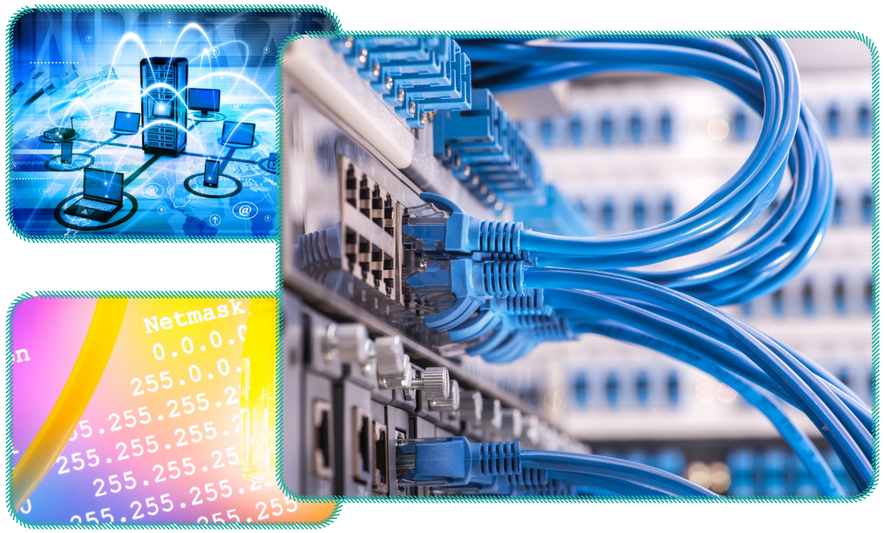
MESLEKİ VE TEKNİK ANADOLU LİSESİ

BİLİŞİM TEKNOLOJİLERİ ALANI

AĞ SİSTEMLERİ VE ANAHTARLAMA 10

DERS KİTABI



AĞ SİSTEMLERİ VE ANAHTARLAMA 10

MESLEKİ VE TEKNİK ANADOLU LİSESİ

BİLİŞİM TEKNOLOJİLERİ ALANI

AĞ SİSTEMLERİ VE ANAHTARLAMA

10

Ders Kitabı

Yazarlar

Ahmet KARBUKAN
Ali GÖKDEMİR
Hasan ACAR
Murat KARATAŞ
Özgü ASKER

T.C. MİLLÎ EĞİTİM BAKANLIĞI

HAZIRLAYANLAR

Dil Uzmanı
Erman Erşan YORGANCILAR

Program Geliştirme Uzmanı
Fulya ÖLKEN

Ölçme ve Değerlendirme Uzmanı
Arzu DURSUN URGUN

Rehberlik Uzmanı
Gülşen YALIN

Görsel Tasarım Uzmanı
Kezban DEMİRALAY

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

İSTİKLÂL MARŞI

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

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

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

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

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

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

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

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

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

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

Mehmet Âkif Ersoy

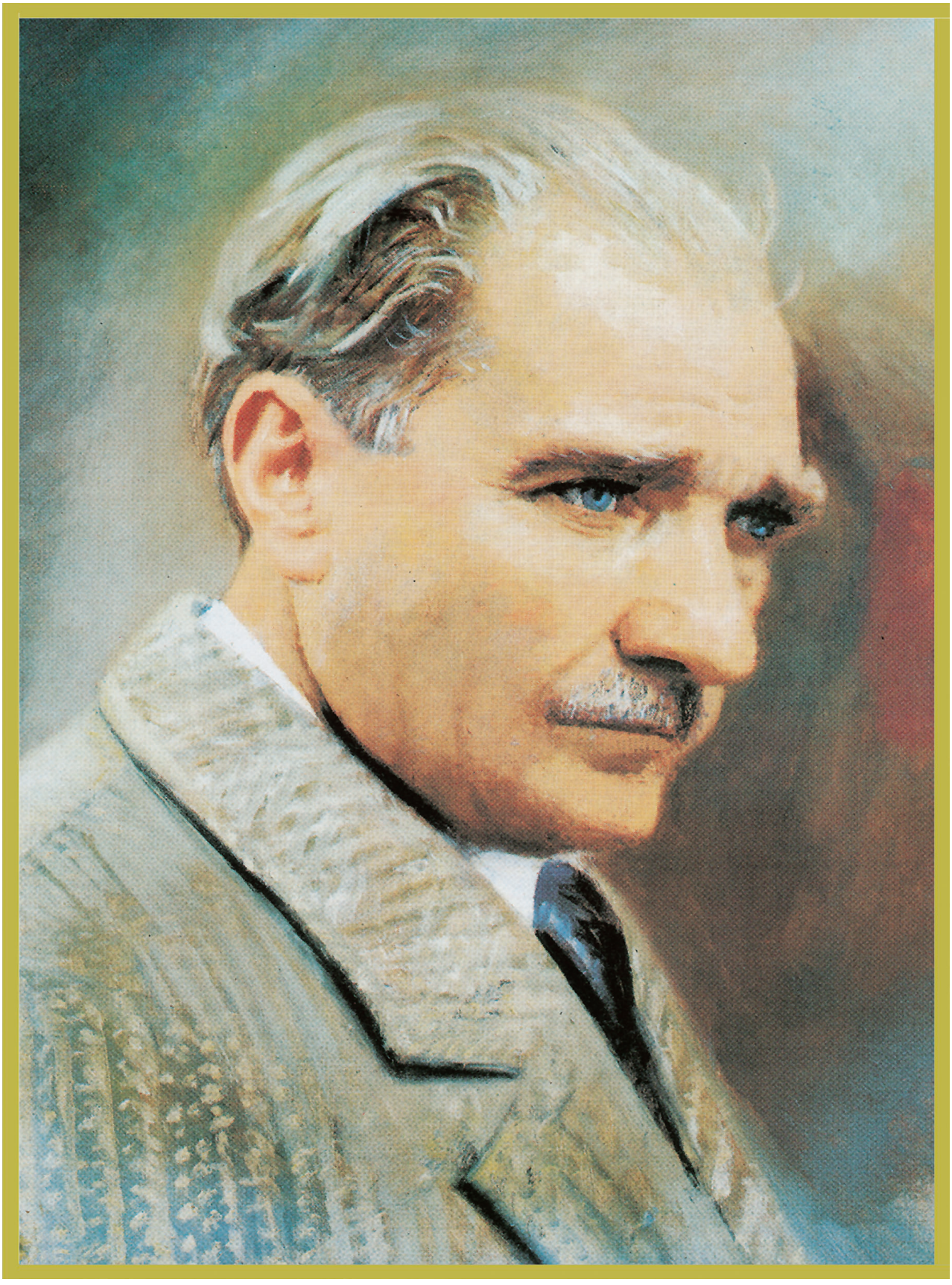
GENÇLİĞE HİTABE

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

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

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

Mustafa Kemal Atatürk



MUSTAFA KEMAL ATATÜRK

İÇİNDEKİLER

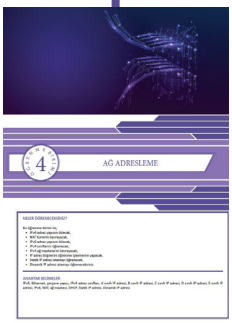
KİTAP TANITIMI 13

ÖĞRENME BİRİMİ 1: AĞLARA GİRİŞ 15
1.1. Ağ Sistemi Tasarımı 16
1.1.1. Ağ İletişimi 16
1.1.1.1. Veri İletiminde Seri İletişim 17
1.1.1.2. Veri İletiminde Paralel İletişim 17
1.1.2. Ağ Çeşitleri 18
1.1.2.1. LAN [Local Area Network (Yerel Alan Ağı)] 18
1.1.2.2. WAN [Wide Area Network (Geniş Alan Ağı)] 20
1.1.2.3. MAN [Metropolitan Area Network (Metropol Alan Ağı)] 21
1.1.2.4. WLAN [Wireless Local Area Network (Kablosuz Yerel Alan Ağı)] 21
1.1.3. Ağ Bağlantı Tipleri 21
1.1.3.1. Kablolu Bağlantı 21
1.1.3.2. Kablosuz Bağlantı 22
1.2. Ağ Topolojileri 22
1.2.1. Fiziksel Topolojiler 22
1.2.1.1. Ortak Yol (Bus) Topolojisi 23
1.2.1.2. Yıldız (Star) Topolojisi 24
1.2.1.3. Halka (Ring) Topolojisi 25
1.2.1.4. Ağaç (Tree) Topolojisi 25
1.2.1.5. Örgü (Mesh) Topolojisi 26
1.2.2. Mantıksal Topoloji 27
1.2.2.1. Broadcast (Yayın Topolojisi) 28
1.2.2.2. Token Passing (Jetonlu Geçiş Topolojisi) 28
ÖLÇME VE DEĞERLENDİRME 1 29

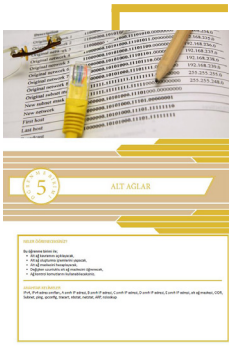
ÖĞRENME BİRİMİ 2: YEREL AĞ SİSTEMLERİ 31
2.1. Ağ Kablosu Hazırlama 32
2.1.1. Bakır Kablo Kullanılarak Ağ Kablosu Hazırlama 32
2.1.1.1. Koaksiyel (Eş Eksenli) Kablo 32
2.1.1.2. Çift Bükümlü [TP (Twisted Pair)] Kablo 32
2.1.1.3. Ağ Kablosu İçin Gerekli Aletler 34
2.1.1.4. Kablolama Standartları 35
2.1.2. Kablo Test Cihazının Kullanılması 36
2.1.2.1. LED Lambalı Kablo Test Cihazı 37
2.1.2.2. Dijital Kablo Test Cihazı 37
2.2. Ağ Cihazları 38
2.2.1. LAN Ağında Kullanılan Ağ Cihazları 38
2.2.2. LAN Cihazlarının Ağdaki Görevleri 40
2.2.3. Dağıtıcılar (Hub) 40
2.2.4. Anahtarlar (Switch) 41
2.2.5. Yönlendiriciler (Router) 43
2.2.6. Kablosuz Erişim Noktaları (Access Point) 44
2.2.7. Modem 45
2.2.8. Ağ Çeşidine Göre Ağ Cihazı Seçme 46
ÖLÇME VE DEĞERLENDİRME 2 48

ÖĞRENME BİRİMİ 3: AĞ HİZMETLERİ 49
3.1. Ağ Hizmetlerinde İletim (Taşıma) Katmanı ve Port Kullanımı 50
3.1.1. İstemci / Sunucu İlişkisi 50
3.1.2. TCP Protokolü 50
3.1.3. UDP Protokolü 51
3.1.4. Taşıma Katmanında Kullanılan Port Numaraları 52
3.1.5. İyi Bilinen Port Numaraları 52
3.1.6. Komut İstemci Kullanarak Port İzleme 53
3.1.6.1. Netstat Komutu ve İşlevi 54
3.2. Uygulama Katmanı Protokolleri 58
3.3. Ağ Protokolleri 65
3.3.1. Açık Sistem Ara Bağlantısı (OSI) Modeli 65
3.3.1.1. OSI Modelindeki Katmanların Özellikleri 67
3.3.2. İletim Denetimi Protokolü / Internet Protokolü (TCP/IP) Modeli 68

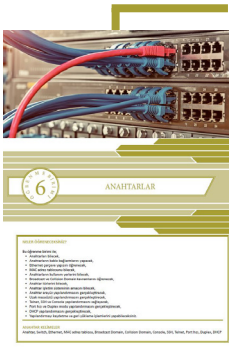
3.3.2.1. TCP/IP Katmanları ve Görevleri 69
3.3.3. Doğru Ağ Protokolünü Seçme ve Kullanma 69
3.3.3.1. Katmanlara Göre Kullanılabilecek Ağ Protokolleri 70
ÖLÇME VE DEĞERLENDİRME 3 74



ÖĞRENME BİRİMİ 4: AĞ ADRESLEME 75
4.1. Kullanıcı Sayısına Göre TCP/IP Adres Sınıfları 76
4.1.1. IPv4 Adres Yapısı 76
4.1.1.1. IPv4 Adres Sınıfları 77
4.1.1.2. Sınıfsız IPv4 Adresi (CIDR/ Classless Inter Domain Routing) 79
4.1.1.3. Özel IP Adresleri (Private IP Address) 80
4.1.2. NAT [Network Address Translation (Ağ Adresi Çeviricisi)] 81
4.1.2.1. Statik NAT 82
4.1.2.2. Dinamik NAT 82
4.1.2.3. Overload NAT (Aşırı Yüklemeli NAT)/PAT 82
4.1.3. IPv6 Adres Yapısı 82
4.1.3.1. IPv6 Başlık Yapısı 83
4.1.3.2. IPv6 Adresi Gösterim Şekli 84
4.1.4. Alt Ağ Maskesi 85
4.2. Ağ Cihazlarına TCP/IP Adresi Girişi 86
4.2.1. IP Adresi Atama Türleri 86
4.2.1.1. Elle (Manuel) IP Adresi Atama 86
4.2.1.2. Dinamik Bilgisayar Konfigürasyon Protokolü (DHCP) 87
4.2.2. DHCP ile IP Adresi Atama 87
4.2.3. Atanmış IP Bilgilerini Öğrenme 89
4.2.4. IP Adresi Atama Türü Seçme 90
4.2.5. Cihazlara Elle IP Adresi Atama 91
ÖLÇME VE DEĞERLENDİRME 4 93

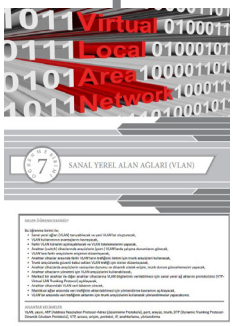


ÖĞRENME BİRİMİ 5: ALT AĞLAR 95
5.1. Alt Ağ Maskesi Hesaplama İşlemleri 96
5.1.1. Alt Ağ 96
5.1.2. Alt Ağ Oluşturma 97
5.1.3. Alt Ağ Maskesi Hesaplama 99
5.1.4. Değişken Uzunluklu Alt Ağ Maskesi [VLSM (Variable Lenght Subnet Mask)] 101
5.1.5. Ağın Gereklerine Göre Alt Ağ Oluşturma 101
5.2. Komutlarla Alt Ağların Kontrol Edilmesi 106
5.2.1. Ağ Kontrol Komutları 106
5.2.1.1. ipconfig Komutu 106
5.2.1.2. ping Komutu 108
5.2.1.3. tracert Komutu 111
5.2.1.4. nbtstat Komutu 112
5.2.1.5. netstat Komutu 114
5.2.1.6. arp Komutu 116
5.2.1.7. nslookup Komutu 118
ÖLÇME VE DEĞERLENDİRME 5 120



ÖĞRENME BİRİMİ 6: ANAHTARLAR 121
6.1. Anahtarların Fiziksel Kurulumu 122
6.1.1. Anahtarlar 122
6.1.1.1. Aktarım Yöntemleri 122
6.1.2. Anahtarların Kablo Bağlantıları 123
6.1.3. Ethernet Çerçeve Yapısı 124
6.1.4. MAC Adres Tablosu 125
6.1.5. Anahtarların Kullanım Yerleri 128
6.1.6. Broadcast ve Collision Domain 128
6.1.6.1. Collision Domain (Çakışma-Çarpışma Etki Alanı) 128
6.1.6.2. Broadcast Domain (Genel Yayın Etki Alanı) 129
6.1.7. Anahtar Türleri 130
6.1.7.1. Omurga Anahtar (Backbone Switch) 130
6.1.7.2. Merkez Anahtar (Core Switch) 131

6.1.7.3. Kenar Anahtarlar (Edge Switches) 131
6.1.7.4 ATM Anahtarlar 132
6.1.7.5. Ethernet Anahtarlar 132
6.2. Komut Arayüzü Kullanarak Temel Anahtar Yapılandırması 132
6.2.1. Anahtar İşletim Sistemi 132
6.2.2. Anahtar Arayüz Yapılandırma 137
6.2.3. Uzak Masaüstü Yapılandırma 144
6.2.4. Telnet, SSH ve Console Yapılandırma 144
6.2.4.1. Console (Konsol) Yapılandırma 145
6.2.4.2. Telnet Yapılandırma 145
6.2.4.3. SSH Yapılandırma 147
6.2.5. Port Hızı ve Duplexmodu Yapılandırma 149
6.2.6. DHCP Yapılandırma 150
6.2.7. Yapılandırmayı Kaydetme ve Geri Yükleme 152
6.2.7.1. Yapılandırmanın Kaydedilmesi 152
6.2.7.2. Geri Yükleme 153
ÖLÇME VE DEĞERLENDİRME 6 155



ÖĞRENME BİRİMİ 7: SANAL YEREL ALAN AĞLARI (VLAN) 157
7.1. VLAN Oluşturma 158
7.1.1. VLAN (Virtual Local Area Network – Sanal Yerel Alan Ağı) 158
7.1.2. VLAN Avantajları 158
7.1.3. VLAN Türleri 159
7.1.4. Anahtarlama Cihazı Arayüz (PORT) VLAN Durumları 163
7.1.4.1. Access Modu 163
7.1.4.2. Trunk Modu 163
7.1.4.3.Desirable Modu 163
7.1.5. Anahtar Cihazlarda Arayüz VLAN Erişim Durumu 163
7.1.6. Anahtar Cihazlarda Arayüz Trunk Durumu 167
7.1.7. Trunk Arayüzler İçin İzin Verilen VLAN Trafiği 170
7.1.8. Anahtar Cihazlarda Arayüz Dinamik Durum Güncellemesi 172
7.1.9. Yönetim VLAN'ları ve VLAN Arayüzleri 173
7.1.10. VTP [VLAN Trunking Protocol (Sanal Yerel Ağ Aktarım Protokolü)] 175
7.1.11. VLAN Veri Tabanını Silme 176
7.2. VLAN'lar Arası Yönlendirme 177
7.2.1. Yönlendirme 177
7.2.2. Yönlendirici Cihazda Farklı Fiziksel Arayüzler ile VLAN Yönlendirme 177
7.2.3. Trunk ile VLAN'lar Arası Yönlendirme 180
ÖLÇME VE DEĞERLENDİRME 7 183

ÖĞRENME BİRİMİ 8: LAN YEDEKLİLİĞİ 185
8.1. Yedeklilik Tasarımlarının Yapılması 186
8.1.1. Yedekleme Gereksinimleri 186
8.1.2. Yedekleme Tasarımları 186
8.1.3. Yedekleme Zafiyetleri 187
8.1.3.1. MAC Tutarsızlığı Zafiyeti 187
8.1.3.2. Broadcast Storm (Yayın Fırtınaları) Zafiyeti 190
8.2. STP-SpanningTree Protocol (Kapsama Ağacı Protokolü) 192
8.2.1. STP Amacı 192
8.2.2. Temel Köprü Anahtar (Root Bridge Switch) Seçimi 195
8.2.2.1. MAC Adresi ile Temel Köprü Seçimi 195
8.2.2.2. Öncelik Değeri Değişikliği ile Temel Köprü Anahtar Belirleme 197
8.2.2.3. Komutla Temel Köprü Anahtarı Belirleme 199
8.2.3. Farklı VLAN'lar İçin Temel Köprü Anahtarı Belirleme 201
8.2.4. STP Sürecinde Arayüz Durumları 204
8.2.4.1. Engelleme Durumu 205
8.2.4.2. Dinleme Durumu 205
8.2.4.3. Öğrenme Durumu 205
8.2.4.4. İletim Durumu 205
8.2.5. STP Çalışan Topolojilerde Anahtar Arayüz Rolleri 208

8.2.6. Anahtarlar Arası Çoklu Bağlantı STP Hesaplaması 210
8.2.6.1. Arayüz Maliyet Değerine Göre Yol Seçimi 210
8.2.6.2. Arayüz Numara Değerlerine Göre Yol Seçimi 211
8.2.7. STP Türleri 211
8.2.8. STP Güvenliği 212
8.3. Port Kümeleme 214
8.3.1. Kümelenmiş Yeni Mantıksal Arayüzler Oluşturmak 215
8.3.2. Kümeleme Yöntemleri 215
ÖLÇME VE DEĞERLENDİRME 8 219

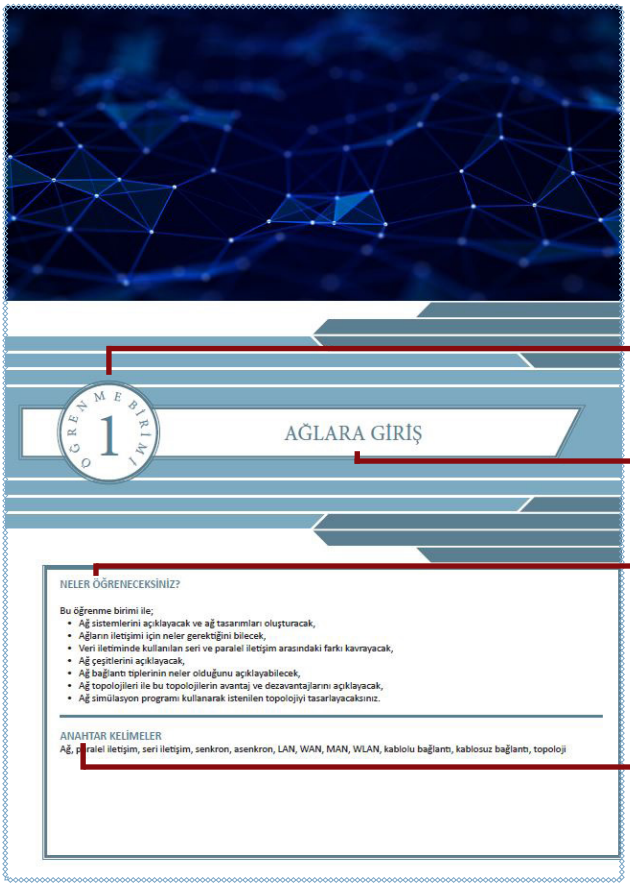
ÖĞRENME BİRİMİ 9: ÜÇÜNCÜ KATMAN ANAHTARLAR 221
9.1. Üçüncü Katman Anahtarların
(Multilayer Switch - Layer 3 Switch) Kullanılması 222
9.1.1. Üçüncü Katman ve İkinci Katman Anahtarlama Cihazı Farkları 222
9.1.2. Üçüncü Katman Anahtarlama ve Yönlendirici Cihazı Farkları 223
9.1.3. Üçüncü Katman Anahtarlama Cihazlarının Kullanım Amaçları 224
9.1.4. Üçüncü Katman Anahtarlama Kavramları 224
9.1.5. Üçüncü Katman Anahtarlama Cihazı Temel Yapılandırması 224
9.1.5.1 Üçüncü Katman Anahtarlama Cihazı Arayüz Konfigürasyonu 224
9.1.5.2. Üçüncü Katman Anahtarlama Cihazlarında Yönlendirme 226
9.1.6. Üçüncü Katman Anahtarlama Cihazında VLAN Yapılandırması 227
9.2. Üçüncü Katman Anahtarlama Cihazında Yönlendirme İşlemi 231
9.2.1. Statik Rota ile Yönlendirme 231
9.2.2. Dinamik Rota ile Yönlendirme 233
ÖLÇME VE DEĞERLENDİRME 9 237

ÖĞRENME BİRİMİ 10: ANAHTAR GÜVENLİĞİ 239
10.1. Anahtar Port Güvenliği Yapılandırması (Switchport Security) 240
10.1.1. Anahtar Güvenliği Port Yapılandırması Parametreleri 243
10.1.2. Anahtar Güvenliği Yapılandırması İhlalleri 244
10.1.3. DHCP Araya Girme (DHCP Snooping) 248
10.1.4. Dinamik ARP (Address Resolution Protocol) Denetlemesi 250
10.1.5. IP Kaynağını Koruma 252
10.1.6. VLAN Atlama (VLAN Hopping) 254
10.1.6.1. Anahtar Sahtekârlığı Yöntemi (Switch Spoofing) 254
10.1.6.2. Çift Etiketleme Yöntemi (Double Tagging) 256
10.2. Hata Yönetiminin Denetlenmesi 257
10.2.1. Debug IP DHCP Snooping 258
10.2.2. Debug IP ICMP Events 258
10.2.3. Debug SW-VLAN Packet 258
ÖLÇME VE DEĞERLENDİRME 10 259

ÖĞRENME BİRİMİ 11: GENİŞ ALAN AĞ SİSTEMLERİ 261
11.1. Geniş Alan Ağ Teknolojileri (WAN) 262
11.1.1. Geniş Alan Ağ Teknolojilerinin Sınıflandırılması 262
11.1.1.1. Bağlantı Durumuna Göre Geniş Alan Ağları 262
11.1.1.2. Anahtarlama Yöntemine Göre Geniş Alan Ağları 262
11.1.1.3. Topoloji Yapısına Göre Geniş Alan Ağları 263
11.2. Geniş Alan Ağ Cihazları 263
11.2.1. ADSL Modem 263
11.2.2. Yönlendiriciler 264
11.2.2.1. Yönlendirici Cihaz Bağlantı Türleri 264
11.2.3. ADSL Modem Kurulumu ve Yapılandırılması 265
ÖLÇME VE DEĞERLENDİRME 11 269

KAYNAKÇA 270
GENEL AĞ KAYNAKÇASI 271
GÖRSEL KAYNAKÇA 272
CEVAP ANAHTARI 274

KİTAP TANITIMI

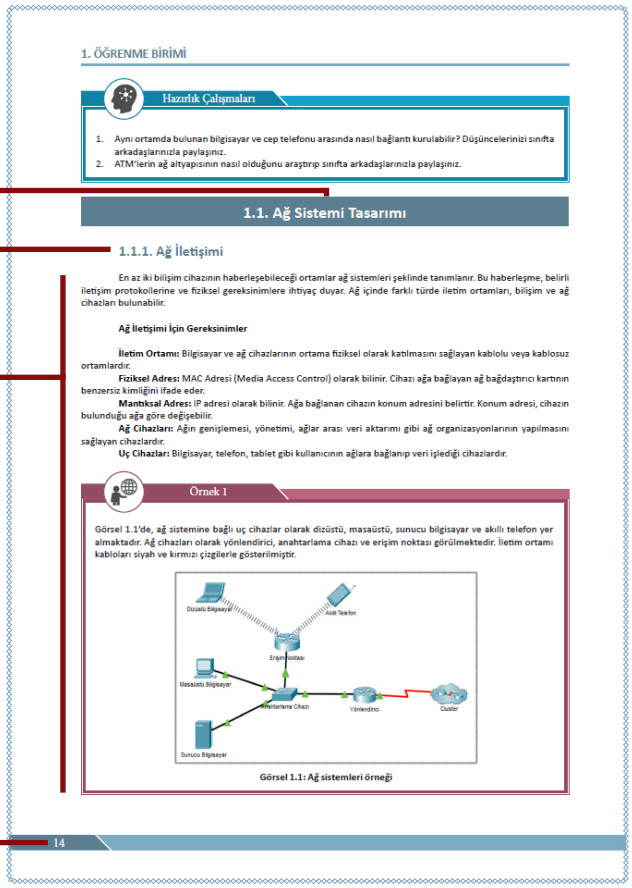


Öğrenme birimi numarasını ifade eden bölümdür.

Öğrenme birimi adını ifade eden bölümdür.

Öğrenme biriminde öğrenilecek konuların yer aldığı bölümdür.

Öğrenme biriminde öğrenilecek konular içinde öne çıkan kavramların yer aldığı bölümdür.



Konu başlığı bölümüdür.

Alt konu başlığı bölümüdür.

Kazanımları destekleyen konu metinlerinin olduğu bölümdür.

Sayfa numarasının belirtildiği bölümdür.

KİTAP TANITIMI

Hazırlık Çalışmaları

1. Aynı ortamda bulunan bilgisayar ve cep telefonu arasında nasıl bağlantı kurulabilir? Düşüncelerinizi sınıfta arkadaşlarınızla paylaşınız.
2. ATM'lerin ağ altyapısının nasıl olduğunu araştırıp sınıfta arkadaşlarınızla paylaşınız.

Öğrencilerin öğrenecekleri konu ile ilgili ön çalışma yaparak bilgi toplamasını, düşünmesini, merak etmesini vb. sağlayacak çalışmalar bu bölümde yer alır.

Bilgi

Bir kafede, okulda, kütüphanede veya herhangi bir yerde bulunan Wi-Fi erişim noktasına bağlanılması kablosuz ağa bağlanıldığını gösterir.

Konuyla ilgili bilgilerin yer aldığı bölümdür.

Dikkat

127.0.0.1 dünya üzerindeki bütün bilgisayarların yerel ağ kartı testi için ayrılmıştır ve geri dönüş **(Loopback)** adresidir.

Konuyla ve yapılan çalışmayla ilgili dikkat edilmesi gerekenler bu bölümde yer alır.

Örnek

Bilgisayarları internete veya başka bir ağa bağlamak için kablolar (Ethernet) kullanılması ya da cep telefonunda yer alan bir dosyanın USB kablosu kullanılarak bilgisayara aktarılması kablolu bağlantı yapıldığını gösterir.

Konuyla ilgili örneklerin verildiği bölümdür.

Araştırma

Çeşitli kablolu bağlantı örneklerinin neler olduğunu araştırarak sınıfta arkadaşlarınızla paylaşınız.

Derinlemesine araştırılması gereken çalışmaların yer aldığı bölümdür.

Uygulama 2

Yıldız topoloji bağlantısı için aşağıdaki yönergeleri uygulayınız.

Adım 1: Anahtar cihazınızın birinci portuna laboratuvardaki bilgisayarı bağlayınız.

Adım 2: Anahtar cihazınızın ikinci portuna laboratuvardaki diğer bilgisayarı bağlayınız.

Öğrencilerin edindiği bilgileri kullanmasını sağlayacak çalışmalar bu bölümde yer alır.

Sıra Sizde

Okulunuzdaki bilgisayar laboratuvarlarında bulunan ağ cihazlarının fiziksel topolojilerini kâğıt üzerine çizerek gösteriniz.

Öğrenilenleri pekiştirmeye yönelik yapılması gereken faaliyetleri gösteren bölümdür.

ÖĞRENME BİRİMİ 1

AĞLARA GİRİŞ

NELER ÖĞRENECEKSİNİZ?

Bu öğrenme birimi ile;

- Ağ sistemlerini açıklayacak ve ağ tasarımları oluşturacak,
- Ağların iletişimi için neler gerektiğini bilecek,
- Veri iletiminde kullanılan seri ve paralel iletişim arasındaki farkı kavrayacak,
- Ağ çeşitlerini açıklayacak,
- Ağ bağlantı tiplerinin neler olduğunu açıklayabilecek,
- Ağ topolojileri ile bu topolojilerin avantaj ve dezavantajlarını açıklayacak,
- Ağ simülasyon programı kullanarak istenilen topolojiyi tasarlayacaksınız.

ANAHTAR KELİMELER

Ağ, paralel iletişim, seri iletişim, senkron, asenkron, LAN, WAN, MAN, WLAN, kablolu bağlantı, kablosuz bağlantı, topoloji

Hazırlık Çalışmaları

1. Aynı ortamda bulunan bilgisayar ve cep telefonu arasında nasıl bağlantı kurulabilir? Düşüncelerinizi sınıfta arkadaşlarınızla paylaşınız.
2. ATM'lerin ağ altyapısının nasıl olduğunu araştırıp sınıfta arkadaşlarınızla paylaşınız.

1.1. Ağ Sistemi Tasarımı

Ağ sistemi tasarımı, ağ altyapısı uygulamasından önce yapılan ağın fiziksel ve mantıksal planlamasıdır. Ağ sistemi tasarımı, ağ simülasyon araçları yardımıyla yapılabildiği gibi çeşitli şablonlar üzerinden de planlaması hazırlanabilir.

1.1.1. Ağ İletişimi

En az iki bilişim cihazının haberleşebileceği ortamlar ağ sistemleri şeklinde tanımlanır. Bu haberleşme, belirli iletişim protokollerine ve fiziksel gereksinimlere ihtiyaç duyar. Ağ içinde farklı türde iletim ortamları, bilişim ve ağ cihazları bulunabilir.

Ağ İletişimi İçin Gereksinimler

İletim Ortamı: Bilgisayar ve ağ cihazlarının ortama fiziksel olarak katılmasını sağlayan kablolu veya kablosuz ortamlardır.

Fiziksel Adres: MAC Adresi (Media Access Control) olarak bilinir. Cihazı ağa bağlayan ağ bağdaştırıcı kartının benzersiz kimliğini ifade eder.

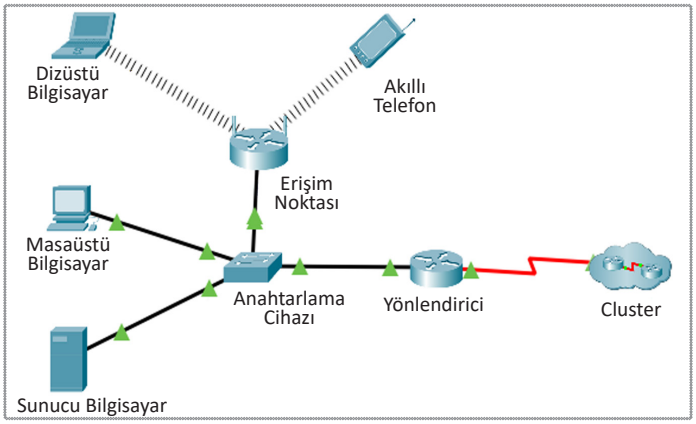
Mantıksal Adres: IP adresi olarak bilinir. Ağa bağlanan cihazın konum adresini belirtir. Konum adresi, cihazın bulunduğu ağa göre değişebilir.

Ağ Cihazları: Ağın genişlemesi, yönetimi, ağlar arası veri aktarımı gibi ağ organizasyonlarının yapılmasını sağlayan cihazlardır.

Uç Cihazlar: Bilgisayar, telefon, tablet gibi kullanıcının ağlara bağlanıp veri işlediği cihazlardır.

Örnek

Görsel 1.1'de, ağ sistemine bağlı uç cihazlar olarak dizüstü, masaüstü, sunucu bilgisayar ve akıllı telefon yer almaktadır. Ağ cihazları olarak yönlendirici, anahtarlama cihazı ve erişim noktası görülmektedir. İletim ortamı kabloları siyah ve kırmızı çizgilerle gösterilmiştir.



Görsel 1.1: Ağ sistemleri örneği

Dikkat

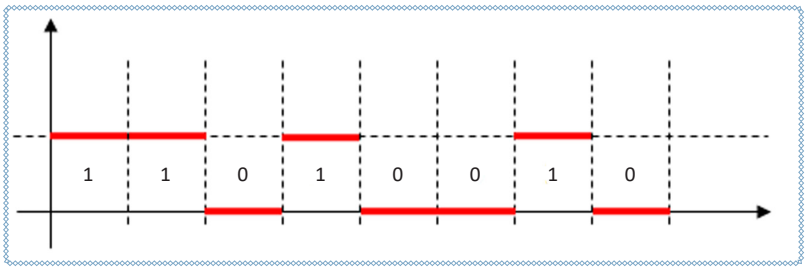
Günlük yaşantınızda ev, okul, iş yeri ağları ve kamuya açık ağlara telefon veya bilgisayarınızla bağlanarak farklı ağ sistemlerine giriş yapmış olursunuz.

Ağ sistemlerinde veriler, uçtan uca iletim ortamlarında elektrik sinyalleri şeklinde aktarılır. Bilişim alanında elektrik sinyalleri, **makine dili** olarak tanımlanır. Makine dili, ikilik sayı düzeninde 0 veya 1'lerle temsil edilir. Her veri aktarılırken 0 veya 1 şeklinde elektrik sinyalleri ile iletim ortamında aktarılır.

1.1.1.1. Veri İletiminde Seri İletişim

Verilerin bir cihazdan diğer cihaza, tek iletim hattında sıra ile aktarımı **seri iletişim** şeklinde adlandırılır. Bilgisayar ağlarında seri iletişimden yararlanılır. Seri iletiminde uç cihazların, verinin başlangıç ve bitiş bitleri ile iletim hızını bilme zorunluluğu vardır (Görsel 1.2 ve Görsel 1.3).

Görsel 1.2: Seri iletişim hattında veri iletimi



Görsel 1.3: Verinin elektrik sinyalleri sayısal gösterimi

Senkron (Eş Zamanlı) İletişim

Alıcı ve verici cihazlar arasında veri gönderilirken veri paketlerinin başlangıç ve bitişi için her iki tarafta ortak bir karakter belirlenir. Belirlenen karakter aralıklarında veri gönderimi ve alımı yapılır. Veri gönderimi olmasa bile cihazlar arasında iletişim aktiftir.

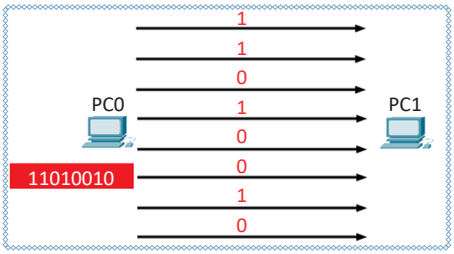
Asenkron (Eş Zamanlı Olmayan) İletişim

İletim hattı yalnızca alıcı ve verici cihazlar arasında iletim varken aktiftir. İletimin varlığını veri paketlerinin başına ve sonuna konan bitler belirler. Bu bitlere başlangıç ve bitiş bitleri denir. Verinin bozulmasına karşı eşlik bitleri eklenir.

1.1.1.2. Veri İletiminde Paralel İletişim

Paralel iletişim, veri sinyallerinin cihazlar arasında birden fazla iletim hatlarından gönderimi ile gerçekleşen iletimdir. Veri sinyalleri tek tek sıra ile değil de bütün gruplar hâlinde gönderilir. İletim hızı, veri tek seferde gruplar

hâlinde gönderildiği için seri iletime göre daha yüksektir ancak her sinyal için ayrı hat kullanılması sebebiyle daha maliyetlidir (Görsel 1.4).



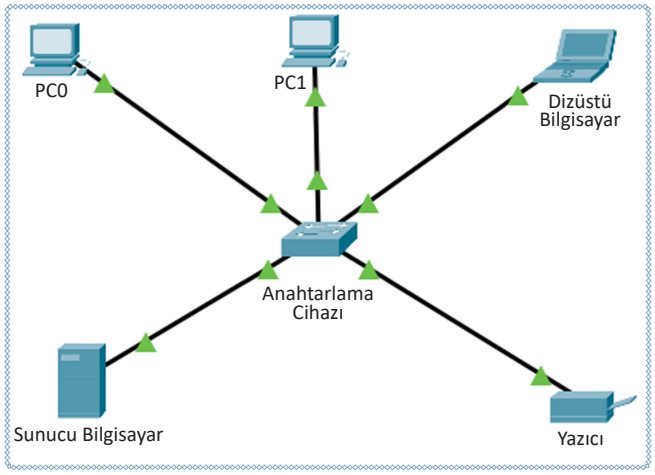
Görsel 1.4: Paralel iletişim hattında veri iletimi

1.1.2. Ağ Çeşitleri

Ağ sistemleri çalıştıkları fiziksel veya mantıksal alanlara göre gruplandırılmıştır.

1.1.2.1. LAN [Local Area Network (Yerel Alan Ağı)]

LAN genellikle coğrafi olarak küçük bir alanı ifade eden ağ çeşididir. Daha çok ev, ofis ve küçük işletmeler için tercih edilen bir ağ sistemidir (Görsel 1.5). Yerel ağın sınırları, iki bilgisayarın eşleşmesi ile başlayıp anahtar cihazlarına bağlı diğer bilgisayarlarla genişleyebilir. Yerel ağlarda anahtarlama cihazları (switch), dağıtıcılar (hub), bilgisayar ve diğer uç cihazlar bulunabilir.

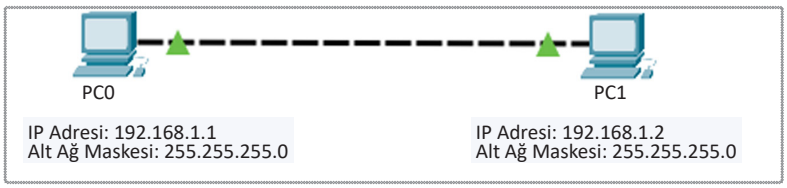


Görsel 1.5: LAN (temsili)

Uygulama 1

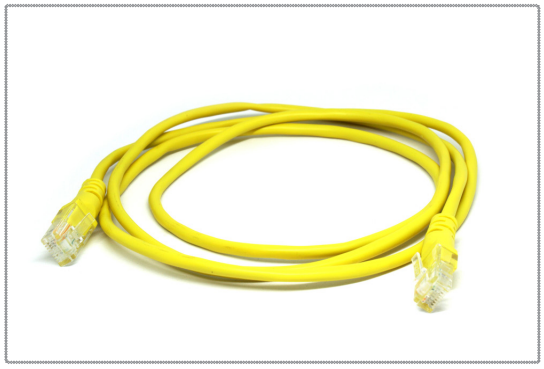
http://kitap.eba.gov.tr/KodSor.php?KOD=21027

İki bilgisayarı birbirine UTP kablo ile bağlayıp eşler arası en küçük yerel ağı oluşturmak için gerekli işlemleri simülasyon programı kullanarak aşağıdaki yönergeler doğrultusunda gerçekleştiriniz (Görsel 1.6).

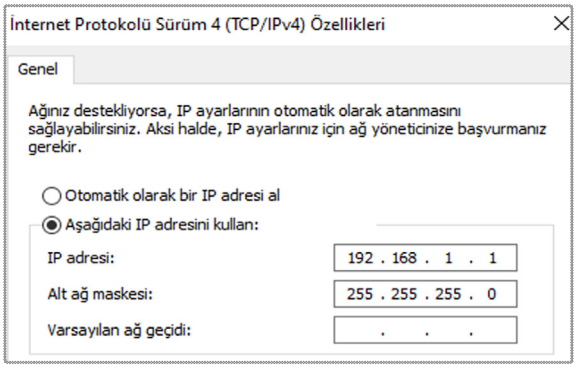


Görsel 1.6: Tek kablo ile bağlanmış eşler arası en küçük yerel ağ

Adım 1: UTP kablonun (Görsel 1.7) iki ucunu iki bilgisayarın ağ kartına takınız.



Görsel 1.7: UTP kablo



Görsel 1.8: IP ayarları

Adım 2: Bilgisayarların IP adreslerini Görsel 1.8'de olduğu gibi güncelleyiniz.

Adım 3: İletişim testini PC0'dan komut istemcisi ile "ping 192.168.1.2" komutuyla PC1'den "ping 192.168.1.1" şeklinde yapınız (Görsel 1.9).

```
C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time=2ms TTL=128
Reply from 192.168.1.2: bytes=32 time=1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)
```

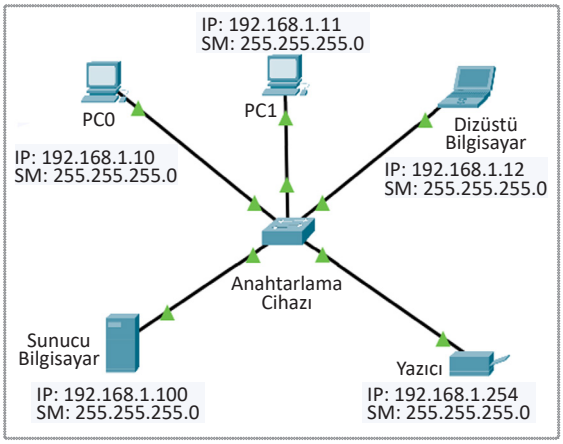
Görsel 1.9: İletişim testinin olması gereken sonucu

Yerel ağlardaki uç cihazlar, kullanıcıların bilgi teknolojilerine erişim istekleri ile beraber artar. Yerel ağlar, yeni katılımcılar ve uç cihazlarla genişler. Yerel ağların genişlemesi için anahtarlama cihazları veya dağıtıcılar kullanılır.

Görsel 1.10: Anahtarlama cihazı - Switch

Sıra Sizde

Görsel 1.11'de verilen yerel alan ağını simülasyon programında veya gerçek cihazlarınızda gerçekleştiriniz. Talimatları uygulayınız.



Görsel 1.11: Yerel alan ağı örneği

- Gerekli kablo bağlantılarını yapınız.
- Uç cihazlara tabloda verilen IP adres değerlerini giriniz (Tablo 1.1).

Tablo 1.1: IP Adres Değeri Tablosu

Uç Cihaz	IP Adresi	Alt Ağ Maskesi
PC0	192.168.1.10	255.255.255.0
PC1	192.168.1.11	255.255.255.0
Dizüstü Bilgisayar	192.168.1.12	255.255.255.0
Sunucu Bilgisayar	192.168.1.100	255.255.255.0
Yazıcı	192.168.1.254	255.255.255.0

- Uç cihazlar arasında iletişim testi yapınız.

1.1.2.2. WAN [Wide Area Network (Geniş Alan Ağı)]

WAN, coğrafi alana göre geniş bölgelere yayılmış ağ türüdür (Görsel 1.12). Ulusal veya uluslararası ağ omurgası ile yayılır. Küçük ve büyük ölçekli işletme, ofis, ev ve mobil kullanıcıları bağlanabilir. WAN sayesinde çok uzaktaki kullanıcılar ve işletmeler bilgi paylaşımında bulunabilir. Bağlantı hizmetlerini internet servis sağlayıcıları yapar. Geniş ağlarda; yönlendiriciler, CSU/DSU cihazları ve 3. katman anahtarlama cihazları bulunabilir.

WAN ile farklı yerel ağlar birbirine bağlanır. Farklı yerel ağları birbirine bağlamak için yönlendirici cihazlar kullanılır. Geniş alan ağlarına; DSL telefon hatları üzerinden, televizyon kablo altyapısı veya uydu hatları üzerinden, sabit veya mobil olarak bir modemle bağlantı yapılır.

Görsel 1.12: WAN

1.1.2.3. MAN [Metropolitan Area Network (Metropol Alan Ağı)]

MAN, geniş alan ağları kadar uzak coğrafyalarda olmasa da daha yakın ölçekli kurumsal yerleşkeler için kullanılan ağlardır.

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

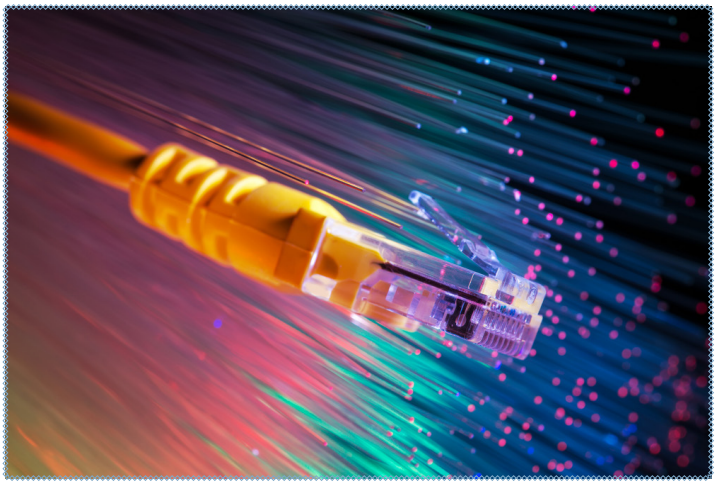
WLAN; ağ iletim ortamının kablosuz olarak hizmet verdiği ağ türüdür. Yerel ve hücresel ağlar için tercih edilir. Kullanıcıların ve uç cihazların hareket hâlinde olması, kablo maliyetinin olmaması kablolu ağlara göre bu ağların tercih edilmesini sağlar.

1.1.3. Ağ Bağlantı Tipleri

Herhangi bir ağ içinde yer alan cihazlar birbirine kablolu veya kablosuz bağlantılar kullanılarak bağlanır.

1.1.3.1. Kablolu Bağlantı

Ağ üzerinde yer alan cihazların birbirleri ile kablo kullanarak (HDMI, USB, Firewire vs.) iletişime geçmelerine **kablolu bağlantı** denir (Görsel 1.13).



Görsel 1.13: Kablo örneği

Örnek

Bilgisayarları internete veya başka bir ağa bağlamak için kablolar (Ethernet) kullanılması ya da cep telefonunda yer alan bir dosyanın USB kablosu kullanılarak bilgisayara aktarılması kablolu bağlantı kullanımına örnek olarak gösterilebilir.

Araştırma

Çeşitli kablolu bağlantı örneklerinin neler olduğunu araştırarak sınıfta arkadaşlarınızla paylaşınız.

1.1.3.2. Kablosuz Bağlantı

Ağ üzerinde yer alan cihazların kablosuz radyo frekansı / RF, Wi-Fi, Zigbee, bluetooth, Wimax, GPS, kızılötesi / IR vs. bağlantılar üzerinden iletişime geçmelerine **kablosuz bağlantı** denir (Görsel 1.14).

Görsel 1.14: Kablosuz bağlantı (temsil)

Bilgi

Bir kafede, okulda, kütüphanede veya herhangi bir yerde bulunan Wi-Fi erişim noktasına bağlanılması kablosuz ağa bağlanıldığını gösterir.

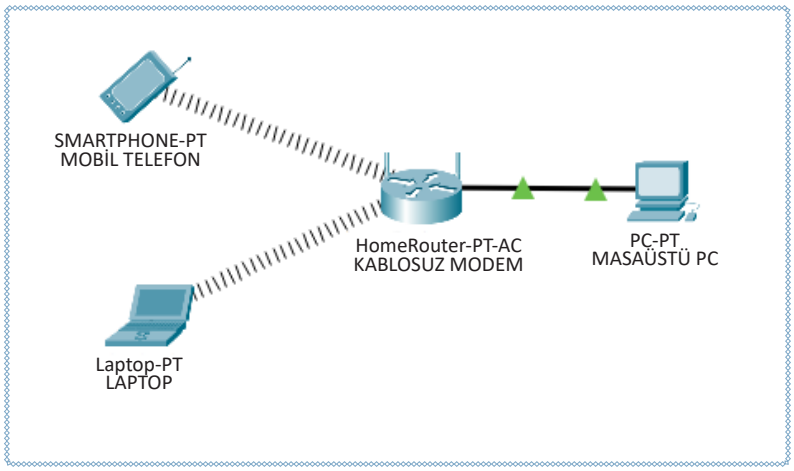
1.2. Ağ Topolojileri

Topoloji, bilgisayar ağlarında kullanılan cihazların ağ üzerinde bulunduğu konumuna, cihazlar arasında kurulan kablolama yapısına ve iletişim için gerekli olan protokollerin tamamına verilen genel bir isimdir.

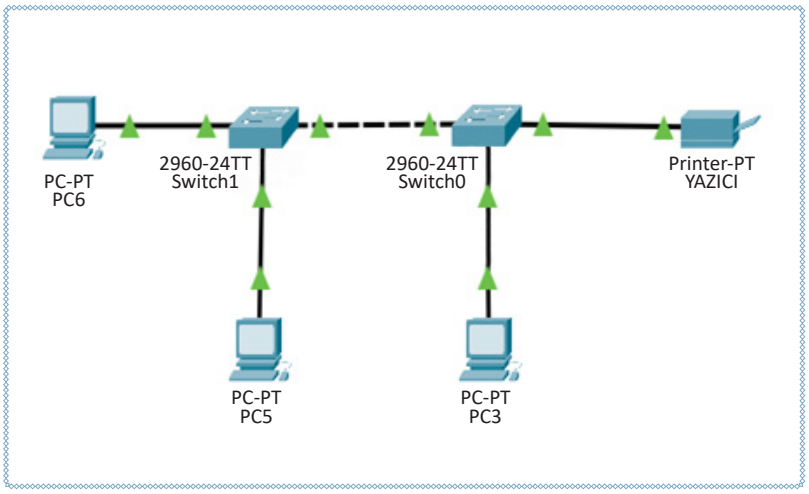
Topolojiler, fiziksel ve mantıksal olarak ikiye ayrılmaktadır.

1.2.1. Fiziksel Topolojiler

Cihazların ağ üzerindeki konumu ve kablolama yapısına **fiziksel topoloji** denir. Ağın yapısında kullanılacak kablolama türü ve kullanılacak cihazlar da bu topolojide belirlenmektedir (Görsel 1.15 ve Görsel 1.16).



Görsel 1.15: Ev tipi fiziksel topoloji örneği



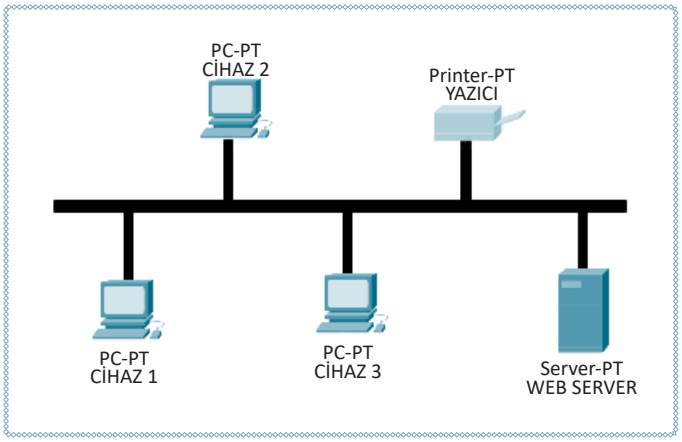
Görsel 1.16: Küçük iş yeri fiziksel topoloji örneği

Sıra Sizde

Okulunuzdaki bilgisayar laboratuvarlarında bulunan ağ cihazlarının fiziksel topolojilerini kâğıt üzerine çizerek gösteriniz.

1.2.1.1. Ortak Yol (Bus) Topolojisi

Ağ cihazlarının tek bir hat üzerinde sıralandığı topoloji yapısına **ortak yol (bus) topolojisi** denir.



Görsel 1.17: Ortak yol topolojisi örneği

Avantajları

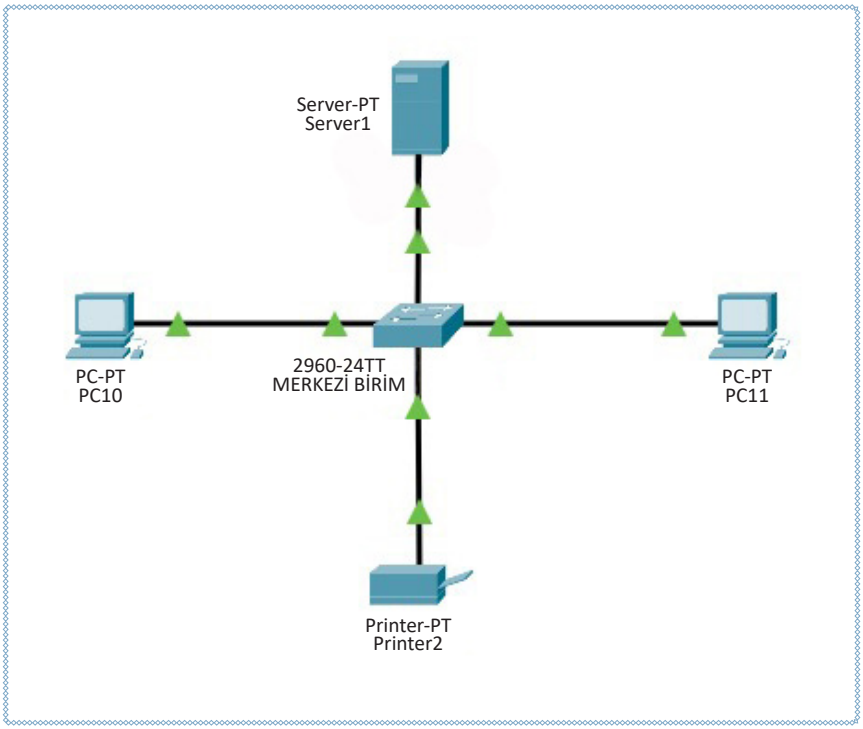
- Ağa yeni bir cihaz eklemek kolaydır.
- Tek kablo kullanıldığı için ekonomiktir ve kolay bir kurulum yapısı vardır.

Dezavantajları

- Kabloda meydana gelecek bir arıza bütün ağı etkiler.
- Merkezî bir cihaz olmadığı için arıza tespiti zordur.
- Ağda kullanılacak cihaz sayısı 30 adet ile sınırlıdır.

1.2.1.2. Yıldız (Star) Topolojisi

Yıldız topolojisinde merkezde anahtarlama cihazı (switch) ya da dağıtıcı (hub) gibi bir birim bulunmaktadır. Ağ cihazları merkezde bulunan bu birime direkt olarak bağlanmaktadır (Görsel 1.18).



Görsel 1.18: Yıldız topoloji örneği

Avantajları

- Merkezî bir birim kullanıldığı için arıza tespiti ve yönetimi kolaydır.
- Yeni bir ağ cihazı eklemek kolaydır.
- Ağ cihazlarından birinde oluşan problem bütün ağı etkilemez.

Dezavantajları

- Merkezî cihazda oluşabilecek bir arıza bütün ağı etkiler.
- Kullanılacak merkezî cihaz dağıtıcı (hub) ise yoğun bir ağ trafiği oluşur.
- Ortak yol (bus) topolojisine göre daha fazla kablo ihtiyacı vardır.

Uygulama 2

Yıldız topoloji bağlantısı için aşağıdaki yönergeleri uygulayınız.

Adım 1: Anahtar cihazınızın birinci portuna laboratuvardaki bilgisayarı bağlayınız.

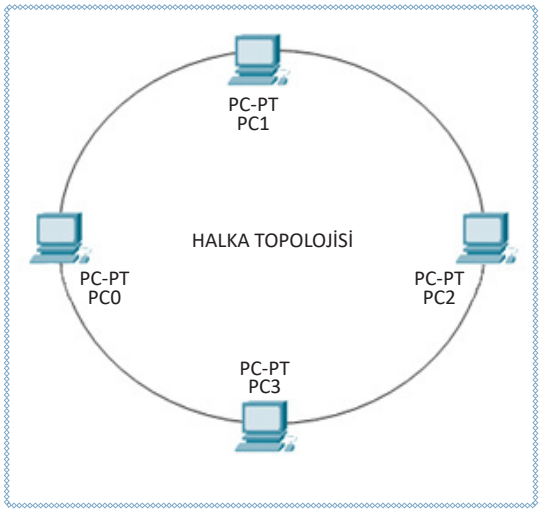
Adım 2: Anahtar cihazınızın ikinci portuna laboratuvardaki diğer bilgisayarı bağlayınız.

Adım 3: Anahtar cihazınızın üçüncü portuna laboratuvardaki bir diğer bilgisayarı bağlayınız.

Adım 4: Oluşan fiziksel ağ topolojisini inceleyiniz.

1.2.1.3. Halka (Ring) Topolojisi

Halka topolojisinde ağ cihazları dairesel bir yapıda bulunan kablolama sistemine bağlıdır. Veriler kaynaktan hedefe doğru bu yapıda gönderilirken bütün ağ cihazlarından geçer. Halka topolojisine bağlı bütün cihazlar ağ üzerinde aynı yetkiye sahiptir (Görsel 1.19).



Görsel 1.19: Halka topolojisi örneği

Avantajları

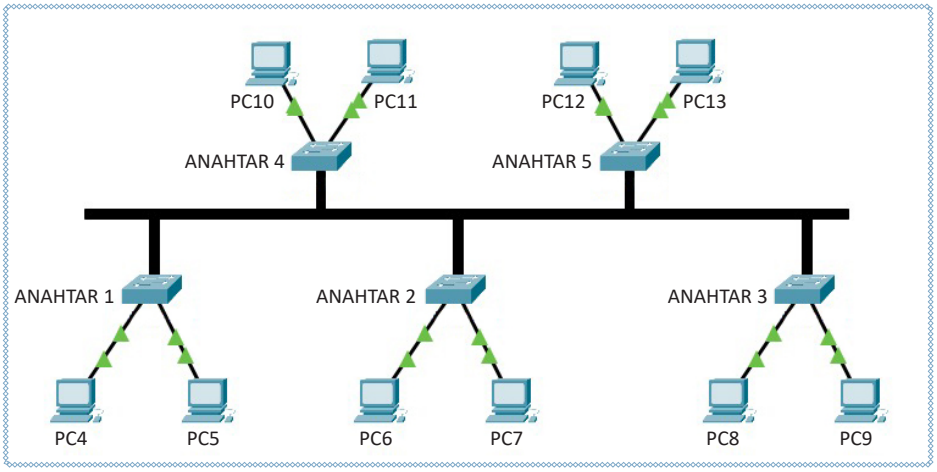
- Ağa katılan cihazlar ağ trafiğini fazlalaştırıp ağı yormaz.
- Uzun mesafelerde kaliteli bağlantı hızı sağlar.
- Yönetimi ortak yol (bus) topolojisine göre kolaydır.

Dezavantajları

- Ağa bağlı cihazların birinde oluşacak bir problem bütün ağı etkiler.

1.2.1.4. Ağaç (Tree) Topolojisi

Ağaç (tree) topolojisi, yıldız topolojisi yapısında bulunan ağları genişletmek ve hiyerarşik bir yapı oluşturmak amacıyla kullanılır. İsmini bir ağacın dallarına benzeyen yapısından almaktadır. Ortak yol (bus) topolojisindeki bir yapı, ağaç topolojisinin omurgasını oluşturmaktadır (Görsel 1.20).



Görsel 1.20: Ağaç topolojisi örneği

Avantajları

- Ağın genişletilmesi kolaydır.
- Ağaç dallarında oluşacak bir problem bütün ağı etkilemez.
- Birçok çalışma grubu bu yapı ile bir araya getirilebilir.

Dezavantajları

- Ana omurgada oluşacak bir problem bütün ağ trafiğini etkiler.
- Kablolama zordur ve maliyeti yüksektir.
- Dal sayısı arttıkça bakım ve yönetim zorlaşır.

Uygulama 3

Yıldız topoloji bağlantısı için aşağıdaki yönergeleri uygulayınız.

Adım 1: Yıldız topoloji uygulamasında oluşturduğunuz yapıyı tekrar kurunuz.

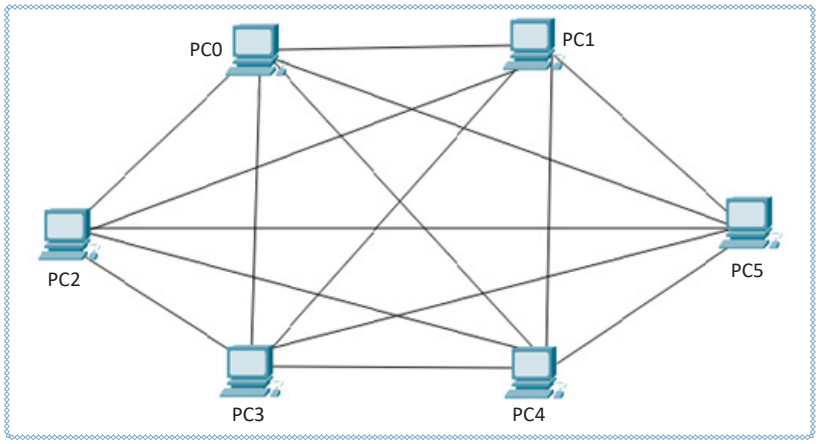
Adım 2: İkinci bir anahtar cihazı ile aynı yapıyı oluşturunuz.

Adım 3: İki anahtar cihazını birbirine bağlayınız.

Adım 4: Oluşan fiziksel ağ topolojisini inceleyiniz.

1.2.1.5. Örgü (Mesh) Topolojisi

Noktadan noktaya bütün cihazların birbirine bağlı olduğu topolojiye **örgü (mesh) topolojisi** denir. Genellikle geniş alan ağlarında (WAN'larda) kullanılır (Görsel 1.21).



Görsel 1.21: Mesh topolojisi örneği

Avantajları

- Ağa bağlı cihazların birinde oluşacak problem ağ trafiğini etkilemez.

Dezavantajları

- Karmaşık bir yapısı vardır.
- Kablolama maliyeti yüksektir ve ağın yönetimi zordur.

Ağ topolojisi seçiminde aşağıdaki unsurları göz önünde bulundurmak gerekir:

- Ağa bağlanacak bilgisayar sayısı
- Veri transfer hızı
- Kurulum kolaylığı
- Yeniden düzenleme kolaylığı
- Ortamdaki bir problemden etkilenen birim sayısı
- Güvenlik
- Maliyet

Uygulama 4

http://kitap.eba.gov.tr/KodSor.php?KOD=21028

Okulumuz Bilişim Teknolojileri Alanı'nda yeni bir ağ yapısı oluşturulacaktır. Alanımızda 4 adet bilişim teknolojileri laboratuvarı ve her laboratuvarda 10 adet bilgisayar bulunmaktadır. Elimizde sadece 5 adet anahtarlama cihazı bulunmaktadır. Bütün ağ cihazlarının iletişim hâlinde olduğu doğru topolojiyi ağ simülasyon programı kullanarak aşağıdaki yönergeler doğrultusunda gerçekleştiriniz.

Adım 1: Dört laboratuvara birer adet anahtarlama cihazı ekleyiniz.

Adım 2: Eklediğiniz anahtarlama cihazlarının her birine onar adet bilgisayar ekleyiniz.

Adım 3: Dört adet anahtarlama cihazının birbirleri arasında iletişim kurabilmesi için anahtarlama cihazından merkezî bir birim ekleyiniz.

Adım 4: Yıldız topolojisini oluşturmak için tüm laboratuvarlarda bulunan bütün anahtarlama cihazlarını merkezî birimde bununan anahtarlama cihazına takınız.

Adım 5: Yıldız topolojisinin bağlantı testini yapınız.

Sıra Sizde

Yeni kurulacak küçük bir ofiste ağ yönetimini sağlayacak merkezî bir cihaz olmasa da ellerinde koaksiyel (eş eksenli) kablo ve sonlandırıcı bulunmaktadır. İsraftan kaçınmak için ellerindeki malzemelerle ağ yapısı oluşturmak istemektedirler. Sizce 5 adet PC ve 1 adet yazıcı bulunan ofise uygun topoloji nedir? Sınıfta dörder kişilik gruplar oluşturup en uygun topolojiyi tasarlayarak çizimle gösteriniz.

Sıra Sizde

Bilişim teknolojileri alanında hizmet veren bir şirketin Finans, Teknik Servis ve AR-GE isminde üç farklı departmanı vardır. Şirkette sadece 3 anahtarlama cihazı ve her birimde 3 adet PC bulunmaktadır. Ellerinde sadece kablo ve sonlandırıcı bulunan şirkete en uygun topoloji nedir? Topoloji tasarımını çizimle gösteriniz.

1.2.2. Mantıksal Topoloji

Ağ üzerindeki cihazların haberleşme şekilleri ve kullandıkları iletişim protokolleri **mantıksal topoloji** ile açıklanır. Mantıksal ağ topolojileri genellikle yayın topolojisi ve jetonlu geçiş topolojisi olmak üzere iki sınıfa ayrılır.

1.2.2.1. Broadcast (Yayın Topolojisi)

Bu topolojide gönderici cihaz veriyi ağa bırakır, veri alıcıya ulaşıncaya kadar tüm ağı dolaşır. Ağa bağlı cihazların öncelik hakkı yoktur ve ağdaki tüm cihazlara veri iletimi gerçekleştirilir.

1.2.2.2. Token Passing (Jetonlu Geçiş Topolojisi)

Halka topolojisinde olduğu gibi tüm ağı dolaşan bir **jeton** (token) veri iletimini gerçekleştirir. Jeton ağ üzerinde dolaşırken sırayla tüm cihazlarla iletişime geçer ve gönderilecek ya da alınacak veri olup olmadığını kontrol eder.

Aşağıdaki soruları dikkatlice okuyunuz ve doğru seçeneği işaretleyiniz.

1. I. IP Adresi
II. MAC Adresi
III. İletim Ortamları
IV. Uç Cihazlar

Yukarıdakilerden hangileri ağ üzerinde yer alan cihazların iletişimi için gereklidir?

A) I ve II B) I ve III C) II, III ve IV D) I, II ve IV E) I,II,III ve IV

2. Aşağıdakilerden hangisi kapsadığı alan bakımından en küçük ağ yapısıdır?

A) MAN B) LAN C) PAN D) WLAN E) WAN

3. Aşağıdakilerden hangisi bir kablosuz iletişim örneği <u>değildir?</u>

A) Bir kafeteryada Wi-Fi bağlantısı kullanarak internete bağlanmak
B) Kızılötesi kullanılarak cep telefonunda yer alan bir belgeyi bilgisayara aktarmak
C) Bir cihazdaki verileri USB kullanarak başka cihaza aktarmak
D) Bir cep telefonu ile diğer bir mobil cihazın bluetooth kullanarak iletişim kurmalarını sağlamak
E) Uzaktan kumanda kullanarak televizyondaki kanalları değiştirmek

4. Aşağıdaki fiziksel topolojilerin hangisi ağ cihazlarının tek bir ağ üzerinde sıralandığı topolojidir?

A) Yıldız topolojisi
B) Ortak yol topolojisi
C) Halka topolojisi
D) Ağ topolojisi
E) Hücresel topoloji

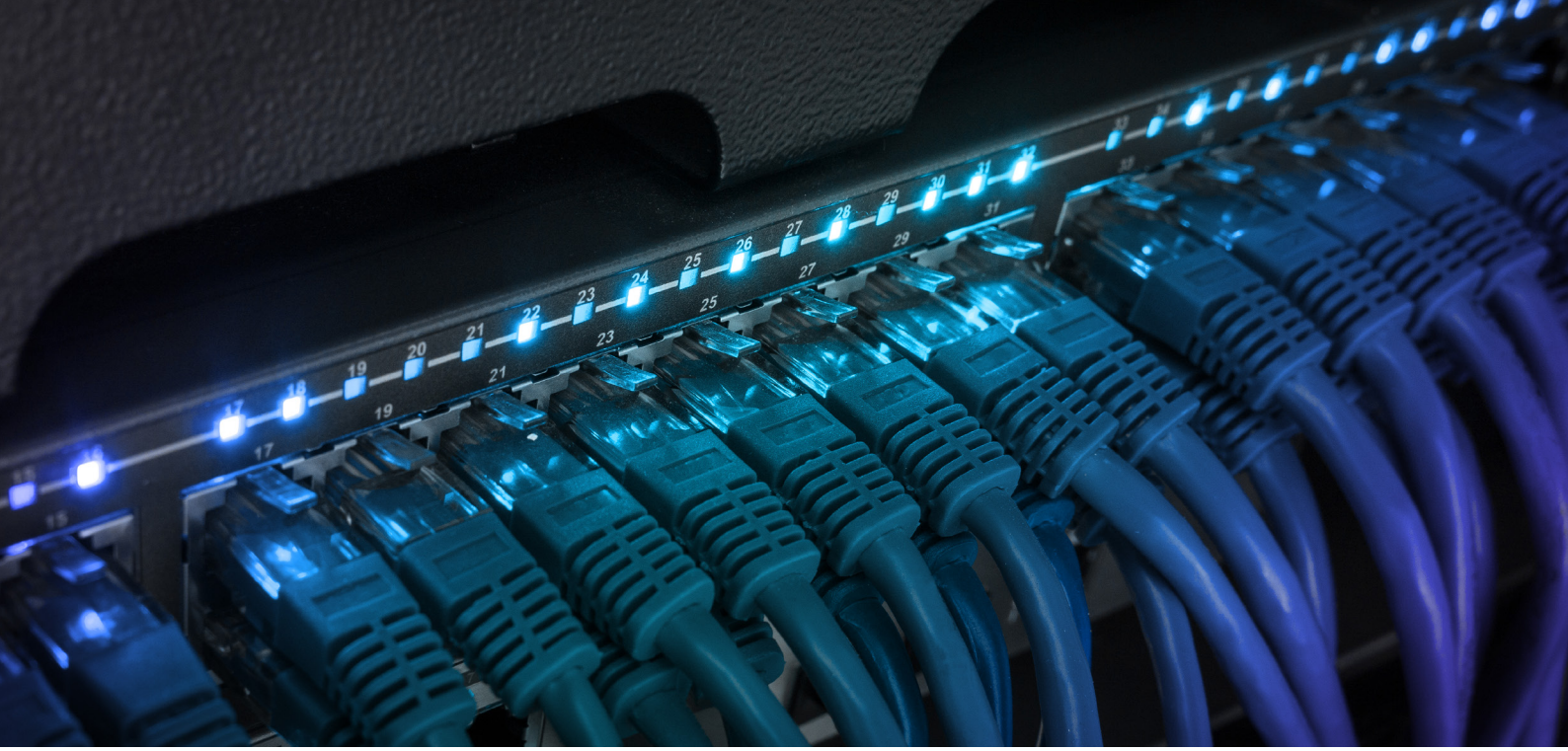
5. Aşağıdakilerden hangisi bir LAN bağlantısı şekli <u>değildir?</u>

A) Yıldız topolojisi
B) Ağaç topolojisi
C) Ortak yol topolojisi
D) Wi-Fi bağlantısı
E) Halka topolojisi

6. A sütununda verilen cümlelerin önündeki parantezlere B sütunundaki seçeneklerden doğru olanının harfini yazınız.

A Sütunu
( ) 1. İletim hattı yalnızca alıcı ve verici cihazlar arasında iletim varken aktiftir.
( ) 2. Ağın genişlemesi, yönetimi, ağlar arası veri aktarımı gibi ağ organizasyonlarının yapılmasını sağlayan cihazlardır.
( ) 3. Noktadan noktaya bütün cihazların birbirine bağlı olduğu topolojidir.
( ) 4. Ağ cihazlarının tek bir hat üzerinde sıralandığı topolojidir.

B Sütunu
A. Örgü Topolojisi
B. Asenkron İletişim
C. Ortak Yol Topolojisi
D. Ağ Cihazları
E. Senkron İletişim



ÖĞRENME BİRİMİ 2

YEREL AĞ SİSTEMLERİ

NELER ÖĞRENECEKSİNİZ?

Bu öğrenme biriminde;

- Ağ kablolarını (bakır) tanıyacak,
- Düz ve çapraz kablolama yapacak,
- Kablo hazırlama işlemlerini ve yapısal kablolamayı bilecek,
- Kablo test işlemini yapacak,
- Dağıtıcıları tanıyacak ve özelliklerini bilecek,
- Anahtarları tanıyacak ve özelliklerini bilecek,
- Yönlendiricileri tanıyacak ve özelliklerini bilecek,
- Kablosuz erişim noktalarını tanıyacak ve özelliklerini bilecek,
- Modemleri tanıyıp özelliklerini bilecek ve öğreneceksiniz.

ANAHTAR KELİMELER

NIC, tekrarlayıcı, dağıtıcı, köprü, anahtar, kablosuz erişim noktası, yönlendirici, güvenlik duvarı, modem, koaksiyel kablo, bükümlü çift (TP) kablo, kategori, sınıf, RJ-45, Cat kablo tipleri, kablo soyucu, kablo sıkma pensesi, T568A, T568B, yapısal kablolama, Yönlendirici Bilgi Protokolü (RIP), İlk Açık Yöne Öncelik Protokolü (OSPF), ADSL

Hazırlık Çalışmaları

1. Evinizde kullandığınız televizyon veya internet kablolarının sağlamlık kontrolünün nasıl yapıldığını açıklayınız.
2. Evinizde internet bağlantısı varsa hangi ağ cihazlarını kullanıyorsunuz? Bu cihazları kullanmak için herhangi bir işlem yaptınız mı? Açıklayınız.

2.1. Ağ Kablosu Hazırlama

Ağ kabloları; bilgisayarlar, yönlendiriciler, anahtarlar ve depolama merkezleri arasında veri iletişimi ve veri aktarımı için kullanılmaktadır. Bu kablolar, içinden verilerin aktığı taşıyıcı bir ortamdır. Genellikle ağ kablolarının çevresi koruyucu malzemelerle kaplanmıştır. Bu sayede dış etkenlerden en üst seviyede korunması ve en az kayıpla veri iletiminin gerçekleşmesi sağlanmıştır.

Günümüzde farklı tipte iletişim kabloları bulunmaktadır. Kullanılacak uygun kablo tipi, sistemin genel mimari yapısına ve topolojisine bağlıdır. Kablosuz cihazların yaygınlaşmasıyla birlikte iletişim mesafelerinin genişliği ve veri güvenliğinin önemi nedeniyle ağ kabloları, hâlâ vazgeçilmez veri iletim aracıdır. En yaygın kullanılan veri iletişim kabloları, **bükümlü çift kablo** olarak adlandırılan kablo çeşididir.

Ağ kabloları, OSI referans modelinin fiziksel katmanında yer alır. Ağın fiziksel yerleşimi, coğrafi genişliği ve veri kapasitesi dikkate alınarak farklı türde kablo standartları oluşturulmuştur. Kablo Uluslararası Standardizasyon Örgütü (ISO) ile Uluslararası Elektroteknik Komisyonu (IEC) ISO / IEC 11801, Avrupa Normları (EN), Amerikan Ulusal Standartlar Enstitüsü (ANSI), Telekomünikasyon Endüstrisi Derneği (TIA) ve Elektronik Endüstriler Birliği (EIA) gibi çeşitli organizasyon ve kuruluşlar tarafından belirlenir.

2.1.1. Bakır Kablo Kullanılarak Ağ Kablosu Hazırlama

Yerel alan ağlarında genellikle bakır iletken tel içeren kablolar kullanılır. Elektrik akımını en iyi ileten iletkenlerden biri olması ve düşük enerji ile veriyi daha uzun mesafelere iletebilmesi sebebiyle bakır tel tercih edilmektedir.

Yerel alan ağlarında eskiden beri kullanılan iki bakır kablo türü **koaksiyel (eş eksenli)** ve **çift bükümlü kablo'**dur. Günümüzde koaksiyel kablo, ağ kablosu olarak neredeyse hiç kullanılmamaktadır.

2.1.1.1. Koaksiyel (Eş Eksenli) Kablo

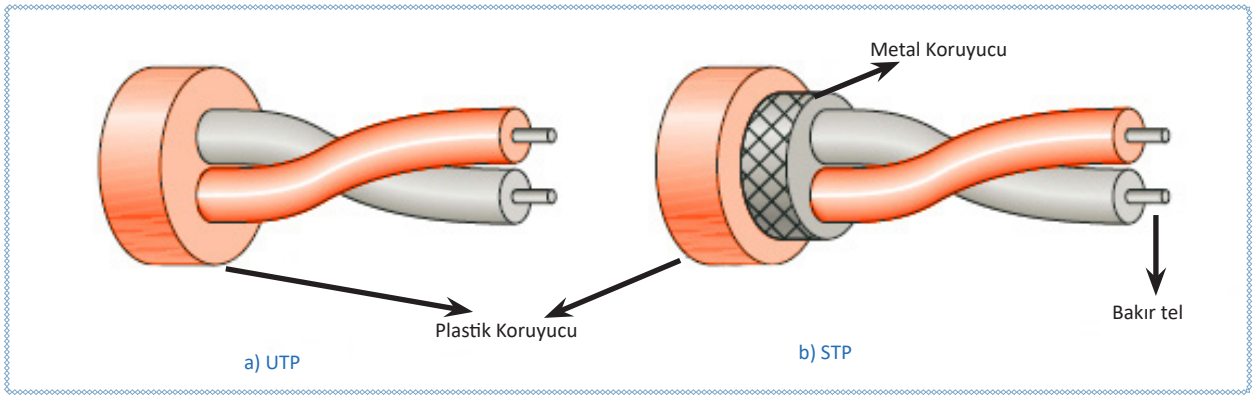
Koaksiyel kablolarının dört katlı bir yapısı vardır. En iç çekirdek kısmında (enerji taşıyan kısımda) genellikle bakır veya alüminyum bir tel bölüm bulunmaktadır. İkinci kısımda ise bu çekirdek bakır veya alüminyum tel kısmı çevreleyen yalıtkan bölümü bulunur. Bu bölümde önce yalıtkan bir tabaka yer alır. Bu tabakanın hemen üzerinde bakır veya alüminyumdan yapılmış örgülü bir kafes bulunur. Bu kafes, kabloyu elektromanyetik parazitlerden (EMI) korumaya yardımcı olur. Son olarak kafesin üzerinde plastik kaplama yer alır. Koaksiyel kablolar 100 Mbps'ye kadar veri iletimi gerçekleştirebilir.

Günümüzde koaksiyel kablolar, televizyonlarda görüntü aktarımı amacıyla kullanılmaktadır.

2.1.1.2. Çift Bükümlü [TP (Twisted Pair)] Kablo

Çift bükümlü kablo, telefon ve yerel alan ağları için geliştirilmiş bakır kablo türüdür. **Bükümlü kablo** adını, kablo boyunca tellerdeki bükülmeden almaktadır. Kablodaki bu bükülmeler, veri iletişimi sırasında sinyal bozulmasından korunmak için yapılmıştır. Bükümlü kabloların veri sinyali bozulmadan verileri iletebilecekleri bir uzunluk sınırı bulunmaktadır. Bükümlü kablolar için bu uzunluk sınırı ortalama 100 metredir. Bu kablolara çift bükümlü denmesinin sebebi, kablo çiftlerinin dört tanesinin bir araya getirilip üzerlerine esnek bir plastik kılıf geçirilmesi ile oluşmasındandır.

Çift bükümlü kablolar, **korumasız [UTP (Unshielted Twisted Pair)]** ve **korumalı [STP (Shielted Twisted Pair)]** olmak üzere iki çeşitten oluşur (Görsel 2.1). UTP, elektromanyetik parazitler ile radyo frekansı parazitlerine karşı koruma sağlama konusunda yetersizdir. Bu kablolar; elektromanyetik alan, ısı, ışık gibi çeşitli kaynaklardan etkilenebilir.



Görsel 2.1: Çift bükümlü kabloların yapısı

Çift bükümlü kablolardan biri alıcıya sinyal taşımak için kullanılırken diğeri topraklama olarak kullanılır. Alıcı, ikisi arasındaki farkı hesaplar. Veriyi gönderen ve alan iki sistem arasında, veri gönderimi sırasında tellerden birinde gönderilen sinyale ek olarak bulunulan ortama göre parazit (gürültü) eklenebilir. Bu parazit, her iki kabloyu da etkileyebilir ve istenmeyen sinyaller oluşturabilir. İstenmeyen sinyallerin veriyi etkilememesi için kablo telleri çiftler hâlinde bükülerek bir denge sağlanmıştır. Örneğin, bir bükülmede bir telin gürültü (veya parazit) kaynağına daha yakın ve diğerinin daha uzak olduğu varsayılırsa bir sonraki bükülmede ise bunun tersi olacaktır. Bükülme, her iki kablonun da dış etkilerden (gürültü veya parazit) eşit derecede etkilenmesine imkân sağlar. Bu, ikisi arasındaki farkı hesaplayan alıcının istenmeyen sinyal almadığı anlamına gelir. İstenmeyen sinyaller çoğunlukla iptal edilir.

STP çift bükümlü kabloların üzerinde elektromanyetik parazite, ısı ve ışık gibi etkilere karşı koruma sağlaması için metalik bir örgü (metal koruyucu) veya folyo sargısı bulunmaktadır. Bu nedenle STP günümüzde ağ iletişiminde yaygın olarak kullanılan bir kablo çeşididir.

Çift bükümlü kablolar dört farklı renk grubu ile kodlanmış sekiz telden oluşmaktadır. Renk kodları ve sıralamaları Tablo 2.1'de gösterilmiştir.

Tablo 2.1: Çift Bükümlü Kablo Renkleri

ÇİFT 1: MAVİ, MAVİ - BEYAZ
ÇİFT 2: TURUNCU, TURUNCU - BEYAZ
ÇİFT 3: YEŞİL, YEŞİL - BEYAZ
ÇİFT 4: KAHVERENGİ, KAHVERENGİ - BEYAZ

Bükümlü kabloların ağ cihazlarına bağlanabilmesi için bir **konnektör** ile sonlandırılması gerekir. **RJ-45**, özellikle yerel alan ağlarında kullanılan bükümlü kablolar için standart bir konnektördür. RJ-45 haricinde GG45, TERA, ARJ45 konnektör çeşitleri de bükümlü kablolarda sonlandırıcı olarak kullanılmaktadır. RJ-45 konnektörü Cat5, Cat6 ve Cat6A ve Cat8.1'de standart olarak kullanılırken Cat7 ve Cat8.2 gibi kablo teknolojilerinde kullanılamaz.

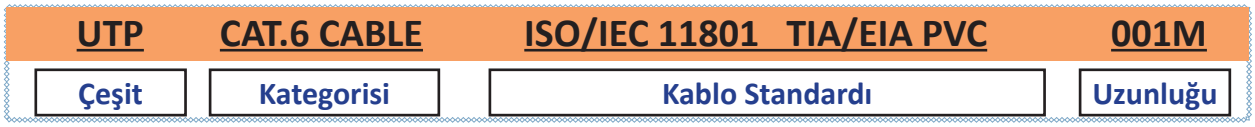
Çift bükümlü kablo seçiminde dikkat edilmesi gereken dört temel özellik bulunmaktadır. Bu özellikler; frekans, mesafe, bant genişliği ve maliyet-dayanım süresidir. **Frekans**, kablonun maksimum sinyal hızını ifade eder. **Kablo mesafesi**, kablonun veriyi kayıpsız ve bozulma olmadan iletebildiği maksimum uzunluğunu belirtir. **Bant genişliği**, kablodan bir saniyede iletilebilecek maksimum veri miktarını belirtir. **Maliyet ve dayanım süresi** ise kablonun ortalama ömrü hesaba katılarak ödenen alım bedelidir. İsraftan kaçınmak için ekonomik kablo tercihleri dikkate alınmalıdır.

ANSI / EIA / TIA, TP kablolama sistemi ve bileşenler için **kategori** (category) terimini kullanırken ISO / IEC 11801 ve EN 50173 **sınıf** (class) terimini kullanır. Tablo 2.2'de günümüzde kullanılan bükümlü kablo standartları ve özellikleri görülmektedir.

Tablo 2.2: TP Kablo Standartları

Standart İsmi	Frekansı	Mesafe	Bant Genişliği	Kablo Tipi	Sonlandırma Türü
Class D / Cat.5e	100 MHz	100 m	100 Mbit/s- 1 Gb/s UTP,	U/UTP - F/UTP - S/FTP	RJ-45
Class E / Cat.6	250 MHz	100 m (55 m'den sonra düşük hız)	1 Gb/s -10 Gb/s UTP,	U/UTP - F/UTP - S/FTP	RJ-45
Class EA / Cat.6A	500 MHz	100 m	10 Gb/s UTP,	U/UTP - F/UTP - S/FTP	RJ-45
Class F / Cat.7	600 MHz	100 m	10 Gb/s	UTP/STP	GG45/TERA/ARJ45
Class FA / Cat.7A	1000 MHz	100 m	10 Gb/s	S/FTP	GG45/TERA/ARJ45
Class I / Cat.8.1	2000 MHz	30 m	25 Gb/s-40 Gb/s	F/UTP – S/FTP	RJ-45
Class II / Cat.8.2	2000 MHz	30 m	40 Gb/s	S/FTP	GG45/TERA/ARJ45

Bükümlü kablo üzerinde birtakım yazılar bulunmaktadır. Bu yazılar; kablonun çeşidi, kategorisi, standardı ve başlangıçtan itibaren kaçıncı metrede olduğu gibi önemli bilgileri belirtir. Görsel 2.2'de çift bükümlü kablo üzerinde yazılı bilgiler ve sonrasında ise bu bilgilerin açıklamaları görülmektedir.



Görsel 2.2: Çift bükümlü kablo bilgileri

Çeşit: Kablo, UTP çeşidi bir kablodur.
Kategori: Kablo, kategori 6 (Cat6) veri iletim standardına göre üretilmiştir.
Kablo Standardı: Kablo, ISO / IEC 11801 ve TIA / EIA PVC standartlarına uygun üretilmiştir. PVC kablo kılıfı türü olarak bilinir. Bu kısımda belirtilen türler yangına karşı kablonun gösterdiği direnci ve yanma durumunda çıkardığı tehlikeli gaz ve duman oranını ifade eder. Kılıfların PVC, CM, CMR ve CMP gibi farklı türleri de bulunmaktadır.
Uzunluk: Kullanılan kablonun metre cinsinden uzunluğudur. Kablo üzerinde bulunan uzunluk değeri kablonun en başından birer metre aralıkla artar. Bu değer, ağda kullanılan kablo miktarını ölçmek ve istenilen uzunlukta kablo parçaları oluşturmak açısından faydalıdır.

Sıra Sizde

Bilişim Teknolojileri Alanına en uygun kablo çeşidini, kategorisini, kablo standardını belirleyebilmek için bir araştırma yapınız. Bu araştırma için fiziki mekânı dikkate alınız. Bulduğunuz sonuçları arkadaşlarınız ile paylaşınız. Öğretmeninize sonuçları göstererek laboratuvarınızda kullanılan kablo ile araştırmada edindiğiniz sonuçları karşılaştırınız.

2.1.1.3. Ağ Kablosu İçin Gerekli Aletler

Bakır iletken tel kullanılan çift bükümlü kabloyla ağ kablosu yapabilmek için aşağıdaki aletlere ihtiyaç duyulmaktadır.

Kablo Kesme, Soyma ve Sıyırma Aleti

Çift bükümlü kabloların uçlarını hazırlamak için kablonun koruyucu plastiğini soymak ve konnektörü ayrılan tel çiftlerinin uçlarındaki fazla kısımı kesmek amacıyla kullanılır.

Kablo Sıkma Pensesi

Kablo sıkma pensesi, kablonun bakır tel uçlarını konnektöre takıp sıkılması amacıyla kullanılır. Birçok kablo sıkma pensesi, kablo soyma ve kesme gibi işleri de yapabilmektedir. Piyasada kolaylıkla bulunabilen kablo sıkma penseleri, ağ iletişiminde kullanılan RJ-45 konnektör ile telefon bağlantıları için kullanılan RJ-11 veya RJ-12 konnektörleri için sıkma işlemini de yapabilir.

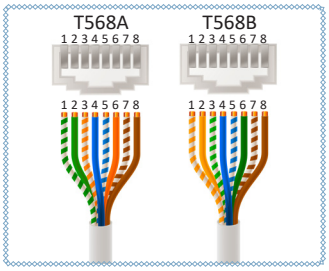
Kablo Test Cihazı

Hazırlanan ağ kablosu kullanılmadan önce test edilmelidir. Kullanım türüne göre sıralanmış (T568A veya T568B) kablo telleri, konnektörlere takılır ve sıkma işlemi yapılır. Kablo uçlarının bağlı olduğu küçük LED lambalarla kontrol yapılabileceği gibi dijital kablo test cihazları da aynı amaçla kullanılır. Hazırlanan kablonun veri iletimini doğru bir şekilde yapıp yapmadığı kontrol edildikten sonra kablo kullanıma hazırdır. Görsel 2.5'te kablo test cihazı bulunmaktadır.

2.1.1.4. Kablolama Standartları

Konnektöre takılmadan önce kablo uçlarının belirli bir dizilimle sıralanması gerekir. Görsel 2.3'te konnektör pinleri görülmektedir. Kablo sıralamaları EIA / TIA-T568 standardı ile belirlenir. Standart içinde **T568A** ve **T568B** olmak üzere iki bağlantı şeması önerilir.

Tablo 2.3'te T568A ve T568B bağlantı pin sırası verilmiştir. Genellikle şema olarak **T568B** kullanılır. Bağlantının ve veri iletiminin sorunsuz devam etmesi açısından konnektör bağlantısının ve değişikliğinin standartlara göre gerçekleştirilmesi önemlidir.



Görsel 2.3: T568A ve T568B kablo standartları

Tablo 2.3: T568A ve T568B Bağlantı Pin Sırası

T568A		
Pin	**Veri**	**Renk**
1	TX+	Beyaz / Yeşil
2	TX-	Yeşil
3	RX+	Beyaz / Turuncu
4		Mavi
5		Beyaz / Mavi
6	RX-	Turuncu
7		Beyaz / Kahverengi
8		Kahverengi

T568B		
Pin	**Veri**	**Renk**
1	TX+	Beyaz / Turuncu
2	TX-	Turuncu
3	RX+	Beyaz / Yeşil
4		Mavi
5		Beyaz / Mavi
6	RX-	Yeşil
7		Beyaz / Kahverengi
8		Kahverengi

Kablo dizilimi belirlemede dikkat edilecek diğer bir nokta da kablonun kullanılacağı ortamdır. Cihazlar arasındaki seri haberleşmede verici [TX (transmitter)] ve alıcı [RX (receiver)] uçların karşılıklı gelmesi gerekir. Kablo uçları, cihazların türüne göre **düz** (straight) veya **çapraz** (cross) olarak belirlenir.

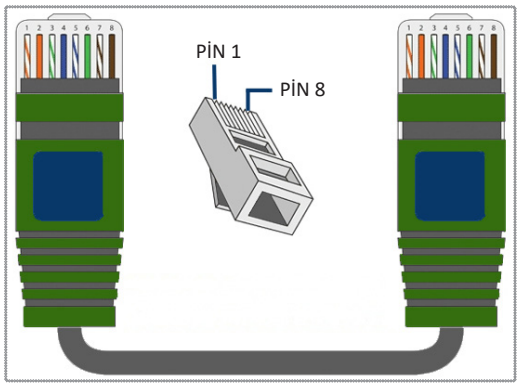
Düz Bağlantı: Kablo, bir bilgisayar ve ağ cihazı arasına veya iki farklı ağ cihazı arasına takılacaksa kablonun her iki ucundaki konnektör de aynı standarda göre hazırlanmalıdır (T568A-T568A ya da T568B-T568B).

Çapraz Bağlantı: Kablo, bir bilgisayardan diğer bilgisayara takılacaksa kablonun uçlarındaki konnektörler birbirinden farklı standartlara göre hazırlanmalıdır (T568A-T568B ya da T568B-T568A).

Uygulama 1

http://kitap.eba.gov.tr/KodSor.php?KOD=21029

Bir bilgisayar ile bir ağ cihazı arasında kullanılmak üzere yönergeler doğrultusunda Görsel 2.4'teki gibi ağ kablosu hazırlayınız. Sonlandırıcı olarak RJ-45 kullanınız.



Görsel 2.4: T568B standarına göre dizilmiş çift bükümlü kablo tellerinin konnektöre takılması

Adım 1: Uygulama yapmak istediğiniz kablo türünü seçiniz.

Adım 2: Uygulama yapılacak kablonun uzunluğu doğrultusunda kablo üzerindeki bilgilere göre kabloyu kesiniz.

Adım 3: Kablo soyucu ve sıyırıcı ile kablonun kılıfını (koruyucu plastik) açınız. Açılacak kısım 1,5 cm ile 2 cm aralığında olmalıdır. Daha az kısım açılması çalışmayı zorlaştırırken fazla kısım açılması konnektöre yerleştirmeyi zorlaştırır.

Adım 4: Bir kablo standardı seçiniz ve seçmiş olduğunuz standarta göre kablo dizilimini gerçekleştiriniz (Görsel 2.4). Yapılmak istenen kablo, bilgisayar ile ağ cihazı arasında kullanılacağından **düz bağlantı standardına** göre hazırlanmalıdır.

Adım 5: Kablo tellerini sıralamaya uygun şekilde RJ-45 konnektör içine yerleştiriniz.

Adım 6: Konnektörü, pense yardımı ile kablo hareket etmeyecek şekilde sıkınız.

Adım 7: Kablonun konnektöre doğru bir şekilde ve yeterli sıkılıkta takılıp takılmadığını kontrol ediniz.

2.1.2. Kablo Test Cihazının Kullanılması

Ağ iletişiminde kullanılacak kablolar hazırlandıktan sora mutlaka test edilmelidir. Kabloların yapımı sırasında gözden kaçan bir durum veya yapılan bir hata kablonun doğru çalışmasını engelleyebilir. Bu durum, veri iletimini imkânsız hâle getirebileceği gibi istenilen hızda iletişimin yapılamaması gibi sorunlara neden olabilir. Bu sebeplerle kabloların doğru şekilde çalışıp çalışmadığını test etmek için geliştirilmiş kablo test cihazlarına ihtiyaç duyulmaktadır.

Kullanılan test cihazları, TIA (Telecommunications Industry Association) veya ISO/IEC (International Organization for Standards) ile uyumlu olmalıdır. Günümüzde ağ kablolarının testi için **Fluke testi** uygulanmaktadır (Fluke Networks tarafından yayınlanmıştır.). Bu test, bir Ethernet kablosunun kalitesini anlamak için en etkili kriter olarak kabul edilmektedir.

Araştırma

Fluke testinde uygulanan prosedürler nelerdir? Bu test ile neler ölçülür? Bu testin yapılması ne gibi faydalar sağlar? Araştırınız ve bulduğunuz sonuçları sınıf arkadaşlarınızla paylaşınız.

2.1.2.1. LED Lambalı Kablo Test Cihazı

Yaklaşık 300 metreye kadar test yapabilen bu cihazlar piyasada rahatlıkla bulunabilir. Bu tür cihazlarda genellikle RJ-45 test edilebilmektedir. Test edilecek kablonun bir ucu test cihazının ana modülüne, kablonun diğer ucu test cihazının yan modülüne bağlanır (Görsel 2.5). Ana modül üzerindeki test düğmesine basılarak belirlenen standarda göre LED lambaların yanma sırası gözlemlenerek test işlemi uygulanır.

Görsel 2.5: LED lambalı kablo test cihazı ve kullanımı

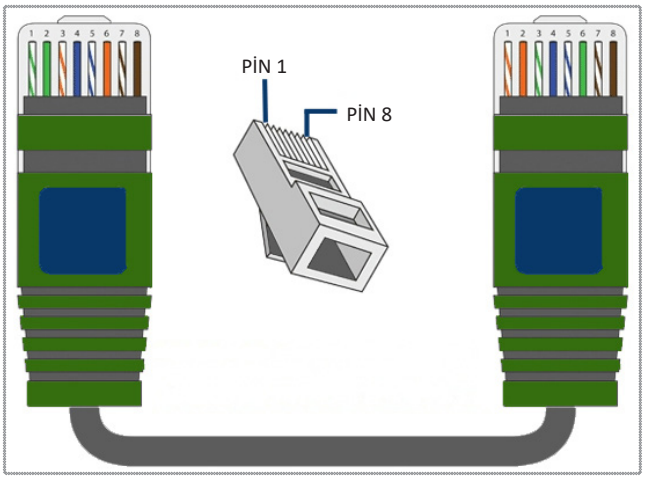
2.1.2.2. Dijital Kablo Test Cihazı

LED lambalı test cihazlarına göre daha uzun mesafelerde ölçüm yapabilen dijital kablo test cihazları, düz bağlantı, çapraz bağlantı, açık bağlantı, kırık tel gibi testleri de gerçekleştirebilmektedir. Bazı modellerde ağ haritası da çıkartılmaktadır (Görsel 2.6).

Görsel 2.6: Dijital kablo test cihazı ve kullanımı

Sıra Sizde

Görsel 2.7'deki çapraz bağlantılı ağ kablo yapısını referans alarak bir çapraz ağ kablosu hazırlayınız. Hazırladığınız kabloyu test cihazı ile test ediniz ve sonucunu öğretmeninize gösteriniz.



Görsel 2.7: Çapraz bağlantı türündeki ağ kablosu

2.2. Ağ Cihazları

Bilgisayarlar ve bilgisayar sistemleri arasında veri iletimi ve haberleşmenin yapılabilmesi için ihtiyaca göre birtakım ağ cihazları kullanılabilir. Kullanılacak ağ cihazlarının seçimi, ağ çeşidine ve fiziksel ortama göre değişebilmektedir.

2.2.1. LAN Ağında Kullanılan Ağ Cihazları

Kısa mesafeli yerel ağlarda kullanılan cihazlar; bilgisayar, bilgisayar sistemleri ve diğer ağ cihazları arasında veri iletimi ve haberleşme amacıyla kullanılmaktadır. Ağ yapısı bu tür cihazların birbirine bağlanmasıyla oluşur. Kullanılan ağ cihazları, ağın özelliklerini ve işlevini belirler. Tablo 2.4'te bu ağ cihazlarının isimleri ve OSI referans modelinde yer aldıkları katmanlar gösterilmiştir.

Tablo 2.4: LAN Cihazları ve OSI Modelinde Çalıştığı Katmanlar

Ağ Cihazı	OSI Modelindeki Katmanı	Açıklaması ve Görevi
Tekrarlayıcı (Repeater)	Fiziksel (Katman 1)	**Tekrarlayıcılar**; ağ sinyallerini alan, onları tam güce geri getirmek için güçlendiren ve ardından bunları ağdaki başka bir düğüme yeniden ileten, ağın fiziksel katmanındaki düşük seviyeli bir yerel iletişim cihazıdır. Tekrarlayıcılar, bir ağda, sinyaller uzun mesafeler kat ettiğinde ortaya çıkan zayıflamaya karşı koymak ve LAN uzunluğunu belirtilen maksimumun üzerine çıkarmak dâhil olmak üzere çeşitli amaçlarla kullanılır.
Merkez (Hub)	Fiziksel (Katman 1)	**Merkez (Hub)**; bir veriyi başka bilgisayar veya ağ cihazlarına gönderen aygıtlardır. Bir bilgisayar veya cihazdan veri paketi gönderildiğinde bu veriyi üzerinde mevcut tüm portlarına ileten ağ aygıtıdır.

Modem	Veri Ağı (Katman 2)	**Modem**, bilgisayarın telefon hatları ile bağlantısını kurarak ağa bağlanmasını sağlayan cihazlardır. **ADSL** ve **CSU / DSU** gibi yaygın iki tipi mevcuttur.
Ağ Arabirim Kartı (NIC)	Veri Ağı (Katman 2)	Bilgisayarların ve diğer cihazların bir ağa bağlanmasını sağlayan donanım bileşenine **ağ arabirim kartı (NIC)** denir. Ağ arabirim kartları, OSI referans modelinin **veri bağı (katman 2)** katmanında çalışır. Her ağ arabirim kartına, başka hiçbir ağ kartında olmayan bir numara tanımlanır. Bu numara o ağ kartını tanımlayan ayırt edici bir numaradır (adres). Bu adrese ortam erişim kontrol **MAC (Media Access Control) adresi** denir. 48 bit uzunluğundaki MAC adresi, altı çift hâlinde, on altılık sayı sisteminde ifade edilen **AA-8F-33-1E-0F-89** gibi bir adrestir. Bu adres, ağ arabirim kartı üzerinde bulunan **ROM yongasında** yazılıdır. Bluetooth ve Wi-Fi gibi ağ arabirim kart veya modülleri de eşsiz bir MAC adresine sahiptir.
Köprü (Bridge)	Veri Ağı (Katman 2)	Köprüler, tekrarlayıcı gibidir. Ancak bir tekrarlayıcının elektrik sinyallerini kuvvetlendirmesi bakımından farklılık gösterir. Köprüler veri bağı katmanında çalıştıkları için, dijital sinyalleri yükseltir. Gelen çerçeveleri dijital olarak kopyalar. Bir LAN'ın bir kısmından veya farklı teknolojiye sahip farklı bir LAN'dan gelen çerçevelerin başka bir LAN'a taşınmasını sağlar. Bununla birlikte hasarlı bir çerçeveyi bir ağdan diğerine veya aynı ağın başka bir kısmına gönderemez. Ağı MAC adreslerine göre ayırmak (segmentlere) için kullanılır. Köprüler, dinamik bir köprü tablosu kullanarak her segmentteki tüm cihazların MAC adreslerini kaydeder ve adres bilgilerine göre ağı segmentlere ayırır. Bu köprü tablosu oluşturma işlemi, cihazlar arasındaki trafik miktarının azaltılmasına yardımcı olur.
Kablosuz Erişim Noktaları (WAPs)	Veri Ağı (Katman 2)	**Erişim noktaları**; kablolu bir ağa, kablosuz erişim sağlamak için kullanılan kablosuz ağ cihazlarıdır. Erişim noktaları, kablosuz tarafta kullandıkları radyo frekansını (RF)tüm cihazlara paylaştırdığı için hublara benzer. Erişim noktaları, mevcut bir ağın kablosuz kapsama alanını genişletmek ve ona bağlanabilecek kullanıcı sayısını artırmak için kullanılır.
Anahtar (Switch)	Veri Ağı (Katman 2) veya Ağ (Katman 3)	**Anahtarlar**, bağlantı noktalarından (port) gelen veriyi MAC veya IP adresi bilgisine göre filtreleyerek ilgili portlardaki bilgisayar veya bilgisayarlara ileten ağ cihazlarıdır. Anahtar, gelen veriyi sadece istenilen cihaz veya cihazlara gönderirken hub ise veriyi tüm cihazlara gönderir ve sadece ilgili aygıt veriyi alır. Anahtarlar, her bağlantı noktasını kendi çarpışma etki alanı hâline getirir.
Yönlendirici (Router)	Ağ (Katman 3)	Yönlendiriciler, tüm ağ cihazları arasında en akıllı olanlardır. Verileri istenen bilgisayarlara iletmek için en verimli rotayı kullanmak üzere programlanabilir. OSI modelinin Ağ Katmanı 3 üzerinde çalışır ve veri paketlerini IP adreslerine göre bir ağdan diğerine yönlendirebilir.
Güvenlik Duvarı (Firewall)	Ağ (Katman 3) veya Uygulama (Katman 7)	**Güvenlik duvarları**, son kullanıcıları internetteki kötü niyetli trafikten koruyan donanım ve / veya yazılım sistemleridir. Veriler; internet üzerinden gönderildiğinde, verilerin nereden geldiği ve nereye gitmesi gerektiği hakkında bilgilerin yanı sıra, hangi uygulama için olduğuna dair bir gösterge ile paketlenmiş olarak gelir. Güvenlik duvarı; bir dizi kural tarafından belirlenen kriterleri karşılayıp karşılamadıklarını görmek için bu paketleri filtreler, kötü niyetli görünüyorsa atar, zararsız görünüyorsa ağa iletir. Örneğin; güvenlik duvarı, internetteki rastgele bir bilgisayarın ağınızın içindeki bilgisayara bağlanmaya çalıştığı yönünde veri akışı görürse verileri atar ve kullanıcıyı bağlantı girişiminde bulunma konusunda uyarır.

Ağa uygun LAN cihazları kullanım amacına göre ve çalışacağı katmana göre tercih edilir.

Sıra Sizde

Bilgisayarınızın ve kullandığınız mobil telefonunuzun MAC adresini öğreniniz. MAC adresini öğrendikten sonra bilgisayar ve mobil aygıtınızın MAC adreslerini karşılaştırınız. Arkadaşlarınız ile bulduğunuz MAC adreslerini inceleyiniz ve sonuçları sınıfınız ile paylaşınız.

2.2.2. LAN Cihazlarının Ağdaki Görevleri

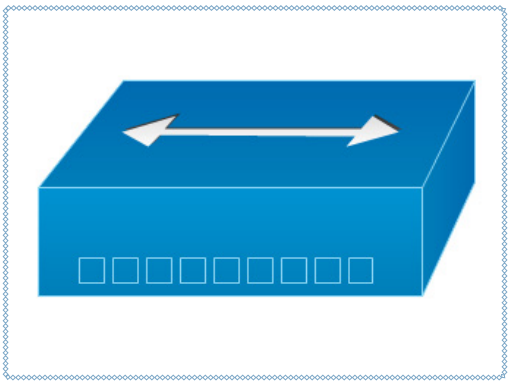
LAN cihazları, bilgisayarlar arası iletişim ve haberleşmenin en kısa sürede, en az kayıpla yapılması amacıyla kullanılır. Bu nedenle ağa en yüksek verimi sağlayacak şekilde yerleştirilir. Günümüzde kullanılan LAN cihazları, teknolojik gelişmeye ve ağ trafiğinin artmasına bağlı olarak gelişimlerini sürdürmektedir.

Ağ büyüdükçe ağın performansını artırmak için daha küçük ağlara veya ağ segmentlerine bölünmesi gerekir. Ağda çok fazla bilgisayar bulunması ağ trafiğinde tıkanıklığa neden olabilir. Aynı anda çok fazla paket iletildiğinde ağın performansı düşer. Büyük ağlar, ağ trafiği tıkanıklığını önlemek için genellikle küçük ağ segmentlerine bölünür. Bu şekilde gruplandırılmış ağlar ortaya çıkar. Ortaya çıkan ağ grupları kendi aralarında iletim ve haberleşme yaparken diğer ağ veya ağ grupları ile iletişime geçmek için ağların arasına yerleştirilmiş bir ağ cihazına ihtiyaç duyar. Bu cihazlar, bir ağdan gelen trafiği diğer ağa aktarmak / aktarmamak ve iletişimi başlatmak / bitirmek gibi görevleri üstlenir. Bir ağın alt ağa bağlanması anahtar, yönlendirici ve köprü gibi ağ aygıtları aracılığıyla mümkündür. Dağıtıcılar (hub) ve erişim noktaları gibi bazı ağ cihazları da bir ağda yaygın olarak kullanılır.

2.2.3. Dağıtıcılar (Hub)

Dağıtıcı, bir veriyi başka bilgisayar veya ağ cihazlarına gönderen aygıta denir. Genellikle **hub** olarak bilinir. Hub, yalnızca fiziksel katmanda çalışan bir cihazdır. Bir ağ içinde bilgi taşıyan sinyaller zayıflamadan, verilerin bütünlüğünü tehlikeye atmadan önce sabit bir mesafeye gidebilir. Tekrarlayıcı bir sinyali alır ve bu sinyali çok zayıflamadan veya bozulmadan önce orijinal bit modelini yeniden oluşturur. Daha sonra yenilenmiş sinyali tekrar gönderir. Geçmişte Ethernet LAN'lar, veri yolu (bus) topolojisini kullanırken koaksiyel kablonun uzunluk kısıtlamasının üstesinden gelmek için bir LAN'ın iki bölümünü bağlamak için bir tekrarlayıcı kullanılmaktaydı. Ancak günümüzde Ethernet LAN'lar yıldız topolojisini kullanmaktadır. Yıldız topolojide bağlantı noktası olarak hizmet eden ve aynı zamanda bir **tekrarlayıcı** olarak görev alan çok bağlantı noktalı cihaza **hub** denir (Görsel 2.8).

Bir bilgisayar veya cihazdan veri paketi gönderildiğinde hub, bu veriyi üzerindeki mevcut tüm portlara iletir. Hub kullanılan ağlar, fiziksel olarak yıldız topolojisine benzese de verinin tüm portlara iletilmesi nedeniyle mantıksal olarak veriyolu (bus) topolojisi gibi çalışır. Bu, ağ üzerinde çarpışma oluşmasına ve ağın yavaşlamasına sebebiyet verebilir. Gelen veri, ağdaki tüm istasyonlara gönderildiği için güvenlik açığı oluşabilir. Hub'lar günümüzde tercih edilmediği için üretilmemektedir.

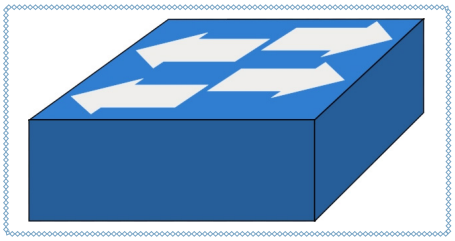


Görsel 2.8: Hub sembolü

2.2.4. Anahtarlar (Switch)

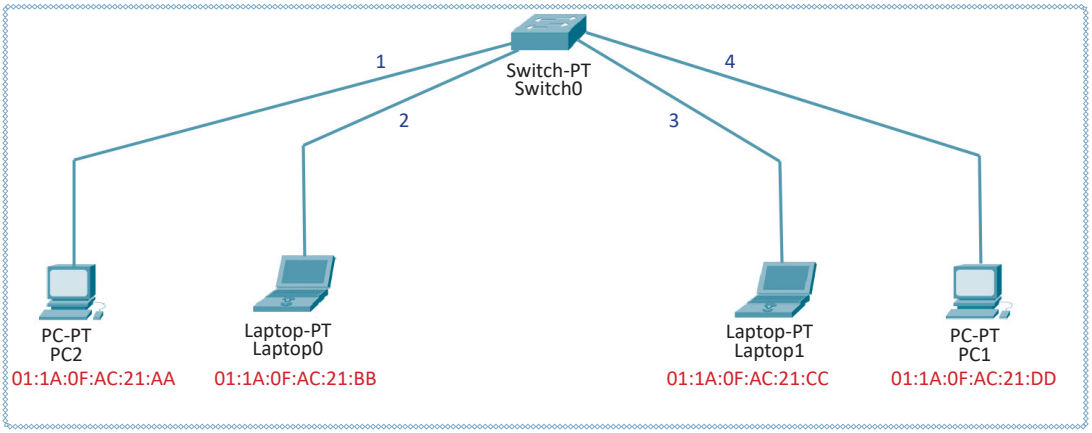
Anahtar, ağ segmentlerini veya Ethernet, token, ring LAN'lar gibi iki küçük ağı birbirine bağlayan ağ cihazıdır. Köprü gibi dinamik bir tablo yardımıyla ağdaki çerçeveleri filtreler ve iletir. Bu noktadan noktaya yaklaşım; anahtarın aynı anda birden fazla segment çiftini bağlamasına izin vererek, birden fazla bilgisayarın aynı zamanda veri iletmesine izin verir (Görsel 2.9). Anahtarların, gelen veriyi **MAC** ya da **IP adresi** bilgisine göre filtreleyerek ilgili portlardaki bilgisayar veya bilgisayarlara ileten ağ cihazları olması sebebiyle hub ve köprülere göre performansları daha yüksektir.

Anahtarlar ilk geliştirildiklerinde, statik olan anahtarlama tabloları oluşturulurdu. Sistem yöneticisi, anahtar kurulumu sırasında her tablo girişini manuel olarak (el ile) yapmak zorundaydı. Süreç basitti ama pratik değildi. Bir bilgisayarın ağa eklenmesi veya ağdan silinmesi durumunda tablonun manuel olarak değiştirilmesi gerekiyordu. Bilgisayara yeni bir ağ kartı takıldığında MAC adresini de tanımlamak gerekiyordu.



Görsel 2.9: Anahtar sembolü

Statik tabloya daha iyi bir çözüm arayışı ile adresleri bağlantı noktalarına (arayüzlere) otomatik olarak eşleyen çerçevelerin hareketlerinden kademeli olarak öğrenen, dinamik tablolar geliştirilmiştir. Bunu yapmak için anahtar, anahtardan geçen her çerçevede hem hedef adresini hem de kaynak adreslerini inceler. Hedef adres, yönlendirme için kullanılır (tablo araması). Kaynak adresi ise tabloya giriş eklemek ve güncelleme amacıyla kullanılır. Görsel 2.10'da bu süreç detaylandırılmıştır.



Görsel 2.10: Basit anahtar ağ yapısı

1. PC2 bilgisayarı, PC1 bilgisayarına bir çerçeve gönderdiğinde anahtar, PC2 veya PC1 için herhangi bir bilgiye sahip değildir (Görsel 2.11.a). Çerçeve, üç bağlantı noktasının (portunun) hepsinden gönderilir. Anahtar, kaynak adresine bakarak PC2 bağlantı noktasının 1 numaralı porta bağlandığını öğrenir. Bu, gelecekte PC2'ye yönelik çerçevelerin bağlantı noktası 1 üzerinden gönderilmesi gerektiği anlamına gelir. Anahtar, PC2 bilgisayarının MAC adres bilgisini bu port için kendi tablosuna ekler. Tablonun ilk girişi yapılmıştır (Görsel 2.11.b).

Adres	Port

Görsel 2.11.a: Anahtar tablosu boş

Adres	Port
01:1A:0F:AC:21:AA	1

Görsel 2.11.b: PC1'in MAC bilgisinin tabloya işlenmesi

2. PC1 bilgisayarı, Laptop0 bilgisayarına bir çerçeve gönderdiğinde anahtarın bu bilgisayar için herhangi bir bilgisi yoktur (tabloya işlenmiş bir bilgi). Bu nedenle ağı yeniden tarar. Bu sırada, PC1 bilgisayarın MAC bilgisini tabloya ekler (Görsel 2.12).

Adres	Port
01:1A:0F:AC:21:AA	1
01:1A:0F:AC:21:DD	4

Görsel 2.12: PC0'ın MAC bilgisininde switch tablosuna eklenmesi

3. Öğrenme süreci, tablo her bağlantı noktası hakkında bilgi alana kadar devam eder (Görsel 2.13). Ancak öğrenme sürecinin uzun sürebileceği unutulmamalıdır. Örneğin, bir bilgisayar bir haberleşme isteği veya veri göndermezse bilgisayarın bilgileri tabloya hiçbir zaman eklenmez.

Adres	Port
01:1A:0F:AC:21:AA	1
01:1A:0F:AC:21:DD	4
01:1A:0F:AC:21:BB	2
01:1A:0F:AC:21:CC	3

Görsel 2.13: Tüm anahtar portlarına bağlı bilgisayarların MAC bilgilerinin tabloya işlenmesi

Uygulama 2

http://kitap.eba.gov.tr/KodSor.php?KOD=21030

Ağ simülatör programını kullanarak Görsel 2.14'te gösterilen yerel alan ağ yapısını oluşturunuz. İşlemi aşağıdaki yönergeler doğrultusunda gerçekleştiriniz.

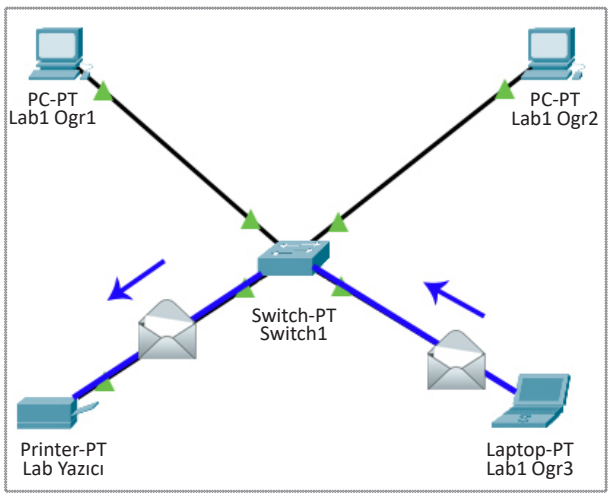
Adım 1: Ağdaki bilgisayarlara el ile IP adresi ve DNS adresi ataması yapınız.

Adım 2: Cihazların MAC adreslerini öğreniniz.

Adım 3: Anahtar MAC ve IP tablosunu inceleyiniz.

Adım 4: Ağda anahtar cihaz üzerinden veri iletimini gerçekleştiriniz.

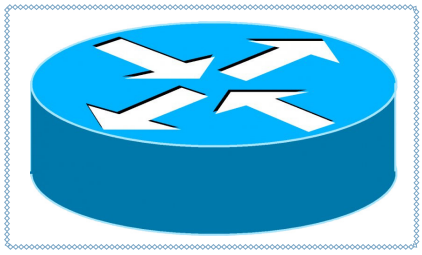
Adım 5: Simülasyon oluşturarak paketlerin hareketini gözlemleyiniz.



Görsel 2.14: Anahtar uygulaması

2.2.5. Yönlendiriciler (Router)

Yönlendirici, mantıksal ve fiziksel olarak farklı iki veya daha fazla ağı birbirine bağlamak için kullanılan ağ iletişim cihazıdır. Bu cihazlar; ağlar arasındaki paketlerin başlığındaki hedef adres bilgilerini, yönlendirme tablosu ile karşılaştırarak yönlendirme kararlarını verip aktarımını gerçekleştiren kontrol merkezi niteliğindeki cihazlardır (Görsel 2.15).



Görsel 2.15: Yönlendirici sembolü

Yönlendiriciler, LAN'ı başka bir LAN'a, LAN'ı WAN'a veya bir LAN'ı internete bağlamak için kullanılabilir. Yönlendiriciler, IP adresi temelinde çalıştıkları için OSI referans modelinin ağ katmanında çalışır ve IOS olarak bilinen yerleşik işletim sistemine sahiptir. Bu işletim sistemi üzerinden programlanabilir. Uzak bir ağa erişmek için mevcut yollardan en iyisini seçerek yönlendirme işlemini yapabillir.

Ağdaki bir yönlendiricinin, herhangi bir paketin hedef adresine bakıp ardından paketi o adrese ulaştırmak için hangi çıkış bağlantı noktalarının (portunun) en iyi seçenek olduğunu belirlemesi gerekir. Yönlendirici bu kararı, bir yönlendirme tablosuna bakarak alır. Yönlendirmenin en önemli kısmı, veri iletimi yapılacak herhangi iki düğüm arasındaki en düşük maliyetli yolu bulmaktır.

Yönlendirme işlemi için bazı yönlendirme protokolleri bulunmaktadır.

Yönlendirici Bilgi Protokolü [RIP (Router Information Protocol)]: RIP, uzaklık-vektör tabanlı bir yönlendirme protokolüdür. Bu protokolü çalıştıran yönlendiriciler, kendi yönlendirme tablolarının tamamını belirli aralıklarla (30 saniye gibi) bütün portlarından komşu yönlendiricilere gönderir. Yönlendiriciler, ulaşabildikleri yönlendiricilere kendilerine bağlı olan bilgisayar veya ağ cihazlarının bilgilerini paylaşır. Yönlendirme tablosunda; kaynak IP adresi, ağ geçidi, mesafe, port numarası, zamanlayıcılar gibi bilgiler kaydedilir. Bu sayede bir yönlendirici, hedefe ulaşabilmek için hangi yol üzerinden gidebileceğini hesaplayabilir. RIP protokolü en iyi yolu seçerken en uygun yol atlama sayısına bakarak hesaplama yapar. Her varış adresi için en iyi yol bilgisi tabloda tutulur. Uygulamada RIP için atlama sayısının en fazla 15 olacağı kabul edilmiştir. Bu değerden daha uzak yerler, ulaşılmaz durum olarak değerlendirilir. Atlama sayısı 16 ve daha büyükse bu hedef **ulaşılamaz (unreachable)** olarak nitelendirilir.

Avantajları

- Küçük ağlarda RIP kullanımı basit ve kolaydır. Bu yüzden yaygın olarak kullanılan bir protokoldür.

Dezavantajları

- En fazla 15 atlamaya imkân verir.
- Doğrudan bağlı olan komşu yönlendiricilere sürekli ve belirli aralıklarla yönlendirme tablosunu gönderdiği için ağ trafiği artar.
- Büyük ağlarda sorunlara neden olmaktadır.

İlk Açık Yöne Öncelik Protokolü [OSPF (Open Shortest Path First)]: RIP protokolünde bulunan bazı eksik yanları gidermek ve düzeltmek için geliştirilmiş bir yönlendirme protokolüdür. Bu protokolde yönlendiriciler, ağdaki iki nokta arasında bulunan tüm yolların bilgisine ulaştıktan sonra **SPF** [Shortest Path First (Önce En Kısa Yol)] algoritmalarını kullanarak hangi yolun en iyisi olduğuna karar verir. OSPF algoritması, gidilmek istenilen herhangi bir yere bizi en kısa yoldan ulaştıran navigasyon cihazlarına benzetilebilir. Hedefe gidilecek en kısa yolu seçtikten sonra her 10 saniyede bir, küçük "hello" paketleri göndererek bağlantının canlı kalması sağlanır. OSPF ile haberleşen yönlendiriciler; gidilecek yön bilgisini paylaşmak için komşu, yani her bacağının bağlı olduğu yönlendiricilerin bilgilerini bilir. OSPF, cihazlar arası bilgi paylaşımı yaparak tablo bilgileri gibi verileri de tüm yönlendiriciler ile paylaşır.

Avantajları

- OSPF protokolü uzaklık vektörü protokolleri gibi metrik kullanmaz. Herhangi bir basamak sayısı sınırlaması yoktur.
- Yol bilgisi daha hızlı öğrenilir.
- Büyük ağları destekler.

Dezavantajları

- Yapılandırılıp yönetilmesi daha zordur.

Uygulama 3

Üç yönlendiricinin olduğu bir ağda OSPF protokollerini kullanarak yönlendirme tablosunu elde ediniz. İşlemi aşağıdaki yönergeler doğrultusunda gerçekleştiriniz.

Adım 1: Üç adet yönlendirici yerleştiriniz ve seri porttan birbirlerine bağlayınız.

Adım 2: IP bloklarını yapılandırarak tüm yönlendiricilerin konfigurasyon ayarlarını yapınız.

Örneğin:
Yönlendirici 1 için: 192.168.1.10/24
Yönlendirici 2 için: 192.168.1.20/24
Yönlendirici 3 için: 192.168.1.30/24

Adım 3: Yönlendirici üzerinde OSPF yapılandırmasını yapınız. Bunun için aşağıdaki komutları kullanınız veya kendinize referans edininiz ve diğer 2 yönlendirici için aynı işlemleri yapınız.

```
Router adı# conf t
Router adı(config)# router ospf 10
Router adı(config-router)# network 192.168.1.10 0.0.0.255 area 0
Router adı(config-router)# network 10.1.1.0 0.0.0.2 area 0
Router adı(config-router)# end
```

Adım 4: Yapılandırma tamamlanınca simülasyonu çalıştırınız ve ağ tablolarına ulaşınız.

Sıra Sizde

Üç yönlendiricinin bulunduğu bir ağda RIP protokollerini kullanarak yönlendirme tablosunu elde ediniz. Elde ettiğiniz tabloyu öğretmeninize gösteriniz.

2.2.6. Kablosuz Erişim Noktaları (Access Point)

Bir erişim noktası (AP), teknik olarak kablolu veya kablosuz bağlantı içerebilirken genellikle kablosuz cihaz anlamına gelir. Bir AP ikinci OSI katmanında, veri bağlantısı katmanında çalışır. Standart bir kablolu ağı kablosuz aygıtlara bağlayan bir köprü olarak veya veri aktarımlarını erişim noktasından diğerine geçiren bir yönlendirici olarak

çalışabilir. Kablosuz erişim noktası, kablolu bir ağı kablosuz hâle çevirerek dizüstü bilgisayar ve tablet gibi kablosuz aygıtlara radyo dalgaları ile ağ erişimi sağlar.

Kablosuz erişim noktaları (WAP), bir kablosuz LAN (WLAN) oluşturmak için kullanılan bir verici ve alıcı (alıcı-verici) cihazdan oluşur. Erişim noktaları tipik olarak yerleşik bir anten, verici ve adaptöre sahip ayrı ağ cihazlarıdır. Ağın boyutuna bağlı olarak tam kapsama sağlamak için bir veya daha fazla AP gerekebilir. Daha fazla kablosuz istemciye erişim sağlamak ve kablosuz ağın menzilini genişletmek için ek AP'ler kullanılır.

Bir kablosuz AP'ye bağlanmak için hizmet seti tanımlayıcı (SSID) adına ihtiyaç vardır. 802.11 kablosuz ağları, aynı ağa ait olan tüm sistemleri tanımlamak için SSID'yi kullanır. İstemci istasyonlarının AP'ye kimlik doğrulaması için SSID ile yapılandırılması gerekir. AP, SSID'yi yayınlayarak bölgedeki tüm kablosuz istemcilerin AP'nin SSID'sini görmesine izin verebilir. Güvenlik nedenleriyle AP'ler, SSID'yi yayınlamayacak şekilde yapılandırılabilir; bu da yöneticinin, istemci sistemlere SSID'yi otomatik olarak keşfetmesine izin vermek yerine, izin vermesi gerektiği anlamına gelir. Kablosuz cihazlar; varsayılan SSID'ler, güvenlik ayarları, kanallar, şifreler ve kullanıcı adlarıyla birlikte gönderilir. Güvenlik nedenleriyle bu varsayılan ayarları mümkün olan en kısa sürede değiştirmek tavsiye edilir. Çünkü birçok internet sitesi, üreticiler tarafından kullanılan varsayılan ayarları listelemektedir.

Uygulama 4

Bir kablosuz erişim noktası cihazını ağınıza ekleyiniz. Bu işlemi aşağıdaki yönergeler doğrultusunda gerçekleştiriniz.

Adım 1: Kablosuz erişim noktasını bir ağ kablosu ile bilgisayara bağlayınız. Bunun için düz bağlantıya sahip bükümlü kablo kullanabilirsiniz.

Adım 2: Kablosuz erişim noktasına güç veriniz. PoE [Power Over Ethernet (Ethernet Üzerinden Güç)] destekli bir cihaz için elektrik kablosuna gerek yoktur. Çalışması için gerekli enerjiyi doğrudan Ethernet üzerinden alacaktır.

Adım 3: Kablosuz erişim noktasının IP adresini, bilgisayardaki web tarayıcısına yazınız ve erişim noktasının web arayüzüne bağlayınız. Genellikle 192.168.0.1 veya 192.168.1.1 gibi IP adresleri verilmiştir. Bunun için cihaz veya kutusu üzerine bakınız.

Adım 4: Kablosuz erişim noktasını, web arayüzündeki ayarlardan "Etkinleştir" yapınız.

Adım 5: Aynı arayüz içinde SSID tanımlaması yapınız. SSID, ağı tanımlamak için kullanılan "Hizmet Kümesi Tanımlayıcısıdır". Çoğu erişim noktasının üretici firma tarafından ayarlanmış, varsayılan bir ismi bulunmaktadır. Ağ özelleştirmesi ve güvenlik için kendine özgü bir isim atayınız.

Adım 6: WEP şifrelemesini aktifleştiriniz ve tahmin edilmesi zor bir şifre belirleyiniz.

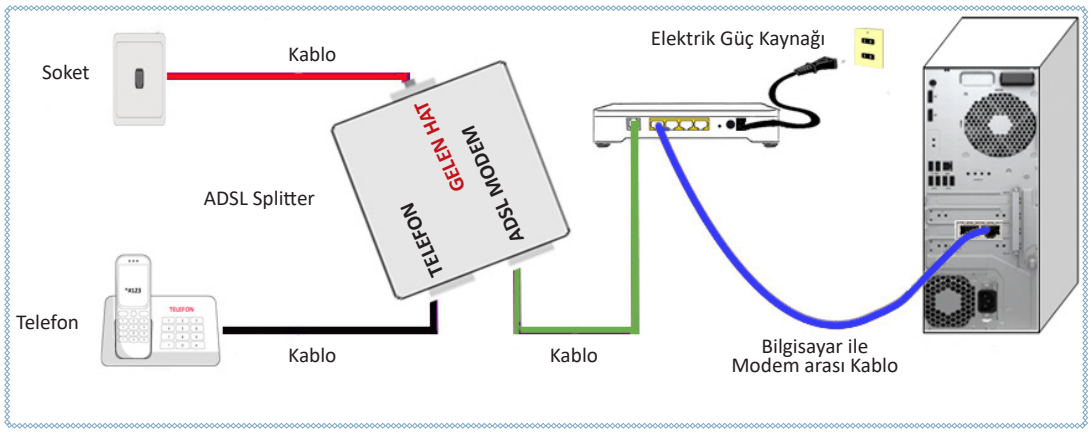
Adım 7: MAC adresi filtrelemeyi kullanarak güvenliği daha da arttırınız. Bu işlem, MAC adreslerine göre ağa erişmesine izin verilen veya reddedilen kablosuz ağ istemcilerinin bir listesini oluşturmaya yardımcı olur.

Adım 8: Birbirine yakın birden fazla erişim noktası varsa bunları, farklı kanallarda yayın yapacak şekilde ayarlayınız. Yayın yapılan 11 kanaldan birini seçiniz. Kablosuz ağdaki tüm erişim noktaları ve bilgisayarlar, aynı kanalı kullanmalıdır. Bilgisayarlar sık sık bağlantılarını kaybediyorsa başka bir kanala geçiniz.

2.2.7. Modem

Bilgisayarın, telefon hatları ile bağlantısını kurarak ağa bağlanmasını sağlayan cihazlardır. Bilgisayardan aldıkları digital verileri analog sinyallere dönüştürerek telefon hatlarına aktarılmasını sağlar. Haricî olarak bilgisayara takılıp kullanılır. DSL ve optik gibi daha hızlı türleri de modemler arasında kullanılmaktadır. Günümüzde daha çok iki türde modem kullanılmaktadır.

ADSL Modem: ADSL, Asimetrik Dijital Abone Hattı anlamına gelir. Bakır telefon çiftlerinin, geniş bant bağlantısı sağlamak için kullanılan bir ağ teknolojisidir. Bilgisayar ve ADSL modemi açıldığında otomatik olarak kurulan bir ağ bağlantısı sağlar (Görsel 2.16).

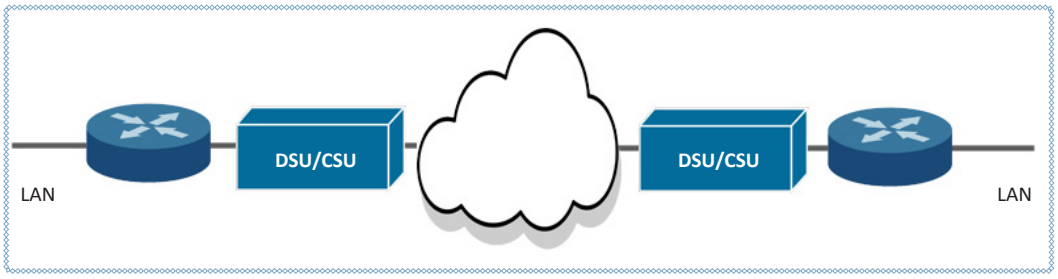


Görsel 2.16: ADSL bağlantı şeması

Sıra Sizde

İhtiyacınız olan telefon kablosu ve UTP kablo kullanarak Görsel 2.16'daki gibi bir ADSL bağlantısı gerçekleştiriniz. Tamamladığınız çalışmanızı öğretmeninize gösteriniz.

CSU/DSU Modemler: CSU/DSU modemler iki farklı dijital sinyali birbirine dönüştürmek için kullanılır. Buradaki iki farklı sinyal yerel alan ağından veya geniş alan ağından gelen veri çerçevesidir (data frame). Bu modemler yerel alan ağındaki verinin geniş alan ağı verisine veya geniş alan ağındaki verinin yerel alan ağı verisine dönüştürülmesini sağlayan cihazlardır. Aynı zamanda bu modemler fiziksel katmanda hata tespiti de yaparlar (Görsel 2.17).



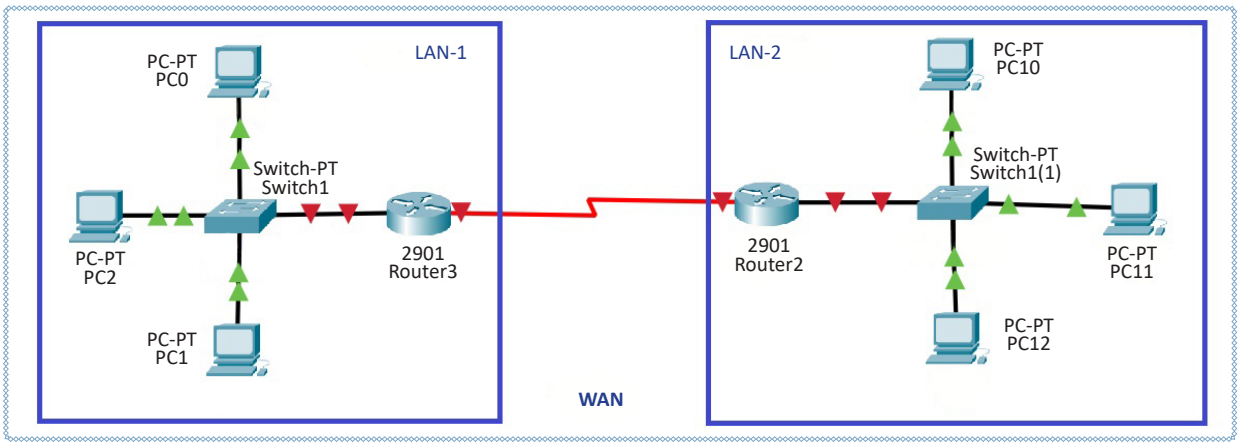
Görsel 2.17: CSU/DSU iletim görseli

2.2.8. Ağ Çeşidine Göre Ağ Cihazı Seçme

Bir bilgisayar ağına yeni cihazlar eklenmesi ile ağ giderek büyür. Bununla beraber ağın yönetimi zorlaşır ve ağ performansı düşer. Bu nedenle ağ yöneticileri bütün ağı küçük ağlara böler. Bir ağın daha küçük ağ bölümlerine bölünmesine **alt ağ oluşturma** denir.

Bir ağın alt ağa bağlanması yalnızca anahtarlar, yönlendiriciler ve köprüler gibi ağ aygıtları aracılığıyla mümkündür. Erişim noktaları gibi diğer bazı ağ cihazları da bir ağda yaygın olarak kullanılır. Bu ağ cihazları olmadan veriler, LAN veya WAN ağında bir bilgisayardan diğerine aktarılamaz. Bu cihazlar, bir segmentten diğerine veri iletişimi yapmak için tüm yerel ve uzak ağ segmentlerini birbirine bağlar. Büyük bir ağın iki önemli cihazı, yönlendirici ve anahtardır. Uygun şekilde yerleştirilmiş ve yapılandırılmış yönlendiriciler, anahtarlar gibi ağ cihazlarına sahip (iyi bir altyapıya sahip) bir bilgisayar ağı; genel işletim maliyetini düşürmede, performansı, yönetilebilirliği ve güvenilirliği artırmada etkili olur.

LAN tipi ağlarda genellikle anahtar, modem veya yönlendirici seçimi maliyet açısından uygundur. Genel olarak tek bir yönlendirici ve modem ile beraber kullanılacak anahtarlar yeterli olacaktır. Ancak daha büyük WAN gibi ağlarda ise yönlendiricilerin kullanımı büyük öneme sahiptir. WAN'ları oluşturan LAN'lar, yönlendiriciler aracılığı ile birbirine bağlanır (Görsel 2.18). LAN içinde küçük alt ağlar, anahtarlar aracılığıyla oluşturulabilir.



Görsel 2.18: LAN ve WAN kullanılan ağ cihazları

Sıra Sizde

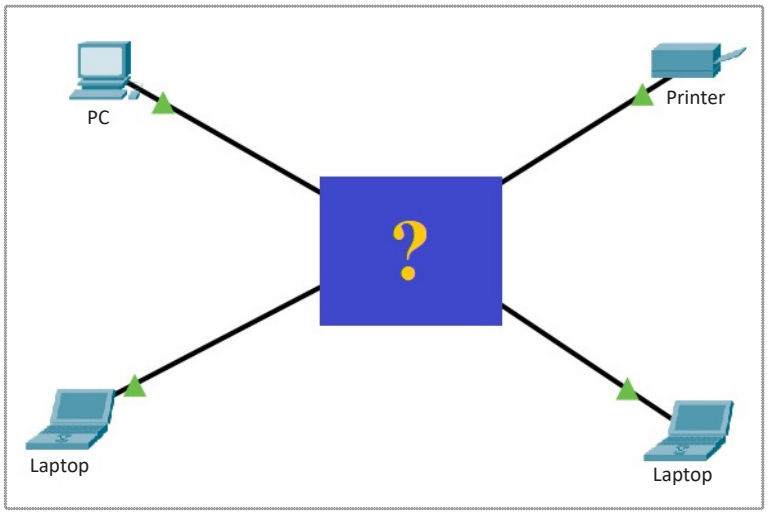
Bir arkadaşınızla birlikte evinizde 1 adet masaüstü bilgisayar, 2 adet dizüstü bilgisayar ve ortak kullanmak istediğiniz 1 adet yazıcıdan oluşan yerel bir ağ kurmak istediğinizi düşününüz (Görsel 2.19). Kurulan ağda tüm bilgisayarlar yazıcıya ulaşabilecek ve kullanılabilecektir. Bu duruma göre:

a. Uygun kablonun hangisi olduğunu açıklayınız.

b. Uygun ağ cihazının hangisi olduğunu açıklayınız.

c. Ağ simülatör programı içinde benzer bağlantıyı kurarak tasarladığınız ağ yapısını çalıştırınız ve test ediniz.

d. Oluşturduğunuz sistemin maliyetini göz önüne alarak daha düşük maliyet ile aynı sistemin oluşturulup oluşturulamayacağını açıklayınız. Sınıfınız ile paylaşınız.



Görsel 2.19: Örnek ağ bağlantı yapısı

A. Aşağıdaki cümlelerde parantezlerin içine yargılar doğru ise (D), yanlış ise (Y) yazınız.

1. ( ) Yaygın LAN / WAN cihazları hub'lar, köprüler, anahtarlar ve yönlendiricilerdir.
2. ( ) RJ-45 veri taşımada kullanılan bir konnektör çeşididir. RJ-11 konektörü ise telefon veya modem bağlantısı için kullanılır.
3. ( ) LAN, sınırlı alan içindeki bilgisayarları birbirine bağlayan bir bilgisayar ağıdır.
4. ( ) Ateş duvarları verileri olduğu gibi tüm portlarına dağıtan LAN cihazlarıdır.

B. Aşağıdaki soruları dikkatlice okuyunuz ve doğru seçeneği işaretleyiniz.

5. Aşağıdaki hangi kablo kombinasyonu çapraz kabloyu oluşturur?

A) T568A ve T568B
B) T568A ve T568A
C) T568B ve T568B
D) T568A ve T568C
E) T568B ve T568C

6. Aşağıdakilerden hangisi veri paketlerini LAN bölümleri arasında iletmek için tasarlanmış bir veri bağlantı katmanı (Katman 2) cihazıdır?

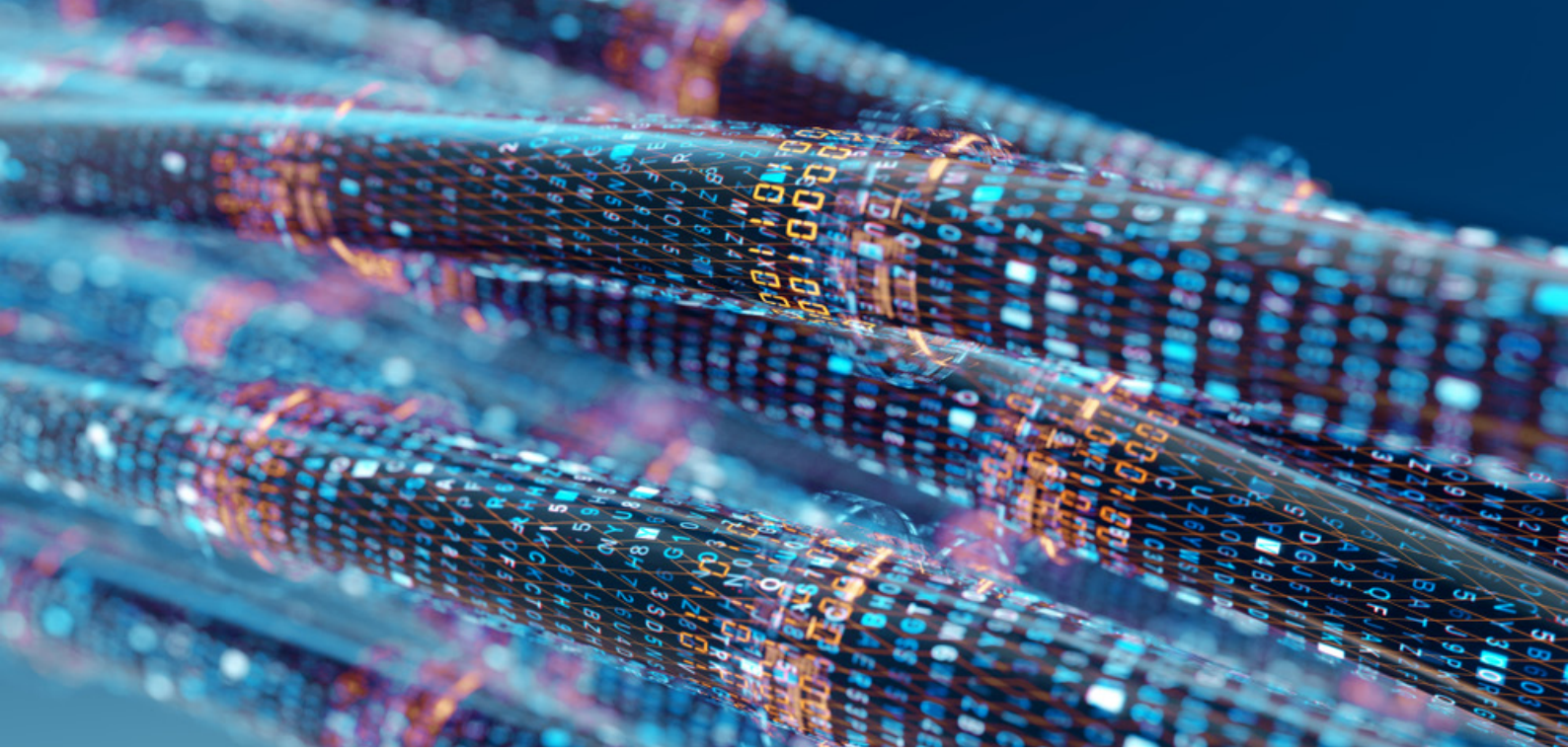
A) Anahtar B) Güvenlik Duvarı C) Dağıtıcı D) Köprü E) Yönlendirici

7. Aşağıdakilerden hangisi IP paketlerini farklı bilgisayar ağları arasında filtrelemek ve aktarmak için tasarlanmış cihaza ne ad verilir?

A) Switch
B) Güvenlik Duvarı
C) Hub
D) Yönlendirici
E) Yük dengeleyici

8. Aşağıdaki kısaltmalardan hangisi, hem verileri hem de elektrik gücünü, tek bir bükümlü çift Ethernet kablosu üzerinden taşımaya izin veren teknolojiyi ifade eder?

A) RJ-11 B) PoE C) MAC D) ADSL E) RJ-45



ÖĞRENME BİRİMİ 3

AĞ HİZMETLERİ

NELER ÖĞRENECEKSİNİZ?

Bu öğrenme birimi ile;

- İstemci ve sunucu kavramlarını öğrenecek,
- OSI (Open Systems Interconnection) modelini ve katmanlarını bilecek,
- TCP/IP modelini ve katmanlarını bilecek,
- TCP (Transmission Control Protocol) protokollerini kullanabilecek,
- UDP (User Datagram Protocol) protokolünü kullanabilecek,
- Port kavramını bilecek ve iyi bilinen port numaralarını uygulamalarda kullanabilecek,
- Portlaların dinlenmesini uygulayabilecek,
- TCP/IP uygulama katmanı protokollerinin simülasyon üzerinde uygulama yapmasını öğreneceksiniz.

ANAHTAR KELİMELER

OSI, TCP/IP, port, UDP, protokol

Hazırlık Çalışmaları

1. Farklı binalardaki bilgisayarlar birbirleri ile nasıl haberleşebilir? Kendi aralarında bir iletişim kuralı var mıdır, tartışınız.
2. Bilgisayarda çalıştırdığınız uygulamalar doğru verileri nasıl elde ediyor ve işlem yapıyor; düşüncelerinizi arkadaşlarınızla paylaşınız.

3.1. Ağ Hizmetlerinde İletim (Taşıma) Katmanı ve Port Kullanımı

Bilgisayarlar yapılandırmalarına göre ikiye ayrılır. Bunlar; kaynak ve hizmet sağlayan bilgisayarlar (sunucu bilgisayarlar), bu kaynak ve hizmeti talep eden bilgisayarlar (istemci bilgisayarlar) olarak nitelendirilebilir.

3.1.1. İstemci / Sunucu İlişkisi

İstemci Bilgisayarlar: Bir ağ üzerinde, uzaktaki bir sunucu bilgisayarlardan hizmet alan kullanıcı bilgisayarlarına **istemci (client)** denir. İstemcilerin bilgiye erişim yetkileri sunucular tarafından belirlenir.

Sunucu Bilgisayarlar: Bir ağ üzerinden istemciler olarak bilinen diğer bilgisayarlara; kaynaklar, veriler, hizmetler veya programlar sağlayan bir bilgisayar veya sistemdir. İstemciler sunucuya bağlanarak bu hizmet, kaynak veya verilerden faydalanabilir. Örneğin internete bağlı olan bir bilgisayar, herhangi bir internet sitesine ulaşmak istediğinde internet sitesi sunucu (server) olurken, ulaşım sağlayan bilgisayar ise istemci (client) rolünü üstlenir.

İstemci-Sunucu modeli, birden çok bileşenin iletişim kurmak için kesin olarak tanımlanmış rollerde çalıştığı bir bilgi işlem modelidir. Bu model, hizmet taleplerini başlatan istemcilerden, bu işlevi veya hizmeti sağlayan sunuculardan oluşan bir uygulamada, iş birliği yapan programlar arasındaki ilişkiyi belirtmektedir. Sunucu, istemci tarafından tüketilecek kaynakların ve hizmetlerin çoğunu barındırır, sunar ve yönetir. İstemciler ise ihtiyaç duyduğu işlevi sunuculardan talep eder.

Örneğin bir sunucu tarafından barındırılan bir web sitesine erişmek için bir istemci bilgisayarda çalıştırılan bir tarayıcı üzerinden URL girilir. DNS sunucusu, web sunucusunun IP adresini arar ve tarayıcıya gönderir. Tarayıcı bir HTTP veya HTTPS isteği oluşturur ve sunucu istenilen web sitesine ait dosyaları gönderir. İstemci bilgisayar bu dosyaları alır işler. Daha sonra iletişim için takip eden diğer talepleri gönderir. Sunucu gelen talepleri değerlendirir ve iletişim sürdürülür.

Farklı türdeki bilgisayarların ve ağ cihazlarının birbirleri arasındaki iletişimi organize eden, belirli bir düzene sokan, bazı modeller geliştirilmiştir. OSI Modeli ve TCP /IP Modeli bu modeller arasında en önemli olanlarıdır.

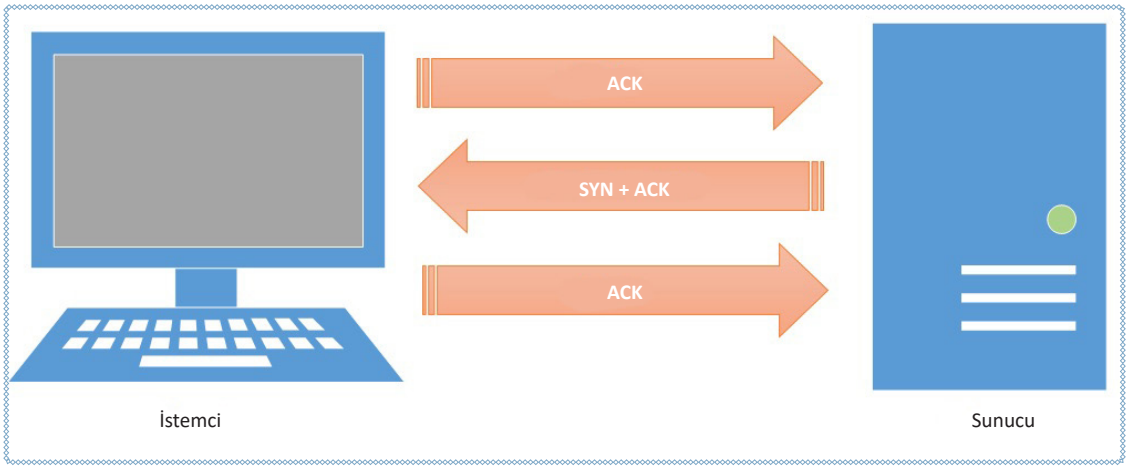
3.1.2. TCP Protokolü

Bağlantı temelli protokollerden biri olan TCP, internet protokolleri arasındaki en önemli protokollerden biridir. Bağlantı temelli bir protokoldür. İstemci ile sunucu arasında veri aktarılmadan önce bir bağlantı kurulması gerekir. TCP, noktadan noktaya güvenilir iletişim kuran bir protokoldür. Güvenilir olarak belirtilmesinin sebebi, verilerin sıralı ve kayıpsız bir şekilde teslim edilmesidir. TCP'de tanımlı temel görevler şu şekilde sıralanabilir:

- Bağlantı noktaları arasında veri iletişimini sağlama
- Güvenli veri iletimi sağlama
- Bağlantıda olan iki bilgisayar arasında akış kontrolü sağlama
- Çoklama (Multiplexing) yöntemi ile birden fazla bağlantıya izin verme
- Sadece bağlantı kurulduktan sonra veri iletimi sağlama
- Gönderilen mesaj parçaları için öncelik ve güvenlik tanımlaması yapılabilme

TCP'de uçlar arasında veri alışverişi yapılmadan önce, mantıksal bir bağlantı kurulur. Uçlar, veri iletimi öncesinde birbirlerine kontrol paketi gönderir. Bağlantı öncesinde gerçekleştirilen bu üç aşamalı oturum oluşturma

ve onaylama işlemine **TCP üç yönlü el sıkışma (three way handshake)** denir. Görsel 3.1'de TCP üç yönlü el sıkışma görülmektedir.



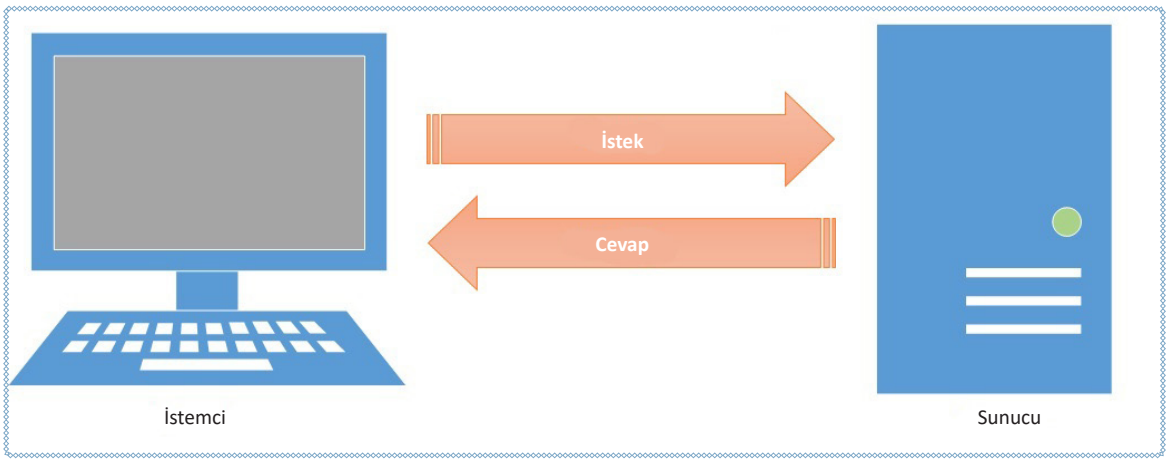
Görsel 3.1: Üçlü el sıkışma

Bu bağlantı yönteminde gerçekleştirilen işlem adımları şu şekildedir:

- İstemci bilgisayar, sunucu bilgisayara SYN (synchronize) adlı bir istek paketi gönderir.
- Sunucu bilgisayar, istek için bir bağlantı açar ve SYN + ACK (synchronize + acknowledged) adı verilen bir onay paketini geri gönderir.
- İstemci bilgisayar, ACK paketini aldığını ve oturumun veri aktarımı için kullanılmaya hazır olduğunu söyleyerek başka bir onay gönderir. Veri oturumu tamamlandığında oturumu kapatmak için benzer bir işlem kullanılır.

3.1.3. UDP Protokolü

Bağlantısız protokollerden biri olan **UDP**, güvenilir olmayan bir veri aktarım protokolüdür. Taşıma katmanı protokolü olan UDP paketleri IP tarafından mevcut verilere yeni veriler eklenir (kapsülleme işlemi) ve taşınır. Görsel 3.2'de UDP bağlantı yapısı görülmektedir.



Görsel 3.2: UDP bağlantısı

UDP'de istemci bilgisayar sunucu bilgisayara bir istek paketi gönderir. Bu iki bilgisayar arasında veri alışverişinin başladığı anlamına gelir. TCP'nin aksine veri gönderiminin sırası ve doğruluğu garanti edilmez. Datagramlar sırası bozulmuş bir şekilde, çift olarak gelebilir ya da tamamen kaybolabilir. UDP, kontrol işlemi olmaması nedeniyle TCP'ye göre daha hızlı çalışmaktadır.

Sıra Sizde

İnternet altyapısında TCP ve UDP protokolleri aynı anda kullanılabilir mi? Oluşturacağınız küçük gruplarla TCP ve UDP protokollerinin aynı anda kullanılmasının veya kullanılmamasının ne gibi avantaj ve dezavantajları olduğunu tartışınız ve elde ettiğiniz sonuçları sınıfınızla paylaşınız.

3.1.4. Taşıma Katmanında Kullanılan Port Numaraları

Bilgisayar ağlarındaki **port** kavramı, bir uygulama için verinin gönderilip alınacağı mantıksal bir kanalı işaret etmektedir. Bilgisayarlardaki fiziksel bağlantı noktaları (USB, PS/2 gibi), klavye ve fare gibi çevresel aygıtlarla iletişim kurmaya ve Ethernet kabloları aracılığıyla internet aygıtlarına bağlanmaya olanak tanır. Portlar, bilgi ve verinin bilgisayardaki bir uygulamadan başka bir uygulamaya veya aynı ağdaki başka bilgisayara gönderilmesine imkân sağlar. Herhangi bir yazılım veya işletim sistemi üzerinde çalışan bir başka uygulama veya hizmetler ile iletişim kurması için bağlantı noktasına (porta) ihtiyaç bulunmaktadır. Portlar, 0 ile 65535 arasında değişen pozitif 16 bitlik işaretsiz tam sayılarla tanımlanır. Diğer hizmetler, hizmet veya uygulama ile iletişim kurmak için bu port numarasını kullanır. Port numaraları üç grupta incelenebilir:

- **0** ile **1023** arasındaki portlar **iyi bilinen (Well-known)** port olarak adlandırılır. HTTP: 80, Telnet:23 ve SMTP:25 numaralı portlara örnektir.
- **1024** ile **49151** arasındaki portlar ise **kayıtlı (Registered)** portlar olarak adlandırılır. MongoDB-27017, Skype-23399 kayıtlı port örnekleridir.
- **49152** ile **65535** arasındaki portlar **kısa ömürlü (Ephmeral, Dynamic, Private)** port olarak adlandırılır. Kısa ömürlü portlar ise bilgisayarın istemci rolü ile yer aldığı durumlarda kullanılmaktadır.

3.1.5. İyi Bilinen Port Numaraları

Bir uygulama port numarasını değiştirebilse de bilgisayarda bulunan portlardan bir kısmı İnternet Tahsisli Sayılar ve İsimler Kurumu [ICANN (Internet Corporation for Assigned Names and Numbers)] tarafından bazı uygulamalara tahsis edilmiştir.

0 ile **1023** arasındaki portlar **iyi bilinen** (Well-known) port olarak adlandılır. İşletim sistemleri genel olarak uygulamaların bu portları kullanabilmesi için yönetici hesabı ile çalıştırılmalarını şart koşar. Bu sayede kullanıcı seviyesi işlemlerin bu portları kullanması engellenir. Tablo 3.1'de iyi bilinen portlara ait bilgiler verilmiştir.

Tablo 3.1: TCP/IP Protokolünde İyi Bilinen Port Numaraları ve Özellikleri

Protokol	TCP / UDP	Port Numarası	Açıklama
Dosya Aktarım Protokolü (FTP)	TCP	20 / 21	**FTP**, internette ve özel ağlarda en sık kullanılan dosya aktarım protokollerinden biridir. FTP kontrolü, TCP bağlantı noktası 21'de gerçekleştirilir ve veri aktarımı, belirli yapılandırmaya bağlı olarak dinamik bağlantı noktalarının yanı sıra TCP bağlantı noktası 20'yi kullanabilir.
Güvenli Kabuk (SSH)	TCP	22	**SSH**, ağ cihazlarını komut düzeyinde güvenli bir şekilde yönetmek için kullanılan birincil yöntemdir. Genellikle güvenli bağlantıları desteklemeyen Telnet'e güvenli bir alternatif olarak kullanılır.
Telnet	TCP	23	**Telnet**, ağ aygıtlarını komut düzeyinde yönetmek için kullanılan birincil yöntemdir. Güvenli bir bağlantı sağlayan SSH'nin aksine güvenli bağlantı sağlamaz. Daha düşük seviyeli ağ cihazlarının çoğu bazı ek işlemler gerektirdiği için SSH'yi değil, Telnet'i destekler. Giriş kimlik bilgileri açık bir şekilde iletileceği için halka açık bir ağ üzerinden Telnet kullanan bir cihaza bağlanırken dikkatli olunmalıdır.

Basit Posta Aktarım Protokolü (SMTP)	TCP	25	**SMTP**, iki temel işlev için kullanılır. E-postayı, posta sunucuları arasında kaynaktan hedefe aktarmak ve son kullanıcılar tarafından bir posta sistemine e-posta göndermek için kullanılır.
Alan Adı Sistemi (DNS)	TCP / UDP	53	**DNS**, internette ve özel ağlarda alan adlarını tipik olarak ağ yönlendirmesi için IP adreslerine çevirmek amacıyla yaygın olarak kullanılan bir sistemdir.
Dinamik Ana Bilgisayar Yapılandırma Protokolü (DHCP)	UDP	67 / 68	**DHCP**, statik IP adresi ataması kullanmayan ağlarda kullanılır. Bir istemci cihazı açıldığında yerel DHCP sunucusundan bir IP adresi talep edebilir. Havuzda kullanılabilir bir adres varsa cihaza atanabilir. Bu atama kalıcı değildir, belirli bir süre sonra sona erer.
Önemsiz Dosya Aktarım Protokolü (TFTP)	UDP	69	**TFTP**, FTP'nin kullandığı oturum oluşturma gereksinimleri olmadan bir dosya aktarımı yöntemi sunar. TFTP, TCP yerine UDP kullanıldığı için, dosyanın düzgün bir şekilde aktarıldığından emin olmanın bir yolu yoktur. Bu sebeple alıcı cihazın dosyayı kontrol etmesi gerekir.
Köprü Metni Aktarım Protokolü (HTTP)	TCP	80	**HTTP**, web tarayıcıları tarafından kullanılan ana protokoldür.Bu nedenle sunucularda bulunan dosyaları kullanan herhangi bir istemci tarafından kullanılır.
Postane Protokolü (POP) sürüm 3	TCP	110	**POP sürüm 3**, bir sunucudan posta almak için kullanılan protokolden biridir.
Ağ Zaman Protokolü (NTP)	UDP	123	**NTP**, internetteki cihazları senkronize etmek için kullanılır. Çoğu modern işletim sistemi bile saati doğru tutmanın temeli olarak NTP'yi destekler.
NetBIOS	TCP / UDP	137 / 138 / 139	**NetBIOS**, kendi başına bir protokol değildir. Tipik olarak TCP/IP üzerinden NetBIOS (NBT) protokolüyle IP ile birlikte kullanılır. NBT, uzun süredir kapalı kaynak işletim sistemi makinelerini birbirine bağlamak için kullanılan merkezî protokoldür.
İnternet Mesaj Erişim Protokolü (IMAP)	TCP	143	**IMAP sürüm 3**, bir sunucudan posta almak için kullanılan ana protokolden biridir. POP daha geniş bir desteğe sahipken IMAP sürüm 3 kullanıcılara yardımcı olabilecek daha geniş bir uzak posta kutusu işlemini destekler.
Basit Ağ Yönetim Protokolü (SNMP)	TCP / UDP	161 / 162	**SNMP**, ağ cihazlarını izleme, yapılandırma ve kontrol etme yeteneği dâhil olmak üzere bir dizi farklı beceriye sahiptir.
Sınır Ağ Geçidi Protokolü (BGP)	TCP	179	**BGP sürüm 4**, genel internette ve İnternet Servis Sağlayıcıları (ISP) tarafından çok büyük yönlendirme tablolarını, trafik işlemeyi sürdürmek için yaygın olarak kullanılmaktadır. BGP, halka açık olan internette bulunması gereken astronomik yönlendirme tablolarıyla başa çıkmak için tasarlanmış birkaç protokolden biridir.
Hafif Dizin Erişim Protokolü (LDAP)	TCP / UDP	389	**LDAP**, dağıtılmış dizin bilgilerine erişmeyi ve bunları korumayı sağlar. LDAP, ITU-T X.500 standardını temel alır. Basitleştirilmiş ve TCP/IP ağları üzerinden çalışmak üzere değiştirilmiştir.

3.1.6. Komut İstemci Kullanarak Port İzleme

IP adresi, bir ağdaki bilgisayarı veya herhangi bir ağ cihazını tanımlayan adrestir. Ağa bağlı bilgisayar diğer bir bilgisayara veri paketi gönderdiğinde IP adresine bakar. IP adresi gelen veri paketini uygun yere yönlendirmek için kullanılır. Gönderen tarafından gönderilmiş veri paketi, diğer cihaza ulaştığında bu paketin hangi uygulamaya veya servise ait olduğunu tespit etmesi gerekmektedir. Bu noktada **port** kavramı devreye girmektedir. Her IP adresi,

portlara (sanal veri yolları) bölünmüştür. Bu sayede, aynı anda aynı IP adresinden farklı programlarla veri alışverişi yapılabilmektedir. Örneğin; aynı anda, bir bilgisayardan 110 No.lu portu kullanarak e-posta uygulaması ile e-mail gönderirken, 25 numaralı portu kullanırken aynı anda 80 numaralı portu kullanarak internette gezilebilir..

Bilgisayar kullanıcısı portlar üzerinde kontrole sahiptir. Kullanıcı dilerse bazı portları kapatıp açabilir. Bu sayede ilgili portu kullanan programlara izin vermiş ya da programları engellemiş olur.

Bir portu kullanan uygulamayı tespit etmenin birçok yolu bulunmaktadır. Bunun için uygulamalarda en yaygın ve ücretsiz olarak kullanılan **Komut İstemi (Command Prompt)** tercih edilmiştir. Komut istemci üzerinde kullanılacak olan **Network İstatistikleri Görüntüleme (netstat)** komutu ile ağ bağlantıları (gelen ve giden), yönlendirme tabloları ve ağ arayüzü istatistikleri görüntülenebilir.

3.1.6.1. Netstat Komutu ve İşlevi

Netstat (network statistics), komut satırından ağ bağlantılarını kontrol etmeye yarayan yardımcı bir programdır. Gelen ve giden bağlantılarla birlikte yönlendirme tablolarını da göstermektedir. Ağ kartlarına ait istatistiklerle beraber sistemdeki açık portları kontrol etmeye yardımcı olan bir komuttur.

Netstat komutu bilgisayarın bağlı olduğu ağ hakkında aşağıdaki istatistikleri sağlamaktadır:

- Protokol-Protokol ismi (TCP veya UDP)
- Local (Yerel) Adres-Bilgisayarın IP adresi ve kullanımda olan portları, -n parametresi belirtilmediği sürece bilgisayarın ismine karşılık gelen IP adresi ve port adı gösterilir.
- Foreign (Yabancı) Adres-Bağlantı kurulan bilgisayarın IP adresi ve port numarası, -n parametresi belirtilmediği sürece bilgisayarın ismine karşılık gelen IP adresi ve port adı gösterilir.
- STATE: TCP bağlantısının durumu hakkında bilgi verir.

Bu durumlar şunlardır:

ESTABLISHED: Soket bağlantı gerçekleşmiş durumdadır.
SYN_SENT: Soket bağlantı kurmaya çalışılıyor.
SYN_RECV: Ağdan bir bağlantı isteği gelmiştir.
FIN_WAIT1: Soket kapatılmış, bağlantı sonlandırılmak üzeredir.
FIN_WAIT2: Bağlantı sonlandırılmıştır. Soket karşı ucun bağlantıyı sonlandırmasını beklemektedir.
TIME_WAIT: Soket kapandıktan sonra gelebilecek paketleri alabilmek için beklemektedir.
CLOSED: Soket kullanılmamaktadır.
CLOSE_WAIT: Karşı uç bağlantıyı kapatmıştır. Soketin kapanması beklenmektedir.
LAST_ACK: Karşı uç bağlantıyı sonlandırmış ve soketi kapatmıştır. Onay beklenmektedir.
LISTEN: Soket gelebilecek bağlantılar için dinleme konumundadır.
CLOSING: Yerel ve uzak soketler kapatılmış fakat tüm verilerini göndermemiş durumdadır. Tüm veriler gönderilmeden soketler kapanmaz.

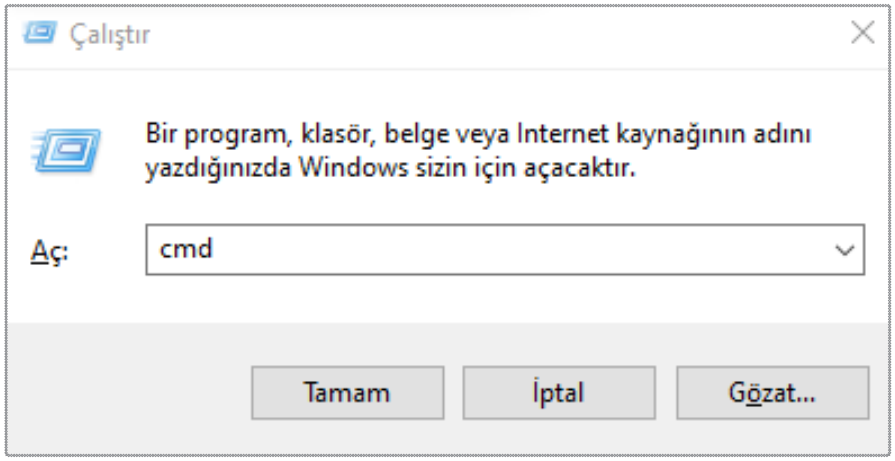
Netstat komutu birçok parametre ile beraber çalışmaktadır. Bu nedenle sadece istenilen bilgiler filtrelenebilir ve görüntülenebilir. Netstat komutu parametreleri ve kullanım şekilleri aşağıda verilmiştir.

netstat -n: Aktif TCP bağlantılarını görüntüler. Adresler ve bağlantı noktası numaraları sayısal olarak ifade edilir, herhangi bir isim belirlemesi yapılmaz.
netstat -a: Tüm aktif bağlantıları ve bilgisayarın dinlediği TCP ve UDP portları görüntüler.
netstat -an: Dosya alırken karşıdakinin IP adresini gösterir.
netstat -b: Her bağlantı veya dinleme bağlantı noktasıyla ilişkili çalıştırılabilir dosyayı gösterir.
netstat -e: Ethernet istatistiklerini gösterir.
netstat -o: Her bağlantıyla ilişkili sahip işlem kimliğini gösterir.
netstat -p: İletişim kuralının bağlantılarını gösterir.
netstat -r: Yönlendirme tablosunu gösterir.
netstat -s: Her iletişim kuralı için istatistikleri gösterir.
netstat -v: En önemli netstat komutu olan -v, -b ile birlikte kullanılırsa tüm çalışan dosyalar için bağlantı ve bağlantı noktası oluşumu ile ilgili bileşenlerin sırasını gösterir.

Uygulama 1

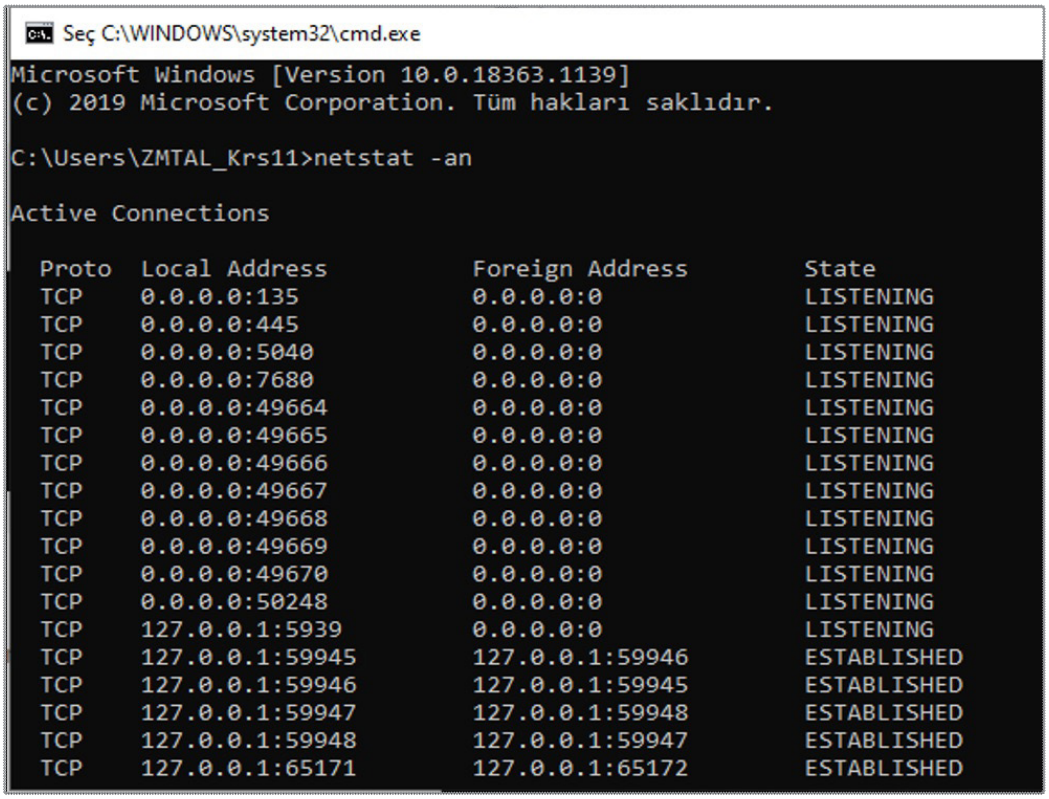
Bilgisayardaki açık portları görmek için gerekli işlemleri kendi bilgisayarınızı kullanarak aşağıdaki yönergeler doğrultusunda gerçekleştiriniz.

Adım 1: ***Windows Tuşu + R*** tuşlarına basarak **"Çalıştır"** penceresini açınız (Görev çubuğundaki arama kısmına Çalıştır yazarak da açılabilir.). Açılan **Çalıştır** penceresine "**cmd**" yazıp "Enter" tuşuna basınız (Görsel 3.3).



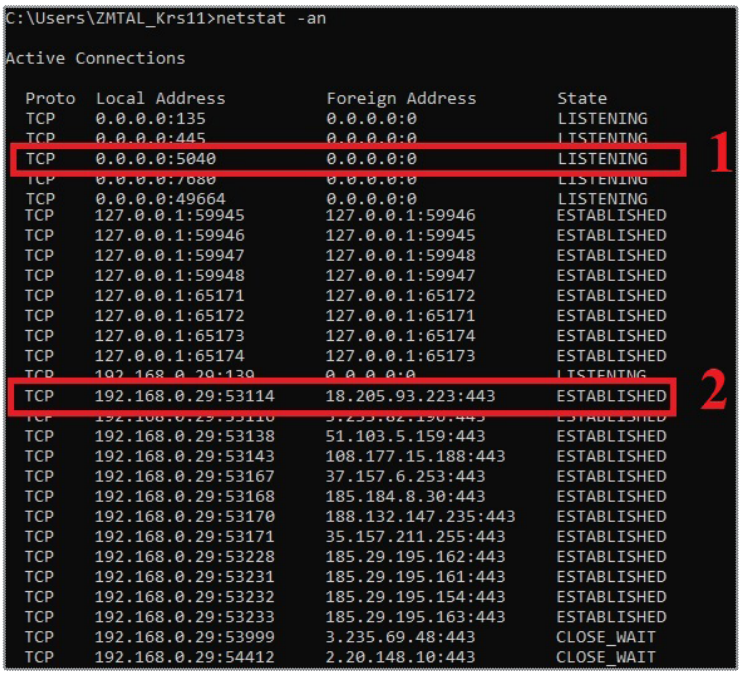
Görsel 3.3: Komut istemcisinin çalıştırılması

Adım2: Komut istemciye, bilgisayardaki tüm bağlantıları ve dinleme bağlantı noktalarını göstermesi için "**netstat –an**" komutunu yazıp "Enter" tuşuna basınız (Görsel 3.4).



Görsel 3.4: Bilgisayardaki dinleme ve bağlantı noktalarını gösteren komutun çalıştırılması

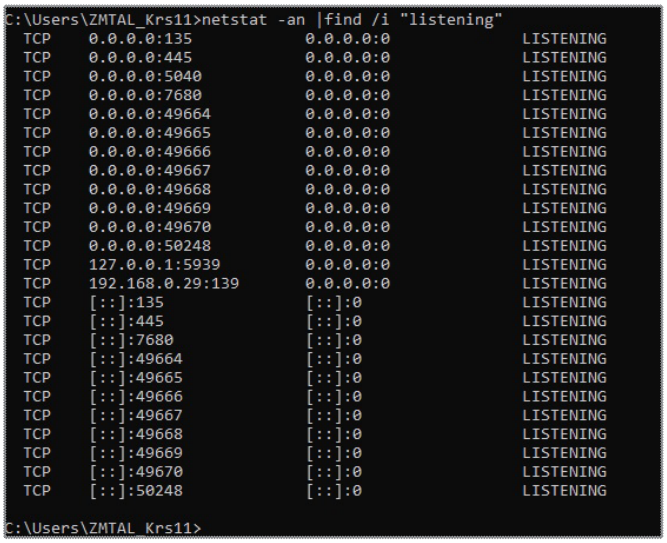
Adım 3: Bilgisayarın bağlantı kurduğu diğer bilgisayarların IP adreslerini görmek için netstat komutunun parametresini – an olarak değiştiriniz (Görsel 3.5).



Görsel 3.5: Netstat komutu ile –an parametrelerinin kullanımı

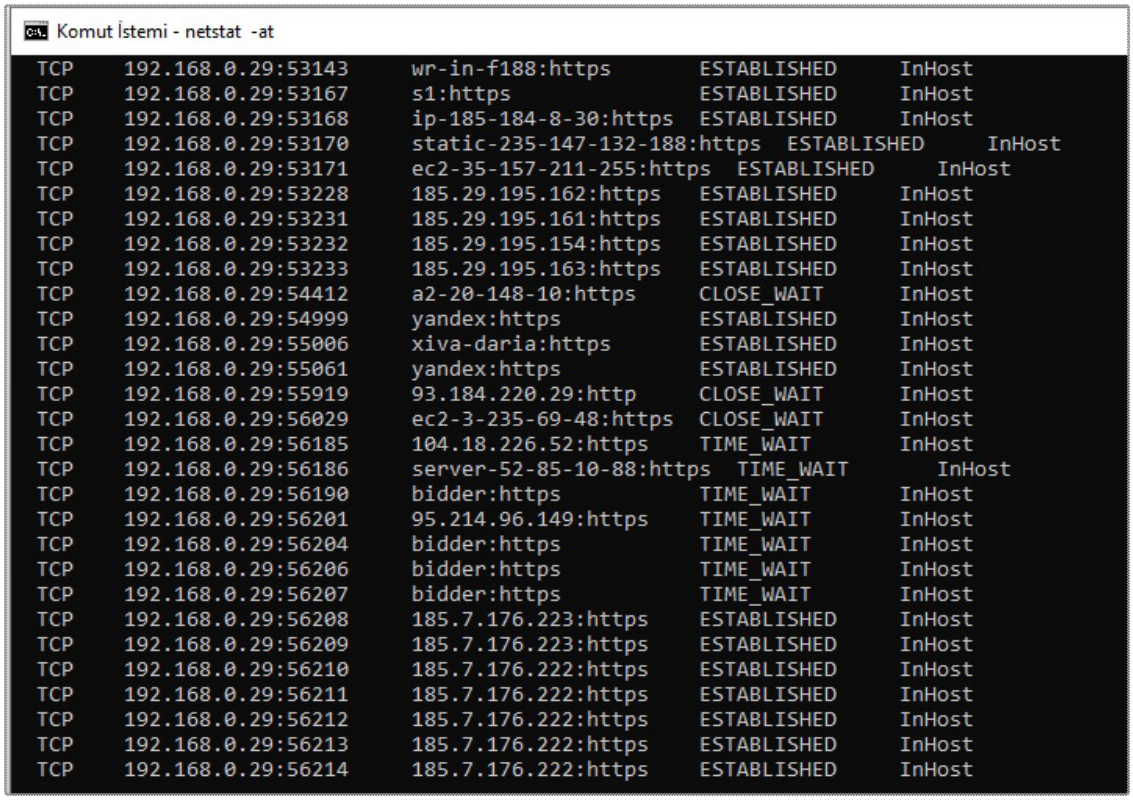
1 numaralı alanda, 5040 numaralı port **dinleme (LİSTENİNG)** durumundadır. Listening durumu, dış IP adresinden gelecek bağlantı isteğinin kabul edileceği ve bağlantı kurulacağı anlamına gelmektedir.
2 numaralı alanda, kurulu olan mevcut bağlantı (**ESTABLİSHED**) görülmektedir. 192.168.0.29 numaralı IP adresinin 53114 numaralı port kullanılarak dış (yabancı) IP adresi olan 18.205.93.223 ile o bilgisayarın 80 numaralı portuyla iletişim kurmuştur.

Adım 4: Bilgisayardaki açık portların tespit edilebilmesi için **netstat** komutu ile **find** komutunu beraber kullanınız. Bunun için komut istemciye aşağıdaki komut satırını yazınız ve "Enter" tuşuna basınız (Görsel 3.6). Bu şekilde bilgisayarın açık olan tüm portlarını listeleyiniz.
>>***Netstat –an \| find /i "listening"***



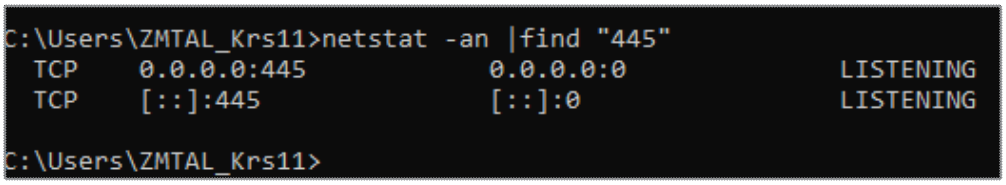
Görsel 3.6: Netstat komutu ile sadece açık olan portları listeleme

Adım 5: SadeceTCP portlarını gösteren komut dizisi "**netstat –at**"dir (Görsel 3.7).



Görsel 3.7: Netstat komutu kullanarak sadece TCP portlarını izleme

Adım 6: Eğer özel bir portun açık olup olmadığı kontrol edilmek istenirse "***netstat -an |find "Port_Numarası***" komut satırını yazınız (Görsel 3.8). Örnekte sisteme ait 445 numaralı port, dinleme durumunda olup yabancı adresten gelecek bağlantı isteğini kabul edecek ve bağlantı kurulacaktır.



Görsel 3.8: 445 numaralı portun dinlemesi

Sıra Sizde

Netstat komutunu kullanarak;

- Ethernet kartının tüm istatistiklerini listeleyen,
- Dinleme yapan tüm bağlantıları listeleyen,
- Bağlantı kurulan tüm uygulama adlarını ve IP adreslerini gösteren komut satırlarını yazarak ekran sonuçlarını arkadaşlarınız ve öğretmenlerinizle paylaşınız.

Araştırma

Port numaralarını dinlemek için başka yöntemler araştırınız. Bu amaçla yazılmış programlar olup olmadığını kontrol ediniz ve varsa programların kullanımı ile ilgili bir sunum hazırlayınız. Hazırladığınız sunumu arkadaşlarınız ve öğretmeninize ile paylaşınız.

3.2. Uygulama Katmanı Protokolleri

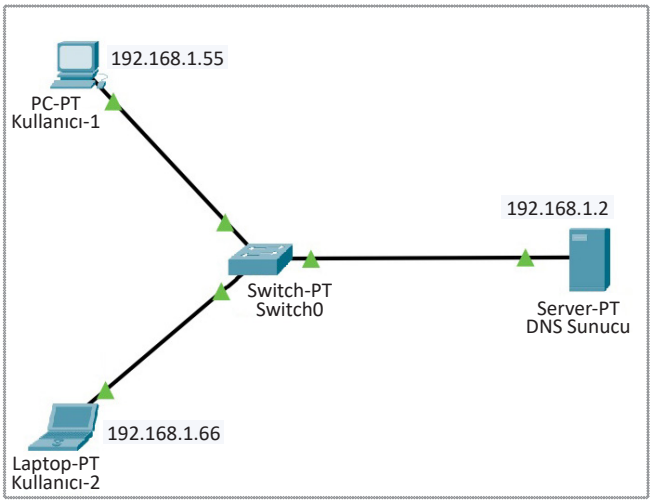
Uygulama katmanı için tanımlı olan protokoller, bir üst katmanda bulunan işletim sisteminin kullanıcıya sunduğu program arayüzlerine hizmet verir. Kullanıcıya hizmet veren programın türüne göre uygulama katmanında farklı protokoller çalıştırılır. Bu protokoller; HTTP-HTTPS, FTP, DNS, SMTP, DHCP, Telnet, SSH, POP3, IMAP vb.dir.

Uygulama katmanı, kullanıcılar tarafından ihtiyaç duyulan arayüz ve protokolleri sağlayan TCP/IP modelinin **en yüksek soyutlama katmanıdır**. OSI modelinin oturum katmanının, sunum katmanının ve uygulama katmanının işlevlerini birleştirir. İki uygulama katmanı, sanki iki katman arasında bir köprü varmış gibi birbirleri arasında mesaj alışverişi yapar. Uygulama katmanı, tüm ağ uygulamalarını destekler. Uygulama katmanı, taşıma katmanıyla portlar aracılığıyla haberleşir. Portlar, numaralandırılmış standart uygulamalardır (HTTP:80, FTP:21 vs.) ve taşıma katmanında gelen paket içeriği türünün anlaşılmasında rol oynar.

Uygulama 2

http://kitap.eba.gov.tr/KodSor.php?KOD=21031

Görsel 3.9'da bir PC ve bir laptoptan oluşan DNS sunucu simülasyon ekran görüntüsü görülmektedir. İstenilenler ile birlikte verilen simülasyon uygulamasını aşağıdaki yönergeler doğrultusunda gerçekleştiriniz.



Görsel 3.9: DNS uygulaması ekran görüntüsü

Adım 1: Ağ topolojinizi DNS uygulaması için seçiniz.

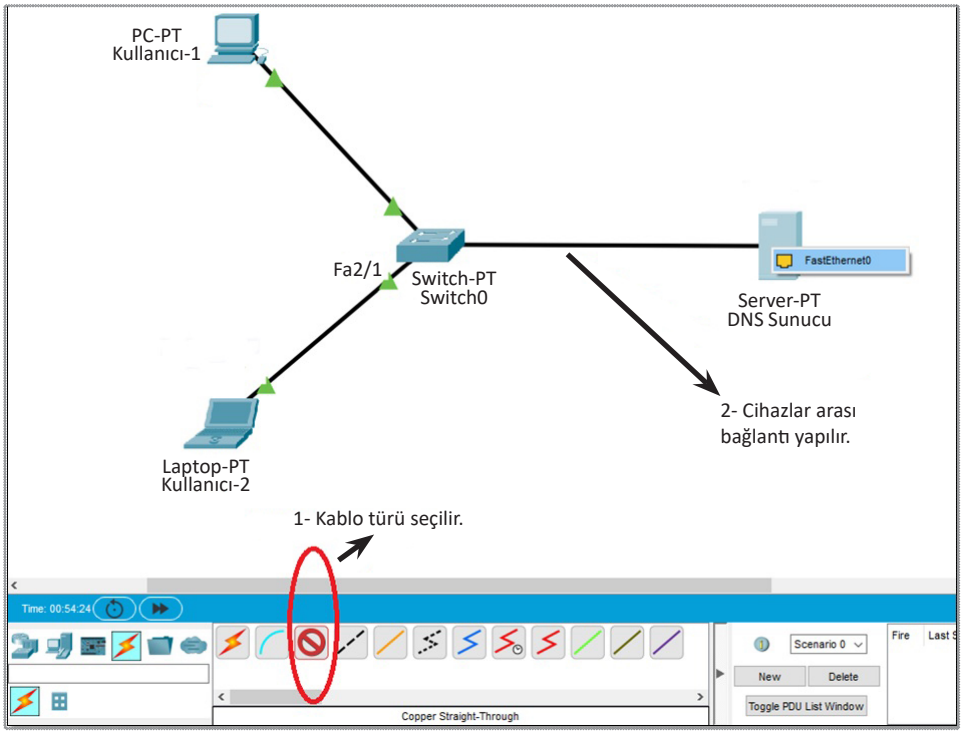
Adım 2: IP adreslemelerini yapılandırınız.

Adım 3: DNS sunucu için gerekli olan yapılandırmaları tamamlayınız.

Adım 4: Simülasyonu ping komutu ile test ediniz.

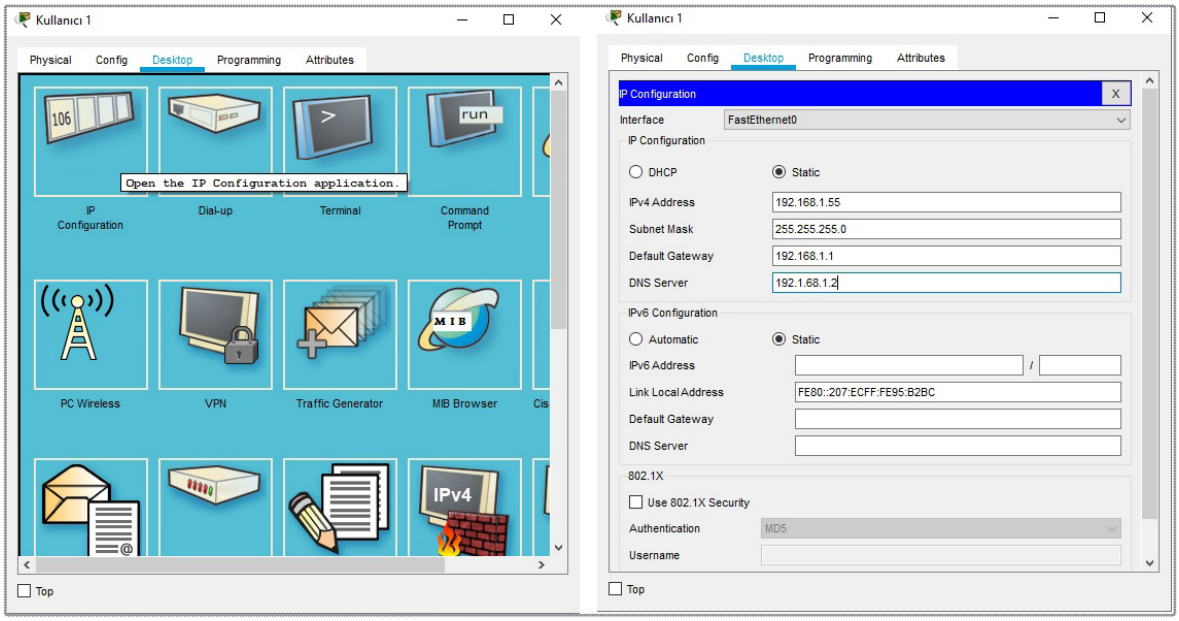
Adım 5: Simülasyon programını açınız ve DNS uygulaması için gerekli olan ağ cihazlarını seçip editöre yerleştiriniz.

Adım 6: Verilen DNS uygulaması ekran görüntüsündeki ağ topolojisi, bir **yıldız topoloji**dir. Yıldız topolojiye uygun kablolama işlemlerini gerçekleştiriniz (Görsel 3.10).



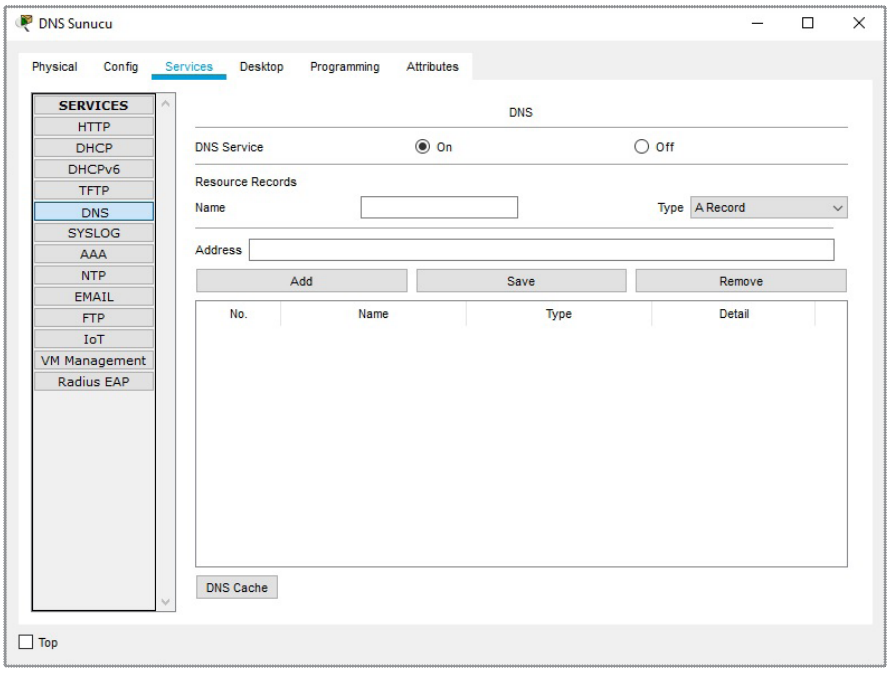
Görsel 3.10: Yıldız topolojiye uygun kabloların seçilmesi ve yerleştirilmesi

Adım 7: Tüm ağ cihazlarının IP adreslerini yapılandırmak için cihaza farenin (mouse) sol tuşu ile tıklayıp açılan penrede **IP Configuraton** seçerek ilgili alanları Görsel 3.11'deki gibi doldurunuz. Bu işlemleri tüm ağ cihazları için yapınız.



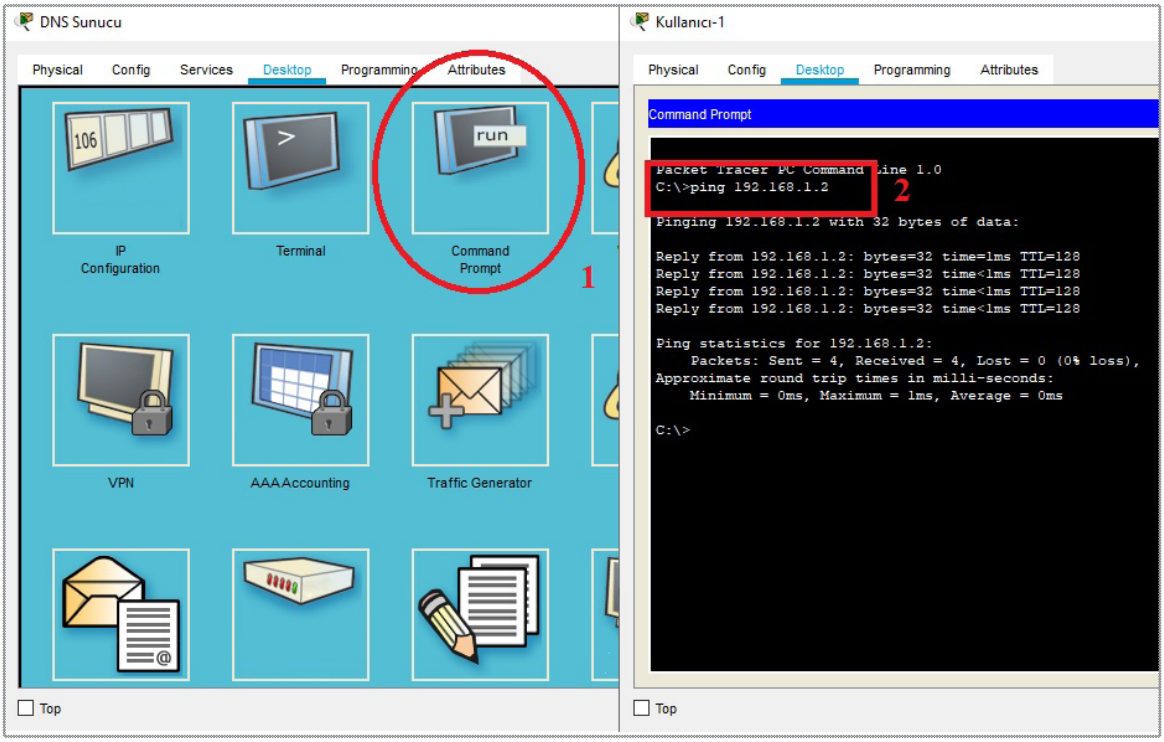
Görsel 3.11: DNS uygulaması için IP yapılandırması

Adım 8: DNS sunucusunu yapılandırınız. Bu yapılandırmada DNS sunucusunun DNS servisini aktif hâle getirmek gerekir (Görsel 3.12).



Görsel 3.12: DNS sunucusu için DNS servisinin aktif hâle getirilmesi

Adım 9: Test işlemi için herhangi bir "Kullanıcı" seçiniz ve fareyle sol tık yapınız. Gelen pencereden **Desktop** sekmesi altındaki **Command Prompt** (Görsel 3.13'te 1 numara ile gösterilmiştir.) butonuna basınız ve **DNS IP** adresi verilerek (Görsel 3.13'te 2 numara ile gösterilmiştir.) **ping** işleminin yapılıp yapılmadığını test ediniz. Test sonucunda veriler başarılı bir şekilde gönderiliyorsa simülasyonunuz başarılı olmuştur.



Görsel 3.13: Simülasyonun ping komutu ile test edilmesi

Sıra Sizde

Uygulama 2'de yer alan DNS simülasyonunda neden yıldız topolojisi seçilmiştir? Bu konuyu arkadaşlarınızla tartışınız ve farklı topolojiler ile aynı simülasyonu tekrar uygulamayı deneyiniz. Elde ettiğiniz sonuçları içeren bir sunumu sınıfla paylaşınız.

Uygulama 3

http://kitap.eba.gov.tr/KodSor.php?KOD=21032

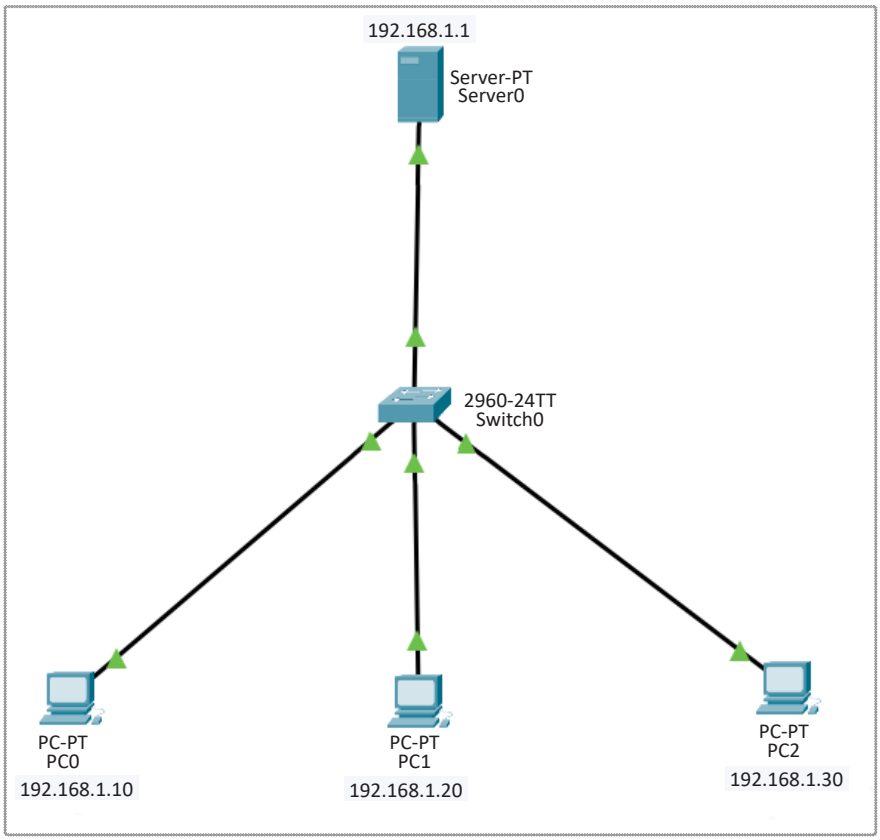
Görsel 3.14'te üç adet PC, birer adet anahtar ve sunucudan oluşan HTTP-HTTPS sunucu simülasyon ekranı görülmektedir. İstenilenler ile birlikte verilen simülasyon uygulamasını aşağıdaki yönergeler doğrultusunda gerçekleştiriniz.

Adım 1: Ağ topolojinizi DNS uygulaması için seçiniz.

Adım 2: IP adreslemelerini yapılandırınız.

Adım 3: DNS sunucu için gerekli olan yapılandırmaları tamamlayınız.

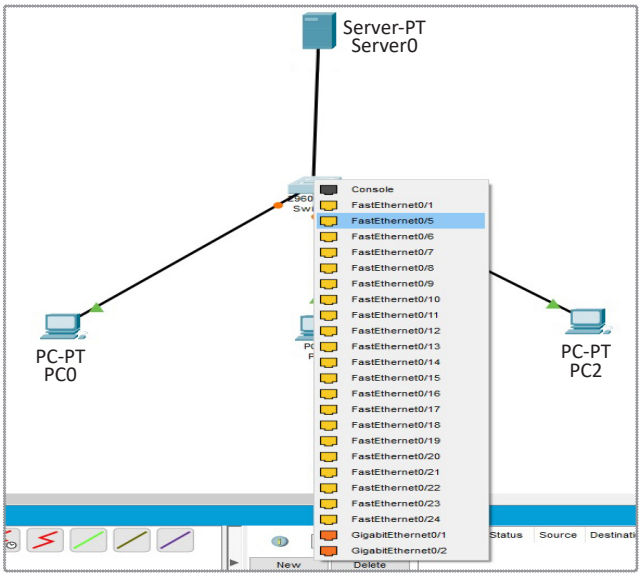
Adım 4: Simülasyonu ping komutu ile test ediniz.



Görsel 3.14: HTTP-HTTPS simulasyon uygulaması

Adım 5: Simülasyon programını açınız ve HTTP-HTTPS uygulaması için gerekli olan ağ cihazlarını seçip editöre yerleştiriniz.

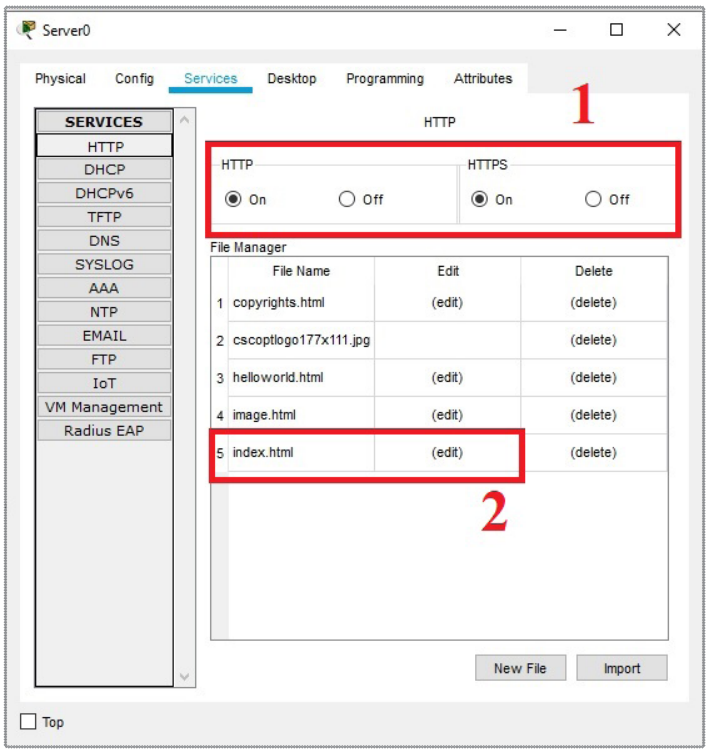
Adım 6: Verilen HTTP-HTTPS uygulaması ekran görüntüsündeki ağ topolojisi bir **yıldız topoloji**dir. Yıldız topolojiye uygun kablolama işlemlerini gerçekleştiriniz (Görsel 3.15).



Görsel 3.15: Ağ cihazları arası kablolama işlemleri

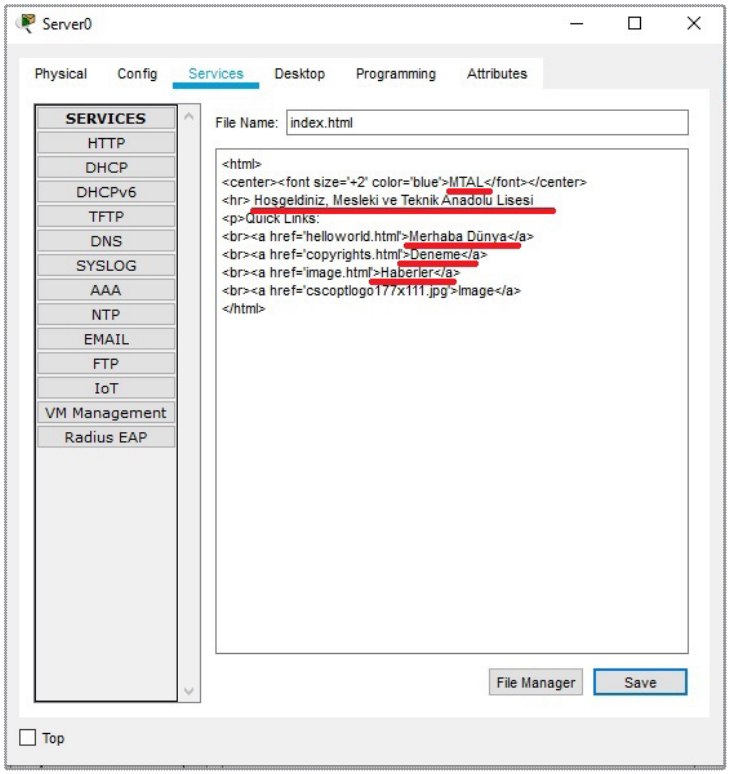
Adım 7: Tüm ağ cihazlarının IP adreslerini yapılandırmak için cihaza farenin sol tuşu ile tıklayıp açılan penreden **IP Configuraton** seçerek ilgili alanları Görsel 3.14'teki gibi doldurunuz. Bu işlemleri tüm ağ cihazları için yapınız.

Adım 8: HTTP-HTTPS sunucusunun yapılandırılmasını tamamlayınız. Bu yapılandırmada HTTP-HTTPS sunucusunun HTTP ve HTTPS servisini aktif hâle getirmek gerekir (Görsel 3.16'da 1 numaralı bölüm). Görsel 3.16'da 2 numara ile gösterilen **index.html**'nin bulunduğu satırda (**edit**) ile belirtilen yere tıklayarak sunucu çalıştığında karşılama sayfasının düzenlemesini yapınız.



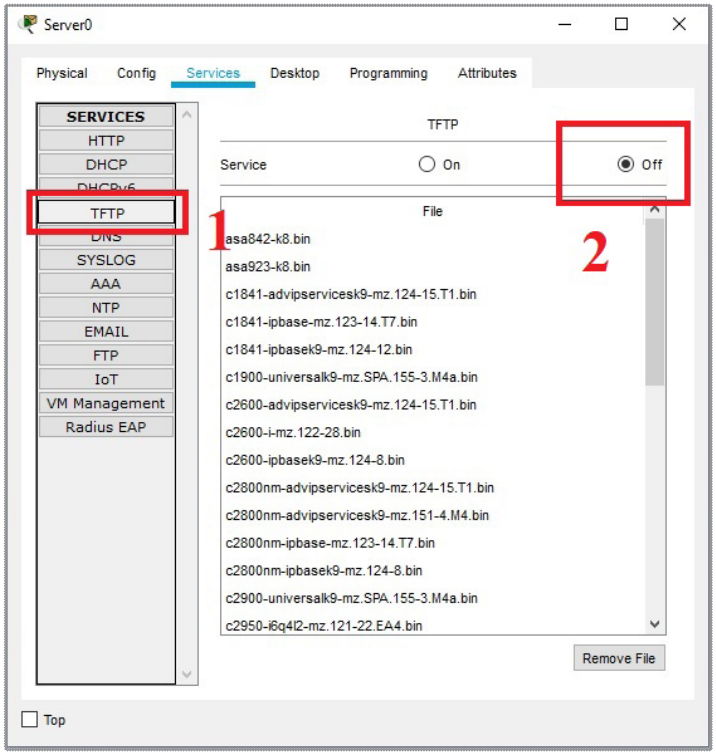
Görsel 3.16: HTTP ve HTTPS servislerinin açılması işlemi

Adım 9: Açılan pencereden **index.html** içeriğini Görsel 3.17'deki gibi düzenleyiniz.



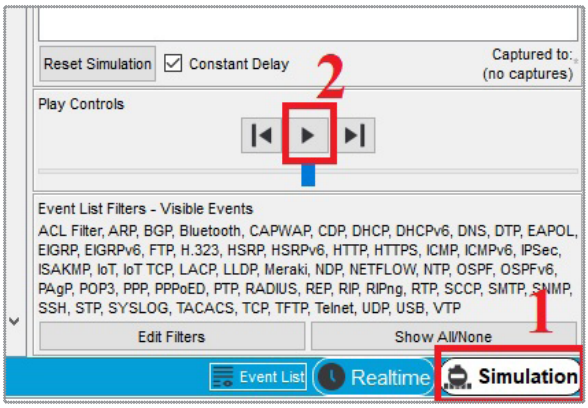
Görsel 3.17: index.html içeriğinin düzenlenmesi

Adım 10: Sol taraftaki menüden **TFTP** butonunu tıklayınız ve **TFTP** servisini kapatınız (Görsel 3.18).



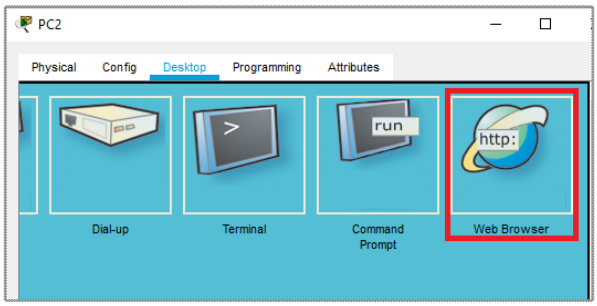
Görsel 3.18: TFTP servisinin kapatılması

Adım 11: Simulasyon editörünün sağ alt tarafında bulunan **simülasyonu çalıştır** butonuna (Görsel 3.19-1 numaralı alan) ve hemen yukarısındaki **çalıştır (play)** butonuna (Görsel 3.19-2 numaralı alan) tıklayınız.



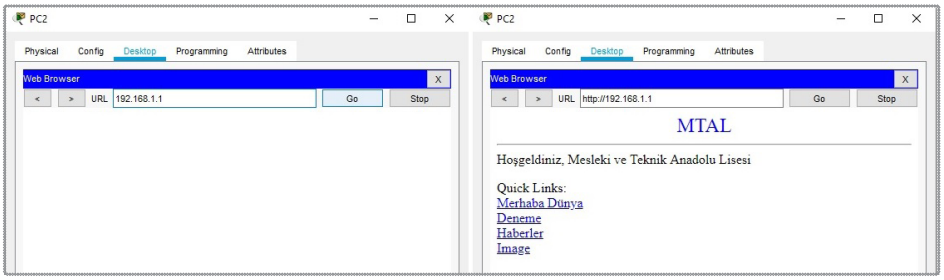
Görsel 3.19: Simülasyonun çalıştırılması

Adım 12: Web sitesi çalıştırılacak herhangi bir PC seçiniz. Açılan pencereden **Desktop** sekmesi altındaki **Web Browser** butonuna basınız (Görsel 3.20).



Görsel 3.20: DNS sunucu uygulaması için internet tarayıcının simülasyon içinde çalıştırılması

Adım 13: Adres satırına sunucunun IP adresini yazınız (192.168.1.1) ve **Git** butonuna basınız (Görsel 3.21). Sunucu doğru bir şekilde yapılandırılmışsa düzenlenmesi yapılan **index.html** sayfası ekranda görüntülenecektir (Görsel 3.22).



Görsel 3.21: Adres çubuğuna sunucu IP adresi yazılması **Görsel 3.22: HTTP-HTTPS servisinin çalıştırılması**

Sıra Sizde

TCP/IP uygulama katmanı protokolleri olan FTP, SMTP ve DHCP simülasyon uygulamalarını yapınız ve test ediniz. Elde ettiğiniz sonuçları öğretmeninize gösteriniz.

3.3. Ağ Protokolleri

Ağ hizmetlerinde protokoller, iletişimin kurallarıdır. Bir ağdaki iletişim kuralları, protokoller tarafından düzenlenir. Bilgisayarların birbirleriyle iletişim kurabilmesi için aynı ya da uyumlu protokolleri kullanmaları gerekmektedir.

Farklı türdeki bilgisayarların, ağ cihazlarının birbirleri arasındaki iletişimi organize eden ve belirli bir düzen veren bazı modeller geliştirilmiştir. **OSI Modeli** ve **TCI/IP** Modeli bunlar arasında en önemli olanlardır.

3.3.1. Açık Sistem Ara Bağlantısı (OSI) Modeli

Bilgisayarlar ilk geliştirildiklerinde başka cihazlar ile iletişim kurmayan, sadece kendi başlarına çalışan cihazlardı. Bir bilgisayardan başka bir bilgisayara veri aktarılmak istendiğinde bu işlemler manuel olarak (el ile) yapılmaktaydı. Dosyaların disklerde bilgisayardan bilgisayara taşınması gerekiyordu. Birden fazla bilgisayarın başka bilgisayarlarla işletişim hâlinde olması, birbiri ile haberleşmesine ihtiyaç duyulmaya başlanması, bilgisayar donanım ve yazılım üreticilerinin bunu sağlamak için çalışmalar başlatmasına sebep oldu. Bunu mümkün kılmak için donanım ve yazılımın standartlaştırılması gerekiyordu. Bu çabaya yardımcı olmak ve bilgisayar iletişimini kolaylaştırmak için **Uluslararası Standardizasyon Örgütü (ISO), Açık Sistemler Bağlantısı (OSI) Modeli**ni geliştirdi.

Veri iletişimi ve ağ oluşturmada, bir protokol hem gönderenin hem de alıcının ve tüm ara cihazların etkili bir şekilde iletişim kurabilmeleri için uyması gereken kuralları tanımlar. İletişim basit olduğunda, yalnızca tek bir basit protokole ihtiyaç olabilir; iletişim karmaşık olduğunda, görevi farklı katmanlar arasında bölmek gerekebilir. Bu durumda her katmanda bir protokole veya protokol katmanlaşmasına ihtiyaç olabilir. **OSI**, en yaygın kullanılanı olmasa da ağ iletişim protokolü standardı olarak işlev gören açık bir mimari modeldir. OSI'ye rakip **İletim Kontrol Protokolü / İnternet Protokolü (TCP/IP) Modeli** en yaygın kullanılan modeldir. Hem OSI hem de TCP/IP modeli biri kaynak ögede, diğeri hedef ögede olmak üzere iki protokol yığını kullanır.

OSI modelinin gelişimi, bir ağ üzerinden bir iletişim görevinin yedi katmana bölünebileceği ve her bir katmanın görevinin farklı bir bölümünü temsil ettiği güvenli bir yapıya dayanmaktadır. Protokolün her katmanı farklı hizmetler sağlamaktadır. Her katmanın yalnızca kendine komşu (alt ve üst) katmanlarla iletişim kurmasını sağlamaktadır. Kaynak bilgisayardan hedef bilgisayara gönderilen bilgiler en üst katmandan başlayarak en alt katmana kadar ağ ortamı üzerinden aşağıya doğru hareket eder. Alıcı olan hedef bilgisayarda da tam tersi yönde, aşağıdan en tepeye doğru hareket eder. Her katman gelen bilgiyi alt katmana veya üst katmana iletmek amacıyla tasarlanmıştır. Bu nedenle katmanlar arası iletişimi kolaylaştırmak için katmanlar arasındaki arayüzler standartlaştırılmıştır. Bununla birlikte her katmanın işlevselliği, üstündeki ve altındaki diğer katmanların işlevlerini etkilememektedir.

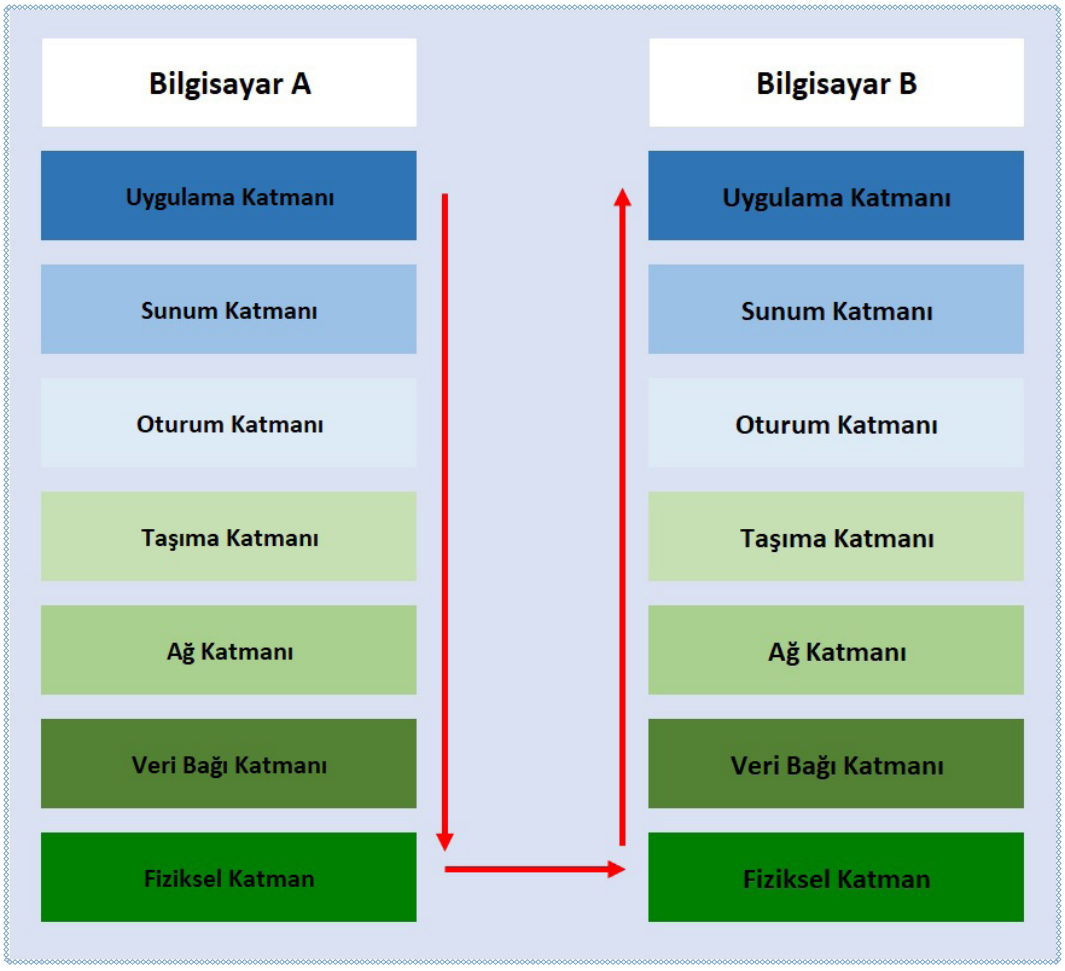
Tablo 3.2, yedi katmandan oluşan bir OSI modelini ve her katmanda sağlanan hizmetlerin açıklamalarını göstermektedir.

Tablo 3.2: OSI Katmanları ve Görevleri

	Sıra	OSI Katmanı	Katman Görevi
ANA BİLGİSAYAR KATMANLARI	7	Uygulama	Kullanıcı uygulamalarına servis sağlar.
	6	Sunum	Kullanıcı uygulaması için verinin dönüşümünü sağlar. Veriyi yeniden düzenler.
	5	Oturum	Sistemler arasında iletişim kurar (oturum oluşturma, yönetme ve durdurma işlemleri).
	4	Taşıma	Üst katmanlardan gelen veriyi ağ paketi boyutunda parçalara böler.
ORTAM KATMANLARI	3	Ağ	Ağ bağlantısını düzenler, devam ettir ve sonlandırır. Mantıksal adresleme ve yönlendirme yapar. Hata teşhisi yapar ve hata düzeltir.
	2	Veri Bağı	Veri çerçeveleme ve adresleme işlemleri gerçekleştirilir. Hata tespiti yapar. Fiziksel katmanın gereksinimlerini tanımlar.
	1	Fiziksel	Verileri bit olarak iletir. Bu katmanda ağ kablosu (medya) ile iletişim kurulur.

Bir bilgisayar başka bir bilgisayar ile haberleşmek istediğinde bilginin yolculuğu, en üstte bulunan **uygulama katmanından** başlayarak en alt katmana doğru devam eder. Alıcı bilgisayarda ise en alt katman olan **fiziksel katmandan** başlayarak en üst katmana doğru tüm katmanları teker teker geçerek hareket eder. Her katman, üstündeki katmandan iş kabul edecek ve işi altındaki katmana aktaracak şekilde tasarlanmıştır. Veriler, gönderen makinenin katmanından katmanına geçerken katman başlıkları verilere eklenir ve bu da veri katarının büyümesine neden olur. Her katman başlığı, o katmanın uzak sistemdeki eşi için bilgiler içerir. Bu bilgi, paketin ağ üzerinden nasıl yönlendirileceğini veya alıcı bilgisayardaki katmanlara geri verilirken pakete ne yapılması gerektiğini göstermektedir.

Görsel 3.23, OSI modelini kullanan iki eş bilgisayar arasındaki mantıksal bir iletişim modelini göstermektedir. Tablo 3.3, katmanlar arasında hareket ederken eklenen başlık bilgileriyle birlikte datagramı göstermektedir.



Görsel 3.23: OSI Modelini kullanan iki bilgisayar arasındaki iletişim yönü

Tablo 3.3: OSI Katmanlarında Taşınan Veri Birimleri ve Katmanlara Ait Ağ Cihazları

Sıra	Katman Adı	Katmanda Taşınan Veri Birimi	Katmana Ait Ağ Cihazları
7	Uygulama	Veri	Ağ Geçiti (Getway)
6	Sunum	Veri	Ağ Geçiti
5	Oturum	Veri	Ağ Geçiti
4	Taşıma	Segment	Ağ Geçiti
3	Ağ	Paket	Yönlendirici (Router) L3Anahtar(L3 Switch)
2	Veri Bağı	Çerçeve (Frame)	Köprü (Bridge) Switch (Anahtar) Ağ arabirim kartı (NIC)
1	Fiziksel	Bit	Tekrarlayıcı (Repeater) Merkez (Hub)

3.3.1.1. OSI Modelindeki Katmanların Özellikleri

OSI modelindeki katmanların özellikleri aşağıdaki başlıklar altında incelenebilir.

Uygulama Katmanı (Application Layer / Katman 7)

OSI modelinin en üsttünde bulunan katmandır. Bu katman kullanıcının verileriyle doğrudan etkileşime girmektedir. Bilgileri doğrudan kullanıcılardan alır ve gelen verileri kullanıcıya görüntüler. Web tarayıcıları ve e-posta istemcileri gibi yazılım uygulamaları, bu katmanda hizmet vermektedir. Hiper Metin Transfer Protokolü (HTTP), Dosya Aktarım Protokolü (FTP), Posta Ofisi Protokolü (POP), Basit Posta Aktarım Protokolü (SMTP) ve Etki Alanı Adı Sistemi (DNS) gibi servis ve protokoller bu katmanda hizmet vermektedir.

Sunum Katmanı (Presentation Layer / Katman 6)

Sunum katmanı, verilerin uygulama katmanı tarafından kullanılabilmesi için hazırlanmasından sorumludur. Bu katman, gelen verileri alıcı cihazın uygulama katmanının anlayabileceği bir söz dizimine çevirmekten, verilerin dönüştürülmesinden (makine tarafından anlaşılabilir formata dönüştürme), şifrelenmesinden (verinin hassasiyetini koruma) ve sıkıştırılmasından sorumludur.

Oturum Katmanı (Session Layer / Katman 5)

Bu katmanın görevi, farklı sistemler arasındaki bağlantıyı kurmak ve sürdürmektir. İki cihaz arasındaki iletişimi açmak ve kapatmaktan sorumlu olan oturum katmanının temelde üç ana görevi bulunmaktadır.

Kimlik Doğrulama: Bir bilgisayar başka bir bilgisayar ile haberleşmeye başlamadan önce bilgisayarın kimlik doğrulaması gereklidir. Kimlik doğrulama sonrası bağlantı kurma işlevi, oturum katmanının görevidir.
Yetkilendirme: İki bilgisayar sistemi arasında bir bağlantı kurulduktan sonra oturum katmanı, bağlı bilgisayarın verilere erişme yetkisinin olup olmadığını kontrol eder. Bu yetkilendirme kontrolü de oturum katmanının görevidir.
Oturum Yönetimi: Göndericiden gelen veri paketlerinin hangi uygulamaya ait olduğunu kontrol eder.

Taşıma Katmanı (Transport Layer / Katman 4)

Taşıma katmanı, gönderilecek verilerin tamamının kaynak ana bilgisayardan hedef ana bilgisayara teslim edilmesinden sorumludur. Taşıma katmanının ana rolü, veri iletişiminin güvenilirliğini kontrol etmektir. Bu katman, verileri oturum katmanından alarak alt katmana (katman 3) göndermeden önce **segment** adı verilen parçalara ayırır.

Taşıma katmanı aynı zamanda akış kontrolü ve hata kontrolünden de sorumlu olan katmandır.

Akış Kontrolü: Farklı hızlarda veri alan ve gönderen bilgisayarlar arasında veri iletişimini sağlamak için en uygun iletim hızını belirleme işlemidir.
Hata Kontrolü: Taşıma katmanı, alınan verilerin eksiksiz olmasını sağlar. Değilse yeniden iletim talep ederek alıcı tarafta hata kontrolü işlemini gerçekleştirmektedir. TCP, SPX ve UDP protokolleri bu katmanda çalışmaktadır.

Ağ Katmanı (Network Layer / Katman 3)

Bu katmanın ana görevi, veri segmentlerini taşıma katmanından almak ve bunları bir bilgisayardan başka ağdaki bir bilgisayara aktarmaktır. Bu katman, veri paketlerinin kaynaktan hedefe uygun adresleme ve yönlendirme yoluyla teslim işlemlerini yönetmektedir. Ağ katmanı, taşıma katmanından gelen segmentleri, **paket** adı verilen daha küçük birimlere ayırır ve bu paketleri alıcı cihazda yeniden birleştirir. Verilerin hedefine ulaşması için en iyi fiziksel yolu bulma işleminden de sorumludur. Bu işlem **yönlendirme (routing)** olarak adlandırılır. RIP, EIGRP ve OSPF gibi protokoller yönlendirme işlemleri için kullanılan protokollerdir.

Veri Bağı Katmanı (Data Link Layer / Katman 2)

Veri bağlantı katmanı, paketleri ağ katmanından alır ve bunları **çerçeve (frame)** adı verilen daha küçük parçalara böler. Bu katmanın ana görevi, fiziksel katman tarafından bağlanan iki düğüm arasında bir bağlantı kurmak ve sonlandırmaktır. Bu katman iki bölümden oluşmaktadır.

Mantıksal Bağlantı Kontrolü (LLC): Ağ protokollerini tanımlayan, hata denetimi gerçekleştiren ve çerçeveleri senkronize eden katmandır.

Ortam Erişim Kontrolü (MAC): Cihazları bağlamak, veri iletmek ve veri almak amacıyla izinleri tanımlamak için MAC adreslerini kullanan katmandır.

Ağ dünyasında, anahtarların çoğu Katman 2'de çalışır. Bazı anahtarlar, yönlendirme yeteneklerine sahip olduğundan (Layer 3 Switch) Katman 3'te de çalışır.

Fiziksel Katman (Physical Layer / Katman 1)

OSI modelinin birinci ve en alt katmanıdır. Bu katmanın görevi, bireysel bitleri bir düğümden diğerine fiziksel bir ortam üzerinden iletmektir. Bu katmanda veriler **bit** olarak iletilir. Veriler, alıcı tarafındaki fiziksel katman tarafından alınır ve onu bitlere dönüştürür.

3.3.2. İletim Denetimi Protokolü / Internet Protokolü (TCP/IP) Modeli

TCP/IP çok sayıda protokol ve yardımcı programlardan oluşan bir protokol kümesidir. Günümüzün internetinde kullanılan protokoldür. TCP/IP, internet ve birçok intranet tarafından çoğu ağ protokolü paketinde yaygın olarak kullanılmaktadır. Ancak TCP/IP modeli, OSI modeliyle tam olarak eşleşmemektedir. Örneğin, OSI modelinin yedi katmanı bulunurken TCIP/IP modelinin 4 katmanı (Bazı kaynaklarda 5 katmanda incelenmiştir. Bu ders kitabında 4 katman olarak anlatılacaktır.) bulunmaktadır (Görsel 3.24). TCIP/IP Modeli İletim Kontrol Protokolü (TCP) ve İnternet Protokolü (IP) iki ana protokolden oluşmaktadır.

TCP/IP modeli, her biri belirli bir işlevsellik sağlayan etkileşimli katmanlardan oluşan hiyerarşik bir modeldir.

Görsel 3.24: OSI ve TCI/IP Modelleri Gösterimi

3.3.2.1. TCP/IP Katmanları ve Görevleri

TCP/IP modelinin katmanlarının özellikleri ve görevleri aşağıdaki başlıklar altında incelenebilir.

Ağ Erişim Katmanı

Ağ Erişim Katmanı (Donanım katmanı olarak da bilinir.), bir üst katmandan gelen bilgilerin internet ortamına iletilebilmesi için gerekli tüm fiziksel katmanların bilgilerini, yerel alan ağı ve geniş alan ağı bilgilerini düzenlemektir. Bu katman OSI protokolünün fiziksel ve veri bağı katmanına denktir.

İnternet Katmanı

IP katmanı olarak da adlandırılan bu katmanda verilerin gideceği adres veriye eklenir. İnternet katmanı, paketleri kaynak bilgisayardan hedef bilgisayara giden yol boyunca yönlendiriciden yönlendiriciye taşıyan bir protokol olan İnternet Protokolünü (IP) içerir. IP ayrıca bu katmanda kullanılan adreslerin biçimini ve yapısını da tanımlar. IP, en yaygın kullanılan ağ katmanı protokolüdür. IP, akış kontrolü, hata kontrolü ve tıkanıklık kontrol hizmetleri sağlamayan bağlantısız bir protokoldür. Bu katman, kendi yapısı içinde tek noktaya yayın (bire bir-unicast) ve çok noktaya yayın (birden çoğa-multicast) yönlendirme protokollerini içerir. En uygun yol seçimi için yönlendirme algoritmaları kullanılır.

Taşıma Katmanı

Bir mesaj, uygulama katmanından taşıma katmanına aktarılır. Taşıma katmanı bu mesajı segment olarak adlandırılan veri katarına çevirir ve mantıksal (hayali) bağlantı aracılığıyla hedef bilgisayara gönderir. Başka bir deyişle taşıma katmanı, uygulama katmanına hizmet vermekten sorumludur. Kaynak bilgisayarda çalışan bir uygulama programından bir mesaj alır ve bu mesajı hedef bilgisayardaki ilgili uygulama programına teslim eder.

Günümüz internet ağında taşıma katmanının iki standart protokolü bulunmaktadır. Bunlar İletim Kontrol Protokolü (TCP) ve Kullanıcı Datagram Protokolüdür (UDP). TCP, bağlantı odaklı bir hizmet sağlar ve tüm uygulama katmanı paketlerinin hedeflerine teslim edilmesini garanti eder. Bu garanti aşağıdaki iki mekanizmaya dayanmaktadır:

- Ağda herhangi trafik sıkışıklığı olduğunda gönderici bilgisayarın iletim hızını yavaşlatan **tıkanıklık kontrolü**
- Veri akış hızını senkronize etmek ve paket düşüşünü (paketin bozulması veya anlamsızlaşması) azaltmak için gönderici ve alıcı bilgisayarların hızlarını eşleştirmeye çalışan **akış kontrol mekanizması**

TCP, uygulama katmanı paketlerinin teslimine dair garantiler sunarken UDP ise bu tür garantiler sunmamaktadır. Sadece teslimatla ilgilenir ve onay olmadan bağlantısız bir hizmet sağlar. Ancak çok daha verimlidir, video ve müzik akışı gibi gerçek zamanlı veriler için tercih edilen bir protokoldür.

Uygulama Katmanı

OSI modelindeki uygulama katmanına çok benzeyen bu katman, kullanıcı arabirimine uygulama işlevleri açısından zengin kaynaklar sağlar. İki uygulama katmanı, sanki iki katman arasında bir köprü varmış gibi birbirleri arasında mesaj alışverişi yapar. Uygulama katmanı tüm ağ uygulamalarını destekler. Uygulama katmanı taşıma katmanıyla portlar aracılığıyla haberleşir. Portlar, numaralandırılmış standart uygulamalardır (HTTP:80, FTP:21 vs.), taşıma katmanından gelen paket içeriğinin türünün anlaşılmasında rol oynar.

3.3.3. Doğru Ağ Protokolünü Seçme ve Kullanma

Oluşturulacak ağ yapısı için kullanılması gereken ağ protokolü seçilirken değerlendirilmesi gereken bir dizi faktör bulunmaktadır. Bunlar arasında aşağıda verilen dört ana faktör ön plana çıkmaktadır:

İletişim Türü: İletişimin bağlantılı mı yoksa bağlantısız mı yapılacağının belirlendiği faktördür. Bağlantılı iletim TCP, bağlantısız iletim UDP protokolleri aracılığıyla yapıldığından güvenilir veya güvensiz iletişim yöntemi de belirlenmiş olur.

Sistem Yapılandırması: Ağ içinde kullanılacak tüm ağ cihazlarının, ağ topolojilerinin ve iletim ortamının belirlendiği faktördür. Yanlış ağ cihazı, topoloji veya yapılandırma seçimi doğrudan ağ performansını etkileyecektir.

Uygulama Kolaylığı: TCP ve UDP yüksek verimli ağ protokollerindendir. Ancak seçim aynı zamanda uygulama kolaylığını da etkilemektedir.

Maliyet: Sistem yapılandırması, iletişim türü ve uygulama kolaylığı doğrudan maliyeti etkiler. Her bir faktörde tercih edilen öncelikler ağ protokolünün işletim maliyetini de etkileyecektir.

3.3.3.1. Katmanlara Göre Kullanılabilecek Ağ Protokolleri

Katmanlara göre kullanılabilecek çeşitli ağ protokolleri aşağıda verilmiştir.

Ağ Erişim Katmanındaki Protokoller

- **ARP (Adres Çözümleme Protokolü)**, bir IP adresinin hangi ağ kartına (MAC adresine) ait olduğunu bulmaya yarayan protokoldür. TCP/IP veri iletiminde, veriyi hangi bilgisayara göndereceğini bulmak için kullanılmaktadır. IP adresini yeni almış olan bir bilgisayar, o IP adresinin sadece kendisinde olduğunu ARP kullanarak teyit eder.
- **RARP (Ters ARP) Protokolü**, ARP'nin tersi işlemi yapar. Hangi MAC adresinin hangi IP adresini kullandığını bulan protokoldür. Bir TCP/IP ağında RARP'nin çalışacağı garanti edilemez edilemez çünkü RARP bir RARP sunucusuna ihtiyaç duymaktadır.

İnternet Katmanındaki Protokoller

- **ICMP (Internet Yönetim Mesajlaşması Protokolü)**, hata ve bilgi mesajlarını ileten protokoldür. Bir ping işlemi ICMP protokolünü kullanır.
- **RIP (Router Bilgi Protokolü)**, yönlendirici cihazların, yönlendirme tablolarının otomatik olarak oluşturulması için geliştirilmiş protokoldür.
- **OSPF (En Kısa Yola Öncelik) Protokolü**, bir TCP/IP ağındaki yönlendiricilerin birbirini otomatik olarak tanımasında kullanılan protokoldür. RIP protokolündeki gibi yönlendiricilerin, yönlendirme tablolarını otomatik olarak üretebilmesini sağlar. OSPF, RIP'den daha gelişmiş bir protokoldür.
- **IGMP (Internet Grup Mesajlaşma Protokolü)**, bir sistemin internet yayınlarına (multicast) abone olmasına ve aboneliği durdurmasına yarar. Bu yayınlar, UDP üzerinden yapılır ve genelde çoklu ortam (radyo veya video) içerikli olur.
- **DHCP (Dinamik Cihaz Ayar Protokolü)**, bir TCP/IP ağına bağlanan herhangi bir cihaza otomatik olarak IP adresi, ağ maskesi, ağ geçidi ve DNS sunucusu atanması için kullanılan protokoldür.

Taşıma Katmanındaki Protokoller

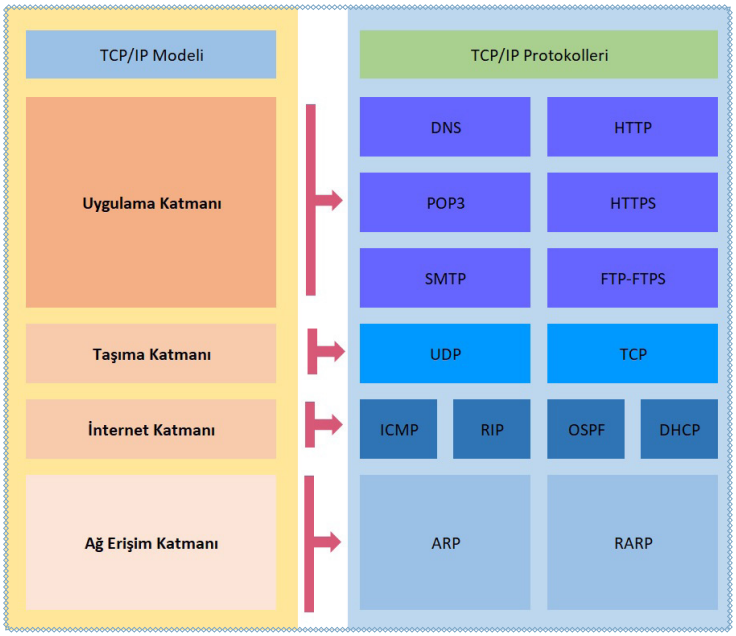
- **UDP (Kullanıcı Veri Protokolü)**, IP üzerinden veri yollamaya yarayan protokoldür. Verilerin alıcıya ulaşacağını garanti etmez. UDP paketlerinin maksimum boy sınırları vardır. UDP son derece basit ve bağlantı gerektirmeyen (connectionless) bir protokoldür.
- **TCP (Gönderim Kontrol Protokolü)**, gönderilen verilerin IP üzerinden alıcıya ulaşmasını garanti eden protokoldür. Herhangi bir boyda veri gönderilmesine imkân tanımaktadır. UDP'den farklı olarak TCP'de iki cihazın iletişim kurabilmesi için önce birbirlerine bağlanmaları gerekmektedir.

Uygulama Katmanındaki Protokoller

- **DNS (Alan Adı Hizmeti)**, alan adı olarak verilen isimler (örneğin www.meb.gov.tr) ile IP adreslerini birbirine eşleştiren sistemdir. Paylaştırılmış bir veri tabanı olarak çalışır. UDP veya TCP üzerinden çalışabilir.
- **HTTP (Hiper Metin Yollama Protokolü)**, ilk başta HTML sayfaları göndermek amacıyla geliştirilmiş olan bir protokol olup günümüzde her türlü verinin gönderimi için kullanılır. TCP üzerinden çalışır.
- **HTTPS (Güvenli HTTP)**, HTTP'nin RSA şifrelemesi ile güçlendirilmiş hâlidir. TCP üzerinden çalışır.

- **POP3 (Postane Protokolü 3)**, e-posta almak için kullanılan bir protokoldür. TCP üzerinden çalışır.
- **SMTP (Basit Mektup Gönderme Protokolü)**, e-posta göndermek için kullanılan bir protokoldür. TCP üzerinden çalışır.
- **FTP (Dosya Gönderme Protokolü)**, dosya göndermek ve almak için kullanılır. HTTP'den farklı olarak kullanıcının sisteme giriş yapmasını gerektirir. Veri ve komut alışverişi için iki ayrı port kullanır. TCP üzerinden çalışır.
- **FTPS (Güvenli FTP)**, FTP'nin RSA ile güçlendirilmiş hâlidir. TCP üzerinden çalışır.

Görsel 3.25'te TCP/IP modelindeki katmanlara karşılık gelen protokoller gösterilmiştir.



Görsel 3.25: TCP/IP modeli katmanları ile bu katmanlarda çalıştırılan protokoller

Sıra Sizde

www.meb.gov.tr adresinin IP adresini bularak internet tarayıcınızda bulduğunuz IP adresini çalıştırınız.

Uygulama 4

LAN'da bilgisayarlar haberleşmek için birbirlerinin MAC adreslerine ihtiyaç duyar. Aynı ağ içinde birbirlerinin IP adreslerini bilen iki ağ cihazının haberleşebilmesi için MAC adreslerinin bilinmesi gerekir. Bunun için ARP protokolü kullanılmaktadır.

Aşağıdaki tablo referans alınarak aynı ağ üzerinde iki cihaz birbiri ile haberleşirken gerçekleşen işlemler belirtilmiştir.

Tablo 3.4: Uygulama 4 İçin Referans Değerler

Bilgisayar	IP Adresi	MAC Adresi
PC-1	192.168.0.29	aa:bb:cc:00:11:22
PC-2	192.168.0.28	33:44:55:dd:ee:ff

1. PC-1 ağa bir istek (ARP request) paketi gönderir. ARP olarak adlandırılan bu pakette MAC adresini (aa:bb:cc:00:11:22) belirterek haberleşmek istediği IP adresinin (192.168.0.28) MAC adresini ister.
2. Bu istek paketi, tüm ağa bağlı cihazlara gönderilir (Bu işleme broadcast denir.). Çünkü her PC sadece kendi MAC numarasını bildiğinden istek paketi tüm PC'lere gönderilmesi gerekmektedir.
3. 192.168.0.28 IP numarasına sahip bilgisayar gelen istek paketine bakarak kendi IP numarasının yazılı olduğunu ve kendisinin MAC adresinin istendiğini anlar.
4. Sadece 192.168.0.28 IP adresine sahip bilgisayar bu isteği cevaplar.
5. Cevapladığı pakette (ARP reply) benim MAC adresim "33:44:55:dd:ee:ff" bilgisini gönderir.
6. Bu şekilde iki bilgisayar da (PC-1 ve PC-2) birbirlerinin IP adresini ve MAC adresini bilirler ve kendi içlerinde ARP Tablosu denilen tablolarda bu bilgiler saklanır.

Adım 1: Kendi bilgisayarınız (PC-1 olsun) üzerinde ARP tablosunu elde ediniz. Bunun için komut istemci açınız ve ***arp –a*** komutunu çalıştırınız (Görsel 3.26).

Kullanılan bilgisayarın (PC-1) IP Adresi: 192.168.0.29

```
Komut İstemi
Microsoft Windows [Version 10.0.18363.1139]
(c) 2019 Microsoft Corporation. Tüm hakları saklıdır.

C:\Users\ZMTAL_Krs11>arp -a

Interface: 192.168.0.29 --- 0xa
  Internet Address      Physical Address      Type
  100.117.73.46         fc-4a-e9-15-de-92     dynamic
  192.168.0.1           00-10-18-de-ad-05     dynamic
  192.168.0.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.2             01-00-5e-00-00-02     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

C:\Users\ZMTAL_Krs11>
```

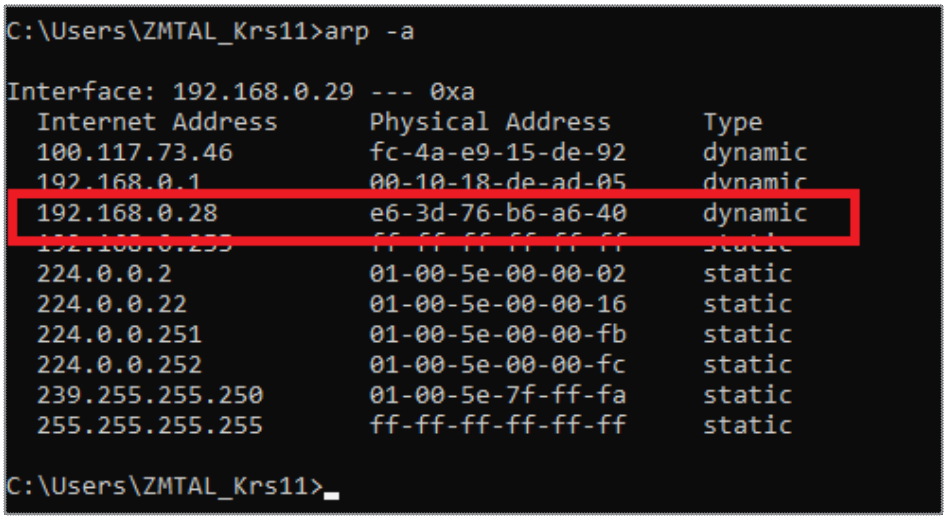
Görsel 3.26: ARP tablosunun elde edilmesi

Adım 2: İletişim kurmak istediğiniz bilgisayarın IP numarası (192.168.0.28) üzerinden haberleşmek istenilen bilgisayarın IP adresine bir istek gönderiniz. Bu işlem için komut istemciye ***ping 192.168.0.28*** yazınız ve "Enter" tuşuna basınız (Görsel 3.27).

```
C:\Users\ZMTAL_Krs11>ping 192.168.0.28

Pinging 192.168.0.28 with 32 bytes of data:
Reply from 192.168.0.28: bytes=32 time=421ms TTL=64
Reply from 192.168.0.28: bytes=32 time=1011ms TTL=64
Reply from 192.168.0.28: bytes=32 time=36ms TTL=64
Reply from 192.168.0.28: bytes=32 time=250ms TTL=64

Ping statistics for 192.168.0.28:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 36ms, Maximum = 1011ms, Average = 429ms

C:\Users\ZMTAL_Krs11>
```

Görsel 3.27: 192.168.0.29'dan 192.168.0.28'e iletişim sağlanması

Adım 3: Ping işleminde iletişim kurmak isteyen PC-1 ile iletişimi yanıtlayan PC-2 arasında MAC bilgileri paylaşımı yapılmıştır. Artık yeniden arp –a yaparak PC-1'in ARP tablosunda PC-2'nin MAC adresi kaydedilmiş olduğu görüntülenecektir (Görsel 3.28).



Görsel 3.28: ARP tablosuna yeni bir ağ cihazının MAC adresinin eklenmesi

Sıra Sizde

Komut istemci kullanarak aşağıdaki işlemleri gerçekleştiriniz.
- **RARP** ile MAC adresinden IP adresi elde etme uygulamasını yapınız ve öğretmeninize gösteriniz.
- **DCHP** üzerinden yeni bir IP adresi isteyen uygulamayı yapınız ve öğretmeninize gösteriniz.

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

1. ( ) Diğer bilgisayar ve bilgisayar sistemlerine kaynak ve / veya hizmet sağlayan bilgisayarlara istemci bilgisayar denir.

2. ( ) TCP protokolü, UDP protokolüne göre daha güvenli ancak daha yavaş bir iletişim imkânı sağlar.

3. ( ) OSI Modelinde 4 katman bulunurken TCP/IP Modelinde 7 katman bulunur.

4. ( ) Taşıma (iletim) katmanında kullanılan port numaralarından 0 ile 1023 arasındaki port numaraları "iyi bilinen portlar" olarak tanımlanmıştır.

B. Aşağıdaki soruları dikkatlice okuyunuz ve doğru seçeneği işaretleyiniz.

5. OSI Modeli Ağ Katmanında taşınan bilgi hangi isimle ifade edilir?

A) Bit B) Çerçeve C) Paket D) Segment E) Veri

6. Aşağıdakilerden hangisi Uygulama Katmanı Protokollerinden biri değildir?

A) DHCP B) HTTP C) POP3 D) SSH E) UDP

7. Aşağıdakilerden hangisi TCP/IP internet katmanı protokollerinden biridir?

A) ARP B) DNS C) FTP D) OSPF E) SMTP

ÖĞRENME BİRİMİ 4

AĞ ADRESLEME

NELER ÖĞRENECEKSİNİZ?

Bu öğrenme birimi ile;

- IPv4 adres yapısını bilecek,
- NAT türlerini kavrayacak,
- IPv6 adres yapısını bilecek,
- IPv4 sınıflarını öğrenecek,
- IPv4 ağ maskelerini kavrayacak,
- IP adres bilgilerini öğrenme işlemlerini yapacak,
- Statik IP adresi atamayı öğrenecek,
- Dinamik IP adresi atamayı öğreneceksiniz.

ANAHTAR KELİMELER

IPv4, Ethernet, çerçeve yapısı, IPv4 adres sınıfları, A sınıfı IP adresi, B sınıfı IP adresi, C sınıfı IP adresi, D sınıfı IP adresi, E sınıfı IP adresi, IPv6, NAT, ağ maskesi, DHCP, Statik IP adresi, Dinamik IP adresi

Hazırlık Çalışmaları

1. Bir bilgisayarın internete nasıl bağlandığını ve internette bilgi dolaşımının nasıl gerçekleştiğini araştırınız.
2. Uzaktaki bir büyüğünüzün bayramını kutlamak için hangi yöntemleri kullanabilirsiniz?
3. Modem ile bilgisayar, tablet, cep telefonu gibi cihazlar nasıl haberleşebilir? Düşüncelerinizi arkadaşlarınızla paylaşınız.

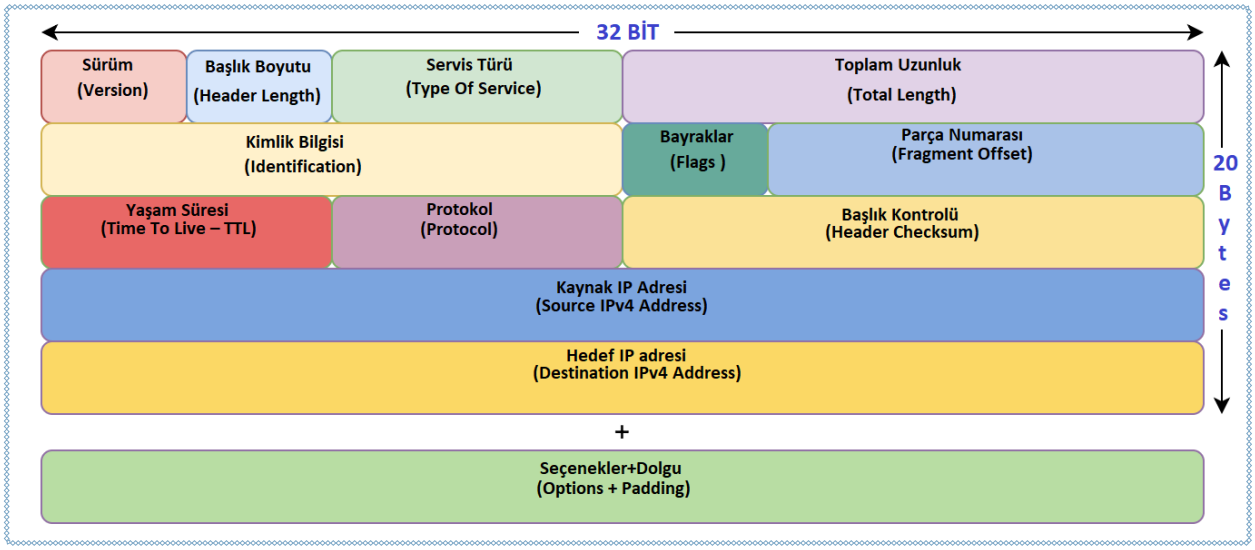
4.1. Kullanıcı Sayısına Göre TCP/IP Adres Sınıfları

TCP/IP [Transmission Control Protocol (Internet Protocol)], ağ cihazlarının birbirleriyle haberleşebilmesi amacıyla kullanılan protokol kümesidir. Örneğin evde kullanılan bilgisayar sistemleri, internete bağlanmak için TCP/IP protokolünü kullanır. Genel veya yerel ağ üzerinde haberleşecek her cihaz bir IP adresi kullanır. Kullanılan IP adreslerinin her biri birbirinden farklıdır.

IP adresleme, TCP/IP protokol kümesinin internet katmanı (OSI 3.katman / ağ katmanı) protokolü ile kullanılır.

4.1.1. IPv4 Adres Yapısı

İnternet protokolü (IP), ağ adreslemesinde temel iletişim protokolüdür. İnternet protokolü (IP), ağ cihazları arasında paketlerin yönlendirilmesini sağlayan bağlantısız bir protokoldür.



Görsel 4.1: IPv4 başlık yapısı

IPv4 başlık yapısı **32 bit** genişliğinde ve minimum **20 byte (bayt)** uzunluğundadır. Başlık yapısında bulunan alanlar ve uzunlukları Görsel 4.1'de verilmiştir. Bu alanların görevleri şunlardır:

Version (Sürüm): IP paketinin sürümünü belirten alandır. IPv4 için onluk (decimal) **4** değerine eşit olan ikilik (binary) **0100** değeridir.

Header Length (Başlık Boyutu): 4 bit olan bu alan başlık bilgisinin boyutunu gösterir.

Type Of Service (Servis Türü): 8 bitlik bu alanda paket önceliği, gecikmesi, güvenilirliği ve iletim hızı bilgileri yer alır.

Total Length (Toplam Uzunluk): IP paketinin toplam uzunluğu belirtilir. En büyük değeri 65.536 bayttır.

Identification (Kimlik Bilgisi): İletilen ve alınan paketin hangi verinin parçası olduğunu gösterir. Aynı veriyi oluşturan bütün parçalar için kimlik bilgisi değeri aynıdır.

Flags (Bayraklar): Bu alan 3 bittir ve ilk biti 0'dır. İkinci bit parçalanma bayrağıdır. Üçüncü bit ise daha fazla parçalanma bayrağıdır. Bu değer "0" ise ya o parça son parçadır ya da veri parçalanmaya uğramamıştır.

Fragment Offset (Parça Numarası): Parçaların hangi sırada birleşerek veriyi oluşturacağını gösteren 13 bit değerindeki alandır.

Time To Live–TTL (Yaşam Süresi): Paket ömrünü sınırlamak için kullanılan alandır. Amacı paket hedef adrese belirli bir sürede ulaşamazsa internette dolaşmasını engellemektir. Saniye veya durak sayısı cinsinden bir değer tutulur. Yönlendirici üzerinden her geçişte bu değer bir azalır ve "0" olduğunda paket silinir.

Protocol (Protokol): Üst katman protokol bilgilerinin bulunduğu 8 bitlik alandır. Protokol numaraları IANA'ya göre belirlenmiştir. Örnek: ICMP(0x01), TCP(0x06), UDP(0x11)

Header Checksum (Başlık Kontrolü): Pakette hata olup olmadığı bu bölümde kontrol edilir. Verinin geçtiği bütün yönlendiricilerde bu alan tekrar hesaplanarak doğrulanır.

Source IPv4 Address: Kaynak IPv4 adresini gösteren alandır.

Destination IPv4 Address: Hedef IPv4 adresini gösteren alandır.

Options (Seçenekler): Boyutu değişkendir. Gerektiği zaman kullanılmak üzere güvenlik, kaynak, yönlendirme, yolun kaydedilmesi ve zaman gibi bilgilerin tutulduğu alanlardır.

Padding (Dolgu): Paketin genişliğinin 32 bit olarak sınırlanması için kullanılan alandır.

İnternete bağlı her cihazın sadece kendisini tanımlamak için kullanılan 32 bit uzunluğunda bir IP adresi vardır. Kolayca okunabilmeleri için her biri **oktet** adı verilen 8 bit uzunluğunda dört parçaya ayrılır. Ondalık düzene çevrilir ve aralarına nokta konur. Örneğin 192.168.1.2 adresinin 32 bitlik karşılığı Tablo 4.1'de gösterilmiştir.

Tablo 4.1: IP Adresi Ondalık ve İkilik Gösterimi

Ondalık Gösterim	192	168	1	2
32 bit Gösterim	11000000	10101000	00000001	00000010

4.1.1.1. IPv4 Adres Sınıfları

Günümüz internet adresleme yapısı IP protokolünün 4. sürümü (IPv4) üzerine kurulmuştur. IPv4 adresleme sınıf (class) sistemine dayalı bir sözleşmedir. IP adresleri beş sınıfa ayrılmıştır. Bu sınıflar ve değer aralıkları Tablo 4.2'de verilmiştir.

Tablo 4.2: IPv4 Adres Sınıfları

Sınıf	**Ağ Sayısı**	**Adres Sayısı**	**İlk Oktet Değeri**	
A	125	16.777.214	0-127	00000000-01111111
B	16.382	65.534	128-191	1000 0000-1011 1111
C	2.097.152	256	192-223	1100 0000-1101 1111
D	Multicast kullanım için ayrılmıştır.		224-239	1110 0000-1110 1111
E	Gelecekte kullanım için ayrılmıştır.		240-255	1111 0000-1111 1111

A Sınıfı Adres: A sınıfı adreste ilk bit her zaman "0"dır. Ondalık olarak 0 ile 127 arasındaki adresleri kullanabileceği anlamına gelir. İlk oktet, ağı temsil ederken diğer üç oktet, kullanıcıları temsil eder. Alt ağ maskesi 255.0.0.0'dır. Dünya üzerinde A sınıfı IP adresi kullanan 126 tane ağ vardır. Her bir ağ içinde de 16.777.214 cihaz bulunabilmektedir. Geniş alan ağlarında kullanılan adres sınıfıdır. "127"ile başlayan IP adresi haricîndeki adresler kullanılabilir. Örnek: 75.48.2.5 – 10.0.0.2 – 38.1.1.253

Dikkat

127.0.0.1 dünya üzerindeki bütün bilgisayarların yerel ağ kartı testi için ayrılmıştır ve geri dönüş **(Loopback)** adresidir.

B Sınıfı Adres: B sınıfı adreste ilk oktetin ilk iki biti her zaman "10"dur. Ondalık olarak 128 ile 191 arasındaki adresleri kullanabileceği anlamına gelir. Dört oktetin ilk ikisi ağı temsil ederken diğer ikisi kullanıcıları temsil eder. Alt ağ maskesi 255.255.0.0'dır. Dünya üzerinde 16.384 tane B sınıfı IP adresi kullanan ağ vardır. Her bir ağ içinde de 65.534 cihaz bulunabilmektedir. Büyük ve orta büyüklükteki ağlar için kullanılır. Birçok büyük üniversite ve ISS'ler bu tür adres sınıfına sahiptir. Örnek: 128.1.2.3 – 148.0.0.2 – 191.254.254.38

C Sınıfı Adres: C sınıfı adreste ilk oktetin ilk üç biti "110"dur. Ondalık olarak 192 ile 223 arasındaki adresleri kullanabilir. Dört oktetin ilk üçü, ağı temsil ederken son oktet, kullanıcıları temsil eder. Alt ağ maskesi 255.255.255.0'dır. Dünya üzerinde 2.097.152 tane C sınıfı IP adresi kullanan ağ vardır. Her bir ağ içinde de 254 cihaz bulunabilmektedir. Küçük yerel ağlar için kullanılır. Örnek: 192.168.1.2 – 195.50.40.30 – 223.192.1.253

D Sınıfı Adres: D sınıfı adreste ilk oktetin ilk dört biti "1110"dur. 224 ile 239 arasındaki adresleri kullanabilir. Birden çok cihazı hedefleyen çoklu yayın (Multicast) amacıyla kullanılır.

E Sınıfı Adres: E sınıfı adreste ilk oktetin ilk dört biti "1111"dir. 240 ile 255 arasındaki adresleri bu sınıfı için ayrılmıştır. E sınıfı adresler internette kullanılamaz. IETF (Internet Engineering Task Force) E sınıfı adresleri özel araştırmalar için kendilerine ayırmıştır.

Dikkat

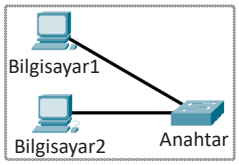
IP adreslemesinde dikkat edilmesi gereken hususlar şunlardır:

- Bir IP adresinin tamamı 0 ve 255 sayılarından oluşamaz. "0.0.0.0" bir ağ içinde IP adresi olmayan bir cihazın ilk haberleşme anında kullandığı adrestir ve **kaynak adres (source adress)** olarak bilinir.
- "255.255.255.255" adresi ise **genel yayın (Broadcast)** adresi olarak bilinir. Tüm ağa yayın yapılacağı zaman hedef adres olarak kullanılır.

Uygulama 1

IPv4 adres yapısında yerel ağ oluşturma işlemini aşağıdaki yönergeler doğrultusunda gerçekleştiriniz.

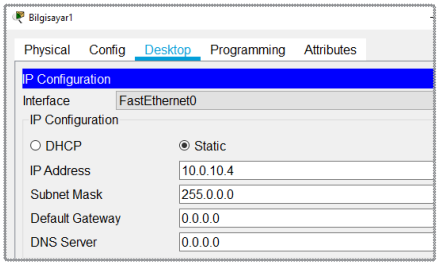
Adım 1: Ağ simülasyon programını açınız.



Görsel 4.2: Yerel ağ

Adım 2: Görsel 4.2'de verilen yerel ağı oluşturunuz.

Adım 3: Bilgisayar 1 için IPv4 adresi olarak 10.0.10.4 adresini ve 255.0.0.0 alt ağ maskesini atayınız (Görsel 4.3).

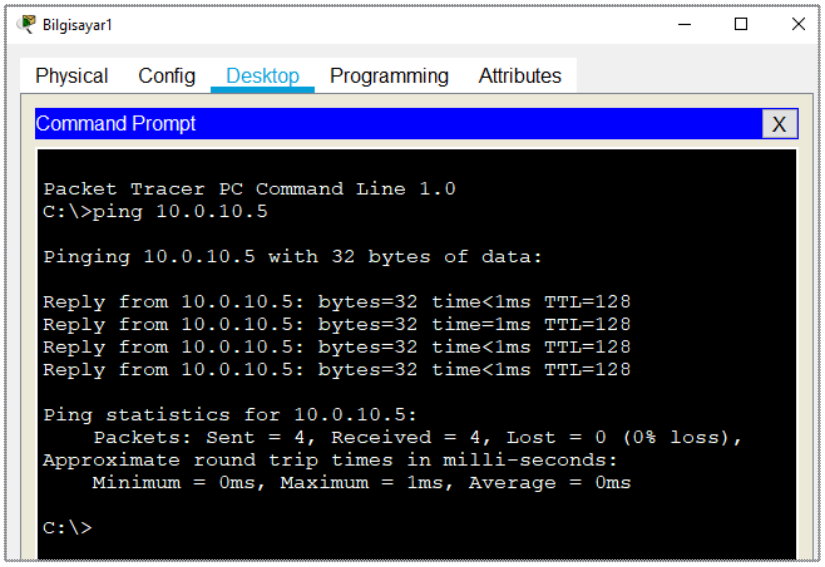


Görsel 4.3: IPv4 adresi ve alt ağ maskesi atama

Adım 4: Bilgisayar 2 için IPv4 adresi olarak 10.0.10.5 adresini ve 255.0.0.0 alt ağ maskesini atayınız.

Adım 5: Bilgisayar 1 komut ekranını açınız.

Adım 6: ping 10.0.10.5 komutunu çalıştırınız ve paketlerinin ulaştığını gözlemleyiniz (Görsel 4.4).



Görsel 4.4: Ping komutu

Sıra Sizde

Uygulama 1'de yapılan işlemin aynısını B ve C sınıfı IPv4 adresleri için gerçekleştiriniz.

4.1.1.2. Sınıfsız IPv4 Adresi (CIDR/ Classless Inter Domain Routing)

IPv4 adresi için herhangi bir sınıflama yapılmamıştır. CIDR (Classless InterDomain Routing), sınıfsız adresleme yapısında IPv4 adreslerin sonuna bir takı eklenir. IPv4 adresinden son "/" işareti ile adresin soldan sağa kaç bitinin ağı adreslediğini gösterir. Tam sayı olan bu değer **1** ile **32** arasında olabilir. Örneğin 195.24.224.13 / 24 şeklinde kullanılır. Alt ağ maskesindeki ilk 24 bit "1", kalan sekiz bit "0" değerindedir (Tablo 4.3).

Tablo 4.3: Sınıfsız IP Adresi Gösterimi

	Sınıflı Gösterim				**Sınıfsız (CIDR Gösterim)**
IPv4 adresi	195	24	224	13	195.24.224.13
Alt ağ maskesi	11111111	11111111	11111111	00000000	/24

Sınıfsız (CIDR) IP adresleme ile standart ağ maskeleri ve sınıflara göre daha verimli bir kullanım sağlar. Herhangi bir sınıfa ait IPv4 adresinden gerekli büyüklükte bir ağ elde edilebilir.

Sınıfsız IP adreslemenin getirdiği esneklik aşağıdaki örnekte açıklanmaktadır.

- Sınıflı adres yapısında C sınıfı 198.48.6.0 ağ adresini ISP (İnternet servis sağlayıcı), bir tek müşteriye verebilir. Müşteri bu ağda 254 cihaz tanımlayabilir.

- Aynı ağ adresi için CIDR'de 24 bit maske seçilerek yine C sınıfı bir adres gibi oluşturulur ve 198.48.6.0 / 24 şeklinde gösterilir.
- ISP'nin her birinde 12 ağ cihazı olan iki ağ müşterisi varsa ve ağ adresi vermek için sınıflı adresleme kullanırsa fazladan IP adresi atanmış olur. Bunun yerine CIDR ile adres üç bölüme ayrılabilir. İki tanesi bu iki müşteri için yeterli uzunlukta olacak şekilde ve geri kalanı gelecekteki müşteriler için ayrılır.
- Örneğin bir müşteriye 198.48.6.0 / 28 ve diğerine 198.48.6.16 / 28 ağ adresleri verilebilir. Böylece her iki müşteri de 14 ağ cihazına IP adresi verebilir. ISP'nin elinde ise daha sonra kullanılmak üzere 224 IP adresi kalır. Bu iki müşteri aynı alt ağ maskesini kullanır fakat farklı alt ağlarda olur (Alt Ağ Maskesi: 255.255.255.240).

Uygulama 2

192.168.1.2/25 şeklinde CIDR gösterimi yapılan IP adresinin alt ağ maskesini hesaplama işlemini aşağıdaki yönergeler doğrultusunda gerçekleştiriniz.

Adım 1: Alt ağ maskesinin ilk 25 bit değeri "1" kalan 7 bit değeri "0" olacak şekilde yazınız (Tablo 4.4).

Tablo 4.4: Alt Ağ Maskesi

Alt Ağ Maskesi	1. Oktet (8 Bit)	2. Oktet (8 Bit)	3. Oktet (8 Bit)	4. Oktet (8 Bit)
	11111111	11111111	11111111	10000000

Adım 2: İkilik sayı sistemi ile yazılan oktetleri onluk sayı düzenine çeviriniz (Tablo 4.5).

Tablo 4.5: Alt Ağ Maskesi Onluk Sayı Sistemine Dönüşümü

Alt Ağ Maskesi	1. Oktet (8 Bit)	2. Oktet (8 Bit)	3. Oktet (8 Bit)	4. Oktet (8 Bit)
İkilik sayı sistemi	11111111	11111111	11111111	10000000
Onluk sayı sistemi	255	255	255	128

Adım 3: 192.168.1.2/25 gösterimine ait alt ağ maskesi olarak 255.255.255.128 değerini elde ediniz.

Araştırma

/32 maskesi ile kaç adet ağ cihazının adreslenebileceğini araştırınız.

Sıra Sizde

18.81.0.0/1 şeklinde tanımlanan bir ağ adresi kullanılmak istenirse neler olabilir? Düşüncelerinizi arkadaşlarınızla paylaşınız

4.1.1.3. Özel IP Adresleri (Private IP Address)

A, B, C IP adresi sınıfları içinde IANA tarafından rezerve edilen 3 adres bloku vardır. Bu IP adresleri, yerel bir ağın kendi içinde ağ katmanı seviyesinde haberleşebilmesi için kullanabileceği IP adresi havuzu olarak tanımlanabilir.

Örneğin okul veya evdeki bilgisayarların IP yapılandırılmaları bu şekildedir.

Özel IP adres blokları arasındaki aynı adresler dünyada farklı yerel ağlar tarafından kullanılır (Tablo 4.6).

Tablo 4.6: Özel IP Adresleri

Sınıfı	Başlangıç IP Adresi	Bitiş IP adresi
A	10.0.0.0	10.255.255.255
B	172.16.0.0	172.31.255.255
C	192.168.0.0	192.168.255.255

Özel IP adresleri sadece yerel ağda kullanıldığı için internete yönlendirilmez. Bu aralıkta IP adreslerini kullanan yerel ağların internet çıkışı için servis sağlayıcılar tarafından belirlenmiş resmî (public) IP'ye ihtiyacı vardır.

Her IP adres sınıfında belirli IP adresleri ağ üzerindeki cihazlara atanamaz. Bu adresler aşağıda başlıklar hâlinde belirtilmiştir.

Ağ Adresi: Ağı tanımlamak için kullanılan adrestir. Kullanıcı bitlerinin tamamı 0 (sıfır) olan adresler, ağ adresi için özel olarak ayrılmıştır. Örneğin, A sınıfı için **10.0.0.0** IP adresi bir kullanıcıya asla verilemez.

Genel Yayın (Broadcast) Adresi: Ağa bağlı tüm cihazlara veri yollamak için "genel yayın adresi" gereklidir. Genel yayın (Broadcast) adresleri, IP adresinin kullanıcı için ayrılmış oktetlerindeki tüm bitlerin 1 yapılması ile elde edilir. Örneğin, A sınıfı için **10.255.255.255** IP adresi bir kullanıcıya asla verilemez.

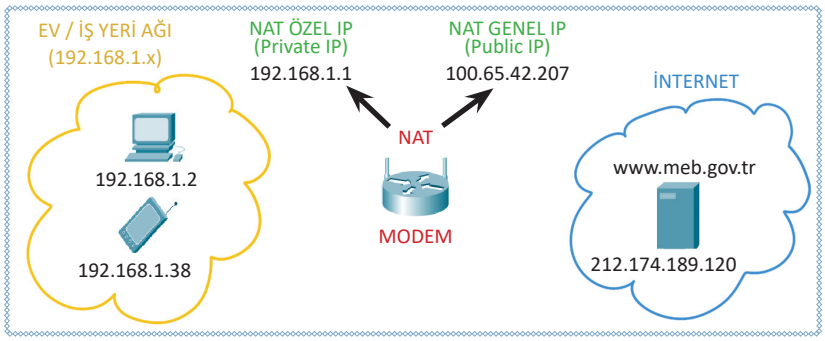
Dikkat

Ağ ve alt ağlarda, kullanılabilir IP adresi adedinden iki eksik IP adresi cihazlara atanabilir çünkü her ağın veya alt ağın, kendi ağ adresinin tanımlanması ve genel yayın adresi için birer adet olmak üzere iki adet IP adresine ihtiyacı vardır.

4.1.2. NAT [Network Address Translation (Ağ Adresi Çeviricisi)]

NAT [Network Address Translation (Ağ Adresi Çeviricisi)]; bir ağda bulunan cihazın, kendi ağı dışında başka bir ağa veya internete erişmek için farklı bir IP adresi kullanabilmesi için geliştirilen bir internet protokolüdür. IPv4 sisteminin adres yetersizliği sebebiyle NAT sistemi kullanılmaktadır. İnternet servis sağlayıcıları, iş yerlerinde ve evlerde internet bağlantısı için abonelerine tek bir genel (public) IP adresi tanımlar. Bu IP adresi üzerinden yerel ağda bulunan diğer cihazların internete erişmesi için NAT protokolü kullanılır.

NAT sayesinde evde bulunan ve internete bağlanan bütün cihazlar için ayrı birer genel (public) IP adresine ihtiyaç kalmaz. Evdeki cihazlar (cep telefonu, bilgisayar, televizyon vb.), modemde bulunan yönlendirici tarafından oluşturulan yerel ağa dâhil olarak birer özel (private) IP adresi alır. Bu cihazların internet ortamına çıkışı yapılırken yerel ağda kullandıkları IP adresleri, modem içinde bulunan yönlendirici tarafından NAT işlemine tabi tutulur.Servis sağlayıcının verdiği genel IP adresine dönüştürülür (Görsel 4.5). Bu işlem NAT tablosuna kaydedilir.



Görsel 4.5: NAT işlemi

Dikkat

NAT işleminin sağladığı bir başka avantaj da yerel IPv4 adreslerini dış ağlardan gizleyerek ağın gizliliğini ve güvenliğini artırmasıdır.

4.1.2.1. Statik NAT

Statik NAT, yerel ağda kullanılan özel IP adreslerini genel IP adreslerine ağ yöneticisi tarafından elle eşleştirilmesidir. NAT tablosuna kaydedilmeyen yerel ağdaki IP adresleri internet ortamına çıkamaz.

4.1.2.2. Dinamik NAT

Dinamik NAT, NAT yönlendiricisi üzerinden yerel ağdaki IP adreslerinin internete erişimi esnasında genel IP adresleriyle otomatik olarak eşleştirir. Yeterli sayıda genel IP adresi varsa yerel ağdaki cihazların hepsi otomatik olarak eşleşerek internete çıkabilir. Yeterli sayıda genel IP adresi yoksa ilk eşleşen cihaz internete çıkar. Bu cihazın bağlantısı kesildikten ve NAT tablosundan silindikten sonra bir diğer cihaz internete çıkabilir.

4.1.2.3. Overload NAT (Aşırı Yüklemeli NAT)/PAT

Aşırı yüklemeli NAT (Overload NAT) olarak da bilinen **port adresi çevirisi** (PAT), çok sayıda ağ cihazının özel IP adreslerinin daha az sayıda veya tek bir genel IP adresine eşleştirilmesidir. Pek çok ev veya küçük iş yerlerindeki modem ya da yönlendiriciler bu şekilde çalışmaktadır. İnternet servis sağlayıcısından yönlendiriciye tek bir adres verilir, ancak ev veya iş yerinde pek çok cihaz internete aynı anda erişebilir. Kullanımı en yaygın NAT biçimidir.

Bir ağ cihazı, TCP/IP oturumu başlattığında oturumu tanımlamak için benzersiz şekilde üretilen bir TCP veya UDP kaynak port değeri belirler. NAT yönlendiricisine yerel ağdan bir veri paketi geldiğinde cihazın yerel IP adresiyle birlikte kaynak port numarasını da NAT/PAT tablosuna kaydeder (Tablo 4.7).

Tablo 4.7: NAT/PAT Dönüşümü

Cihaz IP Adresi	Kaynak Portu	NAT Özel IP Adresi	NAT Genel IP Adresi
192.168.1.2	12345	192.168.1.2:12345	100.65.42.207:12345
192.168.1.38	14785	192.168.1.38:14785	100.65.42.207:14785

Dikkat

Ağda bulunan farklı cihazların aynı kaynak port numarasını göndermesi durumunda ikinci gelen port numarası bir arttırılarak kaydedilir.

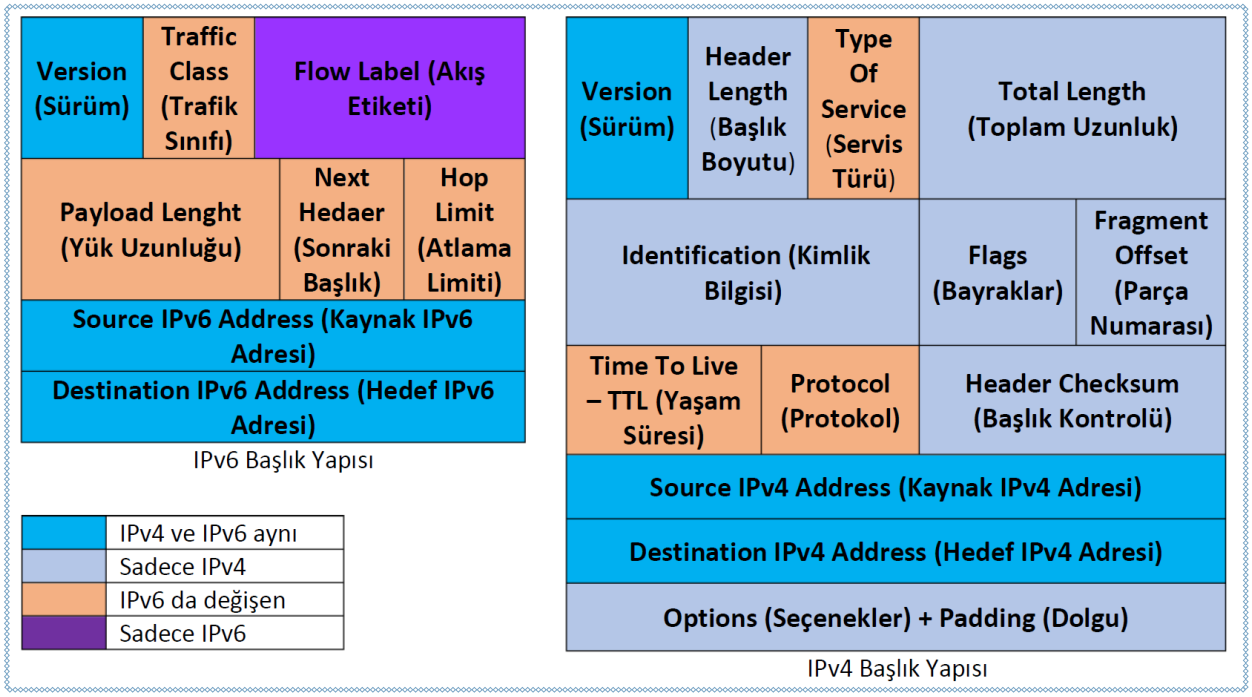
4.1.3. IPv6 Adres Yapısı

IPv6, TCP/IP'nin yönlendirme katmanı için geliştirilen yeni nesil protokoldür. İnternete bağlanan cihaz sayısının her geçen gün artmasıyla 32 bitlik mevcut IPv4 adres yapısı yetersiz kalmaya başlamıştır. Protokollerden sorumlu IETF (Internet Engineering Task Force) tarafından üniversiteler, endüstri devletler ve çeşitli organizasyonların ortak çalışmaları ve araştırmalarıyla 128 bitlik IPv6 geliştirilmiştir.

Bu genişlemenin sağladığı teorik adreslenebilir düğüm sayısı yaklaşık olarak $340x10^{33}$ adettir. IPv6 ile yapılan değişiklikler sadece adres sayısı ile kalmayıp protokol tamamen yenilenmiştir. Bu yenilemeyle başlık yapısı sadeleştirilmiş, servis kalitesi ve güvenlik özellikleri arttırılmış, otomatik adres yapılandırılması gibi özellikler geliştirilmiştir.

4.1.3.1. IPv6 Başlık Yapısı

IPv6 ve IPv4 arasındaki farklar, başlık yapıları incelendiğinde açık bir şekilde ortaya çıkmaktadır (Görsel 4.6).



Görsel 4.6: IPv4 ve IPv6 başlık yapısı

IPv4 ve IPv6 arasındaki farklar şunlardır:

- Her iki protokolde de bulunan 4 bitlik "Sürüm" bölümü IPv4 için 4, IPv6 için 6 değerini almaktadır.
- IPv6 veri paketleri 40 baytlık sabit uzunlukta başlık bilgisine sahip olduğu için IPv4 başlığında bulunan "Toplam Uzunluk" bölümü IPv6'da kaldırılmıştır. Ağ cihazları başlık uzunluğunun algılanması için harcanan zaman ve işlem gücünden tasarruf etmektedir.
- "Servis Tipi" ve "Trafik Sınıfı" alanları öncelik atama ve servis kalitesi (Quality of Service) gibi fonksiyonlarda kullanılmaktadır.
- "Akış Etiketi" kısmı IPv6'yla getirilen yeni bir özelliktir. IPv6 da tercihli olarak kullanılabilen bu bölümle beraber, gerçek zamanlı verilerin bu bölümdeki etiketlere bakılarak hızlı bir şekilde yönlendirilmesi ya da MPLS (Multi Protocol Label Switching) gibi alt katmandaki teknolojilerin verimli kullanılması mümkün olmaktadır.
- IPv6 başlık yapısındaki en önemli değişiklerinden biri yönlendirici gibi ağ cihazlarında parçalama ve hata kontrolü yapılmamasıdır. Bu işlemler üst protokol olan TCP tarafından yapılmaktadır. Böylece bu işlevleri yerine getirmek için kullanılan "Tanıtım", "Bayraklar", "Parça Telafisi" ve "Başlık Sağlama Toplamı" alanları IPv6'da bulunmamaktadır.
- "Yaşam Süresi" ve "Sıçrama Limiti" alanları farklı adlandırılmış olsalar da aynı işlevi gerçekleştirmektedir. Veri paketinin ağ üzerinde ne kadar süre kalacağına karar vermek için kullanılır.
- "Sonraki Başlık" ise bir üst katmanda kullanılacak protokolü belirtmektedir.

4.1.3.2. IPv6 Adresi Gösterim Şekli

IPv4 adresleri gibi onluk (decimal) değil, onaltılık (hexadecimal) sayı sistemi ile ifade edilir. IPv6 adreslerinin üç farklı gösterim şekli bulunmaktadır.

- Tercih edilen gösterim şekli, her biri 16 bit uzunluğu olan X:X:X:X:X:X:X:X şeklinde 8 blok hâlindedir. Blokların arası "**:**" ile ayrılır. Örnek olarak **ABCD:0001:2345:FEDC:6789:0009:8765:4321** adresi verilebilir. Aynı adres, **ABCD:1:2345:FEDC:6789:9:8765:4321** şeklinde blokların sol tarafındaki sıfırlar yazılmadan da kısaltılmış şekilde gösterilebilir.
- Bazı IPv6 adreslerinde arka arkaya gelen uzun sıfır dizileri bulunmaktadır. Bu adresleri daha kolay ifade edebilmek amacıyla sıfırları sıkıştırarak oluşturulmuş olan gösterim geliştirilmiştir. Buna göre "**::**" gösterimi bir ya da daha fazla 16 bitlik sıfır dizisini göstermektedir. Bir adreste "**::**" işareti sadece bir defa kullanılabilir (Tablo 4.8).

Tablo 4.8: IPv6 Kısaltılmış Gösterim

Genel Gösterim	Kısaltılmış Gösterim
2001:BDE0:4838:0:0:0:0:1	2001:BDE0:4838::1
FFFA:0:0:0:0:0:0:255	FFFA::255
ABC0:0:0:0:9632:0:0:AA	ABC0::9632:0:0:AA
0:0:0:0:0:0:0:1	::1

- IPv4 ve IPv6 adresleri, uyumluluk için birlikte kullanılabilmektedir. Bu gibi durumlar için X:X:X:X:X:X:A.A.A.A şeklindeki gösterimde X'ler 16 bitlik altı adet bloku onaltılık sayı sisteminde, A'ler ise 8 bitlik dört adet bloku onluk sayı sisteminde göstermektedir. Bu gösterimde A ile ifade edilen kısımlar, standart IPv4 adresleme gösterimidir (Tablo 4.9).

Tablo 4.9: IPv4 ve IPv6 Birlikte Gösterim

Genel Gösterim
2001:4BD0:0:0:0:0:100.64.50.117
0:0:0:0:0:FFFF:128.45.192.2

IPv4 adres yapısında kullanılan genel yayın (Broadcast) adresleri, IPv6 adres yapısında kullanılmamaktadır. Genel yayın görevleri de çoklu gönderim (Multicast) adresleri tarafından yapılır. Böylece hem işlemci verimli kullanılır hem de gereksiz ağ trafiği azaltılır. **FF00::/8** IPv6 adres düzeni çoklu gönderim adresleri için tahsis edilmiştir.

Dikkat

IPv6 adreslemede **0:0:0:0:0:0:0:0 (::)** adresi boş adres, **0:0:0:0:0:0:0:1 (::1)** adresi de loopback (geri) için saklı tutulmuş özel adreslerdir.

Araştırma

IPv6 adres yapısındaki "**::**" adresi ile "**::1**" adreslerinin IPv4 adres yapısındaki karşılıklarını araştırınız.

Sıra Sizde

IPv4 ve IPv6 protokollerinin kıyaslamasını arkadaşınızla birlikte sunum hazırlayarak sınıfta paylaşınız.

4.1.4. Alt Ağ Maskesi

IPv4 adresinin bir bölümü ağı, bir bölümü de cihazın ağdaki numarasını göstermektedir. Bu bölümler ön ek / ağ kimliği (Prefix/Network ID) ve son ek / cihaz kimliği (Suffix/Host ID) olarak adlandırılır. Bu iki bölümden oluşan hiyerarşi, veri paketinin iletilmesinde yönlendirilmesini kolaylaştırır.

Ağ Kimliği (Prefix/Network ID): IP adresinin prefix bölümü, ağ cihazının bağlı bulunduğu ağın adresidir. Bu adrese **ağ adresi** (network address) denir. Bu adres, bir ağa bağlı tüm cihazların IP adreslerinde prefix (ön ek) olarak yazılacak olan adrestir.

Cihaz Kimliği (Suffix/Host ID): IP adresinin suffix bölümü, bir ağ içindeki bir ağ cihazını diğer ağ cihazlarından ayıran bölümdür. Bir ağ içinde bulunan her bir cihazı tanımladığı için kullanılan tüm suffix'ler farklı olmak zorundadır. IP adresinin suffix bölümüne host adresi denir.

Bir cihaz, sahip olduğu IP adresinin hangi bölümünün ağı (prefix), hangi bölümünün ağdaki cihazları (suufix) tanımladığını anlamak için alt ağ maskesi adı verilen bir değer kullanılır. Alt ağ maskesi ile IP adresine mantıksal **VE** (And) işlemi uygulandığında elde edilen sonuç, ağın sahip olduğu IP adresini vermektedir. Örneğin IP adresi 192.168.48.2 bir cihaz ve alt ağ maskesi 255.255.255.0 olan bir ağın IP adresi 192.168.48.0'dır (Tablo 4.10).

Tablo 4.10: Ağ Maskesi ile Ağ Adresi Bulma

11000000.	10101000.	0011 0000.	0000 0010	(192.168.48.2)	IP Adresi
11111111.	11111111.	11111111.	0000 0000	(255.255.255.0)	Ağ Maskesi
Mantıksal VE (And) işlemi					
11000000.	10101000.	011 0000.	0000 0000	192.168.48.0	Ağ Adresi
Ağ Kimliği (Prefix/Network ID)			Cihaz Kimliği (Suffix/Host ID)		

Alt ağ maskesi kullanılarak elde edilen adresler ile ağdaki bir cihaz, iletişim kurmak istediği cihaz ile aynı ağda olup olmadığını belirleyebilir. Ağ cihazı kendi ağından farklı bir ağdaki cihaza erişmeye çalıştığı durumlarda yerel ağ dışına çıkabilmesi için bir yönlendiriciye ihtiyaç duyulur. Bu yönlendiricinin IP adresi, **ağ geçidi** olarak adlandırılmaktadır. Yönlendiriciler farklı ağlara göndereceği paketi, hedef IP adresindeki NetID (Ağ No.su) kısmına bakarak yönlendirir.

Uygulama 3

Aşağıda Tablo 4.11'de IP adresleri ve ağ maskeleri verilen cihazların hangi ağda olduğunu bulmak için hesaplama işlemini aşağıdaki yönergeler doğrultusunda gerçekleştiriniz.

Tablo 4.11: IP Adresleri ve Ağ Maskeleri

	IP adresi	Ağ maskesi
Cihaz 1	128.154.25.254	255.255.0.0
Cihaz 2	179.168.1.3	255.255.255.0
Cihaz 3	128.154.48.2	255.255.0.0
Cihaz 4	179.168.38.234	255.255.255.0

Adım 1: IP adreslerini ve ağ maskelerini "mantıksal VE" işlemine tabi tutunuz, elde ettiğiniz sonuçları defterinize yazınız (Tablo 4.12).

Tablo 4.12: Mantıksal VE İşlemi

	Cihaz 1	Cihaz 2	Cihaz 3	Cihaz 4
IP Adresi	128.154.25.254	179.168.1.3	128.154.48.2	179.168.38.234
Ağ Maskesi	255.255.0.0	255.255.255.0	255.255.0.0	255.255.255.0
Mantıksal VE İşlemi				
Ağ Adresi	128.154.0.0	179.168.1.0	128.154.0.0	179.168.38.0

Adım 2: Bulduğunuz ağ adreslerini inceleyiniz. Cihaz 1 ve Cihaz 3'ün 128.154.0.0 ağında olduğunu, Cihaz 2 ve Cihaz 4'ün 179.168.38.0 ağında olduğunu gözlemleyiniz.

Sıra Sizde

IP adresleri verilen cihazların hangi ağda olduklarını hesaplayınız (Tablo 4.13).

Tablo 4.13: IP Adresleri ve Ağ Maskeleri

	IP adresi	Ağ maskesi
Cihaz 1	192.168.18.81	255.255.0.0
Cihaz 2	192.168.19.38	255.255.0.0
Cihaz 3	172.16.5.2	255.255.255.0
Cihaz 4	172.16.3.254	255.255.0.0
Cihaz 5	188.19.20.0	255.255.0.0
Cihaz 6	188.119.38.0	255.0.0.0
Cihaz 7	29.10.19.23	255.255.255.0

4.2. Ağ Cihazlarına TCP/IP Adresi Girişi

Ağ cihazlarının birbirleriyle doğru bir şekilde haberleşebilmeleri için IP adreslerinin, ağ maskelerinin ve varsayılan ağ geçidi adreslerinin doğru bir şekilde yapılandırılması gerekmektedir.

4.2.1. IP Adresi Atama Türleri

Ağa bağlanan cihazların IP adreslerinin yapılandırılmasında elle (Manuel / Statik) ya da otomatik (Dinamik) olmak üzere iki yöntem kullanılır.

4.2.1.1. Elle (Manuel) IP Adresi Atama

Ağda bulunan tüm cihazların IP adreslerinin ağ yöneticisi tarafından elle sabit olarak atanmasıdır. Elle IP adresi atanırken cihazın; IP adresi, alt ağ maskesi, varsayılan ağ geçidi ve DNS sunucu adreslerinin doğru bir şekilde

atamasının yapılması gerekmektedir. Cihazın adres atamalarından bir tanesinin hatalı olması, iletişim esnasında problemlere sebep olacaktır. Özellikle büyük ağlarda bu yöntem, hatalı adres tanımlaması yapma olasılığı sebebiyle elverişsizdir. Birden fazla cihaza aynı IP adresi atanması "IP çakışması" sorununu ortaya çıkaracaktır. Böylece ağ üzerindeki paketler doğru hedefe ulaşmayacağı için cihazların iletişim kuramamasına neden olacaktır.

Elle IP yapılandırılması özellikle ağ sunucuları, yazıcılar gibi adresinin değişmesi sorun olabilecek ağ cihazlarında kullanılır.

4.2.1.2. Dinamik Bilgisayar Konfigürasyon Protokolü (DHCP)

Dinamik yapılandırmada cihazlara IP adresi, alt ağ maskesi gibi TCP/IP parametrelerinin belirlenen adres havuzu içinden atamasının yapılmasıdır. Bu işleme **Dinamik Makine Yapılandırma Protokolü-DHCP (Dynamic Host Configuration Protocol)** denir.

TCP/IP parametrelerinin her ağ cihazına elle girilmesi zaman kaybına yol açarken ayrıca yanlış yazılma olasılığı da vardır. DHCP ile otomatik IP adresi ataması güvenli ve kullanışlı bir yöntemdir. Sisteme DHCP sunucusu (modem, yönlendirici, anahtar, server vb.) kurulduktan sonra ağ cihazlarına belirlenen IP adresi aralığından (havuzundan) belirli bir süre için atama yapılır. Bu işleme **IP adresi kiralama** da denir.

DHCP ile IP adresi atama işlemi dört aşamada gerçekleşir:

- IP adresi olmayan cihaz (istemci) **DHCP DISCOVER (DHCP KEŞİF)** mesajı ile ağda bulunan DHCP sunucudan IP adresi ister. Bu mesajda cihazın IP adresi 0.0.0.0 ve hedef IP adresi 255.255.255.255'tir.
- DHCP sunucusu veri tabanına bakarak istemciye vereceği IP adresini ve ne kadar süre ile vereceğini belirler. Sunucu belirlenen bu bilgileri onaylanması için istemciye geri gönderir. Bu mesaja **DHCP OFFER (DHCP ÖNERİ)** denir.
- IP adresi isteğinde bulunan istemci, IP adresini kabul edip kiraladığına dair **DHCP REQUEST (DHCP İSTEK)** mesajını DHCP sunucuya gönderir.
- Mesajı alan sunucu, istemciye gereken IP adresini, ağ maskesini, varsayılan ağ adresi, DNS adresi bilgilerini **DHCP ACKNOWLEDGEMENT (DHCPACK / DHCP ONAY)** mesajı ile gönderir.

Bu mesajı alan istemci (ağ cihazı) artık TCP/IP haberleşmesi kullanarak ağda iletişime geçebilir.

Dikkat

DHCP ile IP adresi atama işlemi, genel yayın (broadcast) mesajlarıyla olduğu için ağı oluşturan her bölümde bir DHCP sunucusu olmalıdır ya da diğer bölümlerde IP atama işlemi hizmetini veren DHCP sunucusuna yönlendirme yapılmalıdır.

4.2.2. DHCP ile IP Adresi Atama

DHCP ile otomatik IP adresi atamak için IP adresini alacak cihazın ayarlarından otomatik IP yapılandırmasına izin verilmelidir.

Uygulama 4

Bilgisayarınıza DHCP ile IP adresi atama işlemini aşağıdaki yönergeler doğrultusunda gerçekleştiriniz.

Adım 1: Bilgisayarınızın **Ayarlar** menüsünü açınız.

Adım 2: Açılan pencereden **Ağ ve İnternet** menüsünü açınız.

Adım 3: Karşınıza gelen ekranda **Ağ durumu** bölümünden **Özellikler** butonunu tıklayınız.

Adım 4: Açılan pencereden **IP ayarları** bölümünde **Düzenle** butonunu tıklayınız.

Adım 5: Karşınıza gelen **IP ayarlarını düzenle** penceresinden "**Otomatik**"i **(DHCP)** seçiniz.

Adım 6: Kaydet butonunu tıklayınız.

Adım 7: Özellikler bölümünden IP adresinizi kontrol ediniz.

Uygulama 5

http://kitap.eba.gov.tr/KodSor.php?KOD=21033

Ağ simülasyon programında cihazlara otomatik IP adresi atama işlemini aşağıdaki yönergeler doğrultusunda gerçekleştiriniz.

Adım 1: Ağ simülasyon programını çalıştırınız.

Adım 2: Bir wireless modem (kablosuz modem) ekleyiniz.

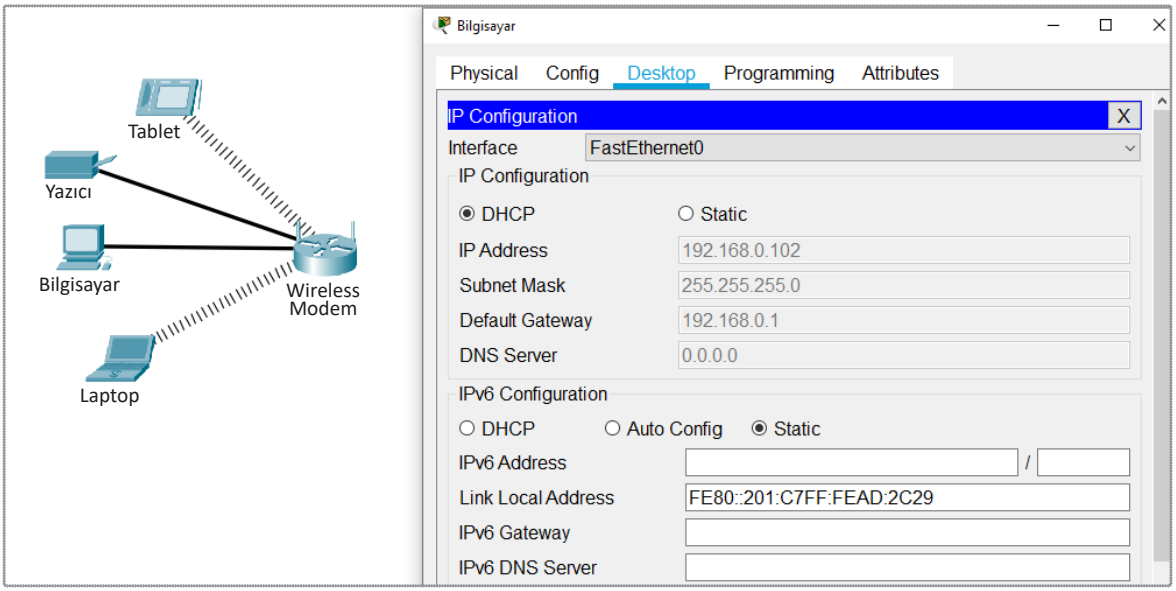
Adım 3: Bir bilgisayar, bir laptop, bir yazıcı ve bir tablet ekleyiniz.

Adım 4: Bilgisayar ve yazıcının modeme kablo ile bağlantısını yapınız.

Adım 5: Bilgisayar arayüz ekranından IP ayarları ekranını açarak **IP Configuration** sekmesinden **DHCP**'yi seçiniz.

Adım 6: Aynı işlemi diğer ağ cihazları için de gerçekleştiniz.

Adım 7: DHCP üzerinden otomatik IP adresi alıp almadığını kontrol ediniz (Görsel 4.7).



Görsel 4.7: DHCP üzerinden otomatik IP adresi atama

Sıra Sizde

Evde kullandığınız ağ cihazlarının modem üzerinden DHCP ile otomatik IP adresi atamasını yapınız.

4.2.3. Atanmış IP Bilgilerini Öğrenme

Bilgisayarlara atanmış IP adreslerini, ağ maskesini ve diğer TCP/IP parametrelerini öğrenmek için komut istemcisinde **ipconfig** komutu çalıştırılır. **ipconfig** komutunun parametrelerini ve kullanım örneklerini görmek için " **/?**" (soru işareti) parametresi çalıştırılır.

Uygulama 6

http://kitap.eba.gov.tr/KodSor.php?KOD=21034

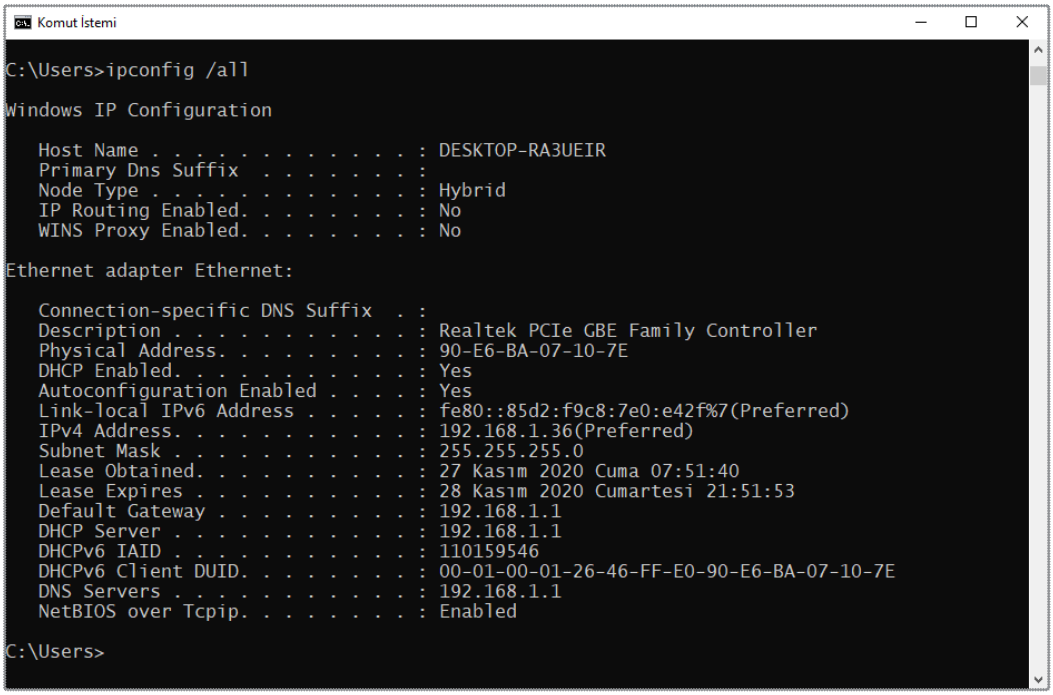
ipconfig komutuyla bilgisayarınızın IP adresi ve diğer TCP/IP parametrelerini öğrenme işlemini aşağıdaki yönergeler doğrultusunda gerçekleştiriniz.

Adım 1: Bilgisayarınızın komut istemcisini çalıştırınız.

Adım2: ipconfig /? komutunu çalıştırarak kullanılabilecek parametreleri, açıklamalarını ve kullanım örneklerini görünüz.

Adım 3: ipconfig komutunu tek çalıştırınız ve atanmış IP adresi, alt ağ maskesi ve varsayılan ağ geçidi adreslerini inceleyiniz.

Adım4: ipconfig /all komutu ile bilgisayarınıza atanmış tüm TCP/IP protokol kümesi yapılandırmalarını inceleyiniz (Görsel 4.8).



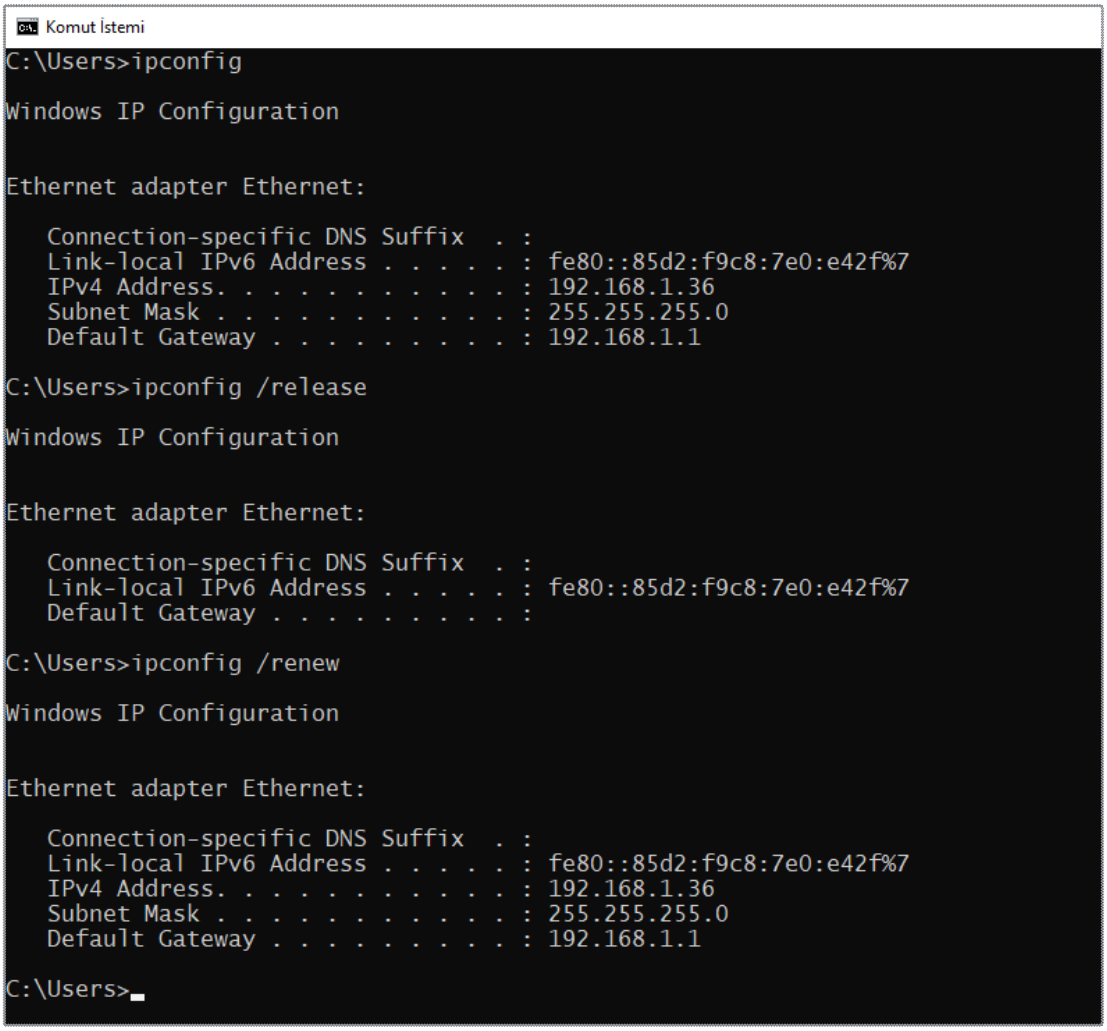
Görsel 4.8: ipconfig /all komutu

Adım 5: ipconfig /release komutu ile DHCP tarafından atanmış IP adresi bilgilerini temizleyiniz.

Adım 6: ipconfig /renew komutu ile DHCP tarafından yeni IP adresi bilgilerini atayınız (Görsel 4.9).

Dikkat

"**release6 ve renew6**" parametreleri IPv6 adres bilgileri için kullanılır.



Görsel 4.9: ipconfig, release ve renew komutları

Adım 7: ipconfig /flushdns komutu ile DNS önbelleğini temizleyiniz.

4.2.4. IP Adresi Atama Türü Seçme

Ağda bulunan farklı cihazların birbirleriyle iletişimde bulunabilmesi için bir IP adresine sahip olması gerekir. Bu IP adresi dinamik (DHCP) ya da statik (elle) olmak üzere iki farklı şekilde verilebilir.

Elle (Statik) IP adresi atama işleminde cihaza verilen IP adresi rezerve edilir. Cihaz devamlı aynı IP adresini kullanarak bağlantı yapar.

Elle IP atamanın avantaj ve dezavantajları şunlardır:

- Cihazlara uzaktan erişmek istendiğinde IP adresinin statik olması gerekir.
- İnternet ortamında statik IP adresleri genellikle kamu kurumları, büyük özel işletmeler, web siteleriyle veri merkezlerinin barındığı sunucu gibi yerlerde kullanılır. Bu tür yerlerin IP adresinin sürekli değişmesi bu yerlere ulaşmayı engeller.
- Ev / küçük iş yeri gibi ortamlarda ağ üzerinde yazıcı, depolama alanları gibi cihazların IP adreslerinin statik olması onlara ulaşımı kolaylaştırır.
- Taşınabilir cihazlarla başka ağlara bağlanıldığında elle IP atama işleminin bağlanılan ağa göre yeniden yapılması gerekir.
- Hatalı IP adresi yazımı gibi durumlarda bağlantı gerçekleşmez.

Örneğin Millî Eğitim Bakanlığının web sayfasının (www.meb.gov.tr) bulunduğu web sunucusunun IP adres ataması "**212.174.189.120**" şeklinde statik olarak yapılmıştır.

Dinamik IP adresi atama işlemindeyse cihaz, ağa her bağlandığında yeniden IP adresi tanımlanır. Her seferde, IP adres havuzundan geçici olarak bir adres tahsis edilir.

Dinamik IP atama işlemlerinin tercih edilme sebebi şunlardır:

- Ev ve küçük iş yeri gibi ortamlarda bilgisayar, cep telefonu gibi son kullanıcı cihazların IP adresi atama işlemleri dinamik yapılarak hata olasılığı ortadan kaldırılır.
- İnternet ortamında IP adresinin değişmesinin sorun olmadığı cihazlarda kullanılır.
- Büyük ağlarda IP atama işlemlerin hatasız ve hızlı yapılmasını sağlar.
- Ağa sürekli farklı cihazların bağlanması durumunda kullanılır.

4.2.5. Cihazlara Elle IP Adresi Atama

Ağ cihazlarına elle IP adresi ataması yapılırken ağ geçidi adresi bilinmelidir. Evlerde / iş yerlerinde ağ geçidi adresi modemin üzerinde ve kullanma kılavuzunda bulunur.

Uygulama 7

Bilgisayarınıza elle IP adresi atama işlemini aşağıdaki yönergeler doğrultusunda gerçekleştiriniz.

Adım 1: Bilgisayarınızın **Ayarlar** menüsünü açınız.

Adım 2: Açılan pencereden **Ağ ve İnternet** menüsünü açınız.

Adım 3: Karşınıza gelen ekranda **Ağ durumunu** bölümünden **Özellikler** butonunu tıklayınız.

Adım 4: Açılan pencereden **IP ayarları** bölümünde **Düzenle** butonunu tıklayınız.

Adım 5: Karşınıza gelen **IP ayarlarını düzenle** penceresinden "El ile girilen" seçiniz.

Adım 6: IPv4'ü açık hâle getiriniz.

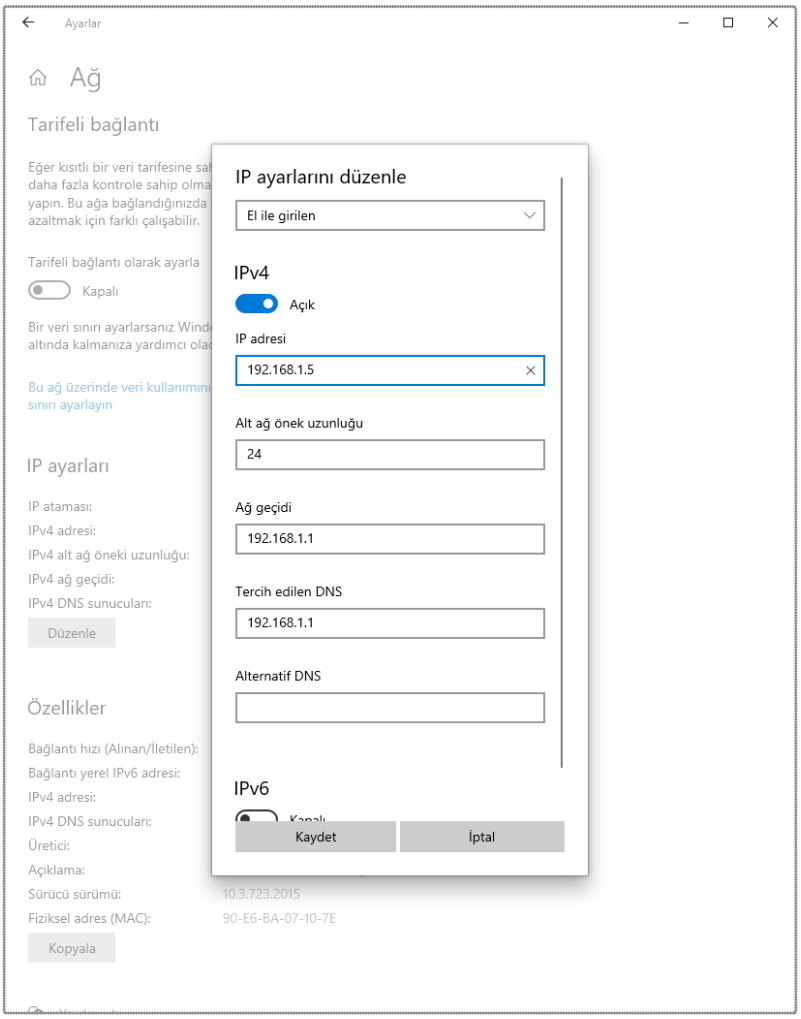
Adım 7: IP adresi olarak 192.168.1.5 (Ağ geçidinize göre belirleyiniz.) değerini giriniz.

Adım 8: Alt ağ öneki uzunluğu olarak 24 giriniz (alt ağ maskesi 255.255.255.0).

Adım 9: Ağ geçidi olarak 192.168.1.1 (ağ geçidi) adresini giriniz.

Adım 10: DNS adresi olarak ağ geçidinizin adresini giriniz ve kaydet butonunu tıklayınız (Görsel 4.10).

Adım 11: Komut istemciyi çalıştırınız ve **ipconfig /all** komutuyla ayarlarınızı kontrol ediniz.



Görsel 4.10: El ile IP adresi atama

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

1. ( ) Özel IP adresi kullanan bilgisayar internete çıkmak için NAT tablosundaki IP adreslerinden birisiyle eşleşir.
2. ( ) Ipv6 128 bitlik adresleme yapılabilir.
3. ( ) Ağdaki bilgisayarlara DHCP ile IP adresi ataması yapılırsa IP adres çakışması olur.
4. ( ) IPv6 başlık yapısında kaynak IP adresi bulunmaz.
5. ( ) DHCP servisi ağdaki tüm cihazlara otomatik IP adresi atar.

B. Aşağıdaki soruları dikkatlice okuyunuz ve doğru seçeneği işaretleyiniz.

6. Aşağıdakilerden hangisi alt ağ maskesinin görevidir?

A) Ağ cihazları arasında veri iletimini sağlar.
B) Ağ cihazlarına IP adresi ataması yapar.
C) D ve E sınıfı IP adresler için tasarlanmıştır.
D) İnternete paket göndermek için kullanılır.
E) Bilgisayarların ağ tanımlayıcılarını bulmayı sağlar.

7. Ipv4 protokolündeki adresler kaç bittir?

A) 16 B) 32 C) 64 D) 128 E) 256

8. I. Kaynak IP Adresi
II. Hedef IP Adresi
III. Kaynak MAC Adresi
IV. Yaşam Süresi

IPv4 başlık yapısında aşağıdakilerden hangileri bulunur?

A) I-II B) I-III-IV C) I-II-IV D) I-II-III E) II-III-IV

9. Aşağıdakilerden hangisi IPv4 adresi <u>değildir?</u>

A) 192.168.0.1
B) 10.0.5.2
C) 172.16.25.254
D) 127.0.0.1
E) 192.168.255.3

10. Aşağıdaki IPv6 adreslerinden hangisi <u>yanlıştır?</u>

A) 2001:1:2020::1
B) 2001:BDE0::38:255
C) 2001:ABCD::DE::5
D) 2001:2045:48:1:2:1:78:81
E) 2001:FFE0:A:B:C:D:E:F

11. Aşağıdaki IPv6 adreslerinden hangisi loopback adresidir?

A) ::
B) ::0
C) ::1
D) ::127
E) 192::1

12. A sınıfı IP adreslerinde kullanıcı kısmı kaç oktetten oluşur?

A) 0
B) 1
C) 2
D) 3
E) 4

13. Genel yayın adresi olarak aşağıdakilerden hangisi kullanılır?

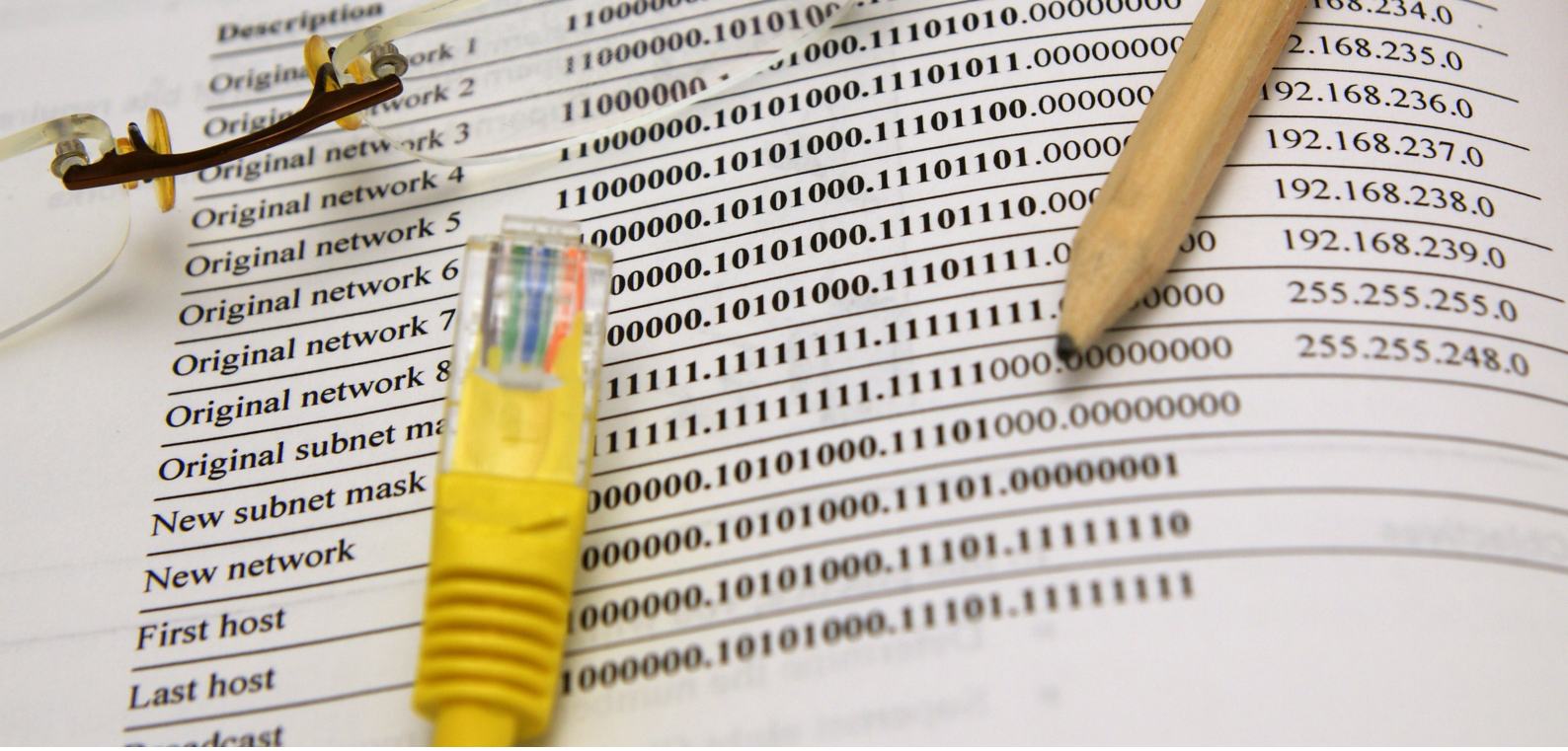
A) 0.0.0.0
B) 111.111.111.111
C) 128.128.128.128
D) 192.168.1.1
E) 255.255.255.255

14. 10.11.9.5/26 ip adresinin alt ağ maskesi değeri aşağıdakilerden hangisidir?

A) 255.255.255.0
B) 255.255.255.128
C) 255.255.255.192
D) 255.255.255.224
E) 255.255.255.240

15. Bilgisayara atanmış IP adresi bilgilerini öğrenmek için hangi komut kullanılır?

A) ping
B) iping
C) config
D) ipconfig
E) iconfig



ÖĞRENME BİRİMİ 5

ALT AĞLAR

NELER ÖĞRENECEKSİNİZ?

Bu öğrenme birimi ile;

- Alt ağ kavramını açıklayacak,
- Alt ağ oluşturma işlemlerini yapacak,
- Alt ağ maskesini hesaplayacak,
- Değişken uzunluklu alt ağ maskesini öğrenecek,
- Ağ kontrol komutlarını kullanabileceksiniz.

ANAHTAR KELİMELER

IPv4, IPv4 adres sınıfları, A sınıfı IP adresi, B sınıfı IP adresi, C sınıfı IP adresi, D sınıfı IP adresi, E sınıfı IP adresi, alt ağ maskesi, CIDR, Subnet, ping, ıpconfig, tracert, nbstat, netstat, ARP, nslookup

Hazırlık Çalışmaları

1. Bir öğretmen, okulunuzun tüm öğrencilerini tek bir sınıfa toplayıp ders yapmak isteseydi nasıl bir ortam oluşurdu? Fikirlerinizi arkadaşlarınızla paylaşınız.
2. Sınıfınıza yeni gelen arkadaşınızla aynı sokakta oturduğunuzu nasıl öğrenirsiniz?

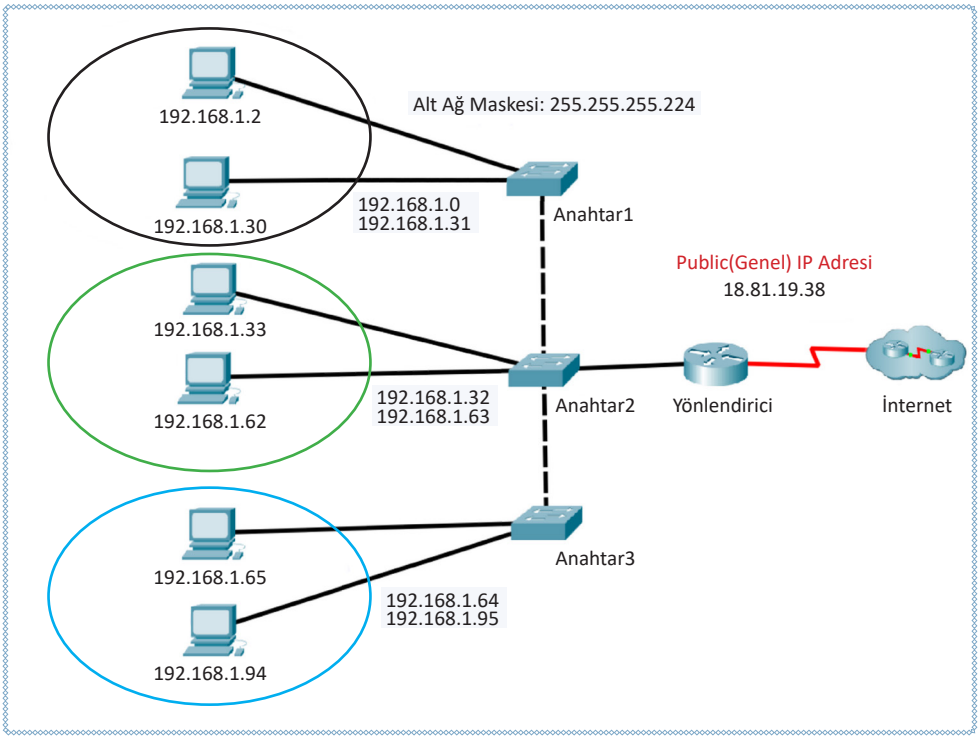
5.1. Alt Ağ Maskesi Hesaplama İşlemleri

Ağ yapısı genişledikçe genel yayın etki alanı da büyüyecek ve ağdaki tüm cihazlar, yoğun bir genel yayın etki alanı trafiğine maruz kalacaktır. Bu durum ağ performansını olumsuz yönde etkileyecektir. Ağın yönetimi de zorlaşacaktır.

5.1.1. Alt Ağ

Ağ tasarımında, IP adresleri cihazlara verilirken ağı daha küçük birimlere ayırarak alt ağlar (subnets) oluşturulur. Böylece hem birbirinden bağımsız hem de yönetimi daha kolay bir ağ yapısı elde edilir.

Örneğin bir meslek lisesi, B sınıfı bir IP adresi aldığında bunu okulda bulunan alanlara bölerek alanlar bazında yerel alt ağlar oluşturup cihazlara atamasını yapabilir. Böylece internetin hiyerarşik yapısı korunarak adresler yapılandırılabilir. Bu sayede ağ trafiği bölünerek daha verimli ve yönetimi kolay bir ağ yapısı elde edilir. Herhangi bir cihazın adresine bakılarak hangi alt ağda olduğu rahatlıkla tespit edilebilir (Görsel 5.1). Bu yapı, yerleşim yeri adreslerine benzer. Adresin önce illere sonra ilçelere ardından mahalle, cadde ve sokaklara ayrılması gibidir.



Görsel 5.1: Alt ağ yapılandırma

Alt ağ oluşturma işlemi hem birbiri ile hem de ilgili olan birimlerin kendi aralarında haberleşmeleri sırasında hızdan kazanç sağlayacaktır. Diğer ağ birimleri ile iletişime geçileceği sırada yönlendirme işlemi daha çabuk gerçekleşecektir.

Bütün bir ağ;

- Ağ trafiğini azaltmak böylece ağdan daha verimli bir şekilde yararlanmak,
- Aynı ağ üzerinde kullanılamayan topoloji ve teknolojilerin kullanımını sağlamak,
- Daha kolay yönetim ve denetleme sağlamak gibi nedenlerle bölünerek alt ağlara ayrılır.

Bir ağ, alt ağlara bölündüğünde ne olur?

- Alt ağlara bölme işlemi adres esnekliği sağlar.
- Ağı alt ağlara bölme işlemi yayın etki alanı (broadcast domain) büyüklüğünü azaltır.
- Alt ağ adresleri ağ yöneticisi tarafından yerel olarak tahsis edilir.

Alt ağ kavramı aslında **cihaz kimliği** (Host ID) alanındaki bazı bitlerin **ağ kimliği** (Network ID) olarak kullanılmasıdır. Böylece eldeki adrese tanımlanabilecek bilgisayar sayısı düşürülerek tanımlanabilecek ağ sayısını yükseltmek mümkün olmaktadır.

5.1.2. Alt Ağ Oluşturma

IPv4 adresinin bir bölümü ağı, bir bölümü de cihazın ağdaki numarasını göstermektedir. Bu bölümler **ön ek / ağ kimliği (Prefix/Network ID)** ve **son ek / cihaz kimliği (Suffix/Host ID)** olarak adlandırılır. Aynı ağ üzerinde bulunan tüm bilgisayarların ağ kimlikleri (N/Network ID) aynıdır. Aynı ağ içinde yer alan bilgisayarların ayırt edilmesini IP adresi üzerindeki yer alan cihaz kimliği (h/Host ID) bölümü sağlar. A sınıfı ağları tanımlamak için ilk 8 bit (ilk oktet), B sınıfı bilgisayar ağlarını tanımlamak için ilk 16 bit (ilk iki oktet), C sınıfı ağları tanımlamak için ise ilk 24 bit (ilk üç oktet) kullanılır (Tablo 5.1).

Tablo 5.1: IP Adres Sınıflarına Göre Varsayılan Alt Ağ Maskeleri

IPv4 Sınıf	Varsayılan Alt Ağ Maskesi					
		1. Oktet	2. Oktet	3. Oktet	4. Oktet	
A Sınıfı	Onluk (Decimal)	255	0	0	0	8 Bit
	İkilik (Binary)	11111111	00000000	00000000	00000000	
	Türü	NNNNNNNN	hhhhhhhh	hhhhhhhh	hhhhhhhh	
B Sınıfı	Onluk (Decimal)	255	255	0	0	16 Bit
	İkilik (Binary)	11111111	11111111	00000000	00000000	
	Türü	NNNNNNNN	NNNNNNNN	hhhhhhhh	hhhhhhhh	
C Sınıfı	Onluk (Decimal)	255	255	255	0	24 Bit
	İkilik (Binary)	11111111	11111111	11111111	00000000	
	Türü	NNNNNNNN	NNNNNNNN	NNNNNNNN	hhhhhhhh	

Varsayılan alt ağ maskesi dikkatlice incelendiğinde ağ adresinin bulunduğu oktetlerdeki bitlerin "1", cihaz adresinin bulunduğu oktetlerdeki bitlerin "0" olduğu görülür. Örneğin 195.175.1.0 IP adresi, C sınıfı bir ağı tanımlar. Bu IP adresi tanımında ilk 24 bit ağı tanımlarken ağdaki cihazları tanımlamak için son 8 bit kullanılır. Bu durumda 2^8=256 adet adres atanabilir. Bir IP adresi ağı tanımlamak için, bir tanesi de genel yayın için kullanılır. Böylece ağdaki cihazlara atanabilecek IP adresi sayısı 256-2=254 adettir.

Dikkat

Bir ağda adreslenebilecek cihaz sayısı 2^n-2 formülüyle bulunur (***n*** cihaz kimliği bitleri sayısı).

Alt ağ oluşturmak için IP adreslerinin ayrıldığı cihaz kimliği (Host ID) bölümünün başındaki (solundaki) bitler ödünç alınarak ağ kimliğine (Network ID) eklenir (Tablo 5.2).

Tablo 5.2: IP Adresi Bölümleri

Ağ Kimliği (Network ID)	Cihaz Kimliği (Host ID)	
	Alt Ağ Numarası (Ödünç Bitler)	Cihaz Numarası

Her bit 2^n adet alt ağ oluşturmaya imkân tanır. Bit sayısı arttıkça oluşturulabilecek alt ağ sayısı 2'nin kuvvetleri şeklinde artacaktır. Örneğin bir IP adresinde, 1 bit ödünç alındığında 2 alt ağ, 3 bit ödünç alındığında 8 alt ağ oluşturulabilmektedir.

Dikkat

Alt ağ oluşturma işlemi 2'nin kuvvetleri şeklinde arttığı için 3 adet alt ağa ihtiyaç varsa 4 tane, 12 adet alt ağa ihtiyaç varsa 16 tane alt ağ oluşturulur.

Uygulama 1

"145.134.0.0" B sınıfı bir IP adresinde 8 adet alt ağ oluşturmak için gerekli işlemleri aşağıdaki yönergeler doğrultusunda gerçekleştiriniz.

Adım 1: IP adresini onluk ve ikilik gösterimini oktetlerine ayırarak yazınız (Tablo 5.3).

Tablo 5.3: IP Adresinin Onluk ve İkilik Düzende Gösterimi

Ağ Adresi Gösterimi	**Ağ Kimliği (Network ID)**		**Cihaz Kimliği (Host ID)**	
	1. Oktet	**2. Oktet**	**3. Oktet**	**4. Oktet**
Onluk	145	143	0	0
İkilik	10010001	10001111	00000000	00000000

Adım 2: 8 adet alt ağ oluşturmak için 2^n=8 formülüne göre cihaz kimliğinden 3 bit ödünç alarak alt ağ adreslerini hesaplayınız (Tablo 5.4).

Tablo 5.4: Alt Ağ IP Adresleri

Alt Ağlar	**İkilik Gösterim**					**Onluk Gösterim**
	1. Oktet	**2. Oktet**	**3. Oktet**		**4. Oktet**	
	Ağ Kimliği (Network ID)		**Alt Ağ biti**	**Cihaz Kimliği (Host ID)**		
1. Alt Ağ Adresi	10010001	10001111	000	00000	00000000	145.143.0.0
2. Alt Ağ Adresi	10010001	10001111	001	00000	00000000	145.143.32.0
3. Alt Ağ Adresi	10010001	10001111	010	00000	00000000	145.143.64.0
4. Alt Ağ Adresi	10010001	10001111	011	00000	00000000	145.143.96.0
5. Alt Ağ Adresi	10010001	10001111	100	00000	00000000	145.143.128.0
6. Alt Ağ Adresi	10010001	10001111	101	00000	00000000	145.143.160.0
7. Alt Ağ Adresi	10010001	10001111	110	00000	00000000	145.143.192.0
8. Alt Ağ Adresi	10010001	10001111	111	00000	00000000	145.143.224.0

Adım 3: Her bir alt ağda cihaz adreslemek için 13 bit kullanılabilir olduğuna göre 2^{13}-2=8190 tane cihaza IP adresi verilebildiğini unutmayınız.

Sıra Sizde

C sınıfı bir IP adresinde 2 bit ödünç alarak dört adet alt ağ oluşturunuz.

5.1.3. Alt Ağ Maskesi Hesaplama

IP adresinin bir bölümü ağ kimliğini bir bölümü de cihaz kimliğini oluşturur. Bu iki bölümün hangi bitten ayrılacağını bulmak için ağ maskesi (Subnet Mask) kullanılmaktadır. IP adresiyle alt ağ maskesi "mantıksal **VE**" işlemine tabi tutularak cihazın hangi ağda olduğu tespit edilir.

Alt ağ maskesinin "1" olan bitleri ağ kimliğini, "0" olan bitleri cihaz kimliğini temsil eder. Alt ağ oluşturmak için ödünç verilen bitler için alt ağ maskesinin cihaz kimliği bitleri 0'dan 1'e çevrilir.

Alt ağ maskesinde "1" olan bitler, mantıksal VE işlemine göre ağ adresinde değişikliğe sebep olmaz. Alt ağ maskesinde "0" olan bitler ile IP adresi, mantıksal VE işlemine tabi tutulduğunda adresler değişecek ve bölünen ağlardaki IP adreslerini verecektir.

Uygulama 2

"192.168.1.0" C sınıfı bir IP adresinde 2 adet alt ağ oluşturarak alt ağ maskesini hesaplamak için gereken işlemleri aşağıdaki yönergeler doğrultusunda gerçekleştiriniz.

Adım 1: IP adresini ve varsayılan alt ağ maskesini onluk ve ikilik gösterimini alt alta yazınız (Tablo 5.5).

Tablo 5.5: IP Adresi, Varsayılan Alt Ağ Maskesi Gösterimi

		Ağ Kimliği Bitleri			Cihaz Kimliği Bitleri
IP adresi	192.168.1.0	11000000	10101000	00000001	00000000
Alt Ağ Maskesi	255.255.255.0	**11111111**	**11111111**	**11111111**	***00000000***

Adım 2: İki adet alt ağ oluşturmak için cihaz kimliği bitlerinden 1 bit ödünç alarak yeni alt ağ maskesini oluşturunuz (Tablo 5.6).

Tablo 5.6: Alt Ağ Maskesi Ödünç Bit Alma ve Yeni Alt Ağ Maskesi

		Ağ Kimliği Bitleri			*Alt Ağ İçin Ödünç Bit*	Cihaz Kimliği Bitleri
Alt Ağ Maskesi	255.255.255.128	**11111111**	**11111111**	**11111111**	***1***	***0000000***

Adım 3: Oluşturduğunuz alt ağ maskesini kullanarak alt ağları ve ağ adreslerini hesaplayınız (Tablo 5.7).

Tablo 5.7: Oluşturulan Alt Ağlar

			Ağ Kimliği			Alt Ağ Ödünç Bit	*Cihaz Kimliği*
Alt Ağ 1	IP adresi	192.168.1.0	11000000	10101000	00000001	**0**	*0000000*
	Alt Ağ Maskesi	255.255.255.128	**11111111**	**11111111**	**11111111**	***1***	*0000000*
	Mantıksal VE İşlemi						
	Ağ Adresi	192.168.1.0	11000000	10101000	00000001	**0**	*0000000*
Alt Ağ 2	IP adresi	192.168.1.128	11000000	10101000	00000001	**1**	*0000000*
	Alt Ağ Maskesi	255.255.255.128	**11111111**	**11111111**	**11111111**	***1***	*0000000*
	Mantıksal VE İşlemi						
	Ağ Adresi	192.168.1.128	11000000	10101000	00000001	***1***	*0000000*

Adım 4: Oluşturduğunuz alt ağlarda kullanılabilecek başlangıç ve bitiş IP adreslerini hesaplayınız (Tablo 5.8).

Tablo 5.8: Alt Ağlarda Kullanılabilecek Başlangıç ve Bitiş IP Adresleri

			Ağ Kimliği			Alt Ağ Ödünç Bit	*Cihaz Kimliği*
Alt Ağ 1	IP Adresi Başlangıç	192.168.1.0	11000000	10101000	00000001	**0**	*0000000*
	IP Adresi Bitiş	192.168.1.127	11000000	10101000	00000001	**0**	*1111111*
	Alt Ağ Maskesi	255.255.255.128	**11111111**	**11111111**	**11111111**	***1***	***0000000***
	Ağ Adresi	192.168.1.0	11000000	10101000	00000001	**0**	*0000000*
Alt Ağ 2	IP adresi Başlangıç	192.168.1.128	11000000	10101000	00000001	**1**	*0000000*
	IP adresi Bitiş	192.168.1.255	11000000	10101000	00000001	**1**	*1111111*
	Alt Ağ Maskesi	255.255.255.128	**11111111**	**11111111**	**11111111**	***1***	***0000000***
	Ağ Adresi	192.168.1.128	11000000	10101000	00000001	**1**	*0000000*

Dikkat

Oluşturulan alt ağların **başlangıç IP adresi ağ adresini** (Network Address), **bitiş IP adresi** ise alt ağ **genel yayın** (Broadcast) **adresini** verir.

Sıra Sizde

C sınıfı bir IP adresinden 2 bit ödünç alarak dört adet alt ağ oluşturup bu alt ağlarda kullanılacak alt ağ maskesini ve ağ adresini hesaplayınız.

5.1.4. Değişken Uzunluklu Alt Ağ Maskesi [VLSM (Variable Lenght Subnet Mask)]

Alt ağ oluşturma işlemi yapılırken her bir alt ağdaki cihaz sayısı aynı olur. Alt ağlarda kullanılan cihaz (host) sayısı genellikle eşit olmaz. Örneğin birinci alt ağda 110 cihaz, ikinci alt ağda 50 cihaz bulunan bir ağ tasarımında C sınıfı bir IP adresinden 2 alt ağ oluşturularak sorun çözülür. Oluşturulan her bir alt ağa 126 adet cihaz bağlanabilir. Birinci alt ağda 16, ikinci alt ağda 76 tane olmak üzere 92 tane IP adresi kullanılmayacaktır. 30 cihazı bulunan bir üçüncü alt ağ eklemek istendiğinde mecburen yeni bir C sınıfı IP adresi tahsis edilmesi gerekir.

IP adreslerinin daha verimli kullanılması amacıyla alt ağlara bölerken **değişken uzunlukta alt ağ maskesi** [**VLSM** (Variable Lenght Subnet Mask)] geliştirilmiştir. VLSM kullanırken alt ağ maskesi, oluşturulan bazı alt ağlar için kaç adet cihaz kimliği (host) biti ödünç alındığına bağlı olarak değişecektir. VLSM kullanılırken ağ, ilk önce alt ağlara bölünür, ardından oluşturulan alt ağlar, tekrar alt ağa bölünür. Bu işlem, çeşitli boyutlarda alt ağlar oluşturmak için birden fazla tekrarlanabilir. Böylece IP adresleri boşa harcanmadan adreslenebilir.

Değişken uzunlukta alt ağ maskesi kullanımında CIDR gösterimi kullanılır. CIDR gösteriminde IP adresinden sonra "**/**" ile baştan kaç bitin ağ kimliğini temsil ettiği belirtilir. 172.16.0.0/18 gösteriminde baştan 18 bit alt ağ maskesinde "1" değerindedir.

Bir önceki örneğimiz değişken uzunlukta alt ağ maskesi ile tekrar alt ağlara bölünürse birinci alt ağ 126, ikinci alt ağ 62, üçüncü alt ağ ise 30 IP adresi ayrılır. İleride kullanılmak üzere 30 adet IP adresi kalır (Tablo 5.9).

Tablo 5.9: Değişken ve Sabit Uzunluklu Alt Ağ Maskesi Kullanılarak Oluşturulan Ağ Yapısı

	IP adresi Alt Ağ Maskesi	Kullanacak Cihaz Sayısı	Kullanılabilecek Cihaz IP Adresi Sayısı	Artan IP Adresi Sayısı
Sabit Uzunluklu Alt Ağ Maskesi	192.168.1.0/25 255.255.255.128	100	126	26
	192.168.1.0/25 255.255.255.128	50	126	76
	192.168.2.0/24 255.255.255.0	30	254	224
Değişken Uzunluklu Alt Ağ Maskesi	192.168.1.0/25 255.255.255.128	100	126	16
	192.168.1.0/26 255.255.255.192	50	62	12
	192.168.1.0/27 255.255.255.224	30	30	0

5.1.5. Ağın Gereklerine Göre Alt Ağ Oluşturma

Alt ağlara ayırma işlemi, **ihtiyaç duyulan alt ağ sayısı ve ihtiyaç duyulan kullanıcı sayısı** olmak üzere iki farklı duruma göre belirlenebilir.

Uygulama 3

Tek bir binada hizmet veren bir iş yerinin bünyesinde 130 adet (bilgisayar, tablet benzeri) cihaz bulunmaktadır. Bu cihazlara ek, 5 tanesi ağda kullanılacak yazıcı ve tarayıcı gibi ortak cihaz bulunmaktadır. Bu iş yeri sonraki yıl 30 adet yeni cihaz almayı planlamaktadır. Bu iş yerinin ağ yapılandırmasını oluşturmak için gereken işlemleri aşağıdaki yönergeler doğrultusunda gerçekleştiriniz.

Adım 1: İş yerinde, eklenecek cihazlarla birlikte toplam 130+5+30=165 adet cihaz olacağına dikkat ediniz.

Adım 2: C sınıfı bir IP adresi 254 adet cihazı adresleyebildiği için yeterli olacağını göz önünde bulundurunuz.

Adım 3: Alt ağlara ayırma ihtiyacı bulunmadığını fark ediniz.

Adım 4: C sınıfı bir IP adresine göre ağ yapılandırması Tablo 5.10'daki gibi olmalıdır. Tabloyu inceleyiniz.

Tablo 5.10: C Sınıfı Tek Bir Ağdan Oluşan IP Adresi Yapısı

Ağ Adresi (Network Address)	192.168.1.0
Alt Ağ Maskesi (Subnet Mask)	255.255.255.0
Kullanılabilecek IP Adres Aralığı	192.168.1.1 – 192.168.1.254
Yayın Adresi (Broadcast)	192.168.1.255

Uygulama 4

http://kitap.eba.gov.tr/KodSor.php?KOD=21035

Dört farklı birimden oluşan bir firmada her birimde ellişer adet cihaz bulunmaktadır. Bu firmanın ağ yapılandırmasını oluşturmak için gerekli işlemleri aşağıdaki yönergeler doğrultusunda gerçekleştiriniz.

Adım 1: Firmada kullanılan toplam cihaz sayısının 50X4=200 adet olacağına dikkat ediniz.

Adım 2: C sınıfı bir IP adresinin yeterli (192.168.5.0) olacağını göz önünde bulundurunuz.

Adım 3: Firma dört ayrı birimden oluştuğu için dört tane alt ağ oluşturmanın ağın yönetimini kolaylaştıracağını unutmayınız.

Adım 4: C sınıfı bir IP adresine göre ağ yapılandırması Tablo 5.11'deki gibi olmalıdır. Tabloyu inceleyiniz.

Tablo 5.11: C Sınıfı 4 Adet Alt Ağdan Oluşan IP Adresi Yapısı

1. Alt Ağ	Ağ Adresi	11000000.10101000.00000101.00000000	192.168.5.0
	Alt Ağ Maskesi	11111111. 11111111. 11111111.11000000	255.255.255.192
	Kullanılabilecek IP Adres Aralığı	11000000.10101000.00000101.00000001 11000000.10101000.00000101.00111110	192.168.5.1 – 192.168.5.62
	Yayın Adresi	11000000.10101000.00000101.00111111	192.168.5.63

2. Alt Ağ	Ağ Adresi	11000000.10101000.00000101. 01000000	192.168.5.64
	Alt Ağ Maskesi	11111111. 11111111. 11111111.11000000	255.255.255.192
	Cihazlara Verilebilecek IP Adresi	11000000.10101000.00000101.01000001 11000000.10101000.00000101.01111110	192.168.5.65 – 192.168.5.126
	Yayın Adresi	11000000.10101000.00000101.01111111	192.168.5.127
3. Alt Ağ	Ağ Adresi	11000000.10101000.00000101.10000000	192.168.5.128
	Alt Ağ Maskesi	11111111. 11111111. 11111111.11000000	255.255.255.192
	Kullanılabilecek IP Adres Aralığı	11000000.10101000.00000101.10000001 11000000.10101000.00000101.10111110	192.168.5.129 – 192.168.5.190
	Yayın Adresi	11000000.10101000.00000101.10111111	192.168.5.191
4. Alt Ağ	Ağ Adresi	11000000.10101000.00000101.11000000	192.168.5.192
	Alt Ağ Maskesi	11111111. 11111111. 11111111.11000000	255.255.255.192
	Cihazlara Verilebilecek IP Adresi	11000000.10101000.00000101.11000001 11000000.10101000.00000101.11111110	192.168.5.193 – 192.168.5.254
	Yayın Adresi	11000000.10101000.00000101.11111111	192.168.5.255

Uygulama 5

Her bölgede iki milyona yakın kullanıcı bulunan sekiz farklı bölgede hizmet vermeyi planlamakta olan bir ISP (internet servis sağlayıcı) IP adresi tahsisi için başvuru yapmıştır. ISP tarafından 14.0.0.0 IP adresi verilmiştir. Buna göre ISP'nin ağ yapılandırmasını oluşturmak için işlemleri yönergeler doğrultusunda gerçekleştiriniz.

Adım 1: ISP'ye tahsis edilen 14.0.0.0 adresinin A sınıfı bir adres olduğuna dikkat ediniz.

Adım 2: ISP, 8 bölgede hizmet vereceği için 8 adet alt ağ oluşturulması gerektiğini unutmayınız.

Adım 3: 8 adet alt ağ için 3 bit ödünç alınması gerektiğine dikkat ediniz.

Dikkat

3 bit ödünç alındığı zaman cihaz adreslemek için 21 bit kalır. 2^n-2 formülüne göre her bir alt ağda, 2.097.150 adet cihaza IP adresi verilebilir. Bu sayı, bölgelerde kullanıcı sayısından fazla olduğu için yeterlidir.

Adım 4: A sınıfı bir IP adresine göre ağ yapılandırması Tablo 5.12'deki gibi olmalıdır. Tabloyu inceleyiniz.

Tablo 5.12: A Sınıfı 8 Adet Alt Ağdan Oluşan IP Adresi Yapısı

1. Alt Ağ	Ağ Adresi	00001110.00000000.00000000.00000000	14.0.0.0
	Alt Ağ Maskesi	11111111.11100000.00000000.00000000	255.224.0.0
	Kullanılabilecek IP Adres Aralığı	00001110. 00000000.00000000.00000001 00001110.00011111.11111111.11111110	14.0.0.1 – 14.31.255.254
	Yayın Adresi	00001110.00011111.11111111.11111111	14.31.255.255

2. Alt Ağ	Ağ Adresi	00001110.00100000.00000000.00000000	14.32.0.0
	Alt Ağ Maskesi	11111111.11100000.00000000.00000000	255.224.0.0
	Kullanılabilecek IP Adres Aralığı	00001110.00100000.00000000.00000001 00001110.00111111.11111111.11111110	14.32.0.1 – 14.63.255.254
	Yayın Adresi	00001110.00111111.11111111.11111111	14.63.255.255
3. Alt Ağ	Ağ Adresi	00001110.01000000.00000000.00000000	14.64.0.0
	Alt Ağ Maskesi	11111111.11100000.00000000.00000000	255.224.0.0
	Kullanılabilecek IP Adres Aralığı	00001110.01000000.00000000.00000001 00001110.01011111.11111111.11111110	14.64.0.1 – 14.95.255.254
	Yayın Adresi	00001110.01011111.11111111.11111111	14.95.255.255
4. Alt Ağ	Ağ Adresi	00001110.01100000.00000000.00000000	14.96.0.0
	Alt Ağ Maskesi	11111111.11100000.00000000.00000000	255.224.0.0
	Kullanılabilecek IP Adres Aralığı	00001110.01100000.00000000.00000001 00001110.01111111.11111111.11111110	14.96.0.1 – 14.127.255.254
	Yayın Adresi	00001110.01111111.11111111.11111111	14.127.255.255
5. Alt Ağ	Ağ Adresi	00001110.10000000.00000000.00000000	14.128.0.0
	Alt Ağ Maskesi	11111111.11100000.00000000.00000000	255.224.0.0
	Kullanılabilecek IP Adres Aralığı	00001110.10000000.00000000.00000001 00001110.10011111.11111111.11111110	14.128.0.1 – 14.159.255.254
	Yayın Adresi	00001110.10011111.11111111.11111111	14.159.255.255
6. Alt Ağ	Ağ Adresi	00001110.10100000.00000000.00000000	14.160.0.0
	Alt Ağ Maskesi	11111111.11100000.00000000.00000000	255.224.0.0
	Kullanılabilecek IP Adres Aralığı	00001110.10100000.00000000.00000001 00001110.10111111.11111111.11111110	14.160.0.1 – 14.191.255.254
	Yayın Adresi	00001110.10111111.11111111.11111111	14.191.255.255
7. Alt Ağ	Ağ Adresi	00001110.11000000.00000000.00000000	14.192.0.0
	Alt Ağ Maskesi	11111111.11100000.00000000.00000000	255.224.0.0
	Kullanılabilecek IP Adres Aralığı	00001110.11000000.00000000.00000001 00001110.11011111.11111111.11111110	14.192.0.1 – 14.223.255.254
	Yayın Adresi	00001110.11011111.11111111.11111111	14.223.255.255
8. Alt Ağ	Ağ Adresi	00001110.11100000.00000000.00000000	14.224.0.0
	Alt Ağ Maskesi	11111111.11100000.00000000.00000000	255.224.0.0
	Kullanılabilecek IP Adres Aralığı	00001110.11100000.00000000.00000001 00001110.11111111.11111111.11111110	14.224.0.1 – 14.255.255.254
	Yayın Adresi	00001110.11111111.11111111.11111111	14.255.255.255

Uygulama 6

http://kitap.eba.gov.tr/KodSor.php?KOD=21036

24 cihazlık bilgi işlem, 28 cihazlık muhasebe, 52 cihazlık pazarlama, 60 cihazlık üretim ve 12 cihazlık depolama birimlerinden oluşan bir firma, ISP'den kullanmak üzere IP adresi talebinde bulunmuştur. Ağ yapılandırmasını oluşturmak için işlemleri aşağıdaki yönergeler doğrultusunda gerçekleştiriniz.

Adım 1: Firma bünyesinde toplam 176 adet cihaz olduğunu ISP'den C sınıfı bir adres istenmesi gerektiğini fark ediniz.

Dikkat

ISP C sınıfı 195.175.39.0 adresini tahsis etmiştir.

Adım 2: Firma bünyesinde 5 birim bulunduğu için 8 alt ağ oluşturmak gerekir. Bu durumda her bir alt ağ için 30 adet kullanılabilir IP adresi kalır. Fakat bazı birimlerde 30'dan fazla cihaz bulunduğu için bu durumda oluşturulan sabit uzunluklu alt ağların yetersiz kaldığını gözlemleyiniz.

Adım 3: Değişken uzunluklu alt ağ maskesi ile 5 tane alt ağ oluşturulabilir. Her bir alt ağ kullanılacak cihaz sayısına göre tanımlanır. Cihaz sayısı fazla olan alt ağlardan bölümlenmeye başlanır (Tablo 5.13). Tabloyu inceleyiniz.

Tablo 5.13: C Sınıfı 5 Adet Değişken Uzunluklu Alt Ağdan Oluşan IP Adresi Yapısı

	Cihaz Sayısı	Maske Değeri	Alt Ağ Maskesi	Ağ Adresi	Kullanılabilecek IP Adres Aralığı	Yayın Adresi
Üretim	60	/26	255.255.255.192	195.175.39.0	195.175.39.1-195.175.39.62	195.175.39.63
Pazarlama	52	/26	255.255.255.192	195.175.39.64	195.175.39.65-195.175.39.126	195.175.39.127
Muhasebe	28	/27	255.255.255.224	195.175.39.128	195.175.39.129-195.175.39.158	195.175.39.159
Bilgi İşlem	24	/27	255.255.255.224	195.175.39.160	195.175.39.161-195.175.39.190	195.175.39.191
Depolama	12	/28	255.255.255.240	195.175.39.192	195.175.39.193-195.175.39.206	195.175.39.207

Sıra Sizde

1. Okulunuzda bulunan alanlardaki cihaz sayısına göre ağ yapılandırmasını oluşturunuz.
2. 29.10.19.23/28 IP adresi için aşağıdaki verileri hesaplayınız.
   a) Alt ağ maskesi (Subnet Mask) nedir?
   b) Ağ adresi nedir?
   c) Her bir alt ağa kaç bilgisayar bağlanır?
   d) Broadcast (Yayın) adresi nedir?
   e) Ağa toplam kaç adet bilgisayar bağlanır?

5.2. Komutlarla Alt Ağların Kontrol Edilmesi

Bir ağın tasarımı, uygulanması, çalışması esnasında bazı hatalar ve sorunlar oluşabilir. Bu hatalar veya sorunlar, hızlı ve doğru bir şekilde çözülerek ağ en kısa sürede tekrar çalışır hâle getirilmelidir. Ağda karşılaşılan durumları incelemek ve varsa sorunları çözmek için çeşitli komutlar bulunmaktadır. Bu komutlar bazı ayarları yapma, çeşitli verileri toplama ve durum bildirimlerini inceleme imkânı sağlar.

5.2.1. Ağ Kontrol Komutları

Ağ test komutları, bilgisayarın komut istemcisinde (**command promt**) çalışmaktadır. Bu komutların görsel kullanımını sağlamak amacıyla çeşitli programlar da bulunmaktadır. Ağ testi için sıkça kullanılan komutlar Tablo 5.14'te verilmiştir. Bu komutlar birçok parametreyle çalışmaktadır. Komutların çalıştığı parametreleri görmek için komuttan sonra "**/?**" kullanılır.

Tablo 5.14: Ağ Test Komutları ve İşlevleri

Komut	İşlevi
ipconfig	Bilgisayarın tüm IP ayarlarını görmek için kullanılan komuttur.
ping	İki cihazın birbirleri ile haberleşip haberleşemediğini gösterir.
tracert	Gönderilen paketlerin hedef cihaza giderken geçtiği yönlendiricilerin listesini verir.
nbstat	NETBIOS ad çözümleme sorunlarını gidermek için kullanılır.
netstat	Bilgisayarın ağ durumunu ve aktif bağlantılarını gösterir.
arp	IP adresinden MAC adreslerine çevirme işlemindeki listelere bakmak ve değiştirmek için kullanılır.
nslookup	İnternet adreslerinin IP adreslerine çevrilme işindeki problemleri anlamada kullanılır.

Dikkat

Ağ test komutları İngilizce olduğu için komut istemcisine yazımı esnasında Türkçe karakter desteği bulunmamaktadır.

5.2.1.1. ipconfig Komutu

ipconfig komutuyla bilgisayarda bulunan tüm ağ aygıtlarının hakkında detaylı bilgiler görüntülenebilir. Aktif TCP/IP bağlantı ayarlarında değişiklik yapmak için kullanılır. Bu komutla kullanılabilecek parametreler Tablo 5.15'te verilmiştir.

Tablo 5.15: ipconfig Parametreleri

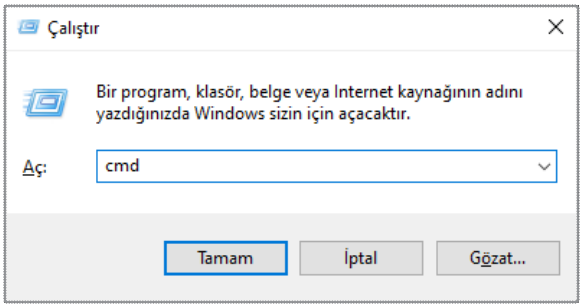
Parametre	İşlevi
/all	Tüm yapılandırma bilgisini görüntülenir.
/release	Belirtilen bağdaştırıcı için IPv4 adresini serbest bırakır.
/release6	Belirtilen bağdaştırıcı için IPv6 adresini serbest bırakır.
/renew	Belirtilen bağdaştırıcı için IPv4 adresini yeniler.
/renew6	Belirtilen bağdaştırıcı için IPv6 adresini yeniler.
/flushdns	DNS çözümleyici önbelleğini temizler.
/registerdns	Tüm DHCP kiralarını yeniler ve DNS adlarını yeniden kaydettirir.

/displaydns	DNS çözümleyici önbelleğinin içeriğini görüntüler.
/showclassid	Bağdaştırıcı için izin verilen tüm IPv4 DHCP sınıf kimliklerini görüntüler.
/setclassid	IPv4 DHCP sınıf kimliğini değiştirir.
/showclassid6	Bağdaştırıcı için izin verilen tüm IPv6 DHCP sınıf kimliklerini görüntüler.
/setclassid6	IPv6 DHCP sınıf kimliğini değiştirir.

Uygulama 7

ipconfig komutuyla bilgisayarınızın ağ yapılandırmasını görüntülemek için işlemleri aşağıdaki yönergeler doğrultusunda gerçekleştiriniz.

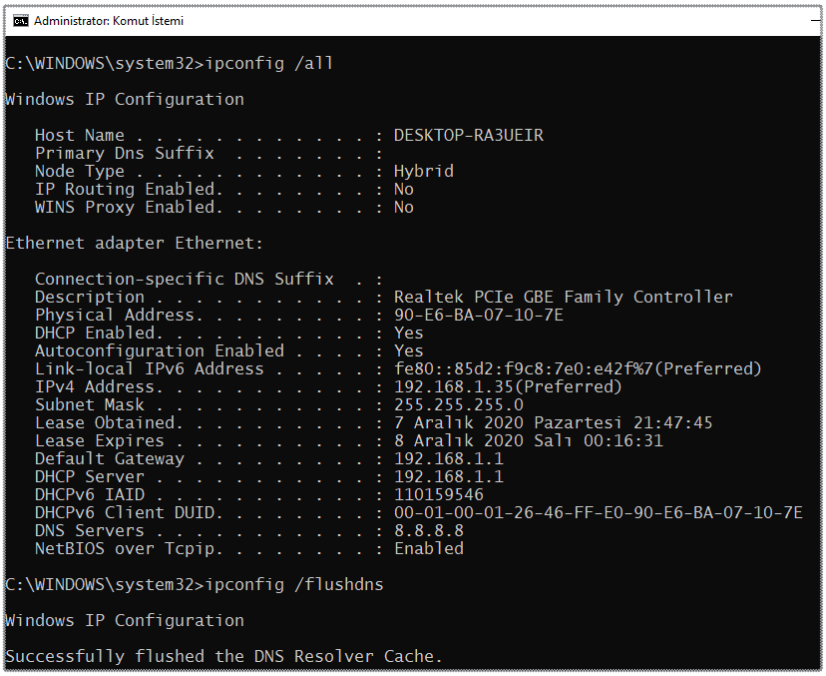
Adım 1: Çalıştır penceresi açınız. Açılan **Çalıştır** penceresine "***cmd***" yazıp "Enter" tuşuna basarak komut istemcisini çalıştırınız (Görsel 5.2).



Görsel 5.2: Komut istemcisinin çalıştırılması

Adım 2: Komut istemcisine ***ipconfig*** yazıp "Enter" tuşuna basınız ve bilgisayarınızın IP yapılandırmasını inceleyiniz.

Adım 3: ***ipconfig /all*** komutuyla tüm yapılandırma bilgilerini görüntüleyiniz (Görsel 5.3).



Görsel 5.3: ipconfig /all komutu

Adım 4: ***ipconfig /release*** komutuyla bilgisayarınızın IP yapılandırmasını serbest bırakınız.

Adım 5: ***ipconfig /renew*** komutuyla bilgisayarınızın DHCP sunucundan yeni IP adresi kiralayınız.

Adım 6: ***ipconfig /displaydns*** komutuyla bilgisayarınızın yerel DNS önbelleğini görüntüleyiniz.

Adım 7: ***ipconfig /flushdns*** komutuyla bilgisayarınızın yerel DNS önbelleğini temizleyip ardından tekrar DNS önbelleğini görüntüleyiniz (Görsel 5.3).

Adım 8: ***ipconfig /registerdns*** komutuyla bilgisayarınızın DHCP kiralarını yenileyiniz ve DNS sunucusuna kaydını yaptırınız.

5.2.1.2. ping Komutu

ping, ağ üzerinden başka bir cihaza gönderilen (echo) ve daha sonra aynı şekilde geri dönen (echo replay) 32 baytlık ICMP [Internet Control Message Protocol (İnternet Denetim İletisi Protokolü)] veri paketidir. Veri paketinin gidip gelmesi arasında geçen süre **milisaniye (ms)** cinsinden ölçülür. Hedef cihaz ne kadar uzaksa bu süre de o kadar artar. Örneğin ülkemizde bulunan bir web sayfasına erişim süresi 40 ms iken Azerbaycan'da bulunan bir web sayfasına erişim 100 ms olabilir. Bu komut ile kullanılabilecek parametreler Tablo 5.16'da verilmiştir.

Tablo 5.16: ping Komutu Parametreleri

Parametre	Açıklama
-t	Durduruncaya kadar ping komutu çalıştırılmaya devam eder. Ctrl+C tuş kombinasyonu kullanılarak bu işlem durdurulur.
-a	IP adresinden alan adının çözülmesini sağlar.
-n count	Gönderilecek paketlerin sayısı belirlenir.
-f	Veri paketlerinin bölünmeden iletilmesini sağlar. IPv4'te çalışır.
-i TTL	Gönderilen paketin yaşam süresini ayarlar. 1 ile 255 arasında bir değer verilebilir (Varsayılan 128 değeridir.).
-w TimeOut	Milisaniye cinsinden, paketlerinin ne kadar bir süre kullanılabilir olduğunu belirler. Değer belirlenmezse otomatik olarak bu değer 4000'e (4000 milisaniye = 4 saniye) ayarlanır.
-l size	Uzunluk ile belirtilen büyüklükte veri içeren ECHO paketleri gönderir. Aksi söylenmediği sürece 64 sekizlidir, en fazla 8192 olabilir.
-4	IPv4 kullanılacağını belirtir.
-6	IPv6 kullanılacağını belirtir.

Dikkat

ping komutu IP adresi verilerek çalışır. Tanımlı bir DNS varsa alan adları kullanılabilir.

Uygulama 8

http://kitap.eba.gov.tr/KodSor.php?KOD=21037

ping komutu ve parametrelerini çalıştırmak için gerekli işlemleri aşağıdaki yönergeler doğrultusunda gerçekleştiriniz.

Adım 1: Bilgisayarınızda komut istemcisini çalıştırınız.

Adım 2: Komut istemciye **ping** yazıp "Enter" tuşuna basınız ve ping komutuyla kullanabileceğiniz parametreleri inceleyiniz (Görsel 5.4).

```
C:\WINDOWS\system32>ping

Usage: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
            [-r count] [-s count] [[-j host-list] | [-k host-list]]
            [-w timeout] [-R] [-S srcaddr] [-c compartment] [-p]
            [-4] [-6] target_name

Options:
    -t             Ping the specified host until stopped.
                   To see statistics and continue - type Control-Break;
                   To stop - type Control-C.
    -a             Resolve addresses to hostnames.
    -n count       Number of echo requests to send.
    -l size        Send buffer size.
    -f             Set Don't Fragment flag in packet (IPv4-only).
    -i TTL         Time To Live.
    -v TOS         Type Of Service (IPv4-only. This setting has been deprecated
                   and has no effect on the type of service field in the IP
                   Header).
    -r count       Record route for count hops (IPv4-only).
    -s count       Timestamp for count hops (IPv4-only).
    -j host-list   Loose source route along host-list (IPv4-only).
    -k host-list   Strict source route along host-list (IPv4-only).
    -w timeout     Timeout in milliseconds to wait for each reply.
    -R             Use routing header to test reverse route also (IPv6-only).
                   Per RFC 5095 the use of this routing header has been
                   deprecated. Some systems may drop echo requests if
                   this header is used.
    -S srcaddr     Source address to use.
    -c compartment Routing compartment identifier.
    -p             Ping a Hyper-V Network Virtualization provider address.
    -4             Force using IPv4.
    -6             Force using IPv6.
```

Görsel 5.4: ping komutu parametreleri

Adım 3: ***ping 192.168.1.2*** komutuyla yerel ağınızdaki bir cihazın paket cevap sürelerini ve TTL (Paket Yaşam Süresi) değerini inceleyiniz (Görsel 5.5).

Adım 4: ping kocasinan.bel.tr komutuyla ile ülkemizdeki bir belediyenin web sayfasının paket cevap ve TTL değerini inceleyiniz (Görsel 5.5).

Adım 5: ***ping www.edu.gov.az*** komutuyla Azerbaycan Eğitim Bakanlığı web sayfasının paket cevap ve TTL değerini inceleyiniz (Görsel 5.5).

Adım 6: ***ping*** **www.meb.gov.tr** komutunu yazarak Millî Eğitim Bakanlığı web sayfasının paket cevap sürelerini inceleyiniz (Görsel 5.5).

Dikkat

Bazı sunucular güvenlik nedeniyle ping komutlarına kapalıdır ve cevap vermez.

```
C:\WINDOWS\system32>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:
Reply from 192.168.1.2: bytes=32 time<1ms TTL=64
Reply from 192.168.1.2: bytes=32 time=1ms TTL=64
Reply from 192.168.1.2: bytes=32 time<1ms TTL=64
Reply from 192.168.1.2: bytes=32 time=1ms TTL=64

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\WINDOWS\system32>ping kocasinan.bel.tr

Pinging kocasinan.bel.tr [92.45.25.229] with 32 bytes of data:
Reply from 92.45.25.229: bytes=32 time=34ms TTL=46
Reply from 92.45.25.229: bytes=32 time=34ms TTL=46
Reply from 92.45.25.229: bytes=32 time=35ms TTL=46
Reply from 92.45.25.229: bytes=32 time=34ms TTL=46

Ping statistics for 92.45.25.229:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 34ms, Maximum = 35ms, Average = 34ms

C:\WINDOWS\system32>ping www.edu.gov.az

Pinging edu.gov.az [31.170.236.84] with 32 bytes of data:
Reply from 31.170.236.84: bytes=32 time=111ms TTL=47
Reply from 31.170.236.84: bytes=32 time=111ms TTL=47
Reply from 31.170.236.84: bytes=32 time=110ms TTL=47
Reply from 31.170.236.84: bytes=32 time=126ms TTL=47

Ping statistics for 31.170.236.84:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 110ms, Maximum = 126ms, Average = 114ms

C:\WINDOWS\system32>ping www.meb.gov.tr

Pinging www.meb.gov.tr [212.174.189.120] with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 212.174.189.120:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Görsel 5.5: ping komutu

Adım 7: ***ping -t 192.168.1.2*** komutuyla **sonlandırılana kadar devam eden ping isteği** oluşturunuz. Ctrl+C tuş kombinasyonu ile komutu durdurunuz.

Adım 8: ***ping -n 8*** **kocasinan.bel.tr** komutuyla 8 adet ping isteği oluşturunuz (Görsel 5.6).

```
C:\WINDOWS\system32>ping -n 8 www.kocasinan.bel.tr

Pinging www.kocasinan.bel.tr [92.45.25.229] with 32 bytes of data:
Reply from 92.45.25.229: bytes=32 time=40ms TTL=46
Reply from 92.45.25.229: bytes=32 time=33ms TTL=46
Reply from 92.45.25.229: bytes=32 time=37ms TTL=46
Reply from 92.45.25.229: bytes=32 time=34ms TTL=46
Reply from 92.45.25.229: bytes=32 time=38ms TTL=46
Reply from 92.45.25.229: bytes=32 time=45ms TTL=46
Reply from 92.45.25.229: bytes=32 time=33ms TTL=46
Reply from 92.45.25.229: bytes=32 time=984ms TTL=46

Ping statistics for 92.45.25.229:
    Packets: Sent = 8, Received = 8, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 33ms, Maximum = 984ms, Average = 155ms
```

Görsel 5.6: Belirli sayıda ping isteği

Adım 9: ***ping -a 195.175.39.39*** komutuyla IP adresinin alan adını çözümleyiniz (Görsel 5.7).

```
C:\WINDOWS\system32>ping -a 195.175.39.39

Pinging dns39.turktelekom.com.tr [195.175.39.39] with 32 bytes of data:
Reply from 195.175.39.39: bytes=32 time=24ms TTL=245
Reply from 195.175.39.39: bytes=32 time=23ms TTL=245
Reply from 195.175.39.39: bytes=32 time=21ms TTL=245
Reply from 195.175.39.39: bytes=32 time=22ms TTL=245

Ping statistics for 195.175.39.39:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 21ms, Maximum = 24ms, Average = 22ms
```

Görsel 5.7: IP adresinin çözümlenmesi

Sıra Sizde

1. Arkadaşınızın bilgisayarının IP adresine ping isteği gönderiniz.
2. Yerel belediyenizin web sayfasına ve coğrafi olarak uzak başka bir belediyenin sayfasına ping isteği gönderiniz. Elde ettiğiniz bilgileri arkadaşlarınızla paylaşarak karşılaştırınız. Benzerlikleri ve farklılıkları bulunuz.

5.2.1.3. tracert Komutu

tracert komutu, gönderilen veri paketinin hedef cihaza giderken geçtiği yönlendiricilerin listesini verir. Veri paketi hedefe giderken yol üzerindeki her yönlendirici, veri paketini gönderene ayrı ayrı yanıt verir. Böylece paketin alıcısına ulaşıp ulaşmadığı veya hangi atlamadan sonra kaybolduğu belirlenebilir. Bu komutla kullanılabilecek parametreler Tablo 5.17'de verilmiştir.

Tablo 5.17: tracert Komutu Parametreleri

Parametre	İşlevi
-d	IP adresleri (yönlendiricilerin) adlarının çözülmesini engeller.
-h maximum_hops	Hedefe ulaşıncaya kadar geçilecek olan en büyük atlama sayısını belirler. 1 ile 255 arası değer verilebilir. Varsayılan değer 30'dur.
-w timeout	Milisaniye cinsinden, paketlerinin ne kadar bir süre kullanılabilir olduğunu belirler. Değer belirlenmezse otomatik olarak bu değer 4.000'e (4.000 milisaniye =4 saniye) ayarlanır.
-r	Gidiş / Dönüş yolunu izler. Sadece IPv6 adreste kullanılır.
-s srcaddr	İletilerde kullanılacak kaynak adresini belirler. Sadece IPv6 adreste kullanılır.
-4	IPv4 kullanılacağını belirtir.
-6	IPv6 kullanılacağını belirtir.

Uygulama 9

http://kitap.eba.gov.tr/KodSor.php?KOD=21038

tracert komutu ve parametrelerini çalıştırmak için gerekli işlemleri aşağıdaki yönergeler doğrultusunda gerçekleştiriniz.

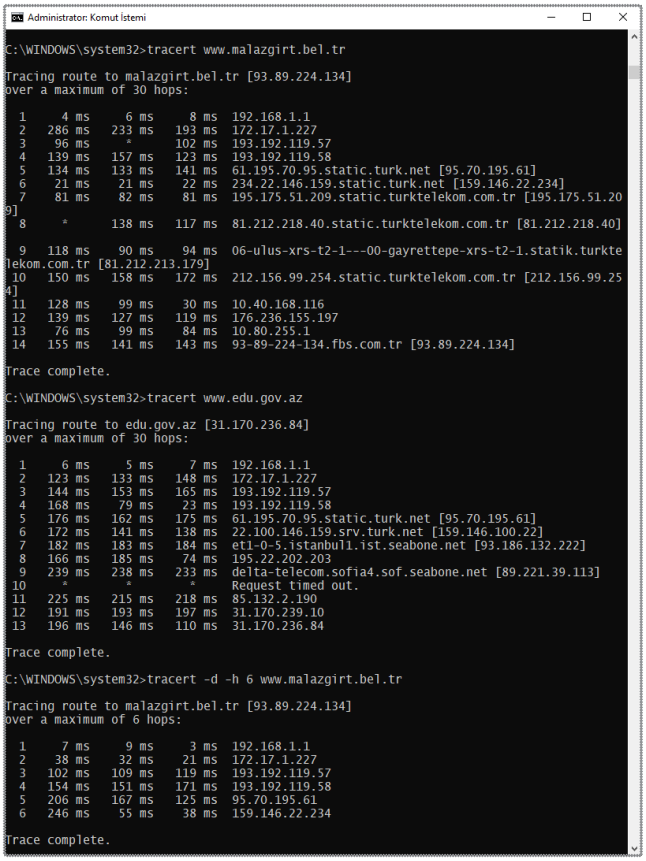
Adım 1: Komut istemcisini çalıştırınız.

Adım 2: Komut istemciye ***tracert*** yazıp "Enter" tuşuna basarak tracert komutuyla kullanabileceğiniz parametreleri inceleyiniz.

Adım 3: ***tracert www.malazgirt.bel.tr*** komutuyla Malazgirt Belediyesi web sayfasına erişmek için geçilen yönlendiricileri ve sürelerini inceleyiniz (Görsel 5.8).

Adım 4: ***tracert edu.gov.az*** komutuyla Azerbaycan Eğitim Bakanlığı web sayfasına erişmek için geçilen yönlendiricileri ve geçen süreyi inceleyiniz (Görsel 5.8).

Adım 5: ***tracert -d -h 6 www.malazgirt.bel.tr*** komutuyla Malazgirt Belediyesi web sayfasına giden paketlerin izlediği yoldaki ilk 6 yönlendiriciyi adları çözümlenmeden görünüz (Görsel 5.8).



Görsel 5.8: tracert komutu

5.2.1.4. nbtstat Komutu

nbtstat komutu, NetBIOS bağlantılarının detaylarını görmeyi sağlar. **NetBIOS** [Network Basic Input/Output System (Temel Ağ Giriş / Çıkış Sistemi)], yerel ağ üzerindeki farklı cihazların birbirleriyle iletişim kurmasını sağlayan bir sistemdir. Bu komut ile kullanılabilecek parametreler Tablo 5.18'de verilmiştir.

Tablo 5.18: nbtstat Komutu Parametreleri

Parametre	İşlevi
-a UzakAd	Uzaktaki bilgisayarın NetBIOS ad tablosunu görüntüler. Bilgisayar adı girilir.
-A IPAdresi	Uzaktaki bilgisayarın NetBIOS ad tablosunu görüntüler. Bilgisayarın IP adresi girilir.
-c	NetBIOS ad önbelleğinin içeriğini, NetBIOS adları tablosunu ve onların çözümlenmiş IP adreslerini görüntüler.
-n	Sisteme yerel olarak kaydedilmiş adları görüntüler.
-r	Genel yayın (Broadcast) ya da WINS tarafından çözülmüş adları listeler.
-R	Uzak önbellek adı tablosunu temizler ve yeniden yükler.
-RR	Bir WINS sunucusuna kaydettirilen NetBIOS adlarını serbest bırakır ve ardından bunların kaydını yeniler.
-s	Geçerli NetBIOS oturumlarını ve durumlarını listeler.
-S	Hedef IP adresleri ile birlikte oturum tablosunu listeler.

Dikkat

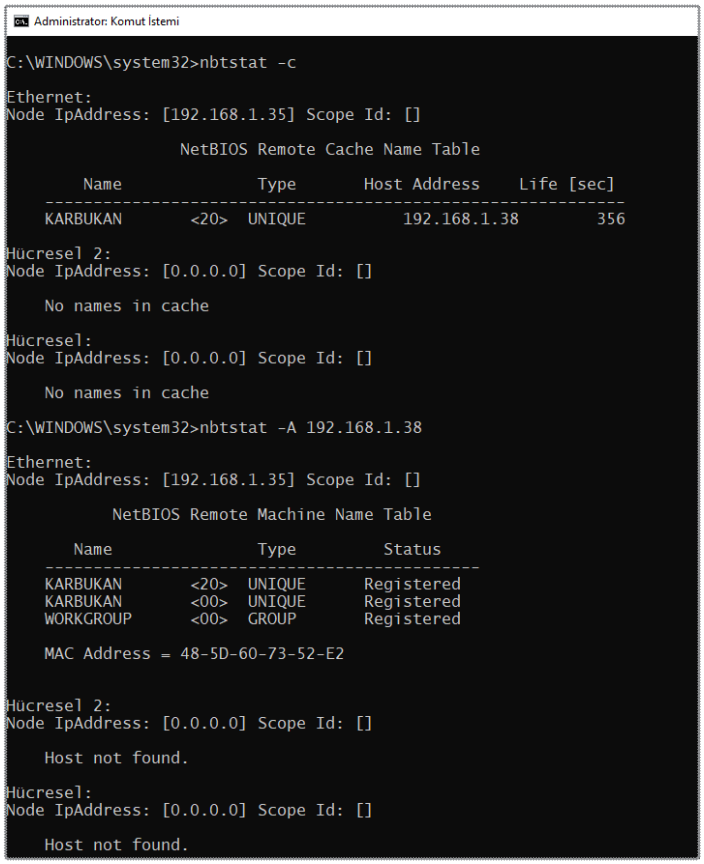
nbtstat komut satırı parametreleri, büyük / küçük harfe duyarlıdır.

Uygulama 10

nbtstat komutu ve parametrelerini çalıştırmak için işlemleri yönergeler doğrultusunda gerçekleştiriniz.

Adım 1: Komut istemcisini çalıştırınız.

Adım 2: ***nbtstat -c*** komutuyla NetBIOS ad önbelleğinin içeriğini görüntüleyiniz (Görsel 5.9).



Görsel 5.9: nbtstat -c ve -A parametresi

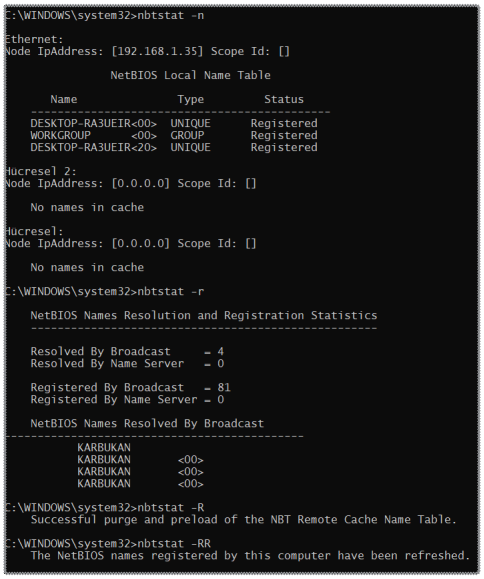
Adım 3: ***nbtstat -A 192.168.1.38*** yazıp "Enter" tuşuna basarak IP adresini bildiğiniz uzak bilgisayarın NetBIOS isim tablosunu görüntüleyiniz (Görsel 5.9).

Adım 4: ***nbtstat -n*** komutuyla yerel olarak kaydedilmiş NetBIOS adlarını görüntüleyiniz (Görsel 5.10).

Adım 5: ***nbtstat -r*** komutuyla genel yayın (Broadcast) veya WINS tarafından çözümlenmiş isimleri görüntüleyiniz (Görsel 5.10).

Adım 6: ***nbtstat -R*** komutuyla uzak önbellek isim tablosunu temizleyiniz (Görsel 5.10).

Adım 7: ***nbtstat -RR*** komutuyla kayıtlı NetBIOS tablosunu yenileyiniz (Görsel 5.10).



Görsel 5.10: nbtstat parametreleri

5.2.1.5. netstat Komutu

netstat komutu, bilgisayardaki etkin TCP/IP bağlantılarını gösterir. Gelen ve giden bağlantılarla birlikte yönlendirme tablolarını da göstermektedir. Ağ kartlarına ait istatistiklerle beraber sistemdeki açık portları kontrol etmeye yardımcı olan bir komuttur. Bu komut ile kullanılabilecek parametreler Tablo 5.18'de verilmiştir.

Tablo 5.18: netstat Komutu Parametreleri

Parametre	İşlevi
-a	Tüm aktif bağlantıları ve bilgisayarın dinlediği TCP ve UDP portları görüntüler.
-an	Dosya alırken karşıdaki cihazın IP adresini gösterir.
-b	Her bağlantı veya dinleme bağlantı noktasıyla ilişkili çalıştırılabilir dosyayı gösterir. Komut istemci yönetici olarak çalıştırılmalıdır.
-e	Ethernet istatistiklerini gösterir.
-o	Her bağlantıyla ilişkili, sahip işlem kimliğini gösterir.
-p Proto	İletişim kuralının bağlantılarını gösterir. Protokol ismi ile hangi protokolün hangi bağlantıda kullanıldığına dair istatistiksel veriler gösterilir. Proto parametresi olarak **tcp**, **udp**, **tcpv6** ya da **udpv6** isimleri girilebilir.
-r	Yönlendirme tablosunu gösterir.
-n	Aktif TCP bağlantılarını görüntüler. Adresler ve bağlantı noktası numaraları sayısal olarak ifade edilir, herhangi bir isim belirlemesi yapılmaz.
-s	İletişim kuralına göre istatistikleri gösterir. Varsayılan olarak TCP, UDP, ICMP ve IP iletişim kuralı istatistiklerini gösterir.
-v	-b ile kullanılırsa tüm çalışan dosyalar için bağlantı ve bağlantı noktası oluşumu ile ilgili bileşenlerin sırasını gösterir.
interval	Belirlenen saniye cinsinden süre sonunda ekrandaki bilgiler tazelenir. Örneğin bu değer, 10 olarak belirlenirse her 10 saniyede bir ekranda **netstat** komutu ile gösterilmiş olan veriler yenilenir.

Uygulama 11

http://kitap.eba.gov.tr/KodSor.php?KOD=21039

Bilgisayardaki açık portları görmek için gerekli işlemleri aşağıdaki yönergeler doğrultusunda gerçekleştiriniz.

Adım 1: Komut istemcisini çalıştırınız.

Adım 2: netstat -a yazdıktan sonra "Enter" tuşuna basıp bilgisayardaki tüm aktif bağlantıları ve dinlediği portların bağlantılarını listeleyerek inceleyiniz.

Adım 3: netstat -an yazdıktan sonra "Enter" tuşuna basıp bağlantı kurulan diğer cihazların IP adreslerini listeleyerek inceleyiniz.

Adım 4: netstat –an | find /i "listening" komutuyla sadece dinlenen portları listeleyiniz.

Adım 5: netstat –an | find /i "established" komutuyla sadece bağlantı kurulu olan portları listeleyiniz.

Adım 6: netstat -p tcp komutuyla iletişim kuralında TCP ile yapılan bağlantıları listeleyerek bağlantıları inceleyiniz (Görsel 5.11).

Adım 7: netstat -e komutuyla Ethernet istatistiklerini listeleyiniz ve inceleyiniz (Görsel 5.11).

Adım 8: netstat -o komutuyla bağlantıların sahip işlem kimliğini listeleyerek inceleyiniz (Görsel 5.11).

Adım 9: netstat -v -b komutuyla aktif çalışan dosyalar için bağlantı ve bağlantı noktalarını listeleyerek inceleyiniz (Görsel 5.11).

```
C:\WINDOWS\system32>netstat -p tcp

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    192.168.1.35:52014     1drv:https             ESTABLISHED
  TCP    192.168.1.35:57175     52.114.132.73:https    TIME_WAIT
  TCP    192.168.1.35:57180     52.184.213.187:https   TIME_WAIT
  TCP    192.168.1.35:52638     a2-20-148-10:https     ESTABLISHED
  TCP    192.168.1.35:54879     51.103.5.159:https     ESTABLISHED
  TCP    192.168.1.35:54880     ec2-3-235-82-188:https  ESTABLISHED
  TCP    192.168.1.35:54924     ec2-52-202-62-217:https  ESTABLISHED
  TCP    192.168.1.35:55228     wl-in-f188:5228        ESTABLISHED
  TCP    192.168.1.35:55238     51.103.5.159:https     ESTABLISHED
  TCP    192.168.1.35:55496     server-54-192-233-74:https  ESTABLISHED
  TCP    192.168.1.35:57214     52.109.68.21:https     TIME_WAIT

C:\WINDOWS\system32>netstat -e
Interface Statistics

                           Received            Sent

Bytes                    1252699368       268954284
Unicast packets           100034076        38237972
Non-unicast packets         7950312         4136332
Discards                          0               0
Errors                            0              36
Unknown protocols                 0

C:\WINDOWS\system32>netstat -o

Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    192.168.1.35:52014     1drv:https             ESTABLISHED     240
  TCP    192.168.1.35:52158     ec2-3-235-82-213:https  CLOSE_WAIT      15396
  TCP    192.168.1.35:52581     ec2-63-33-106-135:https  ESTABLISHED     13260
  TCP    192.168.1.35:52638     a2-20-148-10:https     ESTABLISHED     5872
  TCP    192.168.1.35:54879     51.103.5.159:https     ESTABLISHED     9900
  TCP    192.168.1.35:54880     ec2-3-235-82-188:https  ESTABLISHED     15396
  TCP    192.168.1.35:54924     ec2-52-202-62-217:https  ESTABLISHED     15396
  TCP    192.168.1.35:55228     wl-in-f188:5228        ESTABLISHED     13260

C:\WINDOWS\system32>netstat -v  -b

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    192.168.1.35:52014     1drv:https             ESTABLISHED
 [WINWORD.EXE]
  TCP    192.168.1.35:52158     ec2-3-235-82-213:https  CLOSE_WAIT
 [Zoom.exe]
  TCP    192.168.1.35:52581     ec2-63-33-106-135:https  ESTABLISHED
 [chrome.exe]
  TCP    192.168.1.35:52638     a2-20-148-10:https     ESTABLISHED
 [Video.UI.exe]
  TCP    192.168.1.35:54879     51.103.5.159:https     ESTABLISHED
```

Görsel 5.11: netstat komutu

Adım 10: netstat -r komutuyla yönlendirme tablosunu listeleyerek inceleyiniz (Görsel 5.12).

```
C:\WINDOWS\system32>netstat -r
===========================================================================
Interface List
  7...90 e6 ba 07 10 7e ......Realtek PCIe GBE Family Controller
  1...........................Software Loopback Interface 1
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0    192.168.1.1    192.168.1.35     35
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    331
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    331
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    331
      192.168.1.0    255.255.255.0         On-link      192.168.1.35    291
     192.168.1.35  255.255.255.255         On-link      192.168.1.35    291
    192.168.1.255  255.255.255.255         On-link      192.168.1.35    291
        224.0.0.0        240.0.0.0         On-link         127.0.0.1    331
        224.0.0.0        240.0.0.0         On-link      192.168.1.35    291
  255.255.255.255  255.255.255.255         On-link         127.0.0.1    331
  255.255.255.255  255.255.255.255         On-link      192.168.1.35    291
===========================================================================
Persistent Routes:
  None

IPv6 Route Table
===========================================================================
Active Routes:
 If Metric Network Destination      Gateway
  1    331 ::1/128                  On-link
  7    291 fe80::/64                On-link
  7    291 fe80::85d2:f9c8:7e0:e42f/128
                                    On-link
  1    331 ff00::/8                 On-link
  7    291 ff00::/8                 On-link
===========================================================================
Persistent Routes:
  None
```

Görsel 5.12: netstat -r parametresi

5.2.1.6. arp Komutu

Ağ ortamında cihazlar birbirleri ile haberleşmek için TCP/IP protokolünü kullanır. Bu durumda haberleşme, IP adresleri üzerinden gerçekleşir. Yerel ağda haberleşmek için veri alışverişi yapılacak cihazın fiziksel (MAC) adresi bilinmelidir. **arp** komutu, IP adresi bilinen cihazın fiziksel adresinin öğrenilmesini sağlar. Bu komut ile kullanılabilecek parametreler Tablo 5.19'da verilmiştir.

Tablo 5.19: arp Komutu Parametreleri

Parametre	İşlevi
-a	Tüm arabirimlerin geçerli ARP önbellek tablolarını görüntüler.
-g	-a komutu ile aynı görevi görür.
-v	Geçerli ve geçersiz ARP bilgilerini özet olarak görüntüler.
inet_addr	İnternet adresini belirtir.
-Nif_addr	if_addr ile belirtilen ağ arabiriminin ARP girdilerini görüntüler.
-d	Belirtilen ana bilgisayarı siler.
-s	ARP tablosuna bilgisayar eklemek için kullanılır.
eth_addr	Fiziksel adresi belirtir.
if_addr	Bu adres kullanıldığında adreste yazan değer işleme alınır, yazılmazsa ilk uygun değer kullanılır.

Uygulama 12

http://kitap.eba.gov.tr/KodSor.php?KOD=21040

arp komutu ve parametrelerini çalıştırmak için işlemleri yönergeler doğrultusunda gerçekleştiriniz.

Adım 1: Komut istemcisini çalıştırınız.

Adım 2: arp -a yazdıktan sonra "Enter" tuşuna basıp bilgisayar ARP önbelleğinde kayıtlı tabloyu görüntüleyerek inceleyiniz (Görsel 5.13).

Adım 3: arp -s 192.168.1.41 fc-3d-93-93-fe-b6 komutuyla ARP önbelleğine eklenmek istenilen IP adresini ve fiziksel (MAC) adresini giriniz (IP ve fiziksel adres olarak arkadaşınızın bilgisayarının adreslerini giriniz.).

```
C:\WINDOWS\system32>arp -a

Interface: 192.168.1.35 --- 0x7
  Internet Address      Physical Address      Type
  192.168.1.1           8c-59-73-2a-78-26     dynamic
  192.168.1.2           04-bf-6d-2a-d9-d2     dynamic
  192.168.1.34          48-5d-60-73-83-09     dynamic
  192.168.1.38          48-5d-60-73-52-e2     dynamic
  192.168.1.47          bc-ae-c5-10-8e-0a     dynamic
  192.168.1.254         30-b5-c2-42-27-bb     dynamic
  192.168.1.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.2             01-00-5e-00-00-02     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

C:\WINDOWS\system32>arp -s 192.168.1.41 fc-3d-93-93-fe-b6

C:\WINDOWS\system32>arp -a

Interface: 192.168.1.35 --- 0x7
  Internet Address      Physical Address      Type
  192.168.1.1           8c-59-73-2a-78-26     dynamic
  192.168.1.2           04-bf-6d-2a-d9-d2     dynamic
  192.168.1.34          48-5d-60-73-83-09     dynamic
  192.168.1.38          48-5d-60-73-52-e2     dynamic
  192.168.1.41          fc-3d-93-93-fe-b6     static
  192.168.1.47          bc-ae-c5-10-8e-0a     dynamic
  192.168.1.254         30-b5-c2-42-27-bb     dynamic
  192.168.1.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.2             01-00-5e-00-00-02     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

Görsel 5.13: arp komutu

Adım 4: *arp -a* yazdıktan sonra "Enter" tuşuna basıp bilgisayar ARP önbelleğinde kayıtlı tabloyu görüntüleyerek eklediğiniz IP adresi ve fiziksel adresi görüntüleyiniz (Görsel 5.13).

Adım 5: İlk görüntülediğiniz liste ile ikinci listeyi kıyaslayınız ve değişikliği arkadaşlarınızla tartışınız.

Adım 6: *arp -a -v* komutuyla bilgisayardaki tüm geçerli ve geçersiz arabirimler için ARP önbelleğindeki kayıtlı tabloyu görüntüleyerek inceleyiniz.

Adım 7: *arp -d 192.168.1.41* komutuyla ARP önbelleğinde bulunan bir kaydı siliniz ve ARP tablosunu tekrar listeleyerek işlemi kontrol ediniz.

**Adım 8: *arp -d ** ** komutuyla ARP önbelleğini temizleyiniz.

5.2.1.7. nslookup Komutu

nslookup komutu, alan adı sistemi (DNS) altyapısını tanılamak için kullanabilecek bilgileri görüntüler. IP adresini girerek isim sorgusu ya da web adresini girerek IP adresi sorgusu yapılabilir. Komut satırında ***nslookup*** komutunu çalıştırıp önce bilgisayarda kullanılan DNS sunucusu ve IP adresi görünür. Ekrana "**>**" işareti geldikten sonra sadece parametreleri yazarak kullanılabilir. Tekrar komut istemci ana ekranına dönmek için ***Ctrl+C*** tuş kombinasyonu veya ***exit*** komutu kullanılır. Tek bir sorgu yapmak için komutun ardından parametre yazılarak çalıştırılabilir. Bu komut ile kullanılabilecek parametreler Tablo 5.20'de verilmiştir.

Tablo 5.20: nslookup Komutu Parametreleri

Parametre	Anlamı
exit	nslookup komutundan çıkar.
server	Varsayılan sunucuyu belirtilen alan adı sistemine dönüştürür.
set	Aramaları etkinleştiren yapılandırma ayarlarını değiştirir.
setall	Yapılandırma ayarlarının geçerli değerlerini yazdırır.
setclass	Sorgulama sınıfını değiştirir.
setd2	"Tam Hata Ayıklama Modu"nu açar veya kapatır.
setdebug	"Hata Ayıklama Modu"nu açar veya kapatır.
setdefname	Varsayılan DNS etki alanı adını tek bileşen arama isteğine ekler.
set domain	Varsayılan DNS etki alanı adını, belirtilen ada dönüştürür.
setignore	Paket kesme hatalarını yok sayar.
set port	Varsayılan TCP/UDP, DNS ad sunucusu bağlantı noktasını belirtilen değer olarak değiştirir.
setquerytype	Sorgu için kaynak kayıt türünü değiştirir.
setrecurse	DNS ad sunucusunun elinde bilgi yoksa diğer sunucuların sorgulanmasını sağlar.
setretry	Yeniden deneme sayısını belirtir.
setroot	Sorgularda kullanılan kök sunucusunun adını değiştirir.
setsearch	Bir yanıt alınana kadar DNS etki alanı arama listesinde bulunan etki alanı adlarını isteğe ekler.
setsrchlist	Varsayılan DNS etki alanı adını ve arama listesini değiştirir.
settimeout	Bir isteğin yanıtı için beklenecek başlangıç saniye değerini değiştirir.
settype	Sorgu için kaynak kayıt türünü değiştirir.
setvc	Sunucuya istek gönderirken sanal devre kullanılıp kullanılmayacağını belirtir.
ls	DNS etki alanı bilgilerini listeler.
lserver	Varsayılan sunucuyu belirtilen alan adı sistemine dönüştürür.
root	Varsayılan sunucuyu DNS'nin kök sunucusu olarak değiştirir.
view	Daha önceki "ls" alt komut veya komutların çıktılarını sıralar ve listeler.

Uygulama 13

nslookup komutu ve parametrelerini çalıştırmak için gerekli işlemleri aşağıdaki yönergeler doğrultusunda gerçekleştiriniz.

Adım 1: Komut istemcisini çalıştırınız.

Adım 2: nslookup komutunu çalıştırınız, bilgisayarınızın DNS sunucu ve IP adresi bilgilerini görüntüleyerek komuta giriş yapınız (Görsel 5.14).

Adım 3: www.meb.gov.tr adresini yazıp "Enter" tuşuna basınız ve IP adresi bilgisini görüntüleyiniz (Görsel 5.14).

Adım 4: set querytype=ns komutunu çalıştırarak isim sunucuları (name server) sorgusu yapmak üzere ayarlayınız (Görsel 5.14).

Adım 5: edu.gov.az adresinin isim sunucularını görüntüleyiniz (Görsel 5.14).

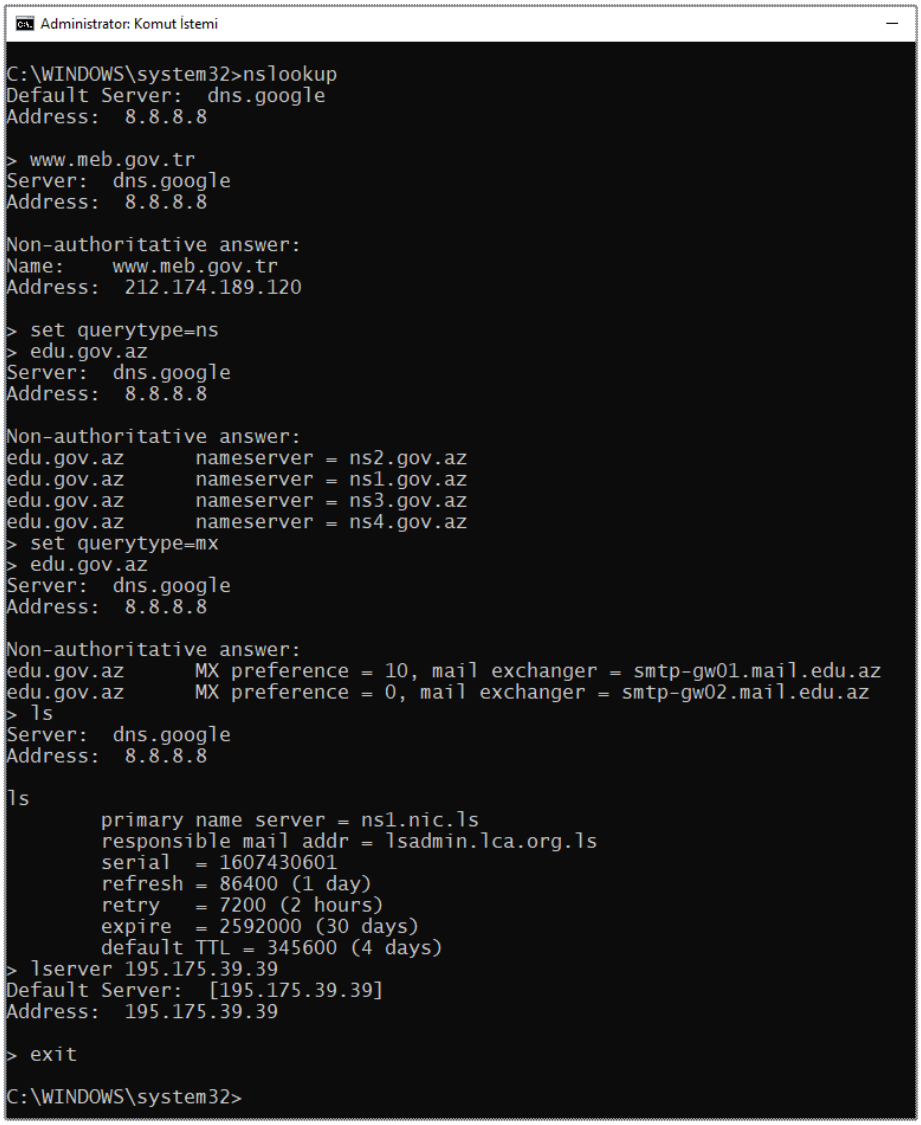
Adım 6: set querytype=mx komutunu çalıştırınız ve bilgisayarın posta servisini görüntülemek üzere ayarlayınız (Görsel 5.14).

Adım 7: edu.gov.az adresinin posta servislerini görüntüleyiniz (Görsel 5.14).

Adım 8: "**ls**" komutuyla DNS bilgilerini görüntüleyiniz (Görsel 5.14).

Adım 9: lserver 195.175.39.39 komutuyla DNS sunucusunu değiştiriniz (Görsel 5.14).

Adım 10: exit komutuyla ana komut istemci ekranına geliniz (Görsel 5.14).



Görsel 5.14: nslookup komutu

Aşağıdaki soruları dikkatlice okuyunuz ve doğru seçeneği işaretleyiniz.

1-3 numaralı sorular aşağıdaki IP adresine göre cevaplandırınız. 26.8.10.71/27 olarak verilen IP adresi için:

1. Alt ağ maskesi (Subnet Mask) nedir?

A) 255.000.000.000 B) 255.255.000.224 C) 255.255.224.000
D) 255.255.255.224 E) 255.255.255.255

2. Ağ adresi (Network Address) nedir?

A) 26.8.10.64 B) 26.8.10.65 C) 26.8.10.95 D) 26.8.10.96 E) 26.8.10.255

3. Bağlı bulunduğu alt ağda en fazla kaç cihaz bağlanabilir?

A) 30 B) 60 C) 126 D) 240 E) 254

4. Aşağıdaki komutlardan hangisi Ethernet kartının fiziksel (MAC) adres bilgisini öğrenmede kullanılır?

A) ipconfig B) ipconfig /all C) nbstat -n D) netstat E) netstat -m

5. Komut istemciye *arp -d ** komutu yazan teknisyen aşağıdakilerden hangisini gerçekleştirmiş olur?

A) ARP tablosunu görüntüler.
B) Fiziksel adres belirtir.
C) ARP tablosunu siler.
D) İnternet adresini belirtir.
E) ARP tablosuna MAC adresleri ekler.

6. İstenilen IP adresine ping komutunun sürekli olarak çalışmasını sağlayan komut aşağıdakilerden hangisidir?

A) ping –a B) ping –f C) ping –r D) ping -s E) ping –t

7. IP adresinin serbest bırakılması için kullanılan komut aşağıdakilerden hangisidir?

A) ipconfig /setclassid
B) ipconfig /renew
C) ipconfig /release
D) ipconfig /all
E) ipconfig /downip

8. I. Yönlendirici adı
II. Yönlendirici IP adresi
III. Yönlendirici sayısı
IV. Yönlendirici MAC adresi

tracert komutu ile bir paketin izlediği yol hakkında yukarıda verilen bilgilerden hangisi ya da hangileri elde edilir?

A) I-II B) II-III C) III-IV D) I-II-III E) I-II-IV

ÖĞRENME BİRİMİ 6

ANAHTARLAR

NELER ÖĞRENECEKSİNİZ?

Bu öğrenme birimi ile;

- Anahtarları bilecek,
- Anahtarların kablo bağlantılarını yapacak,
- Ethernet çerçeve yapısını öğrenecek,
- MAC adres tablosunu bilecek,
- Anahtarların kullanım yerlerini bilecek,
- Broadcast ve Collision Domain kavramlarını öğrenecek,
- Anahtar türlerini bilecek,
- Anahtar işletim sisteminin amacını bilecek,
- Anahtar arayüz yapılandırmasını gerçekleştirecek,
- Uzak masaüstü yapılandırmasını gerçekleştirecek,
- Telnet, SSH ve Console yapılandırmasını sağlayacak,
- Port hızı ve Duplex modu yapılandırmasını gerçekleştirecek,
- DHCP yapılandırmasını gerçekleştirecek,
- Yapılandırmayı kaydetme ve geri yükleme işlemlerini yapabileceksiniz.

ANAHTAR KELİMELER

Anahtar, Switch, Ethernet, MAC adres tablosu, Broadcast Domain, Collision Domain, Console, SSH, Telnet, Port hızı, Duplex, DHCP

Hazırlık Çalışmaları

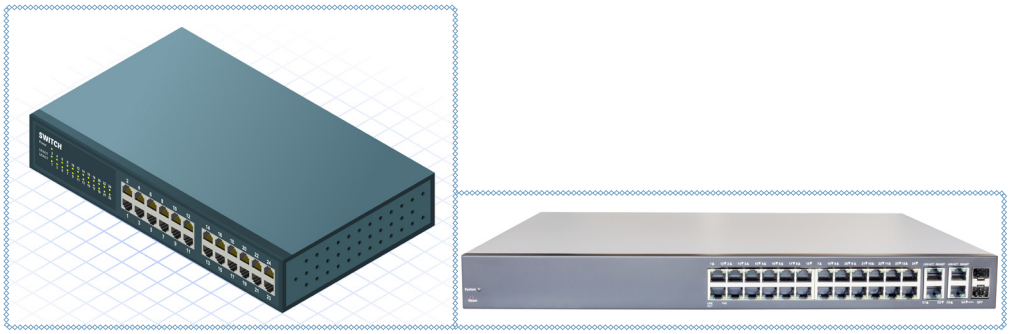
1. Anahtarlar kendilerine bağlı cihazların mesajlarını karıştırsalardı neler olurdu? Arkadaşlarınızla beyin fırtınası yaparak fikirlerinizi paylaşınız.
2. Ağdaki tüm kullanıcılar anahtarların yapılandırmalarını değiştirebilseydi ağ iletişimi nasıl etkilenirdi? Düşüncelerinizi arkadaşlarınızla paylaşınız.
3. Küçük iş yeri, ev gibi ortamlarda kullandığımız anahtar ile büyük işletmelerde kullanılan anahtarlar arasında ne gibi farklar olabilir? Açıklayınız.

6.1. Anahtarların Fiziksel Kurulumu

Anahtarlar (Switch), bilgisayar, yazıcı gibi ağ cihazlarını birbirine bağlayarak anahtarlama yöntemi ile haberleşmelerini sağlayan ağ cihazıdır. Genellikle OSI modelinin ikinci katmanı olan veri bağı katmanında çalışırlar. Üçüncü katmanda da (ağ katmanında) çalışan ve yönlendirme işlevini de destekleyen anahtarlar da bulunmaktadır.

6.1.1. Anahtarlar

Anahtarlar (Switch), kendisine gelen veri trafiğini arayüzleri (portları) arasında anahtarlayarak aktarmaktadır. Arayüzlerine (portlarına) bağlı cihazların hepsine ayrı birer yol tahsis eder. Anahtar, veriyi gönderen cihaz ile alan cihaz arasında yol kurarak iletim gerçekleştirir. Ağ uygulamalarında en çok kullanılan ağ cihazı türlerinden biridir (Görsel 6.1).



Görsel 6.1: Anahtar (Switch)

Anahtar cihazların üstünde hiçbir trafik yokken tüm portları birbirinden yalıtılmış durumda beklemektedir. Dolayısıyla anahtara bağlı tüm sistemler arasında bağlantı kopuktur denilebilir. Ancak bir sistem diğeri ile iletişimde bulunmak isterse ikisinin bağlı olduğu portlar, anahtar üzerinden birbirine bağlanır. Bu işleme **anahtarlama** denir. Anahtarlama işlemi için anahtar arayüzlerine bağlı cihazların 48 bitlik MAC (Media Access Control) adreslerini kullanır.

6.1.1.1. Aktarım Yöntemleri

Bir ağ anahtarının kullanabileceği dört çeşit iletme yöntemi vardır.

Depola ve İlet (Store And Forward)

- Paketi giriş portundan aldıktan sonra buffer'a atar.
- Pakette hata olup olmadığını kontrol eder. Hatalıysa iletmez.
- Ardından paketi ilgili çıkış portuna gönderir.

Kestirme (Cut-Through)

- Paketi iletmeden önce hedef adresi belirler.
- Adresin çıkış portuna bu paketi iletir.
- Paketteki hataları kontrol etmez, bu nedenle daha hızlıdır.
- Bozuk paketler ağda ilerler.

Serbest Parça (Fragment Free)

Kestirme ile **Depola ve İlet** yöntemlerinin avantajlarından faydalanmaya çalışan bir yöntemdir.

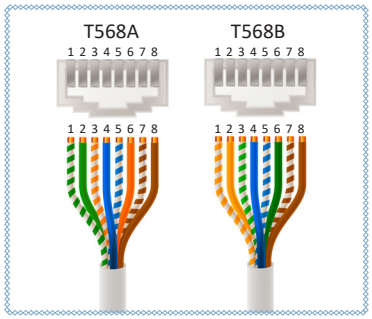
- Paketin adresleme bilgisinin bulunduğu ilk 64 byte (bayt) okunur.
- Veri boyutu 64 byte olmayan paketler silinir.
- Kontrol toplamı oluşturulmadan iletilir.

Uyarlamalı Anahtarlama (Adaptive Switching)

Diğer üç yöntem arasında kendi kendine seçim yapan özel bir yöntemdir.

6.1.2. Anahtarların Kablo Bağlantıları

Anahtarlar, birbirleri ve diğer cihazlar arasındaki bağlantıların sağlanması amacıyla üç tür kablo yapısı ile bağlanır. Kablolar belirlenen standartlara göre hazırlanmalıdır. Arıza oluşması durumunda arızanın tespiti ve giderilmesi kolaylaşır. UTP kablo standart sıralaması Görsel 6.2'de gösterilmiştir.



Görsel 6.2: UTP kablo standardı

Düz Kablo Bağlantısı (Straight-through): Düz kablo bağlantısıyla anahtarların diğer ağ cihazları ile bağlantıları sağlanır. Düz kablo hazırlamak için UTP kablonun her iki ucunu da aynı standarda göre sıralamak gerekir.

Çapraz Kablo Bağlantısı (Crossover): Çapraz kabloyla anahtarlar arası bağlantı sağlanır. Çapraz kablo hazırlamak için UTP kablonun bir ucunu **T568A** diğer ucunu **T568B** standardına göre sıralamak gerekir.

Konsol Kablo Bağlantısı (Rollover): Bilgisayarın komut istemcisi aracılığıyla anahtarların yapılandırılmaları amacıyla kullanılır. Anahtarların ilk yapılandırmaları konsol kabloları aracılığıyla yapılabilir. Rollover kablo hazırlamak için UTP kablonun bir ucu **T586A** standardına göre sıralandıysa diğer ucu T586A'nın tersine göre sıralanmalıdır. Bilgisayara bağlanacak ucu da seri porta ya da USB portuna çevrilmelidir (Görsel 6.3).

Görsel 6.3: Konsol kablosu ve dönüştürücü

Uygulama 1

Anahtarın kablo bağlantılarını yapma işlemini aşağıdaki yönergeler doğrultusunda gerçekleştiriniz.

Adım 1: Düz hazırlanmış UTP kabloyla anahtar ile bilgisayarları bağlayınız.

Adım 2: Çapraz hazırlanmış UTP kabloyla iki anahtarı birbirine bağlayınız.

Adım 3: Konsol kablosuyla anahtarınızın konsol portunu ve bilgisayarınızın serial portunu ya da USB portunu serial çevirici aracılığıyla bağlayınız.

6.1.3. Ethernet Çerçeve Yapısı

Ağ iletişiminde çerçeve biçimi, çerçeve boyutu, zamanlama ve kodlama gibi birçok yönünü Ethernet standartlarıyla tanımlar. Ethernet ağında ağ cihazları arasında mesaj gönderilirken cihazlar standartların belirttiği çerçeve düzenine göre iletilerini biçimlendirir.

Ethernet II çerçevesi toplam 64 ile 1518 arası byte'tan oluşmaktadır. Bu aralığın değişmesinin sebebi çerçeve (frame) içinde yollanan veri (data) miktarıdır. Tablo 6.1'de Ethernet çerçeve yapısı görülmektedir.

Tablo 6.1: Ethernet Çerçeve Yapısı

802.3 Ethernet Çerçeve Yapısı									
Layer	**Başlangıç (Preamble)**	**Çerçeve Sınırlayıcı Başlangıcı (SOF)**	**Hedef MAC Adresi (Destination)**	**Kaynak MAC Adresi (Source)**	**802.1Q Etiket (Varsa)**	**Ethertype (Ethernet II) ve ya Uzunluk (IEEE 802.3)**	**Kapsüllenmiş Veri (Data)**	**Çerçeve Kontrol Sırası (32-bit CRC)**	**Çerçeveler Arası Boşluk**
	7 Byte	1 Byte	6 Byte	6 Byte	(4 Byte)	2 Byte	46(42)–1500 Byte	4 Byte	12 Byte
L2 Ethernet Frame			← 64–1518(1522) Byte →						
L1 Ethernet Bits	← 72–1526(1530) Byte →								

Ethernet çerçevesi üzerindeki alanların boyutu byte cinsinden belirtilmektedir. Data (veri) 1500 byte kapasitesinden daha büyük olamaz. Bu çerçevede bulunan alanlar şu şekilde açıklanabilir:

Preamble: Başlama ekidir.
SOF: Çerçeve sınırlayıcı başlangıcıdır.
Hedef (Destination) MAC Adres: Verinin aktarılacağı hedef (Destination) MAC adresidir.
Kaynak (Source) MAC Adres: Verinin çıktığı kaynak (Source) MAC adresidir.
EtherType: Tür / uzunluk alanı, iletişimin kurulduğu protokol yapısıdır.
Data: Bu alanda iki nokta arasında taşınacak veri (Data) bulunur. En az 46 byte, en çok 1500 byte'tan oluşur.
Pad: Dolgu alanıdır (Küçük çevreler için kullanılır.).
CRC Checksum: Gelen çerçeve içindeki veriler kontrol edilerek iletim esnasında verinin bozulup bozulmadığını denetlemek amacıyla kullanılır.

Dikkat

Çerçeveler arası boşluk değerleri Ethernet hızını belirler.

Tablo 6.2: Ethernet Hızı

Süre	Ethernet Hızı
9.6 µs	10 Mbit/s Ethernet
0.96 µs	100 Mbit/s Fast Ethernet
96 ns	Gigabit Ethernet
9.6 ns	10 Gigabit Ethernet
0.96/2.4 ns	100/40 Gigabit Ethernet

Araştırma

Ethernet çerçevesinde önce hedef MAC adresinin sebebi ne olabilir? Araştırınız ve bulduğunuz sonuçları arkadaşlarınızla paylaşınız.

6.1.4. MAC Adres Tablosu

Anahtarlar veri iletimini arayüzlerine bağlı cihazların MAC adreslerini tanımlayarak yapar. Bu nedenle anahtar cihazlar üzerinde MAC adreslerinin tutulduğu bir tablo (MAC tablosu) bulunur. Anahtarlar MAC adresleri tablosu sayesinde arayüzlerine bağlı cihazların MAC adreslerini bilir ve veriyi ilgili port aracılığıyla alıcı cihaza gönderir (Görsel 6.4).

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

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

   1    0004.9a2e.28ed    DYNAMIC     Fa0/1
   1    000a.418b.708e    DYNAMIC     Fa0/3
   1    0060.2f6c.3aa7    DYNAMIC     Fa0/2
   1    00e0.f9ad.c4b6    DYNAMIC     Fa0/4
Anahtar#
```

Görsel 6.4: Bir anahtarın MAC adres tablosu

Bir veri paketi (veri çerçevesi), anahtarın arayüzlerinden birine ulaştığında anahtar, kaynak MAC adresini ve gönderilen arayüzün (port-kapı) numarasını MAC adres tablosuna kaydeder. Veri paketinin iletileceği MAC adresini MAC tablosunda arar. Hedefe ait bir kayıt bulunamazsa veri paketi, gelen arayüz hariç bütün arayüzlere gönderilir. MAC adresi biliniyorsa bu durumda veri paketi sadece hedef arayüze gönderilir. Gönderenin ve alıcının MAC adresleri aynıysa paket silinir. Anahtarlar, belirli süre veri iletişimi olmazsa MAC tablosunu temizler.

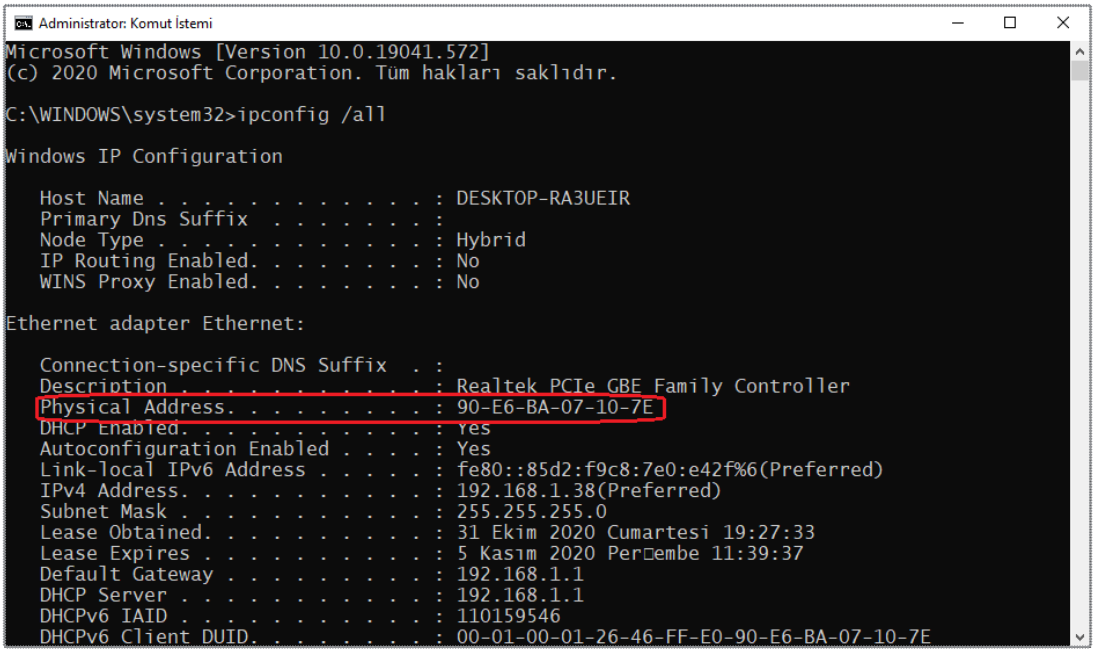
Uygulama 2

Bilgisayarınızın MAC adresini öğrenmek için gerekli işlemleri aşağıdaki yönergeler doğrultusunda gerçekleştiriniz.

Adım 1: Bilgisayarınızın komut istemini çalıştırınız.

Adım 2: ipconfig /all komutunu yazınız ve "Enter" tuşuna basınız.

Adım 3: Karşınıza gelen bilgiler içinde **Physical Address (Fiziksel Adres)** bölümünü not alınız (Görsel 6.5).



Görsel 6.5: Bilgisayar MAC adresi

Araştırma

Evde kullandığınız bilgisayar, cep telefonu veya tabletin MAC adreslerini öğreniniz.

Uygulama 3

Anahtar MAC tablosu incelemek için gerekli işlemleri aşağıdaki yönergeler doğrultusunda gerçekleştiriniz.

Adım 1: Ağ simülasyon programında dört bilgisayar, bir anahtardan oluşan yeral ağ kurunuz.

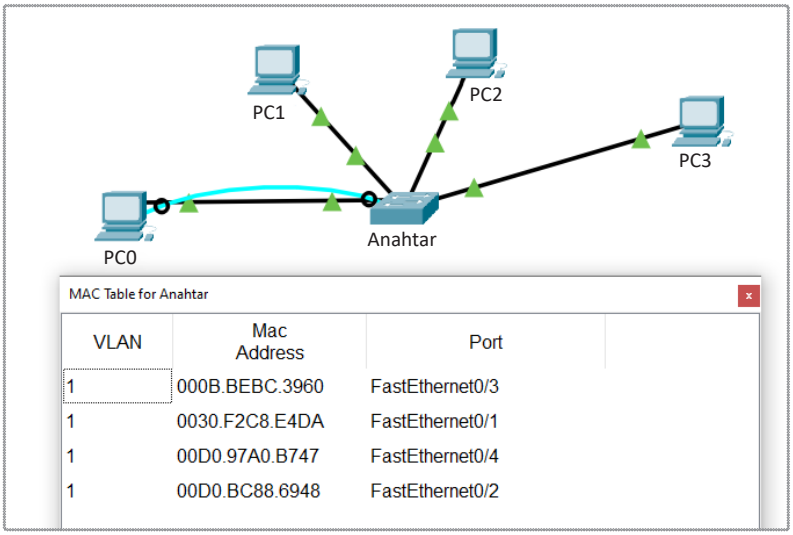
Adım 2: Bilgisayarlara el ile IP adreslerini ve alt ağ maskelerini tanımlayınız.

Adım 3: Bilgisayarlardan bir tanesinden diğer üç tanesine ping atınız.

Adım 4: Simülasyon programında inspect (inceleme) komutunu (büyüteç simgesi) tıklayınız ve anahtarın üzerine büyüteci getirerek tıklayınız.

Adım 5: Açılan menüden MAC Table (MAC Tablosunu) seçiniz.

Adım 6: Ekrana gelen tabloyu inceleyiniz (Görsel 6.6).



Görsel 6.6: Bir anahtarın MAC adres tablosu

Uygulama 4

Anahtar komut ekranından MAC tablosunu incelemek için gerekli işlemleri aşağıdaki yönergeler doğrultusunda gerçekleştiriniz.

Adım 1: Ağ simülasyon programında dört bilgisayar, bir anahtardan oluşan yeral ağ kurunuz.

Adım 2: PC0 numaralı bilgisayarı konsol kablosuyla anahtara bağlayınız.

Adım 3: Bilgisayarlara el ile IP adreslerini ve alt ağ maskelerini tanımlayınız.

Adım 4: Bilgisayarlardan bir tanesinden diğer üç tanesine ping atınız.

Adım 5: PC0 üzerinden terminal programı ile anahtara bağlanınız.

Adım 6: **Anahtar>enable** komutuyla ayrıcalıklı kullanıcı moduna geçiniz.

Adım 7: **Anahtar#show mac-address-table** komutuyla anahtarın MAC tablosunu görüntüleyiniz.

Araştırma

Hedef MAC adresi FF:FF:FF:FF:FF olursa anahtar cihazı nasıl davranır, araştırınız.

6.1.5. Anahtarların Kullanım Yerleri

Anahtarlar, birçok ağ uygulamasında karşımıza çıkar. Anahtarlar veri iletimini MAC adresi (fiziksel adres) üzerinden gerçekleştirdiği için donanım tabanlı bir filtreleme yöntemi kullanılır. Anahtarlar ile filtreleme yapmak çerçevelerdeki MAC adres bilgilerini kullandığı için hızlı bir yöntemdir.

Aynı ağa bağlanmaya çalışan kullanıcı sayısı arttıkça çakışma sayısı da artar. Bu artış ağ performansında tolere edilemeyen bir düşüklük oluşturur. Ağ performansının düşmesine engel olmak amacıyla dağıtıcı yerine anahtar kullanılır.

Anahtar kullanmanın en önemli amacı, ağı çarpışma alanlarına (collision domain) bölmektir. Böylece ağ ortamı daha verimli kullanılmış olur. Anahtar kullanarak ağdaki çarpışma alanı sayısını arttırılır ve verinin çarpışma ihtimali azaltılmış olur.

Sanal yerel ağ (VLAN), anahtara bağlı cihazları mantıksal olarak gruplayarak ve bu cihazlar aynı fiziksel anahtarı paylaşsalar bile bu gruplar arasındaki trafiği sınırlayarak güvenliği artırır.

Anahtarların genel olarak kullanım yerleri şunlardır:

- Yerel ağlar oluşturmak
- Güvenli sanal ağ oluşturmak
- Yerel ağın arayüzler ve cihazlar arasında güvenliğini sağlamak
- Paket anahtarlamalı farklı ağları birbirine bağlamak
- Bina ve iş yeri gibi birçok yerel ağın bulunduğu ortamda ağları tek merkezde toplayarak yönetmek.

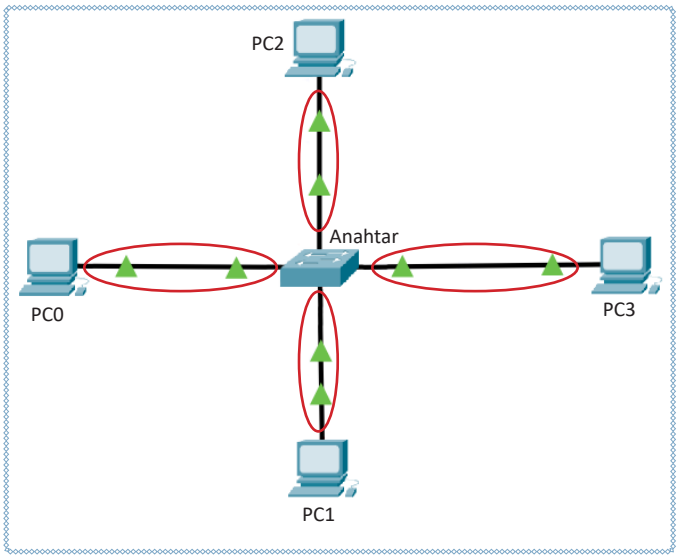
6.1.6. Broadcast ve Collision Domain

http://kitap.eba.gov.tr/KodSor.php?KOD=21041

Bazı veri paketlerinin ağda bulunan tüm cihazlara iletilmesi gerekebilir. Buna **genel yayın (boardcast)** denir. Ağ cihazlarının iletişimi esnasında bazı veri paketleri çarpışarak bozuk veri paketleri oluşturur. Buna da **çakışma-çarpışma (collision)** denir.

6.1.6.1. Collision Domain (Çakışma-Çarpışma Etki Alanı)

Çakışma-çarpışma etki alanı, ağ cihazlarının iletişimi esnasında veri paketlerinin çarpışmasının meydana gelebileceği ağın bir bölümüdür. Paylaşılan ağda, iki ağ cihazı aynı anda veri paketi gönderdiğinde bir çarpışma meydana gelir. Özellikle half-duplex (tek yönlü) iletişim yapan, veri gönderim yaparken veri alımı yapamayan cihazlarda meydana gelir. Anahtarların tüm arayüzleri birbirinden yalıtılarak iletişim sağlandığı için her bir arayüz ayrı çakışma alanıdır (Görsel 6.7).



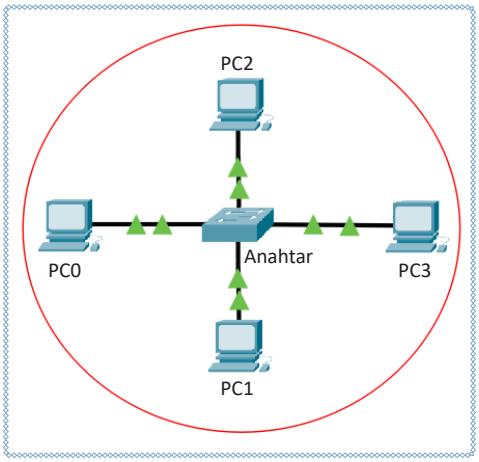
Görsel 6.7: Anahtar çakışma etki alanı

Dikkat

Çakışma-çarpışma etki alanı ne kadar çoksa çakışma-çarpışma ihtimali o kadar az olur.

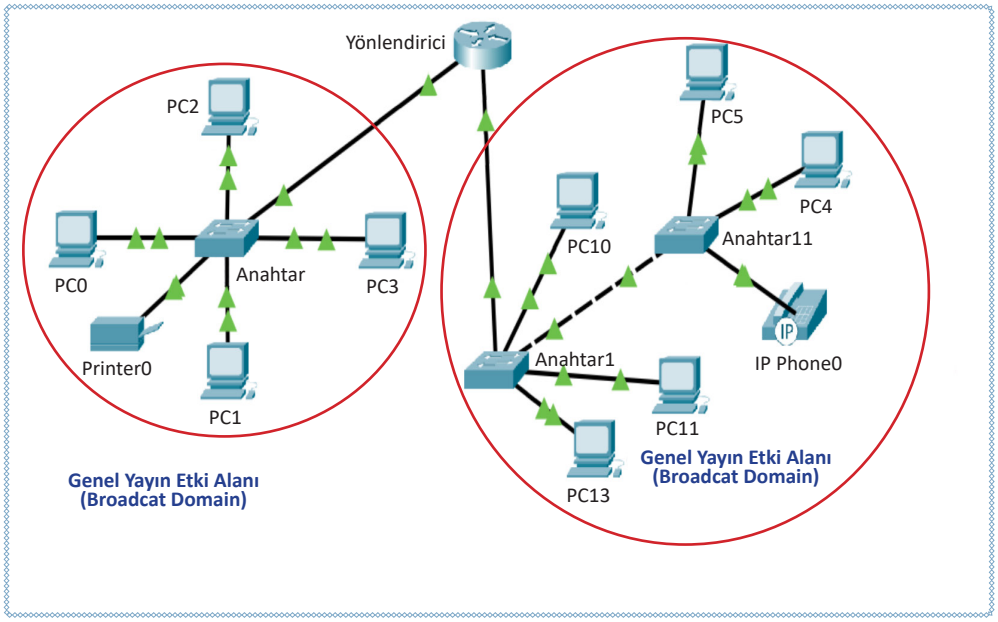
6.1.6.2. Broadcast Domain (Genel Yayın Etki Alanı)

Ağ üzerinde bir cihazın ağdaki tüm cihazlara veri paketi göndermesine **genel yayın (broadcast)** denir. Bir ağ cihazı başka bir ağ cihazının MAC adresini sormak istediğinde özel olarak bir broadcast (genel yayın) paketi oluşturur ve bunu ağ üzerindeki her kullanıcıya genel yayın adresi ile gönderir (Görsel 6.8).



Görsel 6.8: Broadcast domain

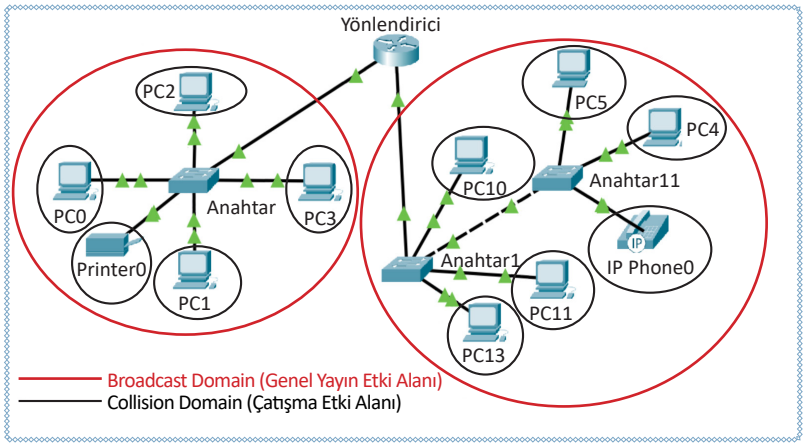
Görsel 6.8'deki basit ağ üzerinde, anahtara bağlı PC0 ortama broadcast (yayın) paket gönderirse anahtar bu paketi diğer tüm portlarına iletir. Anahtara bağlı tüm bilgisayarlar, aynı broadcast domain içindedir. Broadcast domainin sınırı yönlendiricidir. Görsel 6.9'da görüldüğü gibi bir yönlendiricinin her bir bacağı (interface) farklı bir broadcast domaindir (Görsel 6.10).



Görsel 6.9: Broadcast domain

Dikkat

Broadcast, tüm portlara yayın yapmak için kullanılan MAC adresi ise **FF:FF:FF:FF:FF:FF**'dir. Ağ katmanı düzeyinde de **255.255.255.255** IP adresi kullanılır.



Görsel 6.10: Broadcast ve collision domain

Dikkat

Birbirine bağlı anahtarlar tek bir genel yayın etki alanı oluşturur.

6.1.7. Anahtar Türleri

Anahtar, ağ içinde konuşlanacağı yere ve içerdiği teknolojiye göre yapılır. Ağ içinde konuşlanacağı yere göre merkez ve kenar anahtar olarak, kullanılan teknolojiye göre Ethernet ve ATM anahtar olarak sınıflanır.

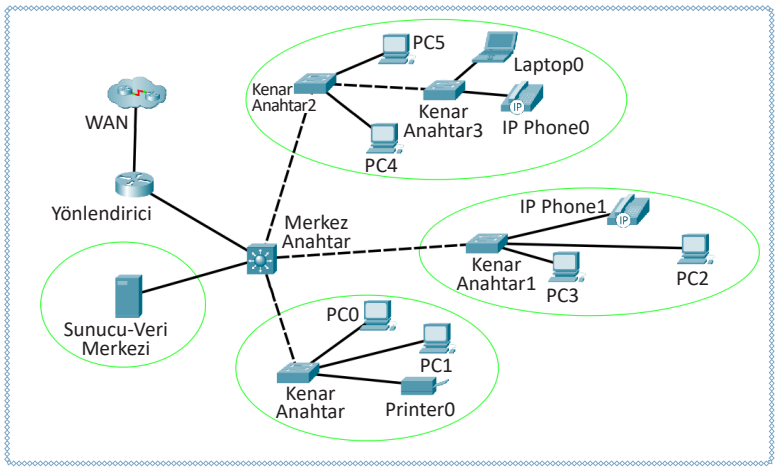
6.1.7.1. Omurga Anahtar (Backbone Switch)

Omurga anahtarlar, ağ sistemlerini oluşturan birçok anahtarın yükünün toplandığı veya ana yükün başladığı anahtardır. Anahtarlama kapasiteleri, veri iletim hızları yüksektir. Yapılandırmasına göre tüm ağın iletişimini toplar veya anahtarlar arasında iletişim yükünü paylaştırır. Büyük ağların merkezindedir. Diğer anahtarlar, omurga anahtar üzerinden iletişime geçer. Genellikle omurga anahtara son nokta ağ cihazları direkt bağlanmaz (Görsel 6.11).

Görsel 6.11: Omurga anahtarlar

6.1.7.2. Merkez Anahtar (Core Switch)

Merkez anahtar, hiyerarşik yapıda oluşan ağın merkezinde bulunur (Görsel 6.12). Merkez anahtarların performansı, ağın tüm performansını etkileyebileceğinden kenar anahtarlara göre daha güçlü işlemciye, yüksek kapasiteli ve hızlı belleğe, yüksek hızlı portlara ve büyük boyutlu MAC tablosuna sahip olmalıdır (Görsel 6.13). Merkez anahtarlarda, kendisine doğrudan bağlı olsun olmasın, ağdaki tüm sistemlerin MAC adresleri tutulur. Bu sayede kendisi üzerinden geçecek çerçevelerin nereye anahtarlanacağını belirleyebilir.



Görsel 6.12: Hiyerarşik bir ağ uygulaması

Görsel 6.13: Merkez (Core) anahtar

6.1.7.3. Kenar Anahtarlar (Edge Switches)

Kenar anahtarlar, genellikle hub, bilgisayar ve yazıcı gibi ağ cihazlarının doğrudan bağlantılarının yapıldığı anahtarlardır (Görsel 6.14). Kenar anahtarlar, kendine bağlı sistemlerin gereksinim duyduğu anahtarlama ihtiyacını karşılayacak ölçüde kapasiteye sahip olur. Anahtarlama gücü ve MAC tablosu boyutu sınırlıdır. Ağın sınırlı bir bölümüne ait cihazları toplayıp merkez anahtara bağlar. Kenar anahtar tüm ağdan sorumlu olmadığı için kendi altındaki bağlantıların kontrolünü yapması yeterlidir.

Görsel 6.14: Kenar anahtar

6.1.7.4 ATM Anahtarlar

Eş zamansız aktarım modu (Asynchronous Transfer Mode=ATM), verileri 53 byte sabit büyüklükte hücreler hâlinde anahtarlayarak ileten bir ağ tekniğidir. Hücrelere isim vererek taşır. Bağlantı temelli bir teknolojidir. ATM hücrelerinin ATM anahtarlar arasında aktarılması çok hızlıdır. ATM yüksek performanslı çoklu ortam ağları için tasarlanmıştır. Bu anahtarların yerel ağlarda kullanımı kısıtlı kalmış, günümüzde daha çok iletişim ve bilgisayar ağları arasında hızlı omurga (backbone) yapıları oluşturmak için kullanılmıştır.

6.1.7.5. Ethernet Anahtarlar

Ethernet anahtarlar kendi içinde ikiye ayrılır.

Yönetilemez Ethernet Anahtarlar: Basit ağ uygulamalarında kullanılır. Herhangi bir konfigürasyon ayarına izin vermez. Bu anahtarların ayrıca bir kuruluma ihtiyaçları yoktur. Tak çalıştır özelliğine sahip oldukları için amatör kullanıcılar dahi ağ uygulamalarında kullanabilir. Örneğin evlerde kullanılan anahtarlar, yönetilemez Ethernet anahtarlardır.

Yönetilebilir Ethernet Anahtarlar: Ağ uygulamasının yönetilmesi, trafiğinin izlenmesi, portların kontrol edilmesi gereken yerlerde kullanılır. Karmaşık yapıya sahip ve pahalı cihazlardır. Konfigürasyonu yapılmazsa yönetilemez, Ethernet anahtarlar gibi davranır. Yapılandırılarak ağın kontrolü sağlanır.

6.2. Komut Arayüzü Kullanarak Temel Anahtar Yapılandırması

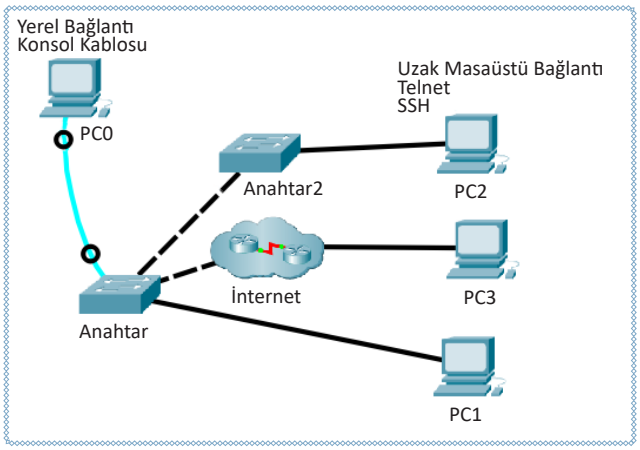
Ağın yönetilmesi amacıyla sistemde kullanılan bazı anahtarların ayarlarının yapılandırılmasına ihtiyaç vardır. Birçok anahtarın yapılandırması komut arayüzü üzerinden gerçekleştirilebilir.

6.2.1. Anahtar İşletim Sistemi

Yönetilebilir anahtarlarda yönlendiricilere benzer CLI komut satırı kullanılmaktadır. Yeni nesil çoklu katman anahtarlar, 3. katman mantıksal adres yönlendirmesi yaptığı için bu ürünlerde daha kapsamlı işletim sistemi bulunmaktadır. Özel durumlar haricînde yönetilebilir anahtar, fabrika çıkış ayarları ile standart bir anahtar olarak çalışır. Ağın yönetimi için gerekli ayarlar, kullanılacağı ağın genel yapısına göre yapılandırılmalıdır.

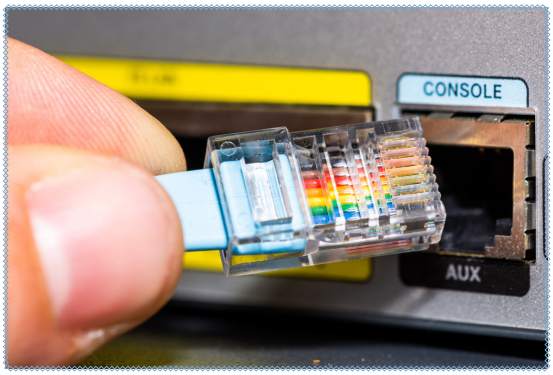
Anahtarın kontrol ve yapılandırma işlemleri için bilgisayar ile anahtar arasında bağlantı kurulmalıdır (Görsel 6.15). Anahtar ile bilgisayar arasında aşağıdaki bağlanma yöntemleri vardır:

- Konsol portu ile bağlanma
- Telnet ile bağlanma
- SSH ile bağlanma



Görsel 6.15: Anahtara bağlanma yöntemleri

Anahtarın ilk yapılandırma işlemi için mutlaka konsol portu (console) üzerinden bağlanması gerekir. Konsol bağlantısı yapıldığında Telnet veya SSH bağlantısıyla uzaktan erişimin sağlanması için gerekli konfigürasyon yapılandırılabilir. Konsol portuna genelde RJ-45 bağlantısıyla roll-over olarak hazırlanmış konsol kablosu ile bağlanılır (Görsel 6.16).



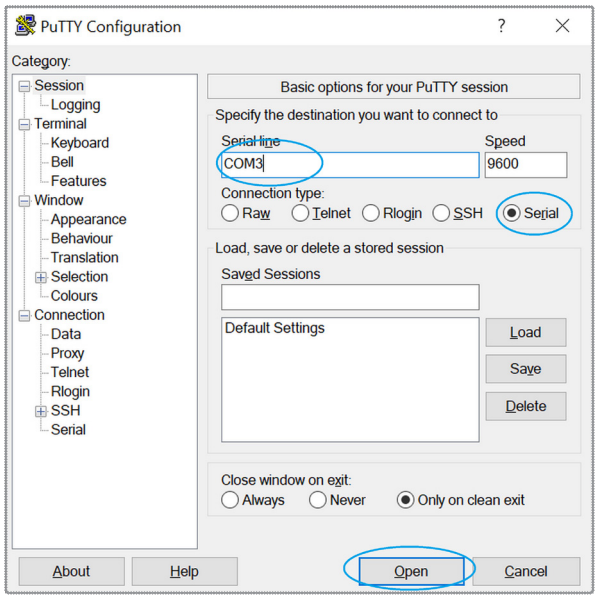
Görsel 6.16: Konsol portu kablo bağlantısı

Uygulama 5

Anahtarın yapılandırma bağlantısını yapmak için aşağıdaki yönergeleri uygulayınız.

Adım 1: Anahtarın konsol (console) portuna konsol kablosunun RJ-45 konnektör ucunu bağlayınız.

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



Görsel 6.17: Putty programı

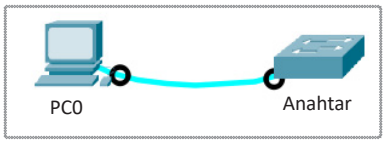
Adım 3: Bilgisayar üzerinde Putty programını açınız (Görsel 6.17).

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

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

Uygulama 6

Simülasyon progamında anahtarın konsol kablosuyla bağlantısı ve yapılandırma ekranı açmak için gerekli işlemleri aşağıdaki yönergeler doğrultusunda gerçekleştiriniz.



Görsel 6.18: Anahtarın konsol kablosu ile bağlantısı

Adım 1: Simülasyon programını açınız.

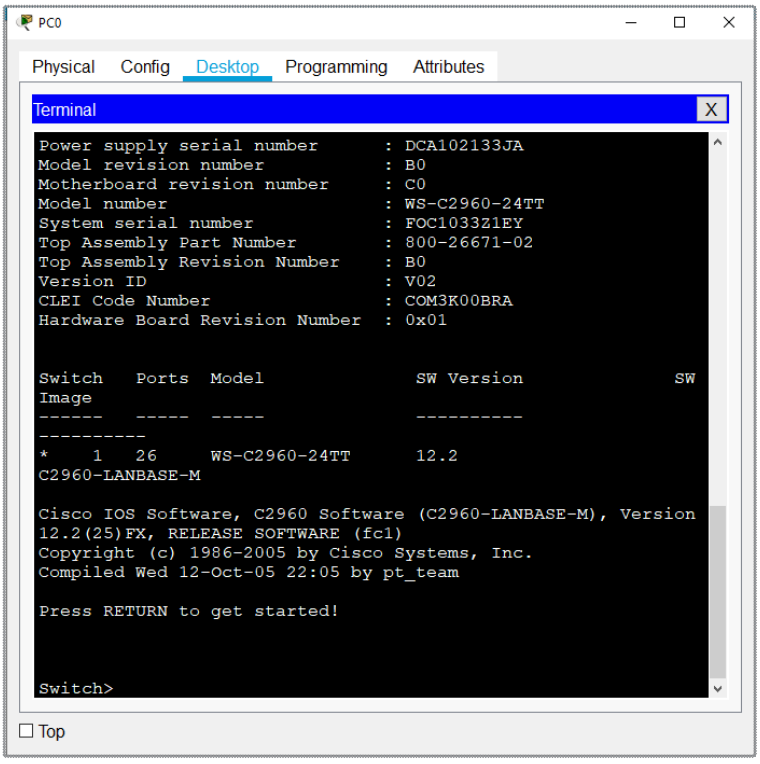
Adım 2: Simülasyon ortamına bir anahtar ve bilgisayar ekleyiniz (Görsel 6.18).

Adım 3: Kablo türü olarak konsol kablosunu seçiniz.

Adım 4: Bilgisayarın **RS232** ve anahtarın **console** portunu seçerek bağlantıyı oluşturunuz.

Adım 5: Bilgisayara tıklayıp açılan ekrandan **terminal programını** tıklayınız.

Adım 6: Karşınıza gelen ekrandan **OK** seçeneğine tıklayınız ve komut arabirimini açınız (Görsel 6.19).



Görsel 6.19: Anahtar komut arabirim ekranı

Komut arabirimi hiyerarşik yapıdadır. Yapılandırma işlemlerinin gerçekleştirileceği farklı modları vardır. Her modda yürütülebilecek komutlar ve yapılabilecek işlemler farklıdır. Dolayısıyla yapılandırma işlemleri gerçekleştirilirken 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 6.3).

Tablo 6.3: Komut Modu Görünümü ve İşlevi

Komut Modu Görünümü	İşlevi	
Switch>	Kullanıcı Modu	***user/EXEC Mode***
Switch#	Ayrıcalıklı Kullanıcı Modu	***Privileged EXEC Mode***
Switch(config)#	Global Konfigürasyon Modu	***Global Configuration Mode***
Switch(config-if)#	Arayüz Konfigürasyon Modu	***Interface Configuration Mode***

Uygulama 7

Anahtarın kullanıcı modu arabirimini ve komutlarını görüntülemek için gerekli işlemleri aşağıdaki yönergeler doğrultusunda gerçekleştiriniz.

Adım 1: Simülasyon programını açarak bir bilgisayar ve anahtarı konsol kablosu ile bağlayınız.

Adım 2: Bilgisayarı ve açılan ekrandan terminal programını tıklayınız.

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

Adım 4: "***switch>***" komut satırını görünüz.

Adım 5: " ***?*** " karakterini yazıp "Enter" tuşuna basınız ve karşınıza gelen ekrandan kullanıcı (user/EXEC) modunda kullanılabilecek komutları inceleyiniz.

Uygulama 8

Ayrıcalıklı kullanıcı modunu ve komutlarını görüntüleme işlemini aşağıdaki yönergeler doğrultusunda gerçekleştiriniz.

Bu moda geçiş yapmak için kullanıcı modundayken "***enable***" komutu kullanılır. İlk kullanım haricînde geçiş yaparken şifre oluşturulduysa güvenlik açısından sorgulaması yapılır. Ayrıcalıklı kullanıcı modunda anahtar adından sonra "***#***" karakteri görülür. Kullanıcı moduna geri dönmek için "***disable***" komutu kullanılır.

Adım 1: Simülasyon programını açınız ve bir bilgisayar ve anahtarı konsol kablosu ile bağlayınız.

Adım 2: Bilgisayarı tıklayınız ve açılan ekrandan terminal programını tıklayarak komut arabirimini açınız.

Adım 3: "***switch>***" komut satırını görünüz.

Adım 4: "***enable***" ya da "***en***" komutunu yazıp "Enter" tuşuna basınız. Ekranda ***Switch#*** görülür.

Adım 5: " ***?*** " karakteri yazıp "Enter" tuşuna basınız ve karşınıza gelen ekrandan ayrıcalıklı kullanıcı (Privileged/EXEC) modunda kullanılabilecek komutları inceleyiniz.

Uygulama 9

Anahtarın global konfigürasyon modu arabirimini ve komutlarını görüntüleme işlemini aşağıdaki yönergeler doğrultusunda gerçekleştiriniz

Bu moda geçiş yapmak için ayrıcalıklı kullanıcı modunda "**configure**" komutu "**terminal**" parametresiyle çalıştırılır. Bu moda geçiş yapılan anahtarın isminin arkasında "**(config)**" şeklinde yazı belirir. Bu moddan çıkış için "**exit**" veya "**end**" kullanılır (Görsel 6.20).

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

Görsel 6.20: Global konfigürasyon modu

Adım 1: Simülasyon programını açınız ve bir bilgisayar ve anahtarı konsol kablosu ile bağlayınız.

Adım 2: Bilgisayarı tıklayınız ve açılan ekrandan terminal programını tıklayarak komut arabirimini açınız.

Adım 3: "***switch>***" komut satırını görünüz.

Adım 4: "***enable***" komutunu yazıp "Enter" tuşuna basınız. Ekranda ***Switch#*** görülür.

Adım 5: "***configure terminal***" ya da "***conf t***" komutunu giriniz. Ekranda "***Switch(config)***" görülür.

Adım 6: " ***?*** " karakteri yazıp "Enter" tuşuna basınız ve karşınıza gelen ekrandan global konfigürasyon (Global Configuration Mode) modunda kullanılabilecek komutları inceleyiniz.

Uygulama 10

Anahtarın Arayüz konfigürasyon modu arabirimini ve komutlarını görüntülemek için gerekli işlemleri aşağıdaki yönergeler doğrultusunda gerçekleştiriniz (Görsel 6.21).

Özel olarak belirli bir portun konfigürasyonu için kullanılır. Bu moda geçiş yapmak için global konfigürasyon modundayken "***interface***" komutundan sonra ilgili portun adı yazılır.

Adım 1: Simülasyon programını açınız ve bir bilgisayar ve anahtarı konsol kablosu ile bağlayınız.

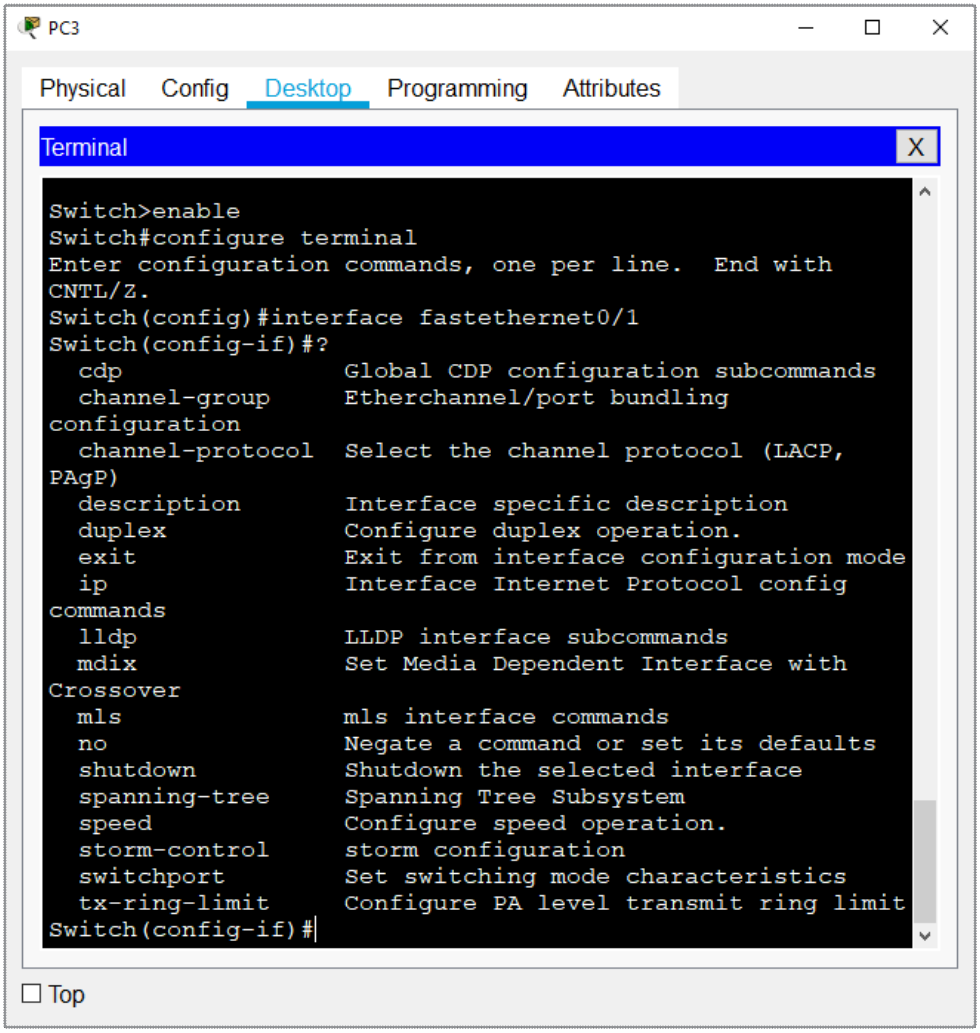
Adım 2: Bilgisayarı tıklayınız ve açılan ekrandan terminal programını tıklayarak komut arabirimini açınız.

Adım 3: "***switch>***" komut satırını görünüz.

Adım 4: "***enable***" komutunu yazıp "Enter" tuşuna basınız.

Adım 5: "***configure terminal***" ya da "***conf t***" komutunu giriniz.

Adım 6: ***İnterface fastethernet 0/1***



Görsel 6.21: Arayüz konfigürasyon modu

Adım 7: "**?**" karakteri yazıp "Enter" tuşuna basınız ve karşınıza gelen ekrandan arayüz konfigürasyon (Interface Configuration) modunda kullanılabilecek komutları inceleyiniz.

6.2.2. Anahtar Arayüz Yapılandırma

Anahtar arayüzleri yapılandırılırken öncelikle anahtarlar isimlendirilmeli, güvenlik için şifreleme işlemleri yapılmalı, uzaktan erişim için gerekli ayarlar yapılandırılmalıdır.

Uygulama 11

http://kitap.eba.gov.tr/KodSor.php?KOD=21042

Anahtarlara isim verme işlemini aşağıdaki yönergeler doğrultusunda gerçekleştiriniz.

Anahtara isim vermek için global konfigürasyon modunda **hostname** komutu kullanılır.

Adım 1: Simülasyon programını açınız ve bir bilgisayar ve anahtarı konsol kablosu ile bağlayınız.

Adım 2: Bilgisayarı tıklayınız ve açılan ekrandan terminal programını tıklayıp komut arabirimini açınız.

Adım 3: Global Konfigürasyon Moduna geçiniz.

Adım 4: ***hostname Mevlana*** komutunu giriniz.

Adım 5: Anahtarın isminin değiştiğini gözlemleyiniz (Görsel 6.22).

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

Görsel 6.22: Anahtara isim verme

Uygulama 12

http://kitap.eba.gov.tr/KodSor.php?KOD=21043

Anahtarlara erişim parolası verme işlemini aşağıdaki yönergeler doğrultusunda gerçekleştiriniz.

Anahtar yapılandırmasına yetkisiz kişilerin erişiminin engellemesi ve ayrıcalıklı kullanıcı modu için parola belirlenerek güvenlik sağlanmalıdır. Parola işlemleri global konfigürasyon modunda ayarlanır.

Adım 1: Simülasyon programını açınız ve bir bilgisayar ve anahtarı konsol kablosu ile bağlayınız.

Adım 2: Bilgisayarı tıklayınız ve açılan ekrandan terminal programını tıklayıp komut arabirimini açınız.

Adım 3: Global Konfigürasyon Moduna geçiniz.

Adım 4: "***enable password MEB_1071***" komutunu giriniz.

Adım 5: ***exit*** komutu ile global konfigürasyon modundan çıkınız.

Adım 6: ***exit*** komutu ile ayrıcalıklı kullanıcı modundan çıkınız.

Adım 7: Anahtara tekrar giriş yaparak şifreyi kontrol ediniz.

Adım 8: Global konfigürasyon moduna geçiniz.

Adım 9: "***enable secret MEB_1453***"

Adım 10: ***exit*** komutu ile global konfigürasyon modundan çıkınız.

Adım 11: ***exit*** komutu ile ayrıcalıklı kullanıcı modundan çıkınız.

Adım 12: Anahtara tekrar giriş yaparak şifreyi kontrol ediniz.

Adım 13: ***show running-config*** komutu ile çalışan ayarları gözlemleyiniz.

Dikkat

password parametresiyle verilen şifre çalışan ayarlara bakıldığı zaman kriptolanmadığı için açıkça görülür. Bu durumu engellemek için **service password-encryption** komutu kullanılır.

Sıra Sizde

Anahtara "***Ankara_1920***" parolasını veriniz ve parolayı kriptolayarak gizleyiniz.

Araştırma

Anahtara password ve secret parametrelerinin her ikisiyle de şifre atanırsa anahtar hangi şifreyi kullanırız? Nedenini araştırınız.

Uygulama 13

http://kitap.eba.gov.tr/KodSor.php?KOD=21044

Anahtarlara karşılama mesajı ekleme işlemini aşağıdaki yönergeler doğrultusunda gerçekleştiriniz.

Anahtarın konsol ekranına giriş yapıldığında bir karşılama mesajı veya açıklama bilgisi eklemek için "***banner motd x.....x***" komutu kullanılır (Görsel 6.23).

Dikkat

Karşılama mesajı oluştururken girilen "**x**" işaretleri, metnin başlangıç ve bitişini temsil eder. Bunlar karşılama mesajında görünmez. İstenirse başka bir karakter de kullanılabilir (Türkçe karakter desteği bulunmamaktadır.).

```
Mevlana>en
Password:
Mevlana#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Mevlana(config)#banner motd xMilli Egitim Bakanligi-Yetkisiz Giris
Yasaktir!x
Mevlana(config)#
```

Görsel 6.23: Karşılama mesajı

Adım 1: Simülasyon programını açınız ve bir bilgisayar ve anahtarı konsol kablosu ile bağlayınız.

Adım 2: Bilgisayarı tıklayınız ve açılan ekrandan terminal programını tıklayıp komut arabirimini açınız.

Adım 3: Global konfigürasyon moduna geçiniz.

Adım 4: ***banner motd xMilli Eğitim Bakanligi-Yetkisiz Giris Yasaktirx*** komutunu giriniz.

Adım 5: ***exit*** komutu ile global konfigürasyon modundan çıkınız.

Adım 6: ***exit*** komutu ile ayrıcalıklı kullanıcı modundan çıkınız.

Adım 7: Anahtara tekrar giriş yaparak şifreyi kontrol ediniz.

Adım 8: Anahtar komut satırını çalıştırınız ve karşılama mesajını görüntüleyiniz.

Uygulama 14

Anahtarlarda çalışan yapılandırmayı incelemek ve hata tespiti için ***show*** komutu kullanılır. **show** komutu ile incelenebilecek bölümleri görmek için komut satırına yazılan "?" işareti komut verildiğinde kullanılabilecek parametreleri gösterir. Uygulamayı aşağıdaki yönergeler doğrultusunda gerçekleştiriniz.

Dikkat

Komut satırında komutlar, **TAB** tuşuna basıldığında tamamlanır. Ayrıcalıklı kullanıcı modunda çalışan **show** gibi komutlar, global konfigürasyon modunda çalıştırılmak istenirse başlarına "**do**" eklenerek "**do show running-config**" şeklinde çalıştırılabilir.

Adım 1: Simülasyon programını açınız ve bir bilgisayar ve anahtarı konsol kablosu ile bağlayınız.

Adım 2: Ayrıcalıklı kullanıcı moduna geçiniz.

Adım 3: show version komutu ile çalışan işletim sistemi versiyonunu inceleyiniz.

Adım 4: show running-config komutu ile çalışan yapılandırma ayarlarını inceleyiniz.

Adım 5: show interface komutu ile arayüzleri inceleyiniz.

Adım 6: show ip interface brief komutu ile arayüz detaylarını inceleyiniz.

Adım 7: show mac-address-table komutu ile MAC tablosunu inceleyiniz.

Adım 8: show flash: komutu ile flash hafızadaki dosyaları görüntüleyiniz.

Sıra Sizde

Diğer görüntülüme komutlarını bir arkadaşınız ile birlikte deneyerek inceleyiniz ve ortak bir sunum hazırlayınız.

Uygulama 15

Anahtar arayüzlerine geçiş işlemini aşağıdaki yönergeler doğrultusunda gerçekleştiriniz.

Anahtar arayüzlerini (portlarını) yapılandırmak için global konfigürasyon modunda **interface** komutu kullanılır. Arayüz yapılandırmasına geçerken hangi arayüzde işlem yapılacağına dikkat edilmelidir (Görsel 6.24).

```
Milli Eitim Bakanligi

Anahtar>en
Anahtar#conf t
Enter configuration commands, one per line.  End with
CNTL/Z.
Anahtar(config)#in
Anahtar(config)#interface ?
  Ethernet          IEEE 802.3
  FastEthernet      FastEthernet IEEE 802.3
  GigabitEthernet   GigabitEthernet IEEE 802.3z
  Port-channel      Ethernet Channel of interfaces
  Vlan              Catalyst Vlans
  range             interface range command
Anahtar(config)#interface
```

Görsel 6.24: Arayüz (interface) çeşitleri

Anahtarın hangi arayüzünde işlem yapılacaksa global konfigürasyon modunda **interface** komutundan sonra o arayüzün adı ve anahtar üzerindeki port numarası yazılır.

Adım 1: Simülasyon programını açınız ve bir bilgisayar ve anahtarı konsol kablosu ile bağlayınız.

Adım 2: Global konfigürasyon moduna geçiniz.

Adım 3: interface fastethernet 0/1 komutu ile FastEthernet 0/1 arayüzüne geçiniz.

Adım 4: exit komutu ile çıkınız.

Adım 5: interface gigabitethernet 0/1 komutu ile gigabitEthernet 0/1 arayüzüne geçiniz.

Adım 6: exit komutu ile çıkınız.

Adım 7: interface vlan1 komutu ile vlan1 arayüzüne geçiniz.

Adım 8: exit komutu ile çıkınız.

Adım 9: interface ethernet 0/1 komutu ile Ethernet 0/1 arayüzüne geçiniz.

Adım 10: exit komutu ile çıkınız.

Dikkat

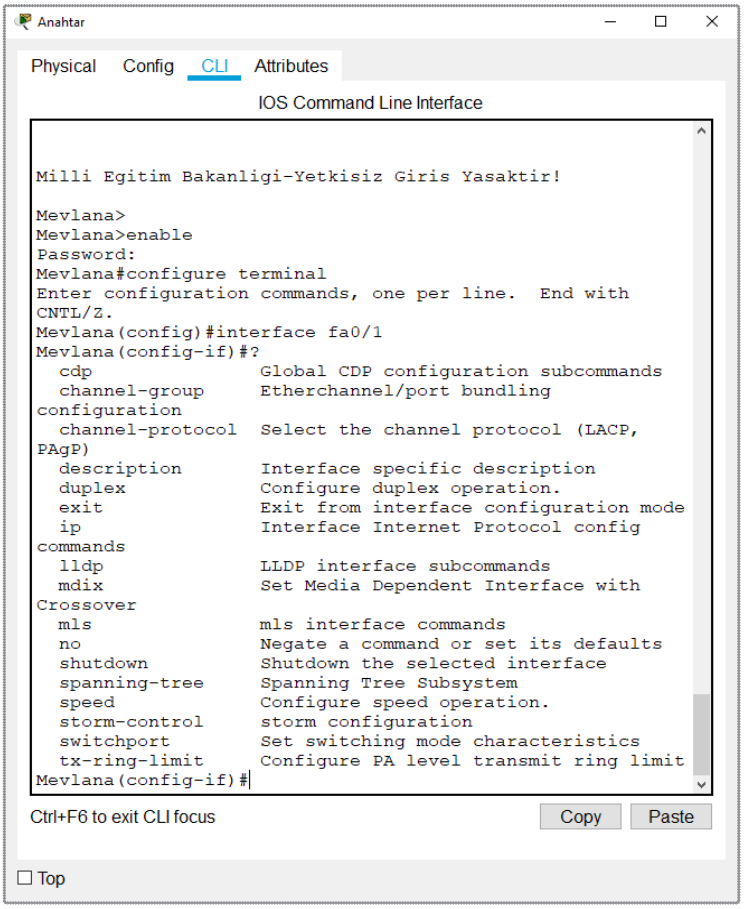
Anahtar üzerinde bulunmayan arayüzlere geçiş yapılmak istenildiğinde hata mesajı alınır.

Adım 11: "**interface range fastEthernet 0/1-5**" komutu ile 1'den 5'inci porta kadar olan arayüzlerine geçiş yapınız, ayarlarını sağlayınız.

Adım 12: interface range fastEthernet 0/1, fastEthernet 0/5, fastEthernet 0/7 komutu ile 1, 5 ve 7 numaralı portların arayüzüne geçiş yapınız.

Adım 13: Anahtar(config)# interface FastEthernet 0/1 komutunu çalıştırınız.

Adım 14: Anahtar(config-if)# ? komutu arayüz içindeyken uygulanabilecek komutları inceleyiniz (Görsel 6.25).



Görsel 6.25: Arayüz komutları

Uygulama 16

Anahtarlarda arayüzleri yapılandırmak için gerekli işlemleri aşağıdaki yönergeler doğrultusunda gerçekleştiriniz.

Adım 1: Simülasyon programını açınız ve üç bilgisayar ve bir anahtardan oluşan bir ağ oluşturunuz.

Adım 2: Bilgisayarlardan bir tanesini konsol kablosu ile anahtara bağlayınız.

Adım 3: Global konfigürasyon moduna geçiniz.

Adım 4: ***Anahtar(config)#interface vlan 10*** vlan 10 arayüzünü oluşturunuz.

Adım 5: ***Anahtar(config-if)#no shutdown*** komutu ile vlan 10 arayüzünü aktifleştiriniz.

Adım 6: ***Anahtar(config)#interface fa0/1*** komutu ile 1 No.lu arayüze geçiş yapınız.

Adım 7: ***Anahtar(config-if)#shutdown*** komutu ile arayüzü kapatınız ve simülasyon programında arayüzün kapandığını gözlemleyiniz.

Adım 8: ***Anahtar(config-if)#no shutdown*** komutu ile kapattığınız arayüzü tekrar açınız.

Adım 9: ***Anahtar(config-if)#switchport access vlan 10*** komutuyla uygulayarak arayüzü vlan 10 atayınız.

Adım 10: ***Anahtar(config-if)#description Sunucu Portu -> meb.gov.tr*** komutunu uygulayarak 1 numaralı arayüze açıklama ekleyiniz.

Adım 11: ***Anahtar (config-if)#end***

Adım 12: ***Anahtar# show running-config*** komutunu uygulayarak yapılandırmayı inceleyiniz (Görsel 6.26).

```
Anahtar#conf t
Enter configuration commands, one per line.  End with
CNTL/Z.
Anahtar(config)#interface vlan 10
Anahtar(config-if)#no shutdown
Anahtar(config-if)#exit
Anahtar(config)#interface fa0/1
Anahtar(config-if)#shutdown

Anahtar(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state
to administratively down

%LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/1, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan10,
changed state to down

Anahtar(config-if)#no shutdown

Anahtar(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state
to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan10,
changed state to up

Anahtar(config-if)#switchport access vlan 10
Anahtar(config-if)#description Sunucu Portu -> meb.gov.tr
Anahtar(config-if)#end
```

Görsel 6.26: Arayüz yapılandırma

Sıra Sizde

Simülasyon programında bir anahtar ile beş bilgisayardan oluşan bir ağ kurunuz. Anahtarınızın 1 ve 2 numaralı arayüzlerine "**Laboratuvar**", 3 numaralı arayüzüne "**Ogretmenler Odasi**", 5 numaralı arayüzüne "**İnternet**" açıklamalarını ekleyiniz. 4 numaralı arayüzünü "**vlan 20**"ye atayınız. 2 numaralı arayüzünü kapatınız.

6.2.3. Uzak Masaüstü Yapılandırma

Anahtara uzaktan erişim için IP yapılandırma işleminin yapılması gerekir. Öncelikle varsayılan olarak pasif olan VLAN1'in aktif hâle getirilmesi gerekir.

Uygulama 17

Anahtara IP adresi atamak için gerekli işlemleri aşağıdaki yönergeler doğrultusunda gerçekleştiriniz.

Adım 1: Simülasyon programını açınız ve üç bilgisayar ve bir anahtardan oluşan bir ağ oluşturunuz.

Adım 2: Bilgisayarlardan bir tanesini konsol kablosu ile anahtara bağlayınız.

Adım 3: Global konfigürasyon moduna geçiniz.

Adım 4: *Anahtar(config)#interface vlan 1* komutu ile VLAN 1 arayüzüne geçiş yapınız.

Adım 5: *Anahtar(config-if)#ip address 192.168.1.253 255.255.255.0* vlan 1'de kullanılacak IP adresi ve alt ağ maskesini atayınız.

Adım 6: *Anahtar(config-if)#no shutdown* komutu ile arayüzü açık (aktif) hâle getiriniz.

Adım 7: *Anahtar(config-if)#ip default-gateway 192.168.1.1* komutu ile uzaktan erişim için ağın varsayılan ağ geçidi adresini tanımlayınız.

Adım 8: *Anahtar(config-if)#do wr* komutuyla ayarlarınızı kaydediniz.

Adım 9: Çalışan ayarları görünteleyerek yapılandırmanızı kontrol ediniz.

Adım 10: Simülasyon programındaki çalışmanızı kaydediniz (Görsel 6.27).

```
Anahtar#
Anahtar#conf t
Enter configuration commands, one per line.  End with
CNTL/Z.
Anahtar(config)#interface vlan 1
Anahtar(config-if)#ip address 192.168.1.253 255.255.255.0
Anahtar(config-if)#no shutdown

Anahtar(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1,
changed state to up

Anahtar(config-if)#ip default-gateway 192.168.1.1
Anahtar(config)#do wr
Building configuration...
[OK]
Anahtar(config)#
```

Görsel 6.27: Anahtara IP adresi atama

6.2.4. Telnet, SSH ve Console Yapılandırma

Bilgisayarın yapılandırması amacıyla sağlanan Telnet, SSH ve Console bağlantılarının güvenlik açısından yapılandırılması gerekmektedir.

6.2.4.1. Console (Konsol) Yapılandırma

Konsol portu kullanılarak ağdaki cihazlara konsol kablosu ile erişim sağlanabilir. İlk yapılandırma işlemleri konsol kablosu ile yapılır ve konsol erişimi varsayılan olarak şifresizdir.

Uygulama 18

http://kitap.eba.gov.tr/KodSor.php?KOD=21045

Console (Konsol) yapılandırmak için gerekli işlemleri aşağıdaki yönergeler doğrultusunda gerçekleştiriniz.

Adım 1: Simülasyon programını açınız ve iki bilgisayar ve bir anahtardan oluşan ağ oluşturunuz.

Adım 2: Konsol bağlantısı ile anahtara bağlanıp global konfigürasyon moduna geçiniz.

Adım 3: *Anahtar(config)#line console 0* komutu ile konsol arayüzü yapılandırmaya geçiniz.

Adım 4: *Anahtar(config-line)#password meb_1920* komutu ile konsol arayüzüne erişim şifresi ekleyiniz.

Adım 5: *Anahtar(config-line)#login* komutu ile aktif hâle getiriniz.

Adım 6: *Anahtar(config-line)#exit* komutu ile konsol arayüzünden çıkınız.

Adım 7: *Anahtar(config)#exit* komutu ile global konfigürasyon modundan çıkınız (Görsel 6.28).

Adım 8: *Anahtar#show running-config* komutu ile çalışan ayarları görünteleyerek yapılandırmanızı kontrol ediniz.

Adım 9: Anahtarın yapılandırma arayüzünden çıkarak tekrar konsol üzerinden bağlantı sağlayınız ve şifre ile giriş yapınız.

```
Anahtar#conf t
Enter configuration commands, one per line.  End with
CNTL/Z.
Anahtar(config)#line console 0
Anahtar(config-line)#password meb_1920
Anahtar(config-line)#login
Anahtar(config-line)#exit
Anahtar(config)#
```

Görsel 6.28: Console yapılandırma

6.2.4.2. Telnet Yapılandırma

Telnet'in açılımı, **Telecommunication Network-İletişim Ağı**'dır. TCP/IP protokolünü kullanan sanal bir terminal protokolüdür. Uzaktaki hostlara bağlantı yapmak için kullanılır. Telnet sunucularının ağ terminallerine uzaktan erişim yapabilme yetenekleri vardır.

Dikkat

Telnet iletişiminde veriler şifrelenmez. Bundan dolayı güvensiz bir protokoldür.

Anahtarlar, telnet oturumlarını çoklu olarak aynı anda gerçekleştirebilir. Telnet hattı oluşturulurken belirlenen kadar VTY (Veri Transfer Yolu) ya da telnet hattı kullanılır. Belirlenen sayıda oturumu aynı zamanda alabilir.

Uygulama 19

http://kitap.eba.gov.tr/KodSor.php?KOD=21046

Telnet yapılandırmak ve telnet üzerinden anahtara bağlanmak için gerekli işlemleri aşağıdaki yönergeler doğrultusunda gerçekleştiriniz (Görsel 6.29).

Adım 1: Uzak masaüstü yapılandırmasında yaptığınız uygulamayı açınız.

Adım 2: Konsol bağlantısı ile anahtara bağlanıp global konfigürasyon moduna geçiniz.

Adım 3: ***Anahtar(config)#line vty 0 3*** komutu ile anahtara aynı anda bağlanabilecek kullanıcı sayısı belirleyiniz.

Adım 4: ***Anahtar(config-line)#password malazgirt*** komutu ile telnet erişim şifresini oluşturunuz.

Adım 5: ***Anahtar(config-line)#login*** komutu ile telnet erişimini açık hâle getiriniz.

Adım 6: ***Anahtar(config-line)#exit*** komutu ile çıkınız.

```
Anahtar(config)#line vty 0 3
Anahtar(config-line)#password malazgirt
Anahtar(config-line)#login
Anahtar(config-line)#exit
Anahtar(config)#
```

Görsel 6.29: Telnet erişiminin yapılandırılması

Adım 7: Simülasyondaki diğer bilgisayar üzerinden **telnet/ssh** programını açınız.

Adım 8: Bağlantı tipi olarak Telnet seçiniz.

Adım 9: IP adresi olarak bir önceki uygulamada anahtarın VLAN arayüzüne atadığınız IP adresini giriniz.

Adım 10: Açılan ekranda telnet bağlantısı için oluşturduğunuz şifreyi giriniz.

Adım 11: Telnet bağlantısını kapatmadan başka bir bilgisayardan aynı şekilde bağlantı yapmayı deneyiniz.

Adım 12: Üçüncü bir bilgisayar üzerinden komut satırını açınız ve ekrana "**telnet anahtarın-ip-adresi**" yazarak "Enter" tuşuna basınız.

Adım 13: Telnet için oluşturduğunuz şifreyi girerek bağlantıyı sağlayınız.

```
C:\>telnet 192.168.1.253
Trying 192.168.1.253 ...Open


User Access Verification

Password:
Anahtar>
```

Görsel 6.30: Bilgisayara komut isteminden telnet ile anahtara erişim

6.2.4.3. SSH Yapılandırma

SSH'nin açılımı "Secure Shell" yani "Güvenli Kabuk"tur. SSH protokolü, bir bilgisayarın aynı ağda bulunan bir sunucuya uzaktan bağlanmasını sağlayan bir protokoldür. TELNET protokolünden en önemli farkı şifreli olarak çalışmasıdır. Bir bağlantı yaparken kullanıcı adı ve şifreler açık metin olarak değil, şifrelenmiş olarak iletilir.

Uygulama 20

http://kitap.eba.gov.tr/KodSor.php?KOD=21047

SSH yapılandırma anahtara bağlanma için gerekli işlemleri aşağıdaki yönergeler doğrultusunda gerçekleştiriniz.

Adım 1: Uzak masaüstü yapılandırmasında yaptığınız uygulamayı açınız.

Adım 2: Konsol bağlantısı ile anahtara bağlanıp global konfigürasyon moduna geçiniz.

Adım 3: ***Anahtar(config)#ip domain name MTAL*** komutu ile anahtara alan adı (domain name) veriniz.

Adım 4: ***Anahtar(config)#username fatih password 1453*** komutu ile anahtara kullanıcı adı ve şifresini atayınız.

Dikkat

Kullanıcı adı belirlenmezse **admin** varsayılan olarak kullanılır.

Adım 5: ***Anahtar(config)#crypto key generate rsa*** komutu ile **rsa şifreleme** oluşturunuz.

Adım 6: Ekrana gelen "How many bits in the modulus [512]:" sorusuna **1024** değerini giriniz.

Dikkat

Şifrelemede kullanılacak bit sayısını belirlemek için kullanılır. 360 ile 2048 bit arasında bir değer verilebilir.

Adım 7: ***Anahtar(config)#ip ssh version 2*** komutu ile **ssh versiyonu** belirleyiniz.

Adım 8: ***Anahtar(config)#line vty 0 15*** komutu ile anahtara aynı anda bağlanabilecek **kullanıcı sayısı** belirleyiniz.

Adım 9: ***Anahtar(config-line)#password malazgirt*** komutu ile **ssh erişim şifresini** oluşturunuz.

Adım 10: ***Anahtar(config-line)#transport input ssh*** komutu ile **ssh protokülünü** aktifleştiriniz.

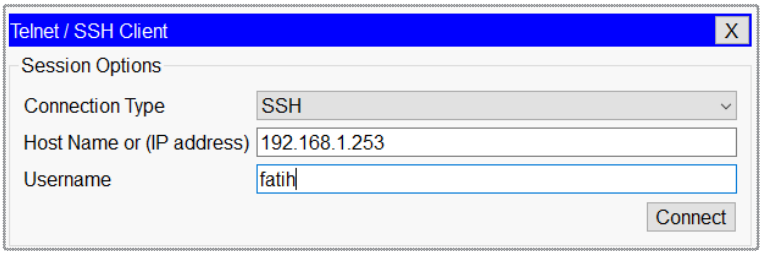
Adım 11: ***Anahtar(config-line)#login local*** komutu ile **veri girişini** sağlayınız.

Adım 12: ***Anahtar(config-line)#exit*** komutu ile çıkınız.

Adım 13: ***Anahtar(config)#do wr*** komutu ile yapılandırmayı kaydediniz.

Adım 14: ***Anahtar(config)#do show ssh*** komutuyla **ssh ayarlarını** kotrol ediniz.

Adım 15: *Simülasyondaki diğer bilgisayar üzerinden **telnet/ssh programını** açınız (Görsel 6.31).*



Görsel 6.31: SSH bağlantısı

Adım 16: Bağlantı tip olarak SSH seçiniz.

Adım 17: IP adresi olarak bir önceki uygulamada anahtarın VLAN arayüzüne atadığınız IP adresini giriniz.

Adım 18: Username olarak **mevlana** giriniz.

Adım 19: Açılan ekranda ssh bağlantısı için oluşturduğunuz şifreyi giriniz (Görsel 6.32).

Adım 20: SSH bağlantısını kapatmadan başka bir bilgisayardan aynı şekilde bağlantı yapmayı deneyiniz.

Adım 21: Üçüncü bir bilgisayar üzerinden komut satırını açınız ve ekrana "**ssh -l fatih 192.168.1.253**" yazarak "Enter" tuşuna basınız.

Adım 22: Fatih kullanıcısı ssh için oluşturduğunuz şifreyi girerek bağlantıyı sağlayınız (Görsel 6.33).

```
Anahtar#conf t
Enter configuration commands, one per line.  End with
CNTL/Z.
Anahtar(config)#ip domain name MTAL
Anahtar(config)#username fatih password 1453
Anahtar(config)#crypto key generate rsa
% You already have RSA keys defined named Anahtar.MTAL .
% Do you really want to replace them? [yes/no]: y
The name for the keys will be: Anahtar.MTAL
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]: 1024
% Generating 1024 bit RSA keys, keys will be non-
exportable...[OK]

Anahtar(config)#ip ssh version 2
*Mar 1 17:10:12.162: %SSH-5-ENABLED: SSH 2 has been
enabled
Anahtar(config)#line vty 0 15
Anahtar(config-line)#transport input ssh
Anahtar(config-line)#login local
Anahtar(config-line)#exit
Anahtar(config)#do wr
Building configuration...
[OK]
Anahtar(config)#
```

Görsel 6.32: SSH yapılandırma

```
C:\>ssh -l fatih 192.168.1.253

Password:



Anahtar>
```

Görsel 6.33: Komut istemi ile SSH bağlantısı

Dikkat

Anahtarın ayrıcalıklı kullanıcı modu için parola oluşturulmadıysa telnet/ssh vasıtasıyla yapılandırmaya izin vermeyecektir (Görsel 6.34).

```
C:\>ssh -l fatih 192.168.1.253

Password:



Anahtar>en
% No password set.
Anahtar>
```

Görsel 6.34: Ayrıcalıklı kullanıcı modu parolası oluşturulmamış

Araştırma

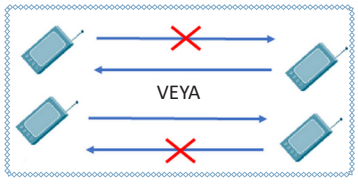
SSH uygulamanızda oluşturduğunuz RSA anahtar çiftini silmek için "***crypto key zeroize rsa***" genel yapılandırma modu komutunu kullanınız. RSA anahtar çifti silindikten sonra SSH sunucusunu kontrol ediniz ve durumunu açıklayınız.

6.2.5. Port Hızı ve Duplexmodu Yapılandırma

Port hızı, anahtarın portlarından saniyede aktarılacak veri kapasitesinin bit üzerinden ifade eder. Ağın kullanımı esnasında bağlantı hız sorunu yaşanmaması için anahtara bağlanacak cihazların port hızlarına göre anahtarın **uplink** portlarının hızı belirlenmelidir. Buna göre anahtar seçimi yapılmalıdır.

Duplex, çift yönlü iletişim demektir. Full Duplex ve Half Duplex olmak üzere iki şekilde kullanılır.

- **Half duplex** bağlantılar, eş zamanlı çift yönlü veri akışına izin vermez. Bu davranışa örnek olarak telsiz sistemi verilebilir. Telsizde bir taraf konuşurken diğeri aynı zamanda konuşamamaktadır (Görsel 6.35).



Görsel 6.35: Half duplex iletişim

- **Full duplex** bağlantılarda, veri akışı çift yönlüdür. Aynı anda hem veri gönderimi hem de veri alımı yapılabilir. Ethernet, Fast Ethernet ve Gigabit Ethernet kartları full duplex yeteneğine sahiptir (Görsel 6.36).

Görsel 6.36: Full duplex iletişim

Uygulama 21

Port hızı ve duplex yapılandırması için gerekli işlemleri aşağıdaki yönergeler doğrultusunda gerçekleştiriniz.

Adım 1: Uzak masaüstü yapılandırmasında yaptığınız uygulamayı açınız.

Adım 2: Anahtara SSH ile bağlanıp global konfigürasyon moduna geçiniz.

Adım 3: ***Anahtar(config)#interface fastEthernet 0/1*** komutuyla bir numaralı arayüze geçiş yapınız.

Adım 4: ***Anahtar(config-if)#speed 100*** komutu ile port hızını 100Mbs olarak ayarlayınız.

Adım 5: ***Anahtar(config-if)#duplex full*** komutu ile duplex ayarını full yapınız.

Adım 6: ***Anahtar(config-if)#exit***

Adım 7: ***Anahtar(config)# do show running-config*** komutu ile yaptığınız ayarları kontrol ediniz (Görsel 6.37).

```
Anahtar#conf t
Enter configuration commands, one per line.  End with
CNTL/Z.
Anahtar(config)#interface fa0/1
Anahtar(config-if)#speed 100
Anahtar(config-if)#duplex full
Anahtar(config-if)#
%LINK-3-UPDOWN: Interface FastEthernet0/1, changed state
to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/1, changed state to down
```

Görsel 6.37: Port hızı ve duplex yapılandırma

Sıra Sizde

Anahtarınızın gigabit ethernet portunun port hızını 1 Gbps olarak, duplex ayarını otomatik (auto) olarak belirleyiniz.

6.2.6. DHCP Yapılandırma

DHCP (Dinamic Host Configuration Protokol), ağa bağlı cihazlara TCP/IP protokol takımını veren bir ağ servisidir. Temel görevi ağda bulunan bilgisayarların ve diğer cihazların dinamik olarak IP adresi, alt ağ maskesi, varsayılan ağ geçidi, DNS gibi yapılandırmaları otomatik olarak almasını sağlamaktır.

El ile IP adresi vermek birçok olası hataya yol açabilir. Yanlışlıkla birden fazla cihaza aynı IP adresi atanabilir ya da yazımda hata yapılabilir. Böyle sorunlar ağlar arası iletişimde hatalara yol açar. Bu sebeple dinamik olarak atanan IP adresleri daha çok tercih edilir.

Otomatik IP adresi vermek için anahtarlarda sanal ağların (VLAN) oluşturulması gereklidir.

Uygulama 22

http://kitap.eba.gov.tr/KodSor.php?KOD=21048

DHCP yapılandırması için gerekli işlemleri aşağıdaki yönergeler doğrultusunda gerçekleştiriniz.

Adım 1: Simülasyon programını açınız ve dört bilgisayar ve bir anahtardan oluşan bir ağ oluşturunuz.

Adım 2: Konsol bağlantısı ile anahtara bağlanıp global konfigürasyon moduna geçiniz (Görsel 6.38).

Adım 3: ***Anahtar(config)# interface vlan 1*** komutu ile VLAN1 arayüzüne geçiniz.

Adım 4: Anahtar(config-if)#*ip address 192.168.1.1 255.255.255.0* komutu ile VLAN1 için IP adresi ve alt ağ maskesini tanımlayınız.

Adım 5: ***Anahtar(config-if)#no shutdown*** komutu ile aktifleştiriniz.

Adım 6: ***Anahtar(config-if)#exit*** komutu ile VLAN arayüzünden çıkınız.

Adım 7: ***Anahtar(config)#ip dhcp pool bilisim*** komut ile DHCP havuzu oluşturunuz.

Adım 8: ***Anahtar(dhcp-pool)#network 192.168.1.0 255.255.255.0*** komutuyla ağ adresi ve alt ağ maskesini tanımlayınız.

Adım 9: ***Anahtar(dhcp-pool)#default-router 192.168.1.1*** komutuyla varsayılan yönlendirici adresini tanımlayınız.

Adım 10: ***Anahtar(dhcp-config)#dns-server 195.175.39.39*** komutuyla DNS sunucu adresini tanımlayınız.

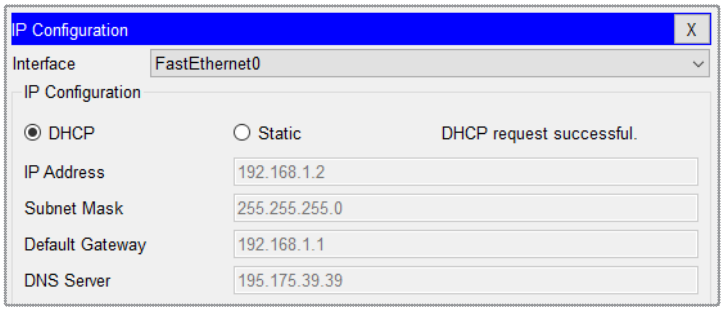
Adım 11: ***Anahtar(dhcp-config)#do write*** komutuyla yapılandırmayı kaydediniz.

```
Anahtar(config)#
Anahtar(config)#interface vlan 1
Anahtar(config-if)#ip address 192.168.1.1 255.255.255.0
Anahtar(config-if)#no shutdown
Anahtar(config-if)#exit
Anahtar(config)#ip dhcp pool bilisim
Anahtar(dhcp-config)#network 192.168.1.0 255.255.255.0
Anahtar(dhcp-config)#default-router 192.168.1.1
Anahtar(dhcp-config)#dns-server 195.175.39.39
Anahtar(dhcp-config)#do write
Anahtar(dhcp-config)#exit
```

Görsel 6.38: Anahtar DHCP yapılandırma

Adım 12: Anahtar yapılandırmasından çıkınız ve bilgisayarın arayüzünden otomatik IP adresini aktifleştiriniz ve IP adresi almasını bekleyiniz.

Adım 13: Anahtara bağlı diğer cihazlara da otomatik IP adresi aldırınız (Görsel 6.39).



Görsel 6.39: DHCP ile otomatik IP adresi alma

Adım 14: Çalışmanızı **DHCP** adıyla kaydediniz.

Sıra Sizde

Simülasyon programında beş bilgisayar ve bir anahtardan oluşan bir ağ oluşturunuz. Anahtarınızda **şehrinizin adıyla 10.10.2.0** ağında **255.0.0.0** alt ağ maskesi olan bir DHCP havuzu oluşturunuz. Ağınızdaki bilgisayarların DHCP havuzundan IP adreslerini otomatik almasını sağlayınız.

6.2.7. Yapılandırmayı Kaydetme ve Geri Yükleme

Anahtar üzerinde yapılan konfigürasyon değişikliklerinin sürekliliğinin sağlanması için bu değişikliklerin **kaydedilmesi** gerekmektedir. Herhangi bir sebeple ayarların bozulması durumunda önceden kaydedilen yapılandırmanın **geri yüklenmesi** gerekebilir.

6.2.7.1. Yapılandırmanın Kaydedilmesi

Anahtarın konfigürasyonunda yapılan değişiklikler RAM'deki çalışan mevcut konfigürasyona kaydedilir. Anahtarlarda yapılan değişiklikler dört farklı alana kaydedilebilir.

flash: Anahtarın flash hafızasına
ftp: Ağ üzerindeki bir ftp sunucuya
startup-config: Anahtarın açılış hafızasına
tftp: Ağ üzerindeki bir tftp sunucusuna

Ftp ve tftp sunucularına kaydetmek için ağ üzerindeki adreslerinin bilinmesi gerekmektedir. **Flash** ve **startup-config** seçenekleri ise cihazın üzerinde bulunan hafızalardır.

Uygulama 23

Anahtar yapılandırması kaydetme işlemini aşağıdaki yönergeler doğrultusunda gerçekleştiriniz.

Adım 1: DHCP adıyla kaydettiğiniz çalışmanızı açınız.

Adım 2: Anahtar bağlantısı sağlayınız, ayrıcalıklı kullanıcı moduna geçiniz.

Adım 3: ***Anahtar#copy running-config startup-config*** komutuyla yapılan değişikleri **başlangıç dosyasına** kaydediniz.

Adım 4: ***Anahtar#copy running-config flash:*** komutuyla yapılan değişikleri flash hafızaya kaydediniz.

Adım 5: Ekrana gelen ***destination filename [running-config]*** kısmına dosya adı olarak ***bilisim*** adını veriniz.

Adım 6: ***Anahtar#show flash*** komutuyla anahtarın hafızasında kaydettiğiniz dosyayı görünüz (Görsel 6.40).

```
Anahtar>en
Anahtar#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
Anahtar#copy running-config flash:
Destination filename [running-config]? bilisim
Building configuration...
[OK]
Anahtar#show flash:
Directory of flash:/

    3  -rw-        1427          <no date>  bilisim
    1  -rw-     4414921          <no date>  c2960-lanbase-
mz.122-25.FX.bin
    2  -rw-        1427          <no date>  config.text

64016384 bytes total (59598609 bytes free)
Anahtar#
```

Görsel 6.40: Ayarları kaydetme

Adım 7: Çalışmanızı bilisim adıyla kaydediniz.

Sıra Sizde

Anahtarın başlangıç ayarlarını flash alanına okul numaranız ve adınız ile kaydediniz.

6.2.7.2. Geri Yükleme

Anahtar üzerinde yapılan herhangi bir değişiklik sonucunda ya da anahtar ayarlarının bozularak düzgün çalışmaması durumunda daha önce kaydedilen ayarlar geri yüklenebilir. Bu işlemde yapılandırmanın kaydedilmesi gibi ***copy*** komutu ile gerçekleştirilir.

Uygulama 24

Kaydedilen yapılandırmayı geri yükleme işlemini aşağıdaki yönergeler doğrultusunda gerçekleştiriniz.

Adım 1: bilisim adıyla kaydettiğiniz çalışmanızı açınız.

Adım 2: Anahtar bağlantısı sağlayınız, ayrıcalıklı kullanıcı moduna geçiniz.

Adım 3: ***Anahtar#copy flash: startup-config*** komutuyla hafızadan, yapılandırma ayarlarını başlangıç ayarları olarak geri yükleyiniz.

Adım 4: Ekrana gelen ***Source filename []?*** kısmına dosya adı olarak ***bilisim*** yazarak daha önce kaydedilen ayarları **kaynak dosya** olarak belirtiniz.

Adım 5: Ekrana gelen ***Destination filename [startup-config]?*** kısmında **hedef dosya adını** onaylayınız ve geri yükleme işlemini tamamlayınız (Görsel 6.41).

```
Anahtar>en
Anahtar#copy flash: startup-config
Source filename []? bilisim
Destination filename [startup-config]?
[OK]

1427 bytes copied in 0.416 secs (3430 bytes/sec)
Anahtar#
```

Görsel 6.41: Yapılandırmayı geri yükleme

Sıra Sizde

Anahtarın flash alanına kaydettiğiniz dosyayı çalışan ayarlara geri yükleyiniz.

Aşağıdaki soruları dikkatlice okuyunuz ve doğru seçeneği işaretleyiniz.

1. Aşağıdaki iletişim türlerden hangisinde bir taraf veri gönderirken diğer taraf beklemektedir?

A) Duplex
B) Single Duplex
C) Half Duplex
D) Full Duplex
E) Triplex

2. Aşağıdaki komutlardan hangisiyle anahtara doğru bir şekilde isim verilir?

A) Anahtar>name MTAL
B) Anahtar#hostname MTAL
C) Anahtar(config)#hostname MTAL
D) Anahtar(config)#name MTAL
E) Anahtar(config-if)#hostname MTAL

3. Anahtarın ilk yapılandırma ayarlarında hangi kablo kullanılır?

A) Koaksiyel Kablo
B) Fiber Optik Kablo
C) Crossover Kablo
D) Düz Kablo
E) Rollover Kablo

4. Aşağıdakilerden hangisi arayüzlerde kullanılabilecek komut ve parametreleri görmek için kullanılır?

A)? B) % C) ! D) * E) #

5. Broadcast domain için hangi MAC adresi kullanılır?

A) AA:AA:AA:AA:AA:AA
B) 00:00:00:00:00:00
C) 11:11:11:11:11:11
D) 00:00:00:00:00:01
E) FF:FF:FF:FF:FF:FF

6. Ethernet çerçeve yapısında aşağıdakilerden hangisi <u>bulunmaz?</u>

A) Hedef MAC Adresi
B) Kaynak MAC Adresi
C) Data
D) CRC
E) Yönlendirici IP Adresi

7. Aşağıdakilerden hangisi anahtarın konsol portuna parola vermek için kullanılan komuttur?

A) Anahtar(config)#line vty 0 4
Anahtar(config-line)# enable password 123
Anahtar(config-line)#login

B) Anahtar(config)# line console 0
Anahtar(config-line)# password 123
Anahtar(config-line)#login

C) Anahtar(config)# line vty 0 4
Anahtar(config-line)# password 123
Anahtar(config-line)#login

D) Anahtar(config)# line console 0
Anahtar(config-line)# enable password 123
Anahtar(config-line)#login

E) Anahtar(config)# line telnet console 0
Anahtar(config-line)#password 123
Anahtar(config-line)#login

8. Veri paketinde hata olup olmadığını kontrol eden iletim yöntemi aşağıdakilerden hangisidir?

A) Kestirme (Cut-Trough)
B) Depola ve İlet (Store-and-Forward)
C) Serbest parça (Fragment-Free)
D) Uyarlamalı (Adaptive)
E) Uyarla ve İlet (Adapt and Forward)

9. Anahtar üzerinde çalışan yapılandırmayı aşağıdaki komutlardan hangisi kullanılır?

A) Anahtar>show running-config
B) Anahtar#show running-config
C) Anahtar#show startup-config
D) Anahtar>show startup-config
E) Anahtar#show ip interfaces

10. Anahtar MAC tablosunu görmek için aşağıdaki komutlardan hangisi kullanılır?

A) Anahtar>show mac-table-address
B) Anahtar#show mac-table
C) Anahtar>show mac-address-table
D) Anahtar#show mac-table-address
E) Anahtar#show mac-address-table

ÖĞRENME BİRİMİ 7

SANAL YEREL ALAN AĞLARI (VLAN)

NELER ÖĞRENECEKSİNİZ?

Bu öğrenme birimi ile;

- Sanal yerel ağları (VLAN) tanıyabilecek ve yeni VLAN'lar oluşturacak,
- VLAN kullanımının avantajlarını kavrayacak,
- Farklı VLAN türlerini açıklayabilecek ve VLAN listelemelerini yapacak,
- Anahtar (switch) cihazlarında arayüzlerin (port-) VLAN'larda çalışma durumlarını görecek,
- VLAN'lara farklı arayüzlerin erişimini düzenleyecek,
- Anahtar cihazlar arasında farklı VLAN'ların trafiğinin iletimi için trunk arayüzleri kullanacak,
- Trunk arayüzlerde güvenli kabul edilen VLAN trafiği için izinler düzenleyecek,
- Anahtar cihazlarda arayüzlerin varsayılan durumu ve dinamik olarak erişim, trunk durum güncellemesini yapacak,
- Anahtar cihazların yönetimi için VLAN arayüzlerini kullanabilecek,
- Merkezî bir anahtar ile diğer anahtar cihazlarına VLAN bilgilerinin verilebilmesi için sanal yerel ağ aktarım protokolünü (VTP-Virtual LAN Trunking Protocol) açıklayacak,
- Anahtar cihazındaki VLAN veri tabanını silecek,
- Mantıksal ağlar arasında veri trafiğinin aktarılabilmesi için yönlendirme kavramını açıklayacak,
- VLAN'lar arasında veri trafiğinin aktarımı için trunk arayüzlerini kullanarak yönlendirmeler yapacaksınız.

ANAHTAR KELİMELER

VLAN, yayın, ARP (Address Resolution Protocol-Adres Çözümleme Protokolü), port, arayüz, trunk, DTP (Dynamic Trunking Protocol-Dinamik Gövdem Protokolü), VTP, access, erişim, protokol, IP, anahtarlama, yönlendirme

Hazırlık Çalışmaları

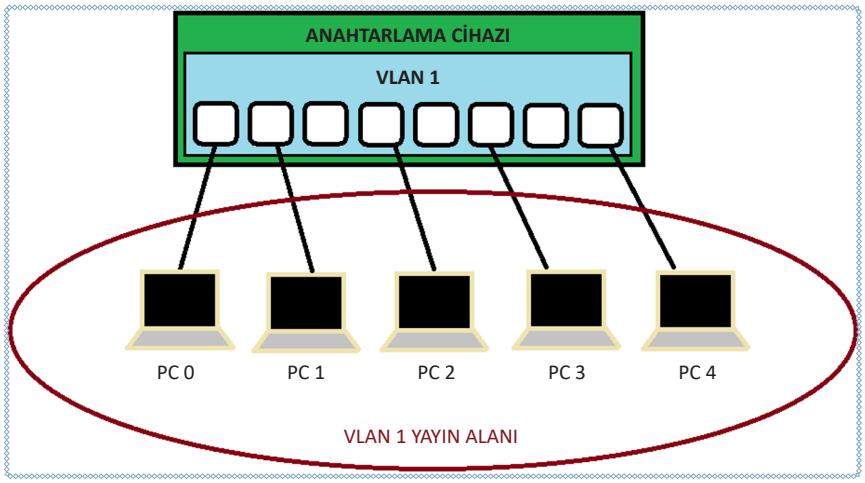
1. Hangi ağ cihazları ile farklı bilişim cihazlarını bir yerel ağa dâhil edip cihazların görüşmesi sağlanabilir? Araştırınız.
2. Anahtar cihazlarda farklı mantıksal ağlar oluşturulabilirse ağ için ne gibi faydaları olabilir? Tahminlerinizi arkadaşlarınızla paylaşınız.
3. Farklı mantıksal ağların haberleşebilmesi için ağda ne gibi gereksinimler olabilir? Açıklayınız.

7.1. VLAN Oluşturma

Anahtar cihazlarında yayın alanlarını küçültmek ve farklı ağlara bölmek için sanal yerel ağlardan yararlanılır. Bu ağ modeli, ağ yöneticisi tarafından anahtar cihazda oluşturulan mantıksal bir yapılandırmadır. Anahtar arayüzleri oluşturulan sanal ağlara dâhil edilerek ağ içinde kullanılır.

7.1.1. VLAN (Virtual Local Area Network – Sanal Yerel Alan Ağı)

Anahtarlama cihazları (switch) fiziksel olarak kendisine bağlı tüm cihazlarda tek ağa hizmet verecek gibi çalışsa da mantıksal olarak farklı ağlara bölünerek birden fazla ağa hizmet verebilmesi sağlanır. Oluşturulan bu mantıksal ağlar **VLAN** olarak adlandırılır. Anahtarlama cihazları varsayılan olarak bir VLAN ile yapılandırılır ve başka VLAN'lar yapılandırılmazsa tüm anahtar portları varsayılan VLAN 1 ile çalışacaktır. Oluşturulan yeni VLAN'lar ile ayrılmış ağların yayın trafiği sadece kendi VLAN ağı ile sınırlı kalacaktır. Anahtarlama cihazındaki diğer VLAN'lar bu trafikten etkilenmeyecektir (Görsel 7.1).



Görsel 7.1: VLAN 1 ile tek yayın alanı

7.1.2. VLAN Avantajları

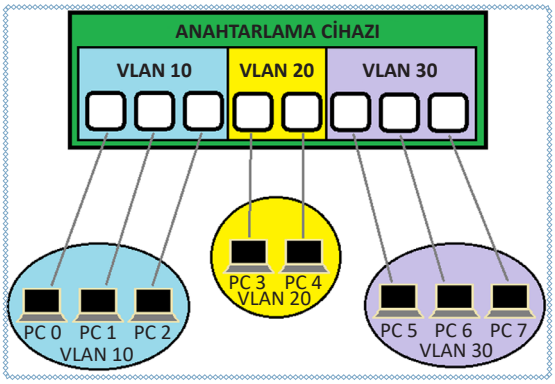
Avantajlar aşağıda başlıklar hâlinde verilmiştir.

Güvenlik: Ağlar mantıksal olarak bölündüğü için VLAN'lardaki cihazlar, diğer VLAN'lardaki ağlardan ayrılır. Bu da cihazların bağımsız alanlarda kalmasını ve güvenliğin artmasını sağlar.

Performans: VLAN'lar arasında ayrı trafik oluştuğu için bir VLAN'ın ağ trafiği diğerini etkilemez ve her VLAN'da ağ iletişim performansı artar.

Yayın Alanı: Her VLAN'ın ayrı mantıksal ağı olduğu için ayrı bir yayın alanı oluşur. VLAN'larda oluşan yayın paketleri diğer VLAN'lara aktarılmaz.

Maliyet: Anahtarlama cihazı içinde ayrı VLAN'lar oluşturularak yeni anahtar (switch) gereksinimleri ortadan kalkar. Böylelikle maliyet düşer, tasarruf edilir (Görsel 7.2).



Görsel 7.2: VLAN'lar ile ayrı yayın alanlarına bölünmüş anahtarlama cihazı

7.1.3. VLAN Türleri

VLAN'lar taşıdıkları trafik türüne veya işlevlerine göre tanımlanabilir.

Data VLAN'ı: Kullanıcılar için oluşturulmuş VLAN'lardır. Kullanıcı veri trafiğini taşımak için kullanılır.

Default VLAN: Anahtar başlangıç yapılandırmasında var olan VLAN'dır. Varsayılan olarak anahtar üzerindeki tüm portlar bu VLAN'a dâhildir. Varsayılan VLAN anahtarlama cihazlarında VLAN 1 şeklinde adlandırılmıştır. VLAN 1 yeniden adlandırılamaz ve silinemez.

Native VLAN: 802.1q protokolü ile farklı VLAN trafiğinin switchten çıkışı sağlanır. Varsayılan VLAN 1 başlangıç için native olarak kabul edilir ancak VLAN 1 etiketsiz olarak çıkış yapar ve 802.1q protokolü yerine Ethernet II protokolünü kullanır. Veri trafiğinin etiketsiz aktarımını önlemek için switchlerden native VLAN'ın başka bir VLAN ile değiştirilmesi önerilir.

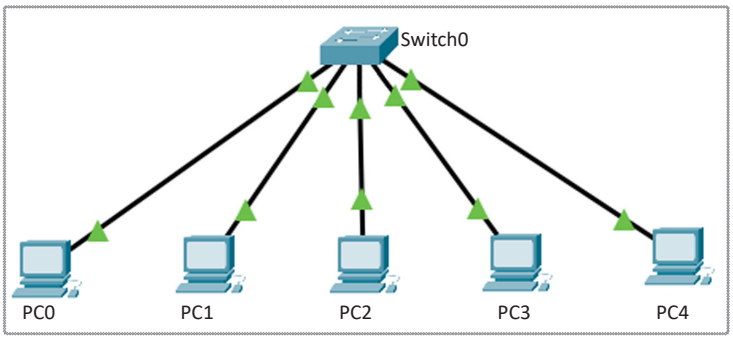
Yönetim VLAN'ı: VLAN'lara IP adresi atanabilir. IP adresi almasındaki amaç uzaktan telnet, ssh gibi uygulamalarla yönetilebilmesidir. Uzaktan erişim ile cihazın yönetilmesini sağlayan VLAN'lar **yönetim VLAN'**ıdır. VLAN'ların IP adresi alacak sanal arayüzü **SVI** şeklinde tanımlanır.

Ses VLAN'ları: Ağlardaki ses veri trafiğini aktarmak için kullanılan VLAN'lara **ses VLAN'ı** denir.

Reserved VLAN: Anahtar cihazının başlangıcında yapılandırılmış, özel amaçlı protokollerin kullanılması için var olan bu VLAN'lar, default VLAN 1 gibi silinemez ve değiştirilemez.

Uygulama 1

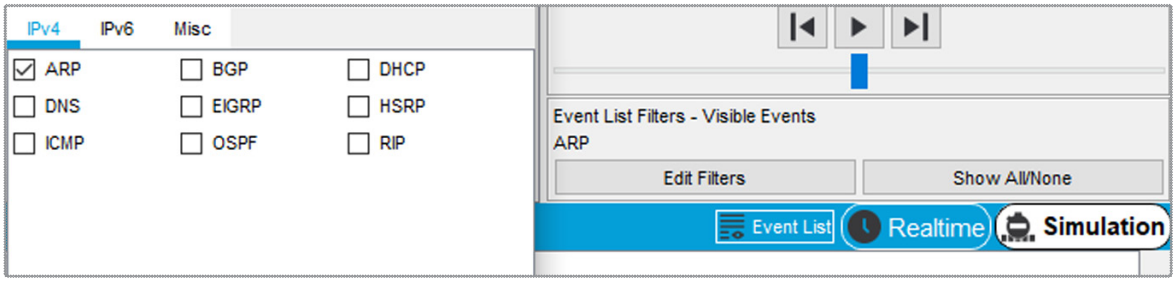
Görsel 7.3'te anahtar cihazında başlangıç için varsayılan VLAN 1 yayın alanını görmek için topolojiyi hazırlayıp gerekli işlemleri aşağıdaki yönergeler doğrultusunda gerçekleştiriniz.



Görsel 7.3: Topoloji örneği

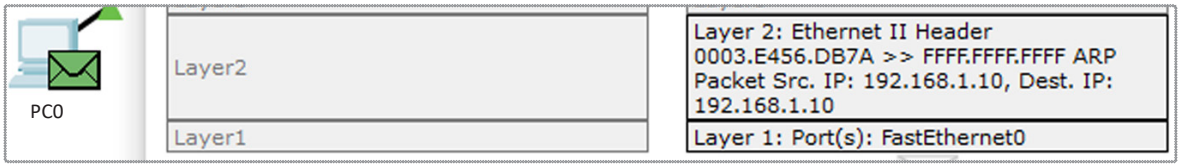
Adım 1: Görsel 7.3'te görülen topolojiyi ağ simülasyon programında kurunuz. Sırası ile bilgisayarları anahtarlama cihazında 1, 5, 10, 15 ve 20. portlara bağlayınız.

Adım 2: Ağ paketlerini gözlemlemek için **Simülation\Show All/None\Edit Filters** düğmeleri ile sadece **ARP** paketini seçiniz (Görsel 7.4).



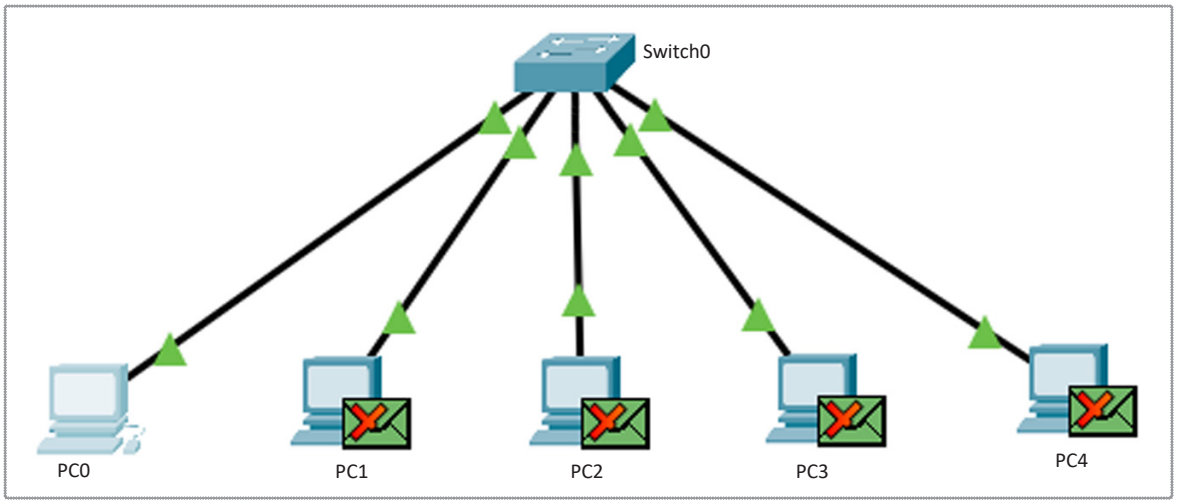
Görsel 7.4: Ağ Simülasyonunda ARP paketi seçimi

Adım 3: PC 0 için el ile 192.168.1.10 IP adresini ve 255.255.255.0 alt ağ maskesini giriniz. PC0 üzerinde ARP paketi belirecektir. ARP, LAN içinde IP çakışmasını önlemek için oluşturulan kontrol protokolüdür. Paketin üzerine tıklandığında OSI modeline göre 2. katmanda Ethernet II çerçevemizin hedef MAC adresinin FFFF.FFFF.FFFF olduğu görülür. Hedef MAC adresin FFFF.FFFF.FFFF olması paketin bir **yayın paketi** olduğu anlamına gelir. Yayın paketleri bulundukları VLAN üzerinde tüm portlardaki bilgisayarlara iletilir (Görsel 7.5).



Görsel 7.5: ARP paketi yayın çerçevesi

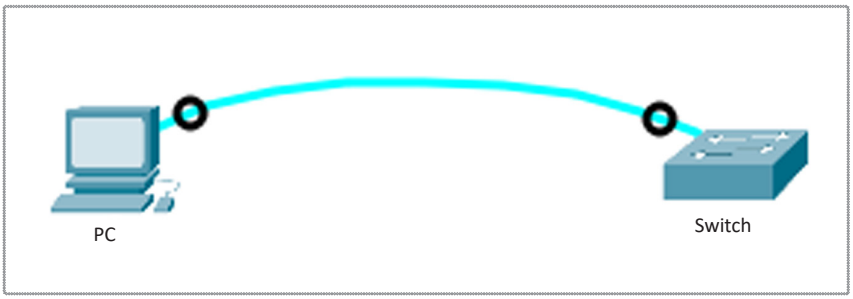
Adım 4: Anahtarlama cihazında başlangıçta VLAN 1 tek olduğu için tüm portlar VLAN 1'e dâhildir. Simülasyonu oynat düğmesinden ilerlettiğinizde ARP yayın paketleri Anahtarlama cihazındaki 5, 10, 15 ve 20. portlardaki PC1, PC2, PC3, PC4 bilgisayarlarına gönderilecektir (Görsel 7.6).



Görsel 7.6: Uygulama 1 için VLAN 1 yayın alanı

Uygulama 2

Görsel 7.7'de anahtarlama cihazlarındaki VLAN'lar gösterilmiştir. Bu örneği gerçek cihazlar üzerinde veya simülasyon programı kullanarak işlemi aşağıdaki yönergeler doğrultusunda gerçekleştiriniz.



Görsel 7.7: Uç cihaz, anahtar cihaz konsol bağlantısı

Adım 1: PC ve anahtarlama cihazını konsol kablosuyla Görsel 7.7'deki gibi bağlayınız ve bir terminal programı ile anahtar (switch) işletim sistemini açınız.

Adım 2: Sırasıyla

Switch>enable
Switch#configure terminal
Switch#show vlan komutlarını terminal ekranında yazınız.

Adım 3: "**show vlan**" komutuyla anahtarlama cihazındaki VLAN'ların listesini görebilirsiniz (Görsel 7.8). Burada anahtarda daha önce VLAN yapılandırılmadığı için data VLAN'larında sadece 1 numaralı VLAN görünür. Bu varsayılan-default VLAN 1 satırıdır. VLAN 1 başlangıçta aktiftir ve başlangıç için VLAN'daki fiziksel tüm ethernet portları VLAN 1'e dâhildir. Data VLAN'ları 1001 sayısına kadar numaralandırılabilir.

```
Switch#show vlan

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

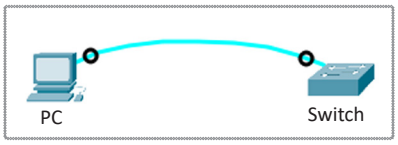
Görsel 7.8: Anahtar cihazda VLAN tablosu

Dikkat

1002, 1003, 1004, 1005 VLAN'ları özel protokolleri gerçekleştirmek için yapılandırılmış **Reserved VLAN**'lardır. Değiştirilemez ve silinemez.

Uygulama 3

Görsel 7.9'daki anahtar PC bağlantısını yaparak tabloda verilen VLAN'ları aşağıdaki yönergeler doğrultusunda gerçekleştiriniz.



Görsel 7.9: Uygulama 3 için anahtar (switch) PC bağlantısı

Tablo 7.1: Uygulama 3 İçin İstenen VLAN Tablosu

VLAN	ADI
VLAN 10	Oda1
VLAN 20	Oda2
VLAN 30	Oda3

Adım 1: Anahtar cihazının terminal ekranını açınız. Yeni VLAN'lar oluşturmak için aşağıdaki komutları yazınız.

```
Switch(config)#vlan 10
Switch(config-vlan)#name Oda1
Switch(config-vlan)#exit
Switch(config)#vlan 20
Switch(config-vlan)#name Oda2
Switch(config-vlan)#exit
Switch(config)#vlan 30
Switch(config-vlan)#name Oda3
Switch(config-vlan)#exit
```

Dikkat

Yeni VLAN'lar oluşturmak için "vlan *Numara*" komutu yazılır. Numara data VLAN'ları için 1 ile 1001 arasında olabilir. "name *isim*" komutu ile VLAN'a uygun bir adlandırılma yapılır.

Adım 2: Oluşturulan VLAN'ları "show vlan" komutu ile listeleyiniz (Görsel 7.10).

```
Switch#sh vlan

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                 Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                 Gig0/1, Gig0/2
10   Oda1                              active
20   Oda2                              active
30   Oda3                              active
```

Görsel 7.10: Anahtar cihaz oluşturulmuş VLAN listesi

Dikkat

Oluşturulan yeni VLAN'lar listede bulunur. Henüz port atamaları yapılmadığı için yeni VLAN'larda herhangi bir port yoktur. Anahtarlama cihazı yayın alanı olarak VLAN 1'e dâhil tüm anahtar portlarını kullanır.

7.1.4. Anahtarlama Cihazı Arayüz (PORT) VLAN Durumları

Anahtarlama cihazı arayüzleri, taşıdığı veri trafiği ve kullandığı protokollere göre farklı durumlarda yapılandırılabilir. Anahtar arayüzlerinde VLAN durum yapılandırmasını gerçekleştirmek için terminal yazılımında arayüz satırına giriş yapılması gerekir.

7.1.4.1. Access Modu

Anahtar portunun sadece tek VLAN trafiğini taşıyacağı durumdur. Aşağıdaki komut ile arayüz tek VLAN kullanım durumuna getirilir.

Switch(config-if)#switchport mode *access*

7.1.4.2. Trunk Modu

Anahtar portunun birden fazla VLAN trafiğinin geçişine izin verdiği durumdur. Aşağıdaki komut ile arayüz birden fazla VLAN'ın trafiğine izin verir.

Switch(config-if)#switchport mode *trunk*

7.1.4.3.Desirable Modu

Anahtar arayüzünün, karşısında yer alan bir diğer anahtar arayüzünün konumuna göre kendisini güncellediği durumdur. Aşağıdaki komut ile arayüz kendini karşı anahtardaki arayüzün durumuna göre ayarlamaktadır.

Switch(config-if)#switchport mode *dynamic auto/desirable*

Dikkat

Arayüzler varsayılan olarak **dynamic auto** olarak yapılandırılır.

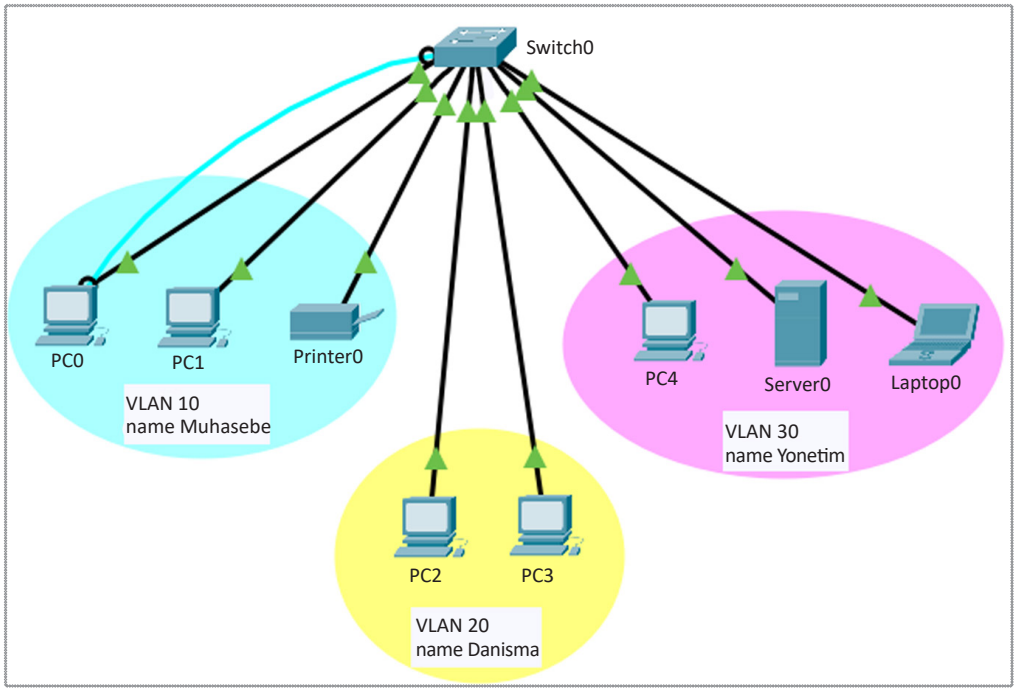
7.1.5. Anahtar Cihazlarda Arayüz VLAN Erişim Durumu

Anahtar arayüzleri erişim durumundayken tek VLAN için atanabilir. Varsayılan olarak tüm arayüzler VLAN 1'e atanmış olarak yapılandırılmıştır. Yeni oluşturulan VLAN'lara atanarak sadece o VLAN'ın ağ trafiği yayın alanı içinde kalması sağlanabilir. Bunun için
Switch(config-if)#switchport access vlan*vlanNumarası* komutu kullanılır.

Uygulama 4

http://kitap.eba.gov.tr/KodSor.php?KOD=21049

Görsel 7.11'de verilen topolojiyi gerçekleştirerek Tablo 7.3'te verilen VLAN'ları oluşturunuz ve gerekli arayüz atamalarını Tablo 7.2 verildiği gibi yapınız. Her VLAN için yayın paketlerini gözlemleyiniz. Uygulamayı aşağıdaki yönergeler doğrultusunda gerçekleştiriniz.



Görsel 7.11: Uygulama 4 için uç cihaz VLAN topolojisi

Tablo 7.2: Uygulama 4 İçin Uç Cihaz Anahtar Arayüz Bağlantısı

Kablo Arayüz Bağlantı Tablosu	
PC0	Fa0/1
PC1	Fa0/2
Printer0	Fa0/3
PC2	Fa0/6
PC3	Fa0/7
PC4	Fa0/11
Server0	Fa0/12
Laptop0	Fa0/13

Adım 1: İlk olarak Tablo 7.3'te verilen VLAN'ları oluşturunuz.

Tablo 7.3: Uygulama 4 İçin İstenen VLAN Tablosu

VLAN	Ad	Arayüz
VLAN 10	Muhasebe	fa0/1,fa0/2,fa0/3,fa0/4,fa0/5
VLAN 20	Danisma	fa0/6,fa0/7,fa0/8,fa0/9,fa0/10
VLAN 30	Yonetim	fa0/11,fa0/12,fa0/13,fa0/14,fa0/15

```
Switch(config)#vlan 10
Switch(config-vlan)#name Muhasebe
Switch(config-vlan)#exit
Switch(config)#vlan 20
Switch(config-vlan)#name Danisma
Switch(config-vlan)#exit
Switch(config)#vlan 30
Switch(config-vlan)#name Yonetim
Switch(config-vlan)#exit
```

Adım 2: İlgili arayüzleri VLAN'lara atayınız.

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

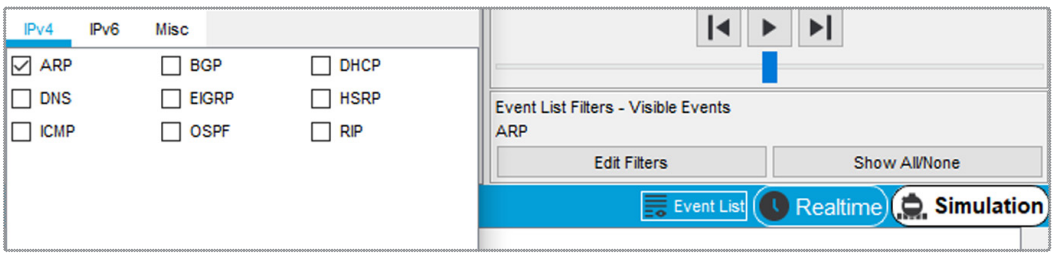
Adım 3: Arayüzlerin VLAN'lar ile eşleşmesini kontrol etmek için VLAN tablosunu görüntüleyiniz (Görsel 7.12).

```
Switch#show vlan
```

```
Switch#show vlan

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                                 Fa0/20, Fa0/21, Fa0/22, Fa0/23
                                                 Fa0/24, Gig0/1, Gig0/2
10   Muhasebe                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
20   Danisma                           active    Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10
30   Yonetim                           active    Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                 Fa0/15
1002 fddi-default                      active
```

Görsel 7.12: Anahtar cihazda oluşturulmuş VLAN listesi

Adım 4: Ağ paketlerini gözlemlemek için **Simulation\Show All/None\Edit Filters** düğmeleri ile sadece **ARP** paketini seçiniz (Görsel 7.13).



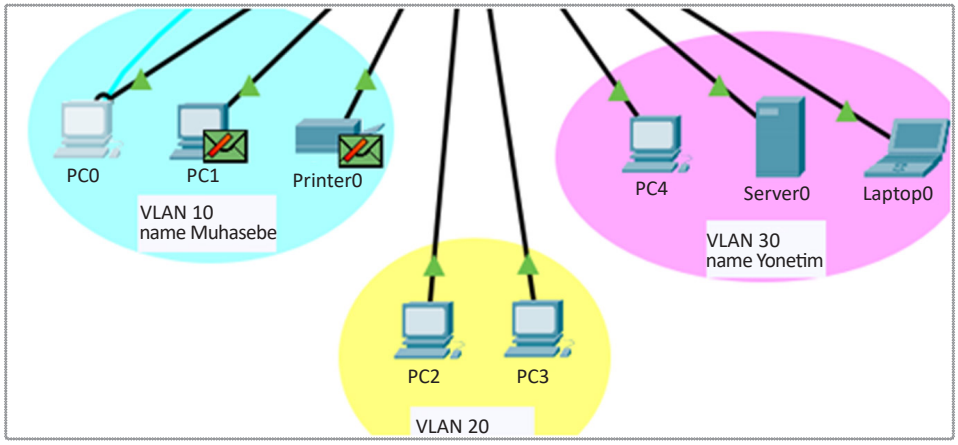
Görsel 7.13: Ağ simülasyonunda ARP paketi seçimi

Adım 5: PC0 için el ile 192.168.1.10 IP adresini ve 255.255.255.0 alt ağ maskesini giriniz.

Adım 6: PC0 üzerinde ARP paketi belirecektir. ARP, LAN içinde IP çakışmasını önlemek için oluşturulan kontrol protokolüdür. Paketin üzerine tıklandığında OSI modeline göre 2. katmanda Ethernet II çerçevesinin hedef MAC adresinin FFFF.FFFF.FFFF olduğu görülür. Hedef MAC adresin FFFF.FFFF.FFFF olması paketin bir yayın paketi olduğu anlamına gelir (Görsel 7.14). Yayın paketleri bulundukları VLAN üzerinde tüm portlardaki bilgisayarlara iletilir (Görsel 7.14).

Görsel 7.14: ARP paketi yayın çerçevesi

Adım 7: Simülasyon oynatıldığında PC0, VLAN 10 arayüzlerinden birine bağlı olduğu için ARP yayın paketleri sadece VLAN 10'un arayüzlerine bağlı diğer PC'lere gidecektir. VLAN20 ve VLAN30 arayüzlerine yayın paketi gönderilmeyecektir (Görsel 7.15).



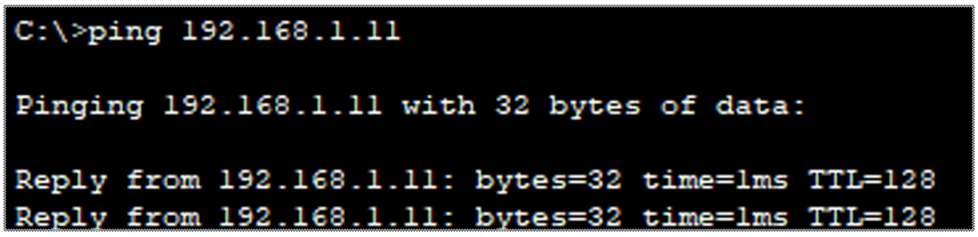
Görsel 7.15: VLAN10 için ARP yayın alanı

Adım 8: Simülasyon programında **Realtime** düğmesi ile gerçek zamanlı duruma geliniz (Görsel 7.16).

Görsel 7.16: Simülasyon programında gerçek zamanlı durum

Adım 9: PC1'e el ile 192.168.1.11 IP atamasını yapınız.

Adım 10: PC0'dan PC1'e ping komutu ile iletişim testi gerçekleştiriniz. Sonuç aşağıdaki görseldeki gibi başarılı olacaktır (Görsel 7.17).



Görsel 7.17: Başarılı ping iletişim testi

Adım 11: PC1'i anahtarlama cihazında fa0/8 arayüzüne bağlayınız ve yeniden ping komutu ile iletişim testi yapınız. Sonuç, Görsel 7.18'deki gibi olacaktır. PC1 artık VLAN10 arayüzlerinde olmadığı için VLAN 10'daki PC0'dan gelen trafik iletilemez.

```
C:\>ping 192.168.1.11

Pinging 192.168.1.11 with 32 bytes of data:

Request timed out.
```

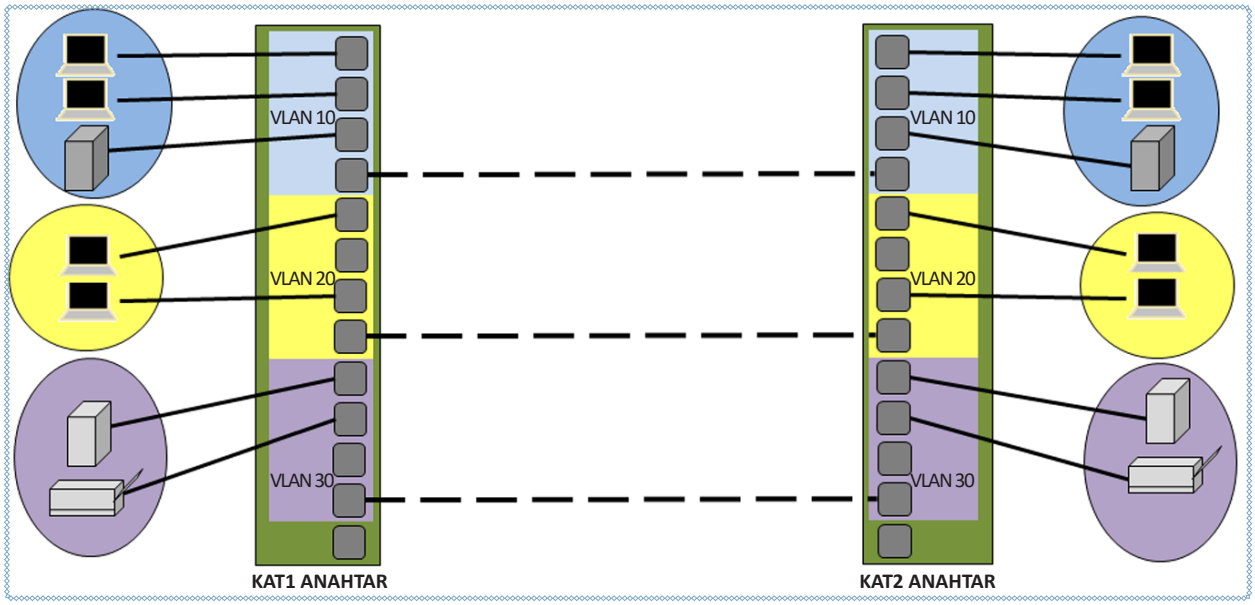
Görsel 7.18: Başarısız ping iletişim testi

Sıra Sizde

Görsel 7.11'dekiler VLAN için ayrı mantıksal ağlarda bilgisayarlara IP vererek yayın paketlerini simülasyon ortamında gözlemleyiniz. Elde ettiğiniz sonuçları sınıfla paylaşınız.

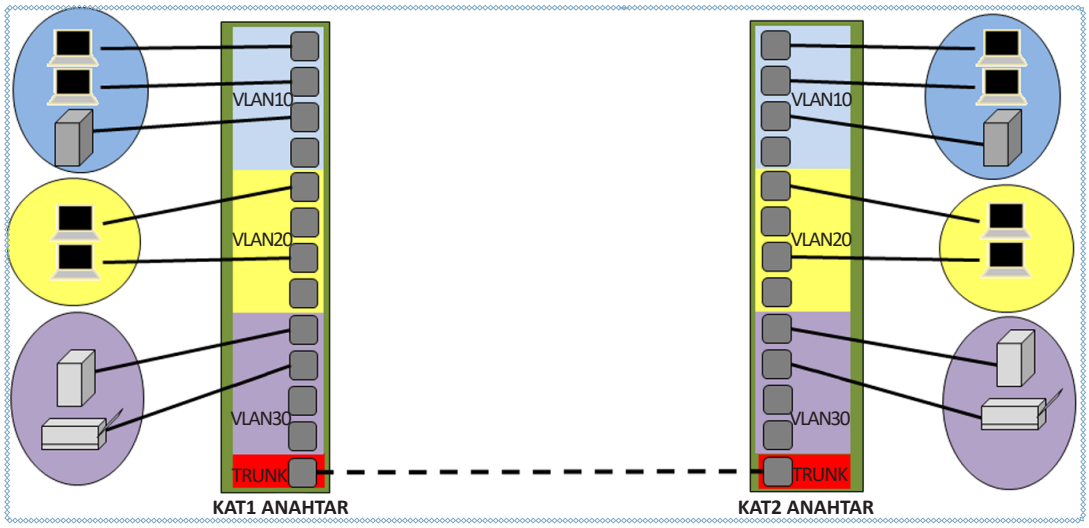
7.1.6. Anahtar Cihazlarda Arayüz Trunk Durumu

Farklı VLAN'ların trafiğini anahtar cihazdan başka bir cihaza aktarmak için arayüzün birden fazla VLAN'ın trafiğini aktaracak bir protokole sahip olması gerekir. Arayüzler tek VLAN'a erişim durumunda Ethernet II protokolünü kullanırken farklı VLAN trafiklerini aktarım için 802.1q protokolünü kullanır. Arayüzü 802.1q protokolünü konuşmaya hazır hâle getiren işleme **trunk durumu** denir.



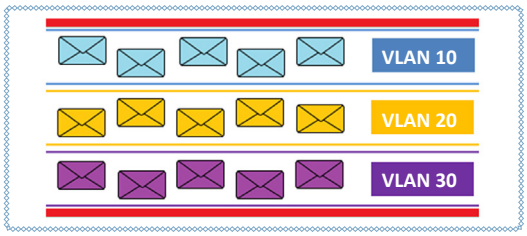
Görsel 7.19: Anahtar cihazlarda trunk olmadan VLAN'lar arası bağlantı

Farklı anahtarlama cihazları ile VLAN'ların fiziksel alanları genişletilebilir. Anahtarlama cihazları arasında VLAN'ları haberleştirmek için her VLAN'ın arayüzünden karşılıklı olarak kablo kullanılabilir ancak bu, her VLAN için ayrı bir kablo ve maliyetin artması anlamına gelir (Görsel 7.19). Bunun yerine ayrılmış arayüzleri trunk durumuna getirerek tüm VLAN'ların trafiği karşılıklı olarak aktarılabilir.



Görsel 7.20: Trunk ile anahtar cihazlar arasında bağlantı

Görsel 7.20'de VLAN 10, 20 ve 30 trafiği tek bir kablo ile trunk arayüzlerinden aktarılır. İlgili arayüzü trunk durumuna almak için arayüzde "switchport mode trunk" komutu kullanılır (Görsel 7.21).

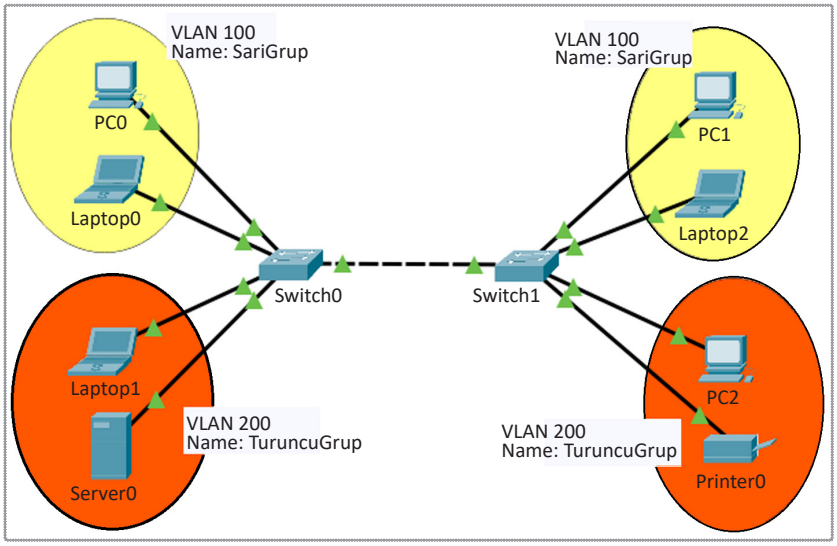


Görsel 7.21: Trunk arayüzlerde VLAN trafiği

Uygulama 5

http://kitap.eba.gov.tr/KodSor.php?KOD=21050

Görsel 7.22'de verilen ağ topolojisini aşağıdaki yönergeler doğrultusunda gerçekleştiriniz.



Görsel 7.22: Uygulama 5 için uç cihaz VLAN topolojisi

Adım 1: Görsel 7.22'deki ağ haritasını simülasyon programında oluşturunuz.

Adım 2: Tablo 7.4'te verilen IP adreslerini ve anahtar arayüz bağlantılarını gerçekleştiriniz. İki anahtar cihaz arasındaki bağlantıyı iki cihazda da **fastethernet0/24.** arayüzden yapınız.

Tablo 7.4: Uygulama 5 İçin Uç Cihaz IP ve Anahtar Arayüz Tablosu

PC	IP	Anahtar Cihaz	Arayüz
PC0	192.168.0.10	Switch0	Fa0/1
Laptop0	192.168.0.11	Switch0	Fa0/2
Laptop1	172.24.1.10	Switch0	Fa0/11
Server0	172.24.1.11	Switch0	Fa0/12
PC1	192.168.0.12	Switch1	Fa0/1
Laptop2	192.168.0.13	Switch1	Fa0/2
PC2	172.24.1.12	Switch1	Fa0/11
Printer	172.24.1.13	Switch1	Fa0/12

Adım 3: Tablo 7.5'teki bilgilerle anahtarlama cihazlarının VLAN yapılandırmalarını yapınız.

Tablo 7.5: Uygulama 5 İçin VLAN Tablosu

Anahtar Cihaz	VLAN Numara ve Adı	Arayüzler
Switch0	vlan 100, name SariGrup	Fa0/1,2,3,4,5
Switch0	vlan 200, name TuruncuGrup	Fa0/11,12,13,14,15
Switch1	vlan 100, name SariGrup	Fa0/1,2,3,4,5
Switch1	vlan 200, name TuruncuGrup	Fa0/11,12,13,14,15

Adım 4: Her iki anahtar cihazda VLAN'lar için aşağıdaki yapılandırmaları gerçekleştiriniz.

```
Switch(config)#vlan 100
Switch(config-vlan)#name SariGrup
Switch(config-vlan)#exit
Switch(config)#vlan 200
Switch(config-vlan)#name TuruncuGrup
Switch(config-vlan)#exit

Switch(config)#interface range fastEthernet 0/1-5
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 100
Switch(config-if-range)#exit
Switch(config)#interface range fastEthernet 0/11-15
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 200
Switch(config-if-range)#exit
```

Adım 5: Anahtarlarınızda VLAN'ları görmek için "show vlan" komutunu uygulayınız.

Adım 6: PC0 ve PC1, Laptop1 ve PC2 arasında iletişim testini ping komutu ile gerçekleştiriniz. Testin, *"Request time out"* cevabı döndürdüğü görülür. İletişim bu aşamada başarısızdır.

Adım 7: VLAN 100 ve VLAN 200 trafiğinin her iki anahtar cihazda gönderimi için fastethernet0/24 arayüzlerini trunk konumuna getiriniz. Bunun için fastethernet0/24 arayüzünde *"switchport mode trunk"* komutu kullanınız.

```
Switch(config)#interface fastEthernet 0/24
Switch(config-if)#switchport mode trunk
```

Adım 8: Anahtarlarda VLAN'ları görmek için tekrar *"show vlan"* komutunu uygulayınız (Görsel 7.23).

```
Switch#sh vlan

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                 Fa0/10, Fa0/16, Fa0/17, Fa0/18
                                                 Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                 Fa0/23, Gig0/1, Gig0/2
100  SariGrup                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5
200  TuruncuGrup                       active    Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                 Fa0/15
```

Görsel 7.23: Anahtar cihazlarda oluşturulmuş VLAN listesi

Dikkat

VLAN tablosunda Fa0/24 arayüzü görülmeyecektir. Fa0/24 belirli bir VLAN'a erişmek için değil tüm VLAN'ların trafiğini aktarmak için ayrılmış bir trunk arayüzdür. Anahtardaki trunk arayüzleri "show interface trunk" komutu ile listelenir.

Adım 9: Anahtar cihazlarda "show interface trunk" komutunu uygulayınız. Görsel 7.24'teki sonuç elde edilir. Bu görsel bize Fa0/24 arayüzünün trunk işlemi için ayrıldığını gösterir.

```
Switch#sh interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/24      on           802.1q         trunking      1
```

Görsel 7.24: Trunk arayüz listesi

Adım 10: PC0 ve PC1, Laptop1 ve PC2 arasında yeniden iletişim testini ping komutu ile gerçekleştiriniz. Testin sonunda "Reply from 192.168.0.12: bytes=32 times=1ms TTL=128" cevabı döndürdüğü görülür ise iletişim başarılı olmuştur. Hata alınıyorsa uygulamayı kontrol edip tekrar deneyiniz.

Adım 11: Simülasyon ortamında sadece ARP paketlerini seçerek PC1'in IP adresini 192.168.0.20 olarak değiştiriniz. ARP paketlerin yayın alanını gözlemleyiniz. ARP paketlerinin Anahtar 1 cihazı VLAN 100 uç cihazlarına PC1 ve Laptop2'ye eriştiği gözlemlenecektir.

7.1.7. Trunk Arayüzler İçin İzin Verilen VLAN Trafiği

Trunk trafiği izin verilen VLAN'lar için filtrelenebilir. Bu güvenlik veya trafik yoğunluğunu düşürmek için yapılan bir uygulama olabilir. İzin komutunda belirtilmeyen VLAN'lar trunk arayüzünün diğer tarafına geçemeyecektir. Anahtar cihazlarında varsayılan olarak tüm VLAN'ların trafiği trunk arayüzlerinde izinlidir.

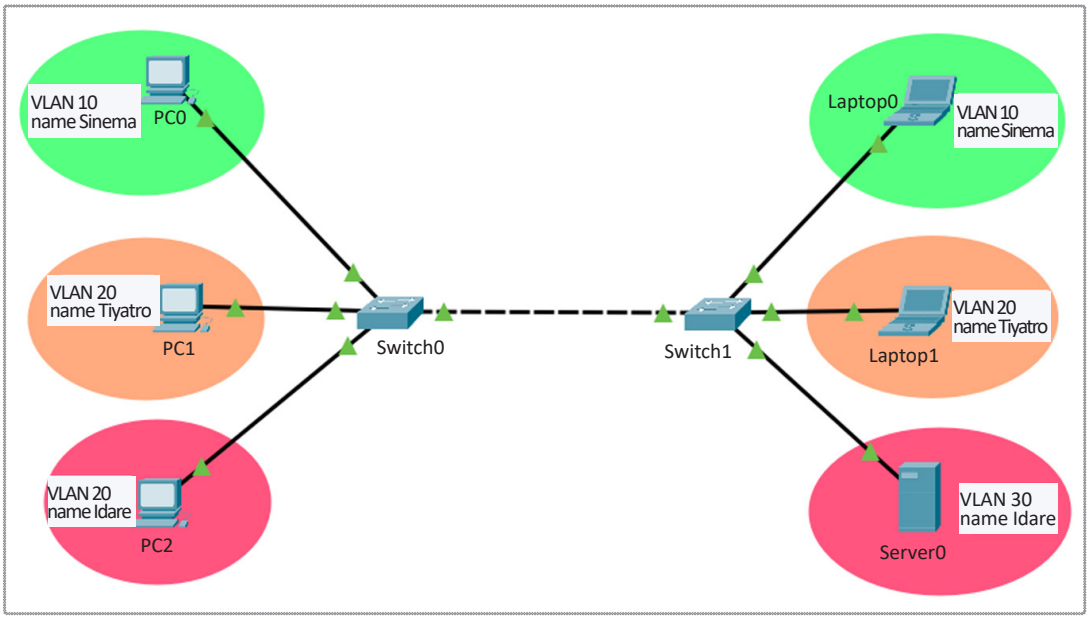
İzin verilen VLAN bildirimi için trunk arayüzünde;

Switch(config-if)#switchport trunk allowed vlan *Numara* komutu kullanılır. Numara ile VLAN numarası yazılır. VLAN numaraları arasına "," koyularak birden fazla VLAN'a izin verilir.

Uygulama 6

http://kitap.eba.gov.tr/KodSor.php?KOD=21051

Görsel 7.25'te verilen topolojiyi gerçek veya simülasyon programında aşağıdaki yönergeler doğrultusunda gerçekleştiriniz. Bilgisayarların IP ve bağlantılarını IP tablosuna uygun olarak belirleyiniz (Tablo 7.6).



Görsel 7.25: Uygulama 6 için uç cihaz VLAN topolojisi

Tablo 7.6: Uygulama 6 İçin Uç Cihaz IP ve Anahtar Arayüz Tablosu

Bilgisayar	IP	Anahtar Arayüzü
PC0	192.168.1.10	Fa0/1
PC1	192.168.2.10	Fa0/6
PC2	192.168.3.10	Fa0/11
Laptop0	192.168.1.11	Fa0/1
Laptop1	192.168.2.11	Fa0/6
Server0	192.168.3.11	Fa0/11

Adım 1: Anahtar 1 ve Anahtar 2'de 10, 20 ve 30 VLAN'larını görseldeki isimleri kullanarak oluşturunuz.

```
Switch(config)#vlan 10
Switch(config-vlan)#name Sinema
Switch(config-vlan)#exit
Switch(config)#vlan 20
Switch(config-vlan)#name Tiyatro
Switch(config-vlan)#exit
Switch(config)#vlan 30
Switch(config-vlan)#name Idare
Switch(config-vlan)#exit
```

Adım 2: Her iki anahtar cihazda Tablo 7.7'deki gibi arayüzleri VLAN'larla ilişkilendiriniz.

Tablo 7.7: Uygulama 6 İçin VLAN Tablosu

VLAN	Arayüz
10	Fa0/1,fa0/2,fa0/3,fa0/4,fa0/5
20	Fa0/6,fa0/7,fa0/8,fa0/9,fa0/10
30	Fa0/11,fa0/11,fa0/12,fa0/13,fa0/14,fa0/15

```
Switch(config)#int range fa0/1-5
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 10
Switch(config-if-range)#exit
Switch(config)#int range fa0/6-10
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 20
Switch(config-if-range)#exit
Switch(config)#int range fa0/11-15
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 30
Switch(config-if-range)#exit
```

Adım 3: Her iki anahtar cihazında fa0/24 arayüzü trunk durumunda olacaktır. Bunun için Anahtar 1 cihazında **Switch(config-if)#switchport mode trunk** komutunu uygulayınız.

Adım 4: PC2'den Server0 için ping testi gerçekleştiriniz. İletişim başarılı olacaktır.

Adım 5: Anahtar 1 cihazında sadece VLAN 10 ve 20 trafiğine izin veriniz. Bunun için **Switch(config-if)#switchport trunk allowed vlan 10,20** komutunu kullanınız.

Adım 6: Tekrar PC2 ve Server0 için ping testi gerçekleştiriniz. İletişim bu kez *"Request time out"* cevabı ile başarısız olacaktır. Bunun sebebi Laptop0 ve Server0 cihazlarının VLAN 30'da olması ve VLAN 30 trafiğinin trunk arayüzünde izinli olmamasıdır.

Adım 7: PC0 ve Laptop0, PC1 ve Laptop1 cihazları arasında iletişim testi yapınız. Bu cihazlar VLAN 10 ve 20 ağlarına dâhil oldukları ve trafiklerine izin verildiği için testler başarılı olacaktır.

7.1.8. Anahtar Cihazlarda Arayüz Dinamik Durum Güncellemesi

Anahtar cihazlarda arayüzler, erişim ve trunk modlarının dışında karşı arayüzün durumuna göre kendini konumlandırma özelliği ile varsayılan olarak yapılandırılır. Bu dinamik trunk protokolü (DTP) ile gerçekleşen bir arayüz işlemidir. Arayüzlerin dinamik olarak yapılandırılması için arayüzde;
Switch(config-if)#switchport mode dynamic auto veya **Switch(config-if)#switchport mode dynamic desirable** komutları kullanılır. Arayüzler dynamic auto ile anahtar cihazlarda varsayılan olarak yapılandırılmıştır.

Anahtar cihazlarda arayüz durum tablosu Tablo 7.8'deki gibidir.

Tablo 7.8: Arayüz Durum Tablosu

Anahtar 1 / Anahtar 2	Dynamic Auto	Dynamic Desirable	Trunk	Access
Dynamic Auto	Access	Trunk	Trunk	Access
Dynamic Desirable	Trunk	Trunk	Trunk	Access
Trunk	Trunk	Trunk	Trunk	Önerilmez
Access	Access	Access	Önerilmez	Access

Uygulama 7

Görsel 7.26'daki topolojiyi aşağıdaki yönergeler doğrultusunda gerçekleştiriniz.

Görsel 7.26: Değişen arayüz durumları örneği topolojisi örneği

Adım 1: Anahtar 1 ve Anahtar 2 cihazlarını Anahtar 1 fa0/21 ve Anahtar 2 fa0/22 arayüzlerinden bağlantı yapınız.

Adım2: Anahtar 1 fa0/21 arayüzünü trunk olarak yapılandırınız.

```
Switch(config)#interface fastEthernet 0/21
Switch(config-if)#switchport mode trunk
```

Adım 3: Anahtar 2 cihazında "show interface trunk" komutunu uygulayınız. Görsel 7.27'deki trunk arayüzleri tablosu görülecektir.

```
Switch#sh interface trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/22      auto         n-802.1q       trunking      1
```

Görsel 7.27: Otomatik uyarlanmış trunk arayüzleri listesi

Anahtar 2 cihazı fa0/22 arayüzünde trunk yapılandırılmamış olmasına rağmen otomatik olarak trunk durumuna geçiş yaptığı görülür. Otomatik olarak öğrenilmiş trunk arayüzleri auto durumunda ve n-802.1q ile tabloda belirtilir.

Adım 4: Anahtar 1 cihazı fa0/21 arayüzünü *"switchport mode access"* komutu ile erişim durumuna getiriniz.

Adım 5: Anahtar 2 cihazında tekrar "show interface trunk" komutunu kullanınız. Bu kez Arayüz tablosu boş bir şekilde görülecektir. Bunun sebebi Anahtar 1 cihazda 21. arayüz erişim durumuna gelirse Anahtar 2 cihazında kendisini otomatik olarak erişim durumuna taşıyacaktır.

7.1.9. Yönetim VLAN'ları ve VLAN Arayüzleri

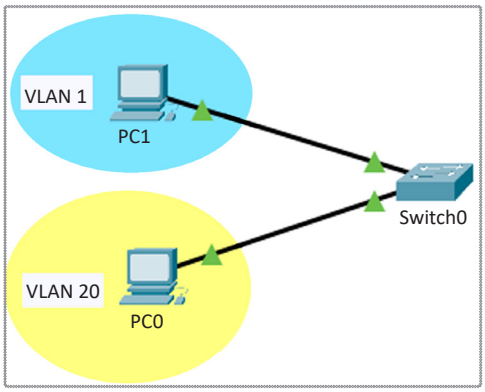
VLAN ağlarında uç cihazların anahtar cihazına erişimi ve yönetimi için VLAN arayüzleri oluşturulur. Bu arayüzler tıpkı VLAN'lar gibi fiziksel olmayıp sanaldır ve IP adresi atanabilir. Bu IP adresi üzerinden anahtar cihazla iletişim kurulabilir. Anahtar cihazlarda fiziksel arayüzler IP adresi alamaz, anahtar cihazın yönetimi için VLAN arayüz yapılandırmalarına IP adresi atanması gerekir.

VLAN'lara IP adresi atamak için *"interface vlan Numara"* komutu ile VLAN arayüzüne giriş yapılmalıdır. Ardından "ip address" komutu ile IP adresi ve alt ağ maskesi girişi yapılmalıdır.

Uygulama 8

http://kitap.eba.gov.tr/KodSor.php?KOD=21052

Görsel 7.28'deki topolojiyi, VLAN ve IP tablosundaki (Tablo 7.9) verilerle aşağıdaki yönergeler doğrultusunda gerçekleştiriniz.



Görsel 7.28: Uygulama 8 için uç cihaz VLAN topolojisi

Tablo 7.9: VLAN Arayüz ve IP Tablosu

VLAN	Arayüzler	IP Adresi
Vlan 1	Fa0/1-Fa0/19	192.168.1.2
Vlan 20	Fa0/20-Fa0/24	192.168.20.2

Tablo 7.10: Uygulama 8 İçin Uç Cihaz IP ve Anahtar Arayüz Tablosu

PC	Arayüzler	IP Adresi
PC1	Fa0/1	192.168.1.10
PC0	Fa0/20	192.168.20.10

Adım 1: PC0 ve PC1 cihazlarını Tablo 7.10'da verilen anahtar arayüzlerine bağlayınız ve IP atamalarını yapınız.

Adım 2: Anahtar cihazında VLAN 1 arayüzüne girip 192.168.1.2 IP adresini ve 255.255.255.0 alt ağ maskesini atayınız.

```
Switch(config)#interface vlan 1
Switch(config-if)#ip address 192.168.1.2 255.255.255.0
```

Adım 3: Anahtar cihazında VLAN 20 arayüzüne girip 192.168.20.2 IP adresini ve 255.255.255.0 alt ağ maskesini atayınız.

```
Switch(config)#interface vlan 20
Switch(config-if)#ip address192.168.20.2 255.255.255.0
```

Dikkat

Bu adımdan önce VLAN 20 oluşturulmamıştır. Doğrudan interface vlan 20 komutu uygulandığında anahtar cihazınız VLAN 20'yi otomatik olarak oluşturacaktır.

Adım 4: Fa0/1 ile Fa0/19 aralığındaki tüm arayüzleri VLAN 1'e, fa0/20 ile fa0/24 aralığındaki arayüzleri ise VLAN 20'ye dâhil ediniz.

```
Switch(config)#interface range fa0/1-19
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 1

Switch(config)#interface range fa0/20-24
Switch(config-if)#switchport mode access
Switch(config-if)#switchport Access vlan 20
```

Adım 5: PC0'dan 192.168.20.2 IP adresi ile anahtar cihazına, PC1'den 192.168.1.2 IP adresi ile anahtar cihazına ping komutu ile iletişim testi gerçekleştiriniz.

Adım 6: Anahtar cihazında uzaktan erişimleri açmak için aşağıdaki komutları giriniz.

```
Switch(config)#line vty 0 4
Switch(config-line)#password 1234
Switch(config-line)#login
```

Adım 7: PC0'dan ve PC1'den sırası ile anahtar cihazına "telnet 192.168.1.2" ve "telnet 192.168.20.2" komutları ile uzaktan erişim gerçekleştiriniz. Erişim parolası 1234 olacaktır.

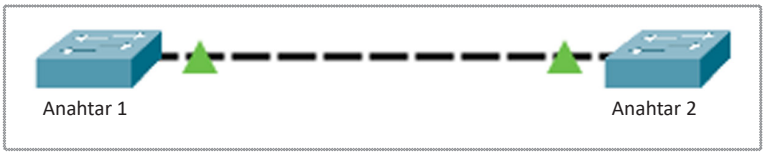
7.1.10. VTP [VLAN Trunking Protocol (Sanal Yerel Ağ Aktarım Protokolü)]

VTP, çoklu anahtar sistemlerinde VLAN'ları trunk arayüzleri üzerinden diğer anahtar cihazlarına aktarmak için kullanılan protokoldür. Protokolün amacı sadece bir anahtarda VLAN'ları oluşturmak ve diğer anahtar cihazlara VLAN'ları aktarmaktır. Böylelikle diğer anahtar cihazlarda VLAN oluşturmaya gerek kalmayacaktır. VTP alanına girecek anahtarlardan biri VLAN aktarımı için sunucu, diğerleri ise VLAN alımı için istemci rolündedir. VTP aktarımı için bir etki alanı ve bu etki alanına girmek için bir parola gereklidir.

Uygulama 9

http://kitap.eba.gov.tr/KodSor.php?KOD=21053

Görsel 7.29'daki topolojiyi aşağıdaki yönergeler doğrultusunda gerçekleştiriniz.



Görsel 7.29: VTP VLAN aktarım topolojisi örneği

Tablo 7.11: Uygulama 9 İçin VLAN Tablosu

VLAN	Adı
vlan 10	Satis
vlan 20	Danisma
vlan 30	Yonetim

Adım 1: Anahtar 1 cihazında Tablo 7.11' de verilen VLAN'ları oluşturunuz.

```
Anahtar1 (config)#vlan 10
Anahtar1 (config-vlan)#name Satis
Anahtar1 (config)#exit
Anahtar1(config)#vlan 20
Anahtar1 (config-vlan)#name Danisma
Anahtar1 (config)#exit
Anahtar1 (config)#vlan 30
Anahtar1 (config-vlan)#name Yonetim
Anahtar1 (config)#exit
```

Adım 2: Anahtar 1 cihaz VLAN'ları aktaracak taraf, Anahtar 2 ise VLAN'ları alıcı taraftır. VTP yapılandırmasında etki adı anahtar.sw olacaktır. VTP parolası ise 123456'dır. Buna göre Anahtar 1 cihazda **vt server** yapılandırmasını yapınız.

Anahtar1(config)#vtp domain *anahtar.sw* komutuyla anahtar.sw adında bir etki alanı oluşturulur.
Anahtar1(config)#vtp password *123456* komutuyla etki alanı için 123456 parolası oluşturulur. Bu komutla yalnızca parola bilgisine sahip anahtarlar etki alanından yararlanabilir.

Anahtar1(config)#vtp mode server komutuyla anahtarın VTP etki alanı içindeki rolü belirlenir. Anahtar 1 için rol "server" şeklindedir.

Adım 3: Anahtar 2'de VTP client yapılandırmasını yapınız.

```
Anahtar2(config)#vtp domain anahtar.sw
Anahtar2(config)#vtp password 123456
Anahtar2(config)#vtp mode client
```

Adım 4: Anahtar 2 cihazında "show vlan" komutunu uygulayıp VLAN tablosunu görüntüleyiniz (Görsel 7.30).

```
Switch#sh vlan

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                 Fa0/21, Fa0/22, Fa0/23, Gig0/1
                                                 Gig0/2
10   Satis                             active
20   Danisma                           active
30   Yonetim                           active
1002 fddi-default                      active
```

Görsel 7.30: Anahtar cihazda oluşturulmuş VLAN listesi

Tabloda görüldüğü gibi 10, 20 ve 30 VLAN'ları VTP ile Anahtar 2 cihazına aktarılmıştır.

7.1.11. VLAN Veri Tabanını Silme

Anahtar cihazlarda VLAN bilgisi startup.config dosyasına yazılmaz. VLAN bilgileri cihazın flash (flaş) belleğine yazılır. VLAN'ları silme ve güncelleme işlemi komutla yapılabileceği gibi doğrudan cihaz flash belleği üzerinden topluca yapılabilir. VLAN veri tabanı dosyası silinirse yeni VLAN'lar oluşturulduğunda yeniden flash bellekte VLAN veri tabanı yazılır. VLAN veri tabanı dosyası cihaz flash belleğinde "vlan.dat" dosya adı ile tutulur.

Uygulama 10

Anahtar cihazdaki VLAN veri tabanı dosyasını görüntüleme ve silme işlemini aşağıdaki yönergeler doğrultusunda gerçekleştiriniz.

Adım 1: Anahtar cihazda VLAN 10, 20 ve 30 ağlarını sırası ile oda1, oda2, oda3 adı ile oluşturunuz.

```
Anahtar1 (config)#vlan 10
Anahtar1 (config-vlan)#name oda1
Anahtar1 (config)#exit
Anahtar1(config)#vlan 20
Anahtar1 (config-vlan)#name oda2
Anahtar1 (config)#exit
Anahtar1 (config)#vlan 30
Anahtar1 (config-vlan)#name oda3
Anahtar1 (config)#exit
```

Adım 2: Anahtar cihazda flash bellek içeriğini "show flash:" komutu ile görüntüleyiniz (Görsel 7.31).

```
Switch#sh flash:
Directory of flash:/

    1  -rw-     4414921          <no date>  c2960-lanbase-mz.122-25.FX.bin
    2  -rw-         736          <no date>  vlan.dat

64016384 bytes total (59600727 bytes free)
```

Görsel 7.31: Anahtar cihazda flash bellek dosya listesi

Görselde VLAN kayıtlarının tutulduğu "vlan.dat" dosyası görülür.

Adım 3: Anahtar cihazında "vlan.dat" dosyasını siliniz.

```
Anahtar1 #delete flash:vlan.dat
```

Adım 4: Cihazı "reload" komutu ile yeniden başlatınız ve "show vlan" komutu ile VLAN tablosunda daha önce oluşturulan VLAN'ların olmadığını teyit ediniz.

7.2. VLAN'lar Arası Yönlendirme

7.2.1. Yönlendirme

Farklı mantıksal ağlar arasındaki trafiğin aktarılması işlemine **yönlendirme**, trafiğin kontrolünü gerçekleştiren cihazlara ise **yönlendirici cihazlar** denir. VLAN'lar anahtarlama cihazlarında farklı mantıksal ağlardan oluştuğundan aralarında veri aktarımı için bir yönlendirici cihaza ihtiyaç duyar. VLAN'ların mantıksal ağlarla bölünmesi sadece farklı ağlardaki cihazların birbirinden tamamen ayrılması için değildir. Yönlendirme ile farklı VLAN'lardaki cihazlar birbirleri ile daha güvenli iletişim kurabilir. Güvenliğin artmasındaki bir sebep de VLAN trafiklerinin karşı tarafa aktarılmasında uç cihazların MAC adreslerinin gizlenmesidir.

7.2.2. Yönlendirici Cihazda Farklı Fiziksel Arayüzler ile VLAN Yönlendirme

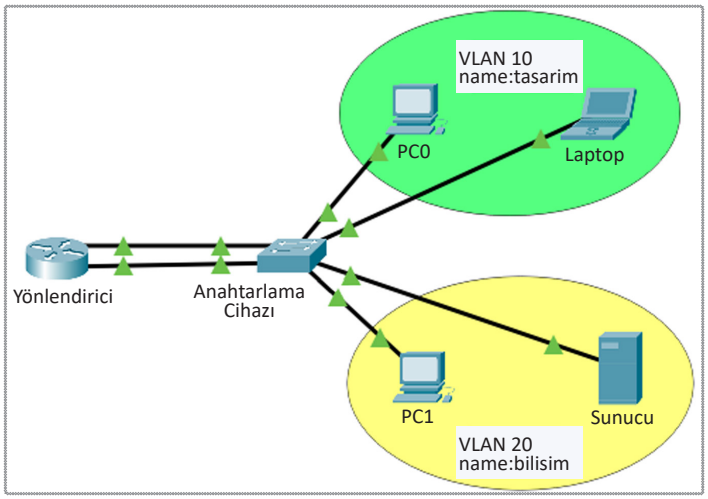
Yönlendirici cihazlarda tıpkı anahtar cihazlarda olduğu gibi Ethernet II protokolü ile konuşabilen yerel ağ bağlantı arayüzleri vardır. Ancak bu arayüzlerin sayısı anahtar cihazlara göre oldukça sınırlıdır ve her yerel ağ için

bir tane arayüz bulunur. Farklı VLAN trafiğinin bu arayüzlere fiziksel olarak bağlanması ve yönlendirici cihazda ilgili arayüzlere uygun mantıksal IP'ler tanımlanması gerekir. Yerel ağlardaki uç cihazlarda ise yönlendirici arayüz IP'sinin varsayılan ağ geçidi olarak tanımlı olması gerekmektedir.

Uygulama 11

http://kitap.eba.gov.tr/KodSor.php?KOD=21054

Görsel 7.32'deki topolojiyi VLAN (Tablo 7.12) ve IP (Tablo 7.13) tablolarında verilen bilgilerle aşağıdaki yönergeler doğrultusunda gerçekleştiriniz.



Görsel 7.32: Uygulama 11 için uç cihaz VLAN topolojisi

Tablo 7.12: Uygulama 11 İçin VLAN Tablosu

VLAN	Name	Arayüzler
Vlan 10	tasarim	Fa0/1-fa0/10 arası
Vlan 20	bilisim	Fa0/11-fa0/20 arası

Tablo 7.13: Uygulama 11 İçin Uç Cihaz IP ve Anahtar Arayüz Tablosu

Cihaz	IP	Alt Ağ Maskesi	Varsayılan Ağ Geçidi	Anahtar Arayüzü
Yönlendirici Arayüz g0/0	192.168.0.1	255.255.255.0		Fa0/1
Yönlendirici Arayüz g0/1	192.168.1.1	255.255.255.0		Fa0/11
PC0	192.168.0.2	255.255.255.0	192.168.0.1	Fa0/2
Laptop	192.168.0.3	255.255.255.0	192.168.0.1	Fa0/3
PC1	192.168.1.2	255.255.255.0	192.168.1.1	Fa0/12
Sunucu	192.168.1.3	255.255.255.0	192.168.1.1	Fa0/13

Adım 1: Anahtar cihazında VLAN 10 ve VLAN 20'yi oluşturunuz.

```
Anahtar1 (config)#vlan 10
Anahtar1 (config-vlan)#name tasarim
Anahtar1 (config)#exit
Anahtar1(config)#vlan 20
Anahtar1 (config-vlan)#name bilisim
Anahtar1 (config)#exit
```

Adım 2: Anahtar cihazında ilgili arayüzleri VLAN'lara dâhil ediniz.

```
Anahtar1 (config)# interface range fa0/1-10
Anahtar1 (config-if-range)#switchport mode access
Anahtar1 (config-if-range)#switchport access vlan 10
Anahtar1 (config-if-range)#exit
Anahtar1 (config)# interface range fa0/11-20
Anahtar1 (config-if-range)#switchport mode access
Anahtar1 (config-if-range)#switchport access vlan 20
Anahtar1 (config-if-range)#exit
```

Adım 3: Uç cihazlarda IP tablosunda (Tablo 7.13) olduğu gibi IP girişlerini yapınız.

Dikkat

Uç cihazların diğer ağlar ile görüşebilmesi için ağ trafiğini diğer ağlara yönlendirecek yönlendirme cihazının IP adresini bilmesi gerekir. Uç cihazlarda yönlendirici IP adresi "varsayılan ağ geçidi" olarak tanımlanır.

Adım 4: Yönlendirici cihazda IP tablosunda olduğu gibi IP girişlerini yapınız. Örneğimizdeki yönlendirici cihazda iki tane arayüz bulunmaktadır. Bu arayüzler sırası ile VLAN 10 ve VLAN 20 ile aynı mantıksal ağ grubunda olacaktır.

```
Router(config)#interface gigabitEthernet 0/0
Router(config-if)#ip address 192.168.0.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#interface gigabitEthernet 0/1
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
```

Dikkat

Yönlendirici cihazlarda varsayılan olarak arayüzler kapalı tanımlanmıştır. IP adresi tanımladıktan sonra arayüzü açmak gerekir. Arayüzü açık hâle getirmek için "no shutdown" komutu kullanılır.

Adım 5: PC0 ile PC1 arasında ping iletişim testi gerçekleştiriniz. İletişimin başarılı olduğu görülecektir (Görsel 7.33).

```
C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time<1ms TTL=127
Reply from 192.168.1.2: bytes=32 time<1ms TTL=127
Reply from 192.168.1.2: bytes=32 time<1ms TTL=127
Reply from 192.168.1.2: bytes=32 time=7ms TTL=127
```

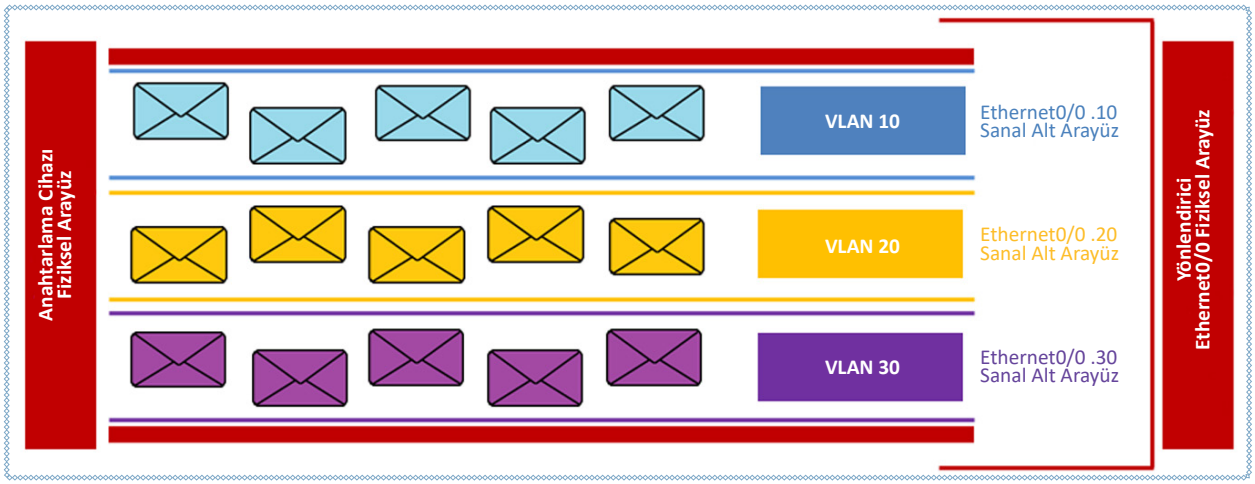
Görsel 7.33: Başarılı ping iletişim testi sonucu

Adım 6: Yönlendirici cihazların anahtara olan bağlantılarını kesiniz ve iletişimi yeniden deneyiniz.

7.2.3. Trunk ile VLAN'lar Arası Yönlendirme

VLAN'lar arasında yönlendirme işleminde her VLAN için yönlendirici arayüzüne fiziksel erişim mümkün olmayabilir. VLAN sayısı arttıkça her VLAN için fiziksel erişim gerekeceğinden yönlendiricide arayüz olmayabilir. Ayrıca bu kablo ve arayüz maliyetinin de artması demektir.

Anahtar cihazlarda arayüzler trunk durumu ile birden fazla VLAN trafiğini aktarabilir. VLAN'lar arası yönlendirme yapılacaksa yine trunk yönteminden yararlanılır. Yönlendiriciye gelen trafik yönlendirici arayüzünde her VLAN için alt sanal arayüzler oluşturularak karşılanır (Görsel 7.34).



Görsel 7.34: Yönlendirici cihaz sanal alt arayüzler

Yönlendirici cihazdaki fiziksel arayüz herhangi bir ağ için tanımlanmaz. Anahtar cihazının trunk arayüzünden gelen her VLAN trafiği için bir sanal arayüz oluşturulur ve bu sanal arayüzlerin trunk VLAN trafiğini aktarabilmesi için 802.1q protokolünü konuşabilmesi gerekir.

Yönlendirici cihazda fiziksel arayüzde sanal alt arayüzler oluşturmak için **Router(config)#interface gigabitEthernet 0/0.*10*** komutu yeterlidir. Fiziksel arayüzün isim ve numarasından sonra "." (nokta) ile VLAN için bir alt arayüz numarası belirlenir. Bu komutta bu numara 10'dur. Bu numara VLAN numarası ile aynı olmak zorunda değildir ancak uyum ve anlaşılırlığın artması için aynı numarayı vermek doğru bir kullanım olacaktır.

Alt arayüzün trunk trafiğini aktarabilmesi için **Router(config-subif)#encapsulation dot1q *10*** komutu kullanılır. Bu komut alt arayüzü 802.1q protokolünü konuşmaya hazır hâle getirir. "encapsulation dot1q" komutundan sonra girilen numara alt arayüzün konuşacağı VLAN'ın numarası ile aynı olmak zorundadır. Bu komut satırında VLAN 10 için dot1q numarası 10 olmalıdır.

VLAN ile konuşabilmesi için alt arayüzde bir IP adres bilgisi gereklidir. Bu IP adresi aynı zamanda VLAN'daki cihazların varsayılan ağ geçidi olacaktır.

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

Yönlendiricide alt arayüz oluşturma işlemi trunk hattından gelen yönlendirme yapılacak tüm VLAN'lar için yapılmalıdır.

Sanal alt arayüzlerin aktif olabilmesi için alt arayüzün içinde olduğu fiziksel arayüzün açık konumda olması gerekir.

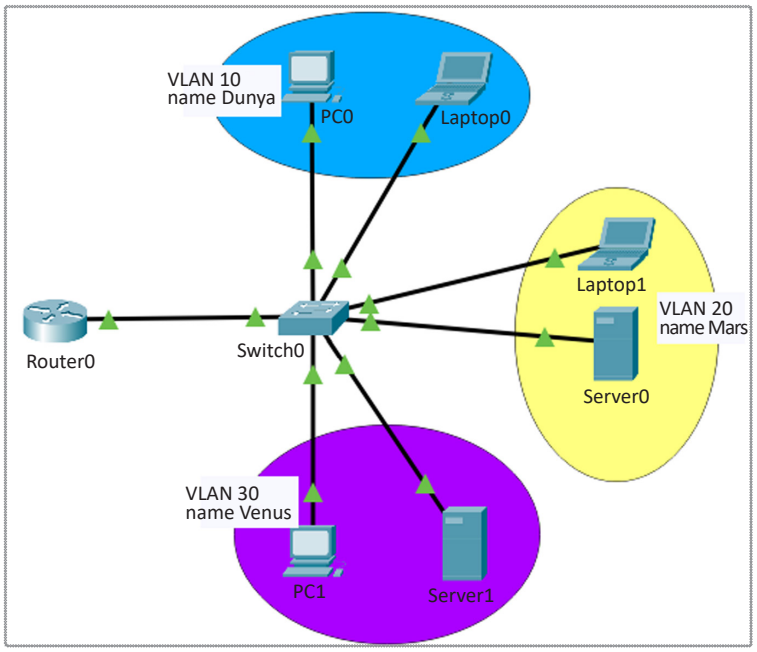
Router(config)#interface gigabitEthernet 0/0

Router(config)#no shutdown komutuyla fiziksel arayüz, tüm alt arayüzler için açık konuma gelir. Alt arayüzlerde tek tek açma işlemi yapılmaz. Fiziksel arayüze herhangi bir IP adresi yazılmaz.

Uygulama 12

http://kitap.eba.gov.tr/KodSor.php?KOD=21056

Görsel 7.35'teki topolojiyi, VLAN ve IP tablosunda verilen bilgilerle aşağıdaki yönergeler doğrultusunda gerçekleştiriniz.



Görsel 7.35: Uygulama 12 için uç cihaz VLAN topolojisi

Adım 1: Aşağıdaki VLAN tablosuna (Tablo 7.14) göre anahtarlama cihazında VLAN'ları oluşturunuz ve arayüzleri ilgili VLAN'lara dâhil ediniz.

Tablo 7.14: Uygulama 12 İçin VLAN Tablosu

VLAN	Name	Arayüzler
vlan 10	Dunya	Fa0/1-fa0/5 arası
vlan 20	Mars	Fa0/1-fa0/5 arası
vlan 30	Venus	Fa0/11-fa0/15 arası

```
Switch(config)#vlan 10
Switch (config-vlan)#name Dunya
Switch (config)#exit
Switch (config)#vlan 20
Switch (config-vlan)#name Mars
Switch (config)#exit
Switch (config)#vlan 30

Switch (config-vlan)#name Venus
Switch (config)#exit

Switch (config)# interface range fa0/1-5
Switch (config-if-range)#switchport mode access
Switch (config-if-range)#switchport access vlan 10
Switch (config-if-range)#exit
```

```
Switch (config)# interface range fa0/6-10
Switch (config-if-range)#switchport mode access
Switch (config-if-range)#switchport access vlan 20
Switch (config-if-range)#exit
Switch (config)# interface range fa0/11-15
Switch (config-if-range)#switchport mode access
Switch (config-if-range)#switchport access vlan 30
Switch (config-if-range)#exit
```

Adım 2: Anahtarlama cihazında fa0/24 arayüzü trunk trafiği aktarımı için yapılandırınız.

```
Switch (config)#interface fa0/24
Switch (config-if-range)#switchport mode trunk
```

Adım 3: Tablo 7.15' e göre yönlendirici ve uç cihazlarda IP yapılandırmasını yapınız.

Tablo 7.15: Uygulama 12 İçin Uç Cihaz IP ve Anahtar Arayüz Tablosu

Cihaz	IP	Alt Ağ Maskesi	Varsayılan Ağ Geçidi	Anahtar Arayüzü
Yönlendirici g0/0.10	192.168.1.1	255.255.255.0		Fa0/24
Yönlendirici g0/0.20	192.168.2.1	255.255.255.0		Fa0/24
Yönlendirici g0/0.30	192.168.3.1	255.255.255.0		Fa0/24
PC0	192.168.1.2	255.255.255.0	192.168.1.1	Fa0/1
Laptop0	192.168.1.3	255.255.255.0	192.168.1.1	Fa0/2
Laptop1	192.168.2.2	255.255.255.0	192.168.2.1	Fa0/6
Server0	192.168.2.3	255.255.255.0	192.168.2.1	Fa0/7
PC1	192.168.3.2	255.255.255.0	192.168.3.1	Fa0/11
Server1	192.168.3.3	255.255.255.0	192.168.3.1	Fa0/12

Adım 4: Yönlendiricide trunk trafiği için tabloda verilen sanal alt arayüzleri oluşturunuz.

```
Router(config)#interface g0/0
Router(config-if)#no shutdown
Router(config)#interface g0/0.10
Router(config-subif)#encapsulation dot1q 10
Router(config-subif)#ip address 192.168.1.1 255.255.255.0
Router(config-subif)#exit

Router(config)#interface g0/0.20
Router(config-subif)#encapsulation dot1q 20
Router(config-subif)#ip address 192.168.2.1 255.255.255.0
Router(config-subif)#exit
Router(config)#interface g0/0.30
Router(config-subif)#encapsulation dot1q 30
Router(config-subif)#ip address 192.168.3.1 255.255.255.0
Router(config-subif)#exit
```

Sıra Sizde

Farklı VLAN içindeki uç cihazlardan ping komutu ile iletişim testi gerçekleştiriniz. Arkadaşınızla birlikte iletişim testinin nasıl gerçekleştiğini uygulama adımları şeklinde yazınız ve uygulayınız.

Aşağıdaki soruları dikkatlice okuyunuz ve doğru seçeneği işaretleyiniz.

1. Aşağıdakilerden hangisi VLAN kullanımının bir avantajı olarak kabul edilemez?

A) Trafiği azaltarak performansı artırır.
B) Bağımsız mantıksal alanlar oluşturarak güvenliği artırır.
C) Anahtarda yayın alanları oluşturarak farklı VLAN trafiklerini izole eder.
D) Yayın alanları içinde bulunan bilgisayarların otomatik IP ihtiyaçlarını karşılar.
E) Farklı yayın alanları oluşturarak yeni anahtar gereksinimini ve maliyeti azaltır.

2. Aşağıdakilerden hangisi bir VLAN türü değildir?

A) Data B) Default C) Native D) Trunk E) Yönetim

3. Anahtar arayüzlerinin VLAN erişim durumu varsayılan olarak aşağıdakilerden hangisidir?

A) Access
B) Dynamic Auto
C) Dynamic Desirable
D) Native
E) Trunk

4. Anahtar cihazlarda farklı VLAN trafiğinin aktarımını sağlayan trunk durumunun kullandığı protokol aşağıdakilerden hangisidir?

A) Ethernet II B) 802.1q C) 802.11b D) 802.11g E) 802.11n

5. Anahtar cihazda VLAN 1, 10, 20, 30, 40 var ise aşağıdaki komut satırlarından hangisi ile sadece 30. VLAN trafiğinin trunk arayüzünden geçişine izin verilmez?

A) switchport trunk allowed vlan 1
B) switchport trunk allowed vlan 30
C) switchport access vlan 30
D) switchport access vlan 1,10,20,40
E) switchport trunk allowed vlan 1,10,20,40

6. Aşağıdaki protokollerden hangisi ile merkezî bir anahtar cihazdan diğer anahtar cihazlar arasında VLAN bilgisi aktarımı yapılır?

A) ARP B) CDP C) DNS D) DTP E) VTP

7. VLAN bilgilerinin tutulduğu vlan.dat dosyasının tutulduğu bellek aşağıdakilerden hangisidir?

A) Flash B) ROM C) RAM D) NVRAM E) Haricî hard disk

8. Farklı VLAN'lar arasında trafiğin aktarımı için kullanılabilecek ağ cihazı aşağıdakilerden hangisidir?

A) Anahtar
B) Dağıtıcı
C) Erişim noktası
D) Güvenlik duvarı
E) Yönlendirici

9. Yönlendirici alt arayüzünü trunk protokolünü konuşmaya hazırlayan komut aşağıdakilerden hangisidir?

A) encapsulation dot1q VlanID
B) switchport mode trunk
C) switchport mode access
D) switchport mode dynamic auto
E) switchport mode dynamic desirable

10. Aşağıdaki komutlardan hangisi ile anahtar cihaz VLAN veri tabanı silinebilir?

A) erase flash:vlan.dat
B) erase startup-config
C) delete flash:vlan.dat
D) delete startup-config
E) delete running-config

ÖĞRENME BİRİMİ 8

LAN YEDEKLİLİĞİ

NELER ÖĞRENECEKSİNİZ?

Bu öğrenme birimi ile;

- Ağ içinde yedekli yollara neden gereksinim duyulduğunu bilecek,
- Yedekli yol bağlantılarının uygulaması esnasında oluşabilecek zafiyetleri öğrenecek,
- Zafiyetlere karşı geliştirilen ağ protokollerini bilecek,
- STP protokollerinin çalışma prensiplerini kavrayacak,
- Yedekli yol tasarımlarında tercih ve yedek yolların nasıl belirlendiğini bilecek,
- Yedek anahtarlı topolojilerde temel köprü anahtar seçimlerini yapacak,
- Anahtar cihazlarında arayüz yol maliyetinin belirlenmesi ve yedek yol seçimindeki rolünü bilecek,
- Daha fazla bant genişliği ve aktarım hızına erişebilmek için bağlantı kümelemeyi yapacak,
- Kümeleme yöntemlerini tanıyacak ve uygulamalarını gerçekleştireceksiniz.

ANAHTAR KELİMELER

MAC tutarsızlığı, Broadcast Storm, yayın fırtınaları, SpanningTree Protokol, STP, RSPT, BPDU, PVST, Root Bridge, köprü anahtar, Root Port, Designated Port, Alternate Port, bağlantı kümeleme, Etherchannel, LACP, PAgP

Hazırlık Çalışmaları

1. Ağınız için çok önemli iki anahtar cihaz arasında kablo bağlantınızın kopma ihtimali karşısında hangi tedbirleri alırsınız?
2. Anahtarlar arasında bant genişliği ve iletim hızının katlanarak artırılması için neler yapılabilir?

8.1. Yedeklilik Tasarımlarının Yapılması

Veri iletiminin ağ içinde devamlılığı, anahtar cihazlarına eşit yük dağılımı, performans, bant genişliği gereksinimlerinden kaynaklı ideal yedekli ağ tasarımlarına ihtiyaç duyulur. Bu gereksinimlerin yanı sıra maliyet ve zafiyetler de gözetilerek ideal ağ tasarımları gerçekleştirilir.

8.1.1. Yedekleme Gereksinimleri

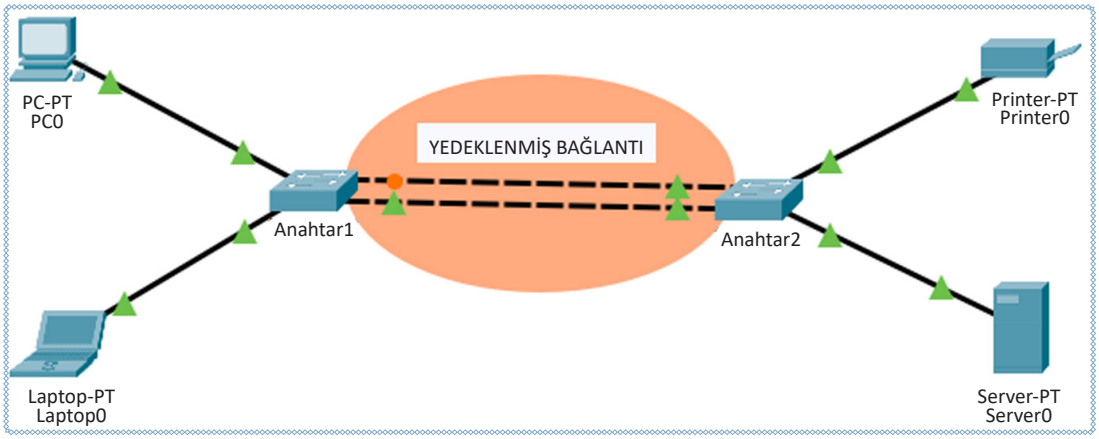
Ağlarda iletişim devamlılığı için fiziksel bağlantı kesilmelerine veya arayüz arızalarına karşı tedbirlerin geliştirilmesi gerekir. Bu tedbirlerin başında, fiziksel kablo bağlantılarının yedeklerinin oluşturulması gelmektedir. Ana bağlantılarda meydana gelebilecek bir arıza durumunda yedek bağlantı aktif hâle gelir ağların iletişimi kesintisiz devam eder. Yedekleme ağa katılmış istemci ve sunucu bilgisayarlarının hizmet alımlarının aksamamasını sağlayıp ağa olan güvenilirliği artıracaktır.

Yedekli yol kullanımı, ağın bant genişliğini artırmak için de kullanılan bir yöntemdir.

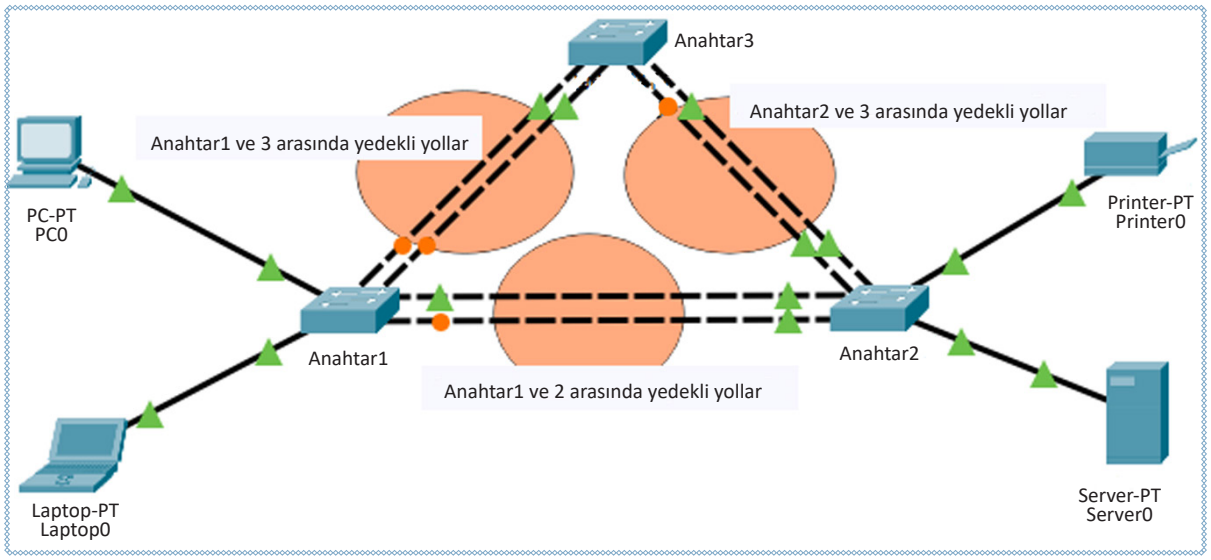
8.1.2. Yedekleme Tasarımları

Ağların önemi, yolun fiziksel problemleri, güvenlik, kritik anahtarlar arasında bağlantı, cihazlar arasında dengeli yük dağılımı, bant genişliği yükseltilmesi gerekçeleri ile yedeklemeler yapılabilir ve yedek yolların sayısında artırımda bulunulabilir. İki veya daha fazla kablo bağlantısı ve cihaz ile yedek bağlantılar çoğaltılabilir ancak her bağlantı aynı zamanda yedekleme zafiyetlerini ve maliyeti de artırır. Tüm etkenler göz önüne alınarak uygun yedekleme tasarımları geliştirilir.

Görsel 8.1 ve 8.2'deki topolojilerden anahtarlar arasında yedek bağlantıların kullanımı gösterilmiştir. Bu bağlantılarda simgesel olarak anahtar cihazının her iki ucunda yeşil olan bağlantılar ana bağlantı hattı, turuncu olanlar ise yedek bağlantı hattını göstermektedir.



Görsel 8.1: İki anahtar arasında yedeklenmiş bir bağlantı tasarımı



Görsel 8.2: Üç anahtar arasında yedekli bağlantı tasarımı

8.1.3. Yedekleme Zafiyetleri

Yedekli anahtarlama sistemleri, ağlar için hizmetin aksamaması için gereksinimken beraberinde beklenmedik ağ zafiyetlerini de oluşturabilir. Bu zafiyetler OSI modeli 2. katman sorunlarıdır. Olası sorunlar MAC tutarsızlığı, yayın fırtınaları ve çoklu çerçeve aktarımıdır. Anahtar cihazlarında bu sorunların yaşanmaması için **STP [SpanningTree Protocol (Kapsama Ağacı Protokolü)]** kullanılır.

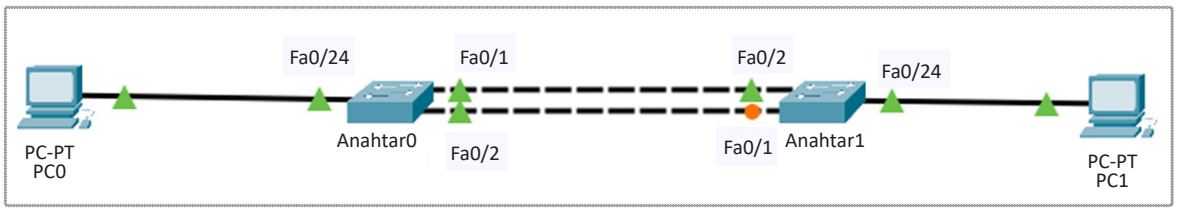
STP, yedek bağlantı hattında veri iletimini engelleyerek tek bağlantı noktasından iletimin akmasını, o iletim noktasında hasar olursa diğer bağlantı noktalarının aktif hâle gelmesini sağlayan bir protokoldür. Anahtar cihazlar, varsayılan olarak STP aktif hâlde çalışır.

8.1.3.1. MAC Tutarsızlığı Zafiyeti

OSI modeline göre 2. katmanda oluşan MAC tutarsızlığı sorunu, yayın paketlerinin ağda tüm anahtarlarda yayılması ve anahtar cihazın gelen yayın paketlerinin kaynak MAC adresine bakarak MAC tablosunda aktif olan alakasız portlara yazabilmesi ile oluşur. Sonuç olarak anahtar, MAC adres tablosunu doğru MAC bilgileri ile oluşturamaz. İlgili MAC, hedef MAC olduğunda MAC tablosu yanlış tutulduğu için yanlış arayüzden paketin iletimini yapmaya çalışır.

Uygulama 1

Görsel 8.3'teki topolojiyi oluşturarak işlemleri aşağıdaki yönergeler doğrultusunda gerçekleştiriniz (Topolojide cihaz bağlantı arayüzleri görselde belirtilmiştir.).



Görsel 8.3: Uygulama 1 için iki anahtar arasında yedekli tasarım

Dikkat

Anahtarlar arasında iki kablo bağlantısı vardır. Bu yollardan bir tanesi pasif durumdadır.

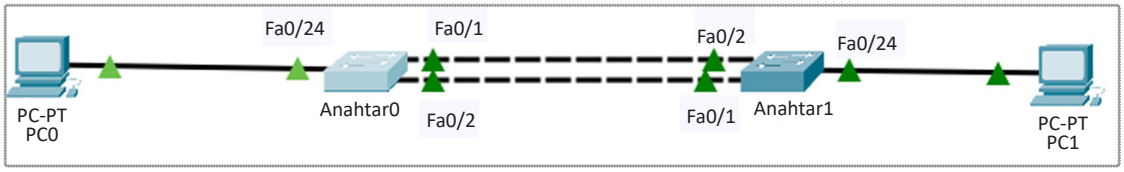
Adım 1: PC0 için 192.168.1.10, PC1 için 192.168.1.11 IP adreslerini el ile giriniz.

Adım 2: Anahtar cihazlar varsayılan olarak yedekleme zafiyetlerinin oluşmaması için STP ile çalışır. Anahar0 ve Anahtar1 cihazlarında STP çalışmasını durdurmak için her iki anahtar cihazda terminal ekranlarını açınız ve aşağıdaki komutları giriniz.

```
Switch(config)#no spanning-tree vlan 1
```

Bilgi

VLAN 1, anahtar cihazda başlangıçta tek sanal ağdır ve anahtar cihazında varsayılan olarak tüm portların dâhil olduğu ağdır. "**no spanning-tree vlan 1**" komutu ile VLAN 1'e dâhil olan tüm portlar STP'den etkilenecektir.



Görsel 8.4: Uygulama 1 için STP olmaksızın iki anahtar arasında yedekli tasarım

Dikkat

Anahtar cihazlarda STP'nin durması ile aynı anda yedek yolunda aktif hâle geldiği görülür (Görsel 8.4).

Adım 3: PC0 MAC adresini PC0 komut ekranından "ipconfig /all" komutu ile öğreniniz (Görsel 8.5).

```
C:\>ipconfig /all

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Physical Address.................: 0050.0F09.375C
   Link-local IPv6 Address.........: FE80::250:FFF:FE09:375C
   IP Address.......................: 192.168.1.10
   Subnet Mask.....................: 255.255.255.0
```

Görsel 8.5: ipconfig /all komutu ile PC MAC adresi öğrenme

Dikkat

Örnekte PC0'ın MAC adresi "0050.0F09.375C"dir. Bu MAC adresi sizlerde farklı olabilir.

Adım 4: PC0'dan PC1'e ping komutu ile iletişim testi yapınız.

Adım 5: Anahtar0 cihazı terminal ekranında "show mac-address-table" komutunu uygulayınız. Anahtar MAC adres tablosu Görsel 8.6'daki gibi olacaktır.

```
Anahtar0#sh mac-address-table
          Mac Address Table
-------------------------------------------

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

   1    0050.0f09.375c    DYNAMIC     Fa0/1
   1    0060.3ebd.8d01    DYNAMIC     Fa0/2
   1    0060.3ebd.8d02    DYNAMIC     Fa0/1
   1    00e0.f752.3d68    DYNAMIC     Fa0/2
```

Görsel 8.6: Uygulama 1 için Anahtar0 cihazında tutarsız MAC tablosu

Dikkat edilirse PC0, anahtar cihazda Fa0/24 arayüzüne bağlıyken anahtar cihaz, PC0 MAC adresini Fa0/1 arayüzüne yazmıştır. Bu istenmedik bir durumdur ve MAC tutarsızlığı gerçekleşmiştir. Bu tutarsızlığın neticesinde hedef MAC adresi PC0'a ait her paket, Anahtar0 cihazında Fa0/24 portu yerine Fa0/1 portundan geri gönderilecektir. Bu sebeple **Adım 4**'teki ping iletişim testi başarısız olacaktır.

Adım 6: Her iki anahtar cihazda "spanning-tree vlan 1" komutu ile STP çalışmasını yeniden **varsayılan etkin** duruma getiriniz.

```
Switch(config)#spanning-tree vlan 1
```

Adım 7: PC0'dan PC1'e ping komutu ile yeniden iletişim testi yapınız.

Adım 8: Anahtar0'da "show mac-address-table" komutunu uygulayınız. Görsel 8.7' deki MAC tablosu, STP ile MAC tutarsızlığının giderilmiş olduğu tablodur. MAC tutarsızlığı ortadan kalktığında **Adım 7**'deki iletişim testi başarılı olacaktır.

```
Anahtar0#sh mac-address-table
          Mac Address Table
-------------------------------------------

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

   1    0050.0f09.375c    DYNAMIC     Fa0/24
   1    0060.3ebd.8d01    DYNAMIC     Fa0/2
   1    00e0.f752.3d68    DYNAMIC     Fa0/1
```

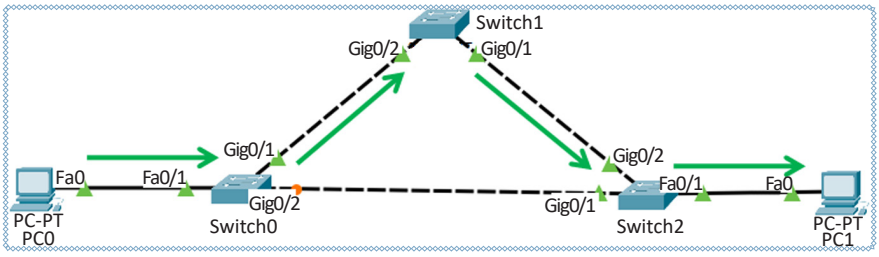
Görsel 8.7: Uygulama 1 için Anahtar0 cihazında tutarlı MAC tablosu

Bilgi

Anahtar cihazlar kendi portlarına bağlı diğer cihazların MAC adreslerini öğrenebilir. MAC adres tablosunda öğrendikleri diğer cihazlara ait MAC adreslerini yazar. Bu işlem OSI modeline göre 2. katmanda ARP veya STP protokolleri ile gerçekleşir.

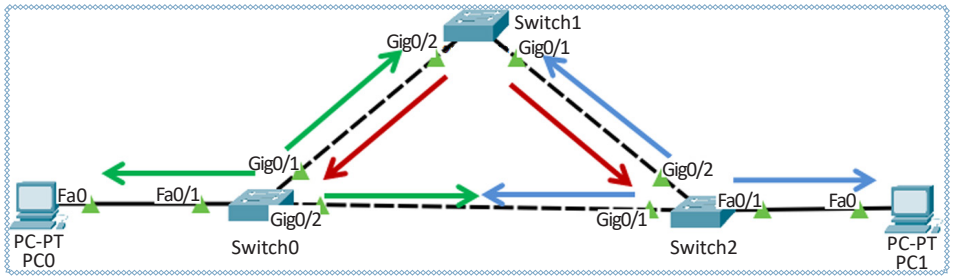
8.1.3.2. Broadcast Storm (Yayın Fırtınaları) Zafiyeti

Yedekli anahtar bağlantılarında hatlardan biri aktif olarak seçilir, diğerleri ise iletişim için pasif konumda olur. Bu kontrollü bir iletişimi sağlayacaktır. STP'nin devre dışı olduğu durumlarda ise yedek bağlantı, ana bağlantı ayrımı ortadan kalkar. Bu durum, özellikle yayın paketlerinin anahtarlar arası iletiminde kaosa sebep olur. Anahtar, gelen yayın paketlerini kendisine bağlı tüm anahtarlara göndermeye çalışır. Paketi alan anahtar, yine kendisine bağlı tüm anahtarlara yayın paketlerini gönderir. Anahtarlar arasında döngüsel olarak birbirlerine yayın paketi gönderimi gerçekleşir. Döngüsel yayın fırtınaları şeklinde adlandırılan bu süreç, ağda ciddi boyutta trafik oluşmasına ve anahtar cihazların işlemcilerine çok fazla yük binmesine sebep olur. Sürecin sonunda hizmet aksamaları ve ağın kullanılamaması gibi olumsuzluklar meydana gelir.



Görsel 8.8: STP algoritması kullanılan bir ağda yayın trafiği

Görsel 8.8'de STP aktif anahtar cihazlar için PC0 merkezli yayın paketlerinin yönü Switch0 cihazından sırası ile Switch1 ve Switch2 şeklindedir. Switch0 ve Switch2 arasındaki yedek yol pasif konumdadır. Yayın trafiğini pasif yollar iletmez.

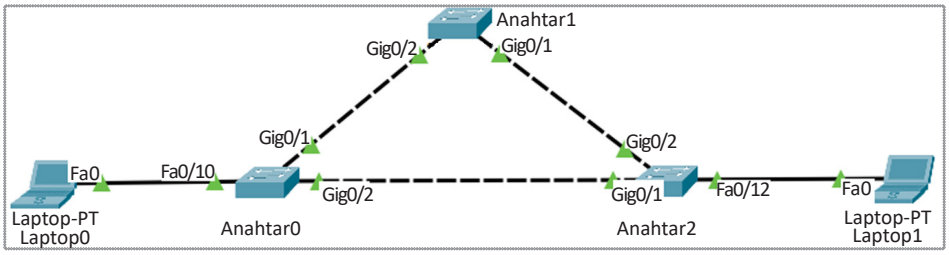


Görsel 8.9: STP algoritması kullanılmadan yayın paketlerinin anahtar cihazlardaki trafiği

Görsel 8.9'da STP devre dışıyken anahtar cihazlarının davranışları gösterilmektedir. Anahtarlarda tüm bağlantılar etkin konumda olduğu için yedek bağlantı tanımlı değildir. Anahtar tüm bağlantılarını etkin kabul edip yayın paketlerini tüm etkin bağlantılardan gönderir. Bu, tüm anahtarlar için tekrarlanan bir döngüye dönüşür.

Uygulama 2

Görsel 8.10'daki topolojiyi simülasyon programında oluşturarak işlemleri aşağıdaki yönergeler doğrultusunda gerçekleştiriniz.

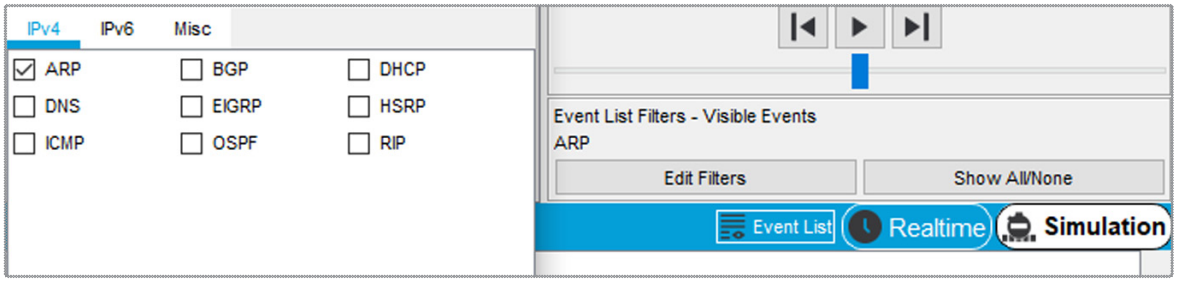


Görsel 8.10: Uygulama 2 STP olmaksızın anahtar yedekliliği topolojisi

Adım 1: Her üç anahtar cihazı terminal ekranında varsayılan olarak etkin bulunan STP'yi devre dışı bırakınız.

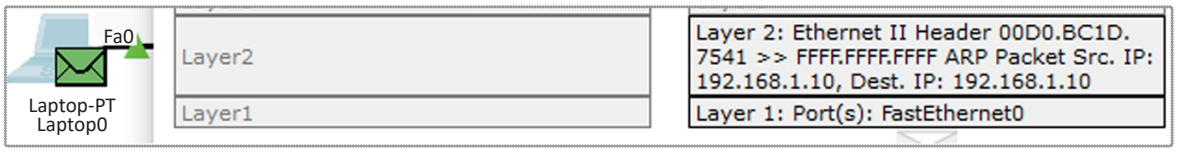
```
Switch(config)#no spanning-tree vlan 1
```

Adım 2: Ağ paketlerini gözlemlemek için "Simülation\Show All/None\EditFilters" düğmeleri ile sadece ARP paketini seçiniz (Görsel 8.11).



Görsel 8.11: ARP paketi seçimi

Adım 3: Laptop0'a 192.168.1.10 IP adresini atayınız. Laptop0, atadığınız IP'nin kendi ağında başka bir cihazda olmadığından emin olmak için ağa bir yayın ARP paketi gönderir (Görsel 8.12).

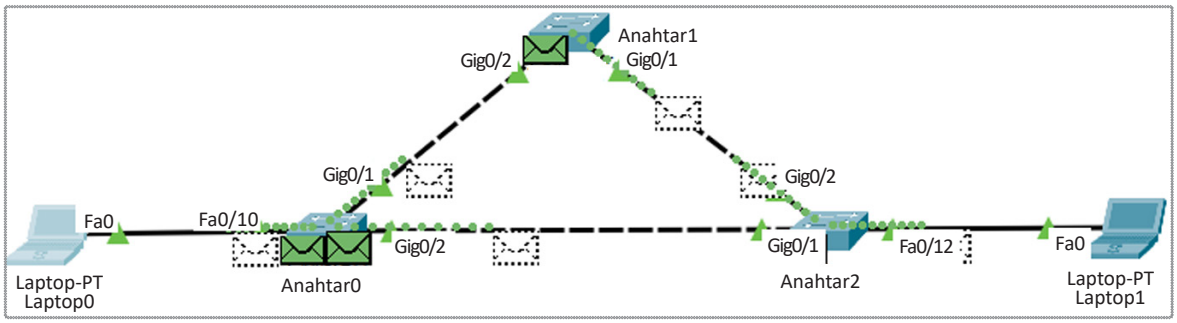


Görsel 8.12: ARP yayın paketi

Dikkat

Paketin bir yayın paketi olduğu simülasyon programında paketin üstüne tıklanarak OSI modeli tablosu, ikinci katman hedef MAC adresinden görülür. Hedef yayın MAC adresi "FFFF.FFFF.FFFF"dir. Gerçek ağ ortamlarında ise bilgisayarınıza kuracağınız ağ izleyici programlarından yararlanarak yayın paketlerinin MAC adreslerini öğrenebilirsiniz.

Adım 4: Yayın paketlerinin ağda nasıl bir karmaşaya sebep olduğunu görmek için animasyonu oynatınız (Görsel 8.13).



Görsel 8.13: Uygulama 2 için yayın fırtınası

Dikkat

Laptop0'ın IP alma sürecinde Anahtar0'dan başlayarak tüm anahtarlar, tüm portlarından sürekli yayın paketleri gönderecektir (Görsel 8.13). Olası ağa diğer cihazlarında katılımı ile yayın paketleri gönderildiğini düşünürsek bu durum ağ trafiğini aşırı artıracak ve anahtar işlemcilerine taşıyamayacakları miktarda yük binecektir. Bu süreç döngü hâlinde devam eder. Sonunda ağ çalışamaz hâle gelir. Ağdaki PC'ler aldıkları çerçeveleri tekrar almak durumunda kalabilir.

Adım 5: Programınızda simülasyondan çıkıp "Realtime"a gelerek Laptop 1'e 192.168.1.12 IP'sini atayınız. Ardından Laptop 0'dan Laptop 1'e komut satırından ping testi gerçekleştiriniz. İletişim, ağdaki yayın fırtınaları nedeniyle başarılı olmayacaktır (Görsel 8.14).

```
C:\>ping 192.168.1.12

Pinging 192.168.1.12 with 32 bytes of data:

Request timed out.
```

Görsel 8.14: Yayın fırtınası olan bir ağda iletişim testi

Adım 6: Topolojideki anahtarları varsayılan konuma getirip STP'yi yeniden aktifleştiriniz.

```
Switch(config)#spanning-tree vlan 1
```

Adım 7: Laptop 0 ve Laptop 1 arasında ping iletişim testini yeniden deneyiniz.

Bilgi

STP'nin yeniden aktifleşmesi sürecinin ardından iletişim başarılı olur.

Adım 8: Programı yeniden simülasyon konumuna getiriniz. Laptop 0'a yeni 192.168.1.20 IP'sini el ile atayarak ARP paketlerini takip ediniz. STP ile çalışan anahtarlarda yayın fırtınası olmayacaktır.

8.2. STP-SpanningTree Protocol (Kapsama Ağacı Protokolü)

STP (Spannig Tree Protocol), IEEE (The Institute of Electricaland Electronics Engineers) 802.1 D standardında geliştirilmiş anahtar cihazlar arasında, kullandığı algoritmalarla veri iletimi için en ideal yolun bulunmasını sağlar.

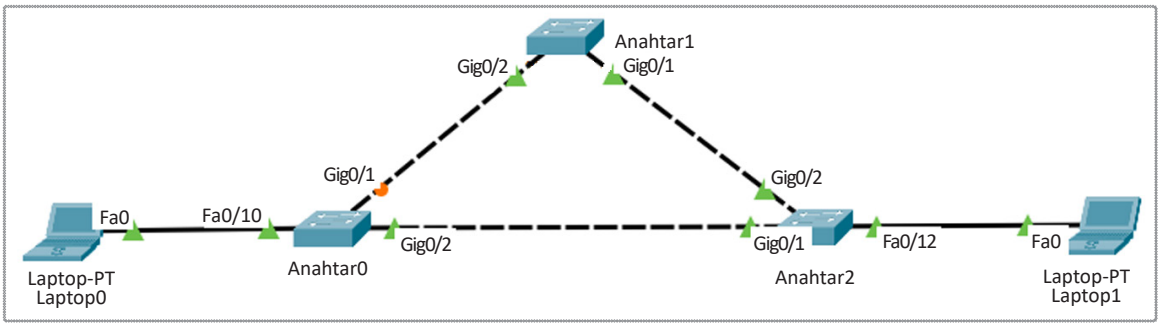
8.2.1. STP Amacı

STP, yayın fırtınası ve MAC tutarsızlığı gibi ağda döngüsel hataların oluşmaması için yedek yolları veri iletimine engeller. İdeal yolda fiziksel veya yönetimsel bir kopma meydana geldiğinde yedek yollardan en idealini bularak etkinleştirir. Böylelikle hizmetin aksaması önlenmiş olur.

Uygulama 3

http://kitap.eba.gov.tr/KodSor.php?KOD=21057

Görsel 8.15'teki topolojiyi simülasyon programında oluşturarak gerekli işlemleri aşağıdaki yönergeler doğrultusunda gerçekleştiriniz.



Görsel 8.15: Uygulama 3 yedekli yola geçiş topolojisi

Bilgi

Simülasyon programında, yedek yolun Anahtar0 ve Anahtar1 arasındaki bağlantı olduğunu Anahtar0 üzerindeki turuncu bağlantı ışığından anlayabilirsiniz.

Dikkat

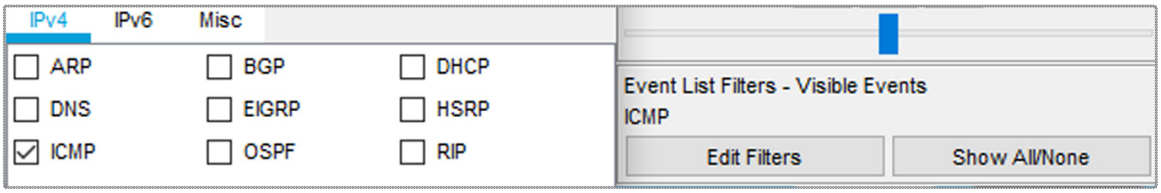
Uygulamanızda yedek yolun yerinde değişkenlik olabilir. Bu uygulamanın amacı, ana yolda kopma olduğunda yedek yolun etkin konuma gelmesini gözlemlemektir.

Adım 1: Laptop0'a 192.168.1.10, Laptop1'e 192.168.1.12 IP adreslerini giriniz.

Adım 2: Ağ paketlerini gözlemlemek için Simülation\Show All/None\EditFilters düğmeleri ile sadece ICMP paketini seçiniz (Görsel 8.16).

Bilgi

Ping iletişim testi ICMP paketleri kullanan bir uygulamadır.

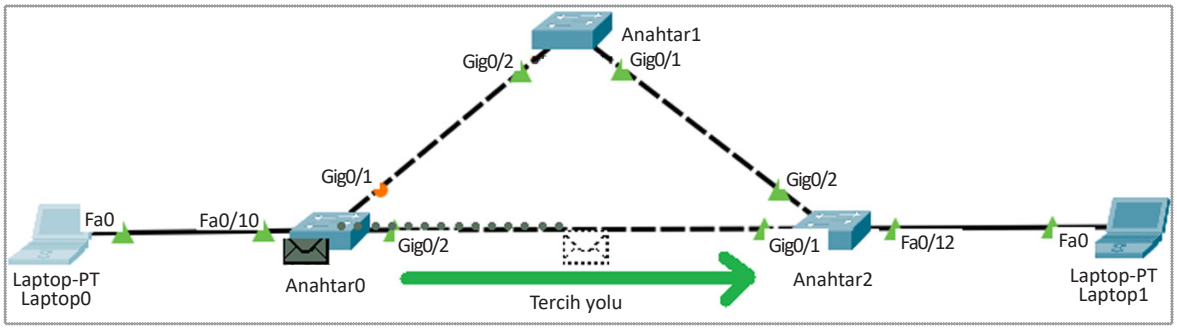


Görsel 8.16: ICMP paket seçimi

Adım 3: Laptop0'da komut ekranını açarak Laptop1 ile ping iletişim testi yapınız.

```
ping 192.168.1.12
```

Adım 4: Laptop0 ve Laptop1 arasında paketin tercih edilen gidiş güzergâhını Simülasyon/Oynat düğmesi ile gözlemleyiniz.



Görsel 8.17: STP ile tercih edilmiş yol gözlemi

Gözlem neticesinde veri paketlerinin Anahtar0'dan Anahtar2'ye doğru giderek kaynaktan hedefe iletildiğini görürsünüz. Bu STP tarafından tercih edilen yoldur. Anahtar0 ve Anahtar1 arasındaki yol, yedek durumdadır ve veri iletimi bu güzergâhtan yapılmaz (Görsel 8.17).

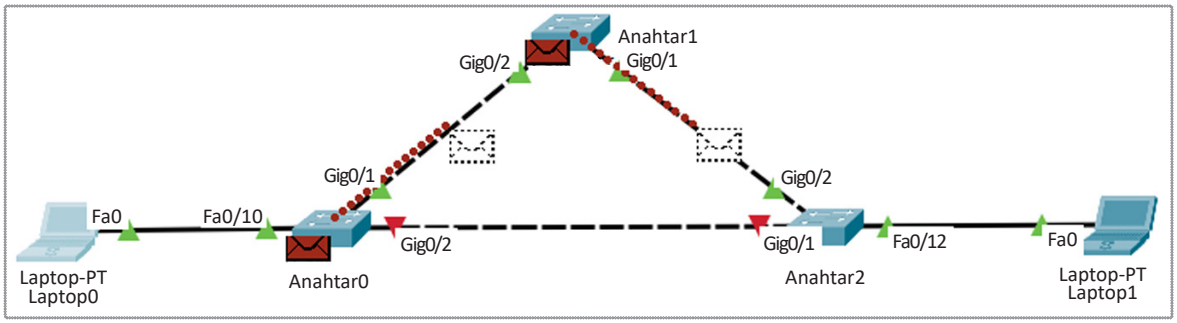
Adım 5: Anahtar0 terminal ekranına giriniz ve tercih edilen Gig0/2 arayüzünü kapatınız.

```
Anahtar0(config)#interface g0/2
Anahtar0(config-if)#shutdown
```

Adım 6: Yeniden Laptop0'da komut ekranını açıp Laptop1 ile ping iletişim testi yapınız.

```
ping 192.168.1.12
```

Adım 7: Yeniden Laptop0 ve Laptop1 arasında paketin tercih edilen gidiş güzergâhını Simülasyon/Oynat düğmesi ile gözlemleyiniz.



Görsel 8.18: STP ile yedek yolun etkinleşmesi

Anahtar0 ve Anahtar2 arasındaki birinci yol kapatılınca Anahtar0, Anahtar1 ve Anahtar2 arasındaki yol STP ile tercih edilen etkin yol durumuna gelmiştir (Görsel 8.18).

8.2.2. Temel Köprü Anahtar (Root Brıdge Swıtch) Seçimi

Yerel ağ içinde kaynaktan hedefe en uygun yolu bulup diğer yolları yedek konuma getirmek için anahtarlar kendi aralarında Spanning Tree Protocol'ü kullanır. Bu protokol sürekli aktiftir ve iki saniyelik periyotlarla anahtarlar karşılıklı olarak BPDU paketleri göndererek süreci devam ettirir. BPDU paketleri ile anahtarların birbirlerinin BID (Bridge ID-Köprü Değeri) bilgisini öğrenmesi sağlanır. BID köprü öncelik değeri ve MAC adres bilgisinden oluşur. Sürecin sonunda BID öncelik numarası ve MAC adresi az olan anahtar **temel köprü (Root Bridge)** olarak kabul edilir. Temel köprü anahtarı, veri trafiğinin mutlak suretle tercih edeceği anahtardır.

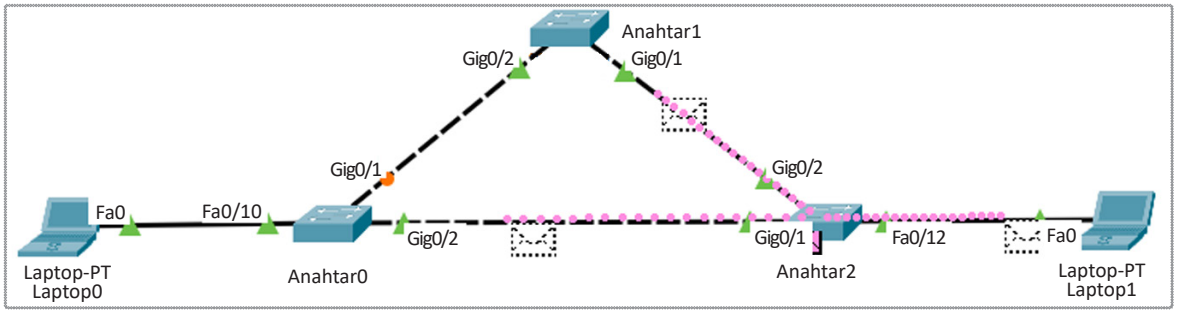
8.2.2.1. MAC Adresi ile Temel Köprü Seçimi

Anahtar cihazlarda herhangi bir köprü öncelik değeri bildirilmemişse MAC adresi temel köprü seçiminde kullanılacak tek referanstır. MAC adres değeri en küçük olan anahtar, ağda temel köprü anahtar (Root Switch) olarak STP tarafından belirlenir.

Uygulama 4

Görsel 8.15'teki topolojiyi simülasyon programında oluşturarak gerekli işlemleri aşağıdaki yönergeler doğrultusunda gerçekleştiriniz.

Adım 1: Ağ paketlerini gözlemlemek için Simülation\Show All/None\EditFilters\Misc düğmeleri ile STP paketini seçiniz. Simülasyon\Oynat düğmesi ile ağı gözlemleyiniz (Görsel 8.19).



Görsel 8.19: STP BPDU paketleri hareketi

Dikkat

Bu adımda STP'nin anahtarlar arasında hep aktif olduğu görülmektedir. STP ilk hesaplanırken tüm anahtarlar birbirlerine BPDU çerçeveleri ile köprü öncelik ve MAC değerlerini söyler. Temel köprü anahtar bulunduktan sonra STP BPDU çerçevelerinin yönü temel köprü anahtardan diğerlerine doğrudur. Anahtar köprü öncelik değerlerinde değişiklik olursa STP algoritma süreci yeniden işler.

Bilgi

STP paketleri yalnızca anahtarlar arasında gönderimi olan bir çoklu yayın MAC adresi kullanır.

Adım 2: Topolojinizi **Realtime /Gerçek Zamanlı** duruma getiriniz.

Adım 3: Anahtarların terminal ekranlarını açınız ve "show version" komutunu giriniz. MAC adreslerini öğreniniz (Görsel 8.20).

Dikkat

Bu adımda anahtar MAC adres bilgileri sizlerde farklı olabilir.

Anahtar0#show version

```
Anahtar0#sh version
Cisco IOS Software, C2960 Software (C2960-LANBASE-M), Ver
Copyright (c) 1986-2005 by Cisco Systems, Inc.
Compiled Wed 12-Oct-05 22:05 by pt_team

ROM: C2960 Boot Loader (C2960-HBOOT-M) Version 12.2(25r)E

System returned to ROM by power-on

Cisco WS-C2960-24TT (RC32300) processor (revision C0) wit


24 FastEthernet/IEEE 802.3 interface(s)
2 Gigabit Ethernet/IEEE 802.3 interface(s)

63488K bytes of flash-simulated non-volatile configuratio
Base ethernet MAC Address       : 00E0.8F7C.DC4A
Motherboard assembly number     : 73-9832-06
```

Görsel 8.20: Anahtar cihaz MAC adresi

Anahtar0MAC adresi: 00e0.8f7c.dc4a şeklindedir.
Anahtar1#show version

Anahtar1MAC adresi: 0060.70ba.191d şeklindedir.
Anahtar2#show version

Anahtar2MAC adresi: 000a.4169.cc7b şeklindedir.

Bilgi

Anahtar BID değeri varsayılan olarak 32.768'dir. VLAN numarası eklenmesi ile BID öncelik değeri (Priority) hesaplanır. Uygulama için BID öncelik numaraları 32768+1=32769 olur.

Bilgi

Anahtarlarda BID numarası değişikliği yapılmadığından temel köprü anahtarı, MAC adresi en düşük olan Anahtar2 olacaktır.

Adım 5: Anahtarlarda STP için temel köprü anahtarını görmek için her anahtarda "show spanning-tree" komutunu uygulayınız (Görsel 8.21).

```
Anahtar0#show spanning-tree
Anahtar1#show spanning-tree
Anahtar2#show spanning-tree
```

```
Anahtar0#sh spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    32769
              Address     000A.4169.CC7B
              Cost        4
              Port        26(GigabitEthernet0/2)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
```

BID öncelik numarası
Anahtar2 MAC adresi

Görsel 8.21: Anahtar spanning-tree yapılandırması root ve bridge anahtar listesi

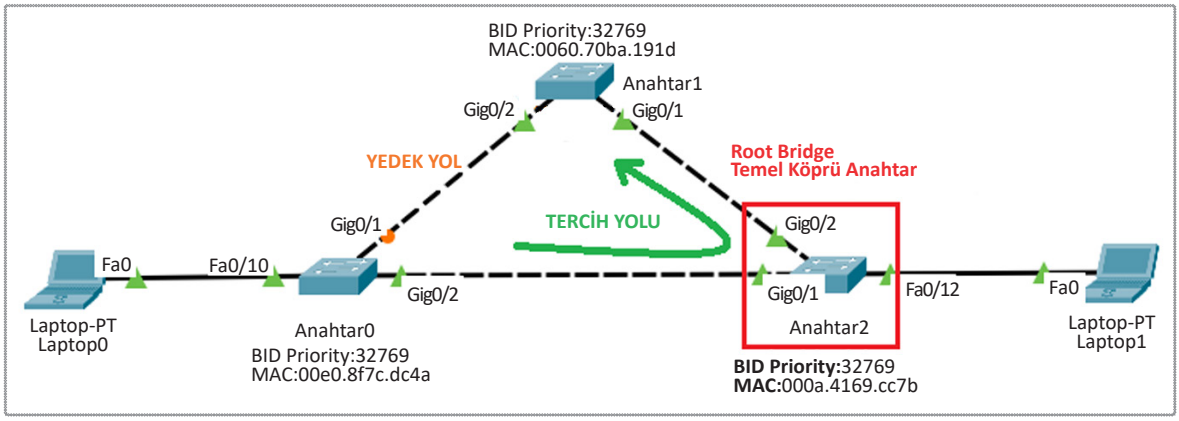
Her üç anahtarda aynı liste elde edilecektir. Topoloji temel köprü anahtarı, komutun çıktısında **Root** olarak görülür. Topolojide temel köprü anahtarı (RootBride) Anahtar2'dir. Anahtar2 etkinliğini kaybederse ikinci en küçük MAC değerine sahip Anahtar1, temel köprü (Root Bridge) olacaktır.

Adım 6: Aşağıdaki bilgilere göre cihazlarda IP atamalarını gerçekleştiriniz.
Laptop0 : 192.168.1.10
Anahtar1 (VLAN1) : 192.168.1.11

Anahtar1 cihazda, VLAN 1 arayüzüne IP adres bilgisini girebilmek için aşağıdaki komutu uygulayınız.

```
Anahtar1(config)#interface vlan 1
Anahtar1(config-if)#ip address 192.168.1.11 255.255.255.0
```

Adım 7: Simülasyon durumunda sadece ICMP paketini seçerek Laptop0 cihazından Anahtar1 cihazına ping komutu ile iletişim testi gerçekleştiriniz. Görsel 8.22'deki iletim yolunu gözlemleyeceksiniz.



Görsel 8.22: BID değeri eşitlik durumunda MAC değeri az olan temel köprü anahtarı

8.2.2.2. Öncelik Değeri Değişikliği ile Temel Köprü Anahtar Belirleme

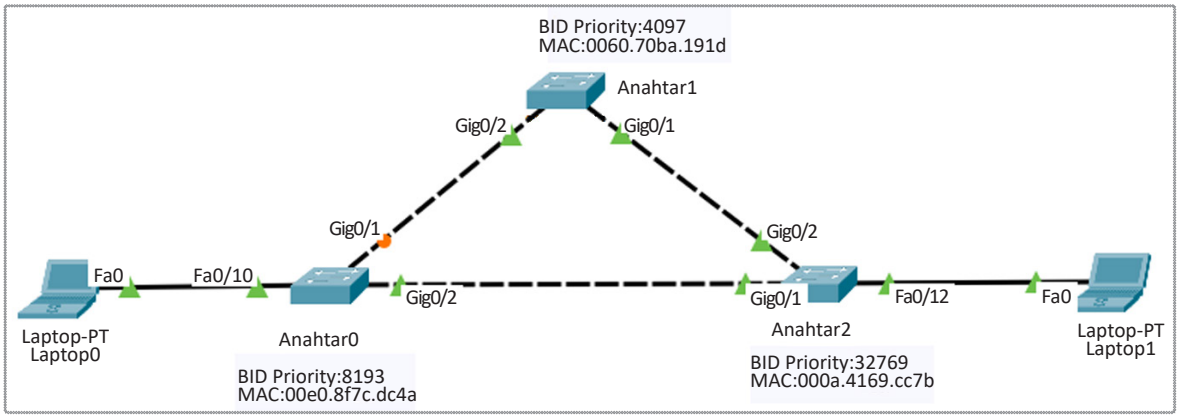
Temel köprü anahtarı belirlenirken BID öncelik değeri MAC adreslerine göre önceliklidir. Anahtar cihazlarda BID değeri 32.768 olarak gelir. BID öncelik değeri VLAN numarası ile toplanarak bulunur. VLAN 1 kullanan bir STP algoritmasının BID öncelik değeri, 32.768 ve 1 toplanarak 32.769 olarak bulunur. Bu değer varsayılan olarak

anahtarlarla gelse de kullanıcı tarafından değiştirilebilir. Bu değişim ile ağdaki temel köprü anahtar (Root Bridge Switch) değişimi de gerçekleşebilir.

BID öncelik değeri anahtarlarda 0 ile 61.440 arasında 4.096 sayısının katları şeklinde atanabilir.

Uygulama 5

Görsel 8.23'teki topolojiyi simülasyon programında oluşturarak işlemleri aşağıdaki yönergeler doğrultusunda gerçekleştiriniz.



Görsel 8.23: Uygulama 5 için BID değerine göre temel köprü anahtar seçimi

Dikkat

Görsel 8.23'te anahtar BID Öncelik (Priority) ve MAC adres değerleri görsel üstünde verilmiştir. MAC adresleri sizde farklı olabilir.

Adım 1: Anahtar cihazlarınızda MAC adreslerini "show version" komutu ile öğreniniz. Her anahtarın altına Görsel 8.23'te olduğu gibi MAC adreslerini yazınız.

Adım 2: MAC adres büyüklük sıralamasına göre Anahtar adlarını belirleyiniz.
Anahtar0 (MAC en büyük)>Anahtar1 MAC> Anahtar2 (MAC en küçük)

Adım 3: Anahtar cihazlarınızda "**show spanning-tree**" komutunu uygulayınız. Görsel 8.23'teki verilere göre BID değerlerinde henüz değişiklik yapılmadığı için varsayılan **32769** değerinde MAC adresi en küçük olan Anahtar2 root (temel köprü anahtarı) olacaktır.

Adım 4: MAC adres değeri küçük olan ikinci anahtarınızın (Anahtar1) VLAN 1 BID öncelik değerini 4096 yapınız. Öncelik değeri VLAN 1 numarası eklenerek 4096+1=4097 olacaktır.

```
Anahtar1(config)#spanning-tree vlan 1 priorty 4096
```

Adım 5: MAC adres değeri en büyük olan anahtarınızın (Anahtar0) VLAN 1 BID öncelik değerini 8192 yapınız. Öncelik değeri VLAN 1 numarası eklenerek 8192+1=8193 olacaktır.

```
Anahtar0(config)#spanning-tree vlan 1 priorty 8192
```

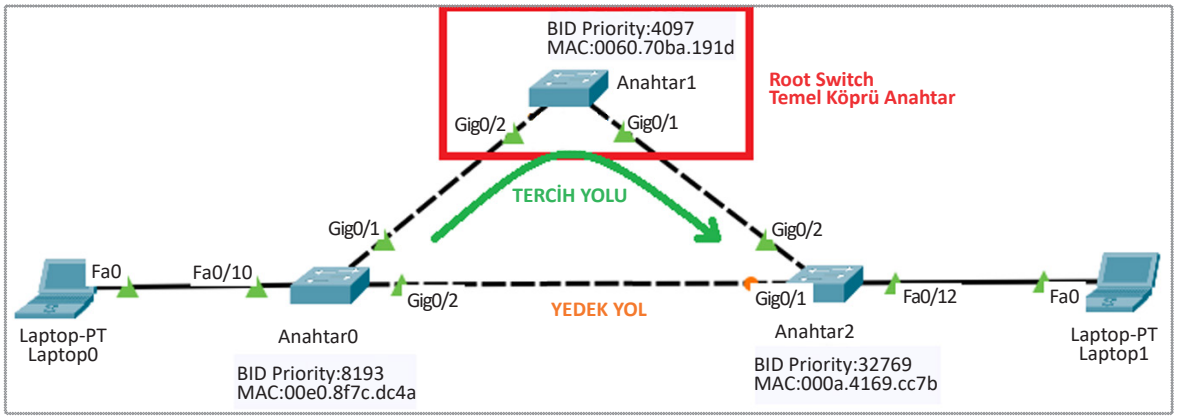
Adım 6: Topolojide yeni temel köprü anahtarını bulmak için anahtar cihazlarda "show spanning-tree" komutunu uygulayınız (Görsel 8.24).

```
Anahtar2#show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    4097        Anahtar1, Vlan1 BID Öncelik değeri
              Address     0060.70BA.191D
              Cost        4
              Port        26(GigabitEthernet0/2)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
```

Görsel 8.24: BID öncelik değeri en küçük olan anahtar root olarak seçilir.

Adım 7: Aşağıdaki bilgilere göre cihazlarda IP atamalarını gerçekleştiriniz.
Laptop0 : 192.168.1.10
Laptop1 : 192.168.1.12

Adım 8: Simülasyon durumunda ICMP paketini seçerek Laptop0 cihazından Laptop1 cihazına ping komutu ile iletişim testi gerçekleştiriniz. Görsel 8.25'teki iletim yolunu gözlemleyeceksiniz.



Görsel 8.25: BID öncelik değeri en küçük olan anahtar temel köprü anahtarıdır.

Görsel 8.25'te temel köprü anahtarı Anahtar1 olmuştur. Anahtar1'in hizmet aksamasına uğraması durumunda Anahtar0 temel köprü olacaktır. Anahtar1'in tüm bağlantıları aktifken Anahtar2, Anahtar0 arası bağlantı yedek yol durumuna gelmiştir. Veri aktarımında Anahtar1 bağlantılarının olduğu yollar öncelikli olacaktır. Anahtar0, Anahtar2 arasındaki yedek yol pasif duruma geçip veri transferi yapılmayacaktır.

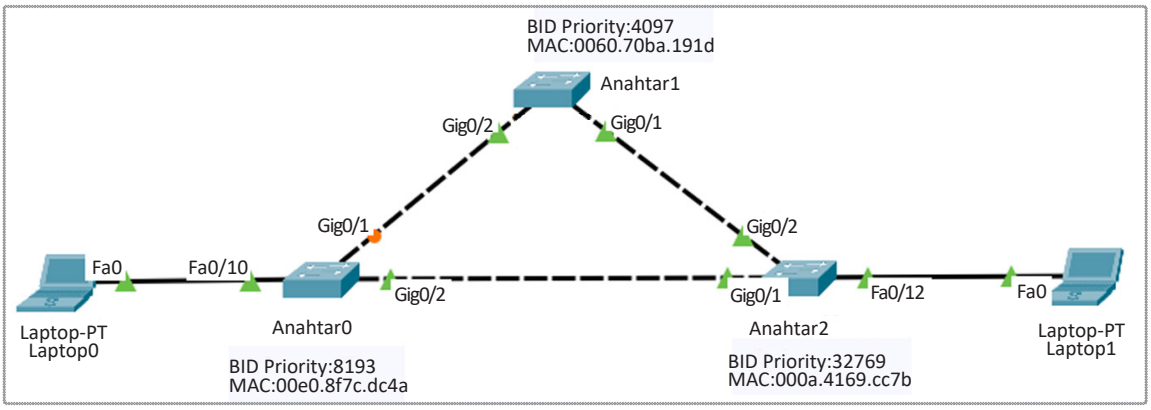
8.2.2.3. Komutla Temel Köprü Anahtarı Belirleme

Yedekli ağ sistemlerinde sayısal olarak anahtarların MAC ve BID öncelik numarası, temel köprü anahtarını belirlemede kullanılırken doğrudan komutla da anahtarları temel köprü veya ikincil köprü şeklinde belirleyebilirsiniz. Komut yöntemi, BID öncelik değerini anahtarda 0 yaparak anahtarın temel köprü anahtar olmasını sağlar. Komut, uygulandığı topolojide daha önce el ile girilmiş BID öncelik değeri ve MAC adresine göre daha belirleyicidir.

Temel köprü anahtarı belirleyiciliğinde sıralama şu şekildedir:
MAC < Köprü Önceliği Numarası (BID Priority) < Komut

Uygulama 6

Görsel 8.26'daki topolojiyi simülasyon programında oluşturarak işlemleri aşağıdaki yönergeler doğrultusunda gerçekleştiriniz. Bu uygulama, Uygulama 5'in devamı şeklinde olacaktır.



Görsel 8.26: Uygulama 6 için BID değerine göre temel köprü anahtar seçimi

Adım 1: Uygulama 5'teki tüm adımları gerçekleştiriniz. Köprü öncelik değeri en küçük olan Anahtar1 temel köprü anahtarıdır.

Adım 2: VLAN 1 için Anahtar0'ı temel köprü anahtarı olarak yapılandırınız. Bunun için Anahtar0 terminal ekranında aşağıdaki komutu giriniz.

```
Anahtar0(config)#spanning-tree vlan 1 root primary
```

Adım3: VLAN 1 için Anahtar1'i ikinci köprü anahtarı olarak yapılandırınız. Bunun için Anahtar1 terminal ekranında aşağıdaki komutu giriniz.

```
Anahtar1(config)#spanning-tree vlan 1 root secondary
```

Anahtar1, Anahtar0'da hizmet aksaması durumunda temel köprü anahtarı olarak aktif olacaktır.

Adım 4: Anahtar2'de terminal ekranını açarak "show spanning-tree" komutunu giriniz.

```
Anahtar2(config)#show spanning-tree
```

```
Anahtar2#sh spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    1
              Address     00E0.8F7C.DC4A
              Cost        4
              Port        25(GigabitEthernet0/1)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
```

Temel Köprü Anahtarı Anahtar0 dır.

Görsel 8.27: Komutla temel köprü anahtarı belirlenmiş bir ağda spanning-tree komutu

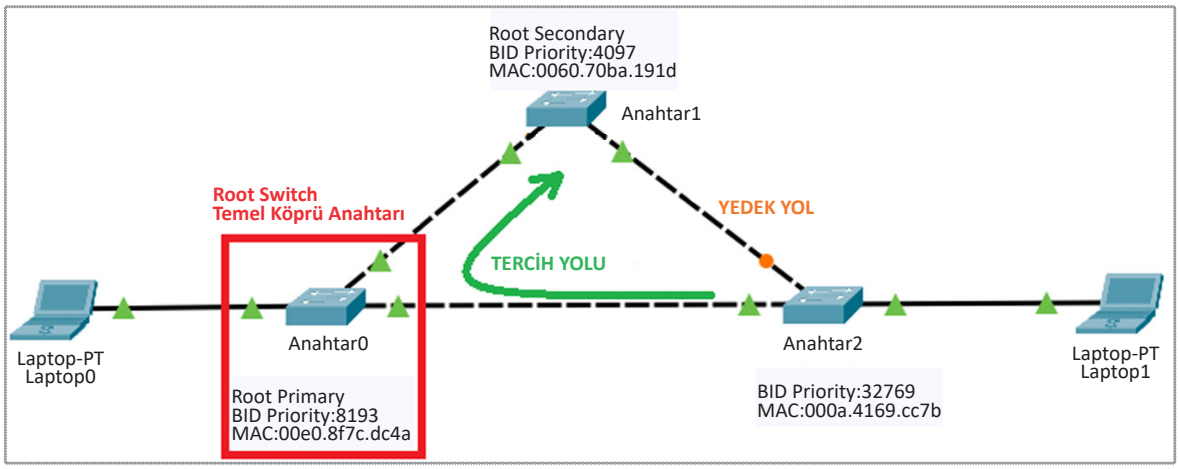
Görsel 8.27'de ağın temel köprü anahtarı VLAN 1 için Anahtar0 olarak belirlenmiştir. Bu, MAC adresinden anlaşılabilir. Priority (BID önceliği), önceki adımlarda 4096 olarak girilse de bu değerin 1 olduğu görülmektedir. Komutla temel köprü anahtarı (root) belirlenirken köprü öncelik değeri (BID) sıfırlanmıştır. Öncelik bulunurken VLAN değeri ile toplanmış, sonuç olarak 1 öncelik değeri elde edilmiştir.

Adım 5: Aşağıdaki bilgilere göre cihazlarda IP atamalarını gerçekleştiriniz.
Laptop1 : 192.168.1.12
Anahtar1 (VLAN1) : 192.168.1.11

Anahtar1 cihazda VLAN 1 arayüzüne IP adres bilgisini girebilmek için aşağıdaki komutu uygulayınız.

```
Anahtar1(config)#interface vlan 1
Anahtar1(config-if)#ip address 192.168.1.11 255.255.255.0
```

Adım 6: Simülasyon durumunda ICMP paketini seçerek Laptop1 cihazından Anahtar1 cihazına ping komutu ile iletişim testi gerçekleştiriniz. Görsel 8.28'deki iletim yolunu gözlemleyeceksiniz.



Görsel 8.28: Komutla bildirilen Anahtar, temel köprü anahtarıdır.

Görsel 8.28'de temel köprü anahtarı Anahtar0 olmuştur. Anahtar0 hizmet aksamasına uğraması durumunda Anahtar1 temel köprü olacaktır. Anahtar0'ın tüm bağlantıları aktifken Anahtar2 ile Anahtar1 arası bağlantı yedek yol durumuna gelmiştir. Veri aktarımında Anahtar0 bağlantılarının olduğu yollar öncelikli olacaktır. Anahtar1 ile Anahtar2 arasındaki yedek yol pasif duruma geçip veri transferi yapılmayacaktır.

8.2.3. Farklı VLAN'lar İçin Temel Köprü Anahtarı Belirleme

IEEE 802.1 D standardında çalışan STP algoritması, tek VLAN sistemine göre çalışır. VLAN 1, tüm fiziksel arayüzlerin varsayılan ağı olduğundan yedek anahtar ve yol belirleme VLAN 1 için yapılır. Anahtar cihazlarda birden fazla VLAN gereksinimi, her VLAN için ayrı yedekli yol ihtiyacı da doğurur. Bunun için üreticiler yeni STP türleri geliştirerek çoklu VLAN'lar için farklı temel köprü anahtar belirleyecek ve farklı yedek yollar kullanacak algoritmalar geliştirmiştir. Böylelikle VLAN'lardaki trafik aktarılırken değişik yollar güzergâh olarak kullanılabilir. Sonuç olarak ağdaki trafiğin fiziksel olarak daha dengeli akması sağlanır. Tek anahtarda işlem ve veri yükünün birikmesi önlenmiş olur. Bu yeni standartlarda BPDU BID değerinin içinde genişletilmiş sistem ID numarası eklenmiştir. Bu numara ile farklı VLAN'ları seçebilecek VLAN bilgileri de BID alanı içine eklenmiş olur.

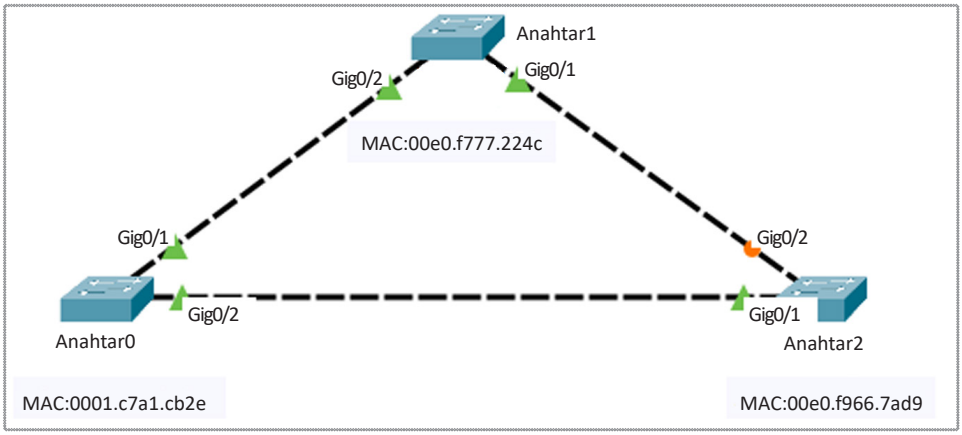
Dikkat

BID Alanı: Öncelik Numarası + Genişletilmiş ID + MAC adresi

Uygulama 7

http://kitap.eba.gov.tr/KodSor.php?KOD=21058

Görsel 8.29'daki topolojiyi simülasyon programında oluşturarak aşağıdaki işlemleri yönergeler doğrultusunda gerçekleştiriniz.



Görsel 8.29: Uygulama 7 için ağ topolojisi

Adım 1: Anahtar cihazlarda "show version" komutu ile MAC adreslerini öğrenerek MAC adres değerlerine göre azdan çoğa doğru anahtar cihazları sırası ile Anahtar0, Anahtar1 ve Anahtar2 şeklinde adlandırıp topolojide uygun şekilde bağlantıları yapınız.

Adım 2: Anahtar cihazlarda temel köprü anahtarı bulmak için "show spanning-tree" komutunu uygulayınız (Görsel 8.30).

```
Anahtar1#sh spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    32769
              Address     0001.C7A1.CB2E      Temel Köprü: Anahtar0
              Cost        4
              Port        26(GigabitEthernet0/2)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
```

Görsel 8.30: Varsayılan BID değerinde temel köprü seçimi

Anahtarlarda BID değeri girişi yapılmadığı ve komutla temel köprü anahtarı belirlenmediği için MAC adresi en küçük olan Anahtar0, VLAN 1 için temel köprü anahtarıdır.

Adım 3: Tablo 8.1'e göre VLAN yapılandırmalarını gerçekleştiriniz. IP alt ağ maskesi tüm anahtar VLAN'ları için 255.255.255.0 olacaktır.

Tablo 8.1: Uygulama 7 İçin VLAN Tablosu

VLAN ID	ADI	IP Adresi		
		Anahtar0	Anahtar1	Anahtar2
VLAN 1	*Default	192.168.1.10	192.168.1.11	192.168.1.12
VLAN 10	Satis	192.168.10.10	192.168.10.11	192.168.10.12
VLAN 20	Danisma	192.168.20.10	192.168.20.11	192.168.20.12

Dikkat

Anahtar cihazlarda VLAN 1 ismi varsayılan olarak "Default"tur ve değiştirilemez.

Anahtar0 için gerekli kodlar:

```
Anahtar0(config)#vlan 10
Anahtar0 (config-vlan)#name Satis
Anahtar0 (config-vlan)#exit
Anahtar0 (config)#vlan 20
Anahtar0 (config-vlan)#name Danisma
Anahtar0 (config-vlan)#exit
Anahtar0 (config)#interface vlan 1
Anahtar0 (config-if)#ip address 192.168.1.10 255.255.255.0
Anahtar0 (config)#interface vlan 10
Anahtar0 (config-if)#ip address 192.168.10.10 255.255.255.0
Anahtar0 (config-if)#exit
Anahtar0 (config)#interface vlan 20
Anahtar0 (config-if)#ip address 192.168.20.10 255.255.255.0
Anahtar0 (config-if)#exit
```

Anahtar0 için uygulanan VLAN IP yapılandırma komutlarını Anahtar1 ve Anahtar2 cihazlarına Tablo 8.1'deki verilere göre uyarlayınız.

Adım 4: Çoklu VLAN trafiğinin aktarımı için anahtar cihazlarda bağlantı arayüzlerini trunk durumuna getiriniz.

```
Anahtar0(config)#interface range GigabitEthernet 0/1-2
Anahtar0(config-if-range)#switchport mode trunk
```

Trunk yapılandırma komutlarını Anahtar1 ve Anahtar2 cihazlarına da uygulayınız. Tüm anahtarlarda bağlantılar, Görsel 8.29'da olduğu gibi GigabitEthernet arayüzleri ile yapılmıştır.

Adım 5: Anahtar cihazlarda "show interface vlan 10" ve "show interface vlan 20" komutlarıyla VLAN 10 ile VLAN 20 sanal arayüzlerin MAC adreslerini öğreniniz.

Dikkat

Öğrenilen MAC adresleri, Adım 1'de görülen MAC adreslerinden farklı olsa da VLAN 10 ve VLAN 20 sanal ağları için temel köprü anahtarını değiştirecek değerlerde olmayacaktır.

Adım 6: VLAN 10 için köprü öncelik değerini değiştirerek Anahtar1'i temel köprü anahtarı olarak belirleyiniz. Anahtar1 cihazında aşağıdaki komutu uygulayınız.

```
Anahtar1(config)#spanning-tree vlan 10 priority 4196
```

Adım 7: VLAN 20 için komutla Anahtar2'yi temel köprü anahtar cihazı olarak belirleyiniz. Anahtar2 cihazında aşağıdaki komutu uygulayınız.

```
Anahtar2(config)#spanning-tree vlan 20 root primary
```

Adım 8: Anahtarlarda "show spanning-tree" komutunu uygulayarak her VLAN için temel köprü anahtarını görüntüleyiniz. Görsel 8.31'deki çıktıyı elde ediniz.

```
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    32769
              Address     0001.C7A1.CB2E
              Cost        4
              Port        26(GigabitEthernet0/2)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32769  (priority 32768 sys-id-ext 1)
              Address     00E0.F777.224C
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

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

VLAN0010
  Spanning tree enabled protocol ieee
  Root ID     Priority    4106
              Address     00E0.F777.224C
              This bridge is the root
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    4106  (priority 4096 sys-id-ext 10)
              Address     00E0.F777.224C
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

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

VLAN0020
  Spanning tree enabled protocol ieee
  Root ID     Priority    24596
              Address     00E0.F966.7AD9
```

VLAN 1 İÇİN TEMEL KÖPRÜ: Anahtar0

VLAN 10 İÇİN TEMEL KÖPRÜ: Anahtar1

VLAN 20 İÇİN TEMEL KÖPRÜ: Anahtar2

Görsel 8.31: Çoklu VLAN'larda farklı temel köprü anahtarlar

Görsel 8.31'de görüldüğü gibi ağdaki farklı VLAN'lar için farklı temel köprü anahtarlar belirlenmiştir. Topoloji ağ trafiğinde her VLAN için kendi temel köprü anahtarları üzerinden veri aktarımı öncelik olacaktır. VLAN'ların yedek yolları, temel köprü anahtarları aynı olmadığından farklı olacaktır.

Adım 9: Simülasyon ortamında sadece ICMP paketlerini seçerek, anahtar cihazlarda farklı VLAN IP adreslerini kullanarak ping testi gerçekleştiriniz. Her VLAN için seçilen öncelikli yolları gözlemleyiniz.

8.2.4. STP Sürecinde Arayüz Durumları

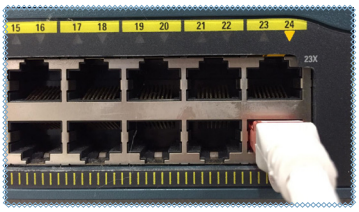
STP yedekli yol bulma algoritması aşamasında anahtar arayüzleri belirli bir süreçten geçer. Bu süreç, anahtar arayüzünün yönetimsel olarak açılmasından başlar. STP algoritması hesaplamasının sonucunda, arayüzün pasif veya ağ için tercih edilen aktif bir yol olup olamayacağına karar verilir. Arayüz yönetimsel olarak kapalı ise süreç çalışmaz. Arayüz tüm ağ trafiğine kapalıdır. STP sürecinde arayüzler dört durumda çalışır. Arayüz durumları; engelleme, dinleme, öğrenme ve iletim şeklindedir. STP kullanılan bir anahtarda arayüz ağa dâhil olduğunda bu dört durumun işleyeceği süreç, arayüz için çalışır. Arayüzler için STP süreci Tablo 8.2'de verilmiştir.

Tablo 8.2: STP Sürecinde Anahtar Arayüz Durumları

İzin Verilen İşlem	ARAYÜZ DURUMU				
	Engelleme	Dinleme	Öğrenme	İletim	Kapalı Arayüz
STP BPDU Paket Alımı	Evet	Evet	Evet	Evet	Hayır
Arayüzde Alınan Veri Çerçeveleri İletimi	Hayır	Hayır	Hayır	Evet	Hayır
Farklı Arayüzden Anahtarlanan Veri Çerçevelerinin İletimi	Hayır	Hayır	Hayır	Evet	Hayır
MAC Adresi Öğrenimi	Hayır	Hayır	Evet	Evet	Hayır

8.2.4.1. Engelleme Durumu

Engelleme, ağa katılan arayüzün STP sürecindeki ilk durumudur. Bu durumdayken arayüz sadece STP BPDU paketlerini alır. Diğer veri trafiğine kapalıdır. Öteki anahtarlardan gelen MAC bilgilerini öğrenmez. Bu durum 20 saniye sürer. Arayüz LED ışığı turuncudur. Görsel 8.32'deki 24. arayüz LED ışığı gibi sabit şekilde yanar.



Görsel 8.32: Anahtar cihazda STP engelleme durumundaki bir arayüz

8.2.4.2. Dinleme Durumu

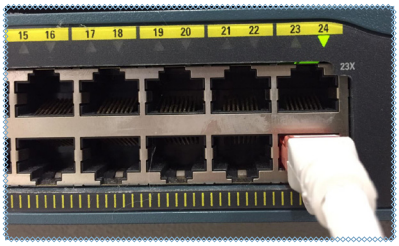
Dinleme durumunda, ağda yayın fırtınalarına bağlı döngüsel bir trafiğin olup olmadığı kontrol edilir. Döngüsel bir trafik varsa arayüz kendini engelleme durumuna geri alır. Bu süreç 15 saniyedir. Arayüz LED'i turuncu renk ile sürekli yanıp söner.

8.2.4.3. Öğrenme Durumu

Öğrenme durumunda, engelleme ve dinleme durumlarından farklı olarak çevre anahtarların MAC adresleri öğrenilebilir. Anahtar MAC adres tablosunun oluşturulduğu durumdur. LED turuncudur ve öğrenme durumu 15 saniye sürer.

8.2.4.4. İletim Durumu

Tüm veri trafiği için arayüz açıktır. Diğer üç durumun süreçleri tamamlanmıştır. Anahtarda STP BPDU paket trafiği ve MAC öğrenme işlemleri devam eder. Arayüz LED'i yeşil yanar. STP ile arayüz aktif iletim durumuna gelene kadar geçen süre 50 saniyedir (Görsel 8.33).



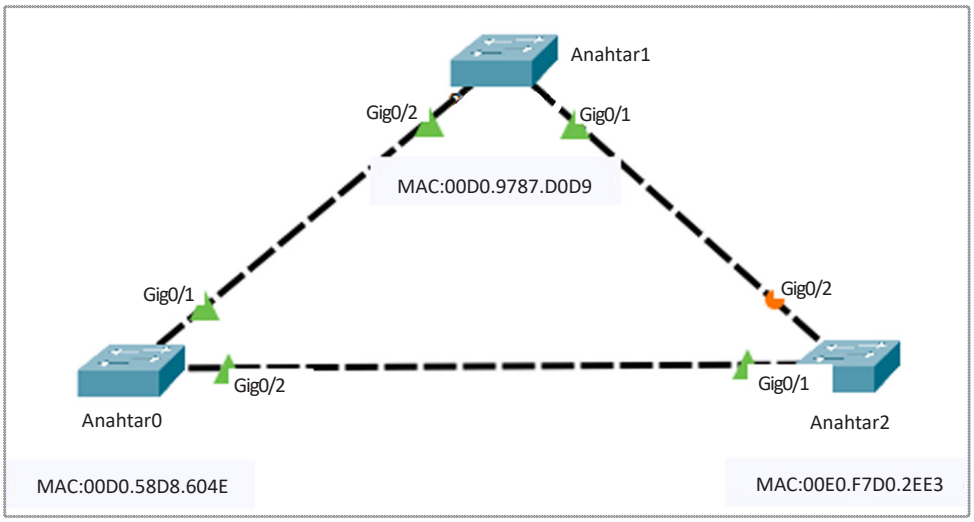
Görsel 8.33: Anahtar cihazda STP iletim durumundaki bir arayüz

Dikkat

Yönetimsel olarak kapalı olan arayüzler, tüm STP süreçlerine ve veri trafiğine kapalıdır.

Uygulama 8

Görsel 8.34'teki topolojiyi oluşturarak aşağıdaki işlemleri yönergeler doğrultusunda gerçekleştiriniz.

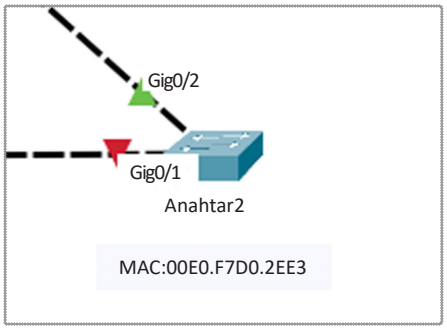


Görsel 8.34: Anahtarlar için STP port durumları

Adım 1: Anahtar yerleşiminde "show version" komutu ile anahtar MAC adres değerlerini öğreniniz. MAC değerine göre küçükten büyüğe sırası ile Anahtar0, Anahtar1 ve Anahtar2 yerleşimlerini yapınız.

Adım 2: Terminal ekranından komut ile Anahtar2 Gig0/1 fiziksel arayüzünü kapatınız.

```
Anahtar2(config)#interface gigabitEthernet 0/1
Anahtar2(config-if)#shutdown
```

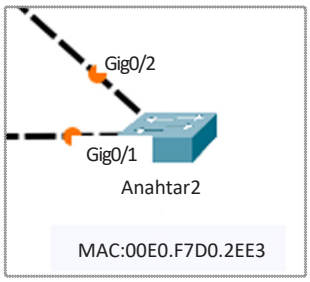


Görsel 8.35: Gig0/1 kapalı arayüz

Gig0/1 arayüzü kapalı olduğundan arayüzde STP dâhil tüm trafik akışı durdurulmuştur. Gig0/2 yedek yolu iletim durumuna geçmiştir (Görsel 8.35).

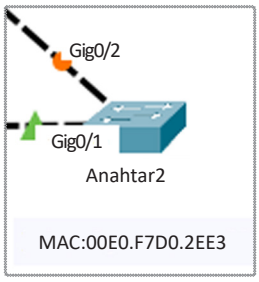
Adım 3: Anahtar2 Gig0/1 fiziksel arayüzünü terminal ekranından komut ile açınız.

```
Anahtar2(config)#interface gigabitEthernet 0/1
Anahtar2(config-if)#no shutdown
```



Görsel 8.36: Gig 0/1 engelleme, dinleme ve öğrenme durumları

Anahtar cihaz için STP süreci çalışmaya başladığı andan itibaren Görsel 8.36'da olduğu gibi arayüz turuncu yanar. Arayüzlerde yeniden STP algoritması hesaplamaları yapılır.



Görsel 8.37: Gig0/1 iletim durumunda

Arayüz iletim durumuna geçtiği andan itibaren arayüz yeşil yanar. Arayüz tüm veri trafiğine açıktır (Görsel 8.37).

Adım 4: Anahtar 2 cihazında STP arayüz durumlarını görüntülemek için "show spanning-tree" komutunu uygulayınız.

```
Anahtar2#sh spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    32769
              Address     0001.C7A1.CB2E
              Cost        4
              Port        25(GigabitEthernet0/1)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32769  (priority 32768 sys-id-ext 1)
              Address     00E0.F966.7AD9
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

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

Görsel 8.38: STP çalışan arayüz durumları

Görsel 8.38'de, STP sürecinin sonunda anahtarda arayüz durumlarını görürsünüz. Gi0/1 arayüzü, iletim (forward-FWD) durumundayken Gi0/2 arayüzü, engelle (BLK) durumundadır. Gi0/2 ağ trafiğini engelleyen arayüzdür ve bağlı olduğu yol yedektir.

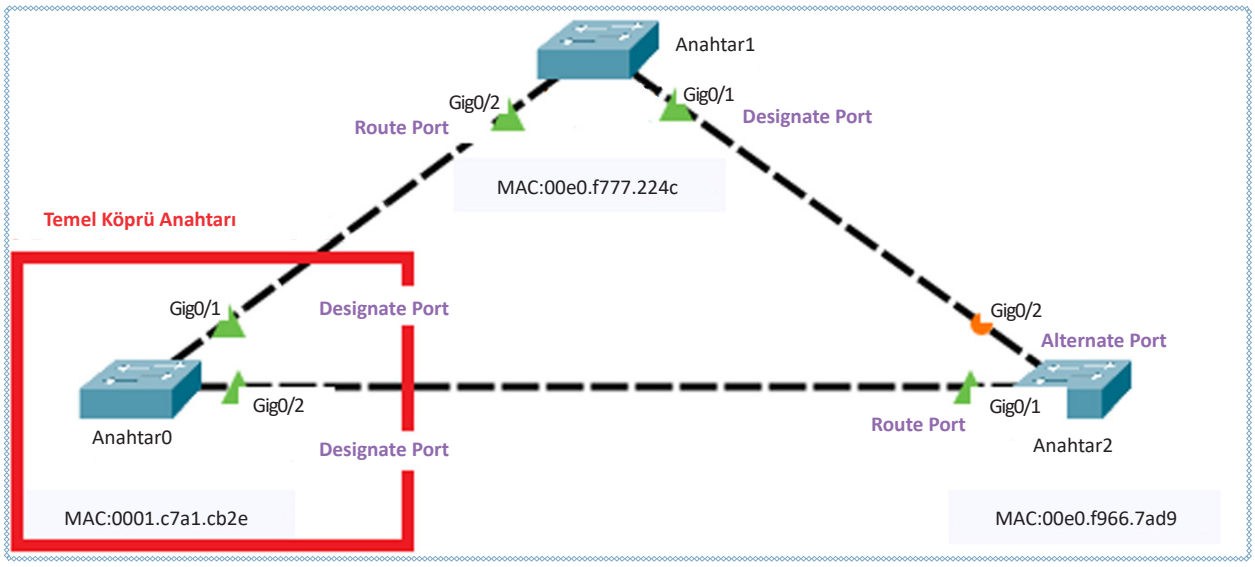
8.2.5. STP Çalışan Topolojilerde Anahtar Arayüz Rolleri

STP algoritması tamamlanmış ve çalışan anahtarlı sistemlerde arayüzlerin alacağı roller, yedekli yolun ve tercih yolun konumunu belirler. Anahtar işletim sisteminde hangi arayüzlerin veri iletiminde tercih edilen yolu kullandığı STP rollerine bakılarak anlaşılır.

Root Port: Temel köprü anahtarı ile bağlantısı olan arayüzlerdir. Bu arayüzler, temel köprü anahtarı olmayan ancak bağlantısı olan anahtarlarda bulunur. Bu portların durumu aynı zamanda iletim (forward) konumundadır.

Designated Port: Root olmayan veri iletiminde etkin portlardır. Temel köprü anahtarındaki tüm arayüzler, **designated port** rolündedir. Bu portların durumu aynı zamanda iletim (forward) konumundadır.

Alternate Port: Veri iletimine açık olmayan yedek yol için tanımlanmış arayüzlerdir. Bu portların durumu aynı zamanda engelle (bloke) konumundadır.



Görsel 8.39: STP arayüz rolleri

Görsel 8.39'da görüldüğü gibi Anahtar0, temel köprü anahtarıdır. Tüm arayüzleri **designate port** rolündedir. Anahtar1 ve Anahtar2'de Anahtar0 bağlantılı arayüzler ise **route port** rolündedir. Anahtar2'nin Anahtar1 ile bağlantısını kuran Gig0/2 arayüzü **alternate port** rolündedir. Topolojideki diğer tüm arayüzler ise **designate port** rolündedir.

Alternate portlar yedek yollar için kullanılacak arayüzlerdir. Veri trafiğini engellemiş durumda çalışır. Topolojide alternate portu belirleyen STP algoritmasıdır. Alternateport, en yüksek BID veya MAC adresine sahip anahtarda, kendisi ile bağlantılı ikinci en yüksek BID veya MAC adresine sahip anahtara bağlı olan arayüzdür.

Anahtar cihazlarda arayüz rolleri "show spanning-tree" komutu ile öğrenilir.

Uygulama 9

Görsel 8.39'daki topolojiyi oluşturarak aşağıdaki işlemleri yönergeler doğrultusunda gerçekleştiriniz.

Adım 1: Anahtar MAC adreslerini "show version" komutu ile öğreniniz. Adres değerlerine göre sırası ile küçükten büyüğe doğru Anahtar0, Anahtar1 ve Anahtar2 adlandırmalarını yapınız.

Adım 2: Topoloji ekranında turuncu ile yanan arayüz alternate porttur.

Adım 3: Anahtar cihazlarda sırası ile "show spanning-tree" komutunu uygulayınız. Temel köprü anahtarını ve port rollerini görünüz.

```
Anahtar0#show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    32769
              Address     0001.C7A1.CB2E
              This bridge is the root
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32769  (priority 32768 sys-id-ext 1)
              Address     0001.C7A1.CB2E
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

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

Görsel 8.40: Temel köprü anahtar cihazda arayüz rolleri

Temel köprü seçilen anahtar cihazının Görsel 8.40'ta olduğu gibi tüm arayüzleri designate porttur.

```
Anahtar1#show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    32769
              Address     0001.C7A1.CB2E
              Cost        4
              Port        26(GigabitEthernet0/2)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32769  (priority 32768 sys-id-ext 1)
              Address     00E0.F777.224C
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

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

Görsel 8.41: Temel köprü anahtar olmayan cihazda arayüz rolleri

Temel köprü olmayan anahtarın temel köprü anahtarla bağlantı kurduğu Gi0/2 arayüzü root port, diğer arayüz designate porttur (Görsel 8.41).

```
Anahtar2#show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    32769
              Address     0001.C7A1.CB2E
              Cost        4
              Port        25(GigabitEthernet0/1)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32769  (priority 32768 sys-id-ext 1)
              Address     00E0.F966.7AD9
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

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

Görsel 8.42: Alternate porta sahip bir anahtar cihaz

Görsel 8.42'de görüldüğü gibi Anahtar2, Gig0/2 arayüzü alternate porttur. Bu arayüzün durumu aynı zamanda engelleme [BLK (Bloke)] konumundadır.

8.2.6. Anahtarlar Arası Çoklu Bağlantı STP Hesaplaması

İki anahtar arasında birden fazla bağlantı ile yedekli yollar konulmuşsa STP algoritması bu yollardan sadece birini tercih eder. Bu arayüz veri iletiminin gerçekleşeceği yolu tayin eder. Diğer yollar yedek bağlantı yolları olacaktır. Tercih edilen yolda aksama olursa yedek yollardan biri yine STP hesaplaması ile tercih edilen yol olur.

8.2.6.1. Arayüz Maliyet Değerine Göre Yol Seçimi

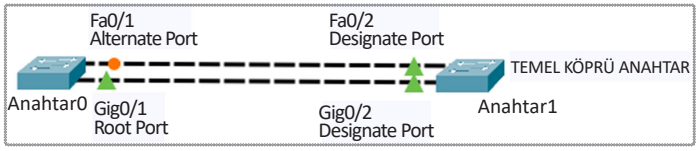
Anahtarlar arasında birden fazla yedek yol olması durumunda bu yolların arayüz bağlantı hızlarına bakılır. Maliyeti en az olan yol, tercih yolu olacaktır. Tablo 8.3'te bağlantı hızlarına göre arayüzlerin maliyet değerleri verilmiştir.

Tablo 8.3: Arayüz Bağlantı Hızı Maliyet Tablosu

Bağlantı Hızı	Maliyet
10 Gbps	2
1 Gbps	4
100 Mbps	19
10 Mbps	100

Uygulama 10

Görsel 8.43'te verilen topolojiyi oluşturarak işlemleri yönergeler doğrultusunda gerçekleştiriniz.



Görsel 8.43: Farklı bağlantı hızlarında STP tercih yolları

Adım 1: Görsel 8.43'te Anahtar0 ve Anahtar1 arasında 100 Mbps'lik FastEthernet ve 1 Gbps hızında GigabitEthernet arayüzlerin bağlantı durumunda maliyeti az olan GigabitEthernet arayüzler iletim için tercih edilen yol olarak kullanılacaktır. Bunu Görsel 8.43 anahtar bağlantı simgelerinden de anlayabilirsiniz.

Adım 2: Anahtar cihazlarda "show spanning-tree" komutu ile anahtar cihazlarda arayüz rollerini ve maliyetleri görünüz.

```
Anahtar0#show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    32769
              Address     0009.7C4D.CDEB
              Cost        4
              Port        25(GigabitEthernet0/1)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32769  (priority 32768 sys-id-ext 1)
              Address     00E0.F72C.9C19
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

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

Görsel 8.44: Uygulama 10 için Anahtar0 arayüz maliyetleri

Görsel 8.44'te Anahtar0 arayüzleri için maliyetleri **Cost** sütunundan görebilirsiniz. Temel köprü olmayan Anahtar0 için Fa0/1 portu maliyetinin Gi0/1'e göre büyük olmasından kaynaklı Alternate rolündedir ve durum olarak engellenmiştir.

```
Anahtar1#show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    32769
              Address     0009.7C4D.CDEB
              This bridge is the root
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32769  (priority 32768 sys-id-ext 1)
              Address     0009.7C4D.CDEB
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- --------
Fa0/2            Desg FWD 19        128.2    P2p
Gi0/2            Desg FWD 4         128.26   P2p
```

Temel Köprü Anahtar

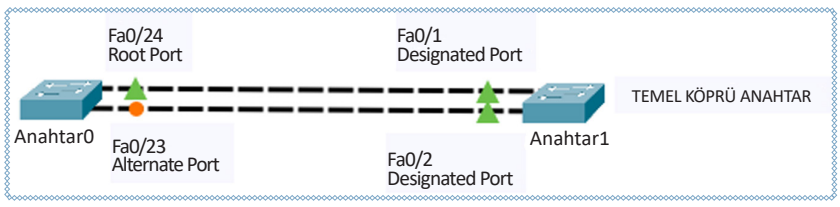
Görsel 8.45: Uygulama 10 için Anahtar1 arayüz maliyetleri

Anahtar1, MAC adres değerinin küçük olması sebebiyle temel köprü anahtarıdır. Görsel 8.45'te Anahtar1 Fa0/2 ve Gi0/2 arayüzlerinin değerleri görülmektedir. Her iki arayüzde designated (Desg) rolünde ve iletim (FWD) durumundadır. Ancak Fa0/2'nin karşılığı anahtar Fa0/1 arayüzü, engelleme durumunda olduğu için aralarındaki yol yedek konumundadır. Veri iletimi için kullanılmayacaktır.
Arayüz maliyet değerleri Tablo 8.3'te verildiği gibi otomatik olarak belirlenir ancak STP'nin tercih yolunu değiştirmek için maliyeti, komut ile de değiştirilebilir. Bunun için anahtar işletim sisteminde ilgili arayüz satırına gelerek maliyet değerinin elle yazılması gerekir. Bağlantı hızından bağımsız olarak yapılan bu değişiklik ile STP için tercih arayüzlerinin sıralaması değiştirilebilir. Aşağıdaki komut satırları ile fastEthernet0/1 arayüzünün STP maliyeti, 1 olarak belirlenmiştir.

```
Anahtar0(config)#interface fastEthernet0/1
Anahtar0(config-if)#spanning-tree cost 1
```

8.2.6.2. Arayüz Numara Değerlerine Göre Yol Seçimi

Aynı arayüz bağlantı hızlarındaki çoklu yolların tercihinde belirlenen kural, temel köprü anahtar cihazında en küçük arayüz numarasına sahip yolun, veri iletiminde tercih edilmesidir. Görsel 8.46'da aynı hızlara sahip fastEthernet arayüzlerinden bağlantılı Anahtar0 ve Anahtar1 cihazlarında, Anahtar1 cihazı fastEthernet0/1 arayüzü veri iletimi için tercih edilmiştir.



Görsel 8.46: Eşit bağlantı hızına sahip arayüz bağlantılarında tercih edilen yol

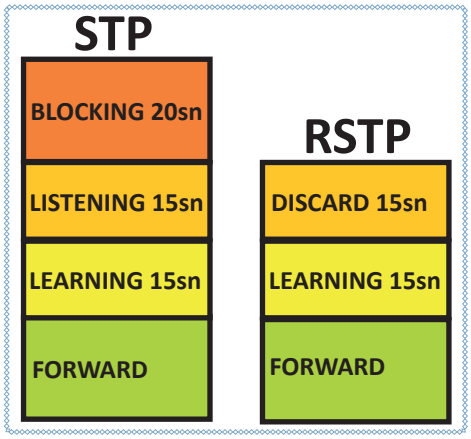
8.2.7. STP Türleri

Yerel ağ içinde yayın döngülerinin oluşmaması için uygulanan bağlantı yedekleme teknolojileri, zaman içinde farklı algoritma ve üreticilerin ortaya koyduğu yeni standartlarla gelişmektedir.

STP: IEEE802.1 D standardında oluşturulmuş temel yedekleme protokolüdür. VLAN sayısından bağımsız çalışır.

PVST: Farklı VLAN'lar için temel köprü anahtarlar belirlenmesini sağlayan protokoldür. Her VLAN için ayrı STP örnekleri oluşturur. Trunk protokolü 802.1q ile çalışmaz.

RSTP: IEEE 802.1 W standardında, STP ye göre daha hızlı durum geçişi sağlayan protokoldür. BPDU paketleri STP'de olduğu gibi yine 2 saniyelik periyotlarla anahtarlar arasında gönderilirken cevap bekleme süresi 3 BPDU süresi kadardır. Bu süre, RSTP ile toplam 6 saniyeyken STP'de engelleme durumu 20 saniyedir. RSTP'de engelleme ve listening durumları yoktur. Görsel 8.47'de olduğu gibi **discard** durumu vardır. STP'de olduğu gibi VLAN'lardan bağımsız çalışır. trunk protokolünü 802.1q kullanabilir.



Görsel 8.47: STP ve RSTP durum süre farkları

PVST+: Özel üreticiye özgü bir STP protokolüdür. Farklı VLAN'lar için temel köprü anahtarlar belirlenmesini sağlayan protokoldür. Her VLAN için ayrı STP örnekleri oluşturur. PVST'den farklı olarak trunk protokolü 802.1q ile çalışır.

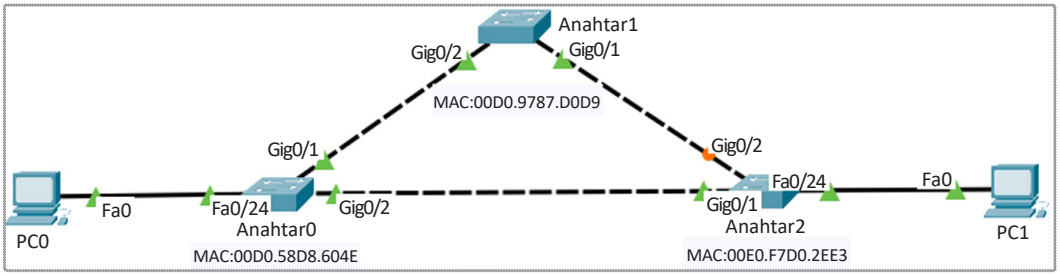
Rapit PVST: Özel üreticiye özgü bir protokol olup RSTP ve PVST+ ın birleşimi gibi davranır.

8.2.8. STP Güvenliği

Varsayılan olarak anahtar cihazlar, bağlantının diğer tarafındaki cihazın türüne bakmaksızın tüm arayüzlerinden STP paketleri gönderir. STP paketlerinin anahtar haricî cihazlara gönderimi, bağlantının diğer tarafında bilgisayar gibi cihazlar varsa zararlı kullanıcılar tarafından paket çözümlemesi yapıldığında ağa zarar verebilecek durumlar ortaya çıkarabilir. Bu durumu ortadan kaldırmak için anahtar cihazlarda yalnızca anahtardan anahtara bağlantılarında STP'nin aktif olarak çalışması istenmelidir. Bunun için bağlantısı anahtar olmayan arayüzleri STP çalışmasına kapatmak gerekecektir. Kapatma işlemi arayüzde "spanning-tree bpduguard enable" komutu uygulaması ile gerçekleşir. Arayüzlerde bu işlemi yapabilmek bir PVST özelliğidir.

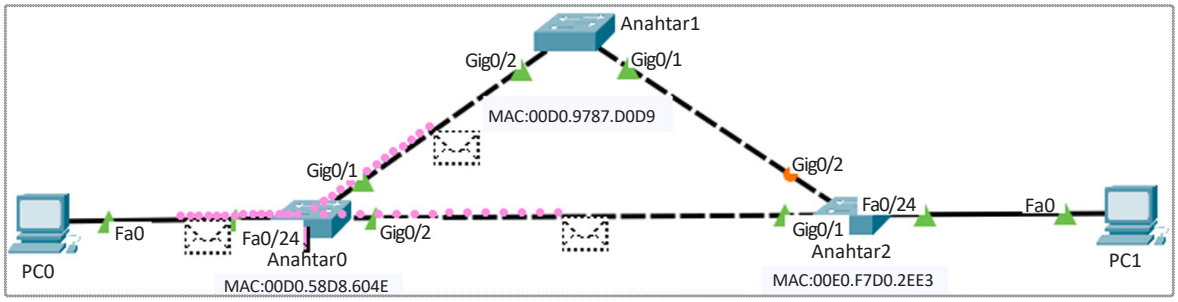
Uygulama 11

Görsel 8.48'de verilen topolojiyi oluşturarak aşağıdaki işlemleri yönergeler doğrultusunda gerçekleştiriniz.



Görsel 8.48: Uygulama 11 için ağ topolojisi

Adım 1: Ağ paketlerini gözlemlemek için Simülation\Show All/None\EditFilters\Misc düğmeleri ile STP paketini seçiniz. Simülasyon\Oynat düğmesi ile ağı gözlemleyiniz.



Görsel 8.49: STP paket dağılımı

Görsel 8.49'da olduğu gibi Anahtar0 STP paketleri tüm arayüzlerden dağılır. Ağdaki diğer anahtar cihazlara gittiği gibi kendisine doğrudan bağlı PC0'a da gönderilir. PC0'ı kullanan ağa zarar verebilecek bir kullanıcı ise bu STP paketinin içeriğini ağ izleme programları ile açıp görüntüleyebilir. Edindiği bilgilerle ağa zarar verebilir.

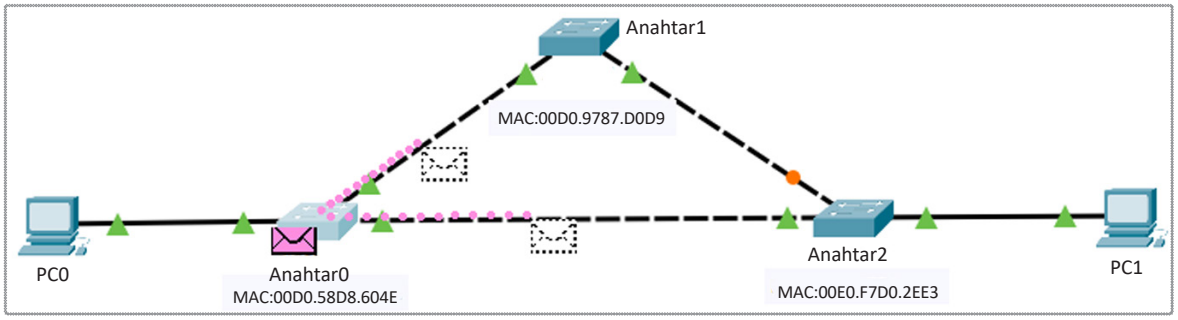
Adım 2: Anahtar0 STP türünü PVST olarak değiştiriniz.

```
Anahtar0(config)#spanning-tree mode pvst
```

Adım 3: Anahtar0 cihazı ile PC0'ın bağlantısını gerçekleştirdiği FastEthernet 0/24 arayüzüne girerek STP çalışmasını durdurunuz.

```
Anahtar0(config)#interface fastEthernet 0/24
Anahtar0(config-if)#spanning-tree bpduguard enable
```

Adım 4: Simülasyonu tekrar oynatıp Anahtar0 ve PC0 arası STP paketlerini gözlemleyiniz. Anahtar0'dan PC0'a paket gönderimi olup olmadığını kontrol ediniz.

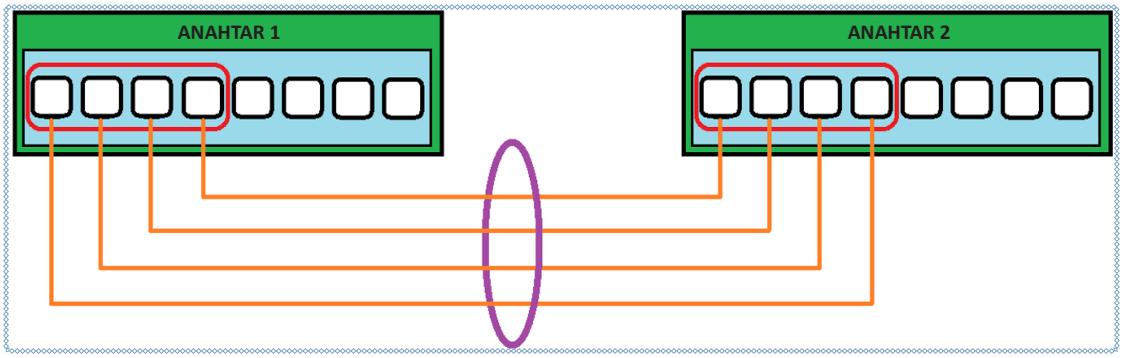


Görsel 8.50: STP'nin istenmeyen arayüzlere gönderimi engellenmesi

Görsel 8.50'de olduğu gibi STP paketleri PC0'a gönderilmez.

8.3. Port Kümeleme

Anahtardan anahtara bağlantılarında fiziksel arayüzleri kümeleyerek karşılıklı yeni mantıksal arayüzler oluşturulabilir. Kümeleme işlemi anahtarlarda karşılıklı olarak yapılır (Görsel 8.51).



Görsel 8.51: Anahtarlar arası arayüz kümeleme

Anahtar arayüzlerini kümelemedeki en önemli amaç, anahtarlar arasındaki bant genişliğini artırmaktır. Arayüzlerin kümelenerek oluşturdukları yeni mantıksal arayüzlerin bant genişliği, kümeye katılan arayüzlerin bant genişliği kadar olabilir. Örneğin 100Mbps bant genişliğine sahip 4 arayüzün kümelenerek oluşturduğu yeni bağlantının hızı 4x100 Mbps= 400 Mbps olacaktır. Bant genişliğini artırmak genellikle trunk ile VLAN trafiğini aktarmak için tercih edilen bir yöntemdir.

STP, kümelenen arayüzlerin her birinde ayrı ayrı çalışmaz. Her fiziksel arayüz oluşturulan yeni mantıksal bağlantıda tek arayüz gibi davranır. Veri iletiminde paketler, küme içindeki fiziksel arayüzler arasında dengelenerek gönderilir. Böylelikle kümedeki tek arayüze veri yükünün binmesi önlenmiş olur. STP yeni mantıksal bağlantıyı tek arayüz olarak hesaplar.

Özellikleri

- Fiziksel arayüzleri birleştirerek yüksek bant genişlikli yeni mantıksal arayüz oluşturulur.
- Bant genişliği artacağı için VLAN trafikleri için daha çok tercih edilir.
- Küme içinde her arayüz, yeni mantıksal arayüz içinde aktiftir ve yük dengelemesi yapar.
- STP küme içinde çalışmaz. STP yeni mantıksal arayüzü hesaplar.
- Fiziksel bağlantılardan birinde hizmet aksaması olduğunda kümelenmiş mantıksal arayüzün çalışması devam eder.

Kümeleme İçin Dikkat Edilmesi Gerekenler

- Kümelenen arayüzlerin, aynı hız ve eşit bant genişliğine sahip olması gerekir.
- Kümelenen arayüzlerin hepsi veri iletiminde tam yönlü ya da yarı yönlü iletimde olmalıdır.
- Kümelenmiş mantıksal arayüzlerde trunk yapılandırması yapılacaksa izin verilen VLAN'lar her iki anahtar tarafında aynı olmalıdır.
- Anahtarlarda karşılıklı olarak bağlantıların aynı numaralı fiziksel arayüzlerde yapılması zorunlu değildir.
- En fazla 6 adet kümelenmiş mantıksal arayüz oluşturulabilir.

Bilgi

Port kümeleme teknolojisi anahtardan anahtara cihazlarda daha çok tercih edildiği gibi sunucu bilgisayar-anahtar cihaz bağlantılarında da artan veri ihtiyacı nedeni ile kullanılabilir.

8.3.1. Kümelenmiş Yeni Mantıksal Arayüzler Oluşturmak

Anahtar cihazda farklı fiziksel arayüzler kümelenerek mantıksal arayüz oluştuğu için anahtar cihazlarda kümeye girecek arayüzlerde, yeni mantıksal arayüzün bildirimi gerekir. Bu bildirim için aşağıdaki komutları uygulamak gerekir.

Anahtar0(config)#interface range fa0/1-4
Anahtar0(config-if-range)#channel-group 1(küme numarası)**mode on/auto/desirable/active/passive**(küme bağlantı modu)

8.3.2. Kümeleme Yöntemleri

Anahtar cihazlar üç farklı yöntemle kümeleme bağlantıları yapabilir. Bunlar:

Statik: Protokol bağımsız çalışır. Anahtarlar arasında otomatik anlaşma yoktur. Her iki anahtarda etkinleştirilmesi gerekir (Görsel 8.52).

Bu yöntemde bağlantılar sadece "on" durumunda etkindir. Anahtarlarda arayüzler "channel-group 1 mode on" şeklinde yapılandırılmalıdır.

Statik		Anahtar1
Anahtar2		On
	On	Evet

Görsel 8.52: Statik kümeleme bağlantı durumu

LACP: IEEE'nin 802.3ad standardı ile geliştirilmiş endüstriyel bir protokoldür. Sahip olduğu modlarla anahtarların anlaşmasını otomatik sağlayabilir (Görsel 8.53).

LACP yönteminin pasif (Passive) ve aktif (Active) şeklinde iki farklı durumu vardır. Her iki anahtarı yapılandırırken sadece Passive-Passive durumunda bağlantı etkin olmaz. Diğer durumların hepsinde bağlantı etkindir. Anahtarlarda arayüzler, "channel-group 1 mode passive/active" şeklinde yapılandırılmalıdır.

LACP		Anahtar1	
		Passivve	Active
Anahtar2	Passive	Hayır	Evet
	Active	Evet	Evet

Görsel 8.53: LACP kümeleme yöntemi ile bağlantı durumu

PAgP: Özel üreticinin geliştirmiş olduğu bir protokoldür. LACP ile aynı şekilde çalışır (Görsel 8.54).

PAgP yönteminin Auto ve Desirable şeklinde iki farklı durumu vardır. Her iki anahtar yapılandırılırken sadece Auto-Auto durumunda bağlantı etkin olmaz. Diğer durumların hepsinde bağlantı etkindir. Anahtarlarda arayüzler, "channel-group 1 modeauto / desirable" şeklinde yapılandırılmalıdır.

PAgP		Anahtar1	
		Auto	Desirable
Anahtar2	Auto	Hayır	Evet
	Desirable	Evet	Evet

Görsel 8.54: PAgP kümeleme yöntemi ile bağlantı durumu

Uygulama 12

http://kitap.eba.gov.tr/KodSor.php?KOD=21059

Görsel 8.55'te verilen topolojiyi oluşturarak aşağıdaki işlemleri yönergeler doğrultusunda gerçekleştiriniz.

Görsel 8.55: Uygulama 12 için anahtardan anahtara kümelenmemiş bağlantısı

Adım 1: Anahtarlar arası arayüz bağlantılarını aşağıdaki gibi yapınız.

Anahtar0		Anahtar1
Fa0/1	--->	Fa0/2
Fa0/2	--->	Fa0/1
Fa0/3	--->	Fa0/4
Fa0/4	--->	Fa0/3

Bilgi

Anahtar arayüzleri varsayılan olarak STP ile çalıştığı için dört bağlantıdan biri tercih edilir. Diğerleri yedek duruma gelir.

Adım 2: Her iki anahtarda kullanılan arayüzlerde LACP kümeleme işlemini aşağıdaki komutlarla yapınız.

Anahtar0 için:
Anahtar0(config)#interface range fa0/1-4
Anahtar0(config-if-range)#channel-group 1 mode active

Anahtar1 için:
Anahtar1(config)#interface range fa0/1-4
Anahtar1(config-if-range)#channel-group 1 mode active

Görsel 8.56: Uygulama 12 için anahtardan anahtara kümelenmiş bağlantısı

Bilgi

Kümelenmiş 4 fiziksel arayüz, her iki anahtarda da tek mantıksal arayüz şeklinde tanımlanır. STP oluşturulan tek mantıksal arayüz için çalışacağından hattın her iki tarafındaki tüm arayüzler, iletim durumundadır (Görsel 8.56).

Adım 3: Anahtarlarda "show ip interface brief" komutu ile yeni **Port-channel 1** mantıksal arayüzünün varlığını kontrol ediniz (Görsel 8.57).

```
Anahtar1#sh ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
Port-channel1          unassigned      YES manual up                    up
FastEthernet0/1        unassigned      YES manual up                    up
FastEthernet0/2        unassigned      YES manual up                    up
FastEthernet0/3        unassigned      YES manual up                    up
```

Görsel 8.57: Anahtar cihazlarda port-channel arayüz listeleri

Adım 4: Görsel 8.58'de verilen VLAN tablosuna göre her iki anahtarda VLAN'lara verilen IP'leri giriniz.

	Adı	Anahtar0 IP	Anahtar1 Ip	Alt Ağ Maskesi
VLAN 10	Oda1	192.168.10.10	192.168.10.11	255.255.255.0
VLAN 20	Oda2	192.168.20.10	192.168.20.11	255.255.255.0

Görsel 8.58: Uygulama 12 için anahtar VLAN tablosu

Anahtar0 için:
Anahtar0(config)#vlan 10
Anahtar0(config-vlan)#name Oda1

```
Anahtar0(config)#vlan 20
Anahtar0(config-vlan)#name Oda2
Anahtar0(config)#interface vlan 10
Anahtar0(config-if)#ip address 192.168.10.10 255.255.255.0
Anahtar0(config-if)#exit
Anahtar0(config)#interface vlan 20
Anahtar0(config-if)#ip address 192.168.20.10 255.255.255.0
```

Anahtar1 için:

```
Anahtar1(config)#vlan 10
Anahtar1(config-vlan)#name Oda1
Anahtar1(config)#vlan 20
Anahtar1(config-vlan)#name Oda2
Anahtar1(config)#interface vlan 10
Anahtar1(config-if)#ip address 192.168.10.11 255.255.255.0
Anahtar1(config-if)#exit
Anahtar1(config)#interface vlan 20
Anahtar1(config-if)#ip address 192.168.20.11 255.255.255.0
```

Adım 5: Anahtar cihazda oluşturulan VLAN'ların kontrolünü "show ip interface brief" komutu ile gerçekleştiriniz (Görsel 8.59).

```
GigabitEthernet0/1     unassigned      YES manual down                  down
GigabitEthernet0/2     unassigned      YES manual down                  down
Vlan1                  unassigned      YES manual up                    up
Vlan10                 192.168.10.11   YES manual up                    up
Vlan20                 192.168.20.11   YES manual up                    up
```

Görsel 8.59: Anahtar cihazlarda VLAN arayüz listeleri

Adım 6: Anahtarlarda kümelenmiş yeni mantıksal arayüz olan port-channel 1'i trunk şeklinde yapılandırınız.

Anahtar0 için:

```
Anahtar0(config)#interface port-channel 1
Anahtar0(config-if)#switchport mode trunk
```

Anahtar1 için:

```
Anahtar1(config)#interface port-channel 1
Anahtar1(config-if)#switchport mode trunk
```

Adım 7: Anahtar cihazlarda trunk arayüzlerini "show interfaces trunk" komutu ile listeleyiniz (Görsel 8.60).

```
Anahtar1#show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Po1         on           802.1q         trunking      1

Port        Vlans allowed on trunk
Po1         1-1005

Port        Vlans allowed and active in management domain
Po1         1,10,20

Port        Vlans in spanning tree forwarding state and not pruned
Po1         1,10,20
```

Görsel 8.60: Anahtar cihazda trunk arayüz listesi

Adım 8: Anahtar cihazlarda kümelenmiş mantıksal arayüzlerin özet bilgisini almak için "show etherchannel summary" komutunu uygulayınız. Bu komut; küme ID bilgisi, protokol türü, küme içine giren fiziksel arayüzlerin ID bilgilerini verecektir.

```
Anahtar1#sh etherchannel summary
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


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

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

1      Po1(SU)           LACP    Fa0/1(P) Fa0/2(P) Fa0/3(P) Fa0/4(P)
```

Görsel 8.61: Anahtar cihazda kümelenmiş arayüz özet bilgisi

Görsel 8.61'de görüldüğü gibi kümeleme yöntemi olarak LACP protokolü kullanılmıştır.

Adım 9: Anahtar cihazlarda "show etherchannel port-channel" komutu ile kümelenmiş arayüzler hakkında daha detaylı bilgi alınız (Görsel 8.62).

```
Age of the Port-channel   = 00d:01h:16m:00s
Logical slot/port   = 2/1       Number of ports = 4
GC                  = 0x00000000      HotStandBy port = null
Port state          = Port-channel
Protocol            =   LACP
Port Security       = Disabled

Ports in the Port-channel:

Index   Load   Port     EC state        No of bits
------+------+------+------------------+-----------
  0     00     Fa0/4    Passive            0
  0     00     Fa0/2    Passive            0
  0     00     Fa0/1    Passive            0
  0     00     Fa0/3    Passive            0
Time since last port bundled:    00d:01h:15m:37s    Fa0/3
```

Görsel 8.62: Anahtar cihazda kümelenmiş arayüz detay bilgisi

Adım 10: Anahtar cihazlarda VLAN IP'leri ile ping iletişim testi yapınız. Bu testin sonucu başarılı olacaktır.

Adım 11: Adım 2'de anahtar cihazlarda LACP kümeleme yönteminin Active-Active eşleşmesine göre kümeleme yapılmıştı. Siz de sırası ile Anahtar0 ve Anahtar1'de Active-Passive, Passive-Active ve Passive-Passive durumlarına göre LACP yöntemi ile kümeleme yapınız.

Adım 12: Diğer kümeleme yöntemi PAgP ile anahtar cihazlar arasında aynı fiziksel arayüzlerde Desirable-Desirable, Auto-Desirable, Desirable-Auto, Auto-Auto durumları ile kümeleme yapınız. Tüm uygulama adımlarını yeniden gerçekleştiriniz.

Aşağıdaki soruları dikkatlice okuyunuz ve doğru seçeneği işaretleyiniz.

1. Aşağıdakilerden hangisi yerel ağ içinde yedeklemenin ortaya çıkarabileceği zafiyetlerden biridir?

A) Yedek yol seçimi
B) Tercih yol seçimi
C) Döngüsel yayın fırtınaları
D) IP kontrolü amaçlı yayın paketleri
E) STP durumlarından kaynaklı arayüzün iletime geçme süresi

2. Aşağıdaki komutlardan hangisi ile Anahtar cihazda MAC tutarsızlığının olduğunu anlayabiliriz?

A) show version
B) show ip interface brief
C) show spanning-tree
D) show vlan
E) show mac-address-table

3. "Üç adet anahtarı bulunan yedeklenmiş bir ağ topolojisinde BID değerleri varsayılan olan anahtarların MAC adresleri sırası ile aşağıdaki gibidir:
Anahtar0: 000d.58af.24c9
Anahtar1: 00e0.0001.0002
Anahtar2: 0001.1ae9.a84d"

Buna göre ağdaki temel köprü anahtarı aşağıdakilerden hangisidir?

A) Anahtar0
B) Anahtar1
C) Anahtar2
D) Anahtar2 ve Anahtar1
E) Temel köprü anahtar tanımlanmaz.

4. Anahtar0 BID:4096
Anahtar1 BID:8192
Anahtar2 BID:32768

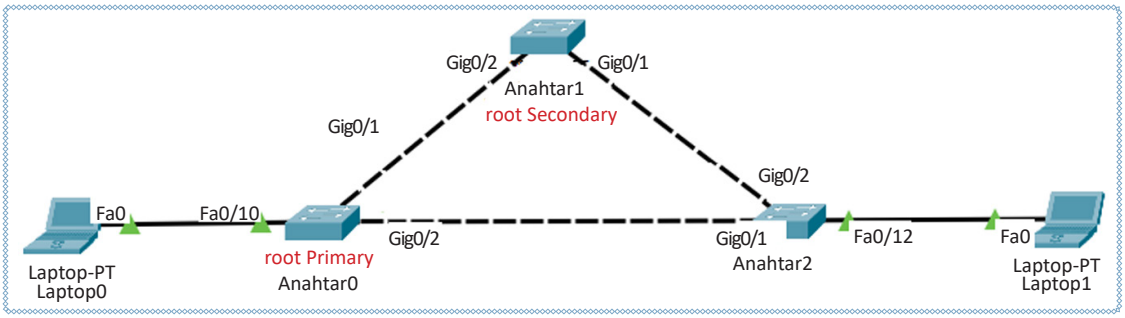
Üç adet anahtarı bulunan yedeklenmiş bir ağ topolojisinde BID değerleri yukarıda verilen anahtarların hangisi temel köprü anahtarıdır?

A) Anahtar0
B) Anahtar1
C) Anahtar2
D) Anahtar0 ve Anahtar1
E) Temel köprü anahtar tanımlanmaz.

5. Aşağıdakilerden hangisi bir STP türü <u>değildir?</u>

A) PVST B) BPDU C) RSTP D) PVST+ E) Rapid PVST

6.



Görsel 8.63: Ölçme ve değerlendirme testi 6. soru topolojisi

Görsel 8.63'te verilen topolojideki anahtarlara komut ile temel köprü anahtar bildirimleri yapılmıştır. **Görsele bakarak hangi anahtar arayüzünün Alternate Port durumunda olduğunu seçiniz.**

A) Anahtar0,Gig0/1
B) Anahtar1,Gig0/1
C) Anahtar1,Gig0/2
D) Anahtar2,Gig0/2
E) Anahtar2,Gig0/1

7. Aşağıdakileri STP durumlarından hangisinde anahtar sürekli turuncu yanar ve ağ trafiğini hiçbir şekilde kabul etmez?

A) Blocking (Engelleme)
B) Listening (Dinleme)
C) Learning (Öğrenme)
D) Forward (İletim)
E) KapalıArayüz

8. "İki anahtar arasında, beşer adet arayüzle yedekli bağlantı topolojisi oluşturulmuştur. Anahtar1 MAC adresi: 000e.91ac.82d1 Anahtar2 MAC adresi:0009.1abe.9783'tür. Bağlantılar karışıklı olarak yapılmıştır.

Verilen bilgiye göre hangi seçenekteki yol, tercih yolu olacaktır?

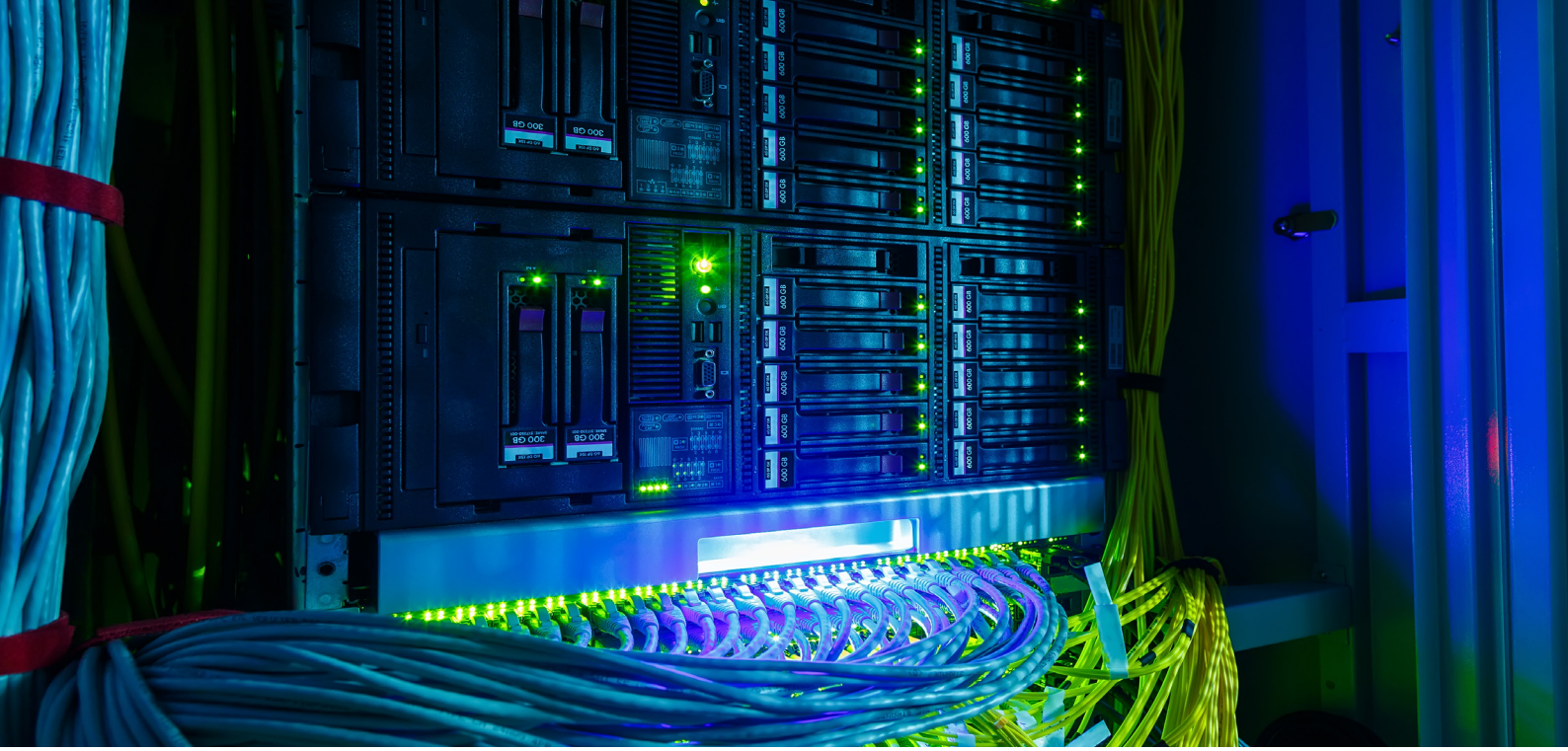
	Anahtar1		Anahtar2
A)	Fa0/1	->	Fa0/5
B)	Fa0/2	->	Fa0/4
C)	Fa0/3	->	Fa0/3
D)	Fa0/4	->	Fa0/2
E)	Fa0/5	->	Fa0/1

9. İki anahtar arasında yapılacak bir arayüz kümeleme işleminde üçer adet 100Mbps hızında arayüz karşılıklı kullanılıyor. Buna göre oluşacak yeni mantıksal arayüz bağlantısının hızı aşağıdakilerden hangisidir?

A) 100 Mbps B) 300 Mbps C) 30 Mbps D) 3000 Mbps E) 33.3Mbps

10. Aşağıdakilerden hangisi bir kümeleme türü durumu değildir?

A) Active B) Passive C) Auto D) Enable E) Desirable



ÖĞRENME BİRİMİ 9

ÜÇÜNCÜ KATMAN ANAHTARLAR

NELER ÖĞRENECEKSİNİZ?

Bu öğrenme birimi ile;

- Üçüncü katman anahtarlama cihazlarının özelliklerini bilecek,
- Üçüncü katman anahtarlama cihazlarının kullanım amaçlarını bilecek,
- Üçüncü katman anahtarlama cihazı ile yönlendirme cihazları arasındaki farkı kavrayacak,
- Üçüncü katman anahtarlama cihazı ile ikinci katman anahtarlama cihazı arasındaki farkı kavrayacak,
- Üçüncü katman anahtarlama cihazında VLAN oluşturacak,
- Üçüncü katman anahtarlama cihazında temel yapılandırma işlemlerini öğrenecek,
- Üçüncü katman anahtarlama cihazı ile VLAN'lar arası yönlendirme yapacak,
- Üçüncü katman anahtarlama cihazı kullanarak dinamik ve statik yönlendirmeyi öğreneceksiniz.

ANAHTAR KELİMELER

Multilayer Switch, Layer 3 Switch, üçüncü katman anahtar, switchport, show ip interface brief, ip routing, SVI, ASIC, FIB, RIB, AT, CEF

Hazırlık Çalışmaları

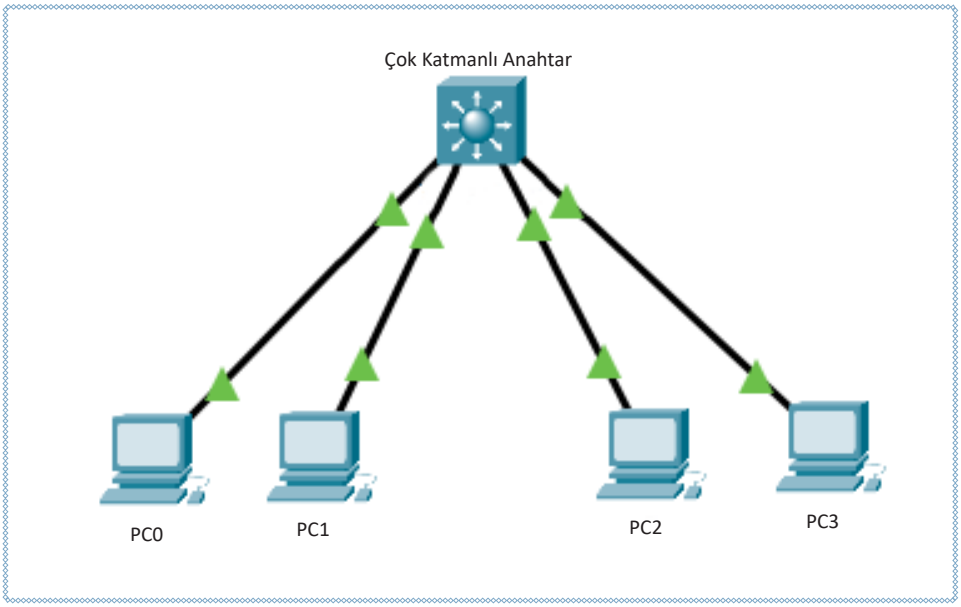
1. Anahtarlama cihazlarını bir yönlendirici gibi kullanabilir miyiz?
2. VLAN'lar arası iletişimi sadece anahtarlama cihazlarını kullanarak yapabilir miyiz? Düşüncelerinizi sınıfta arkadaşlarınızla paylaşınız.

9.1. Üçüncü Katman Anahtarların (Multilayer Switch - Layer 3 Switch) Kullanılması

Anahtarlama cihazları (switch), yerel alan ağlarında MAC adreslerine bakarak veri iletişimini sağlayan cihazlardır. Anahtarlama cihazları veri paketlerini hafızalarında tuttukları MAC adresi tablolarına bakarak diğer cihazlara ulaştırır.

Anahtarlama cihazları OSI referans modelinin ikinci katmanı olan **veri bağı katmanında** çerçeveleri diğer cihazlara iletir. OSI referans modelinin üçüncü katmanı olan **ağ katmanında** ise veri paketlerinin diğer ağda bulunan cihazlara yönlendirme işlemleri yapılır. Dolayısıyla ağ katmanında yönlendirme işlemi yapabilmek için yönlendirici (Router) cihazlar kullanılır. Tüm bu bilgilere ek olarak istisnai bir durum vardır. Çok katmanlı anahtarlama cihazları (Multilayer Switch) hem OSI modeli ikinci katmanında çalışarak Ethernet çerçevelerini iletir hem de bir yönlendirici gibi farklı ağ ya da farklı VLAN'da bulunan cihazlara yönlendirme işlemini yapabilir.

Çok katmanlı anahtarlama cihazları, katman 2 anahtarlama cihazlarının tuttuğu MAC adres tablolarını hafızalarında tuttuğu gibi IP yönlendirme tablosu tutarak aynı zamanda üçüncü katman bir cihaz gibi işlem yapar. Bilgisayarların üçüncü katman anahtarlama cihazına takılması ikinci katman anahtarlama cihazları ile aynıdır (Görsel 9.1).

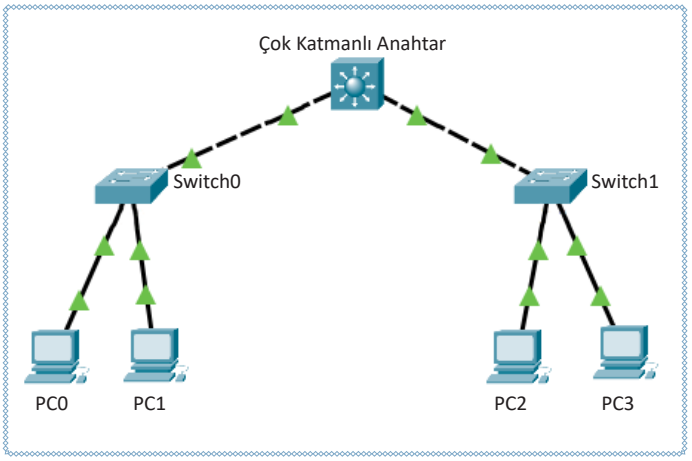


Görsel 9.1: Üçüncü katman anahtarlama cihazı bağlantısı

9.1.1. Üçüncü Katman ve İkinci Katman Anahtarlama Cihazı Farkları

Üçüncü katman ve ikinci katman anahtarlama cihazları, Ethernet paketlerinin iletiminden sorumludur. İkinci katman anahtarlar bu işlemi MAC adres tablosunu tutarak yapar, üçüncü katman anahtarlar ise hem MAC adres tablosunu tutar hem de yönlendirme tablosu tutar. Böylelikle ikinci katman anahtarlama cihazlarından farklı olarak yönlendirme özelliğine sahiptir.

Üçüncü katman anahtarlama cihazları üzerinde sadece Ethernet portları bulunmaktadır ve diğer anahtar cihazlarına bu portlar aracılığı ile fiziksel olarak bağlanmaktadır (Görsel 9.2).



Görsel 9.2: Üçüncü katman ve ikinci katman anahtarlama cihazının fiziksel bağlantısı

9.1.2. Üçüncü Katman Anahtarlama ve Yönlendirici Cihazı Farkları

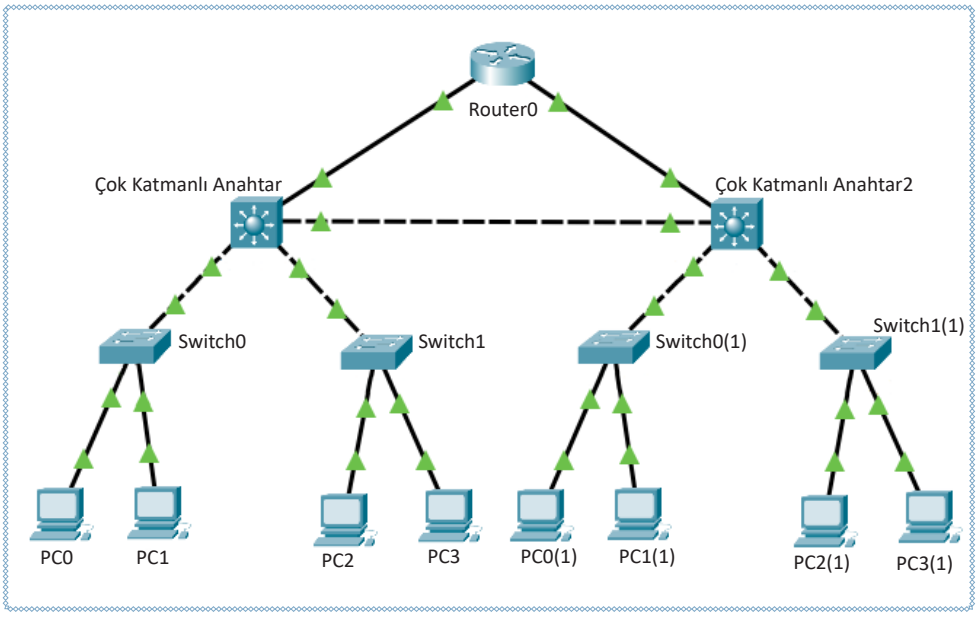
Üçüncü katman anahtarlama cihazları ve yönlendirici cihazlarının ikisi de yönlendirme işlemi yapabilmektedir fakat özellikleri arasında bazı farklılıklar bulunur.

Üçüncü katman anahtarlama cihazları yönlendirme kararlarını verirken bu işlemi donanım olarak gerçekleştirmektedir. Bu işlem, **ASIC** ismi verilen yönlendirme yapma amacıyla önceden hazırlanan ve programlanmış çiplere sahip devreler tarafından sağlanır. Bu sayede çok hızlı anahtarlama işlemi gerçekleştirebilmektedir. Yönlendirici cihazlar ise yönlendirme işlemini yazılımla gerçekleştirmektedir ve hızlı anahtarlama yapamamaktadır.

Üçüncü katman anahtarlama cihazlarında sadece Ethernet portları bulunmaktadır. Yönlendirici cihazlarda ise Ethernet, Seri Port, ISDN portları üzerinden yönlendirme gerçekleştirebilmektedir (Görsel 9.3). Aradaki bu farktan dolayı yönlendirici cihazlar, üçüncü katman anahtarlama cihazlarına oranla daha yüksek maliyetlidir.

Yönlendirici cihazların temel özelliği veri paketlerinin yönlendirmesi olduğu için üçüncü katman cihazlara oranla daha büyük topolojilerde, daha büyük yönlendirme tabloları tutabilmektedir.

Yönlendirici cihazlar; NAT, IPSec, Tünelleme, Güvenlik Duvarı (Firewall) gibi edge (kenar) teknolojileri ile MPLS ve VPN servisleri bünyesinde barındırabilirken üçüncü katman anahtarlama cihazları bu teknolojiye sahip değildir.



Görsel 9.3: Üçüncü katman ve yönlendirme cihazının fiziksel bağlantısı

9.1.3. Üçüncü Katman Anahtarlama Cihazlarının Kullanım Amaçları

Aynı yerel alan ağlarında farklı VLAN'lar birbiri ile iletişime geçmek istediğinde VLAN'lar arası iletişim kullanılmaktadır. VLAN'lar arası yönlendirme yapmanın bilgisayar ağlarında birçok faydası bulunmaktadır. Doğru cihaz kullanımı, iletişimin daha hızlı gerçekleşmesini sağlarken ağ performansını ve verimliliğini arttırmaktadır.

VLAN'lar arasında yönlendirme yapılırken yerel alan ağlarının performansı da düşmemelidir. VLAN'lar arası yönlendirmede üçüncü katman anahtarlama cihazlarının kullanılması, yönlendirici cihaza göre maliyeti düşürerek israfı önler. Bunun yanında üçünü katman anahtarlama cihazları sadece Ethernet teknolojisi kullandığı için yüksek ağ trafiği olan ortamlarda yönlendirici cihazlarına göre daha hızlı VLAN iletişimi sağlar.

Yönlendirici cihazların, farklı geniş alan ağları (WAN) protokollerini desteklemek gibi fazladan görevleri vardır. Üçüncü katman anahtarlama cihazları, böyle bir gereksinimi olmadığı için yerel ağ trafiğini daha hızlı yönetebilmektedir. Üçüncü katman anahtar cihazları yönlendirme işlemini **ASIC**'ler sayesinde donanım yolu ile yönlendirici cihazlar ise yazılım yoluyla yapmaktadır. Yönlendirici cihazların yazılım ile yaptığı yönlendirme işlemi sırasında VLAN'lar arası iletişim trafiğinde verimlilik düşer. Bütün bu maliyet ve performans sıkıntıları göz önünde bulundurulduğunda VLAN trafiğini yönetmek için en uygun ağ cihazının üçüncü katman anahtarlama cihazları olduğu görülmektedir.

9.1.4. Üçüncü Katman Anahtarlama Kavramları

Üçüncü katman anahtarlama cihazlarının veri paketlerini nasıl yönlendirdiğini ve yönlendirici cihazlardan farkını daha iyi anlamak için bazı kavramların bilinmesi gerekmektedir.

Yönlendirme Bilgi Tabanı [FIB (Forwarding Information Base)]: Yönlendirme işlemi yapılırken paket bilgilerinin bir sonraki durağının neresi olacağı bilgisini tutan veri tabanıdır. Ağda yönlendirme veya topoloji değişiklikleri meydana geldiğinde IP yönlendirme tablosu bilgileri güncellenir ve bu değişiklikler FIB'ye yansıtılır. FIB, IP yönlendirme tablosundaki bilgilere göre veri paketlerinin sonraki gideceği adres bilgilerini saklar. Yönlendirme tablosundan buraya aktarılan bilgiler CACHE bellekte tutulduğu için cihaz işlemcisi üzerinde de yük oluşturmamaktadır.

Yönlendirme Tablosu [RIB (Routing Information Base)]: Üçüncü katman anahtarlama cihazlarının yönlendirme işlemini yapabilmesi için gerekli rota bilgilerinin tutulduğu tablodur. **Yönlendirme tablosu** ismiyle bilinir ve üçüncü katman anahtarlama cihazlarında **ip routing** komutu ile aktif hâle getirilir.

Komşuluk Tabloları [AT(Adjacency Tables)]: İki cihaz birbirine direkt olarak bağlı ise bu cihazlar **birbirine komşu cihazlar** olarak adlandırılır. Komşuluk bilgileri tablolarda saklanmaktadır ve daha hızlı iletişim kurulması adına cihazların MAC adresleri komşuluk tablosunda tutulur.

CEF: Çeşitli ağ firmaları, yönlendirmenin daha verimli ve hızlı olması için çeşitli teknolojiler üretmiştir. **CEF**, üçüncü katman anahtarlama cihazlarında daha hızlı yönlendirme sağlayan bir mekanizmadır. CEF teknolojisi olmayan cihazlar sadece yönlendirme tablolarına bakarak yönlendirme işlemini gerçekleştirir. Küçük ölçekli ağlarda sadece RIB ile yönlendirmeyi sağlamak sorun yaratmazken daha büyük ölçekli ağlarda trafiğe sebebiyet vererek gecikmeler yaşanmaktadır. Bu durum cihaz işlemcisine de yük bindirerek verimliliği düşürür. CEF teknolojisi ile cihazlar sadece RIB'e değil, FIB ve komşuluk tablolarından (AT) da bilgi alarak donanım bileşenleriyle yönlendirme işlemini gerçekleştirmektedir. CEF teknolojisi **merkezî** ve **dağıtılmış** olarak iki modda çalışmaktadır.

Yönlendirilmiş Bağlantı Noktası (Routed Port): Cihazlarda IP adresi atanabilen portlara verilen isimdir. Üçüncü katman anahtarlama cihazında bulunan bütün portlar isteğe göre anahtar portu ya da routed port olarak kullanılabilir. Üçüncü katman bir cihaz routed port yapılmak istendiğinde ilgili porta **no switchport** komutunun girilmesi gerekir.

9.1.5. Üçüncü Katman Anahtarlama Cihazı Temel Yapılandırması

Üçüncü katman anahtarlama cihazlarının yapılandırması, ikinci katman anahtarlama cihazı ve yönlendirme cihazlarının yapılandırmalarının birleşimi gibidir.

9.1.5.1 Üçüncü Katman Anahtarlama Cihazı Arayüz Konfigürasyonu

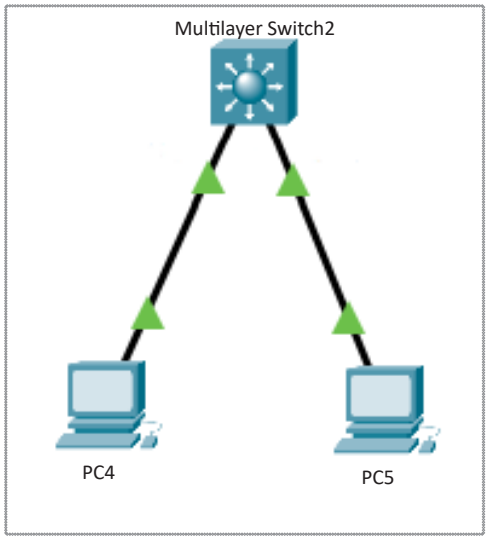
Üçüncü katman anahtarlama cihazının bir yönlendirici gibi çalışması istendiğinde Ethernet portları

yapılandırılmalıdır. “no switchport” komutu kullanılarak anahtar portun ikinci katman yerine üçüncü katmanda çalışması sağlanabilir.

Uygulama 1

http://kitap.eba.gov.tr/KodSor.php?KOD=21060

Görsel 9.4’teki topolojiyi hazırlayarak üçüncü katman anahtarlama cihazının portlarını kontrol ederek **GigabitEthernet 0/1** portunun üçüncü katmanda çalışması işlemini aşağıdaki yönergeler doğrultusunda gerçekleştiriniz.



Görsel 9.4: Arayüzü yönlendirici moduna almak

Adım 1: Çok katmanlı anahtarlama cihazını ağ simülasyon programında ekleyiniz. Aşağıdaki komutları girerek portların bilgilerini görüntüleyiniz (Görsel 9.5).

Switch>**enable**
Switch#**configure terminal**
Switch(config)#**show ip interfaces brief**

```
FastEthernet0/22       unassigned      YES unset  down
down
FastEthernet0/23       unassigned      YES unset  down
down
FastEthernet0/24       unassigned      YES unset  down
down
GigabitEthernet0/1     unassigned      YES unset  down
down
GigabitEthernet0/2     unassigned      YES unset  down
down
Vlan1                  unassigned      YES unset  administratively
down down
```

Görsel 9.5: Arayüz özellikleri

Adım 2: Öncelikle **GigabitEthernet 0/1** portuna girerek IP adresi vermeyi deneyiniz (Görsel 9.5).

Dikkat

IP adresi girişi başarısız olacaktır. Girmek istediğiniz port şu an ikinci katmanda çalışan bir Ethernet portudur (Görsel 9.6).

```
Switch>enable
Switch#configure terminal
Switch(config)#interface gigabitEthernet 0/1
Switch(config-if)#ip address 192.168.1.1 255.255.255.0
```

```
Switch(config-if)#ip address 192.168.1.1 255.255.255.0
                             ^
% Invalid input detected at '^' marker.
```

Görsel 9.6: Komut çıktısı

Adım 3: Portun üçüncü katmanda çalışabilmesi için aşağıdaki komutları giriniz.

```
Switch>enable
Switch#configure terminal
Switch(config)#interface gigabitEthernet 0/1
Switch(config-if)#no switchport
Switch(config-if)#ip address 192.168.1.1 255.255.255.0
```

Adım 4: Aşağıdaki komutları girerek yapılandırmayı kontrol ederek doğrulayınız (Görsel 9.7).

```
Switch>enable
Switch#configure terminal
Switch(config)#show ip interfaces brief
```

```
FastEthernet0/23       unassigned      YES unset  down
down
FastEthernet0/24       unassigned      YES unset  down
down
GigabitEthernet0/1     192.168.1.1     YES manual down
down
GigabitEthernet0/2     unassigned      YES unset  down
down
Vlan1                  unassigned      YES unset  administratively
down down
```

Görsel 9.7: Yapılandırma doğrulama

9.1.5.2. Üçüncü Katman Anahtarlama Cihazlarında Yönlendirme

Üçüncü katman anahtarlama cihazlarında yönlendirme özelliği, varsayılan olarak **kapalı** konumdadır. Yönlendirme özelliği kazandırmak için global yapılandırma moduna girerek **ip routing** komutu ile yönlendirme özelliği aktif hâle getirilir.

```
Switch>enable
Switch#configure terminal
Switch(config)#ip routing
```

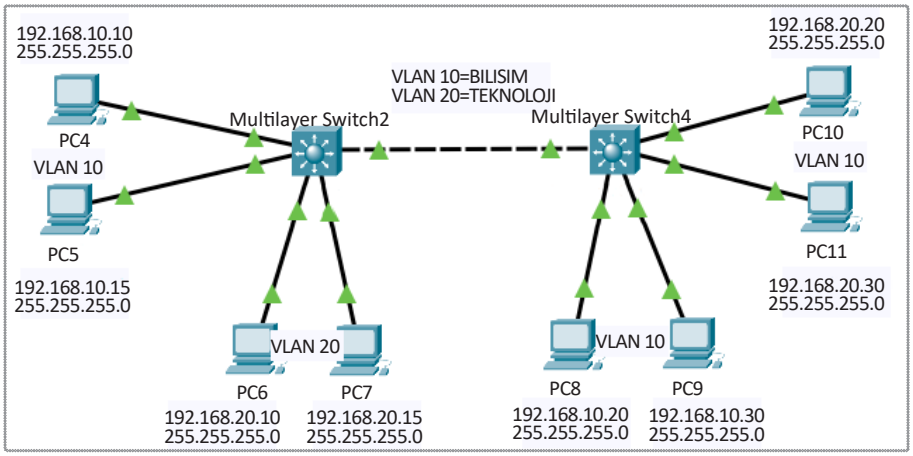
9.1.6. Üçüncü Katman Anahtarlama Cihazında VLAN Yapılandırması

Anahtarlama cihazlarında ağ trafiği sadece kendi yayın alanındaki VLAN'lara ulaşır. Yönlendirme cihazları sayesinde farklı VLAN'lar arası iletişim kurulur. Üçüncü katman cihazlarda **SVI (Switch Virtual Interface)** sayesinde sanal VLAN arayüzleri oluşturarak yönlendirme cihazlarına ihtiyaç duymaksızın VLAN trafiği farklı yayın alanlarına yönlendirilir.

Uygulama 2

http://kitap.eba.gov.tr/KodSor.php?KOD=21061

Görsel 9.8'deki topolojiyi hazırlayarak VLAN'ları oluşturunuz. Oluşturduğunuz VLAN'larda bulunan bütün cihazların haberleşmesini sağlama işlemini aşağıdaki yönergeler doğrultusunda gerçekleştiriniz.



Görsel 9.8: Üçüncü katma anahtarlama VLAN yapılandırma topolojisi

Adım 1: Bütün cihazlarınıza belirtilen IP yapılandırmalarının girişini yapınız.

Adım 2: BILISIM (VLAN 10) ve **TEKNOLOJI (VLAN 20)** isimlerinde VLAN'ları aşağıdaki komutları girerek oluşturunuz.

```
Switch>enable
Switch#configure terminal
Switch(config)#vlan 10
Switch(config-vlan)#name BILISIM
```

Aşağıdaki komutları kullanarak VLAN 20'yi oluşturunuz.

```
Switch>enable
Switch#configure terminal
Switch(config)#vlan 20
Switch(config-vlan)#name TEKNOLOJI
```

Yukarıdaki komutları kullanarak oluşturduğunuz VLAN'ları diğer üçüncü katman anahtarlama cihazında da oluşturunuz.

Adım 3: Üçüncü katman anahtarlama cihazının portlarına bağlı olan bilgisayarların ilgili VLAN'lara atamasını aşağıdaki komutları kullanarak yapınız (FastEthernet 0/1-2 VLAN 10 üyesi FastEthernet 0/3-4 VLAN 20 üyesidir.).

```
Switch>enable
Switch#configure terminal
```

Switch(config)#**interface range fastethernet0/1-2**
Switch(config-if-range)#**switchport mode access**
Switch(config-if-range)#**switchport Access vlan 10**
Switch(config-if-range)#**exit**
Switch(config)#**interface range fastethernet0/3-4**
Switch(config-if-range)#**switchport mode access**
Switch(config-if-range)#**switchport Access vlan 20**

Yukarıdaki komutları diğer anahtarlama cihazında da uygulayınız.

Adım 4: Oluşturduğunuz VLAN yapılandırmasını aşağıdaki komutları girerek kontrol ediniz (Görsel 9.9).

Switch>**enable**
Switch#**show vlan**

```
Switch#show vlan

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

Görsel 9.9: VLAN yapılandırmasının kontrolü

Adım 5: Birbirine **GigabitEthernet0/1** portundan bağlanmış olan üçüncü katman anahtarlama cihazının portlarını aşağıdaki komutları girerek **trunk port** olarak yapılandırınız.

Switch>**enable**
Switch#**configure terminal**
Switch(config)#**interface GigabitEthernet0/1**
Switch(config-if)#**switchport trunk encapsulation dot1q**
Switch(config-if-range)#**switchport mode trunk**

Adım 6: Trunk yapılandırmasının kontrolünü aşağıdaki komutları girerek görüntüleyiniz (Görsel 9.10).

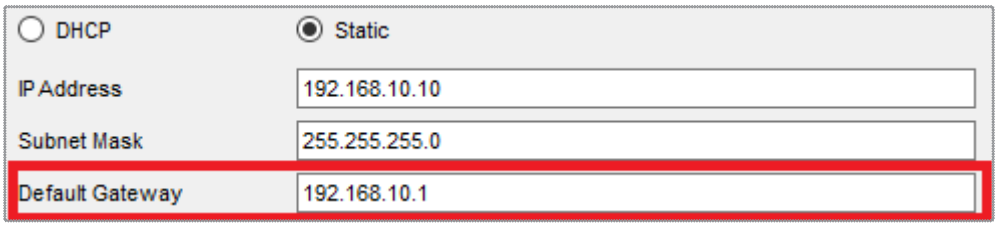
Switch>**enable**
Switch#**show interfaces trunk**

```
Switch#show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Gig0/1      auto         n-802.1q       trunking      1

Port        Vlans allowed on trunk
Gig0/1      1-1005

Port        Vlans allowed and active in management domain
Gig0/1      1,10,20

Port        Vlans in spanning tree forwarding state and not pruned
Gig0/1      1,10,20
```

Görsel 9.10: Trunk yapılandırmasının kontrolü

Adım 7: Oluşturduğunuz VLAN'ların haberleşebilmesi için üçüncü katman anahtarlama cihazlarında aşağıdaki komutları girerek SVI (Switch Virtual Interface) oluşturunuz. Oluşturduğunuz sanal arayüzlere **IP adresi** atayarak bu adreslerin ilgili VLAN için **ağ geçidi adresi** olmasını sağlayınız (Görsel 9.11).

```
Switch>enable
Switch#configure terminal
Switch(config)#interface vlan 10
Switch(config-if)#ip address 192.168.10.1 255.255.255.0
Switch(config-if)#exit
Switch(config)#interface vlan 20
Switch(config-if)#ip address 192.168.20.1 255.255.255.0
```



Görsel 9.11: Bilgisayarlara "Ağ Geçidi Adresi" girişi

Aynı yapılandırmayı diğer üçüncü katman anahtarlama cihazı ve bilgisayarlar için de yapınız.

Adım 8: Yaptığınız VLAN yapılandırmasının kontrolünü aşağıdaki komutları girerek görüntüleyiniz (Görsel 9.12).

```
Switch>enable
Switch#show ip interface brief
```

```
FastEthernet0/23       unassigned      YES unset  down
down
FastEthernet0/24       unassigned      YES unset  down
down
GigabitEthernet0/1     unassigned      YES manual up
up
GigabitEthernet0/2     unassigned      YES unset  down
down
Vlan1                  unassigned      YES unset  administratively
down down
Vlan10                 192.168.10.1    YES manual up
up
Vlan20                 192.168.20.1    YES manual up
up
```

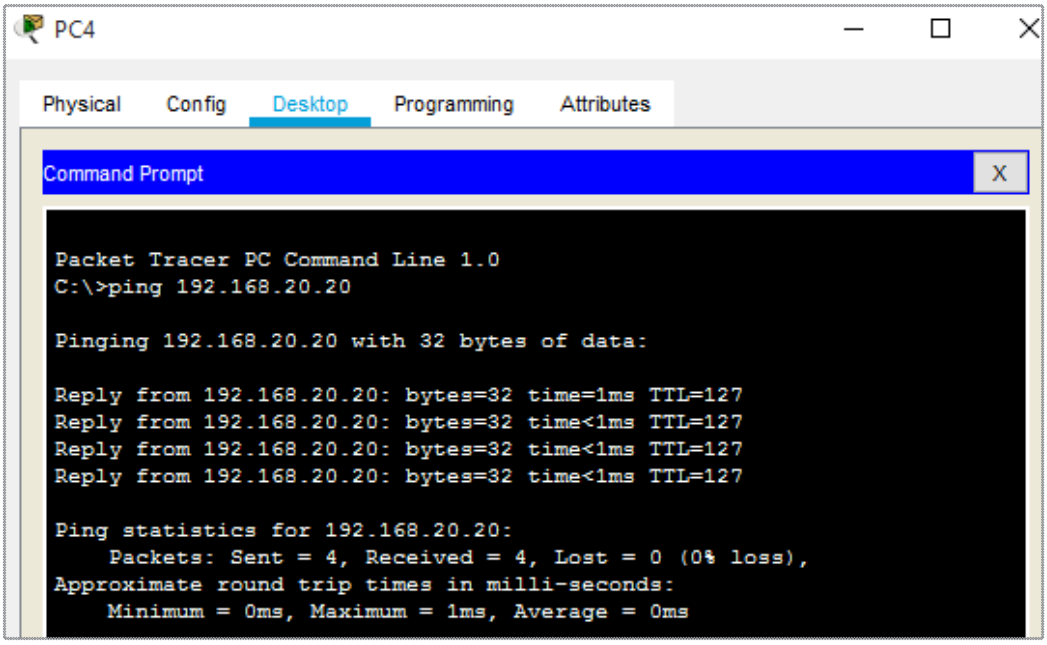
Görsel 9.12: VLAN IP yapılandırması kontrolü

Adım 9: Üçüncü katman anahtarlama cihazınız şu an sadece ikinci katmanda işlem yapmaktadır. VLAN'lar arası iletişim kurabilmek ve IP paketlerinin gidebileceği rotaları oluşturmak için "ip routing" komutunu aşağıdaki gibi girerek cihazınızı üçüncü katmanda veri iletişimi sağlayabilecek duruma getiriniz.

```
Switch>enable
Switch#configure terminal
Switch(config)#ip routing
```

Aynı yapılandırmayı diğer üçüncü katman anahtarlama cihazı için de yapınız.

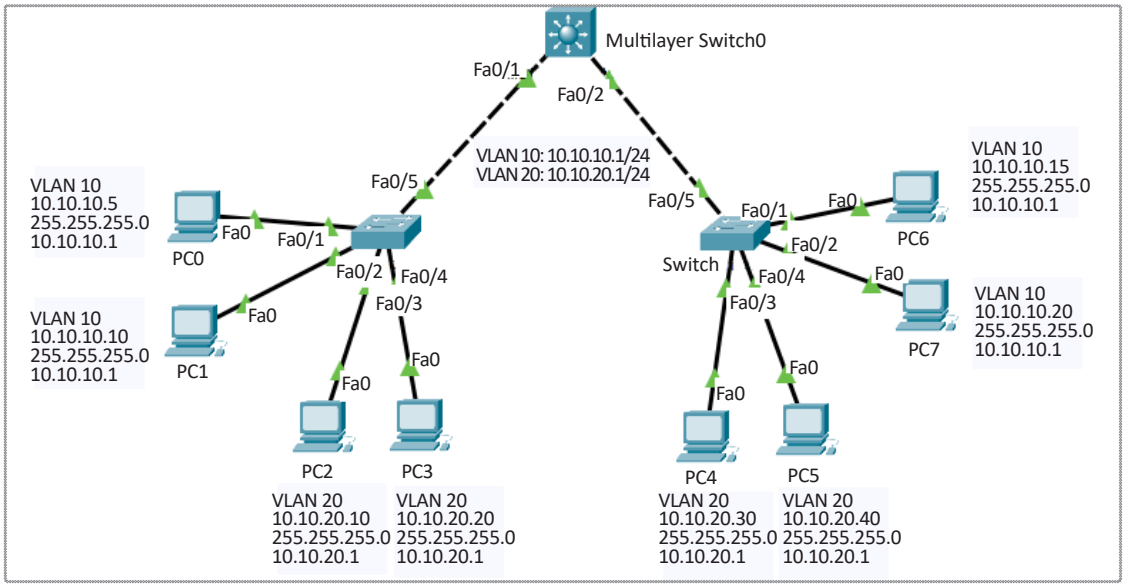
Adım 10: Farklı VLAN'larda bulunan cihazlara ping isteği göndererek gerçekleştirdiğiniz yapılandırmanın kontrolünü sağlayınız (Görsel 9.13).



Görsel 9.13: VLAN'lar arası iletişim kontrolü

Sıra Sizde

Görsel 9.14'te bulunan topolojiyi hazırlayınız. Görselde belirtilen IP adresi yapılandırmalarını bilgisayarlara giriniz. Gerekli VLAN'ları oluşturunuz ve üçüncü katman anahtar cihazını doğru şekilde yapılandırınız. Bütün yapılandırmayı hazırladıktan sonra VLAN'lar arası iletişim (Inter VLAN Routing) yapılandırmasının kontrolünü sağlayarak doğrulayınız.



Görsel 9.14: VLAN'lar arası iletişim topolojisi

9.2. Üçüncü Katman Anahtarlama Cihazında Yönlendirme İşlemi

Üçüncü katman anahtarlama cihazı, gerekli yapılandırmalarla yönlendirici cihaz gibi veri paketlerini iletebilmektedir. Üçüncü katman anahtarlar, statik ve dinamik olarak rotaları yönlendirmektedir. Üçüncü katman anahtar cihaza yönlendirme işlemi yaptırabilmek için Ethernet portlarını anahtar portu olmaktan çıkarmak gerekir. Bu işlem "no switchport" komutu ile yapılabilir. Bu komutun girildiği port, artık üçüncü katmanda paket iletebilecek konuma gelir.

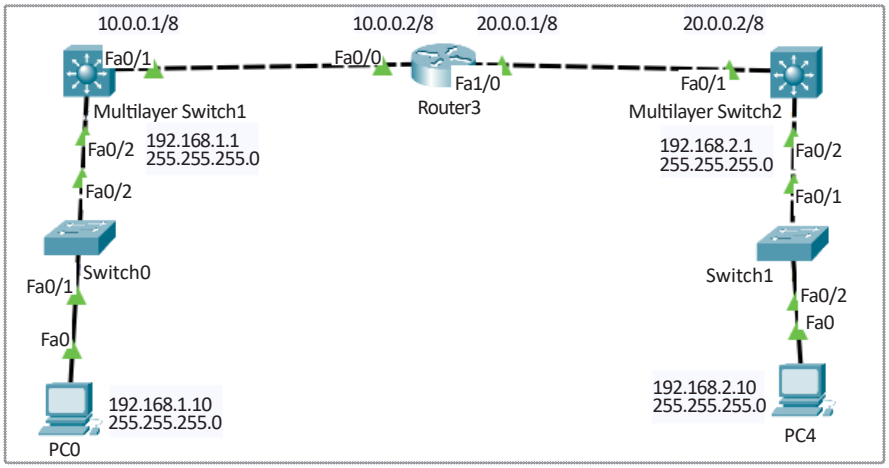
9.2.1. Statik Rota ile Yönlendirme

Üçüncü katman anahtarlama cihazında, yönlendiricilerde kullanılan statik rota komutlarıyla paketlerin farklı ağlara ulaşması sağlanabilir. Bu işlem için **ip route** komutu kullanılır.

Uygulama 3

http://kitap.eba.gov.tr/KodSor.php?KOD=21062

Görsel 9.15'teki topolojiyi hazırlayarak gerekli statik rotaları giriniz. PC0'dan PC4'e iletişimin başarılı olmasını sağlama işlemini aşağıdaki yönergeler doğrultusunda gerçekleştiriniz.



Görsel 9.15: Üçüncü katman anahtarlama cihazında statik yönlendirme

Adım 1: Bütün bilgisayarlara belirtilen IP yapılandırmalarının girişini yapınız.

Adım 2: Üçüncü katman anahtarlama cihazlarını anahtar modundan çıkarıp IP adres girişlerini aşağıdaki komutları kullanarak yapınız.

```
Switch>enable
Switch#configure terminal
Switch(config)#interface fa0/2
Switch(config-if)#no switchport
Switch(config-if)#ip address 192.168.1.1 255.255.255.0
Switch(config-if)#exit
Switch(config)#interface fa0/1
Switch(config-if)#no switchport
Switch(config-if)#ip address 10.0.0.1 255.0.0.0
```

IP adres girişlerini ve anahtar modundan çıkarma işlemlerini diğer üçüncü katman anahtar cihazı için de yapınız.

Adım 3: Yönlendirici cihazın IP adres yapılandırmasını aşağıdaki komutları kullanarak hazırlayınız.

```
Router>enable
Router#configure terminal
Router(config)#interface fa0/0
Switch(config-if)#no shutdown
Switch(config-if)#ip address 10.0.0.2 255.0.0.0
Switch(config-if)#exit
Switch(config)#interface fa0/0
Switch(config-if)#no shutdown
Switch(config-if)#ip address 20.0.0.1 255.0.0.0
```

Adım 4: Üçüncü katman anahtarlama cihazlarının yönlendirme yapabilme özelliğini aşağıdaki komutları kullanarak aktif ediniz.

```
Switch>enable
Switch#configure terminal
Switch(config)#ip routing
```

Aynı işlemi diğer üçüncü katman anahtar cihazı için de uygulayınız.

Adım 5: Üçüncü katman anahtar cihazın statik rotalama işlemini aşağıdaki komutları kullanarak yapınız.

```
Switch>enable
Switch#configure terminal
Switch(config)#ip route 192.168.2.0 255.255.255.0 10.0.0.2
Switch(config)#ip route 20.0.0.0 255.0.0.0 10.0.0.2
```

Diğer anahtar cihaz için de statik rota tanımlamasını aşağıdaki komutları kullanarak yapınız.

```
Switch>enable
Switch#configure terminal
Switch(config)#ip route 192.168.1.0 255.255.255.0 20.0.0.1
Switch(config)#ip route 10.0.0.0 255.0.0.0 20.0.0.1
```

Anahtar cihazların arasında kullandığınız yönlendirici cihazların rotaları bulabilmesi için yönlendirici cihaza da statik rota tanımlamasını aşağıdaki komutları kullanarak yapınız.

```
Router(config)#ip route 192.168.2.0 255.255.255.0 20.0.0.2
Router(config)#ip route 192.168.1.0 255.255.255.0 10.0.0.1
```

Adım 6: Üçüncü katman anahtar cihazın rotalarını aşağıdaki komutları kullanarak görüntüleyiniz (Görsel 9.16).

```
Switch>enable
Switch#show ip route
```

```
Switch#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 not set

C    10.0.0.0/8 is directly connected, FastEthernet0/1
S    20.0.0.0/8 [1/0] via 10.0.0.2
C    192.168.1.0/24 is directly connected, FastEthernet0/2
S    192.168.2.0/24 [1/0] via 10.0.0.2
```

Görsel 9.16: Üçüncü katman anahtarlama cihazının tanımlanmış rotaları

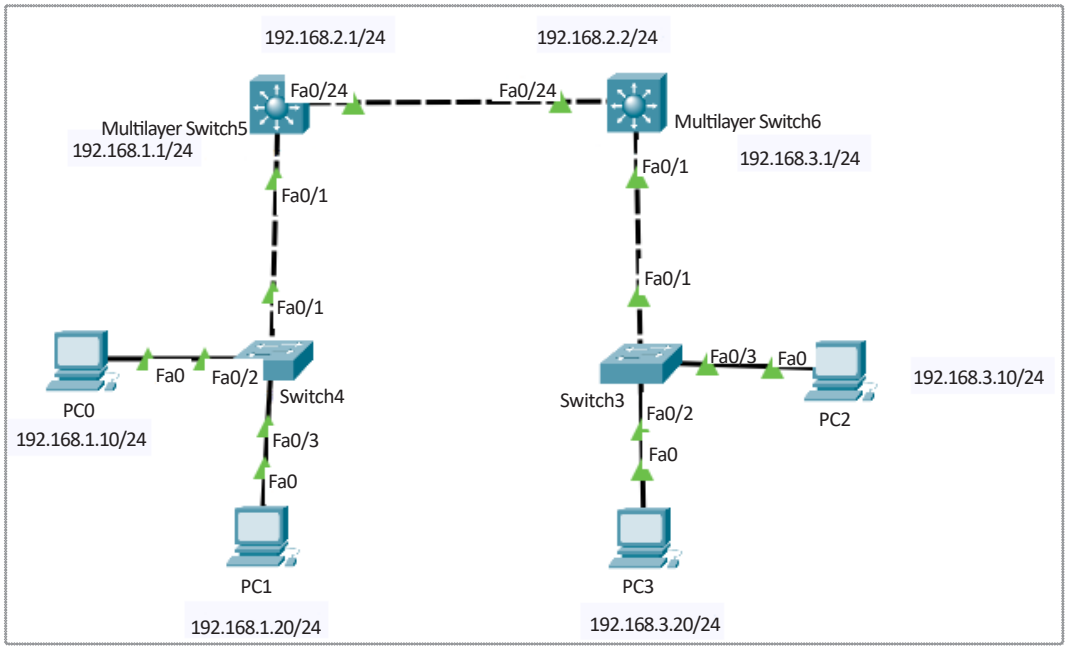
Adım 7: PC0'dan PC4'e ping isteği göndererek yapılandırmayı test ediniz (Görsel 9.17).

```
C:\>ping 192.168.2.10

Pinging 192.168.2.10 with 32 bytes of data:

Reply from 192.168.2.10: bytes=32 time<1ms TTL=125
Reply from 192.168.2.10: bytes=32 time=1ms TTL=125
Reply from 192.168.2.10: bytes=32 time<1ms TTL=125
Reply from 192.168.2.10: bytes=32 time=1ms TTL=125

Ping statistics for 192.168.2.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Görsel 9.17: Bağlantı testinin ekran görüntüsü

Sıra Sizde

Görsel 9.18'de gördüğünüz topolojiyi statik yönlendirme protokolünü kullanarak veri paketlerinin başarılı bir şekilde ulaşmasını sağlayınız.



Görsel 9.18: Statik yönlendirme topolojisi

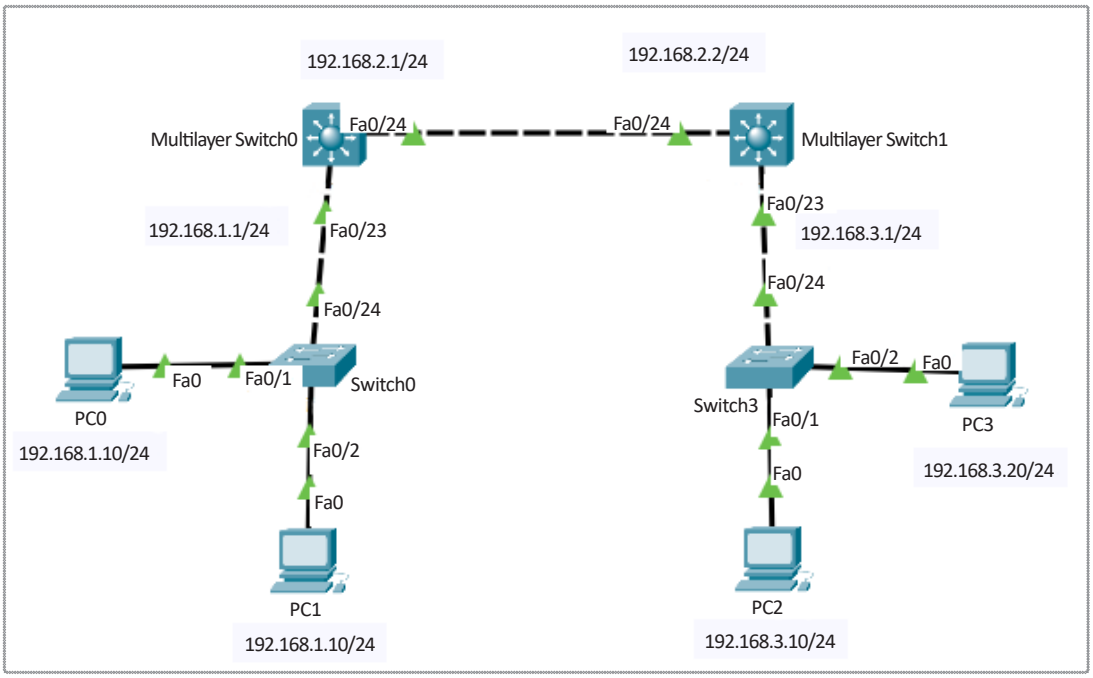
9.2.2. Dinamik Rota ile Yönlendirme

Üçüncü katman anahtarlama cihazında, yönlendiricilerde kullanılan dinamik rota komutlarını uygulayarak paketlerin farklı ağlara ulaşması sağlanır. Bu işlem için **RIP** veya **OSPF** protokolleri kullanılabilir.

Uygulama 4

http://kitap.eba.gov.tr/KodSor.php?KOD=21063

Görsel 9.19'daki topolojiyi RIP dinamik yönlendirme protokolünü kullanarak veri paketlerinin başarılı bir şekilde ulaşması işlemini yönergeler doğrultusunda gerçekleştiriniz.



Görsel 9.19: Dinamik yönlendirme topolojisi

Adım 1: Görseldeki tüm bilgisayarlara belirtilen IP yapılandırmalarının girişini yapınız.

Adım 2: Üçüncü katman anahtarlama cihazlarını anahtar modundan çıkarıp IP adres girişlerini aşağıdaki komutları kullanarak yapınız.

```
Switch>enable
Switch#configure terminal
Switch(config)#interface fa0/23
Switch(config-if)#no switchport
Switch(config-if)#ip address 192.168.1.1 255.255.255.0
Switch(config-if)#exit
Switch(config)#interface fa0/24
Switch(config-if)#no switchport
Switch(config-if)#ip address 192.168.2.1 255.255.255.0
```

IP adres girişlerini ve anahtar modundan çıkarma işlemlerini diğer üçüncü katman anahtar cihazı için de yapınız.

Adım 3: Üçüncü katman anahtarlama cihazlarının yönlendirme yapabilme özelliklerini aşağıdaki komutları kullanarak aktif ediniz.

```
Switch>enable
Switch#configure terminal
Switch(config)#ip routing
```

Aynı işlemi diğer üçüncü katman anahtar cihazı için de uygulayınız.

Adım 4: Üçüncü katman anahtar cihazının RIP protokolü ile dinamik rotalama işlemini aşağıdaki komutları kullanarak yapınız.

```
Switch>enable
Switch#configure terminal
Switch(config)#router rip
Switch(config-router)#network 192.168.1.0
Switch(config-router)#network 192.168.2.0
```

Aynı işlemi diğer üçüncü katman anahtar cihazı için de aşağıdaki kodlarla uygulayınız.

```
Switch>enable
Switch#configure terminal
Switch(config)#router rip
Switch(config-router)#network 192.168.2.0
Switch(config-router)#network 192.168.3.0
```

Adım 5: Üçüncü katman anahtar cihazının rotalarını aşağıdaki komutları kullanarak görüntüleyiniz (Görsel 9.20).

```
Switch>enable
Switch#show ip route
```

```
Switch#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 not set

C    192.168.1.0/24 is directly connected, FastEthernet0/23
C    192.168.2.0/24 is directly connected, FastEthernet0/24
R    192.168.3.0/24 [120/1] via 192.168.2.2, 00:00:11,
FastEthernet0/24
```

Görsel 9.20: Üçüncü katman anahtarlama cihazının tanımlanmış rotaları

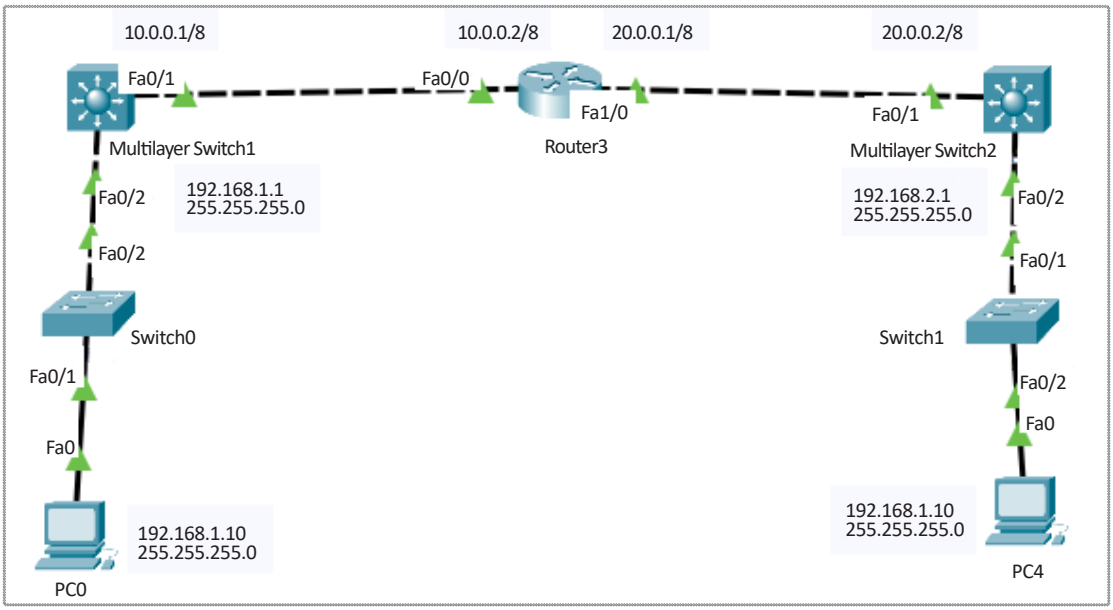
Adım 6: PC1'den PC2'ye ping isteği göndererek yapılandırmayı test ediniz (Görsel 9.21).

```
C:\>ping 192.168.3.10

Pinging 192.168.3.10 with 32 bytes of data:

Reply from 192.168.3.10: bytes=32 time=1ms TTL=126
Reply from 192.168.3.10: bytes=32 time<1ms TTL=126
Reply from 192.168.3.10: bytes=32 time<1ms TTL=126
Reply from 192.168.3.10: bytes=32 time<1ms TTL=126

Ping statistics for 192.168.3.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Görsel 9.21: Bağlantı testinin ekran görüntüsü

Sıra Sizde

Görsel 9.22'deki topolojiyi dinamik yönlendirme protokolünü (RIP ya da OSPF) kullanarak veri paketlerinin başarılı bir şekilde ulaşmasını sağlayınız.



Görsel 9.22: Dinamik rota topolojisi

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

1. ( ) Üçüncü katman anahtar cihazları ASIC'ler sayesinde, donanım özelliklerini kullanarak yönlendirme işlemini gerçekleştirilmektedir.
2. ( ) Üçüncü katman bir cihazı **routed port** yapmak için ilgili porta **no shutdown** komutunu girmek gerekmektedir.
3. ( ) **show ip interfaces brief** komutunu kullanarak anahtarlama cihazı portlarının bilgileri görüntülenmektedir.
4. ( ) Üçüncü katman anahtarlama cihazlarına yönlendirme özelliği kazandırabilmek için global yapılandırma modunda **ip routing** komutunu girmek gerekmektedir.
5. ( ) Üçüncü katman cihazlarda, **SVI (Switch Virtual Interface)** sayesinde sanal VLAN arayüzleri oluşturulmaktadır.
6. ( ) Üçüncü katman cihazlarda sadece statik yönlendirme yapabilme özelliği vardır.
7. ( ) Üçüncü katman anahtarlama cihazları ile VLAN'lar arası yönlendirme yapabilmek için mutlaka router (yönlendirici) kullanmak gerekmektedir.

B. Aşağıdaki soruları dikkatlice okuyunuz ve doğru seçeneği işaretleyiniz.

8. Aşağıdaki seçeneklerde verilen komutların hangisi ile üçüncü katman anahtarlama cihazının yönlendirme rotaları görüntülenebilir?

A) show ip route
B) show ip interface brief
C) show vlan
D) no switchport
E) show ip address

9. Üçüncü katman anahtarlama cihazının yönlendirme işlemi yapılırken paket bilgilerinin bir sonraki durağının neresi olacağı bilgisini tutan veri tabanı aşağıdakilerden hangisidir?

A) RIB
B) FIB
C) AT
D) CEF
E) ASIC

10. Üçüncü katman anahtarlama cihazları üzerinde bulunan portlara verilen isim aşağıdakilerden hangisidir?

A) Enable
B) Interface
C) Brief Port
D) Routing
E) Ethernet

11. Üçüncü katman anahtarlama cihazlarında yönlendirme bilgileri aşağıdaki komutlardan hangisi ile öğrenilir?

A) Show ip route
B) Show brief port
C) Show interface brief
D) Show routing
E) Show fastethernet

ÖĞRENME BİRİMİ 10

ANAHTAR GÜVENLİĞİ

NELER ÖĞRENECEKSİNİZ?

Bu öğrenme birimi ile;

- Anahtar port güvenliğini bilecek,
- Dinamik IP verme sürecinde yapılabilecek saldırı ve önlemleri bilecek,
- Adres çözümleme protokolü açıklarını ve açık önlemlerini kavrayacak,
- IP paketleri kullanılarak yapılabilecek ataklar ve atakların önlemlerini bilecek,
- VLAN açıkları ve güvenlik önlemlerini bilecek,
- Anahtarlama cihaz güvenliğindeki hata izleme metotlarını öğrenecek,
- Anahtarlama cihazlarındaki hataları çözümleme yollarını öğreneceksiniz.

ANAHTAR KELİMELER

DHCP Snooping, IP Source guard, Port güvenliği, VLAN hopping, Switchport Security, Dinamik ARP, Adres Çözümleme Protokolü, VLAN, VLAN atlama, binding, Trunk Port, Shutdown, restrict, protect

Hazırlık Çalışmaları

1. Siber saldırı size ne ifade ediyor? Açıklayınız.
2. Daha önce siber saldırıya uğradınız mı? Cevabınız evet ise neler yaşadığınızı arkadaşlarınızla paylaşınız.
3. Siber saldırılara karşı hangi önlemler alınabilir? Düşüncelerinizi sınıfta paylaşarak arkadaşlarınızla birlikte alınabilecek önlemler listesi oluşturunuz.

10.1. Anahtar Port Güvenliği Yapılandırması (Switchport Security)

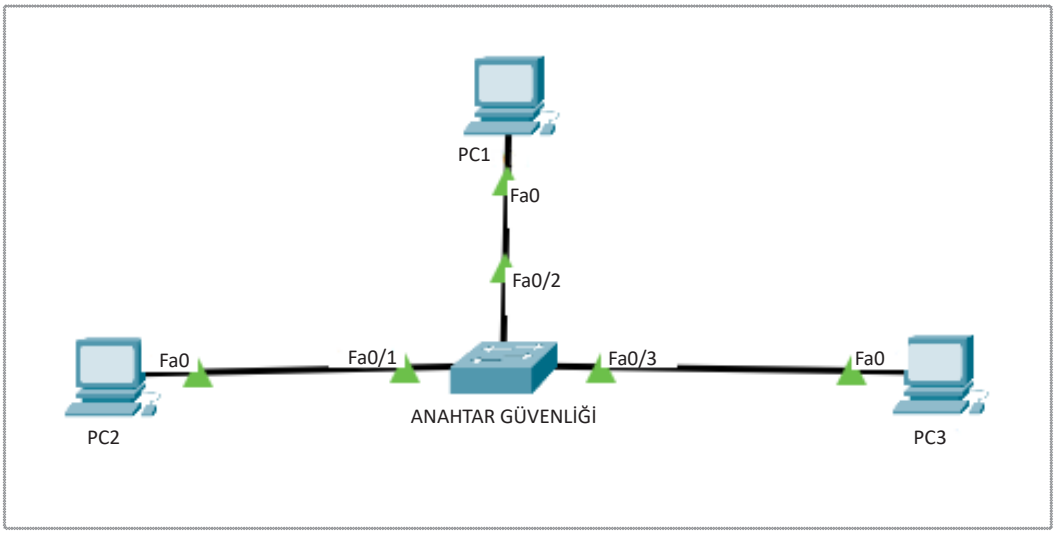
Anahtarlama cihazları (switch), yerel alan ağlarında birden fazla cihazın aynı ağa bağlanmasını sağlar. Birden fazla kullanıcılı ağlarda güvenliği sağlamak ve saldırıların önüne geçmek amacıyla anahtarlama cihazı üzerinde **switchport security** yapılandırması yapılır.

Switchport Security yapılandırması ile anahtarlama cihazı üzerinde bulunan portlara, yetkisiz bağlantı yapılmasının önüne geçilir. Switchport security ile anahtarlama cihazları yapılandırılırken MAC adresleri kullanılmaktadır. 48 bitlik ve her cihazda benzersiz olan MAC adresleri, anahtar portları ile ilişkilendirilerek yetkisiz girişler izlenmektedir. İlgili anahtar portunun hangi davranışı sergileyeceği yapılandırılmaktadır (Görsel 10.1).

Switchport Security yapılandırması kullanılarak; anahtar portlarından her birine bağlanabilecek MAC adres sayısı kısıtlanabilir, aktif olarak kullanılmayan portlar devre dışı bırakılabilir ya da kayıtlı olan MAC adresleri dışında gelecek istekler engellenebilir.

Uygulama 1

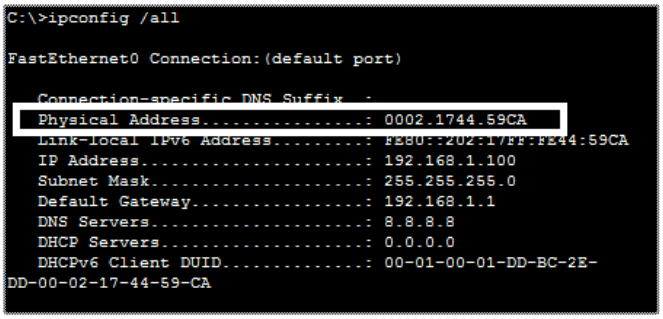
Ağ simülasyon yazılımı kullanarak 1 anahtarlama cihazı ve 3 adet PC ekleyiniz. Bilgisayarların MAC adreslerini öğrenip diğer bilgisayarlarla bağlantı testini yaparak anahtarlama cihazı MAC tablosunu kontrol ediniz. Uygulamayı aşağıdaki yönergeler doğrultusunda gerçekleştiriniz (Görsel 10.1).



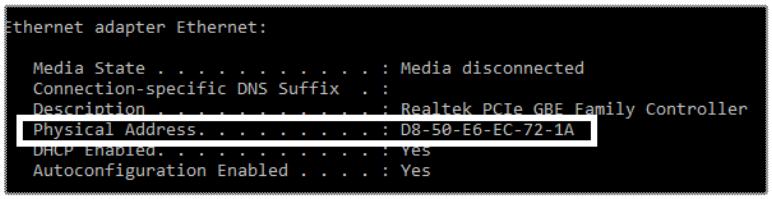
Görsel 10.1: Anahtar port güvenliği topolojisi

Adım 1: Bilgisayarları anahtarlama cihazı 1, 2 ve 3 No.lu portlarına takınız ve aynı ağda olmasını sağlayacak şekilde IP yapılandırmasını giriniz.

Adım 2: Bilgisayarların komut satırlarına ipconfig /all yazarak IP yapılandırmalarını kontrol ediniz. Bilgisayarların MAC adreslerini not alınız (Görsel 10.2 ve Görsel 10.3).

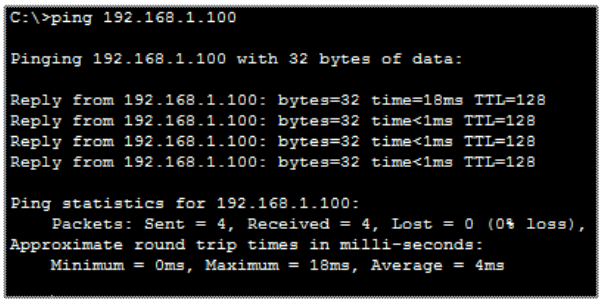


Görsel 10.2: Ağ simülasyon yazılımında komut çıktısı görüntüsü



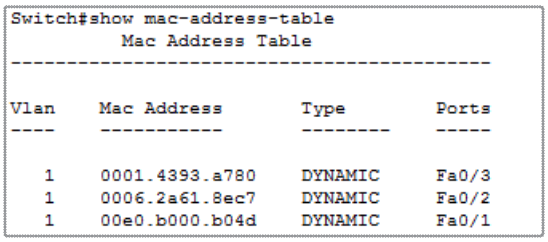
Görsel 10.3: Gerçek cihazda komut çıktısı görüntüsü

Adım 3: Bilgisayarların bağlantılarını ping komutu kullanarak test ediniz (Görsel 10.4).



Görsel 10.4: Ping komutu çıktısı

Adım 4: Anahtarlama cihazına "**Switch# show mac-address-table**" komutunu girerek MAC adres tablosunu görüntüleyiniz ve MAC tablosu doğruluğunu kontrol ediniz (Görsel 10.5).



Görsel 10.5: MAC adres tablosu

Anahtarlama cihazı üzerinde **port güvenliğini** aktif edebilmek için **switchport port-security** komutu kullanılmaktadır. Komutu kullanmak için sınırlandırılmak istenen anahtar portunun arayüzüne giriş yapmak gerekmektedir. Giriş yaptıktan sonra arayüz ile MAC adresini eşleştirerek yetkisiz kullanıcıların ilgili port üzerinden anahtar cihazına bağlanmasının önüne geçilir.

Port güvenliği uygulanırken belirlediğiniz MAC adreslerinin girişini kullanıcı, statik olarak yapabileceği gibi ilk takılan cihazın MAC adresi ile dinamik olarak eşleşmesi de sağlanabilir (Görsel 10.6).

```
Switch(config-if)#switchport port-security mac-address ?
  H.H.H    48 bit mac address
  sticky   Configure dynamic secure addresses as sticky
```

Görsel 10.6: Port security komutu

Uygulama 2

http://kitap.eba.gov.tr/KodSor.php?KOD=21064

Görsel 10.1'deki uygulamada hazırlanan topolojide 2 No.lu bilgisayarın MAC adresi ile anahtarlama cihazının 1 numaralı portunu eşleştirerek port güvenliğini sağlayınız. Yetkisiz cihaz girişi yapmaya çalışarak test ediniz. Uygulamayı aşağıdaki yönergeler doğrultusunda gerçekleştiriniz.

Adım 1: Anahtarlama cihazı 1 No.lu portunun arayüzüne giriş yapınız. Aşağıdaki komutları girerek anahtar güvenliğini aktif hâle getiriniz.

Dikkat

Anahtar güvenliğini aktif ettirmeden önce anahtar portlarını **dinamik moddan Access moduna** almanız gerekmektedir. Aksi takdirde anahtar güvenliği aktif olmaz ve aşağıdaki hatayı alırsınız (Görsel 10.7).

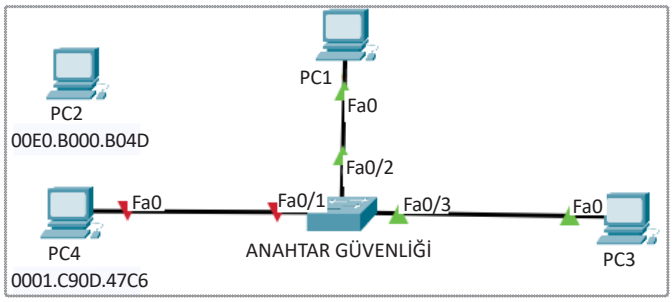
```
Switch(config-if)#switchport port-security
Command rejected: FastEthernet0/3 is a dynamic port.
```

Görsel 10.7: Port security komutu hatası

```
Switch>enable
Switch#configure terminal
Switch(config)#interface fastethernet 0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security mac-address 00E0.B000.B04D
```

Adım 2: Yapılandırmayı cihazlara ping atarak test ediniz. Bağlantıları başarılı olarak test ettikten sonra 2 No.lu bilgisayarın bağlantısını anahtarlama cihazından çıkarınız ve yeni bir cihaz ekleyiniz.

Adım 3: Yeni eklediğiniz bilgisayarı, anahtarlama cihazının 1 No.lu portuna takınız ve bağlantıyı tekrar test ediniz (Görsel 10.8).



Görsel 10.8: Anahtar güvenliği topolojisi

Yaptığınız test sonucunda yeni eklenen bilgisayar, anahtarlama cihazı ile bağlantısını kopartacaktır.

Sıra Sizde

Yaptığınız uygulamayı **Switch(config-if)#switchport port-security mac-address sticky** komutunu kullanarak anahtarlama cihazı 2 ve 3 No.lu portları üzerinde tekrar ediniz ve MAC adreslerinin dinamik olarak port güvenliğine uygulandığını test ediniz.

10.1.1. Anahtar Güvenliği Port Yapılandırması Parametreleri

Switch(config-if)#switchport port-security komutu ile kullanılabilecek 4 adet parametre bulunmaktadır (Görsel 10.9).

```
Switch(config-if)#switchport port-security ?
  aging          Port-security aging commands
  mac-address    Secure mac address
  maximum        Max secure addresses
  violation      Security violation mode
```

Görsel 10.9: Port Security parametreleri

Aging: Anahtarlama cihazı hafızasında MAC adresinin ne kadar süreyle tutulacağını belirleyen komuttur (Görsel 10.10).

```
Switch(config-if)#switchport port-security aging time ?
  <1-1440>  Aging time in minutes. Enter a value between 1 and 1440
```

Görsel 10.10: Port security aging time komutu

Aging time komutu ile beraber kullanıldığında 1 ile 1440 (dk.) değerleri arasında MAC adresinin anahtarlama cihazı hafızasında tutulmasını sağlamaktadır.

Mac-address: Yukarıdaki örnekte görüldüğü gibi MAC adreslerinin, dinamik veya statik olarak anahtar güvenliği yapılandırmasına eklenmesini sağlamaktadır.

Maximum: 1'den 132'ye kadar MAC adresinin ilgili anahtar portuna atanmasını sağlayan parametredir. Girilen rakam değeri kadar MAC adresi, ilgili porta bu parametre ile bağlanabilmektedir. Varsayılan olarak bir adet MAC adresi ilgili porta atanmaktadır (Görsel 10.11).

```
Switch(config-if)#switchport port-security maximum ?
  <1-132>  Maximum addresses
```

Görsel 10.11: Port security maximum komutu

Violation: Güvenlik ihlali gerçekleştiği takdirde anahtarlama cihazı tarafından yapılması gereken işlem, bu parametre ile belirlenmektedir. Varsayılan olarak port üzerinde kapatma (Shutdown) işlemi uygulanmaktadır (Görsel 10.12).

```
Switch(config-if)#switchport port-security violation ?
  protect    Security violation protect mode
  restrict   Security violation restrict mode
  shutdown   Security violation shutdown mode
```

Görsel 10.12: Port security violation parametleri

10.1.2. Anahtar Güvenliği Yapılandırması İhlalleri

Anahtarlama cihazı, switchport security işlemi uygulanıp kural ihlali tespit edildiğinde üç farklı parametre ile işlem yapabilmektedir. Bu parametreler şunlardır:

- Shutdown
- Restrict
- Protect

Shutdown: Anahtarlama cihazı, kural ihlali tespit ettiğinde varsayılan olarak port **kapatma (Shutdown)** işlemini uygulamaktadır. Shutdown işlemi uygulanan port, tamamen kapalı hâle gelir. Sonrasında doğru cihaz takılsa bile anahtarlama cihazı, port tekrar kapatılıp açılmadıkça iletişim başlamaz. Shutdown modu aktifken iletişim ihlali gerçekleştirdiği takdirde **violation sayacını** 1 arttırarak yöneticiye bilgi verir (Görsel 10.13).

```
Switch#show port-security interface fa0/1
Port Security              : Enabled
Port Status                : Secure-shutdown
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0001.C90D.47C6:1
Security Violation Count   : 1
```

Görsel 10.13: Anahtar güvenliği komut çıktısı

Restrict: Anahtarlama cihazı, kural ihlali tespit ettiğinde portu tamamen kapatmaz ancak iletişim de gerçekleşmez. **Syslog** mesajı üreterek cihaz yöneticisine bilgi verir. Anahtarlama cihazı portu ile eşleştirilen cihaz takıldığında iletişim tekrar başlar. İletişim ihlali gerçekleştiğinde violation sayacını 1 arttırır (Görsel 10.14).

```
Switch#show port-security interface fa0/4
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Restrict
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 00E0.B000.B04D:1
Security Violation Count   : 1
```

Görsel 10.14: Anahtar güvenliği komut çıktısı

Protect: Anahtarlama cihazı kural ihlali tespit ettiğinde portu tamamen kapatmaz ancak iletişim de gerçekleşmez. Ayrıca restrict modundan farklı olarak sisteme Syslog mesajı da göndermez. Anahtarlama portu ile eşleştirilen cihaz takıldığında iletişim tekrar başlar. İletişim ihlallerinde violation sayacını da arttırmaz (Görsel 10.15).

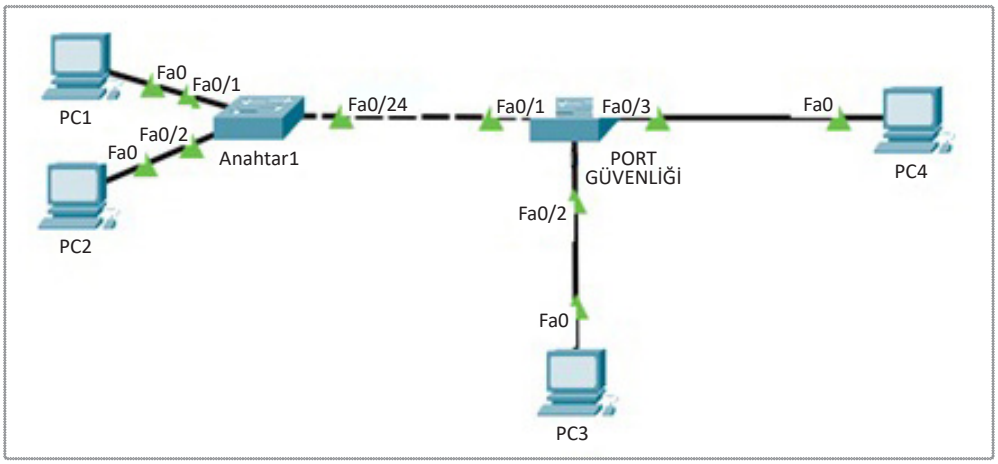
```
Switch#show port-security interface fa0/4
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Protect
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 00E0.B000.B04D:1
Security Violation Count   : 0
```

Görsel 10.15: Anahtar güvenliği komut çıktısı

Uygulama 3

http://kitap.eba.gov.tr/KodSor.php?KOD=21065

Görsel 10.16'daki topolojiyi ağ simülasyon programı kullanarak aşağıdaki yönergeler doğrultusunda gerçekleştiriniz.



Görsel 10.16: Anahtar güvenliği topolojisi

Adım 1: Bilgisayar IP yapılandırmalarını aynı ağda olacak şekilde hazırlayınız ve bağlantıyı test ediniz.

Adım 2: Port Güvenliği isimli anahtar cihazı üzerinde **show mac-address-table** komutunu uygulayarak MAC adreslerini ve takılan portları kontrol ediniz (Görsel 10.17).

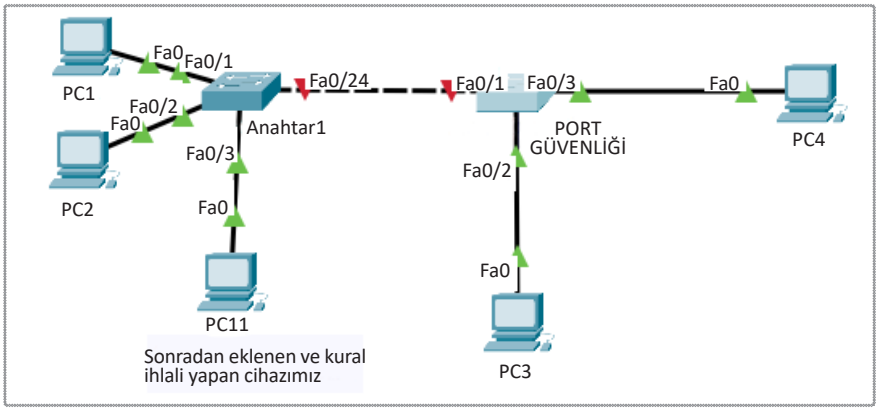
```
Switch#show mac-address-table
          Mac Address Table
-------------------------------------------

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

   1    0002.4a7e.0e18    DYNAMIC     Fa0/1
   1    000c.8569.5828    DYNAMIC     Fa0/3
   1    000d.bd8e.3ddc    DYNAMIC     Fa0/2
   1    0060.473a.2cc2    DYNAMIC     Fa0/1
   1    0090.2160.0beb    DYNAMIC     Fa0/1
```

Görsel 10.17: MAC tablosu çıktısı

Adım 3: Aşağıdaki komutları girerek Port Güvenliği anahtar cihazınızın 1 numaralı portundan dinamik olarak takılan 2 MAC adresinin bağlanmasını sağlayınız. Kural ihlali olursa portun kapatılmasını sağlayınız.

```
Switch>enable
Switch#configure terminal
Switch(config)#interface fastethernet 0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security mac-address sticky
Switch(config-if)#switchport port-security maximum 2
Switch(config-if)#switchport port-security violation shutdown
```

Adım 4: Anahtar1 cihazına yeni bir bilgisayar ekleyerek (Görsel 10.18) kural ihlalini test ediniz ve kontrolünü sağlayınız (Görsel 10.19).



Görsel 10.18: Anahtar güvenliği topolojisi

```
Switch#show port-security interface fa0/1
Port Security              : Enabled
Port Status                : Secure-shutdown
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 2
Total MAC Addresses        : 1
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 1
Last Source Address:Vlan   : 0090.2160.0BEB:1
Security Violation Count   : 1
```

Görsel 10.19: Anahtar güvenliği komut çıktısı

Adım 5: PC3 bilgisayarının MAC adresini Port Güvenliği anahtar cihazının 2 numaralı portu ile eşleştirip port security işlemini uygulayınız. Anahtarlama cihazı, kural ihlali gerçekleştiği takdirde gelen veri paketlerini doğru MAC adresli cihaz bağlanana kadar geçirmemelidir. Sistem yöneticisine mesaj vererek bilgilendirmelidir.

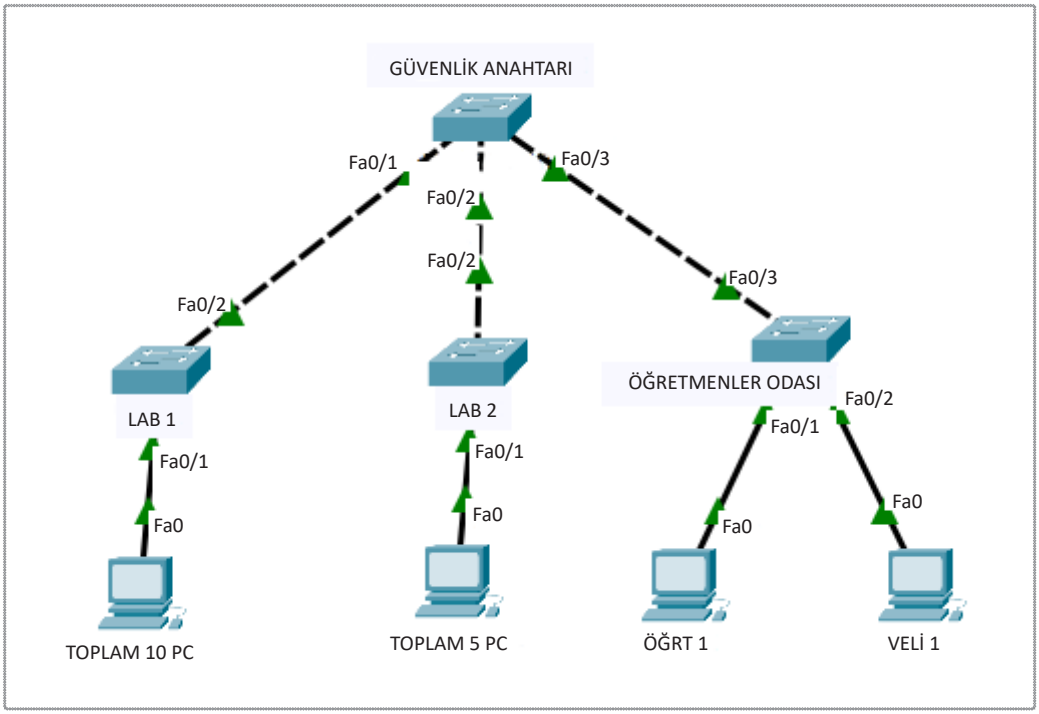
Switch>**enable**
Switch#**configure terminal**
Switch(config)#**interface fastethernet 0/2**
Switch(config-if)#**switchport mode access**
Switch(config-if)#**switchport port-security**
Switch(config-if)#**switchport port-security mac-address (PC3 MAC ADRESİ GİRİLECEKTİR)**
Switch(config-if)#**switchport port-security violation restrict**

Adım 6: PC4 bilgisayarının MAC adresini Port Güvenliği anahtar cihazının 3 numaralı portu ile dinamik olarak eşleştirerek port security işlemini uygulayınız. Anahtarlama cihazı kural ihlali gerçekleştirdiği takdirde gelen veri paketlerini doğru MAC adresli cihaz bağlanana kadar geçirmemelidir. Sistem yöneticisine mesaj vererek bilgilendirme ihtiyacı duyulmamaktadır.

Switch>**enable**
Switch#**configure terminal**
Switch(config)#**interface fastethernet 0/2**
Switch(config-if)#**switchport mode access**
Switch(config-if)#**switchport port-security**
Switch(config-if)#**switchport port-security sticky**
Switch(config-if)#**switchport port-security violation protect**

Sıra Sizde

Görsel 10.20'de verilen topolojiyi aşağıdaki yönergeleri gerçekleştiriniz.



Görsel 10.20: Anahtar güvenliği topolojisi

1. Bütün bilgisayarlar aynı ağda olacak şekilde IP yapılandırmasını hazırlayınız.
2. Güvenlik Anahtarı isimli cihazın 1 numaralı portunda anahtar port güvenliği uygulanacaktır. 1 numaralı port üzerinde dinamik olarak maksimum 10 adet MAC adresi isteği kabul edilecektir. Kural ihlali olduğunda port kapalı (Shutdown) konuma geçecektir.
3. Güvenlik Anahtarı isimli cihazın 2 numaralı portunda anahtar port güvenliği uygulanacaktır. 2 numaralı port üzerinde dinamik olarak maksimum 5 adet MAC adresi isteği kabul edilecektir. Kural ihlali olduğunda iletişim kesilecek fakat kural sağlandığında bağlantı otomatik olarak devam edecektir. Cihaz yöneticisine kural ihlalleri raporlanacaktır.
4. Öğretmenler Odası anahtar cihazı üzerinde port güvenliği uygulanacaktır. Statik olarak ÖĞRT1 ve VELİ 1 cihazlarının MAC adresleri tanımlanarak farklı bir cihaz takıldığında sistem, güvenli moda geçerek veri paketlerini geçirmeyecektir. Sistem yöneticisine herhangi bir rapor göndermesine gerek yoktur.
5. Güvenlik Anahtarı üzerinde kural ihlallerinin gerçekleşip gerçekleşmediğini show komutlarını kullanarak inceleyiniz.

Araştırma

Anahtarlama cihazları üzerinde MAC adresleri varsayılan olarak ne kadar süre tutulmaktadır? Bu süreler değiştirilmek istendiğinde hangi komutların kullanılması gerekmektedir? Araştırınız.

10.1.3. DHCP Araya Girme (DHCP Snooping)

DHCP (Dynamic Host Configuration Protocol), istemci cihazlara IP yapılandırmasını dinamik bir şekilde veren protokolün ismidir. DHCP ile IP adresi, alt ağ maskesi, varsayılan ağ geçidi ve DNS adres bilgilerini, istemci cihazlar otomatik olarak alır. Ağ ortamında bulunan bir DHCP sunucusu, IP yapılandırma isteği gönderen cihazlara adres havuzu içinden uygun olanını gönderir.

Cihazlar, IP yapılandırması almak istediklerinde **DHCP Discover** paketini kullanarak ağ ortamına Broadcast yayını yapar. Ağ üzerinde bulunan DHCP sunucuları da bu paketi alarak karşılığında içeriğinde IP yapılandırma bilgilerinin olduğu **DHCP Offer** paketini yayınlar. DHCP Offer paketinin ulaştığı cihaz, IP yapılandırmasını almak için DHCP sunucusuna **DHCP Request** paketini göndererek, belirtilen yapılandırmayı almaya hazır olduğunu tekli yayın yaparak bildirir. DHCP sunucu ise yapılandırmayı **DHCP Ack** paketini cihaza göndererek süreci tamamlar.

Bilgisayar ağlarında büyük bir kolaylık sağlayan DHCP protokolü, aynı zamanda güvenlik açıklarını da beraberinde getirir. Ağdaki cihazlar IP yapılandırmasını dinamik olarak almak istediklerinde kendisine ilk olarak cevap veren DHCP sunucusu havuzundan bu yapılandırmayı alır. Yerel ağ üzerinde sahte bir DHCP sunucusu oluşturan saldırgan, ağdaki cihazlara sahte yapılandırmalar göndererek sistemi kandırabilir.

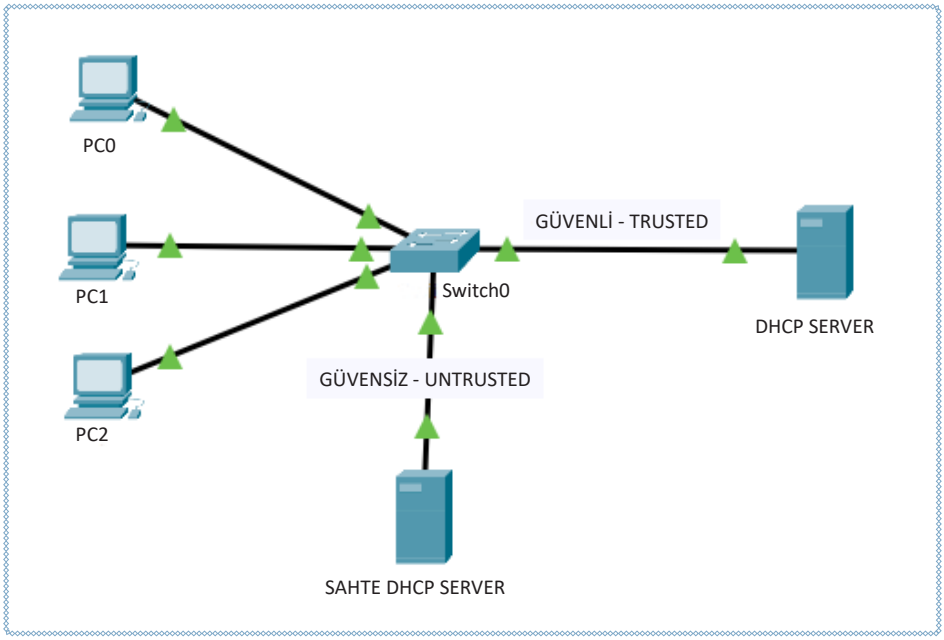
Yerel alan ağlarında sahte DHCP sunucusu oluşturabilecek saldırganlar, cihazların IP isteklerine cevap vererek, varsayılan ağ geçidi adreslerini kendi adresleri olarak gösterebilir. Böylelikle ağ dışına çıkmak isteyen paketler, ağ geçidi sahte olduğundan öncelikle saldırganın cihazına gelecektir. Paketler, gitmek istedikleri yerlere saldırganın cihazı üzerinden gidecektir. Böylelikle saldırgan, bütün paketleri izleme imkânına sahip olacaktır. Saldırganın kuracağı sahte web sunucular (server) ile yönlendirdiği internet adreslerine gidecek olan istemci istekleri, verilerin izlenmesi dışında, verilerin çalınması gibi geri dönüşü zor olacak problemler yaşatabilir.

Anahtarlama cihazı üzerinde **DHCP Araya Girme (DHCP Snooping)** yapılandırmasıyla bu tarz saldırıların önüne geçilmektedir. Yerel alan ağlarında istemciye IP yapılandırması veren sunucu cihazların, anahtar cihaz ile olan bağlantısının **güvenli bağlantı (Trusted)** moduna alınması ile anahtar, farklı portlardan gelen DHCP Request isteklerini engelleyecektir. Böylelikle IP yapılandırmasını sahte sunucuların vermesinin önüne geçilecektir.

Uygulama 4

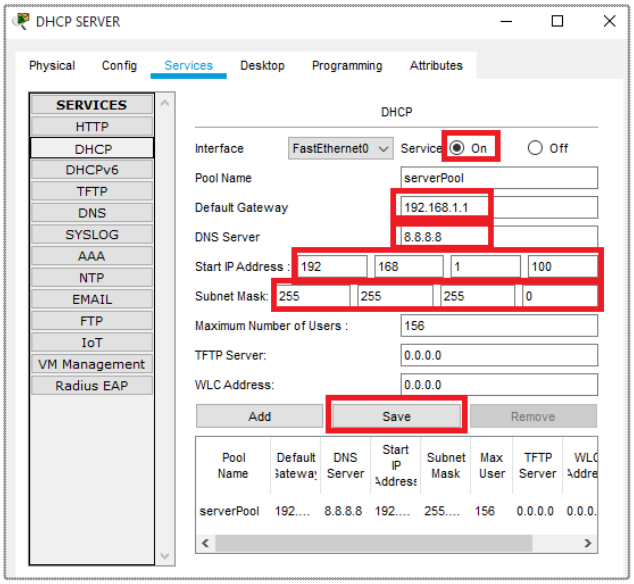
http://kitap.eba.gov.tr/KodSor.php?KOD=21066

Görsel 10.21'deki topolojiyi hazırlayarak sahte DHCP sunuculardan gelecek istekleri engelleyiniz. Gerçek sunucunun bulunduğu anahtar portunu güvenli port yapınız. Uygulamayı aşağıdaki yönergeler doğrultusunda gerçekleştiriniz.



Görsel 10.21: DHCP araya girme topolojisi

Adım 1: Otomatik IP yapılandırması alacak topolojiyi hazırlayınız ve DHCP sunucusunun servis (Services) bölümüne IP yapılandırma bilgilerini girip aktif (on) konuma getiriniz (Görsel 10.22).



Görsel 10.22: DHCP SERVER yapılandırması

Adım 2: Anahtar cihazına ikinci bir DHCP sunucusu ekleyiniz.

Dikkat

Eklediğiniz ikinci sunucu, **sahte DHCP sunucu** olacaktır ve hatalı IP yapılandırma bilgileri içerecektir.

Adım 3: Anahtarlama cihazına sahte DHCP sunucuların yapılandırma vermesinin önüne geçmek amacıyla 4 numaralı anahtar portuna takılı olan gerçek sunucu için DHCP Snooping komutlarını aktif ederek ağ güvenliğini sağlayınız. Aşağıda verilen komutları anahtarlama cihazına giriniz.

```
Switch>enable
Switch#configure terminal
Switch(config)#ip dhcp snooping
Switch(config)#interface fastethernet 0/4
Switch(config-if)#ip dhcp snooping trust
```

Adım 4: DHCP sunucu için yaptığınız güvenli bağlantıyı kontrol ediniz (Görsel 10.23).

```
Switch#show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
none
Insertion of option 82 is enabled
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Interface                  Trusted    Rate limit (pps)
-----------------------    -------    ----------------
FastEthernet0/4            yes        unlimited
```

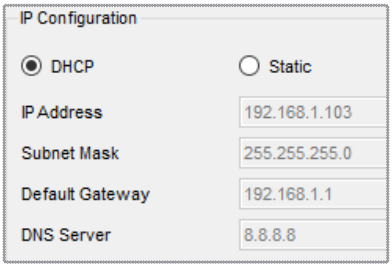
Görsel 10.23: DHCP snooping güvenilir port komut çıktısı

Adım 5: Aynı yapılandırmayı VLAN'a uygulamak için komutları Görsel 10.24'teki gibi kullanınız.

```
Switch(config)#ip dhcp snooping vlan ?
  WORD  DHCP Snooping vlan first number or vlan range, example:
1,3-5,7,9-11
```

Görsel 10.24: DHCP araya girme komut çıktısı

Adım 6: Cihazların otomatik IP yapılandırmasını güvenli porttan aldığının kontrolünü yapınız (Görsel 10.25).



Görsel 10.25: Dinamik IP alma

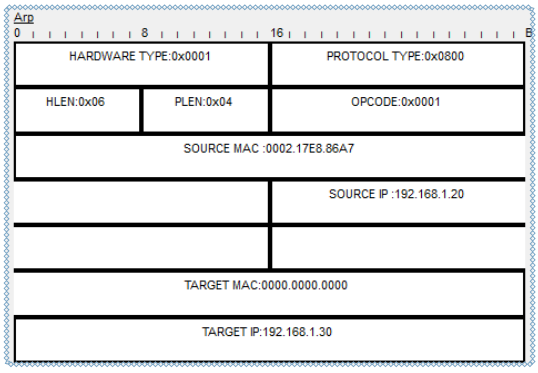
Sıra Sizde

3 adet bilgisayarın bulunduğu bir topoloji hazırlayınız. Anahtarlama cihazı 1, 2 ve 3 numaralı portlarına bilgisayarları takınız. Ortama bir DHCP sunucu ekleyerek sunucuyu 4 numaralı anahtar portuna takınız. DHCP servisini aktif ederek bu cihaz üzerinden bilgisayarların otomatik IP yapılandırması almasını sağlayınız. 5 numaralı anahtar portuna bir DHCP sunucu daha ekleyiniz ve yapılandırma bilgilerini girerek aktif ediniz. Anahtar cihazı üzerinde 5 numaralı portu güvenli port hâline getirerek 4 numaradan gelecek yapılandırma isteklerinin kabul edilmesini önleyiniz. Bilgisayarların tekrar otomatik olarak IP yapılandırması almasını sağlayınız.

10.1.4. Dinamik ARP (Address Resolution Protocol) Denetlemesi

Bilgisayar ağlarında haberleşme, farklı protokoller kullanarak gerçekleşmektedir. Birbirinden farklı ağlarda iletişim gerçekleştirmek istendiğinde IP adresleri kullanılırken yerel alan ağlarında (LAN) iletişim, MAC adresleri kullanılarak sağlanmaktadır. Yerel alan ağlarında MAC adres bazlı haberleşme sağlanırken **Adres Çözümleme Protokolü (ARP)** kullanılır.

IP adresi bilinen cihazların MAC adreslerini öğrenmek için kullanılan ARP protokolü sayesinde, **OSI modeli 2. katmanında** iletişim kurulabilmesi sağlanmaktadır. Yerel alan ağlarında anahtarlama cihazına gelen bir veri paketinde hedef IP adresi yer almaktadır fakat hedef MAC adresi bilinmemektedir (Görsel 10.26).



Görsel 10.26: ARP protokolü IP paket yapısı

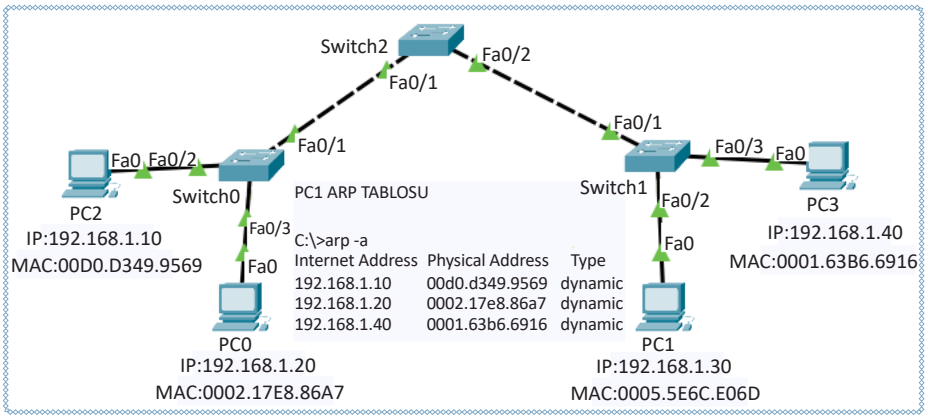
ARP protokolü sayesinde hedef cihaz dâhil bütün cihazlara **arp request** isteği gönderilir fakat bu isteğe sadece hedef cihaz yanıt verir. İsteğe verilen cevap sonucunda hedef IP'lerin MAC adresleri öğrenilmektedir. Öğrenilen MAC adresleri ise cihazların hafızalarında tablo hâlinde tutulur (Görsel 10.27).

```
C:\>arp -a
  Internet Address      Physical Address      Type
  192.168.1.10          00d0.d349.9569        dynamic
  192.168.1.20          0002.17e8.86a7        dynamic
  192.168.1.40          0001.63b6.6916        dynamic
```

Görsel 10.27: ARP komutu çıktısı

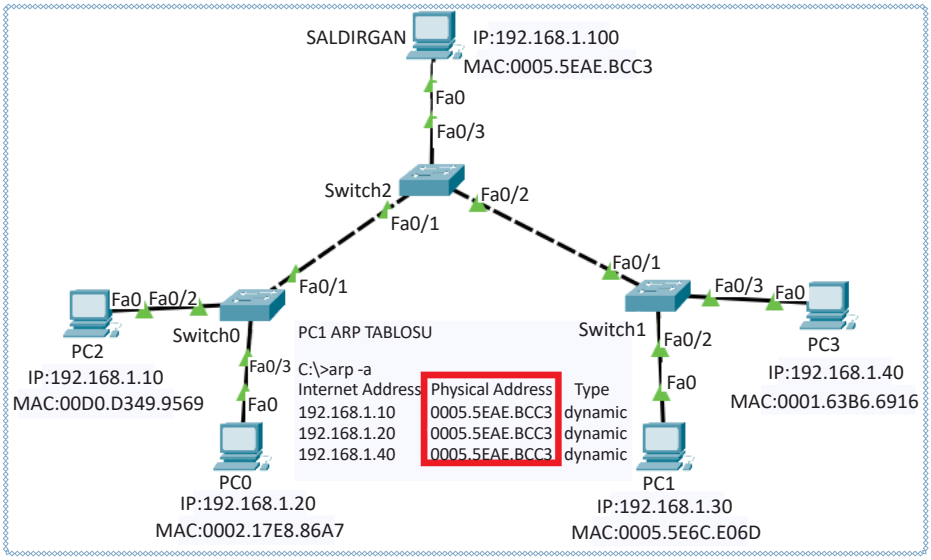
Anahtarlama cihazlarının portlarına bağlanabilecek bir saldırgan çok kolay bir şekilde ARP isteklerini kandırabilir. Bütün ARP isteklerine kaynak MAC adresi olarak kendi adresini verip tabloyu yanıltabilir. Saldırgan bu şekilde bütün ağ trafiğini kendi cihazı üzerinden geçirerek kullanacağı çeşitli araçlarla tüm ağı izleyebilir.

Saldırgan, dinamik ARP isteklerini yanıltarak **ARP sahtekârlığı (spoofing), ARP İstilası (flooding), ARP Zehirlenmesi (poisoning)** gibi saldırılarda bulunabilir.



Görsel 10.28: ARP protokolü topolojisi

Normal bir lokal ağ iletişiminde PC1 için ARP tablosu Görsel 10.28'deki gibi olmaktadır.



Görsel 10.29: ARP protokolü topolojisi

Anahtarlama cihazı portlarına bağlanan saldırgan bilgisayar, ağı kandırarak tabloyu Görsel 10.29'daki gibi değiştirmektedir. Böylece PC1, diğer cihazlarla bağlantı kurmak istediğinde bile bütün veri paketleri saldırgan cihazına gönderilecek, böylelikle saldırgan ağı izleyebilecektir.

Bu tarz saldırıların önüne geçebilmek için anahtarlama cihazında birtakım önlemler alınabilmektedir. Bu önlemlerden biri anahtarlama cihazının portlarını güvenli hâle getirmektir. Anahtarlama cihazının bir portu için bir IP adresi ve bir MAC adresi tanımlaması yapılarak sahte ARP isteklerinin önüne geçilmektedir. Bu işleme **Dinamik ARP Denetlemesi (Dynamic ARP Inspection)** denilmektedir.

Uygulama 5

Görsel 10.29'daki örnekte gösterilen topolojiyi hazırlayarak saldırganın sahte ARP isteği göndermesinin önüne geçiniz. Uygulamayı aşağıdaki yönergeler doğrultusunda gerçekleştiriniz.

Adım 1: Cihazların IP yapılandırmasını Görsel 10.29'da gösterildiği şekilde hazırlayınız.

Adım 2: PC1'in bağlı olduğu anahtarlama cihazında 1 numaralı port üzerinden gelecek sahte isteklerin önüne geçmek için portu güvenli hâle getiriniz. Aşağıdaki komutları anahtarlama cihazına giriniz.

```
Switch>enable
Switch#configure terminal
Switch(config)#ip arp inspection vlan 1
Switch(config)#interface fastethernet 0/1
Switch(config-if)#ip arp inspection trust
```

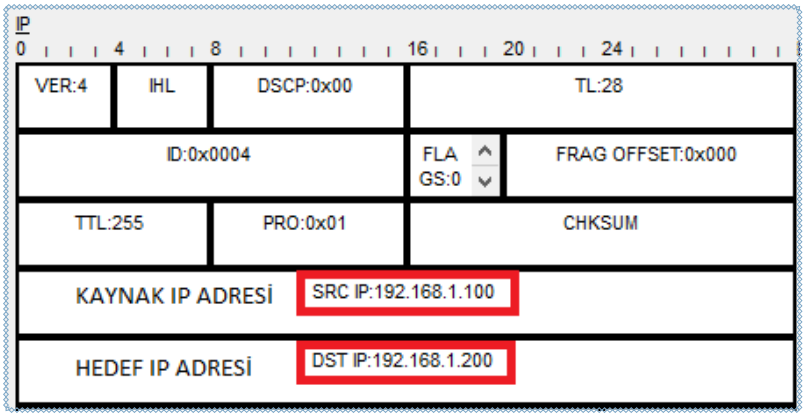
Varsayılan olarak bütün cihazlar VLAN 1 çatısı altında oluşturulmaktadır. Ağ yapımızda farklı VLAN'lar varsa numaraları girilerek portların güvenli olması sağlanabilir.

Araştırma

Gruplara ayrılarak adres çözümleme protokolü kandırılarak yapılacak diğer saldırı türlerine alınabilecek önlemlerin neler olduğunu araştırınız. Elde ettiğiniz sonuçları diğer gruplarla karşılaştırınız.

10.1.5. IP Kaynağını Koruma

IP adreslerinin paket yapısında kaynak IP adresi ve paketin gideceği hedefin IP adresi bulunur (Görsel 10.30). 2. katman iletişimde, IP adresi bilinen cihazlar, ARP sorgusuyla MAC adreslerini öğrenir; iletişim, yerel alan ağı düzeyinde gerçekleşir.



Görsel 10.30: IP paket yapısı

IP adres paketlerinde bulunan kaynak adresler, kullanılan saldırı programlarıyla değiştirilerek anahtar cihazların MAC adres tablosunu yanıltmaktadır. Böylelikle anahtar cihaz üzerinden gönderilen bütün veriler, saldırgan cihazın üzerinden geçmekte olup ciddi veri kaybı ve veri hırsızlığına sebebiyet vermektedir.

Ağda bulunan cihazlar, IP yapılandırması almak istediğinde DHCP sunucu üzerinden 4 aşamalı bir paket aktarımı sonucunda dinamik olarak IP yapılandırmasına sahip olabilmektedir. Anahtarlama cihazına bağlı saldırgan, kullanacağı çeşitli programlar veya kod parçacıklarıyla kendilerini DHCP sunucusu gibi gösterip anahtarlama cihazını kandırabilmektedir.

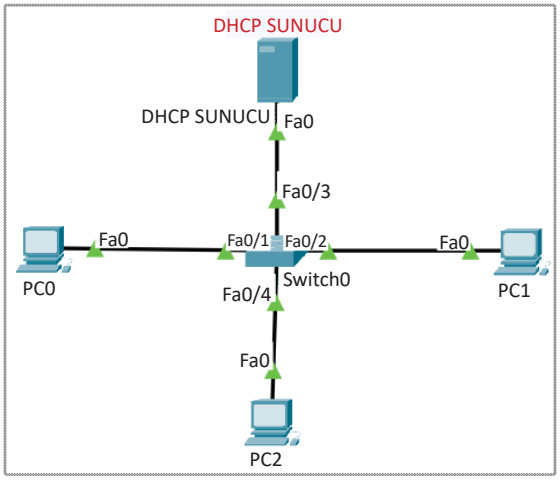
IP kaynağını koruma (IP Source Guard) yöntemi ile anahtarlama cihazı arayüzlerinde **DHCP Snooping** veri tabanı tarafından tanımlanmış trafiğin dışında olan hiçbir IP paketine izin vermez. Ağ iletişiminin güvenli bir şekilde gerçekleşmesi sağlanır. Bu aşamada **IP Source Binding** tablosu ile ağ trafiği yönlendirilir. IP Source Binding tablosunda dinamik ya da statik olarak oluşturulmuş DHCP Snooping Binding ve IP Source Binding verileri bulunmaktadır.

Güvenliği sağlamak isteyen kullanıcı, anahtarlama cihazının portlarına IP kaynağını koruma (IP Source Guard) yapılandırmasını girerek DHCP Snooping Binding tablosundaki MAC adresi, IP adresi ve VLAN bilgilerinin karşılaştırmasını yapar. Böylelikle tabloda olan IP adreslerinin veri paketlerini geçirmesi sağlanır. Ağ trafiğini filtreleyerek güvenlik sağlanmış olur.

IP kaynağını koruma (IP Source guard) yapılandırmasını kullanabilmek için ağ ortamında DHCP sunucusu bulunmalıdır. DHCP Snooping özelliğinin aktif olması gerekmektedir. Yapılandırma işleminden sonra statik IP adresi girilirse **ip source binding** yapılandırması ile tabloya adreslerin eklenmesi gerekir. Aksi hâlde yapılandırılmış anahtarlama cihazı, IP paketlerinin geçmesine izin vermez.

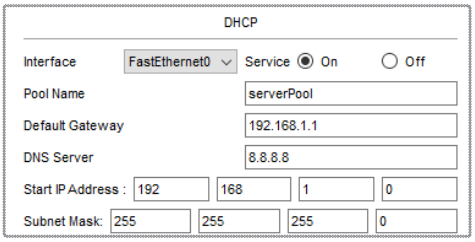
Uygulama 6

Görsel 10.31'de gösterilen topolojiyi kurunuz. Saldırganın IP kaynağını kandırmasının önüne geçiniz. Ağ simülasyon programında **IP Source Guard** uygulamasını aşağıdaki yönergeler doğrultusunda gerçekleştiriniz.



Görsel 10.31: IP kaynağını koruma topolojisi

Adım 1: DHCP sunucu IP yapılandırmasını girip DHCP servisini açarak havuza geçerli IP yapılandırması bilgilerini giriniz (Görsel 10.32).



Görsel 10.32: DHCP servisini aktif etme

Adım 2: Aşağıdaki kodları girerek **ip dhcp snooping** özelliğini aktif ediniz.

```
Switch>enable
Switch#configure terminal
Switch(config)#ip dhcp snooping
Switch(config)#interface fastethernet 0/4
Switch(config-if)#ip dhcp snooping trust
```

Adım 3: Yapılandırmayı ağ simülasyon programında gerçekleştirmek mümkün değildir. Aşağıdaki kodları gerçek cihaza girerek uygulayınız.

```
Switch(config)#interface fastethernet 0/4
Switch(config-if)#ip veriy source
Switch(config-if)#ip veriy source  port security
```

Adım 4: IP Source Guard yapılandırma ve **dhcp snooping** verilerini aşağıdaki komutları girerek görüntüleyiniz (Görsel 10.33).

```
Switch#Show ip source binding
Switch#Show ip verify source
Switch#Show ip dhcp snooping
```

```
-----------------  ---------------  ----------  -------------  ----
00:02:4A:A8:9C:63   192.168.1.1      86400       dhcp-snooping  1
00:60:2F:71:D6:A0   192.168.1.2      86400       dhcp-snooping  1
00:D0:D3:C3:B6:4D   192.168.1.3      86400       dhcp-snooping  1
Total number of bindings: 3
```

Görsel 10.33: IP kaynağını koruma komut çıktısı

10.1.6. VLAN Atlama (VLAN Hoppıng)

VLAN, lokal ağlara bağlı cihazların mantıksal olarak gruplandırılması tekniğine verilen isimdir. Ağ üzerinde bulunan cihazlar bu VLAN'lara üye olarak iletişime geçer ve güvenli aynı zamanda hızlı bir ağ trafiği gerçekleşir. 2. katmanda birbiri ile aynı VLAN üyesi olmayan cihazlar iletişime geçemez. İletişime geçebilmeleri için bir yönlendirici cihaza ve iletişim için de VLAN'lar arası yapılandırmaya (Intervlan routing) ihtiyaç duyulur.

2. katmanda iletişim ARP protokolü aracılığı ile sağlanır. Gönderilen ARP istekleri sadece ait oldukları VLAN'da bulunan cihazlara ulaşır. Diğer VLAN'lar bu ARP isteklerini alamaz. Dolayısıyla iletişim gerçekleşmez.

Doğru kurgulanmamış, güvenlik önlemleri alınmamış ağlarda **VLAN atlama saldırıları** sonucunda ulaşılamayan diğer VLAN'lara erişilebilir. Yetkisiz kullanıcılar ağda gezinebilir. VLAN atlama saldırıları iki şekilde gerçekleşir.

- Anahtar Sahtekârlığı Yöntemi (Switch Spoofing)
- Çift Etiketleme Yöntemi (Double Tagging)

Bu yöntemler çeşitli araçlar ve anahtarlama cihazlarındaki güvenlik açıkları kullanılarak VLAN bilgilerininin elde edilmesine dayanmaktadır. Anahtarlama cihazında DTP protokolü ve "Trunk", "Access" yapılandırmaları kullanılarak saldırılar gerçekleşir.

10.1.6.1. Anahtar Sahtekârlığı Yöntemi (Switch Spoofing)

VLAN'lar oluşturulurken anahtarlama cihazının portları "access" ya da "trunk" olarak yapılandırılmalıdır. Anahtarlama cihazı üzerinden bilgisayarlara bağlanan portlar **access**, anahtarlama cihazından farklı bir anahtarlama cihazına ya da yönlendirici cihaza bağlanan portlar ise **trunk** olarak yapılandırılmaktadır.

Anahtarlama cihazı, access portlar üzerinden sadece tek bir VLAN bilgisini geçirirken trunk portlarından birden fazla VLAN bilgisini geçirebilmektedir. Dolayısıyla anahtarlama portlarını son kullanıcıya ya da diğer anahtarlama / yönlendirici aygıtlarına takılmasına göre yapılandırmak gerekir. Yapılandırma işlemi el ile yapabileceği gibi DTP (Dynamic Trunking Protocol) protokolü ile anahtarlama cihazının dinamik bir şekilde bu işlemi yapması sağlanabilir.

DTP protokolü çeşitli modlarda çalışmaktadır. Bu modlar; **Dynamic Auto, Dynamic Desirable, Access, Trunk** olarak adlandırılır. Anahtarlama cihazı, **varsayılan** olarak **Dynamic Desirable** modundadır.

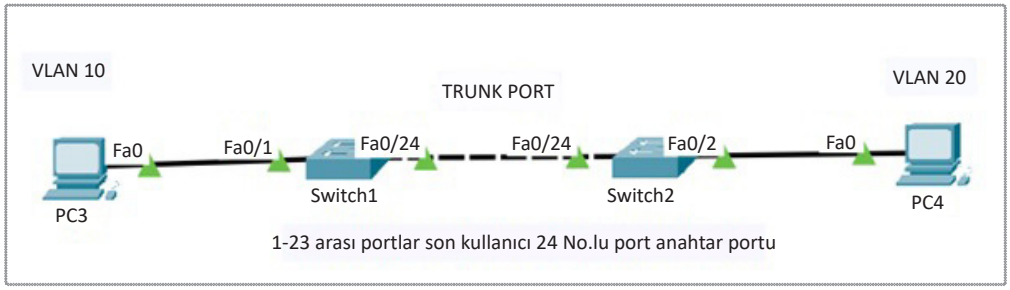
Dynamic Desirable modunda anahtarlama cihazı, başka bir anahtarlama cihazı takılı olan portunu, DTP protokolü sayesinde otomatik olarak algılamaktadır. Birbirlerine bağlı olan portlarını birden fazla VLAN bilgisinin aktarılabilmesi için "trunk" port olarak yapılandırmaktadır. Bağlı olan port, son kullanıcı bilgisayar portu ise bu portu otomatik olarak "access" portu belirlemektedir.

Dinamik modda bir DTP yapılandırmasında anahtar portlarına takılı cihazlardan gelen "trunk" port isteği, otomatik olarak cevaplanmakta ve portlar "trunk" moduna geçirilmektedir. Böylelikle karşı tarafta "access" olması gereken bir bilgisayar dahi olsa kullanacağı programlar yardımıyla DTP paketlerini yanıltarak anahtarlama cihazına "trunk" port olma ve birden fazla VLAN bilgisini geçirme isteği gönderirler. Yapılandırılmamış ve otomatik modda kalmış bu portlar, isteği kabul ederek hemen "trunk" moda geçer. Beraberinde büyük bir güvenlik açığı doğar ve diğer VLAN'ların bilgisine ulaşabilir, ağ dinleme yazılımları ile bütün ağ trafiğini dinleyebilir. Bu tarz saldırıların önüne geçmek için son kullanıcılara ulaşan portlar yapılandırılmalıdır. DTP protokolüne kapatılarak DTP paketlerinin ulaşması engellenmelidir.

Uygulama 7

http://kitap.eba.gov.tr/KodSor.php?KOD=21067

Görsel 10.34'teki topolojiyi kurarak IP ve VLAN yapılandırmalarını oluşturunuz. Anahtar sahtekârlığı saldırısının önüne geçebilecek güvenlik önlemlerini alınız. Uygulamayı aşağıdaki yönergeler doğrultusunda gerçekleştiriniz.



Görsel 10.34: VLAN atlama topolojisi

Adım 1: Aşağıdaki komutları girerek 1 No.lu anahtarlama cihazında 2 No.lu anahtarlama cihazına bağlanan portu **trunk** yaparak DTP protokolünü kapatınız.

```
Switch>enable
Switch#configure terminal
Switch(config)#interface fastethernet 0/24
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport nonegotiate
```

Adım 2: Aşağıdaki komutları girerek 1 No.lu anahtarlama cihazında 1 ile 23 arasındaki portları **Access** olarak yapılandırınız.

```
Switch>enable
Switch#configure terminal
Switch(config)#interface range fastethernet 0/1-23
Switch(config-if-range)#switchport mode Access
```

Sıra Sizde

Görsel 10.34'teki anahtarlama cihazı 2'nin yapılandırmasını gerçekleştiriniz.

10.1.6.2. Çift Etiketleme Yöntemi (Double Tagging)

Anahtar üzerinde bulunan portlar sadece tek bir VLAN üyesi olabilir. Örneğin anahtar üzerinde 10 numaralı porta bir bilgisayar takılı ve bu port VLAN 10 üyesi ise aynı porttaki cihaz VLAN 20'ye üye yapılamaz.

Bir anahtar portundan birden fazla VLAN bilgisinin iletilebilmesi için IEEE 802.1q yapılanması olmalıdır. IEEE 802.1q yapılanması olan portlar VLAN bilgilerini birbirine aktarabilmektedir. Bu portlar, gelen çerçevelere **etiket (Tag)** dediğimiz 4 baytlık (byte) bir veri ekler. Sadece etiketlenmiş bu çerçeveleri iletir, etiketlenmemiş (Untagged) çerçeveler ise iletilmez. **Native VLAN** şeklinde adlandırılan yerel VLAN ise bu tanımlamanın dışında kalmaktadır. **Yerel VLAN** ismi verilen "Native VLAN" herhangi bir etiketlenme yapılmadan IEEE 802.1q yapılandırması olan portlardan aktarılabilmektedir.

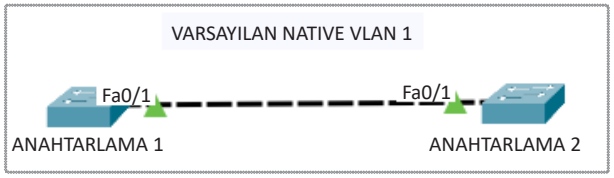
Anahtarlama cihazlarında Native VLAN'lar, varsayılan olarak VLAN 1 numarasını alır. Bunu bilen saldırgan, kendi VLAN etiketine değiştirilmemiş olan Native VLAN numarasını ekleyerek sahte bir çerçeve oluşturabilir. Çeşitli programlar aracılığı ile oluşturulan bu sahte çerçevelerle saldıracağı anahtarda bulunan VLAN bilgisini de ekleyerek anahtarlama cihazlarından Native VLAN'mış gibi geçerek saldırı gerçekleştirebilir. Bu tarz saldırılarda güvenliği sağlamak için varsayılan değeri 1 olan Native VLAN numarası değiştirilebilir. Bunun yanında anahtar cihazının son kullanıcı portlarını da mutlaka **Access Port** olarak yapılandırmak gerekir.

Uygulama 8

http://kitap.eba.gov.tr/KodSor.php?KOD=21068

Anahtarlama cihazının varsayılan yerel VLAN (Native VLAN) portunu değiştiriniz. Uygulamayı aşağıdaki yönergeler doğrultusunda gerçekleştiriniz.

Adım 1: Görsel 10. 35'teki topolojiyi hazırlayınız.



Görsel 10.35: Native VLAN uygulaması

Adım 2: Aşağıdaki komutları girerek anahtarlama 1 cihazı için varsayılan Native VLAN'ı 99 olarak değiştiriniz.

```
Switch1>enable
Switch1#configure terminal
Switch1(config)#vlan 99
Switch1(config)#interface fa0/1
Switch1(config-if)#switchport mode trunk
Switch1(config-if)#switchport trunk native vlan 99
```

Adım 3: Aynı yapılandırmayı aşağıdaki komutları girerek anahtarlama 2 cihazı için de yapınız.

```
Switch2>enable
Switch2#configure terminal
```

```
Switch2(config)#vlan 99
Switch2(config)#interface fa0/1
Switch2(config-if)#switchport mode trunk
Switch2(config-if)#switchport trunk native vlan 99
```

Adım 4: Yapılandırmanızı aşağıdaki komutu yazarak kontrol edip sonuçları görüntüleyiniz (Görsel 10.36).

```
Switch1#show interface trunk
```

```
Switch#show interface trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       on           802.1q         trunking      99
```

Görsel 10.36: Native VLAN port öğrenme komut çıktısı

Sıra Sizde

3 anahtarlama cihazının bulunduğu ve cihazların birbirine bağlı olduğu bir topoloji hazırlayınız. Hazırladığınız topolojiyi VLAN atlama ataklarına karşı yapılandırınız. Native VLAN numarası olarak 50 kullanınız.

10.2. Hata Yönetiminin Denetlenmesi

Anahtarlama cihazlarında, yapılandırmalarda oluşabilecek hataları denetlemek ve önlemler almak için birçok komut bulunmaktadır. Anahtarlama cihazı üzerinde **debug** komutları kullanarak hata denetimlerini izlemek mümkündür.

```
Switch#debug ?
  ip         IP information
  sw-vlan    vlan manager
```

Görsel 10.37: debug ? komutu çıktısı

Anahtarlama cihazında **debug ?** komutu yazıldığında IP ve VLAN hakkında hata yönetimi yapabileceğini göstermektedir (Görsel 10.37).

```
Switch#debug ip ?
  dhcp  Dynamic Host Configuration Protocol
  icmp  ICMP transactions
Switch#debug sw-vlan ?
  packets  vlan manager packets
  vtp      vtp protocol debugging
```

Görsel 10.38: debug ip komutu çıktısı

Debug komutunun IP parametresini kullanarak anahtarlama cihazının DHCP ve ICMP paketleri ile ilgili hata ayıklama işlemi, SW-VLAN komutuyla VLAN paketlerini, VTP protokolü ile ilgili hata ayıklama işlemleri yapılabilir (Görsel 10.38).

10.2.1. Debug IP DHCP Snooping

Anahtarlama cihazlarında DHCP IP alma sürecinde oluşabilecek hataları denetlemek ve düzeltmeler yapmak için kullanılan komuttur.

```
Switch>enable
Switch#debug IP dhcp snooping
```

10.2.2. Debug IP ICMP Events

Ping paketleri veya sorgularında oluşabilecek hatalar ve problem çözümleri için kullanılmaktadır.

```
Switch>enable
Switch#debug IP icmp events
```

10.2.3. Debug SW-VLAN Packet

VLAN paketlerinin iletişiminde oluşabilecek hataları görmek ve problem çözümleri için kullanılmaktadır.

```
Switch>enable
Switch#debug sw-vlan packet
```

Araştırma

Anahtarlama için kullanılabilecek diğer debug komutlarını araştırarak komutların görevlerini defterinize yazınız ve sınıf arkadaşlarınızla paylaşınız.

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

1. ( ) Anahtarlama cihazı üzerinde port güvenliğini aktif edebilmek için switchport port-security komutu kullanılmaktadır.
2. ( ) Aging Time, anahtarlama cihazı hafızasında MAC adresinin ne kadar süreyle tutulacağının belirlendiği komuttur.
3. ( ) 2. katmanda dinamik IP yapılandırması kullanılırsa herhangi bir siber saldırı gerçekleştirilemez.
4. ( ) Debug Ip Dhcp Snooping, anahtarlama cihazlarında DHCP IP alma sürecinde oluşabilecek hataları denetlemek ve düzeltmeleri yapmak için kullanılan komuttur.

B. Aşağıdaki soruları dikkatlice okuyunuz ve doğru seçeneği işaretleyiniz.

5. Aşağıdaki modların hangisinde anahtarlama cihazı kural ihlali tespit ettiğinde portu tamamen kapatmaz ancak iletişim de gerçekleşmez?

A) Access
B) No Shutdown
C) Restrict
D) Shutdown
E) Trust Port

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

A) Çift Etiketleme
B) Debug
C) DNS server
D) Switch port security
E) VLAN Trunk Port

7. Anahtarlama cihazı tarafından güvenlik ihlali gerçekleştiği takdirde yapılması gereken işlem için hangi komut parametresi kullanılır?

A) arp -a
B) Enable
C) Interface
D) Shutdown
E) Violation

8. Aşağıdakilerden hangisi switchport port-security komutu ile kullanılabilecek dört adet parametreden biri değildir?

A) aging
B) mac-address
C) maximum
D) Violation
E) VLAN tagging

9. Anahtarlama cihazlarında DHCP IP alma sürecinde oluşabilecek hataları denetlemek için kullanılan komut aşağıdakilerden hangisidir?

A) debug IP dhcp snooping
B) debug IP icmp events
C) debug sw-vlan packet
D) debug mac- address
E) interface trunk

ÖĞRENME BİRİMİ 11

GENİŞ ALAN AĞ SİSTEMLERİ

NELER ÖĞRENECEKSİNİZ?

Bu öğrenme birimi ile;

- Anahtar port güvenliğini bilecek,
- Dinamik IP verme sürecinde yapılabilecek saldırı ve önlemleri bilecek,
- Adres çözümleme protokolü açıklarını ve açık önlemlerini kavrayacak,
- IP paketleri kullanılarak yapılabilecek ataklar ve atakların önlemlerini bilecek,
- VLAN açıkları ve güvenlik önlemlerini bilecek,
- Anahtarlama cihaz güvenliğindeki hata izleme metotlarını öğrenecek,
- Anahtarlama cihazlarındaki hataları çözümleme yollarını öğreneceksiniz.

ANAHTAR KELİMELER

DHCP Snooping, IP Source guard, Port güvenliği, VLAN hopping, Switchport Security, Dinamik ARP, Adres Çözümleme Protokolü, VLAN, VLAN atlama, binding, Trunk Port, Shutdown, restrict, protect

Hazırlık Çalışmaları

1. Veri paketleri lokal ağın dışına çıktığında hangi cihazlar yoluyla haberleşme sağlayabilir? Düşüncelerinizi arkadaşlarınızla paylaşınız.
2. Modem ayarlarını yapılandırarak kablosuz ağın güvenliğini nasıl sağlanır? Açıklayınız.

11.1. Geniş Alan Ağ Teknolojileri (WAN)

Birbirinden uzak yerel alan ağlarının (LAN) bir araya gelerek oluşturduğu büyük yapıdaki ağlara, **geniş alan ağları [WAN (Wide Area Network)]** denir. Geniş alan ağlarındaki bağlantılar, coğrafi olarak büyüklüğüne ve şekline göre fiber optik kablolar ya da uydular üzerinden gerçekleştirilir. Geniş alan ağlarında bağlantı kurabilmek için yönlendirici ya da özel tünel bağlantılarını sağlayabilecek ekipmanlara ihtiyaç duyulmaktadır.

Geniş alan ağlarında modemler, Frame Relay (FR), X25, ISDN, ATM, SMDS, xDSL gibi teknolojiler kullanılmaktadır. Topolojinin büyüklüğü ve coğrafi alanın özellikleri dikkate alınarak WAN teknolojilerinden biri ya da birkaçı aynı sistemin içinde kullanılabilir.

Geniş alan ağları yapı olarak yerel alan ağlarından farklıdır. Farklı tür cihaz ve bağlantılar ile iletişim sağlanır. Yapılandırmalar genellikle ISP olarak bilinen internet servis sağlayıcıları üzerinden abone olma yoluyla tanımlanır.

11.1.1. Geniş Alan Ağ Teknolojilerinin Sınıflandırılması

Geniş alan ağları, kullanılan cihazların hızı ve bant genişliği ile ağın kurgulandığı coğrafi yapıya göre üçe ayrılır.

- Bağlantı durumuna göre geniş alan ağları
- Anahtarlama yöntemine göre geniş alan ağları
- Topoloji yapısına göre geniş alan ağları

11.1.1.1. Bağlantı Durumuna Göre Geniş Alan Ağları

Bağlantı durumuna göre geniş alan ağlarında noktadan noktaya bağlantı ve bulut bağlantı kullanılmaktadır.

Noktadan noktaya bağlantılar özellikle internet servis sağlayıcılarından (ISP) edinilecek kiralık hatlar ile kullanılmaktadır. Servis sağlayıcılar, iki nokta arasındaki mesafe ve istenen bant genişliğine göre bu hizmeti ücretlendirmektedir. Noktadan noktaya bağlantılara **E1/T1**, **Fractional E1/T1**, **E3/T3**, **Switched 56** gibi teknolojiler örnek olarak verilebilir.

Bulut bağlantı (cloud), iletişim yapılmadan önce bağlantı kurulması esasına dayanan geniş alan ağları teknolojisidir. X25, ISDN, Frame Relay gibi teknolojiler bu bağlantı şekline örnek olarak verilebilir. Bulut teknolojisinde bant genişliği diğer teknolojilere göre çok daha verimli kullanılmaktadır. Bulut teknolojisinin yönetimi, diğer geniş alan ağ teknolojilerine oranla daha az cihaz uğraşı gerektirdiği için nispeten kolaydır.

11.1.1.2. Anahtarlama Yöntemine Göre Geniş Alan Ağları

Anahtarlama yöntemi, iki noktanın [Node (düğüm)] bulut içinde birbiri ile bağlantı kurduğu geniş alan ağları teknolojisidir. Özellikleri bakımından bulut bağlantı yöntemine benzemektedir.

Anahtarlama yöntemine göre bağlantılar üç kategoride sınıflandırılır.

- Devre Anahtarlama (Circuit Switching)
- Paket Anahtarlama (Packet Switching)
- Hücre Anahtarlama (Cell Switching)

Devre Anahtarlama (Circuit Switching): Devre anahtarlama bağlantı yöntemi kullanılan ağlarda öncelikli olarak iki düğüm arasında iletişimin kurulması gerekmektedir. İki nokta arasında bir yol belirlenir ve bağlantı o yol üzerinden gerçekleştirilir. Telefon hat bağlantıları, devre anahtarlama yöntemine bir örnektir. Devre anahtarlama yöntemi kullanılan ağlarda iki düğüm noktası arasında çok sayıda anahtar cihaz kullanılır. Böylelikle birçok alternatif rota oluşur. Gerek bağlantı hızı gerek bant genişliği bakımından hangi yol topoloji daha uygunsa devre anahtarlamalı bağlantılarda o yol üzerinden iletişim kurulur. Devre anahtarlamada en büyük dezavantaj, devre üzerinde iletişim olsun ya da olmasın iletim hattının tamamı aboneye tahsis edilmiş durumdadır, bu da ağ trafiğinin verimsiz olmasına yol açar. Düşük bant genişliği gerektiren sistemlerde, ses iletişimlerinde ve PSTN ağlarında yaygın olarak devre anahtarlama kullanılır.

Paket Anahtarlama (Packet Switching): Haberleşme esnasında veriler karşı tarafa ulaştırılırken küçük parçalara ayrılır, bu küçük parçalara **veri paketi** denir. Paket anahtarlamalı ağlarda veriler gönderilirken bütün olarak veriyi iletmek mümkün değildir. Küçük paketlere ayrılan verilere birtakım bilgiler daha eklenerek karşı tarafa ulaştırılması yöntemi kullanılır. Hata düzeltme, yönlendirme ve iletişim kontrol bitleri gibi bilgiler paketlere eklenir. Verilerin karşı tarafa daha doğru, daha hızlı bir şekilde aktarılması amaçlanır. Paketler karşı tarafa ulaşırken her zaman aynı yolu kullanmaz. Yönlendirme bilgilerine göre veriler farklı yollardan karşı tarafa ulaşabilir. Paket anahtarlama yönteminde tek bir bağlantı sırasında birden fazla paket gönderilebilir. Tahsis edilen anahtarlama devresinde birden fazla abone, aynı devreyi kullanarak iletişim kurabilir. Yerel alan ağlarının birbirleri ile bağlantısında sıklıkla kullanılmaktadır. X25, IP ve IPX protokolleri paket anahtarlama teknolojisine örnektir.

Hücre Anahtarlama (Cell Switching): Hücre anahtarlama yöntemi, devre anahtarlama yöntemine benzemekle birlikte, iletişim için **hücre** ismi verilen değişken uzunluklardaki paketleri kullanır. İletişim için öncelikli olarak bağlantı kurulması gerekir. İki nokta arasında sanal bağlantılar kurulur ve hücreler bu sanal yolları kullanarak karşı tarafa ulaşır. Hücreler yollarını sanal devre üzerindeki numaralandırmalar sayesinde bulur. Bağlantı kurulurken abonelere tahsis edilen bu devre numaraları, bağlantı sonlandırılana kadar kalır. Bağlantı esnasında sadece bu numaralar kullanılır. Paket anahtarlama yönteminde kullanılan alıcı ve gönderici bilgileri, hücre anahtarlama yönteminde kullanılmaz. ATM bağlantıları hücre anahtarlama teknolojisine örnektir. Ses, veri, video iletiminde sıkça kullanılır.

11.1.1.3. Topoloji Yapısına Göre Geniş Alan Ağları

Topoloji yapısına göre geniş alan ağları, hiyerarşik ve örgü topoloji olmak üzere iki kategoriye ayrılır. Kullanıcıların gereksinimlerine göre iki topoloji de kullanılmaktadır.

Hiyerarşik Topoloji: Yapının kök kısmında merkez bulunmaktadır. Yönlendirme yeteneği en iyi olan cihaz, yapının kök kısmında bulunur. Cihazlar, sorumluluk yeteneklerine göre hiyerarşik olarak sıralanır. Hiyerarşik yapılarda yönetim kolaydır.Ağ cihazları yapıda bulunduğu konuma göre verimli bir şekilde kullanılır. Ara veya alt düğümlerde oluşacak trafik yoğunluğu, hiyerarşinin üst kısımlarındaki trafiği etkilemez.

Örgü Topoloji: İnternet, örgü topolojiye en uygun örnektir. Farklı boyutlarda birçok cihaz birbirine farklı yollardan örgüsel olarak bağlıdır. Farklı kapasitede cihazlar, hiyerarşik bir yapı olmadan birbirine bağlanmış durumdadır. Hatlardan bazılarının sıkıntı yaşaması bağlantıyı engellemez. Ağa yeni bir düğüm eklemek kolaydır fakat bir düzen olmadığı için trafikte gecikmeler yaşanabilir.

11.2. Geniş Alan Ağ Cihazları

Geniş alan ağlarında ADSL modemler, yönlendiriciler ve ISP tarafında bulundurulan çeşitli ağ araçları kullanılmaktadır.

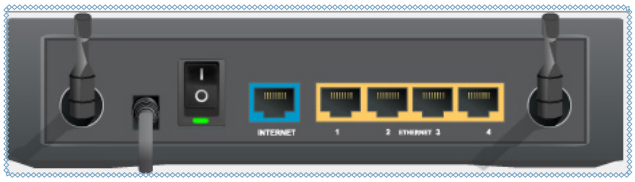
11.2.1. ADSL Modem

ADSL [Asymmetric Digital Subscriber Line (Asimetrik Sayısal Abone Hattı)], xDSL teknolojisinde en çok tercih edilen geniş alan ağları bağlantı yöntemlerindendir. Asimetrik kavramı, veri indirme (download) ve veri yükleme (upload) hızlarının farklı olması anlamına gelir. ADSL teknolojisinin bir avantajı da özel bir hatta ihtiyaç duymadan işlem yapabilmesidir. ADSL teknolojisini kullanabilmek için modeme ihtiyaç duyulmaktadır (Görsel 11.1).

ADSL servisinde, telefon hattının her iki ucunda ADSL modeme ihtiyaç vardır. ADSL modem sıradan modemlerden farklıdır. Eski tip modemler, bilgisayardan dijital sinyalleri alır ve analog sinyallere çevirerek telefon hattından gönderir. Alıcı modem, bu analog sinyalleri yeniden dijital bilgiye çevirir. ADSL modemler ise bunu yapmak yerine verileri dijital formda alır ve gönderir. Analog sinyallere çevirme işi hiçbir zaman yapılmaz.

ADSL, telefon hattını üç kanala ayırır. Bu üç kanal; veri almak, veri göndermek, telefon görüşmesi yapmak için kullanılır. Bu durum, internete bağlıyken aynı zamanda telefonla görüşebilmeyi sağlamaktadır. Telefon hattı fiziksel olarak her zaman üçe ayrılamaz. Bunun yerine modülasyon teknikleri kullanılarak üç ayrı tipte sinyal ayırt edebilir. Bu sinyaller; ses, gönderme ve almadır. Gönderme ve alma kanalları çeşitli hızlarda ayrılabilir.

Teknolojinin gelişmesiyle beraber ADSL modemlere ek olarak **Fiber modemler** ve **VDSL modemler** kullanılmaya başlanmıştır.



Görsel 11.1: Standart ADSL modem

11.2.2. Yönlendiriciler

Yönlendiricilerin temel görevi, veri paketlerini yerel alan ağlarından geniş alan ağlarına ulaştırmaktır. OSI modelinin üçüncü katmanında görev yapan yönlendiriciler, üzerinde bulunan işletim sistemleri ve programlanabilir yapısıyla verilerin en kısa sürede diğer ağlara ulaşacağı yolların tespitini yapar.

Yönlendiriciler, üzerinde bulunan arayüzler ve haricî olarak takılabilen modülleri sayesinde ikinci katman ağlarda çalışan cihazlara takılabilir. Böylelikle farklı ağlarda bulunan cihazların verilerinin yönlendirmesi yapılabilir.

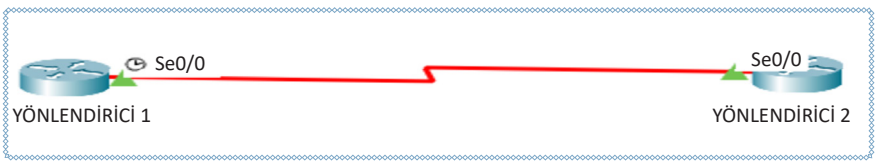
Yönlendiriciler, ileteceği verilerin rotalarını bulmak için çeşitli matematiksel işlemler yapabilmektedir. Yönlendiriciler; OSPF (Open Shortest Path First), IGRP (Interior Gateway Routing Protocol), BGP (Border Gateway Protocol) , IS-IS (Intermediate System - Intermediate System), RIP (Routing Information Protocol) gibi protokoller kullanarak dinamik bir şekilde veri paketlerinin iletimlerini sağlayabildiği gibi statik olarak da programlanarak verileri yönlendirebilmektedir.

11.2.2.1. Yönlendirici Cihaz Bağlantı Türleri

Yönlendirici cihazı kullanarak fiziksel bağlantılar yapmak istendiğinde yönlendirici üzerinde bulunan çeşitli arayüzler kullanabilmektedir. Yönlendirici cihazın üzerinde bulunan “Seri Arayüz” ve “Ethernet Arayüz” kullanılarak diğer cihazlar ile bağlantı kurulabilmektedir (Görsel 11.2).

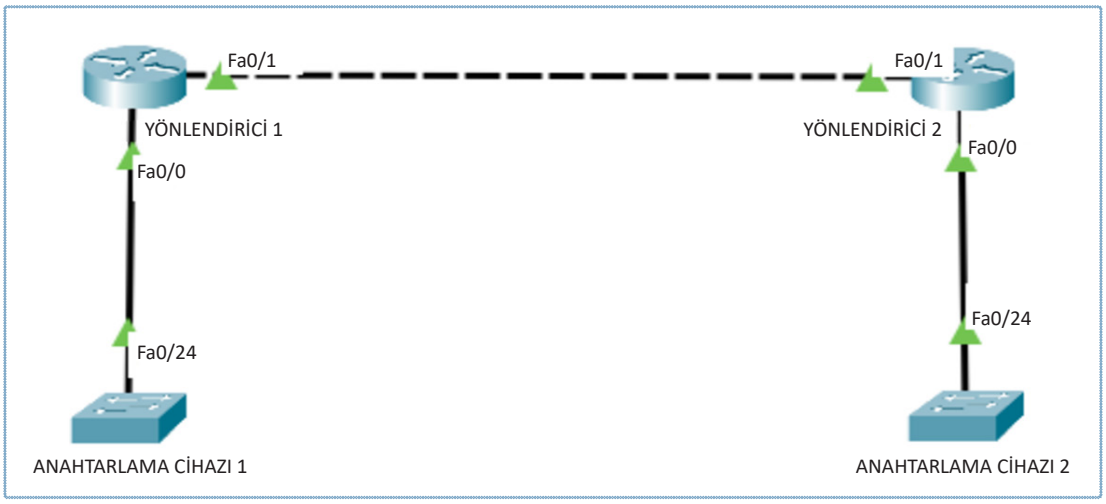
Görsel 11.2: Yönlendirici cihaz bağlantı portları

Seri arayüz bağlantısını kurabilmek için **seri kablo** kullanmak gerekmektedir. Seri kablo, yönlendirici cihazın başka bir yönlendirici cihaz ile bağlantısında kullanılan kablodur. Seri bağlantılar, uzak mesafelerde bulunan yönlendirici cihazların bağlantısında tercih edilmektedir (Görsel 11.3).



Görsel 11.3: İki yönlendirici cihazın seri kablo ile bağlantısı

Ethernet arayüz bağlantısı kullanılarak yönlendirici cihaz, farklı ağ cihazlarına bağlanabilir. Ethernet arayüzünü kullanırken bağlanacak cihaz, başka bir yönlendirici ise **çapraz kablo** seçilmelidir. Anahtar cihazı gibi farklı bir ağ cihazı ise **düz kablo** seçilmelidir (Görsel 11.4, Görsel 11.5).



Görsel 11.4: Fast Ethernet arayüzünde çapraz kablo kullanımı

Görsel 11.5: Fast Ethernet arayüzünde düz kablo kullanımı

Sıra Sizde

Ağ simülasyon yazılımı kullanarak dört adet yönlendirici cihazın bağlantısını seri arayüzler kullanarak hazırlayınız.

11.2.3. ADSL Modem Kurulumu ve Yapılandırılması

Günümüzde ağ cihazı üreten birçok firma bulunmaktadır. Firmalar ürettikleri cihazlara kendi arayüzlerini yüklemektedir. Dolayısıyla farklı ADSL modemlerde ayarlama yapılacak yerler değişse de kurulum ve yapılandırma mantıkları aynıdır.

Birçok modem, içinde barındırdığı kurulum sihirbazları ile rahat bir yapılandırma fırsatı sunarken web tarayıcıları üzerinden de kurulum ve yapılandırma işlemleri yapılabilmektedir.

Uygulama 1

http://kitap.eba.gov.tr/KodSor.php?KOD=21069

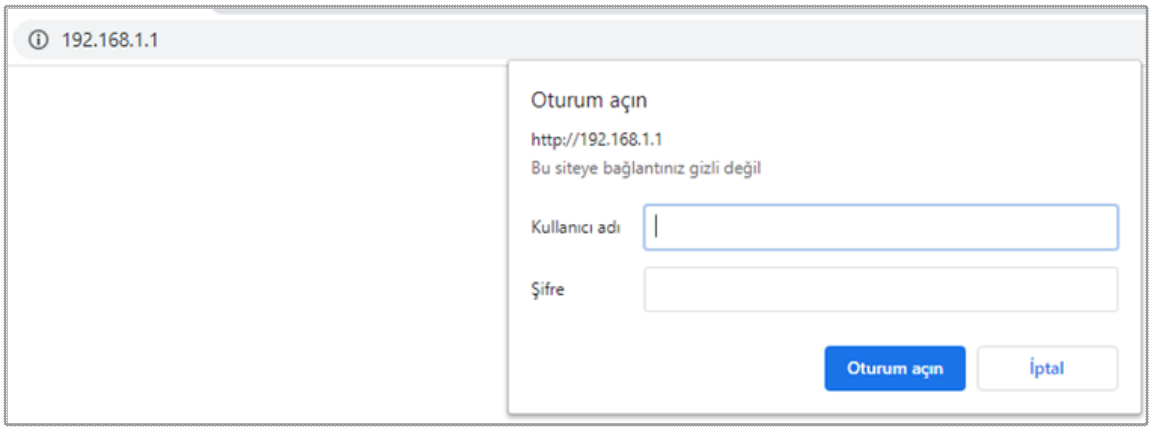
ADSL modeminize web tarayıcısı üzerinden bağlanarak kurulum ayarlarını yapma işlemini yönergeler doğrultusunda gerçekleştiriniz.

Adım 1: ADSL modem üzerinde bulunan Ethernet portlarına ağ kablonuzun bir ucunu takıp diğer ucunu bilgisayarınızın ağ kartına takınız.

Adım 2: Kablo bağlantılarını yaptıktan sonra bilgisayarınızda bulunan herhangi bir web tarayıcısının adres satırına 192.168.1.1 yazınız (Görsel 11.6).

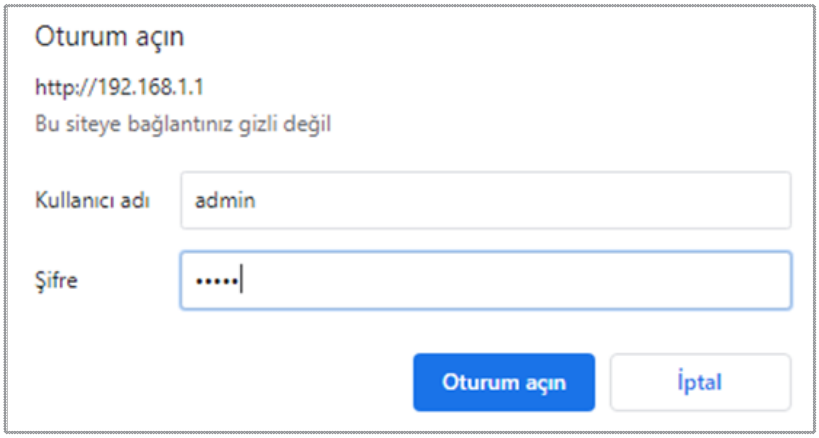
Dikkat

Modem üreticilerinin varsayılan olarak cihaza erişim IP adresleri değişkenlik gösterebilmektedir. Modem arayüz IP adresi 192.168.1.1 olabildiği gibi 192.168.2.1 veya 10.0.0.1 de olabilir. Bu adres bilgisi için üretici firmanın modem kullanım kılavuzunun kontrol edilmesi gerekmektedir.



Görsel 11.6: Web tarayıcısı kullanarak modem arayüzüne giriş yapma

Adım 3: Modem üretici firması tarafından varsayılan olarak belirlenmiş kullanıcı adı ve şifresini girerek arayüz yazılımına ulaşınız (Görsel 11.7).



Görsel 11.7: Kullanıcı adı ve şifre ile arayüze giriş yapma

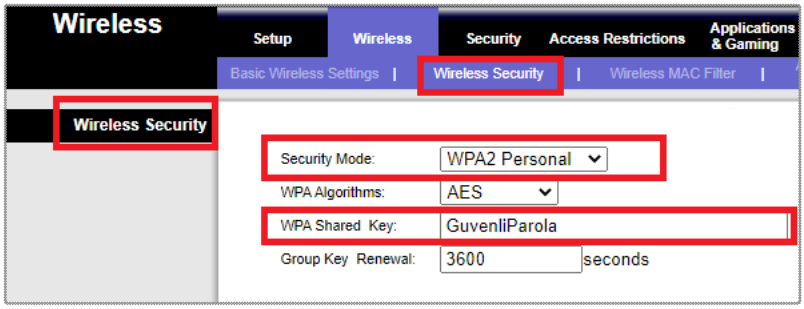
Adım 4: Modem arayüzüne girdikten sonra kurulum sihirbazı varsa yönergeleri izleyerek ISP firmanız tarafından size verilen kullanıcı adı ve şifresini "username" ve "password" alanlarına giriniz.

Sihirbazı yoksa ya da sihirbazı kullanmadan kurulum yapmak için genellikle modem WAN ayarlarında bulunan "PPoA bağlantı ayarları" seçeneğini bulup ilgili kullanıcı adı ve şifre alanına veri girişini yaptıktan sonra VPI alanına 8, VCI alanına 35 değerlerini girerek yapılandırmanızı kaydederek kurulumu tamamlayınız.

Adım 5: ADSL modem kurulumunu yaptıktan sonra temel yapılandırma işlemlerini gerçekleştirmelisiniz. Kablosuz ağ bağlantı ismini değiştirmek için modem ayarlarında **Wireless** ya da **kablosuz ağlar** yazan kısımdan giriş yapınız. Kablosuz modeminizin yayın yaptığı isme SSID adı verilir. Cihaz ayarlarında **SSID** kısmını bularak yayın adınızı **BILISIMTEK** yapınız (Görsel 11.8).

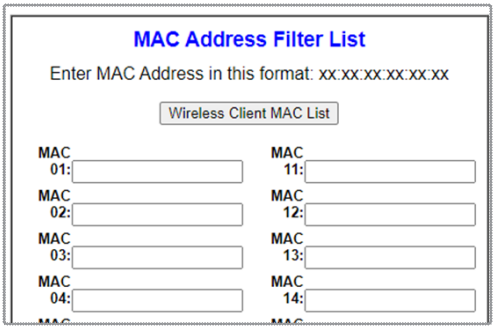
Görsel 11.8: SSID yapılandırması

Adım 6: Kablosuz modem güvenlik ayarları (Wireless Security) seçeneğine giriniz. Uygun şifreleme tekniğini (Security Mode) seçerek ağınıza bağlanacak cihazlar için güvenli bir kablosuz ağ girişi şifresi belirleyiniz (Görsel 11.9).



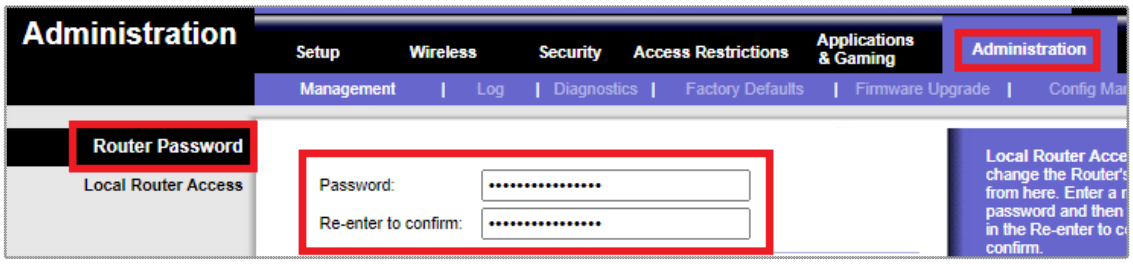
Görsel 11.9: Kablosuz şifre ayarları yapılandırma

Adım 7: Kablosuz ağınızın daha güvenli olmasını istiyorsanız "Wireless MAC Filter" alanından ağa bağlanmasını istediğiniz cihazların MAC adreslerini giriniz. Böylelikle istenmeyen cihazların kablosuz ağınıza bağlanmasını engellemiş olacaksınız (Görsel 11.10).



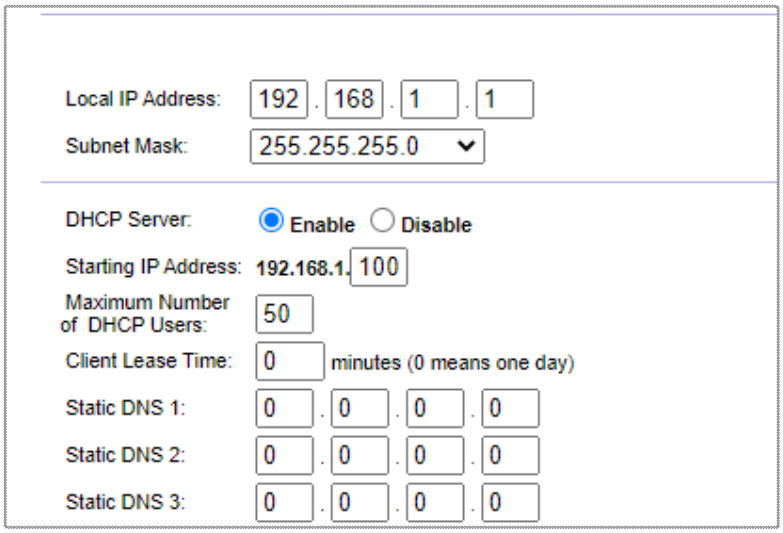
Görsel 11.10: MAC adres filtreleme

Adım 8: Cihazınıza web tarayıcısı üzerinden ulaşmak istediğinizde sizden istenen ve varsayılan olarak belirlenmiş kullanıcı adı ve parolayı yönetim paneli alanından değiştiriniz (Görsel 11.11).



Görsel 11.11: Varsayılan modem giriş şifre ve kullanıcı adını değiştirme

Adım 9: DHCP ve DNS ile ilgili ayarları temel yapılandırma kısmından yapınız (Görsel 11.12).



Görsel 11.12: DHCP ve DNS ayarlarını yapılandırma

Sıra Sizde

Mevcut kablosuz ağınızın ayarlarına girerek SSID ismini ANAHTARLAMA olarak yapılandırınız. Modem ayarlarından sadece tek bir cihazın kablosuz ağa bağlanmasını sağlayınız.

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

1. ( ) ADSL modemlerin kablosuz ağ görünürlük isimlerine SSID adı verilir.
2. ( ) İki adet yönlendirici birbiri ile sadece seri arayüz aracılığı ile bağlanmaktadır.
3. ( ) Devre anahtarlama bağlantı yöntemi kullanan ağlarda öncelikli olarak iki düğüm arasında iletişimin kurulması gerekmektedir.

B. Aşağıdaki soruları dikkatlice okuyunuz ve doğru seçeneği işaretleyiniz.

4. Aşağıdakilerden hangisi geniş alan ağı teknolojilerinden değildir?

A) Frame Relay
B) ATM
C) X25
D) T1
E) ADSL

5. Aşağıdakilerden hangisi ADSL modemlerde istenmeyen cihazların ağa giriş yapmasını engellemek için kullanılan yöntemlerden biridir?

A) IP engelleme
B) MAC filtreleme
C) Şifre değiştirme
D) SSID değiştirme
E) DNS değiştirme

6. Farklı lokal ağların ve uzaktaki ağların birbirine bağlanması için kullanılan ağ cihazının adı aşağıdakilerden hangisidir?

A) Yönlendirici
B) Anahtarlama cihazı
C) Dağıtıcı
D) Güvenlik duvarı
E) Erişim noktası

KAYNAKÇA

COMER E. Douglas, **Bilgisayar Ağları ve İnternet**, Nobel Akademik Yayıncılık, Ankara, 2016.

ÇÖLKESEN Rıfat, Bülent ÖRENCİK, **Bilgisayar Haberleşmesi ve Ağ Teknolojileri**, Papatya Yayıncılık, İstanbul, 2012.

DİRİCAN Can Okan, **TCP/IP ve Ağ Güvenliği**, Açık Akademi Yayınları, İstanbul, 2005.

ODOM Wendell, **Cisco CCNA #640-607 Sınavı Sertifikasyon Rehberi**, Sistem Yayıncılık, 2004.

RFC 3513; Deering, S., Hinden, R., Internet Protocol Version 6 (IPv6) Addressing Architecture, 2003.

Şahin, M., IPv6 Sistem Geçişi, Yüksek Lisans Tezi, İstanbul Teknik Üniversitesi, İstanbul, 2006.

TANER Cemal, **Ağ Yöneticiliğinin Temelleri**, Abaküs Yayınları, İstanbul, 2017.

GENEL AĞ KAYNAKÇASI

http://yunus.hacettepe.edu.tr/~b0045188/veri_iletisim_modelleri/html_dosyalar/tcp-ip.htm (Erişim Tarihi: 05.11.2020).

http://web.deu.edu.tr/doc/lis/lis-8.html (Erişim tarihi: 08.11.2020).

http://web.firat.edu.tr/mbaykara/tcpipveinternet.pdf (Erişim Tarihi: 08.11.2020).

http://www.cisn.odtu.edu.tr/ozel/tufan.php (Erişim Tarihi: 12.11.2020).

https://acikders.ankara.edu.tr/mod/resource/view.php?id=105811 (Erişim zamanı 13.11.2020 saat 16:00).

https://acikders.ankara.edu.tr/pluginfile.php/155286/mod_resource/content/0/10.3.%20IP%20Protokulu.pdf (Erişim Tarihi: 08.11.2020).

https://bidb.itu.edu.tr/seyir-defteri/blog/2013/09/07/alt-aglara-bolme-subnetting (Erişim tarihi: 13.11.2020 saat 16:20).

https://bidb.itu.edu.tr/seyir-defteri/blog/2013/09/06/arp-(adres-%C3%A7%C3%B6z%C3%BCmleme-protokol%C3%BC) (Erişim tarihi: 13.11.2020).

https://bidb.itu.edu.tr/seyir-defteri/blog/2013/09/07/ipv4-(internet-protocol-version-4---internet-protokol%C3%BC-s%C3%BCr%C3%BCm-4) (Erişim tarihi: 08.11.2020).

https://bidb.itu.edu.tr/seyir-defteri/blog/2013/09/07/ospf-(open-shortest-path-first---ilk-a%C3%A7%C4%B1k-y%C3%B6ne-%C3%B6ncelik)-protokol%C3%BC#:~:text=OSPF%20protokol%C3%BC%20uzakl%C4%B1k%20vekt%C3%B6r%C3%BC%20protokolleri,ters%20orant%C4%B1l%C4%B1%20olan%20de%C4%9Ferler%20kullan%C4%B1r. (Erişim tarihi: 12.11.2020).

https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/ (Erişim tarihi: 14.11.2020).

https://docs.microsoft.com/tr-tr/dotnet/framework/network-programming/ipv6-addressing (Erişim tarihi: 15.11.2020).

https://ipv6.metu.edu.tr/tr/node/1 (Erişim tarihi: 05.11.2020).

https://sozluk.gov.tr/

https://ulakbim.tubitak.gov.tr/sites/images/Ulakbim/ipv6_el_kitabi.pdf (Erişim tarihi: 05.11.2020).

https://www.iso.org/standards.html (Erişim tarihi: 12.11.2020).

https://www.tdk.gov.tr/

https://www.tiafotc.org/ansi-tia-568-d/ (Erişim tarihi: 10.11.2020).

GÖRSEL KAYNAKÇA

GÖRSEL NO	ERİŞİM ADRESİ	ID	ERİŞİM TARİHİ
Kitap Kapak Resmi	https://www.shutterstock.com/	753201955	
	https://www.shutterstock.com/	283947308	
	https://tr.123rf.com/	36609883	
Kitap İkonları	https://www.shutterstock.com/	1463676065	
ÖĞRENME BİRİMİ 1			
Öğrenme Birimi Kapak Resmi	https://www.shutterstock.com/	1707871144	
Görsel 1.7	https://www.shutterstock.com/	1607329045	
Görsel 1.12	https://www.shutterstock.com/	705041551	
Görsel 1.13	https://www.shutterstock.com/	271649435	
Görsel 1.4	https://www.shutterstock.com/	1134830735	
ÖĞRENME BİRİMİ 2			
Öğrenme Birimi Kapak Resmi	https://www.shutterstock.com/	670623523	
Görsel 2.3	https://www.shutterstock.com/	1362035846	
Görsel 2.5	https://www.shutterstock.com/	1320531266	
Görsel 2.6	https://www.shutterstock.com/	1337502335	
Görsel 2.16	Komisyon üyesi tarafından hazırlanmıştır.		
ÖĞRENME BİRİMİ 3			
Öğrenme Birimi Kapak Resmi	https://www.shutterstock.com/	1075244474	
ÖĞRENME BİRİMİ 4			
Öğrenme Birimi Kapak Resmi	https://www.shutterstock.com/	1729259665	
Görsel 4.1	Komisyon üyesi tarafından hazırlanmıştır.		
Görsel 4.5	Komisyon üyesi tarafından hazırlanmıştır.		
ÖĞRENME BİRİMİ 5			
Öğrenme Birimi Kapak Resmi	https://www.shutterstock.com/	252050350	
ÖĞRENME BİRİMİ 6			
Öğrenme Birimi Kapak Resmi	https://www.shutterstock.com/	311303981	
Görsel 6.1	https://www.shutterstock.com/	231329083 ve 653477872	
Görsel 6.2	https://www.shutterstock.com/	1362035846	
Görsel 6.3	https://www.shutterstock.com/	88620712, 370639280 ve 1666298785	
Görsel 6.11	Komisyon üyesi tarafından çekilmiştir.		
Görsel 6.13	https://www.cisco.com/		20.01.2021
Görsel 6.14	https://www.shutterstock.com/	71153056	
ÖĞRENME BİRİMİ 7			
Öğrenme Birimi Kapak Resmi	https://www.shutterstock.com/	340166957	
ÖĞRENME BİRİMİ 8			
Öğrenme Birimi Kapak Resmi	https://www.shutterstock.com/	1062915260	
Görsel 8.32	Komisyon üyesi tarafından hazırlanmıştır.		
ÖĞRENME BİRİMİ 9			
Öğrenme Birimi Kapak Resmi	https://www.shutterstock.com/	397990186	
ÖĞRENME BİRİMİ 10			
Öğrenme Birimi Kapak Resmi	https://www.shutterstock.com/	1695042067	
ÖĞRENME BİRİMİ 11			
Öğrenme Birimi Kapak Resmi	https://www.shutterstock.com/	744596659	

KAREKOD KAYNAKÇASI

ÖĞRENME BİRİMİ	UYGULAMA NO	KAREKOD LİNKİ
1	1	http://kitap.eba.gov.tr/KodSor.php?KOD=21027
	4	http://kitap.eba.gov.tr/KodSor.php?KOD=21028
2	1	http://kitap.eba.gov.tr/KodSor.php?KOD=21029
	2	http://kitap.eba.gov.tr/KodSor.php?KOD=21030
3	2	http://kitap.eba.gov.tr/KodSor.php?KOD=21031
	3	http://kitap.eba.gov.tr/KodSor.php?KOD=21032
4	5	http://kitap.eba.gov.tr/KodSor.php?KOD=21033
	6	http://kitap.eba.gov.tr/KodSor.php?KOD=21034
5	4	http://kitap.eba.gov.tr/KodSor.php?KOD=21035
	6	http://kitap.eba.gov.tr/KodSor.php?KOD=21036
	8	http://kitap.eba.gov.tr/KodSor.php?KOD=21037
	9	http://kitap.eba.gov.tr/KodSor.php?KOD=21038
	11	http://kitap.eba.gov.tr/KodSor.php?KOD=21039
	12	http://kitap.eba.gov.tr/KodSor.php?KOD=21040
6	sayfa 128	http://kitap.eba.gov.tr/KodSor.php?KOD=21041
	11	http://kitap.eba.gov.tr/KodSor.php?KOD=21042
	12	http://kitap.eba.gov.tr/KodSor.php?KOD=21043
	13	http://kitap.eba.gov.tr/KodSor.php?KOD=21044
	18	http://kitap.eba.gov.tr/KodSor.php?KOD=21045
	19	http://kitap.eba.gov.tr/KodSor.php?KOD=21046
	20	http://kitap.eba.gov.tr/KodSor.php?KOD=21047
	22	http://kitap.eba.gov.tr/KodSor.php?KOD=21048
7	4	http://kitap.eba.gov.tr/KodSor.php?KOD=21049
	5	http://kitap.eba.gov.tr/KodSor.php?KOD=21050
	6	http://kitap.eba.gov.tr/KodSor.php?KOD=21051
	8	http://kitap.eba.gov.tr/KodSor.php?KOD=21052
	9	http://kitap.eba.gov.tr/KodSor.php?KOD=21053
	11	http://kitap.eba.gov.tr/KodSor.php?KOD=21054
	12	http://kitap.eba.gov.tr/KodSor.php?KOD=21056
8	3	http://kitap.eba.gov.tr/KodSor.php?KOD=21057
	7	http://kitap.eba.gov.tr/KodSor.php?KOD=21058
	12	http://kitap.eba.gov.tr/KodSor.php?KOD=21059
9	1	http://kitap.eba.gov.tr/KodSor.php?KOD=21060
	2	http://kitap.eba.gov.tr/KodSor.php?KOD=21061
	3	http://kitap.eba.gov.tr/KodSor.php?KOD=21062
	4	http://kitap.eba.gov.tr/KodSor.php?KOD=21063
10	2	http://kitap.eba.gov.tr/KodSor.php?KOD=21064
	3	http://kitap.eba.gov.tr/KodSor.php?KOD=21065
	4	http://kitap.eba.gov.tr/KodSor.php?KOD=21066
	7	http://kitap.eba.gov.tr/KodSor.php?KOD=21067
	8	http://kitap.eba.gov.tr/KodSor.php?KOD=21068
11	1	http://kitap.eba.gov.tr/KodSor.php?KOD=21069

CEVAP ANAHTARI

ÖĞRENME BİRİMİ 1'İN CEVAP ANAHTARI

1	2	3	4	5	6			
E	B	C	B	D	B	D	A	C

ÖĞRENME BİRİMİ 2'NİN CEVAP ANAHTARI

1	2	3	4	5	6	7	8
D	D	D	Y	A	A	D	B

ÖĞRENME BİRİMİ 3'ÜN CEVAP ANAHTARI

1	2	3	4	5	6	7
Y	D	Y	D	C	E	D

ÖĞRENME BİRİMİ 4'ÜN CEVAP ANAHTARI

1	2	3	4	5	6	7	8	9	10	11
D	D	Y	Y	Y	C	B	C	E	C	C
12	13	14	15							
D	E	C	D							

ÖĞRENME BİRİMİ 5'İN CEVAP ANAHTARI

1	2	3	4	5	6	7	8
D	A	A	B	C	E	C	D

ÖĞRENME BİRİMİ 6'NIN CEVAP ANAHTARI

1	2	3	4	5	6	7	8	9	10
C	C	E	A	E	E	B	B	B	E

ÖĞRENME BİRİMİ 7'NİN CEVAP ANAHTARI

1	2	3	4	5	6	7	8	9	10
D	D	A	B	E	E	A	E	A	A

ÖĞRENME BİRİMİ 8'İN CEVAP ANAHTARI

1	2	3	4	5	6	7	8	9	10
A	E	C	A	B	D	A	E	B	D

ÖĞRENME BİRİMİ 9'UN CEVAP ANAHTARI

1	2	3	4	5	6	7	8	9	10	11
D	Y	D	D	D	Y	Y	A	B	E	A

ÖĞRENME BİRİMİ 10'UN CEVAP ANAHTARI

1	2	3	4	5	6	7	8	9
D	D	Y	D	C	A	E	E	A

ÖĞRENME BİRİMİ 11'İN CEVAP ANAHTARI

1	2	3	4	5	6
D	Y	D	E	B	A