YILDIZ TEKNİK ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

AĞ GÜVENLİĞİ VE GÜVENLİK DUVARINDA VPN VE NAT UYGULAMALARI

Elektronik Mühendisi Zeynep YÜKSEL

FBE Eleketrik-Elektronik Anabilim Dalı Haberleşme Programında
Hazırlanan

YÜKSEK LİSANS TEZİ

Tez Danışmanı : Yrd. Doç. Dr. N. Özlem ÜNVERDİ

İSTANBUL, 2007

YILDIZ TEKNİK ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

AĞ GÜVENLİĞİ VE GÜVENLİK DUVARINDA VPN VE NAT UYGULAMALARI

Elektronik Mühendisi Zeynep YÜKSEL

FBE Eleketrik-Elektronik Anabilim Dalı Haberleşme Programında
Hazırlanan

YÜKSEK LİSANS TEZİ

Tez Savunma Tarihi : 10 Ekim 2007
Tez Danışmanı : Yrd. Doç. Dr. N. Özlem ÜNVERDİ
Jüri Üyeleri : Yrd. Doç. Dr. Soner ÖZGÜNER
Prof. Dr. Osman Nuri UÇAN

İSTANBUL, 2007

İÇİNDEKİLER

Sayfa

KISALTMALAR

AAA	Authentication, Authorization, and Accounting
ACE	Access Control Entry
ACK	Acknowledgment
ACL	Access Control List
ARP	Address Resolution Protocol
ASDM	Adaptive Security Device Manager
ASP	AppleTalk Session Protocol
ATM	Asynchronous Transfer Mode
BootP	Bootstrap Protocol
BPDU	Bridge Protocol Data Unit
BSS	Basic Service Set
CCK	Complementary Code Keying
CDP	Cisco Discovery Protocol
CERT	ComputerEmergencyResponseTeam
CF	Contention Free
CFP	Contention Free Period
CHAP	Challenge-Handshake Authentication Protocol
CP	Contention Period
CRC	Cyclic Redundancy Check
CS	Carrier Sense
CSMA/CA	Carrier Sense Multiple Access with Collison Avoidance
CSMA/CD	Carrier Sense Multiple Access with Collision Detect
CTS	Clear To Send
DA	Destination Address
DBPSK	Differential Binary Phase Shift Keying
DC	Doğru Akım
DCF	istributed Cordination Function
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DHCP	Dynamic Host Configuration Protocol
DIFS	Distributed Cordination Function Interframe Space
DMZ	Demilitarized Zone
DNASCP	Digital Network Arcitecture Session Control Protocol
DoD	Department of Defense
DQPSK	Differential Quadrature Phase Shift Keying
DS	Distribution System
DSA	Sayısal İmza Algoritması
DSAP	Destination SAP
DSS	Distribution System Service
EIFS	Extended Interframe Space
EIGRP	Enchanced Interior Gateway Routing Protocol

ESS	Extended Service Set
FC	Frame Control
FCS	Frame Check Sequance
FH	Frequany Hopping
FHSS	Frequany Hopping Spread Spectrum
FTP	File Transfer Protocol
GFSK	Gaussian Frequancy Shift Keying
GRE	Generic Routing Encapsulation
IAPP	Inter Access Point Protocol
IBSS	Independed Basic Service Set
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IFS	Interframe Space
IGRP	Interior Gateway Routing Protocol
IKE	Internet Key Exchange
IP	Internet Protocol
IPsec	IP Security
IPX	Internetwork Packet Exchange
IR	Infrared
ISAKMP	he Internet Security Association and Key Management Protocol
ISM	Industrial, Scientific and Medical
ISO	International Organization for Standardization
L2TP	Layer 2 Tunneling Protocol
LAN	Local Area Network
LEAP	Lightweight Extensible Authentication Protocol
LLC	Logical Link Control
MAC	Medium Access Control
MAC	Media Access Control
MAC	Media Access Control
MPLS	Multiprotocol Label Switching
MRTG	Multi Router Traffic Grapher
NAT	Network Address Translation
NAV	Network Allocation Vector
NFS	Network File System
NIC	Network Interface Card
NIC	Network Interface Card
NTP	Network Time Protocol MD5
OSI	Open System Interconnection
OSPF	Open Shortest Path First
PAP	Password Authentication Protocol
PAT	Port Address Translation
PC	Point Coordinator
PC	Personal Computer
PCF	Point Coordinator Function
PDU	Protocol Data Units
PGP	Pretty Good Privacy
PHY	Physical (Layer)
PHY-SAP	hysical Layer Service Access Point
PIFS	Point Coordination Function Interframe Space

PLCP	Physical Layer Convrgence Protocol
PLME	Physical Layer Menagemant Entity
PMD	Physical Medium Dependent
PoE	Power Over Ethernet
PPTP	Point-to-Point Tunneling Protocol
RA	Reciever Address
RADIUS	Remote Access Dial In User Service
RADIUS	Remote Authentication Dial In User
RARP	Reverse Address Resolution Protocol
RF	Radio Frequancy
RIP	Routing Information Protocol
RPC	Revate Procedure Call
RSA	Rivest, Shamir ve Adleman
RTS	Request To Send
SA	Source Address
SAP	Service Access Point
S-HTTP	Secure Hypertext Transfer Protocol
SIFS	Short Interframe Space
SNAP	SubNetwork Access Protocol
SNMP	Simple Network Management Protocol
SOHO	Small Office Home Office
SQL	Structured Query Language
SSAP	Source SAP
SSID	Service Set Identifier
SSL	Secure Sockets Layer
STP	Spanning Tree Protocol
TACACS	Terminal Access Controller Access-Control System
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
VPN	Virtual Private Network
WAN	Wide Area Network
WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access

ŞEKİL LİSTESİ

TABLO LİSTESİ

ÖNSÖZ

Yapılan bu çalışmada kısaca ağ güvenliğini ilgilendiren her türlü bileşen incelenmiş ve son zamanlarda dünya çapında hızla yaygınlık kazanan güvenlik duvarı ile VPN ve NAT uygulamaları detaylı bir şekilde incelenmiştir.

Bu çalışmanın hazırlanması sürecinde yol göstericiliğinden ve özellikle gelecekte çok fazla kullanılacak olan bu teknoloji ile daha yakından ilgilenmemi sağlayan sayın hocam Yrd.Doç.Dr. N.Özlem Ünverdi'ye teşekkürlerimi sunuyorum.

Çalışmam esnasında bana gerekli donanımı sağlayan Logicom Bilgi Teknolojileri Dağtım Ltd. Şirketine teşekkürlerimi sunarım.

Son olarak tüm hayatım boyunca bana olan sevgi ve desteklerinden dolayı çok değerli aileme sonsuz sevgi, saygı ve teşekkürlerimi sunuyorum

ÖZET

Yapılan bu çalışmada ağ güvenliğini ilgilendiren her türlü bileşen incelenmiş ve son zamanlarda dünya çapında hızla yaygınlık kazanan güvenlik duvarı ile VPN ve NAT uygulamaları detaylı bir şekilde ele alınmıştır.

İstenilen hedefe ulaşabilmek için ilk bölümde genel işaretleşme kavramları, modülasyon teknikleri ve iletim ortamları ele alındıktan sonra bir sonraki bölümde yerel alan ağlarında TCP/IP ve katman güvenliği incelenmiştir.

Üçüncü bölümde kablosuz yerel alan ağı sistemleri ve bu sistemlerde uygulanan güvenlik stratejileri vurgulamıştır.Daha sonraki bölümde bilgisayar ağının güvenliğini ilgilendiren her türlü bileşenin yönetimi ile ilgili stratejinin resmi şekilde yazılı olarak ifade edildiği güvenlik politikaları ve güvenlik duvarı mimarileri ve bileşenleri detaylı bir şekilde ele alındıktan sonra bir sonraki bölümde ağ cihazları üzerinde nasıl önlemler alınabileceği irdelenmiş ve güvenliğin bir bütün olarak incelenmesinin gerekliliği vurgulanmıştır.

Uygulamalarımızın olduğu son bölümde ise güvenlik duvarında VPN ve NAT uygulamaları incelenmiş ve sonuç kısmında ise ağ güvenliğinin önemi vurgulanmıştır.

Anahtar Kelimeler: Ağ Güvenliği, Güvenlik Duvarı , VPN, NAT

ABSTRACT

In this project every component which is including network security were examined and firewall ,NAT and VPN technology studies which is growing rapidly were discussed.

To reach the aim, firstly general signal concepts , modulation varieties and transmission media were analyzed after that in following chapter ,TCP /IP and layer security were examined in local area network.

In the third chapter wireless local area network and its security were analyzed. In the next step Security policies and firewall architecturals which is including network security were emphasized.In other chapter it was discussed how to guard on the network equipment and security were examined as a whole.

In the conclusion, NAT and VPN technology studies in firewall which will be available in the future were introduced.

Keywords: Network Security,Firewall , VPN, NAT

1. GİRİŞ

Genel işaretleşme kavramları, modülasyon teknikleri ve iletim oranlarına genel bir giriş yapılmıştır. Ayrıca veri haberleşme kodları ve makinelerin birbirlerine iletim yaparken eşzamanlamanın nasıl sağlandığı konularına değinilmiştir.

1.1 Veri Haberleşme Sistemleri İşlemleri ve Verinin İletilmesi

Bilgisayarların, veri haberleşmesinin ve ağların amacı veriyi bilgiye çevirmektir. Veri bir bilgisayarda saklanır ve bir haberleşme sistemi üzerinden ikilik tabanda (0 veye 1' ler biçiminde) iletilir.

Bir bilgisayardaki bitler elektrik işaretinin polarizasyon seviyeleri ile gösterilirler. Bir bilgisayardaki saklama elemanı içindeki yüksek-seviye işareti 1'i ve alçak-seviye işareti 0'ı gösterebilir. Bu elemanlar birlikte dizilerek belirlenmiş kodlara göre sayı ve karakterleri oluştururlar.

Veri; haberleşme yolu üzerinden bilgisayar-yönlendirmeli cihazlar arasında elektrik işaretleri ve bit katarları ile iletilir. Bu elektrik işaretleri ve bit katarları harf ve karakterleri belirtir. Bazı durumlarda, veri ışık işaretleri ile gösterilir (fiber optik hatlarda). Bit dizileri kullanıcı verisini ve kontrol verisini tanımlar. Kontrol verisi, haberleşme ağını ve kullanıcı verisi akışını yönetmek için kullanılır.

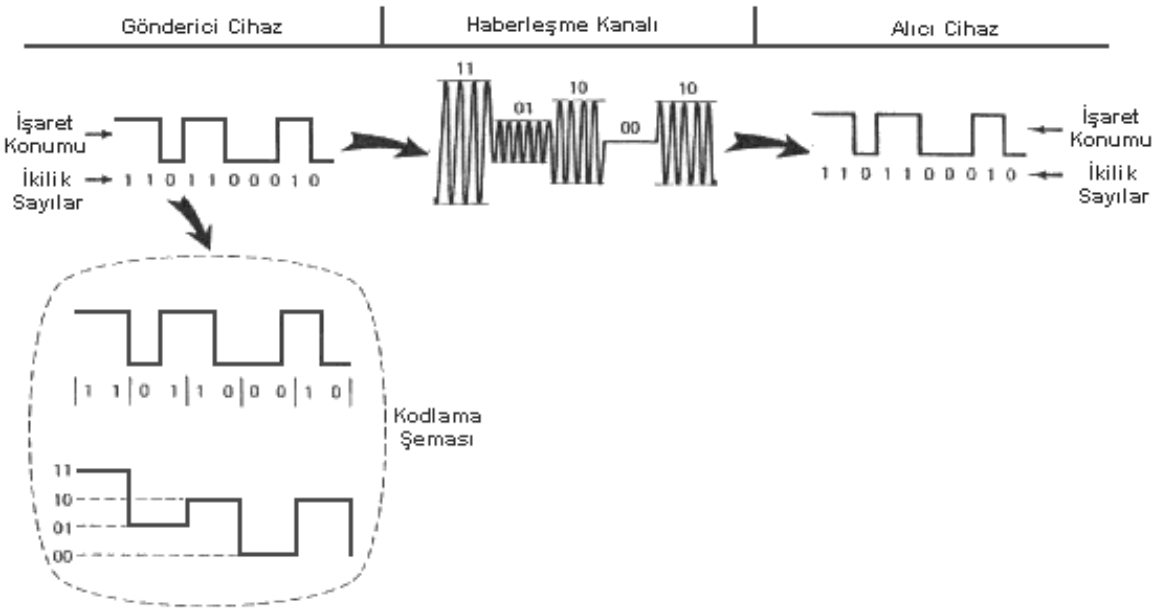
Şekil 1-1'de, verinin gönderici cihazdan çıkışı, haberleşme ortamından geçişi ve alıcı cihaza gelişi görülmektedir. İkilik veri kodu, terminaller ve çıkışlarda on tabanına çevrilirek gösterilir.

Saniye başına bit (bit/sn) terimi iletim hızını belirtmek üzere kullanılır. Bu terim haberleşme yolu veya parçası üzerinden saniyede iletilen bit sayısını verir. Örneğin 2400 bit/sn'lik bir hat, bir sayı veya karakteri belirtmek için 8-bit'lik kodlar kullanıyorsa, saniyede iletilen karakter sayısı 300 (2400 / 8) olur. Haberleşme hızı genelde bit/sn oranı ile verilir.

1.1.1 İletim Karakteristikleri

Veri haberleşmesini anlamak için, elektriğin iletim karakteristikleri hakkında genel bir bilgiye sahip olunmalıdır. Hat kapasitesi, hata kontrol teknikleri, haberleşme yazılımı, ve diğer pek çok ağ bileşeni elektriğin yapabildikleri ve sınırlamaları çerçevesinde analiz edilir ve tasarlanır.

Şekil 1.1'den de görüldüğü gibi veri, haberleşme kanalı üzerinden elektrik işaretinin değişimleri ile iletilir. Bu değişimler 1 ve 0'ları gösterir. Elektrik işaretinin konumu kendini ya bir işaret seviyesi ya da bir başka kompleks elektrik işareti şeklinde gösterir. Bir işaretin iletim yolu üzerindeki hareketine işaret yayılması denir. Bir kablo yolu üzerinde, işaret yayılması elektrik akımı şeklindedir. Bilgisayar siteleri arasındaki radyo transmisyonu ise, havada elektromanyetik dalga olarak yayılan elektrik işaretlerinin algılanması ile başarılır.



Şekil 1.1 Verinin İletilmesi

Tüm maddeler temel parçaların bileşiminden oluşur. Bu parçalar elektriksel yük taşıyabilirler. Bu parçalardan bazıları, sırası ile negatif ve pozitif polarizasyonlu elektronlar ve protonlardır. Bu parçalar belli bir düzende birleşerek atomları oluştururlar. Negatif ve pozitif atomlar birbirlerini çekerek atomun kararlığını sağlarlar. Elektrik akımı haberleşme yolu veya iletkeninin bir ucundan elektrik yükü girişi ile sağlanır. Örneğin, iletkenin gönderici ucuna negatif yük yerleştirirsek, bu yük yoldaki

negatif yüklü elektronları diğer uca itecek ve bir akım oluşacaktır. Esasen, elektrik akımı, dolayısıyla bir veri haberleşme işareti, bu elektronların iletken yol üzerindeki hareketleridir [1].

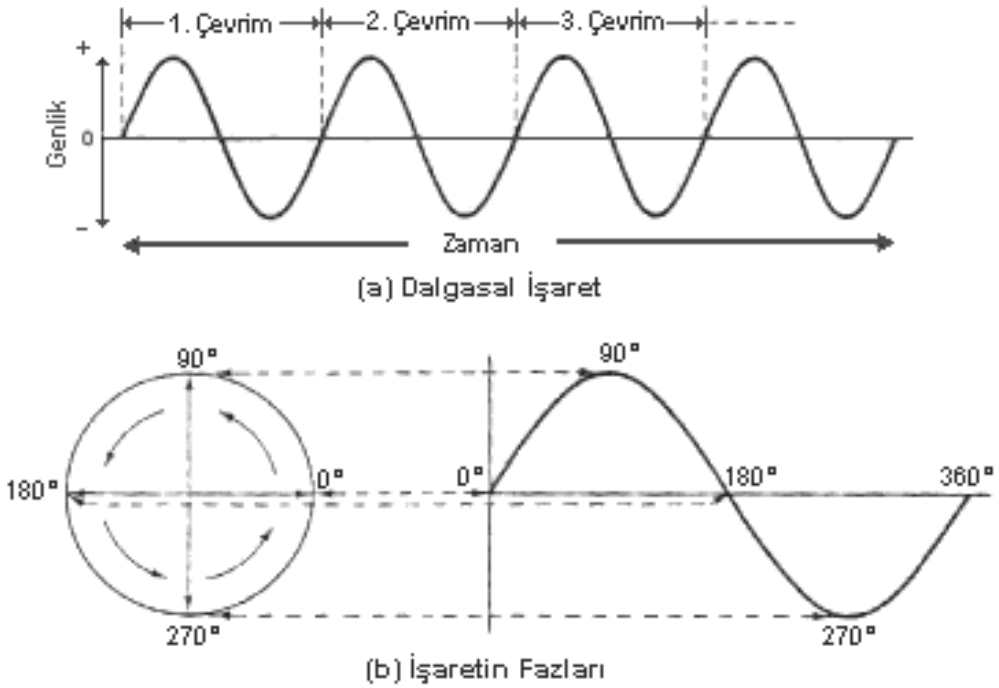
Haberleşme kanalındaki birçok işaret Şekil 1.1 ve Şekil 1.2(a)'da görüldüğü gibi salınım yapan dalga şekilleri içerir. Bilgisayar verilerinin taşınmasını sağlamak için salınım yapan işaretlerin üç parametresi değiştirilebilir (genlik, frekans, faz). Genlik veya gerilim kablo üzerine düşen elektrik yükü miktarı ile belirlenir. Şekil 1.1'den bu gerilimin ikilik konumlara (1 veya 0) bağlı olarak yüksek veya düşük olduğu durumlar görülmektedir.

Elektriğin bir diğer karakteristiği watt birimi ile ölçülen güçtür. İşaret gücü, işaretin bir kablolu haberleşme devresinde gidebileceği veya yayılabileceği mesafeyi belirler.

Baud terimi de veri haberleşmesinde sıkça kullanılır. Bu terim hat üzerindeki işaretin değişme oranını tanımlar. Bunu işaret hızı olarak da açıklayabiliriz. Örnek olarak, Şekil 1.1'deki gönderici cihaz bitleri ikili gruplar halinde toplamakta (00,01,10,11) ve bunlardan her bir grup için farklı genliklerde salınım yapan dalga şekilleri elde etmektedir. Bu örnekte, bit transfer oranı baud'un (ya da işaret değişme oranının) iki katıdır. Günümüzde kullanılan modemler her bir baud için 8-bit oranlarına kadar çıkarak daha büyük bir işaret transfer kapasitesine ulaşırlar.

Şekil 1.1'de görülen işleme modülasyon denir. Bu terim veri katarının haberleşme yolu için değiştirilmesi veya modüle edilmesi anlamındadır.

İşaret aynı zamanda frekansından, başka bir deyişle belli bir zaman aralığında yaptığı tam salınım sayısından tanınır. Frekans saniye başına yapılan salınım sayısı ile ölçülür. Elektrik endüstrisinin tanımladığı 1 Hz birimi, saniyede bir salınım demektir.



Şekil 1.2 Salınım Yapan İşaret

Frekansı tanımlamak için kullanılan bir başka terim birim saniyedeki çevrim sayısıdır (cps: cycles per second). Dalganın frekansının, genliği ile ilgisi yoktur. İşaretler genlik ve frekansın değişik kombinasyonlarına sahip olabilirler. Genlik işaret seviyesini ve negatif veya pozitif gerilim değerini belirtirken frekans, işaret salınım oranını (Hz birimi ile) belirtir.

İşaretin fazı, işaretin çevrimine ne kadar ileriden başladığını tanımlar. Şekil 1-2(b)'de işaretin fazı; başlangıç (0°), ¼ çevrim (90°), ½ çevrim (180°), ¾ çevrim (270°) ve tam çevrim (360°) noktalarında gösterilmektedir. Dalga, şekilde görüldüğü üzere, sinüs dalgasında veya bir çemberde olduğu gibi dereceler ile de etiketlenebilir. Sinüs dalgası denmesinin sebebi, dalganın trigonometrik sinüs fonksiyonunda olduğu gibi değişim göstermesindendir. Sinüs dalgası, çembersel hareketten üretilmiştir. Elektrik işaretlerinin trigonometri kullanılarak tanımlanması mühendisler için çok değerlidir.

Bir yoldaki veri işaretinin bilgi oranı kısmi olarak işaretin genlik, frekans (veya frekanslar) ve fazına bağlıdır. Şekil 1.1'den görüldüğü gibi bilgi oranı (bit/sn), işaretin hangi sıklıkta durum değiştirdiğine bağlıdır. İşaretin genlik, frekans ve fazındaki değişiklikler hat üzerinde bir durum değişimi oluştururlar. Bu değişim 0'ı 1'e veya 1'i

0’a çevirir. İkilik 1’ler ve 0’lar, hat üzerinde bilgisayarlar arası akan, kullanıcı veri mesajlarındaki karakter ve harfleri temsil etmek üzere kodlanırlar.

1.1.2 Analog İletim

Yukarıda bahsedilen işarete analog işaret denir çünkü sürekli yani ayrık olmayan bir karakteristik gösterir. Bu şekildeki bir iletim, bilgisayarlarda kullanılan ayrık ikilik sayıların iletimi için tasarlanmamıştır. Geniş bir kullanım alanına sahip olmasının nedeni, ilk zamanlarda veri haberleşme ağları geliştirilirken analog kolaylıklar sağlayan telefon sisteminin halihazırda mevcut olmasıdır.

Telefon hattı, analog bir doğası olan sesi taşımak için tasarlanmıştır. İnsan sesi analog dalga şeklinde çıkar. İşaretler hava basıncının değişmesi ile salınım yapan örneklerdir. Bu mekanik titreşimler telefon mikrofonu tarafından hissedilir ve elektriksel gerilim örneklerine çevrilir.

Analog ses işareti ve dönüştürüldüğü elektriksel işaret tek bir frekansta değildir.Bir başka ifadeyle ses ve onun telefon hattındaki elektriksel karşılığı, birçok farklı frekanstaki dalga şekillerini içerir. Bu frekansların belirli bileşimleri sesi ve sesin perdesini tayin eder. Doğadaki bir çok olay farklı frekansların bileşimi ile meydana gelir. Örneğin, gökkuşağındaki renkler farklı ışık dalgası frekanslarından, müzik sesleri yüksek veya alçak perdelerin oluşturduğu farklı akustik frekanslardan oluşur. Bu olaylar frekans bandları veya aralıkları içerirler.

İnsan kulağı 40 Hz ile 18000 Hz arası sesleri algılayabilir. Telefon sistemi bu frekans bandının tümünü iletmez. Tam aralık, ses işaretini alıcıda oluşturmak için gerekli değildir. Ekonomik nedenlerden dolayı telefon hatlarında 300 Hz ile 3300 Hz bandı iletilir (tam aralık biraz daha fazladır). Bu nedenle telefonla yaptığımız konuşmalarda sesimiz doğal halinden farklıdır.

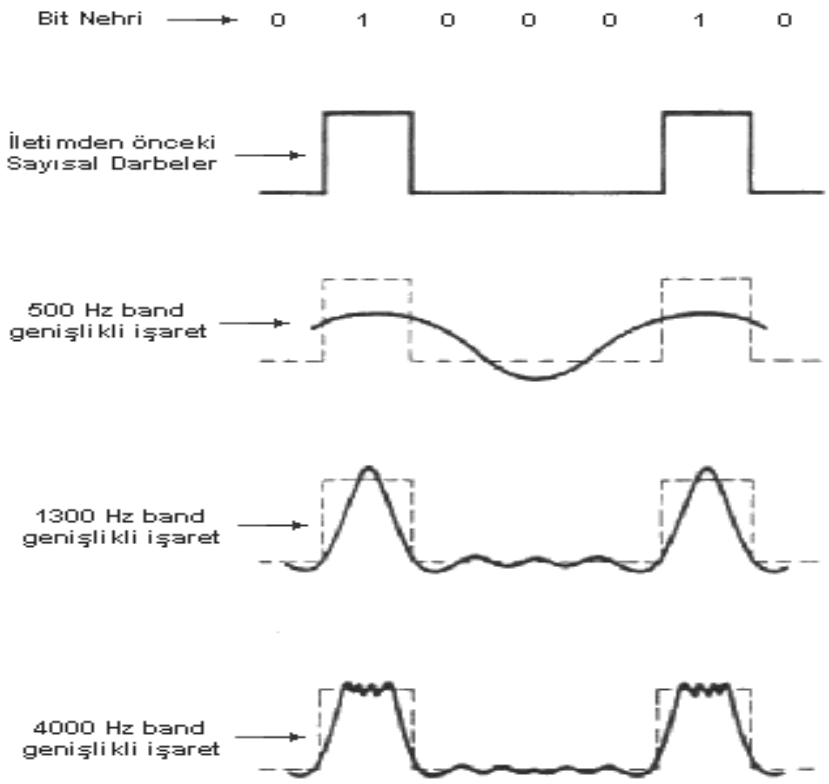
1.1.3 Band Genişliği

Bir haberleşme hattının taşıyabildiği frekans aralığı, hattın band genişliği olarak tanımlanır. Band genişliği veri haberleşmesi için çok önemli bir etkendir çünkü haberleşme hattının kapasitesini (bit/sn), hattın band genişliği belirler. Eğer telefon kanalının band genişliği 3 kHz ’den (300-3300 Hz) 20 kHz ’e çıkarılsaydı, kanal sesin

tüm karakteristiğini taşıyacaktı. Bu, aynı zamanda iletilen verinin doğruluğunu arttırır. Daha büyük band genişliği kullanılarak daha iyi bir veri iletim oranı sağlanacağı açıktır.

Band genişliğinin etkileri Shanonon, Fourier ve Nyquist gibi bilim adamları tarafından saptanmıştır. Fourier, periyodik işaretlerin sinüzoidal fonksiyonların toplamı biçiminde elde edilebileceğini göstermiştir. Periyodik olmayan fonksiyonlar da bazı koşullar altında bu şekilde elde edilebilir. Böylece elde edilen toplama Fourier serisi denir[1]. Şekil 1-3'te hattın durumu saniyede 2000 kez değişmektedir; başka bir söyleyişle işaret değişme oranı 2000 baud'tur. 500 Hz ile sınırlı bir band genişliği işaretin doğru olarak algılanması için yeterli olmaz. Band genişliği büyüdükçe sayısal seviyeler daha doğru bir biçimde ortaya çıkacaktır.

Daha büyük band genişliği, daha yüksek hat kapasitesi demektir. Bu durum, Tablo 1-1'in incelenmesi ile anlaşılabilir. Elektromanyetik frekans spektrumu aralıkları göreceli olarak sınırlıdır. Bu aralık, ses frekans bandından başlar, X-ışını veya kozmik ışık bandına kadar sürer. Yüksek frekansların önemi, ses frekans spektrumu ve mikrodalga veya koaksiyel kablo iletim ortamları incelenerek anlaşılabilir. 1 kHz ve 10 kHz arası band genişliği 9 kHz'dir ki bu hemen hemen 3 kHz'de ses taşıyan hatların 3 katıdır. 10 MHz ile 100 MHz arası (HF ve VHF spektrumu) band genişliği 90 MHz'dir ki bu da teorik olarak ses-sınıfı hattın 30000 katına eşdeğerdir. Bu küçük örnek, haberleşme endüstrisinin daha büyük band genişliği kapasitesi için niye yüksek radyo frekanslarını kullanan teknolojilere yöneldiğini göstermektedir.



Şekil 1.3 Band Genişliğinin Etkisi

Tablo 1-1 Frekans Spektrumu

Yaklaşık Frekans	İsim	Kullanım Yeri
10^3	—	Telefon sesi frekansları
10^4	VLF	Yüksek-hızlı modemlerdeki ses frekansları
10^5	LF	Koaksiyel denizaltı kabloları; bazı yüksek-hızlı batch veri transferleri
10^6	MF	Kara koaksiyel kabloları; AM radyo yayınları
10^7	HF	Kara koaksiyel kabloları; kısa-dalga radyo yayınları
10^8	VHF	Kara koaksiyel kabloları; VHF ses ve TV yayınları
10^9	UHF	UHF TV yayınları
10^{10}	SHF	Kısa-link dalga-kılavuzları; mikrodalga yayın
10^{11}	EHF	Sarmal dalga-kılavuzları
10^{12}	—	Kızılötesi iletim
10^{13}	—	Kızılötesi iletim
10^{14}	—	Fiber optikler; görünür ışık
10^{15}	—	Fiber optikler; morötesi
10^{19}-10^{23}	—	X-ışınları ve gamma ışınları

1.1.4 Periyot ve Dalga Boyu

Bir çevrim için gereken süreye periyot denir. Örneğin, 2400 Hz'deki bir işaret, 0.000416 sn'lik bir çevrim periyoduna sahiptir (1 sn / 2400 = 0.000416 sn). Periyot (T), 1/F olarak hesaplanır ki burada F frekanstır (Hz).

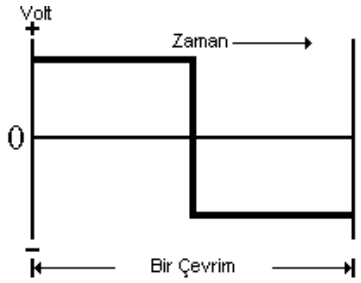
$$WL = S / F \qquad (1\text{-}1)$$

WL : Dalga boyu
S : İşaretin yayılma hızı
F : Frekans

İşaretin dalga boyu ağ cihazı seçiminde, protokol tasarımında ve cevap-zamanı analizinde çok önemlidir[2]

1.1.5 Diğer Dalga Şekilleri

Çok yaygın olan diğer bir yaklaşım da ikilik değerleri simetrik kare dalga kullanarak iletmektir (Şekil 1-4). Kare dalga pozitif polarizasyondan negatif polarizasyona anlık sürede geçen bir gerilimi gösterir. Kare dalga, sayısal veri iletimi için mükemmel bir şekildir, çünkü ikilik durumlar olan 1 ve 0'ları, pozitif ve negatif değerler ile gösterebilir[1].



Şekil 1.4 Kare Dalga

1.1.6 DC İşaretler

Bir çok haberleşme sistemi analog (AC) iletim kullanmaz. Doğru-akım (DC) iletim, daha basit bir yaklaşımdır. DC işaretler, yalnızca ayrık 1'ler ve 0'ları gösterebilen simetrik kare dalgaya benzerler. Ancak DC iletici, salınım yapan dalga şekli yerine, açık-kapalı elektrik enerjisi darbelerini kullanır. Ek olarak, DC işaret olduğu gibi iletilir,

üzerine başka işaret veya frekans bindirilmez. Bir AC işaret, başka frekanslar tarafından taşınmak üzere (yeterlilik, hız ve iletim mesafesi etkenleri yüzünden) yeniden şekillendirilir. Bu işaret şekillendirilmesi modülasyon olarak anılır. Bir çok sistem sınırlı bir mesafede çalıştığı için daha güçlü ve daha pahalı olan AC iletime ihtiyaç duymaz, bunun yerine DC işaretleşmeyi kullanır. Sinüzoidal dalga şekli, simetrik kare dalga gibi, uzak mesafe veri haberleşme hatları için gerekli iletim tipidir. Sayısal bit katarları hem DC hem de AC işaretlerle taşınabildiği halde, uzak mesafe iletiminde AC işaretler kullanılır.

Telgraf, DC işaretleşme için iyi bir örnektir. Telgraf cihazının düğmesi bir anahtardır ve operatör tarafından basılınca devreyi kapayarak hattın gönderici ucuna bir gerilim düşürür. Gerilim, hat üzerinde bir akım oluşturur ve alıcıda darbe olarak algılanır. Alıcı, akım darbesini kısa, duyulabilir bir tona çevirir. İlk sistemlerde iletilen akım, alıcı tarafta pille beslenen bir elektromıknatısla aktif edilmekteydi. Elektromıknatıs gelen işarete göre anahtarı çeker veya iterdi (devreyi kapar veya açardı). Bu yapıda çalışan bir anahtarlama cihazına röle denir. Anahtarın mekanik hareketi ile, duyulabilir tıklamalar üretilirdi ve bu tıklamalar bir kod deseni oluştururdu. Anahtarın basılma süresi meşhur Morse Kodu'nun nokta ve çizgilerini belirlerdi.

1.1.7 İletim Sığası, Hız ve Gecikme

Bir haberleşme sisteminin iletim sığası (kapasitesi) bit/sn olarak gösterilir. Bilgisayar üzerinde çalışan kullanıcı uygulamaları için cevap süresi ve veri akışı, sistemin sığasına bağlıdır. Örneğin; 4800 bit/sn'lik hat, 2400 bit/sn'lik hattın iki katı sığaya sahiptir. Bu da arttırılmış bir akış ve daha kısa bir cevap-süresi sağlar. Belirli sınırlar dahilinde bu gerçekten başarılabilir. Ancak haberleşme sistemlerinde kısıtlamalar vardır ve bunlar iletim oranlarına sınırlarlar.

Telefon ağı ses taşımak için üretilmiştir ve düşük band genişlikli işaretlerle çalışır. Yeterli ses kalitesi 3 kHz'lik bir frekans spektrumu gerektirir. Ses-sınıfı devrelerin frekans spektrumu, yüksek bit/sn oranlarının iletimini gerçekleştiremez.

Band genişliği, işaret gücü ve iletken üzerindeki gürültü, iletim sığasını sınırlayan etkenlerdir. Gerçekten de arttırılmış bir işaret gücü hat sığasını arttırır ve aynı zamanda

daha uzak mesafelere işaret yayılımı yapılabilmesini sağlar. Ancak aşırı güç, sistemdeki parçalara zarar verebilir ve/veya ekonomik olarak karşılanamayabilir.

Hattaki gürültü problemi hattın tabiatında olan ve ortadan kaldırılamayan bir problemdir. Gürültü (Termal, Gaussian, beyaz veya arka plan gürültüsü), elektronların iletken üzerindeki sabit, rasgele hareketlerinden meydana gelir ve kanal sığasına bir sınırlama getirir. Telefon hatlarında işittiğimiz ıslığa benzer ses böyle bir gürültüdür. Tüm elektrik iletkenleri birer gürültü kaynağıdır. Gürültü gücü, band genişliğe ile doğru orantılıdır, yani band genişliğini arttırmak ek gürültüye yol açacaktır. Eklenen gürültüyü azaltmak için süzme olarak bilinen bir elektronik teknik kullanılır.

Haberleşmenin temel kanunlarından biri Shannon Kanunu'dur. Shannon bir iletim yolunun sığasını aşağıdaki formülle göstermiştir:

$C = W \log_2 (1+S/N)$ (1-2)

C = bit/sn olarak maksimum sığa, W = Band genişliği,
S/N = İşaret gücünün (S) gürültü gücüne (N) oranı

Bir kanal üzerinden gönderilebilecek maksimum bilgi miktarı 'kanal sığası' olarak adlandırılır. Formül incelendiğinde W'yi arttırmanın, işaret gücünü arttırmanın veya gürültü seviyelerini düşürmenin müsaade edilen bit/sn oranını arttıracağı görülebilmektedir. 1000'e 1 S/N oranı olan bir ses-sınıfı hattın müsaade edebileceği maksimum sığa 25900 bit/sn'dir. Shannon kanunu ile bulunan teorik limit, pratikte daha düşüktür. İletimde oluşan hatalar nedeniyle Shannon kanunu tam sınırları ile kullanılamaz. Örneğin; 25900 bit/sn oranı o kadar küçük bir zaman ister ki (1 sn/25900 = 0,00004 bit zamanı) hattaki ufak bir kusur bile bitlerin bozulmasına neden olabilir. İşaret konumunun kendi başına 1 bitten fazlasını göstermesi sağlanarak, yani baud değeri arttırılarak Shannon kanununun zorlamaları hafifletilebilir.

S/N oranını yükseltmek için kullanılan bir yöntem, hatta daha çok işaret yükselticisi koymaktır. İşaret hatta ilerlerken, yükselticiler tarafından periyodik olarak güçlendirilir. Hat boyunca gürültü sabit olduğundan, yükselticiler işaret gücünün belli bir seviyenin altına düşmemesini sağlayacak yeterli aralıklarla yerleştirilmelidir. Ancak yükselticilerin sık aralıklarla yerleştirilmesi S/N oranını arttırırken, aynı zamanda oldukça masraflı olur. Dikkat edilmesi gereken bir nokta da, yükselticilerin dikkatli bir

biçimde tasarlanarak işaretle birlikte yükseltilen gürültü oranının en düşük seviyede tutulmasını sağlamaktır.

Tablo 1-2 İletim Gereksinimleri

İletim Tipi	Tipik Bit sayısı	9.6 kbit/sn ile iletim zamanı (sn)
Bir sayfa veya tam CRT ekranı metin (sıkıştırılmamış)	$1\text{-}4 \times 10^4$	1-4
Fotokopi resim, siyah beyaz, iki-ton (sıkıştırılmamış)	$2\text{-}6 \times 10^5$	20-60
Tam sayfa, renkli resim, yüksek kaliteli (iyice sıkıştırılmış)	$2\text{-}10 \times 10^6$	200-1000
20 cm floopy disk, tek-yönlü, double-density	5×10^6	500
720-m bilgisayar tape makarası (6250 BPI tipi) veya iki orta-büyüklükte disk ünitesi (IBM 3310)	1×10^9	100,000 (29 saat)
PCM olarak kodlanmış bir saniyelik telefon konuşması	6.4×10^4	7
PCM olarak kodlanmış bir saniyelik telefon konuşması (iyice sıkıştırılmış)	2.4×10^3	0.25
Bir saniyelik hareketli video resmi	6.3×10^6	660

Sayısal iletim tekniği kullanılarak bir devrenin gerçekten de 25.9 kbit/sn oranından çok daha büyük işaret oranlarını taşıyabilmesi sağlanabilmektedir. Ancak sayısal iletim daha büyük band genişliği ve daha sık aralıklar ile sayısal tekrarlayıcıların (analog yükselticinin sayısal eşdeğeri) kullanılmasını gerektirir. Sayısal iletim için yüksek bir S/N oranı gerekmez çünkü Shannon kanunundan görüldüğü gibi, göreceli olarak, band genişliğindeki küçük bir artma, S/N oranındaki çok daha büyük bir azalma ile karşılanabilir.

Günümüzde, farklı hat hızlarını destekleyen, geniş bir fiyat yelpazesine sahip ürün seçeneklerinin sayısı hızla artmaktadır. Seçim, kaçınılmaz olarak kullanıcı ihtiyacı ve bu ihtiyacın karşılanması için gereken maliyete göre yapılır. Tablo 1-2'de, bazı bulunabilir iletim hız aralıkları ve bunları kullanan tipik kullanıcı uygulamaları görülmektedir. Görüldüğü gibi çok geniş bir seçenek aralığı mevcuttur, ve kbit/sn mertebelerindeki iletim oranları birçok iletim tipi için uygun olmamaktadır.

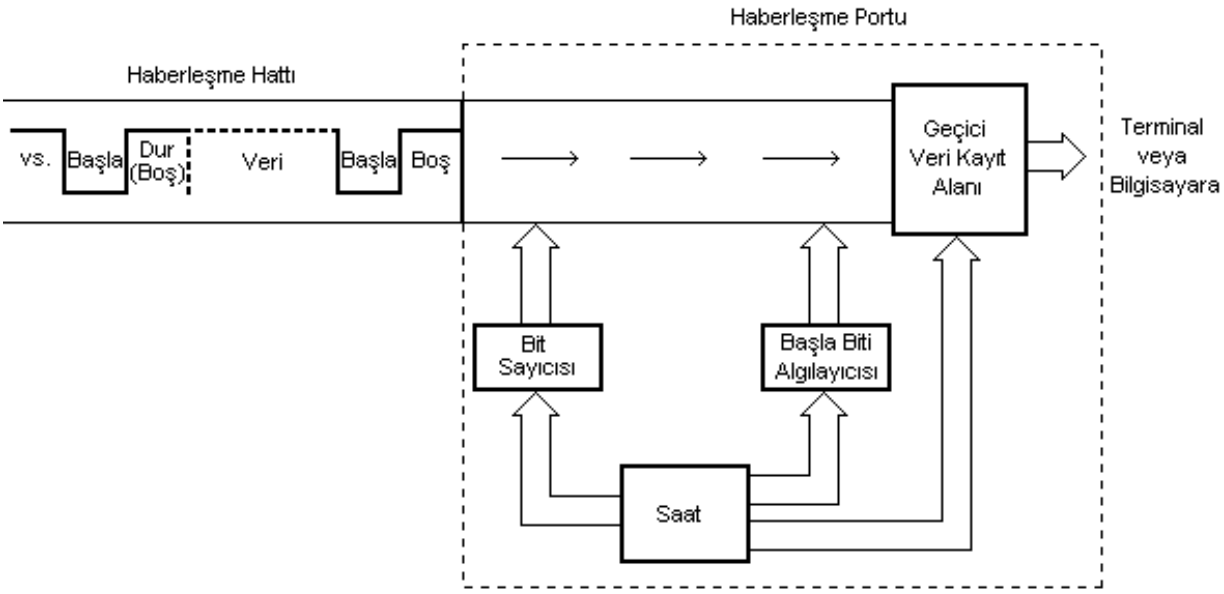
İşaretin iletim veya yayılma gecikmesi, mühendis ve kullanıcılar için göz önüne

alınacak bir başka konudur. Yayılma gecikmesi; kullanılan devrenin türü, alıcı ile verici arasındaki ara noktaların sayısı ve bu noktaların türü gibi çeşitli etkenlere bağlıdır. Yaklaşık olarak koaksiyel kablo ve mikrodalga yolları üzerindeki iletim, 130,000 mil/sn hızındadır. Ancak, işaretin hızı frekansa bağlı olarak değişir. Örneğin, tipik bir telefon hattı (19 gauge) 10 kHz'de yaklaşık 110,000 mil/sn hızında ve 50 kHz'de 125,000 mil/sn hızında çalışmaktadır. Frekans ve kablonun belirli elektriksel karakteristikleri nedeniyle bu hızlar hattın teorik hızı olan 186,000 mil/sn'den daha yavaş olmaktadır. Mesaj ağ üzerinde ara istasyonlara girip çıkarken ek ve önemli gecikmeler meydana gelebilir. Ancak öncelikli iletim gecikmesi, hattın kendinden kaynaklanmaktadır. Anahtarlar ve bilgisayarlar gibi ara parçalar gecikmeye sebep verseler de, genelde çok yüksek hızlarda çalışırlar (nanosaniyeler veya saniyenin milyarda biri mertebelerinde). Tabii ki, bu istasyonların mesajları disk veya teyplerine saklamaları durumunda göz önüne alınması gereken ek gecikmeler meydana gelebilir.

1.2 Eşzamansız ve Eşzamanlı İletim

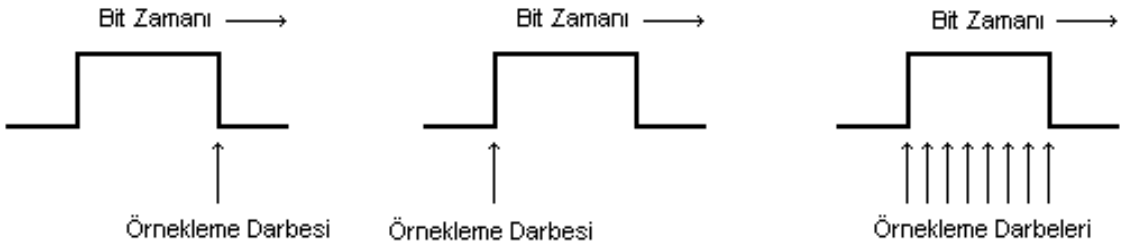
Şekil 1-5'te basit bir iletim süreci gösterilmiştir. İletilen bitler birbirlerini tam olarak eşit zaman aralıkları ile izlemektedirler ve alıcı taraftaki algılama ve zamanlama mekanizmaları ile ölçülmektedirler. Başla biti, veri karakterinin önünde gelir ve alıcı tarafa verinin yolda olduğunu belirtir (başla bitinin algılanması). Başla biti gelmeden önce yol veya hat 'boştur' denir ve bir başla biti gelene kadar hat boş konumunda kalır. Boş konumda kaldığı sürece, hat akım çeker. Bu seviyeden düşük işaret seviyesine geçiş; alıcı cihazdaki örnekleme, sayma ve veri biti katarı alıcısı (bit sayıcısı) mekanizmalarını başlatır. Veri bitleri akım varsa mark (ikilik 1), akım yoksa space (ikilik 0) olarak algılanır.[2]

Kullanıcı veri bitleri, register veya tampon (buffer) gibi geçici bir saklama alanına aktarılır. Daha sonra da bu bitler işlenmek üzere bilgisayara veya terminale aktarılır. Dur biti, bir yada daha fazla mark işaretinden oluşur ve alıcı tarafa (eski cihazlarda) sıradaki karakter için mekanizmasını hazırlayacak bir zaman aralığı sağlar. Dur bitinden sonra işaret boş seviyesine geçer ve sıradaki karakterin 1-0 geçişi ile başlamasını garanti eder. Eğer önden gelen karakter hep 0'lardan oluşursa ve dur biti, gerilim yüksek veya boş seviyeye alınarak gösterilmezse, başla biti algılayıcısı şaşıracaktır.



Şekil 1.5 Eşzamansız İletim Süreci

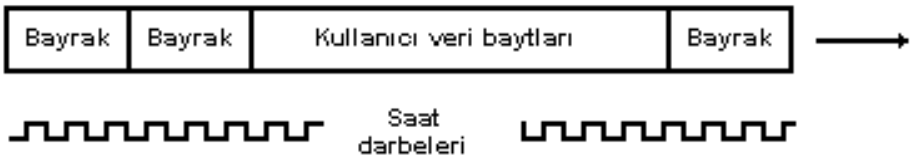
Alıcı ve verici arasında sürekli bir eşzamanlama olmadığı için bu haberleşmeye eşzamansız iletim denmektedir. Bu iletim veri karakterinin, ön bir zamanlama işaretine bakılmaksızın, herhangi bir anda iletilebilmesini sağlamaktadır. Zamanlama işareti veri işaretinin bir parçasıdır. Eşzamansız iletim genelde yazıcılarda ve düşük hızlı bilgisayar terminallerinde kullanılır. Birçok kişisel bilgisayar eşzamansız iletimi kullanır. Eşzamansız iletimin avantajı basit olmasıdır.



Şekil 1.6 Bit Örnekleme

Saat cihazı bir veri haberleşme sisteminin en önemli unsurlarından biridir. Kullanılma amacı, hat üzerinde önceden tanımlanmış işaret seviyelerinin varlığını veya yokluğunu sürekli olarak incelemek ve örneklemektir. Ayrıca tüm iç parçaların eşzamanlamasını sağlamaktadır. Saatin hızı, bir saniyede ürettiği darbe sayısı ile belirlenir. Şunu da not edelim ki saat, sistemi oluşturan diğer elemanlara da bağlanarak tüm elemanların tutarlı bir biçimde zamanlamasını sağlar.

Gerçekte, örnekleyici saat haberleşme hattını gelen veriden daha hızlı bir oranda örnekleme işlemini gerçekleştirir. Örneğin; veri 2400 bit/sn'de gelirken zamanlama mekanizması belki de saniyede 19,200 kere (gelen işaretin 8 katı) örnek almaktadır. Daha sık örnek almak, alıcının 1-0 ve 0-1 geçişlerini daha erken algılamasını sağlar. Bu sayede alıcı ve verici cihaz daha yakın bir eşzamanlılıkta tutulmaktadır. Örnekleme hızının önemi Şekil 1.6'da açıkça görülebilmektedir. 2400 bit/sn hızındaki bir hatta bit zamanı 416 msn olur. Saniyede yalnızca 2400 örnek alınırsa bitin başlangıcında ve sonunda bitten örnek alınabilir. Her iki durumda da bit algılanmaktadır. Ancak, bir işaretin hafifçe değişmesi ve hat üzerinde daha kısa veya daha uzun bir süre bulunması muhtemeldir. Yavaş bir örnekleme oranı hat üzerindeki durum değişimini doğru zamanda örnekleyemez ve işaret sürüklendikçe, bitler alıcı istasyondan doğru olarak alınamaz.



Şekil 1.7 Eşzamanlı İletim Süreci

Daha etkin bit yöntem olan eşzamanlı iletimde, alıcı ve verici istasyonlarda ayrı zamanlama işaretleri vardır. Şekil 1.7'de eşzamanlı iletim şeması görülmektedir. Bu yöntemle veri, kontrol bitleri arasına yerleştirilmektedir. Bu bitlere genelde bayrak (flag) denir. Bunlar alıcıya mesajın geldiğini haber verirler. Kısa mesafeli devrelerde cihazlar arası zamanlama işaretlerini sağlamak üzere ayrı bir kanal kullanılabilir.

Eşzamansız iletimde olduğu gibi, alıcı cihaz bayrak bitlerini arar, ancak yerel olarak zamanlama işareti üreterek, gelen işareti ne zaman ve ne sıklıkta örnekleyeceğine karar verir. Zamanlama işareti, alıcıdaki ve vericideki zamanlama cihazlarının eşzamanlamasını sağlar. Cihazlar arasında eşzamanlama bir kez sağlandı mı artık cihazlar bu konumda kalırlar. Saatler biraz kayabilir, fakat sıradan osilatör saatleri 1/100,000 çözünürlükte çalışırlar. Yani bu osilatörler 100,000 sn süresinde 1 sn şaşırmaktadırlar. Böylece saniyede 2500 kez örnekleme yapan bir osilatör belirli saniyeler boyunca eşzamanlı kalmaktadır. Eşzamanlama için kullanılan bir başka

yöntem de, özel kodlar ile periyodik aralıklarla eşzamanlamayı yeniden sağlamaktır. Bu kodlara zamanlama kodları denir.

Alıcı, bayrağı kullanıcı verisinden ayırabilmelidir. Üreticiler bu işareti, farklı bit katarları kullanarak belirtirler. Yaygın bir yaklaşım bir bayrağı göstermek için 8 bitlik 01111110 değerini kullanmaktır.

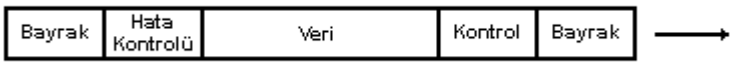
1.3 Temel Terimler ve Kavramlar

1.3.1 Çerçeveler Başlıklar ve Kodlar

Elektrik işaretleri ve bit katarları Şekil 1.8'de de gösterildiği gibi hat üzerinden çerçeveler biçiminde iletilirler. Çerçeve, kullanıcı verisi, kontrol verisi veya her ikisinin birden bulunduğu mantıksal bir birimdir. Bir çerçeve genelde aşağıdaki alanları içerir:

· Kullanıcı verisi: Bir ya da daha çok alanı kapsar. Kullanıcı verisi, bir terminal operatörü tarafından tuş takımı ile veya bir bilgisayar programının çıkışı ile oluşturulur.
· Bayraklar: Bir önceki bölümde izah edilmiştir.
· Adres alanı: Hat üzerindeki alıcı ve vericiyi tanıtmak üzere yegane rakamlar veya harfler içerir.
· Kontrol karakterleri: Çerçevelerin doğru bir sıra ile akmasını sağlarlar.
· Hata kontrol: Başarılı, hatasız bir iletim yapılıp yapılmadığını öğrenmek için kullanılırlar.

Bit katarları, karakterleri özel kod kümelerine dayanarak belirtirler. Günümüzde birçok kod çeşidi mevcuttur. Veri haberleşmesinde kullanılan eski kodlar telgraf iletimi için tasarlanmıştır. Örneğin; Morse kodunda noktalar ve çizgiler vardır ve belirli dizilişlerle karakterleri, sayıları ve özel karakterleri belirlerler. Nokta ve çizgiler, telgraf operatörünün ileticinin düğmesine basma süresine göre oluşur.



Şekil 1.8 Eşzamanlı İletimde Kullanılan Tipik Çerçeve Formatı

1970'lerin başlarında, endüstri tarafından bir çok 5-bitlik kod geliştirildi. Modern sistemlerde kullanılmamasına rağmen Baudot kodu bugün dahi kullanılan bu 5-bitlik kodlardan biridir. Bir çok kod Morse ve Baudot kodlarından türetilmiştir. Bugün en yaygın kullanıma sahip kodlar EBCDIC (Extended Binary Coded Decimal Interchange Code) ve ASCII (American National Standart Code for Information Interchange) kodlarıdır. EBCDIC, IBM mimarisinde yaygın olarak kullanılmaktadır. EBCDIC, 8-bit ikilik bir koddur. Böylece kod kümesinde maksimum 256 karakter bulunabilir. ASCII, veri haberleşmesinde en yaygın kullanılan koddur (Şekil 1-9). Bu kod, 7-bit artı hata-algılama amacı ile eklenmiş bir bitten (toplam 8-bit) oluşur. Kod ilk kez 1963'te geliştirilmiştir[3]

American National Standart for Information Interchange

Bitler				7	0	0	0	0	1	1	1	1
				6	0	0	1	1	0	0	1	1
4	3	2	1	5	0	1	0	1	0	1	0	1
0	0	0	0	NUL		DLE	SP	0	@	P	\	p
0	0	0	1	SOH		DC1	!	1	A	Q	a	q
0	0	1	0	STX		DC2	"	2	B	R	b	r
0	0	1	1	ETX		DC3	#	3	C	S	c	s
0	1	0	0	EOT		DC4	$	4	D	T	d	t
0	1	0	1	ENQ		NAK	%	5	E	U	e	u
0	1	1	0	ACK		SYN	&	6	F	V	f	v
0	1	1	1	BEL		ETB	'	7	G	W	g	w
1	0	0	0	BS		CAN	(	8	H	X	h	x
1	0	0	1	HT		EM	)	9	I	Y	i	y
1	0	1	0	LF		SUB	*	:	J	Z	j	z
1	0	1	1	VT		ESC	+	;	K	[	k	{
1	1	0	0	FF		FS	'	<	L	\	l	:
1	1	0	1	CR		GS	-	=	M	]	m	}
1	1	1	0	SOH		RS	.	>	N	^	n	~
1	1	1	1	SI		US	/	?	O	-	o	DEL

Şekil 1.9 ASCII Kodu

Şekil 1-9'da görüldüğü gibi, bazı 7-bit yapıları birden fazla karakteri göstermektedir. Bazı kodlar haberleşme sistemlerinde kullanılan kontrol işaretlerini gösterir. Haberleşme sistemlerinde farklı kodların kullanımının, uyumsuzluklar yaratacağı açıktır. Bu nedenle farklı kodlara sahip haberleşme cihazlarının birbirleriyle haberleşebilmeleri için kod çevirme paketleri geliştirilmiştir.

1.3.2 Haberleşme Oturumları

Bir ağdaki iki parça arasındaki haberleşme akışına oturum denir. Oturum çeşitli şekillerde olabilir. Örneğin, bir oturum, terminalleri aracılığı ile ağdaki iki operatör arasında, bilgisayarlar arasında, iki yazılım programı arasında veya ağ kontrol programları arasında olabilir. Elbette ki başka oturum şekilleri de mevcuttur. Şekli ne olursa olsun, oturumlar son kullanıcıya hizmet etmek için kurulur. Örneğin bu hizmet, bir terminal operatörü veya uygulama programı için verilebilir[2].

Oturumlar çerçeve başlıklarındaki bilgileri (veya başka parametreleri) kullanırlar. Örneğin; A sitesindeki bir terminal operatörünün yaptığı veri tabanı gönderme isteği mesajında bir başlık bulunmalıdır. Bu başlıkta; B sitesindeki bir adres, veri tabanının yeri veya veri tipi gibi tanımlayıcı bazı bilgileri bulunur. Çerçeve ağ üzerinde giderken, başlığı incelenir ve uygun kaynaklar anlaşılır. Böylece bu kaynaklar servis isteğine tahsis edilir. Günümüzde ileri ağlar, kaynakları sağlamak için haberleşme mantığını katmanlara ayırırlar.

1.3.3 Hat Karakteristikleri

İletim yolu veya hattı, kullanıcılar arası veri alışverişi için gerekli ortamı sağlar. Alışveriş; oturumun kurulmasını, kullanıcı mesajlarının alışverişini ve oturumun sonlandırmasını içerir. Hattın elektriksel özelliklerine ek olarak, diğer karakteristikler de başarıma ve haberleşme sisteminin tasarımına önemli şekilde etki ederler. Bu başlık altında bir haberleşme kanalının aşağıdaki karakteristikleri incelenecektir:

· Uçtan-uca ve çok-uçlu (multi-drop) yapılar
· Simplex, yarı-duplex, duplex düzenlemeler
· Anahtarlamalı ve kiralık hatlar (leased lines)

1.3.3.1 Uçtan-Uca ve Çok-Uçlu Yapılar

Uçtan-uca bir hat iki istasyonu birbirine bağlar (Şekil 1-10a). Çok-uçlu bir hat üzerinde ise ikiden fazla istasyon vardır (Şekil 1-10b). Bu yapılardan birinin seçilmesi çeşitli etkenlere bağlıdır. İlk olarak, uzun süre gerekli olan bir kullanıcı-kullanıcı oturumu gerekli ise, belki de yalnızca uçtan-uca düzenlemesi uygun bir seçim olabilir. İkinci olarak, iki kullanıcı arasındaki trafik hacmi, diğer istasyonların hattı kullanımına engel

olacak ölçüdeyse yine uçtan-uca bir yapı uygun bir seçim olacaktır. Bazı bilgisayar-bilgisayar oturumları ancak uçtan-uca hatla gerçekleştirilebilir. Üçüncü olarak, iki kullanıcı belki de prosese katılacak maksimum sayıdır. Çok-uçlu düzenlemeler genelde düşük-hızlı terminallerin birbirleri ile veya bir bilgisayar ile haberleştiği durumlarda kullanılırlar. Hat, en yüksek verimi elde etmek amacıyla istasyonlar tarafından paylaşımlı olarak kullanılabilir.

Çok-uçlu hatlar, uçtan-uca hatlara göre daha özel kontrollere ihtiyaç duyarlar. Çok-uçlu yoldaki istasyonlar hattın tahsisi ve paylaşımı için denetlenmelidir. Oturumların oluşturulmasına dahili olarak izin verilebilmeli ve daha önemli oturumlara öncelik tanınabilmelidir. Veri bağlantı kontrolleri (data link controls), bu oturumlardaki mesaj akışını kontrol etmekte kullanılır.

1.3.3.2 Simplex, Half-Duplex ve Duplex Düzenlemeler

Bu terimler sık sık birden çok yoruma uğramaktadırlar. Genelde hat üzerinde akan mesaj trafiği konusunda referans terimler olarak kullanılırlar. Daha az yaygın yorum ise iletime katılan fiziksel yolların sayısı ile ilgili olduklarıdır. Aşağıda iki bakış açısı da incelenecektir.

1.3.3.3 Trafik Akışı

Simplex iletim, çerçevelerin yolda ancak bir yönde hareket edebilmelerini sağlamaktadır. Alıcı mesaj gönderemez ve gönderici mesaj alamaz. Radyo yayınları simplex iletime bir örnektir. Simplex düzeni çeşitli uygulamalarda kullanılır. Örneğin, çevresel süzme ve örnekleme sistemleri genelde simplex yapıyı kullanırlar. Burada su veya havadan örneklenen veri, tek yönde ilerleyerek, analizinin yapılacağı bilgisayara gider.

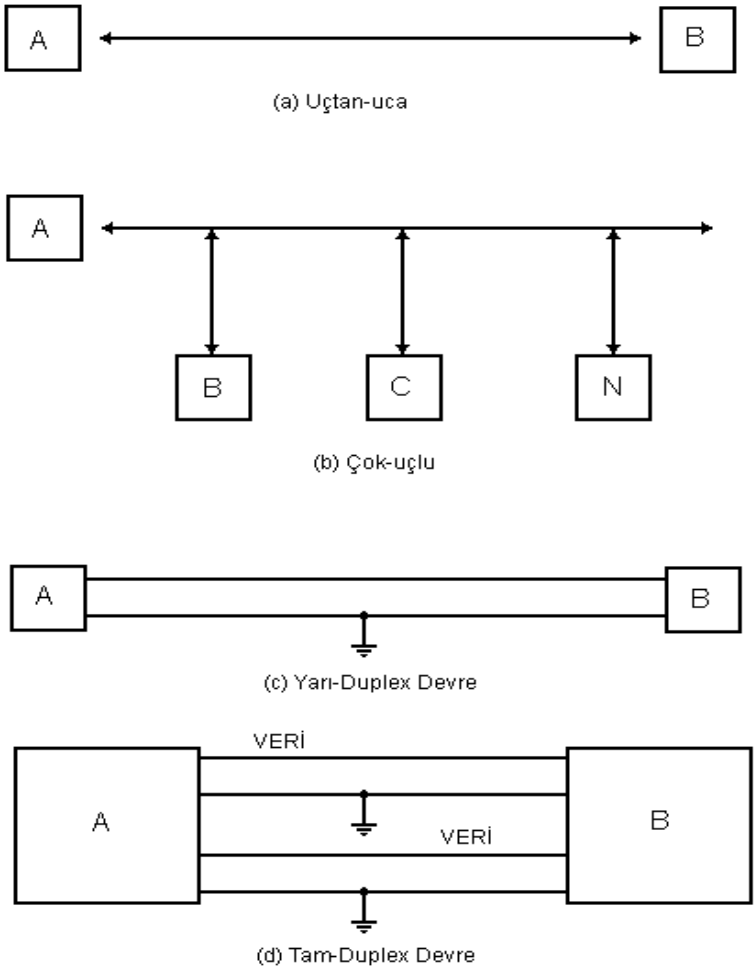
Yarı-duplex iletim verinin hat üzerinde iki yönde de hareket edebilmesini sağlar ancak iletim bir kerede yalnızca bir yönde olur. İnsan tarafından işletilen tuş takımlı bilgisayarlar genelde bu yaklaşımı kullanırlar. Terminal ve diğer istasyon, hattı dönüşümlü kullanırlar; gönderici istasyon bir başka mesaj göndermek için cevap bekler.

Duplex iletim (full-duplex de denmektedir) istasyonlar arasında iki yönlü, eşzamanlı iletime olanak sağlar. Çok-uçlu hatlar sıklıkla bu yöntemi kullanırlar. Örneğin, A istasyonu, trafiğini merkez bilgisayara yönlendirmişken, merkez bilgisayar aynı anda trafiğini B istasyonuna yönlendirebilir. Duplex iletim, oturumlarda iç-izine olanak sağlar ve kullanıcı verisinin birçok istasyon arasında akmasına müsaade eder.

1.3.3.4 Fiziksel Yol

Fiziksel hatlar bazen yarı-duplex ve duplex devreler olarak tanımlanır. Şekil 1-10(c)'de yarı-duplex yapı görülmektedir. Bu yapıda iki adet iletken bulunmaktadır ancak yalnızca bir tanesi mesaj alışverişi için kullanılmaktadır. İkinci iletken devreyi tamamlamak üzere varolan bir dönüş kanalıdır veya bir topraktır. Bu devreye iki-tel devresi demek daha doğrudur[3].

Şekil 1-10(d)'de ise bir duplex devre görülmektedir. Bu durumda dört iletken; iki adet iletim yolu ve iki adet dönüş kanalı sağlamaktadır. Bu devreye de dört-tel devresi demek daha doğru olacaktır. Dikkat edilmelidir ki iki-tel devresinde devre üzerindeki trafik akışı mutlaka yarı-duplex olacaktır denilemez.



Şekil 1.10 Hat Yapıları

1.3.3.5 Anahtarlamalı ve Kiralık Hatlar

Telefon ağı anahtarlamalı hatların kullanımına verilebilecek en güzel örnektir. Anahtarlamalı hatlarda iki site arasındaki çağrı süresince geçici bir bağlantı kurulur. Aynı siteler arası daha sonraki bir çağrı, telefon sisteminin farklı devre ve cihazlarını kullanabilir. Kiralık hat ise iki site arasında kurulan kalıcı bir bağlantıdır. Haberleşme yolunu oluşturmak için çevirmeli bir bağlantı kurmayı gerektirmez. Anahtarlamalı ve kiralık hatların avantajları ve dezavantajları aşağıdaki gibidir:

· Anahtarlamalı hat, bir çağrıyı tamamlamak ve bağlantıyı sağlamak için birkaç saniyeye ihtiyaç duyar. Çevirme gecikmesinin kabul edilemeyeceği durumlarda kullanıcı kiralık hat kullanmalıdır.

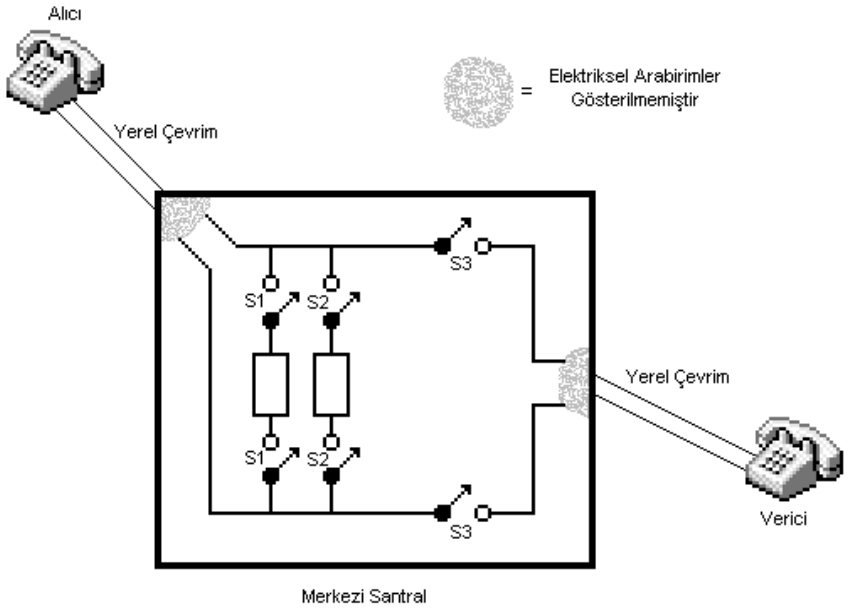
· Kiralık hatlar, daha iyi başarım ve daha az hata sağlayabilirler. Birincisi, kiralık hat donanımları ekranlandırılarak ve uygun ortamlara yerleştirilerek başarımları arttırılabilir çünkü bağlantı donanımları sabittir. İkincisi, bazı anahtarlama sistemleri hat üzerine gürültü yükleyebilmektedir ve gürültü bazen verinin bozulmasına neden olabilmektedir.

· Düşük-hacimli trafiği olan kullanıcılar, kiralık hatların yüksek maliyetleri nedeniyle anahtarlamalı hatları tercih ederler. Bir hat periyodik olarak kullanılacaksa çevirmeli bağlantı yaklaşımı, kiralık hat yaklaşımından daha uygun olacaktır.

· Anahtarlamalı hatlar oldukça esnektir. Kullanıcı bir devreyi kaybederse yalnızca kullandığı ağı yeniden araması (redial) yeterlidir. Bir kiralık hattaki bozulmanın giderilmesi, daha fazla çaba gerektirir ve ek gecikmelere neden olur.

Kiralık ve anahtarlamalı hat seçimi, bir organizasyon için dikkat edilecek çok önemli bir unsurdur. Kiralık veya anahtarlamalı hat kullanmak için mantıklı bir karar vermeden önce önkoşul; trafik hacmi, akış başarımı, tepe yükler, cevap süresi gibi parametrelerin analizini yapmaktır[3]

1.3.4 Telefon Ağının Kullanımı



Şekil 1.11 Bir Çağrının Kurulması

Bu bölümde, telefon sisteminin bir çağrıyı nasıl gerçekleştirdiğine dair bir fikir verilmeye çalışılacaktır.

Şekil 1.11'de yerel telefon ve santrallerde bulunan bazı parçalar gösterilmiştir. Telefonun ahize yükü ile açık tutulan anahtarları (switch hooks-SH) vardır. Ahize 'on hook' konumunda olduğu sürece açık kalan anahtar, telefonun santral ile elektriksel bağlantı kurmasını engeller. Kullanıcı ahizeyi kaldırınca SH anahtarı kapanır. Bu konuma 'off hook' denmektedir. Bu konumda, kapalı SH anahtarı santrale DC akım gitmesini sağlar. Bu akım, merkezi santral tarafından algılanır. Bir bilgisayar veya başka bir cihaz da, bir devre aracılığı ile off-hook sağlayarak santrale çağrı gönderebilir.

Santralde, gelen bölgesel çevrim hatlarını tarayan bir algılayıcı bulunur. Yaklaşık 100 msn'de bir off-hook durumunu algılamak için bir DC akımın hattan akıp akmadığına bakılır.

Merkezi santralde çağrıları kurmak üzere anahtarlar bulunur. Santral bölgesel aboneden gelen DC akım akışını algılayınca S1 anahtarını kapayarak hatta çevir sesi (dial tone) verir ve bu 480 Hz'lik bir işaretin arayan telefona gitmesini sağlar. Abone çevir sesi ile birlikte numarayı çevirmek için uyarılır. Numara, ya kadranlı telefonun kadranı çevrilerek ya da tuş takımlı telefonun tuşlarına basılarak girilir. Bazı telefon devreleri çevirme işlemlerini kendileri de yapabilir.

İşaret bölgesel santrale gelir ve çağrı bölgesel geçiş merkezine aktarılır. Çağrıyı telefon sistemi içinde rotalamak için bilgisayarlar kullanılır. Bilgisayar, çevrilmiş numarayı alınca rotalama tablosunu inceleyerek hangi yolun kullanılacağına karar verir. Eğer çağrı ülkenin başka bir bölgesinde ise çağrı uzak geçiş merkezine aktarılacaktır. Çağrı çeşitli geçiş merkezleri seviyelerine kadar rotalanıp, anahtarlanabilir.

Çağrı saniyeler içinde alıcının bölgesel santraline varır. Bu santral, uygun bölgesel çevrimin meşgul olup olmadığına bakar. Santral bunu, hatta bir DC akımın varlığına veya yokluğuna göre anlar. Son santral S2 anahtarını kapatarak aranan telefonun zil mekanizmasını harekete geçirir. S2'nin kapanması ile 20 Hz'lik bir işaret telefona gönderilir.

Aranan telefon açılıp ‘off hook’ konumuna getirilirse S2 açılarak zil işareti kaldırılır. Bağlantı, S3’ün kapanması ile tamamlanır. Şehirlerarası anahtarlanan bir çağrı tipik olarak 4-9 anahtarlama merkezinden geçmektedir[1]

Bu bölümde veri haberleşme ağlarındaki temel parçalar anlatılmıştır. Ağ topolojileri, paket anahtarlama, terminaller, front-end işlemcileri, modemler, yayın (broadcast) ağları ve anahtarlamalı ağ temelleri bu bölümde sunulmuştur. Ek olarak bu bölümde LAN ve WAN’ların bir karşılaştırması bulunabilir. Internetworking temelleri ve paket-anahtarlamalı ağlar da bu bölüme eklenmiştir. Bölüm bu parçalara bir giriş niteliği taşımaktadır.

2.1 Ağ Topolojileri

Haberleşme ağları kaynakların paylaşımını kolaylaştırmak üzere tasarlanmıştır, ancak haberleşme harcamalarını düşürmek, akışı arttırmak ve servislerin gecikmesinin azaltılması da tasarım parametreleridir. Bu nedenle ağın topolojisi göz önüne alınması gereken önemli bir parametredir. Çeşitli ağ topolojileri vardır. Bu bölümde en çok kullanılan topolojiler açıklanacaktır. Yıldız topolojisi birçok ağda kullanılan bir topolojidir. Şekil 2.1(a)’da da gösterildiği gibi her istasyon bire-bir bağlantı ile merkez siteye bağlanmıştır. Merkez site (hub veya anahtar denir) istasyonlar arası trafiği düzenleme yeteneğine sahiptir. Bu yaklaşımın çekici tarafı; ağa yeni site veya siteler eklense dahi; her sitenin kendine ayrılmış hattı ile haberleşmeye devam edecek olmasıdır.

Yıldız topolojisi, PBX’lerde ve mesaj anahtarlama tabanlı ağlarda yaygın olarak kullanılır. Genelde böyle bir ağa bağlanan istasyonlar başlıca haberleşme görevlerini yerine getiremezler. Bu görevleri merkezi hub yürütür. Bu topolojinin dezavantajı, merkezi hub’ın çökmesi durumunda tüm ağın haberleşmesinin de çökmesidir.

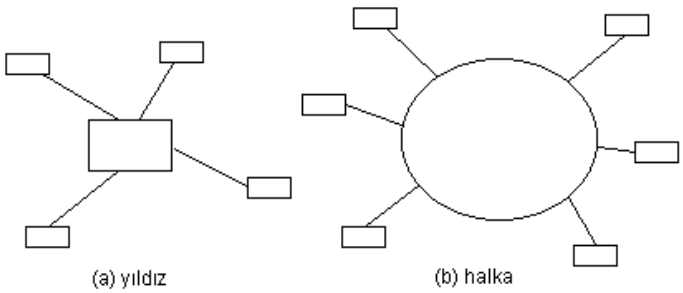
Şekil 2.1(b)’de gösterilen halka topolojisi yıllardır LAN’larda kullanılmaktadır. Her istasyon, halkaya bağlanmıştır ve halkadaki tüm bilgileri alır. Sonuçta bu ağ bir yayın (broadcast) teknolojisi kullanır. Yani, bir istasyonun yayınladığı bir mesaj, halkadaki tüm istasyonlar tarafından alınır. Her bir istasyon halkadan geçen her mesajda bulunan varış adresi bilgisini inceler. Eğer mesajın varış adresi kendi adresi ile eşleşiyorsa istasyon mesajı alır, aksi takdirde istasyon bu mesajı işleme almaz.

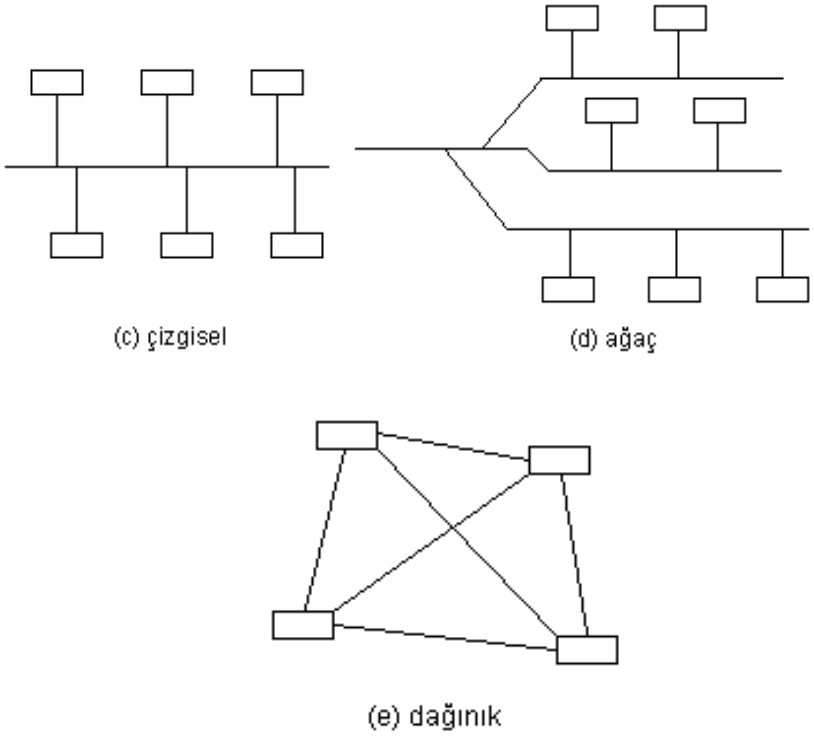
Halka genelde tek yönlüdür. Yani, trafik halka çevresinde tek yönlü akar. Ancak günümüzde birçok halka ağı, iki halka kullanmaktadır ve böylece iki yönlü iletim trafiği sağlanabilmektedir.

Şekil 2.1(c)'de gösterilen çizgisel topoloji de halka topolojisine benzerdir ve bir yayın ağıdır. Hattaki her bir istasyon, tüm mesajları inceler fakat sadece kendine ait mesajları dikkate alır. Bu tip ağdaki akış trafiği iki yönlüdür. Gönderici-istasyon işaretleri kanala verir ve bu işaretler her iki yönde de yayılırlar. Bu yaklaşımdan dolayı çizgisel topoloji aynı anda birden fazla istasyonun ortama işaret göndermesini engellemelidir, aksi halde işaretler birbirlerine girişeceklerdir. Çizgisel ağda bu biçimde bir iletişim yöntemi kullanılması, birden fazla istasyonun ortama bilgi iletmesi nedeniyle işaretler arası girişim oluşmasına yol açabilir. Bunu önlemek için hattın paylaşımına olanak tanıyan bir iletişim protokolünün geliştirilmesi zorunludur.

Ağaç topolojisi de veri haberleşme ağlarında yaygın olarak kullanılan bir yaklaşımdır. İletim ortamının belirli tel veya kablolar ile bölünmesi dışında çizgisel topolojiye benzerdir.

Şekil 2.1(e)'de görülen dağınık topoloji fazla düğüm içermeyen bazı ağlarda kullanılır. Her istasyon, diğer tüm istasyonlar ile bağlantılıdır. Bu yaklaşım tam-bağlantılılık isteyen sistemler için kullanışlıdır. Çok kısa bir cevap-zamanı sağlar. Ek olarak, istasyonlar pahalı protokollere ihtiyaç duymazlar çünkü anahtarlama fonksiyonları gerekmez. Bununla birlikte, dağınık topolojili ağlar, her yeni istasyonun ağa eklenmesi ile daha pahalı hale gelirler. Çünkü yeni istasyon ağdaki diğer tüm istasyonlara ayrı ayrı haberleşme hatları ile bağlanmalıdır. Bu nedenle, bu yaklaşım endüstride sınırlı kullanıma sahiptir.





Şekil 2.1 Ağ Topolojileri

2.2 Ağ Transfer Kapasitesi

Makineler arası veri iletiminde, kodları oluşturmak için bit katarları kullanılır. Veri iletiminin hızı saniye başına bit (bit/sn) ile tanımlanır. Veri iletimindeki tipik hızlar Tablo 2.1'degörülmektedir.

Veri haberleşme bilgisayarları, kişisel bilgisayara göre daha yavaş çalışmaktadırlar. Bu yavaş hız, veri haberleşmesinde, bilgisayarların iletişim için genelde telefon hatlarını kullanmasından ileri gelir. 1960'larda endüstri; bilgisayarları geliştirip, bunları terminaller ve diğer bilgisayarlarla birbirlerine bağlamaya başladığında; en çok kabul gören ve hazır bulunan iletim ortamı telefon hatlarıydı. Telefon hatları yüksek-hızlı bilgisayarlar arasındaki hızlı iletim için değil, veri iletimi için istenen hızı gerektirmeyen ses iletimi için tasarlanmıştır.

Tablo-2-1 Bağlantı Hızları ve Kullanım Alanları

Bit/sn olarak tipik hız	Tipik kullanımları
0-600	Telgraf,eski terminaller; telemetry
600-2,400	İnsan-operatörlü terminaller; kişisel bilgisayarlar
2,400-19,200	Hızlı cevap ve/veya akış gerektiren uygulamalar; bazı batch ve dosya transfer uygulamaları
32,000-64,000	Ses; yüksek-hızlı uygulamalar; bazı videolar
64,000-1,544,000	Çoklu kullanıcılar için çok yüksek hız; bilgisayar-bilgisayar trafiği; ağlar için omurga linkleri; video
1,544,000'dan büyük	Ağlar için omurga linkleri; yüksek-kaliteli video; çoklu sayısal ses

2.3 Ağ Tipleri

Veri iletim ağları veri haberleşme parçaları ihtiva etmektedirler. Bu parçaların belli bir miktarı kaynakların paylaşımı için beraberce çalıştırılırsa bir ağ oluşturulmuş olur. Bu parçalar arasındaki bilgi alışverişi anahtarlar veya bir çeşit iletim trafiği ile ortam üzerinden sağlanmaktadır.

Telefon ağları veri ağlarına oldukça benzerdir. Çünkü telefon ağının telefon kullanıcısına servis verdiği biçimde, veri ağı da veri haberleşme kullanıcısına (genelde bu bir bilgisayar kullanıcısı olmaktadır) servis vermektedir.

2.3.1 Anahtarlamalı Ağlar ve Yayın Ağları

Ağlar, yayın ağları ve anahtarlamalı ağlar biçiminde sınıflandırılabilir. Yayın ağları birden-çoğa (one-to-many) iletim karakteristiği gösterirler. Bu bir haberleşme cihazı, birden çok cihaza iletim yapmaktadır anlamına gelir. Bu özellik, bir istasyonun birçok alıcıya veri ilettiği radyo ve televizyon yayınlarında görülmektedir.

Yayın ağları yaygın olarak bulunabilen ağlardır çünkü makineler kapalı bir çevre içindedirler ve sınırlı sayıda ortam aracılığı ile işareti tüm istasyonlara göndermek göreceli olarak kolaydır. Ek olarak, yayın tekniği uydu iletiminde de oldukça gözdedir. Uydu istasyonu, trafiği (potansiyel olarak) binlerce alıcıya aktarabilir.

Yayın ağları ile karşılaştırırsak, anahtarlamalı bir ağ birden-çoğa ilişkisi ile iletim yapmak üzere tasarlanmamıştır. Her bir veri paketi fiziksel cihaza (anahtar denir) yollanır ve anahtar veriyi nasıl ileri yollayacağına karar verir. Bu yaklaşım,

anahtarlamalı ağlar yayın topolojisini kullanamaz demek değildir (ki gerçekte kullanabilir). Ancak, anahtarlamalı bir ağda trafiği tüm taraflara göndermek ne ekonomik olarak ne de teknik olarak mümkün olmaktadır.

2.3.2 LAN ve WAN

Şimdiye kadar WAN ve LAN'ları tanımlamak ve farklılıklarını göstermek göreceli olarak kolaydı. Bugün bu o kadar kolay değildir çünkü 'wide area' ve 'local area' terimleri bir zamanlar taşıdıkları anlamları artık taşımıyorlar. Örneğin; 1980'lerde LAN, bir bina ve bir kampüsteki birbirlerine olan uzaklıkları bir kaç yüz veya birkaç bin ayağı geçmeyen parçalardan oluşurdu. Bugün LAN'lar kilometrelerce alan kaplayabiliyorlar.

Yine de, bu ağların belli karakteristikleri farklıdır. Bir WAN genelde üçüncü bir kurum tarafından oluşturulur. Örneğin, bir telefon kurumu ve/veya bir servis sağlayıcı kaynakların sahibidir, kaynakları yönetir ve bu servisleri kullanıcılara satar. Karşılaştırırsak, bir LAN genelde kurumun kendisine aittir (birinci elden sahiplidir). Kablolar ve parçalar kurum tarafından alınır ve ağ kurum tarafından yönetilir.

Tablo-2-2 Yerel ve Geniş Alan Ağları

WAN:
• Bir çok bilgisayar, birbirlerine bağlanmıştır.
• Makineler geniş bir coğrafi alana dağılmıştır.
• Makineler arası haberleşme kanalı genelde üçüncü bir kurum tarafından sağlanmıştır. (Örneğin; telefon kurumu, bir servis sağlayıcısı, bir uydu taşıyıcısı)
• Kanallar göreceli olarak düşük kapasitelidir. (kilo bit/sn mertebelerinde)
• Kanallar göreceli olarak hataya yatkındır. (Örneğin; 100.000 bitte 1-bit hata oranı)
LAN:
• Bir çok kullanıcı bilgisayarı birbirlerine bağlanmıştır.
• Makineler, küçük bir coğrafi alana dağılmışlardır.
• Makineler arası haberleşme kanalları genelde kuruma aittir.
• Kanallar göreceli olarak yüksek kapasitelidir. (megabit/sn mertebelerinde)
• Kanallar göreceli olarak hatadan bağımsızdır. (Örneğin; 10^9 bitte 1-bit hata oranı)

LAN ve WAN'lar iletim kapasiteleri açısından da karşılaştırılabilirler. Birçok WAN kbit/sn mertebelerinde çalışır, ancak LAN'lar Mbit/sn mertebelerinde çalışırlar.

Bu iki ağı ayıran bir özellikte de hata oranıdır (iletim hattının hataya sebep verme sıklığı). WAN'lar iletim ortamlarının kat etmek zorunda olduğu geniş coğrafi alanlardan dolayı LAN'lardan daha çok hataya yatkındırlar. LAN'lar göreceli olarak selim

ortamlarda çalışırlar çünkü veri haberleşme parçaları nem, ısı ve elektriğin kontrol altında olduğu binalar içindedir.

Bilgisayar ağları kullanılmaya başlandığı ilk zamanlarda sadece aynı üreticinin ürettiği cihazlar birbirleriyle iletişim kurabiliyordu. Bu da şirketleri tüm cihazlarını sadece bir üreticiden almalarını zorunlu kılıyordu. 1970'lerin sonlarına doğru ISO (International Organization for Standardization) tarafında, OSI (Open System Interconnection) modeli tanımlanarak bu kısıtlamanın önüne geçildi. Böylece farklı üreticilerden alınan cihazlar aynı ağ ortamında birbirleriyle haberleşebileceklerdi[9]

OSI Referans Modeli 7 katman (layer)'dan oluşmuştur. Bu katmanlar sırasıyla;

Application
Presentation
Session
Transport
Network
Data Link
Physical

Şimdi bu katmanları teker teker ayrıntılı bir şekilde inceleyelim.

a) Application Layer (Uygulama Katmanı): Kullanıcı tarafından çalıştırılan tüm uygulamalar bu katmanda tanımlıdırlar. Bu katmanda çalışan uygulamalara örnek olarak, FTP (File Transfer Protocol), SNMP (Simple Network Management Protocol), e-mail uygulamalarını verebiliriz.

b) Presentation Layer (Sunuş Katmanı): Bu katman adını amacından almıştır. Yani bu katman verileri uygulama katmanına sunarken veri üzerinde bir kodlama ve dönüştürme işlemlerini yapar. Ayrıca bu katmanda veriyi sıkıştırma/açma, şifreleme/şifre çözme, EBCDIC'dan ASCII'ye veya tam tersi yönde bir dönüşüm işlemlerini de yerine getirir. Bu katmanda tanımlanan bazı standartlar ise şunlardır;PICT ,TIFF ,JPEG ,MIDI ,MPEG.

c) Session Layer (Oturum Katmanı): İletişimde bulunacak iki nokta arasındaki oturumun kurulması, yönetilmesi ve sonlandırılmasını sağlar. Bu katmanda çalışan protokollere örnek olarak NFS (Network File System), SQL (Structured Query

Language), RPC (Revate Procedure Call), ASP (AppleTalk Session Protocol) ,DNA SCP (Digital Network Arcitecture Session Control Protocol) ve X Window verilebilir.

d) Transport Layer (İletişim Katmanı): Bu katman iki düğüm arasında mantıksal bir bağlantının kurulmasını sağlar. Ayrıca üst katmandan aldığı verileri segment'lere bölerek bir alt katmana iletir ve bir üst katmana bu segment'leri birleştirerek sunar. Bu katman aynı zamanda akış kontrolü (flow control) kullanarak karşı tarafa gönderilen verinin yerine ulaşıp ulaşmadığını kontrol eder. Karşı tarafa gönderilen segment'lerin karşı tarafta gönderenin gönderdiği sırayla birleştirilmesi işinden de bu katman sorumludur.

e) Network Layer (Ağ Katmanı) : Bu katman , veri paketlerinin ağ adreslerini kullanarak bu paketleri uygun ağlara yönlendirme işini yapar. Yönlendiriciler (Router) bu katmanda tanımlıdırlar. Bu katmanda iletilen veri blokları paket olarak adlandırılır. Bu katmanda tanımlanan protokollere örnek olarak IP ve IPX verilebilir. Bu katmandaki yönlendirme işlemleri ise yönlendirme protokolleri kullanılarak gerçekleştirilir. Yönlendirme protokollerine örnek olarak RIP,IGRP,OSPF ve EIGRP verilebilir. Burada dikkat edilmesi gereken önemli bir nokta da yönlendirme protokolleri ile yönlendirilebilir protokollerin farklı şeyler olduğudur. Bu katmanda kullanılan yönlendirme protokollerinin görevi ,yönlendirilecek paketin hedef'e ulaşabilmesi için geçmesi gereken yolun hangisinin en uygun olduğunu belirlemektir. Yönlendirme işlemi yukarıda bahsettiğimiz yönlendirme protokollerini kullanarak dinamik bir şekilde yapılabileceği gibi ,yönlendiricilerin üzerinde bulunan yönlendirme tablolarına statik olarak kayıt girilerek de paketlerin yönlendirilmesi gerçekleştirilebilir.

f) Data Link Layer (Veri Bağı Katmanı) :Network katmanından aldığı veri paketlerine hata kontrol bitlerini ekleyerek çerçeve (frame) halinde fiziksel katmana iletme işinden sorumludur. Ayrıca iletilen çerçevenin doğru mu yoksa yanlış mı iletildiğini kontrol eder ,eğer çerçeve hatalı iletilmişse çerçevenin yeniden gönderilmesini sağlamak da bu katmanın sorumluluğundadır. Bu katmanda ,iletilen çerçevenin hatalı olup olmadığını anlamak için CRC (Cyclic Redundancy Check) yöntemi kullanılır. Switch'ler ve Bridge'ler bu katmanda tanımlıdırlar.

g) Physical Layer (Fiziksel Katman):Verilerin fiziksel olarak gönderilmesi ve alınmasından sorumlu katmandır. Hub'lar fiziksel katmanda tanımlıdırlar.Bu katmanda

tanımlanan standartlar taşınan verinin içeriğiyle ilgilenmezler. Daha çok işaretin şekli ,fiziksel katmanda kullanılacak konnektör türü , kablo türü gibi elektiriksel ve mekanik özelliklerle ilgilenir. Örneğin V.24 ,V.35, RJ45 ,RS-422A standartları fiziksel katmanda tanımlıdırlar[8].

2.3.3 Data Encapsulation

Veriler ,ağ üzerindeki cihazlar arasında iletilirken OS'nin her bir katmanında enkapsülasyona uğrar.OSI 'nın her katmanı iletişim kurulan diğer cihazdaki aynı katmanla iletişim kurar.OSI modelindeki her katman iletişim kurmak ve bilgi alışverişi için PDU (Protocol Data Units) 'ları kulllanırlar. Aşağıdaki tabloda herbir katmanın kullandığı PDU gösterilmiştir.

Tablo-2-3 PDU

Katman	PDU (Protocol Data Units)
Transport Layer	Segment
Network Layer	Packet
Data-Link	Frame
Physical	Bit

2.3.4 Ethernet Ağları

Ethernet ,kolay kurulumu ,bakımı ve yeni teknolojilere adapte olabilme özellikleriyle günümüzde en çok kullanılan ağ teknolojilerinin başında yer alır. Ethernet ağlarda yola erişim yöntemi olarak CSMA/CD (Carrier Sense Multiple Access with Collision Detect) kullanılır. Bu yöntemde aynı anda birden fazla cihazın aynı yol üzerinden veri göndermesi engellenmiş olur. Veri gönderecek cihaz ilk önce yolu dinler ve eğer yolda herhangi bir veri yoksa kendi verisini yola çıkarır. Eğer iki cihaz aynı anda yola veri çikarmaya çalışırlarsa bu durumda collision(çakışma) olur ve bu iki cihazda hatı bırakır. Ardından yeniden hatta çıkmak için restgele hesaplanan bir süre beklerler. Bu süreyi hesaplamak için kulllanılan algoritmalar "back-off" algoritmaları olarak adlandırılır.

Ethernet ağlarda adresleme için MAC (Media Access Control) adresleri kullanılır. MAC adresleri herbir NIC(Network Interface Card) 'in içine donanım olarak kazınmıştır ve 48 bitlik bir sayıdır. Bu 48 bitin ilk 24 bit'i bu kartı üreten firmayı tanımlayan koddur. Geriye kalan 24 bit ise o karta ait tanımlayıcı bir koddur. Bir ethernet ağda aynı MAC adresine sahip iki cihaz olamaz. Zaten MAC adresleride dünyada bulunan herbir NIC için tekdir. Örnek bir MAC adresi A0-CC-AC-03-55-B9 şeklindedir.

Tablo-2-4 Ethernet Ağ Standartları

Standart	Band Genişliği	Maksimum Mesafe	Kullanılan Kablo
10Base-2 (Thinnet)	10 Mbps	185 metre	50 μηο'luk sonlandırıcı ile sonlandırılmış ince koaksiyel kablo.
10Base-5 (Thicknet)	10 Mbps	500 metre	50 μηο'luk sonlandırıcı ile sonlandırılmış kalın koaksiyel kablo.
10Base-T	10 Mbps	100 metre	Cat 3, Cat 4 ,Cat 5 UTP kablo.
10Base-F	10 Mbps	2 Km	Fiber Optik
100Base-TX	100 Mbps	100 metre	Cat 5 UTP veya Type 1 STP
100Base-T4	100 Mbps	100 metre	Cat 3,Cat 4,Cat 5 UTP
100Base-FX	100 Mbps	450 metre-2 Km	Fiber Optik
1000Base-LX	1000 Mbps	440 metre-3 Km	Single Mod veya Multi Mod Fiber Optik kablo.
1000Base-SX	1000 Mbps	260 –550 metre	Multi Mod Fiber Optik kablo.
1000Base-CX	1000 Mbps	25 metre	Bakır kablo.
1000Base-T	1000 Mbps	100 metre	Cat 5 UTP

Önemli bir nokta da aslında birbirinden farklı olan Ethernet ile IEEE'nin 802.3 standartının birbirleriyle karıştırılmasıdır.Aslında bu iki teknoloji birbirlerine çok benzerler ve bu yüzden karıştırılırlar. Ethernet DEC ,Intel ve Xerox firmaları tarafından 1980 yılıda duyurulmuştur.

Ethernet standartlarında kullanılan dört farklı tipte çerçeve (frame) mevcuttur. Bunlar;

· Ethernet_II

· Ethernet_802.3 (Novell Uyumlu)

· IEEE 802.3

· IEEE 802.3 SNAP (SubNetwork Access Protocol)

Yukarıdaki dört çerçeve tipi de Ethernet ağlarda kullanılabilir. Fakat bu çerçeve

tipleri birbirleriyle uyumlu değillerdir. Yani aynı ağda farklı çerçeve tiplerini kullanan iki cihaz haberleşemezler. Bu iki cihazın birbirleriyle haberleşebilmeleri için enkapsülasyon (encapsulation)işleminin yapılması gerekir. Yani çerçeve tiplerinin birbirlerine dönüştürülmesi gerekir. Şimdi sırasıyla bu çerçeve tiplerini inceleyelim.

1. Ethernet_II :

Bu çerçevedeki Preamle kısmı 64 bit uzunlupunda olup senkronizasyon için kullanılır. DA(Destination Address) ,hedef adresi gösterir ve 6 byte uzunluğundadır. SA(Source Address) kısmında ise gönderenin 6 Byte uzunlupundaki MAC adresi bulunur. EType (Ether-type) kısmında ise 2 Byte'lık bir değer bulunur ve bu değer taşınan verinin hangi protokole ait olduğunu belirtir. Örneğin IP için bu değer 0800 'dür. Üst kasman verisi kısmında ise bir üst katmandan alınan veri bulunur. Çerçevenin sonunda bulunan 4 Byte 'lık CRC ise hata sezme algoritmaları kullanılarak hesaplanmış bir değerdir ve karşı taraf bu değere bakarak çerçevenin doğru iletilip iletilmediğini anlar.

2. Ethernet_802.3 :

Bu çerçeve tipi yukarıda anlatılan Ethernet_II tipine çok benzer . Tek farkı bu çerçevede üst katman'dan alınan verinin başında 2 Byte uzunluğunda bir null-checksum bulunur.

3. IEEE 802.3

Preamle	DA	SA	Length	DSAP	SSAP	Control	Üst Katman verisi	CRC

Endüstride Ethernet_802.2 ve Cisco'nun adlandırmasıyla SAP ,802.2 başlık bilgisi

ile DSAP(Destination SAP) ve SSAP(Source SAP) bilgisini içerir. Buradaki DSAP kısmı 1 Byte uzunluğunda olup hedef servis erişim noktasının değeridir. SSAP ise yine 1 Byte uzunluğunda olup kaynak servis erişim noktasını gösterir. Control kısmı ise 1 veya 2 Byte uzunlupunda bir değer olup LLc katmanındaki bağlantının connection-oriented mi yoksa connectionless mi olduğunu gösterir.

4. IEEE 802.3 (SNAP) :

Preamle	DA	SA	Length	DSAP	SSAP	Control	Vendor Code	Type	Üst Katman verisi	CRC

Endüstride Ethernet_SNAP olarak bilinen bu çerçeve formatında 802.2 çerçeve başlığına 5 Byte uzunluğunda SNAP bilgisi eklenmiştir. Bu çerçevedeki Vendor Code kısmında 3 Byte uzunluğunda bir değer bulunur ve bu kod üreticiyi tanımlayan bir koddur.Type kısmında ise 2 Byte'lık bir değer bulunur ve çerçevede taşınan verinin ait olduğu protokolu belirtir[7].

2.3.5 Bağlantı Temelli ve Bağlantısız Protokoller

- Connection -Oriented (Bağlantı - Temelli) Protokoller : Bu protokoller iki uç nokta arasındaki veri iletimini güvenli ve garantili bir şekilde sağlar. Yani verinin gidip gitmediğini ,gitdiyse verinin doğru gidip gitmediğini kontrol eder. Eğer veri yanlış iletilmişse karşı taraftan verinin doğrusunu istemekte bu protokollerin görevidir. Bu protokollerin genel karakteristik özellikleri ise şöyledir.
- Session Setup :İki uç sistem arasında iletişime başlamadan önce sanal birdevre kurulur.
-Acknowledgements : Gönderen tarafa verinin iletildiğine dair bir mesaj yollanır.
- Sequencing : Gönderilen çerçevelerin iletim ortamında kaybolup kaybolmadığı kontrol edilir.
- Flow Control : Veri gönderim hızını kontrol eder. Bir uçtaki sistem diğer uçtaki sisteme veri gönderim hızını yavaşlatmasını söyleyebilir.
- Keepalives :Veri iletiminin olmadığı zamanlarda bağlantının kopmamasını sağlar.

- Session Teardown : Uç sistemlerden gelen bağlantı kesme istekleri doğrultusunda aradaki sanal devreyi koparır.
-Connectionless(Bağlantısız) Protokoller:Bu protokoller veriyi gönderir.Fakat gönderilen verinin doğru yere gidip gitmediğini ,doğru gidip gitmediğini kontrol etmezler. Bunun en önemli faydası gönderilen verilere kontrol bitlerini eklemedikleri ve verinin doğru gidip gitmediğini kontrol etmedikleri için hızlıdırlar[3].

2.3.6 IEEE Data Link Altkatmanları

IEEE ,OSI'nin Data Link katmanını LLC(Logical Link Control) ve MAC (Media Access Control) olmak üzere iki alt katmana ayırmıştır. Böylece aynı network kartı ve kablosu üzerinden birden fazla protokol ve çerçeve tipi iletişim kurabilir. Şimdi kısaca bu katmanları inceleyelim.

1. LLC (Logical Link Control) Katmanı:Network katmanı ile donanım arasında transparan bir arayüz sağlar. Bu katmanda protokoller çerçeve içindeki bir byte'lık SAP(Service Access Point) numarasıyla adreslenir. Örneğin SNA 'nın SAP numarası 04,NETBIOS 'un Sap numarası F0 'dır. Bunun haricinde LLC üst katman protokollerine connection-oriented veya connectionless servis verebilir. Bu servisler type 1,type 2 ve type 3 kategorileri olarak adlandırılırlar.

2. MAC (Media Access Control) Katmanı :NIC kartlarını kontrol eden sürücüler (driver) bu katmanda tanımlıdırlar. Bu sürücüler protokollerden bağımsız çalışırlar ve taşınan çerçevede hangi protokolun olduğunu dikkate almazlar[7].

2.3.7 Half-Duplex ve Full-Duplex Haberleşme

Half –Duplex iletişimde ,iletişimin yapıldığı iki sistem arasında aynı anda sadece bir tanesi iletim yapabilir. Diğer sistem bu sırada karşı sistemden gönderilen verileri almakla meşguldür.

Full-Duplex iletişimde ise her iki sistem de aynı anda veri alıp gönderebilirler.

Üç Katmanlı Hiyerarşi

Ağ planlaması sırasında ve donanımların yerlerinin belirlenmesi sırasında sunulan üç katmanlı yapıyı gözönünde bulundurmak gerekir. Bu yapı aşağıdaki üç katmandan oluşur;

- Core Layer
- Distribution Layer
- Access Layer

Bu modelde ,herbir katmanda çalışacak ağ cihazlarının özellikleri ve fonksiyonları açıklanmıştır.

Şimdi kısaca bu katmanlara bir göz atalım;

1. Core Layer : Bu katmandaki ağ cihazları network'ün omurgasında kullanılmalıve yüksek hızlara sahip olmalıdır.

2. Distribution Layer : Bu katmandaki ağ cihazları core katmanındaki cihazlara bağlantı için kullanılır. Ayrıca bu cihazlar broadcast ve multicast trafiğini kontrol ederler.

3. Access Layer : Bu katmandaki ağ cihazları ağa bağlanacak kullanıcılar için bir bağlantı noktasıdır. Bu katmanda kullanılabilecek ağ cihazlarına örnek olarak switch,bridge ve hub verilebilir.

2.3.8 Layer-2 Anahtarlama

Layer-2 Anahtarlama , donanım tabanlı bir filtreleme yöntemidir ve bu yöntemde trafiği filtrelemek için NIC kartlarının MAC adresleri kullanılır. Layer-2 anahtarlama ,filetreleme için Ağ katmanı bilgilerinin yerine çerçevelerdeki MAC adreslerini kullandığı için hızlı bir yöntemdir. Layer-2 anahtarlama kullanmanın en önemli amacı ,ağı collision domain'lere bölmektir. Böylece ağ ortamı daha verimli kullanılmış olur. Switch kullanarak ağ ortamını segmentlere bölebilirsiniz. Böylece ağdaki collision domain sayısını arttırarak collision'u azaltmış olursunuz. Fakat switch kullanılarak yapılan segmantasyon işleminden sonra bile mevcut ağ tek bir broadcast domain olarak kalır. Yani yapılan tüm broadcast mesajlar ağın tamamını etkiler. Eğer ağı birden fazla broadcast domain'e bölmek istiyorsanız o zaman segmentasyon işlemi için router kullanmalısınız.

Layer-2 anahtarlamanın başlıca üç fonksiyonu vardır. Bunlar ;

- Adres Öğrenme :Layer –2 swicth ve bridge'ler , herbir arayüzlerinden aldıkları çerçevelerin kaynak adreslerini öğrenerek bu adresleri kendi MAC veritabanlarına kayıt ederler.

- İletme/Filtreleme Kararı :Switch , arayüzlerinden aldığı herbir çerçevenin hedef adresine bakar ve bünyesinde bulundurduğu MAC veritabanına bakarak bu çerçevenin hangi arayüzünden çıkarılacağına karar verir.

- Döngüden Kaçınma :Eğer ağdaki switch'ler arasında birden fazla bağlantı varsa ,bu switchler arasında bir dönğü ağı oluşabilir. Bu durumu önlemek için STP (Spanning Tree Protocol) protokolu kullanılır

- STP (Spanning Tree Protocol) :

STP protokolü birden fazla link üzerinden birbirine bağlanmış switch'ler arasında bir ağ döngüsü olmasını engeller. Bunun için , kullanılan yedek linkleri kapatır. Yani STP ağdaki tüm likleri bularak bu linklerin yedek olanlarını kapatıp döngü oluşmasını engeller. Bunu gerçekleştirmek için ağ üzerindeki switch'lerden bir tanesi "root bridge" olarak seçilir. Bu switch'in portları da "designated port" olarak adlandırılır. Bu portlar üzerinden trafik alış verişi olur.Ağdaki diğer switch'ler ise "nonroot bridge" olarak adlandırılır.Root switch , ağ üzerinde daha düşük öncelikli ID'ye ve MAC adresine sahip olan switch olur.Root switch'in dışındaki switch'ler kendileri ile root switch arasındaki en düşük cost değerine sahip yolu seçerler. Bu yolun haricindeki diğer yollar yedek olarak kalır ve birinci yol aktif olduğu müddetçe bu yollar kullanılmaz. STP protokolü , BPDU (Bridge Protocol Data Unit) tipinde çerçeveler kullanır.

LAN Switch Tipleri

LAN'larda kullanılabilecek üç tip anahtarlama modeli vardır. Bunlar;

- Store and forward
- Cut-through
- Fregment Free

Store and forward modelinde bir çerçevenin tamamı tampon belleğe alınır. CRC'si kontrol edilir ve daha sonra MAC tablosuna bakılarak iletilmesi gereken arayüze gönderilir. Cut-through modelinde ise alınan çerçevelerin tamamının tampon belleğe gelmesi beklenmeden sadece çerçevedeki hedef adrese bakılır ve MAC tablosundaki karşılığına bakılarak uygun arayüzden çıkartılır. Fregment Free modelinde ise

çerçevenin ilk 64 byte'ına bakılır ve daha sonra MAC tablosundaki karşılık gelen arayüzden çıkarılır[7]

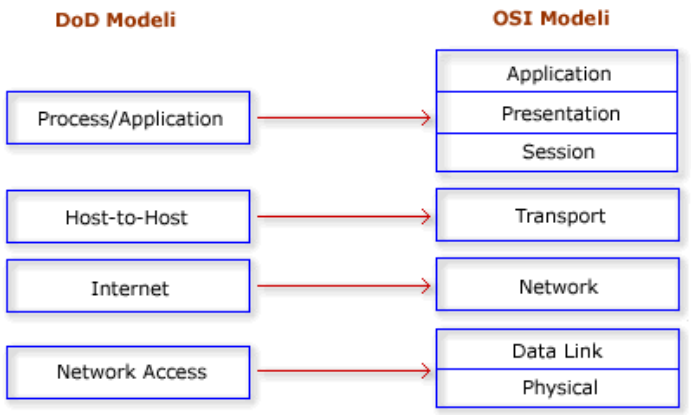
2.3.9 TCP/IP ve DoD Modeli

TCP/IP protokol kümesi Department of Defense (DoD) tarafından geliştirilmiştir. DoD modeli daha önce açıkladığımız OSI modelinin özetlenmiş hali gibi düşünülebilir. Bu modelde 4 katman mevcuttur. Bu katmanlar şunlardır;

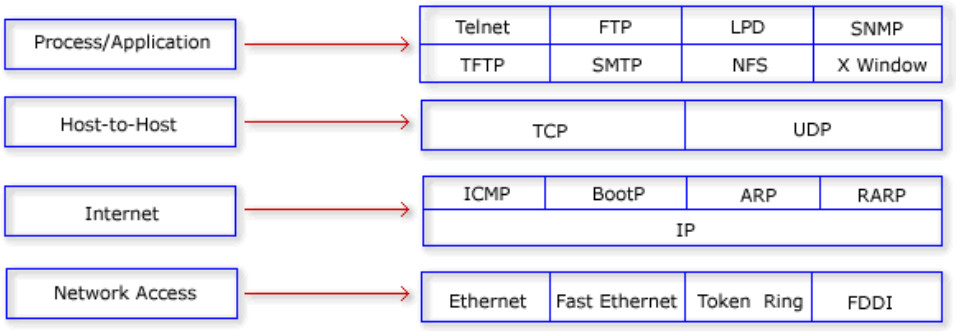
- **Process/Application katmanı**
- **Host-to-Host katmanı**
- **Internet katmanı**
- **Netword Access katmanı**

Bu modelle OSI modelini karşılaştırırsak, bu modeldeki hangi katmanın OSI modelindeki hangi katmana denk düştüğünü aşağıdaki şekilden görebilirsiniz.

Tablo-2-5 OSI ve DoD Modeli



Şimdi de DoD modelinde her bir katmanda tanımlı olan protokolleri inceleyelim.



2.3.9.1 Process/Application Katmanı Protokolleri

Telnet : Telnet bir terminal emülasyon protokolüdür. Bu protokol, kullanıcıların telmet istemci programlarını kullanarak Telnet sunuculara bağlanmalarını sağlar. Böylece telnet sunucuları uzaktan yönetilebilir.

FTP (File Transfer Protocol) : İki bilgisayar arasında dosya alıp vermeyi sağlayan bir protokoldür.

TFTP (Trivial File Transfer Protocol) : Ftp protokolünün bazı özellikleri çıkartılmış halidir. Mesela bu protokolde FTP protokolünde bulunan klasör-gözatma (directory-browsing) ve kullanıcı doğrulama (authentication) yoktur. Genellikle küçük boyutlu dosyaların lokal ağlarda aktarılması için kullanılır.

NFS (Network File System) : Bu protokol farklı tipte iki dosya sisteminin bir arada çalışmasını sağlar.

SMTP (Simple Mail Transfer Protocol) : Bu protokol mail göndermek için kullanılır.

LPD (Line Printer Deamon) : Bu protokol yazıcı paylaşımını gerçekleştirmek için kullanılır.

X Window : Grakfiksel kullanıcı arayüzü tabanlı istemci sunucu uygulamaları geliştirmek için tanımlanmış bir protokoldür.

SNMP (Simple Network Management Protocol) : Bu protokol network cihazlarının göndermiş olduğu bilgileri toplar ve bu bilgileri işler. Bu özelliğe sahip cihazlar SNMP yönetim programları kullanılarak uzaktan izlenip yönetilebilir.

DNS (Domain Name Service) : Bu protokol internet isimlerinin IP adreslerine dönüştürülmesini sağlar.

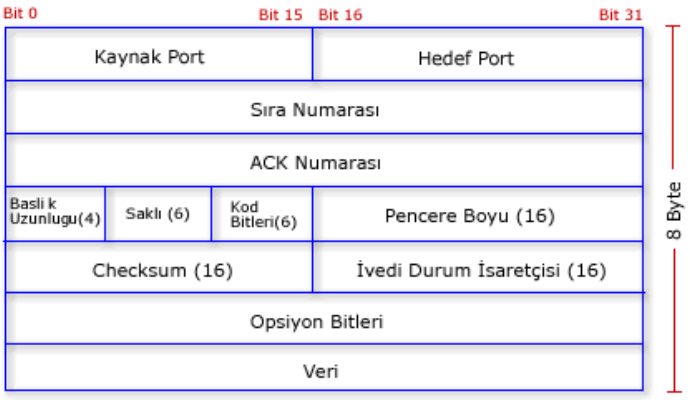
BootP (Bootstrap Protocol) : Bu protokol disket sürücüsü olmayan bilgisayarların IP adres almalarını sağlar. Şöyleki network'e bağlı disket sürücüsüz bir bilgisayar ilk açıldığında ağa bir Boot P istediğini broadcast yapar. Ağdaki BootP sunucu bu isteği duyar ve gönderenin MAC adresini kendi tabanında arar. Eğer veritabanında bu istemci için bir kayıt bulursa bu istemciye bir IP adresini TFTP protokolünü kullanarak yollar. Ayrıca yine TFTP protokolünü kullanarak istemciye boot edebilmesi için gereken dosyayı yollar.

DHCP (Dynamic Host Configuration Protocol) : Bu protokol ağ üzerindeki istemcilere dinamik olarak IP adresi dağıtma işlemini yapar. Istemcilere IP adresinin yanısıra alt ağ maskesi (subnet mask), DNS sunucusunun IP adresi, ağ geçici adresi, WINS sunucunun adresi gibi bilgilerde dağıtılabilir.

2.3.9.2 Host-to-Host Katmanı Protokolleri

TCP (Transmission Control Protocol) : TCP protokolü uygulamalardan aldığı verileri daha küçük parçalara (segment) bölerek ağ üzerinden iletilmesini sağlar. Iki cihaz arasında TCP iletişimi başlamadan önce bir oturumun kurulması gerekir. Yani TCP connection-oriented türünde bir protokoldür. Bunun yanında TCP full-duplex ve güvenilir bir protokoldür. Yani gönderilen datanın ulaşıp ulaşmadığını, ulaştıysa doğru iletilip iletilmediğini kontrol eder. Bir TCP segmentinin formatı ise aşağıdaki şekildedir.

Tablo-2-6 TCP Segment Formatı

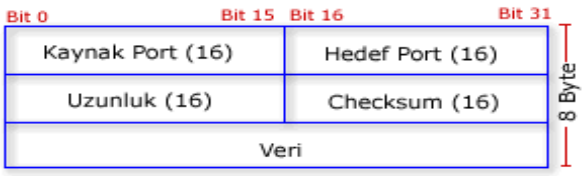


TCP başlığı 20 byte uzunluğundadır. Şimdi bu başlıktaki alanları teker teker inceleyelim. Kaynak port kısmında paketin ait olduğu uygulamanın kullanıldığı portun numarası bulunur. Hedef port kısmında ise alıcı uygulamanın port numarası bulunur. Sıra numarası kısmındaki sayı TCP'nin parçalara verdiği sayı numarasıdır. Paketler bu

numaraya göre karşı tarafa gönderilir ve karşı tarafta paketleri bu sırayla birleştirir. ACK kısmındaki sayı ise TCP'nin özelliği olan güvenilirliğin bir sonucudur ve karşı tarafın gönderen tarafa hangi sıra numarasına sahip paketi yollaması gerektiğini belirtir. Yani karşı taraf birinci paketi aldığında gönderen tarafa ACK'sı 2 olan bir paket yollar. HLEN ise başlık uzunluğunu ifade eder. Saklı alanındaki bitler ise daha sonra kullanılmak üzere saklı bırakılmışlardır ve hepsi 0'dır. Kod bitleri kısmındaki değer ise bağlantının kurulması ve sonlandırılmasını sağlayan fonksiyonlar tarafından kullanılır. Pencere kısmındaki değer ise karşı tarafın kabul edeceği pencere boyutunu ifade eder. Checksum kısmındali değer CRC değeridir ve TCP tarafından hesaplanır. İvedi-durum işaretçisi eğer paketin içinde öncelikle değerlendirilmesi gereken bir veri varsa onun paket içindeki başlangıç noktasını işaret eder.

UDP (User Datagram Protocol) : Bu protokol TCP'nin aksine connectionless ve güvensiz bir iletişim sunar. Yani iletime başlamadan önce iki uç sistem arasında herhangi bir oturum kurulmaz. Ayrıca UDP'de gönderilen verinin yerine ulaşıp ulaşmadığı kontrol edilmez. Buna karşılık UDP TCP'den daha hızlıdır. Aşağıda bir UDP segmentinin formatı gösterilmiştir. Buradaki alanların işlevleri TCP segmentindeki alanlarla aynıdır.

Tablo-2-7 UDP Segmenti Formatı



2.3.9.3 Internet Katmanı Protokolleri

IP (Internet Protocol) : IP protokolü internet katmanının temel protokolüdür. Bu katmanda tanımlı olan diğer protokoller IP protokolünün üzerine inşa edilmişlerdir. Bu protokolde ağ üzerindeki her bir cihaza bir IP adresi tanımlanır. Bu katmanda çalışan ağ cihazları (örneğin router) kendisine gelen paketlerdeki IP adres kısmına bakarak bu paketin hangi ağa yönlendirilmesi gerektiğine kara verir.

ICMP (Internet Control Message Protocol) : Bu protokol IP tarafından değişik servisler için kullanılır. ICMP bir yönetim protokolüdür ve IP için mesaj servisi sağlar. Bu protokolü kullanan servislere örnek olarak ping, traceroute verilebilir.

ARP (Address Resolution Protocol) : Bu protokol ağ üzerinde IP adresi bilinen bir cihazın MAC adresinibulmak için kullanılır.

RARP (Reverse Address Resolution Protocol) : Bu protocol ise ARP'nin tam tersini yapar. Yani MAC adresi bilinen bir cihazın IP adresini öğrenmek için kullanılır.

IP adresi sayısal bir değer olup IP ağlardaki her bir cihazın sahip olması gerekir. IP adresleri MAC adreslerinin tersine donanımsal bir adres değil sadece yazılımsal bir değerdir. Yani istenildiği zaman değiştirilebilir. IP adresleri iki kısımdan oluşur. Birinci kısım Network ID olarak bilinir ve cihazın ait olduğu ağı belirtir. İkinci kısım ise Host ID olarak adlandırılır ve IP ağındaki cihazın adresini belirtir. Her bir cihaz için IP adresi tüm ağda tek olmalıdır.

2.3.10 IP Adresleri

IP adresleri 32 bit uzunluğundadır ve birbirinden nokta ile ayrılmış dört oktetden oluşur. Bu sayılar 0 ile 255 arasında bir değer olabilir. Örnek bir IP adresi 192.168.10.101'dir. Peki network'teki cihaz hangi ağa sahip olduğunu nasıl anlar? Bunu anlamak için subnet mask (alt ağ maskesi) denilen değeri kullanır. IP adresi ile subnet mask değerini lojik AND işlemine tabii tutarak kendi Network ID'sini bulur. Her bir IP adres sınıfı için bu subnet mask değeri farklıdır. Burada yeni bir kavram karşımıza çıktı. IP Adres Sınıfları. Şimdi bu IP adres sınıflarını inceleyelim.

1.) **A Sınıfı Adresler**: IP adresindeki ilk oktet 0 ile 127 arasındadır ve varsayılan subnet mask ise 255.0.0.0 'dır. A sınıfı IP adreslerinde ilk oktet network ID'yi diğer üç oktet ise host ID'yi gösterir. Burada ilk oktet'in 0 ve 127 olma durumları özel durumlardır ve network'te kullanılmazlar. Örneğin 127.0.0.1 yerel loopback adresidir. Dolayısıyla A sınıfı IP adresi kullanılabilecek ağ sayısı 126'dır. A sınıfı IP adresine sahip bir ağda tanımlanabilecek host sayısı ise şu formülle hesaplanır; $2^{24} - 2$. Bu işlemin sonucu olarakta 16.777.214 adet host olabilir. Peki burada kullandığımız 24 nereden geldi? A sınıfı adreste host'u tanımlamak için son üç oktet (sekizli) kullanılıyordu. Yani toplam 24 bit'i host tanımlamak için kullanabiliyoruz. Bu bitler ya 0 ya da 1 olmak zorunda. Bu yüzden birbirinden farklı kaç kombinasyon olacağını 2^{24} ile bulabiliriz. Bu sayıdan 2 çıkarmamızın nedeni ise bu 24 bit'in hepsinin 0 veya 1 olmasının özel bir anlamı olduğu ve herhangi bir host'a IP adresi olarak verilemediği içindir. Örnek bir A sınıfı IP adresi 49.19.22.156 olarak verilebilir. Burada 49 bu IP adresinin ait olduğu ağın ID'sini 19.22.56 ise bu IP adresine sahip host'un host ID'sini gösterir.

2.) **B Sınıfı Adresler**: IP adresindeki ilk oktet 128 ile 191 arasındadır ve kullanılan subnet mask ise 255.255.0.0 ‘dır. Bu da demektir ki bu tür bir IP adresinde ilk iki oklet Network ID’sini, diğer iki oklet ise Host ID’yi gösterir. B sınıfı IP adresinin kullanılabileceği ağ sayısı 16.384 ve her bir ağda kullanılabilecek host sayısı ise 65.534’dür. Örnek bir B sınıfı IP adresi 160.75.10.110.olarak verilebilir.

3.) **C Sınıfı Adresler**: IP adresindeki ilk oktet’in değeri 192 ile 223 arasında olabilir ve varsayılan subnet mask değeri ise 255.255.255.0 ‘dır. Yani bu tür bir IP adresinde ilk üç oktet Network ID’yi son oktet ise Host ID’yi belirtir. Örneğin 192.168.10.101 IP adresini inceleyelim. Bu IP adresi C sınıfı bir IP adresidir. Bunu ilk oktetin değerine bakarak anladık. Bu IP adresinin ait olduğu ağın ID’si ise 192.168.10’dur. Bu IP adresine sahip cihazın host numarası ise 101’dir. C sınıfı IP adreslerinin kullanılabileceği ağ sayısı 2.097.152 ve bu ağların herbirinde tanımlanabilecek host sayısı ise 254’dür.

Bu üç IP sınıfının haricinde D ve E sınıfı IP adresleride mevcuttur. D sınıfı IP adresleri multicast yayınlar için kullanılır. E sınıfı adresler ise bilimsel çalışmalar için saklı tutulmuştur.

2.3.11 Altağlara Bölme İşlemi

Subnetting yani alt ağlara bölme işlemi, IP adresindeki host’lar için ayrılmış kısımdaki bitlerden ihtiyaç olduğu kadarını subnet yapmak için alınır. Bu bitleri alırken gözönünde bulundurulması gereken birkaç önemli nokta vardır. Bu noktalardan birincisi; kaç tane alt ağa ihtiyaç olacağını belirlememiz ayrıca her bir alt ağda kaç tane host bulunacağınıda gözönünde bulundurmamız gerekiyor. Alt ağ sayısını hesaplarken bu alt ağlar arasındaki bağlantılarıda bir alt ağ olarak hesaba katmalıyız. Host sayısını hesaplarken ise bu alt ağlar arası bağlantının sağlandığı arayüzleri de ayrı birer host gibi düşünüp hesaba katılmalıdır.

Aşağıdaki tablolarda A, B ve C sınıfı IP adreslerinde kullanılabilecek alt ağ maskeleri ile bu alt ağ maskelerine denk düşen alt ağ sayısı ve her bir alt ağdaki host sayısını bulabilirsiniz.

Tablo2-8 A Sınıfı IP Adreslerinde Subnetting

Subnet Mask	Alt ağ Sayısı	Host Sayısı	Kullanılabilecek Toplam Host Sayısı
255.192.00	2	4194302	8388604
255.224.0.0	6	2097150	12582900
255.240.0.0	14	1048574	14680036
255.248.0.0	30	524286	15728580
255.252.0.0	62	262142	16252804
255.254.0.0	126	131070	16514820
255.255.0.0	254	65534	16645636
255.255.128.0	510	32766	16710660
255.255.192.0	1022	16382	16742404
255.255.224.0	2046	8190	16756740
255.255.240.0	4094	4094	16760836
255.255.248.0	8190	2046	16756740
255.255.252.0	16382	1022	16742404
255.255.254.0	32766	510	16710660
255.255.255.0	65534	254	16645636
255.255.255.128	131070	126	16514820
255.255.255.192	262142	62	16252804
255.255.255.224	524286	30	15728580
255.255.255.240	1048574	14	14680036
255.255.255.248	2097150	6	12582900
255.255.255.252	4194302	2	8388604

Tablo2-9 B Sınıfı Adreslerde Subnetting

Subnet Mask	Alt ağ Sayısı	Host Sayısı	Kullanılabilecek Toplam Host Sayısı
255.255.192.0	2	16382	32764
255.255.224.0	6	8190	49140
255.255.240.0	14	4094	57316
255.255.248.0	30	2046	61380

255.255.252.0	62	1022	63364
255.255.254.0	126	510	64260
255.255.255.0	254	254	64516
255.255.255.128	510	126	64260
255.255.255.192	1022	62	63364
255.255.255.224	2046	30	61380
255.255.255.240	4094	14	57316
255.255.255.248	8190	6	49140
255.255.255.252	16382	2	32764

Tablo2-10 C Sınıfı IP Adreslerinde Subnetting

Subnet Mask	Altağ Sayısı	Host Sayısı	Kullanılabilecek Toplam Host Sayısı
255.255.255.192	2	62	124
255.255.255.224	6	30	180
255.255.255.240	14	14	196
255.255.255.248	30	6	180
255.255.255.252	62	2	124

2.3.12 TCP/IP'de Güvenlik

İnternet verinin gizliliği ve bütünlüğü konusunda yetersizdir.Gizli,değerli ve saldırıya açık veriler için kriptografiye başvurmalıdır.

2.3.12.1 Kriptografi

İnternette yollanan veri paketleri birçok halka açık ağlardan geçer, bu da bu paketlere ulaşmayı mümkün kılar. Son derece gizli bilgiler internette nakil olurken, bu durum önemli bir kaygı halini alır. Bu tür bilgileri korumak mümkün olmadıkça, internet iş yapmak veya gizli, şahsi yazışmalarda bulunmak için asla güvenli bir yer olmayacaktır. Bilgi güvenliği başkası tarafından dinlenme, bilginin değiştirilmesi, kimlik taklidi gibi tehditlerin ortadan kaldırılması ile sağlanır ve bu amaçla kullanılan temel araç kriptografidir. Kriptografi bilgi güvenliğini inceleyen ve anlaşılabileni anlaşılamaz yapan bir bilim dalıdır. Güvenilirlik, veri bütünlüğü, kimlik doğrulama gibi bilgi güvenliği konularıyla ilgilenen matematiksel yöntemler üzerine yapılan çalışmalar kriptografinin önemli konularıdır.

Kriptografi genel olarak şu ana konularla ilgilenir:

- **Gizlilik:** Bilgi istenmeyen kişiler tarafından anlaşılamamalıdır

- **Bütünlük:** Bir iletinin alıcısı bu iletinin iletim sırasında değişikliğe uğrayıp uğramadığını öğrenmek isteyebilir; davetsiz bir misafir doğru iletinin yerine yanlış bir ileti koyma şansına erişmemelidir. Saklanan veya iletilmek istenen bilgi farkına varılmadan değiştirilememelidir.

- **Reddedilemezlik:** Bilgiyi oluşturan ya da gönderen, daha sonra bilgiyi kendisinin oluşturduğunu veya gönderdiğini inkar edememelidir. Bir gönderici daha sonrasında bir ileti göndermiş olduğunu yanlışlıkla reddetmemelidir.

- **Kimlik belirleme:** Gönderen ve alıcı, birbirlerinin kimliklerini doğrulayabilirler. davetsiz bir misafir başkasının kimliğine bürünme şansına erişmemelidir.

Bir göndericinin bir alıcıya açık ağlar üzerinden bir ileti göndermek istediği zaman, açık ağlardan gönderilen iletiler üçüncü şahıslar tarafından dinlenme ve değiştirilme tehdidi altındadırlar. Burada söz konusu ileti düz metindir. Bazı kullanımlarda "düz metin" adı da verilir. Bir iletinin içeriğini saklamak üzere yapılan gizleme işlemi de şifrelemedir. Bu işlem düz metini şifreli metine dönüştürür. Bilginin içeriğinin başkalarının anlamayacağı hale gelir. Bu bilgi bir yere iletilmek amacıyla şifrelenen bir mesaj veya saklanmak amacıyla şifrelenen bir bilgi olabilir. Şifrelenmiş bir ileti "şifreli metin" dir. Şifreli metni düz metne geri çevirme işlemi şifre çözümüdür. Bu işlemler Şekil 2.2'te gösterilmektedir.

Şekil 2.2 Şifreleme ve Şifre Çözme İşlemleri

Anahtar ise kriptografi algoritmasının şifreleme ve şifre çözme amacıyla kullandığı sayı dizisidir. Anahtar uzunluğu ne kadar büyük olursa şifrenin kırılması o kadar zorlaşır.

Gizli anahtarlı (simetrik) ve açık anahtarlı (asimetrik) olmak üzere iki çeşit şifre sistemi vardır. Gizli anahtarlı kriptografide; şifrelemede de, şifre çözümünde de aynı anahtar kullanılır. Bugün en çok kullanılan gizli anahtarlı şifre sistemi DES (Veri Şifreleme Standardı)'tir. DES algoritması üzerinde geniş ölçüde çalışmalar yapılmıştır ve dünyada en çok bilinen ve kullanılan algoritmadır.İlk tasarlandığında, amaç donanım uygulamalarında kullanmaktı. İletişim amaçlı kullanımda hem gönderen, hem de alıcı şifreleme ve şifre çözümünde kullanılan aynı gizli anahtar üzerinde anlaşmış olmalıdır. Gizli anahtarın güvenli bir biçimde dağıtılması zor olabilir, bu amaçla gizli anahtarların açık ağlar üzerinden güvenli aktarımını sağlamak için açık anahtarlı yapılar kullanılır. DES aynı zamanda, sabit diskte veri saklamak gibi tek kullanıcılı şifreleme amaçlı da kullanılabilir.

Açık anahtarlı kriptografide, her kullanıcının bir açık bir de gizli olmak üzere iki anahtarı vardır. Açık anahtar kamuya açıktır, isteyen herkes elde edebilir. Gizli anahtar ise saklı tutulur, sahibi dışında herhangi biri tarafından elde edilmemeli ve kullanılamamalıdır. Şifreleme açık anahtarla, şifre çözümü ise gizli anahtar ile yapılır. Günümüzde en çok kullanılan açık anahtarlı şifreleme sistemi RSA (Rivest, Shamir ve Adleman; RSA şifre sistemini bulan bilim adamları)'dır. RSA şifreleme sistemi, hem şifreleme hem de sayısal imza atma olanağı tanıyan açık anahtarlı bir kriptografik yapıdır.RSA sisteminin güvenliği, çarpanlarına ayırma probleminin zorluğu temeline dayanır. Çarpanlarına ayırma işleminin kolay bir yönteminin bulunması, RSA algoritmasının kırılması anlamına gelir.

DSA (Sayısal İmza Algoritması) da oldukça yaygın kullanılan açık anahtarlı bir şifreleme yöntemi olmasına rağmen, sadece imzalamada kullanılabilir, şifrelemede kullanılamaz. DSA, NIST (Uluslararası Teknoloji ve Standartlar Enstitüsü) tarafından sayısal imza standardı olarak yayınlanmıştır[6][7].

DSA algoritması da, RSA gibi açık anahtarlı bir kriptografik algoritmadır. RSA'dan farkı sadece imzalama amaçlı kullanılabilmesi, şifreleme yapılamamasıdır.

Yukarıda bahsedilen sayısal imza,imzalanacak metin ve imzalayacak kişinin gizli anahtarı kullanılarak elde edilen bir dizi karakterden oluşur. Elle atılan imzanın elektronik ortamdaki karşılığıdır. Sayısal imza, doğru şekilde kullanıldığında, mesajın

bütünlüğünün korunmasını, kaynağın doğruluğunun ispatlanmasını ve reddedilemez olmasını sağlar.Sayısal imzanın nasıl işlediğini anlamak için yeni bir kriptografik algoritmadan, özet fonksiyonundan bahsetmek gerekir. Asimetrik (açık anahtarlı) şifreleme yöntemleri şifreleme ve şifre çözme için farklı anahtarlar, simetrik (gizli anahtarlı) şifreleme yöntemleri ise iki işlem için de aynı anahtarı kullanır. Özet fonksiyonları ise sadece şifreler. Özet fonksiyonlarından orijinal mesaja geri dönüş hiç bir şekilde mümkün değildir.Özet fonksiyonları mesajın parmak izini çıkartır. Bir mesajı imzalamak, öncelikle mesajın, özet fonksiyonundan geçirerek özetini çıkarmak ve çıkan özeti şifrelemek anlamına gelir.

2.3.12.1.1 Uygulama Katmanında Güvenlik

Uygulama katmanı güvenliği ağ üzerinde uygulama koşturan iki konak arasında uçtan uca güvenlik sağlar ve aktarım mekanizması ile ilgilenmez.Tüm güvenlik istekleri bütünlük,güvenlik ve reddedilemezlik bu katmanda sağlanır.Uygulama katmanı güvenliği tam bir çözüm olamamaktadır.Çünkü her bir uygulama ve istemci güvenlik servislerini sağlamaya adapte olmalıdır.

- **PGP**

İnternet'te alınacak güvenlik tedbirleri, iletilerin doğru kişiye ve değişmeden ulaştığından
emin olunmasını sağlamanın yanında 3. kişilerin bilgiye ulaşmalarını da engellemelidir.
PGP programında dijital imza ile aynı temel prensip üzerine kurulmuş ve bunun yanında
birtakım ek prosedürlerin de yardımcı olduğu oldukça güvenli bir şifreleme sistemi
mevcuttur. PGP dünya çapında kullanıcıların elektronik posta mesajlaşmaları sırasında güvenlik ve sayısal sinyalleşme amaçlı kullandıkları uçtan uca güvenlik sağlayan bir şifreleme sistemidir.

- **S-HTTP**

S-HTTP (Güvenli Hipermetin Taşıma Protokolü) , İnternet üzerinde güvenlik servislerini sağlayan bir protokoldür. Tasarlanma amacı gizlilik, kimlik doğrulama,

bütünlük, ve reddedeme (kendisinden başkası olduğunu söyleyememe) olan S-HTTP, aynı zamanda birden çok anahtar-yönetimi mekanizmasını ve şifreleme algoritmasını, taraflar arasındaki aktarımda yer alan seçenek kararlaştırılması yoluyla destekler. S-HTTP, kendisini hayata geçirmiş olan belirli yazılımlarla sınırlıdır, ve her bir mesajı ayrı ayrı şifreler[7].

2.3.12.1.2 Aktarma Katmanı'nda Güvenlik

Aktarma katmanı güvenliği konaklar arasında işlemden işleme güvenlik , TCP'nin güvenli ve bağlantı temelli iletişim kurmasını sağlar.Çoğu aktarım katmanı güvenlik mekanizmaları güvenlik yararlarına ulaşmak için uygulamalarda değişiklikler talep eder. Güvenli uygulamalar standart güvenli olmayan uygulamalara göre farklı portlar kullanırlar.

- **SSL**

SSL(Güvenli Soket Katmanı), Netscape tarafından İnternet üzerinde güvenlik sağlamak amacıyla geliştirilen bir şifreleme yöntemidir. SSL Veri İletim katmanında işlev görür, güvenli bir şifreli veri kanalı oluşturduğu için bir çok veri tipini şifreleyebilir. Bu en yaygın olarak, Communicator güvenli bir WWW sitesine bağlandığı, ve güvenli bir belgeyi görüntülemek istediğinde görülür. SSL, Netscape Haberleşme şirketinin diğer veri şifrelemelerinin olduğu kadar, Communicator'ın da güvenli iletişim temellerini oluşturur.

- **SSH**

SSH (Güveli Kabuk), uzak sistemlere giriş yapabilmenizi, ve şifreli bir bağlantı kurabilmenizi sağlayan programlar grubudur. Kullanıcıların kimliğini doğrulamak için ve iki bilgisayar arasındaki iletişimi şifrelemek için açık anahtarlı şifreli yazım tekniğini kullanır. Uzaktaki bir bilgisayara güvenli şekilde giriş yapmak veya bilgisayarlar arasında veri kopyalama yapmak, ama bu sırada gelebilecek ortadaki-adam (oturum kaçırma) ve DNS taklit saldırılarını engellemek amacıyla kullanılabilir.

- **Filtreleme**

Aktarma katmanında görev yapan yönlendiricilerce her bir arayüzden blok ve ileri işlemleri ile kontrol sağlanır.Bu paketlerin ileri ya da atılması işlemleri erişim-listelerinin ışığında gerçekleştirilir.Aktarma katmanı bilgisi standart erişim-listelerince değil belli bir protokolün parametrelerine bağlı uzatılmış erişim-listelerince filtre

edilir.TCP filtreleme seçenekleri kurulmuş bağlantıları, port numaralarını ve çeşitlerini, servis çeşitlerini içerir.UDP filtreleme seçenekleri sadece port numaralarını içerir[7]

2.3.12.1.3 Ağ Katmanın Güveliği

Ağ katmanı güvenliği daha üst katmanlarda bulunan uygulama ve aktarım protokollerine güvenli trafik hizmeti sağlar.

- **IPSec**

IPSec (İnternet Protokol Güvenliği) kullanıldığında programlar değiştirilmeden güçlü bir güvenlik sağlar.Mevcut güvenlik standartlarının bir çoğu uygulama seviyesinde çalışmaktadır.Bu protokoller web,elektronik posta,FTP gibi sınırlı sayıda uygulamayı desteklerken IPSec gibi ağ katmanında çalışan güvenlik protokolleri, IP ağı üzerinden veri iletiminde bilginin gizliliğini,bütünlüğünü ve güvenirliğini sağlar.

IPSec, IPSec komşuları denilen iki nokta arasında güvenli haberleşme sağlar.Bu haberleşmede Sas (Güvenlik Kurumları) kümesi kullanılır.Sas hangi güvenlik protokollerinin,parametrelerinin uygulanacağını belirler.İki komşu arasında birden fazla IPSec oturumu kurulabilir ve her IPSec oturum için aynı Sas seti kullanılır.

IPSec üç temel fonksiyonu yerine getirir:

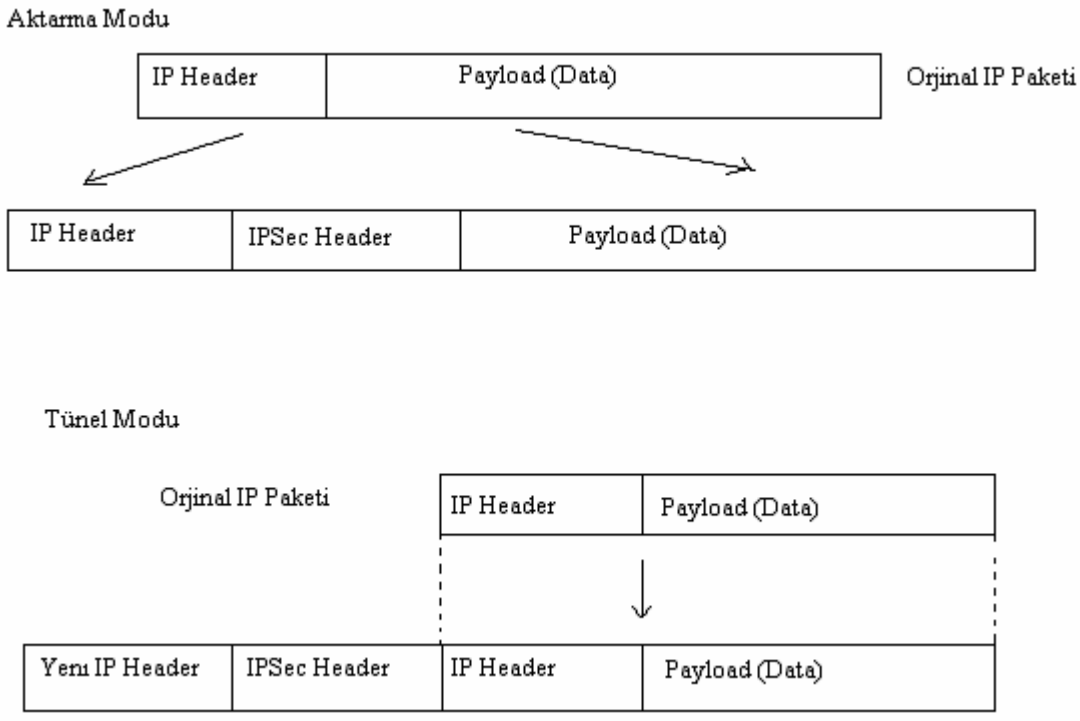
- **AH (Yetkilendirme Protokolü):**Bu protokol IPSec'te paket yetkilendirmesi sağlar.Komşular IPSec haberleşmede,aktarım mod ve tünel mod olmak üzere iki mod kullanır.

- **ESP (Yetkilendirme veya Gizlilik Protokolü) :**Bu protokol yetkilendirme ve veri şifrelemesi sağlar.ESP tek başına kullanılacağı gibi AH protokolü ile beraber kullanılabilir.ESP hem aktarım modda hem tünel modda kullanılabilir.

- **IKE (Internet Anahtar Değiş-Tokuşu) Protokolü** :(Anahtar değişimi elle de yapılabilir) SAs parametrelerinin tanımlanması IKE tarafından otomatik olarak yapılır.Manual IPSec'te SAs parametreleri ağ yöneticisi tarafından önceden tanımlanır.Böylece konfigürasyona bağımlılık ya da yanlış tanımlamalar gibi sakıncalar doğmaktadır.Ayrıca tanımlanan parametrelerin süresi hiç dolmamaktadır ve böylece güvenlik açığı oluşmaktadır.IKE protokolü elle yapılan IPSec'e göre bir çok avantaj sağlar. Bunlar:

- Anahtarların elle tanılanmasına gerek yoktur
- IPSec SAs için hayat süresi belirlenebilir
- Şifreleme anahtarlarının IPSec oturumu boyunca değişimine izin erir.Komşuların dinamik olarak yetkilendirilmesine izin verir

IPSec göndericinin (veya onun yerine görev yapan geçiş kapısının) her IP paketinin kimlik denetimini yapmasını, şifrelemesini veya her iki fonksiyonu birden pakete uygulamasını sağlar. Bu iki fonksiyonu birbirinden ayırmak IPSec kullanmak için mod denilen iki metodun gelişmesine neden olmuştur. Aktarım modunda, IP paketinin sadece veri kısmının kimlik denetimi yapılır veya şifrelenir.Bu modun avantajı IP paketine fazla yeni bytelar ilave edilmemesidir.IP paketinin tamamına kimlik denetimi veya şifreleme yapan öteki yaklaşıma ise tünel modu denir. IPSec aktarım modu pek çok alanda faydalı olurken, tünel modu belirli ataklara karşı çok daha iyi koruma ve İnternette oluşacak trafik izlemeyi sağlar.



Şekil 2.3 IPSec Modları

IPSec güvenliği,gizliliği ve bütünlüğü tüm sistemde sağlamak için birkaç değişik güvenlik teknolojilerini birlikte kullanır.Şifreleme için DES,bütünlük için SHA(ki bu özet fonksiyonunu baz alır) ve yetkilendirme için ise IKE farklı metodları destekler.

- **Filtreleme**

Paket filtreleri yönlendiriciler ve üçüncü katmanda çalışan diğer ağ cihazları üzerinde kaynak ve hedef IP adreslerinin kontrolü için kullanılabilir.Standart erişim-listeleri kaynak adresleri üzerinden filtreleme yapar.Uzatılmış erişim-listeleri ise ağ katmanında ICMP veya IP protokolleri ile filtreleme yapabilir.ICMP ile filtreleme belirli mesajlara dayandırarak yapabilir.Bunun nedeni ICMP mesajı IP paketinin veri bölümünde taşınır.Bu tüzden ICMP paketlerinin dağıtım güvenilirliği,IP paketlerinin dağıtım güvenilirliği ile sınırlı kalmaktadır. ICMP paketleri ortamda geri besleme sağlar.Bu yolla ciddi problemleri ,haberleşen birimlere bildirerek bir hata bildirim mekanizması oluştururlar.IP filtreleme aktarma katmanındaki port numaralarını içerir ki buna göre belirli servislere belirli adresler arasında izin verilir veya izin verilmez. Erişim-listeleri ile ayrıca IPX veya AppleTalk gibi protokol grublarıda kontrol edilir.

2.3.12.1.4 Veri İletim Katmanında Güvenlik

Veri iletim katmanında güvenlik noktadan noktaya yapılır ve hattın şifrelenmesi ve şifre çözümü konularını içerir.Askeriye,hükümet ve çeşitli banka kuruluşları bu yaklaşımı çok yaygın bir şekilde kullanırlar.Büyük ağlarda kullanılamayabilir,bunun nedeni paketlerin şifrelenmiş biçimde yönlendirilememesidir.

- **Doğrulama**

Doğrulama, uzaktan erişim söz konusu olduğunda en önemli fonksiyondur. Güçlü bir doğrulama olmaksızın ağa girişimin kontrol altına alınması olanaksızdır ve bunun sonucu kurumsal bilgilerin yetkilendirilmemiş kişilerin eline geçmesi çok kolay olacaktır.Doğrulama,ağ üzerindeki her cihaza ölçeklenebilirlik,esneklik ve kontrol sağlar.

Güvenlik duvarı,yönlendiriciler ve uzak erişim sunucuları ağ güvenliğini sağlayan cihazlardır.Konfigüre edilen bu cihazlarla ağa birçok yoldan erişmek isteyen ağ yöneticisi ve kullanıcıların ağa daha kolay ve güvenli ulaşması merkezi bir veritabanı kullanmalarıyla mümkün olur.Doğrulama sunucuları,ağa çeşitli cihazlardan gelen ulaşma isteklerini ve ricalarını çeşitli parametrelerle doğrular.TACACS+(Sonda Bulunan Erişim Kontrolörü Erişim Kontrol Sistemi +), RADIUS(Uzaktan Erişim Dial-IN Kullanıcı Servisi),Kerberos doğrulama sunucuları aracılığı ile onay mekanizması kullanmaktadır.

- **TACACS+**

TACACS+ doğrulama sunucu sistemidir ve kullanıcı ID(Tanımlayıcı) ve parolasını kullanarak ağa girdiğinde güvenlik sisteminin desteği ile kişilik belirlemesi yapar.

TACACS'ın en son sürümüdür.

TACACS+'ın belli özellikleri:

- TACACS ve RADIUS'un en son sürümü aktarma için UDP'yi kullanırken,TACACS+ , TCP (port 49 ile) ile güvenilir bir aktarma yapar

- TACACS+ istemci ve sunucu arasındaki tüm iletişimleri şifreler

TACACS+ birçok protokolü destekler.örneğin IPX,ARA (AppleTalk Uzaktan Erişim), NASI (Novell Asenkron Servis Arayüzü),X25 vb

- **RADIUS**

RADIUS uzaktan erişimli kullanıcılar ile var olan bilgisayar ağı arasında kullanıcı ID 'si ve parola bilgilerinin güvenli olarak değiş tokuşunu sağlamakla görevlidir. RADIUS açık bir protokol standarttır ve uzaktan erişimli kullanıcılarının merkezi olarak uzaktan erişimini sağlar.

RADIUS'un belli özellikleri:

- Aktarım için UDP kullanır
- RADIUS istemci ve sunucu arasındaki tüm iletşimi parolamak yerine ,yalnızca parolayı şifreler
- RADIUS birçok protoklü desteklemez

- **Kerberos**

Kerberos, MIT'teki (Massachusetts Teknoloji Enstitüsü) Athena Projesi tarafından geliştirilen bir kimlik doğrulama sistemidir. Kullanıcı sisteme giriş yaptığında, Kerberos kullanıcının kimliğini doğrular (bir parola kullanarak), ve kullanıcıya ağa dağılmış diğer sunucular ve bilgisayarlara kimliğini kanıtlamak için bir yol sağlar. Bir Kerberos alanı tüm kullanıcıları,konakları ve ağ sunucularının kayıtlarını Kerberos sunucusunda kayıtlı olarak tutar.Kerberos asimetrik anahtar kriptolojisi kullanır ve Kerberos alanına katılan her kullanıcının ve her ağ kaynağının şifresini kayıt eder.Her kullanıcı ve her ağ kaynağının bir Kerberos hesabına ihtiyacı vardır.Bu bilinen şifre kimliğinin var olduğunun bir ispatıdır.Kerberos sistem anahtarı ile şifrelenmiş tüm parolaları saklar ve sistem anahtarında uzlaşılmışsa tüm paraloların tekrar yaratılması gerekir.

3.1 Kablosuz Yerel Ağlar

Wireless LAN " wireless local area network" (kablosuz yerel alan ağı) ifadesinin kısaltılmışıdır. Geleneksel (kablolu) LAN yapılarında bilgisayarlar birbirilerine kablolar kullanılarak bağlanmaktadır. Kablosuz yerel alan ağı sistemlerinde iletim ortamı havadır ve iletim elektromagnetik dalgalar aracılığı ile yapılır. Kablosuz yerel alan ağı sistemleri 2.4 GHz ISM (Industrial–Scientific-Medical) Bandında çalışmaktadır

3.1.1 İstasyon, Erişim Noktası, Ağ Ara Yüz Kartı ve RADIUS Sunucu Tanımları

En basit anlamda istasyon, kablosuz yerel alan ağının olanaklarından yararlanan kullanıcı ve kullanıcının kullanıdığı cihazdaki (örneğin dizüstü bilgisayar) kablosuz ağ ara yüz kartı olarak tanımlanabilir.

Erişim noktası, kablosuz yerel alan ağı sistemlerinde, mevcut kablolu ağın kablosuz ağa genişletilmesi için kullanılan birimdir. Erişim noktaları, kablolu ağdaki verileri hava ortamına taşımak için kullanılır. Dolayısı ile erişim noktaları kullanıcıların kullandığı

cihazlardaki ağ ara yüz kartları ile kablolu ağ arasındaki iletimi sağlarlar. Böylece mevcut kablolu ağ kablosuz ortama genişletilmiş olur.

Ağ ara yüz kartı ise geleneksel ağ yapılarından da bilindiği üzere cihazlar ile ağ arasında ara yüz oluşturan bileşendir. Ağ ara yüz kartı, kullanıcının kullandığı cihaz ve erişim noktası arasında (iletim ortamının hava olduğu unutlmamalıdır) ara yüz oluşturur.

RADIUS (**R**emote **A**uthentication **D**ial-**I**n **S**ervice) Sunucu ayrık bir erişim kontrol sunucusudur ve ağları izinsiz girişe karşı korumak için kullanılır. Genel amaçlı kullanılan bir sunucu olmasına rağmen kablosuz yerel alan ağı sistemleri için tasarlanmış olanları mevcuttur ve ek güvenlik önlemleri getirmektedirler. RADIUS sunucuda kullanıcıların güvenlik ve ağa erişim ile ilgili tüm bilgileri tutulur. Her hangi bir kullanıcı ağa erişmek istediğinde RADIUS sunucu veri tabanından kullanıcının bilgilerini kontrol eder ve eğer doğru ise erişime izin verir.

3.1.2 Ad – Hoc Ağlar

Ad – Hoc ağ yapısı, özel amaçla kurulan ve telsiz ortamda birbirileri ile doğrudan iletişim kurabilecek noktalar arasında oluşturulan ağ yapılarının genel adıdır. Kablosuz yerel alan ağı sistemleri buna müsade etmektedir. Ağ konfigürasyonlarından kurulumu en kolay ve hızlı olan konfigürasyondur. Hiçbir ön ayar gerektirmez. Geleneksel ağ yapılarında kurulan noktadan noktaya bağlantılara karşı üstünlüğü ise arada kablo olmaması ve birden çok birimin birbirine bağlanabilmesidir. Bu konfigürasyona özel olarak Bağımsız Servis Birimi (**I**ndependent **B**asic **S**ervice **S**et) (IBSS) denilmektedir.

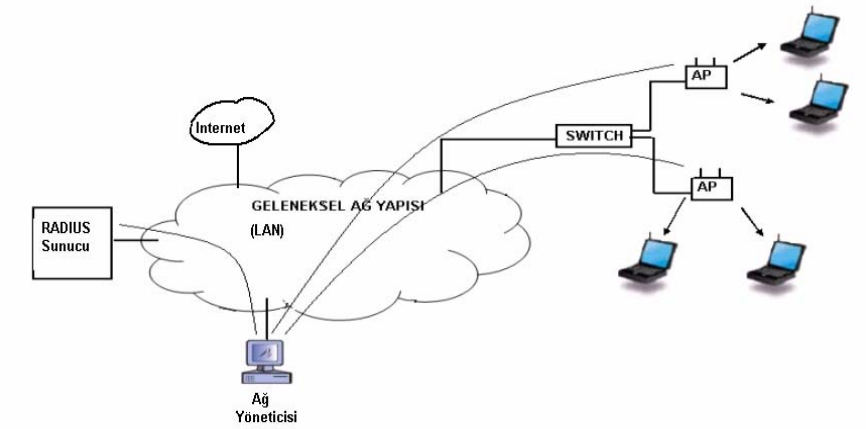
Şekil 3.1 Ad – Hoc Konfigürasyonu

3.1.3 Omurgaya entegre edilen Kablosuz Yerel Alan Ağı Konfigürasyonu

Bu konfigürasyona literatürde “infrastructure” konfigürasyonu denilmektedir. Kablolu ağ yapısı ile kablosuz ağ yapısı bir veya birden çok erişim noktası aracılığı ile birleştirilir ve cihazların kablolu ağ yapısının servislerini kullanması sağlanmış olur. Bu tip konfigürasyonlar bir bina veya kampüs alanının tamamını kapsanmasının istenildiği

durumlarda uygun seçenek olmaktadırlar. Genişletilmesi geleneksel ağ yapılarından daha hızlı ve kolay olmaktadır. Bu konfigürasyon en çok kullanılan konfigürasyondur.

Şekil 3.2 Örnek Konfigürasyonu



Şekil 3.3 Pratikte Kullanılan Örnek Konfigürasyon

Şekil 3.3'te pratikte kullanılan omurgaya entegre edilmiş bir ağın genel görünümü verilmiştir. Burada ağ yöneticisi olan kullanıcı Web yada Telnet üzerinden erişim noktalarına ve RADIUS sunucusuna erişerek bunların konfigürasyonlarını istenilen özelliklere uygun olarak yapabilir. Burada ek bir güvenlik önlemi olması açısından RADIUS sunucunun önüne firewall cihazları da konulmaktadır.

3.2 IEEE 802.11/b Kablosuz Yerel Alan Ağı Standardı

IEEE 802.11/b standardı kablosuz yerel alan ağı sistemleri üzerine çıkartılmış ilk standarttır. Standart aynı zamanda bir ANSI (**A**merican **N**ational **S**tandarts **I**nstitute) standardı olarakta kabul edilmiştir. Bu standart sayesinde farklı cihaz üreticisi firmaların

ürettikleri cihazların bir arada çalışılabilirliği sağlanmıştır.Standart yerel alanda ağ kurulumu için gerekli hava ortamı ile ilgili tanımlamaları yapmıştır. Standart, katmanlı bir yapıda tanımlanmıştır. Bunlar

- Fiziksel Katman (**Phy**isical Layer) (PHY)
- Ortam Erişim Katmanı (**M**edium **A**ccess **C**ontrol) (MAC)

olmak üzere iki katmandan oluşmaktadır. Bu katmanlarda tanımlanmış işlemler erişim noktası ve istasyon olarak tanımlanmış olan birimler tarafından yerine getirilir[11]

3.3 IEEE 802.11/b Kablosuz Yerel Alan Ağı Standardının Topolojisi

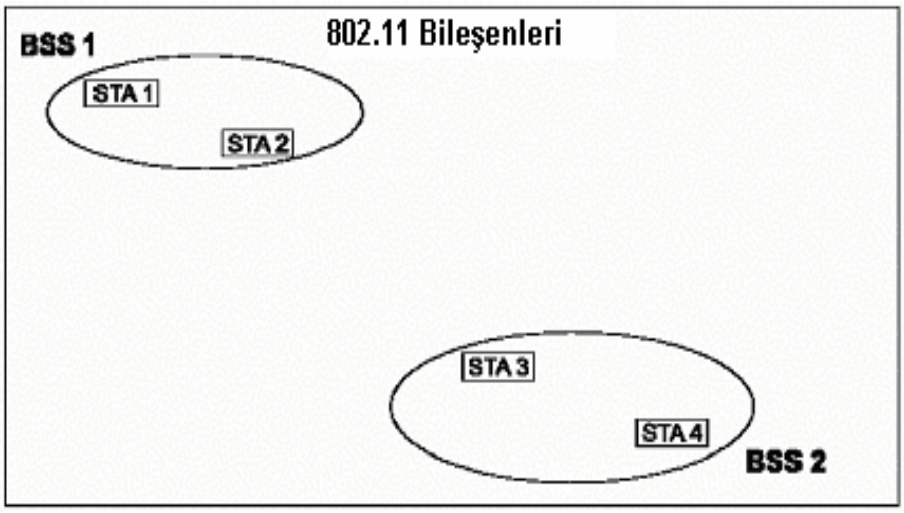
Bu kısımda standardın kulanım açısından uygun görerek tanımlamış olduğu topolojiler üzerinde durulacaktır. Standartta birimlerin bağlantısını ve hareketliliğini sağlamak üzere birbirileri ile etkileşim halinde olan bileşenler tanımlanmıştır. Bunlar şu şekilde sıralanabilir

- Temel Hizmet Birimi (**B**asic **S**ervice **S**et) (BSS)
- Bağımsız Temel Hizmet Birimi (**I**ndependent **B**asic **S**ervice **S**et) (IBSS)
- Dağıtım Sistemi (**D**istribution **S**ystem) (DS)
- Genişletilmiş Hizmet Birimi (**E**xtended **S**ervice **S**et) (ESS)

Bunları sırayla tanıtmak anlaşılırlık açısından faydalı olacaktır.

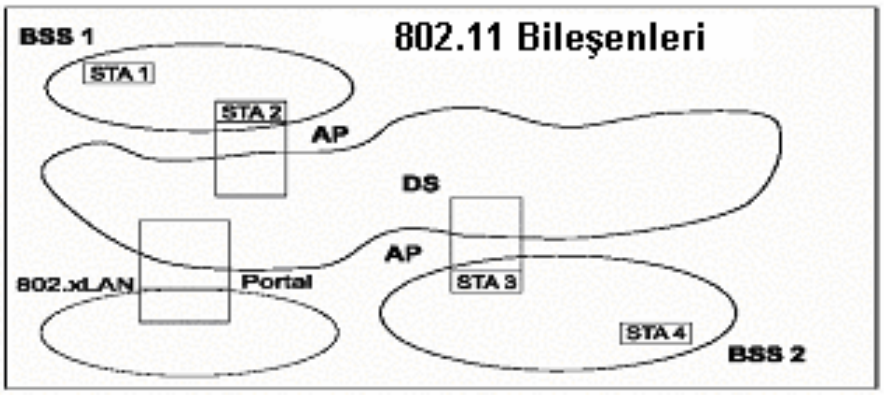
BSS, ortama erişim için aynı yöntemi kullanan istasyonlar kümesidir. En küçük hizmet birimini oluşturmaktadır. Aynı BSS içindeki istasyonlar BSS içinde kalmak koşulu ile hareket edebilirler ancak başka bir BSS'e ait istasyonlar ile direkt olarak iletişim kuramazlar.

IBSS'de aynı BSS gibidir, benzer ve birbirileri ile neredeyse örtüşen tanımları mevcuttur. IBSS hiçbir şekilde bir omurgaya (Ethernet gibi) bağlı değildir.



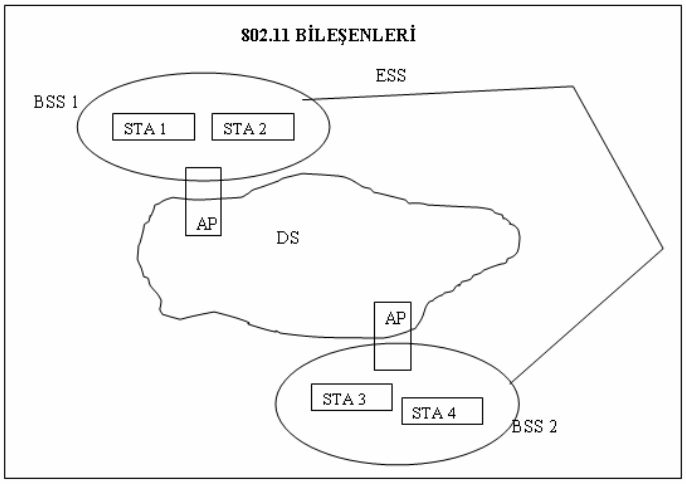
Şekil 4.1 BSS

DS, BSS'leri bir mevcut omurga ağ gibi birbirilerine bağlayarak ESS oluşturulmak için tanımlanmış sistemdir. Kablosuz yerel alan ağlarının çok özel bir yanı bu noktada ortaya çıkmaktadır. Kablosuz ağ yapıları geleneksel ağ yapıları ile ara yüz oluşturacak bir cihaz ile geleneksel ağ yapılarına bağlanabilirler ve böylece kablosuz ağ kullanıcıları geleneksel ağ sisteminin sağladığı servislere de ulaşabilirler. Burada DS, IEEE tarafından tanımlanmış bir yapı ise (Ethernet gibi, IEEE 802.3 Standardı ile tanımlıdır) burada ara yüz oluşturan cihaz (mantıksal noktanın) daha öncede belirtildiği üzere erişim noktasıdır. Ancak DS'nin IEEE tarafından tanımlanmamış bir ağ yapısı olması durumunda ara yüz oluşturan mantıksal nokta "portal" ismini almaktadır.



Şekil 4.2 DS ve BSS'lerin birleştirilmesi

ESS, birden fazla BSS ve DS bileşenlerinden oluşmuş geniş ölçekli ağ yapısıdır. BSS'ler birbirine DS aracılığı ile bağlıdır.



Şekil 4.3 ESS

Standart ayrıca hareket yeteneklerine göre üç tip istasyon tanımlaması yapmıştır. Bunlar şu şekilde sıralanmaktadır.

- Geçişsiz
- BSS Geçişli
- ESS Geçişli

Geçişsiz olarak tanımlanan istasyon türü sadece kendi bulunduğu BSS içinde kalabilmekte ve o BSS'in istasyonları ile iletişim kurabilmektedir.
BSS geçişli istasyon ise bir ESS içindeki BSS'ler arasında hareket edebilmektedir.
ESS geçişli istasyon ise adından da anlaşılacağı üzere farklı ESS'lerin BSS'leri arasında geçiş yapabilir ancak standart bu noktada bağlantının sürekliliği için tam bir garanti vermemektedir.

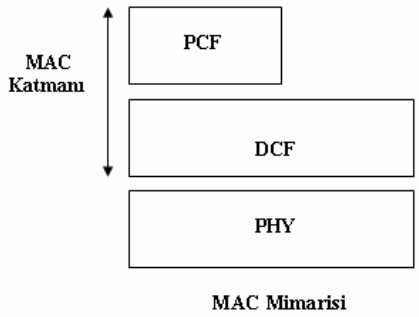
3.4 IEEE 802.11 Kablosuz Yerel Alan Ağı Standardı Mimarisi

IEEE 802.11/b Standardı, kablosuz yerel alan ağı sistemlerinde yerine getirilen işlemlerin tanımlandığı katmanlı yapıdan oluşmaktadır. Bu katmanlar temel olarak olarak iki adettir. Bunlar

- Fiziksel Katman (**Phy**isical Layer) (PHY)
- Ortam Erişim Katmanı (**M**edium **A**ccess **C**ontrol) (MAC)

katmanlarıdır. Bu katmanlar OSI referans modelinin alt katmanlarına karşı gelmektedir. Standardının geleneksel ağ standartlarından ayrılan yanı hareketliliğe destek vermesi ve güvenlik konularını içermesidir. Çünkü kablosuz yerel alan ağlarında iletim ortamı haberleşme için oldukça güçlükler yaratan hava ortamıdır ve burada güvenlik sorunları ortaya çıkmaktadır. Ayrıca bant genişliği ayarları ve frekans ayarlamaları da ayrı birer güçlük yaratmaktadır. Standard tüm bu sorunlara çözüm getirmiştir.

Bu katmanların detaylı olarak incelenmesi sistemin çalışma prensibinin anlaşılması açısından oldukça önemlidir. Bu aşamadan sonra bu katmanlar teker teker incelenecektir.



Şekil 4.4 IEEE 802.11/b Standardı Mimarisi

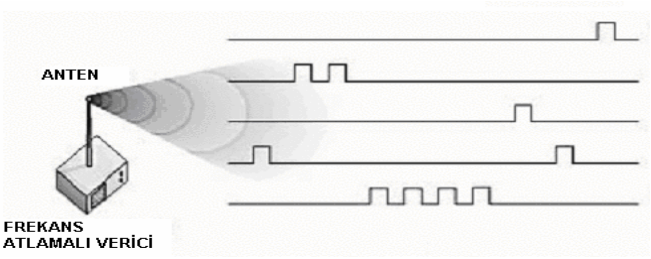
3.4.1 Fiziksel Katman

IEEE 802.11/b standardında hava ortamında 3 tip iletim tekniği tanımlanmıştır. Sistemlerinde kullanılacak cihazlarda bu üç iletim tekniğinden birine destek verecek şekilde üretirler. Buna genellikle cihazın desteklediği modülasyon tipi denir. Ayrıca her biri başlı başına birer güvenlik tedbiridir. Bu teknikler aşağıdaki gibi sıralanabilirler.

- Frekans Atlamalı Yayılı Spektrum (**F**requancy **H**opping **S**pread **S**pectrum) (FHSS)
- Direkt Dizi Yayılı Spektrum (**D**irect **S**equance **S**pread **S**pectrum) (DSSS)
- Infrared (IR PHY)

Görüldüğü üzere kablosuz yerel alan ağı sistemlerinde yayılı spektrum tekniği kullanılmaktadır. Yayılı spektrum tekniği askeri amaçlarla geliştirilmiş bir güvenlik önlemidir. Bu teknikte sinyal geniş bir banda yayılır ve böylece kestirilmesi güçleşir ayrıca gürültüye karşı daha az duyarlı hale getirilmiş olur.

FHSS ; iletim tekniğinde veri paketlere bölündükten sonra paketler zaman içinde taşıyıcı frekansı zamana bağlı olarak değişen bir verici kullanılarak iletilir. Yani esas verinin zaman içinde iletilirken farklı frekanslarda iletildiği söylenebilir. Bu sistemde alıcının verici ile eş zamanlı olarak çalışması gerektiği açıktır ve bu sebeple bazı senkronizasyon mesaj ve teknikleri kullanılmaktadır. Bu teknik daha öncede belirtildiği gibi veriyi daha güvenli ve girişime karşı daha az duyarlı hale getirir.

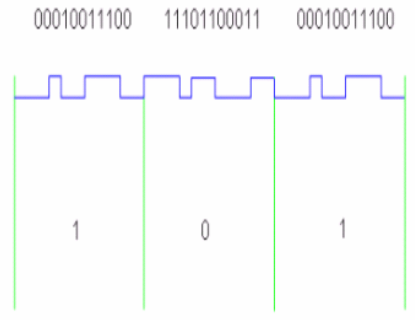


Şekil 4.5 FHSS tekniği ile çalışan verici

Bu teknik ile veri iletimi yapılırken frekans atlama sırası bir algoritmaya göre belirlenmektedir. Ayrıca frekans atlaması yapılabilecek kanalların sayısı ülkeden ülkeye değişebilmektedir. Çünkü ülkeler 2.4 GHz bandı civarını kendileri tahsis ederler. Ayrıca atlama yapılabilecek kanal seçilimi yapılırken harmonik distorsiyon etkisi de göz önüne alınmaktadır. Her bir kanalın genişliği 1 MHz olup saniyede yapılacak atlama sayısı da yine otoriteler tarafından belirlenir, standartta bu konu ile ilgili bir rakam verilmemiştir. FHSS tekniğinde kullanılan modülasyon tekniği GFSK (**G**aussian **F**requancy **S**hift **K**eying) olarak tanımlanmıştır.

Direkt Dizi Yayılı Spektrum ;Bu teknik ile veriler gönderilirken her bir bit (1 veya 0), bir bit dizisi ile temsil edilerek iletilir. Böylece verinin daha güvenli iletimi sağlanmış olur ve iletilen işaret girişime duyarlılığı daha aza indirgenmiş olur. Standartta minimum 11 bit ile temsil edilmesi önerilmiştir.

Şu durum tekniğin avantajının açıklanması için yararlı bir örnek olabilir. Eğer havada bir bit iletiyorsak onu kaybettiğimiz zaman ne olması gerektiğini kestirmemiz oldukça zor olacaktır. Ancak bu bit, bir bit dizisi ile iletilmiş olsa ve bu diziden bir bit kaybetmiş olsak bunun 1 yada 0 mantıksal değerlerinden hangisine karşılık geleceğini kestirmemiz oldukça kolay olacaktır.



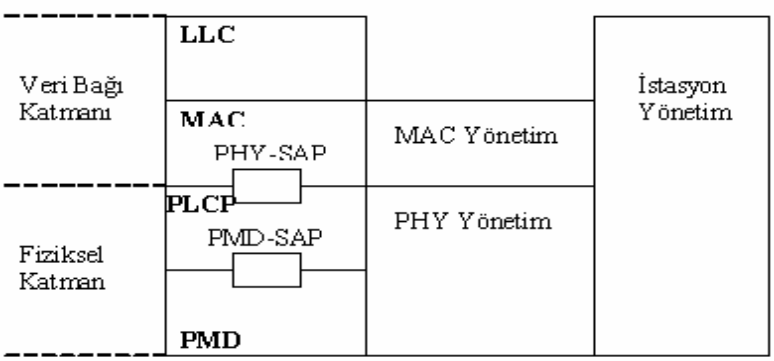
Şekil 4.6 DSSS tekniği ile veri iletimi

Bu teknikte kullanılan modülasyon teknikleri DBPSK (**D**ifferential **B**inary **P**hase **S**hift **K**eying) ve DQPSK(**D**ifferential **Q**uadrature **P**hase **S**hift **K**eying) olarak tanımlanmıştır.Infrared ;IEEE 802.11/b Standardı tarafından elektromagnetik dalgalar ile iletime alternatif olarak tanımlanmış bir yöntemdir, bunun sebebi bazı özel uygulamalarda avantaj sağlamasıdır. İletimde, dalga boyları 850 – 900 nm arasında değişen infrared ışığı kullanılır. Burada tanımlanan sistemde genellikle infrared ışığın yansımasından yararlanılarak iletim hedeflenmiştir. Böylece cihazların birbirilerinin görüş alanı içerisinde olma zorunluluğu ortadan kalkmış olmaktadır.

Fiziksel Katmanının ve Alt Katmanlarının incelenmesi

Her PHY Katmanı kendi içinde katmanlı yapıdan oluşur ve hava ortamında yapılacak işlemleri tanımlar. En temelde üç işlem tanımlar, bunlar, ortamı dinleme, alma, gönderme işlemleridir. PHY katmanının alt katmanları şunlardır. (Ortamı dinleme işleminin gerekliliğinden MAC katmanı incelenirken detaylı bir şekilde bahsedilecektir, bu aşamada sadece isim olarak bilinmesi yeterli olacaktır)

- Fiziksel Katman Uyumluluk Protokolü (**P**HY **L**ayer **C**onvergence **P**rotocol) (PLCP)
- Fiziksel Katman Ortam Bağı Protokolü (**P**HY **M**edium **D**ependent Protocol) (PMD)
- Fiziksel Katman Yönetim Alt Katmanı (PHY Menagement Sublayer)



Şekil 4.7 PHY ve Alt Katmanları

Bu üç alt katmanın incelenmesi anlaşılırlığı arttıracaktır.

PLCP alt katmanında paket yapılır. Bir üst katman olan MAC katmanından bilgi geldiği zaman paketler hazırlanır. PLCP ayrıca gelen paketlerin MAC katmanına ulaşmasını sağlar. PLCP'nin en temel görevi MPDU (**M**AC **P**rotocol **D**ata **U**nit) isimli veri paketlerinin PMD üzerinden gönderilecek mekanizmayı oluşturmasıdır. Şekilde görülen SAP (**S**ervice **A**ccess **P**oint) isimli yapılar ise katmanların birbirileri arasındaki iletişimi sağlarlar.

PMD alt katmanının görevi ise sinyalleşme için modülasyon ve kodlama tekniğinin belirlenmesidir. PLCP'nin kontrolü altında, PMD birimler arasında fiziksel katman bileşenlerinin kablosuz ortam üzerinden alınmasını ve gönderilmesini sağlar. Modülasyon ve demodülasyon işlemleri bu katmanda yapılır. PMD paketlerin başlık kısımlarındaki bilgiden ne tür modülasyon kullanacağına karar verir.

PHY yönetim alt katmanı adından da anlaşılacağı üzere bu katmanın yönetimini üstlenen katmandır. PHY türleri için gerekli kanal ayarlamaları burada yapılır.

3.4.1.1 Fiziksel Katmanının İşlevleri

Daha öncede belirtildiği gibi PHY katmanını üç temel işlevi vardır. Bunlar

- Ortamı dinleme
- Gönderme
- Alma

olarak sıralanırlar.

Ortamı dinleme işlemi PMD tarafından gerçek olarak yerine getirilir (bu iş MAC katmanında sanal olarak yerine getirilir). PLCP ise bu işi gelen sinyalleri inceleyerek yapar ve istasyonun alımda yada gönderimde olduğuna karar verir.

Gönderme fonksiyonunda PLCP, PMD ve MAC katmanları birlikte çalışırlar. PLCP, MAC katmanından emir alınca PMD'yi gönderme moduna geçirir. MAC katmanı oktet sayısı ve veri hızını içeren bilgiyi gönderir. PMD antenden gönderme yapar. Gönderme başarılı olduğunda PLCP MAC katmanına bir mesaj gönderir ve vericiyi kapatıp PMD'yi alma moduna geçirir.

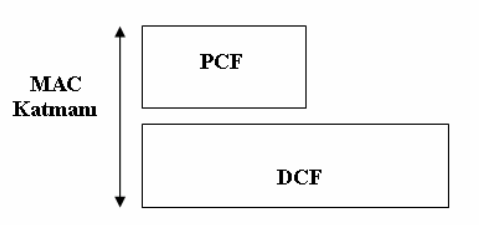
Alma fonksiyonunda ise yine aynı birimler rol alır. PLCP ortamı dinlerken geçerli bir başlık alırsa sonrasında gelen başlığı da inceler ve PLCP MAC katmanını gelen sinyal olduğuna dair uyarır. PLCP son okteti alırken yine MAC katmanını iletimin bitmek üzere olduğuna dair uyarır.

3.4.2 Ortama Erişim Kontrolü Katmanı

MAC Katmanı adından da anlaşılacağı üzere ortama erişimi düzenleyen katmandır. Katmanın en önemli üç görevi güvenli veri iletimi,erişim kontrolü ve güvenliktir.
Bu katmanda kendi içinde iki alt katmandan oluşmaktadır. Bu iki alt katman aşağıda verilmiştir.

- DCF (**D**istributed **C**oordination **F**unction)
- PCF (**P**oint **C**oordination **F**unction)

MAC katmanının katmanlımimarisi aşağıdaki şekilde mevcuttur.



Şekil 4.8 MAC Katmanının alt katmanları

DCF her türlü trafiğin kapışmalı bir şekilde akmasına izin veren ve CSMA/CA (**C**arrier **S**ense **M**ultiple **A**ccess with **C**ollission **A**voidence) algoritması kullanan bir yapı tanımlamaktadır.
PCF ise zamana duyarlı verilerin bir PC (**P**oint **C**oordinator) kontrolü altında kapışmasız olarak akmasına izin veren bir yapı tanımlar.
Bu iki alt katmanın incelenmesi anlaşılırlığı arttıracaktır.

3.4.2.1 DCF Alt Katmanı

DCF'nin temel fonksiyonu kablosuz ortamın istasyonlar arasında otomatik olarak kapışmalı ve çarpışmayı azaltacak şekilde kullanımını sağlamaktır. CSMA/CA olarak da bilinir.

CSMA/CA algoritması çarpışmayı en aza indirgemek için tanımlanmıştır. Özellikle ortamdaki iletim bittiği anda birden fazla istasyon ortamın kontrolünü almak isteyecektir ki bu en kritik zaman dilimidir. İşte bunun için CSMA/CA algoritması bir "backoff" zamanı tanımlamıştır. Her istasyon kendine rasgele bir backoff zamanı üreterek ortamı bu ek süre içinde dinler. Algoritmanın temelinde ortamı dinleme, boş ise veriyi iletme, değil ise boşalana kadar bekleme mantığı yatmaktadır. DCF katmanında ortamı dinleme işlemi, PHY Katmanına karşılık, sanal olarak yapılır. Bu sanal olarak dinleme işlemi ise kanal rezervasyonu ile yapılmaktadır. Bu konuları detaylı olarak incelemek yaralı olacaktır. Ancak bundan önce anlaşılırlığı arttırması açısından bu alt katmanda kullanılan bazı mesajların kısa tanımlarını vermek faydalı olacaktır.

Gönderim İsteği Mesajı (**R**equest **T**o **S**end) (RTS) : Bu mesaj türü gönderici istasyon tarafından gönderilir ve hedef istasyon adresini içerir. Adından da anlaşılacağı üzere gönderim isteğini belirtmektedir. Ayrıca beklenen iletişim zamanı bilgisinide içerir ve kanlın ne kadar bir süre ile kullanılacağını belirtir yani kanal rezervasyon bilgisi içerir.

Alıma Hazır Mesajı (**C**lear **T**o **S**end) (CTS): Bu mesaj türü hedef istasyon tarafından RTS alındıktan sonra gönderilir ve alıma hazır olunduğu bilgisini içerir. Ayrıca bu mesajda kanal rezervasyonu bilgisini içerir.

Alındı Onay Mesajı (**Ack**nowledgment) (ACK): Bu mesaj da yine hedef istasyon tarafından gönderilir ve verinin doğru bir şekilde alındığını teyit eder ayrıca ACK mesajı da yine kanal rezervasyon bilgisi içerir.Bu mesaj türlerinin dışında anlaşılırlığı arttırmak için bazı zaman türlerinden bahsetmek uygun olacaktır. Bu zaman türleri istasyonların ortama erişime kalkışmadan önce beklemeleri gereken zamanlardır. Bu zamanlar üstünlük yaratmak için kullanılırlar. En kısa süre bekleyenin kanala erişim açısından en üst mertebede olacağı açıktır. Bu zaman türlerine IFS (**I**nter **F**ame **S**pace) denilmektedir. Bu zaman türleri aşağıdaki gibi, en kısadan en uzuna doğru şöyle sıralanırlar:

Kısa IFS (**S**hort **IFS**) (SIFS): En kısa bekleme zamanıdır ve acil cevap gerektiren öncelikli durumlarda kullanılır (RTS alındığı zaman CTS göndermek için gibi).

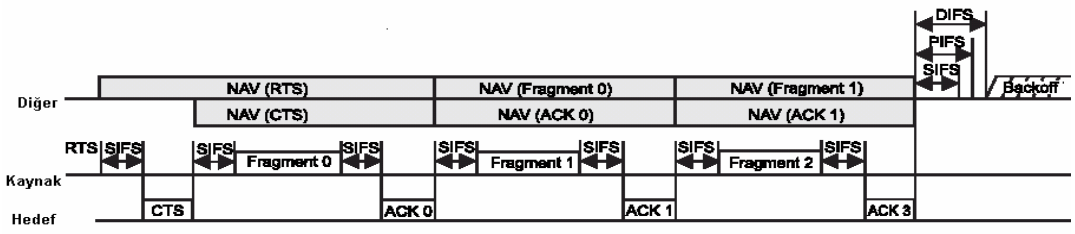
PIFS (**P**oint Coordinator **IFS**): En kısa ikinci zamandır. PC tarafından kullanılır. CFP (**C**ontention-**F**ree **P**eriod) (kapışmasız zaman aralığı,yönetimi PC yapar) zamanında kullanılır.

DIFS (**D**istirbuted Coordination Function **IFS**) : En kısa üçüncü zamandır. Adından da anlaşılacağı üzere yönetimin CSMA/CA algoritmasına göre yapıldığı yani CP (**C**ontention **P**eriod) (kapışmalı erişim zamanı) zamanında kullanılır.

Burada PIFS ve DIFS zamanlarına bakacak olursak PCF'nin DCF'ye göre daha öncelikli olduğu görülür. Yani eğer PC isterse tüm DCF trafiğini kesebilir bunu önlemek için "superframe" zamanı tanımlaması yapılmıştır. Superframe iki kısımdan oluşur ve birinci zaman diliminde kanal yönetimi PC'dedir ve kapışmasız trafik akar kanalda. İkinci zaman aralığında ise kapışmalı zaman aralığıdır ve CSMA/CA algoritması kullanılır.Genişletilmiş IFS (**E**xtended **IFS**)(EIFS): Bu zaman aralığı hata oluşması durumunda kullanılır.

- **Ortamı Dinleme Mekanizması**

Bu mekanizma sanal olarak gerçekleştirilir. İletim ortamında iletim olup olmadığının incelenmesidir. Bu mekanizmada NAV (**N**etwork **A**llocation **V**ector) kullanılır. Daha öncede belirtildiği gibi RTS, CTS ve ACK mesajları kanal rezervasyon bilgileri içerirler ve bu mesajlar tüm istasyonlar tarafından alınır ve hedef istasyon dışındaki istasyonlar bu bilgiye göre kendi NAV değerlerini üretirler. NAV belli bir değerden sıfıra doğru sayma yapan bir sayıcı olarak düşünülebilir. NAV değeri sıfır olduğunda istasyon kanala erişim için gerekli prosedürleri uygulayabilir ancak aksi durumunda istasyon bekleme konumundadır ve sadece kanalı dinler.

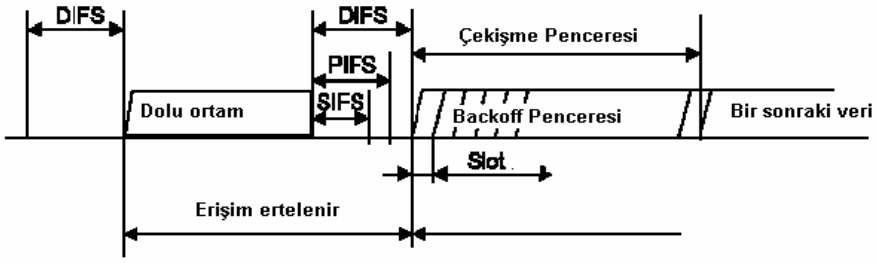


Şekil 4.9 NAV Kullanımı

Yukarıdaki şekilde de görüldüğü üzere RTS, CTS ve ACK mesajlarından bilgiyi alan hedef ve gönderici istasyonlar dışındaki istasyonlar NAV değerlerini yenilerler ve bu süre boyunca iletime geçmezler.Bu işlem kanalın sanal olarak dinlenmesidir ve verilerin havada çarpışma riskini azaltmak için kullanılır.

- **Ortama Erişim Metodu**

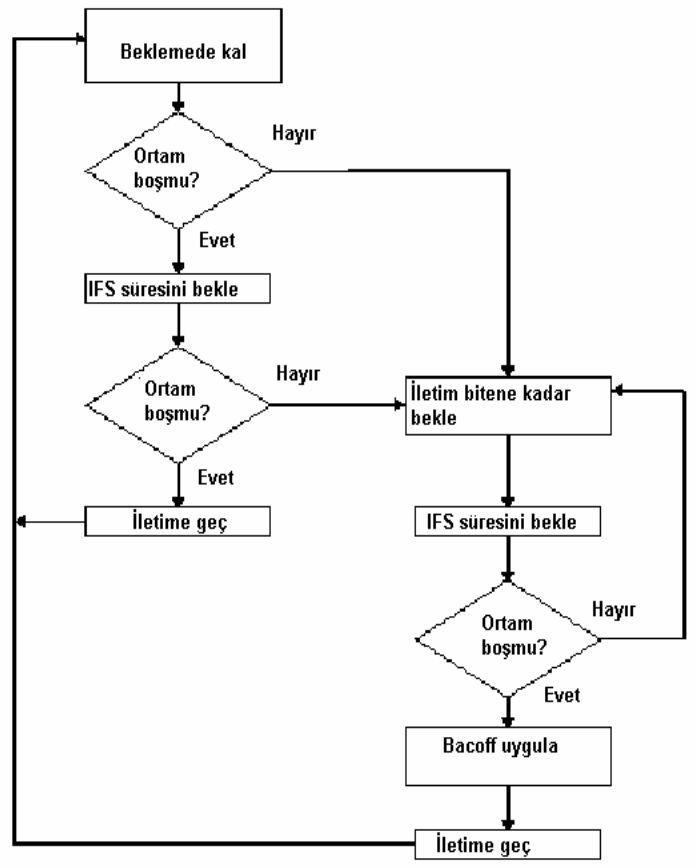
Ortama erişim ile ilgili daha öncede söylendiği gibi, kullanılan teknik, kanalın dinlenmesi, boş ise iletime geçilmesi, aksi durumda kanal boşalana kadar beklenmesi temeline dayanmaktadır. Bunu detaylı olarak incelemek anlaşılırlığı arttıracaktır.



Şekil 4.10 Temel Erişim Metodu

Yukarıdaki şekil ve aşağıdaki algoritma incelenecek olursa ortama erişimin şu şekilde olduğu anlaşılır.İletecek verisi olan istasyon ortamı dinler eğer ortam boş ise IFS süresi kadar daha ortamı dinler eğer ortam hala boş ise verisini gönderir. Eğer ortam dolu ise mevcut iletim bitene kadar bekler ve tekrar bir IFS süresi kadar daha ortamı dinler eğer ortam boş ise rasgele bir "backoff" zamanı üretir ve bu zaman dolduğunda ortamda boş ise iletime geçer.

Buradan çıkartılacak sonuç backoff prosedürünün dolu ortam durumundan sonra uygulamaya sokulmasıdır. Ayrıca yukarıdaki şekilde backoff prosedüründe zaman dilimlerinin bulunduğu görülmektedir. İstasyon bu her bir zaman diliminde de ortamı dinler ve boş olması durumunda değerini azaltır ve değer sıfır olunca iletime geçer. Eğer ortam dolu ise değerini askıya alır.
Ayrıca algoritmadaki IFS zamanlarını önceden tanımlanmış dört adet IFS zamanından herhangi biri olabileceği unutulmamalıdır.



Şekil 4.11 Temel Ortam Erişim Algoritması

MAC katmanında hatalı veya fazla veri iletimleri gerçekleştirilebilir. Bu nedenle hata kurtarma önemli bir işlemdir. Hata kurtarma, iletişimi başlatan istasyonun sorumluluğundadır. Hata tespiti durumunda istasyon başarılı iletim veya tekrar deneme limitine ulaşana kadar, veri tekrar iletilmeye çalışılır.

Ayrıca MAC katmanında çok etkin bir veri iletim mekanizması da mevcuttur. Bu RTS, CTS ve ACK mesajlarını ve SIFS zamanını kullanarak sağlanır.Yukarıda anlatılan tüm bu işlemler MAC katmanını güvenli veri iletimi, erişim kontrolü ve güvenlik işlemlerini nasıl yerine getirdiğini açıklamaktadır ve sistemin CP esnasındaki çalışma mantığını açıklamaktadır.

3.4.2.2 PCF Alt Katmanı

PCF katmanı daha öncede belirtildiği üzere DCF katmanının üzerinde yer almaktadır ve kapışmasız (CFP) iletime olanak sağlamaktadır. Ortama erişim ve ortamda dolaşan verinin bir yönetici tarafından (PC) yönetilmesine dayanan bir sistemdir. Bu işleme "polling" denir ve PC tarafından yapılır, PC ise erişim noktası içinde yer almaktadır.

Polling işlemi iletişim sırasında uç birimlerin iletime hazır olup olmadıklarının ve uç birimlere iletişim için izin verilmesi işlemi olarak tanımlanabilir. PC polling işlemi sırasında, daha öncede belirtildiği üzere, PIFS ek bekleme zamanını kullanmaktadır. Ortama erişim PC'nin kullandığı polling algoritması ile yapılır. Tüm veriler PC'nin üzerinden geçtikten sonra hedeflerine ulaşırlar.

PC her CFP başında bir "beacon mesajı" gönderir ve tüm istasyonlara CFP'nin başlamış olduğunu bildirir ve istasyonlar NAV değerlerini ayarlarlar ve ortama erişme girişiminde bulunmazlar. Beacon mesajı ayrıca erişim noktasının saat bilgisinide içerir ve senkronizasyonda rol alır.

CFP zamanında istasyonlar CF-pollable ve non-CF-pollable olarak önceden ayarlanabilirler. CF-pollable istasyonlar CFP zamanı içinde DCF'de olduğu gibi RTS/CTS mekanizmasını kullanmazlar. Eğer iletim sırasında adreslenmiş istasyon non-CF-pollable ise bu istasyon cevap verirken DCF'nin prosedürlerini uygular.

- **Temel Ortama Erişim Prosedürü**

CFP başlamadan önce PC ortamı PIFS süresi ile dinler ve ortama bir "beacon mesajı" gönderir. Bu mesajı alan tüm istasyonlar kendi NAV değerlerini ayarlar ve CFP'nin sonuna kadar ortama erişme girişiminde bulunmazlar. PC daha sonra en az bir SIFS süresi kadar bekledikten sonra CFP zamanında kullanılan veri tiplerinden birini gönderir. Bu veri tipleri konunu anlaşılırlığını arttırdığından ileride tanımlanmışlardır. Her CFP'nin bitiminde PC bir CF-End mesajı gönderir ve CFP'nin bittiğini tüm istasyonlara bildirir ve bu mesajı alan istasyonlar NAV değerlerini sıfırlarlar. Herhangi bir hata oluşması durumunda PC iletime kaldığı yerden devam eder.

3.4.2.2.1 CFP Zamanında kullanılan veri tipleri

Data : PC'den veri göndermek için kullanılır

Data + CF-ACK : PC'den veri göndermek için kullanılır ve bu durumda önceden onaylanması gereken bir veri alınmıştır.

Data + CF-Poll : PC'den veri gönderileceği ve bir sonraki göndericinin adreslenmiş bir istasyon olacağı durumda gönderilir.

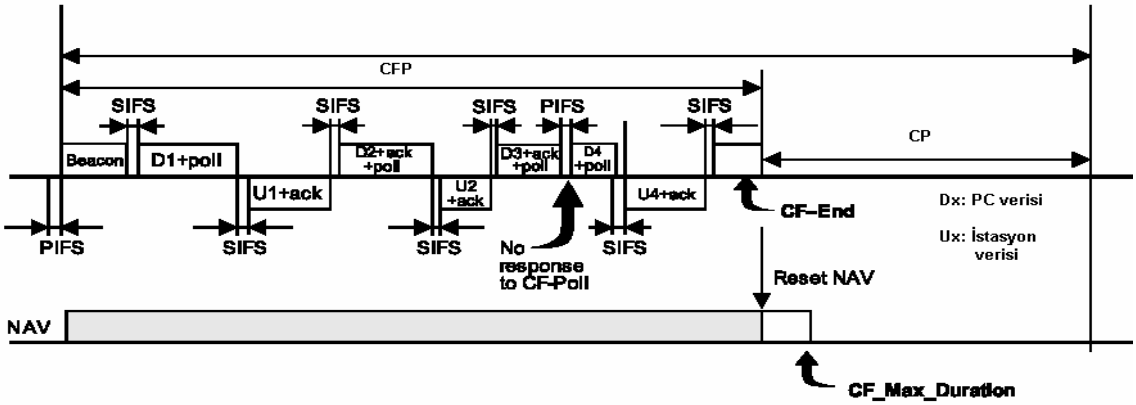
Data + CF-ACK + CF-Poll : Hem öncesinde onaylanması gereken bir verinin alınmış ve bir sonraki göndericinin adreslenmiş bir istasyon olması ve PC'nin veri göndereceği durumda kullanılır.

CF-Poll : Bir sonraki göndericinin adreslenmiş bir istasyon olacağı ve PC'nin gönderecek bir verisi olmadığı durumlarda kullanılır.

CF-ACK + CF-Poll : Önceki iletimde onay gerektiren bir veri gönderilmiş ve bir sonraki göndericinin adreslenmiş bir istasyon olacağı ancak PC'nin gönderecek bir verisi olmadığı durumlarda kullanılır.

CF-ACK : PC'nin adresleme yapmadığı veya veri göndermediği ancak önceki iletimde onay gerektiren bir verinin alındığı durumlarda kullanılır.

Yukarıda tanımlanmış durumlar altında gönderilen mesajlar tanımlanmıştır ve tüm yönetim PC tarafından yapılmaktadır. Uygun durumlar altında uygun mesajlar gönderilir. Adresleme işlemi PC'nin bir istasyonu iletime davet etmesi veya ona veri göndermesi yani iletişime geçmesidir.



Şekil 4.12 CFP Zamanında Örnek İletim

Yukarıdaki örnek iletim şeklinde görüldüğü üzere bir beacon mesajı gönderilmiş ve CFP zamanı oluşturulmuştur. Daha sonrasında ise PC hedef istasyonu Data + Poll mesajı iletime davet etmiş ve veri göndermiştir. İstasyonda PC'ye SIFS zamanı içinde cevap vererek iletime geçmektedir ve CFP sonunda PC bir CF-End mesajı göndererek CFP'nin bittiğini bildirmiş ve CP başlamıştır. Şekilde dikkat edilirse CFP'nin PIFS zamanı beklenerek başlatıldığı görülür buda PC'nin neden tüm CP trafiğini kesebileceğinin sebebidir.

Aynı alanda birden fazla PC'nin yönetimi altında çalışan BSS'ler örtüşüyor olabilir bu durumda girişim riski artmaktadır. Bu sorunun önüne geçilebilmesi için PC'ler CFP zamanına başlamadan önce bir backoff prosedürü uygulayabilirler.

Bu aşamada IEEE 802.11/b standardının katmanlı yapısı incelenmiş oldu ve sistemin çalışma prensibi ile ilgili bilgiler verilmiş oldu. Bu aşamadan sonra sistemde kullanılan paket yapılarını incelenmesi ile IEEE 802.11/backoff Standardı konusu bütünlük kazanacaktır.

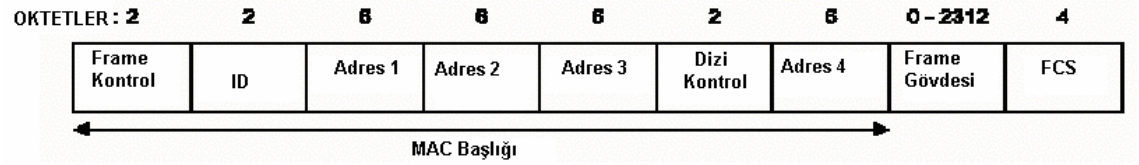
3.5 Kullanılan Paket Yapıları

Her sistemde olduğu gibi kablosuz yerel alan ağları sistemininde kendine özgü iletimde kullanılan paket yapıları vardır. Veriler hava ortamında iletilirken paketler halinde iletilir. Üç tip paket yapısı vardır.Bunlar

- Yönetim paketleri
- Veri paketleri
- Kontrol paketleri

şeklindedir.

MAC katmanında kullanılan paket yapılarının genel formatı aşağıdaki şekilde verilmiştir.

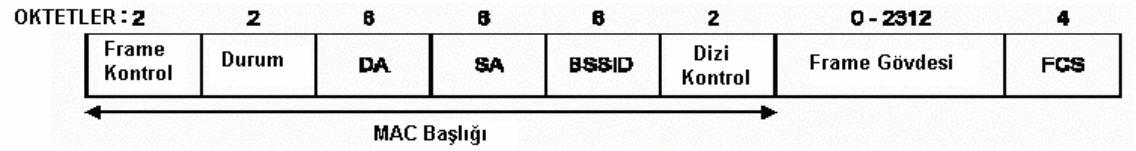


Şekil 4.13 Genel Paket Yapısı

Frame kontrol kısmı paketin genel yapısı ile ilgili bilgiyi yani ne tür bir paket olduğu bilgisini ve iletim esansındaki kontrol bilgilerini taşır.ID boşluğu iletimin ne kadar süreceği bilgisi içerir. Bu bilgi daha önceki bölümlerde de belirtildiği üzere kanal rezervasyonu yapılabilmesi için kullanılır. Adres boşlukları ise bulunan durumlara göre farklı adresleri temsil edebilirler. Yerine göre hedef, kaynak veya transfer eden istasyonların adreslerini temsil edebilirler.

Dizi kontrol boşluğu alıcı ve verici istasyonlar arasında transfer edilen verilerin miktar ve sırası ile ilgili bilgiler içerir. Bu bilgiler kopya mesaj alınması durumunda kullanılan bilgilerdir.Frame Gövdesi boşluğu ise uzunluğu değişebilen ve bağımsız paketlerin türünü belirten kısımdır. FCS (Frame Check Sequance) kısmı ise paketin kendi içinde bütünlüğünü kontrol eden kısımdır. Konunu anlaşılırlığının arttırılması açısından yukarıda belirtilen üç genel paket yapısının tanıtılması faydalı olacaktır.

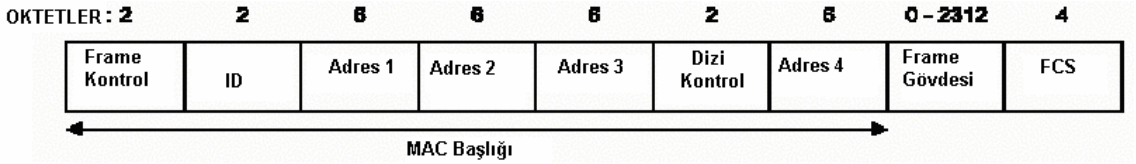
Yönetim Paketleri : Erişim noktaları ve istasyonlar arasında başlangıç bağlantısı kurulurken bu paketler kullanılır. Yönetim paketlerinin genel yapısı aşağıdaki şekilde verilmiştir.



Şekil 4.14 Yönetim Paketlerinin Genel Yapısı

Buradaki frame kontrol ve durum kısımlarından yukarıda bahsedilmişti. Genel paket yapısındaki adres boşlukları burada kaynak (SA) ve hedef istasyon (DA) adresleri olmuştur. Eğer bir istasyon aldığı paketin kaynak adresi kısmı ile kendi adresini eşleştirirse mesajın tamamını kabul eder aksi halde mesajı reddeder. Frame gövdesi kısmının yapısına göre ise alt yönetim paketlerinin türleri belirlenir. Bunların arasında beacon, izin vb. paketler gösterilebilir.

Veri Paketleri : Veri paketleri adında da anlaşılacağı üzere veri taşımada kullanılırlar. Genel veri paket yapısı aşağıdaki şekilde verilmiştir.



Şekil 4.15 Genel Veri Paketi Yapısı

Kontrol Paketleri : Kontrol paketleri güvenli veri iletimi için kullanılan paketlerdir. Bu paketlerin kullanımından MAC ve PCF katmanlarında bahsedilmiştir. Bunlar arasında en önemlileri RTS, CTS ve ACK gösterilebilir. Ayrıca PCF katmanında kullanılan ACK ve Poll uzantılı paketlerde kontrol paketleridir.

Bu bölüme kadar IEEE 802.11/b Standardı ve sistemin genel çalışma prensibi, paket yapıları ve tipik işlemler tanıtılmıştır. Bunlar okuyucuların sistem ile ilgili yeter seviyede genel bilgi edinmesi için yeterlidir.

3.6 IEEE 802.11/b Kablosuz Yerel Alan Ağları Standardındaki Güvenlik Uygulamaları

Kablosuz yerel alan ağı sistemlerinin iletim ortamı havadır ve havada verilere ulaşmak oldukça kolaydır. Bu sebeple kablosuz iletişimin her türünde güvenlik konusu oldukça sıkı sorgulanan bir kavramdır. Özellikle kablosuz yerel alan ağları gibi büyük ölçekli firmalarında kullandığı sistemlerde bu oldukça titiz bir şekilde sorgulanır çünkü hiçbir firma ve/veya kimse hassas bilgilerinin başkası tarafından elde edilmesini istemez. Ayrıca cihazlar 2.4 GHz frekansında çalışmaktadır ve bunun sonucunda radyo dalgaları duvarlardan penetre edebilmektedir böylece verilerin komşu bir odadan dinlenmesi olası bir durumdur.

IEEE Kablosuz Yerel Alan Ağları Standardında en temel güvenlik önlemleri FHSS, DSSS ve IR iletim tekniklerinden kaynaklanmaktadır. Ancak standart dışında pratikte kullanılan güvenlik tedbirleri de mevcuttur ve bu bölümde ikisi üzerinde de durularak tam bir görüş oluşturulmaya çalışılacaktır[12]

FHSS iletim tekniğinde daha önce de değinildiği üzere paketlere ayrılmış veri zamanın fonksiyonu olarak farklı frekanslarda gönderilmektedir. Gönderme işlemi ise belirli bir algoritmaya göre yapılmaktadır. Yani sistemden izinsiz olarak veri almak isteyen bir kimse tüm bu bilgileri bilerek, atlama algoritmasına göre doğru zamanda doğru frekansta bulunmalıdır ki bu oldukça zor bir işlemdir.

DSSS tekniğinde ise 1 ve 0 bitlerinin farklı bit dizileri ile temsil edildiği ve bu şekilde gönderildikleri belirtilmişti. Buda bir şifreleme işlemi gibi düşünülebilir ve kestirimin güçleştiği görülebilir.

Infrared (IR) ile iletimde ise infrared ışığın penetrasyon özelliğinden dolayı kapsama alanı bir oda yada ofis ile sınırlı kaldığından bir güvenlik tedbiri oluşturur.

Bu temel güvenlik tedbirlerinin yanında standartta olan ve/veya pratikte uygulanılan güvenlik tedbirlerinin listesi aşağıda verilmiştir.

WEP (**W**ired **E**quivalent **P**rivacy)
Açık İzin Prosedürü
Paylaşılmış Anahtarlı İzin Prosedürü
EAP (**E**xtensible **A**utehntication **P**rotocol)
MAC Adresi Filtrelemesi
LEAP (**L**ightweight **E**xtensible **A**uthentication **P**rotocol)

WPA (**W**i-Fi **P**rotected **A**ccess)
SSID (**S**ervice **S**et **ID**entifier)

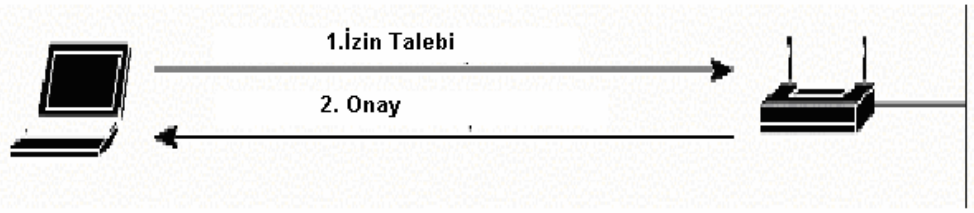
Bu güvenlik önlemlerinin tanıtılması anlaşılırlığı arttırmak için oldukça yararlı olacaktır.

3.6.1 Kabloluya Eşdeğer Gizlilik Protokolü

Kabloluya Eşdeğer Gizlilik Protokolü (WEP) standartta bulunan ve ağa atak yapacak kişilere karşı oluşturuluş ilk güvenlik tedbiridir. WEP, istasyon ve erişim noktası arasındaki verinin şifrelenmesidir. Erişim noktası ve istasyon radyo sinyallerini şifrelemek için aynı WEP şifresini kullanmaktadır. Ancak burada statik WEP şifrelemesi kullanılmamalıdır çünkü ağa atak eden kişi trafiği dinleyerek veriyi çözecekler hesaplar yaparak yeterli mesaj aldığında şifreyi çözebilmektedir. Bu sebeple EAP tarafından sağlanan dinamik WEP şifreleri kullanılmaktadır. 40, 128ve 356 bit kriptolama mevcuttur.

3.6.2 Açık İzin Prosedürü

Bu prosedür, herhangi bir kullanıcı ile erişim noktası arasında iletişim kurulmasına yönelik uygulanan bir prosedürdür. Burada cihazın ve erişim noktasının WEP şifreleri aynı olmalıdır. Buda standart bir prosedürdür ve sunucu tabanlı değildir.



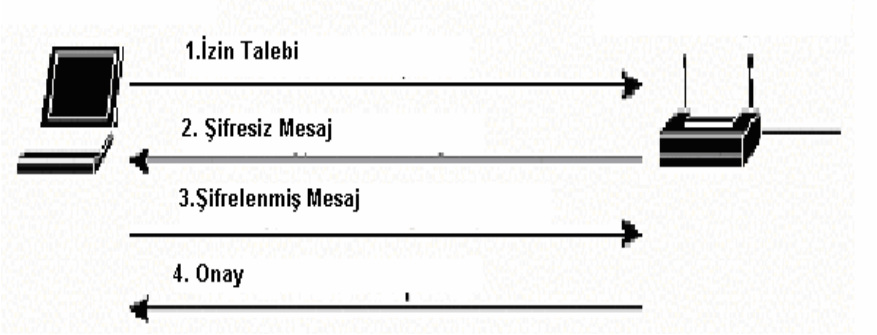
Şekil 4.16 Açık İzin Prosedürü

3.6.3 Paylaşılmış Anahtarlı İzin Prosedürü

Bu prosedürde standart bazlı ve sunucu tabanlı olmayan bir güvenlik tedbiridir. Bu açık izin prosedürüne göre daha güvenli gibi görünen bir izin prosedürüdür. Burada erişim noktası iletişim kurmak isteyen istasyona bir metin gönderir ve istasyon bunu ikisinde de ortak olarak bulunan şifre ile şifreleyip erişim noktasına geri gönderir. Erişim noktası

şifreli metni çözer ve ilk gönderdiği metin ile karşılaştırır. Eğer birbiri ile aynı ise iki metin erişim izni verilir, aksi durumda erişim izni verilmez

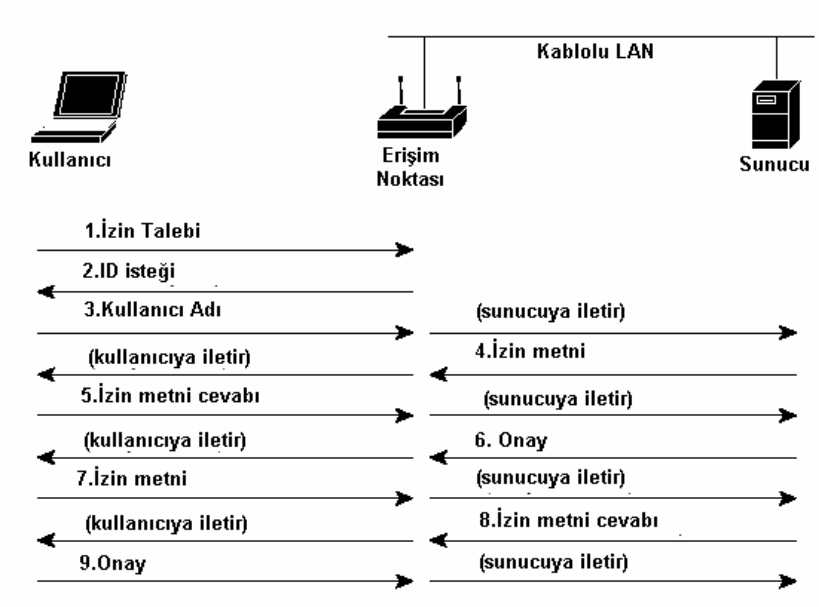
Bu prosedürün akış şemasından dolayı bu prosedür çokta güvenli sayılmaz. Çünkü açık ve şifreli metinde hava ortamında iletilmektedir ve bunları alan bir şifreyi çözebilir.



Şekil 4.17 Paylaşılmış Anahtarlı İzin Prosedürü

3.6.4 Geliştirilebilir İzin Protokolü

Geliştirilebilir İzizn Protokolü (EAP) tedbiri ağa erişimde yüksek güvenlik sağlamaktadır. Sunucu bazlıdır. RADIUS sunucu erişim noktasına kullanıcıya özel ve dinamik WEP şifresi gönderir ve erişim noktası bunu kendi WEP şifresi ile şifreleyerek istasyona gönderir. İstasyon doğru metni gönderebilirse erişimi RADIUS sunucu tarafından onaylanır ve bu onay alındıktan sonra bir kez de tersine doğru tekrarlanır.



Şekil 4.18 RADIUS Sunucu İzin Mekanizması

3.6.5 MAC Adres Filtrelemesi

Bu güvenlik tedbiri de sunucu bazlıdır ve kullanıcıların kullandıkları cihazların MAC adreslerini filtreleme mantığına dayanır. Burada RADIUS sunucu ağa erişim isteyen cihazın MAC adresini izinli MAC adresleri listesinden kontrol eder. MAC adreslerinin her cihaz için tek olması garanti altındadır.

3.6.6 Yalın Geliştirilebilir İzin Protokolü

Cisco tarafından geliştirilen Yalın Geliştirilebilir İzin Protokolü (LEAP) ve standart olma yolunda giden bir güvenlik tedbiridir. Sunucu bazlı, kullanıcı adı/şifresi kullanıldığı, oturum süresince dinamik şifrelerin kullanıldığı çift yönlü bir izin mekanizmasıdır. Diğer üretici firmaların LEAP desteği olan cihazları ile ağa erişim mümkün olmaktadır.

3.6.7 Yalın Geliştirilebilir İzin Protokolü

Wi-Fi Korumalı Erişim (WPA), Wi-Fi grubu tarafından üretilmiş bir güvenlik tedbiridir ayrıca cihazların uyumluluğunu da sağlamaktadır.

3.6.8 Hizmet Kümesi Kimliği

Hizmet Kümesi Kimliği (SSID), aslında mevcut çalışmakta olan kablosuz yerel alan ağının tanımlayıcı parametresidir ancak ağa erişim izni isteyen kullanıcılara sorgusu yapılarak bir güvenlik önlemi haline gelmektedir.

Bu aşamaya kadar kablosuz yerel alan ağı sistemlerinin genel tanıtımı, standardının incelenmesi ve güvenlik tedbirlerinin incelenmesi ile sistem tanıtılmış ve belirli bir bilinç seviyesine ulaşılmıştır.

4.BİLİŞİMDE GÜÇLÜ GÜVENLİK POLİTİKALARI

Bilginin ve kaynakların paylaşılması gereksinimi sonucunda kurumlar, bilgisayarlarını çeşitli yollardan birbirine bağlayarak kendi bilgisayar ağlarını kurmuşlar ve sonra dış dünyayla iletişim kurabilmek için bilgisayar ağlarını İnternet'e uyarlamışlardır. Eskiden kilitli odalarla sağlanan güvenlik kavramı, bilgisayar ağları ve İnternet gibi ortamların gündeme gelmesiyle boyut değiştirmiştir. İnternet yasalarla denetlenemeyen bir sanal dünyadır. Bu sanal dünyada saldırganlar bilgiye ulaşmada ağların zayıf noktalarını kullanarak yasadışı yollar denemektedirler. Sadece yapılan saldırılarla değil, aynı zamanda kullanıcıların bilinçsizce yaptıkları hatalar nedeniyle birçok bilgi başka kişilerin eline geçmekte veya içeriği değiştirilmektedir. Kurumlarda oluşan kayıplar maddi olabileceği gibi güven yitirme gibi manevi zararlar da olabilmektedir. Bu tür durumlarla başa çıkabilmek için bazı kuralların belirlenmesi gerekmektedir.

Kurumların kendi kurmuş oldukları ve İnternet'e uyarladıkları ağlar ve bu ağlar üzerindeki kaynakların kullanılması ile ilgili kuralların genel hatlar içerisinde belirlenerek yazılı hale getirilmesi ile ağ güvenlik politikaları oluşturulur. Ağ güvenliği sağlanırken temel aldığımız nokta ağ güvenlik politikalarıdır.Ağ güvenlik politikası, kısaca bilgisayar ağının güvenliğini ilgilendiren her türlü bileşenin yönetimi ile ilgili stratejinin resmi şekilde yazılı olarak ifade edilmesidir. Bu bölümde güvenlik politikalarının kurumlar için önemi belirtilmekte ve bilgisayar ağlarında uygulanması için gereken çalışmalara değinilmektedir

Güvenlik politikasının en önemli özelliği yazılı olmasıdır ve kullanıcıdan yöneticiye kurum genelinde tüm çalışanların, kurumun sahip olduğu teknoloji ve bilgi değerlerini nasıl kullanacaklarını kesin hatlarıyla anlatmasıdır. Ağ güvenlik politikaları mümkünse sistem kurulmadan ve herhangi bir güvenlik sorunuyla karşılaşmadan önce oluşturulmalıdır. Bu aynı zamanda, kurulu olan bir sistemin güvenlik politikasını oluşturmaktan daha kolaydır. Güvenlik politikası olmadan güvenli bir bilgisayar ağı gerçekleştirilemez .

Ağ güvenlik politikaları, kurumların yapılarına ve gereksinimlerine göre değiştiğinden bir şablondan söz etmek mümkün değildir. Bu bölümde güvenlik politikası oluştururken dikkat edilmesi gerekenler belirtilmiştir. Bilgi ve ağ güvenlik politikalarından söz edildiğinde birçok alt politikadan söz etmek mümkündür. Bunun nedeni, politikaların konuya veya teknolojiye özgü olmasıdır . Ağ güvenliğinin sağlanması için gerekli olan temel politikalar aşağıda sıralanmıştır :

- Kabul edilebilir kullanım politikası
- Erişim politikası
- Ağ güvenlik duvarı politikası
- İnternet politikası
- Şifre yönetimi politikası
- Fiziksel güvenlik politikası

4.1 Kabul Edilebilir Kullanım Politikası

Ağ ve bilgisayar olanakların kullanımı konusunda kullanıcıların hakları ve sorumlulukları belirtilir. Kullanıcıların ağ ile nasıl etkileşimde oldukları çok önemlidir. Yazılacak politikada temelde aşağıdaki konular belirlenmelidir:

- Kaynakların kullanımına kimlerin izinli olduğu
- Kaynakların uygun kullanımının nasıl olabileceği
- Kimin erişim hakkını vermek ve kullanımı onaylamak için yetkili olduğu
- Kimin yönetim önceliklerine sahip olabileceği
- Kullanıcıların hakları ve sorumluluklarının neler olduğu

- Sistem yöneticilerin kullanıcılar üzerindeki hakları ve sorumlulukların neler olduğu

- Hassas bilgi ile neler yapılabileceği

Kurumun yapısına göre başka maddeler de eklemek mümkündür.

4.2 Erişim Politikası

Erişim politikaları kullanıcıların ağa bağlanma yetkilerini belirler. Her kullanıcının ağa bağlanma yetkisi farklı olmalıdır. Erişim politikaları kullanıcılar kategorilere ayrıldıktan sonra her kategori için ayrı ayrı belirlenmelidir. Bu kategorilere sistem yöneticileri de girmektedir. Sistem yöneticisi için erişim kuralları belirlenmediği takdirde sistemdeki bazı kurallar sistem yöneticisinin yetkisine bırakılmış olacağından, bu sistem üzerinde istenmeyen güvenlik açıkları anlamına gelebilecektir[5].

4.3 Ağ Güvenlik Duvarı Politikası

Ağ güvenlik duvarı , kurumun ağı ile dış ağlar arasında bir geçit olarak görev yapan ve İnternet bağlantısında kurumun karşılaşabileceği sorunları çözmek üzere tasarlanan çözümlerdir. Ağın dışından ağın içine erişimin denetimi burada yapılır. Bu nedenle erişim politikaları ile paraleldir. Güvenlik duvarları salt dış saldırılara karşı sistemi korumakla kalmaz, performans arttırıcı ve izin politikası uygulayıcı amaçlar için de kullanılırlar. Bu çözümler yazılım veya donanımla yazılımın bütünleşmesi şeklinde olabilir. Güvenlik duvarlarının grafiksel arabirimleri kullanılarak kurumun politikasına uygun bir şekilde erişim kuralları tanımlanabilmektedir. Güvenlik duvarı aşağıda belirtilen hizmetlerle birlikte çalışarak ağ güvenliğini sağlayabilmektedir :

- **Vekil Sunucu**: Vekil sunucu bir bağlantı uygulamasında araya giren ve bağlantıyı istemci için kendisi gerçekleştiren bir hizmettir. Vekil Sunucu'nun kullanımı, uygulama temelli güvenlik duvarı olarak da adlandırılabilir. Bu tür bir uygulama aynı zamanda kimlerin bu hizmetleri kullanacağını belirlemek ve performans amaçlı olarak bant genişliğinin daha etkin kullanılmasını sağlamak için de kullanılır.

- **Anti-Virüs Çözümleri**: HTTP(Hipermetin Transfer Protokolü),FTP(Dosya Transfer Protokolü) ve SMTP (Basit Posta Transfer Protokolü) trafiğini üzerinden

geçirerek virüs taramasını yapmayı ve kullanıcıya gelmeden önce virüslerden temizlemeyi hedefleyen sistemlerdir.

- **İçerik Süzme :** Çeşitli yazılımlarla ulaşılmak istenen web sayfalarını, gelen e-posta'ları süzmeye yarayan sistemlerdir.

- **VPN (Özel Sanal Ağlar) :** Ortak kullanıma açık veri ağları üzerinden kurum ağına bağlantıların daha güvenilir olması için VPN kullanılmaktadır. İletilen bilgilerin şifrelenerek gönderilmesi, Genel/Özel anahtar kullanımı ile sağlanır. VPN kullanan birimler arttıkça daha sıkı politika tanımları gerekli hale gelmektedir.

- **IDS (Nüfuz Tespit Sistemleri) :** Şüpheli olayları, nüfuz ve saldırıları tespit etmeyi hedefleyen bir sistemdir. IDS, şüpheli durumlarda e-posta veya çağrı cihazı gibi yöntemlerle sistem yöneticisini uyarabilmektedir.

Bu servislerin hepsinin konfigürasyonu ve kullanacakları kuralların belirlenmesi güvenlik politikasına uygun olarak yapılmalıdır[3].

4.3.1 Güvenlik Duvarları

İnternet'e bağlı bilgisayarlarda güvenlik sağlamak üzere değişik yaklaşımlar kullanılmaktadır. Güvenlik Duvarları ağ güvenliğini oldukça iyi bir şekilde sağlarlar.

İnternet Güvenlik Duvarları binaların bölmelerini birbirinden ayıran ve olası bir yangın durumunda ateşin bir bölmeden diğerine geçişini engelleyen bina Güvenlik Duvarları ve eski kalelerde bulunan ve kaleye tek giriş çıkış noktası olan kapılara da benzetilebilirler.Bu kapıların kalenin güvenliği açısından sağladığı avantajlar dışardan içeriye girmek isteyen insanların kontrol edilmesini mümkün kılması, kaleye tek giriş noktasının bu kapı olmasından dolayı tüm güvenlik unsurlarının bu kapı üzerinde yoğunlaştırılması ve kaleden dışarı çıkışların kontrol altında tutulmasıdır.

İnternet Güvenlik Duvarları yerel ağın İnternet'e açıldığı noktaya yerleştirilir ve İnternet'ten yerel ağa gelen tüm trafik,yerel ağdan İnternet'e giden tüm trafik Güvenlik Duvarları üzerinden geçmek zorundadır.Böylece Güvenlik Duvarları yerel ağ ve İnternet arasındaki tüm trafiği kontrol eder.

Güvenlik Duvarları tüm trafiği kontrol ederek kabul edilebilir olanların geçişine müsade ederler.Yani her ağın kendine özel değişik seviyelerde kısıtlamalar getiren güvenlik politikalarının sınırlamalarına uyar.Güvenlik Duvarları salt dış saldırılara karşı sistemi korumakla kalmaz, performans arttırıcı ve izin politikası uygulayıcı amaçlar için de kullanılırlar.

İnternet güvensiz bir ağdır , onu güvensiz kılan paylaşımın fazlalığı ve insanın doğal yok etme içgüdüsüdür. İnternet bağlantısında bir kurumun karşılaşabileceği sorunlar aşağıdaki gibidir:

- Dış dünyadan kurum ağına (içeriye) yapılacak saldırılar

- İnternet'te dolaşırken kullanıcı bilgisayarına, bilgisayardan da sisteme virüs bulaşması

- İmesh, edonkey, overnet gibi programlarla dosya paylaşımının yapılması ve bant genişliğinin (İnternet veri yolu kapasitesinin) maksadı dışında kullanılması

- İnternet'te özellikle vakit kaybettirici bazı sitelere ulaşımın kurum içerisinde, kurum zamanında (mesai saatlerinde) yapılması

- İçeriden yetkisiz kişilerin dışarıya bilgi göndermesi

- Yetkisiz kullanıcıların İnternet'te gezinmesi

Yerel ağdaki özel bilgiler İnternet'in getirdiği risklerden yalıtılmak isteniyorsa kullanılabilecek sistemlere de yukarıda anlatıldığı gibi Güvenlik Duvarları denir.Birden fazla ağ parçası arasına kurulan Güvenlik Duvarları sistemleri bu ağların yalıtılması işlemini gerçekleştirir.Bu ağlar İnternet , bayi ağı , müşteri ağı , hizmet alınan şirketlerin ağı yada yerel şirket ağı olabilir.Kullanım alanını sadece İnternet ile sınırlamak yanlıştır. Bu ağlar arası geçiş için çeşitli kural zincirleri ve erişim yetkileri belirler, böylece söz konusu ağlardaki kötü niyetli insanlardan etkilenme oranı büyük ölçüde düşer.

Ağlar arası yetkilendirme göründüğü yada bahsedildiği kadarda basit bir kavram değildir. Bunun için çeşitli yöntemler uygulanmaktadır ve uygulanan yöntemler Güvenlik Duvarları mimarilerini de çeşitlendirmektedir. Amacın sadece gelen paketi portuna, protokolüne veya geldiği yere bakarak filtrelemek olduğunu düşünmek bugün oldukça ilerlemiş olan Güvenlik Duvarları sistemlerini yok saymak ile aynı düşüncedir. Çünkü bu sistemlerin farkları arasında statik paket filtreleme , dinamik paket filtreleme ve uygulama vekil sunucu gibi mimari farklılıkları , donanım veya yazılım çözümü olmaları, üzerinde çalıştıkları işletim sistemleri sayılabilir.

Çeşitli ağ parçalarının birbirleriyle iletişim kurmalarını kısıtlamak ve bir ağı veya sunucuyu korumak amaçlı olarak Güvenlik Duvarları kullanılabilir. Bugün Güvenlik Duvarları ihtiyaç olarak düşünülmelidir , çünkü gelişen teknoloji ve saldırı teknikleri sahip olunan bilgileri yeterince büyük bir risk altında bırakmaktadır. Kaldı ki bireysel olarak İnternet'e bağlanan kullanıcılarda bile güvenlik sağlamak önemli olmaktaysa ticari kurumlarda güvenlik çok daha ileride olmak zorundadır. Bireysel kullanıcılara her gün çeşitli Truva saldırıları, DOS atakları gerçekleşirken kurumsal kullanıcılara da çok daha fazla saldırı gerçekleşmektedir.

Saldırıları engellemenin tabi ki tek yolu Güvenlik Duvarları değildir ve bunu düşünmekte bir hatadır. Ama güvenlik politikalarında önemli bir yeri olması gereken bileşenlerdendir. Ağda doğru şekilde düzenlenmiş bir Güvenlik Duvarları gerek hız gerekse de güvenlik sağlayacaktır. Tüm bahsi geçen saldırıları önlemek için öncelik Güvenlik Duvarları sistemlerini düzenlemekten geçmektedir. Ağın dış dünyaya çeşitli kapılarla açıldığı unutulmamalıdır, eğer bu kapıların bazıları kapatılmazsa ya da bu kapılardan gelen/giden paketler takip edilmezse davetsiz misafirleri ağda bulma olasılığı yükselir. Ağın ve bilgilerin mahremiyetini korumak için ilk ve en önemli bileşenlerden olan Güvenlik Duvarları sistemleri saldırganları karşılayacak ilk sistem olması sebebiyle ciddi bir önem arz etmektedir. Eğer bir sunucu için yerel ağın erişim yetkileri düzenlemek isteniyorsa , güvenilmeyen ağların veya kişilerin ağa girişleri kontrol altına alınmak isteniyorsa ve çalışanların çeşitli ağlara erişimleri kısıtlanmak isteniyorsa Güvenlik Duvarları bu amaçlar için ciddi bir gereklilik teşkil etmektedir[14].

4.3.1.1 Güvenlik Duvarları Mimarileri ve Farkları

Günümüzde Güvenlik Duvarları sistemleri genel olarak üç ayrı yapı ile birbirlerinden ayrılmaktadırlar. Bu yapılar Güvenlik Duvarlarına çeşitli artılar ve eksiler kazandırmaktadır. Bu kısımda üç yapı hakkında çeşitli bilgiler verilerek ve karşılaştırmalar yapılarak Güvenlik Duvarları arasındaki farklar incelenecektir.

İlk mimari, statik paket filtreleme teknolojisidir. Bu mimari eskimiş olmasına rağmen halen Linux IPChains gibi bazı Güvenlik Duvarları sistemlerinde kullanılmaktadır. Gelen ve giden paketleri sadece geldiği yer ,erişmek istediği port numarası , protokolü gibi değerleri ile inceler ve bu değerlerden paketin erişimine izin olup olmadığının saptamasını yapar. Örneğin bir http isteği eline geldiğinde erişmek isteği portun 80,protokolün TCP ve geldiği yerin 1.2.3.4 IP'si olduğunu görür ve içerideki sunucuya ulaşmasına izin verilmişse, bu paketin içerideki sunucuya gitmesine izin verir. Basit bir mimaridir. Günümüzde ticari Güvenlik Duvarları sistemlerinde kullanılmamaktadır. En büyük zayıflığı paketleri ilk gönderen sistemi yani oturumu ilk başlatan sistemi saptayamıyor olmasıdır. Bu durum ciddi riskler oluşturmaktadır, kaynak portu taramaları ve bağlantıları bu risklere örnektir. Bir örnek ile incelemek gerekirse ağdaki bir çalışanın FTP portundan iletişim kurabilmesi için izin verilmiştir. Oturumun işleyişi ise önce çalışanın 21/TCP portunu hedef port olarak belirleyerek bir sisteme dosya isteği göndermesi ile başlar, hedef sistem, kaynağı portu 20/TCP olan paketler ile çalışana dosya transferi yapar. Böyle bir durumda saldırgan ağa kaynak portu 20/TCP olan bir paket gönderdiğinde Güvenlik Duvarları sistemi bu paketi görecek ve içeriden bu pakete istek gelmeseydi bu paket gönderilmezdi mantığına dayanacak ve paketin içeriye girmesine izin verecektir. Güvenlik Duvarı'nın paketin hedef portuna bakmaması sebebiyle saldırgan kaynak portu 20/TCP olan paketlerle içerideki herhangi bir sistemin örneğin 139/TCP portuna ulaşabilecektir. Böylece Güvenlik Duvarı üzerindeki erişim kontrol listeleri etkisiz kalacaktır.

Bu sebeple oturumun baştan sona takip edilmesi , kimin ne istediği ve kimin ne gönderdiği bir tabloda tutulacak ve karşılaştırılacak bir sistem yaratılmıştır ve dinamik paket filtreleme sistemi olarak adlandırılmıştır.

Dinamik paket filtreleme mimarisindeki Güvenlik Duvarları'nda yukarıdaki örnekte anlatıldığı gibi klasik paket filtrelemenin yanı sıra oturumu takip etme özelliği de vardır. Checkpoint firmasının ürettiği bu teknoloji yine bu firmanın tescilli markası olan

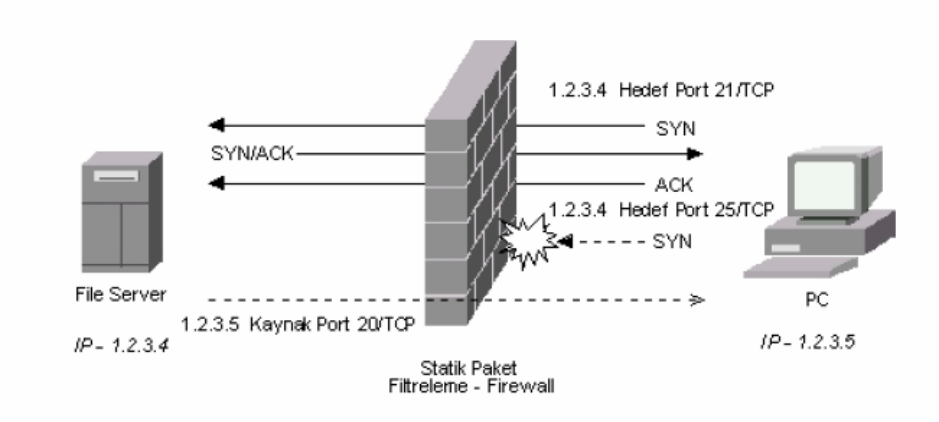
Stateful Inspection ismiyle anılmaktadır. Günümüz Güvenlik Duvarları sistemleri genelde bu sistem ile çalışmaktadırlar. Temel olarak TCP oturumları bir başı , ortası ve sonu olan oturumlardır. Hiçbir oturum başından veya ortasından kurulamaz. Bu durumda Güvenlik Duvarları kuralları sadece SYN bayrakları ile gönderilen paketlere (nereden gönderildiği önemli değil) uygular ve geriye kalan paketler oturumun tutulduğu tabloya bakılarak takip edilir. Böylece örneğin FIN veya SYN/ACK bayraklı paketlerin bir oturumun devamı olmadığından geçişi engellenebilir. Oturumun SYN bayraklı paketler ile başlayacağını düşünerek tasarlanan bu sistemin kuralları bu paketlere uygulaması oldukça mantıklı ve güvenlidir. Ayrıca TCP için olan bu oturum izleme işlemi ICMP ve UDP paketlerine de uygulanabilmektedir. Ticari olmayan ürünlerden IPFilter , ticari ürünlerden Checkpoint FW-1 , Netscreen , Cisco PIX gibi birçok Güvenlik Duvarları bu teknolojiye dayanır. Ancak bu teknolojinin zayıflıkları da vardır, paketlerin içeriğini kontrol etmemeleri bu zayıflıklarının başlıca sebebidir, ayrıca FTP protokolünün vekil sunucu özelliğini desteklemesi ve bunun kötüye kullanım oranın oldukça fazla olması Statik Güvenlik Duvarları sistemlerinin en büyük dezavantajlarındandır.

Vekil sunucu mimarisini destekleyen Güvenlik Duvarları'nda ise oturum, başlatan ve hedef arasında gerçekleşmez.Oturum açmak isteyen taraf isteği Güvenlik Duvarı'na gönderir ve Güvenlik Duvarı bu paketi hedefe ulaştırır, hedeften cevap yine Güvenlik Duvarı gelir ve Güvenlik Duvarı tarafından oturumu açmak isteyen tarafa iletilir. Oturum açıldıktan sonrada aynı şekilde devam eder. Böylece iki sistem arası tamamen yalıtılır ve Güvenlik Duvarı paketlerin gerek içeriklerine , gerek hedef ve kaynak portlarına gerekse de gönderenin IP adresine müdahale edebilir.Paketlerin içeriğini kontrol edebilme Vekil Sunucu Güvenlik Duvarları'nın en büyük artılarındandır, böylece istenmeyen komutlar (HTTP paketlerinde POST komutunun kullanılmaması gibi) veya içerik (Java , ActiveX gibi) filtrelenebilir. Özellikle FTP protokolü kesinlikle vekil sunucu olarak hizmet vermelidir, aksi taktirde FTP protokolünün pasif FTP seçeneği ile saldırgan FTP sunucusundan içerideki sistemlere ulaşabilir, FTP vekil sunucu kullanımı bu tür isteklerin Güvenlik Duvarı tarafından filtrelenmesini sağlamaktadır. Statik Güvenlik Duvarları gibi oturumu takip etmek zorunda değildir ; çünkü oturum zaten kendisi tarafından devam ettirilmektedir. Bu proxyler transparan (görünmeyen) vekil sunucular olabileceği gibi normal vekil sunucularda olabilmektedir. Yetersiz olduğu noktalara gelince araya girmesi ve paketleri kendisinin iletmesinin

doğal sonucu olan yavaşlık ortaya çıkmaktadır. Ciddi bir yavaşlık olmamasına rağmen artan bağlantı sayısı ve yoğun ağlardaki veri trafiği , hızı olumsuz yönde etkilemektedir.

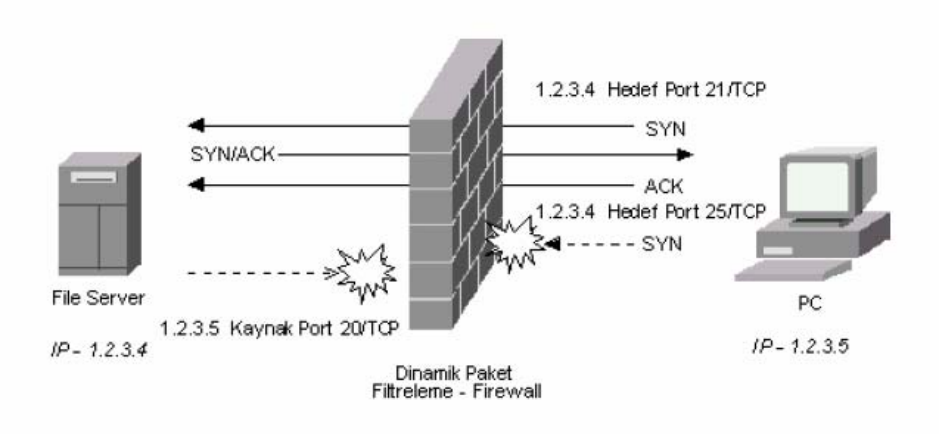
Bu mimarilerin iki veya daha fazlasını barındıran Güvenlik Duvarı sistemleri de bulunmaktadır, bu sistemlere Hybrid sistemler denir. Bazı protokoller için vekil sunucu (Örneğin FTP, SMTP,HTTP) diğer protokoller için ise Statik çalışabilen yada sürekli Statik çalışabilen gereğinde vekil sunucu kullanılabilecek sistemlerdir. Yoğun ağlarda Statik Güvenlik Duvarları , daha az yoğun yada güvenliğin önemli olduğu noktalarda Vekil Sunucu Güvenlik Duvarları tercih edilmektedir.

Örnek şekiller ile bu mimarilerdeki farklılıklar aşağıda gösterilmiştir:



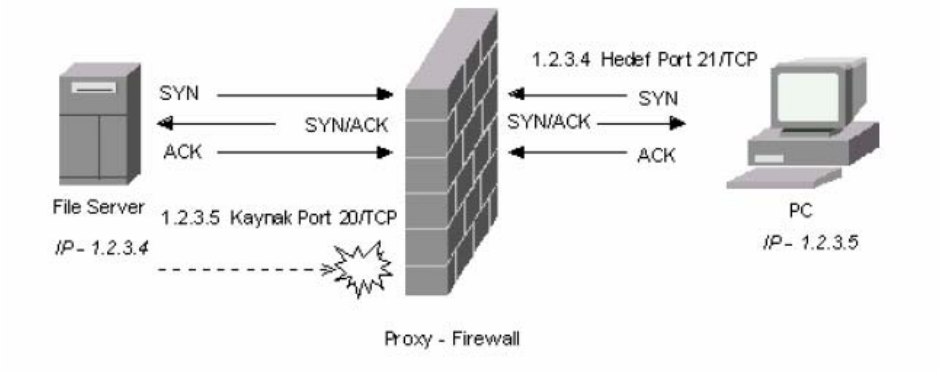
Şekil 5.1 Statik Paket Filtreleme

İlk şekilde Statik Paket Filtreleme'nin nasıl olduğu görülmektedir. PC 1.2.3.4 IP'li dosya sunucusunun 21/TCP portuna bağlanırken Güvenlik Duvarı izin veriyor. Ancak 25/TCP portuna bağlanmak istediğinde Güvenlik Duvarı izin vermiyor. Dosya sunucusu ise isterse kaynak portunu 20/TCP yaparak PC'ye istediği porttan ulaşabilir. Çünkü Güvenlik Duvarı PC'nin bir isteğinin karşılığında bu paketlerin gönderildiğini düşünür.



Şekil 5.2 Dinamik Paket Filtreleme

İkinci şekilde ise Dinamik Paket Filtreleme sisteminin nasıl işlediği görülmektedir. PC'nin isteklerinde sonuç değişmezken dosya sunucusunun kaynak portu 20/TCP olan paketi ise engellenmektedir.



Şekil 5.3 Vekil Sunucu

Son şekilde ise Vekil Sunucu Mimarisi'nin işleyişi görülmektedir. PC'nin istekleri Güvenlik Duvarı'na gelmekte ve Güvenlik Duvarı üzerinden dosya sunucusuna ulaşmaktadır, cevaplar ise yine Güvenlik Duvarı üzerinden PC'ye ulaşmaktadır. Kaynak portu 20/TCP olan paketler için yine engelleme söz konusudur.

4.3.1.2 Güvenlik Duvarı ve Bileşenleri

Güvenlik Duvarı belirli bir makinayı denetlemek için o cihaz üzerine kurulabileceği gibi, bir bilgisayar ağını denetlemek için de kurulabilir. Güvenlik Duvarı, yazılım veya donanımla yazılımın entegre olduğu çözümler şeklinde olabilir.Donanım ve yazılımın entegre olduğu çözümler Güvenlik Duvarı cihazlarıdır.Bununla beraber bilgisayarlar

üzerinde koşturulan yazılımlar ve yönlendiriciler üzerinde yapılan uygun konfigurasyonlarla ,yönlendiricilere ve bilgisayarlara Güvenlik Duvarı özelliği katılabilir.Bir Güvenlik Duvarı çözümünde verilebilecek servislere örnek olarak aşağıdakiler sayılabilir:

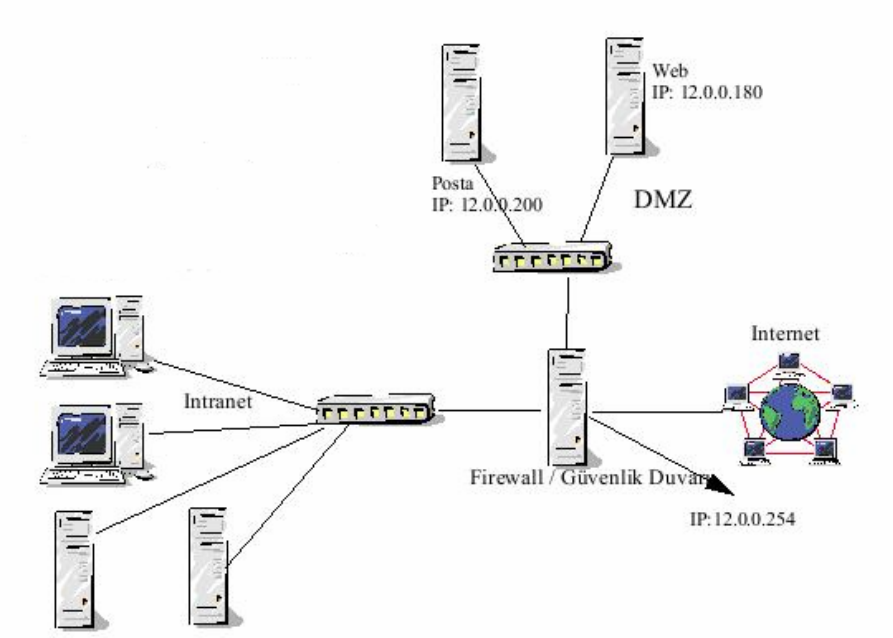
- **NAT :** İç ağda İnternet'e çıkamayacak özel IP şemaları tanımlanır ve dış bağlantılarda NAT sunucusunun reel IP'si kullanılarak iç ağ konusunda saldırganın bilgi sağlaması engellenir. Güvenlik için artıları olmakla beraber, NAT çoğunlukla adres yönetimi için kullanılmaktadır.

- **Paket Filtreleme:** En basit Güvenlik Duvarı'dır. Yönledirici, modem gibi cihazlarla birlikte gelir. Erişim listelerinin kullandıkları yöntemdir. Bu yöntemle Güvenlik Duvarı'ndan geçen her üçüncü seviye (IP, IPX ..vb) paketine bakılır ve ancak belli şartlara uyarsa bu paketin geçişine izin verilir. Paket Filtreleme, Güvenlik Duvarı'nın her fiziksel bağlantısı üzerinde ayrı ayrı ve yöne bağlı (dışarıya çıkış, içeriye giriş) olarak uygulanabilir. Uygulamaların bağlantı için kullandıkları portlar (icq, imesh ..vb portları) baz alınarak hangi ağların veya kişilerin ne zaman bu uygulamalarla bağlantı kurabileceği belirlenebilir. Paket Filtreleme'de birim zamanda tek bir pakete bakıldığı ve önceki paketler hakkında bir bilgiye sahip olunmadığı için bu yöntemin çeşitli zayıflıkları bulunmaktadır.

- **Dinamik Filtreleme:** Paket Filtreleme'den farkı, paketin sırf protokolüne bakarak karar verilmesi yerine, Güvenlik Duvarı'nın bir bağlantıyı hangi tarafın başlattığını takip etmesi ve çift yönlü paket geçişlerine buna göre karar vermesidir. Her bağlantı için durum bilgisi tablolarda tutulduğu için Paket Filtreleme'deki zayıflıklar bulunmamaktadır. Dezavantajı ise Dinamik Filtreleme'nin çok daha fazla işlemci gücüne ve belleğe ihtiyaç duymasıdır. Özellikle bağlantı sayısı arttıkça işlem ihtiyacı da artacaktır. Paket Filtreleme yerine Dinamik Filtreleme tercih edilmelidir.

- **DMZ (Silahtan Arındırılmış Bölge):** Ağınızda İnternet'den erişimi olması gereken web, posta gibi sunucular bulunabilir. DMZ, Güvenlik Duvarı tarafından daha az korunan, daha fazla erişime izin verilen bir bölgedir. Güvenlik Duvarı'na üçüncü bir ağ çıkışı eklenmesi ve İnternet'e servis verecek olan makinaların buraya konulması ile oluşturulur. Örneğin DMZ'deki makinalara NAT uygulanmayabilir, tahsisli IP

numaralarına sahip olabilirler. Güvenlik Duvarı, telnet, ssh gibi kimi protokollerin buraya erişimini filtreleyerek DMZ bölgesindeki makinalara güvenlik sağlar. Dikkat edilecek nokta, DMZ'de bulunan makinaların daha fazla erişime (ve dolayısıyla saldırıya) açık olmasıdır. Buradaki makinalar dikkatli kurulmalı, güvenliğe aykırı protokoller vs. burada yer almamalıdır[2].



Şekil 5.4 Silahtan Arındırılmış Bölge (DMZ)

DMZ oluşturmak için ek ekipman ve IP numarası gerekir. Güvenlik Duvarı'nda üçüncü bir ağ birimi, ayrı bir Anahtar, daha fazla adette tahsisli IP numarası, ve iç ağınızda başka herhangi bir görev görmeyecek olan sunucu makinalar gerekir. Eldeki imkanlar buna yetişmeyebilir. Böyle durumlarda, Güvenlik Duvarı'nızdaki filtreleme politikasını değiştirerek iç ağınızdaki kimi makinalara dışarıdan sınırlı erişim imkanı verebilirsiniz. Örneğin Güvenlik Duvarı'nız ağınızın genelinde dışarıdan gelen SMTP protokolünü filtrelerken, sadece posta sunucunuza dışarıdan SMTP protokolü erişimini verebilir. NAT ile birleştirileceğinden, bu dışarıdan bakıldığı zaman sanki güvenlik duvarınız posta sunuculuğu yapıyormuş izlenimini verir.

- **Vekil Sunucu:** Vekil Sunucu bir bağlantı uygulamasında araya giren ve bağlantıyı istemci için kendisi gerçekleştiren bir servistir. Vekil Sunucu'nun kullanımı, uygulama temelli Güvenlik Duvarı olarak da adlandırılabilir. Bu tür bir uygulama aynı zamanda şu amaçlar için kullanılabilir:

  - Kimlerin bu servisleri kullanacağını belirlemek

  - Performans amaçlı olarak özellikle aynı isteklerin bir defaya indirgeyerek bağlantı sayısını azaltmak ve bandgenişliğinin daha etkin kullanılmasını sağlamak

- **Anti-Virus Çözümleri:** HTTP, FTP ve SMTP trafiğini üzerinden geçirerek virüs taramasını yapmayı ve kullanıcıya gelmeden önce virüslerden temizlemeyi hedefleyen sistemlerdir.

- **İçerik Filtreleme :** Çeşitli yazılımlarla ulaşılmak istenen web sayfalarını, gelen e-posta'ları filtrelemeye yarayan sistemlerdir.

- **Kayıtlama ve Raporlama:** Kayıtlama ve etkinlik raporları birçok Güvenlik Duvarı tarafından sağlanmaktadır. Bu kayıtlar çok detaylı ve çok fazla veri içerebilmektedir. Bazı Güvenlik Duvarları bu kayıtlamaların incelenmesini kolaylaştırmak için çeşitli analiz ve raporlama servisleri sunmaktadır. Kayıtlar sistemlerin zayıflıklarının ve saldırıların belirlenmesinde işe yaramaktadır.

- **Saldırı Tespiti (ID):** Saldırı tespit sistemleri (IDS)'nin ana amacı ağınıza apılan saldırıları tespit etmek, bunların başarılı olup olmadığını görmektir.

Saldırı Tespit Sistemleri dört ayrı bölüme ayrılmaktadır ve iki faktörün kombinasyonlarıdırlar. İlk olarak bir sistem 'Aktif' yada 'Pasif' olabilir. İkincisi, 'Host tabanlı' yada 'Ağ tabanlı' olabilir. Bu ikisini birleştirdiğimizde bir saldırı tespit sistemi 'Aktif/Host tabanlı', 'Pasif/Host tabanlı', 'Aktif/Ağ tabanlı' yada 'Pasif/Ağ tabanlı'dır. IDSler için daha başka tanımlamalarda yapılabilir fakat İnternet Güvenlik Sistemleri (ISS) tarafından ortaya atılan bu model hepsini kapsamaktadır.

Bir sistemin Aktif olarak sınıflandırılabilmesi için sistemin tespit edilen bir saldırıya gerçek-zamanlı olarak (yada buna yakın) cevap vermesi (Güvenlik Duvarı kurallarını saldırıya göre düzenlemek yada komut konsolunu saldırı hakkında uyarmak gibi) gerekir. Pasif sistemler genelde aktiviteyi kayıt ederler ve daha sonraki bir tarihte incelenmek üzere saklarlar. Cihaz tabanlı sistemler hedeflenen sistemler üzerinde bulunurlar. Ağ Tabanlı sistemler ağda, hedef ve saldırgan arasında bir yerde bulunurlar ve akan trafiği saldırı olup olmadığını tespit için dinlerler. Genelde ağ tabanlı sistemler ya DMZlerde ya ağın Güvenlik Duvarı ile servis sağlayıcı arasında ya Güvenlik Duvarı ile iç ağ arasında ya da bunların herhangi bir kombinasyonunda bulunurlar.

Saldırı Tespit Sistemleri, başlangıcından beri 'saldırı izleri/işaretleri' fikrine dayanmaktadır. Yani her saldırının kendini diğer saldırılardan ve normal ağ trafiğinden ayıran bazı izleri vardır. Bu pek çok virüs tarayıcısının dizaynına benzemektedir. Sistem trafiği tarar ve bilinen bir saldırınınkine benzeyen bir işaret gördüğünde neye ayarlanmışsa onu yapar (sistem yöneticisine çağrı mesajı göndermek, güvenlik duvarı kurallarını güncellemek, konsolu haberdar etmek vs.) .

Saldırı Tespit'te, sık rastlanmayan, tanınlanmayan saldırıları tespit olayı ise Anomali Tespit'tir. Anomali Tespit sistemi ile ağ normalde bulunan trafik göz ardı edilir ve normal trafikte bulunmayacak bitler ağ yöneticisinin dikkatine sunulur. Bunun belirli bazı avantajları vardır.

İnternet'e bağlı olan her makinenin güvenliği üzerindeki tehdit sistemdeki açıkların daha keşfedilmemiş olmasıdır. Yeni bir güvenli açığı bulununca açığı bulan kişi açıktan yararlanmak için bir exploit kodu yazar. Bu kod bir süre sonra güvenlikle ilgilenen toplumun eline geçer ve bir yama hazırlanır. Bu sure zarfında Saldırı Tespit Sistemleri güvenli değillerdir. Çünkü bir saldırıyı tespit edebilmek için o saldırının ağda hedef sisteme yol alırken neye benzediğini bilmek gerekir.

Etkili bir Anomali Tespit Sistemi'nin herhangi bir linux platformu üzerine yazılımlar ve değişiklikler yapılarak kurulması mümkündür. Bu araçlar, ipchains/ipfwadm, portsentry, logcheck, gnumeric ve bir eposta adresidir.

Her sistemde, ipchains/ipfwadm dinlenmeyen portlara giden trafiği kaydedecek şekilde ayarlıdır. Eğer bu bir web suncusu ise ve ssh kullanılıyorsa, ipchains 22/tcp ve 80/tcp haricindeki tüm portlara giden paketler loglanır. Portsentry logcheck'i çalıştırcak şekilde ayarlanır. Portsentry -actp kullanılır. Logcheck alışılmadık aktivitelerde epost

adresine mesaj atacak şekilde ayarlanır. Gnumeric ya da diğer bir spreadsheet programı ile her makinada kötü amaçlı trafiğin kayıtları tutulur. IP adresi, aktivitenin tarih ve saati, kullanılan portlar (kaynak port dahil) saldırganın IPsinin cihaz adı, kontak bilgileri ve IP'nin sahipleri gibi bilgileri tutulur.

Bu sistem ile ağa giren ve ağa ait olmayan her paket izlemiş olur. Böylece saldırgan sisteme girebilmek için hangi servislerin çalıştığı, kullanılan işletim sistemi bilgisini elde edene kadar zaman kazanılmış olur. Şüpheli olayları ve saldırıları tespit etmeyi hedefleyen bir servis olan Saldırı Tespit Sistemleri, şüpheli durumlarda e-posta veya çağrı cihazı gibi yöntemlerle sistem yöneticisini haberdar edebilmektedirler.

- **VPN (Sanal Özel İletişim Ağı):** Ortak kullanıma açık veri ağları üzerinden kurum ağına bağlantıların daha güvenilir olması için VPN kullanılmaktadır. İletilen bilgilerin şifrelenerek gönderilmesi esas olarak alınır.

4.3.2 VPN Teknolojisi

Dağınık yapıdaki özel iletişim ağlarının üzerinde bulunan bilgilerin, kamu iletişim ağı altyapısını kullanarak paylaşılması sırasında, kamu iletişim ağı üzerinden geçen bilgilerin üçüncü kişiler tarafından deşifre edilmesinin engellenmesi gerekmektedir.

VPN bu sorunu ortadan kaldırmak için geliştirilmiş bir sistemdir. VPN sayesinde, özel iletişim ağına ait uzaktaki kullanıcıların, güvenilir olmayan kamu iletişim ağları üzerinden, kendi iletişim ağları ile serbestçe ve güvenilir bir şekilde haberleşmesi sağlanabilmektedir. VPN kurabilmek için özel iletişim ağı ile kamu iletişim ağı arasına çeşitli üreticilerin VPN donanım ve yazılımlarını (bundan sonra VPN sistemi olarak kullanılacaktır) koymak gerekmektedir. Dolayısı ile kullanıcılarınızdan biri, uzakta bulunan bir ağınızdaki kullanıcı ile haberleşmek istediğinde, kullanıcınızın haberleşme paketleri önce kendi özel iletişim ağında bulunan VPN sistemine gelmekte, buradan da kamu iletişim ağı üzerinde uzaktaki haberleşmek istediği kullanıcının özel iletişim ağını koruyan VPN sistemine gitmekte ve buradan da kullanıcıya ulaşmaktadır. Özel iletişim ağlarınız arasında, her ağda bulunan VPN sistemleri kendi aralarında sanal "tüneller" oluşturmaktadır.

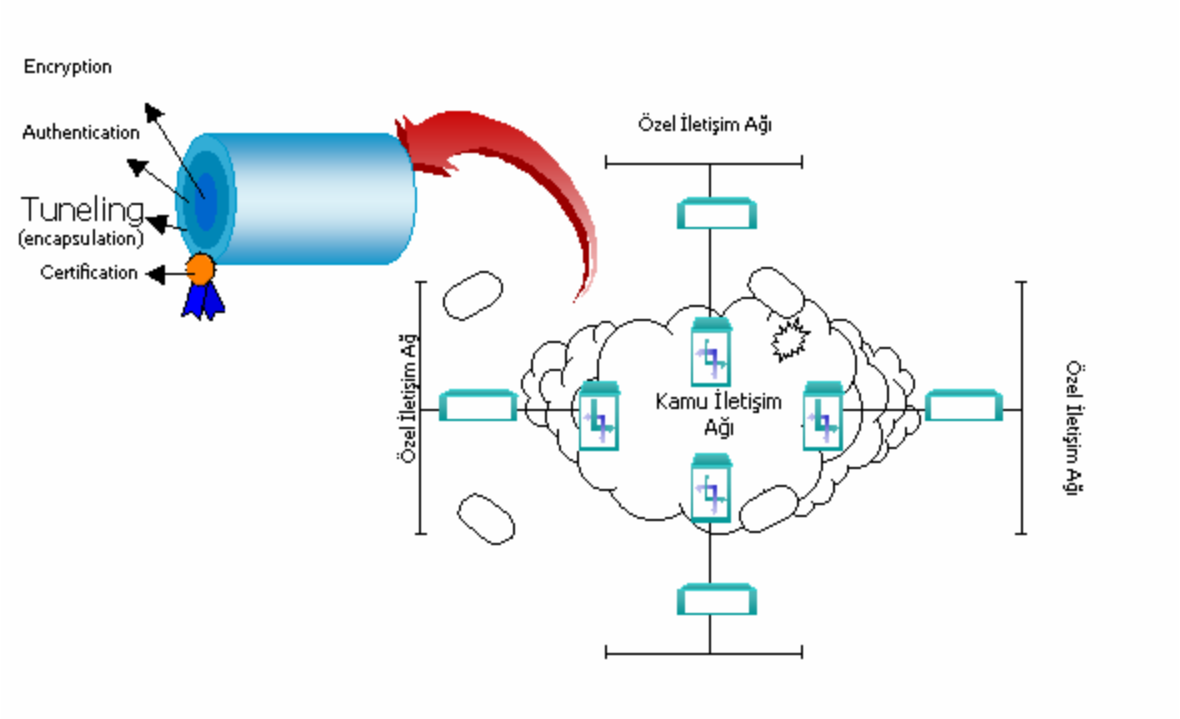
VPN sistemi, bir haberleşme paketini bir özel iletişim ağından diğerine göndermeden önce, bu paketi bir "şifreleme" yöntemi ile şifrelemekte ve VPN sistemleri arasında

sanal “tünel”lere “yeni bilgilerin eklenmesi” yöntemi koyup ilgili iletişim ağı üzerindeki diğer VPN sistemine göndermektedir.

4.3.2.1 VPN sistemlerinde bilginin korunması

VPN sistemleri kendi özel bilgilerinizi taşıyan haberleşme paketlerinin korunmasını, kendi aralarında yarattıkları sanal tünellerin sayesinde yapabilmektedir.

VPN sistemlerinde dört seviyeye kadar güvenlik sağlanabilmektedir. Bu seviyeler, “Sertifikasyon, Şifreleme, Tanımlama-Sorgulama ve Tünelleme” olarak sayılabilir. Bu seviyeler aşağıda açıklanmaktadır[2].



Şekil 4.5 VPN Sistemi ve Seviyeleri

- **Sertifikasyon :**

Tüm iletişim ağı içerisinde bulunan VPN sistemleri aynı sertifikasyon ismini taşımalıdır. Bu isme sahip olmayan VPN sistemine, diğer VPN sistemleri tarafından güvenilmeyecek ve bağlantı kurulmayacaktır.

- **Şifreleme :**

Özel iletişim ağından, kamu iletişim ağına paketler iletilmeden önce şifrelenmektedir. Aşağıdaki şekilden de anlaşılacağı gibi, herkese açık olan kamu iletişim ağında paketler

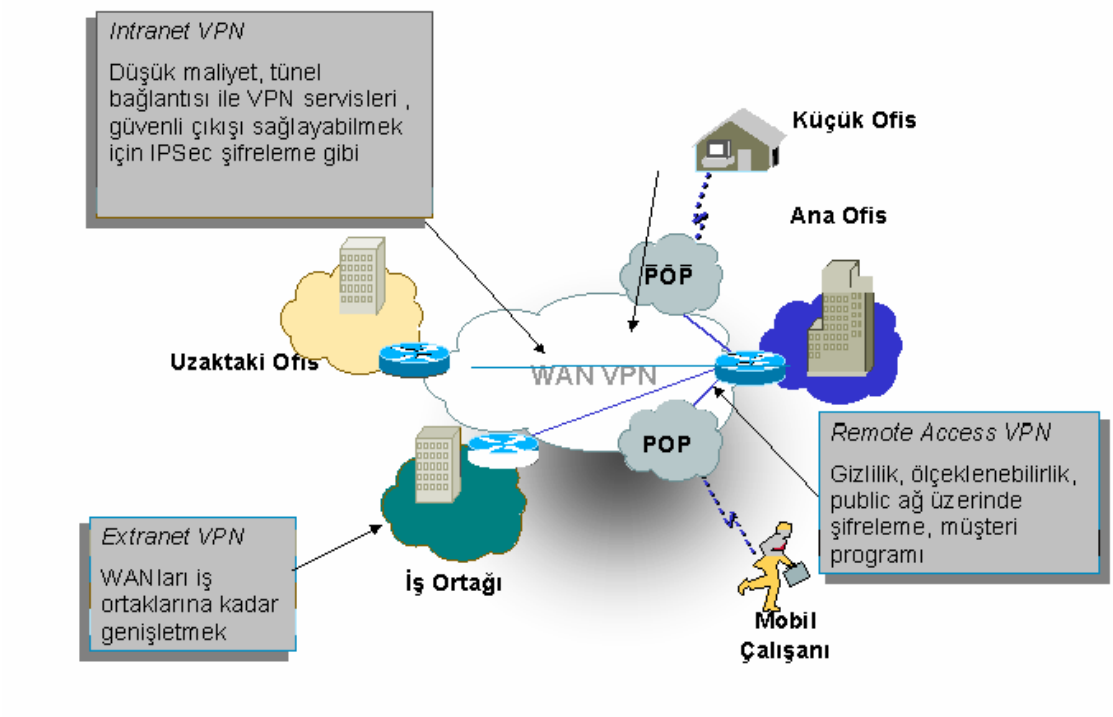
başkaları tarafından incelense bile içeriği anlaşılamayacaktır. Şifreleme belli kurallarla yapılmaktadır ve bu kurallar bir anahtar kod ile belirlenmektedir. Bu kod VPN sistemleri arasında sürekli, belli aralıklarla değişmektedir. Bu sayede bu kodun öğrenilmesi mümkün olmamaktadır.

- **Tanımlama-Sorgulama :**

Şifrelenmiş paketler, aynı zamanda şifreleme işlemini yapan kaynak VPN sisteminin imzasını taşımaktadır. Bu imzanın konmasının iki amacı bulunmaktadır. Birincisi gönderilen veya alınan mesajın güvenilir olduğunu garantiye almak, ikincisi ise gönderen kişinin kimliğinin ortaya çıkarmaktır.

- **Tünelleme :**

VPN sistemleri, şifrelenmiş haberleşme paketlerini, diğer VPN sistemlerine, güvenliğin olmadığı kamu iletişim ağları üzerindeki sanal tüneller içerisinden yollarlar. Bu tüneller, gönderen ve alan VPN sistemlerinin IP adreslerinden oluşmaktadır. Gönderilen bilgi ise bu paketler içerisine "yeni bilgi ekleme" yöntemi ile konulmuştur. Gerçek gönderen ve alan kullanıcıların IP adresleri de bu sayede saklanmış olmaktadır.



Şekil 5.6 VPN Çözümleri

Yukarıdaki şekilde VPN çözümleri ile ilgili bir örnek uygulama görülmektedir. Çizimden de anlaşılacağı gibi, yerel iletişim ağında kurabilecek "Intranet" yapısını, İnternet'te de tam güvenli bir yapıda kurulabilir. Bu ağa bağlanmak istenildiğinde, uzaktaki iletişim ağlarına birer adet VPN sistemi konulmakta ve uzaktaki ağlarla İnternet altyapısı kullanılarak güvenli bir şekilde haberleşilebilmektedir. Ayrıca İnternet üzerindeki bir kullanıcı da güvenli olarak özel iletişim ağı ile haberleşebilmektedir. Bu kullanıcının üzerine özel bir yazılım yüklenmesi yeterlidir.

Şirketler kamu iletişim ağlarını kullanarak, uçtan uca, özel iletişim ağlarına güvenli bir şekilde ulaşabilmek için sanal güvenlik ağlarını VPN kullanırlar. VPN tipleri iki ana başlıktan ele alınabilir[14].

- **Girişim VPNleri:**

o Siteden Siteye VPNler: İnternet gibi bir ağ üzerinden çeşitli şifreleme metodları ile uzaktaki ofislerin, merkezdeki ofislere güvenli bir şekilde bağlantısını sağlar
o Uzak Erişim VPNler: Gezici kullanıcıların (modem kullanıcıları, uzak kullanıcılar) şirket içi ağlarına İnternet üzerinden, şifreli ve güvenli bir şekilde bağlatısını sağlar
o VPN-İstemciler: Donanım, yazılım, kablosuz istemci çözümleri ile merkezdeki VPN cihazlara bağlanarak, güvenli bir şekilde şirket içi ağa ulaşma imkanını sağlar

- **Servis Sağlayıcı VPNler :**

o MPLS Çözümleri: MPLS tabanlı VPN ağları Frame Relay ve ATM'in güvenlik ve servis kalitesini, IP'nin de ölçeklenebilirlik özelliklerini aynı anda kullanıcıya sunmaktadır. MPLS IP yönlendirme yapan bir omurga üzerinde çalışmakta ve verilen servisle ilgili kararlar omurganın uç noktalarında ek bir işlem yükü gerektirmeden yapılabilmektedir. MPLS-VPN aynı zamanda Frame Relay'de ve ATM'de yapılması gereken karmaşık protokol ve adres dönüşümlerini ortadan kaldırmaktadır Sonuç olarak Frame Relay ve ATM ağlarında güvenlik için gerekli olan dört öge; adres alanı ayrılması, yönlendirmenin tamamen bağımsız yapılması, saldırılara dirençli olması ve IP Spoofing'e karşı dirençli olması özellikleri MPLS'de de sağlanmaktadır. Bu anlamda ikinci ve üçüncü seviye arasında çalışan bir protokol olarak düşünülebilen MPLS en az Frame Relay ve ATM kadar güvenlidir

- IPSec çözümleri: Bakınız: 2.3.12.1.3 IPSec

4.3.2.2 VPN'in Sağladığı Avantajlar

- Kiralık Hat bağlantılara göre daha düşük maliyet sağlar . Merkez-şube bağlantılarında %20-40 , gezici kullanıcıların ofis bağlantilarında %60-80 oranında bir kazanç sağlar
- Klasik WAN bağlantılarına göre daha esnek ve ölçeklendirilebilir bir yapı sağlar. Yeni şubeleri kolay ve hızlı bir şekilde bağlamak mümkündür
- Yönetim yükü, servis sağlayıcıya devredilebilir. Bu sayede ana ağa daha çok yogunlaşılabilir.
- Ağ topolojisinde basitlik sağlar. Servis sağlayıcının Frame Relay , ATM altyapısı kullanılarak Full-Mesh bir ağ topolojisi ile ağ karmaşası önlenir ve maliyet düşürülebilir
- Servis sağlayıcı üzerinden, WAN bağlantı yedekliliği ile Ağ bitiş süresini arttırmak mümkündür

4.3.3 Güvenlik Kuralları

4.3.3.1 Tüneller ve Şifreleme

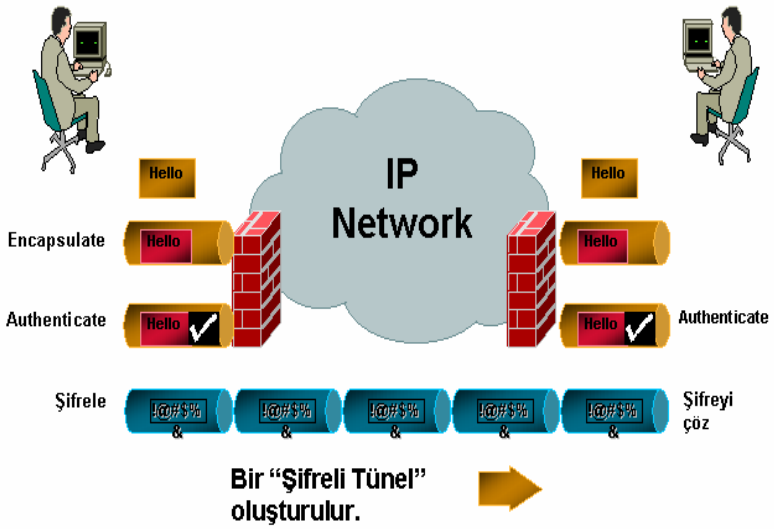
VPN çözümü ile gerektiğinde, şifrelenmiş tüneller kullanarak, bilgiye sadece izin verilen yerlerden ulaşılması ve çoklu protokol yeni bilgi ekleme sağlanabilir. Tüneller uçtan uca lojik bağlantı sağlarlar. Şifreleme, tünellenmiş bağlantıdaki, sadece izin verilmiş gönderen ve alıcıya ait veriye uygulanır. Güvenliğin daha az ihtiyaç olduğu durumlarda tünelleri şifrelemeden kurmak da mümkündür.

4.3.3.2 Tünel Teknolojileri

- **IPSec:** IETF tarafından geliştirilmiş, IP iletişim ağları üzerinden güvenli iletişimi sağlayan açık bir standarttır
- **PPTP:** Bir istemci-sunucu tünel protokolüdür. Bilgi transferi için GRE kullanır
- **L2TP:** Cisco ve bir çok firma tarafından da desteklenen "dial access VPN" de kullanılan açık standartlardir. Bir çok özelliğini LTF ve PPTP den almıştır
- **GRE:** Cisco ya özel bir protokoldür. Protokol spesifik tünel oluşturabilen bir yeni bilgi ekleme yöntemidir, şifrelemeyi desteklemez

4.3.3.3 Paket Doğrulaması

Paylaşılmış bir ağda verinin güvenilirliği en çok kaygı duyulan durumdur. Güvenilir olmayan bir ağda, bilginin içeriğinin değiştirilip, hatalı bir şekilde gönderilmesi mümkündür. Paket tanımlama-sorgulama, IP paketinin başına başlık ekleyerek paketin doğruluğunu kontrol eder.



Şekil 4.7 Paket Doğrulaması

4.3.4 Linux'ta Güvenlik Duvarı Kavramı

İnternet'ten korunmak için geliştirilmiş olan bir güvenlik önlemi olan bilgisayarlardaki Güvenlik Duvarı'nın en basit hali bir Linux cihazıdır.Bir ethernet kartı ile İnternet'e diğer ethenet kartı ile de ağa bağlıdır.İnternet'in akan ya da İnternet'e giden verilerin filtreleme işlemini yapar.Böylece ağ içinde servisleri denetleme konusuna daha az özen gösterilebilir.Güvenlik Duvarı kurma aşamasında Ipchains adı verilen bir program kullanılır.Örneğin aşağıdaki komut ;

#ipchains –l input –p TCP –s 192.168.1.11 telnet –j DENY –l

belirtilen IP numarasından gelen telnet portuna ulaşımı engelleyecektir.Ayrıca yine Ipchains kullanarak 6000:60003 arası portlara ulaşımı dışardan kapatmak yaralı olacaktır;

#ipchains –A input –i eth0 –p tcp –y –destination –port 6000:60003 –j DENY

IP Tables/Netfilter ise yine Linux ortamnıda kullanılabilen Ipchains programının bir üst versiyonu olan Güvenlik Duvarıdır.Paket filtreleme ,NAT gibi uygulamaların gerçekleştirilmesini sağlar.

4.4 İnternet Politikası

Kurum bazında her kullanıcının dış kaynaklara yani İnternet'e erişmesine gerek yoktur. İnternet erişiminin yol açabileceği sorunlar aşağıdaki gibidir:

- **Zararlı kodlar:** Virüs veya Truva Atı gibi zararlı yazılımların sisteme girmesine yol açabilir. Virüslerden korunmak için her kullanıcının makinesına bir anti virüs yazılımının kurulmasını sağlamak veya İnternet (http, e-posta, ftp) trafiğini sunucularda tarayıp temizledikten sonra kullanıcıya ulaştırmak gibi önlemler alınabilir. Sistemde güvenlik açıklarına neden olacak Truva Atlarını engellemek için güvenlik duvarlarında kesin kurallar konulmalıdır.

- **Etkin Kodlar:** Programların web üzerinde dolaşmalarına olanak sağlayan Java ve ActiveX gibi etkin kodlar saldırı amaçlı olarak da kullanılabilmektedir. Java, denetim düzenekleri ile bu tür saldırıların gerçekleşmesini önleyen bazı olanaklar sunmasına karşın ActiveX için aynı şeyden söz etmek mümkün eğildir. Bu nedenle bu kodların kullanıma ilişkin ayarlar İnternet tarayıcısı üzerinde yapılmalıdır.

- **Amaç dışı kullanım:** İnternet hattı, kurumun amacı dışında da kullanılabilmektedir. Bu durum hat kapasitesinin gereksiz yere dolduracağından kurumun dış kaynaklara erişim hızında yavaşlamalara yol açabilecektir.

- **Zaman Kaybı:** İnternet hattının amaç dışı kullanımı iş verimini azaltabilir. Bunu engellemek için kurum politikasında bazı kullanıcılara İnternet erişimi verilmeyebilir veya belirli saatlerle kısıtlanabilir. Farklı bir çözüm ise web erişimini denetim altına almak ve ulaşılabilecek web sitelerini belirlemektir. Bu denetimler farklı kullanıcı gruplarına farklı şekillerde uygulanabilir.

Kurumda dış kullanıcılardan (çalışanlar, ortaklar, müşteriler veya diğerleri) kimlerin kurum ağındaki hizmetlere erişebilecekleri ve ne tür erişim haklarına sahip oldukları tanımlanmalıdır.

4.5 Şifre Yönetimi Politikası

Şifreler kullanıcıların ulaşmak istedikleri bilgilere erişim izinlerinin olup olmadığını anlamamızı sağlayan bir denetim aracıdır. Şifrelerin yanlış ve kötü amaçlı kullanımları güvenlik sorunlarına yol açabileceğinden güvenlik politikalarında önemli bir yeri vardır. Eğer gerekli güvenlik sağlanamamışsa, yeterli kaynak ve zaman olduğunda her şifre kırılabilmektedir . Ayrıca kurumlar güvenlik politikalarında şifre seçimi ile ilgili aşağıdaki kısıtlamaları belirleyebilmektedirler[5].

- Şifrenin boyutu ve içeriği
- Süre dolması (eskime) politikası
- Tek kayıt ile herşeye erişim (SSO) politikası

4.6 Fiziksel Güvenlik Politikası

Bilgisayar veya aktif cihazlara fiziksel olarak erişebilen saldırganın cihazın kontrolünü kolaylıkla alabileceği unutulmamalıdır. Ağ bağlantısına erişebilen saldırgan ise kabloya özel ekipmanla erişerek hattı dinleyebilir veya hatta trafik gönderebilir. Açıkça bilinmelidir ki fiziksel güvenliği sağlanmayan cihaz üzerinde alınacak yazılımsal güvenlik önlemlerinin hiç bir kıymeti bulunmamaktadır. Kurumun ağını oluşturan ana cihazlar ve hizmet sunan sunucular için alınabilecek fiziksel güvenlik politikaları kurum için belirlenmelidir[2].

5. AĞ CİHAZLARI

Bilgisayar ağları üzerinde farklı işlevler sahip iletişim birimleri kullanılır.Bu birimlerin işlevleri incelendiğinde, OSI modelindeki ilk üç katmanın işlevlerinin yerine getirdikleri görülür.Gateway dediğimiz donanım/yazılım birimlerinin işlevlerinde ise böyle bir kısıtlama olmayıp bazen OSI'nin yedi katmanının tamamının işlevlerini içere bilmektedirler.
Ağ donanım birimleri yerel ağlar üzerinde ve yerel ağlar veri iletişiminde ortaya çıkan sınırlamaları ve problemleri aşmak için kullanılan donanım birimleridir.Bu problemler:

- LAN ortamının sınırlaması/kısıtlanmasından kaynaklanan problemler(mesafe, kullanıcı sayısı vb)

- Farklı ortam erişim yöntemi kullanan farklı ağlar arasında veri paketlerinin iletilmesi gerekliliği karşısında ortaya çıkan problemler(Ethernet,Token-Ring vb)

- Uyumsuz (farklı)ağ katmanı protokollerini kullanan sistemlerin iletişiminin gerektiği durumlarda karşılaşılan problemler

5.1 Ağ Bağlantı Birimleri

- **İletişim Ortamı Konnektörleri**

Her birim gerek iletişim ortamına gerekse birbirlerine bağlamak için konnektör kullanmak gereklidir.T-Konnektör,RJ-45,IBM konnektör,DB-25, DB-15.V-35,V-24 gibi örnekleri vardır[13].

- **Ağ Arabirim Kartları**

Ağ arabirim kartları fiziksel ya da mantıksal olarak bilgisayar ya da diğer ağ birimleri ile aktarım ortamını birleştiren elemanlardır.

➢ **Tranciever:**Bütün ağ arabirim kartları bazı tip trancieverları yapılarında bulundururlar.Trancieverlar iletişim ortamına elektrik ya da elektromagnetik olarak sinyalleri gönderip alan cihazlardır.

➢ **Ağ Arabirim Kart(NIC):**Ağ kartları ya da ağ adaptörleri konağı ağ ortamına adapte eden yardımcı cihazlardır.Bu kartlar genelde bilgisayarın ana kartında bir slota takılabilen baskı devreli kartlardır.Notebook,laptop tipi cihazlarda ise PCMCIA kartı büyüklüğünde olur.Ağ kartları ikinci katman cihazlarıdır.

➢ **Taşıma Ortam Adaptörü :** Bu cihazlar farklı iletişim ortamına bağlı farklı tipteki konnektör kullana ortamlarına birbirine bağlamak için kullanılır[2].

- **Modemler**

Modemler sayısal sinyal kullanan bilgisayarları telefon hatları ya da elektromagnetik dalgaları kullanarak birbirine bağlayan cihazlardır. Modemler sayısal sinyal kullanan ortamdan aldığı sinyali analog sinyale çevirerek aktarım ortamı üzerinden karşı modeme iletir.Karşı modem de ters işlemden geçirdiği sinyali buradaki sayısal sinyal kullanan bilgisayara iletir.

- **Tekrarlayıcılar**

Sayısal ve analog sinyaller sayısal bilgi taşırlar.Sinyal zayıflaması,gürültü gibi etkenlerden veri bütünlüğü bozulmadan ancak belirli bir mesafe uzaklığı gidebilir.Basit bir sinyal kuvvetlendirici iyi bir çözüm değildir.Çünkü bu sinyal kuvvetlendirici sadece sinyali kuvvetlendirmekle kalmayacak sinyalle birlikte olan gürültüyü de güçlendireceklerdir.Tekrarlayıcılar tekrar sinyal üretme ve verinin aktarımı ile ilgilendirdiklerinden fiziksel katman birimi olarak çalışırlar. Tekrarlayıcı diğer katmanlara ilişkin adres şemaları ve verinin yapısı ile ilgili herhangi bir işlem yapmazlar sadece alınan veriyi tekrar iletirler.Bir tekrarlayıcı,gelen veriyi saklar ve bunu tekrar oluşturarak sinyali diğer tarafa gönderir.Yeni sinyal alınan orijinal sinyalin aynısıdır ve yeni segmentte ilerleyebilmektedir.Teorik olarak bu işlem gerektiği kadar kullanılabilir.Ancak pratikte birçok bilgisayara ağı alıcı ve verici arasındaki tekrarlayıcı sayısına sınırlama getirmektedir.

- **Köprüler**

Köprü, veri iletim katmanında iki yerel ağ parçasını bağlamak için kullanılmaktadır. Veri iletim katmanı olarak köprü istasyonların fiziksel adreslerini kullanmaktadır. Bir defa belirlendikten sonra, köprüler, fiziksel adres bilgisine bağlı olarak mesajı diğer parçaya iletmekte ya da iletmemektedir. Köprüler tekrarlayıcılardan farklı olarak seçicidirler. Köprüler fiziksel adreslerine göre LAN segmentleri arası iletilen çerçeveleri filtreleyerek, LANlar arası tekrarlayıcılar gibi iletişim köprüsü sağlamanın yanında parçalardaki veri trafiklerini birbirinden ayrı tutarak her bir parçanın daha verimli çalışmasını sağlayan birimlerdir. OSI modelinin veri iletim katmanına kadar olan kısmında çalışırlar.Eğer bir fiziksel parçanız ya da tekrarlayıcılar ile birbirine bağlanmış fiziksel parçalarınız varsa ve hattın performansı kabul edilemez düzeylerde ise parçaları bölerek bunları köprülerle birbirine bağlamanız gerekir.Köprüler veri iletim katmanına kadar çalıştıkları için tekrarlayıcılar ile aynı işlevleri gerçekleştirmelerinin yanı sıra filtreleme sayesinde LAN'ın toplam performansını arttırırlar ve bütün üst düzey protokol paketlerini uygun parçalar arasında iletilirler.Köprüler tipik olarak benzer ortam erişim protokollerini birbirine bağlarlar.Fakat tanım olarak farklı protokolleri de birbirine bağlama özellikleri vardır.Saydam Köprü,Kaynak-Yönlendirme Köprü ,Kaynak-Yönlendirme-Saydam Köprü ve Uzak Köprü olmak üzere çeşitleri vardır.

- **Hublar**

Bu cihazlar da tıpkı tekrarlayıcılar gibi ağ sinyallerini bit seviyesinde kuvvetlendirirler.Tek fark hubların bu işlemi birden fazla konak için yapmasıdır.Bu sebeple bu cihazlara çok portlu tekrarlayıcı denilir.

Hub kullanma sebeplerinde ikisi kablolama yapısı için bir merkez oluşturmak ve ağın güvenilirliğini arttırmaktır.Tek bir kabloda oluşan hatanın tüm ağa dağılarak ağın çökmesi hub kullanılarak önlenmiş olur.Oysa hat topolojide kabloda oluşan hata tüm ağın çökmesine sebep olabilir.Hublarda OSI fiziksel katman cihazlarıdır.çünkü sadece aldıkları işareti güçlendirerek diğer tüm portlara iletirler.

Hublar için değişik sınıflandırmalar mevcuttur.Bunlardan ilki aktif ve pasif hublardır.Günümüzde kullanılan hublar aktiftir.Bunlar bir güç biriminden enerji alarak ağ işaretini tekrarlarlar.Pasif hublar ise aldıkları işareti sadece çoğullar.Bu cihazlar işareti tekrar oluşturmadıkları için kablo uzunluğundan doğacak sorunları gideremezler.

Hublar için yapılan ikinci sınıflandırmada ise cihazlar akıllı ve aptal olarak ikiye ayrılırlar.Akıllı hubların konsol portları bulunur.Böylece cihazın konsola bağlanıp ağ trafiğini yönetmek üzere programlamak mümkündür.Diğerlerinde ise herhangi bir yönetim ya da programlama imkanı yoktur[2].

- **Çoğullayıcı**

Birden fazla iletim ortamından gelen sinyalleri tek bir iletim ortamı ile iletmek için kullanılan cihazlardır. Bu cihaz OSI referans modelinin fiziksel katmanında çalışır.

- **Anahtar**

Anahtarlar ikinci katman cihazlarıdır ve çok potlu köprü adlandırılır. Tıpkı tekrarlayıcı hub arasında olduğu gibi köprü anahtar arasındaki fark da anahtarın birden fazla parça bir araya getirebilmesidir.Parçalara Ayırma ,aynı fiziksel ortamı paylaşımlı olarak kullanan kullanıcıların özel birimler aracılığı ile ağ trafiği açısından birbirlerinden ayrılmış daha küçük fiziksel ortamların yaratılması olayıdır.Fiziksel ortamın bölüştürülmesi ağ trafiğinin de bölüştürülmesi sonucunu beraberinde getirir.Bu da kullanıcıların aynı ortamdan daha fazla bant genişliği kullanabilmelerine olanak tanır.İlk bakışta hub ve anahtarlar birbirine oldukça benzer görünürler.Her ikisinin de birçok portu vardır ve bağlantıları bir noktada toplayarak ağdaki karmaşayı azaltırlar.Hub ve anahtar arasındaki fark cihazın işlevidir .

Anahtarların fiziksel adreslerine göre bazı kararlar alabilme yetenekleri vardır.Hublar ise hiçbir karar verebilme mekanizmasına sahip değillerdir.Anahtarlama ağ ortamındaki çerçevelerin içerdikleri başlık bilgisine göre köprülerde olduğu gibi yönlendirilmelerini sağlayan bir işlemdir.Bu yönlendirilmede esas alınan fiziksel adreslerdir.Bu yönlendirme tekniğinde aynı anda birden fazla port arasında köprü kurulabilmektedir.Bu özelliği sayesinde bazı anahtar gerçekleştirmeleriyle sanal LANlar oluşturulabilmektedir.Anahtarlar bu yetenekleri sayesinde bir LAN'ı daha hızlı ve verimli hala getirirler. Anahtarlama işlemi alınan veriyi sadece uygun porta yönlendirirken diğer portları meşgul etmemiş olur.Oysa hub veriyi tüm portlarına gönderir ve her konak bu veriyi işlemek zorunda kalır.İki çeşit anahtarlama yöntemi vardır:

- **Depola ve Gönder:** Gelen çerçeveler çıkış portuna gönderilmeden önce bir tampon alanda tutulur, CRC kontrolünden geçirilirler ve kontrol sonucu hatasız çıkan çerçeve

çıkış portuna aktarılır,hata bulunan çerçeve ise çöpe atılır.Yani bu tür anahtarlarda çerçeveler üzerinde tam bir hata kontrolü yapılmaktadır.Böylece ağın güvenilirliği artmaktadır.Ayrıca çöpe atılan çerçevelerin çıkış portuna gönderilmemesi gereksiz ağ trafiğinin oluşmasını önler,bant genişliği korunmuş olur.Ancak bu anahtarlama da gecikme değeri büyük olmaktadır.

- **Doğrudan-Kes:**Bu metodda tüm çerçeve değil sadece çerçevenin başlık kısmı üzerinde işlem yapılır. Bu başlık kısmında fiziksel adres bilgileri yer almaktadır.Bu anahtarlamada gecikme parametresi olarak sadece anahtarın fonksiyonel gecikmesi ve gerekli değerlendirme kısmının gecikmesi yer alır.Bu anahtarlama yöntemi Depola ve Gönder anahtarlamaya göre 20 ile 30 kat daha hızlıdır.Bu yönteme göre geliştirilmiş üç tür alt yöntem vardır. Bunlar;

  - **Doğru- Doğrudan-Kes:** Bu anahtarlama yönteminde çerçevelerin ilk altı baytlık bölümü (ki burada bilindiği üzere hedef konağın fiziksel adresi saklıdır) incelenerek, anahtarlanarak çıkış portu belirlenir.

  - **Fragment-free-cut-through:** Bu tip anahtarlarda bant genişliği kullanımını arttırmak için tanımlanandan daha kısa çerçeveler anahtar üzerinde seçilerek elenir. Bu anahtarlamada çerçevenin ilk 64 baytlık kısmı okunur ve incelenir. Dolayısıyla gecikme değeri Doğru-Doğrudan-Kes'e göre gecikme daha fazladır.

  - **Adaptif-Doğrudan-Kes:** Bu anahtarlama yöntemi bundan önceki iki yöntemi birlikte kullanır ve en iyi performans ve ağ güvenliğini sağlar .

Ağ üzerinde bir konak diğerine veri göndereceği zaman onun hem mantıksal hem de fiziksel adresini bilmek zorundadır.Mantıksal adresi bilinen bir makinenin fiziksel adresini öğrenmek için ARP kullanılır. ARP adreslerini bulmanın çeşitli yolları vardır. Bazı cihazlar kendileriyle aynı LAN üzerinde bulunan tüm cihazların fiziksel adresini ve mantıksal adreslerini bir tabloda tutarlar. Bu tablo ARP tablosu olarak anılır. Bir mantıksal adrese veri gönderecekleri zaman bu tabloda eşleştirerek fiziksel adresini elde ederler.Eğer tablosunda bu bilgi yoksa ARP isteği adı verilen bir işlem başlatır. Önce bir ARP istek paketi oluşturulur. Bu pakette MAC adresini öğrenmek istediği cihazın IP

adresi yer alır. Basitçe bu paket “IP adresi x olan konağın MAC adresi nedir?” sorusunu içermektedir.

Oluşturulan ARP istek paketi tüm ağa yollanır. (Yayınlanan) Paketi yayın yapmak için hedef adresi olarak yayınlanan MAC adresi (FF FF FF FF FF FF) kullanılır. ARP isteği LAN üzerindeki tüm cihazlar tarafından alınır ve her cihaz pakette yer alan IP adresini kendisininkiyle karşılaştırır. Eğer pakette yer alan IP adresi kendi IP adresi ise bu isteğe cevap olarak kendi MAC adresini gönderir. Bu pakete de ARP cevabı adı verilir. Bu cevabı alan konak ARP tablosuna bu bilgiyi ekler.

Aynı fiziksel segment içinde bulunan cihazlar ARP sayesinde birbirlerinin MAC adresini öğrenebilirler ve ARP Yayınlanan (broadcast) yoluyla çalışmaktadır. Bir yönlendirici ile bağlı farklı parçalar olduğunda ve parçalar arası veri iletimi gerektiğinde (Normalde yönlendiriciler parçalar arası yayın trafiğini geçirmez), kaynak konak veriyi zorunlu ağ geçidine gönderir.Zorunlu ağ geçidi, kaynak konağın bulunduğu parçanın bağlı olduğu yönlendirici arayüzüdür [2].

5.2 Ağlar Arası Bağlantı Birimleri

- **Yönlendiriciler**

Yönlendiriciler Ağ katmanı cihazlarıdır. Bu cihazların da anahtarlar gibi karar verme mekanizmaları vardır. Ancak anahtarlardan farklı olarak fiziksel adres yerine ağ adresine bakarlar. Ayrıca birbirinden farklı ikinci katman ağlarını(FDDI, Token-Ring, Ethernet gibi) birbirine bağlayarak bunlar arasında geçiş görevi görürler. Ağ katmanı bilgilerini baz alarak paketleri yönlendirebilen yönlendiriciler bu yeteneklerinden ötürü İnternet’in iskeletini oluşturmaktadırlar. Yönlendiricilerin temel görevi gelen paketi incelemek, bu paket için ağ üzerinde en iyi yolu belirlemek ve bu yolu izlemek üzere paketi en uygun portundan dışarı göndermektir. Yönlendiriciler özellikle büyük ağlarda trafiği düzenlemek için kullanılan en önemli cihazlardır. Bir yönlendirici çok çeşitli tipte portlara sahip olabilir:WAN bağlantısı için seri port, yönetim için konsol port, LAN bağlantısı için ethernet port.

Genelde bir ağ üzerinde kaynaktan hedefe doğru birden fazla yol bulunmaktadır. Bu yollar arasından en uygun yolu seçmek yönlendiricin görevidir ve yönlendirme olarak adlandırılır. Yönlendirici yol seçimi yaparken tüm ağ yapısını göz önünde bulundurur. Ağ yapısına ait bu bilgiler sistem yöneticisi tarafından konfigüre edilebilir ki buna statik

yönlendirme denir. Statik yönlendirme; yönlendirme bilgilerinin sistem yöneticisi tarafından elle yönlendiricilere tanımlanması ve gerektiğinde güncellenmesidir. Yani bu yöntemde yönlendirme tabloları elle oluşturulur ve topolojide herhangi bir değişiklik olduğunda tablo yine aynı şekilde güncellenir. Ağ üzerinde bazı işlemler sayesinde yönlendirme işlemi dinamik olarak da yapılabilir.Buna dinamik yönlendirme denir. Dinamik yönlendirme işleminde ise bilgiler yönlendirme protokolleri sayesinde otomatik olarak güncellenir. Topolojide veya trafik akışında herhangi bir değişiklik olduğunda yönlendiriciler birbirlerine mesaj göndererek bu değişikliği haber verir ve tablolarını günceller. Dinamik yönlendirme özellikle büyük ağlarda statik yönlendirmeye tercih edilmelidir. Sistem yöneticilerine büyük kolaylık sağlaması dışında ağın en etkin biçimde kullanılmasını da sağlamaktadır. Dinamik yönlendirme işleminin başarısı temel olarak yönlendiricide iki işlemin düzgün yapılmasına bağlıdır:

- Yönlendirme tablosunun bakımı
- Güncelleme bilgilerinin zamanında ve eksiksiz olarak bazı standartlar içerinde diğer yönlendiricilere iletilmesi

Dinamik yönlendirme bilgi paylaşımını sağlamak için yönlendirme protokollerini kullanır. Yönlendirme Protokolü, yönlendiriciler arasında yönlendirme bilgilerini paylaşmak için kullanılır. Mesaj alış verişi sadece yönlendirici arasındadır ve birbirleriyle yönlendirme tablolarını paylaşmalarını sağlar. RIP, IGRP, EIGRP, OSPF yönlendirme protokolleridir. Örneğin bir yönlendirme protokolü

- güncelleme mesajlarının nasıl gönderileceğini
- bu mesajların içinde hangi bilgilerin bulunacağını
- bu mesajların ne zaman gönderileceğini
- mesajları kimlerin alması gerektiğini

belirler. Ağ katmanı, verinin kaynaktan hedefe doğru en iyi şartlarla iletilmesi için IP yönlendirme tabloları kullanmaktadır. Bu tablolar temel olarak hedef ağ adresi ve sonraki adım çiftlerinden oluşur. Yönlendirici kendisine bir paket geldiğinde bunun hedef adresine bakar. Bu hedef adresinin kendi yönlendirme tablosunda bulunup

bulunmadığını kontrol eder. Eğer varsa bu hedef için belirlenmiş olan sonraki adımı öğrenir ve paketi o porta yollar. Eğer hedef adresini tabloda bulamazsa paket zorunlu yönlendiriciye gönderilir. Yönlendirme işlemi sırasında IP paketleri her seferinde sadece bir adım atarak bir sonraki cihaza ulaşırlar ve her durakta gidilecek sonraki nokta yönlendirme tablosuna bakılarak yeniden belirlenir.

Özetle; bir yönlendirici verilerin ağ üzerinde iletimini iki temel fonksiyon kullanarak gerçekleştirir:

- Yol seçimi
- Anahtarlama

Yol seçimi, paketlerin hedefe ulaşmak için kullanacakları en uygun yolun belirlenmesidir.Anahtarlama işlemi ise paketin yönlendirici tarafından bir arayüzden kabul edilip başka bir arayüzden dışarı gönderilmesi, yani paketin bir arayüzden diğerine yönlendirilmesi işlemidir. Bu yönlendirme ise yol seçimi sonucunda alınan karara göre yapılmaktadır.

Bir yönlendirme algoritmasının, yönlendirme tablolarını oluşturuken, en önemli amacı tablonun en iyi bilgilerden oluşmasını sağlamaktır. Her algoritma en iyinin hangisi olduğuna kendine ait bir yolla karar verir. Bu karar verme mekanizması sırasında ağ üzerinde her yola bir numara verir. Bu numaraya metrik adı verilir. Genellikle metriği en küçük olan yol en iyi yoldur.

Metrikleri yolun tek bir özelliğine bakarak belirlemek mümkündür. Ya da birkaç özelliğin gözönüne alınmasıyla daha karışık ancak daha etkin metrik değerleri hesaplanabilir. Yönlendiriciların en çok kullanığı metriklerden bazıları şunlardır:

- **bant genişliği :** Hattın veri taşıma kapasitesi (Örneğin 10 Mbps Ethernet hattı, 64 Kbps bir hatta tercih edilebilir)
- **gecikme :** Paketin kaynaktan hedefe ulaşması için geçen sürenin uzunluğu
- **yük :** Hat üzerindeki aktivite miktarı
- **güvenilirlik :** Hat üzerindeki hata oranı

- **adım sayısı :** Paketin yolculuğu sırasında kaç adet yönlendiricidan geçtiği
- **maliyet :** Genellikle bant genişliği, parasal değer, ya da başka bir ölçüte göre sistem yöneticisi tarafından keyfi olarak belirlenen bir değer.

Her yönledirme protokolü farklı metrik kullanır. Örneğin RIP (Yönlendirme Bilgi Protokolü) tek bir metrik (adım sayısı) kullanırken, başka protokoller örneğin IGRP, birden fazla metriği birarada kullanır.

5.3 Ağ Cihazlarının Güvenliği

Birçok kurum, bir güvenlik duvarı aldığında güvenlik sorunlarının çoğunu çözdüğünü sanmakta ve diğer önlemleri önemsemektedir. Oysa güvenlik yönetimi ağ üzerinde çalışan bütün elemanların güvenliğini içerir ve sürekli devam eden bir süreç olarak ele alınmalıdır.

Ağ cihazları yönetim açısından, yönetilebilir veya yönetilemez cihazlar olarak ikiye ayrılmaktadır.Yönetilebilir cihazların kendilerine özgü bir işletim sistemi ve konfigürasyonu bulunmaktadır. Cisco cihazlarda IOS ve CatOS, Alcatel XEON'larda XOS, Avaya cihazlarında Unixware, Juniper'de Free BSD örnek olarak verilebilir. Diğer cihazlarda da genelde UNIX tabanlı işletim sistemleri bulunmaktadır. Ağ cihazlarının ayarlanması, yönetimi ve kontrolü aşağıdaki şekillerde sağlanabilmektedir:

- HTTP protokolü ile
- Telnet veya SSH ile
- SNMP protokolü ile
- TFTP veya FTP ile
- Konsol portuyla

Konsol portu aracılığıyla erişimde fiziksel güvenlik ön plana çıkmaktadır. Diğer erişim türlerinde ise TCP/IP protokolü kullanılacağından bu protokolün zayıflıklarına karşı önlem alınması gerekecektir.

Cihazların ayarları menüler aracılığıyla, komut yazarak veya grafik arayüzlerle yapılabilmektedir. Cihazlarda kurulum sırasında oluşan varsayılan ayarların, kullanıcı tarafından aktif edilen bazı ayarların iptal edilmesi veya düzgün olarak tekrar ayarlanması gerekebilmektedir.

5.3.1 Fiziksel Güvenlik

Cihaza fiziksel olarak erişebilen saldırganın konsol portu aracılığıyla cihazın kontrolünü kolaylıkla alabileceği unutulmamalıdır. Ağ bağlantısına erişebilen saldırgan ise kabloya özel bir ekipmanla kabloya erişerek hattı dinleyebilir veya hatta trafik gönderebilir.Açıkça bilinmelidir ki fiziksel güvenliği sağlanmayan cihaz üzerinde alınacak yazılımsal yöntemlerin hiç bir kıymeti bulunmamaktadır. Bazı fiziksel güvenlik önlemleri aşağıda verilmiştir:

- Cihazlar sadece ağ yöneticisinin veya onun yardımcısının açabileceği kilitli odalarda tutulmalıdır. Oda ayırmanın mümkün olmadığı yerlerde özel kilitli dolaplar (kabinetler) içine konmalıdır

- Cihazlara fiziksel olarak kimin ve ne zaman eriştiğini belirten erişim listeleri tutulmalı ve bu listeler sık sık güncellenmelidir

- Kablolar tek tek etiketlenmeli ve kayıtları tutulmalıdır. Kullanılmayan kablolar devre dışı bırakılmalıdır

- Cihazların yakınına güvenlik bilgileri (şifre, IP adresi) gibi bilgiler yapıştırılmamalı ve gizli tutulmalıdır

- Cihazlara fiziksel erişim mümkün ise kullanılmayan portlar kaptılmalıdır

- Aktif cihazların elektriği aldığı güç kaynaklarının yeri belirlenmeli ve saldırganın bu güç kaynaklarını kesmesi engellenmelidir. Devamlı güç kaynaklarına (ups) yatırım yapılmalıdır

- Aktif cihazların fiziksel erişime açık olduğu yerlerde saldırganın güç kablosunu çıkartmasını engellemek için cihazın üstünde çeşitli aparatlar kullanmalı, güç kablosunu gözden ırak tutmalı, mümkünse uzakta ve fiziksel güvenliği sağlanan bir prize bağlanmalıdır

- Her ne kadar aktif cihazların çalınması pek olası olmasa da bu tür olayları engellemek için mümkünse çeşitli kilit ve alarm mekanizmaları kullanılmalıdır

5.3.2 Şifre Yönetimi

Şifreler cihazlara her türlü izinsiz erişim de hesaba katılarak iyi seçilmelidir. İyi şifrelerin özellikleri aşağıdaki gibidir :

- Büyük ve küçük harf içerirler
- Noktalama işaretleri ve rakamlar içerirler
- Bazı kontrol karakterleri ve/veya boşluklar içerirler
- Kolaylıkla hatırlanabilirler ve bu nedenle bir yere not edilme ihtiyacı duymazlar
- En az yedi veya sekiz karakter uzunluğundadırlar
- Kolay ve hızlı yazılırlar; ve böylece etraftan bakan birisi ne yazdığını anlayamaz

Şifre yönetmenin en iyi yolu TACACS+ veya RADIUS doğrulama sunucuları aracılığıyla onay mekanizmasını kullanmaktır. Bu sistem kullanılsa bile yetkili haklar için o cihaza yerel tanımlı bir şifre, konfigürasyon dosyasında bulunmalıdır. Birçok yönetilebilir cihaz, kullanıcı modu ve yetkili mod gibi iki ayrı login mekanizmasına sahiptir. Kullanıcı modunda sadece arayüzler incelenebilirken yetkili modda ek olarak cihaz konfigürasyonu da yapılabilmektedir.

5.3.3 Cihaz Erişim Protokollerine Dair Ayarlar

Ağ cihazlarının ayarlanması, yönetimi ve kontrolünde kullanılan HTTP, Telnet, SSH, SNMP, TFTP ve FTP; TCP/IP protokolünün alt elemanları olduklarından, bu protokolün zayıflıklarına karşı önlem alınması gerekmektedir. Bu türden erişimlerde denetim, bu cihazların ve dolayısıyla ağ trafiğinin güvenliği için çok gereklidir.

- **HTTP Erişimi**

HTTP protokolü ile web arayüzünden erişim, cihaza interaktif bağlantı demektir. Yönetilebilir cihazlarının birçoğunun üzerinde web sunucusu çalışır. Bu da 80 nolu portta bir web sunucunun kurulu beklediğini gösterir.HTTP servisi verilecekse bu ağ yönetimini sağlayan belirli IPlere kısıtlı olarak verilmelidir. Cihaz güvenliği nedeniyle mümkün olduğunca bu tür web üzerinden yönetimin kullanılmaması gerektiği önerilmektedir. Ama web üzerinden yönetim gerekiyorsa web sunucusu sadece sistem

yöneticisinin bileceği başka bir port üzerinden, örneğin 500 nolu portta çalıştırılabilecek şekilde ayarlanmalıdır.

HTTP protokolünde doğrulama mekanizması ağda şifrenin düz metin şeklinde gönderimi ile sağlandığı için efektif değildir ama farklı üreticilerin değişik çözümleri bulunmaktadır. Doğrulama mekanizması, onay sunucuları (Tacacs+, Radius …vb) kullanılarak yapılabilir. Cisco IOS'de doğrulama mekanizması ip http authentication komutuyla sağlanmaktadır [18].

- **Telnet ve SSH Erişimi**

Telnet ile erişimlerde saldırganın ağ üzerinden dinlenme yoluyla iletilen bilgiyi elde etmesi mümkün olduğundan, iletilen veriyi şifreleyen SSH protokolü mümkün olduğunca kullanılmaldır. Güvenli Kabuk, uzaktan erişim amacıyla kullanılan telnet ve FTP`nin güvenli bir alternatifidir. Güvenli olmasının nedeni , SSH `ta kullanıcı şifreleri de dahil olmak üzere tüm veri iletişiminin kriptolanarak şifreli olarak gerçekleşmesidir.Bu sayede ağ trafiği dinlenebilse bile, şifrenizin ya da iletilen başka herhangi bir verinin trafik içerisinden çıkartılması mümkün değildir. Bir makineye SSH`la bağlanabilmek için sunucu ve istemci tarafında çalışan bazı yazılımlar gerekir.

SSH şu anda bütün cihazlar ve cihaz işletim sistemleri tarafından desteklenmemektedir. Bu konuda üretici firmanın cihaz dökümantasyonu incelenmelidir.

- **SNMP Erişimi**

Basit Ağ Yönetim Protokolü, cihaz ve ağ yönetimi için vazgeçilmez bir protokoldür. Trafik istatistiklerinden bellek ve CPU(Merkezi İşlem Birimi) kullanımına kadar bir cihaz hakkında çok detaylı bilgiler edinilebilmektedir. Bir veya daha fazla Ağ Yönetim İstasyonu, üzerlerinde çalışan yazılımlarla belirli aralıklarla ağ cihazları ve sunuculardan bu istatistikleri toparlayacak şekilde ayarlanmalıdır. Cihazda gözlenen CPU, bellek veya hat kullanımının fazla olması bir saldırı tespiti olabilmektedir. Toplanan verileri grafiksel olarak görüntüleyen MRTG(Multi Yönlendirici Trafik Çizgeci) gibi programlar bulunmaktadır.

SNMP protokolünün,özellikle SNMP Version 1'in bir çok uygulamasında zayıflık olduğu CERT (Bilgisayar Acil Yanı Takımı) 'in raporlarında belirtilmiştir. Birçok cihaz üretecisi bu konuda yama çıkartmış ve önerilerde bulunmuştur.SNMP Version 1 ,

düz metin doğrulama dizileri kullandığından bu doğrulama dizilerinin parodi edilmesi söz konusu olabilmektedir. Bu yüzden MD5'a dayanan öz doğrulama şeması kullanan ve çeşitli yönetim verilerine kısıtlı erişim sağlayan SNMP Version 2'nin kullanılması gerekmektedir. Mümkünse her cihaz için ayrı bir MD5 gizli değeri kullanılmalıdır.
Öneriler:

- Sadece Oku ve Oku-Yaz erişimleri için kullanılan varsayılan SNMP şifre adları değiştirilmeli ve bu iki parametre birbirinden farklı olmalıdır

- SNMP şifrelerine kritik bir UNIX makinasındaki root şifresi gibi davranılmalıdır

- SNMP erişimi hakkı sadece belirli güvenilir IP'lere (Ağ Yönetim istasyonlarına) sağlanmalıdır

- Ağ Yönetim İstasyonu tarafından SNMP erişimi yapılırken "Sadece Oku" parametresi kullanılmalıdır. Mümkünse cihazlarda "Oku-Yaz" parametresi iptal edilmelidir

- Ağ Yönetimi için ayrı bir Alt ağ, mümkünse VLAN (Sanal Yerel Alan Ağı) yaratılmalıdır. Erişim-listesi ve Güvenlik Duvarı kullanılarak bu ağa dış ağlardan gelen trafik kısıtlanmalıdır

- Ağ Yönetim İstasyonları, ağdaki cihazlara ait SNMP şifre dizileri gibi doğrulama bilgileri bulundurdukları için doğal bir saldırı hedefi durumuna gelmektedir. Bu yüzden bu makinaların fiziksel, yazılımsal ve ağ güvenlikleri sağlanmalıdır

- **Yardımcı Port**

Yönlendiricilerde acil durumlarda telefon hatları üzerinden modem kullanılarak erişimin sağlanması için Yardımcı port bulunmaktadır. Bu tür bir erişim için PPP'de (Noktadan Noktaya Protokolü) PAP (Parola Onay Protokolü) yerine CHAP (Sorgulama Challenge Tokalaşma Onay Protokolü) doğrulama methodu kullanılmalıdır. CHAP, dial-up ve noktadan noktaya bağlantılarda uç noktayı engelleyerek izinsiz erişimleri engellemektedir.

- **TFTP- FTP ile Erişim**

Cihazlara yeni işletim sistemleri veya konfigürasyonları TFTP veya FTP gibi protokollerle yüklenebilmekte veya Ağ Yönetim İstasyonu'na yedek amaçlı alınabilmektedir. Özellikle TFTP protokolü, UDP kullanması ve kullanıcı-cihaz doğrulama sistemleri kullanmamasından dolayı bilinen bazı güvenlik açıklarına sahiptir. Bu yüzden bu protokoller cihazlarda erişim-listesi ile kontrol altına alınmalı ve dosya transferi belirli IPlerle sınırlandırılmalıdır. TFTP sunucu olarak kullanılan Ağ Yönetim İstasyonu'nda da bu protokolü kullanırken uygulayacağı ek güvenlik ayarları yapılmalı, mümkünse bu servis bu makinada sadece kullanılacağı zaman açılmalıdır. Cihaz FTP'yi destekliyorsa bu protokolün kullanılması tercih edilmelidir[2][3][13].

5.3.4 Yönlendiriciler Üzerinde Yapılacak Ayarlar

Yönlendiricilerin ağ trafiğinin önemli bir bölümünü taşıması onları saldırılar için çok önemli birer hedef haline getirmektedir. Hedef kuruluşun yönlendiricilerini ele geçiren bir saldırgan, yapabileceği pek çok başka saldırının yanında, ağı çalışmaz hale getirebilir.

- **Konfigürasyonların Düzenli Yedeklenmesi**

Yönlendiricinin ayarını her değiştirildiğinde, yapılandırma dosyasının bir kopyasını güvenlikli bir ortamda yedeklenir; bu amaçla TFTP ya da SNMP protokolünü kullanılır. Yapılandırma dosyaları erişim şifreleri gibi hassas bilgileri de içerdiğinden yedeklerinin güvenlikli ortamda saklandığından emin olunmalıdır.

Yedek yapılandırma dosyaları, bir saldırı sonrasında ağı yeniden işler duruma getirirken ya da yapılandırmada karşılaştırma yapmak için kullanılabilir.

Eğer mümkün ise, yapılandırma dosyaları üzerinde RCS(Konfigürasyon Yönetim Sistemi) gibi bir sürüm yönetim sistemi çalıştırabilir; böylece yönlendirici ayarlarını ne zaman, kimin, nasıl ve niye değiştirdiğini takip etmek çok daha kolay olur.

- **Gereksiz Tüm Hizmetlerin Durdurulması**

Yönlendiricinin temel işlevselliği için gerekmeyen ve pek az yapılandırmada kullanmanızın anlamlı olabileceği tüm hizmetleri durdurulur:

- **no cdp run :** CDP(Cisco Keşif Protokolü) hizmeti durdurulmaktadır.Eğer Cisco RMON kullanılmıyorsa bu hizmete ihtiyaç olmaz.

- **no service udp-small-servers :** UDP temelli echo, discard ve chargen hizmetlerinin durdurulmasını sağlar. Bu hizmetlerin verilmesi hiçbir zaman gerekli olmadığından çalışmamaları problem teşkil etmez.

- **no service tcp-small-servers :** TCP temelli echo, discard, chargen ve daytime hizmetlerinin durdurulmasını sağlar. Bu hizmetlerin verilmesi de hiçbir zaman gerekli olmadığından, çalışmamaları bir probleme neden olmaz.

- **no ip finger ya da no service finger :** CISCO IOS sürümünüze göre iki biçiminden birisi olarak geçerli olacaktır. Çalışan bir finger hizmeti, yönlendiriciye ya da erişim sunucusuna bağlı kullanıcıların bir listesinin alınmasına imkan verecektir. Bu komut, finger hizmetini tümüyle devre dışı bırakmayı sağlar.

- **no ntp server :**Yönlendirinin NTP(Ağ Zaman Protokolü) hizmetlerini durdurur. Eğer zaman senkronizasyonu için sunucu olarak yönlendirici kullanılmıyorsa (ya da bilgisayar sistemlerinin arasında zaman senkronizasyonunu hiç kullanmıyorsa) bu hizmet hiç endişe edilmeden durdurabilir.

- **no ip bootp server:**BOOTP hizmetini durdurmak içindir. Eğer disksiz istemciler açılış için Cisco yönlendiriciden BOOTP hizmeti almıyorsa (ya da hiç disksiz istemci yok ise) bu hizmetin durdurulması herhangi bir probleme neden olmayacaktır.

- **no snmp-server :** SNMP hizmetini durdurmak için kullanılır. Eğer bir ağ yönetim sistemine (MRTG, HP Openview vb.) sahip değinilse bu hizmet durdurabilir.

- **no ip http server :**Yönlendiricinin yönetimi için kullanılan web sunucu yazılımının

durdurulmasını sağlar. Yapılandırmanın web üzerinden yapılması özellikle tercih edilmiyorsa web sunucusuna ihtiyaç yoktur; pek çok Cisco yönlendirici öntanımlı olarak web sunucusu çalışmayacak biçimde ayarlıdır.

o **no ip identd :**Tanımlama hizmetini devre dışı bırakır.

- **Parola Denetiminin Kullanılması**

Ön tanımlı olarak, telnet erişimleri parola denetimsiz gerçekleşir. Parola denetimini gerçekleştirmek üzere aşağıdaki biçimde parola ataması yapabilir:

```
Router>en
Router #configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router (config)#line vty 0 4
Router (config-line)#login
Router (config-line)#password PAROLAM
Router (config-line)#access-class 2 in
Router (config-line)#exit
Router (config)#
```

- **Kaynaktan Yönlendirmenin Durdurulması**

Kaynaktan yönlendirme modern bir ağ üzerinde hiçbir zaman kullanılamayacak bir özelliktir. Kaynağından yönlendirilmiş paketlerin ağa girmesine müsaade edilmesi pek çok tehlikeyi de beraberinde getirir. Bunu engellemek üzere aşağıdaki komut ile kaynaktan yönlendirme durdurabilir:

```
Router (config)#no ip source-route
```

- **Yapılandırmanın Tamamlanması**

Çok popüler bir DOS(Hizmet Kesintisi) saldırısı olan Smurf,yönlendiricilerin eksik yapılandırmalarından faydalanır. Yönlendirilmiş yayınların ağa girmesinin engellenmesi, bir Smurf saldırısına alet olmayı engelleyecektir. Her bir ağ ara yüzü için aşağıdaki gibi bir komut setini işletmek gerekmektedir:

Router (config)#interface ethernet 0
Router (config-if)#no ip directed-broadcast

- **Günlük Kayıtların İzlenmesi**

Yönlendiricinin günlük kaydı aktif hale getirilir ve kurum içerisindeki bir UNIX syslog sunucusuna kayıt yapacak biçimde ayarlanır:

logging buffered
service timestamps log date msec local show-timezone
logging trap info
logging facility daemon
logging 10.0.0.1 bu satırda, kurum bünyesinde kayıt tutacak olan UNIX sunucusunun IP adresi verilmelidir.

UNIX sunucusu üzerindeki syslog yazılımının ayarları yapılarak yönlendiriciden gelen syslog kayıtlarını almasına izin verilmelidir.Günlük kayıtları UNIX sunucuya aktarılmaya başlandıktan sonra düzenli olarak izlenmeli ve tespit edilen problemlere hızla müdahale edilmelidir. Yönlendiricinin syslog kayıtlarını izlemek için logsurfer, swatch ya da logwatch gibi popüler özgür yazılımlardan faydalanılabilir[13].

- **Parolaların MD5 ile Korunması**

Parolaların daha güvenilir bir şifreleme algoritması olan MD5 ile şifrelenmiş biçimde depolandığından emin olunmalıdır; bu amaçla enable password komutu değil, enable secret komutu kullanmalıdır. no enable password komutu kullanılarak enable passwordler silinmeli yerine enable secret yeni şifreniz ile yeniden şifreler girilmelidir. Yönlendirici yapılandırılmasının bir kopyasının bir saldırganın eline geçmesi durumunda MD5 ile şifrelenerek saklanan parolanın deneme-yanılma ile bulunması çok daha uzun sure gerektirecektir:

Router >en
Router #configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router (config)#no enable password

Router (config)#enable secret yeni_şifreniz

- **Adres Şaşırtmacasına Geçit Verilmemesi**

IP erişim denetim listelerini kullanarak, yönlendiricinin adres şaşırtmacası saldırılarına karşı korunması sağlanmalıdır. Bu sayede, örneğin, yönlendiricinin İnternet'e bakan ara yüzünden iç ağınızdaki bir bilgisayarın IP adresi ile paketlerin ağa girmesi engellenebilir. İç ağın 10.0.0.0/24 C sınıfı adres aralığında ve ethernet 0 ara yüzüne bağlı olduğu, yönlendiricinin yalnızca İnternet ile iç ağın arasında konumlandırıldığı ve internet bağlantısının ethernet 1 ara yüzü ile gerçekleştirildiği durum için örnek yapılandırma satırları aşağıdaki gibidir:

Router (config)# no access-list 110
Router (config)# access-list 110 permit ip 10.0.0.0 0.0.0.255 any
Router (config)#access-list 110 deny udp any range 1 65535 any log
Router (config)#access-list 110 deny tcp any range 1 65535 any log
Router (config)#access-list 110 deny ip any any log
Router (config)#interface ethernet 0
Router (config-if)#ip access-group 110 in
Router (config-if)#exit
Router (config)#interface ethernet 1
Router (config-if)#ip access-group 110 out
Router (config-if)#exit

- **Ayrılmış Adres Bloklarından Ağa Girişinin Engellenmesi**

IANA tarafından özel amaçlar ve kurum içi kullanımlar için rezerve edilmiş IP adres bloklarından ağa paketlerin gelmesine engel olunması gerekir; internet üzerinde kullanılması beklenmeyen IP adreslerinden ağa doğru paketlerin gelmesinin makul bir açıklaması yoktur. IP erişim denetim listeleri ile bu engelleme gerçekleştirilebilir. İnternet bağlantısının ethernet 0 ara yüzü ile sağlandığı bir durum için örnek yapılandırma aşağıda verilmiştir:

Router (config)# no access-list 111
Router (config)#access-list 111 deny ip 10.0.0.0 0.255.255.255 any log
Router (config)# access-list 111 deny ip 127.0.0.0 0.255.255.255 any log

```
Router (config)#access-list 111 deny 169.254.0.0 0.0.255.255 any log
Router (config)# access-list 111 deny 172.16.0.0 0.0.255.255 any log
Router (config)# access-list 111 deny 192.168.0.0 0.0.255.255 any log
Router (config)# access-list 111 deny 224.0.0.0 0.255.255.255 any log
Router (config)# access-list 111 deny ip host 0.0.0.0 any log
Router (config)# interface ethernet 0
Router (config-if)#ip access-group 111 in
Router (config-if)#exit
```

- **Gereksiz ICMP Paketleri Filtreleme**

Yalnızca çok gerekli ICMP paketlerinin ağa girmesine müsaade ederek dağınık hizmet kesintisi saldırılarının (DDoS) bir kısmından kurtulunabilinir:

```
Router (config)# no ip access-list 112
Router (config)# access-list 112 deny icmp any any fragments
Router (config)# access-list 112 permit icmp any any echo
Router (config)# access-list 112 permit icmp any any echo-reply
Router (config)# access-list 112 permit icmp any any packet-too-big
Router (config)# access-list 112 permit icmp any any source-quench
Router (config)# access-list 112 permit icmp any any time-exceeded
Router (config)# access-list 112 deny icmp any any
Router (config)# access-list 112 permit ip any any
Router (config)#interface ethernet 0
Router (config-if)#ip access-group 112 in
Router (config)#exit
```

- **Router üzerinde NAT konfigürasyonu yapılması:**

Günümüzde iç ağda bulunan tüm konakların hemen hepsi tahsisli olmayan IP numaraları kullanmaktadır(Bkz:Tablo 3.1) ve bu adresleri içeren paketler İnternet üzerinde yönlendirilmez. Dış ağa açılan yönlendiriciler ise İnternet'de bilinen ve kendisine yönlendirme yapılabilen bir IP numarasına sahiptir. İç ağdaki konaklara erişimin sağlanabilmesi için NAT(Ağ Adres Çevrimi) desteği olan yönlendiriciler, kendisine iç ağdan gelen her paketin kaynak adresini kendi adresi olarak değiştirir. Kendisine İnternet'den gelen paketlerin de hedef adresini iç ağdaki ilgili konağın adresi

olarak değiştirir ve bu yolla iç ağdaki konakların İnternet üzerindeki konaklarla haberleşmesini sağlar. Bu işleme Ağ Adres Çevrimi denir.

Tablo 3.1 Tahsisli Olmayan Adresler

Ağ Maskesi	Ağ Adresi
255.0.0.0	10.0.0.0 – 10.255.255.255
255.255.0.0	172.16.0.0 – 172.31.255.255
255.255.255.0	192.168.0.0 – 192.168.255.255

NAT yapıldığı zaman, oluşan trafiğin İnternet'den görülen hali, İnternet'de bulunan tek bir konağın bazı İnternet alışverişleri yaptığıdır. İnternet'e, bu konağın arkasındaki ağın büyüklüğü, bu ağdaki konakların cinsi, sayısı, ağın yapısı vs. hakkında herhangi bir bilgi gitmez. Dolayısıyla NAT, yalnızca tahsissiz ağlardan İnternet'e erişimi sağlamakla kalmaz, ağınızdaki konaklar hakkında bilgi edinilmesini (ve dolayısıyla size karşı yapılabilecek saldırıları) zorlaştırır. Fakat bunun bir Güvenlik Duvarı olduğu düşünülmemelidir ama bazı Güvenlik Duvarları bileşenleri içinde NAT özeliği mevcuttur.

NAT desteği olan yönlendiricilerde üç çeşit konfigürasyon uygulanmaktadır:

- **Statik Çevrim :** Birebir iç bloktaki IP adreslerini dış IP adreslerine çevirme işlemidir.
- **Dinamik Çevrim:** Bir havuz yaratarak dinamik olarak içerdeki adresleri bu havuzdaki dış IP bloklarıyla eşleme işlemidir.
- **PAT (Port Adres Çevrimi):** Bütün konakları konak sayısına oranla daha az IP adresiyle dışarıya çıkarma işlemidir.PAT, çevrimleri birbirinden ayırmak için İç ağımızı dış ağa tanıtacak,dışarıda yönlendirilebilir adreslerde yegane port numaraları kullanır.Bu port numaraları 16 bit olarak kodlanabilir.Teorik olarak iç ağda kullanılan tahsissiz 65536 IP adresi dış ağa çıkarken tahsisli tek bir IP adresi kullanır.Ama bu pratikte karşımıza 4000 tahsissiz IP adresi olarak çıkar[7][8].

5.3.5 Anahtarlar Üzerinde Yapılacak Uygulamalar

Günümüzde artık her ağ teknolojisinin anahtarlar üzerine inşa ediliyor olması onları saldırılar için hedef haline getirmiştir. Günümüzde kullanımı azalsa da eskiden büyük güvenlik risklerini de beraberinde getiren hubların yerini alan anahtarlar de hublardan farklı olarak oturum sadece istemci ve sunucu arasında geçmekte ve bu şekilde anahtarlanmaktadır, böylece veri iletişimi çerçevede yapılmadığı için diğer sistemler paketleri okuyamamaktadır. Oysa hub kullanılan ağlarda oturum, iki sistemin iletişiminin çerçeve üzerinden akması ve bu trafiğin diğer sistemler tarafından da istenildiği durumda görülmesi büyük risk taşımaktaydı..Bu durumun riski çok açıktır;bu risklere en iyi örnekler bu iki sistem üzerinde akmakta olan verinin üçüncü şahıslarca yakalanması ya da araya girilmesidir.Bu noktada anahtarların sağladığı güvenliğin yeterli olduğu düşünülebilir; ancak durum hiçte öyle değildir. Aşağıdaki 3 yöntem kullanılarak bu koruma mekanizması aşılmaktadır.

1. ARP Spoofing
2. MAC Duplicating
3. MAC Flooding

Bu yöntemlerin temel amacı paketlerin saldırganın sistemi üzerinden geçmesini sağlamaktır;yani istemci paketlerini saldırganın sistemine saldırganda sunucunun sistemine göndermeli , cevaplarda yine bu şekilde sunucudan saldırgana ,saldırgandan istemciye gönderilmelidir. Böylece saldırgan istediği paketleri inceleme hakkı kazanacak, belki istemciye hiç söylemeyerek sunucuya, istemci göndermiş gibi bazı özel paketler göndererek yetki kazanmak isteyecektir. Yukarıda bahsi geçen 3 yönteminde aşağıda kısaca açık getirelim ;

- **ARP Spoofing** : Amacı ARP isteklerini dinlemek ve dinlenmesi gereken bir oturum olması durumunda o ARP isteğine sahte cevaplar vermek olan saldırı yöntemidir.
- **MAC Duplicating** : Bu tekniğin amacı ise yukarıda bahsi geçene çok benzer bir ethernet kartına birden fazla fiziksel adres atanarak ARP isteklerine yine sahte cevaplar vermeyi sağlayan yöntemdir.
- **MAC Flooding** : Diğerlerinden farklı olarak bu teknik anahtarı hedef almaktadır, çok fazla rastgele fiziksel adres göndererek anahtarın fiziksel adres tablosunu taşırmaya

ve bu şekilde paketlerin çerçeve üzerinden akmasını sağlamaya çalışır. Başarılı olması durumunda hedef anahtar ile hub arasında hiçbir fark kalmayacaktır.

Yukarıda bahsi geçen 3 atak (ARP Spoofing, MAC Duplicating, MAC Flooding) türü için oldukça fazla koruma yöntemi mevcuttur;anahtarlı mimarinin güvenli olduğu yanılsaması ve saldırıların içeriden gelme riskinin az olduğunun düşünülmesi(Hataların en büyüğüdür, CERT raporlarında %80 civarı saldırı şirket içi çalışanlardandır.) bu önlemlerin alınmasını engeller.Eğer sağlıklı ve güvenli çalışan bir ağa sahip olmak isteniyorsa bazı güvenlik önlemlerini almanın gerekliliği unutulmamalıdır, bu güvenlik önlemlerinden bazıları şu şekilde sıralanmaktadır :

- Anahtarlarda her porta bir adet fiziksel adres gelecek şekilde yapılabilecek bir değişiklik

- ARPwatch gibi bir program aracılığıyla ARP tablosundaki değişikliklerini takip etmek

- Yerel ağdaki tüm sistemlerde statik ARP tabloları oluşturmak ve kullanmak

- RARP programı ile ağda 2 adet aynı MAC adresinin bulunmasını saptamak

Statik yönlendirmeler belirlemekte bir güvenlik önlemidir;ancak yapılan testlerde windows sahte ARP istekleri karşılığında yönlendirme tablosunda statikten dinamiğe çevirmektedir.
Daha farklı önlemlerde bulunmasına karşın en etkili olanı ilk çözüm olan anahtarlarda her porta bir MAC adresinin eşlenmesini sağlamaktır. Böylece MAC flooding yapılmasında engellenebilir. Bazı kaliteli anahtarlar MAC Flooding'den etkilenmemektedirler.
Ayrıca VLAN (sanal ağ) kullanarak kullanıcıları fiziksel lokasyonundan bağımsız olarak gruplayıp, farklı alt ağlarda toplayarak da bazı güvenlik önlemleri almak mümkündür.Bir VLAN aygıtların veya kullanıcıların mantıksal gruplanmasıdır.Bu aygıtlar veya kullanıcılar fiziksel yerleri ne olursa olsun fonksiyonlarına,bağlı oldukları departmanlarına ya da uygulamalarına göre gruplandırılabilir.Sanal ağ tanımları anahtar üzerinde yazılım ile yapılır.Bu yazılımlar standart olmadığı için tüm ürünlerde farklılık

göstermektedir. Sanal ağ uygulaması kullanmak tek başına bir güvenlik önlemi sayılmamakla beraber bir güvenlik artışı olmaktadır. Ağ yönetimi için ayrı bir sanal ağ yaratılmalıdır. Bölgeler sanal ağ trafiklerine göre eleme yapılarak ayrılmalı, sadece o bölgede kullanılan sanal ağlar iletilmelidir.

Sanal ağ bilgilerini ve bütün ağ trafiğini aktif cihazlar arasında taşımak için kullanılan cihaz portları trunk olarak tanımlanmaktadır. Trunk olmayacak portların trunk olarak tanımlanması o porta bağlı cihazın bütün ağ trafiğini almasını sağlayacağından bu tür yanlış tanımlamalar mutlaka düzeltilmelidir.

Cihazların kullanılmayan portlarını OSI 3.katman bağlantısı verilmemiş bir sanal ağa atamalı veya portlar disable edilmelidir. Böylece saldırganın cihazın boş portuna girip ağa ulaşması engellenmiş olmaktadır.

Anahtarın port numarasına, cihazın fiziksel adresine veya kullanılan protokole göre dinamik sanal ağ ataması uygulanarak cihazların sanal ağ ve mantıksal adres bilgileri tek noktadan kontrol edilebilmekte ve daha güvenilir ağ yapısı oluşturulmaktadır. Böylelikle sadece kayıtlı fiziksel adreslerine sahip cihazlar izin verilen ağlara ulaşabilmektedir[7][9].

5.3.6 Kayıtlama Ayarları

Ağ cihazları çeşitli hadiseler hakkında kayıtlama özelliğine sahiptir. Bu kayıtlar, güvenlik hadiselerinin belirlenmesinden ve önlem alınmasında kritik önem taşıyabilmektedir. Ara yüzlerin durum değişikliği, sistem konfigürasyon değişikliği, erişim listelerine takılan bağlantılar gibi güvenlik açısından önemli olan bilgilerin kaydı tutulabilmektedir. Cihazda kayıtlama aşağıdaki şekillerde yapılabilmektedir:

SNMP Trap Logging: Sistem durumunda karakteristik değişikliklerde Ağ Yönetim İstasyonuna uyarı göndermektedir.

Sistem Kayıtlaması: Sistem konfigürasyonuna bağlı olarak hadiselerin kaydını tutmaktadır. Sistem kayıtlaması farklı yerlere yapılabilmektedir:

- Sistem konsoluna bağlı ekrana logging console komutuyla
- Üzerinde UNIX'in syslog protokolü çalışan ağdaki bir sunucuya logging ip-address ve logging trap komutlarıyla

Ör: logging 200.100.17.2

- Telnet veya benzeri protokolle açılan VTY remote oturumlara logging monitor ve terminal monitor komutlarıyla

- Yerel buffer olan RAM'ine logging buffered komutuyla yapılabilmektedir

Kayıtlar düzenli olarak takip edilmeli ve sistemin düzgün çalışıp çalışmadığı kontrol edilmelidir. Farklı cihazlardan Ağ Yönetim İstasyonu'na gönderilen mesajların zamana göre senkronize olması için cihazlarda NTP çalıştırılmalıdır.

6. Güvenlik Duvarında VPN ve NAT Uygulama Örnekleri

Cisco ASA 5500 Serisi uyarlanabilir güvenlik uygulamaları, yenilikçi Cisco Uyarlanabilir Tanımlama ve Hafifletme (AIM) mimarisi ile sınıfının en iyisi güvenlik ve VPN servislerini birleştiren amaca-özel-tasarlanmış çözümlerdir. Cisco Kendini-Savunan Ağ mimarisinin bir anahtar bileşeni olarak tasarlanan Cisco ASA 5500 Serisi ağa yayılmadan önce atakları durduran, ağ aktivitelerini ve uygulama trafiğini kontrol eden ve esnek VPN bağlantısı sağlayan proaktif tehdit savunması sağlar. Sonuç; tüm konumlandırma ve çalışma maliyetlerini ve bu yeni seviyedeki güvenliği sağlayan karmaşıklığı azaltırken KOBİ ve kurumsal ağların korunması için güvenlik genişliği ve derinliği sağlayan çok güçlü ve çok fonksiyonlu ağ güvenlik uygulamasıdır.

ASA 5500 Serisi SSL VPN ve IPSec VPN servislerinin güvenlik duvarı teknolojisiyle koruyan ilk modeli olup, Trend Micro ‘nun saldırı korumadaki ve içerik kontrolündeki uzmanlığını Cisco’nun çözümleriyle birleştirerek antivirüs,anti-spyware,dosya engelleme,anti-spam,antiphishing,URL engelleme ve filtreleme ile içerik filtrelemesi konusunda koruma sağlar.İnternet ortamında daha önceki bölümlerde belirttiğimiz büyük dert açan kurtçuk tipi virüsler ,uygulama katmanı saldırıları ,işletim sistemi seviyesinde saldırılar ,uçtan uca dosya paylaşımı ,anlık mesajlaşma ,spyware ,rootkits gibi geniş çaplı tehditlere karşı tam kapsamlı ,proaktif saldırı tespit sistemi sunar.Cisco Güvenlik Aygıtı Yönetici (ASDM) ile tek aygıt yönetimi ve izlemesi ,Cisco Security Manager(Güvenlik Yöneticisi) ile kurumların ihtiyaçlarını karşılıyacak çoklu cihaz yönetim servisleri sunar.Saldırı korumalı VPN özellikleri sayesinde çalışanların ve işortaklarının güvenli bir şekilde şirketinizin bilgisayar ağlarına uzaktan erişilmesini sağlar.

Uygulamada kullanıcağımız modelin temel özellikleri iki adet Power over Ethernet (Ethernet üzerinden Elektrik-PoE) çıkışıyla birlikte 8 adet 10 /100 çıkış,ikinci katman saydam güvenlik duvarı,uygulama seviyesi güvenlik sağlayan 10 IPSec VPN ,2 SSL VPN ucu ile bir genişleme yuvası bulunan modelidir.

- Cihaza ilk bağlanıldıktan sonra ilk karşılaşılan ve cihaz hakkında detaylı bilgiye ulaşıcağımız pencere ile cihazın üzerindeki yazılım ve bu yazılımlarını versiyonları

hakkında bilgi alınabilen Cihaz Bilgisi ,cihaz üzerinde yer alan Ethernet ara yüzleri hakkında detaylı bilgi sahibi olunucak Arayüz Durumları,VPN bağlantılar hakkında bilgi alınan VPN tünelleri bölümü ,ASA üzüerindeki CPU ve RAM değerleri hakkında bilgi alacağımız Sistem Kaynakları Durumu ,ASA üzerinden geçen trafik hakkında bilgi alacağımız Trafik Durumu ve en altta cihazın sistem loglarını görülür.

- Kaynaklara güvenli erişimi sağlayıcı güvenlik unsurlarının sistem yöneticinin geniş bir alan üzerinde kimlik doğrulaması (Authentication),erişim hakkı verilmesi (Authorization) ,ActiveX filtreleme ve servis plan kuralları tanımlamaları

VPN kısaca, herkese açık bir ağ olan internet üzerinden verilerinizi güvenli bir şekilde geçirme olarak tanımlanabilir. Şirketlerin VPN'i tercih etmesi için pek çok sebep sıralanabilir. Fakat en önemlisi şirketlerin interneti kullanarak iletişim maliyetlerini düşürmek istemesidir.VPN sayesinde şirketlerin ofislerini birbirine ya da mobil kullanıcılarını merkeze bağlamak için kendi ağ omurgalarını kurmasına gerek kalmaz. VPN ile her lokasyon, diğer lokasyonlarla arasındaki bağlantıyı internet üzerinden kesintisiz ve yüksek hızla gerçekleştirir. VPN, şirketlerin internet omurgasını kendi omurgaları gibi kullanmalarına imkan vermektedir.

Güvenlik, verilerin bir noktadan diğerine aktarılırken şifrelenmesi ile gerçekleştirilir. Kiralık hat, Frame Relay, ISDN, gibi bağlantı şekilleri kullanılarak şirket ofisleri birbirine bağlandığında aradaki hat özel bir hat olduğu için verilerin çalınması veya değiştirilmesi mümkün olmamaktadır. Fakat internet üzerinden verilerin taşınması söz konusu olduğunda verilerin güvenlik amacıyla şifrelenmesi gerekmektedir. VPN teknolojileri bunu sağlar[14].

VPN'i kullanım şekillerine göre ikiye ayırabiliriz:

- Site-to-Site VPN
- Remote Access VPN

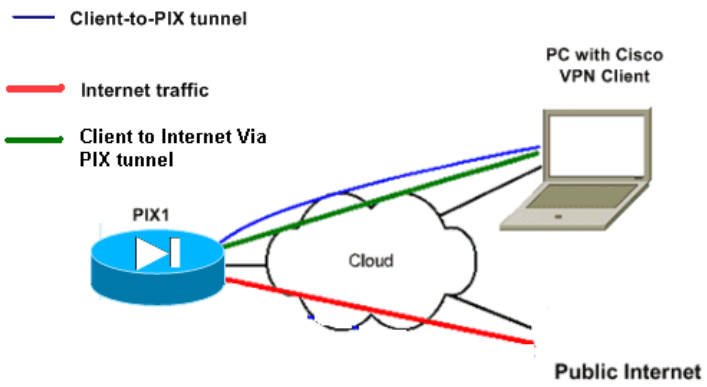
Site-to-Site VPN tüm lokasyonları ve merkezi güvenli bir biçimde birbirine bağlar. Remote Access VPN ise şirket dışında çalışmak durumunda olan mobil kullanıcıları, dial-up bağlantı kullanan küçük ofisleri ve ev-ofisleri güvenli bir şekilde merkeze bağlamak için kullanılır.VPN uzak bölgelerde, farklı ülkelerde ya da kıtalarda ofisleri olan veya farklı bölgelerde çok sayıda mobil kullanıcısı olan şirketler için ideal bir çözümdür.Cisco VPN çözümleri ve içerdiği ürün ailesi şirket lokasyonları ve mobil kullanıcılar için güvenli bağlantı sağlar. Cisco VPN çözümleri Cisco SAFE mimarisini

temel alır. SAFE tanımlamaları ve Cisco VPN ürün ailesi müşterilerine uçtan-uca bir güvenlik stratejisi sunar.Cisco VPN çözümleri tünelleme teknolojileri, kompleks şifreleme prosedürleri ve kimlik doğrulama protokollerini içerir. Değerli bilgileri açık ağ olan internet üzerinden geçerken yetkisiz erişimlerden korur.

Tünelleme interneti kullanarak bir lokasyondan diğerine veri paketlerinin koruyucu bir şifreleme algoritmasıyla iletilmesi yöntemidir. Protokol başlığı ve VPN bağlantısı için kullanılacak protokolün başlık bilgisine eklenir. Veri iletişimi başladığında, veri paketleri bu yeni ve güvenli protokol başlığı bilgisini kullanır. IPSec Cisco ürünlerinin desteklediği en çok kullanılan güvenlik protokolüdür. IPSec internet üzerinden veri taşınması işleminde tünelleme, şifreleme ve kimlik doğrulama için kullanılan standart bir güvenlik protokolüdür.

Cisco Site-to-Site VPN Çözümleri

- Şirket verilerinin bir lokasyondan diğerine güvenli şekilde taşınmasını sağlar.
- Mevcut Frame Relay veya ATM ağından yararlanırken şifreleme yeteneklerini ekleyerek maliyetleri azaltır.
- Band genişliği yetersiz, sürekli kopan dial-up bağlantılara sahip eski ağınızı değiştirebilmeniz için, ucuz ve verimli bir yöntem sunar.
- Çok noktadan Internete ve web-temelli uygulamalara erişim sağlar.
- Geniş Alan Ağınızı başka ülkelere, uzak ofislere bağlantılarla ucuz ve güvenli bir şekilde genişletmenizi sağlar.
- Şirket ağınızı iş ortakları ve tedarikçilerinize bağlantılarla genişletmenizi sağlar.



Şekil 6.1 Site-to-Site VPN

6.1 ASDM Kullanarak Uzak VPN Server Konfigürasyonu

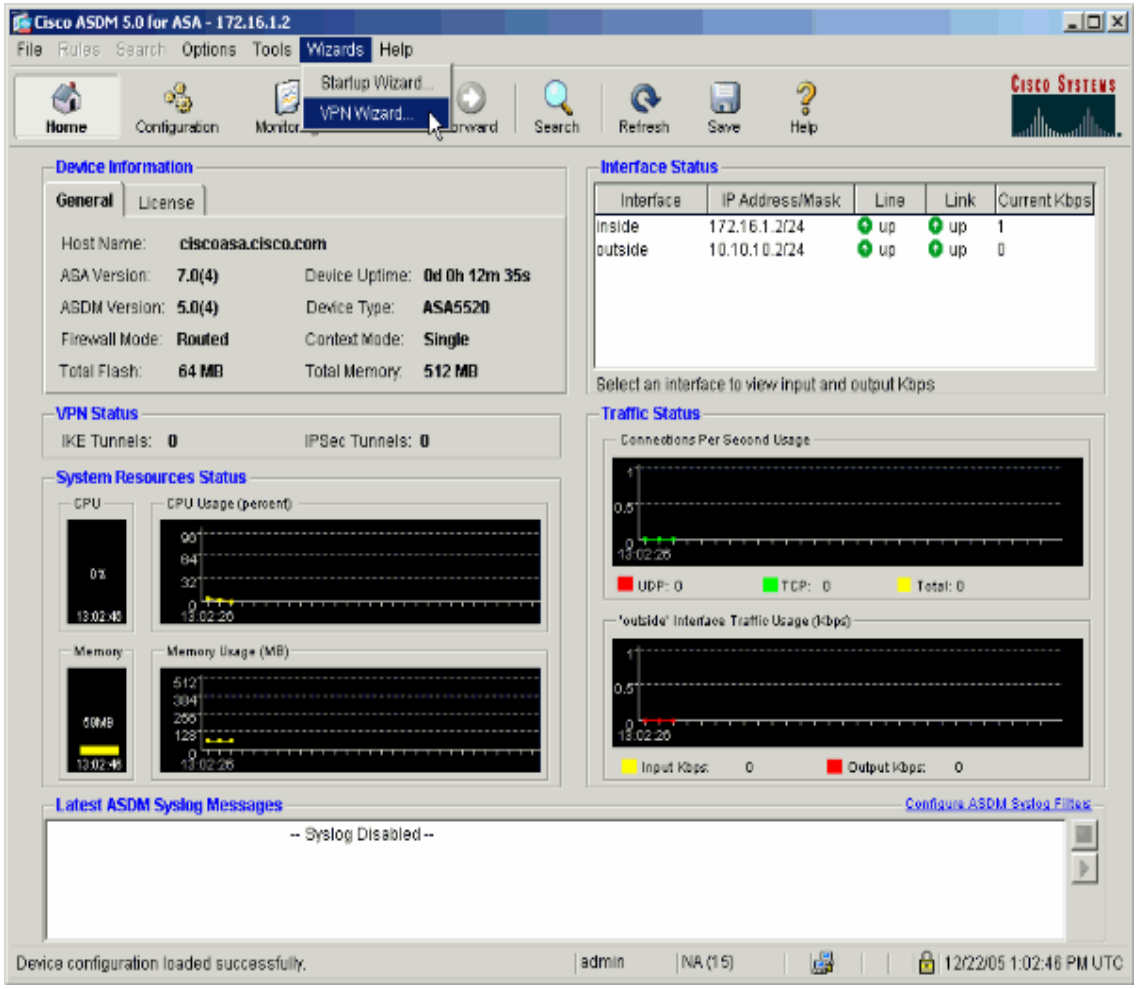
Bu örnekte güvenlik duvarı üzerinde ASDM veya CLI kullanarak remote VPN nasıl konfigüre edileceği gösterilecektir.Uzak erişim konfigürasyonu Cisco VPN Client lar için örneğin mobil kullanıcılar için güvenli uzak erişim sağlar.Uzak erişim VPN,uzak kullanıcılara merkezi ağ kaynaklarına güvenli bir şekilde erişime olanak sağlar[17].

Security uygulamalarının konfigürasyonunda ve VPN'lerin güvenli yönetiminde gruplar ve kullanıcılar ana kavramlardır.Bunlar VPN kullanımı ve kullanıcı erişimi için tanımlanan özellikleri belirtirler.Bir grup tek bir varlık gibi davranan kullanıcıların grubudur.Kullanıcılar group policylerden özelliklerini alır.Tunnel Groupları specifik bağlatılar çin group policy tanımlar.Eğer bir kullanıcıya şahsi grup policy atanmazsa bağlantılar için group policy uygulanır.

The Internet Security Association and Key Management Protocol (ISAKMP), IPSec Security Association nasıl yapılandırıldığına razı olan host'ların hemfikir olduğu birde IKE olarak adlandırılan bir müzakere protokolüdür.Her ISAKMP müzakeresi iki bölüme ayrılır. Phase1 ve Phase 2.Phase 1 ISAKMP müzakere mesajları için korunan ilk tüneli yaratır.Phase 2 güvenli bağlantı boyunca seyahet eden veriyi koruyan tuneller yaratır.

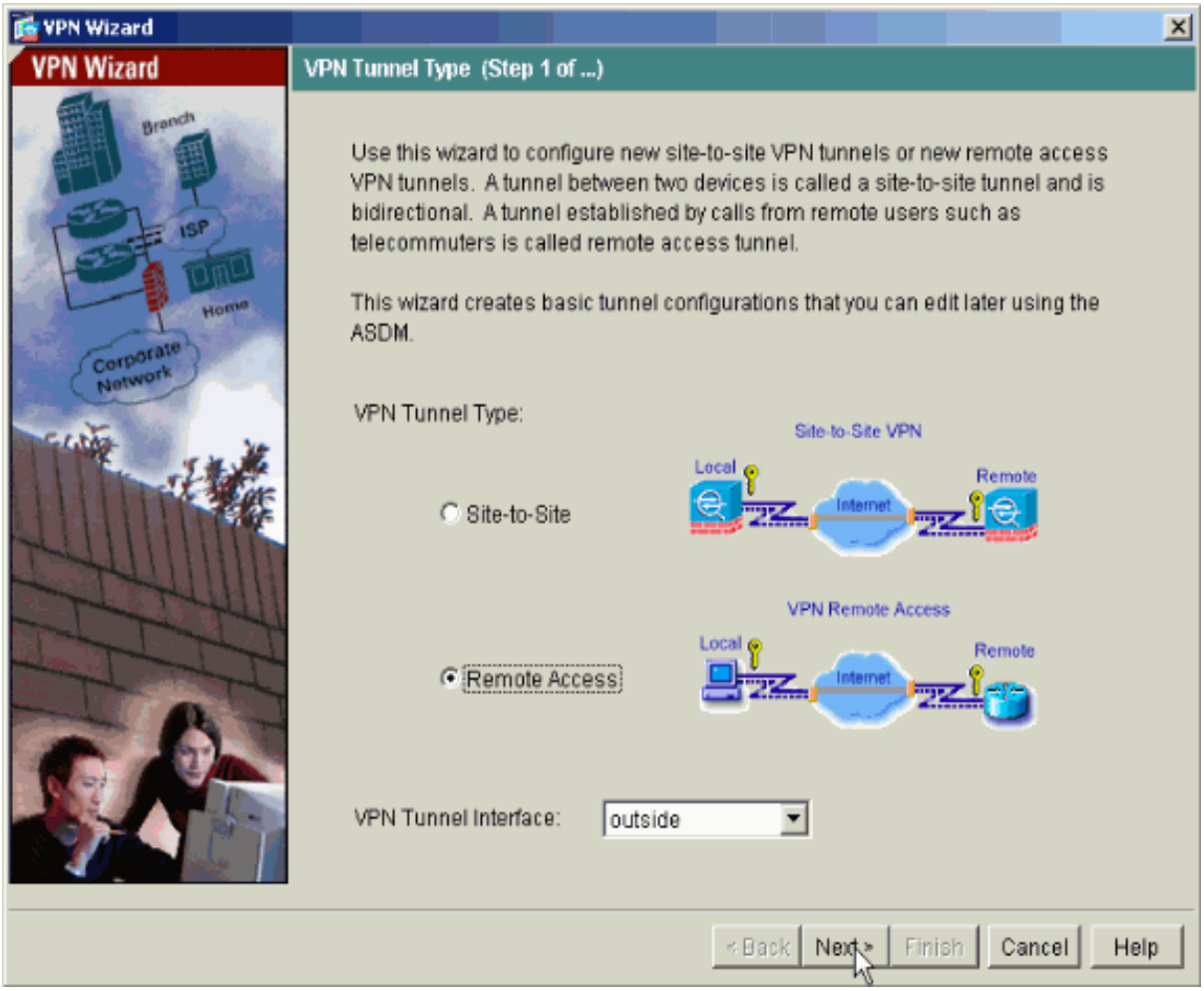
ASDM Kullanarak Remote VPN Konfigürasyonu ;

- Ana pencereden **Wizards > VPN Wizard** seçilir.



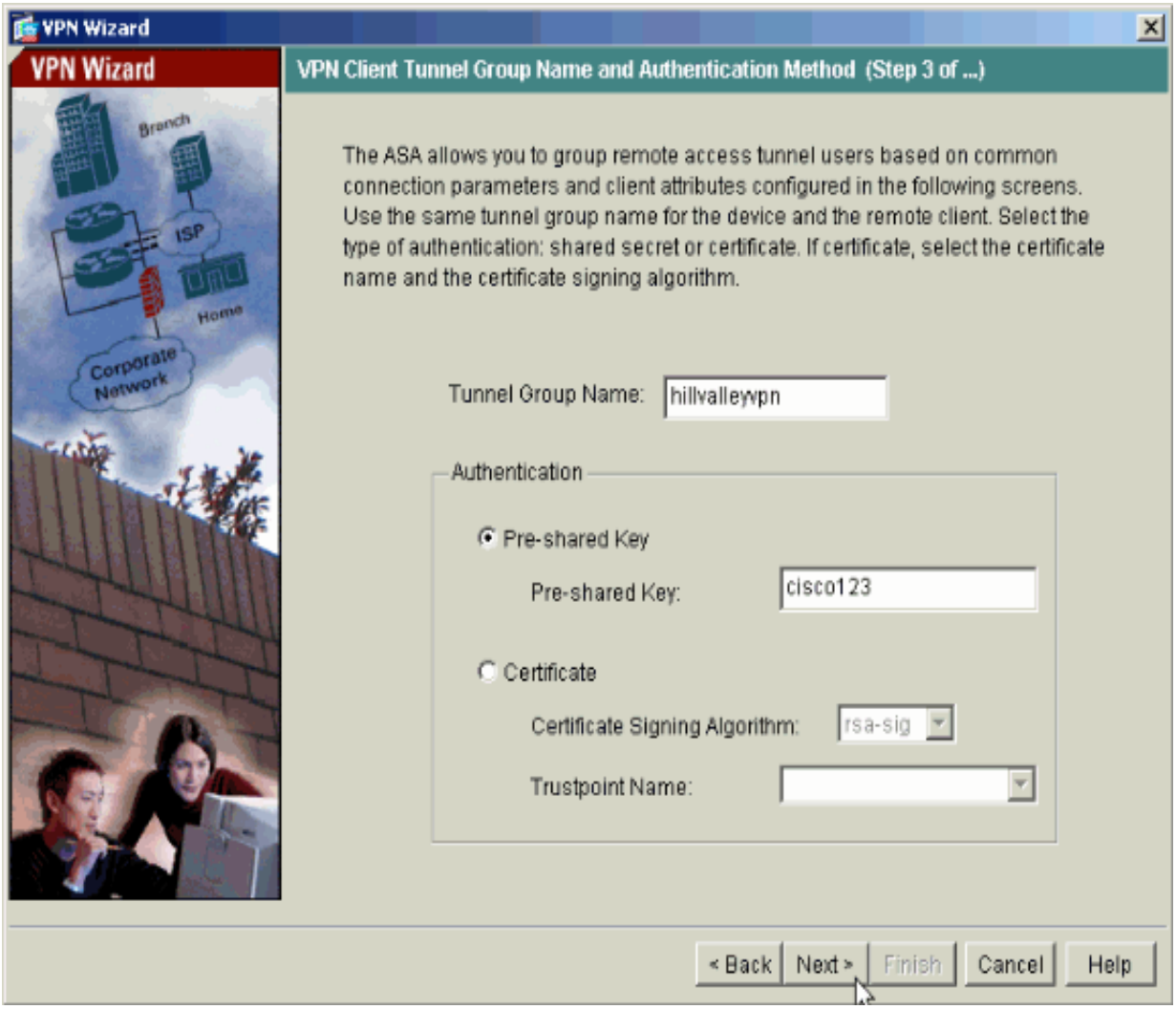
Şekil 6.2 ASDM Ana Sayfadan VPN Wizard Seçimi

- **Remote Access** VPN çeşidi seçilir



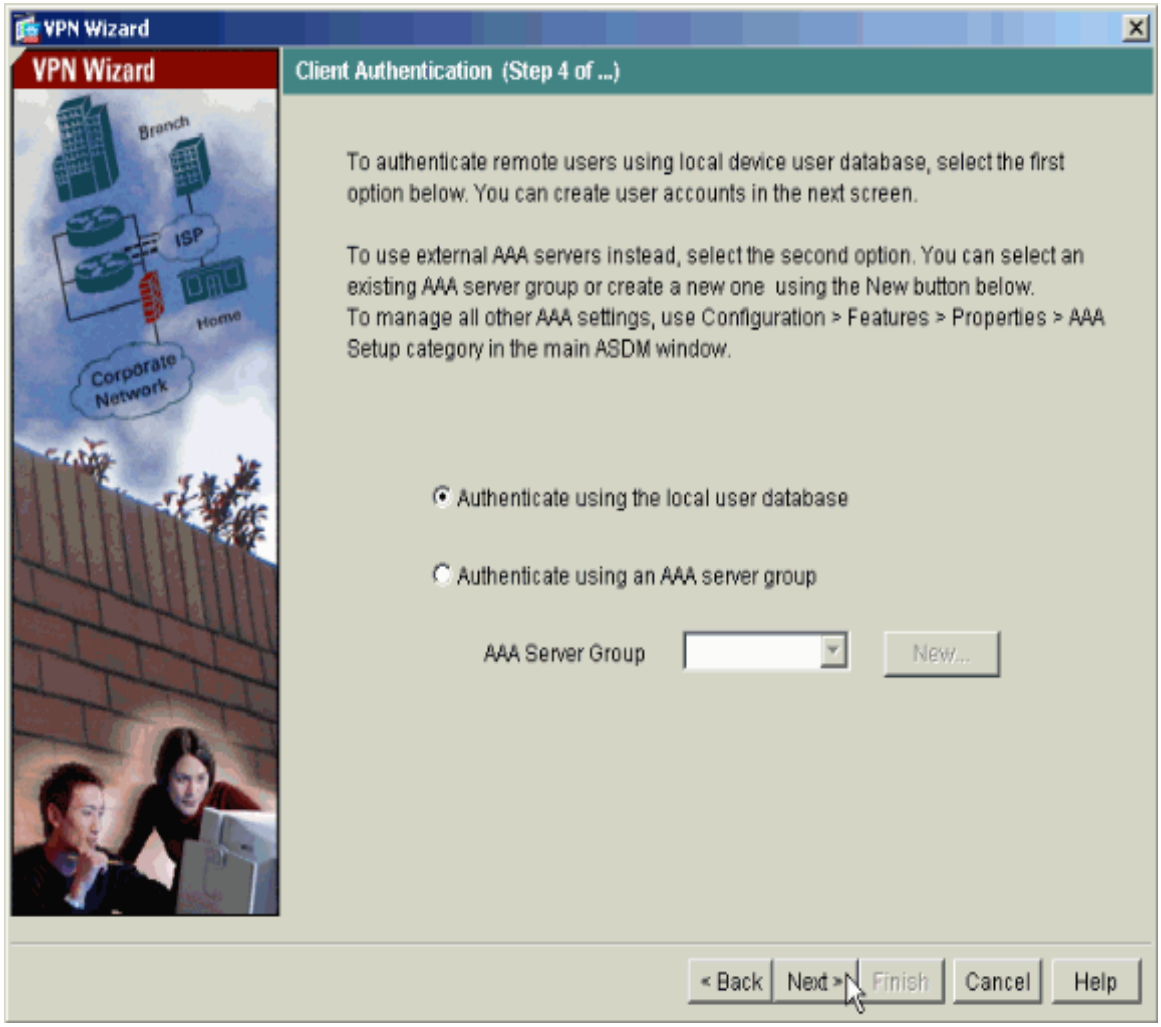
Şekil 6.3 Remote Access VPN

- Tünel grup ismi için bir ad girilir ve doğrulama bilgisi tanımlanır.Aşağıdaki örnekte **Pre-shared Key** seçilmiştir.



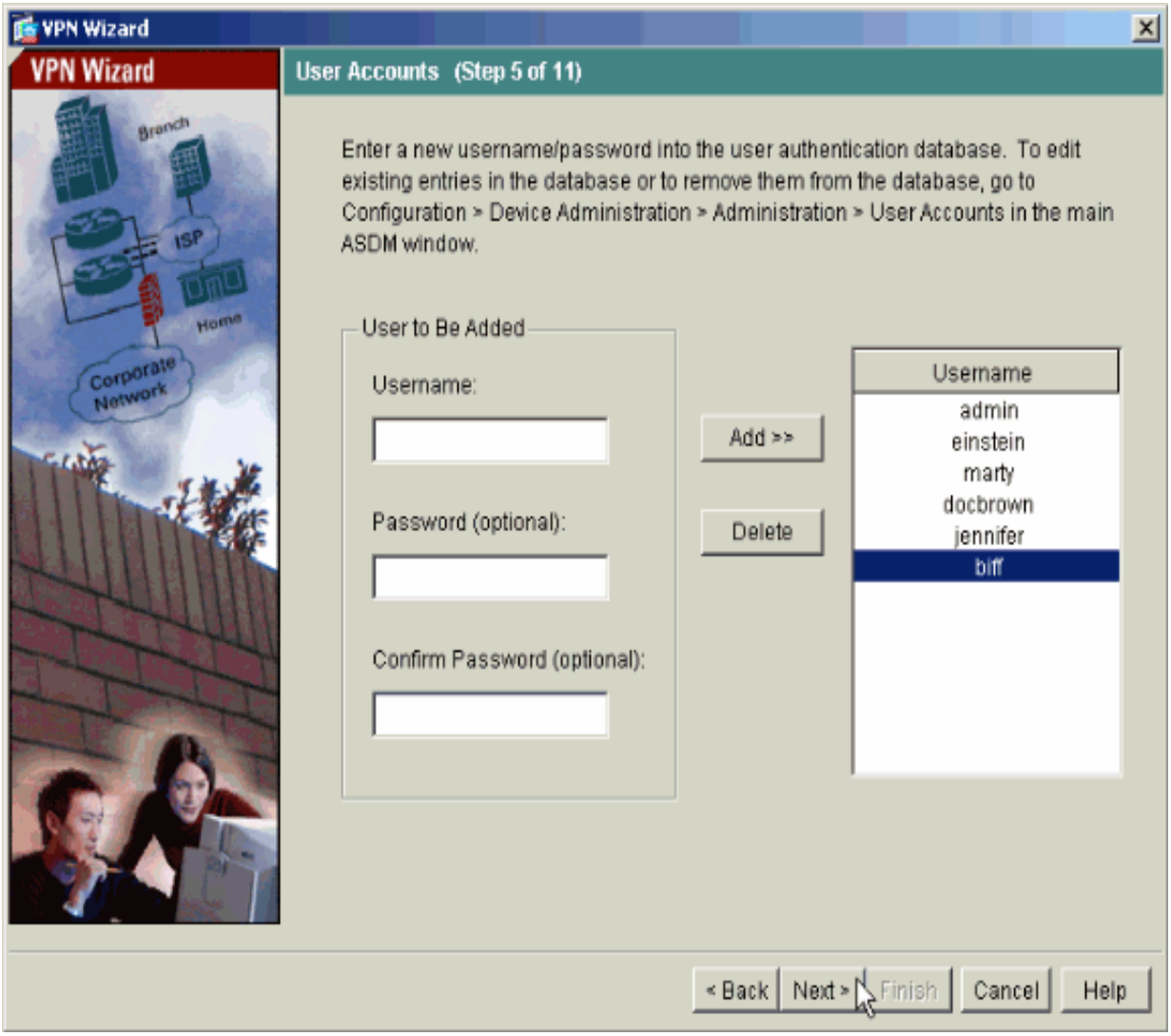
Şekil 6.4 VPN Client Grup İsmi Ve Doğrulama Methodu

- Eğer uzak kullanıcıların yerel kullanıcı veritababına veya harici AAA server grubuna doğrulanması için aşağıdaki örnekteki gibi seçim yapılır.Burada yerel kullanıcı veri tabanı kullanılara doğrulama seçilmiştir..



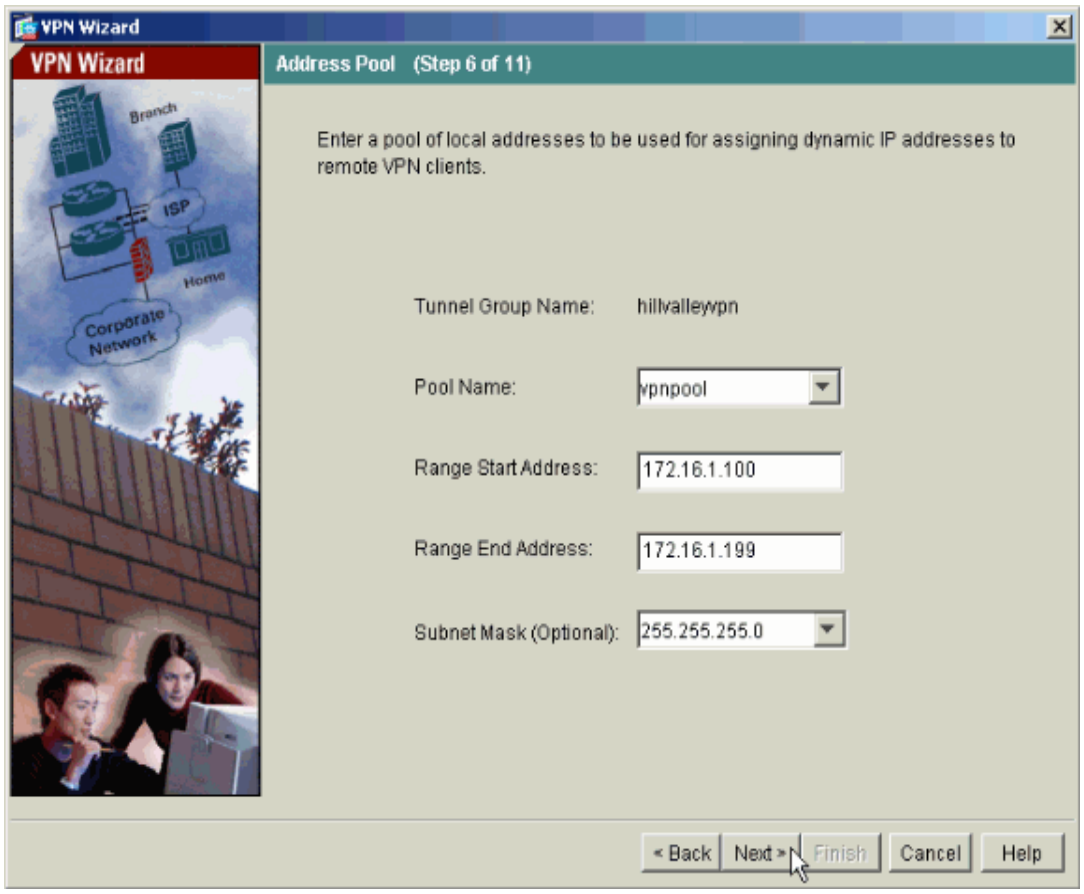
Şekil 6.5 Client Doğrulama

- Gerekirse yerel veritabanına kullanıcılar ilave edilir.



Şekil 6.6 Kullanıcı Hesapları

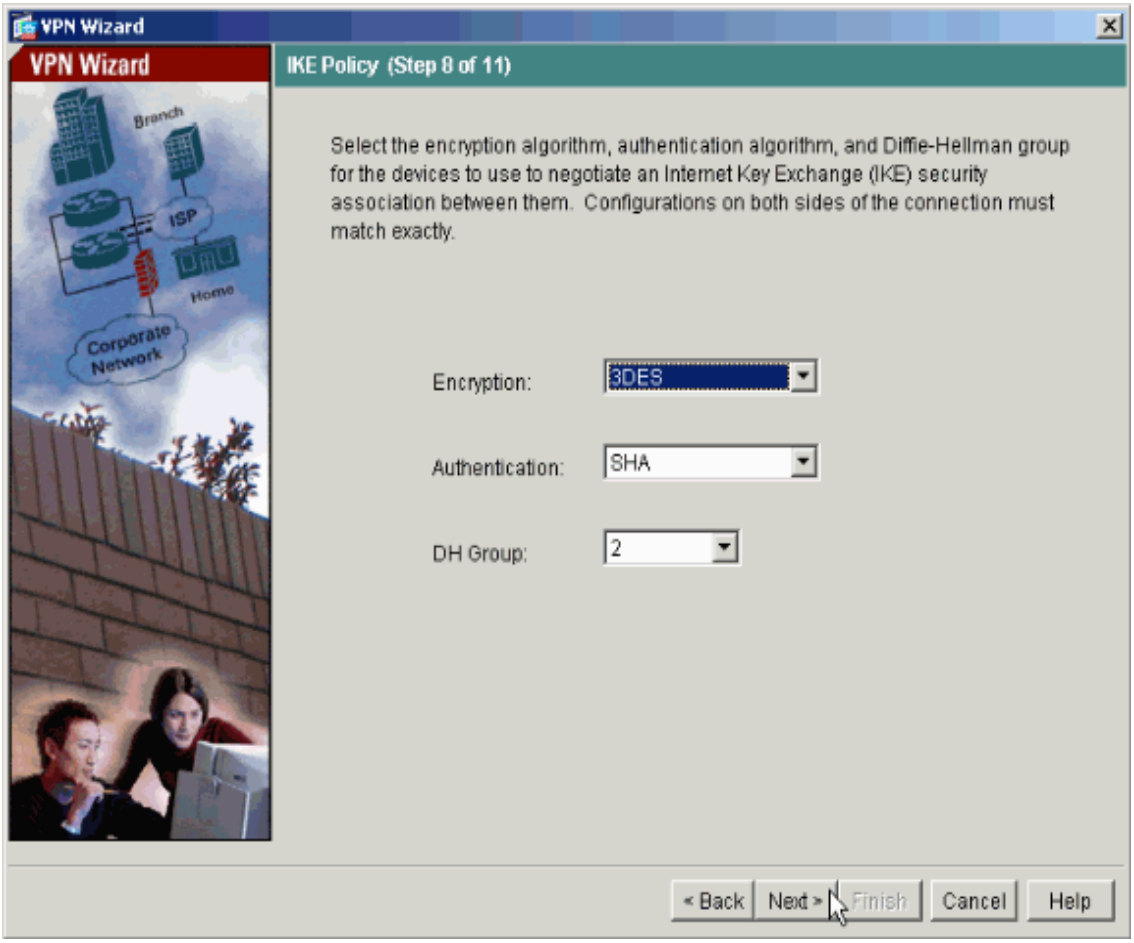
- Uzak VPN Client ‘lar bağlandığı zaman dinamik olarak adres ataması için yerel adres havuzu tanımlanır.



Şekil 6.7 Adres Havuzu

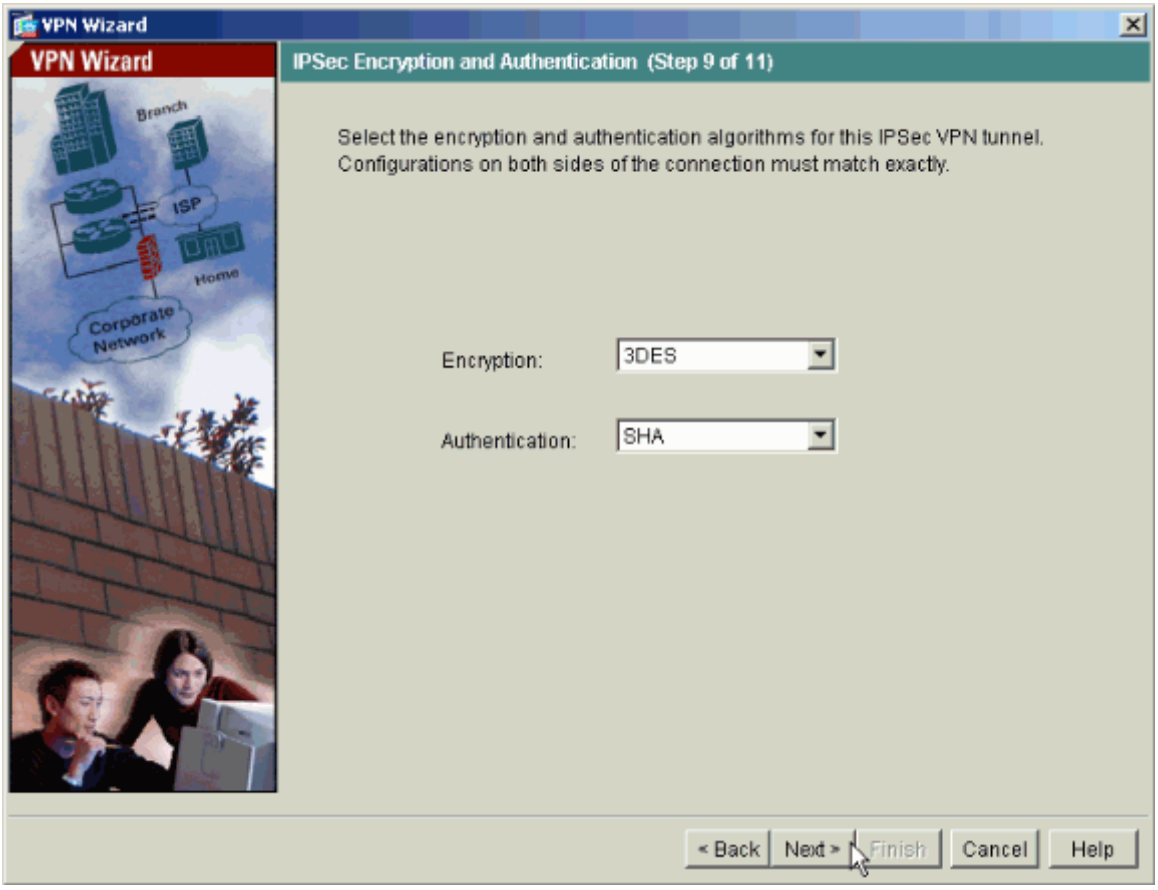
- Internet Key Exchange için parametreler tanımlanır.

Tünelin her iki yakasındaki konfigürasyonlar tam olarak eşleşir.Fakat Cisco VPN Client otomatik olarak kendi için düzgün konfigürasyonu seçer.Bu nedenle PC kullanıcıları züerinde IKE konfigürasyonu gerekli değildir.



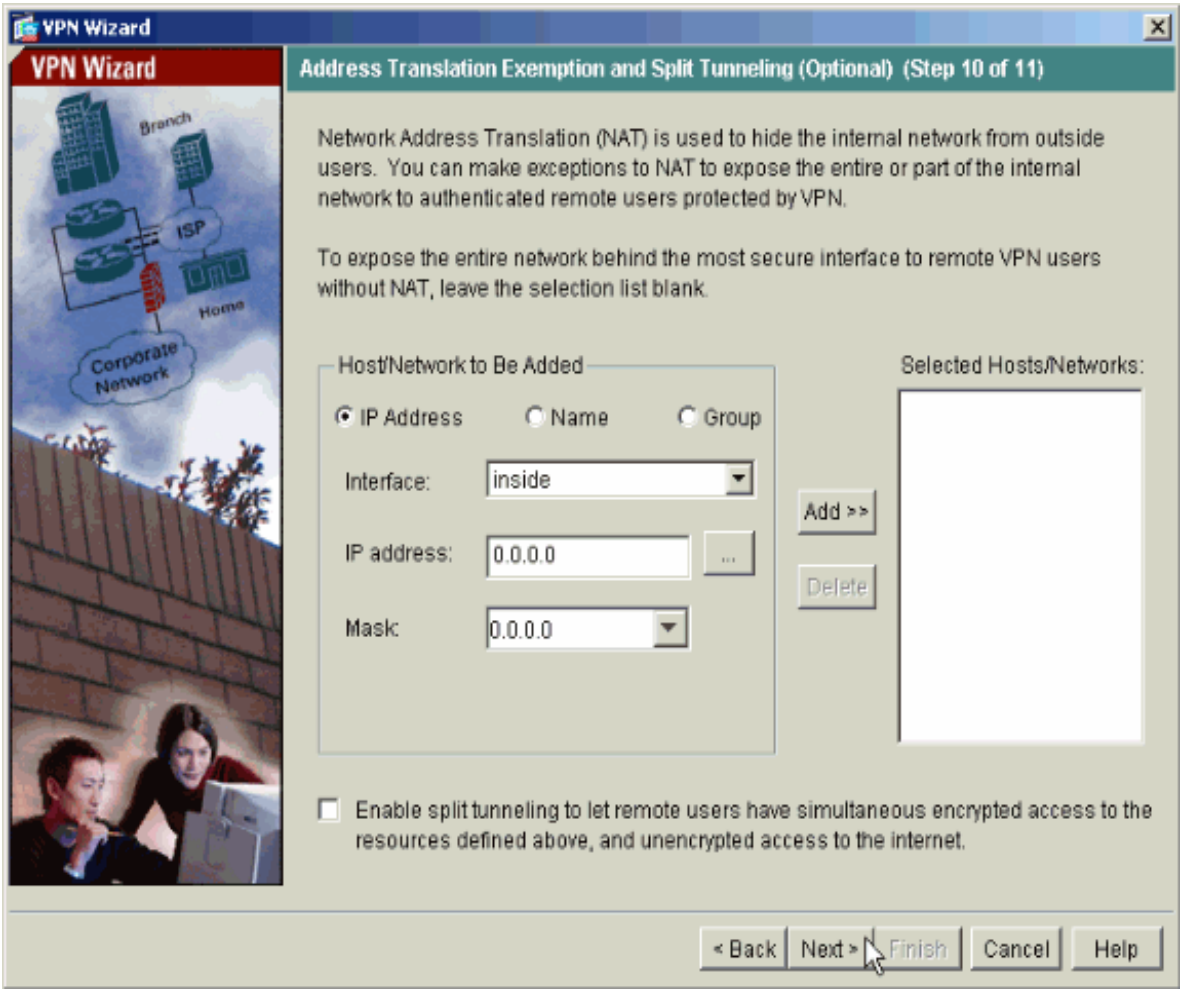
Şekil 6.8 IKE Policy

- IPSec için parametreler tanımlanır. Tünelin her iki yakasındaki konfigürasyonlar tam olarak eşleşir.Fakat Cisco VPN Client otomatik olarak kendi için düzgün konfigürasyonu seçer.Bu nedenle PC kullanıcıları üzerinde IKE konfigürasyonu gerekli değildir.



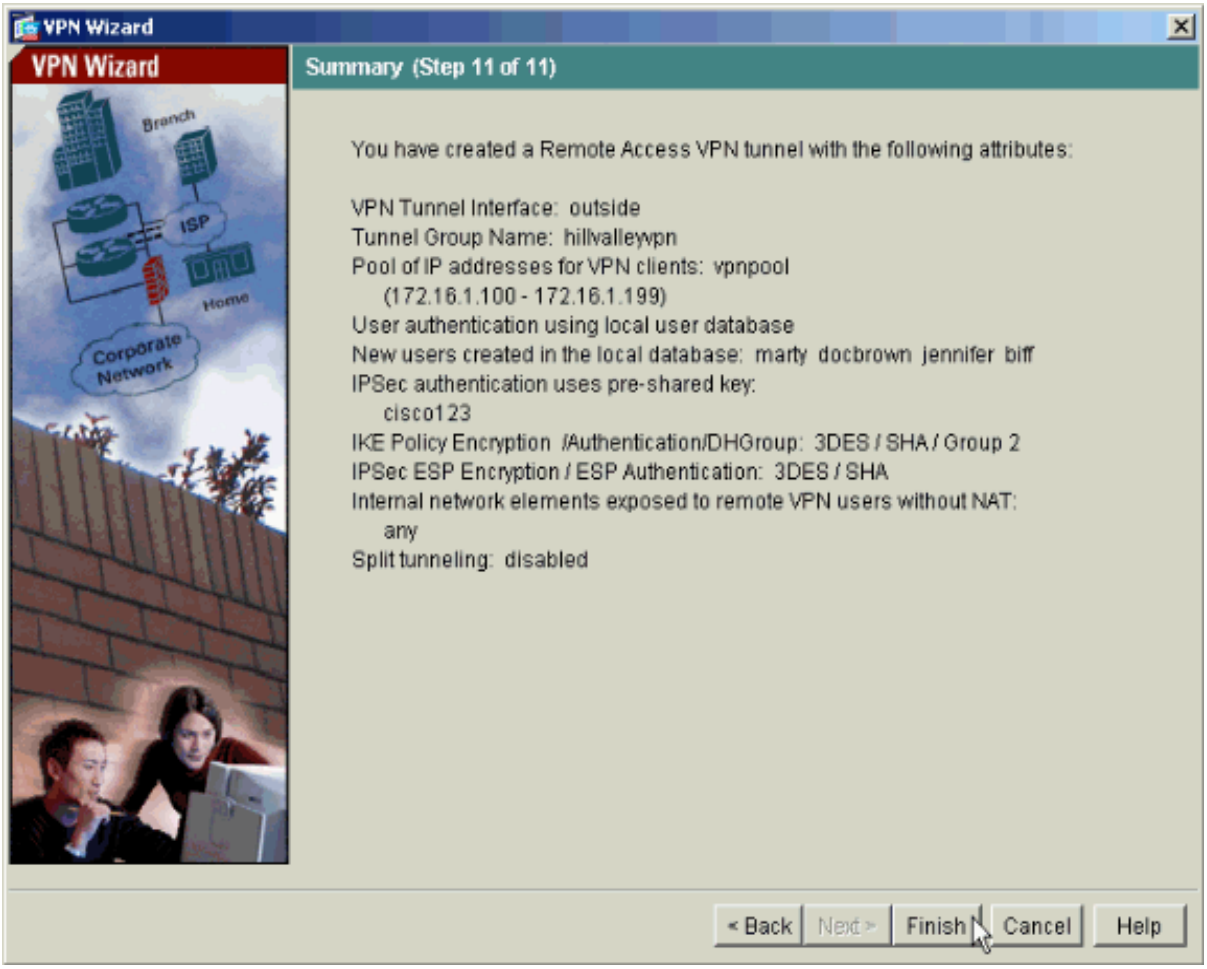
Şekil 6.9 IPSEC Şifreleme ve Doğrulama

- NAT dış kullanıcılardan iç ağı saklamak için kullanılır.Eğer bu liste boş bırakılırsa ,uzak VPN kullanıcılarına güvenlik duvarının iç ağına erişimine olabak sağlanır.Aşağıdaki pencere üzerinde bir de split tunneling ‘e imkan sağlanır.Split tunneling trafiği şifreler.eğer Split tunneling kullanılmazsa uzak VPN kullanıcılarındn tüm trafik güvenlik duvarına tünellenir.Bu da çok fazla bant genişliği ve işlemci yoğunluğuna sebep olur.



Şekil 6.10 NAT

- Bu pencere yapılmış işlemlerin özetini gösterir. Finish'e tıklanarak konfigürasyon tamamlanır..



Şekil 6.11 Remote Access VPN İşlemini Tamamlama

CLI Kullanarak Remote VPN Konfigürasyonu;

ASA-AIP-CLI(config)#**ip local pool vpnpool**
172.16.1.100-172.16.1.199 mask 255.255.255.0

ASA-AIP-CLI(config)#**username marty password 12345678**

ASA-AIP-CLI(config)#**tunnel-group hillvalleyvpn general-attributes**

ASA-AIP-CLI(config-tunnel-general)#**address-pool vpnpool**

ASA-AIP-CLI(config)#**tunnel-group hillvalleyvpn ipsec-ra**

ASA-AIP-CLI(config)#**tunnel-group hillvalleyvpn ipsec-attributes**

ASA-AIP-CLI(config-tunnel-ipsec)#**pre-shared-key cisco123**

ASA-AIP-CLI(config)#**isakmp policy 1 authentication pre-share**

ASA-AIP-CLI(config)#**isakmp policy 1 encryption 3des**

ASA-AIP-CLI(config)#**isakmp policy 1 hash sha**

ASA-AIP-CLI(config)#**isakmp policy 1 group 2**

ASA-AIP-CLI(config)#**isakmp policy 1 lifetime 43200**

ASA-AIP-CLI(config)#**isakmp enable outside**

ASA-AIP-CLI(config)#**crypto ipsec transform-set ESP-3DES-SHA esp-3des esp-sha-hmac**

ASA-AIP-CLI(config)#**crypto dynamic-map outside_dyn_map 10 set transform-set ESP-3DES-SHA**

ASA-AIP-CLI(config)#**crypto dynamic-map Outside_dyn_map 10 set reverse-route**

ASA-AIP-CLI(config)#**crypto dynamic-map outside_dyn_map 10 set security-association lifetime seconds 288000**

ASA-AIP-CLI(config)#**crypto map Outside_map 10 ipsec-isakmp dynamic Outside_dyn_map**

ASA-AIP-CLI(config)#**crypto map outside_map interface outside**

ASA-AIP-CLI(config)#**crypto isakmp nat-traversal**

ASA-AIP-CLI(config)#**group-policy hillvalleyvpn interna**

ASA-AIP-CLI(config)#**group-policy hillvalleyvpn attributes**

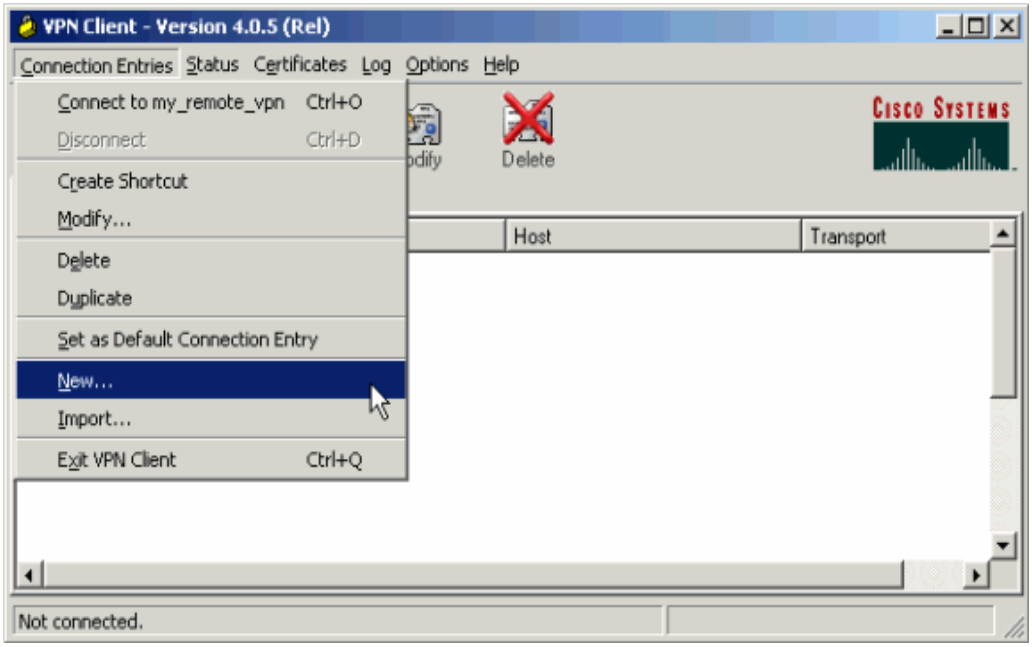
ASA-AIP-CLI(config)#(config-group-policy)#**dns-server value 172.16.1.11**

ASA-AIP-CLI(config)#(config-group-policy)#**vpn-tunnel-protocol IPSec**

ASA-AIP-CLI(config)#(config-group-policy)#**default-domain value test.com**

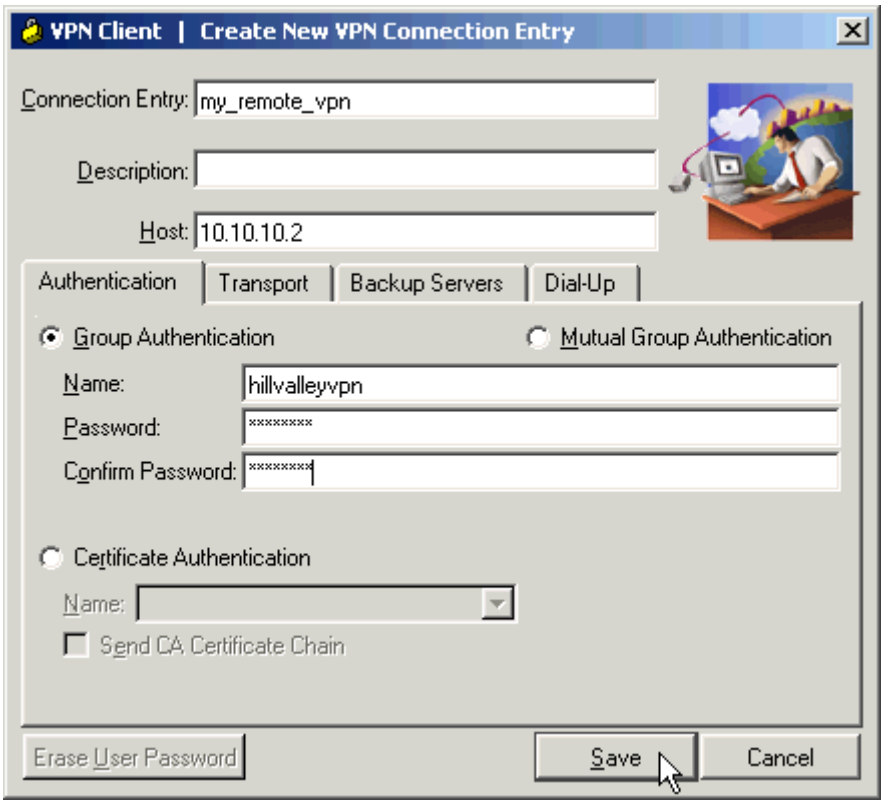
6.2 Güvenlik Duvarına Cisco VPN Client Kullanarak Bağlanılması

- **Connection Entries > New** seçilir.



Şekil 6.12 VPN Client

- Yeni bağlantının detayları doldurulur.



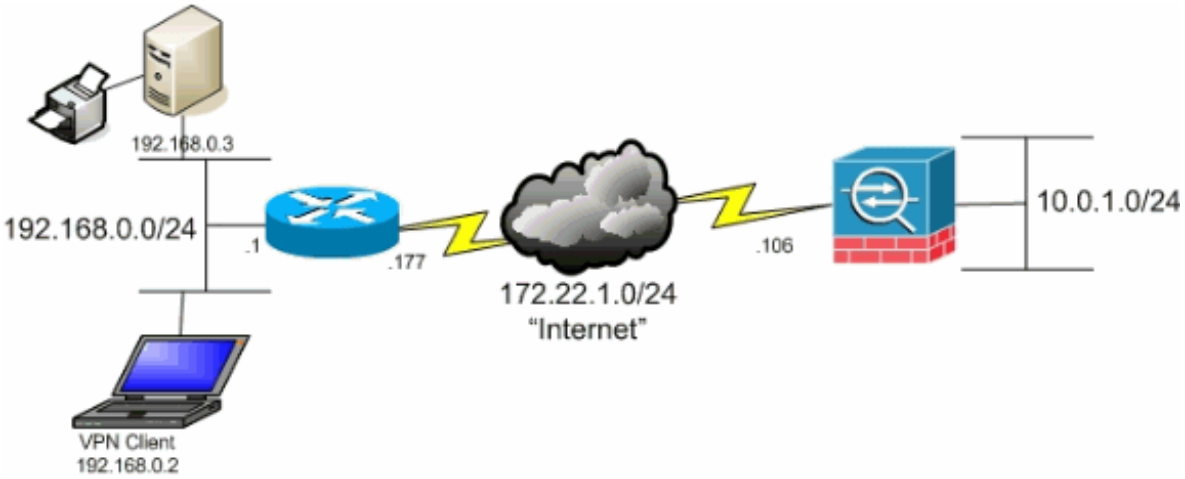
Şekil 6.13 Yeni VPN Bağlantısı Yaratılması

- Yeni yaratılan bağlantı seçilir ve Connect tıklanır.
- Doğrulama için kullanıcı adı ve şifresi girilir.

6.2.1 VPN Client 'ın Yerel Ağ Erişimine İzin Verilmesi

Güvenlik duvarı üzerinden tunelleme ile LAN erişim için Cisco VPN Client nasıl kullanılacağını adım adım incelenecektir.IPSec üzerinde konfigürasyon VPN Client 'lara merkezi kaynaklara güvenli erişim için olanak sağlar.

Aşağıdaki ağda VPN Client tipik bir SOHO ağı üzerine yerleşmiştir ve merkez ofisten Internet'e erişim sağlanır[17]

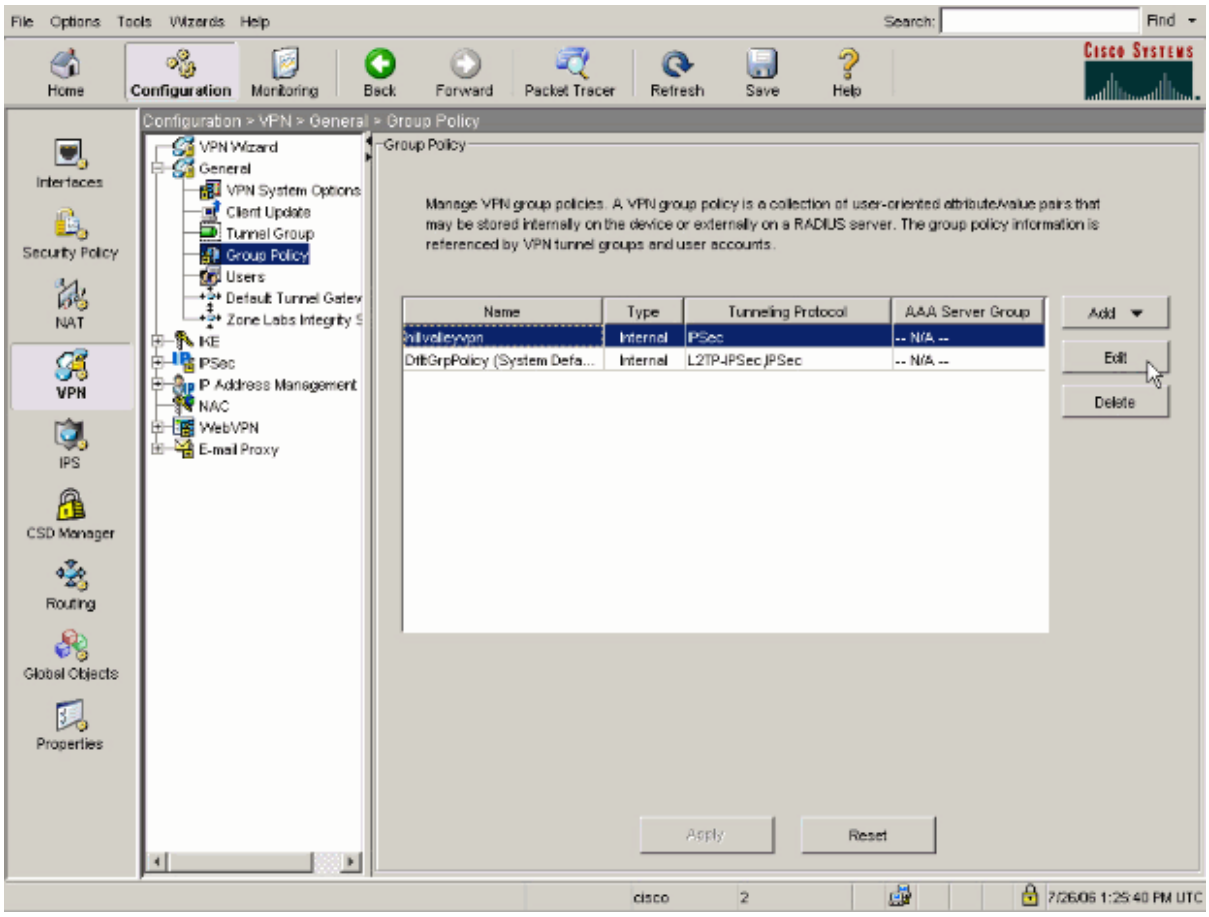


Şekil 6.14 VPN Client 'ın Yerel Ağ Erişimine İzin Verilmesi

Ağ üzerinde yerleşmiş cihazlara şifresiz haberleşen kullanıcılara izin veren VPN kullanıcılar için LAN erişim sağlandığı zaman farklı klasik bir spilt tunneling örneğinde tüm trafik şifresiz gderilir.Örneğin;VPN Client güvenlik duvarına bağlıyken printerdan çıktı almak için yerel ağa erişebilir ,fakat tunel üzerinden trafik gödnerilmezse Internet'e erişemez.Güvenlik duvarı üzerinde anı yolla konfigüre edilen split tunneling yerel LAN erişim için kullanılır.Fakat , şifrelenmiş ağ tanımları yerine ,bu durumda access list ler şifrelenmeyen ağlarlarla tanımlanır.Bir de farklı split tunneling uygulamalaında ,listedeki gerçek ağların bilinmeye ihtiyacı yoktur.Onun yerine ,güvenlik duvarı 0.0.0.0/255.255.255.255 varsayılan ağa atanır.

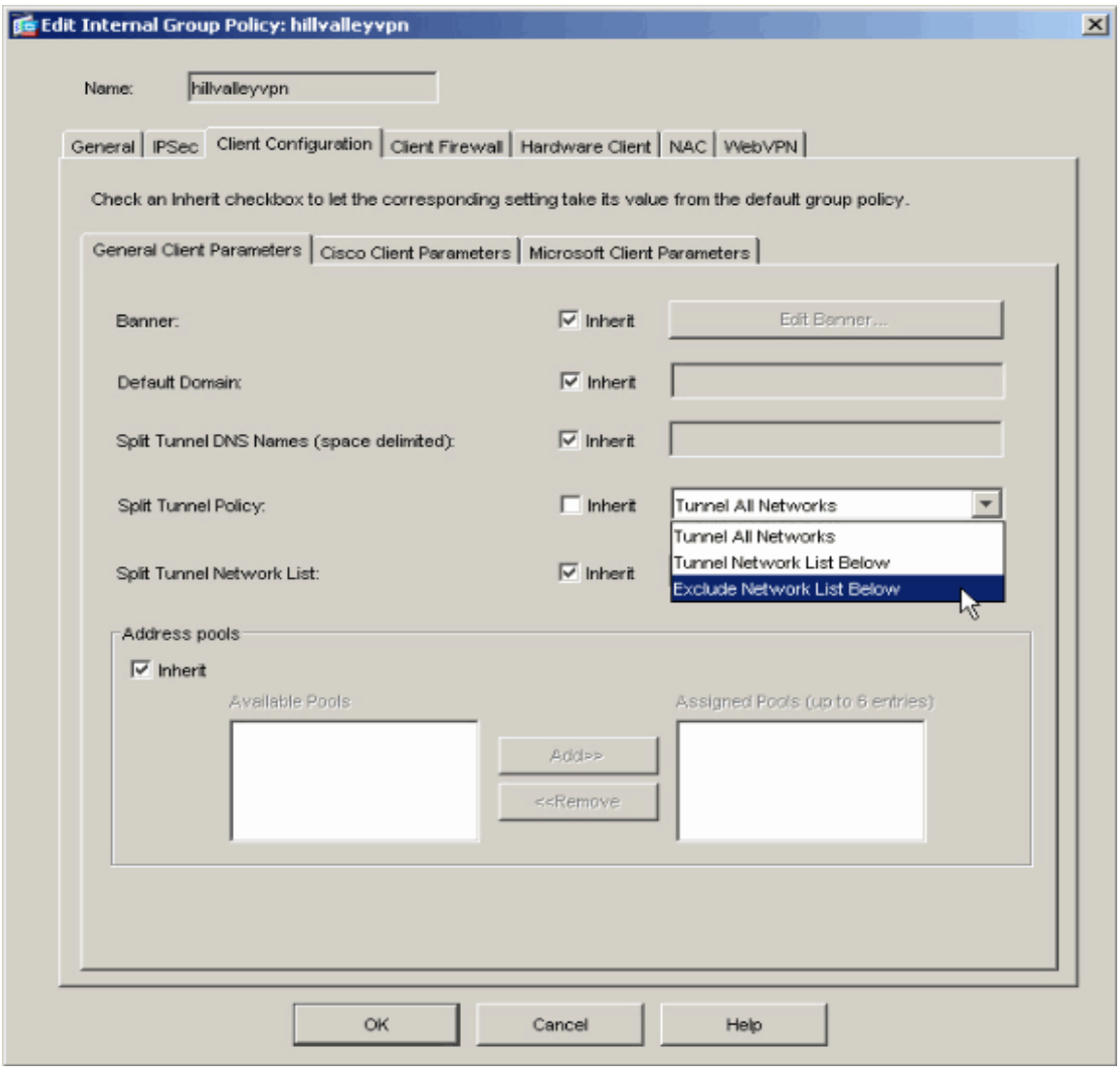
ASDM Kullanarak güvenlik duvarını konfigüre etmek;

- **Configuration > VPN > General > Group Policy seçilir ve LAN erişim sağlamak için** Group Policy seçilir ,ardından Edit tıklanır



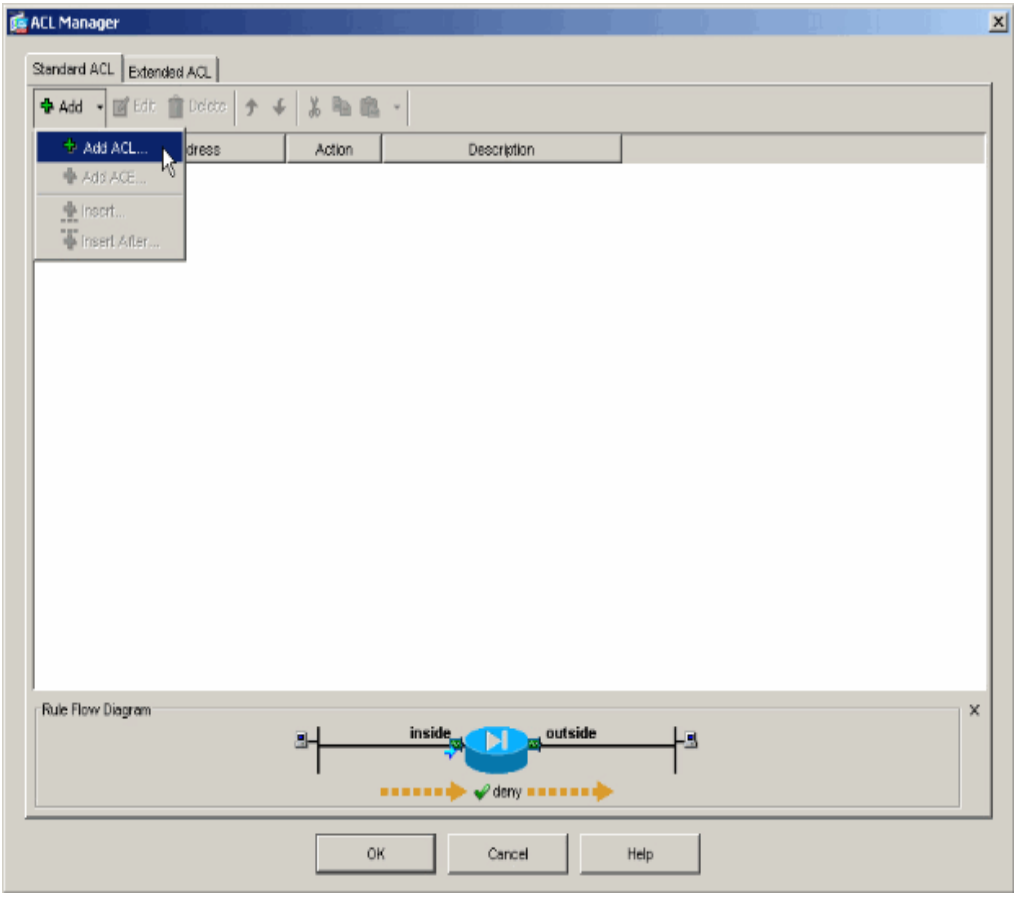
Şekil 6.15 Grup Policy

- **Client Configuration** seçilir.
- Split Tunnel Policy için Inherit kutusu kaldırılır ve **Exclude Network List Below** seçilir.



Şekil 6.16 İç Grup Policy Düzenlemesi

- Split Tunnel Network List için Inherit kutusu kaldırılır ve Manage tıklanır
- ACL Manager içindeki yeni bir access list seçmek için **Add > Add ACL** seçilir.



Şekil 6.17 ACL Manager

- ACL için bir isim sağlanır ve OK tıklanır.
- ACL yaratılınca , ACE (Access Control Entry) ilave etmek için **Add > Add ACE...** seçilir.
- Client'ın yerel ağ ile haberleşmesini sağlamak için ACE tanımlanır.
- Permit seçilir ve 0.0.0.0 Ip adresi ve 255.255.255.55 Netmask seçilir ve opsiyonel olarak tanımlamayaratılabilir ve OK tuşuna tıklanır.
- Split Tunnel Network List için yaratılmış ACL seçilir
- OK tıklanır ve Group Policy konfigürasyonuna geri dönülür.
- Apply tıklanır ve ardından güvenlik duvarına komutları göndermek için (gerekirse) send tıklanır.

CLI Kullanarak Güvenlik Duvarını Konfigüre Etmek;

- Konfigürasyon Moduna gir;

ciscoasa>enable

Password:

ciscoasa#configure terminal

ciscoasa(config)#

- Yerel ağ erişime izin vermek için acces list yaratmak için ;

ciscoasa(config)#access-list Local_LAN_Access remark VPN Client Local LAN Access

ciscoasa(config)#access-list Local_LAN_Access standard permit host 0.0.0.0

- Group Policy konfigürasyon moduna policy yaratmak için gir.

ciscoasa(config)#group-policy hillvalleyvpn attributes

ciscoasa(config-group-policy)#

- split tunnel policy tanımlamak için ;

ciscoasa(config-group-policy)#split-tunnel-policy excludespecified

- **Split Tunnel Access List** tanımlanır ,bu durumda Local_LAN_Access listedir**.**

ciscoasa(config-group-policy)#split-tunnel-network-list value Local_LAN_Access

- İki konfigürasyon moddan çıkılır

ciscoasa(config-group-policy)#exit

ciscoasa(config)#exit

ciscoasa#

- NVRAM'e konfigürasyon kaydedilir ve Enter tuşuna basılır.

ciscoasa#copy running-config startup-config

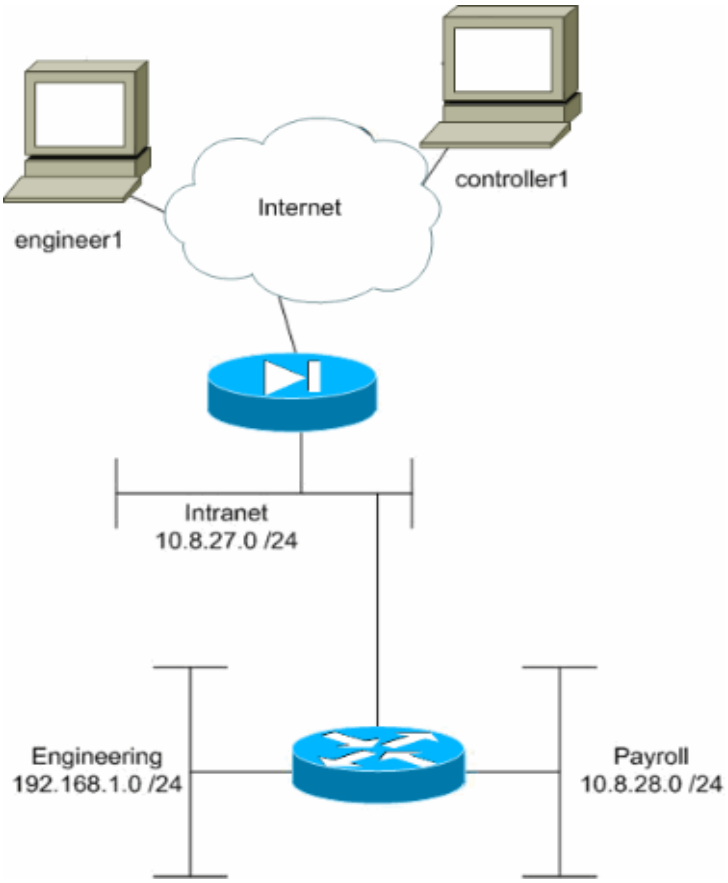
Source filename [running-config]?

Cryptochecksum: 93bb3217 0f60bfa4 c36bbb29 75cf714a

3847 bytes copied in 3.470 secs (1282 bytes/sec)

ciscoasa#

6.2.2 Güvenlik Duvarında Uzak Erişim VPN Kullanıcılarının Ağ Erişiminin Sınırlandırılması

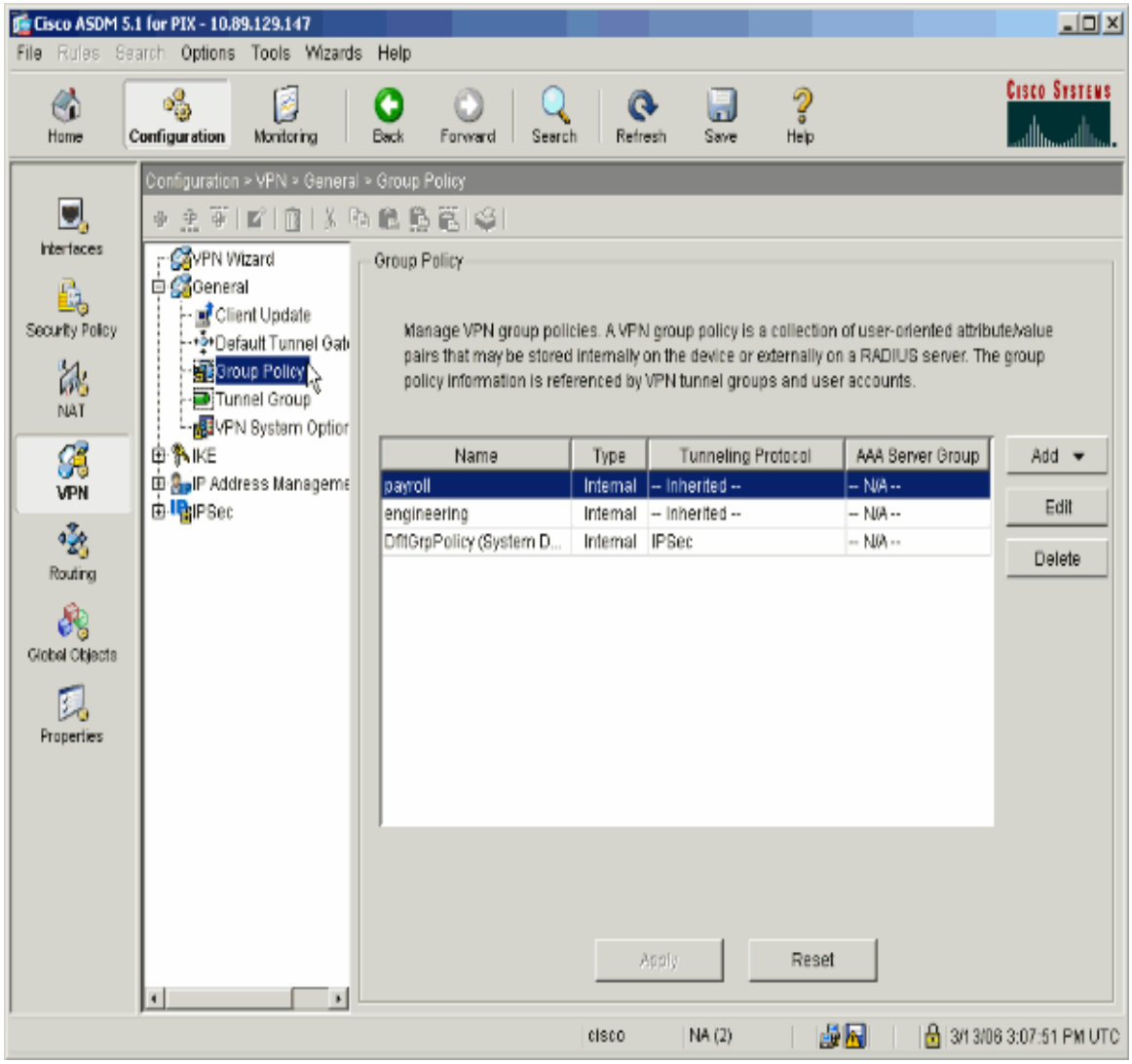


Şekil 6.18 Network Diyagram 2

Bu çalışmada üç alt ağa sahip merkezi bir ağ şekillendirilmiştir.Bu üç alt ağ Intranet, Engineering, ve Payroll 'dur.Bu çalışma ile Payroll personelinin Payroll ve Intranet subnetine uzak erişimine izin vermek ve Engineering subnetine erşimini önlemek için kongigğrasyon çalışması yapılacaktır.Bir de Intranet ve Engineering subnetlerine erişim uzaktan erişelebilir,fakat Payroll subnetine erişilemez.Bu çalışmadaki Payroll kullanıcısı "controller1"'dir.Engineering kullanıcısı "engineer1"'dir[17].

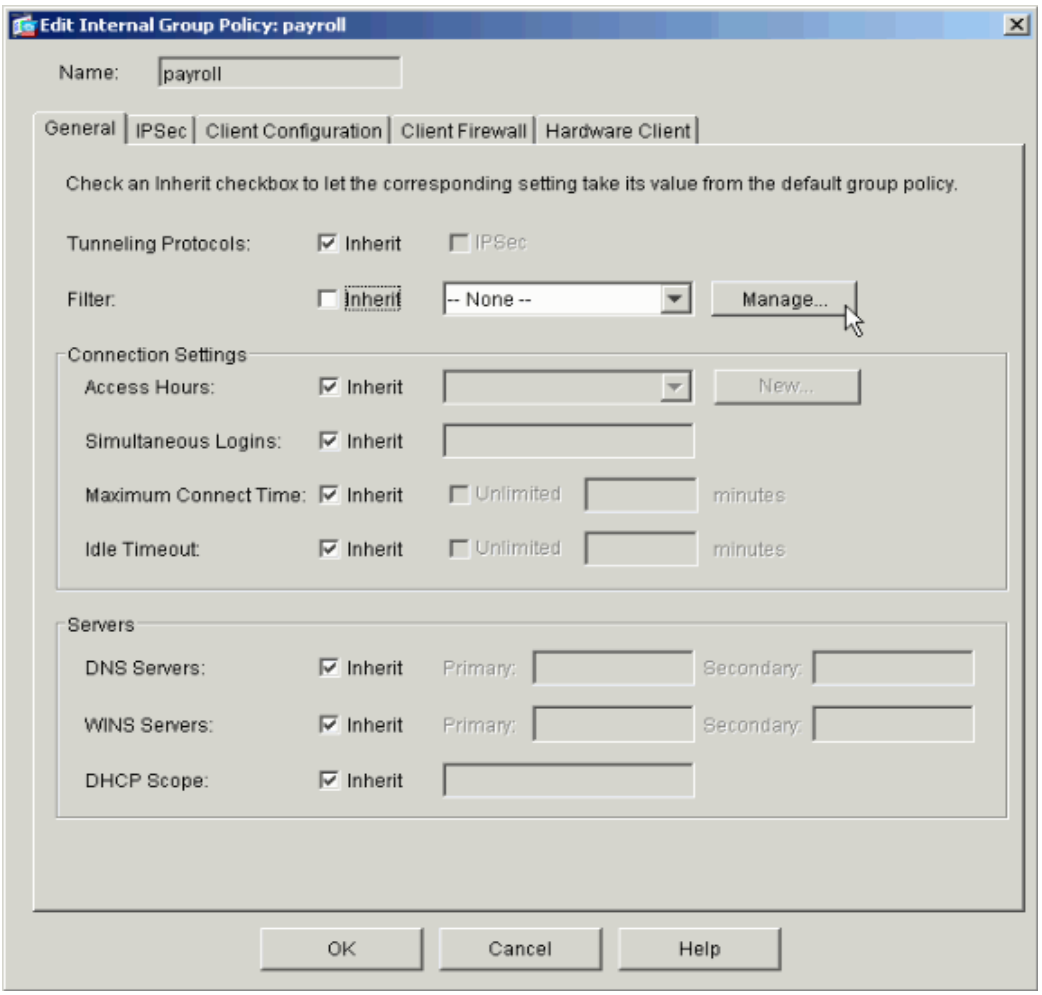
ASDM İle Konfigürasyon ;

- **Configuration > VPN > General > Group Policy** seçilir.



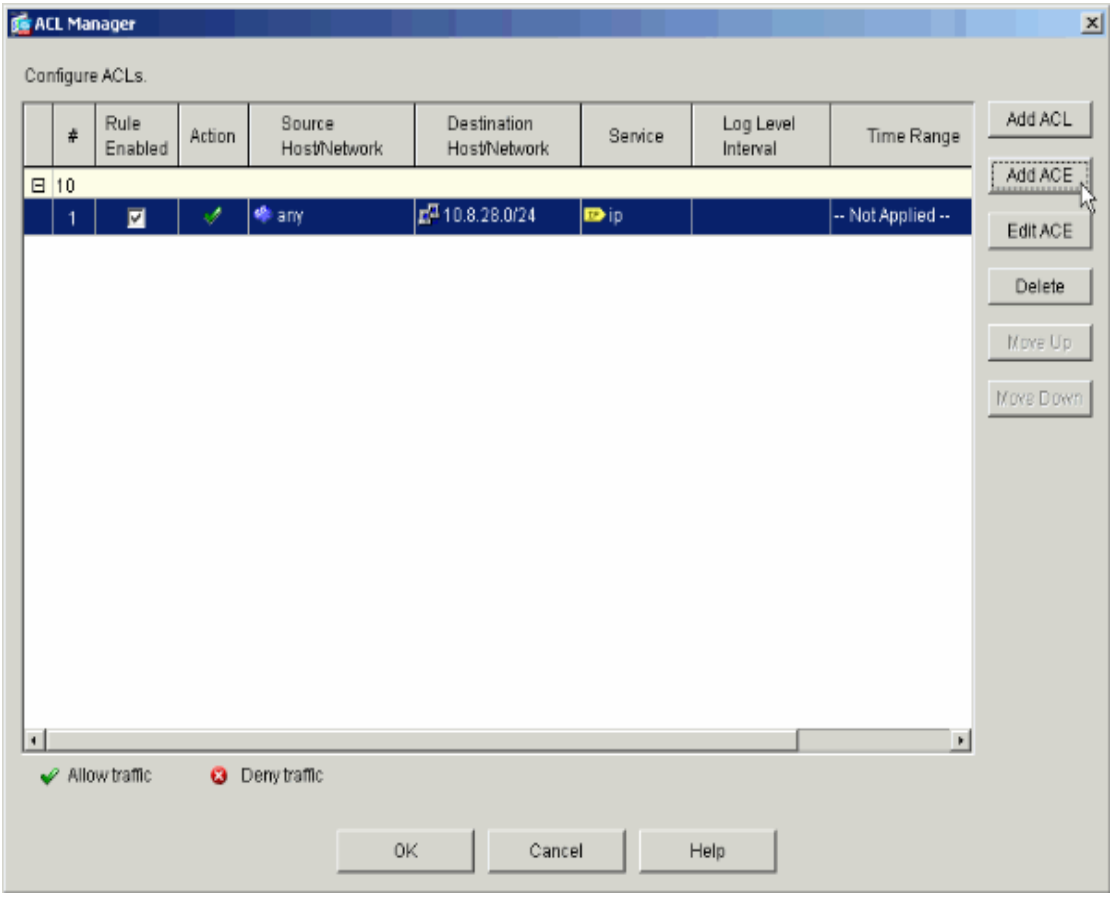
Şekil 6.19 VPN Grup Policy Yönetimi

- Group Policy'ler önceden tanımlanmışsa ,seçilir ve Edit'e tıklanır.Diğer türlü Add tıklanır ve **Internal Group Policy** seçilir**.**
- Gerekirse ,Açılan pencerenin en üstünde Group Policy'in ismi değiştrilir veya yeniden girilir.
- Filter'ın bitişindeki Inherit kutusu kaldırılır ve Manage Tıklanır.



Şekil 6.20 Access List Yaratılması

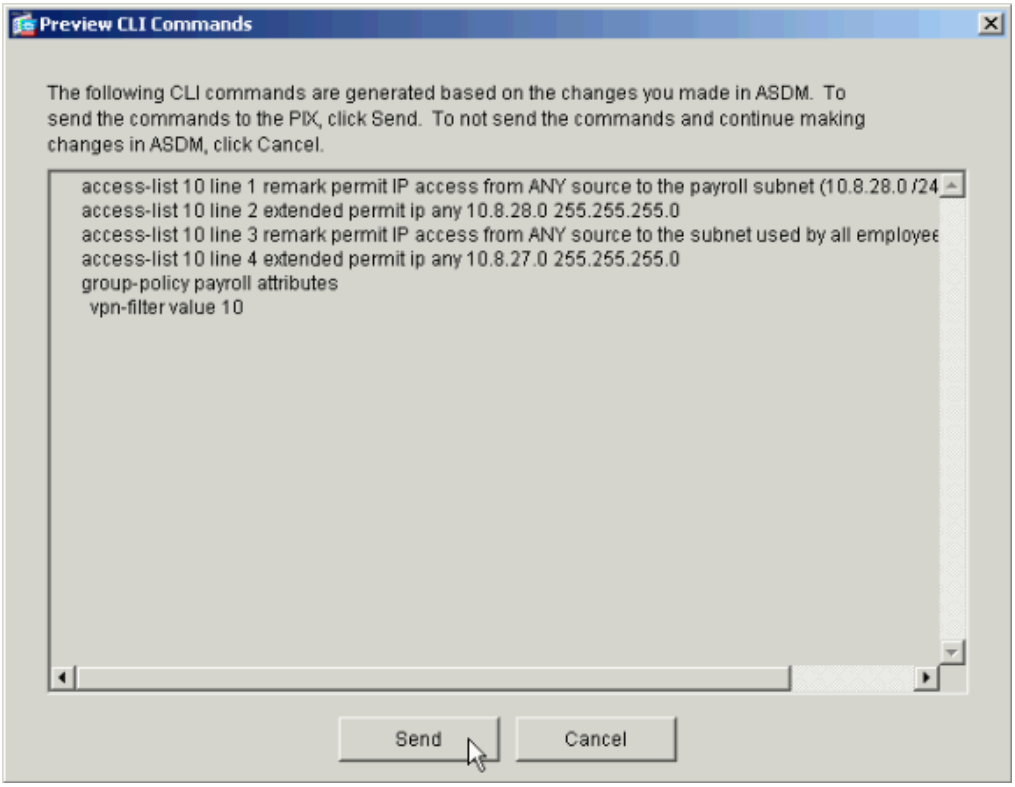
- Gözüken ACL Manager penceresinde yeni bir access list yaratmak için ACL ilave edilir.
- Yeni access list için bir numara seçilir ve Ok tıklanır.
- Listeye yeni bir erişim kontrol girdisi ilave etmek için Add ACE tıklanır .
- Bu çalışmada herhangi kaynaktan Payroll subnetine ACL içindeki ACE 10 IP erişimine izin verilir.Varsayılan olarak ASDM sadece protokol olarak TCP seçer.Full IP erişimine izin vermek ya da engellemek için IP seçmelidir.Bitirdiğin zaman OK tıklanır.
- Önceden ilave edilen listede ACE gözükmektedir.Access List'e herhangi bir ilave hat eklemek için add ACE seçilir.



Şekil 6.21 Yeni Bir Access List Yaratılması

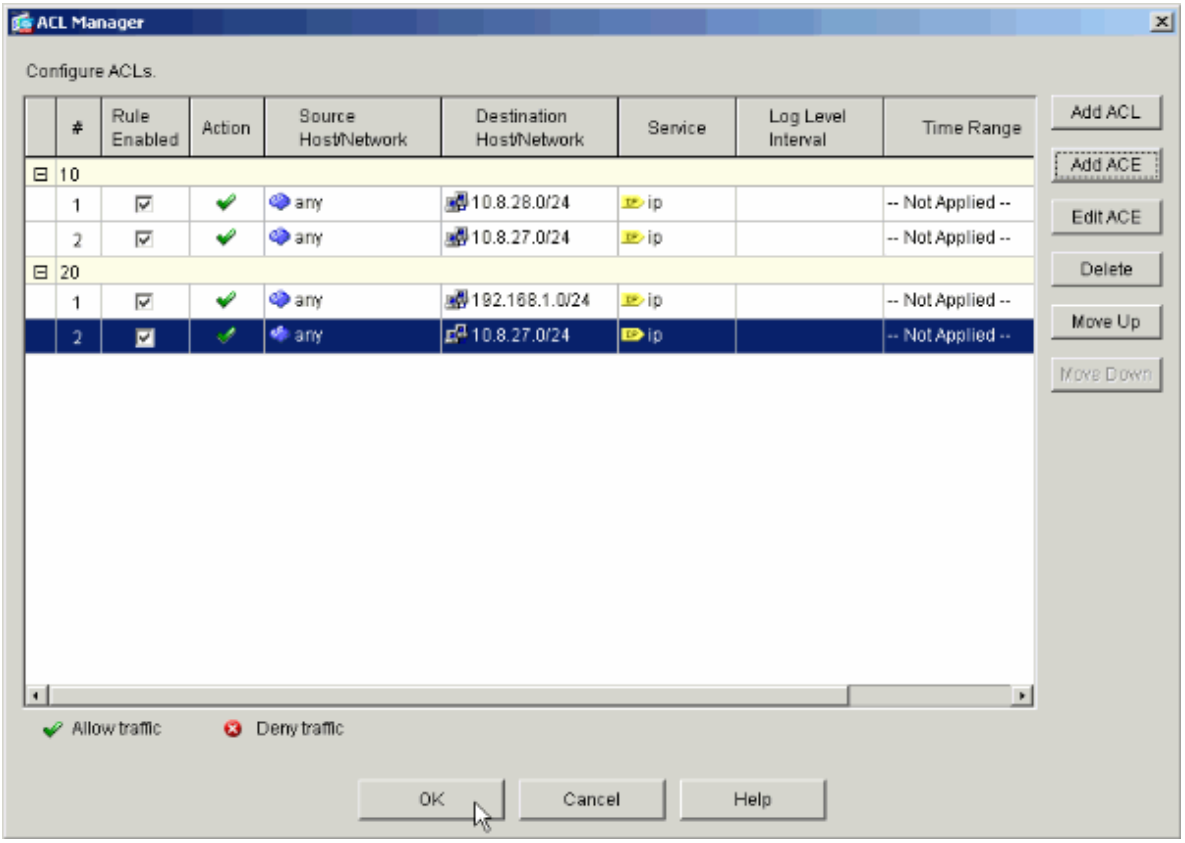
Bu çalışmada Intranet Subnetine erişime izin vermek için ACL 10 ‘a ikinci bir ACE eklenir.

- OK tıklanır.
- Group Policy için seçilen ve filtrelenen son adımlarda tanımlanan ACL seçilir. **OK** tıklanır
- Güvenlik duvarına değişiklikler gönderilir ve Apply seçilir.
- ASDM’de yapılan değişiklikler ,Send komutuna basılırsa güvenlik duvarına gönderilir.



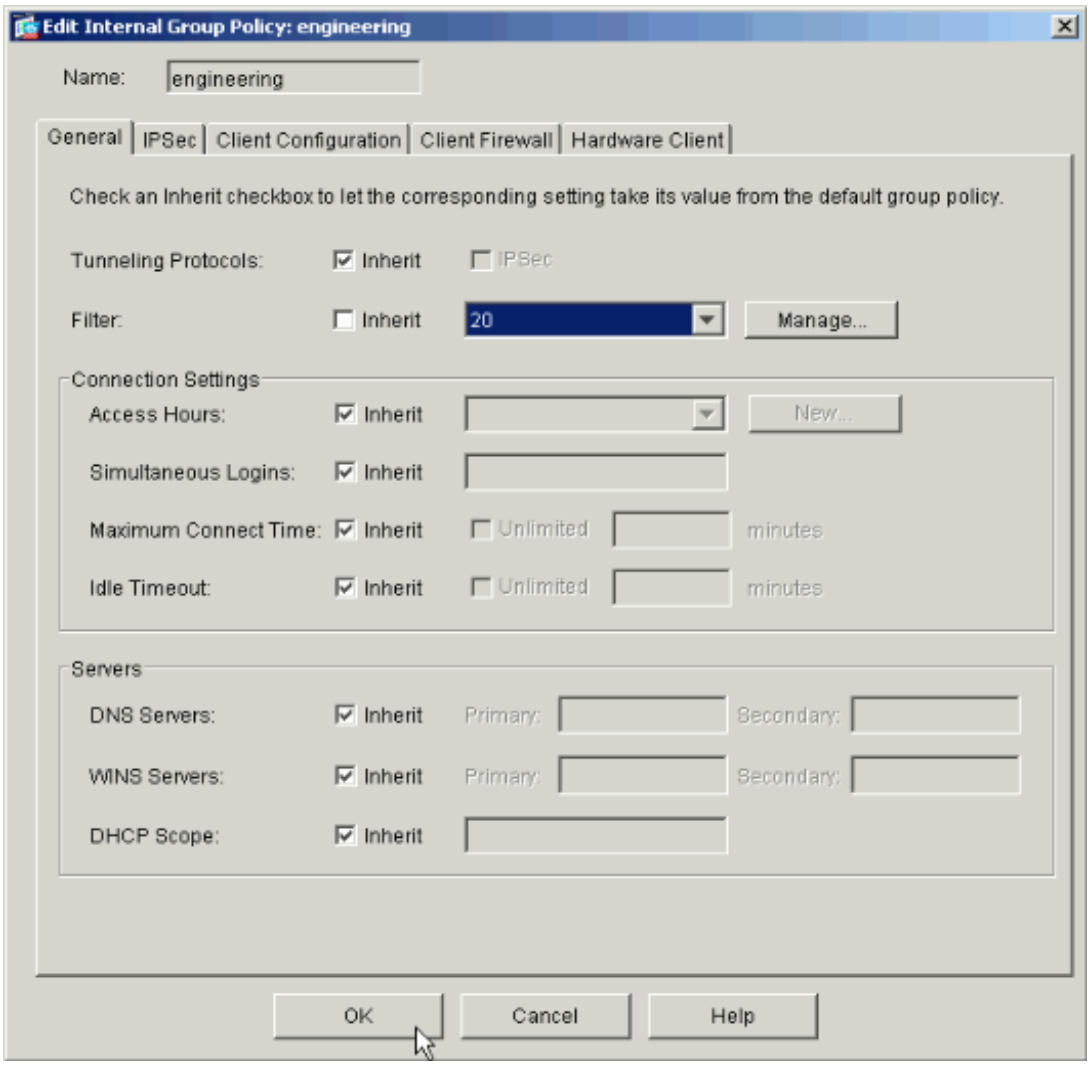
Şekil 6.22 CLI Komutlarının ASDM Üzerinde Gözükmesi

- Yaratığın veya şekillendirdiğin doğru tünel grubu olan Group Policy'i uygula ve sol çerçevedeki Tunnel Group 'u tıklanır.
- Edit' e tıklanır;
- Eğer Group Policy otomatik olarak yaratılırsa,açılan kutuda Tanımlana Group Policy konfigüre edilir.Eğer Group Policy otomatik oalrak yaratılmazsa,açılan kutudan seçilir ve OK tıklanır.
- Apply tıklanır ve hazırsa Send tıklanır ve güvenlik duvarına değişiklikler eklenir.Eğer Group Policy önceden seçilmişse "No changes were made." Mesajı alınır ve OK tıklanır.



Şekil 6.23 Access List'i Konfigüre Edilmesi

- Engineering Group Policy de bir filtre olarak **Access List 20** seçilir.



Şekil 6.24 Filtre Seçimi

- Engineering Tunnel Group için Engineering Group Policy tanımlanır.

CLI kullanarak Konfigüre Etmek;

- İki farklı Access Control List (15 ve 20) uzak erişim VPN'ine bağlanana kullanıcılara uygulanır.

ASAwCSC-CLI(config)#access-list 15 remark permit IP access from ANY source to the payroll subnet (10.8.28.0/24)

ASAwCSC-CLI(config)#access-list 15 extended permit ip any 10.8.28.0 255.255.255.0

ASAwCSC-CLI(config)#access-list 15 remark Permit IP access from ANY source to the subnet used by all employees (10.8.27.0)

ASAwCSC-CLI(config)#access-list 15 extended permit ip any 10.8.27.0 255.255.255.0

ASAwCSC-CLI(config)#access-list 20 remark Permit IP access from ANY source to the Engineering subnet (192.168.1.0/24)

ASAwCSC-CLI(config)#access-list 20 extended permit ip any 192.168.1.0 255.255.255.0

ASAwCSC-CLI(config)#access-list 20 remark Permit IP access from ANY source to the subnet used by all employees (10.8.27.0/24)

ASAwCSC-CLI(config)#access-list 20 extended permit ip any 10.8.27.0 255.255.255.0

- İki farkli VPN adres havuzu yaratılır.Payroll ve Engineerin uzak kullanıcıları için birer tane yaratılır.

ASAwCSC-CLI(config)#ip local pool Payroll-VPN 172.10.1.100-172.10.1.200 mask 255.255.255.0
ASAwCSC-CLI(config)#ip local pool Engineer-VPN 172.16.2.1-172.16.2.199 mask 255.255.255.0

- Bağlanıldığı zaman Payrolliçin policy yaratılır**.**

ASAwCSC-CLI(config)#group-policy Payroll internal

ASAwCSC-CLI(config)#group-policy Payroll attributes

ASAwCSC-CLI(config-group-policy)#dns-server value 10.8.27.10

ASAwCSC-CLI(config-group-policy)#vpn-filter value 15

!--- Call the ACL created in step 1 for Payroll.

ASAwCSC-CLI(config-group-policy)#vpn-tunnel-protocol IPSec

ASAwCSC-CLI(config-group-policy)#default-domain value payroll.corp.com

ASAwCSC-CLI(config-group-policy)#address-pools value Payroll-VPN

!--- Call the Payroll address space that you created in step 2.

- 3. adımdakiyle aynı ama bu engineering group için geçerlidir

ASAwCSC-CLI(config)#group-policy Engineering internal

ASAwCSC-CLI(config)#group-policy Engineering attributes

ASAwCSC-CLI(config-group-policy)#dns-server value 10.8.27.10

ASAwCSC-CLI(config-group-policy)#vpn-filter value 20

!--- Call the ACL that you created in step 1 for Engineering.

ASAwCSC-CLI(config-group-policy)#vpn-tunnel-protocol IPSec

ASAwCSC-CLI(config-group-policy)#default-domain value Engineer.corp.com

ASAwCSC-CLI(config-group-policy)#address-pools value Engineer-VPN

!--- Call the Engineering address space that you created in step 2.

- Yerel kullanıcılar yaratılır ve onların kaynaklara erişimini sınırlandırıcı özellikler atanır.

ASAwCSC-CLI(config)#username engineer password cisco123

ASAwCSC-CLI(config)#username engineer attributes

ASAwCSC-CLI(config-username)#vpn-group-policy Engineering

ASAwCSC-CLI(config-username)#vpn-filter value 20

ASAwCSC-CLI(config)#username marty password cisco456

ASAwCSC-CLI(config)#username marty attributes

ASAwCSC-CLI(config-username)#vpn-group-policy Payroll

ASAwCSC-CLI(config-username)#vpn-filter value 15

- Payroll kullanıcıları için bağlantı policyleri içeren tunnel-group ları yaratılır.

ASAwCSC-CLI(config)#**tunnel-group Payroll type ipsec-ra**

ASAwCSC-CLI(config)#**tunnel-group Payroll general-attributes**

ASAwCSC-CLI(config-tunnel-general)#**address-pool Payroll-VPN**

ASAwCSC-CLI(config-tunnel-general)#**default-group-policy Payroll**

ASAwCSC-CLI(config)#**tunnel-group Payroll ipsec-attributes**

ASAwCSC-CLI(config-tunnel-ipsec)#**pre-shared-key time1234**

- Engineering kullanıcıları için bağlantı policyleri içeren tunnel-groups yaratılır.

ASAwCSC-CLI(config)#tunnel-group Engineering type ipsec-ra

ASAwCSC-CLI(config)#tunnel-group Engineering general-attributes

ASAwCSC-CLI(config-tunnel-general)#address-pool Engineer-VPN

ASAwCSC-CLI(config-tunnel-general)#default-group-policy Engineering

ASAwCSC-CLI(config)#tunnel-group Engineering ipsec-attributes

ASAwCSC-CLI(config-tunnel-ipsec)#pre-shared-key Engine123

Yaptığımız çalışmayı monitörleyebilmek için ;

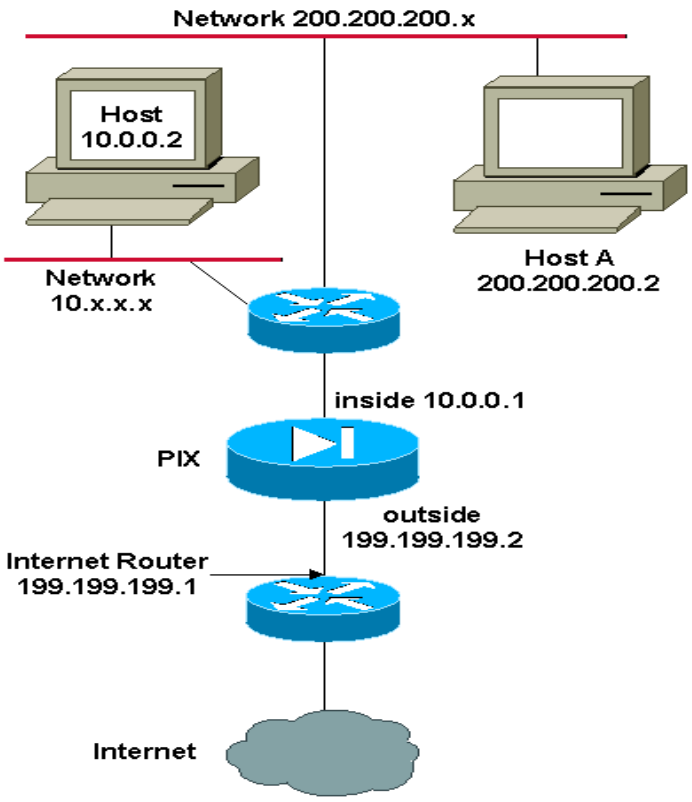
- Monitoring > VPN > VPN Statistics > Sessions seçilir ve Details tıklanır .

6.3 NAT

Günümüzde iç ağda bulunan tüm konakların hemen hepsi tahsisli olmayan IP numaraları kullanmaktadır ve bu adresleri içeren paketler İnternet üzerinde yönlendirilmez. Dış ağa açılan yönlendiriciler ise İnternet'de bilinen ve kendisine yönlendirme yapılabilen bir IP numarasına sahiptir. İç ağdaki konaklara erişimin sağlanabilmesi için NAT(Ağ Adres Çevrimi) desteği olan firewalllar , kendisine iç ağdan gelen her paketin kaynak adresini kendi adresi olarak değiştirir. Kendisine İnternet'den gelen paketlerin de hedef adresini iç ağdaki ilgili konağın adresi olarak değiştirir ve bu yolla iç ağdaki konakların İnternet üzerindeki konaklarla haberleşmesini sağlar. Bu işleme Ağ Adres Çevrimi denir.NAT yapıldığı zaman, oluşan trafiğin İnternet'den görülen hali, İnternet'de bulunan tek bir konağın bazı İnternet alışverişleri yaptığıdır. İnternet'e, bu konağın arkasındaki ağın büyüklüğü, bu ağdaki konakların cinsi, sayısı, ağın yapısı vs. hakkında herhangi bir bilgi gitmez. Dolayısıyla NAT, yalnızca tahsissiz ağlardan İnternet'e erişimi sağlamakla kalmaz, ağınızdaki konaklar hakkında bilgi edinilmesini (ve dolayısıyla size karşı yapılabilecek saldırıları) zorlaştırır. Fakat bunun bir Güvenlik Duvarı olduğu düşünülmemelidir ama Cisco Güvenlik Duvarları bileşenleri içinde NAT özeliği mevcuttur. Bu da sistemin güvenliğini artırmaktadır.Cisco ASA serisi üzerinde temel NAT ve PAT konfigürasyon örnekleri verilecektir[7][2][8].

6.3.1 NAT -Control Komutu

ASA üzerindeki NAT kontrol komutu güvenlik duvarı boyunca trafiğin geçmesi için özel iletim girdisine sahip olmak zorunda olan güvenlik duvarları boyunca tüm trafiği belirler. Bu özelliğin devre dışı bırakılmasıyla ASA paketleri konfigürasyondaki özel nakil girdisi olmaksızın yüksek güvenlkli arayüzden daha düşük güvenlikli arayüze iletir.Daha düşük güvenliklikli arayüzden daha yüksek arayüze trafiğin geçmesi için trafiğe izin veren access list ler kullanılır.ASA o zaman tarfiği iletir.



Şekil 6. 25 Multiple NAT Durumu

Bu örnekte ISP 199.199.199.1 den 199.199.199.63'e dizilmiş adreslerle ağ yönetimi sağlar.Ağ yönetimi Internet Router'ın üzerindeki iç arayüze 199.199.199.1 , 199.199.199.2 de güvenlik duvarının dış bacağına verilir.Ağ yönetici Internet'e erişmek için C sınıfı bir IP adresine 200.200.200.0/24 sahiptir,fakat iç lokasyonda 10.0.0.0/8 ağını kullanmaktadır.Bu ağ dizaynını sağlamak için aşağıdaki konfigürasyon yapılmalıdır;

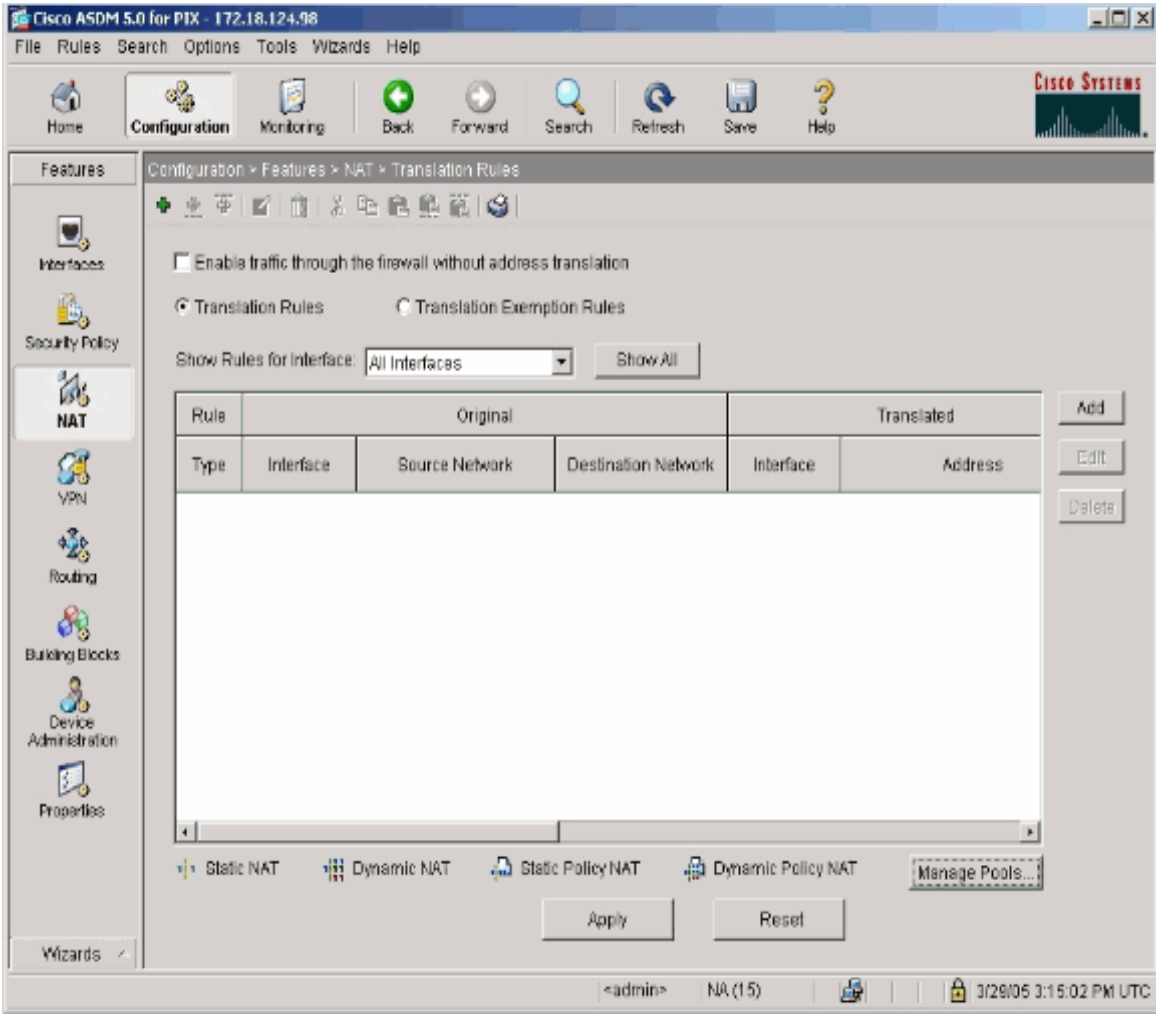
global (outside) 1 199.199.199.3-199.199.199.62 netmask 255.255.255.192
nat (inside) 0 200.200.200.0 255.255.255.0 0 0
nat (inside) 1 10.0.0.0 255.0.0.0 0 0

Bu konfigürasyon 10.0.0.0/8 ağındaki kaynak adresini 199.199.199.3 - 199.199.199.62 dizisizndeki bir adrese çevirir.

Aynı örneği ASDM kullanarak yaparsak ;

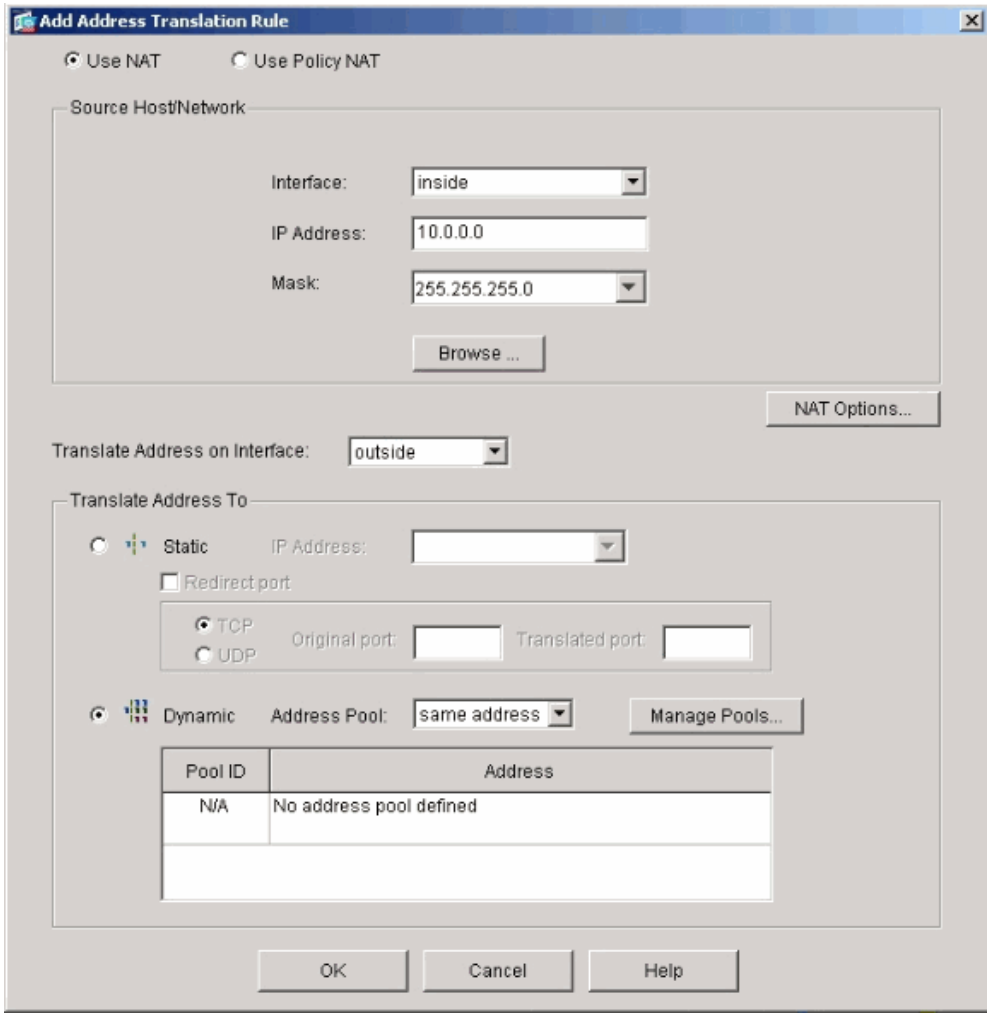
- ASDM açılınca ana ekrandaki Configuration'a basılır ve NAT tıklanır

- Yeni bir kural yazmak için + add ‘e basılır.



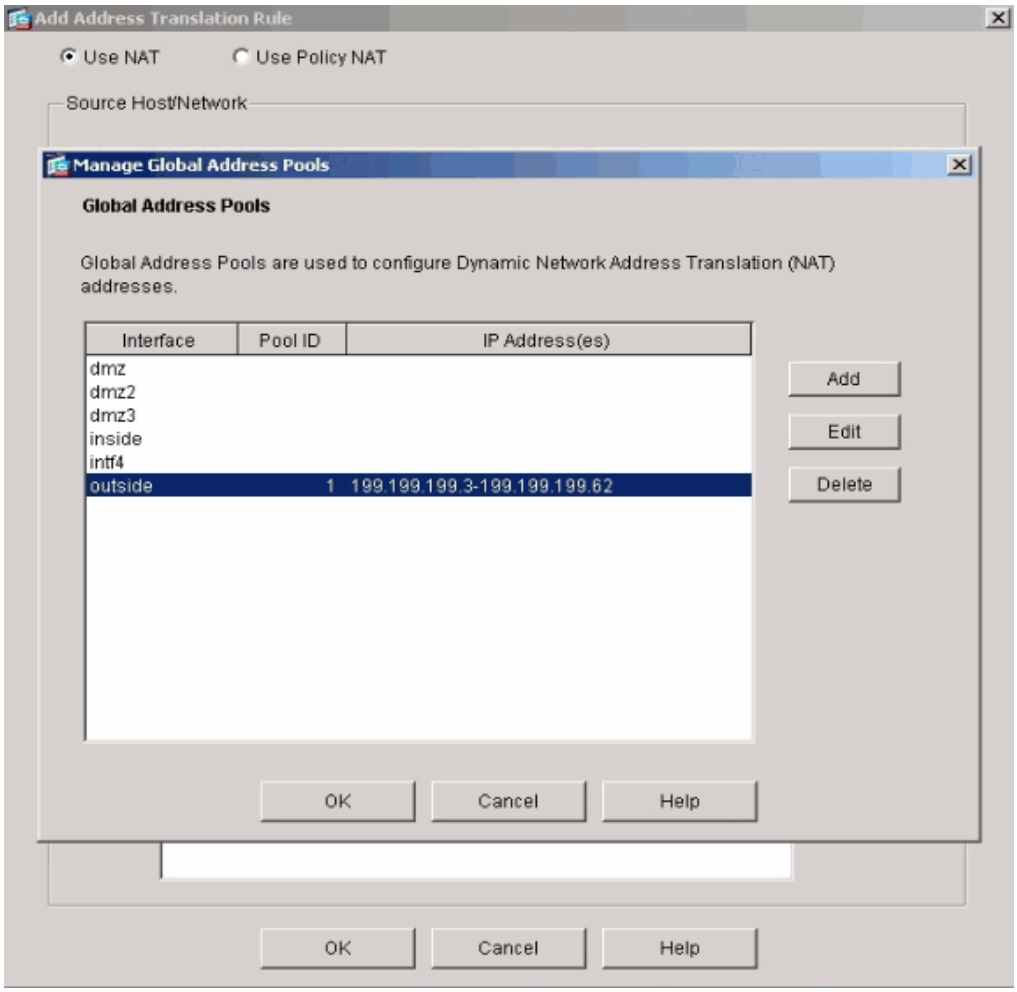
Şekil 6.26 ASDM Üzerinde NAT Konfigürasyonu

- Bu pencere bu NAT girdisi için NAT seçeneklerini değiştirmek için kullanıcılara izin verir.Bu örnekte ; 10.0.0.0/24 ağından kaynaktaki iç arayüze varan paketler üzerinde NAT sağlanır. Güvenlik duvarı bu paketleri dış bacak üzerindeki dinamik IP havuzuna nakil eder.Bu NAT’a hangi trafiği aktardığı bilgisi girildikten sonra ,nakil edilen trafik için IP adres havuzu tanımlanır.Yeni bir IP havuzu yaratmak içim Manage Pools tıklanır[15].



Şekil 6.27 Adres Havuzu Tanımlaması

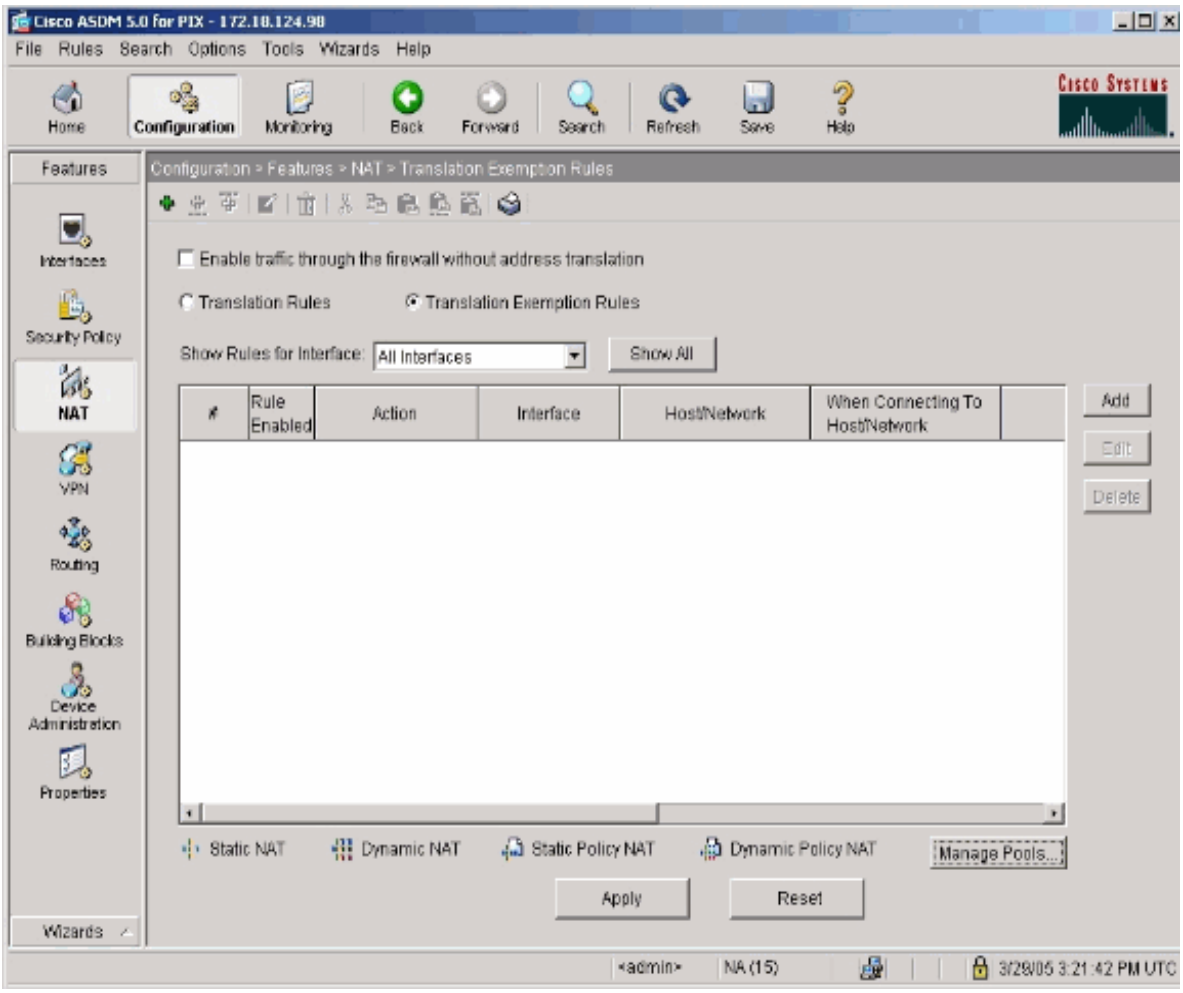
- Outside seçilir ve Add tıklanır.
- Havuz için IP dizisi tanımlanır ve havuza tamsayı ID Number verilir.
- Uygun değerler girildikten sonra ok tuşuna basılır ve dış arayüz için yeni bir tanımlı havuz görülür.



Şekil 6.28 Global Adres Havuz Tanımı

- Havuz tanımlandıktan sonra NAT Kural Konfigürasyon penceresine dönmek için OK tuşuna tıklanır.

- Güvenlik duvarı boyunca bir NAT yaratıldı.Fakat hangi trafiğin NAT olmayıcağını belirticek NAT girdisi yaratmaya ihtiyacı var.Pencerenin üzerindeki Translation Exemption Rules tıklanır. Ardından yeni bir kural yaratılır.



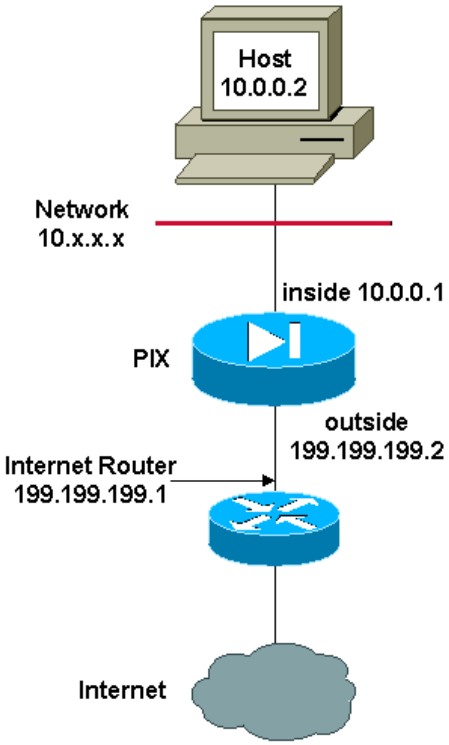
Şekil 6.29 NAT Yapılmıycak Trafiğin Belirlenmesi

- Kaynak olarak iç arayüzü seç ve 200.200.200.0/24 tanımlanır .

Konfigürasyon çıktısı ;

access-list inside_nat0_outbound extended permit
ip 200.200.200.0 255.255.255.0 any
global (outside) 1 199.199.199.3-199.199.199.62 netmask 255.255.255.192
nat (inside) 0 access-list inside_nat0_outbound
nat (inside) 1 10.0.0.0 255.255.255.0

6.3.1.1 İki IP Dizisi İle NAT Uygulaması

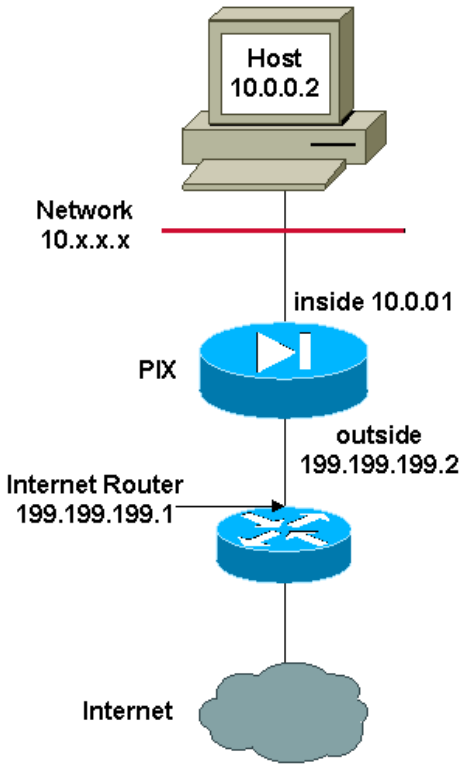


Şekil 6.30 İki IP Dizisi İle NAT Uygulaması Network Diyagramı

Bu örnekte ağ yöneticisi Internet üzerinde kayıtlı iki IP adres dizisine sahiptir.Ağ yöneticisi iç adreslerin hepsini kayıtlı adresler içinde 10.0.0.0/8 dizisine dönüştürmelidir.IP adres dizilerini ağ yöneticisi 199.199.199.1 -199.199.199.62 ve 150.150.150.1 -150.150.150.254 arasında kullanmalıdır..Ağ yöneticisi aşağıdaki tanımlamaları yapabilir;

global (outside) 1 199.199.199.3-199.199.199.62 netmask 255.255.255.192
global (outside) 1 150.150.150.1-150.150.150.254 netmask 255.255.255.0
nat (inside) 1 0.0.0.0 0.0.0.0 0 0

6.3.2 Karışım NAT ve PAT Konfigürasyonu



Şekil 6. 31 NAT ve PAT Network Diyagramı

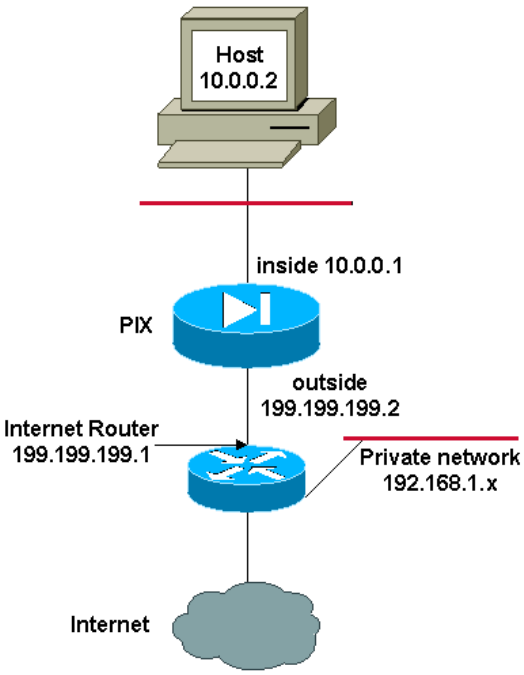
Bu örnekte ISP Şirket kullanımı için 199.199.199.1 'den 199.199.199.63'e adres dizini ağ yöneticisine sağlar.Ağ yöneticisi Internet yönlendiricisi üzerindeki iç arayüzü için 199.199.199.1 tanımlar ve 199.199.199.2 güvenlik duvarı üzerindeki dış arayüzü içindir.NAT havuzu için geri kalan 199.199.199.3-199.199.199.62 arası ayrılır.Fakat, Ağ yöneticisi bilir ki 60 kişiden daha fazla kullanıcı güvenlik duvarı dışına gitmeyi deneyebilir.Bu nedenle ağ yöneticisi 199.199.199.62 alır ve onu PAT adresi yapar ve böylelikle birçok kullanıcı aynı zamanda br adresi paylaşabilir.

global (outside) 1 199.199.199.3-199.199.199.61 netmask 255.255.255.192
global (outside) 1 199.199.199.62 netmask 255.255.255.192
nat (inside) 1 0.0.0.0 0.0.0.0 0 0

Bu komutlar güvenlik duvarını geçmek için 59 iç kullanıcının 199.199.199.3-199.199.199.1 61 kaynak adresine çevirimine yol gösterir.Bu adresler tükendikten sonra

,güvenlik duvarı NAT havuzunda boşta olan adreslerin birine kadar sonraki tüm kaynak adreslerini 199.199.199.62 çevirir.

6.3.3 NAT 0 Access-List ile Çoklu NAT Durumu



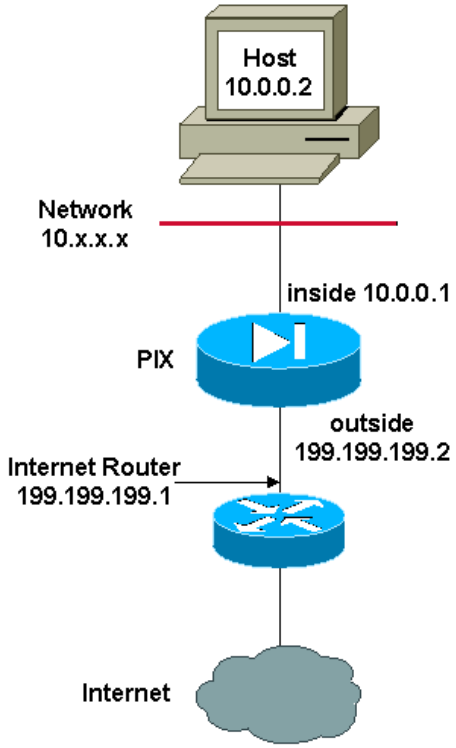
Şekil 6.32 Çoklu NAT Network Diyagramı

Bu örnekte ISP Şirket kullanımı için 199.199.199.1 'den 199.199.199.63'e adres dizini ağ yöneticisine sağlar. Ağ yöneticisi Internet yönlendiricisi üzerindeki iç arayüzü için 199.199.199.1 ve 199.199.199.2 güvenlik duvarı üzerindeki dış arayüzü için tanımlar.Fakat bı seneryo içinde LAN segmenti Internet Router'ının dışına yerleştirilir.Ağ yöneticisi bu iki ağ içindeki hostların birbirleri ile konuşucağı zaman global havuzdan adres değerlendireyi tercih etmez.

access-list 101 permit ip 10.0.0.0 255.0.0.0 192.168.1.0 255.255.255.0
global (outside) 1 199.199.199.3-199.199.199.62 netmask 255.255.255.192
nat (inside) 0 access-list 101
nat (inside) 1 10.0.0.0 255.0.0.0 0 0

Bu konfigürasyon 10.0.0.0/8 ‘nın bir kaynak adresi ve 192.168.1.0/24 ‘nı bir varış adresi ile bu adresleri çevirmez. 199.199.199.3 ‘den 199.199.199.62 adres dizisinden bir adres 192.168.1.0/24 adresinde herhangi bir yere varmak için 10.0.0.0/8 ağı içinden herhangi bir trafik başlangıcındaki kaynak adresine çevirir

6.3.4 Policy NAT



Şekil 6.33 Policy NAT Network Diyagramı

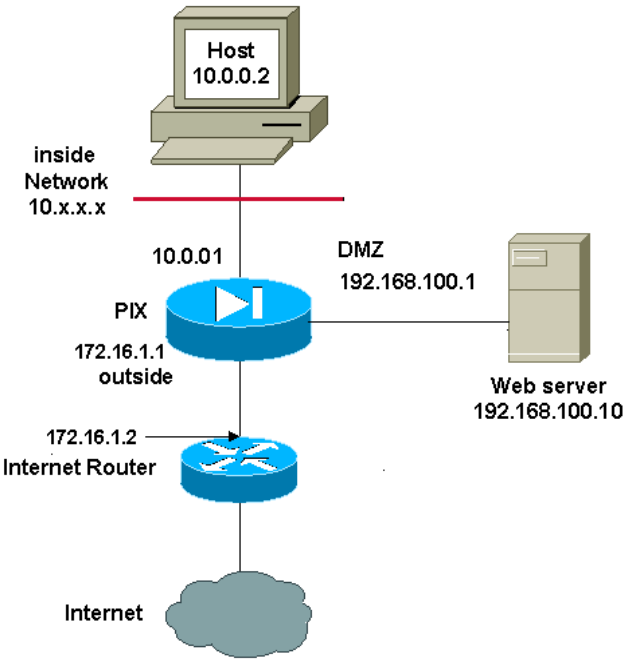
Sıfırdan farklı herhangi bir NAT ID için NAT Command ile access list kullanıldığı zaman ,Policy NAT kullanılabilir.Policy NAT bir access list içinde kaynak ve varış adreslerini tanımladığın zaman adres çevrimi için yerel trafiği tanımlamana olanak sağlar.Regular NAT kaynak adreslerini/portlarını kullanır,Policy NAT ise hem kaynak hemde varış adres/portlarını kullanır:Policy NAT ile her koşul için tek olan kaynak/port ve varış adresi/port için aynı lokal adreste tanımlanan çoklu NAT veya statik durumlar yaratabilirsiniz.Her kaynak/port ve Varış Noktası/Port çifti için farklı global adresler eşleşebilir.

Bu örnekte ağ yöneticisi varış IP adresi 209.165.201.11 port 80 (web) ve port 23 (Telnet) için erişim sağlayabilir ama kaynak adresi olarak iki farklı IP adresi

kullanmalıdır.WEB için kaynak IP adresi olarak 199.199.199.3 kullanılır.Telnet için 199.199.199.4 kullanılır ve 10.0.0.0/8 dizindeki iç adreslerin hepsine çevrilmelidir.Konfigürasyon aşağıdaki gibi olacaktır;

access-list WEB permit tcp 10.0.0.0 255.0.0.0 209.165.201.11
255.255.255.255 eq 80
access-list TELNET permit tcp 10.0.0.0 255.0.0.0 209.165.201.11
255.255.255.255 eq 23
nat (inside) 1 access-list WEB
nat (inside) 2 access-list TELNET
global (outside) 1 199.199.199.3 255.255.255.192
global (outside) 2 199.199.199.4 255.255.255.192

6.3.5 Static NAT



Şekil 6.35 Static NAT Network Diyagramı

Statik NAT konfigürasyonu noktadan noktaya haritalama ve özel adresten bir diğer adrese çevrim sağlar. Konfigürasyonun bu çeşidi NAT tablosu içinde düzenli bir girdi yaratır.Bu çoğunlukla mail,web ,FTP ve diğer uygulama servisleri sağlayan kullanıcılar için yararlıdır.

Statik NAT konfigürasyonu ;

static (*real_interface*,*mapped_interface*) *mapped_ip real_ip* netmask *mask*

Yukarıdaki örnekte DMZ üzerindeki server a içlokasyondaki arayüz erişimi üzerinde kullanıcılar vermek için statik çeviri yapılır.İç lokasyondaki ve DMZ üzerindeki serverın adresi ve iç lokasyondaki bir adres arasında bir haritalama yaratılır.İç lokasyondaki kullanıclar iç adreslerle DMZ üzerindeki servera erişim sağlayabilirler.

static (DMZ,inside)10.0.0.10 192.168.100.10 netmask 255.255.255.255

DMZ üzerindeki server'a dış arayüz erişiminde kullanıcılar vermek için statik çeviri yaratılır.DMZ üzerindeki server'ın adresi ve dış arayüz üzerindeki adres arasında haritalama yaratılır.Dışarıdan gelen kullanıcılar dış adresler vasıtasıyla servera erişebilirler.

static (DMZ,outside) 172.16.1.5 192.168.100.10 netmask 255.255.255.255

Statik çeviride haritalanmış adreslere Access List kullanıcı erişimi vermelidir.Aşağıdaki konfigürasyonda sadece web üzerinde 80 (www/http) ve 443 (https) portlarına erişime izinlidir.

access-list OUTSIDE extended permit tcp any host 172.16.1.5 eq www
access-list OUTSIDE extended permit tcp any host 172.16.1.5 eq https

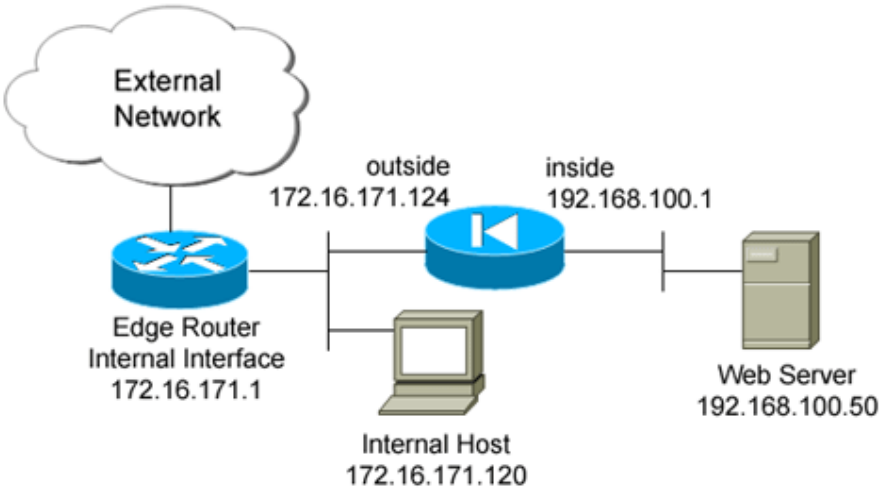
Access List dış arayüze uygulanmalıdır.

access-group OUTSIDE in interface outside

6.3.6 Çoklu Global Ip Adresi Statik Policy NAT Kullanarak Tek Lokal Ip Adresine Çevirme

Bu konfigürasyonda güvenlik duvarı ASA arkasında yerleşmiş 192.168.100.50 IP adresine sahip bir web server mevcuttur.172.16.171.125 bu serverın dış Ip adresidir.192.168.100.50 özel Ip adresi sadece 172.16.171.0/24 ağına erişebilir.İlave olarak, Internet Control Message Protocol (ICMP) ve 80port trafiği iç web server 'a

erişim hakkına sahip protokollerdir.İki global IP adresinin tek lokal bir IP adresine eşleşmesi durumuda ,policy NAT kullanılmasına ihtiyaç vardır[16].



Şekil 6.36 Çoklu Global Ip Adresi Statik Policy NAT Kullanarak Tek Lokal Ip Adresine Çevirme Network Diyagramı

Konfigürasyon ;

ciscoasa(config)#**show run**
: Saved
:
ASA Version 7.2(2)
!
hostname ciscoasa
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface GigabitEthernet0/0
 nameif outside
 security-level 0
 ip address 172.16.171.124 255.255.255.0
!
interface GigabitEthernet0/1
 nameif inside
 security-level 100

```
!
interface GigabitEthernet0/2
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/3
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Management0/0
 nameif management
 security-level 100
 ip address 192.168.1.1 255.255.255.0
 management-only
!
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
!--- policy_nat_web1 and policy_nat_web2 are two access-lists that match the source
!--- address we want to translate on.  Two access-lists are required, though they
!--- can be exactly the same.

access-list policy_nat_web1 extended permit ip host 192.168.100.50 any
access-list policy_nat_web2 extended permit ip host 192.168.100.50 any

!--- The inbound_outside access-list defines the security policy, as previously described.
!--- This access-list is applied inbound to the outside interface.
```

access-list inbound_outside extended permit tcp 172.16.171.0 255.255.255.0 host 192.168.100.50 eq www
access-list inbound_outside extended permit icmp 172.16.171.0 255.255.255.0 host 192.168.100.50 echo-reply
access-list inbound_outside extended permit icmp 172.16.171.0 255.255.255.0 host 192.168.100.50 echo
access-list inbound_outside extended permit tcp any host 172.16.171.125 eq www
access-list inbound_outside extended permit icmp any host 172.16.171.125 echo-reply
pager lines 24
logging asdm informational
mtu management 1500
mtu inside 1500
mtu outside 1500
no failover
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400

!--- This first static allows users to reach the translated global IP address of the
!--- web server. Since this static appears first in the configuration, for connections
!--- initiated outbound from the internal web server, the ASA translates the source
!--- address to 172.16.171.125.

static (inside,outside) 172.16.171.125 access-list policy_nat_web1

!--- The second static allows networks to access the web server by its private
!--- IP address of 192.168.100.50.

static (inside,outside) 192.168.100.50 access-list policy_nat_web2

!--- Apply the inbound_outside access-list to the outside interface.

access-group inbound_outside in interface outside

route outside 0.0.0.0 0.0.0.0 172.16.171.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout uauth 0:05:00 absolute
http server enable
http 192.168.1.0 255.255.255.0 management
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
telnet timeout 5
ssh timeout 5
console timeout 0
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect esmtp
  inspect sqlnet

```
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
!
service-policy global_policy global
prompt hostname context
```

7. SONUÇ

Birçok kurum, bir güvenlik duvarı aldığında güvenlik sorunlarının çoğunu çözdüğünü sanmaktadır ve diğer önlemleri önemsemektedir. Oysa güvenlik yönetimi ağ üzerinde çalışan bütün elemanların güvenliğini içerir ve sürekli devam eden bir süreç olarak ele alınmaldır. Bu çalışamda , ağ trafiğinin üzerinden aktığı ağ cihazlarında alınması gereken temel güvenlik önlemleri ele alınmış ve bazı ipuçları verilmiştir.

Dağınık yapıdaki özel iletişim ağlarının üzerinde bulunan bilgilerin, kamu iletişim ağı altyapısını kullanarak paylaşılması sırasında, kamu iletişim ağı üzerinden geçen bilgilerin üçüncü kişiler tarafından deşifre edilmesinin engellenmesi gerekmektedir.VPN bu sorunu ortadan kaldırmak için geliştirilmiş bir sistemdir. VPN sayesinde, özel iletişim ağına ait uzaktaki kullanıcıların, güvenilir olmayan kamu iletişim ağları üzerinden, kendi iletişim ağları ile serbestçe ve güvenilir bir şekilde haberleşmesi sağlanabilmektedir.Yapılan bu çalışmada ağ güvenliğini ilgilendiren her türlü bileşen incelenmiş ve son zamanlarda dünya çapında hızla yaygınlık kazanan güvenlik duvarı ile VPN ve NAT uygulamaları üzerinde durulmuştur.Bu uygulamalar için detaylı bir araştırma yapılarak konfigürasyon aşamaları araştırılıp ,güvenlik duvarı konfigürasyonu öğrenilmiştir.

Bilgi güvenliğinde tek çözümle etkin bir korunma sağlamanın mümkün olmayacağını dile getiren güvenlik uzmanları teknolojinin son dönemde gittiği noktanın bütünleşik çözümlerin olacağı yönündedir.Bu nedenle hızla çeşitlenen uygulama ve platformlar ve bunlara yönelik güvenlik tehditlerine karşı, farklı çözümlerin bütünleştirme ve yönetimini yürütecek, farklı tehditlere karşı tek bir çözümle güvenlik sağlama ihtiyacının ortaya çıkacağını bu nedenle tümleşik çözümlere yönelik çalışmalar hızla sürmektedir.

Yerel alan ağlarında güvenlik tüm bu sebeplerden dolayı üzerinde önemle durulması gereken
bir konudur.

KAYNAKLAR

[1] Analog Haberleşme , Veri Haberleşmesi Temelleri ,Yasin Kaplan

[2] Internetworking & TCP/IP,Armada Eğitim Merkezi,

[3] BİLGİSAYAR HABERLEŞMESİ VE AĞ TEKNOLOJİLERİ, Dr. Rifat ÇÖLKESEN, Prof.Dr. Bülent ÖRENCİK

[4] Bilgisayar Ağları; Dr. B. Demir Öner

[5] GÜVENLİK POLİTİKALARI Bitirme Tezi,Yalçın Tosun

[6] Increasing security on IP Networks, http://www.cisco.com/univercd/cc/td/doc/cisintwk/ics/cs003.htm

[7] CCNA Flash Cards and Exam Practice Pack (CCNP Self-study) by Eric Rivard

[8] CCNA: Cisco Certified Network Associate Study Guide (640-801) by Todd Lammle

[9]Understanding TCP, http://www.cisco.com/en/US/products/sw/secursw/ps743/products_user_guide_chapter09186a008007f2df.html

[10] TCP/IP Overview, http://www.cisco.com/en/US/tech/tk365/technologies_white_paper09186a008014f8a9.shtml

[11] Cisco Systems, (2007), "Cisco Aironet Antennas and Accessories", Cisco Systems, USA

[12] Wired Equivalent Privacy (WEP) on Aironet Access Points and Bridges, http://www.cisco.com/en/US/tech/tk722/tk809/technologies_tech_note09186a0080094581.shtml

[13] Ağ Cihazlarının Güvenliğinin Sağlanma Yöntemleri,Enis Karaaslan, Ege Üniversitesi Kampüs Network Güvenlik Grubu

[14] Enterprise Branch Security Design Guide ,Cisco Systems

[15]NAT and PAT Statement ,

http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/products_configuration_example09186a008046f31a.shtml

[16]Translate Multiple Global IP Adress to Single IP Adress;
http://www.cisco.com/en/US/products/ps6120/products_configuration_example09186a00807d2874.shtml

[17]http://www.cisco.com/en/US/products/ps6120/prod_configuration_examples_list.html,Cisco Systems,

ÖZGEÇMİŞ

Adı Soyadı : Zeynep Yüksel
Doğum Yeri ve Tarihi : İstanbul 18.06.1981
Adres : Cengiz Topel Cad. Adem Yavuz Sk.
Seven Koop. Evleri D Blok Daire 4 Kartal/İstanbul
Telefon : 0216 353 89 38
Cep Telefonu : 0533 234 93 97

Öğrenim
Lise : Kartal Lisesi
Lisans : Yıldız Teknik Üniversitesi
Elektronik ve Haberleşme Mühendisliği

Yabancı Dil Bilgisi **:** İngilizce (İyi Derecede)

Bilgisayar Bilgisi **:** Microsoft Officcce Tools (Word, Excel, Powerpoint, Access); Microsoft İşletim Sistemleri (95,98,2000,ME,XP);Elektronic Workbench, Mathlab, Mathcad, Pascal, Assembly, Photoshop, Dreamweaver, Front Page,Cisco Config Maker ,TCP/IP,Routing & Switching, Cisco - Firewall Uygulamaları , Frame Relay ,Hubs / Routers (Konfigürasyonu ve Kablolaması) , ISDN , Local Area Network - Lan , WAN ,MRTG,VOIP(FXO,FXS) , VPN , NAT Netscreen Firewall, SSL VPN, IDP Juniper Networks (Konfigürasyonu ve Kablolaması)

Stajlar
Probil Bilgi İşlem Destek Ve Danışmanlık San.Ve Tic. Şti.,2003
Turkcell A.Ş.,2002

İş Tecrübesi
PL4C Teknoloji Çözümleri, (01.07.05- 21.05.06)
Logicom Bilgi Teknolojileri Ltd.Şti.,(22.05.06- ?)