T.C.
MİLLÎ EĞİTİM BAKANLIĞI

BİLİŞİM TEKNOLOJİLERİ

AĞ HİZMETLERİ

Ankara, 2014

- 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

ALAN	**Bilişim Teknolojileri**
DAL/MESLEK	**Ağ İşletmenliği**
MODÜLÜN ADI	**Ağ Hizmetleri**
MODÜLÜN TANIMI	Ağ referans modelleri, taşıma ve uygulama katmanındaki protokolleri kullanma becerilerinin kazandırıldığı bir öğrenme materyalidir.
SÜRE	40/32
ÖN KOŞUL	TCP/IP Protokolü modülünü başarmış olmak
YETERLİK	Ağ referans modellerini, taşıma ve uygulama katmanındaki protokolleri ve özelliklerini kullanmak
MODÜLÜN AMACI	**Genel Amaç** Bu modül ile gerekli ortam sağlandığındataşıma katmanındaki tehlikeleri sezebilecek, uygulama katmanı hizmetlerini amacına uygun kullanacak, en uygun ağ protokolünü seçebileceksiniz. **Amaçlar** **1.** Taşıma katmanı protokollerini kullanabileceksiniz. **2.** Uygulama katmanı uygulamalarını kullanabileceksiniz. **3.** Ağ referans modellerindeki katmanlar arasındaki ilişkiyi açıklayabileceksiniz.
EĞİTİM ÖĞRETİM ORTAMLARI VE DONANIMLARI	**Ortam:** Bilgisayar laboratuvarı **Donanım:** Yönlendirici, anahtarlayıcı, dağıtıcı, modem, köprü, bilgisayar, cihaz kılavuzları
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.

GİRİŞ

Sevgili Öğrenci,

Bilgisayarlar, geçmişten bugüne çok fazla yol alarak artık yaşamımızın her alanına girdi. Abaküs halindeki basit makineler, "şimdilerde ellerimizde taşıdığımız avuç içi bilgisayarlara dönüştü ve bilgisayarlar yaşamımızın ayrılmaz parçası haline geldi.

Gelişen bu iletişim ortamında haberleşme dışında bilgilerin de paylaşılması ihtiyacı oluştu. Nasıl insanların bir şeyler paylaşmak için birbirlerini arayıp konuşmaları gerekiyorsa bilgisayarların da işledikleri bilgileri paylaşmak için birbirleriyle iletişim kurmaları gerekiyor. Bilgisayarlar arasına, evlere bağlanan telefon kablolarına benzer kablolar bağlandı. Fakat bilgisayarlar nasıl konuşacaktı?

Nihayet bilgisayarların konuşup iletişim kurmaları için farklı iletişim metotları bulundu, bilgiler paylaşılmaya başlandı. Önceleri, kullandıkları sistemve dil birbirinden farklı olduğu için yalnızca aynı dili konuşan, aynı tip bilgisayarlar anlaşabiliyordu.

İnternet ortamında birçok bilgisayar var. Nasıl tüm dünyada İngilizce ortak dil olarak belirlenmişse farklı milletlerden insanlar anlaşabilmek için İngilizce konuşuyorsa farklı sistemler kullanan, farklı diller konuşan bilgisayarların da birbirleri ile iletişim kurmaları için ortak bir lisan geliştirildi. Böylece ellerimizde taşıdığımız küçük bilgisayarlardan devasa sunucu bilgisayarlara kadar hepsi haberleşebilir, hepsi bilgilerini paylaşabilir hale geldi. Artık çok güvenli banka sistemleri ile evlerimizde kullandığımız basit kişisel bilgisayarlar iletişim kurabiliyor, banka işlemlerimizi evimizin rahatlığında yapabiliyoruz.

İşte bu iletişim ortamını sağlayan ortak lisanın adı TCP/IP olarak belirlenmiş, bütün sistemlerde tanınmıştır. Bilgisayarlar iletişim kurarken bu dilin kurallarına göre konuşmak, bu dilin kurallarına göre iletişim kurmak zorundadır.

Bu modül sonunda bu dilin kuralarını ve nasıl konuşulduğunu, bilgisayarların birbirlerine bilgileri nasıl gönderdiğini, en çok kullandığınız e-postaların nasıl iletildiğini öğreneceksiniz. Evinizdeki bilgisayarın, dünya üzerinde nerede olduğu hakkında bir fikrinizin bile olmadığı bilgisayarları bulup aradığınız bilgileri size nasıl taşıdığını öğreneceksiniz.

ÖĞRENME FAALİYETİ – 1

AMAÇ

Taşıma katmanı protokollerini kullanabileceksiniz.

ARAŞTIRMA

- Taşıma katmanında kullanılan protokolleri ve bunların özelliklerini araştırınız.
- Kullandığınız işletim sisteminin "services" dosyasını inceleyiniz. Topladığınız bilgileri rapor haline getiriniz. Hazırladığınız raporu sınıfta öğretmeninize ve arkadaşlarınıza sununuz.

1. TAŞIMA KATMANI PROTOKOLLERİ

1.1. İstemci - Sunucu İlişkisi

İnsanlar her gün başkalarıyla iletişim kurmak ve rutin görevlerini yerine getirmek için ağ ve internet üzerinden sağlanan hizmetleri kullanmaktadır. En yaygın kullanılan internet uygulamalarının çoğu, birçok farklı sunucu ve istemci arasındaki karmaşık etkileşimlere dayanır.

Sunucu, ağa bağlı diğer konak bilgisayarlara bilgi veya hizmet sağlayan bir yazılım uygulamasını çalıştıran konak bilgisayarı ifade eder.

İstemci ise, sunucunun bilgi veya hizmetini talep eden bilgisayarları ifade eder.

Bir web sayfası incelenirkenkullanıcının bilgisayarı ve web tarayıcısı, istemci olarak adlandırılır. Web sayfasını, veritabanlarını ve uygulamaları üzerinde barındıran gelişmiş bilgisayarlar da sunucu olarak adlandırılır.Web tarayıcısı, web sunucusundan bir istekte bulunur ve sunucu istenen bilgileri toplar ve onu bir web sitesi şekline getirerek web tarayıcısına geri yollar. Kullanıcılar da ekranda web sitesini görmüş olur.Bu karmaşık etkileşimlerin gerçekleşmesini sağlayan en önemli faktör, tümünün üzerinde anlaşılmış standartları ve protokolleri kullanmasıdır.

İstemci/sunucu sistemlerinin en önemli özelliği, istemcinin sunucuya bir istek göndermesi ve sunucunun istemciye bilgiyi geri göndermek gibi bir işlev yürüterek yanıt vermesidir. Web tarayıcısı ve web sunucusu bileşimi büyük olasılıkla en yaygın kullanılan istemci/sunucu sistemi örneğidir.

Ağ üzerinde sadece web sunucuları bulunmaz. Dosya aktarımı için FTP sunucular, IP adresi dağıtımı için DHCP sunucular, web sitelerinin IP adresini bulmak için DNS sunucular, e-posta alıp göndermek içinde e-posta sunucuları da ağ üzerinde yer alan sunucular arasındadır.

1.2. Taşıma Katmanı Protokolleri

TCP/IP'de taşıma katmanı için TCP ve UDP olmak üzere iki protokol tanımlıdır. TCP bağlantı temelli bir protokoldür. Bu yüzdengönderici ve alıcı, veri iletişimi başlamadan önce iki taraf iletişim yapma konusunda istek ve onaylı mesajlarını birbirlerine gönderir. UDP ise bağlantısız basit bir protokoldür. Bu protokolde iletişim başlamadan önce gönderici ve alıcı arasında paket alışverişi yoktur.

1.2.1. TCP

Gelişmiş bilgisayar ağlarında ve paket anahtarlamalı bilgisayar iletişiminde, kayıpsız veri gönderimi sağlayabilmek için TCP protokolü kullanılmaktadır. HTTP, HTTPS, POP3, SMTP ve FTP gibi protokollerin veri iletimi TCP aracılığıyla yapılır. TCP aşağıdaki işlemleri gerçekleştirir.

Bağlantılı haberleşme: Bilgisayarlar iletişime geçmeden önce aralarında bir oturum açar. Oturumun açılması sırasında bilgisayarlar, kendi iletişim parametrelerini birbirlerine iletir ve bu parametreleri dikkate alarak iletişimde bulunur. Bu işleme el sıkışma (handshaking) adı verilir.

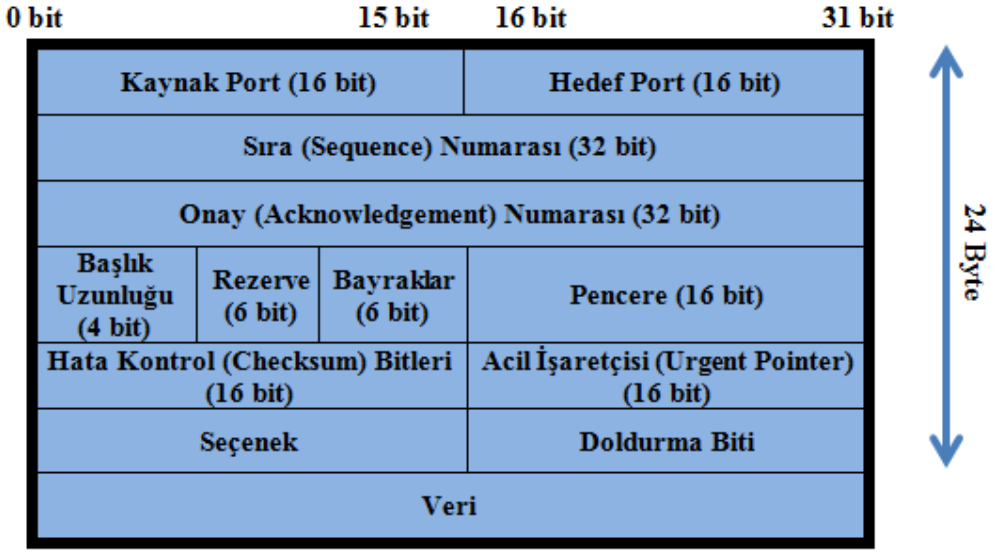
Güvenli haberleşme: Bilginin karşı tarafa gittiğinden emin olma durumudur. Bu güvenilirlik, bilginin alındığına dair karşı taraftan gelen bir onay mesajı ile sağlanır. Eğer bilgi gönderildikten belli süre sonra bu mesaj gelmezse paket yeniden gönderilir.

TCP'de tanımlı temel görevler aşağıdaki şekilde sıralanabilir:

- Bir üst katmandan gelen verinin uygun uzunlukta parçalara bölünmesi
- Her bir parçaya, alıcı kısımda aynı biçimde sıraya koyulabilmesi amacıyla sıra numarası verilmesi
- Kaybolan veya bozuk gelen parçaların tekrarlanması
- Uygulamalar arasında yönlendirme yapılması
- Güvenilir paket dağıtımının sağlanması

1.2.1.1. TCP Protokolünün Yapısı

TCP, taşıma katmanında verileri parçalara bölerek her bir parçanın önüne başlık bilgisi ekler. Başlık bilgisiyle birlikte bu veriye, TCP Segmenti denir.TCP başlık bilgisi 20 byte'tır. TCP Segmenti aşağıdaki gibidir.



Resim1.1: TCP segment yapısı

Kaynak port: Veriyi gönderen bilgisayarın kullandığı TCP portudur.

Hedef port: Hedef bilgisayarın TCP portudur.

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.

Başlık uzunluğu: TCP segmentinin uzunluğunu gösterir.

Rezerve: İleride kullanılmak üzere saklı tutulur.

Bayraklar: Segment ile ilgili kontrol bilgilerini taşır. 6 tane bayrak biti bulunmaktadır. Bunlar:

- **Acil (urgent) bayrağı:** Bu bayrak, acil işaretçisi alanının geçerli olup olmadığını belirtir.
- **Alındı (acknowledgement) bayrağı:** Bu bayrak, acknowledgement alanının geçerli olup olmadığını belirtir.
- **Push bayrağı:** Bu bayrak, modülün push fonksiyonunu işletip işletmeyeceğini belirtir.Push metodu, gönderilecek verinin hemen gönderilmesi için kullanılır.
- **Reset bayrağı:** Bu bayrak, bağlantının resetlenmesi gerektiğini belirtir. Bağlantıyı, anormal durumlarda, başlangıç durumuna getirir.
- **Synchronize bayrağı:** Bu bayrak, sıra numaralarının eş zamanlanmasının oluşturulmaya çalışıldığını bildirir. Bağlantı kurma segmentlerindehandshaking (el sıkışma) işlemlerinin oluştuğunu belirtmek için kullanılır.
- **Finish bayrağı:** Bu bayrak, göndericinin gönderecek daha fazla verisinin olmadığını belirtir.

Pencere: Akış kontrolü için kullanılır. Art arda kaç veri paketi gönderileceğini belirler.

Hata kontrol bitleri: Segmentin hatalı ulaşıp ulaşmadığını kontrol etmek için kullanılır.

Acil işaretçisi: Bir verinin acil olarak iletilmek istendiği durumlarda kullanılır.

Seçenek: TCP segmentinin maksimum boyutunun bilgisini taşır.

Doldurma biti: Seçenek bitinin boyutunu, 32 bit'e tamamlamak için kullanılır.

Veri: Verinin bulunduğu kısımdır.

1.2.1.2. TCP ile İletişim

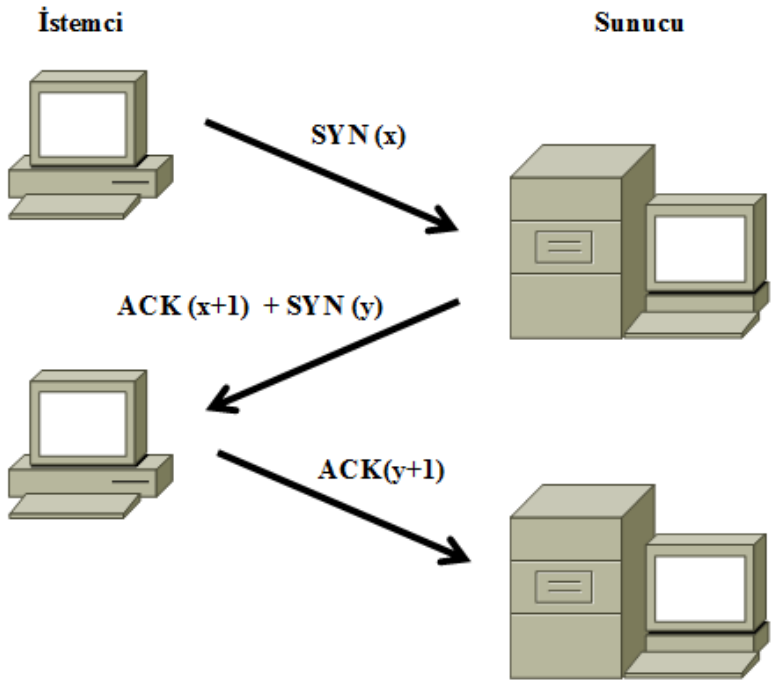
TCP veri iletiminin başlaması için aşağıdaki işlemler gerçekleşir:

1.İstemci, sunucu ile bir TCP oturumunu başlatmak için sunucuya bir SYN paketi gönderir ve dinlemeye geçer.

2.SYN başlatma paketini alan sunucu, ACK onay paketiyle birlikte SYN paketi gönderir ve dinlemeye geçer.

3.İstemci, sunucunun gönderdiği SYN paketine karşılık ACK onay paketi gönderir. Sunucu, ACK onay paketini aldıktan sonra oturum başlatılır.

Bu işleme üç aşamalı el sıkışma (3way-handshake) adı verilir.



Resim 1.2: 3 aşamalı el sıkışma

1.2.1.3. Servis Saldırıları

SYN saldırısı (SYN flood), hizmet engelleme saldırısının bir biçimidir. Bu saldırı biçiminde saldırgan, sistemi isteklere cevap veremeyecek duruma getirmek için sunucu kaynaklarını tüketme girişiminde bulunarak hedef alınan sisteme ardışık SYN istekleri (SYN requests) gönderir.

Normal olarak bir istemci bir sunucuya TCP bağlantısı başlatma isteğinde bulunduğunda, sunucu ve istemci bir dizi mesaj takas eder ve bu durum şöyle işler:

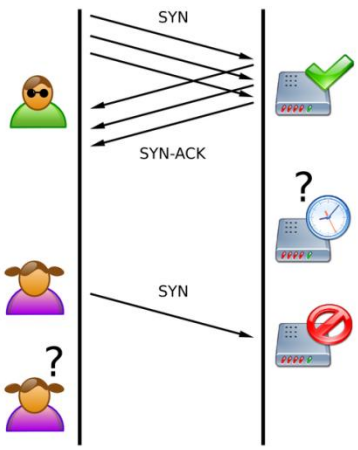
1. İstemci sunucuya bir SYN (synchronize) mesajı göndererek bir bağlantı kurmak ister.
2. Sunucu bu mesajı, SYN-ACK mesajlarını istemciye dönerek kabul eder.

3. İstemci ACK ile yanıt verir ve bağlantı kurulmuş olur.

Bu TCP üçlü el sıkışma olarak adlandırılır ve bütün TCP protokolü kullanan kurulmuş bağlantılar için temeldir.

SYN saldırısı, sunucununbeklediği ACK kodunu göndermeyerek çalışan bir ataktır. Kötü niyetli istemci ya basit bir şekilde beklenen ACK'yı göndermez ya da sahte IP adresi kullanarak SYN'deki IP adres kaynağını zehirler. Çünkü sunucu, sahte IP adresine SYN-ACK göndermeye çalışır. Ancak ACK gönderemeyecektir. Çünkü o adresle bir SYN gönderilmediğini bilir.

Sunucu bir süre ACK için bekleyecektir fakat saldırılarda bu istekler sürekli artan şekilde olduğundan sunucu yeni bağlantı oluşturamaz duruma gelir.



Resim 1.3: SYN saldırısı

1.2.2. UDP

UDP, TCP / IP protokol grubunun iki taşıma katmanı protokolünden birisidir. Gelişmiş bilgisayar ağlarında paket anahtarlamalı bilgisayar iletişiminde bir datagrammodu oluşturabilmek için UDP protokolü oluşturulmuştur. Bu protokol minimum protokol mekanizmasıyla bir uygulama programından diğerine mesaj göndermek için bir yöntem içerir.

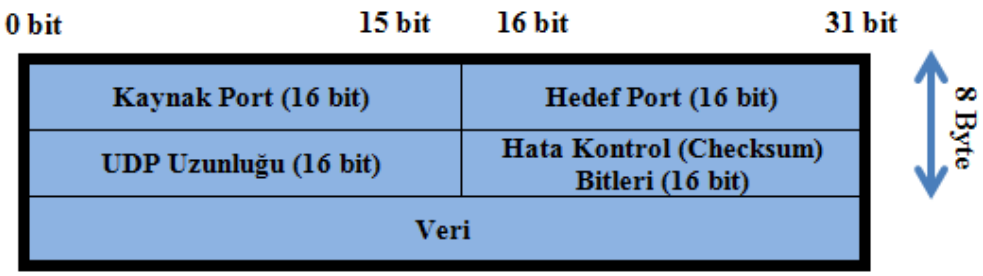
Bu protokol hareket yönlendirmelidir. Paketin teslim garantisini isteyen uygulamalar TCP protokolünü kullanır. Geniş alan ağlarında (WAN) ses ve görüntü aktarımı gibi gerçek zamanlı veri aktarımlarında UDP kullanılır. UDP bağlantı kurulum işlemlerini, akış kontrolü ve tekrar iletim işlemlerini yapmayarak veri iletim süresini en aza indirir. UDP ve TCP aynı iletişim yolunu kullandıklarında UDP ile yapılan gerçek zamanlı veri transferinin servis kalitesi TCP'nin oluşturduğu yüksek veri trafiği nedeniyle azalır.

UDP güvenilir olmayan bir aktarım protokolüdür. UDP protokolü ağ üzerinden paketi gönderir ve gidip gitmediğini takip etmez ve paketin yerine ulaşıp ulaşmayacağına onay verme yetkisi yoktur. UDP protokolünü kullanan programlara örnek olarak 161 numaralıportu kullanan SNMP servisini verebiliriz.

1.2.2.1. UDP Protokolünün Yapısı

UDP,datagramların belirli sıralara konmasının gerekli olmadığı uygulamalarda kullanılmak üzere tasarlanmıştır. TCP'de olduğu gibi UDP'de de bir başlık vardır. Ağ yazılımı bu UDP başlığını iletilecek bilginin başına koyar. Ardından UDP bu bilgiyi IP katmanına yollar. IP katmanı kendi başlık bilgisini ve protokol numarasını yerleştirir, bu kez numarası alanına UDP'ye ait değer yazılır. Fakat UDP, TCP'nin yaptıklarının hepsini yapmaz. Bilgi burada datagramlara bölünmez ve yollanan paketlerin kaydı tutulmaz. UDP'nin tek sağladığı port numarasıdır. Böylece pek çok program UDP'yi kullanabilir. Daha az bilgi içerdiğinden UDP başlığı TCP başlığına göre daha kısadır.

UDP başlığı her biri 16 bit uzunluğunda olmak üzere 4 alandan oluşur. Başlık, kaynak ve hedef port numaraları, UDP uzunluğu ve hata kontrol bitlerini içerir. UDP başlık bilgisinin boyutu 8 Byte'tır.



Resim 1.4: UDP yapısı

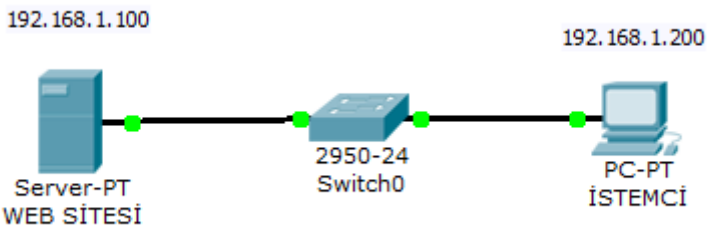
1.3. Portlar

TCP ve UDP, üst protokollerle bağlantıda portları kullanır. 65535 adet port vardır veIANA (Internet AssignedNumbersAuthority) ilk 1024 portu,iyi bilinen (Well-known) portlar olarak ilan etmiştir.

Bir bilgisayar, bir IP adresi ve bir port belirlediğinde buna soket (socket) ismi verilmektedir. Yani "X IP adresindeki bilgisayara, Y port'undan bilgi gönderildiğinde, bu bilgi şu işlem için ele alınacaktır." şeklinde bir önerme ortaya çıkar.

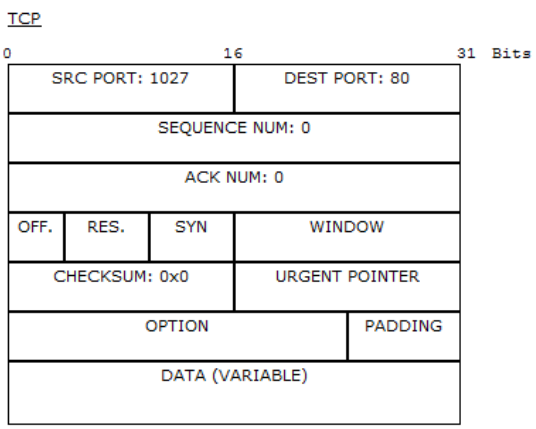
Örneğin istemci bir web sitesine bağlanmak istediğinde TCP segmentindeki, Hedef Port bilgisi 80 olur. HTTP'nin varsayılan port numarası 80'dir. İsteği alan sunucu, hedef port bilgisine bakarak kendisine gelen isteği ilgili uygulama katmanındaki servise gönderir.

Örnekte, ağ benzetim programı ile hazırlanmış basit bir ağ yapısı gözükmektedir. Web sayfasının olduğu sunucunun IP adresi 192.168.1.100, istemcinin ise 192.168.1.200'dür.



Resim 1.5: Örnek ağ yapısı

İstemci web sayfasını görüntülemek istediğinde sunucuya bir veri paketi gönderilir. Aşağıdaki resimde, TCP segmentininiçeriği şekilde gösterilmektedir.

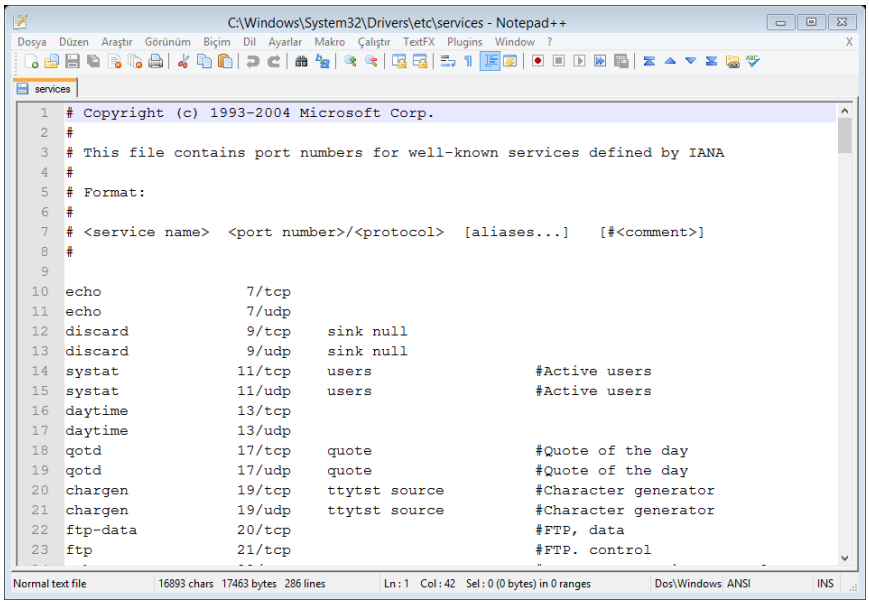


Resim 1.6: TCP segment yapısı

SRC PORT alanı (kaynak port), istemcinin portunu gösterir ve sunucudan istemciye gelecek olan bilgiler bu port numarası ile uygulama katmanına geçecektir. Kaynak port, iki aygıt arasındaki iletişimi tanımlamak için gönderen aygıt (istemci) tarafından rastgele oluşturulur.DEST PORT (hedef port) alanı ise sunucunun port numarasıdır. Bu port numarası sunucuya HTTP hizmeti istendiğini belirtir.

Birçok TCP/IP ve UDP/IP servisi, bu port numaraları ile tanınır. Port numaraları üç ayrı sınıfta toplanır. Bunlar:

0 ile 255 arasındaki port numaraları standart uygulama katmanlarına erişim için kullanılmıştır. Örneğin telnet için port 23, ftp için port 21 kullanılır. Windows İşletim Sisteminde, bilgisayarın hangi uygulama programı için hangi port numarasını kullandığı C:\Windows\System32\Drivers\etc\services dosyasından öğrenilebilir.



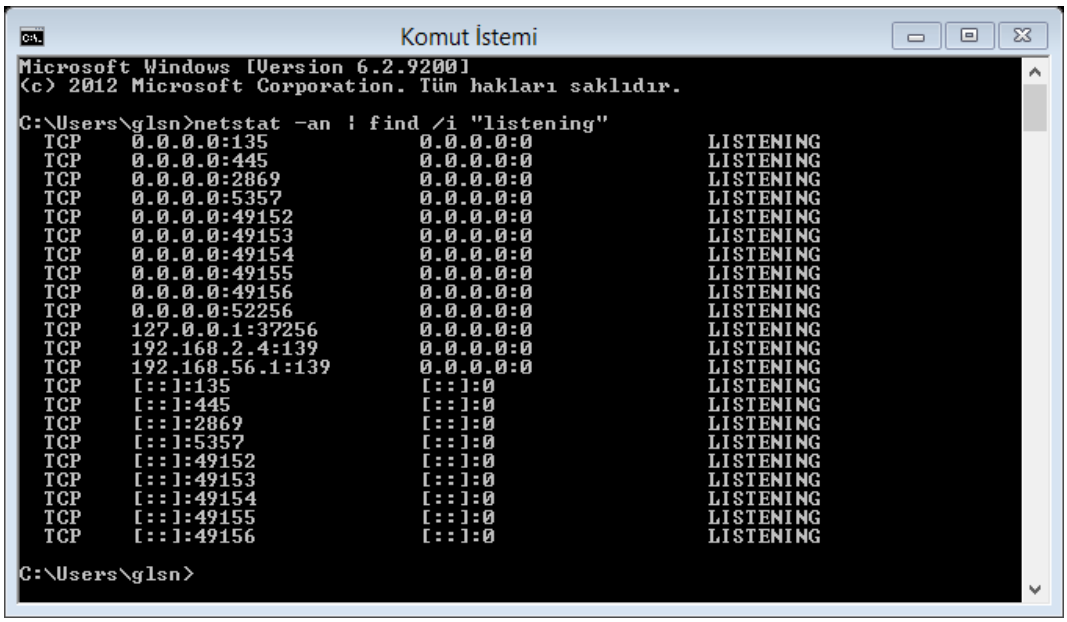
Resim 1.7: Services dosyası

255 ile 1023 arasında bulunan portlar, ticari şirketlerin geliştirdiği uygulamalar için kullanılır.

1024 ve üzerinde bulunan portlar,herhangi bir düzenlemeye tabi tutulmamıştır. Sunucuya istek yapıldığında kaynak port olarak bu portlardan atama işlemi yapılır.

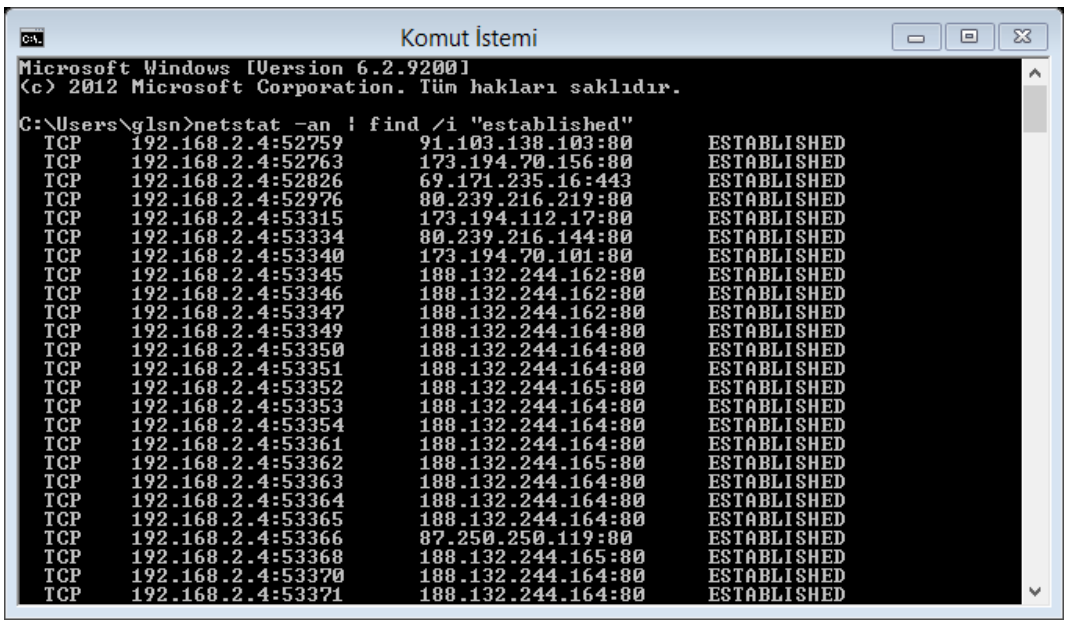
Netstat (**net**work **stat**istics); ağ bağlantıları (hem gelen hem giden), yönlendirme tabloları ve ağ ara yüzü istatistiklerini görüntülemek için kullanılan bir komut satırı aracıdır. Netstat komutu UNIX, Linux ve Windows NT tabanlı işletim sistemlerinde kullanılabilir.

Açık ve dinlenme durumunda olan portları görüntülemek için **netstat –an | find /i "listening"** komutu kullanılır.



Resim 1.8: Netstat komutunun kullanımı

İletişimde olan portları görüntülemek için **netstat –an | find /i "established"** komutu kullanılır.



Resim 1.9: Netstat komutunun kullanımı

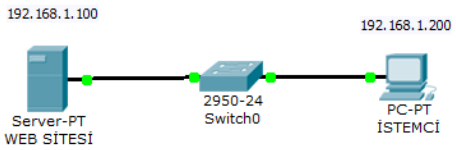
1.3.1. Port Numaraları

En çok kullanılan port numaraları aşağıda listelenmiştir.

- FTP: 20-21. port
- HTTP: 80. port (Alternatif Port: 8080)
- HTTPS: 443. port
- SMTP: 25. port
- TELNET: 23. port
- SSH: 22. port
- IMAP: 143. port
- POP3: 110. port
- SMPTS: 465. port
- POP3S: 995. port
- IMAPS: 993. port
- DNS: 53. port
- DHCP: 67-68. port

UYGULAMA FAALİYETİ

Aşağıdaki işlem basamaklarını takip ederek faaliyeti gerçekleştiriniz.

İşlem Basamakları	Öneriler
➢ Ağ benzetim programı ile üç aşamalı el sıkışma olayını ve veri paketleri inceleyiniz.	➢ Aşağıdaki basit ağ yapısını oluşturunuz.  ➢ Ağ benzetim programında "simulation" moduna geçiniz. ➢ Web sitesindeki sayfayı görüntülemek için istemcinin internet tarayıcısından web sitesinin IP adresini yazın. ➢ İstemci ve web sitesinin gönderdiği paketleri inceleyiniz.
➢ Bilgisayarınızdaki açık ve dinlenmekte olan portlar ile iletişimde olan portları görüntüleyiniz.	➢ Açık ve dinlenmekte olan portları görüntülemek için **netstat –an | find /i "listening"** komutunu kullanabilirsiniz. ➢ İletişim halinde olan portları görüntülemek için **netstat –an | find /i "established"** komutunu kullanabilirsiniz.

ÖLÇME VE DEĞERLENDİRME

Aşağıdaki soruları dikkatlice okuyunuz ve doğru seçeneği işaretleyiniz.

1. Ağdaki iletişim başlangıcı öncesinde, gönderici ve alıcının iletişim yapma konusunda istek ve onay mesajlarını birbirlerine gönderdiği protokol hangisidir?
A) UDP
B) DHCP
C) IP
D) TCP
E) HTTP

2. Hangisi TCP'de tanımlanmış temel görevlerden biri değildir?
A) Uygulamalar arasında yönlendirme yapması
B) Bozuk gelen verileri tekrarlamaması
C) Üst katmandan gelen veriyi uygun uzunlukta parçalara bölmesi
D) Güvenilir paket dağıtımının sağlanması
E) Her veri paketine sıra numarası vermesi

3. İstemci ve sunucunun ilk defa iletişime geçmeden önce yaptığı işlemin adı nedir?
A) Üç aşamalı el sıkışma
B) Oturum açma
C) Onaylama
D) Senkronizasyon
E) Veri bağı

4. UDP başlığı kaç byte'tır?
A) 8
B) 16
C) 24
D) 32
E) 36

5. Windows işletim sisteminde, hangi uygulamanın hangi portu kullandığını gösteren dosyanın adı nedir?
A) Hosts
B) Ports
C) Services
D) Etc
E) Formats

6. Varsayılan olarak HTTP kaç numaralı portu kullanmaktadır?
A) 20
B) 21
C) 443
D) 80
E) 143

7. Varsayılan olarak DNS kaç numaralı portu kullanmaktadır?
A) 465
B) 995
C) 53
D) 110
E) 22

8. Varsayılan olarak TELNET kaç numaralı portu kullanmaktadır?
A) 21
B) 22
C) 23
D) 55
E) 67

9. Bilgisayardaki, sadece iletişim halinde olan portları görüntülemek için hangi komut kullanılır?
A) netstat –an | find /i "established"
B) netstat –an | find "listening"
C) netstat –an
D) netstat
E) netstat –an | find "open"

10. Kaç tane port numarası vardır?
A) 65535
B) 36535
C) 2048
D) 1024
E) 255

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

Uygulama katmanındaki uygulama ve protokolleri kullanabileceksiniz.

ARAŞTIRMA

- Uygulama katmanında kullanılan protokolleri ve bunların özelliklerini araştırınız. Topladığınız bilgileri rapor haline getiriniz. Hazırladığınız raporu sınıfta öğretmeninize ve arkadaşlarınıza sununuz.

2. UYGULAMA KATMANI UYGULAMALARI

2.1. TCP/IP Uygulama Katmanı

TCP/IP'nin uygulama katmanında, veriyi göndermek isteyen uygulama ve kullandığı dosya biçimi bulunarak gönderilen verinin türüne göre farklı protokoller çalıştırılır (HTTP, SMTP, FTP, Telnet, vs.).Programlarla taşıma protokollerinin haberleşmesi sağlanır. Uygulama katmanı, taşıma katmanıyla portlar aracılığıyla haberleşir. Portlar numaralandırılmış standart uygulamalardır (HTTP:80, FTP:21, vs.) ve taşıma katmanında gelen paket içeriğinin türünün anlaşılmasında rol oynar.Bu katman, TCP/IP uygulama protokollerini ve programların ağı kullanmak için taşıma katmanı hizmetleriyle nasıl bir arabirim oluşturacağını tanımlar.

2.2. Uygulama Katmanı Protokolleri

2.2.1. DNS

İnternet bağlı ve farklı alanlarda olan binlerce sunucu, her gün internette kullanılan hizmetleri sağlar. Bu sunucuların her birine, bağlı olduğu yerel ağda, sunucuyu tanımlayan benzersiz bir IP adresi atanır.

İstemcilere hizmet veren bu sunuculara erişmek için sunucuların IP adreslerinin bilinmesi gerekir. Fakat tüm sunucuların IP adreslerinin akılda tutulması mümkün değildir. Bunun yerine, kullanıcı dostu internet adresleri (www.meb.gov.tr gibi) kullanılmaktadır.

DNS(Domain Name System, Etki Alanı Adlandırma Sistemi), www.meb.gov.tr gibi internet adreslerinin, IP adreslerine çevrimini sağlar.

2.2.1.1. DNS'nin Tarihçesi

İnternet yaygınlaşmamış ve internet üzerindeki bilgisayar sayısı azken internet adresi-IP adresi çözümlemesi, HOST adında metin dosyası ile yapılmaktaydı. İnternet adresi ve karşılığındaki IP adresi, bu dosyaya elle kayıt edilmekte ve internetteki bilgisayarların her birinde bu dosyanın bir kopyası bulunmaktaydı. Bir bilgisayar, bir başka bilgisayara ulaşmak istediğinde bu dosyayı inceliyor,eğer dosyada o bilgisayarın kaydı bulunuyorsa IP adresini alıyor ve iletişime geçiyordu.

Bu sistemin iyi işleyebilmesi için HOSTS dosyası içeriğinin hep güncel kalması gerekiyordu. Bunu sağlamak için de dosyanın aslının saklandığı ABD'deki Stanford Üniversitesi'ne belli aralıklarla bağlanarak kopyalama yapılıyordu.

Ama internetteki bilgisayarların sayısı arttıkça hem bu dosyanın büyüklüğü olağanüstü boyutlara ulaşmaya başladı hem de internetteki bilgisayarların dosyayı kopyalamak için yaptığı bağlantı Standford'daki bilgisayarları kilitlenmeye başladı.

Tek bir HOSTS dosyası kullanmanın başka bir kötülüğü de şuydu: Bütün bilgisayarlar aynı düzeyde yer aldığı için bir bilgisayar isminin bütün internette bir eşinin daha bulunmamasını sağlamak gerekiyordu.

Bu sorunlar yüzünden internet yetkili organları, 1984 yılında DNS'yi ürettiler.DNS hem bilgisayar veri tabanını dağıtık bir yapıya sokmaktahemde bilgisayarlar arasında hiyerarşik bir yapı kurulmasını sağlamaktadır.

DNS'de dağıtık veri tabanı şöyle sağlanır. Bilgisayarlar bulundukları yerlere,ait oldukları kurumlara göre sınıflandırılmaktadır. Örneğin, Türkiye'deki bilgisayarların listesi (.tr domaini), Türkiye'den sorumlu bir DNS sunucu makinedetutulmaktadır. Böylece internet ortamındaki bütün bilgisayarların bilgisinin tek bir yerde tutulması zorunluluğu kalmamıştır.

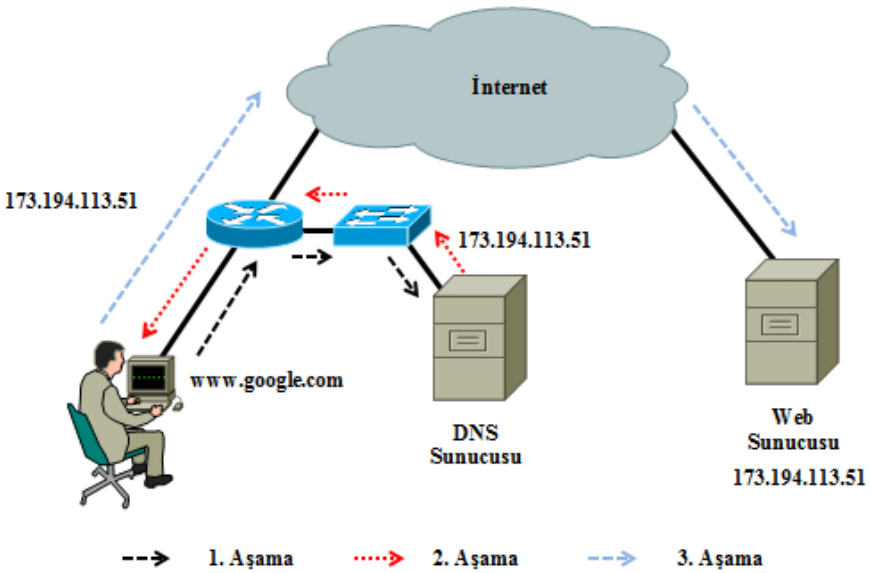
İnternet adresleri ülkelerden sonra alt bölümlere ayrılır. Bu bölümlere üst düzey domainler denir. Bu domainlerin ifade ettikleri bölümler şunlardır:

- .com: Ticari kuruluşlar (COMmercial)
- .edu: Yükseköğrenim kurumları (EDUcation)
- .org: Sivil toplum kuruluşları (ORGanizations)
- .gov: Hükümete ait kurumlar (GOVernment)
- .mil: Askeri kurumlar (MILitary)
- .net: Büyük ağ hizmetleri veren kuruluşlar (NETwork)
- .int: Uluslararası organizasyonlar (INTernational)
- .num: Telefon numaraları bulabileceğiniz yerler (NUMbers)
- .arpa: Ters DNS sorgulaması yapılan yerler

2.2.1.2. DNS Çözümleme

DNS sunucusunda, sunucu adlarını karşılık gelen IP adresleriyle ilişkilendiren bir tablo yer alır. Bir istemcide, sunucunun adı (örneğin, bir web adresi) bulunuyor ancak IP adresinin istemci tarafından bulunması gerekiyorsa DNS sunucusuna hedef portu 53 olan bir istek gönderir. İstemci, IP yapılandırmasındaki DNS ayarlarında yapılandırılmış, DNS sunucusunun IP adresini kullanır.

DNS sunucusu isteği aldığında, IP adresinin bir web sunucusuyla ilişkilendirilmiş olup olmadığını belirlemek için tablosunu kontrol eder. Yerel DNS sunucusunda, istenen ada ilişkin giriş yoksa sunucu etki alanı içindeki başka bir DNS sunucusunu sorgular. DNS sunucusu IP adresini öğrendiğinde, bu bilgi istemciye geri gönderilir. DNS sunucusu IP adresini belirleyemezse istek zaman aşımına uğrar ve istemci web sunucusuyla iletişim kuramaz.

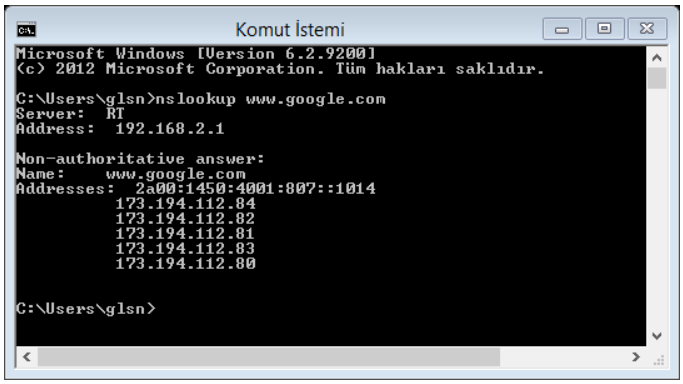


Resim 2.1: IP çözümleme işlemi

2.2.1.3. NSLOOKUP Komutu

Nslookup, IP adresini girerek isim sorgusu ya da internet adresi girerek IP adresi sorgusu yapılmasına yarayan birkomuttur. Bu komutun çalışması, Windows ve Linux sistemlerinde ortaktır.

Bir web sitesinin, IP adresini sorgulamak için nslookup yazıp bir boşluk bırakarak web sitesi adresini yazmanız yeterlidir. Komut çalıştığında,DNS'de çözümleme işlemi yapılacak ve size web sitesinin IP adresini görüntüleyecektir. Ayrıca "Server" alanı ile hangi DNS sunucusunu kullandığınızı ve "Address" alanı ile de DNS sunucusunun IP adresini görebilirsiniz.



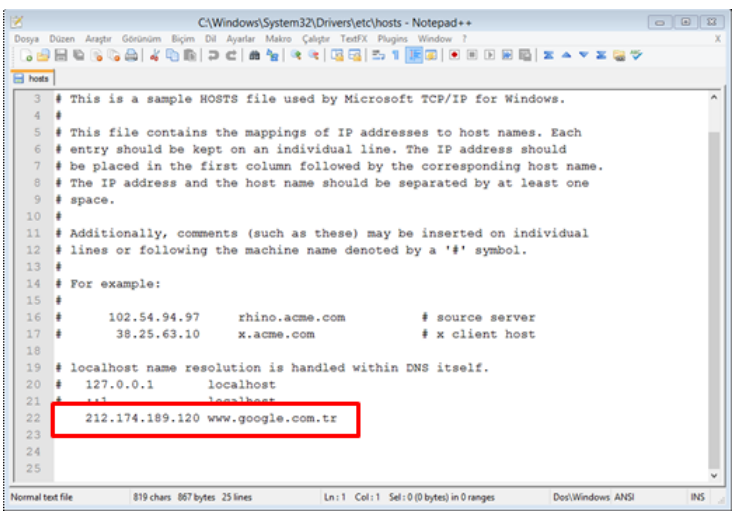
Resim 2.2: NSLOOKUP komutunun kullanımı

2.2.1.4. Host Dosyası

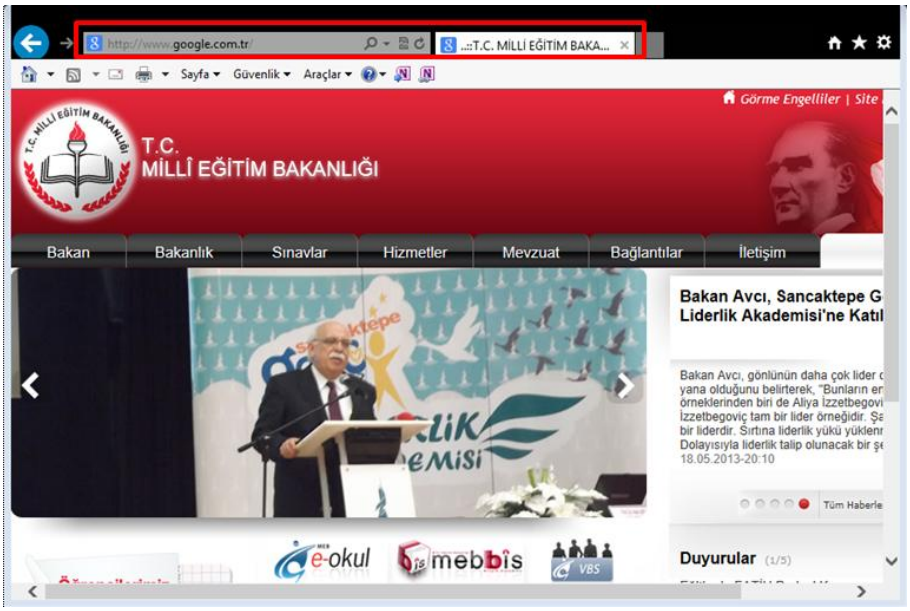
DNS oluşturulmadan önce IP çözümlemesi için her bilgisayar hostdosyası kullanmaktaydı ve bu dosyanın sürekli güncellenmesi gerekmekteydi. DNS oluşturulduktan sonra bu işleme gerek kalmamıştır. Fakat işletim sistemlerinde bu host dosyaları hala bulunmakta ve kullanılmaktadır. Bu dosya, Windows işletim sistemlerinde "C:\Windows\System32\Drivers\etc\host", Linux işletim sistemlerinde ise "etc\host" dizinindedir.

Tarayıcıya bir web sitesi adresi yazıldığında, önce host dosyasına bakılır, burada web adresi-IP adresi yoksa DNS sunucudan IP çözümlemesi yapılır. Bu dosyayı elle kendiniz güncelleyebilirsiniz.

Aşağıdaki resimde,host dosyasında www.google.com.tr için farklı bir IP adresi verildiğini görebilirsiniz. Tarayıcıya www.google.com.tr yazdığınızda, aşağıda belirtilen IP adresine gidilecektir.



Resim 2.3: Host dosyası



Resim 2.4: Host dosyasının etkisi

2.2.2. FTP ve TFTP

2.2.2.1. FTP (File Transfer Protocol)

File Transfer Protocol (FTP);veriyi,bir uç aygıttan diğerine iletim için kullanılır. Bir dosyayı FTP kullanarak başka bir TCP/IP ağı üzerindeki kullanıcıya yollamak için o ağdaki bilgisayarda geçerli bir kullanıcı ismi ve şifresi gerekmektedir. Birçok FTP sunucusu, kullanıcı ismi ve parola olmadan erişim için "anonim FTP" (anonymous FTP) desteği verir. Bu kullanım için kullanıcı adı olarak “anonymous” parola olarak ise bir e-mail adresi girilmesi gerekmektedir.

FTP, TCP 20 ve 21 numaralı portlardan hizmet vermektedir. TCP port 20 üzerinden veri transferi gerçekleştirilirken TCP port 21 ise kontrol amaçlı kullanılmaktadır.

FTP istemcileri iki farklı modda yapılandırılabilir.

- Aktif FTP

Bu FTP çeşidinde istemci aktif rol alır. Günümüz internet altyapısında çeşitli sorunlara yol açtığı için pasif FTP daha fazla tercih edilmektedir. Aktif FTP’de çıkan sorunlar pasif FTP’nin geliştirilmesini sağlamıştır.

FTP istemcisi, TCP port 21 üzerinden sunucuya bir kontrol kanalı açar. Bu işlem sırasında FTP istemcisi rastgele bir port numarası kullanır. Örneğin istemci 1025 numaralı kanalı kullanmış olsun.

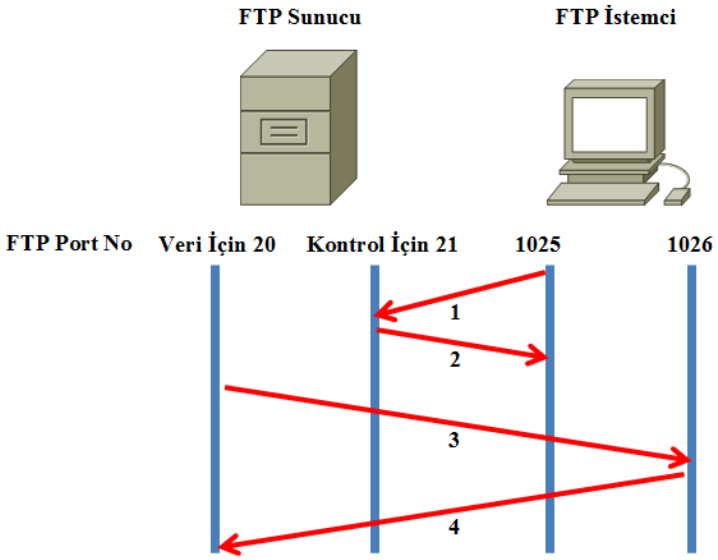
FTP sunucusu, gerekli karşılama mesajı ve kullanıcı adı sorgulamasını gönderir.
İstemci gerekli erişim bilgilerini girer.

Sunucu erişim bilgilerini kontrol eder, bilgiler doğru ise istemciye FTP komut satırını açar.

İstemci kendi tarafında 1024'ten büyük bir port numarası açar ve bunu PORT komutu ile FTP sunucuya bildirir.

FTP sunucusu, istemcinin bildirdiği port numarasından bağlantı kurar ve gerekli aktarım işlemleri başlar.

İstemci onay mesajı gönderir.



Resim 2.5: Aktif FTP'nin çalışması

- Pasif FTP

Pasif FTP, günümüz internet dünyasında kullanılan güvenlik duvarı, NAT cihazları gibi trafikte değişiklik yapan sistemlerden kaynaklanan FTP problemlerini sunucu tarafında halledebilmek için çıkarılmış FTP çeşididir. PasifFTP'de istemci pasif roldedir, sunucu aktif roldedir.

FTP istemcisi, TCP port 21 üzerinden sunucuya bir kontrol kanalı açar. Bu işlem sırasında FTP istemcisi rastgele bir port numarası kullanır. Örneğin istemci 1025 numaralı kanalı kullanmış olsun.

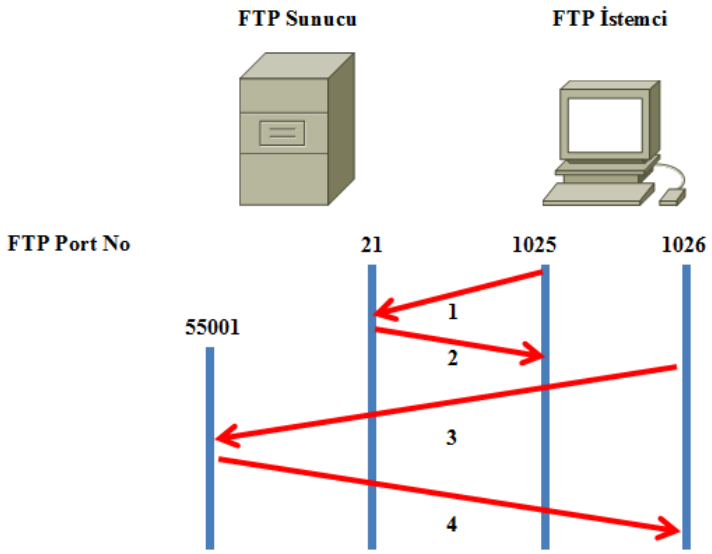
FTP sunucusu, gerekli karşılama mesajı ve kullanıcı adı sorgulamasını gönderir.
İstemci gerekli erişim bilgilerini girer.

Sunucu erişim bilgilerini kontrol eder, doğru ise istemciye FTP komut satırını açar.

FTP istemcisi PASV komutu aracılığıyla sunucudan ek port açmasını bekler. Sunucu, yapılandırma dosyasında belirtilen port aralığından bir port açarak bunu istemciye belirtir.

İstemci, sunucudan gelen bu porta bağlanarak veri alışverişini başlatır.

İstemci onay mesajı gönderir.



Resim 2.6: Pasif FTP'nin çalışması

2.2.2.2. TFTP (Trivial File Transfer Protocol)

TFTP (Trivial File Transfer Protocol), FTP'nin temel fonksiyonel şekli olarak ifade edilen basit bir dosya transfer protokolüdür.Basit yapısından dolayı kullanılması esnasında çok az bellek tüketilmektedir. Bu özelliğinden dolayı, yeterli yığın bellek cihazı (massstoragedevice) olmayan yönlendiricilerin önyüklemesinde kullanılır.

Bu protokol UDP üzerinde 69. port kullanılarak uygulanmıştır.TFTP basit ve uygulanması kolay olacak şekilde tasarlanmıştır ve bu nedenle çoğu FTP özelliğinden yoksundur.TFTP sadece dosya alma ve gönderme işlemlerini yapar.Dizinleri listelemez ve şu anda kullanıcı kimlik doğrulaması için bir kural yoktur.

2.2.3. HTTP ve HTTPS

HTTP (HyperText Transfer Protocol),web sayfalarını istemciye ulaştıran temel protokoldür.

Bir web adresine bakılmak istendiğinde, istenilen sayfa bilgisayara gelmeden önce arka planda bir dizi işlem gerçekleşir. İlk önce, internet tarayıcısı görüntülenmek istenen web sayfasının adresini ve port numarası olarak 80'i, sunucuya bildirir. Sunucu 80 numaralı porttan bir istek aldığında bunun http isteği olduğunu anlar ve istemciye web sayfasını gönderir.Web sayfalarındaki bilgi HTML, XML veya XHTML dilleri kullanılarak kodlanır. İşlem gerçekleşmezse hata mesajı alınır. İşlemin gerçekleşmesi hâlinde son olarak http servisiyle yapılan bağlantı kesilir.

1990 yılından beri kullanımda olan http, internet adreslerinin önüne "http://" yazılarak kullanılır. Girilecek adresin önüne "http://" getirilmese bile internet tarayıcıları bu eksikliği tamamlayarak internette sorunsuzca gezinti yapılmasını sağlar.

HTTP protokolü güvenli bir protokol değildir; bilgi ağ üzerinden gönderilirken başka kullanıcılar tarafından kolayca müdahale edilebilir. Verilerin güvenliğini sağlamak amacıyla güvenli taşıma protokolü olan HTTPSkullanılır. HTTPS istekleri,443 numaralı portu kullanır. Bu istekler için tarayıcıdaki site adresinde "http://" yerine "https://" kullanılması gerekir.

2.2.4. E-Posta Protokolleri

2.2.4.1. SMTP

SMTP (Simple Mail Transfer Protocol), bir e-posta göndermek için sunucu ile istemci arasındaki iletişim şeklini belirleyen protokoldür. Sadece e-posta yollamak için kullanılan bu protokolde basitçe, istemci bilgisayar SMTP sunucusuna bağlanarak gerekli kimlik bilgilerini gönderir, sunucunun onay vermesi halinde gerekli e-postayı sunucuya iletir ve bağlantıyı sonlandırır.

E-posta almak için POP3 ya da IMAP protokolü kullanılır.

Outlook, Thunderbird, gibi e-posta istemcileri, e-postaları göndermek üzere sunucuya iletirken SMTP servisinden faydalanır.

25 numaralı port SMTP sunucusu için ayrılmıştır.

2.2.4.2. POP3

POP3 (Port Office Protocol 3), istemciye gönderilmiş olan e-postaları istemcinin bilgisayarına indirmeye yarayan bir protokoldür. Bu protokol kimlik doğrulaması gerektirdiği için kullanıcı adı ve parola, istemcinin kullandığı yazılımın ilgili alanlarına girilmesi gerekir.

POP istemcilerini destekleyen bir sunucu, kullanıcılarına adreslenen iletileri alır ve depolar. İstemci e-posta sunucusuna bağlandığında, iletiler istemciye indirilir. Varsayılan olarak iletiler istemci tarafından erişildikten sonra sunucuda tutulmaz. İstemciler, 110 numaralı port ile POP3 sunucularıyla iletişim kurar.

2.2.4.3. IMAP4

IMAP (Internet Message Access Protocol), e-posta almak için kullanılan bir protokoldür.

IMAP istemcilerini destekleyen bir sunucu, kullanıcılarına adreslenen iletileri alır ve depolar. Ancak bu sunucu, iletileri kullanıcı silmediği sürece sunucudaki posta kutularında tutar. En güncel IMAP sürümü, 143 numaralı porttan istemci isteklerini dinleyen IMAP4'tür.

POP3'e göre aşağıdaki avantajları bulunmaktadır.

- İstemci, e-posta sunucusuna POP3 protokolü ile bağlandığında tüm yeni mesajlar istemciye çekilir ve bağlantı kapatılır.IMAP protokolü kullanıldığında ise oturum açıldıktan sonra bağlantı sadece istek olduğu durumlarda açık kalır (Bir mesajın açılması ve içeriğinin görüntülenmesi gibi).
- POP3 protokolü bir posta kutusunda aynı anda tek kullanıcıyı destekler. Tersi durumda işleyiş tarzı sorun yaratır. Bunun sebebi, tüm yeni mesajların istemciye çekilmesidir. IMAP ise çok kullanıcıyı destekler. Bir kullanıcının yaptığı değişiklik eş zamanlı olarak diğer oturum açmış kullanıcı tarafından görülebilir.
- Nerdeyse bütün e-posta mesajları MIME (Multipurpose Internet Mail Extensions-Çok İşlevli Internet Posta Uzantıları) formatında gönderilir. Bir e-posta yazı bölümü, ekli dosya bölümü gibi bölümlere ayrılır. IMAP bu bölümleri birbirinden bağımsız olarak çekebilir. Örneğin, mesajı açmadan mesaj ekindeki bir dosya bilgisayara kopyalanabilir.

2.2.5. DHCP

DHCP (Dynamic Host Configuration Protocol), sistemdeki bilgisayarlara IP adreslerini ve buna ek olarak değişik parametreleri (Alt Ağ Maskesi, Varsayılan Ağ Geçidi, DNS Sunucusu gibi) atamak için kullanılan servistir.DHCP'nin temel özelliği, sistemi kuran kişilerin tek tek tüm makineleri gezip aynı veya benzer parametreleri defalarca eliyle girmesini engellemek,böylece zaman kazanmak ve sistem yöneticisinin işini kolaylaştırmaktır.DHCP aşağıdaki şekilde çalışır:

- DHCP Discover

İstemci bilgisayar ilk defa açıldığında öncelikle tüm ağa DHCP discovermesajını yollar. Bu mesajın içeriği, "Sistemde herhangi bir DHCP sunucu bulunuyor mu? Eğer var ise bir IP adresi istiyorum." olarak özetlenebilir.

Ağa gönderilen DHCP istek paketinde, istekte bulunulan IP adresi, MAC adresi ya da paketi gönderen bilgisayarın IP adresi bilinmediğinden, paketin içeriği aşağıdaki şekilde oluşacaktır:

1-Hedef IP adresi (Bilinmiyor): 255.255.255.255 (broadcast)
2-Hedef MAC adresi(Bilinmiyor): FF.FF.FF.FF.FF.FF(broadcast)
3-Kaynak IP adresi(Bilinmiyor): 0.0.0.0
4-Kaynak MAC adresi:00-A0-CC-66-73-1F (Bu adres istemci bilgisayarın adresidir ve örnek olarak yazılmıştır.)

- DHCP Offer

DHCP istemci tarafından sisteme atılan yayın paketi(broadcastpacket), DHCP sunucu tarafından alınır.IP veritabanı sorgulanır,istemciye verilecek IP adresi ve kira süresi belirlenir. Sunucudan çıkan isteğin onaylanması için istemciye bu belirlenen bilgiler geri yollanır.

Sistemde birden fazla DHCP sunucu bulunabilir. Bu durumda, istemci ağa bir istek gönderdiği zaman en hızlı DHCP offer mesajı yollayanın IP bilgilerini benimseyecek ve bu tanımlarla ağa bağlanacaktır. DHCP sunucusunun gönderdiği yanıt paketi aşağıdaki gibidir:

1-Hedef IP adresi (Henüz onaylanmadı): 0.0.0.0
2-Hedef MAC adresi(Biliniyor,istemci bilgisayar):00-A0-CC-66-73-1F
3-Kaynak IP adresi(Biliniyor,DHCP sunucu): 10.0.0.1
4-Kaynak MAC adresi(Biliniyor, DHCP sunucu):00-A0-C0-B6-12-6F

- DHCP Request

DHCP offer mesajını alan DHCP istemci, kendisine tahsis edilmiş IP adresini kiraladığına dair sunucuya bir yayın mesajı yollar. Eğer DHCP istemci birden fazla DHCP offer mesajı almış ise ikinci bir broadcast mesajı daha yollar ve diğer DHCP sunuculara artık bir IP adresine sahip olduğunu belirtir.

- DHCP Acknowledgement

DHCP request mesajını alan DHCP sunucu artık DHCP istemci için gerekli kayıtları gerçekleştirip ona gerekli olan IP,ağ maskesi,DNS adres veya adreslerini yollayacaktır.

2.2.6. TELNET

Telnet, internet ağı üzerindeki çok kullanıcılı bir sunucuya, uzaktaki başka bir bilgisayardan bağlanmak için geliştirilen bir TCP/IP protokolü ve bu işi yapan programlara verilen genel isimdir. Bağlanılan bilgisayara girebilmek için bir kullanıcı isminizin ve bağlantının gerçekleşebilmesi için bir telnet erişim programınızın olması gereklidir.

Telnet 23 numaralı portu kullanmaktadır.

Telnet güvensiz bir protokoldür. Tüm veriler, şifrelenmemiş olarak gönderilir. Bu yüzden telnet oturumundan, sniffer(koklayıcı) programları yardımıyla kolaylıkla önemli bilgilere ulaşılabilir.

2.2.7. SSH

SSH, telnet gibi ağ üzerindeki bir sunucuya, uzakta bulunan bir başka bilgisayardan bağlantı sağlayan bir protokoldür. SSH açık haliyle "Secure Shell" yani güvenli kabuk anlamına gelir. Telnet'te, kullanıcı şifreleri dahil tüm iletişim açık yani şifrelenmeden gerçekleştirilirken SSH güvensiz makineler arasındaki iletişimi, güçlü bir kripto yöntemiyle şifreler.

SSH ile bağlantının gerçekleştirilebilmesi için Telnet ile bağlantıda olduğu gibi bağlanılmak istenen sunucu makinede bir kullanıcı hesabının ve kullanıcı şifresinin bulunması gereklidir. Bunların dışında bir de SSH istemci programlarından birine ihtiyaç olacaktır. SSH ile bir bilgisayara bağlanabilmek için kullanıcı, öncelikle kimliğini ispatlayabilmelidir.SSH, 22 numaralı portu kullanır.

2.2.8. SNMP

SNMP (Simple Network Management Protocol), ağ cihazlarının yönetimini ve izlenmesini kolaylaştıran bir uygulama katmanı protokolüdür. Bu protokol sayesinde ağdaki hemen her türlü cihaz izlenebilir hatta yapılandırmaları değiştirilebilir. SNMP, TCP/IP protokol kümesinin bir bileşenidir ve bir uygulama katmanı protokolü, veri tabanı şeması, veri nesneleri gibi standartlar barındırır.

SNMP'nin üç temel bileşeni vardır. Bunlar:

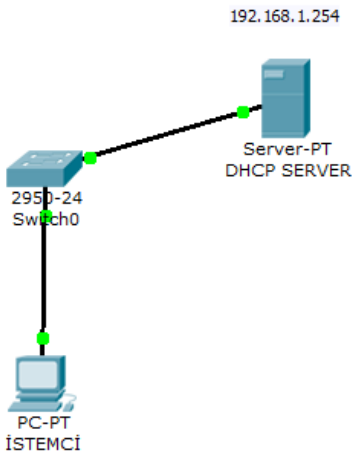
- **NMS (Network Management System):** Yönetici tarafında çalışan SNMP yazılımıdır.
- **Agent:** Yönetilen cihaz tarafında çalışan yazılımdır.
- **MIB (Management Information Base):** Her cihazın yerelinde bulunan, cihazdaki agent tarafından erişim sağlanan ve cihazla ilgili bilgileri bulunduran bir veri tabanıdır.

SNMP'nin çalışma mekanizması istek gönderme ve isteğe cevap alma şeklindedir ve bunun için taşıma katmanında kullandığı protokol UDP'dir. NMS istekleri herhangi bir portundan Agent'ın 161. portuna gönderir. İletişimi Agent'ın başlatması durumunda bildirimler NMS'in 162. portuna gönderilir.

SNMP sayesinde bir cihazdan bilgi alınabileceği gibi cihazdaki bilgi değiştirilebilir ve cihazda yeni bir yapılandırma uygulanabilir. Örneğin cihaz baştan başlatılabilir, cihaza bir yapılandırma dosyası gönderilebilir ya da cihazdan alınabilir.

UYGULAMA FAALİYETİ

Aşağıdaki işlem basamaklarını takip ederek faaliyeti gerçekleştiriniz.

İşlem Basamakları	Öneriler
➢ www.meb.gov.trve www.google.com.tr internet adreslerinin IP adreslerini öğreniniz.	➢ IP çözümlemesi yapmak için komut satırından NSLOOKUP komutunu kullanabilirsiniz.
➢ Ağ benzetim programında DHCP sunucudan IP alma işlemini gerçekleştiriniz. ➢ İstemci ile sunucu arasındaki paketleri inceleyiniz.	➢ Aşağıdaki basit ağ yapısını oluşturup"Simulation" mod ile paketleri inceleyebilirsiniz. 

ÖLÇME VE DEĞERLENDİRME

Aşağıdaki soruları dikkatlice okuyunuz ve doğru seçeneği işaretleyiniz.

1. İnternet adreslerinin IP adreslerine çevrimini sağlayan sistemin adı nedir?
A) DNS
B) DHCP
C) TCP
D) UDP
E) FTP

2. Eğitim kuruluşların domain'i hangisidir?
A) edu
B) org
C) com
D) int
E) net

3. Veriyi bir uçtan diğerine iletmek için kullanılan protokol hangisidir?
A) DNS
B) DHCP
C) SMTP
D) POP3
E) FTP

4. FTP kaç numaralı portları kullanmaktadır?
A) 22 – 23
B) 20 – 21
C) 53 – 54
D) 80 – 8080
E) 21 – 22

5. TFTP hangi taşıma katmanı protokolünü kullanır?
A) UDP
B) TCP
C) DNS
D) FTP
E) DHCP

6. Web sayfalarını istemciye güvenli bir şekilde ulaştıran protokol hangisidir?
A) HTTP
B) SMTP
C) HTTPS
D) DHCP
E) TFTP

7. HTTPS istekleri kaç numaralı portu kullanır?
A) 80
B) 8080
C) 143
D) 443
E) 533

8. İstemcilere, IP adresi, ağ geçidi, ağ maskesi ve DNS sunucu adresi gibi parametreleri atamak için kullanılan protokol hangisidir?
A) DNS
B) FTP
C) TFTP
D) DHCP
E) IMAP4

9. Ağ cihazlarının yönetimi ve izlenmesi için kullanılan protokol hangisidir?
A) SNMP
B) SNTP
C) POP
D) UDP
E) TCP

10. İstemciler, POP3 sunucu ile iletişim kurmak için kaç numaralı portu kullanır?
A) 143
B) 112
C) 110
D) 115
E) 98

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

Ağ referans modellerinde katmanlar arasındaki ilişkiyi açıklayabileceksiniz.

ARAŞTIRMA

- Ağ referans modellerini araştırınız.
- Verinin, referans modeli katmanları arasında dolaşırken aldığı ek bilgileri araştırınız. Topladığınız bilgileri rapor haline getiriniz. Hazırladığınız raporu sınıfta öğretmeninize ve arkadaşlarınıza sununuz.

3. MODELLER VE PROTOKOLLER

3.1. OSI Modeli ve Katmanları

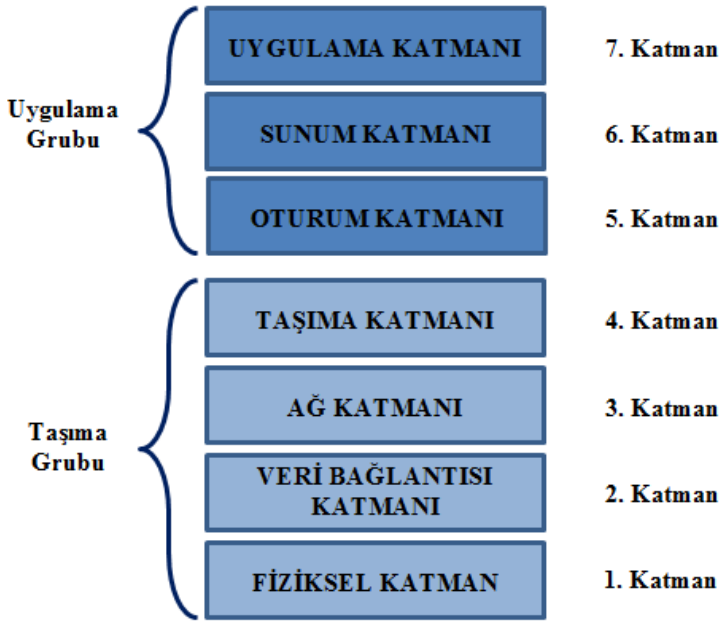
Bilgisayar ağları kullanılmaya başlandığı ilk zamanlarda sadece aynı üreticinin ürettiği cihazlar birbirleriyle iletişim kurabiliyordu. Bu da şirketlerin, tüm cihazlarını sadece bir üreticiden almalarını zorunlu kılıyordu. 1970'lerin sonlarına doğru ISO (International OrganizationforStandardization – Uluslararası Standartları Örgütü) tarafından, OSI (Open SystemInterconnection) modeli tanımlanarak bu kısıtlamanın önüne geçildi. Böylece farklı üreticilerden alınan cihazlar aynı ağ ortamında birbirleriyle haberleşebileceklerdi.

OSI modeli, 7 katmandan oluşmakta ve karmaşıklığı azaltmak, yeni standartlar geliştirmek amacıyla oluşturulmuştur.

OSI düzenlemelerinin en iyi fonksiyonlarından biri, tamamen farklı kullanıcı makineleri arasında veri transferine yardımcı olmasıdır. Yani, bir Unix host'u ve bir PC veya bir Mac arasında veri transferi yapılmasına izin verir.

Buna rağmen, OSI fiziksel bir model değildir. Daha çok uygulama geliştiricilerin, bir ağda çalışan uygulamaları oluşturmak ve tamamlamak için kullanabildikleri bir kurallar bütünüdür. Ayrıca, ağ kurulumu standartları, cihazlar ve ağlar arası iletişim planları oluşturmak ve tamamlamak için bir iskelet oluşturur.

OSI, temel olarak 2 gruba ayrılmış 7 katmana sahiptir. Üstteki üç katman, uç istasyonlardaki uygulamaların birbirleri ve kullanıcılar ile nasıl iletişim kuracaklarını açıklar. Alttaki dört katman, verinin uçtan uca nasıl aktarılacağını açıklar.



Resim 3.1: OSI referans modeli

3.1.1. Uygulama Katmanı

Kullanıcıların bilgisayarlar ile iletişime geçtiği ve kullanıcıya en yakın olan katmandır. Uygulama katmanı bilgisayar ile ağ arasında monitör görevi görür. Diğer katmanlarda olduğu gibi bir üst katmanı olmadığı için o katmana servis sağlaması gibi bir durum da söz konusu değildir. Uygulamaların ağ üzerinde çalışması bu katmandan kontrol edilir. HTTP, TELNET, SSH, DNS, DHCP, SMTP, SNMP, FTP, TFTP gibi protokoller bu katmana aittir.

3.1.2. Sunum Katmanı

Bu katmanda genel olarak yapılan iş, verinin diğer bilgisayarlar tarafından anlaşılabilir hâle gelmesini sağlamaktır. Verinin formatının belirlendiği katmandır. Ayrıca verinin sıkıştırılma, açılma ve şifrelenmesi gibi işlemlerin yapıldığı katmandır.

3.1.3. Oturum Katmanı

İki bilgisayar arasında oturumun kurulması, kullanılması ve sonlanması bu katmanda yapılır. Bu katman, cihazlar veya düğümler arasında diyalog kontrolü de sağlar. Üç farklı mod (simplex, halfduplex ve fullduplex) önererek sistem ve hizmetler arasındaki iletişimi koordine eder ve düzenler. Birden fazla bilgisayarla iletişim halinde olunması durumunda doğru bilgisayarla haberleşmeyi sağlar. SMB, NFS, ISO8326, ISO 8327 protokolleri bu katmana aittir.

3.1.4. Taşıma Katmanı

Taşıma katmanında üst katmandan gelen veri,segmentlere bölünür. Bu şekilde veri kaybı olması durumunda veriler daha küçük boyutlu olacağı içinverilerin tekrardan gönderilmesi daha kolay olur. Bu katmanda verinin uçtan uca iletimi sağlanır. Veri iletimi sırasında verinin iletilip iletilmediği bu katmanda kontrol edilir ve gerekirse tekrardan gönderilme işlemi bu katmanda yapılır. Bu katmanda çalışan TCP ve UDP en bilinen protokollerdir.

3.1.5. Ağ Katmanı

Ağ katmanı, verinin diğer ağlara gönderilmesi gerektiği durumda kullanılan IP adresinin eklendiği katmandır. Bu katmanda, verinin en iyi yoldan nasıl gönderileceği kararlaştırılır. Yönlendirme işlemi bu katmanda yapılan bir işlemdir. IP, ICMP ve ARPgibi protokoller bu katmanda görev yapar.

3.1.6. Veri Bağlantısı Katmanı

Bu katmanda fiziksel katmana ulaşım için protokoller vardır. Yani verinin fiziksel ortama akışını kontrol eden katmandır. Bu katmanda geçerli olan adres,MAC adresleridir. Yani ikinci katman cihazları MAC adresine göre anahtarlama yapar. Anahtar (Switch) ikinci katman cihazlarına örnektir. Bu katmanda akış kontrolü ile hatalı paketler kontrol edilip tekrar gönderilir. Ethernet, Token-Ring ve Wi-Fi bu katmanda çalışan protokollerdir.

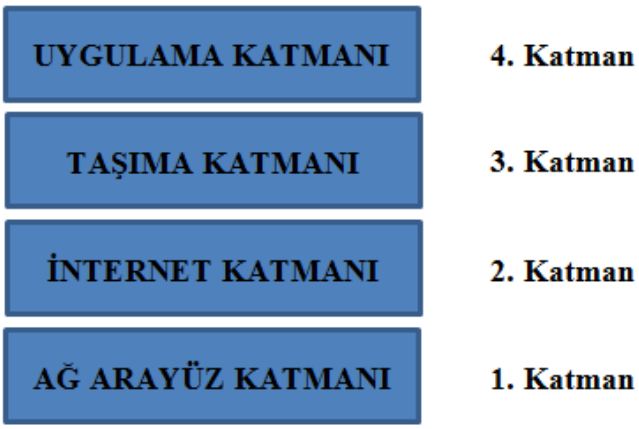
3.1.7. Fiziksel Katman

Fiziksel katman, adından da anlaşılabileceği gibi verinin fiziksel ortamlarda aktarımını sağlayan katmandır. Burada veri, bitler halinde gönderilir. Veri, farklı fiziksel ortamlarda gönderilebilir. Yani tüm başlıkları eklenmiş halde bulunan frameler elektrik, ışık veya dalga sinyalleri şeklinde gönderilebilir. Bu sinyallerin geçtiği fiziksel ortamlar da farklılık gösterir. Metal kablolar, fiber optik kablolar veya havadan kablosuz bir şekilde iletilebilir. Tüm bu işlemlerin olmasını sağlayan protokoller sadece fiziksel katmanda tanımlıdır. Bu katmanda çalışan cihaz olarak Dağıtıcı (Hub) örnek gösterilebilir. Dağıtıcı kendisine gelen sinyali tüm portlarına eşit bir şekilde iletir.

3.2. TCP/IP Modeli ve Katmanları

TCP/IP, DARPA (Defense Advanced ResearchProjectsAğency) ve Berkeley Software Distribution tarafından geliştirilen ve UNIX'de kullanılan bir protokoller grubudur. Günümüzde internetin temel protokolü olarak yerini almış TCP/IP'nin açılımı TransmissionControl Protocol / Internet Protocol'dür.

TCP/IP modeli, OSI modelinden çok daha önce standartlaştığı için OSI içinde referans olmuş 4 katmanlı bir yapıdır.



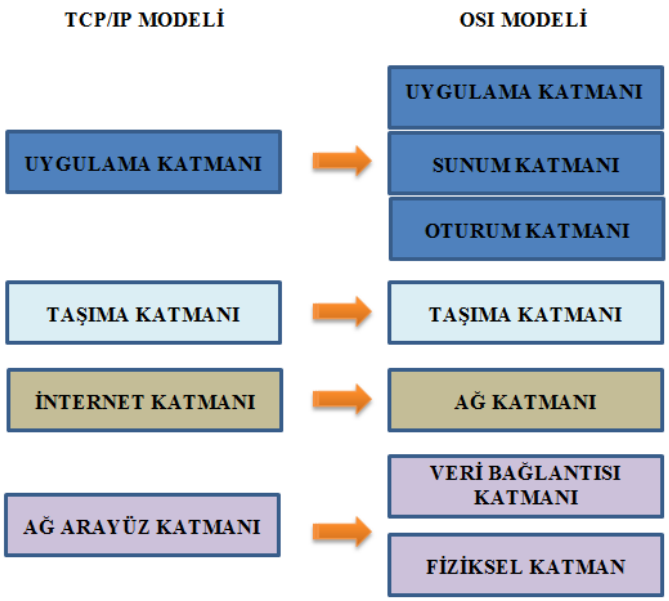
Resim 3.2: TCP/IP referans modeli

- **Uygulama katmanı:** OSI modelindeki Uygulama, Oturum ve Sunum katmanlarına karşılık gelmekte ve o katmanların işlevlerini yerine getirmektedir. Bu katmanda TFTP, FTP, SMTP, SNMP gibi protokoller çalışmaktadır.

- **Taşıma katmanı**: OSI modelindeki Taşıma katmanıyla birebir eşleştirilebilir. Bu katmanda iki farklı sınıfa ayrılabilecek iki protokol kullanılır. TCP ve UDP

- **Internet katmanı:** OSI modelindeki Ağ katmanına denktir ve adresleme, en iyi yol seçimi gibi işlevleri yerine getirir.Bu katmanda IP, ICMP,BOOTP, DHCP, ARP ve RARP gibi protokoller çalışmaktadır.

- **Ağarayüz katmanı:**OSI modelindeki Veri Bağlantısı ve Fiziksel katmana denkgelmektedir.



Resim 3.3: OSI ve TCP/IP referans modellerinin karşılaştırılması

3.3. Veri Paketleme

Veri paketleri her katmandan geçtikçe hem başına hem de sonuna gerekli eklemeler yapılır ya da içeriği değiştirilebilir. Bu noktada katmanların her biri (ister OSI modeli içinde olsun isterse TCP/IP içinde), verileri her seferinde bir parça değiştirir ve içeriğini bozmadan verilerin nereye gideceği, ne iş için kullanılacağı ya da hangi katmanda değerlendirilmesi gerektiği gibi bilgiler eklenir. TCP/IP protokolünün katmanlarından çıkan bir veri paketinin başlık kısmında, temelde port numarası, ulaşacağı IP adresi yazılıdır. Veri paketleri, OSI katmanlarında hareket ettikçe, değişikliğe uğrar.

Ethernet teknolojisiyle taşınacak IP paketleri artık Ethernet teknolojisi ile gönderilecek şekle dönüştürülür. Bu dönüştürme işlemi için IP paketleri Ethernet paketlerinin (EthernetFrame'lerinin) içine eklenir. Bu işleme ise (kapsülleme manasına gelen) encapsulation adı verilmiştir.

ARP işlemi ve ARP protokolünün getirdiği veriler ise Ethernet Frame'lerine eklenmektedir. IP paketinin başlığında hedef ve kaynak IP adresleri yazar, Ethernet Frame'inin başlığında ise hedef ve kaynak MAC adresleri yazmaktadır.

Veri paketleme 5 adımdan oluşur:

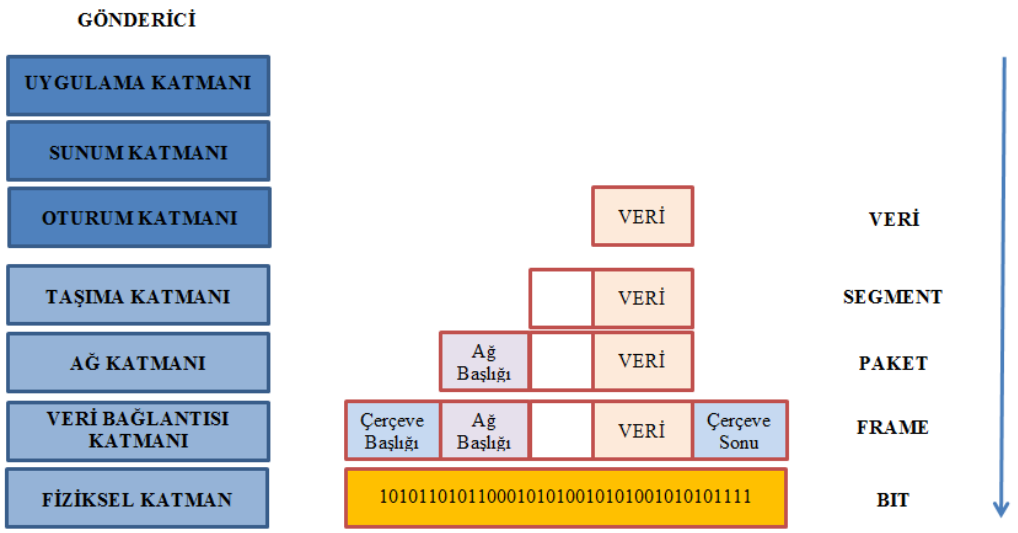
Uygulama, Sunum ve Oturum Katmanları kullanıcının girdiği veriyi 4. katman yani Taşıma katmanına kadar getirir.

Taşıma katmanı kendisine gelen bilgiyi segment adı verilen bölümlere ayırır ve verinin hangi protokolle gönderileceği (TCP - UDP) bilgisini de ekleyerek ağ katmanına gönderir.

Bu katmana gelen segment burada paketlere ayrılır ve IP başlığı denen, hedef ve kaynak IP'ler gibi bilgileri, bulunduğu başlığı ekleyerek bir alt katman olan Veri Bağlantısı katmanına gönderir.

Burada veri artık framelere çevrilir ve MAC adresleri eklenir.

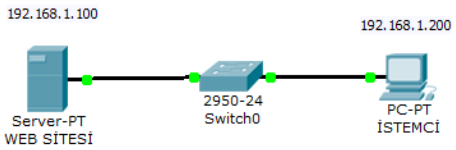
Frame yapısı katmanlara ayrılır ve iletilir.



Resim 3.4: Veri kapsülleme

UYGULAMA FAALİYETİ

Aşağıdaki işlem basamaklarını takip ederek faaliyeti gerçekleştiriniz.

İşlem Basamakları	Öneriler
➢ Ağ benzetim programı katmanlar arasındaki veri paketleme işlemini inceleyiniz.	➢ Aşağıdaki basit ağ yapısını oluşturunuz.  ➢ Ağ benzetim programında "Simulation" moduna geçiniz. ➢ Web sitesindeki sayfayı görüntülemek için istemcinin internet tarayıcısından web sitesinin IP adresini yazınız. ➢ İstemci ve web sitesinin birbirlerine gönderdikleri paketleri inceleyiniz. ➢ Verilerin katmanlar arasındaki değişimlerini inceleyiniz.

ÖLÇME VE DEĞERLENDİRME

Aşağıdaki soruları dikkatlice okuyunuz ve doğru seçeneği işaretleyiniz.

1. ISO tarafından 1970'lerin sonuna doğru tanımlanan ve 7 katmandan oluşan modelin adı nedir?
A) OSI
B) TCP/IP
C) IOS
D) FTP
E) TFTP

2. Hangisi Uygulama katmanında çalışan bir protokol değildir?
A) TELNET
B) DNS
C) FTP
D) SSH
E) TCP

3. İletilecek veya alınacak verinin formatının belirlendiği, sıkıştırılma, açılma ve şifrelenme gibi işlemlerin yapıldığı katman hangisidir?
A) Sunum Katmanı
B) Oturum Katmanı
C) Uygulama Katmanı
D) Taşıma Katmanı
E) Ağ Katmanı

4. İki bilgisayar arasındaki oturumun kurulması, kullanılması ve sonlanması işlemlerinin yapıldığı katman hangisidir?
A) Sunum Katmanı
B) Oturum Katmanı
C) Uygulama Katmanı
D) Taşıma Katmanı
E) Ağ Katmanı

5. Verinin başka ağlara gönderilebilmesi için IP başlığının eklendiği katman hangisidir?
A) Sunum Katmanı
B) Oturum Katmanı
C) Uygulama Katmanı
D) Taşıma Katmanı
E) Ağ Katmanı

6. Hangisi TCP/IP modelinin katmanlarından değildir?
A) Uygulama
B) Taşıma
C) İnternet
D) Veri Bağlantısı
E) Ağ Arayüz

7. Bir üst katmandan gelen veriler, Taşıma Katmanında bölündüğünde hangi isimle anılır?
A) Paket
B) Frame
C) Segment
D) Bit
E) Çerçeve

8. Bir üst katmandan gelen verilere, MAC adresi hangi katmanda eklenir?
A) Veri bağlantısı katmanı
B) Fiziksel katman
C) Ağ katmanı
D) Taşıma katmanı
E) Oturum katmanı

9. İletilecek verilere her katmanda bazı özel bilgilerin eklenmesi işlemine ne ad verilir?
A) Veri bağlantısı
B) Encapsulation
C) Frame
D) Ethernet
E) SYN flood

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. Ağ üzerindeki sunucunun bilgi veya hizmetini talep eden bilgisayara ne ad verilir?
A) İstemci
B) Sunucu
C) Server
D) Tablet
E) PDA

2. TCP başlık bilgisi kaç byte'tır?
A) 8
B) 16
C) 24
D) 32
E) 36

3. Saldırgan tarafından sunucuya çok fazla sayıda SYN isteği göndererek sunucu hizmetini engelleme saldırısına ne ad verilir?
A) ACK Saldırısı
B) SYN-ACK Saldırısı
C) Oltalama
D) Ortadaki Adam
E) SYN Saldırısı

4. Bilgisayardaki sadece açık ve dinlenen portları görüntülemek için hangi komut kullanılır?
A) netstat –an | find "established"
B) netstat –an | find /i "listening"
C) netstat –an
D) netstat
E) netstat –an | find "open"

5. Varsayılan olarak DHCP kaç numaralı portu kullanmaktadır?
A) 21
B) 22
C) 23
D) 55
E) 67

6. Ticari kuruluşların domain'i hangisidir?
A) edu
B) org
C) com
D) int
E) num

7. IP adresi girerek web sitesi adresi, web sitesi adresi girerek IP adresi sorgulaması yapmak için hangi komut kullanılır?
A) TRACERT
B) PING
C) IPCONFIG
D) NSLOOKUP
E) NETSTAT

8. Sunucunun aktif, istemcinin pasif olduğu FTP türü hangisidir?
A) TFTP
B) Pasif FTP
C) Aktif FTP
D) Etkin FTP
E) PFTP

9. E-posta yollamak için kullanılan protokol hangisidir?
A) POP3
B) SMTP
C) IMAP4
D) SNMP
E) HTTP

10. Uzak bir sunucuya güvenli bir bağlantı sağlamak ve iletişimi şifrelemek için kullanılan protokol hangisidir?
A) TELNET
B) SSH
C) FTP
D) DNS
E) DHCP

11. Kullanıcıların, bilgisayarlar ile iletişime geçtiği ve kullanıcıya en yakın olan OSI katmanı hangisidir?
A) Sunum Katmanı
B) Oturum Katmanı
C) Uygulama Katmanı
D) Taşıma Katmanı
E) Ağ Katmanı

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 modüle geçmek için öğretmeninize başvurunuz.

CEVAP ANAHTARLARI

ÖĞRENME FAALİYETİ-1'İN CEVAP ANAHTARI

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

ÖĞRENME FAALİYETİ-2'NİN CEVAP ANAHTARI

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

ÖĞRENME FAALİYETİ-3'ÜN CEVAP ANAHTARI

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

MODÜL DEĞERLENDİRME'NİN CEVAP ANAHTARI

1	**A**
2	**C**
3	**E**
4	**B**
5	**E**
6	**C**
7	**D**
8	**B**
9	**B**
10	**B**
11	**C**

KAYNAKÇA

- www.cizgi-tagem.org
- www.mshowto.org