T.C.
MİLLÎ EĞİTİM BAKANLIĞI

ELEKTRİK-ELEKTRONİK TEKNOLOJİSİ

AĞ GÜVENLİĞİ VE AĞ PROTOKOLLERİ
481BB0007

Ankara, 2011

- Bu modül, mesleki ve teknik eğitim okul/kurumlarında uygulanan Çerçeve Öğretim Programlarında yer alan yeterlikleri kazandırmaya yönelik olarak öğrencilere rehberlik etmek amacıyla hazırlanmış bireysel öğrenme materyalidir.
- Millî Eğitim Bakanlığınca ücretsiz olarak verilmiştir.
- PARA İLE SATILMAZ.

İÇİNDEKİLER

AÇIKLAMALAR

KOD	**481BB0007**
ALAN	**Elektrik Elektronik Teknolojisi**
DAL/MESLEK	**Dal Ortak**
MODÜLÜN ADI	**Ağ Güvenliği ve Ağ Protokolleri**
MODÜLÜN TANIMI	Ağ sistemlerinde protokollerin ve ağ güvenliğinin tanımını, denetimini, ayarlarını yapabilme ilgili temel bilgi ve becerilerin kazandırıldığı bir öğrenme materyalidir.
SÜRE	40/16
ÖN KOŞUL	Ağ İşletim Sistemleri modülünü almış olmak
YETERLİK	Ağ protokollerini kurmak
MODÜLÜN AMACI	**Genel Amaç** Ağ protokolü ve ağ güvenliğine ait tanımlamaları ve düzenlemeleri yapabileceksiniz. **Amaçlar** **1.** Ağ protokollerini tanıyarak protokol tanımlamalarını yapabileceksiniz. **2.** İnternet adres sınıflarını tanıyarak alt ağlara ayırma (subnet mask) ayarlarını yapabileceksiniz. **3.** Ağ yönlendirme elemanlarını tanıyarak IP yönlendirme işlemini yapabileceksiniz. **4.** Güvenlik düzeylerini tanıyarak ağ güvenliği ile ilgili tanımlamaları yapabileceksiniz.
EĞİTİM ÖĞRETİM ORTAMLARI VE DONANIMLARI	**Ortam:** Bilgisayar laboratuvarı **Donanım:**Ağ sistemi, ağ işletim sistemi, bilgisayar
ÖLÇME VE DEĞERLENDİRME	Modül içinde yer alan her öğrenme faaliyetinden sonra verilen ölçme araçları ile kendinizi değerlendireceksiniz. Öğretmen modül sonunda ölçme aracı (çoktan seçmeli test, doğru-yanlış testi, boşluk doldurma, eşleştirme vb.) kullanarak modül uygulamaları ile kazandığınız bilgi ve becerileri ölçerek sizi değerlendirecektir.

GIRIŞ

Sevgili Öğrenci,

İletişim hayatımızın ayrılmaz bir parçasıdır. İnsanlar çeşitli bilgileri, duyguları iletişim yoluyla birbirlerine aktarırlar. Bu sayede aralarında bir bağ oluşur. Bilgisayarlarda da insanlarınkine benzeyen bir iletişim zinciri vardır. Her bilgisayar sahibi kendinde bulunmayan bilgilere başka makinelere bağlanarak ulaşır. Yine aynı yöntemle kendi bilgilerini de başka kullanıcılara ulaştırır. Tüm bu işlemler ağ protokolleri sayesinde gerçekleşir.

İletişimin belli kuralları vardır. Bunlardan birisi de gizliliktir. Nasıl gerçek dünyada insanlarla ilişkilerimizde gizli olan noktalar varsa sanal âlemde de gizliliğin önemli olduğu yerler vardır. Bu gizlilik de ağ güvenliği sayesinde sağlanır.

Günümüzde bilgisayar ve internet teknolojisindeki gelişmelerle birlikte ağ teknolojilerinde de gelişmeler olmuştur. Bilgisayar ağları okullarda, iş yerlerinde, bankalarda ve daha pek çok alanda veri aktarımı ve paylaşımını sağlamasının yanında bazı bilgilerin de istenmeyen kişilerin eline geçmesini önlemek amacıyla kullanılmaktadır.

Bu modülü bitirdikten sonra bilgisayarlar arasındaki veri iletişiminin hangi kurallar içinde gerçekleştiğini, ağ protokol ayarlarının nasıl yapıldığını, veri paylaşımında gizliliğin nasıl sağlandığını kavrayacak ve bu sistemleri verimli bir şekilde kullanabileceksiniz. Bu sayede bilgiye ulaşıp saklamanız son derece kolay olacaktır.

ÖĞRENME FAALİYETİ-1

AMAÇ

Mevcut olan bir ağ sisteminde ağ protokollerini tanımlayarak kontrol edebilecek ve bunları ayarlayarak protokol sunucularını kurabileceksiniz.

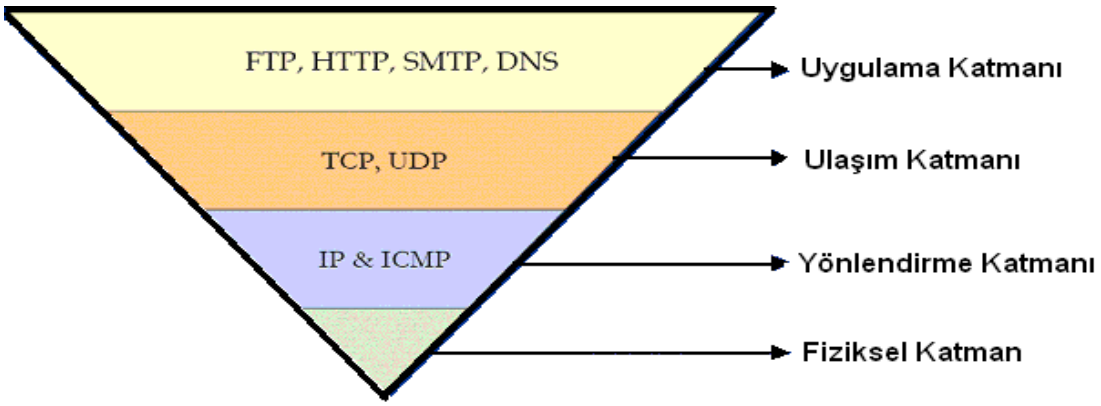
ARAŞTIRMA

- Ağ bağlantısında kullanılan donanım elemanlarını araştırınız.
- Bir internet laboratuvarının kablo bağlantılarını ve ağ protokol ayarlarını araştırınız.
- Bir yerel ağda bilgi alışverişinde bulunan bilgisayarların nasıl bilgi alışverişinde bulunduğunu ve hangi ayarların yapıldığını araştırınız.
- Araştırmalarınız için internet ortamını kullanınız. Okulunuzun bilgisayar laboratuvarını gezerek kullanılan ağ donanımları ve ağ ayarları hakkında ön bilgi edininiz.

1. AĞ PROTOKOLLERİ

1.1. TCP/IP Mimarisi ve Katmanları

İnternet ağ mimarisi katmanlı yapıdadır. Uygulama katmanı sayılmazsa temel dört katman vardır. Bilgisayarlar arası iletişim için gerekli bütün iş, bu dört katman tarafından yürütülür. Her katmanda yapılacak görevler protokoller tarafından paylaşılmıştır. TCP ve IP farklı katmanlarda bulunan farklı protokollerdir. Fakat ikisi birlikte TCP/IP olarak kullanıldığında bütün katmanları ve bu katmanlarda bulunan protokollerin tamamını ifade eder. Bu sebeple TCP/IP bir protokol kümesi olarak bilinir.



Şekil 1.1: TCP/IP katmanı

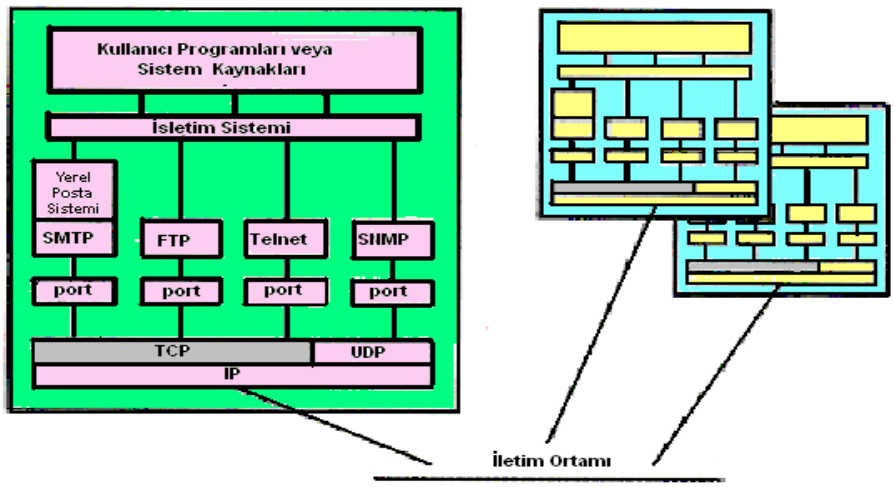
TCP/IP katmanında kullanıcının kullandığı programlar ve işletim sisteminin arka planda yürüttüğü programlar uygulama programı katmanlarıdır. Uygulama programının altında bulunan katmanlar iletişim işini yapan katmanlardan oluşur. Bu katmanlarda bir hizmetin yapılabilmesi için bir alt katmandan hizmet beklenir.

Uygulama programlarının bulunduğu katman sayılmaz ise dört katman vardır. Bunlar; uygulama, ulaşım, yönlendirme ve fiziksel katmanlardır (Şekil 1.1). Uygulama katmanında SMTP (Simple Mail Transfer Protocol-Basit Posta Aktarım Protokolü), TELNET (Telecommunication Network-İletişim Ağı), FTP (File Transfer Protocol-Dosya Aktarım Protokolü), SNMP (The Simple Network Management-Basit Ağ Yönetim Protokolü), (Remote Login-Uzaktan Erişim) gibi protokolleri vardır. Ulaşım katmanında TCP (Transmission Control Protocol-İletişim Kontrol Protokolü) ve UDP (User Datagram Protocol-Kullanıcı Veri Bloğu İletişim Protokolü) protokolleri, yönlendirme katmanında IP (Internet Protocol-İnternet Protokolü), ICMP (Internet Control Management Protocol-İnternet Kontrol Yönetim Protokolü) protokolleri vardır. Fiziksel katmanda ise gelen bilgileri iletim ortamına aktarmakla görevli protokoller olan Ethernet, Switch, X25 gibi protokoller vardır.

Uygulama programları, uygulama katmanındaki protokoller aracılığı ile iletişimdedir. Bir e-posta (e-mail, e-mektup) SMTP ile belirlenen kurallarla gideceği adrese gönderilir. Bu protokol bir e-mail'in gönderilecek adrese nasıl gönderileceğini belirler. Ağ üzerindeki başka bir bilgisayara dosya aktarımı ve bağlanma için de FTP protokolü kullanılır. FTP, bilgisayarlar arasında dosya alışverişi için kullanılan bir uygulama katmanı protokolüdür.

Ağ cihazları, genel olarak TCP/IP'nin ilk üç katmanıyla işlem yapar. Eğer ağ cihazı yapılan uygulamada protokollerini kendi bünyesinde de çalıştıracaksa dördücü katmanı da kullanır.

Şekil 1.1'deki katman ve protokolleri, Şekil 1.2'de değişik bir açıdan inceleyelim.



Şekil 1.2: TCP/IP protokolleri arasındaki ilişki

Şekil 1.2'de görüldüğü gibi işletim siteminin hemen altında uygulama protokolleri vardır. Bu protokoller bir port üzerinden TCP ve UDP'nin bulunduğu katmana erişir.

TCP protokülünde her uçta 2^{16} adet farklı port tanımlıdır. Bu 16 bitlik port numarası veya adresi ve 32 bitlik IP adresi beraberce kullanıldığında ortaya çıkan adrese soket numarası denir. TCP bağlantılar, bu soketler üzerinden sağlanır. Bir soket, Şekil 1.3'te görüldüğü gibi iki parçadan oluşur.

Soket Numarası

Port Nu.	IP Adresi

Şekil 1.3: TCP bağlantı soketleri

Bir IP adresindeki birbirinden farklı servisleri kullanmak için verilmiş numaralara port numarası denir. Port numaraları 0 ile 255 arasında numarandırılmış, standart uygulama katmanı hizmetlerine erişim için ayrılmıştır. Örneğin; FTP için port 21, TELNET için port 23 gibi birçok port numarası belirli uygulamalar için kullanılır.

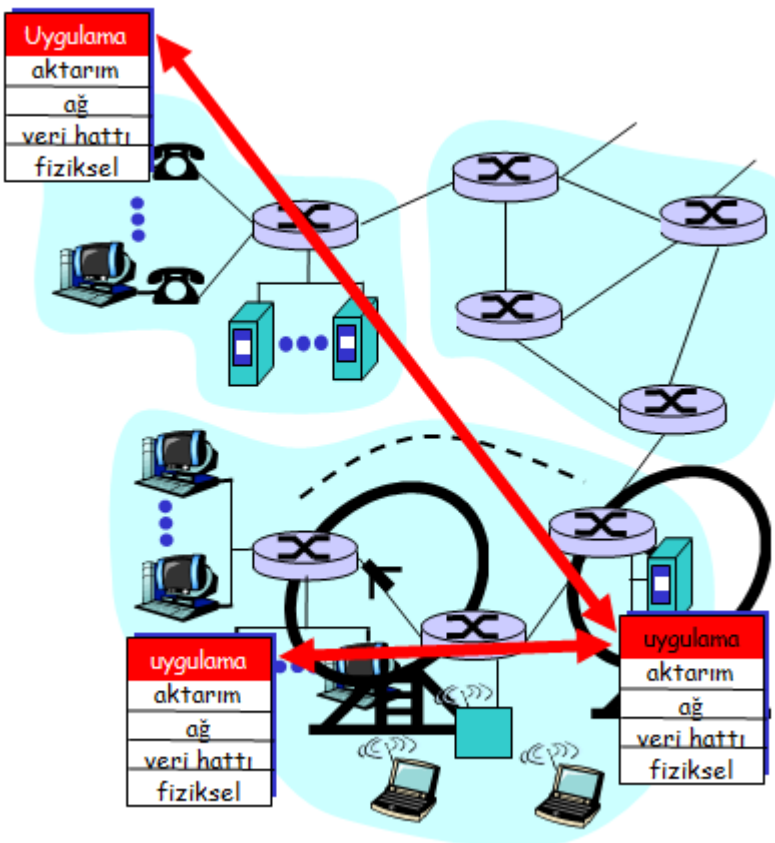
Katmanların sahip olduğu görevlerin anlaşılması için en temel hizmet olan e-posta örneği üzerinde durulabilir. E-posta, yazma ortamı sunan bir yardımcı program aracılığıyla yazılır daha sonra uygulama katmanında SMTP protokolüne gönderilir. Burada alıcı ve gönderici adresleri yazıldıktan sonra hazırlanan mektup bir alt katmana yani ulaşım katmanına gönderilir. Bu katmanda kullanılan protokol TCP'dir. Burada TCP protokolünün görevi, bir üst katmandan gelen veri paketini gönderebilecek şekilde parçalara ayırarak onlara sıra numarası vermektir. Daha sonra bir alt katman olan yönlendirme katmanında IP protokolüne gönderir. IP protokolü gelen veri paketlerinin önüne gidecek olan yerin adres

bilgilerini yerleştirir. Adres bilgilerini de alan veri paketleri, bir alt katman olan fiziksel katman aracılığı ile karşı bilgisayarlara iletilir.

Özellikle TCP ve IP protokolleri, bilgi alışverişlerinde çok büyük bir görev üstlenmektedir. TCP protokolü bir üst katmandan gelen verilerin önüne kendi başlığını ekleyerek bir alt katmandaki IP protokolüne gönderir. Bu protokol, gelen veriye adres bilgileri yerleştirerek fiziksel katmana gönderir.

1.1.1. Uygulama Katmanı Protokolleri

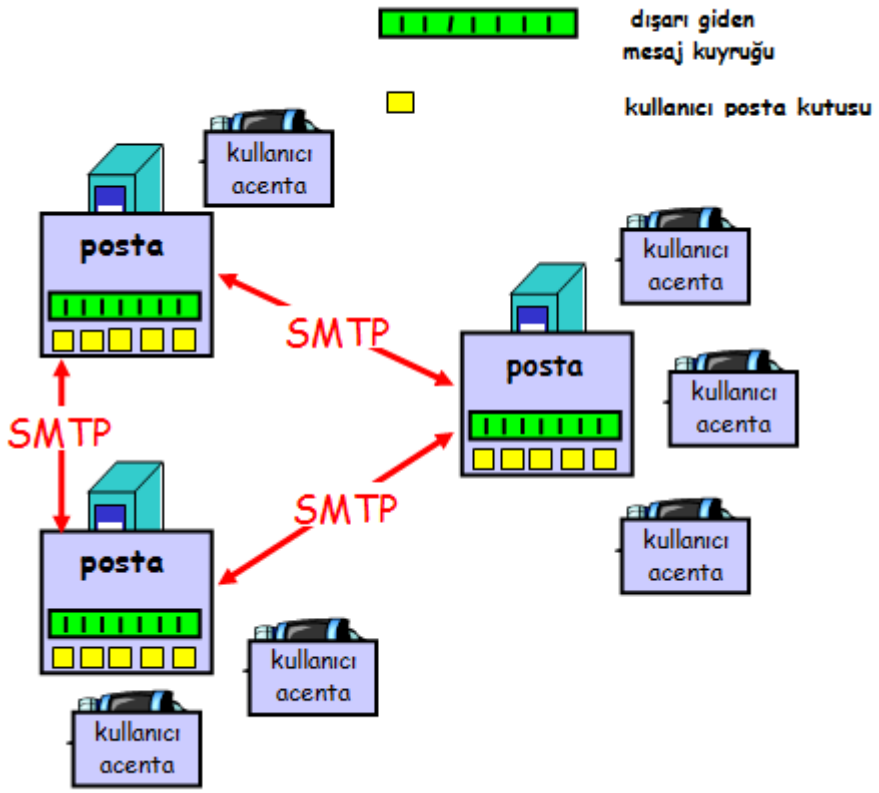
Uygulama katmanı için tanımlı olan prokoller, bir üst katmanda bulunan işletim sisteminin kullanıcıya sunduğu program arayüzlerine hizmet verir. Kullanıcıya hizmet veren programın türüne göre uygulama katmanında farklı protokoller çalıştırılır. Çalıştırılan protokoller işlem yapar (Şekil 1.4). Uygulama katmanında bulunan protokollerin görevleri şunlardır:



Şekil 1.4: Uygulama katmanı

- **SMTP (Simple Mail Transport Protocol-Basit Posta Aktarım Protokolü)**

E-postayı aktaran Basit Posta Aktarım Protokolü, POP3 hizmetiyle birlikte e-posta hizmetlerinin bir parçası olarak yüklenir. SMTP, e-postanın internet boyunca aktarılıp hedef sunucuya teslim edilme yöntemini denetler. POP3 hizmeti e-postayı posta sunucusundan kullanıcının bilgisayarına alırken SMTP hizmeti sunucular arasında e-posta alır ve gönderir.



Şekil 1.5: SMTP protokolünün işleyişi

- **SNMP (Simple Network Management Protocol-Basit Ağ Yönetim Protokolü):** Ağ yapısının fiziksel katmanında bulunan yönlendirici (router), anahtar (switch) ve hub gibi cihazların yönetimini sağlar. SNMP desteği olan ağ cihazları SNMP mesaj alışverişi ile uzaktan yönetilebilir.
- **TELNET (Telecommunication Network-İletişim Ağı):** Kullanıcının bir başka makineye sanki o makinenin istasyonuymuş gibi bağlantı kurmasını sağlayan protokoldür.
- **FTP (File Transfer Protocol-Dosya Aktarım Protokolü):** Bir bilgisayardan başka bir bilgisayara bağlanarak dosya aktarımını sağlar. İnternet üzerindeki iki sistem arasında dosya aktarımı için kullanılan temel protokoldür.
- **NNTP (Network News Transport Protocol-Ağ Haberleri Aktarım Protokolü):** USENET postalanma hizmetinin yürütülmesini sağlar.

- **HTTP (The Hypertext Transfer Protocol-Yüksek Metin İletişim Protokolü):** Web sayfalarının alışverişini sağlar.

Yukarıda bahsedilen bütün protokoller istemci-sunucu mantığına göre çalışır. Bağlanılan makinede hizmet sunan programa sunucu, bağlantı yapan ve böylelikle hizmet alan programa da istemci denir. İstemci ve sunucu programların bilgi transferi yapabilmesi için her iki makinede ilgili protokol programları yüklenmiş ve gerekli ayarlar yapılmış olmalıdır. Meselâ, dosya transferini sağlayabilmek için istemci ve sunucu makinelerde FTP protokolünün kurulmuş olması gerekir.

1.1.2. Ulaşım Katmanı Protokolleri

TCP ve UDP ulaşım katmanı protokolleri, bir üst katmandan gelen veriyi paketleyip bir alt katmana gönderir. Veri bir seferde gönderilmeyecek kadar uzunsa alt katmana verilmeden önce parçalara ayrılır. Her birine sıra numarası verilir. Bu işlemleri genelde TCP protokolü yapar. UDP protokolü daha çok sorgulama amaçlı kullanılmaktadır.

1.1.3. Yönlendirme Katmanı Protokolleri

Yönlendirme katmanında tanımlı IP ve ICMP protokolleri, bir üst katmandan gelen segmentleri alıcıya uygun yoldan ve hatasız ulaştırmakla yükümlüdür. Bu amaçla IP katmanında gelen segmentlere özel bir IP başlık bilgisi eklenir. ICMP protokolü kontrol amaçlı bir protokoldür. Genel olarak sistemler arası kontrol mesajları ICMP protokolü üzerinden gönderilir.

1.1.4. Fiziksel Katman Protokolleri

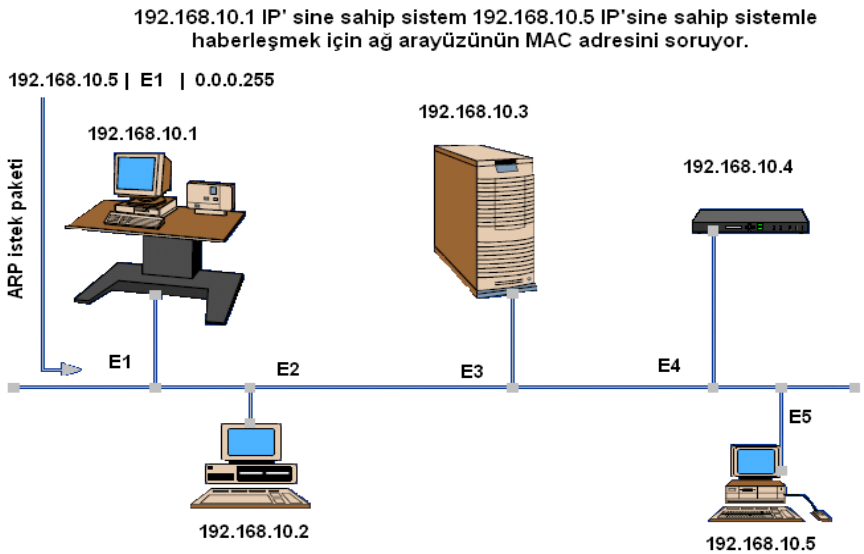
Bu katmanda herhangi bir protokol tanımlı değildir. IP başlığı oluşturulmuş bir bilgi hem kaynak bilgisayarın IP'sini hem de hedef bilgisayarın IP'sini tutar. Fakat yerel ağ içerisinde bilgi transferi yapılacak makineye ulaşmak için makinenin Ethernet kartının MAC (Media Access Control-Ortama Erişim Adresi) olarak bilinen donanım adresinin tespit edilmiş olması gerekir. Bu sebeble bir LAN içerisinde IP adresi bilinen bir bilgisayarın MAC adresini bulmak üzere ARP (Adress Resolution Protocol-Adres Çözümleme Protokolü) protokolü kullanılır. İletişime geçeceği makinenin IP adresini bilen bir bilgisayar ARP protokolü ile IP adresini ağdaki bütün bilgisayarlara gönderir. Ağdaki bilgisayarların tümü bu mesajı alır. Mesajdaki IP adresine sahip bilgisayar kendi MAC adresini karşı tarafa bildirir ve böylelikle iletişim başlar.

1.1.5. Adres Çözümleme Protokolleri

Günümüzde yerel ağların oluşturulmasında en çok kullanılan ağ arayüzü Ethernet'tir denilebilir. Sistemlere Ethernet bağdaştırıcısı (arayüzü) görevi gören kartlar takılarak yerel ağlara kolayca eklenmektedir. Ethernet bağdaştırıcıları birbirlerine veri paketi göndermeleri için kendilerine üretim sırasında verilen fiziksel adresi kullanır. 48 bit olan bu adresler her bir bağdaştırıcı için farklıdır.

Ancak TCP/IP protokol kümesinin kullanıldığı ağlarda, 32 bit olan IP adresleri kullanılır. Fiziksel katmanda Ethernet bağdaştırıcı kullanılıyorsa IP adresten fiziksel adrese dönüşüm işinin yapılması gerekir. Bunun için sistemlerde adres çözümleme protokolü (ARP) ve ARP tabloları kullanılır.

IP paketi içinde hem alıcı hem de gönderici IP adresi vardır ancak paketin yerel ağ içindeki bir sisteme gönderilebilmesi için donanımın yani ağ bağdaştırıcısının fiziksel adresi de bilinmelidir. IP, paketin gideceği fiziksel adresi öğrenmek için o yerel ağ içindeki bilgisayarlara özel bir sorgulama paketi yayar. ARP istek paketi olarak anılan bu pakette alıcı sistemin IP adresi vardır ve bunun karşılığı olan fiziksel adresin gönderilmesi istenir. Ağ üzerinde ARP'leri etkin olan bütün düğümler bu istek paketlerini görür ve kendilerini ilgilendiriyorsa istek paketini gönderen yere fiziksel adreslerini gönderir (Şekil 1.6).



Şekil 1.6: Adres çözümleme protokolü (ARP)

1.1.6. Ipv6 Yeni Nesil Yönlendirme Protokolü

IPv6 (IP version 6) diğer adlandırmayla Ipng (IP next generation), TCP/IP'nin yeni nesil yönlendirme katmanı protokolüdür. Günümüzde tarih itibariyle kullanılan yönlendirme katmanı protokolleri, genel isimlendirmeyle IPv4 olarak anılır. IPv6 ile IPv4'te olan birçok kısıtlamalar giderilmeye çalışılmış ve IP başlıklarında çok az kullanılan alanlar kaldırılmıştır. IPv6'da ilk göze çarpan yenilik adresleme alanı genişliğidir. IPv4'te 32 bit olan adresler IPv6'da 128 bit olmuştur. Böylece adres alanı darlığı giderilmiş ve çok daha geniş adres elde edilmiştir.

IPv6 ile genel olarak şu özellikler kazanılmıştır:

- Yeni adresleme şekli
- Güvenliğin artması
- Otomatik kurulum gibi yeni protokol işlemleri

- RIP, OSPF gibi protokollerin genişletilmesi
- Yeni IP paket yapısı
- Değişik protokoller için IP başlığı düzenlenmesi
- Ses ve görüntü aktarma desteği

1.2. TCP/IP'nin Yapısı

TCP/IP 'de 4 katmanlı bir yapıdan söz edilir.

Windows Sockets NetBIOS	**Uygulama (Application)**
TCP, UDP	**Ulaşım Katmanı**
ICMP, IGMP, IP, ARP	**Yönlendirme Katmanı**
Ethernet, Token-Ring, FDDI, Frame Relay X-25, SLIP, PPP	**Fiziksel Katmanı**

Şekil 1.7: TCP/IP'nin dört katmanı

Fiziksel katman; bilgisayarda bulunan ağ kartını, kabloları vb. şeyleri gösterir. Veri paketlerinin ağa iletilmesinden ve ağdan çekilmesinden bu katman sorumludur. Yönlendirme katmanında IP'ye göre düzenlenmiş veri paketleri bulunmaktadır. Ulaşım katmanından gelen veriler burada veri paketleri hâline gelir. Paketlerin yönlendirilmesi ile ilgili işlemler de burada yapılır.

TCP/IP katmanlarındaki protokoller aşağıda anlatılmıştır.

1.2.1. TCP (Transmission Control Protocol-İletişim Kontrol Protokolü)

TCP'de tanımlı temel görevler aşağıdaki gibi sıralanabilir:

- Bir üst katmandan gelen verinin uygun uzunlukta parçalara bölünmesi
- Her bir parçaya alıcı kısımda aynı biçimde sıraya koyabilmesi amacıyla sıra numarası verilmesi
- Kaybolan veya bozuk gelen parçaların tekrarlanması imkân verilmesi

TCP kendisine atanmış olan bu görevleri yapabilmek amacıyla ulaşım katmanında veri parçalarının önüne başlık bilgisi ekler. Başlık bilgisiyle veri parçası, ikisi birlikte TCP segmenti olarak anılır. TCP segmenti bir alt katmana (IP katmanına) gönderilir, oradan da bu segmente IP başlığı eklenerek alıcıya yönlendirilir.

TCP segmentin genel formatı Şekil 1.8'de görüldüğü gibidir.

Şekil 1.8: TCP segment formatı

- **Gönderici port numarası:** Bir üst katmanda TCP hizmetini isteyen uygulama protokolünün kimliği durumundadır. Karşı mesaj geldiğinde bir üst katmana iletmek için o protokolün adı değil de port numarası kullanılır.
- **Alıcı port numarası:** Gönderilen veri paketinin alıcı tarafta hangi uygulamaya ait olduğunu belirtir.
- **Sıra numarası:** Gönderilen paketin sıra numarasını gösterir. Gönderilmeden önce daha küçük parçalara ayrılan verinin alıcı kısımda yeniden aynı sırada elde edilmesinde kullanılır.
- **Onay numarası:** Gönderilen verinin en son hangi sekizlisinin alındığını göndericiye iletmek için kullanılır. Meselâ n sayısı gönderilirse n'ye kadar bütün sekizlilerin alındığı belirtilir.
- **Başlık uzunluğu:** TCP başlığında var olan 32 bit uzunluğundaki sözcüklerin sayısını gösterir.
- **Saklı tutulmuş:** İlerde yapılacak eklemeler için saklı tutulmuştur.
- **Kod bitleri:** Kontrol bilgilerini taşımak için kullanılır.
- **Pencere:** Alış tampon belleğindeki kullanılabilir alanın sekizli cinsinden boyudur ve alış denetimi için kullanılır.
- **Hata sınama bitleri:** Verinin ve başlığın hatasız aktarılıp aktarılmadığını sınamak için kullanılır.
- **Acil işaretçisi:** İvedi olarak aktarımı sonlandırma vb. durumlarda kullanılır. Acil veri, alıcının uygulama katmanında öncelikle değerlendirilmesi gereken veridir.
- **Veri:** İvedi olarak değerlendirilmesi istenen verinin bölüm içindeki yerini işaret eder.

1.2.2. UDP (User Datagram Protocol-Kullanıcı Veri Bloğu İletişim Protokolü)

Ulaşım katmanında tanımlı tek protokol TCP değildir. UDP de bu katmanda tanımlıdır. UDP'nin farkı, sorgulama ve sınama amaçlı, küçük boyutlu verinin aktarılmasını sağlamasıdır. Veri, küçük boyutlu olduğu için parçalamaya gerek duyulmaz. Dolasıyla UDP protokolü TCP protokolüden bu yönden farklıdır.

Gönderici Port Numarası
Alıcı Port Numarası
Uzunluk
Hata Sınama Bitleri
Kullanıcı Vericisi

Şekil 1.9: UDP segment formatı

Gönderici ve alıcı port numaraları TCP protokolüyle aynı işleve sahiptir. Uzunluk alanı veri ve başlığın boyunu gösterir. Kullanılması seçimlik olan hata sınama bitleri ise paketin hatadan arınmış olarak alınıp alınmadığını sınamak için kullanılır.

1.2.3. ARP (Adress Resolution Protocol-Adres Çözümleme Protokolü)

Gönderilecek olan IP paketinin içinde alıcının ve göndericinin IP adresi bulunmaktadır. Eğer IP paketi yerel ağ içindeki bir bilgisayara gönderilecek ise donanımın (ağ bağdaştırıcısının) fiziksel adresinin bilinmesi gerekir. Burada IP, paketin gideceği fiziksel adresi öğrenmek için o yerel ağ içindeki bilgisayarlara özel bir sorgulama paketi yayar. İşte bu pakete ARP istek paketi (ARP request packet) denir. Bu pakette alıcı sistemin IP adresi vardır. Bu paket ARP yardımıyla ağ içindeki IP'leri tarayarak uygun olan sistemi bulur ve IP paketini gönderir.

İletişime geçeceği bilgisayarın IP adresini bilen bilgisayar ARP protokolü ile "Bu IP adresi kiminse bana MAC adresini söylesin." seklinde bir mesaj oluşturur ve bu mesajı gönderir. Ağda bulunan tüm bilgisayarlar mesajı alır ve eğer söz konusu IP adresi kendilerinin değilse gelen mesaja karşılık vermeyerek çöpe atar. Mesajdaki IP adresi kendine ait olan bilgisayar ise "Bu IP numarası bana ait ve MAC adresim de şu. " şeklinde bir mesaj ile cevap verir. Bu şekilde veri paketi gönderilecek olan bilgisayarın adresini öğrenmiş olur ve veriyi gönderir. Şekil 1.6'da ARP protokolünün ağ sistemi üzerindeki görevini görebiliriz.

1.2.4. MAC Adress (Media Access Control-Ortama Erişim Adresi)

MAC adresi, bilgisayarların ağ kartının ya da benzer ağ cihazlarının içine değiştirilemez bir şekilde yerleştirilmiş olan bir adrestir.

0020AFF8E771 örneğinde olduğu gibi on altılık düzende (hexadecimal) rakamlardan oluşur. MAC adresi yerine donanım adresi ya da fiziksel adres terimleri de kullanılabilir.

1.3. Dinamik Bilgisayar Konfigürasyon Protokolü (DHCP)

TCP/IP protokolünü kullanan bir ağda her bilgisayar için ortalama beş adet parametre tanımlamak gerekir. Bunlar; IP adresi, subnet maskesi, default gateway adresi, DNS sunucu adresi, WINS sunucu adresidir.

Ağdaki bilgisayar sayısı artıkça bu parametrelerin bilgisayarlara girilmesi büyük bir yük getirir. Meselâ, 100 kullanıcılı bir ağda toplam 500 adet parametrenin doğru şekilde girilmesi gerekir. 500 adet parametreyi girerken mutlaka hata yapılır. IP adresleri çakışır, bu yüzden iletişim kurulamaz. Subnet maskeleri yanlış verilirse kendi ağımızdaki ve başka ağlardaki makinelere erişemeyiz. Default gateway adresi yanlış verilirse kendi ağımızdaki makinelerle iletişim kurabiliriz ama bir başka ağa bağlanamayız. DNS ve WINS adresleri yanlış verilirse isim-IP adresi çözümlemesini DNS sunucudan ya da WINS sunucudan yapamayız.

Bu parametreleri doğru bir şekilde girmenin daha kolay bir yolu vardır ve bu sistemin adı DHCP'dir.

1.3.1. DHCP Sunucu Hizmetinin Amacı

DHCP, bilgisayarlara IP adresi ve subnet maskesi başta olmak üzere TCP/IP parametrelerini otomatik olarak dağıtan bir protokoldür. DHCP, daha eski bir protokolün, BOOTP protokolünün geliştirilmişidir.

- DHCP kullanımı şu şekilde gerçekleştirilir:

Bir makine DHCP sunucu olarak kurulur. DHCP sunucu da diğer bilgisayarlara dağıtılacak adresler için bir adres aralığı ve bir subnet maskesi tanımlanır. IP adresi ve subnet maskesi dışında dağıtılabilecek parametreler de (default gateway, DNS ve WINS sunucu adresleri gibi) tanımlanabilir.

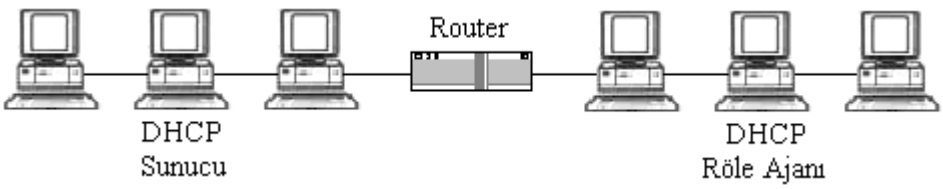
DHCP istemci olarak belirlenmiş bilgisayarlar DHCP sunuculara başvurduklarında adres havuzlarından uygun bir adres seçilerek subnet maskesi ile birlikte istemciye gönderilir. Bu sırada seçimlik bilgiler (default gateway adresi, WINS sunucu ve DNS sunucu adresleri gibi) de istemciye gönderilebilir.

Eğer istemci bilgisayar bu adres önerisini kabul ederse önerilen adres istemciye belli bir süre için verilir. Eğer IP adres havuzunda verilebilecek bir adres kalmamışsa ve istemci başka bir DHCP sunucudan da adres alamıyorsa TCP/IP iletişimine geçilemez.

1.3.2. DHCP Sunucularının Kurulduğu Yerler

DHCP ile IP adres alımı broadcast mesajlara dayandığı için ağımızı oluşturan her bölüme bir DHCP sunucu kurmak gerekmektedir. Bölümlerin birine kuracağımız DHCP sunucu ile diğer bölümlere de hizmet vermek mümkündür. DHCP sunucular; büyük alanlara kurulu olan üniversitelerde, çeşitli devlet kuruluşlarında, okullarda kurulmaktadır.

Tek bir DHCP sunucunun bulunduğu ağlarda, diğer bölümlere birer bilgisayar DHCP röle ajanı konfigüre edilir. DHCP röle ajanı konumundaki bilgisayarlar kendi bölümlerindeki DHCP isteklerini DHCP sunucuya aktarır. DHCP sunucu üzerinde alt ağların her biri için farklı adres aralıkları bulunur. DHCP sunucu kendisine bir röle ajan tarafından IP isteği iletilince bu ajanın adresine bakarak hangi IP adres aralığından adres vermesi gerektiğini bulur. O IP adres aralığında boş bir adres varsa onu röle ajanına gönderir. Röle ajanı da IP adresi istekte bulunan bilgisayara aktarır (Şekil 1.10).



Şekil 1.10: DHCP röle ajanı

1.3.3. DHCP Veri Tabanının Yedeklenmesi ve Yedekten Yüklenmesi

DHCP sunucuda bulunan DHCP veri tabanı varsayılan olarak 60 dakikada bir yedeklenir. Veri tabanının yedeklendiği yer ise Winnt\System32\DHCP\Backup\Jet\New klasörünün içidir. Yedek alma zaman aralığını registry ile oynayarak değiştirebilirsiniz. Bunun için registry'deki

"HKEY_LOCAL_MECHINE\SYSTEM\CurrentControlSet\Services\DHCPServer\Parameters" yolunu izleyerek burada bulunan **BackupInterval** anahtarındaki değeri, istediğiniz bir değerle değiştirerek yedekleme zaman aralığını ayarlayabilirsiniz.

DHCP veri tabanı, DHCP servisinin her başlamasında kontrol edilir ve herhangi bir bozulma olduğu anlaşılırsa yedekten onarılır. Bu işlem DHCP servisi tarafından otomatik olarak yapılır. Bu işlemi manuel olarak yapmak istersek registry'deki;

"HKEY_LOCAL_MECHINE\SYSTEM\CurrentControlSet\Services\DHCPServer\Parameters" yolunu izleyerek burada bulunan **RestoreFlag** parametresini 1 yapmamız gerekiyor. Ardından DHCP servisini yeniden başlatırsanız DHCP veri tabanı onarılacaktır. Onarım işlemi başarıyla tamamlandıktan sonra **RestoreFlag** parametresi 0'a eşitlenecektir.

Bu veri tabanını yeniden yüklemenin bir diğer yolu da **Winnt\System32\Dhcp\Backup\Jet\New** klasorünün içindekileri **Winnt\System32\Dhcp** klasörü içine kopyalayıp DHCP servisini yeniden başlatmaktır.

DHCP veri tabanının boyutu, DHCP sunucunun hizmet verdiği istemci sayısına bağlı olarak değişir ve istemcilerin her IP adresi alışlarında bu veri tabanı büyür. Bu veri tabanını belli aralıklarla küçültmek gerekir. Bu küçültme işlemi sırasında DHCP veri tabanında bulunan geçerli kayıtlar silinir ve böylece dosyanın boyutu küçülür.

DHCP veri tabanını küçültme işleminde dinamik ve offline olmak üzere iki metod kullanılır. Dinamik güncelleme işlemi DHCP sunucunun boş olduğu zamanlarda otomatik olarak başlar. DHCP sunucudaki veri tabanında herhangi bir güncelleme olmadığı bir zamanda, bu veri tabanı otomatik olarak birleştirilmeye başlanır. Offline birleştirme işleminde ise **Jetpack** komutu kullanılır. Offline birleştirme işlemi eğer DHCP sunucu çok yoğunsa yani dinamik birleştirme yapacak kadar boş kalmıyorsa gerçekleştirilebilir. Jetpack komutunun syntax'ı aşağıdaki gibidir.

jetpack <database_adı> <geçici_database_adı>

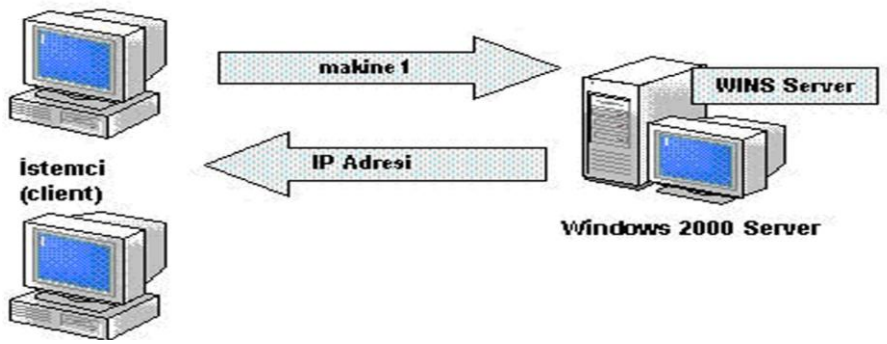
database_adı: DHCP sunucuda bulunan orjinal DHCP veri tabanın adıdır.

Geçici _database_adı: Birleştirme işlemi sırasında kullanılanacak geçici bir veri tabanı dosyası adıdır.

1.4. Windows İnternet İsimlendirme Servisi (Wins)

Bildiğimiz gibi Windows 2000 DNS adları kullanmaktadır. Ancak eski Windows işletim sistemleri ve uygulamalar için NetBIOS adlarını kullanmak durumunda kalır. Bilgisayar networklerinde NetBIOS adları kaynakların bulunması için bir ad çözümleme (name resolation) hizmeti verir.

WINS (Windows Internet Naming Service) hizmeti NetBIOS ad çözümlemesi için bir yöntemdir ve istemcilerin bilgisayarların NetBIOS adlarını bulmasını sağlar. Bu anlamda açılan istemci bilgisayarlar NetBIOS adlarını ve IP adreslerini WINS Server'a yazar (Şekil 1.11).



Şekil 1.11: WINS Server

Windows ad çözümleme hizmetinin işleyişinde aşağıdaki dört işlem vardır:

- Name Registraion (ad yazmak)
- Registration Renewal (kayıt yenilemek)
- Name Query (ad sorgulamak)
- Name Release (adı serbest bırakmak)

İstemci bilgisayar açıldığında NetBIOS adını ve IP adresini WINS Server'a yazar. Bu işlemin ardından WINS Server istemciye kayıt işleminin başarılı olduğuna ilişkin bir mesaj döndürür. Kayıt işleminin bir süresi vardır. Bu süreye TTL (Time To Live) adı verilir. WINS istemcisinin adı ve IP adresi değiştiğinde WINS Server veri tabanı güncellenir.

Bunun dışında istemci kaydının süresi bittiğinde yenileme işlemi yapılır. Eğer yenileme yapılmazsa ad kaydı sona erdirilir. WINS hizmetinin doğal hizmeti adların sorgulanmasıdır. Bu, bir istemcinin diğer bir istemcinin NETBIOS adını WINS Server'da istemesidir. WINS Server'dan diğer istemcinin IP adresini alan istemci network iletişimi yapar.

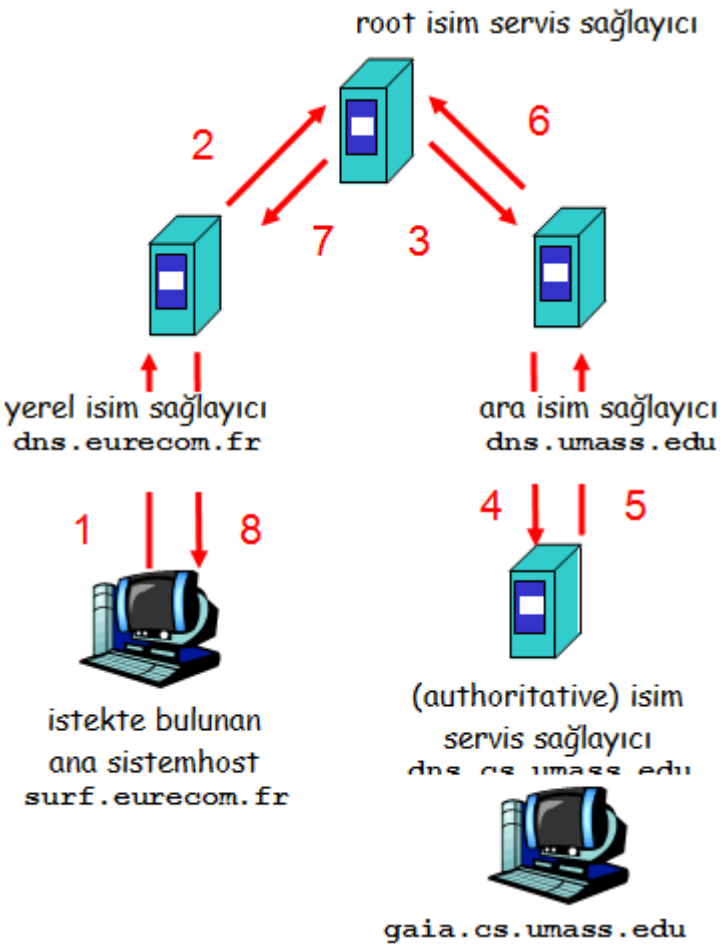
1.5. Alan İsim Sistemi (DNS)

1.5.1. DNS'nin Yapısı

DNS, 256 karaktere kadar büyüyebilen host isimlerini IP' ye çevirmek için kullanılan bir yöntemdir. Host ismi, hem bilgisayarın ismini hem de bilgisayarın bulunduğu internet domaini gösterir.

İnternette kullanılan çeşitli domainler:

com : Ticari kuruluşlar
edu : Eğitim kurumları
org : Ticari olmayan, hükümete de bağlı bulunmayan kurumlar
net : İnternet omurgası işlevini üslenen ağlar
gov : Hükümete bağlı kurumlar
mil : Askeri kurumlar
arpa : Ters DNS sorgulaması yapılabilecek yerler



Şekil 1.12: DNS'nin çalışması

1.5.2. Yetki Bölgesi

Belli bir adres aralığıdır. Örneğin, **megep.meb.gov.tr'**de "meb.gov.tr" bir yetki bölgesidir. Her yetki bölgesinden sorumlu bir DNS sunucu vardır.

DNS sunucunun yetki bölgesi en az bir tane domain içerir. Bu domain bölgenin kök domaini olarak adlandırılır. Bir DNS sunucu birden fazla bölgeyi yönetebilir.

1.5.3. DNS Sunucu Çeşitleri

- **Birincil İsim Sunucu (Primary Name Server):** Bölgesiyle ile ilgili bilgileri kendisinde bulunan bölge dosyasından elde eder. Bu dosyaya bilgiler elle, tek tek girilir. O bölgede bulunan bilgisayarlara da DNS sunucu adresi olarak birincil DNS sunucunun adresi verilir. Böylece, daha önce anlatılan işlemler gerçekleşir.
- **İkincil Name Server (Secondary Name Server):** Bölgesiyle ilgili bilgileri bağlı bulunduğu bir DNS Server'dan alır yani bilgiler bu sunucuya elle girilmez. İkincil DNS sunucu, bölgesindeki bilgisayarların bilgisini bağlı bulunduğu birincil DNS sunucudan alır. Buna "zone transfer" denir. Bu ayrıca bir sorun olduğunda sistemin ayakta kalabilmesini sağlar. Her bölgenin bilgisi ayrı dosyalarda saklanır yani bir sunucu bir bölge için birincil iken diğeri için ikincil olabilir.
- **Yalnızca İsim Saklayan Sunucu (Caching-Only Name Server):** Kendisinde bölge bilgilerinin tutulduğu bir dosya bulunmaz. Bağlı bulunduğu sunucuya sorarak topladığı bilgileri (isimleri) hem istemcilere ulaştırır hem de kendisinde tutar.

1.6. Basit Ağ Yönetim Protokolü (SNMP)

Ağ yönetimi için çesitli protokollar tanımlanmıştır. Bunlar içinde en yaygın olanı TCP/IP protokol kümesi içindeki SNMP'dir. Bir TCP/IP ağ içerisindeki ağ cihazlarının ve bilgisayar sistemlerinin ağ yönetim yazılımı (Network Management Software) ile denetlenmesi için herbirinde SNMP yazılım parçası (agent) olmalıdır. Bu yazılım parçası ile ilgili cihazın durum bilgileri ağ yönetim yazılımına (NMS) bildirilir. SNMP yazılım parçasına sahip olmayan cihazlar ağ yönetim yazılımı (NMS) ile yönetilemez. Ağ yönetim desteği olan cihazlara, örneğin anahtara veya HUB'a, yönetilebilir anahtar (manageable switch) veya yönetilebilir HUB (manageable HUB) denir.

1.7. Dosya Aktarım Protokolü (FTP) ve İletişim Ağı (TELNET)

Şekil 1.13: FTP'nin çalışması

FTP (File Transfer Protocol) internete bağlı bir bilgisayardan diğerine (her iki yönde de) dosya aktarımı yapmak için geliştirilen bir internet protokolü ve bu işi yapan uygulama programlarına verilen genel addır. İlk geliştirilen internet protokollerinden biridir. FTP protokolü ile bir bilgisayardan başka bir bilgisayara dosya aktarımı yapılırken o bilgisayar ile etkileşimli aynı anda (on-line) bağlantı kurulur ve protokol ile sağlanan bir dizi komutlar yardımıyla iki bilgisayar arasında dosya alma/gönderme işlemleri yapılır.

TELNET, internet ağı üzerindeki çok kullanıcılı bir makineye uzaktaki başka bir makineden bağlanmak için geliştirilen bir TCP/IP protokolü ve bu işi yapan programlara verilen genel isimdir. Bağlanılan makineye girebilmek (login) için orada bir kullanıcı isminizin (user name) ve bağlantının gerçekleşebilmesi için bir TELNET erişim programınızın olması gereklidir.

UYGULAMA FAALİYETİ

Ağ sistemine ve kurulan ağ işletim sistemine uygun olarak protokol düzenlemelerini yapınız.

İşlem Basamakları	Öneriler
➢ Ağ işletim sistemi içinde bulunan ağ ayarları ile ilgili kısmı çalıştırınız. ➢ Ağ protokollerini kontrol ediniz. ➢ Gerekiyorsa protokol ayarlarını değiştiriniz. ➢ DHCP sunucu kurunuz. ➢ Ağdaki diğer bilgisayarlara IP numarası veriniz. ➢ DNS kurunuz. ➢ FTP ve TELNET düzenleyiniz. ➢ Ağ üzerinde dosya alışverişi yapınız. ➢ SNMP'yi düzenleyiniz.	➢ Mevcut olan ağ sistemin bağlantı kablolarına ve ağ donanım parçalarının düzenine dikkat ediniz. ➢ Kullanılan ağ işletim sisteminin çalışmasını etkileyecek komut ya da komutlar kullanmayınız. ➢ Enerji ile çalışan donanım parçalarının gerilimlerine dikkat ediniz.

KONTROL LİSTESİ

Bu faaliyet kapsamında aşağıda listelenen davranışlardan kazandığınız beceriler için **Evet**, kazanamadığınız beceriler için **Hayır** kutucuğuna (X) işareti koyarak kendinizi değerlendiriniz.

Değerlendirme Ölçütleri	Evet	Hayır
1. DHCP sunucusunu kurabildiniz mi?		
2. DNS'I kurabildiniz mi?		
3. FTP ile TELNET'i düzenleyebildiniz mi?		
4. Ağ üzerinde dosya alışverişi yapabildiniz mi?		
5. SNMP'yi düzenleyebildiniz mi?		

DEĞERLENDİRME

Değerlendirme sonunda **"Hayır"** şeklindeki cevaplarınızı bir daha gözden geçiriniz. Kendinizi yeterli görmüyorsanız, öğrenme faaliyetini tekrar ediniz. Bütün cevaplarınız **"Evet"** ise "Ölçme ve Değerlendirme"ye geçiniz.

ÖLÇME VE DEĞERLENDİRME

Aşağıdaki soruları dikkatlice okuyunuz ve doğru seçeneği işaretleyiniz.

1. Aşağıdakilerden hangisi DNS protokolünün görevidir?
A) Host isimlerini IP adresine çevirir.
B) Göndericinin ve alıcının IP adresini tutar.
C) Veri aktarılmasını sağlar.
D) Bir üst katmandan gelen veriyi uygun uzunlukta parçalara ayırır.

2. Aşağıdakilerden hangisi DHCP protokolü tarafından dağıtılmaz?
A) IP adresi B) Subnet maskesi C) DNS sunucu adresi D) Host ismi

3. Aşağıdaki protokollerden hangisi ağ içerisinde elektronik mektup alışverişini sağlar?
A) HTTP B) SMTP C) ICMP D) TCP

4. Aşağıdaki eşleştirmelerden hangisi yanlıştır?
A) edu→ Eğitim kurumları
B) com→ Ticari kuruluşlar
C) mil→ Askeri kurumlar
D) gov→ Ticari olmayan hükümete te bağlı olmayan kurumlar

5. İnternet üzerinde dosya aktarımı yapmak için kullanılan protokol aşağıdakilerden hangisidir?
A) TELNET B) SNMP C) FTP D) WINS

6. Aşağıdakilerden hangisi ulaşım katmanı protokollerindendir?
A) IP-ICMP B) TCP-UDP C) HTTP D) DNS

7. Aşağıdakilerden hangisi Ethernet kartında bulunan değiştirilemeyen bir adrestir?
A) ARP B) UDP C) MAC D) WINS

8. Aşağıdakilerden hangisi TCP/IP mimarisi katmanlarından değildir?
A) Sunum B) Uygulama C) Ulaşım D) Fiziksel

DEĞERLENDİRME

Cevaplarınızı cevap anahtarıyla karşılaştırınız. Yanlış cevap verdiğiniz ya da cevap verirken tereddüt ettiğiniz sorularla ilgili konuları faaliyete geri dönerek tekrarlayınız. Cevaplarınızın tümü doğru ise bir sonraki öğrenme faaliyetine geçiniz.

ÖĞRENME FAALİYETİ-2

AMAÇ

İnternette adres sınıflarını tanıyarak bir yerel ağı, alt ağlara ayırma (subnet mask) işlemini yapabileceksiniz.

ARAŞTIRMA

- İnternet erişimi olan bir bilgisayardan değişik adreslere girerek adres sınıflarının uzantılarına ve nasıl gruplandırıldığına dikkat ediniz.
- İnternete girdiğimizde bilgisayarımıza IP adresinin nasıl atandığını araştırınız.
- Okulunuzda veya bilgisayar laboratuvarınızdaki yerel ağın alt ağlara bölünüp bölünmediğini araştırınız.

2. İNTERNET ADRES SINIFLARI VE ALT AĞLAR

İnternet ortamına giren her bilgisayara bir adres verilir. Bu adrese IP adresi denilir. IP adresi, ağ üzerinde bulunan makinenin adresini ifade eder. Bu adres ile bir makine diğerlerine ulaşma imkânı bulur. Ağ üzerinde bulunan herhangi bir bilgisayarı ifade etmek için 32 bitlik bir IP adresi kullanılır. TCP/IP protokolü kullanılan bir ağda her bilgisayarın mutlaka bir IP adresi olmak zorundadır.

32 bitlik bir IP adresi 8 bitlik dört oktet hâlinde ifade edilir. Bunun amacı, okumayı kolaylaştırmaktır. Adresleme için toplam 32 bitimiz varsa 232 = 4 milyar 294 milyon 967 bin 196 tane bilgisayar adreslenebilir. Ancak bu gerçekte böyle değildir. 32 bitlik bir adres diyelim ki 1000010.00011011.00001100.00001100 şeklinde ifade edilmiş olsun bu adresin okunması için ikilik sistemde bir okuma gerekmektedir, ancak bu şekilde de okuma oldukça zor olduğunda yazdığımız adres onluk sisteme çevrilerek 194.27.12.12 şekline dönüşür ve bu tür bir ifadeye noktalı yazım (dotted decimal notation) denir. Nokta ile ayrılan kısımların her biri 0 ile 255 arasında bulunan birer tam sayı olmak zorundadır.

2.1. Adres Sınıflaması

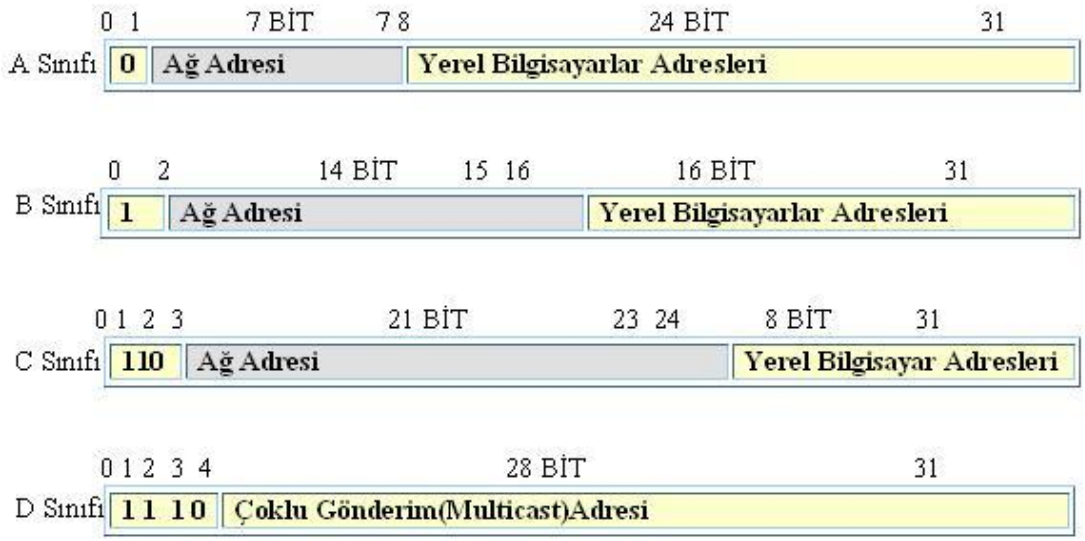
İnternete bağlı büyüklü küçüklü binlerce ağ vardır ve bu ağlar için gerekli IP adresleri sayısı birbirinden oldukça farklı olabilmektedir. Adres dağıtımını ve ağlara atanan adreslerin ağ aygıtlarına yerleşimini kolaylaştırmak amacıyla IP adres alanı alt kümelere bölünmüştür yani sınıflandırılmıştır. Beş temel sınıflama vardır. Bunlar; A,B,C,D ve E sınıfı adresler olarak adlandırılır. Bunlardan hangisinin gerektiğini doğrudan bu adreslerin kullanılacağı ağın büyüklüğü belirler.

Şekil 2.1: Ağ adresi

Adresler iki parçaya ayrılır. Parçanın soldaki kısmı ağ adresi, sağdaki kısmı ise sistem adresi olarak adlandırılır. Ağ adresleri yönlendiriciler için daha anlamlıdır. Tüm yönlendirme işlemleri ağ adreslerine bakılarak yapılır. Şekil 2.1'de sınıflanmış bir ağın ayrılmış hâli görülmektedir.

Sınıflamalı adreslemede 32 bitlik adresin kaçar bitinin ağ ve sisteme ait olduğunu belirlemek için ağ maskesi kullanılır. Ağ maskesi IP adresiyle mantıksal VE işlemine tabii tutulur ve sonuç ağ adresini verir. Örneğin, 167.34.1.1 IP adresine ve 255.255.0.0 ağ maskesine sahip bir bilgisayarın VE işleminden sonra ağ adresi 167.34.0.0 ve sistem adresi 1.1 olur.

Sınıflamalı adreslemede IP adresleri A,B,C,D ve E şeklinde ayrılır.



Şekil 2.2: IP adreslerinin sınıflandırılması

Noktalı gösterimde Şekil 2.2'den de anlaşılacağı üzere her sınıf için tanımlanabilecek maksimum sayıda bilgisayar adedi vardır. Bu bilgisayarlar internet ortamında "host" diye

adlandırılır. Her bir sınıf için tanımlanabilecek host sayısı şekilsel olarak aşağıda belirtilmiştir.

h: "host" ağ üzerinde tanımlanacak olan bilgisayarlar
A Sınıfı: 001.hhh.hhh.hhh'den 126.hhh.hhh.hhh'ye kadar
B Sınıfı: 128.001.hhh.hhh'den 191.254.hhh.hhh'ye kadar
C Sınıfı: 192.000.001.hhh'den 223.255.254.hhh'ye kadar
D Sınıfı: 224.000.000.000'dan 239.255.255.255'e kadar

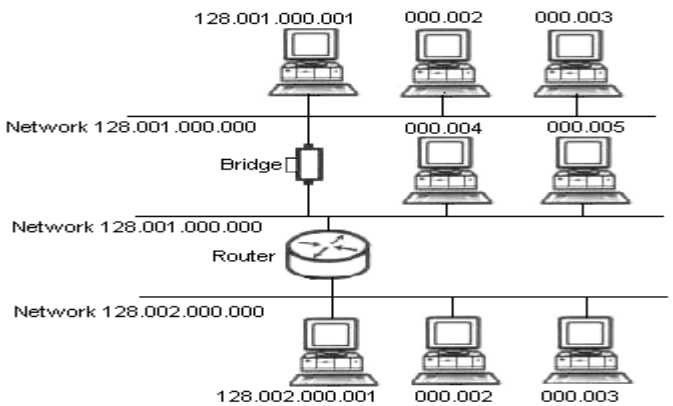
2.1.1. A Sınıfı Adresler

A sınıfı adreslerde ağ adresi ilk oktet ile belirlenir. Geri kalan diğer oktetler ise o ağdaki bir bilgisayarı gösterir. IBM firması A sınıfı bir adres kullanmaktadır. İlk oktet 0 ile 126 arasında ise o adres bir A sınıfı adrestir. A sınıfı adres her biri 16 777 214 tane bilgisayar içeren 126 tane alt ağa izin verir. 16 777 214 sayısı (224 – 2)'den hesaplanır. Burada iki sayısının çıkarılması A sınıfı adreslemede iki adresin özel amaçlı olarak kullanılmasıdır. 126 sayısı ise (27-2)' den hesaplanır. Burada da iki çıkarılmıştır çünkü 0.0.0.0 ve 127.0.0.0 adresleri özel amaçlı kullanılmaktadır. 0.0.0.0 adresi varsayılan yönlendirme ve 127.0.0.0 adresi ise yerel çevrim için kullanılır.

2.1.2. B Sınıfı Adresler

B sınıfı ağlar 14 bit, ağ içindeki bilgisayarlar ise 16 bit ile ifade edilir. İlk iki biti 1 0 şeklindedir. B sınıfı her biri 65 534 bilgisayar içeren 16 384 tane alt ağa izin verir. Bu tür adres alanı büyük ve orta büyüklükte ağlar için kullanılır. Birçok büyük üniversite ve ISS' ler bu tür adres alanına sahiptir.

Şekil 2.3'te, 128.001.000.000 ve 128.002.000.000 IP adreslerine sahip olan B sınıfı iki ayrı ağ router ile birbirinden ayrılmış ve bu ağlardan 128.001.000.000 IP adresine sahip olan ağ kendi içinde mantıksal iki ayrı alt ağa köprü (bridge) yardımı ile ayrılarak ağ kurulumun sağlanması görülmektedir.



Şekil 2.3: B sınıfı adresleri kullanarak örnek ağ uygulaması

2.1.3. C Sınıfı Adresler

C sınıfı adres alanı içinde ağlar 21 bit, ağ içindeki bilgisayarlar 8 bit ile temsil edilir. Kamu kuruluşlarına C sınıfı adresler verilmektedir.

2.1.4. D Sınıfı Adresler

D sınıfı adresler özel amaçlı adresler olup bir datagramın birçok sisteme dağıtılması için kullanılır.

2.1.5. E Sınıfı Adresler

E sınıfı adreslerin özelliği gizli tutulmuştur.

2.2. Alt Ağlar (Subnets)

Alt ağ kavramı, sahip olunan IP adreslerini daha küçük adres gruplarına parçalamak anlamına gelir. Örneğin, C sınıfı bir adresde 256 tane IP adresi vardır ancak LAN içerisinde 50 tane sistem varsa yaklaşık 200 tane IP adresi boşa gidecektir. Bu durumda C sınıf adres parçalanarak alt ağlara ayrılır ve yeni oluşturulan alt ağ içindeki adresleri kullanır.

2.2.1. Alt Ağ Maskesi (Subnet Mask)

Bir bilgisayar ancak aynı ağda bulunan bir bilgisayarla doğrudan iletişime geçebilir. Aynı ağda değillerse dolaylı olarak iletişime geçer. Aynı ağda olup olmadığını IP adreslerini kullanarak anlarız. IP adresinin bir bölümü ağı, diğer bölümü de bilgisayarın ağ içindeki adresini tanımlar. Hangi bölümü ile ağı, hangi bölümü ile bilgisayarı tanımladığını bilmek için alt ağ maskesi kullanırız. Dört bölümden oluşur ve ağ adresinin hangi bölüme kadar geldiğini göstermek için kullanılır. Bilgisayar kendi ağ tanımlayıcılarını bulmak için alt ağ maskesi kullanır. Bu yüzden alt ağ maskesinin doğru şekilde girilmesi gerekir. Yanlış girilirse bilgisayarın diğer bilgisayarlarla iletişimi engellenebilir.

Bilgisayar ağ tanımlayıcısını bulmak için alt ağ maskesi ile IP adresi VE mantıksal işleminden geçirilir.

Örnek: IP adresi 195.134.67.200 olsun ve alt ağ maskesi de 255.255.255.0 olsun. Bilgisayarın bu bilgilere dayanarak bulunduğu ağ tanımlayıcısını yani ağ adresini bulabiliriz. IP adresi ile alt ağ maskesini VE işlemine tabi tutalım:

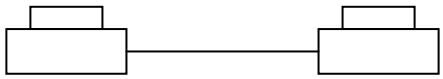
195.134.67 .200 = 1100 0011.1000 0110.0100 0011.1100 1000

VE

255.255.255.0 = 1111 1111.1111 1111.1111 1111.0000 0000

Sonuç: 195.134.67. 0 = 1100 0011.1000 0110.0100 0011.0000 0000

Şimdi, iki bilgisayardan oluşan bir ağ düşünelim. Şekle bakalım:

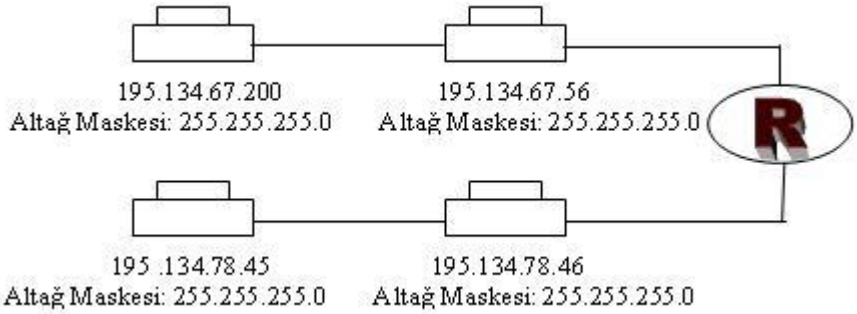


195.134.67.200 Alt ağ maskesi: 255.255.255.0

195.134.67.56 Alt ağ maskesi: 255.255.255.0

Şekilde görülen 195.134.67.0 adresli bilgisayarın diğer bilgisayarla iletişime geçmesi için aynı ağda olmaları gerekir. Bu yüzden hedef bilgisayarın aynı ağda olup olmadığına bakılır. Bunun için bilgisayarların ağ adreslerine bakarız.

195.134.67.200 VE 255.255.255.0 ile işleme koyduktan sonra çıkan sonuç: 195.134.67.0 olacaktır. Bu bilgisayarın kendi ağ adresidir. Hedef bilgisayarın ağ adresi ise: 195.134.67.56 ile 255.255.255.0 VE işleme konularak 195.134.67.0 sonucu görürüz. Aynı ağ adresleri çıktığı için bu bilgisayarların iletişime geçeceklerini söyleyebiliriz. Yeni örneğimiz için aşağıdaki şekle bakalım.



Bu kurulan ağda 195.134.67.200 adresli bilgisayar ile 195.134.78.46 numaralı bilgisayar iletişime geçmek isterse ilk olarak aynı ağda olup olmadıklarına bakmaları için IP adresleri ile alt ağ adresini VE'leyerek kendi ağ adreslerini bulur. Aynı işlemi hedef bilgisayar için de yapar. Sonuç aynı çıkmaz. Bunun sonucu olarak 195.134.67.200 numaralı bilgisayar iletmek istediği veriyi yönlendiriciye gönderir, o da gelen pakete bakıp 195.134.78.46 numaralı bilgisayarı hedeflediğini anlar ve veriyi ona aktarır. Eğer alt ağ adresini 255.255.0.0 şeklinde yanlış girmiş olsaydık VE'lediğimiz sonucu bize aynı ağda olduğunu gösterecektir. Ulaşmaya çalışacaktık ama erişemeyecektik.

IP adresini ve alt ağ adresini DHCP dağıtıcısı ile dağıtırız. Yukarıdaki bilgisayarda ilk ağ için 195.134.67. 0, ikinci ağ için 195.134.78.0 ağ adresimizdir. Demek ki ilk ağda hiçbir bilgisayara 195.134.67.0 adresini veremeyiz. Bu adres ilk ağın tümünü belirtiyor. Aynı şekilde 2. ağ için de 195.134.78.0 adresini veremeyiz. Dolayısıyla bize son oktet için 256 bilgisayarı tanımlayabilecek 255 adres tanımlayabiliriz.

Benzer şekilde 195.134.67.255 adresini hiçbir bilgisayara veremeyiz. Bu adres, bu ağın broadcast adresidir. O zaman tanımlanabilecek adresler şöyle bir kural ile hesaplanır: IP

adresine hem ağ tanımlayıcısı kısım hem bilgisayar tanımlayıcı kısım 0 (0000 0000) ya da 255 (1111 1111) olamaz. Böylece ağ adres sayısı 2^n-2 ile hesaplanır.

Yukarıdaki örnekte C sınıfı adres söz konusu olduğu için ilk 3 oktet sabittir. Biz yalnızca son okteti serbestçe kullanırız. Bu oktet, 8 olduğuna göre 2^8-2'den 254 adet bilgisayar adresi tanımlayabiliriz.

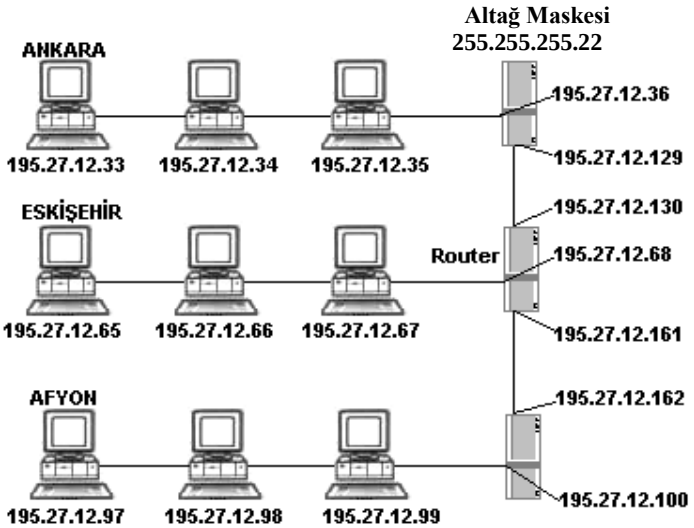
2.2.2. Alt Ağlara Ayırma (Subnetting)

Alt ağlara ayırma işlemi verilen bir adres aralığını bölümlemek demektir. İnternete erişim için yetkili bir kurumdan ağ adresi alırız ve bu adres diyelim ki 195.27.12.0 gibi bir adres olsun. Buradan anlaşılacağı üzere bu adres, C sınıfı bir adrestir. C sınıfı bir adres için de 255.255.255.0 gibi bir alt ağ maskemiz vardır. Bu durumda kurum ağımızda 254 adet bilgisayar adresi tanımlayabiliriz çünkü bize adres belirleme için son oktet yani 8 bit kalıyor. Adres kuralımızı uygularsak 2^8-2=254 adet bilgisayar adresi verebiliriz. Kurumumuz bilgisayarlarının Ankara, Eskişehir ve Afyon gibi üç ayrı ilde olduğunu varsayalım. Bu durumda kurumumuzda üç ayrı ağ segmenti bulunacak ve bunlar yönlendiriciler (router) aracılığı ile birbirlerine bağlanacaktır. Burada alt ağlara ayırma işlemini adresimiz C sınıfı bir adres olduğundan IP numaramızın son oktetinde gerçekleştireceğiz. Her bir şehirdeki bilgisayarlar (Ankara, Eskişehir ve Afyon olmak üzere 3 tane alt ağ) ve iki şehir arasında kalan bölümlerde (Ankara-Eskişehir ve Eskişehir-Afyon olmak üzere 2 tane alt ağ) birer alt ağdır. Yani 5 tane alt ağ tanımlamamız gerekiyor. Bu sebeple değişiklik yapabildiğimiz tek oktet olan 4. oktetin ilk üç bitini alt ağ için ayırmamız gerekiyor. Üç bit olmasının sebebi ise 5=101 olmasıdır.

C sınıfı ağımız ikili sistemde: 11000011.00011011.00001100.00000000 şeklinde gösterilir. Bu IP adresinin sadece son okteti ile oynama yaparak alt ağları oluşturacağız.

Ağ	Başlangıç Adresi	Bitiş Adresi
1	11000011.00011011.00001100.**001**00001 (195.27.12.33)	11000011.00011011.00001100.**001**11110 (195.27.12.62)
2	11000011.00011011.00001100.**010**00001 (195.27.12.65)	11000011.00011011.00001100.**010**11110 (195.27.12.94)
3	11000011.00011011.00001100.**011**00001 (195.27.12.97)	11000011.00011011.00001100.**011**11110 (195.27.12.126)
4	11000011.00011011.00001100.**100**00001 (195.27.12.129)	11000011.00011011.00001100.**100**11110 (195.27.12.158)
5	11000011.00011011.00001100.**101**00001 (195.27.12.161)	11000011.00011011.00001100.**101**11110 (195.27.12.190)
6	11000011.00011011.00001100.**110**00001 (195.27.12.193)	11000011.00011011.00001100.**110**11110 (195.27.12.222)

Tablo 2.1: Alt Ağ adresleri



Şekil 2.4: Yönlendiriciler ile ağ kurulumu

Bu dağılımı yaptıktan sonra her ildeki ağ adreslerinin son oktetinin geriye kalan 5 bitini de ağ içindeki bilgisayarları tanımlamak için kullanılır. Kuralımıza göre 2^5-2= 30 olarak bulunur ve bir ağımızda 30 adet bilgisayar tanımlayabiliriz. Toplam 6 adet ağ tanımlama hakkımız vardı. Buna göre 6.30=180 adet bilgisayarı bu ağımız için tanımlamamız mümkündür. İlk başta bize verilen IP adresine göre toplam 254 adet bilgisayar tanımlama hakkımız vardı ancak alt ağlara ayırdıktan sonra sadece 180 bilgisayar tanımlayabiliz. Buradaki 74 adet adres alt ağlara ayırma işlemi sırasında boşa gitti.

Bir IP adresinde ağ tanımlayıcı ve bilgisayar tanımlayıcı bölümleri alt ağ maskesi (subnet mask) ile belirleriz. Yukardaki örnekte en fazla altı olabilecek, beş adet ağ bölümümüz (segment) var. Dolayısıyla bize yetkili kurum tarafından verilen 255.255.255.0 maskesini kullanamayız. Bu maskeyi ancak bütün bilgisayarlar tek bir bölümde bulunduğu zaman kullanırız. Bizim tanımlayacağımız alt ağ maskesi sayesinde her şehirdeki (bölümdeki) bilgisayar hem kendi aralarında hem de şehirler arası (başka bölümdeki) bilgisayarlarla haberleşmelidir.

Adreslerin ve dolayısıyla alt ağ maskesinin ilk üç oktetinde değişiklik yapamayız. Sadece son oktette değişiklik yapabiliriz. Örneğimizde tüm ağlarda ağı belirleyen kısım son oktetin ilk üç bitidir. O zaman alt ağ maskemiz 255.255.255. 1110 0000 olmalıdır yani 255.255.255.224. Şimdi alt ağ maskemizi sınayalım:

Ankara'daki 195.27.12.33 numaralı bilgisayarla sınayalım:
195.27.12.33 VE 255.255.255.224 = 195.27.12.32 olur.
Ankara'daki 195.27.12.35 numaralı bilgisayarla sınayalım:
195.27.12.35 VE 255.255.255.224 = 195.27.12.32 olur.

İkisi de aynı sonucu verdiği için aynı ağ üzerinde olduğunu varsayacaktır ve iletişime geçecektir.

İstanbul ile haberleştirmeye çalışalım.195.27.12.66 VE 255.255.255.224 = 195.27.12.64 olur. İki işlem sonucu farklı olduğu için hedef bilgisayarın başka bir ağ bölümünde olduğunu varsayacaktır. Başka bir bölümdeki bilgisayarla doğrudan iletişime geçemeyecek ve veri paketini yönlendiriciye yollayacaktır. Yönlendiricilerin her bir bacağına IP adresi vermemiz gerekiyor. Bu adresler yönlendirici bacaklarının bağlı oldukları bölümlere uygun olarak verilmelidir. Örneğimizde yönlendiricinin Ankara'ya bakan bacağına 195.27.12.36, İstanbul'a bakan bacağına 195.27.12.68, Afyon'a bakan bacağına ise 165.27.12.100 IP adresleri verilmelidir. Ayrıca Ankara-İstanbul ve İstanbul-Afyon arasındaki bacaklara da IP adresi atamamız gerekmektedir. Çünkü buralar da birer alt ağdır. Bu adresler Ankara'dan Afyon'a doğru sırasıyla 195.27.12.129, 195.27.12.130, 195.27.12.161 ve 195.27.12.162'dir. Buradaki IP adres değerleri yukarıdaki tablodan 4 ve 5. ağ başlangıç adreslerinden gelmektedir.

Bu konuyla ilgili özet maddeler aşağıda sıralanmıştır:

- Ağı alt ağlara ayırırken ilk önce kaç tane ayrı ağ istendiğine karar verilmelidir.
- Buna göre kaç tane yönlendirici kullanılacağı belirlenmelidir.
- Toplam alt ağ sayısı belirlenirken yönlendiriciler arasında kalan kısımlar unutulmamalıdır. Onlar da ayrı birer alt ağdır. Hesaba onlar da dahil edilmelidir.
- Kurum adresimizde bizim sorumluluğumuza bırakılan kısma bakıp oluşturulacak alt ağlar için buradaki birler kullanılmalıdır.
- 2^n-2 kuralına uygun olarak alt ağ belirlerken kaç adet bit kullanılacağı saptanmalıdır. Çıkan sayı da bitleri alt ağ tanımlayıcılarını belirlemekte kullanılmalıdır. Geriye kalan bitlerle de alt ağlardaki bilgisayarlar tanımlanmalıdır.
- Kurum çapında geçerli olan yeni alt ağ maskesi belirlenmelidir. Bu yeni alt ağ maskesinde alt ağ tanımı için kullanılan bitlerin yerleri bir olmalıdır.

UYGULAMA FAALİYETİ

Ağ sistemine göre adres sınıflandırmasını yapınız.

İşlem Basamakları	Öneriler
➢ Ağ sistemine göre adres sınıflandırmasını yapınız. ➢ Gerekli hesaplamaları yaparak IP adreslerini tanımlayınız.	➢ İnternet ayarlarının özelliklerine dikkat ediniz. ➢ Ağ işletim sisteminin çalışmasını etkileyecek komutları kullanırken dikkatli olunuz. ➢ Yerel ağda IP adreslerinin düzenine dikkat ediniz.

KONTROL LİSTESİ

Bu faaliyet kapsamında aşağıda listelenen davranışlardan kazandığınız beceriler için **Evet**, kazanamadığınız beceriler için **Hayır** kutucuğuna (X) işareti koyarak kendinizi değerlendiriniz.

	Değerlendirme Ölçütleri	Evet	Hayır
1.	Ağ sistemine göre adres sınıflandırmasını yapabildiniz mi?		
2.	Gerekli hesaplamaları yaparak IP adreslerini tanımlayabildiniz mi?		

DEĞERLENDİRME

Değerlendirme sonunda **"Hayır"** şeklindeki cevaplarınızı bir daha gözden geçiriniz. Kendinizi yeterli görmüyorsanız, öğrenme faaliyetini tekrar ediniz. Bütün cevaplarınız **"Evet"** ise "Ölçme ve Değerlendirme"ye geçiniz.

ÖLÇME VE DEĞERLENDİRME

Aşağıdaki soruları dikkatlice okuyunuz ve doğru seçeneği işaretleyiniz.

1. 1100 0011.1000 0110.0100 0011.1100 1000 IP adresi aşağıdakilerden hangisidir?
A) 195.134.67.200 B)192.143.0.25
B) 212.45.142.131 D) 24.124.1.56

2. 130.15.1.5 hangi sınıf IP adresidir?
A) A sınıfı B) B sınıfı C) C sınıfı D) D sınıfı

3. IP adresi 192.128.63.50, altağ maskesi 255.255.255.0 ise ağ adresi aşağıdakilerden hangisidir?
A) 192.0.0.0 B) 123.4.53.50 C) 192.128.63.0 D) 123.4.0.0

4. 132.45.53.4 ve 132.45.78.123 IP adreslerine sahip bilgisayarlar için aşağıda verilenlerden hangisi doğrudur?
A) İkisi de farklı ağlarda oldukları için router ile iletişime geçer.
B) Aynı ağda oldukları için doğrudan iletişime geçer.
C) Bilgisayarlar birbiri ile bilgi alışverişi yapamaz.
D) Her iki IP adresi C sınıfı IP adresidir.

5. Aşağıdakilerden hangisi alt ağ maskesinin görevidir?
A) Bilgisayarlar arası veri alışverişini sağlar.
B) Bilgisayarlara IP numarası verir.
C) D ve E sınıfı IP adresleri için tasarlanmıştır.
D) Bilgisayarların ağ tanımlayıcılarını bulmayı sağlar.

DEĞERLENDİRME

Cevaplarınızı cevap anahtarıyla karşılaştırınız. Yanlış cevap verdiğiniz ya da cevap verirken tereddüt ettiğiniz sorularla ilgili konuları faaliyete geri dönerek tekrarlayınız. Cevaplarınızın tümü doğru ise bir sonraki öğrenme faaliyetine geçiniz.

ÖĞRENME FAALİYETİ-3

AMAÇ

Bir ağda, ağ yönlendirme elemanlarını tanıyarak ve görevlerinin ne olduğunu öğrenerek IP yönlendirme işlemini yapabileceksiniz.

ARAŞTIRMA

- Okulunuzda IP yönlendirme cihazı olup olmadığını araştırınız.
- Yönlendirici olarak kullanılan cihazın çalışma prensibini araştırınız.
- Yerel bir ağda bütün bilgisayarların internete bağlanabilmesi için IP yönlendirme cihazları kullanmak gerekli midir? Araştırınız.

3. IP YÖNLENDİRME

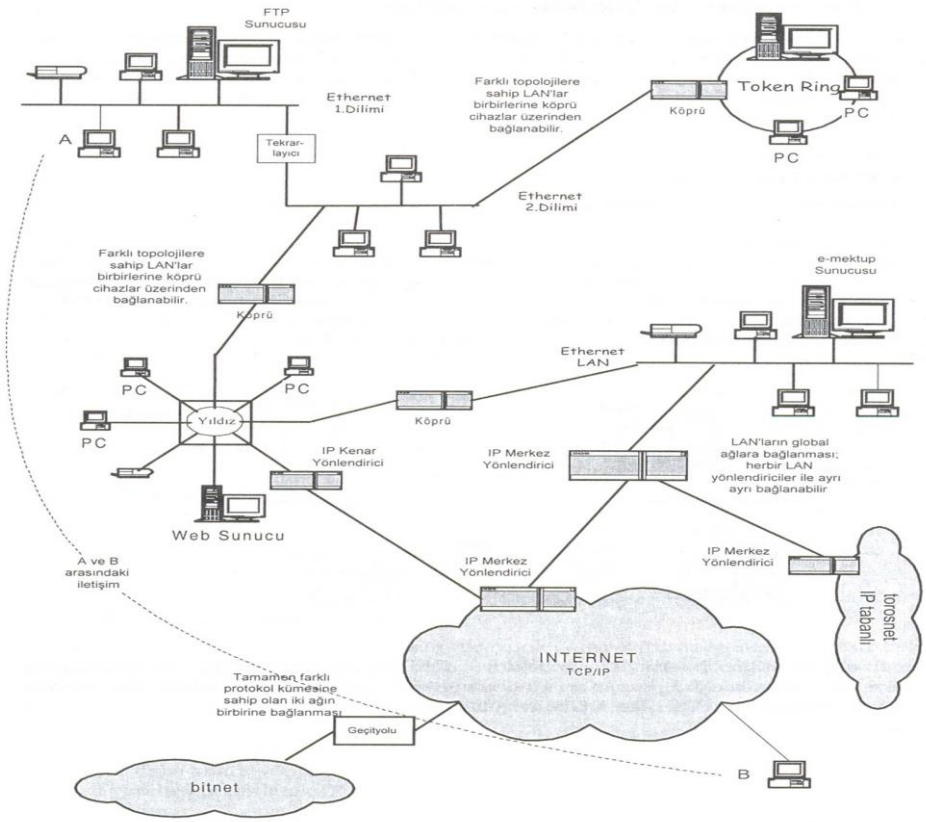
IP yönlendirme, TCP/IP ağlarının bel kemiği denilebilir. Ağlar arası IP paket aktarımı, paketlerin en uygun yolları takip ederek bilgisayar sistemleri arasında gidip gelmesi IP yönlendirme tarafından gerçekleştirilir. Yönlendirme görevi, temel olarak yönlendiriciler ve geçit yolu cihazlarına bırakılmıştır. Komple ağ oluşturulmasında, bağlantı/geçit noktası konumuna sahip bu cihazların başarısı ve yönlendirmede kullandıkları algoritmalar göz önüne alınması gereken önemli unsurlardır.

Yalın (tek segmentli) bir TCP/IP ağda IP yönlendirmeye o kadar gerek yoktur. Sistemlere yalnızca IP adresi ve ağ maskesinin ayarlarının yapılması yeterli olur çünkü bütün aktarım LAN içerisinde kalmaktadır. Ancak bir ağ, birkaç tane LAN'ın birleşmesinden oluşmuşsa veya internet gibi global bir ağa bağlıysa sistemlere yerleştirilen IP bilgilerine ek olarak yönlendirme bilgileri de verilmelidir.

Yönlendirme işinin gerçekleştirilmesi için sistemler üzerinde yönlendirme tablosu (routing table) tutulur. Bu tablo, gönderilecek veri paketlerinin alıcısına ulaşması için hangi yolun izleneceğini belirten yönlendirme bilgilerini tutar. Bu bilgiler, ya ağ yöneticisi (network administrator) tarafından elle verilir ya da kullanılan yönlendirme algoritmasınca doldurulur ve güncellenir.

3.1. Bir Ağda Yönlendirme

Yerel bir ağ olan LAN üzerinde yönlendirme işi kolayca yapılır. Bu tür ağlarda yapılması gereken, sistemlere TCP/IP'nin yüklenmesi ve sistemlere atanacak IP adresi ile ağ maskesinin ayarlarının yapılması yeterlidir.



Şekil 3.1: Geniş bir ağın uygulamadaki topolojisi

Eğer mevcut ağ Şekil 3.1'deki gibi ise yönlendirme işleri biraz karışır. Şekilde internet, Bitnet, torosnet gibi üç tane geniş alan ağı (WAN) ve farklı topolojilere sahip dört tane de LAN görülmektedir. Bu bağlantı şekli, aslında var olan uygulamanın bir kesitidir denilebilir. Şekildeki LAN'lar herhangi bir kurumdaki LAN'lar olabilir.

Şekil 3.1'e bakıldığında farklı topolojilere sahip LAN'ların birbirine köprü cihazlar ile bağlandığı ve daha sonra iki ayrı noktadan yönlendirici ile internet ve bitnet ağlarına bağlandığı görülür.

Genel olarak bir IP paketi, alıcısına ulaşıncaya kadar birçok noktadan geçer. Her nokta, gelen veri paketi kendisine ait değilse onu alıcısına ulaşacak biçimde doğru yönlendirmelidir. Bunun için yönlendirme görevi yapılan her noktada, yönlendirme parametrelerine bakılarak gelen veri paketleri ileriye doğru aktarılır.

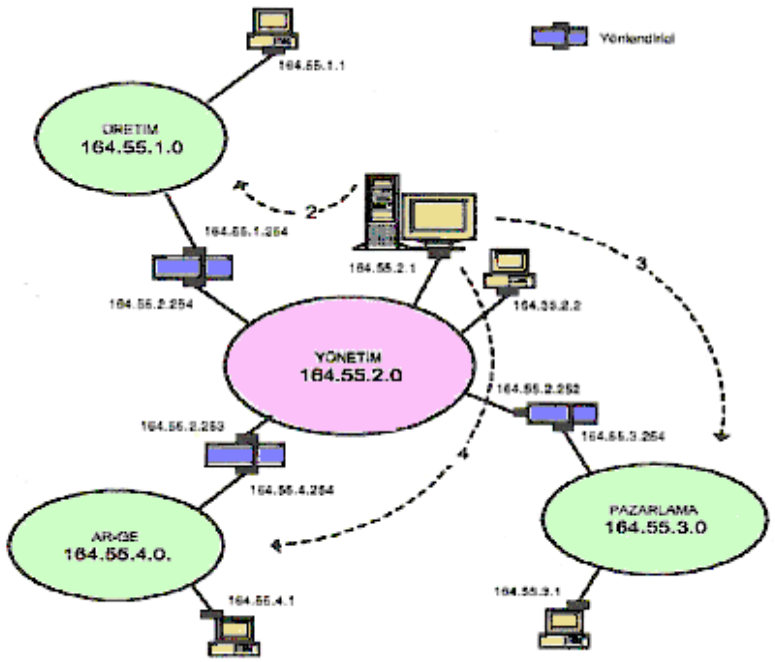
3.2. Yönlendirici Cihazlar İçin Ip Bilgisi

İnternet üzerinde büyüklü küçüklü binlerce IP yönlendirici cihazlar vardır. Küçük bir yerel ağdaki bilgisayarların internete girebilmesi için IP yönlendiricili cihazlar kullanılır. Ağ üzerindeki IP yönlendiriciler, internetin temel çatısını oluşturur ve minimum IP bilgisine ek

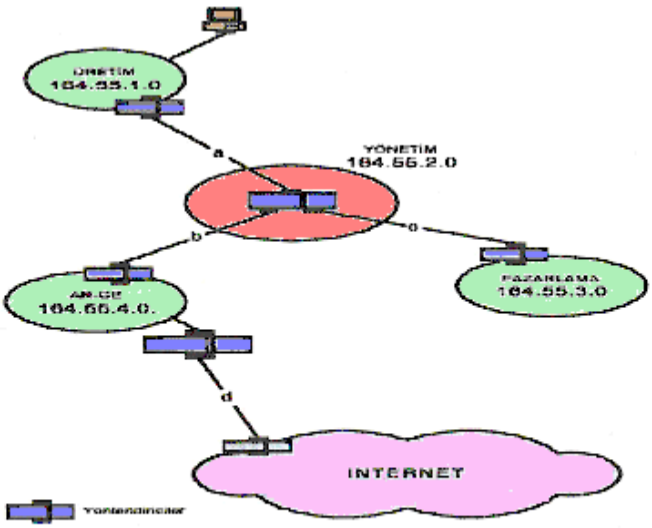
olarak başka bilgilerin yerleştirilmesine gerek duyar. Minimum IP bilgisi yönlendirici için gerekli şarttır ancak bu yeterli değildir. Çünkü IP bilgisi yönlendiricinin ağa eklenmesini yani ona ağ üzerinden erişilmesini sağlar ancak onun asıl işlevi olan yönlendirme görevini yerine getirmesini sağlamaz. Yönlendiricilere minumum IP bilgisi dışında WAN portu kurulumu için gerekli parametreler ve hangi yönlendirme algoritmasının yapılacağı bilgisi verilmektedir.

3.3. IP Yönlendirme Cihazları ve Yönlendirme

Birbirinden bağımsız LAN'ların birbiriyle iletişim kurabilmesi için IP yönlendirici (router) cihazlar kullanılır. LAN'lar birbirine çok yakınsa Şekil 3.2'de olduğu gibi aynı yönlendirici cihazın LAN portları üzerinden bağlanabilir. Ancak uzak iseler Şekil 3.3'te görüldüğü gibi her LAN tarafına bir yönlendirici koyulur veya var olan yönlendiricinin diğer WAN portu üzerinden bağlantı yapılır. Bu durumda yönlendiriciler arasındaki bağlantılar da birer alt ağ gibi davranır.



Şekil 3.2: Sistemlerin örnek ağdaki konumları



Şekil 3.3: Örnek ağın internete bağlantısı

IP yönlendirici cihazlar kendilerine gelen paketleri, paket başlığı içerisindeki alıcı adres kısmına ve kendinde tanımlı ağ maskesi değerine bakarak gitmesi gereken ilgili porta aktarır. Yönlendiriciler tekil olarak IP adresinin kendisiyle değil de ağ adresiyle ilgilenir.

Yönlendirici, yalnızca bir LAN'ı bağlayan bir kenar yönlendirici ise fazla karmaşa yoktur. Ancak merkez yönlendiricilerde birçok port vardır. Yönlendirme tablosu oldukça dolu ve karmaşık olabilir. Örneğin, paket başlığındaki alıcı IP adresi ile kendine girilmiş olan ağ maskeleri işleme sokulduğunda aynı paket için birden çok alıcı portu çıkabilir. Bu durumda hangi porta yönlendirme yapacağı, en uzun uyuşma gösteren algoritmaya göre belirlenir yani en küçük alt ağa yönlendirme yapılır. Bundan dolayı karmaşık yönlendirme tabloları düzenlenirken dikkatli olunmalıdır. Aksi durumda bazı IP adreslerine ulaşılmıyor olabilir.

UYGULAMA FAALİYETİ

IP adreslerini tespit edip gerekli yönlendirmeleri yapınız.

İşlem Basamakları	Öneriler
➢ IP yönlendirmesine ihtiyaç duyulan elemanları belirleyiniz. ➢ IP adreslerini tespit ediniz. ➢ Gerekli yazılım ayarlarını yapınız.	➢ IP yönlendirici cihazların ayarlarına dikkat ediniz. ➢ IP yönlendirme cihazlarının çalışmasını etkileyecek komut veya komutları kullanırken dikkat ediniz.

KONTROL LİSTESİ

Bu faaliyet kapsamında aşağıda listelenen davranışlardan kazandığınız beceriler için **Evet**, kazanamadığınız beceriler için **Hayır** kutucuğuna (X) işareti koyarak kendinizi değerlendiriniz.

Değerlendirme Ölçütleri	Evet	Hayır
1. IP yönlendirmesine ihtiyaç duyulan elemanları belirleyebildiniz mi?		
2. IP adreslerini tespit ettiniz mi?		
3. Gerekli yazılım ayarlarını yapabildiniz mi?		

DEĞERLENDİRME

Değerlendirme sonunda "**Hayır**" şeklindeki cevaplarınızı bir daha gözden geçiriniz. Kendinizi yeterli görmüyorsanız, öğrenme faaliyetini tekrar ediniz. Bütün cevaplarınız "**Evet**" ise "Ölçme ve Değerlendirme"ye geçiniz.

ÖLÇME VE DEĞERLENDİRME

Aşağıdaki cümlelerin başında boş bırakılan parantezlere, cümlelerde verilen bilgiler doğru ise D, yanlış ise Y yazınız.

1. ( ) Ağlar arası yönlendirmeler IP yönlendirme cihazları tarafından yapılır.

2. ( ) Birbirinden bağımsız yerel ağlar iletişim kurabilmek için IP yönlendiricili (router) cihazlar kullanır.

3. ( ) IP yönlendiricili cihazların IP değerleri sabittir, değiştirilemez.

4. ( ) IP yönlendirmenin amacı ağlar arası IP paket aktarımı, paketlerin en uygun yolları takip ederek bilgisayar sistemleri arasında gidip gelmesini sağlar.

5. Gönderilecek veri paketlerinin alıcısına ulaşması için hangi yolun izleneceğini belirten yönlendirme bilgilerini tutan tabloya .... denir.

DEĞERLENDİRME

Cevaplarınızı cevap anahtarıyla karşılaştırınız. Yanlış cevap verdiğiniz ya da cevap verirken tereddüt ettiğiniz sorularla ilgili konuları faaliyete geri dönerek tekrarlayınız. Cevaplarınızın tümü doğru ise bir sonraki öğrenme faaliyetine geçiniz.

ÖĞRENME FAALİYETİ-4

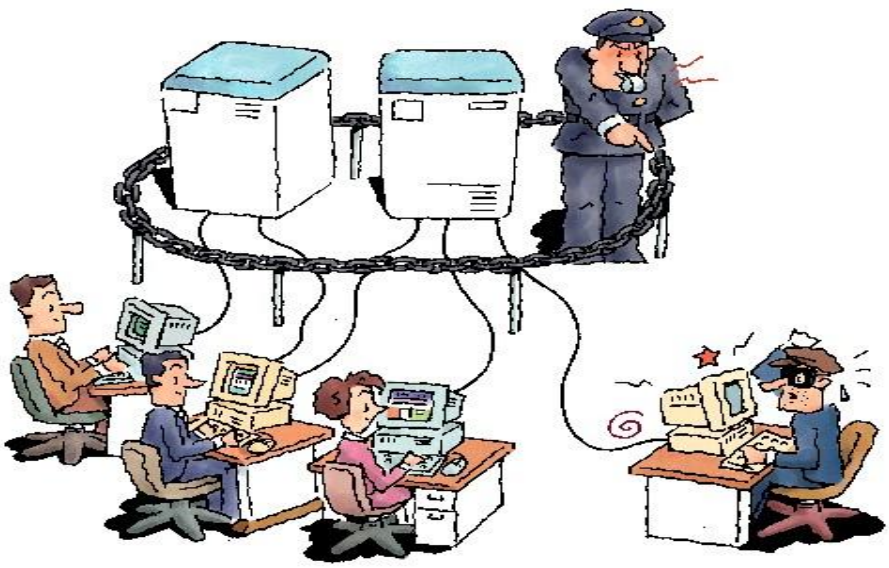
AMAÇ

Ağ güvenlik düzeylerini tanıyarak ağ güvenliği ile ilgili tanımlamaları yapabileceksiniz.

ARAŞTIRMA

- Sizce neden ağ güvenliği olmalıdır? Araştırınız.
- Çevrenizde veya okulunuzda bulunan ağ sisteminin güvenliği nasıl sağlanmaktadır? Araştırınız.
- Günümüzde kullanılan işletim sistemleri, yerel ağlardan veya internet ortamından gelebilecek saldırılara karşı ne kadar güvendedir? Araştırınız.

4. AĞ GÜVENLİĞİ



Resim 4.1: Bir zincir ancak en zayıf halkası kadar güçlüdür.

Günümüzde bilgisayar ağlarından beklenen hizmet ve hizmet kalitesi her geçen gün artmaktadır. Bilgisayarların birbiriyle iletişim kurabilmesi, birbiriyle veri alışverişinde bulunması bilgisayar ağlarından beklenmektedir. Bu nedenle kurum ve kuruluşlar kendi bünyesinde ağ oluşturmakta, internet gibi büyük bir ağa bağlanmaktadır. Artık günümüzde büyük ya da küçük bilgisayar ağları kurulmakta, tek bir cihaz yardımıyla da internet dünyasına tüm bilgisayarlar giriş yapmaktadır. Durum böyle olunca da veri alışverişinde, dosya paylaşımında bulunurken özel bilgilerimizin diğer kullanıcıların eline geçmisine istemeyiz. Bundan dolayı kurum ve kuruluşlar, ağlarının güvenliğini sağlamak zorunda kalmıştır. Bu bölümde ağ güvenliğinin nasıl sağlandığı ve ne gibi ayarlamalar yapıldığı açıklanacaktır.

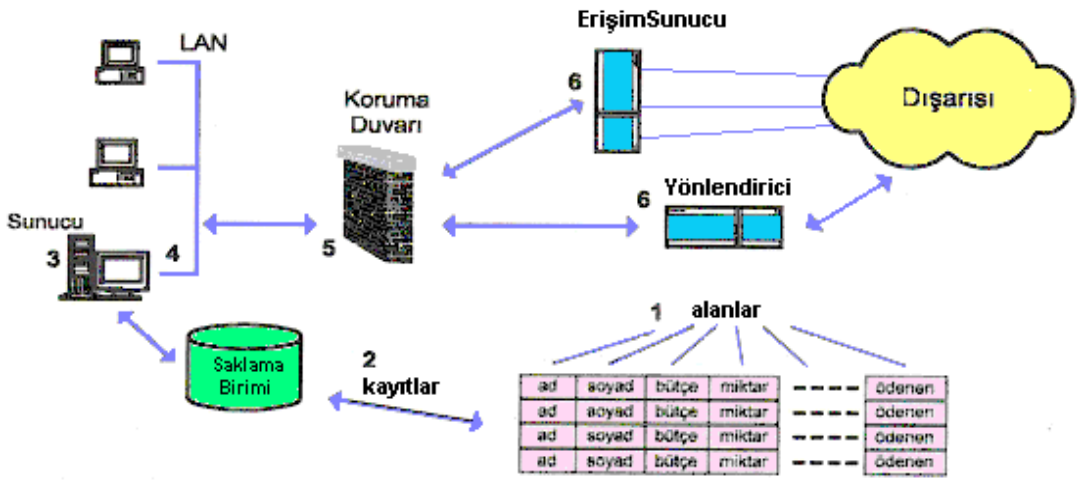
İnternetin gelişmesiyle beraber ağ uygulaması da beklenmedik şekilde genişlemiştir. Bu gelişmeye paralel olarak ağ kurulup çalıştırıldıktan sonra ağ yönetimi ve ağ güvenliği büyük önem kazanmıştır. Artık bilgisayar ağları değerlendirilirken ağ perfonmansı ile ağ güvenliği ölçüt alınmıştır.

4.1. Güvenlik Düzeyleri

Güvenlik düzeyi, özel bir bilginin saklı olduğu yerde hangi düzeyde korunacağını gösterir. Ağ ortamındaki bilgisayarlarda bilgi çeşitli düzeylerde korunabilir. Meselâ, bir veri tabanına ait veri kaydının belirli alanlar şifrelenerek o bilgilere erişilmesi denetim altına alınabilir. Böylece koruma altına alınan alanlara sadece erişim hakkı olanlar veya şifreyi bilenler erişebilir.

Güvenlik Düzeyleri		Görevi
1.	Kayıt alanı düzeyinde koruma	Bu düzeyler en sıkı korumayı sağlar. İyi bir şifreleme ve şifre anahtarı üretme algoritması kullanılmaktadır.
2.	Veri kaydı düzeyinde koruma	
3.	Uygulama programı düzeyinde sorgulama/koruma	Uygulama programına girişi sorgular.
4.	Bilgisayara bağlanmayı sorgulama	Bilgisayar sistemine girişi denetler.
5.	Ağ kaynaklarını hizmet türleri açısından koruma	Ağa dışarıdan bağlanmayı ve ağ üzerinde sunulan hizmetlere erişimi denetler. Bu güvenlik düzeyleri genel olarak koruma duvarları (firewall) tarafından sağlanır.
6.	Ağa girişi sorgulama/koruma	

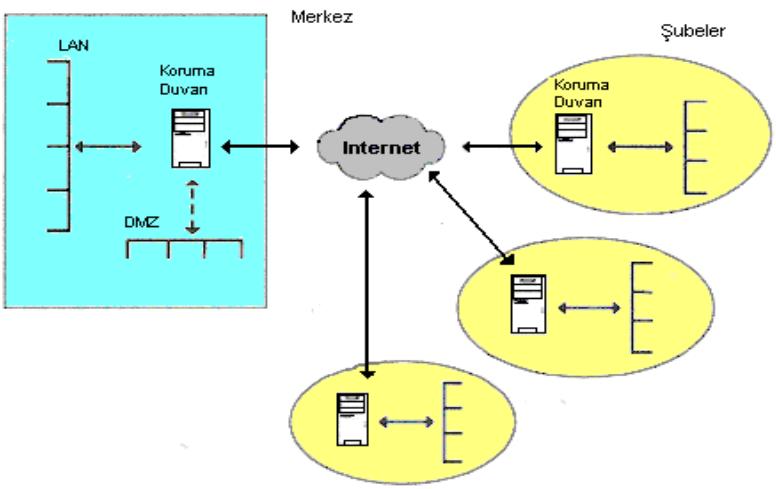
Tablo 4.1: Güvenlik Düzeyleri ve Görevleri



Şekil 4.1: Güvenlik düzeyleri

4.2. Özel Sanal Ağlar (VPN)

Özel sanal ağ, kişi veya kurumlara ait olan özel bilgi ve verinin herkese açık hâle getirilmesini ya da internet gibi büyük bir ağ üzerinden bilgi ve verilerin aktarılmasını sağlar. Büyük kurum ve kuruluşlar uzak yerdeki birimleri ile iletişimi internet üzerinden özel bir sanal ağ oluşturarak sağlar. Şekil 4.2'de bir kurumun merkezi ile şubeleri arasındaki bağlantının internet üzerinden gerçekleştirilmesi görülmektedir.



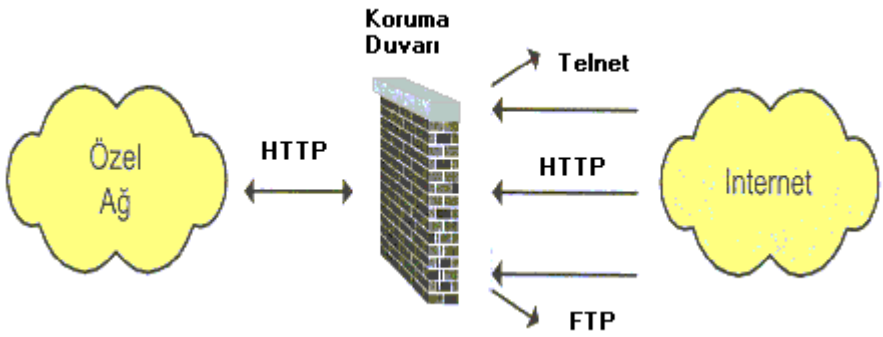
Şekil 4.2: İnternet üzerinden sanal özel ağ (VPN) oluşturulması

Şekil 4.2'de görüldüğü gibi merkez ve şubelerin internete çıkışlarında birer güvenlik duvarı vardır. Bu güvenlik duvarlarının işlevi, iletişim yapılacak noktalar arasında tünel oluşturmasıdır. Bu tünel üzerinden, özel bilgi ve veri internete çıkarılmadan önce şifrelenir ve gelen şifrelenmiş paketlerden gerçek veri elde edilir. Dolayısıyla VPN uygulamasında en önemli konu, aktarılacak bilgi ve verinin şifrelenmesidir.

Özel sanal ağ uygulamasında biri kullanıcı-geçit yolu, diğeri geçit yolu-geçit yolu olarak adlandırılan iki tür bağlantı yapılır. Kullanıcı-geçit yolu bağlantısında doğrudan kullanıcı bilgisayarı ile geçit yolu arasında şifrelenmiş tünel kurulur. Kullanıcı tarafından yüklü olan yazılım gönderme işleminde, kullanıcı önce veriyi şifreler ve VPN üzerinden alıcı taraftaki geçit yoluna gönderir. Geçit yolu, önce kullanıcının geçerli biri olup olmadığını sorgular ve gönderilen şifrelenmiş paketi çözerek korunmuş alandaki alıcıya gönderir. Alıcının verdiği cevap da yine önce geçit yoluna gider ve orada şifrelenerek kullanıcıya gönderilir. Geçit yolu-geçit yolu bağlantısında Şekil 4.2'de görüldüğü gibi birbiriyle iletişimde bulunacak sistemler, kendi taraflarında bulunan geçit yoluna başvurur. Kullanıcı sistemleri, verilerini geçit yollarına gönderir ve onlar kendi aralarında şifreli olarak iletişimde bulunur. Bu durum farklı yerlerdeki LAN'ların internet gibi herkese açık ağ üzerinden güvenli bir şekilde bağlanması için kullanılır.

4.3. Güvenlik Duvarı (Firewall)

Bir ağ diğer ağların ve internet gibi büyük bir ağın erişimine açık ise o ağdaki gizli bilgiler güvende değildir. Her an paylaşmak istemediğimiz bilgilerimiz başkalarının eline geçebilir. İşte, bu noktada ağın güvenliğini sağlamak için ağın giriş ve çıkış noktasına güvenlik duvarı (firewall) koyulması gerekir. Güvenlik duvarı ağ yöneticisine tüm ağa olan erişimlerin bir noktadan denetlenmesi imkânı sağlar. Böylece bilgilerimiz daha güvende olur ve dışarıdan gelecek saldırılara karşı da bir tedbir alınmış olur.



Şekil 4.3: Güvenlik duvarı

Yazılım ve donanım tabanlı olarak geliştirilebilen güvenlik duvarları genel olarak aşağıdaki görevleri yerine getirir:

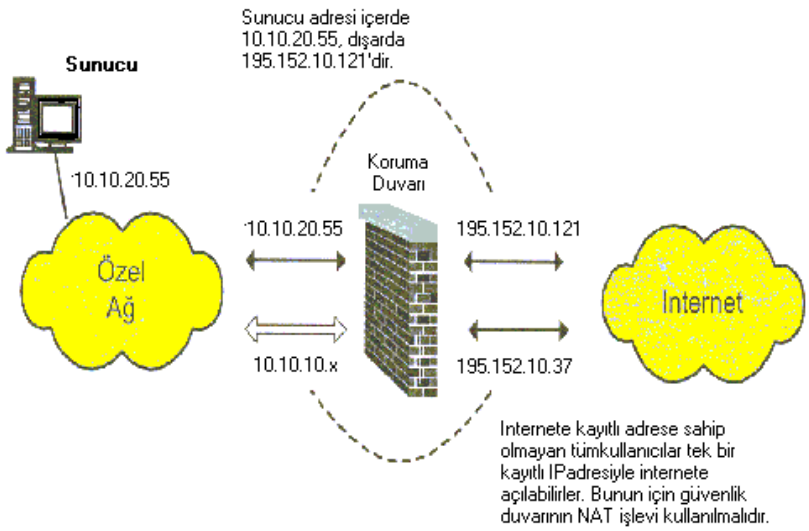
- Kullanıcı sınırlaması yapılır.
- Ağ içi erişim ve ağ dışı erişim kısıtlaması ve gözlenmesini sağlar.

- Bilginin şifrelenmesini sağlar.
- Sanal özel ağ oluşturur.
- Ağın dışarıdan gizlenmesi sağlar.

Güvenlik duvarı, özel ağ ile internet arasına konan ve istenmeyen erişimleri engelleyen bir sistemdir. Bu sistemle ağ güvenliği tam olarak sağlanır ve erişim hakları düzenlenebilir. Ancak güvenlik duvarı kurulurken dikkat edilmesi ve göz önüne alınması gereken bazı noktalar vardır. Bunlardan en önemlisi güvenlik duvarının belirli bir stratejiye göre hazırlanmasıdır. Güvenlik duvarı kurulmadan önce ne tür bilgilerin korunacağı, ne derecede bir güvenlik uygulanacağı ve kullanılacak güvenlik algoritmaları önceden belirlenmelidir.

Güvenlik duvarının sistem üzerinde tam olarak etkili olabilmesi için ağ ortamı ile internet arasındaki tüm trafiğin güvenlik duvarı üzerinden geçirilmesi gerekir.

Güvenlik duvarlarının tercih edilmesinin en büyük sebeplerinden biri de adres dönüşüm (NAT, Network Adres Translation) özelliğidir. Sadece tek bir IP adresi ile tüm ağ kullanıcıları internete çıkabilir ve yerel ağ ortamındaki IP adresleri tamamen internet ortamından yalıtılmış şekilde kullanılabilir. Böylece herhangi bir ISS (İnternet Servis Sağlayıcı) değişikliğinde iç IP adresleri değişikliğine gerek kalmaz.



Şekil 4.4: NAT işlevi açısından güvenlik duvarı

4.3.1. Kısıtlama–İzin Verme

Bir güvenlik duvarının getireceği kısıtlama ve izin verme, uygulanacak ağa göre düşünülmelidir. Kısıtlamada yani engellemede belirli hizmetler dışında tüm sistem erişimi engellenir. İzin verme yani serbest bırakmada ise belirli hizmetler dışında tüm sistem erişiminin serbest bırakılır. Bu şekilde güvenlik duvarı ile ağ erişimlerine kısıtlama ve izin verme işlemi yapılır.

4.3.2. Güvenlik Duvarı Türleri

Güvenlik duvarı tasarımı için çeşitli teknikler vardır. Kullanılan güvenlik duvarı tekniği güvenlik duvarının türünü belirtir. Güvenlik duvarı türleri şunlardır:

- Paket süzmeli güvenlik duvar (Packet-filtering firewall)
- Devre düzeyli geçit yolu (Circuit-level gateway)
- Uygulama düzeyli geçit yolu (Application-level gateway)

4.3.2.1. Paket Süzmeli Güvenlik Duvarı (PFFW)

Güvenlik duvarı oluşturmanın en kolay yollarından birisidir. Veri paketlerinin başlık alanı içindeki bilgilerine bakarak kontrol edip istenmeyen paketleri karşı tarafa geçirmez. Bu amaçla bir kurallar tablosu oluşturulur. Bu tabloda belirtilen kurallara uymayan paketler karşı tarafa geçirilmeyip süzülür. Belirli bir düzeyde koruma sağlayan bir güvenlik duvarıdır. Ancak bazı durumlarda çok sıkı bir koruma sağlayamaz. Ağlarda IP yönlendiriciler, paket süzmeli güvenlik duvarı yeteneğini desteklemektedir.

Paket süzmeli güvenlik duvarları OSI başvuru modeline göre 3. katman olan ağ katmanında çalışır. Bundan dolayı bu tür güvenlik duvarları 3. seviye güvenlik duvarı olarak söylenir. Dolayısıyla bu tür güvenlik duvarı oluşturmanın en kolay yolu konfigüre edilebilir bir yönlendirici kullanmaktır. Bilindiği gibi yönlendiriciler, yönlendirme işlemini ağlar arası ortam içinde gelen paketlerin alıcı ve gönderici adreslerine bakarak yapar. Paket süzmeli güvenlik duvarları da benzer yapıda çalışır. Gelen paketler başlık alanı içerisindeki bilgilere bakılarak analiz edilir, ona göre geçirilir veya atılır.

Tüm IP yönlendiriciler paket süzmeli güvenlik duvarı yeteneğini desteklemektedir. Bu yetenek ya yönlendiriciyle beraber hazır olarak gelir ya da daha sonra yazılım güncellemesi yapılarak yönlendiriciye yüklenir.

- **Belirli Servise Bağlı PFFW**

Paket süzmeli güvenlik duvarı kullanılan algoritmaya göre çalışır. Bu güvenlik duvarı sadece belirli bir hizmet portu üzerinden işlem yapar. TELNET sunucu sistemi uzak bağlantıları 23. TCP portundan, SMTP sunucu sistemi ise 25.TCP portu üzerinden dinleme işlemi yapar. Bu sistemde izin verilmiş olan ana makine listesi bulunur. Bu listede bulunan ana makinelere uygun port numarasıyla gelen paketlere geçiş izni verilir. Diğerlerinin geçişi engellenir.

- **PFFW İçin Değerlendirme**

Karmaşık bir süzgeçleme kullanılacaksa kurulum işlemi gittikçe zorlaşır. Genellikle süzgeçleme arttıkça yönlendirici üzerinden geçen paket sayısı azalır. Yönlendirici güvenlik duvarı işlevini yerine getirirken kendi görevi yanında yani paketin başlık bilgisini yönlendirme tablosunda arama işlemi yanında süzme işlemlerini de o pakete uygulamalıdır. Bu durumda süzme yapmak için yönlendiricinin işlemciyi (CPU) kullanması gerekir. Bu da performansta bir düşüklüğe yol açabilir.

PFWR kullanımında IP paketleri seviyesinde erişim denetimi yapıldığından ve uygulama seviyesine çıkılamadığından güvenlik bazı uygulamalar için yetersiz kalabilir.

4.3.2.2. Devre Düzeyli Geçit Yolu (Circuit Level Gateway)

OSI başvuru modelinin 4. katmanı olan oturum katmanı düzeyinde çalışır. Özel ağın güvenliği için arada vekil sistem kullanılır. Paket süzmeli güvenlik duvarına göre daha sıkı koruma sağlar. Oturum kurulurken ilgili port sorgulamaları yapılır ve oturum açıldıktan sonra o portu, oturumun kurulmasını başlatan taraf sonlandırıncaya kadar sürekli açık tutar. Bu koruma duvarında oturum bir kez kabul edilip kurulduktan sonra her paket için denetim yapılmaz. En önemli özelliği iç kullanıcı ile dış bir sunucu arasında doğrudan bağlantı olmamasıdır. Özel ağın yapısını dışarıya karşı iyi korur.

4.3.2.3. Uygulama Düzeyli Geçit Yolu (Application Level Gateways)

Uygulama düzeyli geçit yolları en sıkı koruma sağlayan güvenlik duvarı tekniğidir. OSI başvuru modeline göre uygulama katmanı düzeyinde çalışır. Böylelikle tam denetim yapma imkânı sunar. Genel olarak güçlü bir iş istasyonu üzerine yüklenen yazılımla gerçekleşir. Bu tür geçit yolları devre düzeyli geçit yollarına benzer. Ancak oturum açıldıktan sonra bile paketlerin sınaması yapılır. Bu da beklenmedik saldırılara karşı korumayı kuvvetlendirir.

Bu yöntem, ağ yöneticisine paket süzmeli ve devre düzeyli geçit yoluna göre daha güvenli, daha sıkı bir koruma sağlama imkânı verir. İstenen programların çalışmasına izin verilirken yasak olanlar engellenir. Bu tür güvenlik duvarı kullanılması durumunda ağ yöneticisine büyük bir sorumluluk düşer. Bu sorumlulukları yerine getirmek için ağ yöneticisi gerekli kurulumları kendisi yapmalıdır.

Uygulama düzeyli geçit yolunda, kabul edilecek veya kabul edilmeyecek kuralları içeren bir tablo oluşturulur. Bu tablo üzerindeki bir kurala uyan ve geçme hakkı elde eden paketler karşı tarafa geçirilir. Aksi durumda bu paketlerin geçişleri engellenir.

UYGULAMA FAALİYETİ

İstenen güvenlik ayarlamalarını yazılım aracılığıyla yapınız.

İşlem Basamakları	Öneriler
➢ Ağ sistemi için kullanılacak güvenlik seviyesini tespit ediniz. ➢ Güvenlik yazılımını sisteme yükleyiniz. ➢ İstenen güvenlik ayarlamalarını yazılım aracılığıyla yapınız.	➢ Güvenlik duvarını (firewall) oluştururken ağ sisteminin çalışmasını etkileyecek komut ya da komutları kullanırken dikkat ediniz. ➢ Enerji ile çalışan donanım parçalarının gerilimlerine dikkat ediniz.

KONTROL LİSTESİ

Bu faaliyet kapsamında aşağıda listelenen davranışlardan kazandığınız beceriler için **Evet**, kazanamadığınız beceriler için **Hayır** kutucuğuna (X) işareti koyarak kendinizi değerlendiriniz.

Değerlendirme Ölçütleri	Evet	Hayır
1. Ağ sistemi için kullanılacak güvenlik seviyesini tespit edebildiniz mi?		
2. Güvenlik yazılımını sisteme yükleyebildiniz mi?		
3. İstenen güvenlik ayarlamalarını yazılım aracılığıyla yapabildiniz mi?		

DEĞERLENDİRME

Değerlendirme sonunda **"Hayır"** şeklindeki cevaplarınızı bir daha gözden geçiriniz. Kendinizi yeterli görmüyorsanız, öğrenme faaliyetini tekrar ediniz. Bütün cevaplarınız **"Evet"** ise "Ölçme ve Değerlendirme"ye geçiniz.

ÖLÇME VE DEĞERLENDİRME

Aşağıdaki cümlelerin başında boş bırakılan parantezlere, cümlelerde verilen bilgiler doğru ise D, yanlış ise Y yazınız.

1. ( ) Kayıt alanı düzeyinde koruma en sıkı korumadır.
2. ( ) Güvenlik duvarı (firewall) ağa dışarıdan bağlanmayı ve ağ üzerinde sunulan hizmetlere erişimi denetler.
3. ( ) Özel sanal ağ (Virtual Private Networks) kişi ve kurumlara ait olan özel bilgi ve verileri paylaşıma açmaz.
4. ( ) Güvenlik duvarı (firewall) ile ağ erişimlerine kısıtlama ve izin verme işlemi yapılır.
5. ( ) Güvenlik duvarı (firewall) kullanıcı sınırlaması yapmaz.

DEĞERLENDİRME

Cevaplarınızı cevap anahtarıyla karşılaştırınız. Yanlış cevap verdiğiniz ya da cevap verirken tereddüt ettiğiniz sorularla ilgili konuları faaliyete geri dönerek tekrarlayınız. Cevaplarınızın tümü doğru ise "Modül Değerlendirme"ye geçiniz.

MODÜL DEĞERLENDİRME

Aşağıdaki soruları dikkatlice okuyunuz ve doğru seçeneği işaretleyiniz.

1. Aşağıdakilerden hangisi DNS protokolünün görevidir?
A) Host isimlerini IP adresine çevirir.
B) Göndericinin ve alıcının IP adresini tutar.
C) Veri aktarılmasını sağlar.
D) Bir üst katmandan gelen veriyi uygun uzunlukta parçalara ayırır.

2. Aşağıdakilerden hangisi DHCP protokolü tarafından dağıtılmaz?
A) IP adresi B) Subnet maskesi C) DNS sunucu adresi D) Host ismi

3. Aşağıdaki protokollerden hangisi ağ içerisinde elektronik mektup alışverişini sağlar?
A) HTTP B) SMTP C) ICMP D) TCP

4. Aşağıdaki eşleştirmelerden hangisi yanlıştır?
A) edu→ Eğitim kurumları
B) com→ Ticari kuruluşlar
C) mil→ Askeri kurumlar
D) gov→ Ticari olmayan hükümete de bağlı olmayan kurumlar

5. İnternet üzerinde dosya aktarımı yapmak için kullanılan protokol aşağıdakilerden hangisidir?
A) TELNET B) SNMP C) FTP D) WINS

6. Aşağıdakilerden hangisi ulaşım katmanı protokollerindendir?
A) IP-ICMP B) TCP-UDP C) HTTP D) DNS

7. Aşağıdakilerden hangisi Ethernet kartında bulunan, değiştirilemeyen bir adrestir?
A) ARP B) UDP C) MAC D) WINS

8. Aşağıdakilerden hangisi TCP/IP mimarisi katmanlarından değildir?
A) Sunum B) Uygulama C) Ulaşım D) Fiziksel

9. 1100 0011.1000 0110.0100 0011.1100 1000 IP adresi aşağıdakilerden hangisidir?
A) 195.134.67.200 C)192.143.0.25
B) 212.45.142.131 D) 24.124.1.56

10. 130.15.1.5 hangi sınıf IP adresidir?
A) A sınıfı B) B sınıfı C) C sınıfı D) D sınıfı

11. IP adresi 192.128.63.50, altağ maskesi 255.255.255.0 ise ağ adresi aşağıdakilerden hangisidir?
A) 192.0.0.0 B) 123.4.53.50 C) 192.128.63.0 D) 123.4.0.0

12. 132.45.53.4 ve 132.45.78.123 IP adreslerine sahip bilgisayarlar için aşağıda verilenlerden hangisi doğrudur?

A) İkisi de farklı ağlarda oldukları için router ile iletişime geçer.
B) Aynı ağda oldukları için doğrudan iletişime geçer.
C) Bilgisayarlar birbiri ile bilgi alışverişi yapamaz.
D) Her iki IP adresi C sınıfı IP adresidir.

13. Aşağıdakilerden hangisi alt ağ maskesinin görevidir?

A) Bilgisayarlar arası veri alışverişini sağlar.
B) Bilgisayarlara IP numarası verir.
C) D ve E sınıfı IP adresleri için tasarlanmıştır.
D) Bilgisayarların ağ tanımlayıcılarını bulmayı sağlar.

Aşağıdaki cümlelerin başında boş bırakılan parantezlere, cümlelerde verilen bilgiler doğru ise D, yanlış ise Y yazınız.

14. ( ) Birbirinden bağımsız yerel ağlar iletişim kurabilmek için IP yönlendiricili (router) cihazlar kullanır.
15. ( ) IP yönlendiricili cihazların IP değerleri sabittir, değiştirilemez.
16. ( ) Kayıt alanı düzeyinde koruma en sıkı korumadır.
17. ( ) Güvenlik duvarı (firewall) ağa dışarıdan bağlanmayı ve ağ üzerinde sunulan hizmetlere erişimi denetler.
18. ( ) Özel sanal ağ (Virtual Private Networks) kişi ve kurumlara ait olan özel bilgi ve verileri paylaşıma açmaz.
19. ( ) Güvenlik duvarı (firewall) ile ağ erişimlerine kısıtlama ve izin verme işlemi yapılır.
20. ( ) IP yönlendirmenin amacı ağlar arası IP paket aktarımı, paketlerin en uygun yolları takip ederek bilgisayar sistemleri arasında gidip gelmesini sağlar

CEVAP ANAHTARLARI

ÖĞRENME FAALİYETİ-1'İN CEVAP ANAHTARI

1	**A**
2	**D**
3	**B**
4	**D**
5	**C**
6	**B**
7	**C**
8	**A**

ÖĞRENME FAALİYETİ-2'NİN CEVAP ANAHTARI

1	**A**
2	**B**
3	**C**
4	**B**
5	**D**

ÖĞRENME FAALİYETİ-3'ÜN CEVAP ANAHTARI

1	**Doğru**
2	**Doğru**
3	**Doğru**
4	**Doğru**
5	**Yönlendirme Tablosu**

ÖĞRENME FAALİYETİ-4'ÜN CEVAP ANAHTARI

1	**Doğru**
2	**Doğru**
3	**Yanlış**
4	**Doğru**
5	**Yanlış**

MODÜL DEĞERLENDİRMENİN CEVAP ANAHTARI

1	**A**
2	**D**
3	**B**
4	**D**
5	**C**
6	**B**
7	**C**
8	**A**
9	**A**
10	**B**
11	**C**
12	**B**
13	**D**
14	**Doğru**
15	**Doğru**
16	**Doğru**
17	**Doğru**
18	**Doğru**
19	**Yanlış**
20	**Doğru**

ÖNERİLEN KAYNAKLAR

- ÖRENCİK Bülent, Rıfat ÇÖLKESEN, **Bilgisayar Haberleşmesi ve Ağ Teknolojileri**, Papatya Yayıncılık, İstanbul, Ankara, İzmir, Adana, 2002.
- YILDIRIMOĞLU Murat, **TCP/IP ve İnternetin Evrensel Dili,** Pusula Yayıncılık, 2004.

KAYNAKÇA

- ÖRENCİK Bülent, Rıfat ÇÖLKESEN, **Bilgisayar Haberleşmesi ve Ağ Teknolojileri**, Papatya Yayıncılık, İstanbul, Ankara, İzmir, Adana, 2002.
- YILDIRIMOĞLU Murat, **TCP/IP ve İnternetin Evrensel Dili,** Pusula Yayıncılık, 2004.
- ÇÖLKESEN Rıfat, **Veri Yapıları ve Algoritmalar,** Papatya Yayıncılık, 2002.