T.C.
MİLLÎ EĞİTİM BAKANLIĞI

# MEGEP

(MESLEKİ EĞİTİM VE ÖĞRETİM SİSTEMİNİN
GÜÇLENDİRİLMESİ PROJESİ)

## BİLŞİM TEKNOLOJİLERİ

## TCP/IP İLETİM KATMANI

ANKARA 2008

Milli Eğitim Bakanlığı tarafından geliştirilen modüller;

- Talim ve Terbiye Kurulu Başkanlığının 02.06.2006 tarih ve 269 sayılı Kararı ile onaylanan, Mesleki ve Teknik Eğitim Okul ve Kurumlarında kademeli olarak yaygınlaştırılan 42 alan ve 192 dala ait çerçeve öğretim programlarında amaçlanan mesleki yeterlikleri kazandırmaya yönelik geliştirilmiş öğretim materyalleridir (Ders Notlarıdır).
- Modüller, bireylere mesleki yeterlik kazandırmak ve bireysel öğrenmeye rehberlik etmek amacıyla öğrenme materyali olarak hazırlanmış, denenmek ve geliştirilmek üzere Mesleki ve Teknik Eğitim Okul ve Kurumlarında uygulanmaya başlanmıştır.
- Modüller teknolojik gelişmelere paralel olarak, amaçlanan yeterliği kazandırmak koşulu ile eğitim öğretim sırasında geliştirilebilir ve yapılması önerilen değişiklikler Bakanlıkta ilgili birime bildirilir.
- Örgün ve yaygın eğitim kurumları, işletmeler ve kendi kendine mesleki yeterlik kazanmak isteyen bireyler modüllere internet üzerinden ulaşılabilirler.
- Basılmış modüller, eğitim kurumlarında öğrencilere ücretsiz olarak dağıtılır.
- Modüller hiçbir şekilde ticari amaçla kullanılamaz ve ücret karşılığında satılamaz.

# İÇİNDEKİLER

# AÇIKLAMALAR

| | |
|---|---|
| **KOD** | **481BB0061** |
| **ALAN** | **Bilişim Teknolojileri** |
| **DAL/MESLEK** | **Ağ İşletmenliği** |
| **MODÜLÜN ADI** | **TCP/IP ve IP Adresleme** |
| **MODÜLÜN TANIMI** | Bu modül; öğrencinin gerekli ortam sağlandığında, yönlendirme sorunlarını giderebileceği öğrenme materyalidir. |
| **SÜRE** | 40/24 |
| **ÖN KOŞUL** | "Yönlendiriciler-1 (Temel Yönlendirici Sorunları)" modülünü almış olmak |
| **YETERLİK** | TCP/IP protokol uygulamalarını yapmak |
| **MODÜLÜN AMACI** | **Genel Amaç**<br>Bu modül ile gerekli ortam sağlandığında, TCP/IP protokol uygulamalarını yapabileceksiniz.<br>**Amaçlar**<br>**1.** İletim katmanı protokollerini kavrayacak, servis saldırılarına karşı önlemler alabileceksiniz<br>**2.** İletim katmanındaki portları kavrayacak, portları test edebileceksiniz. |
| **EĞİTİM ÖĞRETİM ORTAMLARI VE DONANIMLARI** | Ağla birbirine bağlı bilgisayar laboratuvarı. |
| **ÖLÇME VE DEĞERLENDİRME** | Modül içinde yer alan her öğrenme faaliyetinden sonra verilen ölçme araçları ile kendinizi değerlendireceksiniz.<br>Modül sonunda kazandığınız bilgi ve becerileri belirlemek için öğretmeniniz tarafından hazırlanacak ölçme aracıyla değerlendirileceksiniz. |

# GİRİŞ

**Sevgili Öğrenci,**

Okul yaşantınızda öğreneceğiniz her konu, yaptığınız uygulama ve tamamladığınız her modül, bilgi dağarcığınızı geliştirecek ve ileride atılacağınız iş yaşantınızda size başarı olarak geri dönecektir. Eğitim sürecinde daha öz verili çalışır ve çalışma disiplinini kazanırsanız; başarılı olmamanız için hiçbir neden yoktur.

Günümüzde hepimiz öyle ya da böyle herhangi bir bilgisayar ağ ortamına bağlanıp bilgi alışverişinde bulunuyoruz. Bu süreçte bilgisayarımız yavaşlıyor, bilgilerimiz çalınıyor ya da daha büyük saldırılara maruz kalıyoruz. Çoğu zaman bu durumlara işletim sistemim çöktü, bilgisayarıma virüs bulaştı ya da bilgisayarımda trojen var diyerek bilgisayar sistemimizi en baştan kuruyoruz. Oysaki her gün yeni bir gelişme, yeni bir kod, yeni bir program, yeni açıklar ve yeni saldırı şekilleri öğrenip uygulamaya geçirmeye çalışıyoruz. Tüm bunları yaparken çoğumuz saldırı metotlarına kafa yorduğumuzdan savunmayı pek önemsemiyoruz. Daha doğrusu saldırının neden kaynaklandığını, niçin bilgisayarımızın saldırıya maruz kaldığını bilmiyoruz. Ağda bilgi alışverişi gerçekleşirken hangi süreçlerden geçtiğini bilirsek saldırılardan korunmak için doğru yöntemleri kullanabiliriz.

Bu modülle, TCP/IP iletim katmanı protokollerini, iletim portlarını ve servis saldırılarına karşı önlemler alabilmeyi öğreneceksiniz.

# ÖĞRENME FAALİYETİ-1

## AMAÇ

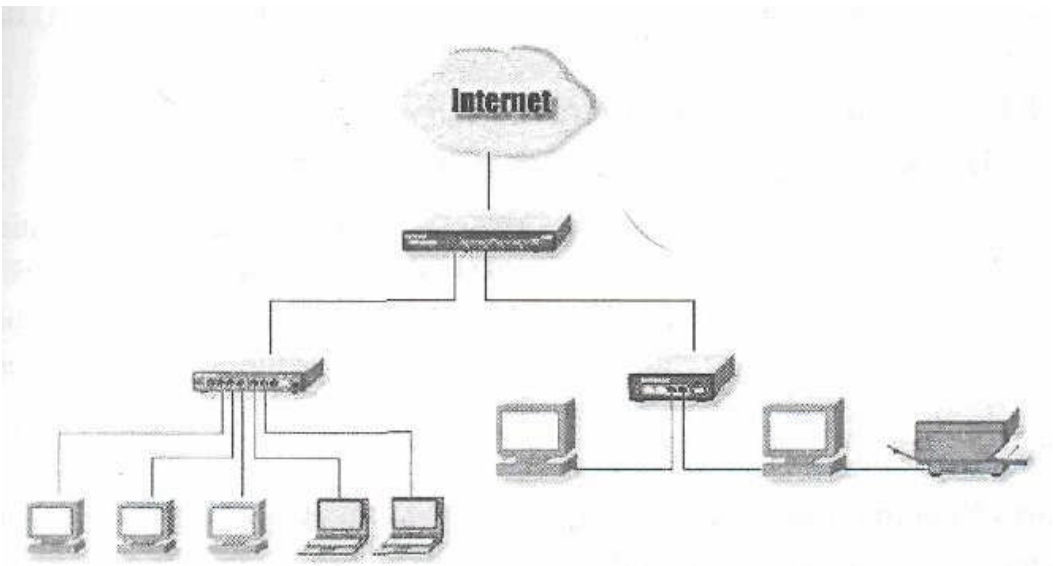
İletim katmanı protokollerini kavrayacak, servis saldırılarına karşı önlemler alabileceksiniz.

## ARAŞTIRMA

Bu faaliyet öncesinde yapmanız gereken öncelikli araştırmalar şunlardır:

- Bilgisayarınıza yerel bir ağ bağlantısı kurarken ağ bağlantısı ile ilgili özellikleri ve ne gibi ayarlar yapabileceğinizi araştırınız.
- Bilgisayarınıza TCP/IP protokolü kurarken işletim sisteminizin izin verdiği bağlantı kısıtlamaları nelerdir? Araştırınız.
- İnternette, bilgi alışverişinde bulunan bilgisayarların nasıl bilgi alışverişinde bulunduğunu ve veri akış kontrolünün nasıl ayarlandığını araştırınız.

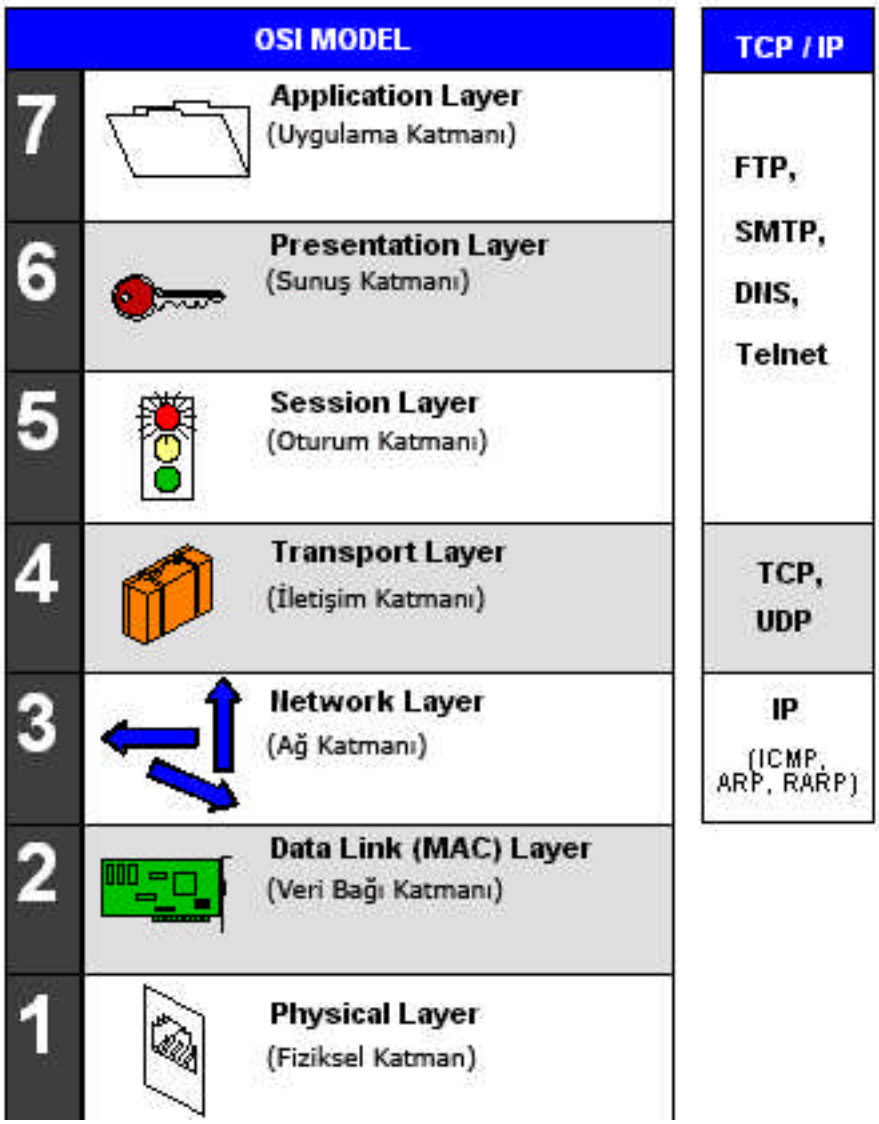
Araştırma işlemleri için İnternet ortamını kullanınız, okulunuzun bilgisayar laboratuvarında kullanılan ağ donanımlarını ve ağ ayarlarını inceleyerek ön bilgi edininiz.




**Şekil 1.1:Yerel Ağ ve İnternet**

# 1. İLETİM KATMANI PROTOKOLLERİ

TCP/IP protokolü OSI (Open Systems Interconnection-değişik işletim sistemine sahip makinelerin birbiriyle haberleşmesini sağlayan model) modeli içerisinde, uygulamalar arasında iletişimi sağlayan katmanı ( transmission layer) oluşturur. TCP/IP, TCP ve UDP olmak üzere data iletişimini farklı şekillerde sağlamakla görevli olan iki protokolü bünyesinde barındırır. TCP (Transmission Control Protocol); son uçtan son uca veri dağıtım fonksiyonu sağlar; verinin güvenli iletimi için gerekli mekanizmaları içerir. Bu mekanizmalar hata denetimi, sıra numarası, onay ve yeniden gönderim fonksiyonlarını içerir. TCP güvenli ve sıralı hâle getirilmiş veriyi uygulama katmanına sunar. UDP (User Datagram Protocol) ise; veri iletimi sırasında gönderilen bilgi paketlerinin hedef bilgisayarlara ulaşacağını garanti edemez ve akış kontrolü sağlayamaz. UDP, gönderilen paketlerin sadece belirli bir bilgisayarı hedef aldığı uygulamalarda kullanılmaktadır. Bu uygulamalardan bazıları: DNS, toplu yayın (broadcast) ve grup yayını (multicast) ve RIP protokolü uygulamalarıdır. TCP güvenli iletişim için birçok kontrolü mekanizmasını işletim sırasında devreye soktuğundan üzerinde çalıştığı kullanıcıya yük getirir ve iletişimde bir miktar gecikmeye neden olur. TCP ve UDP, İnternet protokolünün üzerinde çalışır ve bu protokol üzerinden aldığı hizmetlere işlevsellik kazandırır. TCP ve UDP protokollerini kullanarak uzaktaki makinelere doğrudan veri iletimi yapılmaz. Bunun yerine bilgisayarda çalışan uygulamalar arasında veri iletimi yapılır.




**Şekil 1.2 OSI Modeli ve TCP/IP Modeli Karşılaştırması**

Kısaca iletim katmanı; OSI modelindeki aktarım katmanının karşılığıdır. Temel fonksiyonu, uygulamalar arasındaki haberleşmeleri sağlamaktır. İnternet katmanı sadece bir veri dağıtım servisi sağlar. Aktarım katmanı ise güvenli iletişim, hata düzeltme, gecikme kontrolü ve benzeri fonksiyonlarla ilgilenir. Bu fonksiyonlarla uygulama katmanına servis sunar.

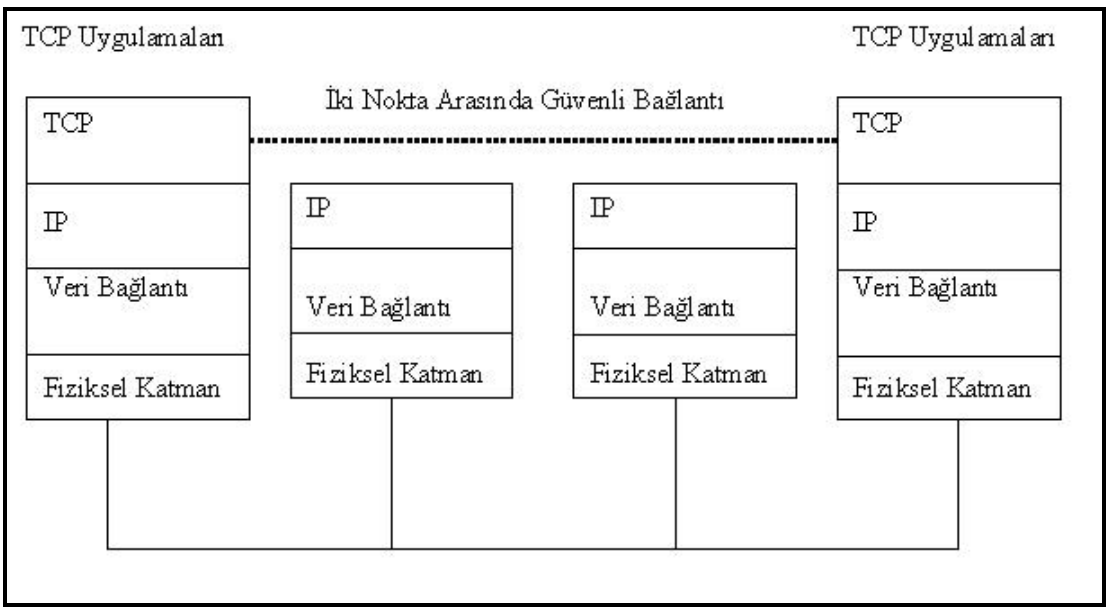
## 1.1. TCP

TCP yani Transmission Control Protocol yedi katmanlı OSI referans modelinin, aktarım katmanında yer alır. TCP iki hostun birbirleriyle güvenilir ve bağlantılı haberleşmesini sağlar. Telnet, FTP, SMTP gibi protokoller TCP' yi kullanır.

### 1.1.1. TCP Protokolünün Yapısı

TCP protokolü, bağlantılı ve güvenli veri akışını sağlayarak iletim katmanına çok önemli hizmetler sunar. Çoğu uygulama kendi veri iletişim kontrol mekanizmasını oluşturmaktansa TCP protokolünün sağlamış olduğu hizmetleri kullanır. TCP, sunduğu hata denetimi, veri akış kontrolü gibi hizmetler sayesinde kendisini kullanan uygulamalara tatmin edici düzeyde güvenlik, hata denetimi ve akış kontrolü sağlar.

TCP protokolü, bilgisayarlarda çalışan uygulamalar arasında <İstemci IP Adresi, Port Numarası>, <Sunucu IP Adresi, Port Numarası> ikililerini temel alan bağlantılar kurar. Her TCP bağlantısı, bu ikililerle ifade edilir. İnternet protokolü bağlantısızdır ve gönderilen paketlerin hedeflerine ulaşmalarını garanti edemez. Bu sorunları ortadan kaldırmak için TCP protokolüne ihtiyaç duyulur. Bu protokol, güvenli bilgi akışını sağlayabilmek için çeşitli yöntemler kullanır.




**Şekil 1.3: IP ağları arasında TCP protokolü işleyişi**

TCP en çok kullanılan, bağlantıda olan bilgisayarlar arasında güvenli veri iletişimi sağlayan, sanal devre bağlantısı mantığı ile çalışan iletim protokolüdür. TCP sıklıkla IPv4 ve IPv6 protokolleriyle beraber kullanılır. TCP çalıştığı bilgisayar ağı alt yapısından bağımsızdır. Ağ altyapısı ve mimarisi sadece veri iletim hızını etkiler.

TCP protokolünün en önemli özellikleri şunlardır:

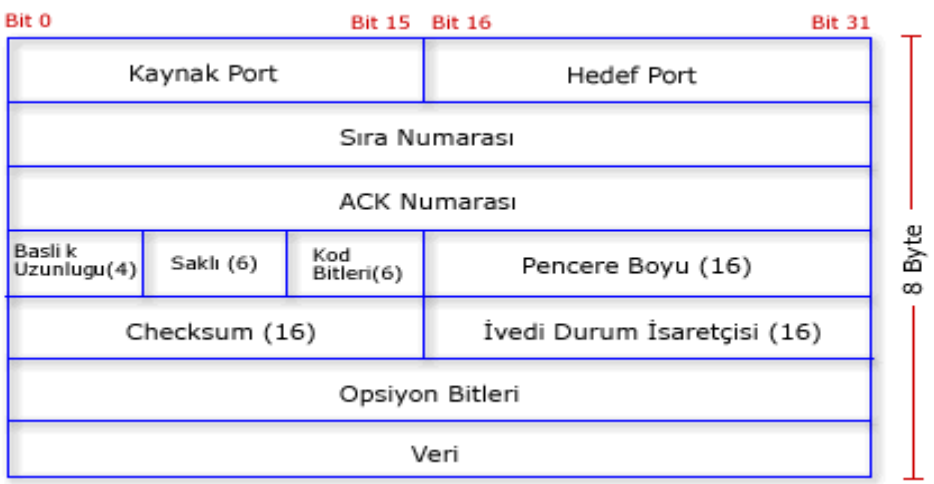
- Bağlantı noktaları arasında veri iletişimini sağlaması
- Güvenli veri iletimi sağlaması
- Bağlantıda olan iki bilgisayar arasında akış kontrolü sağlaması
- Çoklama (Multiplexing) yöntemi ile birden fazla bağlantıya izin vermesi
- Sadece bağlantı kurulduktan sonra veri iletimi sağlaması
- Gönderilen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

### 1.1.2. TCP ile İletişim

TCP'de tanımlı temel görevleri aşağıdaki gibi sıralayabiliriz:

- 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 dağıtımın sağlanması
- Hostlarda veri taşmasının önlenmesi

TCP kendisine atanmış olan bu görevleri yapabilmek amacıyla aktarım katmanında veri parçalarının önüne başlık bilgisi ekler. Başlık bilgisi ve veri parçası birlikte TCP segmenti olarak anılır. Her segmente sıra numarası verilir. Bu segmentler belli sayılarda gönderilir. Alıcı bilgisayar da frameler yani segmentler kendine ulaştıkça bunları tampon belleğine yerleştirir. İki ardışık çerçeve tampon belleğe yerleşince alıcı bilgisayar, gönderilen en son çerçeve için bir onay mesajını gönderici bilgisayara yollar. TCP segmentinde başlık içindeki alanların kullanımı amaçları aşağıdaki gibidir.




**Şekil 1.4: TCP segment formatı**

1. **Kaynak Port (Source Port):** Gönderen bilgisayarın kullandığı TCP portu. Bir üst katmanda TCP isteyen protokol sürecinin kimliği durumundadır. Karşı mesaj geldiğinde bir üst katmana iletmek için, o protokolün adı değil de port numarası kullanılır. 16 bitlik kaynak port alanı bulunur.

2. **Hedef Port (Destination Port):** Alıcı bilgisayarın kullandığı TCP portu. Gönderilen veri paketinin alıcı tarafta hangi uygulama sürecine ait olduğunu belirtir. Varış noktasındaki üst katman protokolünün portunu gösterir. 16 bitliktir.

3. **Sıra Numarası (Sequence Number):** Gönderilen paketin sıra numarasını gösterir. Gönderilmeden önce daha küçük parçalara ayrılan verinin, alıcı kısımda yeniden aynı sırada elde edilmesinde kullanılır. 32 bitliktir.

4. **ACK Numarası (Acknowledgment Number):** Gönderilen verinin en son hangi sekizlisinin alındığını göndericiye iletmek için kullanılır.

5. **Başlık Uzunluğu (Header Length):** TCP segmentinin uzunluğu, TCP başlığında var olan 32 bit uzunluğundaki sözcüklerin sayısını gösterir.

6. **Saklı Tutulmuş (Reserved):** İleride olabilecek genişleme için saklı tutulmuştur. Gelecekte kullanılmak üzere saklı tutulmuş anlamına gelir.

7. **Kod Bitleri (Bayraklar , Flags):** Kontrol bilgilerini taşımak için kullanılırlar. Segmentin içeriğine dair bilgi taşırlar.

8. **Pencere (Window):** TCP penceresinde ne kadar alan olduğunu gösterir. Alış denetimi için kullanılır. 16 bitliktir.

9. **Hata Sınama Bitleri (Cheksum):** Verinin ve başlığın hatasız aktarılıp aktarılmadığını sınamak için kullanılır. 16 bitliktir.

10. **Acil İşaretçisi (Urgent Pointer):** Acil olarak aktarımı sonlandırma, bayraklar kısmında acil olan bir verinin iletilmesi gibi durumlarda kullanılır. Acil veri, alıcının uygulama katmanında öncelikle değerlendirmesi gereken veridir.

TCP protokolü İnternette kullanılan ana protokoldür. Dosya transferi ve uzak oturumlar gibi kritik işleri sağlar. TCP diğer protokollerden farklıdır. Güvensiz bir iletişim ortamında verilerin aynı şekilde hedefe ulaşacağından emin olamazsınız. Ancak TCP gönderilen verilerin gönderildiği sırayla karşı tarafa ulaşmasını sağlayarak güvenli veri iletimini sağlar.

TCP iki makine arasında kurulan sanal bir bağlantı üzerinden çalışır. Üç kısımlı bir işlemden oluşur. Bu bağlantı ve three-part handshake olarak bilinir. (TCP/IP three way

handshake) TCP/IP üzerinde yapılan bazı saldırı tekniklerini iyi anlayabilmek için TCP'nin çalışma mantığını iyi anlamak gerekmektedir.

Three-way handshake işleminde öncelikle istemci sunucuya port numarasıyla birlikte bir bağlantı isteği gönderir. İsteği alan sunucu bu isteğe bir onay gönderir. En sonunda da istemci makine sunucuya bir onay gönderir ve bağlantı sağlanmış olur. Bağlantı yapıldıktan sonra veri akışı her iki yönde de yapılabilmektedir. Buna genellikle full-duplex iletişim denmektedir.

TCP aynı zamanda hata kontrol mekanizması da sağlıyor. Gönderilen her veri bloğu için bir numara üretilmektedir. Karşılıklı iki makine de bu numarayı kullanarak transfer edilen blokları tanımaktadır. Başarılı olarak gönderilen her blok için alıcı makine, gönderici makineye bir onay mesajı gönderir. Ancak transfer sırasında hata olursa alıcı makine ya hata mesajları alır ya da hiçbir mesaj almaz. Hata oluştuğu durumlarda, oturum kapanmadığı sürece, veriler tekrar gönderilir.

TCP protokolü ile verinin iki makine arasında nasıl transfer edildiğini gördük. Şimdi istemcinin isteğinin karşı tarafa ulaştığında ne olup bittiğine bakalım. Bir makine başka bir makineye bağlantı isteği gönderdiği zaman belli bir hedef adresi belirtir. Bu adres bir IP adresi ve fiziksel adrestir. Ancak sadece bu adreste yeterli değildir, istemci karşı makinede hangi uygulamayla konuşmak istediğini de belirtmek durumundadır.

Connection-oriented veri iletiminde gönderilen veri paketler kullanıcıya aynı düzende ve güvenli bir şekilde iletilmelidir. Eğer herhangi bir paket kaybolur, zarar görür, aynısı gönderilir veya alıcı tarafından aynı düzende alınamazsa protokol başarısız olmuş sayılır. Bunun en kolay çözüm yolu ise her gönderilen paketten sonra bir sonraki paketin bilgisini alıcıya göndermektir.

Eğer gönderici her gönderilen paketten sonra diğer paketin bilgisini gönderirse bu iş/zaman oranında önemli ölçüde düşüşe neden olur. Birçok Connection-oriented güvenlik protokolü, ağ üzerinden iletişim zamanın çok önemli olduğundan aynı anda birden fazla paket gönderir. Alıcı tarafından alınan bu paketlerden sonra gönderilen paketlerin tümü ile alakalı olan bir bilgi alıcıya gönderilir. İşte buna pencere boyutu veya pencereleme denilir.

Bir cihazdan diğer bir cihaza güvenli bir iletişim veri tekrarlaması veya kaybı olmadan veri dizisinin iletimini garanti eder. Pozitif bilgilendirme verinin güvenli bir şekilde iletildiğini garanti eden bir tekniktir. Bu teknikte belirli sayıda veri paketleri gönderildikten sonra alıcı tarafından paketlerin güvenli bir şekilde alındığı kaynağa iletilir. Kaynak cihaz, bu bilgilerin tamamını tutar ve istenmeyen bir durum olduğunda hedef kaynağa paketlerin yeniden gönderilmesi için başka bir bilgi paketi göndererek verinin tamamı düzgün gelene kadar bu işlem sürer.

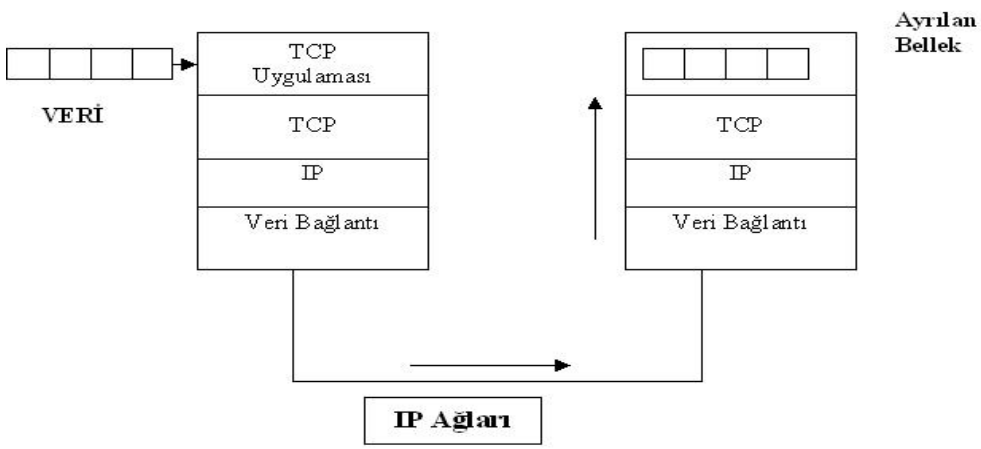
### 1.1.3. Veri Transferi

TCP protokolünün en önemli özelliği sürekli ve her iki yönde veri akışını sağlamasıdır. Gönderilen veriler 8 bitlik (oktet) gruplar hâlindedir. Bu veriler, bağlantıda

olan sistemlerde yürütülen TCP protokolünü işleten uygulamalara parçalar hâlinde iletilir. Mesaj parçaları değişik uzunluklarda olabilir. Bu parçalar gönderilebilecek en büyük parça değerini aşmayacak uzunlukta olmalıdır. TCP protokolünde mesaj uzunluğunu sınırlandıracak herhangi bir kısıtlama yoktur. Gönderilen datagramların uzunluğunu sınırlamak IP katmanının görevidir. Bu nedenle TCP protokolü, bağlantıların daha etkin ve verimli olabilmesi için "MSS" (Maksimum Segment Size-En büyük Parça Büyüklüğü) için bir değer belirlemek zorundadır. MSS gönderilecek en büyük parça büyüklüğüdür. Kurulan her bağlantı için tanımlanır.

TCP protokolünde gönderilen mesaj segmentleri sekiz bitlik veriler hâlindedir. TCP protokolü gönderilen ve alınan her biti işaretleyerek takip eder. İşaretleyerek gönderdiği her parça için bağlantıda olduğu uçtan cevap bekler. Bu işaretleme sistemi sayesinde iletim sırasında kaybolan parçalar yeniden transfer edilebilir. Çoklama (Multiplexing) yöntemi ile TCP, iki bilgisayar arasında birden fazla bağlantı kurabilir. Bu protokol her büyüklükte verinin gönderilmesi için uygundur. Gönderilen paketler sadece bir oktetlik veri içerebileceği gibi, paketler 100 mega oktetlik veri transfer işleminde de kullanılabilir. TCP gönderdiği her okteti numaralandırır. Bu numaralar kullanılarak gönderilen verilerin gönderildiği sıra ile bağlantıda olan alıcı tarafından alınması sağlanır. Buna (sequencing of oktet) alınan oktetlerin sıralanması adı verilir.

Uygulamalar TCP protokolünü kullanarak, her defasında birden fazla oktet içeren segmentler gönderebilir. TCP aldığı bu mesaj segmentlerini depolar; bunları tek bir parça veya parçalar hâlinde gönderir. TCP protokolü ilettiği verinin gönderdiği sıra ile alınmasını garanti etmek zorundadır. Örneğin TCP uygulamasının 1024 oktetlik veri yollaması gerekirse, bu bilgiler 1024 tane 1 oktetlik veya 256 tane 4 oktetlik parçalar hâlinde gönderilebilir.




**Şekil 1.5: İnternet protokolü kullanımı ile veri iletimi**

TCP protokolü verileri sıra ile dizilmiş bilgiler hâlinde iletir. Gönderilen oktetlerde mesajın sonu olduğunu anlatacak herhangi bir belirteç yoktur. Tüm verilerin gönderildiğini

TCP modülüne anlatabilmek için, TCP protokolünün “push” fonksiyonunu kullanması gerekir. “Push” fonksiyonu alınan paketin bir üst katmana iletilmesini sağlar.

TCP tarafından gönderilen verilerin herhangi bir yapısal özelliği yoktur. TCP protokolü, gönderilen verilerin yapısı hakkında herhangi bir bilgiye sahip değildir. Protokol veritabanı bilgileri veya şifrelenmiş veriler taşıyabilir. Yapısal olarak bu verilerin hangi uygulamalara ait olduğunu belirleyemez. Bu, ancak TCP protokolü kullanan uygulamalar tarafından sağlanabilir. Alınan verileri çözümleyen uygulamalar bu bilgileri kendi içlerinde kullanacakları şekillere uyar.

TCP protokolünün en önemli özelliği iki nokta arasında güvenli bağlantı sağlamasıdır. Bunun için TCP zarar görmüş, kaybolmuş, iki defa gönderilmiş ve düzenli sıraya göre gönderilmemiş datagramlarla uğraşmak ve bu hatalardan kaynaklanan sorunları gidermek zorundadır. Bunun için TCP “Pozitif Bilgilendirme Şeması” (Positive Acknowledgement Scheme) olarak bilinen PAR yöntemini kullanır. Alınan her veri parçasına karşılık bir bilgi paketi gönderilir.

TCP protokolü, gönderdiği her veriye karşılık bir dizi numarası (sequence number) yaratır ve buna karşılık gönderdiği her veri mesajına karşılık bir bilgi numarası (acknowledgement number) bekler. Eğer gönderdiği veriye karşılık belirlenen süre (timeout süresi) sonunda bilgi (ACK) alamazsa, paketi yeniden göndermek durumunda kalır. Gönderilen verilere dizi (sequence) numarası atanması, verilerin belirli bir sıra hâlinde gönderilmesini ve iki defa yinelenmesini önler. Gelen paketlerdeki herhangi bir bozulma TCP başlığında yer alan “kontrol toplamı değeri” alanından (TCP header checksum) tespit edilir. Alınan paketlerdeki kontrol toplam alanı (checksum) geçerli değilse paketler önemsenmez ve kullanıma konulmaz.

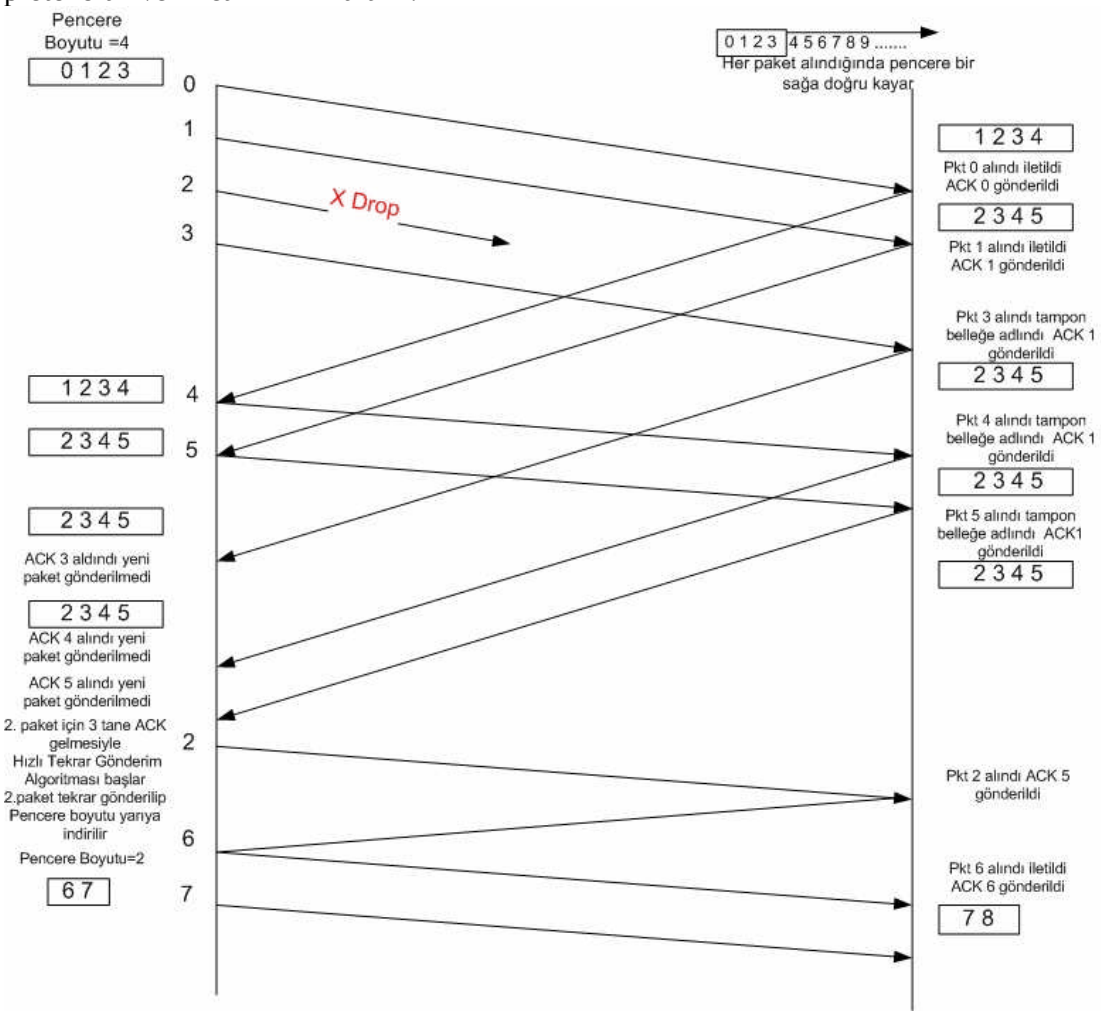
### 1.1.4. Akış Kontrolü

İletim katmanı veri gönderirken güvenlikli olduğu için hiç veri kaybolmaz. Alıcı kullanıcı veriyi aldığında güvenlik protokolleri nedeniyle veriyi hemen işleyemez. TCP kullanılarak gönderilen veride bunlar olurken UDP kullandığımız takdirde daha az güvenlik ihtiyacı olan veriler gönderilir ve güvenlik protokolleri kullanılmadığı için alıcı veriyi daha kolay işleyerek kullanıcını üzerindeki yükü azaltır ve daha hızlı veri transferi sağlar.

TCP protokolü, veri parçalarını alan ve gönderen bilgisayarlar CPU hızı ve ağ bant genişliği gibi nedenlerden dolayı farklı hızlarda çalışabilirler. Bu nedenle, veri gönderen bilgisayarın karşı tarafın baş edemeyeceği hızda bilgi akışı sağlaması olasıdır. TCP akış kontrolü mekanizması ile gönderilen verinin miktarını kontrol eder. Protokol, kayan pencere (sliding window) tekniği kullanarak bağlantıda olan bilgisayarların senkronize olarak veri alışverişi yapmasını sağlar. TCP protokolünde akacak olan her veri oktetler (8 bitlik gruplar) halinde numaralandırılır. Oktetlere verilen her numaraya dizi numarası (sequence number) denir.

Alıcı, gelen verileri aldıktan sonra karşı tarafa bilgi paketi ile beraber, kabul edebileceği büyüklükteki dizi (sequence) numarasını gönderir. Kabul edilebilir dizi (sequence) numarası aralığına pencere (window) denir. Pencere, karşı taraftan gönderme izni

alındıktan sonra göndericinin iletebileceği oktet sayısını belirler. Böylece gönderici verilerin alındığına dair bilgi mesajı almadan belirtilen miktarda veri transfer edebilir. Bu da protokolün veri iletim hızını artırır.



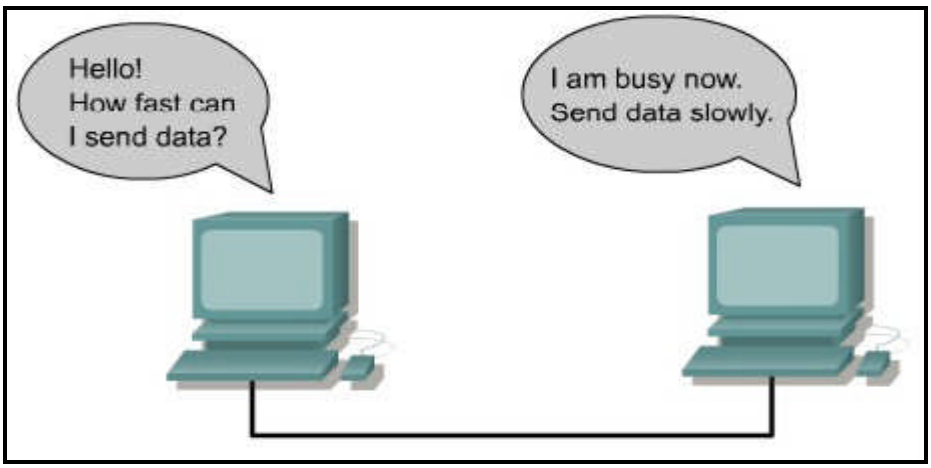

**Şekil 1.6: Pencereleme**

TCP veri akış kontrol mekanizması şöyle özetlenebilir:

1. Pencere alanı dışında solda yer alan oktetler gönderilmiş ve cevap alınmış oktetlerdir.
2. Pencere alanı içinde yer alan oktetler beklenilmeden yollanabilecek oktetlerdir. Pencere içindeki oktetlerin bir bölümü gönderilmiş ve yanıt bekliyor olabilir. Diğer oktetler ise gönderilmeyi bekleyen oktetlerden oluşabilir.
3. Pencere alanı dışında sağ tarafta yer alan oktetler pencere alanı içine girmediği sürece gönderilmeyecek olan oktetlerdir.

Pencere alanı, alıcının alınacak olan veri için ayırdığı bellek (buffer) büyüklüğünü bildirir. Eğer bellek dolarsa alıcı daha küçük pencere alanı ayırır. Bazı durumlarda

gönderenin sadece bir oktet gönderilmesinin istenmesi de olasıdır. Bu duruma " silly window syndrome" denir.




**Şekil 1.7: Akış Konrolü**

### 1.1.5. Servis Saldırıları

Bilgisayar ağlarında, istenmeyen bir bilgisayar, ağ iletişimini kullanarak bilgisayar hafızasını ele geçirebilir. Servis hareketlerinin reddedilmesi (DoS), sunucuların iletişim kurma çabalarını reddetmek amacı ile dizayn edilmiştir. DoS (Denial Of Services) hareketlerinin genel yöntemi hackerların sistem cevaplarından yararlanmaktır. Bu senkronizasyon taşması olarak da bilinir. DoS açılımı Denial Of Services olan bu saldırı çeşidi bir hizmet aksatma yöntemidir. Bir kişinin sisteme arka arkaya yaptığı saldırılar sonucunda hedef sistemin hiç kimseye hizmet veremez hâle gelmesi veya o sisteme ait tüm kaynakların tüketimini amaçlayan bir saldırı çeşididir.

DoS saldırılarında saldırgan, senkronizasyonu başlatır. Fakat kaynak adresini kandırırlar. Kandırmalar, alım sürecinde kullanılarak, mevcut olmayan cihaz yanıtları, ulaşılamayan IP adresleri gibi sorunlar oluşturur. Ondan sonra olayı başlatan kimsenin onay verilerinin bitmesi için durum-bekle politikası uygulanır. Gerçek olmayan aygıtın bir şeye cevap verdiği dönemdir, ulaşılamayan bir adrestir. Başlangıçtan en son onaylama olmayı beklerken bekleme durumunda konumlanır. Bekleme isteği kuyruk bağlantısında ve hafızadaki tutma bölgesinde konumlanır. Bu bekleme durumu, aygıtın hafıza gibi sistem kaynaklarına saldırmasını sağlar. Bağlantı süresi bitene kadar bekleme işlemine devam eder. Saldırganlar sahte senkronizasyon ile sunucuya saldırıları başlatacaklardır. Tekrar kaynaklara bağlanarak sahte bağlantılar için beklerler.

Bu saldırılara karşı korunmak için sistem yöneticileri zaman dışı iletişim sürecini artırabilirler ve iletişim kuyruk büyüklüğünü artırabilirler. Ayrıca bu tip saldırılardan korunmak için ve savunmaya yönelik ölçümü başlatmak için yazılımlar mevcuttur. Bu tür yazılımlara Firewall (Güvenlik Duvarı) adı verilmektedir. Masaüstü bilgisayarlara kurulan güvenlik duvarı, bilgisayara İnternet ve/veya yerel ağ üzerinden gelen ve bilgisayardan İnternet'e ve/veya yerel ağa gönderilen paketleri, kendi tanım dosyasında bulunan güvenlik

sorunu oluşturan paketlerle karşılaştırır ve bunlar arasından sorunlu olanları kullanıcıya haber verir. Güvenlik duvarı, dışardan bilgisayara gelen ve bilgisayardan dışarıya giden tüm paketleri inceler. Güvenlik duvarı sayesinde o anki TCP/IP/UDP gelen giden paketleri izleyebilme, saldırganın IP'sini görme gibi bilgilere ulaşılmasını sağlar. Firewall'un güzel bir tarafı da bilgisayarımızın dışarıyla/yerel ağla haberleşmesini sağlayan portları kontrol etmeyi sağlamasıdır. Nette kullanmayacağımız, işimize yaramayacak portları Firewall ile kapatmalıyız. Saldırgan, sistemlere saldıracağında öncelikle port taraması yöntemini kullanacaktır. Sizin açık portlarınız, eğer kapatmadıysanız gözükecek ve saldırgan bu port üzerinden size bağlanmaya çalışacaktır. Günümüzde Zone Alarm, MCAfee, Kaspersky, Norton İnternet Security gibi birçok firewall programı kullanılmaktadır. Bunun dışında Windows XP işletim sisteminin içinde de bir güvenlik duvarı mevcuttur.

Bir de DDoS (Distributed Denial Of Services) saldırı çeşidi vardır. Bir saldırgan daha önceden tasarladığı birçok makine üzerinden hedef bilgisayara saldırı yaparak hedef sistemin kimseye hizmet veremez hâle gelmesini amaçlayan saldırı çeşididir. Koordineli olarak yapılan bu işlem, hem saldırının boyutunu artırır hem de saldırıyı yapan kişinin gizlenmesini sağlar. Bu işlemleri yapan araçlara zombi denir. Bu saldırı çeşidinde saldırganı bulmak zorlaşır. Çünkü saldırının merkezinde bulunan saldırgan, aslında saldırıya katılmaz. Sadece diğer IP numaralarını yönlendirir. Eğer sadece tek bir IP adresinden yapılırsa bir Firewall bunu rahatlıkla engelleyebilir. Fakat saldırının daha yüksek sayıdaki IP adresinden gelmesi Firewall'ın devre dışı kalmasını sağlar. İşte bu özelliği onu DoS saldırısından ayıran en önemli özelliğidir.

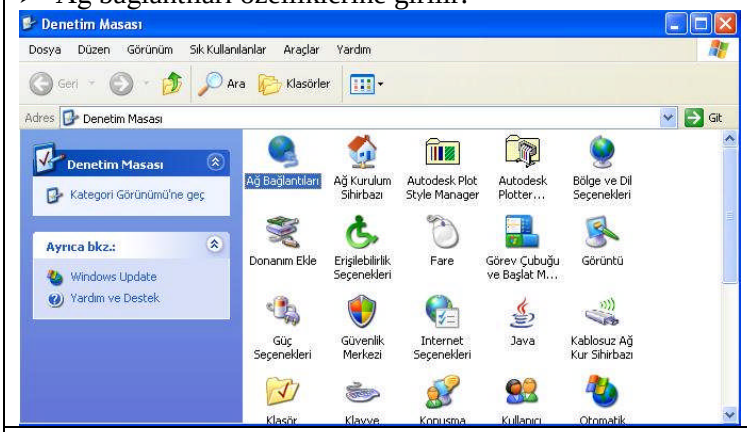
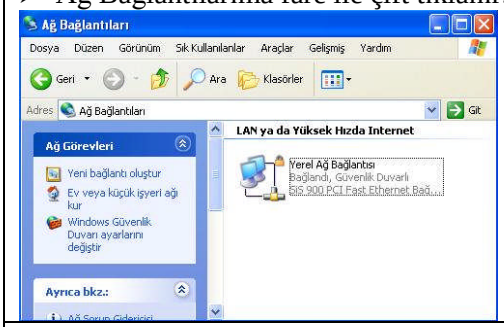
Şimdi bilgisayarımızı bir ağ ortamına dâhil ederek önce TCP/IP yükleyelim, ardından güvenlik duvarı ayarını yapalım. Daha önceki derslerinizde de gördüğünüz gibi bilgisayarımızı ağ ortamına dâhil etmek için Ethernet kartı, switch ya da hub, cat5 kablo yardımı ile ağa bağlayabiliriz.

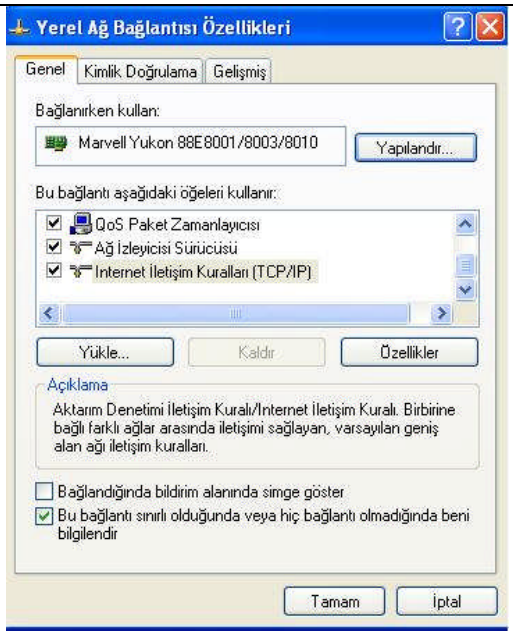
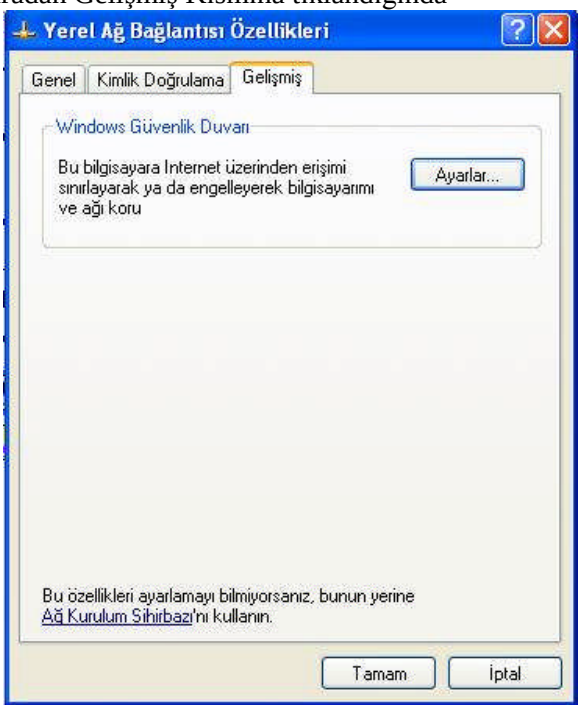
Basit TCP/IP Hizmetlerini yüklemek için

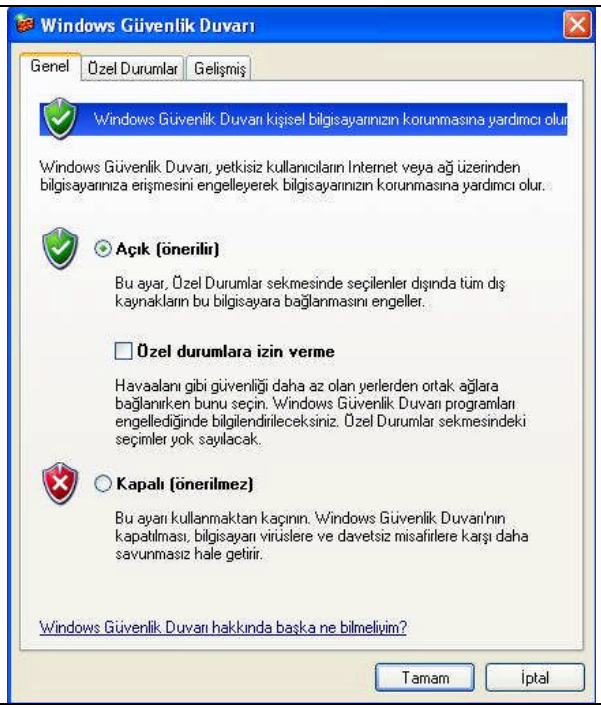
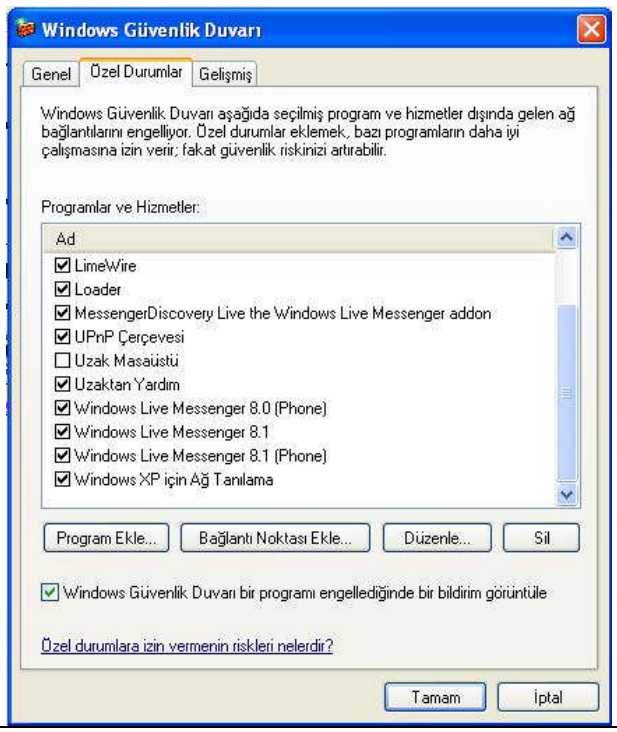
1. Denetim Masası'nda **Program Ekle/Kaldır'ı** açın.
2. **Windows Bileşenlerini Ekle/Kaldır**'ı tıklatın.
3. **Bileşenler**'den **Ağ Hizmetleri**'ni ve sonra da **Ayrıntılar**'ı tıklatın.
4. **Ağ Hizmetleri**'nde, **Basit TCP/IP Hizmetleri**'ni seçin ve **Tamam**'ı tıklatın.
5. **İleri**'yi tıklatın.
6. İstenirse, dağıtım dosyalarının bulunduğu yolu yazın ve sonra **Tamam**'ı tıklatın.
7. **Son**'u sonra da **Kapat**'ı tıklatın.

Şimdi bilgisayarımızdaki Windows güvenlik duvarı ayarlarının nasıl yapıldığına bir bakalım:

## UYGULAMA FAALİYETİ

| İşlem Basamakları | Öneriler |
|---|---|
| ➢ Ağ bağlantıları özelliklerine girilir.<br>  | ➢ Denetim Masasından Ağ Bağlantılarına tıklayarak gelebilirsiniz. |
| ➢ Ağ Bağlantılarıma fare ile çift tıklanır.<br>  | |
| ➢ Yerel Ağ Bağlantısı seçeneğine gelindiğinde, fare sağ tuş ile özellikler seçeneğine tıklanır. | ➢ Özellikler sekmesine tıklandığında yandaki resimde görünen ekran karşımıza gelecektir. Aynı işlemi **Denetim Masasından Güvenlik Duvarı** seçeneğinden de yapabilirsiniz. |

<table>
<tr>
<td> 
</td>
<td></td>
</tr>
<tr>
<td>➢ Buradan Gelişmiş Kısmına tıklandığında<br> 
</td>
<td>➢ Bilgisayarımız internete bağlandığında istediğimiz programlara; internet üzerinden erişim verip istediğimizi sınırlandırabiliriz. Bu işlemi başka bir firewall programı kullanarak da yapabilirsiniz.</td>
</tr>
<tr>
<td>➢ Ayarlar kısmına tıkladığımızda Windows Güvenlik Duvarı ile ilgili seçenekler karşımıza gelecektir.</td>
<td>➢ Buradaki ayarları yaparken Açık işaretlenmesi tavsiye edilir. Böylece</td>
</tr>
</table>

<table>
<tr>
<td></td>
<td> 
</td>
<td>bilgisayarımızda herhangi bir firewall programı olmasa da kısmen güvenliliğini sağlamış oluruz.</td>
</tr>
<tr>
<td>➢ Buradan istediğimiz programlara izin vermek ya da kısıtlamak için Özel Durumlar sekmesini seçmemiz gerekir.<br> 
</td>
<td>➢ Bu işlemi CMD (komut istemi) kısmından da yapabiliriz. Hangi programın hangi portu kullandığını biliyorsanız o portu açıp kapatarak da aynı işlemi gerçekleştirmiş olursunuz.<br>➢ Ayrıca burada Bağlantı Noktası Ekle seçeneğini de kullanarak TCP ya da UDP bağlantı noktası ekleyebilirsiniz.</td>
</tr>
</table>

## 1.2. UDP (User Datagram Protocol)

UDP, TCP / IP protokol grubunun iki aktarım katmanı protokolünden birisidir.

Gelişmiş bilgisayar ağlarında paket anahtarlamalı bilgisayar iletişiminde bir data gram modu oluşturabilmek için UDP protokolü yazılmıştır. Bu protokol minimum protokol mekanizmasıyla bir uygulama programından diğerine mesaj göndermek için bir prosedür içerir. Bu protokol 'transaction' yönlendirmelidir.

- 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 geçek zamanlı veri transferinin servis kalitesi TCP'nin oluşturduğu yüksek veri trafiği nedeniyle azalır.

UDP'yi kullanan genel protokoller DNS, TFTP, ARP, RARP ve SNMP protokolleridir. Uygulama programcıları birçok zaman UDP'yi TCP'ye tercih eder. Çünkü ağ üzerinde fazla bant genişliği kaplamaz.

UDP güvenilir olmayan bir aktarım protokolüdür. UDP protokolü ağ üzerinden paketi gönderir ve gidip gitmediğini takip etmez. Paketin yerine ulaşıp ulaşmayacağına onay verme yetkisi yoktur.

UDP protokolü basit bir protokol olduğu için hızlı iletişim kurmamız gereken yerlerde kullanmamız yararımıza olacaktır. Buradaki basitlikten kasıt TCP protokolü gibi verinin gönderilmesi gibi kontrolleri içermediği içindir. UDP protokolünü kullanan programlara örnek olarak 161 nu.lu portu kullanan SNMP servisini verebiliriz.


**Şekil 1.8: UDP segment formatı**

UDP datagramların belirli sıralara konmasının gerekli olmadığı uygulamalarda kullanılmak üzere dizayn edilmiştir. 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 sefer protokol 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 içerdiği için doğal olarak UDP başlığı TCP başlığına göre daha kısadır. Başlık, kaynak ve varış port numaraları ile kontrol toplamını içeren tüm bilgidir.

## ÖLÇME VE DEĞERLENDİRME

# OBJEKTİF TESTLER (ÖLÇME SORULARI)

**Aşağıdaki soruları dikkatlice okuyarak seçenekli sorularda uygun şıkkı işaretleyiniz. Boşluk doldurmalı sorularda boşluklara uygun cevapları yazınız.**

**1.** Aşağıdakilerden hangisi UDP için geçerli değildir?

**A)** UDP protokolü, veri iletimi sırasında gönderilen bilgi paketlerinin hedef bilgisayarlara gönderileceğini garanti edemez.

**B)** UDP protokollerini kullanarak uzaktaki makineden doğrudan veri iletimi yapılamaz.

**C)** UDP, gönderilen paketlerin sadece belirli bir bilgisayarı hedef aldığı uygulamalarda kullanılmaktadır.

**D)** UDP veri alışverişinde güvenli veri akışı gerçekleştirir.

**2.** Aşağıdakilerden hangisi TCP'yi kullanmaz?

**A)** Telnet

**B)** DNS

**C)** SMTP

**D)** FTP

**3.** Aşağıdakilerden hangisi TCP protokolünün özelliklerindendir?

I. Güvenli veri iletimi sağlaması

II. Sadece bağlantı kurulduktan sonra veri iletimi sağlaması

III. Birden fazla bağlantıya izin vermemesi

IV. Bağlantıda olan iki bilgisayar arasında akış kontrolü sağlaması

**A)** I-II

**B)** I-II-III

**C)** I-II-IV

**D)** I-III-IV

**4.** TCP penceresinde ne kadar alanın olduğunu aşağıdakilerden hangisi gösterir?

**A)** Kod Bitleri(Bayraklar)

**B)** Saklı Tutulmuş

**C)** Başlık uzunluğu

**D)** Pencere(Window)

**5.** Aşağıdaki eşleştirmeden hangisi doğrudur?

**A)** Sıra Numarası (Sequence Number)- 32 Bit

**B)** Hata Sınama Bitleri (Checksum)- 32 Bit

**C)** Kod Bitleri (Bayraklar)- 16 Bit

**D)** Onay Numarası (Acknowledgement Number)- 16 Bit

**6.** TCP protokolünde gönderilen mesaj verileri kaç bitliktir?

**A)** 8
**B)** 16
**C)** 32
**D)** 4

**7.** TCP protokolünde mesaj uzunluğunu sınırlandıracak herhangi bir kısıtlama yoktur. Gönderilen datagramların uzunluğunu sınırlamak ……. katmanının görevidir.

**8.** ……..…… olan bu saldırı çeşidi bir hizmet aksatma yöntemidir.

**9.** Hizmet aksatma saldırılarından korunmak için …… kullanılır.

## DEĞERLENDİRME

Cevaplarınızı cevap anahtarı ile karşılaştırınız. doğru cevap sayınızı belirleyerek kendinizi değerlendiriniz. Yanlış cevap verdiğiniz ya da cevap verirken tereddüt yaşadığınız sorularla ilgili konuları faaliyete dönerek tekrar inceleyiniz.

Tüm sorulara doğru cevap verdiyseniz diğer faaliyete geçiniz.

# ÖĞRENME FAALİYETİ-2

## AMAÇ

İletim katmanındaki portları kavrayacak, portları test edebileceksiniz.

## ARAŞTIRMA

- Bu faaliyet öncesinde yapmanız gereken öncelikli araştırmalar şunlardır:
- Bilgisayarınız herhangi bir ağa bağlandığında hangi portların aktif olduğunu araştırınız.
- Bilgisayarınız ağa bağlı iken hangi portlarda hangi IP numaralar olduğunu tespit etmek için neler yapılabilir araştırınız.

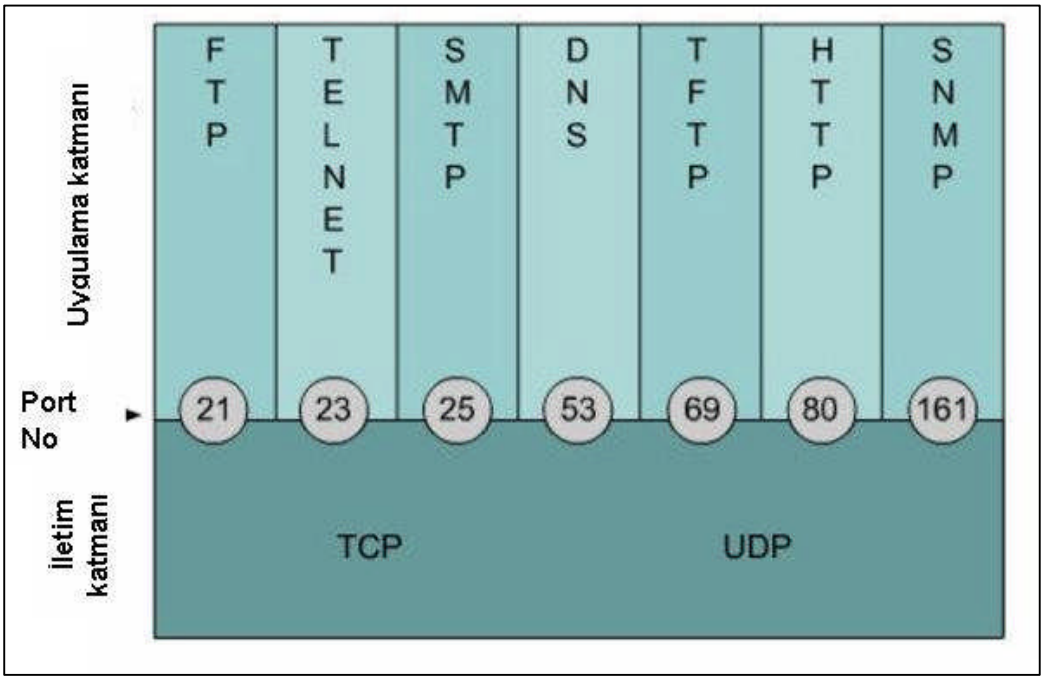
Araştırma işlemleri için İnternet ortamını kullanınız, okulunuzun bilgisayar laboratuvarında kullanılan ağ donanımlarını ve ağ ayarlarını inceleyerek ön bilgi edininiz.

# 2. İLETİM KATMANI PORTLARI

## 2.1. İletim Katmanı Servisleri

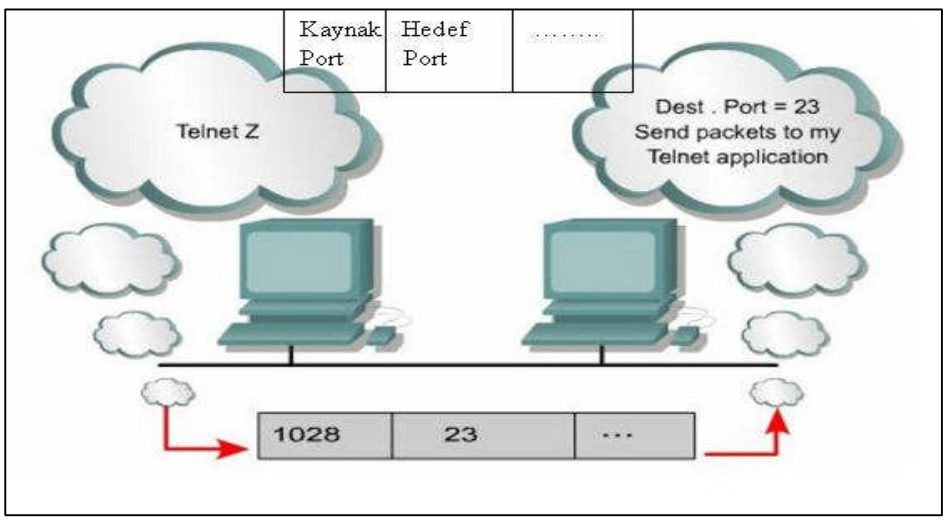
TCP protokolü, tek bir makine üzerinden birçok TCP servisi sunulmasını sağlar. Bu sayede ağlarda binlerce bilgi paketi, yüzlerce birbirinden farklı servise taşınmaktadır. Genellikle sunucular, paketlerin adreslenmesi için adreslerde çok az problem yaratan çapraz servisler kullanır. Eğer sunucu SMTP ve WWW'nin her ikisini çalıştırıyorsa, o servisin istediği bölgeyi belirlemede kullanılır. Sadece sunucu IP adresleri için paket oluşturulamaz. Çünkü hedef, servisin ne olduğunu bilemez. Port numaraları, sunucular arasındaki diyalog ile ilişkilendirilmiş olmalıdır. Sunucuda uygun servislerde paket ulaştırılabilir. İstemcinin e-mail, web sayfalarını gözlemleme gibi işlemleri kısa bir sürede bir sunucu kullanarak yapmaya gücü yetmez. İletim katmanı uygulamaları için ayrılmış metotlar kullanılmalıdır.

İletim katmanında sunucular, TCP/IP ile ilişkilendirilmiş portları çalıştırırlar. Aynı zamanda ağda farklı çapraz diyalogları yakalamak için port numaraları kullanılır. Port numaralarına, sunucu çoklu servis çalıştıran sunucularla iletişime geçtiği zaman ihtiyaç duyulur. TCP ve UDP'nin ikisi de port ve soket numaralarını üst katmanın bilgilerine geçmek için kullanır. FTP (File Transfer Protocol-Dosya Aktarım Protokolü) uygulamasını standart olarak 21 numaralı porttan kullanır.




**Şekil 1.1:TCP port numaraları**

Veri alışverişi uygulamaları ile iyi bilinen port numaralarını karıştırmazlar. Özel bir sıra içerisinden karışık olarak seçilmişlerdir. Port numaraları TCP parçasında kaynak ve hedef adresleri kullanır.




**Şekil 2.2: TCP veri iletimi**

Port numaraları aşağıdaki görev dizisindedirler:

- 255'ten aşağı numaralar halka açık uygulamalar için ayrılmıştır.
- 255t'ten 1023 e kadar olan numaralar satılabilir uygulamalar için şirketlere ayrılmıştır.
- 1023'ten yukarı düzenlenmemiştir.

Son sistemler uygun uygulamalarda seçilen port numaralarını kullanır. Kaynak port numaraları sunucu tarafından dinamikleştirilir. Genellikle 1023'ten büyük numaralardır. Port numaraları 0-1023 arasında ise Internet Numara Yetkilendirme Dairesi (IANA) tarafından kontrol edilir.

Posta ofisi kutu numaraları, port numaraları için iyi bir benzetmedir. Mesajın bir kısmı posta şehir koduna, şehre ve posta kutusuna gönderilebilir. Şehir kodu ve şehir, posta kutusuna mektubun doğru bir şekilde gelmesini sağlar. Posta kutusu, mektubun adreslendiği yere ulaşmasını sağlarken, posta ve şehir kodu genel mesaj seklinde yollanır.

Posta numaraları için iyi bir ön sıralamadır. Mesajın bir kısmi posta, şehir koduna gönderilebilir. Posta kutusu mailin adreslendiği yere ulaşmasını sağlarken, posta ve şehir kodu genel mesaj seklinde yollanır. Benzer olarak IP adresleri doğru server'a gönderilir fakat TCP ve UDP numaraları paketlerin doğru başvuruya geçtiğini garantiler. Benzer olarak IP adresleri paketleri doğrudan sunucuya gönderir. Fakat TCP ya da UDP port numaraları paketlerin doğru uygulamaya garantili bir şekilde geçmesini sağlar.

## 2.2. Servis Portları

Port numaraları, servisler sunucularda çalışırken iletişimde bulunabilmeleri için gereklidir. Servisler uzaktaki sunucuya bağlantı istedikleri zaman iletim katmanı protokolü ve portları kullanmak isteyecektir. Bazı portlar RFC 1700'ün içinde tanımlıdır. TCP ve UDP her ikisinin içerisinde saklanmış iyi bilinen portlardır.

| Decimal | Keyword | Description |
|---|---|---|
| 0 | | Reserved |
| 1-4 | | Unassigned |
| 5 | RJE | Remote Job Entry |
| 7 | ECHO | Echo |
| 9 | DISCARD | Discard |
| 11 | USERS | Active Users |
| 13 | DAYTIME | Daytime |
| 15 | NETSTAT | Who is Up or NETSTAT |
| 17 | QUOTE | Quote of the day |
| 19 | CHARGEN | Character Generator |
| 20 | FTP-DATA | File Transfer Protocol (data) |
| 21 | FTP | File Transfer Protocol |
| 23 | TELNET | Terminal Connection |
| 25 | SMTP | Simple Mail Transfer Protocol |
| 37 | TIME | Time of Day |
| 39 | RLP | Resource Location Protocol |

**Şekil 2.3:Servis Portları**

Çok sık kullanılan portlar uygulamalarda tanımlanmıştır. İletim katmanı protokollerinin üstünde çalışabilir. Örnek verecek olursak; sunucular FTP servisini kullanırken TCP bağlantılarını 20.portu kullanarak iletirler ve 21.porttan FTP uygulamalarını gerçekleştirirler. Alışveriş başladığında yolda sunucu, uzaktaki kullanıcının hangi servisi kullanmak istediğine karar verir. TCP ve UDP iletimde doğru servise karar vermek için port numaralarını kullanırlar.

| Decimal | Keyword | Description |
|---|---|---|
| 42 | NAMESERVER | Host Name Server |
| 43 | NICNAME | Who Is |
| 53 | DOMAIN | Domain Name Server |
| 67 | BOOTPS | Bootstrap ProtocoalServer |
| 68 | BOOTPC | Bootstrap Protocol Client |
| 69 | TFTP | Trivial File Transfer Protocol |
| 75 | | Any Private Dial-out Service |
| 77 | | Any Private RJE Service |
| 79 | FINGER | Finger |
| 80 | HTTP | HyperText Transfer Protocol |
| 95 | SUPDUP | SUPDUP Protocol |
| 101 | HOSTNAME | NIC Host Name Server |
| 102 | ISO-TSAP | ISO-TSAP |
| 110 | POP3 | Post Office Prorotol for client to retrieve mails from mail server |
| 113 | AUTH | Authentication Service |
| 117 | UUCP-PATH | UUCP Path Service |

**Şekil 2.4: Servis portları**

## 2.3. İstemci Portları

İstemciler, sunuculardaki servislere bağlanmak durumunda kaldığında kaynak ve hedef portları belirtmek zorundadır. TCP ve UDP parçaları kaynak ve hedef portları belirtmek için alan bulundurur. Hedef portları ya da servisin herkesin bildiği çok kullanılan portlar tanımlanır.

İstemciler genelde kaynak portları 1023'den yukarı olan karışık olarak seçerek tanımlar. Mesela; istemci iletişim kurmak istediğinde web sunucusu ile TCP'yi kullanırken 80.portu kullanır ve kaynak portu ise 1045'tir. Paket sunucudan vardığında iletim katmanından geçmiş demektir. Sonunda http servisi ile 80.portta işletilir. http sunucu istemcilere 80.portu kullanarak cevap verir. Hedef olarak 1045 portu kullanılır. Alışveriş yapılırken yolda sunucular ve servisler ilişkilendirildikleri portları kullanırlar.

| Kaynak Portu | | | Hedef Portu |
|---|---|---|---|
| Sıra Numarası | | | |
| Alındı Bilgisi Numarası | | | |
| Veri Ofseti (4Bit) | Ayrılmış Bit (6Bit) | Bayraklar (6Bit) | Pencere (16Bit) |
| Kontrol Toplamı (16Bit) | | | Acil İşaretciler (16Bit) |
| Opsiyonlar-Değişkenler (32Bit) | | | |
| Veri | | | |
| ..... | | | |

**Tablo 2.1:TCP'de gönderilen Bilgi Paketi**

## 2.4. Port Numaraları

TCP katmanı içindeki veya dışındaki herhangi bir communication circuit (iletişim merkezi) iki numaranın birleşmesinden oluşan socket numaraları tarafından tanımlanır. Bu numaralar makinenin IP adresi ve TCP yazılımı tarafından kullanılan port numarasıdır.

Port numaraları, TCP ve UDP parçaların çerçevelerinde 2 bayt ile ifade edilir. Bu 16 bit değerine denk gelmektedir. Port numaraları 0'dan 65535'e kadar değişmektedir. Aralarında iletişim olan makinelerde korunan bir port tablosu vardır. Bu tabloda iletişimde bulunan makinelerin kaynak ve hedef port numaraları karşılıklıdır. Port numaraları üç farklı kategoriye bölünmüştür:

- **İyi bilinen portlar**: İlk 1023 port en çok bilinen portlardır. Ağ servislerinde iyi bilindikleri için bu isim kullanılmıştır.FTP, Telnet ya da DNS gibi.
- **Kayıtlı portlar**: 1024'ten 49151'e kadar kayıtlı portlardır.
- **Dinamik ya da özel portlar:** 49152 ile 65535 arasındaki portlardır.

| Ağ Servisi | PORT NO |
|---|---|
| FTP veri transferi | TCP Port 20 |
| FTP kontrol | TCP Port 21 |
| Telnet | TCP Port 23 |
| SMTP | TCP Port 25 |
| DNS | UDP Port 53 |
| http | TCP/UDP Port 80 |
| POP3 | TCP Port 110 |
| SHTTP | TCP/UDP Port 443 |

**Tablo 2.2: TCP port numaraları**

Port numaraları sunucular arasındaki çoklu oturumlar ortaya çıkabildiği için kullanılırlar. Kaynak ve hedef port numaraları soketten ağ adresleri ile bütünleşiktir. Soket çiftleri her sunucuda bir tanedir. Örneğin bir telnet bağlantısı için port 23'tür. Bazı zamanlar Net'te gezerken port 80 olabilir. IP ve MAC adresleri aynı olabilir. Çünkü paketler aynı sunucudan gelebilir. Bu yüzden diyalog kaynakta kendi port numarasına ihtiyaç duyabilir. Her server yanıtlarken kendi port numarasına ihtiyaç duyabilir.

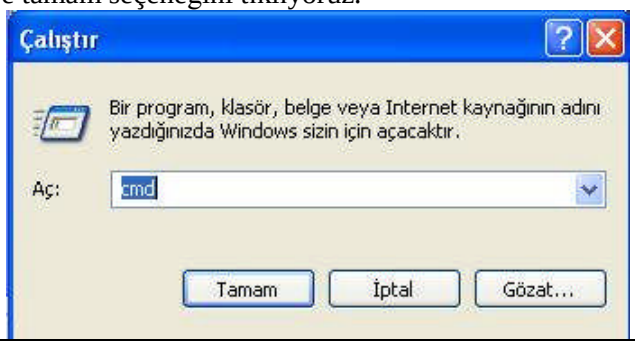
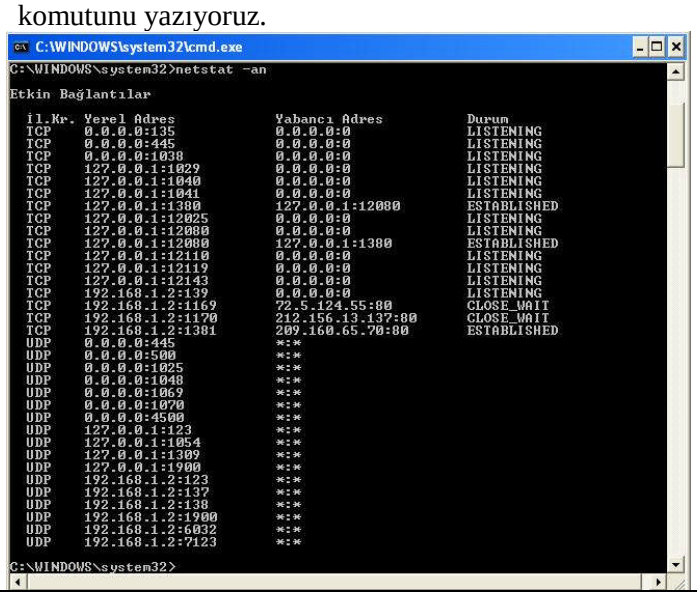
Örneğin bir mektupta adresler isim, sokak, şehir ve ülkeyi barındırır. Ağ verisi için port, MAC ve IP adresleri kullanarak karşılaştırma yapabiliriz. Port numarası ismi, Mac adresi sokak adresini, şehir ve ülke adresini de IP adresi olarak düşünelim. Çoklu mektuplar sokak adreslerine, şehir ya da ülkeye gönderilebilir. Fakat mektuplardaki alıcıların isimleri farklıdır. Örneğin elimizde bir adrese Baki SAKALLI ve Fevzi SAKALLI adına iki mektup gönderilmiş olsun. Bunu farklı port numaralarına benzetebiliriz.

Bilgisayarımız herhangi bir ağa bağlandığında etkin TCP bağlantılarını, bilgisayarın bağlı olduğu bağlantı noktalarını (port) görebilmemiz mümkündür. Bunu birtakım programlar yapabildiği gibi cmd (dos ekranı) de "netstat" komutuyla da görebiliriz. Komut satırında yürütülen "netstat" komutu etkin TCP bağlantılarını, bilgisayarın bağlı olduğu bağlantı noktalarını, Ethernet istatistiklerini, IP yönlendirme tablosunu, IP, ICMP, TCP ve UDP iletişim kuralları için IPv4 istatistikleri ile IPv6, ICMPv6, IPv6 üzerinden TCP ve IPv6 iletişim kuralları üzerinden UDP için IPv6 istatistiklerini görüntüler. Parametreler olmadan kullanılan "netstat", etkin TCP bağlantılarını görüntüler.

Şimdi netstat komutunu kullanarak bilgisayarımızdaki etkin TCP bağlantılarını görüntüleyelim.

## UYGULAMA FAALİYETİ

Aktif portları tespit etmek

| İşlem Basamakları | Öneriler |
|---|---|
| ➢ Öncelikle bilgisayarımızın Başlat seçeneğinden Çalıştır komutunu tıklıyoruz. | |
| ➢ Buradan Dos komut istemcisini açmak için cmd yazıyoruz ve tamam seçeneğini tıklıyoruz.   | |
| ➢ Karşımıza gelen ekrana "netstat –an" ya da "netstat" komutunu yazıyoruz.   | ➢ Aynı işlemi herhangi bir firewall ya da IP numarası izleyen programlar (xns5,ipscan vs.) yardımı ile yapmak mümkündür. |

Burada;

**"Proto"** ("İl.Kr.") başlığı altındaki karakterler ilgili port için kullanılan protokol tipini gösterir.

**"Local Address"** (Yerel Adres) ise bilgisayarınızın ağ üzerindeki isminin yanı sıra gelen bağlantıları kabul ettiğiniz ve rastgele üretilen port numarasını gösterir.

**"Foreign Address"** (Yabancı Adres) kısmı ise uzak bilgisayarın adını ve bağlantıyı gerçekleştirmek için kullandığı port numarasını gösterir.

Adından da anlaşılacağı üzere "State" (Durum) bağlantının durumunu gösterir. Bu başlık altında görülebilecek durumlar şunlardır:

- ESTABLISHED - İki bilgisayar da bağlı.
- CLOSING - Uzak bilgisayar bağlantıyı kapatmaya karar vermiş.
- LISTENING - Bilgisayarınız gelen bir bağlantı isteği için bekliyor.
- SYN_RECV - Uzak bir bilgisayar bağlantı isteğinde bulunmuş.
- SYN_SENT - Bilgisayarınız bağlantı isteğini kabul etmiş.
- LAST_ACK - Bilgisayarınız bağlantıyı kapatmadan önce paketleri siliyor.
- CLOSE_WAIT - Uzak bilgisayar bilgisayarınızla olan bağlantıyı kapatıyor.
- FIN_WAIT 1 - Bir istemci bağlantıyı kapatıyor.
- FIN_WAIT 2 -İki bilgisayar da bağlantıyı kapatmaya karar vermiş.

**Komutun Parametreleri**

Netstat [-a ] [-e ] [-n ] [-o ] [-p Protokol] [-r ] [-s ] [Aralık]

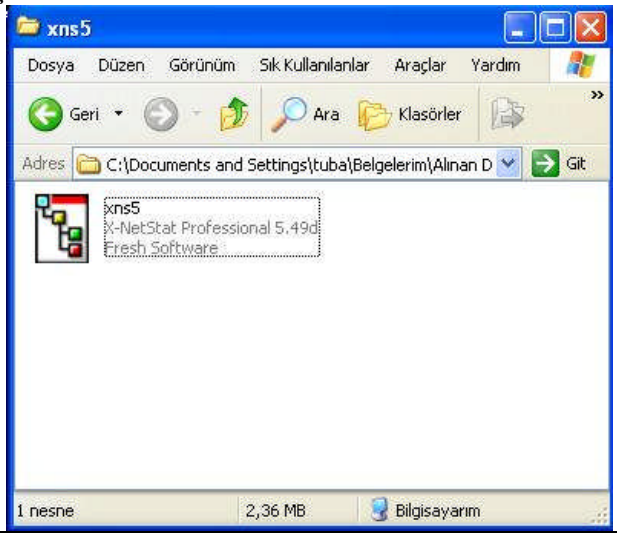
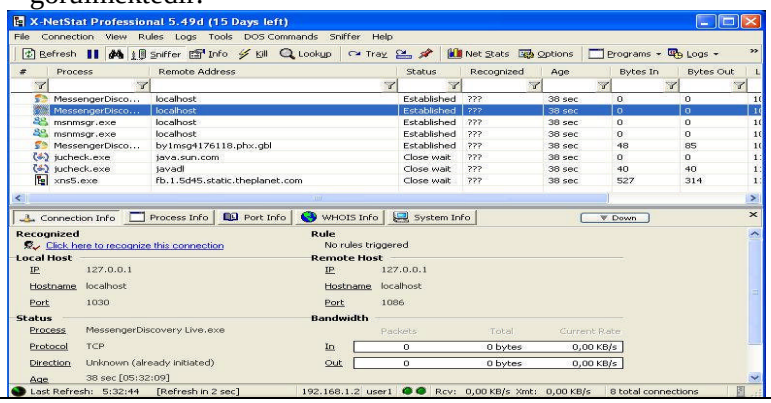
| |
|---|
| **-a** |
| Tüm etkin TCP bağlantılarıyla birlikte, bilgisayarın bağlı olduğu TCP ve UDP bağlantı noktalarını görüntüler. |
| **-e** |
| Gönderilen ve alınan bit ve paket sayısı gibi, Ethernet istatistiklerini görüntüler. Bu parametre -s ile birleştirilebilir. |
| **-n** |
| Etkin TCP bağlantılarını görüntüler. Ancak adresler ve bağlantı noktası numaraları sayısal olarak ifade edilir, herhangi bir ad konulmaz. |
| **-o** |
| Etkin TCP bağlantılarını görüntüler ve her bağlantının işlem kimliğini (PID) içerir. Uygulamaları PID'e göre bulmak istiyorsanız, Windows Görev Yöneticisi içindeki İşlemler sekmesine bakın. Bu parametre -a , -n ve -p ile birleştirilebilir. |
| **-p İletişim Kuralı** |
| İletişim Kuralı tarafından belirlenmiş iletişim kuralı bağlantılarını gösterir. Bu durumda İletişim Kuralı; tcp, udp, tcpv6 veya udpv6 olabilir. Bu parametre, iletişim kuralına göre istatistikleri görüntülemek üzere -s ile birlikte kullanılırsa, İletişim Kuralı; tcp, udp, icmp, ip, tcpv6, udpv6, icmpv6 veya ipv6 olabilir. |
| **-s** |
| İletişim kuralına göre istatistikleri gösterir. Varsayılan olarak, TCP, UDP, ICMP ve IP iletişim kuralı istatistikleri gösterilir. IPv6 protokolü yüklü ise, IPv6 üzerinden TCP istatistikleri, IPv6, ICMPv6 ve IPv6 protokolleri üzerinden UDP istatistikleri gösterilir. -p parametresi bir küme iletişim kuralını belirtmek için kullanılabilir. |
| **-r** |
| IP yönlendirme tablosunun içeriğini görüntüler. Bu, "route print" komutu ile eş değerdir. |

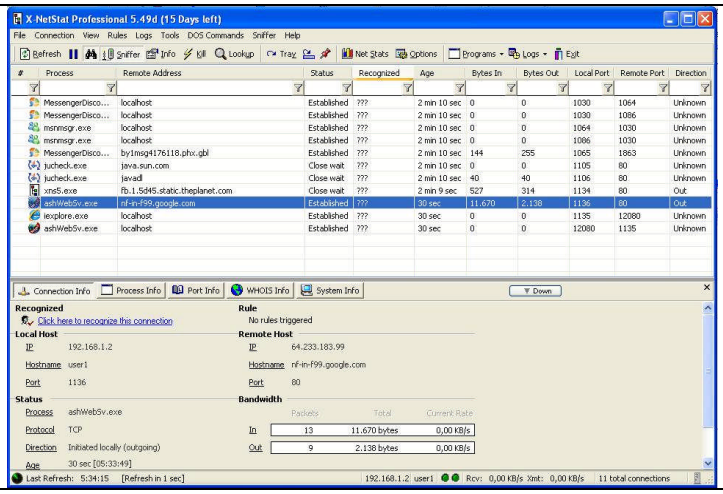
Yukarıdaki uygulamayı başka bir program kullanarak gerçekleştirelim:

Bilgisayarınıza herhangi bir port kontrol programı kurunuz. Burada kullanılan program “xns5” adında bir IP izleyici programdır.

## UYGULAMA FAALİYETİ

Aktif Portları tespit etmek

| İşlem Basamakları | Öneriler |
|---|---|
| ➢ Bu tür programları İnternetten bulabilirsiniz. Programı çalıştıralım.<br>  | |
| ➢ Programı çalıştırdığımızda ekrana bilgisayarımızda açık olan programlar ve bu programların hangi portları kullandıkları görülmektedir.<br>  | |
| ➢ Program aracılığıyla hangi programın hangi portu kullandığı yerel ağda ve uzak bağlantısında aldığı IP numarası görülebilmektedir. | |


X-NetStat Professional 5.49d (15 Days left)
File Connection View Rules Logs Tools DOS Commands Sniffer Help
Refresh Sniffer Info Kill Lookup Tray Net Stats Options Programs Logs Exit
# Process Remote Address Status Recognized Age Bytes In Bytes Out Local Port Remote Port Direction
MessengerDisco... localhost Established ??? 2 min 10 sec 0 0 1030 1064 Unknown
MessengerDisco... localhost Established ??? 2 min 10 sec 0 0 1030 1086 Unknown
msnmsgr.exe localhost Established ??? 2 min 10 sec 0 0 1064 1030 Unknown
msnmsgr.exe localhost Established ??? 2 min 10 sec 0 0 1086 1030 Unknown
MessengerDisco... by1msg4176118.phx.gbl Established ??? 2 min 10 sec 144 255 1065 1863 Unknown
jucheck.exe java.sun.com Close wait ??? 2 min 10 sec 0 0 1105 80 Unknown
jucheck.exe javadl Close wait ??? 2 min 10 sec 40 40 1106 80 Unknown
vns6.exe fb.1.5d45.static.theplanet.com Close wait ??? 2 min 9 sec 527 314 1134 80 Out
ashWebSv.exe nf-in-f99.google.com Established ??? 30 sec 11.670 2.138 1136 80 Out
iexplore.exe localhost Established ??? 30 sec 0 0 1135 12080 Unknown
ashWebSv.exe localhost Established ??? 30 sec 0 0 12080 1135 Unknown
Connection Info Process Info Port Info WHOIS Info System Info Down
Recognized
Click here to recognize this connection
Rule
No rules triggered
Local Host
IP 192.168.1.2
Hostname user1
Port 1136
Remote Host
IP 64.233.183.99
Hostname nf-in-f99.google.com
Port 80
Status
Process ashWebSv.exe
Protocol TCP
Direction Initiated locally (outgoing)
Age 30 sec [05:33:49]
Bandwidth
Packets Total Current Rate
In 13 11.670 bytes 0,00 KB/s
Out 9 2.138 bytes 0,00 KB/s
Last Refresh: 5:34:15 [Refresh in 1 sec]
192.168.1.2 user1 Rcv: 0,00 KB/s Xmt: 0,00 KB/s 11 total connections

# ÖLÇME VE DEĞERLENDİRME

## ÖLÇME SORULARI

**Aşağıdaki soruları dikkatlice okuyarak seçenekli sorularda uygun şıkkı işaretleyiniz. Boşluk doldurmalı sorularda boşluklara uygun kelimeleri yazınız.**

**1.** FTP uygulamaları genel olarak hangi porttan yapılır?
**A)** 23
**B)** 21
**C)** 53
**D)** 161

**2.** Port numaraları TCP parçasında hangi adresleri kullanır?
**A)** 1028.port
**B)** Kaynak port
**C)** Hedef port
**D)** Kaynak ve hedef port

**3.** Aşağıdakilerden hangisi yanlıştır?
**A)** 255'ten aşağı numaralar özeldir.
**B)** 255'ten aşağı numaralar halka açık uygulamalar için ayrılmıştır.
**C)** 255'ten 1023'e kadar olan numaralar satılabilir uygulamalar için şirketlere ayrılmıştır.
**D)** 1023'ten yukarı düzenlenmemiştir.

**4.** Port numaraları için; aşağıdakilerden hangisi doğrudur?
**A)** Port numaraları 0'dan 65538'e kadar değişmektedir.
**B)** Aralarında iletişim olan makinelerde korunan bir port tablosu vardır.
**C)** Port numaraları 2 farklı kategoriye bölünmüştür.
**D)** Port numaraları 16 bit ile ifade edilir.

**5.** Aşağıdaki eşleştirmelerden hangisi yanlıştır?
**A)** SMTP- TCP port 25
**B)** POP3- TCP port 110
**C)** http- TCP/UDP port 23
**D)** DNS- UDP port 53

**6.** Komut satırında yürütülen …… komutu etkin TCP bağlantılarını gösterir.

**7.** İstemci iletişim kurmak istediğinde web sunucusu ile TCP'yi kullanırken ….portu kullanır ve kaynak portu ise 1045'tir.

**8.** Port numaraları, TCP ve UDP parçaların çerçevelerinde ……bayt ile ifade edilirler.

**9.** Sunucular FTP servisini kullanırken TCP bağlantılarını ….portu kullanarak iletir ve …..porttan FTP uygulamalarını gerçekleştirir.

**10.** ……..…… yöntemi ile TCP, iki bilgisayar arasında birden fazla bağlantı kurabilir.

## DEĞERLENDİRME

Cevaplarınızı cevap anahtarı ile karşılaştırınız. Doğru cevap sayınızı belirleyerek kendinizi değerlendiriniz. Yanlış cevap verdiğiniz ya da cevap verirken tereddüt yaşadığınız sorularla ilgili konuları faaliyete dönerek tekrar inceleyiniz.

# MODÜL DEĞERLENDİRME

**PERFORMANS TESTİ (YETERLİK ÖLÇME)**

Modül ile kazandığınız yeterliği, öğretmeniniz işlem basamaklarına göre 0 ile 10 puan arasında olacak şekilde değerlendirecektir.

| | Değerlendirme Ölçütleri | Puan |
|---|---|---|
| **1.** | Bilgisayarı ağa bağlayabilme | |
| **2.** | Sistemi çalıştırabilme | |
| **3.** | TCP'deki tehlikelere karşı güvenlik duvarı kurabilme | |
| **4.** | TCP'deki tehlikelere karşı güvenlik duvarı ayarlarını yapabilme | |
| **5.** | Portları test etmek için komut satırını çalıştırabilme | |
| **6.** | Komut satırında gerekli komutu kullanabilme | |
| **7.** | Komutun parametrelerini kullanabilme | |
| **8.** | Aktif portları tespit edebilme | |
| **9.** | Aktif portlardaki IP adreslerini tespit edebilme | |
| **10.** | Tüm portları test edebilme | |
| | **Toplam (100 puan olabilir)** | |

**DEĞERLENDİRME**

Yaptığınız değerlendirme sonucunda eksikleriniz varsa öğrenme faaliyetlerini tekrarlayınız.

Modülü tamamladınız, tebrik ederiz. Öğretmeniniz size çeşitli ölçme araçları uygulayacaktır, öğretmeninizle iletişime geçiniz.

# CEVAP ANAHTARLARI

## ÖĞRENME FAALİYETİ-1 CEVAP ANAHTARI

| | |
|---|---|
| **1** | **D** |
| **2** | **B** |
| **3** | **C** |
| **4** | **D** |
| **5** | **A** |
| **6** | **A** |
| **7** | **IP** |
| **8** | **DoS** |
| **9** | **Firewall(güvenlik duvarı)** |

## ÖĞRENME FAALİYETİ-2 CEVAP ANAHTARI

| | |
|---|---|
| **1** | **B** |
| **2** | **D** |
| **3** | **A** |
| **4** | **C** |
| **5** | **C** |
| **6** | **netstat** |
| **7** | **80.port** |
| **8** | **2 byte** |
| **9** | **20-21.port** |
| **10** | **Çoklama(Multiplexing)** |

# ÖNERİLEN KAYNAKLAR


- ATAY Saib, **Bitirme Ödevi, CISCO Ağ Akademisi-1**, Fırat Üniversitesi, Elazığ, 2006.
- BALIK H.Hasan, Ayhan AKBAL, **TCP/ IP'nin Dünü Bügünü Yarını**, Fırat Üniversitesi, Elazığ.
- DOĞAN Haşim, **Bitirme Ödevi**, **CISCO Ağ Akademisi-2**, Fırat Üniversitesi, Elazığ, 2005.