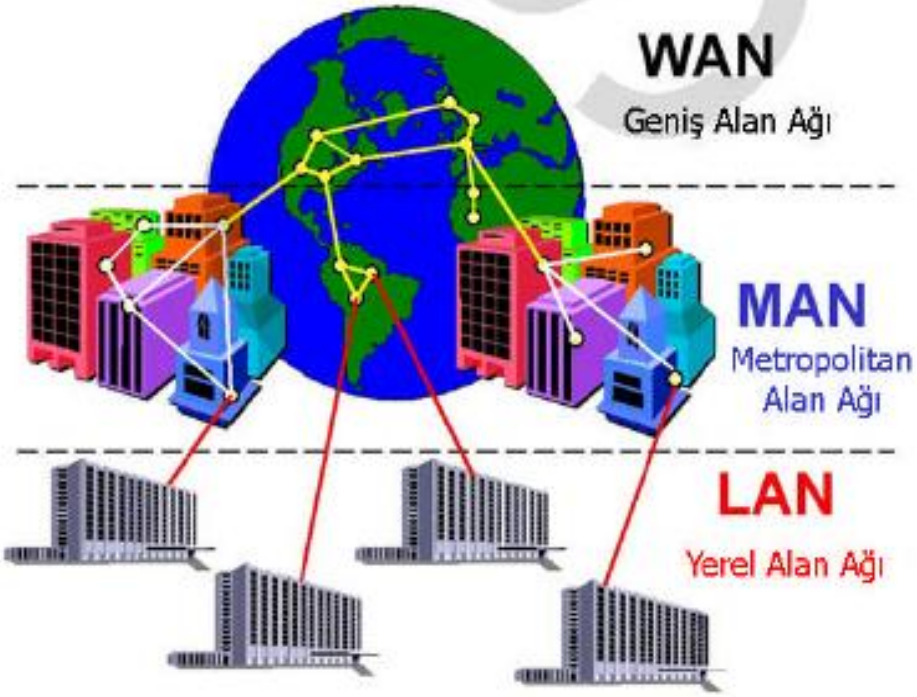
BİLGİSAYAR AĞLARI



İÇİNDEKİLER

1 BÖLÜM 9
1.1 BİLGİSAYAR AĞLARINA GİRİŞ TARİHÇESİ 9
1.1.1 BANT GENİŞLİĞİ 9
1.1.2 TEMEL BAND 10
1.1.3 GENİŞ BAND 10
1.2 AĞ TÜRLERİ 10
1.3 BİLGİSAYAR AĞLARININ SINIFLANDIRILMASI 11
1.3.1 Yerel Bilgisayar Ağları (LAN, Local Area Networks) 11
1.3.2 LAN İletişim Metodları 12
1.3.3 Geniş Alan Bilgisayar Ağları (WAN, Wide Area Network) 13
1.3.4 Şehirsel Bilgisayar Ağları (MAN, Metropolitan Area Network) 14
1.4 AĞ TOPOLOJİLERİ 15
1.4.1 (Topology) nedir? 15
1.4.2 Fiziksel topoloji 15
1.4.3 Mantıksal topoloji 15
1.5 Topoloji tipleri 15
1.5.1 Bus topoloji 15
1.5.2 Halka(Ring) topoloji 16
1.5.3 Yıldız(Star) topoloji 17
1.5.4 Mesh(ağ) topoloji 17
1.5.5 Tree (Ağaç) topoloji: 18
1.5.6 Melez(Hybrid) topolojiler 18
1.6 AĞ KABLO TİPLERİ 20
1.6.1 Koaksiyel Kablo (Coaxial Cable) 20
1.6.2 Dolanmış Çift Kablo (Twisted Pair Cable) 22
1.6.3 Kaplamalı Dolanmış Çift (Shielded Twisted Pair-STP) 23
1.6.4 Kaplamasız Dolanmış Çift (Unshielded Twisted Pair-UTP) 23
1.6.5 Fiber Optik 25
1.6.6 Kablo türlerinin karşılaştırılması 28
1.6.7 KAYNAKÇA 29
2 BÖLÜM 30

2.1 AĞ TEKNOLOJİLERİ 30
2.1.1 Ethernet Teknolojisi 30
2.1.2 Token-Ring Teknolojisi 30
2.1.3 Asynchronous Transfer Mode (ATM) Teknolojisi 30
2.1.4 Fiber Distributed Data Interface (FDDI) Teknolojisi 30
2.1.5 Frame Relay Teknolojisi 31
2.1.6 ISDN (Integrated Services Digital Network) 31
3 BÖLÜM 32
3.1 Ağ Nedir? 32
3.1.1 Temel Ağ Bileşenleri 32
3.1.2 Bilgisayarın Ağdaki Rolleri 33
3.1.3 Ağ Topolojileri 33
3.1.4 Kaynak Kanal Hedef 34
3.1.5 İletişim Kuralları 34
3.1.6 İleti Kodlama 35
3.1.7 İleti Biçimlendirme 36
3.1.8 İleti Boyutu 37
3.1.9 İleti Zamanlama 37
3.1.10 Erişim Yöntemi 37
3.1.11 Akış Denetimi 37
3.1.12 Yanıt Zaman Aşımı 38
3.1.13 İleti düzenleri 38
3.1.14 İletişimde Protokol Kullanımı 38
3.1.15 Protokollerin Önemi 39
3.1.16 Protokollerin Standartlaşması 39
3.1.17 Fiziksel Adresleme 40
3.2 Ethernet İletişimi 41
3.2.1 Ethernet Ağlarının Hiyerarşik Tasarımı 41
3.2.2 Mantıksal Adresleme 42
3.2.3 Erişim ve Dağıtım Katmanı ve Cihazlar 42
3.2.4 Erişim Katmanı 43
3.2.5 Dağıtıcıların İşlevi 43
3.2.6 Anahtarların İşlevi 44

3.2.7 Dağıtım Katmanı 45
3.2.8 Yönlendiricilerin İşlevi 46
3.2.9 Varsayılan Ağ Geçidi 47
3.2.10 Yönlendiriciler Tarafından Korunan Tablolar 47
3.2.11 Köprü 48
3.2.12 Yineleyici 48
3.3 Ağa Erişim Metotları 49
3.3.1 PSTN 49
3.3.2 ISDN 49
3.3.3 ADSL 49
3.3.4 Topoloji Tipleri 50
3.4 KAYNAKLAR 52
4 BÖLÜM 53
4.1 OSI MODELİ VE FİZİKSEL KATMAN 53
4.1.1 OSI nedir ? 53
4.1.2 Fiziksel Katman (Physical Layer) 54
4.2 İşaretlerin Kodlanması: 58
4.2.1 Analog İşaretlerin Kodlanması: 59
4.2.2 Sayısal İşaretin Kodlanması: 60
4.3 Kablosuz Yerel Ağ (Wireless Local Area Network) 62
4.3.1 Kablosuz Yerel Ağların Çalışması 63
4.3.2 Kablosuz Ağ Türleri 63
4.4 Lan Bağlantı Standartları 65
4.4.1 Bnc Alt Yapısı 65
4.4.2 Utp Sistemler 66
4.4.3 Rj 45 Konnektör 66
4.4.4 Cross Bağlantı 67
4.4.5 Tr Bağlantı Konnektörü 67
4.4.6 Fiberoptik Konnektör Türleri 68
4.4.7 AUI ve MII Standartları 69
4.5 KAYNAKLAR 69
5 BÖLÜM 70
5.1 TAŞIMA KATMANI 70

5.1.1 Taşıma Katmanı Nasıl Çalışır? ... 70
5.1.2 Taşıma Katmanının İki Önemli Fonksiyonu ... 70
5.1.3 TCP (Transmission Control Protocol) ... 70
5.1.4 Tcp/Ip Modeli ... 71
5.2 Uygulama Katmanı ... 71
5.3 Taşıma Katmanı ... 72
5.4 Ağ Katmanı ... 72
5.5 Fiziksel Katman ... 72
5.6 Özetle Tcp ... 72
5.7 Bağlantı Kurulumu ... 73
5.8 TCP Fonksiyonları ... 73
5.8.1 Güvenlilik (Reliability) ... 74
5.8.2 Akış Kontrolü (Flow Control) ... 75
5.8.3 Ara Bellekleme (Buffering) ... 75
5.8.4 Tıkanıklıktan Kaçma (Congestion Avoidance) ... 75
5.8.5 Pencereleme (Windowing) ... 76
5.8.6 UDP(user datagram protokol) ... 77
5.9 MULTİPLEXİNG ... 81
5.10 DEMULTİPLEXİNG ... 81
5.11 TCP SEGMENT YAPISI ... 81
5.12 Transport Katmanı Port Numaraları ... 83
5.13 TAŞIMA KATMANI GÜVENLİ İLETİŞİM PROTOKOLLERİ ... 83
5.13.1 SSH Nedir? ... 83
5.13.2 SSH ile ilgili temel tanımlar ... 84
5.13.3 SSL (Secure Socket Layer) Nedir? ... 87
5.13.4 PCT Nedir? ... 92
5.13.5 TLS Nedir? ... 92
5.13.6 TCP'DE TIKANIKLIK KONTROLÜ ... 93
5.14 Kablosuz Ağlarda Tıkanıklık ... 94
5.14.1 Tıkanıklık Önleme Yöntemleri ... 94
5.15 KAYNAKLAR ... 95
6 BÖLÜM VERİ BAĞLANTI KATMANI ... 97
6.1 Veri Bağlantı Katmanı (Data Link Layer) ... 97

6.1.1 Veri Bağlantı Katmanının İletişim Kuralları 97
6.1.2 Veri Bağlantı Katmanı Temel Fonksiyonları 98
6.1.3 Veri Bağlantı Katmanının Bileşenleri 101
6.2 HATA TESPİTİ VE DÜZELTİLMESİ 102
6.2.1 HATA TESPİT TEKNİKLERİ 103
6.3 HATA DÜZELTME TEKNİKLERİ 105
6.3.1 HAMMING KODLAMASI 106
6.3.2 ARQ (AUTOMATIC REPEAT REQUEST – OTOMATİK TEKRAR İSTEĞİ) 106
6.3.3 DUR VE BEKLE PROTOKOLÜ 107
6.3.4 SÜREKLİ TEKRAR İSTEMİ (Continious RQ) 109
6.3.5 SEÇMELİ TEKRAR (SELECTİVE REPEAT) 109
6.3.6 N ÇERÇEVE GERİLE (GO BACK N) 111
6.4 KABLOSUZ AĞ TEKNOLOJİSİ 111
6.4.1 Yerel Alan Bilgisayar Ağları (LAN, Local Area Networks) 112
6.4.2 Geniş Alan Bilgisayar Ağları (WAN, Wide Area Network) 112
6.4.3 Şehirsel Bilgisayar Ağları (MAN, Metropolitan Area Network) 113
6.4.4 Kişisel Alan Ağları (PAN,Personel Area Network) 113
6.5 KABLOSUZ AĞ TEKNOLOJİLERİ 113
6.5.1 Bluetooth 113
6.5.2 Home RF 114
6.5.3 IrDA (Infrared Data Association) 115
6.6 ÇOKLU ERİŞİM PROTOKOLLERİ 116
6.6.1 Aloha 116
6.6.2 CSMAP (Carrier Sense Multipli Access Protocol) 116
6.6.3 CSMA/CD 118
6.6.4 Çarpışmasız Protokoller 118
6.7 AĞ BİLEŞENLERİ 119
6.7.1 Yineleyici (Repeater) 119
6.7.2 Bridge (Köprü) 119
Şeffaf Köprüler (Transparent Bridges) 120
Kaynaktan Yönlendirilmeli Köprüler (Source Routing Bridges) 120
Çevirici Köprüler (Translating Bridges) 120
Uzaktan Bağlantı Köprüleri (Remote Bridges) 120

6.7.3 Hub 121
6.7.4 Anahtarlar (Switch) 122
6.7.5 Router (Yönlendirici) 123
7 BÖLÜM 124
7.1 UYGULAMA KATMANI 124
7.1.1 Uygulama Katmanı İletişim Kuralları 124
7.1.2 KRİPTO YÖNTEMİ: 136
7.1.3 RLOGİN (REMOTE LOGİN) : 136
7.2 POP3 özellikleri: 137
7.3 IMAP özellikleri: 137
7.4 FTP Nedir? 138
7.4.1 FTP Yapmak İçin Nelere İhtiyaç Var? 138
7.4.2 Anonymous FTP Nedir? 138
7.4.3 SNMP nedir? 138
7.4.4 SNMP'yi Oluşturan Bileşenler 139
7.5 KAYNAKLAR 140
8 BÖLÜM 141
8.1 UYDU NEDİR? 141
8.1.1 Uyduların Yörüngesi 141
8.1.2 Uyduların Enerji Kaynakları 141
8.1.3 Uzayda Uydunun Dengesi 141
8.1.4 Uydunun Ömrü 141
8.2 UYDU İLETİŞİM SİSTEMLERİ 142
8.2.1 TV Yayını Ve Uydu Frekansları 142
8.2.2 X Bandı Yayını : 142
8.2.3 C Band Yayınları : 142
8.2.4 KU Bandı Yayını : 142
8.3 UYDU ÇEŞİTLERİ 143
8.3.1 Yeryüzüne olan Yüksekliklerine Göre Sınıflandırılması 143
8.3.2 Kullanım Amaçlarına Göre Sınıflandırılması [2] 143
8.4 UYDULARIN YAPISI, YÖRÜNGESİ VE ENERJİSİ 144
8.4.1 Uydu Haberleşme Sistemleri 144
8.4.2 Uyduların Yapısı: 144

8.4.3 Uyduyu Oluşturan Bileşenler 145
8.5 UYDULARIN YÖRÜNGELERİ 145
8.5.1 Kutup Yörüngeli Uydular: 145
8.5.2 Ekvatoral Uydular 145
8.5.3 Eliptik Yörüngeli Uydular 145
8.6 UYDU İLETİŞİM SİSTEMERİNDE ÇOKLAYICI YÖNTEMLER 146
8.6.1 Frekans paylaşmalı çoklayıcı geçiş 146
8.6.2 Zaman paylaşmalı çoklayıcı geçiş 149
8.6.3 Kod paylaşımlı çoklu geçiş 150
8.7 TÜRKSAT 3A UYDUSU 151
8.7.1 Teknik özellikler 151
8.7.2 Türksat A.Ş 151
8.7.3 TÜRKSAT 3A KAPSAMA ALANI 153
8.7.4 TÜRKSAT 4A 155
8.7.5 MİLLİ UYDU TÜRKSAT 5A 155
8.8 YER İSTASYONLARI 155
8.8.1 Alıcı Yer İstasyonu (Downlink) 156
8.8.2 Verici Yer İstasyonu (Uplink) 157
8.8.3 YER İSTASYONUNUN ANTEN SİSTEMİ 157
8.9 KAYNAKLAR 160
9 BÖLÜM 161
9.1 BİYOMETRİ NEDİR ? 161
9.2 BİYOMETRİK TANIMA NASIL ÇALIŞIR? 161
9.3 BİYOMETRİNİN UYGULAMA ALANLARI 162
9.4 BİYOMETRİK TEKNOLOJİLER 162
9.4.1 Parmak İzi Tanıma 162
9.4.2 İris ve Retina Tanıma 163
9.4.3 Ses Tanıma 163
9.4.4 İmza Tanıma 164
9.5 BİYOMETRİK TEKNOLOJİLER STANDART MIDIR ? 164
9.6 BİREY AYIRT ETME KAYNAKLARI KARŞILAŞTIRMA TABLOSU 164
9.7 KAYNAKÇA 166

1 BÖLÜM

1.1 BİLGİSAYAR AĞLARINA GİRİŞ TARİHÇESİ

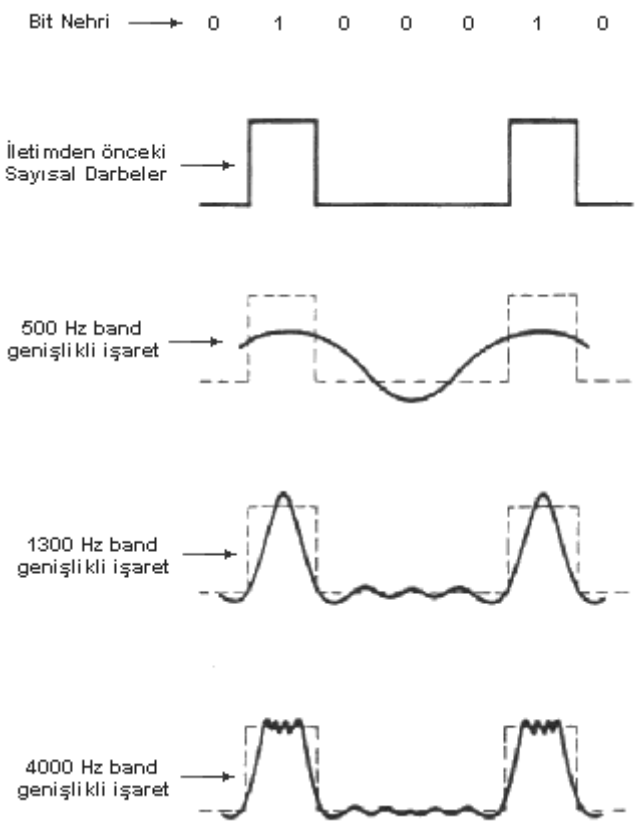
ARPA (Advanced Research Project Agency) adlı organizasyon aracılığıyla yapılan, askeri kaynakların finanse ettiği çalışmalar sonucunda 1970'lerin başında ARPANET adlı binlerce km uzaklıktaki bigisayarlarla sabit bigisayarların oluşturduğu bir geniş iletişim ağı ortaya çıkmıştır.

ARPA' nın geniş iletişim ağlarıyla, yerel iletişim ağlarını birbirine bağlama düşüncesi bugünkü adıyla Internet projesinin temelini ortaya çıkartmıştır. ARPA'nın farklı ağlar arasındaki uyumsuzluk problemine çözüm olması amacıyla desteklediği çalışmalar sonunda, Internet teknolojisinin temelini oluşturan TCP/IP (Transmission Control Protocol/Internet Protocol) ortaya çıkmıştır.
1983 yılı Internet'in deneysel olmaktan çıktığı yıldır. Bu yıldan sonra sivillerin de kullanmasına izin verilen ARPANET, Berkeley Üniversitesinin ARPA tarafından desteklenen BSD (Berkeley Software Distribution) adlı projesiyle yaygınlaşmıştır.

Amerikan Ulusal Bilim Vakfı'nın (National Science Foundation -NSF) ve ARPA'nın katkılarıyla 1985'de üniversite ve araştırma merkezlerinin kullanımı için NSFNET isimli ağ kurulmuştur. Bu durum ağların özellikle Avrupanın gelişmiş ülkelerinde de yaygınlaşmasını sağlamıştır. TCP/IP iletişim protokollerine paralel olarak, 1980'lerin başında başlıyarak Uluslar arası Standartlar Organizasyonu (International Standards Organization), daha sonraki yıllarda, uluslararası bir iletişim protokolleri standardı oluşturmuştur. Bu çalışma sonucunda Açık Sistemler Bağlantı modeli (Open Systems Interconnection -OSI) ortaya çıkmıştır.[1]

1.1.1 BANT GENİŞLİĞİ

Bir haberleşme hattının taşıyabildiği frekans , hattın bant genişliği olarak tanımlanır. Bant genişliği veri haberleşmesi için çok önemlidir. Çünkü haberleşme hattının miktarını (bit/sn), hattın bant genişliği belirler. Eğer telefon kanalının bant genişliği 3 kHz 'den (300-3300 Hz) 20 kHz 'e çıkartılırsa, kanal sesin tüm özelliklerini taşıyacaktı. Bu, aynı zamanda iletilen verinin doğruluğunu arttırır. Daha büyük bant genişliği kullanılarak daha iyi bir veri iletim oranı sağlanacağı açıktır. Bant genişliği büyüdükçe sayısal seviyeler daha doğru bir biçimde ortaya çıkacaktır. Daha büyük bant genişliği, daha yüksek hat kapasitesi demektir. 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 sanayisinin bant genişliği daha büyük kapasitesi için niye yüksek radyo frekanslarını kullanan teknolojilere yöneldiğini göstermektedir.



ŞEKİL 1.1. Değişik Bant değerleri [2]

1.1.2 TEMEL BAND

İletim ortamında kullanılan tek bir frekanstır. Bu durumda, teorik olarak iletim ortamının kapasitesi tamamıyla bir kanal için kullanılabilir. Örneğin; ethernet, temel bantı kullanan bir protokoldür.

1.1.3 GENİŞ BAND

Bir kullanıcıya ait sinyallerin sayısal verilere dönüştürülerek çok yüksek frekanslarda iletilmesidir. Gönderilen veriler alıcı üzerinde demodülatör (kip çözücü) yardımıyla ayıklanır. Bu iletim kanalı, ses iletim kanalına oranla daha geniş bir bant genişliğine sahiptir. Farklı frekans bant genişlikleri sayesinde belirli bir zamanda içinde çok daha fazla veri iletilebilir. İletişim cihazları ve cep telefonları kablosuz geniş bant kullanır.[3]

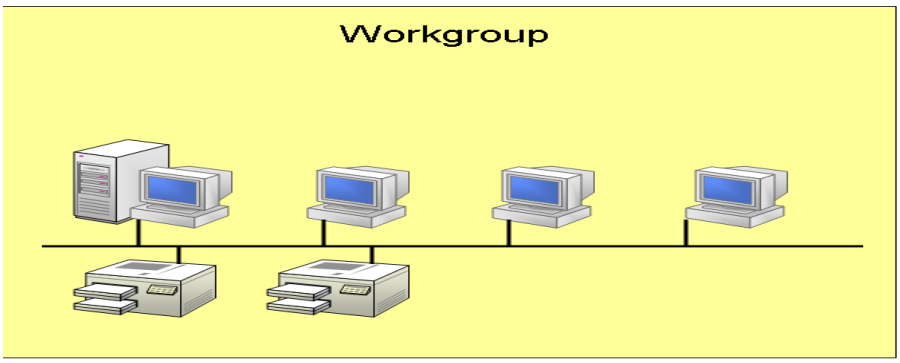
1.2 AĞ TÜRLERİ

Ağ üzerinde bilgisayarların nasıl iletişim kurduklarına göre ağlar ikiye ayrılır:

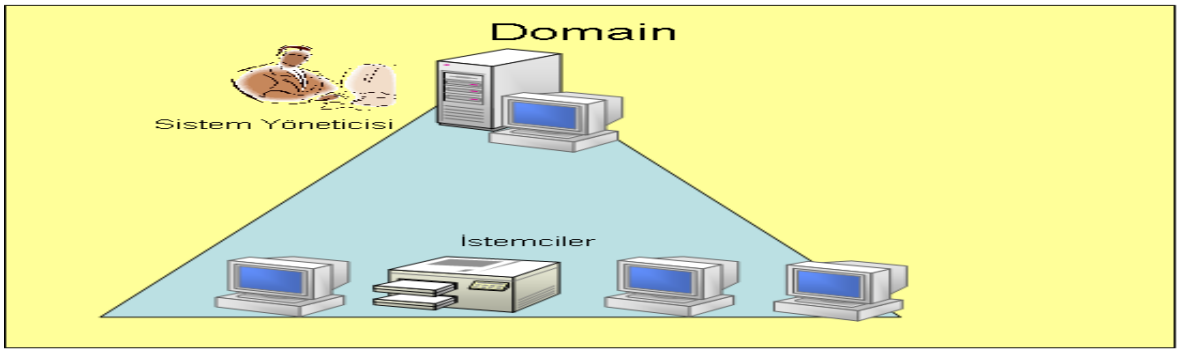
-Peer-to-peer Network (eşler arası)

-Server-Based (client/server) Network

Eşler-arası (peer-to-peer) ağlarda genellikle sınırlı bilgisayar birbirine bağlıdır. Bu bilgisayarlar seviye olarak aynıdır. Yani içlerinden birisinin ana bilgisayar olarak kullanılması söz konusu değildir . Bir bağlantı aracılığıyla isteyen kullanıcılar birbirleriyle iletişim kurar ya da dosya alıp gönderebilirler. Server-based (client/server) ağlarda bir ana makine vardır. Buna ana makine (dedicated server) denir. Ana makine üzerinde ağ yöneticiliği yapılır. Ayrıca ağa girecek (login) ya da bağlanacak herkes bu anabilgisayar üzerinde yer alan kullanıcı hesaplarına göre kontrol edilerek bağlantı gerçekleştirilir. Böylece kullanıcı ve dosya temelinde güvenlik sağlanmış olur. Bunun dışında kullanıcının girişinde kimlik bilgilerinin kontrolü (authentication) işlemi yapılmış olur. [4]



ŞEKİL 1.2 : PEER-TO-PEER (EŞLER ARASI) NETWORK.



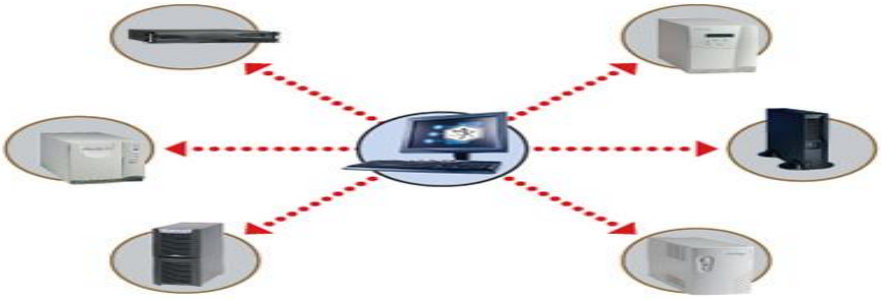
ŞEKİL 1.3 : SERVER-BASED (SUNUCU TABANLI) NETWORK.

1.3 BİLGİSAYAR AĞLARININ SINIFLANDIRILMASI

1.3.1 Yerel Bilgisayar Ağları (LAN, Local Area Networks)

[LAN] Local Area Network Yerel alan ağları (local area network) bilgisayar sistemlerinin belli bir çerçeve içerisinde, devlete veya özel bir kuruma ait resmi iletişim hatları kullanılmadan, kurum veya şahısların kendi imkânları ile tesis ettiği kablolu veya kablosuz birbirlerine bağlanması şeklinde oluşturulan ağ yapılarıdır.Bir ağ yapısının yerel alan ağı olabilmesi için ağ içerisinde bulunan bilgisayarların birbirlerine olan mesafeleri

dikkate alınmaz. Bazen bir yerleşke içerisinde 50 km mesafeye fiber optik kablolar yardımıyla hat çekilebilir ve bu hattı kurum ya da şahıs kendi imkanları içinde sağladığı ve bilgisayarın tanımlama numarasını aynı yönlendiriciden sağladığı için yapının adı yerel alan ağı olacaktır. Ancak birbirlerine çok yakın örneğin 50m. Mesafede olan fakat arasından sokak geçen iki binaya şahıs ya da kurumun kablo çekme yetkisi olmadığı için bağlantıyı sağlamak adına resmi iletişim kanalları kullanılmak zorunda kalınacak ve tanımlama numaraları farklı yönlendiricilerden verileceği için ağ yapısı geniş alan ağı olacaktır. Yerel ağlar yapılandırılırken kullanılan belli başlı topolojiler vardır. Bunlar yol (bus), halka (ring), yıldız(star) topolojileridir.[1]



ŞEKİL 2.1 : Örnek ağ yapısı

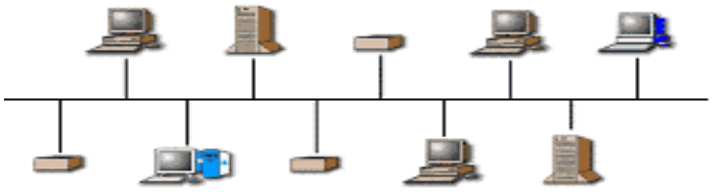
Yerel Alan Ağları bilgisayarlar, ethernet, ağ kabloları, ağ trafik kontrol cihazları ve diğer çevresel cihazlardan oluşmuştur. Bu gruba giren network'lerde bir ofis veya bir bina içersinde yazıcı, dosya ve program paylaşımı gibi işler kolaylıkla ve daha çabuk bir biçimde yapılabildiği gibi elektronik haberleşme dediğimiz e-posta ve video konferans uygulamaları da başarılı bir biçimde yerine getirilmektedir. Yerel Alan Ağları sınırlı mesafeler içersinde hizmet sunan hata olasılığı az olan hızlı network'lerdir. Bu network'ler kabaca veriyi, elektronik iletişimi ve bilgisayarların işlem gücünü birleştirir. [1]

1.3.2 LAN İletişim Metodları

3 ana kategori vardır.

- Unicast İletişim
- Multicast İletişim
- Broadcast İletişim

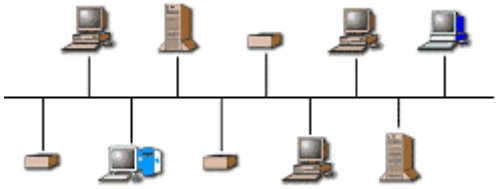
1.3.2.1 Unicast İletişim



Şekil 2.2 : Unicast İletişim

Tek bir veri paketinin, tek bir kaynaktan tek bir adrese gönderilmesiyle yapılan iletişime Unicast İletişim denir.[5]

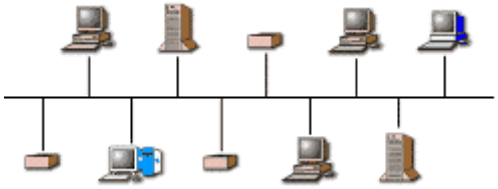
1.3.2.2 Multicast İletişim



Şekil 2.3. Multicast İletişim

Tek bir veri paketi, ağda kopyalanarak birkaç özel hedef adrese gönderilmişse, bu şekilde olan iletişime Multicast İletişim denir.[5]

1.3.2.3 Broadcast İletişim

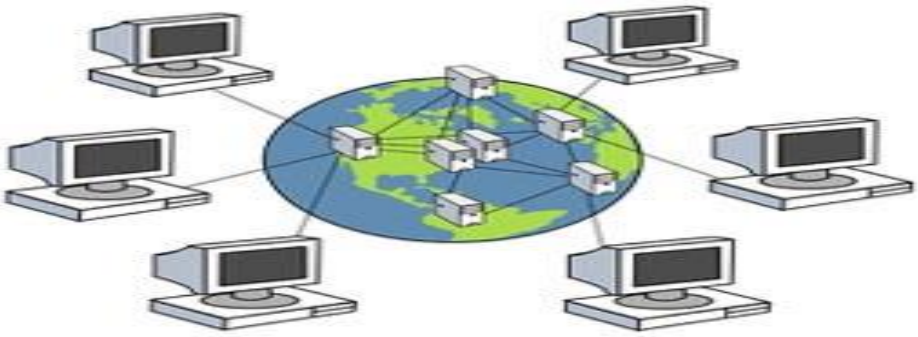


Şekil 2.4. Broadcast İletşim

Tek bir veri paketi, kopyalanarak ağda bulunan bütün bilgisayarlara gönderiliyorsa, bu tür iletişime Broadcast İletişim denir.[5]

1.3.3 Geniş Alan Bilgisayar Ağları (WAN, Wide Area Network)

Bir ülke ya da dünya çapında yüzlerce veya binlerce kilometre uzaklık arasında iletişimi sağlayan ağlardır. Coğrafi olarak birbirinden uzak yerlerdeki (şehirlerarası/ülkelerarası) bilgisayar sistemlerinin veya yerel bilgisayar ağlarının (LAN) birbirleri ile bağlanmasıyla oluşturulur. Genellikle kablo ya da uydular aracılığı ile uzak yerleşimlerle iletişimin kurulduğu bu ağlarda çok sayıda iş istasyonu kullanılır. WAN lar üzerinde on binlerce kullanıcı ve bilgisayar çalışabilir.

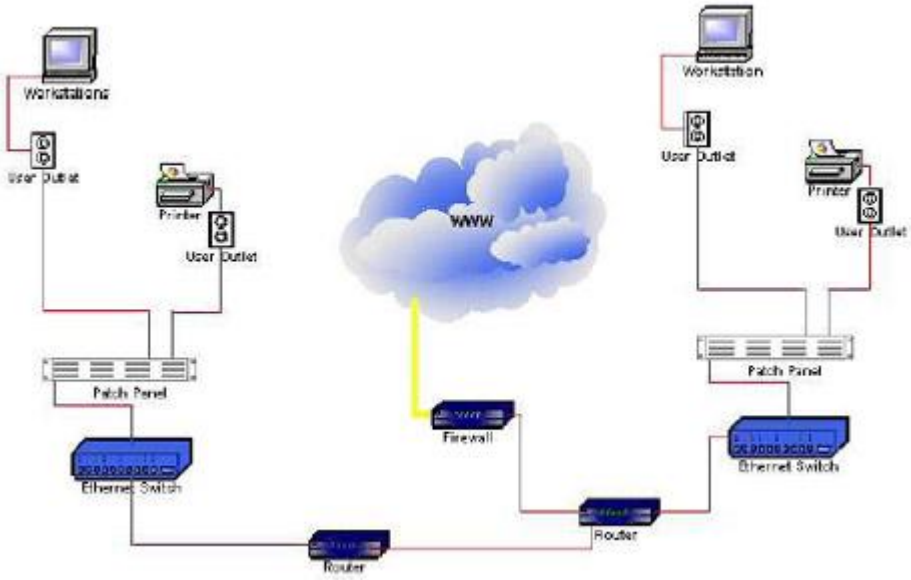


Şekil 2.5 : WAN

Şirketinizin Elazığ, Mersin ve Adana şubelerini bir WAN bağlantısı ile birleştirdiğinizde, Elazığ'da bulunsanız bile Adana'daki bir makineyi tıpkı önündeymiş gibi yönetebilirsiniz.[1]

1.3.4 Şehirsel Bilgisayar Ağları (MAN, Metropolitan Area Network)

LAN' ın kapsadığı alandan daha geniş, fakat WAN' ın kapsadığından daha dar mesafeler arası iletişimi sağlayan ağlardır. Genellikle belli bir şehirde ki bilgisayar sistemlerinin birbirleriyle bağlanmasıyla oluşturulur. [1]



Şekil 2.6 : MAN

1.4 AĞ TOPOLOJİLERİ

1.4.1 (Topology) nedir?

Her bilgisayar ağı verinin sistemler arasında gidip gelmesini sağlayacak bir yola ihtiyaç duyar. Aradaki bu yol çoğu zaman bir çeşit kablodur. Bununla beraber kablosuz çözümler alternatif olarak sunulmaya başlandı.. Ancak kablosuz çözümler henüz kabloya her noktada rakip olmaktan uzaktır. Belli bir sayının üstünde bilgisayar barındıran ağlarda alt yapı hala kablo şeklindedir. Topoloji değişik ağ teknolojilerinin yapısını ve çalışma şekillerini anlamada başlangıç noktasıdır.

Topoloji bilgisayarların birbirine nasıl bağlandığını ve nasıl iletişim kurduklarını anlatır.Topolojiyi anlamanın en kolay yolu iki farklı ve bağımsız bölüme ayırarak incelemektir:

1. Fiziksel Topoloji
2. Mantıksal Topoloji [6]

1.4.2 Fiziksel topoloji

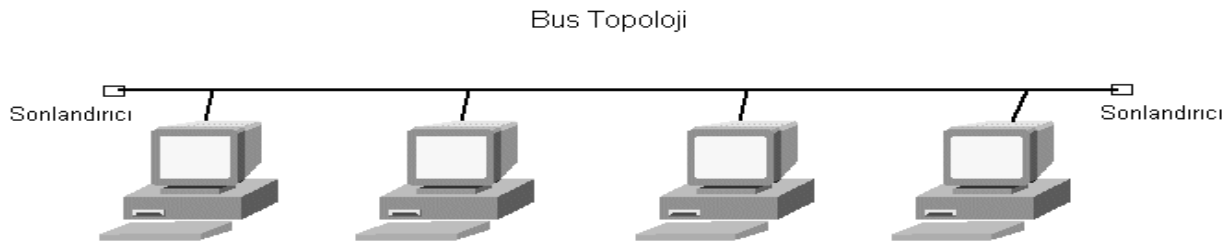
Aralarında ağ kurulu bir grup bilgisayara baktığımızda gördüğümüz şeydir. Yani kablo bilgisayarlar arasında nasıl dolaşıyor, bilgisayarlar birbirlerine nasıl bağlanmışlar gibi gözle görülen kısmı fiziksel topolojiyi belirler.[6]

1.4.3 Mantıksal topoloji

Kabloların bağlantı şeklinden ayrı olarak bilgisayar ağlarının veriyi nasıl gönderdiklerini açıklar. Topoloji aslında tek başına ağ ile alakalı bir çok konuyu açıklık getirmez. Örneğin kullanılan kablonun cinsi, maksimum uzunluğu, bilgisayarların kablonun kullanımda olup olmadığını nasıl tespit edecekleri gibi konular sadece topoloji ile tanımlanamaz. Ancak zaman içinde piyasa şartlarının da etkisi ile standartlar oluşmuştur. Değişik topolojileri kullanan değişik ağ sistemleri vardır. Bu teknolojiler Ethernet, Token Ring veya FDDI gibi isimlere sahiptir.
Her ağ teknolojisi kullandığı topolojiyle beraber, kullanılacak kablo tipi, maksimum uzunluk, bantgenişliği gibi konulara da açıklık getirir.[6]

1.5 Topoloji tipleri

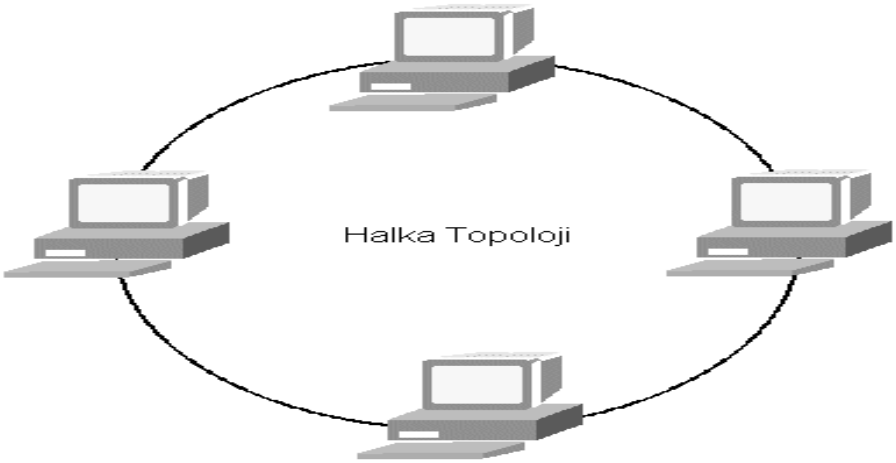
1.5.1 Bus topoloji



Şekil 3.1 : Bus topoloji

Fiziksel bus tüm bilgisayarların aynı kabloya bağlı oldukları topolojidir. Kablonun her iki ucuna sonlandırıcı adı verilen dirençler takılır. Bu topoloji hem mantıksal hem de fiziksel olarak varlığını sürdürmektedir. Kurulumu kolaydır. En büyük dezavantajı kablonun bir noktasında oluşan kopukluğun tüm sistemi yıkmasıdır.Mantıksal bus ise, gönderilen bir verinin tüm sistemlere de ulaşması demektir.[6]

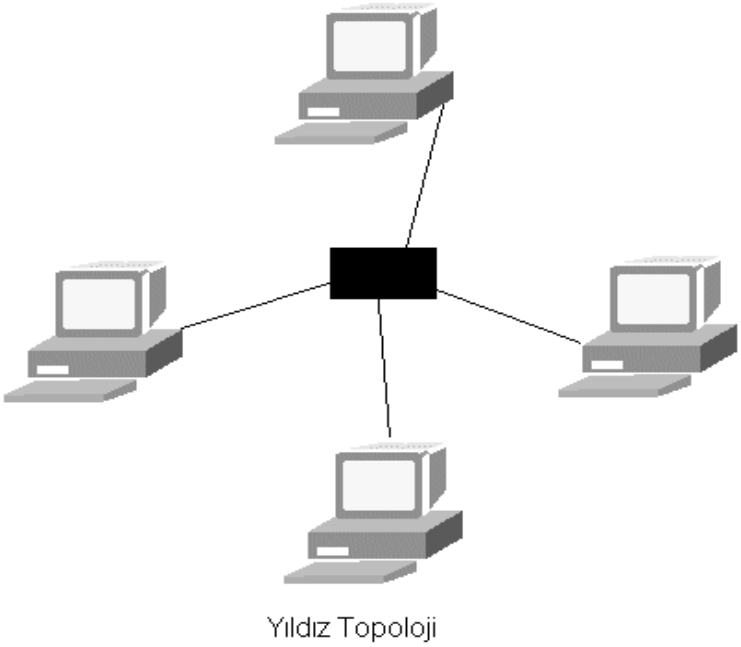
1.5.2 Halka(Ring) topoloji



Şekil 3.2 : Halka topoloji

Mantıksal Ring topoloji ise jeton-Ring adı verilen ilk başta IBM'in geliştirdiği, sonraları IEEE ve ISO tarafından geliştirilmeye devam eden ağ sisteminin kullandığı topolojidir.Jeton-Ring'de bilgisayarlar kablolarla merkez bir kutuya bağlıdır(fiziksel yıldız). Ancak sistemde veri aktarımını sağlayan bir sinyal sürekli olarak sırayla tüm sistemleri gezmektedir. Token adı verilen bu sinyal bir bir tüm sistemlere uğradığı için Ring/Halka ismi buradan gelmektedir.[6]

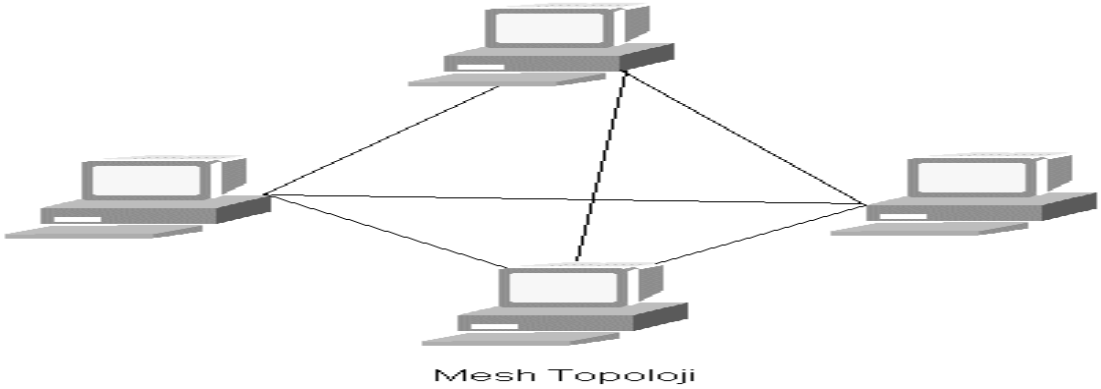
1.5.3 Yıldız(Star) topoloji



Şekil 3.3 : Yıldız topoloji

En yaygın kullanılan fiziksel topolojidir. Her bilgisayardan çıkan bir kablo merkezdeki bir kutuya (hub) girer. En büyük farkı bir kabloda oluşan problemin sadece o kabloya bağlı bilgisayarı etkilemesidir.Mantıksal yıldız topoloji yoktur.[6]

1.5.4 Mesh(ağ) topoloji



Şekil 1.5 : Mesh topoloji

Bu topolojide tüm bilgisayarlar diğer bilgisayarlara farklı bir kablo ile bağlıdır. Teorik olarak öne çıkan bağlantı şeklidir.Aradaki kablo miktarı bağlantı sayısı arttıkça katlanarak arttığı için gerçek hayatta sadece çok özel durumlarda ve az sayıda bilgisayar arasında kullanılır.[6]

1.5.5 Tree (Ağaç) topoloji:

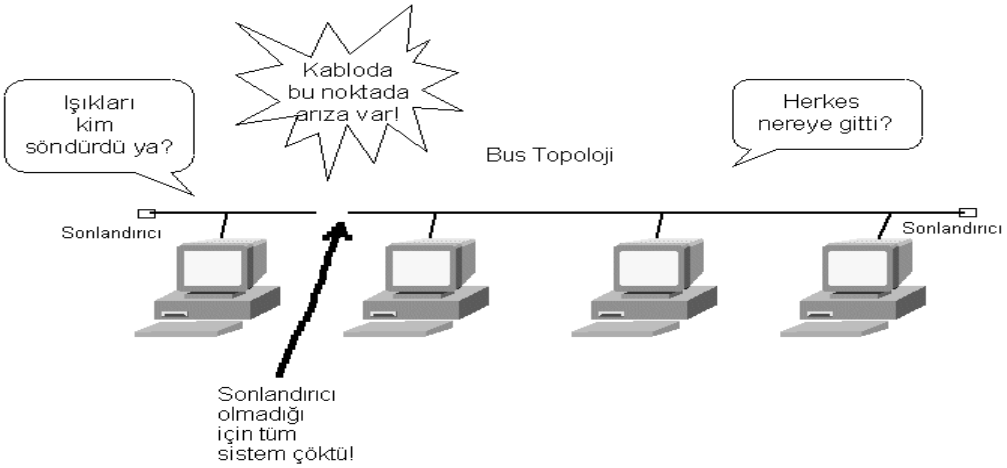
Temel olarak tıpkı doğrusal topoloji de ki gibi bağlantı noktalarından alınan ekler yöntemine göre çalışılmaktadır. Sadece ağaç topolojisi ağ bağlantıları için tercih edilmektedir. Daha çok ağaç ve doğrusal topolojisi birlikte kullanılır (BUS/TREE topoloji).[6]

1.5.6 Melez(Hybrid) topolojiler

Bu topolojileri sıfır noktası olarak alıp geliştirilen değişik ağ teknolojileridir. Jeton halka ve Ethernet protokolleri bu teknolojilerden sözünü etmeye değer ikisidir. Jeton halka bir ağ görme ihtimaliniz de çok az olduğu için onu bir kenara bırakırsak, elimizde sadece Ethernet protokolü kalır. Bugün "ağ oluşturuyorum" ya da "ağ kurduk " diyen birisi %100 Ethernet'ten bahsediyordur.

Ethernet ilk başta bus topoloji olarak tasarlandı. Koaksiyel bir kablo sırayla tüm bilgisayarları dolaşıyordu. Ethernet ağında bilgisayarlar bu kabloya bağlı olduklarını düşünürler. Bir diğer sisteme veri gönderdiklerinde, veri aslında aynı kabloya bağlı tüm sistemlere ulaşır. Tüm bilgisayarlardan sadece "doğru" olanı bu veriyi alır ve işler. Ethernet ağında her bilgisayar, daha doğrusu her ethernet farklı bir adrese sahiptir (MAC adresi). Veri kablo üzerine yerleştirilirken veri üzerine alıcı ve gönderenin MAC adresleri yazılır. Böylece veriyi alan tüm sistemlerden sadece "doğru" olanı veriyi alır ve işleme koyar, diğerleri kendilerine gelmeyen veriyi göz ardı eder.Bu noktada ilk ethernetin hem mantıksal, hem de fiziksel olarak bus yapıda çalıştığı anlaşılıyor

Zamanla fiziksel bus yapı ihtiyaçlara cevap veremez hale gelmiştir. Fiziksel bus yapıda, yani tüm bilgisayarların aynı kabloya bağlandıkları sistemde kablonun bir noktasında oluşan kopukluk veya kısa devre tüm ağı çökertir.



Şekil 1.6 : Bus topolojide kopma

Ağa yeni bir bilgisayar eklemek, kablonun bir bölümüne ek yapmak demektir bu işlem sırasında ağ çalışamaz vaziyettedir.

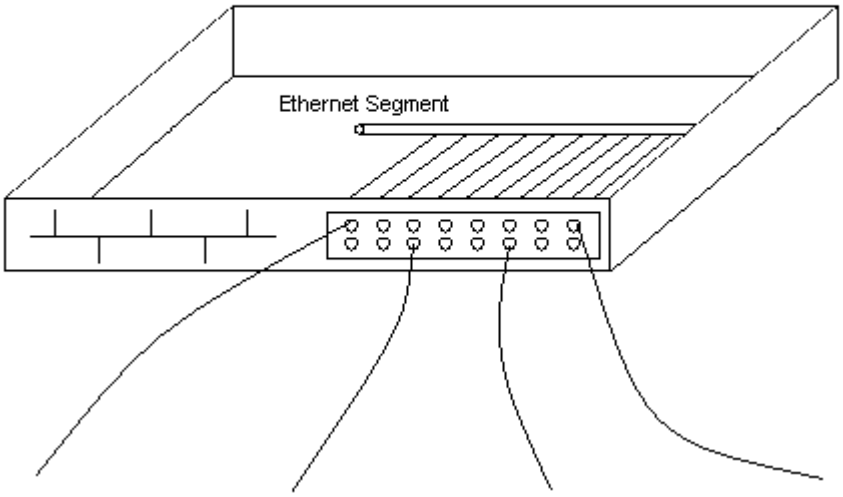
Ağ'da arıza olduğu zaman tüm sistemleri dolaşan tek bir kablonun herhangi bir yerindeki arızayı bulmak çok uğraştırıcıdır.

Yapısal kablolama dediğimiz, çok fazla sayıda bilgisayarın kullanıldığı yapılarda veya kampüsler de gerçekleştirilen kablolama ve kurulumlarda fiziksel bus yapı kullanmak olanaksızdır. Çünkü bus yapı ağacın dalları gibi merkezden binanın katlarına oradan da odalara dallanan bir yapıya izin vermez.

Sonuç itibariyle fiziksel bus topolojinin ihtiyaçları karşılamaktan uzak olduğu anlaşılıp yeni bir sistem arayışına gidildi. Çözüm ethernetin mantıksal topolojisini koruyup, fiziksel topolojiyi, yani kablolama yapısını yıldız topoloji ile değiştirmekti. Yıldız topolojide her bilgisayardan ayrı bir kablo merkezi bir hub a gider. Kablolardan birinde oluşan arıza sadece o bilgisayarı etkiler.

Ethernet için uygun fiziksel topoloji yıldız topolojidir. Kullanılan kablo da koaksiyelden UTP'ye dönüşmüştür. Ancak temelde ethernet hala bus topoloji kullanır. Böylece yıldız'a geçmeden önce kurulmuş binlerce ethernet ağı devre dışı kalmamış olur. Fiziksel yıldız topolojide kullanılan hub içinde mantıksal bir bus yapı vardır. Bilgisayarlardan birisinin yolladığı veri paketi hub'a ulaşınca, hub bu paketin kopyalarını oluşturup tüm portlarına yollar. Yani bus yapıda olduğu gibi data paketi diğer bütün bilgisayarlara erişir ve sadece alması gereken bu data paketini alır ve işler diğerleri ise siler.

Ethernet Hub'ın iç yapısı



Şekil 3.7

Bunu daha iyi anlamak için bir ethernet hub'ı yukarıdaki gibi sembolik olarak gösterebiliriz.
Hub'a bağlı bilgisayarlar yıldız topoloji kullanmalarına ragmen, hub içinde aynı bus gibi tek bir hat olduğunu düşünebiliriz.

Koaksiyel kablolu fiziksel bus ethernet ve utp kablolu fiziksel yildiz ethernet bir arada rahatça kullanılabilir. Çünkü çalışma mantıkları yani mantıksal topolojileri aynıdır.

Tümüyle ethernet hub'larda bir adet te koaksiyel kablo girişi vardır. Böylece fiziksel yıldıza geçiş ethernet için kolay olmuş, zaten en büyük ekonomik güce sahip ethernet

çeşitleri, fiziksel yıldızın tartışmasız avantajınıda ele geçirince,günümüzde en yaygın ağ teknolojisi haline gelmiştir.

Ethernetin kullandığı bu karma topoloji bazen yıldız-bus topoloji olarak anılır.Tek karma topoloji star-bus değildir. IBM'in geliştirdiği ve günümüzde prestijini kaybeden, ancak zamanında geniş bir kullanım alanı bulmuş olan jeton Ring ağ teknolojisi de yıldız-ring karma topolojisini kullanır. Bu sistemde de dışarıdan baktığımızda aynı ethernetin yıldız-bus'ı gibi kablolama yıldız şeklindedir. Her merkezden ayrı bir kablo ethernet'teki hub'ın benzeri bir kutuya girer. Ancak bu kutunun içinde jeton Ring ağlarının kullandığı mantıksal bir halka(ring) oluşum mevcuttur.[6]

1.6 AĞ KABLO TİPLERİ

Bilgisayarlar kablolarla birbirlerine bağlanırlar.Kablolama teknikleri ve kablo türleri çok çeşitlidir.

-Koaksiyel (Coaxial)

-Twisted-Pair

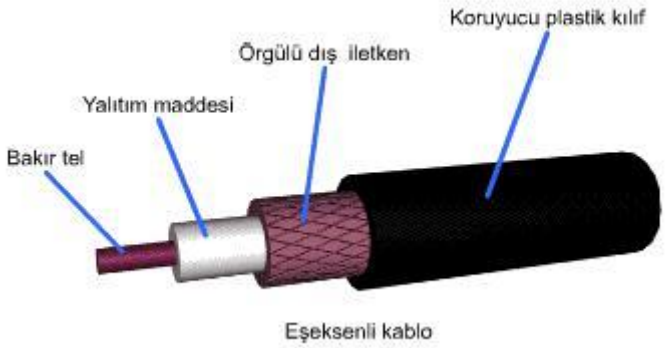
-UTP (Unshielded Twisted-Pair / Koruyucusuz Dolanmış-Çift)

-STP (Shielded Twisted-Pair / Koruyuculu Dolanmış-Çift)

-Fiber-Optik[7]

1.6.1 Koaksiyel Kablo (Coaxial Cable)

Koaksiyel (eş eksenli) kablolar genel olarak kullanılan ağ kablolarıdır. Bu kabloların genel olarak kullanılmasının başlıca nedenleri fiyatı uygunluğu, hafifliği, esnekliği ve kolay kullanımıdır. Bir koaksiyel kablo bir iletken metal telin önce plastik bir koruyucu ile, ardından bir metal örgü ve dış bir kaplamadan oluşur. Bu koruma katları iletilen verinin dış etkenlerden korunmasını sağlar. Koaksiyel kablonun içindeki tel iletken verileri oluşturan elektronik sinyallerin taşınmasını sağlar. İç tel genellikle bakırdır.



Şekil D.1 : Koaksiyel kablo yapısı

Koaksiyel kablonun iki tipi vardır:

-Thin (thinnet)

-Thick (thicknet)

Thinnet (ince) koaksiyel kablo .25 inç genişliğindedir. Yaygın olarak kullanılır. Verileri sağlıklı olarak 185 metre uzağa iletebilirler. Thinnet koaksiyel kablolar RG-58 standardı olarak değişik biçimde üretilmektedir. [7]

Kablo	Açıklama
RG-58 /U	Tekli bakır tel
RG-58 A/U	İpli tel
RG-58 C/U	RG-58 A/U'nun askeri amaçlısı
RG-59	Broadband iletim için (kablolu televizyon)
RG-6	Broadband iletim için
RG-62	ArcNet networkleri için

Tablo 1: Koaksiyel kablo tipleri

Thicknet ise daha kalın bir koaksiyel kablodur. Thicknet kablolar 0.5 inç kalınlığındadır. Bu yüzden thicknet kablolar daha uzun mesafe veri iletiminde kullanılırlar. 500 m mesafe için kullanılan thicknet koaksiyel kablolar tipik olarak thinnet networkler için bir backbone oluşturmada kullanılır.

Mesafe	Koaksiyel kablo
185 m	Thinnet
500 m	Thicknet

Tablo 2 : Koaksiyel kablo çeşitleri

Bir thinnet koaksiyel kabloyu thicknet kabloya bağlamak için ise transceiver denilen ara birim kullanılır. Transceiver'ın network adaptörüne bağlanması için AUI ya da DIX adı verilen çıkış kullanılır. AUI (Attachment Unit Interface) anlamındadır. DIX (Digital Intel Xerox) anlamına gelir.

Koaksiyel kabloların network adaptörüne bağlanması için, ayrıca iki kablonun birbirine eklenmesi için değişik birimler kullanılır. Bu birimler şunlardır:

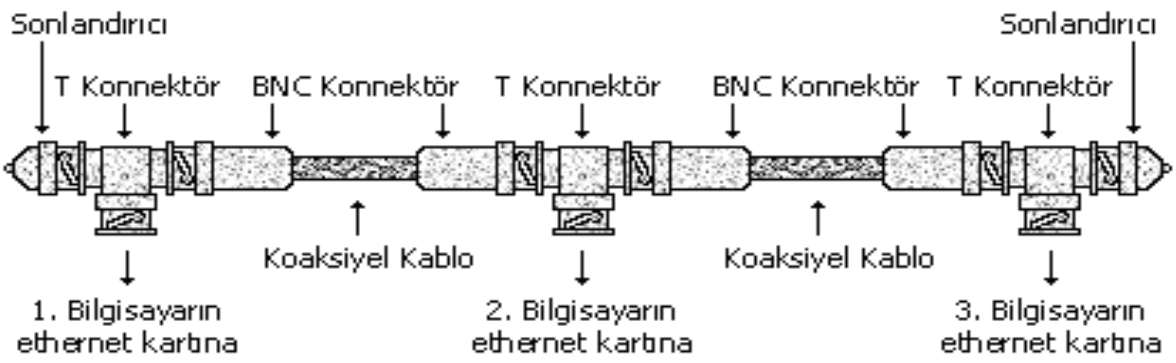
-BNC kablo konnektörü

-BNC T konnektör

-BNC Barrel konnektörü

-BNC Sonlandırıcı

BNC kablo konnektörü kablonun ucunda yer alır. T konnektör ise koaksiyel kabloyu network adaptörüne bağlamak için kullanılır. Barrel konnektör ise iki koaksiye kablonun birbirine bağlanmasını sağlar. Kablonun sonunda sonlandırıcılar yer alırlar.



Şekil 4.2 : BNC konnektör bağlantıları

Bus yerleşim biçiminde kurulan network'lerde kullanılan koaksiyel kablonun iki ucunda sonlandırıcı kullanılır. Bu sonlandırıcılar kablonun sonuna gelen sinyali yok ederler.**[7]**

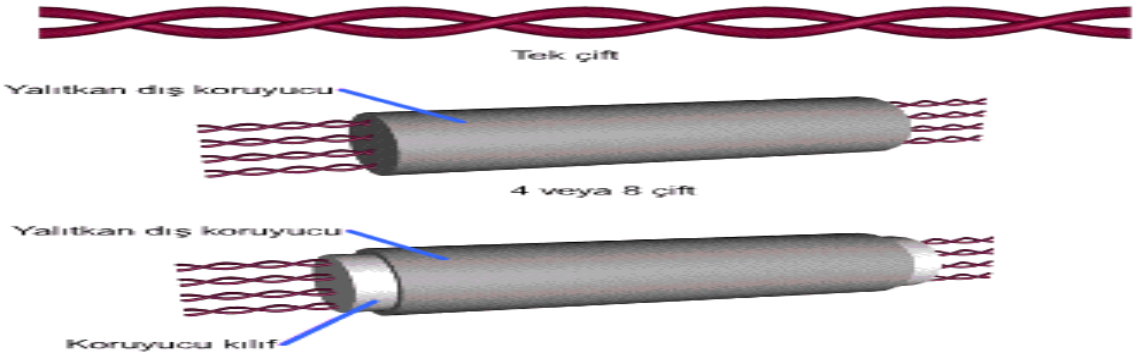
1.6.2 Dolanmış Çift Kablo (Twisted Pair Cable)

LAN'larda ve sınırlı veri iletiminde kullanılan bir diğer kablolama türü de twisted-pair kablolardır. Twisted-Pair (Dolanmış-çift) kablo iki telden oluşan bir kablodur. Twisted-pair kablolar iki türdür:

-UTP (Unshielded Twisted-Pair)

-STP (Shielded Twisted-Pair)

10BaseT network'lerde ve diğer LAN ortamlarında yaygın olarak UTP kablolar kullanılır. Maksimum UTP kablo uzunluğu 100 m dir. UTP kablo iki izoleli bakır kablodan oluşur.

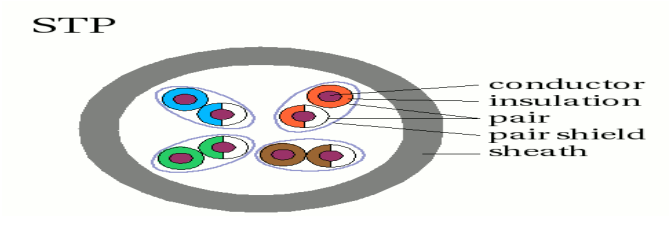


Şekil 1.4 : UTP kablo yapısı

İki tip TP kablo mevcuttur.[7]

1.6.3 Kaplamalı Dolanmış Çift (Shielded Twisted Pair-STP)

Bu tip kabloda dolanmış tel çiftleri koaksiyel kabloda olduğu gibi metal bir zırh ile kaplıdır.



Şekil D.4 : STP kablo yapısı

Kalkanlı çift bükümlü kablo kalkan, bozma ve bükümleme tekniklerinin bir karışımıdır. Her kablo çifti metal kılıf içerisine yerleştirilmiştir. Metal kılıf içerisine yerleştirilen dört çift kablonun tamamı ayrıca bir metal kılıf içine daha yerleştirilmiştir. 150 ohmluk bir kablodur. Ethernet ağlarında kullanılan STP, elektriksel alandan etkilenmezler. Örnek olarak elektromotor kuvvetin yaratmış olduğu elektromanyetik dalgalar veya radyo frekanslar ı verilebilinir. STP kablo her ne kadar dış etkenlerden daha az etkilense de UTP kablodan hem daha pahalı hem de kurulumu UTP' ye göre daha zor. [7]

1.6.4 Kaplamasız Dolanmış Çift (Unshielded Twisted Pair-UTP)

İşte geldik günümüzde tartışmasız en yaygın kullanılan ağ kablosuna.

Resim1 : Konnektör

Kalkansız bükümlü kablo çifti (UTP) bazı ağlarda kullanılan ve dört parçadan oluşan kablo çeşididir. UTP kablosunu oluşturan 8 tane kablodan her birinin etrafı bir yalıtkan malzemeyle kaplıdır. Buna ek olarak her kablo çifti diğer çift üzerine bükülüyor. Bu tip kablolarda EMI veya RFI dan kaynaklanan sinyal kesim etkileri basitçe önlenebiliyor. UTP kablolarının arasındaki sinyal kesimini azaltmak kabloların büküm sayısına bağlıdır. STP kablolarına benzer olarak UTP kablolarının da bir adımdaki büküm sayısı kablonun değişik özellikler sergilemesini sağlar.[7]

1.6.4.1 Kategoriler

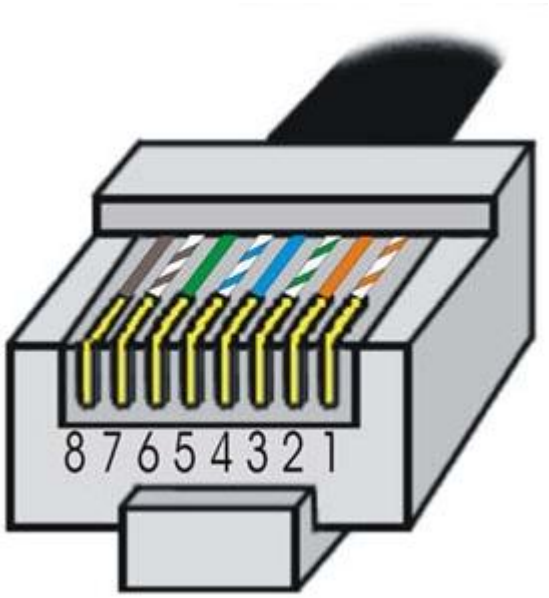
Kategori	Uygulama Alanı
1 (CAT1)	Yanlızca ses veri iletimi yapılmaz
2	Ses ve 1 Mbps' ye kadar veri iletimi.
3	Ses ve 10 Mbps' ye kadar veri iletimi.
4	Ses ve 20 Mbps' ye kadar veri iletimi
5	Ses ve 100 Mbps' ye kadar veri iletimi.
5e	Ses ve 622 Mbps' ye kadar veri iletimi.
6	Ses ve 1 Gps' ye kadar veri iletimi.
7	Ses ve 10 Gps' ye kadar veri iletimi.

Tablo 3: Kategoriler

Bilgisayar ağlarında önce 10 Mbit ethernet döneminde CAT3 kablo yoğun olarak kullanılmış, 100 Mbit ethernetin geliştirilmesiyle CAT5 kablolar üretilmeye başlanmış ve kullanılmaktadır. UTP kablolar dış görünüş olarak birbirine çok benzer. Ancak her kablonun üzerinde kategorisi yazmaktadır.

Resim 2 : Kategori

Kablonun kategorisi üretim kalitesiyle ilgilidir. Yapılan çeşitli testler ile kablonun belirtilen hızlarda elektrik sinyalini ne kadar sağlıklı ve az kayıpla iletebildiği, manyetik alan etkisine karşı sinyali ne kadar koruduğu ölçülür. Testler ile ortaya konan değerler kategorinin kriteridir. Bu kriterleri sağlayabilen kablo bu kategoriyi almaya hak kazanır. CAT5 ile 100 Mbit hızında veri aktarımı yapılabilir. Bir sonraki standart CAT5e (Enhanced CAT5, gelişmiş CAT5) standardıdır. Bu CAT5 ile aynı yapıda olup, daha üst seviye değerlere erişebilen bir kablodur. CAT5e ile gigabit hızına ulaşılabilir. Gigabit ethernet'te CAT5 kullanılabilmekle beraber CAT5e tavsiye edilir. CAT6'da da aynı durum söz konusu CAT5e'den de daha yüksek değerlere erişebilir. CAT6 şu anda 568A standardına eklenmiş kullanıma sunulmuştur. 1000Mhz hızı için, yani Gigabit ethernet için en uygun kablodur.



Şekil 4.5 : Cat5 yapısı

CAT7 henüz geliştirilme aşamasındadır. Diğerlerinin tersine farklı bir yapısı olacaktır. Her tel çifti metal folyo ile kaplı, hepsi birden diğer bir folyo ile kaplıdır. CAT7 RJ-45'ten tamamen farklı bir jak kullanacaktır.

UTP kablo ile ilgili bir diğer bir konu ise "stranded" ve "solid" kablo ayrımıdır. Yani çok damarlı veya tek damarlı kablo. Eğer mavi veya mavi-beyaz dediğimiz tel(veya diğerleri) tek parça bakır ise bu tek damarlıdır. Eğer ince-ince birden çok telden oluşmuşsa buna da çok damarlı diyoruz.[7]

1.6.5 Fiber Optik

Fiber kablolar iletişim teknolojisi dışında, farklı çeşitleri tıpta damarların içinin ve organların görüntülenmesi gibi görüntüleme sistemlerinde de oldukça popüler olarak kullanılmaktadır. [8]

1.6.5.1 Fiber Optik Kablonun Avantajları

- Geniş band aralığı
- Düşük kayıp
- Elektromagnetik bağışıklık
- Güvenilirlik
- Hafiflik
- Küçük boyut

Avantajlarına baktığımızda avantajların çoğunun iletişime yönelik olduğunu görürüz bu avantajlar yüzünden fiber özellikle uzak mesafe iletişimi için vazgeçilmezdir.Fiber en çok telefon iletişiminde kullanıldığına göre karşılaştırma tablosuna bakarsak; [8]

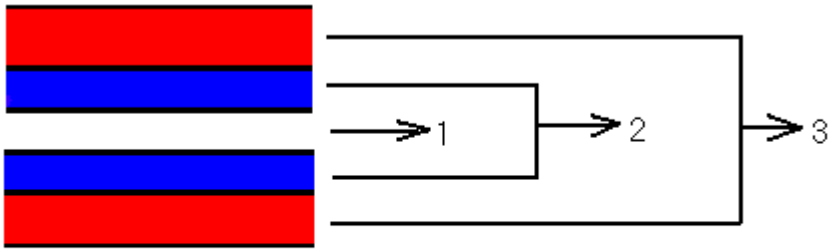
ORTAM	BİT ORANI(Mbps)	SES KANALI	TEKRARLAYICI BOŞLUGU (km)
KOAKSİYEL	1,5	24	1 - 2
	3,1	48	
	6,3	96	
	45	672	
	90	1344	
FİBEROPTİK	45	672	6-15 ÇOK MODLU
	90	1344	
	180	2688	30 –40 TEK MODLU
	405 – 435	6048	
	565	8064	
	1700	24192	

Tablo 4 : Kablo karşılaştırılması

1.6.5.2 Fiber Optik Kablonun Çalışması

Fiberin çalışma prensibi temel optik kurallarına dayanır. Bir ışın demeti az yoğun bir ortamdan daha yoğun bir ortama geçerken geliş açısına bağlı olarak yansıması ya da kırılarak ortam dışına çıkması mantığına dayanır.

Şimdi standart bir fiber kabloya bakalım. Kablo 3 kısımdan oluşur.



yukarıdaki şekil bir fiber kablonun yapısını gösterir 1 numaralı bölüm (beyaz) nuve 2 numaralı bolum (mavi) kılıf 3 numaralı bölüm (kırmızı) kaplamadır ve genelde plastiktir

Şekil 1.6 : Fiber optik kablo

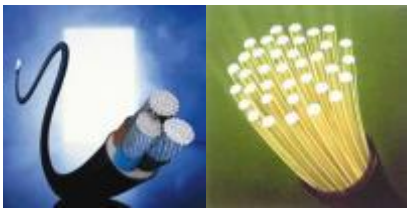
İndis: Bir ışık ışınının madde içersinde ilerlemesine gösterilen zorluk katsayısı

Kırılma İndisi: Işığın boşluktaki hızının madde içerisindeki ışık hızına oranına kırılma indisi denir.

Nüve: Işığın içerisinde ilerlediği ve kablonun merkezindeki kısımdır. Çok saf camdan yapılmıştır ve esnektir. Yani belirli sınırlar dahilinde eğilebilir cinsine göre çapı tek modlu veya çok modlu oluşuna göre 8 mikrometre ile 100 mikrometre arasında değişir

Kılıf: Tipik olarak 125 mikrometre çapında nüveyi saran ve fibere enjekte edilen ışının nüveden çıkmasını engelleyen kısımdır aynı nüve gibi camdan yapılmıştır ancak indis farkı olarak yaklaşık %1 oranında daha azdır bu indis farkından dolayı ışık ışını nüveye enjekte edildikten sonra kılıfa geçmez ışın kılıf nüve sınırından tekrar nüveye döner ve böyle yansımalar dizisi halinde nüve içerisinde ilerler.

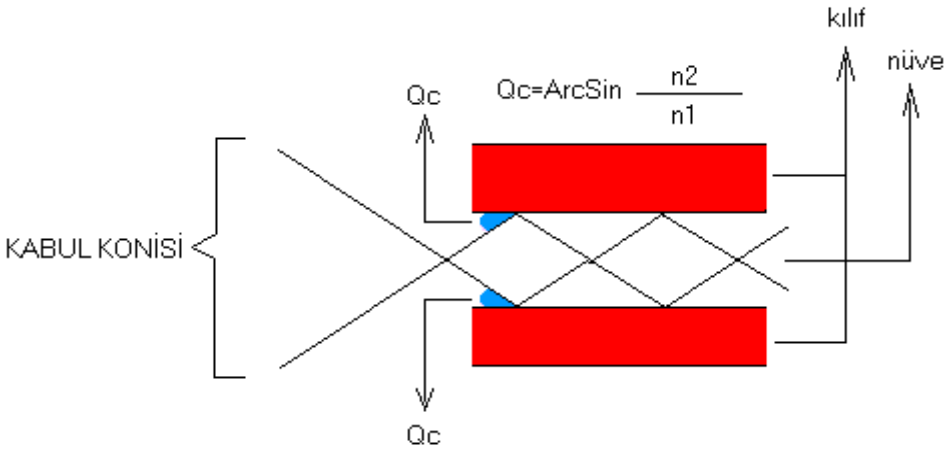
Kaplama: Optik bir özelliği olmayan kaplama polimer veya plastik olabilir bir veya birden fazla katmanı olabilir. Optik bir özelliği yoktur sadece fiberi darbe ve şoklardan korur.[9]



Resim 3 : Fiberoptik kablo çeşitlerinden bazıları

1.6.5.3 Işın Demetinin Fibere Enjekte Edilmesi

Gönderilecek ışın yada sinyal fiberin nüvesine enjekte edilir. Ancak fiber içerisinde kılıfa geçmemesi için belirli bir açı dahilinde nüveye girmeli ki nüve kılıf sınırından tam yansıma yapabilsin bu açıya kritik açı denir. Formüle edilmiş hali aşağıdadır.



Şekildeki kabul konisi olarak gösterdiğim bölüm kritik açının oluşturduğu ve tamamen fiber kablonun parametrelerine göre değişebilen bir konidir. 3 boyutlu düşünürsek daha kolay anlayabilirsiniz. Qc'yi göstermek için çizdiğim ışınlar gelebilecek en büyük ışın açısını

gösterir. Bu açılardan küçük gelen her ışın demeti fibere girer. Formüldeki n1 nüve n2 kılıf indisleridir.[9]

1.6.5.4 Fiber Optik Kablo Çeşitleri

1-Cam Fiberler: Nüvesi ve kılıfı camdan imal edilir. Veri iletimi açısından en iyi performansı gösterir. Yapımında kullanılan cam ultra saf silikon dioksit veya kuartz kristalidir. Yukarıda bahsettiğim indisi ayarlamak için; imalat aşamasında indisi azaltmak için, flor veya bor, indisi artırmak için, germanyum veya fosfor ile katkılanır.

2-Plastik Kaplı Silisyum Fiber: Cam nüveye plastik kılıfa sahiptirler. Ücret olarak cam fiberlere göre daha ucuz ama performans açısından daha verimsizdir.

3-Plastik Fiberler: En ucuz fiber tipidir. Nüvesi de kılıfı da plastiktir. Performansı en zayıf fiyatı en uygun fiberdir genelde kaplamaları yoktur. Kısa mesafe iletişimi için uygundur.[9]

1.6.6 Kablo türlerinin karşılaştırılması

Ethernet Adı	Kablo Tipi	Max. Veri Transfer Hızı	Max. Veri Transfer Uzaklığı	Açıklama
10Base5	Kalın Koaksiyel	10 Mbps	500 metre	BNC, T
10Base2	İnce Koaksiyel	10 Mbps	185 metre	BNC, T
10BaseT	UTP	10 Mbps	100 metre	RJ-45
100BaseT	UTP	100 Mbps	100 metre	RJ-45
1000BaseT	UTP	1000 Mbps	100 metre	RJ-45, CAT5 ve üstü
1000BaseTX (Gigabit Ethernet)	UTP	1000 Mbps	100 metre	RJ-45, CAT5 ve üstü
10BaseFL	Fiber (multimode)	10 Mbps	2000 metre	Ağlar arası, Fiber optik hub ve NIC arası bağlantı
100BaseFX	Fiber (multimode)	100 Mbps	2000 metre	100 Mbps Ethernet ağlarda
1000BaseSX	Fiber (multimode)	1000 Mbps	260 metre	SC, PC ve hub arası bağlantı için tasarlanmıştır.
1000BaseLX	Fiber (singlemode)	1000 Mbps	550 metre	1000BaseSX'in daha uzun mesafeler arası kullanması için, genellikle omurga olarak kullanılır.

Tablo 5 : Kablo türlerinin karşılaştırılması[7]

1.6.7 KAYNAKÇA

[1]
http://209.85.135.132/search?q=cache:J7p_3ePwLYJ:members.comu.edu.tr/boraugurlu/courses/bm109/content/week8/slayt8.pdf+bilgisayar+a%C4%9Flar%C4%B1&cd=14&hl=tr&ct=clnk&gl=tr&client=firefox-a

[2]

http://www.networkturk.net/cisco/band-genislig-i-nedir.html

[3]

http://www.webmastersitesi.com/webmaster-sozlugu/genisbant-nedir.23204

[4]

http://209.85.135.132/search?q=cache:R7RRnV2oV-wJ:akmyo.kocaeli.edu.tr/agbilesenleri.ppt+utp+kablolar&cd=23&hl=tr&ct=clnk&gl=tr&client=firefox-a

[5]

http://www.forumacil.com/network-ve-internet-forumu/27553-lan-karakteristikleri-ve-iletisim-metodlari.html

[6]

222967-topoloji-nedir.html

[7]

ag-kablo-cesitleri_37924331.html

[8]

w3.gazi.edu.tr/~sirin/kaynaklar/ppt/Ag/Donanim_kablo.ppt

[9]

http://www.nuveforum.net/attachments/21711d1238277908-fiber-optik-kablolar-zip

2 BÖLÜM

2.1 AĞ TEKNOLOJİLERİ

2.1.1 Ethernet Teknolojisi

Ethernet Carrier Sense Multiple Access With Collision Detection (CSMA/CD)'ı kullanan bir teknolojidir. CSMA/CD aynı anda iki makine ağa veri gönderdiğinde ağ aygıtlarının nasıl cevapvereceklerini belirleyen kurallardan oluşur. Ethernetler kabloları dinlerler ve kablo boş olduğunda veripaketlerini göndermeye başlarlar. Aynı anda başka bir makine de veri paketi yollarsa kabloda Collision olur. Ethernet bunu algılar ve veriyi tekrar gönderir.

2.1.2 Token-Ring Teknolojisi

Fiziksel olarak Star topolojisine benzer, Multistation Access Unit (MSAU) olarak adlandırılan hub'a bağlıdır. Mantıksal olarak halkaya benzer. Token-Ring ağlarında açılan ilk makine bir sinyal oluşturur. Ağdaki bir makine diğer bir makineye veri göndermek istediğinde ağda dolaşan bu sinyalin kendisine ulaşmasını bekler. Sinyal kendisine ulaştığında göndereceği bilgi paketini ve paketin ulaştırılacağı makinenin adresini sinyale ekler ve sinyali tekrar ağa bırakır. Veri paketi gideceği adrese ulaşana kadar ağdaki diğer makinelerle veri alış-verişi yapmaz. Sinyal veriyi ulaştırdıktan sonra tekrar ağda dolaşmaya başlar.

2.1.3 Asynchronous Transfer Mode (ATM) Teknolojisi

ATM (asynchronous transfer mode), bir paket anahtarlama teknolojisidir. ATM, verileri byte büyüklüğünde hücrelere (cell) ayırır ve aynı anda 53 hücrelik paketler halinde iletir. ATM, daha çok donanım tabanlıdır ve yüksek veri işleme/iletme hızları elde edilebilir. LAN ve WAN'ler arası haberleşmede kullanılır. Point To Point haberleşme metodunu kullanır. ATM Switch'ler arası bağlantı Fiber-Optic kablo ile yapılır. Böylece ATM'ler arası veri aktarımı hızlı ve güvenli olur. En çok kullanılan standart hızlar, 155 Mbps ve 622Mbps dir. 10Gbps hızlara kadar da çıkılmıştır (1996 sonu itibarıyla). ATM, BISDN protokolünün de en temel elemanıdır.

2.1.4 Fiber Distributed Data Interface (FDDI) Teknolojisi

FDDI çeşitli ağ tipleri arasında yüksek hızda haberleşme sağlar. FDDI Token-Ring teknolojisine benzer yapıdadır. FDDI'da iki adet halka vardır. Birincisi Primary Ring ikincisi Secondary Ring'dir. Primary Ring'de kablo kırılması gibi bir hata oluştuğunda halka kendini veri paketlerini Secondary Ring'e gönderecek şekilde yeniden tasarlar.

2.1.5 Frame Relay Teknolojisi

Frame Relay, verilerin çok yüksek hızlarda dijital ağlar üzerinden iletilmesini sağlayan bir teknolojidir. Veriler, "Frame" olarak adlandırılan paketler halinde iletilir. Frame Relay, veri aktarımı süresince, kesintisiz ve sadece o verinin iletileceği (dedicated) bağlantılar üzerinden yapılır. Buyüzden, ses ve normal data iletişiminde pek uygun olmadığını söyleyebiliriz. Frame Relay'de, iletilenpaketler için "iletim sırasında herhangi bir anda" hata kontrolü yapılmaz. Verinin iletileceği nokta hatakontrolünden sorumludur. Bunu sonucunda, paket iletim hızları çok yüksektir ve yaklaşık 1.5-2MBit/saniye mertebelerine çıkabilir.

Frame Relay LAN ve WAN'lar arası yüksek hızda haberleşme sağlar. Point To Point haberleşmemetodunu kullanır. Bağlantı kesintisiz ve sanal veri yolu üzerinde oluşur.

2.1.6 ISDN (Integrated Services Digital Network)

ISDN (Integrated Services Digital Network), özellikle normal telefon hatları (ve diğer bazı ortamlar) üzerinden daha yüksek hızlı entegre ses (analog) ve veri (dijital) aktarılmasını sağlayan bir dizi iletişim protokolüne verilen addır. ISDN'de, her iki uçta da, modemin dışında, bazı özel adaptörler kullanmak gerekir. Bu şekilde, 64kbps ve 128 kbps gibi hızlara (normal hatlar üzerinden) çıkmak münkün olmaktadır.

ISDN'de iki temel seviye hızı vardır : (1) Basic Rate (2) Primary Rate. Her iki seviyede de, iki farklı tip kanal bulunur : B (bearer) kanalları (sayıları birden çok olabilir) ve D (delta) kanalı (1 tane). B kanalları, her türlü ses, veri vb taşırlar. D kanalı ise iletişimde kullanılacak kontrol ve yönlendirme bilgilerini taşır. "Basic Rate" seviyesi daha çok evden kişisel kullanımlar ve küçük şirketlerin kullanımları için tasarlanmıştır ve iki tane 64Kbps B kanalı ile 1 tane 16Kbps D kanalı içerir. Ulaşılabilecek en yüksek hız 128 Kbps olmaktadır. "Primary Rate" seviyesi ise, daha yoğun kullanımlar için tasarlanmıştır ve 23 tane 64Kbps B kanalı (Avrupa için 30 tane) ve 1 tane 64Kbps D kanalı içerir. Ulaşılabilecek en yüksek hız ise yaklaşık 7 Mbps e kadar çıkar. Yeni geliştirilen BISDN (Broadband ISDN) teknolojisi ise, Frame Relay'a bir alternatif olarak düşünülebilir. ISDN kullanımı (özellikle evden kişisel bağlantılarda) artan oranlarda yaygınlaşmaya başlamıştır.

ISDN üzerinden video konferans sistemleri oldukça popüler uygulamalardır.

3 BÖLÜM

3.1 Ağ Nedir?

Farklı hizmet türleri sağlayan çok sayıda ağ tipi vardır. Sıradan bir günde, birisi telefon araması yapabilir, televizyon programı izleyebilir, radyo dinleyebilir, İnternet'te bir şeyler arayabilir ve hatta başka ülkedeki birisiyle video oyunu oynayabilir. Bu aktivitelerin tümü sağlam ve güvenilir ağlara dayanır. Ağlar, dünyanın neresinde olursa olsun kişi ve ekipmanları bağlama yeteneği sağlar. İnsanlar da ağların nasıl çalıştığını ve ağların var olmaması durumunda her şeyin nasıl olabileceğini düşünmeden ağları kullanır.

1990'lar ve öncesindeki iletişim teknolojisi, ses, video ve bilgisayar verilerinin iletişimleri için ayrı ve adanmış ağlar gerektiriyordu. Bu ağların her birine erişim için de farklı tipte bir aygıt gerekiyordu. Telefonlar, televizyonlar ve bilgisayarlar iletişim kurmak için belirli teknolojileri ve farklı adanmış ağ yapılarını kullanıyordu. Peki ya insanlar bu ağ hizmetlerinin tümüne aynı anda ve muhtemelen tek bir aygıt kullanarak erişmek isterlerse?

Yeni teknolojiler, tek bir hizmet tipinden fazlasını sunan yeni bir ağ çeşidi oluşturmuştur. Adanmış ağlardan farklı olarak bu yeni tümleşik ağlar, ses, video ve veri hizmetlerini aynı iletişim kanalı veya ağ yapısı üzerinden sunabilmektedir.

Günümüzde tümleşik bilgi ağlarının yeteneklerinden yararlanan yeni ürünler piyasaya giriyor. Şimdi insanlar bilgisayarlarında canlı video yayınlarını izleyebiliyor, İnternet üzerinden telefon araması yapabiliyor veya televizyonlarını kullanarak İnternet'te arama yapabiliyor. İşte bunların hepsi tümleşik ağlar sayesindedir.

3.1.1 Temel Ağ Bileşenleri

Kişisel bilgisayarlar, sunucular, ağ iletişim cihazları ve kablolar gibi, ağı oluşturan birçok bileşen vardır. Bu bileşenler dört ana kategoriye ayrılabilir:

- Konak Bilgisayarlar
- Paylaşılan çevresel aygıtlar
- Ağ iletişim cihazları
- Ağ iletişim ortamı

İnsanların en çok alışkın olduğu ağ bileşenleri konak bilgisayarlar ve paylaşılan çevresel aygıtlardır. Konak bilgisayarlar, doğrudan ağ üzerinden iletiler gönderip alan cihazlardır.

Paylaşılan çevresel aygıtlar ise doğrudan ağa bağlı olmayıp konak bilgisayarlara bağlıdır. Bu durumda konak bilgisayar da ağ üzerinde çevresel aygıtların paylaşımından sorumludur. Konak bilgisayarlarda, ağdaki kişilerin bağlı çevresel aygıtları kullanmasını sağlamak üzere yapılandırılmış bilgisayar yazılımı bulunur.Ağ iletişimi ortamları gibi, ağ cihazları da konak bilgisayarları birbirine bağlamak için kullanılır.

Bazı cihazlar bağlantı şekillerine göre birden çok rol oynayabilir. Örneğin, bir konak bilgisayara (yerel yazıcı) doğrudan bağlı bir yazıcı çevresel aygıttır. Doğrudan bir ağ cihazına bağlanarak doğrudan ağ iletişimine katılan bir yazıcı, konak bilgisayardır.

3.1.2 Bilgisayarın Ağdaki Rolleri

Bir ağa bağlı olup doğrudan ağ iletişimine katılan tüm bilgisayarlar konak bilgisayarlar olarak sınıflandırılır. Konak bilgisayarlar ağda iletiler gönderip alabilir. Modern ağlarda konak bilgisayarlar bir istemci, sunucu veya her ikisi olarak hareket edebilir. Bilgisayara yüklenen yazılım, söz konusu bilgisayarın oynayacağı rolleri belirler.

Sunucular, ağdaki diğer konak bilgisayarlara e-posta veya web sayfası gibi bilgileri sağlamalarına olanak veren yazılımların yüklü olduğu konak bilgisayarlardır. Her hizmet için ayrı bir sunucu yazılımı gerekir. Örneğin, bir konak bilgisayarın ağa web hizmetleri sağlaması için web sunucusu yazılımına ihtiyacı vardır.

İstemciler de, sunucudan alınan bilgileri istemesine ve görüntülemesine olanak veren yazılımların yüklü olduğu konak bilgisayarlardır. İstemci yazılımına örnek olarak, Internet Explorer gibi bir web tarayıcısı verilebilir.Sunucu yazılımı olan bir bilgisayar aynı anda bir veya birkaç istemciye hizmet sağlayabilir.

Ek olarak tek bir bilgisayar birden çok sunucu yazılımı tipini çalıştırabilir. Ev veya küçük bir işletmede bir bilgisayarın dosya sunucusu, web sunucusu ve e-posta sunucusu olarak hareket etmesi gerekebilir.

Tek bir bilgisayar birden çok istemci yazılımı tipini de çalıştırabilir. Gerekli her hizmet için istemci yazılımı olması gerekir. Birden çok istemci yüklüyken konak bilgisayar aynı anda birden çok sunucuya bağlanabilir. Örneğin, kullanıcı bir yandan anlık mesajlaşıp İnternet radyosunu dinlerken, diğer yandan e-postasını kontrol edip bir web sayfasını görüntüleyebilir.

3.1.3 Ağ Topolojileri

Birkaç bilgisayardan oluşan basit bir ağda, çeşitli bileşenlerin tamamının bağlanma şeklini görselleştirmek kolaydır. Ağ büyüdükçe, her bileşenin konumunu ve ağa bağlanma şeklini takip etmek daha da zorlaşır. Kablolu ağların tüm ağ konak bilgisayarlarına bağlantı sağlaması için çok sayıda kablo ve ağ cihazı gerekir.

Ağlar yüklendiğinde, her konak bilgisayarın bulunduğu yeri ve ağa bağlanma şeklini kaydetmek için fiziksel topoloji haritası oluşturulur. Fiziksel topoloji haritası aynı zamanda kabloların döşendiği yerleri ve konak bilgisayarlara bağlanan ağ iletişim cihazlarının konumlarını da gösterir. Topoloji haritasında gerçek fiziksel cihazları temsil etmek için simgeler kullanılır. Gelecekte yapılacak kurulum ve sorun giderme çalışmalarına yardımcı olması için fiziksel topoloji haritalarının korunması ve güncellenmesi çok önemlidir.

Fiziksel topoloji haritasına ek olarak bazen ağ topolojisinin mantıksal görünümünün de olması gerekir. Mantıksal topoloji haritası, konak bilgisayarları fiziksel olarak bulundukları yerleri dikkate almadan ağı kullanma şekillerine göre gruplandırır. Konak bilgisayar adları, adresleri, grup bilgileri ve uygulamalar mantıksal topoloji haritasına kaydedilebilir.

3.1.4 Kaynak Kanal Hedef

Tüm ağların birincil amacı, bilgiyi iletme yöntemi sağlamaktır. En eski ilkel insanlardan günümüzün en gelişmiş bilim adamlarına kadar, başkalarıyla bilgi paylaşımı insanlığın gelişiminde her zaman çok önemli olmuştur.

Bütün iletişimler, bir kişi veya cihazdan diğerine gönderilmesi gereken bir ileti ya da bilgiyle başlar. İletileri göndermek, almak ve yorumlamak için kullanılan yöntemler, teknoloji geliştikçe değişime uğrar.

Ancak tüm iletişim yöntemlerinin üç ortak öğesi vardır. Bu öğelerden birincisi, ileti kaynağı veya gönderendir. İleti kaynakları, bir iletiyi başka kişi veya cihazlara iletmesi gereken kişiler veya elektronik cihazlardır. İletişimin ikinci öğesi, iletinin hedefi veya alıcıdır. Hedef, iletiyi alır ve yorumlar. Üçüncü öğe de kanal olarak adlandırılır ve iletinin kaynaktan hedefe gidebileceği yolu sağlar.

3.1.5 İletişim Kuralları

İki kişi arasındaki tüm iletişimlerde, iletinin başarıyla iletilip anlaşılmasını sağlamak için her iki kişinin de uyması gereken birçok kural veya protokol vardır. İnsanların başarıyla iletişim kurmasını sağlayan protokoller arasında şunlar bulunur:

- Gönderenin ve alıcının tanımlanması
- İki tarafın da kabul ettiği bir ortam veya kanal (yüz yüze, telefon, mektup, fotoğraf)
- Uygun iletişim kipi (sözlü, yazılı, görsel, etkileşimli veya tek yönlü)
- Ortak dil
- Dilbilgisi ve cümle yapısı
- İletim hızı ve zamanlaması

İnsanların birbiriyle iletişimini belirleyen herhangi bir protokol veya kuralın olmaması durumunda neler olacağını düşünün. İnsanları anlayabilir miydiniz? Yaygın olarak kabul edilmiş protokollere uymayan bir paragrafı okuyabilir miydiniz?

Protokoller, ileti kaynağının, kanalının ve hedefinin özelliklerine özgüdür. Bir ortam (örn. telefon görüşmesi) üzerinden iletişim kurmakta kullanılan kurallar, başka bir ortam (örn. mektup) üzerinden iletişim kurmakta kullanılan kurallarla aynı olmak zorunda değildir.

Protokoller, iletinin iletilme ve teslim edilme şeklinin ayrıntılarını tanımlar. Bu ayrıntılardan bazıları şunlardır:

- İleti biçimi
- İleti boyutu
- Zamanlama
- Kapsülleme
- Kodlama
- Standart ileti düzeni

İnsanların iletişimini güvenilir ve anlaşılabilir hale getiren kavram ve kuralların çoğu bilgisayar iletişimi için de geçerlidir.

3.1.6 İleti Kodlama

İletiyi göndermenin ilk adımlarından biri iletiyi kodlamaktır. Yazılı sözcükler, resimler ve konuşulan dillerin hepsi, paylaşılan düşünceleri ifade etmek için benzersiz kodlar, sesler, hareketler ve/veya simgeler kümesi kullanır. Kodlama, düşünceleri iletmek için dil, simge veya seslere dönüştürme işlemidir. Kod çözme ise, düşünceyi yorumlamak için bu işlemin tersini gerçekleştirmektir.

Güneşin batışını izleyip daha sonra güneşin batışının ne kadar güzel olduğunu anlatmak için telefonla başkasını arayan bir kişiyi düşünün. Gönderenin iletiyi iletmek için öncelikle güneşin batışı hakkındaki düşünce ve algılarını sözcüklere dönüştürmesi veya kodlaması gerekir. Sözcükler, iletinin aktarılması için kullanılan dilin ses ve tonlamaları kullanılarak telefona söylenir. Telefon hattının diğer ucunda açıklamayı dinleyen kişi, gönderenin açıkladığı güneşin batışı görünümünü aklında görselleştirmek için sesleri alır ve seslerin kodunu çözer.

Bilgisayar iletişiminde de kodlama gerçekleşir. Konak bilgisayarlar arasındaki kodlama, ortama uygun biçimde olmalıdır. Ağ üzerinden gönderilen iletiler ilk olarak,

gönderen konak bilgisayar tarafından bit'lere dönüştürülür. Her bit, iletildiği ağ ortamına bağlı olarak ses, ışık dalgası veya elektrik darbesi düzenine kodlanır. Hedef konak bilgisayar, iletiyi yorumlamak için sinyalleri alır ve sinyallerin kodunu çözer.

3.1.7 İleti Biçimlendirme

Bir ileti, kaynaktan hedefe gönderilirken belirli bir biçim veya yapıyı kullanmalıdır. İleti biçimleri, iletinin tipine ve iletiyi teslim etmek için kullanılan kanala bağlıdır.

Mektup yazmak, insanların kullandığı en yaygın yazılı iletişim biçimlerinden biridir. Kişisel mektup yazmaya yönelik kabul görmüş biçim yüzyıllardır değişmemiştir. Birçok kültürde kişisel mektup aşağıdaki öğeleri içerir:

- Alıcı tanımlayıcısı
- Selamlama
- İleti içeriği
- Kapanış sözü
- Gönderen tanımlayıcısı

Doğru biçim kullanımının yanı sıra, kişisel mektupların çoğunun teslim edilmesi için bir zarfa koyulması veya kapsüllenmesi gerekir. Zarfın üzerinde uygun yerlerde gönderenin ve alıcının adresi bulunur. Hedefin adresi ve biçimlendirmesi doğru olmazsa, mektup teslim edilmez.

Bir ileti biçiminin (mektup) başka bir ileti biçimine (zarf) yerleştirilmesi işlemine kapsülleme denir. Alıcı tarafından bu işlemin tersi gerçekleştirilip mektup zarftan çıkarıldığında, kapsül açma işlemi gerçekleşir.

Mektup yazan kişi, mektubun alıcıya teslim edilmesini ve anlaşılmasını sağlamak için kabul edilen bir biçim kullanır. Aynı şekilde, bilgisayar ağı üzerinden gönderilen bir ileti de teslim edilip işlenmesi için belirli biçim kurallarını izler. Mektubun teslim edilmesi için zarfa koyulması gibi, bilgisayar iletileri de kapsüllenir. Her bilgisayar iletisi, ağ üzerinden gönderilmeden önce çerçeve adı verilen belirli bir biçime kapsüllenir. Çerçeve tıpkı bir zarf gibi hareket eder; amaçlanan hedefin adresini ve kaynak konak bilgisayarın adresini sağlar. Çerçevenin biçim ve içeriklerini, gönderilen iletinin tipi ve iletinin iletildiği kanal belirler. Doğru şekilde biçimlendirilmemiş iletiler hedef konak bilgisayara teslim edilmez veya hedef konak bilgisayar tarafından işlenmez.

3.1.8 İleti Boyutu

İnsanlar birbiriyle iletişim kurarken, gönderdikleri iletiler genellikle küçük bölümlere veya cümlelere ayrılır. Bu cümleler, alıcı kişinin bir defada işleyebileceği boyutla sınırlandırılır. İletinin her bölümünün alınıp anlaşılmasını sağlamak için tek bir konuşma birçok küçük cümleden oluşabilir.

Benzer şekilde, bir konak bilgisayardan diğerine ağ üzerinden uzun bir ileti gönderilirken, iletilerin küçük bölümlere ayrılması gerekir. Ağ üzerinden iletilen bölümlerin veya çerçevelerin boyutunu belirleyen kurallar oldukça sıkıdır. Bu kurallar, kullanılan kanala bağlı olarak farklılık da gösterebilir. Çok uzun veya çok kısa olan çerçeveler teslim edilmez.

Çerçevelerin boyut kısıtlaması, kaynak konak bilgisayarın uzun bir iletiyi hem minimum hem de maksimum boyut gereksinimlerine uygun olacak şekilde ayrı bölümlere ayırmasını gerektirir. Her bölüm, adres bilgileriyle ayrı bir çerçeveye kapsüllenir ve ağ üzerinden gönderilir. Alıcı konak bilgisayarda iletilere kapsül açma işlemi uygulanır ve iletiler işlenip yorumlanması için yeniden bir araya getirilir.

3.1.9 İleti Zamanlama

İletinin doğru şekilde alınıp anlaşılmasını etkileyen faktörlerden biri de zamanlamadır. İnsanlar, konuşma zamanlarını, hızlarını ve yanıt bekleme sürelerini belirlemek için zamanlamayı kullanır. Bunlar iletişimde belirleyici olan kurallardır.

3.1.10 Erişim Yöntemi

Erişim Yöntemi, kişinin ileti gönderebileceği zamanı belirler. Bu zamanlama kuralları, ortamı temel alır. Örneğin, ne zaman söyleyecek bir şeyiniz olduğunda konuşabilirsiniz. Bu ortamda, bir kişi konuşmadan önce herkesin susmasını beklemelidir. İki kişi aynı anda konuşursa, bilgi çatışması oluşur ve bu durumda iki kişinin de susup yeniden başlaması gerekir. Bu kurallar iletişimin başarılı olmasını sağlar. Benzer şekilde, bilgisayarların da bir erişim yöntemini tanımlaması gerekir. Ağdaki konak bilgisayarların, ileti göndermeye başlayacakları zamanı ve hata oluşunca nasıl yanıt vereceklerini bilmesi için bir erişim yöntemine ihtiyaçları vardır.

3.1.11 Akış Denetimi

Zamanlama, gönderilebilecek bilgi miktarını ve bilginin teslim edilme hızını da etkiler. Birisi çok hızlı konuşursa, diğer kişinin iletiyi duyup anlaması zorlaşır. Alıcı kişinin gönderenden yavaş konuşmasını istemesi gerekir. Ağ iletişiminde, gönderen konak bilgisayar iletileri hedef konak bilgisayarın alıp işleyebileceği düzeyden daha yüksek hızda iletebilir. Kaynak ve hedef konak bilgisayarlar, başarılı iletişim için doğru zamanlama üzerinde anlaşmak üzere akış denetimini kullanır.

3.1.12 Yanıt Zaman Aşımı

Birisi bir soru sorup kabul edilebilir süre içinde bir yanıt alamazsa, söz konusu kişi yanıt gelmediğini varsayarak ona göre hareket eder. Bu durumda kişi soruyu tekrar sorabilir veya konuşmaya devam edebilir. Ağdaki konak bilgisayarların da yanıt bekleme sürelerini ve yanıtın zaman aşımına uğraması durumunda uygulanacak eylemi belirten kuralları vardır.

3.1.13 İleti düzenleri

Bazen birisi tek bir kişiye bilgi iletmek ister. Başka zaman ise kişinin aynı anda bir grup insana hatta aynı alanda bulunan tüm insanlara bilgi göndermesi gerekebilir. İki kişi arasındaki konuşma, bire bir iletişim düzenine örnektir. Bir grup alıcının aynı anda aynı iletiyi alması gerektiğinde, birden fazlasıyla veya birden tümüne ileti düzeni gereklidir.

İleti gönderenin, iletinin hedefe başarıyla teslim edildiğinden emin olması gerektiği zamanlar da vardır. Bu tür durumlarda, alıcının gönderene alındı bildirimi göndermesi gerekir. Alındı bildirimi gerektirmeyen ileti düzeni, alındı bildirimi yapılmamış olarak ifade edilir.Ağdaki konak bilgisayarlar da iletişim kurmak için benzer ileti düzenlerini kullanır. Bire bir ileti düzenine tekli yayın denir, bu ifade ileti için yalnızca bir hedef olduğunu belirtir.

Konak bilgisayarın birden fazlasıyla düzenini kullanması gerektiği zamanlarda bu düzene çoklu yayın denir. Çoklu yayın, bir iletinin aynı anda bir konak bilgisayar hedefleri grubuna teslim edilmesini ifade eder.

Ağdaki tüm konak bilgisayarların aynı anda ileti alması gerekiyorsa, yayın düzeni kullanılır. Yayın, birden tümüne ileti düzenini temsil eder. Ayrıca, konak bilgisayarlar alındı bildirimi yapılmış ve alındı bildirimi yapılmamış iletilerini gerektirir.

3.1.14 İletişimde Protokol Kullanımı

İnsanların ve bilgisayarların kullandığı tüm iletişimler, önceden belirlenmiş kurallar veya protokollerle yönetilir. Bu protokolleri kaynağın, kanalın ve hedefin özellikleri belirler. Protokoller, kaynak, kanal ve hedefi temel alarak ileti biçimi, ileti boyutu, zamanlama, kapsülleme, kodlama ve standart ileti düzeni konularının ayrıntılarını tanımlar.

3.1.15 Protokollerin Önemi

Bilgisayarlar da tıpkı insanlar gibi iletişim kurmak için kurallar ve protokoller kullanır. Özellikle yerel ağda protokoller çok önemlidir. Kablolu bir ortamda, yerel ağ tüm konak bilgisayarların "aynı dili konuşması" gerektiği veya bilgisayar terimleriyle açıklamak gerekirse, "ortak bir protokolü paylaşması" gerektiği bir alan olarak tanımlanır.

Aynı odadaki herkes farklı bir dil konuşursa, iletişim kuramazlar. Benzer şekilde, yerel ağdaki cihazlar aynı protokolleri kullanmazsa, onlar da iletişim kuramazlar.

Yerel kablolu ağlarda kullanılan en yaygın protokol kümesi, Ethernet'tir. Ethernet protokolü, yerel ağ üzerinde iletişimin birçok yönünü tanımlar, bunlardan bazıları şunlardır: ileti biçimi, ileti boyutu, zamanlama, kodlama ve ileti düzenleri.

3.1.16 Protokollerin Standartlaşması

Ağ iletişiminin kullanıldığı ilk zamanlarda her satıcı, ağ cihazlarını ve ağ iletişim protokollerini birbirine bağlamak için kendilerine ait ve kendilerine özgü yöntemleri kullanırdı. Bir satıcının ekipmanı, diğer satıcının ekipmanıyla iletişim kuramazdı.

Ağlar yaygınlaşmaya başladıkça, farklı satıcıların ağ ekipmanlarının çalıştırılacağı kuralları tanımlayan standartlar geliştirildi. Standartlar ağ iletişimine birçok şekilde yarar sağlar:

- Tasarımı kolaylaştırır.
- Ürün gelişimini basitleştirir.
- Rekabeti artırır.
- Tutarlı ara bağlantılar sağlar.
- Eğitimi kolaylaştırır.
- Müşteriler için daha fazla satıcı seçeneği sunar.

Resmi bir yerel ağ iletişimi standart protokolü yoktur ancak zamanla bir teknoloji (Ethernet) diğerleri arasında daha yaygın hale gelmiştir. Diğer bir deyişle Ethernet fiili standart haline gelmiştir.

Elektrik Elektronik Mühendisleri Enstitüsü veya IEEE, Ethernet ve kablosuz bağlantı standartları gibi ağ iletişim standartlarını korur. IEEE komiteleri, bağlantı standartlarının, ortam gereksinimlerinin ve iletişim protokollerinin onaylanmasından ve korunmasından sorumludur. Her teknoloji standardına, o standardı onaylamak ve korumaktan sorumlu komiteyi ifade eden bir numara atanır. Ethernet standartlarından sorumlu komite 802.3'tür.

1973'te Ethernet'in oluşturulmasından bu yana, daha hızlı ve daha esnek sürümlerini belirtmek için standartlar geliştirilmiştir. Ethernet'in bu kadar yaygın kullanılmasının en önemli nedenlerinden biri de bu zamanla gelişme yeteneğidir. Ethernet'in her sürümünün ilişkilendirilmiş bir standardı vardır. Örneğin, 802.3 100BASE-T, büklümlü çift kablo standartlarını kullanan 100 Megabit Ethernet'i temsil eder. Bu standart gösterimi şu şekilde yorumlanır:

- 100, Mbps cinsinden hızdır
- BASE, temel bant iletimini ifade eder
- T, kablo tipini ifade eder, bu örnekteki kablo tipi büklümlü çifttir.

Ethernet'in önceki sürümleri 10 Mbps'de nispeten daha yavaştı. En yeni Ethernet sürümleri, saniye başına 10 Gigabit veya daha yüksek hızda çalışmaktadır. Bu yeni sürümlerin özgün Ethernet ağlarından ne kadar daha hızlı olduğunu düşünün.

3.1.17 Fiziksel Adresleme

Tüm iletişimler, kaynak ve hedefi tanımlama yolunu gerektirir. İnsanların iletişiminde kaynak ve hedef, isimlerle temsil edilir.

Bir isim söylendiğinde, o isme sahip kişi iletiyi dinler ve yanıtlar. Odadaki diğer kişiler iletiyi duysalar da kendilerine yöneltilmediği için yok sayarlar.

Ethernet ağlarında da kaynak ve hedef konak bilgisayarları tanımlamak için benzer bir yöntem kullanılır. Konak bilgisayarın ağda tanımlanmasını sağlamak için Ethernet ağına bağlı her konak bilgisayara bir fiziksel adres atanır. Her Ethernet ağ arayüzüne üretim aşamasında bir fiziksel adres atanır. Bu adres, Ortam Erişim Denetimi (MAC) adresi olarak bilinir. MAC adresi, ağdaki kaynakları ve hedef konak bilgisayarları tek tek tanımlar.

Ethernet ağları kablo tabanlıdır, diğer bir deyişle, bakır veya fiber optik bir kablo konak bilgisayarları ve ağ iletişim cihazlarını bağlar. Konak bilgisayarlar arasında iletişimi sağlamak için kullanılan kanal budur.

Ethernet ağındaki bir konak bilgisayar iletişime geçtiğinde, amaçlanan alıcının MAC adresini ve kaynak olarak kendi MAC adresini içeren çerçeveleri gönderir. Çerçeveyi alan konak bilgisayar, çerçevenin kodunu çözer ve hedef MAC adresini okur. Hedef MAC adresi, NIC'de (Ağ Ara yüz Kartı) yapılandırılmış adresle aynıysa, NIC iletiyi işler ve konak bilgisayar uygulamasının kullanması için saklar. Hedef MAC adresi, konak bilgisayar MAC adresiyle aynı değilse, NIC iletiyi yok sayar.

3.2 Ethernet İletişimi

Ethernet protokolü standartları, çerçeve biçimi, çerçeve boyutu, zamanlama ve kodlama gibi ağ iletişiminin birçok yönünü tanımlar.

Bir Ethernet ağında konak bilgisayarlar arasında iletiler gönderilirken, konak bilgisayarlar standartların belirttiği çerçeve düzenine göre iletileri biçimlendirir. Çerçevelere Protokol Veri Birimleri (PDU) de denir.

Ethernet çerçevelerinin biçimi, hedef ve kaynak MAC adreslerinin konumunu ve aşağıda örnekleri yer alan ek bilgileri belirtir:

- Sıralama ve zamanlama için başlama eki
- Çerçeve sınırlayıcının başlangıcı
- Çerçeve uzunluğu ve tipi
- İletim hatalarını algılamak için çerçeve kontrolü sırası

Ethernet çerçevelerinin boyutu, maksimum 1518 bayt ve minimum 64 bayt olarak sınırlandırılmıştır. Bu sınırlamalara uymayan çerçeveler alıcı konak bilgisayar tarafından işlenmez. Ethernet standartları, çerçeve biçimleri, boyutları ve zamanlamasına ek olarak çerçeveleri oluşturan bit'lerin kanalda kodlandırılma şeklini de tanımlar. Bit'ler bakır kablolardan elektrik darbeleri olarak veya fiber optik kablolardan ışık darbeleri olarak iletilir.

3.2.1 Ethernet Ağlarının Hiyerarşik Tasarımı

Ağ iletişiminde, cihazları katmanlı bir yaklaşımla düzenlenmiş birden çok ağ şeklinde gruplandırmak için hiyerarşik tasarım kullanılır. Bu tasarımda, yerel trafiğin yerel kalmasını sağlayan küçük ve daha yönetilebilir gruplar bulunur. Yalnızca diğer ağları hedefleyen trafik daha yüksek bir katmana taşınır.

Hiyerarşik ve katmanlı tasarım, verimliliğin artmasını, işlevin en iyi duruma getirilmesini ve hızın yükselmesini sağlar. Var olan ağların başarımı etkilenmeden ek yerel ağlar eklenebildiği için, bu tasarım ağın gerektiği şekilde ölçeklendirilmesini de sağlar.

Hiyerarşik tasarımda üç temel katman bulunur:

Erişim Katmanı - yerel bir Ethernet ağında konak bilgisayarlara bağlantı sağlar.

Dağıtım Katmanı - daha küçük yerel ağların birbirine bağlanmasını sağlar.

Çekirdek Katmanı - dağıtım katmanı cihazları arasında yüksek hızlı bağlantı sağlar.

Bu yeni hiyerarşik tasarımda, konak bilgisayarın konumunu tanımlayabilen mantıksal adresleme şeması gerekir. Bu, İnternet Protokolü (IP) adresleme şemasıdır.

3.2.2 Mantıksal Adresleme

Kişilerin adı genellikle değişmez. Ancak kişilerin adresi yaşadıkları yerle ilgili olduğundan değişebilir. Konak bilgisayarlarda MAC adresi değişmez; bu adres, konak bilgisayar NIC'sine fiziksel olarak atanır ve fiziksel adres olarak bilinir. Fiziksel adres, konak bilgisayarın ağda bulunduğu yer dikkate alınmaksızın aynı kalır.

IP adresi ise kişilerin adresine benzer. Bu adres, konak bilgisayarın bulunduğu yer temel alınarak mantıksal olarak atandığından, mantıksal adres olarak bilinir. IP adresi veya ağ adresi, yerel ağ temel alınarak her bir konak bilgisayara ağ yöneticisi tarafından atanır.

IP adresleri iki bölümden oluşur. Bu bölümlerden biri yerel ağı tanımlar. IP adresinin ağ bölümü, aynı yerel ağa bağlı tüm konak bilgisayarlarda aynıdır. IP adresinin ikinci bölümü tek bir konak bilgisayarı tanımlar. Aynı yerel ağ içinde, IP adresinin konak bilgisayar bölümü her bir konak bilgisayar için benzersizdir.

Bir kişinin mektup göndermesi için kişinin hem ismi hem de adresinin gerekli olması gibi, bir bilgisayarın hiyerarşik ağda iletişim kurması için de hem fiziksel MAC adresi hem de mantıksal IP adresi gereklidir.

3.2.3 Erişim ve Dağıtım Katmanı ve Cihazlar

IP trafiği, şu üç katmanın her biriyle ilişkilendirilmiş özellikler ve cihazlar temel alınarak yönetilir: Erişim, Dağıtım ve Çekirdek. Trafiğin yerel kalması mı yoksa hiyerarşik ağ katmanlarında yukarı taşınması mı gerektiğini belirlemek için IP adresi kullanılır.

Erişim Katmanı, son kullanıcı cihazları için ağa bağlantı noktası sağlar ve birden çok konak bilgisayarın, genellikle dağıtıcı veya anahtar gibi bir ağ cihazı üzerinden diğer konak

bilgisayarlara bağlanmasına izin verir. Genellikle tek bir Erişim Katmanındaki tüm cihazların IP adreslerinin ağ bölümü aynıdır.

İleti yerel bir konak bilgisayara hedeflenirse, IP adresinin ağ bölümü temel alınarak ileti yerel kalır. Farklı bir ağa hedeflenirse, ileti Dağıtım Katmanına geçer. Dağıtıcılar ve anahtarlar, genellikle yönlendirici gibi Dağıtım Katmanı cihazlarına bağlantı sağlar.

Çekirdek Katmanı, artıklı (yedek) bağlantıları olan yüksek hızlı bir omurga katmanıdır. Bu katman, birden çok uç ağ arasında büyük miktarda verilerin taşınmasından sorumludur. Çekirdek Katmanı cihazları arasında genellikle çok güçlü, yüksek hızlı anahtarlar ve yönlendiriciler yer alır. Çekirdek Katmanının ana hedefi, verileri hızla taşımaktır. Dağıtıcılar, anahtarlar ve yönlendiriciler sonraki iki bölümde ayrıntılı olarak ele alınmıştır.

3.2.4 Erişim Katmanı

Erişim Katmanı, ağın en temel düzeyidir. Burası ağın, diğer konak bilgisayarlara, paylaşılan dosyalara ve yazıcılara insanların erişebildiği bölümdür. Erişim Katmanı, konak bilgisayarlardan ve bunların bağlı olduğu ağ iletişim cihazlarının birinci hattından oluşur.

Ağ iletişim cihazları, birçok konak bilgisayarı birbirine bağlamamızı ve bu konak bilgisayarların ağ üzerinden sunulan hizmetlere erişmesini sağlar. Tek bir kabloyla bağlanmış iki konak bilgisayardan oluşan basit ağlardan farklı olarak, Erişim Katmanındaki her konak bilgisayar bir ağ iletişim cihazına bağlıdır. Bu bağlantı tipi grafikte gösterilmektedir.

Bir Ethernet ağı içinde her konak bilgisayar, noktadan noktaya kablo kullanarak doğrudan bir Erişim Katmanı ağ iletişim cihazına bağlanabilir. Bu kablolar belirli Ethernet standartlarını karşılamak üzere üretilir. Kabloların her biri konak bilgisayar NIC'sine ve daha sonra da ağ iletişim cihazındaki bir bağlantı noktasına takılır. Konak bilgisayarları Erişim Katmanına bağlamak için kullanılabilen, Ethernet dağıtıcıları ve anahtarlar gibi birçok tipte ağ iletişim cihazı vardır.

3.2.5 Dağıtıcıların İşlevi

Dağıtıcı, Ethernet ağının Erişim Katmanına takılan bir tip ağ iletişim cihazıdır. Dağıtıcılarda, konak bilgisayarları ağa bağlamak için kullanılan birden çok bağlantı noktası bulunur. Dağıtıcılar, ağdaki konak bilgisayarlar arasında gönderilen iletilerin kodunu çözmek için gerekli elektroniklerin bulunmadığı basit cihazlardır. Belirli bir iletiyi hangi konak bilgisayarın alması gerektiğini dağıtıcılar belirleyemez. Dağıtıcı yalnızca bir bağlantı noktasından gelen elektronik sinyalleri kabul eder ve diğer tüm bağlantı noktalarından aynı iletiyi yeniden oluşturur (veya yineler).

Bir konak bilgisayardaki NIC'nin yalnızca doğru MAC adresine yönelik iletileri kabul ettiğini unutmayın. Konak bilgisayarlar kendi adreslerine yönelik iletileri yok sayar. Yalnızca iletinin hedef adresinde belirtilen konak bilgisayar iletiyi işler ve gönderene yanıt verir.

Ethernet dağıtıcısındaki bağlantı noktalarının tümü, ileti gönderip almak için aynı kanala bağlanır. Tüm konak bilgisayarların o kanaldaki kullanılabilir bant genişliğini paylaşması gerektiğinden, dağıtıcıya paylaşılan bant genişliği cihazı da denir. Bir Ethernet dağıtıcısı üzerinden aynı anda yalnızca bir ileti gönderilebilir. Bir dağıtıcıya bağlı iki veya daha fazla konak bilgisayar aynı anda ileti göndermeyi deneyebilir. Bu durumda, iletiyi oluşturan elektronik sinyaller dağıtıcıda birbiriyle çatışır.

Çatışma, iletilerin bozulmasına ve konak bilgisayarlar tarafından okunamamasına yol açar. Dağıtıcı iletilerin kodunu çözmez; dolayısıyla dağıtıcı iletinin bozuk olduğunu algılamadığından tüm bağlantı noktalarından iletiyi yineler. Konak bilgisayarın çatışmadan dolayı bozuk ileti alabileceği ağ alanı, çatışma etki alanı olarak bilinir.

Çatışma etki alanında, bir konak bilgisayar bozuk ileti aldığında çatışmanın oluştuğunu algılar. Gönderen her konak bilgisayar kısa bir süre bekler ve daha sonra iletiyi göndermeyi veya yeniden iletmeyi dener. Dağıtıcıya bağlı konak bilgisayarların sayısı arttıkça, çatışma oluşması ihtimali de artar. Çatışmaların artması, yeniden iletimlerin de artmasına yol açar. Aşırı miktarda yeniden iletim, ağı tıkayarak ağ trafiğini yavaşlatabilir. Bu nedenle, çatışma etki alanının boyutunu sınırlandırmak gerekir.

3.2.6 Anahtarların İşlevi

Ethernet anahtarı, Erişim Katmanında kullanılan bir cihazdır. Dağıtıcı gibi anahtar da birden çok konak bilgisayarı ağa bağlar. Ancak dağıtıcıdan farklı olarak, anahtar belirli bir konak bilgisayara ileti iletebilir. Bir konak bilgisayar anahtardaki başka bir konak bilgisayara ileti gönderdiğinde, anahtar, çerçeveleri kabul eder ve iletinin fiziksel (MAC) adres bölümünü okumak için çerçevelerin kodunu çözer.

Anahtardaki bir tabloda (MAC adresi tablosu denir), tüm etkin bağlantı noktalarının bir listesi ve bunlara bağlı konak bilgisayar MAC adresleri bulunur. Konak bilgisayarlar arasında bir ileti gönderildiğinde, anahtar, hedef MAC adresinin tabloda olup olmadığını kontrol eder. MAC adresi tablodaysa, anahtar, kaynak ve hedef bağlantı noktaları arasında devre adı verilen geçici bir bağlantı oluşturur. Bu yeni devre, iki konak bilgisayarın üzerinde iletişim kurabileceği adanmış bir kanal sağlar. Anahtara bağlı diğer konak bilgisayarlar bu kanaldaki bant genişliğini paylaşmaz ve kendi adreslerine yönelik olmayan iletileri almaz. Konak bilgisayarlar arasındaki her yeni iletişim için yeni bir devre oluşturulur. Bu ayrı devreler, çatışma oluşmadan aynı anda birçok iletişimin gerçekleşmesine izin verir.

Anahtar, henüz MAC adresi tablosunda bulunmayan yeni bir konak bilgisayarın adresine gönderilen bir çerçeve aldığında ne olur? Hedef MAC adresi tabloda bulunmuyorsa, anahtar ayrı bir devre oluşturmak için yeterli bilgiye sahip değildir. Anahtar, hedef konak bilgisayarın bulunduğu yeri belirleyemediğinde, iletiyi tüm bağlı konak bilgisayarlara iletmek için taşma adı verilen bir işlemi gerçekleştirir. Konak bilgisayarların her biri iletideki hedef

MAC adresini kendi MAC adresiyle karşılaştırır ancak yalnızca doğru hedef adrese sahip olan konak bilgisayar iletiyi işler ve gönderene yanıt verir.

Yeni bir konak bilgisayarın MAC adresi nasıl MAC adresi tablosuna girer? Anahtar, konak bilgisayarlar arasında gönderilen her çerçevenin kaynak MAC adresini inceleyerek MAC adresi tablosunu oluşturur. Yeni bir konak bilgisayar ileti gönderdiğinde veya taşmış bir iletiye yanıt verdiğinde, anahtar hemen onun MAC adresini ve bağlı olduğu bağlantı noktasını öğrenir. Anahtar her yeni bir kaynak MAC adresi okuduğunda, tablo dinamik olarak güncellenir. Böylece anahtar, bağlı konak bilgisayarların tümünün MAC adresini hızlı bir şekilde öğrenir.

Bazen dağıtıcı gibi başka bir ağ iletişim cihazının bir anahtar bağlantı noktasına bağlanması gerekir. Ağa bağlanabilen konak bilgisayar sayısını artırmak için bu yapılır. Bir anahtar bağlantı noktasına dağıtıcı bağlandığında, anahtar o dağıtıcıya bağlı tüm konak bilgisayarların MAC adreslerini anahtardaki tek bir bağlantı noktasıyla ilişkilendirir. Zaman zaman, bağlı dağıtıcıdaki bir konak bilgisayar, aynı dağıtıcıya bağlı başka bir konak bilgisayara ileti gönderir. Bu durumda anahtar çerçeveyi alır ve hedef konak bilgisayarın bulunduğu yeri görmek için tabloyu kontrol eder. Kaynak ve hedef konak bilgisayarlar aynı bağlantı noktasında bulunuyorsa, anahtar iletiyi atar.

Bir anahtar bağlantı noktasına dağıtıcı bağlandığında, dağıtıcıda çatışmalar oluşabilir. Dağıtıcı, çatışmadan kaynaklanan bozuk iletileri tüm bağlantı noktalarına iletir. Anahtar bozuk iletiyi alır ancak dağıtıcıdan farklı olarak anahtar, çatışmadan kaynaklanan bozuk iletileri iletmez. Sonuç olarak her anahtar bağlantı noktası ayrı bir çatışma etki alanı oluşturur. Bu iyi bir şeydir. Çatışma etki alanında ne kadar az konak bilgisayar bulunursa, çatışma oluşması ihtimali de o kadar az olur.

3.2.7 Dağıtım Katmanı

Ağlar büyüdükçe genellikle bir yerel ağın birden çok Erişim Katmanı ağına bölünmesi gerekir. Aşağıda örnekleri verilen farklı ölçütler temel alınarak ağları bölmenin birçok yolu vardır:

- Fiziksel konum
- Mantıksal işlev
- Güvenlik gereksinimleri
- Uygulama gereksinimleri

Dağıtım Katmanı, bu bağımsız yerel ağları bağlar ve aralarındaki trafiği denetler. Bu katman, yerel ağda konak bilgisayarlar arasındaki trafiğin yerel kalmasını sağlamaktan sorumludur.

Yalnızca diğer ağları hedefleyen trafik iletilir. Dağıtım Katmanı, güvenlik ve trafik yönetimi için gelen ve giden trafiği de filtreleyebilir.

Dağıtım Katmanını oluşturan ağ iletişim cihazları, tek tek konak bilgisayarları değil, ağları birbirine bağlamak üzere tasarlanmıştır. Ayrı ayrı konak bilgisayarlar dağıtıcı ve anahtar gibi Erişim Katmanı cihazları üzerinden ağa bağlanır. Erişim Katmanı cihazları da, yönlendirici gibi Dağıtım Katmanı cihazı üzerinden birbirine bağlanır.

3.2.8 Yönlendiricilerin İşlevi

Yönlendirici, yerel ağı başka yerel ağlara bağlayan bir ağ iletişim cihazıdır. Ağın Dağıtım Katmanında yönlendiriciler trafiği yönlendirir ve ağ işleminin verimliliği açısından kritik olan diğer işlevleri gerçekleştirir. Anahtarlar gibi yönlendiriciler de kendilerine gönderilen iletilerin kodunu çözüp iletileri okuyabilir. Ancak yalnızca MAC adresi bilgilerini içeren çerçevelerin kodunu çözen (kapsül açma işlemini gerçekleştiren) anahtarlardan farklı olarak, yönlendiriciler çerçeve içinde kapsüllenmiş paketin kodunu çözer.

Paket biçiminde, hedef ve kaynak konak bilgisayarların IP adresleri ve bu konak bilgisayarların arasında gönderilen iletilerin verileri bulunur. Yönlendirici, hedef IP adresinin ağ bölümünü okur ve bağlı ağlardan hangisinin iletiyi hedefe yönlendirmek için en iyi yol olduğunu bulmak üzere bu bölümü kullanır.

Kaynak ve hedef konak bilgisayarların IP adreslerinin ağ bölümü birbiriyle aynı olmadığında, iletiyi iletmek için yönlendiricinin kullanılması gerekir. 1.1.1.0 ağında bulunan bir konak bilgisayarın 5.5.5.0 ağındaki bir konak bilgisayara ileti göndermesi gerekirse, konak bilgisayar iletiyi yönlendiriciye iletir. Yönlendirici iletiyi alır ve hedef IP adresini okumak için iletiyi kapsül açma işlemini gerçekleştirir. Ardından iletiyi nereye ileteceğini belirler. Paketi yeniden bir çerçeveye kapsüller ve çerçeveyi hedefine iletir.

Yönlendirici, hedef ağa ulaşması için iletinin gönderileceği yolu nasıl belirler?

Yönlendirici üzerindeki her bağlantı noktası veya arayüz farklı bir yerel ağa bağlanır. Her yönlendiricide yerel olarak bağlı tüm ağların ve bu ağları bağlayan arayüzlerin bir tablosu bulunur. Bu yönlendirme tablolarında, yönlendiricinin yerel olarak bağlı olmayan diğer uzak ağlara ulaşmak için kullandığı rotalar veya yollar hakkında bilgiler de yer alabilir.

Yönlendirici bir çerçeve aldığında, hedef IP adresini içeren pakete ulaşmak için çerçevenin kodunu çözer. Hedefin adresini, yönlendirme tablosunda bulunan ağların tümüne eşleştirir. Hedef ağ adresi tabloda bulunuyorsa, yönlendirici paketi göndermek için yeni bir çerçeveye kapsüller. Hedef ağa giden yolla ilişkilendirilmiş arayüzden yeni çerçeveyi iletir. Paketleri hedef ağına iletme işlemine yönlendirme denir.Yönlendirici arayüzleri, yayın MAC

adresine yönelik iletileri iletmez. Bunun sonucu olarak da, yerel ağ yayınları diğer yerel ağlara yönlendiriciler üzerinden gönderilmez.

3.2.9 Varsayılan Ağ Geçidi

Konak bilgisayarın uzak ağdaki bir hedefe ileti göndermek için kullandığı yöntem, aynı yerel ağda ileti göndermek için kullandığı yöntemden farklıdır. Bir konak bilgisayarın aynı ağda bulunan başka bir konak bilgisayara ileti göndermesi gerektiğinde, konak bilgisayar iletiyi doğrudan iletir. Konak bilgisayar, hedef konak bilgisayarın MAC adresini keşfetmek için ARP'yi kullanır. Konak bilgisayar pakete hedef IP adresini ekler ve paketi hedefin MAC adresini içeren bir çerçeveye kapsülleyerek iletir.

Diğer yandan konak bilgisayarın uzak bir ağa ileti göndermesi gerektiğinde yönlendiriciyi kullanması gerekir. Konak bilgisayar daha önceki gibi paketin içine hedef konak bilgisayarın IP adresini ekler. Ancak paketi çerçeveye kapsüllerken, çerçevenin hedefi olarak yönlendiricinin MAC adresini kullanır. Böylece yönlendirici çerçeveyi alıp MAC adresini temel alarak kabul eder.

Kaynak konak bilgisayar, yönlendiricinin MAC adresini nasıl belirler? Konak bilgisayara TCP/IP (İletim Denetim Protokolü/İnternet Protokolü) ayarlarında yapılandırılan varsayılan ağ geçidi adresi üzerinden yönlendiricinin IP adresi verilir. Varsayılan ağ geçidi adresi, kaynak konak bilgisayarla aynı yerel ağa bağlı yönlendirici ara yüzünün adresidir. Yerel ağdaki tüm konak bilgisayarlar iletileri yönlendiriciye göndermek için varsayılan ağ geçidi adresini kullanır. Konak bilgisayar, varsayılan ağ geçidi IP adresini öğrendikten sonra, MAC adresini belirlemek için ARP'yi kullanabilir. Daha sonra yönlendiricinin MAC adresi, başka bir ağı hedefleyen çerçeveye yerleştirilir.

Yerel ağdaki konak bilgisayarların her birinde doğru varsayılan ağ geçidinin yapılandırılmış olması önemlidir. Konak bilgisayar TCP/IP ayarlarında herhangi bir varsayılan ağ geçidi yapılandırılmamışsa veya yanlış bir varsayılan ağ geçidi belirtilmişse, uzak ağlardaki konak bilgisayarların adreslerine gönderilen iletiler teslim edilemez.

3.2.10 Yönlendiriciler Tarafından Korunan Tablolar

Yönlendiriciler yerel ve uzak ağlar arasında bilgi taşır. Bunu yapmak için yönlendiricilerin bilgileri saklamak üzere ARP'yi ve yönlendirme tablolarını kullanması

gerekir. Yönlendirme tabloları, ayrı ayrı konak bilgisayarların adresleriyle ilgili değildir. Yönlendirme tablolarında ağların adresleri ve bu ağlara ulaşılacak en iyi yol bulunur. Yönlendirme tablosuna iki şekilde giriş yapılabilir: ağdaki diğer yönlendiricilerden alınan bilgilerle dinamik şekilde güncellenerek veya ağ yöneticisi tarafından manuel girilerek. Yönlendiriciler, bir iletiyi amaçlanan hedefe iletmek üzere kullanılacak ara yüzü belirlemek için yönlendirme tablolarını kullanır.

Yönlendirici iletinin iletileceği yeri belirleyemezse, iletiyi bırakır. Ağ yöneticileri, hedef ağa giden yolun yönlendirme tablosunda bulunmaması yüzünden paketin bırakılmasını önlemek için, varsayılan rotanın bulunduğu bir yönlendirme tablosu yapılandırır. Varsayılan rota, yönlendiricinin bilinmeyen hedef IP ağ adresini içeren paketleri iletmekte kullandığı ara yüzdür. Bu varsayılan rota, genellikle paketi son hedef ağına iletebilecek başka bir yönlendiriciye bağlanır

Yönlendirici çerçeveyi şu iki yerden birine iletir: gerçek hedef konak bilgisayarın bulunduğu doğrudan bağlı bir ağa veya hedef konak bilgisayara ulaşma yolundaki başka bir yönlendiriciye. Yönlendirici çerçeveyi bir Ethernet ara yüzünden iletmek için kapsüllediğinde, hedef MAC adresini de eklemelidir.

Hedef konak bilgisayar, yönlendiriciye yerel olarak bağlı bir ağın parçasıysa, bu hedef MAC adresi, gerçek konak bilgisayarın MAC adresidir. Yönlendiricinin paketi başka bir yönlendiriciye iletmesi gerekirse, bu durumda yönlendirici bağlı yönlendiricinin MAC adresini kullanır. Yönlendiriciler bu MAC adreslerini ARP tablolarından alır.

Her yönlendirici arayüzü, bağlı olduğu yerel ağın bir parçası olup o ağ için kendi ARP tablosunu korur. ARP tablolarında, söz konusu ağdaki ayrı ayrı konak bilgisayarların tümünün MAC adresleri ve IP adresleri bulunur.

3.2.11 Köprü

Paketleri, aynı iletişim protokolünü kullanan iki ağ kesimi arasında bağlayan ve geçiren cihaz. Genelde, çercevenin MAC adresine göre gelen bir çerçeveyi filtreler, iletir veya taşırır.

3.2.12 Yineleyici

Kablonun kapasitesinden daha fazla mesafelere bağlantı kurulması gerektiğinde araya bir yükseltici konularak sinyalin güçlendirilmesini sağlayan cihazdır

OSI'nin 1. katmanında çalıştığı için verinin içeriğine bakmaz, sadece sinyalleri güçlendirir. Ağ trafiğini yönetmez.

- Ağ kablosunun erişebileceği maksimum mesafeyi uzatırlar
- Ağdaki maksimum düğüm sayısını arttırır.
- Kablo arızalarının etkisini azaltabilir.
- Farklı kablo tipleri kullanan ağları birleştirebilir.

3.3 Ağa Erişim Metotları

- PSTN (Public Switched Telephone Network)
- ISDN (Integrated Services Digital Network)
- Remote Access
- ADSL (Asymmetric Digital Subscriber Line)

3.3.1 PSTN

Halka Açık Anahtarlamalı Telefon Ağı (PSTN)

Hem kablolu hem de kablosuz teknolojiler üzerinden telefon aramalarına izin veren ve internet erişimi sağlayan kablolu ağ

3.3.2 ISDN

Integrated Services Digital Network (Tümleşik Hizmetler Sayısal şebekesi) sözcüklerinin baş harflerinden oluşan ISDN ses, görüntü, veri gibi her türlü bilginin Sayısal bir ortamda birleştirilip ayni hat üzerinden iletilmesinin sağlandığı bir haberleşme ağıdır. İletim kalitesi normal telefon hattından daha yüksektir. ISDN hata oranı düşük, güvenli ve sınırsız bir haberleşme sağlar.

3.3.3 ADSL

DSL de telefon hatlarını kullanır ama çevirmeli bağlantının aksine DSL, İnternet'e sürekli bağlantı olanağı sağlar. Bu bağlantı seçeneğinde genel olarak DSL sinyalini telefon sinyalinden ayıran ve bir konak bilgisayara veya LAN'a Ethernet bağlantısı sağlayan özel bir yüksek hızlı modem kullanılır.

DSL, 512 kbps ve üzeri hızlarda yüksek hızlı dijital iletim olanağı sağlayan bir geniş bant teknolojisidir. 512 kbps hızla bağlıysanız, 5 MB'lık bir dosyanın indirilmesi yaklaşık bir dakika sürer. Yükleme ve indirme hızları coğrafi bölgeye, ISP'ye olan uzaklığa ve sunulan ISP hizmetlerine bağlı olarak değişiklik gösterir.

DSL'in birçok farklı çeşidi vardır. Bir ev kullanıcısı genellikle indirme hızının yükleme hızından daha yüksek olduğu Asimetrik Sayısal Abone Hattı'nı (ADSL) kullanır. DSL hizmetinin Simetrik Sayısal Abone Hattı (SDSL) olarak adlandırılan başka bir çeşidi daha vardır. SDSL'de yükleme ve indirme hızları aynıdır ve bu nedenle bu hizmet, küçük ve orta büyüklükteki işletmeler için daha kullanışlı olabilir.

Remote Access

Bu bağlantı türü uzaktaki bir bilgisayara bazı özel işlemlerle bağlanmanızı sağlar. Vpn ve Dial up bu bağlantı türlerinin kendi özel protokolleri olup bugünkü torrent programları ve hamachi gibi karşılıklı ağ kurma programları bu alt yapıyı kullanılır.

3.3.4 Topoloji Tipleri

- Bus Topoloji
- Halka(Ring)Topoloji
- Yıldız(Star)Topoloji
- Mesh(ağ)Topoloji
- Melez(Hybrid)Topolojiler
- Ağaç(Tree)Topoloji

3.3.4.1 Bus Topoloji

Fiziksel bus tüm bilgisayarların aynı kabloya bağlı oldukları sistemdir. Kablonun her iki ucuna sonlandırıcı adı verilen dirençler takılır. Bu topoloji hem mantıksal hem de fiziksel olarak varlığını sürdürmektedir. Kurulumu kolaydır. En büyük dezavantajı kablonun bir noktasında oluşan kopukluğun tüm sistemi çökertmesidir.

3.3.4.2 Halka(Ring) Topoloji

Mantıksal Ring topoloji ise Token-Ring adı verilen ilk başta IBM'in geliştirdiği, sonraları IEEE ve ISO tarafından geliştirilmeye devam eden ağ sisteminin kullandığı sistemdir. Token-Ring'de bilgisayarlar kablolarla ortadaki merkez bir kutuya bağlıdır(fiziksel yıldız). Ancak sistemde veri aktarımını sağlayan bir sinyal sürekli olarak sırayla tüm

sistemleri dolaşmaktadır. Token adı verilen bu sinyal tek tek tüm sistemlere uğradığı için Ring/Halka terimi buradan gelmektedir.

3.3.4.3 Yıldız Topolojileri

Bir yıldız topolojide, her cihaz tek bir bağlantı aracılığıyla merkezi bir noktaya bağlanır. Merkezi nokta genel olarak bir anahtar veya bir kablosuz erişim noktasıdır. Yıldız topolojisinin avantajı, bağlanan cihazlardan biri arızalandığında bu durumdan yalnızca o cihazın etkilenmesidir. Ancak merkezi cihaz, örneğin anahtar, arızalandığında, bağlanan cihazların tümünün bağlantısı kesilir.

Birden çok anahtarın birbiriyle bağlantılı olduğu veya papatya zincir ile birbirine bağlandığı durumlarda ise, bir yıldızdaki merkezi cihaz başka bir yıldızın merkezi cihazına bağlanarak genişletilmiş yıldız oluşturulur.

3.3.4.4 Örgüsel Topolojiler

Bir ağdaki Çekirdek Katmanları'nın çoğu, tam örgüsel veya kısmi örgüsel topolojide kablolanır. Tam örgüsel topolojide her cihazın diğer tüm cihazlara bağlantısı vardır. Tam örgüsel topolojilerin tam artıklı bir ağ sunmalarına rağmen, kablolanmaları ve yönetilmeleri zor olabilir ve daha pahalıdırlar.

Daha büyük kurulumlarda, değiştirilmiş bir kısmi örgüsel topoloji kullanılır. Bir kısmi örgüsel topolojide her cihaz en az iki başka cihaza daha bağlıdır. Bu düzenleme, tam örgüsel topolojinin karmaşıklığı olmaksızın yeterli artıklık sağlar.

Kısmi veya tam örgüsel topolojiler aracılığıyla yedekli bağların uygulanması ağ cihazlarının, arıza durumunda verileri göndermek için alternatif yollar bulabilmelerini sağlar.

3.3.4.5 Melez(Hybrid)Topolojiler

Network dizaynında iki veya daha fazla topolojiden yararlanılmasıdır.

- Star-Bus: Kendi içinde Star topolojide kurulu Network ortamlarının birbirine bus topoloji vasıtası ile bağlanmasıdır. Tek bir bilgisayarın çökmesi sistemi etkilemez ancak Network komlimenti örnek olarak Hub arızası sistem trafiğini etkiler.
- Star-Ring: Kendi içinde star topolojide kurulu Network ortamlarının birbirine Ring topoloji vasıtası ile bağlanmasıdır. Tek bilgisayarın çökmesi sistemi etkilemez.

3.4 KAYNAKLAR

Not: Bu dosyadaki tüm dokümanlar **CSNA (Cisco Systems Networking Academi)** internet ortamından alınmıştır.

4 BÖLÜM

4.1 OSI MODELİ VE FİZİKSEL KATMAN

4.1.1 OSI nedir ?

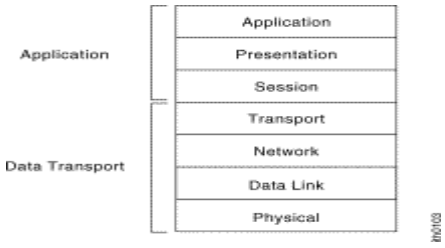
OSI (Open Systems Interconnection- Açık Sistem Bağlantıları) 1980 yılında ISO (International Standards Organization– Uluslararası Standartlar Organizasyonu) tarafından geliştirilen ve bilgisayarlar arası iletişimin nasıl olacağını tanımlayan kurallar bütünüdür. Herhangi bir network aygıtı/protokolü gözetmeksizin ortak bir alanda anlaşmalarını sağlamayı amaçlar.

4.1.1.1 OSI Referans Modeli

OSI Modeli herhangi bir donanım ya da network tipine özel değildir. OSI network iletişimini düzenleyen bir modeldir.
Bir dosya transferi, bir dosya download veya bir uygulamayı çalıştırırken gereken protokol düzenini bir sıraya koyan ve kontrolünü sağlayan kurallar bütünüdür. Ağ ile ilgili her türlü veri alışverişi bu kurallar çerçevesinde uygulanır. TCP/IP nin de içerisinde olduğu tüm protokoller OSI referans modelinin ortaya koyduğu kurallar çerçevesinde çalışır. Ağ içerisinde bulunan router, ethernet, ağ kabloları ve programların hepsi OSI modelinin bir katmanında işlem görür ve belirlenen kurallar çerçevesinde üst veya alt katmana aktarılarak veri akışının sürekliliği sağlanır.

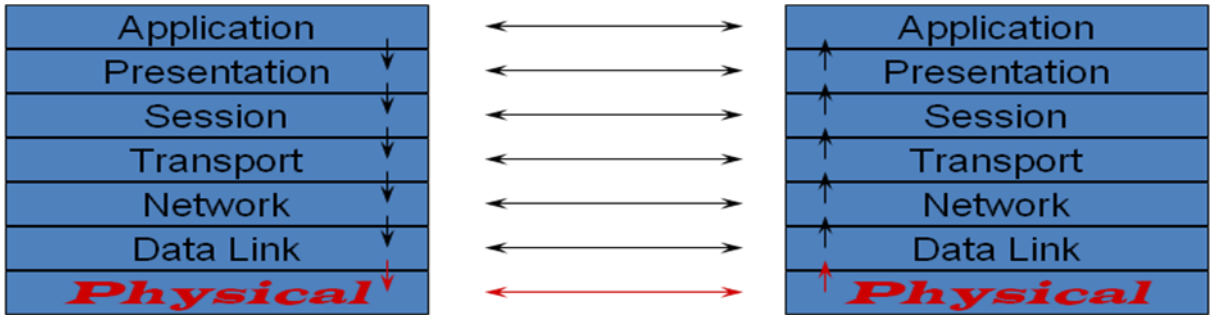
4.1.1.2 OSI Başvuru Modeli Mimarisi

OSI başvuru modelinde tam bir hiyerarşik yapı vardır. Hiyerarşinin en üstünde kullanıcıların koşturduğu uygulama programları ve en altta ise verinin bit düzeyinde aktarılması vardır. Ara katmanlar bu iki katman arasında uyarlamaları içerir. Her katman bir üst katmana hizmet sunarken bir alt katmanda kendisi için hizmet ister. [5]



Şekil 1

OSI modeli 7 katmanda incelenir:



Şekil 2

No	Katman	İşlevi
7	**Uygulama Katmanı** (Application Layer)	Kullanıcı uygulamalarına servis sağlar
6	**OSI Sunum Katmanı** (Presentation Layer)	Kullanıcı uygulaması için verinin dönüşümünü sağlar.
5	**Oturum Katmanı** (Session Layer)	Sistemler arasındaki iletişimi sağlar.
4	**Taşıma Katmanı** (Transport Layer)	Temel network bağlantısı sağlayan 1 ve 3. katman ile uygulama iletişimini sağlayan 5 ve 7. üst üç katman arasındaki bu katman bu bölümleri birbirinden ayırır.
3	**Network Katmanı** (Network Layer)	Network bağlantısını düzenlemek, devam ettirmek ve sonlandırmaktan sorumludur.
2	**Veri Hattı Katmanı** (Data Link)	Fiziksel bağlantıyı sağlar. Veri frame'lerini düzenler.
1	**Fiziksel Katman** (Physical Layer)	Veri iletimi ortamı düzeyinde verilerin elektrik sinyalleri olarak iletimini sağlar.

4.1.2 Fiziksel Katman (Physical Layer)

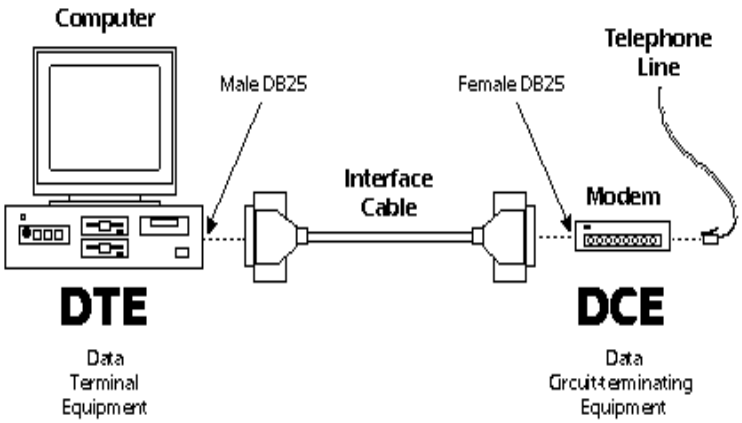
Fiziksel katman bitlerin bir bilgisayardan diğerine gönderildiği bir katmandır. Diğer bir deyişle network' ün ta kendisidir. Bu katmanda network kablosu ile iletişim kurulur. Network üzerinde iki istasyon arasındaki bağlantı bakır bir kablo, UTP (Unshielded Twisted Pair), fiber-optik, radyo sinyalleri, mikrodalga, infrared ya da ortama göre değişen bir medya olabilir. Fiziksel iletimle ilgili yaygın olarak IEEE 802.3, 802.4 ve 802.5 Token ring standartları kullanılır. Fiziksel katman verilerin bit olarak (elektronik olarak) iletimiyle ilgilenir. Veri paketleriyle, framelerle , adreslerle ya da verinin ulaşacağı hedef ile ilgilenmez. Fiziksel katman bağlantı arayüzleri ise iki açıdan ele alınabilir. DTE-DCE ve LAN olarak ele alınabilir. [1]

4.1.2.1 DTE-DCE Bağlantı Standartları

DTE-DCE terimleri ilk defa ITU (International Telecommunication Union 'Uluslararası Haberleşmeciler Birliği') tarafından ortaya atılmıştır ve genel olarak bilgisayar, terminal gibi cihazların sahip oldukları standart portlar üzerinden ağ yapılabilmesini tanımlamaktadır. Bu amaçla ortaya atılan ve geniş kabul gören standartlar, günümüzde, özellikle WAN ağ cihazlarında yoğun olarak kullanılmaktadır. ITU, WAN iletişimini düzenlemeye çalışan bir kurumdur. Ülke genelinde, WAN bağlantı hizmeti, sağlayan şirketler 'Türk Telekom ' gibi resmi ya da özel kurumlardır ve WAN işletimi bu kurumların sorumluluğundadır. ITU yaklaşımında DCE'ler bu kurumların sorumluluğundadır ya da kurumca onaylanmış olmaları gerekir. Böylece son kullanıcılar kendi sorumluluklarında olan uç düğümlerini DTE-DCE arayüzünde tanımlı protokollere göre çalışmak zorunda bırakılmışlardır. ITU yaklaşımında, DCE'nin görevi gönderilecek bilginin kanala uygun hale sokulması ve gelen bilginin kanaldan alınarak DTE'nin yorumlayabileceği bir şekle getirilmesidir. [1]

DTE, ağa bağlanarak veri iletişim hizmetinden yararlanacak olan kişisel bilgisayar, terminal ya da network host türü (server gibi) bir donanım olabilir. DCE, devre sonlandırıcı modem cihazı olup ağ ile DTE arasındaki arabirimdir.[2]

DTE-DCE arasındaki fiziksel katman protokolü, lojik işaretlerin elektriksel işaretlere dönüştürülmesinde, yaygın olarak NRZ-L (Düz sıfıra dönüşsüz kodlama (non return zero – Level NRZ-L)) kodlama tekniğini kullanmaktadır. [1]



Şekil 3

4.1.2.2 DTE-DCE Standartları

RS-232: İlk olarak 1962 yılında çıkmıştır. RS önadı (recommended Standard – Önerilen Standart") anlamında kullanılmaktadır. Seri asenkron olarak gönderilen verinin alınması veya iletilmesini gerçekleştiren cihazlar arasında bu tür haberleşmenin sağlanabilmesi için geliştirilen bir standarttır. . RS–232 seri portu genellikle COM 1, COM 2, RS–232 veya seri olarak belirlenmiştir.

RS-232 C: 1969 yılında RS-232 nin üçüncü versiyonu olarak çıkmıştır. Kullanılan en yaygın konektör tipi DB25'dir ve 25 pinlidir. "D" tipi konektörlerdir. Bu tip konektörler "D" şeklinde olduğu için bu adı almışlardır. Amerika Birleşik Devletleri dışında bu DB–25 konektörü kablosu V.24 ve V.28 olarak bilinir. EIA (Electronic Industries Assosiation)

tarafından daha bilgisayarın başlangıç zamanları sayılan o yıllarda tasarlanmıştır. EIA' da çalışan mühendisler gelecek için nasıl bir şey geliştireceklerinden pek emin değillerdi. Böylece RS–232 C standardının mümkün olduğu kadar esnek olması için çok sayıda farklı sinyal hatları sağlamışlardır. Fakat günümüzde bu sinyal bağlantılarının çoğu kullanılmamaktadır.

RS232C'nin dezavantajları:

• Data iletim hızı 20 Kbps ile sınırlıdır.
• İletim mesafesi 15 metredir.
• RS232C için kullanılan konnektör verimli değildir.

Bu dezavantajlar göz önünde bulundurularak, yeni bir standart oluşturmak için bazı amaçlar düşünüldü. Bu amaçlar;

• RS232C standardının uygulanabilirliğini sürdürmek. Özellikle, yeni standardın gereklerini yerine getirerek çalışabilmesi için RS232 C sisteminin tümüyle değiştirilmesini gerektirmemeli.
• Daha yüksek veri iletim oranı elde etmek.
• Daha uzun mesafelere iletim yapabilmek.
• RS232C konnektöründen kaynaklanan mekanik kayıpları ortadan kaldırmak.

Bu amaçla, EIA 1977 yılında yeni bir standart olan RS449(hem 37 pinli, hem de 9 pinli) geliştirildi.

RS-449A iki kablo belirler; bir tanesi 37 tellidir ve seri veri iletiminde kullanılır, diğeri 9 tellidir ve ikincil tanı bilgisinde kullanılır. İki standart arasındaki en önemli fark, RS-449A'da birincil veri ve ikincil tanı kanallarının iki kabloya ayrılmasıdır.[1]

Daha sonra, RS232C'nin elektriksel karakteristiklerinin yenilendiği iki yeni standart daha geliştirildi.

• RS422A Electrical Characteristics Of Balanced Voltage Digital İnterface Circuits (Elektrik özelliklerinin dengeli gerilim arayüz devreleri) **(Aralık 1978)**

• RS423A Electrical Characteristics Of Unbalanced Voltage Digital İnterface Circuits (Elektrik özelliklerinin dengesiz gerilim arayüz devreleri) **(Eylül 1978)**

RS422A ve RS423A'nın RS232C'ye göre elektriksel karakteristik olarak avantajı fark(differantial) sinyaller kullanmasıdır. [4]

IBM'in standartları belirlemede bir üstünlüğü olduğundan dolayı o zamanlarda bazı üretici firmalar tarafından 9 pinli konektörler desteklenmiştir. Böylece DB–25 ve DB–9 olmak üzere iki çeşit konnektör kullanılmaya başlanmıştır. 9 Pinli konnektörün çıkışına sebep olarak 25 pinli konektörde kullanılan uçların hepsinin kullanılmadığını gösterebiliriz. IBM uyumlu bilgisayarların arkasında kullanılan bu portların dişisi paralel, erkeği seri olduğunu belirtir. Diyelim ki, bir seri bağlantı yapacağız. O zaman kullanılacak olan kablonun ucu dişi (female) olsun ki, bilgisayarın arkasındaki erkek konnektörle bağlantı yapabilsin. Bu işlem paralel bir bağlantı için tam tersi olmaktadır. [1]

Şekil 4

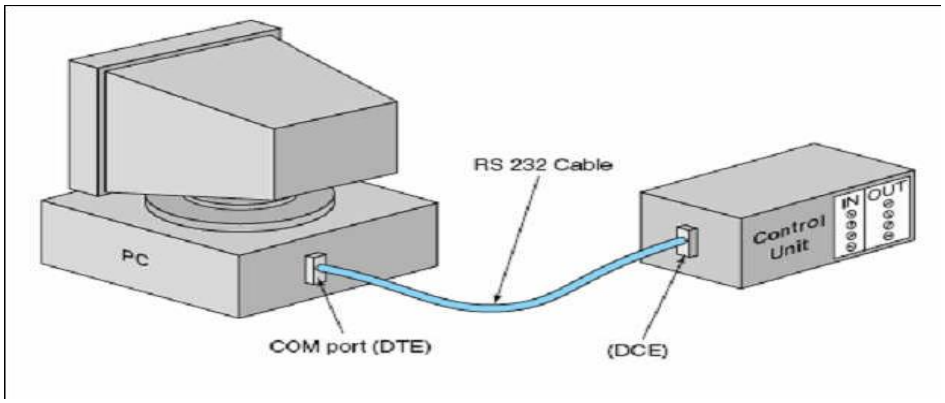
4.1.2.3 DTE-DCE Arasında Veri İletimi

DTE-DCE arasındaki iki cihaz arasında haberleşmeye örnek olarak PC - MODEM bağlantısındaki sinyallerin anlam ve kavramları aşağıdaki tabloda sıralanmıştır.[3]

9 pin	25 pin	DTE	DTE Sinyal Adı	DTE Yönü	DCE	DCE Sinyal Adı	DCE Yönü	Açıklama
1	8	DCD	Data Carrier Detect (veri taşıyıcı algılama)	IN (giriş)	DCD	Data Carrier Detect	OUT (çıkış)	Modem iletişime hazır.
4	20	DTR	Data Terminal Ready (terimal verisi hazır)	OUT	DTR	Data Terminal Ready	IN	PC iletişime hazır
5	7	SG	Signal Ground (Toprak sinyali)		SG	Signal Ground		
6	6	DSR	Data Set Ready (veri kümesi hazır)	IN	DSR	Data Set Ready	OUT	Modem iletişime hazır
7	4	RTS	Request To Send (Gönderme için istek)	OUT	RTS	Request To Send	IN	PC veri gönderimine hazır
8	5	CTS	Clear To Send (gönderime için temizleme)	IN	CTS	Clear To Send	OUT	Modem gönderim isteğine hazır
9	22	RI	Ring Indicator (Çağrı göstergesi)	IN	RI	Ring Indicator	OUT	Telefon hattından çağrı yapıldı
2	3	RxD	Receive Data (Veri Kabulü)	IN	TxD	Transmit Data	OUT	PC gönderilen baytı alır
3	2	TxD	Transmit Data (Veri İletimi)	OUT	RxD	Receive Data	IN	PC dışarıya bayt gönderir

Şekil 5

Bir RS–232 standardı ile çalışırken ve iletişimi sağlayan birim DCE (Data Communication Equipment) olarak adlandırılır. DCE en genel şekilde modem'dir. Modemler, telefon hatları üzerinden haberleşirler. Normalde bilgisayar içindeki haberleşme paralel bir şekilde yapılmaktadır. Karşımıza şöyle bir sorun çıkmaktadır. Bu da bilgisayarın dışına yapılacak olan veri akışının seri bir şekilde olmasıdır. Dolayısıyla bilgisayardaki datayı dışarıya göndermek için bunu seri bir forma dönüştürmemiz gerekir. Bu işlem UART (universal asynchronous receiver/transmitter (seri yada parallel data iletişimini sağlayan yonga, çıkış birimi)) olarak adlandırılan arabirim devreleri (IC) ile yapılmaktadır. Bu devrelerin birçok çeşidi bulunmaktadır. Aynı zamanda bu devreler bilgisayar içinde kullanılan sinyal seviyeleri olan TTL(transistor–transistor logic) (+5V ve 0V)'yi RS–232 Sinyal seviyeleri olan +12V, -12V 'a dönüştürürler. Daha sonar gönderilecek veriler, RS–232 portundan dışarıya bir RS–232 kablo ile ulaşılması istenen DCE birimine gönderilir (DCE olarak bir MODEM kullandığımızı düşünüyoruz).



Şekil 6

Görülebileceği gibi bu standart bir DTE ile bir DCE arasındaki iletişimi sağlar. Yani DTE' nin ve DCE' nin belirlenmesi gerekir. Yukarıdaki örnekte bilgisayar olarak DTE, modem olarak da DCE' yi belirledik. [1]

4.2 İşaretlerin Kodlanması:

İkili düzende sıralanmış bir veriyi kablolu bir iletişim ortamından aktarabilmek için ikili veriyi oluşturan her öğenin (ikilin) elektrik işaretine dönüştürülmesi gerekir. Çünkü telefon hattı aracılığıyla gönderilen elektrik işaretleri analog işarettir. Elektrik işaretine dönüştürülen veriler bir telefon hattı aracılığıyla alıcı bilgisayara iletilir ve tekrar elektrik işaretinden ikili veriye dönüştürülür.

4.2.1 Analog İşaretlerin Kodlanması:

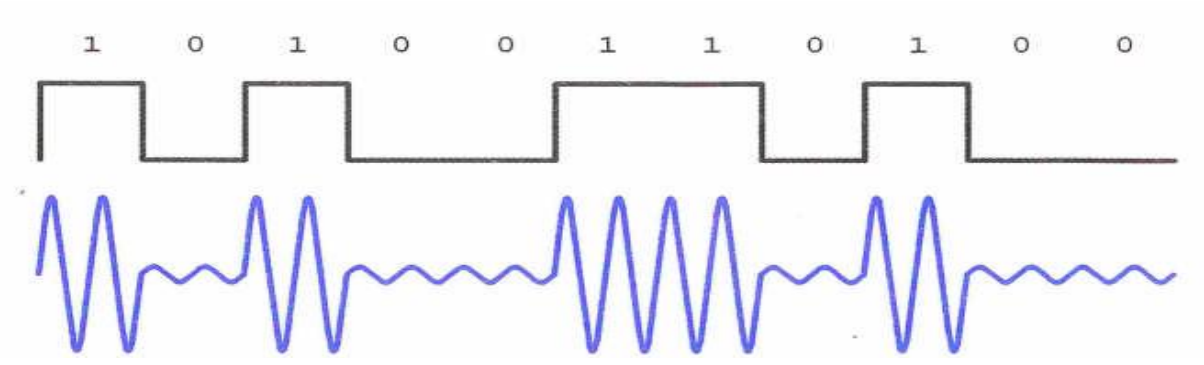
Analog bir işaret üzerinden sayısal bir veriyi göndermek (kodlamak) için, işaretin temel bileşenlerinden (genlik, sıklık ve evre) bir veya birkaçını değiştirme yöntemi kullanılır. Bu yöntemler:

1. Sayısal genlik kiplenimi, ASK (Amplitude-shift keying),
2. Sayısal sıklık kiplenimi, FSK (Frequency-shift keying),
3. Evre kaydırmalı kiplenim, PSK (Phase-shift keying)

4.2.1.1 Sayısal Genlik Kiplenimi (ASK):

ASK, sayısal verinin işaret genliğini iki ya da daha çok düzey arasında değiştirerek gösterir.

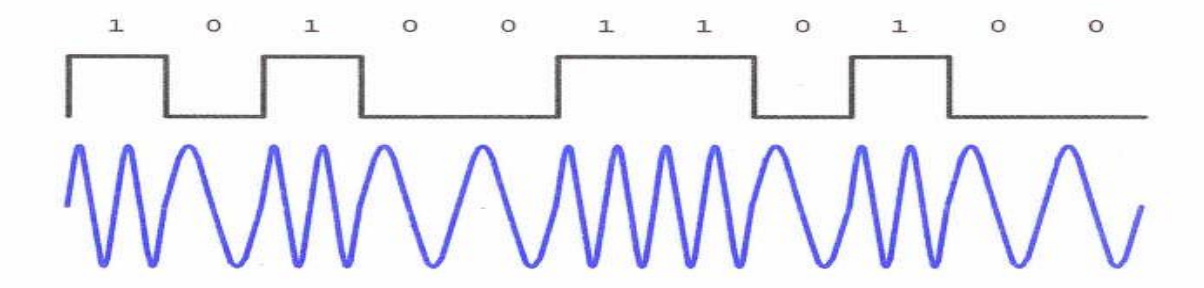
Örneğin Şekilde 1011001 ikillerinin genlik kiplemesi kullanılarak gönderilmesi örneklenmektedir. Bu örnekte işaretin sıklık ve evre bileşenleri sabit tutulurken, 1 ikili 1 voltluk genlik düzeyi ile, 0 ikili ise 0-0.05 genlik düzeyi arasında değiştirilerek kodlanmıştır.



Şekil 7

4.2.1.2 Sayısal Sıklık Kiplenimi (FSK):

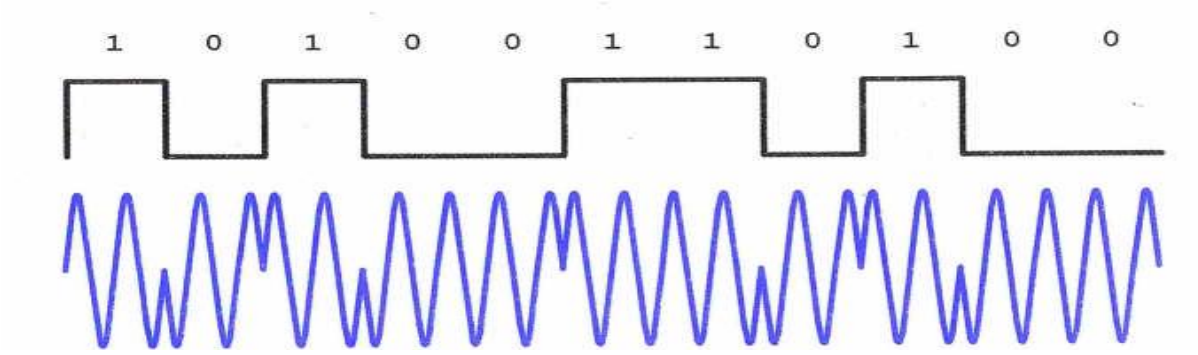
FSK, sayısal işaretleri farklı sıklıklarda kodlayarak gönderir. Şekilde, 10100110100 ikillerinin farklı sıklıklar kullanılarak gönderilmesi örneklenmektedir.



Şekil 8

4.2.1.3 Evre Kaydırmalı Kiplenim (PSK):

PSK ise, işarette bir evreden diğerine geçişi sağlayarak ikili 0 ve 1'i kipler. Örneğin, evre açısındaki 180 derecelik bir kayma sayısal işaretin değiştiğini gösterir, ikili bit eğer 1 ise 0'a veya 0 ise 1'e geçildiğini gösterir.



Şekil 9

4.2.2 Sayısal İşaretin Kodlanması:

Sayısal işaret, ikili bir verinin voltaj değişimleri kullanılarak kodlanmasıdır. Sayısal işaret iletim ortamına kodlanarak çıkartılır; alıcı taraf bu kodlamaya dayanarak kendisine gelen veriyi algılar. Kodlama yöntemi olarak temelde iki farklı yöntem kullanılır. Birinde, lojik değerlerin gösterilmesi için sabit gerilim düzeyleri kullanılırken (NRZ-L, NRZ-I), diğer yöntemde her bir bitin ortasında 0'dan 1'e veya tersi şeklinde geçiş yapılır (Manchester, Farksal Manchester).

Sayısal İşaretlerin Kodlanmasında Kullanılan Teknikler

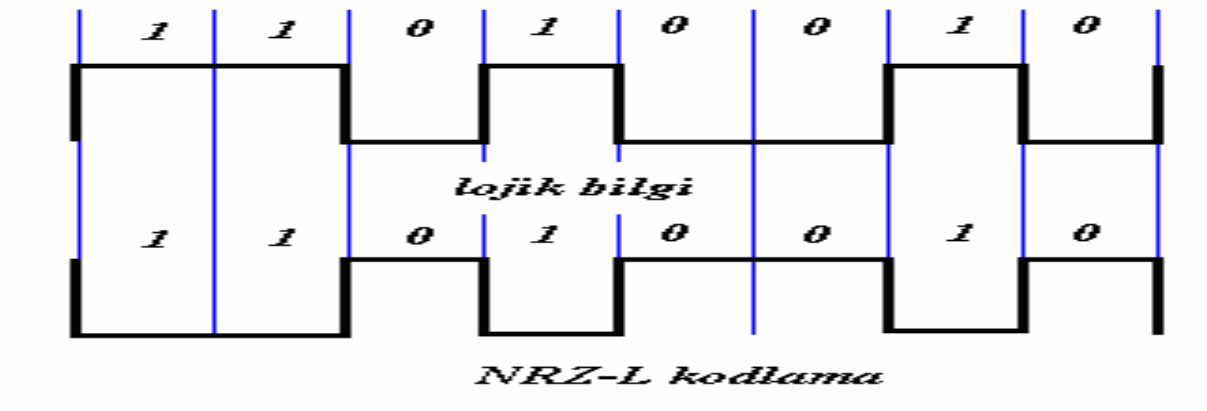
1. Sıfıra dönüşsüz kodlama (non return zero - NRZ),
2. Ters sıfıra dönüşsüz kodlama (non return zero-invertive NRZ-I).
3. Manchester kodlama (manchester encoding),
4. Fark Manchester kodlama (differential machester encoding)

4.2.2.1 Sıfıra Dönüşsüz Kodlama(NRZ):

Sıfıra dönüşsüz kodlamanın NRZ-L ve NRZ-I olmak üzere iki çeşidi vardır.

4.2.2.2 Sıfıra Dönüşsüz Kodlama(NRZ-I):

NRZ-L kodlamada 0 biti pozitif gerilim ile 1 biti negatif gerilim ile temsil edilir. Genellikle seri haberleşmede kullanılır.

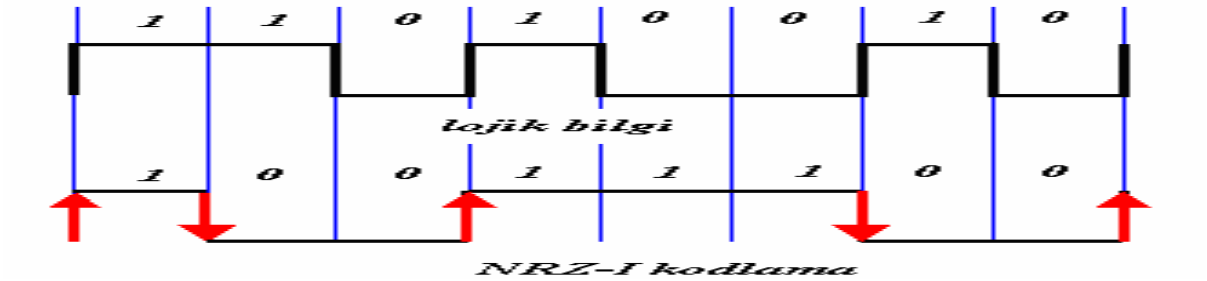


Şekil 10

Sıfıra dönmeyen kodlama tekniği, hem eşzamanlı hem de eşzamansız iletimde kullanılır. Genellikle düşük hızlı aktarımlar için uygundur. Kolay uygulanabilen bu tekniğin dezavantajı art arda aynı tür ikili veri gönderildiğinde (sürekli ikili 0 ya da sürekli ikili 1) voltaj düzeyinde hiçbir değişiklik olmamasıdır. Örneğin bir Ethernet yerel ağında binlerce ikili 1 art arda gönderilebilir. Bu durumda alıcı ve vericinin eş zamanlaması arasındaki en küçük bir kayma bile gelen işarete bakarak düzeltilemez.

4.2.2.3 Ters Sıfıra Dönüşsüz Kodlama(NRZ-I):

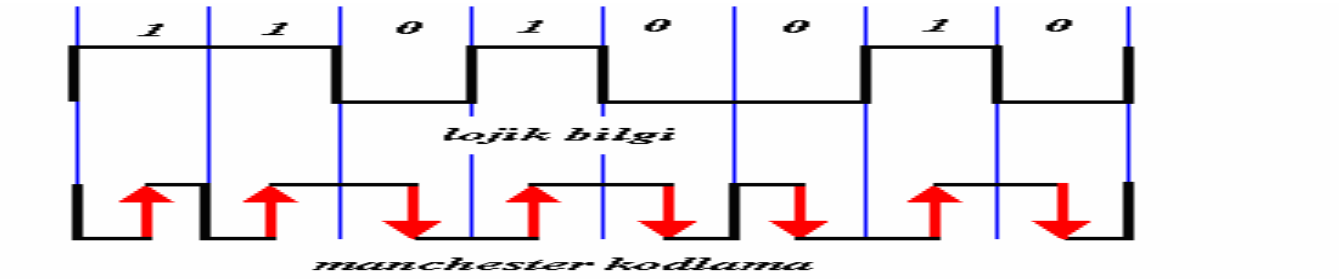
NRZ-I kodlamada ise 1 biti önceki bitin tersi, 0 biti önceki bitin aynı olarak kodlanır. Diğer bir deyişle 0 biti kodlanırken gönderilen sinyalde hiçbir değişme olmaz aynen devam eder, 1 biti yollanırken gönderilen sinyal önceki bitin tersine çevrilir.



Şekil 11

4.2.2.4 Manchester Kodlama:

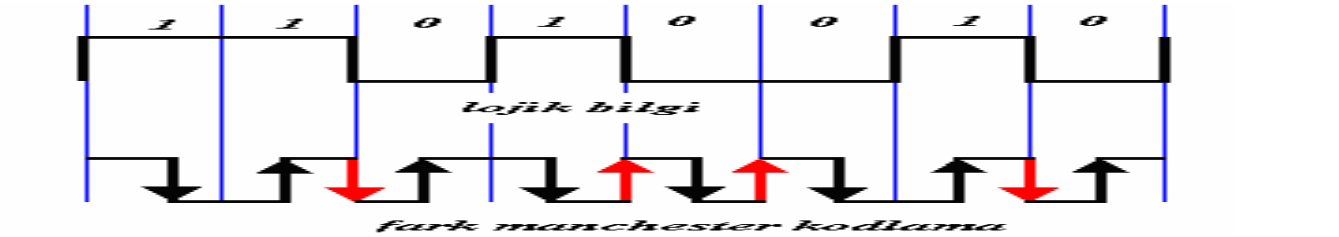
Manchester kodlamada, bitlerin tam orta yerlerinde, 1 biti 0 dan 1 e geçiş ile 0 biti 1 den 0 a geçiş ile ifade edilir. Böylece gerçek bilgi değiştirilmeden bilginin kodlanması değiştirilmiş olur.



Şekil 12

4.2.2.5 Ayrımsal Manchester Kodlaması:

Fark Manchester Kodlamada bitlerin orta noktalarında yine 0 dan 1 e ve 1 den 0 a geçişler olur. Fakat burada geçiş yönlerinin bir önemi yoktur yani 0 için 0 dan 1 e, 1 için 1 den 0 a geçişler olabilir. Bu kodlamada önemli olan bit başlangıç anlarında geçiş olup olmadığıdır. 0 biti için başlangıç anında geçiş vardır, (şekilde kırmızı oklar) 1 biti için başlangıç anında geçiş yoktur. Diğer bir deyimle sinyal, 1 biti için önceki konumu aynen devam ettirirken 0 biti önceki konumun tersine çevrilir. [1]



Şekil 13

4.3 Kablosuz Yerel Ağ (Wireless Local Area Network)

Kablosuz yerel ağ, kablolu iletişime alternatif olarak uygulanabilecek esnek bir iletişim sistemidir. Radyo frekans (RF) teknolojisini kullanarak havadan bilgi alışverişi yapar böylece kablolu bağlantı miktarını azaltır. Kablosuz yerel alan ağı (Wireless Local Area Netowrk) , kablolu ağların yerini alan hatta bu ağlara göre daha fazla fonksiyonları bulunan yeni haberleşme şeklidir. Radyo frekans (RF) teknolojisini kullanan WLAN ile veri iletimi/alımı havadan, duvarlar arasından geçerek sınır tanımayan bir iletişim kablosuz olarak sunulmaktadır. Bazı hız kısıtlamaları dışında WLAN iletişimi, geleneksek LAN iletişim teknolojilerinin tüm özelliklerini kapsamakta hatta daha da fazla özellik içerebilmektedir.

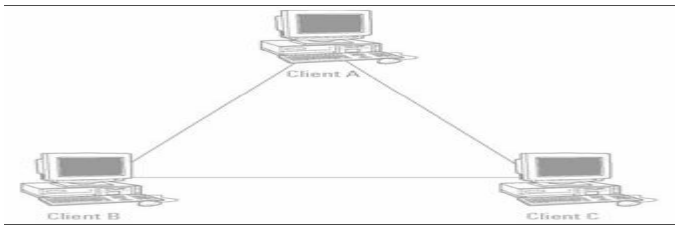
4.3.1 Kablosuz Yerel Ağların Çalışması

Tipik bir kablosuz yerel ağ uygulamasında, erişim noktası denilen hem alıcı hem verici konumundaki cihaz standart kablolamayla, kablolu ağa bağlanır. Erişim noktası kablolu ağ omurgası ve kablosuz ağ arasında veri alışverişini üstlenir. Erişim noktası genelde yüksek bir noktaya konur fakat istenilen kapsama alanı sağlandıkça her noktaya konulabilir. Uç noktalar ise kablosuz ağa, kablosuz ağ adaptörleriyle, dizüstü bilgisayarda PCMCIA kartlarla, masaüstü bilgisayarlarda ise ISA kartlarla erişirler. Kablosuz ağ adaptörleri sunucudaki ağ işletim sistemi ile manyetik dalgalar arasında bir anten yardımıyla köprü oluştururlar.

Standart kablosuz ağlar şu 2 moddan biri ile çalışırlar.

4.3.1.1 Peer-to-peer (Makinadan makinaya) Model

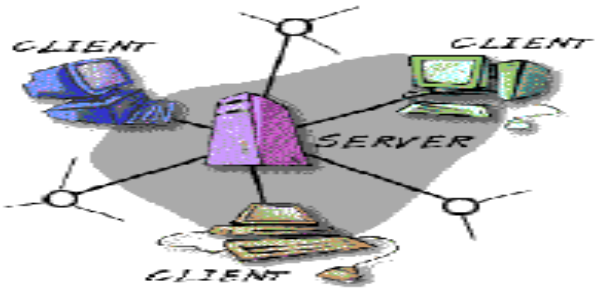
Bu mod, birbirleri ile iletişim mesafesinde olan kullanıcılar için tasarlanmıştır.



Şekil 14

4.3.1.2 Client/Server (İstemci/Sunucu) Modeli

Burada tüm bilgisayarlar erişim noktası (acces point) adlı ürünle mevcut olan kablolu ağa bağlanmıştır.



Şekil 38: Client/Server Modeli

Şekil 15

4.3.2 Kablosuz Ağ Türleri

Bugünlerde 4 tip kablosuz ağ vardır. Bunlar ucuz ve yavaş olandan, pahalı ve hızlı olana doğru sıralanırsa

4.3.2.1 BlueTooth

Bluetooth henüz çok fazla yaygın bir kullanıma sahip değil ve bilgisayarlar arasında yüksek hızlı veri transferinde yer alması beklenmiyor. Kısa mesafelerde kullanılır, cep telefonlarındaki iletişimi örnek verebiliriz.

Şekil 16

4.3.2.2 IrDA (Infrared Data Association)

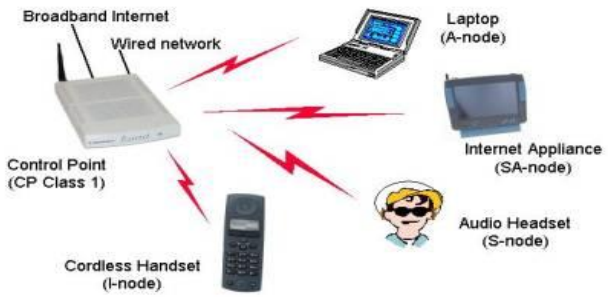
IrDA, kızıl ötesi direkt ulaşım olarak karşımıza çıkıyor ve iletişimde kızılötesi ışın vurumları kullanan cihazlar için standarttır. IrDA aygıtlar kızılötesi ışınlar kullandığından beri diğeri ile iletişim kurabilmek için aralarında direkt bir görüş açısı bulunmak zorundadır. IrDA kullanan kablosuz ağlar veri transferi için en fazla 4 Mpbs kullanabilmektedir. Kullanım Alanları: Cep Telefonları, PDA'lar, dizüstü bilgisayarlar.

Şekil 17

4.3.2.3 HomeRF

Home RF'ler ortak kablosuz iletişim protokolüne sahiptir. Temel olarak SWAP (Shared Wireless Acces Protokol)'a göre geliştirilmişlerdir. Hızı 1 Mbps ile 2 Mbps

arasındadır, menzili ise 23 ile 38 metre arasındadır. Küçük ağlarda kullanılır ev ağı gibi. Eğer ağda video kullanmak ve oyun oynamayı düşünmüyorsak bu ağ bizim için yeterlidir.



Şekil 18

4.3.2.4 WECA (Wi-Fi)

Wi-Fi kablosuz ağlar, HomeRF' e göre tamamen farklı bir yönde gitmektedir. Wi-Fi ağlar ev kullanıcılarından çok ofis kullanıcılarını hedeflemektedir. Wi-Fi 'nin IEEE de karşılığı 802.11b'dir ve kablosuz bağlılık (Wireless Fidelity) olarak karşımıza çıkmaktadır. Wi-Fi aygıtlar, eğer mümkünse 11 Mbps hızına ulaşmaktadır. [6]

Şekil 19

4.4 Lan Bağlantı Standartları

Local Area Network Bağlantıları, kullanılan network (Ethernet) kartının ve kablo altyapısının hızına bağlı olarak önceleri BNC standardında, günümüzde ise UTP standardında yaygın olarak kullanılmaktadır. Önümüzdeki yıllarda standart haline gelecek olan fiber optik altyapı ise fiyatından dolayı henüz çok ciddi altyapılarda kullanılmaktadır.

4.4.1 Bnc Alt Yapısı

BNC altyapısı, tüm ağda tek bir kablo kullanma şeklindedir. Yani kablo 1 numaralı bilgisayardan başlar, son bilgisayara kadar uzanır. Her bilgisayarın olduğu yerde kabloya

BNC soket takılır. Kablonun en başına ve en sonuna da sonlandırıcı soketler takılır. Bu iki soket arasındaki toplam direnç 52 OHM olmalıdır.

4.4.2 Utp Sistemler

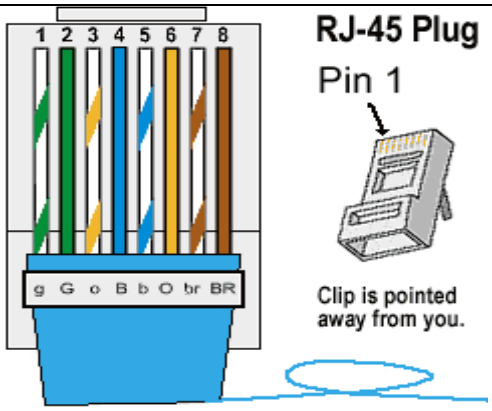
BNC sistemlerin hız dezavantajını aşmak için, gönderilen ve alınan sinyallerin ayrı kanallardan yapılacağı, çok kablolu sistemler düşünülmüştür. Böylece içinde 8 adet kablo bulunan RJ-45 kabloların kullanıldığı UTP sistemler devreye girmiştir. Bu sistemin belirgin özelliği, HUB adını verdiğimiz ağ sinyal dağıtıcı ve düzenleyici aygıta ihtiyaç duymasıdır. Her makineden HUB'a bir utp kablo gelmelidir. Bu görüntüden dolayı bu sistem YILDIZ'A benzetilir.

4.4.3 Rj 45 Konnektör

Atipi ve B tipi olmak üzere iki tip bağlantı şekli vardır. A Tipi Bağlantı, Dünya standardıdır. Ancak ülkemizde genelde B tipi bağlantı kullanılmıştır. Soldan sağa renk sıralaması dikkate alınarak. Kablonun ucundaki iki jaka aynı bağlantı yapılır.

A Tipi Bağlantı

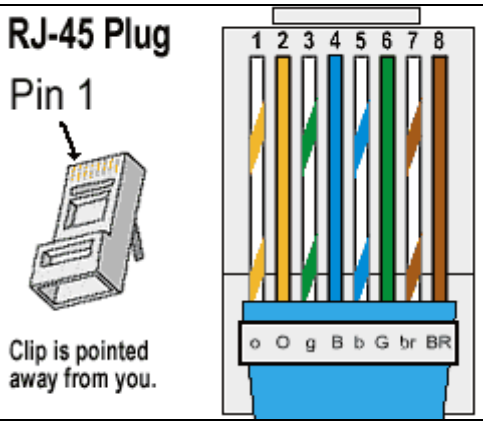
1 nolu pin: yeşil-beyaz
2 nolu pin: yeşil
3 nolu pin: turuncu-beyaz
4 nolu pin: mavi
5 nolu pin: mavi-beyaz
6 nolu pin: turuncu
7 nolu pin: kahve-beyaz
8 nolu pin: kahve



Şekil 20

B Tipi Bağlantı

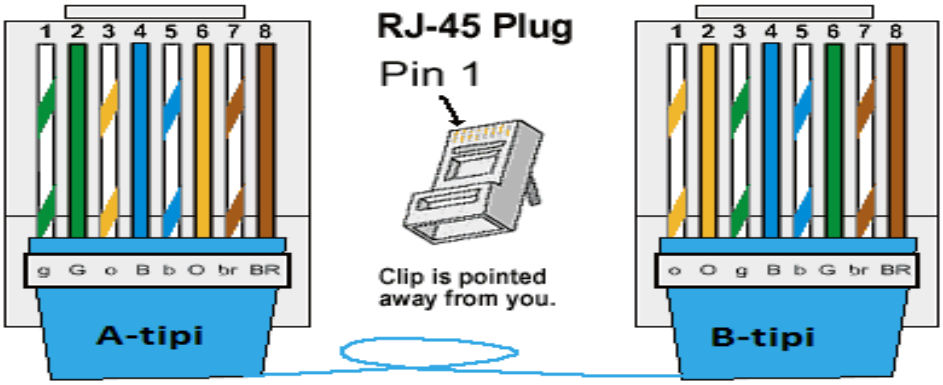
1 nolu pin : turuncu-beyaz
2 nolu pin : turuncu
3 nolu pin : yeşil-beyaz
4 nolu pin : mavi
5 nolu pin : mavi-beyaz
6 nolu pin : yeşil
7 nolu pin : kahve-beyaz
8 nolu pin : kahve



Şekil 21

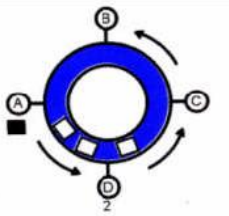
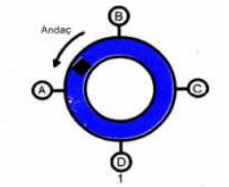
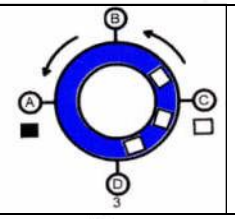
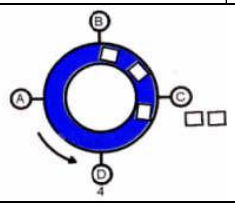
4.4.4 Cross Bağlantı

UTP kablosu kullanarak yalnızca iki makineyi HUB kullanmadan bağlayabiliriz. Yapılması gereken kablonun bir ucundaki jaka A tipi bağlantı, diğer ucundaki kabloya da b tipi bağlantıyı uygulamaktır. [7]



Şekil 22

4.4.5 Tr Bağlantı Konnektörü

	A bilgisayarı çerçeveyi halka üzerinden göndermeyi başlatır.
	A bilgisayarı kontrol andacın üstteki komşusundan kendisine gelmesini bekler.
	C bilgisayarı kendisine gönderilen çerçeveyi kopyalar. Çerçeve halka etrafında dolaşmaya devam eder.
	A bilgisayarı çerçeve başının alınmasını ve kendisine yeniden dönmesini bekler ve çerçeveyi siler.

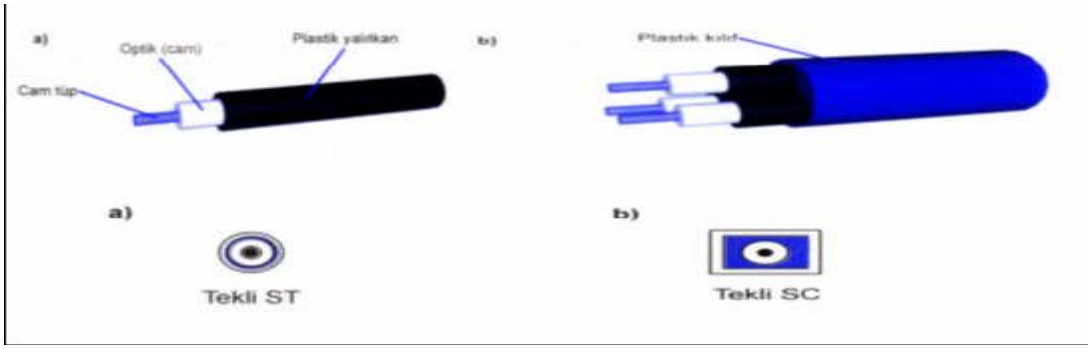
4.4.5.1 Konnektör ve Yapısı

- Bu ağlarda kullanılan kablonun fiber veya bakır olmasına göre konnektör türleri farklıdır.
- Jetonlu halka da farksal manchester kodlaması ve buna ek olarak çerçeve ayracı anlamında her çerçeve arasında boş bir bit kullanır.
- TR konnektörünün bağlandığı noktaya "MAU"(MEDİA ADAPTOR UNİT) denir.

4.4.6 Fiberoptik Konnektör Türleri

4.4.6.1 Fiberoptik Kablo Türleri

Veri iletimini ışınlarla sağlar. Optik bir iletişim sisteminin 3 bileşeni vardır: Işık kaynağı, iletişim ortamı ve algılayıcılardır. Işık kaynağı(ışık yayan diyot-LED) tarafından gerçekleştiren bir ışık atımı sayısal 1'i gösterirken, ışığın kaybolması sayısal 0'ı gösterir. İletişim ortamı tarafından algılayıcıya(FOTODİYOT) aktarılan ışınlar elektrik sinyaline çevrilir.



Şekil 23

ST SC

Şekil 24

4.4.7 AUI ve MII Standartları

Bir örnekle anlatmaya çalışalım. Ethernet portumuz var ve bu ethernet portumuz 10Base-T standardına uygun olsun. Öyleyse bu porta 10Base-T standardında bir bağlantı yapılabileceği anlamına gelir. Aynı cihaz farklı arayüz standartlarına sahip ağlarda kullanılmaz. Dolayısıyla üretici firmalar makine üzerine ağlar arası bağlantı sağlayan bir veya birkaç tane esnek port arayüzü koymaktadır. Bunlar;

4.4.7.1 AUI(Attachment User İnterface)

10Mbps ethernet uygulamalarında fiziksel katman kablolama esnekliği sağlamak için

4.4.7.2 MII(Medium Independent Interface)

100Mbps ethernet uygulamalarında kullanılır.[1]

Şekil 25 - AUI (DB15)

4.5 KAYNAKLAR

- http://www.asafvarol.com/dnotlar/bag/b_ag_kitabi.zip
- http://www.teknohaber.net/makale.php?id=30217
- www.swisstech.ca/PinoutRS232.html
- http://www.x-paylasim.com/dijital-uydu-cihazlari/5139-rs-232ye-giris.html
- http://www.bilgiportal.com/v1/idx/35/911/Network/makale/OSI-Katmanlar.html
- http://www.gencmuhendis.org , http://www.uzmanweb.net
- http://img1.loadtr.com/b-315925-RJ45_Ba%C4%9Flant%C4%B1%5Balax%5D.gif

5 BÖLÜM

5.1 TAŞIMA KATMANI

Taşıma Katmanı ağın karmaşıklığını üst katman işlevlerinden gizlemek için tasarlanmıştır. Aktarım katmanı olarak da bilinir. Bilginin son alıcıda her türlü hatadan arındırılmış olarak elde edilmesini sağlar. Taşıma katmanının oluşturduğu bilgi bloklarına bölüm (segment) denir. Bunlar son alıcıya sırası bozulmuş olarak gelirse, düzgün olarak sıralanmalıdır. Bunun için bölümler numaralanır. Yüksek düzey mesajları bölümlere ayırır ve bu bölümleri güvenilir biçimde oturum katmanına ya da daha üst katmanlara iletir.

Taşıma katmanı genelde güvenilir veya bağlantı-tabanlı servislerin yokluğunu dengelemektedir. Güvenilir kelimesi tüm verinin her zaman ulaştırılabileceği anlamına gelmemektedir. Örneğin eğer kabloda bir kopukluk olursa Aktarım Katmanı verinin ulaştırılmasını garanti edemez. Halen, güvenilir aktarım katmanı protokol gerçekleştirimleri genelde verinin alındığını onaylar ya da reddeder. Eğer alıcı birimde veri düzgün biçimde alınamamışsa, aktarım katmanı verinin yeniden gönderilmesini başlatabilir ya da üst katmanları haberdar eder. Üst katmanlar gerekli düzeltme işlemini gerçekleştirebilir ya da kullanıcıya bazı seçenekler sunabilir [1].

5.1.1 Taşıma Katmanı Nasıl Çalışır?

Taşıma katmanı üst katmanlardan gelen veriyi ağ paketi boyutunda parçalara böler. TCP, UDP, SPX protokolleri bu katmanda çalışır. Bu protokoller hata kontrolü gibi görevleri de yerine getirir. Bu katmanda veriler kesim (segment) halinde taşınır. Taşıma katmanı üst katmanlara taşıma servisi sağlar ayrıca ağın servis kalitesini artırır (QoS – Quality of Service). Taşıma katmanı verinin uçtan uca iletimini sağlar. Verinin hata kontrolü ve zamanında ulaşıp ulaşmadığı kontrol edilir. Taşıma katmanı ayrıca veriyi üst katmanlara taşıma görevi yapar [2].

5.1.2 Taşıma Katmanının İki Önemli Fonksiyonu

- **Güvenlilik:** Veri transferinin aksaksız bir şekilde hedefe ulaşmasını, ulaşmazsa bu işlemin tekrar edilmesini sağlayan fonksiyondur.
- **Akış Kontrolü:** Kaynak bilgisayarın gönderdiği veri bazen hedef bilgisayarın kabul edebileceği maksimum miktardan da fazla olabilir. Böyle olunca akış kontrolü fonksiyonu çalışır [3].

5.1.3 TCP (Transmission Control Protocol)

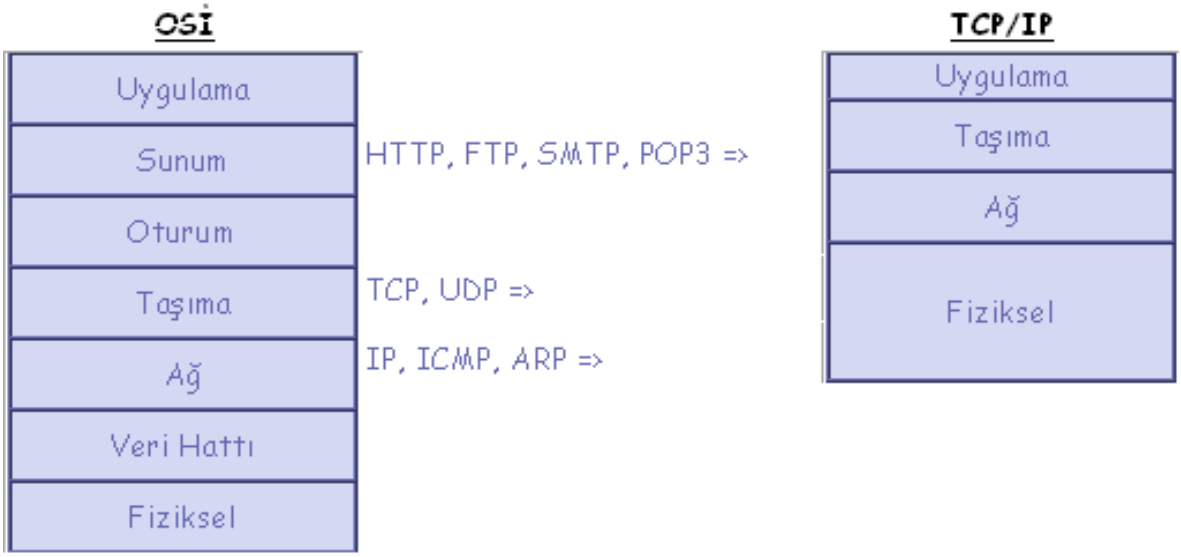
TCP/IP protokol takımının iki aktarım katmanı protokolünden birisidir.

Gelişmiş bilgisayar ağlarında paket anahtarlamalı bilgisayar iletişiminde kayıpsız veri gönderimi sağlayabilmek için TCP protokolü yazılmıştır. HTTP,HTTPS, POP3, SMTP ve FTP gibi internet'in kullanıcı açısından en popüler protokollerinin veri iletimi TCP vasıtasıyla yapılır.

TCP, gönderilen veriler için özel bir TCP kabul (Ethereal gibi araçlarda ve birçok kaynakta kısaca *TCP ACK* da denir) paketi gönderir. Bu paket, gelmiş olan paketlerden hangi byte'a kadar olan kısmının doğru olarak alındığını gösterir. Gönderen taraf, kabul gelmediği sürece paketi arka arkaya birkaç kez yollar [4].

5.1.4 Tcp/Ip Modeli

Unix tarafından OSİ referans alınarak geliştirilmiş bir iletişim modelidir. Gerçek anlamda kullanılan tek protokoldür. Sebebi donanımdan bağımsız oluşudur. Yani bu protokol kullanılarak Macintosh ile PC arasında gerekli yazılım ve ağ kurulabilirse bu iki bilgisayar birbirleriyle konuşabilirler. TCP\IP tek bir protokol değil birden fazla protokolü içinde barındıran bir protokoller ailesidir. TCP (Transmission Control Protocol) ve IP (Internet Protocol) protokollerinin birleşiminden oluşmaktadır.En yavaş ama En güvenilir modeldir. 4 Katmandan oluşur. Her katmanda tanımlı protokoller vardır ve aşağıda sıralanmıştır [5].



5.2 Uygulama Katmanı

OSİ'deki ilk üç katmana karşılık gelir. Bu katmanda genellikle değişik uygulamalarla tanımlanmış protokoller vardır. Bu protokollerden bazıları http, ftp, smtp, pop3'tür. Bu protokoller bir alt katman ile ilişkiyi portlarla sağlarlar.

5.3 Taşıma Katmanı

OSİ'deki Taşıma Katmanına karşılık gelir. İki adet Protokol kullanır : TCP ve UDP TCP ve UDP protokollerinde gönderici ve alıcı iletişimine başlamadan önce birbirleriyle anlaşırlar. Bu anlaşmalar istek ve onay şeklindedir. Bu nedenle bu protokole bağlantı yönelimli (Connection Oriented) iletişim adı verilir.

Görevleri :
- Bir üst katmandan gelen verinin uygun parçalara (segment) ayrılması (segmentlerin boyu 64 kb'ı geçmez.).
- Her bir parçaya alıcı kısımda aynı sıraya konulabilmesi için sıra numaralarını verilmesi. Bu aynı zamanda kaybolan veya bozuk gelen parçaların tekrarlanmasını sağlar. [Her bir parçaya ilişkin bilgiler başlık (header) olarak o parçaya (segmente) eklenir.]

5.4 Ağ Katmanı

OSİ'deki Ağ Katmanına karşılık gelir. IP, ICMP ve ARP gibi protokoller kullanır. Taşıma Katmanında oluşan segmentlere birer header daha eklenerek bu segmentler paket haline getirilir.

5.5 Fiziksel Katman

OSİ'deki son iki Katmana karşılık gelir. Bazılar ARP protokolünün burada yer aldığını söylerler. Bu katmanda Taşıma katmanında oluşan paketlere yeni bir header eklenerek paketler fiziksel adreslerle donatılırlar ve frame adını alırlar. Bu düzeyde bilgisayarlar birbirlerini fiziksel adresler sayesinde tanırlar.

5.6 Özetle Tcp

- Bağlantının kurulması ve sonlanması (Connections)
- Güvenilirlik (Reliability)
- Akış kontrolü (Flow control)
- Çoğullama ((Multiplexing)
- Temel veri aktarımı (BAsic data transfer)
- Çift yönlü işlem (Full dublex process) [6].

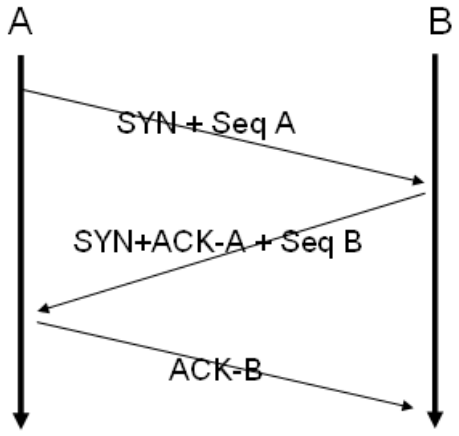
5.7 Bağlantı Kurulumu

A bilgisayarı B bilgisayarına TCP yoluyla bağlanmak istediğinde şu yol izlenir:

- A bilgisayarı B bilgisayarına TCP **SYN**chronize mesajı yollar
- B bilgisayarı A bilgisayarının isteğini aldığına dair bir TCP **SYN**+**ACK**nowledgement mesajı yollar
- A bilgisayarı B bilgisayarına TCP **ACK** mesajı yollar
- B bilgisayarı bir **ACK** "TCP connection is **ESTABLISHED**" mesajı alır

Üç zamanlı el sıkışma adlı verilen bu yöntem sonucunda TCP bağlantısı açılmış olur [7].

Aşağıdaki şekilde bu olay anlatılmaktadır [8]:



5.8 TCP Fonksiyonları

TCP (Transmission Control Protocol) güvenilir bir bağlantı temelli, uçtan uca protokoldür. Alıcının paketleri doğru bir şekilde aldığını belirten bir el sıkışma mekanizmasını içinde barındırır. TCP günümüzde en çok kullanılan protokollerden biridir. Ancak içinde bulunduğumuz ağlarda, protokol istenildiği kadar güvenilir olmamaktadır. Çünkü, bazı nedenlerle paket kayıpları yaşanmaktadır. Örneğin, ağda bir hata meydana gelmesi, ağda tıkanıklık oluşması ve yönlendiricilerin paketleri düşürmesi gibi. Burada TCP'nin fonksiyonları önem kazanmaktadır. TCP bir paket kaybı oluşması durumunda buna tepki verir ve oluşan hatayı düzeltmeye çalışır. TCP bir paket yolladığında arkasından bir zamanlayıcıyı da beraberinde başlatır. Eğer bir *ACK* (*ACK*nowledgement) zaman aşımı periyodu içerisinde dönmemiş ise o zaman o segmenti yeniden gönderir[9].

Şu an kullanılan taşıma protokolleri yeni uygulama alanlarında ve yeni ağ teknolojilerinde kullanıldığı zaman bir takım kısıtlamalarla karşılaşmaktadır. Örneğin,

multimedya uygulamaları tıkanıklık kontrolüne ihtiyaç duyarlar ancak gerekli bir şekilde düzenleme ve güvenilir bir dağıtımda isterler. Bunu ne TCP ne de UDP protokolü sağlamaz. Bu nedenle performansı artırıcı yeni tasarımlar insanların kafalarında oluşmaya başlar. Paket kayıplarının oluştuğu ortamlarda TCP performansını geliştirmeye yönelik çalışmalar yapılmıştır. TCP düşük bant genişliği ve düşük gecikme durumlarında işe yaramıştır ancak günümüzdeki şartlarda yeterli olması mümkün değildir [10]. Bu nedenle yüksek hızlı ve uzun mesafeli ağlar için farklı sürümler geliştirilmiştir. Bu sürümlerde yüksek bant genişliğinden dolayı oluşan gecikme ve zaman kayıpları en aza indirilmiştir.

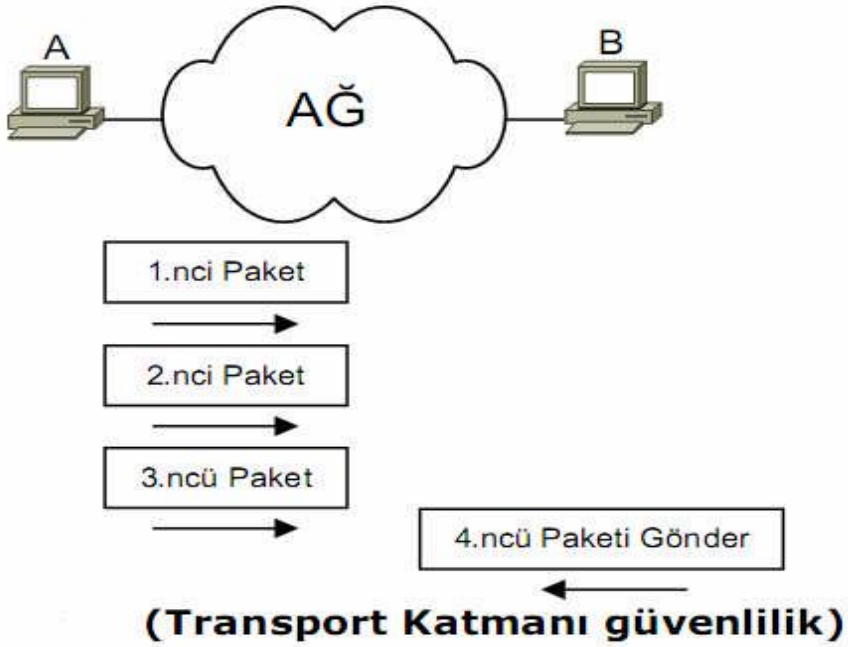
TCP'nin genel olarak iki önemli fonksiyonu vardır. Bunlar;

- Güvenlilik (Reliability)
- Akış Kontrolü (Flow Control)

5.8.1 Güvenlilik (Reliability)

Bildiğimiz gibi alt katmanlar güvenilir olmayan bir iletim ortamı sunuyor. Uygulamalar bu iletim sırasında oluşacak problemleri gidermek için karmaşık kontrol mekanizmaları geliştirmek zorundalar. Bu yükü her bir uygulama için tekrarlamak yerine internette çalışacak güvenilir bir protokole ihtiyaç var.

Akış yönelimli iki uç arasında veri iletimi olurken veriler bitler halinde akar ve 8 bitlik parçalarla iletilir. Kaynaktan bu 8 bitlik paketler hangi sırada çıkmışsa hedefe de aynı sırayla gelir[11].



A bilgisayarı B bilgisayarına 3 data paketi göndermiş ve bu dataların alındığını onaylamak istemektedir. Gönderilen her bir data Transport Katmanı protokolü tarafından numaralandırılmaktadır. B bilgisayarı da gönderilen dataları aldığını ve bir sonraki data paketlerini beklediğini belirten bir onay mesajı gönderir. Bu mesaja gönderim onayı (forward acknowledgement) denir. Eğer A bilgisayarının gönderdiği data paketlerinden 2. paket B bilgisayarı tarafından alınmamışsa bu A bilgisayarına bildirilir. A bilgisayarı da ya sadece 2 nolu paketi ya da 2'den sonraki bütün paketleri tekrar gönderir[12].

5.8.2 Akış Kontrolü (Flow Control)

İletişim halindeki bilgisayarlardan gönderen bilgisayar, data paketlerini alan bilgisayarın alabileceği kapasiteden daha fazla olabilmektedir. Dolayısıyla datayı alan bilgisayar, data paketlerini yok edebilmektedir. Ayrıca gönderen bilgisayar, ağda bulunan anahtar ve yönlendirici gibi ağ cihazlarının kapasitesini zorlayabilmektedir. Aynı şekilde bu cihazlar da data paketlerini yok edeceklerdir. Bazen datayı alan bilgisayarın arabelleği (buffer) yeteri kadar büyük olmayabilir veya işlemcisi çok miktarda datayı işliyor olabilir. Bütün bu sebeplerden dolayı tıkanma (congestion) olmaktadır. Bu tıkanıklığı giderebilmek için data gönderim miktarını kontrol etmek üzere akış kontrol sistemi kullanılmaktadır. Bu sistemde 3 metod kullanılmaktadır[13].

Bunlar;

• Ara Bellekleme (Buffering)

• Tıkanıklıktan Kaçınma (Congestion Avoidance)

• Pencereleme (Windowing)

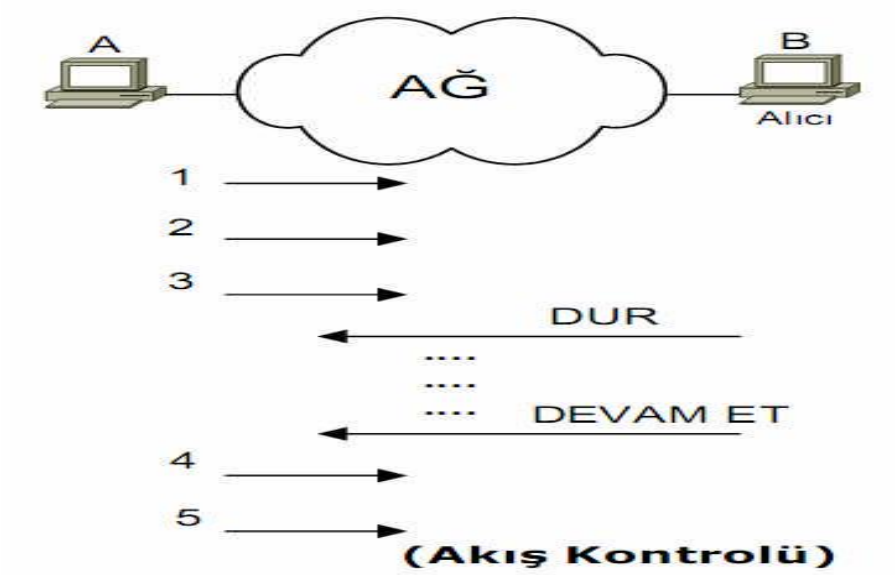
5.8.3 Ara Bellekleme (Buffering)

Data akış hızına müdahale etmeden alınan data, bilgisayarın kapasitesini aştığı durumlarda bilgisayarın ara belleğinde yer açma işlemidir. Böylece belli bir süre ara bellekte tutulan data,bilgisayarın yükü azaldığı zaman hemen işleme sokulmaktadır[14].

5.8.4 Tıkanıklıktan Kaçma (Congestion Avoidance)

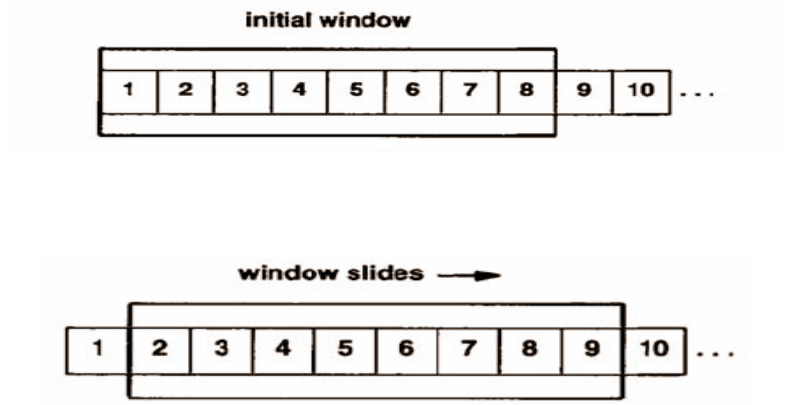
Tıkanıklık yani congestion oluşması büyük bir hattan veri akışının gelmesi ve küçük bir hattan da çıkışının yapılması durumunda meydana gelir. Tıkanıklık ayrıca bir router'a çıkış kapasitesinden fazla giriş verisinin gelmesinden dolayı da oluşur. Bir göndericide iki tür paket kaybı oluşur: İlki bir zamanaşımı (timeout) oluşumasından, ikincisi ise duplike

ACK'ların alınmasıyladır. Bununla beraber, bir hasardan dolayı oluşan paket kaybı oranı çok küçük olarak hesaplanmıştır. Bu nedenle, bir paket kaybının görülmesi, kaynak ile hedef arasında bir tıkanıklık olduğunu işaret etmektedir[15].

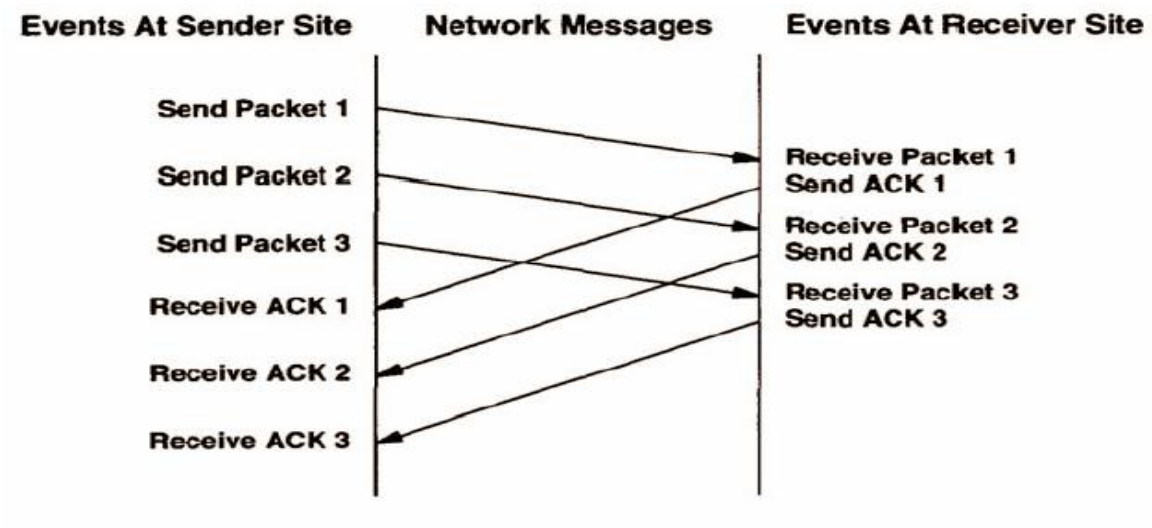


5.8.5 Pencereleme (Windowing)

İletimin daha verimli gerçekleşmesini sağlamak için geliştirilmiştir. Kayan pencerede birbiri ardına dizilmiş paketler olduğunu düşünelim. Protokol dizilen paketlerin üzerine sabit uzunlukta bir pencere yerleştirir ve bu pencere içerisinde kalan paketleri iletir ve iletilen paketlere iletildi bilgisi geldikçe pencereyi kaydırır.



Kayan pencere protokolünün verimliliği pencere boyuna ve ağın iletim hızına bağlıdır. Protokol hangi paketlerin teyit edildiğini bilir ve teyit edilmeyen paketler için bir zamanlayıcı tutar. Paket kaybolmuşsa zamanlayıcı bittiğinde paket tekrar iletilir. Pencere kaydırılırken teyit edilmiş bütün paketler geçilir[16].



5.8.6 UDP(user datagram protokol)

UDP (User Datagram Protocol – Kullanıcı Datagram Protokolü) TCP ile birlikte aynı taşıma katmanında bulunan, kararlı bir iletim gerektirmeyen uygulamalar için geliştirilmiş basit bir iletim protokolüdür.
Birbirine bağlı bilgisayarların oluşturduğu bir ağ içerisinde paket anahtarlamalı bilgisayar iletişiminin datagram modunu kullanılabilir hale getirmek için tanımlanmıştır. TCP gibi bağlantılı, güvenli, garantili bir iletim yapmaz. Aklınıza bu soru gelebilir. UDP güvenli değil, neden kullanılıyor? UDP, TCP'den daha hızlı çalışıyor ve daha hızlı iletim yapıyor. TCP her veri paketini gönderdikten sonra alıcıdan onay bekler, paket hatalı iletilmiş mi, bağlantı zayıflamış mı, alıcı doğru paketi mi almış, araya başka bağlantılar mı girmiş, karşı tarafın alabileceğinden daha fazla mı veri gönderilmiş, onay gelmemiş paketleri belirlendi mi, onlar tekrar gönderildi mi gibi birçok olasılığı sürekli kontrol eder. Bu olasılıkların her biri gerçekleştiği anda ayrı ayrı çözümleniyor ve veri iletimi kesinlikle tam olarak gerçekleştirilmiş oluyor. Buraya kadar her şey güzel de, bizim göndereceğimiz verilerin arada kayıplara uğraması çok da önemli değilse ve hızlı bir şekilde iletilmesini istiyorsak TCP bizi yavaşlatacaktır. Örneğin İnternet üzerinde ses iletimi, görüntü iletimi, bunlar hızlı iletilmesi gereken bilgilerdir. Arada birkaç paket kayba uğrasa seyreden bunu fark edemez. Ya da bir karelerin birkaçının sırası karışsa, saniyede geçen 25 karenin arasında bunu kim fark edebilir? Bu kontroller yüzünden görüntünün kare kare gelmesini, duraklamasını kimse istemez. İşte bu noktada UDP devreye giriyor ve bu kontrollerin hiçbirini yapmaz. İki bilgisayar arasında bir bağlantı kurulduğu anda karşı bilgisayarın paketleri başarılı bir şekilde aldığını varsayarak sürekli bir gönderim yapar. Göndereceği veri bittikten sonra da bağlantıyı kapatır. Böylece bizim görüntü bilgileri kontrollere uğramadan, hızlı bir şekilde iletilmiş olur. Biz de arada birkaç kare kaybı fark bile etmeyiz. Şimdi UDP'yi biraz tanıyalım.

UDP protokolü üst katmanında bulunan uygulama programlarına, minimum protokol mekanizması kullanarak hedef bilgisayarda bulunan diğer uygulama programlarına mesaj gönderebilmeleri için bir prosedür sağlar. TCP bağlantı merkezlidir (connection oriented), bağlantının sağlamlığı önceliklidir, UDP ise işlem merkezlidir (transaction oriented), öncelik veri iletme işlemindedir. UDP rastgele iletim yapmaz. Hata kontrolü yapar fakat TCP kadar detaylı değildir. TCP'nin verdiği ulaştırma ve mükerrer iletim yapmama garantisi vermez. Bu yüzden sıralı bir şekilde güvenli ve güvenilir bir iletim gerektiren uygulamalar UDP değil TCP kullanırlar.

5.8.6.1 UDP başlığı

UDP datagramların belirli sıralara konmasının gerekli olmadığı uygulamalarda kullanılmak üzere dizayn edilmiştir. TCP'de olduğu gibi UDP' de de bir başlık vardır. Ağ yazılımı bu UDP başlığını iletilecek bilginin başına koyar. Ardından UDP bu bilgiyi IP katmanına yollar. IP katmanı kendi başlık bilgisini ve protokol numarasını yerleştirir (bu sefer protokol numarası alanına UDP' ye ait değer yazılır). Fakat UDP TCP'nin yaptıklarının hepsini yapmaz. Bilgi burada datagramlara bölünmez ve yollanan paketlerin kaydı tutulmaz. UDP'nin tek sağladığı port numarasıdır. Böylece pek çok program UDP'yi kullanabilir. Daha az bilgi içerdiği için doğal olarak UDP başlığı TCP başlığına göre daha kısadır. Başlık, kaynak ve alıcı port numaraları ile kontrol toplamını içeren tüm bilgidir.

Kaynak Port																**Hedef Port**															
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
Uzunluk																**Hata Kontrolü**															
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
Veri																															

Şekil 1. UDP paket formatı

5.8.6.2 Alanlar

Kaynak port: İsteğe bağlı bir alandır, anlamlı olduğunda, gönderen sürecin portunu belirtir ve başka bir bilginin yokluğunda adreslenen yanıtın portu olacağı varsayılır. Kullanılmamışsa sıfır değeri yerleştirilmiş gibi ele alınır.

Hedef port: Belirli bir ağ hedef adresi bağlamı içinde anlamlıdır. Bilgi adreslerinin iletileceği hedef adresi belirler.

Uzunluk: Başlığı ve veriyi içeren kullanıcı veri datagramının sekizliler cinsinden uzunluğudur. Bu durumda veri olmasa bile başlık alanları nedeniyle paketin minimum uzunluğu 8 bayt olacaktır.

Hata kontrölü: kavramsal olarak, kaynak adresi, hedef adresi, protokol ve UDP uzunluğunu içeren UDP başlığının önüne gelir. Bu bilgi veri datagramlarının yanlış yönlendirilmesine karşı koruma sağlar. Bu hata kontrol yordamı TCP'deki ile aynıdır.

```
 0      7 8     15 16    23 24    31
+--------+--------+--------+--------+
|          kaynak adresi          |
+--------+--------+--------+--------+
|          hedef adresi           |
+--------+--------+--------+--------+
| sıfır |protokol|  UDP uzunluğu   |
```

Eğer hesaplanan sağlama toplamı sıfırsa, tamamı birlerden oluşmuş gibi aktarılır (bire tümleyen aritmetiğinde eşdeğeri). Tamamı sıfırlardan oluşmuş bir hata kontrol değeri aktarımcının bir hata kontrol değeri üretmediği anlamına gelir.

5.8.6.3 Kullanıcı arayüzü

Bir **UDP** kullanıcı arayüzü,

- Yeni alıcı portların oluşturulmasına,
- Alım portlarında, geri dönen veri baytları ile kaynak port ve adres işareti alım işlemlerine,
- Bir datagramın gönderileceği hedef adresi ve portu ile veriyi belirterek bir veri datagramının gönderilmesine izin veren bir işleme olanak sağlamalıdır.

5.8.6.4 IP ara yüzü

UDP modülü, ağ başlığından kaynak ve hedef ağ adreslerini ve protokol alanını saptayabilmelidir. Olası bir UDP/IP arayüzü, alım işlemine yanıtta ağ başlığının tamamını içeren ağ veri datagramının tamamını döndürmelidir. Böyle bir arayüz ayrıca, gönderecek

IP'ye başlığıyla tam bir ağ veri datagramını aktaracak UDP'ye izin vermelidir. IP, belirli alanları tutarlılık için doğrulamalı ve ağ başlığının hata kontrol alanını hesaplamalıdır.

5.8.6.5 Yalancı başlığın içeriği

Alan	**Uzunluk**	**Açıklama**
Source Address	32 bit	Göndericinin standart IP adresi
Destination Address	32 bit	Alıcının standart IP adresi
Protocol Code	16 bit	UDP' nin oluşturduğu datagramı gösteren standart IP kodu. UDP için değer 17' dir.Yani bu alan heksadesimal kodda 0x0011' dir.
UDP Length	16 bit	Başlığı içeren byte sayısı.

Şekil 2. Yalancı başlığın içeriği

IP sadece kendi başlığı üzerinde hata kontrol işlemi yapar. UDP verisi üzerinde hata kontrolü yapmaz. UDP deki hata kontrolü sadece hatasız taşımanın bir ölçüsüdür. Yeniden gönderim veya güvenilirlik sağlamaz.

Yalancı başlık kaynak adres, hedef adres, protokol ve UDP uzunluğunu içeren kavramsal bir önektir.

1. Örnek UDP paketi:

04 89 00 35 00 2C AB B4 00 01 01 00 00 01 00 00 00 00 00 00 04 70 6F 70 64 02 69 78 06 6E
65 74 63 6F 6D 03 63 6F 6D 00 00 01 00 01

UDP Header 04 89 00 35 00 2C AB B4
Data 00 01 01 00 00 01 00 00 00 00 00 00 04 70 6F 70 64 02 69 78 06 6E 65
74 63 6F 6D 03 63 6F 6D 00 00 01 00 01

Source Port 04 89
Destination Port 00 35
Length 00 2C
Checksum AB B4
Data DNS Message

Başlık blokları iletimden önce veriye eklenir.Paket alındığında başlıklar işlenir ve paketten çıkarılır.Bu işlemler yığıt modelini tanımlar.Internet protokolleri yedi katmanlı ISO OSI modelinde yığıta benzer tanımlanır.

5.9 MULTİPLEXİNG

Bir iletim ortamının iletim kapasitesini birden fazla kullanıcı arasında paylaştırarak,

bölüştürerek, ayın iletim ortamı üzerinden aynı anda birden fazla iletişim olanağı sağlanmasına multiplexing (çoğullama) denir. Örneğin elektronik cihazlarda multiplexing birden fazla analog sinyallerin dijital sinyale dönüştürülüp (analog-to-digital ADC) işlenmesini (process) sağlar veya telekomünikasyonda birden fazla telefon görüşmesinin aynı fiziki kablo üzerinden aktarılması sinyallerin multiplex edilmesiyle gerçekleşir. Ağ dünyasında çoklamak ile kast edilen ise bir hattıbirden fazla bilgisayarın veya birden fazla programın kullanmasıdır. Çoğullama, iletim ortamının verimli kullanılmasını ve böylece iletim maliyetinin düşürülmesini sağlar.

5.10 DEMULTİPLEXİNG

Demultiplexing**,** daha önceden multiplex edilmiş sinyalin birden fazla kanallara ayrılmasıdır, orijinal haline getirilmesidir. Demultiplexing Multiplexing`in karşıtıdır. Multiplex edilmiş sinyallerdemultiplex edilmeden kullanılamazlar. Multiplexing düşük seviyeli kanalların kapasitesini sanal bölmelere ayırıp yüksek seviyeli mantıksal kanallar yaratır ve bu kanallar üzerinde sadece tek bir sinyal gönderilebilir. Gönderilen bu sinyaller alıcı makine tarafından demultiplex edilip orijinal hallerine geri dönüştürülür.

5.11 TCP SEGMENT YAPISI

TCP'nin (Transmission Control Protocol-İletişim Kontrol Protokolü) temel işlevi, üst katmandan (uygulama katmanı) gelen bilginin segment'ler haline dönüştürülmesi, iletişim ortamında kaybolan bilginin tekrar yollanması ve ayrı sıralar halinde gelebilen bilginin doğru sırada sıralanmasıdır. Peki, bu segmentlere ayrılma işi nasıl gerçekleşmekte? TCP kendisine atanmış olan bu görevleri yapabilmek amacıyla, ulaşım katmanında veri parçalarının önüne başlık bilgisi ekler. Başlık bilgisi veri parçası, ikisi birlikte TCP segmenti olarak anılır. TCP segmenti bir alt katmana (IP katmanına) gönderilir, oradan da bu segmente IP başlığı eklenerek alıcıya yönlendirilir.

Şekil 1.8: TCP segment formatı

- Gönderici Port: Gönderen bilgisayarın çalıştırdığı uygulamanın portu.(2 byte)
- Alıcı Port: Alan bilgisayarın çalıştıracağı uygulamanın portu.(2 byte)
- Sıra No: Gönderilen paketin sıra numarasını gösterir.(4 byte)
- Onay No: Gelecek TCP oktetinin ilk bitinin sıra numarasıdır. (4 byte)
- Başlık Uzunluğu: TCP başlığında var olan 32 bit uzunluğundaki sözcüklerin sayısını gösterir (4 bit)
- Saklı Tutulmuş(Reserved): Sıfır olarak ayarlanmıştır.(6 bit)
- Kod Bit: Oturumun oluşturulması ve kesilmesi gibi kontrol fonksiyonları (6bit)
- Pencere: Gönderilecek maksimum data miktarını belirler.(2 byte)
- Hata sınama bitleri (Checksum): Data ve başlık alanlarını kullanarak yapılan bir hesap.(2 byte)
- Acil işaretcisi(Urgent): Acil datanın sona erdiğini belirtir. (2 byte)
- Seçenekler: Sadece bir tane tanımlanmıştır. Maksimum TCP segment büyüklüğü ya da 32 bittir.

 Kullanıcı Verisi: Üst katmandan gelen datadır.

5.12 Transport Katmanı Port Numaraları

Port : TCP ve UDP, bilgiyi üst katmanlara iletmek için port (yada socket) adı verilen servis erişim noktalarını kullanırlar.

Örnegin bir web sunucuya gelen istek paketinin HTTP servisine iletilebilmesi için, paketin HTTP servisinin kullandığı port olan TCP 80'e yollanması gerekir. Cevap verecek olan web sunucu da paketi, istek yapan bilgisayarın çıkış portuna yollamalıdır

ÖNEMLİ PORT NUMARALARI:

7 => echo, Bu porttan sunucuya ne yollarsanız aynen geri yollar.

11 => systat, Kullanıcılar hakkında bilgiler verir.

13 => daytime, Tarih ve zaman bilgisi. Bilgisayarın nerede oldu u bulunabilir.

15 => netstat, Network ile ilgili bilgiler

21 => ftp, Bildiğiniz ftp portu

23 => telnet, Telnet portu

25 => smtp, Smtp (Simple Mail Transfer Protocol) Server portu

37 => time, Zaman.

43 => whois, Host hakkında bilgiler.

53 => dns Domain name server

79 => finger, Kullanıcılar hakkında bilgi.

80 => http, Web sunucu

110 => pop, Gelen mail

5.13 TAŞIMA KATMANI GÜVENLİ İLETİŞİM PROTOKOLLERİ

5.13.1 SSH Nedir?

SSH(Secure Shell / Güvenli Kabuk) ağ üzerinden başka bilgisayarlara erişim sağlamak, uzak bir bilgisayarda komutlar çalıştırmak ve bir bilgisayardan diğerine dosya

transferi amaçlı geliştirilmiş bir protokoldür. Güvensiz kanallar(internet vs) üzerinden güvenli haberleşme olanağı sağlar. Bir iletişimde SSH aşağıda belirtilen temel unsurları sağlar.

• authentication /Kimlik denetimi

• encryption /Şifreleme

• Integrity /Bütünlük.

5.13.2 SSH ile ilgili temel tanımlar

SSH1, Tatu Ylönen tarafından geliştirilen ilk orijinal SSH ürünü. SSH-1 Protokolü temel alınarak geliştirilmiştir.

SSH2, Tatu Ylönen tarafından geliştirilen SSH-2 ürünü.

SSH-1, SSH protokol 1.

SSH-2, SSH protokol 2. Günümüzde yaygın kullanımda olan ve kullanımı tavsiye edilen ssh sürümü. IETF SECSH çalışma grubu tarafından standartları belirlenmiştir.

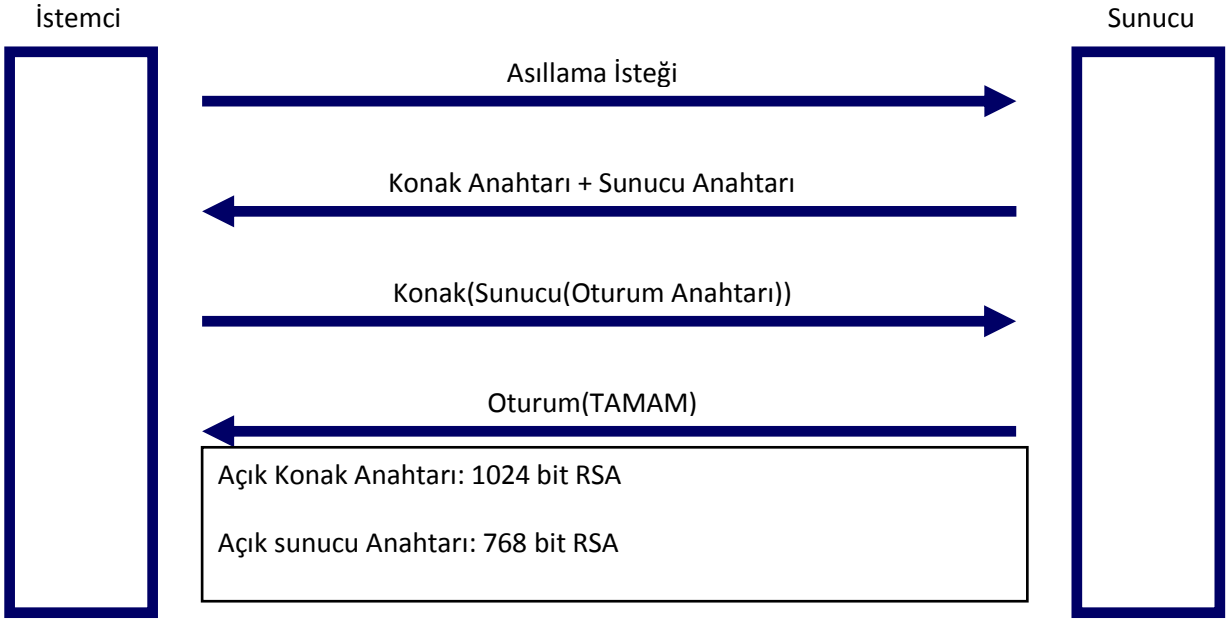
5.13.2.1 SSH Tarihçesi ve Open SSH

SSH-1 protokolü ve SSH1, ilk olarak 1995 yılında Helsinki Teknoloji Üniversitesinde araştırma görevlisi olan "Tatu Ylönen" tarafından geliştirilmiştir. Aynı yılın Haziran ayında SSH1 kaynak kodları ile birlikte özgür olarak dağıtılmaya başlamıştır. SSH protokolünün özgür bir uyarlaması olan OpenSSH *BSD Unix'lerin asi çocuğu olarak adlandırılan OpenBSD projesi çerçevesinde yürütülen SSH1 ve SSH2 protokollerini içeren yazılım takımıdır. OpenSSH son özgür SSH versiyonu olan **ssh1.2.12** den türetilmiştir. **Markus**

Friedl (Aaron Campbell, Bob Beck, Niels Provos, Theo de Raadt, Dug Song**)** önderliğinde geliştirilen OpenSSH projesi dünya üzerinde birçok yazılımcının katılımı ile iyi bir yol kat etmiştir. Göreceli olarak özgür yazılım projeleri arasında en fazla kullanılan yazılımlardan biridir. OpenBSD ile birlikte dağıtılan OpenSSH sürümü hariç diğer tüm sürümler OpenBSD için geliştirilen sürümün gerekli sisteme uyarlanmış halleridir(port edilmiş).

5.13.2.2 Kullanım Alanları

SSH güvenli iletişimin gerektiği her ortamda kullanılabilir. Sadece karşı sisteme bağlanıp komut çalıştırmak ya da dosya aktarımı yapmak için değil, doğasında güvensiz(şifrelenmemiş trafik) olarak çalışan protokoller SSH üzerinden güvenli bir şekilde kullanabilir. Mesela POP3 servisi ağ üzerinden tüm iletişimini şifrelenmemiş şekilde gerçekleştirir, biz pop3 servisini SSH üzerinden aktararak şifrelenmiş ve güvenli hale getirebiliriz.



İstemcinin gönderdiği asıllama isteğine sunucu açık konak anahtarını ve açık sunucu anahtarını göndererek yanıt verir. Konak anahtar çifti konağa özeldir ve sunucunun kurulması sırasında oluşturulur. Bu anahtar daha sonra değiştirilmez. Sunucu anahtar çifti fazladan güvenlik için eklenmiştir. Genelde saatte bir değişecek şekilde ayarlanır. Konak aldığı bu anahtarlarla yarattığı bir simetrik oturum anahtarını iki kere şifreleyerek sunucuya gönderir. Ayrıca, yaratılan oturum anahtarına şifrelenmeden önce fazladan güvenlik için rastgele sayılar da eklenir. Daha sonra, sunucu oturum anahtarıyla şifrelenmiş bir onay iletisi gönderir. Bu

güvenli oturumun ilk iletisidir. Bundan sonraki iletiler oturum anahtarıyla şifrelenmiş olarak iletilecektir.

İstemcinin sunucuyu geçerli sayması için iletişim kuralında herhangi bir tanımlama yoktur.

Sunucunun asıllanmasının önceden istemciye yerleştirilmiş bir konak anahtarı - konak adresi listesi ile yapıldığı varsayılır. Listede kayıtlı olmayan bir konak anahtarı ile karşılaşıldığında istemci tarafındaki yazılım kullanıcıyı uyaracaktır. Kullanıcının onayı olursa, istemci yazılım bu yeni konak anahtarını kaydeder. Sunucu anahtarı hiçbir zaman istemci tarafında kaydedilmez. Sunucu tarafından kullanıcı asıllaması gerekirse bu iki farklı yolla yapılabilir: Eğer parola ile asıllama yapılacaksa bu parola zaten şifrelenmiş olan hattan gönderilir. Eğer RSA asıllaması yapılacaksa sunucu yarattığı rastgele bir sayıyı kullanıcının açık anahtarı ile şifreleyerek gönderir. İstemci tarafında yazılımın kullanıcının gizli anahtarını kullanabilmesi için bir parola sorulur. Bu parolanın onaylanmasıyla yazılım kullanıcının gizli anahtarı ile metni çözerek yaratılan rastgele sayıyı bulur. Yanıt olarak sunucuya rastgele sayının özü ve bağlantıyla ilgili bazı ek bililer gönderilir.

5.13.2.3 SSH ile Dosya Transferi

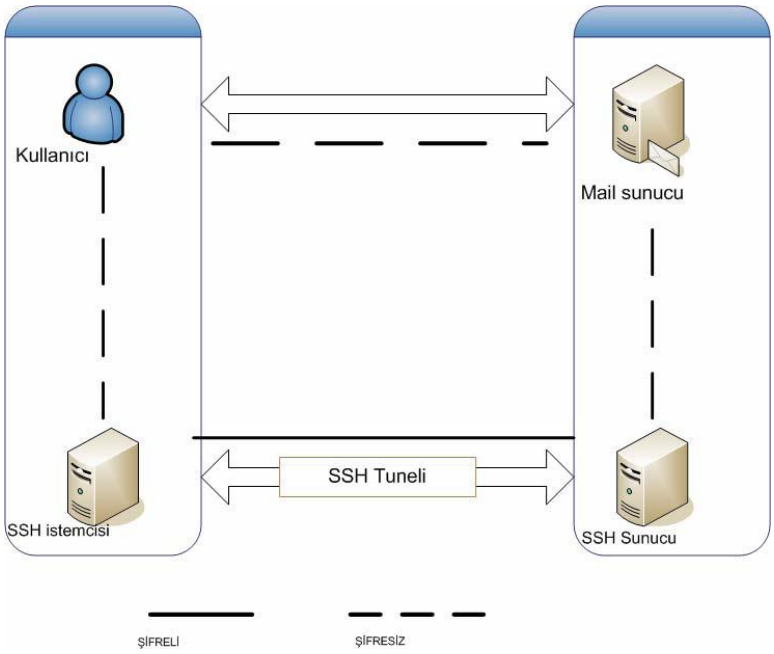
Günümüzde kullanılan en popüler dosya transfer aracı FTP'dir. SSH kullanarak hem ftp kolaylığında dosya transferi yapılabilir; hem de transfer edilen dosya şifrelenerek meraklı gözlerden korunmuş olur. SSH ile dosya transferinde temel iki seçenek var; biri SCP(Secure Copy) diğeri de Sftp(Secure FTP). Temel bazı farklılıklar dışında her iki yöntem ile yapılabilecekler aynıdır.

5.13.2.4 SSH ile ileri seviye Uygulamalar

Anahtar ile Kimlik doğrulama

SSH, kullanıcı adi/parola ikilisi haricinde şifreli anahtarlar aracılığı ile de kimlik kontrolü yapabilir.

public key authentication



Anahtarlar şifreleme dünyasındaki kimliklerimizdir. Kimliğimiz 2 anahtardan oluşur; biri açık anahtarımız -ki bunu herkesle paylaşırız-. Diğeri de gizli anahtarımız bunu sadece biz biliriz.

Anahtar ile kimlik doğrulama adımları;

1. ssh istemcisi sunucuya xxx kullanıcı adi ile bağlanmak istediğini belirtti

2. sunucu istemciden gelen isteği alır ve istemcinin kendini kanıtlaması için challenge mesajı gönderir

3. istemci challenge olarak gizli anahtarını ve gelen challenge verisini kullanarak sunucuya cevap döner

4. sunucu kendi tarafında gelen şifreyi karsılaştırarak kullanıcıya giriş hakki tanır ya da reddeder.

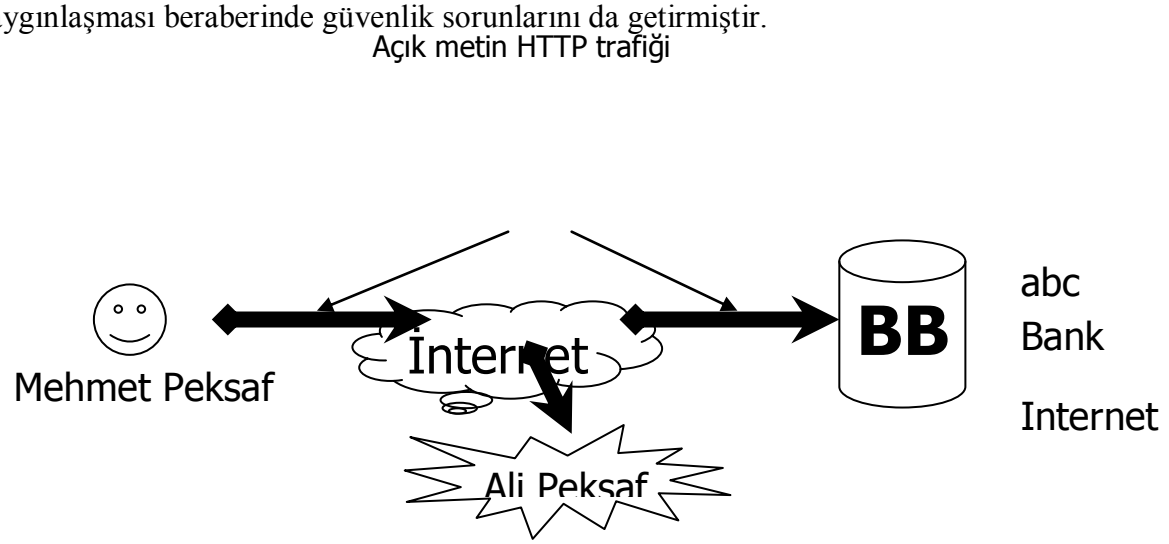
NOT: Burada dikkat edilmesi gereken nokta bu iletişimde arada ne açık anahtar ne de gizli anahtar geçmediğidir.

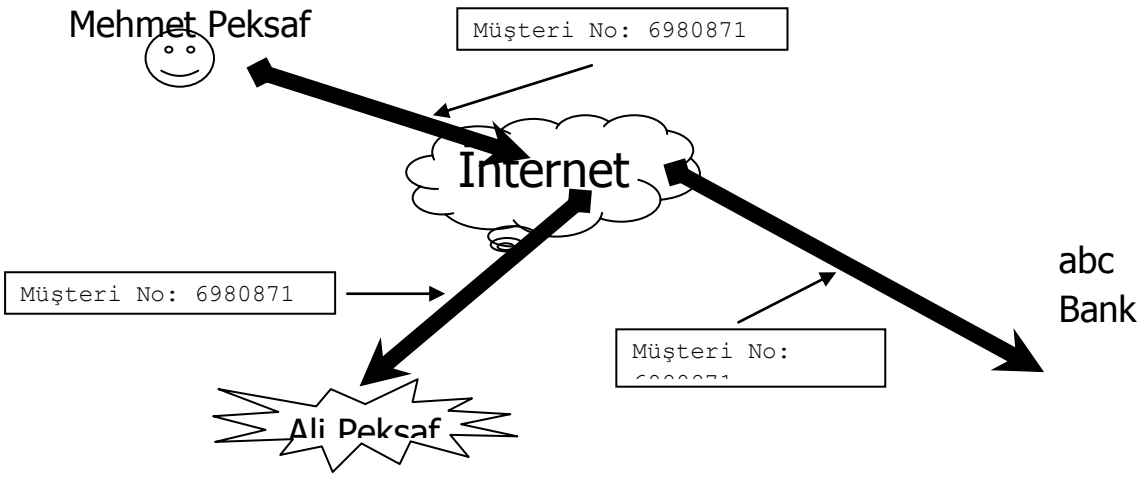
5.13.3 SSL (Secure Socket Layer) Nedir?

SSL network üzerindeki bilgi transferi sırasında güvenlik ve gizliliğin sağlanması amacıyla Netscape tarafından geliştirilmiş bir güvenlik protokolüdür. 1996 yılında 3,0 versiyonunun çıkarılmasıyla hemen bütün İnternet tarayıcılarının (Microsoft Explorer, Netscape Navigator vb) desteklediği bir standart haline gelmiş ve çok geniş uygulama alanları bulmuştur. SSL gönderilen bilginin kesinlikle ve sadece doğru adreste deşifre edilebilmesini

sağlar. Bilgi gönderilmeden önce otomatik olarak şifrelenir ve sadece doğru alıcı tarafından deşifre edilebilir. Her iki tarafta da doğrulama yapılarak işlemin ve bilginin gizliliği ve bütünlüğü korunur. Veri akışında kullanılan şifreleme yönteminin gücü kullanılan anahtar uzunluğuna bağlıdır. Anahtar uzunluğu bilginin korunması için çok önemlidir. Örneğin; 8 bit üzerinden bir iletimin çözülmesi son derece kolaydır. Bit, ikilik sayma düzeninde bir rakamı ifade eder. Bir bit, 0 veya 1 olmak üzere 2 farklı değer alabilir. 8 bit ise sadece 28=256 olası farklı anahtar içerir. Bir bilgisayar bu 256 farklı olasılığı sıra ile inceleyerek bir sonuca ulaşabilir. SSL protokolünde 40 bit ve 128 bit şifreleme kullanılmaktadır. 128 bit şifrelemede 2128 değişik anahtar vardır ve bu şifrenin çözülebilmesi çok büyük bir maliyet ve zaman gerektirir. Kötü niyetli bir kişinin 128 bit'lik şifreyi çözebilmesi için 1 milyon dolarlık yatırım yaptıktan sonra 67 yıl gibi bir zaman harcaması gerekir. Bu örnekten anlaşıldığı gibi SSL güvenlik sistemi tam ve kesin bir koruma sağlar.

Bildiğimiz gibi Internet herkese açık bir ortamdır. Teknolojinin ilerlemesi ile beraber artık internet gündelik hayatımızın vazgeçilmez bir parçası haline gelmiştir. İnternetin bu denli yaygınlaşması beraberinde güvenlik sorunlarını da getirmiştir.





İletişim kuralları yığınında yerleştiği yerden ötürü SSL kullanan yazılımlar ile kullanmayan yazılımların kapı numaraları çakışmaktadır. Bunun çözümü üç şekilde olabilir: SSL destekleyen her bir uygulama iletişim kuralı için yeni bir kapı numarası atanır, alışıldık kapı numaraları kullanılarak güvenlik seçenekleri uygulama iletişim kuralına bırakılır ya da TCP paketlerine SSL kullanılıp kullanılmadığını belirten bir alan eklenir. Şu an için görünen ilk seçeneğin kullanıldığı.

Şekilde görüldüğü gibi SSL iki ayrı katmana ayrılır: SSL kayıt katmanı ve SSL tokalaşma katmanı. SSL kayıt katmanı üstündeki iletişim kurallarından aldığı verinin parçalanması, asıllanması ve şifrelenmesi ile ilgilenir. Bu katmanın üzerinde SSL'in diğer katmanları çalışır. Bunların en önemlisi tokalaşma iletişim kuralıdır.

SSL tokalaşma iletişim kuralının ereği sunucu ile istemci arasında bir bağ oluşturmak, şifreleme, sıkıştırma kurallarını belirlemek, gerekirse tarafları asıllamak, oturum için gerekli anahtarları oluşturmaktır.

İşte verinin güvenliksiz bir ortam olan internette bir yerden bir yere taşınması sorununa bir çözüm olması için SSL ortaya atılmıştır. SSL'i ilk ortaya atan Netscape firmasıdır. Daha sonra IETF tarafından bir güvenlik standardı olarak kabul edilmiş ve Netscape'ten devralınmıştır. SSL, güvenli olmayan bir ortamda verinin göndericiden alıcıdan güvenli bir şekilde iletimini sağlamak amacı ile hem herkese açık bir anahtar şifrelemesini hem de özel anahtar şifrelemesini aynı anda kullanabilen bir yapıda tasarlanmıştır. Veriyi sunan Web Server, Sertifika otoritesi tarafından imzalanmış özel ve herkese açık bir anahtara sahiptir. Bu anahtar değerleri verinin alıcı tarafından sunucudan güvenli bir şekilde alınmasını sağlar.

SSL teknolojisi, veri iletimi esnasında Hashing metodunu kullanır. Hashing metodolojisi ile sunucu, veriden tek bir hash değeri yollar. İstemciye veri ile beraber bu hash değerini de yollar. İstemci bu data paketini aldığında, aynı hash fonksiyonunu kullanarak, gelen bu paketten yeni bir hash değeri üretir. Burada altının çizilmesi gereken nokta, veri İstemcisinin ürettiği anahtar değerinin, sunucunun kullanmış olduğu aynı hash fonksiyonu ile üretilmiş olmasıdır. İstemci ile sunucu, aralarında bağlantı sağlarken, aynı hash fonksiyonu kullanmak için anlaşırlar. İstemcinin üretmiş olduğu bu yeni hash değeri, sunucunun yolladığı hash

değeri ile aynı olmak zorundadır. Eğer aynı değilse veri değişmiştir. Aynı değilse verinin değişmediğinden sunucu emin olmuş olur.

SSL, web sunucusunda tanımlanmış olan digital imzaları kullanır.

Böylece web sunucusunun yayınlamış olduğu digital imza sayesinde, browserdan web sunucusuna erişen İstemci, gerçekten alışverişte bulunacağı firma ile bir bağlantının kurulduğundan emin olur. Bir sunucu sertifikası, sunucuda tanımlanmış olan bir dijital imza ile bellidir. Ve sunucunun gerçek kimlik bilgilerini içerir. Sertifika otoritesi, bahsi geçen sertifikayı sunucu firmaya verirken, öncesinde o da bir kimlik denetiminde bulunur. Güvenilir bir firma olduğuna kanaat getirdiğinde, sunucu firmaya sertifika verir. Sertifika Otoritesinin vermiş olduğu bu sertifika, sunucu firmanın güvenilir ve onaylanmış bir firma olduğunu belgeler. Sertifika otoritesi, Verisign gibi firmalardır. Ve bu sertifika otoriteleri, internette alışveriş hizmeti sağlamak isteyen firmalara dağıtabilecekleri sertifikaları, bir onay aşamasından sonra verir.

Sunucuya İstemciden bir SSL isteği geldiğinde, İstemcinin web browser'ı, sunucu ile irtibata geçer. Ve sunucu, İstemciye Sertifika Otoritesi tarafından kendisine verilmiş olan sertifikayı yollar. İşte kısaca diyebiliriz ki, sertifika, bir dijital imzadan ibarettir. İstemci, sunucunun yollamış olduğu bu sertifikayı aldığında, bu sertifikadan sunucunun firma kimlik bilgilerini ve herkese açık anahtar bilgisini okuyabilir. İstemci, sertifika otoritesinin herkese açık anahtarı ile sayısal imzayı çözer ve otoritenin ürettiği hash değerini bulur. Daha sonra sertifika içinden kendisi de bir hash değeri üretir. Bu iki hash değerinin aynı olması gerekmektedir. Eğer aynı ise, web sunucusu, Sertifika Otoritesi tarafından onaylanmıştır ve İstemcinin gerçekten iletişime geçmek istediği bir firma demektir.

Böylelikle sunucu ve İstemci arasında bir SSL "güvenli" bir bağlantı kurulumu gerçeklenmiş olur ve bu bağlantı esnasında giden gelen paketler şifrelendiği için üçüncü kişiler, sunucu ile İstemci arasında gidip gelen veri paketlerini okuyamaz. Eğer üçüncü şahıslar, veri okumaya başlayabilirse, bundan anında hem sunucunun hem de İstemcinin haberi olur ve bağlantı hemen kesilir. SSL ile yukarıda da görebildiğimiz gibi hem sunucu İstemciye kendini tanıtır hem de İstemci sunucuya kendini tanıtır. Böylelikle iki taraflı bir güven ilişkisi kurulmuştur.

O halde İstemci ile sunucu arasında iki taraflı bir el sıkışması yapılır. (HandShake). Bu el sıkışma anlaşması, İstemci sunucuya ilk ulaştığı anda yapılır. El sıkışma aşamaları şöyle cereyan eder:

- İstemci, sunucuya ilk ulaştığında el sıkışma başlar ve her iki taraf, güvenlik amacı ile kullanılacak olan şifreleme fonksiyonu üzerinde anlaşır.
- İstemci, sunucunun kimliğini denetler.
- İstemci, sunucudan almış olduğu dijital imzadan bir anahtar oluşturur ve bunu sunucuya yollar.
- Sunucu bu anahtarı alınca, kontrol eder.

- Eğer istenirse, sunucu da tarayıcıdan bir kimlik denetimi isteyebilir. Bu da demek ki, çift taraflı bir güven anlaşması desteklenmektedir.

Bu el sıkışma aşamaları başarılı bir biçimde gerçeklenirse, sunucu ve İstemci arasında bir veri iletişim kanalı açılmıştır ve veri iletişimi başlar.

Konuya daha açıklık getirmek istersek, şunları da burada yeri geldiğinde söylemekte fayda var:

-El sıkışma başladığında, İstemci sunucudan kimlik bilgilerini ister. Bunun üzerine sunucu, İstemciye sertifikasını yollar.

-İstemci aldığı bu bilgiler eşiğinde simetrik bir anahtar oluşturur. Daha sonra sunucunun herkese açık anahtarı ile bu bulduğu anahtarı şifreler. Ve bu değeri sunucuya yollar.

-Kendi özel anahtarını kullanarak, sunucu, İstemcinin yolladığı bu şifrelenmiş anahtarı çözer.

Bu aşamalar sonucu İstemci ve sunucunun birbirine yollamış olduğu anahtarlar eğer aynı ise,

El sıkışma başarılı bir biçimde kurulmuş demektir ve veri alışverişi başlar.

Bu el sıkışma protokolü ve verinin şifrelenerek İstemci ve sunucu arasında yollanması işlemleri, OSI referans modelinin Application ve Presentation seviyelerinde gerçeklenir.

(Application seviyesinde, İstemci ve tarayıcı World Wide Web üzerinden oturum açıp veri alışverişinde bulunurlarken, şifreleme işlemleri Presentation seviyesinde yapılır.)

Burada değinilmesi gereken bir diğer nokta ise, yapılan şifreleme tekniğidir.

3 farklı şifreleme tekniği kullanılır.

A. Hash Tekniği ile Şifreleme: Veri trafiği esnasında, verinin değişmediğinin ve bütünlüğünün korunduğunu anlamak için kullanılır.

B. Anahtar Değişim Tekniği ile Şifreleme: İstemci ve sunucunun, el sıkışma sonrasında, veriyi şifrelemek amacı ile kullandıkları simetrik anahtarı nasıl birbirine ulaştıracağını belirlemek için kullanılır.

C. Simetrik Veri Şifreleme: Veri şifrelenmesinde kullanılacak olan RC2 gibi bir veri şifreleme tekniğidir.

SSL desteği veren web sunucunun barındırdığı web adresleri “http” ile başlar.

O SSL tekniği ile güvenliği sağlanmış olan bir web sunucuya bir istemci bağlanıp veri alışverişini başlatmak istediğinde şu adımlar gerçeklenir:

Öncelikle Web sunucu, bir Sertifika Otoritesinin kendisine tahsis etmiş olduğu sertifikayı yüklemiş olması gerekmektedir. Böylelikle, Sertifika Otoritesi, sunucuyu onayladığını, istemcilere garanti etmiş olur.

İstemci, sunucuya bağlandığında aralarında bir el sıkışma protokolü kurumu başlatılır. Bu bağlamda, İstemci ve sunucu hangi şifreleme tekniğini kullanacakları konusunda anlaşırlar.

Sunucu, istemciye, kendisine Sertifika Otoritesi tarafından verilmiş olan sertifikayı yollar.

İstemci, sunucunun kendine yollamış olduğu sertifikayı kullanarak sunucunun kimlik denetimini yapar.

İstemci, bu kimlik denetiminden sonra, eğer geçerli bir sertifika aldı ise; bu sertifika bilgisinden, simetrik şifreleme anahtarını yaratır ve bunu sunucuya yollar. Bu şifreleme anahtarı, sunucu ve İstemci arasındaki verinin şifrelenmesi için kullanılacaktır.

Sunucu, İstemciye veri yollarken, bu şifre anahtarı ile veriyi şifreler, veri için bir hash değeri üretir. Şifrelenmiş veri ve hash değeri istemciye yollanır.

İstemci veriyi alır, bir hash değeri üretir. Veriyi ve hash değerini simetrik anahtar ile şifreler, sunucuya yollar.

Sunucu aldığı bu şifrelenmiş veriyi ve hash değerini çözer. Veri için yeni bir hash değeri üretir. İki hash değerini karşılaştırır. Aynı ise, iletişime devam edilir.

Bu adımlar, İstemci ve sunucu arasındaki veri trafiği boyunca devam eder.

SSL teknolojisi, 40 bit, 56 bit ve 128 bit veriyi destekler. Ama daha güvenli olması için tercih edilen 128 bitlik veri alışverişidir.

5.13.4 PCT Nedir?

PCT (Private communication technology, kişisel iletişim teknolojisi) Microsoft tarafından 1995 yılında Netscape'e karşılık vermek amacıyla çıkarılmış, temelinde SSL 2,0'dan farkı olmayan bir iletişim kuralıdır. Dört ileti ile bağ kurulur. PCT kayıt iletişim kuralı üzerinde çalışan PCT tokalaşma iletişim kuralından oluşan iki katlı bir yapısı vardır.

5.13.5 TLS Nedir?

IETF tarafından SSL 2,0, SSL 3,0, SSH 2,0 ve PCT 1,0 temel alınarak geliştirilmiştir. İlk taslağı SSL 3,0 taslağı kopyalanarak oluşturulmuş, daha sonra üzerinde değişiklikler yapılmıştır. Öncelikle HMAC yapısı geliştirilmiş ve IPSec TLS' de kullanılır şekle getirilmiştir. SSL' de bulunan yayınlanmamış teknolojiler taslaktan çıkarılmıştır. TLS kayıt ve tokalaşma iletişim kuralları ayrılarak geliştirilmiş ve belgeleri hazırlanmıştır. Tüm bunların yanında geriye uyumu sağlamak amacıyla TLS 1,0 SSL 3,0 ile çalışabilecek şekilde tasarlanmıştır. Kerberos asıllamasının ve parola asıllamasının taslağa eklenmesi önerilmiştir.

5.13.6 TCP'DE TIKANIKLIK KONTROLÜ

Bir ağda fazla yükten dolayı paketlerin bekleme süreleri artarsa, paket kayıpları yaşanırsa ve ağın etkinliği azalırsa bu ağ tıkanmış demektir.

• Ağın etkinliğinin azalması, kaybolan paketlerin yeniden gönderilmesini gerektirmekte ve ağa fazladan yük getirmektedir.

• TCP nin önemli özelliklerinden birisi de tıkanıklık durumundaki davranışıdır. Günümüz ağlarında paket kaybı donanım arızalarından çok tıkanıklıktan dolayı oluşabilmektedir.

İletim protokolleri tıkanıklıkta kaybolan paketlerin bir kopyasını daha ileterek problemi daha da büyütebilir.

Eğer tıkanıklık çok sayıda yeniden iletimi tetiklerse tıkanıklık çökmesi denen durum ortaya çıkar. Bu sorunun olmaması için TCP paket kaybını tıkanıklık göstergesi olarak algılar ve yeniden iletim oranını azaltır. TCP iletimi tamponlara bağlıdır. Alıcı bir pencere boyu ilan eder ve gönderen onay almadan önce pencereyi dolduracak kadar veri gönderebilir. Veri hızını sınırlandırmak için TCP pencere boyunda kısıtlama koyar geçici olarak pencere boyunu küçülterek gönderen TCP'nin veri hızını azaltması sağlanır.

• TCP tıkanıklık kontrolü paket kaybolduğunda çalışır. Alıcının tamponunu dolduracak kadar veriyi tekrar iletmek yerine TCP veri içeren tek bir mesaj göndererek başlar. Eğer onay gelirse

• TCP iletilen veriyi iki katına çıkarır ve iki mesaj gönderir. Eğer iki onay da gelirse TCP iki katı daha veri gönderir.

• Katlı artım alıcının pencere boyunun yarısına ulaşana kadar bu şekilde devam eder.

Bu miktardan sonra artış yavaşlar ve TCP lineer olarak artırmaya devam eder.

TCP tıkanıklık kontrolü internetteki artan trafikte iyi çalışır. Hızlıca veri iletimini yavaşlatarak tıkanıklığı gidermeye yardımcı olur. Eğer TCP yazılımları standarttaki gibi davranırsa tüm TCP'ler tıkanıklıkta yavaşlar ve tıkanıklık çökmesini engeller.

5.14 Kablosuz Ağlarda Tıkanıklık

Tıkanıklık, kablolu ağlarda olduğu gibi kablosuz ağlarda da ağın performansını etkileyen en önemli konulardan biridir. Kablolu ağlarda birçok tıkanıklık denetleme ve önleme yöntemi kullanılmaktadır.

• Kablosuz ağlar fiziksel yapılarından dolayı kablolu ağlar gibi yüksek bant genişliğine sahip değildir ve bu ağlarda hareketli yapılarından dolayı sık sık bağlantı kopuklukları yaşanabilmektedir. Bu farklılıklardan dolayı kablolu ağlarda kullanılan yöntemler kablosuz ağlarda olduğu gibi kullanılamamaktadır.

• Kablosuz ağlar için kullanılacak olan yönlendirme ve tıkanıklık giderme protokolü bu tür ağların özelliklerine uygun olmalıdır.

5.14.1 Tıkanıklık Önleme Yöntemleri

Temel olarak iki çeşit tıkanıklık önleme yöntemi vardır. Bunlar, rezervasyon tabanlı ve isteğe bağlı metotlarıdır.

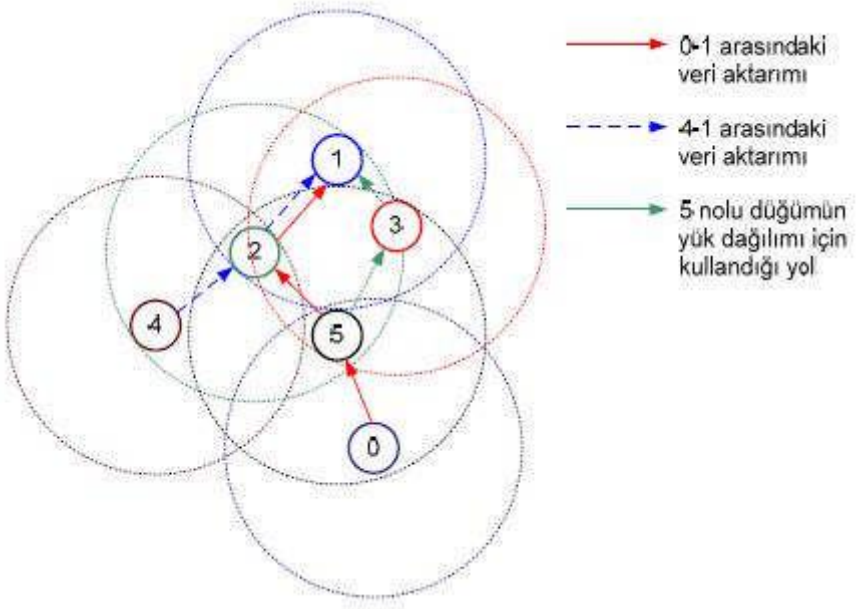
• Bir kullanıcının ihtiyacı olan hizmet kalitesi için önceden ağ üzerinde kaynak ayrılır. Kullanıcı istediği zaman bu kaynakları kullanarak ağ üzerinden bilgi transfer eder. Bu yöntem rezervasyon tabanlı olarak adlandırılabilir.

• Alternatif olarak kullanıcı gerek duyduğu anda ağdaki kaynakları rezerve etmek isteyebilir.

Fakat ağdaki mevcut yük dolayısı ile istediği kalitede hizmet alamayabilir.

İkinci metot rezervasyonsuz ağlarda kullanılır. Bu durumda kullanıcılar kendilerini değişen ağ durumuna adapte etmek durumundadırlar.

• İsteğe bağlı planda ise ağın yolun kontrol edilmesi ve buna göre karar verilmesinin bir maliyeti vardır. Fakat ilk kurulan yol en kısa yol olduğu için bu yolun tamamen devre dışı bırakılarak yeni yol üzerinden aktarımın devam ettirilmesi uzun süren aktarımlarda fazladan maliyet demektir.



Şekil'de örnek bir topoloji üzerinde, önerilen tıkanıklık önleme yönteminin nasıl çalıştığı görülmektedir. 0 numaralı düğüm ile 1 numaralı düğüm veri aktarımı yaparken, 4 numaralı düğüm 1 numaralı düğüme veri göndermeye başlamaktadır.

5 numaralı düğümün 2 numaralı düğüme bakan ara yüzündeki kuyruk uzunluğu, eşik değeri aştığı için

5 numaralı düğüm hedefe giden ikinci bir yol belirlemekte ve buradan aktarıma devam etmektedir.

5.15 KAYNAKLAR

- [1] http://www.cisco.com.tr
- [2] http://www.bidb.itu.edu.tr/?d=496
- [3], [6], [11], [12], [14] Bilgisayar Ağları-I Ders Kitabı
- [4], [7] www.wikipedia.org
- [5] http://ogrenci.hacettepe.edu.tr/~b0244877/modeller/index.html
- [8] Fatih Üniversitesi MYO. Öğr. Gör. Mustafa SARIÖZ, Ağ Teknolojilerinin Temelleri Dersi
- [9], [10], [15] Ahmet Kemal AYGIN Gebze Yüksek Teknoloji Enstitüsü, Bilgisayar Mühendisliği Bölümü (14.11.2009)
- [13], [16] Yrd.Doç.Dr. İ. Taner OKUMUŞ Muğla Üniversitesi (14.11.2009)
- http://technet.microsoft.com/tr-tr/library/cc780893(WS.10).aspx (14.11.2009)
- http://www.ciscotr.com/forum/network-genel/92-tcp-ip-transmission-control-protocol
- 11) http://www.bilisimcell.net/udp.html

- 12) http://www.hell-world.org/ownz/udp-icmp-yi-biraz-daha-acalim/
- 13) *www.belgeler.org/rfc/rfc768.html*
- Rıfat Çölkesen, Bülent Örencik - Bilgisayar Haberleşmesi ve Ağ Teknolojileri
- http://www.cisco.com/tr
- http://ansiklopedi.turkcebilgi.com
- www.forumvefa.com/
- www.networkogren.com/

6 BÖLÜM VERİ BAĞLANTI KATMANI

6.1 Veri Bağlantı Katmanı (Data Link Layer)

Veri Bağlantı Katmanı (Data Link Layer) OSİ (Open System Interconnection) modelinin ikinci katmanıdır.Birinci katman olan Fiziksel Katman (Physical Layer) ile üçüncü katman olan Ağ Katmanı (Network Layer) arasında veri akışını ve bağlantıyı sağlar.

Veri bağlantı katmanının büyük bir bölümü ağ kartı üzerinde gerçekleşir.Ağ üzerindeki diğer bilgisayarları tanımlama, kablonun o anda kimin tarafından kullanıldığının tespiti ve fiziksel katmandan gelen verilerin hata kontrolü görevini yerine getirir.[1]

Veri bağlantı katmanı, ağ katmanından aldığı veri paketlerine hata kontrol bitlerini ekleyerek çerçeve (frame) şeklinde fiziksel katmana iletir.İletilen çerçevenin doğru mu yoksa yanlış mı iletildiğini kontrol eder, eğer hatalı iletilmişse çerçevenin yeniden gönderilmesini sağlar.

6.1.1 Veri Bağlantı Katmanının İletişim Kuralları

6.1.1.1 Ethernet

Ethernet bilgisayarlar arasında bir ağ oluşturmaya yarayan yöntemdir. Bilgisayarların ethernet aracılığı ile birbirlerine bağlanabilmeleri için ethernet kartı adı verilen bir donanım gerekmektedir. Bu karta bağlantıyı sağlayan giriş/arabirim ADSL modem gibi aksesuarların bağlanması için de kullanılabilmektedir.[2]

6.1.1.2 Token Ring

Fiziksel olarak Star topolojisine benzer, Multistation Access Unit (MSAU) olarak adlandırılan hub'a bağlıdır. Mantıksal olarak halkaya benzer. Token-Ring ağlarında açılan ilk makine bir sinyal oluşturur. Ağdaki bir makine diğer bir makineye veri göndermek istediğinde ağda dolaşan bu sinyalin kendisine ulaşmasını bekler. Sinyal kendisine ulaştığında göndereceği bilgi paketini ve paketin ulaştırılacağı makinenin adresini sinyale ekler ve sinyali tekrar ağa bırakır. Veri paketi gideceği adrese ulaşana kadar ağdaki diğer makinelerle veri alış-verişi yapmaz. Sinyal veriyi ulaştırdıktan sonra tekrar ağda dolaşmaya başlar.[2]

6.1.1.3 Fiber Distributed Data Interface(FDDI)

Kullanılan fiber optik kablo sayesinde yüksek hızlarda çalışan (100 Mbps'nin üzerinde) token ring LAN'dır. FDDI kablolamada çift kablolama tekniği kullanılır. Bu durumda bir taraf saat yönünde iletim yaparken diğer taraf saatin tersi yonünde iletim yapar. FDDI 'da A ve B sınıfı olmak üzere iki istasyon vardır. A sınıfı istasyonlar hayati önemli veriler ilettiğinden her iki fibere de bağlanır. B sınıfı istasyonlar ise fiberlerden sadece birine bağlanır.[2]

6.1.1.4 Point to Point Protocol(PPP)

İnternet protokol takımına ek olarak farklı taşıma protokolleri gerektiğinde cihazları bağlamaya yarayan protokol. "Noktadan Noktaya Bağlantı" olarakta bilinen bu tür protokol 'ler çoğunlukla dosya paylaşım ve mesajlaşma programlarınca kullanılmaktadır.[2]

6.1.1.5 High Level Data Link Control(HDLC)

OSI (Open System Interconnection) 2. katmanında yer alan bir iletim protokolüdür. HDLC, PPP (Poin to Point Protocol) gibi WAN iletişiminde paketlerin yerine nasıl ulaştırıldığını belirleyen yaygın protokollerden birisidir.[2]

6.1.1.6 Frame Relay

Tüm dünyada yaygın olarak kullanılan paket anahtarlamalı bir teknolojidir. Leased Line'a göre daha ucuz olduğu için daha çok tercih edilen bir haberleşme teknolojisidir. Frame Relay bağlantısı için en yakın Türk Telekom Frame Relay Switch'ine yüksek bant genişliğine sahip modem ve Router ile bağlanmanız gerekmektedir. Anahtarlanmış paket teknolojisine dayanan Frame Relay veriyi küçük paketlere bölerek gönderir. Bu paketler gönderilecek olan adresi, gönderenin adresini ve orijinal mesajın bir parçasını içerir.[2]

6.1.2 Veri Bağlantı Katmanı Temel Fonksiyonları

Veri bağlantı katmanı, fiziksel bir bağlantı üzerinden hatalardan arındırılmış bir iletişim kurulması için gerekli araçları sağlar ve veri bağlantılarının etkinleştirilmesi, sürdürülmesi ve etkisizleştirilmesi işlevlerini yerine getirir. Bu katmanın görevlerini aşağıdaki gibi sıralayabiliriz.

- ✓ Çerçeveleme: Ağ katmanının teslim ettiği veriye veri bağlantı katmanına ait başlık ve son ek(trailer) bilgilerini ekleyerek, başlangıcı ve bitişi bayraklar ile tanımlanmış olan ve çerçeve adı verilen blokların elde edilme sürecidir.
- ✓ Akış kontrolü: Gönderen makinenin veri gönderme hızını alıcının veri alma hızını aşmayacak şekilde ayarlamasıdır.
- ✓ Hata kontrolü: İletim ortamındaki gürültü ve diğer olumsuz etkenler nedeniyle oluşan hataların sezilmesi ve düzeltilmesidir.
- ✓ Adresleme: Kurulan veri bağlantılarının bir kimlik numarası ile tanımlanmasıdır. Buna veri bağlantı kimliği denir.(ID Data Link Connection-DLCI)

- ✓ Bağlantı yönetimi: Karşılıklı iki makinenin veri bağlantı katmanları arasındaki bağlantıların kurulması, tutulması ve çözülmesi ile ilgili protokollerin yürütülmesidir.[3]

6.1.2.1 Akış Kontrolü

Veri gönderen makinenin veri iletim hızını veriyi alan makineye göre ayarlaması işlemine akış kontrolü denir.

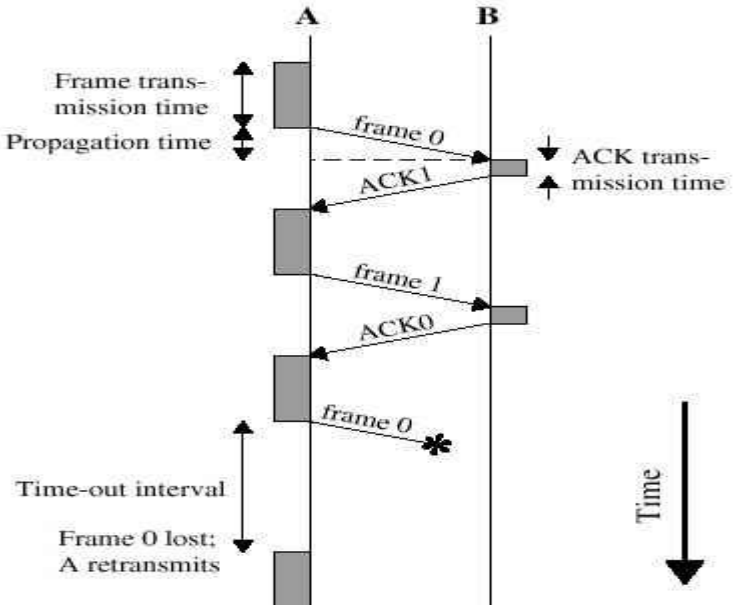
İletim ortamının hatasız olduğu ve alıcı tampon belleğinin sınırsız olduğu durumda, veri gönderen makine akış kontrolüne ve hata denetimine ihtiyaç duymadan veri çerçevelerini art arda gönderebilir. Veri alındığı zaman, alıcı, veri yükseksevyeli yazılıma geçmeden önce işlemin gerçek miktarını yapmalıdır.

Veri gönderen makinenin veri gönderme hızı alıcı makinenin çerçeveleri işleme hızını aştığı zaman, alıcıda çerçeveler kaybolmaya başlar. Kontrol olmadığı zaman, eski verilerin işlendiği sırada alıcının buffer'ı dolabilir ve fazla akış gerçekleşebilir. Bu durum, hızlı ya da az yüklü bir bilgisayarın yavaş ya da çok yüklü bir bilgisayara veri göndermesi sırasında ortaya çıkabilir. Bir geri besleme mekanizmasıyla alıcının durumunu göndericiye bildiren çeşitli akış kontrol yöntemleri ile bu durumun oluşması önlenebilir.[4]

6.1.2.2 Dur ve Bekle(Stop&Wait) Akış Kontrolü

En basit akış kontrol protokolü "stop and wait" (dur ve bekle) protokolüdür.Bu yöntemde ağ katmanından alınan her pakete başlık eklenerek gönderilir ve gönderilen her çerçeve için bir alındı beklenir. Alıcıya gelen çerçeve veri bağlantı katmanında doğruluk kontrolünden geçtikten sonra, eğer geçerli bir çerçeve ise üzerinde işlem yapılır ve veri alanı fiziksel katmana teslim edilir. Bu işlem bittikten sonra veri bağlantı katmanı bir sonraki çerçeveyi almaya hazır olduğuna dair gönderen makinenin veri bağlantı katmanına bir ACK (Acknowledge Character) alındı paketi gönderir. Alıcının veri bağlantı katmanı bir sonraki çerçevenin alınması için hazır duruma gelinceye kadar alındı göndermeyi bekletir. Gönderici bir önceki çerçevenin alındısını almadan bir sonraki çerçeveyi göndermez. Alındıda doğru olarak alınan çerçeveden bir sonra beklenen çerçevenin sıra numarası belirtilir. Örneğin Çerçeve 0 gönderilmişse alıcı Çerçeve 1'i beklediği anlamında ACK 1 gönderir.

Alınan çerçevenin hatalı olması durumunda alıcı NAK (Negative Acknowledgement) paketi gönderir. NAK çerçevesinde hatalı paketin sıra numarası belirtilir. Alıcı hatalı çerçeve alması üzerine NAK gönderdikten sonra ya da belli bir süre içinde ACK ya da NAK göndermemesi durumunda gönderici son çerçeveyi tekrar gönderir.[4]



Şekik1: Dur ve Bekle(Stop and Wait) akış kontrolü

6.1.2.3 Kayan Pencereler(Sliding Windows) Akış Kontrolü

Bağlantının bit türünden uzunluğunun çerçeve uzunluğundan büyük olduğu durumda bağlantı kullanım oranı düşüktür. Böyle durumlarda art arda birden fazla çerçeve göndererek hat kullanım oranı arttırılabilir.

A ve B makineleri arasındaki tam çift yönlü bir bağlantıda bir defada N çerçeve gönderilmesi durumunda B makinesi tampon bellekte en çerçevelik yer ayırır. Böylece A makinesi alındı beklemeden N çerçeveyi art arda gönderebilir. Hangi çerçevelerin alındısının geldiğini takip edebilmek için her çerçeveye bir sıra numarası verilir. B makinesi aldığı bir çerçevenin alındısını göndermek için ACK çerçevesinin içinde bir sonra beklediği çerçevenin sıra numarasını gönderir bu aynı zamanda " Bu numara ile başlayan N çerçeveyi almaya hazırım" anlamına gelir

Bu yöntem bir tek alındı ile birden fazla çerçevenin alındığını belirtmek için kullanılır. Örneğin B makinesi 2, 3, 4 numaralı çerçeveleri aldıktan sonra sıra numarası 5 olan (ACK5) gönderir böylece 2, 3, 4 numaralı çerçeveler için alındı göndermeye gerek kalmaz. A makinesi gönderme izni olan çerçevelerin sıra numaralarının listesini tutar B makinesi de almaya hazır olduğu çerçevelerin sıra numaralarının listesini tutar. Bu listeleri çerçeveler penceresi olarak düşünebiliriz.

Çerçeve sıra numarasının çerçeve içinde olabildiğince az yer tutması amaçlanır. Çerçeve sıra numarası için k bitlik yer ayrılmışsa maksimum pencere genişliği N=2k-1 çerçeve olabilir.[4]

6.1.3 Veri Bağlantı Katmanının Bileşenleri

Veri bağlantı katmanı iki alt katmandan oluşur.Bunlar ortam erişim denetimi(Media Access Control-MAC) ve mantıksal bağlantı kontrolü(Logical Link Control-LLC) dür.

<table>
<tr><td rowspan="2">Veri Bağlantı Katmanı</td><td>LLC</td></tr>
<tr><td>MAC</td></tr>
</table>

Şekil2: Veri bağlantı katmanının yapısı

6.1.3.1 Ortam Erişim Kontrolü(Media Access Control-MAC)

OSI katmanlarına göre 2. katman olan veri bağlantı katmanı (Data Link Layer) protokolüdür. Temel görevi aynı ağda bulunan ve birbiri ile temas halindeki bilgisayarların veri iletişimini sağlamaktır. Kısaca MAC adı da verilen bu kontrol aynı zamanda bilgisayarların üzerindeki ortama erişirken kullanılan cihazlar için bir de adresleme yapmaktadır. Bu adrese MAC adresi adı verilmektedir ve dünya üzerinde sadece tek bir cihaz Ağ bağlantı Kartı (Network Interface Card-NIC) üzerinde olabilecek bu numara IEEE tarafından dağıtılmaktadır.Ortam erişim kontrolünün diğer bir görevi ağ üzerine aynı anda erişmekte olan birden fazla bilgisayar arasındaki uyumu sağlamaktır.Görevleri:

- ✓ Ağ katmanından aldığı veri paketlerine hata kontrol bitlerini ekleyerek çerçeve(Frame) halinde fziksel katmana iletme işinden sorumludur.
- ✓ İletilen çerçevenin doğru mu yoksa yanlış mı iletildiğini kontrol eder, eğer çerçeve hatalı iletilmişse çerçevenin yeniden gönderilmesini sağlar.
- ✓ MAC alt katmanı veriyi hata kontrol kodu (Cyclic Redundancy Check-CRC) , alıcı ve gönderenin MAC adresleri ile beraber paketler ve fiziksel katmana aktarır.
- ✓ Alıcı tarafta da bu işlemleri tersine yapıp veriyi veri bağlantısı içindeki ikinci alt katman olan LLC'ye aktarmak görevi yine MAC alt katmanına aittir.

MAC Adresleri IP gibi, host (bilgisayar) ve ağ (network) olarak parçalara ayrılmamıştır. Dolayısıyla bir MAC adresine bakarak bir bilgisayar ile aynı ağda olunup olunulmadığı anlaşılamaz. Bir MAC adresi 48 bitten oluşur ve onaltılık (hexadecimal) tabanda 6 adet ikili olarak ifade edilir.Örneğin: 00-00-00-00-00-00 şeklinde gösterilir.

6.1.3.2 Mantıksal Bağlantı Kontrolü(Logical Link Control-LLC)

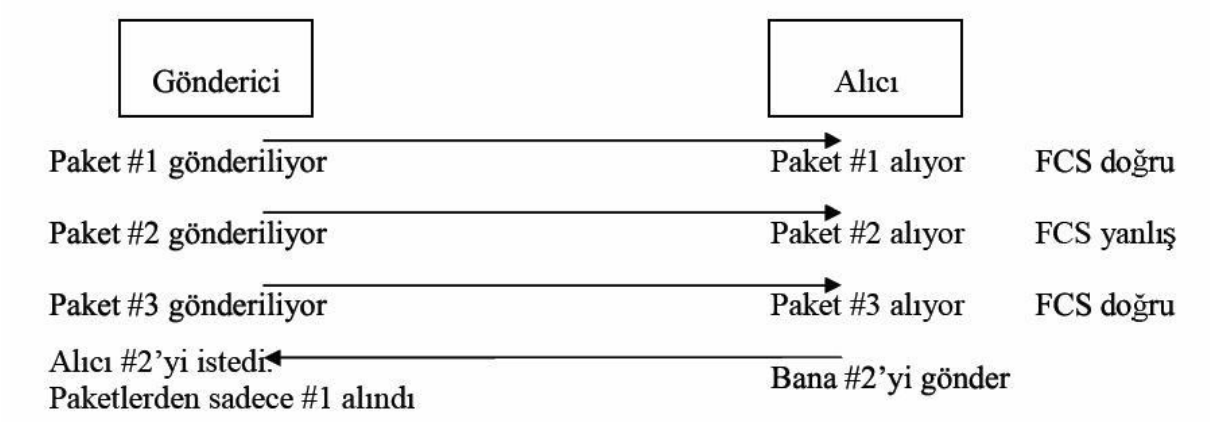
LLC alt katmanı bir üst katman olan ağ katmanı (3. katman) için geçiş görevi görür. Protokole özel mantıksal portlar oluşturur (Service Access Points, SAP). Böylece kaynak makinede ve hedef makinede aynı protokoller iletişime geçebilir (örneğin TCP/IP-TCP/IP). LLC ayrıca veri paketlerinden bozuk gidenlerin (veya karşı taraf için alınanların) tekrar gönderilmesinden sorumludur. Flow Control yani alıcının işleyebileceğinden fazla veri paketi gönderilerek boğulmasının engellenmesi de LLC'nin görevidir.

6.2 HATA TESPİTİ VE DÜZELTİLMESİ

Veri bağlantı katmanı, fiziksel katmandan aldığı veriyi bir üst katmana iletirken verinin doğruluğunu kontrolünü gerçekleştirir. Bunu her çerçeve sonuna bir kontrol dizisi ekleyerek sağlar. (FCS Frame Check Sequence) FCS alanına kaydeder. Akıcı cihaz aynı matematiksel işlemler yapar ve sonucu çerçeve içerisinde FCS alanına kaydeder. Alıcı cihaz aynı matematiksel işlemleri tamamladığında elde ettiği değeri aldığı çerçeve üzerindeki FCS alanı ile karşılaştırır. Bu iki değer eşit değilse iletim esnasında bazı bit hataları oluştuğu tespit edilir. Hata olduğu anlaşıldığında gelen paket işlenmez. Hata giderme ise, protokolün veri kaybı olduğunda harekete geçerek verinin yeniden istenmesini sağladığı anlamına gelir. Birçok protokol hata giderme mekanizmaları sunarlar. İletilen veri etkilenir ya da numaralandırılır. Veri alındıktan sonra alıcı hata tespit ederse hatalı olan veri paketini bu numara ile yeniden ister.

Veri iletiminde patlama (burst) ve rasgele (random) hata olarak adlandırılan iki tip hatayla karşılaşır. Patlama hatasında, çevre koşulları nedeniyle bir süre alıcıya gerçek olmayan anlamsız bir bilgi gelir. Bu süre 1–100 ms olabilir; bu süre içinde iletim ortamından geçen tüm bitler bozulabilir. Rasgele hatada, iletim yolundaki gürültü nedeniyle bilgi katarı içindeki rasgele bir bitin bozulması söz konusudur. Bu bazen bir bit bazen birkaç bit olabilir[1].

Gönderici paketleri sıralı bir şekilde gönderir. Alıcı taraf her paket için FCS kontrolü yapar. Ve bir diğer paketi alır. Bu işlem belirli bir paket alındıktan sonra alıcı taraf paket isteğinde bulunur. Bu şekildeki gibi 4. paket isteği gittiğinde ilk 3 paketin doğru bir şekilde iletildiğini gösterir. Paketlerin numaralandırılması bazı protokollerde 0 olan başlar bazılarında gönderici makine tarafından belirlenir. Bazı protokollerde numara çerçeveye, pakete verilirken bazı protokollerde gönderilen byte büyüklüğünü verir.



Şekil – 2 Hata Giderme

Hata giderme işlemi göndericiden gelen veriler alıcı tarafında FCS kontrolünden geçer ve hata tespit edildiğinde hatalı olan veri tekrar istenir. Alıcının hatalı istediği veri başarılı veri iletişimin olduğu son veridir. Bazı protokollerde hata düzeltme işlemi sadece hatalı veriyi içerir. Bazılarında ise hatalı olan veriden sonraki veriler de tekrar gönderilir.

6.2.1 HATA TESPİT TEKNİKLERİ

Gönderilen veri bitleri hata sezmeye uygun kodlama yapılarak iletilirse, alıcı her hata sezdiğinde vericiye aynı veriyi tekrarlama isteği gönderir. Çeşitli hata sezme teknikleri vardır. Bunlardan bazıları yalnızca hata olup olmadığını kontrol ederken, bazıları da hataları belirli oranda hata düzeltmesi yapar[2].

6.2.1.1 YANKILAMA (ECHOPLEX)

Bu yöntem daha çok bir merkeze (host) bağlı terminallerde kullanılmaktadır; terminalde tuşa basıldığında bu tuşa karşı düşen karakter merkeze gider. Merkez hem bu karakteri işler, hem de gönderen terminale geri yankılar. Terminal merkezden gelen bu karakteri ekrana çıkarır veya yazıcıya aktarır. Böylece terminal başındaki kullanıcı hataları görebilir.

6.2.1.2 EŞLİK DENETİMİ (PARITY CHECK)

$$m + r + 1 \leq 2^r$$

m: gönderilecek bitlerin sayısı
r: Eşlik bitlerinin sayısı

Şekil 2 Sıralı Veri İletimi

En sık kullanılan hata saptama yöntemidir. Eşitliğin (parity) hesaplanması iletilen verinin içerisinde ki birlerin bulunmasıyla yapılır. Tek eşitlik kullanılıyorsa birlerin sayısı eşlik biti ile beraber tek olur. Çift eşitlik kullanılıyorsa birlerin sayısı eşlik biti ile beraber çift olur. Örneğin; dört bitlik veri 0110 ise çift denklik kullanılmışsa denklik biti 0 olur. Tek denklik kullanılmışsa denklik biti 1 olur.

Eğer veri içinde çift sayıda hata olursa, hata sezilmeden kalır; hata tek sayıda ise sezilir. Bu uygulama daha çok boyu 7,8 bit gibi kısa veri aktarılmasında kullanılır[3].

6.2.1.3 İKİ BOYUTLU EŞLİK DENETİMİ (DIMENSIONAL PARITY)

İki boyutlu eşlik sınamasında verilerin her birinin Eşlik bitlerinin haricinde bit sırasına göre de eşlik biti oluşturulur. Bu yöntemde hata tespit edilebildiği gibi hangi bitin hatalı olduğu da bulunabilir. Her veri için bir eşlik bitinin haricinde ayrıca eşlik verisinin gönderilmesi gerekmektedir.

$$G = [\ I{:}A\ ]$$

G: Üreteç Matris
I: Birim Matris
A: Eşlik üreten matris

Şekil – 3 Dimensional Parity

6.2.1.4 TOPLAMA DENETİMİ (CHECKSUM)

Veri dizelerini modül toplamlarının kullanıldığı hata denetleme yöntemidir. Toplama işlemi genellikle son byte'ın toplama sınaması numarasını ifade ettiği byte paketleri üzerinde gerçekleştirilir. Paket içindeki tüm sayıları topladığınızda mod 256 üzerinden toplam sıfır olmalıdır. Eğer değilse hata oluştuğu tespit edilir.

6.2.1.5 CRC (ÇEVRİMLİ FAZLALIK DENETİMİ – CYCLIC REDUNDANCY CHECK)

Bu yöntemde CRC olarak adlandırılan ve gönderilen veri bloğundan hesaplanan bir sınama bloğu, bu veri bloğunun sonuna eklenir. CRC bloğunu hesaplamak için donanım desteği veren iletişim yongaları mevcuttur.

Uygulaması kolay ve güvenliği güçlü bir tekniktir. CRC tekniği veri çerçevelerinin koruması için kullanılır. Gönderici her çerçeveye n bitlik FCS (Frame Check Squence) dizi ekler. CRC (dönüşümlü fazlalık sınaması) veri iletiminde kullanılan en yaygın hata denetimi yöntemidir. Az bir ek bilgi ile daha fazla hata tespiti sağlar.

CRC veri bitlerini polinom kodlar olarak ele alır. Veriler, gönderici tarafından çerçevenin içeriğine göre her çerçevenin sonuna eklenecek bir denetim seti (check digits) hesaplanarak gönderilir. Alıcı taraf veri üzerinde aynı denetim işlemlerini gerçekleştirerek aldığı veride hata olup olmadığını kontrol eder. İki sonuç uymuyorsa bu hata olduğunu gösterir. N bitlik FCS için n+1 bit bir P polinomu kullanılır. Amaç FCS'yi Q/P sıfır olacak şekilde elde etmektir.

0110 - 0	Çift Denklik
0110 - 1	Tek Denklik

CRC oluşturulması ilk olarak veri içeriği iki üzeri n ile çarpılır. Bu verinin sonuna n adet 0 ekleme demektir. İkinci adımda P üreteç polinomu ile bölünmesi, üçüncü adımda kalanın FCS olarak iletilmesidir.

CRC kontrolü ise ilk olarak veri çerçevesi alınır. İkinci adımda P üreteç polinomuna bölünür. Üçüncü adımda kalan kontrol edilir. Kalan sıfır ise veri doğru olarak alınmıştır. Eğer sıfırdan farklı ise hata oluşmuştur.

6.3 HATA DÜZELTME TEKNİKLERİ

Göndericinin bilgiyi bozulma durumunda tekrar göndermesinin güç olduğu bazı uygulamalarda, uygun kodlama ile hatanın alıcıda düzeltilmesine çalışılır. Yolda bozulabilecek bit sayısının üst sınırının bilindiği varsayılır.

Hata düzeltme (error correction) kodlaması kullanılırsa, alıcı, vericinin gönderdiği veriyi belirli bir bozulama ölçüsüne kadar düzeltebilir. Yani, verinin tekrar gönderilmesi istenmeden hata giderilebilir. Bu tür yöntem sadece iletim yolu çok pahalı ise ya da büyük bir gecikme oluşturuyorsa kullanılmaktadır[3].

6.3.1 HAMMING KODLAMASI

Hamming kodlaması, genel olarak tek bit hataların düzeltilmesi veya veri içerisinde iki bitlik hataların tespitini sağlar. Temel olarak eşlik kontrolü yapar. Hamming kodu uygulamada tek veya çift bit hataların tespiti veya yalnızca tek bit hataların düzeltilmesi için kullanılır. Bu işlem birden fazla eşlik bitinin kullanılmasıyla sağlanır. Gereken eşlik veya hata kontrolü gönderilecek bitlerin bir fonksiyonu olan hamming kuralı ile belirlenir. Veri bitlerine eklenen hesaplanmış eşlik bitlerine hamming kodu mesajı denir.

1	0	0	1	0	1	0	**1**
0	0	0	1	1	0	0	**0**
0	1	0	0	0	1	1	**1**
0	1	1	0	1	0	1	**0**
0	0	1	0	1	1	0	**1**
1	0	0	1	0	1	0	**1**
1	0	1	0	1	0	1	**0**
1	**0**	**1**	**1**	**0**	**0**	**1**	**0**

Veri iletimi, veri ve hata saptama kodları birleştirerek gerçekleştirilir. Birleştirilmiş veri kod sözcük (Codeword) olarak adlandırılır. n=m+r bit kod sözcük m bit veri ile r bit hata saptama kodunun birleşmesinden oluşur. İki kod sözcüğü farklılaştığı en düşük bit konumu sayısı kodun hamming uzaklığı tanımlanır. Hamming uzaklığı bulmak için önce iki kod sözcüğüne XOR işlemi gerçekleştirilir ve işlem sonucunda elde edilen birlerin sayısı toplanır.

Burada hesaplama yapıldığında hamming uzaklığın 2 olduğu görülüyor. Çünkü geçerli her kod sözcüğü en az iki bitte farklıdır. Bu da bize bu şemanın 2 bit hatayı saptayamayacağını gösterir.

Tek bit hata oluşursa geçersiz kod sözcüğü ortaya çıkacağından bunu saptayabilir. Hamming uzaklığı üç olan bir kod sözcük tek bit hataları düzeltebilir, iki bit hataları bulabilir. n hatayı saptaya bilmek için n+1 koda n hatayı düzeltmek içinse 2n+1 koda gerek duyulur.

Hamming kod mesajı veri bitlerinin G üreteç matrisi ile veri bitinin mantıksal işlemlerle çarpımı sonucu elde edilir. Elde edilen kod mesaj vektörü olarak adlandırılır. Bu asıl veri bitleri ve hesaplanan eşlik bitlerinden oluşur.

6.3.2 ARQ (AUTOMATIC REPEAT REQUEST – OTOMATİK TEKRAR İSTEĞİ)

İletim sırasında verinin bütünlüğü ve doğru bir şekilde iletilmesi için ARQ kullanılır. ARQ için uygulanan yöntemler olumlu doğrulama, zaman aşımı sonrasında yeniden gönderim, olumsuz doğrulama ve yeniden gönderim. Olumlu doğrulama: Alıcı hatasız aldığı tüm çerçeveler için bir doğrulama iletisi gönderir. Zamanaşımı sonrasında yeniden gönderim: Gönderici gönderdiği veri çerçeveleri için belirli bir sürede olumlu doğrulaşma almadığı zaman çerçeveyi yeniden göndermesi. Olumsuz doğrulama ve yeniden gönderim:

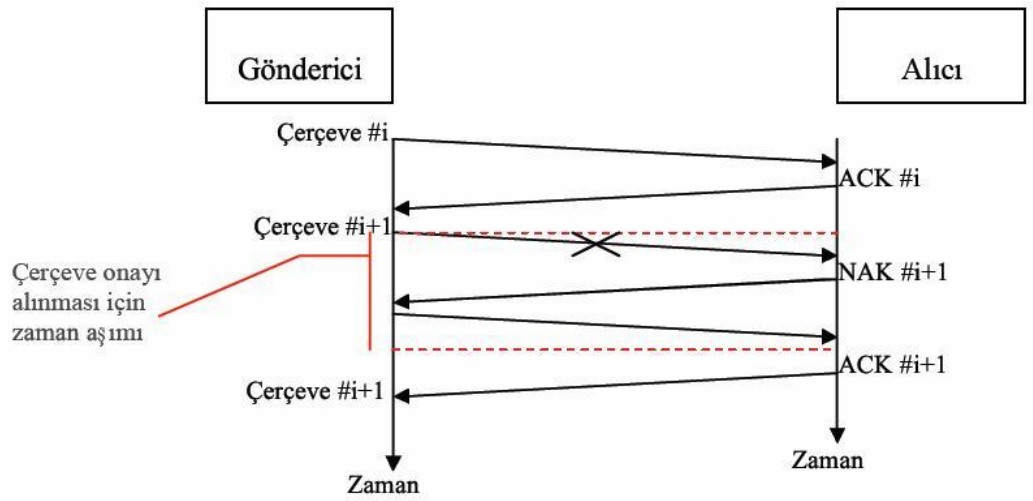
Alıcı hatalı alınan bir çerçeveden sonra olumsuz doğrulama iletisi göndererek hatalı çerçevenin yeniden gönderilmesini sağlar.

İki tür ARQ istemi ve bunlara ait iletişim kuralları vardır. Beklemeli Tekrar İstemi (Idle RQ) ve Sürekli Tekrar İstemi (Continious RQ).

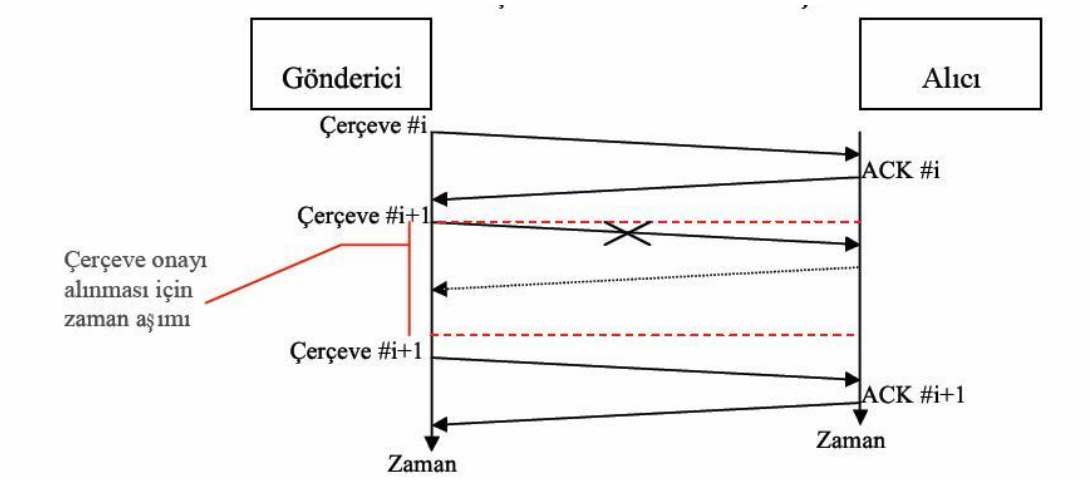
0000000 0
0000001 1
0000010 1
0000011 0

6.3.3 DUR VE BEKLE PROTOKOLÜ

Beklemeli tekrar isteme hata denetimi, veri çerçevelerinin gönderen ile alıcı arasında güvenilir bir biçimde iletilmesinden sorumludur. Veri çerçevesi alıcıya gönderildikten sonra doğru olarak gönderilip gönderilmediği bilgisi geri dönene kadar beklenir. Veri hatasız alındığı onaylandıktan sonra bir sonraki çerçeve gönderilir.



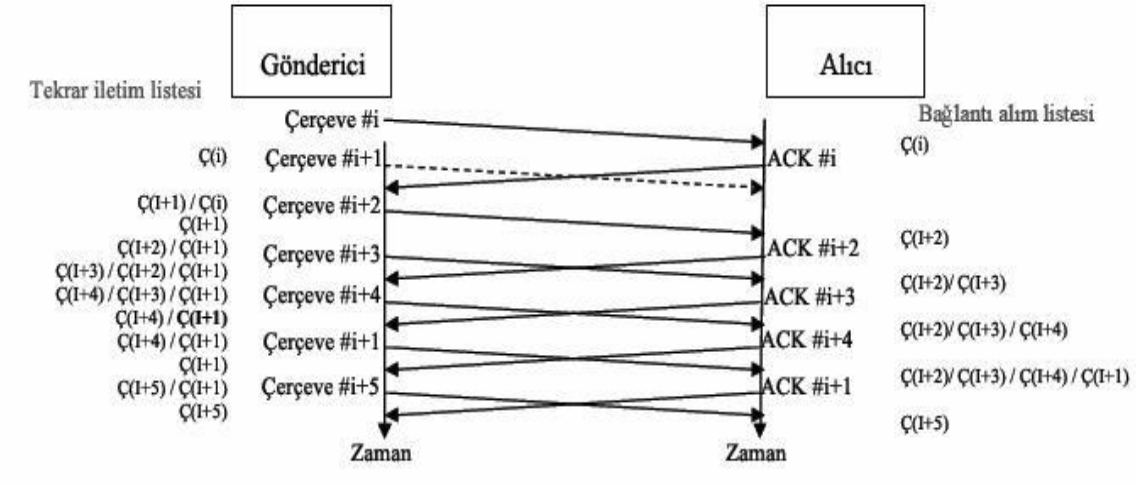
Şekil – 4 Normal Veri Akışı



Şekil – 5 Gönderilen Çerçevenin Bozulması

Veri iletim sırasında gönderilen çerçevelerden biri iletim sırasında bozulursa alıcı taraftan bir onay cevabı gelmeyecektir. Onay alınması için daha önceden belirlenen çerçeve iletim zamanı içerisinde onay alınmadığından zaman aşımı işleme devreye girecektir. Son gönderilen veri tekrar gönderilir. Bu işlem onay cevabının bozulması durumunda da gerçekleşir. Fakat alıcı tarafa bu kez aynı çerçeveden iki tane alınmış olur. Bunlardan biri silinir. Bu şekilde veri bütünlüğü sağlanır.

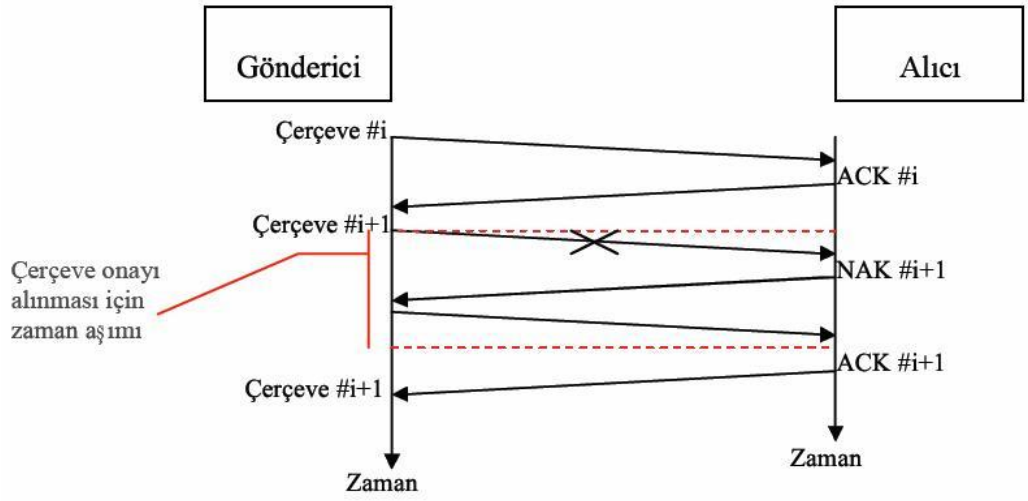
Dur bekle protokolünde bir başka durumda hatalı verilerinde bildirilmesidir. Alıcı tarafta alınan çerçevede bozulma tespit edildiğinde NAK hatalı çerçeve bilgisi gönderir. Gönderici taraf gelen bu hatalı çerçeveyi tekrar gönderir. NAK hatalı çerçeve bilgisinin kullanılması zaman aşımı süresini beklemeksizin devam ettirilir ve iletişim hattı daha verimli kullanılır.



Şekil – 6 Gönderilen Çerçevenin Bozulması ve NAK Gönderilmesi

6.3.4 SÜREKLİ TEKRAR İSTEMİ (Continious RQ)

Sürekli tekrar isteminde gönderici alıcı taraftan ACK çerçevelerinin gelmesini beklemeden art arda veri çerçevelerini gönderir. Kaynak birden çok çerçevenin doğrulamasını bekler bu durumda çerçevenin tekrar gönderilme olasılığına karşı kopyasını saklar. ACK çerçevesi alındığında ise tekrar iletim listesinden ACK'da belirtilen çerçeve silinir. Alıcı tarafta sırası farklı olarak gelebilir. Alınan çerçeveler bağlantı alım listesinde tutulur. Sürekli tekrar istemi ve hata denetim işlemi çift yönlü bir iletişim gerektirir. Gönderici tarafta ACK çerçevelerinin alınmasını beklemeden gönderilen çerçeve sayısı tekrar iletim listesinin büyüklüğü ile sınırlıdır.

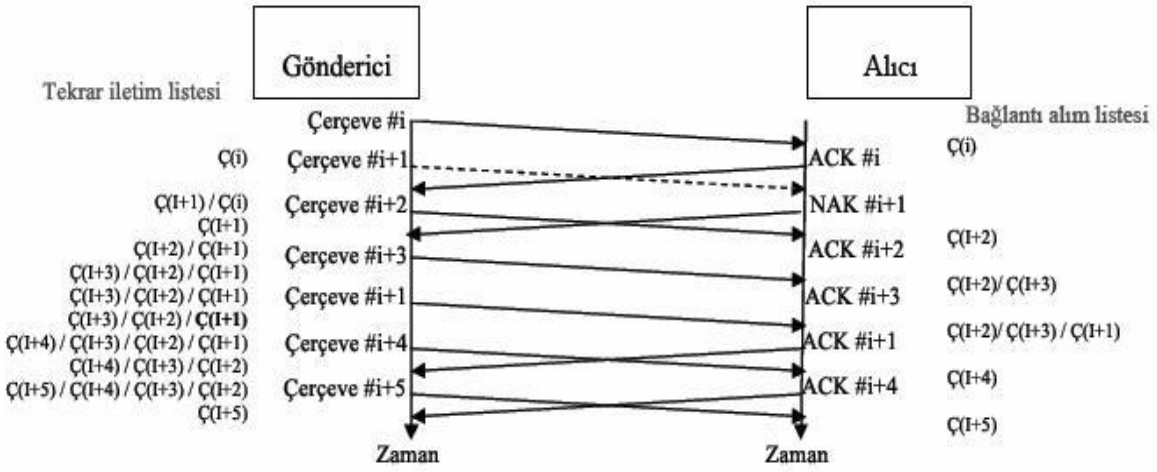


6.3.5 SEÇMELİ TEKRAR (SELECTİVE REPEAT)

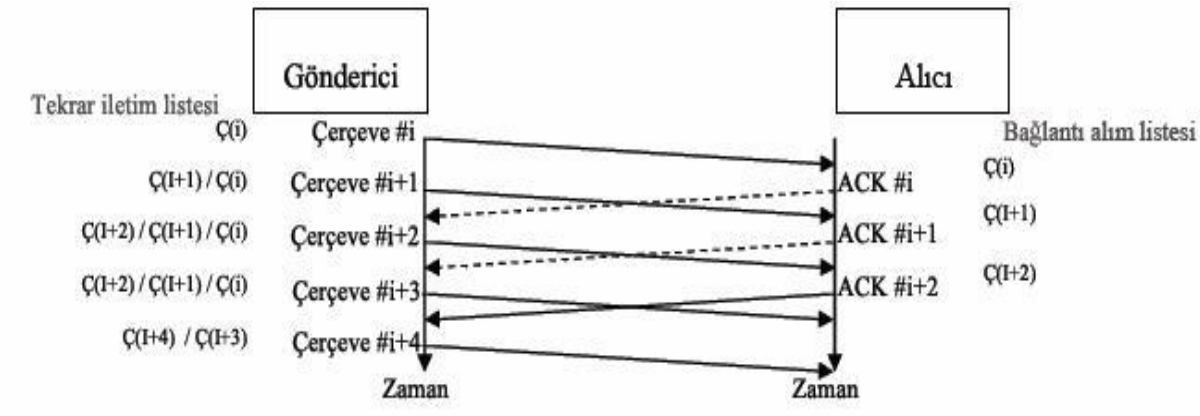
Veri iletişiminde bir hata oluştuğunda hatanın giderilmesi için seçmeli tekrar (selective repeat) veya N çerçeve gerile yöntemden biri kullanılır. Seçmeli tekrar yönteminde alıcı taraf veri dizisindeki hatalı çerçeveyi saptar ve yalnızca hatalı çerçevelerin tekrar iletilmesini sağlar. N çerçeve gerile yönteminde ise alıcı sıra dışında bir çerçevenin alındığını saptar ve doğrulanmış son çerçeveden başlayarak tekrar iletim listesinde bekleyen tüm doğrulanmamış son çerçeveden başlayarak tekrar iletim listesinde bekleyen tüm doğrulanmış çerçeveleri yeniden ister.

Seçmeli tekrar işlemi iki şekilde yürütülür. Belirsiz tekrar gönderim ve belirli tekrar gönderim. Belirsiz tekrar gönderimde alıcı hatasız alınan çerçeveleri doğrular ve gönderici ack çerçevelerini kontrol ederek eksik çerçeve olup olmadığına karar verir. Belirgin istekte ise alıcı sıralamada eksik olan bir çerçeve için özel bir olumsuz doğrulama gönderir. Her iki

durumda da çerçeve sıra dışı alınırsa alıcı bunları bir sonraki çerçeve gelinceye kadar bağlantı alım listesinde tutar.



Şekil – 8 Çerçevenin Bozulma Durumu ve Tekrar Gönderim



Şekil – 9 Çerçevenin Bozulma Durumu ve Belirgin Tekrar Gönderim

6.3.6 N ÇERÇEVE GERİLE (GO BACK N)

Alıcı taraf sıra dışı bir çerçeve aldığı zaman belirtilen çerçeve numarasından başlayarak çerçevelerin yeniden iletilmesini ister. Bunu özel bir olumsuz doğrulama çerçevesi göndererek yapar. Alıcı taraftan hatalı olan çerçeve istendiği zaman gönderici tekrar iletim listesinden bu çerçeveden sonrakileri gönder.

Göndericiye herhangi bir NAK hata mesajı gelmediğinden veri iletimine devam edilir. Gönderici ACK i + 2 doğrulama mesajını aldığı anda i + 2 ve önceki verilerin doğru olduğunu saptar ve iletim tablosundan bunları çıkarır. N çerçeve gerile stratejisi doğru çerçeve sıralamasının korunduğu ve iletişim için tampon belleğin en aza indirgendiği gösterir. Ancak doğru olarak gönderilen çerçevelerin bazıları tekrar iletildiğinden iletişim ortamını seçmeli tekrar iletim yöntemine göre daha fazla kullanılır.

6.4 KABLOSUZ AĞ TEKNOLOJİSİ

Kablosuz haberleşme teknolojisi, noktadan noktaya veya bir ağ yapısı şeklinde bağlantı sağlayan, bir teknolojidir. Kablosuz haberleşme teknolojisi, günümüzde hala en çok kullanılan kablolu veya fiber optik iletişim teknolojisiyle benzerlik göstermektedir. Kablosuz haberleşme teknolojisi iletim ortamı olarak havayı kullanması diğerlerinden ayıran en büyük özelliğidir. Metal kablolar, elektrik akımını iletirken kablosuz ve optik iletim sistemleri belli frekanstan elektro-manyetik dalga iletmektedir.

Kablosuz iletişim bir bina ya da bir grup bina içinde yani daha küçük alanlar içinde sunucular, yazıcılar ve diğer uç nokta aygıtlara bağlanmak için radyo dalgalarını kullanır.

Bununla birlikte kablosuz teknoloji cep telefonları ile konuşan, dizüstü bilgisayarlar ile donatılmış, zamanının çoğunu çalışma masasından uzakta geçiren, toplantılara katılan, çapraz organizasyonlu takımlarında çalışan hareketli kullanıcıları akla getirir.

Kablosuz iletişim bu şekilde çalışan, bilgilerine herhangi bir yerden, kafeteryadan, toplantı odasından bilgilerine ulaşmak isteyen çalışanlar için uygun bir ortam sağlar.

Wi-Fi ; "Wireles Fidelity" kelimelerinin kısaltması olup kablosuz bağlılık veya kablosuz bağlantı anlamına gelir. Wi-Fi ürünlerin kablosuz bağlantı sağlayabildiğini gösteren bir uyumluluk göstergesidir ve IEEE 802.11a, IEEE 802.11b, IEEE 802.11g ve IEEE 802.11n standartlarına göre belirlenir.

Wi-Fi dizüstü bilgisayarlar, PDA' lar ve diğer taşınabilir cihazların yakınlarındaki kablosuz erişim noktaları aracılığıyla yerel alan ağına bağlanabilmesini sağlar. Bağlantı, kablosuz erişim noktaları ve cihazın ortak desteklediği, IEEE 802.11 protokolüne bağlı olarak 2.4 GHz veya 5 GHz radyo frekansında gerçekleştirilir.

6.4.1 Yerel Alan Bilgisayar Ağları (LAN, Local Area Networks)

Yüksek hızlı, küçük alanları (bir bina, bir firma, bir departman, bir oda) kapsayan bir veri ağıdır. Yerel ağ içinde bilgisayarlar, yazıcılar, çiziciler, CDROM sürücüleri ve diğer çevre birimleri yer alabilir. Yerel ağlar bilgisayar kullanıcılarına uygulamalara ve cihazlara ulaşım, bağlı kullanıcılar arasında dosya değişimi, elektronik posta ve diğer uygulamalar yoluyla haberleşme gibi çeşitli avantajlar sağlarlar.

İntranet ve yerel ağ birbirlerinden ayrı tutulamayan iki kavramdır. Eğer bir LAN şirket içinde kurulmuşsa ve şirket personeli tarafından kullanıma açık ise "intranet" adını alır. Bu ağ üzerinde http sunucu, ftp dosya sunucusu, veri tabanı sunucuları ve haber öbekleri bulunur.

Yerel ağlar, yazıcı, CDROM gibi pahalı donanımlar, uygulama programları ve daha önemlisi kullanıcıların işlerini yapmaları için gerekli bilgi gibi hayati kaynakları elektronik olarak paylaşmalarına olanak sağladıkları için kısa sürede popüler hale gelmişlerdir. Yerel ağların geliştirilmesinden önce bilgisayarlar diğerlerinden izole edilmiş ve kendi uygulamalarına göre sınırlandırılmışlardı. Bu kişisel bilgisayarların birbiri ile bağlanmasıyla, verimlilikleri büyük ölçüde artmıştır. Fakat LAN yapısı itibarı ile yerel bir ağ olduğu için ancak bir bina veya bir kat içerisinde kurulabilir. Bilgisayar ağlarının tam anlamıyla faydalanmak, coğrafi olarak nerde olursa olsun, fiziksel olarak nasıl ayrılırsa ayrılsın, birbirinden ayrı yerel ağların tüm çalışanları ve bilgi-işlem kaynaklarını bir araya getirecek şekilde bağlanmasıyla gerçekleşir

6.4.2 Geniş Alan Bilgisayar Ağları (WAN, Wide Area Network)

Bir ülke ya da dünya çapında yüzlerce veya binlerce kilometre mesafeler arasında iletişimi sağlayan ağlardır.Coğrafi olarak birbirinden uzak yerlerdeki (şehirlerarası/ülkelerarası) bilgisayar sistemlerinin veya yerel bilgisayar ağlarının birbirleri ile bağlanmasıyla oluşturulur. Genellikle kablo ya da uydular aracılığı ile uzak yerleşimlerle iletişimin kurulduğu bu ağlarda çok sayıda iş istasyonu kullanılır. WAN' lar üzerinde on binlerce kullanıcı ve bilgisayar çalışabilir. Şirketinizin Ankara, İzmir ve İstanbul şubelerini bir

WAN bağlantısı ile birleştirdiğinizde, Ankara'da bulunsanız bile İstanbul'daki bir makineyi tıpkı önündeymiş gibi yönetebilirsiniz.

6.4.3 Şehirsel Bilgisayar Ağları (MAN, Metropolitan Area Network)

LAN' ın kapsadığı alandan daha geniş, fakat WAN' ın kapsadığından daha dar mesafeler arası iletişimi sağlayan ağlardır. Genellikle şehir içi bilgisayar sistemlerinin birbirleriyle bağlanmasıyla oluşturulur.

6.4.4 Kişisel Alan Ağları (PAN,Personel Area Network)

Bu bağlantı çeşidi kişisel iki cihazın birbiri ile kablosuz olarak bağlantı kurmasıdır. Buradaki amaç yakın mesafedeki cihazların birbirleri ile kolayca etkileşim içinde olmasını sağlamaktır. *Bluetooth, homeRF, ırDA* gibi bağlantı çeşitleri birer kişisel alan ağı kurulmasında kullanılır. Bu dokümanda özellikle kişisel alan ağları üzerine yoğunlaşılacaktır.

6.5 KABLOSUZ AĞ TEKNOLOJİLERİ

6.5.1 Bluetooth

Bluetooth™; Ericsson, Nokia, IBM, Intel ve Toshiba tarafından IrDA ve kablolu bağlantılara alternatif olarak geliştirilen kısa mesafede yüksek hızda veri aktarımı sağlayan güvenli bir kablosuz iletişim yöntemidir, denebilir. "Yöntem" denmesinin nedeni, Bluetooth' un fiziksel araçtan, iletişim sözleşmesine kadar tamamen baştan tasarlanmış olmasıdır. Esasen beş üretici tarafından geliştirilen bu standart, halka ilk defa 1998 yılında tanıtıldı. Bluetooth kablo bağlantısını ortada kaldıran kısa mesafe Radyo Frekansı(RF) teknolojisinin adıdır.

Bluetooth bilgisayar, çevre birimleri ve diğer cihazların birbirleri ile kablo bağlantısı olmadan görüş doğrultusu dışında bile olsalar haberleşmelerine olanak sağlar.721 Kbp' sa kadar veri aktarabilen bluetooth destekli cihazların etkin olduğu mesafe yaklaşık 10 veya 100 metredir. Bluetooth da 2,45 GHz ISM bandını kullanıyor. Parazitleri büyük ölçüde önleyebilmek için FHSS (Frequency Hopping Spread Spectrum) yöntemine başvuruluyor.

Yöntemde 2,402 GHz ile 2,480 GHz frekans aralığı l MHz' lik aralıklarla 78 kanala bölünüyor. Bölünme sonucu, saniyede 1.600 frekans atlaması gerçekleşebiliyor. Bu sayede de Bluetooth bağlantılar diğerlerine oranla çok daha kararlı oluyorlar.

6.5.2 Home RF

Home RF, evler için kablosuz ağ çözümüdür. Home RF, evlere ve küçük ofislere anında ve kablosuz Internet bağlantısı özgürlüğü sağlar. Sadece bir geniş bant, DSL ya da kablo bağlantısını kullanarak ailenin her üyesi kablosuz olarak Internet'e aynı anda bağlanabilir. Farklı dizüstü, bilgisayar ya da Web cihazları kullanarak ev yakınlarında istenilen zaman internette gezinti yapılabilme imkanı sağlar.

Home RF, en düşük maliyetli kablosuz şebeke çözümlerinden biridir. Önceleri sadece büyük işletmelere sunulan yüksek hız ve güvenilir şebeke sistemi, bu teknoloji sayesinde evdeki kullanıcılara ve ev-ofis çalışanlarına da sağlanmaktadır. Home RF ayrıca, apartman ve şehir merkezi gibi yüksek yoğunluktaki merkezlerde çalışma avantajına sahip olmakla birlikte mikrodalga gibi evdeki diğer radyo frekanslarıyla karışmaz. CDROM aracılığıyla yükleme; hızlı, basit ve görsel olarak anında gerçekleşir ve bütün ev birkaç dakika içinde şebekeye dahil edilir.

1999 yılında "Home RF Working Group" kablosuz ağ kullanımı üretebilmek için DECT ve IEEE 802.11 standartlarını bir araya getirdi. Kablosuz İnternet Erişim Protokolü (Shared Wireless Access Protocol-SWAP) olarak adlandırılan çözüm, son kullanıcılara yönelik. Sistemin içinde yer alan DECT sistemi konuşma hizmetlerini, paket tabanlı veri iletimini ve “Streaming Media” gibi uygulamalarda ihtiyaç duyulan kesin aktarım hızı hizmetlerini sağlıyor.

Home RF, ISM frekans sınırı içinde 2,4 GHz ile, maksimum 100 mW' lık performansla yayın yapıyor. Tıpkı IEEE 802.11 gibi Home RF de FHSS (Frequency Hopping Spread Spectrum) mekanizmasını kullanıyor. Home RF sistemi 1.6 Mbit/sn' lik veri aktarım hızına ulaşabiliyor, iletişimi hem birebir olarak hem de bir kontrol noktası (Control Point "CP") üzerinden kurmak mümkün. Buradaki Control Point, IEEE 802.11 standardında kullanılan Erişim Noktası uygulamasına benziyor. Konuşma için kullanılan Kontrol Noktası, aynı anda sekiz telefon görüşmesini yapabilecek kapasitede olmalı. Bir ağa 256 CP bağlanabilir. Güvenlik nedeniyle her ağ yapısının ayrı bir ağ ID' si (Network ID) bulunuyor. Bu ID' nin gizli tutulmasıyla, ağa dışardan izinsiz girişler önlenir. Teorik olarak Home RF çok başarılı olmalıydı, ancak endüstrinin çıkarları farklı yönlerde olduğu için, sistem pratikte fazla tutulmadı, gelecekte yerini tamamen başka teknolojiye bırakacak gibi görünüyor.

Home RF özel veri ağlarında kullanılabilir. Ayrıca sistemi koordine eden ve telefon şebekesine (ses ve veri) bir modem sunan bir bağlantı noktasının altında da Home RF kullanılabilir.

6.5.3 IrDA (Infrared Data Association)

Bir çeşit kızılötesi iletişim teknolojisidir. IrDA teknolojisiyle çalışan en tanınmış elektronik ürün uzaktan kumandadır.1993 yılında, aralarında Hewlett Packard ve IBM'in de bulunduğu yaklaşık 30 firma, kızılötesi ışınlarla veri aktarımını standartlaştırmak için bir araya geldi. İlk standart kızılötesi arabirimi (SIR), 115.2 Kbp 'ler. Daha sonra Tiny Transport protokolü üzerinden asıl veri alışverişi gerçekleşir. Bu protokolün üzerine farklı üç protokol daha kurulu; Yerel ağ girişi için IrLAN, veri alışverişi için Infrared Object Exchange Protocol (IrOBEX), seri ve paralel arabirimlerin oluşturulması için Ir-COMM. Sonuncu protokole mobil internet erişimi için ihtiyaç duyulur. IrDA özellikle cep telefonu ve PDA pazarında yaşanan patlamadan sonra popüler oldu. IrDA hem mobil internet erişimi için hem de masaüstü bilgisayarı ile dizüstü bilgisayarı arasında veri alışverişi için kullanılıyor. Enfraruj, infrared veya IrDA olarak da bilinir.

Kızılötesi ışınların önemli kullanış yerleri son yıllarda yaygınlaşmıştır. Pek çok maddenin kimyasal analizi bu tür ışınların yardımıyla gerçekleştirilmektedir.

Özellikle İkinci Dünya Savaşında yansıyıp gelen kızılötesi ışınların görünür hale getirilmesiyle, karanlıktaki cisimler fark edilmiştir. Bu tür ışınların ısı etkisini kullanan fırınlar ve cilt hastalıkları tedavisinde kullanılan lambalar yapılmıştır. Geliştirilen yeni hassas filmlerle, ışık vermeyen fakat sıcak cisimlerin fotoğrafını çekmek mümkün olmaktadır. Bu tür fotoğraflar gün ışığında olabildiği gibi, karanlıkta da çekilebilir. Özellikle askeri sahada kullanılması, gün geçtikçe artmaktadır.

Ayrıca vücudun sıcaklık durumunun araştırılmasında, sanayide ve gözle görülemeyen yıldızların tespitinde, astronomide kullanılır. Bunun yanında polisiye olaylarda görülmeyen yazıların, parmak izlerinin ve lekelerinin tespitinde de istifade edilir.

Kızılötesi, görülebilen kırmızı ışıktan daha uzun dalga boyuna sahip, gözle görülmeyen ışınlardır. Kızılötesi ışınlar olarak da anılırlar. Isı detektörleri ile tespit edilenler en uzun dalga boyu olanlarıdır. Yaklaşık olarak, dalga boyları 0,8 mikron ile 1000 mikron arasındadır. Normal fotoğraf filmlerine tesir etmezler ve normal optik aletlerle fark edilmezler. Bunun sebebi, enerjilerinin görülen ışığın enerjisinden oldukça düşük olmasıdır. Fark edilmeleri ancak ortaya çıkardıkları ısı sonucu olur. IrDA kısa menzillidir (birkaç metre), ve cihazların iletişim kurabilmesi için birbirlerini doğrudan görüyor olmaları gerekir. IrDA kullanan cihazlar arasında dizüstü bilgisayarlar, PDA' lar ve cep telefonları da bulunmaktadır.

Kızılötesi iletişimin doğru çalışması için, kızılötesi alıcı-vericileri bakış hizası temelinde çalışmalıdır (30 derece açıyla ve 1 metreden (yaklaşık 40 inç) az arayla yerleştirilmelidir). IrDA teknik özellikleri arasında IrPHY, IrLAP, IrLMP, IrCOMM, Tiny TP, IrOBEX, ve IrLAN bulunmaktadır.

IrDA çeşitli hızlarda veri alışverişine izin verebilir. SIR (Serial Infrared) 9600 bit/s, 19.2 kbit/s, 38.4 kbit/s, 57.6 kbit/s ve 115.2 kbit/s; MIR (Medium Infrared) 0.576 Mbit/s ve 1.152 Mbit/s; FIR (Fast Infrared) ise 4 Mbit/s hızlarında çalışabilir. 16 Mbit/s hızına çıkabilen VFIR (Very Fast Infrared) ve 100 Mbit/s hızına çıkabilen UFIR (Ultra Fast Infrared) üzerinde çalışılmaktadır.

6.6 ÇOKLU ERİŞİM PROTOKOLLERİ

İletişim ortamı bazı durumlarda statik olarak yapılandırılırken bazı durumlarda dinamik olarak yapılandırılır. Bunun amacı iletişim ortamının daha verimli olarak kullanılmasıdır. Dinamik olarak paylaştırılan ortamda çoklu erişim için birçok algoritma kullanılmaktadır. Bunlar genel olarak çarpışma tabanlı ve çarpışmasız protokoller olarak bilinir. Aloha, CSMA, CSMA/CD çarpışama tabanlı protokollerdir. Çarpışmasız protokoller ise FDDI, jetonlu halka, DQDB gibi. [5]

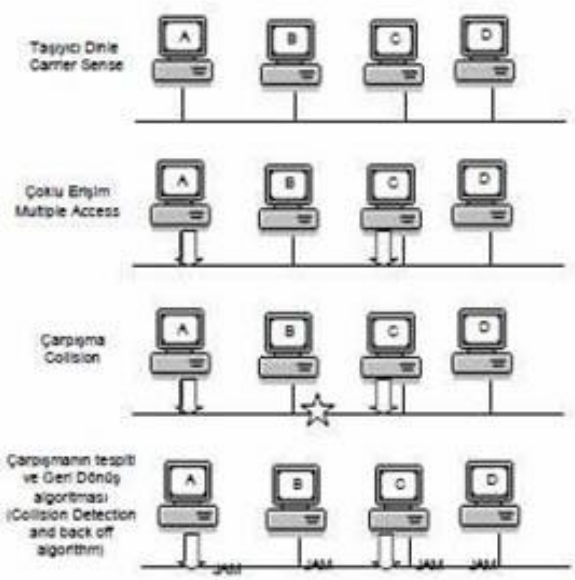
6.6.1 Aloha

1960'ların sonunda Amerika'da Hawaii adaları arasındaki iletişimi sağlamak üzere University of Hawaii ALOHA adıyla bir geniş alan ağı kurdu. İlk iletişim protokolü çerçeve göndermek isteyen her bilgisayar çerçevesini gönderebilir. Fakat şanslı olan bilgisayarların çarpışma olmadan çerçevelerini iletirler. Çarpışma olduğunda bilgisayarlar belirli bir süre bekleyip tekrar şanslarını denerler.[4] Bu iletişim ortamının verimini oldukça azaltır. Bunu gidermek için 1972 yılında yeni bir sürüm hazırlandı. İletişim ortamı zamana göre bölünerek kullanıldı. Zaman bölmeli Aloha, çerçeveler belirli zaman aralıklarında gönderilmesi sağlanır. İletişim kanalı böylelikle daha verimli olarak kullanılır[3].

6.6.2 CSMAP (Carrier Sense Multipli Access Protocol)

CSMA protokolde bir bilgisayar iletişim hattını kullanmadan önce dinler. Hat boş ise çerçevesini gönderir. Hat dolu ise başka bir bilgisayar veri gönderiyor demektir.[3] O zaman hattınboşalmasını bekleyecektir. Bu yöntemde birkaç bilgisayar aynı anda hattın boş olduğunu görüp veri gönderebilir. O zaman çarpışma oluşur ve çerçeveler bozulur. Çarpışmaları önlemek için CSMA/CD kullanılır. CSMA/CD erişim metodunda, listen-before-transmit iletişimden önce dinle modunda çalışmayla veri network cihazlarına iletilir. Bunun

anlamı cihaz veri iletmek istediği zaman ilk olarak aktarım ortamının meşgul olup olmadığı kontrol etmelidir. Eğer node, ağın meşgul olduğunu tanımlarsa, tekrar denemeden önce rastgele bir süre bekleyecek. Eğer node network'ün meşgul olmadığını tanımlarsa node iletme ve dinleyişe başlayacak. Node diğer istasyonların, aynı anda 68 iletmiyor olduğundan emin olmak için dinler.[1] Veri iletimini tamamladıktan sonra cihaz, dinleme moduna döner.

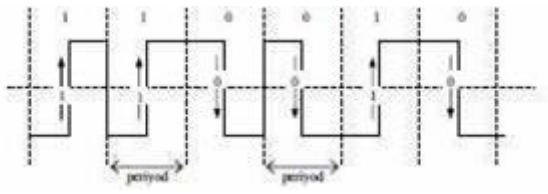


Şekil 3 Ağ üzerinde çarpışma oluşması

Kontrol yapan Ağ cihazları, network medyasında sinyalin büyüklüğü, arttığı zaman çarpışma tespit ederler. Çarpışma gerçekleştiğinde, bütün cihazlar, çarpışmayı saptadığında Backoff algoritması uygulanır. Cihazlar çarpışmayı bildirmek için JAM sinyali gönderirler. JAM sinyalini alan düğümler, iletişimi rastgele bir zaman dilimi için durdururlar. Gecikme zamanı, sona erdiğinde, ağda bütün cihazlar, ağ ortamına erişimi kazanmak için çalışırlar. Veri iletimi, ağda yeniden başladığında, çarpışmada içeren cihazlar, veriyi göndermek için önceliğe sahip değillerdir.

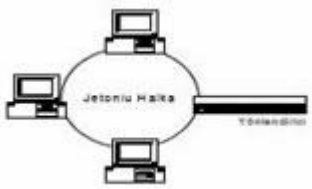
6.6.3 CSMA/CD

CSMA/CD fiziksel katman topolojisi ilk zamanlar pasif ortak yoldan ibaretti; ancak anahtar cihazların uygulamada yaygınlaşmasıyla birlikte yıldız-anahtarlamalı yol da kullanılmaktadır.802.x protokolleri LAN fiziksel katmanlarında çoğunlukla Manchester kodlaması veya 4B5B diye adlandırılan kodlama tekniği kullanılır. Manchester kodlamasında bit süresinin ortasında çıkan ya da düşen kenar, bitin 1 ya da 0 olarak değerlendirilmesini sağlar.[5]



Şekil 4 Manchester Kodlaması

Yukarıdaki şekilden görüleceği gibi Manchester kodlaması ile ne iletilirse iletsin, hat üzerinde her zaman bir titreşim olur ve titreşim sayesinde herhangi bir düğüm hattın meşgul ya da boş olduğunu kolayca ayırt edebilir. Hattaki titreşim bir taşıyıcı işareti andırdığı için 802.3 türü LAN için taşıyıcı sezmeli sözcüğü kullanılır.[5]



Şekil 5 Jetonlu Halka

6.6.4 Çarpışmasız Protokoller

İletişim ortamını her an sadece bir bilgisayarın kullanılmasını garanti eden protokollerdir. İletişim hattını kontrol için bir jeton kullanılır. Jeton kimde ise o bilgisayar çerçeve iletimini gerçekleştirir. İletişimini tamamlayan bilgisayar jetonu ortama bırakarak başka bilgisayarların kullanmasını sağlar. İletişim ortamındaki tüm bilgisayarlar bir mantıksal halka oluşturularak birbirine bağlanır. Bu halkada iletişimi kontrol etmek için bir jeton oluşturulur. Bu jeton sırasıyla oluşturulan halka bilgisayarları dolaşır. Çerçeve göndermek

isteyen bilgisayar jetonu alır ve çerçevesini gönderir. Gönderme işlemi tamamlandığında jetonu tekrar halkaya bir başka bilgisayarın kullanımına sunar. Böylelikle iletişim ortamının her an bir bilgisayarın kullanımı garanti altına alınır. Çarpışmaların önüne geçilmiş olur.[2]

6.7 AĞ BİLEŞENLERİ

6.7.1 Yineleyici (Repeater)

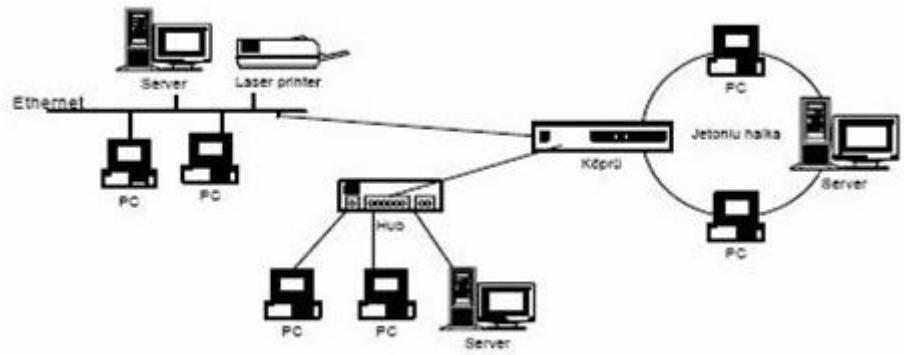
Kablonun kapasitesinden daha fazla mesafelere bağlantı kurulması gerektiğinde araya bir yükseltici konularak sinyalin güçlendirilmesini sağlayan cihazdır.

- Ağ kablosunun erişebileceği maksimum mesafeyi uzatırlar.
- Ağdaki maksimum düğüm sayısını arttırır.
- Kablo arızalarının etkisini azaltabilir.
- Farklı kablo tipleri kullanan ağları birleştirebilir.

6.7.2 Bridge (Köprü)

İki ağı birleştirirler ve bilgi paketlerinin geçişini sağlayan cihazdır. Köprüler genel anlamda yineleyicilerin yaptığı işi yaparlar. Köprülerin birleştirdiği yerel alan ağlarının herbirine bölüt (segment) adı verilir. Bridge'nin fonksiyonu gelen sinyalleri diğer network parçasına geçip geçmeyeceğini karar verir.[5]

- Büyük ağları küçük parçalara ayırırlar.
- Küçük ağları büyütmeyi sağlarlar.
- Trafik yoğunluğunu azaltırlar.
- Farklı fiziksel iletim ortamı birleştirilebilir.
- Köprüler farklı ağlarda kullanılamazlar.
- Stratejik olarak yerleştirilirse ağ performansını büyük ölçüde arttırır.



Şekil 6 Farklı Topolojideki Ağların Köprü ile Birbirine Bağlanması

Köprü, ağ trafiğini düzenlerler. İki girişi vardır. Aldıkları bilgiyi kontrol eder. Başlığa ve port numarasına bakarak bir nevi bekçi görevi yapar. Bir ağda oluşan hatayı diğer ağa ansıtmazlar. Köprüyü çok girişli yaparak switch'leri oluştururuz.[4]

6.7.2.1 Köprü Türleri

Şeffaf Köprüler (Transparent Bridges)

Aynı veri bağı katmanı protokolüne sahip olan LAN'ları birbirine bağlayan protokollerdir. Şeffaf denmesinin nedeni köprülerin ağa bağlı makineler tarafından görülmemesidir.

Kaynaktan Yönlendirilmeli Köprüler (Source Routing Bridges)

Bilginin varış adreslerini kaynak kullanıcı tarafından belirlenmesine olanak veren köprü türüdür. Bu köprüler yönlendirici sayılmazlar.

Çevirici Köprüler (Translating Bridges)

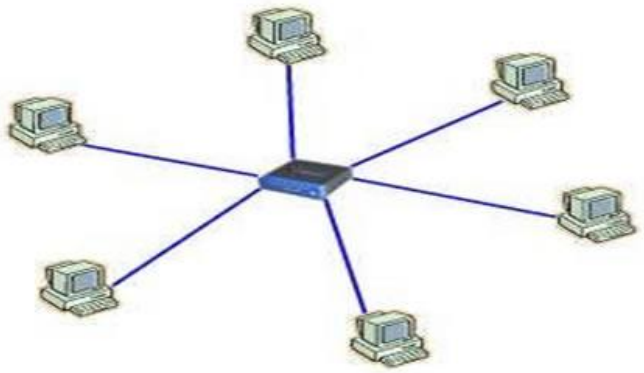
Mac alt katmanları farklı olan LAN'lar arasında kullanılır.

Uzaktan Bağlantı Köprüleri (Remote Bridges)

Bunlar birbirlerine kiralık hatlar ile bağlanır. Noktadan-Noktaya veri bağı protokolünü kullanırlar.

6.7.3 Hub

HUB, en yalın ağ cihazıdır; kendisine bağlı olan sistemlere paylaşılan bir yol sunar. HUB' a bağlı tüm sistemler aynı yolu kullandığı için, aktarım yapmak isteyen birçok bilgisayar olsa da aynı anda tek bir iletim yapılabilir; diğerleri yolun boş olmasını beklemelidir.[5]



Şekil 7 Hub

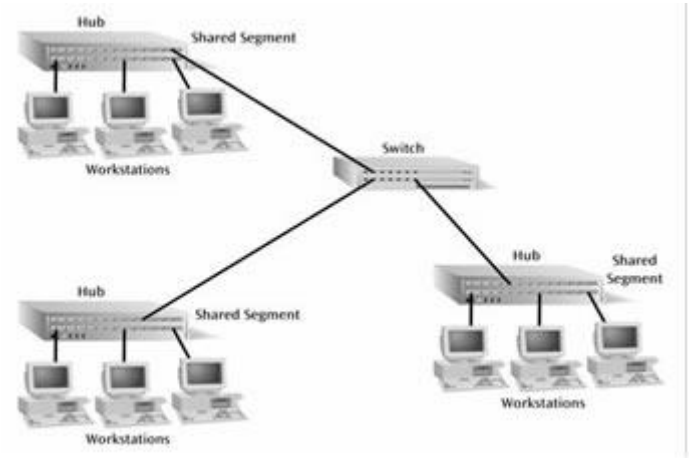
Şekil 8 Hub

- Hublar birbirine bağlanarak ağ büyütülebilir.
- Verinin içeriğiyle ilgilenmez, veriyi bütün bilgisayarlara gönderir. Bu yüzden güvenilir değildir.
- Yıldız ağ topolojisinde kullanılır.

- Gelen bilgileri hepsini tüm bilgisayarlara gönderir.
- Bu bir ağ kurarken kullanılabilecek en basit ağ gerecidir.
-

6.7.4 Anahtarlar (Switch)

Yerel ağlarda bant genişliğini arttırarak ağı hızlandıran köprülere benzeyen fakat daha hızlı olan cihazlardır. Kendisine bağlı sistemleri anahtarlamalı bir yol ortamı sunar; aynı anda birden çok iletim yapma olanağı vardır bunlara akıllı HUB' da denir. Fakat HUB' dan daha pahalıdır. Gelen bilgileri sadece belli bir bilgisayarlara gönderir. Ağ durumunu izler, veriyi gönderip, iletim işleminin yapılıp yapılmadığını test eder.[5]



Şekil 9 Switch

6.7.4.1 Anahtarların Veri Aktarım Yöntemleri

Cut – Through

Paketin tamamı alınmadan alıcının MAC adresini okuduktan sonra yönlendirmeye başlayan anahtar çeşididir. Bu teknik hızlıdır ve uzun paketlerde verimi yüksektir. Dezavantajı hatalı gelen paketler üzerinde düzenleme yapmadan gönderir.[3]

Store-And-Forward

Paketin tamamı alındıktan sonra alıcıya yönlendirilir. Kullanıcıya filtre koyma ve trafiğin akışını denetleme imkânı tanır. Dezavantajı yavaş olmasıdır.[3]

6.7.5 Router (Yönlendirici)

Switch'ler gibi paket yönlendirir fakat farklı sistemleri de birbirine bağlar. Ağlar arası (LAN-LAN, LAN-WAN, WAN-WAN) haberleşmenin yapılabilmesi için ara bağlantıyı sağlar. Routerin bir işlemcisi, epromu ve üzerinde bir işletim sistemi IOS (Internal Operating System) vardır. Bu yüzden Gelen paketin başlığından ve yönlendirme tablosu bilgilerinden yararlanarak yönlendirme kararlarını verme yeteneğine sahiptir.

Büyük ve değişik protokollere sahip bilgisayar ağlarını birleştirirler. Yönlendiriciler bir ağ üzerindeki tüm bilgisayarların adreslerini bilir ve buna göre kendilerine gelen paketi en uygun şekilde hedefe yollar. Yönlendiriciler genellikle dinamik yönlendirmeyi kullanır. Bunun anlamı kendisine gelen bir paketin tüm ağ taranarak en güvenli ve hızlı yolun denenmesidir. Verinin içeriğini inceler ve iletilmesi gerekmiyorsa iletmez. Eğer herhangi bir sorun çıkarsa, alternatif bir yol arayarak mutlaka paketi hedefine ulaştırmaya çalışırlar. Yönlendiriciler ağa bağlı özel bir araç veya ağa bağlı bir bilgisayar olabilirler.[5]

7 BÖLÜM

7.1 UYGULAMA KATMANI

Uygulama katmanı veya 7. katman (İngilizce: application layer), programların ağı kullanabilmesi için araçlar sunar. Bilgisayar uygulaması ile ağ arasındaki arabirim görevini yerine getirmektedir.

Katmanların sıralanışında kullanıcıya en yakın olanıdır. Sadece bu katman diğer katmanlara servis sağlamaz. Uygulama katmanında ise uygulamaların network üzerinde çalışması sağlanır.

Uygulama katmanı ağ hizmetini kullanacak olan programdır. Bu katman kullanıcının gereksinimlerin karşılar. Örneğin veritabanı uygulaması ya da e-mail uygulaması.

Microsoft API'leri uygulama katmanında çalışır. Bu API'leri kullanarak program yazan bir programcı, örneğin bir ağ sürücüsüne erişmek gerektiğinde API içindeki hazır aracı alıp kendi programında kullanır. Alt katmanlarda gerçekleşen onlarca farklı işlemin hiçbirisiyle uğraşmak zorunda kalmaz.

Uygulama katmanı için bir diğer örnek HTTP'dir. HTTP çalıştırılan bir program değil bir protokoldür. Yani bir kurallar dizesidir. Bu dizeye göre çalışan bir tarayıcı (browser), aynı protokolü kullanan bir Web sunucuya erişir.[1]

7.1.1 Uygulama Katmanı İletişim Kuralları

HTTP
SMTP
UUCP
NNTP
SIP
RTP
NTP
TELNET
NFS
SSH
POP
FTP
SNMP

7.1.1.1 HTTP (İngilizce Hypertext Transfer Protocol, Türkçe Hipermetin Aktarma İletişim Kuralı)

Bir kaynaktan dağıtılan ve ortak kullanıma açık olan hiperortam bilgi sistemleri için uygulama seviyesinde bir iletişim kuralıdır.

Geçmişi HTTP, 1990 yılından beri Dünya Çapında Ağ (WWW) üzerinde küresel bilgi girişimi için kullanılmaktadır.

HTTP/0.9 olarak anılan ilk sürüm HTTP İnternet üzerinden ham verinin taşınması amaçlı, basit bir iletişim kuralıydı. RFC 1945 dâhilinde tanımlanan HTTP/1.0, taşınan verinin meta-bilgilerini ve istek/cevap semantiği düzenleyicilerini içeren ve MIME ilgileri taşıyan mesajların taşınabilmesi gibi yenilikler ile bir önceki sürümü genişletmiştir. Yine de HTTP/1.0 hiyerarşik vekil sunucuların (proxy), önbelleğin, kalıcı bağlantı ihtiyaçlarının ve sanal sunucuların etkilerini göz önünde bulundurmada yetersiz kalmaktaydı. Ek olarak, HTTP/1.0 olarak anılan uygulamaların, tam olarak kesinleştirilememiş yöntemleri, birbirleriyle iletişim içinde bulunan iki uygulamanın kapasitelerinin tam olarak anlaşılması için yetersiz kalmakta ve bu sürümün bir yeniliğe gidilme ihtiyacını zorunlu kılmaktaydı.

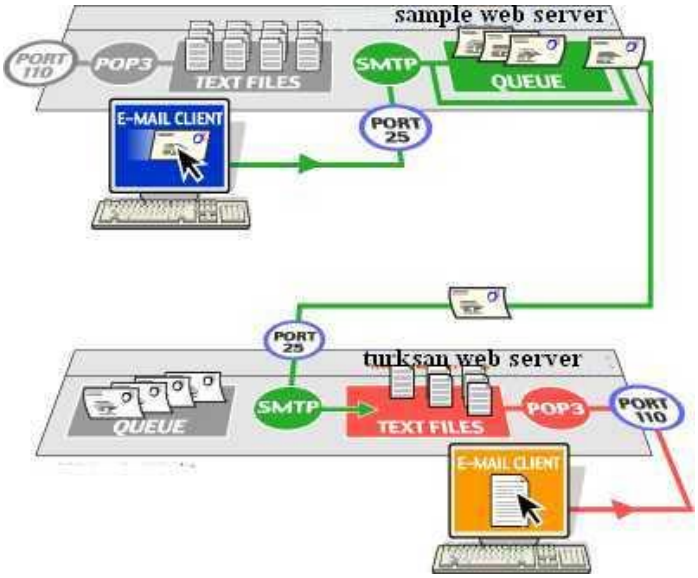
HTTP/1.1 olarak bilinen bu yeni sürüm, iletişim kuralının güvenilir bir biçimde uygulanmasında ihtiyaç duyulan dizisel gereksinimleri içermekte ve 1.0 sürümüne sahip iletişim kuralından daha güvenli olarak görülmektedir.

Uygulamalı bilgi sistemleri, basit bir şekilde bilgi almaktan çok daha fazla uygulamaya ihtiyaç duyar. Bu uygulamalar arama, son kullanıcı ara yüzünün güncellenmesi ve etkileşimli olarak bilgi girişi gibi işlevleri de gerektirmektedir. HTTP, bir isteğin amacının ne olduğunu anlatan bir takım açık uçlu yöntemler ve üstbilgi kullanımına izin vermektedir. Bir tekbiçimli kaynak tanımlayıcısı, yer belirleyici ya da kaynak ismi tarafından sağlanan kaynağa, bir yöntemin uygulanışını bildiren bir dizi kural üzerine kurulmuştur. Gönderiler, Çok Amaçlı İnternet Posta Uzantıları tarafından tanımlandığı ve İnternet postasında kullanılana benzer bir biçimde aktarılmaktadır.

HTTP aynı zamanda, SMTP, NNTP ve FTP gibi iletişim kurallarını destekleyen İnternet sistemleri ile kullanıcı istemcileri, vekil sunucular ve Geçitler arasında iletişim için özelleştirilmiş bir iletişim kuralı olarak da kullanılır. Bu haliyle HTTP, muhtelif uygulamalar tarafından sağlanan kaynaklara, basit hiperortam erişimine izin vermektedir. Günümüzde hayatın önemli bir parçası haline gelen İnternet, HTTP sayesinde her türlü bilgiye sorunsuz erişimi kolay kılmaktadır.[2]

7.1.1.2 SMTP

Günümüzde kullanılan e-mail sistemlerinde sunucu makinede iki farklı server çalışmaktadır. Bunlardan biri Simple Mail Transfer Protokol' ün kısaltması olan SMTP serverdır. SMTP server giden mailleri yönetir. Diğer sunucu ise POP3 server veya IMAP serverlardan biridir. Bu serverlar gelen mailleri yönetmektedirler. POP, Post Office Protokol; IMAP ise Internet Mail Access Protokolün kısaltmasıdır. Tipik bir e-posta sunucusu aşağıdaki gibidir:

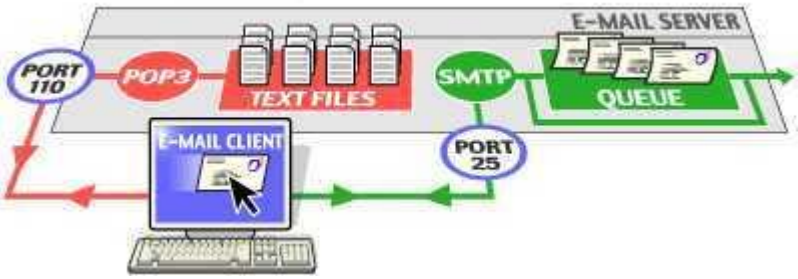


Şekil1

SMTP server 25 numaralı portu, POP3 110 numaralı portu ve IMAP 143 numaralı portu kullanır.

7.1.1.3 SMTP Server

Bir e-posta gönderilmek istendiğinde e-mail client programı SMTP ile etkileşime girer.



Şekil 2

Bir mail göndermek istediğimizi farzedelim. E-posta adresimiz info olsun ve sample.com' da bir hesabımız bulunsun. info@turksan.com adresine bir mail atmak isteyelim. E-mail client olarak Outlook Express kullanılsın.

Sample' da bir hesap açıldığı zaman Outlook Express' te mail server kısmına mail.sample.com yazılmalıdır. Bir mesaj yazılıp gönder butonuna tıklandığında aşağıdaki olaylar gerçekleşir.

1- Outlook Express mail.sample.com' daki SMTP servera 25 numaralı portu kullanarak bağlantı kurar.

2- Outlook Express SMTP server ile iletişim kurar. SMTP servera göndericinin adresini, alıcının adresini ve mesaj gövdesini anlatır.

3- SMTP server posta gönderilecek mail adresini iki parçaya böler. Yani info (alıcı ismi) ve turksan.com (alan adı) olmak üzere iki parçaya ayırır.

4- SMTP server domain name server (DNS) ile haberleşir. DNS' e turksan.com adresi için bir IP sorar. DNS bu sorguyu turksan.com' un IP adresiyle cevaplar.

5- sample.com' daki SMTP server turksan.com adresindeki SMTP server ile bağlantı kurar. Bu bağlantı 25 numaralı port üzerinden gerçeleşir. Gönderilen mesaj alıcı servera ulaşır. turksan.com' daki SMTP server e-mail adresinin doğru olup olmadığını kontrol eder. Sonuç olumluysa mail turksan.com' un POP3 serverına ulaşır ve buradan mail listesinde görülebilir.

Herhangi bir sebepten ötürü sample.com adresindeki SMTP server turksan.com' daki SMTP server ile haberleşemezse mesaj sıraya girer. Bu sayede mesaj tekrar tekrar gönderilmeye çalışır.

SMTP server bazı basit text komutlarını anlayabilir. En çok kullanılan komutlar:

HELO: kendini tanıt

EHLO : kendini tanıtıp, erişim istemek

MAIL FROM : göndericiyi tanımla

RCPT TO : alıcıyı özelleştir.

DATA : mesaj gövdesini tanımla (to, from ve subject ilk üç satır olmalıdır.)

RSET : reset

QUIT : oturumu kapat

HELP : komutlarda yardım al

VRFY : adresi tanımla

EXPN : adresi genişlet

VERB : gereksiz sözlerle dolu[3]

7.1.1.4 UUCP

Unix'den Unix'e kopyalama anlamına gelen UUCP, en eski dial-up ağıdır. Çoğunlukla Unix makinelerini birbirine bağlar. Esas olarak e-mesaj servisi verir. Pek çok yerde Usenet ile iç içe geçmiştir. Mesajlar bir makineden komşu makineye gider. Adreslerken bir miktar yol bilgisini bilmek gerekir: yol üzerindeki önemli bazı makineleri belirtmek gerekir.

USENET ise uucp temelli Network News dağıtımında ortaya çıkan bir ağdır. UUCP ve USENET dağıtık bir yapıya sahip, gönüllü esasına göre demokratik bir şekilde yönetilirler. Merkezi bir otorite yoktur. UUCP e-mesaj ve News ile yetinmek isteyenler için ucuz bir alternatiftir. [4]

7.1.1.5 NNTP

NNTP, Network News Transfer Protokolün kısaltmasıdır. Genellikle Usenet erişimi, ve Usenet trafiği taşıyan sunucular tarafından kendi aralarında kullanılır.

İnternet erişiminin atası sayılabilinecek iletişim protokol formatıdır. Daha html standartlarının beta olmaktan öteye geçemediği zamanlarda görsel grafik arabirimden çok uzak bir şekilde daha çok text içerikli genel bilgi içeriği taşıma amacıyla oluşturulmuştur. Daha sonra binary özelliği kazandırılarak geliştirilmesi bir noktada sonlandırılmış olsa da düşük miktarda veri iletişimi açısından zamanla unutulacağı öngörülerini haksız çıkararak bir noktada kalıcılığını ispat etmiş bir iletişim protokolü olarak kendini ispatlamıştır.[5]

7.1.1.6 SIP

Protokolü) iki veya daha fazla katılımcı arasında bağlantı kuran bir Ağ protokolüdür. Bu protokol RFC 3261 (daha önce RFC 2543) dokümanlarında açıklanmıştır. Ayrıca SIP internet Telefonu için kullanılan en yaygın protokoldür.

SIP, uygulama katmanında çalışır ve HTTP protokolüne çok benzer düz metin bir protokoldür. Oturum açar, oturum parametrelerini değiştirir, oturumu sonlandırır. Oturumlar IP telefon çağrıları, multi medya sunumlar veya konferans şeklinde olabilir.Aynı zamanda mevcut bir oturuma kullanıcı çağırabilir. Mevcut oturuma medya ekleyebilir, çıkarabilir.

SIP'in bir oturum kurmak için ve sonlandırmak için gerçekleştirdiği 5 fonksiyon vardır:

- Kullanıcı konumunu belirlemek.
- Bağlantıya katılacak kullanıcıları tespit etmek.
- Araçların kapasitelerini tespit edip o şekilde medya parametrelerini ayarlamak.
- Çağrı yapma ve iki uçtaki çağrı parametrelerini ayarlamak.
- Oturum yönetmek.
- SIP'in kendisi bir veri taşıma protokolü değildir. SIP veriyi RTP gibi bir protokolle gerçek zamanlı taşıyabilir.

7.1.1.7 RTP (Real-time Transport Protocol)

Gerçek zamanlı ses, görüntü ya da simülasyon verilerinin uçtan ucu taşınmasını sağlayan protokoldür. RTP, kaynak ayrımı (resource reservation) yapmaz ve hizmet kalitesini garanti etmez. RTCP (RTP Control Protocol), RTP protokolu ile birlikte çalışır ve oturumda yer alan tüm kullanıcılara periyodik olarak kontrol paketleri göndererek alma kalitesi (reception quality) ile ilgili bilgi sağlar. Eğer sıkışıklık oluşmaya başlamışsa, uygulama veri hızını azaltabilir.

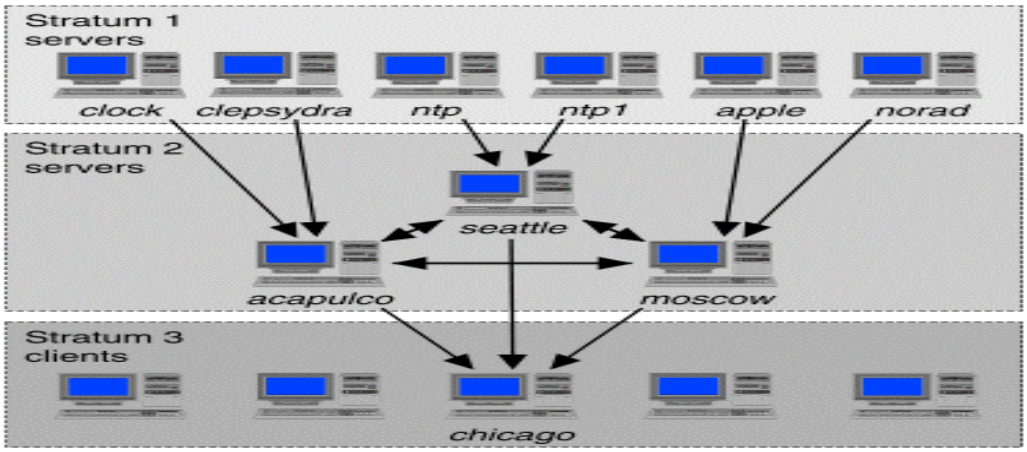
7

7.1.1.8 NTP (NETWORK TİME PROTOCOL)

Cihazların zaman ve tarih bilgileri başka bir kaynaktan alabilmeleri sağlayan protokol NTP(Network Time Protokol) dür .

Kurumsal firmalarda gelişen ihtiyaçlar doğrultusunda kullanıcılara zaman bazlı kurallar uygulamaya başladılar. Cisco cihazlarda dâhili saat bulunmamaktadır. Cihazlar kapatılıp açıldığında üzerinde bulunan saati kaybedip varsayılan zaman değerine dönmektedir. Cihazlar varsayılan değerine döndüğü için cihaz üzerinde zaman bazlı yazılan kurallar çalışmaz hale gelir . İşte burada NTP devreye girmektedir [5] .

Kurumsal network içinde bütün cihazların (router , switch ,firewall , server) zaman ayarlarının doğru olması gerekir . Zaman ayarı doğru olmazsa cihazların kontrolü, ne zaman yeniden başladığı, oluşan hatanın ne zaman olduğunu anlayamayız.



7.1.1.9 TELNET

Telnet, internet ağı üzerindeki çok kullanıcılı bir makineye uzaktaki başka bir makineden bağlanmak için geliştirilen bir TCP / IP protokolü ve geliştirilen programlara verilen addır. Bağlanılan makineye girebilmek (login) için orada bir kullanıcı isminizin(username) ve bağlantının gerçekleşebilmesi için bir telnet erişim programınızın olması gerekir. Fakat bazı kütüphane ve herkese açık telnet bazlı web servisleri, bağlantı sırasında kullanıcı ismi (numarası) istemeyebilirler ya da kullanıcı isim ve parola olarak ne yazmanız gerektiği bağlandığınızda otomatik olarak karşınıza çıkar.

Telnet, BBS (Bullettin Board Systems) sistemlere internet üzerinden erişimde günümüzde yaygın olarak kullanılmaktadır.

BBS: Kullanıcıların mesaj bıraktıkları elektronik bülten panosudur. Çok kullanıcılı işletim sistemleri (UNİX ve VMS) genellikle kullanıcılara metin tabanlı bir arayüz sunar ve bu sistemlerde tüm işlemler klavye vasıtasıyla komut isteminden (command prompt) gerçekleştirilir.

Telnet programı ile sanal sunucuya bağlandığımızda, uzaktan unix işletim sistemine bağlanmış oluruz.

Peki, bu ne anlama geliyor?

Bu, sanki makinenin karşısındaymışız gibi unix komutlarımızı yazabileceğimiz, programları çalıştırabileceğimiz, web sitemizi düzenleyebileceğimiz anlamına gelir .

Telnet güvensiz bir protokolüdür.

Peki niçin?

Telnet protokolü kullanıcı adı (username) ve şifrenizi (password) bağlı bulunduğumuz ağda kolaylıkla görebileceğimiz bir format olan PLAİN TEXT (düz metin) düzeninde göndermektedir. Buda ağdaki herkes tarafından kolayca görülebileceği anlamına gelir.

Üzerinde herhangi bir windows işletim sistemi yüklü bir makineden telnet İle bir bağlantı gerçekleştirebilmek için şu işlemler takip edilir:

1-) Başlat (start) - > çalıştır (run) menüsünü çalıştırın

2-) Komut satırına “ telnet ” ile bağlanmak istediğiniz makinenin ip adresini veya hostname ‘ ini yazarak “ ENTER ” tuşuna basınız.

3-) Eğer adresi doğru girdiyseniz bu işlemden sonra karşımıza komut satırı gelecektir.

4-) Kullanıcı adını ve kullanıcı şifrenizi girdikten sonra artık sunucuya bağlanmış olursunuz.

7.1.1.10 NFS (NETWORK FİLE SYSTEMS)

Oldukça yüksek hızlarda veri transferi yapmak için kullanılan, SUN firması tarafından geliştirilen bir dosya paylaşım sistemidir .

NFS servisi bir bilgisayarda hem server, hem client hem de client/server olarak çalıştırılabilir.

Disksiz bilgisayarlara hizmet verebilir.

Bir NFS server lokal diski olmayan bilgisayarlara hizmet verebilir.

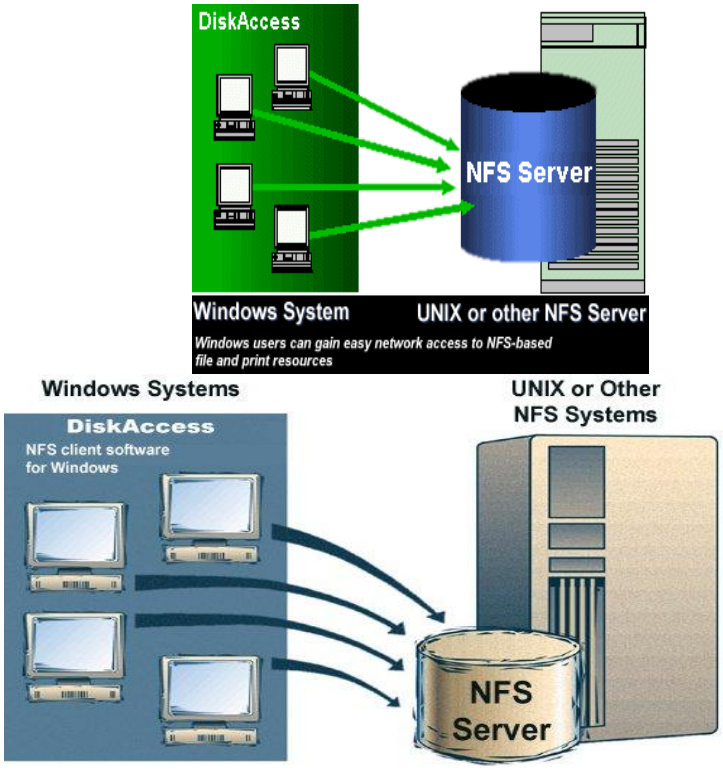
Disksiz bir bilgisayar sadece client görevinde olabilir ve tamamıyla dosyaları üzerinde barındıran NFS server ‘ a bağımlıdır.

Client bir bilgisayar, paylaştırılan dosyaları yükleyerek ayağa kalkabilir.

NFS bağlantıları, NFS servisi 2049. Portta udp ve tcp üzerinden çalışır.

NFS, çok uzun zamandır unix ve linuxta kullanılmasına karşın Windows sürümlerinde direkt olarak desteklenmemekteydi. Piyasada yalnız olmadığını farkeden Microsoft Windows 2008 , windows vista ve Windows 7 sürümleriyle direkt olarak destek vermektedir.

Microsoft ‘un bunu sağlamanın başlıca nedeni çok hızlı olmasının yanında yüksek donanım ihtiyacı hissetmemesidir.



Şekil 4

7.1.1.11 NFS DOSYA SİSTEMİ ve WEBNFS

Servisi ile paylaştırılan objeler bir dizinin tümü ya da bir parçası olabileceği gibi bir tek dosya dahi olabilir. Bir NFS server daha önce paylaştırılmış ve bu paylaşımla kesişen ikinci bir paylaşıma izin vermez.

Örnek : “ /var/mail ” ve ardından “ / var “ paylaştırılamaz.
NFS üzerinden printer ve modem paylaştırılamaz.
Sonuç olarak NFS üzerinden sadece dosya ve dizin bazlı paylaşımlar mevcuttur.
WEBNFS : WebNFS paylaşımıyla kişiler nfs desteği olan browserlardan ilgili paylaşımları görebilirler . Ve verilen yetkilere göre işlem yapabilirler.

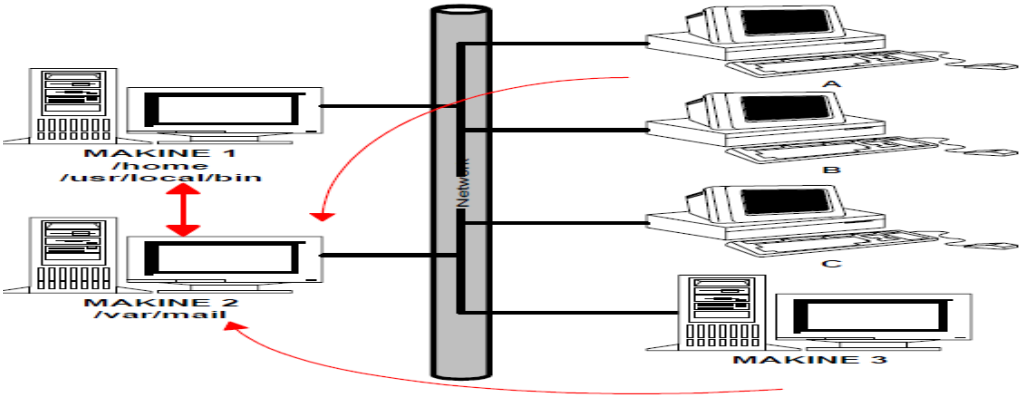
NFS ‘ nin Faydaları

1-) Aynı dosyaları birçok bilgisayara kullanabilir. Böylece ağ üzerindeki herkes aynı veriye ulaşır.
2-)Veri depolamada ucuzluk sağlar. Her bir uygulama için yerel diske kurulum yapma yerine uygulamaların paylaştırılması sağlanır.
3-)Veri tutarlığı ve esnekliği sağlar çünkü tüm kullanıcılar aynı dosya kümelerini kullanacaklardır.
4-)Kullanıcılardan bağımsız, şeffaf bir dosya erişimi sunar.
5-)Heterojen bir ortam sağlar.
6-)Sistem yönetimindeki zorlukları azaltır.

1000 Mbit hızında bir bağlantı, anlık olarak 125 Mbit hızında dosya transferi sağlamaktadır. Hem NFS hem de SAMBA bu hızlarda yapılabilecek dosya transferini kolayca yönetebilmektedirler.
Burada performans etkeni olarak hız değil, anlık yapılan bağlantı sayısı ana etken olarak alınmaktadır.

7.1.1.12 SAMBA:

Linux ve Unix işletim sistemleri ile Windows NT ve Windows 98 işletim sistemleri arasında bağlantıyı sağlayan bir uygulamadır.



Şekil 5

7.1.1.13 SSH (SECURE SHELL)

SSh güvenli kabuk anlamına gelir. Ağ üzerindeki başka bilgisayarlara erişmek, bir bilgisayarda komutlar çalıştırmak ve bir bilgisayardan diğerine dosya transferi amaçlı geliştirilmiş bir protokoldür. Güvensiz kanallar üzerinden (internet vs) güvenli haberleşme olanağı sağlar. SSH aşağıda belirtilen unsurları sağlar [6] .

Authentication (Kimlik Denetimi)

Encryption (Şifreleme)

Integrity (Bütünlük)

SSH Helsinki Teknoloji Üniversitesi ’ nden Tatu Ylönen tarafından ve hali hazırda iki farklı sürümü mevcuttur.

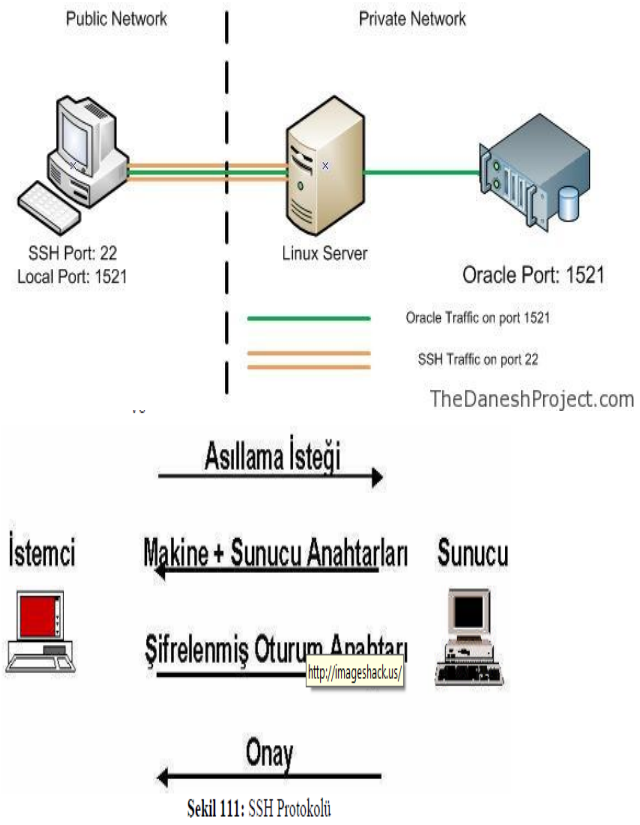
1-) Ücretsiz olarak SSh ana sayfasından indirilip kullanılabilecek sürümü

2-) Değişik UNIX sistemleri ve Windows 3x / NT , OS / 2 , MacOS için geliştirilmiş olan ticari sürümü F-Secure SSH ‘ tır .

Telnet ve rlogin kullanıcı şifreleri dahil tüm iletişim açık yani şifrelenmeden gerçekleştirilirken, SSH ise güvensiz makineler arasındaki iletişimi güçlü bir kripto yöntemiyle şifreler.

SSH içinde bağlantının gerçekleşebilmesi için Telnet ile bağlantıda olduğu gibi bir kullanıcı adına ve kullanıcı şifresine ihtiyaç duyulmaktadır. Bunların dışında birde SSH istemci programlarından birine ihtiyaç duyulmaktadır.

SSH ile kullanıcı önce kimliğini ispatlayabilmelidir.



Şekil 6

7.1.1.14 SSH İLE BAĞLANMA ADIMLARI

1-) İstemci sunucuya asıllama isteğinde bulunur.

2-) Sunucu istemciye 1024 bitlik açık makine anahtarını (host key) ve 768 bitlik RSA sunucu anahtarını (server key) gönderir.

a-Host Key : Doğru sunucuya (istenilen) bağlanmak için kullanılır .

b-Server Key : Host key ele geçse bile mesajın açılmasını önlemek amacıyla kullanılır .

3-) Eğer istemci makine anahtarını kabul ederse oturum anahtarı olarak kullanmak üzere 256 bitlik rasgele bir sayı üretir ve bu sayıyı açık makine ve sunucu anahtarıyla 2 defa şifreleyerek sunucuya gönderir.

4-) Sunucu bu mesajı açar ve oturum anahtarını elde eder. Sunucu istemciye şifreli olarak bir onay gönderir.

5-) Bu onay mesajının alınması istemciye sunucunun oturum anahtarını elde ettiği bilgisini verir.

Bazı durumlarda istemcinin de asıllaşması gerekebilir. Bunun için 2 yöntem vardır. Bunlar:

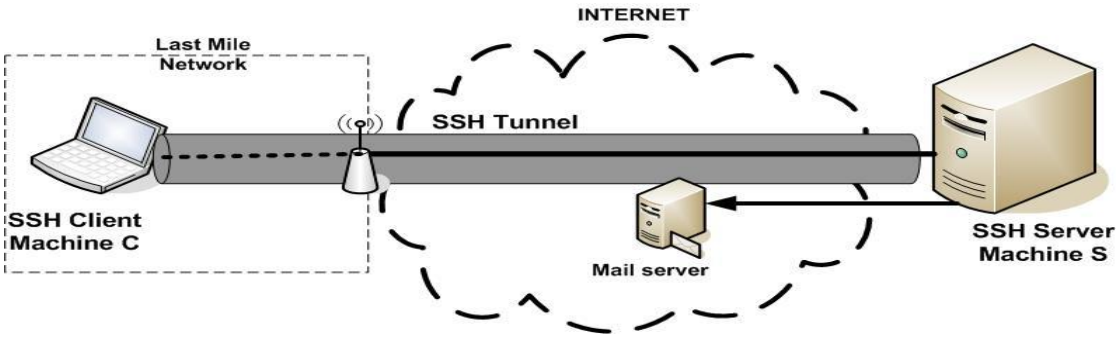
c-Şifre Asıllaması: Kullanıcı şifresi SSH ile şifrelenmiş olarak sunucuya gönderir.

d-RSA Asıllaması: Sunucu rasgele ürettiği bir sayıyı kullanıcının açık anahtarı ile şifreleyerek istemciye gönderir. İstemci sadece kullanıcının gizli anahtarını biliyorsa bu sayıyı açabilir Kullanıcı açtığı bu sayıyı MD5 ile özünü alır ve sunucuya gönderir .

Her iki durumda da sunucu bir asıllama başarılı \ başarısız mesajı gönderir. Eğer kullanıcı başarıyla asıllandıysa oturum başlar, aksi durumda kullanıcının oturum isteği reddedilir.

7.1.1.15 RSA :

Ron Rivest , Adi Shamer ve Len Adleman ‘ ın soy isimlerinden oluşan bir şifreleme algoritmasıdır (RSA) .



Şekil 7

7.1.1.16 .SSH Hangi Saldırılara Karşı Koruma Sağlar?

1-) IP gizleme yöntemiyle gerçekleşen saldırılar.

2-) IP yönlendirme yöntemiyle yapılan saldırılar.

3-) Saldırganın server isimlerinin bulunduğu kayıtları kullanarak gerçekleşen saldırılar.

4-) İki makine arasındaki veri trafiğinin aradaki başka bir makine tarafından önünün kesilerek verilerin değiştirilmesi.

5-) İletişimin gerçekleştiği iki makine arasındaki herhangi bir sunucuda bulunan kötü niyetli kişilerin verileri değiştirmesiyle gerçekleşen saldırılar.

SSH protokolünün gerçekleşen saldırılara karşı koruma sağlamasındaki uyguladığı temel politika net üzerinden gelen hiçbir iletişime güvenmemesi ve bu iletişimi şifrelemesidir.

Net üzerinden gerekli izni olmayan biri SSH bağlantısını kesebilir ancak iletişim sırasındaki şifrelenmiş veri trafiğini çözemez buda verilerin güvenli bir şekilde iletilmesi anlamına gelir.

Tüm bu şifrelemelere karşın kötü niyetli biri root kullanıcı hesabıyla sisteme girebilir ve SSH protokolünü rahatlıkla geçebilir. Yine bu kötü niyetli kullanıcı home dizinine girdiği takdirde güvenlik yok olmuş demektir. Bu durum eğer home dizini NFS ile oluşturulmuşsa sıkça karşılaşılır.

7.1.1.17 SSH ile TELNET Arasındaki Farklar

1-) SSH bağlantının tüm içeriğini, ağ üzerinde gerçekleşebilecek tüm saldırılara karşı güçlü bir kripto yöntemiyle şifrelerken Telnet protokolünde şifreleme yoktur ve iletişim açık bir şekilde gerçekleştirilir.

2-) Telnet protokolü sunucu üzerindeki bazı ayarların değiştirilmesine olanak sağlarken SSH ve bazı modern TELNET ‘ ler buna izin vermez çünkü sunucu üzerindeki bazı ayarların değiştirilmesi güvenlik problemlerine neden olabilmektedir.

3-) SSH ile ilgili bir diğer önemli özellik ise bağlanılmak istenen sunucuya şifre girme sorumluluğu olmamasıdır. SSH buna imkân sağlar. Rlogin protokolü de şifresiz bağlantıyı sağlar, fakat bunu güvensiz bir şekilde yapar. SSH ise bu işlemi daha güvenli bir şekilde gerçekleştirir.

4-) Son olarak SSH sunucuya bağlanmamızı ve otomatik olarak komut göndermemizi sağlar . Bu şekilde gönderilen komut sunucu tarafından işlendikten sonra bağlantı kesilir.

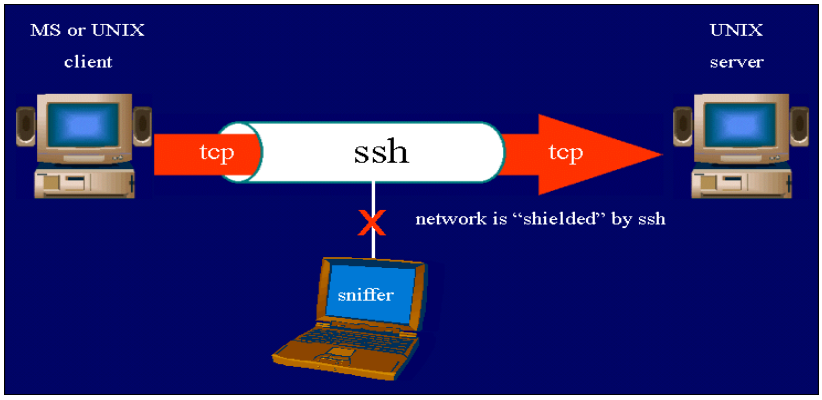
7.1.2 KRİPTO YÖNTEMİ:

Kripto yöntemi kişiler arası veya özel kurumlar arası mesajlaşmalardan tutunda sistemin oluşumunda ve işleyişinde uygulanan bir güvenlik yöntemidir.

7.1.3 RLOGİN (REMOTE LOGİN) :

Remote login . Uzaktan erişim veya uzaktan oturum açma anlamına gelir. Telnet gibi uzaktaki bir sunucuya başka bir makineden bağlantıyı sağlayan bir protokoldür.

Sonuç olarak şunu diyoruz ki SSH temel bağlantı yollarından (telnet ,rlogin….) daha iyidir .



Şekil 8

IMAP Serverlar

IMAP (Internet Message Access Protocol) ve POP3 (Post Office Protocol-Version 3), Microsoft Outlook Express, Netscape Messenger ve Mozilla Thunderbird gibi e-posta tarayıcıları kullandığınız zaman e-postalarınıza kolaylıkla ulaşabilmenizi sağlayan ve aralarında bazı farklılıklar bulunan e-posta okuma servisleridir. IMAP4 istemcilerin çeşitli kıstaslara göre sunucu üzerinde mesaj araması yaptırmasına ve sadece bu mesajların görüntülenmesine izin verir. POP3 ise mesajları bütün olarak çeker, arama istemci tarafında yapılır.

7.2 POP3 özellikleri:

E-postalar sabit diske kopyalanır.

Sabit diske e-postalarınızı indirirken eğer tercih ettiyseniz e-postalar sunucudan silinebilir.

E-postalarınızın sunucuda kalmasını isteyebilirsiniz, ancak sabit diskinizden silinen dosyaların sunucu üstünden de silinmesi için gerekli ayarları yapmanız gerekir.

Sunucu üstünde e-postaları ayırmak için farklı dizinler yarattıysanız bu dizinler sabit diskte olmadıkları için gözükmezler.

7.3 IMAP özellikleri:

E-postalar sunucu üstünde tutulur. Sunucu üzerinde sizin oluşturduğunuz ya da sistemin yarattığı dizinlere ulaşabilirsiniz. En temel POP3 uygulamasında sunucu her bir e-mail hesabına bir text dosyası düşecek şekilde kontrol eder. Bir mesaj geldiğinde POP3 sunucusu bu dosyayı alıcı dosyasının altına ilave eder.

Eposta adresi kontrol edildiğinde e-mail client yazılımı POP3 sunucusuna 110 numaralı port ile bağlanır. POP3 sunucusu kullanıcı adı ve parolaya ihtiyaç duyar. Bir kez giriş yapıldıktan sonra POP3 sunucusu text dosyasını açar ve erişimi mümkün kılar.

7.4 FTP Nedir?

FTP (FILE TRANSFER PROTOCOL) internete bağlı bir bilgisayardan diğerine (her iki yönde de) dosya aktarımı yapmak için geliştirilen bir internet protokolü ve bu işi yapan uygulama programlarına verilen genel addır. FTP ilk geliştirilen internet protokollerinden biridir. FTP protokolü ile

1) Bir başka bilgisayardan bir başka bilgisayara dosya aktarımı yapılırken, o bilgisayar ile etkileşimi aynı anda bağlantı kurulur.

2) Protokol ile sağlanan bir dizi komutlar yardımıyla iki bilgisayar arasında dosya alma/gönderme işlemleri yapılır.

7.4.1 FTP Yapmak İçin Nelere İhtiyaç Var?

- Bağlanacağımız bilgisayarın internet adresi,
- Bağlanacağımız bilgisayarda bilgilere ulaşmak için hesap adı ve şifresi,
- İnternet erişimi olan,üzerinde FTP yazılım programı bulunan bilgisayar
- Bağlanacağımız bilgisayarda, FTP protokol komutlarını yorumlayacak çalışır durumda bir FTP servis programı yani FTP sitesi gereklidir.

7.4.2 Anonymous FTP Nedir?

FTP işlemleri sırasında güvenlik açısından bağlanacağımız makinede kullanıcı numarasını (user name) ve password (parola) bilgilerini bilmemiz gerekir. (Program bunları bize sorar. Bağlanılan makine, kişiye özel ve parolasını sadece bizim bildiğimiz bir makine olabileceği gibi, herkese açık bir arşivde olabilir. Böylece herkesin kolayca erişip dosya almasını sağlayan tek tip bir kullanıcı numarası tanımlanmıştır. O da; ANONYMOUS ya da FTP. Bu merkezlere FTP yapıldığında kullanıcı ismi olarak anonymous (ya da FTP) girildiğinde bizden parola olarak kendi: E POSTA ADRESİMİZİ girmemiz istenir. (Parola yazılırken görülmez) Şifre olarak kesinlikle kendi bilgisayarımızın şifresini girmeyiniz.

7.4.3 SNMP nedir?

SNMP, ağ cihazlarında yönetimsel bilgi alışverişinin sağlanması için oluşturulmuş bir uygulama katmanı protokolüdür. TCP/IP protokolünün bir parçası olan SNMP; ağ yöneticilerinin ağ performansını arttırması, ağ problemlerini bulup çözmesi ve ağlardaki genişleme için planlama yapabilmesine olanak sağlar. Günümüzde kullanımda olan 3 tane SNMP sürümü mevcuttur.

İstemci ile sunucu arasındaki iletişim protokolüdür. RFC 1157 ‘de tanımlanmıştır. İletişimde UDP paketleri ve ön tanımlı olarak 161. port kullanılır. Sunucuların, güvenlik duvarlarının ve yönlendiricilerin (router) işlemsel istatistiklerini tuttukları OID (Object Identifier) ‘ler SNMP standardında belirtilen bilgi ağacında (SMI) belirtildiği şekilde düzenlenmiştir. Bilgi ağacı bir kök düğümünden başlayıp dallara, yapraklara doğru ilerler. Ağaçtaki adres yolu oluşturulurken her düğümden sonra bir nokta yazılır. Örneğin; *enterprises* için adres yolu *1.3.6.1.4.1* ‘dir. MIB ‘ler her bir OID dalının metin halinde ifade edilmesidir. Aşağıdaki şekilde bir OID yapısı görülmektedir:

SNMP sürüm 1: SNMP ‘nin ilk protokolüdür. Sistem kaynaklarını fazla kullanmadan aygıt istatistikleri ve hata raporlama amaçlıdır. Veri iletişimi şifreli değildir. Okuma/yazma için sadece SNMP istemcisinin IP adresine erişim izni verilmiştir.

SNMP sürüm 2: Bu sürüm 1. sürümle uyumlu olup 1. sürüme çok daha detaylı hata raporlama ve aygıt bilgisi elde etme özelliği eklemiştir.

SNMP sürüm 3: Önceki sürümlerin güvenliği artırılıp uzaktan yönetilebilme özellikleri eklenmiştir. Sadece bir IP adresine değil birden fazla IP kümesine ve SNMP kullanıcılarına okuma/yazma izni verilebilir. Veri iletişimi şifreli olup bu iletişim esnasında oluşan hataları sezme özelliği geliştirilmiştir.

SNMP sürümleri arasındaki farkları bilmeniz SNMP sorguları yaparken lazım olacağından tavsiye edilir.

7.4.4 SNMP’yi Oluşturan Bileşenler

- Ajan uygulama: SNMP hizmetini cihaz üzerinde çalıştırıp gerekli bilgileri kayıtlı tutarak yönetici birime aktaran veya yönetici birimden gelen değişikliği cihaza uygulayan uygulamaya verilen isim.
- Yönetici uygulama: Ajan uygulamadan ihtiyaç duyulan bilgileri alıp kullanıcıya gösteren ve kullanıcının değiştirmek istediği değerleri cihaza gönderen uygulama.
- Ağ Yönetim Sistemi (NMS): Yönetici birimde çalışan ve bir ağa bağlı tüm cihazların izlenmesini ve yönetimini sağlayan uygulamaya verilen isimdir.[7]

7.5 KAYNAKLAR

[1]http://tr.wikipedia.org/wiki/Uygulama_katman%C4%B1

[2] http://tr.wikipedia.org/wiki/HTTP

[3] Bilgisayar Ağları Kitabı -James F. Kuroso

[4] http://www.bydigi.net/bilgisyar-donanim-destegi/40512-http-nedir.html

[5]http://webdeyim.net/tr/e_dergi/ubuntu-turkiye/sudo/12/16

[6] http://www.bilginipaylas.com/cisco-genel-makaleleri/network-time -protocol-ntp-ve- cisco-routerlar-üzerinde-zaman-bazli-acil-uygulamasi-2.html

[7]http://pcwin.com/media/images/screen/66071-nfs_windows_client_to

8 BÖLÜM

8.1 UYDU NEDİR?

Her hangi bir bölgeden gönderilen sinyalleri, üzerinde bulunan elektronik devrelerden geçirerek, almış olduğu sinyali istenilen bölgelere değişik frekans bantları aralığında gönderen ileri teknoloji ile hazırlanmış cihazlardır.

Herhangi bir gezegenin çevresindeki bir yörüngeye yeryüzünden fırlatılarak yerleştirilmiş uydulara da yapma uydu denir. Günümüzde çok çeşitli amaçlarla uzaya gönderilen uydular vardır. Uyduların temel görevi yeryüzündeki iletişimi ve haberleşme sistemlerini geliştirmektir.

Bir gezegenin çekiminde bulunarak onun çevresinde dolanan gökcismi; çeşitli amaçlarla Yer'den fırlatılan ve genellikle kapalı bir yörünge çizerek Yer'in ya da başka bir gezegenin veya doğal bir uydunun çevresinde dolanan aygıt (yapay uydu).[1]

8.1.1 Uyduların Yörüngesi

Uydu yörüngeleri genel olarak dünyaya olan uzaklıklarına, kullanım amaçlarına ve yörünge düzlemlerine göre sism alırlar.

8.1.2 Uyduların Enerji Kaynakları

Uyduların enerji kaynakları güneştir. Enerji depolama işini de yine üzerinde bulunan solar bataryalarla gerçekleştirir.

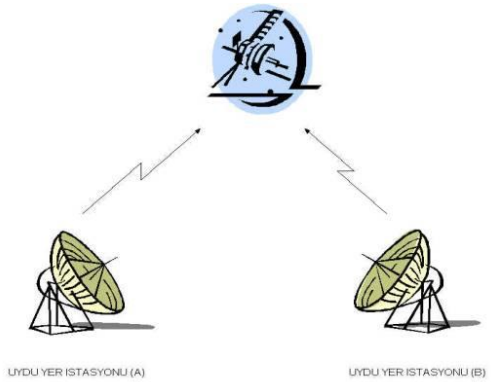
8.1.3 Uzayda Uydunun Dengesi

Yörüngede bulunan uydular yeryüzünün çekim kuvveti ile merkezkaç kuvvetinin eşit olduğu bir ortamda sabit olarak durmaktadırlar.

8.1.4 Uydunun Ömrü

Yaklaşık olarak bir uydunun ömrü 12- 15 yıl arasında değişmektedir. Başka bir anlatımla uyduyu dengede tutmaya yarayan roketlerin yakıtı bittiğinde uydu da ömrünü tamamlamış olur.

8.2 UYDU İLETİŞİM SİSTEMLERİ



8.2.1 TV Yayını Ve Uydu Frekansları

Uydular dünyaya değişik bantlar üzerinden sinyal gönderirler.uydulardan alınan TV yayınları frekans bantları ile tanımlanır.

8.2.2 X Bandı Yayını :

Frekansları 3 GHz'in altında olan ve genellikle haberleşme amaçlı kullanılan yayın türüdür.

8.2.3 C Band Yayınları :

3,5 GHz frekansında kullanılan yayın türüdür. Alıcı antenleri elek şeklindedir.

8.2.4 KU Bandı Yayını :

10.95 ve 11.70 GHz frekans bantlarını kapsar. Ve TV yayınlarının büyük bölümü bu banddan yapılır.

8.3 UYDU ÇEŞİTLERİ

Uydular iki şekilde sınıflandırılır. Bunlar:

8.3.1 Yeryüzüne olan Yüksekliklerine Göre Sınıflandırılması

8.3.1.1 Alçak Yörünge Uyduları(Low Earth Orbit- LEO):

Yeryüzünden 200- 3000 km yükseklikte konumlanmışlardır.Ömürleri kısadır.

8.3.1.2 Orta Yörünge Uyduları (Medium Earth Orbit- MEO):

5000-13000 km yükseklikte konumlanmışlardır. Gps hizmetleri gibi yer konum belirlemede kullanılırlar.

8.3.1.3 Yerdurağan Yörünge Uyduları (Geostationary Earth Orbit-GEO):

Yeryüzüne yaklaşık 36000 km yükseklikte bulunurlar. Ekvator düzleminde olan uydulardır.

Dönme periyodları dünya ile eştir, dünyadan bakıldığında sabit görünürler. 3 GEO ile tüm dünyayı kapsayabiliriz.

8.3.1.4 **Yüksek Yörüngeli Uydular(High Eliptical Orbit- HEO):**

Diğer Uyduların erişemediği kutup bölgelerinde etkilidir. Daha çok bilimsel çalışmalar için kullanılırlar.

8.3.2 Kullanım Amaçlarına Göre Sınıflandırılması [2]

8.3.2.1 Askeri Amaçlı Uydular

- Casus Uydular
- Fotoğraf Uyduları
- Elektronik Uydular
- Okyonus Gözlem Uyduları
- Erken Uyarı Uyduları

8.3.2.2 Haberleşme Uyduları

Genellikle yeryüzünden 36-40 bin km uzaklıkta bulunurlar.iletişimleri günde 24saat kesintisiz sürmektedir.

8.3.2.3 Yön Bulma Uyduları

Konumlandırma uyduları hem dost hem düşman kuvvetlerinin yerlerinin saptanmasında kullanılmaktadır. ABD yalnızca 5 m sapma yapan Navstar konumlandırma sistemini geliştirmiştir.

8.3.2.4 Meteoroloji Uyduları

Bir füzenin rotasındaki hava durumunu bildirmekte ve füzenin doğru olarak yönlendirilmesini sağlamaktadır.

8.4 UYDULARIN YAPISI, YÖRÜNGESİ VE ENERJİSİ

8.4.1 Uydu Haberleşme Sistemleri

Bu sistem uydunun uzaydaki durumu denetleyen bir yer istasyonundan, uydu üzerindeki transponder(alma frekansını gönderme frekansına çevirici) ve iltişim trafiğinin gönderilmesini ve alınmasını sağlayan yer terminal ağından oluşur.

8.4.1.1 Yer İstasyonları

Bu yapı anten modülü, anten modülüne bağlı uydudan sinyallerialgılayan arama modülü ve alma-gönderme modüllerinden oluşur.

8.4.2 Uyduların Yapısı:

- Dış Katman
- Haberleşme Sistemleri
- Bilgisayar Ve Veri ToplamaSistemleri
- Güç Kaynakları
- Pozisyon Belirleme Ve Sabitleme Üniteleri

8.4.3 Uyduyu Oluşturan Bileşenler

8.4.3.1 Transponder

Tekrarlayıcı mantığı ile çalışır. Temel olarak antene gelen sinyali filtreleyip yükselttikten sonra ulaşması gereken yer terminaline istenilen frekansta iletir. [3]

8.4.3.2 Antenler

Temel görevleri şunlardır.

- Kurulduğu bölgede istenilen frekansdaki radyo frekans dalgalarını toplamak.
- Mümkün olduğunca az istenmeyen sinyal toplamak
- İstenen frekansdaki radyo dalgalarını iletmek
- Anten hüzmesi dışındaki alanlara minumum güç yaymak.

Uydunun Akü Ve Güneş Pilleri: Güneş panolarının verimi çevresel sebeplerden dolayı değişir. Bu sebepler; mor ötesi radyasyon, parçacık radyasyonu, mikro meteorlar ve tutulmalar. Bu durumlarda uydunun ömrünün devamlılığı için akü bulunur. Genellikle Ni-Cd tür akü kullanılır.

Ayrıca uydularda günümüzde kullanılan solar enerji yakın zamanda yerini nükleer enerji sistemine bırakacaktır. Bu durumda uyduda bulunan donanımın iyi korunması gerekmektedir.

8.5 UYDULARIN YÖRÜNGELERİ

8.5.1 Kutup Yörüngeli Uydular:

Bu uydular yer kürenin boylam çizgilerine paralel olarak uzanırlar.Kutup bölgeleri, erozyonlar, maden ve petrol yataklarının tespiti ve askeri bölgelerdeki hareketlilik gibi bilgi toplama işlemleri bu tip uydular ile yapılır.

8.5.2 Ekvatoral Uydular

Yerin ekvator düzlemine paralel ve o düzlem için içinde dolanan uydulardır. Haberleşme amacı ile atılan uydular, erken uyarı askeri uyduları ve meteoroloji uyduları bu tip uydulardır. Yaşam süreleri daha uzundur.

8.5.3 Eliptik Yörüngeli Uydular

Ekvator düzlemine yerleştirilmiş dairesel yörüngeli uydulardır. Bu eş zamanlı uydulardan yapılan doğrudan tv yayını ekvator düzlemindeki ülkeler için çok faydalıdır.

8.6 UYDU İLETİŞİM SİSTEMERİNDE ÇOKLAYICI YÖNTEMLER

Uydular üzerinden milyarlarca bilgi alışverişi gerçekleştirilmektedir. Bilgi akışı bu denli fazla olduğundan çoğullama yöntemlerine ihtiyaç duyulmaktadır. Bu yöntemler uydu ile yer istasyonları arasındaki bilgi alışverişinin nasıl gerçekleştirileceği ile ilgilidir. Frekans, zaman ve kod paylaşmalı çoklayıcı geçiş olmak üzere 3 çeşit yöntemi vardır.

8.6.1 Frekans paylaşmalı çoklayıcı geçiş

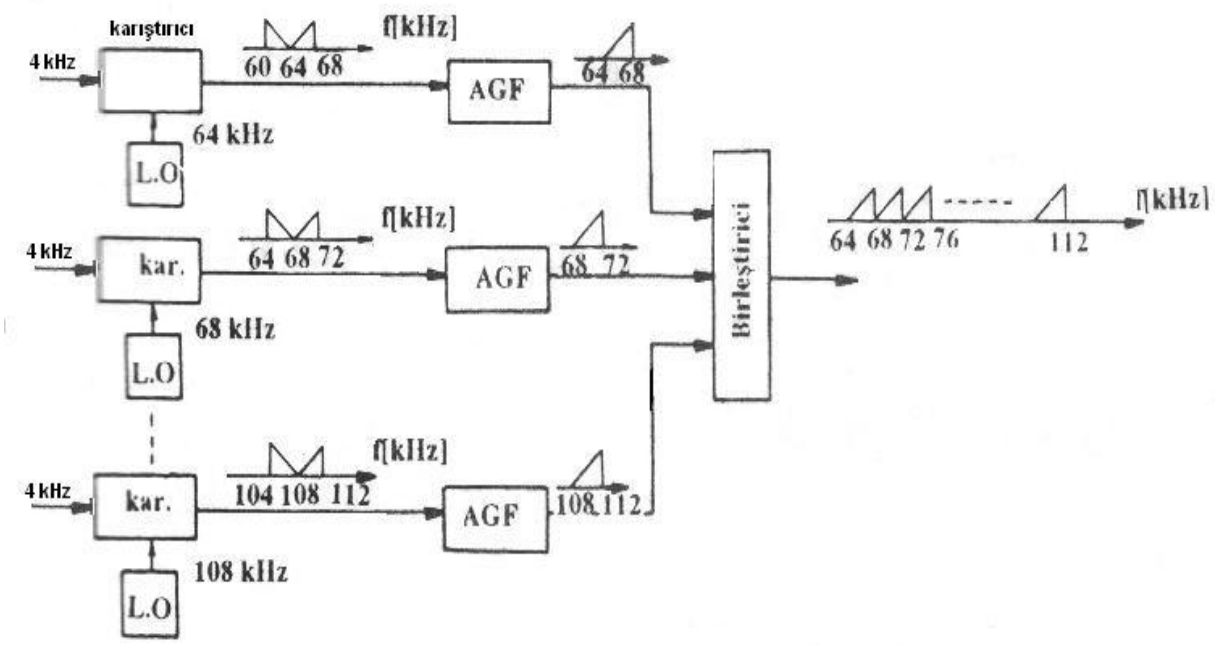
İki veya daha çok giriş işaretini tek bir birleşik işaret haline getirerek, bu işareti bir taşıyıcı işareti ile nakletmek tekniğine çoğullama denir Çoğullama zaman veya frekans domeninde olabilir. Çoğullanmış işaret bir taşıyıcı ile modüle edilip nakledilebilir. Alıcıda, demodülasyon işlemi sonucu çoğullanmış işaret daha sonra bu işaretten de haber işaretleri elde edilir. Haberleşme sistemlerinde çoğullama tekniği iki önemli avantaj sağlamaktadır.

1. Tek bir taşıyıcı işareti ile tek bir hat üzerinden binlerce telefon konuşması nakledilebilir.

2. Diğeri hattın band genişliği etkin olarak kullanılabilinir. Örneğin 12 telefon konuşması işaretleri çoğullanarak tek bir işaret elde edilebilir. Her işaretinin band genişliği 3 [kHz] olarak alınabilir.

Çoğullayıcıda, her giriş işareti farklı frekansta taşıyıcıların genlikleri modüle edilmektedir. Modülasyon işlemi dengeli modülatörlerde gerçekleştirilmektedir. Dengeli modülatörün çıkışında taşıyıcısı bastırılmış çift yan bandla genlik modülasyonlu işaret elde edilmektedir.

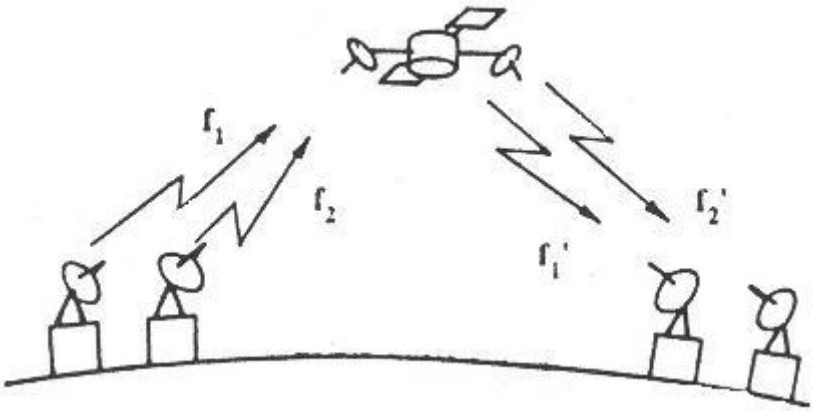
Her modüle edilmiş işaret filtreden geçmektedir. Böylece üst yan bantlar kırpılmaktadır. Elde edilen işaretler tek yan band işaretleridir. Bundan sonra tüm 12 tek yan band işareti toplanmaktadır.



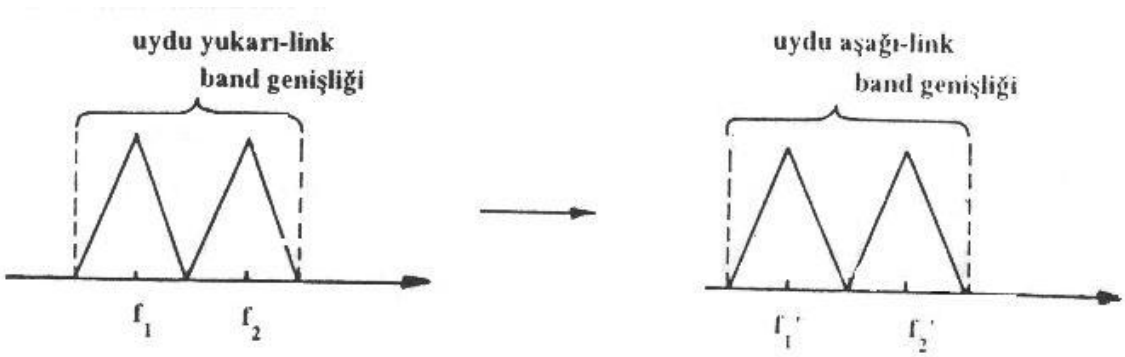
Şekil 1: Telefon İşaretlerinin Çoğullanmış ve Frekanslarının Birleştirilmiş Çıkışı

Şekil 1'de, karıştırıcının çıkışında telefon taşıyıcısı bastırılmış çift yan band işareti elde edilmektedir. Bu çoklayıcı sistemde her ses işareti 4 [kHz] lik band genişliğine sahiptir. Çoklanmış çıkış işaretinin toplam band genişliği 48 [kHz] oluyor (60 [kHz]-108 [kHz]). Bu çoklama tekniğine frekans paylaşmada çoklayıcı giriş işaretleri farklı frekansları paylaşmaktadır. Çoklanmış çıkış işareti 12 tane birbirinden bağımsız teflon işaretinden oluşmaktadır. Bu işaretler tek bir taşıyıcı işareti ile tek bir hat üzerinden nakledilebilir.

- Çoğullanabilecek işaret sayısı,
- Çoğullanacak işaretlerin band genişliğinden,
- Taşıyıcı işaretin band genişliğinden ve
- Kullanılan modülasyon türünden belirlenebilir.



Şekil 2: Uydu İletişim Sistemi



Şekil 3: FPÇG Uydu Sisteminde Yukarı ve Aşağı Link Frekans Spektrumları

FPÇG'de Band Seçimi…

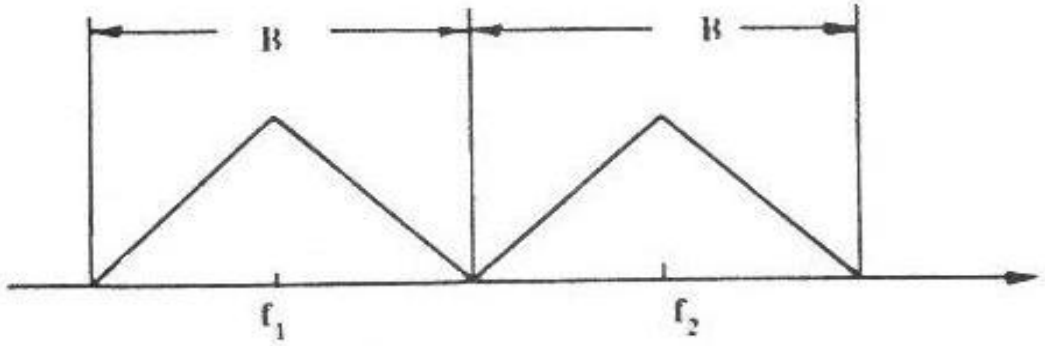
FPÇG en basit çoklayıcı yöntemidir. Her yukarı-link taşıyıcısı ayrı yer istasyonundan kaynaklanmakta veya birkaç taşıyıcı belirli bir istasyondan da gönderilebilmektedir. İki tür band seçimi vardır:

1. Her taşıyıcıya, yukarı-linkte belirli bir frekans bandı ayrılır ve bu ayrılmış frekans bandı yukarı-linkteki diğer taşıyıcılar tarafından kullanılamaz.

2. Aynı frekans band' ları birkaç taşıyıcı tarafından paylaşılabilir. Bu çeşitte taşıyıcı sayısı artırılmakta ve yer istasyon iletişim donanımı genişlemektedir.

Not:

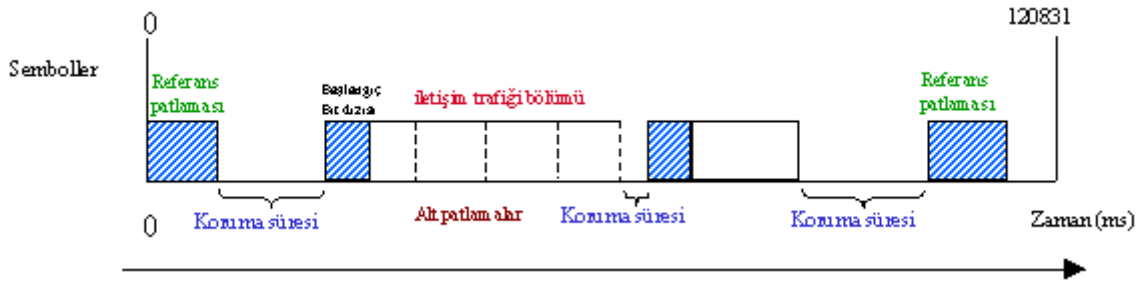
FPÇG'i kullanan sistemlerde, taşıyıcı merkez frekansları arasında belirli minimum mesafenin korunması gerekmektedir. Aksi takdirde n kanallar arasında girişim meydana gelmektedir.



Şekil 4: FPÇG Sisteminde Frekans Spektrumu

8.6.2 Zaman paylaşmalı çoklayıcı geçiş

Kısaca TDMA olarak tanımlanan zaman paylaşımlı çoklu erişim modunda, her kullanıcı, uydu transponderine aynı taşıyıcı frekansını kullanarak, belli bir referans zamanına göre belli zaman bölmelerinde erişir. TDMA çerçevesi adı verilen bir zaman aralığı belirlenmiştir, bu süre içinde, ağdaki tüm kullanıcılar, kendilerine ayrılan zaman bölmeleri içinde bilgi paketlerini iletirler. Bu zaman çerçevesinin uzunluğu 2 ms, ya da 120832 semboldür. Her ağ kullanıcısına tahsis edilen zaman bölmeleri, çerçevede (frame) ne kadar iletişim trafiği iletileceğine ya da alınacağına bağlı olarak değişir. Tipik bir uydu TDMA çalışma sistemi, Şekil-5'te gösterilmiştir.



Şekil 5: TDMA Zaman Planlaması

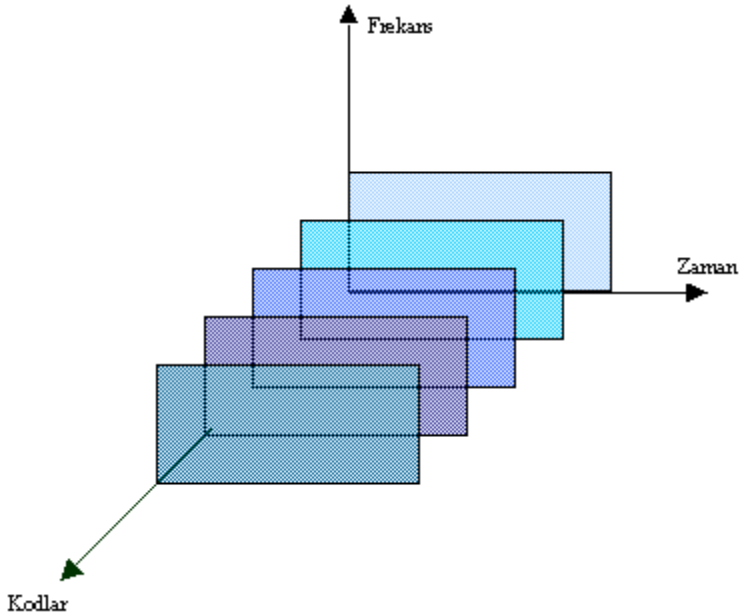
İki ya da daha fazla FDM/FM sinyal aynı anda doğrusal olmayan bir yükselteç tarafından yükseltilirse, bir FDM/FM taşıyıcının temelbandına başka taşıyıcılardan karışma olur. Bu meydana geldiğinde, doğrusal olmayan yükseltecin genlik modülasyonu/faz

modülasyonu özellikleri, taşıyıcıda genlik modülasyonu oluşturur, bu da diğer taşıyıcılarda faz modülasyonu meydana getirir (AM/PM conversion). TDMA sayesinde diğer taşıyıcılarda oluşturulacak faz modülasyonu sorunu çözülmektedir, dolayısıyla uydu güç yükselteci, doyum modunda çalıştırılabilmektedir.

8.6.3 Kod paylaşımlı çoklu geçiş

Kısaca CDMA olarak adlandırılan Kod Paylaşımlı Çoklu Erişim teknolojisi II. Dünya Savaşı sırasında müttefik kuvvetlerinin, haberleşmeleri sırasında düşman karıştırıcı sinyallerinden etkilenmemesi amacıyla geliştirilmiştir. Günümüzde ise askeri uygulamaların yanı sıra sivil uygulamalarda da sıklıkla kullanılan bir çoklu erişim yöntemidir. Bu metot sayesinde tüm kullanıcılar aynı frekans bandını kullanabilirler. Her kullanıcıya ait bilgi yine o kullanıcı için rastgele yaratılmış bir kod dizisiyle çarpılarak tüm band boyunca yayılır.

Kullanılan kod dizileri birbirlerinden bağımsız olduğu için alıcı tarafında hangi kullanıcıya ait bilgi alınmak isteniyorsa, alınan sinyaller o kullanıcının kodu ile tekrar çarpılarak istenilen bilgiye ulaşılır. CDMA tekniği yukarıda açıkladığımız yöntem sayesinde, kullanıcıların aynı frekans bandını istedikleri zamanda kullanabilmesine olanak vermektedir, literatürde CDMA, SSMA olarak da adlandırılmaktadır. Şekil-6'da CDMA modunun basit çalışma sistemi gösterilmektedir.



Şekil 6: CDMA Kodlama Tekniği

8.7 TÜRKSAT 3A UYDUSU

8.7.1 Teknik özellikler

- **Üretici Firma:** Thales Alenia Space Industries (Alcatel)
- **Platform:** SpaceBus 4000B2
- **Stabilizasyon Tipi:** 3 Eksen Kontrol
- **Fırlatma Tarihi:** 13 Haziran 2008
- **Uydu Tasarım Ömrü:** 15 Yıl
- **Uydu Manevra Ömrü:** 20 Yıl
- **Boyut:** 2.8 m x 2.3 m x 1.8 m
- **Kanat Açıklığı:** 30 m.
- **Yörünge Lokasyonu:** 42 º Doğu Boylamı (Türksat 2A ile aynı lokasyonda

8.7.2 Türksat A.Ş

22.07.2004 tarihinde Türksat kuruldu.

01.07.2005'de Kablo TV Türksat'a devredildi.

11 Ağustos 1994'de uzaydaki yerini alan Türksat 1B,

10 Temmuz 1996'da uzaya gönderilen Türksat 1C,

1 Şubat 2001'de hizmete başlayan Türksat 2A ,

13 Haziran 2008'de uzaydaki yerini alan Türksat 3A,

Türksat'ın uydu filosunu oluşturmaktadır.

8.7.2.1 HİZMET ALANLARI:

Türksat Uydularının Kontrolü ve İşletmesi

8.7.2.2 UYDU ÜZERİNDEN VERİLEN HİZMETLER:

Kırsal ve Uluslararası Telefon Haberleşmesi

VSAT (Very Small Aperture Terminal)

Radyo-TV Yayın

Uzaktan Algılama

Kablo TV Hizmetleri

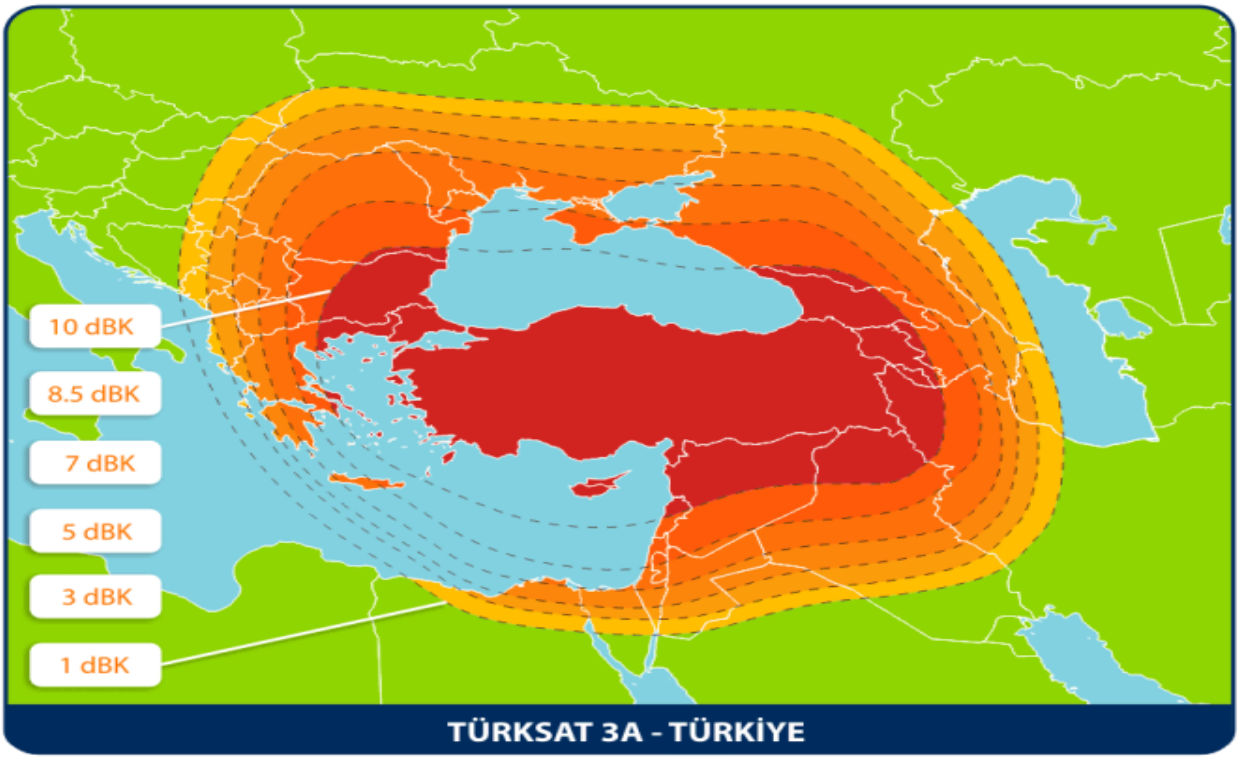
E-Devlet Kapısı

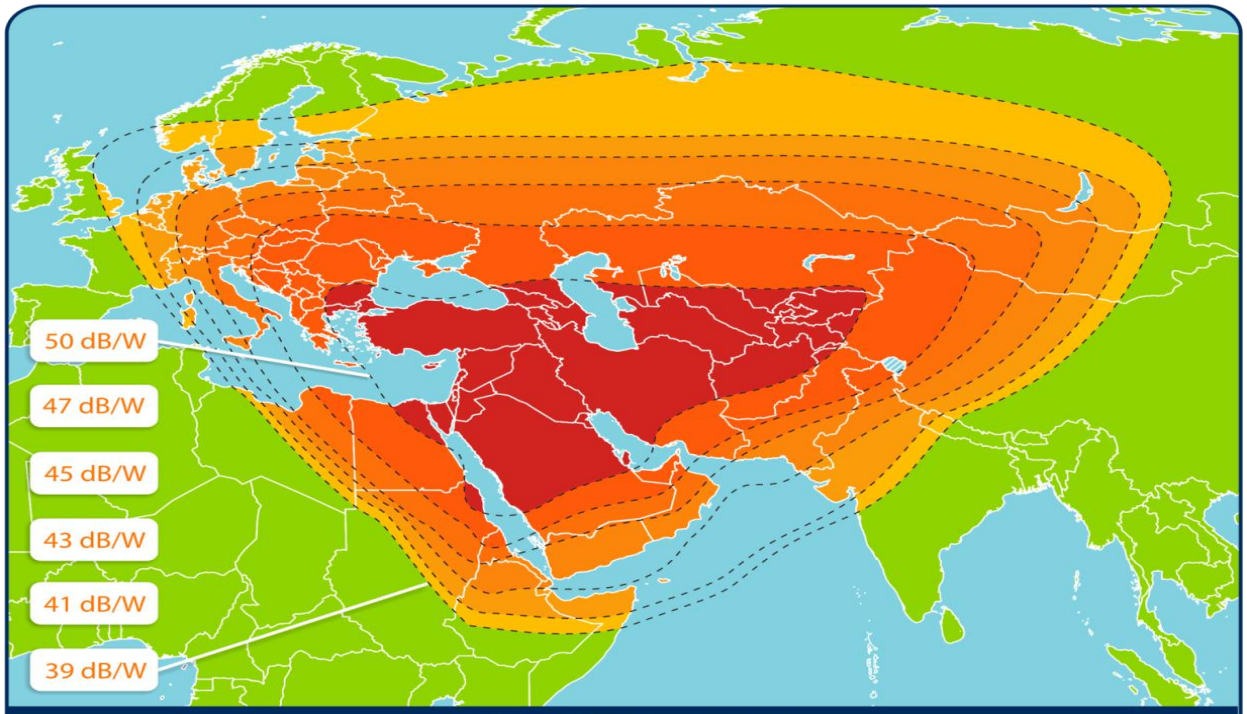
8.7.2.3 Türksat 3A uydusunun özellikleri ve Türksat uydu filosuna getirdiği yenilikler

- Türkiye'nin sahip olduğu uydular arasında en gelişmiş özelliklere sahip olandır. Türkiye'nin beşinci haberleşme uydusudur.
- Türkiye ile birlikte Avrupa, Ortadoğu, Kuzey Afrika, Orta Asya ve Çin'e kadar uzanan geniş bir kapsama alanında, televizyon yayıncılığı ile birlikte internet, ses ve data aktarımları için kullanılır.
- Türksat 3A uydusu üzerinden VSAT uygulamalarında kurumsal müşteriler 50-60 cm gibi küçük çaplı antenlerle yayın alabilir ve 1 Wattlık HPA'larla uplink yapabilirler. Bu özelliği ile Türksat 3A uydusu VSAT kurulumlarında önemli oranda maliyet azalmasına imkân tanır.
- Türksat 3A, 1296 Mhz'lik pazarlanabilir kapasiteye sahiptir. Bu kapasite, Türksat 1C uydusunun yaklaşık iki katı kadar büyüklükte bir kapasiteye denk gelmektedir.
- Türksat 3A, Türksat 1C uydusunun mevcut trafiğinin tamamını karşılamaktadır.
- Türksat 3A'nın 42 derece doğu lokasyonunda devreye girmesiyle birlikte mevcut televizyon, radyo ve VSAT aktarımları çok yüksek hız ve kalitede gerçekleşmektedir.

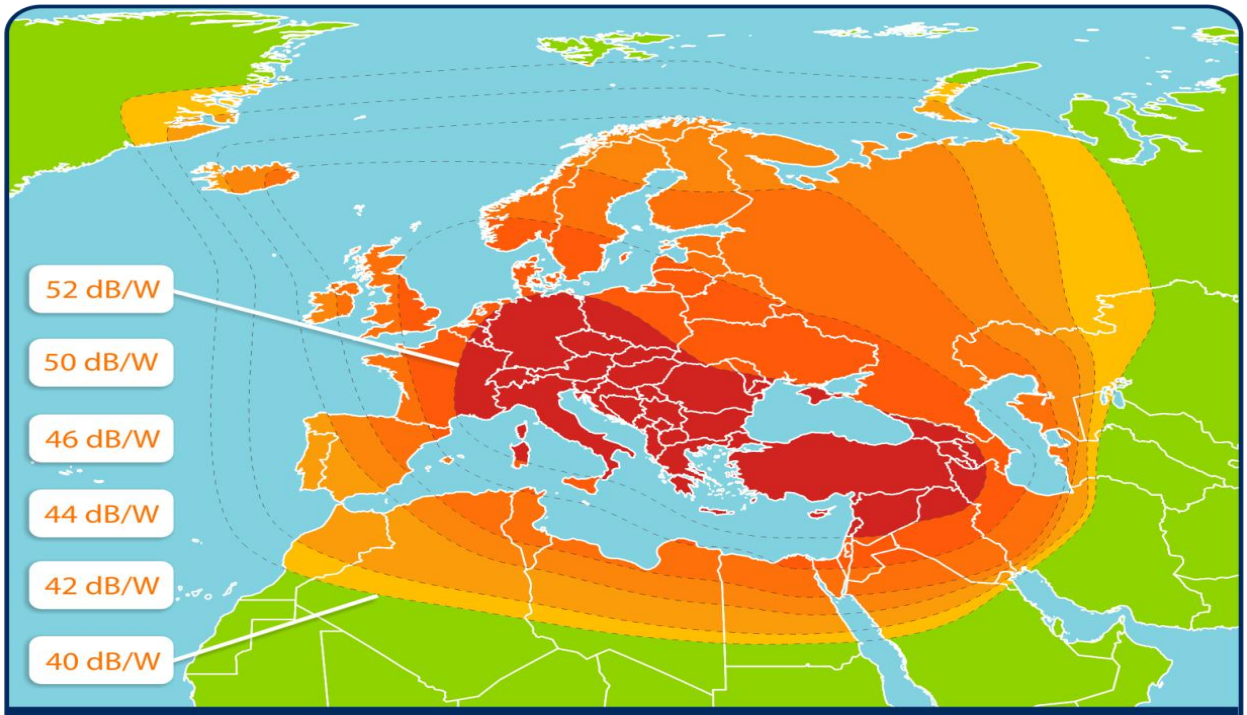
- Toplamda daha fazla bant genişliği,
- Türkiye alış kapsama alanı özelliği ile daha küçük antenlerden Türkiye'den çıkış olanağı,
- Daha geniş Batı ve Doğu kapsama alanları,
- Daha yüksek yükseltici gücü,
- Uyduya yetkisiz erişimin önlenmesine (authentication) ek olarak, gönderilen komutların içeriğinin şifrelenmesi (encryption) özelliği,
- Kapsama alanları arasında yüksek anahtarlanabilme olanağı,
- Beacon vericisi ile hareketli antenler için daha kolay izlenebilirlik, bu verici üzerinden telemetri gönderebilme özelliği,
- Sıfır momentuma sahip olması,
- Hafif ama yüksek kapasiteye sahip Li-Ion bataryalar,
- Yıldız İzler (Star Tracker) ile hassas yönelim denetimi bulunmaktadır.

8.7.3 TÜRKSAT 3A KAPSAMA ALANI





TÜRKSAT 3A - DOĞU



TÜRKSAT 3A - BATI

8.7.4 TÜRKSAT 4A

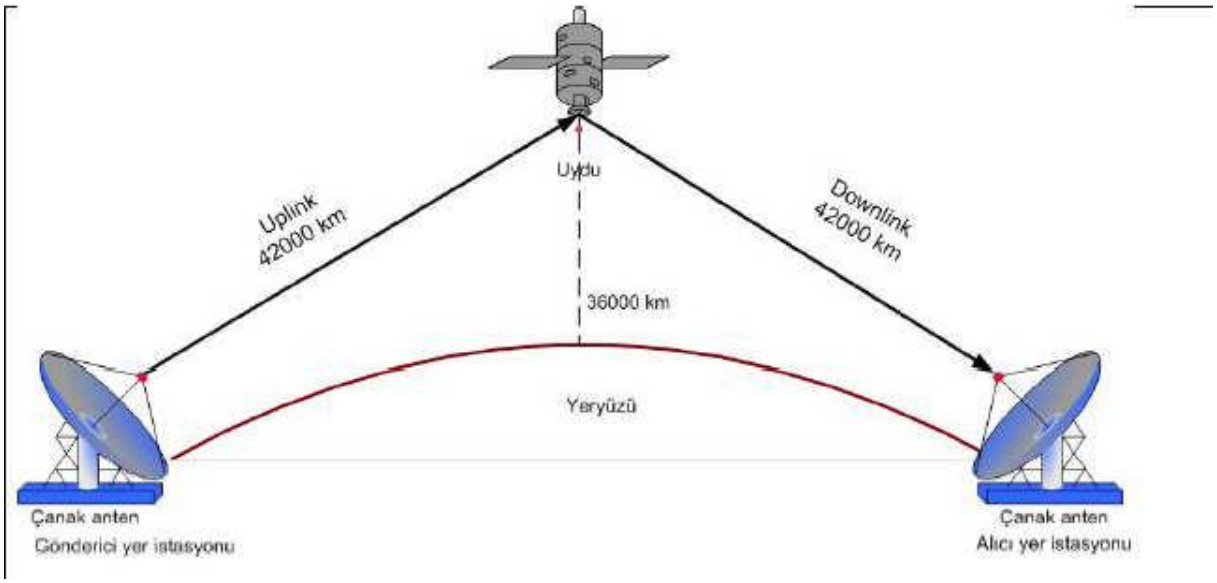
Mevcut doğu ve batı kapsama alanına ilave olarak kuzey ve orta Afrika'yı kapsayacak, böylece Türk uydularının kapsama alanı Amerika'nın doğu sahillerinden Çin'e ve güneyde Arap Yarımadası'nın ardından orta Afrika'ya kadar uzanacak. Türksat 4A'nın hizmete girmesi ile teknik olarak 42 derece doğu boylamından kapsayabileceğimiz maksimum alana ulaşmış olacağız [5].

8.7.5 MİLLİ UYDU TÜRKSAT 5A

Türkiye‘nin ilk milli uydusu TÜRKSAT 5A’nın yazılımı yüzde 100 yerli olacak [6].Uydunun üretimine TAI‘de kurulacak “uydu üretim ve entegre tesisi”nde 2012'de başlanacak [7]. 2014'te uzaya gönderilmesi planlanmaktadır.

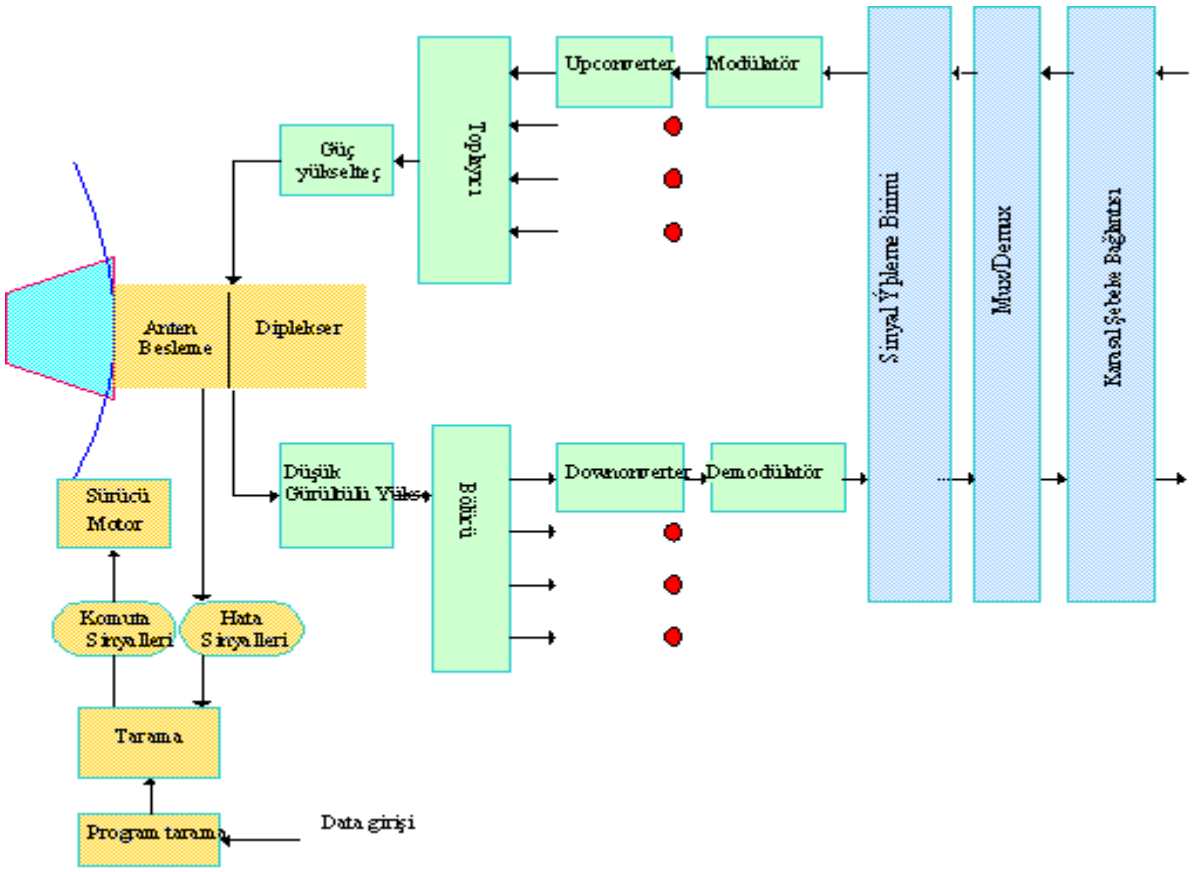
8.8 YER İSTASYONLARI

Abonelerden alınan bilgileri, uydu haberleşme sistemine uygun bir duruma getirerek uyduya göndermek ve uydudan gönderilen bilgileri alarak bunları yer istasyonlarını aboneye bağlayan sistemlere aktarmaktır. [1]



Şekil- 1: Yer İstasyonları

Yer istasyonlarının genel blok yapısı Şekil- 2 de gösterilmiştir. Yer istasyonları; anten modülü, anten modülüne bağlı uydudan gelen “ beacon ” sinyalini algılayan arama modülü, alma ve gönderme modüllerinden oluşur. Ayrıca karasal haberleşme şebekesiyle bağlantı sağlayan alt yapı ve sistem monitörleme modülleri de bulunmaktadır. Yer istasyonu sayesinde uydu haberleşme sistemindeki tüm parametreler (güç, uydunun yörüngesi , yer terminalleri parametreleri vb.) monitör edilebilir ve kontrol edilebilir. Böylece olağandışı durumlarda sistemdeki aksaklıklar monitör edilip gerekli önlemlerin alınması sağlanmış olur. [2]



Şekil- 2: Yer İstasyonlarının Genel Blok Yapısı

Yer istasyonları; alıcı yer istasyonları (Downlink) ve Verici Yer İstasyonları (Uplink) olmak üzere ikiye ayrılır.

8.8.1 Alıcı Yer İstasyonu (Downlink)

Uyduya gönderilen bir mikrodalga sinyalinin yer istasyonu tarafından alınması işlemine “ downlink” denir. Bir yer istasyonu alıcı sistemi anten, dönüştürücü ve demodülatör kartlarından oluşur.

Antenden gelen RF sinyali düşük gürültü kuvvetlendirici yada blok çeviriciden geçerek gürültü bileşenleri bastırılır. Dönüştürücü birimi RF sinyalini düşük frekanslı IF sinyaline dönüştürür. Demodülatör birimiyse bu sinyalden asıl bilgiyi (ses , data, görüntü) içeren Baseband sinyalini elde etmeyi sağlar. [1]

8.8.2 Verici Yer İstasyonu (Uplink)

Yer istasyonundan uyduya erişim işlemine temel olarak "uplink" denir. Bir yer istasyonunun verici sistemi anten, modülatör ve dönüştürücü elemanlarından oluşmaktadır.

Giriş kısmında giriş işaretleri birleştirilerek Baseband elde edilir. Modülatör kısmındaysa elde edilen Baseband frekans modülasyonu işlemine tabi tutulur.Modülasyon işleminden sonra dönüştürücü biriminde modülasyon işleminin frekansı Uplink frekansına kaydırılır. YGK birimi ise çıkışı uzaydaki kayıpları yenebilecek güce getirir. [1]

I NTELSAT sisteminde en yaygın olarak frekans modülasyonlu frekans paylaşımlı çoklayıcı kullanım yöntemi uygulanmaktadır. Bu yöntemde, sistemdeki yer istasyonlarının her birine 5,925- 6,425 GHz bandından bir veya birkaç taşıyıcı ayrılmaktadır. Bugün bir taşıyıcı ile en çok 1092 kanal, en az 12 kanal göndermek mümkündür. Ancak uydunun en verimli şekilde kullanılmasını sağlamak ve yer istasyonu sahibi ülkelerin ihtiyaçlarını karşılamak amacıyla, taşıyıcı frekansların yer istasyonlarına dağıtımı INTELSAT tarafından yapılmaktadır. Bu nedenle INTELSAT 132 kanallık trafiği olan bir yer istasyonuna bir taşıyıcı verebildiği gibi, uydudaki transponderlerin (RF kanalı devresi)durumuna göre aynı sayıda trafiği olan bir başka ülke yer istasyonuna biri 60 diğeri 72 kanallı olmak üzere iki taşıyıcı ayırabilmektedir. INTELSAT sisteminde kullanılan bu taşıyıcıların daha birçok özellikleri INTELSAT tarafından belirlenir. [4]

8.8.3 YER İSTASYONUNUN ANTEN SİSTEMİ

Uydu antenlerinin temel görevleri aşağıdaki gibi sıralanabilir:

- Kurulduğu bölgedeki istenen frekans ve polarizasyondaki radyo frekans dalgalarını toplamak.
- Mümkün olduğunca az istenmeyen sinyal toplamak.
- İstenen frekans ve polarizasyondaki radyo frekans dalgalarını iletmek.
- Anten hüzmesi dışındaki alanlara minimum güç yaymak

Uydu haberleşmesinde kullanılan antenler aşağıdaki şekilde sınıflara ayrılabilirler:

- Horn Antenler
- Phased Array Antenler
- Parabolik Antenler

Horn Antenler yüksek Kazanç/Gürültü (G/T) oranı sağlasalar da küçük boyutlardaki tipleri dahi çok pahalı olduğundan artık kullanılmamaktadır.

Phase Array Antenler özellikle hareketli uydu haberleşme sistemlerinde avantaj sağlamasına rağmen kullanılan teknolojinin zorluğu ve maliyetinin yüksek oluşu, bu anten tipinin kullanımını sınırlamaktadır.

Uydu haberleşme sistemlerinde en sık kullanılan anten tipi **Parabolik Reflektör Antenler**dir. Bu tip antenler 3 ayrı gruba ayrılırlar, bunlar sırasıyla:

- Simetrik veya Eksen-simetrik Antenler
- Offset Antenler
- Cassegrain Antenler [5]

Bir yer istasyonu anteni uydudan gönderilen çok düşük düzeydeki işaretleri alacak ve bu işaretleri gürültüden ayırabilecek nitelikte olmalıdır. Bugün INTELSAT (International Telecommunications Satellite) sisteminde çalışan bir yer istasyonunda aranılan en önemli özellik kazanç- gürültü sıcaklığı oranıdır [G/ T]. [1] [8]

Antenin kazanç, sıcaklık, polarizasyon gibi özellikleri yer istasyonunun uyduya veriş ve uydudan alış yapmasında kullanılan 500 MHz lik band genişliğinde sağlanması zorunludur. [1]

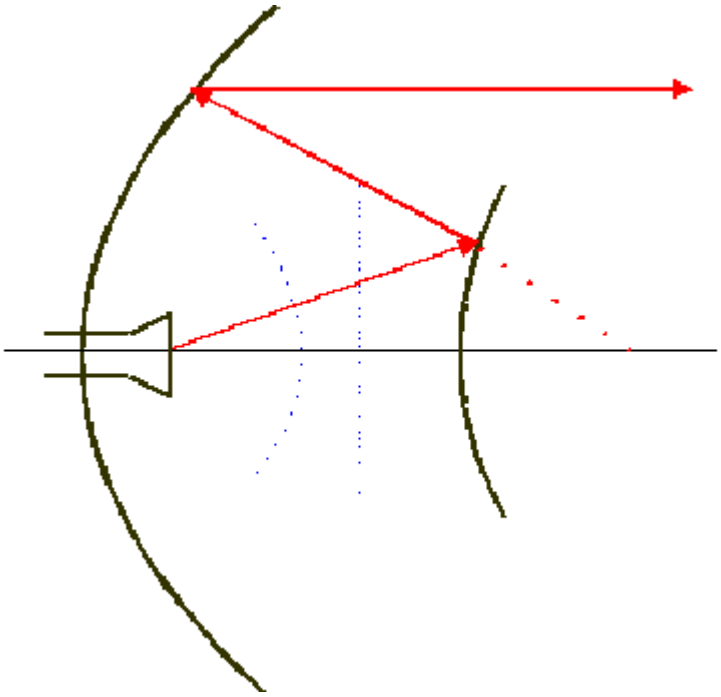
Uydu haberleşmesinde kullanılan antenlerin montajları:

- Yerel- Yükseklik Montajı
- X- Y Montajı
- Polar Montaj

Şeklinde olabilmektedir. [1]

Yukarıda saydığımız anten tiplerinden yaygın olarak kullanılan çift reflektörlü Cassegrain tipi anten yapısı gösterilmektedir. [7]

8.8.3.1 Cassegrain Anten



Bugün uydu yer istasyonlarında çok yaygın olarak kullanılan bu antenlerde uydudan gönderilen işaretler ana paraboloidal reflektör tarafından alınarak alt reflektör aracılığıyla ikisi elipsoidal ve ikisi düzlemsel dört yansıtıcıdan oluşan sisteme gönderilmektedir. Böylece antenden alınan ışın demeti çok küçük bir kayıpla aşağıda bulunan horna ulaşabilmektedir. [1]

Cassegrain Anten Sistemi Avantajları

- Yüksek kazanç
- Düşük gürültü
- Kullanılan alt reflektörün profilini biçimlendirmek suretiyle ışıma diyagramını kontrol edebilmek
- Beslemenin ve radyo frekans ön kuvvetlendiricinin yerleştirebilme imkanı
- Montajının kolaylığı

Bütün bu özelliklerden dolayı Cassegrain antenler yer istasyonlarında çok kullanılmaktadır. [1] [6]

8.9 KAYNAKLAR

[1] Bilgisayar Ağları Kitabı- Fırat Üniversitesi

[2] http://www.qsl.net/ta1kb/aselsan/uyduhabsistemi.htm

[3] http://www.cscrs.itu.edu.tr/page.tr.php?id=73

[4] http://www.elektrotekno.com/about1691.html

[5] http://www.forumtayfa.com/bilgisayar-ve-elektronik/101575-uydu-haberlesme-sistemi.html

[6] http://www.radartutorial.eu/06.antennas/an13.tr.html

[7] http://ddmcck.blogspot.com/2008/11/uydu-haberleme.html

[8] http://www.uludagsozluk.com/k/intelsat/

9 BÖLÜM

9.1 BİYOMETRİ NEDİR ?

Biyometrik tanıma, datayı kodlama veya şifreleme/deşifreleme için vücut özelliklerini kullanan bir süreçtir. Parmak izi, retina ve iris, avuç içi izi, yüz yapısı ve ses tanıma günümüzde sıkça araştırılan biyometrik tanıma teknikleridir. Bu özellikler her şahsa özel olduğu için biyometrik yöntemler hırsızlık ve dolandırıcılığa kısmen de internet üzerinden ticarete cevap olabilecektir. Bu yeni teknolojinin özelliği parola veya pin numarası yerine çalınamayan, kaybolmayan veya yeniden oluşturulamayan biyometrik özelliğin kullanılmasıdır. Bugünün biyometrik tanıma süreçleri geçmişteki bazı yaygın biyometrik tekniklerden türetilmiştir. Doğal olarak en yaygın olan ve suçluların tespitinde, çalışanların lisanslarında kullanılan parmak izidir. Bu süreç, yazılı kopya üzerinden manuel olarak haftalarca süren bir inceleme sonucunda bazen de yanlış sonuçlar vererek gerçeklenirdi. B Bilgisayar teknolojisinin gelişmesiyle, bazı kuruluşlar, arşivlerini elektronik olarak tutmaya ve parmak izi eşleştirme sürecini daha hızlı ve doğru olarak yapmaya başladılar. Parmak izi tanıma sürecinin sonraki adımı sadece kişileri tanımak değil aynı zamanda belirli yerlere erişimlerini denetlemektir. Bu teknik ile birlikte biyometrik tanıma
koddaki bilginin çözümlenmesiyle, kişilerin belirli yerlere girişlerini sağlayacak biyometrik parola olarak kullanılmaya başlamıştır.
Kişilerin kendilerine has fizyolojik özelliklerinden faydalanarak otomatik kimliklendirme yapan bu teknoloji, güvenliğin öneminin hızla arttığı günümüzde geniş kullanım alanı bulacak teknolojilerden biri olacaktır.
Biyometri, biyolojik özelliklerin istatistiki analiziyle uğraşan bilim dalıdır. Elektronik ortama; güvenlik adına parmak izi, ses, retina gibi karakteristikleri kullanarak kişi tanımlamak olarak geçmiş bir kavramdır. Artan güvenlik ihtiyacının şifrelerle karşılanamayacağı görüldüğü için biyometrik sistemlerin geliştirilmesi kaçınılmaz olmuştur .
Biyometri bireyleri birbirinden ayıran ölçeklenebilir psikolojik ve/ya da davranışsal karakteristiklerin kimlik tespitinde kullanılan bilgisayar kontrollü sistemler olarak tanımlanabilir.

9.2 BİYOMETRİK TANIMA NASIL ÇALIŞIR?

Biyometrik sistemler kişinin sadece kendisinin sahip olduğu ve kendisini diğer kişilerdenayıran fiziksel veya davranışsal özelliklerinin tanınması prensibi ile çalışmaktadır. Bu teknojide parmak izi ve el geometrisinin incelenmesi, yüz özelliklerinin karşılaştırılması, ses ve konuşma analizi, iris ve retina tanımlanması gibi süreçler yer almaktadır. Biyometrik teknolojilerin çalışma prensibi birbirine benzer. Öncelikle kayıtlar toplanır ve bu kayıtlar bir kod olarak ilgili sistemde saklanır. Talep edildiği vakit toplanmış olan bu kayıtlar ile ilgili kişi anında karşılaştırılır ve sonuca varılır. Biyometrik sistemler hızlı çalıştıkları için kısa sürede birçok karşılaştırma yapabilme özelliğine sahiptir.Yanılma olasılığını en aza indirme prensibi ile çalışan bu sistemlerin kart, şifre ya da pin numarası kullanan diğer tanıma metodlarına oranla daha çok tercih edilmesindeki en büyük faktörler, kullanıcının kendini tanıtmak için nüfus kâğıdı gibi tanıtıcıları taşımak mecburiyetinde olmaması ve şifre gibi bilgileri ezberlemek zorunda olmaması olarak sıralanabilir .

9.3 BİYOMETRİNİN UYGULAMA ALANLARI

Biyometrinin uygulandığı örnek uygulamalardan bazıları şunlardır:

- İnternet bankacılığında kullanıcı tanımlama
- ATM'lerde kullanıcı tanımlama
- Çağrı merkezlerinde kimlik tespiti
- Kurumsal ağların güvenliği
- Kredi kartı uygulamaları
- Masaüstü ve dizüstü bilgisayarların güvenliği
- Elektronik imza uygulamaları
- E-ticaret işlemleri
- Kiosklarda kullanıcı tanımlama
- Personel takibi
- SSK, vergi süreçleri gibi kamu hizmetleri
- Havaalanlarındaki giriş ve çıkış işlemleri
- Hastanelerde hasta takibi

9.4 BİYOMETRİK TEKNOLOJİLER

Bu gün birçok biyometrik tanıma uygulaması vardır. Aşağıda bunların türleri verilmiştir:

- Parmak izi tanıma
- İris-retina tanıma
- Ses tanıma
- İmza tanıma
- Yüz yapısı tanıma
- Yazma ritmi tanıma
- Toplardamar izi tanıma
- Avuç içi izi tanıma
- Kulak şeklinden tanıma

Parmak İzi Tanıma

Uygulaması en basit ve ucuz biyometri teknolojisi olduğu için hızla hayatımıza giren parmak izi tanımlama sistemleri, aslında yüzlerce yıldır insanların imzaları olarak kullandıkları parmak izlerini dijital teknoloji ile buluşturuyor. Dizüstü bilgisayar sistemlerinin çalınması veya izinsiz kullanılmasına ya da kullanıcıların sık sık bilgisayarlarındaki onca şifreyi unutmasına karşılık, IBM'in, daha bu sene içinde, kolay ve etkili bir güvenlik sistemi olarak kullanmaya başladığı parmak izi sistemleri, hızla yayılarak mini USB sabit disklere hatta farelere kadar her cihazın üzerinde görülmeye başlandı. Bağlı olduğu cihazı, tanımlı kullanıcılardan başkasının kullanmasına izin vermeyen parmak izi sistemlerinin yaygınlaşacağı ve bankamatik makinelerindeki işlemlerden, mağazalarda alışveriş yapmaya kadar pek çok alanda kullanılacağı tahmin ediliyor.

Elbette, parmak izini yanında taşıyan kullanıcıların da cüzdanlarını onlarca banka ve kredi kartı ile doldurmalarına ve şifre hatırlamaya çalışmasına gerek kalmayacak. Ülkemizde de kolayca bulunan teknolojinin örneklerini parmak izi kontrolü destekli mouse veya sadece parmak izi kontrolü yapan bir aparat (EyeD Hamster) gibi ürünlerde incelemek mümkün. Windows'u açmak, ekran koruyucuyu kapatmak, klasörleri gizlemek veya açmak gibi şifre girişi isteyen uygulamaları parmak izinin tespitine bağlayan farenin üzerindeki okuyucuya parmak bastırmak yeterli oluyor. Şifre hatırlamaya çalışmaktan, şifre çaldırma tehlikesinden, şifre yazma külfetinden kurtaran pratik ve güvenli bir teknolojidir .

9.4.1 İris ve Retina Tanıma

Göz bebeğinin ön kısmında yer alan iris tabakasını veya göz merceğinin ardında görme sinirlerinin toplandığı alan olan retinayı analiz ederek kullanıcının kimliğini tespit eden sistemlerdir. Bu teknoloji de hızla hayatımıza girme potansiyeline sahip. Şu anda Panasonic gibi firmaların, biraz geliştirilmiş bir web kamerası yardımı ile bilgisayar kullanıcılarının iris tabakalarını analiz ederek, klavyenin başına kimin oturduğunu belirleyecek ticari ürünleri mevcuttur. Teknolojinin bir sonraki aşamasında, banka otomatları gibi sistemlerde, Panasonic'in iris tanıma ürününde olduğu gibi kullanıcının eğilip büzülmesine gerek bırakmadan, kişinin yüzünü bulup, gözüne odaklanıp, iris tabakasını analiz eden robot kameralar kullanılması ve insanların, parmak izlerini bile basmaya gerek kalmadan, hesaplarına ulaşabilmeleri, mağazalarda ödemelerini yapabilmeleri gibi senaryolar üzerine çalışılıyor.

9.4.2 Ses Tanıma

Ses tanıma sistemleri oldukça yaygın kullanılan maliyeti düşük ve günümüz teknolojisinde fazladan hiçbir donanım gerektirmeyen güvenlik sistemlerinden biridir [4]. Ses tanıma tekniği genel olarak iki ana gruba ayrılır:

I. Ses Tanıma Sistemleri
II. Konuşma Tanıma Sistemleri

Ses tanıma sistemlerinde kullanıcı sisteme parola olarak belirlediği bir kelimeyi bazı hecelerivurgulu olacak şekilde söyler, sistem parolanın kendisiyle beraber vurguların zamanlamasına ve şiddetine bakarak kullanıcıyı ayırt eder. Konuşma tanıma sistemleri, ses tanıma sistemlerinden teknik manada daha gelişmiştir. Burada vurgu tamamen ortadan kalkar. Yani kullanıcı özellikle bir vurgu yapmaz. Sistemle normal olarak konuşur. Sistem kullanıcıyı konuşma modundan anlamaya çalışır. Ses tanıma sistemleri hassasiyet olarak en düşük biyometrik sistemlerden birisidir. Avantajı ise sahip olma maliyetinin düşüklüğüdür.Burada en büyük dezavantaj sesin bilgisayar ortamına aktarılırken geçirdiği büyük değişim ve formatındaki bozukluktur. Bu sebeplerden dolayı ses tanıma sistemleri vurgu içermeleri açısından konuşma tanıma sistemlerine göre daha güvenilirdir.

Özellikle finans sektöründe, bankalarda, aracı kurumlarda müşteriyi sesinden tanıyarak kimlik doğrulaması yapan ve hizmet vermeye başlayan ürünler, ses tanıma teknolojileri için en iyi örnekleri oluşturmaktadır.

9.4.3 İmza Tanıma

Her insanın gerçek hayatta kullandığı, el yazması metinlerde insanları ayırt edici bir özellik olan imzaları bulunmaktadır. Eskiden beri insanlar kendilerini veya kendi ailelerini betimleyen imza, arma ya da özel işaretler kullana gelmişlerdir. Gerçekten dikkat edilirse imzalarımızı devamlı aynı şekilde, aynı hızda birbirleriyle oldukça benzer biçimde atarız. İmza tanıma sistemlerinin temelinde debu mantık vardır. Eğer herkes imzalarını her zaman aynı biçimde atıyorsa bu imzalar elektronik ortama aktarılarak ayırt edici bir güvenlik sistemi olarak kullanılabilir. Bunun için yazıyı elektronik ortama aktaran cihazlar uzun zamandır kullanımdadır. Bu aletler uygun şekilde kalibre edilerek bu tür bir güvenlik sistemi kurmak oldukça kolaydır. Güvenilirlik seviyesi parmak izi sistemlerine göre oldukça düşüktür.Bilgisayar ağlarında güvenliği sağlamada henüz kullanılmayan ve gelişme aşamasında olan diğer biyometrik teknolojiler ise şunlardır:

- Yüz Yapısı Tanıma
- Yazma Ritmi Tanıma
- Toplardamar İzi Tanıma
- Avuç İçi İzi Tanıma
- Kulak Şeklinden Tanıma

9.5 BİYOMETRİK TEKNOLOJİLER STANDART MIDIR ?

Biyometrik güvenlik sistemleri konusunda uluslararası bir standart söz konusudur. International Committee for Information Technology Standards (INCITS) (Uluslararası Bilgi Teknolojileri Standartları Komitesi) tarafından, parmak izi, iris-retina tabakası, ses tanımı gibi biyometrik tanımlama sistemlerinde kullanılacak işlemlere uluslararası bir standart getirme çabası sonucunda, örneğin, Türkiye'de bir banka hesabı ve parmak izi tanıma sistemi bulunan bankamatiklerden kredi kartı kullanmadan sadece parmak izini göstererek para çekebilen, bankacılık şlemlerine ulaşabilen bir kullanıcının dünyanın başka bir ülkesindeki bir bankanın da bankamatik cihazından, Türkiye'deki mevduat veya kredi hesabına ulaşarak, işlem yapmasını mümkün kılmak için gerekli olan standartlar belirlenmektedir.
Biyometri teknikleri, bugün şimdilik sadece dizüstü bilgisayarları açmak, sabit diskleri kullanabilmek gibi nispeten küçük uygulamalar için kullanılsa da, parmak izi, iris-retina tanımlaması işlemleri elektronik ticaret, web güvenliği gibi alanlarda da etkili olacak. Bu sebeple, dizüstü veya masaüstü sistemde bulunan tanımlama cihazına basılan parmak izi ile web üzerinden ulaşılan banka hesabında kayıtlı parmak izini karşılaştırmak için iki sistemin de okuduğu biyometri verilerinde mutlaka bir standart oluşması gerekiyor ki, biyometri teknolojisi yaygın ve etkin bir biçimde kullanılabilsin.

9.6 BİREY AYIRT ETME KAYNAKLARI KARŞILAŞTIRMA TABLOSU

Biyometri Kaynağı	Ayırt Edicilik	Dayanıklılık	Bulunabilirlik	Performans	Kabul Edilebilirlik	Sistemi Aldatma
Yüz	D	O	Y	D	Y	D
Parmak İzi	Y	Y	O	Y	O	Y
El Geometrsi	O	O	Y	O	O	O
Damar	O	O	O	O	O	Y
İris	Y	Y	O	Y	D	Y
Retina	Y	O	D	Y	D	Y
Ses	D	D	O	D	Y	D
İmza	D	D	Y	D	Y	D

Y: Yüksek **O:** Orta **D:** Düşük

Yukarıdaki Tabloda:

Ayırt edicilik; bu kaynakların bireyleri ayırt edebilme başarısını işaret eder.
Dayanıklılık; bu elemanların zamana ve yaşlanmaya karşı direncini ifade eder
Bulunabilirlik; bu kaynakların elde edilip işlemesinin kolaylığını gösterir
Performans; biyometri elemanlarının doğruluk yüzdesi, hızı ve sağlamlığını anlatır.
Kabul edilebilirlik; gündelik hayatta kabul edilme derecesini gösterir.
Sistemi aldatma sütunu ise bu kaynakları kullanarak sistemi aldatabilme ihtimalini belirtir.

9.7 KAYNAKÇA

[1]
http://209.85.135.132/search?q=cache:J7p_3ePwLYJ:members.comu.edu.tr/boraugurlu/courses/bm109/content/week8/slayt8.pdf+bilgisayar+a%C4%9Flar%C4%B1&cd=14&hl=tr&ct=clnk&gl=tr&client=firefox-a

[2]

http://www.networkturk.net/cisco/band-genislig-i-nedir.html

[3]

http://www.webmastersitesi.com/webmaster-sozlugu/genisbant-nedir.23204

[4]

http://209.85.135.132/search?q=cache:R7RRnV2oV-wJ:akmyo.kocaeli.edu.tr/agbilesenleri.ppt+utp+kablolar&cd=23&hl=tr&ct=clnk&gl=tr&client=firefox-a

[5]

http://www.forumacil.com/network-ve-internet-forumu/27553-lan-karakteristikleri-ve-iletisim-metodlari.html

[6]

222967-topoloji-nedir.html

[7]

ag-kablo-cesitleri_37924331.html

[8]

w3.gazi.edu.tr/~sirin/kaynaklar/ppt/Ag/Donanim_kablo.ppt

[9]

http://www.nuveforum.net/attachments/21711d1238277908-fiber-optik-kablolar-zip