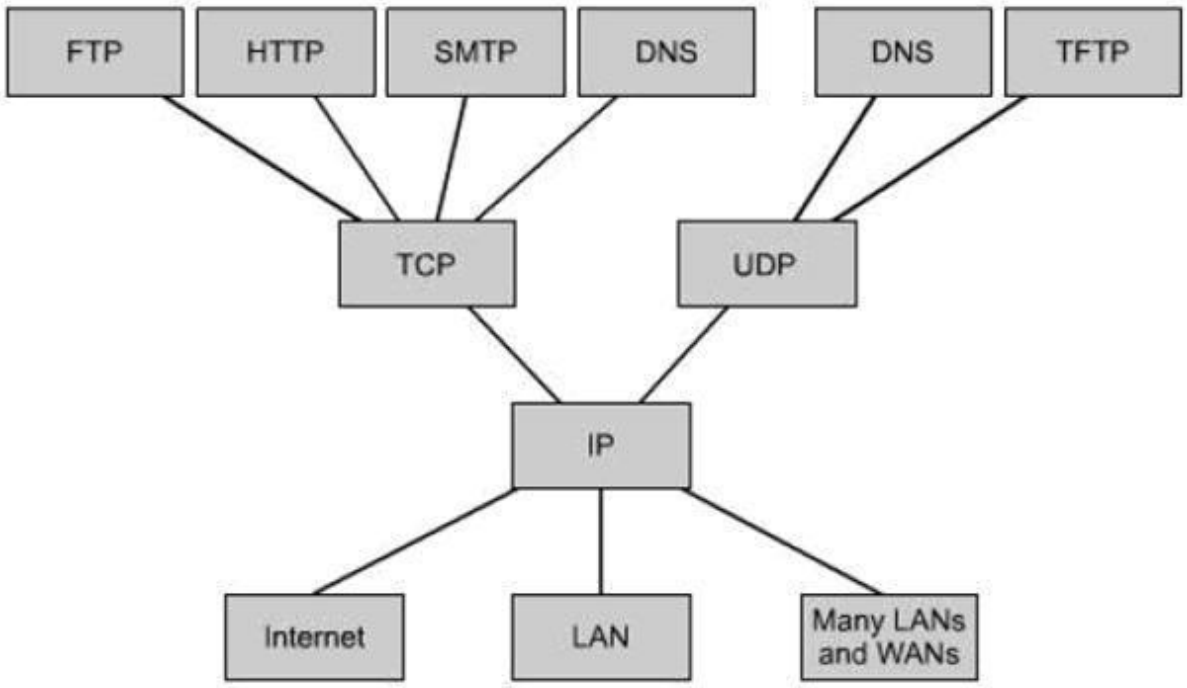
1- TCP/IP MODELİNDE BULUNAN PROTOKOLLER

Ağ üzerinde iki bilgisayarın karşılıklı veri aktarabilmesi ve süreçler (processes) yürütebilmesi için bilgisayarların birlikte çalışabilme (interoperability) yeteneğinin olması gerekir. Birlikte çalışabilme, verici ve alıcı arasında kullanılacak işaretler, veri formatları ve verinin değerlendirme yöntemleri üzerinde anlaşmayla mümkün olur. Bunu da sağlayan kurallar dizisi protokol olarak adlandırılır.

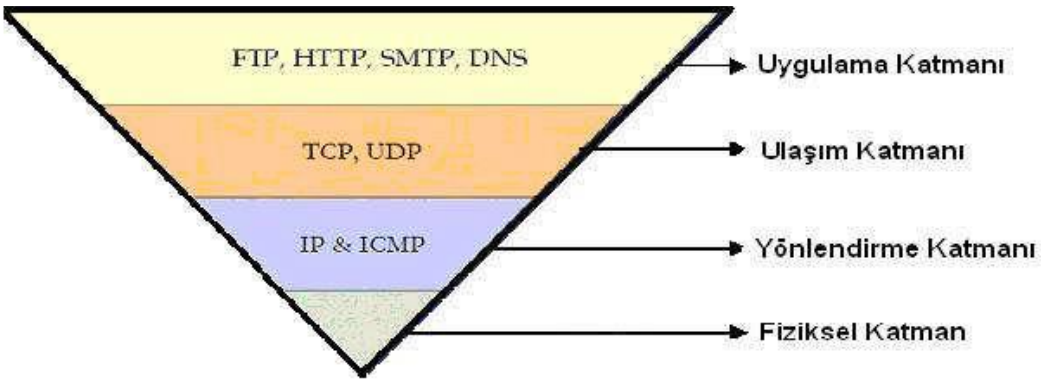
Protokol, ağın farklı parçalarının birbiriyle nasıl etkileşimde ve iletişimde bulunacağını belirler. Standartlar ise her üreticinin uyduğu ortak tanımlamalardır. Verinin ağ içerisinde bir yerden başka bir yere hareket etmesi için ağ içerisindeki tüm cihazların aynı dili konuşması veya protokolü kullanması çok önemlidir. Protokol, ağ içerisindeki iletişimi sağlıklı bir şekilde yapmak için gereken kuralların tümüdür. Bir pilotun uçağını uçururken diğer uçaklar ile veya hava kontrol kulesiyle iletişim sağlaması için kullandığı özel bir dil gibi.

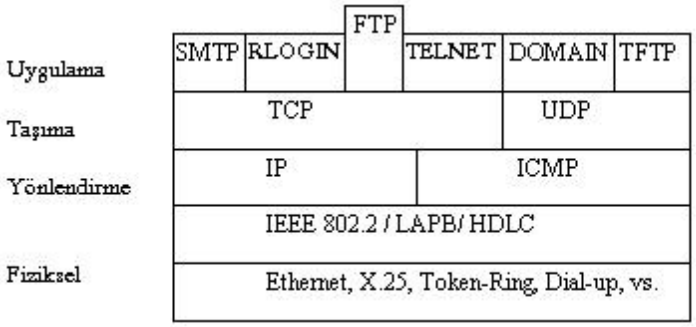


TCP/IP Katmanları

Uygulama programlarının bulunduğu katman sayılmaz ise dört katman vardır. Bunlar; uygulama, ulaşım, yönlendirme ve fiziksel katmanlardır (Şekil 1.1).

- Uygulama katmanında SMTP (Simple Mail Transfer Protocol-Basit Posta Aktarım Protokolü), TELNET (Telecommunication Network-İletişim Ağı), FTP (File Transfer Protocol-Dosya Aktarım Protokolü), SNMP (The Simple Network Management-Basit Ağ Yönetim Protokolü), (Remote Login Uzaktan Erişim) gibi protokolleri vardır.
- Ulaşım katmanında TCP (Transmission Control Protocol-İletişim Kontrol Protokolü) ve UDP (User Datagram Protocol-Kullanıcı Veri Bloğu İletişim Protokolü) protokolleri.
- Yönlendirme katmanında IP (Internet Protocol-İnternet Protokolü), ICMP (Internet Control Management Protocol- İnternet Kontrol Yönetim Protokolü) protokolleri vardır.
- Fiziksel katmanda ise gelen bilgileri iletim ortamına aktarmakla görevli protokoller olan Ethernet, switch, X25 gibi protokoller vardır.





SMTP (Simple Mail Transfer Protocol-Basit Posta İletim Protokolü): Elektronik posta iletimi SMTP protokolünü kullanarak bilgisayarlar arasında veri alışverişini gerçekleştirirler. Elektronik postaların güvenli bir şekilde adreslerine ulaşabilmesi için TCP servislerinden yararlanır. Oluşturulan elektronik posta mesajlarının standart olarak dizayn edilmiş formatı vardır. Mesajların iletimi sırasında bu formata uyması gerekir. Bu uyum istemci ve sunucu arasında elektronik posta veri iletiminin kolaylıkla yapılmasını sağlar. SMTP, iletim sırasında uygulanacak olan kurallar sırasını belirler. Elektronik postaların sunucularda saklanış şekli, depo alanının ne kadar sıklıkla kontrol edilmesi gerektiğini belirten detaylarla ilgilenmez. Elektronik postaların iletimi ASCII metin modundadır. Protokolün istemci ve sunucu arasında veri alışverişi ve senkronizasyonu sağlayan komutları da okunabilir, açık yazı türündedir.

SNMP (Simple Network Management Protocol-Basit Ağ Yönetim Protokolü) : Ağ içerisinde bulunan yönlendirici, anahtar ve HUB gibi cihazların yönetimi için kullanılır. SNMP desteği olan ağ cihazları SNMP mesaj alış verişiyle uzaktan yönetilebilir. Bunun için cihazlarda SNMP parçası (agent) olmalıdır. SNMP farklı türdeki makinelerin kolaylıkla yönetilmesi ve sorunlar hakkında bilgi edinilmesi amacı ile tasarlanmıştır. Farklı türde aletlerin yaptıkları farklı görevleri vardır. Bir yönlendirici yönlendirdiği datagramların (bilgi miktarı) , iletilen, iletilmeyen paketlerin sayısı ve buna benzer bilgileri depolarken, yazıcı kartuşun durumu, modem aldığı karakter sayısını, bağlantı hızı gibi bilgileri kayıt eder. Yönetim merkezi hangi aygıttan kesin olarak ne tür bilgi alacağını tam olarak bilemez. Bu nedenle bilgilerin depolandığı standart bir yapı geliştirilmiştir. SNMP kullanım alanı sadece TCP/IP ağları ile sınırlandırılmamıştır. Aynı zamanda IPX, AppleTalk ve OSI desteği de mevcuttur.

TELNET (Telecommunication Network-İletişim Ağı): Kullanıcının, bir başka makineye sanki o makinenin istasyonuymuş gibi bağlantı kurmasını sağlayan protokoldür. TCP/IP protokolünü kullanan uygulamalardan bazıları kullanıcılara uzakta olan bilgisayara ağ üzerinde oturum açmalarına olanak sağlar. TELNET protokolü TCP bağlantısı yapılarak oturum açılan bilgisayar üzerinde sanal klavye kullanılmasına izin verir. Protokol bilgisayar üzerinde komutları işleterek sunucudan aldığı çıktıların istemcinin ekranı üzerinde görüntülenmesine imkân sağlar. TELNET temel olarak üç prensip üzerine kurulmuştur. NVT(Sanal Ağ Terminali), istemci-sunucu TELNET protokol tercihlerinin uzlaşması ve terminallerin simetrik çalışması. Protokol, bağlantı sırasında kullanılan mesajların şifrelenmemesi, paketlerin iletimi sırasında arada yer alan, iletim vazifesi gören aygıtları kullanan insanların iletilen verileri kolayca okuyabilmesine izin vermesi nedeni ile güvenlik zafiyetlerine açıktır.

Protokol tasarım yapısı itibari ile " oturum ele geçirme" saldırılarına karşı son derece zayıftır. TELNET sağladığı hizmet avantajları sayesinde kullanıcılar arasında son derece popülerdir. NVT (Sanal Ağ Terminali) özelliği sayesinde istemciler bağlandıkları bilgisayarların mimarisi hakkında fazla bilgiye ihtiyaç duymaz. Kullanıcılar, TELNET protokol tanımı içerisinde yer alan düzenlemeler sayesinde uzaktaki bilgisayarlara kolaylıkla hükmedilebilir.

TELNET protokolü istemci ve sunucu arasında verinin iletim şekli, kullanılan karakterlerin yapısı (8 bit karakter modu veya 7 bit ASCII) hakkında anlaşma yapılmasına izin verir. Bu sayede iletilen verilerin türü konusunda meydana gelecek olan hataların önüne geçilmiş olur. TELNET protokolü terminal ve uygulamalar (process) arasında simetrik görünüm sağlar. TELNET bağlantısı kuracak olan bilgisayar, sunucu ile TCP bağlantısı kurar. Bağlantının kurulması ile birlikte istemci klavyeden aldığı tuş basım verilerini sunucuya iletir.

Sunucunun aldığı veriler daha sonra istemcinin monitöründe eko şeklinde görüntülenir.

FTP (File Transfer Protocol-Dosya İletim Protokolü): Bir bilgisayardan başka bir bilgisayara bağlanarak dosya aktarımını sağlar. İnternet üzerindeki iki sistem arasında dosya aktarımı için kullanılan temel protokoldür. TCP/IP mimarisi geliştirilmeden önce de kullanılan bir protokol olan FTP, zaman içerisinde değişimlere uğrayarak günümüzde kullanılan şeklini almıştır. FTP protokolü TCP tabanlıdır. TCP protokolü sayesinde bağlantı kurulmuş olan iki nokta arasında güvenli veri alışverişi sağlanır. Protokol sayesinde tanımlanan erişim yetki sınırlamaları, isimlendirme, farklı işletim sistemleri tarafından kullanılabilme, veri gösterim çeşitliliği gibi etmenler protokolü karmaşık bir hâle getirir. FTP kullanıcı ile sunucu arasında görsel iletişim sunar. Her ne kadar sadece dosya transferi için tasarlanmış olsa da kullanıcının dosyaların listelenmesi, kullanılabilecek komutların gösterilmesi gibi isteklerine cevap verir. FTP, dosya içerisinde yer alan verinin türünün kullanıcılar tarafından tayin edilmesine imkân sağlar. Dosyalar içerisinden açık yazı içeren dokümanlar (ASCII) ya da sayısal veriler (EBCDIC) barındırabilirler. FTP protokolü kullanıcıların kullanıcı ismi ve şifre kullanarak sisteme giriş yapmalarına imkân sağlar. Kullanıcılar istenen kriterleri yerine getirdikten sonra dosya transfer işlemlerini başlatabilirler. İnternet üzerinde aktif olarak çalışan protokollerin işlemesini sağlayan sunucular birden fazla istemciden gelen istekleri cevaplamak üzere tasarlanmıştır. FTP istemcileri TCP protokolünü kullanarak FTP sunucularla bağlantı kurarlar. Sunucu çok sayıda istemciden gelen istekle baş etmek amacıyla kendi kopyalarını oluşturur. Oluşturulan kopyalar yapılması gereken tüm işlemleri yerine getiremezler. Sadece istemcilerle arasındaki kontrol bağlantıları ile ilgilenir. Bağımsız dosya transferleri sağlamak amacıyla birden fazla sayıda süreç oluştururlar. FTP sunucuları 21 numaralı TCP portundan istemcilerden gelen bağlantı isteklerini dinlerler. Port numarasını alan sunucu 20 numaralı TCP portu üzerinden istemci ile bağlantıya geçerek veri transferini başlatır. Dosya transferi sona erdiğinde bağlantı sonlandırılır.

NNP (Network News Transport Protocol-Ağ Haberleri Protokolü): USENET (Dünya üzerindeki milyonlarca ağ kullanıcısının çok değişik konularda haberler, yazılar gönderdiği bir tartışma platformu) postalanma hizmetinin yürütülmesini sağlar.

HTTP (The Hypertext Transfer Protocol-Hiper Metin İletişim Protokolü): Web istemci programları ile sunucuların iletişim kurmasını sağlar. http protokolü istemcileri "ağ tarayıcısı" (web browser) olarak adlandırılır. Protokol genel olarak dokümanları sunuculardan talep eden, sunucuya bilgi gönderilmesini sağlayan komutları tanımlar. İstek-cevap sistemi ile çalışır. Web istemci programı ile sunucu arasında TCP bağlantısı sağladıktan sonra istemci istek mesajını sunucuya iletir. Sunucu bu

isteğe karşılık cevap gönderir. Bu istek-cevaplar komutsal tabanlıdır. Protokol, sunucuya istemci tarafından iletilen her istek mesajı birbirinden bağımsız olacak şekilde tasarlanmıştır.

Protokol iki yönlü veri alışverişine izin verir. Sunucudan istemciye dosya transferine izin verdiği gibi istemciden sunucuya dosya transfer edilmesine de imkân sağlar. HTTP protokolü yazılı ve görsel iletişimi hedef alması itibarı ile sunucu ve istemci arasında karakter uyumunu da gözetmek zorundadır. İstemci ve sunucu veri alışverişi sırasında iletilen karakter türleri arasında uzlaşma sağlarlar. Protokol daha hızlı yüklemeyi sağlamak amacıyla sunuculardan elde edilen verilerin bir dizin altında depolanmasına izin verir. İstemci aynı sayfayı yeniden almak istediği zaman sunucu ile istemci arasında talep edilen sayfanın güncellenip güncellenmediğine dair iletişim kurulabilir. Güncelleme olmadığının tespit edilmesi durumunda depo alanından eski bilgi yeniden yüklenir. İstemci ve sunucular arasında köprü vazifesi görürler.

TCP (Transmission Control Protocol-İletim Denetim Protokolü): 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 Protokolünün Özellikleri

- Bağlantı noktaları arasında veri iletişimini sağlaması.
- Güvenli veri iletimi sağlanması.
- 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.

Gönderici Port No		
Alıcı Port No		
Sıra Numarası		
Onay Numarası (ACK)		
Başlık Uzunluğu	Saklı Tutulmuş	Kod Bitleri
Pencere (Window)		
Hata Sınama Bitleri		
Acil İşaretçisi		
Kullanıcı Verisi		

Tablo 1.1: TCP segment formatı

UDP (User Datagram Protocol): İletim katmanında tanımlı tek protokol TCP değildir; UDP de bu katmanda tanımlıdır. UDP protokolü, bilgisayar ağları arasında paketlerin değişimine imkân sağlamak için tasarlanmıştır. UDP protokolü TCP gibi altyapı olarak IP datagramları kullanır, IP datagramlar içerisinde kapsüllenir. Veri akış kontrolünü sağlayacak, datagramlar arasında iletilirken kendi içerisinde meydana gelecek hataları belirlemek için kullanacağı herhangi bir mekanizması yoktur. Protokol datagramların iletilmesini garanti etmez; IP datagram içerisinde kapsüllenmiş UDP mesajının bir defadan fazla taşınmamasını sağlayamaz. TCP protokolü gibi bağlantı tabanlı değildir.

<table>
<tr><td>Uyarlama</td><td>Başlık</td><td>Hizmet Türü</td></tr>
<tr><td colspan="3">Toplam Uzunluk</td></tr>
<tr><td colspan="3">Kimlik Saptaması (Identification)</td></tr>
<tr><td colspan="2">Bayrak Bitleri</td><td>Parçalanma Ötelemesi (Fragment Ofset)</td></tr>
<tr><td colspan="2">Yaşam Süresi</td><td>Protokol</td></tr>
<tr><td colspan="3">Başlık İçin Hata Sınama Bitleri</td></tr>
<tr><td colspan="3">Gönderici IP Adresi</td></tr>
<tr><td colspan="3">Alıcı IP Adresi</td></tr>
<tr><td colspan="3">TCP Segmenti
(TCP Başlığı+ Kullanıcı Verisi)</td></tr>
</table>

Tablo 1.2.: IP başlığı içindeki alanlar

Uyarlama (Version): O anda kullanılan IP uyarlamasını gösterir. Farklı uyarlamada başlıktaki alanların yerleri değişiklik gösterdiğinden, paketin doğru yorumlanması için kullanılır.

 Başlık Uzunluğu (IP Header Length): Datagram başlığının gerçek uzunluğunu gösterir.

 Hizmet Türü (Service Type): Datagramın nasıl yönlendirileceğini belirler. Yönlendirilmesinde yapılan yol seçiminde ve bağlantıda kullanılır. Datagramlara bu alan aracılığıyla önem düzeyi atanabilir.

 Toplam Uzunluk (Total Length): Tüm IP paketinin (başlık ve veri dâhil) uzunluğunu belirtir.

 Kimlik Saptaması (Identification): Kullanıcı karşı tarafla etkileşim içindeyken, mesajlar parçalanarak bir çok datagram içinde gönderilebilir. Bu alan, aynı kullanıcı mesajının farklı datagramlar içinde bulunması durumunu açıklayan kimlik bilgisini içerir.

 Bayrak Bitleri (Flags): Parçalama (Fragmentation) kontrolünde kullanılır. Bir datagram parçalanıp parçalanmadığı, onun parçalanma izninin olup olmadığı gibi bilgilere ait kodlar taşır. Üç tane olan bayrak bitlerinden ilki (D biti), içinde bulunduğu datagramın kaç parçadan oluştuğunu belirtir. Eğer 1 ise gönderilen verinin tek datagramdan oluştuğu anlaşılır; alıcıya başkası yok bekleme anlamında mesaj iletir. İkinci bayraksa, parçalanıp birçok datagram hâlinde gönderilen verinin en son olduğunu belirtir. Üçüncüsü, saklı tutulmuştur.

 Yaşam Süresi (Time to Live): Datagramın ağ üzerinde dolaşan sürecini belirtir. Verici tarafında yerleştirilen dolaşma değeri her düğümden geçerken azaltılır; sıfıra ulaşırsa kaybolmuş olduğu varsayılarak datagram ağdan çıkarılır.

Protokol (Protocol): Bir datagramın hangi üst katman protokolüne ait olduğunu belirtir. Alıcı tarafın IP katmanı bu alana bakarak paketi bir üstünde bulunan protokollerden hangisine iletileceğini anlar.

 Başlık için Hata Sınama Bitleri (Header Checksum): Datagram başlık kısmının hatasız iletilip iletilmediğini sınamak için kullanılır.

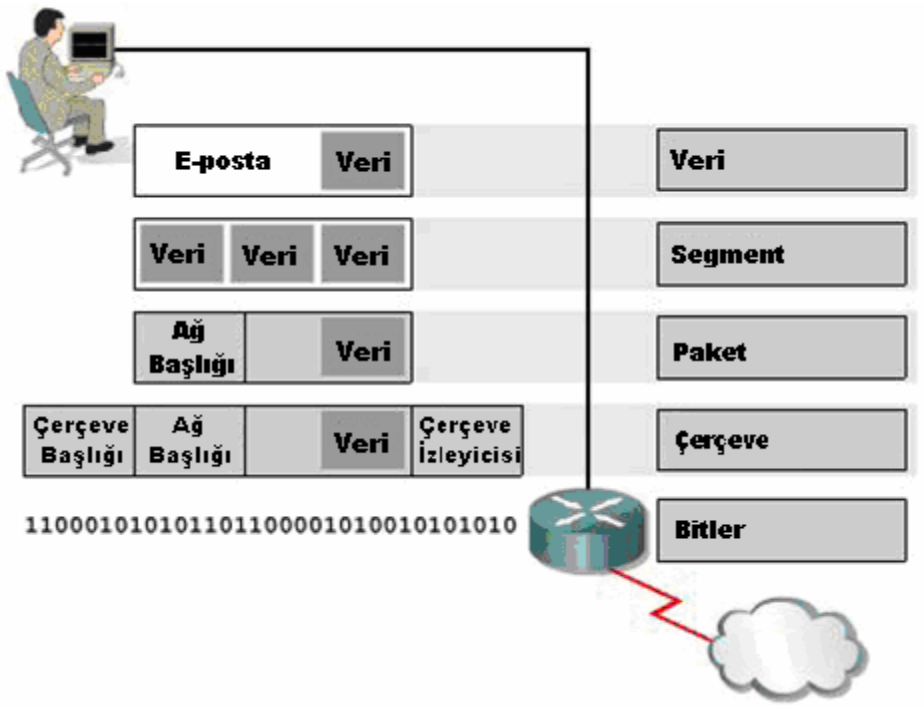
 Gönderici IP Adresi (Source Address): Datagramın gideceği yerin internet adresi yerleştirilir.

 Seçenekler (Options): Bu alan değişik amaçlar için kullanılır. Güvenlik, hata raporlama vs. seçimliktir. Ancak kullanılırsa 32 bitin katları uzunlukta olmalıdır.

 TCP Segmenti: Bir üst katmandan gelen veriyi içerir.

ICMP (Internet Control Message Protocol): ICMP kontrol amaçlı bir protokoldür. Genel olarak sistemler arası kontrol mesajları IP yerine ICMP üzerinden aktarılır. ICMP, IP ile aynı düzeyde olmasına karşın aslında kendisi de IP' yi kullanır. ICMP mesajları, IP üzerinden gönderilir. ICMP mesajlarının amacı haberleşme sırasında meydana gelebilecek problemler hakkında yönlendiricilere veya datagramları oluşturan bilgisayarlara bilgi vermektir. ICMP protokolü, internet protokolünü daha güvenli hâle getirmez. Sadece datagram iletimi sırasında meydana gelen hataların sebepleri ile ilgili bilgi sağlar. Aşağıdaki şekilde ICMP formatını görmektesiniz:

VERİNİN GİYDİRİLMESİ



Ethernet Çerçevesinin Yapısı

Başlama Eki	SFD	Hedef MAC Adresi	Kaynak MAC Adresi	Uzunluk / Tür	Kapsüllenmiş Veriler	FCS
7	1	6	6	2	46 - 1500	4

IEEE 802.3 Ethernet Çerçeve Alanları

Bytes	Alan Adı
7	Başlama Eki
1	Çerçeve Sınırlayıcı Başlangıcı
6	Hedef MAC Adresi
6	Kaynak MAC Adresi
2	Uzunluk/Tür Alanı
46 - 1500	Kapsüllenmiş Veriler
4	Çerçeve Kontrolü Sırası (CRC Sağlaması)

2- LAN Teknolojileri

Ethernet (IEEE 802.x)

- CSMA/CD
- Fast Ethernet
- Gigabit Ethernet

Jetonlu Halka(Token Ring)

Jetonlu Halka(Token Bus)

ATM

FDDI LAN

3- GENİŞ ALAN AĞLARI

Sınıflandırma

Bağlantı Durumuna göre

- Noktadan noktaya
- Çoklu bağlantı teknolojisi

Anahtarlama Yöntemine göre

- Devre anahtarlama
- Paket anahtarlama
- Hücre anahtarlama

Topolojik Yapışma göre

- Hiyerarşik topoloji
- Örgü topoloji

Teknolojiler

•Modem(dial-up)

•Kiralık hat

•X.25

•Frame Relay (FR)

•ISDN

•xDSL

•ATM

•SMDS

4- IP Adresleme

IP adresi, ağ üzerinde bulunan makinenin adresini ifade eder. Bu adres ile bir makine diğerlerine ulaşma imkânı bulur. Ağ üzerinde bulunan herhangi bir bilgisayarı ifade etmek için 32 bitlik bir IP adresi kullanılır. TCP/IP protokolü kullanılan bir ağda her bilgisayarın mutlaka bir IP adresi olmak zorundadır. IP adreslerinin atanması son derece kolay bir işlem olmasına karşın bu adresler atanırken göz önünde bulundurulması gereken birkaç önemli husus vardır. Atanan IP adreslerinin ağ içerisinde "eşinin" bulunmaması gerekir. Bununla birlikte atanan IP adresleri aynı ağ üzerinde bulunan diğer birimlerle tutarlılık göstermelidir.

IPv4 Adresleme

IPv4 (32 bit) ve IPv6 (128 bit) olmak üzere iki çeşit IP adresi vardır. Günümüzde yaygın olarak 32 bitlik (IPv4) adresleme mekanizması kullanılmaktadır. İnternetin yaygınlaşması ve IPv4 adreslerinin çok hızlı tükenmesi ile birlikte IPv6 adreslerinin kullanılmasına yönelim hız kanacaktır. IPv6 işlevselliği, kullanım kolaylığı sayesinde büyük faydalar sağlayacaktır.

32 bitlik bir IP adresi 8 bitlik dört oktet hâlinde ifade edilir. Bunun sebebi, ise okumayı kolaylaştırmak içindir. Adresleme için toplam 32 bitimiz varsa 2^{32} = 4 milyar 294 milyon 967 bin 196 tane bilgisayar adreslenebilir. Ancak bu gerçekte böyle değildir. 32 bitlik bir adres, diyelim ki, 10000100.00011011.00001100.00001100 (194.27.12.12) şeklinde ifade edilmiş olsun.

Bu adresin okunması için ikilik sistemde bir okuma gerekmektedir, ancak bu şekilde de okuma oldukça zor olduğunda yazdığımız adres onluk sisteme çevrilerek 194.27.12.12 şekline dönüşür ve bu tür bir ifadeye noktalı yazım (dotted decimal notation) denir. Nokta ile ayrılan kısımların her biri 0 ile 255 arasında bulunan birer tamsayı olmak zorundadır.

IP adresleri ağ numarası (Net ID) ve bilgisayar numarası (Host ID) olmak üzere iki bölümden oluşur. "Net ID" bilgisayarın bulunduğu ağı belirtirken, "Host ID" ağ içerisinde bilgisayarların birbirlerinden ayrılmasını sağlayan değerleri barındırır. IPv4 bugün var olan internet ağının ana halkası olarak yerini almıştır. Günümüz interneti IP protokolünün 4.sürümü(IPv4) üzerine kurulmuş ve IPv4 tablo 2.1'de görüldüğü gibi sınıf sistemine dayalı bir sözleşmedir.

Sınıf	Ağ Sayısı	Adres Sayısı
A	125	16 Milyon
B	16382	65534
C	2 Milyon	256
D	Multicast kullanım için ayrılmıştır	
E	Gelecekte kullanım için ayrılmıştır	

Tablo 2.1: IPv4 sınıfları

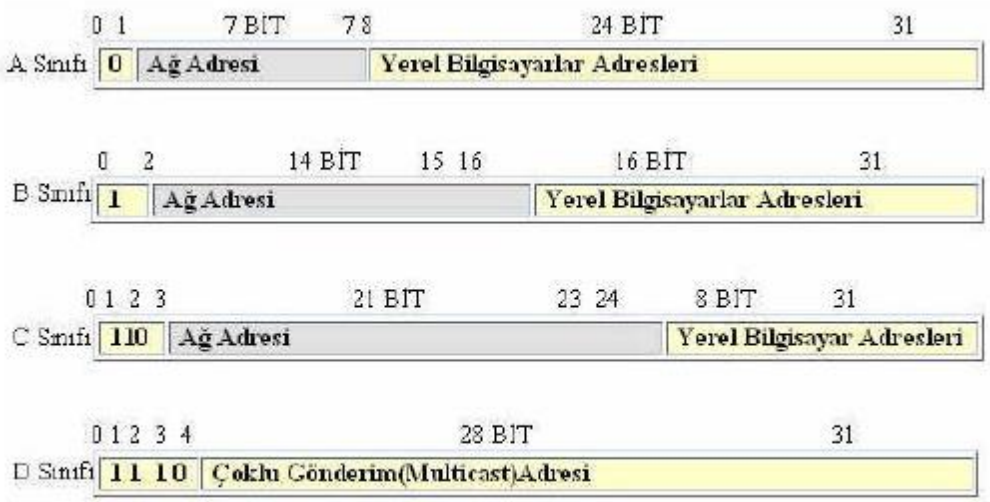
IP Adres Sınıfları

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

Adresler iki parçaya ayrılır; parçanın soldaki kısmı ağ adresi, sağdaki kısım ise sistem adresi olarak adlandırılır. Ağ adresleri yönlendiriciler için daha anlamlıdır. Tüm yönlendirme işlemleri ağ adreslerine bakılarak yapılır. Şekil 2.2'de sınıflanmış bir ağın ayrılmış hâli görülmektedir.

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

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



Şekil 2.13: IP adres sınıfları

Class A	Network	Host		
Octet	1	2	3	4

Class B	Network		Host	
Octet	1	2	3	4

Class C	Network			Host
Octet	1	2	3	4

Class D	Host			
Octet	1	2	3	4

A Sınıfı: 001.hhh.hhh.hhh'dan 126.hhh.hhh.hhh'a kadar
B Sınıfı: 128.001.hhh.hhh'dan 191.254.hhh.hhh'a kadar
C Sınıfı: 192.000.001.hhh'dan 223.255.254.hhh'a kadar
D Sınıfı: 224.000.000.000'dan 239.255.255.255'a kadar

IP Adres Sınıfı	Minimum	Maksimum
A	0	126
B	128	191
C	192	223
D	224	238
E	240	247

Tablo 2.2: IP adres tanım aralıkları

IP Address Class	High Order Bits	First Octet Address Range	Number of Bits in the Network Address
Class A	0	0 - 127 *	8
Class B	10	128 - 191	16
Class C	110	192 - 223	24
Class D	1110	224 - 239	28

A Sınıfı Adres

A sınıfı adres 16 milyon kullanıcı adresi barındıran geniş ağlar için kullanılan adres sınıfıdır. Sadece ilk oktet ağı temsil eder diğer üç oktet kullanıcıları temsil eder. İlk bit her zaman "0" dır. 127.0.0.0 adresi haricinde her adresi kullanabilir. Bu adres ise makinelerin kendilerine paket göndererek test amaçlı kullanılır.

1.2.3.2. B Sınıfı Adres

B sınıfı adres 4 oktetin ilk ikisini kullanarak adresleme yapan sınıftır. İlk oktetin ilk iki biti her zaman "10" dır. Buda 128 ile 191 arasındaki adresleri kullanabileceği anlamına gelir. B sınıfı her biri 65 534 bilgisayar içeren 16 382 tane alt ağa izin verir. Bu tür adres alanı büyük ve orta büyüklükte ağlar için kullanılır. Birçok büyük üniversite ve ISS' ler bu tür adres alanına sahiptir.

1.2.3.3. C Sınıfı Adres

C sınıfı adres küçük ağlar için kullanılır. En fazla 254 kullanıcılı ağlar içindir. İlk oktetin ilk üç biti "110" dır. 192 ile 223 arasını kullanabilir.

1.2.3.4. D ve E Sınıfı Adres

D sınıfı adreste ilk dört bit "1110" dır. 224 ile 239 arasını kullanabilir. IETF (Internet Engineering Task Force) E sınıfı adresleri kendi özel araştırmaları için kendilerine ayırmışlardır. E sınıfı adres internette kullanılamaz. 240 ile 255 arası bu adres sınıfı için ayrılmıştır.

Genel ve Özel IP adresleri

İnternet adreslemesinde 0 ve 255'in özel bir kullanımı vardır. 0 adresi, Internet üzerinde kendi adresini bilmeyen bilgisayarlar için (Belirli bazı durumlarda bir makinenin kendisinin bilgisayar numarasını bilip hangi ağ üzerinde olduğunu bilmemesi gibi bir durum olabilmektedir) veya bir ağın kendisini tanımlamak için kullanılmaktadır (144.122.0.0 gibi). 255 adresi genel duyuru "broadcast" amacı ile kullanılmaktadır. Bir ağ üzerindeki tüm istasyonların duymasını istediğiniz bir mesaj genel duyuru "broadcast" mesajıdır. Duyuru mesajı genelde bir istasyon hangi istasyon ile konuşacağını bilemediği bir durumda kullanılan bir mesajlaşma yöntemidir.

Alt Ağlar

Alt ağlar, IP adreslerini yönetmenin başka bir yoludur. Ağ tasarımında IP adresleri sistemlere dağıtılırken ağ daha küçük birimlere parçalanarak alt ağlar oluşturulur. Bu, internetin hiyerarşik adresleme yapısına uygun olduğu gibi, yönlendirme işinin kotarılması için gerekli yapının kurulmasını da kolaylaştırır. Örneğin büyük bir üniversiteye B sınıfı bir adres alındığında, bu adreslerin bölümlerdeki bilgisayarlara alt ağlar oluşturulmadan gelişi güzel verilmesi birçok sorunu da beraberinde getirir. Hâlbuki verilen B sınıfı adres alanı daha küçük alanlardan oluşan alt alanlara bölünse ve bu alt alanların her biri bölümlerdeki LAN' lara atansa birçok kolaylık da beraberinde gelecektir. Adres yerleştirmeleri kolay olacak, hiyerarşik yapı korunacak, adrese bakılarak ilgili sistemin hangi alt ağda olduğu anlaşılacak ve bu sayede oluşan problemlere en kısa zamanda çözüm getirilebilecektir.

Ağ Maskesi

Alt ağ oluşumu ağ üzerindeki yöneticiye beraber çalıştığı her bir ağ parçasının ölçüsünü belirlemeye imkân verir. Ağ üzerinde kaç segment olduğu bir kere belirlendiği zaman hangi ağda hangi aygıtın açık olduğunu belirlemek için alt ağ maskesini kullanabilirler. Bir bilgisayar ancak aynı ağda bulunan bir bilgisayarla doğrudan iletişime geçebilir. Aynı ağda değillerse dolaylı olarak iletişime geçer. Aynı ağda olup olmadığını IP adreslerini kullanarak anlarız. IP adresinin bir bölümü ağı, diğer bölümü de bilgisayarın ağ içindeki adresini tanımlar. Hangi bölümü ile ağı hangi bölümü ile bilgisayarı tanımladığını bilmek için alt ağ maskesi kullanırız. Dört bölümden oluşur ve ağ adresinin

hangi bölüme kadar geldiğini göstermek için kullanılır. Bilgisayar kendi ağ tanımlayıcılarını bulmak için alt ağ maskesi kullanır. Bu yüzden alt ağ maskesinin doğru şekilde girilmesi gerekir. Yanlış girilirse bilgisayarın diğer bilgisayarlarla iletişimi engellenebilir.

Bilgisayar ağ tanımlayıcısını bulmak için alt ağ maskesini IP adresini VE mantıksal işleminden geçirerek kullanırlar. Mesela, IP adresi:195.134.67.200 olsun ve alt ağ maskesi de 255.255.255.0 olsun. Bilgisayarın bu bilgilere dayanarak bulunduğu ağ tanımlayıcısını yani ağ adresini bulabiliriz. IP adresi ile alt ağ maskesini VE işlemine tabi tutalım:

195.134.67 .200 = 1100 0011.1000 0110.0100 0011.1100 1000
VE
255.255.255.0 = 1111 1111.1111 1111.1111 1111.0000 0000
Sonuç: 195.134.67. 0 = 1100 0011.1000 0110.0100 0011.0000 0000

Yayın Adresi

Ağın yayın adresi, alt ağ yapısına bağlı olarak belirlenir ve aynı ağ üzerindeki her bilgisayarda aynı değerin kullanılması gerekmektedir. 255 adresi genel duyuru "broadcast" amacı ile kullanılmaktadır. Duyuru mesajı genelde bir istasyon hangi istasyon ile konuşacağını bilemediği bir durumda kullanılan bir mesajlaşma yöntemidir. Örneğin, ulaşmak istediğiniz bir bilgisayarın adı elinizde bulunabilir; ama onun IP adresine ihtiyaç duydunuz, bu çevirme işini yapan en yakın "name server" makinesinin adresini de bilmiyorsunuz, böyle bir durumda bu isteğinizi yayın mesajı yolu ile yollayabilirsiniz. Bazı durumlarda birden fazla sisteme bir bilginin gönderilmesi gerekebilir, böyle bir durumda her bilgisayara ayrı ayrı mesaj gönderilmesi yerine tek bir yayın mesajı yollanması çok daha kullanışlı bir yoldur. Yayın mesajı yollamak için gidecek olan mesajın IP numarasının bilgisayar adresi alanına 255 verilir. Örneğin 144.122.99 ağı üzerinde yer alan bir bilgisayar yayın mesajı yollamak için 144.122.99.255 adresini kullanır.

Yayın mesajı yollanması birazda kullanılan ağın fiziksel katmanının özelliklerine bağlıdır. Mesela, bir ethernet ağında yayın mümkün iken noktadan noktaya (point-to-point) hatlarda bu mümkün olmamaktadır. Bazı eski sürüm TCP/IP protokolüne sahip bilgisayarlarda yayın adresi olarak 255 yerine 0 kullanılabilmektedir. Ayrıca yine bazı eski sürümler alt ağ kavramına hiç sahip olmayabilmektedir.

Yukarıda da belirttiğimiz gibi 0 ve 255'in özel kullanım alanları olduğu için ağa bağlı bilgisayarlara bu adresler kesinlikle verilmemelidir. Ayrıca adresler asla 0 ve 127 ile ve
223'un üzerindeki bir sayı ile başlamamalıdır.

IPv6

Günümüzde hâlen internet protokolü olarak kullanılan IPv4, bilgisayarların iletişim sırasında uçtan uca adreslenebilmesini sağlamaktadır. IPv4 adresleri 32 bit ve teorik olarak 4.294.967.296 adettir. Ancak pratikte verimsiz adres atama mekanizmalarından dolayı etkin adres sayısı bu sayıya hiçbir zaman ulaşamamaktadır. 1990'lı yıllarda patlayan internetteki host sayısındaki ve web sayfalarındaki artış nedeniyle IPv4, ihtiyacı karşılamakta yetersiz kalmaya başlamıştır. Bu problemler karşısında IPv6 geliştirilmiştir. Internet protokollerinden sorumlu Internet Engineering Task Force (IETF), 1990'lı yılların başında yeni bir çalışma grubu kurulmuş ve o zamanki adıyla IPng (Internet protocol, next generation) çalışma grubu, yeni IP protokolünün geliştirilmesi görevini üstlenmiştir. İnternet mimarisinin temel prensiplerinin korunarak sağlıklı gelişiminin sağlanması ve yeni uygulamaların önünün açılabilmesi için IP protokolünün yeni bir sürümünün geliştirilmesi öngörülmüştür. Yaklaşık 10 yılı aşkın bir süredir endüstri, akademi, hükûmetler ve çeşitli organizasyonların ortak çalışması sonucu IPv6 protokolü oluşmuştur. IPv6 protokolü, IETF' in yayınlamış olduğu bir seri RFC dokümanı vasıtasıyla tanımlanmıştır. IPv6'yı IPv4'ten ayıran en temel özellik 128 bitlik genişletilmiş adres alanıdır. Bu genişlemenin sağlamış olduğu teorik adreslenebilir düğüm sayısı 340.282.366.920.938.463.463.374.607.431.768.211.456 adettir. Böylesine geniş bir adres alanının şu an yaşadığımız adres sıkıntısını çözmenin yanında internet uygulamalarında yeniliklere de yol açması beklenmektedir. Öte yandan, IP üzerinde yapılan değişiklikler sadece bununla da kalmayıp, protokolün tam anlamıyla tekrar gözden geçirilmesi ve yenilenmesi de söz konusu olmuştur. Bunlar arasında basitleştirilmiş ve 64 bitlik işlemcilere göre düzenlenmiş paket başlığı paket bölünmesinin sadece uç noktalarda yapılacak olması yönlendiricilerin veri trafiğini daha seri bir şekilde işleyebilmesi için yapılan değişikliklerdir.

Temel IP başlığının yanı sıra ihtiyaca göre eklenebilir uzantı başlıklarının tanımlanabilmesi protokolün esnekliğini artıran bir faktör olmuştur. Güvenlik için IPsec (IP Security protocol) şartı da IPv6 ile gelen özellikler arasında yer almaktadır.

128 bitten oluşan IPv6 adreslerinin ilk 64 bitlik kısmı alt ağı adreslemek için kullanılan adres blok bilgisini içermektedir. Adres bloğu, bir paketin varacağı son bağa kadar olan yolda yönlendirilmesini sağlamaktadır. Geriye kalan 64 bit ise bu bağa vardığında paketin son alıcısının tespitinde kullanılmaktadır. IPv6 adresleri 16'lık bir düzende aşağıdaki gibi ifade edilir:

2045:ab28::6cef :85a1:331e:a66f:cdd1

Servis sağlayıcılar IPv6 omurgalarını kurup, tamamen IPv6 servisleri hizmete girene kadar geçen sürede, noktadan noktaya IPv6 uygulamalarının IPv4 ağları üzerinden geçirmeleri gerekecektir. Bu, bir IPv6 paketinin bir IPv4 paketinin içerisine sokulmasıyla sağlanılmaktadır.

IPV6 adresleri 8 hanelidir.

•Araları ":" ile ayrılır. Her hane hexadecimal olarak ifade edilir.

•IPV6'da IPV4'de olduğu gibi IP sıkıntısı yaşanmayacaktır.

•Her hane 65536 adet ipv6 adresini barındırır.

•En küçük adres 0 en büyük adres FFFF'dir.

•Örnek : 2001:a98:c040:111d:0:0:0:1

0 1 2 3 4 5 6 7 8 9 (decimal-on tabanlı sayı sistemindeki rakamlar)

0 1 2 3 4 5 6 7 8 9 A B C D E F(hexadecimal-onaltı tabanlı sayı sist.rak)

ipv4 - 4 bölümden oluşur. her bölüm 8 bittir.ipv4 adresi hafızada 8*4=32 bitlik yer kaplar. her bölüm 0-255 arası değerler alabilir. Dünya genelindeki tüm cihazlara dağıtılabilecek IP sayısı 256*256*256*256 ya da 2^{32} = 4.294.967.296 ihtimal. 2 nin üzerindeki 32 nin anlamı,

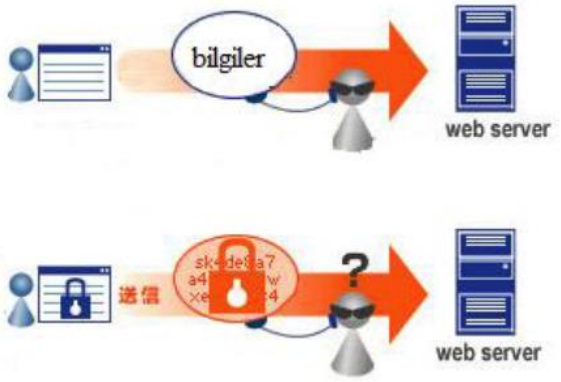
ipv6 - 8 bölümden oluşur.her bölüm 16 bitliktir. hafızada 8*16=128 bit yer kaplar. 2^{128}= 340 desilyon

IPv4	IPv6
8 Bitlik alanlardan oluşur	16 bitlik alanlardan oluşur
4 farklı alandan meydana gelen bir mimarisi vardır.	8 farklı alandan meydana gelen mimari ile hazırlanmıştır.
Toplamda 32 bit adresleme yapabilir	Toplamda 128 bit adresleme yapabilir
Adresler sadece sayılardan oluşmaktadır.	Adreslerde harflerinde kullanımı vardır.
NAT (Network Address Translator) yapılabilmektedir.	NAT (Network Address Translator) yapılamaktadır.
IPSec desteği isteğe bağlı kullanılabilir	IPSec kullanımı zorunludur

Xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

1. AĞ İLETİŞİMİ TEHDİTLERİ

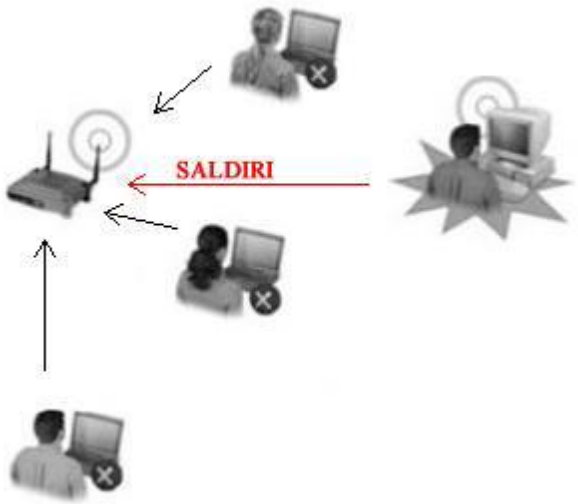
Bilgisayar ağlarının yaygınlaşması, *İnternet* aracılığı ile elektronik işletmelerin ortaya çıkması ve İnternet üzerinden ticaretin yaygınlaşmasıyla birlikte bilgisayar ağları oluşabilecek saldırılara karşı zayıflık göstermeye başlamıştır. Ağlardaki bu zayıflıklar iş uygulamalarında ürün kaybına ve şirketlerin ciddi anlamda zarar görmesine neden olmaktadır.



Resim 1.1: Ağ güvelik önlemleri

1- Ağ Saldırı Riskleri

Saldırıyı gerçekleştirenler, yazılımın zayıflıkları, kullanıcı adına ve bu kullanıcıya ait parolayı tahmin etme ve donanım saldırıları gibi daha düşük düzeyli teknik yöntemlerle kolayca ağa erişim kazanabilir.



Bilgi Hırsızlığı

Bilgi hırsızlığı izinsiz ağa erişimin, korumalı ağ bilgilerini elde etmek amacıyla kullanıldığı bir saldırıdır. Saldırgan, bir sunucuda veya bilgisayarda, daha önce kimlik doğrulaması için çaldığı bilgileri kullanabilir ve dosyalarda saklanan verileri okuyabilir. Saldırgan, ağ iletişimlerini izleyen ve veriyi yakalayan bir aygıt veya program olan, donanım veya yazılım tabanlı paket yoklayıcı kullanarak ağ ortamında geçiş hâlindeki veriyi çalabilir.

Kimlik Hırsızlığı

Kimlik hırsızlığı, kişinin izni olmadan kişisel bilgilerinin elde edilmesidir. Kimlik hırsızlığını kullanılarak kişinin kredi kart numarası, ehliyet numarası, vatandaşlık numarası, İnternet bankacılığı bilgileri, e-posta Şifre parolası ve önemli diğer kişisel bilgilerin bir başkası tarafından çıkar sağlamak amacı ile yapılan dolandırıcılık türüdür. TCK'ye göre bu suç sayılmaktadır.

Kimlik hırsızlığına uğranılmış ise bu birkaç yoldan anlaşılabilir:

- İzinsiz çevrim içi satın almalar yapıldığında,
- Kişi üzerinden çeŞitli kurumlarda kredi veya telefon hattı başvuruları sonucu borçlanma bilgileri geldiğinde,
- Kişinin bilgi dahilinde olmadan sosyal paylaşımlar olduğunda.

Bu gibi durumlarda adli mercilere başvurmak gerekmektedir.

Veri Kaybı ve Veri Kullanma

Kişisel bilgisayarlar ve işletmelerde kullanılan bilgisayarlarda veriler elektronik ortamda saklanmaktadır. Bu verilerin erişilemez veya kullanılamaz hâle gelmesine veri kaybı adı verilmektedir. Veriler ağdaki bilgisayarlar üzerinde saklanabilir veya yedeklenebilir. Herhangi bir bilgisayar ağına gönderilen veri, o veriyi almaya yetkisi olmayan kişilerce ele geçirilebilir. Bu kişiler iletişimi gizlice gözetleyebilir ya da gönderilen bilgi paketini değiştirebilir. Bunu birçok metod kullanarak yapabilir. Örneğin, bilgi iletişiminde bir alıcının IP numarasını kullanarak sanki o alıcıymış gibi gönderilen verileri istediği gibi kullanabilir. Veya Üniversitelerin sistemlerine izinsiz bir giriş yaparak öğrenci not bilgisini geçer bir nota çevirmek gibi.

Hizmet Aksatma

Kişisel veya işletmelerdeki kullanıcıların yasal haklarını kullanmalarını engelleme olarak tanımlanabilir. Ağ haberleşmesinde kullanıcı adı ve parolasını kullanamaması, kullanıcıların web hizmetine bağlanamaması gibi durumlarda ağa dışarıdan müdahale olduğu anlaşılabilir.

Ağ İletişim Tehditleri

Bilişim teknolojilerindeki gelişmeler kullanıcılara büyük kolaylık sağlarken aynı zamanda pek çok tehdidi de beraberinde getirmektedir. İletişim ağlarında ki güvenlik açıkları kullanıcıların sisteminin ele geçirmekten öte kişisel bilgileri ve büyük firmaların gizli bilgilerini ele geçirilmesine ve bu sayede maddi kazançlar elde etmeye yönelik olmaya başlamıştır. Yeni nesil tehditler kullanıcılardan, güvensiz ağlardan kaynaklanabilir.

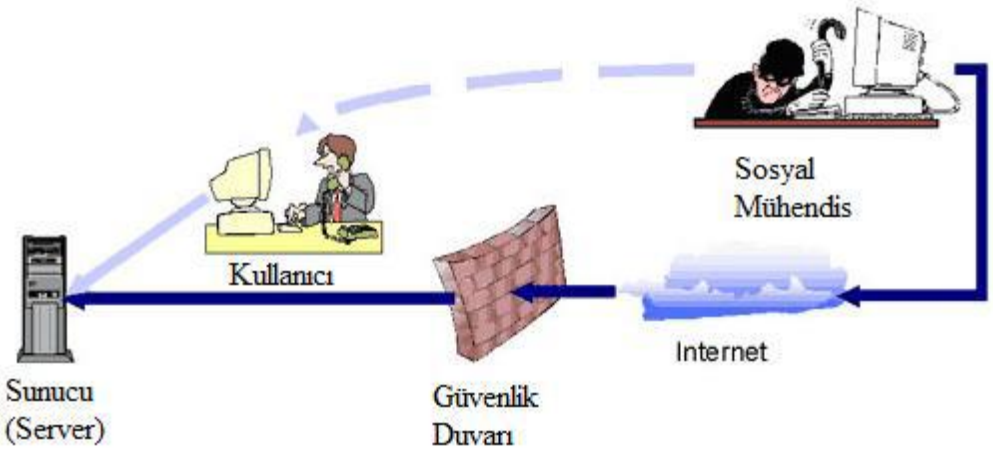
Haricî ve Dâhili Tehditler

Harici tehditler, ağ dışında çalışan kullanıcılardan gelir. Bu kişilerin bilgisayar sistemlerine veya ağa yetkili erişimi bulunmamaktadır. Harici saldırganlar, ağa saldırılarını genellikle *İnternet* üzerinden, kablosuz ağlardan veya çevirmeli erişim sunucularından gerçekleştirir. Bu saldırılar maddi ve manevi zarara yol açar ve engellemek için güvenliğin arttırılması gerekir.

Dâhili tehditler ise; bir kullanıcının hesabı üzerinden ağa yetkisiz erişimi olduğunda ya da ağ ekipmanına fiziksel erişimi olduğunda gerçekleşir. Dâhili saldırgan, ilkeleri ve kişileri tanır. Bu kişiler genellikle hangi bilgilerin ve savunmasız olduğunu ve bu bilgileri nasıl elde edebileceğini bilir. Fakat, dahili saldırılar her zaman kasıtlı olmaz. Bazı durumlarda, dahili bir tehdit, ağ dışındayken bilmeden dahili ağa virüs veya güvenlik tehdidi getiren güvenilir bir çalışandan da gelebilir.

2- Sosyal Mühendislik

Sosyal mühendislik, insanlar arasındaki iletişimdeki ve insan davranışındaki modelleri açıklıklar olarak tanıyıp bunlardan faydalanarak güvenlik süreçlerini atlatma yöntemine dayanan müdahalelere verilen isimdir. Sosyal mühendis, kendisini sistem sorumlusu olduğunu söyleyerek kullanıcının şifresini öğrenmeye çalışmak veya teknisyen kılığında kurumun içerisine fiziksel olarak sızmak veya çöp tenekelerini karıştırarak bilgi toplamak gibi değişik yollarla yapılabilir.



Sosyal mühendislikte en yaygın kullanılan tekniklerden üçü şunlardır: sahte senaryo uydurma, oltalama (phishing) ve sesle oltalama (vishing).

Sahte Senaryo Uydurma

Genellikle telefonla iletişim üzerinden gerçekleşen bir yöntemdir. Saldırganın amacına ulaşmak için sahte bir senaryo oluşturması ve bu senaryonun satırları arasından saldırılanın erişimindeki hassas bilgiye (bir sonraki adımda kullanmak üzere kişisel bilgiler ya da şifreler, güvenlik politikaları gibi erişim bilgileri) ulaşması şeklinde gelişir. Telefondaki işlemlerde yetkilendirme için ihtiyaç duyulan bilgiler genellikle başka kanallardan erişilebilir bilgiler (kimlik numarası, doğum tarihi vb.) olduğu için sahte senaryolar uydurmak ve istenen bilgileri elde etmek çoğunlukla uygulanabilir bir saldırı yöntemi olmaya devam etmektedir. Saldırganın senaryonun ana hattı dışına çıkabilecek durumları da göz önüne alıp hazırlık yapması, başarı oranını artıran bir etkendir.

Oltalama (Phishing)

Kimlik avcısının geçerli bir dış kuruluşu temsil ediyor gibi davrandığı bir sosyal mühendislik biçimidir. Genellikle e-posta üzerinden hedef bireyle (phishee) iletişim kurar. Kimlik avcısı, kullanıcıları kandırmak ve güvenilir bir kurumdan aradığını kanıtlamak için parola veya kullanıcı adı gibi bilgilerin doğrulanmasını isteyebilir.

Sesle / Telefonla Oltalama (Vishing)

Kimlik avcılarının, IP üzerinden ses (VoIP) uygulamasını kullandığı yeni bir sosyal mühendislik biçimidir. Sesle oltalamada, güvenilir bir kullanıcıya geçerli bir telefon bankacılığı hizmeti gibi görünen bir numarayı aramasını bildiren sesli mesaj gönderilir. Daha sonra kullanıcının

yaptığı aramaya bir hırsız tarafından müdahale edilir. Doğrulama için telefondan girilen banka hesap numaraları veya parolalar çalınır.

3- Saldırı Yöntemleri

Saldırılar ağ üzerinden olacağından ağa bağlı cihazlar her zaman saldırıya açık durumdadır durumdadır. Saldırganlar ağ üzeriden hedef makinaya ulaşarak yazılım veya donanıma zarar vermek isteyebilir. Bunun yanı sıra bir işletmenin ağına ulaşarak veritabanındaki verilere erişebilir, değiştirebilir veya silebilir. Saldırgan ağın *İnternet* bağlantısını kesebilir. Hedef makinaya truva tı gibi program yükleyerek kullanıcıyı takibe alabilir. Aynı zamanda saldırgan ağa girebilmek için farklı yöntemler kullanabilir.

Hizmet Reddi (Denial of service–DoS)

Hizmet reddi (Denial of service-DoS) hizmet aksatma amaçlı bir saldırı çeşitidir. Bir sisteme yapılan düzenli saldırılar sonucunda sistem çalışamaz ve hizmet veremez hâle gelebilir. Ayrıca DoS saldırılarıyla hedef sisteme ait kaynakların tüketilmesi de amaçlanır. Bir kişinin bir sisteme düzenli veya arka arkaya yaptığı saldırılar sonucunda hedef sistemin kimseye hizmet veremez hâle gelmesi veya o sisteme ait tüm kaynakların tüketimini amaçlanır. Bu saldırı önemli sunucuların servis vermeyi durdurması gibi büyük sorunlara yol açabilir.

Bir DoS saldırısının yaptıkları;

- Nework'ü trafik ile doldurmak böylece normal network trafiğini engellemek,
- İki makine arasındaki iletişimi bozar, bu sayede bir servise erişimi engeller,
- Özel birinin bir servise erişimini engeller,
- Servisin belirli bir sistem veya kişi ile iletişimini bozar.

Günümüzde en çok karşılaşılan yaygın DoS saldırısı şunlardır:

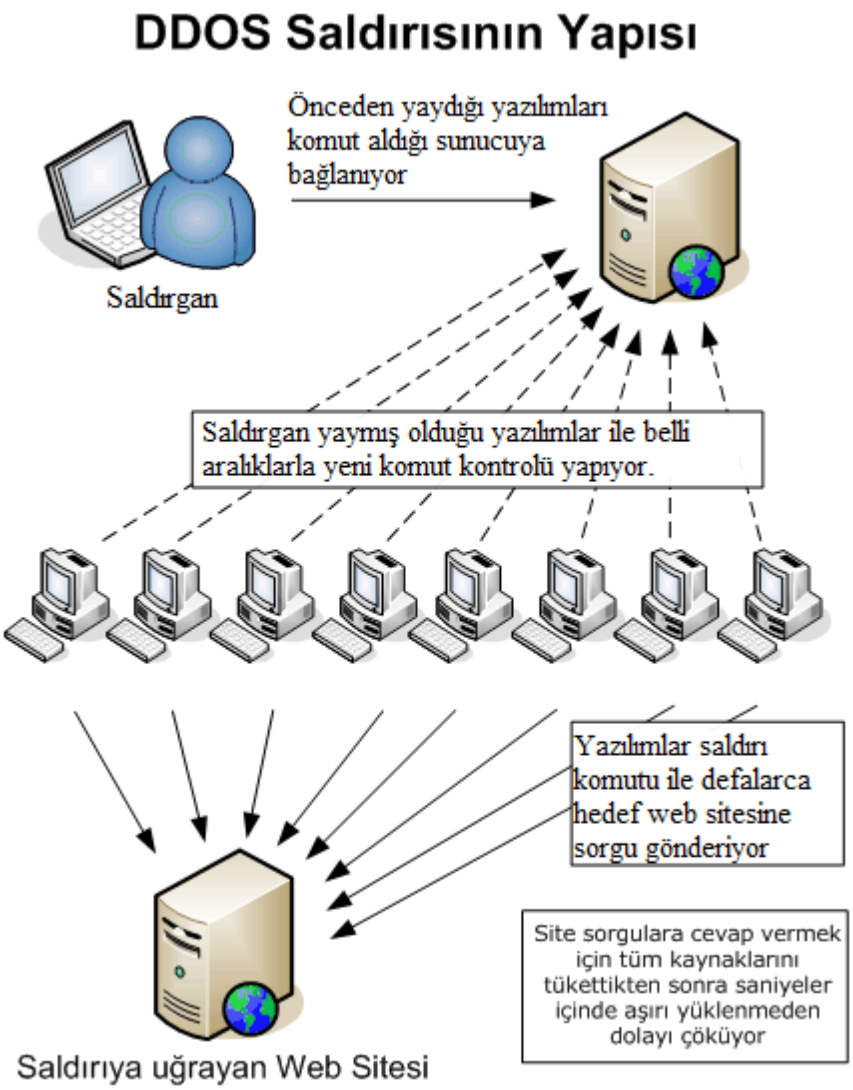
- **SYN (eşzamanlı) taşması: S**unucuya gönderilen ve istemci bağlantısı isteyen paket taşmasıdır. Paketlerde kaynak IP adresleri geçersizdir. Sunucu bu sahte isteklere yanıt vermekle uğraşırken geçerli isteklere yanıt veremez.

- **Ping of death (Ölüm pingi):** Bir cihaza, IP tarafından izin verilen maksimum boyuttan (65,535 bayt) büyük bir paket gönderilir. Bu tür saldırılar artık bilgisayar sistemleri üzerinde etkili değildir.

Dağıtılmış Hizmet Reddi ((Distributed Denial of Service–DDoS)

Dağıtılmış hizmet reddi (DDoS) saldırıları DoS saldırılarının farklı kaynaklardan yapılması ile gerçekleşir. Saldırganlar bazı yazılımlar tasarlayarak (Truva atı, solucan vb.) bu yazılımları *İnternet* kullanıcılarına e-mail ya da çeşitli yollarla yükleyerek geniş kitlelere yayar. Bu şekilde yetki elde ettikleri çok sayıdaki İnternet kullanıcılarının bilgisayarlarını istedikleri zaman istedikleri siteye binlerce sorgu göndermek için kullanır.

Saldırganın kontrolü altındaki onlarca bilgisayardan tek bir sunucuya binlerce sorgu göndermekte; bu da hedef makinenin band tüketmesine ya da tıkanmasına neden olmaktadır.



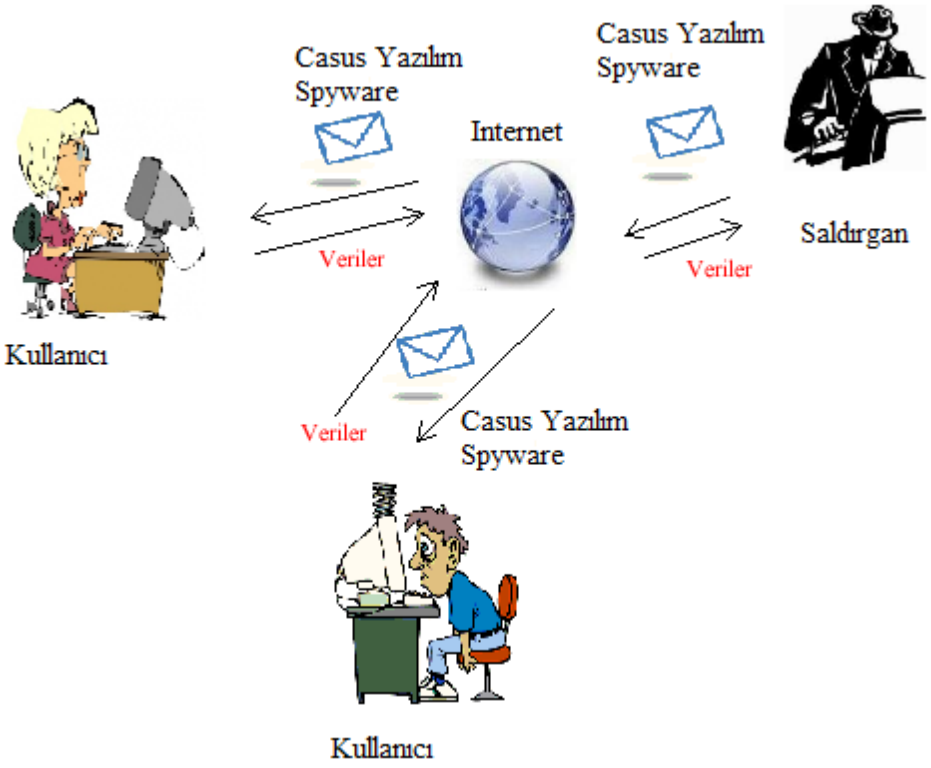
Deneme Yanılma

Ağ kesintilerine yol açan saldırıların tümü özel olarak DoS saldırıları değildir. Hizmet reddine yol açabilen başka bir saldırı türü de deneme-yanılma saldırısıdır. Deneme yanılma saldırılarında hızlı bir bilgisayar, parolaları tahmin etmeye veya bir şifreleme kodunun şifresini çözmeye çalışmak için kullanılır. Saldırgan, koda erişim kazanmak veya kodu çözmek için art arda hızlı şekilde çok sayıda olasılığı dener. Deneme yanılma saldırıları, belirli bir kaynakta aşırı trafik oluşması nedeniyle veya kullanıcı hesaplarının kilitlenmesiyle hizmet reddine yol açabilir.

Casus Yazılımlar

Casus yazılım (spyware) kişisel bilgi toplama veya kullanıcının onayı alınmadan bilgisayarın yapılandırmasını değiştirme gibi belirli davranışları gerçekleştiren programlardır. Casus yazılımlar genellikle kullanıcının onayı alınmadan bilgisayara kurulur. Kurulduktan sonra kullanıcının İnternette gezinti bilgileri toplanabilir. Bu bilgiler reklam veren kişi ya da kuruluşlara veya *İnternet*teki diğer kişilere gönderilir ve parola, hesap numarası gibi bilgileri de içerebilir.

Casus yazılım genellikle bir dosya indirilirken, başka bir program yüklenirken veya bir açılır pencereye tıklandığında bilmeden yüklenir. Bilgisayarı yavaşlatabilir ve dâhili ayarları değiştirerek diğer tehditler için daha fazla zayıflık oluşturabilir. Ayrıca casus yazılımı bilgisayardan kaldırmak çok zor olabilir.



İzleme Tanımlama Bilgileri

İzleme tanımlama bilgileri bir çeşit casus yazılımdır ancak her zaman kötü amaçlı değildir. Bir *İnternet* kullanıcısı web sitelerini ziyaret ettiğinde o kullanıcıya ilişkin bilgileri kaydetmek için tanımlama bilgisi (cookie) kullanılır. Tanımlama bilgileri, kişiselleştirme ve diğer zaman kazandıran tekniklere izin verdiği için kullanışlı ve aranan yazılımlar olabilir. Kullanıcının birçok web sitesine bağlanabilmesi için tanımlama bilgilerinin etkinleştirilmiş olması gerekir.

Reklam Yazılımları

Reklam yazılımı, kullanıcının ziyaret ettiği web siteleri temel alınarak kullanıcı hakkında bilgi toplamak için kullanılan yazılım biçimidir. Bu bilgiler daha sonra hedeflenmiş reklamcılık için kullanılır.

Reklam yazılımı genellikle "ücretsiz" bir ürün karşılığında kullanıcı tarafından yüklenir. Kullanıcı bir tarayıcı penceresini açtığında, Reklam yazılımı kullanıcının *İnternet*teki sörf hareketlerine dayanarak ürün veya hizmetlerin reklamını yapan yeni tarayıcı pencerelerini açabilir. İstenmeyen tarayıcı pencereleri ard arda açılarak, özellikle İnternet bağlantısı yavaş olduğunda *İnternet*te sörf hareketini çok zor hale getirebilir. Reklam yazılımının kaldırılması çok zor olabilir.

Açılır Pencereler

Açılır pencereler bir web sitesi ziyaret edildiğinde görüntülenen ek reklam pencereleridir. Reklam yazılımından farklı olarak, açılır pencereler kullanıcı hakkında bilgi toplamak için tasarlanmamış olup genellikle yalnızca ziyaret edilen web sitesiyle ilişkilidir.

Açılır pencereleri engellemek için tarayıcı özelliklerinden açılır pencere engelleyicisini etkinleştirmek gerekmektedir.

Spam

Bir e-postanın talepte bulunmamış, birçok kişiye birden, zorla gönderilmesi durumunda, bu e-postaya istenmeyen e-posta yani spam denir. Spamlar genellikle kitlesel veya ticari amaçlı olabilir.

Satıcılar bazen hedeflenmiş pazarlamayla uğraşmak istemez. Ürün veya hizmetlerinin birilerinin ilgisini çekmesi umuduyla e-posta reklamlarını olabildiğince fazla son kullanıcıya göndermek ister. Spam; *İnternet* hizmeti sağlayıcısını, e-posta sunucularını ve tek tek son kullanıcı sistemlerini aşırı yükleyebilen ciddi bir ağ tehdidir.

Spam listeleri genellikle arama sayfalarının taranması, tartışma gruplarının üye listelerinin çalınması veya web üzerinden adres aramalarıyla oluşturulur.

4- Güvenlik Önlemleri

Tanımlama ve Kimlik Doğrulama İlkeleri

Bilgisayar ağlarında tanımlama belirli bir kimlik sahibinin gönderilen mesaja bu bilgiyi eklemesi ile ifade edilir. Kimlik doğrulama, sunucu bilgisayar tarafından belirli kullanıcıları tanımlamak ve kendi verilerine erişim izinlerini doğrulamak için kullanılan işlemdir.

Parola ilkeleri

Bilgisayar ağlarında güvenlik önlemlerinde biri de ağa erişim için parola korumasıdır. İnternet erişimi için veya dosya sunucusuna erişim için güvenlik uzmanları parolalı koruma yöntemini geliştirmiştir. Parola ilkeleri, etki alanı hesapları veya yerel kullanıcı hesapları için de kullanılabilir.

Kabul Edilebilir Kullanım İlkeleri

Güvenlik tehditlerinin çoğu tanınmış web sitelerinden gelebilir. Web sitelerine erişimlerini yönetmeyen organizasyonlar risk altındadır. Ağ güvenlik filtreleme çözüm olarak kabul edilebilir. Web kategorisi organizasyonların dünya çapında kabul edilebilir kullanım ilkelerini kolaylıkla yönetmesini, casus yazılım, dolandırıcılık, klavye hareketlerini kaydetme ve diğer tehditleri içeren sitelere erişimi yasaklamasını sağlar.

Uzaktan Erişim İlkeleri

Uzaktan erişerek kullanılacak sistem başka bir binada veya kilometrelerce uzakta olabilir. Telnet, *İnternet*e bağlım herhangi bir makineye uzaktan bağlanmak için geliştirilen bu yöntemin genel adıdır. Uzaktan Erişim yapılacak bilgisayarı bir uzaktan erişim sunucusu gibi çalışmak üzere yapılandırarak, uzak veya hareketli çalışanların kuruluşunuzun ağlarına bağlanması sağlanabilir. Uzak kullanıcılar, bilgisayarları ağa fiziksel olarak bağlıymış gibi çalışabilir.

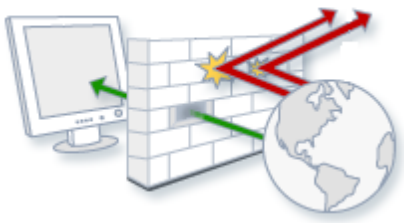
VPN Bağlantıları

Ağ güvenlik önlemlerinden biri de VPN (Virtual Private Network-Sanal Paylaşımlı Ağ) kullanılmasıdır. VPN çalışma mantığı, aslında olmayan ama farklı hatlar üzerinden ki *İnternet* sistemleri, uydu bağlantıları, kablo net yapıları farklı noktada olan iki ağı aynı ağda çalıştırmak kullanılabilir. Örneğin, iki farklı ülkede iki ayrı ağ kurmak için VPN kullanılır. VPN kullanıcıya hem dosyalarını aynı ağda paylaşmasını hem de içerde çalışan programları veya e-posta programlarını VPN yazılımı ile güvenli şekilde yapılacaktır.

GÜVENLİK ARAÇLARI VE UYGULAMALAR

1- Güvenlik Duvarı

Ağ güvenliğini sağlayabilmek için bir ağ güvenlik duvarı (network firewall) kullanılır. Bir ağ güvenlik duvarı kullanarak ağı dış saldırılardan korunabilir, ağa gelen ve ağdan giden verileri denetlenebilir ve yönetilebilir, istenmeyen istemcilerin (client) *İnternet* bağlantısı kesilebilir mevcut İnternet bağlantının bant genişliğini yönetilebilir.



2- Spam Filtresi

Spam Filtreleri, sunucuya gelen e-postaları bir süzgeçten geçirerek istenilmeyen e-postaları tespit eden ve kullanıcının gelen kutusuna (inbox) düşmesine engel olan programlardır. E-postalar spam filtrelerinde birçok kural ve kriterlere göre değerlendirilir. Her bir kural spam filtresi tarafından belirlenmiş olan belli puana sahiptir. Başlangıçta sıfır olan puan spam filtrelerinin kurallarına uyan her hangi bir eşleşme görüldüğünde bu puan toplam puana eklenir.

3- Yamalar ve Güncellemeler

Yazılımlarda zaman zaman hatalar veya eksiklikler keşfedilir. Bilgisayar sistemlerini dışarıdan gelecek saldırılara (virüs ya da bilgisayar korsanı) açık hâle getiren bu zaaflara güvenlik açıklığı denir ve ancak yazılımlar güncellenerek kapatılabilir. Bu açıklıkları giderme amacı ile yazılım ve işletim sistemleri geliştiricileri yeni sürümler, yazılım yamaları, ya da hizmet paketleri yayınlar.

4- Casus Yazılımlardan Korunma Yazılımları

Casus yazılımlar, bilgisayar kullanıcılarının gündemine artarak giren bir problem olmuştur. Casus yazılımlardan bilgisayarı korumak için işletim sistemi dâhilinde olan yazılım (Windows Defender) kullanılabilir. Bu yazılımın haricinde ücretli veya ücretsiz bir yazılım İnternetten indirilerek bilgisayara kurulabilir. "Ad-Aware SE" ve "Spybot Search & Destroy" adlı programlar ücretsiz olarak *İnternet*ten indirilerek bilgisayara kurulabilir. Kendi başlarına bir dereceye kadar etkili olmalarına karşın, beraber kullanıldıklarında hayli etkindir.

5- Açılır Pencere Engelleyicileri

İstenmeden açılan pencereler, tarama sırasında kullanıcıya sormadan kendiliğinden açılan pencerelerdir. Boyutları değişebilir ama genelde ekranın tamamını kaplamaz. Açılır pencereleri engellemek için bilgisayarda kullanılan tarayıcı üzerinde ayarlamaları yapmak yeterli olur. İşletim sisteminin üzerindeki tarayıcı veya kullanıcının kendisinin bilgisayara kurduğu tarayıcılarda bu özellikler bulunmaktadır. Açılır pencereleri engellemek içi öze programlarda kullanılabilir.

6- Antivirüs Yazılımlar

Bilgisayar sistemlerinin düzgün çalışmalarını engelleyen, veri kayıplarına, veri bozulmalarına ve çeşitli yollarla kendisini kopyalayan kötü amaçlı yazılımlara virüs denir. Her geçen gün yeni virüsler çıkmakta veya var olanların özellikleri değiştirilerek tekrar piyasaya sürülmektedir. Virüsler; bilgisayar sistemlerinin çalışmasını aksatma ve bozmanın yanı sıra verilerin silinmesi veya çalınması gibi kötü amaçları gerçekleştirmek için hazırlanmaktadır.

KABLOSUZ ORTAM GÜVENLİĞİ

1- Kablosuz LAN (Yerel Ağ) Güvenliği

Kablosuz ağ, iki veya daha fazla bilgisayar arasında kablo ile oluşturulan yapısal ağın kablo yerine alıcı ve verici cihazlar arasında radyo dalgaları ile iletişim sağlanan ve daha uzak mesafeler arasında ağ imkanı sunan bir teknoloji bütününün adıdır. Kablosuz yerel ağlar sağlık kurumları, hipermarketler, üretim kuruluşları, fabrikalar, akademik kurumlar ve ambarlar gibi birçok alanda yaygın hale gelmiştir. Günümüzde kablosuz yerel ağlar birçok iş sahasında genel amaçlı bağlantı alternatifi olarak kabul edilmektedir.

Kablosuz ağ da kablosuz ağ bağdaştırıcısı (ağ kartı), kablosuz modem veya kablosuz yönlendirici (router) gibi donanımlar kullanılabilir.

Kablosuz ağlardaki en temel güvenlik problemi verilerin havada transfer edilmesidir. Kablolu ağlarda switch ya da hub kullanarak güvenliği fiziksel olarak sağlanabilir ve switche / hub'a fiziksel olarak bağlı olmayan cihazlardan güvenlik önlemi alınabilir. Kablosuz ağlarda tüm iletişim hava üzerinden kurulur.

Kablosuz ağda güvenliği sağlamak için;

Erişim noktasının veya kablosuz modemin arayüz kullanıcı adı şifresi değiştirilebilir. Kablosuz ağda arayüze bağlanmak için tarayıcıya ara yüzün adresi yazılır.

Erişim noktasının (Access point) veya modemin yazılımı güncellenmelidir. Ara yüzü kullanılarak ayarlar sekmesinden yazılımı kullan seçeneği kullanılabilir.

Erişim noktası veya kablosuz modem kullanılmadığı zamanlarda kapatılabilir.

Mac Adresini filtrelemek, kullanıcının Mac adresi ile girilmeyen cihazların erişim noktasına bağlanmasını engeller. Modeminizin ya da erişim noktasının kablosuz ayarlar / güvenlik bölümünde Mac adres filtrelemesi kullanılabilir.

Kablosuz ağda IP havuzu belirlenerek havuzda bulunan IP adreslerinin ağa bağlanması sağlanabilir. Bu yöntem kullanılarak ağ trafiği hızlanabilir.

2- SSID

Hizmet Kümesi Tanıtıcısı (Service Set Identifier / SSID), belirli bir kablosuz ağa verilen addır. Kablosuz ağ adı (SSID) kablosuz yönlendirici üzerinde belirlenir. Kablosuz yönlendirici, atanmış SSID'yi yayınlayacak veya yayınlamayacak şekilde ayarlanabilir. Kablosuz yönlendirici SSID'yi yayınlayacak şekilde ayarlanmışsa kablosuz ağ bir yayın yapan ağdır ve saldırganlar tarafından bu ağ adı görüntülenebilir. Kablosuz yönlendirici SSID 'yi yayınlamayacak şekilde ayarlanmışsa, kablosuz ağ bir yayın yapmayan ağdır.

3- WLAN'a Saldırılar

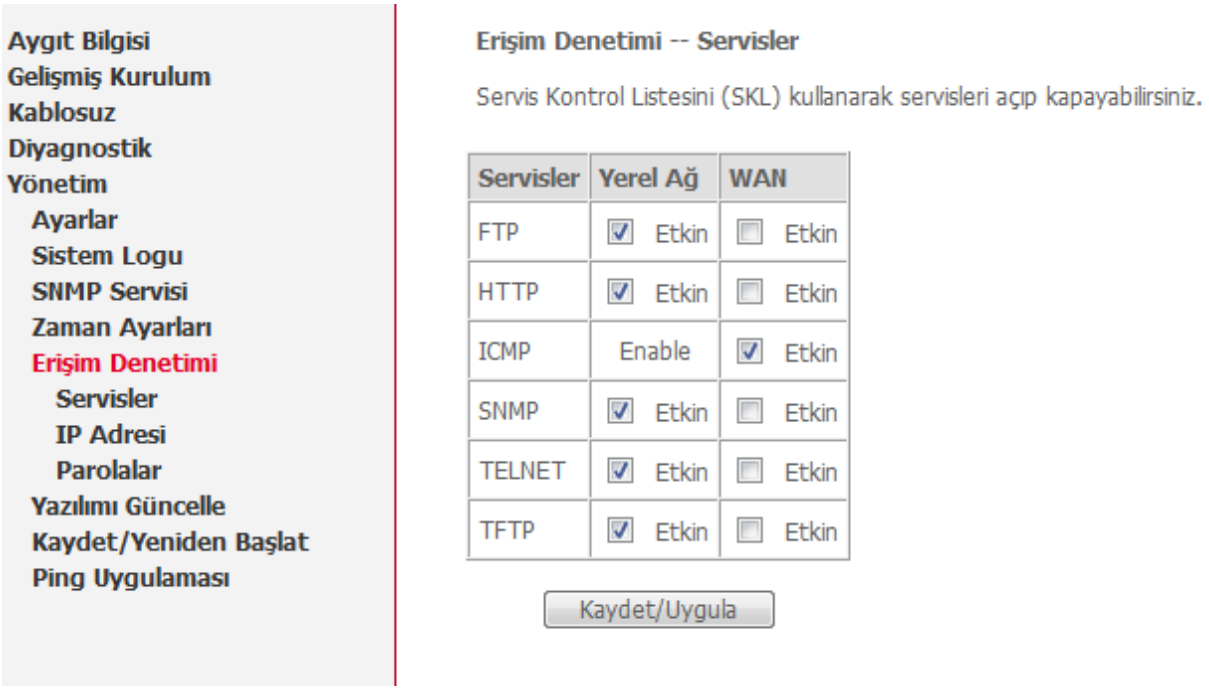
Kablosuz ağlardaki hızlı yaygınlaşma ve hız artışı, güvenlik önlemlerinin de daha fazla dikkate alınmasını mecburi kılmaktadır. Sistem yöneticilerinin ve ev kullanıcılarının konuyla ilgili olarak bilgi sahibi olmaları ve daha bilinçli davranmaları çok önemlidir. Ev kullanıcılarının konuyla ilgili olarak bilinçlendirilmeleri oldukça zordur. Bu nedenle, ev kullanıcılarını ilk etapta koruma görevi, kablosuz ağ erişim noktası satan ve İnternet erişimi sağlayan firmalar tarafından verilmesi en uygun yöntem olacaktır.

MAC adresini dinlemek çok kolaydır. Paket yakalama yazılımı kullanarak saldırgan kullanılan bir MAC adresini tespit eder. Eğer kullandığı kablosuz ağ kartını izin veriyorsa MAC adresini bulduğu yeni MAC adresine değiştirebilir ve artık hazırdır. Eğer saldırgan yanında kablosuz ağ donanımları bulunduruyorsa ve yakınında bir kablosuz ağ varsa aldatma (spoof) saldırısı yapabilir demektir. Aldatma saldırısı yapabilmek için, saldırgan kendine ait olan erişim noktasını yakınındaki kablosuz ağa göre veya güvenebileceği bir *İnternet* çıkışı olduğuna inanan bir kurbana göre ayarlamalıdır. Bu sahte erişim noktasının sinyalleri gerçek erişim noktasından daha güçlüdür. Böylece kurban bu sahte erişim noktasını seçecektir. Kurban bir kere iletişime başladıktan sonra, saldırgan onun şifre, ağ erişim ve diğer önemli bütün bilgilerini çalacaktır. Bu saldırının genel amacı aslında şifre yakalamak içindir.

4- WLAN'a Erişimi Sınırlama

Kablosuz ağ güvenliğinde MAC ve IP adresi filtreleme yöntemlerinden farklı olarak erişim noktası sınırlama ayarları mevcuttur. Güvenlik duvarı arkasında bulunan erişim noktaları incelendiğinde zayıf noktaları olarak kablosuz ağ girişleri, konferans odalarındaki ethernet portları, taşınabilir laptoplar ve yetkilendirme yapılmamış diğer uçlar (PC, yazıcı vs) gözü çarpmaktadır. Bu noktalar ağın toplam güvenliği için ciddi risk oluşturmaktadır.

Kablosuz ağlarda, ağ erişim kontrolü (NAC) de kullanılabilir. NAC kurumların iletişim ağını kullananların, ilgili kurumun güvenlik politikası kurallarına uygunluğunu denetleyen bir güvenlik teknolojisidir. NAC ile sadece şirket ağ politikalarına uyan ve güvenilir olan masaüstü bilgisayar, dizüstü bilgisayar, sunucu ve cep bilgisayarının (PDA) şirket ağına bağlanmasına izin verilmektedir.



5- WLAN'da Kimlik Doğrulama

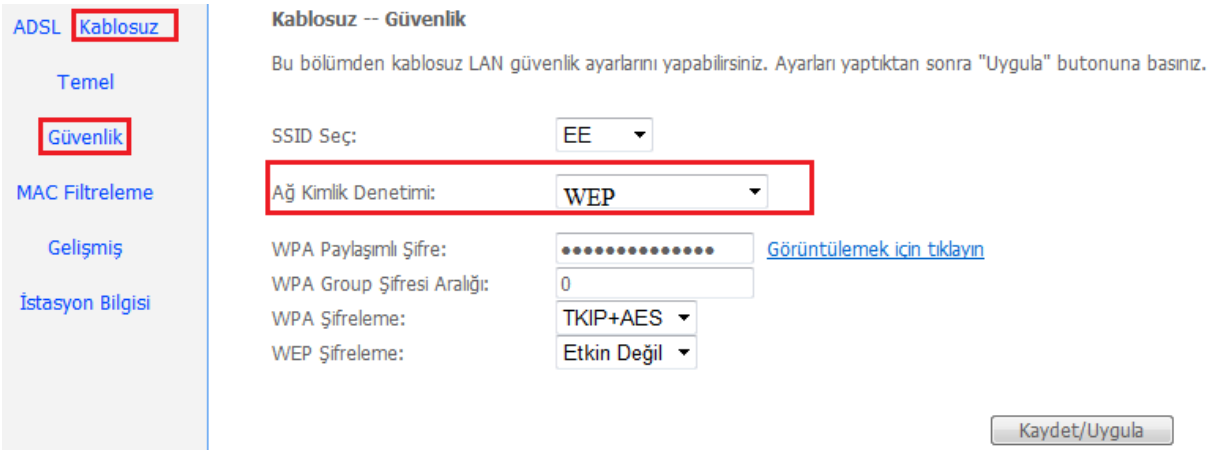
Kablosuz ağ standardı kimlik doğrulama için iki adet mekanizma sunar bunlar, açık kimlik doğrulama ve paylaşılmış anahtar kimlik doğrulamasıdır. Standart dâhilinde olmayana ancak sıkça kullanılan diğer iki yöntem de SSID (Service Set Identifier) ve MAC (Media Access Control) değerlerinin kimlik doğrulamada kullanılmasıdır. SSID değerinin kullanılması aslında ağın mantıksal olarak bölümlere ayrılmasını sağlar ve bir kimlik doğrulama mekanizması olarak düşünülmüş bir yöntem değildir ancak güvenliği artırıcı ek bir önlem olarak değerlendirilebilir. Her hangi bir istemcinin ağdan hizmet alabilmesi için doğru SSID değeri ile yapılandırılmış olması gerekir.

6- WLAN'da şifreleme

Kablosuz ağların güvenliğinin sağlanması için ağların şifrelenmesi yöntemi geliştirilmiştir. Kablosuz ağlarda trafiğin başkaları tarafından izlenmemesi için alınması gereken teme önlemlerden biri de trafiği şifrelemektir. Kablosuz ağlarda şifreleme WEP (Wired Equivalent Privacy) ve WPA (Wi-Fi Protected Access) olarak adlandırılan iki protokol üzerinden yapılır. Her iki protokol de ek güvenlik önlemleri alınmazsa günümüzde güvenilir kabul edilmez.

WEP

802.11 standardı, kablosuz alan ağlarında ortaya çıkan haberleşmelerin tanımlandığı bir standarttır. WEP (Wired Equivalent Privacy) algoritması her türlü haricî saldırıdan kablosuz haberleşmeyi korumak için kullanılır. WEP'in ikinci fonksiyonu ise kablosuz ağa yetkisiz erişimleri engellemektir. WEP bir mobil cihaz istasyonu ve erişim noktası arasındaki kablosuz haberleşme kurmak ve paylaşımda bulunabilmek için bir şifreye ihtiyaç duyar. Bu şifre ya da güvenlik anahtarı veri paketlerini göndermeden önce onları şifrelemek ve gönderim sonrasında değişikliğe uğrayıp uğramadıklarını için diğer bir ifadeyle doğruluk kontrolü yapmak amacıyla kullanılır.



WPA

WPA kablosuz ağlar için geliştirilmiş bir şifreleme standardıdır. Bu standart daha önceki WEP (Wired Equivalent Privacy-Kabloya Eş Güvenlik) sisteminin yetersizliğine karşılık geliştirilmiştir. WPA, veri şifreleme ve kullanıcı kimlik denetimi alanlarında bilgi güvenliği sunmaktadır. WPA, veri şifreleme işlemini geliştirmek için bu konuda yeni bir yöntem sunarak şifreleme anahtarlarını otomatik olarak dağıtır. Bir bit veri bile şifreleme anahtarlarıyla korunur. Bu çözüm aynı zamanda, veri üzerinde bütünsel bir kontrol yaparak, verileri ele geçirmek isteyen kişilerin bilgileri değiştirmesini engeller. WPA, kurumsal kullanıcıların korunması için, ağ üzerindeki her bir kullanıcıya kimlik denetimi uygularken, bu kullanıcıları veri hırsızlığı amacıyla düzenlenmiş ağlara geçişini de engeller. Aynı zamanda WPA ile 48 bitlik bir şifreleme yapılır.

7- WLAN'da Trafik Filtreleme

WLAN'a kimlerin erişim kazanacağının ve iletilen verileri kimlerin kullanabileceğinin denetlenmesinin yanı sıra WLAN üzerinden iletilen trafik türünün de denetlenmesi yararlıdır. Trafik filtrelemesi kullanılarak bu gerçekleştirilir.

Trafik filtrelemesi, istenmeyen trafiğin kablosuz ağa girmesini veya kablosuz ağdan çıkmasını engeller. Trafik, erişim noktası üzerinden geçerken erişim noktası tarafından filtreleme yapılır. Belirli bir MAC veya IP adresinden trafiği kaldırmak ya da belirli bir MAC veya IP adresine trafiği hedeflemek için filtreleme yapılabilir. Bu işlev, belirli uygulamaları da bağlantı noktası numaralarına göre engelleyebilir. İstenmeyen ve şüpheli trafik ağdan kaldırılarak, önemli trafiğin hareketine daha fazla bant genişliği adanır ve WLAN'ın başarımı artırılır. Örneğin, kimlik doğrulama sunucusu gibi belirli bir makineyi hedefleyen tüm telnet trafiğini engellemek için trafik filtreleme kullanılabilir. Kimlik doğrulama sunucusuna yönelik telnet girişimleri şüpheli olarak değerlendirilir ve engellenir.

KAYNAKLAR

1- **Bilgisayar Ağları ve İletişim ,**Murat KARA – *2014*

2- **BİLİŞİM TEKNOLOJİLERİ, Ağ Güvenliği, T.C. Milli Eğitim Bakanlığı, Ankara 2013**