

**Bu kitaba sığmayan
daha neler var!**



Karekodu okutun, bu kitapla
ilgili EBA içeriklerine ulaşın!

eba
www.eba.gov.tr



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

ISBN: 978-975-11-7122-1

Bandrol Uygulamasına İlişkin Usul ve Esaslar Hakkında Yönetmelik'in 5'inci Maddesinin
İkinci Fıkrası Çerçevesinde Bandrol Taşınması Zorunlu Değildir.

ÖDS

**ÖĞRENCİ/ÖĞRETMEN
DESTEK SİSTEMİ**

<https://ods.eba.gov.tr>

- Konu Anlatımlı Ders Videoları
- Soru Çözüm Videoları
- Ders Anlatım Videoları
- Çoktan Seçmeli Sorular



BİLİŞİM TEKNOLOJİLERİ ALANI

AĞ SİSTEMLERİ VE YÖNLENDİRME

11

DERS MATERYALİ

MESLEKİ VE TEKNİK ANADOLU LİSESİ

BİLİŞİM TEKNOLOJİLERİ ALANI

11 DERS
MATERYALİ

AĞ SİSTEMLERİ VE YÖNLENDİRME



```
Router>enable
Router#conf t
Router(config)#hostname Mesleki_Egitim
Bilisim(config)#enable password Bilisim
Bilisim(config)#
```



MESLEKİ VE TEKNİK ANADOLU LİSESİ
BİLİŞİM TEKNOLOJİLERİ ALANI

AĞ SİSTEMLERİ
VE YÖNLENDİRME

11
DERS MATERYALİ

YAZARLAR

Dr. Arzu KİLİTCİ CALAYIR

Ahmet KARBUKAN

Hasan ACAR

Murat KARATAŞ

Volkan ÇINAR



MİLLÎ EĞİTİM BAKANLIĞI YAYINLARI.....	8338
YARDIMCI VE KAYNAK KİTAPLARI DİZİSİ.....	2230

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

HAZIRLAYANLAR

Dil Uzmanı

Melek DEMİR

Program Geliştirme Uzmanı

Murat DAĞ

Ölçme ve Değerlendirme Uzmanı

Filiz İSNAÇ

Rehberlik Uzmanı

Feyza SÜNBÜL

Görsel Tasarım Uzmanı

Cem Emrah GÜN

ISBN: 978-975-11-7122-1

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,
Medeniyet 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 İlahî, 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 cerihamdan İlahî, boşanıp kanlı yaşım,
Fışkırır ruh-ı mücerret gibi yerden na'sım;
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 hürriyet;
Hakkıdır Hakk'a tapan milletimin istiklâl!

Mehmet Âkif Ersoy

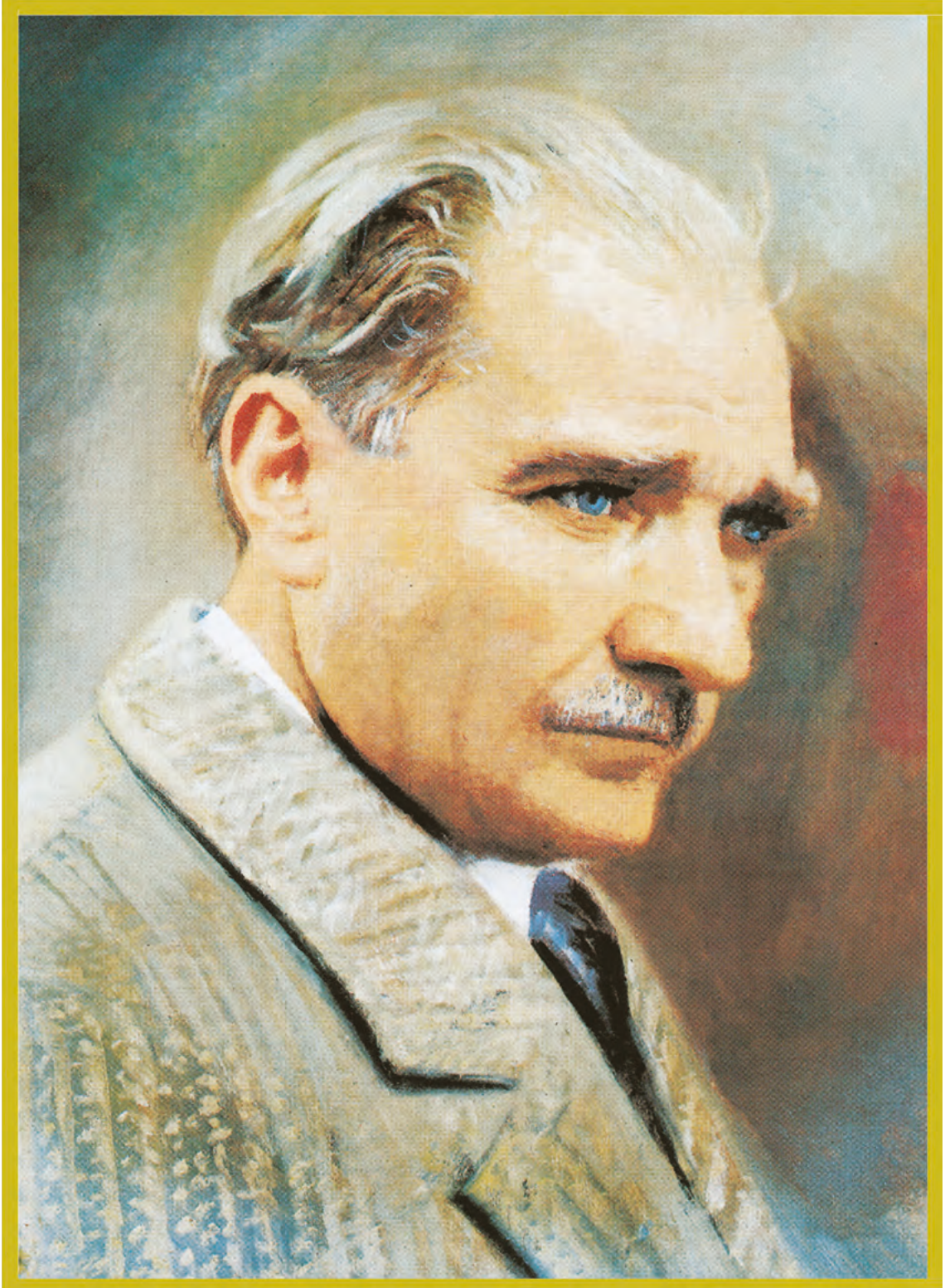
GENÇLİĞE HİTABE

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 namûsait 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 SİMÜLASYONU	14
1.1. SİMÜLASYON PROGRAMI	16
1.1.1. Simülasyon Programının Kurulumu	16
1.1.2. Kullanıcı Arayüzü	18
1.1.3. Simülasyon Ortamına Cihaz Yerleşimi	19
1.1.4. Cihaz Konfigürasyonu	19
1.1.5. Simülasyon Modu	21
1.1.6. Packet Tracer Dosya Türleri	22
1.2. LAN SİMÜLASYONU	22
1.3. WAN SİMÜLASYONU	24
1.4. KABLOSUZ AĞ SİMÜLASYONU	26
ÖLÇME VE DEĞERLENDİRME	31
2. ÖĞRENME BİRİMİ: KABLOSUZ AĞLAR	32
2.1. KABLOSUZ AĞ STANDARTLARI VE BİLEŞENLERİ	34
2.1.1. Kablosuz Ağ Teknolojileri	34
2.1.2. Kablosuz Ağ Standartları	37
2.1.3. Kablosuz Ağ Bileşenleri	39
2.1.4. Kablosuz Ağa Bağlantı	40
2.1.5. Kablosuz Ağ Kanal Seçimi	44
2.2. KİŞİSEL ALAN AĞLARI	45
2.3. KABLOSUZ AĞ YAPILANDIRMASI	48
2.3.1. Kablosuz Ağ	48
2.3.2. Kablosuz Ağ Çeşitleri	49
2.3.3. Kablosuz Ağ Yapıları	49
2.3.4. WLAN Avantaj ve Dezavantajları	51
2.3.5. Kablosuz Ağ Yapılandırması	51
2.3.6. Kablosuz Ağ Tehditleri	55
2.3.7. Kablosuz Ağ Güvenliği	56
2.3.8. Kablosuz Ağ Testi	59
2.3.9. Kablosuz Ağ Simülasyonu	60
ÖLÇME VE DEĞERLENDİRME	67
3. ÖĞRENME BİRİMİ: YÖNLENDİRİCİLER	68
3.1. YÖNLENDİRİCİLERİN YAPISI VE BAĞLANTILARI	70
3.1.1. Yönlendirici Bileşenleri	70
3.1.2. Yönlendirici Arayüz Bağlantıları	71
3.2. KOMUT ARAYÜZÜ KULLANARAK KULLANICI GİRİŞİ	75
3.2.1. Yardım Komutları	79
3.3. TEMEL YÖNLENDİRİCİ TANIMLAMALARI	80
3.3.1. Yönlendirici Cihaza İsim Verme	80
3.3.2. Yönlendirici Şifreleme	80
3.3.3. Seri Arayüz Yapılandırma	83
3.3.4. Ethernet Arayüz Yapılandırma	84



3.3.5. Yapılandırma Değişikliklerini Kaydetme	85
3.4. ARAYÜZ YAPILANDIRMA	86
3.4.1. Arayüz Tanımlama	86
3.4.2. Arayüz Bağlantı Mesajları	88
3.4.3. Yönlendirici Açılış Mesajları	89
3.4.4. Yönlendirici Host Tablosu	89
3.4.5. Kullanıcı Seviyeleri Oluşturma	92
3.4.6. Yapılandırma Dosyalarını Uzak Sunucuya Yedekleme	93
ÖLÇME VE DEĞERLENDİRME	97
4. ÖĞRENME BİRİMİ: YÖNLENDİRME TEMELLERİ VE	
STATİK YÖNLENDİRME	98
4.1. YÖNLENDİRME İŞLEMLERİ	100
4.1.1. Yönlendirme Tabloları	100
4.1.2. Yönlendirme Komutları	101
4.2. YOL TANIMLAMA PROTOKOLLERİ	102
4.2.1. Doğrudan Bağlı Rotalar	102
4.2.2. Statik Rotalar	102
4.2.3. Dinamik Olarak Güncellenmiş Rotalar	103
4.2.4. Varsayılan Rotalar	103
4.3. STATİK YÖNLENDİRME İŞLEMLERİ	104
4.3.1. Statik Yönlendirme Uygulaması	142
4.3.2. Varsayılan Yönlendirme Uygulaması	107
4.3.3. NAT (Ağ Adresi Dönüştürme) Protokolü	110
4.3.4. Dinamik NAT Uygulaması	118
4.3.5. Statik NAT Uygulaması	121
ÖLÇME VE DEĞERLENDİRME	123
5. ÖĞRENME BİRİMİ: DİNAMİK YÖNLENDİRME İŞLEMLERİ	124
5.1. DİNAMİK YÖNLENDİRME	126
5.1.1. Dinamik Yönlendirme Parametreleri	126
5.1.2. Dinamik Yönlendirme Tablolarının Oluşumu	127
5.1.3. Dinamik Yönlendirme Protokolü Grupları	128
5.2. YÖNLENDİRME BİLGİSİ PROTOKOLÜ (RIP)	130
5.2.1. RIP Özellikleri	130
5.2.2. RIP Yapılandırması	130
5.2.3. RIP ve RIPv2'nin Farklılıkları	137
5.2.4. Yönlendirici Arayüzlerinde RIP Paketlerinin Gönderiminin Engellenmesi	146
5.3. OSPF YÖNLENDİRME PROTOKOLÜ	148
5.3.1. OSPF Özellikleri	148
5.3.2. OSPF Aşamaları	148
5.3.3. OSPF Yönlendirici Çeşitleri	148
5.3.4. OSPF Yapılandırması	149
5.3.5. OSPF Rota Maliyet Hesaplama	156
5.3.6. Yayın Ağlarında OSPF	164
5.3.7. OSPF ile Kimlik Doğrulama	173



5.3.8. Farklı OSPF Alanları ve Varsayılan Rota Dağıtımı	176
5.4. EIGRP YÖNLENDİRME PROTOKOLÜ.....	181
5.4.1. EIGRP Özellikleri	181
5.4.2. EIGRP Paket Türleri.....	182
5.4.3. EIGRP Yapılandırması.....	182
5.5. SINIR AĞ GEÇİDİ PROTOKOLÜ (BGP)	193
5.5.1. BGP Özellikleri	194
5.5.2. BGP Mesajları	194
5.5.3. BGP Komşuluk Türleri.....	195
5.5.4. BGP Komşuluğu Aşamaları	195
5.5.5. BGP Yapılandırması	196
ÖLÇME VE DEĞERLENDİRME	202
6. ÖĞRENME BİRİMİ: WAN KONSEPTİ	204
6.1. POINT-TO-POINT BAĞLANTILAR	206
6.1.1. Kapsülleme (Encapsulation)	206
6.1.2. Bağlantı Kontrol Protokolü (Link Control Protocol-LCP)...	207
6.1.3. Ağ Kontrol Protokolü (Network Control Protocol-NCP) ...	207
6.1.4. PPP Yapılandırma.....	207
6.1.5. PPP Kimlik Doğrulama Protokolleri	208
6.2. ERİŞİM KONTROL LİSTELERİ (ACL)	212
6.2.1. Standart Erişim Kontrol Listeleri (Standard Access List)...	213
6.2.2. Genişletilmiş Erişim Kontrol Listeleri (Extended Access List)	215
6.2.3. İsimli Erişim Kontrol Listeleri (Named Access List)	217
6.3. AĞ GÜVENLİĞİ VE AĞ İZLEME	220
6.3.1. Ağ İzleme Yazılımı	220
6.3.2. Servis Kalitesi (QoS).....	222
6.3.3. Ağ Sorunları.....	223
ÖLÇME VE DEĞERLENDİRME	225
7. ÖĞRENME BİRİMİ: GÜVENLİK DUVARI TEKNOLOJİLERİ	226
7.1. GÜVENLİK DUVARI.....	228
7.2. IDS YAPILANDIRMA	229
7.3. IPS YAPILANDIRMA.....	229
ÖLÇME VE DEĞERLENDİRME	237
CEVAP ANAHTARLARI	238
KAYNAKÇA	239
GÖRSEL KAYNAKÇA	240



Öğrenme biriminin numarasını gösterir.

**1. ÖĞRENME BİRİMİ
AĞ SİMÜLYASYONU**

KONULAR

- 1.1. SİMÜLYASYON PROGRAMI
- 1.2. LAN SİMÜLYASYONU
- 1.3. WAN SİMÜLYASYONU

ANAHTAR KELİMELER

- Ağ simülasyonu
- Packet Tracer
- Kablosuz ağlar
- Adresleme
- LAN ağları
- WAN ağları

NELER ÖĞRENECEKSİNİZ?

- Simülasyon programının temel özellikleri
- Simülasyon programının kurulumu
- Doğru çarpın LAN simülasyonu
- Doğru çarpın WAN simülasyonu
- Doğru çarpın kablosuz ağ simülasyonu

Öğrenme biriminin bölümlerini gösterir.

Öğrenme biriminin kavramlarını gösterir.

Öğrenme biriminde neler öğrenileceğini gösterir.

Öğrenme biriminin adını gösterir.

Öğrenme biriminin numarasını gösterir.

Öğrencilerin öğrenme birimiyle ilgili ön bilgilerini harekete geçirmek ve konuya ilgilerini çekmek için yapılacak çalışmaları gösterir.

Alt konu başlıklarını gösterir.

Sayfa numarasını gösterir.

1. ÖĞRENME BİRİMİ

HAZIRLIK ÇALIŞMALARI

- Ağ cihazı hakkında bildiklerinizi arkadaşlarınızla paylaşınız.
- Veri iletim ortamları hakkında bildiklerinizi arkadaşlarınızla paylaşınız.

1.1. SİMÜLYASYON PROGRAMI

Simülasyon programı, ağ tasarımı yapmaya olanak sağlayan bir modelleme aracıdır. Bu program ile özel ekipmanlara gereksinim duymadan kurmuş ağ sistemleri modellemek, Packet Tracer, yenilikçi bir ağ simülasyon ve görselleştirme aracıdır. Bu ücretsiz yazılım masaüstü bilgisayar, Android veya iOS tabanlı bir mobil cihaz aracılığıyla çalıştırılabilir ve sorularınızı öğrenme becerilerinizi geliştirmeye yardımcı olur. Packet Tracer hem Linux hem de Windows masaüstü ortamları için mevcuttur.

Packet Tracer, gerçek ağların simüle edilmesini sağlar. Packet Tracer programı, pahalı laboratuvar ekipmanlarının kullanılmadığı çeşitli boyuttaki ağları tasarlamak ve kurmak için kullanıma hazır bir araçtır. Paketli yönlendiriciler, anahtarlar, güvenlik duvarları ve sunucular kullanılarak ağ tasarımlarını ucuz ve hızlı bir şekilde gerçekleştirilmesine olanak sağlar.

1.1.1. Simülasyon Programının Kurulumu

www.netacad.com sayfasına girilerek, Üst menüdeki Kaynaklar (Resources) bölümünden Packet Tracer programına ilişkin gerekli indirme ve kurulum bilgilerine ulaşılır. Görsel 1.1, Görsel 1.2, Görsel 1.3, Görsel 1.4, Görsel 1.5, Görsel 1.6'da verilen sırayla kurulumu tamamlayınız.

Resources

Ad	Yazın	Yayın Yılı
1. Packet Tracer Kurulumu	1.1.1.1	2018
2. Packet Tracer Kurulumu	1.1.1.2	2018
3. Packet Tracer Kurulumu	1.1.1.3	2018
4. Packet Tracer Kurulumu	1.1.1.4	2018
5. Packet Tracer Kurulumu	1.1.1.5	2018
6. Packet Tracer Kurulumu	1.1.1.6	2018

Görsel 1.1: Packet Tracer dosyası

Konu içindeki öğrenci çalışmalarını gösterir.

Konu içinde dikkat edilmesi gereken yerleri gösterir.

Öğrenme biriminin adını gösterir.

UYARI

Çalışan ayarları bakiyede zaman password parametresiyle verilen yitre kriptolanmadığı için açıkça görülür. Bu durumu engellemek için service password-encryption komutu kullanılır. Bu komut ile yapılacak kriptolama, secret ile yapılacak kriptolama işlemi kadar güçlü değildir.

```
Router(config)#service password-encryption
```

SIRA SİZDE

Yönlendiriciye "Ankara1920" parolaşını veriniz ve parolaşını kriptolayarak gösteriniz.

ARASTIRMA

Yönlendiriciye password ve secret parametrelerinin her ikisiyle de yitre atanması yönlendirici hangi yitreyi kullanır?

3.3.2.3. Konstel Anayışıklı Yönlendirme

Yönlendirici cihazına konstel bağılantısı ile yapılacak yitkisi gösterir, global yapılandırma modunda yitre verileri engellenir.

Konstel bağılantıları yitirmek için aşağıdaki komutlar kullanılır:

```
Router>
Router>enable
Router(config)#terminal
Router(config)#line console 0
Router(config)#line password MEVLANA
Router(config)#line logging
```

3.3.2.4. TELNET Bağlantısı Yönlendirme

TELNET, yönlendirici cihazı uzaktan erişim sağlayarak cihazın yapılandırmasını sağlayan bir bağılantı türüdür. Yönlendirici cihazı TELNET bağılantısı ile yapılacak yitkisi gösterir, global yapılandırma modunda yitre verileri engellenir.

TELNET bağılantılarını yitirmek için aşağıdaki komutlar kullanılır:

```
Router>
Router>enable
Router(config)#terminal
Router(config)#line vty 0 4
Router(config)#line password BULDUZ
Router(config)#line logging
```

Adım 12: Router0 yönlendiricisinde "show ip route" komutu ile yönlendirici tablosunu görüntüleyiniz.

İşlevsel olarak ip route

```
192.0.0.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.0.0.0/24 is directly connected, FastEthernet0/0
C 192.0.0.0/24 is directly connected, FastEthernet0/0
192.168.1.0/24 is variably subnetted, 4 subnets, 2 masks
C 192.168.1.0/24 is directly connected, FastEthernet0/0
C 192.168.1.0/24 is directly connected, FastEthernet0/0
C 192.168.1.0/24 is directly connected, FastEthernet0/0
C 192.168.1.0/24 is directly connected, FastEthernet0/0
```

Göröl 5.25: RIPv2'nin yönlendirme tablosu

Göröl 5.25'te Router0 yönlendiricisi, Router1 ve Router2 yitir altı ağı maskeleri ile öğrenmiştir. 192.168.1.64/26 ağına 1 metrik değeri ile, 192.168.3.128/26 ağına 2 metrik değeri ile ulaşılabilmektedir.

Adım 13: PC0'ın PC1 ve PC2'nin IP adreslerini "ping" komutu ile iletişim testi gerçekleştiriniz. İletişim testi başarılı oldu mu? Doğru yönlendirme tablolarına sahip olduğun için iletişim testleri başarılı olacaktır.

SIRA SİZDE

Router1 ve Router2 yönlendiricilerinde "show ip route" komutu ile yönlendirici tablosunu görüntüleyip inceleyiniz.

UYGULAMA 4

Göröl 5.26'da bir firma için verilen ağı topolojiyi simülasyon programında oluşturunuz. Tablo 5.5'te yer alan IP bağılantıları kullanıp ilgili cihazları yapılandırarak uygulama ademinizi gerçekleştiriniz.

Göröl 5.26: Uygulama 4'in ağı topolojisi

Konu içindeki öğrenci araştırmalarını gösterir.

Uygulama faaliyetlerini gösterir.

Etkileşimli kitap, video, ses, animasyon, uygulama, oyun, soru vb. kaynaklara ulaşılabilecek link ve karekodu gösterir.

Ölçme ve değerlendirme çalışmalarını gösterir.

KONULANDIRMA TEMELLERİ VE TERCİH KONULANDIRMA

ÖLÇME VE DEĞERLENDİRME

Aşağıdaki soruları dikkatlice okuyarak doğru seçeneği işaretleyiniz.

1. Aşağıda yönlendirme tablosu ile ilgili verilen ifadelerden hangisi yanlıştır?

A) Farklı bir yitir yönlendiricisi gerektirir ve her zaman için geçerlidir.

B) Yönlendirme tablosu tüm cihazlarda bulunur.

C) Metrik değeri sadece doğrudan yitirler için bulunur.

D) Yönlendirme tablosu değeri yüksek yitirler öncelikli olarak kabul edilir.

E) Sadece doğrudan yitirler tablosunda bulunur.

2. Aşağıdakilerden hangisi yönlendirme tablosundaki verilerin yönlendirme için kullanılan birimdir?

A) R

B) S

C) D

D) S

E) C

3. Aşağıdaki komutlardan hangisi statik yönlendirme için kullanılır?

A) ip route

B) ipconfig

C) ip route

D) ip address

E) tracert

4. Aşağıdaki ifadelerden hangisi statik yönlendirme için doğrudur?

A) Yönlendirme tablosu değeri yüksek yitirler öncelikli olarak kabul edilir.

B) Yönlendirme tablosu değeri yüksek yitirler öncelikli olarak kabul edilir.

C) Değişken yitirler statik yitirler olarak kabul edilir.

D) Yönlendirme tablosu değeri yüksek yitirler öncelikli olarak kabul edilir.

E) Statik yitirler öncelikli olarak kabul edilir.

5. Aşağıda NAT işlemi ile ilgili verilen ifadelerden hangisi yanlıştır?

A) Yitir ağına dış IP adreslerini genel IP adreslerine çevirir.

B) Yitir ağına dış IP adreslerini genel IP adreslerine çevirir.

C) Statik NAT işlemi, yitir ağına dış IP adreslerini genel IP'ye bir bir çevirir.

D) Dinamik NAT işlemi, yitir ağına dış IP adreslerini dinamik olarak harayarak IP'ye çevirir.

E) NAT Overload (PAT) işlemi için IP portları kullanılır.



KONULAR

1.1. SİMÜLASYON PROGRAMI

1.2. LAN SİMÜLASYONU

1.3. WAN SİMÜLASYONU

ANAHTAR KELİMELER

- Ağ simülasyonu
- Packet Tracer
- Kablolu iletişim
- Kablosuz iletişim
- LAN iletişimi
- WAN iletişimi



1. ÖĞRENME BİRİMİ

AĞ SİMÜLASYONU

NELER ÖĞRENECEKSİNİZ?

- Simülasyon programının temel özellikleri
- Simülasyon programının kurulumu
- Doğru çalışan LAN simülasyonu
- Doğru çalışan WAN simülasyonu
- Doğru çalışan kablosuz ağ simülasyonu



HAZIRLIK ÇALIŞMALARI

1. Ağ cihazı hakkında bildiklerinizi arkadaşlarınızla paylaşınız.
2. Veri iletim ortamları hakkında bildiklerinizi arkadaşlarınızla paylaşınız.

1.1. SİMÜLASYON PROGRAMI

Simülasyon programı, ağ tasarımı yapmaya olanak sağlayan bir modelleme aracıdır. Bu program ile özel ekipmanlara gereksinim duyulmadan karmaşık ağ sistemleri modellenir.

Packet Tracer, yenilikçi bir ağ simülasyon ve görselleştirme aracıdır. Bu ücretsiz yazılım masaüstü bilgisayar, Android veya IOS tabanlı bir mobil cihaz aracılığıyla ağ yapılandırmasını ve sorun giderme becerilerini geliştirmeye yardımcı olur. Packet Tracer hem Linux hem de Windows masaüstü ortamları için mevcuttur.

Packet Tracer, gerçek ağların simüle edilmesini sağlar. Packet Tracer programı, pahalı laboratuvar ekipmanlarının kullanılacağı çeşitli boyutlardaki ağları tasarlamak ve kurmak için kullanımı kolay bir araçtır. Fiziksel yönlendiriciler, anahtarlar, güvenlik duvarları ve sunucular kullanılarak ağ tasarımlarının ucuz ve hızlı bir şekilde gerçekleştirilmesine olanak sağlar.

1.1.1. Simülasyon Programının Kurulumu

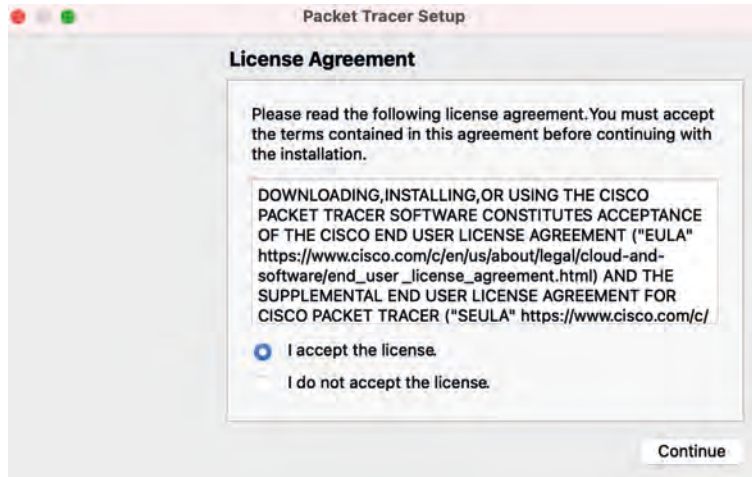
www.netacad.com sayfasına üye olunarak, üst menüdeki Kaynaklar (Resources) bölümünden Packet Tracer programının bilgisayarın işletim sistemine uygun olanı seçilip bilgisayara indirilir. Görsel 1.1, Görsel 1.2, Görsel 1.3, Görsel 1.4, Görsel 1.5, Görsel 1.6'da verilen sırayla kurulumu tamamlayınız.

Name	Size	Last Modified
Cisco Packet Tracer FAQs 8.0.pdf	303.56 kB	28 Jan 2021 1:02 PM
PacketTracer800_Build211_32bit_setup-signed.exe	144.57 MB	28 Jan 2021 1:59 AM
PacketTracer800_Build212_64bit_setup-signed.exe	156.65 MB	25 Jan 2021 1:08 PM
PacketTracer800_Build212_mac_notarized.dmg	189.51 MB	28 Jan 2021 2:00 AM
PacketTracer_800_amd64_build212_final.deb	175.3 MB	28 Jan 2021 2:05 AM

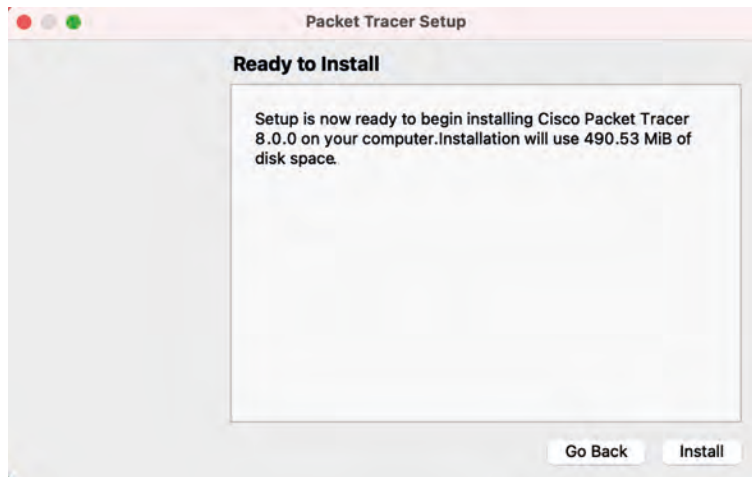
Görsel 1.1: Packet Tracer dosyaları



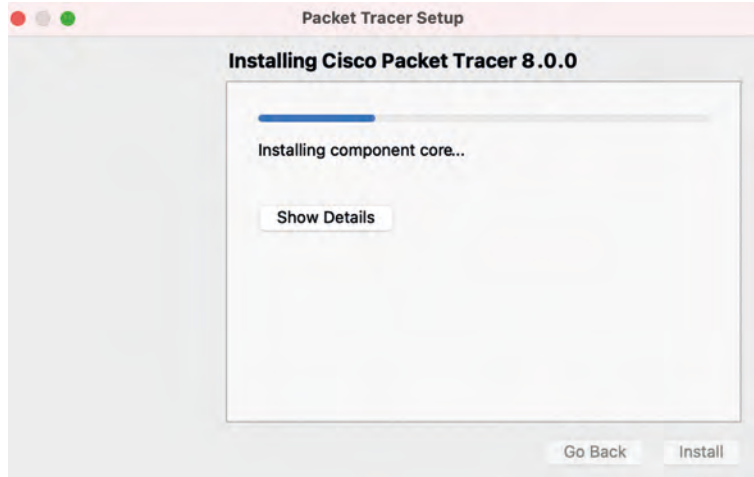
Görsel 1.2: Packet Tracer kurulum sihirbazı



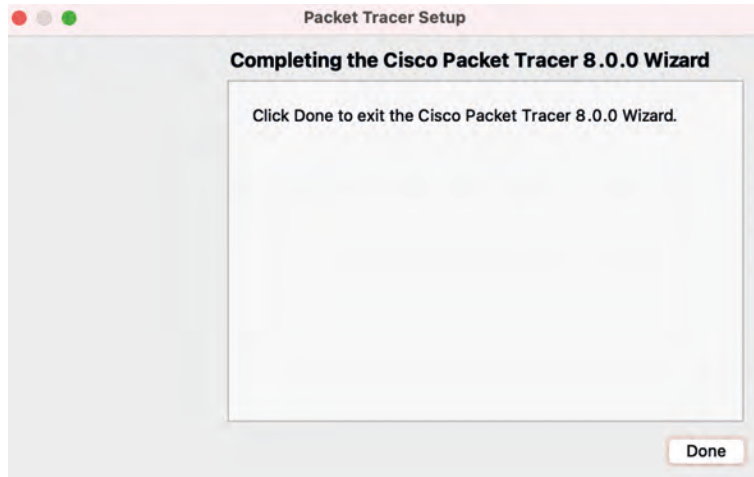
Görsel 1.3: Packet Tracer sözleşme kabul seçeneği



Görsel 1.4: Packet Tracer yükleme ekranı



Görsel 1.5: Packet Tracer bileşenlerinin yüklenmesi



Görsel 1.6: Packet Tracer yüklemenin tamamlanması

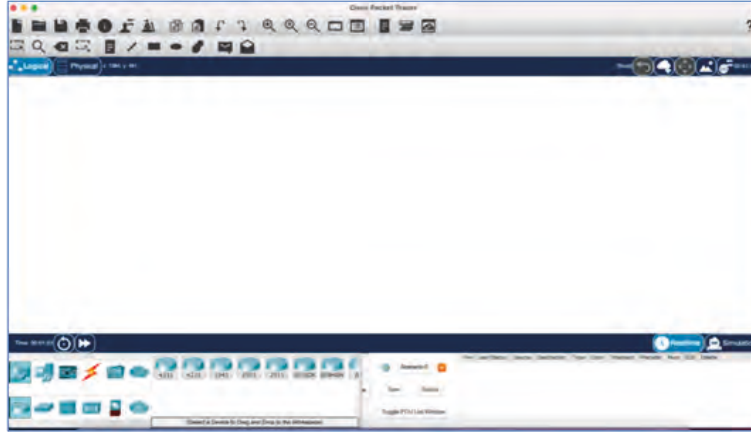
1.1.2. Kullanıcı Arayüzü

Packet Tracer sayesinde cihazlar çalışma ortamına eklenip, birbirlerine kablolu veya kablosuz olarak bağlanabilir. Ayrıca ağdaki bileşenler seçilip silme, inceleme, etiketleme ve gruplandırma işlemleri gerçekleştirilebilir. Packet Tracer çalışma ortamında oluşturulan ağlar da yönetilebilir.

Ağ yönetimi menüsü kullanılarak şu işlemler yapılabilir:

- Mevcut veya örnek bir ağ açılabilir.
- Oluşturulan ağ kaydedilebilir.
- Kullanıcı profil veya tercihleri de değiştirilebilir.

Üst menü çubuğunda bulunan Dosya menüsü kullanılarak **Aç**, **Kaydet**, **Farklı Kaydet** ve **Çık** komutları çalıştırılabilir (Görsel 1.7).

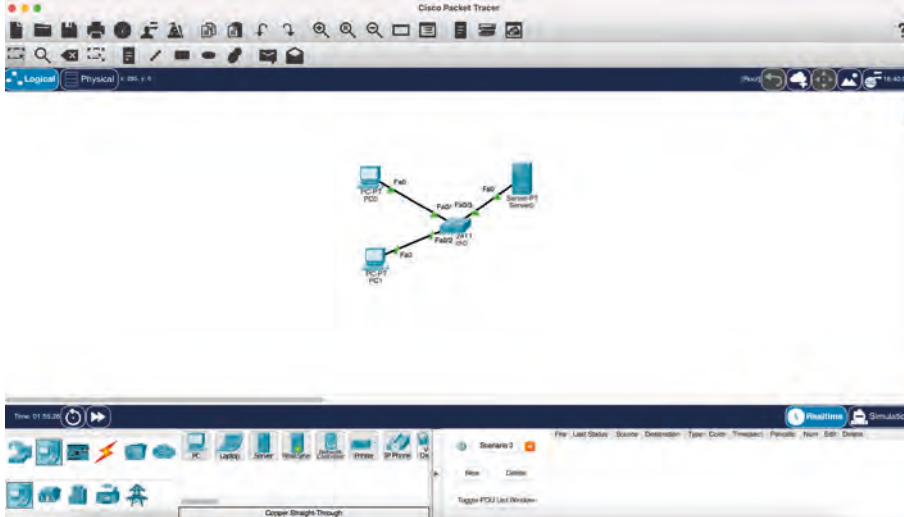


Görsel 1.7: Packet Tracer kullanıcı arayüzü

1.1.3. Simülasyon Ortamına Cihaz Yerleşimi

Packet Tracer ile ağlar ve ağ trafiği simüle edilir. Fiziksel ağ simülasyonu için ağ tasarımındaki cihazlarda Cihaz Tipi Seçim Kutusu (Device-Type Selection Box) kullanılır. Cihaz Tipi Seçim Kutusunda kategoriler (categories) ve alt kategoriler (sub-categories) bulunur (Görsel 1.8).

Kategoriler içinde Ağ Cihazları (Networking Devices), Uç Cihazlar (End Devices), Bileşenler (Components), Bağlantılar (Connections), Çeşitli (Miscellaneous) ve Çok Kullanıcı Bağlantı (Multiuser Connection) yer alır. Her kategori, en az bir alt kategori grubunu içerir.



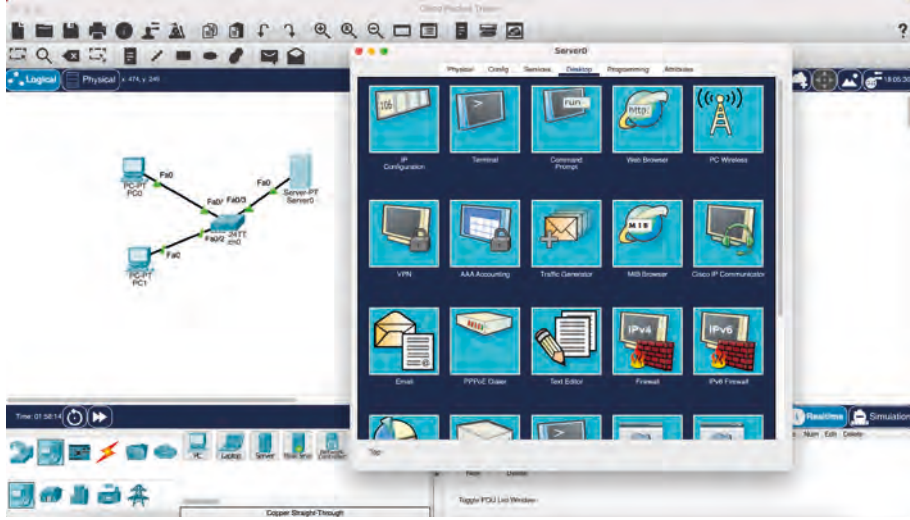
Görsel 1.8: Packet Tracer'ın mantıksal bölümü

1.1.4. Cihaz Konfigürasyonu

Görsel 1.9'daki ağ oluşturulduktan sonra cihazları ve bileşenleri yapılandırma işlemine başlanır. Packet Tracer, ağı oluşturan farklı ağ cihazlarını ve kullanıcı cihazlarını yapılandırma özelliğine sahiptir. Herhangi bir cihazın konfigürasyon arayüzüne erişilmek istendiğinde önce konfigüre edilecek cihaza tıklanır. Sonrasında bir dizi sekmeyi gösteren bir açılır pencere görüntülenir. Açılan pencerede farklı cihaz türlerinin farklı arayüzleri bulunur.

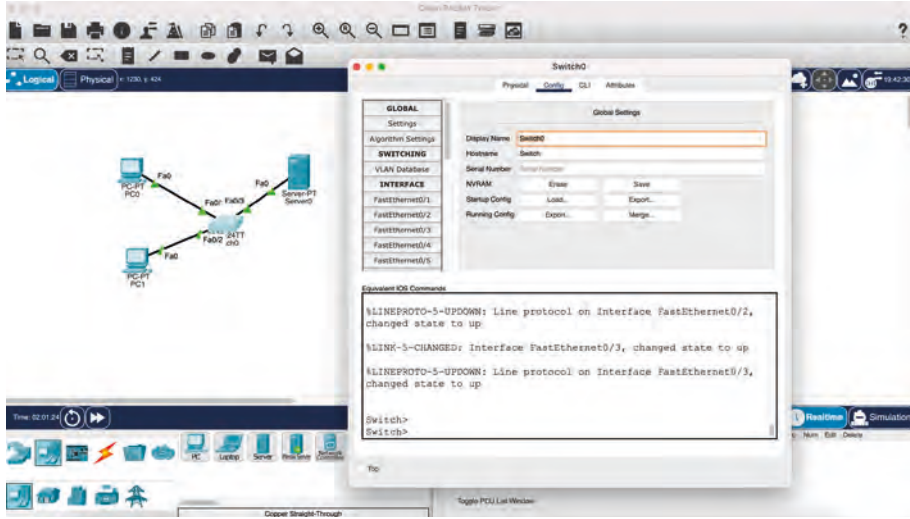
1. ÖĞRENME BİRİMİ

Packet Tracer; PC'ler ve dizüstü bilgisayarlar gibi bazı uç cihazlar için IP yapılandırmaya, kablosuz yapılandırmaya, komut istemine, web tarayıcısına ve çok daha fazlasına erişim için bir masaüstü arabirimi sağlar.

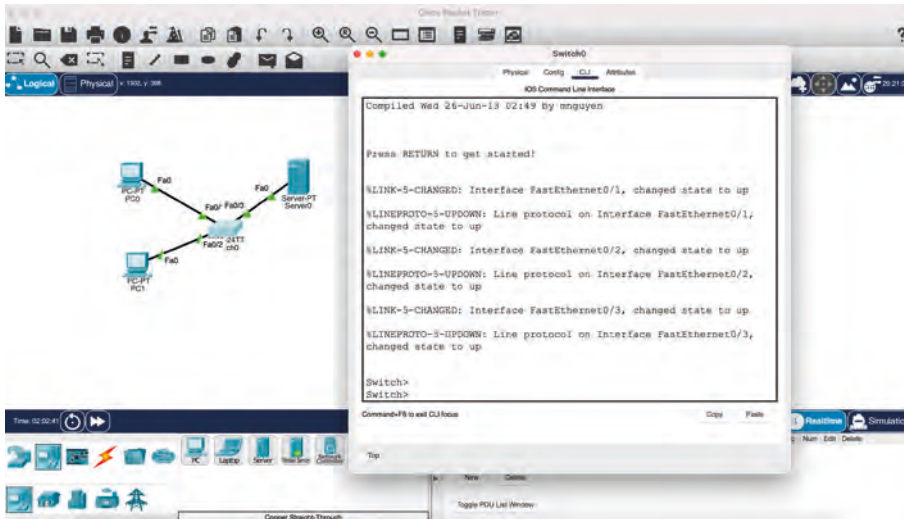


Görsel 1.9: Packet Tracer'da GUI ve CLI'ya erişim

Yönlendiriciler (router) ve anahtarlar (switch) gibi ağ cihazları için iki farklı yapılandırma yöntemi vardır. Aygıtlar, yapılandırma sekmesinde bulunan grafik kullanıcı arayüzü (GUI) veya bir komut satırı arayüzü (CLI) aracılığıyla yapılandırılabilir (Görsel 1.10 ve Görsel 1.11).



Görsel 1.10: Anahtar grafik kullanıcı arayüzü (GUI)



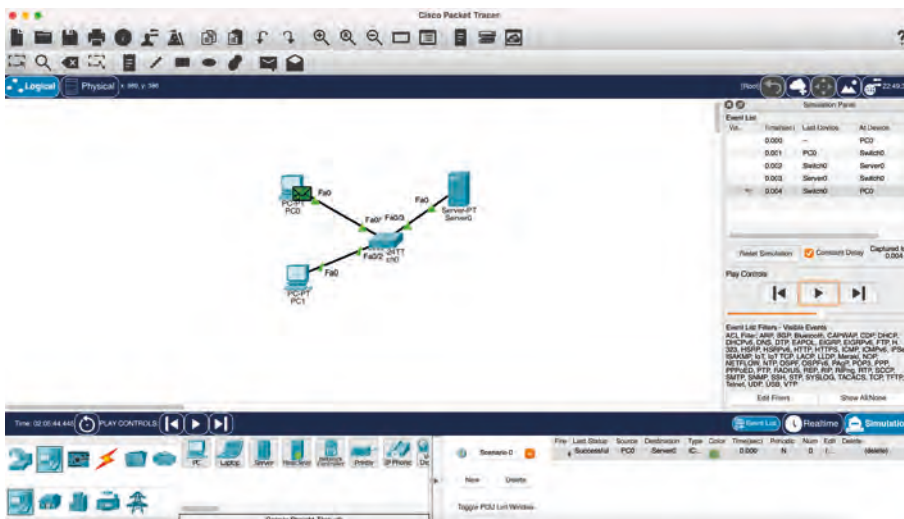
Görsel 1.11: Anahtar komut satırı arayüzü (CLI)

1.1.5. Simülasyon Modu

Packet Tracer, ağdaki farklı işlevleri kontrol etmek için PDU'lar oluşturulmasına ve yakalanmasına izin veren bir simülasyon modu sunar. Simülasyon modu ile şu sorulara cevap bulunabilir:

- Tüm cihazlar temel bağlantılar sayesinde birbiriyle iletişim kurabilir mi?
- Güvenlik için erişim listeleri tasarlandığı gibi çalışıyor mu?
- DNS, HTTP ve FTP gibi uygulamalar ve hizmetler tasarlandığı gibi çalışıyor mu?

Packet Tracer için varsayılan mod seçeneği gerçek zamanlı (realtime) moddur. Gerçek zamanlı modda, çalışma sayfasının sağ alt köşesinde görülen saat sürekli çalışır. Simülasyon modunda veri trafiği her seferinde bir paket görüntülenmesine izin verilmesi için istendiği zaman kullanıcılar tarafından durdurulabilir veya yavaşlatılabilir. Simülasyon modu doğrudan kullanıcı tarafından kontrol edilir ve zamanla birlikte ağ trafiğini ayrıntılı olarak gözlemlemek için kullanılır (Görsel 1.12).



Görsel 1.12: Simülasyon modu

1.1.6. Packet Tracer Dosya Türleri

Packet Tracer, üç farklı dosya türü oluşturma yeteneğine sahiptir. Dosya türleri .pkt, .pkz ve .pka olabilir. Bu dosya türleri farklı amaçlar için kullanılır.

- **.pkt** uzantılı dosya türü, Packet Tracer’da simüle edilmiş bir ağ oluşturulup kaydedildiği zaman kullanılır. .pkt uzantılı dosyada gömülü arka planlar da bulunabilir.
- **.pkz** uzantılı dosya türü çok sık kullanılmaz. Packet Tracer dosyalarıyla birlikte .pdf uzantılı dosyalar gibi farklı dosyaların uygulamaya dâhil edilmesini sağlayan sıkıştırılmış bir dosya türüdür.
- **.pka** dosya türü ise Packet Tracer Aktivite dosyasıdır. Bu dosya türü, bir Packet Tracer etkinliği ve bir talimat penceresi (instruction window) içerir. Talimatlar; faaliyeti, ödevi veya değerlendirmeyi tamamlamak için gerekli süreçlerin özetini sunar. Ayrıca talimat penceresi aktivitenin ne kadarının başarıyla tamamlandığını izlemek için bir tamamlama yüzdesi gösterir. Geri bildirim sağlamak için de yapılandırılabilen bir kontrol sonuçları (check results) özelliği vardır.

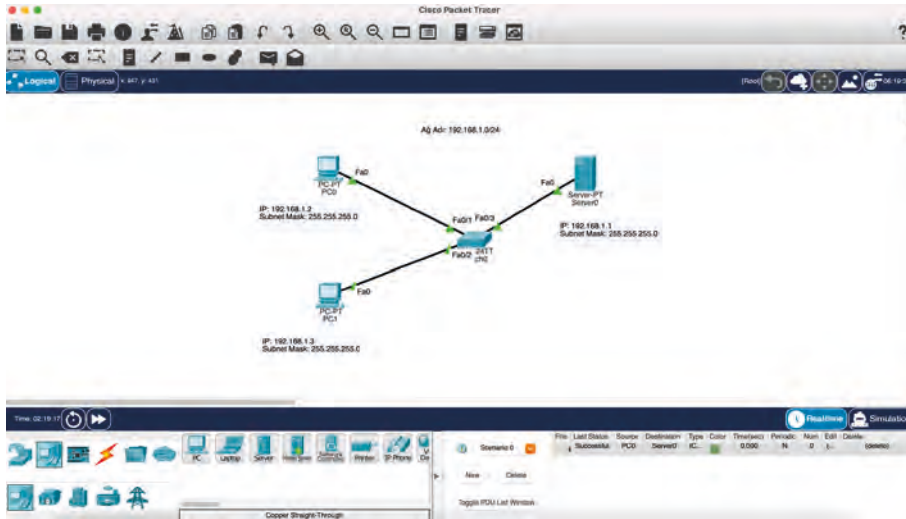
1.2. LAN SİMÜLASYONU



1. UYGULAMA

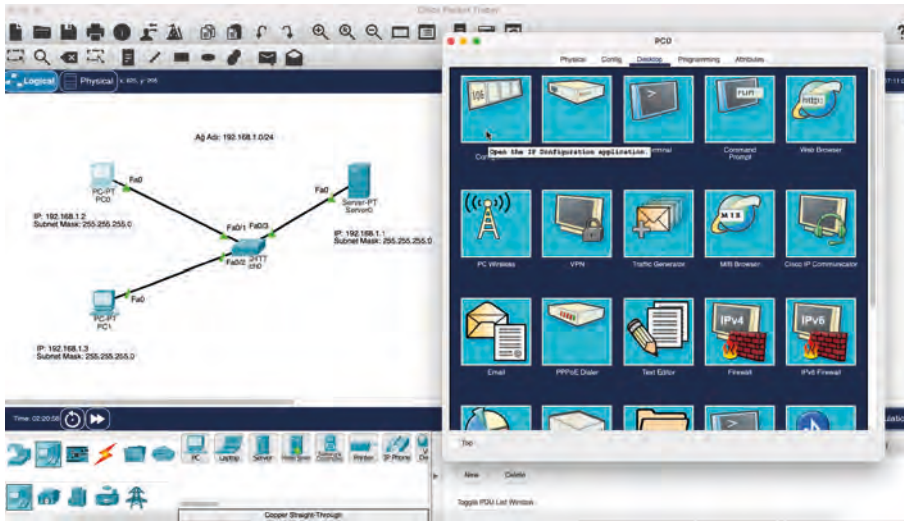
LAN Simülasyonu

İşlem adımlarına göre Görsel 1.13’teki LAN topolojisini simülasyon programında hazırlayınız.

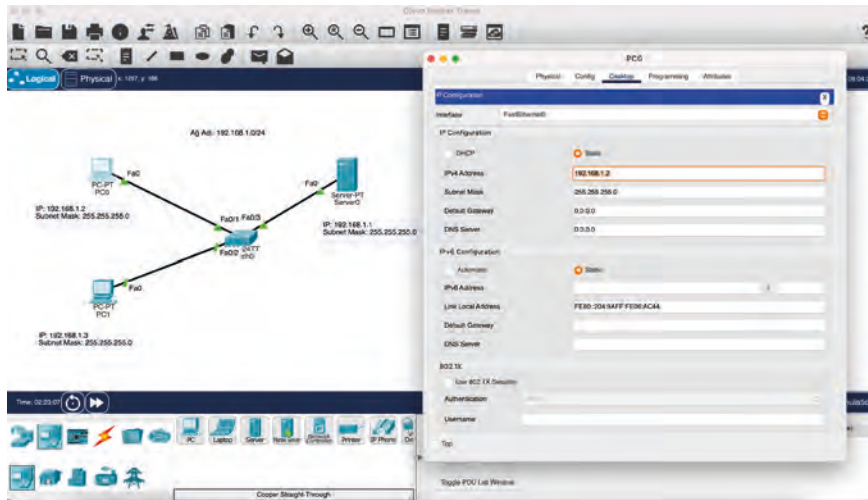


Görsel 1.13: LAN ağ topolojisi

1. Adım: Görsel 1.13’teki ağ topolojisini oluşturunuz. PC0, PC1 ve Server0 cihazlarının IP, Alt Ağ Maskesi (Subnet Mask) bilgileri Görsel 1.14 ve Görsel 1.15’te verilmiştir.



Görsel 1.14: PC0 Masaüstü (Desktop) GUI ayarları



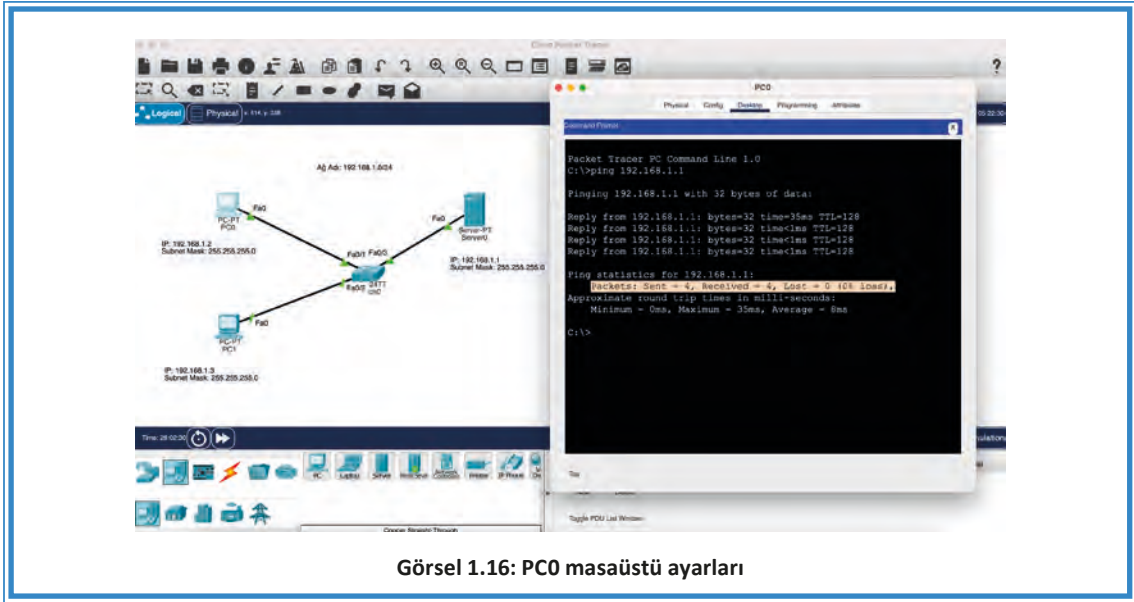
Görsel 1.15: PC0 IP konfigürasyon (IP Configuration) ayarları



SIRA SİZDE

PC1 ve Server0 cihazlarının IP, alt ağ maskesi bilgilerini kullanıcı arayüzünü kullanarak giriniz.

2. Adım: GUI arayüzüne girerek sırasıyla PC0, PC1 ve Server0 cihazlarının arasındaki iletişimi “ping” komutu ile doğrulayınız (Görsel 1.16).



Görsel 1.16: PC0 masaüstü ayarları



SIRA SİZDE

PC1 ve Server0 cihazları için “ping” komutunu kullanınız.

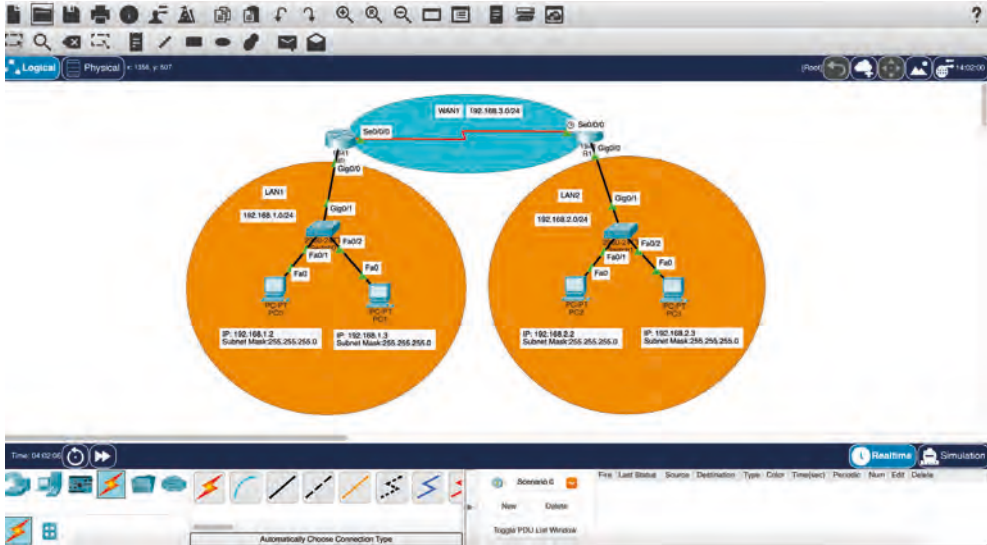
1.3. WAN SİMÜLASYONU



2. UYGULAMA

WAN Simülasyonu

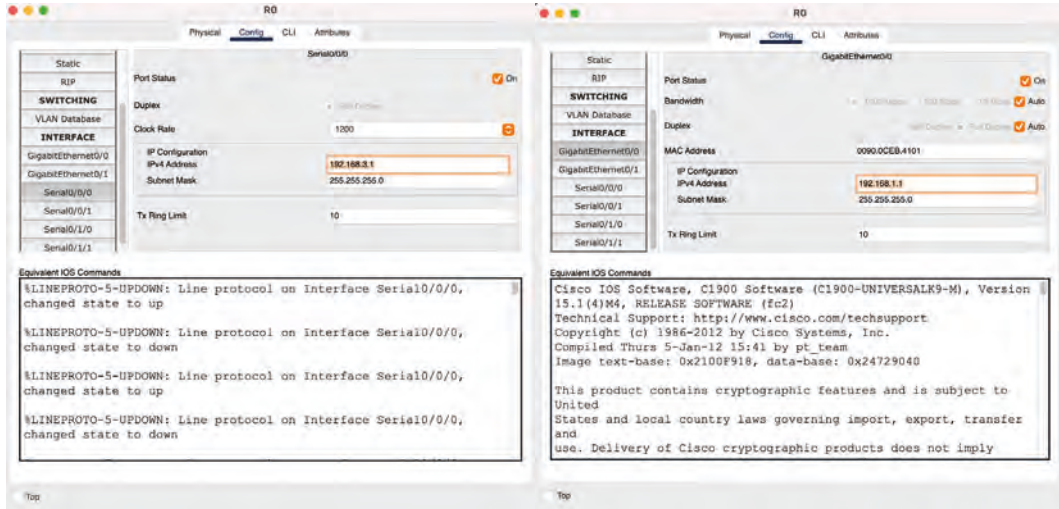
İşlem adımlarına göre Görsel 1.17’deki WAN topolojisini simülasyon programında hazırlayınız.



Görsel 1.17: WAN ağ topolojisi

1. Adım: Görsel 1.17'deki ağ topolojisini oluşturunuz. Routerlar arasındaki bağlantı için seri kablo kullanınız.

2. Adım: Görsel 1.18'deki R0 için Gig0/0/0 arayüzü (interface) ve Se0/0/0 arayüzü için IP konfigürasyon ayarlarını yapınız. Port durumunu (Port Status) On olarak ayarlayınız.



Görsel 1.18: R0 IP konfigürasyon ayarları



SIRA SİZDE

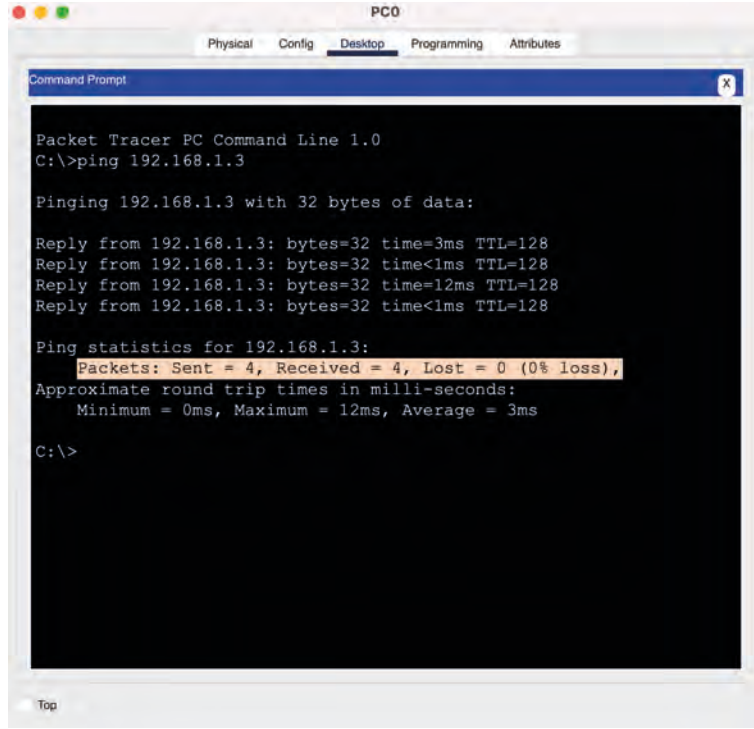
R1'de Gig0/0/0 arayüzü ve Se0/0/0 arayüzü için IP konfigürasyon ayarlarını yapınız. Port durumunu On olarak ayarlayınız.

3. Adım: LAN1'deki PC0 için IP konfigürasyon ayarlarını yapınız (Görsel 1.19).



Görsel 1.19: PC2 IP konfigürasyon ayarları

4. Adım: GUI arayüzüne girerek sırasıyla LAN1’de yer alan PC0 ve PC1 arasındaki iletişimi “ping” komutu ile doğrulayınız (Görsel 1.20).



Görsel 1.20: PC0 ile PC1 arasındaki iletişimin doğrulanması



SIRA SİZDE

LAN2’deki PC2 ve PC3 arasındaki iletişimi “ping” komutu ile doğrulayınız. LAN1’de bulunan PC’ler ile LAN2’de bulunan PC’ler arasında iletişim olmadığını “ping” komutu ile doğrulayınız. Farklı LAN’larda bulunan PC’lerin haberleşmesi için R0 ve R1 cihazlarında yapılması gereken yönlendirme konfigürasyonu ile ilgili araştırma yapınız.

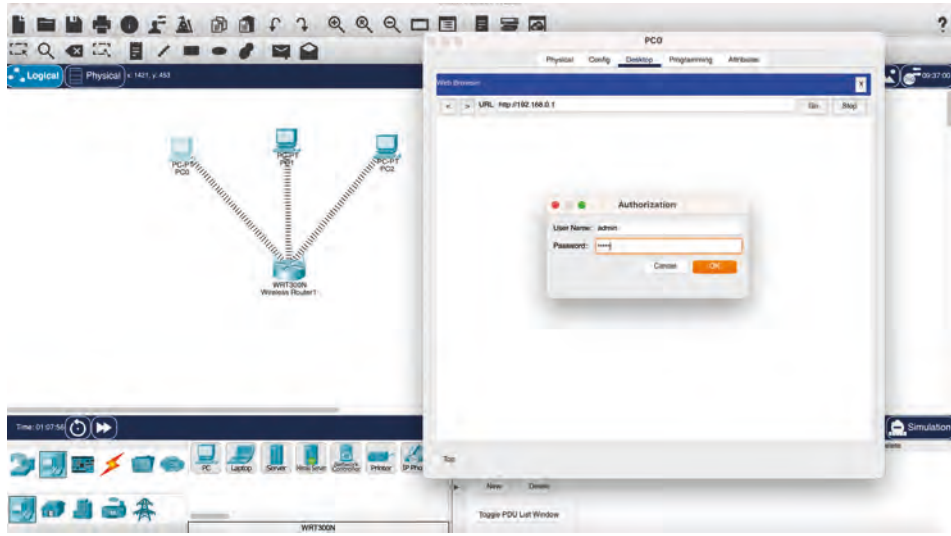
1.4. KABLOSUZ AĞ SİMÜLASYONU



3. UYGULAMA

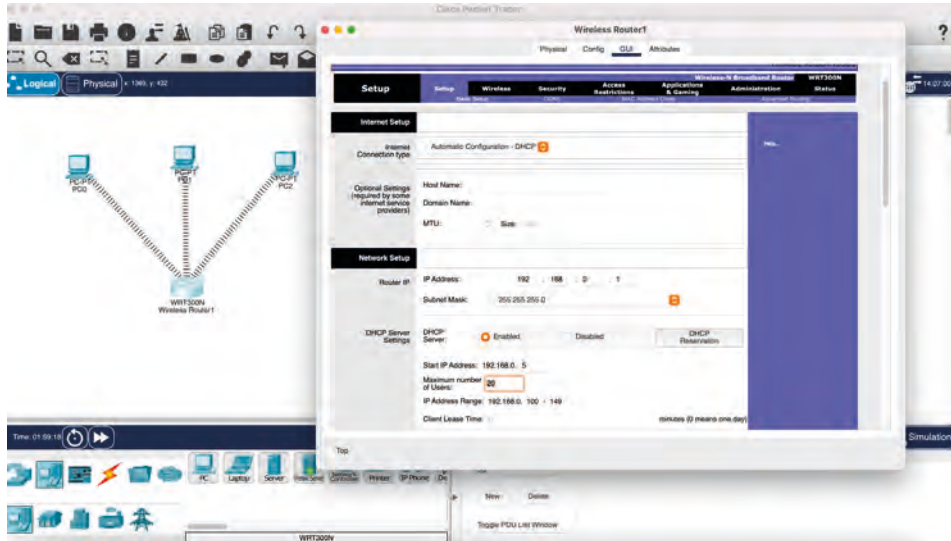
Kablosuz Ağ Simülasyonu

İşlem adımlarına göre Görsel 1.21’deki kablosuz ağ topolojisini simülasyon programında hazırlayınız.



Görsel 1.23: Kullanıcı adı ve parola doğrulaması

3. Adım: Wireless Router0'da DHCP özelliğini “enabled” seçeneğine tıklayarak aktif duruma getiriniz. DHCP adres aralığını 192.168.0.100 ile 192.168.0.149 arasında olacak şekilde ayarlayınız (Görsel 1.24). PC0 ayarlarını da DHCP’yi “enabled” seçeneğine tıklayarak aktif duruma getiriniz (Görsel 1.25).

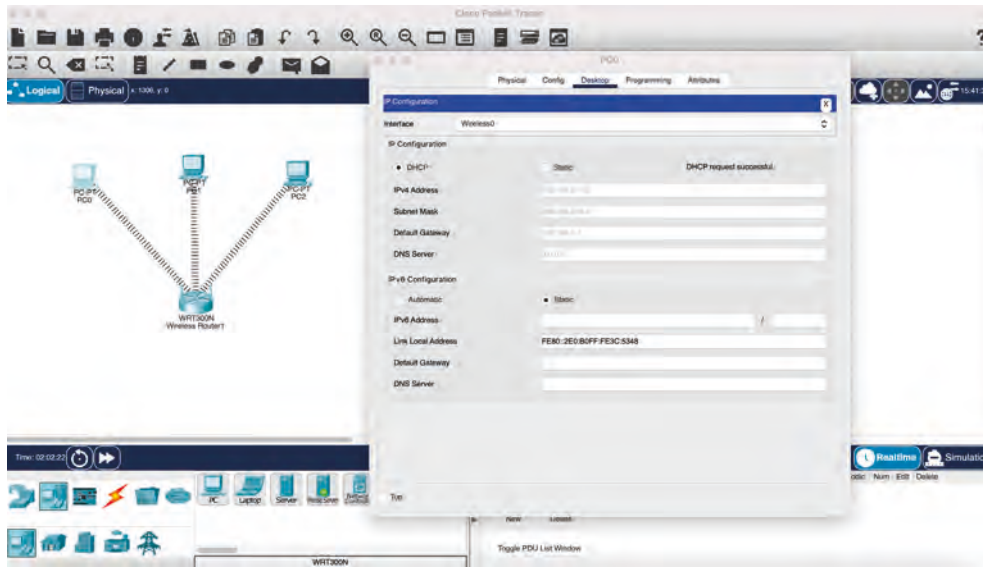


Görsel 1.24: Wireless Router0 DHCP ayarları



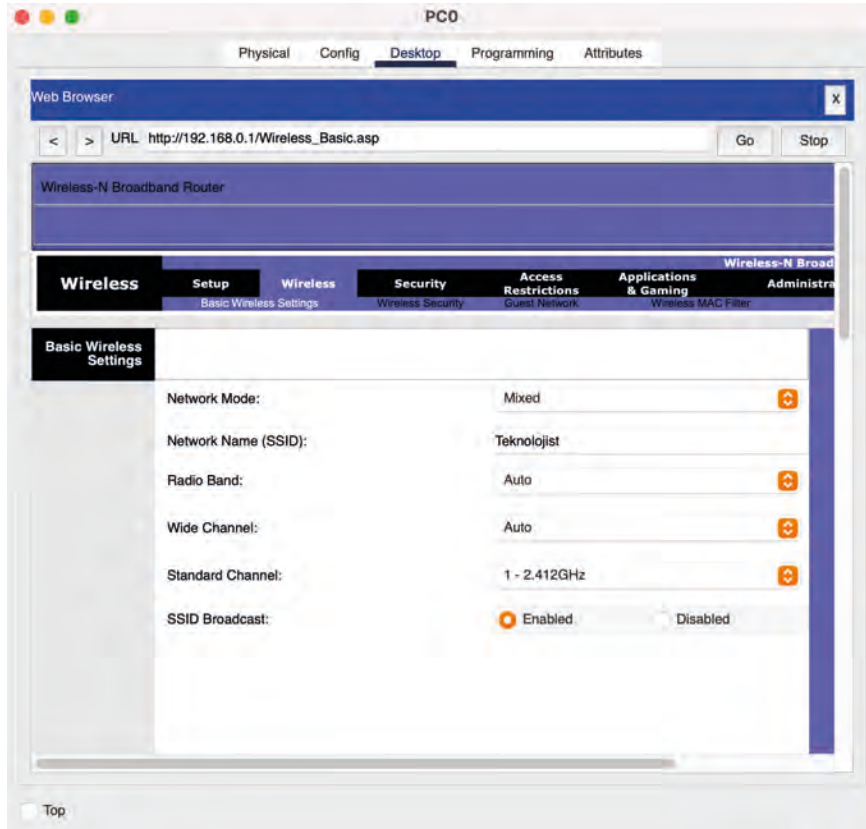
SIRA SİZDE

PC1 ve PC2 için de DHCP’yi “enabled” seçeneğine tıklayarak aktif duruma getiriniz.



Görsel 1.25: PC0 DHCP ayarları

4. Adım: PC0 için Wireless sekmesinde bulunan ayarları gerçekleştiriniz (Görsel 1.26).



Görsel 1.26: Wireless ayarları



SIRA SİZDE

PC1 ve PC2 için de Wireless sekmesinde bulunan ayarları gerçekleştiriniz.



ÖLÇME VE DEĞERLENDİRME

Aşağıdaki soruları dikkatlice okuyarak doğru seçeneği işaretleyiniz.



1.

Yukarıda verilen simgede simülasyon modu, Packet Tracer ekranının sağ alt köşesinde bulunur. Aşağıdakilerden hangisi Packet Tracer’da bu simgeyi kullanan kullanıcının yaptığı işlem-dir?

- A) Arka plan eklemek
- B) PDU’lar kullanarak bağlantıyı test etmek
- C) Yeni bir ağ tasarımı yapmak
- D) Ağ tasarımından bileşenleri silmek
- E) Geniş alan ağ oluşturmak

2. Aşağıdakilerden hangisi Packet Tracer programında bulunmaz?

- A) Sanal çalışma alanı
- B) Mantıksal çalışma alanı
- C) Simülasyon çalışma alanı
- D) Fiziksel çalışma alanı
- E) Cihazları kablolu ve kablosuz bağlama özelliği

3. Simülasyon modu ile ilgili aşağıdaki ifadelerden hangisi yanlıştır?

- A) Cihazlar arası iletişim kontrol edilir.
- B) Erişim kontrol listeleri test edilir.
- C) DNS test edilir.
- D) HTTP test edilir.
- E) FTP test edilemez.

4. Aşağıdakilerden hangisi Packet Tracer’da oluşturulabilen üç farklı dosya türüdür?

- A) .gkt, .pkz ve .pka
- B) .hkt, .pkz ve .pka
- C) .pkt, .gkz ve .fka
- D) .dkt, .pkz ve .pka
- E) .pkt, .pkz ve .pka

5. Aşağıdakilerden hangisi Packet Tracer’daki kategorilerde bulunmaz?

- A) Bileşenler (Components)
- B) Çoklu Görev (Multitasking)
- C) Bağlantılar (Connections)
- D) Uç Cihazlar (End Devices)
- E) Ağ Cihazları (Networking Devices)



KONULAR

2.1. KABLOSUZ AĞ STANDARTLARI VE BİLEŞENLERİ

2.2. KİŞİSEL ALAN AĞLARI

2.3. KABLOSUZ AĞ YAPILANDIRMASI

ANAHTAR KELİMELER

- Wireless
- Access Point
- Ad Hoc Mode
- Peer to Peer
- MAC adresi
- Şifreleme
- Güvenlik

2. ÖĞRENME BİRİMİ

KABLOSUZ AĞLAR

NELER ÖĞRENECEKSİNİZ?

- Kablosuz ağ standartları
- Kablosuz ağ bileşenleri
- Kişisel alan ağı oluşturma
- Kablosuz ağ güvenliğini sağlama
- Kablosuz ağı test etme





HAZIRLIK ÇALIŞMALARI

1. Kablosuz ağda veriler aktarılırken birbirlerine karışmadan nasıl ilerler? Düşüncelerinizi sınıf arkadaşlarınızla paylaşınız.
2. Kablosuz ağ kullanan araçlardan bildiklerinizi arkadaşlarınızla paylaşınız.

2.1. KABLOSUZ AĞ STANDARTLARI VE BİLEŞENLERİ

Verilerin bir noktadan başka bir noktaya kablo hattı kullanmadan taşınmasına kablosuz iletişim denir. Kablosuz iletişimi kablolu iletişimden ayıran önemli nokta, iletim ortamı olarak havanın kullanılmasıdır.

Heinrich Rudolph Hertz'in 1800'lü yılların radyo dalgası olarak bilinen elektromanyetik dalgaları keşfetmesiyle kablosuz ağın temeli atılmıştır.

Bugünkü ağ ve internet teknolojilerinin temeli 1950 ve 1960'larda atılmıştır. Bu yıllarda nükleer saldırılardan etkilenmeyecek bir askerî komuta kontrol sisteminin tasarlanmasına başlanmıştır. Telefon ve telgraf iletişiminin kablolu gerçekleştirildiği dönemlerde hat üzerindeki kilit noktalara verilen bir zarar, hattın iletişiminin kesilmesine yol açardı. Bu sebeple iletişimde merkezî noktaların kullanımı yerine iletişim aygıtlarının uçtan uca gerçekleşmesi düşüncesi ortaya çıktı.

Buna bağlı olarak 1969'da ABD'de The Advanced Research Projects Agency (ARPA), ABD'nin savunma sistemi için The Advanced Research Projects Agency Network (ARPANET) adında bir çalışma başlattı. İlk kablosuz bağlantı dört üniversite arasında yapıldı ve bağlanan kuruluş sayısı kısa süre içinde arttı. 1980'den sonra kablosuz olarak bağlanan kuruluş sayısı hızla çoğaldı ve günümüzde dünyayı saran bir ağ hâline geldi.

2.1.1. Kablosuz Ağ Teknolojileri

Kablosuz ağlar, iki nokta arasındaki haberleşmeyi radyo frekansları (RF) veya kızılötesi (IR) ile gerçekleştirir. Bant genişliği ve mesafe bakımından çeşitli kablosuz ağ teknolojileri vardır (Görsel 2.1).



Görsel 2.1: Wi-Fi

2.1.1.1. IrDA (Infrared Data Association)-Kızılötesi

IrDA (Infrared Data Association-Kızılötesi Veri Örgütlenmesi), kızılötesi ışınlar kullanılarak oluşturulan kablosuz ağ teknolojisidir. Bu teknolojinin en yaygın kullanıldığı yer televizyon kumandasıdır. IrDA ile cihazların haberleşebilmesi için alıcı ve verici gözlerin birbirlerini görmesi gerekir (Görsel 2.2).



Görsel 2.2: Kızılötesi

Kızılötesi; hedef tespiti, gözlemlleme, gece görüşü, ısı verimlilik analizi, uzaktan sıcaklık ölçme, kısa mesafeli kablosuz iletişim, hava tahmini gibi alanlarda da kullanılır.

IrDA ile güçlü aletlerde 2 metreye, düşük güçlü aletlerde 30 santimetreye kadar iletişim kurulabilir. Veri transfer hızı, kullanılan aletlerin türüne göre 115,2 Kbps-4 Mbps aralığında olabilir.

2.1.1.2. Bluetooth

Bluetooth, RF altyapısını kullanan bir teknolojidir. Bluetooth, kablo bağlantısını ortadan kaldıran kısa mesafe radyo frekansı (RF) teknolojisinin adıdır (Görsel 2.3). Bluetooth, 1994 yılında cep telefonları ve diğer mobil cihazları kablosuz olarak birbirine bağlamak ve aralarında iletişim kurmak için geliştirilmiştir.



Görsel 2.3: Bluetooth

Bluetooth teknolojisi; bilgisayar, çevre birimleri ve diğer cihazların birbirleriyle kablo bağlantısı olmadan alıcı ve verici aygıtlar görüş doğrultusu dışında kalsalar bile haberleşmesine olanak sağlar. Bluetooth teknolojisi, 2.4 GHz ISM frekans bandında çalışıp ses ve veri iletimi yapabilir. 24 Mbps'a kadar veri aktarabilen Bluetooth destekli cihazların etkin olduğu mesafe yaklaşık 10 ile 100 metre arasındadır.

2.1.1.3. Wireless USB

Wireless USB; yazıcılar, oyun konsolları ve tarayıcılar gibi donanımların bilgisayarla kablosuz haberleşmesini sağlayan teknolojidir (Görsel 2.4). Radyo frekanslarını kullanarak kısa mesafede ve yüksek bant genişliğinde iletişim kurar. 3 metrelik bir alanda 480 Mbps'a kadar, 10 metrelik bir alanda 110 Mbps'a kadar veri iletimine olanak sağlar.



Görsel 2.4: Wireless USB Adapter

2.1.1.4. Z-Wave

Z-Wave, akıllı ev uygulamalarında cihazların kablosuz olarak kontrolü için kullanılır. Z-Wave'in bant genişliği 960 bps-40 Kbps arasındadır ve maksimum haberleşme mesafesi 30 metre civarındır.

Z-Wave, ev otomasyonu için kullanılır. Cihazdan cihaza iletişim kurmak için düşük enerjili radyo dalgalarını kullanan bir ağıdır. Bu sistem; konut cihazları, aydınlatma kontrolü, güvenlik sistemleri, termostatlar, pencereler, kilitler, yüzme havuzları, garaj gibi diğer cihazların kablosuz kontrolüne izin verir. Z-Wave; sistemi akıllı telefon, tablet veya bilgisayar ile internet üzerinden veya yerel olarak akıllı kablosuz anahtarlık aracılığıyla kontrol edilebilir.

Z-Wave bir mesh ağıdır. Birden fazla düğüm noktası birbirine eklenerek iletim sağlanabilir. Her bir düğüm hem veri kaynağı hem de aktarıcı olarak görev yapabilir. Böylece iletilecek veri, düğümler arasında dolaşarak hedefine ulaştırılır.

2.1.1.5. ZigBee

ZigBee hem ekonomik hem de güvenli bir tür kablosuz ağ teknolojisidir. Z-Wave teknolojisinde olduğu gibi uzaktan kontrol sistemlerinde cihazlarla haberleşmeyi sağlar ve 20 Kbps ile 900 Kbps arasında bant genişliğine sahiptir. ZigBee, 10 ile 75 metre mesafe aralığında iletişim sağlar.

ZigBee de Z-Wave gibi bir mesh ağıdır. ZigBee, global standart 2.4 GHz ISM frekans bandını kullanır. Z-Wave ise 915 MHz ISM bandını (ABD'de) ve 868 MHz RFID bandını (Avrupa'da) kullanır.

2.1.1.6. Home RF

Home RF; evde bulunan bilgisayar, telefon ve diğer cihazlar arasında kablosuz haberleşme sağlayan ağ teknolojisidir. 2.4 GHz frekans bandında, en fazla 10 Mbps hızında ve 50 metre mesafeye kadar kablosuz iletişim sağlar.

2.1.1.7. Wimax

Wimax, Wi-Fi teknolojisinin çok daha büyük versiyonudur. IP tabanlı bir teknolojidir. Wimax'ın kapsama alanı sabit istasyonlarda 50 km, mobil istasyonlarda ise maksimum 15 km civarındır (Görsel 2.5). 75 Mbps bant genişliğine sahip Wimax, 4G teknolojisinin bir parçasıdır ve aynı hat üzerinden hem telefon hem internet hem de televizyon altyapısı kullanılabilir.



Görsel 2.5: Wimax

2.1.1.8. LMDS

Yerel çok noktalı dağıtım sistemi (Local Multipoint Distribution System-LMDS), dijital televizyon yayınları için tasarlanmıştır. Günümüzde ev ve iş yerleri için de kullanılan kablosuz geniş bant ağ teknolojisidir. LMDS 2,4 km mesafe ve 38 Mbps'a kadar bant genişliği sağlayabilir.

2.1.2. Kablosuz Ağ Standartları

Kablosuz ağ standartları 1997 yılından itibaren Elektrik ve Elektronik Mühendisleri Enstitüsü (Institute of Electrical and Electronics Engineers-IEEE) tarafından geliştirilmeye başlanmıştır. Geliştirilen bu standardın genel adı IEEE 802.11'dir ve ağ üzerinden iletişim kurulurken kullanılan iletişim kurallarını temsil eder.

2.4 GHz frekansında çalışan 802.11 standardı, maksimum 75 metreyi kapsar ve 1-2 Mbps aralığında veri iletimi hızı sunar. Bu standardın teknolojik gelişmeler sonucunda yetersiz hâle gelmesiyle 802.11x adı verilen standartlar serisi geliştirilmiştir. Bu standartlar, aradaki farklara rağmen temel olarak 802.11 ailesi ile aynı iletişim kurallarını kullanır. 802.11a, 802.11b, 802.11g ve yeni geliştirilen 802.11n bu standartlardan en çok tercih edilenlerdir.

2.1.2.1. 802.11a

Bu standart, 802.11 standardının zamanla yetersiz hâle gelmesiyle 1999 yılında geliştirilmiştir. 802.11a standardı 802.11 ile benzer olmasına rağmen 5 GHz frekansında çalışır. Bu standart, 54 Mbps veri iletim hızı sunar. Açık alanlarda maksimum 100 metreyi kapsayacak şekilde çalışabilir.

802.11a'yı diğer kablosuz ağ standartlarından ayıran en önemli özellik, daha fazla kapasiteye destek vermesi ve daha fazla kanal kapasitesine sahip olmasıdır. Böylelikle daha fazla bant genişliği kullanımına olanak sağlar.

Diğer standartların aksine 802.11a'nın 5 GHz frekansında çalışmasının olumlu yanı; Bluetooth, mikro-

dalga fırın ve kablosuz telefon gibi diğer elektronik cihazların farklı frekans aralığını kullandığı için kanal kapasitesinin artması ve veri iletim hızının daha yüksek olmasıdır. Bu standardın dezavantajı ise 5 GHz frekansında yapılan yayınların duvar gibi engeller tarafından daha fazla emilmesi nedeniyle 802.11a'nın kapalı alanlardaki kapsama alanının diğer standartlara göre daha düşük olmasıdır.

Bu teknoloji, yüksek veri iletim hızına ihtiyaç duyan kullanıcılar ve video dağıtım sistemleri tarafından aktif olarak kullanılır. Daha pahalı cihazlarda bulunmasına rağmen iş hayatında kurumsal kullanıcılar tarafından bu teknoloji tercih edilir.

2.1.2.2. 802.11b

Bu standart, 802.11a ile beraber 1999 yılında piyasaya sürülmüştür. 802.11a'ya göre çok daha kısa bir sürede yaygınlaşarak bütün dünyada kullanılmaya başlanmıştır. 802.11b, 802.11 gibi 2.4 GHz frekans bandında çalışır ve 11 Mbps veri iletim hızına çıkabilir. İlk çıktığında erişebildiği veri iletim hızının etkisiyle Ethernet teknolojisine rakip hâle gelmiş ve kablosuz ağ kullanımının yaygınlaşmasında büyük rol oynamıştır.

Bu standardın en önemli avantajı, kapsama alanı mesafesinin fazla olmasıdır. 2.4 GHz frekansında yayın yaptığı için kapalı alanlarda yaklaşık olarak 38 metre, açık alanlarda ise 150 metreyi aşacak şekilde bir alanı kapsayabilir. Ayrıca maliyet açısından da diğer standartlara göre oldukça uygundur.

Bluetooth teknolojisi mikrodalga fırın ve kablosuz telefon gibi farklı elektronik cihazlar ile aynı frekansa çalıştığı için işaretler birbiriyle karışır. 802.11b standardının veri iletim hızı ve bant genişliği 802.11a'ya göre daha düşüktür.

802.11b genellikle ofis, hastane, depo ve fabrika gibi ortamlarda kullanılmaya uygundur. Özellikle kablo çekmenin tehlikeli olduğu noktalarda ağ bağlantısının sağlanması için uygun bir teknolojidir. Kısaca taşınabilirliğin gerekli olduğu ve orta hızlı ağ bağlantılarına ihtiyaç duyulduğu alanlarda 802.11b standardı kullanılır.

2.1.2.3. 802.11g

Bu standart 2003 yılında geliştirilmiştir ve 2.4 GHz frekansında çalışır. 802.11b standardının bir uzantısıdır. Veri iletim hızı ve kullanılan bant genişliğinde önemli ölçüde gelişme sağlanmıştır. 802.11a ve b'nin gelişmiş özelliklerinin bir bütünü gibidir.

Bu standart, 802.11b ile çalışan cihazlarla uyum sorunu yaşadığı ve pahalı olduğu için yaygınlaşmamıştır. Veri iletim hızını ortalama 22 Mbps'a ulaştırmıştır. Maksimum ulaşabileceği hız 54 Mbps'dır. Kapasite alanının genişliği nedeniyle yüksek hız gerektiren video ve çoklu ortam uygulamalarında 802.11g standardı kullanılır.

2.1.2.4. 802.11n

Kullanıcı sayısının artması, kullanıcıların farklı uygulamaları tercih etmesi, daha fazla bant genişliği, daha fazla erişilebilirlik ve daha geniş kapsama alanı gibi ihtiyaçlardan dolayı IEEE 802.11n standardı geliştirilmiştir.

802.11n, MIMO (Multiple Input / Multiple Output) adı verilen bir protokol sayesinde 2.4 GHz ve 5 GHz frekanslarının her ikisini de aynı anda kullanabilir. MIMO, Çoklu Giriş / Çoklu Çıkış demektir.

MIMO teknolojisinde veri parçalara ayrılıp farklı antenler üzerinden karşı tarafa gönderilir ve karşı taraf da birden fazla anten ile gönderilen yayınları birleştirir. Gönderilen veriler; duvarlardan, kapılardan, diğer eşyalardan yansarak ve ayrı rotalar takip ederek alıcı antene farklı zamanlarda ulaşır. MIMO teknolojisi sayesinde sinyalin daha uzaklara iletilmesi sağlanır.

802.11n standardında veri iletim hızı yaklaşık 130 Mbps seviyesindedir. Maksimum veri iletim hızı

ise 600 Mbps'dır. Kapalı alanlarda 70 metre, açık alanlarda ise 250 metre kadar bir alanı kapsayabilir. Bu teknolojinin en önemli özelliklerinden biri de eski standartlarla uyumlu çalışabilmesidir.

802.11n henüz tamamlanmamış bir standart olmasına rağmen vadettiği veri hızı, güvenilirlik ve olması beklenen yüksek fiyatı ile internet telefonu, müzik ve video yayını, IPTV gibi daha fazla bant genişliği isteyen uygulamalar için yeterli olacaktır.

2.1.2.5. 802.11ac

802.11ac standardı sadece 5 GHz bağlantıyı destekler. 802.11ac tamamen kablolu bağlantı performansını yakalamak için yenilenmiş ve kullanılan kanalların bant aralığı artırılmıştır. En son sürümde bant aralığı 80 MHz seviyesine çıkartılmıştır. 802.11ac'de 20 MHz, 40 MHz, 80 MHz ve 160 MHz genişliğinde kanallar kullanılabilir. Bu standart teorikte 5GHz ISM bandını kullanarak uygun aygıt altyapısı ile 433 Mbps'dan maksimum 7 Gbps veri transfer hızını sağlayabilir.

802.11ac standardında MU-MIMO (Multi User-Multiple Input Multiple Output) teknolojisi kullanılır. MIMO teknolojisiyle benzer olmasına rağmen MU-MIMO teknolojinin farkı, aynı kanal üzerinden aynı anda dört istemciye kadar veri gönderebilmesidir.

5 GHz bağlantıyı desteklemesi, bu standardın kapsama alanının daralmasına sebep olur. Bu standardın diğer dezavantajı ise şu an pahalı olmasıdır. Kablosuz ağ standartları karşılaştırılması Tablo 2.1'de verilmiştir.

Tablo 2.1: Kablosuz Ağ Standartlarının Karşılaştırılması

Standart	Frekans	Maksimum Hız	Hız (Kapasite)	Kullanılan Kanal Sayısı	Maksimum Mesafe	Modülasyon Tekniği
802.11	2.4	2 Mbps	1 Mbps	12	100 m	-
802.11a	5	54 Mbps	27 Mbps	12	100 m	OFDM
802.11b	2.4	11 Mbps	5 Mbps	11	150 m	FHSS
802.11g	2.4	54 Mbps	22 Mbps	11	150 m	OFDM
802.11n	2.4-5	600 Mbps	130 Mbps	22	250 m	OFDM - DSSS
802.11y	3.7	54 Mbps	23 Mbps	12	5000 m	-
802.11ac	5	7000 Mbps	433 Mbps +	4	100 m	256-QAM

2.1.3. Kablosuz Ağ Bileşenleri

Kablosuz ağ bileşenleri; modem, Access Point (Erişim Noktası), kablosuz ağ kartı ve antendir.

2.1.3.1. Modem

Bilgisayarda bulunan verinin servis sağlayıcısı ile telefon hattı üzerinden taşınabilmesi için analog sinyale çevrilmesi gerekir. Aynı zamanda telefon hatları üzerinden gelen analog sinyalin de bilgisayarın anlayabileceği dijital sinyale çevrilmesi gerekir. Modemler, bilgisayarda kullanılan dijital verileri dağıtım ortamlarında iletebilecek analog verilere, dağıtım ortamlarından gelen analog verileri de bilgisayarda kullanılabilecek dijital verilere dönüştüren cihazlardır (Görsel 2.6).



Görsel 2.6: Modem

Modem terimi, modülatör ve demodülatör kelimelerinin birleşmesiyle ortaya çıkmıştır. İnternet hizmeti alabilmek için mutlaka modem kullanılması gerekir.

Modemler, haricî (External) ve dâhilî (Internal) olmak üzere iki sınıfa ayrılabilir.

- **Haricî (External) Modemler:** Haricî modemler bilgisayar kasasının dışında bulunur, bilgisayara kabloyla veya kablosuz bağlanır. Haricî modemlerde kasa dışında olmaları sebebiyle ısınma kaynaklı performans kaybı yaşanmaz. Haricî modemlerin ön tarafında modemin anlık durumunu gösteren ışıklar bulunur. Bu modemler herhangi bir arıza durumunda çok kolay bir şekilde sökülerek tamire götürülebilir.

- **Dâhilî (Internal) Modemler:** Dâhilî modemler, adından da anlaşılacağı gibi genellikle bilgisayar kasalarındaki slotlara takılan ve boyutları çok küçük olan modemlerdir. Kasa içinde bulunmaları sebebiyle bu modemler oldukça fazla ısınır ve bu durum, modemin performansını doğrudan etkiler. Günümüzde bu modemlerin kullanımı yok denecek kadar azdır.

Modemler kullandıkları teknolojilere göre de gruplandırılır.

- **ADSL Modemler:** Asymmetric Digital Subscriber Line (Asimetrik Sayısal Abone Hattı) olan ADSL, verilerin bakır telefon hattı üzerinden iletildiği bir teknolojidir. Bu modemler çok yüksek hızlara ulaşmaz.

- **VDSL Modemler:** Very High Data Rate DSL (Çok Yüksek Hızlı Sayısal Abone Hattı) olan VDSL, ADSL ile aynı altyapıyı kullanmasına rağmen ADSL'den çok daha gelişmiş bir ağ teknolojisidir. Bu modemler yüksek hızda internet erişimi sağlar.

- **Fiber Modemler:** Fiber teknolojisi, veri iletiminde ışığın kullanıldığı teknolojidir. Fiber kablolar, içinde yansıtıcı cam bulunan ve ışığın yansıma yoluyla karşı tarafa dijital olarak iletilmesini sağlayan kablolardır. Bant genişlikleri çok yüksek olduğu için fiber modemlerin veri iletim hızı çok yüksek seviyelere ulaşabilir. Bu modemlerin kurulum maliyetleri oldukça fazladır.

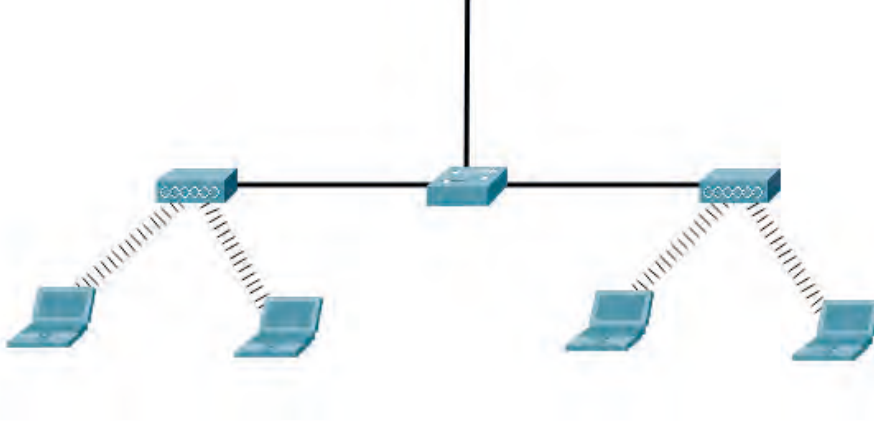
Fiber optik internet hızı 1 Gbps'dır, 50-100 Mbps kablodan 10 ile 20 kat daha hızlıdır. Aşırı yüklenmeye daha az duyarlı olduğu için yavaşlamaz. Fiber optik internet sağlayıcıları daha az sinyal kaybına ve 10 kat daha fazla bant genişliğine sahiptir.

- **Kablonet Modemler:** Kablonet modemler hâlihazırda kurulu olan kablolu televizyon altyapısını kullanır. Bu modemler, ADSL ve VDSL modemlere göre çok daha yüksek hızlarda veri alışverişi yapar.

- **Dial-up (Çevirmeli Ağ) Modemler:** Dial-up modemler günümüzde çok yaygın bir şekilde kullanılmayan modemlerdir. Bu modemler tıpkı telefonla arama gibi internet servis sağlayıcılar tarafından belirlenen numaraları çevirerek bağlantılarını gerçekleştirir.

2.1.3.2. Access Point (Erişim Noktası)

Access Point cihazı, bir kablosuz ağ düğüm noktasıdır (Görsel 2.7). Bu cihazın kullanım amaçlarına göre bazı çalışma modları vardır.

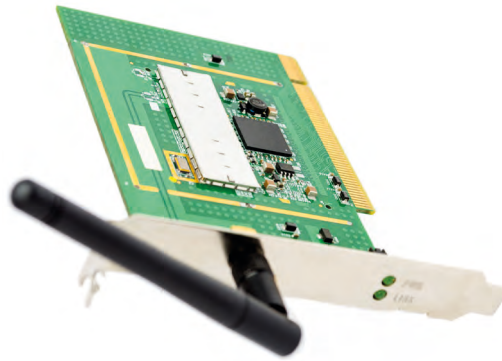


Görsel 2.7: AP Tasarım

- **Access Point Modu:** AP cihazlar bu mod ile kablolu bir internetin kablosuz bir internete dönüşümünü sağlar.
- **Repeater (Tekrarlayıcı) Modu:** AP cihazlar repeater modunda çalıştırılırsa kablosuz ağın sinyalinin tekrarlanarak daha uzak mesafelere ulaştırılmasını sağlar.
- **Client (İstemci) Modu:** AP cihazlar client modunda çalıştırılırsa kablosuz ağı kablolu bir ağıya dönüştürür.

2.1.3.3. Kablosuz Ağ Kartı

Kablosuz ağ kartları, dâhilî bir ağ kartına sahip olmayan veya kablolu bir ağ kartına sahip olan bilgisayarların kablosuz ağına dâhil olabilmesi için masaüstü bilgisayarlarda kasa içine, uygun slotu (PCMCIA, USB) bulunan dizüstü bilgisayarlarda ise bu uygun slotlara takılan kartlardır (Görsel 2.8).



Görsel 2.8: Kablosuz ağ kartı

2.1.3.4. Anten

Antenler kablosuz ağın olmazsa olmaz bileşenlerindendir. Antenler, kablosuz iletişimin sağlanması

2. ÖĞRENME BİRİMİ

amacıyla kablosuz sinyalin iletilmesi ve alınmasında görevli elemanlardır (Görsel 2.9). Antenler çoğu cihazda dâhilî olarak cihazın içinde görünmeyecek şekilde konumlandırılır ancak gerek alan darlığı gerekse sinyalin güçlendirilmesi için bazen kablosuz ağ kartlarının üzerinde bulunan çıkışlara haricî takılarak da kullanılır.



Görsel 2.9: Anten

2.1.4. Kablosuz Ağa Bağlantı



1. UYGULAMA

Cihazı Kablosuz Bir Ağa Dâhil Etme

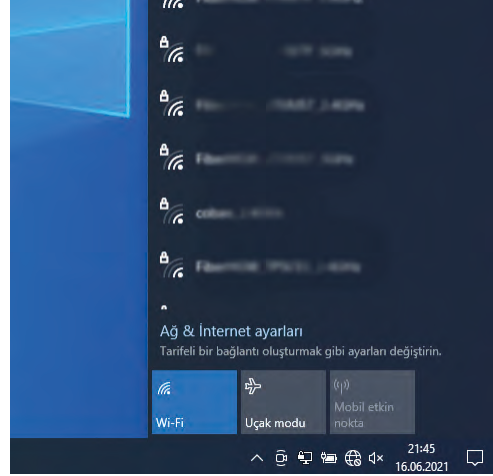
İşlem adımlarına göre cihazı kablosuz bir ağa dâhil ediniz.

1. Adım: Etraftaki kablosuz ağları taramak için bilgisayarın masaüstünde alt bölgedeki görev çubuğunun sağ tarafında bulunan simgelerden internet erişimine tıklayınız (Görsel 2.10).



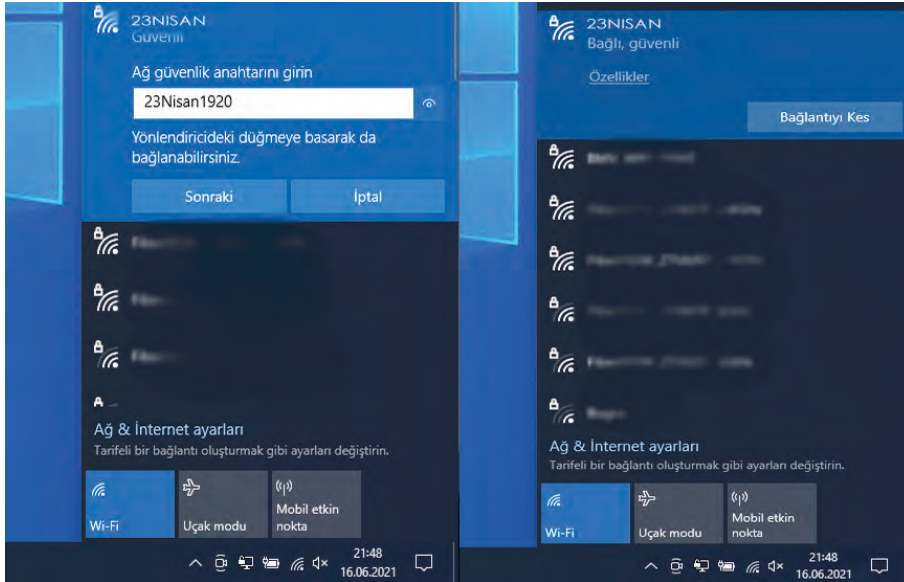
Görsel 2.10: İnternet erişimi

2. Adım: Açılan listeden dâhil olmak istediğiniz ağı seçiniz ve Bağlan tuşuna basınız (Görsel 2.11).



Görsel 2.11: Ağ & İnternet

3. Adım: Bağlanılmak istenen ağ, parola ile korunan bir ağ ise Görsel 2.12'deki gibi bir ekranla karşılaşılır. Ağ kurucusunun belirlediği parolayı işaretli kutuya girerek Sonraki tuşuna basınız ve ağa bağlanınız. Ağ parolasızsa bu ekranla karşılaşılmadan direkt bağlantı sağlanır.



Görsel 2.12: Ağ & İnternet



SIRA SİZDE

Evdeki veya okuldaki bilgisayarınızı kablosuz ağa bağlayınız.

2.1.5. Kablosuz Ağ Kanal Seçimi

İnternet servis sağlayıcısından alınan hızı kablosuz bağlantı ile en yüksek kalitede kullanabilmek için bilinmesi gereken ince ayarlardan biri, doğru Wi-Fi kanal ayarı seçimidir. Ağlarda 802.11 (ac,b,g,n) standartlarından birine sahip, 2.4 GHz ve 5 GHz bandında çalışan modem veya router cihazlar kullanılır.

Yönlendiricinin ayarlarında birden çok kanal ayarı bulunur. Çoğu yönlendiricide bu ayar “Otomatik” olarak seçilmiştir ancak listeye bakılırsa birçok Wi-Fi kanalı vardır. Uygun Wi-Fi kanalını seçmek, Wi-Fi kapsamını ve performansını önemli ölçüde artırabilir. 2.4 GHz Wi-Fi için en popüler kanallar 1, 6 ve 11’dir çünkü bu kanallar birbirleriyle çakışmaz.

5 GHz bandı 2.4 GHz bandından sonra çıktığı için 5 GHz bandının her zaman daha iyi olduğu sonucuna varılabilir ancak her iki bandın da birbirlerine göre avantajları ve dezavantajları vardır. 2.4 GHz daha uzun bir kapsama alanı sağlar ancak verileri daha düşük hızlarda iletir. 5 GHz bandı ise daha az kapsama alanı sağlar ancak verileri daha yüksek hızlarda iletir. Yüksek frekanslar, duvarlar ve ağaçlar gibi katı nesnelerden zor geçer. Bu nedenle 5 GHz bandı uzun aralıklarda veri yayınlamak için kullanışlı değildir.

Modem hem 2.4 GHz hem de 5 GHz kanal bandını aynı anda kullanmayı desteklemezse bantlar bağımsız olarak denenip en yüksek verim alınan bant tercih edilmelidir.

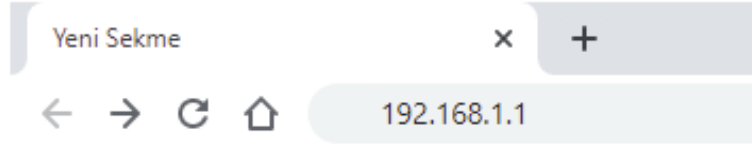


2. UYGULAMA

Kanal Seçimi

İşlem adımlarına göre kanal seçimini yapınız.

1. Adım: Öncelikle bir tarayıcı ekranı açınız. Açılan pencerede adres çubuğuna modemin yerel IP adresini yazınız ve Enter tuşuna basınız (Görsel 2.13).



Görsel 2.13: Tarayıcı

2. Adım: Açılan pencereye modem arayüzüne girmek için kullanıcı adını ve şifresini yazınız (Görsel 2.14).



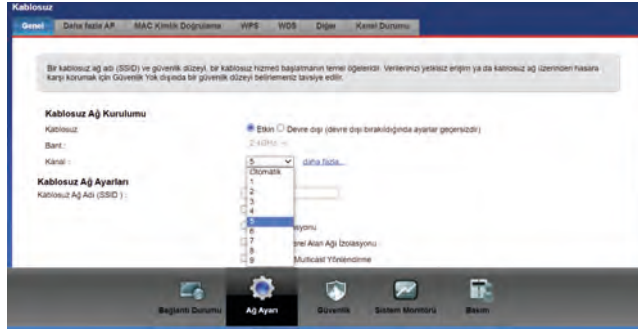
Görsel 2.14: Kullanıcı girişi

3. Adım: Açılan pencerede ağ ayarları kısmındaki Kablosuz alanına tıklayınız (Görsel 2.15).



Görsel 2.15: Bağlantı durumu

4. Adım: Karşınıza gelen penceredeki Kanal açılır düğmesinde modem desteklediği kanallar listelenecektir. Geçiş yapmak istediğiniz kanalı seçip Uygula butonuna tıklayınız (Görsel 2.16).



Görsel 2.16: Kablosuz ayarları

5. Adım: Sayfayı yeniledikten sonra modemi açıp kapatınız. Böylece yeni kanala geçilir. Kanalın performansını test ederek, size uygun olup olmadığına karar veriniz.

2.2. KİŞİSEL ALAN AĞLARI

Kişisel alan ağları; ev veya ofis gibi küçük ağlarda kullanılan bilgisayar, yazıcı, tarayıcı, hoparlör gibi çevre birimlerinin birbirlerine bağlanmasını sağlayan kablosuz ağ teknolojisidir (Görsel 2.17).



Görsel 2.17: Kişisel alan ağı

Teknolojinin ilerlemesiyle birlikte günlük yaşamda kişiler birden fazla sayıda cihaz taşırlar ve iletişim- de büyük kolaylıklara sahip olurlar. Bu cihazların birbirleriyle olan iletişimini sağlamak için ortaya çıkan PAN teknolojisi yaklaşık 10 metrelik bir alanı kapsayan, kişisel alan cihazlarının birbirlerine bağlanmasıyla oluşturulan ağı tanımlar. Örneğin saat, cep telefonu ve dizüstü bilgisayar gibi cihazlar taşıyan bir kişi, bu cihazlar arasında uygun bir veri paylaşım ağı kurduğunda basit anlamda bir PAN oluşturur.

Bir kablosuz kişisel alan ağı; IrDA, Bluetooth, kablosuz USB, Z-Wave ve ZigBee gibi kablosuz ağ tekno- lojilerini kullanabilir.

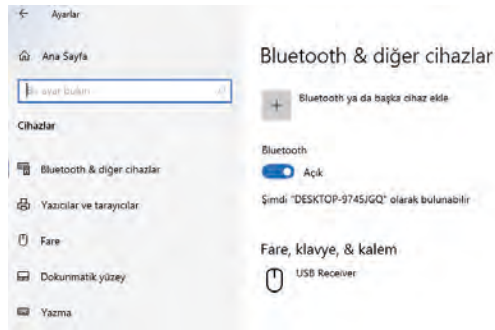


3. UYGULAMA

Kişisel Alan Ağı Oluşturma

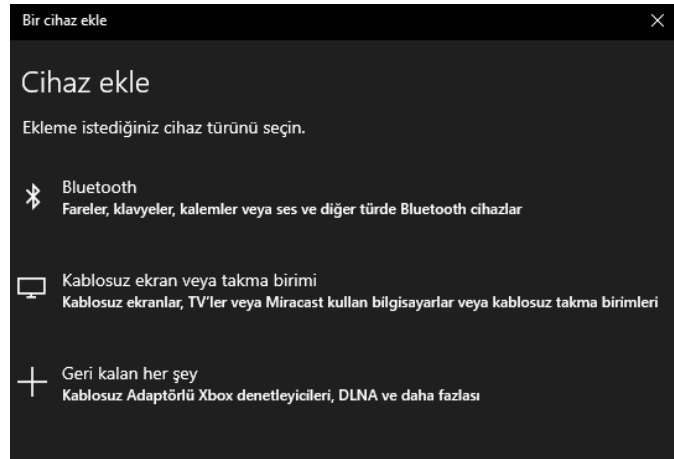
İşlem adımlarına göre kişisel alan ağı oluşturunuz.

1. Adım: Başlat menüsü > Ayarlar > Cihazlar adımlarını takip ederek Cihazlar sayfasını açınız. Açılan sayfadan Bluetooth ya da başka cihaz ekle kısmına tıklayınız (Görsel 2.18).



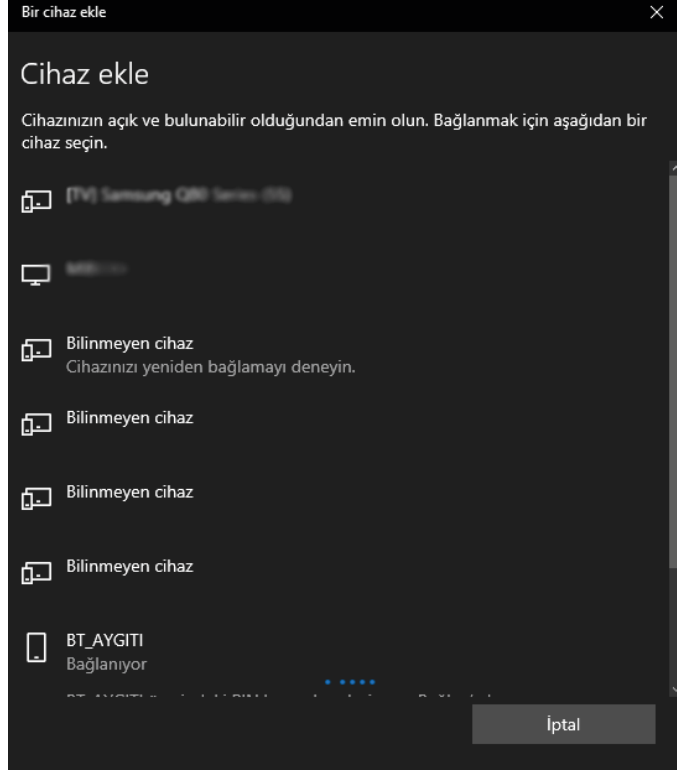
Görsel 2.18: Cihazlar

2. Adım: Açılan pencereden Bluetooth alanına tıklayınız (Görsel 2.19).



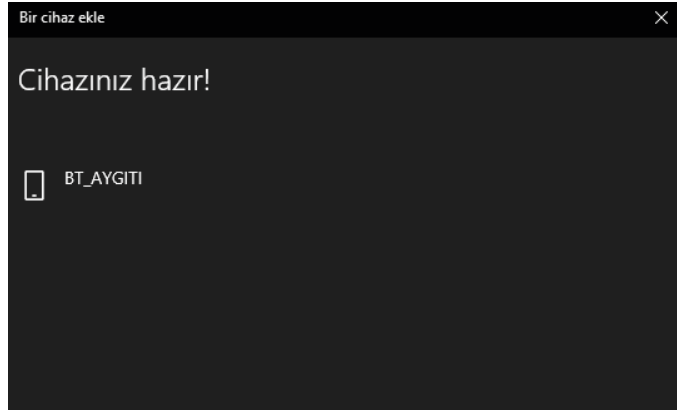
Görsel 2.19: Cihaz ekle

3. Adım: Karşınıza gelen pencerede yakındaki Bluetooth cihazları listelenir. Bağlanmak istediğiniz cihaza tıklayınız (Görsel 2.20).

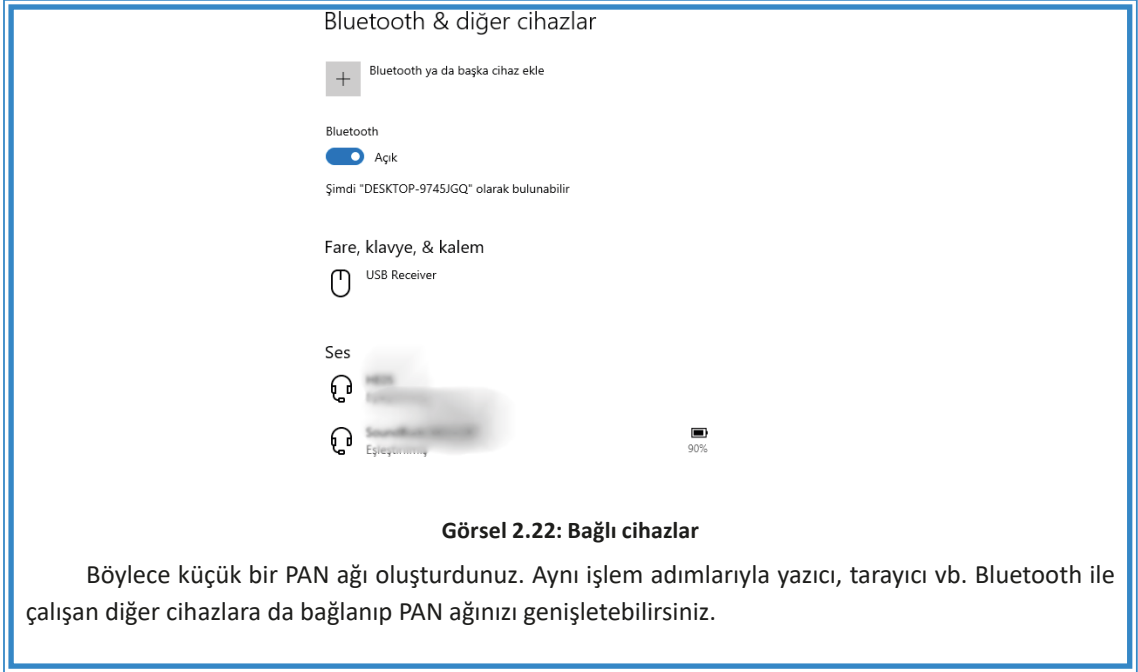


Görsel 2.20: Cihaz listesi

4. Adım: Bağlantı tamamlandı. Bitti butonuna tıklayınız (Görsel 2.21).



Görsel 2.21: Cihazınız kullanıma hazır ekranı



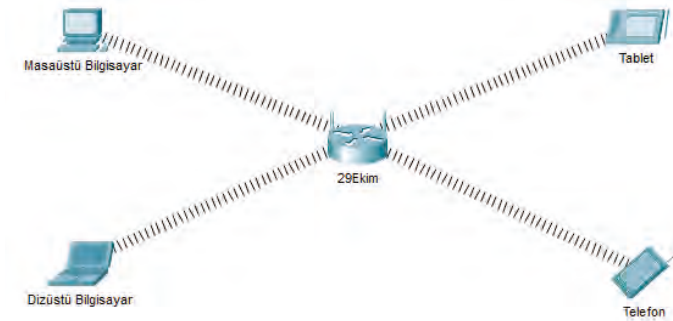
2.3. KABLOSUZ AĞ YAPILANDIRMASI

2.3.1. Kablosuz Ağ

WLAN, bir veya daha fazla cihaza merkezî bir nokta vasıtasıyla kablosuz olarak veri iletimi sağlayan bir ağ teknolojisidir (Görsel 2.23).

WLAN bağlantısına bağlanan cihazlardan bazıları şunlardır:

- Mobil cihazlar
- Dizüstü bilgisayarlar
- Tabletler
- Televizyonlar
- Ses sistemleri
- Oyun konsolları
- İnternet kullanan diğer cihazlar



Görsel 2.23: Kablosuz ağ

WLAN bağlantıları, cihazların içindeki radyo sinyali alıcı ve vericileri yardımıyla çalışır. Kablosuz ağları kullanmak için kablo yardımına ihtiyaç yoktur. Radyo sinyal alıcı ve vericileri çoğunlukla cihazın görünmeyen iç tasarımında yer alır.

2.3.2. Kablosuz Ağ Çeşitleri

Kablosuz ağ çeşitleri WPAN, WLAN, WMAN, WWAN olmak üzere dörde ayrılır.

WPAN: Kablosuz kişisel alan ağı demektir. Ara nokta olmadan cihazların kablosuz olarak birbirlerine bağlanmasıdır.

WLAN: Kablosuz yerel alan ağıdır ve bir ara düğüm cihazı bulunur. Diğer cihazlar bu ara düğüm cihazına kablosuz olarak bağlanır ve birbirleriyle haberleşir.

WMAN: Bir şehir alanında kurulan kablosuz bağlantıdır. Karşılıklı antenler vasıtasıyla kurulabilir.

WWAN: Dünya genelinde oluşturulmuş kablosuz ağ ortamıdır. Uydu üzerinden bağlantı sağlayabilir. Cep telefonları, 3G, 4.5G, TV uydu sistemleri WWAN'a örnek olarak gösterilebilir.

2.3.3. Kablosuz Ağ Yapıları

WLAN bağlantılarının Ad-Hoc veya Access Point olmak üzere iki türü vardır.

- **Wi-Fi Ad-Hoc:** Peer to Peer (Eşten Eşe) aktarım yöntemiyle gerçekleşen bağlantılardır. Bu yöntem, iletişim için bir ara noktaya ihtiyaç duymaz. Mobil cihazdan mobil cihaza Wi-Fi, Bluetooth veya kızılötesi gibi kablosuz standartlarla yapılan aktarımlar Ad-Hoc bağlantı türüne örnek olabilir. Ad-Hoc bağlantı türü az sayıda cihaz için pratik bir çözümdür ancak çok sayıda cihaz için verimi düşük bir alternatiftir.



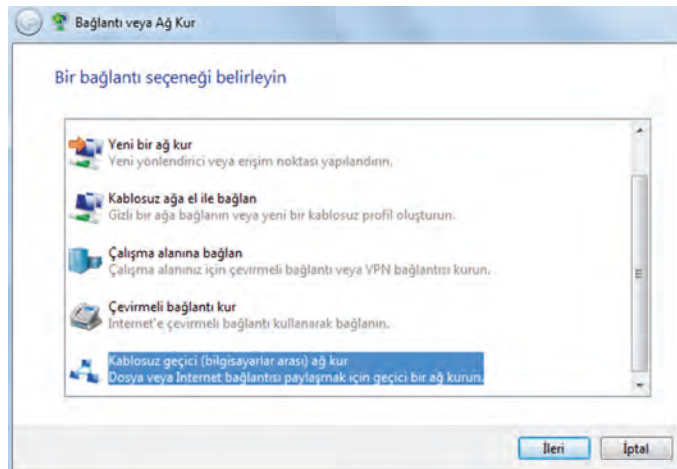
4. UYGULAMA

Eşten Eşe Bağlantı Oluşturma

İşlem adımlarına göre eşten eşe bağlantı oluşturunuz.

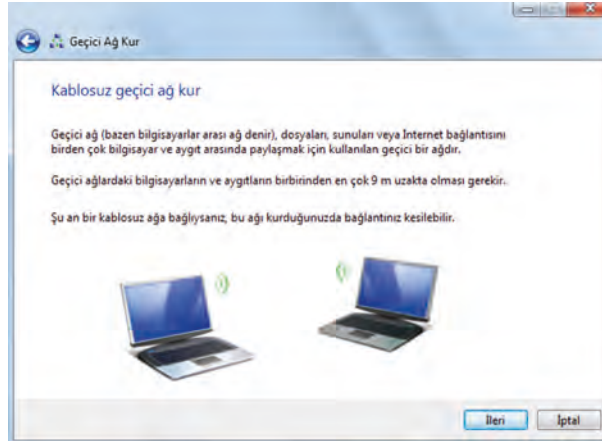
1. Adım: Denetim Masasına girerek Ağ Paylaşım Merkezini açınız ve Yeni bir bağlantı veya ağ kurun düğmesine tıklayınız.

2. Adım: Karşınıza gelen ekrandan Kablosuz geçici (bilgisayarlar arası) ağ kur seçip İleri tuşuna basınız (Görsel 2.24).



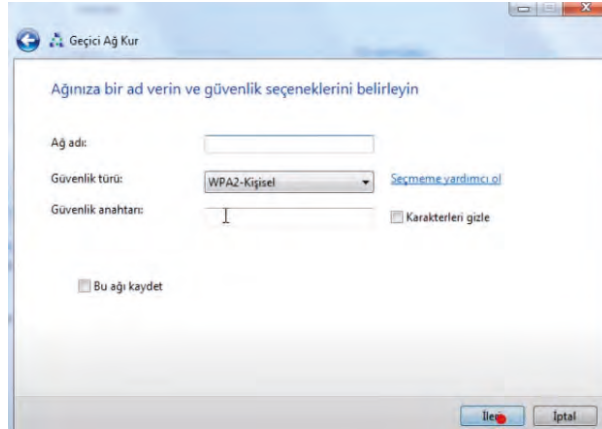
Görsel 2.24: Bağlantı veya Ağ Kur

3. Adım: Karşınıza gelen ekrandan İleri tuşuna tekrar basınız (Görsel 2.25).



Görsel 2.25: Geçici Ağ Kur

4. Adım: Ağınıza bir isim veriniz ve bir şifre belirleyiniz. İleri tuşuna bastığınızda ağı hazır. Diğer bilgisayardan ağ taraması yapıldığında kurduğunuz geçici ağ, tarama listesinde görünecektir. Artık ağa bağlanabilirsiniz (Görsel 2.26).



Görsel 2.26: Geçici Ağ Kur

Ağ Paylaşım Merkezinde geçici ağ oluşturma seçeneği yoksa aynı işlemleri Komut İstemini açarak şu komutlarla da gerçekleştirebilirsiniz:

- `netsh wlan set hostednetwork mode=allow ssid=29Ekim key=10+Kasım+&1938`
- `netsh wlan start hostednetwork`

Ağı durdurmak için şu komut kullanılabilir:

- `netsh wlan stop hostednetwork`

2.3.4. WLAN Avantaj ve Dezavantajları

WLAN'ın kullanıcılara sağladığı avantajlar şunlardır:

- Cihazlar, kapsama alanındaki herhangi bir yerden ağ kaynaklarına güvenli bir şekilde erişebilir.
- Cihazlar, sabit olmadıklarında bile ağa bağlı kalabilir.
- Ziyaretçiler için internet ve iş verilerine güvenli konuk erişimi sağlanabilir.
- Bir yerden fiziksel olarak kablo geçirmek gerekmediği için kurulum hem hızlı hem de düşük maliyetli olur.
- Herhangi bir sebeple ağ hızla genişletmek gerekebilir. Kablosuz ağlar genellikle ekstra bir ekipmana gerek kalmadan genişletilebilir.
- Genişletmeler sırasında kablolu maliyetlerini ortadan kaldırdığı veya azalttığı için bir kablosuz ağın işletim maliyeti daha düşüktür.
- Geniş bir cihaz yelpazesi tarafından desteklenir.
- WLAN ağını kurmak, kablolu ağlara kıyasla daha basittir. Deneyimsiz kullanıcılar bile basit bir router kurulumuyla WLAN ağını kullanıma hazır hâle getirebilir.
- WLAN ağlarına katılmak kolaydır. Kablonun uzunluğu veya yetişip yetişmediği gibi sorunlar yoktur.
- WLAN ağları oldukça yaygındır. Ev veya ofis dışında, kamuya açık alanlarda kullanılacak onlarca Wi-Fi noktasına bağlanılabilir.

WLAN'ın dezavantajları şunlardır:

- WLAN ağlarının kırılması kolay, bağlantı yönetiminin ve güvenliğinin sağlanması daha zordur. Bu nedenle WLAN ağları için bir şifre kullanmak şarttır.
- Kablosuz bağlantılar, kablolu bağlantılarla kıyaslandığında çoğu zaman daha düşük bağlantı hızı sunar.
- Sinyalin yetersiz kalması hâlinde ek bir Wi-Fi sinyal güçlendirici kullanmak gerekir ki bu durum ekstradan maliyet anlamına gelir.

2.3.5. Kablosuz Ağ Yapılandırması

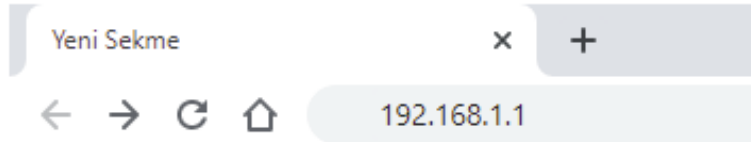


5. UYGULAMA

Modem Yapılandırması

İşlem adımlarına göre modemi yapılandırınız.

1. Adım: Tarayıcıya modem IP adresini yazınız. Gelen pencerede kullanıcı adı ve şifrenizi girerek modem arayüz sayfasını açınız (Görsel 2.27 ve Görsel 2.28).



Görsel 2.27: Tarayıcı

Görsel 2.28: Kullanıcı girişi

2. Adım: Açılan pencerede Ağ Ayarları > Kablosuz menüsünü izleyerek Kablosuz Ağ Ayarları penceresini açınız.

3. Adım: Tüm ayarları tamamladıktan sonra sayfanızda bulunan Uygula / Kaydet butonuna basarak kablosuz ağ ayarlarının uygulanmasını sağlayınız.



BİLGİ

Modemin türüne göre menü yeri değişiklik gösterebilir. Karşılaşılabilecek ekran, modem türüne göre değişse de genel hatlarıyla benzer başlıkları içerir. Bu sayfadan kablosuz ağ kapatılıp açılabilir, ağın aramalarda çıkacak ismi değiştirilebilir, ağ güvenliği yapılandırılabilir, kablosuz ağ kanal seçimi yapılabilir ve çalışma frekansı değiştirilebilir (Görsel 2.29).

Görsel 2.29: Kablosuz Ağ Kurulumu

Kablosuz ağ kurulumunda yararlanılacak bölümler şunlardır:

Kablosuz: Kablosuz ağ bu kısımdan kapatılabilir veya açılabilir. Bu kısmın devre dışı yapılması hâlinde modem sadece kablolu ağını kullanacak, kablosuz ağını kapatacaktır.

Kablosuz Ağ Adı (SSID): Bu sayfadan da anlaşılabilceği üzere kablosuz ağın aramalarda görünecek olan ismine SSID denir. Görsel 2.29’da SSID’i “29Ekim” olarak belirlenmiştir.

Bant: Modem desteklerse çalışma frekansı bu kısımdan ayarlanabilir. Görsel 2.29’daki modem yalnızca 2.4 GHz desteklediği için bu kısım kilitlidir.

Kanal: Kablosuz ağın çalışma kanalı bu alandan değiştirilebilir. Görsel 2.29'da 5 No.lu kanal kullanılmıştır. Bu kısım, otomatik seçim olarak da bırakılabilir.

Güvenlik Seviyesi: Bu alanda kablosuz ağa bir şifre belirlenebilir, kullanılacak şifrenin türü değiştirilebilir. Görsel 2.29'daki kablosuz ağa "10Kasım1938" parolası belirlenmiştir.



6. UYGULAMA

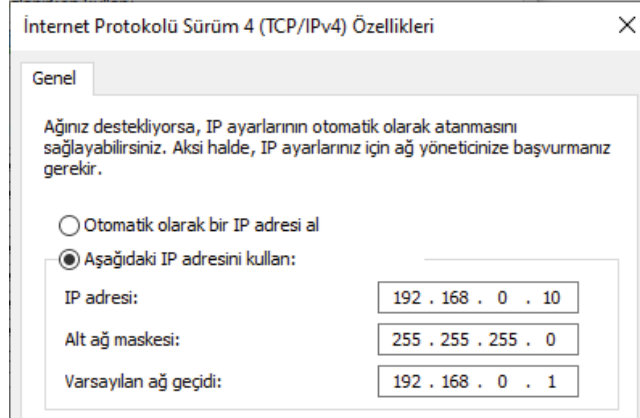
Access Point Yapılandırması

İşlem adımlarına göre Görsel 2.30'daki gibi tasarlanmış bir ağ içindeki Access Point cihazının kablo vasıtasıyla ağınıza bağlantısını sağladıktan sonra kurulumunu yapınız.



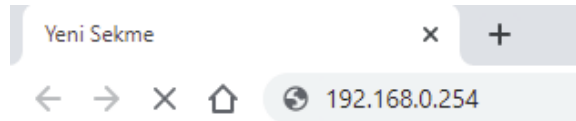
Görsel 2.30: Access Point ağı

1. Adım: AP cihazınız ile bilgisayarınız haberleşmek için aynı ağdan IP adresi almalıdır. Örnekteki AP cihazı 192.168.0.0 ağından IP verilmiş hâlde fabrika çıkışı programlanmıştır. Öncelikle Denetim Masasından Ağ Paylaşım Merkezini açarak bilgisayarınıza bu ağdan IP veriniz. Görsel 2.31'deki bilgisayara 192.168.0.10 IP'si verilmiştir.



Görsel 2.31: IPv4

2. Adım: Bir tarayıcı penceresi açarak AP cihazınızın arkasında yazan IP adresini tarayıcı adres alanına yazınız (Görsel 2.32).



Görsel 2.32: Tarayıcı adres

3. Adım: Karşınıza gelen kullanıcı adı ve şifre alanlarına yine AP cihazınızın arkasında veya kullanım kılavuzunda yazan fabrika çıkışı kullanıcı adı ve şifre bilgilerini giriniz (Görsel 2.33).

Görsel 2.33: Kullanıcı girişi

4. Adım: AP cihazınızın kurulum ekranı ana sayfasında Quick Setup kısmından hızlı ayarlar ile kurulum yapabilirsiniz. Quick Setup linkine tıklayınız ve gelen pencerede Next düğmesine basınız (Görsel 2.34).

Görsel 2.34: Hızlı ayar

5. Adım: Karşınıza AP çalışma modu seçenekleri gelir. Kablosuz ağı kablolu bir ağa çevireceğiniz için Access Point modunu seçip Next düğmesine tıklayınız (Görsel 2.35).

Görsel 2.35: Operasyon modu

6. Adım: Karşınıza gelen ekranda Wireless Network Name (SSID) kutucuğuna AP cihazınızın taramalarda görünecek ismini, Wireless Security Mode kutucuğuna ağ güvenlik türünü ve Wireless Password kutucuğuna da kablosuz ağ şifrenizi giriniz. Ardından Next butonuna tıklayıp kurulumu tamamlayınız (Görsel 2.36).

AP Mode Setting:

Wireless Network Name(SSID): 19MAYIS (also called SSID)

Region: Turkey

Warning: Ensure you select a correct country to conform local law. Incorrect settings may cause interference.

Channel: Auto

Wireless Security Mode: Most Secure(WPA/WPA2-PSK)

Wireless Password: 19+Mayis+1919

You can enter ASCII or Hexadecimal characters. For Hexadecimal, the length should be between 8 and 64 characters; for ASCII, the length should be between 8 and 64 characters. For good security it should be of ample length and should

Görsel 2.36: Mod seçenekleri



BİLGİ

Bazı AP cihazlarda işlem burada sonlanırken bazı cihazlarda bir ekranla daha karşılaşılabılır. Bu son ekranda Finish butonuna tıklanarak AP cihazının kurulumu tamamlanabilir.

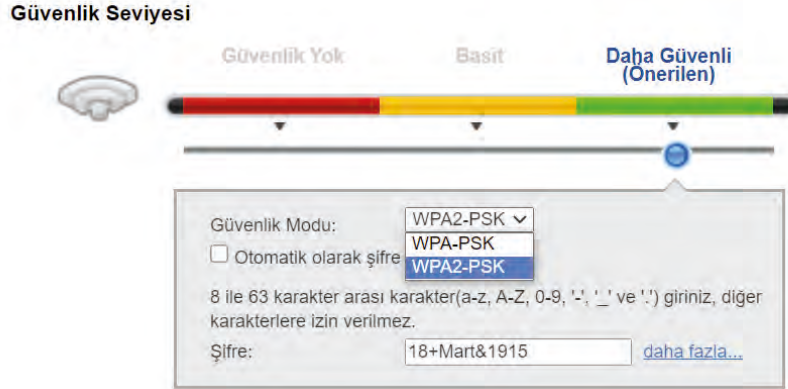
2.3.6. Kablosuz Ağ Tehditleri

Kablosuz ağlar güvenlik açısından risklidir çünkü sinyaller hava yolu ile iletildiği için genele yayılır. Kablosuz ağların maruz kaldığı güvenlik riskleri şunlardır:

- Ağın içine sızma
- Ağ trafiğinin dinlenmesi
- İstenmeyen yerlere servis verme
- Ağ topolojisinin belirlenmesi
- Kullanıcıların yetkisi dışındaki erişim noktalarına bağlanması
- Servis dışı bırakma (DoS-Denial of Service)
- MAC adres sahteciliği
- Güvenli olmayan ağa bağlama
- IP adresi yanıltma

2.3.7. Kablosuz Ağ Güvenliği

Kablosuz ağ güvenli tutmak zorunludur, aksi takdirde birçok sorunla karşılaşılabilir. Güvenlik seviyeleri Görsel 2.37’de verilmiştir.



Görsel 2.37: Güvenlik Seviyesi

7. UYGULAMA

Modem Güvenlik Ayarları

İşlem adımlarına göre modem güvenlik ayarlarını yapınız.

1. Adım: Kablosuz Ağ Ayarları menüsünü açınız. Karşınıza gelen pencerede güvenlik ile ilgili bir alan olacaktır. Örnek modemde Güvenlik Seviyesi alanından bu ayarları yapınız.

2. Adım: Pencerede bulunan Güvenlik Modu alanından kablosuz ağınız için kullanacağınız şifrenin güvenlik seviyesini belirleyiniz.

Güvenlik modu ile ilgili bilgiler şunlardır:

- **WEP (Wired Equivalent Privacy):** İlk kabul edilen güvenlik protokolüdür. 256 bite kadar şifreleme yapabilir. Çok fazla güvenlik açığı vardır ve şifreler birkaç dakika içinde kırılabilir. Bu nedenle asla kullanılması gereken bir güvenlik protokolüdür.
- **WPA (Wi-Fi Protected Access):** WEP'in bilinen açıklarını kapatarak geliştirilmiştir. 256 bit anahtar sistemini destekler. Message Integrity Checks ile paketlerin ele geçirilip geçirilmediğini anlaması en önemli özelliğidir. WEP'ten aldığı bazı kalıtlımlar yüzünden güvenlik açıkları vardır.
- **WPA2:** WPA'nın yerini resmî olarak almıştır. AES algoritmasını zorunlu kılar. CCMP ile TKIP kullanımı bırakılmıştır (WPA kullanımı için hâlen gereklidir ve aktif edilebilir.). Ev ağıları için maksimum güvenlik sağlar.

BİLGİ

Modemde WPS özelliği varsa, WPS kullanılan ağlarda güvenlik açıkları olduğu için WPS kullanılmazsa WPS devre dışı bırakıldığında maksimum güvenliğe ulaşılır. WPS, modeme şifre girilmeden cihaz eklenmesini sağlayan bir özelliktir. WPS düğmesine birkaç saniye basılı tutulduğunda o anda ağa bağlanmaya çalışan cihazlar otomatik olarak ağa dâhil edilir.

Görsel 2.37’de WPA2+PSK seçilerek en güvenli mod kullanılmıştır.



BİLGİ

Yenilenen teknoloji ile birlikte WPA3 güvenlik protokolü geliştirilmiş ve güvenlik seviyesi daha yukarılara taşınmıştır.

Güvenlik modunu belirlemek tek başına yeterli bir uygulama değildir. Buna ek olarak güçlü bir parola belirlenmesi şarttır.

Görsel 2.38’de görüldüğü gibi şifrelerin karakter uzunluğu ile kırılabilme süresi arasında bir orantı vardır. Belirlenen şifre ne kadar uzun olursa kırılma süresi de o derecede uzar.

Şifrenizin Karakter Uzunluğu	Sadece Sayı	Küçük ve Büyük Harf Karışık	Sayılar, Küçük ve Büyük Harf Karışık	Sayılar, Küçük ve Büyük Harf Karışık ve Semboller Karışık
3	Hemen	Hemen	Hemen	Hemen
4	Hemen	Hemen	Hemen	Hemen
5	Hemen	Hemen	3 Saniye	10 Saniye
6	Hemen	8 Saniye	3 Dakika	13 Dakika
7	Hemen	5 Dakika	3 Saat	17 Saat
8	Hemen	3 Saat	10 Gün	57 Gün
9	4 Saniye	4 Gün	153 Gün	12 Yıl
10	40 Saniye	169 Gün	1 Yıl	928 Yıl
11	6 Dakika	16 Yıl	106 Yıl	71 Bin Yıl
12	1 Saat	600 Yıl	6 Bin Yıl	5 Milyon Yıl
13	11 Saat	21 Bin Yıl	108 Bin Yıl	423 Milyon Yıl
14	4 Gün	778 Bin Yıl	25 Milyon Yıl	5 Milyar Yıl
15	46 Gün	28 Milyon Yıl	1 Milyar Yıl	2 Trilyon Yıl
16	1 Yıl	1 Milyar Yıl	97 Milyar Yıl	193 Trilyon Yıl
17	12 Yıl	36 Milyar Yıl	6 Trilyon Yıl	14 Katrilyon Yıl
18	126 Yıl	1 Trilyon Yıl	374 Trilyon Yıl	1 Kentrilyon Yıl

Görsel 2.38: Şifre gücü

Güçlü şifre oluşturma ilk adımı, şifrede fazla sayıda karakter kullanmaktır. Güçlü şifreler;

- En az 8 karakterden oluşmalı,
- En az bir tane büyük harf içermeli,
- En az bir tane özel karakter içermeli (ör. !^+%&/()=?),
- En az bir tane sayı içermelidir.

Kablosuz ağın güvenliğini artırmak için ayarlar penceresinde SSID gizle seçeneği işaretlenerek SSID adı gizli tutulabilir ve aramalarda çıkmaması sağlanabilir. Gizli SSID’ye sahip ağa bağlanırken aramada görünmeyeceği için ağ ismini el ile yazmak gerekir.

Kablosuz ağda en güvenli yol, MAC adres filtreleme kullanımıdır. MAC adresi, bilgisayarlardaki ağ kartlarının kendilerine özel ve benzersiz kimlik kodlarıdır.



8. UYGULAMA

MAC Adres Filtreleme

İşlem adımlarına göre MAC adresini filtreleyiniz.

1. Adım: Ağ kartının MAC adresini öğrenmek için Başlat menüsüne girip Komut İstemi yazınız. Enter tuşuna basıp, açılan Komut İstemi penceresine **ipconfig /all** komutunu yazarak ağ kartının MAC adresini öğreniniz. Komut, çıktı olarak bilgisayarınızdaki tüm kartların bilgilerini verecektir. Bu bilgiler içindeki Fiziksel Adres alanları, kartların MAC adreslerini temsil eder (Görsel 2.39).

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Version 10.0.19042.985]
(c) Microsoft Corporation. Tüm hakları saklıdır.

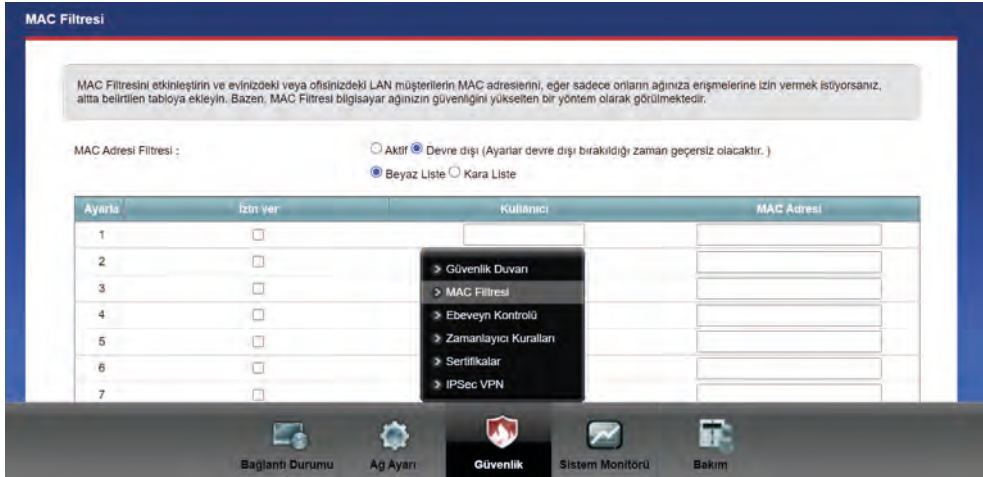
C:\Users\VOLKAN>ipconfig /all

Wireless LAN adapter Wi-Fi:

Connection-specific DNS Suffix . . . : 
Description . . . . . : Qualcomm-Atheros AR5WB222 Wireless Network
Physical Address. . . . . : 68-94-23-78-9A-7F
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::2cc7:1214:7e19:bfb8%18(Preferred)
IPv4 Address. . . . . : 192.168.1.4(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : 16 Haziran 2021 Çarşamba 22:50:29
Lease Expires . . . . . : 17 Haziran 2021 Perşembe 22:50:29
Default Gateway . . . . . : 192.168.1.1
DHCP Server . . . . . : 192.168.1.1
DHCPv6 IAID . . . . . : 90739747
DHCPv6 Client DUID. . . . . : 00-01-00-01-28-01-1E-C1-68-94-23-78-9A-7F
DNS Servers . . . . . : 8.8.8.8
```

Görsel 2.39: ipconfig

2. Adım: MAC filtreleme ayarı için kablosuz ağ ayarları sayfasında Ağ Güvenliği > MAC Filtresi menüsünü kullanarak filtreleme sayfasını açınız (Görsel 2.40).



Görsel 2.40: MAC Filtresi

3. Adım: Filtrelemenin çalışma şeklini seçtikten ve Aktif seçeneğini işaretledikten sonra Kaydet / Uygula butonuna basarak filtreyi etkin hâle getiriniz.



BİLGİ

MAC adres filtreleme işlemi iki şekilde çalışır. Bazı cihazların ağa dâhil olması istenmeyebilir ve bu engellenebilir. Ağa sadece seçilen cihazların dâhil olması istenebilir ve bu sağlanabilir. Modemin türüne göre bu listeler Beyaz Liste / İzin Ver – Kara Liste / Engelle şeklinde olabilir. Beyaz Liste / İzin Ver seçili olduğunda sadece tabloya eklenen MAC adresleri ağa dâhil olabilir, başka hiçbir cihaz ağa dâhil olamaz. Kablosuz ağın en güvenli hâli budur. Ağa yeni bir cihaz eklendiğinde bu tabloya o cihazın MAC adresinin de eklenmesi gerekliliği bu yöntemin dezavantajıdır. Kara Liste / Engelle seçili şekilde aktif edilirse tabloya eklenen MAC adreslerinin ağa dâhil olması engellenir.

2.3.8. Kablosuz Ağ Testi

Kablosuz ağa bağlanıp bağlanmadığı, ping ve ipconfig gibi komutlar kullanılarak test edilebilir.



9. UYGULAMA

Kablosuz Ağ Testi

İşlem adımlarına göre kablosuz ağ testini yapınız.

1. Adım: ipconfig komutu ile bilgisayarınızın IP'sini görünüz. Ağa sorunsuz dâhil olmuşsanız kablosuz ağ aygıtınız doğru şekilde IP alacaktır.

2. Adım: Komut İstemi'ni açarak > **ipconfig** komutunu çalıştırınız. Gelen listede Wireless LAN Adapter aygıtının IP alıp almadığını kontrol ediniz (Görsel 2.41).

```
Wireless LAN adapter Wi-Fi:

Connection-specific DNS Suffix  . : 
Link-local IPv6 Address . . . . . : fe80::2cc7:1214:7e19:bfb8%18
IPv4 Address. . . . . : 192.168.1.33
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.1.1
```

Görsel 2.41: Wi-Fi bilgileri

Diğer yöntem ise ağdaki herhangi bir bilgisayara veya modem IP adresine ping atmaktır. Komut İstemi'ni açarak > **ping 192.168.1.1** komutunu çalıştırınız ve modeme ulaşıp ulaşmadığınızı kontrol ediniz (Görsel 2.42).

```

C:\Users\VOLKAN>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
Reply from 192.168.1.1: bytes=32 time=3ms TTL=64
Reply from 192.168.1.1: bytes=32 time=2ms TTL=64

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 3ms, Average = 1ms

```

Görsel 2.42: Ping

3. Adım: Her iki yöntemle de yapılan kontrolde ağa sorunsuz bir şekilde dâhil olduğunuzu test ediniz.

2.3.9. Kablosuz Ağ Simülasyonu

Görsel 2.43'te masaüstü bilgisayarlar 30Ağustos isimli switch'e kablolü şekilde direkt bağlıdır. Packet Tracer programında ağa kablosuz olarak bir adet dizüstü bilgisayar eklenir.



Görsel 2.43: Packet Tracer

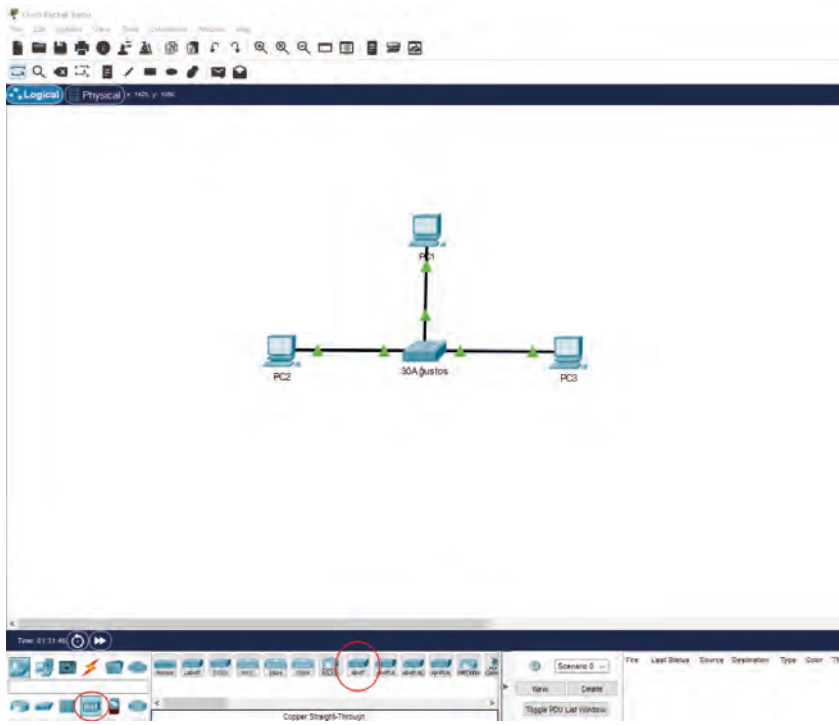


10. UYGULAMA

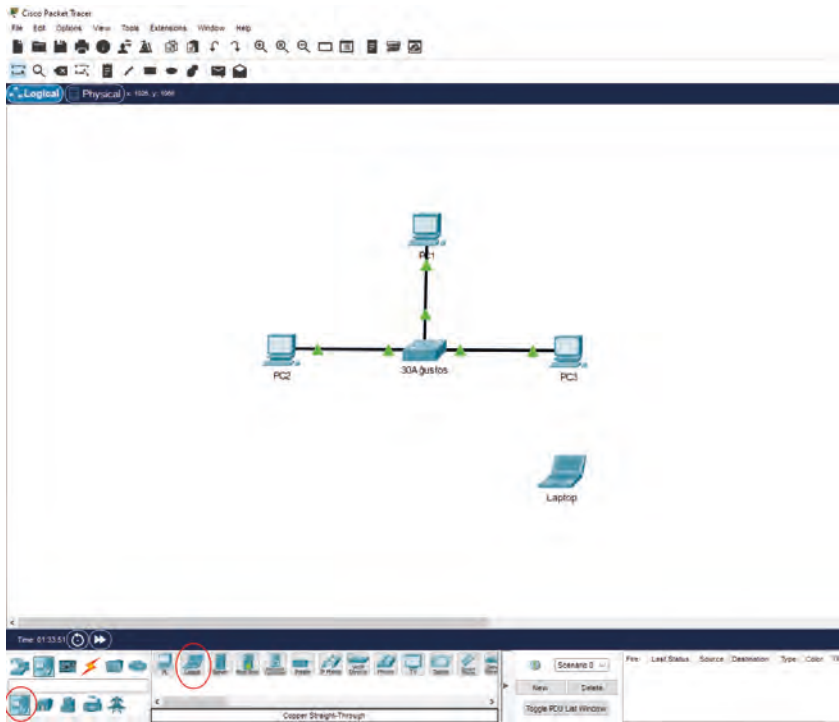
Kablosuz Ağ Simülasyonu Oluşturma

İşlem adımlarına göre kablosuz ağ simülasyonu oluşturunuz.

1. Adım: Görsel 2.43'teki Wireless Devices ve Görsel 2.44'teki End Devices alanlarını kullanarak senaryoya bir adet Access Point ve bir adet laptopu sürükleyip bırak yöntemi ile ekleyiniz.

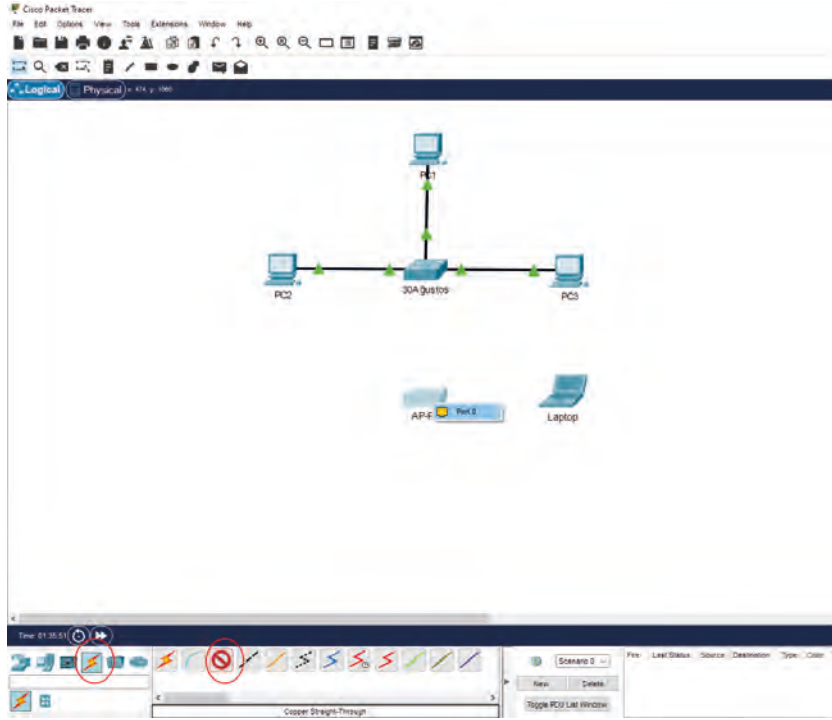


Görsel 2.44: Devices ekranı

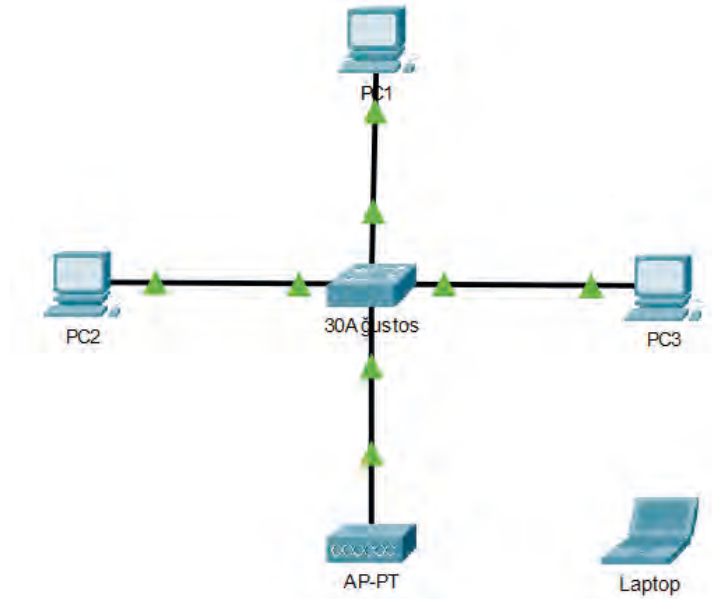


Görsel 2.45: Son kullanıcı cihazları

2. Adım: Görsel 2.46'da görüldüğü gibi kablolar kısmından düz kabloyu seçerek AP-1453 Access Point cihazının Port 0 portunu 30Ağustos switchinin herhangi bir portuna bağlayınız. Görsel 2.47'deki görüntüyü elde ediniz.

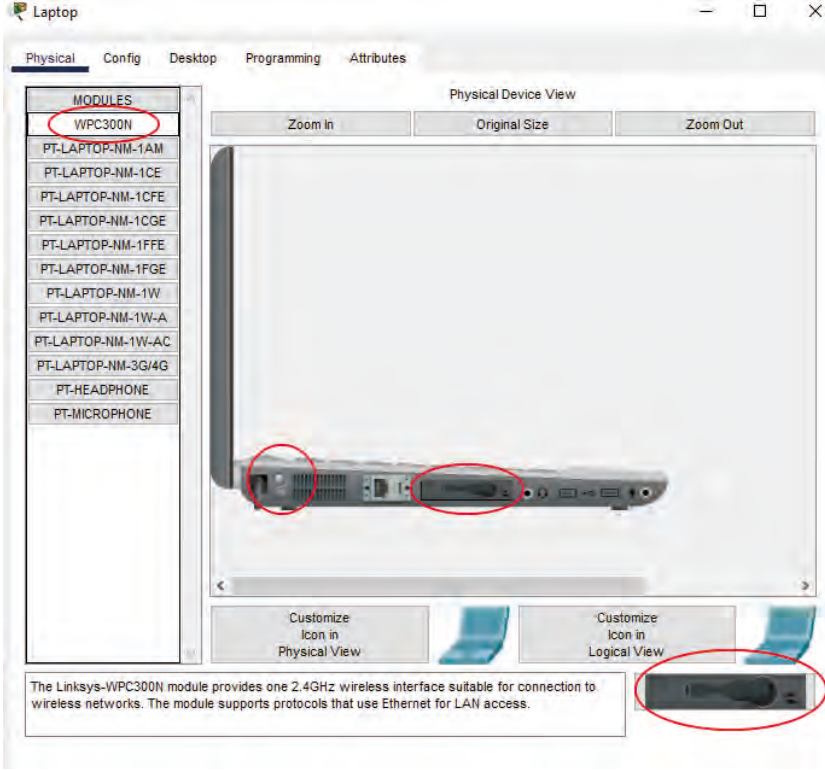


Görsel 2.46: Kablolar



Görsel 2.47: AP ekleme

3. Adım: Senaryoya eklediğiniz laptop bilgisayara sol tuş ile tıklayıp açılan Görşel 2.48'deki pencereden WPC300N aygıtını seçiniz. Daha sonra 1 No.lu alandan laptopu kapatıp 2 No.lu alandaki aygıtı 3 No.lu alana sürükleyiniz ve tekrar 1 No.lu alana tıklayarak laptopu çalıştırınız.



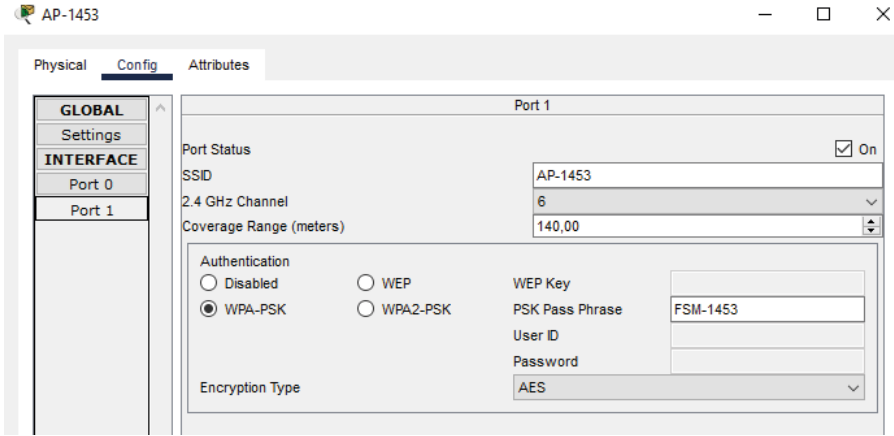
Görşel 2.48: Modül ekleme

4. Adım: AP-PT isimli Access Point cihazına tıklayıp, açılan Görşel 2.49'daki pencereden Config sekmesine gelerek Port 1 alanına basınız. Burada SSID kısmına AP-1453 yazınız. Authentication alanından şifreleme türünü WPA-PSK seçiniz. Şifre olarak FSM-1453 yazınız.



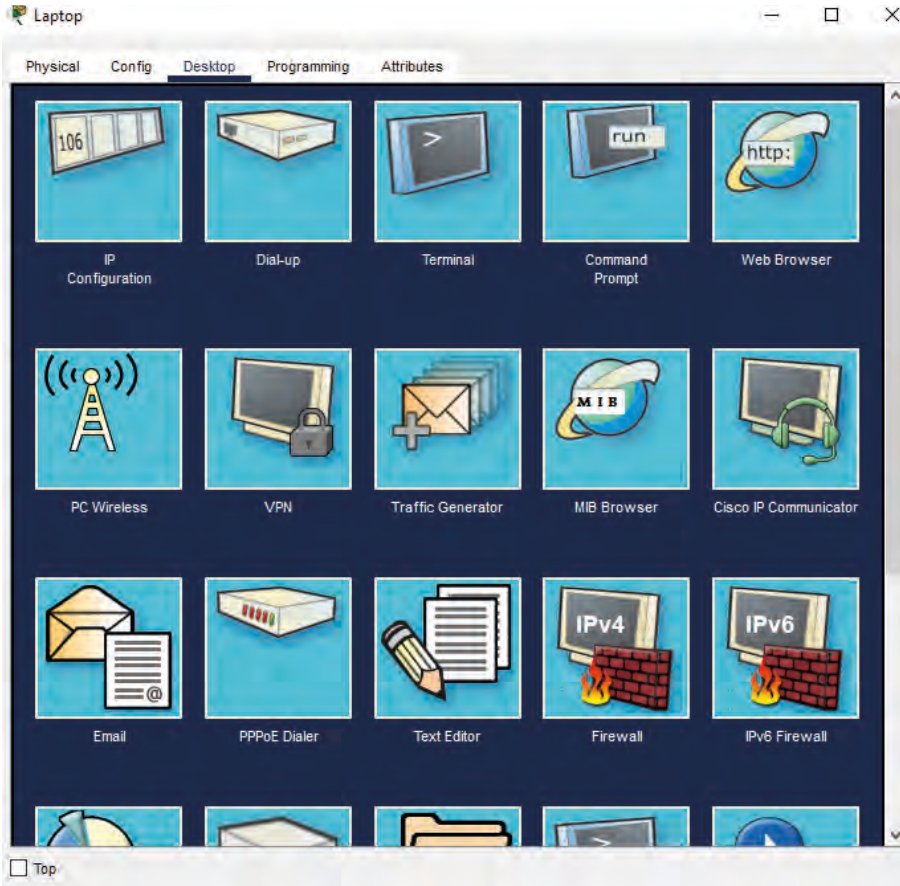
BİLGİ

Aynı pencerenin global>settings alanından AP cihazının adı AP-1453 yapılabilir.



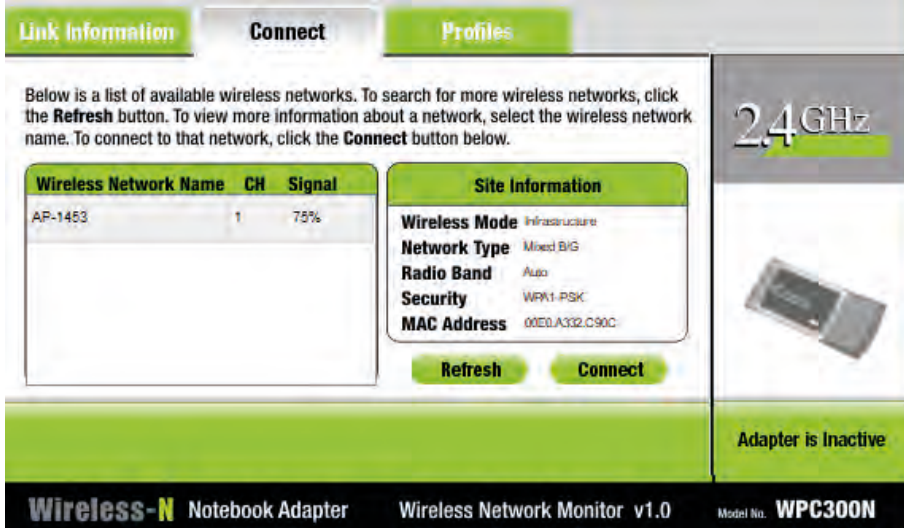
Görsel 2.49: AP ayarları

5. Adım: Laptop cihazına tıklayarak açılan pencerede üst taraftaki Desktop sekmesine geçiniz ve PC Wireless uygulamasını çalıştırınız (Görsel 2.50).



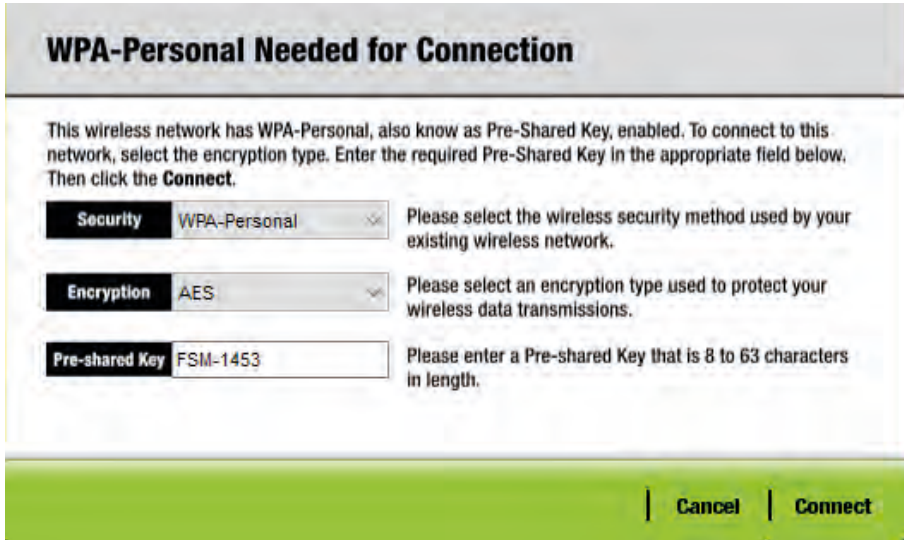
Görsel 2.50: Desktop

6. Adım: Açılan pencereden Connect sekmesine geçiniz ve Refresh butonuna basınız. Biraz beklediğinizde laptop cihazınız AP-1453 kablosuz ağını bulacaktır. Ardından Connect tuşuna basınız (Görsel 2.51).

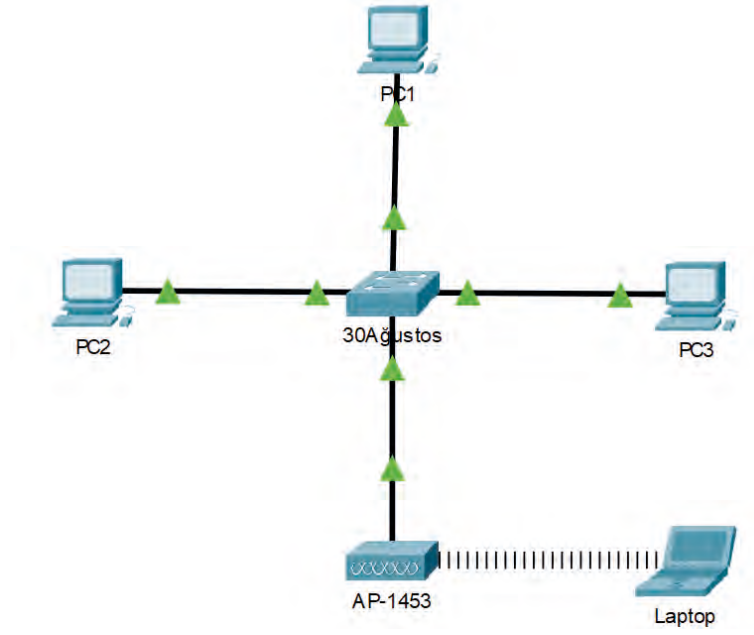


Görsel 2.51: Wireless bağlantı

7. Adım: Karşınıza gelen Görsel 2.52'deki pencereden Pre-shared Key alanına belirlediğiniz FSM-1453 şifresini girerek Connect butonuna basınız. Artık laptop bilgisayarınızı kablosuz ağa dâhil ettiniz (Görsel 2.53).



Görsel 2.52: Şifre ekranı



Görsel 2.53: Kablosuz ağ simülasyonu



Aşağıdaki soruları dikkatlice okuyarak doğru seçeneği işaretleyiniz.

1. Aşağıdakilerden hangisi kablosuz ağın bileşenleri arasında yoktur?

- A) Modem
- B) Access Point
- C) Anten
- D) Switch
- E) Kablosuz ağ kartı

2. Aşağıdakilerden hangisi en hızlı standarttır?

- A) 802.11b
- B) 802.11ac
- C) 802.11n
- D) 802.11g
- E) 802.11

3. Aşağıdakilerden hangisi kişisel alan ağında yer almaz?

- A) Yazıcı
- B) Kulaklık
- C) Bağlantı kablosu
- D) Bilgisayar
- E) Saat

4. Ağda bir bilgisayara bağlantının olup olmadığı aşağıdaki hangi komutla kontrol edilebilir?

- A) Control
- B) Show
- C) Connect
- D) Test
- E) Ping

5. Aşağıdakilerden hangisi kablosuz ağ güvenlik yöntemlerinden en iyisidir?

- A) WEP
- B) WPA
- C) MAC Filtreleme
- D) WPA2
- E) WPA3



KONULAR

- 3.1. YÖNLENDİRİCİLERİN YAPISI VE BAĞLANTILARI
- 3.2. KOMUT ARAYÜZÜ KULLANARAK KULLANICI GİRİŞİ
- 3.3. TEMEL YÖNLENDİRİCİ TANIMLAMALARI
- 3.4. ARAYÜZ YAPILANDIRMA

ANAHTAR KELİMELER

- Interface
- Router
- TFTP Server
- Kullanıcı Modu
- Privilege
- IOS
- ROM
- Flash
- NVRAM
- Seri Port
- Ethernet
- Fast Ethernet
- Gigabit Ethernet

3. ÖĞRENME BİRİMİ

YÖNLENDİRİCİLER

NELER ÖĞRENECEKSİNİZ?

- Yönlendiricilerin ethernet, seri ve konsol bağlantılarını yapma
- Terminal programını kullanma
- Yönlendirici cihaza uzaktan bağlanma
- Kullanıcı modları arasında geçiş yapma
- Yönlendirici yardım komutlarını kullanma
- Yönlendirici temel yapılandırma işlemleri
- Yönlendirici komutlarını kullanarak arayüzleri yapılandırma





HAZIRLIK ÇALIŞMALARI

1. Yönlendirici cihazlar ile bilgisayarların çalışması arasında nasıl bir bağ kurulabilir? Düşüncelerinizi sınıfta arkadaşlarınızla paylaşınız.
2. Yönlendirici cihazlarda ağ genişledikçe fiziki nasıl değişiklikler olabilir? Araştırıp sınıfta arkadaşlarınızla paylaşınız.
3. Yönlendirici cihazlarda şifreleme ve kullanıcı yetkilendirmesi yapılmazsa ne gibi problemler ortaya çıkabilir? Düşüncelerinizi sınıfta arkadaşlarınızla paylaşınız.

3.1. YÖNLENDİRİCİLERİN YAPISI VE BAĞLANTILARI

Yönlendiriciler, ağ trafiğinin iletilmesi gereken en iyi yolu belirlemek üzere bir veya daha fazla ölçeği kullanan ve OSI modelinin 3. katmanında “Network (Ağ) katmanı” kullanılan ağ cihazlarıdır. Yönlendiriciler, Network katmanı bilgilerine göre paketleri bir ağdan diğerine iletir. Yönlendiriciler, kendi işletim sistemlerine sahiptir. Dolayısıyla yönlendiriciler programlanabilir ve gerekli yapılandırma işlemleri gerçekleştirildiğinde uzak bir ağa erişmek için mevcut birden fazla yol arasında kullanılacak en iyi yolun seçimini yapabilir. Bu işleme Best Path Determination (En İyi Yolu Belirlenmesi) adı verilir.

Yönlendirici, cihaz yapısı gereği fiziksel olarak üzerinde çeşitli arayüzleri bulundurur. Yönlendirici cihaz, içeriğinde bir işletim sistemi barındırır. İşletim sistemi ise çeşitli bileşenler yardımıyla çalışarak yönlendirme işlemini gerçekleştirir. Yönlendirici işletim sistemi (IOS), kullanıcıya komut arayüzü (CLI) sayesinde yönlendirici cihazı yönetme imkânı verir.

3.1.1. Yönlendirici Bileşenleri

RAM (Random Access Memory): Yönlendirici cihazın üzerinde o an çalışan konfigürasyon dosyalarının tutulduğu bellek birimidir. Yönlendiricinin çalıştığı andaki konfigürasyonuna **running-config** adı verilir. Yönlendirici cihaz yeniden başlatıldığında veya kapatıldığında RAM bellek üzerinde tutulan bilgiler silinir.

ROM (Read Only Memory): ROM, silinemeyen ve değiştirilemeyen sadece okunabilir bellek türüdür. Yönlendirici üzerinde bulunan ROM bellek, yönlendiriciyi başlatmaya yarayan “bootstrap” dosyasını içerir. ROM belleğin birçok bileşeni vardır. Bu bileşenler şöyle sıralanabilir:

- **Bootstrap:** Yönlendirici cihazın çalıştırılmasını sağlayan yazılımı içerir.
- **Post:** Yönlendirici cihaz başlatıldığında devreye giren ekrandır. Yönlendiricinin donanım testini gerçekleştirir.
- **ROM Monitör:** Yönlendirici cihazın BIOS’u gibidir. Düşük seviye hata ayıklama işlemleri için kullanılır.
- **MinIOS:** Yönlendirici işletim sisteminde bir sorun meydana geldiği takdirde sorunları çözebilecek kadar sistemin çalışmasını sağlayan bölümdür.
- **Flash:** Yönlendirici işletim sisteminin bulunduğu hafıza birimidir. Flash hafıza; silinebilir, değiştirilebilir veya yeniden yüklenebilir bir hafıza türüdür.
- **NVRAM:** Kalıcı ve silinemez RAM türüdür. Başlangıç yapılandırma dosyaları NVRAM üzerinde tutulur. Startup-config denilen başlangıç yapılandırma dosyalarının yönlendirici cihaz açıldığında RAM üzerinde çalışmasını sağlar.
- **CPU:** Yönlendirici cihazın işlemcisidir. Yönlendirme işleminin gerçekleşmesi için gerekli adımları

ve ağ arayüzleri kontrol eden birimdir.

• **INTERFACES:** Yönlendirici cihaza erişmek veya fiziksel olarak bağlantılar yapmak için kullanılan arabirimdir. Yönlendirici cihazlarda **Seri arayüz** ve **Ethernet arayüzü** olmak üzere iki şekilde karşılaşırlar.



ARAŞTIRMA

Yönlendirici işletim sistemi zarar gördüğünde nasıl bir yol izlenir? Araştırarak sınıfta arkadaşlarınızla paylaşınız.

3.1.2. Yönlendirici Arayüz Bağlantıları

Yönlendirici cihaz komut arayüzüne ulaşmak için çeşitli yöntemler kullanılır. Bu yöntemler;

- Konsol portu bağlantısı,
- TELNET bağlantısı,
- Aux port bağlantısıdır.

Yönlendirici cihaza TELNET yöntemiyle uzaktan bağlanılabildiği gibi Aux portu aracılığı ile modem kullanılarak da erişim sağlanabilir. Konsol portu ile bağlantı en çok tercih edilen fiziksel bağlantı yöntemidir. Konsol portu ile bağlanılan yönlendirici cihazda başlangıç bilgileri, hatalar ve ayarlar görülür.

3.1.2.1. Yönlendirici Konsol Bağlantısı

Yönlendirici konsol bağlantısı, bilgisayarın komut istemcisi aracılığıyla yönlendiricilerin yapılandırılması için kullanılır. Yönlendiricilerin ilk yapılandırılması konsol kabloları aracılığıyla yapılabilir. Bu arayüzün veri iletim hızı 9600 bps'dir. Rollover kablo hazırlamak için UTP kablonun bir ucu T586B standardına göre sıralandıysa diğer ucu T586B'nin tersine göre sıralanmalıdır. Konsol kablosunun bilgisayara bağlanacak ucu da seri porta veya USB portuna çevrilmelidir (Görsel 3.1).



Görsel 3.1: Konsol kablosu ve dönüştürücü



1. UYGULAMA

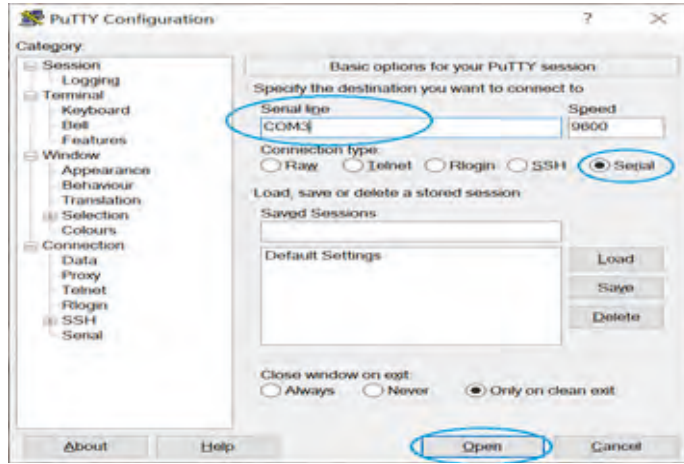
Yönlendirici Yapılandırma Ekranını Açma

İşlem adımlarına göre yönlendiriciyi yapılandırınız.

1. Adım: Yönlendiricinin konsol (Console) portuna konsol kablosunun RJ-45 konnektör ucunu bağlayınız.

2. Adım: Bilgisayarın varsa doğrudan serial portuna, yoksa dönüştürücü ile USB portuna konsol kablosunun diğer ucunu bağlayınız.

3. Adım: Bilgisayar üzerinde Putty programını açınız (Görsel 3.2).



Görsel 3.2: Putty programı

4. Adım: Karşınıza gelen ekrandan **Connection Type** seçeneğini **Serial** olarak seçiniz.

5. Adım: **Serial line** alanına bilgisayarınızda tanımlı **serial com** portu yazıp **Open** tıklayınız.



2. UYGULAMA

Ağ Simülasyon Yazılımında Yönlendirici Yapılandırma Ekranını Açma

İşlem adımlarına göre ağ simülasyon programında yönlendiriciyi yapılandırınız.

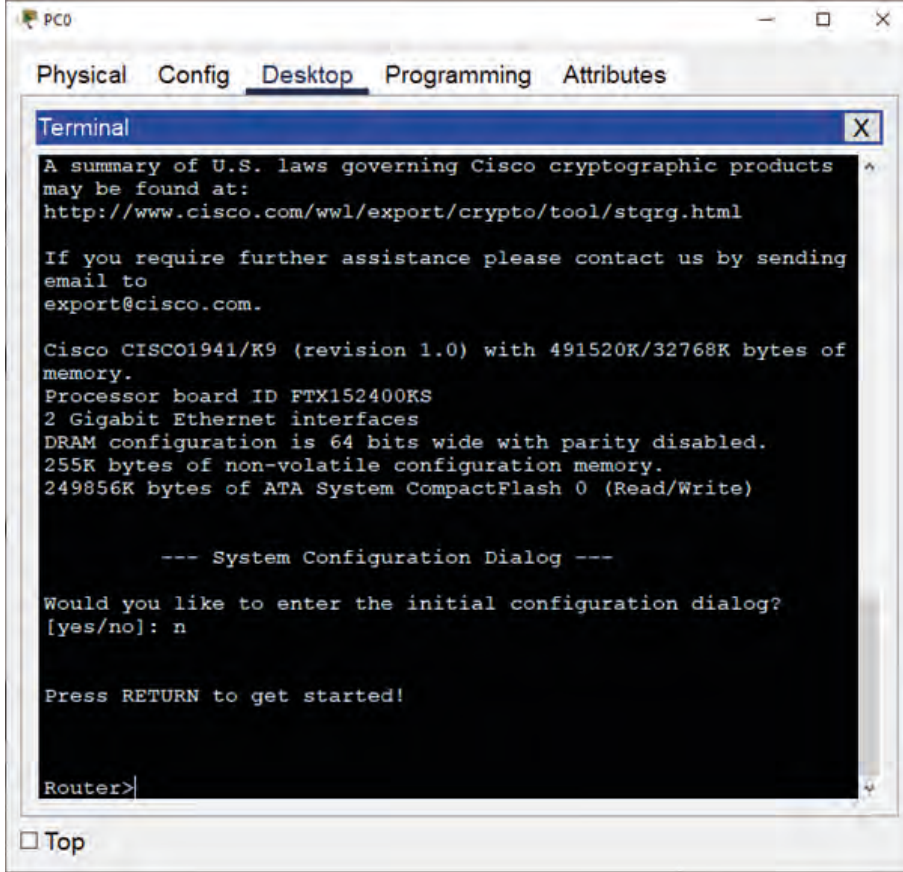
1. Adım: Ağ simülasyon programını açınız.

2. Adım: Simülasyon ortamına bir yönlendirici ve bir bilgisayar ekleyiniz (Görsel 3.3).



Görsel 3.3: Yönlendiricinin konsol kablosu ile bağlantısı

3. Adım: Kablo türü olarak konsol kablosunu seçiniz.
4. Adım: Bilgisayarın RS232 ve yönlendiricinin **Console** portunu seçerek bağlantıyı oluşturunuz.
5. Adım: Bilgisayarı tıklayınız ve açılan ekrandan Terminal programını tıklayınız.
6. Adım: Karşınıza gelen ekrandan **OK** tıklayınız ve komut arabirimini açınız (Görsel 3.4).



Görsel 3.4: Yönlendirici komut arabirim ekranı (CLI)

3.1.2.2. Yönlendirici Seri ve Fast Ethernet Arayüz Bağlantıları

Yönlendirici cihazların birçok arayüzü vardır. Bu arayüzlerin bazıları yönlendirici cihazla beraber temel olarak gelebilir bazıları ise sonradan modül şeklinde cihaza eklenebilir. Yönlendirici cihazların arayüzleri ağın ihtiyacına göre modüller eklenerek genişletilebilir.

Yönlendirici cihazda WAN ve LAN olmak üzere iki temel ağ konfigürasyonu yapılır. WAN bağlantılarında yönlendiricinin serial port denilen seri portları kullanılır (Görsel 3.5). Serial0, Serial1 gibi isimler alan seri portlar DTE veya DCE olarak yapılandırılabilir. Arayüzü DCE olarak yapılandırılan yönlendirici cihaz, arayüzü DTE olan yönlendirici cihaza **clock rate** sağlar. Yönlendirici cihazların yerel ağ (LAN) bağlantılarında ise Ethernet, Fast Ethernet veya Gigabit Ethernet arayüzleri kullanılır.



Görsel 3.5: Yönlendirici seri arayüzleri



3. UYGULAMA

Yönlendiricinin Seri Arayüz Bağlantısını Yapma

İşlem adımlarına göre ağ simülasyon programında yönlendiricinin fiziksel yapılandırma bağlantısını yapınız. Görsel 3.6'daki topolojiyi ağ simülasyon programında hazırlayarak seri kablolar yardımıyla topolojinin fiziksel bağlantısını kurunuz.



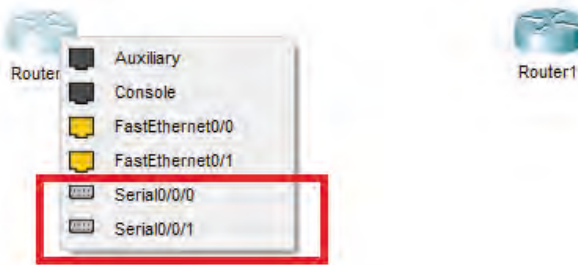
Görsel 3.6: Seri arayüz topolojisi

1. **Adım:** Ağ simülasyon programını açınız.
2. **Adım:** Simülasyon ortamına iki adet yönlendirici ekleyiniz.
3. **Adım:** Kablo türü olarak seri kablo türlerini seçiniz (Görsel 3.7).



Görsel 3.7: Seri arayüz kabloları

4. **Adım:** Router0 cihazının üzerini tıklayarak yönlendiricide mevcut seri arayüzlerden birini seçiniz. Saat sembolü olan kablo türü Serial DCE, diğer sembol ise Serial DTE kablodur. Yönlendirici cihazlardan birini DCE, diğerini DTE olarak seçiniz (Görsel 3.8).



Görsel 3.8: Yönlendirici cihaz portları

5. **Adım:** Router1 cihazında seri arayüzlerden birini seçerek, bağlantıyı fiziksel olarak tamamlayınız.

3.2. KOMUT ARAYÜZÜ KULLANARAK KULLANICI GİRİŞİ

Komut arabirimi hiyerarşik yapıdadır. Yapılandırma işlemlerinin gerçekleştirileceği farklı modları vardır. Her modda yürütülebilecek komutlar ve yapılabilecek işlemler farklıdır. Dolayısıyla yapılandırma işlemleri gerçekleştirilirken yönlendirici komut arabiriminin hangi modda olduğu bilinmeli ve komutun yürütülmesi için uygun moda geçilmelidir. Komut satırına komutlar yazılırken komutun tamamı yazılabileceği gibi kısaltmaları da yazılabilir. Komut satırına ilk bağlanıldığında doğrudan kullanıcı moduna girilir. Gerçekleştirilecek yapılandırma (konfigürasyon) işlemine göre diğer modlara geçilir (Tablo 3.1).

Tablo 3.1: Komut Modu Görünümü ve İşlevi

Komut Modu Görünümü	İşlevi	
Router>	Kullanıcı Modu	User/EXEC mode
Router#	Ayrıcalıklı Kullanıcı Modu	Privileged EXEC mode
Router(config)#	Global Konfigürasyon Modu	Global Configuration Mode
Router(config-if)#	Arayüz Konfigürasyon Modu	Interface Configuration Mode

• **Kullanıcı Modu (User/EXEC mode):** Yönlendirici cihaz açıldığında karşılaşılan ilk moda kullanıcı modu veya **User/Exec mode** ismi verilir. Kullanıcı modunda yönlendirici cihazla ilgili yönetimsel işlemler yapılmaz (Görsel 3.9).

```

--- System Configuration Dialog ---

Would you like to enter the initial configuration dialog?
[yes/no]: n

Press RETURN to get started!

Router>
Router>

```

Görsel 3.9: Kullanıcı modu görünümü

• **Ayrıcalıklı Kullanıcı Modu (Privileged EXEC mode):** Kullanıcı modunda iken komut satırına **“Enable”** yazılarak ayrıcalıklı kullanıcı moduna geçiş yapılır. **Privileged Exec mode** veya **Enable mod** ismi de verilen bu alanda kullanıcılar yönlendiriciye tamamen hâkim olur. Bu yüzden yönlendirici cihazın güvenliğini sağlamak için ayrıcalıklı kullanıcı moduna mutlaka şifre verilmelidir (Görsel 3.10).

```

--- System Configuration Dialog ---

Would you like to enter the initial configuration dialog?
[yes/no]: n

Press RETURN to get started!

Router>enable
Router#

```

Görsel 3.10: Ayrıcalıklı kullanıcı modu görünümü

• **Global Konfigürasyon Modu (Global Configuration Mode):** Ayrıcalıklı kullanıcı modunda (Enable) iken komut satırına **“Configure Terminal”** yazılarak global konfigürasyon moduna geçiş yapılır. **Config mod** ismi de verilen bu alanda kullanıcıların yapacağı değişiklikler yönlendiricinin tamamını etkiler. Yönlendirici ismini değiştirme, şifre verme gibi birçok işlem bu modda yapılır (Görsel 3.11).

```
Router>
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with
CNTL/Z.
Router(config)#
```

Görsel 3.11: Global konfigürasyon modu görünümü

Global yapılandırma modunun birçok alt modu bulunur (Tablo 3.2).

Tablo 3.2: Global Yapılandırma Alt Modları

Interface	Router(config-if)#
Subinterface	Router(config-subif)#
Controller	Router(config-controller)#
Map-list	Router(config-map-list)#
Map-class	Router(config-map-class)#
Line	Router(config-line)#
Router	Router(config-router)#
Route-map	Router(config-route-map)#



4. UYGULAMA

Kullanıcı Modu Komutlarını Görüntüleme

İşlem adımlarına göre yönlendiricinin kullanıcı modu arabirimini ve bu modda kullanılacak komutları görüntüleyiniz.

- 1. Adım:** Simülasyon programını açınız. Bir bilgisayar ve yönlendiriciyi konsol kablosu ile bağlayınız.
- 2. Adım:** Bilgisayarı açınız ve açılan ekrandan Terminal programını tıklayınız.
- 3. Adım:** Karşınıza gelen ekrandan **OK** seçeneğine tıklayınız ve komut arabirimini açınız.
- 4. Adım:** “Router>” komut satırını görünüz.
- 5. Adım:** “?” karakterini yazıp Enter tuşuna basınız ve karşınıza gelen ekrandan kullanıcı (User/EXEC) modunda kullanılacak komutları inceleyiniz.



5. UYGULAMA

Ayrıcalıklı Kullanıcı Modu Komutlarını Görüntüleme

İşlem adımlarına göre yönlendiricinin ayrıcalıklı kullanıcı modu arabirimini ve bu modda kullanılabilecek komutları görüntüleyiniz.

- 1. Adım:** Simülasyon programını açınız. Bir bilgisayar ve yönlendiriciyi konsol kablosu ile bağlayınız.
- 2. Adım:** Bilgisayarı açınız ve açılan ekrandan Terminal programını tıklayınız.
- 3. Adım:** Karşınıza gelen ekrandan **OK** seçeneğine tıklayınız ve komut arabirimini açınız.
- 4. Adım:** “Router>” komut satırını görünüz.
- 5. Adım:** “Router>enable” veya “en” komutunu yazıp Enter tuşuna basınız. Ekranda Router# ifadesini görünüz.
- 6. Adım:** “Router#?” komutunu yazıp Enter tuşuna basınız ve karşınıza gelen ekrandan ayrıcalıklı kullanıcı (Privileged /EXEC) modunda kullanılabilecek komutları inceleyiniz.



UYARI

İlk kullanım dışında kullanıcı modları arasında geçiş yapılırken şifre oluşturulduysa güvenlik sorulaması yapılır. Ayrıcalıklı kullanıcı modunda yönlendirici adından sonra “#” karakteri görülür. Ayrıcalıklı kullanıcı modundan kullanıcı moduna geri dönmek için “disable” komutu kullanılır. Ayrıca üst seviyedeki bir config moddan bir alt seviyedeki moda geçmek için “Ctrl+Z”, “Ctrl+C” kısayolları veya “exit”, “end” komutları kullanılabilir.



6. UYGULAMA

Global Yapılandırma Modu Komutlarını Görüntüleme

İşlem adımlarına göre yönlendiricinin global yapılandırma modu arabirimini ve bu modda kullanılabilecek komutları görüntüleyiniz.

- 1. Adım:** Simülasyon programını açınız. Bir bilgisayar ve yönlendiriciyi konsol kablosu ile bağlayınız.
- 2. Adım:** Bilgisayarı açınız ve açılan ekrandan Terminal programını tıklayınız.
- 3. Adım:** Karşınıza gelen ekrandan **OK** seçeneğine tıklayınız ve komut arabirimini açınız.

4. Adım: “Router>” komut satırını görünüz.

5. Adım: “Router>enable” veya “en” komutunu yazıp Enter tuşuna basınız. Ekranda Router# ifadesini görünüz.

6. Adım: “Router#configure terminal” veya “conf t” komutunu giriniz. Komut satırında Router(-config)# ifadesini görünüz.

Adım 7: “Router(config)#?” komutunu yazıp Enter tuşuna basınız ve karşınıza gelen ekrandan global yapılandırma modunda (Global Configuration Mode) kullanılabilecek komutları inceleyiniz.



7. UYGULAMA

Arayüz Yapılandırma Modu Komutlarını Görüntüleme

İşlem adımlarına göre arayüz yapılandırma modu arabirimini ve bu modda kullanılabilecek komutları görüntüleyiniz.

1. Adım: Simülasyon programını açınız. Bir bilgisayar ve yönlendiriciyi konsol kablosu ile bağlayınız.

2. Adım: Bilgisayarı açınız ve açılan ekrandan Terminal programını tıklayınız.

3. Adım: Karşınıza gelen ekrandan **OK** seçeneğine tıklayınız ve komut arabirimini açınız.

4. Adım: “Router>” komut satırını görünüz.

5. Adım: “Router>enable” veya “en” komutunu yazıp Enter tuşuna basınız. Ekranda Router# ifadesini görünüz.

6. Adım: “Router#configure terminal” veya “conf t” komutunu giriniz. Komut satırında Router(-config)# ifadesini görünüz.

Adım 7: “Router(config)#interface gigabitethernet 0/1” komutunu giriniz.

Adım 8: “Router(config-if)#?” komutunu yazıp Enter tuşuna basınız ve karşınıza gelen ekrandan arayüz konfigürasyon (Interface Configuration) modunda kullanılabilecek komutları inceleyiniz (Görsel 3.12).

```

Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface gigabitEthernet 0/1
Router(config-if)#?
  arp                Set arp type (arpa, probe, snap) or
  timeout             Set timeout
  bandwidth           Set bandwidth informational parameter
  cdp                 CDP interface subcommands
  channel-group       Add this interface to an Etherchannel
  group               group
  crypto              Encryption/Decryption commands
  custom-queue-list   Assign a custom queue list to an
  interface           Specify interface throughput delay
  delay              Interface specific description
  description         Configure duplex operation.
  duplex             Exit from interface configuration mode
  exit               Enable Fair Queuing on an Interface
  fair-queue          Set hold queue depth
  hold-queue          Interface Internet Protocol config
  ip                  commands
  ipv6                IPv6 interface subcommands

```

Görsel 3.12: Arayüz yapılandırma modu görünümü

3.2.1. Yardım Komutları

Yardım (show) komutları sayesinde yönlendiricinin yapılandırması hakkında birçok bilgi alınabilir. Yardım komutları **kullanıcı modda** ve **ayrıcalıklı kullanıcı modda** kullanılabilir.

Yönlendirici yapılandırmasında birçok yardım komutu kullanılır. Bu komutların sık kullanılanları ve görevleri şunlardır:

- **show version:** Yönlendiricide çalışan IOS sürümünü, yönlendiricinin ne kadar süredir çalışır olduğunu, RAM ve arayüz türleri gibi özellikleri görüntüler.
- **show running-config:** Yönlendiricide o an çalışmakta olan yapılandırma bilgisini görüntüler.
- **show startup-config:** Yönlendiricide başlangıçta çalışmakta olan yapılandırma bilgisini görüntüler.
- **show flash:** Yönlendiricinin flash belleğindeki IOS ve diğer dosyalarla birlikte flashta kullanılan boş ve toplam alanları görüntüler.
- **show history:** Yönlendiricide geriye dönük olarak girilmiş son 10 komutu görüntüler.
- **show interfaces:** Yönlendiricideki tüm arayüzlerin donanım ve IP adreslerini, paket miktarını, kaydedilen hataları ve yapılandırmayı görüntüler.
- **show interface arayüz-no:** Belirtilen arayüzün o anki yapılandırmasını, donanım ve IP adreslerini, gidip gelen paket miktarını, kaydedilen hatalarını görüntüler.
- **show protocol:** Yönlendirici üzerinde yapılandırılmış yönlendirme protokollerini görüntüler.
- **show ip route:** Yönlendirme rotalarını ve kullanılan yönlendirme protokollerini görüntüler.
- **show Access-list:** Yönlendirici üzerinde yapılandırılmış erişim denetim listelerini ve bunların kaç kez eşlendiğini görüntüler.

Yardım komutunu Global Config modda kullanmak için **“do show parametre”** şeklinde yazmak gerekir (Görsel 3.13).

```
Router(config)#
Router(config)#do show run
Building configuration...

Current configuration : 691 bytes
!
```

Görsel 3.13: Global yapılandırma modunda show komutunun kullanımı

3.3. TEMEL YÖNLENDİRİCİ TANIMLAMALARI

Yönlendirici cihazın bazı temel yapılandırmalarının yapılması, güvenlik açısından da kullanıcıların cihazları daha kolay yönetebilmesi açısından da çok önemlidir. Yönlendirici cihazın isimlendirilmesi, güvenlik için gerekli bilgilendirme ve şifreleme işlemlerinin yapılması, cihazın yönetimi için uzaktan bağlantı yapılandırmalarının oluşturulması gerekir.

3.3.1. Yönlendirici Cihaza İsim Verme

Kullanıcılar, yönlendirici cihazlar üzerinde işlem yaparken hangi yönlendirici üzerinde işlem yaptığının ayırt edilmesi ve yönetim açısından bir karışıklık doğmaması için yönlendirici cihaza isim verirler. Yönlendirici cihaza isim verme işlemi, global yapılandırma modunda “**Hostname**” komutu kullanılarak gerçekleştirilir.

Yönlendirici cihazın ismini değiştirmek için şu komutlar kullanılır:

```
Router>enable
Router#configure terminal
Router(config)#hostname BILISIM
BILISIM(config)#
```

3.3.2. Yönlendirici Şifreleme

Kullanıcıların yönlendirici cihazlar üzerinde yetkisiz işlem yapmaması için şifreleme tekniği uygulanmalıdır. Yönlendirici cihazın ayrıcalıklı kullanıcı moduna erişimi, konsol bağlantısı erişimi, AUX bağlantısı erişimi ve TELNET ile uzaktan erişimi şifrlenerek cihaz güvenli bir hâle getirilebilir.

3.3.2.1. Ayrıcalıklı Kullanıcı Modu Şifreleme

Yönlendirici cihazın **ayrıcalıklı kullanıcı moduna** yetkisiz girişleri engellemek için global yapılandırma modunda “**Enable**” komutu ve parametreleri kullanılır (Görsel 3.14).

```
Router(config)#enable ?
password Assign the privileged level password
secret Assign the privileged level secret
```

Görsel 3.14: Ayrıcalıklı kullanıcı moduna parola verme işlemi

Görsel 3.14’te görüldüğü üzere ayrıcalıklı kullanıcı moduna parola verilirken “password” veya “secret” parametresi kullanılır. Enable Password, Clear Text olarak parolanın yapılandırma dosyasında açık bir şekilde görünürlüğünü sağlayan şifreleme yöntemidir. Enable Password ile belirlenen şifre, show running-config komutu ile görünür hâlde olacaktır. Enable Secret ise parolanın Clear Text olmadan bir başka deyişle kriptolanarak görünürlüğünün ortadan kaldırılmasını sağlar. Kullanılan şifre show running-config komutu ile incelendiğinde şifrenin md5 algoritmasıyla kriptolandığı görülür.



8. UYGULAMA

Ayrıcalıklı Kullanıcı Moduna Parola Verme

İşlem adımlarına göre şifreleme işlemi ve çalışan konfigürasyon dosyası komutlarını görüntüleyiniz. Yönlendirici cihazın ayrıcalıklı kullanıcı modunu kriptolamadan MEB1234 şifresini veriniz ve çalışan konfigürasyon dosyasında (Running Config) görüntülenmesini sağlayınız.

1. Adım: Simülasyon programını açınız. Bir bilgisayar ve yönlendiriciyi konsol kablosu ile bağlayınız.

2. Adım: Bilgisayarı tıklayınız ve açılan ekrandan Terminal programını seçiniz. Komut arabirimini açınız.

3. Adım: Şifreleme işlemini şu komutları girerek gerçekleştiriniz:

```
Router>
Router>enable
Router#configure terminal
Router(config)#enable password MEB1234
```

4. Adım: Router#show running-config komutunu kullanarak çalışan konfigürasyon dosyasında şifrenin açık bir şekilde görüntülendiğini listeleyiniz (Görsel 3.15).

```
Router#
Router#show running-config
Building configuration...

Current configuration : 717 bytes
!
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Router
!
!
enable password MEB1234
```

Görsel 3.15: Çalışan konfigürasyon komut çıktısı

5. Adım: Şifreleme işleminin doğruluğunu password alanına şifreler girerek test ediniz (Görsel 3.16).

```
Router>
Router>enable
Password:
```

Görsel 3.16: Şifre giriş alanı



UYARI

Çalışan ayarlara bakıldığı zaman password parametresiyle verilen şifre kriptolanmadığı için açıkça görülür. Bu durumu engellemek için service password-encryption komutu kullanılır. Bu komut ile yapılacak kriptolama, secret ile yapılacak kriptolama işlemi kadar güçlü değildir.

```
Router(config)#service password-encryption
```



SIRA SİZDE

Yönlendiriciye “Ankara1920” parolasını veriniz ve parolayı kriptolayarak gizleyiniz.



ARAŞTIRMA

Yönlendiriciye password ve secret parametrelerinin her ikisiyle de şifre atanırsa yönlendirici hangi şifreyi kullanır?

3.3.2.2. Konsol Arayüzünü Şifreleme

Yönlendirici cihazına konsol bağlantısı ile yapılacak yetkisiz girişler, global yapılandırma modunda şifre verilerek engellenebilir.

Konsol bağlantılarını şifrelemek için şu komutlar kullanılır:

```
Router>
Router>enable
Router#configure terminal
Router(config)#line console 0
Router(config-line)#password MEVLANA
Router(config-line)#login
```

3.3.2.3. TELNET Bağlantısını Şifreleme

TELNET, yönlendirici cihaza uzaktan erişim sağlayarak cihazı yapılandıran bir bağlantı türüdür. Yönlendirici cihaza TELNET bağlantısı ile yapılacak yetkisiz girişler, global yapılandırma modunda şifre verilerek engellenebilir.

TELNET bağlantılarını şifrelemek için şu komutlar kullanılır:

```
Router>
Router>enable
Router#configure terminal
Router(config)#line vty 0 4
Router(config-line)#password BILISIM
Router(config-line)#login
```


TELNET bağlantısı şifrelendiğinde güvensiz bir bağlantı oluşur ve ağ izleme yazılımı gibi programlarla veri paketleri dinlendiğinde TELNET şifreleri istenmeyen kişilerin eline geçebilir. Bu güvensiz TELNET bağlantısının önüne geçebilmek ve güvenli bir bağlantı kurabilmek için **SSH bağlantısı** yapılır.

SSH bağlantısı yapabilmek için öncelikle cihaza bir **hostname** verilir. Ardından **username** ve **password** tanımlanır. Sonrasında bir domain tanımlaması yapılarak TELNET şifreleme işlemi gerçekleştirilir. Bu işlemi gerçekleştirebilmek için gerekli komutlar şunlardır:

```
Router>
Router>enable
Router#configure terminal
Router(config)#hostname MESLEKLISESI
MESLEKLISESI(config)#username MEB password 1453
MESLEKLISESI(config)#ip domain-name meb.gov.tr
MESLEKLISESI(config)#crypto key generate rsa
```

The name for the keys will be: MESLEKLISESI.meb.gov.tr
 Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes.
 How many bits in the modulus [512]:
 % Generating 512 bit RSA keys, keys will be non-exportable...[OK]

```
MESLEKLISESI(config)#line vty 0 4
MESLEKLISESI(config-line)#transport input ssh
MESLEKLISESI(config-line)#login local
```

3.3.3. Seri Arayüz Yapılandırma

Yönlendirici cihazlardaki seri arayüzler WAN topolojilerinde kullanılır. İki veya daha fazla yönlendirici cihazın birbirine bağlanmasında seri arayüzler kullanılır. Seri arayüzden haberleşen yönlendiricilerden bir tarafın **DCE (Data Communications Equipment)**, diğer tarafın da **DTE (Data Terminal Equipment)** olması gerekir. DCE, veri iletimindeki hızı belirleyen taraftır ve bunun yapılandırılması gerekir. İletim hızı "clock rate" komutu ile yapılandırılır. Clock rate, saniyede iletilen bit miktarıdır.



9. UYGULAMA

Yönlendirici Seri Arayüz Yapılandırılması

Simülasyon programını kullanarak topolojiye Ankara ve Bursa isiminde iki yönlendirici ekleyiniz. Ankara yönlendiricisi clock rate sinyalini üretir. Seri arayüz yapılandırmasını ve IP adresi girişlerini Görsel 3.17'deki bilgilerden faydalanarak hazırlayınız.



Görsel 3.17: Seri arayüz yapılandırma

İşlem adımlarına göre seri arayüz yapılandırmasını yapınız ve “Clock Rate” değerini atayınız.

1. Adım: Simülasyon programını açınız. Topolojiye iki adet yönlendiriciyi ekleyiniz.

2. Adım: Ankara yönlendiricisine **DCE kablosunu Se0/0/0 seri portundan**, Bursa yönlendiricisine ise **DTE kablosunu Se0/0/0 seri portundan** takınız.

3. Adım: Ankara yönlendiricisine gerekli komutları girerek seri arayüz yapılandırma işlemini gerçekleştiriniz. Ankara yönlendiricisi DCE tarafı olduğu için saat sinyalini üretecektir.

Ankara>

Ankara >enable

Ankara#configure terminal

Ankara (config)#interface se0/0/0

Ankara(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down

Ankara (config-if)#ip address 10.10.10.1 255.255.255.0

Ankara (config-if)#clock rate 56000

4. Adım: Bursa yönlendiricisine gerekli komutları girerek seri arayüz yapılandırma işlemini gerçekleştiriniz. Bursa yönlendiricisi DTE tarafı olduğu için saat sinyalini üreten değil, alan taraf olacaktır.

Bursa>

Bursa >enable

Bursa#configure terminal

Bursa (config)#interface se0/0/0

Bursa (config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down

Bursa (config-if)#ip address 10.10.10.2 255.255.255.0

3.3.4. Ethernet Arayüz Yapılandırma

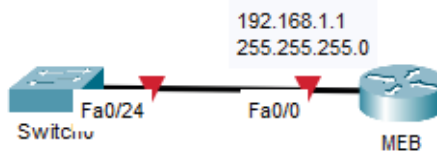
Ethernet arayüzleri genellikle yerel ağlarda (LAN) kullanılır. Yönlendiricide birden fazla Ethernet, Fast Ethernet veya Gigabit Ethernet arabirimi olabilir. “interface f0/0” komutu ile bahsedilen 0 No.lu Fast Ethernet arabirimine girilmesi sağlanır. CLI kullanıcısı “interface f0/0” komutu yazıldıktan sonra arabirim yapılandırma moduna geçecektir. Daha sonra Ethernet arayüzüne IP adresi ve Subnet Maskı verilir.



10. UYGULAMA

Ethernet Arayüz Yapılandırması

Simülasyon programını kullanarak MEB isminde bir yönlendirici ve bir anahtarlama cihazını topolojiye ekleyiniz. MEB yönlendiricisi ile anahtar bağlantısını Ethernet arayüzünden düz kablo kullanarak yapınız. Ethernet arayüz yapılandırması için gerekli IP adresi girişlerini Görsel 3.18'deki bilgilerden faydalanarak hazırlayınız.



Görsel 3.18: Ethernet arayüz yapılandırma

İşlem adımlarına göre Ethernet arayüzünü yapılandırınız.

1. Adım: Simülasyon programını açınız. Bir adet yönlendirici ve bir adet anahtarlama cihazını topolojiye ekleyiniz.

2. Adım: MEB yönlendiricisine düz kabloyu Fa0/0 portundan, anahtarlama cihazına ise Fa0/24 portundan takınız.

3. Adım: MEB yönlendiricisine şu komutları girerek Ethernet arayüz yapılandırma işlemini gerçekleştiriniz:

```
MEB>
MEB>enable
MEB#configure terminal
MEB(config)#interface fastEthernet 0/0
MEB(config-if)#no shutdown
```

%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to down

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

3.3.5. Yapılandırma Değişikliklerini Kaydetme

Yönlendirici cihaz yapılandırılırken yazılan kodlar RAM üzerinde tutulur. RAM'de çalışan yapılandırma dosyası içindeki yapılandırma komutları elektrik kesintisi olması hâlinde hafızadan silinir. Yapılandırmanın NVRAM üzerindeki başlangıç yapılandırma dosyasında bulunması hâlinde ise yapılandırma kayıpları ortadan kalkar. Yapılandırma değişikliklerini startup-config üzerine kaydetme işlemi birden fazla yol ile gerçekleştirilir.

Ayrıcalıklı kullanıcı modunda iken “write” komutu ile o andaki çalışan yapılandırma, startup-config dosyasına yazılır. Global yapılandırma modunda ise “do write” komutu kullanılmalıdır.

```
Router>
Router>enable
Router#write
Building configuration...
[OK]
```

Aynı işlem, copy komutu kullanılarak şu şekilde de yapılabilir:

```
Router#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```



SIRA SİZDE

Ağ simülasyon programını kullanarak topolojiye iki adet yönlendirici cihaz ekleyiniz. Cihazları birbirine seri portlar yardımıyla bağlayınız. Cihaz isimlerinin birini ANKARA, diğerini BURSA yapınız. Yönlendiricilere md5 algoritması ile kriptolanacak şekilde ayrıcalıklı kullanıcı modu şifresini veriniz. ANKARA yönlendiricisini uzaktan TELNET ile bağlanacak şekilde yapılandırınız.

3.4. ARAYÜZ YAPILANDIRMA

Yönlendirici cihazda arayüzler yapılandırılırken cihazın hangi hatta bağlı olduğunun, hangi cihazın yapılandırıldığı ve hazırlanan topolojinin hangi noktasında işlem yapıldığının ezbere bilinmesi birçok hataya sebebiyet verir. Arayüz yapılandırması yapılırken tanımlayıcı ve uyarıcı komutların kullanılması, bu tarz problemlerin çözümünde etkilidir. Bu yüzden arayüzlere tanımlama yapılır ve gerektiğinde yardım (show) komutları kullanılarak hangi arayüzde hangi işlemlerin yapıldığı kolayca algılanır.

3.4.1. Arayüz Tanımlama

Yönlendiricilerin Seri ve Fast Ethernet arayüzlerine tanımlayıcı yapılandırmalar yapılarak hangi arayüz üzerinde çalışıldığı kolayca görülür ve ona göre işlemler gerçekleştirilir.

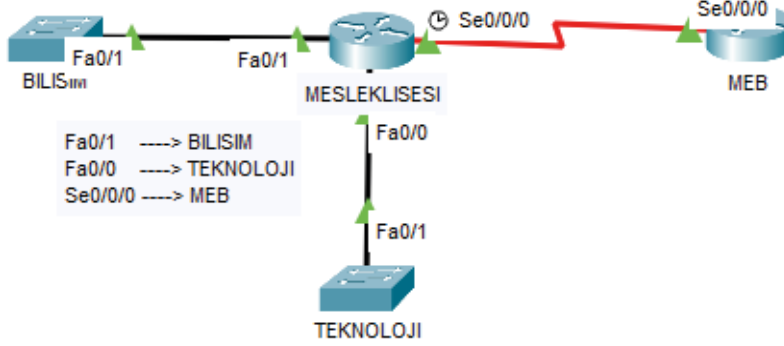
Arayüz tanımlama işlemleri için ilgili arayüzde “description” komutu kullanılır.



11. UYGULAMA

Yönlendirici Cihazda Arayüz Tanımlanması

Simülasyon programını kullanarak MESLEKLİSESİ ve MEB isiminde iki yönlendirici, BİLİSİM ve TEKNOLOJİ isimlerinde iki anahtarlama cihazını topolojiye ekleyiniz. Görsel 3.19'daki bilgilerden faydalanarak arayüz tanımlarını hazırlayınız.



Görsel 3.19: Arayüz tanımlama topolojisi

İşlem adımlarına göre gerekli arayüz tanımlamalarını yapınız.

1. Adım: Simülasyon programını açınız. İki adet yönlendirici ve iki adet anahtarlama cihazını topolojiye ekleyiniz. Görsel 3.19'daki bilgilere göre kablo bağlantılarını hazırlayınız.

2. Adım: MESLEKLİSESİ yönlendiricisi komut satırını açınız. Fa0/1 arayüzü için BİLİSİM, Fa0/0 arayüzü için TEKNOLOJİ ve Se0/0/0 arayüzü için MEB tanımlamalarını şu kodları kullanarak yapınız:

```
MESLEKLİSESİ>
```

```
MESLEKLİSESİ>enable
```

```
MESLEKLİSESİ#configure terminal
```

```
MESLEKLİSESİ(config-if)#interface fastEthernet 0/1
```

```
MESLEKLİSESİ(config-if)#description BİLİSİM
```

```
MESLEKLİSESİ(config-if)#exit
```

```
MESLEKLİSESİ(config)#interface fastEthernet 0/0
```

```
MESLEKLİSESİ(config-if)#description TEKNOLOJİ
```

```
MESLEKLİSESİ(config-if)#exit
```

```
MESLEKLİSESİ(config)#interface se0/0/0
```

```
MESLEKLİSESİ(config-if)#description MEB
```

3. Adım: MESLEKLİSESİ yönlendiricisinde yaptığınız arayüz tanımlamalarını yardım komutlarını kullanarak, yapılandırmayı kontrol edip doğrulayınız. Görsel 3.20'deki komutları yazarak Fa0/1 arayüzünü, Görsel 3.21'deki komutları yazarak Fa0/0 arayüzünü, Görsel 3.22'deki komutları yazarak Se0/0/0 arayüz tanımlamalarını kontrol ediniz.

```
Router#show interfaces fa0/1
FastEthernet0/1 is up, line protocol is up (connected)
  Hardware is Lance, address is 0002.1714.9802 (bia 0002.1714.9802)
  Description: BILISIM
  Internet address is 192.168.1.1/24
```

Görsel 3.20: Fa0/1 arayüz tanımlanmasını doğrulama

```
Router#show interfaces fa0/0
FastEthernet0/0 is up, line protocol is up (connected)
  Hardware is Lance, address is 0002.1714.9801 (bia 0002.1714.9801)
  Description: TEKNOLOJI
  Internet address is 192.168.2.1/24
```

Görsel 3.21: Fa0/0 arayüz tanımlanmasını doğrulama

```
Router#show interfaces se0/0/0
Serial0/0/0 is up, line protocol is up (connected)
  Hardware is HD64570
  Description: MEB
```

Görsel 3.22: Se0/0/0 arayüz tanımlanmasını doğrulama

3.4.2. Arayüz Bağlantı Mesajları

Yönlendiricilerin arayüzlerinin bağlantı durumları yapılandırma mesajları sonucunda öğrenilebilir. Arayüzlerin fiziksel olarak bağlı olup olmadığı, bağlantı problemlerinin olup olmadığı veya doğru bir şekilde yapılandırılıp yapılandırılmadığı gibi bilgiler mesajlar sayesinde öğrenilebilir.

Arayüz bağlantı mesajları için ilgili yardım komutları kullanılır ve verilen mesaja göre arayüz durumu hakkında bilgi alınır (Görsel 3.23).

```
MESLEKLISESI(config)#do sh int fa0/0
FastEthernet0/0 is administratively down, line protocol is down (disabled)
  Hardware is Lance, address is 0002.1714.9801 (bia 0002.1714.9801)
  Description: TEKNOLOJI
```

Görsel 3.23: Arayüz bağlantı mesajı çıktısı

Arayüz bağlantı durumlarını öğrenmek için şu kodlar yönlendirici cihaz komut satırına girilir:

```
MESLEKLISESI#show interfaces se0/0/1
```

```
Serial0/0/1 is administratively down, line protocol is down (disabled)
```

```
MESLEKLISESI#show interface se0/0/0
```

```
Serial0/0/0 is up, line protocol is up (connected)
```


Tablo 3.3: Arayüz Bağlantı Mesajları

BAĞLANTI MESAJI	DURUM
FastEthernet 0/0 is up, lineprotocol is up	Çalışıyor, sorun yok.
Serial 0/0/0 is up, lineprotocol is down	Bağlantı problemi var.
Serial 0/0/0 is down, lineprotocol is down	Arayüz problemi var.
Serial 0/0/0 is administrativelydown, lineprotocol is down	Çalışmıyor.

3.4.3. Yönlendirici Açılış Mesajları

Yönlendirici cihazı yetkisiz kişilerin kullanmasını önlemek için bir güvenlik uyarısı vermek mümkündür. Yönlendirici açılış mesajları kullanılarak TELNET, konsol veya diğer yöntemlerle yönlendirici komut satırına bağlanmak isteyen kişilere bir güvenlik uyarısı mesajı verilebilir.

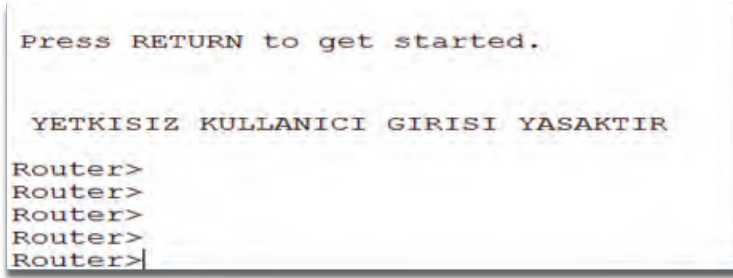
Açılış mesajı eklemek için yapılandırma modunda “banner motd x mesaj x” komutu kullanılır. Verilecek açılış mesajının öncesine ve sonrasına aynı işaretler konulmalıdır. Aynı işaretler kullanıldıktan sonra işaretlerin ne olduğu fark etmez, işaretler arasına verilmek istenen mesaj yazılabilir.

Router>

Router>enable

Router#configure terminal

Router(config)#banner motd x YETKISIZ KULLANICI GIRISI YASAKTIR x



Görsel 3.24: Yönlendirici açılış mesajı

3.4.4. Yönlendirici Host Tablosu

Uzaktaki bir cihaza erişilmek veya TELNET gibi bağlantılar kurulmak istendiğinde IP adresleri kullanılır. Uzaktaki cihaza IP adresleri kullanılarak ulaşmanın yanında bir diğer alternatif ise ulaşmak istenen IP adresine bir isim (hostname) verilip o ismin kullanılmasıdır. Bu işlem için iki yöntem vardır. İlk yöntemde her yönlendirici üzerinde host tablosu yapılandırılır. İkinci yöntemde ise DNS sunucusu üzerinden isim çözümlenir.

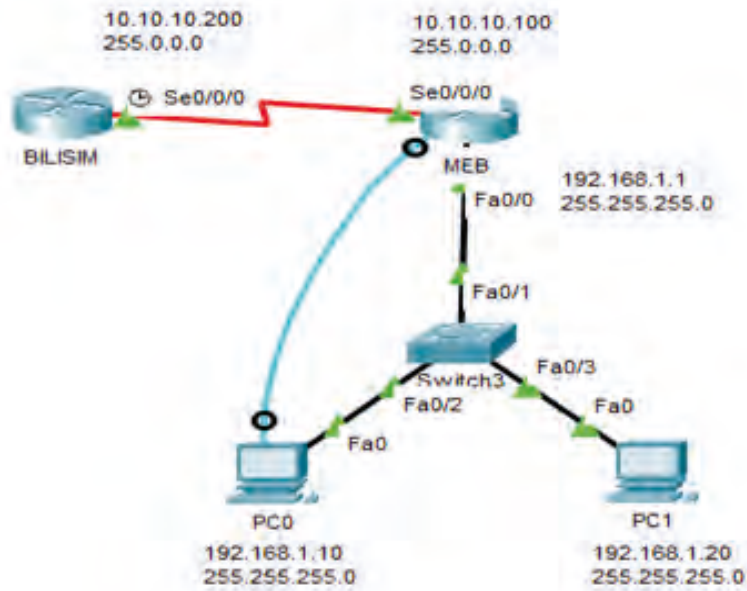
Host tablolarında IP adresleri ve o IP adreslerine karşılık gelen hostname isimlendirmeleri tutulur.



12. UYGULAMA

Host Tablosu Oluşturma

Simülasyon programını kullanarak Görsel 3.25'te verilen topolojiyi hazırlayınız. Hazırladığınız topolojide 10.10.10.200 IP adresi ile BİLİSİM ismini MEB yönlendiricisinde eşleştirip, PC0'dan hostname kullanarak TELNET bağlantısı yapınız.



Görsel 3.25: Host IP eşleştirme topolojisi

İşlem adımlarına göre gerekli hostname IP eşleştirmelerini yapınız.

1. Adım: Simülasyon programını açınız ve Görsel 3.25'te verilen topolojiyi hazırlayınız.

2. Adım: Verilen IP adres yapılandırmalarını cihazlara giriniz.

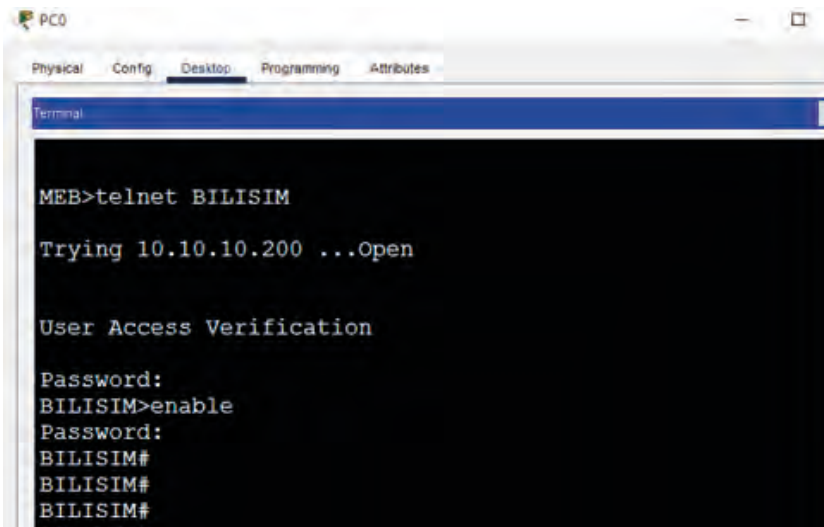
3. Adım: BILISIM yönlendiricisinde TELNET bağlantısı kurabilmek için gerekli yapılandırmaları şu kodları kullanarak yapınız:

```
BILISIM>
BILISIM >enable
BILISIM #configure terminal
BILISIM (config)#enable secret MEB123
BILISIM (config)#line vty 0 4
BILISIM (config-line)#password 1234
BILISIM (config-line)#login
```

4. Adım: MEB yönlendiricisinde BILISIM ismi ile TELNET bağlantısı yapabileceğiniz host IP eşleştirmesi 10.10.10.200 IP adresi BILISIM ismi ile eşleşecek şekilde şu kodları giriniz:

```
MEB>
MEB >enable
MEB#configure terminal
MEB(config)#ip host BILISIM 10.10.10.200 255.0.0.0
```

5. Adım: Konsol kablosu ile bağlanmış PC0 bilgisayarını kullanarak, BILISIM yönlendiricisine hostname ismi ile IP adresi kullanmadan TELNET bağlantısını gerçekleştiriniz (Görsel 3.26).



```

PC0
Physical Config Desktop Programming Attributes
Terminal
MEB>telnet BILISIM
Trying 10.10.10.200 ...Open
User Access Verification
Password:
BILISIM>enable
Password:
BILISIM#
BILISIM#
BILISIM#

```

Görsel 3.26: Hostname ile TELNET Bağlantısı

6. Adım: MEB yönlendiricisine host tablosunu görebilmek için “show hosts” komutunu giriniz ve tablodaki eşleşmeleri doğrulayınız (Görsel 3.27).



UYARI

“show hosts” çıktısında “Flags” sütununun altında “perm” ifadesi yer alır. Bu, kaydın manuel olarak girildiğini gösterir. Burada perm yerine “temp” ifadesi olsaydı kaydın DNS üzerinden çözüldüğü anlaşılabaktı.

```

MEB>enable
MEB#show hosts
Default Domain is not set
Name/address lookup uses domain service
Name servers are 255.255.255.255

Codes: UN - unknown, EX - expired, OK - OK, ?? -
revalidate
      temp - temporary, perm - permanent
      NA - Not Applicable None - Not defined

Host          Port  Flags      Age Type
Address(es)
BILISIM       None  (perm, OK)  0   IP
10.10.10.200

```

Görsel 3.27: Host tablosu görüntüleme

3.4.5. Kullanıcı Seviyeleri Oluşturma

Yönlendirici cihaza kimlerin bağlanıp hangi işleri yapabileceği kullanıcı seviyesi politikalarıyla sınırlandırılabilir. Böylelikle yönlendiricinin daha güvenli yönetimi sağlanabildiği gibi çeşitli kullanıcı seviyeleri oluşturularak esnek bir yönetim de sağlanabilir.

Yönlendiricilerde kullanıcı modu ve ayrıcalıklı kullanıcı modu olarak iki çeşit erişim hakkı vardır. Kullanıcı modunda sadece kontroller yapılabilirken, yönetici modda ek olarak cihaz yapılandırması da gerçekleştirilebilir. Bu iki erişim hakkı; yönlendirici üzerinde 0-15 arasında belirlenmiş, çeşitli yetki seviyesi ile desteklenmiş ve üç erişim seviyesine ayrılmıştır. Erişim seviyeleri şunlardır:

- **Seviye 0:** Bu mod; disable, enable, exit, help ve logout komutlarını içerir ve nadiren kullanılır.
- **Seviye 1:** Kullanıcı Modu
- **Seviye 15:** Ayrıcalıklı Kullanıcı Mod

Seviye 2 ile Seviye 14 arasında ise kullanıcı yetkileri özelleştirilebilir. Alt seviye yetkileri üst seviye yetkilere taşınabilir ve yetkiler kendi aralarında değişiklikler yapabilir.

Bazı küçük şirketlerde her network yöneticisinin ayrıcalık seviyesinin aynı olması sorun oluşturmazken şirket hacmi büyüdüğünde her network yöneticisinin her komutu işletme gereksinimi ortadan kalkar. Örneğin şirkette stajyer olarak çalışan birinin sadece routerda interface durumlarını veya komşuluklarını görmesi istenebilir. Böyle bir çalışanın şirket için hayati öneme sahip bir routerda 15. seviyede yetkiye sahip olması çok akıllı kârı değildir. Bu durumda kullanıcıya özel ayrıcalık tanıma işlemi mantıklı bir yöntem olarak devreye girer.

Kullanıcıların ayrıcalık seviyeleri “show privilege” komutu kullanılarak görüntülenir (Görsel 3.28).

```
MEB#show privilege
Current privilege level is 15
```

Görsel 3.28: Ayrıcalık seviyesini görüntüleme

“username” komutu, belli bir ayrıcalık seviyesine sahip bir kullanıcı oluşturmak için kullanılır. Ayrıcalık seviyesini belirlemek için “privilege” parametresi kullanılır. “enable secret” komutuyla da oluşturulan kullanıcı seviyesine şifre atama işlemi yapılır.

```
MEB>
MEB>enable
MEB#configure terminal
MEB(config)#username MEB privilege 8
MEB(config)#enable secret level 4 Bilisim123
```

Kullanıcının Seviye 8 olarak giriş yapması için yönlendiriciye “enable 8” komutunu girmesi gerekir (Görsel 3.29).

```
MEB>
MEB>enable
MEB#enable 8
MEB#show privilege
Current privilege level is 8
```

Görsel 3.29: Ayrıcalık seviyesi değişikliği

Kullanıcı, 8. ayrıcalık seviyesinde sadece show komutlarını görüntüleyebilir. Kullanıcının Seviye 8’de global yapılandırma moduna girebilmesi için şu komutu kullanması gerekir:

MEB(config)#privilege exec level 8 configure terminal



SIRA SİZDE

5. seviye kullanıcı oluşturunuz ve bu kullanıcı seviyesinde öncelikli olarak global yapılandırma moduna girmeye çalışınız ve girilemediğini doğrulayınız. Sonrasında 5. seviye kullanıcı moduna global yapılandırmaya girilebilecek komutları yazınız.

3.4.6. Yapılandırma Dosyalarını Uzak Sunucuya Yedekleme

Yönlendiricinin yapılandırma dosyalarını uzaktaki bir sunucuya yükleyerek dosyaların yedeğini almak mümkündür. Yönlendirici hafızasının başlangıç (startup) ve çalışan (running) config (ayar) dosyalarının yedeklerini almak için TFTP Server kullanılır. TFTP Server’a yedeklenen yapılandırma dosyası istendiğinde geri yüklenebilir.

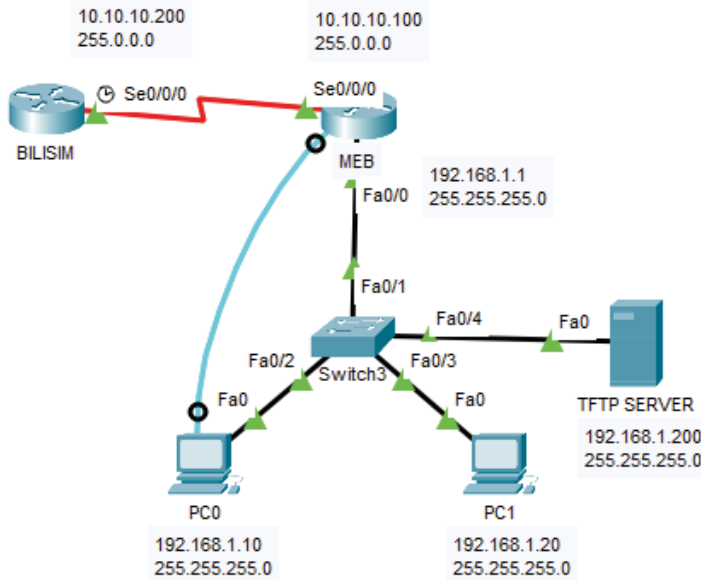
TFTP Server ile yedek alınırken System Image File’in tam dosya adı bilinmelidir. Bu, “show flash” komutu ile öğrenilebilir. Alınan bütün yedekler gibi IOS’in yedeği de TFTP Server tarafından TFTP-Root klasörünün altına atılır.



13. UYGULAMA

Yapılandırma Dosyasını Uzak Sunucuya Yedekleme ve Yedeği Geri Yükleme

Simülasyon programını kullanarak Görsel 3.30’da verilen topolojiyi hazırlayınız. Hazırladığınız topolojide hostname değişikliği yaparak (MEB1) yapılandırmayı kaydediniz. Kaydettiğiniz yapılandırmayı TFTP Server’a yedekleyiniz. Sonrasında yönlendirici yapılandırmasında tekrar hostname değişikliği yaparak (MEB2) kaydediniz. Aldığınız yedeği tekrar yönlendiriciye yükleyerek ilk hâline getiriniz.



Görsel 3.30: Uzak sunucuya yedek alma topolojisi

İşlem adımlarına göre uzak sunucuya yapılandırmayı yükleyiniz ve geri alınız.

1. Adım: Simülasyon programını açınız ve Görsel 3.30'da verilen topolojiyi hazırlayınız.

2. Adım: Görsel 3.30'da verilen IP adres yapılandırmalarını cihazlara giriniz.

3. Adım: MEB yönlendiricisinin ismini MEB1 yapıp, şu komutları kullanarak yapılandırmayı kaydediniz:

```
MEB>
MEB>enable
MEB#configure terminal
MEB(config)#hostname MEB1
MEB1(config)#do write
Building configuration...
[OK]
```

4. Adım: Kaydedilmiş yapılandırma dosyasını 192.168.1.200 IP adresli TFTP Server'a meb1 ismiyle yeniden kaydediniz (Görsel 3.31).

```
MEB1#copy running-config tftp:
Address or name of remote host []? 192.168.1.200
Destination filename [MEB1-config]? meb1

Writing running-config....!!
[OK - 906 bytes]

906 bytes copied in 3.018 secs (300 bytes/sec)
```

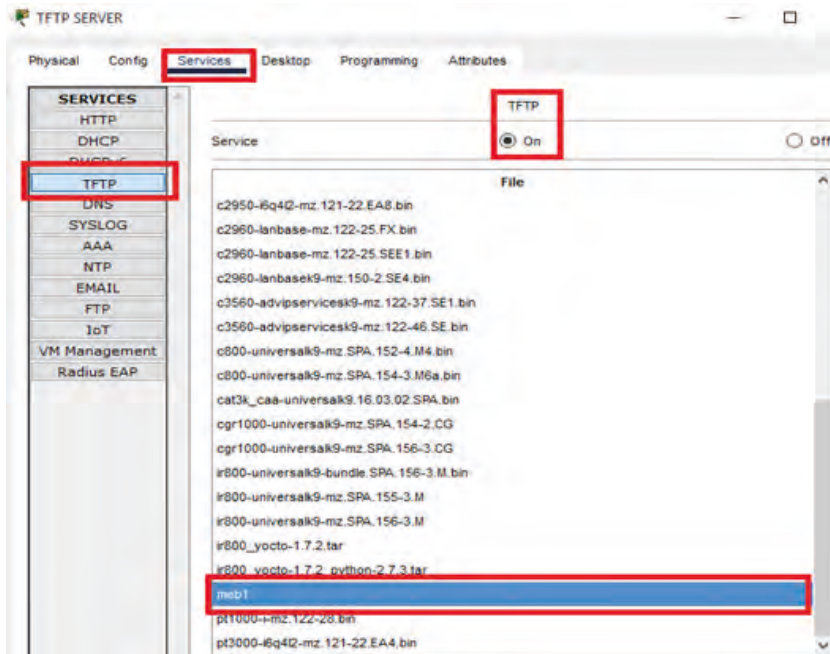
Görsel 3.31: TFTP Server'a yapılandırmayı yedekleme

5. Adım: Yapılandırma yedeğinin başarılı bir şekilde alınıp alınmadığını, TFTP Server bilgisayarına tıklayarak servisler kısmından kontrol ediniz (Görsel 3.32).



SIRA SİZDE

Ağ simülasyon programında orta ölçekli bir şirketin ağını tasarlayınız. Gerekli temel yapılandırmaları, güvenlik yapılandırmalarını ve uzaktan bağlantı için gerekli konfigürasyonları yapınız. Yapılandırmayı kaydediniz ve uzaktaki bir sunucuda yedeğini alınız.



Görsel 3.32: TFTP Server’da yedeği alınan dosyayı görüntüleme

6. Adım: MEB1 ismi verilen yönlendiricinin ismini MEB2 yapıp, şu komutları kullanarak yapılandırmayı tekrar kaydediniz:

```
MEB1>
MEB1>enable
MEB1#configure terminal
MEB1(config)#hostname MEB2
MEB2(config)#do write
Building configuration...
[OK]
```

Adım 7: MEB2 ismi verilen yönlendiricide TFTP Server’a yüklediğiniz meb1 yapılandırmasının yedeğini geri yükleyiniz (Görsel 3.33).

```
MEB2>
MEB2>enable
MEB2#copy tftp running-config
Address or name of remote host []? 192.168.1.200
Source filename []? meb1
Destination filename [running-config]?

Accessing tftp://192.168.1.200/meb1...
Loading meb1 from 192.168.1.200: !
[OK - 906 bytes]

906 bytes copied in 0 secs
MEB1#
%SYS-5-CONFIG_I: Configured from console by console
MEB1#
```

Görsel 3.33: TFTP Server’dan yedeği geri yükleme



SIRA SİZDE

Görsel 3.30'daki topolojide ayrıcalıklı kullanıcı moduna şifre vererek yapılandırmayı kaydediniz. Yapılandırmayı başlangıç konfigürasyonuna kaydediniz. Başlangıç konfigürasyonunu BURSA ismiyle TFTP Server'a yedekleyiniz. Sonrasında şifreyi değiştirip kaydediniz ve BURSA yapılandırmasını TFTP Server'dan geri yükleyiniz.



ÖLÇME VE DEĞERLENDİRME

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

1. () Yönlendirici işletim sistemi Flash üzerinde bulunur.
2. () Yönlendirici cihaza uzak bilgisayarlardan TELNET aracılığı ile bağlanarak yapılandırma yapılır.
3. () Seri arayüzlere takılan kabloların saat sinyali üreten türüne DTE ismi verilir.
4. () Yönlendirici cihazda bütün yapılandırmalar ayrıcalıklı kullanıcı modu kullanılarak yapılabilir.
5. () Yönlendirici cihaza enable secret ile verilen şifreler başlangıç yapılandırmasında kriptolanarak görüntülenir.

B) Aşağıdaki soruları dikkatlice okuyarak doğru seçeneği işaretleyiniz.

6. Yönlendirici arayüzü “FastEthernet 0/0 is up, lineprotocol is up” mesajını veriyorsa aşağıdaki durumlardan hangisi gerçekleşmiştir?

- A) Bağlantı hatası olmuştur. B) Arayüz çalışıyor. C) Arayüz çalışmıyor.
D) Arayüz problemi bulunuyor. E) Kablo sorunu vardır.

7. Aşağıdakilerden hangisi 2. katman saldırılarına verilen isimlerden biridir?

- A) username MEB enable 8
B) username MEB privilege
C) hostname MEB privilege 8
D) username MEB secret 8
E) username MEB password 8

8. Yönlendirme rotaları aşağıdaki hangi yardım komutu sayesinde görüntülenir?

- A) show host B) show map C) show ip route
D) show interface E) show ip brief

9. Aşağıdakilerden hangisi arayüzlere tanımlama yapmak için kullanılan komut parametresidir?

- A) Description B) Interface C) Running-config D) Console E) Privilege

10. Yönlendirici cihazda kaç tane kullanıcı ayrıcalık seviyesi vardır?

- A) 15 B) 10 C) 8 D) 2 E) 0



KONULAR

4.1. YÖNLENDİRME İŞLEMLERİ

4.2. YOL TANIMLAMA PROTOKOLLERİ

4.3. STATİK YÖNLENDİRME İŞLEMLERİ

ANAHTAR KELİMELER

- Yönlendirici
- Rota
- Statik yönlendirme
- Yönetimsel uzaklık
- NAT
- Dynamic NAT
- Overloading NAT
- PAT
- Yönlendirme tablosu
- Varsayılan yönlendirme

4. ÖĞRENME BİRİMİ

YÖNLENDİRME TEMELLERİ VE STATİK YÖNLENDİRME

NELER ÖĞRENECEKSİNİZ?

- Ağ uygun yönlendirme
- Yönlendirme tabloları
- Yönlendirme komutları
- Ağ adreslemesine göre statik yönlendirme
- Komut kullanarak statik yönlendirme
- Varsayılan yönlendirme
- NAT yönlendirme protokolleri
- Statik NAT, dinamik NAT ve PAT yönlendirme protokolleri



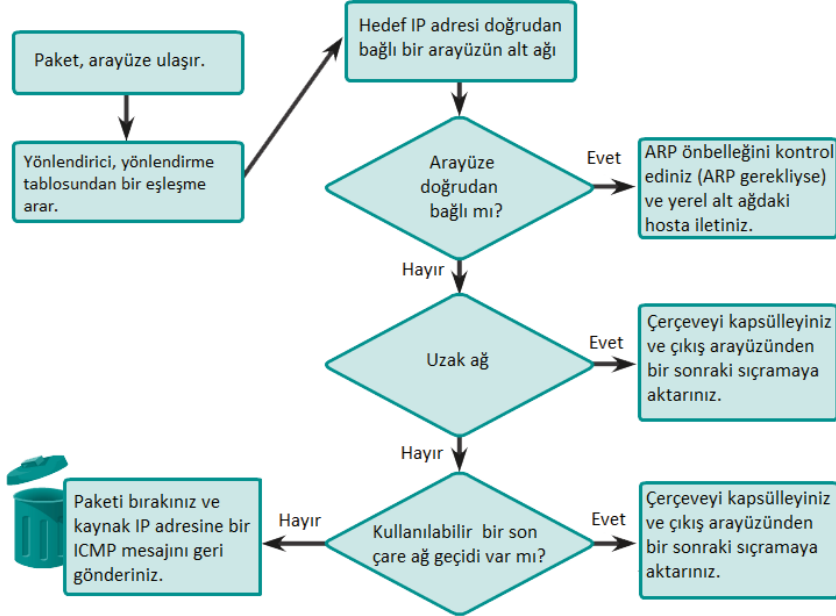


HAZIRLIK ÇALIŞMALARI

1. Yerel ağ bağlantısı hakkında bildiklerinizi arkadaşlarınızla paylaşınız.
2. Yönlendirici hakkında bildiklerinizi arkadaşlarınızla paylaşınız.

4.1. YÖNLENDİRME İŞLEMLERİ

Fiziksel olarak birbirine uzak mesafedeki cihazlar arasında veri alışverişi yapmak için yerel ağ bağlantıları yetersiz kalır. Bu durumda yönlendirici adı verilen cihazlar ile birlikte yönlendirmeye ihtiyaç duyulur. Kaynak cihaz, uzaktaki hedef cihaza bir paket gönderdiğinde yönlendiricilerin ve yönlendirmenin yardımına ihtiyaç duyar. Yönlendiricinin temel işlevlerinden biri, paketleri göndermek için kullanacağı en iyi yolu tespit etmektir. Yönlendirici, paketi hedef IP adresi ile eşleşen ağ adresine ulaştırmak için kullanacağı en iyi yolu yönlendirme tablosunda arar.



Görsel 4.1: Yönlendirici paket iletme karar işlemi

Yönlendirici, bir paket aldığı anda paketi ileteceği yeri belirlemek için paketteki hedef IP adresini inceler. Sonrasında yönlendirme tablosunda eşlenen hedef değeri arar. Yönlendirme tablosunda bulunan her hedef değeri, bir hedef ağ adresini temsil eder.

4.1.1. Yönlendirme Tabloları

Yönlendirme tabloları yönlendiriciye doğrudan bağlı veya öğrenilen uzak ağlar ile ilgili rota bilgilerini saklamak için kullanılır. Yönlendirme tabloları yönlendiricinin geçici hafızasında (RAM) tutulur. Yönlendirme tablosunda ağ veya bir sonraki sıçrama noktası bilgisi bulunur. Sonraki sıçrama noktası, sonraki hedef IP adresi veya çıkış arayüzü olarak tanımlanır.

Yönlendiricideki rotaların dört temel bileşeni şunlardır:

- Hedef değeri
- Alt ağ maskesi
- Ağ geçidi veya arayüz adresi
- Rota maliyeti ve metrik



BİLGİ

Yönlendirme tabloları bir kaynak ağ ile hedef arasındaki yolun tamamını temsil eden bilgileri içermez. Yalnızca yol üzerinde bulunan bir sonraki sekme hakkında bilgiler içerir. Bir sonraki sekme ise yönlendirme tablosundaki doğrudan bağlı bir ağıdır.

4.1.2. Yönlendirme Komutları

Statik yönlendirme için “ip route” komutu kullanılır. Dinamik yönlendirme ise yönlendirme protokolleri ile gerçekleşir.

Küçük ölçekli ağlarda statik yönlendirme ideal bir çözümdür fakat büyük ölçekli ağlarda statik yönlendirme kullanılması, ağın iletişiminin yönetilmesinde hataya neden olabilir. Bu nedenle büyük ölçekli ağlarda dinamik yönlendirme kullanılır.

Küçük ağlar için ideal çözüm olan statik yönlendirme Routing “ip route” komutu kullanılarak Küresel Konfigürasyon modunda yapılır.

Statik yönlendirme yapılırken hedef ağın IP adresi, alt ağ adresi ve hedefe ulaşmak için bir sonraki yönlendiricinin IP adresi kullanılır.

Router(config)#ip route [hedef ağ adresi][hedef ağ alt ağ maskesi][sonraki atlama noktası IP veya çıkış arayüzü] [uzaklık]

Statik yönlendirme komutu yönlendirme tablosundan silinmek istenirse “ip route” komutunun başına “no” ifadesini yazmak yeterlidir.

Komutun kullanımında uzaklık (distance) ifadesini yazmak seçimsel olup gerektiği durumlarda yönlendirme protokolleri arasında öncelik belirlemek için yönetimsel uzaklık değeri değiştirilebilir. Statik yönlendirme için yönetimsel uzaklık değeri varsayılan olarak 1’dir.

Yönetimsel Uzaklık Yönlendirme Kaynağı (Administrative Distance Route Source)	Varsayılan Mesafe (Default Distance)
Bağlı arayüz (Connected interface)	0
Statik (Static)	1
EIGRP Summary	5
External BGP	20
Internal EIGRP	90
IGRP	100
OSPF	110
IS-IS	115
RIP	120
External EIGRP	170
Internal BGP	200
Bilinmeyen (Unknown)	255

Görsel 4.2: Varsayılan yönetimsel uzaklık değerleri

Görsel 4.2’de listelenen yönetsel uzaklık değeri farklı dinamik yönlendirme protokolleri arasında yönlendiricinin öncelikli olarak seçim yapmasını sağlar. Yönlendiriciye doğrudan bağlı ağlar için yönetsel uzaklık değeri 0’dır. Yönlendiricideki statik rotalar için yönetsel uzaklık değeri ise 1’dir.

Yönlendiricide “**show ip route**” komutu ile yönlendirme tablosundaki rotalar görüntülenir.

4.2. YOL TANIMLAMA PROTOKOLLERİ

4.2.1. Doğrudan Bağlı Rotalar

Yönlendiriciye doğrudan bağlı yerel ağ adresleri, yönlendirme tablosunda direkt bağlı rotalar olarak saklanır. Bu rotalar, yönlendirme tablosunda “**C**” harfi ile temsil edilir. Yönlendirme tablosundaki rotalar, arayüz yeniden yapılandırıldığında veya kapatıldığında her seferinde otomatik olarak güncellenir. Görsel 4.3’te R1 yönlendiricisine doğrudan bağlı rotalar listelenmiştir. Görselde R1 yönlendiricisine 10.0.0.0/8 ve 60.0.0.0/8 ağlarının doğrudan bağlı olduğu görülür.

```
R1#
R1#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
        i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
        * - candidate default, U - per-user static route, o - ODR
        P - periodic downloaded static route

Gateway of last resort is not set

C    10.0.0.0/8 is directly connected, Serial0/0/0
C    60.0.0.0/8 is directly connected, FastEthernet0/0
```

Görsel 4.3: R1 yönlendiricisine doğrudan bağlı rotalar

4.2.2. Statik Rotalar

Ağ yöneticileri belirli bir hedef ağı giden statik bir rotayı manuel yapılandırabilir. Statik rotalar yönetici tarafından manuel tekrar yapılandırılınca kadar değişmez. Bu rotalar yönlendirme tablosunda “**S**” harfi ile temsil edilir.

Statik rotalar iki ağ cihazı arasındaki kesin bir yolu ifade eder. Statik rotalar otomatik olarak güncellenmez. Ağ topolojisinde değişiklik olduğunda statik rotaların manuel güncellenmesi gerekir. Statik rotalar, güvenlik ve kaynak verimliliği sağlar. Statik rotalar, dinamik yönlendirme protokollerine göre daha az bant genişliği kullanır. Statik rotaların hesaplanması için işlemci döngüsü kullanılmaz. Statik rotaların sunduğu avantajlar yanında ağ topolojisinin değişmesi durumunda otomatik yeniden yapılandırma olanağını sunmayı dezavantaj sayılabilir.

Görsel 4.4’te R1 yönlendiricisindeki statik rotalar “**S**” ön eki ile listelenmiştir. Görselde R1 yönlendiricisinden 192.168.2.0/24 ağına 192.168.1.2 IP adresi aracılığı ile erişilebileceği görülür. “**via**” kelimesinden sonra gelen IP adresi, rotanın öğrenildiği yönlendiricinin rotayı gönderdiği arayüzünün IP adresidir.

```

R1#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
        i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
        * - candidate default, U - per-user static route, o - ODR
        P - periodic downloaded static route

Gateway of last resort is not set

    172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       172.16.1.0/24 is directly connected, GigabitEthernet0/0
L       172.16.1.1/32 is directly connected, GigabitEthernet0/0
    192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, Serial0/0/0
L       192.168.1.1/32 is directly connected, Serial0/0/0
S       192.168.2.0/24 [1/0] via 192.168.1.2

```

Görsel 4.4: R1 yönlendiricisindeki statik rota

4.2.3. Dinamik Olarak Güncellenmiş Rotalar

Dinamik rotalar, yönlendirme protokolleri tarafından otomatik olarak oluşturulur. Dinamik rotalar, yönlendirme tablosunda yönlendirme protokolüne karşılık gelen ön ek ile tanımlanır. Örneğin dinamik yönlendirmede RIP protokolü kullanılmışsa bu protokol, yönlendirme tablosunda “R” ön eki ile temsil edilir.

Görsel 4.5’te R1 yönlendiricisindeki doğrudan bağlı rotalar “C” ön eki ile listelenmiştir. Görselde R1 yönlendiricisinden 10.0.0.0/8 ağına 192.168.1.249 IP adresi aracılığı ile erişilebileceği, 20.0.0.0/8 ağına ise 192.168.1.245 IP adresi aracılığı ile erişilebileceği görülür. “via” kelimesinden sonra gelen IP adresi, rotanın öğrenildiği yönlendiricinin rotayı gönderdiği arayüzünün IP adresidir.

```

R1#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
        i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
        * - candidate default, U - per-user static route, o - ODR
        P - periodic downloaded static route

Gateway of last resort is not set

R       10.0.0.0/8 [120/1] via 192.168.1.249, 00:00:08, Serial0/0/0
R       20.0.0.0/8 [120/1] via 192.168.1.245, 00:00:09, Serial0/0/1
    192.168.1.0/30 is subnetted, 3 subnets
C       192.168.1.244 is directly connected, Serial0/0/1
C       192.168.1.248 is directly connected, Serial0/0/0

```

Görsel 4.5: R1 yönlendiricisindeki R ön ekiyle gösterilen dinamik rotalar

4.2.4. Varsayılan Rotalar

Varsayılan rota, yönlendirme tablosunda hedef için bir rota bulunmadığında kullanılan bir statik rota tipidir. Genellikle varsayılan rotalar internet servis sağlayıcıya (ISP) giden yolda bir sonraki yönlendiriciyi gösterir. Bir alt ağda yalnız bir yönlendirici varsa bu yönlendirici otomatik olarak varsayılan ağ geçidi olur çünkü o yerel ağa giren ve çıkan tüm ağ trafiği bu yönlendirici üzerinden geçmek zorundadır.

Varsayılan yönlendirme yapılırken hedef ağın IP adresi ve alt ağ adresi “0.0.0.0” şeklinde yazılır. Hedefe ulaşmak için bir sonraki yönlendiricinin IP adresi kullanılır.

Router(config)#IP route [0.0.0.0][0.0.0.0][sonraki atlama noktası IP veya çıkış arayüzü] [uzaklık]

Görsel 4.6’da R1 yönlendiricisindeki varsayılan rotalar S* ön eki ile listelenmiştir.

```
R1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

C    10.0.0.0/8 is directly connected, Serial0/0/0
C    60.0.0.0/8 is directly connected, FastEthernet0/0
S*   0.0.0.0/0 is directly connected, Serial0/0/0
```

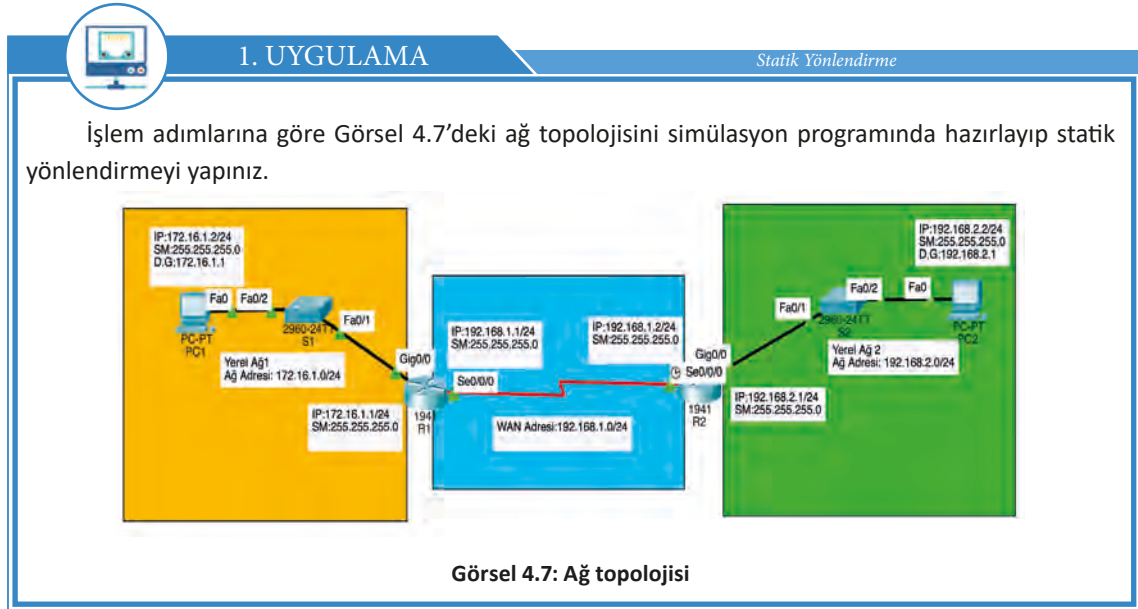
Görsel 4.6: R1 yönlendiricisindeki varsayılan rota

4.3. STATİK YÖNLENDİRME İŞLEMLERİ

4.3.1. Statik Yönlendirme Uygulaması

Statik rotalar manuel olarak yapılandırılır. Statik rotalar manuel olarak yapılandırıldığı için ağ topolojisi içinde değişiklik meydana geldiğinde küçük ağlarda bunları yansıtmak kolaydır fakat büyük ağlarda bu değişiklikleri yapmak zorlaşır. Buna bağlı olarak büyük ağlarda yönlendirme tablosunun bakımı fazla zaman alır. Bu nedenle büyük ağlarda statik yönlendirme yerine dinamik yönlendirme tercih edilir.

Statik yönlendirmeyi etkinleştirmek için yönlendiricinin komut ekranı konfigürasyon satırında “**ip route**” komutu kullanılır. Komuttan sonra hedef ağ adresi bilgisi, maskesi ve sonrasında da hedef ağı erişim için bir sonraki atlama noktasının IP adresi veya yönlendiricinin çıkış arayüzü yazılır.



1. Adım: Görsel 4.7'deki cihazların üzerinde arayüz, IP, alt ağ maskesi ve varsayılan ağ geçidi bilgileri verilmiştir. Statik yönlendirme uygulaması için fiziksel ve mantıksal topolojiyi simülasyon programını kullanarak oluşturunuz.

2. Adım: CLI arayüzüne girerek sırasıyla R1 cihazının arayüzlerine IP bilgilerini atamak için şu kodları uygulayınız:

```
R1(config)#int Se0/0/0
R1(config-if)#ip add 192.168.1.1 255.255.255.0
R1(config-if)#no sh
R1(config-if)#exi
R1(config)#int Gig 0/0
R1(config-if)#ip add 172.16.1.1 255.255.255.0
R1(config-if)#exi
```

3. Adım: CLI arayüzüne girerek sırasıyla R2 cihazının arayüzlerine IP bilgilerini atamak için şu kodları uygulayınız:

```
R2(config)#int Se0/0/0
R2(config-if)#ip add 192.168.1.2 255.255.255.0
R2(config-if)#no sh
R2(config-if)#exi
R2(config)#int Gig 0/0
R2(config-if)#ip add 192.168.2.1 255.255.255.0
R2(config-if)#exit
```

4. Adım: CLI arayüzüne girerek sırasıyla R1 ve R2 cihazında statik yönlendirmeyi yapmak için şu kodları uygulayınız:

```
R1(config)#ip route 192.168.2.0 255.255.255.0 192.168.1.2
R2(config)#ip route 192.168.2.0 255.255.255.0 192.168.1.1
```

5. Adım: CLI arayüzüne girerek sırasıyla R1 ve R2 cihazında yönlendirme tablosundaki "S" ile gösterilen statik rotayı görmek için Görsel 4.8 ve Görsel 4.9'da verilen R1 ve R2'ye şu kodları yazınız:

R1# sh ip route

```
R1#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
        i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
        * - candidate default, U - per-user static route, o - ODR
        P - periodic downloaded static route

Gateway of last resort is not set

    172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       172.16.1.0/24 is directly connected, GigabitEthernet0/0
L       172.16.1.1/32 is directly connected, GigabitEthernet0/0
    192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, Serial0/0/0
L       192.168.1.1/32 is directly connected, Serial0/0/0
S       192.168.2.0/24 [1/0] via 192.168.1.2
```

Görsel 4.8: R1 yönlendirici tablosundaki statik yönlendirme satırı

R2# sh ip route

```

R2#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

    172.16.0.0/24 is subnetted, 1 subnets
S       172.16.1.0/24 [1/0] via 192.168.1.1
    192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, Serial0/0/0
L       192.168.1.2/32 is directly connected, Serial0/0/0
    192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.2.0/24 is directly connected, GigabitEthernet0/0
L       192.168.2.1/32 is directly connected, GigabitEthernet0/0

```

Görsel 4.9: R2 yönlendirici tablosundaki statik yönlendirme satırı

6. Adım: PC1'den PC2'ye "ping" komutunu kullanarak iletişim testi gerçekleştiriniz. İletişim testinin başarılı olduğunu göreceksiniz. Statik yönlendirme sayesinde farklı yerel ağlar arasında haberleşmek için yönlendirme işlemi gerçekleşmiştir. Görsel 4.10 ile Görsel 4.11'de verilen PC1 ve PC2'nin birbirleriyle haberleşebildiğini doğrulayınız.

```

Packet Tracer PC Command Line 1.0
C:\>ping 192.168.2.2

Pinging 192.168.2.2 with 32 bytes of data:

Reply from 192.168.2.2: bytes=32 time=47ms TTL=126
Reply from 192.168.2.2: bytes=32 time=49ms TTL=126
Reply from 192.168.2.2: bytes=32 time=8ms TTL=126
Reply from 192.168.2.2: bytes=32 time=51ms TTL=126

Ping statistics for 192.168.2.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 8ms, Maximum = 51ms, Average = 38ms

```

Görsel 4.10: Statik yönlendirme sayesinde PC2 ile kurulan iletişim

```

Packet Tracer PC Command Line 1.0
C:\>ping 172.16.1.2

Pinging 172.16.1.2 with 32 bytes of data:

Reply from 172.16.1.2: bytes=32 time=57ms TTL=126
Reply from 172.16.1.2: bytes=32 time=69ms TTL=126
Reply from 172.16.1.2: bytes=32 time=64ms TTL=126
Reply from 172.16.1.2: bytes=32 time=38ms TTL=126

Ping statistics for 172.16.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 38ms, Maximum = 69ms, Average = 57ms

```

Görsel 4.11: Statik yönlendirme sayesinde PC1 ile kurulan iletişim

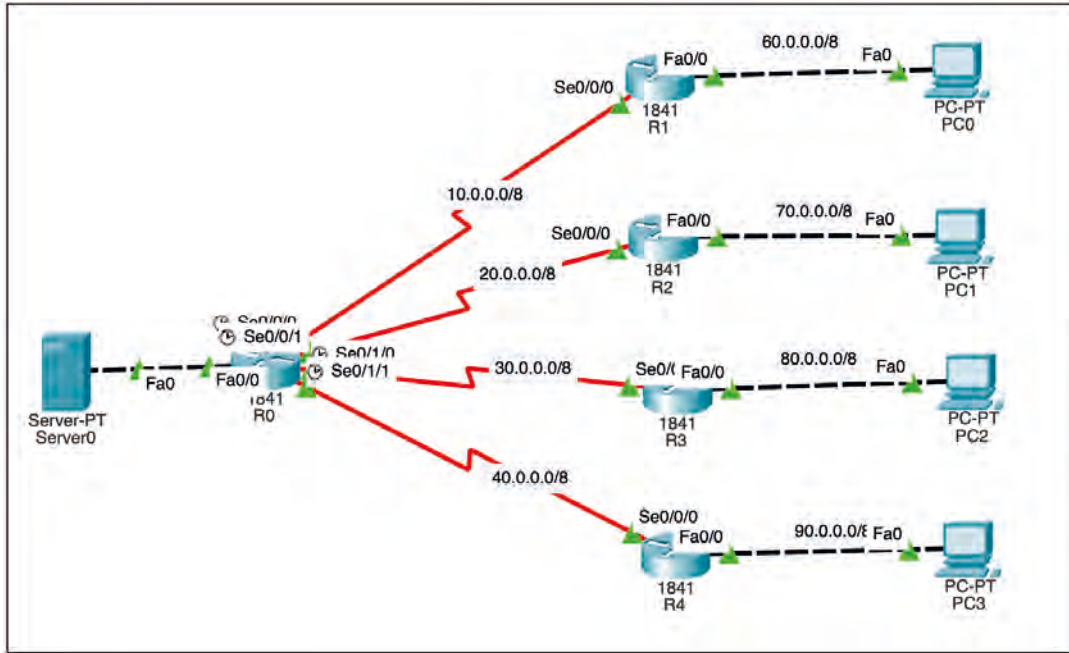
4.3.2. Varsayılan Yönlendirme Uygulaması



2. UYGULAMA

Varsayılan Yönlendirme

İşlem adımlarına göre Görsel 4.12'deki ağ topolojisini simülasyon programında hazırlayıp varsayılan yönlendirmeyi yapınız.



Görsel 4.12: Ağ topolojisi

1. Adım: Görsel 4.12'deki cihazlar için arayüz, IP, alt ağ maskesi ve varsayılan ağ geçidi bilgileri Tablo 4.1'de verilmiştir. Uygulama için fiziksel ve mantıksal topolojiyi simülasyon programını kullanarak oluşturunuz.

Tablo 4.1: Görsel 4.12'deki Cihazlar İçin Arayüz, DCE, IP, Alt Ağ Maskesi ve Varsayılan Ağ Geçidi Bilgileri

Cihaz	Arayüz	DCE	IP	Alt Ağ Maskesi	Varsayılan Ağ Geçidi
R0	Se0/0/0	Evet	10.0.0.1	255.0.0.0	-
	Se0/0/1	Evet	20.0.0.1	255.0.0.0	-
	Se0/1/0	Evet	30.0.0.1	255.0.0.0	-
	Se0/1/1	Evet	40.0.0.1	255.0.0.0	-
	F0/0	Evet	50.0.0.1	255.0.0.0	-
R1	Se0/0/0	-	10.0.0.2	255.0.0.0	-
	F0/0	-	60.0.0.1	255.0.0.0	-
R2	Se0/0/0	-	20.0.0.2	255.0.0.0	-
	F0/0	-	70.0.0.1	255.0.0.0	-
R3	Se0/0/0	-	30.0.0.2	255.0.0.0	-
	F0/0	-	80.0.0.1	255.0.0.0	-
R4	Se0/0/0	-	30.0.0.2	255.0.0.0	-
	F0/0	-	80.0.0.1	255.0.0.0	-
Server0	-		50.0.0.2	255.0.0.0	50.0.0.1
PC0	-		60.0.0.2	255.0.0.0	60.0.0.1
PC1	-		70.0.0.2	255.0.0.0	70.0.0.1
PC2	-		80.0.0.2	255.0.0.0	80.0.0.1
PC3	-		90.0.0.2	255.0.0.0	90.0.0.1

2. Adım: CLI arayüzüne girerek sırasıyla R0 cihazının arayüzlerine IP bilgilerini atamak için şu kodları uygulayınız:

```
R0(config)#int Se0/0/0
R0(config-if)#ip add 10.0.0.1 255.0.0.0
R0(config-if)#no sh
R0(config-if)#exi
```

```
R0(config)#int Se0/0/1
R0(config-if)#ip add 20.0.0.1 255.0.0.0
R0(config-if)#no sh
R0(config-if)#exi
```

```
R0(config)#int Se0/1/0
R0(config-if)#ip add 30.0.0.1 255.0.0.0
R0(config-if)#no sh
R0(config-if)#exi
```



```

R0(config)#int Se0/1/1
R0(config-if)#ip add 40.0.0.1 255.0.0.0
R0(config-if)#no sh
R0(config-if)#exi

R0(config)#int F0/0
R0(config-if)#ip add 50.0.0.1 255.0.0.0
R0(config-if)#no sh
R0(config-if)#exi

```



SIRA SİZDE

CLI arayüzüne girerek sırasıyla R1, R2 ve R3 cihazının arayüzlerine IP bilgilerini atayan kodları uygulayınız.

3. Adım: CLI arayüzüne girerek R1, R2, R3 ve R4 cihazlarında varsayılan yönlendirme komutlarını uygulayınız. Varsayılan yönlendirme yapılandırması için iki seçeneği olan yönlendirme komutunu kullanabilirsiniz. Yönlendirme komutunda çıkış arayüzünü kullanmak isterseniz R0 cihazına bağlı arayüzün adını belirtiniz. Sonraki sekmenin IP adresini kullanmak isterseniz yerel yönlendiriciye bağlı R0 yönlendiricisinin arayüz IP adresini kullanınız.

Yönlendirici (config)# ip route 0.0.0.0 0.0.0.0 [çıkış arabirimi veya sonraki atlama noktasının IP adresi]

```

R1(config)#ip route 0.0.0.0 0.0.0.0 Se0/0/0
R2(config)#ip route 0.0.0.0 0.0.0.0 Se0/0/0
R2(config)#ip route 0.0.0.0 0.0.0.0 30.0.0.1
R2(config)#ip route 0.0.0.0 0.0.0.0 40.0.0.1

```

4. Adım: Görsel 4.13'te görüldüğü gibi PC0'dan R0 yönlendiricisine bağlı sunucuya ping atınız. Ping isteğinin başarılı olmadığını gözlemleyiniz.

```

Packet Tracer PC Command Line 1.0
C:\>ping 50.0.0.2

Pinging 50.0.0.2 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 50.0.0.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>

```

Görsel 4.13: PC0 ile Server0 arasında kurulamayan iletişim

5. Adım: R0'ın kendine gelen paketleri komşu yönlendiricilere yönlendirebilmesi için R0 cihazında CLI arayüzüne girerek şu statik yönlendirme komutlarını uygulayınız:

```
R0(config)#ip route 60.0.0.0 255.0.0.0 10.0.0.2
R0(config)#ip route 70.0.0.0 255.0.0.0 20.0.0.2
R0(config)#ip route 80.0.0.0 255.0.0.0 30.0.0.2
R0(config)#ip route 90.0.0.0 255.0.0.0 40.0.0.2
```

6. Adım: PC0'dan Server0'a ping atınız. Server0'dan da PC0'a ping atarak PC0 ile Server0 arasındaki iletişimin sorunsuz çalıştığını doğrulayınız.



SIRA SİZDE

PC1, PC2 ve PC3'ten Server0'a ping atınız (Görsel 4.14). Server0'dan PC1, PC2 ve PC3'e ve PC'lerden de Server0'a ping atarak iki yönlü iletişimin sorunsuz çalıştığını doğrulayınız (Görsel 4.15).

```
Packet Tracer PC Command Line 1.0
C:\>ping 50.0.0.2

Pinging 50.0.0.2 with 32 bytes of data:

Reply from 50.0.0.2: bytes=32 time=62ms TTL=126
Reply from 50.0.0.2: bytes=32 time=38ms TTL=126
Reply from 50.0.0.2: bytes=32 time=43ms TTL=126
Reply from 50.0.0.2: bytes=32 time=2ms TTL=126

Ping statistics for 50.0.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 62ms, Average = 36ms
```

Görsel 4.14: PC0 ve Server0 arasında ping komutuyla doğrulanan iletişim

```
C:\>ping 60.0.0.2

Pinging 60.0.0.2 with 32 bytes of data:

Reply from 60.0.0.2: bytes=32 time=189ms TTL=126
Reply from 60.0.0.2: bytes=32 time=147ms TTL=126
Reply from 60.0.0.2: bytes=32 time=170ms TTL=126
Reply from 60.0.0.2: bytes=32 time=215ms TTL=126

Ping statistics for 60.0.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 147ms, Maximum = 215ms, Average = 180ms
```

Görsel 4.15: Server0 ve PC0 arasında ping komutuyla doğrulanan iletişim

4.3.3. NAT (Ağ Adresi Dönüştürme) Protokolü

NAT (Network Address Translation) protokolü, yerel ağda kullanılan özel (private) IP adreslerini internet ortamında yönlendirilebilir (routable) genel (public) IP adresine çevirmektir. Bir başka deyişle NAT, ağa bağlı cihazın kullandığı IP adresini istenilen farklı bir adrese dönüştürür.

IPv4 sisteminde kullanılabilir durumda yaklaşık üç milyar IP bulunur. Ağ sistemlerinde kullanılan birbiriyle bağlantılı cihazların artması ile IPv4 sisteminde yer alan IP adreslerinin yetersizliği ortaya çıkınca

çözüm için NAT protokolü geliştirilmiştir. Ağ iletişimde bazı adresler sadece yerel ağlarda kullanılır. Bu adreslere özel adresler (private IP address) denir.

Özel IP adresleri RFC 1918 ile belirlenmiştir. Bunlar;

- 10.0.0.0/8 -> 10.0.0.0 ile 10.255.255.255,
- 172.16.0.0/12 -> 172.16.0.0 ile 172.31.255.255,
- 192.168.0.0/16 -> 192.168.0.0 ile 192.168.255.255 arasındadır.

Birçok işletme ve kurum, kendi yerel ağlarında özel IP adres aralıklarını kullanır. Bu işletme ve kurumlar dış bağlantılarında ise NAT protokolünü destekleyen yönlendiriciler ile yerel ağlarında kullandıkları IP adreslerini genel IP adreslerine (public address) çevirir.

NAT yönlendiricisi, NAT tablosu kullanarak IP adres çevirme işlemini gerçekleştirir. Yerel ağ cihazında özel IP adresleri aralığından bir adres bulunur. Cihaz, yerel ağın içinde olmayan bir cihaz ile iletişim kurmak istediğinde NAT yönlendiricisi kullanıcı tarafından ayarlanan NAT tablosuna bakarak özel IP adresini genel bir IP adresine çevirir. Bu şekilde cihaz dış ağlara veya internete erişim sağlar. Yönlendiricinin çeviri yaparak değiştirdiği IP adresi, cihazın internetteki IP'sidir. Dış ağlardan veya internetten cihaza erişim için bir istek geldiğinde yönlendirici NAT tablosuna bakarak IP'yi kullanıcının özel IP adresine yönlendirir ve mesaj paketini kullanıcının bilgisayarına gönderir.

- **İç Yerel Adres (Inside Local IP Address):** NAT tarafından özel IP adresleri aralığı içinden kullanıcıya yerel ağda kullanması için atanmış IP adresleridir.
- **İç Global Adres (Inside Global IP Address):** NAT'ın dış ağlara bakan yüzünde bulunan ve dış ağlara bağlanırken kullanılan genel IP adresleridir.
- **Dış Global Adres (Outside Global IP Address):** İnternette bulunan herhangi bir kullanıcının veya sunucunun sahip olduğu genel IP adresleridir.

NAT'ın avantajları şunlardır:

- Az sayıda genel IP kullanılarak çok sayıda cihazın internete erişimi sağlanır. Bu sayede cihazların IP yetersizliği sorunu azaltılır. İntranet adı verilen özel IP adreslerinden oluşmuş yerel ağlar ve mümkün olduğunca az sayıda genel IP adresi kullanılarak dış ağlara erişim sağlanır.
- Yerel ağda kullanılan özel IP adresleri ile dış ağlara yönlendirici tarafından çevrilmiş IP adreslerinin bağlantısını kurar. Bu durum, ağın topolojisini dış ağlara karşı gizleyerek yerel ağdaki cihazları koruyacak bir güvenlik sağlar.
- NAT ile genel ağa erişimlerde esneklik sağlanır. Çoklu IP havuzları, yedek IP havuzları ve yük dengeleme havuzları sayesinde güvenilir bir ağ bağlantısı oluşturmak için de NAT kullanılır.

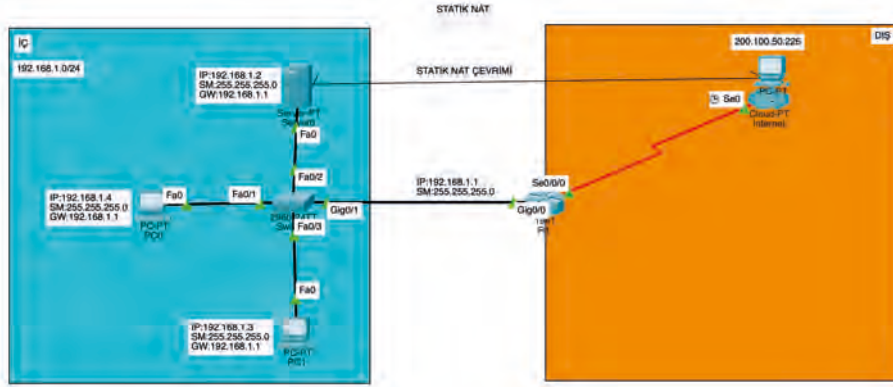
NAT'ın dezavantajları şunlardır:

- IP adresi ve port numaraları değiştirildiği için FTP ve bazı oyun protokolleri çalışmaz. Bazı internet protokollerinin ve uygulamalarının çalışabilmesi için kaynak ve hedef IP adreslerine ihtiyaç duyulur. Örneğin sayısal imza gibi bazı uygulamalar NAT tarafından kaynak IP adresi değiştirildiği için NAT kullanılan yerel ağlarda çalışmaz. Bazen bu sorun sabit (static) NAT kullanılarak ortadan kaldırılabilir.
- Genel IP ile birçok kullanıcının internete erişim sağlamasından dolayı internete erişim sağlayan IP'ler izlenemez. NAT tarafından IP adreslerinin çevrilmesi ile IP paketlerinin izlenmesi veya kaynak IP adresinin bulunması zorlaşır.

- NAT işlemi cihazlar arası iletişimde gecikmelere sebep olabilir. IP paket başlıklarının çevrilmesi ve etiketlenmesi sırasında gecikmeler oluşabilir.
- NAT kullanımı, IPsec gibi tünelleme protokollerinin kullanımını karmaşık hâle getirir.
- NAT kullanılması istenen ağ topolojisini de NAT için uygun tasarlamak gerekir.

NAT tablosundaki eşleştirmeler ağ yöneticisinin veya kullanıcının tercihiyle göre üç farklı şekilde yapılabilir.

4.3.3.1. Statik NAT (Static NAT)



Görsel 4.16: Statik NAT çevirimi

Statik NAT çevirimi, yerel ağda kullanılan özel IP'yi dışarıda kullanılacak genel IP'ye bire bir çevirmez. Bu NAT türünde NAT tablosu doğrudan ağ yöneticisi tarafından doldurulur. Bir başka deyişle ağ yöneticisi, kullanılacak özel IP'leri belirler ve bunları sahip olduğu genel IP adresleriyle kendi eşleştirir. Bu şekilde belirlenmiş adresler dışında hiçbir IP adresi dış ağlara bağlanamaz. Görsel 4.16'da statik NAT tablosunda verilen adresler, dış ağlara her zaman karşısında belirlenen genel IP adresleriyle bağlanır ve bu genel adreslere gelen istekler NAT yönlendiricisi tarafından doğruca eşleştirildiği özel IP adresine yönlendirilir.

Tablo 4.2: Görsel 4.16'daki Cihazlar İçin Statik NAT Bilgileri

İç Yerel Adres	İç Genel Adres R1 Üzerinden Erişilen Adresler
192.168.1.2	200.100.50.226
192.168.1.3	200.100.50.227
192.168.1.4	200.100.50.228

Statik NAT çevirimini manuel yapabilmek için her bir yerel IP adresinin (çevrilmesi gereken) iç küresel IP adresiyle eşlemesi gerekir. Dâhilî yerel IP adresini dâhilî küresel IP adresiyle eşleştirmek için şu komut kullanılır:

Router(config)#ip nat inside source static [iç yerel ip adres] [iç küresel IP adres]

Statik NAT yapılandırmasının adımları şunlardır:

1. IP adresleri tanımlanır.
2. Yerel arayüz adresleri tanımlanır.
3. Küresel arayüz adresleri tanımlanır.



ÖRNEK

• Birinci adımda LP1 bilgisayarına 10.0.0.10 IP adresi verilir. Bu durumda LP1'i 50.0.0.10 IP adresi ile eşleştirmek için şu komut kullanılır:

Yönlendirici (config)#ip nat inside source static 10.0.0.10 50.0.0.10

• İkinci adımda yerel ağa bağlı arayüz tanımlanır. Her iki yönlendiricide de Fa0/0 arayüzü, IP çevirisine ihtiyaç duyan yerel ağa bağlıdır. Bu nedenle Fa0/0 yerel arayüzü için şu komut kullanılır:

Yönlendirici (config-if) #ip nat inside

• Üçüncü adımda ise küresel ağa bağlı arayüz tanımlanır. Her iki yönlendirici için Seri0/0/0 arayüzü küresel ağa bağlanır. Bu nedenle Seri0/0/0 arayüzü şu komutla küresel olarak tanımlanır:

Yönlendirici (config-if) #ip nat global

4.3.3.2. Dinamik NAT (Dynamic NAT)

Dinamik NAT türündeki genel IP adres bloku dinamik bir şekilde özel IP adresleriyle eşleştirilir. Ağ yöneticisinin belirlediği IP adres havuzu ile NAT yönlendiricisi otomatik olarak IP adreslerini eşler ve dış ağlara bağlantısını sağlar. Dinamik NAT'ta sabit NAT'tan farklı olarak IP eşleştirmesi yönlendirici tarafından yapılır. IP adresleri arasında gerçekleşen eşleşme sırasına göre cihazlar internete erişim sağlar. IP adres havuzunda yeterli sayıda genel IP adresi bulunuyorsa özel IP'lerin tamamı eşleştirilerek internete erişim sağlanabilir. Bağlantı kesildikten sonra NAT tablosundaki kayıtlar bir sonraki bağlantı kuruluncaya kadar silinir.

Dinamik NAT yapılandırmasının adımları şunlardır:

1. NAT çevirisinde kullanılacak IP adresleri için bir erişim kontrol listesi belirleme

Yönlendirici(config)# access-list erişim-kontrol-listesi-türü permit/deny eşleşen-parametreler

2. NAT çevirisi için kullanılacak IP adreslerini içeren bir havuz oluşturma

Yönlendirici (config)#ip nat pool [Havuz Adı] [Başlangıç IP adresi] [Son IP adresi] netmask [Alt ağ maskesi]

3. Dinamik NAT yapılandırması

Yönlendirici (config)#ip nat inside source list [erişim kontrol listesinin adı veya sayısı] pool [havuz adı]

4. İç ve dış arayüzlerin tanımlanması

Yönlendirici (config-if)#ip nat inside

Yönlendirici (config-if)#ip nat outside

4.3.3.3. Aşırı Yükleme NAT (Overloading NAT)

Bu NAT türüne aynı zamanda PAT (Port Address Translation-Port Adres Çevirimi) da denir. PAT'ta genel IP adresi olarak bir tane IP bulunur. Dinamik NAT'ta olduğu gibi yönlendirici NAT tablosunu kendi oluşturur. Yerel ağda bulunan bir kullanıcıdan dışarıdaki ağlara bağlanmak için bir istek geldiğinde yönlendirici bu kullanıcının özel IP adresini ve ona verdiği port numarasını NAT tablosuna kaydeder. Genel IP adresini yerel ağda bulunan kullanıcının özel IP adresi ve ona verdiği port numarası ile eşleştirerek internete erişimi sağlar. Farklı bir özel IP'den aynı anda istek geldiği takdirde o IP'ye farklı bir port numarası verilir. PAT sayesinde bütün yerel ağ daha az sayıda genel IP adresi kullanarak internete bağlanır. NAT tablosuna kaydedilen bu IP adresleri ve port numaraları bağlantının sonuna kadar kayıtlı kalır, bağlantı kesilince silinir. Ağ yöneticisi isterse IP adreslerini kendi belirlediği port numaralarına kalıcı olarak atayabilir.

PAT'ı yapılandırma adımları şunlardır:

- “ip nat inside” komutu kullanılarak yönlendiricinin iç arayüzü yapılandırılır.
- “ip nat outside” komutu kullanılarak yönlendiricinin dış arayüzü yapılandırılır.
- Çevrilecek iç kaynak adreslerinin listesini içeren bir erişim kontrol listesi yapılandırılır.
- “ip nat inside source list ACL_Numarasi interface_adı overload” komutu ile PAT kaynak listesindeki “ip nat” etkinleştirilir.

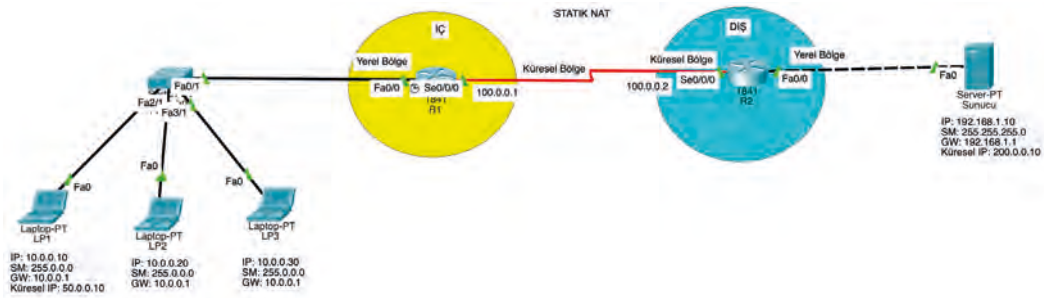
4.3.4. Statik NAT Uygulaması



3. UYGULAMA

Statik NAT Yapılandırma

İşlem adımlarına göre Görsel 4.17'deki ağ topolojisini simülasyon programında hazırlayıp statik NAT yapılandırmasını yapınız.



Görsel 4.17: Ağ topolojisi

1. Adım: Görsel 4.17'deki cihazlar için arayüz, IP, alt ağ maskesi ve varsayılan ağ geçidi bilgileri Tablo 4.2'de verilmiştir. Uygulama için fiziksel ve mantıksal topolojiyi simülasyon programını kullanarak oluşturunuz.

Tablo 4.2: Görsel 4.17'deki Cihazlar İçin Arayüz, DCE, IP, Alt Ağ Maskesi ve Varsayılan Ağ Geçidi Bilgileri

Cihaz	Arayüz	DCE/DTE	IP	Alt Ağ Maskesi	Varsayılan Ağ Geçidi
LP1	-	-	10.0.0.10	255.0.0.0	10.0.0.1
LP2	-	-	10.0.0.20	255.0.0.0	10.0.0.1
LP3	-	-	10.0.0.30	255.0.0.0	10.0.0.1
Sunucu	-	-	192.168.1.10	255.255.255.0	192.168.1.1
R1	Se0/0/0	DCE	100.0.0.1	255.0.0.0	-
	F0/0	-	10.0.0.1	255.0.0.0	-
R2	Se0/0/0	DTE	100.0.0.2	255.0.0.0	-
	F0/0	-	192.168.1.1	255.255.255.0	-

2. Adım: CLI arayüzüne girerek sırasıyla R1 cihazının arayüzlerine IP bilgilerini atamak için şu kodları uygulayınız:

```
R1(config)#int Se0/0/0
R1(config-if)#ip add 100.0.0.1 255.0.0.0
R1(config-if)#clock rate 64000
R1(config-if)#bandwidth 64
R1(config-if)#no sh
R1(config-if)#exit
```

```
R1(config)#int F0/0
R1(config-if)#ip add 10.0.0.1 255.0.0.0
R1(config-if)#no sh
R1(config-if)#exit
```

3. Adım: CLI arayüzüne girerek sırasıyla R2 cihazının arayüzlerine IP bilgilerini atamak için şu kodları uygulayınız:

```
R2(config)#int Se0/0/0
R2(config-if)#ip add 100.0.0.2 255.0.0.0
R2(config-if)#no sh
R2(config-if)#exit

R2(config)#int F0/0
R2(config-if)#ip add 192.168.1.1 255.255.255.0
R2(config-if)#no sh
R2(config-if)#exit
```



SIRA SİZDE

CLI arayüzüne girerek sırasıyla LP1, LP2 ve LP3 cihazının arayüzlerine IP bilgilerini atayan kodları uygulayınız.

4. Adım: CLI arayüzüne girerek R1 ve R2 cihazlarında statik NAT yönlendirme komutlarını uygulayınız.

Tablo 4.3: LP1 ve Sunucu Cihazların İç Yerel-İç Küresel IP Adres Eşleşme Bilgileri

Cihaz	İç Yerel IP Adresi	İç Küresel IP Adresi
LP1	10.0.0.10	50.0.0.10
Sunucu	192.168.1.10	200.0.0.10

```
R1(config)#ip nat inside source static 10.0.0.10 50.0.0.10
R1(config)#interface FastEthernet 0/0
R1(config-if)#ip nat inside
R1(config-if)#exit
```

```
R1(config)#interface Serial 0/0/0
R1(config-if)#ip nat outside
R1(config-if)#exit
```



SIRA SİZDE

CLI arayüzüne girerek R1 cihazında LP2 ve LP3 cihazları için statik NAT yapılandırmasını şu komutları kullanarak yapınız:

```
R1(config)#ip nat inside source static 10.0.0.20 50.0.0.20
R1(config)#ip nat inside source static 10.0.0.30 50.0.0.30
R2(config)#ip nat inside source static 192.168.1.10 200.0.0.10
R2(config)#interface FastEthernet 0/0
R2(config-if)#ip nat inside
R2(config-if)#exit

R2(config)#
R2(config)#interface Serial 0/0/0
R2(config-if)#ip nat outside
R2(config-if)#exit
```

5. Adım: Statik NAT yapılandırmasını test etmeden önce R1 ve R2 cihazlarında şu statik IP yönlendirme yapılandırmasını yapınız:

```
R1 (config) #ip route 200.0.0.0 255.255.255.0 100.0.0.2
R2 (config) #ip route 50.0.0.0 255.0.0.0 100.0.0.1
```

6. Adım: Görsel 4.18'de görüldüğü gibi LP1'de "ipconfig" komutunu çalıştırınız. Statik NAT yapılandırmasını test etmek için LP1'den sunucunun küresel IP adresi 200.0.0.10'a ping atınız. LP1'den sunucunun küresel adresi ile iletişiminin sorunsuz çalıştığını doğrulayınız.



SIRA SİZDE

LP1'den masaüstüne tıklayıp, Web Browser'a sunucunun IP adresi 200.0.0.10'u yazarak LP1 ile sunucu arasındaki iletişimi test ediniz.

```

Bluetooth Connection:(default port)
Connection-specific DNS Suffix...:
Link-local IPv6 Address.....: ::
IPv6 Address.....: ::
IPv4 Address.....: 0.0.0.0
Subnet Mask.....: 0.0.0.0
Default Gateway.....: ::
0.0.0.0

FastEthernet0 Connection:
Connection-specific DNS Suffix...:
Link-local IPv6 Address.....: FE80::260:5CFF:FE8C:4886
IPv6 Address.....: ::
IPv4 Address.....: 10.0.0.10
Subnet Mask.....: 255.0.0.0
Default Gateway.....: ::
10.0.0.1

C:\>ping 200.0.0.10

Pinging 200.0.0.10 with 32 bytes of data:

Reply from 200.0.0.10: bytes=32 time=46ms TTL=126
Reply from 200.0.0.10: bytes=32 time=1ms TTL=126
Reply from 200.0.0.10: bytes=32 time=53ms TTL=126
Reply from 200.0.0.10: bytes=32 time=51ms TTL=126

Ping statistics for 200.0.0.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 53ms, Average = 37ms

```

Görsel 4.18: LP1 ve sunucunun küresel IP adresi arasında ping komutu ile doğrulanan iletişim

7. Adım: Görsel 4.19'da görüldüğü gibi LP1'den sunucunun yerel IP adresi 192.168.1.10'a ping atınız. LP1'den sunucunun yerel adresi ile iletişiminin olmadığını doğrulayınız. İletişimin olmamasının nedeni, IP adresi 10.0.0.10 olan LP1 cihazının NAT yapılandırmasıdır. Bu sebeple yalnızca 10.0.0.10 IP adresli LP1 cihazı uzaktaki sunucuya erişebilir.



SIRA SİZDE

Statik NAT, IP adresi 10.0.0.10 olan LP1 cihazı için yapılandırıldı. Bu nedenle sadece IP adresi 10.0.0.10 olan LP1 cihazı uzaktaki sunucuya erişebilir. Siz de LP2 ve LP3 için statik NAT yapılandırmasını gerçekleştiriniz.

```

C:\>ping 192.168.1.10

Pinging 192.168.1.10 with 32 bytes of data:

Reply from 10.0.0.1: Destination host unreachable.
Reply from 10.0.0.1: Destination host unreachable.
Reply from 10.0.0.1: Destination host unreachable.
Request timed out.

Ping statistics for 192.168.1.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 192.168.1.10

Pinging 192.168.1.10 with 32 bytes of data:

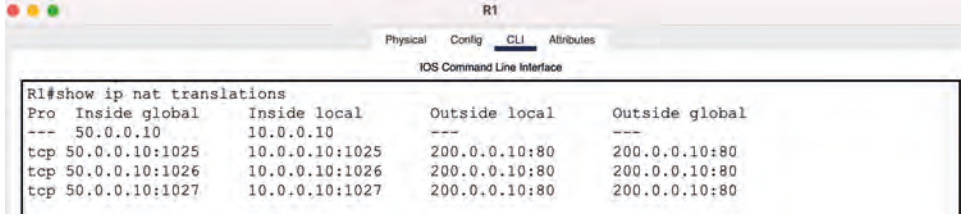
Reply from 10.0.0.1: Destination host unreachable.
Reply from 10.0.0.1: Destination host unreachable.
Reply from 10.0.0.1: Destination host unreachable.
Reply from 10.0.0.1: Destination host unreachable.

Ping statistics for 192.168.1.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

```

Görsel 4.19: LP1 ile sunucunun yerel IP adresi arasında kurulamayan iletişim

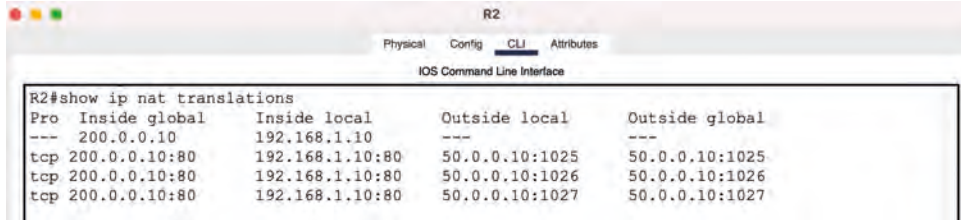
8. Adım: Görsel 4.20 ve Görsel 4.21’de görüldüğü gibi statik NAT çevirimini R1 ve R2 yönlendiricileri için “**show ip nat translations**” komutunu kullanarak doğrulayınız.



R1#show ip nat translations

Pro	Inside global	Inside local	Outside local	Outside global
---	50.0.0.10	10.0.0.10	---	---
tcp	50.0.0.10:1025	10.0.0.10:1025	200.0.0.10:80	200.0.0.10:80
tcp	50.0.0.10:1026	10.0.0.10:1026	200.0.0.10:80	200.0.0.10:80
tcp	50.0.0.10:1027	10.0.0.10:1027	200.0.0.10:80	200.0.0.10:80

Görsel 4.20: R1 yönlendiricisindeki statik NAT tablosu



R2#show ip nat translations

Pro	Inside global	Inside local	Outside local	Outside global
---	200.0.0.10	192.168.1.10	---	---
tcp	200.0.0.10:80	192.168.1.10:80	50.0.0.10:1025	50.0.0.10:1025
tcp	200.0.0.10:80	192.168.1.10:80	50.0.0.10:1026	50.0.0.10:1026
tcp	200.0.0.10:80	192.168.1.10:80	50.0.0.10:1027	50.0.0.10:1027

Görsel 4.21: R2 yönlendiricisindeki statik NAT tablosu

4.3.4. Dinamik NAT Uygulaması



4. UYGULAMA

Dinamik NAT Yapılandırma

İşlem adımlarına göre Görsel 4.17’deki ağ topolojisini simülasyon programında hazırlayıp dinamik NAT yapılandırmasını yapınız.

1. Adım: Üçüncü uygulamadaki birinci adımı gerçekleştiriniz.

2. Adım: Üçüncü uygulamadaki ikinci adımı gerçekleştiriniz.

3. Adım: Üçüncü uygulamadaki üçüncü adımı gerçekleştiriniz.

4. Adım: Tablo 4.4’te verilen IP adres bilgilerine göre CLI arayüzüne girerek R1 ve R2 cihazlarında dinamik NAT yönlendirme komutlarını uygulayınız.

Tablo 4.4: LP1, LP2 ve Sunucu Cihazların İç Yerel-İç Küresel IP Adres Eşleşme Bilgileri

Cihaz	İç Yerel IP Adresi	İç Küresel IP Adresi
LP1	10.0.0.10	50.0.0.10
LP2	10.0.0.20	50.0.0.2
Sunucu	192.168.1.10	200.0.0.10

```
R1#configure terminal
R1(config)#access-list 1 permit 10.0.0.10 0.0.0.0
R1(config)#access-list 1 permit 10.0.0.20 0.0.0.0
R1(config)#access-list 1 deny any
R1(config)#ip nat pool bilisim 50.0.0.1 50.0.0.2 netmask 255.0.0.0
R1(config)#ip nat inside source list 1 pool bilisim
```

```
R1(config)#interface FastEthernet 0/0
R1(config-if)#ip nat inside
R1(config-if)#exit
```

```
R1(config)#interface Serial0/0/0
R1(config-if)#ip nat outside
R1(config-if)#exit
```

```
R2>enable
R2#configure terminal
R2(config)#ip nat inside source static 192.168.1.10 200.0.0.10
```

```
R2(config)#interface Serial 0/0/0
R2(config-if)#ip nat outside
R2(config-if)#exit
```

```
R2(config)#interface FastEthernet 0/0
R2(config-if)#ip nat inside
R2(config-if)#exit
```

5. Adım: Dinamik NAT yapılandırmasını test etmeden önce R1 ve R2 cihazlarında şu statik IP yönlendirme yapılandırmasını yapınız:

```
R1(config)#ip route 200.0.0.0 255.255.255.0 100.0.0.2
R2(config)#ip route 50.0.0.0 255.0.0.0 100.0.0.1
```

6. Adım: “ipconfig” komutunu çalıştırınız. Dinamik NAT yapılandırmasını test etmek için LP1’den sunucunun küresel IP adresi 200.0.0.10’a ping atınız. LP1’den sunucunun küresel adresi ile iletişiminin sorunsuz çalıştığını doğrulayınız.



SIRA SİZDE

Görsel 4.22’de görüldüğü gibi LP1’den masaüstüne tıklayıp, Web Browser’a sunucunun IP adresi 200.0.0.10’u yazarak LP1 ile sunucu arasındaki iletişimi test ediniz.

```

C:\>ipconfig

Bluetooth Connection:(default port)

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address . . . . .: ::
    IPv6 Address . . . . .: ::
    IPv4 Address . . . . .: 0.0.0.0
    Subnet Mask . . . . .: 0.0.0.0
    Default Gateway . . . . .: ::

FastEthernet0 Connection:

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address . . . . .: FE80::260:5CFF:FE8C:4886
    IPv6 Address . . . . .: ::
    IPv4 Address . . . . .: 10.0.0.10
    Subnet Mask . . . . .: 255.0.0.0
    Default Gateway . . . . .: ::

C:\>ping 200.0.0.10

Pinging 200.0.0.10 with 32 bytes of data:

Reply from 200.0.0.10: bytes=32 time=46ms TTL=126
Reply from 200.0.0.10: bytes=32 time=1ms TTL=126
Reply from 200.0.0.10: bytes=32 time=53ms TTL=126
Reply from 200.0.0.10: bytes=32 time=51ms TTL=126

Ping statistics for 200.0.0.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 53ms, Average = 37ms

```

Görsel 4.22: LP1 ve sunucunun küresel IP adresi arasında ping komutu ile doğrulanan iletişim

7. Adım: Görsel 4.23'te görüldüğü gibi LP3'ten sunucunun yerel IP adresi 200.0.0.10'a ping atınız. LP3 ile sunucunun iletişiminin olmadığını doğrulayınız. İletişimin olmamasının nedeni, NAT'ın sadece 10.0.0.10 ve 10.0.0.20 IP adresli cihazlar için yapılandırılmasıdır. Bu sebeple yalnızca 10.0.0.10 ve 10.0.0.20 IP adresli cihazlar uzaktaki sunucuya erişebilir.

```

C:\>ipconfig

Bluetooth Connection:(default port)

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address . . . . .: ::
    IPv6 Address . . . . .: ::
    IPv4 Address . . . . .: 0.0.0.0
    Subnet Mask . . . . .: 0.0.0.0
    Default Gateway . . . . .: ::

FastEthernet0 Connection:

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address . . . . .: FE80::200:CFF:FE89:9E23
    IPv6 Address . . . . .: ::
    IPv4 Address . . . . .: 10.0.0.30
    Subnet Mask . . . . .: 255.0.0.0
    Default Gateway . . . . .: ::

C:\>ping 200.0.0.10

Pinging 200.0.0.10 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 200.0.0.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

```

Görsel 4.23: LP3 ile sunucunun yerel IP adresi arasında kurulamayan iletişim

8. Adım: Dinamik NAT yapılandırmasını R1 ve R2 yönlendiricileri için “show ip nat translations” komutunu kullanarak doğrulayınız. Oluşturulan erişim kontrol listesi, istenmeyen trafiği NAT'a ulaşmadan önce filtreler. ACL tarafından kaç paketin engellendiği şu komut kullanılarak görülür:

R1#show ip access-lists 1



SIRA SİZDE

LP3 için dinamik NAT yapılandırmasını gerçekleştiriniz.

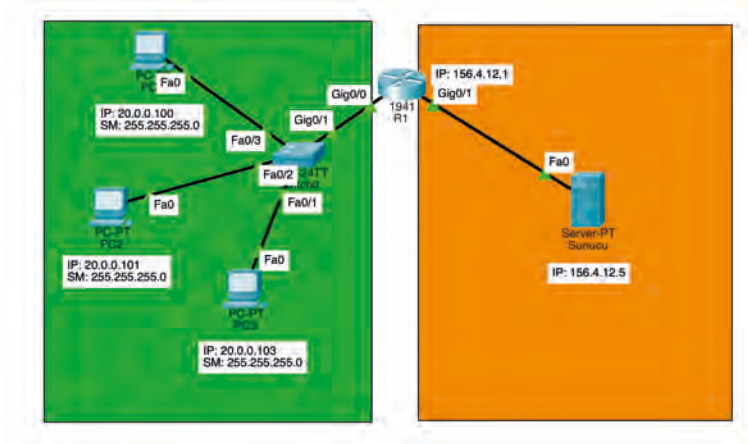
4.3.5. Statik NAT Uygulaması



5. UYGULAMA

Statik NAT Yapılandırma

Görsel 4.24'teki ağ topolojisini simülasyon programında hazırlayıp statik NAT yapılandırmasını yapınız.



Görsel 4.24: Ağ topolojisi

1. Adım: Görsel 4.24'teki cihazlar için arayüz, IP, alt ağ maskesi ve varsayılan ağ geçidi bilgileri verilmiştir. Uygulama için fiziksel ve mantıksal topolojiyi simülasyon programını kullanarak oluşturunuz. R1 üzerinde dış ve iç arayüzleri Tablo 4.5'e göre yapılandırınız.

Tablo 4.5: Özel IP Adresi-Genel IP Adresi Eşleşme Bilgileri

İç Yerel IP Adresi	İç Küresel IP Adresi
20.0.0.100:1055	156.4.12.1:1055
20.0.0.101:1056	156.4.12.1:1056
20.0.0.102:1057	156.4.12.1:1057

```
R1(config)#int Gi0/0
R1(config-if)#ip nat inside
```

```
R1(config-if)#int Gi0/1
R1(config-if)#ip nat outside
```

2. Adım: Çevrilmek istenen tüm özel IP adresleri için bir erişim kontrol listesi tanımlayınız. Bu oluşturulan erişim kontrol listesi 20.0.0.0-20.0.0.255 aralığındaki tüm IP adreslerini kapsar.

```
R1(config-if)#access-list 1 permit 20.0.0.0 0.0.0.255
```

3. Adım: İkinci adımda oluşturulan erişim kontrol listesi için NAT'ı etkinleştiriniz.

```
R1(config)#ip nat inside source list 1 interface Gi0/1 overload
```

4. Adım: Görsel 4.25'te görüldüğü gibi NAT çevirisini doğrulamak için “**show ip nat translation**” komutunu kullanınız.

20.0.0.100, 20.0.0.101 ve 20.0.0.102 IP adreslerini çevirmek için aynı IP adresinin (156.4.12.1) kullanıldığına dikkat ediniz. Genel IP adresinin port numarası ise her bağlantı için benzersizdir. Dolayısıyla R1, 156.4.12.1:1026'ya yanıt verdiğinde NAT çevirileri tablosuna bakıp cevabı 20.0.0.102:1025'e iletir.

```
R1#show ip nat translations
Pro Inside global Inside local Outside local Outside global
tcp 156.4.12.1:1024 20.0.0.100:1025 156.4.12.5:80 156.4.12.5:80
tcp 156.4.12.1:1025 20.0.0.101:1025 156.4.12.5:80 156.4.12.5:80
tcp 156.4.12.1:1026 20.0.0.102:1025 156.4.12.5:80 156.4.12.5:80
```

Görsel 4.25: Doğrulan NAT çevirimi



ÖLÇME VE DEĞERLENDİRME

Aşağıdaki soruları dikkatlice okuyarak doğru seçeneği işaretleyiniz.

1. Aşağıda yönlendirme tablosu ile ilgili verilen ifadelerden hangisi yanlıştır?

- A) Paketin nereye yönlendirmesi gerektiğine dair rotaları içerir.
- B) Yönlendirme tablosu tüm cihazlarda bulunur.
- C) Metrik değeri sadece dinamik rotalar için bulunur.
- D) Yönetimsel uzaklık değeri küçük olanlar yüksek önceliğe sahiptir.
- E) Süre değeri sadece dinamik rotalarda bulunur.

2. Aşağıdakilerden hangisi yönlendirme tablosunda varsayılan yönlendirme için kullanılan ön ektir?

- A) R
- B) S*
- C) D
- D) S
- E) C

3. Aşağıdaki komutlardan hangisi statik yönlendirme için kullanılır?

- A) ping
- B) ipconfig
- C) ip route
- D) ip address
- E) tracert

4. Aşağıdaki ifadelerden hangisi statik yönlendirme için doğrudur?

- A) Yönetim uzaklık değeri sıfırdır.
- B) Yüksek sistem kaynağı harcar.
- C) Değişen rotalar otomatik olarak güncellenir.
- D) Büyük ağlar için statik yönlendirme yapılandırması kolaydır.
- E) Statik rotalar anons edilmez ve güvenilirdir.

5. Aşağıda NAT işlemi ile ilgili verilen ifadelerden hangisi yanlıştır?

- A) Yerel ağdaki özel IP adreslerini genel IP adreslerine çevirir.
- B) Yerel ağlar arasında iletişim kurmak için kullanılır.
- C) Statik NAT işlemi, yerel ağdaki IP adresini küresel IP'ye bire bir çevirir.
- D) Dinamik NAT işlemi, yerel ağdaki IP adreslerini dinamik olarak havuzdaki IP'lere çevirir.
- E) NAT Overload (PAT) işlemi için IP portları kullanılır.



PIN MA

KONULAR

5.1. DİNAMİK YÖNLENDİRME

5.2. YÖNLENDİRME BİLGİSİ PROTOKOLÜ (RIP)

5.3. OSPF YÖNLENDİRME PROTOKOLÜ

5.4. EIGRP YÖNLENDİRME PROTOKOLÜ

5.5. SINIR AĞ GEÇİDİ PROTOKOLÜ (BGP)

ANAHTAR KELİMELER

- Dinamik yönlendirme
- İç ağ geçidi
- Dış ağ geçidi
- Uzaklık vektörü
- RIP / RIPv2
- OSPF
- Bant genişliği
- Sınır ağ geçidi
- Yol vektörü
- Otonom sistem
- IGP
- EGP
- EIGRP
- BGP
- eBGP
- iBGP
- Bağlantı durum protokolü

5. ÖĞRENME BİRİMİ

DİNAMİK YÖNLENDİRME İŞLEMLERİ

NELER ÖĞRENECEKSİNİZ?

- Dinamik yönlendirmenin amacı
- İç ağ geçidi ve dış ağ geçidi yönlendirme protokollerinin çalışma yapıları
- Rota hesaplamada kullanılan farklı protokoller ve algoritmalar
- Doğru dinamik yönlendirme protokolünün seçimi
- Dinamik yönlendirme tablolarını okuma
- Yönlendiricilerde RIP yönlendirmelerini kullanan ağları hazırlama
- RIP ile hedef rotalar için uzaklık vektörü protokolünün hesaplanması
- Yönlendiricilerde OSPF yönlendirmelerini kullanan ağları hazırlama
- OSPF ile bağlantı durum protokolünün hesaplanması
- Yayın ağlarında OSPF yönlendiricilerinin rolleri
- Yönlendiricilerde EIGRP kullanan ağları hazırlama
- EIGRP ile uzaklık vektörü ve bağlantı durum protokollerinin birlikte kullanımı
- RIP, OSPF ve EIGRP protokollerini daha güvenli yapacak önlemler
- BGP ve otonom sistem mantığı
- Farklı dinamik yönlendirme protokolleri ve otonom sistemler arasında yönlendirme uygulamaları





HAZIRLIK ÇALIŞMALARI

1. Geniş alanlarda çalışan kurumsal yapılar sizce veri haberleşmesini nasıl gerçekleştirir?
2. İnternetin dünyanın her yerine genişleyebilmesi, daima çalışır ve erişilebilir olması sizce nasıl mümkündür?

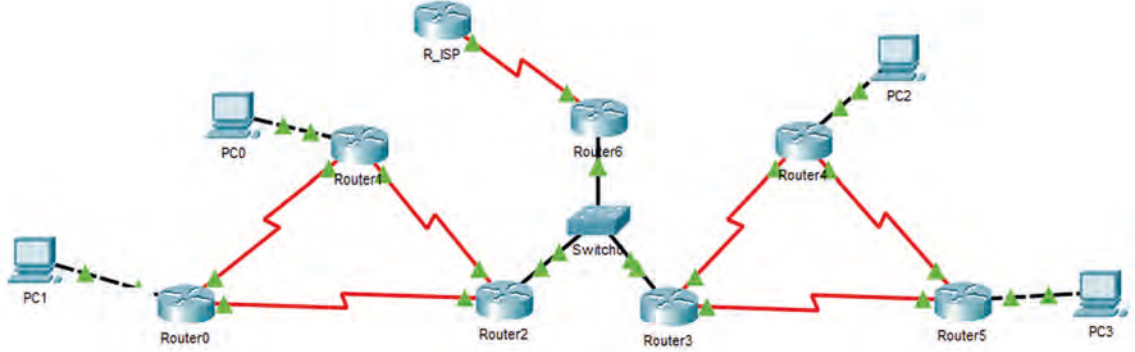
5.1. DİNAMİK YÖNLENDİRME

Ağların ve ağlar arasındaki yönlendiricilerin sayısı arttıkça haberleşmeyi aktif tutabilmek ve en iyi rota seçimlerini yapabilmek statik yönlendirmelerde oldukça zor bir hâle gelir. Yönlendiricilerin kullandığı algoritmalarla dinamik olarak hedef ağları bulma ihtiyacı doğmuştur. Ağ sistemlerinde bu işlemler dinamik yönlendirme protokolleri ile gerçekleştirilir.

Dinamik yönlendirmeler ile;

- Uzak ağların keşfedilmesi,
- Hedefe giden en iyi rotaların bulunması,
- Yeni ağların katılımı ile ağların genişleyebilmesi (ölçeklenebilme),
- Hedef ağ adresi değişimlerinde yeni adres bilgilerine göre yeniden rota hesaplanabilmesi,
- Ağlarda oluşabilecek sorunlarda alternatif yolların bulunması işlemleri yapılabilir (Görsel 5.1).

Ağların sayısı arttıkça dinamik yönlendirme ihtiyaçları da artar.



Görsel 5.1: Dinamik yönlendirmede sayısı artan ağlar

Statik yönlendirme yapılandırmaları, dinamik yönlendirme yapılandırmaları ile karşılaştırıldığında ağ yöneticileri için daha karmaşıktır ancak dinamik yönlendirmeler kullanıldıkları yönlendiricilerde daha fazla işlem yüküne ve ağ trafiğinin artmasına sebep olur.

5.1.1. Dinamik Yönlendirme Parametreleri

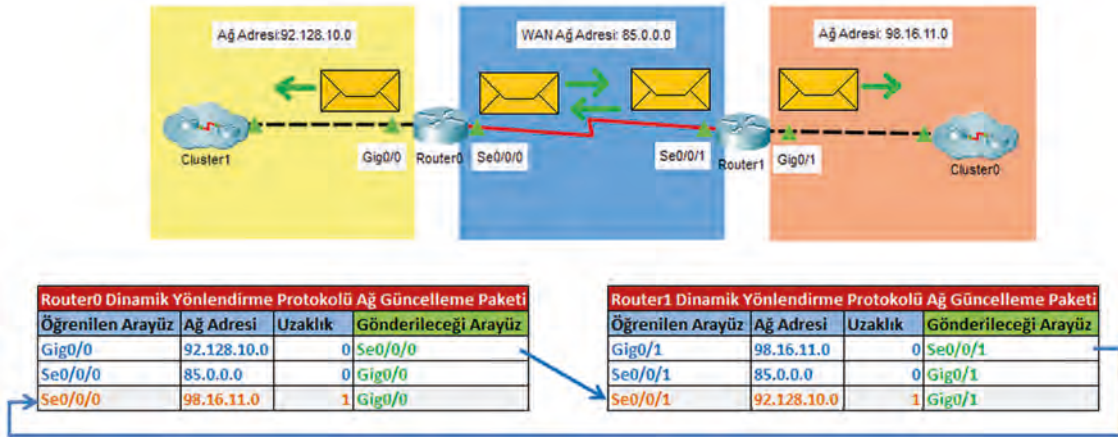
Dinamik yönlendirme protokolleri; farklı ağlar arasında kaynaktan hedefe giden en iyi rotayı sekme sayısı, bant genişliği, gecikme süresi, maliyet gibi değerlerin hesaplanması ile bulabilir. Hesaplanan sonuçlar, yönlendiricilerin yönlendirme tablosuna metrik değeri olarak yazılır. En iyi metrik sonuç, hedefe giden en iyi rotayı bulmada kullanılır.

Bazı dinamik yönlendirme parametreleri şunlardır:

- **Sekme Sayısı:** Kaynak ve hedef ağ arasındaki yönlendirici sayısıdır.
- **Bant Genişliği:** Fiziksel arayüzden iletim ortamına saniyede aktarılan veri miktarıdır.
- **Gecikme Süresi:** Yönlendiriciler arasındaki iletimin yanıtlanma süresidir.
- **Maliyet:** Kaynaktan hedefe giden yolun maliyetidir. Maliyet diğer parametrelerle birlikte hesaplanır.

5.1.2. Dinamik Yönlendirme Tablolarının Oluşumu

Yönlendiriciler hedefe giden en iyi rotayı yönlendirme tablolarından okur. İdeal yönlendirme tablolarının oluşması için yönlendiriciler güncel ağ bilgilerini komşu yönlendiricilerle paylaşır (Görsel 5.2). Böylelikle yönlendiriciler komşu ve uzak ağlar hakkında bilgi sahibi olur. Güncellenmiş ağ bilgileri ve yönlendirme parametrelerinin hesaplanması ile yönlendirme tabloları oluşturulur (Görsel 5.3). Yönlendiricilerde yönlendirme tablolarını görmek için “show ip route” komutu kullanılır.



Görsel 5.2: Ağ güncelleme paketleri gönderimi



BİLGİ

Uzaklık vektörü ile çalışan dinamik yönlendirme protokolleri döngüsel sorunlarla karşılaşmamak için ağ bilgisini öğrendikleri arayüzden aynı ağın güncelleme bilgisini göndermez.

Güncelleme paketlerinin gönderilmesinin gereksiz olduğu ağlar için yönlendiricinin arayüzden güncelleme paketlerini göndermesi ağ yöneticisi tarafından durdurulabilir.

```
R0#show ip route
      85.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       85.0.0.0/8 is directly connected, Serial0/0/0
L       85.0.0.10/32 is directly connected, Serial0/0/0
      92.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       92.0.0.0/8 is directly connected, GigabitEthernet0/0
L       92.128.10.1/32 is directly connected, GigabitEthernet0/0
R       98.0.0.0/8 [120/1] via 85.0.0.11, 00:00:12, Serial0/0/0
```

Görsel 5.3: Dinamik yönlendirme protokolü kullanan yönlendirme tablosu

• **R:** Yönlendirme protokolünün türüdür. Dinamik yönlendirme protokolü harfleri, yönlendirme protokolü türüne göre R-RIP, O-OSPF, D-EIGRP, B-BGP şeklindedir.

• **98.0.0/8:** Dinamik yönlendirme ile öğrenilmiş ağ bilgisidir.

• **120:** Dinamik yönlendirme protokolünün yönetimsel uzaklık değeridir. EIGRP: 90, OSPF: 110, RIP: 120 şeklindedir. Yönetimsel uzaklık değeri az olan protokol, tanımlandığı ağ topolojisinde önceliklidir.

• **/1:** Metrik değeridir. Metrik değeri; hedef ağ ile yönlendirici arasındaki sekme sayısı, bant genişliği, maliyet değerlerine bakılarak hesaplanır. Görsel 5.3'teki yönlendirme tablosunda kullanılan yönlendirme protokolü RIP'tir. RIP sadece uzaklık vektörü algoritması kullanan protokol olduğu için hedef ağ ile aradaki sekme sayısı yazılır. Diğer yönlendirme protokolleri OSPF ve EIGRP kullanılan bir sistemde metrik değerleri farklı hesaplanabilir.

• **85.0.0.11:** Hedef ağa gitmek için ilk ulaşılmaması gereken komşu yönlendirici IP değeridir.

• **00:00:12:** Güncelleme paketinin anonsundan sonra geçen süredir.

• **Serial0/0/0:** Hedef ağa gitmek için yönlendiricide çıkış yapılması gereken arayüz bilgisidir.

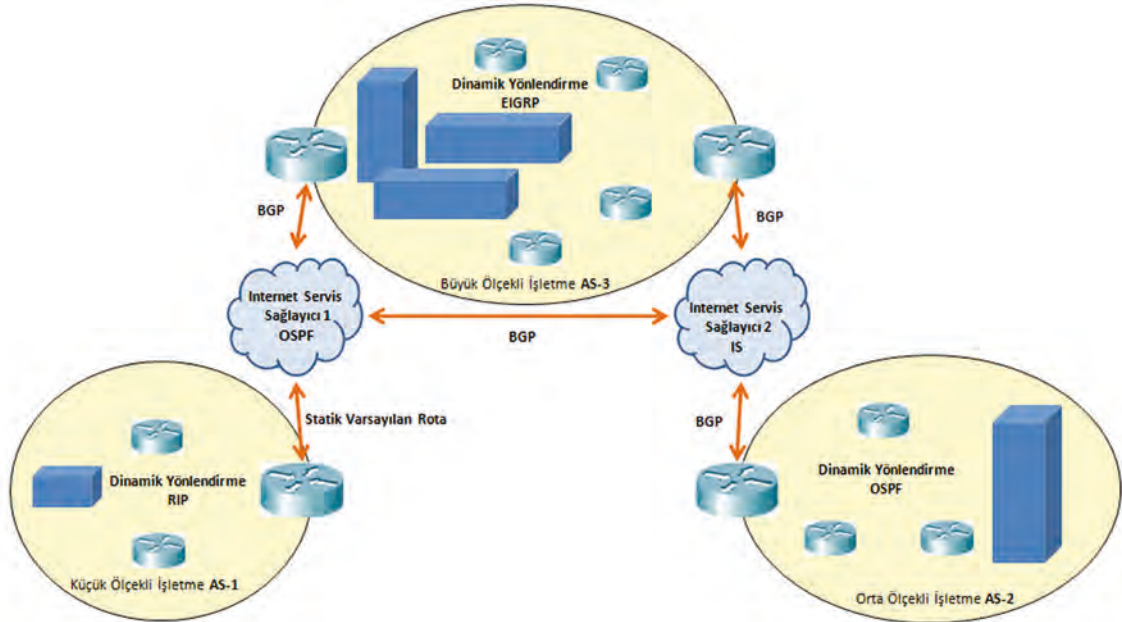
5.1.3. Dinamik Yönlendirme Protokolü Grupları

Dinamik yönlendirme protokolleri amaç, işleyiş ve davranış biçimlerine göre gruplandırılabilir.

5.1.3.1. İletişim Kurallarına Göre Dinamik Yönlendirme Protokolleri

Yönlendirme protokolleri ile çalışan her bağımsız ağ topolojisi ayrı bir otonom sistem olarak kabul edilir. Otonom sistemler küçük ofisler, orta ve büyük ölçekli işletme ağları olabilir. Otonom sistemlerin içinde farklı ağları yönlendirmek için İç Ağ Geçidi (IGP) protokolleri kullanılırken farklı otonom sistemler arasında veya İnternet Servis Sağlayıcı (ISP) ağlarına çıkış yapmak için Dış Ağ Geçidi (EGP) protokolleri kullanılır (Görsel 5.4).

İç Ağ Geçidi (IGP) dinamik yönlendirme protokolü ile RIP, OSPF, IGRP ve EIGRP yönlendirmeleri çalışır. Dış Ağ Geçidi (EGP) dinamik yönlendirme protokolü ise BGP yönlendirmesi ile çalışır.



Görsel 5.4: Farklı sistemlerde dinamik yönlendirme protokolleri

Tablo 5.1: Dinamik Yönlendirme Protokolü Özelliklerinin Karşılaştırılması

Özellik	Uzaklık Vektörü				Bağlantı Durumu
	RIPv1	RIPv2	IGRP	EIGRP	OSPF
Birleştirme Hızı	Yavaş	Yavaş	Yavaş	Hızlı	Hızlı
Genişleyebilme	Küçük	Küçük	Küçük	Büyük	Büyük
Sınıfsız Ağ	Hayır	Evet	Hayır	Evet	Evet
Kaynak Kullanımı	Düşük	Düşük	Düşük	Orta	Yüksek
Uygulama Kolaylığı	Basit	Basit	Basit	Karmaşık	Karmaşık

5.2. YÖNLENDİRME BİLGİSİ PROTOKOLÜ (RIP)

RIP, uzaklık vektörü protokolü kullanan ve genellikle küçük ağlar için tercih edilen bir dinamik yönlendirme protokolüdür. RIP, Bellman-Ford algoritmasını kullanarak yönlendirme rota hesaplamasını yapar. Rota hesaplamaları yapmak için yönlendiriciler kendi ağ bilgilerini komşu yönlendiriciler ile periyodik olarak paylaşır. Her yönlendirici, komşu yönlendiricinin ağ bilgisini öğrenebilir ve hedef ağlara hangi yoldan gidileceğini hesaplayabilir. Hedef rotaya ulaşmak için en az yönlendirici kullanılarak gidilecek yol, rota tercih yolu olarak bulunur.

RIP ortaya çıktıktan sonra RIP'in ikinci versiyonu RIPv2 geliştirilmiştir.

5.2.1. RIP Özellikleri

RIP'in özellikleri şu şekilde sıralanabilir:

- Uzaklık vektörü protokolünü kullanır.
- Hedef rota için en ideal yol, kaynak ile hedef ağ arasında en az yönlendirici sayısının bulunduğu yoldur.
- Sadece yönlendirici sayıları hesaplandığı için CPU kaynak tüketimi diğer dinamik yönlendirme protokollerine göre daha azdır.
- Art arda en fazla 15 yönlendirici için rota hesaplaması yapılabilir. Bu yüzden RIP daha küçük ölçekli ağlar için tercih edilebilir.
- Yönetimsel değeri 120'dir.
- Periyodik ağ güncellemeleri her 30 saniyede düzenli olarak yapılır. Bu güncelleme ile her yönlendirici, bağlı olduğu ağ bilgilerini komşuları ile paylaşır. Böylelikle her yönlendirici, komşu diğer yönlendiricilerdeki ağlar hakkında bilgi edinir. Doğrudan bağlı ağlarda bir değişiklik olmuşsa güncelleme bilgisi 30 saniyelik periyodik süre beklenmeden komşu yönlendiricilere iletilir.
- RIP, güncelleme paketi alınmayan ağları yönlendirme tablosunda 240 saniye tutar (flushed after time). 240 saniye sonra o ağ bilgisini yönlendirme tablosundan siler.
- Statik yönlendirmelerden farklı olarak RIP kullanan cihazlar arasında kimlik doğrulaması yapılabilir.
- RIP yapılandırması kolaydır.

5.2.2. RIP Yapılandırması

Yönlendiricilerde RIP yapılandırmasını gerçekleştirmek için yönlendirici arayüzleri ağ adreslerinin protokol bilgisi olarak bildirilmesi gerekir. RIP etkinleştirme bildirimi, yönlendirici komut ekranı konfigürasyon

satırında “router rip” komutu ile yapılır. Bağlı arayüz ağ adresi bilgisi “network” komutu ile bildirilir. Yönlendirici ağ bilgileri, fiziksel arayüzlerden ağ güncelleme paketleri ile komşu yönlendiricilere gönderilir.

Yönlendirici(config)#router rip

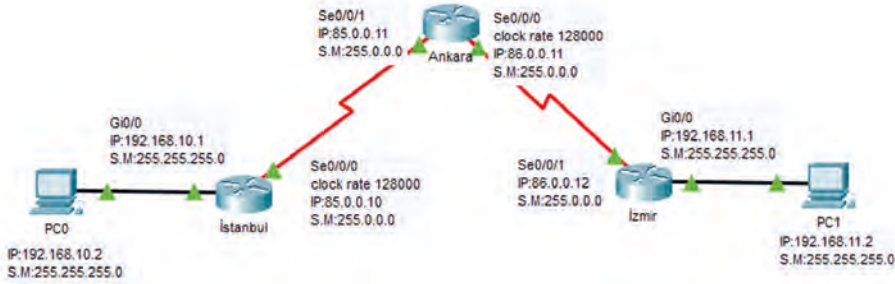
Yönlendirici(config-router)#network Arayüz Ağ Adresi



1. UYGULAMA

RIP Yapılandırması

İşlem adımlarına göre Görsel 5.6'daki ağ topolojisini simülasyon programında hazırlayıp RIP yapılandırması yapınız.



Görsel 5.6: Birinci uygulamanın ağ topolojisi

1. Adım: Görsel 5.6'da cihazların üzerinde fiziksel arayüz, IP, alt ağ maskesi ve varsayılan ağ geçidi bilgileri verilmiştir. Cihazlara görselde verilen IP'leri giriniz.

İstanbul yönlendiricisi için arayüz yapılandırması komut satırları:

İstanbul(config)#interface Serial0/0/0

İstanbul(config-if)#ip address 85.0.0.10 255.0.0.0

İstanbul(config-if)#clock rate 128000

İstanbul(config-if)#no shutdown

İstanbul(config-if)#exit

İstanbul(config)#interface GigabitEthernet 0/0

İstanbul(config-if)#ip address 192.168.10.1 255.255.255.0

İstanbul(config-if)#no shutdown



SIRA SİZDE

Ankara ve İzmir yönlendiricileri ile PC0 ve PC1'in IP yapılandırmalarını yapınız.

2. Adım: PC0'dan PC1 için “ping 192.168.11.2” komutu ile iletişim testi gerçekleştiriniz. İletişim testinin başarısız olduğunu göreceksiniz (Görsel 5.7). Bunun sebebi, PC0 ve PC1'in farklı yerel ağlarda olmasıdır. Farklı yerel ağlar arasında haberleşmek için yönlendirme işleminin gerçekleşmesi gerekir.

```
C:\>ping 192.168.11.2

Pinging 192.168.11.2 with 32 bytes of data:

Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.

Ping statistics for 192.168.11.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Görsel 5.7: Hedef ağı bulamamış başarısız ping iletişim testi

3. Adım: İstanbul, Ankara ve İzmir yönlendiricileri için RIP yapılandırılmalarını yapınız. İstanbul yönlendiricisi için RIP yapılandırması komut satırları:

Istanbul(config)#router rip	RIP ile yönlendirme bildirimi
Istanbul(config-router)#network 85.0.0.0	Bağlı WAN ağ adresi
Istanbul(config-router)#network 192.168.10.0	Bağlı Yerel Ağ 1 ağ adresi

Ankara yönlendiricisi için RIP yapılandırması komut satırları:

Ankara(config)#router rip	RIP ile yönlendirme bildirimi
Ankara(config-router)#network 85.0.0.0	Bağlı WAN ağ adresi
Ankara(config-router)#network 86.0.0.0	Bağlı WAN ağ adresi

İzmir yönlendiricisi için RIP yapılandırması komut satırları:

Izmir(config)#router rip	RIP ile yönlendirme bildirimi
Izmir(config-router)#network 86.0.0.0	Bağlı WAN ağ adresi
Izmir(config-router)#network 192.168.11.0	Bağlı Yerel Ağ 2 ağ adresi

4. Adım: PC0'dan PC1 için "ping 192.168.11.2" komutu ile tekrar iletişim testi gerçekleştiriniz. Bu kez iletişim testi başarılı olacaktır (Görsel 5.8).

```
C:\>ping 192.168.11.2

Pinging 192.168.11.2 with 32 bytes of data:

Reply from 192.168.11.2: bytes=32 time=11ms TTL=126
Reply from 192.168.11.2: bytes=32 time=5ms TTL=126
Reply from 192.168.11.2: bytes=32 time=3ms TTL=126
Reply from 192.168.11.2: bytes=32 time=4ms TTL=126

Ping statistics for 192.168.11.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 3ms, Maximum = 11ms, Average = 5ms
```

Görsel 5.8: RIP ile yapılandırılmış ağlarda başarılı bir ping iletişim testi

5. Adım: İstanbul, Ankara ve İzmir yönlendiricilerinde "show ip route rip" komutu ile sadece RIP yönlendirme tablolarını görüntüleyiniz (Görsel 5.9).

```
Istanbul#show ip route rip
      85.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
R       86.0.0.0/8 [120/1] via 85.0.0.11, 00:00:15, Serial0/0/0
      192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
R       192.168.11.0/24 [120/2] via 85.0.0.11, 00:00:15, Serial0/0/0
```

Görsel 5.9: Yönlendirici tablosunda RIP satırı

İstanbul yönlendiricisi için RIP yönlendirme tablosu Görsel 5.9'da verilmiştir. İstanbul yönlendiricisi, 86.0.0.0/8 ve 192.168.11.0/24 ağlarını RIP ile öğrenmiştir.

192.168.11.0/24 ağı için yönlendirme tablosundan şu veriler tespit edilir:

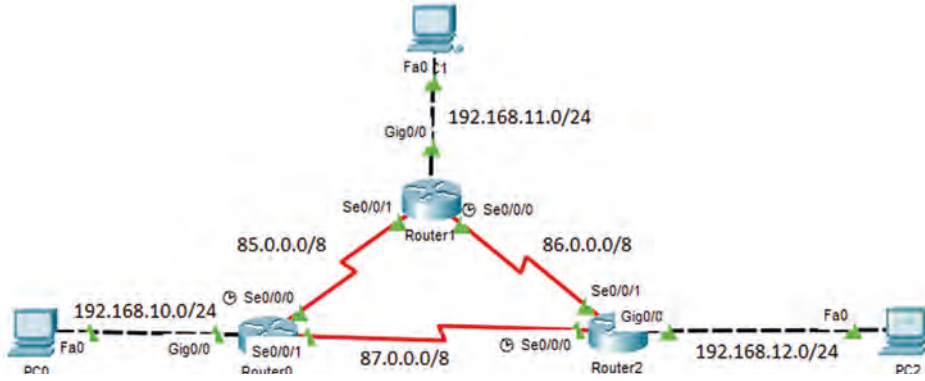
R	: RIP 192.168.11.0/24: Öğrenilmiş hedef ağ bilgisi
120	: RIP yönetimsel uzaklık değeri
/2	: Hedef ağ ile aradaki sekme (Ankara ve İzmir yönlendiricileri) sayısı
85.0.0.11	: Hedef ağa ulaşmak için ilk çıkış yapılan komşu yönlendirici IP adresi
00:00:15	: RIP güncelleme paketi anons süresi
Serial0/0/0	: Hedef ağa ulaşmak için yönlendiricinin kullandığı arayüz bilgisi



2. UYGULAMA

RIP Yapılandırması

Görsel 5.10'daki ağ topolojisini simülasyon programında oluşturunuz. İşlem adımlarına göre Tablo 5.2'de yer alan IP bilgilerini kullanarak ilgili cihazların RIP yapılandırmasını yapınız.



Görsel 5.10: İkinci uygulamanın ağ topolojisi

Tablo 5.2: İkinci Uygulamanın IP Bilgileri

Cihaz	Arayüz	DCE	IP	Alt Ağ Maskesi	Varsayılan Ağ Geçidi
Router0	Serial0/0/0	√ Clock rate 128000	85.0.0.10	255.0.0.0	
	Serial0/0/1		87.0.0.10	255.0.0.0	
	Gi0/0		192.168.10.1	255.255.255.0	
Router1	Serial0/0/0	√ Clock rate 128000	86.0.0.10	255.0.0.0	
	Serial0/0/1		85.0.0.11	255.0.0.0	
	Gi0/0		192.168.11.1	255.255.255.0	
Router2	Serial0/0/0	√ Clock rate 128000	87.0.0.12	255.0.0.0	
	Serial0/0/1		86.0.0.12	255.0.0.0	
	Gi0/0		192.168.12.1	255.255.255.0	
PC0			192.168.10.2	255.255.255.0	192.168.10.1
PC1			192.168.11.2	255.255.255.0	192.168.11.1
PC2			192.168.12.2	255.255.255.0	192.168.12.1

1. Adım: Router0 yönlendiricisine şu komutları girerek arayüz yapılandırmalarını yapınız:

```
Router0(config)#interface Serial0/0/0
Router0(config-if)#ip address 85.0.0.10 255.0.0.0
Router0(config-if)#clock rate 128000
Router0(config-if)#no shutdown
Router0(config-if)#exit
Router0(config)#interface Serial0/0/1
Router0(config-if)#ip address 87.0.0.10 255.0.0.0
Router0(config-if)#no shutdown
Router0(config-if)#exit
Router0(config)#interface GigabitEthernet 0/0
Router0(config-if)#ip address 192.168.10.1 255.255.255.0
```



SIRA SİZDE

Router1 ve Router2 yönlendiricilerini Tablo 5.2'de verilen IP'ler ile yapılandırınız.

2. Adım: Router0 için RIP yapılandırmasını şu komutlarla gerçekleştiriniz:

```
Router0(config)#router rip
Router0(config-router)#network 85.0.0.0
Router0(config-router)#network 87.0.0.0
Router0(config-router)#network 192.168.10.0
```



SIRA SİZDE

Router1 ve Router2'nin bağlı olduğu ağların adresleri ile RIP yapılandırmalarını yapınız.

3. Adım: RIP doğrulamasını gerçekleştirmek için sırasıyla Router0, Router1 ve Router2 yönlendiricilerinde yönlendirme tablosu bilgisini görüntüleyiniz.

Router0 için şu komut kullanılır:

```
Router0#show ip route rip
```

```
Router0#show ip route rip
      85.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
R       86.0.0.0/8 [120/1] via 85.0.0.11, 00:00:12, Serial0/0/0
          [120/1] via 87.0.0.12, 00:00:08, Serial0/0/1
      192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
R       192.168.11.0/24 [120/1] via 85.0.0.11, 00:00:12, Serial0/0/0
R       192.168.12.0/24 [120/1] via 87.0.0.12, 00:00:08, Serial0/0/1
```

Görsel 5.11: İkinci uygulamanın Router0 yönlendirme tablosu

Görsel 5.11'de Router0, RIP ile üç ağ bilgisi öğrenmiştir.

RIP, 192.168.11.0/24 ve 192.168.12.0/24 ağları için metrik değeri en az olan rotaları tercih etmiştir. Router0'da her iki yerel ağ için 1 metrik değeri ile en yakın yönlendiriciler üzerinden rota geçişi olur. 192.168.11.0/24 ağı için 85.0.0.11 IP'sini kullanan Router1 yönlendiricisi, 192.168.12.0/24 ağı için ise 87.0.0.12 IP'sini kullanan Router2 yönlendiricisi tercih edilmiştir.

Hedef 86.0.0.0/8 ağı için eşit metrik değerli iki rota bulunur. Eşit metrik değere sahip rotalar sırasıyla kullanılır.

4. Adım: “traceroute” komutu ile Router0'dan PC2'ye giden rotayı görüntüleyiniz.

Router0#traceroute 192.168.12.2

```
Router0#traceroute 192.168.12.2
Type escape sequence to abort.
Tracing the route to 192.168.12.2
```

1	87.0.0.12	0 msec	3 msec	1 msec
2	192.168.12.2	3 msec	0 msec	1 msec

Görsel 5.12: Yönlendiricilerde “traceroute” komutunun uygulanması

Görsel 5.12'de olduğu gibi PC2'ye (192.168.12.2) gidinceye kadar sadece Router2 yönlendiricisinden (87.0.0.12) geçiş yapılır.



SIRA SİZDE

Diğer yönlendiricilerden PC'lere rota bilgisini “traceroute” komutu ile görüntüleyiniz.

5. Adım: Ağlarda meydana gelebilecek olumsuzluklarda dinamik yönlendirme protokolünün yeni rota keşfini görebilmek için Router0 Serial0/0/1 arayüzünü “shutdown” komutu ile kapatınız.

Router0(config)#interface Serial0/0/1

Router0(config-if)#shutdown

6. Adım: Router0'da “show ip route rip” komutu ile tekrar yönlendirme tablosunu görüntüleyiniz.

```
Router0#show ip route rip
85.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
R 86.0.0.0/8 [120/1] via 85.0.0.11, 00:00:01, Serial0/0/0
192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
R 192.168.11.0/24 [120/1] via 85.0.0.11, 00:00:01, Serial0/0/0
R 192.168.12.0/24 [120/2] via 85.0.0.11, 00:00:01, Serial0/0/0
```

Görsel 5.13: Yönlendirici tablosunda rota güncellemesi

Görsel 5.13'te görüldüğü gibi Serial0/0/1 arayüzünün kapatılması ile 86.0.0.0/8 ağına giden rota bilgisi 1'e düşmüştür. 192.168.12.0 ağına giden rota metrik değeri ise 2'ye çıkmıştır. Rota değişikliği sonucunda hedef ağ ile Router0 arasında 2 sekme olduğu görülür.



SIRA SİZDE

Router1 ve Router2 yönlendiricilerinde yönlendirme tablolarını inceleyip rota bilgilerinin değişimlerini gözlemleyiniz.

7. Adım: “traceroute” komutu ile Router0’dan PC2’ye giden rota bilgisini tekrar görüntüleyiniz.

Router0#traceroute 192.168.12.2

```
Router0#traceroute 192.168.12.2
Type escape sequence to abort.
Tracing the route to 192.168.12.2

 1  85.0.0.11      1 msec  1 msec  1 msec
 2  86.0.0.12      4 msec  1 msec  2 msec
 3  192.168.12.2   4 msec  1 msec  6 msec
```

Görsel 5.14: “traceroute” ile güncellenmiş rota bilgisi

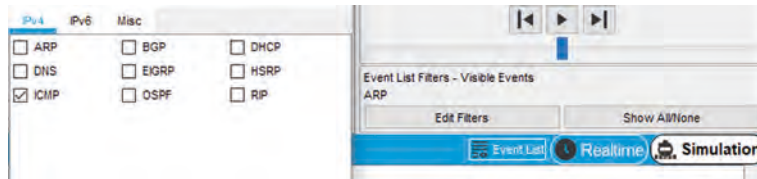
Görsel 5.14’te görüldüğü gibi Router0, 87.0.0.0/8 ağından iletişime geçemediği için alternatif rotaları kullanmıştır. Rota güzergâhı önce Router1 (85.0.0.11) sonra Router2 (86.0.0.12) üzerinden geçerek PC2’ye (192.168.12.2) ulaşmıştır.



SIRA SİZDE

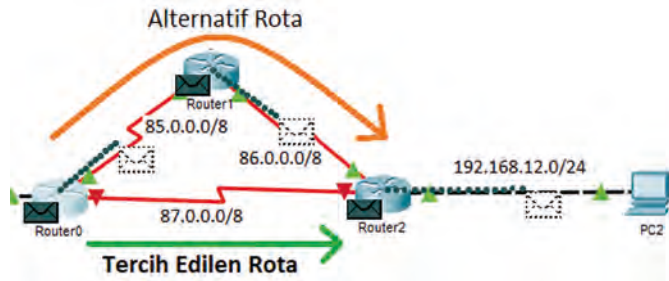
Diğer yönlendiricilerden PC’lere rota bilgisini “traceroute” komutu ile görüntüleyiniz.

8. Adım: Simülasyon ortamında rotaları gözlemlemek için Simulation\Show All/None/EditFilters düğmeleri ile sadece ICMP paketini seçiniz (Görsel 5.15).



Görsel 5.15: Simülasyon ortamına geçiş

9. Adım: Router0’dan “ping 192.168.12.2” komutu ile PC2’ye iletişim testi gerçekleştirerek Router0 ile PC2 arasındaki ICMP paketlerinin geçiş rotasını gözlemleyiniz (Görsel 5.16).



Görsel 5.16: Simülasyon ortamında rota

Yedinci adımda “traceroute” komutu ile elde ettiğiniz rotayı simülasyon ortamında gözlemleyebilirsiniz (Görsel 5.16).

10. Adım: Router0’da çalışan dinamik yönlendirme protokolünü doğrulamak için “show ip protocols” komutunu uygulayınız (Görsel 5.17).

```
Router0#show ip protocols
Routing Protocol is "rip"
Sending updates every 30 seconds, next due in 26 seconds
Invalid after 180 seconds, hold down 180, flushed after 240
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Redistributing: rip
Default version control: send version 1, receive any version
Interface          Send Recv Triggered RIP Key-chain
GigabitEthernet0/0  1      2  1
Serial0/0/0         1      2  1
Automatic network summarization is in effect
Maximum path: 4
Routing for Networks:
  85.0.0.0
  87.0.0.0
  192.168.10.0
Passive Interface(s):
Routing Information Sources:
  Gateway         Distance      Last Update
  85.0.0.11        120           00:00:18
Distance: (default is 120)
```

Görsel 5.17: RIP ile çalışan yönlendirme protokolü



SIRA SİZDE

Diğer RIP doğrulama komutlarının girişlerini (“show ip rip database”, “debug ip rip”, “debug ip rip events”) ikinci uygulamadaki yönlendiricilerde yaparak sonuçları gözlemleyiniz.

5.2.3. RIP ve RIPv2’nin Farklılıkları

RIPv2, RIP dinamik yönlendirme protokolünün geliştirilmiş versiyonudur. RIP’in eksik ve geliştirilme ihtiyacı olan özellikleri RIPv2 ile güncellenmiştir. RIP ve RIPv2’nin farklılıkları Tablo 5.3’te verilmiştir.

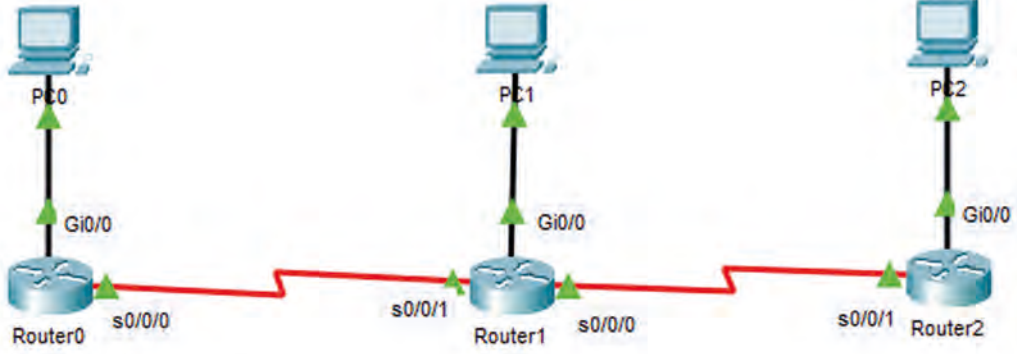
Tablo 5.3: RIP ve RIPv2’nin Farklılıkları

RIP	RIPv2
Yayın (Broadcast) IP’si ile yayın yaptığı için komşu cihaz protokolünü gözetmez.	Çoklu Yayın (Multicast) IP’si ile yayın yaptığı için yalnızca RIPv2 protokolü kullanan cihazlarla haberleşme yapar.
Yayın IP adresi: 255.255.255.255	Çoklu Yayın IP adresi: 224.0.0.9
Protokol paketi, ağların alt ağ maskesi bilgisini taşımaz.	Protokol paketi, ağların alt ağ maskeleri bilgisini taşır.
Otomatik özetleme yapar. Sınıflı ağ teknolojileri ile çalışır.	İstenirse otomatik özetleme yapmaz. Sınıfsız ağ teknolojilerini (VLSM) destekler.
RIP paketlerinin aktarımı için kimlik doğrulaması yapmaz.	RIP paketlerinin güvenli kaynaklardan aktarımı için kimlik doğrulaması yapabilir.

3. UYGULAMA

RIPv2 Yapılandırması

Görsel 5.18'deki topolojiyi Tablo 5.4'te verilen IP bilgilerine göre simülasyon programında oluşturunuz. İşlem adımlarına göre RIPv2 yapılandırmasını yapınız.



Görsel 5.18: Üçüncü uygulamanın ağ topolojisi

Tablo 5.4: Üçüncü Uygulamanın IP Bilgileri

Cihaz	Arayüz	DCE	IP	Alt Ağ Maskesi	Varsayılan Ağ Geçidi
Router0	Serial0/0/0	√ Clock rate 128000	85.0.0.1	255.0.0.0	
	Gi0/0		192.168.1.1	255.255.255.192	
Router1	Serial0/0/0	√ Clock rate 128000	86.0.0.1	255.0.0.0	
	Serial0/0/1		85.0.0.2	255.0.0.0	
Router2	Gi0/0		192.168.1.65	255.255.255.192	
	Serial0/0/1		86.0.0.2	255.0.0.0	
PC0			192.168.1.2	255.255.255.192	192.168.1.1
PC1			192.168.1.66	255.255.255.192	192.168.1.65
PC2			192.168.1.130	255.255.255.192	192.168.1.129

1. Adım: Router0, Router1, Router2 yönlendirici IP yapılandırmalarını Tablo 5.4'e göre gerçekleştiriniz.

```

Router0(config)#interface Serial0/0/0
Router0(config-if)#ip address 85.0.0.1 255.0.0.0
Router0(config-if)#clock rate 128000
Router0(config-if)#no shutdown
Router0(config-if)#exit

Router0(config)#interface GigabitEthernet 0/0
Router0(config-if)#ip address 192.168.1.1 255.255.255.192
Router0(config-if)#no shutdown
Router0(config-if)#exit

```



SIRA SİZDE

Diğer yönlendirici IP yapılandırmalarını gerçekleştiriniz.

2. Adım: Router0, Router1, Router2 yönlendirici RIP yapılandırmalarını yapınız.

```
Router0(config)#router rip
```

```
Router0(config-router)#network 85.0.0.0
```

```
Router0(config-router)#network 192.168.1.0
```

```
Router1(config)#router rip
```

```
Router1(config-router)#network 85.0.0.0
```

```
Router1(config-router)#network 86.0.0.0
```

```
Router1(config-router)#network 192.168.1.64
```

```
Router2(config)#router rip
```

```
Router2(config-router)#network 86.0.0.0
```

```
Router2(config-router)#network 192.168.1.128
```

3. Adım: PC0'dan PC1 ve PC2'nin IP adreslerine "ping" komutu ile iletişim testi gerçekleştiriniz. İletişim testi başarılı oldu mu? İletişim testi başarısız ise bunun nedeni sizce nedir?

4. Adım: Üçüncü adımdaki PC'ler birbirleriyle iletişim kuramayacaktır çünkü yönlendiricilerin yerel ağ adresleri sırasıyla 192.168.1.1/26, 192.168.1.65/26 ve 192.168.1.129/26 IP'leri ile sınıfsız değişken uzunluklu alt ağ maskesi (VLSM) kullanılarak tanımlanmıştır. RIP versiyon1, VLSM teknolojisini desteklemez. Yönlendiriciler RIP paketleri ile alt ağ maskesi bilgisini aktarmadığı için diğer yönlendiriciler alt ağ bilgisini alamaz.

Router0'da "show ip route" komutunu kullanarak, Router0 yönlendiricisinin Router1 ve Router2 yerel ağlarını öğrenip öğrenmediğini kontrol ediniz.

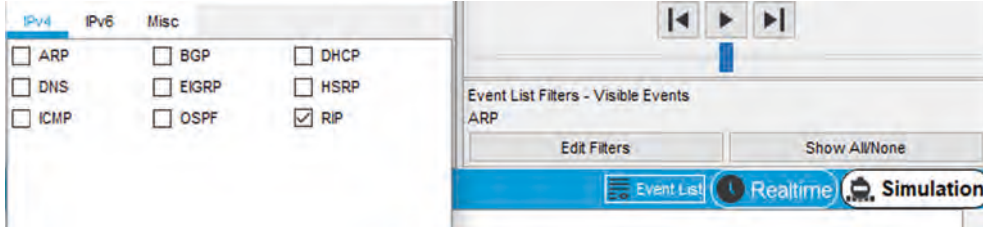
```
R0#sh ip route

      85.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       85.0.0.0/8 is directly connected, Serial0/0/0
L       85.0.0.1/32 is directly connected, Serial0/0/0
R       86.0.0.0/8 [120/1] via 85.0.0.2, 00:00:03, Serial0/0/0
      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/26 is directly connected, GigabitEthernet0/0
L       192.168.1.1/32 is directly connected, GigabitEthernet0/0
```

Görsel 5.19: RIP ile sınıfsız alt ağları öğrenememiş yönlendirme tablosu

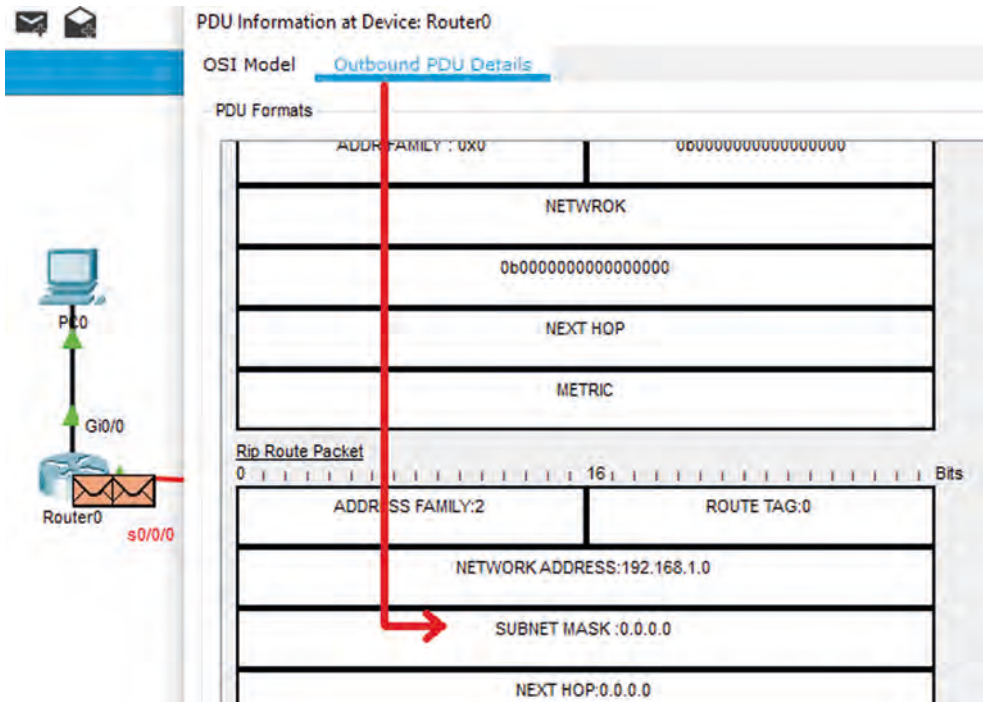
Görsel 5.19'daki yönlendirici sadece 192.168.1.0/24 ağının alt ağlarını kendi ağları olarak görür. Router0 yönlendiricisi, 192.168.1.64/26 ve 192.168.1.128/26 yerel ağlarını öğrenememiştir. Router0 yönlendiricisi, RIP ile sadece 86.0.0.0/8 sınıflı ağın öğrenmiştir.

5. Adım: Simülasyon ortamında RIP paketi alt ağ maskesi bilgisini gözlemlemek için Simulation\Show All/None>EditFilters düğmeleri ile sadece RIP paketini seçiniz (Görsel 5.20). “Simülasyon ileri hareket ettir.” düğmesine basınız.



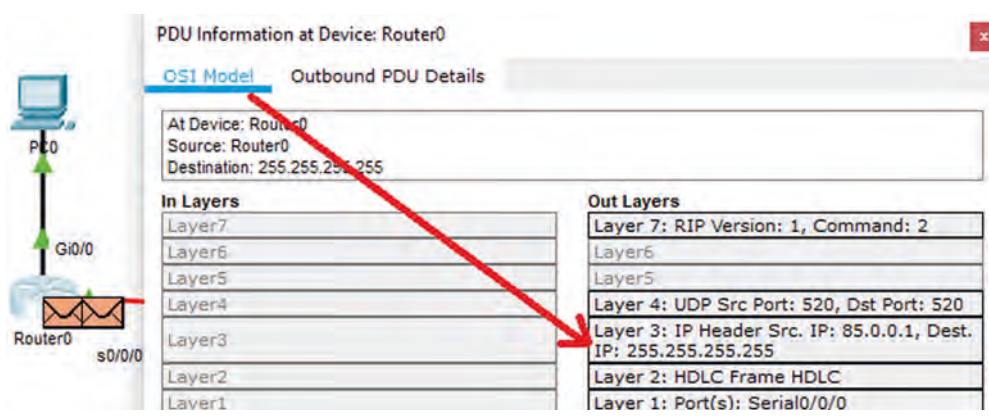
Görsel 5.20: Simülasyon ortamında RIP seçimi

6. Adım: Router0'da oluşan RIP paketlerinin üzerine tıklayınız ve “Outbound PDU Details” sekmesine geliniz. Sekmenin alt kısmındaki “Rip Route Packet” tablosuna bakıldığında Subnet Mask (Alt Ağ Maskesi) satırının 0.0.0.0 olduğu görülür (Görsel 5.21). RIP'in 1.versiyonu, alt ağ maskesi bilgisini taşımaz.



Görsel 5.21: RIP'in 1.versiyonu yönlendirme paketi incelemesi

7. Adım: Router0'da oluşan RIP paketlerinin üzerine tıklayınız ve “OSI Model” sekmesini açınız (Görsel 5.22). 3.katmanda, Destination (Hedef) IP kısmında 255.255.255.255 adresi ile RIP'in yayın paketi olduğu görülür.



PDU Information at Device: Router0

OSI Model Outbound PDU Details

At Device: Router0
Source: Router0
Destination: 255.255.255.255

In Layers	Out Layers
Layer7	Layer 7: RIP Version: 1, Command: 2
Layer6	Layer6
Layer5	Layer5
Layer4	Layer 4: UDP Src Port: 520, Dst Port: 520
Layer3	Layer 3: IP Header Src. IP: 85.0.0.1, Dest. IP: 255.255.255.255
Layer2	Layer 2: HDLC Frame HDLC
Layer1	Layer 1: Port(s): Serial0/0/0

Görsel 5.22: RIP'in 1.versiyonu yayın IP adresi

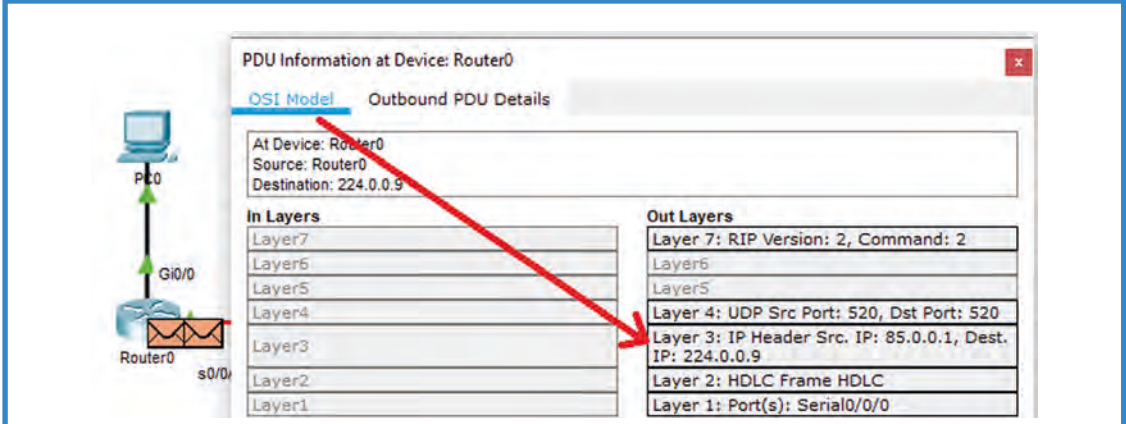
8. Adım: Yönlendiricilerde RIP versiyonunu RIPv2'ye yükseltmek için "version 2" komutunu kullanınız.

```
Router0(config)#router rip
Router0(config-router)#version 2
Router1(config)#router rip
Router1(config-router)#version 2
Router2(config)#router rip
Router2(config-router)#version 2
```

9. Adım: RIPv2, sınıfsız ağların bildirimini kendiliğinden yapmaz. Varsayılan olarak ağ adresini sınıflı şekilde tanımlar. Bu olaya otomatik özetleme (auto-summary) denir. RIPv2'nin otomatik özetleme işlemini iptal etmek için komut ekranı yönlendirme satırında "no auto-summary" komutunu el ile yazmak gerekir. Bu işlem, bir RIPv2 özelliğidir ve 1.nesil RIP tarafından desteklenmez.

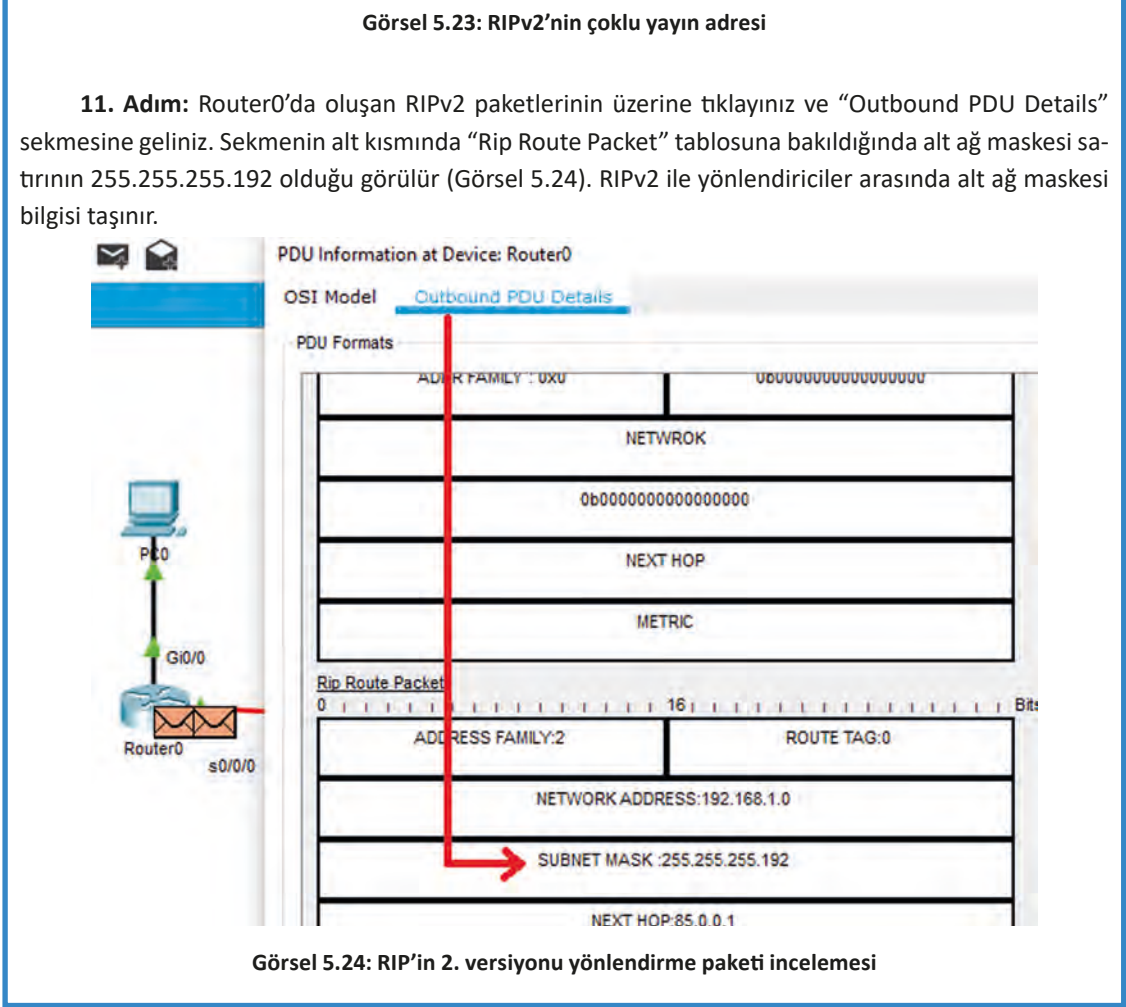
```
Router0(config)#router rip
Router2(config-router)#no auto-summary
Router1(config)#router rip
Router2(config-router)#no auto-summary
Router2(config)#router rip
Router2(config-router)#no auto-summary
```

10. Adım: Yönlendiricilerde tekrar simülasyon ortamına geliniz. Router0'da oluşan RIP paketlerinin üzerine tıklayınız ve "OSI Model" sekmesini açınız (Görsel 5.23). 3. katmanda, Hedef IP satırında 224.0.0.9 adresinin RIPv2'nin çoklu yayın adresi olduğu görülür.



Görsel 5.23: RIPv2'nin çoklu yayın adresi

11. Adım: Router0'da oluşan RIPv2 paketlerinin üzerine tıklayınız ve "Outbound PDU Details" sekmesine geliniz. Sekmenin alt kısmında "Rip Route Packet" tablosuna bakıldığında alt ağ maskesi satırının 255.255.255.192 olduğu görülür (Görsel 5.24). RIPv2 yönlendiriciler arasında alt ağ maskesi bilgisi taşınır.



Görsel 5.24: RIPv2'nin 2. versiyonu yönlendirme paketi incelemesi



BİLGİ

Otomatik özetleme "no auto-summary" komutu ile kapatılmamış RIPv2 yapılandırmalarında protokol, 192.168.1.0 ağ adresini 255.255.255.0 alt ağ maskesi ile özetler.

12. Adım: Router0 yönlendiricisinde “show ip route” komutu ile yönlendirici tablosunu görüntüleyiniz.

```
Router0#show ip route
      85.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       85.0.0.0/8 is directly connected, Serial0/0/0
L       85.0.0.1/32 is directly connected, Serial0/0/0
R 86.0.0.0/8 [120/1] via 85.0.0.2, 00:00:08, Serial0/0/0
      192.168.1.0/24 is variably subnetted, 4 subnets, 2 masks
C       192.168.1.0/26 is directly connected, GigabitEthernet0/0
L       192.168.1.1/32 is directly connected, GigabitEthernet0/0
R 192.168.1.64/26 [120/1] via 85.0.0.2, 00:00:08, Serial0/0/0
R 192.168.1.128/26 [120/2] via 85.0.0.2, 00:00:06, Serial0/0/0
```

Görsel 5.25: RIPv2'nin yönlendirme tablosu

Görsel 5.25'te Router0 yönlendiricisi, Router1 ve Router2 yerel ağlarını doğru alt ağ maskeleri ile öğrenmiştir. 192.168.1.64/26 ağına 1 metrik değeri ile, 192.168.1.128/26 ağına 2 metrik değeri ile ulaşabilir.

13. Adım: PC0'dan PC1 ve PC2'nin IP adreslerine “ping” komutu ile iletişim testi gerçekleştiriniz. İletişim testi başarılı oldu mu? Doğru yönlendirme tablolarına sahip olduğu için iletişim testleri başarılı olacaktır.



SIRA SİZDE

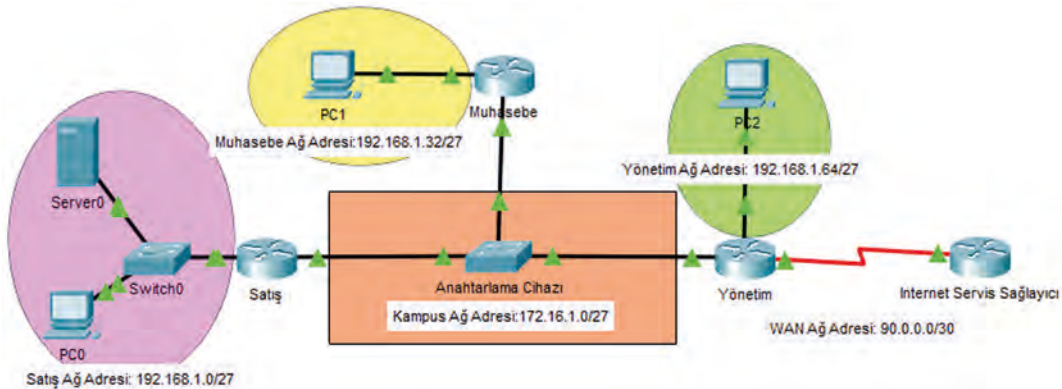
Router1 ve Router2 yönlendiricilerinde “show ip route” komutu ile yönlendirici tablolarını görüntüleyip inceleyiniz.



4. UYGULAMA

RIPv2 Yapılandırması

Görsel 5.26'da bir firma için verilen ağ topolojisini simülasyon programında oluşturunuz. İşlem adımlarına göre Tablo 5.5'te yer alan IP bilgilerini kullanıp ilgili cihazların RIPv2 yapılandırmasını yapınız.



Görsel 5.26: Dördüncü uygulamanın ağ topolojisi

Tablo 5.5: Dördüncü Uygulamanın Firma IP Bilgileri

Cihaz	Arayüz	DCE	IP	Alt Ağ Maskesi	Varsayılan Ağ Geçidi
Satış Yönlendiricisi	Gi0/0		172.16.1.1	255.255.255.224	
	Gi0/1		192.168.1.1	255.255.255.224	
Muhasebe Yönlendiricisi	Gi0/0		172.16.1.2	255.255.255.224	
	Gi0/1		192.168.1.33	255.255.255.224	
Yönetim Yönlendiricisi	Gi0/0		172.16.1.3	255.255.255.224	
	Gi0/1		192.168.1.65	255.255.255.224	
	Se0/0/0		90.0.0.2/30	255.255.255.252	
ISP Yönlendiricisi	Se0/0/0	V Clock rate 128000	90.0.0.1/30	255.255.255.252	
PC0			192.168.1.2	255.255.255.224	192.168.1.1
Sunucu (Server)			192.168.1.30	255.255.255.224	192.168.1.1
PC1			192.168.1.34	255.255.255.224	192.168.1.33
PC2			192.168.1.66	255.255.255.224	192.168.1.65

1. Adım: Yönetim yönlendiricisinde arayüzlere şu komutlarla IP atamalarını gerçekleştiriniz:

Yonetim(config)#interface GigabitEthernet 0/0

Yonetim(config-if)#ip address 172.16.1.3 255.255.255.224

Yonetim(config-if)#no shutdown

Yonetim(config-if)#exit

Yonetim(config)#interface GigabitEthernet 0/1

Yonetim(config-if)#ip address 192.168.1.65 255.255.255.224

Yonetim(config-if)#no shutdown

Yonetim(config-if)#exit

Yonetim(config)#interface Serial 0/0/0

Yonetim(config-if)#ip address 90.0.0.2 255.255.255.252

Yonetim(config-if)#no shutdown

Yonetim(config-if)#exit



SIRA SİZDE

Muhasebe, Satış ve İnternet Servis Sağlayıcı yönlendiricilerinin IP atamalarını Tablo 5.5'te verilen değerlerle yapınız.

2. Adım: Yönetim yönlendiricisi yerel ağları için RIPv2 ile dinamik yönlendirme işlemlerini yapınız. Yönlendiricilerde otomatik özetleme yaptırmayınız.

```
Yonetim(config)#router rip
Yonetim(config-router)#version 2
Yonetim(config-router)#network 172.16.1.0
Yonetim(config-router)#network 192.168.1.64
Yonetim(config-router)#no auto-summary
```



SIRA SİZDE

Muhasebe ve Satış yönlendiricileri için RIPv2 ile yönlendirme işlemlerini yapınız. İnternet Servis Sağlayıcı yönlendiricisi için herhangi bir RIP yönlendirme işlemi yapmayınız.

3. Adım: Satış yönlendiricisinde “show ip route rip” komutu ile RIP yönlendirme tablosunu görüntüleyiniz (Görsel 5.27).

```
Satis#show ip route rip
      192.168.1.0/24 is variably subnetted, 4 subnets, 2 masks
R       192.168.1.32/27 [120/1] via 172.16.1.2, 00:00:04, GigabitEthernet0/0
R       192.168.1.64/27 [120/1] via 172.16.1.3, 00:00:19, GigabitEthernet0/0
```

Görsel 5.27: Beşinci uygulamanın Satış yönlendiricisi yönlendirme tablosu

Görsel 5.27’de Satış yönlendiricisinin Muhasebe ve Yönetim yönlendiricilerinin yerel ağlarına RIP ile ulaşabildiği görülür.

4. Adım: Satış ağındaki sunucu bilgisayardan PC1 ve PC2’ye “ping” komutu ile iletişim testi yapınız. Görsel 5.27’deki yönlendirme tablosuna göre iletişim testi başarılı olacaktır.

5. Adım: Firma otonom sistemi yönlendiricileri WAN ağına Yönetim yönlendiricisi üzerinden çıkar. Varsayılan rotalar, bilinmeyen ağ sistemlerine çıkmak için kullanılan bir yönlendirme türüdür. Yönetim yönlendiricisinden WAN ağına çıkış için varsayılan rotayı yapılandırınız.

```
Yonetim(config)#ip route 0.0.0.0 0.0.0.0 serial0/0/0
```

6. Adım: Diğer yönlendiricilerin WAN ağına çıkabilmesi için Yönetim yönlendiricisinin RIP yapılandırmasında diğer yönlendiricilere varsayılan rota bildirimini yapınız.

```
Yonetim(config)#router rip
Yonetim(config-router)#redistribute rip metric 1
```

Bu adımda varsayılan rota ile farklı bir otonom sisteme çıkış yapan yönlendiricinin diğer yönlendiriciler için varsayılan rotayı bildirme işlemi görülür.

7. Adım: Satış yönlendiricisinde yönlendirme tablosunu “show ip route rip” komutu ile tekrar görüntüleyiniz.

Görsel 5.28'deki Satış yönlendiricisi, Yönetim yönlendiricisinden gelen varsayılan rota bildirimini yönlendirme tablosuna son satırda yazmıştır. Varsayılan rotalar, RIP yönlendirme tablosu içinde R* satırı ile belirtilir.

```
Satis#show ip route rip
      192.168.1.0/24 is variably subnetted, 4 subnets, 2 masks
R       192.168.1.32/27 [120/1] via 172.16.1.2, 00:00:24,
GigabitEthernet0/0
R       192.168.1.64/27 [120/1] via 172.16.1.3, 00:00:23,
GigabitEthernet0/0
R*  0.0.0.0/0 [120/1] via 172.16.1.3, 00:00:12, GigabitEthernet0/0
```

Görsel 5.28: RIPv2 ile varsayılan rota bildirimli yönlendirme tablosu

8. Adım: Sunucu bilgisayardan İnternet Servis Sağlayıcı yönlendiricisine ping testi yapınız.

Bu adımda ICMP paketleri simülasyon ortamında izlenirse paketlerin sunucudan İnternet Servis Sağlayıcı yönlendiricisine kadar gittiği görülür. Yönetim yönlendiricisinden paketlerin WAN ağına çıkması, varsayılan rota bildiriminin doğru çalıştığını gösterir fakat WAN ağından firma ağına ICMP paketinin geri dönmediği görülür. Bu nedenle ping iletişim testi başarısız olur.

Satış sunucusunun varsayılan rotadan çıkıp İnternet Servis Sağlayıcı yönlendiricisi ile çift yönlü haberleşebilmesi için Yönetim yönlendiricisinde Satış sunucusu için statik NAT tanımlanması gerekir.

9. Adım: Yönetim yönlendiricisinde Satış ağındaki sunucu için statik NAT tanımlaması yapınız.

Yonetim(config)#interface Serial0/0/0

Yonetim(config-if)#ip nat outside

Yonetim(config-if)#exit

Yonetim(config)#interface GigabitEthernet 0/0

Yonetim(config-if)#ip nat inside

Yonetim(config)#ip nat inside source static 192.168.1.30 90.0.0.2

10. Adım: Sunucu bilgisayardan İnternet Servis Sağlayıcı yönlendiricisine “ping” komutu ile iletişim testi yapınız. Test bu kez başarılı olacaktır.

5.2.4. Yönlendirici Arayüzlerinde RIP Paketlerinin Gönderiminin Engellenmesi

Yönlendiriciler, ağ bilgilerini yönlendirme protokolünde belirtilen ağlara bağlı oldukları arayüzlerden anons eder. Bu anons, yönlendirici bulunmayan yerel ağlar için de yapılır. Yönlendirme paketlerinin yerel ağlara gönderimi yönlendirici arayüzünde veri trafiğini artırır, ağ performansını düşürür ve güvenliği azaltır. Yönlendirme paketlerinin gönderiminin engellenmesi için yönlendirme protokolü yapılandırılmasında ilgili arayüz bildirilebilir.



BİLGİ

İç ağa dinamik yönlendirme paketlerinin gönderilmesinin engellenmesi, tersi yönden dinamik yönlendirme paketlerinin okunmayacağı anlamına gelmez.

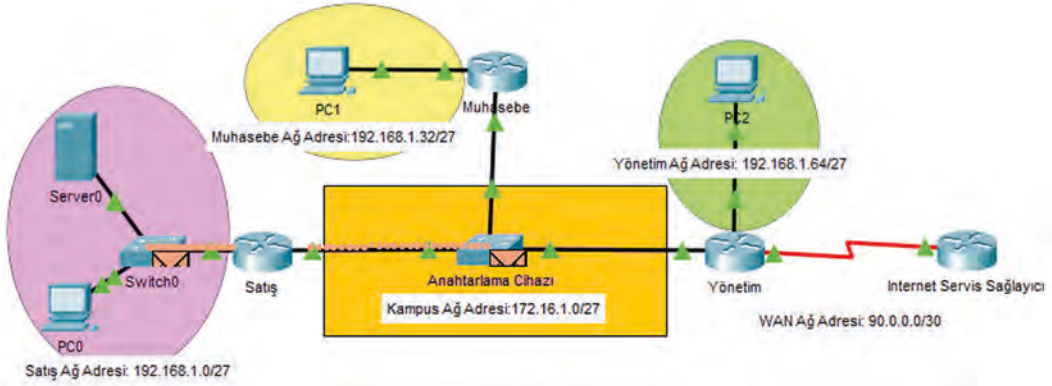


5. UYGULAMA

RIP Paketlerinin Anonsu

Görsel 5.29'da ağ topolojisindeki Satış yönlendiricisi, dördüncü uygulamanın tüm adımları tamamlanarak verilmiştir. İşlem adımlarına göre RIP paketlerinin anonsunu yapınız.

1. Adım: Simülasyon ortamında RIP paketlerini gözlemlemek için Simulation\Show All/None\EditFilters düğmeleri ile sadece RIP paketini seçiniz (Görsel 5.20).“Simülasyon ileri hareket ettir.” düğmesine basınız.



Görsel 5.29: RIP paketlerinin anons yönü

Görsel 5.29'da görüldüğü gibi yönlendirici, RIP paketlerini RIP ağ adreslerinin yazıldığı tüm arayüzlerden gönderir. Bu gönderimler hiç yönlendirici bulunmayan Satış bölümü yerel ağı için de geçerlidir. Satış ağında başka bir RIP ile yapılandırılmış yönlendirici olmadığı için RIP güncelleme paketlerinin gönderilmesi satış ağı için gereksiz veri trafiğine sebeptir.

2. Adım: GigabitEthernet 0/1 arayüzünde güncelleme paketi anonslarını durdurmak için RIP yapılandırmasında “passive-interface” komutunu yazınız.

`Satis(config)#router rip`

`Satis(config-router)#passive-interface GigabitEthernet 0/1`

3. Adım: Simülasyon ortamında RIP paketlerini seçip Satış yönlendiricisini tekrar gözlemleyiniz. GigabitEthernet0/1 arayüzünden RIP güncelleme paketinin gönderilmediği görülecektir.



SIRA SİZDE

Muhasebe ve Yönetim yönlendiricileri yerel ağlarına RIP güncelleme paketlerinin gönderimini durdurmak için yönlendiricilere gerekli komutları yazınız.

5.3. OSPF YÖNLENDİRME PROTOKOLÜ

OSPF (Open Shortest Path First) “ilk açılan en kısa yol” anlamına gelen bağlantı durum yönlendirme protokolüdür. OSPF, farklı marka yönlendirme cihazlarında çalışabilmesi ve kullandığı algoritma ile fazla sayıda yönlendiricinin olduğu ağlarda rota hesaplamalarının yapılabilmesi için genellikle geniş ağlarda yararlanılan bağlantı durum protokolüne dayalı bir dinamik yönlendirme türüdür.

5.3.1. OSPF Özellikleri

OSPF'nin özellikleri şu şekilde sıralanabilir:

- Bağlantı durum protokolüdür.
- Yönlendiriciler tüm ağ haritasını hesaplar.
- Yönlendiricilerde tüm ağ haritası hesaplandığı için kaynak işlemci tüketimi fazladır.
- Hedef rotalar, ağ topolojisinin tümü değerlendirilip, SPF algoritması ile en uygun maliyetli yol hesaplanarak bulunur.
- Yönlendiriciler ağ bilgileri güncelleme paketlerinin paylaşımını OSPF yapılandırmasında ve sonrasında 30 dakikalık periyodik sürelerde yapar. Ağlarda değişiklik oluşmuşsa 30 dakikayı beklemez.
- Ağ değişikliklerini çabuk algılar.
- Varsayılan olarak her 10 saniyede yönlendiriciler arasında Hello (Merhaba) paketleri ile komşu yönlendirici varlığının kontrolü yapılır. 40 saniyede cevap gelmezse komşuluk düşümü olur.
- Sınıfsız ağ bilgisi kullanımını destekler.
- Varsayılan olarak otomatik özetleme yapmaz.
- Yönetimsel uzaklık değeri 110'dur.
- 255 yönlendiriciye kadar komşuluk kurulabildiği için genellikle büyük ölçekli ağlarda kullanılabilir.
- Çoklu yayın IP adresi 224.0.0.5'tir.

5.3.2. OSPF Aşamaları

OSPF ile dört aşama sonucunda yönlendirme tablolarına en ideal rota bilgileri yazılır. OSPF aşamaları şunlardır:

- **Hello Paketi:** Komşu yönlendiricilerin 10 saniye aralıklarla komşuluk kontrollerini gerçekleştirmesidir.
- **LSA Paketi Gönderimi:** Yönlendiriciler kendi ağları için arayüz durum bilgilerini diğer yönlendiriciler ile paylaşır.
- **LSDB Oluşumu:** Tüm yönlendiriciler komşu yönlendiricilerden gelen ağ bilgileri ile ortak bir veri tabanı (LSDB) oluşturur.
- **SPF Algoritma Hesaplaması:** Yönlendiriciler ortak LSDB bilgileri ile rotalar için en uygun maliyetli yol bilgilerini bulur.

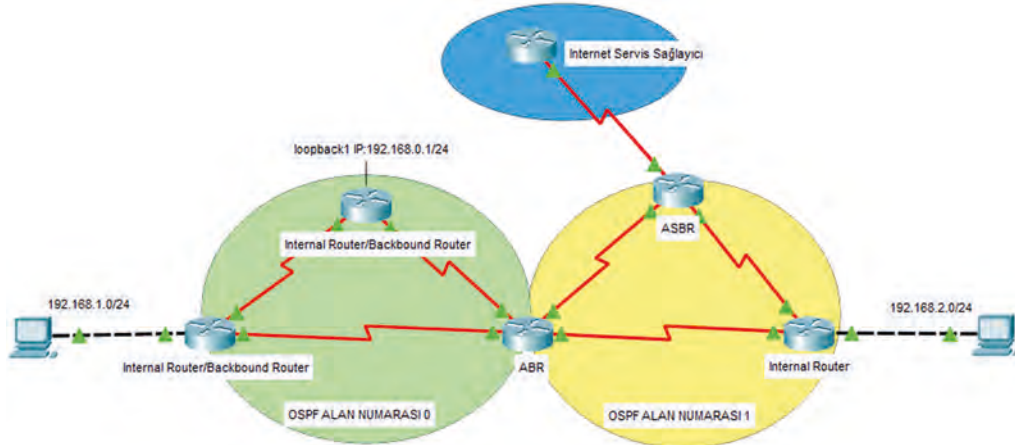
5.3.3. OSPF Yönlendirici Çeşitleri

OSPF yönlendiricileri ağ topolojisinde bulundukları konuma göre farklı isimlendirilir (Görsel 5.30).

- **İç Yönlendirici (IR-Internal Router):** Tek OSPF alanında çalışan yönlendiricilerdir.
- **Omurga Yönlendirici (BR-Backbone Router):** 0 numaralı OSPF alanında çalışan yönlendiriciler-

dir. Omurga yönlendiriciler aynı zamanda iç yönlendiricilerdir.

- **ABR:** Farklı OSPF alanlarında çalışan yönlendiricilerdir.
- **ASBR:** OSPF kullanmayan farklı bir otonom sistem alanına geçiş yönlendiricileridir.



Görsel 5.30: OSPF yönlendirici çeşitleri

5.3.4. OSPF Yapılandırması

Yönlendiricilerde OSPF yapılandırmasını gerçekleştirmek için yönlendirici OSPF işlem numarası, arayüzlerin ağ ve wildcard adresleri, OSPF alanı numarasının protokol bilgisi olarak bildirilmelidir.

OSPF etkinleştirme bildirimi, yönlendirici komut ekranı konfigürasyon satırında “**router ospf** ‘processid’ ” komutu ile yapılır. ‘Processid’, OSPF’nin yönlendiricide işlem numarasıdır. İşlem numarası 1 ile 65536 arasında bir değer alabilir. OSPF dinamik yönlendirme protokolü ile haberleşecek yönlendiriciler aynı işlem numarasını kullanmak zorunda değildir.

OSPF ağ bildirimi ise “**network** ‘ağ adresi’ ‘wildcard adresi’ **area** ‘areaid’ ” şeklinde tanımlanır. ‘Ağ adresi’, yönlendirici arayüzlerinin ağ adresidir. ‘Wildcard adresi’, arayüz ağı alt ağ maskesinin tersi şeklindedir. Wildcard adresi, ağın alt ağ maskesinin her hanesi 255.255.255.255 IP değerinden çıkarılarak bulunabilir. ‘Area id’, OSPF dinamik yönlendirme protokolü ile haberleşecek yönlendiricilerin kullandığı ortak alan numarasıdır. Aynı ortak alandaki yönlendiricilerin alan numarası aynı olmak zorundadır.

`Yönlendirici(config)#router ospf ‘processid(işlem numarası)’`

`Yönlendirici(config-router)#network ‘Arayüz Ağ Adresi’ ‘Wildcard Adresi’ area ‘areaid’`

OSPF işlem numarası 1 olan 0 alanı için 192.168.5.0/24 ağının OSPF network bildirimi şu şekildedir:

`Yönlendirici(config)#router ospf 1`

`Yönlendirici(config-router)#network 192.168.5.0 0.0.0.255 area 0`

OSPF network bildirimlerinin diğer yöntemi de arayüzlerde ayrı ayrı OSPF bildirimleri yapmaktır. Bunun için arayüz yapılandırmalarına girilerek “**ip ospf** ‘processid’ area ‘area id’ ” komutu uygulanır. Bu komutla arayüzün hangi OSPF alanları için çalışacağı belirtilir.

OSPF işlem numarası 1 olan 0 alanı için Serial0/0/0 arayüzünde OSPF network bildirimi şu şekildedir:

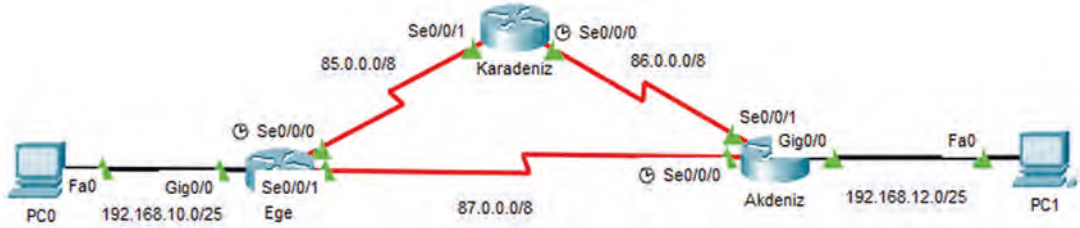
`Yönlendirici(config)#interface serial0/0/0`

`Yönlendirici(config-router)#ip ospf 1 area 0`

6. UYGULAMA

OSPF Yapılandırma

Görsel 5.31’de verilen ağ topolojisini simülasyon programında oluşturunuz. İşlem adımlarına göre Tablo 5.6’da yer alan IP bilgilerini kullanarak ilgili cihazların OSPF yapılandırmasını yapınız.



Görsel 5.31: Altıncı uygulamanın ağ topolojisi

Tablo 5.6: Altıncı Uygulamanın IP Bilgileri

Cihaz	Arayüz	DCE	IP	Alt Ağ Maskesi	Varsayılan Ağ Geçidi
Ege Yönlendiricisi	Serial0/0/0	√ Clock rate 128000	85.0.0.10	255.0.0.0	
	Serial0/0/1		87.0.0.10	255.0.0.0	
	Gi0/0		192.168.10.1	255.255.255.128	
Karadeniz Yönlendiricisi	Serial0/0/0	√ Clock rate 128000	86.0.0.10	255.0.0.0	
	Serial0/0/1		85.0.0.11	255.0.0.0	
Akdeniz Yönlendiricisi	Serial0/0/0	√ Clock rate 128000	87.0.0.12	255.0.0.0	
	Serial0/0/1		86.0.0.12	255.0.0.0	
	Gi0/0		192.168.12.1	255.255.255.128	
PC0			192.168.10.2	255.255.255.128	192.168.10.1
PC1			192.168.12.2	255.255.255.128	192.168.12.1

1. Adım: Tablo 5.6’da cihazlara ait IP bilgileri verilmiştir. Buna göre IP yapılandırmalarını yapınız.

Ege yönlendiricisi için arayüz yapılandırması komut satırları:

```
Router(config)#hostname Ege
Ege(config)#interface serial0/0/0
Ege(config-if)#ip address 85.0.0.10 255.0.0.0
Ege(config-if)#clock rate 128000
Ege(config-if)#no shutdown
Ege(config-if)#exit
Ege(config)#interface serial0/0/1
Ege(config-if)#ip address 87.0.0.10 255.0.0.0
Ege(config-if)#no shutdown
Ege(config-if)#exit
Ege(config)#interface GigabitEthernet 0/0
Ege(config-if)#ip address 192.168.10.1 255.255.255.128
Ege(config-if)#no shutdown
```

2. Adım: Yönlendiriciler için OSPF yapılandırmasını yapınız.

Ege yönlendiricisi için OSPF yönlendirme yapılandırması komut satırları:

```
Ege(config)#router ospf 1
```

```
Ege(config-router)#network 85.0.0.0 0.255.255.255 area 0
```

```
Ege(config-router)#network 87.0.0.0 0.255.255.255 area 0
```

```
Ege(config-router)#network 192.168.10.0 0.0.0.127 area 0
```

Ege yönlendiricisinde OSPF işlem numarası 1 olarak belirlenmiştir. Bu numaranın diğer yönlendiricilerde aynı olma zorunluluğu yoktur ancak anlaşılabilirliği artırmak için aynı numaranın tercih edilmesi önerilebilir.

OSPF alan numarası 0 olarak belirlenmiştir. Aynı otonom sistem içinde alan numarası diğer yönlendiricilerde de eşit olmak zorundadır.

Wilcard adresi 85.0.0.0/8 ve 87.0.0.0/8 ağları için 0.255.255.255'tir. Bu ağların alt ağ maskesi 255.0.0.0'dır. Bu ağların wilcard adreslerini bulmak için şu işlem yapılır:

$$(255.255.255.255)-(255.0.0.0)=(0.0.0.255)$$

192.168.10.0/25 ağının wilcard adresi 0.0.0.127'dir. Bu ağın wilcard adresini bulmak için şu işlem yapılır:

$$(255.255.255.255)-(255.255.255.128)=(0.0.0.127)$$
**SIRA SİZDE**

Karadeniz ve Akdeniz yönlendiricilerinde OSPF dinamik yönlendirme yapılandırmalarını yapınız.

Yönlendiricilerde OSPF yapılandırmaları tamamlandıktan sonra OSPF komşulukları kurulur. OSPF komşuluk bildirimi komut ekranına otomatik olarak gelir (Görsel 5.32).

```
00:00:20: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.10.1 on Serial0/0/0 from LOADING to FULL, Loading Done
00:00:20: %OSPF-5-ADJCHG: Process 1, Nbr 86.0.0.11 on Serial0/0/1 from LOADING to FULL, Loading Done
```

Görsel 5.32: OSFP komşuluk bildirimi

Görsel 5.32'de görülen Akdeniz yönlendiricisi komut ekranında OSPF komşuluk bildirimi satırları verilmiştir. İlk satır için "Nbr 192.168.10.1", komşu Ege yönlendiricisinin ID numarasıdır. "on Serial0/0/0", Ege yönlendiricisi ile hangi arayüzden iletişim kurulduğu bilgisidir. "LOADING to FULL, Loading Done", OSPF komşuluk durumunun başarıyla tamamlandığı anlamına gelir. İkinci satır, Karadeniz yönlendiricisi için OSPF komşuluk durumunun başarıyla tamamlandığı anlamına gelir.

3. Adım: Yönlendiricilerde OSPF komşuluk tablosunu "show ip ospf neighbor" komutu ile görüntüleyiniz (Görsel 5.33).


```
Akdeniz#show ip ospf neighbor
```

Neighbor ID	Pri	State	Dead Time	Address	Interface
192.168.10.1	0	FULL/ -	00:00:38	87.0.0.10	Serial0/0/0
86.0.0.11	0	FULL/ -	00:00:38	86.0.0.11	Serial0/0/1

Görsel 5.33: OSPF komşuluk tablosu

Görsel 5.33'te Akdeniz yönlendiricisi için OSPF komşulukları tablosu verilmiştir. Akdeniz yönlendiricisi OSPF ile Ege ve Karadeniz yönlendiricileriyle komşuluk kurmuştur. OSPF komşuluk tablosu başlık açıklamaları şunlardır:

- **Neighbor ID:** Komşu yönlendirici ID numarasıdır. OSPF için yönlendirici ID numarası el ile girilmemişse arayüzlerindeki en büyük IP numarasıdır. "192.168.10.1" Ege yönlendiricisinin aynı zamanda Router ID değeridir.

- **Pri:** WAN gibi noktadan noktaya bağlı ağlar için OSPF Priority değeri 0'dır. Broadcast ağlar için bu değer 1'dir.

- **State:** OSPF komşuluk durumudur. FULL, OSPF komşuluğunun başarıyla tamamlandığı anlamına gelir.

- **Dead Time:** Komşu yönlendirici için komşuluğun kopma süresidir. Varsayılan olarak 40 saniyedir. OSPF Hello paketi süresi 10 saniyede bir olduğu için sağlıklı çalışan bir OSPF komşuluğunda "dead time" süresi 30 saniyeden aşağı düşmez.

- **Address:** Komşu yönlendiricinin arayüzden iletişim kurduğu IP numarasıdır.

- **Interface:** Yönlendiricinin komşu yönlendirici ile iletişim kurduğu arayüzün adıdır.

4. Adım: Yönlendiricilerde oluşan OSPF yönlendirme tablolarını "show ip route ospf" komutu ile görüntüleyiniz.

Ege yönlendiricisi için yönlendirme tablosu Görsel 5.34'te verilmiştir.

```
Ege#show ip route ospf
O    86.0.0.0 [110/128] via 85.0.0.11, 00:32:39, Serial0/0/0
    [110/128] via 87.0.0.12, 00:32:39, Serial0/0/1
    192.168.12.0/25 is subnetted, 1 subnets
O    192.168.12.0 [110/65] via 87.0.0.12, 00:32:39, Serial0/0/1
```

Görsel 5.34: Yönlendiricide OSPF yönlendirme tablosu

Ege yönlendiricisi OSPF ile 85.0.0.0 ağı ve 192.168.12.0/25 ağı olmak üzere iki yeni ağ öğrenmiştir. Yönlendirme tablosunun ikinci satır açıklamaları şu şekildedir:

- **O:** OSPF yönlendirme satırıdır.
- **192.168.12.0:** OSPF ile öğrenilmiş hedef ağ adresidir.
- **[110/65]:** 110, OSPF yönetimsel değeridir. 65 ise hedef ağ için toplam maliyet metrik değeridir.
- **Via 87.0.0.12:** "192.168.12.0" ağına gitmek için kullanılacak rotadaki komşu yönlendirici IP bilgisidir.
- **00:32:39:** OSPF komşuluğu kurulduğu andan itibaren geçen süredir.
- **Serial0/0/1:** "192.168.12.0" ağına gitmek için yönlendiricide çıkış yapılan arayüz adıdır.

OSPF yönlendirme tablosunda SPF algoritmasına göre hesaplanmış en az metrik değerine sahip yol, tercih yolu olarak yönlendirme tablosuna yazılır. Alternatif yollar, birinci rotada aksaklık meydana gelirse yeniden hesaplanarak bulunabilir.

Görsel 5.34'teki Ege yönlendiricisi ilk satırında 86.0.0.0 hedef ağı için eşit metrik değerine sahip [110/128] iki farklı rota vardır. Eşit metrik değerine sahip rotalar yönlendirme tablosuna yazılır. Bu ağlara erişim, rotaların sırayla kullanılması şeklinde gerçekleşir.

5. Adım: PC0'dan PC1'e "tracert 192.168.12.2" komutu ile rota görüntülemesi yapınız (Görsel 5.35).

```
C:\>tracert 192.168.12.2

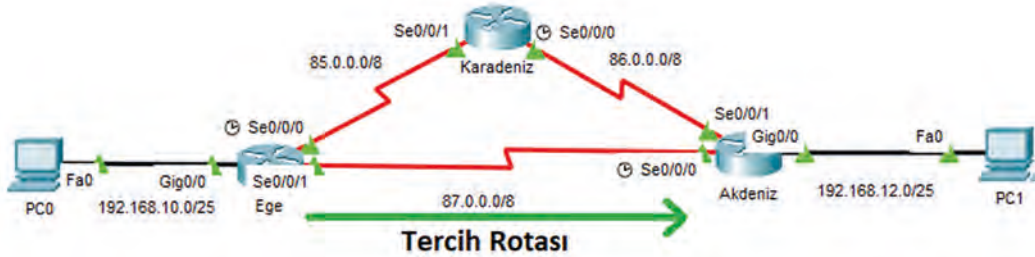
Tracing route to 192.168.12.2 over a maximum of 30 hops:

  1  0 ms    0 ms    0 ms    192.168.10.1
  2  4 ms    1 ms    1 ms    87.0.0.12
  3  1 ms    2 ms    1 ms    192.168.12.2

Trace complete.
```

Görsel 5.35: Tracert komutu ile PC0, PC1 rota tespiti

Tracert ICMP paketleri PC0'dan PC1'e gitmek için sırası ile üç adımda 192.168.10.1 (Ege Yönlendiricisi), 87.0.0.12 (Akdeniz Yönlendiricisi) ve 192.168.12.2 (PC1) güzergâhını kullanmıştır. Görsel 5.36'da bu güzergâhı tercih rotası olarak görebilirsiniz.



Görsel 5.36: OSPF tercih rotası

6. Adım: Ege yönlendiricisinde Serial0/0/1 arayüzünü "shutdown" komutu ile kapatınız.

```
Ege(config)#interface Serial0/0/1
```

```
Ege(config-if)#shut down
```

Kapatılan arayüz, Akdeniz yönlendiricisi ile doğrudan bağlantı kuran arayüzdür. Komşuluğun düşüğünü komut satırında "%OSPF-5-ADJCHG: Process 1, Nbr 192.168.12.1 on Serial0/0/1 from FULL to DOWN, NeighborDown: Interface down or detached" mesajı ile görebilirsiniz.

7. Adım: Ege yönlendiricisinde "show ip route ospf" komutu ile güncellenmiş yönlendirme tablosunu tekrar görüntüleyiniz (Görsel 5.37).

```
Ege#sh ip route ospf
O    86.0.0.0 [110/128] via 85.0.0.11, 00:00:10, Serial0/0/0
    192.168.12.0/25 is subnetted, 1 subnets
O    192.168.12.0 [110/129] via 85.0.0.11, 00:00:10, Serial0/0/0
```

Görsel 5.37: Metrik değerleri yenilenmiş OSPF yönlendirme tablosu

Görsel 5.37’de görüldüğü gibi hedef ağlar için metrik değerleri yeniden hesaplanmıştır. İlk satırda 86.0.0.0 ağı için 85.0.0.11 IP’si ile (Karadeniz yönlendiricisi) tek rota kalmıştır. İkinci satırda 192.168.12.0 ağı için metrik değeri hesaplanmış ve 65’ten 129’a çıkmıştır. Rota ise 85.0.0.11 IP’si ile (Karadeniz yönlendiricisi) üzerinden tanımlanmıştır.

8. Adım: PC0’dan PC1’e “tracert 192.168.12.2” komutu ile rota görüntülemesini tekrar yapınız (Görsel 5.38).

```
C:\>tracert 192.168.12.2

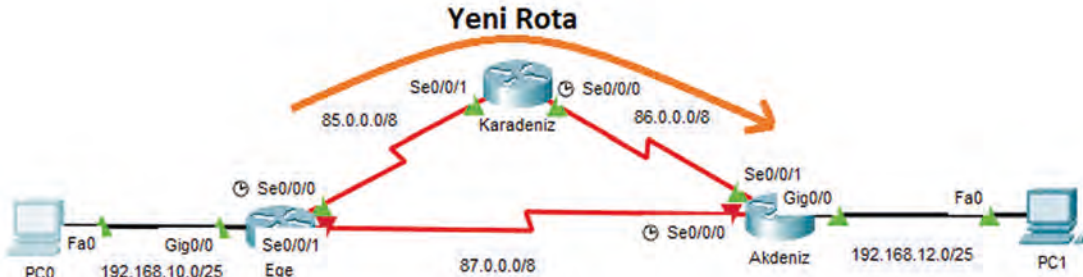
Tracing route to 192.168.12.2 over a maximum of 30 hops:

  0  0 ms    0 ms    0 ms    192.168.10.1
  1  1 ms    1 ms    1 ms    85.0.0.11
  2  1 ms    2 ms    2 ms    86.0.0.12
  3  4 ms    0 ms    0 ms    192.168.12.2

Trace complete.
```

Görsel 5.38: Tracert komutu ile PC0 ve PC1 arası yenilenmiş rota bilgisi

Tracert ICMP paketleri PC0’dan PC1’e gitmek için sırası ile dört adımda 192.168.10.1 (Ege yönlendiricisi), 85.0.0.11 (Karadeniz yönlendiricisi), 86.0.0.11 (Akdeniz yönlendiricisi) ve 192.168.12.2 (PC1) güzergâhını kullanmıştır. Beşinci adımdaki rota, Görsel 5.39’daki gibi değişmiştir.



Görsel 5.39: Yenilenmiş rota güzergâhı

9. Adım: Ege yönlendiricisinde Serial0/0/1 arayüzünü yeniden kullanıma açıp PC0’dan PC1 için “ping 192.168.12.2” komutu ile iletişim testi gerçekleştiriniz. İletişim testi başarılı olacaktır. Bu adımda rotalar yeniden ilk hâli gibi metrik değerleri ile hesaplanıp güncellenecektir.

10. Adım: Ege yönlendiricisinde “show ip protocols” komutunu kullanarak aktif yönlendirme protokolünü görüntüleyiniz (Görsel 5.40).

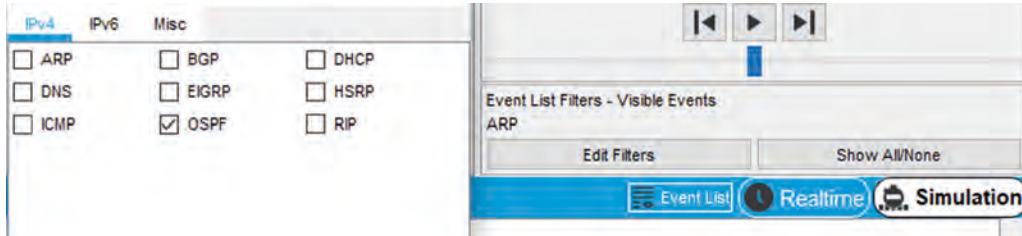
Görsel 5.40’ta Ege yönlendiricisi için yönlendirme protokol tablosundan aktif yönlendirmenin “OSPF 1”, yönlendirici ID numarasının “192.168.10.1”, yönetimsel uzaklık değerinin “110” olduğu görülür. Tabloda “Routing for Networks” satırlarında yönlendiricide bildirimi yapılan ağlar, “Routing Information Source” satırlarında yönlendirme bilgisi okunan kaynaklar görülebilir. Yönlendirme protokolü tablosu, yönlendiricilerde doğrulama amaçlı kullanılabilir.

```
Ege#sh ip protocols
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed
state to up

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 192.168.10.1
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    85.0.0.0 0.255.255.255 area 0
    192.168.10.0 0.0.0.127 area 0
    87.0.0.0 0.255.255.255 area 0
  Routing Information Sources:
    Gateway         Distance      Last Update
    86.0.0.11        110           00:23:28
    192.168.10.1      110           00:00:00
    192.168.12.1      110           00:00:05
  Distance: (default is 110)
```

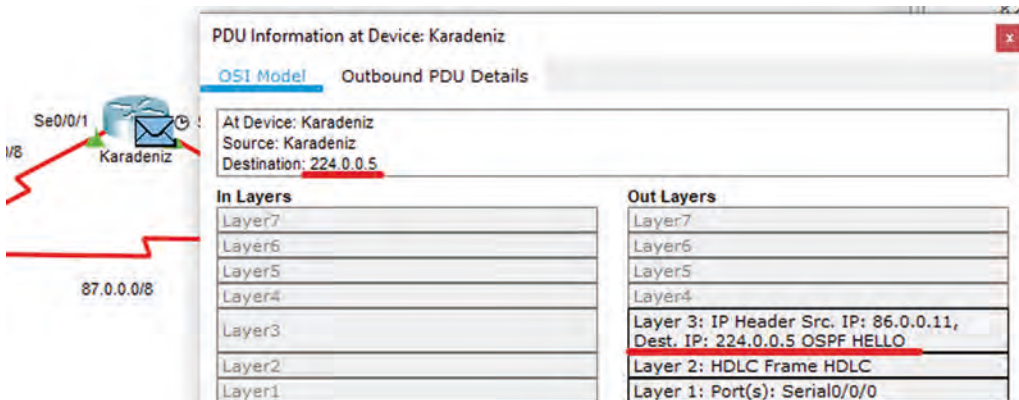
Görsel 5.40: Ege yönlendiricisinin aktif yönlendirme protokolü bilgisi

11. Adım: Simülasyon ortamında OSPF Hello paketi çoklu yayın IP adresini görmek için Simulation\Show All/None>EditFilters düğmeleri ile sadece OSPF paketini seçiniz (Görsel 5.41). “Simülasyon ileri hareket ettir.” düğmesine basınız.



Görsel 5.41: Simülasyon programında OSPF paket seçimi

Topolojide yönlendiriciler için oluşan OSPF paketlerinden birinin üzerine tıklayınız ve Görsel 5.42’deki gibi OSPF çoklu yayın IP adresinin 224.0.0.5 olduğunu gözlemleyiniz.



Görsel 5.42: OSPF çoklu yayın adresi

12. Adım: Ege ve Akdeniz yönlendiricilerinde yerel ağlara OSPF Hello paketleri gönderimini durdurmak için yönlendirici OSPF yapılandırılmalarında “passive-interface GigabitEthernet0/0” komutunu uygulayınız.

```
Ege(config)#router ospf 1
Ege(config-router)#passive-interface GigabitEthernet0/0
Akdeniz(config)#router ospf 1
Akdeniz(config-router)#passive-interface GigabitEthernet0/0
```

13. Adım: Simülasyon programında Realtime düğmesine basınız. Ege yönlendiricisi komut satırında “debug ip ospf events” komutunu giriniz (Görsel 5.43).

```
Ege#debug ip ospf events
OSPF events debugging is on
Ege#
02:08:06: OSPF: Rcv hello from 86.0.0.11 area 0 from Serial0/0/0 85.0.0.11

02:08:06: OSPF: End of hello processing

02:08:13: OSPF: Rcv hello from 192.168.12.1 area 0 from Serial0/0/1 87.0.0.12

02:08:13: OSPF: End of hello processing

02:08:16: OSPF: Rcv hello from 86.0.0.11 area 0 from Serial0/0/0 85.0.0.11

02:08:16: OSPF: End of hello processing

02:08:23: OSPF: Rcv hello from 192.168.12.1 area 0 from Serial0/0/1 87.0.0.12

02:08:23: OSPF: End of hello processing
```

Görsel 5.43: Yönlendiricilerde OSPF Hello paketi olay görüntüleme

Görsel 5.43'te Ege yönlendiricisinde OSPF Hello paketlerinin olay izlemesi açılmıştır. Komşu yönlendiricilerden 10 saniyede bir gelen Hello paketleri bu şekilde gözlemlenebilir. OSPF sorunlarında Hello paketinin kontrolü amacı ile bu gözlem kullanılabilir. Bu işlemi iptal etmek için yönlendirme komut satırında “no debug ip ospf events” komutunu uygulayınız.

5.3.5. OSPF Rota Maliyet Hesaplama

OSPF, SPF algoritmasını kullanan dinamik yönlendirme protokolüdür. SPF algoritması, kaynaktan hedefe doğru tüm yönlendiricilerin arayüz bağlantı bilgilerine bakıp, toplam yol maliyetini metrik değeri olarak bulur. En az maliyetli yollar öncelikli rota tercihi olarak kullanılır. Arayüz maliyetleri bulunurken arayüzün fiziksel bant genişliği bilgisi öncelikli değerlendirilir. Bant genişliği yüksek olan arayüz bağlantılarının maliyet değeri daha düşük hesaplanacağı için öncelikli olarak tercih edilen rotalarda kullanılır.

Arayüzlerin bant genişlikleri veya doğrudan maliyet bilgisi komutla değiştirilerek rotalar da değiştirilebilir.

Arayüz türleri, varsayılan bant genişlikleri ve maliyetleri Tablo 5.7’de verilmiştir.

Tablo 5.7: Arayüz Türü, Varsayılan Bant Genişliği ve Maliyet Tablosu

Arayüz Türü	Bant Genişliği	Maliyet
Serial	1544 Kilobit/s	64
Fast Ethernet	100.000 Kilobit/s	1
Gigabit Ethernet	1.000.000 Kilobit/s	1

Arayüz maliyetleri, varsayılan bant genişliği referans değerinin arayüz bant genişliklerine bölünmesi ile hesaplanır. Bulunan sonuç tam sayıya yuvarlanır.

Maliyet=Varsayılan Bant Genişliği Referans Değeri / Arayüz Bant Genişliği

Serial arayüzler için $100.000/1544=64,78$ olarak hesaplanır. 64,78 ondalık sayısı 64’e yuvarlanır.

Fast Ethernet için $100.000/100.000=1$ olarak hesaplanır.

Gigabit Ethernet için $100.000/1.000.000=0,1$ olarak hesaplanır. 0,1 ondalık sayısı 1’e yuvarlanır.

Dikkat edilirse Fast Ethernet ve Gigabit Ethernet maliyetleri 1 olarak hesaplanmıştır.

Yönlendiricilerde Gigabit ve Fast Ethernet arayüzlerinin farklı hesaplanması için arayüz varsayılan bant genişliği referans değerini değiştirmek mümkündür. Yönlendirici OSPF yapılandırmasında varsayılan bant genişliği referans değerini değiştirmek için “auto-costreference-bandwidth ‘Mbit değeri’” şeklinde komut kullanılır. Fast Ethernet ve Gigabit Ethernet arayüzlerinin kullanıldığı yönlendiricilerdeki OSPF yapılandırmasında bu değerin “auto-cost reference-bandwidth 1000” komutu ile 1 Gigabite çıkarılması önerilir.

Yönlendirici arayüz bant genişliği değerini değiştirmek için arayüz içinde “bandwidth ‘Kilobit değeri’” yazılır. Yönlendirici arayüz maliyet değerini doğrudan değiştirmek için arayüz içinde “cost ‘Maliyet değeri’” yazılır.



BİLGİ

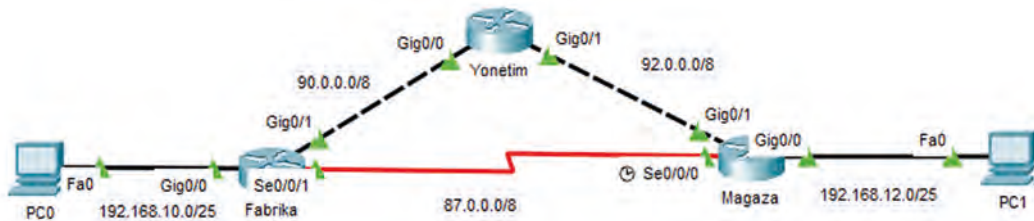
Bant genişlik bilgisi değiştirilen arayüzlerde fiziksel bant genişliği aktarım hızlarında değişiklik olmaz. Bu bilginin değişimi rotalara müdahale içindir.



7. UYGULAMA

OSPF Yapılandırma

Görsel 5.44’te verilen ağ topolojisini simülasyon programında oluşturunuz. İşlem adımlarına göre Tablo 5.8’de yer alan IP bilgilerini kullanıp ilgili cihazların OSPF yapılandırmasını yapınız.



Görsel 5.44: Yedinci uygulamanın ağ topolojisi

Tablo 5.8: Yedinci Uygulamanın IP Bilgileri

Cihaz	Arayüz	DCE	IP	Alt Ağ Maskesi	Varsayılan Ağ Geçidi
Fabrika Yönlendiricisi	G0/1		90.0.0.10	255.0.0.0	
	Serial0/0/1		87.0.0.10	255.0.0.0	
	G0/0		192.168.10.1	255.255.255.128	
Yönetim Yönlendiricisi	G0/0		90.0.0.11	255.0.0.0	
	G0/1		92.0.0.11	255.0.0.0	
Mağaza Yönlendiricisi	Serial0/0/0	v Clock rate128000	87.0.0.12	255.0.0.0	
	G0/1		92.0.0.12	255.0.0.0	
	G0/0		192.168.12.1	255.255.255.128	
PC0			192.168.10.2	255.255.255.128	192.168.10.1
PC2			192.168.12.2	255.255.255.128	192.168.12.1

1. Adım: Fabrika, Yönetim ve Mağaza yönlendiricilerinde IP yapılandırmasını yapınız.

Fabrika yönlendiricisi için arayüz IP yapılandırmaları:

```
Fabrika(config)#interface Serial0/0/1
```

```
Fabrika(config-if)#ip address 87.0.0.10 255.0.0.0
```

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

```
Fabrika(config-if)#exit
```

```
Fabrika(config)#interface GigabitEthernet 0/1
```

```
Fabrika(config-if)#ip address 90.0.0.10 255.0.0.0
```

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

```
Fabrika(config-if)#exit
```

```
Fabrika(config)#interface GigabitEthernet 0/0
```

```
Fabrika(config-if)#ip address 192.168.10.1 255.255.255.128
```

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

```
Fabrika(config-if)#exit
```

2. Adım: Fabrika, Yönetim ve Mağaza yönlendiricilerinde OPSF işlem numarası 1, OSPF alanı 0 olarak yönlendirme yapılandırmalarını yapınız.

Fabrika yönlendiricisi için OSPF komutları şunlardır:

```
Fabrika(config)#router ospf 1
```

```
Fabrika(config-router)#network 90.0.0.0 0.255.255.255 area 0
```

```
Fabrika(config-router)#network 87.0.0.0 0.255.255.255 area 0
```

```
Fabrika(config-router)#network 192.168.10.0 0.0.0.127 area 0
```



SIRA SİZDE

Yönetim ve Mağaza yönlendiricilerinin OSPF yapılandırmalarını gerçekleştiriniz.

3. Adım: Fabrika yönlendiricisinde OSPF yönlendirme tablosunu “show ip route ospf” komutu ile görüntüleyiniz (Görsel 5.45).

```
Fabrika#sh ip route ospf
O    92.0.0.0 [110/2] via 90.0.0.11, 00:00:04, GigabitEthernet0/1
    192.168.12.0/25 is subnetted, 1 subnets
O    192.168.12.0 [110/3] via 90.0.0.11, 00:00:04, GigabitEthernet0/1
```

Görsel 5.45: Fabrika yönlendiricisi OSPF yönlendirme tablosu-1

192.168.12.0 ağı için metrik maliyeti 3 olarak hesaplanmıştır. Rota yönü ise 90.0.0.11 IP'si ile Yönetim yönlendiricisi üzerinden yapılmıştır.

4. Adım: PC0'dan PC1'e rota bilgisini görüntülemek için “tracert 192.168.12.2” komutunu uygulayınız (Görsel 5.46).

```
C:\>tracert 192.168.12.2

Tracing route to 192.168.12.2 over a maximum of 30 hops:

  1  1 ms    0 ms    0 ms    192.168.10.1    Fabrika
  2  0 ms    0 ms    0 ms    90.0.0.11      Yonetim
  3  0 ms    0 ms    0 ms    92.0.0.12      Magaza
  4  0 ms    0 ms    1 ms    192.168.12.2
```

Görsel 5.46: PC0'dan PC1'e giden rota tablosu-1

Fabrika, Yönetim ve Mağaza yönlendiricileri güzergâhı ile PC0'dan PC2'ye gidilmiştir (Görsel 5.46).

Rota hesaplanırken yönlendirici sayısı en az olan yol tercih edilmemiştir. OSPF, bağlantı durumlarına göre SPF algoritması ile rota hesabı yaptığı için arayüzlerin bant genişlikleri hesaplanarak rota metrik maliyet değeri en az olan yol tercih edilmiştir.

Fabrika yönlendiricisinden Yönetim yönlendiricisine bağlantı Gigabit Ethernet ile yapılmıştır. Fabrika yönlendiricisinde GigabitEthernet0/1 arayüz maliyet değeri 1'dir.

Yönetim yönlendiricisinden Mağaza yönlendiricisine bağlantı Gigabit Ethernet ile yapılmıştır. Yönetim yönlendiricisinde GigabitEthernet0/1 maliyet değeri 1'dir.

Mağaza yönlendiricisinde PC2'ye bağlantı Gigabit Ethernet ile yapılmıştır. Mağaza yönlendiricisinde GigabitEthernet0/0 arayüzü maliyet değeri 1'dir.

Rota metrik değeri (Fabrika->Yonetim :1)+(Yonetim->Magaza:1)+(Magaza->PC2:1)=3 olarak bulunmuştur.



UYARI

Altıncı uygulamanın ağ topolojisi, 192.168.12.0 ağının metrik değerini serial arayüzler kullanıldığı için 65 olarak bulmuştur (Görsel 5.34). Rota yönü ise PC0'dan PC1'e doğru Fabrika, Mağaza, PC1 şeklindedir (Görsel 5.35, Görsel 5.36).

5. Adım: PC0, PC1 arasındaki rotayı değiştirmek için arayüz bant genişliklerini şu şekilde düzenleyiniz:

Fabrika yönlendiricisi GigabitEthernet0/1 arayüzü bant genişliği: 5 Mbit

Yönetim yönlendiricisi GigabitEthernet0/1 arayüzü bant genişliği: 4 Mbit

`Fabrika(config)#interface GigabitEthernet 0/1`

`Fabrika(config-if)#bandwidth 5000`

`Yonetim(config)#interface GigabitEthernet 0/1`

`Yonetim(config-if)#bandwidth 4000`

6. Adım: Fabrika yönlendiricisinde “show ip route ospf” komutu ile OSPF yönlendirme tablosunu tekrar görüntüleyiniz.

Görsel 5.47’de 90.0.0.0 ve 192.168.12.0 ağları için toplam metrik değeri değişmiştir. 92.0.0.0 ve 192.168.12.0 ağları için rota değişmemiştir.

```
O 92.0.0.0 [110/45] via 90.0.0.11, 00:00:31, GigabitEthernet0/1
  192.168.12.0/25 is subnetted, 1 subnets
O   192.168.12.0 [110/46] via 90.0.0.11, 00:00:31, GigabitEthernet0/1
```

Görsel 5.47: Fabrika yönlendiricisi OSPF yönlendirme tablosu-2

192.168.12.0 ağı için yapılan işlemlerde;

Fabrika yönlendiricisi GigabitEthernet0/1 arayüzü bant genişliği 5 Megabit ve maliyet değeri 100000/5000=20,

Yönetim yönlendiricisi GigabitEthernet0/1 arayüzü bant genişliği 4 Megabit ve maliyet değeri 100000/4000=25,

Mağaza yönlendiricisi GigabitEthernet0/0 arayüzü bant genişliği 1 Gigabit ve maliyet değeri 100000/1000000=1 (yuvarlanarak),

Toplamda metrik değeri 20+25+1=46 olarak bulunmuştur.

7. Adım: Fabrika yönlendiricisinde Serial0/0/1 arayüzünün bant genişliğini 20 Megabit yapınız.

`Fabrika(config)#interface Serial0/0/1`

`Fabrika(config-if)#bandwidth 20000`

8. Adım: Fabrika yönlendiricisinde “show ip route ospf” komutu ile OSPF yönlendirme tablosunu tekrar görüntüleyiniz.

Görsel 5.48’de 92.0.0.0 ve 192.168.12.0 ağları için metrik değeri ve rota değişmiştir.

```
Fabrika#sh ip route ospf
O 92.0.0.0 [110/6] via 87.0.0.12, 00:00:02, Serial0/0/1
  192.168.12.0/25 is subnetted, 1 subnets
O   192.168.12.0 [110/6] via 87.0.0.12, 00:00:02, Serial0/0/1
```

Görsel 5.48: Fabrika yönlendiricisi OSPF yönlendirme tablosu-3

192.168.12.0 ağı için yapılan işlemlerde Fabrika yönlendiricisi Serial0/0/1 arayüzü 20 Megabit olarak değişmiştir. Arayüzün yeni maliyet değeri 100000/20000=5 olarak hesaplanmıştır. Mağaza yönlendiricisinin GigabitEthernet 0/0 arayüz maliyet değeri 1’dir. İki arayüzün toplam maliyet metrik değeri 5+1=6 şeklinde hesaplanmıştır. Ayrıca rota yönü, 87.0.0.12 IP’si ile doğrudan Mağaza yönlendiricisi üzerinden belirlenmiştir.

9. Adım: PC0'dan PC1'e yeni rota bilgisini görüntülemek için "tracert 192.168.12.2" komutunu uygulayınız (Görsel 5.49).

```
C:\>tracert 192.168.12.2

Tracing route to 192.168.12.2 over a maximum of 30 hops:

  1  2 ms    2 ms    2 ms    192.168.10.1  Fabrika
  2  5 ms    5 ms    5 ms    92.0.0.12    Magaza
  3  7 ms    7 ms    7 ms    192.168.12.2

Trace complete.
```

Görsel 5.49: PC0'dan PC1'e giden rota tablosu-2

Görsel 5.49'da görüldüğü gibi PC0'dan PC1 için rota bilgisi, 192.168.10.1 Fabrika yönlendiricisi ve 92.0.0.12 Mağaza yönlendiricisi üzerinden yapılmıştır.



BİLGİ

OSPF arayüz maliyet metrik değerleri, veri trafiğinin arayüzden çıkış yönü için hesaplanır.

10. Adım: Yönetim ve Mağaza yönlendiricilerinde OSPF yönlendirme tablolarını "show ip route ospf" komutu ile görüntüleyerek hedef ağlar için toplam maliyet metrik değerlerini bulunuz.

11. Adım: Simülasyon programında simülasyon durumuna gelerek ICMP paketlerini seçiniz ve PC'ler arasında ping iletişim testi gerçekleştirerek rotaları ICMP paketleri ile izleyiniz.



8. UYGULAMA

OSPF Maliyet Yapılandırması

İşlem adımlarına göre yedinci uygulamadaki ağ topolojisini (Görsel 5.44) ve IP bilgilerini (Tablo 5.8) kullanarak OSPF maliyet yapılandırmasını yapınız. Yedinci uygulama yapılmış ise üçüncü adım ve sonrası adımlar gerçekleştirilebilir.

1. Adım: Fabrika, Yönetim ve Mağaza yönlendiricilerinde IP yapılandırmalarını gerçekleştiriniz.

Mağaza yönlendiricisi için arayüz IP yapılandırmaları:

```
Magaza(config)#interface Serial0/0/0
Magaza(config-if)#ip address 87.0.0.12 255.0.0.0
Magaza(config-if)#clock rate 128000
Magaza(config-if)#no shutdown
Magaza(config-if)#exit
Magaza(config)#interface GigabitEthernet 0/1
Magaza(config-if)#ip address 92.0.0.12 255.0.0.0
Magaza(config-if)#no shutdown
Magaza(config-if)#exit
```

```
Magaza(config)#interface GigabitEthernet 0/0
Magaza(config-if)#ip address 192.168.12.1 255.255.255.128
Magaza(config-if)#no shutdown
Magaza(config-if)#exit
```

2. Adım: Fabrika, Yönetim ve Mağaza yönlendiricilerinde OPSF işlem numarası 1, OSPF alanı 0 olarak yönlendirme yapılandırmalarını yapınız.

Fabrika yönlendiricisi için OSPF komutları şunlardır:

```
Magaza(config)#router ospf 1
Magaza(config-router)#network 92.0.0.0 0.255.255.255 area 0
Magaza(config-router)#network 87.0.0.0 0.255.255.255 area 0
Magaza(config-router)#network 192.168.12.0 0.0.0.127 area 0
```

3. Adım: Mağaza yönlendiricisi için OSPF yönlendirme tablosunu “show ip route ospf” komutu ile görüntüleyiniz (Görsel 5.50).

```
Magaza#sh ip route ospf
O    90.0.0.0 [110/2] via 92.0.0.11, 00:01:34, GigabitEthernet0/1
    192.168.10.0/25 is subnetted, 1 subnets
O    192.168.10.0 [110/3] via 92.0.0.11, 00:01:34, GigabitEthernet0/1
```

Görsel 5.50: Mağaza yönlendiricisi OSPF yönlendirme tablosu-1

Mağaza yönlendiricisinin 90.0.0.0 ağı için 2, 192.168.10.0 ağı için 3 toplam maliyet metrik değeri ile erişebildiği Görsel 5.50'deki yönlendirme tablosundan anlaşılır. Rota yönü ise 92.0.0.11 ile Yönetim yönlendiricisinden yapılır.

4. Adım: Mağaza yönlendiricisi GigabitEthernet 0/1 arayüz maliyet değerini “ip ospf cost 10” komutu ile arayüzde güncelleyiniz.

```
Magaza(config)#interface GigabitEthernet 0/1
Magaza(config-if)#ip ospf cost 10
```

5. Adım: Yönetim yönlendiricisinde GigabitEthernet 0/0 arayüz maliyet değerini “ip ospf cost 30” komutu ile arayüzde güncelleyiniz.

```
Yonetim(config)#interface GigabitEthernet 0/0
Yonetim(config-if)#ip ospf cost 30
```

6. Adım: Mağaza yönlendiricisi için OSPF yönlendirme tablosunu “show ip route ospf” komutu ile tekrar görüntüleyiniz (Görsel 5.51).

```
Magaza#sh ip route ospf
O    90.0.0.0 [110/40] via 92.0.0.11, 00:00:49, GigabitEthernet0/1
    192.168.10.0/25 is subnetted, 1 subnets
O    192.168.10.0 [110/41] via 92.0.0.11, 00:00:49, GigabitEthernet0/1
```

Görsel 5.51: Mağaza yönlendiricisi OSPF yönlendirme tablosu-2

Mağaza yönlendiricisi için hedef 90.0.0.0 ve 192.168.10.0 ağları toplam maliyet metrik değerleri sırası ile 40 ve 41 şeklinde güncellenmiştir. Hedef ağlar için rota yönü ise değişmemiştir. Rota yönü yine Yönetim yönlendiricisi üzerinden yapılır. Mağaza yönlendiricisi GigabitEthernet0/1 arayüz maliyet değeri 10, Yönetim yönlendiricisi GigabitEthernet0/0 arayüz maliyet değeri 30 şeklinde güncellenmiştir. 90.0.0.0 hedef ağı için her iki yönlendirici arayüz maliyet toplamı $10+30=40$ şeklinde hesaplanmıştır. 192.168.10.0 ağı için ise Fabrika yönlendiricisinin GigabitEthernet0/0 arayüz maliyeti de eklenerek $10+30+1=41$ şeklinde toplam maliyet metrik değeri hesaplanmıştır. Serial arayüzlerin maliyet değeri 64 ve $64>40$ olduğu için rota yönünde bir değişiklik görülmemiştir.

“ip ospf cost” komutu ile bant genişliği değeri verilmeden maliyet değeri arayüzlere doğrudan atanmıştır.

7. Adım: Mağaza yönlendiricisi Serial0/0/0 arayüz maliyetini “ip ospf cost 25” komutu ile güncelleyiniz.

Mağaza(config)#interface Serial0/0/0

Mağaza(config-if)#ip ospf cost 25

8. Adım: Mağaza yönlendiricisi için OSPF yönlendirme tablosunu “show ip route ospf” komutu ile tekrar görüntüleyiniz (Görsel 5.52).

```
Mağaza#sh ip route ospf
O    90.0.0.0 [110/40] via 92.0.0.11, 00:15:53, GigabitEthernet0/1
    192.168.10.0/25 is subnetted, 1 subnets
O    192.168.10.0 [110/26] via 87.0.0.10, 00:01:51, Serial0/0/0
```

Görsel 5.52: Mağaza yönlendiricisi OSPF yönlendirme tablosu-3

Görsel 5.51’de hedef 192.168.10.0 ağı için rota yönü 87.0.0.10 IP’si ile doğrudan Fabrika yönlendiricisi olmuştur. Rota metrik maliyet değeri ise $25+1=26$ şeklinde güncellenmiştir. Hedef 90.0.0.0 ağı için rota, Yönetim yönlendiricisi üzerinden devam etmiştir. Bunun sebebi, yedinci uygulamada Fabrika yönlendiricisi GigabitEthernet0/1 arayüzünün bant genişliği değerinin 5000 kilobit şeklinde ayarlanmasıdır. 5000 kilobit için maliyet değeri $100000/5000=20$ şeklinde hesaplanır. Mağaza yönlendiricisi ile 90.0.0.0 ağına serial arayüz bağlantısı üzerinden bağlanılırsa Fabrika yönlendiricisinin GigabitEthernet0/1 arayüzünden rota tamamlanır.

Bu durumda maliyet $25+20=45$ olacaktır. Mağaza yönlendiricisi, 90.0.0.0 ağına Yönetim yönlendiricisi üzerinden $10+30=40$ metrik değerinde toplam maliyetle bağlanabilir. Yönetim yönlendiricisi ile bağlanmak daha az maliyet oluşturduğu için 90.0.0.0 ağına giden rota, 92.0.0.11 IP’si ile Yönetim yönlendiricisi üzerinden yapılır (Yedinci uygulamayı gerçekleştirmeden bu uygulamayı yapanlar için OSPF yönlendirme tablosu değerleri farklı olacaktır.).

9. Adım: PC1’den PC0’a giden rotayı “tracert 192.168.10.2” komutu ile görüntüleyiniz (Görsel 5.53).


```

C:\>tracert 192.168.10.2

Tracing route to 192.168.10.2 over a maximum of 30 hops:

  1  0 ms    0 ms    0 ms    192.168.12.1    Mağaza
  2  2 ms    0 ms    0 ms    87.0.0.10      Fabrika
  3  1 ms    0 ms    1 ms    192.168.10.2

Trace complete.

```

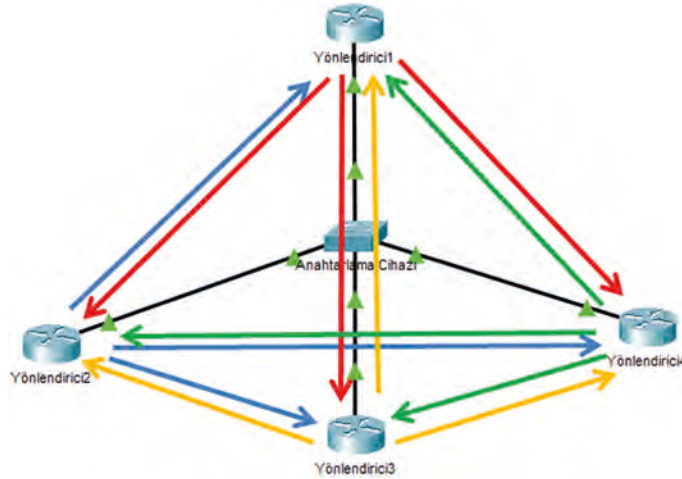
Görsel 5.53: PC1'den PC0'a giden rota tablosu

10. Adım: Simülasyon programında simülasyon durumuna gelerek ICMP paketlerini seçiniz ve PC'ler arasında ping iletişim testi gerçekleştirerek rotaları ICMP paketleri ile izleyiniz.

5.3.6. Yayın Ağlarında OSPF

OSPF protokolü ile çalışan yayın ağlarında yönlendirici ağ bilgilerinin LSA paketleriyle yönlendiriciler arasında taşınması, ağda büyük bir yük oluşumuna yol açar. OSPF ile yönlendiriciler ağın tüm haritasını çıkarmak zorunda olduğu için ağdaki OSPF protokolünü kullanan diğer tüm yönlendiricilerin bilgisine ihtiyaç duyar. Yayın ağlarında her yönlendirici sürekli olarak kendi bilgilerini diğer tüm yönlendiricilerle paylaştığında LSA taşıma deneni sorun meydana gelir. Bu sorun, merkezî bir yönlendirici belirlenip, ağdaki yönlendiricilerin bilgilerinin toplanarak diğer yönlendiricilere gönderilmesi yöntemiyle çözülür.

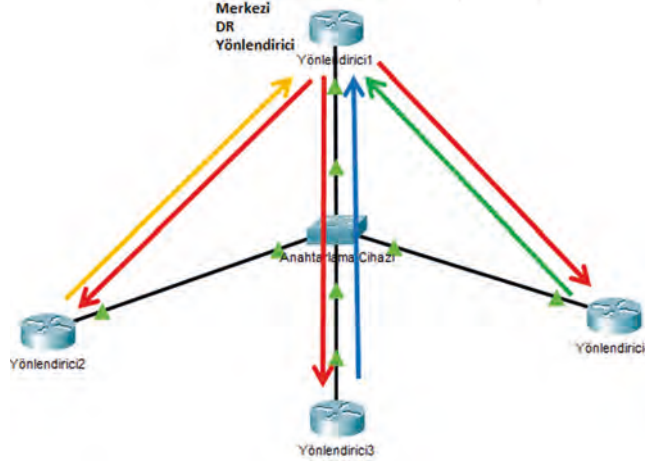
Görsel 5.54'te yönlendiricilerin her biri ağ bildirimini diğer yönlendiricilerle yaparak LSA taşıma sebepleri olur. LSA taşıma oluşan bir ağda toplam yönlendirici sayısı n ile $n-1$ 'in çarpımı kadar LSA paketi gönderilmesine yol açar. Bu durum özellikle yönlendirici sayısı fazla olan sistemlerde ağ trafiği yükünü artırır.



Görsel 5.54: LSA taşıma oluşmuş yayın ağı

Görsel 5.55'te ise merkez bir yönlendirici belirlenmiştir. Diğer yönlendiriciler ağ bilgilerini merkez yönlendiriciye, merkez yönlendirici ise LSA paketlerini diğer yönlendiricilerle paylaşarak tüm yönlendirici-

lerin doğru OSPF topoloji haritalarını çıkarması sağlanır. Böylelikle ağ trafiğinin yükü hafifler ve LSA taşıma da önlenir. OSPF protokolü kullanan yayın ağlarında LSA paketlerinin diğer yönlendiricilere gönderimini yapan yönlendirici merkez (DR), yedek merkez yönlendirici (BDR) ve diğer yönlendiriciler (DROther) şeklinde adlandırılır.



Görsel 5.55: Merkezî yönlendirici ile LSA dağılımı

5.3.6.1. OSPF Yayın Ağlarında Merkezî Yönlendirici Belirlenmesi

Ağdan sorumlu teknisyenler merkezî yönlendiriciyi belirlerken işlem gücü yüksek olan yönlendiriciden yararlanmalıdır. Merkezî yönlendiriciler bütün yönlendiricilerin ağ bilgilerini topladığı ve tüm ağın LSA paketlerini diğer yönlendiricilere aktardığı için işlemci gücüne daha fazla ihtiyaç duyar ancak OSPF, merkezî yönlendiriciyi işlemci gücüne göre belirlemez. Merkezî yönlendiriciyi OSPF yapılandırmaları belirler. OSPF algoritmaları merkezî yönlendiriciyi belirlerken önce ağdaki yönlendiricilerin ağa bağlandıkları arayüz OSPF öncelik değerine, öncelik değerleri eşitse Router ID numarasına bakar. Öncelik değeri büyük olan veya Router ID değeri büyük olan yönlendirici DR yönlendirici, ikinci en yüksek değere sahip yönlendirici BDR ve diğer yönlendiriciler DROther şeklinde adlandırılır.

5.3.6.2. OSPF Protokolüyle Router ID Belirlenmesi

OSPF protokolü ile çalışan yönlendiriciler en ideal yol hesaplamalarını yapabilmek için ağın tüm haritasına ulaşmak ister. OSPF protokolü ile çalışan yönlendiriciler ağın bütün haritasını çıkarabilmek için tüm yönlendiricilerin kimlik bilgilerine erişmelidir. Yönlendiricilerde OSPF kimliği "Router ID" numarası şeklinde tanımlanır. Yönlendirici Router ID numarası, ağ teknisyeni tarafından doğrudan verilerek veya loopback ve fiziksel arayüzlerinden değeri büyük olan IP adresi seçilerek elde edilir.

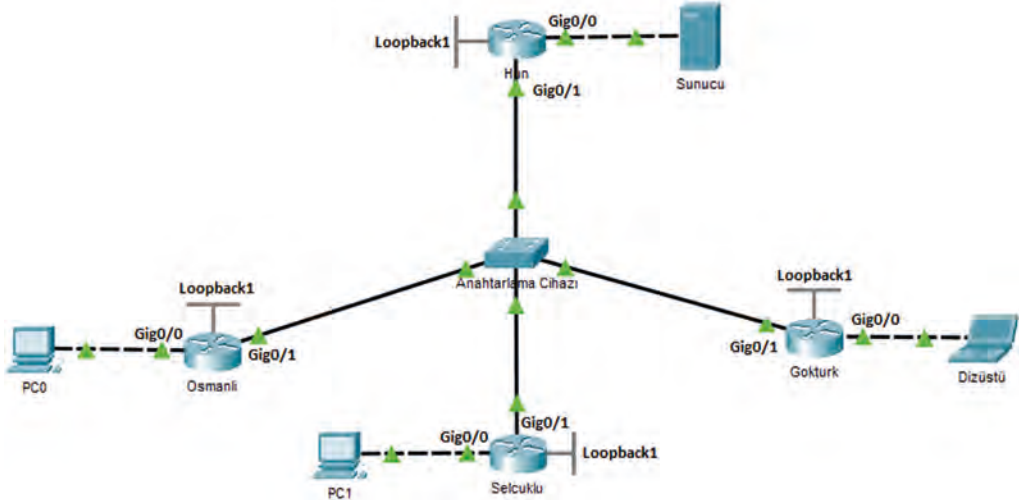
Router ID belirlenmesinde öncelik sıralaması şu şekildedir:

1. Komutla Router ID verilmesi
2. Router ID komutla verilmemişse loopback arayüzlerinden büyük olan IP değeri seçimi
3. Router ID komutla verilmemişse ve loopback arayüz adresi yoksa fiziksel arayüzlerden büyük olan IP değeri seçimi

9. UYGULAMA

OSPF Protokolüyle Router ID Belirlenmesi

Görsel 5.56'da verilen ağ topolojisini simülasyon programında oluşturunuz. İşlem adımlarına göre Tablo 5.9'da yer alan IP bilgilerini kullanıp, ilgili cihazları yapılandırarak OSPF protokolüyle Router ID belirleyiniz.



Görsel 5.56: Dokuzuncu uygulamanın yayın ağı topolojisi

Tablo 5.9: Dokuzuncu Uygulamanın IP Bilgileri

Cihaz	Arayüz	IP	Alt Ağ Maskesi	Varsayılan Ağ Geçidi	Router ID
Hun Yönlendiricisi	Gig0/0	192.168.1.1	255.255.255.192		1.1.1.1
	Gig0/1	172.24.7.1	255.255.0.0		
	Loopback 1	128.0.0.4	255.255.255.255		
Göktürk Yönlendiricisi	Gig0/0	192.168.1.65	255.255.255.192		4.4.4.4
	Gig0/1	172.24.7.2	255.255.0.0		
	Loopback 1	128.0.0.3	255.255.255.255		
Selçuklu Yönlendiricisi	Gig0/0	192.168.1.129	255.255.255.192		3.3.3.3
	Gig0/1	172.24.7.3	255.255.0.0		
	Loopback 1	128.0.0.2	255.255.255.255		
Osmanlı Yönlendiricisi	Gig0/0	192.168.1.193	255.255.255.192		2.2.2.2
	Gig0/1	172.24.7.4	255.255.0.0		
	Loopback 1	128.0.0.1	255.255.255.255		
PC0	FastEthernet	192.168.1.194	255.255.255.192	192.168.1.193	
PC1	FastEthernet	192.168.1.130	255.255.255.192	192.168.1.129	
Dizüstü	FastEthernet	192.168.1.66	255.255.255.192	192.168.1.65	
Sunucu	FastEthernet	192.168.1.2	255.255.255.192	192.168.1.1	

1. Adım: Yönlendirici ve bilgisayar cihazlarının fiziksel arayüzleri için IP yapılandırmasını yapınız. Yönlendiricilerde loopback1 arayüzlerin IP yapılandırması yedinci adımda, Router ID atamaları on üçüncü adımda yapılandırılacaktır.

Hun yönlendiricisi için arayüz IP yapılandırmaları:

```
Hun(config)#interface GigabitEthernet 0/0
Hun(config-if)#ip address 192.168.1.1 255.255.255.192
Hun(config-if)#no shutdown
Hun(config-if)#exit
```

```
Hun(config)#interface GigabitEthernet 0/1
Hun(config-if)#ip address 172.24.7.1 255.255.0.0
Hun(config-if)#no shutdown
Hun(config-if)#exit
```

2. Adım: Yönlendiricilerde OSPF yapılandırmalarının işlem numarasını 1, alan numarasını 0 olarak yapılandırınız.

```
Hun(config)#router ospf 1
Hun(config-router)#network 192.168.1.0 0.0.0.63 area 0
Hun(config-router)#network 172.24.0.0 0.0.255.255 area 0
```

```
Gokturk(config)#router ospf 1
Gokturk(config-router)#network 192.168.1.64 0.0.0.63 area 0
Gokturk(config-router)#network 172.24.0.0 0.0.255.255 area 0
```

```
Selcuklu(config)#router ospf 1
Selcuklu(config-router)#network 192.168.1.128 0.0.0.63 area 0
Selcuklu(config-router)#network 172.24.0.0 0.0.255.255 area 0
```

```
Osmanli(config)#router ospf 1
Osmanli(config-router)#network 192.168.1.192 0.0.0.63 area 0
Osmanli(config-router)#network 172.24.0.0 0.0.255.255 area 0
```

3. Adım: Göktürk yönlendiricisinde “show ip protocols” komutu ile yönlendirici OSPF Router ID değerini görüntüleyiniz.

```
Gokturk#show ip protocols

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 192.168.1.65
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    192.168.1.64 0.0.0.63 area 0
    172.24.0.0 0.0.255.255 area 0
```

Görsel 5.57: Aktif dinamik yönlendirme protokolü bilgisi ve Router ID

Görsel 5.57’de görüldüğü gibi Göktürk yönlendiricisi OSPF dinamik yönlendirme protokolü ile çalışmaya başlamıştır. Yönlendirici Router ID değeri, yönlendiricinin iki fiziksel arayüzü IP adresinden büyük olan IP 192.168.1.65 seçilerek belirlenmiştir.



SIRA SİZDE

Hun, Selçuklu ve Osmanlı yönlendiricilerinde “show ip protocols” komutu ile OSPF Router ID değerlerini görüntüleyiniz.

4. Adım: Göktürk yönlendiricisinde “clear ip ospf process” komutu ile OSPF sürecini yenileyiniz. Bu işlem sonucunda Router ID değeri güncellenecektir.

Gokturk#clear ip ospf process

Reset ALL OSPF processes? [no]: yes



SIRA SİZDE

Diğer yönlendiricilerde de bu işlemi uygulayınız.



BİLGİ

Yayın ağlarında ilk yapılandırılan yönlendirici, kendini diğer yönlendiricilere merkez yönlendirici olarak ilan eder. Topolojinin OSPF komşuluklarında merkezî yönlendiricinin doğru seçimi için yapılan-
dırılmış yönlendiricilerin birinde “clear ip ospf process” komutu kullanılmalıdır.

5. Adım: Göktürk yönlendiricisinde “show ip ospf neighbor” komutu ile OSPF komşuluklarını görüntüleyiniz (Görsel 5.58).

Gokturk#show ip ospf neighbor

Gokturk#show ip ospf neighbor

Neighbor ID	Pri	State	Dead Time	Address	Interface
192.168.1.1	1	2WAY/DROTHER	00:00:33	172.24.7.1	GigabitEthernet0/1
192.168.1.129	1	FULL/BDR	00:00:36	172.24.7.3	GigabitEthernet0/1
192.168.1.193	1	FULL/DR	00:00:30	172.24.7.4	GigabitEthernet0/1

Görsel 5.58: Dokuzuncu uygulamanın OSPF komşuluk tablosu-1

Görsel 5.58’de Göktürk yönlendiricisine ait OSPF komşuluk tablosu verilmiştir. Neighbor ID sütununda komşu yönlendiricilerin Router ID değerleri sıralanmıştır. 192.168.1.193 Router ID numarasının durum (State) sütununa bakıldığında DR olduğu görülür. Bu, Osmanlı yönlendiricisinin topolojide merkez yönlendirici olduğu bilgisini verir. 192.168.1.129 Router ID numarasına sahip Selçuklu yönlendiricisinin ise BDR yedek merkez yönlendirici olduğu, diğer 192.168.1.1 Router ID’sine sahip Hun yönlendiricisinin ise DROTHER şeklinde tanımlandığı görülür. Topolojide yalnızca bir DR ve BDR olacağı için komutun uygulandığı Göktürk yönlendiricisi de DROTHER yönlendiricidir.



BİLGİ

Komşuluk tablosunda LSA paketleri gönderimi yapabilen yönlendiricilerin durumu FULL olarak tanımlanır. Yayın ağlarında LSA paket dağılım görevi DR ve BDR yönlendiricilerde olduğu için bu yönlendiriciler FULL olarak tanımlanmıştır. DROther yönlendiriciler LSA dağıtımını yapmaz. Sadece OSPF komşuluğunun kurulduğu, LSA dağıtımını yapmayan yönlendiricilerin durumu OSPF komşuluk tablosunda 2WAY şeklinde tanımlanır.



SIRA SİZDE

Hun, Selçuklu ve Osmanlı yönlendiricilerinde “show ip ospf neighbor” komutu ile OSPF komşuluklarını görüntüleyiniz.

6. Adım: Göktürk yönlendiricisi OSPF yönlendirme tablosunu görmek için “show ip route ospf” komutunu uygulayınız (Görsel 5.59).

```
Gokturk#show ip route ospf
192.168.1.0/24 is variably subnetted, 5 subnets, 2 masks
O       192.168.1.0 [110/2] via 172.24.7.1, 00:10:57, GigabitEthernet0/1
O       192.168.1.128 [110/2] via 172.24.7.3, 00:10:57, GigabitEthernet0/1
O       192.168.1.192 [110/2] via 172.24.7.4, 00:10:57, GigabitEthernet0/1
```

Görsel 5.59: Dokuzuncu uygulamanın Göktürk yönlendiricisi yönlendirme tablosu

Görsel 5.59’da görüldüğü gibi OSPF süreçleri tamamlanmıştır. Göktürk yönlendiricisi, diğer yönlendiricilerin iç ağlarını bilir. OSPF, varsayılan olarak otomatik özetleme yapmamıştır.

7. Adım: Tablo 5.9’da verilen IP bilgileri ile yönlendiricilerde loopback1 arayüzlerini yapılandırınız.

```
Hun(config)#interface loopback 1
Hun(config-if)#ip address 128.0.0.4 255.255.255.255
```

```
Gokturk(config)#interface loopback 1
Gokturk(config-if)#ip address 128.0.0.3 255.255.255.255
```

```
Selcuklu(config)#interface loopback 1
Selcuklu(config-if)#ip address 128.0.0.2 255.255.255.255
```

```
Osmanli(config)#interface loopback 1
Osmanli(config-if)#ip address 128.0.0.1 255.255.255.255
```

8. Adım: Tüm yönlendirici cihazlarda çalışan yapılandırmanızı onaylayarak başlangıç yapılandırmanızı “copy run start” komutu ile kaydediniz ve yönlendirici cihazlarınızı “reload” komutu ile yeniden başlatınız.

Selcuklu#copy run start

Selcuklu#reload

9. Adım: Cihazlar tekrar açıldığında yönlendiricilerde “show ip protocols” komutunu uygulayınız. Görsel 5.60’ta olduğu gibi Selçuklu yönlendiricisinde Router ID değeri, loopback1 IP adres değeri 128.0.0.2 ile değişmiştir. Loopback arayüz adres değeri, fiziksel arayüz adres değerine göre Router ID belirlemede önceliklidir. Diğer yönlendiricilerde de bu değişikliği gözlemleyiniz.

Selcuklu#show ip protocols

```
Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 128.0.0.2
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    192.168.1.128 0.0.0.63 area 0
    172.24.0.0 0.0.255.255 area 0
```

Görsel 5.60: Çalışan dinamik protokolü bilgisi ve loopback adresi ile Router ID

10. Adım: Selçuklu yönlendiricisinde değişen Router ID değerlerine göre “show ip ospf neighbor” komutu ile yeni OSPF komşuluk tablosunu görüntüleyiniz (Görsel 5.61).

Selcuklu#show ip ospf neighbor

Neighbor ID	Pri	State	Dead Time	Address	Interface
128.0.0.3	1	FULL/BDR	00:00:31	172.24.7.2	GigabitEthernet0/1
128.0.0.4	1	FULL/DR	00:00:32	172.24.7.1	GigabitEthernet0/1
128.0.0.1	1	2WAY/DROTHER	00:00:30	172.24.7.4	GigabitEthernet0/1

Görsel 5.61: Dokuzuncu uygulamanın OSPF komşuluk tablosu-2

Görsel 5.61’de değişen komşuluk tablosu loopback adreslerine göre yeni Router ID değeri en yüksek olan Hun yönlendiricisi (128.0.0.4) DR, en yüksek ikinci değere sahip Göktürk yönlendiricisi (128.0.0.3) BDR, Osmanlı yönlendiricisi (128.0.0.1) DROTHER şeklinde tanımlanmıştır. Selçuklu yönlendiricisi ise (128.0.0.2) DROTHER yönlendiricidir.



SIRA SİZDE

Hun, Göktürk ve Osmanlı yönlendiricilerinde OSPF komşuluk tablolarını görüntüleyiniz.

11. Adım: Yönlendiricilerde loopback1 arayüz adreslerinin OSPF yapılandırmasında ağ bildirimini yapınız.

Hun(config)#router ospf 1

Hun(config-router)#network 128.0.0.4 0.0.0.0 area 0

Gokturk(config)#router ospf 1

Gokturk(config-router)#network 128.0.0.3 0.0.0.0 area 0

```
Selcuklu(config)#router ospf 1
```

```
Selcuklu(config-router)#network 128.0.0.2 0.0.0.0 area 0
```

```
Osmanli(config)#router ospf 1
```

```
Osmanli(config-router)#network 128.0.0.1 0.0.0.0 area 0
```

12. Adım: Selçuklu yönlendiricisinde OSPF yönlendirme tablosunu “show ip route ospf” komutu ile görüntüleyiniz (Görsel 5.62).

```
Selcuklu#sh ip route ospf
128.0.0.0/32 is subnetted, 4 subnets
O    128.0.0.1 [110/2] via 172.24.7.4, 00:00:12, GigabitEthernet0/1
O    128.0.0.3 [110/2] via 172.24.7.2, 00:00:47, GigabitEthernet0/1
O    128.0.0.4 [110/2] via 172.24.7.1, 00:08:02, GigabitEthernet0/1
192.168.1.0/24 is variably subnetted, 5 subnets, 2 masks
O    192.168.1.0 [110/2] via 172.24.7.1, 00:22:58, GigabitEthernet0/1
O    192.168.1.64 [110/2] via 172.24.7.2, 00:00:47, GigabitEthernet0/1
O    192.168.1.192 [110/2] via 172.24.7.4, 00:22:48, GigabitEthernet0/1
```

Görsel 5.62: Dokuzuncu uygulamanın Selçuklu yönlendiricisi yönlendirme tablosu

13. Adım: Tablo 5.9’da verilen yönlendiricilerde Router ID değerlerinin girişini yapınız.

```
Gokturk(config)#router ospf 1
```

```
Gokturk(config-router)#router-id 4.4.4.4
```

```
Selcuklu(config)#router ospf 1
```

```
Selcuklu(config-router)#router-id 3.3.3.3
```

```
Osmanli(config)#router ospf 1
```

```
Osmanli(config-router)#router-id 2.2.2.2
```

```
Hun(config)#router ospf 1
```

```
Hun(config-router)#router-id 1.1.1.1
```

14. Adım: Tüm yönlendiricilerde “clear ip ospf process” komutu ile OSPF sürecini yenileyiniz. Bu işlem sonucunda Router ID değerleri güncellenecektir.

15. Adım: Yönlendiricilerde değişen Router ID değerini görmek için “show ip protocols” komutunu uygulayınız.

Hun yönlendiricisi için OSPF protokol bilgisi:

```
Hun#show ip protocols

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 1.1.1.1
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    192.168.1.0 0.0.0.63 area 0
    172.24.0.0 0.0.255.255 area 0
    128.0.0.4 0.0.0.0 area 0
```

Görsel 5.63: Router ID değerinin el ile değiştirilmesi

Görsel 5.63'te görüldüğü gibi komutla Router ID değeri girilmiş, OSPF yapılandırmalarında Router ID değeri arayüzlere bakılmaksızın değişmiştir.

16. Adım: Hun yönlendiricisinde değişen Router ID değerlerine göre “show ip ospf neighbor” komutu ile yeni OSPF komşuluk tablosunu görüntüleyiniz (Görsel 5.64).

```
Hun#show ip ospf neighbor
```

Neighbor ID	Pri	State	Dead Time	Address	Interface
2.2.2.2	1	3WAY/DROTHER	00:00:35	172.24.7.4	GigabitEthernet0/1
4.4.4.4	1	FULL/DR	00:00:37	172.24.7.2	GigabitEthernet0/1
3.3.3.3	1	FULL/BDR	00:00:33	172.24.7.3	GigabitEthernet0/1

Görsel 5.64: Dokuzuncu uygulamanın OSPF komşuluk tablosu-3

Görsel 5.64'te değişen komşuluk tablosuna göre yeni Router ID değeri en yüksek olan Göktürk yönlendiricisi (4.4.4.4) DR, en yüksek ikinci değere sahip Selçuklu yönlendiricisi (3.3.3.3) BDR, Osmanlı yönlendiricisi (2.2.2.2) DROTHER şeklinde tanımlanmıştır. Hun yönlendiricisi ise (1.1.1.1) DROTHER yönlendiricidir.



BİLGİ

Router ID değeri komutla girilmiş yönlendiriciler, DR olmakta diğer yönlendiricilere göre ayrıcalıklıdır.



SIRA SİDE

Selçuklu, Göktürk ve Osmanlı yönlendiricilerinde OSPF komşuluk tablolarını görüntüleyiniz.

17. Adım: Yayın ağlarında merkez yönlendiriciyi belirlemek için ağa bağlı arayüzün OSPF öncelik değeri (priority) Router ID değerine göre daha önceliklidir. Selçuklu yönlendiricisinin yayın ağına bağlandığı GigabitEthernet 0/1 arayüzünün öncelik değerini 10 olarak değiştiriniz. Ardından OSPF sürecini yenilemek için “clear ip ospf process” komutunu kullanınız.

```
Selcuklu(config)#interface GigabitEthernet 0/1
```

```
Selcuklu(config-if)#ip ospf priority 10
```

```
Selcuklu#clear ip ospf process
```



BİLGİ

Arayüzlerde OSPF öncelik değeri varsayılan olarak 1'dir.

18. Adım: Hun yönlendiricisinde değişen öncelik değerlerine göre “show ip ospf neighbor” komutu ile yeni OSPF komşuluk tablosunu görüntüleyiniz (Görsel 5.65).

```
Hun#show ip ospf neighbor
```

Neighbor ID	Pri	State	Dead Time	Address	Interface
2.2.2.2	1	2WAY/DROTHER	00:00:37	172.24.7.4	GigabitEthernet0/1
3.3.3.3	10	FULL/DR	00:00:39	172.24.7.3	GigabitEthernet0/1
4.4.4.4	1	FULL/BDR	00:00:30	172.24.7.2	GigabitEthernet0/1

Görsel 5.65: Dokuzuncu uygulamanın OSPF komşuluk tablosu-4

Görsel 5.65’te arayüz öncelik değeri 10 olarak belirlenen Selçuklu yönlendiricisi, DR olarak değişmiştir. Öncelik değerleri eşit yönlendiricilerden Router ID değeri en yüksek (4.4.4.4) Göktürk yönlendiricisi BDR olarak tanımlanmıştır.

19. Adım: Bilgisayarlar arasında ping iletişim testi yaparak sistemin çalışmasını kontrol ediniz.

5.3.7. OSPF ile Kimlik Doğrulama

Ağ teknisyenlerinin ve mühendislerinin bilgisi dışında ağa eklenebilecek yeni bir yönlendirici, ağda çalışan yönlendiriciler üzerinde yanıltıcı rota bildirimlerine sebep olabilir. Bu durum, ağın güvenliğini ve performansını zayıflatır. Özellikle yayın ağlarında ağı yanıltmak için yerleştirilen yönlendiricilerle ağa zarar verilebilir. Yabancı yönlendiricilerin ağa katılımını engellemek için OSPF protokolü ile çalışan yönlendiricilerde kimlik doğrulaması yapılır. Yapılandırılmış yönlendiriciler bu uygulama sayesinde yalnızca ağ yöneticisi tarafından belirlenmiş anahtar kelime ile OSPF ağına katılır.

OSPF ile kimlik doğrulama iki aşamada yapılır.

```
Yönlendirici(config)#router ospf 1
```

```
Yönlendirici(config-router)#area 0 authentication message-digest
```

```
Yönlendirici(config)#interface serial0/0/0
```

```
Yönlendirici(config-if)# ip ospf message-digest-key 1 md5 "parola"
```

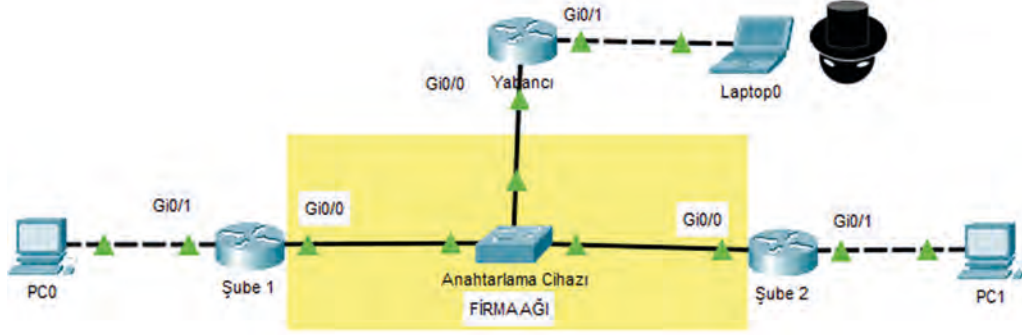
Aynı OSPF alanında çalışan yönlendiriciler için kimlik bildirimi kontrolü sağlanacağı “area 0 authentication message-digest” komutu ile yönlendiriciye bildirilir. Yönlendirici arayüzlerinde ise şifreleme türü “md5” ve komşu yönlendirici arayüzüne bildirilecek “parola” yazılmalıdır.



10. UYGULAMA

OSPF ile Kimlik Doğrulama

Görsel 5.66’da verilen Firma ağ topolojisinde ağa yabancı bir kişi tarafından yönlendirici kullanılarak şube ağlarına izinsiz giriş yapılmak istenir. Hacker, Firma ortak ağındaki anahtar cihazında bir güvenlik boşluğundan yararlanarak kendi yönlendiricisini Firma ağına bağlamıştır. İşlem adımlarına göre Tablo 5.10’da yer alan IP bilgilerini kullanıp, ilgili cihazları yapılandırarak Yabancı yönlendiriciyi engellemek için OSPF ile kimlik doğrulaması yapınız.



Görsel 5.66: Onuncu uygulamanın ağ topolojisi

Tablo 5.10: Onuncu Uygulamanın IP Bilgileri

Cihaz	Arayüz	IP	Alt Ağ Maskesi	Varsayılan Ağ Geçidi
Şube 1 Yönlendiricisi	Gig0/0	90.0.0.10	255.0.0.0	
	Gig0/1	192.168.0.1	255.255.255.0	
Şube 2 Yönlendiricisi	Gig0/0	90.0.0.11	255.0.0.0	
	Gig0/1	192.168.1.1	255.255.255.0	
Yabancı	Gig0/0	90.0.0.12	255.0.0.0	
	Gig0/1	192.168.30.1	255.255.255.0	
PC0	FastEthernet	192.168.0.2	255.255.255.0	192.168.0.1
PC1	FastEthernet	192.168.1.2	255.255.255.0	192.168.1.1

1. Adım: Şube 1, Şube 2 ve Yabancı yönlendiricisini Tablo 5.10’da verilen IP’lerle yapılandırınız.

2. Adım: Şube 1, Şube 2 yönlendiricilerinde OSPF yapılandırmalarını yapınız.

```
Sube1(config)#router ospf 1
```

```
Sube1(config-router)#network 90.0.0.0 0.255.255.255 area 0
```

```
Sube1(config-router)#network 192.168.0.0 0.0.0.255 area 0
```

```
Sube2(config)#router ospf 1
```

```
Sube2(config-router)#network 90.0.0.0 0.255.255.255 area 0
```

```
Sube2(config-router)#network 192.168.1.0 0.0.0.255 area 0
```

3. Adım: Şube 1 ve Şube 2 yönlendiricilerinde md5 şifreleme tekniği ve “T29101923C” anahtar parolası ile kimlik doğrulaması yapınız.

```
Sube1(config)#router ospf 1
```

```
Sube1(config-router)#area 0 authentication message-digest
```

```
Sube1(config-router)#exit
```

```
Sube1(config)#interface GigabitEthernet 0/0
```

```
Sube1(config-if)#ip ospf message-digest-key 1 md5 T29101923C
```

```

Sube2(config)#router ospf 1
Sube2(config-router)#area 0 authentication message-digest
Sube2(config-router)#exit
Sube2(config)#interface GigabitEthernet 0/0
Sube2(config-if)#ip ospf message-digest-key 1 md5 T29101923C

```

4. Adım: Şube 1 yönlendiricisinde yönlendirme tablosunu “show ip route ospf” komutu ile görüntüleyiniz (Görsel 5.67).

```

Sube1#show ip route ospf
O    192.168.1.0 [110/2] via 90.0.0.11, 00:00:26, GigabitEthernet0/0

```

Görsel 5.67: Onuncu uygulamanın yönlendirme tablosu-1

Görsel 5.67’de Şube 1 yönlendiricisi, Şube 2 yerel ağını (192.168.1.0) öğrenmiştir.

5. Adım: Yabancı yönlendiricisinde OSPF ağ yapılandırmalarını yapınız.

```

Yabanci(config)#router ospf 1
Yabanci(config-router)#network 90.0.0.0 0.255.255.255 area 0
Yabanci(config-router)#network 192.168.30.0 0.0.0.255 area 0

```

6. Adım: Şube 1 ve Şube 2 yönlendiricileri arasında OSPF kimlik doğrulaması sağlandığı için Yabancı yönlendiricisinde OSPF ağ yapılandırmaları yapılmış olsa bile OSPF komşulukları kurulamamıştır ve Yabancı yönlendirici, şube ağlarını öğrenememiştir. Yabancı yönlendiricisinde “show ip ospf neighbor” ve “show ip route ospf” komutlarını uygulayınız.

7. Adım: Yabancı yönlendiricisinde deneme yanılma yöntemini kullanarak yanlış parola ile OSPF kimlik doğrulaması yapınız.

```

Yabanci(config)#router ospf 1
Yabanci(config-router)#area 0 authentication message-digest
Yabanci(config-router)#exit
Yabanci(config)#interface GigabitEthernet 0/0
Yabanci(config-if)#ip ospf message-digest-key 1 md5 P123456

```

Yabancı yönlendiricisi bir anahtar parolası kullansa da bu parola Şube 1 ve Şube 2 yönlendiricisinin anahtar parolaları ile eşleşmediği için OSPF komşulukları kurulamayacaktır.

8. Adım: Şube 1 ve Şube 2 yönlendiricilerinin iç ağlarına OSPF bildirimi yapmayı durdurunuz.

```

Sube1(config)#router ospf 1
Sube1(config-router)#passive-interface GigabitEthernet 0/1
Sube2(config)#router ospf 1
Sube2(config-router)#passive-interface GigabitEthernet 0/1

```

9. Adım: Laptop0’dan PC0 ve PC1’e, PC0’dan PC1’e, PC1’den PC0’a ping iletişim testi gerçekleştiriniz.

5.3.8. Farklı OSPF Alanları ve Varsayılan Rota Dağıtımı

OSPF alanı genişledikçe farklı yönlendiriciler ve bağlantılar topolojiye girer. Bu nedenle ağ haritası karmaşıklaşır ve bazı sorunlar meydana gelebilir. Topoloji farklı OSPF alanlarına bölünerek bu sorunların üstesinden gelinebilir. Topolojide farklı OSPF alanlarının kullanılma nedenleri şunlardır:

- Ağlar farklı yönlendiriciler ile genişledikçe daha büyük ve karmaşık yönlendirme tabloları oluşur. OSPF sisteminin alanlara bölünmesi, her alanda daha küçük yönlendirme tabloları ile çalışmasını sağlar.
- Yayın ağlarında LSA dağılımının bölünmüş OSPF alanlarında yapılması, ağ performansını artırır.
- Yönlendiricilerde daha küçük OSPF veri tabanı (LSDB) oluşmasını sağlar.
- OSPF ile çalışan yönlendiriciler ağ haritasını çıkarmak için SPF algoritmasını kullanır. Topoloji farklı OSPF alanlarına bölündüğünde ağlardaki yönlendirici sayısı azalacağı için yönlendirici işlemcilerine daha az yük düşer.

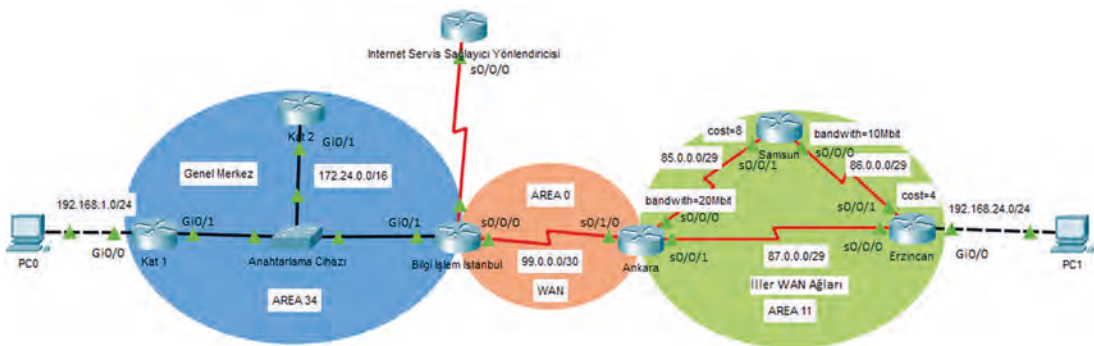
OSPF alanları yapılandırma içinde “area” şeklinde tanımlanır. Varsayılan olarak 0 alanı kullanılır. Sistemde farklı alanlar varsa area 0 OSPF alanları genellikle omurga şeklinde yapılandırılır. OSPF 0 alanı, farklı alanlar arasında geçiş görevi görür. Area 0 içinde bulunan yönlendiriciler bu nedenle omurga (backbone) yönlendiriciler şeklinde adlandırılır. Diğer OSPF alanlarındaki yönlendiriciler iç (internal) yönlendirici şeklinde adlandırılır. Birden fazla OSPF alanında çalışan yönlendiriciler ABR, diğer sistemlere çıkış yapılmasını sağlayan yönlendiriciler ise ASBR şeklinde tanımlanır.



11. UYGULAMA

Farklı OSPF Alanları ve Varsayılan Rota Dağıtımı

Görsel 5.68’de verilen ağ topolojisini simülasyon programında oluşturunuz. İşlem adımlarına göre Tablo 5.11’de yer alan IP bilgilerini kullanıp, ilgili cihazları yapılandırarak farklı OSPF alanlarını ve varsayılan rota dağıtımını yapınız.



Görsel 5.68: On birinci uygulamanın ağ topolojisi

Tablo 5.11: On Birinci Uygulamanın IP Bilgileri

Cihaz	Router ID	Arayüz	DCE	IP	Alt Ağ Maskesi	Varsayılan Ağ Geçidi
Kat 1 Yönlendiricisi	11.0.0.1	Gig0/0		192.168.1.1	255.255.255.0	
		Gig0/1		172.24.0.11	255.255.0.0	
Kat 2 Yönlendiricisi	22.0.0.1	Gig0/0				
		Gig0/1		172.24.0.12	255.255.0.0	
Bilgi İşlem Yönlendiricisi	10.0.0.1	Gig0/0				
		Gig0/1		172.24.0.10	255.255.0.0	
		Se0/0/0	Cl. rate 128000	99.0.0.1	255.255.255.252	
		Se0/0/1		93.0.0.2	255.255.255.252	
Ankara Yönlendiricisi		Se0/0/0	Cl. rate 128000	85.0.0.1	255.255.255.248	
		Se0/0/1		86.0.0.1	255.255.255.248	
		Se0/1/0		99.0.0.2	255.255.255.252	
Samsun Yönlendiricisi		Se0/0/0	Cl. rate 128000	86.0.0.3	255.255.255.248	
		Se0/0/1		85.0.0.3	255.255.255.248	
Erzincan Yönlendiricisi		Se0/0/0	Cl. rate 128000	87.0.0.2	255.255.255.248	
		Se0/0/1		86.0.0.2	255.255.255.248	
		Gig0/0		192.168.24.1	255.255.255.0	
ISP Yönlendiricisi		Se0/0/0	Cl. rate 128000	93.0.0.1	255.255.255.252	
PC0		FastEth.		192.168.1.2	255.255.255.0	192.168.1.1
PC1		FastEth.		192.168.24.2	255.255.255.0	192.168.24.1

1. Adım: Yönlendirici ve bilgisayarlarda IP yapılandırılmalarını Tablo 5.11'deki değerlerle yapınız. Yapılandırma ile ilgili arayüzler Görsel 5.68'de verilmiştir.

2. Adım: Genel Merkez ağındaki yönlendiricilerin Router ID değerlerini giriniz.

Kat1(config)#router ospf 1

Kat1(config-router)#router-id 11.0.0.1

Kat2(config)#router ospf 1

Kat2(config-router)#router-id 20.0.0.1

BilgiIslem(config)#router ospf 1

BilgiIslem(config-router)#router-id 10.0.0.1

3. Adım: Genel Merkez ağı yönlendiricilerinde alan numarası 34 olacak şekilde OSPF yönlendirme yapılandırmalarını yapınız.

```
Kat1(config)#router ospf 1
```

```
Kat1(config-router)#network 192.168.1.0 0.0.0.255 area 34
```

```
Kat1(config-router)#network 172.24.0.0 0.0.255.255 area 34
```

```
Kat2(config)#router ospf 1
```

```
Kat2(config-router)#network 172.24.0.0 0.0.255.255 area 34
```

```
BilgiIslem(config)#router ospf 1
```

```
BilgiIslem(config-router)#network 172.24.0.0 0.0.255.255 area 34
```

4. Adım: Bilgi İşlem yönlendiricisinde “show ip ospf neighbor” komutu ile OSPF komşuluklarını görüntüleyiniz (Görsel 5.69).

```
BilgiIslem#show ip ospf neighbor
```

```
BilgiIslem#show ip ospf neighbor
```

Neighbor ID	Pri	State	Dead Time	Address	Interface
20.0.0.1	1	FULL/DR	00:00:30	172.24.0.12	GigabitEthernet0/1
11.0.0.1	1	FULL/BDR	00:00:36	172.24.0.11	GigabitEthernet0/1

Görsel 5.69: Bilgi İşlem yönlendiricisi Genel Merkez ağı OSPF komşuluk tablosu

Görsel 5.69’da Bilgi İşlem yönlendiricisi için doğru komşulukların kurulduğu ve Genel Merkez ağı için LSA paket dağıtımlarını yapacak merkezî yönlendiricinin (DR) Kat2 yönlendiricisi olduğu görülür.

5. Adım: Kat2 yönlendiricisinde OSPF yönlendirme tablosunu “show ip route ospf” komutu ile görüntüleyiniz.

```
Kat2#show ip route ospf
```

```
192.168.1.0 [110/2] via 172.24.0.11, 00:13:28, GigabitEthernet0/1
```

Komut neticesinde Kat2 yönlendiricisinde OSPF yönlendirmelerinin çalıştığı ve Kat1 yönlendiricisi iç yerel ağının (192.168.1.0) Kat2 yönlendiricisi tarafından öğrenildiği görülür.

6. Adım: Genel Merkez ağında güvenliği artırmak için yönlendiriciler arasında kimlik doğrulama uygulamasını yapınız. Kimlik parola şifrelemesi md5 ile yapılacak ve parola “MK19051919A” olacaktır.

Kat2 yönlendiricisi için OSPF kimlik doğrulama satırları:

```
Kat2(config)#router ospf 1
```

```
Kat2(config-router)#area 34 authentication message-digest
```

```
Kat2(config)#interface GigabitEthernet 0/1
```

```
Kat2(config-if)#ip ospf message-digest-key 1 md5 MK19051919A
```



SIRA SİZDE

Genel Merkez ağındaki diğer yönlendiricilerin kimlik doğrulama işlemlerini doğru OSPF alanı için ilgili arayüzlerde yapınız.

7. Adım: İller WAN ağları için OSPF yönlendirme yapılandırmalarını yapınız. İller OSPF alan numarası 11 olacaktır.

```
Erzincan(config)#router ospf 1
Erzincan(config-router)#network 192.168.24.0 0.0.0.255 area 11
Erzincan(config-router)#network 86.0.0.0 0.0.0.7 area 11
Erzincan(config-router)#network 87.0.0.0 0.0.0.7 area 11
```

```
Samsun(config)#router ospf 1
Samsun(config-router)#network 86.0.0.0 0.0.0.7 area 11
Samsun(config-router)#network 85.0.0.0 0.0.0.7 area 11
```

```
Ankara(config)#router ospf 1
Ankara(config-router)#network 85.0.0.0 0.0.0.7 area 11
Ankara(config-router)#network 87.0.0.0 0.0.0.7 area 11
```

8. Adım: Ankara yönlendiricisi Serial0/0/0 arayüzü bant genişliğini 20000 Kilobit, Samsun yönlendiricisi Serial0/0/0 arayüzü bant genişliğini 10000 Kilobit olacak şekilde ayarlayınız.

```
Ankara(config)#interface serial0/0/0
Ankara(config-if)#bandwidth 20000
```

```
Samsun(config)#interface serial0/0/0
Samsun(config-if)#bandwidth 10000
```

9. Adım: Erzincan yönlendiricisi Serial0/0/1 arayüzü maliyet değerini 4, Samsun yönlendiricisi Serial0/0/1 arayüzü maliyet değerini 8 yapınız.

```
Samsun(config)#interface serial0/0/1
Samsun(config-if)#ip ospf cost 8
```

```
Erzincan(config)#interface serial0/0/1
Erzincan(config-if)#ip ospf cost 4
```

10. Adım: Samsun yönlendiricisinde “show ip route ospf” komutu ile yönlendirme tablosunu görüntüleyiniz (Görsel 5.70).

```
Samsun#sh ip route ospf
O    87.0.0.0 [110/72] via 85.0.0.1, 00:02:17, Serial0/0/1
O    192.168.24.0 [110/11] via 86.0.0.2, 00:05:58, Serial0/0/0
```

Görsel 5.70: On birinci uygulamanın yönlendirme tablosu-2

11. Adım: Ankara ve Bilgi İşlem (İstanbul) yönlendiricilerinde OSPF yapılandırmalarını WAN omurga ağı için alan numarası 0 olarak yapılandırınız.

```
BilgiIslem(config-router)#network 99.0.0.0 0.0.0.3 area 0
Ankara(config-router)#network 99.0.0.0 0.0.0.3 area 0
```

Üçüncü adımda Bilgi İşlem (İstanbul) yönlendiricisi OSPF alanı 34 ve yedinci adımda Ankara yönlendiricisi için OSPF alanı 11 ağ tanımlamaları yapılmıştır. On birinci adımda ise bu yönlendiricilerin Area 0 için ağ bildirimleri yapılarak iki alanda OSPF tanımlamaları gerçekleştirilmiştir. Böylelikle yönlendiriciler her iki alandan gelen ağ güncellemelerini diğer alana aktararak omurga görevi görür.

12. Adım: Tüm sistemin internete çıkışı Bilgi İşlem (İstanbul) yönlendiricisi üzerinden yapılacaktır. Bilgi İşlem (İstanbul) yönlendiricisinde İnternet Servis Sağlayıcı yönlendiricisi için varsayılan rota bildiriminde bulununuz.

```
Bilgislem(config)#ip route 0.0.0.0 0.0.0.0 serial0/0/1
```

13. Adım: Bilgi İşlem yönlendiricisinin varsayılan rota bildirimini diğer tüm yönlendiricilere bildirmesi için Bilgi İşlem yönlendiricisinde gerekli yapılandırmayı yapınız.

```
Bilgislem(config-router)#default-information originate
```

14. Adım: Kat2 ve Samsun yönlendiricilerinde “show ip route ospf” komutu ile OSPF yönlendirme tablolarını görüntüleyiniz (Görsel 5.71 ve Görsel 5.72).

```
Kat2#show ip route ospf
```

```
Kat2#show ip route ospf
O IA 85.0.0.0 [110/70] via 172.24.0.10, 00:04:53, GigabitEthernet0/1
O IA 86.0.0.0 [110/80] via 172.24.0.10, 00:04:53, GigabitEthernet0/1
O IA 87.0.0.0 [110/129] via 172.24.0.10, 00:04:53, GigabitEthernet0/1
  99.0.0.0/30 is subnetted, 1 subnets
O IA 99.0.0.0 [110/65] via 172.24.0.10, 00:04:53, GigabitEthernet0/1
O 192.168.1.0 [110/2] via 172.24.0.11, 00:04:53, GigabitEthernet0/1
O IA 192.168.24.0 [110/81] via 172.24.0.10, 00:04:33, GigabitEthernet0/1
O*E2 0.0.0.0/0 [110/1] via 172.24.0.10, 00:03:12, GigabitEthernet0/1
```

Görsel 5.71: On birinci uygulamanın yönlendirme tablosu-3

```
Samsun#show ip route ospf
```

```
Samsun#show ip route ospf
O 87.0.0.0 [110/72] via 85.0.0.1, 00:06:51, Serial0/0/1
  99.0.0.0/30 is subnetted, 1 subnets
O IA 99.0.0.0 [110/72] via 85.0.0.1, 00:06:51, Serial0/0/1
O IA 172.24.0.0 [110/73] via 85.0.0.1, 00:06:51, Serial0/0/1
O IA 192.168.1.0 [110/74] via 85.0.0.1, 00:06:51, Serial0/0/1
O 192.168.24.0 [110/11] via 86.0.0.2, 00:06:41, Serial0/0/0
O*E2 0.0.0.0/0 [110/1] via 85.0.0.1, 00:05:00, Serial0/0/1
```

Görsel 5.72: On birinci uygulamanın yönlendirme tablosu-4

Görsel 5.71 ve Görsel 5.72’de sırası ile Kat2 ve Samsun yönlendiricilerinin yönlendirme tabloları görülür. Her iki yönlendiriciye de farklı alanlardan gelen ağların bilgisi ulaşmıştır.

Yönlendirme tablosunda “O IA”, farklı alanlardan gelen ağ satırlarını ifade eder. “O*E2” ise OSPF ile bildirilen varsayılan rota satırını gösterir.

Rotaların metrik toplam maliyet değerlerine dikkat ederek diğer yönlendiricilerde de yönlendirme tablolarını görüntüleyiniz.

15. Adım: Bilgi İşlem yönlendiricisinde PC0 ve PC1'in İnternet Servis Sağlayıcısı yönlendiricisine çıkabilmesi için statik NAT tanımlaması yapınız.

```
Bilgislem(config)#interface Serial0/0/1
Bilgislem(config-if)#ip nat outside
Bilgislem(config)#interface Serial0/0/0
Bilgislem(config-if)#ip nat inside
Bilgislem(config)#interface GigabitEthernet0/1
Bilgislem(config-if)#ip nat inside
Bilgislem(config)#ip nat inside source static 192.168.1.2 93.0.0.2
```

16. Adım: PC0 ile PC1 arasında ve PC0 ile PC1'den İnternet Servis Sağlayıcı yönlendiricisine ping iletişim testi gerçekleştiriniz.

17. Adım: PC0 ile PC1 arasında ve PC0 ile PC1'den İnternet Servis Sağlayıcı yönlendiricisine "tracert" komutu ile rota geçiş testi gerçekleştirerek sistemin çalıştığını kontrol ediniz.

5.4. EIGRP YÖNLENDİRME PROTOKOLÜ

EIGRP (Enhanced Interior Gateway Routing Protocol) "gelişmiş iç ağ geçidi protokolü" anlamına gelen, uzaklık vektörü tabanlı, aynı zamanda bağlantı durum protokolü ile de çalışabilen, gelişmiş iç ağ geçidi yönlendirme protokolü türüdür.

5.4.1. EIGRP Özellikleri

EIGRP'in özellikleri şu şekilde sıralanabilir:

- Yönlendiriciler uzaklık vektörü protokolünü kullanarak ağın diğer kısmı için gerekli bilgileri komşu yönlendiricilerden öğrenir.
- Uzaklık vektörü protokolü ile çalışırken bağlantı durum protokolünü de kullanabilen gelişmiş ve karma bir yapıya sahiptir.
- Dağıtılmış güncelleme algoritmasını (DUAL) kullanarak yedek rotaların bilgisini tercih edilen yollara alternatif olarak hazırda tutar.
- Yönlendirme rotalarının oluşturulması hızlıdır.
- TCP/IP modeline göre taşıma katmanında kendine özgü RTP protokolünü kullanır.
- EIGRP, RTP protokolü ile ilk zamanlar sadece markaya özgü cihazlar için iletişimi desteklerken son zamanlarda tüm marka yönlendiricilerde kullanılabilir duruma gelmiştir.
- Sınıflı ve sınıfsız ağ yapısını destekler. Yönlendirici işletim sistemlerindeki son geliştirmeler ile varsayılan olarak sınıfsız ağları kullanır.
- Bağlantı durum protokolü ile de çalışabildiği için yönlendirici arayüzlerinde rota belirlerken bant genişliği, iletim gecikmesi gibi parametreleri de kullanabilir.
- Yönetimsel uzaklık değeri 90'dır. EIGRP rotaları, yönlendiricide OSPF veya RIP rotaları varsa yönetimsel değeri daha düşük olduğu için öncelikli kullanılır.

- EIGRP protokolü ile çalışan ağlar 255 yönlendiriciye kadar genişleyebilir.
- Yönlendiriciler EIGRP ile ağ güncelleme paketlerini yalnızca komşuluk kurulumunda ve ağlarda değişiklik olduğunda gönderir.
- Komşuluk kontrolleri Hello paketleri ile yapılır. Hello paketi gönderim süresi 5 saniyedir. Komşuluğu koruma süresi ise (Hold Time) 15 saniyedir.
- EIGRP'in kullanıldığı yönlendiricilerin işlemci kaynak tüketimi OSPF'den az, RIP'ten fazladır.
- Eşit metrikli rotalarda sırası ile paket gönderimi yapılır (Load Balancing). İstenirse eşit olmayan metrikli rotalarda da sırası ile paket gönderimi yapılabilir.
- Yönlendiriciler arasında kimlik doğrulama yapılarak protokolün güvenliği artırılabilir.
- EIGRP'in çoklu yayın IP numarası 224.0.0.10'dur.

5.4.2. EIGRP Paket Türleri

EIGRP ile çalışan ağ sistemlerinde protokol dört paket türü ile yönlendirme sürecini devam ettirir.

- **Hello Paketleri:** Bu paketler komşu yönlendiricide EIGRP sürecinin aktif olup olmadığını kontrol eder. 5 saniyede bir periyodik olarak yönlendiriciler arasında paket gönderimi olur. Hello paketinin bekleme süresi 15 saniyedir. 15 saniye içinde Hello paketi göndermeyen yönlendirici komşuluktan düşer.
- **Update Paketleri:** Ağ güncelleme paketleridir. Yönlendiriciler topolojiye katıldığında veya yönlendiricilerin bulunduğu ağ adreslerinde değişim olduğunda güncelleme paketleri ile diğer komşu yönlendiricilere kendi ağları hakkında bilgi verir.
- **Query Paketleri:** Sorgu paketleridir. Yönlendiricide EIGRP rotalarında kayıp söz konusu olduğunda veya alternatif rotalar hakkında komşu yönlendiriciden bilgi talep edildiğinde kullanılan paketlerdir.
- **ACK:** EIGRP sürecinin en ideal yönlendirme tablosu oluşturularak tamamlandığına dair bilgi paketidir.

5.4.3. EIGRP Yapılandırması

Yönlendiricilerde EIGRP yapılandırması temel olarak otonom sistem numarası ve yönlendirici ağ adreslerinin bildirimi ile gerçekleştirilir.

Yönlendirici(config)#router eigrp 'otonom sistem numarası'
Yönlendirici(config-router)#network 'Arayüz Ağ Adresi' veya
Yönlendirici(config-router)#network 'Arayüz Ağ Adresi' 'Wildcard Adresi' şeklindedir.

Otomatik özetleme yapmayan yönlendirici işletim sistemi için wildcard adresi girilmeksizin ağ bildirimi yapılabilir. Bu durumda EIGRP protokolü, yönlendirici arayüzündeki alt ağ maskesine göre ağ tanımlar.

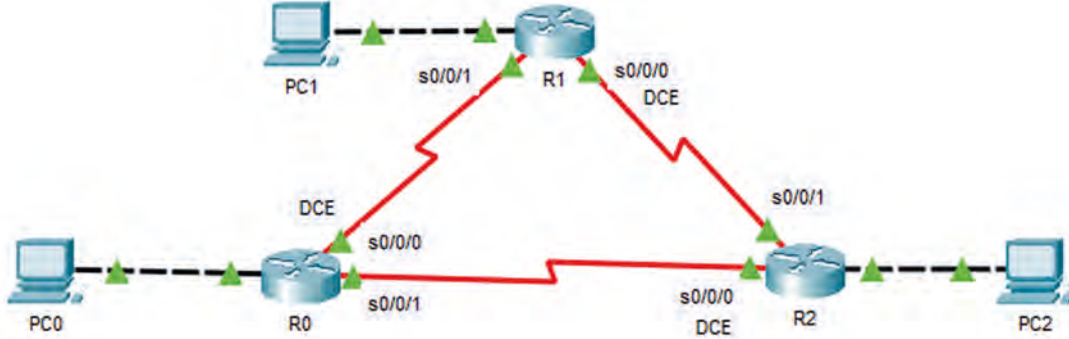
Otomatik özetleme yapan yönlendirici işletim sistemlerinde EIGRP ile ağ bildirimi yapılırken wildcard adresinin girilmesi ve "no auto-summary" komutu ile özetlemenin iptal edilmesi gerekir.



12. UYGULAMA

EIGRP Yapılandırması

Görsel 5.73'te verilen ağ topolojisini simülasyon programında oluşturunuz. İşlem adımlarına göre Tablo 5.12'de yer alan IP bilgilerini kullanarak ilgili cihazların EIGRP yapılandırmasını yapınız.



Görsel 5.73: On ikinci uygulamanın ağ topolojisi

Tablo 5.12: On İkinci Uygulamanın IP Bilgileri

Cihaz	Arayüz	DCE	IP	Alt Ağ Maskesi	Varsayılan Ağ Geçidi
R0 Yönlendiricisi	Gig0/0		172.24.10.1	255.255.255.0	
	Se0/0/0	Cl. rate 128000	95.0.0.10	255.0.0.0	
	Se0/0/1		97.0.0.10	255.0.0.0	
R1 Yönlendiricisi	Gig0/0		172.24.11.1	255.255.255.0	
	S0/0/0	Cl. rate 128000	96.0.0.11	255.0.0.0	
	Se0/0/1		95.0.0.11	255.0.0.0	
R2 Yönlendiricisi	Gig0/0		172.24.12.1	255.255.255.0	
	Se0/0/0	Cl. rate 128000	97.0.0.12	255.0.0.0	
	Se0/0/1		96.0.0.12	255.0.0.0	
PC0	FastEthernet		172.24.10.2	255.255.255.0	172.24.10.1
PC1	FastEthernet		172.24.11.2	255.255.255.0	172.24.11.1
PC2	FastEthernet		172.24.12.2	255.255.255.0	172.24.12.1

1. Adım: Yönlendirici ve bilgisayarlarda IP yapılandırmalarını Tablo 5.12'deki değerlerle yapınız. Yapılandırma ile ilgili arayüzler Görsel 5.73'te verilmiştir.

R0 yönlendiricisi için arayüz yapılandırması komut satırları:

```

R0(config)#interface Serial0/0/0
R0(config-if)#ip address 95.0.0.10 255.0.0.0
R0(config-if)#clock rate 128000
R0 (config-if)#no shutdown
R0 (config-if)#exit

```

```

R0(config)#interface Serial0/0/1
R0(config-if)#ip address 97.0.0.10 255.0.0.0
R0(config-if)#no shutdown
R0(config-if)#exit
R0(config)#interface GigabitEthernet 0/0
R0(config-if)#ip address 172.24.10.1 255.255.255.0
R0(config-if)#no shutdown

```

2. Adım: Yönlendiricilerde EIGRP dinamik yönlendirme yapılandırmasını yapınız. EIGRP otonom sistem numarasını 100 olarak yapılandırınız.

R0 yönlendiricisi için EIGRP yönlendirme yapılandırması komut satırları:

```

R0(config)#router eigrp 100
R0(config-router)#network 95.0.0.0 0.255.255.255
R0(config-router)#network 97.0.0.0 0.255.255.255
R0(config-router)#network 172.24.10 0 0.0.0.255

```



SIRA SİZDE

R1 ve R2 yönlendiricilerinde EIGRP dinamik yönlendirme yapılandırmalarını yapınız.

EIGRP yapılandırmaları yönlendiricilerde tamamlandıktan sonra EIGRP komşulukları kurulur. Başarı ile tamamlanmış EIGRP komşuluk bildirimi “new adjacency” tanımı ile komut ekranına otomatik olarak gelir (Görsel 5.74).

```

%DUAL-5-NBRCHANGE: IP-EIGRP 100: Neighbor 96.0.0.11 (Serial0/0/1) is up: new adjacency
%DUAL-5-NBRCHANGE: IP-EIGRP 100: Neighbor 97.0.0.10 (Serial0/0/0) is up: new adjacency

```

Görsel 5.74: EIGRP komşuluk bildirimi

3. Adım: Yönlendiricilerde EIGRP komşuluk tablosunu “show ip eigrp neighbor” komutu ile görüntüleyiniz (Görsel 5.75).

```

R2#show ip eigrp neighbors
IP-EIGRP neighbors for process 100
H   Address             Interface             Hold Uptime          SRTT    RTO    Q    Seq
                               (sec)                (ms)                Cnt    Num
0   96.0.0.11             Se0/0/1               10   00:07:59   40     1000    0    10
1   97.0.0.10             Se0/0/0               10   00:07:59   40     1000    0    10

```

Görsel 5.75: EIGRP komşuluk tablosu

Görsel 5.75'te R2 yönlendiricisi için EIGRP komşuluk tablosu verilmiştir. Address sütununda komşu yönlendiricilerin IP adres bilgisi, Interface sütununda komşu yönlendirici ile bağlantı kuran arayüz bilgisi, Hold sütununda son Hello paketinin gönderiminden sonra komşuluğun düşmesi için kalan süre, Uptime sütununda komşuluk kurulduktan sonra geçen süre belirtilmiştir.

4. Adım: Yönlendiricilerde EIGRP topolojilerini “show ip eigrp topology” komutu ile görüntüleyiniz (Görsel 5.76).

```
R0#sh ip eigrp topology
IP-EIGRP Topology Table for AS 100/ID(172.24.10.1)

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - Reply status

P 95.0.0.0/8, 1 successors, FD is 2169856
   via Connected, Serial0/0/0
P 96.0.0.0/8, 2 successors, FD is 2681856
   via 95.0.0.11 (2681856/2169856), Serial0/0/0
   via 97.0.0.12 (2681856/2169856), Serial0/0/1
P 97.0.0.0/8, 1 successors, FD is 2169856
   via Connected, Serial0/0/1
P 172.24.10.0/24, 1 successors, FD is 5120
   via Connected, GigabitEthernet0/0
P 172.24.11.0/24, 1 successors, FD is 2172416
   via 95.0.0.11 (2172416/5120), Serial0/0/0
P 172.24.12.0/24, 1 successors, FD is 2172416
   via 97.0.0.12 (2172416/5120), Serial0/0/1
```

Görsel 5.76: EIGRP topoloji tablosu

Görsel 5.76’da hedef ağlar için başarılı rota satırları R0 yönlendiricisi topoloji tablosunda görüntülenmiştir. Hedefe ulaşabilen rotalar için “successors” satırları tanımlanır. FD (Feasible Distance), rotaya ulaşmak için kullanılan toplam maliyet metrik değeridir. Son satırda 172.24.12.0/24 ağı için FD değeri 2172416’dır. 172.24.12.0/ ağına 97.0.0.12 adresli komşu yönlendiriciden erişim Serial0/0/1 arayüzü ile yapılabilir. Komşu yönlendiricinin hedef ağa erişim metrik değeri ise 5120’dir.

5. Adım: Yönlendiricilerde oluşan EIGRP yönlendirme tablolarını “show ip route eigrp” komutu ile görüntüleyiniz.

R0 yönlendiricisi için yönlendirme tablosu Görsel 5.77’de verilmiştir.

```
R0#show ip route eigrp
 95.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
D   96.0.0.0/8 [90/2681856] via 95.0.0.11, 00:44:31, Serial0/0/0
    [90/2681856] via 97.0.0.12, 00:44:18, Serial0/0/1
 172.24.0.0/16 is variably subnetted, 4 subnets, 2 masks
D   172.24.11.0/24 [90/2172416] via 95.0.0.11, 00:44:30, Serial0/0/0
D   172.24.12.0/24 [90/2172416] via 97.0.0.12, 00:44:17, Serial0/0/1
```

Görsel 5.77: R0 yönlendiricisinde EIGRP yönlendirme tablosu

R0 yönlendiricisi, EIGRP ile üç yeni hedef ağ rota bilgisi öğrenmiştir. Yönlendirme tablosunun son satırının açıklamaları şu şekildedir:

- **D:** EIGRP yönlendirme satırıdır.
- **172.24.12.0/24:** EIGRP ile öğrenilmiş hedef ağ adresidir.
- **[90/2172416]:** 90, EIGRP yönetimsel değeridir. 2172416 ise hedef ağ için toplam maliyet metrik değeridir.
- **Via 97.0.0.12:** “172.24.12.0” ağına gitmek için kullanılacak rotadaki komşu yönlendirici IP bilgisidir.
- **00:44:17:** EIGRP komşuluğu kurulduğu andan itibaren geçen süredir.

- **Serial0/0/1:** “172.24.12.0” ağına gitmek için yönlendiricide çıkış yapılan arayüzün adıdır.

Yönlendirme tablosu ilk satırında 96.0.0.0/8 hedef ağı için eşit metrik değerine sahip iki rota vardır. Bu rotalar sırası ile kullanılır.

6. Adım: R0 yönlendiricisinde “show ip protocols” komutu ile çalışan yönlendirme protokolünü inceleyiniz (Görsel 5.78).

```
R0#show ip protocols

Routing Protocol is "eigrp 100 "
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  Redistributing: eigrp 100
  EIGRP-IPv4 Protocol for AS(100)
    Metric weight K1=1, K2=0, K3=1, K4=0, K5=0
    NSF-aware route hold timer is 240
    Router-ID: 95.0.0.10
    Topology : 0 (base)
      Active Timer: 3 min
      Distance: internal 90 external 170
      Maximum path: 4
      Maximum hopcount 100
      Maximum metric variance 1

  Automatic Summarization: disabled
  Automatic address summarization:
  Maximum path: 4
  Routing for Networks:
    95.0.0.0
    97.0.0.0
    172.24.10.0/24
  Routing Information Sources:
    Gateway         Distance         Last Update
    95.0.0.11        90               6673
    97.0.0.12        90               9801
  Distance: internal 90 external 170
```

Görsel 5.78: R0 yönlendiricisinde EIGRP protokol bilgisi

Görsel 5.78’de yönlendirme protokolü otonom numarası değerinin 100 olduğu, yönetimsel değerinin 90 olduğu, otomatik özetlemenin ise kapalı olduğu bilgisi görülür. Ayrıca rota metriklerinin hesaplanmasında kullanılan parametrelerin bilgisi de verilmiştir.

EIGRP rotaları hesaplanırken kullanılan formül şu şekildedir:

EIGRP Toplam Metrik Değeri = $256 * [(K1 * \text{Bant Genişliği}) + (K2 * \text{Bant Genişliği}) / (256 - \text{Ağın Kullanım Oranı}) + (K3 * \text{Gecikme Süresi}) * (K5 / (\text{Güvenilirlik} + K4))]$

Formüldeki K değerlerinin anlamı şunlardır:

K1: Hedef ağı giden rotadaki en küçük bant genişliği

K2: Ağın kullanım oranı

K3: Gecikme süresi

K4: Güvenilirlik

K5: Ağdaki en büyük paket boyutu (MTU)

EIGRP rotaları hesaplanırken, varsayılan olarak K1=1, K2=0, K3=1, K4=0, K5=0 şeklindedir. K değerlerini değiştirmek için EIGRP yapılandırmasında “metric weight 0 1 0 1 0 0” komut satırından yararlanılır.

7. Adım: PC0’da “tracert 172.24.12.2” komutu ile PC1’e giden rotadaki yönlendirici bilgisini görüntüleyiniz (Görsel 5.79).

```
C:\>tracert 172.24.12.2

Tracing route to 172.24.12.2 over a maximum of 30 hops:

  1  0 ms    0 ms    0 ms    172.24.10.1
  2  2 ms    1 ms    1 ms    97.0.0.12
  3  1 ms    0 ms    2 ms    172.24.12.2
```

Görsel 5.79: Tracert komutu ile rota yönlendiricileri listesi

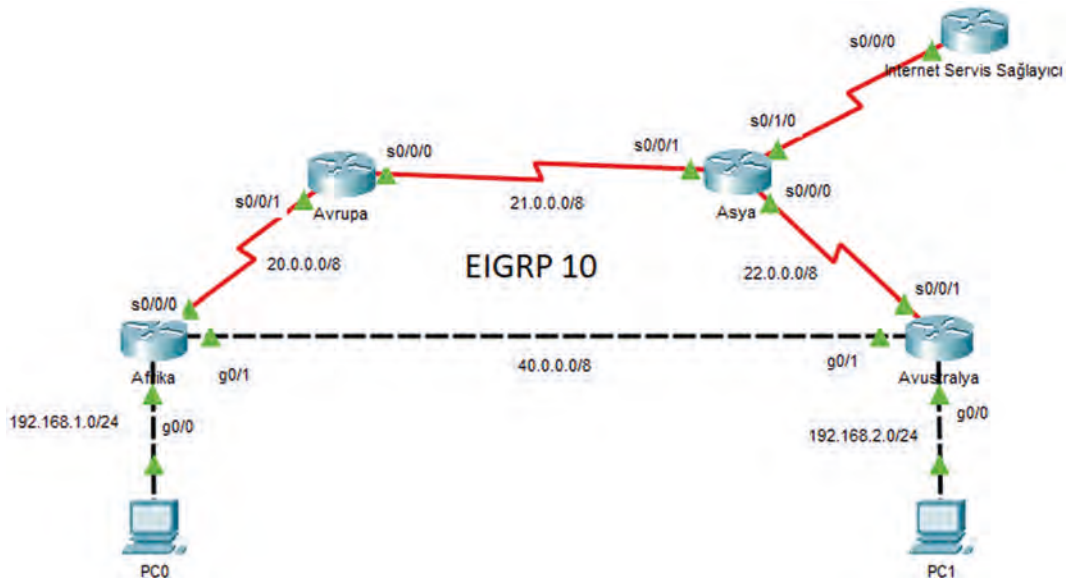
8. Adım: PC0’da “ping 172.24.12.2” komutu ile PC1 için iletişim testi gerçekleştiriniz.



13. UYGULAMA

EIGRP Yapılandırması

Görsel 5.80’de verilen ağ topolojisini simülasyon programında oluşturunuz. İşlem adımlarına göre Tablo 5.13’te yer alan IP bilgilerini kullanarak ilgili cihazların EIGRP yapılandırmasını yapınız.



Görsel 5.80: On üçüncü uygulamanın ağ topolojisi

Tablo 5.13: On Üçüncü Uygulamanın IP Bilgileri

Cihaz	Arayüz	DCE	IP	Alt Ağ Maskesi	Varsayılan Ağ Geçidi
Afrika Yönlendiricisi	Gig0/0		192.168.1.1	255.255.255.0	
	Gig0/1		40.0.0.1	255.0.0.0	
	Se0/0/0	Cl. rate 128000	20.0.0.1	255.0.0.0	
Avrupa Yönlendiricisi	Se0/0/0	Cl. rate 128000	21.0.0.1	255.0.0.0	
	Se0/0/1		20.0.0.2	255.0.0.0	
Asya Yönlendiricisi	Se0/0/0	Cl. rate 128000	22.0.0.1	255.0.0.0	
	Se0/0/1		21.0.0.2	255.0.0.0	
	Se0/1/0		85.0.0.2	255.0.0.0	
Avustralya Yönlendiricisi	Se0/0/1		22.0.0.2	255.0.0.0	
	Gig0/1		40.0.0.2	255.0.0.0	
	Gig0/0		192.168.2.1	255.255.255.0	
ISP	Se0/0/0	Cl. rate 128000	85.0.0.1	255.0.0.0	
PC0	FastEthernet		192.168.1.2	255.255.255.0	192.168.1.1
PC1	FastEthernet		192.168.2.2	255.255.255.0	192.168.2.1

1. Adım: Yönlendirici ve bilgisayarlarda IP yapılandırılmalarını Tablo 5.13'teki değerlerle yapınız. Yapılandırma ile ilgili arayüzler Görsel 5.80'de verilmiştir.

2. Adım: Yönlendiricilerde EIGRP dinamik yönlendirme yapılandırmasını yapınız. EIGRP otonom sistem numarasını 10 olarak yapılandırınız.

Afrika yönlendiricisi için EIGRP yönlendirme yapılandırması komut satırları:

```
Afrika(config)#router eigrp 10
Afrika(config-router)#network 20.0.0.0 0.255.255.255
Afrika(config-router)#network 40.0.0.0 0.255.255.255
Afrika(config-router)#network 192.68.1.0 0.0.0.255
```



SIRA SİZDE

Diğer yönlendiricilerde EIGRP dinamik yönlendirme yapılandırmalarını yapınız.

3. Adım: Asya yönlendiricisinden varsayılan rota ile İnternet Servis Sağlayıcı yönlendiricisine bağlantı yapınız ve varsayılan rotayı EIGRP yapılandırmasında diğer yönlendiricilere bildiriniz.

```
Asya(config)#ip route 0.0.0.0 0.0.0.0 Serial0/1/0
Asya(config)#router eigrp 10
Asya(config-router)#redistribute static
```

4. Adım: Afrika yönlendiricisi EIGRP yönlendirme tablosunu “show ip route eigrp” komutu ile görüntüleyiniz (Görsel 5.81).

```
Afrika#sh ip route eigrp
      20.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
D    21.0.0.0/8 [90/2681856] via 20.0.0.2, 00:04:19, Serial0/0/0
D    22.0.0.0/8 [90/2170112] via 40.0.0.2, 00:03:13, GigabitEthernet0/1
      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
D    192.168.2.0/24 [90/5376] via 40.0.0.2, 00:03:07, GigabitEthernet0/1
D*EX 0.0.0.0/0 [170/7290112] via 40.0.0.2, 00:00:13, GigabitEthernet0/1
```

Görsel 5.81: Afrika yönlendiricisi EIGRP yönlendirme tablosu

Görsel 5.81’de Afrika yönlendiricisi EIGRP yönlendirme tablosu verilmiştir. EIGRP 10 otonom sistemi içinde kalan rotalar D satırı ile gösterilirken sistem dışında öğrenilmiş ağ bilgisi D*EX satırı ile gösterilmiştir.



SIRA SİZDE

Diğer yönlendiricilerin EIGRP yönlendirme tablolarını görüntüleyiniz.

5. Adım: Afrika ve Avustralya yönlendiricileri arasında EIGRP kimlik doğrulama işlemini yapınız.

```
Afrika(config)#key chain Anahtar1
Afrika(config-keychain)#key 1
Afrika(config-keychain-key)#key-string M23041920K
Afrika(config-keychain-key)#exit
Afrika(config-keychain)#exit

Afrika(config)#interface GigabitEthernet 0/1
Afrika(config-if)#ip authentication mode eigrp 10 md5
Afrika(config-if)#ip authentication key-chain eigrp 10 Anahtar1

Avustralya(config)#key chain Anahtar1
Avustralya(config-keychain)#key 1
Avustralya(config-keychain-key)#key-string M23041920K
Avustralya(config-keychain-key)#exit
Avustralya(config-keychain)#exit

Avustralya(config)#interface GigabitEthernet 0/1
Avustralya(config-if)#ip authentication mode eigrp 10 md5
Avustralya(config-if)#ip authentication key-chain eigrp 10 Anahtar1
```

Afrika ve Avustralya yönlendiricilerinde “Anahtar1” adında “1” numaralı ve “M23041920K” parolalı anahtar yapısı oluşturulmuştur. Oluşturulan anahtar GigabitEthernet 0/1 arayüzlerinde md5 ile EIGRP 10 için şifrelenmiştir.

6. Adım: Afrika ve Avustralya yönlendiricilerinin iç ağlarında EIGRP paketlerinin gönderimini kapatınız.

```
Afrika(config)#router eigrp 10
Afrika(config-router)#passive-interface GigabitEthernet 0/0
```

```
Avustralya(config)#router eigrp 10
Avustralya(config-router)#passive-interface GigabitEthernet 0/0
```

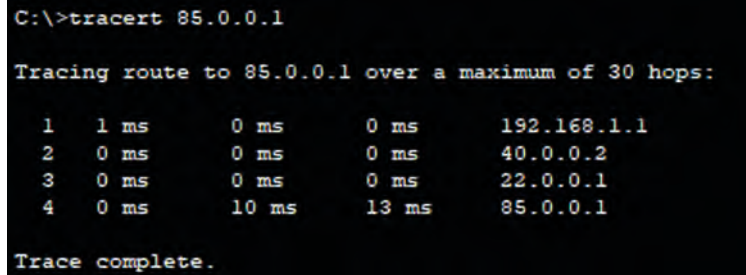
7. Adım: Asya yönlendiricisinde PC0 ve PC1 için statik NAT yapılandırması yapınız.

```
Asya(config)#interface serial0/1/0
Asya(config-if)#ip nat outside
Asya(config-if)#exit
```

```
Asya(config)#interface serial0/0/0
Asya(config-if)#ip nat inside
Asya(config-if)#exit
```

```
Asya(config)#interface serial0/0/1
Asya(config-if)#ip nat inside
Asya(config-if)#exit
Asya(config)#ip nat inside source static 192.168.1.2 85.0.0.2
Asya(config)#ip nat inside source static 192.168.2.2 85.0.0.2
```

8. Adım: PC0'dan İnternet Servis Sağlayıcı yönlendiricisine (85.0.0.1), "tracert" komutu ile rota görüntüleme işlemini yapınız (Görsel 5.82).



```
C:\>tracert 85.0.0.1

Tracing route to 85.0.0.1 over a maximum of 30 hops:

  0  1 ms    0 ms    0 ms    192.168.1.1
  1  0 ms    0 ms    0 ms    40.0.0.2
  2  0 ms    0 ms    0 ms    22.0.0.1
  3  0 ms   10 ms   13 ms    85.0.0.1

Trace complete.
```

Görsel 5.82: Tracert komutu ile EIGRP rota görüntüleme işlemi

Görsel 5.82'de hedefe giden rotanın sırası ile Afrika, Avustralya, Asya yönlendiricileri üzerinden oluştuğu görülür. Bu yol, hedef için en uygun maliyetli metrik değerine sahip rotadır.

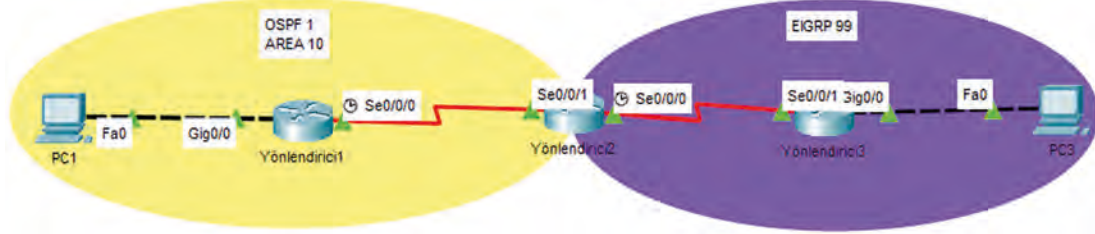
9. Adım: PC0 ve PC1'den İnternet Servis Sağlayıcı yönlendiricisine ve birbirlerine ping komutu ile iletişim testi yapınız.



14. UYGULAMA

EIGRP ve OSPF Yapılandırması

Görsel 5.83'te verilen ağ topolojisini simülasyon programında oluşturunuz. İşlem adımlarına göre Tablo 5.14'te yer alan IP bilgilerini kullanarak ilgili cihazların EIGRP ve OSPF yapılandırmalarını yapınız.



Görsel 5.83: On dördüncü uygulamanın ağ topolojisi

Tablo 5.14: On Dördüncü Uygulamanın IP Bilgileri

Cihaz	Arayüz	DCE	IP	Alt Ağ Maskesi	Varsayılan Ağ Geçidi
Yönlendirici 1	Gig0/0		192.168.1.1	255.255.255.0	192.168.1.1
	Se0/0/0	Cl. rate 128000	90.0.0.1	255.0.0.0	
Yönlendirici 2	Se0/0/0	Cl. rate 128000	91.0.0.1	255.0.0.0	
	Se0/0/1		90.0.0.2	255.0.0.0	
Yönlendirici 3	Gig0/0		192.168.3.1	255.255.255.0	
	Se0/0/1		91.0.0.2	255.0.0.0	
PC1	FastEthernet		192.168.1.2	255.255.255.0	192.168.1.1
PC3	FastEthernet		192.168.3.2	255.255.255.0	192.168.3.1

1. Adım: Yönlendirici ve bilgisayarlarda IP yapılandırmalarını Tablo 5.14'teki değerlerle yapınız. Yapılandırma ile ilgili arayüzler Görsel 5.83'te verilmiştir.

2. Adım: Yönlendirici1 ve Yönlendirici2'de OSPF yapılandırmasını yapınız.

Yönlendirici1(config)#router ospf 1

Yönlendirici1 (config-router)#network 192.168.1.0 0.0.0.255 area 10

Yönlendirici1 (config-router)#network 90.0.0.0 0.255.255.255 area 10

Yönlendirici2(config)#router ospf 1

Yönlendirici2(config-router)#network 90.0.0.0 0.255.255.255 area 10

3. Adım: Yönlendirici2 ve Yönlendirici3'te EIGRP yapılandırmasını yapınız.

Yönlendirici2(config)#router eigrp 99

Yönlendirici2(config-router)#network 91.0.0.0 0.255.255.255

Yönlendirici3(config)#router eigrp 99

Yönlendirici3(config-router)#network 192.168.3.0 0.0.0.255

Yönlendirici3(config-router)#network 91.0.0.0 0.255.255.255

4. Adım: Görsel 5.83'teki ağ topolojisinde OSPF ve EIGRP protokolleri ile çalışan iki farklı otonom sistem görülür. Bu sistemlerdeki iç yönlendiriciler Yönlendirici1 ve Yönlendirici2, farklı otonom sistemdeki ağları tanıyamaz. Bunu görmek için Yönlendirici1'de "show ip route" komutunu kullanınız.

```

90.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C    90.0.0.0/8 is directly connected, Serial0/0/0
L    90.0.0.1/32 is directly connected, Serial0/0/0
192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.168.1.0/24 is directly connected, GigabitEthernet0/0
L    192.168.1.1/32 is directly connected, GigabitEthernet0/0

```

Görsel 5.84: Yönlendirici1'in yönlendirme tablosu

Görsel 5.84'te görüldüğü gibi Yönlendirici1, EIGRP 99 ağlarını tanıyamamıştır. Aynı şekilde Yönlendirici3 de OSPF 10 alanındaki ağları bilemez.

5. Adım: PC1'den PC3'e ping iletişim testi gerçekleştiriniz. Yönlendirici1 yönlendirme tablosunda 192.168.3.0 ağı olmadığı için iletişim başarısız olacaktır.

6. Adım: Yönlendirici2'de "show ip route" komutu ile yönlendirme tablosunu görüntüleyiniz (Görsel 5.85).

```

90.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C    90.0.0.0/8 is directly connected, Serial0/0/1
L    90.0.0.2/32 is directly connected, Serial0/0/1
91.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C    91.0.0.0/8 is directly connected, Serial0/0/0
L    91.0.0.1/32 is directly connected, Serial0/0/0
O    192.168.1.0/24 [110/65] via 90.0.0.1, 00:32:36, Serial0/0/1
D    192.168.3.0/24 [90/2172416] via 91.0.0.2, 00:31:28, Serial0/0/0

```

Görsel 5.85: Yönlendirici2'nin yönlendirme tablosu

7. Adım: Yönlendirici2, EIGRP ve OSPF alanları için köprü yönlendiricidir. Yönlendirici2'nin EIGRP ve OSPF ağları arasındaki iletişimi gerçekleştirebilmesi için OSPF ve EIGRP yapılandırmalarında şu komutları uygulayınız:

```

Yonlendirici2(config)#router ospf 1
Yonlendirici2(config-router)#redistribute eigrp 99 subnets
Yonlendirici2(config)#router eigrp 99
Yonlendirici2(config-router)#redistribute ospf 1 metric 1544 100 255 1 10

```

Yönlendirici2'nin EIGRP yapılandırma satırında OSPF ağlarının bildirimi için gerekli metrik değerleri şunlardır:

- **1544:** Yönlendirici2'nin OSPF alanına bağlı olduğu arayüzün bant genişliği
- **100:** İletim gecikmesinin mikrosaniye cinsinden değeri
- **255:** OSPF alanındaki güvenilirlik oranı
- **1:** OSPF ağının veri kullanım oranı
- **10:** MTU değeri

8. Adım: Yönlendirici1'de "show ip route" komutu ile yönlendirme tablosunu görüntüleyiniz (Görsel 5.86).

```

90.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C    90.0.0.0/8 is directly connected, Serial0/0/0
L    90.0.0.1/32 is directly connected, Serial0/0/0
O E2 91.0.0.0/8 [110/20] via 90.0.0.2, 00:12:25, Serial0/0/0
    192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.168.1.0/24 is directly connected, GigabitEthernet0/0
L    192.168.1.1/32 is directly connected, GigabitEthernet0/0
O E2 192.168.3.0/24 [110/20] via 90.0.0.2, 00:12:25, Serial0/0/0

```

Görsel 5.86: Yönlendirici1'in yönlendirme tablosu

Görsel 5.86'da Yönlendirici1 için yönlendirme tablosu güncellenmiştir. Yönlendirici1, Yönlendirici2'nin aktarımı ile 91.0.0.0/8 ve 192.168.3.0/24 ağlarını öğrenebilmiştir. Bu ağlar EIGRP alanlarından geldiği için O E2 satırı ile yönlendirme tablosunda yazılır.

9. Adım: Yönlendirici3'te "show ip route" komutu ile yönlendirme tablosunu görüntüleyiniz (Görsel 5.87).

```

D EX 90.0.0.0/8 [170/2195456] via 91.0.0.1, 00:14:38, Serial0/0/1
    91.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C    91.0.0.0/8 is directly connected, Serial0/0/1
L    91.0.0.2/32 is directly connected, Serial0/0/1
D EX 192.168.1.0/24 [170/2195456] via 91.0.0.1, 00:14:38, Serial0/0/1
    192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.168.3.0/24 is directly connected, GigabitEthernet0/0
L    192.168.3.1/32 is directly connected, GigabitEthernet0/0

```

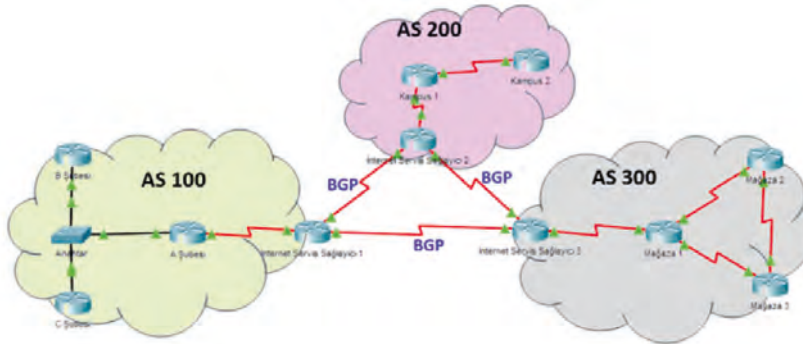
Görsel 5.87: Yönlendirici3'ün yönlendirme tablosu

Görsel 5.87'de Yönlendirici3 için yönlendirme tablosu güncellenmiştir. Yönlendirici3, Yönlendirici2'nin aktarımı ile 90.0.0.0/8 ve 192.168.1.0/24 ağlarını öğrenebilmiştir. Bu ağlar OSPF alanlarından geldiği için D EX satırı ile yönlendirme tablosunda yazılır.

5.5. SINIR AĞ GEÇİDİ PROTOKOLÜ (BGP)

Sınır ağ geçidi protokolü, internette IANA'ya (Internet Assigned Number Authority) kayıtlı farklı otonom sistemler (AS- Autonomous System) arasında yönlendirmeler yapan protokoldür. BGP (Border Gateway Protocol), içinde binlerce farklı yönlendirici ve ağ bulunduran, genellikle internet servis sağlayıcılar gibi çok geniş ağlar arasında yönlendirmeler yapılabilen bir dış ağ geçidi protokolü (EGP-Export Gateway Protocol) türüdür.

Kurum içi ağlar birden fazla noktadan internet servis sağlayıcılarına bağlanıyorsa BGP yönlendirmelerine ihtiyaç duyar.



Görsel 5.88: BGP sınır ağ geçidi protokolü

5.5.1. BGP Özellikleri

BGP'nin özellikleri şu şekilde sıralanabilir:

- BGP ile yönlendirilen her otonom sistem, benzersiz bir otonom sistem numarasına sahiptir (Görsel 5.88).
- Yönlendiricilerin yalnızca bir BGP otonom sistem numarası olabilir.
- Yönlendiriciler hedef rotalar için doğrudan metrik hesaplamaları yapmaz.
- Hedefe giden rotalar için farklı nitelik (Attribute) değerleri kullanılır.
- BGP ile çalışan yönlendiriciler Path (Yol) vektörü protokolünü kullanır. Kaynak ile hedef rotalar arasında tercih edilen otonom sistem numaralarının bilgisi komşudan komşuya aktarılır (Görsel 5.89).



Görsel 5.89: BGP ve yol vektörü protokolü kullanımı

- BGP ile çalışan yönlendiriciler varsayılan olarak otonom sistemler arasında yön bulurken, uzaklık vektörü protokolleri gibi davranıp hedefle arasında en az otonom sistem olan rotaları tercih eder.
- BGP rotaları dışarıdan müdahaleye açıktır ve gerektiğinde el ile değiştirilebilir.
- BGP ile çalışan yönlendiriciler TCP altyapısı ile iletimde bulunur.
- BGP yapılandırmalarında ağ yöneticisi, komşu yönlendiricileri doğrudan yazar ve yönlendiriciler kendi aralarında bire bir bağlantı kurar.
- BGP otonom sistemleri içinde yönlendiricilerin ağ güncellemeleri periyodik olarak yapılmaz. Ağ güncellemeleri yalnızca ağlarda değişiklik meydana geldiğinde yapılır.
- Periyodik olarak komşuluk kontrolü "keepalive" mesajları ile 60 saniyede bir yapılır. Komşuluk düşümü ise 180 saniyedir.
- Aynı otonom sistemler içinde BGP rotalarının yönetimsel uzaklık değeri 200, farklı otonom sistemler arasında BGP rotalarının yönetimsel uzaklık değeri 20'dir.
- İnternet servis sağlayıcılar arasındaki yönlendirmeler için BGP kullanılması bir zorunluluktur.

5.5.2. BGP Mesajları

BGP ile çalışan yönlendiriciler kendi aralarında dört mesaj tipi ile iletişimde bulunur. BGP mesaj türleri şunlardır:

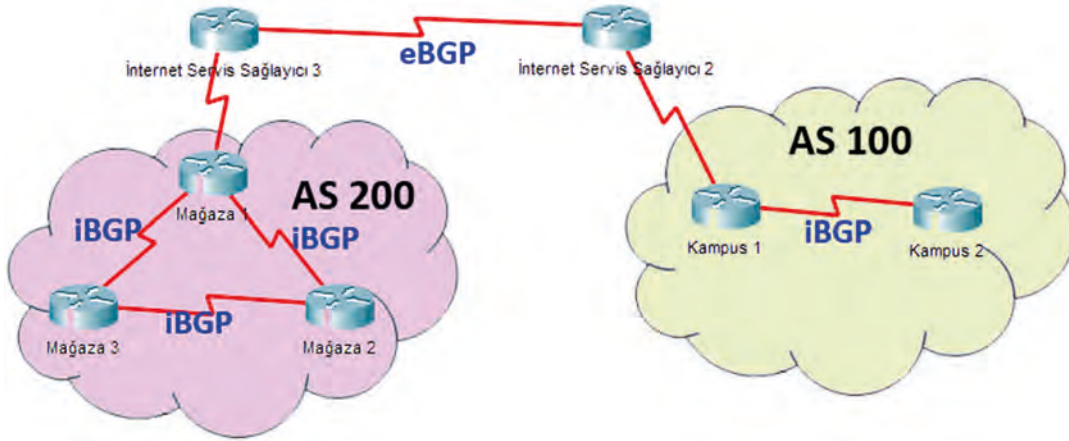
- 1. Open Mesajları:** BGP oturumunu başlatan mesajlardır. Bu mesaj paketleri ile yönlendiriciler arasında BGP versiyon numarası, otonom sistem numarası, komşuluk düşüm süresi, router kimlik (id) bilgisi gibi değerler taşınır.
- 2. Keepalive Mesajları:** Yönlendiriciler arasındaki komşuluğun devamlılığının kontrol edildiği mesajlardır.

3. Update Mesajları: Yönlendiricilerin ağ bilgilerini ve rota üzerindeki otonom sistemlerin numaralarını komşu yönlendiricilere aktardığı mesajlardır. BGP komşuluğu kurulduğunda update mesajları gönderilir. Sonrasında yalnızca yönlendirici ağlarında değişiklik olursa bu işlem gerçekleşir.

4. Notification Mesajları: Hata durumunda BGP komşuluğunu sonlandırma mesajlarıdır.

5.5.3. BGP Komşuluk Türleri

BGP ile çalışan yönlendiriciler bulundukları otonom sistemlerine göre iki farklı BGP oturumu ile komşuluk kurar (Görsel 5.90).



Görsel 5.90: BGP türleri

- **iBGP Oturumu:** Aynı otonom sistem içindeki yönlendiricilerin BGP komşuluğu türüdür. Yönlendiriciler BGP komşuluklarını kurabilmek için doğrudan birbirlerine bağlı veya başka bir iç ağ geçidi protokolü ile iletim hâlinde olmalıdır. Rotaların yönetimsel uzaklık değeri 200'dür.

- **eBGP Oturumu:** Farklı otonom sistemlerdeki yönlendiricilerin birbirleri ile kurdukları BGP komşuluğu türüdür. Rotaların yönetimsel uzaklık değeri 20'dir.

5.5.4. BGP Komşuluğu Aşamaları

BGP ile çalışan yönlendiriciler komşuluklarını tamamlamak için şu aşamaları gerçekleştirmek zorundadır:

- **Idle:** BGP komşuluğunun henüz başlamadığı aşamadır.
- **Connect:** Yönlendiricilerin kendi aralarında TCP ile bağlantı anlaşıması yapmasıdır.
- **Open Sent:** Yönlendiricilerin BGP oturumları açma isteği oluşturduğu aşamadır.
- **Active:** Oturum açma isteğinin bekleme süresidir. Süre sonunda oturum açılması onaylanmazsa süreç başa döner.
- **Open Confirm:** Yönlendiricilerde BGP oturumu açılmasının onaylanmasıdır.
- **Established:** BGP komşuluk kurulumunun oluşturulduğu aşamadır.

5.5.5. BGP Yapılandırması

Yönlendiricilerde BGP yapılandırması temel olarak otonom sistem numarası, komşu yönlendirici IP, komşu otonom sistem numarası ve yönlendirici ağ adreslerinin bildirimi ile gerçekleştirilir.

`Yönlendirici(config)#router bgp 'Otonom Sistem Numarası'`

`Yönlendirici(config-router)#neighbor 'Komşu Yönlendirici IP adresi' remote-as 'Komşu Otonom Sistem Numarası'`

`Yönlendirici(config-router)#network 'Aryüz Ağ Adresi' mask 'Ağ Alt Ağ Maskesi'`

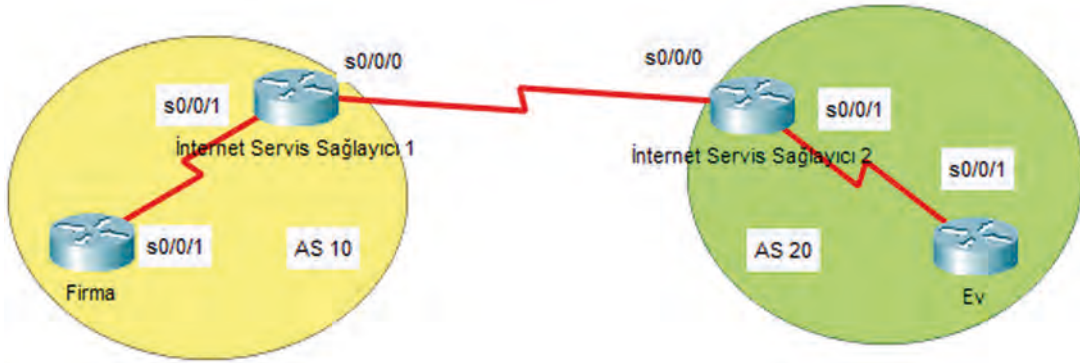
Yönlendiriciler RIP, EIGRP ve OSPF yapılandırmalarından farklı olarak yalnızca bir BGP otonom sistem numarası ile yapılandırılabilir. BGP varsayılan olarak sınıflı ağ yapısı ile çalışır ancak alt ağ maskesi belirtilirse sınıfsız ağları da destekler.



15. UYGULAMA

BGP Yapılandırması

Görsel 5.91'de verilen ağ topolojisini simülasyon programında oluşturunuz. İşlem adımlarına göre Tablo 5.15'te yer alan IP bilgilerini kullanarak ilgili cihazların BGP yapılandırmasını yapınız.



Görsel 5.91: On beşinci uygulamanın ağ topolojisi

Tablo 5.15: On Beşinci Uygulamanın IP Bilgileri

Cihaz	Aryüz	DCE	IP	Alt Ağ Maskesi
ISP1	Se0/0/0	Cl. rate 128000	95.0.0.1	255.0.0.0
	Se0/0/1	Cl. rate 128000	10.0.0.1	255.0.0.0
ISP2	Se0/0/0		95.0.0.2	255.0.0.0
	Se0/0/1	Cl. rate 128000	20.0.0.1	255.0.0.0
Firma	Se0/0/1		10.0.0.2	255.0.0.0
Ev	Se0/0/1		20.0.0.2	255.0.0.0

1. Adım: Yönlendirici ve bilgisayarlarda IP yapılandırmalarını Tablo 5.15'teki değerlerle yapınız. Yapılandırma ile ilgili arayüzler Görsel 5.91'de verilmiştir.

2. Adım: İnternet Servis Sağlayıcı 1 (ISP1) ve İnternet Servis Sağlayıcı 2 (ISP2) yönlendiricilerinde AS 10 ve AS 20 için BGP komşuluk yapılandırmalarını yapınız.

```
ISP1(config)#router bgp 10
```

```
ISP1(config-router)#neighbor 95.0.0.2 remote-as 20
```

```
ISP2(config)#router bgp 20
```

```
ISP2(config-router)#neighbor 95.0.0.1 remote-as 10
```

3. Adım: ISP1 ve ISP2 yönlendiricilerinde “show ip bgp summary” komutu ile BGP komşuluklarının özet (summary) tablosunu görüntüleyiniz (Görsel 5.92).

```
ISP1#show ip bgp summary
```

Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	State/PfxRcd
95.0.0.2	4	20	20	20	1	0	0	00:18:15	4

Görsel 5.92: ISP1 yönlendiricisinin BGP özet tablosu

ISP1 yönlendiricisi için Neighbor sütununda komşuluk kurulan ISP2 yönlendiricisi IP bilgisi (95.0.0.2), V sütununda BGP versiyon numarası (4), MsgRcvd ve MsgSent sütunlarında komşu yönlendirici ile gönderilip alınan paketlerin sayısı (20), TblVer sütununda BGP tablosunun versiyon numarası (1), Up/Down sütununda BGP komşuluğu kurulumundan sonra geçen süre, State/PfxRcd sütununda BGP aşaması bilgisi yazılır. State/PfxRcd sütununda sayı yazılması, komşulukta sorun olmadığını gösterir.



SIRA SİZDE

ISP2 yönlendiricisinde “show ip bgp summary” komutu ile BGP komşuluklarının özet tablosunu inceleyiniz.

4. Adım: ISP1 yönlendiricisinde 10.0.0.0/8 ağının, ISP2 yönlendiricisinde 20.0.0.0/8 ağının bildirimlerini yapınız.

```
ISP1(config)#router bgp 10
```

```
ISP1(config-router)#network 10.0.0.0 mask 255.0.0.0
```

```
ISP2(config)#router bgp 20
```

```
ISP2(config-router)#network 20.0.0.0 mask 255.0.0.0
```

5. Adım: ISP1 ve ISP2 yönlendiricilerinde “show ip bgp” komutu ile BGP tablosunu görüntüleyiniz (Görsel 5.93).

```
ISP1#show ip bgp
```

Network	Next Hop	Metric	LocPrf	Weight	Path
*> 10.0.0.0/8	0.0.0.0	0	0	32768	i
*> 20.0.0.0/8	95.0.0.2	0	0	0	20 i

Görsel 5.93: ISP1 yönlendiricisinin BGP tablosu

BGP tablosu Network sütununda öğrenilmiş ağ adresi bilgisi, Next Hop sütununda ağı öğreten yönlendirici IP numarası, Path sütununda ise hedefe giden otonom sistemlerin numarası bulunur.

Next Hop sütununda "0.0.0.0" bulunuyorsa bu durum, satırın yerel bir ağ bağlantısı olduğunu gösterir. BGP satırı ">" işareti ile başlıyorsa bu satır, tercih edilen rotadır.



SIRA SİZDE

ISP2 yönlendiricisinde "show ip bgp" komutu ile BGP tablosunu inceleyiniz.

6. Adım: ISP1 ve ISP2 yönlendiricilerinde "show ip route bgp" komutu ile BGP yönlendirme tablosunu görüntüleyiniz (Görsel 5.94).

ISP1#show ip route bgp

```
ISP1#show ip route bgp
B    20.0.0.0/8 [20/0] via 95.0.0.2, 00:00:00
```

Görsel 5.94: ISP1 yönlendiricisinin BGP yönlendirme tablosu

Yönlendirme tablolarında BGP satırları "B" ile gösterilir. Farklı otonom sistemlerden öğrenilen BGP rotalarının yönetimsel uzaklık değeri ise 20'dir.



SIRA SİZDE

ISP2 yönlendiricisinde "show ip route bgp" komutu ile BGP yönlendirme tablosunu inceleyiniz.

7. Adım: Firma ve Ev yönlendiricilerinden ISP yönlendiricilerine varsayılan rota çıkışlarını yapınız.

Firma(config)#ip route 0.0.0.0 0.0.0.0 s0/0/1

Ev(config)#ip route 0.0.0.0 0.0.0.0 s0/0/1

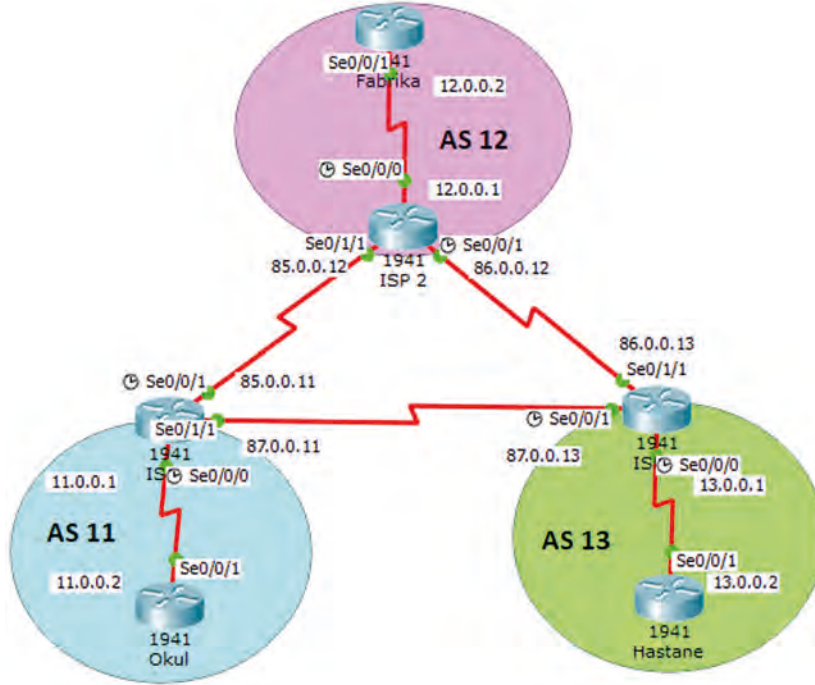
8. Adım: Firma ve Ev yönlendiricilerinde ping komutu ile karşılıklı olarak iletişim testi gerçekleştiriniz. Test başarılı olacaktır.



16. UYGULAMA

BGP Yapılandırması

Görsel 5.95'te verilen ağ topolojisini simülasyon programında oluşturunuz. İşlem adımlarına göre Tablo 5.16'da yer alan IP bilgilerini kullanarak ilgili cihazların BGP yapılandırmasını yapınız.



Görsel 5.95: On altıncı uygulamanın ağ topolojisi

Tablo 5.16: On Altıncı Uygulamanın IP Bilgileri

Cihaz	Arayüz	DCE	IP	Alt Ağ Maskesi
ISP1	Se0/0/0	Cl. Rate 128000	11.0.0.1	255.0.0.0
	Se0/0/1	Cl. Rate 128000	85.0.0.11	255.0.0.0
	Se0/1/1		87.0.0.11	255.0.0.0
ISP2	Se0/0/0	Cl. Rate 128000	12.0.0.1	255.0.0.0
	Se0/0/1	Cl. Rate 128000	86.0.0.12	255.0.0.0
	Se0/1/1		85.0.0.12	255.0.0.0
ISP3	Se0/0/0	Cl. Rate 128000	13.0.0.1	255.0.0.0
	Se0/0/1	Cl. Rate 128000	87.0.0.13	255.0.0.0
	Se0/1/1		86.0.0.13	255.0.0.0
Okul	Se0/0/1		11.0.0.2	255.0.0.0
Fabrika	Se0/0/1		12.0.0.2	255.0.0.0
Hastane	Se0/0/1		13.0.0.2	255.0.0.0

1. Adım: Yönlendirici ve bilgisayarlarda IP yapılandırmalarını Tablo 5.16'daki değerlerle yapınız. Yapılandırma ile ilgili arayüzler Görsel 5.95'te verilmiştir.

2. Adım: ISP1, ISP2 ve ISP3 yönlendiricilerinde otonom sistem AS 11, AS 12 ve AS 13 için BGP komşuluklarını kurunuz.

```
ISP1(config)#router bgp 11
ISP1(config-router)#neighbor 87.0.0.13 remote-as 13
ISP1(config-router)#neighbor 85.0.0.12 remote-as 12
```

```
ISP2(config)#router bgp 12
ISP2(config-router)#neighbor 85.0.0.11 remote-as 11
ISP2(config-router)#neighbor 86.0.0.13 remote-as 13
```

```
ISP3(config)#router bgp 13
ISP3(config-router)#neighbor 87.0.0.11 remote-as 11
ISP3(config-router)#neighbor 86.0.0.12 remote-as 12
```

3. Adım: ISP1, ISP2 ve ISP3 yönlendiricilerinde “show ip bgp summary” komutu ile BGP komşulukları özet tablolarını görüntüleyiniz (Görsel 5.96).

ISP1 yönlendiricisi için BGP komşulukları özet tablosu:

```
ISP1#show ip bgp summary
```

Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	State/PfxRcd
87.0.0.13	4	13	36	36	1	0	0	00:34:05	4
85.0.0.12	4	12	35	36	1	0	0	00:13:55	4

Görsel 5.96: ISP1 yönlendiricisinin BGP komşuluğu özet tablosu

Görsel 5.96'daki ISP1 yönlendiricisi, ISP2 ve ISP3 komşu yönlendiricileri ile BGP komşuluklarını tamamlamıştır.

4. Adım: ISP1, ISP2 ve ISP3 yönlendiricilerinde iç ağ bildirimlerini gerçekleştiriniz.

```
ISP1(config)#router bgp 11
ISP1(config-router)#network 11.0.0.0 mask 255.0.0.0
```

```
ISP2(config)#router bgp 12
ISP2(config-router)#network 12.0.0.0 mask 255.0.0.0
```

```
ISP3(config)#router bgp 13
ISP3(config-router)#network 13.0.0.0 mask 255.0.0.0
```

5. Adım: ISP1, ISP2 ve ISP3 yönlendiricilerinde “show ip bgp” komutu ile BGP tablolarını görüntüleyiniz (Görsel 5.97).

ISP1#show ip bgp

Network	Next Hop	Metric	LocPrf	Weight	Path
*> 11.0.0.0/8	0.0.0.0	0	0	32768	i
*> 12.0.0.0/8	85.0.0.12	0	0	0	12 i
*	87.0.0.13	0	0	0	13 12 i
*> 13.0.0.0/8	87.0.0.13	0	0	0	13 i
*	85.0.0.12	0	0	0	12 13 i

Görsel 5.97: ISP1 yönlendiricisinin BGP tablosu

ISP1 yönlendiricisi BGP tablosunda hedef ağlar için en iyi rotanın Path sütununda en az AS numarası olan satırlar olduğu görülür. Tercih rotaları “>” simgesi ile işaret edilmiştir.

6. Adım: ISP1, ISP2 ve ISP3 yönlendiricilerinde “show ip route bgp” komutu ile BGP yönlendirme tablosunu görüntüleyiniz (Görsel 5.98).

ISP1 yönlendiricisi için BGP yönlendirme tablosu:

ISP1#show ip route bgp

```
ISP1#show ip route bgp
B    12.0.0.0/8 [20/0] via 85.0.0.12, 03:25:08
B    13.0.0.0/8 [20/0] via 87.0.0.13, 03:25:08
```

Görsel 5.98: ISP1 yönlendiricisinin BGP yönlendirme tablosu

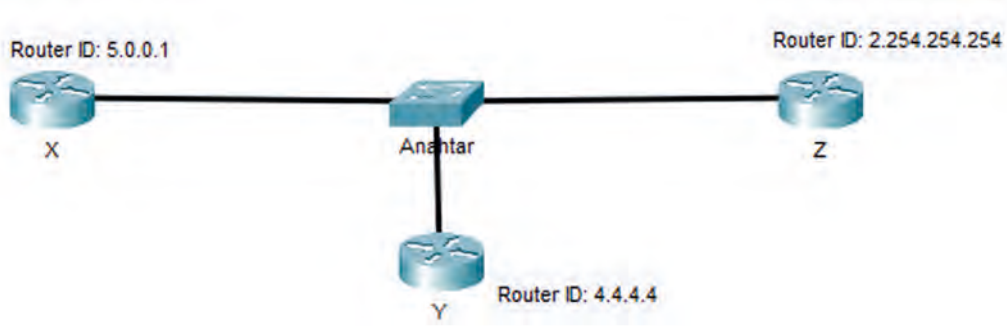
ISP1 yönlendiricisi için yönlendirme satırına 12.0.0.0/8 ve 13.0.0.0/8 ağları eklenmiştir.

7. Adım: Okul yönlendiricisinden Fabrika ve Hastane yönlendiricilerine ping iletişim testi gerçekleştiriniz.

5. Görsel 5.99'da verilen topoloji OSPF dinamik yönlendirme protokolü ile gerçekleştirildiğinde PC0'dan PC1'e giden veri paketlerinin yönlendirici sırasına göre izlediği yol aşağıdakilerden hangisidir?

- A) X-Y-Z-T B) X-Y-T C) X-T D) X-Z-T E) X-Z-Y-T

6.



Görsel 5.100: 6. soru için ağ topolojisi

Görsel 5.100'de verilen ağ topolojisi OSPF yönlendirme protokolü ile çalışır. Verilen yönlendirici ID değerlerine göre LSA dağıtımlarını yapmakta öncelikli DR yönlendirici ve ikinci yönlendirici BDR sırası ile aşağıdakilerden hangisidir?

- A) Z-Y B) Z-X C) Y-Z D) X-Z E) X-Y

7. Aşağıdakilerden hangisi EIGRP yönlendirme protokolünün yönetimsel uzaklık değeridir?

- A) 20 B) 90 C) 110 D) 120 E) 200

8. RIP, OSPF, EIGRP yönlendirme protokollerinin üçü ile de yapılandırılmış yönlendiricilerin olduğu bir ağ topolojisinde tercih edilecek dinamik yönlendirme protokolü aşağıdakilerden hangisidir?

- A) Seçim, ağ yöneticisine bırakılır.
B) RIP tercih edilir.
C) OSPF tercih edilir.
D) EIGRP tercih edilir.
E) Yönlendirmeler çalışmaz.

9. İnternet servis sağlayıcılar gibi içinde binlerce ağ ve yönlendirici bilgisi taşıyabilen otonom sistemler arasındaki yönlendirmelerde kullanılan protokol aşağıdakilerden hangisidir?

- A) Statik B) RIP C) OSPF D) EIGRP E) BGP

10. Aşağıdakilerden hangisi bir BGP mesaj türü değildir?

- A) Query B) Open C) Keepalive D) Update E) Notification



KONULAR

- 6.1. POINT-TO-POINT BAĞLANTILAR
- 6.2. ERİŞİM KONTROL LİSTELERİ
- 6.3. AĞ GÜVENLİĞİ VE AĞ İZLEME

ANAHTAR KELİMELER

- Point-to-Point
- ACL
- QoS
- Ağ izleme
- Ağ sorunları

6. ÖĞRENME BİRİMİ

WAN KONSEPTİ

NELER ÖĞRENECEKSİNİZ?

- Point-to-Point bağlantılar
- Erişim kontrol listeleri
- Ağ izleme yazılımı
- Servis kalitesi
- Ağ sorunları





HAZIRLIK ÇALIŞMALARI

1. Evinizdeki birçok cihazın internetle bağlantısı, internet kullanımınızı nasıl etkiler?
2. Araç trafiğini düzenlemek için neler yapıldığını araştırınız. Ağ trafiğini de benzer şekilde düzenlemek için neler yapılabilir? Düşüncelerinizi arkadaşlarınızla paylaşınız.

6.1. POINT-TO-POINT BAĞLANTILAR

Point-to-Point bağlantılar, iki ağ geçidi arasında bilgi alışverişi sağlamak için kullanılan veri köprüleme protokolüdür. Bu bağlantılar, noktadan noktaya bağlantı olarak da ifade edilir. Point-to-Point Protokolü (PPP), OSI modelinin veri bağı katmanı (Data Link Layer) protokolüdür. Telefon hattı gibi seri bir hat üzerinden bilgi alışverişini yapacak iki noktanın bağlantısını sağlayarak çift yönlü iletim (full-duplex) kurulmasına izin verir. Modem, yönlendirici veya benzer başka bir cihaz yardımıyla seri bağlantılar kurulmasına olanak sağlar.

PPP'nin gelişmesiyle iki bilgisayarın haberleşmesinde internet servis sağlayıcısı (ISP) tarafından atanan IP adresini sisteme tanıtmak için ek bir işleme gerek kalmamıştır. Sistem bu tanıtımı otomatik olarak yapar. PPP, asenkron (farklı zamanlı) hatlara ek olarak senkron (eş zamanlı) hatlar üzerinde de çalışabilir.

Point-to-Point bağlantıların temel amacı, seri bağlantı üzerinden veri paketlerinin aktarılmasıdır. Bu sayede iletişime uygun iki cihazın özel olarak yapılandırılmış veri paketleriyle bilgi alışverişi yapması sağlanır.

Noktadan noktaya protokolü;

- HDLC protokolüyle kapsülleme (Encapsulation),
- Bağlantı kontrol protokolüyle bağlantının kurulması, yapılandırılması ve test edilmesi (Link Control Protocol-LCP),
- Ağ kontrol protokolüyle Layer 3 protokollerinin kullanımı (Network Control Protocol-NCP) olmak üzere üç ana bölümde incelenebilir.

6.1.1. Kapsülleme (Encapsulation)

PPP'nin kapsülleme özelliği sayesinde farklı ağ katmanı protokolleri tek bir bağlantı üzerinde eş zamanlı olarak çalışır ve veri paketlerinin PPP ile gönderilmek üzere nasıl paketleneyeceği belirlenir. Yüksek seviyede veri bağlantı kontrolü (High Level Data Link Control-HDLC), noktadan noktaya bağlantılarda kullanılan temel kapsülleme metodudur. PPP, HDLC protokolünü temel alarak kapsülleme yapar fakat bu protokolden farklı olarak PAP ve CHAP gibi güvenlik mekanizması içerir. PPP, veri bağlama katmanı üzerinden iletimin sağlanabilmesi için veriyi enkapsüle ederek çerçeve hâline getirir.

6.1.1.1. HDLC Enkapsülasyonu

HDLC, iki nokta arasında iletişimin hatasız sağlanması için eş zamanlı seri iletim kullanır. Acknowledgement (alındı bildirimleri) kullanımıyla veri akışının ve hatanın kontrolünü sağlayan veri bağı katmanına (Katman 2) özgü bir çerçeve yapısı tanımlar.

6.1.2. Bağlantı Kontrol Protokolü (Link Control Protocol-LCP)

Bağlantı kontrol protokolü, PPP'nin kullandığı ana protokoldür. LCP, fiziksel katmanda (Katman 1) çalışır. LCP; fiziksel bağlantıyı kurmak, sürdürmek, kontrol etmek ve yapılandırmak için kullanılır. LCP ayrıca kapsülleme parametrelerini ve noktadan noktaya bağlantı kurulduğunda kimlik doğrulama, hata algılama ve sıkıştırma gibi diğer PPP yapılandırma seçenekleri için de kullanılır.

6.1.3. Ağ Kontrol Protokolü (Network Control Protocol-NCP)

PPP; aynı bağlantı üzerinden birden fazla ağ katmanı (Layer 3) IP, IPX ve Apple Talk gibi protokolleri çalıştırır. PPP, bu protokollerin kullanılması ve çalışması için her birine ayrı birer NCP kullanır.

6.1.4. PPP Yapılandırma

Yönlendiricilerde PPP yapılandırmasını gerçekleştirmek için öncelikle arayüzlerin ağ adresleri, bant genişliği ve saat sinyali gibi ayarlar yapılmalıdır. PPP yapılandırmasını etkinleştirmek için yönlendiricinin ilgili arayüzünde "encapsulation ppp" komutu girilir.

```
Ankara(config)#interface serial 0/0/0
```

```
Ankara(config-if)#encapsulation ppp
```



1. UYGULAMA

PPP Yapılandırma

İşlem adımlarına göre Görsel 6.1'de verilen ağ topolojisini kullanarak yönlendiricilerde PPP yapılandırması yapınız.



Görsel 6.1: PPP yapılandırma topolojisi

1. Adım: Görsel 6.1'de cihazların üzerinde fiziksel arayüz, IP, alt ağ maskesi ve varsayılan ağ geçidi bilgileri verilmiştir. Cihazlara görselde verilen IP'leri giriniz.

Ankara yönlendiricisi için arayüz yapılandırması komut satırları:

```
Ankara(config)#interface serial 0/0/0
```

```
Ankara(config-if)#clock rate 128000
```

```
Ankara(config-if)#bandwidth 128
```

```
Ankara(config-if)#ip address 23.4.192.1 255.255.255.0
```

```
Ankara(config-if)#no sh
```

Erzurum yönlendiricisi için arayüz yapılandırması komut satırları:

```
Erzurum(config)#interface serial 0/0/0
```

```
Erzurum(config-if)#bandwidth 128
```

```
Erzurum(config-if)#ip address 23.4.192.2 255.255.255.0
```

```
Erzurum(config-if)#no sh
```

2. Adım: Yönlendiricilerde WAN kapsülleme protokolünü PPP olarak etkinleştirmek için gerekli komutları giriniz.

Ankara yönlendiricisi için komut satırları:

Ankara(config)#interface serial 0/0/0

Ankara(config-if)#encapsulation ppp

Erzurum yönlendiricisi için komut satırları:

Erzurum(config)#interface serial 0/0/0

Erzurum(config-if)#encapsulation ppp

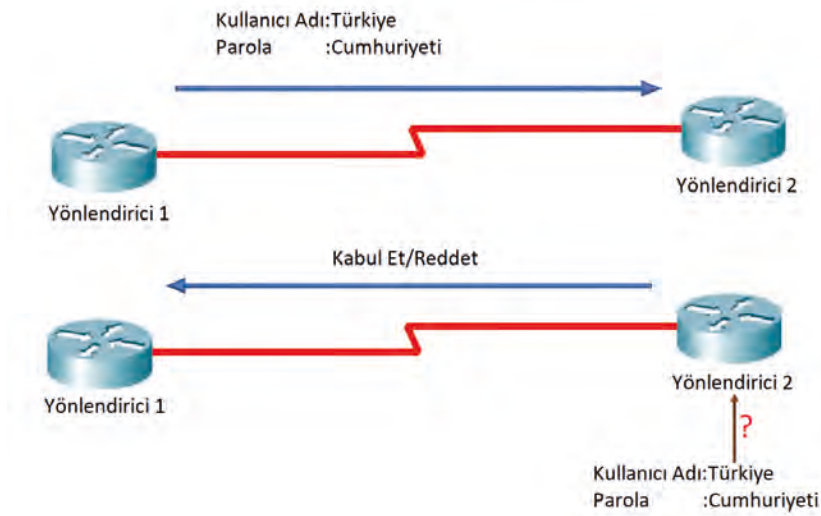
3. Adım: Ankara yönlendiricisinden Erzurum yönlendiricisine iletişimi ping komutu ile test ediniz ve iletişimin başarılı olduğunu gözlemleyiniz.

6.1.5. PPP Kimlik Doğrulama Protokolleri

PPP'nin bir özelliği de birçok genel güvenlik prosedürlerine ek olarak, LCP ile bağlantı kurarken gerçekleştirdiği kimlik denetimidir. PPP ile bağlantılarda güvenliğin sağlanması için PAP (Password Authentication Protocol-Parola Doğrulama Protokolü) ve CHAP (Challenge Handshake Authentication Protocol-Karşılıklı Tokalaşma Kimlik Doğrulaması Protokolü) olmak üzere iki kimlik doğrulama protokolü bulunur. İki nokta arasında kurulacak bağlantı doğrulanarak daha güvenli bir iletişim ortamı oluşturulur. Böylece noktadan noktaya bağlantı yetkisi olmayan cihazlardan korunma sağlanır.

6.1.5.1. Parola Doğrulama Protokolü (Password Authentication Protocol-PAP)

Parola doğrulama protokolünde bağlantı kurulmadan önce yönlendirici tarafından kullanıcı adı ve parolası diğer yönlendiriciye gönderilir. Kullanıcı adı ve parolasını alan yönlendirici bu bilgileri kendi veri tabanından kontrol ederek bilgiler doğruysa bağlantıyı kabul eder, yanlışa reddeder. Gönderilen parola şifrelenmez. Kimlik denetiminden sonra protokolün görevi biter (Görsel 6.2).



Görsel 6.2: PAP ile kimlik doğrulama

PAP ile kimlik doğrulaması için öncelikle yönlendirici komut ekranı konfigürasyon satırında kullanıcı adı ve parola tanımlanmalıdır. Parola doğrulama protokolünü etkinleştirmek için ilgili arayüzde “ppp authentication pap” komutu kullanılır. Tanımlanan kullanıcı adı ve parolayı göndermek için “ppp sent-username kullanıcıadı password parola” komutu kullanılır.

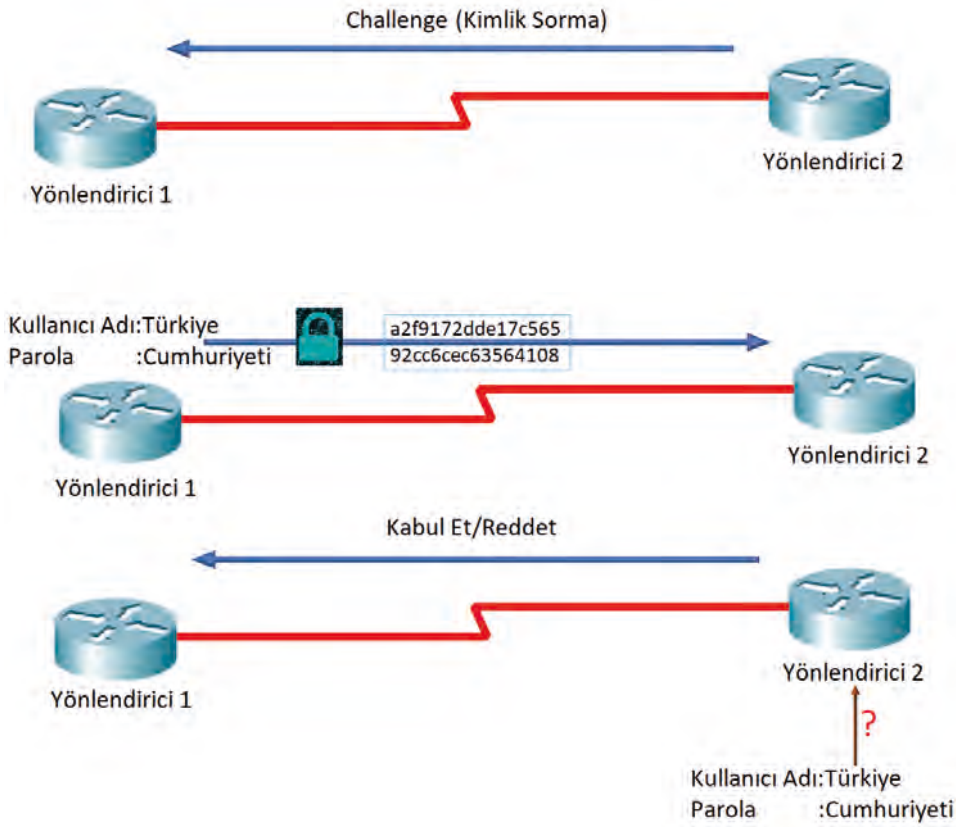
```
Ankara(config)#username kullanıcıadı password parola
```

```
Ankara(config-if)#ppp authentication pap
```

```
Ankara(config-if)#ppp sent-username kullanıcıadı password parola
```

6.1.5.2. Karşılıklı Tokalaşma Kimlik Doğrulaması Protokolü (Challenge Handshake Authentication Protocol-CHAP)

İki nokta arasında bağlantının kurulmasından hemen sonra karşı taraftaki yönlendirici bir kimlik sorgulaması gönderir. Diğer uçtaki yönlendirici ise sorgulama mesajıyla hesaplanan md5 ile şifrelenmiş bir şekilde kullanıcı adını ve parolasını cevap olarak gönderir. Kullanıcı adı ve parolası doğrulanırsa bağlantı onaylanır, doğrulanmazsa bağlantı hemen sonlandırılır (Görsel 6.3).



Görsel 6.3: CHAP ile kimlik doğrulama

Kimlik denetiminde şifreli bir şekilde haberleşmenin yanında CHAP, belirli aralıklarla tekrar kimlik doğrulaması yapar. CHAP bu özelliklerinden dolayı PAP ile kimlik doğrulamadan daha güvenlidir. PAP ve CHAP karşılaştırması Tablo 6.1’de verilmiştir.

Tablo 6.1: PAP ve CHAP Karşılaştırması

PAP	CHAP
İki yönlü el sıkışma yapılır.	Üç yönlü el sıkışma yapılır.
Kullanıcı adı ve parolası açık olarak gönderilir.	Kullanıcı adı ve parolası md5 şifrelemesi ile gönderilir.
Kimlik denetimi bağlantı kurulduktan sonra tekrar edilmez.	Kimlik denetimi belli aralıklarla tekrar edilir.
İki tarafta kullanılan şifreler aynı olmak zorunda değildir.	Şifrelerin aynı olma zorunluluğu vardır.

CHAP ile kimlik doğrulama yapabilmek için öncelikle yönlendirici komut ekranı konfigürasyon satırında kullanıcı adı ve parolası tanımlanmalıdır. Bu protokolü etkinleştirmek için ilgili arayüzde “ppp authentication chap” komutu kullanılır.

Ankara(config)#username kullanıcıadı password parola

Ankara(config-if)#ppp authentication chap

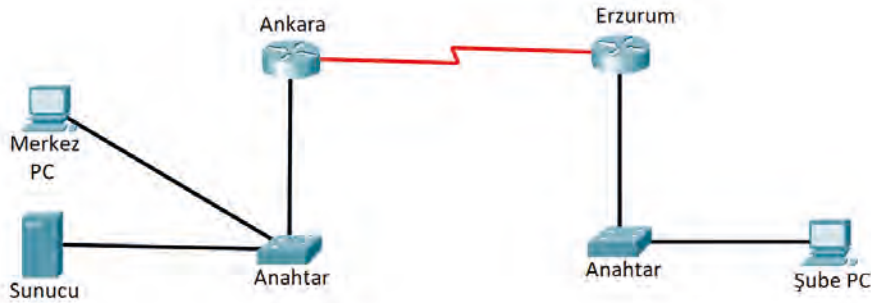
Ankara(config-if)#ppp sent-username kullanıcıadı password parola



2. UYGULAMA

PAP Kimlik Doğrulaması

İşlem adımlarına göre Tablo 6.2’deki adres bilgilerini kullanarak yönlendiricilere PPP yapılandırmasını ve PAP kimlik doğrulamasını kullanıcı adı **Türkiye**, parola **Cumhuriyeti** olacak şekilde yapınız (Görsel 6.4).



Görsel 6.4: PAP ile kimlik doğrulama ağ topolojisi

Tablo 6.2: Point-to-Point Bağlantı PAP Kimlik Doğrulama Yapılandırma Uygulaması IP Adresleri

Cihaz	Arayüz	IP Adresi	Alt Ağ Maskesi	Varsayılan Ağ Geçidi
Ankara Yönlendiricisi	Se0/0/0 (DCE)	23.4.192.1	255.255.255.0	
	Gig0/1	192.168.1.1	255.255.255.0	
Erzurum Yönlendiricisi	Se0/0/0	23.4.192.2	255.255.255.0	
	Gig0/1	29.10.19.23	255.255.255.0	
Şube PC	FastEthernet	29.10.19.24	255.255.255.0	29.10.19.23
Merkez PC	FastEthernet	192.168.1.2	255.255.255.0	192.168.1.1
Sunucu	FastEthernet	192.168.1.254	255.255.255.0	192.168.1.1

1. Adım: Görsel 6.4'te cihazların üzerinde fiziksel arayüz, IP, alt ağ maskesi ve varsayılan ağ geçidi bilgileri verilmiştir. Cihazlara görselde verilen IP'leri giriniz.

Ankara yönlendiricisi için arayüz yapılandırması komut satırları:

```
Ankara(config)#username Türkiye password Cumhuriyeti
Ankara(config)#interface serial 0/0/0
Ankara(config-if)#clock rate 128000
Ankara(config-if)#bandwidth 128
Ankara(config-if)#ip address 23.4.192.1 255.255.255.0
Ankara(config-if)#no sh
```

Erzurum yönlendiricisi için arayüz yapılandırması komut satırları:

```
Erzurum(config)#username Türkiye password Cumhuriyeti
Erzurum(config)#interface serial 0/0/0
Erzurum(config-if)#bandwidth 128
Erzurum(config-if)#ip address 23.4.192.2 255.255.255.0
Erzurum(config-if)#no sh
```

2. Adım: Yönlendiricilerde WAN kapsülleme protokolünü PPP olarak etkinleştirmek için gerekli komutları giriniz.

Ankara yönlendiricisi için komut satırları:

```
Ankara(config)#interface serial 0/0/0
Ankara(config-if)#encapsulation ppp
```

Erzurum yönlendiricisi için komut satırları:

```
Erzurum(config)#interface serial 0/0/0
Erzurum(config-if)#encapsulation ppp
```

3. Adım: Yönlendiricilerde PAP kimlik doğrulamasını etkinleştirmek için gerekli komutları giriniz.

Ankara yönlendiricisi için komut satırları:

```
Ankara(config-if)#ppp authentication pap
Ankara(config-if)#ppp sent-username Türkiye password Cumhuriyeti
```

Erzurum yönlendiricisi için komut satırları:

```
Erzurum(config)# ppp authentication pap
Erzurum(config-if)#ppp sent-username Türkiye password Cumhuriyeti
```

4. Adım: Merkez PC komut ekranından Şube PC ve Erzurum yönlendiricisinin IP adreslerine ping atarak iletişimi test ediniz.


```

C:\>ping 29.10.19.23

Pinging 29.10.19.23 with 32 bytes of data:

Reply from 29.10.19.23: bytes=32 time=1ms TTL=254
Reply from 29.10.19.23: bytes=32 time=1ms TTL=254
Reply from 29.10.19.23: bytes=32 time=2ms TTL=254
Reply from 29.10.19.23: bytes=32 time=1ms TTL=254

Ping statistics for 29.10.19.23:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms

C:\>ping 29.10.19.24

Pinging 29.10.19.24 with 32 bytes of data:

Reply from 29.10.19.24: bytes=32 time=1ms TTL=126
Reply from 29.10.19.24: bytes=32 time=11ms TTL=126
Reply from 29.10.19.24: bytes=32 time=1ms TTL=126
Reply from 29.10.19.24: bytes=32 time=10ms TTL=126

Ping statistics for 29.10.19.24:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 11ms, Average = 5ms

C:\>

```

Görsel 6.5: PAP ile kimlik doğrulama sonrası iletişimi test etme



SIRA SİZDE

Tablo 6.2'deki adres bilgilerine göre Görsel 6.4'te verilen ağ topolojisindeki yönlendiricilere PPP yapılandırmasını ve CHAP kimlik doğrulamasını kullanıcı adı Türkiye, parola Cumhuriyeti olacak şekilde gerçekleştiriniz.

6.2. ERİŞİM KONTROL LİSTELERİ (ACL)

Bir yönlendirici arabirimi üzerinden yapılan veri alışverişi trafiğine uygulanacak koşullar, erişim kontrol listeleriyle (Access Control List-ACL) denetlenir. Erişim kontrol listeleriyle hangi veri paketlerinin ret veya kabul edileceği belirlenir. Bu sayede ağ trafiği yönetilir ve ağa erişim güvenli hâle getirilir.

Erişim kontrol listeleri oluşturmanın temel nedenleri şunlardır:

- Erişim kontrol listeleri, ağ trafiğini sınırlar ve ağ performansını artırır, ağ trafiği akışında kontrolü sağlar. Ağdaki video trafiği sınırlandırılarak bant genişliği verimli kullanılır ve ağın performansı artırılır.
- Erişim kontrol listeleri, ağ erişiminde temel bir güvenlik düzeyi sağlar. Erişim kontrol listeleriyle bir ağ cihazının ağın bir kısmına erişmesine izin verilirken diğer bir ağ cihazının aynı bölgeye erişimi engellenebilir.
- Erişim kontrol listeleri, yönlendirici arabirimlerinde hangi tip trafiğe izin verileceğine veya hangi tip trafiğin engelleneceğine karar verir. Erişim kontrol listeleri FTP trafiğini engellerken e-posta trafiğine izin verilebilir, TELNET trafiğini sadece ağ yöneticisi kullanacak şekilde yapılandırabilir.

Erişim kontrol listeleri, “deny” veya “permit” satırlarından oluşur. İzin verilecek trafik için permit satırları, engellenecek trafik için deny satırları kullanılır. Erişim kontrol listeleri ile yönlendiricinin arayüzüne gelen paketlere (in-giriş) veya arayüzden giden paketlere (out-çıkış) uygulanır. Erişim kontrol listeleri (ACL) oluşturulduktan sonra ilgili arayüze giriş (in) veya çıkış (out) yönünde uygulanmalıdır.

Erişim kontrol listeleri genellikle standart (standard ACL), genişletilmiş (extended ACL) ve isimli (named ACL) olmak üzere üç çeşittir.

6.2.1. Standart Erişim Kontrol Listeleri (Standard Access List)

Standart erişim kontrol listeleri gelen veya giden paketinin “IP Header” bölümüne bakarak filtreleme yapar. Bir başka deyişle sadece kaynak IP (source IP) adresine göre ağ trafiğini filtreler. Standart erişim kontrol listeleri, hedefe en yakın yönlendiricilerde oluşturulur ve 1-99 ile 1300-1999 arasında numaralandırılır. ACL oluşturmak için yönlendirici komut ekranı konfigürasyon satırında “access-list ACLno permit|deny kaynakIPAdresi” komutu yazılır. Daha sonra kuralın uygulanacağı ilgili arayüze geçiş yapılarak kuralın hangi yönde uygulanacağını belirlemek için “ip access-group ACLno in|out” komutu kullanılır.

Ankara(config)#access-list ACLno permit|deny kaynakIPAdresi

Ankara(config)#interface serial 0/0/0

Ankara(config-if)#ip access-group ACLno in|out



UYARI

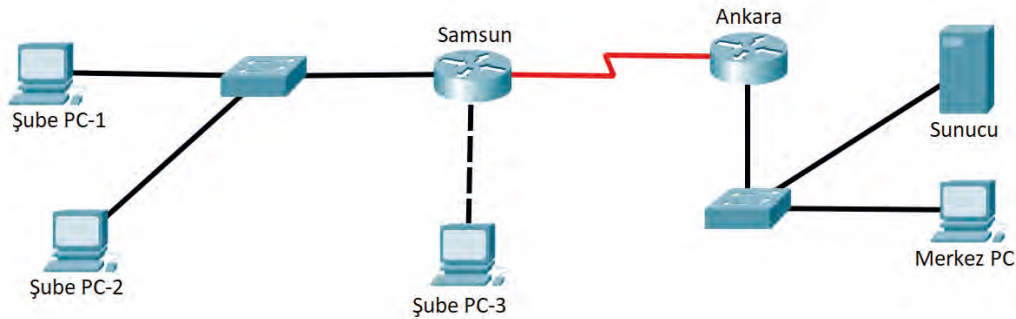
Kaynak IP adresi olarak tüm ağ yazılırsa komutun sonuna Wildcard Mask eklenir.



3. UYGULAMA

Standart ACL Uygulama

İşlem adımlarına göre Tablo 6.3'te yer alan adres bilgilerini kullanarak Ankara yönlendiricisine bağlı sunucuya Şube PC-1 ve Şube PC-3 bilgisayarları dışındaki tüm bilgisayarların ulaşmasını engelleriniz (Görsel 6.6).



Görsel 6.6: Standart ACL uygulama ağ topolojisi

Tablo 6.3: Standart ACL Uygulaması IP Adresleri

Cihaz	Arayüz	IP Adresi	Alt Ağ Maskesi	Varsayılan Ağ Geçidi
Ankara	Se0/0/0 (DCE)	23.4.192.1	255.255.255.0	
Yönlendiricisi	Gig0/1	192.168.1.1	255.255.255.0	
Samsun	Se0/0/0	23.4.192.2	255.255.255.0	
Yönlendiricisi	Gig0/0	19.5.19.19	255.255.255.0	
	Gig0/1	29.10.19.23	255.255.255.0	
Merkez PC	FastEthernet	192.168.1.2	255.255.255.0	192.168.1.1
Sunucu	FastEthernet	192.168.1.254	255.255.255.0	192.168.1.1
Şube PC-1	FastEthernet	29.10.19.24	255.255.255.0	29.10.19.23
Şube PC-2	FastEthernet	29.10.19.25	255.255.255.0	29.10.19.23
Şube PC-3	FastEthernet	19.5.19.20	255.255.255.0	19.5.19.19

1. Adım: Tablo 6.3'te ağ cihazlarının fiziksel arayüz, IP, alt ağ maskesi ve varsayılan ağ geçidi bilgileri verilmiştir. Ağ cihazlarını tabloda verilen bilgilere göre yapılandırınız. Yapılandırma sonrasında bilgisayarların sunucuya eriştiğini ping atarak gözlemleyiniz.

2. Adım: Erişim kontrol listelerini oluşturmak için gerekli komutları giriniz.

Ankara yönlendiricisi yapılandırması komut satırları:

```
Ankara(config)#access-list 1 permit 29.10.19.24
Ankara(config)#access-list 1 deny 29.10.19.0 0.0.0.255
Ankara(config)#access-list 1 permit 19.5.19.20
Ankara(config)#interface serial 0/0/0
Ankara(config-if)#ip access-group 1 in
```

3. Adım: Ankara yönlendiricisi komut ekranında “show ip access-lists” komutuyla oluşturduğunuz erişim kontrol listelerini inceleyiniz (Görsel 6.7).

```
Ankara#show ip access-lists
Standard IP access list 1
 10 permit host 29.10.19.24
 20 deny 29.10.19.0 0.0.0.255
 30 permit host 19.5.19.20
Ankara#
```

Görsel 6.7: Ankara yönlendiricisinde oluşturulan standart erişim kontrol listeleri

4. Adım: Görsel 6.6'daki ağ topolojisinde bilgisayarlardan sunucuya ping atarak oluşturduğunuz erişim kontrol listelerinin doğruluğunu test ediniz.

5. Adım: Oluşturduğunuz bir erişim kontrol listesini iptal etmek için “no Access-list ACLno” komutunu kullanınız. “show access-lists” komutuyla erişim kontrol listelerinin silindiğini kontrol ediniz.

```
Ankara(config)#no access-list 1
Ankara(config)#exit
Ankara#show access-lists
```



SIRA SİZDE

Tablo 6.3'te yer alan adres bilgilerine göre Ankara yönlendiricisine bağlı sunucuya Şube PC-1 ve Şube PC-2 dışındaki tüm bilgisayarların ulaşmasını engelleyecek şekilde erişim kontrol listelerini yapılandırınız (Görsel 6.6). Daha sonra Samsun yönlendiricisine yeni bir bilgisayar bağlayarak yapılan-
dırmanızı test ediniz.



UYARI

“no access-list x” komutu tüm listeyi silecektir. Numaralandırılmış bir erişim kontrol listesinde önceden oluşturulmuş kurallar dışında silme veya ekleme yapılamaz.

6.2.2. Genişletilmiş Erişim Kontrol Listeleri (Extended Access List)

Genişletilmiş erişim kontrol listeleri; ağ trafiğini kaynak ve hedef IP adreslerine, kaynak ve hedef portlarına (UDP, TCP) ve protokol türüne (FTP, DNS, HTTP, ICMP) göre filtreler. Bu sayede standart erişim kontrol listelerinden daha detaylı kontrol listeleri oluşturulur. Örneğin bir bilgisayarın web servislerine erişimine izin verilip FTP servisine erişimi engellenebilir. Bir başka deyişle genişletilmiş erişim kontrol listeleriyle tüm IP trafiğinin değil de belirlenen protokollerin yasaklanması sağlanır. Genişletilmiş erişim kontrol listeleri, kaynağa en yakın yönlendiricilerde oluşturulur ve 100-199 ile 2000-2699 arasında numaralandırılır. Böylece engellenmiş verinin ağ trafiğinde gereksiz yere bant genişliğini doldurmasının önüne geçilir. Genişletilmiş erişim kontrol listesi oluşturmak için yönlendirici komut ekranı konfigürasyon satırında “access-list ACLno permit|deny protokol kaynakIPAdresi hedefIPAdresi Wildcardmaskesi operatör portno” komutu yazılır. Daha sonra kuralın uygulanacağı ilgili arayüze geçiş yapılarak kuralın hangi yönde uygulanacağını belirlemek için “ip access-group ACLno in|out” komutu kullanılır.

```
Ankara(config)#access-list ACLno permit|deny protokol kaynakIPAdresi hedefIPAdresi Wildcard-  
maskesi operatör portno
```

```
Ankara(config)#interface serial 0/0/0
```

```
Ankara(config-if)#ip access-group ACLno in|out
```

Tablo 6.4: Genişletilmiş ACL Operatörleri

OPERATÖR	İŞLEV
eq	Eşittir.
gt	Büyüktür.
lt	Küçüktür.
neg	Eşit değildir.
range	Port numara sırası

Genişletilmiş erişim kontrol listelerinin yazımında operatörler, port numarası veya protokol adıyla birlikte kullanılır.



4. UYGULAMA

Genişletilmiş Erişim Kontrol Listelerini Uygulama

İşlem adımlarına göre Tablo 6.3'te yer alan adres bilgilerini kullanarak Şube PC-1 dışında 29.10.19.0 ağındaki cihazlardan Ankara yönlendiricisine bağlı sunucuyu FTP hizmetine erişimi engellecek fakat web hizmetlerine erişimi sağlanacak şekilde yapılandırınız (Görsel 6.6).

1. Adım: Tablo 6.3'te ağ cihazlarının fiziksel arayüz, IP, alt ağ maskesi ve varsayılan ağ geçidi bilgileri verilmiştir. Ağ cihazlarını tabloda verilen bilgilere göre yapılandırınız. Yapılandırma sonrasında bilgisayarların sunucudaki FTP ve web hizmetlerine eriştiğini gözlemleyiniz.

2. Adım: Genişletilmiş erişim kontrol listelerini oluşturmak için gerekli komutları giriniz.

Samsun yönlendiricisi yapılandırması komut satırları:

```
Samsun(config)#access-list 110 permit tcp host 29.10.19.24 host 192.168.1.254 eq 21
Samsun(config)#access-list 110 deny tcp 29.10.19.0 0.0.0.255 host 192.168.1.254 eq ftp
Samsun(config)#access-list 110 permit tcp 29.10.19.0 0.0.0.255 host 192.168.1.254 eq 80
Samsun (config)#interface gi0/1
Samsun(config-if)#ip access-group 110 in
```

3. Adım: Samsun yönlendiricisi komut ekranında “show ip access-lists” komutuyla oluşturduğunuz genişletilmiş erişim kontrol listelerini inceleyiniz (Görsel 6.8).

```
Samsun#sh access-lists
Extended IP access list ENGEL
 10 permit tcp host 29.10.19.24 host 192.168.1.254 eq ftp
 20 deny tcp 29.10.19.0 0.0.0.255 host 192.168.1.254 eq ftp
 30 permit tcp 29.10.19.0 0.0.0.255 host 192.168.1.254 eq www
Samsun#
```

Görsel 6.8: Samsun yönlendiricisinde oluşturulan genişletilmiş erişim kontrol listeleri

4. Adım: Görsel 6.6'da yer alan ağ topolojisindeki Şube PC-1 ve Şube PC-2 bilgisayarlarından sunucunun FTP ve web hizmetlerine erişiminin olup olmadığını kontrol ederek oluşturduğunuz erişim kontrol listelerinin doğruluğunu test ediniz (Görsel 6.9, Görsel 6.10, Görsel 6.11). Çalışmanızı kaydediniz.

```
C:\>ftp 192.168.1.254
Trying to connect...192.168.1.254
Connected to 192.168.1.254
220- Welcome to PT Ftp server
Username:MEB
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>
```

Görsel 6.9: Şube PC-1 üzerinden sunucunun FTP hizmetlerine erişimi



Görsel 6.10: Şube PC-2 üzerinden sunucunun web hizmetlerine erişimi

```
C:\>ftp 192.168.1.254
Trying to connect...192.168.1.254

%Error opening ftp://192.168.1.254/ (Timed out)
.

(Disconnecting from ftp server)
```

Görsel 6.11: Şube PC-2 üzerinden sunucunun FTP hizmetlerine erişiminin engellenmesi



SIRA SİZDE

Tablo 6.3'te yer alan adres bilgilerine göre Şube PC-1 dışında 29.10.19.0 ağındaki cihazlarda Ankara yönlendiricisine bağlı sunucunun web hizmetine erişimini engelleyecek fakat mail hizmetine erişimini sağlayacak şekilde yapılandırma işlemini gerçekleştiriniz (Görsel 6.6).

6.2.3. İsimli Erişim Kontrol Listeleri (Named Access List)

İsimli erişim kontrol listelerinin yapılandırılması, standart ve genişletilmiş erişim kontrol listelerinin yapılandırılmasıyla benzer şekildedir. İlk önce erişim listesine isim atanır sonra kurallar eklenir. Standart ve genişletilmiş erişim kontrol listelerindeki numaralar yerine bu erişim kontrol listeleri isimle tanımlandığı için akılda daha kalıcıdır. Yeni kural eklemek, oluşturulmuş bir kuralı silmek veya değiştirmek için tüm listeyi silmeden içeriğin değiştirilebilmesi, isimli kontrol listelerinin en önemli özelliğidir. İsimli erişim kontrol listeleri hem standart hem de genişletilmiş olarak oluşturulabilir.

İsimli standart erişim kontrol listesi oluşturmak için “ip access-list standard İSİM” komutu uygulanır.

```
Ankara(config)#ip access-list standart İSİM
Ankara(config-std-nacl)#deny 29.10.19.0 0.0.0.255
Ankara(config)#interface serial 0/0/0
Ankara(config-if)#ip access-group İSİM in|out
```

İsimli genişletilmiş erişim kontrol listesi oluşturmak için “ip access-list extended İSİM” komutu uygulanır.

```
Ankara(config)#ip access-list extended İSİM
Ankara(config-ext-nacl)#permit tcp host 29.10.19.24 host 192.168.1.254 eq 21
Ankara(config)#interface serial 0/0/0
Ankara(config-if)#ip access-group İSİM in|out
```

İsimli erişim kontrol listeleri yapılandırma sırasında hatalı bir satır yazıldığında başına “no” getirilerek satır iptal edilebilir.

```
Ankara(config)#ip access-list extended İSİM
Ankara(config-ext-nacl)#no permit tcp host 29.10.19.24 host 192.168.1.254 eq 21
```



UYARI

İsimli erişim kontrol listesine kural eklemek için oluşturulan kontrol listelerinin satır numaralarını bilmek gerekir. İsimli erişim kontrol listelerine yeni kurallar boş satır numaralarına atanarak eklenir. show access-lists komutuyla oluşturulan listeler ve satır numaraları görülebilir.



5. UYGULAMA

İsimli Erişim Kontrol Listelerini Uygulama

İşlem adımlarına göre dördüncü uygulamada oluşturduğunuz genişletilmiş erişim kontrol listelerini isimli erişim listesi olarak yeniden oluşturduktan sonra Şube PC-3'ün web hizmetlerine erişimini engelleyecek kuralı ekleyiniz ve daha önce oluşturduğunuz FTP kuralını kaldırınız.

1. Adım: Bir önceki uygulamada kaydettiğiniz çalışmayı açınız ve oluşturduğunuz genişletilmiş erişim kontrol listelerini silmek için gerekli komutları giriniz.

Samsun yönlendiricisi yapılandırması komut satırları:

```
Samsun>en
Samsun#conf t
Samsun(config)#no access-list 110
```

2. Adım: İsimli genişletilmiş erişim kontrol listelerini oluşturmak için gerekli komutları giriniz.

Samsun yönlendiricisi yapılandırması komut satırları:

```
Samsun(config)#ip access-list extended ENGEL
Samsun(config-ext-nacl)#permit tcp host 29.10.19.24 host 192.168.1.254 eq 21
Samsun(config-ext-nacl)#deny tcp 29.10.19.0 0.0.0.255 host 192.168.1.254 eq ftp
Samsun(config-ext-nacl)#permit tcp 29.10.19.0 0.0.0.255 host 192.168.1.254 eq 80
Samsun(config-ext-nacl)#exit
```

Samsun (config)#interface gi0/1
 Samsun(config-if)#ip access-group ENGEL in

3. Adım: Şube PC-3'ün web hizmetlerine erişimini engelleyecek kuralı eklemek için gerekli komutları giriniz.

Samsun yönlendiricisi yapılandırma komut satırları:

Samsun(config)#show access-lists

```
Samsun#sh access-lists
Extended IP access list ENGEL
 10 permit tcp host 29.10.19.24 host 192.168.1.254 eq ftp
 20 deny tcp 29.10.19.0 0.0.0.255 host 192.168.1.254 eq ftp
 30 permit tcp 29.10.19.0 0.0.0.255 host 192.168.1.254 eq www
Samsun#
```

Görsel 6.12: İsimli genişletilmiş erişim listesi

Samsun(config)#ip access-list extended ENGEL
 Samsun(config-ext-nacl)#25 deny tcp host 19.5.19.20 host 192.168.1.254 eq 80

4. Adım: İsimli genişletilmiş erişim listesine eklediğiniz kuralı görmek için gerekli komutu giriniz ve Görsel 6.13'teki kural listesini gözlemleyiniz.

Samsun(config-ext-nacl)#do sh access-lists

```
Samsun(config-ext-nacl)#do sh access-lists
Extended IP access list ENGEL
 10 permit tcp host 29.10.19.24 host 192.168.1.254 eq ftp
 20 deny tcp 29.10.19.0 0.0.0.255 host 192.168.1.254 eq ftp
 25 deny tcp host 19.5.19.20 host 192.168.1.254 eq www
 30 permit tcp 29.10.19.0 0.0.0.255 host 192.168.1.254 eq www
Samsun(config-ext-nacl)#
```

Görsel 6.13: İsimli genişletilmiş erişim listesine eklenen kural satırı

5. Adım: Daha önce oluşturduğunuz FTP kuralını kaldırmak için gerekli komutları giriniz.

Samsun yönlendiricisi yapılandırma komut satırları:

Samsun(config)#ip access-list extended ENGEL
 Samsun(config-ext-nacl)#no 20 deny tcp 29.10.19.0 0.0.0.255 host 192.168.1.254 eq ftp

6. Adım: İsimli genişletilmiş erişim listesinden kaldırılan kuralı görmek için gerekli komutu giriniz ve Görsel 6.14'teki kural listesini gözlemleyiniz.

Samsun(config-ext-nacl)#do sh access-lists

```
Samsun(config-ext-nacl)#do sh access-lists
Extended IP access list ENGEL
 10 permit tcp host 29.10.19.24 host 192.168.1.254 eq ftp
 25 deny tcp host 19.5.19.20 host 192.168.1.254 eq www
 30 permit tcp 29.10.19.0 0.0.0.255 host 192.168.1.254 eq www
Samsun(config-ext-nacl)#
```

Görsel 6.14: İsimli genişletilmiş erişim listesi



SIRA SİZDE

Tablo 6.3'te yer alan adres bilgilerine göre Şube PC-3 dışındaki bilgisayarların Ankara yönlendircisine ping isteklerini engelleyecek şekilde isimli genişletilmiş kontrol listesini oluşturunuz. Oluşturduğunuz listeyi Şube PC-1 erişecek şekilde güncelleyiniz (Görsel 6.6).

6.3. AĞ GÜVENLİĞİ VE AĞ İZLEME

6.3.1. Ağ İzleme Yazılımı

Ağda gerçekleşen trafik denetlenebilir ve izlenebilir. Bu işlem için Wireshark, Sguil, Kibana vb. bazı programlar kullanılabilir.



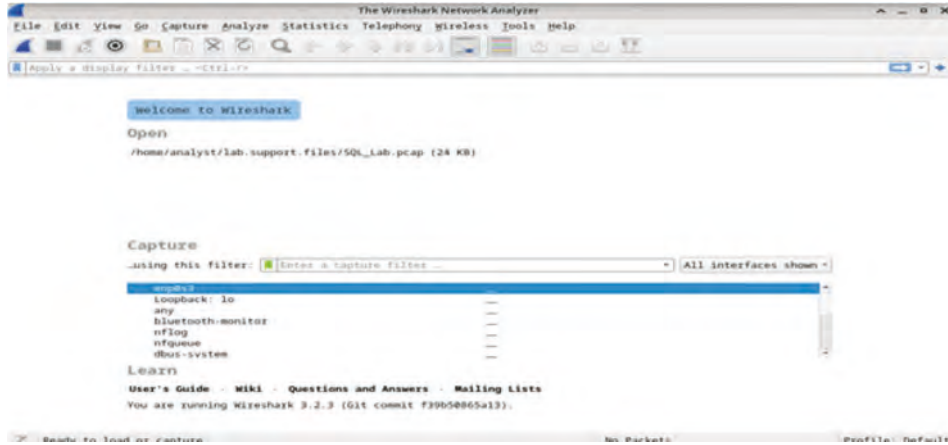
6. UYGULAMA

Wireshark Kullanarak Ağ İzleme ve Analiz Etme

İşlem adımlarına göre Wireshark kullanarak ağ izleyiniz ve analiz ediniz.

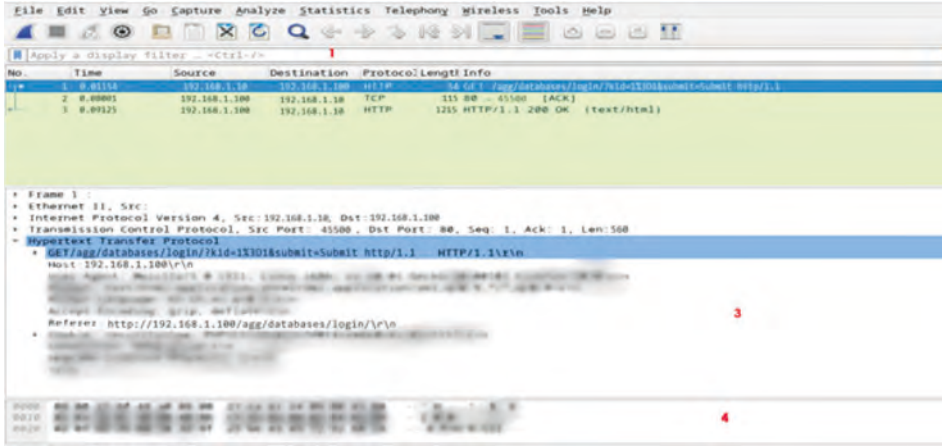
1. Adım: wireshark.org sitesinden işletim sisteminize uygun Wireshark sürümünü bilgisayarınıza indirip kurunuz.

2. Adım: Kurulumu yaptıktan sonra Wireshark programını açarak Görsel 6.15'teki ekranı görünüz.



Görsel 6.15: Wireshark programı

3. Adım: Bu pencerede üstteki Capture  düğmesine basarak ağın izlenmesini başlatınız (Görsel 6.16).



Görsel 6.16: Wireshark ekranı

Bu pencerede 1 numaralı alandan izlenmiş trafik içeriğini filtreleyebilirsiniz. 2 numaralı alan, izlenmiş trafikte gerçekleşmiş eylemlerin listelendiği kısımdır. 3 numaralı alan, 2 numaralı alandan seçilen bir eylemin detaylandırıldığı bölümdür. 4 numaralı alan ise 3 numaralı alandan seçilen bir detayın daha da detaylandırıldığı kısımdır.

4. Adım: Görsel 6.17'deki örnek izlemede 2 numaralı alanı inceleyiniz. 13. satırda 10.0.2.4 IP'li bilgisayardan 10.0.2.15 IP'li bilgisayara bir HTTP GET işleminin yapıldığı görülür (*GET/dwva/vulnerabilities/sqli/?id=1%3D1&submit=Submit http/1.1*).

10	0.015485	10.0.2.4	10.0.2.15	TCP	66	35614 → 80 [ACK] Seq=1019 Ack=3406 Win=3648 Len=0 TSval=45843 TSecr=98
11	0.068625	10.0.2.4	10.0.2.15	HTTP	429	GET /dwva/dwva/css/main.css HTTP/1.1
12	0.070400	10.0.2.15	10.0.2.4	HTTP	1511	HTTP/1.1 200 OK (text/css)
13	174.254430	10.0.2.4	10.0.2.15	HTTP	536	GET /dwva/vulnerabilities/sqli/?id=1%3D1&submit=Submit HTTP/1.1
14	174.254581	10.0.2.15	10.0.2.4	TCP	66	80 → 35618 [ACK] Seq=1 Ack=471 Win=235 Len=0 TSval=82101 TSecr=98
15	174.257989	10.0.2.15	10.0.2.4	HTTP	1801	HTTP/1.1 200 OK (text/html)
16	220.490531	10.0.2.4	10.0.2.15	HTTP	577	GET /dwva/vulnerabilities/sqli/?id=1%3D1&submit=Submit HTTP/1.1
17	220.490637	10.0.2.15	10.0.2.4	TCP	66	80 → 35640 [ACK] Seq=1 Ack=512 Win=235 Len=0 TSval=93660 TSecr=11
18	220.493085	10.0.2.15	10.0.2.4	HTTP	1918	HTTP/1.1 200 OK (text/html)

Görsel 6.17: HTTP GET işlemi

5. Adım: 3 numaralı alandan HTTP GET isteğinin detayını görüntüleyiniz. Bu kısımdan Hypertext Transfer Protocol başlığını inceleyiniz. Görsel 6.18'de /agg/databases/login/ adresine kid isminde, 1=1 şeklinde bir değer gönderilir. Gönderilen bu değer, kullanıcı giriş sayfasını atlatmak için yapılan bir sql injection saldırısıdır.



Görsel 6.18: Hypertext Transfer Protocol detayı

6. Adım: 2 numaralı alandaki 1.satırın üzerindeyken sağ tuşa bastığınızda açılan menüden Follow > Http Stream komutuna tıklayınız. Açılan pencerede mavi ve kırmızı ile yazılmış alanlar görülür. Kırmızı yazılı alanlar bilgisayarınızdan karşı bilgisayara gönderilen veriler, mavi yazılı alanlar ise karşı bilgisayardan bilgisayarınıza gelen cevaplardır. Görsel 6.19'daki HTTP GET isteğine http/1.1 200 OK ile olumlu cevap verildiğini gözlemleyiniz.

```
GET /dvwa/vulnerabilities/sqli/?id=1%3D&Submit=Submit HTTP/1.1
Host: 10.0.2.15
User-Agent: Mozilla/5.0 (X11; Linux i686; rv:50.0) Gecko/20100101 Firefox/50.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.0.2.15/dvwa/vulnerabilities/sqli/
Cookie: security=low; PHPSESSID=ml2n7d0t4rem6k0n4is02u5157
Connection: keep-alive
Upgrade-Insecure-Requests: 1

HTTP/1.1 200 OK
Date: Mon, 06 Feb 2017 14:18:22 GMT
Server: Apache/2.4.18 (Ubuntu)
Expires: Tue, 23 Jun 2009 12:00:00 GMT
Cache-Control: no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 1443
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=utf-8

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">

1 client pkt, 1 server pkt, 1 turn.
```

Görsel 6.19: HTTP GET isteği ve cevabı

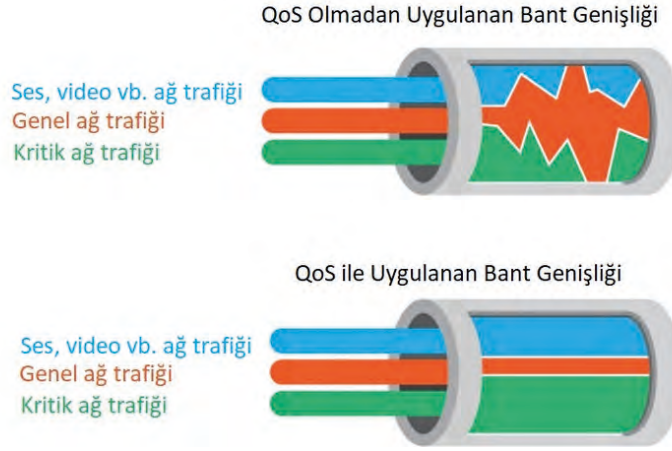


SIRA SİZDE

BT laboratuvarınızın ağını inceleyiniz.

6.3.2. Servis Kalitesi (QoS)

Servis kalitesi (Quality of Service-QoS), ağlarda veri aktarımları esnasında çalışan protokolleri belirli kurallar çerçevesinde öncelik sıralaması yaparak ağda oluşabilecek sorunları azaltmaya çalışan ağ servisi türüdür. Dosya indirme, sesli ve canlı video yayınları gibi uygulamaların çalışmalarını belirli önceliklere göre düzenleyerek ağ trafiğinde oluşabilecek tıkanıklığı azaltmayı amaçlar. Ağ trafiğinin hacmi ağın bant genişliğinin üstünde olduğunda ağ cihazları bu veri paketlerini sıralar. Kuyruğa eklenecek paketlerin sayısı artmaya devam ederse bir süre sonra ağ cihazının belleği dolar ve paketler düşer. Böylece veri ve zaman kayıpları ortaya çıkar. QoS sayesinde kesinti veya paket gecikmesinden etkilenen uygulamalara öncelik sağlanır. Örneğin trafikte ambulans, itfaiye gibi araçların geçiş üstünlüğü vardır. Ağlarda da bazı uygulamaların benzer şekilde öncelik hakkı vardır (Görsel 6.20).



Görsel 6.20: QoS ile bant genişliği

Ağ üzerinde veriler bir cihazdan diğerine TCP veya UDP protokollerinden biri kullanılarak iletilir. Bu iki protokolün arasındaki temel fark, TCP aracılığıyla iletilen verilerde kaybedilen paketlerin yeniden iletilmesidir. Dosya, web sayfası gibi aktarımlarda TCP paketleri kullanılır. UDP paketlerinde ise herhangi bir kayıp olursa paketler yeniden iletilmez. Bunun sebebi, paketlerin sıralı bir akışta olması ve kaybedilen paketin sırası geçtiği için tekrar kullanılamamasıdır. Ses, video gibi aktarımlarda UDP paketleri kullanılır. Ses ve video gibi aktarımlar esnasında paketlerin kaybedilmesi, bu hizmetlerin kalitesinin düşük olmasına ve anlaşılabilir hâle gelmesine yol açar. Ayrıca bu uygulamalardaki gecikmeler de servis kalitesini bozar.

Servis kalitesinin faydaları şunlardır:

- Ağ kaynakları üzerinde kontrol imkânı sağlar.
- Kritik görev ve zaman hassasiyetine sahip uygulamaların yeterli kaynağa sahip olmasını sağlar.
- Kaynakların verimli kullanımını sağlar.
- Bant genişliğinin verimli kullanımını sağlar.

6.3.3. Ağ Sorunları

Ağ bağlantısında kullanıcı, sistem veya altyapı hatalarından dolayı çeşitli sorunlarla karşılaşılabilir. Bu sorunların sebepleri tam olarak tespit edilemese de çözüm için yapılması gerekenleri belirlemeye yardımcı olabilecek çeşitli yöntemler vardır.

6.3.3.1. Fiziksel Bağlantının Testi

Fiziksel bağlantı testinde genellikle ping veya tracert komutları kullanılır.

- **ping:** ICMP protokolü ile bağlantının test edilmesinde kullanılır. Bu komut, kaynaktan hedefe ICMP yankı isteği gönderir. Hedeften ICMP yankı cevabı gelirse bağlantı sağlamdır. Komut ekranında “ping hedef IP adresi” şeklinde yazılır.

Bu komutta hedef IP adresi olarak varsayılan ağ geçidinin IP adresi girilir. İşlem başarılı ise yönlendiriciye veya modeme kadar bağlantı ve yapılandırmalarda (kablolu veya kablosuz) sorun bulunmaz. Test başarısız ise bağlantılarda veya TCP/IP yapılandırmalarında sorun olabilir. Sorunun giderilmesi için varsa kablo bağlantısı kontrol edilir. Cihazın IP adresi, alt ağ maskesi ve varsayılan ağ geçidi ayarları kontrol edilmelidir.

Hedef IP adresi olarak ping komutunda uzak bir cihazın IP veya web adresi girilir. İşlem başarılı olursa bu yolda herhangi bir sorun yok demektir. İşlem başarısız olursa kendi ağ geçidine ping atılmalıdır. Kendi ağ geçidine atılan ping başarılı olursa modem veya yönlendirici ayarları kontrol edilmelidir.



UYARI

Bazı web sayfaları ve yönlendiriciler ICMP mesajlarını engeller. Bu durumda ping komutu başarısızlıkla sonuçlanır.

- **tracert:** ICMP protokolü ile bağlantının uçtan uca test edilmesinde kullanılır. Hedef IP adresine giderken geçilen yönlendirici IP adresleri ve gecikme süreleri bu komutla görüntülenir. Komut ekranında “tracert hedef IP adresi” şeklinde yazılır.

Hedefe giderken bir yönlendiricide bağlantı kesilirse o yönlendiricinin yapılandırılması ve bağlantıları kontrol edilmelidir.

6.3.3.2. Alan Adı Çözümleme Testi

DNS sunucusuna ulaşamaması, WAN ağlarında en çok karşılaşılan sorunlardan biridir. DNS sunucusuna ulaşmayınca uygulama katmanı protokollerinin birçoğu çalışmaz. Cihazın DNS ayarları doğruysa ve DNS sunucularında sorun yoksa hedef IP adresleri yerine web sayfası alan adları kullanılabilir. Web sayfalarına erişimde hata alınıyorsa cihazın TCP/IP bilgileri yapılandırılırken girilen DNS adresi kontrol edilmelidir. Gerekirse farklı bir DNS sunucusunun adresi denenmelidir. Kullanılan cihaza modem veya yönlendirici aracılığıyla DHCP havuzundan otomatik IP bilgileri atanıyorsa bu bilgiler kontrol edilmelidir.

6.3.3.3. Yönlendirici Yapılandırma Sorunları

Yönlendirici yapılandırma sorunları, rota hataları ve güvenlik hataları olmak üzere ikiye ayrılır.

- **Rota Hataları:** Yönlendiriciler yapılandırılırken girilen yönlendirme rotalarının bilgileri kontrol edilmelidir. Yönlendirme tabloları incelendiğinde ulaşamayan yönlendirici tabloda bulunmuyorsa o yönlendiriciye uygun bir rota yazılarak sorun giderilir.

- **Güvenlik Hataları:** Ağ trafiğini engelleyen erişim kontrol listesi yazılmış olabilir. Yönlendiricideki erişim kontrol listeleri görüntülenerek incelenir. İzin verilmesi gereken bir trafik yanlışlıkla engellenmiş (deny) veya yanlış arayüze uygulanmış olabilir. Yanlış yazılmış ACL, yönlendiriciden silinerek sorun giderilir.



ÖLÇME VE DEĞERLENDİRME

Aşağıdaki soruları dikkatlice okuyarak doğru seçeneği işaretleyiniz.

1. Kimlik doğrulama ile bağlantı kuran kapsülleme protokolü aşağıdakilerden hangisidir?
 - A) DTE
 - B) Frame Relay
 - C) HDLC
 - D) PPP
 - E) X.25
2. Aşağıdakilerden hangisi CHAP kimlik doğrulamasının avantajlarından biri değildir?
 - A) Üç yönlü el sıkışma yapılır.
 - B) Kullanıcı adı ve parolası md5 şifrelemesi ile gönderilir.
 - C) Kimlik denetimi belli aralıklarla tekrar edilir.
 - D) Şifrelerin aynı olma zorunluluğu vardır.
 - E) İki yönlü el sıkışma vardır.
3. Herhangi bir web adresine ping atılmazken aynı web sitesinin IP adresine ping atılabiliyorsa karşılaşılan sorun aşağıdakilerden hangisidir?
 - A) Alt ağ maskesi yanlış yapılandırılmıştır.
 - B) Bilgisayar IP adresi yanlış yapılandırılmıştır.
 - C) DNS adresi yanlış yapılandırılmıştır.
 - D) Varsayılan ağ geçidi yanlış yapılandırılmıştır.
 - E) Yönlendirici IP adresi yanlış yapılandırılmıştır.
4. Standart erişim kontrol listelerinin numara aralığı aşağıdakilerden hangisidir?
 - A) 1-99
 - B) 100-199
 - C) 200-299
 - D) 1999-2999
 - E) 3000-3999
5. Aşağıdakilerden hangisi servis kalitesinin (QoS) faydalarından biri değildir?
 - A) Ağ kaynakları üzerinde kontrol imkânı sağlar.
 - B) Bant genişliğinin eşit dağılımını sağlar.
 - C) Kritik uygulamaların yeterli kaynağa sahip olmasını sağlar.
 - D) Kaynakların verimli şekilde kullanımını sağlar.
 - E) Bant genişliğinin verimli kullanımını sağlar.

- ## ANAHTAR KELİMELER

7. ÖĞRENME BİRİMİ

GÜVENLİK DUVARI TEKNOLOJİLERİ

NELER ÖĞRENECEKSİNİZ?

- Güvenlik duvarı teknolojileri
- IDS/IPS sistemleri
- IDS ayarları
- IPS ayarları



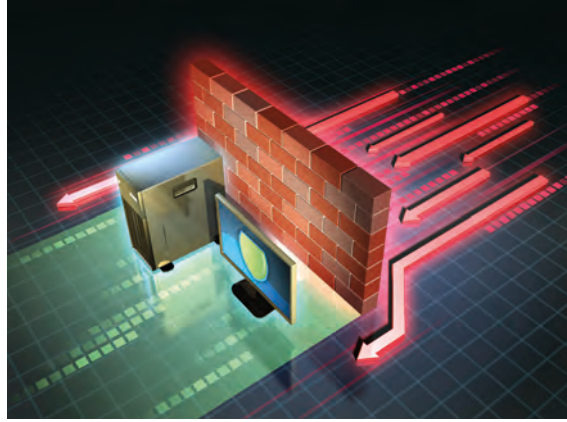


HAZIRLIK ÇALIŞMALARI

1. Evinizi dışarıdan gelebilecek tehditlere karşı korumak için nasıl önlemler alırsınız?
2. Karşılaştığınız bir kişiyi nasıl tanırırsınız? Düşüncelerinizi arkadaşlarınızla paylaşınız.

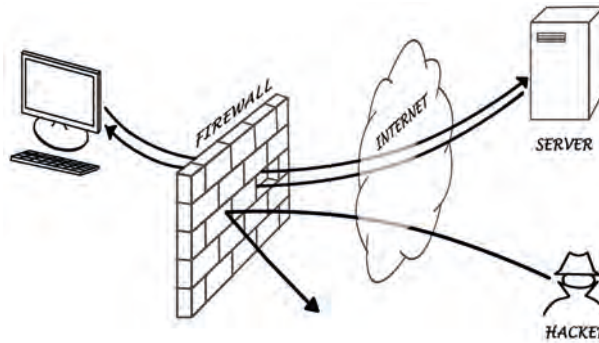
7.1. GÜVENLİK DUVARI

Güvenlik duvarı (firewall) teknolojileri, ağ güvenliğini sağlamaya çalışan yazılım veya donanım tabanlı sistemlerdir. Güvenlik duvarı ile ağın gelen ve giden tüm trafiğinde kontrol sağlanır ve saldırı amaçlı olanlar tespit edilerek saldırının engellenmesi hedeflenir (Görsel 7.1).



Görsel 7.1: Güvenlik duvarı

Güvenlik duvarı; ağ trafiğini belirlenmiş kurallara, protokollere ve imzalara göre filtreler. Bu kurallar, protokoller ve imzalar düzenli bir şekilde güncellenmelidir. Güvenlik duvarı sadece bir cihazı denetlemek için kurulabileceği gibi yerel ağı denetlemek için de kullanılabilir. Genellikle işletim sistemleri ve antivirüs programları, ağı denetlemek için yazılım tabanlı güvenlik duvarını kullanır. Ev veya küçük ölçekli işletmelerde kullanılan modem veya yönlendirici gibi cihazların güvenlik duvarı yapılandırması mevcuttur. Büyük iş yerleri ve kurumlarda saldırılara daha çok maruz kalınması, ağ trafiğinin yoğunluğu sebebiyle donanım tabanlı güvenlik duvarı cihazları kullanılır (Görsel 7.2).



Görsel 7.2: Güvenlik duvarı örneği

Ağ içinde gerçekleşen saldırıları tespit etmek ve engellemek için IDS (Intrusion Detection Systems-Saldırı Tespit Sistemi) ve IPS (Intrusion Prevention Systems-Saldırı Önleme Sistemi) kullanılır. Bu sistemler, ağ ve siber güvenlik uzmanları için tasarlanan yazılım ve donanım tabanlı güvenlik sistemleridir. IDS/IPS, donanım tabanlı olarak haricî cihazlar ile kullanılabileceği gibi yönlendiricilere ek güvenlik yazılımları yüklenerek de kullanılabilir. Donanım tabanlı cihazlara IPS/IDS sensör adı verilir. Donanım tabanlı cihazlar yüksek fiyatlı oldukları için daha çok kurumsal ve büyük işletmeler tarafından tercih edilir (Görsel 7.3).



Görsel 7.3: IPS/IDS sensör cihazları

IDS/IPS'nin firewall sistemlerde bütünleşik olarak kullanılması tercih edilir. Doğru bir şekilde ayarlanmış (konfigürasyonu yapılmış) IDS/IPS; ciddi tehlike ve zararlara yol açabilecek saldırıların tespitinde, yakalanmasında ve önlenmesinde önemlidir. Bu sistemler, ağ ve siber güvenlik uzmanları için tasarlanmıştır.

IDS/IPS'nin genel özellikleri şunlardır:

- Saldırı anında uyarı verme
- Ağ veya güvenlik uzmanına uyarı verme
- Zararlı olarak tespit edilen paketlerin bırakılması
- Saldırı amaçlı bağlantı kaynaklarının kesilmesi
- Kullanıcı veya yazılım kaynaklı saldırıların tespiti
- Adli kayıtların tutulması
- Zararlı kodların tespiti

7.2. IDS YAPILANDIRMA

IDS (Intrusion Detection Systems-Saldırı Tespit Sistemi), belirlenmiş kurallar ve daha önce tespit edilmiş saldırı imzalarına göre ağ trafiğini inceler. IDS herhangi bir eşleşme tespit ederse bunu günlüğe kaydeder ve ağ yöneticisine bildirir. IDS, tespit ettiği bu saldırıya herhangi bir işlem yapmaz. Dolayısıyla saldırının gerçekleşmesini engellemez. Saldırıya karşı gereken önlemleri ağ yöneticisi almalıdır. Ağ trafiğinin kopyası alınarak analiz işlemi yapıldığı için ağ trafiği etkilenmez. IDS, ağa dâhil olmadan pasif izleme yapan yardımcı cihaz görevini üstlenir.

7.3. IPS YAPILANDIRMA

IPS (Intrusion Prevention Systems-Saldırı Önleme Sistemi), IDS'den farklı olarak ağ trafiği engelleyebilir veya veri paketlerini düşürür (Tablo 7.1). IPS teknolojisi, IDS teknolojisinin üzerine inşa edilmiştir. IPS, etkin bir şekilde ağa dâhildir. IPS; saldırı veya kötü niyetli verileri tespit için imza tabanlı algılama, belirlenmiş kurallara göre engelleme ve protokol analizi yapar. Analiz işlemi süresince paketlerin geçişine izin verilmediği için ağ trafiği yavaşlar. İmza tabanlı algılama için güncel imza dosyaları, cihaz üreticisinden veya anlaşma yapılan firmaların web sayfalarından kullanıcı adı ve şifresiyle indirilebilir.

Tablo 7.1: IDS ve IPS'nin Karşılaştırılması

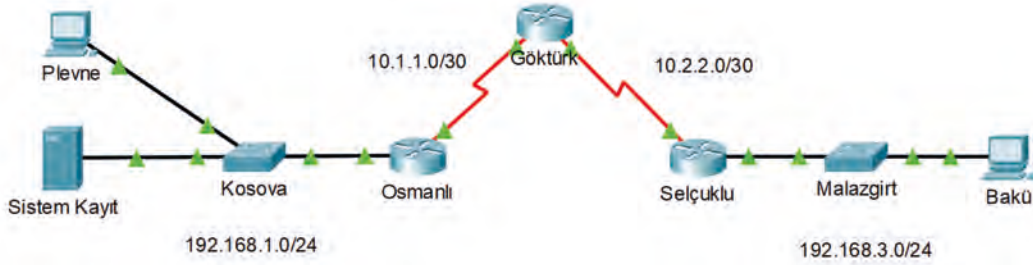
IDS	IPS
Avantajları	Avantajları
Ağa etkisi yoktur.	Saldırıları engeller.
Sensör kapanırsa ağa etki etmez.	Normalizasyon tekniklerini kullanır.
Sensör dolarsa ağa etki etmez.	Kurallara göre kendi müdahale eder.
Dezavantajları	Dezavantajları
Saldırıları engellemez.	Ağ trafiğini geciktirir.
Önlemleri ağ yöneticisi almalıdır.	IPS sensör taşarsa ağ etkilenir.



1. UYGULAMA

IPS Yapılandırma

Görsel 7.4'te verilen ağ topolojisini Tablo 7.2'deki IP adreslerine göre yapılandırınız. İşlem adımlarına göre Osmanlı yönlendiricisine dışarıdan gelen saldırılara karşı IPS yapılandırmasını yapınız.



Görsel 7.4: IPS/IDS yapılandırma ağ topolojisi

Tablo 7.2: IPS/IDS Yapılandırma Uygulaması IP Adresleri

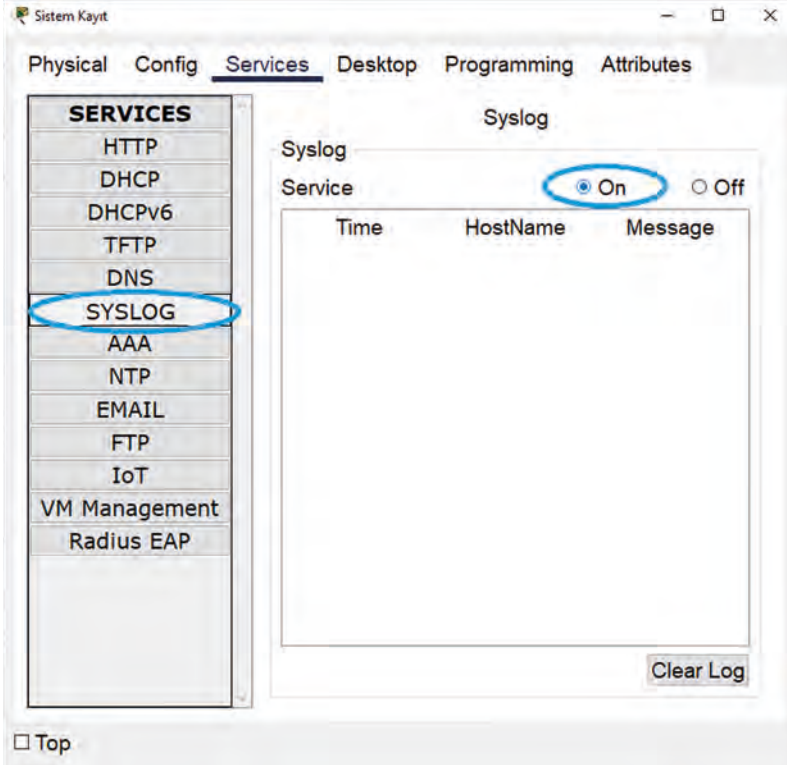
Cihaz	Arayüz	IP Adresi	Alt Ağ Maskesi	Varsayılan Ağ Geçidi
Göktürk Yönlendiricisi	Se0/0/0 (DCE)	10.1.1.2	255.255.255.252	
	Se0/0/1 (DCE)	10.2.2.2	255.255.255.252	
Selçuklu Yönlendiricisi	Gig0/1	192.168.3.1	255.255.255.0	
	Se0/0/0	10.2.2.1	255.255.255.252	
Osmanlı Yönlendiricisi	Se0/0/0	10.1.1.1	255.255.255.252	
	Gig0/1	192.168.1.1	255.255.255.0	
Plevne	FastEthernet	192.168.1.2	255.255.255.0	192.168.1.1
Bakü	FastEthernet	192.168.3.2	255.255.255.0	192.168.3.1
Sunucu (Sistem Kayıt)	FastEthernet	192.168.1.50	255.255.255.0	192.168.1.1

1. Adım: Görsel 7.4'te verilen ağ topolojisini simülasyon programında hazırlayınız.

2. Adım: Yönlendiricilerin ve bilgisayarların IP adreslerini Tablo 7.2'ye göre yapılandırınız.

3. Adım: Yönlendiricileri dinamik yönlendirme protokollerinden birine göre (OSPF, RIP, EIGRP) yapılandırınız.

- 4. Adım:** Bakü bilgisayarından Plevne bilgisayarına ping atıp ulaştığını gözlemleyiniz.
- 5. Adım:** Plevne bilgisayarından Bakü bilgisayarına ping atıp ulaştığını gözlemleyiniz.
- 6. Adım:** Sunucu bilgisayarda sistem kayıtlarının tutulabilmesi için “SYSLOG” servisini aktifleştiriniz (Görsel 7.5).



Görsel 7.5: SYSLOG aktifleştirme

7. Adım: Osmanlı yönlendiricisinde versiyon bilgilerini görmek ve güvenlik paketi lisans bilgilerini etkinleştirmek için gerekli komutları uygulayınız.

`Osmanli#show version` komutuyla yönlendiricinin versiyon bilgisinden güvenlik paketi lisans bilgilerini kontrol ediniz (Görsel 7.6).

```
Technology Package License Information for Module:'c1900'
-----
Technology      Technology-package      Technology-package
Current         Type                    Next reboot
-----
ipbase          ipbasek9                Permanent          ipbasek9
security        disable                  None                disable
data            disable                  None                None
Configuration register is 0x2102
Osmanli#
```

↓
Güvenlik paketi etkin değil

Görsel 7.6: Güvenlik paketi lisans bilgileri

Osmanli#conf t komutuyla global konfigürasyon moduna geçiniz.

Osmanli(config)#license boot module c1900 technology-package securityk9 komutuyla yönlendiricinin güvenlik paketini etkinleştiriniz. Ekrana gelen sözleşmeyi kabul ediniz.

Osmanli(config)#do write komutuyla yaptığınız işlemleri kaydediniz.

Osmanli(config)#do reload komutuyla yönlendiriciyi yeniden yükleyiniz.

Osmanli#show version komutuyla yönlendiricinin versiyon bilgisinden güvenlik paketi lisans bilgilerinin etkinleştirildiğini kontrol ediniz (Görsel 7.7).

```
Technology Package License Information for Module:'c1900'
-----
Technology      Technology-package      Technology-package
Current          Type                    Next reboot
-----
ipbase          ipbasek9                ipbasek9
security        securityk9              securityk9
data            disable                 None
Configuration register is 0x2102
Osmanli#
```

Görsel 7.7: Güvenlik paketi lisans bilgileri

8. Adım: IPS/IDS temel yapılandırması için gerekli komutları uygulayınız (Görsel 7.8).

Osmanli#mkdir ips-ids komutuyla yönlendiricide “ips-ids” adıyla bir klasör oluşturunuz.

Osmanli#show flash: komutuyla oluşturduğunuz klasörü kontrol ediniz.

```
Osmanli#mkdir ips-ids
Create directory filename [ips-ids]?
Created dir flash:ips-ids

Osmanli#show flash:

System flash directory:
File Length Name/status
  3 33591768 c1900-universalk9-mz.SPA.151-4.M4.bin
  6 0 ips-ids
  2 28282 sigdef-category.xml
  1 227537 sigdef-default.xml
[33847587 bytes used, 221896413 available, 255744000 total]
249856K bytes of processor board System flash (Read/Write)
```

Görsel 7.8: Klasör oluşturma ve görüntüleme

Osmanli#conf t komutuyla global konfigürasyon moduna geçiniz.

Osmanli(config)#ip ips config location flash:ips-ids komutuyla IPS/IDS imza dosyalarının depolanacağı klasörü belirleyiniz.

Osmanli(config)#ip ips name hisar komutuyla IPS/IDS kurallarını adlandırınız.

Osmanli(config)#ip ips notify log komutuyla kayıt tutma işlemini etkinleştiriniz.

Osmanli(config)#service timestamps log datetime msec komutuyla tutulan kayıtlara zaman damgası eklenmesini sağlayınız.

Osmanli(config)#logging host 192.168.1.50 komutuyla kayıtların sistem kayıt sunucusuna kaydedilmesini sağlayınız.



UYARI

Zaman damgasında saat ve tarihin doğru yapılandırıldığını kontrol ediniz. Saat ve tarih hatalı ise ayrıcalıklı kullanıcı modunda “clock set saat tarih” komutuyla saat ve tarihi düzeltiniz.

Osmanli# clock set 09:05 10 Nov 1938

9. Adım: IPS/IDS imza kategorilerini kullanabilmek ve yapılandırmak için gerekli komutları uygulayınız (Görsel 7.9).

```
Osmanli(config)#ip ips signature-category
Osmanli(config-ips-category)#category all
Osmanli(config-ips-category-action)#retired true
Osmanli(config-ips-category-action)#exit
Osmanli(config-ips-category)#category ios_ips basic
Osmanli(config-ips-category-action)#retired false
Osmanli(config-ips-category-action)# exit
Osmanli(config-ips-category)# exit
```

Do you want to accept these changes? [confirm] “enter” komutuyla değişiklikleri onaylayınız.

```
Osmanli(config)#ip ips signature-category
Osmanli(config-ips-category)#category all
Osmanli(config-ips-category-action)#retired true
Osmanli(config-ips-category-action)#exit
Osmanli(config-ips-category)#category ios_ips basic
Osmanli(config-ips-category-action)#retired false
Osmanli(config-ips-category-action)#exit
Osmanli(config-ips-category)#exit
Do you want to accept these changes? [confirm]
Applying Category configuration to signatures ...
%IPS-6-ENGINE_BUILDING: atomic-ip - 288 signatures - 6 of 13
engines
%IPS-6-ENGINE_READY: atomic-ip - build time 30 ms - packets
for this engine will be scanned
Osmanli(config)#
```

Görsel 7.9: IPS/IDS imza kategorilerini kullanıma açma

10. Adım: IPS/IDS kuralını arayüze uygulamak için gerekli komutları kullanınız (Görsel 7.10).

Osmanli(config)#interface gigabitEthernet 0/1 komutuyla kuralın uygulanacağı arayüze geçiş yapınız.

Osmanli(config-if)#ip ips hisar out komutuyla IPS/IDS kuralını çıkış yönünde etkinleştiriniz.

```
Osmanli(config)#interface gigabitEthernet 0/1
Osmanli(config-if)#ip ips hisar out
Osmanli(config-if)#
*Mar 10, 13:17:18.1717: %IPS-6-ENGINE_BUILDS_STARTED:
13:17:18 UTC Mar 10 2021
*Mar 10, 13:17:18.1717: %IPS-6-ENGINE_BUILDING: atomic-ip - 3
signatures - 1 of 13 engines
*Mar 10, 13:17:18.1717: %IPS-6-ENGINE_READY: atomic-ip -
build time 8 ms - packets for this engine will be scanned
*Mar 10, 13:17:18.1717: %IPS-6-ALL_ENGINE_BUILDS_COMPLETE:
elapsed time 8 ms
Osmanli(config-if)#
```

Görsel 7.10: IPS/IDS imza kategorilerini kullanıma açma

11. Adım: IPS/IDS imza kuralının eylemini belirlemek için gerekli komutları kullanınız (Görsel 7.11).

```
Osmanli(config)#ip ips signature-definition
Osmanli(config-sigdef)#signature 2004 0
Osmanli(config-sigdef-sig)#status
Osmanli(config-sigdef-sig-status)#retired false
Osmanli(config-sigdef-sig-status)#enabled true
Osmanli(config-sigdef-sig-status)#exit
Osmanli(config-sigdef-sig)#engine
Osmanli(config-sigdef-sig-engine)#engine
Osmanli(config-sigdef-sig-engine)#event-action produce-alert
Osmanli(config-sigdef-sig-engine)#event-action deny-packet-inline
Osmanli(config-sigdef-sig-engine)#exit
Osmanli(config-sigdef-sig)#exit
Osmanli(config-sigdef-sig)#exit
Osmanli(config-sigdef)#exit
```

Do you want to accept these changes? [confirm] “enter” komutuyla değişiklikleri onaylayınız.

```
Osmanli(config)#ip ips signature-definition
Osmanli(config-sigdef)#signature 2004 0
Osmanli(config-sigdef-sig)#status
Osmanli(config-sigdef-sig-status)#retired false
Osmanli(config-sigdef-sig-status)#enabled true
Osmanli(config-sigdef-sig-status)#exit
Osmanli(config-sigdef-sig)#engine
Osmanli(config-sigdef-sig-engine)#event-action produce-alert
Osmanli(config-sigdef-sig-engine)#event-action deny-packet-
inline
Osmanli(config-sigdef-sig-engine)#exit
Osmanli(config-sigdef-sig)#exit
Osmanli(config-sigdef-sig)#exit
Do you want to accept these changes? [confirm]
%IPS-6-ENGINE_BUILDS_STARTED:
%IPS-6-ENGINE_BUILDING: atomic-ip - 303 signatures - 3 of 13
engines
%IPS-6-ENGINE_READY: atomic-ip - build time 480 ms - packets
for this engine will be scanned
%IPS-6-ALL_ENGINE_BUILDS_COMPLETE: elapsed time 648 ms

Osmanli(config)#
```

Görsel 7.11: IPS imza kategorilerini kullanıma açma



UYARI

IPS/IDS imza kuralı işlemleri Görsel 7.12’de gösterilen komut ile tamamlanıp yapılandırma kaydedilirse yönlendirici IDS olarak yapılandırılır ve sadece sistem kayıtlarını sunucuya kaydeder.

```
Osmanli(config)#ip ips signature-definition
Osmanli(config-sigdef)#signature 2004 0
Osmanli(config-sigdef-sig)#status
Osmanli(config-sigdef-sig-status)#retired false
Osmanli(config-sigdef-sig-status)#enabled true
Osmanli(config-sigdef-sig-status)#exit
Osmanli(config-sigdef-sig)#engine
Osmanli(config-sigdef-sig-engine)#event-action produce-alert
Osmanli(config-sigdef-sig-engine)#
```

Görsel 7.12: IDS imza kategorilerini kullanıma açma

12. Adım: Yaptığınız yapılandırmaları görüntülemek için gerekli komutu kullanınız (Görsel 7.13).

Osmanli#show ip ips all

```
Osmanli#show ip ips all
IPS Signature File Configuration Status
Configured Config Locations: flash:ips-ids
Last signature default load time:
Last signature delta load time:
Last event action (SEAP) load time: -none-

General SEAP Config:
Global Deny Timeout: 3600 seconds
Global Overrides Status: Enabled
Global Filters Status: Enabled

IPS Auto Update is not currently configured

IPS Syslog and SDEE Notification Status
Event notification through syslog is enabled
Event notification through SDEE is enabled

IPS Signature Status
Total Active Signatures: 1
Total Inactive Signatures: 0

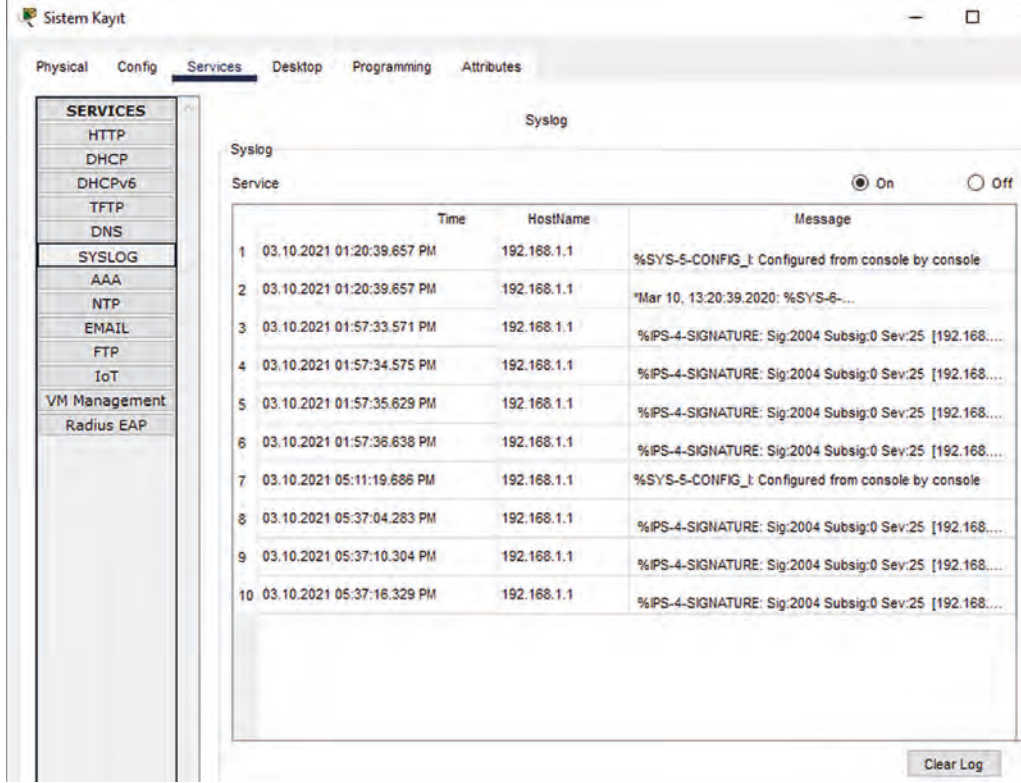
IPS Packet Scanning and Interface Status
IPS Rule Configuration
IPS name hisar
IPS fail closed is disabled
IPS deny-action ips-interface is false
Fastpath ips is enabled
Quick run mode is enabled
Interface Configuration
Interface GigabitEthernet0/1
Inbound IPS rule is not set
Outgoing IPS rule is hisar

IPS Category CLI Configuration:
Category all
Retire: True
Category ios_ips basic
Retire: False
Osmanli#
```

Görsel 7.13: IPS yapılandırmalarını görüntüleme

13. Adım: Plevne bilgisayarından Bakü bilgisayarına, Bakü bilgisayarından Plevne bilgisayarına ping atınız. Elde ettiğiniz sonuçları arkadaşlarınızla karşılaştırınız.

14. Adım: Sistem kayıt sunucu bilgisayarından IPS/IDS kayıtlarını görüntüleyiniz (Görsel 7.14).



Görsel 7.14: Sunucuda IPS/IDS kayıtlarını görüntüleme



SIRA SİZDE

Uygulama topolojisine göre Selçuklu yönlendiricisinin anahtarla bağlantılı arayüzüne IPS yapılandırınız.



ÖLÇME VE DEĞERLENDİRME

Aşağıdaki soruları dikkatlice okuyarak doğru seçeneği işaretleyiniz.

1.

- I. Gerçek iletilen paketleri analiz eder.
- II. Kötü amaçlı trafiği durdurmaz.
- III. Trafik üzerinde hiçbir etkisi yoktur.
- IV. Ağ trafiğinin kopyalarını kullanarak çevrimdışı çalışır.

Yukarıdaki bilgilerden hangisi veya hangileri IDS'nin dezavantajlarındandır?

- A) Yalnız I B) Yalnız II C) I-II D) II-III E) III-IV

2.

- I. Kötü amaçlı trafiği tespit etmek için imza kullanır.
- II. Ağ trafiğinin kopyalarını analiz eder.
- III. Ağ performansı üzerinde minimum etkisi vardır.
- IV. Sensör olarak yerleştirilmiştir.

Yukarıdaki cümlelerden hangileri IDS ve IPS'nin ortak özelliğidir?

- A) I-II B) I-III C) I-IV D) I-II-III E) I-III-IV

3. Ağın trafiğini kontrol ederek güvenliğini sağlayan yazılım veya donanım aşağıdakilerden hangisidir?

- A) Antivirüs B) Internet Security C) IPS D) IDS E) Firewall

4. IDS olarak yapılandırılmış bir yönlendiriciyi IPS olarak yapılandırmak için aşağıdaki hangi komut kullanılır?

- A) event-action deny-packet-inline
- B) event-action allow-packet-inline
- C) event-action produce-alert
- D) event-action deny-packet-all
- E) event-action allow-packet-inline

5. IPS/IDS'de ağ trafiğinin kayıtlarını etkinleştirmek için aşağıdaki hangi komut kullanılır?

- A) ip ips name log
- B) ip ips modify log
- C) ip ips status log
- D) ip ips notify log
- E) ip ips signature log

CEVAP ANAHTARLARI

1. ÖĞRENME BİRİMİNİN CEVAP ANAHTARI

1	2	3	4	5
B	A	E	E	B

2. ÖĞRENME BİRİMİNİN CEVAP ANAHTARI

1	2	3	4	5
D	B	E	E	D

3. ÖĞRENME BİRİMİNİN CEVAP ANAHTARI

1	2	3	4	5
D	D	D	Y	D
6	7	8	9	10
B	B	C	A	A

4. ÖĞRENME BİRİMİNİN CEVAP ANAHTARI

1	2	3	4	5
B	B	C	E	B

5. ÖĞRENME BİRİMİNİN CEVAP ANAHTARI

1	2	3	4	5
D	C	B	C	A
6	7	8	9	10
E	B	D	E	A

6. ÖĞRENME BİRİMİNİN CEVAP ANAHTARI

1	2	3	4	5
D	E	C	A	B

7. ÖĞRENME BİRİMİNİN CEVAP ANAHTARI

1	2	3	4	5
B	C	E	A	D

KAYNAKÇA

- Bilişim Teknolojileri Alanı Çerçeve Öğretim Programı, Ankara, 2020.
- Millî Eğitim Bakanlığı Mesleki ve Teknik Eğitim Genel Müdürlüğü “Ders Bilgi Formu” Bilişim Teknolojileri Alanı-Ağ Sistemleri ve Yönlendirme 11.Sınıf, Ankara, 2020.
- COMER E. Douglas, **Bilgisayar Ağları ve İnternet**, Nobel Akademik Yayıncılık, Ankara, 2016.
- ÇÖLKESEN Rifat, Bülent ÖRENCİK, **Bilgisayar Haberleşmesi ve Ağ Teknolojileri**, Papatya Yayıncılık, İstanbul, 2012.
- ODOM Wendell, **Cisco CCNA #640-607 Sınavı Sertifikasyon Rehberi**, Sistem Yayıncılık, 2004.
- TANER Cemal, **Ağ Yöneticiliğinin Temelleri**, Abaküs Yayınları, İstanbul, 2019.
- Türk Dil Kurumu Türkçe Sözlük, Ankara, 2019.
- Türk Dil Kurumu Yazım Kılavuzu, Ankara, 2012.
- [\(https://bidb.itu.edu.tr/seyir-defteri/blog/2013/09/07/point-to-point-protocol-\(noktadan-nokta-ya-protokol%C3%BC\)\)](https://bidb.itu.edu.tr/seyir-defteri/blog/2013/09/07/point-to-point-protocol-(noktadan-nokta-ya-protokol%C3%BC)) (Erişim Tarihi ve Saati: 15.04.2021-16.20).
- [\(https://bidb.itu.edu.tr/seyir-defteri/blog/2013/09/07/ppp-\(point-to-point-protocol---nokta-lar-aras%C4%B1-ileti%C5%9Fim-kural%C4%B1\)-kimlik-do%C4%9Frulama-metodlar%C4%B1\)](https://bidb.itu.edu.tr/seyir-defteri/blog/2013/09/07/ppp-(point-to-point-protocol---nokta-lar-aras%C4%B1-ileti%C5%9Fim-kural%C4%B1)-kimlik-do%C4%9Frulama-metodlar%C4%B1) (Erişim Tarihi ve Saati: 15.04.2021-19.20).
- [\(https://blogs.salleurl.edu/en/qos-datacenters\)](https://blogs.salleurl.edu/en/qos-datacenters) (Erişim Tarihi ve Saati: 15.04.2021-19.20).

Kaynakça atf sistemi, TDK yazım kuralları ve kaynak gösterme biçimine göre düzenlenmiştir.

GÖRSEL KAYNAKÇA



<http://kitap.eba.gov.tr/karekod/Kaynak.php?KOD=2395>

AMBULANS POLİS
ORMAN JANDARMA
İTFAİYE AFAD



ACİL ÇAĞRI SİSTEMİ