PAKET VE PORT ANALİZİ İLE
AĞ SALDIRI TESPİT SİSTEMLERİ

Erkan ÖZHAN

YÜKSEK LİSANS TEZİ

BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI
Tez Yöneticisi: Yrd.Doç.Dr. Erdem UÇAR

EDİRNE - 2006

T.C.
TRAKYA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

PAKET VE PORT ANALİZİ İLE AĞ SALDIRI TESPİT SİSTEMLERİ

Erkan ÖZHAN

YÜKSEK LİSANS TEZİ
BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI

Tez Yöneticisi: Yrd.Doç.Dr. Erdem UÇAR

EDİRNE – 2006

ÖZET

Bilgiye ulaşma, kullanma, saklama ilk çağlardan beri, toplumların gelişmişlik ve yaşam seviyesinin belirlenmesinde en önemli unsurlardan biri olmuştur. Bu faktör ülkeler arası rekabette bir ülkenin diğerlerinden bir adım önde olmasını sağlamış ve günümüzde daha da büyük önem kazanmıştır. Bilgiye her yerden, hızlı bir şekilde ulaşmak önceleri ilk amaç olarak benimsenmiş ancak günümüzde bu amaçlara bir yenisi daha eklenmiştir. O da güvenliktir. Artık bilgiye her yerden, hızlı ve güvenli bir şekilde ulaşmak amaç olmuştur. Bunun yanında bilgilerin depolandığı ortamlarda değişmiştir. Kitaplar yavaş yavaş terk edilmeye başlanmış ve dijital ortamlarda saklanan elektronik kitaplar tercih edilir olmuştur. Dijital ortamlar, kitaplara ve diğer depolama yöntemlerine göre birçok yönden çok daha avantajlı bir hale gelmiştir. Bu nedenle de bilgiyi kullanmak ve saklamak artık bilgisayarlar tarafından yapılmaya başlamıştır. Bunun bir sonucu olarak da Internet doğmuştur. Çok kapsamlı ve karmaşık bir yapıya sahip olan Internet beraberinde birçok sorunu da getirmiştir. Bu sorunların başında güvenlik gelmektedir. Donanımsal ve yazılımsal problemler güvenliğe göre çok daha az öneme sahiptir. Ancak Güvenliği sağlamak için de kullanılması gereken öğeler donanımlar ve yazılımlardır. Her ne kadar hala problemler olsa da Internet günümüz dünyasının vazgeçilmez bir aracıdır ve artık bir bilim dalı haline gelmiştir. Bu tez çalışmasında, saldırı tespit sistemleri incelenecek, bilgisayar ağlarının güvenliğini yazılım kullanarak sağlamak amacıyla da paket ve port analizi metotları paralelinde örnek yazılımlar geliştirilmeye çalışılacaktır. Ancak, öncelikle bu tez içerisinde yaygın bir şekilde incelenecek olan Bilgisayar Ağları, Haberleşme Yöntemleri, vb. konularıdır. Daha sonra paket ve port analizi ile ağ saldırı tespit sistemi örnekleri programlama dilleri kullanarak elde edilen sonuçlar bu teze aktarılacaktır.

Anahtar sözcükler : Saldırı Tespit Sistemleri, Snort, PHAD, TCP FIN Scan

Yıl : 2006

Sayfa: 82

ABSTRACT

Reaching, using and saving the information has been one of the most important factors in determining the development level of societies since ancient times. This factor has provided a leading step for a country among the others in the international competence and has gained most importance recently. Reaching information from everywhere in a fast manner was seen among the first objectives at the beginning. However a new objective has been added to these ones nowadays: security. "Reaching the information from everywhere in a fast and secure manner" has now become the objective. Moreover, the environment where the information is stored has changed. Hard copy books have been abandoned slowly. Most books have been stored in digital environments. In various manners, digital environments have become more advantageous than books and other storing methods. Therefore, using and saving the information have been conducted by computers. As a result, internet was born. Internet which has a very extensive and complex structure has carried many problems itself. Security is the first problem among all. Hardware and software problems have a very low importance than security. But, in order to provide security the items which must be used are hardware and software. In spite of these problems, internet is one of the tools which cannot be abandoned of today's world and has become a scientific discipline. In this study, attack determination systems will be analyzed. Furthermore, in order to provide security in computer networks by using software, sample software which are parallel to packet and port analysis methods will be developed. The topics like Computer Networks, Communication Methods, etc. which will be widely referred to in this thesis will be given at first. Then, the results obtained by using programming languages on the samples of intrusion detection systems with packet and port analysis will be transferred in the thesis.

Keywords: Intrusion Detection Systems, Snort, PHAD, TCP FIN Scan.

Year : 2006

Page : 82

ÖNSÖZ

Bu tez çalışmasının her aşamasında desteğini esirgemeyen ve tecrübelerini benimle paylaşan değerli hocam Yrd.Doç.Dr. Erdem UÇAR'a, tezimin bitmesini dört gözle bekleyen ve en zor anlarımda yanımda olan sevgili annem ve babama teşekkür ederim.

Erkan ÖZHAN

İÇİNDEKİLER

SİMGELER ve KISALTMALAR LİSTESİ

NIC	: Network Interface Card (Ağ Kartı)
USB	: Universal Serial Bus
LAN	: Local Area Network
Gbps	: Giga Bit Per Second
WAN	: Wide Area Network
Kbps	: Kilo Bit Per Second
UpLink	: Ağ Omurga Bağlantısı
Stack	: Veri Yığını
LinkLayer	: Veri Bağı Katmanı
VCR	: Video CD Recorder (Video CD Kaydedici)
LLC	: Logical Link Control
IEEE	: Elektrik ve Elektronik Mühendisliği Enstitüsü
MAC	: Media Access Control
TR	: Token Ring
FR	: Frame Relay
FDDI	: Fiber Distributed Data Interface
PARC	: Palo Alto Research Center
ISDN	: Integrated Services Digital Network
OSI	: Open Systems Interconnection
ISO	: International Organizations of Standarts
SAP	: Service Access Point

ŞEKİLLER LİSTESİ

ÇİZELGELER LİSTESİ

BÖLÜM I

1.1 BİLGİSAYAR AĞI KULLANMA NEDENLERİ

İletişim, herhangi bir karar alma sürecinde çoğunlukla anahtar öğedir ve bunun varlığı ya da yokluğu bir projeyi başarı ya da başarısızlığa götürür. Bir çalışan işyerinde değilse, bir bilgi notu birisinin masasından kaybolduysa ya da kişiler bir araya gelip bilgi paylaşamayacak kadar meşgulseler, iletişim kopabilir ve kötü bir iş karan alınabilir. Bilgisayarları birbirine bağlayarak, aynı zamanda bilgisayar ekranlarının önünde oturan personelinizi de birbirine bağlarsınız. Bilgisayarın ekran ve klavyesi (varsa mikrofon, hoparlör ve video konferans kamerası) personelin göz ve kulaklarının bir uzantısı haline gelir; bu da personel arasındaki iletişimi daha da kolaylaştırır.

1.1.1 Dosya ve Klasörleri Paylaşma

Birden çok bilgisayarın olduğu ortamlarda er ya da geç dosyaları veya klasörleri paylaşma ihtiyacı doğacaktır. Bir dosya hazırladınız ve işinizi bitirdiniz. Bu dosyayı kullanmak isteyen kişiler ağ ortamı yoksa öncelikle sizin bilgisayarınıza gelip sizden bu dosyanın bir kopyasını diskete vb. ortama almalı daha sonra ise tekrar kendi bilgisayarına giderek bu dosyayı kullanabilir. Tekrar sizin fikrinizi veya düzeltmelerinizi istediğinde ise diskete kopyalamalı ve size ulaştırması gerekir. Disketleri karıştırmadan kullanmak, dosyaların kolay bulunmasını sağlamak amacıyla daha birçok işlem yapmanız gerekir. Bu ve benzeri problemlerden dolayı, ağ kullanmak dosya ve klasör paylaşmak açısından çok önemlidir. Bu sayede yerinizden kalkmadan dosyaları ve klasörleri diğer kişilerle paylaşabilir zamandan ve emekten büyük tasarruf sağlayabilirsiniz. [11]

1.1.2 Belgeleri Güncel Tutma

Belge üzerinde çalışırken aynı anda birçok kişi bu belgenin bir kopyasına disketle ulaşarak çalışma yapmış olabilir. Dolayısı ile aynı belgenin birden çok sürümü

ortaya çıkar. Bu durumda tam bir kabus yaşanır. Düzeltmeler kişiden kişiye değişiklik gösterir. Bu düzeltilmiş belgelerin bir çıktısı alındığında ise aralarında çok fark olduğu görülür. Bunun yanında belgeler üzerindeki işlemlerin de birleştirilmesi, ayıklanması çok zaman alacaktır. Bir işletmede yapılan tüm satışları görmek için, bayan reyonundan ayrı bir tablo, erkek reyonundan ayrı bir tablo vb. gelecek be bunları toplamak listelemek zorunda kalacaksınızdır. Ağ ortamında ise tek bir belge üzerinde tüm departmanlar işlem yaparlar ve hepsi tek bir belgede kaydolunur.

1.1.3 Önemli Belgeleri Koruma

Bir dosyanın tek bir çalışma kopyasının olmasını istediğinizde diğer bilgisayarlarda da yedek kopyasını yapabilirsiniz. Bu yolla, sabit disk sürücüsü zarar görürse ve özgün dosya bozulur ya da kaybolursa, her zaman güvenli bir ağ dosyanız olacaktır. Ağ üzerindeyseniz, yeni bilgisayarlarda bulunan yüksek kapasiteli disk sürücülerinden yararlanarak dosyaları sistem üzerinde bir başka sabit disk sürücüsüne yedekleyebilirsiniz. Bir dosyayı ağda bulunan bir bilgisayardan diğerine taşımak, diskete veya CD'ye yedek kopyalamaktan daha hızlıdır.

1.1.4 CD Karıştırmaktan Kurtulmak

İşletmelerle ilgili bilgilerin çok büyük bir kısmı artık CD'ler üzerinde bulunmaktadır. Ayrıntılı teknik bilgiler, muhasebe ve mühendislik verileri, yasal başvurular ve göndermeler, endüstri standartları, kitap yığınlarına ve basılı kullanım kılavuzlarına alternatif olarak artık CD üzerinde kolayca bulunabilir. CD'lerin tüm kapasitesinden yararlanmanız için çok iyi bir indeksleme yapanız gerekir ki bu çok zahmetlidir. Bir teknik özelliğe, göndermeye ya da başka bilgilere bakma gereği duyduğunuzda, o konuyla ilgili CD'yi bulmanız ve kendi CD sürücünüze takmanız gerekir. Bunu yaparken de birçok kez CD değiştirmeniz gerekebilir. Ağ ortamında ortak kullanım dosyaları alfabetik ve kategorize edilmiş bir şekilde sunucu ortamında bulunmuş olsaydı tüm bunlara gerek kalmayacak ve verimliliğiniz artmış olacaktı.

1.1.5 Yazıcıları Paylaşma

Bilgisayarların yaygınlaşması ile birlikte bilgisayarda elde edilen sonuçların yayınlanması ve çoğaltılması da önem kazanmıştır. Bu amaçla birçok işletmede yazıcı, plotter vb. kullanılmaya başlanmıştır. Kaynakların idareli kullanılması açısından

işletmedeki her bilgisayara ayrı ayrı yazıcı satın almak çok maliyetli ve zahmetli bir iştir. Ağ ortamlarında ise bir yazıcıyı birden çok bilgisayar rahatlıkla kullanabilir. Hem emek hem de maliyetler açısından bu durum kazanç sağlar. Günümüzde yazıcıların bilgisayarlara tanıtılması sorunu da yeni işletim sistemlerindeki sürücü dağıtma özelliği sayesinde ortadan kalkmıştır. Ağdaki bilgisayarlardan birine direkt olarak bir yazıcıyı tanıtıp paylaşıma açtığınızda diğer bilgisayarlar paylaşıma açılan yazıcının sürücülerini otomatik olarak yükleyecek ve kullanmaya başlayacaktır. Bunun yanında günümüz yazıcıları ağ ortamında bir bilgisayar gibi davranarak kendi IP leri sayesinde hiçbir bilgisayara bağımlı olmadan da artık hizmet verebilmektedir.

1.1.6 Internet'i Paylaşma

Internet siber uzaydaki bir toplanma yerinden daha öte bir şeydir. İşletmenizin büyüklüğü ne olursa olsun, Internet önemli bir işletme aracıdır. Internet:

- ürün ve hizmetlerin alınıp satılma yoludur;
- reklam yeridir;
- alıcı ve satıcı ile iletişim demektir;
- nerede olursanız olun, işyerinizle bağlantıda olma yoludur ve
- birçok yönden, işyeri ağınızın bir uzantısı gibi ele alınabilir. İşyeriniz küçükse, herkesle paylaşabileceğiniz yalnızca bir Internet hesabınız olabilir. Bununla birlikte bir çok Internet Servis Sağlayıcılarının (ISS) çoğu, sahip olduğunuz ekran adlarının ve e-posta hesaplarınızın sayısına bakmaksızın, hesap başına yalnızca bir kişinin oturum açmasına izin verir. İşyerinizde Internet'e erişim gereği duyan her bir kişi için ayrı bir Internet hesabı almanız gerekebilir ve bu da zamanla pahalı gelmeye başlar. Ancak istemci/sunucu ağı üzerinde Microsoft Small Business Server kullanıyorsanız, gerçekten kendi Internet sitenize ev sahipliği yapabilirsiniz.

İşyeri bilgisayarınızı bir ağa bağladığınızda, işyerinizdeki herkes tek bir ISS hesabını paylaşabilir. Küçük bir ev işletmeniz varsa, bir modem ve bir telefon hattını da paylaşabilirler. Böylece işyerindeki herkes, tümü aynı zamanda olmak

üzere çevrimiçi sohbet edebilir, web'i tarayabilir ve hatta yazılım yükleyebilir. Paylaşımın bazı kusurları da yok değildir. Birden çok kişi Internet'e bağlı ise tarama ve yükleme yavaşlayabilir. [14]

1.1.7 Çalışma Grubunu Yönetme

Bütün işletmeler, ne kadar küçük olursa olsunlar, bir takım olarak çalışmak zorundadır. Tek kişilik bir dükkan çalıştırsanız bile, işlerinizin yolunda gitmesi için müşteriler, bankacılar, muhasebeciler, avukatlar ya da diğer profesyonellerle birlikte çalışmaya gerek duyarsınız. İki kişiden iki yüz kişiye kadar daha büyük işletmelerde, takım çalışması daha da önemlidir. Programlar koordine edilmeli, gelişmeler denetlenmeli ve zamanı geldiğinde ayrı proje parçaları bir araya getirilmelidir. Eğer parçalar birbirini tutmazsa, tüm takımın önemli bir sorunu var demektir.

Ağ iletişimi çalışma grubunu teşvik ederek takım çalışmasına yardımcı olur. Bir çalışma grubu aynı proje ya da iş üzerinde çalışan iki veya daha çok kişiden oluşur. Bilgisayarlarınız bir ağın parçası olduğunda, takım üyeleri arasındaki yardımlaşma ve işbirliği daha kolay ve verimli olur. [6]

BÖLÜM II

2. AĞ KAVRAMLARI

Bilgisayar ağı, bilgisayar be benzeri sayısal sistemlerin belirli bir protokol[1] altında iletişimde bulunmasını sağlayan sistem ve sistemler bütünüdür. Ağ üzerindeki bilgisayarlar, birbirlerinden çok uzakta olsalar bile aynı protokol sayesinde karşılıklı çalışabilirler. Karşılıklı çalışma, ağ üzerindeki iki sistemin uygulamaya dönük ortak prosesler yürütmesi olarak tanımlanabilir.

Bilgisayar ağı, genel olarak geniş bir anlama sahiptir. Bir ofis içerisindeki birkaç bilgisayar ve bir yazıcının bir HUB(bkz. Sayfa 7) cihazı üzerinden bağlanıp belirli bir protokol altında haberleşmeleri de bir ağ oluşturur, tüm dünyaya yayılmış Internet de bir ağdır. Ağın büyüklüğü ne olursa olsun, ağ kapsamında, iletişimde bulunacak uç sistemler, ağı oluşturan HUB, Switch, Router gibi ağ cihazlar ve kablolama alt yapısı (veya kablosuz iletim ortamı) vardır.

2.1 Kablo Türleri

Kablo bir şehir şebekesinde boru hattı gibi işler görür. Bu hatta meydana gelen problemler veya aksaklıklar ciddi iş kayıplarına neden olabilir. Bu nedenler kablo seçimi bilgisayar ağları kurulumunda son derece önemli yer tutar.

Ethernet ağları, bilgileri diğer ağ bağlantı türlerinden daha hızlı gönderen kablolarla bağlanırlar. Kablolar bağlı olduğu sürece, bilgi akışında çok az girişim olabilir. Şirket ağlarında bilgiler, donanımın hızına ve kullanılan kablolara bağlı olarak, saniyede 10 milyon bit (Mbps), 100 Mbps ya da 1000 Mbps hızlarında kablolardan iletilirler.

Bir dosyanın çevrimiçi (örneğin Internet'ten) yüklenmesini beklemediyseniz, bu sayıların sizin için çok anlamı olmayabilir. Günümüzün en hızlı telefon modemleri, süper bir telefon hattınız varsa, 53.000 bit/sn (bps) hızında dosyaları yükleyebilmektedir. Internet'ten yüklenmesi 10 dakika alan bir dosyanın ağ üzerindeki bir bilgisayardan diğerine geçmesi yalnızca birkaç saniye alır. [7]

---

[1] Protokol, iletişimin nasıl kotarılacağını belirleyen kurallar dizisidir; birbirinden farklı birçok protokol vardır.

Ethernet ağlarında her bilgisayara kablo döşemeniz gerekir. Bilgisayarlar aynı odada ya da bitişik odalardaysa bu sorun değildir ve duvarlara delik açılmasına aldırmazsınız. Bilgisayarlarınız işyerine yayılmışsa, kabloyu asma tavandan geçirmek ya da inşaat veya tadilat sırasında kabloları döşemek gibi birçok duvar delmeden kabloları döşeme şansınız olmadıkça, kablo döşemek bir sorun olabilir.

En yaygın iki kablo türü çift bükümlü olan 10Base-T kablosu ile 10Base2 koaksiyel (ThinNet olarak da bilinir) kablodur. Fiber optik kablolar o kadar yaygın olmasa da giderek göze girmektedir. 10Base-T, çift bükümlü kablonun 10 Mbps maksimum hızından adını alır. 10Base2 is koaksiyel kablonun iç çekirdek ve dış metal örgü olmak üzere iki bölümü olduğu için bu biçimde adlandırılmıştır.

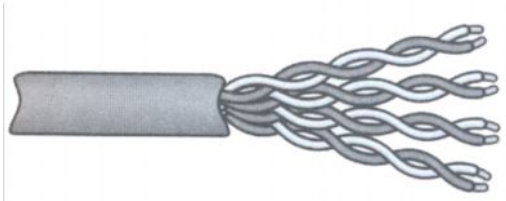
2.1.1 Çift Bükümlü Kablo

Çift bükümlü kablo birbiri üzerine bükülmüş iki bakır tel içeren yuvarlak bir kablodur; bir kablo içinde iki ya da sekiz çift tel olabilir. Çift bükümlü kablonun, Şekil 2.1'de gösterildiği gibi büyük telefon kutularına benzeyen bağlayıcıları vardır. Ağ kablosu bağlayıcıları RJ-45 olarak etiketlenir ve telefon bağlayıcıları RJ-11 olarak etiketlenir; birbirinin yerine kullanılamazlar.

a) RJ-45 Konnektörü b) RJ-11 Konnektörü

Şekil 2.1 Ağ kablosu bağlayıcıları (Konnektörleri)

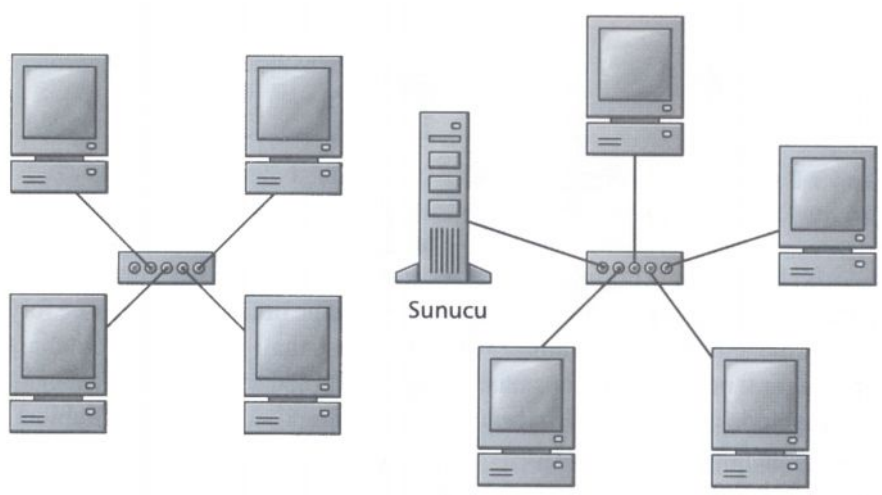
Çift bükümlü kablo iki türde olur: blendajsız çift bükümlü kablo (UTP) ve blendajlı çift bükümlü kablo (STP). Şekil 2.2'de gösterildiği gibi, UTP kablo, bir yalıtkan kılıfın içinde çiftler halinde birbirine bükülmüş sekiz yalıtılmış telden oluşur.



Şekil 2.2 Çift Bükümlü Kablo

STP kablosu UTP kabloya benzer ama telleri dış elektrik sinyallerinden korumak için, plastik kılıfın içinde tellerin çevresine örülmüş bir bakır ve folyo tabakasına sahiptir. STP kablo UTP'den daha pahalı olup, ağır ve daha az esnek olması nedeniyle de çalışması güçtür. Bir kablodaki sinyallerin yanındaki diğer kablodaki sinyallerle karışmasına karşı dirençli olması da STP kablonun avantajıdır.

Çoğu durumda, ağınızı çift bükülmüş kablo türlerinden biriyle döşediğinizde, tüm kablolar Şekil 2.3'te gösterilen hub denilen bir aygıtta birleşmelidir. Hub, tüm yolların bir araya geldiği ve trafiğin herhangi bir yöne akabileceği bir trafik kavşağı gibi davranır. Bu, kabloların tümünü şirketteki merkezi bir konumda birleştirmeniz gerektiği ve bilgisayarların iletişim kurabilmesi için hub'ın açık olması gerektiği anlamına gelir. Tüm iş istasyonları merkezdeki hub'la etkinleştirildiği için, bu tür bir düzene yıldız topolojisi denir. [6]

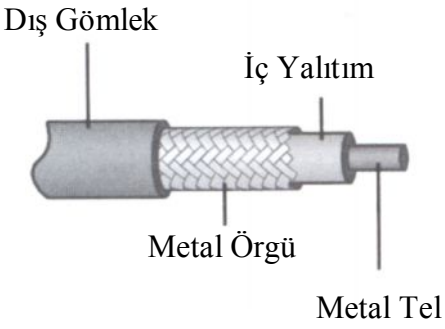


Şekil 2.3 Çift Bükümlü kablo döşenen bir ağda, tüm kablolar hub'da toplanır

Hub bir bilgisayardan bilgi çerçevesi aldığında, çerçevenin hedefinin hangi bilgisayar olduğuna bakmadan, çerçeveyi kendisine bağlı diğer bilgisayarların tümüne gönderir. Her bilgisayar çerçevedeki hedef adresine bakar ve çerçevenin kendisine ait olup olmadığını belirler. Böylece, ağdaki tüm bilgisayarlar paketi görebilir, ama yalnızca paketin gönderildiği bilgisayar paket üzerinde işlem yapabilir.

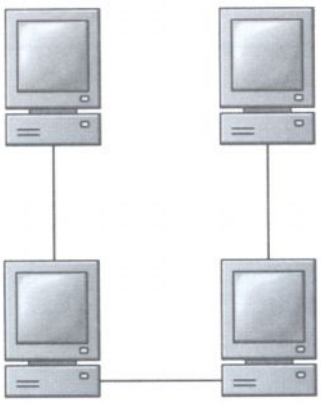
2.1.2 Koaksiyel Kablo

10Base2 koaksiyel kablo çift bükümlü kabloya bir seçenektir. VCR'nizdeki ya da kablo kutunuzdaki koaksiyel kabloya çok benzer, ancak biraz daha ince olup bu yüzden ince Ethernet ya da ThinNet de denir. Şekil 2.4'de gösterildiği gibi, koaksiyel kablo, içinde yalıtılmış bir tel ile dış kılıfının altında bir metal örgü katmanı olan yuvarlak bir kablodur. Diğer koaksiyel kablolardan daha ince olsa da, 10Base2 koaksiyel kablosu çift bükümlü kablodan daha kalındır; bu nedenle duvarlardan geçirip, süpürgelikler boyunca döşenmesi biraz daha zordur.



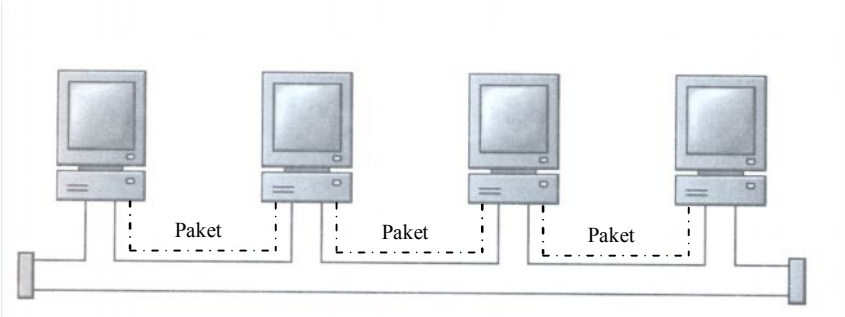
Şekil 2.4 10Base2 Koaksiyel Kablo (ThinNet)

Bir koaksiyel kablo ağı hub'a gerek duymaz. Şekil 2.5'te gösterildiği gibi, kabloyu bir bilgisayardan diğerine döşemeniz yeterlidir. Merkezi bir hub'ın olmayışı odadan odaya ya da katlar arasında döşemeniz gereken kablo miktarını azaltır. Bu tür yerleşime veri yolu topolojisi denir. Daha uzun bir kablo yapmak için, iki koaksiyel kabloyu birleştirebilirsiniz. Bir bağlantıyla birleştirilmiş iki boy koaksiyel kablo, birleştirilmiş iki boy çift bükümlü kablodan daha güvenilirdir. [7]



Şekil 2.5 Koaksiyel kablo hub olmadan bilgisayarları doğrudan birbirlerine bağlar

Bir bilgisayar koaksiyel kabloyu kullanarak bir çerçeve gönderdiğinde, Şekil 2-6'da gösterildiği gibi, çerçeve kablo üzerinde her iki yönde gönderilir. Her bilgisayardan geçer ve yalnızca gönderildiği bilgisayar tarafından kabul edilir.



Şekil 2.6 Koaksiyel kabloda çerçeveler her iki yönde gönderilir

2.1.3 Fiber Optik Kablo

Hızı ve büyük miktarlarda bilgileri işleme becerisi nedeniyle, fiber optik kablolar daha büyük ağlarda giderek yaygınlaşmaktadırlar. Fiber optik kablo, içinden ışık vurularının geçtiği ince bir cam lifinden oluşur. Işık vurulan ağ üzerinden taşman sayısal bilgileri temsil eder.

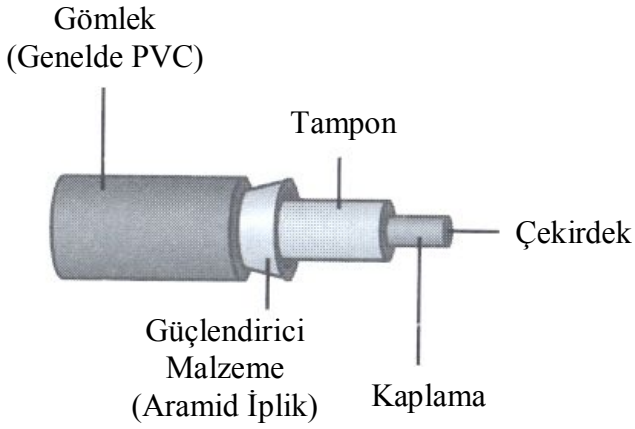
Fiber optik kablonun çok düşük hata oranı vardır ve elektromanyetik girişime maruz kalmaz. Bu kablo saniyede onlarca gigabitlik sinyalleri iletebilir ve her kanal farklı bir ışık dalga boyunda olduğu için, birkaç farklı kanala aynı anda iletebilir. Fiber optik kablolar çok hızlı veri iletimine imkan sağlamalarına rağmen tamamen sorunsuz değildir. Gigabit Ethernet'in sorunu, birçok bilgisayarın bu ağa uyum sağlayamadığı için, çok gelişmiş bilgisayarlarınız olmadıkça, gigabitlik hızların yararını görememenizdir.

Bununla birlikte, fiber optik kablolar çift bükümlü ya da ThinNet kablolardan daha pahalıdır ve kurulmaları daha güçtür. Kabloyu döşerken çok keskin kıvrımlar yapamazsınız ve bu kablo diğer türlerden daha az esnektir. Kendi bağlayıcınızı bir fiber optik kablonun ucuna kurmanız gerekirse, acil onarımlar için bazı bağlayıcılar kabloya sıkıştırarak bağlanabilse de bu durumda epoksi ya da ısıl işlem uygulanmalıdır.

Şekil 2.7' de gösterildiği gibi, fiber optik kabloların beş bölümü vardır:

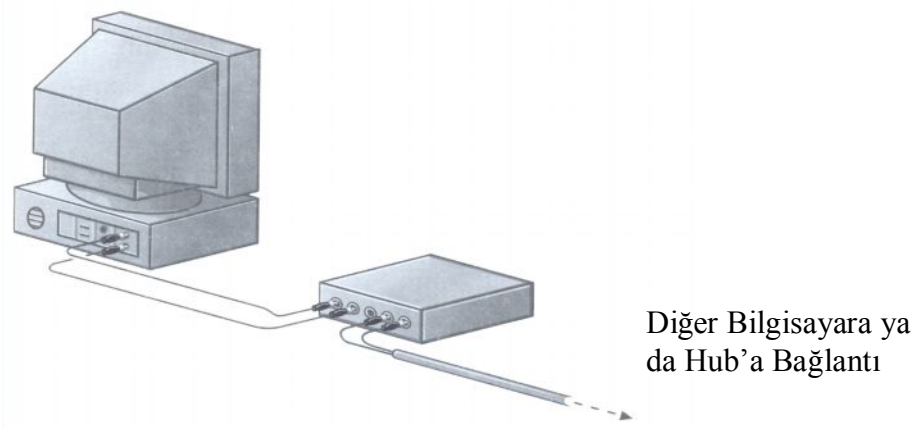
1. Işığı taşıyan cam çekirdek

2. Işığı hiçbir sinyal kaybı olmadan iletilmesi için çekirdeğe geri yansıtan çekirdek çevresindeki cam kaplama
3. Çekirdeği ve kaplamayı zarar görmekten koruyan bir tampon tabaka
4. Kabloyu güçlendiren bir malzeme tabakası
5. PVC plastik gibi bir dış gömlek.



Şekil 2.7 Fiber Optik Kablonun beş parçası vardır

Fiber optik kablodaki iki optik fiber, bilgisayarı Şekil 2-8'de görüldüğü gibi ağ hub'ına bağlar. Bir fiber bilgisayara bilgi taşıdığı diğer fiber de ağa dağıtılmak üzere hub'a bilgi taşıdığı için, fiber optik kablo genellikle aynı gömlek içinde iki fiber kablo olarak satın alınır.



Şekil 2.8 Bir bilgisayarı ağ hub'ına fiber optik kablo ile bağlayabilirsiniz

2.2 Kablosuz Ağlar

Kablosuz ağlar bir dizüstü bilgisayarı masaüstüne bağlamak için idealdir; çünkü dizüstünü istediğiniz yere koyabilir ya da kabloları düşünmeden onu odadan odaya taşıyabilirsiniz. Kablosuz ağlar alıcı-verici denilen bir aygıt aracılığıyla bilgileri radyo dalgalarında olduğu gibi havadan gönderir ve alırlar. Radyo dalgalarını hem gönderdiği hem de aldığı için, ağdaki her bilgisayarda bir alıcı-verici yüklü ya da bağlıdır.

Bir bilgisayarı kablosuz ağa bağlamak için beş yapılandırma vardır: [11]

1. Alıcı-verici işlevi gören bir iç ağ aygıtı ya da NIC
2. Dizüstüne takılan bir bilgisayar kartı biçimindeki alıcı-verici
3. Var olan Ethernet ağı aygıtına bağlanan bir dış alıcı-verici
4. USB bağlantı noktasına bağlanan bir dış alıcı-verici
5. Paralel bağlantı noktasına bağlanan bir dış alıcı-verici

Bir kablosuz ağ aygıtı Ethernet ağ aygıtıyla yaklaşık aynı biçimde yüklenir. Tek fark, kablosuz olanın arkasında anten görevi gören bir çıkıntı olmasıdır. Aygıtı ya da kartı yerine oturacak biçimde takmadan önce, çıkıntıyı bilgisayarın arkasına yerleştirmek için aygıtı ya da kartı hafifçe eğmeniz gerekebilir.

2.3 LAN

LAN'larda temel özellik, sistemlerin aynı ortamda veya birbirlerine yakın mesafede olmalarıdır. Bu nedenle sistemler arasında kullanılacak kabloların seçiminde büyük bir esneklik vardır ve kablolama altyapısı bir kez kurulduktan sonra maliyetsiz büyük bir iletim ortamı sağlar. En basitinden 1 HUB ile LAN kurulabilir. Şekil-2.1.'de 1 Hub ve Switch'den oluşan bir yerel ağ (LAN) görülmektedir.

LAN uygulamasında yüksek hızlara çıkılabilir; kullanılan teknolojiye göre 10, 16, 100, 155, 622 Mbps ve 1 Gbps hızında band genişliğine sahip olunabilir.

- Ethernet (10-100 Mbps, 1 Gbps)
- Token Ring (4-16-100 Mbps)
- FDDI (100 Mbps)
- ATM (155-622 Mbps, 1.2 Gbps)

LAN uygulamalarında biraz da maliyetin düşük olması nedeniyle Ethernet teknolojisi yoğun olarak kullanılır. Ağın büyüklüğü arttıkça LAN omurga kurulmasında ATM ve FDDI teknolojileri de seçimlik olabilmekte, ancak omurgada bunlar kullanılsa bile kenarlarda yine Ethernet teknolojisi kullanılmaktadır. Token Ring endüstriyel uygulamalarda seçimlik olabilmektedir.

2.4 Kampüs Ağı

Kampus ağ, LAN ile benzer özeliklere sahiptir; farkı, daha uzak mesafe gereksinimi ve birden çok LAN'ı içerebilmesidir. Adı üzerinde üniversite kampüsleri gibi sınırlı bir alana dağılmış binalar içerisindeki bilgisayarları, LAN'ları birbirine bağlamak için kullanılır; omurga (backbone) ağ, bu iş için kurulan ve tüm kampusu dolaşan ana çatı durumundadır. Kablo seçiminde LAN uygulamasındaki gibi esneklik yoktur denilebilir; daha uzak mesafelere gidileceği için bakır kablo yerine fiber optik kablo kullanılması gerekebilir.

Kampus uygulamalarında da 34, 100, 155, 622 Mbps ve 1 Gbps, 1.2 Gbps gibi yüksek hızlara çıkılabilir.

Genelde LAN ürünleri kullanılsa da mesafenin yetmediği durumlarda WAN bağlantılara da ihtiyaç duyulur.

2.5 WAN

WAN bağlantısı, birbirinden çok uzakta olan kampüs türü ağları ve LAN'ları birbirine bağlar. WAN uygulamasında anahtar sözcükler mesafe, band genişliği ve aradaki iletişim ortamının bir telekom şirketinden kiralanmasıdır. İletişim ortamı band genişliği sınırlıdır ve band genişliğine göre ücret ödenir; dolayısıyla en iyi şekilde kullanılmalıdır.

WAN bağlantısı için çok değişik seçenekler vardır. Göreceli olarak düşük hızlı (33.6 Kbps, 56 Kbps) telefon hattı üzerinden yapılabilen bağlantıdan tutun da 2 Mbps veya daha yüksek hızlarda bağlantı yapılabilmektedir.

WAN bağlantılarında kullanılan teknolojiler veya standartlar:

- Analog hat (kiralık ve çevrimiçi)

- X.25
- SMDS
- FR
- Switched 56K
- ISDN (BRI, PRI hizmetleri)
- WAN-ATM
- xDSL (ADSL, VDSL, ...)
- Kablolu TV hatları

2.6 Uzak Bağlantı

Uzak bağlantı tek bir bilgisayarın veya küçük bir ofiste bulunan bilgisayar grubunun merkezi yere bağlanmasıdır; WAN' ın bir parçası olarak düşünülebilir; temel özellik birkaç kullanıcı olması ve iletim ortamı olarak büyük band genişliği gerektirmemesidir. WAN bağlantısından farkı, orada olduğu gibi LAN'ları değil de uzaktaki kullanıcıların merkezi yerdeki sistemlere bağlanmasını sağlar. Örneğin evden yapılan Internet bağlantısı bir uzak bağlantı uygulamasıdır.

Uzak bağlantılarda, genel olarak, iletişim ortamı olarak Türk Telekom veya GSM operatörlerinin sunduğu telefon iletişimi kullanılır.

Uzak bağlantılarda kullanılan teknoloji ve standartlar şunlardır:

- Analog Hat (33.6 Kbps, 56 Kbps)
- X.25 (göreceli olarak düşük hız)
- ISDN (BRI: 128 Kbps, PRI: 2 Mbps)
- ADSL (1.5-8 Mbps alış, 16-576 Kbps veriş)
- LMDS (Yüksek hızlı kablosuz hücresel bağlantı)

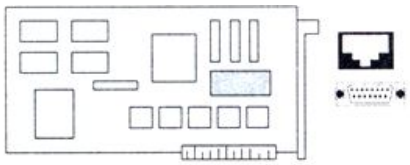
2.7 Ağ Bağlantı Cihazları

Ağ bağlantı cihazları bilgisayar ağım oluşturmak için kullanılan pasif veya aktif sistemlerdir. Ağda bulunan bilgisayar veya benzeri sayısal sistemler, bu cihazlar aracılığıyla birbirleriyle haberleşebilir ve etkileşimli uygulama programları çalıştırabilirler.

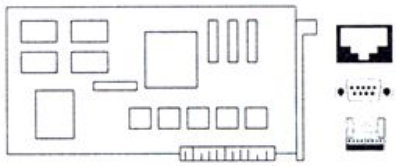
En basitinden bir ağ cihazı doğrudan bilgisayarın içine takılan Ağ Arayüz Kartı (Network Interface Card, NIC) ve bilgisayarları paylaşılan bir ortamdan birbiriyle görüştüren HUB (dağıtıcı) cihazıdır. Yalnızca birkaç kart ve bir HUB cihazıyla küçük bir ofisin bilgisayar ağı kurulabilir. Ancak, komple bir ağın oluşturulmasında bu iki cihaza ek olarak kullanılan anahtar, yönlendirici, ortam dönüştürücü gibi birçok ağ cihazı daha vardır.

2.7.1 Ağ Arayüz Kartları NIC (Network Interface Card)

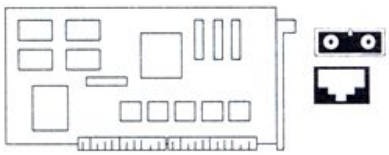
Ağ kartları, üzerinde ağ erişim portu olmayan standart özellikte bilgisayar veya benzeri sayısal sistemlere takılan kart şeklinde bir sistemdir. Genel olarak, LAN içinde bulunan uç sistemlerin ağa bağlanması için kullanılır. Dolayısıyla Ethernet, Token Ring (TR), ATM ve FDDI vs. gibi her LAN teknolojisi veya türü için farklı ağ kartı vardır. Ethernet teknolojisine dayanan bir LAN'a uç sistem bağlanması için Ethernet kart, ATM teknolojisine dayanan bir LAN'a uç sistem bağlanması için ise ATM kart kullanılır. Şekil-lO.l.'de çeşitli ağ kartlarının fiziksel şekilleri ve hemen yanlarında olası konnektör türleri görülmektedir. [8]



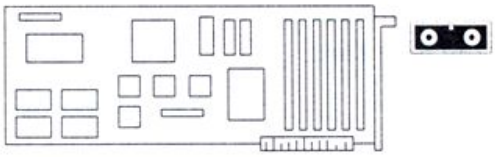
Ethernet Ağ Kartı



TR Ağ Kartı



ATM Ağ Kartı



FDII Ağ Kartı

Şekil 2.9 Çeşitli ağ kartları ve konnektör türleri

Ağ kartları, temel olarak ait olduğu teknolojinin fiziksel katmanına ait fonksiyonları yerine getirir. Ancak, uygulamada, fiziksel katman dışında diğer katman fonksiyonlarının bir kısmını da yerine getirirler. Örneğin Ethernet kartlar, OSI başvuru modeline göre, fiziksel katman ve hemen bir üstünde bulunan MAC alt katmanın (veri

bağı katmanın bir parçası) işlevlerine de sahiptir ve bunlarla ilgili standartları destekleyecek şekilde üretilmiştir. ATM kart ise, sürücü programıyla beraber hemen hemen mimarisinin sahip olduğu tüm katmanlara sahiptir. Böyle olmasına karşın, ağ kartlarından söz edilirken daha çok fiziksel katman özellikleri ve onun standartları akla gelir.

Bilindiği gibi bilgisayarlar 32-bit PCI, 16-bit ISA ve 32 bit EISA gibi çeşitli türde iç yollara sahiptir. Bir kart hem takılacağı bilgisayarın iç yoluna ve hem de bağlanacağı aktif cihazın (Anahtar, HUB vs.) port arayüzüne uygun olmalıdır. Örneğin, bilgisayar 32-bit PCI yoluna ve kartın bağlanacağı aktif ağ cihazı 100 Mbps fiber portlara sahipse, buraya uygun kart ta bu özelliklere sahip olmalıdır (bkz. Şekil 2.9.). Benzer şekilde 100 Mbps Hızlı Ethernet ağ kurulacaksa ağ kartının LAN portu bunu destekleyecek biçimde olmalıdır.

2.7.2 Ethernet Kartı

Ethernet kartlar, Ethernet teknolojisinin LAN uygulamasında yoğun olarak kullanılması nedeniyle oldukça yaygın kullanılır. Bugün için kullanılan tüm ağ kartlarının %85-90'ının Ethernet kart olduğu söylenebilir. Çünkü bir bilgisayarı Ethernet kart ile ağa bağlamak oldukça düşük maliyetli olmakta ve çoğu zaman kullanıcı gereksinimini karşılamaya yetmektedir. Ethernet kartları, aktarım hızı (band genişliği) ve fiziksel port türüne bağlı olarak Çizelge 2.1'de görüleceği üzere çok çeşitli türlerde üretilir.

Çizelge 2.1 Ethernet İçin Çeşitli Kart Türleri

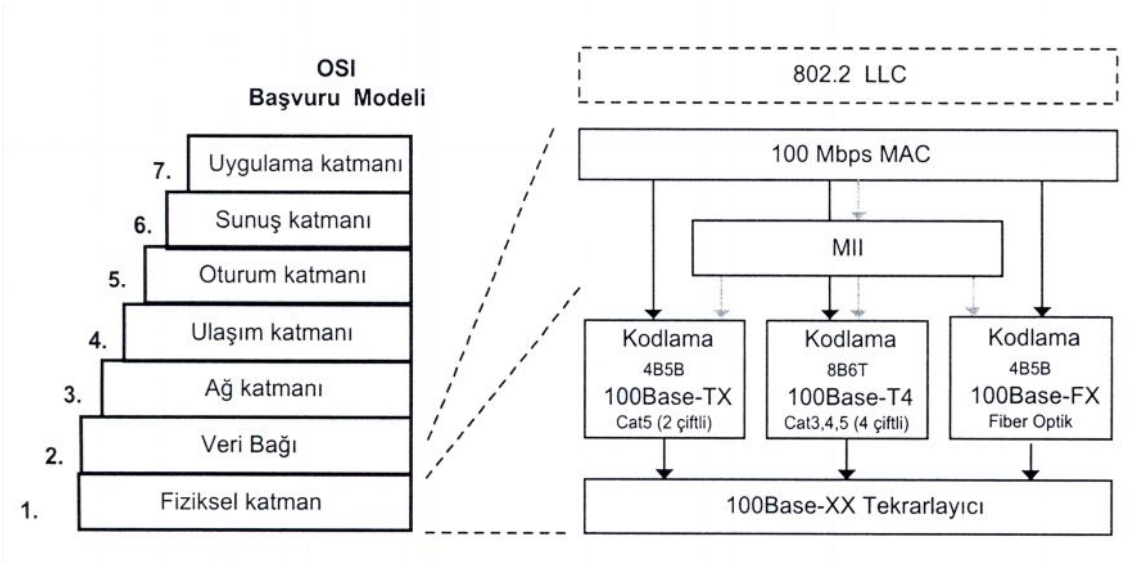
Kart Türü	**Hızı** (Mbps)	**Kablo Türü**	**Port Konnektörü**
10Base-T	10	UTP, STP (bakır)	RJ-45
10Base-F	10	Fiber optik	ST veya SC
100Base-TX	100	UTP, STP (bakır)	RJ-45
100Base-T4	100	UTP, STP (bakır)	RJ-45
100Base-FX	100	Fiber optik	ST veya SC
1000Base-SX	1000 (1G)	Fiber optik	ST veya SC
1000Base-T	1000 (1G)	UTP (bakır)	RJ-45

Birçok üretici, esnek olması açısından Ethernet kartlarını hem 10 Mbps hem de 100 Mbps'te çalışacak biçimde üretmektedirler. Bu tür kartlar (10/100 olarak gösterilir), hangi hızda çalışacağını ya yapılan konfigürasyonla (manuel) anlar, ya da otomatik olarak karşı tarafta hangi hızda bir arayüz varsa, ona kendisini uyarlayarak (autosense) çalışır.

Diğer tüm ağ cihazlarında olduğu gibi Ethernet kart karşı taraftaki porta kablo ile bağlanır. Bu kablo boyunun en uzun ve en kısa ne kadar olabileceği standartlar ile belirlenmiştir. Bu standartların dışına çıkıldığında ağdan beklenen başarım (performans) alınamayabilir veya ağ oldukça yavaşlayabilir. Aşağıda bu uzunlukların ne kadar olduğu özetlenmiştir: [13]

Çizelge 2.2 Kablo kapasiteleri ve maksimum erişim uzunlukları

l0Base T'de 10 Mbps	Cat 3, 4 ve 5 UTP kablo ile 100 metreye kadar
10Base F'de 10 Mbps	Çok Modlu Fiber Optik kablo ile 2 Km.'ye kadar.
100Base TX'de 100 Mbps	Cat 5 UTP kablo ile 100 metreye kadar.
100Base T4'de 100 Mbps	Cat 3, 4, 5 UTP kablo ile 100 metreye kadar.
1000Base T'de 1 Gbps	Cat 5 UTP kablo ile 100 metreye kadar.
1000Base LX'de 1 Gbps	Çok Modlu Fiber Optik kablo (50 u) ile 550 metreye kadar.



Şekil 2.10 100 Mbps Ethernet ağ kartının OSI başvuru modelindeki yeri

2.7.3 TR Kartlar

TR kartlar, Jetonlu Halka teknolojisine sahip portları olan ağ cihazlarına uç sistemleri bağlamak için kullanılır. Genel olarak bir TR kart hem 4 Mbps hem de 16 Mbps'lik bağlantıyı destekler. Fiziksel bağlantının yapıldığı konnektör RJ-45 ve DB-9 şeklindedir (bkz. Şekil 2.9).

2.7.4 FDDI Kart

FDDI ağa bir uç sistem bağlamak için iki tür kart vardır. Biri çift bağlantılı arayüz (DAS), diğeri tek bağlantılı arayüz (SAS) ile bağlanılmasını sağlar. DAS, FDDI'ın var olan 2 halkasına da bağlantı sağlarken, SAS yalnızca aktif halkaya bağlantı sağlar.

2.7.5 ATM Kart

ATM omurgaya bir bilgisayar bağlanması için ATM ağ kartı kullanılır. ATM, uçtan uca hizmet kalitesini garanti eden bir teknolojidir ve doğrudan ATM ağa bağlı uç sistemler, kart ile bütünleşik gelen LAN emülasyon yazılımı aracılığıyla, e-ğer ağda birden fazla LAN varsa tek bir kart ile hepsine üye olabilir. ATM kartlar, genel olarak 155 Mbps'lik üretilmektedir; bakır (Cat5 UTP) ve fiber optik kablo seçenekleri vardır.

2.7.6 HUB / Tekrarlayıcı (Repeater)

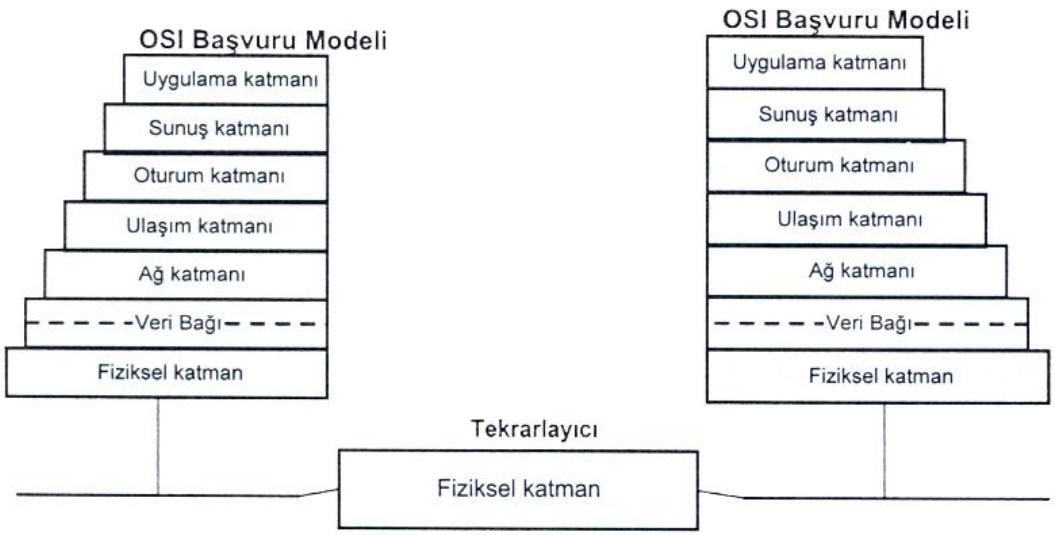
Tekrarlayıcı, ağ dilimlerini (segments) birbirine bağlayarak ağı genişletmek, uzatmak için kullanılır; görevi, iletişim hattının fiziksel uzunluğunu arttırmaktır. Şöyle ki, her hat, üzerindeki elektriksel işareti iletirken belirli bir zayıflatmaya uğratır; bu çok fazla olursa karşı taraf işareti algılayamaz; dolayısıyla iletişim gerçeklenemez. Bu durumda araya zayıflayan işareti kuvvetlendirip karşı tarafa ulaşmasını sağlayan tekrarlayıcı koyulur. Küçük boyutlu, hat uzunluğu belirtilen sınırlar içinde kalan ağ

uygulamalarında tekrarlayıcı gereksinimi olmaz; ancak hat uzunluğu artarsa, araya tekrarlayıcı koyulması gerekir.

Tekrarlayıcılar birden çok ağı birbirine bağlamak için değil de, aynı ağa ait parçaları, yani ağ dilimlerini birleştirmek için kullanılır. Çünkü ağ bağlantısı için kullanılan iletişim kartları ve özellikle bağlantıda kullanılan kabloların iletişim mesafeleri kablo cinsine göre belirlidir ve belirli bir üst sınırı vardır. Eğer arada bir kuvvetlendirme yapılmıyorsa, ancak belirli bir mesafeye kadar iletim sağlanır. Daha uzun bir bağlantı için araya bu kuvvetlendirme işini kotaracak tekrarlayıcı cihazı koyulması gerekir. [8]

Tekrarlayıcı koyularak ağ dilimlerinin birbirine bağlanması, diğer bir deyişle ağın genişletilmesi de belirli bir noktaya kadar yapılır. İstenildiği kadar tekrarlayıcı koyulup genişletilemez. Bunun da bir sınırlaması vardır ve bunu seçilen yöntem belirler.

Tekrarlayıcı OSI referans modelinin 1.katmanı olan fiziksel katmanda tanımlı görevi yapar; gelen verinin içeriğiyle ilgilenmez, yalnızca elektriksel olarak kuvvetlendirip diğer portuna iletir (Şekil 2.11). Kısaca bir tekrarlayıcının temel işlevi, kendisine herhangi bir yönden gelen elektriksel işareti karşıya kuvvetlendirilmiş olarak aktarmaktır.



Şekil 2.11 Tekrarlayıcının OSI başvuru modelindeki yeri

Tekrarlayıcı kullanılarak dilimleri bağlanmış bir ağdaki trafik yoğunluğu, bütün dilimlerin trafik yoğunluklarının toplamıdır. Çünkü tekrarlayıcı, verinin içeriğiyle ilgi-

lenmediği için alıcı adresi göremez ve verinin nereye adreslendiğini sezemez. Dolayısıyla bir dilimin yarattığı trafik doğrudan diğer dilimlere yansır.

HUB cihazı çok portlu tekrarlayıcıya benzer. Ancak çalışma ilkesi benzer olsa da işlevsel farklılık gösterir. HUB, çeşitli yerlere dağılmış uç bilgisayarların bir noktada birleştirilmesi imkanını sağlar; kendisine bağlı olan tüm bilgisayarlara, Ethernet'in başlangıç felsefesi olan paylaşılan bir aktarım ortamı (paylaşılan yol) sunar. Yani HUB'a bağlı bir bilgisayar veri göndermek istediğinde veri paketini yola çıkartır; eğer bir çatışma olmaz ise paketler alıcısı tarafından başarıyla alınır. Eğer bir çatışma olursa, iletişim gerçeklenmez; gönderen bilgisayar rastgele bir süre bekleyip yeniden göndermeye çalışır. Paylaşılan yolun başarımı çatışma oranıyla ters orantılıdır; çatışma sayısı arttıkça başarım düşer. Paylaşılan yola yeni bilgisayarların eklenmesi çatışma olasılığını arttıracağından başarımı düşürür. HUB, fazla trafik yoğunluğu olmayan uygulamalarda optimum çözüm verir. Ancak resim ve görüntü bilgilerinin aktarıldığı uygulamalarda yoğun trafik olacağından HUB kullanımı iyi sonuç vermeyebilir.

HUB cihazı küçük ofis uygulamalarında veya büyükçe bir LAN'da yoğun trafik gereksinimi olmayan çalışma gruplarının bağlantısında kullanılır. Çeşitli sayıda portları olan çok değişik HUB cihazları vardır; 4, 8, 12, 24 portlu HUB cihazları gibi. Bir ağ cihazı portlarına bağlı sistemlere paylaşılan bir ortam sunuyorsa HUB olarak düşünülebilir. Bazı HUB'ların, genel olarak portları l0Mbps iken 1 tane de 100 Mbps'lik porta sahiptir. Bu 100 Mbps'lik port ya HUB'ın LAN omurgaya bağlanmasında (uplink) ya da oraya 100 Mbps'lik bir ana bilgisayar bağlanmasında kullanılır.

HUB cihazları, toplam port sayısının arttırılması için birbirlerine bağlanabilir. Bu a-maçla çoğu HUB cihazında ya özel port bulunur ya da üst üste koyularak yığın (stack) oluşturmak için hızlı özel yola sahip olurlar. İkincisi olması durumunda iki HUB özel bir kablo ile birbirine bağlanır; bu şekilde bir darboğaz oluşturmadan bağlantı sağlanmış olur.

2.7.7 Köprü (Bridge)

Köprü türü cihazlar, genel olarak, benzer teknolojiye sahip LAN'ları birbirine bağlamak için kullanılır; bağlantı sonucu LAN'lar mantıksal açıdan yine tek bir LAN olur. Köprüler, OSI başvuru modeline göre veri bağı katmanında çalışırlar. Dolayısıyla verinin adres kısmına bakıp ona göre davranırlar; veri paketi içindeki alıcı adresi karşı

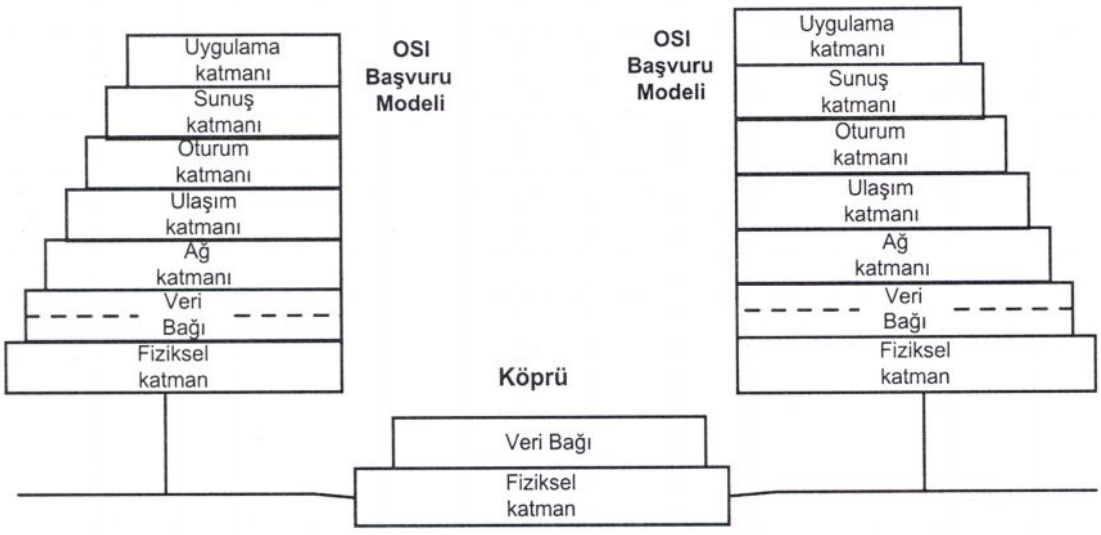
tarafa ait değilse, paketi boşuna karşıya geçirip oranın trafiğini arttırmazlar. Ethernet kartlarda, fiziksel adres olarak ta bilinen MAC düzeyinde adresleme kullanılır.

Köprüler, topolojisi farklı dahi olsa aynı protokolün kullanıldığı iki veya daha fazla bağımsız ağın birbirine bağlanması için kullanılır. İki bağımsız ağ arasına koyulan bir köprü her iki tarafta da aktarılmak istenen paketleri inceler. Eğer paket karşı ağda bulunan bir yeri adresliyorsa, o paketi diğer ağa aktarır; aksi durumda, karşı ağın trafiğini arttırmamak için, orayı adreslemeyen paketleri süzer ve geçirmez. Böylece ağın bir parçasının trafiği diğer parçaların trafiğiyle ağırlaşmamış olur.

Uygulamada, büyük ağların, parçalanıp her biri bağımsız birer ağ niteliğini koruyacak biçimde daha küçük ağlara bölünmesinin ve bunların birbirlerine köprülenerek bağlanmasının (bridging) birçok getirisi olur:

- Trafik yoğunluğu ayrıştırılmış olur; aynı ağı adresleyen trafik diğer ağları etkilemez.
- Herhangi bir ağda olabilecek bir hata veya arıza diğer ağlara yansıtılmamış olur.
- LAN'ların etkin uzunluğu arttırılmış olur.

OSI' nin 1. ve 2. katmanlarına sahip olan köprüler, veri akışını kontrol eder, iletişim hatalarını denetler, fiziksel adreslemeyi ve fiziksel ortama erişilmesini sağlarlar. Bunları sağlamak için de çeşitli veri bağı katmanı (linklayer) protokolleri kullanırlar; Ethernet, TR (Jetonlu Halka) ve FDDI adı en çok duyulan protokollerdir. [11]



Şekil 2.12 Köprü'nün OSI başvuru modelindeki yeri

Ticari olarak 1980'li yılların başında boy gösteren köprü karmaşık yapıda bir aygıt değildir. Kendisine gelen çerçeveleri analiz eder, çerçevenin içerdiği bilgiye dayanarak diğer ağa geçirilip geçirilmeyeceğine karar verir ve gideceği yere yönlendirir. Köprü, 2. katmanın üstünü ilgilendiren veri parçasına bakmadığı için kendisine gelen çerçeveleri hızlı biçimde aktarır.

Uygulamada, komple bir ağın uzaktaki parçaları, örneğin uzaktaki bir şubenin merkeze bağlanması, genelde bir yönlendirici (Router) üzerinden gerçekleştirilir. Bu durumda merkez ile şubedeki ağlar birbirinden bağımsız, her birinin kendi ağ adresleri olan ağlardır ve ikisi arasındaki iletişim yönlendirme protokolü uyarınca gerçekleştirilir. Eğer şubedeki ağ, merkezdeki ağın bir parçası olacak şekilde bağlantı yapılması istenirse yönlendirici saydam köprü (Transparent Bridging) özelliği verilerek konfigüre edilmelidir. Bu durumda, şubedeki ağ, ayrı bir ağ değil merkezdeki ağın devamı olur.

Bazı köprüler MAC[1] katmanlı köprüler olarak sınıflanır. Dolayısıyla bu tür köprüler birbirinin aynı erişim protokolüne sahip ağları bağlamak için kullanılır. Örneğin iki tane IEEE[2] 802.3 gibi. MAC katmanlı olmayan, LLC[3]'yi de içeren diğer köprüler ise farklı erişim topolojisine sahip ağları bağlamak için kullanılır. Örneğin bir IEEE 802.3 ile bir IEEE 802.5 protokolüne sahip ağları bağlaması gibi. [8]

2.7.8 Anahtar (Switch)

Birden çok uç sistemini bir noktada toplayıp, onlar arasında anahtarlama yöntemiyle bağlantı kurulmasını sağlar. HUB'a benzer, ancak HUB kendisine bağlı sistemlere paylaşılan bir ortam sunarken, anahtar atanmış bir yol sunar. Genel olarak veri bağı katmanında çalışır; ancak ağ katmanı işlevlerine sahip anahtarlar da vardır.

Anahtarlar ağ uygulamasında yoğun olarak kullanılan cihaz türlerinden birisidir; işlevi, kendisine gelen veri trafiğini portları arasında anahtarlamaktır.

---

[1]MAC : Media Access Control

[2]IEEE : The Institute of Electrical and Electronics Engineers (Elektrik ve Elektronik Mühendisliği Enstitüsü)

[3]LLC : Logical Link Control

HUB cihazları kendilerine bağlı sistemlere paylaşılan bir ortam sunarlar. Örneğin, 1 tane sunucu, 5 tane kullanıcıdan oluşan 6 tane sistem bir HUB cihazı üzerinden bağlandığı zaman, her bir sisteme düşen ortalama band genişliği 10/(6-1) 'den 2 Mbps olur. Çünkü paylaşılan yol aynı anda yalnızca bir iletişim için kullanılır. İletişimde bulunmak isteyen bir sistem önce yolu boş olarak bulmalıdır. Aynı örnekte HUB cihazı anahtar ile değiştirilse, bilgisayarlara paylaşılan bir yol değilde anahtarlamalı bir yol sağlanmış olur; ağın toplam aktarım başarımı artar. Teorik olarak aynı anda 3 çift bilgisayar birbirleriyle haberleşebilir; böylece HUB kullanılması durumunda port başına ortalama 2 Mbps olan band genişliği 10 Mbps' e çıkmış olur. Ancak bu durum teorik bir sonuçtur; aynı anda tüm bilgisayarların birer çift oluşturacak şekilde haberleşme gereksinimleri olması uygulamada pek karşılaşılabilecek bir durum değildir.

Uygulamada, bilgisayarlar genelde kullanıcı durumundadır ve bunlar büyük bir çoğunlukla Sunucu (Server) olarak adlandırılan sistemlerle iletişim yapmak isterler. Bu durumda anahtar için hesaplanan teorik değer, gerçekte daha küçük olur; gerçek değeri sunucu sayısı ve sunucuların bağlandığı portun band genişliği belirler.

Anahtar cihazlarının üzerlerinde hiçbir trafik yok iken, tüm portları birbirinden yalıtılmış durumda beklemektedir. Dolayısıyla anahtara bağlı tüm sistemler arasında bağlantı kopuktur denilebilir. Ancak bir sistem diğeriyle iletişimde bulunmak isterse, ikisinin bağlı olduğu portlar anahtar üzerinden birbirine bağlanır (anahtarlama işlemi); iletim bittikten sonra yeniden çözülerek başka sistemlerle iletişim için serbest bırakılır. İletişimde bulunacak sistemlerin ayrı ayrı portlara bağlı olması durumunda, aynı anda birden çok çift bilgisayar iletişimde bulunabilir.

Çizelge 2.3 Çizelgede 8. port için iki tane MAC adresi var.

Alıcı MAC Adresi	Bağlı Olduğu Port
08-00-02-1 a-3c-b2	1. Port
00-a0-24-1a-3c-b2	5. Port
08-00-21-a4-c8-92	7. Port
08-00-02-1 a-3c-33	8. Port
08-00-24-1 a-3c-b2	8. Port
00-00-02-1 a-3c-b2	2. Port
00-00-25-1 a-3c-ae	4. Port

Anahtar cihazlarda ağ içerisindeki sistemlere ait MAC adreslerinin tutulduğu birer tablo vardır; bu tablonun boyu oldukça önemlidir. Anahtarlama işlemi bu tabloya dayanılarak gerçekleştirilir; tabloda hangi MAC adreslerin hangi portlarda olduğu tutulur. Böylece bir porttan gelen çerçevelerin hangi porta anahtarlanacağı/alıcısının hangi porta bağlı olduğuna karar verilir. Eğer bir çerçevenin alıcı kısmındaki adres, o andaki tablo içeriğinde yoksa ilgili çerçeve tüm portlara yayın yapılarak aktarılır. Tablonun tutacağı MAC adres sayısı sınırlıdır ve güncelleme için cep bellek algoritmalarından biri kullanılır (bu adresler gönderme anında eklenir). Yani, tablo dolarsa yeni MAC adresleri, ancak, öncekilerden biri tablodan çıkarılarak eklenebilir. Dolayısıyla bu tablonun boyu küçük olursa ve ağın o kısmında çok fazla sistem varsa, yayın türü aktarım oranı artar ve çok sık olarak cep bellek algoritmasının koşturulması gerekir. Merkez anahtar (core switch) konumundaki cihazların MAC adres tablolarının yeterince büyük olması istenir. [13]

Anahtar cihazlar, köprüler gibi OSI referans modelindeki ilk iki katmanın fonksiyonlarına sahiptirler. Ancak 3. katman işlevlerine sahip anahtar cihazlar da üretilmektedir; anahtarlara 3. katman işlevlerini eklemekten amaç, onları birer yönlendirici haline dönüştürmek değil de, anahtarlara sanal ağ desteği sağlamak ve sanal ağ oluşturulması durumunda konfigürasyon esnekliği sağlamak içindir.

2.7.9 Yönlendiriciler (Routers)

Yönlendiriciler OSI başvuru modelinin ilk üç katmanına sahip aktif ağ cihazlarıdır; 3. katman olan ağ katmanında çalışırlar ve LAN'ların WAN' lara veya uzaktaki diğer LAN'lara bağlantısında kullanılırlar. Yönlendiriciler, 3. katmana ait protokoller düzeyinde adres kontrolü yapıp komple bir ağda paketin alıcısına gitmesi için en uygun yolu belirleyebilirler. Aynı zamanda LAN ile WAN teknolojisi arasında bir köprü görevi görür. Örneğin LAN tarafı Token Ring (TR), WAN tarafı Frame Relay (FR) olan bir uygulamada, bağlantının gerçeklenmesi için TR ve FR portu olan bir yönlendirici kullanılabilir.

Yönlendiriciler, veri paketlerinin bir uçtan diğer uca, ağdaki uygun düğümler üzerinden geçirilerek alıcısına ulaştırılması işini kotarırlar. Paketleri gönderen ve alan düğüm arasında birden fazla yol varsa, en uygun yolun seçilmesi ana görevleridir; en uygun yolun belirlenebilmesi için de, ağ topolojisi ve ağın (bağlantı hatların durumu, band genişlikleri vs. gibi) o anki durumu hakkında birtakım bilgileri tutarlar.

Yönlendiricilerde, optimum yolun bulunabilmesi için yönlendirme algoritması koşar; bu tür algoritmalar, en iyi yolun belirlenmesinde kullanılacak parametrelerin tutulduğu bir yönlendirme tablosuna (routing table) sahiptirler. Yönlendirme tablosu, algoritma uyarınca, ağ sürekli sorgulanarak güncellenir. En uygun yolun belirlenmesi için birçok algoritma vardır ve bu algoritmalar en uygun yolu belirleyebilmek için yol uzunluğu (path length), güvenirlik (reliability), gecikme (delay), yolun band genişliği (bandwidth), trafik yoğunluğu (load) ve iletişim maliyeti (communication cost) gibi parametrelerden bir veya birkaçını kullanarak bir metrik değer hesaplarlar. Bu metrik değere göre paketler yönlendirilir.

Basit yönlendirme algoritmalarında metrik değer olarak atlama sayısı (hop count) kullanılır; atlama sayısı bir paketin göndericisinden alıcısına gitmesi için geçmesi gereken yönlendirici sayısıdır. Örneğin, LAN A'dan LAN D'ye gidecek bir paketin atlama sayısı 2; A'dan E'ye ise 3'tür. Bir yönlendiricinin, metrik değeri, yalnızca atlama sayısına dayanarak hesaplaması, uygulamada çoğu zaman en uygun yolun belirlenmesini sağlayamaz; güçlü algoritmalarda bunun yanında yukarıda belirtilen diğer parametreler de kullanılmalıdır.

Yönlendirme tablosu, en uygun yolun belirlenmesi için kullanılan parametrelerin tutulduğu bir matristir. Her yönlendiricide, desteklediği her protokol için birer yönlendirme tablosu tutulur. Örneğin IP yönlendirme için IP yönlendirme tablosu, IPX için ise IPX yönlendirme tablosu tutulur. Yönlendirme tablosu, ağın gerçek durumunu yansıtan bilgileri taze tutabilmesi için sürekli güncellenir. Güncelleme, yönlendiriciler tarafından otomatik yapılıyorsa dinamik, ağ yöneticisi (administrator) tarafından elle yapılıyorsa statik olarak adlandırılır. Her yönlendirici, dinamik yönlendirme algoritması kullanılsa dahi, başlangıçta minimum gereksinimi sağlayacak statik yönlendirmeye ihtiyaç duyar. Dinamik yönlendirme için kullanılan 2 temel algoritma vardır. Bunlar,

- Uzaklık Vektörü Algoritması - DVA (Distance Vector Algorithm)
- Bağlantı Durumu Algoritması - LSA (Link State Algorithm)

olarak adlandırılır ve ikisi arasındaki temel fark metrik hesabı yapılması için kullanılan parametrelerin elde edilme yöntemidir. Birçok yönlendiricide bu iki algoritmadan biri kullanılır.

Yönlendiriciler ağ içinde konuşlandırılacağı yere göre merkez (core) ve kenar (edge) olmak üzere 2 sınıfa ayrılır. Her sınıfın kendine has gereksinimi vardır ve ancak bunların sağlanmasıyla optimum çözüm elde edilir.

- Merkez Yönlendirici
- Kenar Yönlendirici

Merkez yönlendiriciler daha güçlü donanıma ve daha iyi yönlendirme algoritmasına ihtiyaç duyarlarken, kenar yönlendiriciler, genelde, daha basit, işlem gücü fazla olmayan algoritmalarla işlerini kotarırlar.

Merkez Yönlendiriciler farklı türde WAN portu ve standardını desteklemek, esnek bir çözüm sunmak amacıyla şaseli üretilirler. Şase, pasif yapıdadır ve içerisine port modülleri takılabilecek boş yuvalara (slots) sahiptir. Yuvalara, gereksinime göre port modülleri takılır ve bunların bir kısmı ileride yapılabilecek genişlemeler için boş bırakılır. Bu yuvalara takılabilecek port modülleri tipik olarak Çizelge 2.4 'te listelendiği gibi olur: [13]

Çizelge 2.4 Şaseli bir yönlendiricinin tipik port modülleri

Port Modül Adı	Fiziksel Arayüz	Özellik
Ethernet 10Base-T	RJ-45veyaAUI	LAN
Fast Ethernet 100BaseTX	RJ-45 veya Mil	LAN
Jetonlu Halka	DB-9	LAN
FDDI		LAN veya Omurga
ATM (155 Mbps)	RJ-45 veya ST	LAN,Omurga veya WAN
HSSI (Yüksek Hızlı Seri Arayüz)		Omurga veya WAN
Seri Senkron	DB-60	WAN
Channelized E1/ISDN PRI		WAN
ISDNBRI		WAN
ATM-CES		LAN veya WAN

Aktif ağ cihazları sürekli çalışacak şekilde tasarlanırlar ve bozulması en olası birimi güç kaynaklarıdır. Bu nedenle merkez noktada kullanılabilecek cihazlar, yönlendirici olsun, anahtar olsun yedek güç kaynağa sahip olabilecek şekilde üretilir. Genelde i-kinci güç kaynağı cihaz üzerinde gelmez, sonradan eklenir.

Şaseli ağ cihazlarında diğer önemli bir nokta, şasenin sahip olduğu arka alan (backplane) hızı veya band genişliğidir. Arka alan band genişliği modüller arasındaki trafik gereksinimine cevap verebilecek büyüklükte olmalıdır. Arka alan band genişliğinden dolayı bir darboğaz oluşmamalıdır. Örneğin arka alan hızı 1 Mbps olan bir yönlendirici, farklı modüller üzerinde ATM veya E3 portları varsa ve bu portlar arasında yoğun trafik oluşuyorsa bir darboğaz oluşur.

Üreticiler, şaseli ürünlerinde arka alan yolu olarak ortak yol (shared bus) veya her modül arasında bire bir matrisel yol kullanmaktadır. Cihazların arka alan band genişliği değerlendirilirken bu durum da göz önüne alınmalıdır.

2.7.9.1 ROS - Yönlendirici işletim sistemleri (Router Operating Systems)

Bir yönlendirici, temelde, donanım ve yazılım olmak üzere iki parçadan oluşur. Donanım kadar üzerinde koşan yönlendirici işletim sistemi[1] de önemlidir. İşletim sistemi bir yazılımdır ve işlevi, desteklediği 3. katman protokolleri ve kullandığı yönlendirme algoritması için gerekli fonksiyonları sağlamaktır. Bunun yanı sıra ağ yöneticisine konfigürasyonunun yapılması için bir arayüz sunar. Yönlendiricilere, kullanılacak 3. katman protokolüne uygun ROS yüklenmelidir; IP kullanılacaksa IP ROS, IPX kullanılacaksa IPX ROS veya her ikisi kullanılacaksa IP/IPX ROS parçaları yüklenmelidir. Bir yönlendiriciye, hangi 3. katman protokolüne ait ROS yüklenebileceği, ileride doğabilecek uygulama çeşitliliğinin desteklenmesi açısından önemlidir. Örneğin SNA yönlendirmeyi destekleyecek ROS parçası olmayan bir yönlendirici daha sonra böyle bir eklemenin yapılmasını engelleyecektir; böyle bir yönlendiricinin bir başkasıyla değiştirilmesini de gerektirecektir. [8]

---

[1]Yönlendirici İşletim Sistemi: Saldırı Tespit Sistemleri'nin çoğu genelde yönlendirici işletim sisteminin içerisinde ek bir yazılım olarak çalışır. Veri paketleri bilgisayara ulaşmadan önce ileriki bölümlerde belirtilecek olan değişik teknikler kullanılarak filtreden geçirilir. Bu sayede hedef bilgisayara ulaşılmadan önlem alınmış olunur.

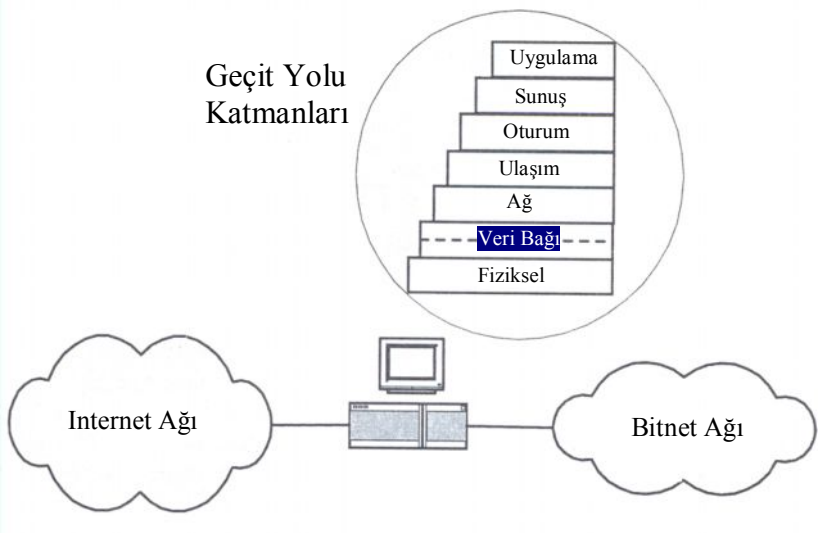
2.7.9.2 BRouter

Köprü, anahtar ve yönlendirici ağ uygulamalarında en çok kullanılan üç cihazdır. Üreticiler, zaman zaman uygulama esnekliği, başarımın arttırılması ve konfigürasyon kolaylığı sağlaması için farklı cihazların özelliklerine sahip tek bir cihaz üretmektedirler. Örneğin, günümüzde yönlendirme modülü olan birçok anahtar cihaz vardır. BRouter cihazı, köprü ile yönlendiricinin özelliklerine sahip bir aktif ağ cihazıdır. Gerçekte, günümüzdeki yönlendirici cihazları, genelde, BRouter yapıdadır. Yönlendirici olarak uzaktaki ağ dilimlerini birbirine WAN protokolü üzerinden bağlar ve sanki bir köprü bağlantısı yapılmış gibi uzaktaki ağ parçalarını tek bir LAN'ın dilimleri gibi birleştirir. Bu tür uygulamalarda, yönlendirici saydam köprü şeklinde konfigüre edilmelidir.

2.7.10 Geçityolu (Gateway)

Geçityolu, OSI başvuru modelinde tanımlanmış olan 7 katmanın tamamının fonksiyonlarını içeren bir ağ cihazıdır (Şekil 2.13); protokolleri tamamen farklı ağların birbirlerine bağlanması ve aralarında bir geçit oluşturulması için kullanılır; güvenlik duvarı oluşturmak için de yoğun olarak kullanılmaktadır. Geçityoluna gelen veri paketleri en üst katman olan uygulama katmanına kadar çıkar ve yeniden ilk katman olan fiziksel katmana iner.

Geçityolu, farklı protokol kullanılan ağlarda iki yönlü protokol dönüşümü yaparak bağlantı yapılmasını sağlar. Örneğin, ISDN ve X.25 ağları veya IP ve IPX ağları birbirine araya geçityolu koyularak bağlanabilir. [6]



Şekil 2.13 Geçityolunun uygulamadaki yeri ve OSI Referans Modeli Katmanları

Geçityolları, güvenlik amacıyla kullanılan koruma duvarı (firewall) olarak adlandırılan sistemlerde de kullanılmaktadır. Bu tür uygulamada görevi protokol dönüşümü yapmak değil de üzerinden geçen paketlerin 7 seviyede kontrolünün yapılmasını sağlamaktır.

2.7.11 Modem

Modemler günümüz ağ ve ağlararası bağlantılarında bolca kullanılmaktadır. Uzak bağlantıların, telefon şirketinin sağladığı bir ortam üzerinden yapılabilmesi için modemlere gereksinim vardır. Bu amaçla değişik hızda ve değişik frekanslarda çalışan çeşitli modemler üretilmektedir. Modemler birbirine uzak olan iki bağımsız ağın bağlantısında da, bir ağın bir düğümünün veya bir diliminin bağlantısında da kullanılmaktadır.

Modemler, genel olarak, sayısal verinin analog iletişim ortamından aktarılması görevini yerine getirirler. Bunun içine kendisine gelen sayısal veriyi, aktarımdan önce modüle (modulation) eder. Alıcı kısımda ters yönlü (demodulation) yapılarak modüle edilmiş işaretten gerçek veri elde edilir. Örneğin telefon hattı, konuşmanın analog olarak iletildiği ortamdır. Bu ve benzeri analog ortamlardan sayısal veri aktarmak için hattın her iki ucuna modem koyulmalıdır.

Bir modemde göz önüne alınması gereken nokta band genişliğidir. Analog modemler için band genişlikleri 28 800 bps, 33 300 bps, 56 Kbps'dir. Analog kiralık hatların her iki ucuna koyulan temel band (baseband) modemler ise 64 Kbps'den başlayıp 2 Mbps'e kadar çıkmaktadır. [13]

2.8 Ethernet / IEEE 802.3

Ethernet ilk olarak, deneysel çalışmaların[1] sonucu olarak ortaya çıkmıştır. İlk Ethernet LAN 2.94 Mbps hızında idi; ancak günümüzde bilgisayar haberleşmesine olan gereksinimin artması ve mikro elektronik teknolojinin gelişmesine paralel olarak daha yüksek hızlara, 10 Mbps, 100 Mbps ve 1000 Mbps gibi hızlara kadar çıkılmıştır. Günümüzde Ethernet ve türevleri olan Fast Ethernet, Gigabit Ethernet LAN tarafında vazgeçilmez (de facto) bir standart haline gelmiştir.

---

[1] 1970 yıllarının sonunda PARC'da yapılan araştırmalarda (Palo Alto Research Center) ortaya çıkmıştır.

Bir IEEE standart olan 802.3 ile Ethernet aslında birbirinden farklı standartlardır. Ancak, ikisi arasındaki fark o kadar çok değildir ve genelde Ethernet ile 802.2 aynı şeylermiş gibi bahsedilir. Farklardan biri çerçeve yapılarıdır.

2.8.1 Ethernet Topolojisi

Ethernet ağların temel topolojisi ortak yol şeklindedir; yani ağa bağlı her bilgisayar aynı yolu paylaşırlar. En temel uygulaması bir koaksiyel kablo dolaştırıp var olan bilgisayarların bu kabloya bağlanması şeklinde olabilir. Bu tür uygulama başlarda oldukça fazla kullanılmıştır. Ancak günümüzdeki Ethernet uygulamasında pek fazla kullanılmamaktadır. Günümüzde paylaşılan yol ortamı olarak HUB cihazları veya bunu başarım (performans) açısından daha ileri götüren ve portlarına bağlı sistemlere anahtarlamalı yol sunan anahtar (switch) cihazları kullanılmaktadır.

Koaksiyel kablolu Ethernet uygulamasında bilgisayarların aynı yola bağlanması için 'tap' olarak adlandırılan fiş kullanılır. Her istasyon, özel bir adrese sahiptir ve ortak yol üzerinde, yalnızca kendini adresleyen veri paketlerini okur.

Paylaşılan yol ortamında aynı anda yalnızca bir tek gönderici etkin olabilir. Aynı anda iki veya daha fazla göndericinin ağı kullanmaya kalkması çatışmaya yol açar. Bunun nedeni Ethernet teknolojisinin fiziksel katmanından temel band (baseband) kullanılıyor olmasıdır. Yani, yol aynı anda tek bir işaret tarafında kullanılır ve yolun tüm band genişliği onu kullanan işaret tarafından harcanabilir. Ek olarak, orada görülmeyen, kabloların uçlarında sonlandırma malzemesinin olmasıdır. Sonlandırma malzemesi, kablo üzerinde akan işaretin geri yanmasının engellenmesi ve azaltılması için kullanılır. Aksi durumda ağın performansı düşer. [13]

2.8.2 Ethernet ve 802.3 Çerçeve Formatı

Ethernet ve 802.3 standardında aktarılacak veri, çerçeveler içinde alıcısına aktarılır. Çerçeveler içinde gönderilecek veri parçasının yanı sıra alıcı-gönderici adresleri, hata sınama bitleri gibi birtakım kontrol bilgileri de gönderilir. Aşağıdaki Çizelge 2.5'de çerçevelerin formatı görülmektedir. [8]

Çizelge 2.5 802.3 ve Ethernet Çerçeve Formatı

IEEE 802.3

Öntakı 7	Başla Ayıracı 1	Alıcı Adresi 6	Gönderici Adresi 6	Paket Uzunluğu 2	VERİ N	Dolgu	FCS 4

Ethernet

Öntakı 8	Alıcı Adres 6	Gönderici Adresi 6	Tip	VERİ N		FCS 4

2.8.2.1 Öntakı (Preamble)

IEEE'nin ilk 7, Ethernet'in 8 sekizlisi ön takı olarak senkronizasyon için kullanılır; bunun için gönderilen bit deseni 101010...11 şeklinde olup, alıcı saati ile gönderici saatinin senkronize olmasını sağlar. 802.3'de 7 sekizli ön takıya ek olarak 1 sekizli de çerçeve başı işaretçisi vardır.

2.8.2.2 Hedef adres (Destination Address)

Çerçeveyi alacak düğümün adresini içerir; varış adresi olarak da adlandırılabilir ve MAC adresi içermelidir. 48 bit uzunlukta olup, birebir, grup ve yayma (broadcast) şeklinde adresleme yapılabilir. Adresin en anlamlı biti adresleme şeklini belirler. Birebir adresler için 0, grup veya yayma adreslemesi için ise 1'dir. En anlamlı bitleri aynı olan grup ve yayma adresleri geri kalan 47 bit ile ayrıştırılır; hepsi 1 ise yayma adresi olarak algılanır; grup adresleme için geri kalan 47 bit 1 ve 0 olabilir.

2.8.2.3 Gönderici adresi (Source Address)

Çerçeveyi gönderen düğümün adresini içerir ve 48 bit uzunluktadır. 6 sekizliden oluşan gönderici bilgisayarın adresidir.

2.8.2.4 Tür (Type)

Bu 2 sekizli tür alanıyla, alınan çerçevelerin hangi üst katman protokolüne veya fonksiyonuna gönderileceği belirlenebilir. Örneğin, üç tür servis sunan bir düğüm kendisine gelen çerçevelerin hangi servise ait olduğunu bu alana bakarak anlayabilir.

2.8.2.5 Veri (Data)

Aktarılacak olan veri parçasını içerir; 46 ile 1500 sekizli arasında olabilir. Gönderilecek verinin en az ne kadar olacağı önemlidir; 10 Mbps'lik Ethernet'te 46 sekizliden daha küçük olmamalıdır. Aksi durumda paylaşılan yol üzerinde olan çatışmalar sezilemez.

2.8.2.6 Çerçeve hata sınaması (Frame Check Squence)

Bu alana çerçeve hata sınaması için hesaplanan 32 bitlik değer yerleştirilir. Hata sınaması ön takı dışında çerçevenin tüm bitleri için yapılır.

2.8.3 Ethernet İle 802.3 Arasındaki Fark

İkisi arasındaki farklardan biri çerçeve yapısındadır. 802.3 çerçeve yapısında Ethernet'te olmayan birkaç alan daha vardır. Biri öntakıda belirtildiği gibi çerçeve başı işaretçisi, diğerleri de uzunluk ve dolgu (pad) alanlarıdır. 802.3'de çerçeve için koyulacak veri uzunluğu konusunda sınırlama yoktur; standardı sağlamak ve minimum değeri oluşturmak için verinin sonuna dolgu sekizlileri yerleştirilir. Diğer farklar ise, 802.3'de 48 bitlik adreslemenin yanı sıra 16 bitlik adreslemenin de desteklenmesi ve bazı elektriksel bağlantı tanımlamaları üzerinedir.

2.8.4 CSMA / CD Fiziksel Katmanı

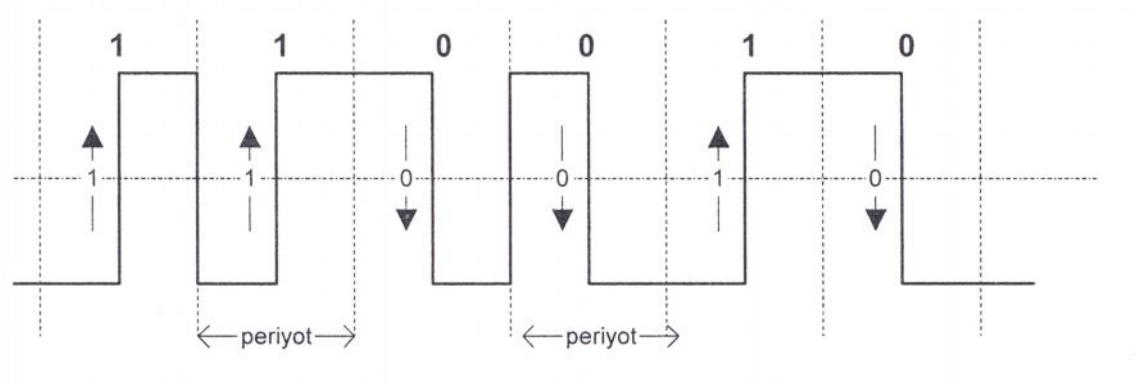
CSMA/CD[1] fiziksel katman topolojisi ilk zamanlar pasif ortak yoldan ibaretti; ancak anahtar (switch) cihazların uygulamada yaygınlaşmasıyla birlikte yıldız-anahtarlamalı yol da kullanılmaktadır. 802.x ailesi LAN fiziksel katmanlarında çoğunlukla Manchester kodlaması veya 4B5B diye adlandırılan kodlama tekniği kullanılır. Manchester kodlamasında bit süresinin ortasında çıkan ya da düşen kenar, bitin 1 yada 0 olarak değerlendirilmesini sağlar; çıkan kenar 1, düşen kenar 0 anlamındadır.

---

[1] CSMA / CD: IEEE 802.3 ve Ethernet standartlarında yola erişim yöntemi olarak kullanılan CSMA/CD'de, bir ethernet düğüm veri aktarmadan önce yolu dinler, eğer yol, o anda diğer düğümler

tarafından veri aktarmak için kullanılıyorsa, yolda bir taşıyıcı (carrier) olduğunu sezer ve kendi verisini yola çıkarmaz, bir süre bekler.

Manchester kodlamasında bit süresinin ortasında çıkan ya da düşen kenar, bitin 1 ya da 0 olarak değerlendirilmesini sağlar; çıkan kenar 1, düşen kenar 0 anlamındadır.



Şekil 2.14 Manchester Kodlaması

Yukarıdaki şekilden görüleceği gibi Manchester kodlaması ile ne iletilirse iletilsin, hat üzerinde her zaman bir titreşim olur ve bu titreşim sayesinde herhangi bir düğüm hattının meşgul ya da boş olduğunu kolayca ayırt edebilir. Hattaki titreşim bir taşıyıcı işareti andırdığı için 802.3 türü LAN için taşıyıcı sezmeli (carrier sense) sözcüğü kullanılır. [13]

2.8.5 Ethernet Adresi

Her Ethernet kartın MAC adresi olarak adlandırılan 6 sekizlik (48 bitlik) özel bir adresi vardır (00-23-c3-45-00-b3 gibi) ve bu adres tektir. LAN içerisindeki yerel erişimler, gerçekte bu adresler kullanılarak gerçekleştirilir.

2.8.6 FDDI (Fiber Distributed Data Interface)

FDDI, iki yollu halka topolojiye sahip türevine göre 100 ile 2 Mbps'e kadar band genişliği sunan ve temelde fiber optik kablo kullanılmasına dayanan bir ağ teknolojisi-dir. Bir LAN teknolojisi olarak geliştirilmesine karşın, Ethernet ve Jetonlu Halka tabanlı LAN'ların daha ucuz çözüm sunmaları ve uygulamada baskın olmalarından olayı, FDDI daha çok Omurga (Backbone) ağ oluşturmak için kullanılmıştır. FDDI'ın ilk uyarlaması 1980'li yılların ortalarında ANSI'nin X3T9.5 standart komitesi tarafından ortaya atılmış olup daha sonra ISO tarafından uluslararası tanımlaması yapılmıştır. FDDI ilk olarak

fiber optik kablo üzerinden 100 Mbps'lik band genişliği sağlayacak bir LAN teknolojisi olarak düşünülmüştür. Ancak daha sonraları Ethernet teknolojisi üzerindeki gelişmeler, Ethernet'in başlangıçta 2-5 Mbps olan band genişliğini sırasıyla 10, 100 ve 1000 Mbps'e çıkarmış ve diğer teknolojilere göre daha az maliyetli bir çözüm olmuştur. Dolayısıyla çok da büyükçe olmayan LAN uygulamalarında Ethernet çözüm olagelmiştir. FDDI ise, daha çok büyükçe LAN uygulamalarında veya kampus uygulamalarında omurga ağ kurulması için seçenek olmuştur.

FDDI, LAN'ları birbirine bağlayan omurga uygulaması için hala 'en güvenilir teknolojidir' denilebilir. Özellikle türevleri olan FDDI-II ve FFOL teknolojileri, çoklu medya veya gerçek zaman uygulamalarının gereksinim duyduğu servis kalitesini (QoS) garanti etmektedirler. FDDI'ın fiber yerine bakır kablolar üzerinde çalışan türevi ise CDDI olarak adlandırılır. [7]

BÖLÜM III

3. OSI (Open Systems Interconnection) REFERANS MODELİ

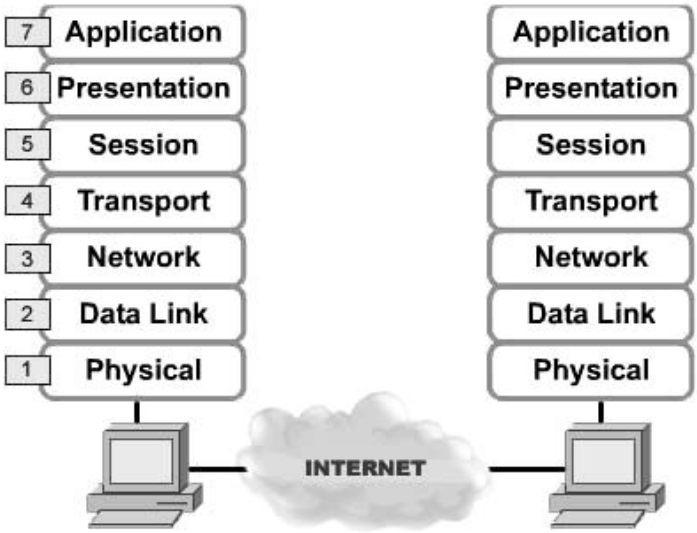
OSI başvuru modeli, bilgisayar veri haberleşmesi sürecinde yapılması gereken işleri katmanlar düzeyinde tanımlayan örnek bir modeldir. Bu modelde veri haberleşmesi için yapılması gereken tüm işler, birbirinden bağımsız olarak kotarılabilecek düzeyde parçalara ayrılmış ve her parçaya ait görev tanımlamaları yapılmıştır. OSI başvuru modeli diğer tüm protokollerin veya standartların açıklanmasında örnek bir başvuru modeli olmuştur. Bu bölümde OSI'nin genel yapısı, katmanları ve katmanların fonksiyonları ele alınmıştır.

OSI standardı ISO (International Organizations of Standarts) tarafından 1979 yılında yayınlandı. Genel yapısı bir düğümün iletişim sürecini çok katmanlı bir yapı şeklinde tanımlamaktır. OSI Modelinde bir uç düğümünde/sistemde, her biri farklı işlevlere sahip 7 katman tanımlıdır. Uç bilgisayarlarda 7 katmanının tamamı bulunurken, bilgisayar ağında yer alan ara düğüm cihazlarda daha az sayıda katman bulunabilmektedir. Örneğin, ağ içerisinde kullanılan ara cihazlardan tekrarlayıcı (Repeater) yalnızca 1. katmana, köprü (Bridge) ve anahtar (switch) cihazları genel olarak 1. ve 2. katmanlara ve yönlendirici (Router) cihazı ise, ilk üç katmana ait işlevlere sahiptirler. Sanki ağ üzerinde bir uç bilgisayar gibi tüm 7 katmanı da içeren geçityolu (Gateway) veya protokol dönüştürücü (protocol converter) de birer ağ cihazıdır. [13]

OSI referans modelini oluşturan yedi katman vardır.

1. Fiziksel (Physical) Katman
2. Veri Bağlantısı (Datalink) Katmanı
3. Ağ (Network) Katmanı
4. İletim (Transport) Katmanı
5. Oturum (Session) Katmanı
6. Sunum (Presentation) Katmanı
7. Uygulama (Application) Katmanı

Yukarıda verilen her bir katmanın kendisine özgü görevleri vardır. Yerine getirdiği hizmetler sayesinde OSI modeli hiyerarşik düzen içerisinde çalışır. Tasarlanan bu yapı sayesinde her katman kendi içerisinde protokollerin tanımlanmasına imkan sağlar. Yaratılan bu hizmetlerden diğer katmanlar da veri akışı sayesinde faydalanır. En alt yapıdan en üst yapıya kadar her katman çalışmak için birbirlerine ihtiyaç duyarlar.



Şekil 3.1 OSI 7 katmanlı başvuru modeli ve katmanlar

3.1 Fiziksel Katman (Physical Layer)

OSI modeli içerisinde tanımlanmış olan ilk katmandır. Fiziksel katman verilerin haberleşme kanalları boyunca bitler halinde iletilmesinden sorumludur. Fiziksel katman yalnızca dataların taşınmasından sorumlu olup, taşıdığı bilginin türü veya yapısı hakkında herhangi bir bilgiye sahip değildir. Bu veriler dijital sinyaller şeklinde (1'ler ve 0'lar) olabileceği gibi analog sinyallerden de oluşabilir.

Fiziksel katman tarafından gönderilen verileri taşıyan değişik türlerde yapılar mevcuttur. Twisted pair, koaksiyel kablo, fiber optik kablolar, kablosuz iletişim (wireless) en çok kullanılan fiziksel iletişim kanallarıdır. Bunlara ek olarak fiziksel katman, taşıdığı verilerin veri bağlantı katmanına aktarılmasından da sorumludur.

OSI referans modeli içerisinde yer alan fiziksel katmanın yerine getirdiği görevler sırası ile aşağıda listelenmiştir.

- Fiziksel katman veri iletişiminin yapıldığı fiziksel kanallar üzerinden yapılan

iletişim ile ilgili görevleri yerine getirir. 1 veya 0 olarak gönderilen verinin karşı taraftan gönderildiği şekli ile algılanması bu katmanının görev ve sorumluluğu içerisinde yer alır.

- Bağlı olan uçlar arasında mekaniksel, elektriksel tanımlamalar yaparak veri hareketine başlanması, sürdürülmesi ve sonlandırılması görevlerini üstlenir.
- Voltaj seviyeleri, voltaj değişim aralıkları, veri iletim hızı, iletilecek verinin erişebileceği en uzak mesafe bu katman içerisinde tanımlanır.

3.2 Veri Katmanı (Data Layer)

Veri bağlantı katmanı, ağ üzerinde bilgisayarların fiziksel olarak adreslenmesinden (Ethernet ağlarında ARP protokolü ile) ve paketlerin aynı fiziksel bağlantı üzerinde olan bilgisayarlara taşınmasından sorumludur. Katmanın görevi şehirlerde bulunan su şebekelerine benzetilebilir. Şebeke suyun apartmanlara kadar taşınmasından sorumludur. Suyun kullanım şekli apartmanda içerisinde yaşayan insanların ihtiyaçlarına göre değişiklik gösterir. Suyun kullanımı ile ilgili şebekenin üstlendiği herhangi bir rol yoktur. Bu katman üzerinde taşınan parçalardan her birine parça (frame) adı verilir. Tüm bu işlevlere ek olarak veri bağlantı katmanı hata denetimi ve data akış kontrolü görevlerini de yerine getirir. [6]

Veri bağlantı katmam, fiziksel katmandan aldığı verileri parçalar (Frame) haline getirir ve ağ (network) katmanına iletir. Her bir parça başlangıcı ve bitişi belli olacak şekilde özel bitlerle işaretlenir. FDDI, SLIP, X.25, ATM, Token Ring ve Ethernet verilerin iletilmesinde kullanılan yapı türlerinden bir kaçıdır.

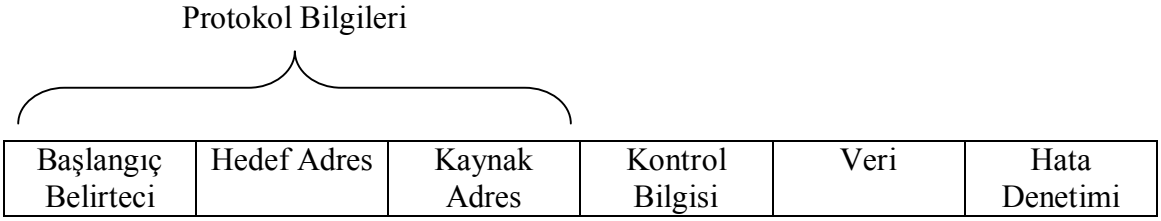
Veri bağlantı katmanı üzerinden iletimi yapılan her parça, kaynak (Source) ve hedef (Destination) adreslerini içerir. Veri bağlantı katmanı hata kontrolünün yapıldığı ilk katmandır. CRC hata kontrolü bu katman üzerinde yapılır. Katmanın görevleri genel özellikleri itibari ile şöyle özetlenebilir:

Veri bağlantı katmanı, fiziksel katmana erişimi ve ağ birimlerini kullanarak gönderilecek verinin hedefinin belirlenmesini sağlar.

MAC (Media Access Control - Ağ Donanımı Erişim Kontrolü) adresleri kullanılarak fiziksel bağlantılar arasında güvenli data iletimine imkan sağlar.

MAC adresinin kullanımı sayesinde bilgisayarların aynı fiziksel bağlantıyı kullanmalarına ve birbirlerinde farklı şekilde tanımlanmalarına yardımcı olur. Her donanım adresi (MAC adresi) birbirlerinden farklı adreslere sahiptir. Ethernet kartlarına atanan donanım adresleri üretimleri sırasında atanır.

Hata denetiminin yapılmasını sağlar. Katman üzerinden gönderilen her bir parça için akış kontrolü sağlar. Eğer parçaların iletimi sırasında hata meydana gelmişse, oluşan hata üst katmanlara iletilir.



Şekil 3.2 Veri Bağlantı Katmanı Üzerinde Veri İletimi

3.3 Ağ Katmanı (Network Layer)

Mantıksal (Logical) adreslemenin yapıldığı katmandır. Ağ katmanı mesajların mantıksal adreslere taşınmasından sorumludur. Bu sayede örnek olarak, İstanbul-Ankara arasında bulunan iki bilgisayarın haberleşmesi sağlanabilir. Mantıksal adresleme bilgisayarlar arasında doğrudan iletişimi sağlayan fiziksel adreslemeden farklıdır. Bir barajdan A apartmanının 10.katında bulunan bir dairenin mutfağına su taşınmasını sağlayan işleyiş mantıksal adreslemeye örnek olarak verilebilir. Amaç suyu belirtilen adrese teslim etmektir.

Ağ katmanı bağlantılı (TCP) ve bağlantısız (UDP) hizmetlerinin sunulmasını sağlar. Bu katman üzerinde yer alan mesaj birimlerine paket veya datagram denir.

Ağ katmanı, veri bağlantı katmanı tarafından sağlanan 'noktadan-noktaya' (node-to-no-de) bağlantı ilkesi üzerine kurulmuştur. Karmaşık ve geniş ağlarda, datagram yönlendirme (Routing) mekanizmasının gerçekleştirildiği katmandır. Daha öncede belirttiğimiz gibi, yaratılan her katmanın sadece kendisinin yerine getirdiği görevleri vardır. Yerine getirdiği bu görevler sayesinde kendisinin üstünde bulunan katmanlara hizmet sağlar. [6]

Fiziksel katman ağ (network) ve medya türlerine göre değişik parça (frame) türleri tanımlar. Değişik mimariye sahip olan ağların birbirleri ile haberleşebilmesi gerekir. Bu gereksinimi karşılamak için ağ (network) katmanı, karmaşık (farklı türde mimariye sahip) ağların, IP adresleme mekanizmasını kullanarak birbirlerine bağlanmalarını sağlar.

Bu katman üzerinde aşağıda verilen protokoller çalışır:

- Internet Protocol (IP - Internet İletişim Protokolü)
- IPX (Internetwork Packet Exchange - Ağlararası Paket Değişimi)
- BGP (Border Gateway Protocol - Sınır Ağ Geçidi Protokolü)
- OSPF (Open Shortest Path First - Öncelikli Olarak Kısa Rotayı Kullan) ve versiyonları
- RIP (Routing Information Protokol - Yönlendirme Bilgi Protokolü) ve versiyonları

Katmanın yerine getirdiği görevleri şöyle sıralayabiliriz:

- Mantıksal iki uç arasında veri iletimi sağlar.
- Her noktanın ayrı ayrı olarak tanımlanmasını sağlayan mantıksal adreslemenin yapıldığı katmandır.
- Farklı ağlar üzerinde bulunan bilgisayarlar arasında paket alışverişine imkan sağlayan yönlendirme (Routing) mekanizmasını tanımlar.
- Değişik mimariye sahip ağlarda iletilen parça (frame) büyüklükleri değişiklik gösterebilir. Bu nedenle ağ katmanı paketlerin ağlar arasında adaptasyonunu sağlayabilmek için parçalama (fragmentation) işleminin nasıl yapılması gerektiğini belirler.
- Yönlendirici (Router) olarak bilinen aygıtlar bu katman üzerinde çalışırlar. IP datagramların ağlar arasında iletilmesi bu katman aracılığı ile gerçekleşir.

3.4 İletim Katmanı (Transport Layer)

Bağlantılı (güvenli) ve bağlantısız (güvenli olmayan) iletimin sağlandığı katmandır. İletim katmanı göndereceği verileri kısım (segment) olarak adlandırılan küçük parçalara ayırır. Bu katman kendisinin üzerinde bulunan yapılara göre saydamdır;

onlara veri akış kontrolü, hata denetimi, belirlenen hataların giderilmesi ve çoklama (multiplexing) gibi hizmetler sunar.

Ağ katmanının sağladığı imkanlarla beraber noktalar arasında (node-to-node) bağlantıların daha güvenli olarak yapılmasını sağlar. İletim katmanı güvenli veri alış iletimini sağlamak amacıyla hata denetim mekanizmaları üzerine kurulmuştur. Katman hata denetiminin yapıldığı son OSI protokol parçasıdır. Eğer fiziksel katman doğru olarak çalışamıyorsa bu katmanın yükleneceği görev yükü daha da artacaktır.

İletim katmanı ayrıca aynı ağ bağlantısı üzerinde birçok mantıksal bağlantı yapmaya olanak sağlar. Aynı fiziksel bağlantıyı paylaşan birden fazla iletim (transport) bağlantısı oluşması ağ terminolojisinde multiplexing olarak adlandırılır.

İletim katmanı OSI modelinin orta bölümünde bulunur. Kendisinin altında bulunan üç katman alt ağ (subnet) olarak adlandırılan yapının tanımlanmasını sağlar. İletim katmanının bir diğer görevi ise alt ağlar oluşturarak ağları daha güvenilir hale getirmektir.

TCP (Transport Control Protocol) ve UDP (User Datagram Protocol) bu katman üzerinde işlevlerini yerine getirir.

İletim katmanı, çoklama (multiplexing) yöntemi ile değişik uygulamaların aynı "sanal adresleri" kullanmasını sağlar. Bu uygulamaların birbirlerinden bağımsız olarak çalışabilmesini sağlayabilmek için ayrıca farklı bir tanımlamaya gereksinim duyulur. Bu tanımlamaya İletim Hizmetleri Erişim Noktası (Transport Service Access Point - TSAP) denir. SAP ve TSAP, OSI modeli içerisinde ağlarda son noktaları tanımlamak için kullanılır. [8]

İletim katmanının OSI mimarisi içerisinde tanımlanmış görevleri şöyle sıralanabilir.

- Akış kontrolü sayesinde bilgisayarlar arasında baş edebilecekleri hızda eşgüdümlü olarak veri iletimi sağlanır.
- İletim Katmanı ağlarda verimliliği artırır. Tek fiziksel bağlantı üzerinden birden fazla iletim (transport) bağlantısı yaratılabilir.
- Hata denetimi sayesinde iletilirken bozulmuş kısımlar (segment) belirlenebilir.
- Hata meydana geldikten sonra yapılacak düzeltme işlevleri yine bu katman üzerinde tanımlıdır. Örneğin iletim sırasında meydana gelmiş kısımların yeniden iletilmesi sağlanabilir.

Bu katman üzerinde çalışan protokollerden bazıları şunlardır.

- TCP (Transmission Control Protocol - İletim Denetimi Protokolü)
- UDP (User Datagram Protocol - Kullanıcı Veri Bloğu İletişim Protokolü)
- SPE (Sequence Packet Exchange - Sıralı Paket Değişimi)
- ATP (Apple Talk Transaction Protocol - Apple Akıcı Konuşma Protokolü)
- NETBEUO (NetBIOS Extended User Interface - NetBIOS Genişletilmiş Kullanıcı
  Arabirimi)
- SMB (Server Message Block - Sunucu Mesaj Bloğu)

3.5 Oturum Katmanı (Session Layer)

Oturum Katmanı, sunum ve iletim katmanları arasında bulunan, OSI modeli içerisinde tanımlanmış olan dördüncü katmandır. İşlevi iletim katmanından hizmet almak; sunum katmanının çalışması için gerekli servisleri sunmaktır.

Oturum (Session) katmanı bilgisayarlar arasında bağlantının kurulumunu, yönetimim, sonlandırılması; uygulama (Application) veya sunum (Presentation) katmanı düzeyinde veri akışım kontrol eder.

Oturum katmanı, genellikle iletim katmanın sunduğu servis türlerini çoğaltmak için kullanılır. Ağ üzerindeki bir bilgisayara bağlanmak, dosya transferi için oturum açmak bu katman üzerinden verilen servislere örnek olarak gösterilebilir. "Diyalog kontrol", jeton yönetimi (Token yönetimi), aktivite yönetimi oturum katmanın OSI modeline sağladığı bazı faydalardır.

Oturum katmanı, karşılıklı çift yönde (full duplex) veri akışına olanak sağlar. Bazı özel durumlarda bağlantıda olan iki noktanın aynı anda kritik olabilecek bir görevi yapmasını engellemek için aynı anda "sadece noktalardan birinin" işleyişine izin verilir. Bu yönetimi sağlamak için "jeton yönetimi" (Token management) kullanılır.

Sıklıkla karşılaşılan bir sorunun çözümünde de oturum katmanı önemli bir görev üstlenir. Genel olarak uzun süren bağlantılar için tanımlanan belirli "zaman aşımı" (timeout) süresi vardır. İki bilgisayar arasında dosya transferi yapılırken, örnek olarak otuz dakika sonunda bağlantı kesintiye uğrayabilir. Transferin veya veri alışverişinin devam etmesini sağlamak için aktivite yönetimi (activity management)

yöntemi kullanılır. Bağlantı kesildiğinde yeni bağlantıda en son senkronizasyon noktasını kullanılarak bağlantı kaldığı yerden yeniden tesis edilir. [13]

Oturum katmanı "port katmanı" olarak da isimlendirilir. Çünkü bilgisayar servisleri port'lar aracılığı ile birbirleri arasında iletişim kurabilirler. Buna örnek olarak HTTP verilebilir. HTTP 80. port üzerinden hizmet verir. Bu katman üzerinden servis veren protokol ve uygulamalar şunlardır.

• RPC (Uzaktan Yordam Çağrısı - Remote Procedure Cali)

• SQL (Yapısal Sorgu Dili - Structured Query Language)

• NetBIOS

TCP/IP ağlan genel olarak oturum katmanını işlevsel olarak kullanmazlar. Bu katmanın uygulamalara sağlamış olduğu faydalar programlar tarafından kendi bünyesinde sağlanır. NFS ve RPC kendi içlerinde oturum katmanının sağladığı hizmetlere sahiptirler. Uygulamaların büyük çoğunluğu oturum katmanını "işlevsiz" olarak kabul eder.

Oturum (Session), Sunum (Presentation), Uygulama (Application) katmanları beraber çalışarak kullanıcı tarafından görülebilen ağ fonksiyonlarını oluştururlar. Diğer katmanların yerine getirdikleri görevler kullanıcıya göre saydamdır. Yani diğer katmanların sağlamış olduğu hizmetler kullanıcı tarafından gözle görülemez.

3.6 Sunum Katmanı (Presentation Layer)

Sunum (Presentation) katmanı verilerin gösterimini sağlar. ASCII, Binary, EBCDIC gibi veri gösterim türleri mevcuttur. Bağlantı noktalarının birbirlerini anlamalarını sağlamak için aynı dilden konuşmaları gerekir. Bunun için veri gösterim sistemlerinin ve semantiğinin aynı olması sağlanmalıdır. SNMP protokolü ASN. 1 , ağ dosya sistemi (NFS - Network File System) XDR'i veri gösterimi için kullanır. Çoğu uygulamalar da ise sunum (Presentation) katmanı işlevsiz olarak kabul edilir.

Sunum katmanı, iletimde olan bilgisayarlar arasında gönderilen verinin alıcı tarafından algılanabilir olmasını sağlar. Katman aynı zamanda;

- Verilerin şifrelenmesini
- Verilerin sıkıştırılmasını
- Grafik Dosyalarının Sıkıştırılması
- ASCII ve EBCDIC karakterleri arasında dönüşüm yapılmasından da sorumludur.

Bu katman üzerinde var olan protokol türleri şunlardır.

- GIF (Graphics Interchange Format - Grafik Dönüşüm Biçimi)
- JPEG (Joint Photographic Experts Group - Birleşik Fotoğraf Uzmanları Grubu)
- TIFF (Tagged Image File Format - Etiket Görüntü Dosya Biçimi)
- ASCII (American Standart Codes for Information Interchange - Bilgi Değişimi İçin Amerikan Standart Kodlama Sistemi)
- MPEG (Moving Picture Experts Group - Hareketli Görüntü Uzmanlar Grubu)
- MIDI (Musical Instrument Digital Interface - Müzikal Çalgı Sayısal Arabirimi)
- HTML (Hyper Text Markup Language - Hiper Metin İşaret Dili)

3.7 Uygulama Katmanı (Application Layer)

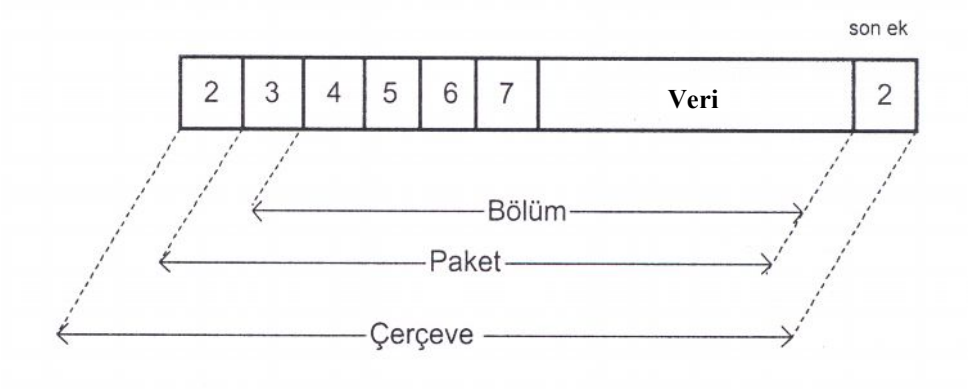
Uygulama katmanı programların ağ kaynaklarına erişimlerini sağlayan arabirimleri oluşturur. Bu uygulama kendisi üzerinde olmayan, sunucu üzerinde olan bir dosyayı açmaya çalışıyor olabilir. Bu durumda bilgisayar, yerel kaynakları kullanarak OSI birimleri vasıtası ile dosyaya erişim sağlar. Uygulamalar ağ kaynaklarım kullanarak uzaktaki servislere komut gönderebilirler. FTP ve TELNET komut yürütme işlevselliği olan uygulamalara örnek olarak gösterilebilir. Uygulama katmanı PSAP (Presentation Layer Service Access Point) aracılığı ile sunum (Presentation) katmanı ile irtibata geçebilir.

Uygulama katmanı kendisine sağlanan imkanları kullanarak protokoller ve uygulamalar oluşturulmasını sağlar. Kullanıcı düzeyinde OSI modelinde bulunan yapılara erişimi sağlar. Uygulama katmanını kullanan uygulamalardan bazıları şunlardır. [8]

- FTP (File Transfer Protocol - Dosya İletim Protokolü)
- HTTP (Hypertext Transfer Protocol - Hiper Metin Aktarım İletişim Kuralı)
- Telnet
- NSF (Network File System - Ağ Dosya Sistemi)
- SMTP (Simple Mail Transfer Protocol - Yalın Elektronik Posta İletim Protokolü)
- SNMP (Simple Network Management Protocol-Yalın Ağ Yönetim Protokolü)

3.8 Katmanlar Arası İletişim

OSI modeline göre uç düğümlerde 7 katmanın tamamı bulunur ve bir düğüm üzerinde i.katmanın, yalnızca (i-l)., ve (i+1).katmanlarla SAP[1] 'lar üzerinden bağlantısı vardır. 7. katmanın uygulama çerçevesinde karşı uçtaki katmana gönderdiği bilgi SAP'lardan geçerek kanala çıkarılırken, bu bilgiye her katman kendi eş katmanıyla anlaşması için gerekli bilgileri de ekler. Dolayısıyla gönderilecek bilgi üst katmandan aşağılara giderken bir miktar genişler (Şekil 3.3).



Şekil 3.3 Verilerin önüne katman başlıklarının eklenmesi

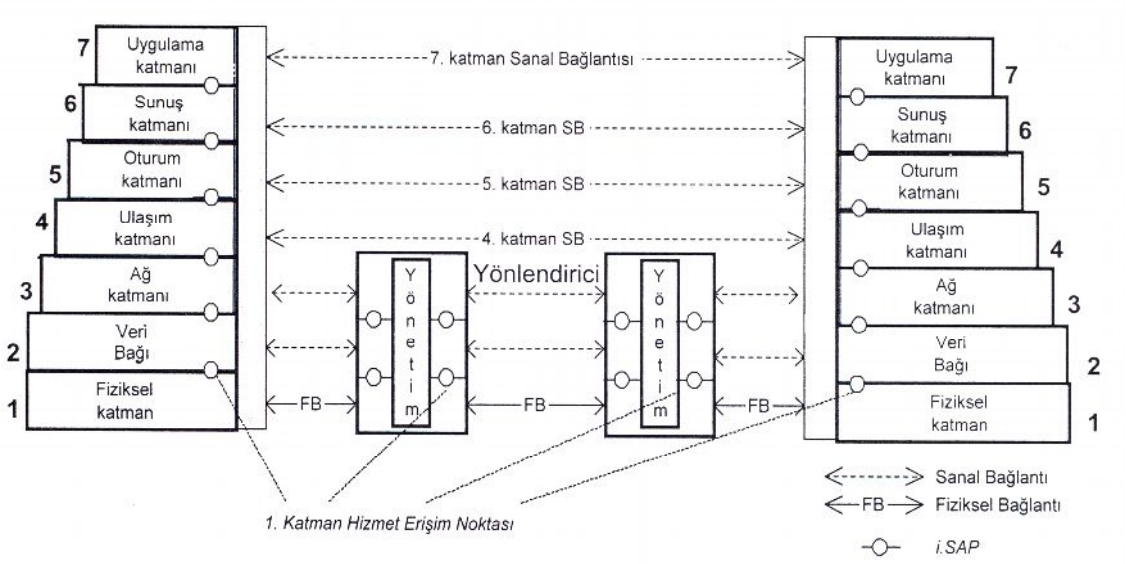
i.katman bir üstünde bulunan i+1. katmandan bir bilgi gönderme isteği olmadan kendi protokolü çerçevesinde bilgi gönderebilir. Bu durumda daha üst katmanla ilgili başlık ve bilgiler çerçevede bulunmaz. Alıcılarda (ara veya uç düğümler) her katman kendisiyle ilgili başlığı değerlendirir, üst katmanlara ait kısmı ise topluca kendi SAP' sinden yukarı teslim eder. [13]

Şekil 3.4'de, 7 katmana da sahip olan iki uç düğüm ve yalnızca ilk 3 katmana sahip olan 2 yönlendirici cihaz arasında var olan fiziksel ve sanal bağlantı durumları görülmektedir. Fiziksel bağlantı yalnızca 1.katman üzerinden yapılmaktadır; ancak tüm katmanlar kendi eşlenikleri olan karşı düğümdeki katmanlarla sanal bağlantı içinde olduğu düşünülür.

Örneğin bir düğümün 3. katmanı ile karşı düğümün 3. katmanı arasında sanal bağlantı vardır. Bu sanal bağlantının kotarılabilmesi için de, katmanlar gönderilecek veri içine başlık bilgisi olarak adlandırılan kendi bilgilerini eklerler.

---

[1] SAP (Service Access Point) : Katmanlar SAP (Hizmet Erişim Noktası) adı verilen katmanlar arası geçiş noktasından işaretleşirler. Katmanların hangi hizmetleri sunacağını ve bu iş için karşı katmanla nasıl bir etkileşim kuracağını belirler.



Şekil 3.4 Ağ üzerinde yönlendiriciler aracılığı ile bağlantı

Katmanlar arasında fiziksel bağlantı yalnızca 1. katmanlar arasında vardır; diğer katmanlar arasında karşılıklı olarak sanal bağlantı olduğu varsayılır.

OSI başvuru modeli, adından da anlaşılacağı üzere veri haberleşmesi için örnek bir modeldir. Öyle ki, farklı gruplar, farklı üretici firmalar tarafından geliştirilen teknolojilerin, mimarilerin açıklanmasında temel alınmaktadır. OSI başvuru modelinde 7 katman tanımlıdır. En altta fiziksel katman bulunurken en üstte uygulama katmanı vardır. Ağ arabağlaşım cihazları, geçityolları hariç, OSI başvuru modeline göre fiziksel katmandan başlayarak alttan 3 veya 3.5 (bazı yönlendiriciler 4. Katmanın birtakım işlevlerine de sahiptirler) katmanın işlevlerine sahip olurlar. Ulaşım katmanı 7 katmanlı modelde ortada bulunur ve modelin ağ hizmet kısmı ile uygulama seviyesi hizmet kısmı arasında önemli bir ilişkiyi sağlar. TCP/IP protokol kümesinin TCP ve UDP protokolleri birer ulaşım katmanı protokolleridir.

BÖLÜM IV

4. TCP/IP PROTOKOL KÜMESİ VE INTERNET

TCP/IP bir protokol kümesidir; marka bağımsız bilgisayar sistemlerinin birbirleriyle karşılıklı çalışabilmesi için en yaygın kullanılan protokol kümesidir denilebilir. Internet'te de TCP/IP (Transmission Control Protocol/Internet Protocol) protokol kümesi kullanılır; bu nedenledir ki, TCP/IP kullanımı çok yaygınlaşmıştır. Öyle ki, kendi LAN'ında TCP/IP dışında farklı bir protokol kümesi kullanan kurumlar, ağlarını Internet'e bağlamak için sistemlerine ya TCP/IP protokol kümesini yüklemekte veya TCP/IP'ye geçiş yapabilecek sistemler eklemektedir.

Internet bir geniş alan ağıdır; ağların ağı da denilmektedir. Bünyesinde binlerce LAN, milyonlarca bilgisayar sistemi vardır ve bunların donanımları, üzerlerinde çalışan işletim sistemleri aynı değildir. Windows[1] , UNIX[2], NetWare[3] gibi birçok işletim sistemi vardır. Bütün bu sistemler, bu kadar çeşitliliğe rağmen tek bir protokol kümesi TCP/IP aracılığıyla birbiriyle iletişim yapabilmektedir. Teknik açıdan bakıldığında, TCP/IP ve Internet hemen hemen aynı anlama gelmeye başlamıştır. [13]

Internet[4] , ağ mimarisi katmanlı yapıdadır; ancak OSI de olduğu gibi 7 katman değil de yalnızca 4 katman tanımlıdır. İletişim için gerekli bütün iş dört katmana ayrıştırılmıştır. Her katmanda yapılacak görevler protokol tanımlamalarıyla belirlenmiştir. TCP/IP, bu protokollerin oluşturduğu kümeye verilen genel isimlendirmedir; TCP ve IP isimleri yalnız başlarına küme içinde birer protokol adıyken, ikisi birlikte protokol kümesine verilen adlandırmadır. TCP/IP protokol kümesi Internet'in yanı sıra birçok ticari ve araştırma ağlarında da yoğun olarak kullanılmaktadır. Küme içindeki protokol tanımları herkese açık olup, serbestçe kullanılabilirler.

---

[1] Windows Microsoft firmasının tescilli ürünüdür.

[2] UNIX, birçok üretici tarafından değişik uyarlamaları geliştirilmiştir; her biri ilgili üreticilerin tescilli ürünüdür.

[3] Netware, Novell firmasının tescilli ürünüdür.

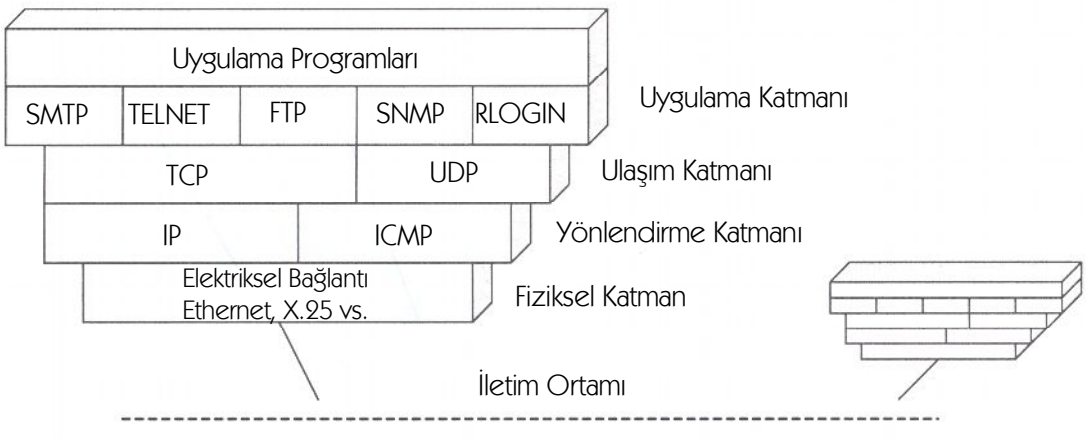
[4] TCP/IP ve Internet üzerine ilk deneysel çalışmalar 1960 yıllarda yapıldı; DARPA (Defence Advanced Research Project Agency) 1965 yılında ARPANET adlı ilk anahtarlamalı ağı kurdu. ARPANET zaman içerisinde önce DoD Internet'e ve ardından günümüzdeki anlamda Internet'e dönüştü. Internet'in bu kadar yaygınlaşması sonucunda da TCP/IP vazgeçilmez bir protokol kümesi haline geldi.

Birçok işletim sistemi, örneğin UNIX ve Windows NT, TCP/IP protokol kümesini kendi bünyelerinde barındırırlar; dolayısıyla böyle sistemleri Internet'e bağlamak için ayrıca üçüncü kişilerce yazılmış TCP/IP yazılımına gerek olmaksızın kendi paketlerinden yüklenebilir.

TCP/IP mimarisinin ikinci katmanında IP ve ICMP yönlendirme protokolleri tanımlanmıştır; ilk uyarlama ile tanımlanan IP protokolü IPv4 olarak adlandırılmıştır; daha sonra yeni nesil yönlendirme protokolü olarak anılan IPv6 (IPng) tanımlanmış olup uygulamada kullanılmaya başlamıştır. IPv6'nın IPv4'den ayrılan en önemli kısmı IP adres uzunluğudur; 32 bit olan IPv4 adresleri 128 bit'e çekilmiştir. Bunun yanı sıra IP paket yapısında da değişiklikler yapılmıştır.

4.1 TCP/IP Mimarisi ve Katmanları

TCP/IP protokol kümesinin sahip olduğu mimari Şekil 4.1'de görüldüğü gibi katmanlı yapıdadır; uygulama programlarının bulunduğu katman sayılmaz ise 4 katmanlıdır. En üstte uygulama programları vardır (bunlar kullanıcının doğrudan etkileşimde bulunduğu programlar da olabilir, işletim sisteminin arka planda (daemon) yürüttüğü programlar da...); altında ise iletişim işini kotaran altkatmanlar bulunur; herbir alt katman OSI başvuru modelinde olduğu gibi bir üstekine hizmet sunarken, bir alttaki katmandan hizmet bekler...



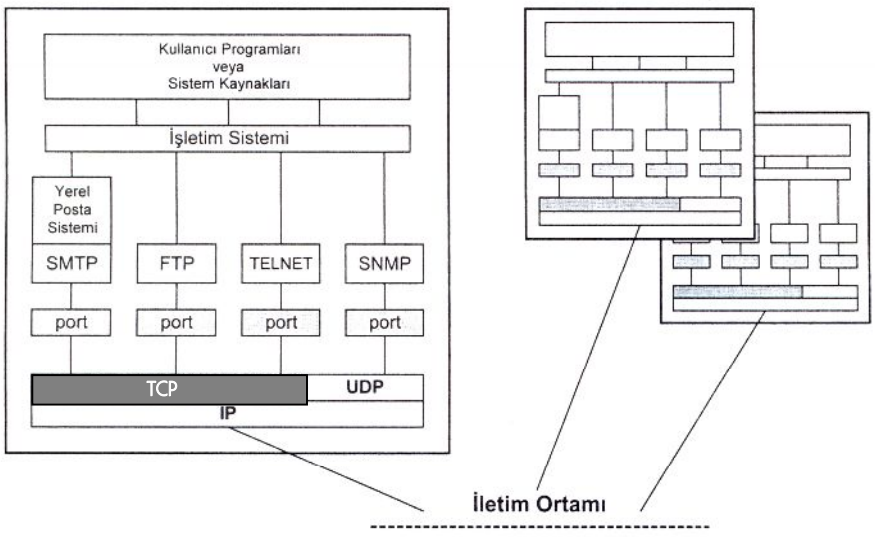
Şekil 4.1 TCP/IP Katmanları

Uygulama katmanının altında da sırasıyla ulaşım, yönlendirme ve fiziksel katmanlar vardır. Ulaşım katmanında TCP ve UDP protokolleri, yönlendirme katmanında IP ve ICMP protokolleri tanımlıdır. Görüldüğü gibi her katmanda birden çok protokol vardır; ancak uygulama programları tarafından istenen bir iş yerine getirilirken, her katmandaki protokollerden yalnızca biri kullanılır. Fiziksel katman ise bir üst katmandan gelen paketleri, içine bakmaksızın iletim ortamından karşı uç sisteme aktarmakla yükümlüdür. Fiziksel katman olarak halihazırda var olan birçok fiziksel katman protokolleri/teknolojileri kullanılmaktadır; örneğin Ethernet, X.25 olabilir. [13]

Uygulama programları, uygulama katmanındaki protokoller aracılığıyla iletişimde bulunabilirler. Örneğin, elektronik mektup (e-mail) SMTP ile belirlenen kurallar uyarınca aktarılır; bu protokol e-mektubun bir kullanıcıya nasıl gönderileceğini belirler. Ağ üzerindeki başka bir bilgisayar dosya aktarımı için bağlanma ve dosya aktarımı için de FTP kullanılır. FTP protokolü karşı uç sistemler arasında dosya alış-verişi için kullanılan bir uygulama katmanı protokolüdür.

Ağ cihazlarını, genel olarak TCP/IP'nin ilk üç katmanıyla ilgilenir; dördüncü katman, eğer ağ cihazı ilgili uygulama protokollerini kendi bünyesinde de çalıştırmak istiyorsa gereklidir. Örneğin bir yönlendirici (Router) cihazı kendisine gelen IP paketlerini optimum bir şekilde alıcısına yönlendirmekle yükümlüdür.

Katmanlar ve onlarda tanımlı protokoller tek tek açıklanmıştır; ancak onların görevlerini anlayabilmek için ağ hizmetlerinden birinin incelenmesi açıklayıcı olur. Şekil 4.2'de TCP/IP'nin katmanlı yapısı, değişik açıdan yeniden gösterilmiştir.

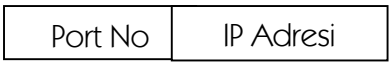


Şekil 4.2 TCP/IP protokolleri arasındaki ilişki

Görüldüğü gibi işletim sisteminin hemen altında uygulama protokolleri vardır; bunlar bir port üzerinden TCP ve UDP'nin bulunduğu katmana erişirler. Çizimde fiziksel katman gösterilmemiştir. [6]

TCP protokolünde her uçta 2^{16} adet farklı port tanımlıdır. Bu 16 bitlik port no (veya adresi) ve 32 bitlik IP adresi beraberce kullanıldığında ortaya çıkan adrese soket numarası denir. TCP bağlantılar bu soketler üzerinden sağlanır. Bir soket aşağıdaki şekilde görüldüğü gibi iki parçadan oluşur:

Soket Numarası



Şekil 4.3 Port No ve IP Adresi

0–255 arasındaki port numaraları, standart uygulama katmanı hizmetlerine erişim için ayrılmıştır. Örneğin, FTP için port 21, TELNET için port 23 gibi birçok port numarası belirli uygulamalar için kullanılır.

Katmanların sahip olduğu görevlerin anlaşılması için, en temel hizmet olan E-mektup örneği üzerinde durulabilir. E-mektup, yazma ortamı sunan bir yardımcı program aracılığıyla yazılır; daha sonra SMTP'de belirli kurallar aracılığıyla alıcıya gönderilir: önce, alıcı ve gönderici adreslerinin belirlenmesi, mektubun konusu ve içeriğinin hazırlanması işleri yapılır. Daha sonra bu protokol uyarınca, hazırlanan mektup bir alt katmana, yani ulaşım katmanına gönderilir. Bu katmanda kullanılan protokol TCP'dir; görevi bir üst katmandan gelen veri paketini gönderilebilecek şekilde parçalara (segments) ayırmak ve onlara sıra numaraları vererek karşı tarafa göndermektir. Tabi ki gönderme işlemini bir altında bulunan yönlendirme katmam IP'den ister. IP protokolü, mektubun doğru adrese ulaştırılması, yani yönlendirilmesi görevini üstlenmiştir. Bu amaçla veri paketinin önüne IP adres bilgilerini yerleştirir; ardından bu mektup fiziksel katman aracılığıyla karşı bilgisayara iletilir.

TCP ve IP, Internet protokol kümesinin kalbini oluşturur. TCP bir üst katmandan gelen veri önüne kendi başlığını ekler ve bir altında bulunan IP'ye gönderir; o da gelen veriye (TCP segmenti olarak anılır) IP başlığı ekleyerek karşı sisteme iletilmesi için fiziksel katmana gönderir.

TC/IP protokol kümesindeki protokoller katmanlara göre sınıflanarak ilerleyen kısımlarda ele alınmıştır:

- **Uygulama Katmanı**

SMTP (Simple Mail Transport Protocol)

SNMP (Simple Network Management Protocol)

TELNET

FTP (File Transfer Protocol)

NNTP (Network News Transport Protocol)

RLOGIN...

- **Ulaşım Katmanı**

TCP (Transmission Control Protocol)

UDP (User Datagram Protocol)

- **Yönlendirme Katmanı**

IP (Internet Protocol)

ICMP (Internet Control Message Protocol)

- **Fiziksel Katman**

Halihazırda kullanılan tüm fiziksel katman standartları kullanılabilmektedir.

4.2 Uygulama Katmanı Protokolleri

Uygulama katmanı için tanımlı olan SMTP, TELNET vs. gibi protokoller bir üstünde bulunan programlara hizmet verirler. Bunların bir üstünde de, ya kullanıcının doğrudan etkileşimde bulunduğu programlar (yani kullanıcı arabirimleri) ya da bilgisayar kaynaklarını başka kullanıcılara erişme olanağı sağlayan (yani hizmet sunan) programlar bulunur. Bunlar, uygulama tipine göre doğrudan uygulama katmanındaki protokollere başvururlar. [1]

- SMTP (Simple Mail Transport Protocol)
  Ağ içerisindeki kullanıcılar arasında elektronik mektup (E- mektup) alış verişini düzenler.

- SNMP (Simple Network Management Protocol)
  Ağ içerisinde bulunan yönlendirici, anahtar ve HUB gibi cihazların yönetimi için kullanılır. SNMP desteği olan ağ cihazları SNMP mesaj alış verişleriyle uzaktan yönetilebilir. Bunun için cihazlarda SNMP parçası (agent) olmalıdır.

- TELNET
  Bir sistem üzerindeki kullanıcının başka bir sisteme bağlanarak, sanki onun terminalindeymiş gibi bağlandığı sistemi kullanmasını sağlar.

- FTP (File Transfer Protocol)
  Bir bilgisayardan başka bir bilgisayara dosya aktarımı için bağlanmasını sağlar. Internet üzerindeki iki sistem arasında dosya aktarımı için kullanılan temel protokoldür.

- NNTP (Network News Transport Protocol)
  USENET postalama hizmetinin kotarılmasını sağlar.

Yukarıdaki protokollerin her biri, biri hizmet sunucu ana makinelerde (server) diğeri hizmet alan uç makinelerde (client) koşmak üzere iki farklı şekilde gerçeklenmiştir. Eğer ağa bağlı sistemler yalnızca bu hizmetleri kullanan uç makine konumunda iseler (kullanıcı olarak anılır), bu protokollerin yalnızca uç uyarlamaları yüklenir. Ancak bir sistem hem hizmet sunuyorsa, hem de hizmet alıyorsa iki uyarlama da yüklenmelidir. Örneğin bir bilgisayara FTP ile bağlanılıp oradan dosya almak için bağlanılan bilgisayarda FTP'nin hizmet sunucu uyarlaması yüklü olmalıdır. Benzer şekilde bir bilgisayardan başka bir bilgisayara FTP ile bağlanılıp oradan dosya çekmek için bağlanan bilgisayarda (alıcıda) FTP'nin uç uyarlaması yüklü olmalıdır.

Örneğin bir bilgisayardan başka bir bilgisayara FTP yapabilmek için, yapanda (kullanıcı-client) FTP kullanıcı arabirimi, yapılanda FTP hizmet (sunucu-server) programı olmalıdır.

4.3 Ulaşım Katmanı Protokolleri

TCP ve UDP ulaşım katmanı protokolleri, bir üst katmandan gelen veriyi paketleyip bir alt katmana verirler; eğer veri bir seferde gönderilmeyecek kadar uzunsa, alt katmana verilmeden önce parçalara ayrılır (segment) ve her birine sıra numarası verilir. Genel olarak TCP kullanılır; UDP daha çok sorgulama amaçlı kullanılır.

4.3.1 TCP (Transmission Control Protocol)

TCP'de tanımlı temel görevler aşağıdaki gibi sıralanabilir:

- Bir üst katmandan gelen verinin uygun uzunlukta parçalara (segmentlere) bölünmesi,

- Her bir parçaya, alıcı kısımda aynı biçimde sıraya koyulabilmesi amacıyla sıra numarası verilmesi ve
- Kaybolan veya bozuk gelen parçaların tekrarlanması olarak verilebilir.

TCP kendisine atanmış olan bu görevleri yapabilmek amacıyla, ulaşım katmanında veri parçalarının önüne başlık bilgisi ekler. Başlık bilgisi ve veri parçası, ikisi birlikte TCP segmenti olarak anılır. Bir alt katmana, örneğin IP katmanına, bu TCP segmenti gönderilir; oradan da bu segmente IP başlığı eklenerek alıcıya yönlendirilir. [11]

TCP segmentin genel formatı Şekil 4.4' te görüldüğü gibidir.

Şekil 4.4 TCP segment formatı

Başlık içindeki alanların kullanım amaçları şöyledir:

- Gönderici Port No (Source Port):
  Bir üst katmanda TCP hizmetini isteyen uygulama protokol prosesinin kimliği durumundadır. Karşı mesaj geldiğinde bir üst katmana iletmek için, o protokolün adı değil de port numarası kullanılır.

- Alıcı Port No (Destination Port) :
  Gönderilen veri paketinin alıcı tarafta hangi uygulama prosesine ait olduğunu belirtir.

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

- Onay Numarası (Acknowledgement Number):
  Gönderilen verinin en son hangi sekizlisinin alındığını göndericiye iletmek için kullanılır. Örneğin n sayısı gönderilirse, n'ye kadar bütün sekizlilerin alındığı belirtilir.

- Başlık Uzunluğu (Header Length) :
  TCP başlığında var olan 32 bit uzunluğundaki sözcüklerin sayısını gösterir.

- Saklı Tutulmuş (Reserved) :
  İlerde olabilecek genişleme için saklı tutulmuştur.

- Kod Bitleri (Bayraklar):
  Kontrol bilgilerini taşımak için kullanılır.

- Pencere (Window):
  Alış tampon belleğindeki kullanılabilir alanın sekizli cinsinden boyu; alış denetimi için kullanılır.

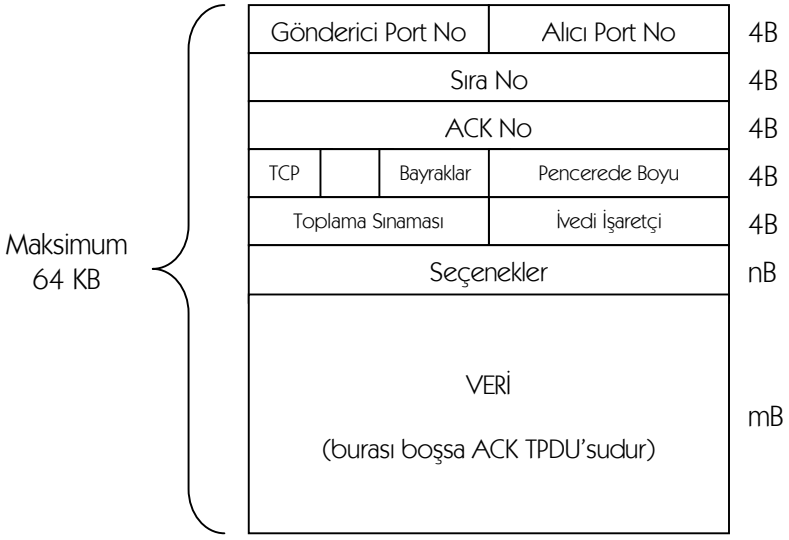
- Hata Sınama Bitleri (Checksum):
  Verinin ve başlığın hatasız aktarılıp aktarılmadığını sınamak için kullanılır.

- Acil İşaretçisi (Urgent Pointer) :
  İvedi olarak aktarımı sonlandırma vb. durumlarda kullanılır. Acil veri, alıcının uygulama katmanında öncelikle değerlendirmesi gereken veridir.

- Veri (Data) :

  İvedi olarak değerlendirilmesi istenen verinin bölüm içindeki yerini işaret eder.

TCP protokolünde bir veri TPDU[1] sunun yapısı aşağıda, Şekil 4.5'de, görülmektedir:



Şekil 4.5 TCP TPDU formatı (n=4,8,12…)

- Sıra No

  TPDU'nun veri alanındaki ilk sekizlinin, bağlantı kurulduğundan bu yana taşınan verinin kaçıncı sekizlisi olduğunu gösterir.

- ACK No

  Karşı uçtan alınması beklenen ilk sekizlinin, bağlantı kurulduğundan bu yana karşıdan gelen verinin kaçıncı sekizlisi olacağını gösterir.

- TCP Başlık Uzunluğu

  4 B biriminde TPDU başlık uzunluğunu verir (3 bit).

[1] TPDU : Ulaşım katmanları arasında karşılıklı değiş tokuş edilen bilgi birimi, Ulaşım Katmanı Veri Birimi (Transport Protocol Data Unit - TPDU) olarak anılır.

- Pencere Boyu

  TPDU gönderildiği anda, alıcının boş durumdaki alış tamponunun boyunu gösterir (birimi sekizli).

- Toplama Sınaması

  TPDU'nun tamamı için 16 bit uzunluklu toplama sınaması karakter dizisi.

- İvedi işaretçi

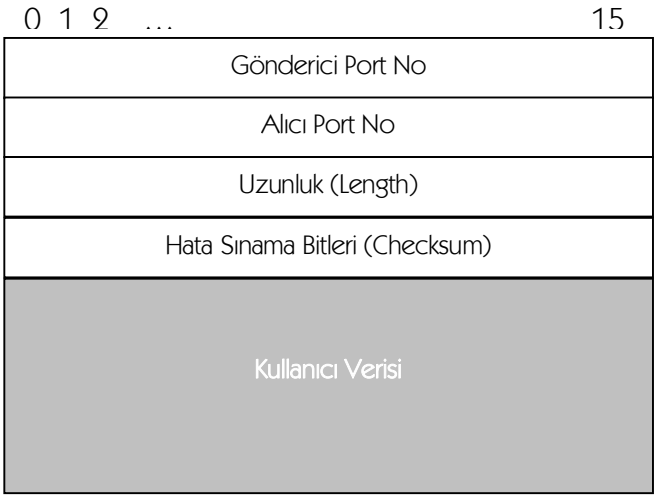
  İvedi verinin bu TPDU'nun taşıdığı veri içindeki yerini işaret eder (sekizli biriminde TPDU'nun ilk veri sekizlisine göre kayıklık değeri). İvedi veri, alıcının uygulama katmanında öncelikle değerlendirilmesi gereken veridir.

- Bayraklar

  TCP TPDU'nun değerlendirilmesine yarayan bit düzeyinde çeşitli belirteçler; ACK, PSH, RST, SYN, FIN ve URG gibi bayraklar vardır. ACK, ACK no geçerli/geçerli değil; PSH, alıcı tarafın TCP modülü bu bayrağı 1 bulursa gelen TPDU'yu bekletmeden bir üst katmanına geçirir; RST, ulaşım bağlantısını yeniden başlatma isteği (karşı taraf önceden gönderdiği tüm TPDU'Iarı tekrarlamak zorundadır); SYN, ulaşım bağlantısı kurma isteği; FIN, ulaşım bağlantısını çözme isteği; URG, ivedi işaretçi geçerli/ geçerli değil gibi anlamlar taşır.

4.3.2 UDP (User Datagram Protocol)

Ulaşım katmanında tanımlı tek protokol TCP değildir; UDP de bu katmanda tanımlıdır. UDP'nin farkı, sorgulama ve sınama amaçlı, küçük boyutlu verinin aktarılması için olmasıdır; veri küçük boyutlu olduğu için parçalanmaya gerek duyulmaz. Dolayısıyla UDP segmenti TCP segmentinden farklıdır; başlık bilgisi daha az alan içerir. Aşağıda (Şekil 4.6' da) UDP segmentinin formatı verilmiştir. [13]



Şekil 4.6 UDP segment formatı

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

4.4 Yönlendirme Katmanı Protokolleri

4.4.1 IP (Internet Protocol)

Yönlendirme katmanında tanımlı IP ve ICMP protokolleri bir üst katmandan gelen segment'leri alıcıya, uygun yoldan ve hatasız ulaştırmakla yükümlüdür. Bu amaçla bu katmanda da gelen segment'lere özel bir IP başlık bilgisi eklenir. IP başlık bilgisinin formatı Şekil 4.7'de görülmektedir.

IP başlığındaki alanların kullanım amaçları aşağıda belirtildiği gibidir:

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

- Başlık Uzunluğu (IP Header length)
  Datagram[1] başlığının gerçek uzunluğunu gösterir (32 sözcük anlamında).

[1] Datagram: Başlık eklenerek göndericiden alıcıya aktarılan veri parçası/birimi.

- Hizmet Türü (Service Type)

  Datagramın nasıl yönlendirileceğini belirler; yönlendirmede yapılan yol seçiminde ve bağlantıda kullanılır. Datagramlara bu alan aracılığıyla önem düzeyi atanabilir.

- Toplam Uzunluk (Total Length)

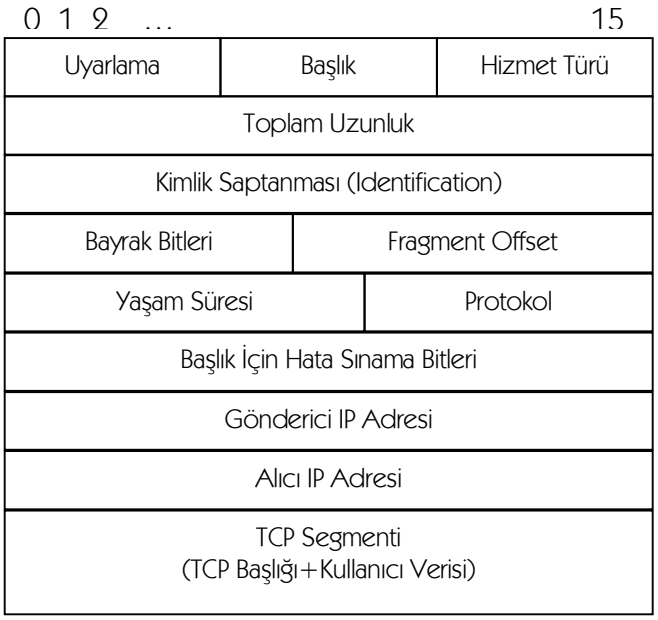
  Tüm IP paketinin (başlık ve veri dahil) uzunluğunu belirtir (sekizli cinsinden olup en fazla 65 535 olabilir).

- Kimlik Saptaması (Identification)

  Kullanıcı karşı tarafla etkileşim içindeyken, mesajlar parçalanarak birçok datagram içinde gönderilebilir, bu alan, aynı kullanıcı mesajının farklı datagramlar içinde bulunması durumunu açıklayan kimlik bilgisi içerir.

- Bayrak Bitleri (Flags)

  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 halinde gönderilen verinin en son olduğunu belirtir. Üçüncüsü saklı tutulmuştur.



Şekil 4.7 IP başlığı içindeki alanlar

- Yaşam Süresi-TTL (Time-to-Live)
  Datagramın ağ üzerinde dolaşma süresini 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 ileteceğini anlar.

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

- Gönderici IP Adresi (Source Address)
  Datagramı gönderen yerin gerçek Internet adresi yerleştirilir.

- Alıcı IP Adresi (Destination Address)
  Datagramın gideceği yerin Internet adresi yerleştirilir.

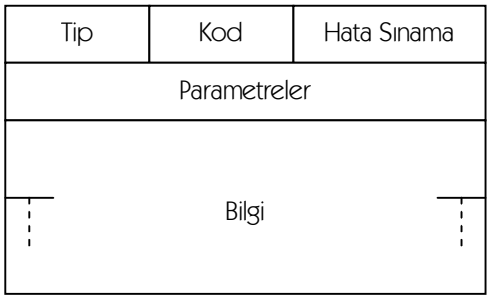
- Seçenekler (Options) çizimde gösterilmemiştir...
  Bu alan değişik amaçlar için kullanılır; güvenlik, hata raporlama gibi vs. seçimliktir; ancak kullanılırsa 32 bitin katları uzunlukta olmalıdır. Yani uzunluğu 32 bitin katlarına tamamlanmalıdır (padding).

- TCP Segmenti:
  Bir üst katmandan gelen veriyi içerir.

4.4.2 ICMP (Internet Control Message Protocol)

ICMP kontrol amaçlı bir protokoldür; genel olarak sistemler arası kontrol mesajları IP yerine ICMP üzerinden aktarılır. [6] ICMP, IP ile aynı düzeyde olmasına

karşın, aslında kendisi de IP'yi kullanır. ICMP mesajları IP üzerinden gönderilir. Aşağıda ICMP formatı görülmektedir:



Şekil 4.8 ICMP formatı

Tip : ICMP mesajlarının tipini gösterir.
Kod : Mesajın parametrelerini belirlemek için kullanılır.
Hata Sınama : Tüm ICMP mesajının hata sınaması için kullanılır.
Parametreler : Parametrelerin daha uzun halinin belirlenmesinde kullanılır.
Bilgi : Mesajla ilgili bilgi.

Birçok ICMP mesaj tipi vardır. Bunlardan bazıları aşağıdaki gibidir:

- Alıcıya erişilemiyor (Destination Unreachable)
- Zaman Aşımı (Time Exceeded)
- Parametre Sorunu (Parameter Problem)
- Yansıma (Echo)
- Yansıma Karşılığı (Echo Reply)
- Zaman Damgası (Time Stamp)
- Zaman Damgası Karşılığı (Time Stamp Reply)
- …..

4.5 Fiziksel Katman

Fiziksel katman için herhangi bir protokol tanımlanmıştır. Paketin iletilmesini kotaran ve halihazırda kullanılan fiziksel aktarım ortamları kullanılabilmektedir.

4.5.1 ARP (Address Resource Protocol)

Günümüzde yerel ağların oluşturulmasında en çok kullanılan ağ arayüzü Ethernet'tir denilebilir. Sistemlere Ethernet arayüzü görevi gören kartlar takılarak yerel ağlara kolayca eklenmektedir. Ethernet arayüzleri birbirlerine veri paketi göndermeleri için, kendilerine üretim sırasında verilen fiziksel adresleri kullanırlar; 48 bit olan bu adresler her bir arayüz için farklıdır.

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

IP paketi içinde hem alıcı hem de gönderici IP adresi vardır; ancak paketin yerel ağ içindeki bir sisteme gönderilebilmesi için donanımın (ağ arayüzünün) fiziksel adresi de bilinmelidir. IP, paketin gideceği fiziksel adresi öğrenmek için o yerel ağ içindeki bilgisayarlara özel bir sorgulama paketi yayar; ARP istek paketi (ARP request packet) olarak anılan bu pakette alıcı sistemin IP adresi vardır ve bunun karşılığı olan fiziksel adresin gönderilmesi istenir.

4.6 IPv6 – Yeni Nesil Yönlendirme Protokolü

IPv6 (IP version 6) diğer adlandırmayla IPng (IP next generation), TCP/IP' nin yeni nesil yönlendirme katmanı protokolüdür. Günümüzdeki tarih itibariyle kullanılan yönlendirme katmanı protokolleri genel isimlendirmeyle IPv4 olarak anılır. IPv6 ile IPv4'de olan birçok kısıtlamalar giderilmeye çalışılmış ve IP başlıklarında çok az kullanılan alanlar kaldırılmıştır. IPv6'da ilk göze çarpan yenilik adresleme alam genişliğidir. IPv4'de 32 bit olan adresler IPv6'da 128 bit olmuştur. Böylece, adres alanı darlığı giderilmiş ve çok daha geniş adres alanı elde edilmiştir. [8]

IPv6 ile genel olarak şu özellikler kazanılmıştır:

- Yeni adresleme şekli
- Güvenliğin artması
- Otomatik konfigürasyon gibi yeni protokol prosesleri
- RIP, OSPF gibi protokollerin genişletilmesi
- Yeni IP paket yapısı
- Değişik protokoller için IP başlığı düzenlemesi

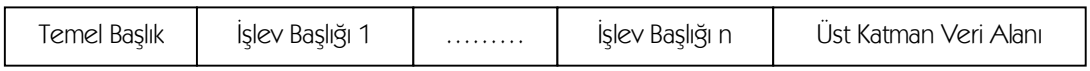
- Ses ve görüntü aktarma desteği...

IP'nin günümüzdeki sürümü olan IPv4 yıllardır büyük bir başarıyla kullanıldı. Başlangıçta umulanın çok ötesinde bir kullanıma ulaştı. Öyle ki 32 bitlik adres uzayının artık tükenme noktasına geldiği söylenebilir. En çok bu nedenle IETF (Internet Engineering Task Force) IP'nin yeni bir sürümünü (IPv6) geliştirdi. IPv6'da adresler 32 yerine 128 bit olarak belirlendi. IPv6'nm hayata geçmesinin diğer nedenleri arasında ise güvenlik ve yönlendirme esnekliğinin önem kazanması gösterilebilir.

IETF, yeni kuşak IP için öneri çağrısını Temmuz 1992'de yaptı; ilk hali toplanan önerilerle şekillendirilerek 1995'te RFC 1752 olarak yayınlandı (The Recommendation for the IP Next Generation Protocol). IPv6'in çeşitli yönlerini tanımlayan diğer RFC'lerRFC1809, RFC 1884, RFC 1886, RFC 1887 şeklinde sıralanabilir.

IPv6, IPv4'ün temel kavramlarını korurken ayrıntılarda önemli sayılabilecek değişikliklere gidildi. IPv6 yine bağlantısız hizmet verip datagram olarak adlandırılan paketlerin aktarımını sağlar. Ancak IPv4 datagram başlığında her işlev için kullanılsın ya da kullanılmasın ayrı bir alan ayrılmışken, IPv6'da her işlev için gerektiğinde kullanılabilecek ayrı başlıklar tanımlanmıştır.

IPv6 datagramı aşağıdaki şekilde görüldüğü gibi bir temel başlık (base header) ve bunun gerekli sayıda (hiç olmayabilir de) işlev başlıkları (extension headers) ile üst katman verisinden oluşur. Bu yaklaşım IP'ye yeni özellikler eklemeyi hayli kolaylaştırmaktadır.



Şekil 4.9 IPV6 datagramı

Temel başlık alanında 128'er bitlik kaynak ve varış adresleri dışında, veri alanı uzunluğu, üzerinden geçilebilecek yönlendirici sayısı üst sınırı (IPv4'teki yaşam süresi alanı), işlev başlıkları için ayrılan alanda her hangi bir işlev başlığı olup olmadığı ve varsa işlev tipi (next header), datagramın tercihli bir yörünge izlemesi isteniyorsa bu yörüngeyi belirleyen bir etiket (flow label) gibi bilgiler için de alanlar ayrılmıştır.

IPv6'nın diğer bir özelliği de ses ve video aktarımını destekleyen mekanizmalar içermesidir; tercihli yörünge atanması ve tüm datagramların göndericiden alıcıya giderken bu yörüngeyi izlemesi gibi.

IPv6'i IPv4'den ayıran bir başka özellik de adreslerin 10 tabanı yerine 16 tabanında yazılmasıdır. Bir örnek vermek gerekirse,

1234:5678:9ABC:DEF0:0FED:CBA9:8765:4321

IPv6 için öngörülen tipik bir adres biçimidir. Öte yandan 32 bitlik IPv4 adreslerini, 128 bitlik IPv6 adres uzayına taşırken yüksek anlamlı 96 bitin 0 alınması kabul edilmiştir. [13]

IPv6'da 3 adres tipi tanımlıdır:

- Tek alıcılı (unicast): Bir düğümün (konak veya yönlendirici) bir arayüzünü gösterir. Aynı arayüzü gösteren birden fazla adres de olabilir. Örneğin iki farklı Internet erişim sunucusuna bağlı bir abonenin her iki erişim sunucusundan görünen adresleri birbirinden farklıdır.

- Herhangi bir alıcı (anycast): Birden çok arayüzü (bunlar farklı düğümlere ilişkin olabilir) belirten bir adrestir. Bu adrese gönderilen bir paket bu adrese sahip arayüzlerden en yakındakine teslim edilir.

- Çok alıcılı: Birden çok arayüzü (bunlar farklı düğümlere ilişkin olabilir) belirten bir adrestir. Bu adrese gönderilen bir paket bu adrese sahip arayüzlerin hepsine birden teslim edilir.

Eğer ön tarafta veya arada değerleri sıfır olan adresler varsa onlar aşağıda gösterildiği gibi yazılmayabilir:

0:0:0:0:0:0:0:1 = ::1

1571:0:0:0:0:0:0:1923 = 1571::1923

IPv6'da 0:0:0:0:0:0:0:0 adresi boş adres, 0:0:0:0:0:0:0:1 adresi de yerel çevrim (loopback) sınaması için saklı tutulmuş özel adreslerdir.

IPv6'in IPv4'ten farklı bir yönü de paket parçalama (fragmentation) işleminin yönlendiricilerde değil yalnızca kaynakta yapılabilmesidir. Bu özellik, yönlendiricilerin yükünü azaltmak için getirilmiştir. Kaynak paketi göndermeden önce varışa giden yörünge üzerindeki izin verilen en büyük paket boyunu (Maximum Transmission Unit - MTU) belirler ve sonra da, paketi bu boyu aşmayan parçalara bölerek yollar. Diğer bir seçenek de parça boyunu 576 sekizliden küçük tutmaktır (Internet ağına bağlanmış bir ağın parçalamadan geçirmek zorunda olduğu en büyük paket uzunluğu).

4.7 UNIX ve TCP/IP

Unix İşletim Sistemleri TCP/IP protokolünü doğrudan kendi bünyesinde barındırarak desteklemektedir. Ku11anıcının bu protokol kümesine erişimi, UNIX çekirdeğine yerleştirilmiş çeşitli yordamların çağrılmasıyla sağlanır. Söz konusu sistem çağrıları kullanıcı/sunucu (client/server) mimarisine uygun şekilde hazırlanmıştır. Bu mimaride, kullanıcılar bir sunucuya çeşitli istekler için başvururlar. Sunucu (veya hizmet veren) her başvuruyu karşılamak için kendi kopyasını, çocuğunu yaratır. Kopyalar paralel çalışırlar; işini bitiren kopya silinerek yok edilir. Sunucu ve kullanıcı taraflarında çağrıların kullanım sırası Şekil 4.10'da verilmiştir.

TCP/IP, genelde, bir dizi değişik protokolde ağ G/Ç işlemleri için soket (socket) adı verilen yapıyı kullanır. Soket, bir iletişim kanalının uç noktasını temsil eder. Böyle bir uç noktasını oluşturabilmek için,

sonuc = socket (giriş parametreleri)

gibi bir sistem çağrısından yararlanılabilir, sonuç değişkenine atanan değer, öpen çağrısının bir dosyaya kimlik (file descriptor) ataması işlemine benzetilebilir. Giriş parametreleri kullanılacak protokolü (örneğin TCP/IP' yi) betimler.

İletişim amaçlı diğer sistem çağrıları şunlardır:

- bind

  Yaratılan bir soketi, numarası belirtilen bir port adresi ile ilişkilendirmek için kullanılır.

- listen

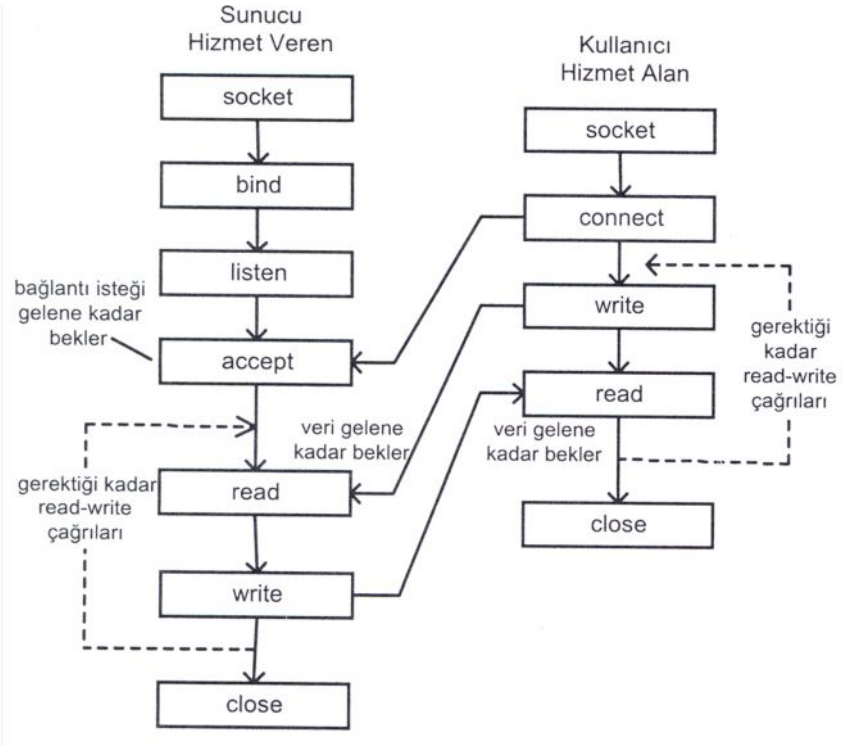
  Yalnızca hizmet veren tarafta kullanılan bir sistem çağrısıdır. Kullanıcılardan, ilgili port adresine (hizmet alan) gelen bağlantı isteklerini bir FIFO kuyruğa aktarıp sıra ile karşılamak için kullanılır. Kuyruk taştığında yeni gelen istekler çöpe atılır.

- accept

  Yalnızca sunucu tarafta kullanılan bir sistem çağrısıdır. Bu çağrı işletildiğinde, sunucu, ilk bağlantı isteği kullanıcıdan ulaşana kadar bloke olarak bekler veya kuyrukta bekleyen bir bağlantı isteği varsa onu değerlendirir. Böyle bir istek ulaştığında, daha önce yaratılmış olan soketin bir kopyası oluşturulur.

y_sonuc = accept (sonuc, ...)

Bu yeni soket, sistem tarafından bağlantı isteğinde bulunanın soket adresinin (port numarası + Internet adresi) yer aldığı bir veri yapısıyla ilişkilendirilir. accept çağrısı yapan sunucu bu aşamada çoğunlukla bir çocuk modül (process) üretip denetimi ona geçirir. Amaç bağlantı isteklerinin birbirinin eş niteliklere sahip modüller tarafından eş zamanlı olarak işlenebilmesidir. Ardından ana modül yeniden accept çağrısında bulunarak beklemeye geçer. [13]



Şekil 4.10 UNIX'te kullanıcı ve sunucu arasındaki sistem çağrı etkileşimi

- connect

  yalnızca hizmet alan tarafta kullanılır, connect çağrısı, hizmet verene bir bağlantı istek TPDU'su gönderir. Ondan gelen olumlu yanıt ile bağlantı kurulur. Olumsuz yanıt veya zaman aşımı durumunda bağlantı kurulmaz, connect çağrısı sonuçlanana kadar hizmet alan bloke kalır.

- read

  soketten okunan veri, parametre alanında işaretlenen bir tampona yerleşir. Yine parametre alanında belirtilen sayıda sekizli alındığında ya da dosya sonu karakteri (EOF) ile karşılaşıldığında read çağrısından dönülür. Bu koşullardan

biri sağlanana kadar çağrıyı yapan bloke kalır. Hem hizmet veren, hem de hizmet alan kullanabilir.

- write

  Read'in tersi işlemi yapan bir sistem çağrısıdır.

- close

  Bağlantının koparılmasını sağlayan sistem çağrısıdır.

Berkeley Unix'te bağlantısız ulaşım protokolünü (UDP) destekleyen sendto, recvfrom gibi sistem çağrıları da tanımlanmıştır.

BÖLÜM V

SALDIRI TESPİT SİSTEMLERİ

Ağ Saldırı Tespit Sistemi (STS), ağlara yapılan saldırıları önlemek için kullanılan, güvenlik duvarı yerleştirilen ağlar arasında belirlenen bir veya birden fazla kural çerçevesinde izolasyon sağlayan ağ parçalarıdır.

İnternet veya yerel ağdan gelebilecek, ağdaki sistemlere zarar verebilecek, çeşitli paket ve verilerden oluşan saldırıları fark etmek üzere tasarlanmış sistemlerdir. [12]

Bu işi yapma üzere tasarlanmış olan güvenlik duvarları[1] yerel ağ dışından gelen saldırıları önlemesine rağmen, saldırıların çoğunun ağ içerisinden düzenlendiği göz önüne alındığında yetersiz kaldığı açıkça görülmektedir.

Bunların önüne geçmek, en az zararla kurtulmak ya da güvenlik sorunlarını bularak aynı hataların tekrarlanmasını önlemek için Saldırı Tespit Sistemleri (Intrusion Detection Systems) kullanılmaktadır. Saldırı Tespit Sistemleri (STS'ler), bilgisayar sistemlerinde veya bilgisayar ağlarında oluşan olayları otomatik olarak belirleyerek güvenlik sorunları oluşturabilecek durumları analiz eden yazılım veya donanım sistemleridir. "2003 CSI/FBI Computer Crime And Security Survey" incelemesinde 1999 yılı itibari ile STS kullanımı %42 iken, 2003 yılında %73 lere ulaşmıştır.

STS'ler analiz yaklaşımına göre kural-temelli(imza-temelli) ve anormallik temelli olmak üzere ikiye ayrılmaktadır. Bu çalışmada heriki sistemin avantajları ve dezavantajları belirtilerek performans analizi yapılmış ve port tarama yazılımı oluşturarak, sistem kaynaklarını zorlamadan saldırıya açık olan portlar ortaya çıkarılarak bunların kapatılması amaçlanmıştır.

---

[1] Güvenlik Duvarı ağ dışındaki bilgisayarların ağdaki bilgisayarlarla doğrudan iletişim kurmasını önler.

5.1 İmza Temelli Saldırı Tespit Sistemi (Snort)

Sistem proseslerinin amacı dışında kullanımını analiz eder, olayları veya bilinen bir saldırıyı tanımlayan olayların önceden tanımlanmış modeli ile benzeyen yanlarını arar. Bilinen saldırıları modelleyen şablona imza adı verildiğinden dolayı bu yönteme imza temelli tespit denir.

Snort IP ağları üzerinde kötüye kullanım tespiti ve gerçek-zamanlı trafik analizi yapabilen yakın zaman önce geliştirilmiş bir ağ-temelli saldırı tespit sistemidir.

Kaynak kodu ile birlikte dağıtılan ve kısa sürede son derece popüler olan Snort yazılımının artan işlevselliği ve becerileri nedeni ile pek çok firma Snort temelli ticari STS çözümleri geliştirmekte ve satmaktadır. Snort günümüzde çok sayıda büyük kuruluş tarafından tercih edilen bir STS haline gelmiştir. [16]

Snort, şablon ekleme tekniğine dayanır ve içerik analizi yapar. Daha önce kayıtlara girmiş kural dışı kullanım kurallarına göre saldırıyı belirler. Snort kural tabanlıdır ve kullanılan dil yeni kurallar eklemeye elverişlidir. Bu sayede kullanıcılar, varolan kuralları kendilerine düzenleyip, ekleyip sisteme esneklik kazandırabilirler. Bu düzenlemeler basit bir txt dosyası içinde yapılmaktadır. Snort kural tanımlama dilinde her bir kural iki kısımdan oluşur.

5.1.1 Kural Başlığı

Kural başlığı beş bölümden oluşur:

1- Kural tepkisi : Saldırı tespit edildiğinde verilecek tepki

2- Uçlar arasındaki kaynak bilgisi

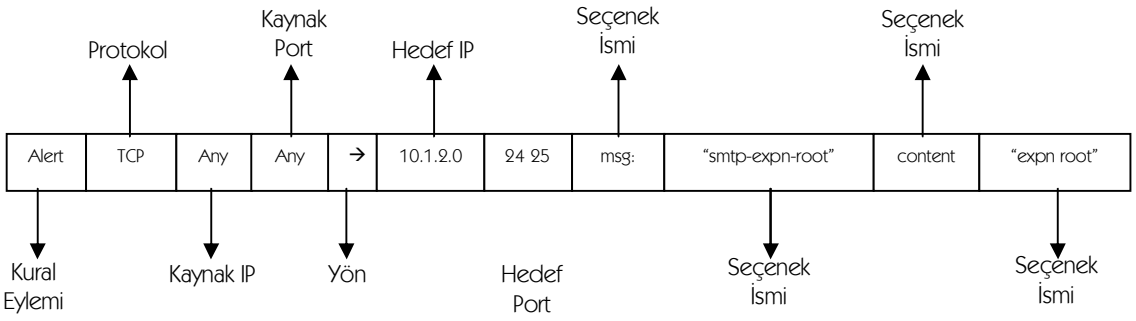
3- Uçlar arasındaki hedef bilgisi: protokole özgü kaynak ve hedef IP adresleri ve port numaralarıdır.

4- Trafik akış yönü bilgisi

5- Protokol türü TCP UDP veya ICMP

Normal şekli aşağıdaki gibi olan bir paket, imza temelli saldırı tespit sistemi ile incelendiğinde Şekil 5.1'deki yapı ortaya çıkar.

alert TCP any any → 10.1.2.0/24 25 (msg: "smtp-expn-root"; content: "expn-root";)



Şekil 5.1 Snort kural yapısı

5.1.2 Kural Seçenekleri

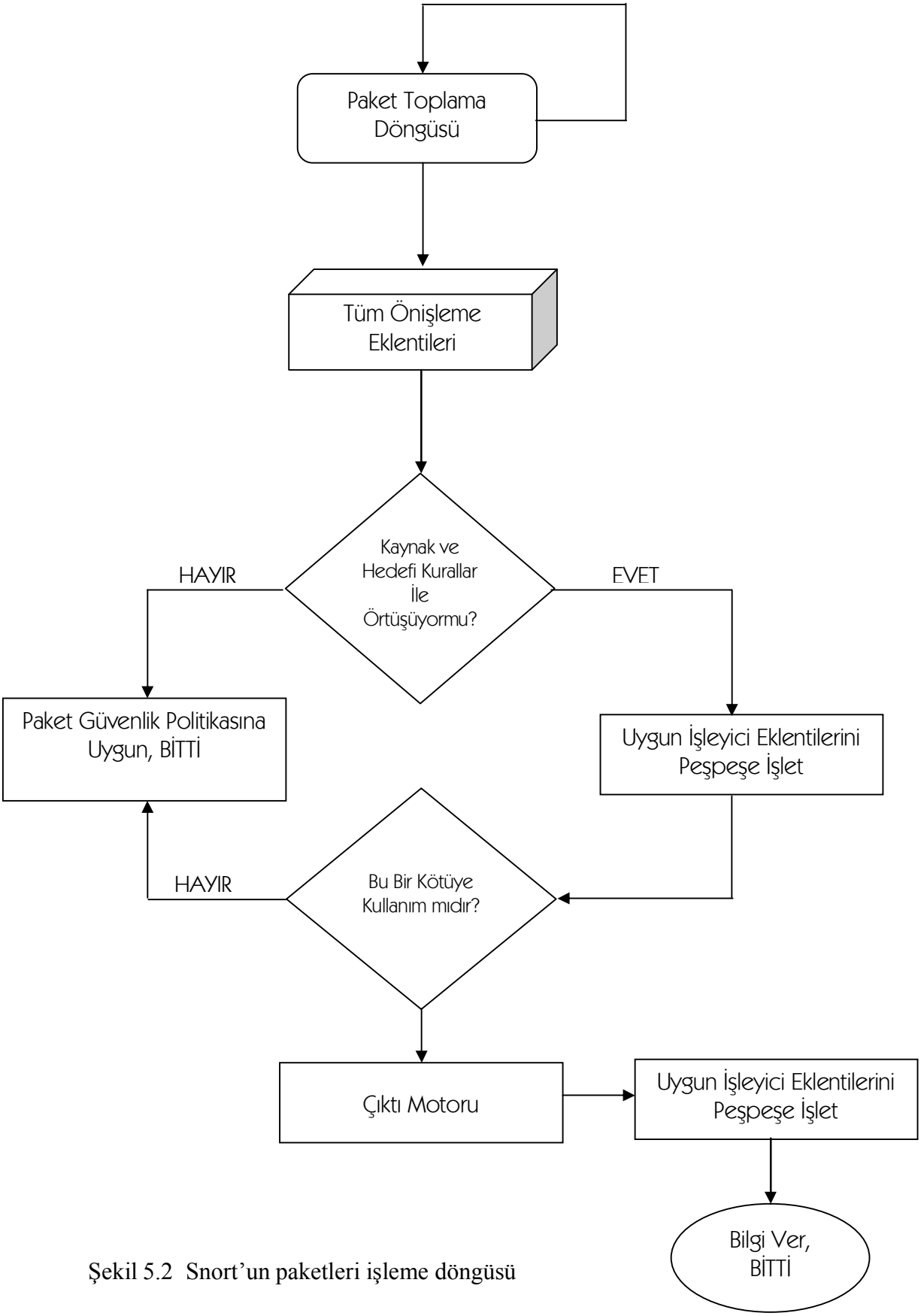
Kural seçenekleri, belirtilen kötüye kullanım işleminin gerçekleşip gerçekleşmediğine karar vermede kullanılan çeşitli şartlardan oluşur. Örnek bir snort kural yapısı yukarıdaki şekilde verilmektedir. Her kuralın ilk alanı eylem dir. Şekil 5.1 deki kuralda seçilen eylem 'alert'tir. Bunun anlamı kuralda belirtilen kriterle eşleşen bir giriş geldiğinde, bir alarm olağanüstü durum oluşturacağıdır. Sonraki alan protokol bilgisini göstermektedir. Örnek kuraldaki protokol TCP'dir. Üçüncü ve dördüncü alanlar kaynak adreslerden oluşur; ilk kısım IP adresi, ikinci kısım kaynak port numarasıdır. Eğer bu alanda any any şeklinde değerler bulunuyorsa bu, paketlerin herhangi bir IP adresinden ve herhangi bir portundan gelebileceğini gösterir. Beşinci alan bilgi akış yönünü göstermektedir. Altıncı ve yedinci alanlar hedef adreslerden oluşur; örnek kuraldaki hedef IP adresi 10.1.2.0/24 olarak verilmiştir ve ilgili bir ağdaki bütün IP adreslerini eşler. Bu örnekte TCP hedef portu 25 olarak ayarlanmıştır. 25 numaralı port, Simple Mail Transfer Protokol (SMTP) için kullanılmaktadır [6].

Hedef adresi takiben seçenekler listesi bulunmaktadır. Her seçenek bir seçenek ismi, varsa seçenek değeri ve seçeneğin bitişini gösteren bir noktalı virgülden oluşur. Şekil 1 'de gösterilen kuralda ilk seçenek msg dir ve eylem mesajını belirtmek için kullanılmıştır. İkinci seçenek olan content, bir şablon eşleşme kriterini belirtmektedir. Örnekte girişin veri alanı kısmında 'expn root' karakter dizisi aratılmaktadır. TCP veri alanında bu karakter dizisine rastlandığı zaman, koşul gerçeklenmiş olur. Bu kriterlerden birinin bile sağlanmaması halinde alarm üretilmez.

Snort'un veri yakalama motoru, Lwarence Berkeley National Laboratuarında geliştirilen libpcap paket yakalama kütüphanesini [7] kullanır. Sistem on taneden fazla Unix türevini ve Ms Windows u desteklemektedir. Ayrıca libpcap kütüphanesini kullanmasından ötürü, farklı ağ ortamlarında çalışabilmektedir. Snort'un başlıca beş bileşeni vardır. [16]

- Paket Yakalama/ ayıklama (dekoder) motoru
- Önişlemci eklenti-yazılımları (plug-ins)
- Tespit motoru
- Kayıt ve alarm sistemi
- Çıkış eklenti-yazılımları

Snort'un paketleri işlemesi Şekil 5.2'de gösterilmektedir.



Şekil 5.2 Snort'un paketleri işleme döngüsü

5.2 İstatistiksel Yaklaşımla Anormallik Temelli STS (PHAD)

Bu bölümde, istatistiksel temelli bir saldırı tespit sistemi olan anormallik tespit yaklaşımlarından Paket Başlığı Davranış Tespiti (PHAD) [10] üzerinde durulmuştur.

PHAD diğer ağ tabanlı davranış tespit sistemlerinden iki yönüyle farklıdır. Bu farklardan ilki PHAD'ın kullanıcı davranışlarından ziyade protokoller modellemesidir. Çünkü birçok saldırı protokol uygulamalarındaki açıklardan faydalanır ve ancak sıra dışı girdi ve çıktıların tespit edilmesi ile anlaşılabilir. Diğer fark da PHAD'ın ağ istatistiklerinin kısa süre içerisindeki hızlı değişiminden uyarılan zaman temelli bir model kullanmasıdır. Bu modellerin temel özellikleri ise şunlardır. [10]

5.2.1 Protokol Modeli

Davranış tespiti sistemlerinin çoğu, yetkili ve yetkisiz kullanıcıları ayırt etmek için tasarlanmıştır. Örneğin yetkili bir kullanıcı ağ topolojisini bildiği için port taramasının yaptığı gibi varolan sunuculara ve hizmetlere bağlanmaya çalışmaz. Ayrıca şifre isteyen sunucular (Telnet, FTP, POP3…) kaynak IP adresleri ile tanımlı yetkili istemcilerden ve/veya günün belirli zamanlarında gelen isteklerden normal davranışı anlar. O halde bu hizmetlere erişmeye çalışan farklı kaynak adresleri için yetkisiz erişim uyarısı verilebilir. Bu tür STS'ler kullanıcı modellemeye dayanmaktadır. Diğer bir yaklaşım ise PHAD'ın da benimsediği protokol modellemesidir. Bilindiği gibi birçok saldırı protokollerin uygulamarındaki açıklardan yararlanır. Örneğin bu tip saldırılar, sendmail, imap ve named protokollerin hatalı uygulamalarını kullanabilirler. Teardrop ve ping of dead saldırıları, IP protokolünün hatalı uygulamalarını deşerler. Bu saldırılar sırasında ağdaki etkinlik bir protokol anormalliğini işaret edebilir. Protokol anormalliklerindeki diğer bir etmen saldıran kodun hatalarından gelir. Aynı sunucuyu veya istemciyi yazan programcının protokolün tüm ayrıntılarını doğru uygulayamaması gibi saldırganda her şeyi doğru yapamaz. Saldırganın, TTL, başlık uzunluğu, doğrulama biti, parçalanma göstergesi gibi IP başlık alanlarını doldururken yaptığı çeşitli hatalar veya alışılmamış uygulamaları ağda olağandışı durumlara yol açabilir.

5.2.2 Zaman Temelli Model

Birçok ağ olayı kendine benzerdir ve değişik periyotlarda kendini tekrarlayan yapıdadır. Ağ olayları birbirinden bağımsız değildir. Tersine uzun vadede bir bağımlılık vardır. Zaman temelli modeli anormallik tespitine uygulamak için eğitim ve test aralıklarında "tn/r" ile bir anormallik skoru hesaplanırİ burada n (herbir alan için uygun türden paketlerin sayısı) ve r (normal değerlerin sayısı) eğitim aralığı boyunca sayılır ve t en son anormalliğin görüldüğü zamandan buyana geçen süredir. [5]

Bu modelde eğitim aşamasında normal olan değerler bulunrak test sırasında normalden sapmalar belirlenir. Örneğin şu eğitim ve test verileri için:

Eğitim safhası (Zaman 0-19) : 00000000000000001111
Test Safhası (Zaman 20-24) : 01223.

Eğitim sırasında izin verilen değerler kümesi kayıt edilir {0,1}; bu kümenin eleman sayısı, r=2, ve gözlem sayısı, n=20 dir. Eğer gözlemler 0 ile başlayan birim aralıklarda yapılırsa eğitim sırasında görülen en son değer olan "1", 16 zamanında gerçekleşir ve zaman değeri test aşamasında kullanılmak üzere tutulur. Test safhasındaki 22, 23 , ve 24. Zamanlardaki "2", "2", ve "3" anormalliktir çünkü bunlar eğitim setinde bulunmamaktadır.

Görülen ilk 2 nin anormallik skoru
tn/r= (22-16)*20/2=60 olarak hesaplanır.

İkinci görülen 2 nin anormallik skoru ;
(23-22)*20/2 = 10 olarak hesaplanır.

"3" ün anormallik skoru
(24-23)*20/2 =10 olarak hesaplanır.

“0” ve “1” in anormallik skorları 0’dır çünkü bunlar eğitim safhasında en az birkez görülmüştür. Bu örnekteki hesaplar tek bir değer baz alınarak yapılmıştır. Birden fazla anormallik özelliğine sahip bir örnek (paket) için anormallik skoru ∑tn/r dir ve burada toplam, anormal özelliklerin üzerinde hesaplanır. [10]

5.2.3 PHAD’ın Anormallik Tespitinde Kullandığı Özellikler

PHAD, ağ paketlerini tespit etmek için kullanılan bir zaman-temelli protokoldür. Her paket için bir skor hesaplar ve gelen ve giden trafik arasında ayrım yapmaz. Paket başlığındaki ilk 4 bayt alanlarına karşılık gelen 33 özelliği modeller. Bir bayttan küçük olan alanlar (TCP bayrakları gibi) bir bayt içinde birleştirilir. 4 bayttan büyük olan alanlar (6 baytlık Ethernet adresleri gibi) bölünür. Özellikler şunlardır:

- Ethernet Başlığı (bütün paketlerde yer alır)
- IP Başlığı
- TCP Başlığı
- UDP Başlığı
- ICMP Başlığı

PHAD, anormal özelliklerin üzerinde Σ tn/r kullanarak bir anormallik skoru hesaplar.

5.3 IDEVAL Değerlendirme Verisi

Yapılan bir bilimsel çalışmanın, varolan çalışmaları geçip geçmediğinin anlaşılabilmesi için diğerleri ile karşılaştırılması gerekir. Bu karşılaştırma işleminin gerçekleşebilmesi ise sonuçların her değerlendirme sonunda tekrar üretilebilir ve güvenilir olması ile mümkündür. Saldırı tespit araçlarının değerlendirilmesi için kullanılan veriler genellikle kişiye aittir ve bu nedenle değerlendirmenin yeniden yapılması halinde aynı sonuçlar alınamamaktadır. Kişisel verilerin başka ellere geçmesi gizlilik ilkesini çiğnediğinden istenmeyen bir durumdur. Bu sorunların üstesinden

gelebilmek için Lincoln Laboratuarı (LL), DARPA'nın sponsorluğunda STS'ler için bir karşılaştırma ortamı sunan IDEVAL veri setini oluşturmuştur [5].

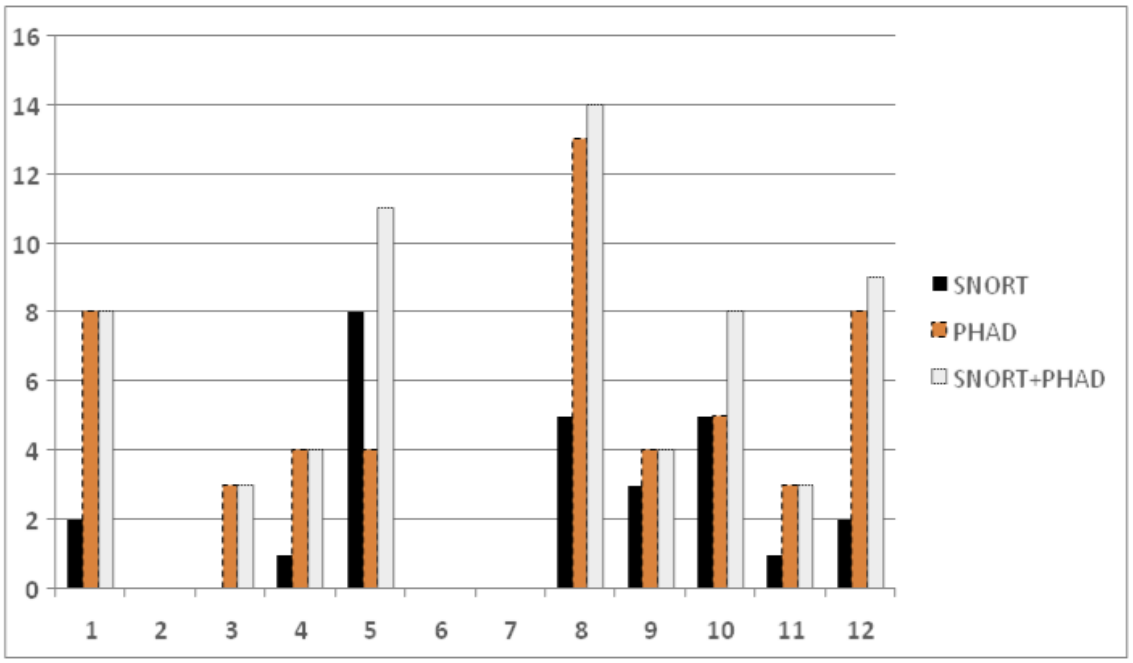
Değerlendirmeler 1998 ve 1999 yıllarında yapılmıştır. 1998 D ARPA çalışmasının amacı, saldın tespit sistemlerinin değerlendirilmesi için ilk standart, yapıyı oluşturmaktı. Saldın tespit sistemlerinin değerlendirilmesi için en uygun durum bilgilerin işleyen bir ağdan alınmasıdır. Ancak bu veriler, kişisel ve gizli bilgiler içerdiği için kullanılamamaktadır. Bu dununda dolayı Amerikan Hava Kuvvetlerindeki bir yerel ağırı simülasyonu gerçeklenmiştir. Bu ağda dns, finger, http, ident, ping, pop, smtp, snmp, telnet, time ve x servislerini içeren yirmiden fazla ağ servisi otomatik olarak oluşturulmuştur. Ağ üzerinde farklı kategorilerde saldırılar denenmiştir [12].

1999 değerlendirmesi önceki yıla ek olarak skor hesaplama yönteminin basitleştirilmesi, anormallik tespit sistemlerinin eğitilmesi için kullanılabilen saldın-içermeyen trafik verisi sağlanması, bir çok yeni saldırının dahil edilmesi ve 1998'de yer alan üç UNIX tabanlı hedef sunucuya bir adet Windows NT sunucusunun eklenmesi gibi iyileştirmeler getirmektedir.

Simülasyonu yapılan ağ içerisinde dört ana "kurban" makine bulunmaktadır. Bunların üzerinde SunOS, Solaris, Linux, ve Windows NT koşmaktadır. Trafik oluşturucular yüzlerce sunucuyu ve çeşitli uygulamalar çalıştıran ve İnternet bağlantısına sahip kullanıcıların simülasyonunu yapmaktadırlar. Ağ üzerinden toplanan veri, dört kurban makineden veya yönlendirici ile kurbanlar arasındaki "iç" ağ yoklayıcısı ve yönlendirici ile İnternet arasındaki "dış" ağ yoklayıcısından toplanmıştır. Saldırılar; İnternet'ten, yerel ağ içerisindeki güvenilen sunuculardan veya yerel ağ ve kurbanlara fiziksel erişime sahip saldırganlardan gelecek biçimde tasarlanmıştır. 1999 değerlendirmesi iki aşamadan oluşmaktadır. Bunun ilk aşamasında katılımcılara üç haftalık eğitim verisi dağıtılmıştır. Bu verilerden birinci ve üçüncü haftalar saldırı içermemektedir ve anormallik tespiti, yapan sistemleri eğitmek üzere kullanılmaktadır. İkinci aşamada katılımcılara sistemlerim test edebilmeleri için iki haftalık test verisi dağıtılmıştır. Bunlar 58 çeşit saldırının 201 tekrarını içerir. [5]

5.4 SNORT ve PHAD Temelli Saldırı Tespit Sistemlerinin Karşılaştırılması

IDEVAL veri seti kullanılarak yapılan testlerde SNORT (İmza Temelli) ile PHAD (İstatistiksel Yaklaşımla Anormallik Tespiti) saldırı tespit sistemi karşılaştırıldığında aşağıdaki grafik elde edilmiştir. [16]



Grafik 5.1 Snort ve PHAD karşılaştırması

5.5 Port Tarama Temelli Model

Birçok işletim sistemi birden fazla programın aynı anda çalışmasına izin vermektedir. Bu programlardan bazıları dışarıdan gelen istekleri (istemci-client/request) kabul etmekte ve uygun gördüklerine cevap (sunucu-server/response) vermektedir. Sunucu programları çalışan bilgisayarlara birer adres verilir (IP adresleri) ve bu adresler kullanılarak istenilen bilgisayarlara ulaşılır. Ulaşılan bu bilgisayar üzerindeki hangi sunucu programdan hizmet almak istendiği belirlemek ise port'lar sayesinde sağlanır.

Bunun için bilgisayarlar üzerinde birtakım soyut bağlantı noktaları tanımlanır ve her birine, adresleyebilmek için pozitif bir sayı verilir (port numarası). Bazı sunucu programları, daha önce herkes tarafından bilinen port'lardan hizmet verirken (örn: telnet->23. port) bazıları da sunucu programını çalıştıran kişinin türüne ve isteğine göre değişik port'lardan hizmet verir. Dolayısıyla, ağ üzerindeki herhangi bir sunucu programa bağlanmak istenildiğinde, programın çalıştığı bilgisayarın adresinin yanında istekleri kabul ettiği port numarasını da vermek gerekir.

Port numarası genellikle 2 byte olarak tutulur. Bu nedenle 65536 adet port numaralamak mümkündür. Genellikle 1024'ten küçük olan port numaraları özel hakları olan kullanıcılar (root) tarafından kullanılırken, büyük olanlar genel kullanıma açıktır.

Port Scanner'ler ise varolan bu port'lar otomatik olarak tarayan yazılımlardır. Scan işleminin birçok çeşidi vardır. Bu çeşitler, hacker ve hacking yöntemlerine karşı artmıştır.

Temel Port Scan türleri aşağıda verilmiştir:

1. TCP SYN Scan
2. SYN/FIN scanning using IP fragments (bypasses packet filters)
3. TCP Xmas Tree Scan
4. TCP Null Scan
5. TCP ACK Scan
6. TCP ftp proxy (bounce attack) scanning
7. TCP Windows Scan
8. TCP RPC Scan
9. UDP Scan
10. Ident Scan
11. TCP FIN Scan

5.5.1 TCP SYN Scan

Bu tarama türü yarı-açık tarama olarak ta anılır. Sebebi ise oturum açma işleminin ilk 2 aşaması olan SYN bayraklı paketi gönderme ve SYN/ACK bayraklı paketi alma işlemini başarıyla yapmasına rağmen ardından RST/ACK bayraklı bir paket göndererek oturumun açılmasını reddetmesidir. Port'un açık olduğu sonucuna SYN/ACK bayraklı paketi alındığında karar verilir. RST/ACK bayraklı paket oturumun resetlenmesi için gönderilen pakettir. Böylece oturum açılmadığından kayıtlara geçme ihtimalimiz azalır.

5.5.2 SYN/FIN Scanning Using IP Fragments

Bu Scan tip aslıda yeni bir yöntem değildir. SYN ve FIN yöntemlerinin geliştirilmiş bir türüdür. Bu yöntemde bir araştırma paketi göndermek yerine paketi daha küçük iki üç IP fragment'i olarak gönderilir. Kısaca TCP paketlerinin başlıklarını paket filtreleşicilerinin işini zorlaştırmak ve yapılan işin anlaşılmaması için çeşitli paketlere bölmektir.

5.5.3 TCP Xmas Tree Scan

Noel ağacı anlamına gelen bu tarama türünde hedef sistemin portuna FIN "No more data from sender", URG "Urgent Pointer field significant" ve PUSH "Push Function" flaglı paket gönderilir ve kapalı olan port'lardan RFC 793'e göre RST cevabı beklenir. Cevapsızlar yine açık port'lardır.

5.5.4 TCP Null Scan

Bu tarama türü ise Xmas Tree'nin tersine hiçbir bayrak taşımayan bir paket gönderir. RFC 793'e göre sistemin kapalı olan portlarından RST cevabı gelir.

5.5.5 TCP ACK Scan

Bu tip taramada temel mantık statik yada dinamik paket filtreleme de firewall'ların bağlantıyı ilk başlatan tarafı hatırlayamamasıdır. Bazı firewall'ların onaylanmış bağlantılara izin verdiğini de düşünürsek bu ACK "Acknowledgment field significant" paketin firewall ya da router'ların içinden engellenmeden geçmesi ve hedefe ulaşması mümkün olabilir. Bu şekilde Firewall'ları bypass ederek hedefe ulaşıp hedefin port'larını tarama şansı kazanırız.

5.5.6 TCP Ftp Proxy (Bounce Attack) Scanning

RFC 959 tanımına göre ftp protokolünün dikkat çekici bir özelliği de proxy ftp bağlantısına izin vermesidir. Bu tür scan tipi ise bu özelliğin yarattığı açığı kullanır. Çünkü bu özellik hacker.com'dan, kurban.com'un FTP server-PI (protocol interpreter) aracılığı ile kontrol haberleşme bağlantısı kurulabilir. Bu bağlantı sayesinde, server-PI'e ağdaki her hangi bir yere dosya yollayabilecek server-DTP (data transfer process) isteği aktif edilebilir. Bu açık özellikle firewall arkasında bağlı bulunan bir ftp'ya bağlandığımız zaman sunucuya kendi port'larını taratması sağlandığı için çok tehlikeli bit tarama türüdür. Çünkü firewall baypas edilmiş olur. [12]

5.5.7 TCP Windows Scan

Bu scan türü TCP Windows Scan raporlarındaki kusurları dikkate alarak bazı işletim sistemlerinde portların açık olup olmadığını ya da filtreli olup olmadığını kontrol eder.

5.5.8 TCP RPC Scan

Bu tarama yöntemiyle RPC (Remote Procedure Call - Uzak işlem çağrıları) port'larından çalışan işlemleri ve sürümlerini anlama şansımız olabilir. Blast virüsü bu açığı kullanarak Service Pack 1 yüklü Microsoft Windows XP sistemlerde otomatik

bilgisayar kapatma prosedürünü başlatarak birçok kullanıcının bilgisayarını istekleri dışında kapatmıştır.

5.5.9 UDP Scan

Bu teknik hedef porta udp paketi göndererek kapalı olan porttan "ICMP port unreachable" mesajının alınması temeline dayanır. Eğer bu mesaj gelmezse port'un açık olduğu anlaşılır.

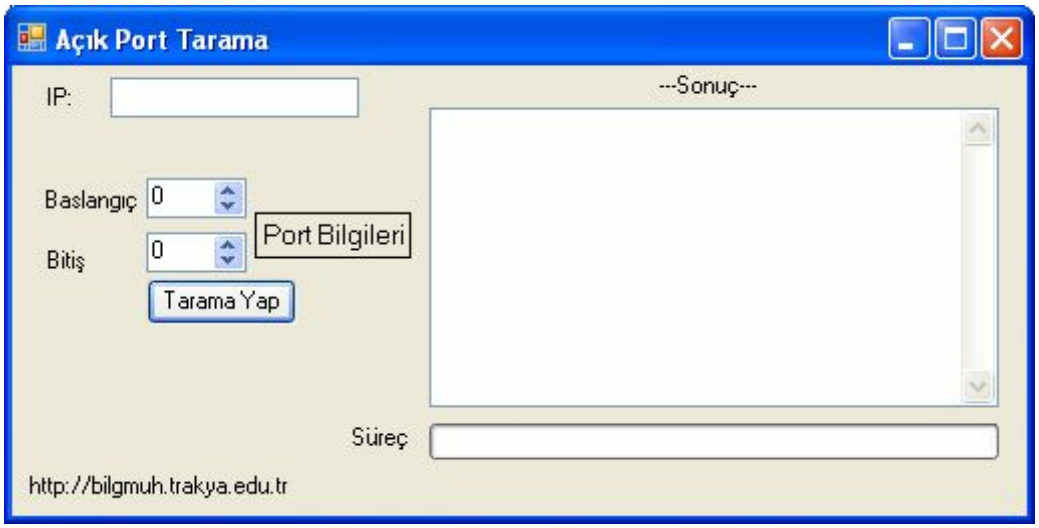
5.5.10 Ident Scan

RFC 1413'te tanımlanmış bir protokol olan Ident protokolü üzerine inşa edilen bir tarama türüdür. Diğer taramalar ile birlikte kullanılır. Hedef sistem üzerinde Ident aktif ise sistemde çalışan servislerin tam listesine ve bu servisleri çalıştıran kullanıcıların isimlerine ulaşılması için yapılır. Ident aktif durumda değil ise bu tarama türü işlevsiz olmaktadır.

5.5.11 TCP FIN Scan

Eğer bir port'u oturum açma işlemlerini kullanmadan taramak istiyorsak kullanabileceğimiz yöntemlerden biri FIN taramadır. Eğer bir sistemin port'larından birine FIN bayraklı bir paket gönderilirse RFC793'e göre sistem kapalı olan portlar için RST cevabı gönderir. Böylece açık olan portların bilgisi alınır. Saldırıların çoğunun oturum açmadan gerçekleştiğinden hareketle, bir TCP FIN Scan uygulaması geliştirilmiş ve aşağıda kodları ve program arayüzü belirtilmiştir.

5.5.11.1 Bir TCP FIN Scan Uygulaması Oluşturulması



Şekil 5.3 Bir TCP FIN Scan Uygulaması

Program Kodu :

```
//Kullanılacak NameSpace ler tanımlanıyor...
using System;
using System.Collections.Generic;
using System.ComponentModel;
using System.Data;
using System.Drawing;
using System.Text;
using System.Net.Sockets;
using System.Windows.Forms;

namespace PortScanner // Port Scanner Adında Bir NameSpace
                      Tanımlanıyor...
{
      public partial class frmMain : Form //frmMain ve Form birer
Class olarak tanımlandı.
      {
            protected int StartPort; // Başlangıç ve Bitiş Portlarının
Değerleri Formda Kullanılabilmesi için
                                  //Integer Olarak Tanımlandı.
```

```
            protected int EndPort;

            public frmMain()         // frmMain Class sınıfının
kullanacağı yöntem be komutlar giriliyor.
            {
                  InitializeComponent();
            }

            private void btnScan_Click(object sender, EventArgs e)
            {


            // Değişkenlerden Değerler Alınarak string türünden int
türüne çevriliyor ve
            // Yeni Değişkenler olan StartPort ve EndPort a
aktarılıyor.
                  StartPort = Convert.ToInt32(numStart.Value);
                  EndPort = Convert.ToInt32(numEnd.Value);
                  // Tranacak Port Sayısı Sıfırlanıyor
                  prgScanning.Value = 0;
                  // Maksimum Taranacak Port Sayısı Hesaplatılıyor
                  prgScanning.Maximum = EndPort - StartPort + 1;
                              // Uygulama Çalışırken Kürsör Bekleme
                     Konumuna  Alınıyor
                  Cursor.Current = Cursors.WaitCursor;
                  // Başlangıç ve Bitiş Portları Belirtilen IP ye
Tarama İşlemi Başlatılıyor
                  for (int CurrPort = StartPort; CurrPort <= EndPort;
CurrPort++) // Anlık Taranan Port CurrPort değişkenine aktarılıyor

// Daha sonra Bitiş Port Sayısına Ulaşana Kadar 1

// Artırılıyor
                  {
                        TcpClient TcpScan = new TcpClient(); // TCP
protokol taraması için istemci oluşturuluyor
                        try
                        {
```

```
                        // Verilen IP ye Anlık Porttan
BAğlanılmaya Çalışılıyor
                        TcpScan.Connect(txtIP.Text, CurrPort);
                        // Eğer istisnai bir durum olmazsa,
porttan yanıt alınırsa port açık seklinde Forma mesaj yazdırılıyor

                        txtLog.AppendText("Port " + CurrPort + "
Açık\r\n");
                    }
                    catch
                    {
                        // Port Yanıt vermezse kapalı olduğu
forma yazılıyor

                        txtLog.AppendText("Port " + CurrPort + "
Kapalı\r\n");
                    }
                    // Diğer portu taramaya geçmeden önce gösterge
çubuğunun değeri bir artırılıyor

                    prgScanning.PerformStep();
                }
                // Bütün portların Taraması Bittikten sonra,
Kullanıcının Yeni Tarama yaptırabilmesi için
            // Kürsör kullanılabilir hala getiriliyor ve İmleç Normal
şekli ile ekranda beliriyor

                Cursor.Current = Cursors.Arrow;
            }

        private void txtIP_TextChanged(object sender, EventArgs e) //
Daha öce IPtextBox a yazılan Değer Sıfırlanıyor
        {

        }

        private void txtLog_TextChanged(object sender, EventArgs e)
        {
```

```
        }

        private void label2_Click(object sender, EventArgs e)
        {

        }

        private void frmMain_Load(object sender, EventArgs e)
        {

        }
    }
}
```

SONUÇLAR

Port tarama temelli bir saldırı tespit sistemi olan TCP FIN Scan yöntemi saldırıların çoğu oturum açmadan gerçekleştirildiğinden ve sistem kaynaklarını verimli kullandığından diğer port tarama yöntemlerine göre daha başarılı olduğu tez çalışmasında yapılan TCP FIN Scan uygulamasına bakılarak gözlenmiştir.

Anormallik tespit sistemleri ile imza temelli sistemlerin birleştirilmesi sonucu oluşan karma sistemin yalnızca imza tespiti yapan sisteme göre çok daha başarılı olduğu görülmüştür.

TARTIŞMA

Daha önce yapılan araştırmalarda, anormallik tespit sistemlerinden istatistiksel temelli bir STS olan PHAD'ın iyileştirilerek Snort'a önişlemci olarak eklenmesiyle katkı sağladığı gözlenmişti. Bu bağlamda, Snort'a, Port Tarama Temelli STS'lerin de eklenmesi başarımı artırabilir.

KAYNAKLAR

[1] Yıldırımoğlu. M, 2000, "TCP/IP Internet'in Evrensel Dili", Pusula

[2] Yihaoliao. V, Rao. V, 2002, "Use of K-Nearest Neighbor classifier for intrusion detection" Computers & Security, Vol 21 Prentice Hall

[3] Ghosh. K, Schwartzbard. A, Shatz. M, 2000, "Learning Program Behavior Profiles for Intrusion Detection" , MacMillan publishing

[4] Mikhail. G, 2002, "Intrusion Detection: Techniques and approaches", Prentice Hall

[5] Fink. G, Levitt. K, 2004, "Automated Detection of Vulnerabilities in Privileged Programs by Execution Monitoring", Computer Science Department Columbia University

[6] Çölkesen. R, 2001, "Network TCP/IP UNIX", Papatya

[7] Dirican. C, 2005, "TCP/IP ve Ağ Güvenliği", Açık Akademi

[8] Kaplan. Y, 2002, "NETWORK Veri Haberleşmesi ve UYGULAMARI", Pusula

[9] Warrender. C, 2003, "Detecting Intrusions Using System Calls: Alternative Data Models" , Prentice Hall

[10] Erman. M, and M. Xu, 2001, "Probabilistic Techniques for Intrusion Detection Based on Computer Audit Data"

[11] Neibauer. A, 2000, "Bilgisayar Ağları", Çeviri, Kaya. D, Arkadaş

[12] Takçı. H, Soğukpınar. İ, 2003. "Saldırı Tespitinde En Yakın k Komşu Uygulaması", Gebze Yüksek Teknoloji Enstitüsü

[13] Çölkesen. R, ve Örencik B, 2002, "Bilgisayar Haberleşmesi ve Ağ Teknolojileri", Papatya

[14] Lockhart A, 2006, "Ağ Güvenliği İpuçları", Çeviri, Şen. Ö, Açık Akademi

[15] Bentham. J, 2000, "TCP/IP LEAN Web Servers for Embedded Systems", CMP Books

[16] Örencik. B, ve Aydın. M, A, 2005, "Ağ ve Bilgi Güvenliği Ulusal Sempozyumu"

[17] http://www.sans.org (Network Security and Architecture Laboratory)

[18] http://www.msakademik.net

[19] http://www.c-sharpcorner.com

[20] KENDALL K. E., KENDALL J. E., 1998 "System Analysis and Design", Prentice Hall

[21] Russel. R, 2003, Snort Intrusion Detection 2.0, Syngress Publishing

[22] Mahoney. M, Chan. V, 2001, Florida Tech

[23] Lippman. R, Haines. J.W, Fred. D.J, Kobra. J, Das. K, 2000, The 1999 DARPA Offline Intrusion Detection Evaluation, Computer Networks

ÖZGEÇMİŞ

Erkan ÖZHAN, 30/11/1978 yılında Malatya'nın Hekimhan ilçesinde doğdu. İlk öğrenimini 09/06/1989 tarihinde Hekimhan ilçesi Güzelyurt kasabası Aşağı Güzelyurt İlkokulu'nda tamamladı. Ortaokulu ise yine Güzelyurt kasabasında bulunan Güzelyurt Lisesi'nde 05/06/1992 de tamamladı. Liseyi 09/06/1995 te Malatya merkez H.Ahmet Akıncı Lisesi'nde bitirdi.

1996 yılında Fırat Üniversitesi Teknik Eğitim Fakültesi Elektronik ve Bilgisayar Eğitimi Bölümü Bilgisayar Öğretmenliği Eğitim-Öğretim programını kazandı ve 20/06/2000 tarihinde buradan mezun oldu. Aynı yıl M.E.B'na bağlı Aksaray Somuncubaba Lisesi'ne bilgisayar öğretmeni olarak atandı. Burada bir yıl çalıştıktan sonra, Trakya Üniversitesi Çorlu Meslek Yüksek Okulunun açtığı öğretim elemanı alım sınavını kazanarak 24/10/2001 de öğretim görevlisi oldu. Halen Namık Kemal Üniversitesi Çorlu MYO' da öğretim görevlisi olarak görev yapmaktadır.