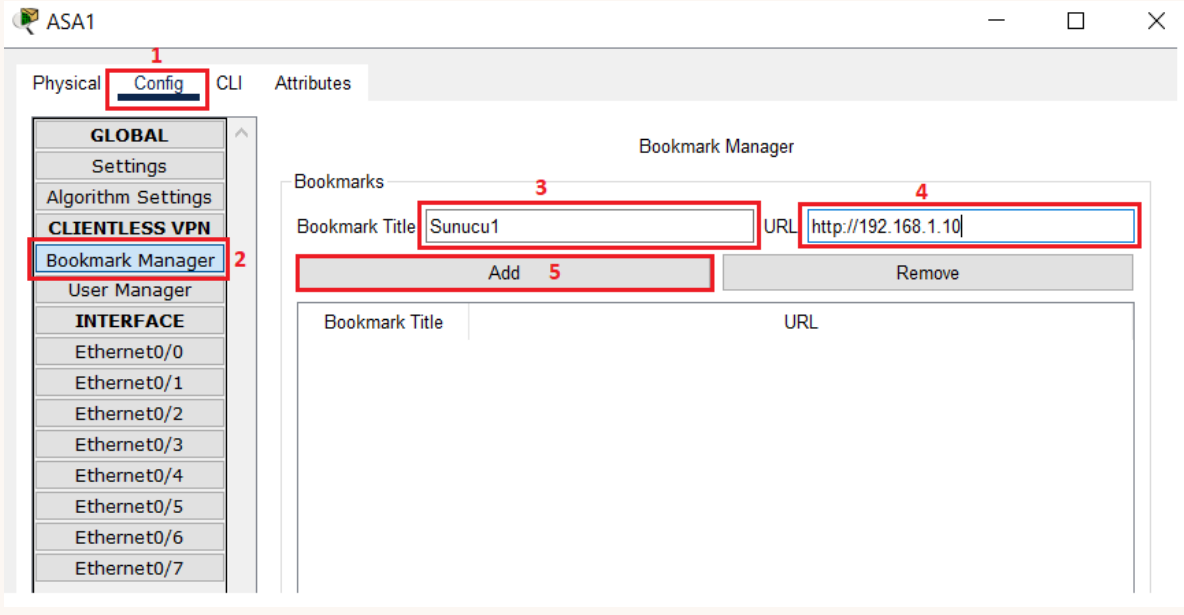
6. Adım: Sunucu1'de **Services** sekmesini açıp **HTTP** servisine tıklayınız.

7. Adım: **HTTP** ve **HTTPS** servislerini **ON** durumuna getirerek aktif ediniz (Görsel 4.26).



Görsel 4.26: Sunucu1'de web sunucu servisinin açılması

8. Adım: ASA1 güvenlik duvarında **Config** sekmesini açıp CLIENTLESS VPN servisine Sunucu1'in web sayfasını ekleyiniz (Görsel 4.27).



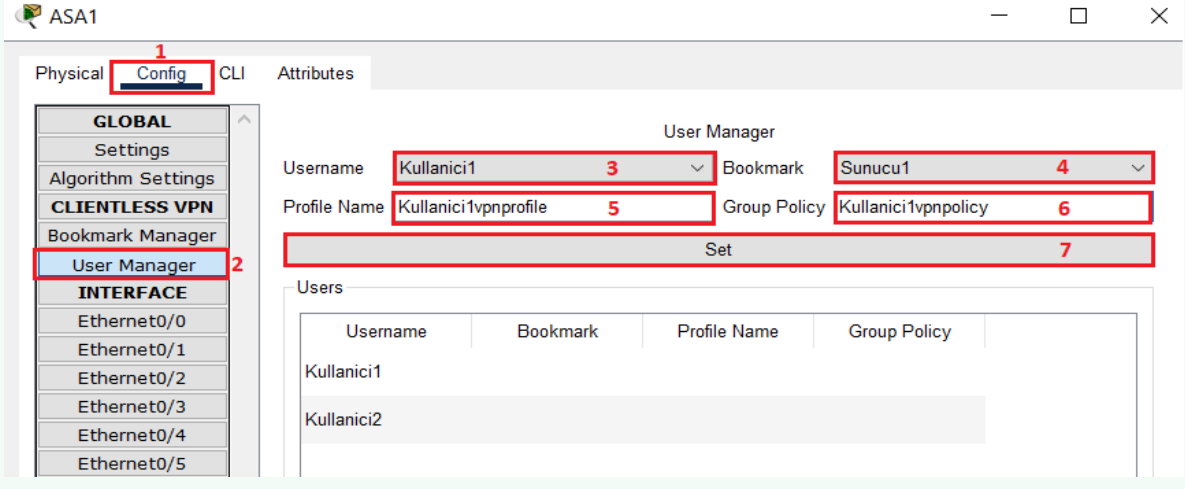
Görsel 4.27: Güvenlik duvarında CLIENTLESS VPN servisine Sunucu1'in web sayfasının adresinin eklenmesi

9. Adım: ASA1 güvenlik duvarında, Sunucu1 üzerindeki web sayfasına erişim sağlayacak kullanıcı veya kullanıcıları CLI moduna girerek aşağıdaki şekilde oluşturunuz.

```
ASA1(config)#username Kullanici1 password Parola1

ASA1(config)#username Kullanici2 password Parola2
```

10. Adım: ASA1 güvenlik duvarında, Görsel 4.28'deki sırayla kullanıcı veya kullanıcılar için profil ve grup ilkesi oluşturunuz.



Görsel 4.28: Kullanıcılar için profil ve grup ilkesi oluşturma

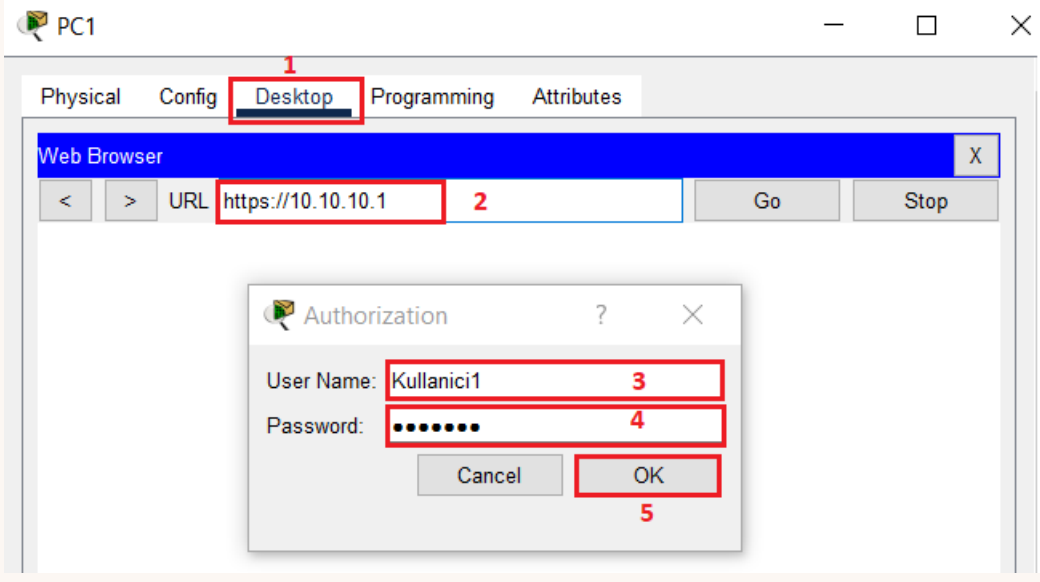
11. Adım: ASA1 güvenlik duvarında VPN'yi CLI moduna girerek aktif ediniz.

```
ASA1(config)#webvpn

ASA1(config-webvpn)#enable outside

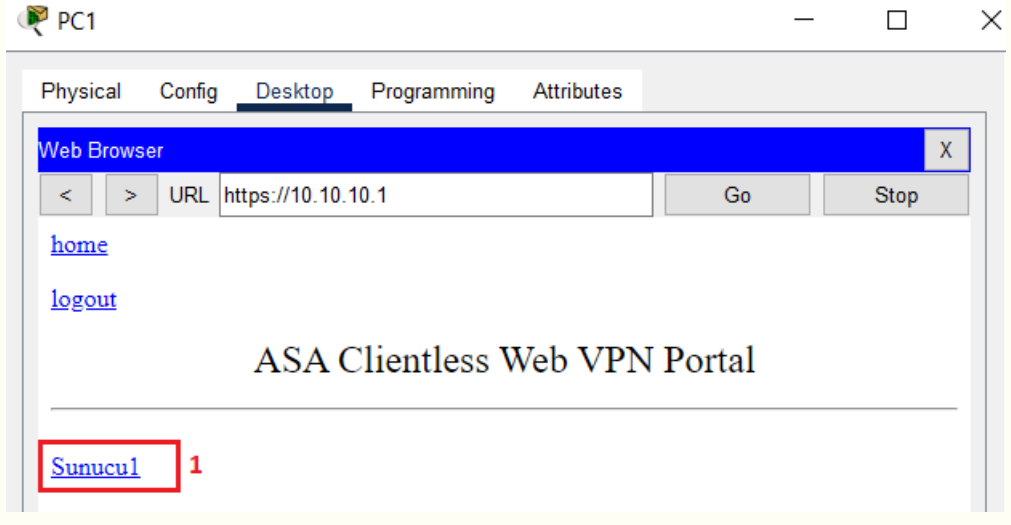
INFO: WebVPN and DTLS are enabled on 'outside'.
```

12. Adım: PC1 web tarayıcısında; ASA1 güvenlik duvarının IP adresini, erişim sağlayacak kullanıcı adı ve parolasını giriniz (Görsel 4.29).



Görsel 4.29: PC1 web tarayıcısından güvenlik duvarına erişim

13. Adım: Görsel 4.30'daki Sunucu1'e tıklayınız (Sunucu üzerindeki web sayfası Görsel 4.31'deki gibi açılır.).



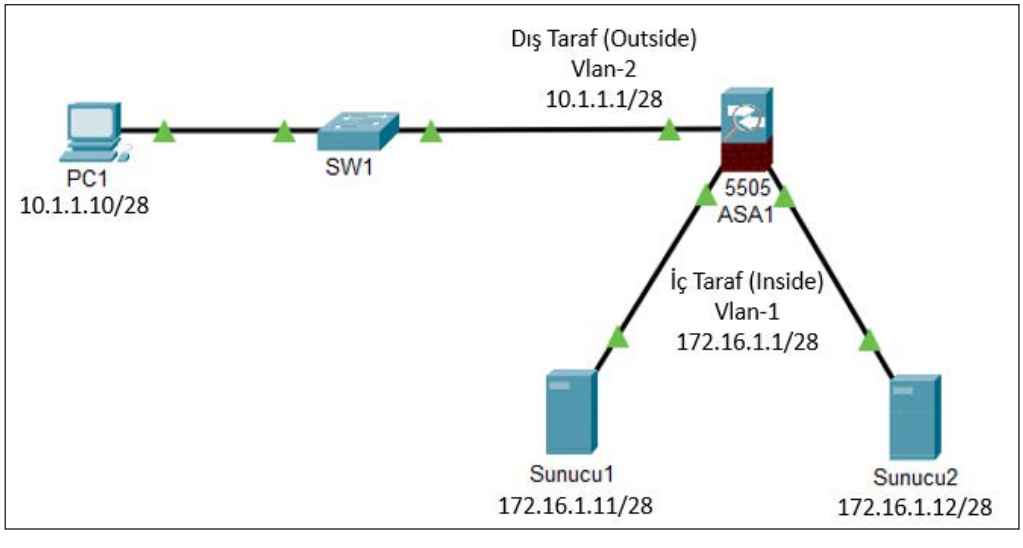
Görsel 4.30: PC1'den güvenlik duvarındaki VPN portalına erişim



Görsel 4.31: PC1'den VPN ile sunucu üzerindeki web sayfasına erişim

SIRA SİZDE

Ağ simülasyon programında Görsel 4.32'deki topolojiyi çizerek görsel üzerinde belirtilen ağ konfigürasyon bilgilerine göre güvenlik duvarı ve bilgisayarın IP adreslerini yapılandırınız. Bir kullanıcı ile sunucular üzerindeki web sayfalarına istemcisiz SSL VPN yöntemini kullanarak erişebilmek için güvenlik duvarı üzerinde gerekli konfigürasyonları yapınız. PC1 üzerinden oluşturduğunuz kullanıcı profili ile sunucular üzerindeki web sayfalarına erişim sağlayınız.



Görsel 4.32: İstemcisiz SSL web VPN ağ topolojisi

DEĞERLENDİRME

Çalışmanız aşağıda yer alan kontrol listesi kullanılarak değerlendirilecektir. Çalışmanızı yaparken değerlendirme ölçütlerini dikkate alınız.

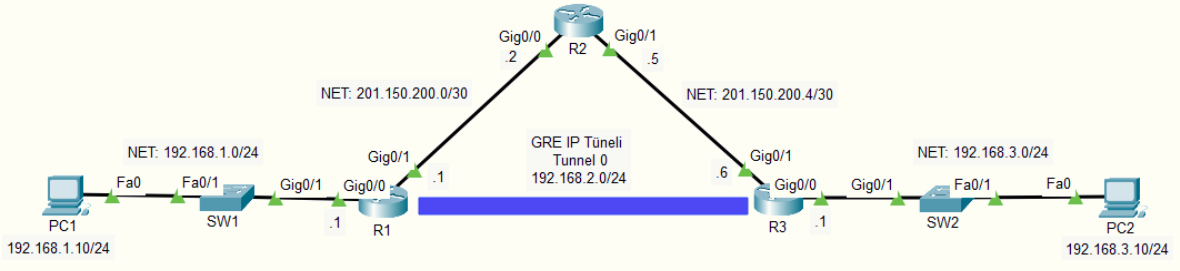
KONTROL LİSTESİ

ÖLÇÜTLER	EVET	HAYIR
1. Ağ topolojisinin çizimini gerçekleştirdi.		
2. Cihazların IP yapılandırmasını gerçekleştirdi.		
3. Sunucu servislerini yapılandırdı.		
4. Kullanıcı profili ve grup ilkesi oluşturdu.		
5. Sunucular ile güvenlik duvarını ilişkilendirdi.		
6. İstemcisi SSL VPN uygulamasını test etti.		

2. UYGULAMA

GRE protokolüyle IP tüneli uygulama işlemini verilen adımlar doğrultusunda gerçekleştiriniz.

1. Adım: Ağ simülasyon programında Görsel 4.33'teki ağ topolojisini oluşturunuz.



Görsel 4.33: GRE protokolü IP tüneli ağ topolojisi

2. Adım: R1 yönlendiricisinin arayüz IP adreslerini CLI moduna girerek aşağıdaki gibi konfigüre ediniz.

```
R1>enable
R1#configure terminal
R1(config)#interface gigabitEthernet 0/0
R1(config-if)#ip address 192.168.1.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface gigabitEthernet 0/1
R1(config-if)#ip address 201.150.200.1 255.255.255.252
R1(config-if)#no shutdown
```

3. Adım: R2 yönlendiricisinin arayüz IP adreslerini CLI moduna girerek aşağıdaki gibi konfigüre ediniz.

```
R2>enable
R2#configure terminal
R2(config)#interface gigabitEthernet 0/0
R2(config-if)#ip address 201.150.200.2 255.255.255.252
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#interface gigabitEthernet 0/1
R2(config-if)#ip address 201.150.200.5 255.255.255.252
R2(config-if)#no shutdown
```

4. Adım: R3 yönlendiricisinin arayüz IP adreslerini CLI moduna girerek aşağıdaki gibi konfigüre ediniz.

```
R3>enable
R3#configure terminal
R3(config)#interface gigabitEthernet 0/0
R3(config-if)#ip address 192.168.3.1 255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#interface gigabitEthernet 0/1
R3(config-if)#ip address 201.150.200.6 255.255.255.252
R3(config-if)#no shutdown
```

5. Adım: R1 yönlendiricisinin tünel konfigürasyonunu CLI moduna girerek aşağıdaki gibi gerçekleştiriniz.

```
R1(config)#interface tunnel 0
R1(config-if)#ip address 192.168.2.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#tunnel source gigabitEthernet 0/1
R1(config-if)#tunnel destination 201.150.200.6
```

6. Adım: R3 yönlendiricisinin tünel konfigürasyonunu CLI moduna girerek aşağıdaki şekilde gerçekleştiriniz.

```
R3(config)#interface tunnel 0
R3(config-if)#ip address 192.168.2.2 255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#tunnel source gigabitEthernet 0/1
R3(config-if)#tunnel destination 201.150.200.1
```

7. Adım: R1 yönlendiricisinin CLI moduna girerek aşağıdaki statik yönlendirme satırlarını giriniz.

R1(config)#ip route 192.168.3.0 255.255.255.0 192.168.2.2

R1(config)#ip route 201.150.200.4 255.255.255.252 201.150.200.2

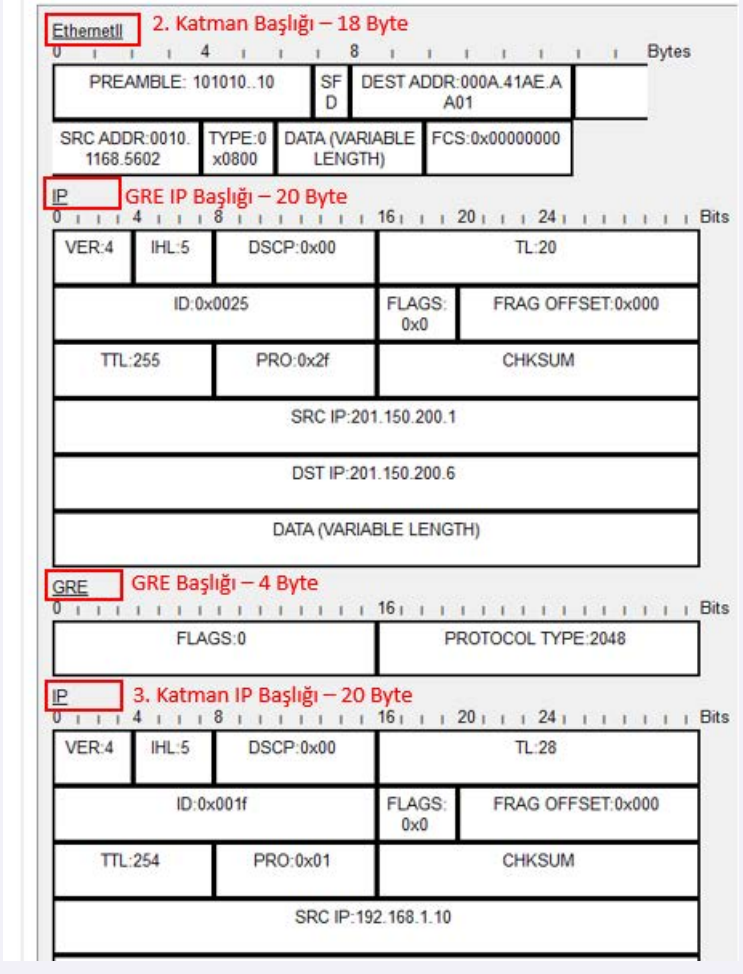
8. Adım: R3 yönlendiricisinin CLI moduna girerek aşağıdaki statik yönlendirme satırlarını giriniz.

R3(config)#ip route 192.168.1.0 255.255.255.0 192.168.2.1

R3(config)#ip route 201.150.200.0 255.255.255.252 201.150.200.5

9. Adım: PC1'in komut sistemine girerek PC2'nin IP adresine ping komutuyla bağlantı testi gerçekleştiriniz.

10. Adım: PC1'den PC2'ye **ping** komutuyla gerçekleştirilen bağlantı testinde simülasyon moduna geçiş yaparak trafik R1 yönlendiricisinin **GigabitEthernet 0/1** arayüzünden çıkarken ethernet çerçevesinin ikinci ve üçüncü katman başlığı arasına GRE başlığı ve yeni IP başlığı eklendiğini görüntüleyiniz (Görsel 4.34).



Görsel 4.34: R1 yönlendiricisinde ethernet çerçevesine GRE ve GRE IP başlığı eklenmesi

11. Adım: PC1'in komut sistemine girip, **tracert** komutuyla PC2'ye giden yolun haritasını çıkararak trafiğin topolojide görünen fiziksel yol üzerinden mi yoksa GRE IP tünelinden mi gittiğini görüntüleyiniz (Görsel 4.35).

```
C:\>tracert 192.168.3.10

Tracing route to 192.168.3.10 over a maximum of 30 hops:

  1    0 ms      0 ms      0 ms      192.168.1.1
  2    1 ms      1 ms      0 ms      192.168.2.2
  3    1 ms      0 ms      1 ms      192.168.3.10

Trace complete.
```

Görsel 4.35: PC1'den tracert komutuyla PC2'ye giden yolun haritasının çıkarılması

12. Adım: PC2'nin komut sistemine girip, tracert komutuyla PC1'e giden yolun haritasını çıkararak trafiğin topolojide görünen fiziksel yol üzerinden mi yoksa GRE IP tünelinden mi gittiğini görüntüleyiniz (Görsel 4.36).

```
C:\>tracert 192.168.1.10

Tracing route to 192.168.1.10 over a maximum of 30 hops:

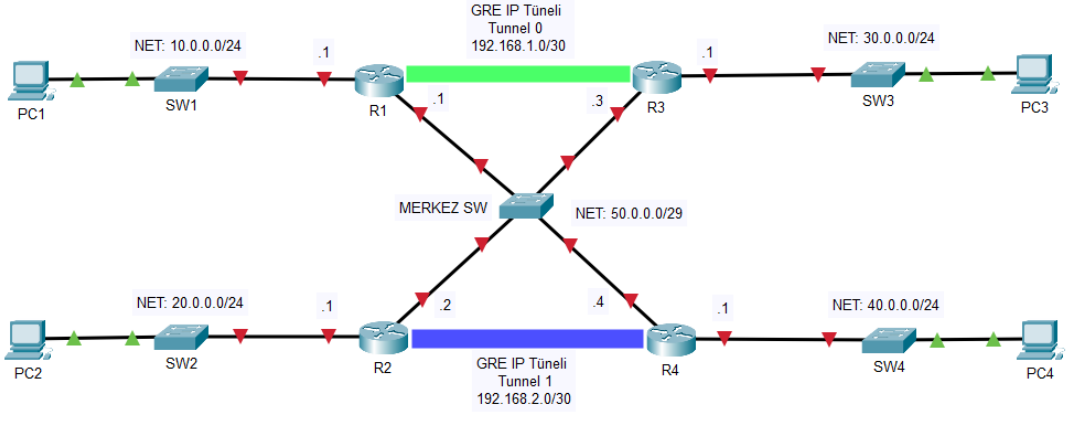
  1    0 ms      0 ms      0 ms      192.168.3.1
  2    0 ms      0 ms      1 ms      192.168.2.1
  3    0 ms      0 ms      0 ms      192.168.1.10

Trace complete.
```

Görsel 4.36: PC2'den tracert komutuyla PC2'ye giden yolun haritasının çıkarılması

SIRA SİZDE

Ağ simülasyon programında Görsel 4.37'deki topolojiyi çizerek görsel üzerinde belirtilen ağ konfigürasyon bilgilerine göre yönlendirici ve bilgisayarların IP adreslerini yapılandırınız. Yönlendiriciler üzerinde gerekli statik yönlendirmeleri yaptıktan sonra GRE IP tünellerini oluşturunuz. PC1-PC3 arasındaki ağ trafiğinin Tunnel 0, PC2-PC4 arasındaki trafiğin Tunnel 1 üzerinden, diğer ağ trafiğinin ise herhangi bir tünele girmeden iletildiğini test ediniz.



Görsel 4.37: GRE protokolüyle oluşturulmuş iki IP tüneli ağ topolojisi

DEĞERLENDİRME

Çalışmanız aşağıda yer alan kontrol listesi kullanılarak değerlendirilecektir. Çalışmanızı yaparken değerlendirme ölçütlerini dikkate alınız.

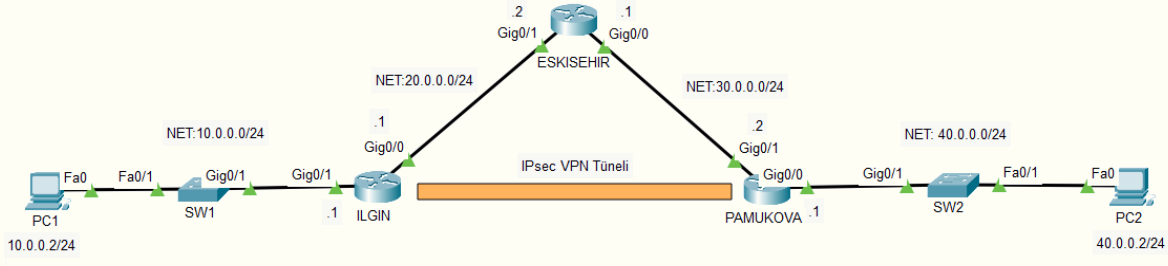
KONTROL LİSTESİ

ÖLÇÜTLER	EVET	HAYIR
1. Ağ topolojisinin çizimini gerçekleştirdi.		
2. Yönlendiricilerin IP yapılandırmasını gerçekleştirdi.		
3. Yönlendiriciler üzerinden gerekli statik yönlendirmeleri gerçekleştirdi.		
4. Yönlendiriciler üzerinden tünel konfigürasyonlarını gerçekleştirdi.		
5. Bilgisayarların IP adreslerini yapılandırdı.		
6. GRE IP tünellerinden iletilmesi gereken ağ trafiğini test etti.		
7. GRE IP tünellerine girmeden iletilmesi gereken ağ trafiğini test etti.		

IPsec VPN tüneli uygulama işlemini verilen adımlar doğrultusunda gerçekleştiriniz.

3. UYGULAMA

1. Adım: Ağ simülasyon programında Görsel 4.38'deki ağ topolojisini oluşturunuz.



Görsel 4.38: IPsec VPN tüneli ağ topolojisi

2. Adım: ILGIN ve PAMUKOVA yönlendiricilerinde, IPsec VPN uygulamasını gerçekleştirebilmek için **securityk9 teknoloji paketini** CLI moduna girerek aşağıdaki şekilde aktif ediniz.

```
ILGIN(config)#license boot module c1900 technology-package securityk9
ILGIN(config)#exit
ILGIN#reload
PAMUKOVA(config)#license boot module c1900 technology-package securityk9
PAMUKOVA(config)#exit
PAMUKOVA#reload
```

3. Adım: ILGIN yönlendiricisinin arayüz IP adresi yapılandırmasını CLI moduna girerek aşağıdaki şekilde konfigüre ediniz.

```
ILGIN(config)#interface GigabitEthernet0/0
ILGIN(config-if)#ip address 20.0.0.1 255.255.255.0
ILGIN(config-if)#no shutdown
ILGIN(config-if)#interface GigabitEthernet0/1
ILGIN(config-if)#ip address 10.0.0.1 255.255.255.0
ILGIN(config-if)#no shutdown
```

4. Adım: ESKISEHIR yönlendiricisinin arayüz IP adresi yapılandırmasını CLI moduna girerek aşağıdaki şekilde konfigüre ediniz.

```
ESKISEHIR(config)#interface GigabitEthernet0/0
ESKISEHIR(config-if)#ip address 20.0.0.2 255.255.255.0
ESKISEHIR(config-if)#no shutdown
ESKISEHIR(config-if)#interface GigabitEthernet0/1
ESKISEHIR(config-if)#ip address 30.0.0.1 255.255.255.0
ESKISEHIR(config-if)#no shutdown
```

5. Adım: PAMUKOVA yönlendiricisinin arayüz IP adresi yapılandırmasını CLI moduna girerek aşağıdaki şekilde konfigüre ediniz.

```
PAMUKOVA(config)#interface GigabitEthernet0/0
PAMUKOVA(config-if)#ip address 40.0.0.1 255.255.255.0
PAMUKOVA(config-if)#no shutdown
PAMUKOVA(config-if)#interface GigabitEthernet0/1
PAMUKOVA(config-if)#ip address 30.0.0.2 255.255.255.0
PAMUKOVA(config-if)#no shutdown
```

6. Adım: ILGIN yönlendiricisinde, CLI moduna girerek IPsec VPN tüneli **faz-1** müzakereleri için ISAKMP politikasını aşağıdaki şekilde oluşturunuz.

```
ILGIN(config)#crypto isakmp policy 10
ILGIN(config-isakmp)#encr aes 256
ILGIN(config-isakmp)#authentication pre-share
ILGIN(config-isakmp)#group 5
```

7. Adım: PAMUKOVA yönlendiricisinde, CLI moduna girerek IPsec VPN tüneli **faz-1** müzakereleri için **ISAKMP** politikasını aşağıdaki şekilde oluşturunuz.

```
PAMUKOVA(config)#crypto isakmp policy 10
PAMUKOVA(config-isakmp)#encr aes 256
PAMUKOVA(config-isakmp)#authentication pre-share
PAMUKOVA(config-isakmp)#group 5
```

8. Adım: ILGIN yönlendiricisine, PAMUKOVA yönlendiricisiyle paylaşılacak anahtarı ve hedef IP adresini giriniz.

```
ILGIN(config)#crypto isakmp key TEST address 30.0.0.2
```

9. Adım: PAMUKOVA yönlendiricisine, ILGIN yönlendiricisiyle paylaşılacak anahtarı ve hedef IP adresini giriniz.

```
PAMUKOVA(config)#crypto isakmp key TEST address 20.0.0.1
```

10. Adım: ILGIN ve PAMUKOVA yönlendiricilerinde, IPsec anlaşması için faz-2 ilkesini aşağıdaki şekilde oluşturunuz.

```
ILGIN(config)#crypto ipsec transform-set ILGIN-PAMUKOVA esp-aes 256 esp-sha-hmac
PAMUKOVA(config)#crypto ipsec transform-set PAMUKOVA-ILGIN esp-aes 256 esp-sha-hmac
```

11. Adım: ILGIN ve PAMUKOVA yönlendiricilerinde, tünel üzerinden şifreli geçiş yapacak trafik için ACL [Access Control List (Erişim Kontrol Listesi)] oluşturunuz.

```
ILGIN(config)#access-list 100 permit ip 10.0.0.0 0.0.0.255 40.0.0.0 0.0.0.255
PAMUKOVA(config)#access-list 100 permit ip 40.0.0.0 0.0.0.255 10.0.0.0 0.0.0.255
```

12. Adım: ILGIN yönlendiricisinde, kripto haritası oluşturunuz ve daha önce oluşturulan ACL ile eşleştirme konfigürasyonunu yapınız.

```
ILGIN(config)#crypto map IPSEC-MAP 10 ipsec-isakmp
ILGIN(config-crypto-map)#set peer 30.0.0.2
ILGIN(config-crypto-map)#set pfs group5
ILGIN(config-crypto-map)#set security-association lifetime seconds 86400
ILGIN(config-crypto-map)#set transform-set ILGIN-PAMUKOVA
ILGIN(config-crypto-map)#match address 100
```

13. Adım: PAMUKOVA yönlendiricisinde, kripto haritası oluşturunuz ve daha önce oluşturulan ACL ile eşleştirme konfigürasyonunu yapınız.

```
PAMUKOVA(config)#crypto map IPSEC-MAP 10 ipsec-isakmp
PAMUKOVA(config-crypto-map)#set peer 20.0.0.1
PAMUKOVA(config-crypto-map)#set pfs group5
PAMUKOVA(config-crypto-map)#set security-association lifetime seconds 86400
PAMUKOVA(config-crypto-map)#set transform-set PAMUKOVA-ILGIN
PAMUKOVA(config-crypto-map)#match address 100
```

14. Adım: ILGIN ve PAMUKOVA yönlendiricilerine varsayılan statik rota yazınız ve trafiği varsayılan ağ geçidine yönlendiriniz.

```
ILGIN(config)#ip route 0.0.0.0 0.0.0.0 GigabitEthernet0/0
PAMUKOVA(config)#ip route 0.0.0.0 0.0.0.0 GigabitEthernet0/1
```

15. Adım: ILGIN ve PAMUKOVA yönlendiricilerinin çıkış arayüzlerine, oluşturulan kripto haritalarını ekleyiniz.

```
ILGIN(config)#interface GigabitEthernet0/0
ILGIN(config-if)#crypto map IPSEC-MAP
PAMUKOVA(config)#interface GigabitEthernet0/1
PAMUKOVA(config-if)#crypto map IPSEC-MAP
```

16. Adım: PC1 ve PC2'nin IP adres yapılandırmasını aşağıdaki gibi konfigüre ediniz.

PC1		**PC2**	
IP Adresi	: 10.0.0.2	**IP Adresi**	: 40.0.0.2
Alt Ağ Maskesi	: 255.255.255.0	**Alt Ağ Maskesi**	: 255.255.255.0
Varsayılan Ağ Geçidi	: 10.0.0.1	**Varsayılan Ağ Geçidi**	: 40.0.0.1

17. Adım: PC1'in komut sistemine girerek PC2'nin IP adresine ping komutuyla bağlantı testi gerçekleştiriniz (Görsel 4.39).

```
C:\>ping 40.0.0.2

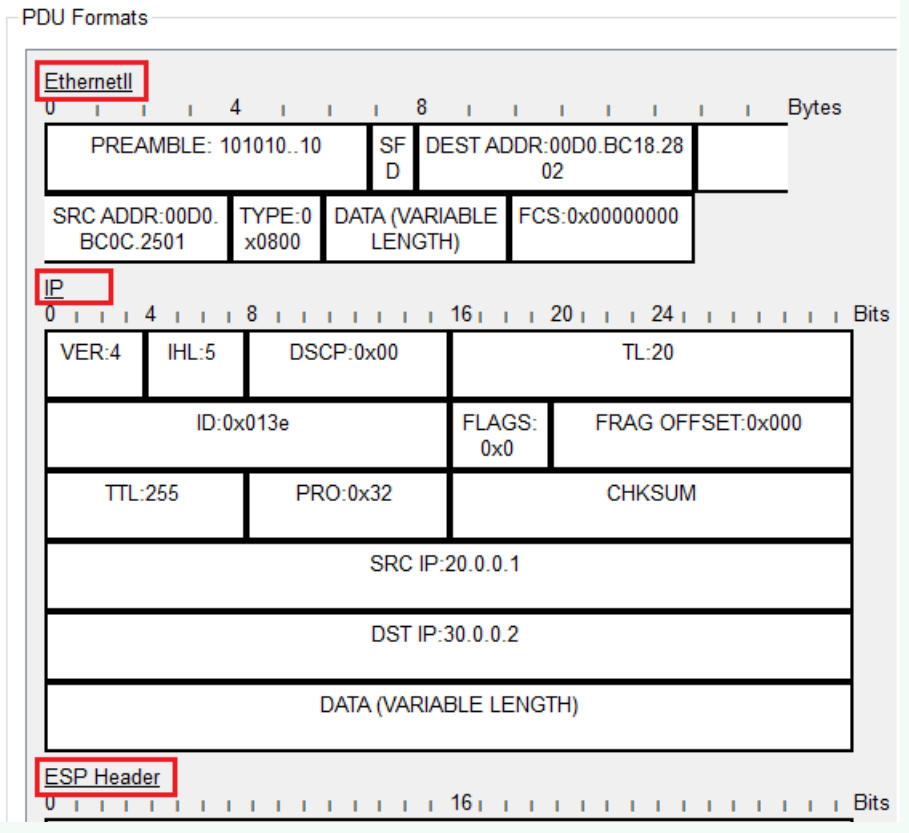
Pinging 40.0.0.2 with 32 bytes of data:

Reply from 40.0.0.2: bytes=32 time<1ms TTL=126
Reply from 40.0.0.2: bytes=32 time=11ms TTL=126
Reply from 40.0.0.2: bytes=32 time<1ms TTL=126
Reply from 40.0.0.2: bytes=32 time=1ms TTL=126

Ping statistics for 40.0.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 11ms, Average = 3ms
```

Görsel 4.39: PC1'den PC2'nin IP adresine ping komutuyla bağlantı testi

18. Adım: PC1'den PC2'ye ping komutuyla gerçekleştirilen bağlantı testinde simülasyon moduna geçiş yaparak trafik **ILGIN** yönlendiricisinin **GigabitEthernet 0/0** arayüzünden çıkarken ethernet çerçevesinin ikinci ve üçüncü katman başlığı arasına **ESP** başlığı ve yeni **IP** başlığı eklendiğini, orijinal IP paketinin şifrelendiğini görüntüleyiniz (Görsel 4.40).



Görsel 4.40: ILGIN yönlendiricisinde ethernet çerçevesine ESP ve yeni IP başlığı eklenmesi

19. Adım: PC1'in komut sistemine girip, tracert komutuyla PC2'ye giden yolun haritasını çıkararak trafiğin topolojide görünen fiziksel yol üzerinden mi yoksa IPsec tünelinden mi gittiğini görüntüleyiniz (Görsel 4.41).

```
C:\>tracert 10.0.0.2

Tracing route to 10.0.0.2 over a maximum of 30 hops:

  1    0 ms      1 ms      1 ms      40.0.0.1
  2    *         *         *         Request timed out.
  3    0 ms      0 ms      0 ms      10.0.0.2

Trace complete.
```

Görsel 4.41: PC1'den tracert komutuyla PC2'ye giden yolun haritasının çıkarılması

20. Adım: PC2'nin komut sistemine girip, tracert komutuyla PC1'e giden yolun haritasını çıkararak trafiğin topolojide görünen fiziksel yol üzerinden mi yoksa IPsec tünelinden mi gittiğini görüntüleyiniz (Görsel 4.42).

```
C:\>tracert 40.0.0.2

Tracing route to 40.0.0.2 over a maximum of 30 hops:

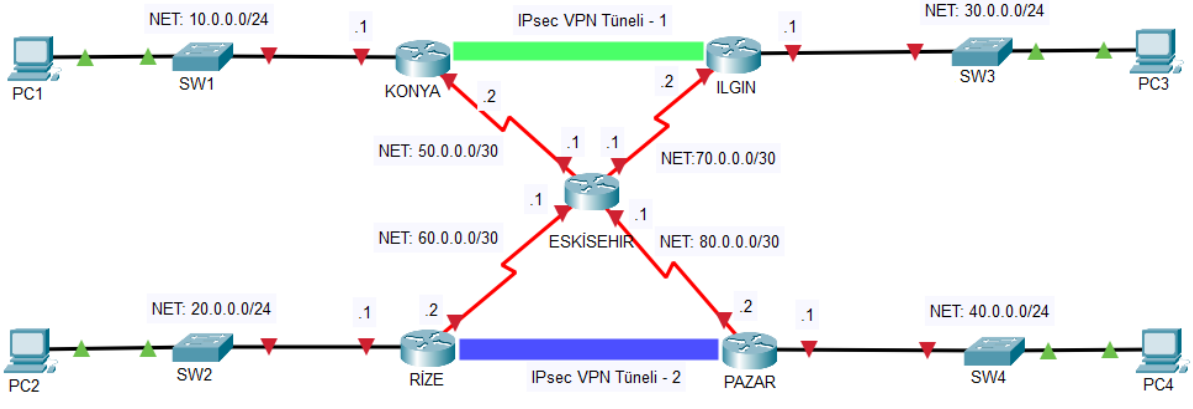
  1    0 ms      1 ms      0 ms      10.0.0.1
  2    *         *         *         Request timed out.
  3    10 ms     0 ms      1 ms      40.0.0.2

Trace complete.
```

Görsel 4.42: PC2'den tracert komutuyla PC1'ye giden yolun haritasının çıkarılması

SIRA SİZDE

Ağ simülasyon programında Görsel 4.43'teki topolojiyi çizerek görsel üzerinde belirtilen ağ konfigürasyon bilgilerine göre yönlendirici ve bilgisayarların IP adreslerini yapılandırınız. Yönlendiriciler üzerinde gerekli statik yönlendirmeleri yaptıktan sonra IPsec VPN tünellerini oluşturunuz. PC1-PC3 arasındaki trafiğin 1 numaralı, PC2-PC4 arasındaki trafiğin 2 numaralı tünel üzerinden, diğer ağ trafiğinin ise herhangi bir tünele girmeden iletildiğini test ediniz.



Görsel 4.43: IPsec protokolüyle iki VPN tüneli oluşturma ağ topolojisi

DEĞERLENDİRME

Çalışmanız aşağıda yer alan kontrol listesi kullanılarak değerlendirilecektir. Çalışmanızı yaparken değerlendirme ölçütlerini dikkate alınız.

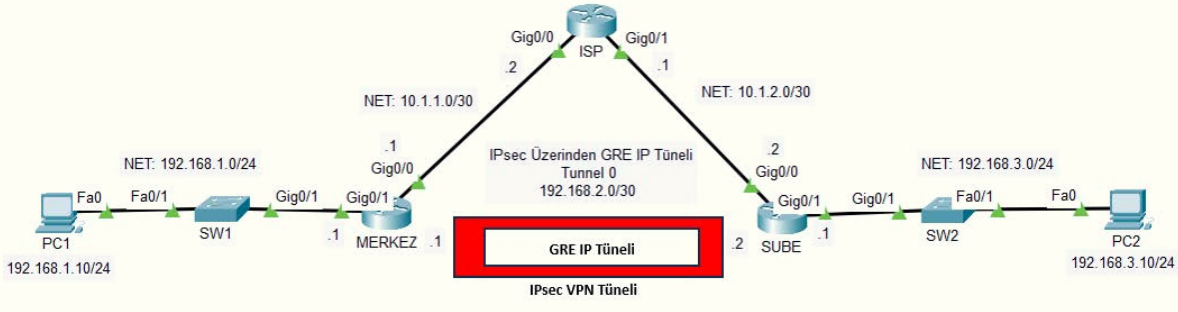
KONTROL LİSTESİ

ÖLÇÜTLER	EVET	HAYIR
1. Ağ topolojisinin çizimini gerçekleştirdi.		
2. Yönlendiricilerin IP yapılandırmasını gerçekleştirdi.		
3. Yönlendiriciler üzerinde gerekli statik yönlendirmeleri gerçekleştirdi.		
4. Yönlendiriciler üzerinde tünel konfigürasyonlarını gerçekleştirdi.		
5. Bilgisayarların IP adreslerini yapılandırdı.		
6. IPsec VPN tünellerinden iletilmesi gereken ağ trafiğini test etti.		
7. IPsec VPN tünellerine girmeden iletilmesi gereken ağ trafiğini test etti.		

IPsec VPN tüneli üzerinden GRE protokolüyle IP tüneli oluşturma ve OSPF dinamik yönlendirme protokolü kullanılarak 192.168.1.0/24 ve 192.168.3.0/24 ağlarının, oluşturulan tünel üzerinden haberleşmesi işlemini verilen adımlar doğrultusunda gerçekleştiriniz.

4. UYGULAMA

1. Adım: Ağ simülasyon programında Görsel 4.44'teki ağ topolojisini oluşturunuz.



Görsel 4.44: IPsec üzerinden GRE protokolüyle IP tüneli ağ topolojisi

2. Adım: MERKEZ ve SUBE yönlendiricilerinde, IPsec VPN uygulamasını gerçekleştirebilmek için securityk9 teknoloji paketini CLI moduna girerek aşağıdaki şekilde aktif ediniz.

```
MERKEZ(config)#license boot module c1900 technology-package securityk9
MERKEZ(config)#exit
MERKEZ#reload
SUBE(config)#license boot module c1900 technology-package securityk9
SUBE(config)#exit
SUBE#reload
```

3. Adım: MERKEZ yönlendiricisinin arayüz IP adreslerini CLI moduna girerek aşağıdaki gibi konfigüre ediniz.

```
MERKEZ>enable
MERKEZ #configure terminal
MERKEZ(config)#interface gigabitEthernet 0/0
MERKEZ(config-if)#ip address 10.1.1.1 255.255.255.252
MERKEZ(config-if)#no shutdown
MERKEZ(config-if)#exit
MERKEZ(config)#interface gigabitEthernet 0/1
MERKEZ(config-if)#ip address 192.168.1.1 255.255.255.0
MERKEZ(config-if)#no shutdown
```

4. Adım: SUBE yönlendiricisinin arayüz IP adreslerini CLI moduna girerek aşağıdaki gibi konfigüre ediniz.

```
SUBE>enable
SUBE #configure terminal
SUBE(config)#interface gigabitEthernet 0/0
SUBE(config-if)#ip address 10.1.2.2 255.255.255.252
SUBE(config-if)#no shutdown
SUBE(config-if)#exit
SUBE(config)#interface gigabitEthernet 0/1
SUBE(config-if)#ip address 192.168.3.1 255.255.255.0
SUBE(config-if)#no shutdown
```

5. Adım: ISP yönlendiricisinin arayüz IP adreslerini CLI moduna girerek aşağıdaki gibi konfigüre ediniz.

```
ISP>enable
ISP#configure terminal
ISP(config)#interface gigabitEthernet 0/0
ISP(config-if)#ip address 10.1.1.2 255.255.255.252
ISP(config-if)#no shutdown
ISP(config-if)#exit
ISP(config)#interface gigabitEthernet 0/1
ISP(config-if)#ip address 10.1.2.1 255.255.255.252
ISP(config-if)#no shutdown
```

6. Adım: MERKEZ yönlendiricisinin GRE tünel konfigürasyonunu CLI moduna girerek aşağıdaki gibi gerçekleştiriniz.

```
MERKEZ(config)#interface tunnel 0
MERKEZ(config-if)#ip address 192.168.2.1 255.255.255.252
MERKEZ(config-if)#no shutdown
MERKEZ(config-if)#tunnel source gigabitEthernet 0/0
MERKEZ(config-if)#tunnel destination 10.1.2.2
```

7. Adım: SUBE yönlendiricisinin GRE tünel konfigürasyonunu CLI moduna girerek aşağıdaki şekilde gerçekleştiriniz.

```
SUBE(config)#interface tunnel 0
SUBE(config-if)#ip address 192.168.2.2 255.255.255.252
SUBE(config-if)#no shutdown
SUBE(config-if)#tunnel source gigabitEthernet 0/0
SUBE(config-if)#tunnel destination 10.1.1.1
```

8. Adım: MERKEZ yönlendiricisinde, OSPF dinamik yönlendirme protokolüyle ağların anonsunu CLI moduna girerek aşağıdaki şekilde gerçekleştiriniz.

```
MERKEZ(config)#router ospf 1
MERKEZ(config-router)#network 192.168.1.0 0.0.0.255 area 0
MERKEZ(config-router)#network 192.168.2.0 0.0.0.3 area 0
```

9. Adım: SUBE yönlendiricisinde, OSPF dinamik yönlendirme protokolüyle ağların anonsunu CLI moduna girerek aşağıdaki şekilde gerçekleştiriniz.

```
SUBE(config)#router ospf 1
SUBE(config-router)#network 192.168.2.0 0.0.0.3 area 0
SUBE(config-router)#network 192.168.3.0 0.0.0.255 area 0
```

10. Adım: MERKEZ yönlendiricisinde, CLI moduna girerek IPsec VPN tüneli faz-1 müzakereleri için ISAKMP politikasını aşağıdaki şekilde oluşturunuz.

```
MERKEZ(config)#crypto isakmp policy 10
MERKEZ(config-isakmp)#encr aes 256
MERKEZ(config-isakmp)#authentication pre-share
MERKEZ(config-isakmp)#group 5
```

11. Adım: SUBE yönlendiricisinde, CLI moduna girerek IPsec VPN tüneli faz-1 müzakereleri için ISAKMP politikasını aşağıdaki şekilde oluşturunuz.

```
SUBE(config)#crypto isakmp policy 10
SUBE(config-isakmp)#encr aes 256
SUBE(config-isakmp)#authentication pre-share
SUBE(config-isakmp)#group 5
```

12. Adım: MERKEZ yönlendiricisine, SUBE yönlendiricisiyle paylaşılacak anahtarı ve hedef IP adresini giriniz.

```
MERKEZ(config)#crypto isakmp key TEST address 10.1.2.2
```

13. Adım: SUBE yönlendiricisine, MERKEZ yönlendiricisiyle paylaşılacak anahtarı ve hedef IP adresini giriniz.

```
SUBE(config)#crypto isakmp key TEST address 10.1.1.1
```

14. Adım: MERKEZ ve SUBE yönlendiricilerinde, IPsec anlaşması için faz-2 ilkesini aşağıdaki şekilde oluşturunuz.

```
MERKEZ(config)#crypto ipsec transform-set MERKEZ-SUBE esp-aes 256 esp-sha-hmac
SUBE(config)#crypto ipsec transform-set SUBE-MERKEZ esp-aes 256 esp-sha-hmac
```

15. Adım: MERKEZ ve SUBE yönlendiricilerinde, tünel üzerinden şifreli geçiş yapacak trafik için ACL oluşturunuz.

```
MERKEZ(config)#access-list 100 permit gre any any
SUBE(config)#access-list 100 permit gre any any
```

16. Adım: MERKEZ yönlendiricisinde, kripto haritası oluşturunuz ve daha önce oluşturulan ACL ile eşleştirme konfigürasyonunu yapınız.

```
MERKEZ(config)#crypto map IPSEC-MAP 10 ipsec-isakmp
MERKEZ(config-crypto-map)#set peer 10.1.2.2
MERKEZ(config-crypto-map)#set pfs group5
MERKEZ(config-crypto-map)#set security-association lifetime seconds 86400
MERKEZ(config-crypto-map)#set transform-set MERKEZ-SUBE
MERKEZ(config-crypto-map)#match address 100
```

17. Adım: SUBE yönlendiricisinde, kripto haritası oluşturunuz ve daha önce oluşturulan ACL ile eşleştirme konfigürasyonunu yapınız.

```
SUBE(config)#crypto map IPSEC-MAP 10 ipsec-isakmp
SUBE(config-crypto-map)#set peer 10.1.1.1
SUBE(config-crypto-map)#set pfs group5
SUBE(config-crypto-map)#set security-association lifetime seconds 86400
SUBE(config-crypto-map)#set transform-set SUBE-MERKEZ
SUBE(config-crypto-map)#match address 100
```

18. Adım: MERKEZ ve ŞUBE yönlendiricilerine, varsayılan statik rotayı yazınız ve trafiği varsayılan ağ geçidine yönlendiriniz.

```
MERKEZ(config)#ip route 0.0.0.0 0.0.0.0 GigabitEthernet0/0
SUBE(config)#ip route 0.0.0.0 0.0.0.0 GigabitEthernet0/0
```

19. Adım: MERKEZ ve SUBE yönlendiricilerinin çıkış arayüzlerine, oluşturulan kripto haritalarını ekleyiniz.

```
MERKEZ(config)#interface GigabitEthernet0/0
MERKEZ(config-if)#crypto map IPSEC-MAP
SUBE(config)#interface GigabitEthernet0/0
SUBE(config-if)#crypto map IPSEC-MAP
```

20. Adım: MERKEZ ve SUBE yönlendiricilerinin yönlendirme tablosundaki OSPF rotalarını CLI moduna girerek aşağıdaki şekilde görüntüleyiniz.

```
MERKEZ#show ip route ospf
O    192.168.3.0 [110/1001] via 192.168.2.2, 01:46:34, Tunnel0

SUBE#show ip route ospf
O    192.168.1.0 [110/1001] via 192.168.2.1, 01:49:22, Tunnel0
```

NOT: OSPF dinamik yönlendirme protokolü çok noktaya yayın (multicast) paketleriyle çalışır. IPsec tüneli çok noktaya yayın trafiğini geçirmez ancak çok noktaya yayın trafiği önce GRE IP tünelinden, GRE IP tüneli de IPsec tünelinden geçirildiğinde trafik sorunsuz bir şekilde iletilir.

21. Adım: PC1 ve PC2'nin IP adres yapılandırmasını aşağıdaki gibi konfigüre ediniz.

PC1		**PC2**	
IP Adresi	: 192.168.1.10	**IP Adresi**	: 192.168.3.10
Alt Ağ Maskesi	: 255.255.255.0	**Alt Ağ Maskesi**	: 255.255.255.0
Varsayılan Ağ Geçidi	: 192.168.1.1	**Varsayılan Ağ Geçidi**	: 192.168.3.1

22. Adım: PC1'in komut sistemine girerek PC2'nin IP adresine ping komutuyla bağlantı testi gerçekleştiriniz (Görsel 4.45).

```
C:\>ping 192.168.3.10

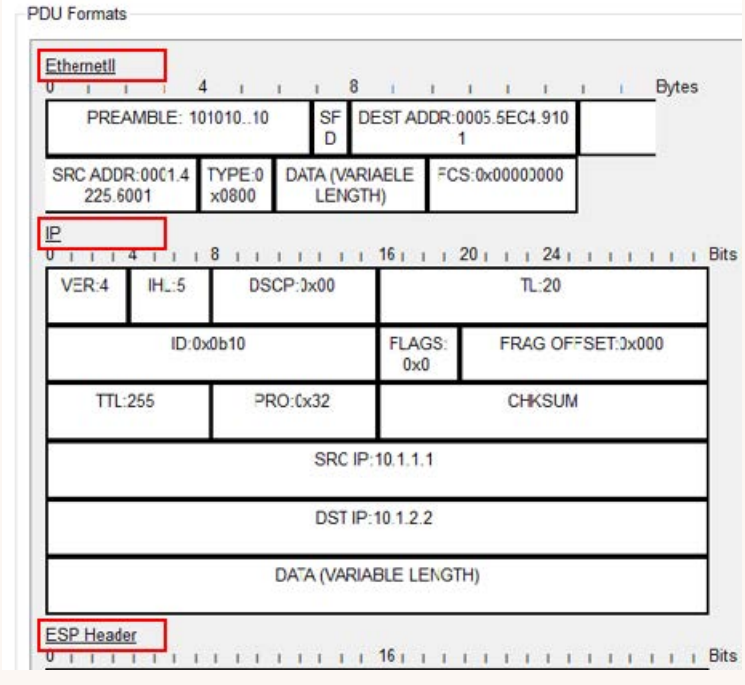
Pinging 192.168.3.10 with 32 bytes of data:

Reply from 192.168.3.10: bytes=32 time=1ms TTL=126
Reply from 192.168.3.10: bytes=32 time=10ms TTL=126
Reply from 192.168.3.10: bytes=32 time=1ms TTL=126
Reply from 192.168.3.10: bytes=32 time=10ms TTL=126

Ping statistics for 192.168.3.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 10ms, Average = 5ms
```

Görsel 4.45: PC1'den PC2'nin IP adresine ping komutuyla bağlantı testi

23. Adım: PC1'den PC2'ye ping komutuyla gerçekleştirilen bağlantı testinde simülasyon moduna geçiş yaparak trafik MERKEZ yönlendiricisinin GigabitEthernet 0/0 arayüzünden çıkarken ethernet çerçevesinin ikinci ve üçüncü katman başlığı arasına, ESP başlığı ve yeni IP başlığı eklendiğini (Görsel 4.46), IPsec VPN tünelinden geçiş yapan GRE paketlerinin ise şifrelendiği için görüntülenmediğini inceleyiniz.



Görsel 4.46: MERKEZ yönlendiricisinde ethernet çerçevesine ESP ve yeni IP başlığı eklenmesi

24. Adım: PC1'in komut sistemine girip, tracert komutuyla PC2'ye giden yolun haritasını çıkararak (Görsel 4.47) trafiğin topolojide görünen fiziksel yol üzerinden mi yoksa GRE IP tünelinden mi gittiğini görüntüleyiniz.

```
C:\>tracert 192.168.3.10

Tracing route to 192.168.3.10 over a maximum of 30 hops:

  1    0 ms      0 ms      0 ms      192.168.1.1
  2    1 ms      1 ms      0 ms      192.168.2.2
  3    1 ms      0 ms      1 ms      192.168.3.10

Trace complete.
```

Görsel 4.47: PC1'den tracert komutuyla PC2'ye giden yolun haritasının çıkarılması

25. Adım: PC2'nin komut sistemine girip, tracert komutuyla PC1'e giden yolun haritasını çıkararak (Görsel 4.48) trafiğin topolojide görünen fiziksel yol üzerinden mi yoksa GRE IP tünelinden mi gittiğini görüntüleyiniz.

```
C:\>tracert 192.168.1.10

Tracing route to 192.168.1.10 over a maximum of 30 hops:

  1    0 ms      0 ms      0 ms      192.168.3.1
  2    0 ms      0 ms      1 ms      192.168.2.1
  3    0 ms      0 ms      0 ms      192.168.1.10

Trace complete.
```

Görsel 4.48: PC2'den tracert komutuyla PC2'ye giden yolun haritasının çıkarılması

26. Adım: MERKEZ yönlendiricisinde ISAKMP politikalarını CLI moduna girerek aşağıdaki gibi görüntüleyiniz (Görsel 4.49).

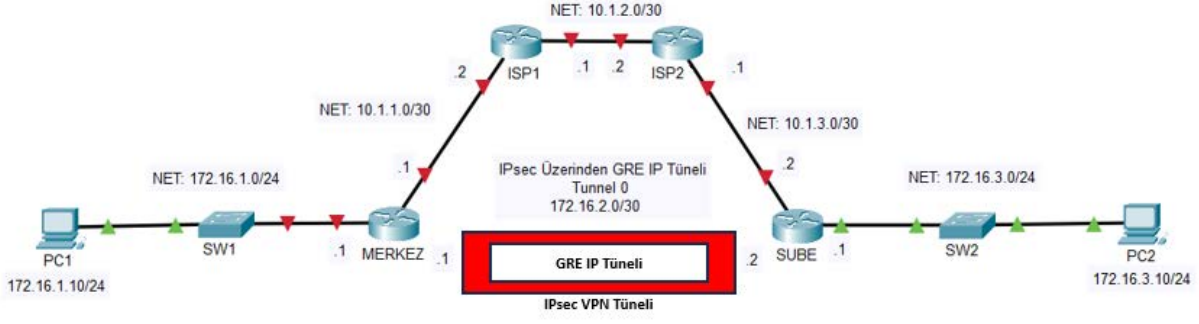
```
MERKEZ#show crypto isakmp policy

Global IKE policy
Protection suite of priority 10
        encryption algorithm:   AES - Advanced Encryption Standard (256 bit keys).
        hash algorithm:         Secure Hash Standard
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #5 (1536 bit)
        lifetime:               86400 seconds, no volume limit
```

Görsel 4.49: ISAKMP politikalarının görüntülenmesi

SIRA SİZDE

Ağ simülasyon programında Görsel 4.50'deki ağ topolojisini çiziniz. Belirtilen ağ konfigürasyon bilgilerine göre yönlendirici ile bilgisayarların IP adreslerini ve GRE IP tünelini yapılandırınız. Yönlendiricileri, 172.16.1.0/24, 172.16.2.0/30 ve 172.16.3.0/24 ağlarını OSPF dinamik yönlendirme protokolünü kullanarak diğer ağları ise statik yönlendirme yöntemi ile haberleşecek şekilde konfigüre ediniz. Yönlendiriciler üzerinde gerekli statik yönlendirmeleri yaptıktan sonra IPsec VPN tünelini oluşturarak GRE trafiğinin bu tünelden geçmesini sağlayınız. PC1-PC2 arasındaki ağ trafiğinin IPsec üzerinden GRE tünelinden gittiğini test ediniz.



Görsel 4.50: IPsec üzerinden GRE protokolüyle IP tünel ağ topolojisi

DEĞERLENDİRME

Çalışmanız aşağıda yer alan kontrol listesi kullanılarak değerlendirilecektir. Çalışmanızı yaparken değerlendirme ölçütlerini dikkate alınız.

KONTROL LİSTESİ

ÖLÇÜTLER	EVET	HAYIR
1. Ağ topolojisinin çizimini gerçekleştirdi.		
2. Yönlendiricilerin IP yapılandırmasını gerçekleştirdi.		
3. GRE IP tüneli yapılandırmasını gerçekleştirdi.		
4. OSPF protokolü yapılandırmasını gerçekleştirdi.		
5. Yönlendiriciler üzerinde gerekli olan statik yönlendirmeleri gerçekleştirdi.		
6. IPsec VPN tünel yapılandırmasını gerçekleştirdi.		
7. GRE trafiğini IPsec VPN tünelinden geçecek şekilde yapılandırdı.		
8. IPsec VPN tünellerinden iletilmesi gereken ağ trafiğini test etti.		

ÖLÇME VE DEĞERLENDİRME

A) Aşağıdaki parantezlerin içine cümlelerde verilen bilgiler doğru ise "D", yanlış ise "Y" yazınız.

1. ( ) VPN, internet üzerinden güvenli bir ağ haberleşmesi sağlamak için kullanılır.

2. ( ) VPN, yüksek maliyetli donanım ve sürekli bakım gerektiren bir teknolojidir.

3. ( ) SSL protokolü, TLS protokolüne göre daha güvenlidir.

4. ( ) AES, simetrik kriptografi algoritmasıdır.

5. ( ) Diffie-Hellman günümüzde kullanılan en güvenilir VPN teknolojisidir.

B) Aşağıdaki cümlelerde boş bırakılan yerlere doğru sözcükleri yazınız.

1. Uzaktan erişim VPN'ler, istemcili ve ..... olmak üzere ikiye ayrılır.

2. Kimlik doğrulama ve şifreleme yapmadan bir IP tüneli oluşturmak için ..... protokolü kullanılır.

3. MPLS sanal özel ağları, OSI referans modeli ikinci ve ..... katmanı arasında etiket anahtarlama yöntemi ile çalışır.

4. TLS protokolünün 1.3. versiyonu ..... yılında yayınlanan son versiyondur.

5. IPsec güvenli anahtar değişim (IKE) süreci ..... ve Faz 2 olmak üzere iki aşamadan oluşur.

C) Aşağıdaki soruları dikkatlice okuyarak doğru cevabı işaretleyiniz.

1. Aşağıdakilerden hangisi uzaktan erişim VPN türüdür?

A) IPsec B) GRE C) IPsec üzerinden GRE D) İstemcili E) MPLS

2. Aşağıdaki paket türlerinden hangisi IPsec tünelinden geçer?

A) Tekil yayın B) Çok noktaya yayın C) Genel yayın

D) Çok noktadan çok noktaya yayın E) Çok noktadan tek noktaya yayın

3. IPsec VPN teknolojisinde kimlik doğrulama için kullanılan asimetrik kriptografi algoritması aşağıdakilerden hangisidir?

A) Diffie-Hellman B) EIGamal C) Eliptic Curve D) SHA-256 E) RSA

4. Aşağıdaki VPN teknolojilerinden hangisi doğrudan şifreleme gerçekleştirmez?

A) IPsec B) MPLS C) İstemcili

D) İstemcisiz E) IPsec üzerinden GRE

5. AH ve ESP protokolleri ile ilgili aşağıdaki ifadelerden hangisi doğrudur?

A) ESP protokolü, AH protokolüne göre daha güvenli değildir.

B) ESP protokolü, kimlik doğrulama ve veri bütünlüğünü kontrol eder ancak şifreleme yapmaz.

C) AH protokolü, kimlik doğrulama ve veri bütünlüğünü kontrol eder ancak şifreleme yapmaz.

D) AH ve ESP protokolleri sadece verilerin bütünlüğünü sağlamak için kullanılır, şifreleme yapmazlar.

E) AH ve ESP protokolleri birlikte kullanılamaz.

5. ÖĞRENME BİRİMİ

YAZILIM TABANLI AĞ (SDN) TEKNOLOJİSİ

KONULAR

5.1. YAZILIM TABANLI AĞLAR
5.2. SPINE-LEAF TEKNOLOJİSİ

NELER ÖĞRENECEKSİNİZ?

- Yazılım tabanlı ağ mimarisini açıklama
- Spine-Leaf Teknolojisini açıklama



TEMEL KAVRAMLAR

Kontrol düzlemi, otomasyon, SDN, Spine-Leaf, veri düzlemi, yönetim düzlemi

HAZIRLIK ÇALIŞMALARI



1. Geleneksel ağ mimarisi ile ilgili neler biliyorsunuz? Bildiklerinizi sınıfta arkadaşlarınızla paylaşınız.
2. Günümüzde kullanılan ağ mimarilerinin avantaj ve dezavantajları neler olabilir? Düşüncelerinizi arkadaşlarınızla paylaşınız.

5.1. YAZILIM TABANLI AĞLAR

Yazılım Tabanlı Ağlar [SDN (Software Defined Networking)]; geleneksel ağ yönetim ve yapılandırma yöntemlerine kıyasla daha esnek, merkezî ve otomatik yaklaşım sunan bir ağ mimarisidir. SDN; ağ donanımı, yönetimi ve yapılandırmasını fiziksel donanım yerine yazılım aracılığıyla gerçekleştirir. Geleneksel ağ mimarisinde performans, güvenlik, yönlendirme gibi işlemler için mevcut altyapılara ara ağ cihazları eklenir. Sisteme sonradan dâhil edilen her bir ağ cihazı, yönetilmesi zor ve karmaşık yapılara sebep olur. SDN ile ağ altyapısı üzerinde oluşturulacak olan yeni teknolojilerin uygulanması daha kolay hâle gelir. SDN; gerçek zamanlı olarak takip edilebilen, kontrol edilebilen ve programlanabilen bir ağ altyapısına sahiptir. Tablo 5.1'de yazılım tabanlı ağ ile geleneksel ağ yaklaşımlarının karşılaştırılması görülür.

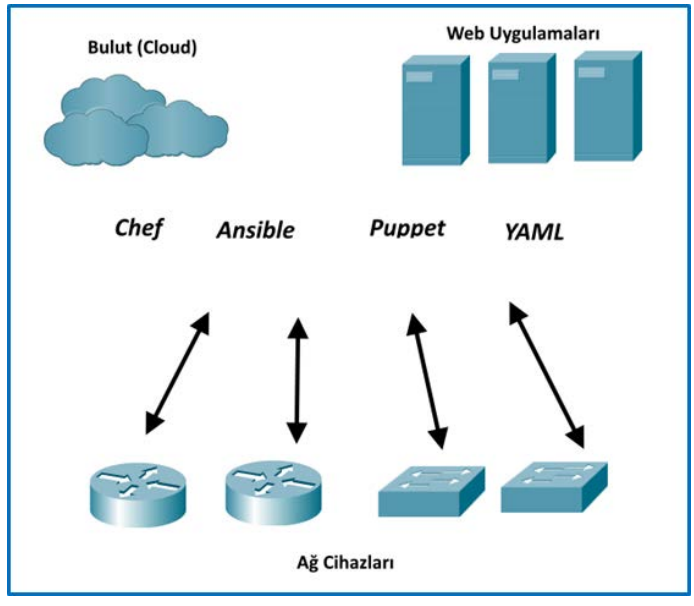
Tablo 5.1: Yazılım Tabanlı Ağlar ile Geleneksel Ağların Karşılaştırılması

Yazılım Tabanlı Ağlar	Geleneksel Ağlar
SDN, yazılım tabanlıdır.	Geleneksel ağ iletişimi donanım tabanlıdır.
Kontrol ve veri düzlemi ayrı varlıklar olup kontrol düzlemi birçok veri düzlemi için merkezî bir denetleyici görevi görür.	Veri ve kontrol düzlemleri tek bir birim olarak birbirine gömülüdür.
SDN mimarisinde ağ cihazları merkezi bir controller üzerinden tek tek veya toplu hâlde yapılandırılır.	Geleneksel ağ mimarisinde ağ cihazlar tek tek yapılandırılır.

5.1.1. Ağ Otomasyonu

Geleneksel ağ yönetimi sürecinde yöneticilerin ağ genelinde bir yapılandırma değişikliği yapması gerektiği zaman her bir cihaz (router, switch vb.) için tekrar eden görevleri yerine getirmesi gerekir. Ağ otomasyonu, bu görevlerin daha otonom bir şekilde çalışmasını sağlayarak ağ yönetimi sürecini basitleştirir. Otomasyon, ağ yöneticilerinin aynı komutları defalarca yazmak ve manuel olarak çalıştırmak zorunda kalmalarını engeller. Bu durum, her bir ağ cihazı ile insan etkileşimini azaltarak ağ cihazlarını daha verimli, hızlı ve daha az hata ile yapılandırmayı sağlar.

Ağ otomasyonu; bir ağdaki fiziksel ve sanal ağ cihazlarının yapılandırılmasının, yönetilmesinin, test edilmesinin, bakımının yapılmasının otomatize hâle getirilmesidir. Ağ yöneticilerinin ağı otomatik olarak yapılandırması, yönetmesi ve izlemesi için Ansible, Puppet, Chef vb. araç ve teknolojiler kullanılır. Bu araç ve teknolojiler ile JSON, XML, YAML veri formatları kullanılarak ağ otomasyonu uygulamaları gerçekleştirilir (Görsel 5.1). Bu araç ve teknolojiler, ağın programlanabilirliğini sağlayarak ağ yönetiminin otomatikleşmesine ve tekrarlayan bakım sürecinin yürütülmesine destek verir. Bu sayede ağ hizmetinin verimliliği ve kullanılabilirliği artar. Ağ otomasyonu ayrıca yazılım tanımlı ağlar (SDN), ağ sanallaştırma ve orkestrasyonunda önemli işlemlerin otomatik çalıştırılmasına izin verir.



Görsel 5.1: Ağ otomasyonunda kullanılan araç ve teknolojiler

Ağ otomasyonu için ağ programcısı, veriyi yapılandırılmış bir biçimde depolamak ve işlemek amacıyla veri formatlarını kullanır. Ağın programlanması için yaygın olarak kullanılan veri formatları şunlardır:



JSON, hafif bir veri değişim formatıdır. İnsanlar tarafından okunabilir ve makineler tarafından kolayca ayrıştırılabilir.



XML, veri depolamak ve taşımak için kullanılan, etiket tabanlı bir işaretleme dilidir.



YAML, veri serileştirme için kullanılan, insan tarafından okunabilir bir format olup kolayca yazılabilir.

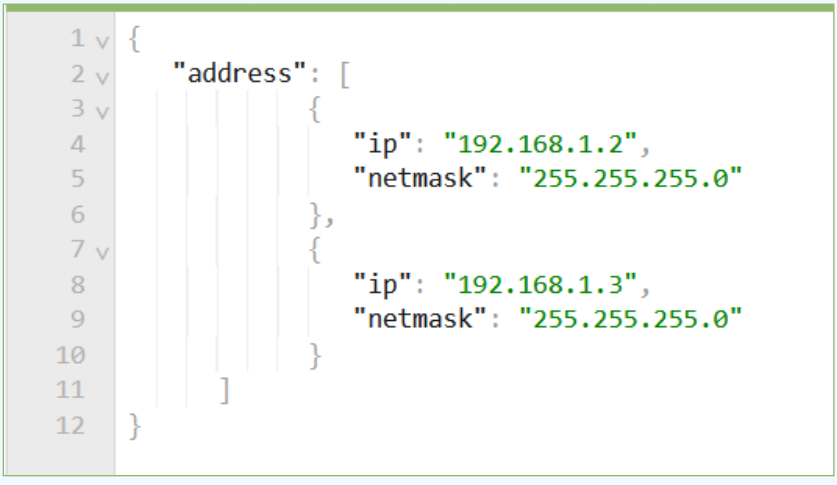
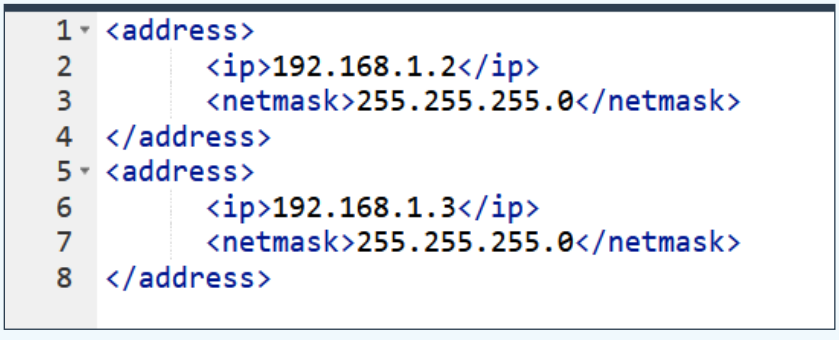
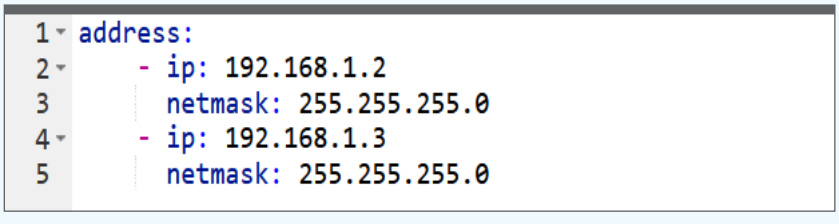
Okunabilirlik: YAML, JSON ve XML'den daha okunaklıdır ancak JSON da oldukça sadedir.

Karmaşıklık: XML, en karmaşık yapıya sahipken JSON ve YAML daha sade ve anlaşılırdır.

Veri Doğrulama: XML, şemalar ile güçlü veri doğrulama seçenekleri sunarken JSON ve YAML bunun için daha sınırlı destek sunar.

Bu formatların her biri, farklı durumlar ve ihtiyaçlar için avantajlar sunar. Hangi formatın kullanılacağı, projenin gereksinimlerine bağlıdır.

Ağ otomasyonunda kullanılan veri formatlarına ilişkin örnekler Görsel 5.2'de verilmiştir.

Veri Formatı	Örnek
JSON	
XML	
YAML	

Görsel 5.2: Ağ otomasyonunda kullanılan veri formatları

Ağ otomasyonunda cihazların programlanması amacıyla gerçekleştirilen veri alışverişi için **Uygulama Programlama Arayüzü [API (Application Programming Interface)]** kullanılır. API'ler; bir uygulamanın diğer uygulamalara, sistemlere veya hizmetlere erişim sağlaması için JSON, XML, YAML gibi formatlarla veri alışverişi gerçekleştirir.

Python: Söz diziminin kolay yapısı, basitliği, netliği ve geniş kütüphane desteği nedeniyle ağ otomasyonunda kullanımı en yaygın programlama dillerinden biridir. Ağ otomasyonunda Python programlama dilinin kullanılması ile ağ yönetimi ve konfigürasyonu hatasız ve hızlı bir şekilde gerçekleştirilir.

Python'ın sağladığı **netmiko**, **paramiko** gibi kütüphaneler; ağ cihazlarını otomatik olarak yapılandırmak, izlemek ve yönetmek için sıklıkla kullanılır. Görsel 5.3'te verilen Python kodu, ağ anahtarında VLAN yapılandırmasını içerir.

main.py +

```python
from netmiko import ConnectHandler
# Switch bilgileri
switches = [
    {
        'device_type': 'cisco_ios',
        'host': '192.168.9.1',  # İlk switch IP adresi
        'username': 'admin',    # Cihaz kullanıcı adı
        'password': 'password', # Cihaz parolası
    },
    {
        'device_type': 'cisco_ios',
        'host': '192.168.9.2',  # İkinci switch IP adresi
        'username': 'admin',    # Cihaz kullanıcı adı
        'password': 'password', # Cihaz parolası
    }
]

# VLAN yapılandırma komutları
vlan_commands = [
    'vlan 10',
    'name Lab1',
    'vlan 20',
    'name Lab2',
    'vlan 30',
    'name Lab3',
    'vlan 40',
    'name Lab4',
    'vlan 50',
    'name Lab5',
]

# Her iki switch için yapılandırma uygulama
for switch in switches:
    with ConnectHandler(**switch) as net_connect:
        output = net_connect.send_config_set(vlan_commands)
 print(f"Switch {switch['host']} VLAN Yapılandırması:")
 print(output)
```

Görsel 5.3: Ağ anahtarında VLAN yapılandırmasını içeren Python kodu örneği

Ansible: Ağı yönetmek, ağ cihazlarını yapılandırmak ve iş akışlarını otomatikleştirmek için kullanılır. Ansible, yapılandırma yönetimi ve otomasyonunu merkezî, basit ve anlaşılır bir biçimde sağlar. Konfigürasyonlar, **playbook** adı verilen YAML dosyalarında tanımlanır (Görsel 5.4).

Input/Edit YAML

```yaml
- name: VLAN Yapılandırması
  hosts: cisco_routers
  connection: network_cli
  gather_facts: no
  tasks:
    - name: VLAN 10 Konfigurasyonu
      cisco.ios.ios_vlan:
        vlan_id: 10
        name: "Personel"
        state: present

    - name: GigabitEthernet0/1 Arayüzü IP Yapılandırması
      cisco.ios.ios_interface:
        name: GigabitEthernet0/1
        ipv4:
          address:
            ip: 192.168.1.3
            mask: 255.255.255.0
        state: present

    - name: GigabitEthernet0/1 Arayüzünün VLAN 10 Ataması
      cisco.ios.ios_interface:
        name: GigabitEthernet0/1
        mode: access
        access_vlan: 10
        state: present
```

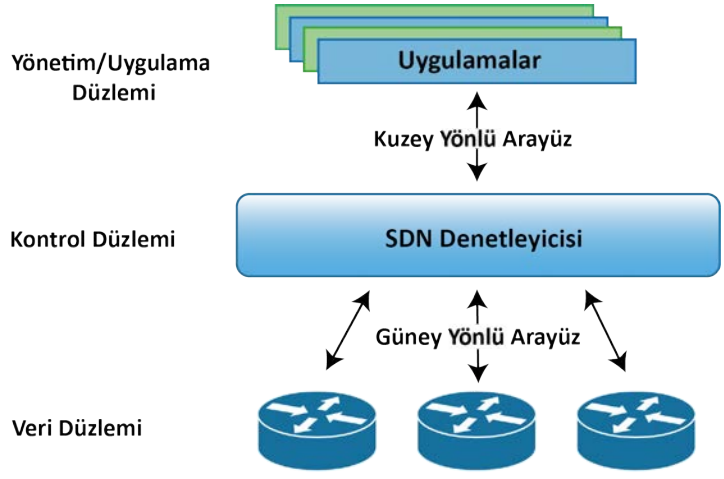
Görsel 5.4: YAML dosyalarında tanımlanan bir konfigürasyon örneği

ARAŞTIRMA Ağ Otomasyonu

Ağ otomasyonunda kullanılan araçlar hakkında araştırma yaparak bu araçlar ve kullanımları ile ilgili rapor hazırlayınız.

5.1.2. Yazılım Tabanlı Ağ Mimarisi Bileşenleri

SDN mimarisi üç katmandan oluşan üç temel bileşene sahiptir. Bunlar; yönetim düzlemi, kontrol düzlemi ve veri düzlemidir (Görsel 5.5).



Görsel 5.5: SDN mimarisindeki üç düzlem

1. **Yönetim/Uygulama Düzlemi (Management/Application Plane):** Ağ yönetim ve kontrol işlevlerini gerçekleştiren yazılım uygulamalarının çalıştığı düzlemdir. Burada yer alan uygulamalar, denetleyici aracılığıyla ağa yönelik politikaları ve ayarları belirler.

2. **Kontrol Düzlemi (Control Plane):** Ağ cihazlarının yönlendirme şekline, uyması gereken politikalara ve ağın yönetim planına dair kararların alındığı düzlemdir. Bu düzlem, SDN'de merkezî bir denetleyici (controller) tarafından yönetilir. Controller, ağın beyni olarak çalışır. Kontrol düzlemindeki kararları alır ve bu kararları veri düzlemine ileterek ağ cihazlarının nasıl davranacağını belirler. Ağın merkezî yönetimini ve programlanabilirliğini sağlar.

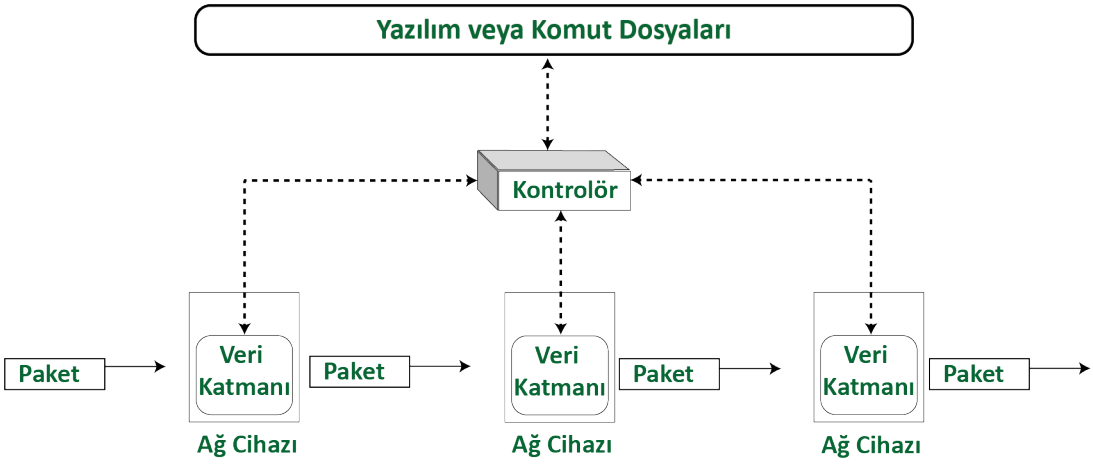
3. **Veri Düzlemi (Data Plane):** Ağ trafiğinin gerçek zamanlı olarak iletildiği düzlemdir. Veri paketlerinin fiziksel olarak iletilip yönlendirilmesini sağlar. Bu düzlemdeki cihazlar (switch, router vb.), merkezî denetleyiciden gelen talimatlara göre hareket eder.

SDN mimarisi, ağ cihazlarının (yönlendiriciler, anahtarlar vb.) veri iletim işlevlerini (veri düzlemi) ve ağın nasıl yönetileceğine dair karar alma süreçlerini (kontrol düzlemi) ayırır.

5.1.3. Yazılım Tabanlı Ağlarda Denetleyiciler

Kontrol düzleminde yer alan ve ağın beyni olarak adlandırılan denetleyiciler, SDN mimarisinde önemli bir yere sahiptir. SDN denetleyicisi, tüm ağın merkezî görünümünü sağlayan sunucu tabanlı bir yazılımdır. SDN denetleyicisi, ağdaki birden fazla düğüme politikaları eşit şekilde uygulamak için kullanılır. **Ağ politikaları;** sahip olunan erişimin düzeyini, izin verilen kaynağın miktarını veya ağa atanan önceliği belirleyen trafik için uygulanan kurallardır. Ağın ve politikaların merkezî bir görünüme sahip olması; daha tekdüze, tutarlı ve basit bir şekilde yönetilmesini sağlar.

Yönlendirici ve anahtarlar gibi tüm geleneksel ağ aygıtları, dağıtılmış kontrol düzlemini kullanırken daha yeni ağ modeli olan yazılım tanımlı ağ, merkezî kontrol düzlemini kullanır. Dağıtılmış kontrol düzlemi, tüm ağ aygıtlarının kontrol düzleminin aygıtın kendisinde bulunduğu anlamına gelir. Merkezî kontrol düzlemi sisteminde tüm cihazların kontrol düzlemini içeren bir cihaz vardır. Bu cihaz, tüm ağ cihazlarının veri düzlemine ait aktivitelerini aynı anda kontrol eder. Bu cihaza, **denetleyici** veya **SDN denetleyici** denir. Şema 5.1'de denetleyici tabanlı ağ oluşturma modeli görülür.



Şema 5.1: Denetleyici tabanlı ağ modeli

Denetleyiciler, ağ cihazlarıyla (örneğin anahtarlar ve yönlendiriciler) iletişim kurarken genellikle OpenFlow gibi protokoller kullanır ve ağdaki trafik akışını yönetir. Bu yazılımların en kritik işlevi, ağ üzerindeki veri iletimini denetleyerek ağın verimli çalışmasını sağlamaktır. Denetleyiciler; ağ trafiğini sürekli izler, trafiği analiz eder ve bu analizlere dayalı olarak **akış kuralları** oluşturur. Bu kurallar, ağ cihazlarına iletilerek trafiğin doğru bir şekilde yönlendirilmesi ve ağın genel performansının iyileştirilmesi sağlanır. SDN denetleyicisi, ağın verimli bir şekilde yönetilmesini sağlamak için bir dizi temel işlevi yerine getirir.

Ağ Yapısının Keşfi ve Haritalandırma: Denetleyici, ağdaki tüm cihazları ve bunlar arasındaki bağlantıları tespit eder. Bu, denetleyicinin ağ topolojisinin ayrıntılı bir haritasını oluşturmasını ve ağın dinamik durumunu gerçek zamanlı olarak izlemesini mümkün kılar.

Akış Kuralları Tablosu Yönetimi: Denetleyici, ağ cihazlarının akış tablolarını yönetir ve hangi verinin hangi yollarla iletileceğini belirler. Bu tablolar, her akış için belirli eşleşme ölçütleri ve yapılacak işlemlerle tanımlanır. Örneğin belirli bir IP adresine gelen verinin nasıl yönlendirilmesi gerektiği gibi kurallar bu tablolarda tanımlanır.

Protokollerle İletişim: SDN denetleyicisi, ağ cihazlarıyla genellikle OpenFlow, NETCONF, RESTful API gibi standart protokoller aracılığıyla veri alışverişi yapar. Bu protokoller, denetleyicinin cihazlara akış kuralları ve yapılandırma talimatları göndermesini sağlar.

Trafik Akışının Dinamik Yönetimi: Ağdaki trafik yoğunluğu veya tıkanıklık gibi durumları izleyen denetleyici, bu verilere dayanarak akış kurallarını anında güncelleyebilir. Trafik türüne ve ağın anlık durumuna göre yapılan bu dinamik değişiklikler, ağın verimli çalışmaya devam etmesini sağlar, yük dengelemesi gibi işlemleri otomatik hâle getirir.

SDN mimarisinde birçok denetleyici kullanılır. Ryu, OpenDaylight, ONOS, POX, NOX, Open vSwitch (OVS) vb. SDN mimarisinde kullanılan açık kaynak denetleyicilerden bazılarıdır.

Ryu: Python tabanlı bir SDN denetleyicisidir. Genellikle küçük ve orta ölçekli ağlar için tercih edilir. Ryu, OpenFlow protokolüyle uyumlu çalışarak ağın trafiğini yönetir. Geliştiriciler, Ryu'yu kullanarak ağ akışını kolayca yazabilir ve uygulama seviyesinde ağ yönetimi yapabilir.

OpenDaylight: Java tabanlı bir SDN denetleyicisidir. Yapısı gereği birçok protokolle uyumlu bir şekilde çalışabilir.

ONOS (Open Network Operating System): Büyük veri merkezleri ve servis sağlayıcı ağları için Java kullanılarak tasarlanmıştır. ONOS, dağıtık bir mimariye sahip olup büyük ölçekli ağ yapılarıyla uyumlu çalışacak şekilde hazırlanmıştır. Yüksek performans ve ölçeklenebilirlik sunarak yük dengeleme, hizmet kesintisi, failover gibi özelliklerle ağ yönetimini sağlar.

POX: Python tabanlı bir SDN denetleyicisidir. Küçük ve orta ölçekli ağlar için uygundur.

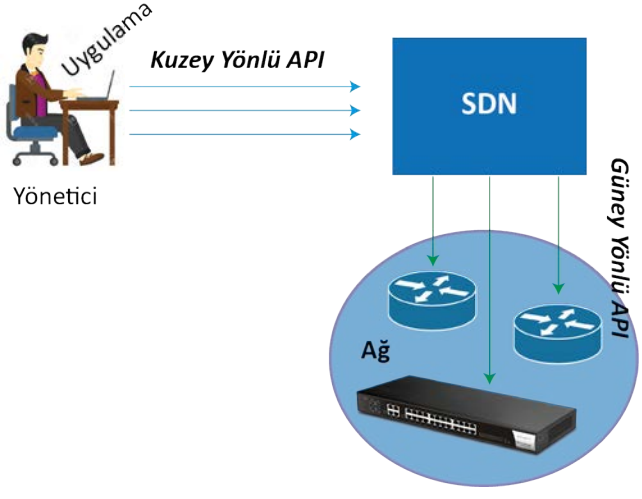
NOX: C++ dilinde yazılmış bir denetleyicidir. Büyük ağlarda kullanılır. NOX, genellikle araştırma ve geliştirme amacıyla tercih edilir.

Open vSwitch (OVS): Sanal ağları yönetmek için tasarlanmış açık kaynaklı bir yazılımdır. SDN mimarisiyle uyumlu çalışarak sanal makineler arasında ağ trafiğinin verimli bir şekilde çalışmasını sağlar. OpenFlow protokolünü destekler ve ağ yönlendirmesi, güvenlik politikaları, trafik yönetimi gibi işlevleri yerine getirir.

5.1.4. Kuzey ve Güney Yönlü Arayüzler

SDN denetleyicisinin **kuzey yönlü arayüz [northbound interface (NBI)]** ve **güney yönlü arayüz [southbound interface (SBI)]** biçiminde adlandırılan iki önemli bileşeni vardır. Denetleyiciyi yapılandırmak ve kullanılan uygulamaya bağlanmak için kuzey yönlü arayüzü kullanır. Denetleyici aracılığıyla yapılan yapılandırmayı uygulamak ve ağ aygıtlarına bağlanmak için güney yönlü arayüzü kullanır.

NBI ve SBI'nın nerede bulunduğunu bilmek için öncelikle SDN denetleyicisinin kendisi düşünülmelidir. SDN denetleyicisi, aynı ağdaki bir sunucuda çalışan bir cihaz veya yazılımdır. Yöneticiler ve ağ cihazları arasında köprü görevi görür. Yöneticilerden talimatlar alır ve bunları ağ cihazlarında uygular. Yöneticiler ve ağ aygıtlarıyla iletişim kurmak için API'leri kullanır. API, farklı eylemler gerçekleştiren ve çeşitli işlevler içeren bir uygulama mantığıdır. SDN ağlarında API'ler, değişiklikleri yönetmek için yöneticilerin kullandığı uygulamadan denetleyiciye bilgi taşır. Ardından denetleyiciden ağ aygıtlarına veri taşır. Görsel 5.6'te kuzey ve güney yönlü API'lerin çalışma şekli görülür.



Görsel 5.6: Kuzey ve güney yönlü API

SDN'de tüm ağ cihazları denetleyiciye bağlanmalıdır. Böylece denetleyici, tüm cihazların veri düzlemlerini düzenleyebilir. Ağ mimarı, ağ mimarisini çizerken genellikle ağ cihazlarını denetleyicinin altına yerleştirir. Denetleyici ile ağ cihazları arasındaki arayüz, denetleyicinin güneyinde yer alır.

Denetleyicinin, ağ cihazlarının veri düzlemini kontrol edebilmesi için ağ hakkında birçok bilgiye ihtiyacı vardır. Tüm bu bilgiler, ağ programcısı tarafından sağlanır. Ağ programcısı, yapması gereken işlevler hakkında çeşitli yazılımlar veya Python, Ruby, Java gibi programlama dilleri ile oluşturulmuş komut dosyaları aracılığıyla denetleyiciye temel bilgileri sağlar. Yine bu yazılımlar veya komut dosyaları, ağ mimarisinde denetleyicinin üstüne yerleştirilir. Yazılım veya komut dosyasının bu yerleşimi, harita kurallarına göre denetleyici ve yazılım arasında kuzey yönünde arayüzler oluşturur. Denetleyici ve yazılımlar arasındaki arayüzler kuzey yönlü arayüzlerdir. Bu arayüzler, ağın programlanabilirliğini sağlar.

5.1.5. OpenFlow Protokolü

Yazılım tabanlı ağlarda çeşitli hizmetler için birçok protokol kullanılır. Güvenlik, sanal ağlar, trafik yönlendirme, ağı yönetme gibi işlemler için tasarlanmış birbirinden farklı protokoller bulunur. OpenFlow, Açık Ağ Vakfı (ONF) tarafından yönetilir. Yazılım tabanlı ağlarda kullanılan ilk açık standart tabanlı protokoldür. OpenFlow, ağ cihazlarının bir yazılım tarafından merkezî olarak yapılandırılması için kullanılır. OpenFlow protokolü sayesinde ağ trafiği, daha verimli ve etkili bir şekilde kontrol edilerek yönetilir.

OpenFlow, güney arayüzü için yaygın olarak kabul edilen protokoldür. Openflow protokolü, geleneksel ağ altyapısında SDN'yi uygulamak için kullanılır. Denetleyici ile ağ altyapısı arasındaki arayüzü tanımlar. Openflow protokolü, yönlendiriciyi veya anahtarı hangi firmanın ürettiğine bakmadan gelen veri paketlerinin nasıl işleneceğini anahtara bildirir. OpenFlow iletişim protokolü, ağ kontrol ve yönlendirme işlevlerini ayıran yazılım tanımlı ağ mimarisinin temel öğesidir. SDN, ağın küresel görünümünü koruyan yazılım tabanlı denetleyicilerde ağ zekâsını ve kontrolünü merkezîleştirir. OpenFlow, SDN denetleyicisi ve ağ donanımı arasında iletişim kurar. Ağları daha dinamik, yönetilebilir, düşük maliyetli ve uyarlanabilir hâle getirerek ağ donanımlarının (sanal anahtarlar, yönlendiriciler vb.) doğrudan programlanmasını sağlar.

OpenFlow protokolünde ağ trafiğini yönlendirmek için akış tabloları kullanılır. Akış tabloları içinde bir takım kurallar bulunur. OpenFlow, ağ cihazlarının akış tablosunda bulunan bu kuralları kullanarak trafiği yönlendirir. SDN kontrol yazılımları bu akış kurallarını statik ya da dinamik olarak kodlar.

OpenFlow'un Temel Özellikleri

Akışlar (Flows): OpenFlow protokolünde kaynak IP adresi, hedef IP adresi, port numarası gibi çeşitli ölçütlere göre belirlenmiş kurallar bulunur. Bu kurallara akış ismi verilir. Ağ trafiği, önceden tanımlanan bu kurallara göre işlenir. Oluşturulan akış bir veya birden fazla ağ cihazı için kullanılabilir.

Akış Tablosu (Flow Table): OpenFlow anahtarları (switchler), ağ trafiğini yönetmek için akış tablosu ismi verilen ve içinde birçok akış barındıran veritabanı benzeri bir yapıyı kullanır. Bu tablo, gelen paketleri belirli eşleşme ölçütlerine göre değerlendirir ve her bir kural, bu paketlere uygulanacak işlemleri tanımlar. SDN kontrol yazılımı, bu eşleşme kurallarını belirleyerek ağdaki trafiğin nasıl yönlendirileceğini ve işleneceğini kontrol eder. Örneğin belirli bir IP adresine sahip paketler için özel bir işlem uygulanabilir.

Eşeleşme Kuralları (Match Rules): Eşleşme kuralları, ağ cihazlarının hangi trafiği hangi şekilde işleyerek yönlendireceğini belirler. Bu kurallar, statik ya da dinamik olabilir ve genellikle paketlerin başlık bilgileri (örneğin IP adresleri, port numaraları vb.) temel alınarak oluşturulur.

Eylemler (Actions): Eşleşen trafiğe uygulanan akış kuralları belirli eylemleri içerir. Bu eylemler, paketlerin yönlendirilmesi, engellenmesi, yönlendirme tablosunun güncellenmesi, diğer ağ cihazlarına iletilmesi gibi işlemleri kapsar. Örneğin bir paket, belirli bir eşleşme kuralıyla uyumlu olduğunda hedef IP adresine göre bir sonraki ağ cihazına yönlendirilir.

Python, SDN denetleyicileriyle (örneğin Ryu veya OpenFlow Python API'leri ile) iletişim kurmak için yaygın olarak kullanılır. RYU, SDN mimarisini destekleyen bir ağ denetleyicisi olup Python programlama dili ile yazılmıştır. Verilen örnekler, Python programlama dili kullanılarak OpenFlow akış kurallarının nasıl hazırlanacağına dairdir.



IP Adresi Temelli Akış Kuralı

Belirli bir kaynak IP adresine sahip paketlerin belirli bir port üzerinden geçmesinin istenmesi durumunda Python'da Ryu Controller kullanarak hazırlanan bir OpenFlow akış kuralı şöyledir:

Kaynak IP adresi 192.168.100.1.

Hedef IP adresi 192.168.100.2.

Protokol TCP (6).

Hedef TCP portu 443 olan paketler, SDN anahtarının port 1 çıkışına yönlendirilecektir.

RYU CONTROLLER KULLANILARAK HAZIRLANAN AKIŞ KURALI

```
from ryu.base import app_manager
from ryu.controller import ofp_event
from ryu.lib.packet import packet, ethernet
from ryu.ofproto import ofproto_v1_3
from ryu.ofproto.ofproto_v1_3 import OFPActionOutput, OFPMatch
class SimpleSwitch(app_manager.RyuApp):
  OFP_VERSIONS = [ofproto_v1_3.OFP_VERSION]
  def __init__(self, *args, **kwargs):
    super(SimpleSwitch, self).__init__(*args, **kwargs)
  @staticmethod
  def add_flow(datapath, priority, match, actions):
    ofproto = datapath.ofproto
    parser = datapath.ofproto_parser
    # Flow entry oluşturuluyor
    inst = [parser.OFPInstructionActions(ofproto.OFPIT_APPLY_ACTIONS, actions)]
    mod = parser.OFPFlowMod(datapath=datapath, priority=priority, match=match, instructions=inst)
    datapath.send_msg(mod)
  @ofp_event.EventOFPStateChange
  def on_state_change(self, ev):
```

```
        datapath = ev.datapath
        ofproto = datapath.ofproto
        parser = datapath.ofproto_parser
        # IP adresine dayalı eşleşme kuralı oluşturma
        match = parser.OFPMatch(eth_type=0x0800, ipv4_src='192.168.100.1', ipv4_dst='192.168.100.2',
ip_proto=6, tcp_dst=443)
         # EYLEM: Çıkış portu 1'e yönlendir.
        actions = [OFPActionOutput(port=1)]
        # AKIŞ KURALI
        self.add_flow(datapath, priority=100, match=match, actions=actions)
```

match: Bu bölümde, gelen paketlerin kaynak IP adresi 192.168.100.1, hedef IP adresi 192.168.100.2, TCP protokolü ve hedef portu 443 olan paketlere eşleşen bir kural tanımlanmaktadır.

actions: Bu eşleşmeye uyan paketler, çıkış portu olarak port 1'e yönlendirilecektir.

ÖRNEK

MAC Adresi Temelli Akış Kuralı

MAC adreslerine dayalı bir akış kuralı şöyle olabilir:

Flow Entry = {

Match Fields: {src_mac = 00:1A:2B:3C:4D:5E, dst_mac = 00:1A:2B:3C:4D:6F}

Actions: {output_port = 2}

}

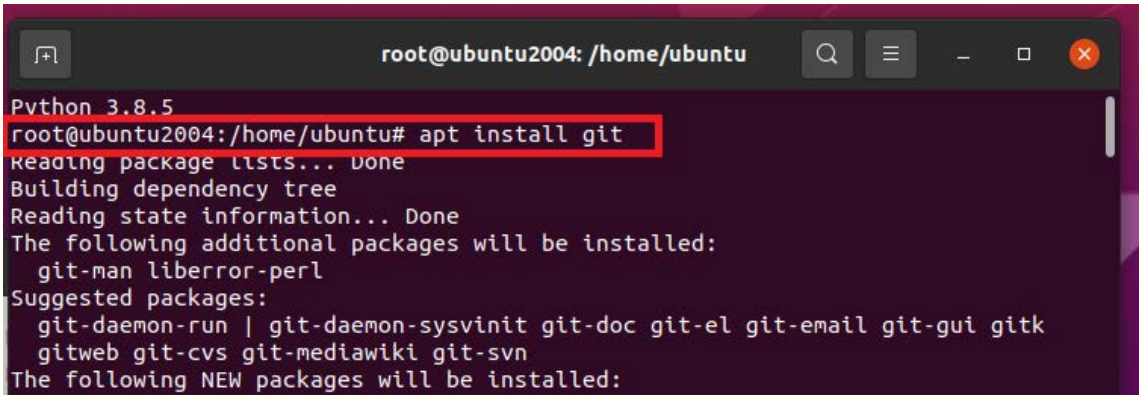
Bu kural, belirli bir kaynağa (src_mac) ve hedefe (dst_mac) sahip Ethernet çerçevelerinin çıkış portu 2'ye yönlendirilmesini sağlar.

1. UYGULAMA

Yazılım tabanlı ağ simülasyon programı ile SDN denetleyicisi olarak Ryu Controller'ın kurulumunu gerçekleştiriniz. Ardından örnek bir ağ topolojisi oluşturarak Ryu Controller üzerinden kontrolünü sağlayınız.

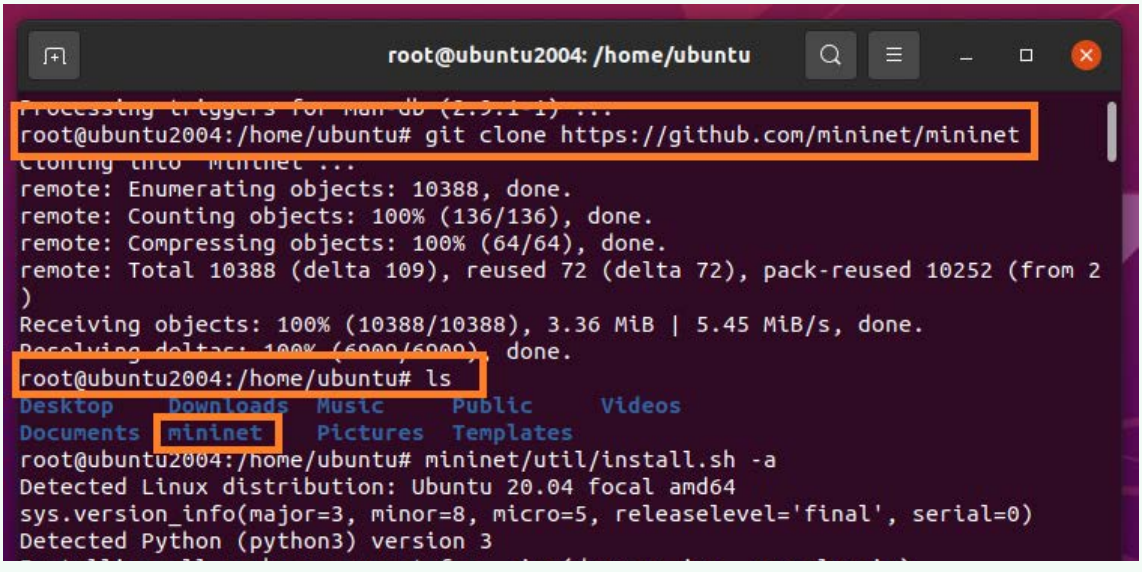
Not: Bu uygulama için işletim sistemi olarak Ubuntu 20.04 kullanılmıştır. Python 3.8.10 versiyonunu kullanarak kurulumlar gerçekleştirilmiştir. Kullandığınız işletim sistemi ve Python versiyonlarına göre ek işlemler ve yüklemeler yapmanız gerekebilir. Ubuntu işletim sisteminde yapılacak olan tüm işlemler root yetkisiyle yapılmalıdır.

1. Adım: Yazılım tabanlı ağ simülasyon programını işletim sistemine indirmeniz için gerekli olan dağıtık sürüm kontrol sistemini yükleyiniz (Görsel 5.7).



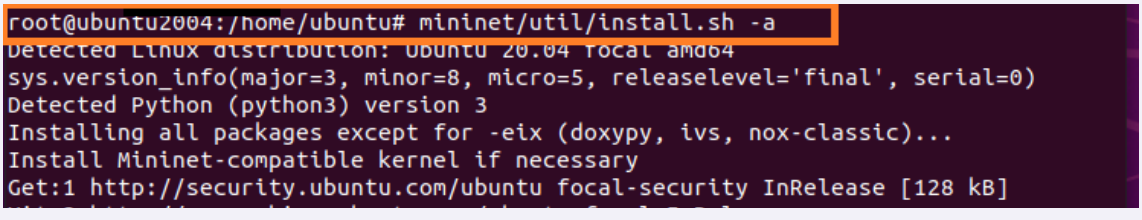
Görsel 5.7: Dağıtık sürüm kontrol sisteminin kurulumu

2. Adım: Yazılım tabanlı ağ simülasyon programının kaynak kodlarını dağıtık sürüm kontrol sistemini kullanarak belirtilen depodan işletim sistemi yerel dizine indiriniz (Görsel 5.8).



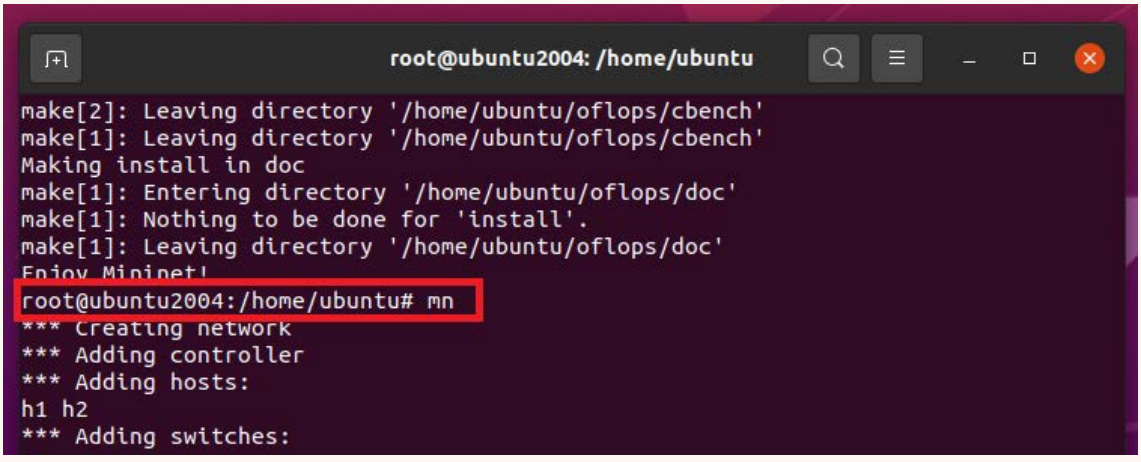
Görsel 5.8: Yazılım tabanlı ağ simülasyon programının kaynak kodlarının indirilmesi

3. Adım: Yazılım tabanlı ağ simülasyon programının tüm ek bileşenleri ile birlikte kurulumunu yapınız (Görsel 5.9).



Görsel 5.9: Yazılım tabanlı ağ simülasyon programının ek bileşenlerinin yüklenmesi

4. Adım: Yazılım tabanlı ağ simülasyon programına giriş yapınız (Görsel 5.10).



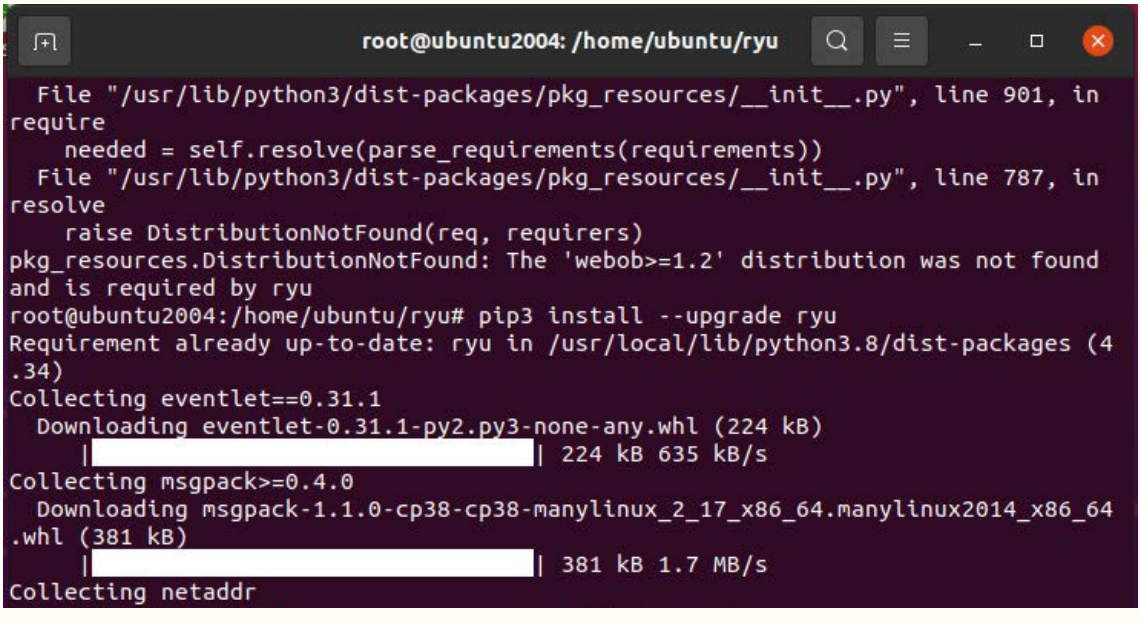
Görsel 5.10: Ağ simülasyon programının giriş ekranı

5. Adım: Aşağıdaki komutu kullanarak SDN denetleyicisi Ryu'nun kaynak kodlarını dağıtık sürüm kontrol sistemi deposundan yerel bir dizine kopyalayıp, kurulumun ardından Ryu dizinine girerek son sürüme güncelleştirme işlemini gerçekleştiriniz (Görsel 5.11).

root@ubuntu2004:/home/ubuntu# git clone https://github.com/faucetsdn/ryu.git

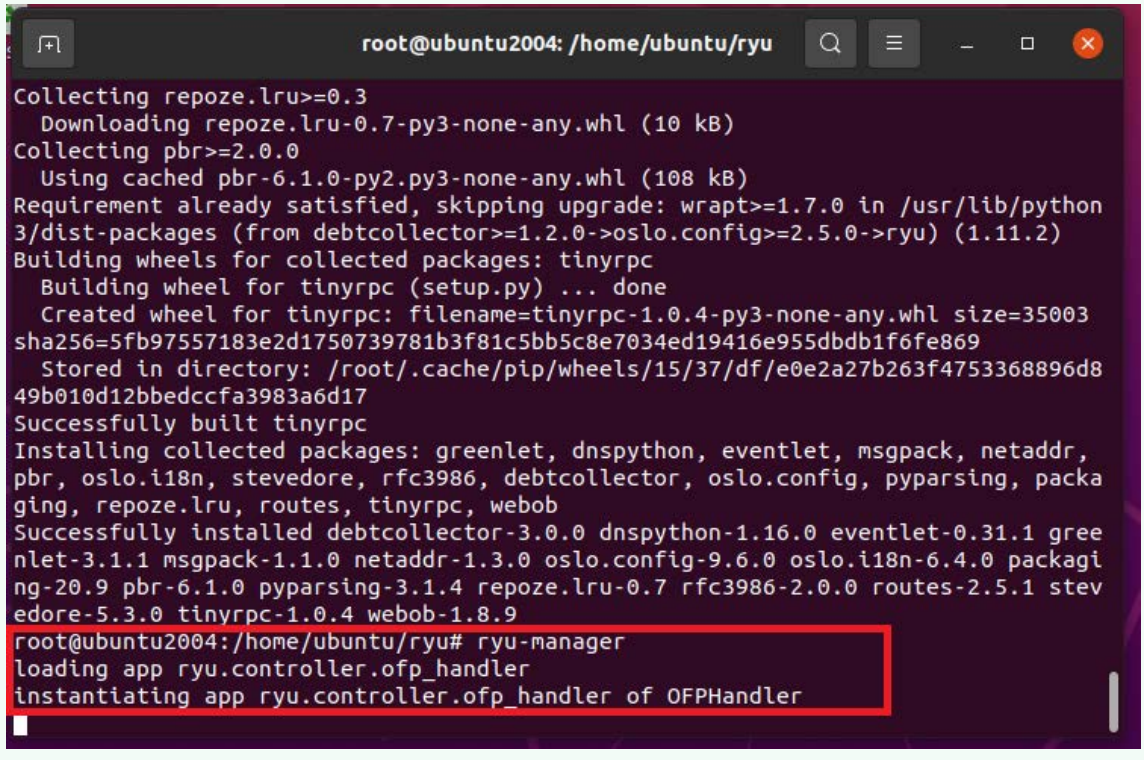
root@ubuntu2004:/home/ubuntu#cd ryu

root@ubuntu2004:/home/ubuntu/ryu# pip3 install --upgrade ryu



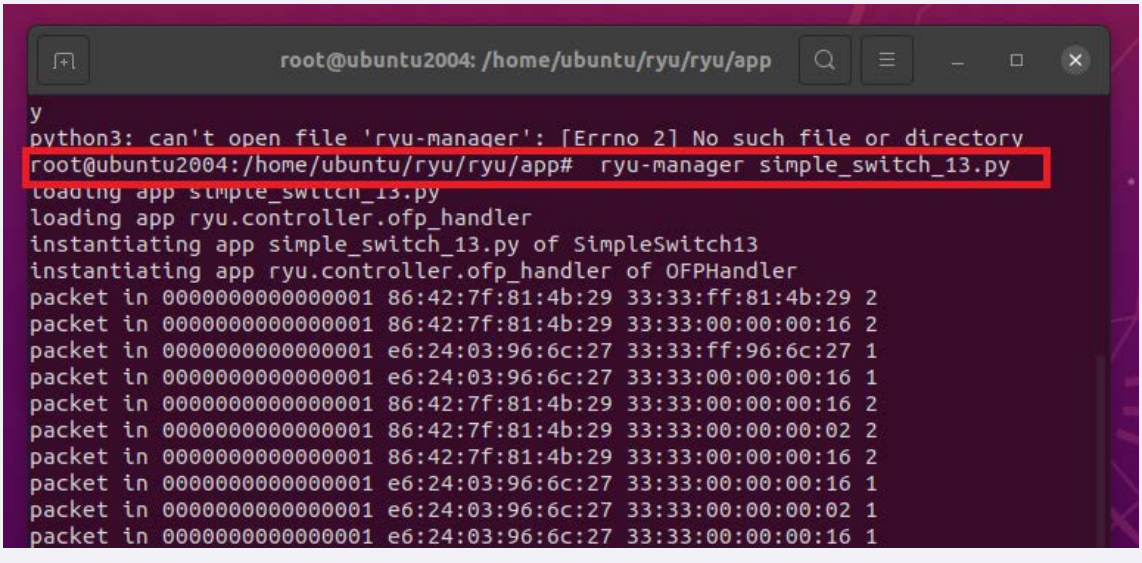
Görsel 5.11: Güncelleştirmelerin yüklenmesi

6. Adım: Ryu SDN Controller'ı başlatmak için gerekli komutu yazınız (Görsel 5.12).



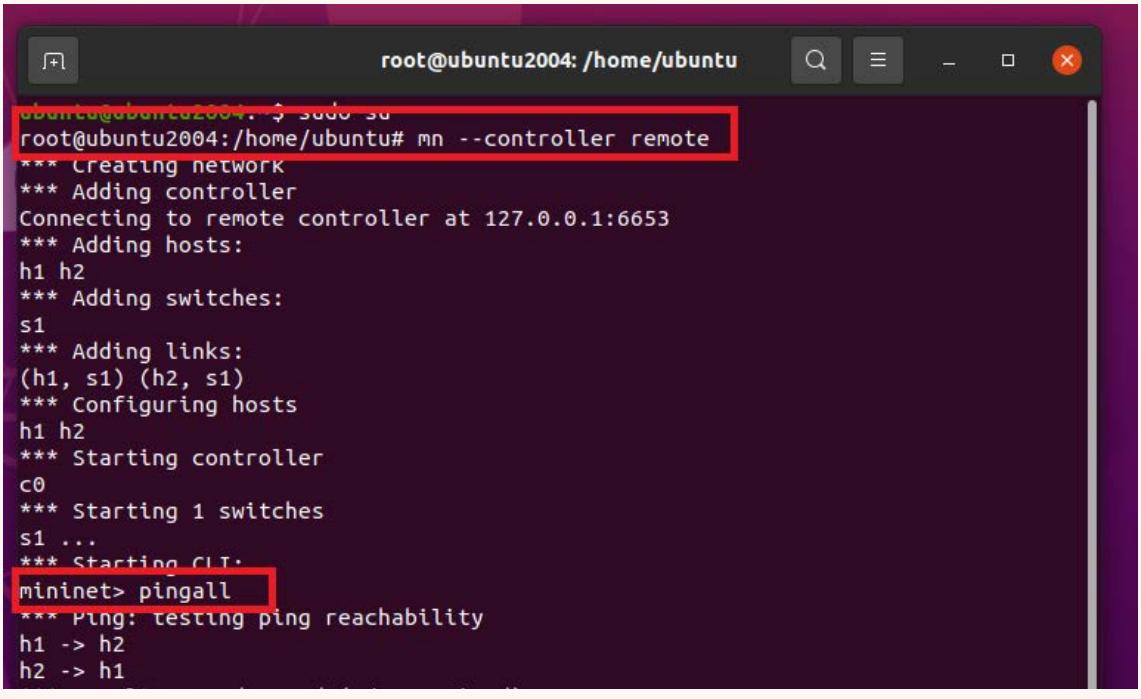
Görsel 5.12: Ryu SDN Controller'ı başlatma

7. Adım: Ryu SDN Controller'ın kendi içindeki /ryu/ryu/app dizininden simple_switch_13 isimli örnek projeyi ryu-manager komutu ile çalıştırınız (Görsel 5.13).



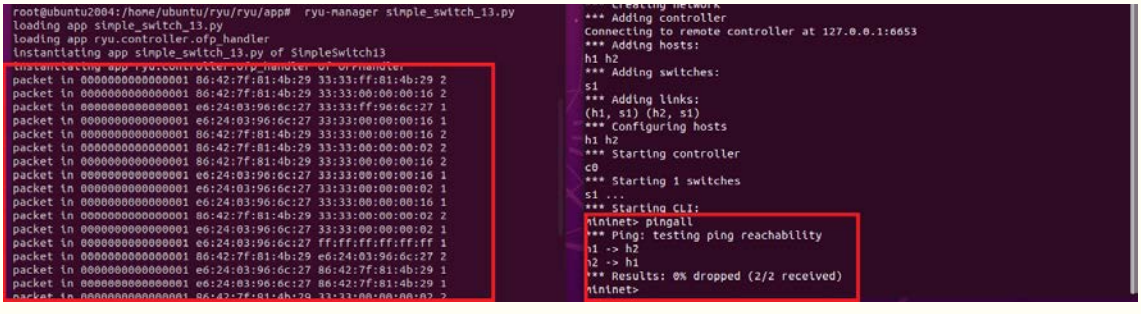
Görsel 5.13: Örnek projenin çalıştırılması

8. Adım: Yazılım tabanlı ağ programını çalıştırarak kontrol düzlemini yerel bir denetleyici (controller) yerine RYU denetleyiciye (remote controller) bağlayınız ve bütün topolojiye ping işlemini gerçekleştiriniz (Görsel 5.14).



Görsel 5.14: Toplojojiye ping işlemi

9. Adım: Sonuc kısmında 0% dropped olduğunu ve Ryu denetleyicisinde paketlerin iletildiğini görüntüleyerek sistemin çalışmasını test ediniz (Görsel 5.15).



Görsel 5.15: Sistemin çalışmasının test edilmesi

5.2. SPINE-LEAF TEKNOLOJİSİ

Spine-Leaf (Omurga-Yaprak) mimarisi, omurga ve yaprak olmak üzere iki anahtarlama katmanından oluşan veri merkezli bir ağ mimarisidir. Yaprak katmanı, sunuculardan gelen trafiği toplayan ve doğrudan omurgaya veya ağ çekirdeğine bağlanan erişim anahtarlarından oluşur. Omurga katmanı ise tüm yaprak anahtarlarını ağ topolojisinde birbirine bağlar. Omurga-Yaprak teknolojisi, üç katmanlı mimarideki sınırlamalardan dolayı geliştirilmiş bir topolojidir.

5.2.1. Üç Katmanlı Ağ Mimarisi

Üç katmanlı mimari, uygulamaları üç mantıksal ve fiziksel bilgi işlem katmanına düzenleyen köklü bir yazılım uygulama mimarisidir. **Sunum katmanı** veya **kullanıcı arayüzü**, verilerin işlendiği **uygulama katmanı** ile uygulama verilerinin depolandığı ve yönetildiği **veri katmanından** oluşur.

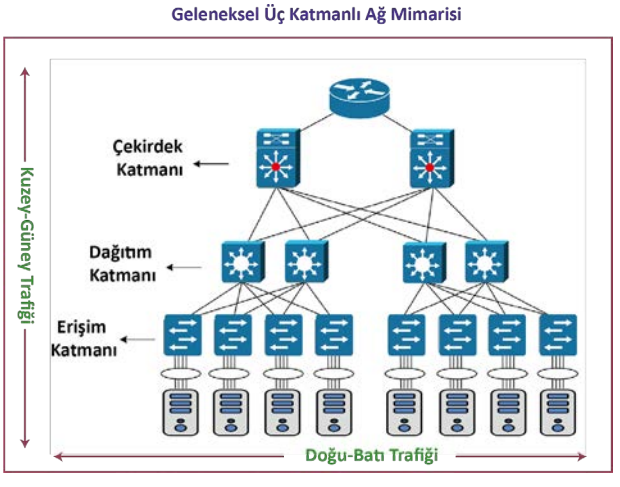
Üç katmanlı ağ mimarisi; **çekirdek katmanı (core layer)**, **dağıtım katmanı (distrubution layer)** ve **erişim katmanı (access layer)** olarak adlandırılan üç önemli katmandan oluşur. Bu katmanlar; ağ mimarisinin performansını, güvenilirliğini ve esnekliğini artırmayı amaçlayan farklı bağlantılar ve işlevler üstlenir.

1. **Çekirdek Katmanı:** Birden fazla dağıtım katmanı anahtarını bağlamaktan sorumlu olan ağın omurgası olarak hizmet eder. Genellikle büyük miktarda veri iletmek, yüksek hız ve bant genişliğine sahip iletişimi sağlamak ve bol miktarda yedekli bağlantı elde etmek için kullanılır. Çekirdek katman, güvenilirliği sağlarken en hızlı veri iletim hızlarına ulaşır.
2. **Dağıtım Katmanı:** Çekirdek katmanını erişim katmanına bağlayan bir aracı görevi görür, trafiği koordine etme ve yönetmede rol oynar. Sorumlulukları arasında erişim kontrolü, politika formülasyonu ve hata izolasyonu bulunur. Dağıtım katmanında veri, alındığı andan itibaren hızlı işleme ve iletme için entegre edilir ve çekirdek katmanına gönderilir.
3. **Erişim Katmanı:** IP telefonları, yazıcılar, bilgisayarlar vb. kullanıcı cihazlarının ağa bağlanmasını sağlar. Kullanıcı cihazları arasında veri iletimini sağlayarak verileri çerçeveler hâlinde işler ve yönlendirir. Veri iletimi sırasında oluşabilecek hataları tespit eder. Erişim katmanı, ağa yetkisiz erişimi önlemek amacıyla güvenlik önlemleri uygular.

Her katmanın kendi altyapısında çalışması nedeniyle ayrı bir geliştirme ekibi tarafından aynı anda geliştirilebilmesi ve diğer katmanları etkilemeden ihtiyaç duyulduğunda güncellenebilir veya ölçeklenebilir olması, üç katmanlı mimarinin başlıca faydasıdır.

Üç katmanlı mimarinin oluşturulma mantığı, veri merkezinin içinde dönen trafiğin doğudan batıya yüksek olmasıdır. Üç katmanlı mimari, **doğudan batıya** ve **kuzeyden güneye** mantığı ile çalışır. Sunucudan sunucuya veya sunucudan depolama/saklama alanına giden trafik, doğu-batı trafiği biçiminde ifade edilir. Kuzey-güney trafiği ise istemci ile sunucu arasındaki veri akışını ifade eder. Genellikle sunum katmanından veri katmanına veya veri katmanından sunum katmanına olan iletişimi içerir. Görsel 5.16'da üç katmanlı topolojinin işleyişi gösterilmektedir.

Çekirdek tarafına gelen veri, direkt olarak bağlı olan toplayıcı görevini üstlenen **Dağıtım** katmanına yönlendirilir. Distrubution katmanına gelen veri ise **Erişim** katmanına ulaştırılarak verinin sunucu veya ilgili hosta ulaşması sağlanır.

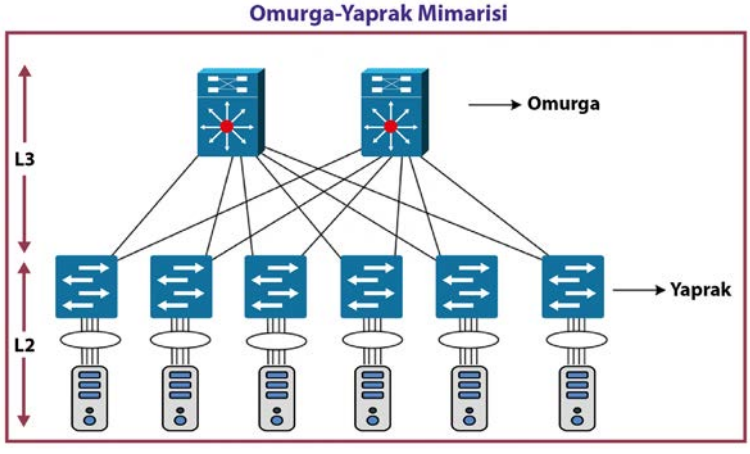


Görsel 5.16: Üç katmanlı ağ mimarisi

Zaman içinde artan trafik ve bant genişliği sebebiyle işleyişle ilgili dezavantajlar oluşmaya başlar. Bu dezavantajlardan en önemlisi zaman aşımı (timeout) süresi ve paket kayıplarıdır. Bir diğeri ise yedeklilik için ihtiyaç duyulan donanım sebebiyle maliyetin artmasıdır. Tüm bu ve buna benzer sebepler Spine-Leaf mimarisinin geliştirilmesinin önünü açar.

5.2.2. Omurga-Yaprak Mimarisi

İki katmanlı topoloji, **omurga** ve **yaprak** olmak üzere iki anahtar katmanından oluşan veri merkezi ağ topolojisidir (Görsel 5.17). Bu topolojinin iki katmanlı oluşu öncelikle paket kaybı ve zaman aşımını ortadan kaldırdığı gibi verinin daha hızlı ve sağlıklı omurga katmanı tarafına iletilebilmesine olanak sağlar. Bir diğer avantajı ise karmaşık bir yapı olmadığından yönetilmesinin kolay olmasıdır. Düzeni karmaşık olmadığından sorun çözümü de işleyişi de kolaydır.



Görsel 5.17: Omurga-Yaprak mimarisi

Omurga katmanı, yönlendirmeyi gerçekleştiren ve ağın çekirdeği olarak çalışan anahtarlardan oluşur. Tüm yaprak anahtarlarını tam örgü (full mesh) bir topolojide birbirine bağlar.

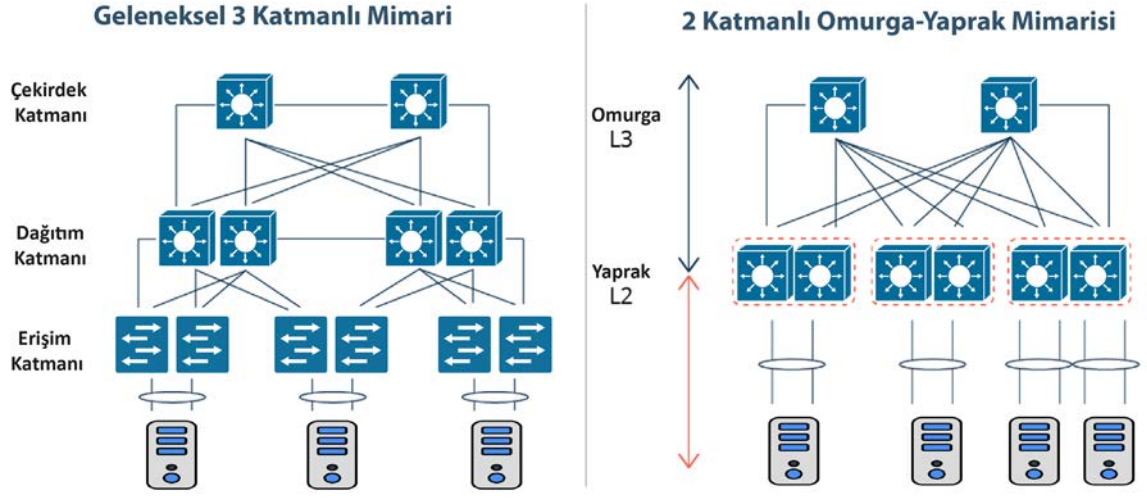
Yaprak katmanı, sunuculardan gelen trafiği toplayan ve doğrudan omurgaya veya ağ çekirdeğine bağlanan erişim anahtarlarını içerir. Bu yapı, veri merkezi ağlarının atlama sayısının düşmesine ve ağ gecikmesinin azaltılmasına yardımcı olur.

Omurga-Yaprak mimarisinde her bir yaprak anahtarı, farklı bir omurga anahtarına bağlanır. Bu tasarımla herhangi bir sunucu diğer bir sunucuyla iletişim kurabilir. Herhangi iki yaprak anahtarı arasında birbirine bağlı birden fazla anahtar yolu yoktur. Omurga-Yaprak mimarisi ile üç katmanlı mimari arasındaki temel fark, ağ katmanlarının sayısı ve dönüştürdükleri trafiğin kuzey-güney veya doğu-batı yönlü olmasıdır.

Üç katmanlı ağ mimarisinde erişim anahtarları, sunuculara ve depolama cihazlarına bağlanır. Dağıtım katmanı, erişim katmanı trafiğini toplar ve erişim katmanında yedekli bağlantılar sağlar. Çekirdek katman, ağ iletimini sağlar ancak bu üç katmanlı topoloji genellikle kuzey-güney ile doğu-batı trafiği için tasarlanır. ve 100'e kadar anahtarı destekleyen STP protokolünü kullanır. Bu durum, ağ verilerinin sürekli genişlemesi hâlinde kaçınılmaz olarak bağlantı noktasının tıkanmasına ve sınırlı ölçeklenebilirliğe yol açar.

Omurga-Yaprak mimarisi, omurganın kuzey-güney ağ mimarisine doğu-batı trafik paralelliğini ekleyerek geleneksel üç katmanlı ağ mimarisinin darboğaz sorununu temelden çözer.

Geleneksel üç katmanlı mimariyle karşılaştırıldığında Omurga-Yaprak mimarisi, yapraklar arasında tek bir atlamayla omurga üzerinden bağlantı sağlayarak gecikmeleri ve dar boğazları en aza indirir (Görsel 5.18). Omurga-Yaprak mimarilerinde anahtar konfigürasyonu, dinamik bir sunucu ortamı için herhangi bir ağ değişikliği gerekmeyecek şekilde sabitlenir. Avantajlarından bir diğeri ise Spine-Leaf topolojisinde, yaprak anahtarları hem sunucu kısmına hem de direkt olarak ağa bağlı olduğundan veri akışının hızlı olmasıdır. Bu sayede veri merkezlerinde yüksek ölçekli trafik ve sunucu barındırabilmesi büyük bir avantaj hâline gelir.



Görsel 5.18: Geleneksel üç katmanlı mimari ve Omurga-Yaprak mimarisi

Avantajları ve yönetim kolaylığı göz önüne alındığında bugün veri merkezlerinde üç katmanlı topolojinin yerini ağırlıklı olarak Spine-Leaf topolojisi almaya başlar.

ÖLÇME VE DEĞERLENDİRME

A) Aşağıdaki parantezlerin içine cümlelerde verilen bilgiler doğru ise "D", yanlış ise "Y" yazınız.

1. ( ) Yazılım tabanlı ağlar, dağıtılmış kontrol düzlemini kullanırlar.

2. ( ) SDN'de güney yönlü arayüzler, denetleyiciler ve anahtarlar ile diğer ağ düğümleri arasında alt düzey bileşenlerle iletişimi sağlayan OpenFlow protokolüdür.

3. ( ) Omurga-Yaprak mimarisi, üç katmanlı mimarideki sınırlamalardan dolayı geliştirilmiş bir mimaridir.

4. ( ) Dağıtım katmanı; çekirdek katmanını erişim katmanına bağlayan bir aracı görevi görür, trafiği koordine etme ve yönetmede rol oynar.

B) Aşağıdaki cümlelerde boş bırakılan yerlere doğru sözcükleri yazınız.

1. Ağı yönetmek, ağ cihazlarını yapılandırmak ve iş akışlarını otomatikleştirmek için ..... kullanılır.

2. SDN mimarisi ....., kontrol düzlemi ve veri düzlemi olmak üzere üç katmandan oluşan üç temel bileşene sahiptir.

3. Java tabanlı bir SDN denetleyicisi olan ....., yapısı gereği birçok protokolle uyumlu bir şekilde çalışır.

C) Aşağıdaki soruları dikkatlice okuyarak doğru cevabı işaretleyiniz.

1. Yazılım tabanlı ağlar ile ilgili aşağıdaki bilgilerden hangisi yanlıştır?

A) Hata eğilimli manuel yapılandırmaya sahiptir.

B) Otomatik yapılandırmaya sahiptir.

C) Yenilikler için kolay yazılım uygulamalarına sahiptir.

D) Geleneksel ağlara göre daha esnek bir yapıya sahiptir.

E) Veri ve kontrol düzlemlerini birbirinden ayırmaya yarar.

2. Aşağıdakilerden hangisi bir ağın programlanması için yaygın olarak kullanılan veri formatlarındandır?

A) Ansible B) Puppet C) Python

D) Rest E) XML

3. Aşağıdakilerden hangisi üç katmanlı ağ mimarisi katmanları arasında yer alır?

A) Sunum katmanı B) Erişim katmanı

C) Veri katmanı D) Fiziksel katmanı

E) Ağ katmanı

CEVAP ANAHTARI

1. ÖĞRENME BİRİMİ

A

1	D	2	Y	3	Y	4	D	5	D

B

1	depola ve ilet	2	tam çift yönlü	3	port kümele-me	4	VLAN	5	fiziksel

C

1	B	2	A	3	D	4	C	5	C

2. ÖĞRENME BİRİMİ

A

1	D	2	D	3	Y	4	D	5	Y

B

1	kayan statik rota	2	uzaklık vektörü ile yönlendirme	3	komşu tablosu	4	show ip ospf neighbor	5	BGP

C

1	E	2	D	3	A	4	B	5	B
6	E	7	B	8	A	9	B	10	C

3. ÖĞRENME BİRİMİ

A

1	D	2	Y	3	D	4	D	5	Y

B

1	WMAN	2	çok yönlü	3	Tethering	4	Beacon	5	EAPOL

C

1	C	2	E	3	B	4	C	5	E
6	B	7	D	8	D				

4. ÖĞRENME BİRİMİ

A

1	D	2	Y	3	Y	4	D	5	Y

B

1	İstemcisiz	2	GRE	3	3.	4	2018	5	Faz 1

C

1	D	2	A	3	E	4	B	5	C

5. ÖĞRENME BİRİMİ

A

1	Y	2	D	3	D	4	D

B

1	Ansible	2	yönetim düzlemi	3	OpenDaylight

C

1	A	2	E	3	B

KAYNAKÇA

- Bağcı, O. (2024, Şubat). *A321 Airbus In-Flight Network Optimization Based On Spanning Tree Protocol. A321 Airbus In-Flight Network Optimization Based On Spanning Tree Protocol* Yüksek Lisans Tezi.
- Cicioğlu, M., & Çalhan, A. (2016). *Yazılım Tanımlı Ağlarda Denetleyiciler. International Academıc Research Congress* (Ines 2016).
- Cicioğlu, M., & Çalhan, A. (2017). *Yazılım tanımlı ağlar–YTA*. Karaelmas Fen ve Mühendislik Dergisi, 7(2), 684-695.
- Çakmak, A. (2018). *Web Güvenliğinde SSL/TLS Kriptografik Protokolü: Açıklıklar, Saldırılar ve Güvenlik Önlemleri. Web Güvenliğinde SSL/TLS Kriptografik Protokolü: Açıklıklar, Saldırılar ve Güvenlik Önlemleri* Yüksek Lisans Tezi. İstanbul.
- Demir, F. (2010). *Güvenli Veri İletiminde Kullanılan Vpn Tiplerinin Uygulaması ve Performans Analizi. Güvenli Veri İletiminde Kullanılan Vpn Tiplerinin Uygulaması ve Performans Analizi* Yüksek Lisans Tezi. İstanbul.
- Göktaş, S. (2010). *Çok Protokollü Etiket Anahtarlama (MPLS) Teknolojisi ve Performans Analizi. Çok Protokollü Etiket Anahtarlama (MPLS) Teknolojisi ve Performans Analizi* Yüksek Lisans Tezi. İstanbul.
- Kırışoğlu, S. (2018). *Kurumsal Ağların Sistematik Tasarımı İçin Yeni Bir Dinamik Vlan Yaklaşımı. Kurumsal Ağların Sistematik Tasarımı İçin Yeni Bir Dinamik Vlan Yaklaşımı* Doktora Tezi. Düzce.
- Kreutz, D., Ramos, F. M., Esteves Verissimo, P., Esteve Rothenberg, C., Azodolmolky, S., & Uhlig, S. (2015). *Software-defined networking: A comprehensive survey*. Proceedings of the IEEE, 103(1), 14-76.
- Liao, J., Sun, H., Wang, J., Qi, Q., Li, K., & Li, T. (2017). *Density cluster based approach for controller placement problem in large-scale software defined networkings*. Computer Networks, 112, 24-35.
- Schaller, S., & Hood, D. (2017). *Software defined networking architecture standardization*. Computer Standards & İnterfaces, 54, 197-202.
- Stancu, A. L., Halunga, S., Vulpe, A., Suciu, G., Fratu, O., & Popovici, E. C. (2015, October). *A comparison between several Software Defined Networking controllers*. In Telecommunication in Modern Satellite, Cable and Broadcasting Services (TELSIKS), 2015 12th International Conference on (pp. 223¬226). IEEE.

- T.C. Millî Eğitim Bakanlığı. (2024). Siber Güvenlik Alanı Çerçeve Öğretim Programı, Ankara.
- Tomovic, S., Yoshigoe, K., Maljevic, I., & Radusinovic, I. (2017). *Software-defined fog network architecture for IoT*. Wireless Personal Communications, 92, 181-196.
- Xia, W., Wen, Y., Foh, C. H., Niyato, D., & Xie, H. (2015). *A survey on software-defined networking*. IEEE Communications Surveys & Tutorials, 17(1), 27-51.
- Xia, W., Wen, Y., Foh, C., H., Niyato, D., & Xie, H. (2015). *A Survey on Software-Defined Networking*. IEEE Communication Surveys & Tutorials, vol. 17, no. 1, first quarter.

* Kaynakça, APA 6 referanslama sistemi kullanılarak oluşturulmuştur.

* Bu materyalde ölçü birimlerinin uluslararası kısaltmaları kullanılmıştır.

GENEL AĞ KAYNAKÇASI VE GÖRSEL KAYNAKÇASI

Bu materyalde bulunan genel ağ kaynakçası ve görsel kaynakçasına, verilen karekodu okutarak veya bağlantı adresini kullanarak ulaşabilirsiniz.

http://kitap.eba.gov.tr/karekod/Kaynak.php?KOD=3437

Notlar: .....