YILDIZ TEKNİK ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

BİLGİSAYAR AĞLARINDA FARKLI HABERLEŞME ORTAMLARININ ORTAK BİR PROTOKOL İLE BİRLEŞTİRİLMESİ

IP ROUTER

Bilgisayar Mühendisi A. Gökhan YAVUZ

F.B.E. Bilgisayar Bilimleri Mühendisliği Anabilim Dalında

hazırlanan

YÜKSEK LİSANS TEZİ

Tez Danışmanı: Prof. M. Yahya KARSLIGİL

İSTANBUL, 1994

İçindekiler

I. Bölüm

II. Bölüm

III.Bölüm

IV. Bölüm

V.Bölüm

Tez çalışmamın başlangıcından tamamlanmasına kadar geçen süre boyunca gerekli araştırma ve çalışma ortamını sağlayan Prof M. Yahya KARSLIGİL'e, yapıcı ve yönlendirici fikirleri ile yol gösteren Doç. Kirkor Harutunyan'a ve çalışmamın her aşamasında desteklerini esirgemeyen araştırma görevlisi arkadaşlarım, A. Tevfik İnan, Zekiye Emiroğlu ve Serhan Meriç'e teşekkür ederim.

ÖZET

Bu tez çalışması IP (internet protocol) yapısındaki bilgileri taşıyan, ama farklı fiziksel ortamlardan oluşan network'ler arasındaki geçişi sağlayan IP router (yönlendirici) gerçekleştirilmesi konusunda yürütülmüştür.

Tez çalışması, teorik araştırma, bilgi toplama ve bunların hangi yöntemler ile pratiğe dönüştürüleceğinin belirlenmesi ve esas pratik çalışmanın yapılması bölümlerinden oluşmaktadır. Bu konu için özellikle bilgisayar dünyasında yer alan ve ticari olan IP router cihazlarının hangi özelliklere sahip oldukları, bu özelliklerden hangilerinin akademik ortam için gerekli olduğu hangilerinin ise seçimlik özellikler olabileceği incelenmiş ve sonuç olarak pratikte geliştirilecek olan IP router'ın hangi özellikleri içeriyor olması gerektiğine karar verilmiştir.

Uygulamanın gerçek hayatta kullanılmasının planlandığı Yıldız Teknik Üniversitesi, Elektrik Elektronik Fakültesi Bilgisayar Bilimleri ve Mühendisliği Bölümünün network imkanları da göz önünde bulundurularak X.25 ve ethernet protokolleri, IP'nin üzerinde çalışacağı alt seviye protokoller olarak belirlenmişlerdir.

Bir sonraki aşama olarak proje kapsamında yer alan X.25, ethernet, IP, ICMP ve ARP konularında kaynak taraması ve eğer varsa daha önce bu konuların akademik ortamlardaki uygulama örnekleri araştırılmış ve bunlardan edinilen tecrübeler de göz önünde bulundurularak uygulamaya geçilmiştir.

Sonuç olarak yapılan çalışma, bu cins bir uygulamanın Türkiye üniversiteleri içinde yeni bir uygulama olması ve bu sebeple sadece yabancı nitelikli kaynaklara başvurulmak durumunda kalınmasına rağmen, başarıyla gerçekleştirilmiştir.

SUMMARY

This thesis work has been carried out to design an IP router in order to allow message communication between IP based networks with different physical media.

To design an efficient and flexible IP router for the academical environment, first, major IP router products from well known caompanies has been inspected and all of their common attributes has been divided into two categories, as required and optional. Then through a careful analysis, attributes from those two categories has been selected to form the IP router.

Since it has been planned to use the developed IP router in a real networking environment in the Computer Sciences and Engineering Department of Technical University of Yıldız, the resources in this department has been evaluated and X.25 and ethernet has been selected as the physical media.

In the next step, a detailed research concerning the topics X.25, ethernet,IP,ICMP and ARP has been done to enable and also simplify the real application phase.

Although, this type of applications are new among the Turkish universities, the thesis work has been developed.

I.1 Bilgisayar Ağlarının Kullanımı

Günümüzde pek çok kuruluşta hatırı sayılır miktarda bilgisayar bulunmakta ve çoğunlukla bu bilgisayarlar birbirleri ile bağlantısız olarak çalışmaktadır. Örneğin birçok üretim merkezi olan bir kuruluşun her üretim merkezinde, o merkezin ihtiyaçlarını karşılamak üzere stok kontrol, muhasebe, personel takibi ve üretim planlaması için kullanılan bilgisayarları vardır. Ancak hiçbir merkez bir diğeri ile bağlantılı olmadığı için, üst düzey yönetim, kuruluşun o anki durumunu göremeyecek dolayısıyla stratejik kararları yeterince doğru ve hızlı alamayacaktır.

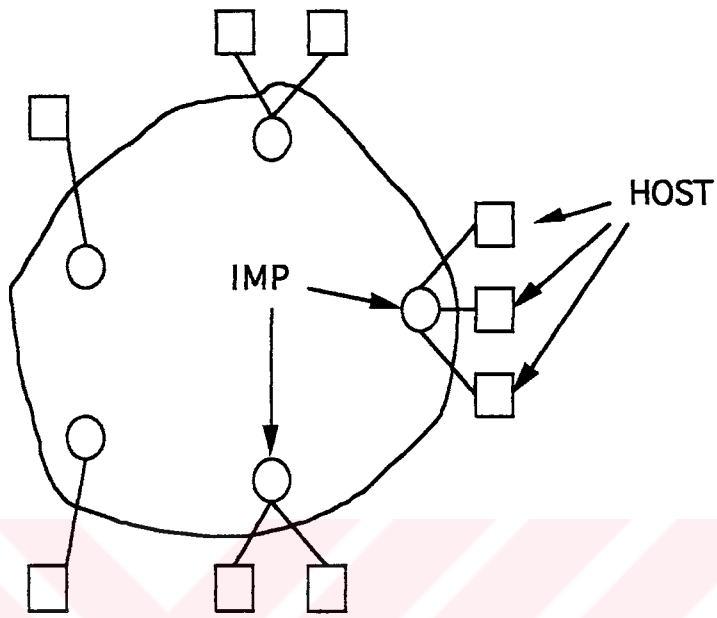
Bilgisayar ağlarının temel amacı hem mevcut donanımın ve yazılımın hem de varolan bilginin paylaşımını, ya da daha genel bir ifade ile mesafeden bağımsız olarak kaynak paylaşımını sağlamaktır.

Bilgisayar ağlarının ikinci amacı ise alternatif kaynakları gerektiğinde devreye sokarak yüksek güvenirlilik sağlamaktır. Örnek olarak bir bankanın müşteri bilgilerini çift kopya olarak tutması gösterilebilir. Kopyaların birinin bulunduğu bilgisayarın herhangi bir neden ile çalışmaması halinde bile diğer bilgisayar işlerin yürümesi için yeterli olabilecek ve aynı networkde bulunan bilgisayarlardan gelecek istekleri cevaplayabilecektir.

Bilgisayar ağları aynı zamanda paradan da tasarruf sağlarlar. Günümüzde küçük boy bilgisayarların fiyat, performans oranları büyük boy bilgisayarlardan daha iyidir. Bu nedenden dolayı network ile birbirine bağlı küçükboy bilgisayarlar yaygınlaşmaktadır.

I.2 Network Yapısı

Büyük networklerden ilki ARPANETtir. Bu networke bağlı olan bilgisayarlara HOST adı verilmiştir. Hostlar birbirine communication subnet (Haberleşme Alt Ağı) ile bağlıdır. Subnet hosttan hosta mesaj taşıma fonksiyonunu gerçekleştirir. Birçok geniş tabanlı bilgisayar ağlarında subnetin iki bileşeni vardır. Transmission lines (iletişim hatları) ve switching elements (anahtarlama elemanları). İletişim hatları (bunlar Circuits, Channels veya Trunks olarak da adlandırılır) ile makinalar arasında bilgi aktarımı sağlanır. Anahtarlama elemanları ise iki veya daha fazla sayıda iletişim hattını bağlayan bilgisayarlardır. ARPANET terminolojisinde anahtarlama elemanları IMP (Interface Message Processors) olarak adlandırılırlar. Bu yapının genel hali şekil 1-1 de gösterilmiştir.



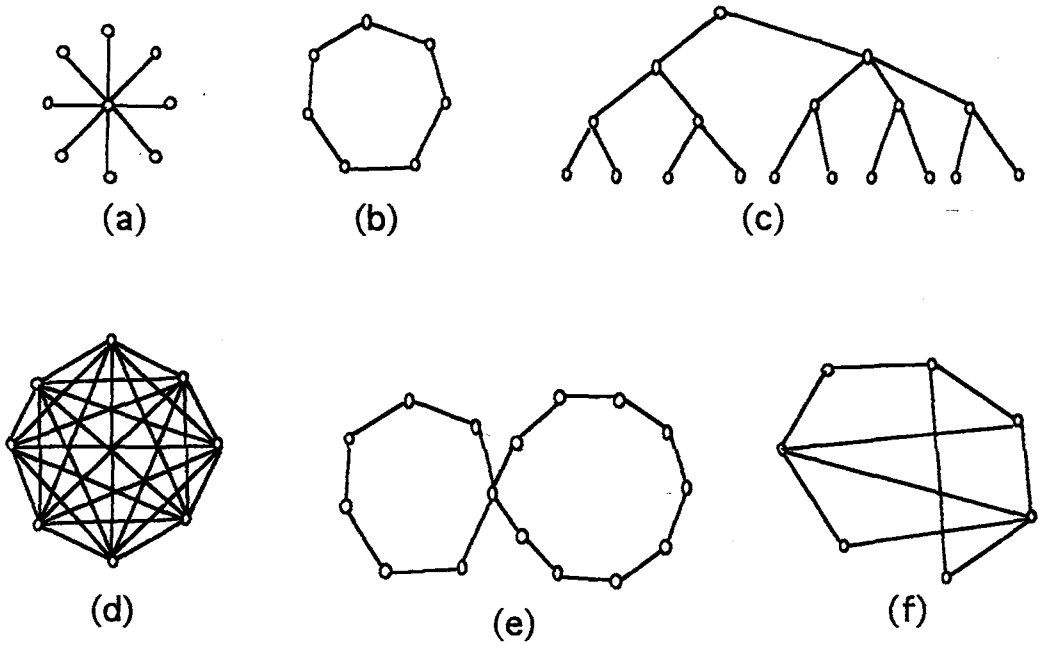
Şekil 1-1

Genel olarak bakıldığında iletişim altyapısı için iki temel tip sözkonusudur.

-Point to Point Channels (noktalar arası bağlantı)

-Broadcast Channels (Yayın kanalı)

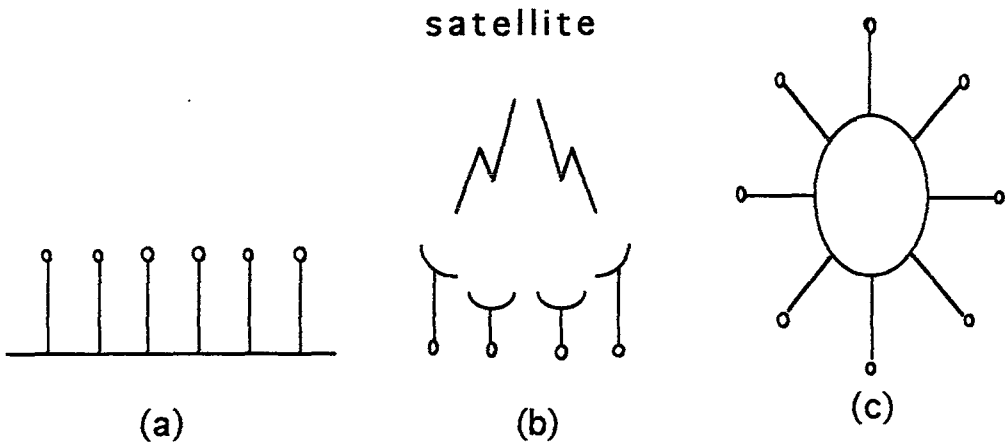
Birinci yapıda network birden fazla kablo ve telefon hattından meydana gelmiştir. Bu kablo ve hatlar IMP'leri birbirine bağlamaktadır. Birbirine doğrudan doğruya bağlantısı olmayan iki IMP diğerlerinin üzerinden geçerek haberleşirler. Bu yapı ile çalışan haberleşme ağlarına store and forward (sakla ve gönder) veya packet switched (paket anahtarlamalı) gibi isimler de verilir.



Şekil 1-2

Şekil 1-2 de point to point çalışmaya örnek değişik haberleşme ağlarının temel yapısı verilmiştir.

İkinci tip haberleşme yapısı ise broadcasting (yayın) yöntemiyle çalışmaktadır. Bu yapıya en güzel örnek Local Area Network (yerel haberleşme ağları) lerdir. Broadcast sistemlerde networke bağlı makinalar tek bir haberleşme kanalını paylaşırlar. Herhangi bir makina tarafından gönderilen bilgiler bu kanala bağlı diğer makinalarca da alınırlar. Bilgilerin içinde bulunan adres alanı, bilginin gerçekte hangi makinaya yönelik olduğunu belirtir. Broadcast sistemler bu yapılarından ötürü bir bilginin tek bir seferde belli bir grup makinaya veya makinaların tamamına gönderilebilmesine olanak vermektedir. Belli bir grup makinanın tamamına tek seferde bilgi gönderilmesi olayına multicasting adı verilir. Şekil 1-3 de broadcast yapısına uygun temel network topolojileri verilmiştir.

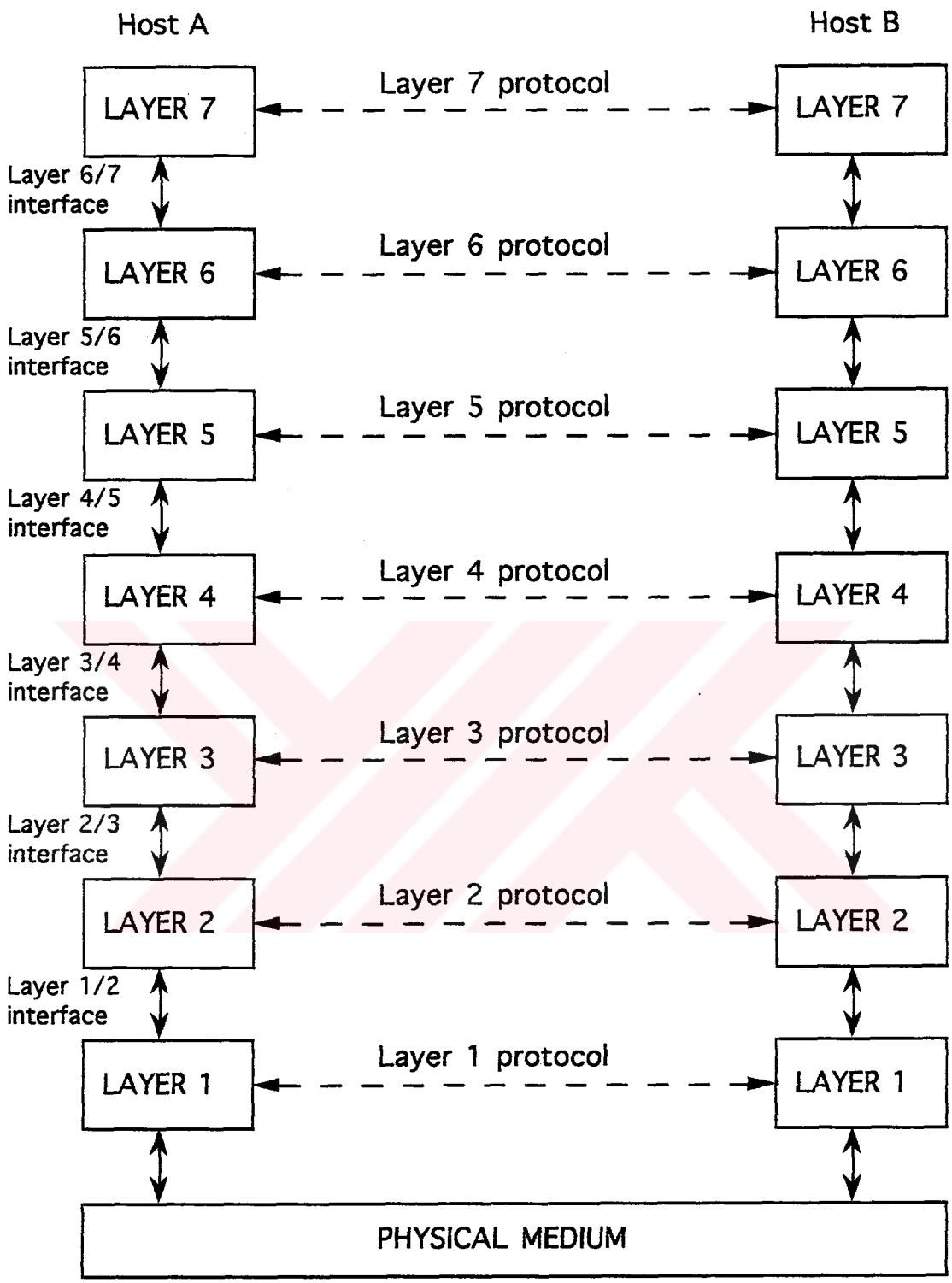


Şekil 1-3

I.3 Network Mimarileri

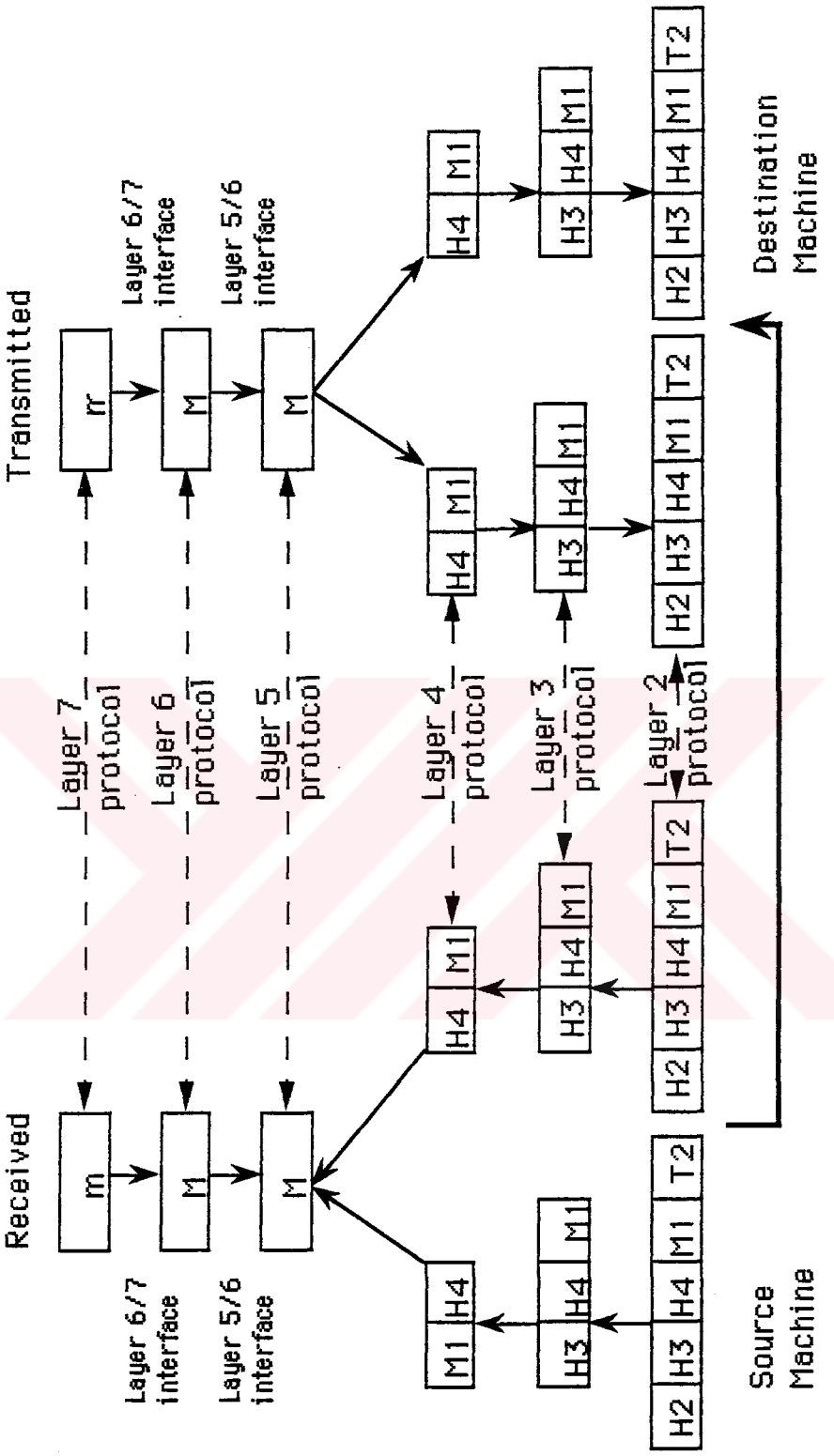
I.3.1 Protokol Hiyerarşileri

Tasarım zorluklarını basite indirgemek amacıyla pekçok network layer (katman) veya level (seviye) olarak adlandırılan parçalardan meydana gelmiştir. Bu katmanların sayısı, isimleri, içerikleri ve fonksiyonları networkden networke değişmektedir. Yine de her katmanın görevi kendisinden bir önce ve bir sonra gelen katmanlara gerekli servisleri sağlamaktır. Network üzerindeki herhangi bir makinada çalışan n. katman yine aynı networkdeki bir başka makinada çalışan n. katmanla belli kurallara ve yapılara uygun olarak haberleşmelidir. Bu kural ve yapıların tamamına protocol (protokol) adı verilir. Şekil 1-4 de 7 katmanlı bir ağ yapısında değişik protokoller gösterilmiştir. Değişik makinalarda aynı katmanı meydana getiren kısımlara peer process (denk işlemler) adı verilir.


Host A
Host B
LAYER 7
Layer 7 protocol
LAYER 7
Layer 6/7 interface
LAYER 6
Layer 6 protocol
LAYER 6
Layer 5/6 interface
LAYER 5
Layer 5 protocol
LAYER 5
Layer 4/5 interface
LAYER 4
Layer 4 protocol
LAYER 4
Layer 3/4 interface
LAYER 3
Layer 3 protocol
LAYER 3
Layer 2/3 interface
LAYER 2
Layer 2 protocol
LAYER 2
Layer 1/2 interface
LAYER 1
Layer 1 protocol
LAYER 1
PHYSICAL MEDIUM

Şekil 1-4

Birinci katmanın altı physical medium (fiziksel medya) olarak isimlendirilir ve haberleşme gerçekte bu medya üzerinden sağlanır. Katmanlar arasında interface (arabirim) adı verilen katmanlar arası işlemleri ve servisleri tanımlayan bir yapı mevcuttur. Network tasarımında en önemli faktörlerden biri de katmanlar arası iyi tanımlanmış interfacelere sahip olmaktır. Sözü geçen katmanların ve protokollerin tamamına network architecture (network mimarisi) adı verilir. Kullanılacak mimarinin özellikleri belirtilirken bu mimarinin uygulanabilmesi için gerekli tüm bilgilerin verilmesine özen gösterilmelidir. Diğer bir önemli nokta da mimari özellikler uygulamanın nasıl yapılacağını belirtmez ama uygulamanın hangi kurallara uygun olması gerektiğini tanımlar. Bu sayede aynı network üzerinde bulunan değişik makinaların haberleşme programları değişik kişiler tarafında yazılmış bile olsalar aynı mimari kurallarına uydukları sürece haberleşebileceklerdir. Bu akış şekil 1-5 de detaylı olarak olarak gösterilmiştir.


Transmitted
Received
rr
M
M
m
M1
M1
Layer 6/7 interface
Layer 5/6 interface
Layer 6/7 interface
Layer 5/6 interface
Layer 7 protocol
Layer 6 protocol
Layer 5 protocol
Layer 4 protocol
Layer 3 protocol
Layer 2 protocol
H4 M1
H3 H4 M1
H2 H3 H4 M1 T2
Source Machine
Destination Machine

Şekil 1-5

I.3.2 Katman Tasarımında Dikkat Edilmesi Gereken Hususlar

Her katman bağlantı kurulması için bir mekanizmaya sahip olmalıdır. Networkü birden fazla makinanın meydana getirdiği gözönüne alınacak olursa mesajların hangi makinaya yönelik olduğunu belirtmek için bazı adresleme yöntemleri kullanılmalıdır.

Tasarımda dikkat edilecek başka bir konu da veri transfer protokolüdür. Bazı sistemlerde veri sadece bir yönde transfer edilir. Buna simplex communication (tek yönlü haberleşme) adı verilir. Bazı sistemlerde ise her iki yönde de transfer edilir. Ancak eş zamanlı değildir. Bu protokol de half-duplex communication (dönüşümlü çift yönlü haberleşme) olarak adlandırılır. Her iki yönde de eş zamanlı olarak yapılan transfer ise full-duplex communication (çift yönlü haberleşme) adını alır. Kullanılacak protokol, aynı zamanda bağlantıda kaç logical channel (mantıksal kanal) kullanılacağına ve bunların önceliklerine de karar verilmesini sağlar.

Hata kontrolü de dikkat edilmesi gereken önemli konulardan biridir. Networklerde kullanılan birçok hata kontrol ve hata düzeltme kodu vardır. Ayrıca alıcının göndericiye, hangi mesajların doğru alındığını hangilerinin doğru ulaşmadığını bildirmesi gerekmektedir.

Birçok katmanda çözülmesi gereken bir başka problem ise işlemlerin değişik uzunluktaki mesajların alınması konusundaki yetersizlikleridir. Bu yüzden mesajların bölünmesi, gönderilmesi ve yeniden birleştirilmesi (disassembling, transmitting, reassembling) için bazı mekanizmalar oluşturulmalıdır.

Her haberleşme işlemi için ayrı bağlantıların kullanılmasının pahalı veya elverişsiz olması durumunda, alttaki katman aynı bağlantının, multiple (çoklu) olarak farklı konuşmalarda kullanılmasına karar verebilir. Bu yöntem, multiplexing ve demultiplexing işleminin transparent (saydam) yapılmasından dolayı her katmanda kullanılabilir.

Kaynak ve varış noktaları arasında birden fazla yol olması durumunda, bunlardan birinin seçilmesi gerekir. Bu karar bazen iki veya daha fazla katman arasında verilebilir.

I.4 OSI Referans Modeli

Şekil 1-6 da OSI modeline göre bir networkde yer alan katmanlar gösterilmektedir.

Bu model ISO OSI Open System Interconnection Reference Model adını alır. OSI modelinde 7 katman vardır. Bu katmanların genel özellikleri şöyle sıralanabilir.

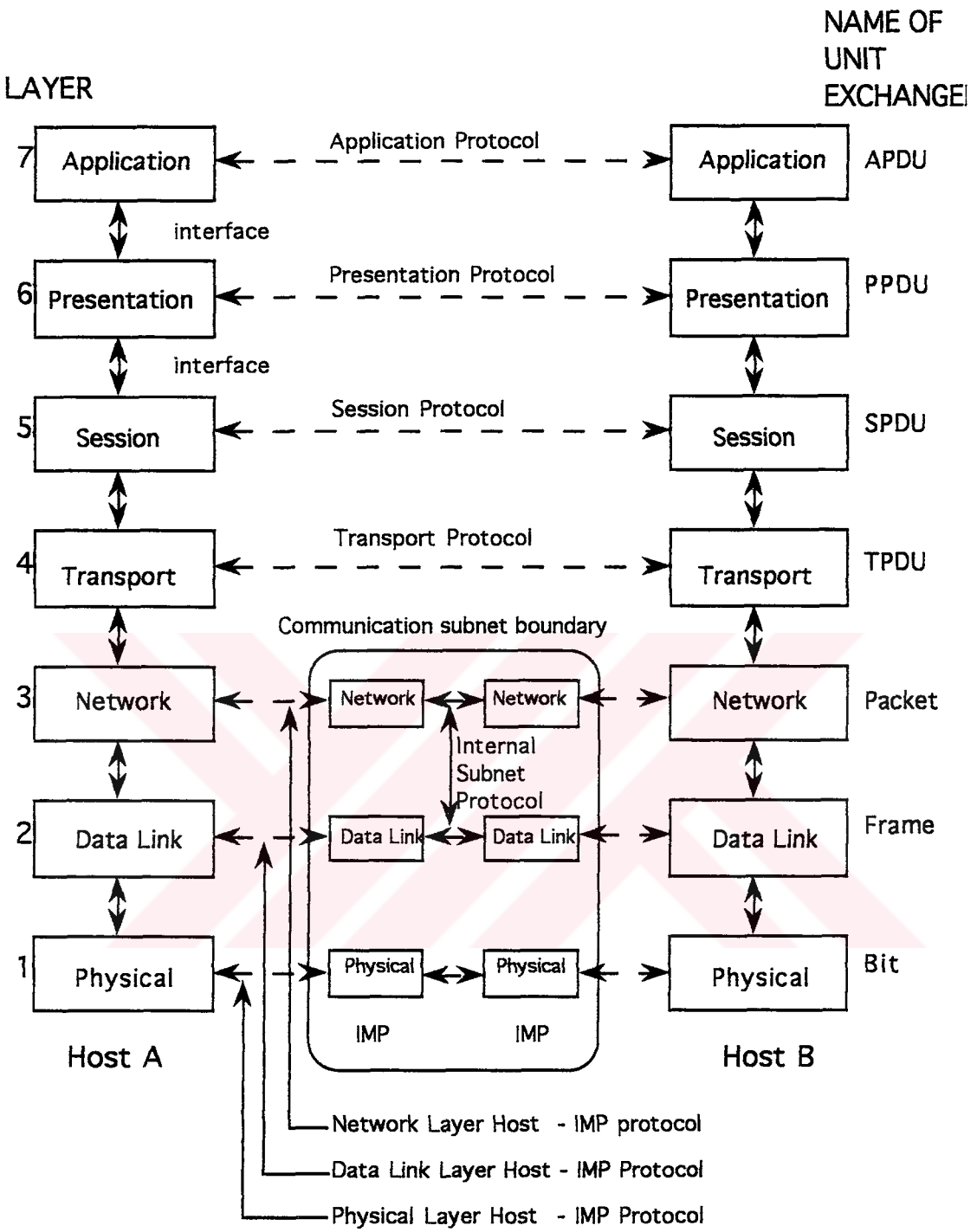
-Bir katman ancak değişik seviyede bir ayırma gerekirse oluşturulur.
-Her katman belli bir fonksiyonu yerine getirir.
-Katmanların fonksiyonları uluslararası standardizasyon protokollerine uygun olarak seçilmelidir.
-Katman sınırları arabirimler arasındaki bilgi akışını minimize edecek şekilde seçilmelidir.
-Katmanların sayısı ayrık fonksiyonları aynı katmana sıkıştırmayacak kadar fazla ama mimariyi kullanılamayacak hale getirecek kadar da az olmamalıdır.

I.4.1 Physical Layer (Fiziksel Katman)

Fiziksel katman işlenmemiş verinin haberleşme kanalı üzerinden gönderilmesini sağlar. Tasarımda karşılaşılan en önemli sorun, taraflardan birinin gönderdiği bilginin karşı tarafta doğru olarak nasıl alınacağıdır. Burada karşılaşılan problemler; 0 ve 1 seviyelerini göstermek için kaç volt kullanılacağı, 1 bitin transferi için kaç mikrosaniye geçeceği, başlangıç bağlantısının nasıl sağlanacağı, her iki tarafın işi bittiğinde nasıl kesileceği, network bağlantı biriminde kaç uç olduğu ve her ucun hangi amaçla kullanıldığı gibi problemlerdir.

I.4.2 Data Link Layer (Data Bağlantı Katmanı)

Bu katmanın esas fonksiyonu veriyi iletim hatalarından arınmış olarak network katmanına göndermektir. Bu işlem, gönderilen veri, önce data frame (veri çerçeveleri) lere ayrılıp, daha sonra ardışık olarak yollanarak ve alıcı tarafından yollanan acknowledgement frame değerlendirilerek gerçekleştirilir. Frame sınırlarının oluşturulması ve tanınması data bağlantı katmanının işidir. Bunu her frame'in başına ve sonuna özel veri grupları ekleyerek gerçekleştirir. Bu özel veri grupları, kazara gönderilen verinin içinde oluşursa karışıklıktan kurtulmak için özel önlemler alınmalıdır.


LAYER
NAME OF UNIT EXCHANGE
7 Application
Application Protocol
Application
APDU
interface
6 Presentation
Presentation Protocol
Presentation
PPDU
interface
5 Session
Session Protocol
Session
SPDU
4 Transport
Transport Protocol
Transport
TPDU
Communication subnet boundary
3 Network
Network
Network
Network
Packet
Internal Subnet Protocol
2 Data Link
Data Link
Data Link
Data Link
Frame
1 Physical
Physical
Physical
Physical
Bit
IMP
IMP
Host A
Host B
Network Layer Host - IMP protocol
Data Link Layer Host - IMP Protocol
Physical Layer Host - IMP Protocol

Şekil 1-6

Üzerinde iletim yapılan hat üzerinde gürültü oluşursa bu bir frame'i tamamen bozabilir. Bu durumda gönderici makina üzerindeki veri bağlantı katmanı yazılımı bu frame'i yeniden göndermelidir. Acknowledgement frame'in bozulması durumunda ise aynı verinin iki defa gönderilmesi problemi ortaya çıkar. Bu tür problemler data bağlantı katmanındaki değişik servisler tarafından çözülür.

Veri iletiminde gönderici ve alıcının hızlarının aynı olmaması, iletim hatları üzerindeki trafiğin düzenlenmesi için bazı protokoller kullanılmasını gerektirmektedir. Eğer bir hat çift yönlü kullanılıyorsa oluşan zorlukları çözmek için piggybacking yöntemi kullanılır.

I.4.3 Network Layer (Network Katmanı)

Bu katman subnetin gerçekleştirdiği işlemlerin kontrolü ile ilgilenir. Buradaki problemlerden en önemlisi paketlerin kaynaktan varışa hangi yol izlenerek gönderileceğidir. Bu yollar; ya network üzerinde az değişen, statik tablolarda tutulur ya da her konuşmanın başında iletimin hangi yol üzerinde yapılacağına karar verilir. Subnet üzerinde aynı anda çok sayıda paket yer alıyorsa bunların birbirinin yolu üzerinde bulunmasından oluşan problemleri de network katmanı çözer. Network katmanının görevleri arasında networkler arasındaki veri iletiminde adresleme yöntemlerinin farklılığı yüzünden oluşan hataların önlenmesi, aktarılan verinin maaliyetinin hesaplanması gibi işlemler de yer alır.

I.4.4 Transport Layer (Taşıma Katmanı)

Bu katmanın görevi oturum katmanından veriyi almak, gerektiği kadar küçük parçalara ayırmak, network katmanına geçirmek ve tüm parçaların diğer tarafa doğru olarak ulaşmasını sağlamaktır. Normal koşullarda taşıma katmanı, oturum katmanı tarafından istenen her taşıma bağlantısı için ayrı bir network bağlantısı yaratır. Eğer taşıma bağlantısı yüksek performans gerektiriyorsa, taşıma katmanı çoklu network bağlantıları oluşturur, veriyi bu bağlantılar arasında dağıtarak performansı dengeler. Bu bağlantıların oluşturulmasının ve bakımının pahalı olduğu durumlarda aynı taşıma bağlantıları tek network bağlantısı üzerinde çoklanarak maliyet azaltılır. En çok kullanılan taşıma bağlantısı error-free (hatasız) point to point channel bağlantısıdır.

I.4.5 Session Layer (Oturum Katmanı)

Bu katman değişik makinalardaki kullanıcıların aralarında oturum gerçekleştirmelerini sağlar. Bir oturum, taşıma katmanının sağladığı normal taşıma işlemini ve ayrıca bazı uygulamalarda gereken özel servisleri sağlar. Oturumlar aynı zamanda kullanıcının değişik makinalar arasında dosya transferi yapmalarını, ve uzak zaman paylaşımlı sistemlere (remote time-sharing systems) bağlanmalarını sağlar. Karşılıklı konuşma kontrolünün yönetimi , simge yönetimi (token management) ve senkronizasyon oturum katmanının görevleri arasındadır.

I.4.6 Presentation Layer (Sunu Katmanı)

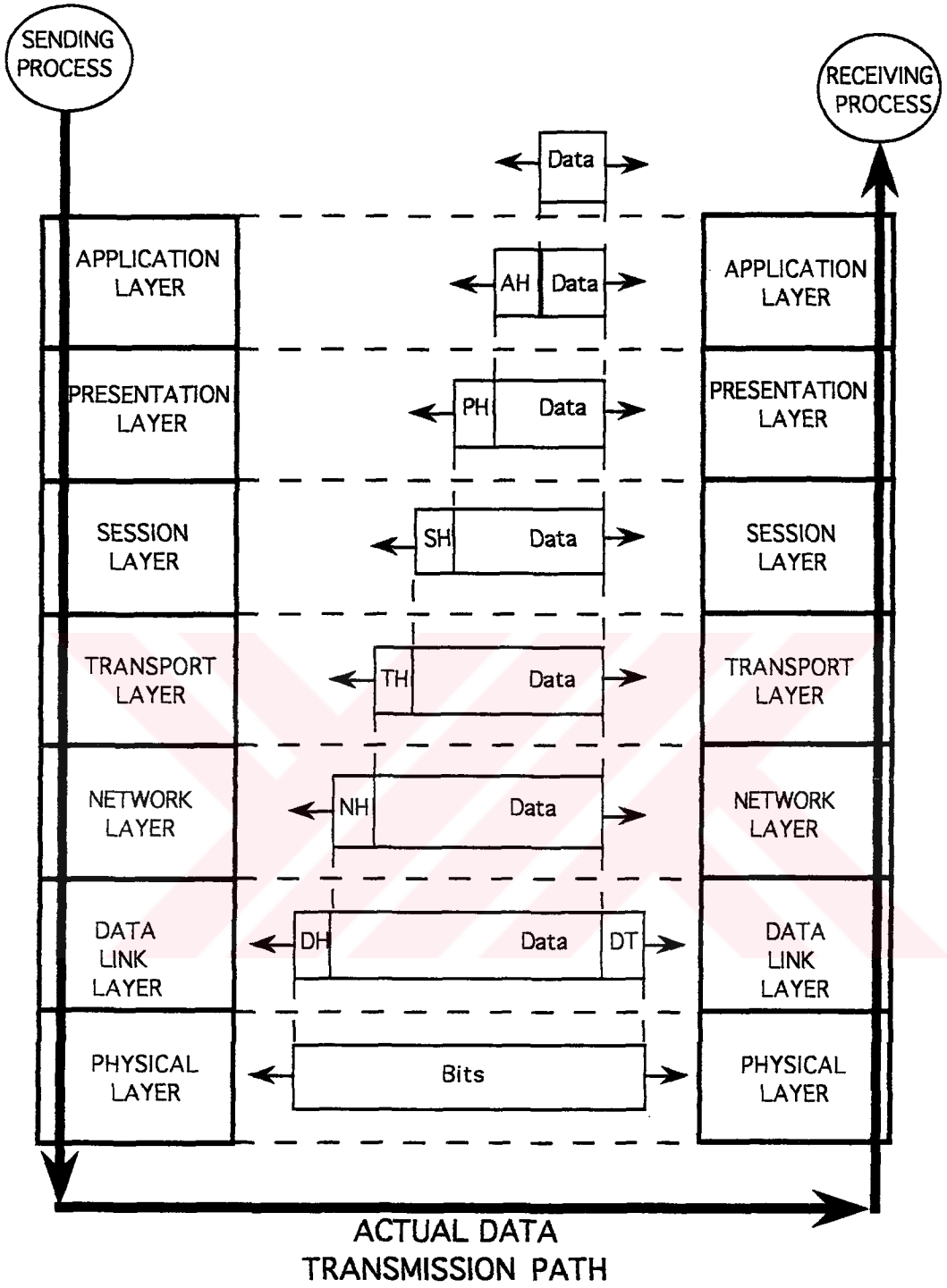
Sunu katmanı diğer katmanların aksine veri iletimiyle ilgilenmez. Özellikle taşınan bilginin sentaks ve semantiği ile ilgilenir. Veri sıkıştırma, kriptografi gibi işlemler bu katmanın görevleri arasındadır. Kullanılan veri yapılarının düzenlenmesi ve kullanılan sistem ile standart network gösterimi arasındaki dönüşümlerin yapılması da bu katmanın görevidir.

I.4.7 Application Layer (Uygulama Katmanı)

Bu katman değişik protokolleri içerir. Mesela değişik bilgisayar sistemlerinde kullanılan birbirleriyle uyumlu olmayan çok sayıda terminal tipi vardır. Bu değişik tip terminallerin network üzerinde uyumlu olarak çalışmaları önemli bir problemdir. Bu problemin çözümlerinden biri de, editörlerin ve diğer programların kullanabileceği network virtual terminaller (görüntü network terminalleri) oluşturmaktır.

I.4.8 OSI Modelinde Veri Taşıma

OSI modelinde veri taşıma işlemi şöyle gerçekleşir. Gönderici taraf, alıcı tarafa göndermek istediği veriyi uygulama katmanına verir. Bu katman verinin baş tarafına application header (uygulama başlığı) AH ekler ve sonucu sunu katmanına iletir. Sunu katmanı bu verinin başına başka bir header ekleyerek bunu oturum katmanına gönderir. Bu verinin hangi kısmının gerçek veri, hangi kısmının header olduğu oturum katmanı tarafından bilinmez. Bu işlem veri, fiziksel katmana ulaşıncaya kadar devam eder. Bu katmanda veri alıcı makinaya iletilir. Bu makinadaki katmanlarda da mesajdaki tüm headerlar çıkartılır ve bu şekilde mesaj alıcı tarafa ulaşmış olur. Şekil 1-7 de bu işlemin nasıl gerçekleştiği görülmektedir.


SENDING PROCESS
RECEIVING PROCESS
Data
APPLICATION LAYER
AH
Data
APPLICATION LAYER
PRESENTATION LAYER
PH
Data
PRESENTATION LAYER
SESSION LAYER
SH
Data
SESSION LAYER
TRANSPORT LAYER
TH
Data
TRANSPORT LAYER
NETWORK LAYER
NH
Data
NETWORK LAYER
DATA LINK LAYER
DH
Data
DT
DATA LINK LAYER
PHYSICAL LAYER
Bits
PHYSICAL LAYER
ACTUAL DATA TRANSMISSION PATH

Şekil 1-7

I.5 Network Standardizasyonu

Bilgisayar ağı kullanımının ilk yıllarında her bilgisayar üreticisi kendine has bir network protokolü geliştirdiler. Mesela IBM'in bir düzineden fazla protokolü vardı. Sonuçta değişik şirketlerden bilgisayar alan kullanıcılar bunları tek network üzerinde birleştiremez hale geldiler. Bu karışıklık kullanıcıların protokoller konusunda bir standart istemelerine yol açtı. Standartlar iki kategoride toplanabilir. de facto ve de jure. De facto (Latince, 'gerçeklerden yola çıkarak' anlamında) , resmi planlar olmaksızın oluşturulmuş standartlardır. Mesela IBM PC standartı kişisel bilgisayarlarda bu şekilde oluşmuş standartlardandır. Bunun oluşum sebebi bilgisayar üreticilerin çoğunun IBM makinalarını olduğu gibi kopya ederek bilgisayar üretmeleridir. De jure (Latince, 'kanun yoluyla' anlamında) standartlar resmi, kanuni standartlardır. Uluslararası standart otoriteleri iki gruba ayrılabilir. İlki hükümet anlaşmalarıyla oluşturulmuş ve uygulanan standartlar, ikincisi de gönüllü anlaşmasız organizasyonlar. Bilgisayar network standartlarında her iki tür standart organizasyonları da önemlidir ve kullanılmaktadır.

I.6 Örnek Bilgisayar Ağları

Günümüzde dünyada pek çok bilgisayar ağı bulunmaktadır. Bunlar mevcut telefon hatları ile birbirine bağlı ya hemen hemen herkese açık ya araştırmaya yönelik ya da ticari nitelikli ağlardır.

I.6.1 Public Networks (Halka Açık Ağlar)

Dünyadaki çoğu ülkede resmi ya da özel kuruluşlar üyelerini bilgisayar ağlarından yararlandırmaktadır. Bunlar genellikle mevcut telefon sistemini kullanan ve kendi kuralları çerçevesinde halka açık yapılardır. Ülkelerdeki network yapıları birbirinden bazı farklılıklar gösterirler. Ancak çoğu OSI modeline sadık olup OSI ya da CCITT protokollerini network katmanlarında kullanırlar.

OSI modelinin alttan üç katmanı için CCITT önerileri hemen hemen tüm dünyadaki bilgisayar ağlarında kullanılmaktadır. Bu standartlar ISO ve CCITT tarafından numaralandırılmıştır.

Fiziksel bağlantı katmanında kullanılan X.21 protokolü bilgisayar ile bilgisayar ağı arasındaki elektriksel ve işlevsel yapıyı tanımlamaktadır.

Data bağlantı katmanında ise standardlar biraz farklılık göstermektedir. Ancak hepsi telefon hatları üzerinde meydana gelen aktarım hataları ile ilgilenmektedir.

Network katmanının üzerindeki standardlar benzerdir. Connection-oriented (bağlantıya yönelik) taşıma katmanı servis ve protokolü ISO 8072 ve ISO 8073 ile tanımlanmıştır.

Oturum katmanında connection-oriented session servisi ve protokolü ISO 8326 ve ISO 8372 ile tanımlanmıştır.

Uygulama katmanında ise FTAM (File Transfer Access and Management), MOTIS (Message Oriented Text Interchange Systems), VTP (Virtual Terminal Protocol), JTM (Job Transfer and Manipulation) ve benzeri protokoller kullanılmaktadır.

I.6.2 ARPANET (Advanced Research Project Agency NETwork)

1960 lı yıllarda Amerikan Savunma Bakanlığı desteğinde Amerikadaki belli başlı üniversite ve özel kuruluşların bilgisayar sistemlerini bir bilgisayar ağı ortamında bir araya getiren projedir. ARPANET, OSI modelini takip etmemiştir.

I.6.3 BITNET (Because It's Time NETwork)

1981 de Amerikan üniversiteleri arası bir bilgisayar ağı kurma isteğinin bir sonucu olarak ortaya çıkmıştır. Avrupadaki EARN (European Academic Research Network) ile bağlıdır. BITNET üzerindeki düğüm noktaları bir diğerine kiralık telefon hatları ile bağlanmışlardır. BITNET, IBM tarafından sağlanan yazılım ve donanım imkanlarını kullanmaktadır.

I.6.4 SNA (Systems Network Architecture)

SNA , IBM'min ağ yapısıdır ve OSI modelinin oluşturulmasına taban teşkil etmiştir. SNA den önce pekçok haberleşme yöntemi denenmiştir. SNA bu karmaşayı ortadan kaldırmak amacı ve IBM bilgisayarları arasında uyumlu bir çalışma yapısı oluşturmak üzere geliştirilmiştir.

II.1 Network'ler Arası Bağlantı

Dünyadaki bütün networklerin aynı yapıda ve birbirleriyle aynı protokol seviyelerine sahip olduğunu kabul etmek çok iyimser bir yaklaşım olur. Bir çok değişik network mevcuttur. Günümüzde dünya üzerinde 20.000'den fazla SNA network, 2000'den fazla DECNET network ve sayılamayacak kadar çok ve çeşitli LAN kullanılmaktadır. Bunlardan ancak çok azı OSI modelini kullanmaktadır.

İleride hala bu kadar çok ve çeşitli network olup olmayacağı şu an için en önemli ve cevaplanamayan sorudur. Ama yine de aşağıdaki sebeplerden ötürü ileride de bir çok farklı networkün ortaklaşa çalışacağı görülmektedir. İlk olarak OSI modelini taban almayan bir çok network şu an dünyada kullanılmakta ve bunların sayısı hızla artmaktadır. IBM ise yeni SNA sistemleri geliştirmekte ve satmaktadır. Bir çok UNIX tabanlı sistem TCP/IP kullanmaktadır. LAN'lar ise seyrek olarak OSI modeline uymaktadır. Bunun böyle devam edeceği çok belirgindir çünkü hiç bir ticari kuruluş kendi satmakta olduğu sistem modelini bırakıpta rakip firmaların sistemlerini satmayı kabul etmeyecektir.

İkinci sebep ise bilgisayarlar ucuzladıkça karar noktaları aşağıya doğru kaymaktadır. Bir çok firmanın karar yapısı şu şekildedir. Bir milyon doları geçen satın alma kararları üst düzey yönetimce, yüz bin doları geçen kararlar orta düzey yönetimce, yüz bin doların altındaki kararlar ise alt düzey yönetimce alınabilmektedir. Bu yüzden bir firma içinde muhasebe bölümü Ethernet tipi bir network, mühendislik bölümü bir token bus (simge yolu) tipi network ve personel bölümü ise token ring simgeli halka) tipi network kurdurtabilir.

Üçüncü olarak, değişik networkler kökten farklı network teknolojilerine sahiptir. Bu yüzden yeni donanım teknolojileri ve bunlara bağlı yeni yazılım teknolojileri geliştirildikçe bunların OSI modeline uyumlu olması beklenemez.

OSI modeline uymayan bir çok networkün olduğu ve bunların birbiriyle haberleşmesi gerektiği bellidir. Bir çok üniversitede, bilgisayar ve elektrik mühendisliği bölümlerinin kendi LAN'ları vardır. Bunların çoğu da birbirlerinden farklıdır. Bu LAN'ların üzerinde bir çok kişisel bilgisayar, workstation (iş istasyonları) ve minibilgisayar çalışmaktadır. İnsanlar sayılarla ve harflerle ilgili bir çok uygulama programı çalıştırmaktadırlar. Sayısal uygulamalar erişilebilir güç, harflerle ilgili uygulamalarsa donanım sorunları sebebiyle merkezi mainframe'lere yollanmakdatırlar. LAN'lar ve mainframe'ler yurtiçi ve yurtdışı WAN'lara ve birbirlerine bağlıdırlar. Şu şekildeki çalışma senaryoları hemen akla gelebilir:

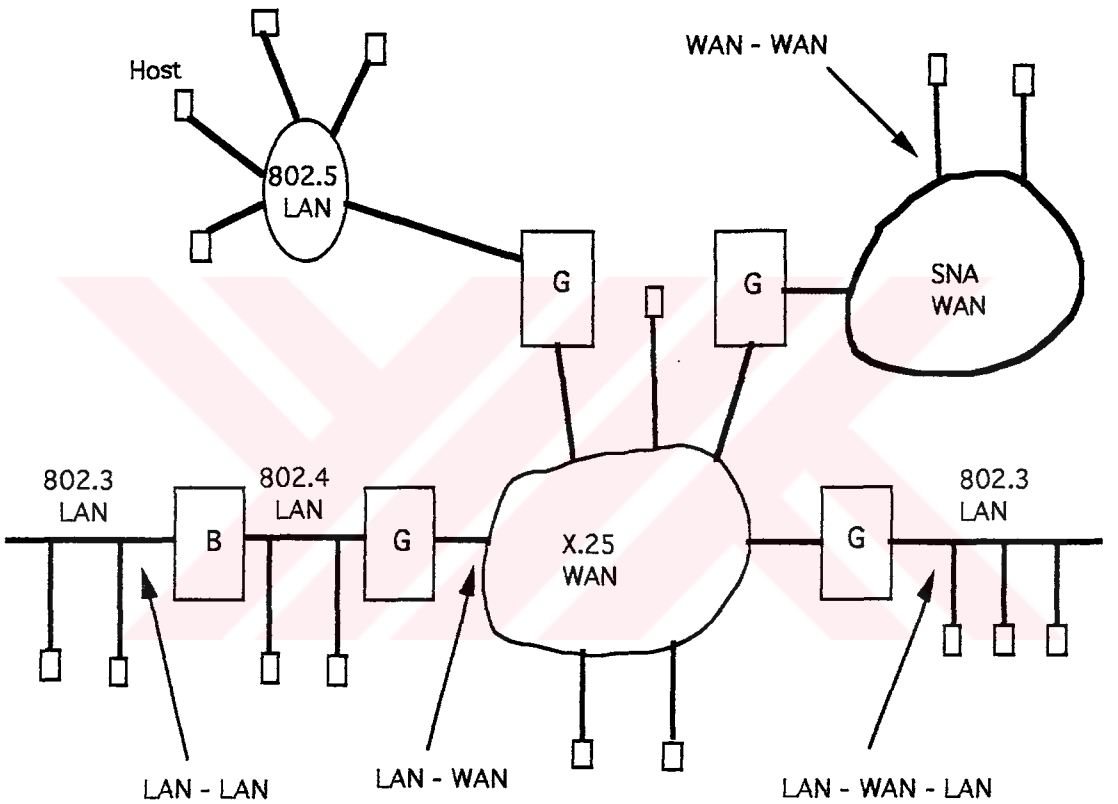
LAN - LAN : Bir bilgisayar mühendisi mühendisliğe bir dosya yolluyor.

LAN - WAN : Bir bilgisayar mühendisi uzak bir fizikçiye mektup yolluyor.

WAN - WAN : İki şair karşılıklı sone yolluyorlar.

LAN - WAN - LAN : Farklı üniversitedeki iki mühendis haberleşiyorlar.

Bu senaryolar şekil 2-1 de genel olarak gösterilmiştir.



Şekil 2-1

Bu işlemler kesikli çizgilerle gösterilmiştir. Her durumda da iki networkün kesişme noktasına bir 'kara kutu' konulmalıdır. İki farklı network arasındaki bilgi alışverişi için gerekli olan çevirimi ancak bu kara kutular sağlamaktadır. Bu cihazların genel adı relay(röle) 'dir. Relay'lar ya iki networkü bağlıyacak gibi (bilateral) ya da bir çok networkü bağlıyacak gibi (multilateral) üretilmiş olabilirler.

II.1.1 OSI ve Networkler Arası Bağlantı

OSI modelinde networkler arası bağlantı network katmanında gerçekleşir. OSI'nin oluşturduğu modelin en geniş kabul gördüğü noktası bu saha ve network güvenliği sahasıdır. Network konusundaki önerilere bakan bir insan networkler arası bağlantının oluşturulan modele çok kısa bir sürede yamanmış olduğu hissine kapılabilir. DARPA (Defense Advanced Research Projects Agency) 10 yılı aşkın bir süredir kendi bünyesindeki yüzlerce birbirine bağlı networkü yönettiği ve pratikte neyin çalışıp neyin çalışmadığını bildiği halde ARPA (Advanced Research Projects Agency) nın ortaya koyduğu karşı çıkışlar beklendiği kadar elle tutulur değildir. Aslında ISO bu başarısızlıkta tek başına değildir. Örnek olarak CCITT networklerin numaralanma planlamasında dört hanenin dünya çapında yeterli olacağını düşündüğü halde sadece 20000 adeti aşkın SNA tipi networkün var olduğu düşünüldüğü zaman bile bunun yetersiz olduğu kolaylıkla anlaşılabilir.

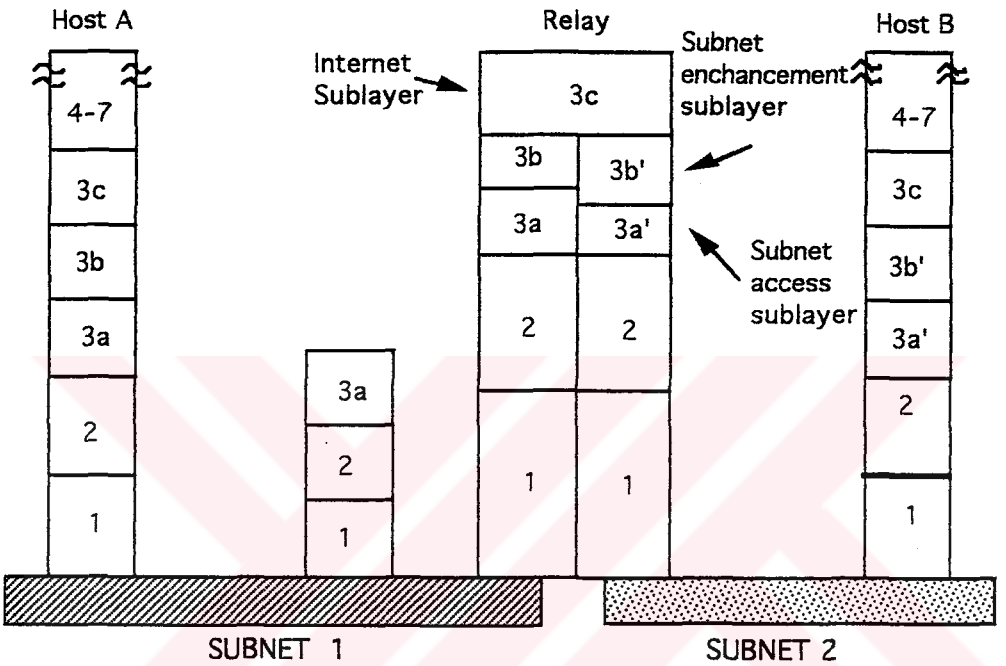
Problem, çoğu zaman sadece düşük tahminlerden değil aynı zamanda yanlış mantık yürütmekten de kaynaklanmaktadır. Örneğin, CCITT'ye göre her ülkenin PTT'si tarafından yürütülen ancak bir veya iki adet genel networkü olabilirdi. Onların görüşüne göre özel networkler çok önemli değildi. 20000 adet SNA tipi network bir gece içinde mucizevi olarak OSI modeline uygun hale getirilse de sahiplerinin bu networklerin kontrolunun tamamen genel bir network altına alınmak istenmesine yanaşmayacakları ise aşikardır.

OSI modelinde networkler arası bağlantı şu şekilde yapılmaktadır. Gerektiğinde network katmanı kendi içinde üç ara katmana ayrılır: Subnet Access Sublayer (Altyapı Erişim Ara Katmanı), Subnet Enhancement Sublayer (Altyapı Geliştirme Ara Katmanı), Internet Sublayer (Networklerarası Ara Katman).

Subnet Access Sublayerin görevi kullanılan ara katmana uygun network katmanı protokolünü çalıştırmaktır. Network katmanının görevlerini yerine getirmenin yanında veri oluşturur, veri toplar ve kontrol paketlerini taşır. Subnet Enhancement Sublayer değişik sevisler sunan bir çok farklı ara katmanın uyumlu olarak çalışmasını sağlar.

Ara katmanlar bir çok noktada farklı olabilirler. Örnek olarak adresleme verilebilir. Internet ara katmanı sadece erişilecek her makine için değil de her erişim noktası için adresleme isteyen NSAP'i kullanabildiği gibi başka yöntemlerde kullanabilir.

Internet ara katmanının en önemli görevi uçtan uca yönlerdirme yapmaktır. Herhangi bir network noktasına gelen bir veri paketi üst katmana iletilir ve bu ara katman onun daha da ilerletilip ilerletilmeyeceği hakkında karar vermek yanında ilerletilecekse hangi ara katmanın kullanılacağına da karar verir. Çünkü çoklu bir relay'in birden fazla ara katmanı vardır. İlk yaklaşım olarak ara katmanlar arası yönlendirmenin bir network içerisinde yönlendirmeden farklı olmadığı söylenebilir. Fakat büyük bir networkler arası bağlantı için hiyerarşik yönlendirmenin en iyisi olduğu açıktır çünkü böylece relay'ler uzak networklerin iç yapılarını bilmek zorunda değillerdir.



Şekil 2-2

Şekil 2-2 deki yapıda relay 3. katmana kadar çıkmakta ve veri paketlerini bu katmanda hareket ettirmektedir. Genel olarak relay'ler her seviyede olabilirler. Relay'lerin genel olan dört tanesi şunlardır:

Katman 1: Repeaters(Tekrarlayıcılar): Kablo parçaları arasında tek tek bitleri kopyalarlar.

Katman 2: Bridges(Köprüler): LAN'lar içerisinde frame'leri saklar ve ilerletirler.

Katman 3: Gateways(Geçiş Yeri): Farklı networkler arası veri paketlerini saklar ve ilerletir.

Katman 4: Protocal Converters (Protokol Çevirici) : Daha yüksek seviyede iletişimi sağlar.

II.1.2 Bridges (Köprüler)

Repeater'lar sadece elektrik sinyallerini güçlendiren düşük seviyeli cihazlardır. Uzun mesafeli iletişimlerde kabloların kayıplarını gidermek içi kullanılırlar.

Bridge'ler repeater'lardan farklı olarak saklama ve ilerletme işlemlerini yaparlar. Bir bridge bir veri paketini bir bütün olarak kabul eder ve onu data link katmanına ilerletir. Burada checksum (hata toplamı) kontrolu yapıldıktan sonra paket yine fiziksel katmana gönderilir. Bridge'ler frame'ler üzerinde ilerletmeden önce bazı ufak başlık değişiklikleri uygulayabilirler. Katman 2'den yukarısına ait hiç bir değişiklik yapamazlar.

Gateway'ler genelde bridge'lere benzerler. Fakat onlar farklı olarak network katmanında bulunurlar. Zaman zaman gateway genel bir ifade olarak kullanılır ve network gateway'ler router diye de adlandırılırlar. Genel kural olarak gateway'e bağlı olan networklerle bridge'lere bağlı olanlar farklıdırlar. Gateway'lerin bridge'lere göre en büyük avantajı farklı adresleme yöntemleri olan networkleri birbirlerine bağlayabilmeleridir. Transport katmanı ve daha yukarısındaki relay'lere genellikle protocol converter adı verilir. Bunun görevi bir gateway'e göre çok daha karmaşıktır. Bunlara bir örnek olarak OSI transport protokolünü TCP protokolüne çeviren bir converter verilebilir. Aslında relay network yapısının hangi seviyesinde olursa olsun asıl sorun bağlanan iki network arasındaki uyum faktörüdür. İki network birbirinden frame, paket, mesaj uzunluğu, checksum algoritması, maksimum paket ömrü, connectionless (bağlantısız) veya connection-oriented (bağlantıya yönelik) protokol, zaman değeri gibi kavramlar açısından farklı olabilir. Bazen ise çeviri ihtiyaçları farklı olduğu için zaman içerisinde her bir bölüm kendi ihtiyacına göre bir LAN kurar. Bunların birbirleriyle aynı olması çok düşük bir olasılıktır. Bir gün bu LAN'ların birbirleriyle haberleşmeleri gerektiği zaman bu işi tek yapabilecek cihaz bir bridge'dir. Böylece bir bridge'in networklerin sahiplerinin farklılığından gerektiği ortaya çıkar.

İkinci olarak, jeolojik dağılımı çok büyük olan bir organizasyonun her binasında tek bir LAN kurması ve bunlar arasında bridge'ler vasıtasıyla haberleşmeyi sağlaması daha ucuz olabilir.

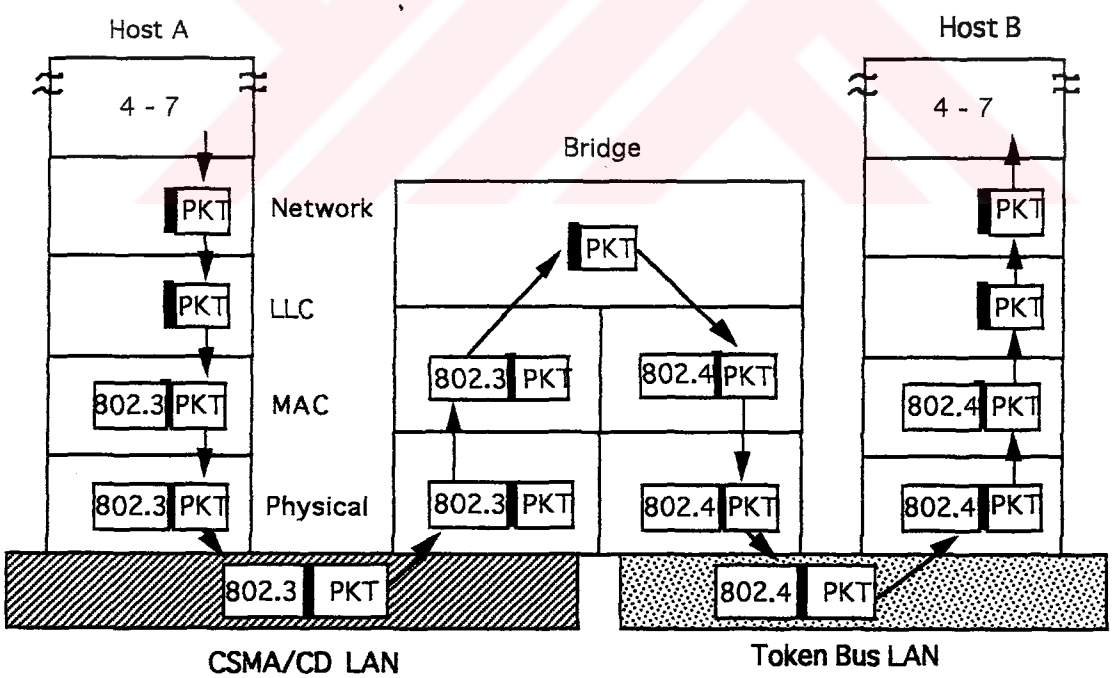
Üçüncüsü aslında tek bir LAN olarak çalışması gereken bir networkü yükü dağıtmak amacıyla bir kaç LAN üzerinden çalıştırmak ve bunlar arasındaki haberleşmeyi bridge'ler üzerinden yapmaktandır.

Dördüncü örnek ise, aslında yine bir network olarak çalışması gerektiği halde bu defa yük sebebiyle değil de kullanıcılar arasındaki mesafe yüzünden hattın networkü yavaşlatacağı düşünüldüğü zaman networkü bölmenin gerekliliği ortaya çıkar. Bölümler arasına yine bridge'ler konulur.

Beşincisi ise güvenilirlik sorunudur. Bir LAN üzerindeki hatalı bir düğüm bütün hattı karıştırabilir. Bu yüzden önemli düğüm noktaları için aralara bridge'ler yerleştirilir. Zaten bridge'lerin repeater'lerden farkı seçici olarak neyi ilerletecekleri ve neyi ilerletmeyeceklerinin tanımlanabilmesidir.

Son olarak bridge'ler bir organizasyondaki güvenlik sorunlarını çözebilir. Normal durumda networkler her türlü dosyanın herkesin erişiminde olmasını sağlar. Bridge'ler sayesinde istenen seviyede güvenlik katmanları yaratılabilir.

Bridge'lerin çalışması ise aşağıda verilmiş olan şekilde incelenebilir. Şekil 2-3 de basit bir çift yönlü bridge görülmektedir. Host A bir packet yollamak istediği zaman, packet LLC ara katmanına indirilir. Burada LLC header'ı alır. Buradan MAC ara katmanına iner ve 802.3 header'ı alır. Bu bilgi kablo üzerinden bridge'e gelir. Burada başlıklar değiştirildikten sonra Host B, paketi bozulmamış olarak alır. Burada dikkat edilecek nokta bir bridge'in içerisinin bir çok MAC ara katmanının varolduğu düşünülerek hazırlanması gerektiğidir.



Şekil 2-3

II.1.3 Gateways (Network Geçitleri)

Bridge'lerden farklı olarak gateway'ler network katmanında çalışırlar. Bu onlara daha çok esneklik kazandırdığı halde aynı zamanda yavaşlatmaktadır. Doğal sonuç olarak gateway'ler WAN'lar arası kullanılmaktadır ki, bunlar arasındaki transfer oranı 10000 paket/saniye mertebelerindedir. Bu seviye bir WAN için normal olduğu halde LAN için çok düşüktür. İki tür gateway vardır. Birincisi connection-oriented, ikincisi connectionless'dır.

II.1.3.1 Connection-Oriented Gateway'ler

Buna virtual circuit (sanal devre) adı verilir. Buradaki fark transferin network katmanında olmasındadır. Bundan başka farklar da vardır. Önemli bir özellik ise şudur. Eğer bir gateway bir organizasyona ait ise bu cihazın nerede duracağının pek bir önemi yoktur. Fakat farklı ülkelerdeki iki organizasyon arasındaki bir gateway için bu söz konusu olamaz. Bunu çözmek için iki farklı half-gateway (yarım ağ geçitleri) denilen cihazlar üretilmiştir. Bunlar bir gateway'in ortadan ikiye ayrılıp, ayrılma noktasından birbirine bir kablo aracılığıyla bağlanmasıyla oluşurlar. Böylece her organizasyon kendi parçasına sahip olur ve bu sorun ortadan kalkar.

Half-gateway'ler kablolar üzerinden CCITT'nin X.75 protokolü aracalığıyla anlaşırlar. Bir networkteki kaynak ve bir başka networkteki varış arasındaki bağlantı beş ara parçadan oluşur. Bunların hepsi birer virtual circuit'dir. Bu modelin temel özelliği kaynaktan hedefe kadar her aşamada bir virtual circuit'in kurulmasıdır. Her gateway kendi üzerinden geçen virtual circuit'leri bir tablo halinde tutar, nereden geldiğini ve nereye gittiğini belirtir. Bu modelde gateway'ler arası X.25 protokolü kullanılmakla beraber her network içinde kendi protokolü kullanılabilir.

II.1.3.2 Connectionless Gateway'ler

Networklerin birbirlerine bağlanması konusunda CCITT'nin diğer bir alternatifi datagram modelidir. Bu modelde yapılan iş transport katmanının verileri ara katmanlara yollaması ve en iyisini beklemesi gibi yorumlanabilir. Bir virtual circuit mantığı yoktur. Bu yüzden bir networkten çıkan bir paket bir başka networke giderken çok farklı yollardan gidebilir. Bu da şu sonuca varır ki, paketler tamemen hedefe ulaşsa bile yollandığı sırada ulaşmayabilir.

Datagram'ların maksimum bir uzunluğu vardır. Eğer bir paket maksimum uzunluktan fazlaysa transport katmanı paketin boyunu paketi parçalama yöntemiyle kısaltır. Networkler arasında hareket edenler bu datagram'lardır. Ancak hedefe ulaşan bir datagram'ın başındaki header bilgileri kaldırılır ve orijinal mesaj elde edilir.

Her network yollanabilecek packet boyu konusunda kısıtlamalara sahiptir. Bu kısıtlamaları yaratan sebeplerden bazıları aşağıdadır:

- Donanım
- İşletim Sistemi
- Protokoller
- Ulusal ve uluslararası bazı standartlara uyma zorunlulukları
- Yeniden iletişime sebep olacak hata sayısını azaltmak
- Bir paketin hattı çok uzun süre meşgul etmesini engellemek

Bu packetlerin bazılarının standart boyları şunlardır:

- HDLC : Prensipte sonsuz
- 802.4 : 65,528 bits
- X.25 : 32,768 bits
- ARPA PRN : 2032 bits
- ARPANET : 1008 bits
- ALOHANET : 640 bits

Asıl sorun değişik standartlar kullanan networkler arası iletişimde değil de değişik uzunlukta paketler kullanan networklerde çıkmaktadır. Zira büyük bir paket ancak ufak bir paket iletebilen bir networke geldiği zaman ne yapılması gerektiği sorusu önem kazanır. Buna bulunan çözümlerden bir tanesi bu paketi çok özel bir yönlendirme ile bu tip networklere uğratmamaktır. Fakat bu çözüm aslında bir çözüm sayılmaz. Bunun gerçek çözümü ise bu paketi fragment'lere (parçalara) ayırmaktır. Fakat bu çözüm beraberinde bir sorun daha getirmektedir. Sorun parçalama işleminde değil, bu defa bu parçaları çıkışta yeniden bir bütün haline getirmekte çıkmaktadır.

III.1 IP (Internet Protocol)

IP, packet-switched (paket anahtarlamalı) bilgisayar ağlarını birbirine bağlamak için tasarlanmıştır. IP, datagram adı verilen data bloklarının, sabit uzunlukta adreslere sahip hostlar arasında taşınmasını sağlar. IP aynı zamanda uzun datagramların fragmante edilmesi (daha küçük parçalara ayrılması) ve fragmante edilen bu parçaların tekrar birleştirilmesi görevini de yerine getirir.

III.1.1 IP' nin Amacı

IP nin tek amacı gönderen ile alıcı arasında bit'lerden oluşan paketleri sıralamadır (sequencing). IP diğer host-to-host haberleşmede alışılmış olan mekanizmaların hiçbirini kullanmaz.

III.1.2 IP' nin İşlevi

Internet protokulünün iki temel işlevi vardır.

- Adresleme
- Fragmantasyon

Internet modülleri, internet header (başlık) da bulunan adreslerden yararlanarak, internet datagramlarını gönderen ile alıcı arasında taşırlar. Bu taşıma işlemi sırasında yol seçme işlemi routing olarak adlandırılır. Yine internet headerda bulunan alanlardan (fields) yararlanarak küçük paket boyutuna sahip networklerde fragmantasyon ve birleştirme işlemi gerçekleştirilir.

Internet protokolü her datagramı bağımsız bir birim olarak ele alır ve verdiği servislerde dört temel mekanizma kullanır. Bunlar:

- Type of Service (servis tipi),
- Time to Live (yaşama süresi),
- Options (seçenekler),
- Header Checksum (başlık bilgisi sağlama toplamı)

olarak sıralanabilir. Bu dört temel mekanizmanın amaçları ve görevleri ise şu şekilde açıklanabilir.

Type of Service:

Bilgi aktarımı sırasında internet modülünden istenilen servisin kalitesini belirlemek için kullanılan parametrelerdir.

Time to Live:

Internet datagramlarının network üzerinde kalma süresinin üst sınırını belirleyen bir değerdir. Datagramı yollayan tarafından belirlenen bu değer yol boyunca işlendiği her noktada bir azaltılır. Datagram, bu değer sıfır olduğunda halen varması gereken noktaya ulaşamamışsa silinir. Bu değer, bir datagramın kendi kendini yok etme süresi olarak da adlandırılabilir.

Options:

Bazı özel durumlarda kontrol fonksiyonlarını yerine getirmek amacıyla kullanılırlar.

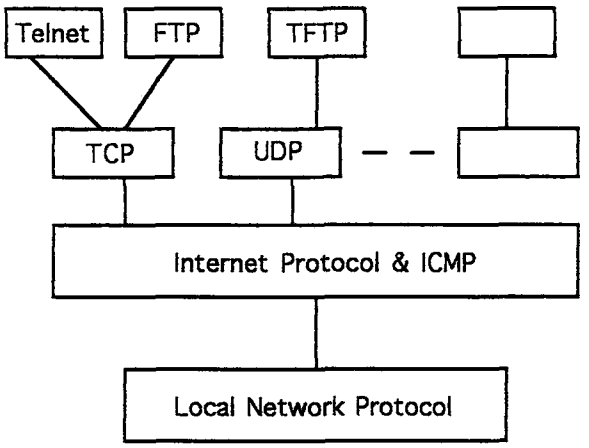
Header Checksum:

Internet datagramlarının doğru iletilip iletilmediğini anlamak için kullanılır. Eğer datagram header'i herhangi bir nedenden dolayı bir bozulmaya uğramış ise, header checksum sayesinde bu hatalı durum belirlenir ve hatalı olan datagram göz ardı edilir.

Internet protokolü güvenilir bir haberleşme sağlamaz. Acknowledgement (alındı bildirimi) , error detection (data için hata kontrolü), flow control (akış kontrolü), retransmission (tekrar yollama) özellikleri yoktur.

Karşılaşılan hatalar, Internet protokol modülü içindeki Internet Control Message Protocol (ICMP) modülü tarafından rapor edilir.

III.1.3 IP'nin diğer protokoller ile bağlantısı



Şekil 3-1

Internet protokolü bir yandan üst seviye host-to-host protokoller, diğer taraftan local network (yerel network) protokolleri ile bağlantılıdır. Local network, bir bina içinde oluşturulmuş basit bir yapı olabileceği gibi ARPANET gibi çok geniş bir yapıyı da kapsayabilir.

III.1.4 Internet'in çalışma şekli

Internetin nasıl çalıştığını daha rahat anlatabilmek amacıyla şu senaryoyu inceleyelim. Bir uygulama programından diğer bir uygulama programına yollanan datagram bir gateway (network geçidi) üzerinden geçmek zorunda olsun.

- Yollama işlemini gerçekleştirecek olan uygulama programı gönderilecek datayı hazırlar ve kendi internet modülünü bu datayı, datagram olarak yollamak üzere çağırır. Bu işlemin yapılabilmesi için varış adresinin ve diğer parametrelerin de internet modülüne aktarılması gereklidir.

- Bilgileri uygulama programından alan internet modülü, datagram için header bilgisini hazırlar ve datayı headerın sonuna ekler. Daha sonra, Internet modülü, verilen internet adresinin hangi local network üzerinde olduğunu tespit eder. Bu örnek için tespit edilen adres, gateway adresi olacaktır. Belirlenen local network adresine datagram local network interface (yerel network arabirimi) kullanılarak yollanır.

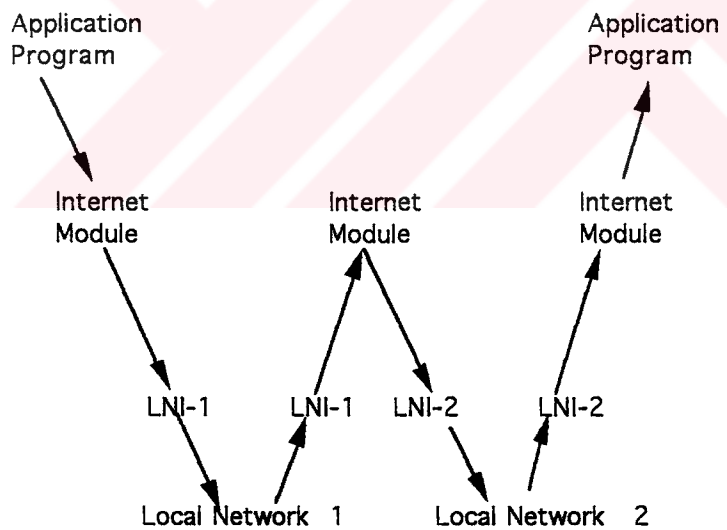
- Local network interface, kendisine aktarılan datagrama local network header (yerel network başlığı) ekleyerek oluşturduğu paketi local network üzerinden yollar.

- Paket, local network headerda belirtilen gatewaye ulaşınca, gateway local network interface header bilgisini ayırır ve datagramı kendi internet modülüne aktarır. Internet modülü, internet adresine bakarak gelen paketin diğer network üzerinde bulunan bir hosta gideceğini anlar ve bu host için local network adresini belirler. Local network interface ile datagramın yollanmasını sağlar.

- Local network interface, local network header yaratarak datagramı bunun arkasına ekler ve alıcısına yollar.

- Varış noktasına ulaşan datagram, local network interface tarafından local network headerdan ayrılarak internet modülüne aktarılır.

- Varış noktasındaki internet modülü gelen datagramın bir uygulama programı için olduğunu anlayınca datagramın içindeki datayı ve bağlantılı parametreleri uygulama programına aktarır.



Şekil 3-2

III.1.5 Adresleme

Internet üzerinde datagramlar birbirleriyle bağlantılı networkler üzerinden geçerek varış noktasına kadar ulaşırlar. Bu yolculuk sırasında internet üzerindeki hostların internet modüllerinden geçmek zorundadırlar. Her internet modülü datagramın nereye gideceğini anlamak için adres bilgisine ihtiyaç duyar. İşte bu nedenden ötürü adresleme internet protokolü için çok önemlidir. Internet protokolünde sıkça kullanılan bazı terimlerin tam olarak anlaşılmasında fayda vardır. Bu terimler,

- Name (isim):

  internet üzerindeki herhangi bir hostun senbolik adını,

- Address (adres):

  internet üzerindeki herhangi bir hostun sayısal adresini,

- Route (yol):

  istenilen hosta hangi yol üzerinden ulaşılacağını belirtmekte kullanılırlar.

İsimleri adreslere çevirmek üst seviye protokollerin, internet adreslerinin local network adreslerine çevrilmesi internet protokolünün, local network adreslerinin yol bilgisine çevrilmesi ise daha alt seviye protokollerin, örneğin local network veya gateway protokollerinin, görevidir. Adres bilgisi sabit uzunlukta olup dört bytetan (otuziki bit) oluşur. Adres bilgisi network number (ağ numarası) ile başlar ve local adres ile sonlanır. Üç sınıf internet adresi vardır:

- A sınıfı:

  En anlamlı biti 0 olup, takip eden 7 bit network adresini, son 24 bit ise local adresi belirler.

- B sınıfı:

  En anlamlı iki biti 1-0 olup, takip eden 14 bit network adresini, son 16 bit local adresi belirler.

- C sınıfı:

  En anlamlı üç biti 1-1-0 olup, takip eden 21 bir network adresini, son 8 bit local adresi belirler.

Internet adreslerini, local network adresleri ile eşlerken oldukça dikkatli olunması gereklidir. Zira bir host, sanki birden fazla hostmuş gibi birden fazla internet adresine sahip olabilir. Ayrıca aynı hostun birden fazla fiziksel interface (arabirim) i de olabilir.

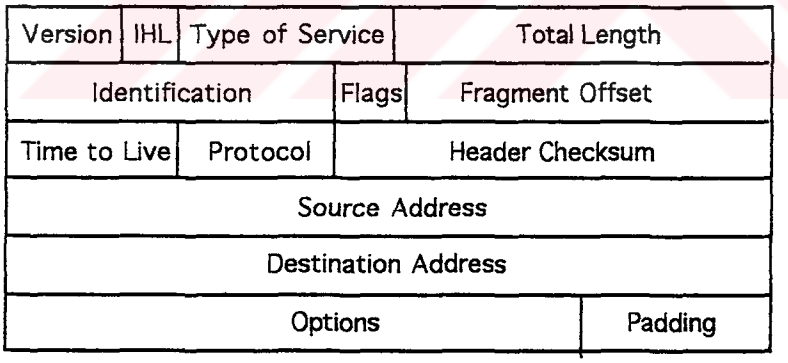
III.1.6 Fragmantasyon

Mesajlar, kaynaktan çıkıp hedeflerine ulaşana kadar, paket büyüklükleri datagramın boyundan küçük olan networklerden geçmek durumunda kalabilirler. Bu durumda datagramların geçtikleri networke uygun paket büyüklüğüne getirilmesi gerekmektedir. Bu olayı imkanlı kılmak amacı ile fragmantasyon mekanizması geliştirilmiştir.

Bazı datagramlar fragmante edilemez olarak işaretlenmiş olabilirler. Bu şekilde işaretli datagramlar, paket büyüklüğü datagramdan uzunluğundan küçük olan networklerden fragmante edilmeden geçemeyecekleri için ortadan kaldırılırlar. Fragmantasyon işlemi, internet protokol modülü açısından bakıldığında tamamen transparent (şeffaf) gerçekleşir.

Fragmantasyon sayesinde uzun bir datagram, biribirini takip eden uygun ve eşit büyüklüklerdeki parçalara ayrılır. Her parçaya ait bir identification field (kimlik alanı) vardır. Bu alan sayesinde aynı datagrama ait parçaları tekrar uygun sırada ve başka datagramların parçalarıyla karıştırmadan birleştirmek mümkün olmaktadır. Uzun bir datagramı fragmante ettiğimizde oluşan her parçanın başına orijinal datagramdaki internet header bilgisinin kopyalanması gerekmektedir.

III.1.7 Internet Header Formatı



Şekil 3-3

- Version :

(4 bit) Internet header formatını belirlemek için kullanılır.

- IHL :

(4 bit) Internet Header Length : Internet Header bilgisinin boyutunu gösterir. Bu 32 bitlik word'ler olarak ifade edilmektedir. Bu aynı zamanda datanın başladığı noktayı da göstermektedir. Dikkat edilmesi gereken nokta düzgün bir header bilgisi için bu deger en az 5 olmalıdır.

- Types of Service:

(8 bit) Bu alandaki bilgiler aşağıdaki tablo uyarınca kodlanmaktadır.

bit 0-2 111 - Network Control
110 - Internetwork control
101 - CRITIC/ECP
100 - Flash override
011 - Flash
010 - Immediate
001 - Priority
000 - Routine

bit 6-7 ileride kullanılmak üzere ayrılmış

Bu bilgiler datagrama internet üzerindeki yolculuğu sırasında nasıl davranılması gerektiğini berlirlerler.

- Total Length:

(16 bit) Datagramın toplam boyutunu belirlemek için kullanılır. Buna header ve data bilgilerinin tamamı dahildir ve octet olarak değerlendirilmelidir. 16 bit ile 65535 octet'lik bir datagram oluşturmak mümkündür. Ancak bu denli büyük datagramı alacak olan host'unda buna göre ayarlanmış olması gerekecektir. Pekçok host 576 octet alacak şekilde ayarlanmıştır. 576 değeri uygun büyüklükte data ve header bilgisi göz önüne alınarak seçilmiştir.

- Identification:

(16 bit) Fragmante edilen datagramların tekrar birleştirilmesine yardımcı olmak amacıyla yollan tarfından verilmiş numaralardır.

- Flag:

(3 bit) Fragmentler ile ilgili bilgileri içerir.

bit 0 her zaman 0 olmalıdır.

bit 1 (DF) 0 - may fragment

1 - don't fragment

bit 2 (MF) 0 - Last fragment

1 - More fragments

- Fragment Offset:

(13 bit) Bu alan fragmanın datagram içinde hangi noktadan itibaren başladığını gösterir. Fragment Offset 8 octet lik birimler ile ölçülür.

- Time to live:

(8 bit) Datagramın internet üzerinde kalabileceği en uzun süreyi belirler.

- Protocol:

(8 bit) Internet datagramının data kısmında kullanılacak bir sonraki seviye protokolü belirler.

- Header Checksum:

(16 bit) Header bilgisinin doğru olup olmadığını kontrol etmek üzere hesaplan bir degerdir.

- Source Address:

(32 bit) Kaynak adresi.

- Destination Address:

(32 bit) Varış adresi

- Options:

(degişken uzunlukta) IP modülleri tarafından değişik ihtiyaçları karşılamak üzere kullanılır.

- Padding:

(variable) Internet header'in uzunluğunu 32 bit sınırına tamamlamak için kullanılır.

III.2 ICMP (Internet Control Message Protocol)

IP (Internet protocol) birbirlerine bağlı networklerden oluşan bir sistem içinde host'lar arası datagram servisinde kullanılan bir protokoldür. Networkleri birbirlerine bağlayan cihazlara Gateway adı verilir. Bu cihazlar da kendi aralarında kontrol amacıyla ile haberleşirler. İşte bu haberleşmeyi imkanlı kılan protokole ICMP (Internet Control Message Protocol) adı verilir. ICMP, IP seviyesinin sağladığı servislerden yararlanan bir üst seviye protokolü gibi görünmesine rağmen, aslında IP protokulünün bölünmez bir parçasıdır.

Değişik durumlarda ICMP mesajları gönderilir. Örneğin, bir datagram gitmesi gereken yere ulaştırılamıyorsa veya gateway'de kendisine gelen datagramı alabilecek kadar buffer alanı kalmadıysa.

Bilindiği gibi IP güvenilir bir protokol olarak tasarlanmamıştır. ICMP ile gönderilen kontrol mesajlarının amacı da IP'ye güvenirlik sağlamak değil, haberleşme sırasında çıkabilecek problemlerden host'ların haberdar olmasını sağlamaktır. ICMP kullanılması durumunda bile hala daha, oluşabilecek problemlerden dolayı kontrol mesajları kaybolabilir veya datagramlar gidecekleri yerlere ulaştırılamayabilirler.

IP ve ICMP'nin daha üstünde çalışan protokoller kendi uygulayacakları mekanizmalar ile güvenirliği arttıran bir yapı oluşturmalıdırlar. ICMP mesajları genel olarak datagramların işlenmesi sırasında oluşan hataları rapor etmek için kullanılırlar. IP'nin güvenilir olmayan yapısı göz önüne alındığında ICMP mesajları, kontrol mesajlarının işlenmesi sırasında meydana gelen hatalar için kullanılmamalıdırlar.

III.2.1 Kontrol mesajlarının yapısı

ICMP mesajları temel IP header'ı kullanılarak gönderilirler. Bu sebeple aslında IP seviyesinde değerlendirildiklerinde ICMP mesajları da birer datagramdırlar. Datagramın bilgi kısmının ilk byte'ı ICMP kontrol mesajının tipni belirtmektedir. Bu alanın içeriği bilginin geri kalan kısmının nasıl değerlendirileceğini belirler.

ICMP mesajları içeren datagramlarının IP header değerleri:

- Version (Uyarlama numarası)

  Şu anda tanımlı olan değeri dörttür.

- IHL (Internet Başlık Boyutu)

  32 bit cinsinden Internet Header (Internet Başlığı) uzunluğu

- Type Of Service (Servis Tipi)

  Bu değer sıfır olmak zorundadır.

- Total Length (Toplam Uzunluk)

  Internet Header ve içindeki bilginin byte cinsinden toplam uzunluğu

- Time To Live (Yaşama Süresi)

  Saniye cinsinden yaşama süresi. Bu değer, datagram ulaşacağı noktaya varana kadar yol boyunca geçmesi ve işlenmesi gereken tüm host'larda her saniyede bir azaltılır.

- Protocol (Protokol)

  ICMP için bu değer bir olmak zorundadır.

- Header Checksum (Başlık Bilgisi Sağlama Toplamı)

  Internet Header'da yer alan tüm 16 bitlik alanların bire tümleyenlerinin toplamının bire tümlenmiş hali. Başlangıç değeri olarak sağlama toplamı sıfır kabul edilmelidir.

- Source Address (Kaynak Adresi)

  ICMP mesajını meydana getiren host'un adresi

- Destination Address (Varış Adresi)

  ICMP mesajının gitmesi gereken host'un adresi

III.2.2 ICMP mesaj tipleri

- Destination Unreachable Message (Varış Noktasına Erişilemiyor Mesajı)

Gateway veya host'un routing (yönlendirme) tablolarında datagramın gitmesi istenen adrese ait bir bilgi yoksa veya olduğu halde o yöne giden hatlar kapalı ise bu kontrol mesajı oluşturulur. Yine bu mesajın gönderilebileceği diğer bir durum da datagramın izin verilmediği halde bölünmesinin gerekmesidir. Datagram bu bölünme sebebiyle gitmesi gereken yere doğru ulaştırılamayacağı için göz ardı edilir ve bu kontrol mesajı ile durum datagramı göndermiş olan host'a rapor edilir.

- Time Exceeded Message (Zaman Doldu Mesajı)

Bu mesaj iki sebepten ötürü gönderilebilir. Birincisi 'Time To Live' alanının değerinin sıfıra ulaştığı durumdur. 'Time To Live' alanı sıfır olan bir datagram göz ardı edilir ve bu datagramı yollamış olan host'a bu durum, 'Time Exceeded Message' ile bildirilir. İkinci durum ise birden fazla parçadan oluşan datagramların tekrar birleştirilme işleminin belli bir zamam içinde yapılamamasıdır. Bu cins datagramlar da göz ardı edilirler.

- Parameter Problem Message (Parametre Problemi Mesajı)

Datagramların işlenmesi sırasında, tanımlı olmayan veya yanlış bir değere rastlandığı zaman gateway ve host bu hatayı datagramı gönderen gateway veya host'a bu kontrol mesajı ile bildirir ve datagramı göz ardı eder. Bu kontrol mesajı ancak ve ancak parametre alanlarında hata datagramın tamamını kullanılmaz hale getiriyorsa yollanmalıdır.

- Source Quench Message (Kaynak Yavaşlatma Mesajları)

Herhangi bir gateway veya host kendisine gelen datagramları buffer alanı yetmediği için alamıyor ve datagramları siliyorsa, bu kontrol mesajı ile datagramları yollayan gateway veya host'a bilgi gönderme hızını düşürmesi gerektiğini bildirmelidir. 'Source Quench' mesajını alan bir gateway veya host, mesajın geldiği hat için bilgi gönderme sıklığını azaltmalıdır. Bu işlem, 'Source Quench' mesajı geldikçe tekrarlanmalıdır. Belli bir süreden daha uzun, 'Source Quench' mesajı gelmezse, datagram yollayan gateway veya host bilgi gönderme sıklığını yavaş yavaş arttırmalıdır.

- Redirect Message (Yön Değiştirme Mesajı)

Herhangi bir gateway, yönlendirme tablolarına bakarak, kendisine gelen datagramın bir başka gateway üzerinden daha kısa bir yolla varış noktasına ulaştırılabileceğine karar verirse bu mesajı, datagramı gönderen host'a yollar, ama yine de kendisine gelmiş olan datagramı gitmesi gereken yere gönderir. Bu sayede datagramı yollamış olan host bundan sonra göndereceği datagramları diğer gateway'a yollayarak datagramların daha kısa bir yol üzerinden varış noktalarına erişmelerini sağlar.

- Echo or Echo Reply Message (Eko veya Eko Cevap Mesajı)

Echo mesajı ile beraber gelen data, Echo Reply Mesajı ile olduğu gibi geri gönderilmelidir. Bu iki mesaj sayesinde bir host veya gateway, ulaşmak istediği host veya gateway'in çalışır durumda olup olmadığını test edebilir.

- Timestamp or Timestamp Reply Message (Zaman Etiketi veya Zaman Etiketi Cevabı Mesajı)

Bu kontrol mesajları sayesinde bir datagramın ne zaman gönderildiği veya gönderilmek üzere gateway veya host'da ne süreyle beklediği belirtilir.

- Information Request or Information Reply Message (Bilgi İsteği veya Bilgi Cevabı Mesajı)

Bu kontrol mesajı sayesinde herhangi bir host hangi ağ üzerinde olduğunu belirleyebilir.

III.3 ARP (Address Resolution Protocol)

IP içinde broadcast (yayın) tipi haberleşme altyapısı kullanılması durumunda internet adreslerinin fiziksel hardware (donanım) adreslerine dönüştürülmesi işlemi ayrı bir önem taşır. Örneğin bir gateway, bağlı bulunduğu esas networkün internet adresini bildiği gibi geçiş imkanı sağladığı ve kendisine bağlı diğer networklerin de internet adreslerini bilir, ama bu networkler arası datagram transferi yapabilmesi için fiziksel interface'lerin hardware adreslerini de bilmelidir. Ayrıca internet adresleri kolay kolay değişmemekle beraber, fiziksel interface'ler bozulma veya diğer problemler sonucunda değiştirilmek zorunda kalabilirler. Bu şartlar altında da çalışabilen ve oluşabilecek değişikliklerden en az düzeyde etkilenip kendini adapte edebilen bir dönüştürme protokolüne ihtiyaç vardır. ARP (Adres Çözümleme Protokolü) bu problemi çözmek amacıyla geliştirilmiştir.

III.3.1 ARP'nin Genel Yapısı

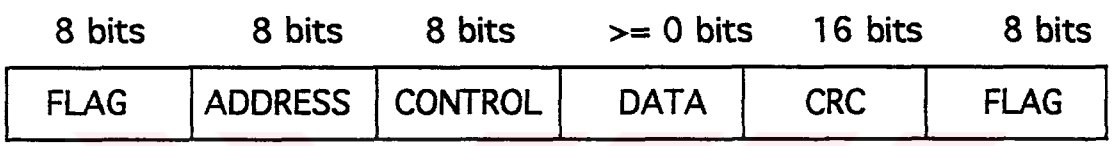
ARP'nin çalışma prensibi, en rahat, broadcast yapıda, ki bunun en temel örneği local area networklerdir, bir network üzerinde bulunan iki host'un haberleşmesi için gerekli adımlar incelenerek anlaşılabilir. 'A' isimli host, 'B' isimli hosta erişmek için bütün hostlara iletilecek bir broadcast paketi ile internet adresi bilinen 'B' isimli hostun hardware adresinin ne olduğunu soran bir paket yollar. Bu paket, broadcast tipinde olduğu için network üzerindeki tüm host'lar tarafından alınır ve sadece internet adresi, pakette belirtilen adresle aynı olan host cevap verir. Bu sayede 'A' isimli host artık 'B' isimli host'un hardware adresini öğrenmiş olacaktır. Bu sayede her iki host arasında haberleşme mümkün hale gelecektir. ARP çalışma prensibinin avantajlı tarafı hardware adresler dinamik olarak öğrenildikleri için network üzerinde meydana gelebilecek hardware değişiklikler çalışma prensibini etkilemeyecektir ve host'lar arası haberleşme devam edecektir. Bu açıdan bakıldığında ARP, üst seviye protokollerden alt seviyedeki fiziksel yapıyı saklayan ve böylece internet ve hardware adres belirlenmesinde kolaylık sağlayan bir alt seviye protokoldür.

ARP'ın çalışması üst seviyedeki protokolleri de etkilediği için hızlı ve esnek olmalıdır. Bu sebeple her seferinde bir host'un adresi arandığında bu sorgunun broadcast yöntemi ile yollanması hem network üzerinde yaratacağı yük hem de oluşturacağı gecikmeler açısından istenilen efektiflikten uzak olacaktır. Bir host'un hardware adresinin çok sık değişmeyeceği göz önüne alınacak olursa her seferinde bir sorgulama yapılması ile zaman kaybetmek yerine sorgu yapıldıktan sonra alınacak cevapların bir cache (ön) bellekde tutulması ve ileride yapılacak sorguların öncelikle cache bellekde aranması zaman.

kazandıracaktır. Cevabı cache bellekde bulunmayan adresler için yukarıda belirtilen broadcast tipinde mesaj gönderme yöntemi kullanılması sayesinde performans arttırılacaktır.

IV.1 HDLC (High Level Data Link Control)

HDLC (Yüksek Seviyeli Veri Bağlantısı Kontrolü) pek çok açıdan, IBM tarafından ortaya atılmış ve geliştirilmiş olan 'Synchronous Data Link Control' SDLC (Senkron Veri Bağlantısı Kontrolü) protokolüne benzemektedir. Hemen hemen aynı zamanlarda Amerikan Standartları Enstitüsü tarafından yönetilen paralel bir çalışma ile de 'Advanced Data Communication Control Procedure' ADDCP (İleri Veri Haberleşmesi Kontrol Yöntemi) protokolü meydana gelmiştir. Yapı olarak HDLC ve ADDCP birbirlerine çok yakındırlar. Aralarındaki temel fark, HDLC protokolünün ISO (International Standarts Organization), yani Uluslararası Standartlar Organizasyonu, ADDCP protokolünün ise Amerikan Standartları Enstitüsü tarafından belirlenmiş olmasıdır. CCITT X.25 protokulü, HDLC protokolünün bir alt kümesi olan 'Link Access Procedure Balanced' LABP (Dengeli Hat Erişim Yönetimi) yapısını kullanmaktadır.



Şekil 4-1

HDLC protokolünün standart frame (çerçeve) formatı şekil 4-1 de görülmektedir. Sekiz bitten oluşan flag (bayrak) bilgisi frame'in hem başında hem de sonunda yer alarak senkronizasyonun ve frame başlangıç ve bitişlerinin belirlenmesini sağlamaktadır. Flag bilgisi olarak binary (ikili) sayı düzeninde '01111110' değeri kullanılmaktadır. Başlangıç ve bitişteki flag bilgisi sayesinde frame'in içeriği konusunda diğer protokollerde karşılaşılan bazı sınırlamalar ortadan kalkmıştır.

Bir HDLC frame'in de temel ikinci alan ise address (adres) alanıdır. Bu alan bir byte, yani sekiz bit, uzunluğunda olup, bilginin hangi adresli station (istasyon) a gideceğini belirler.

Daha sonra gelen kontrol alanı ise frame'in amaç ve fonksiyonunu belirlemek için kullanılır.

Temel olarak üç frame çeşidi tanımlanmıştır. Herbirinin farklı bir kontrol alanı formatı vardır. Information (Informasyon) frame'ler bilgi taşıma amacıyla kullanılmaktadırlar. Supervisory (yönetici) frame'ler temel bağlantı fonksiyonlarını içermektedirler. Unnumbered (numarasız) frame'ler ise temel bağlantı fonksiyonlarına yardımcı amaçla kullanılırlar.

Poll/Final (Sorgulama/Sonuç) ya da kısaca P/F biti, primary station (birincil istasyon) tarafından, secondary station'dan (ikincil istasyon) cevap almak amacıyla kullanılır. Her frame'de P/F bitinin set edilmiş olmasına gerek yoktur. Birbirine bağlı bilgiler, birden fazla frame olarak gönderilecekse son frame içinde P/F bitini set etmek yeterli olacaktır. Fakat primary station, secondary station'ın durumunu öğrenmek veya hala daha çalışır vaziyette olup olmadığını belirlemek amacıyla supervisory ve unnumbered frame'lerde özellikle P/F bitini kullanabilir.

Information frame içinde bulunan N(S) ve N(R) alanları, hem akış hem de hata kontrolü yapılması amacıyla tanımlanmış alanlardır. Bilgi gönderen station, frame'leri sıfırdan başlamak üzere, 8 modülünü taban kabul ederek numaralandırır ve bu numarayı N(S) alanını kullanarak karşı taraftaki station'a bildirir. Karşı taraftaki station aldığı frame'in N(S) alanını kendindeki N(R) değeri ile karşılaştırırak, frame'in doğru sırada gelip gelmediğini kontrol eder. Eğer dogru ise N(R) değerini kendi yollayacağı bir frame içine koyarak karşı tarafa aktarır. Böylece N(S) numarası ile yollanmış olan frame onaylanmış olur. Bu cins onaya piggybacked acknowlegdement ismi verilir. Onaylama işlemi ayrıca supervisory frame'lerdeki N(R) alanından da yararlanılarak yapılabilir. Bu yöntemin sağladığı temel üç fonksiyon vardır.

- Flow Control (Akış Kontrolü)

Herhangi bir station yedi adet frame gönderdikten sonra, ilk gönderdiği frame için bir onay almadığı sürece yeni frame gönderemez.

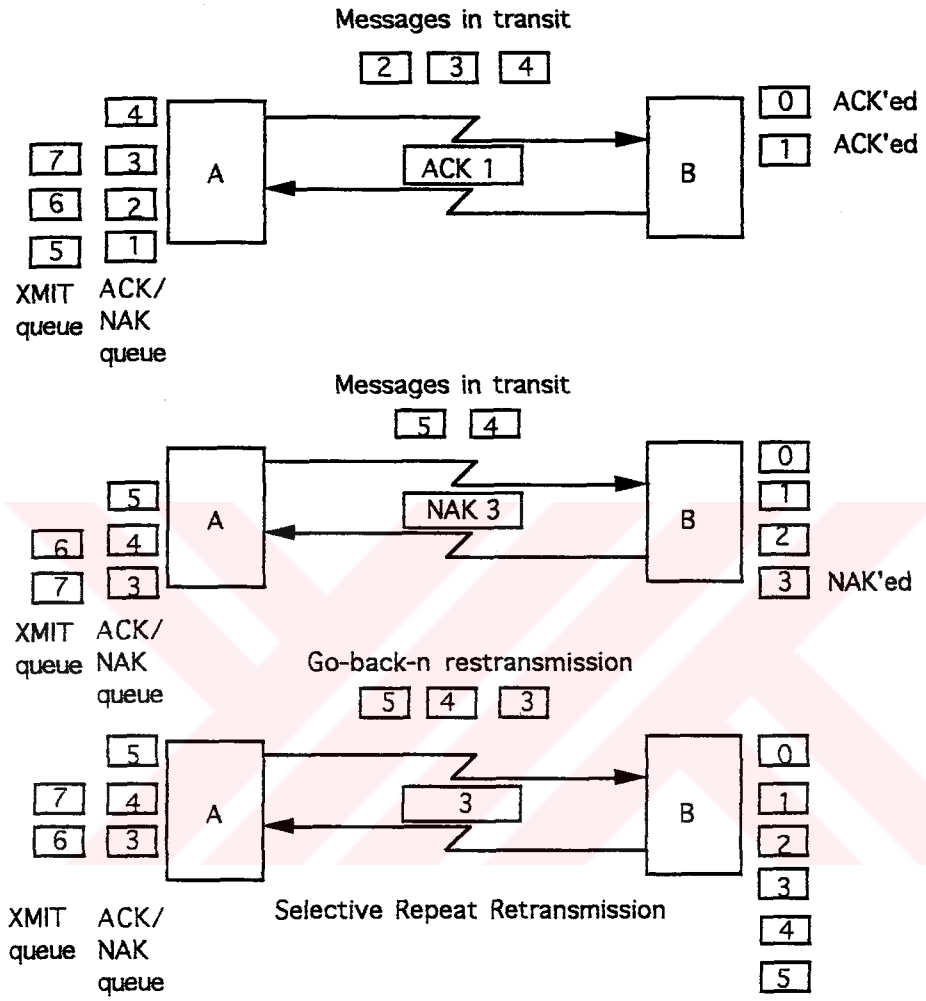
- Error Control (Hata Kontrolü)

Hatalı bir frame alındığı zaman, supervisory frame ile 'NAK' (negatif onay) gönderilerek hangi frame'in hatalı olduğu belirtilebilir. Hatalı frame durumunda, hatanın düzeltilmesi için iki durum söz konusudur. Birincisi 'Go back N' (N adet geriye git) yöntemidir ki, bu yöntemde en son doğru alınan frame'den itibaren tüm frame'ler bir kez daha gönderilirler. Diğer yöntem ise 'Selective Repeat' (Seçici Tekrarlama) yöntemidir. Bu yöntemde ise sadece hatalı frame tekrar yollanır.

- Pipelining

Bu yöntem sayesinde özellikle uydu hatlarındaki gecikme göz önüne alınacak olursa birden fazla frame iletim durumunda olacağından, hattın taşıma kapasitesinden çok daha iyi yararlanılmış olacaktır.

N(S)/N(R) yöntemine sliding window (kayan pencere) protokolü adı da verilmektedir, çünkü bilgi gönderen station hem gönderdiği hem de onay aldığı frame'lere ait ilerleyen bir window (pencere) tutmaktadır. Bu olay şekil 4-2 de gösterilmektedir.



Şekil 4-2

HDLC protokolünde dört adet supervisory frame mevcuttur, bunlar:

- Receive Ready RR (Almaya Hazır):

Bu frame, N(R)-1 e kadar olan frame'lerin düzgün bir şekilde alınmış olduğunu belirtmek amacıyla kullanılır.

- Receive Not Ready RNR (Almaya Hazır Değil):

Frame alınmasını engelleyen geçiçi bir meşguliyet olduğunu, mesela buffer alanının yeterli olmadığını, karşı tarafa aktarmak amacıyla kullanılır.

- Reject REJ (Geri Çevirme):

N(R) numaralı frame'in hatalı alındığını ve hem N(R) hem de N(R) dan sonra gelen frame'lerin tekrar gönderilmesi gerektiğini belirtir.

- Selective Reject SREJ (Seçici Geri Çevirme):

Sadece N(R) numaralı frame'in tekrar gönderilmesini ister.

Temel unnumbered frame'ler ise şu şekildedir:

- Set Asynchronous Balanced Mode SABM (Asenkron Dengeli Moda Geç):

Station'lar arası bilgi transferinin olabilmesi için öncelikle SABM komutunun gönderilmiş ve cevabının alınmış olması gereklidir. Bu komutu alan station N(S) ve N(R) değerlerini sıfırlamalıdır ve cevap olarak 'Unnumbered Acknowledgement' UA (Numarasız Onay) yollamalıdır.

- Disconnect DISC (Bağlantıyı Kes):

Primary ve secondary station arasındaki haberleşmenin ve daha önce SABM ile belirlenmiş olan çalışma modunun sonlandırılmasını sağlar. Cevap olarak UA gönderilmelidir.

- Unnumbered Acknowledgement UA (Numarasız Onay):

Bu frame unnumbered frame'lerin onaylanması amacıyla kullanılmaktadır.

- Disconnect Mode DM (Bağlantı Kesilmiş Durumda):

DM aracılığıyla herhangi bir station karşısındaki station'la mantıksal olarak bağlı olmadığını belirtir. DISC komutunun gelmesinden ve bu komuta cevap olarak UA gönderilmesinden sonra, station mantıksal olarak karşısındaki station'dan ayrılmış durumdadır ve SABM komutu gelene kadar, alacağı tüm unnumbered frame'lere DM ile cevap vermelidir.

- Command Reject CMDR; Frame Reject FRMR (Komut Geri Çevrilmesi; Çerçeve Geri Çevrilmesi):

CMDR veya FRMR cevabı karşı tarafa aynı frame'in bir kez daha gönderilmesiyle düzeltilemeyecek bir hatanın oluştuğunu belirtmek amacıyla kullanılır. Bu hatalar şu şekilde sıralanabilir:

* Hatalı bir komut veya cevabın alınması
* Daha önce belirlenmiş olan değerden daha uzun information frame alınması
* Hatalı N(R) değerinin alınması
* Hatalı uzunlukta supervisory veya unnumbered frame alınması

HDLC protokolünde üç adet çalışma şekli belirlenmiştir:

- Normal Response Mode NRM (Normal Cevap Modu):

Bu çalışma biçimi merkezi kontrol yöntemlerinin uygulandığı ortamlarda kullanılmaktadır. Bir adet primary station, bir veya daha fazla secondary station'a sırayla polling (sorgulama) yöntemiyle önderecekleri bilgi olup olmadığını sorar. Bu işlem sırasında gönderecek bilgisi olan secondary station'lar cevap verirler. Secondary station'lara primary station'dan herhangi bir sorgulama gelmediği sürece bilgi gönderme izni verilmez.

- Asynchronous Response Mode (ARM) (Asenkron Cevap Modu):

NRM yöntemine oldukça benzer ama aradaki temel fark, secondary station'ın bilgi göndermek için primary station'dan izin alması gerekliliğinin olmamasıdır.

- Asynchronous Balanced Mode (ABM) (Asenkron Dengeli Mod):

Bu yöntem, ancak point-to-point (noktadan noktaya) bağlantı yönteminde kullanılabilen bir yapıya sahiptir. Her iki uçtaki station'lar aynı özelliklere ve yeteneklere sahiptirler. Yani her ikisi de hem primary hem de secondary station'ın özelliklerini içerirler. CCITT X.25 protokolü için bağlantı seviyesinin temelini oluşturan yöntemdir.

Şekil 4-3 toplu olarak, information frame, supervisory frame ve unnumbered frame tiplerini, bunların yapılarını tablo halinde göstermektedir.

Control Field Structure

	1	2	3	4	5	6	7	8
Information	0	N(S)			P/F	N(R)		
Supervisory	1	0	TYPE		P/F	N(R)		
Unnumbered	1	1	TYPE		P/F	MODIFIER		

Şekil 4-3

IV.2 X.25

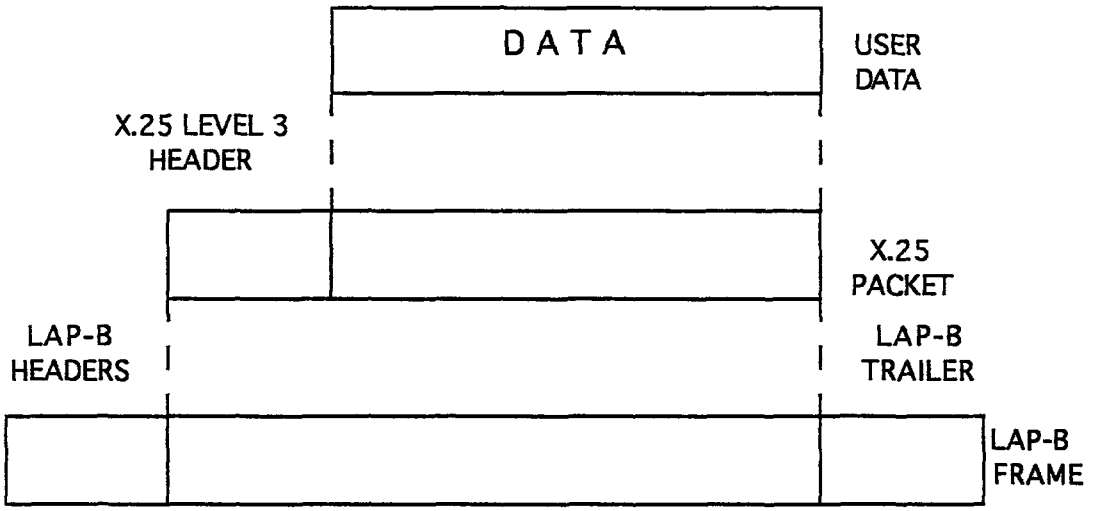
X.25 standartı, ilk defa 1976 yılında ortaya atılmış daha sonra 1980, 1984 ve1988 yıllarında tekrar gözden geçirilmiştir. Bu standart, bir host ile packet switched yapıda çalışan bir network arasındaki bağlantı kurallarını ortaya koymaktadır. X.25 standartı temel olarak üç adet protokol seviyesinden oluşmaktadır.

- Physical level (fiziksel seviye)
- Link level (bağlantı seviyesi)
- Packet level (paket seviyesi)

Bu en altta yer alan üç seviye, OSI network modelinde yer alan alttan üç seviyeye denk düşmektedir. Fiziksel seviye bir station, örneğin bir bilgisayar veya terminal, ile packet switching node (paket anahtarlama noktası) arasındaki fiziksel bağlantıların nasıl olması gerektiğini belirtmektedir. Bu seviyede en yaygın olarak kullanılan protokoller X.21 ve RS-232-C olarak belirtilebilir. Bağlantı seviyesi ise, fiziksel seviye üzerinden bilgilerin, frame'ler halinde güvenilir bir şekilde aktarılması ile ilgili kuralları ve tanımları içermektedir. Bağlantı seviyesi standartı olarak LAPB kullanılmaktadır. Paket seviyesi ise temel olarak virtual circuit (sanal devre) hizmeti sağlamaktadır.

Şekil 4-4 de X.25'in üç seviyesi arasındaki bağlantılar gösterilmiştir. Gönderilmek istenen bilgi, X.25 paket seviyesine gelir. Bu seviye gelen bilgiye kontrol amaçlı gerekli eklemeleri yaptıktan sonra oluşan paketi bir alt seviyeye, yani bağlantı seviyesine aktarır. Bağlantı seviyesi ise kendisine gelen paketin önüne ve arkasına, pakeetin varacağı yerdeki bağlant seviyesinin paketi doğru değerlendirmesini sağlayacak eklemeleri yapar ve son olarak fiziksel seviye bu bilgiyi frame olarak gönderir.

X.25 standartının paket seviyesi çalışma prensiplerinin daha rahat anlaşılabilmesi için, bu standartın network içi çalışma yöntemleri ve dışarıya, yani networke bağlı kullanıcılara verdiği servisler ve bunlar arasındaki bağlantılar incelenmelidir.



Şekil 4-4

IV.2.1 X.25 Network İçi Çalışma Ve Kullanıcıya Sunulan Servis Çeşitleri

Packet switched yapısıyla çalışan networkleri tanımlayan en önemli özellik, datagram yapısında mı yoksa virtual circuit yapısında mı çalıştıklarıdır. Bu iki karakteristiğin packet switched networkleri nasıl etkilediği şekil 4-5a ve şekil 4-5b de gösterilmiştir. Bir station ile herhangi bir network noktası arasında connection-oriented (bağlantıya yönelik) veya connectionless (bağlantıdan bağımsız) hizmet verilebilir. Connection-oriented hizmette, bağlantı kurmak isteyen station, bir call request (çağrı isteği) sayesinde karşıdaki station ile logical connection (mantıksal bağlantı) kurmaya calışır. Bu girişim başarıyla sonuçlanırsa iki station arasında paket alışverişi başlar ve gidip gelen paketler belli bir sırayla numarandırılırlar. Diğer bir özellik de, bu yöntemde paketlerin karşı tarafa gönderildikleri sıra ile varmalarıdır. Bu logical connection genelde virtual circuit olarak adlandırılır ve bu servise de external virtual-circuit service (dış sanal devre servisi) adı verilir. External virtual-circuit service yanısıra bir de internal virtual-circuit service (iç sanal devre servisi) mevcuttur. Connectionless serviste ise, network kendisine gelen paketleri aktarmak için iki station arasında daha önceden bir bağlantı kurulmasını gerektirmez, ama bu durumda da bazı paketler kaybolabilir veya gidecekleri yere gönderildikleri sıra ile ulaşmayabilirler. Bu tip çalışma şekline ise external datagram service (dış datagram servisi) adı verilir ve yapı olarak internal datagram service (iç datagram servisi) mantığından farklıdır. Bu temel yapılardan oluşan networkler şu kategorilere ayrılabilirler:

- External virtual circuit, internal virtual circuit:

Kullanıcı bir virtual circuit kurmak istediğinde network içinde bu işe ayrılmış özel bir yol oluşturulur ve bütün paketler bu yol üzerinden gider.

- External virtual circuit, internal datagram:

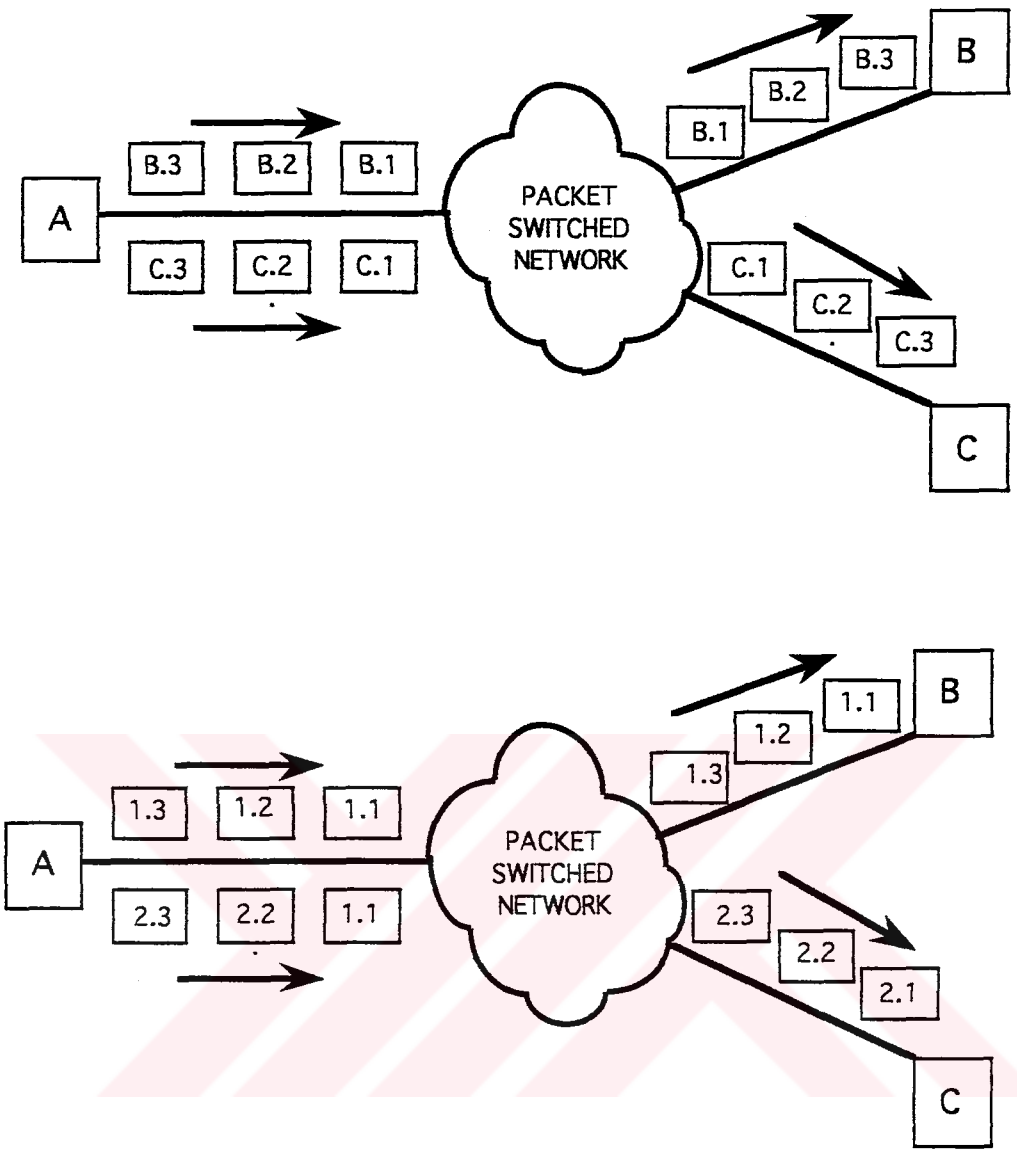
Network paketleri ayrı ayrı değerlendirir. Bu da aynı virtual circuit üzerinden gitmesi gereken iki paketin aslında network içinde farklı yollardan gidebileceği anlamına gelir. Network paketlerin doğru sıra ileteslim edilebilmesi için gerekli önlemleri almak zorundadır.

- External datagram, internal datagram:

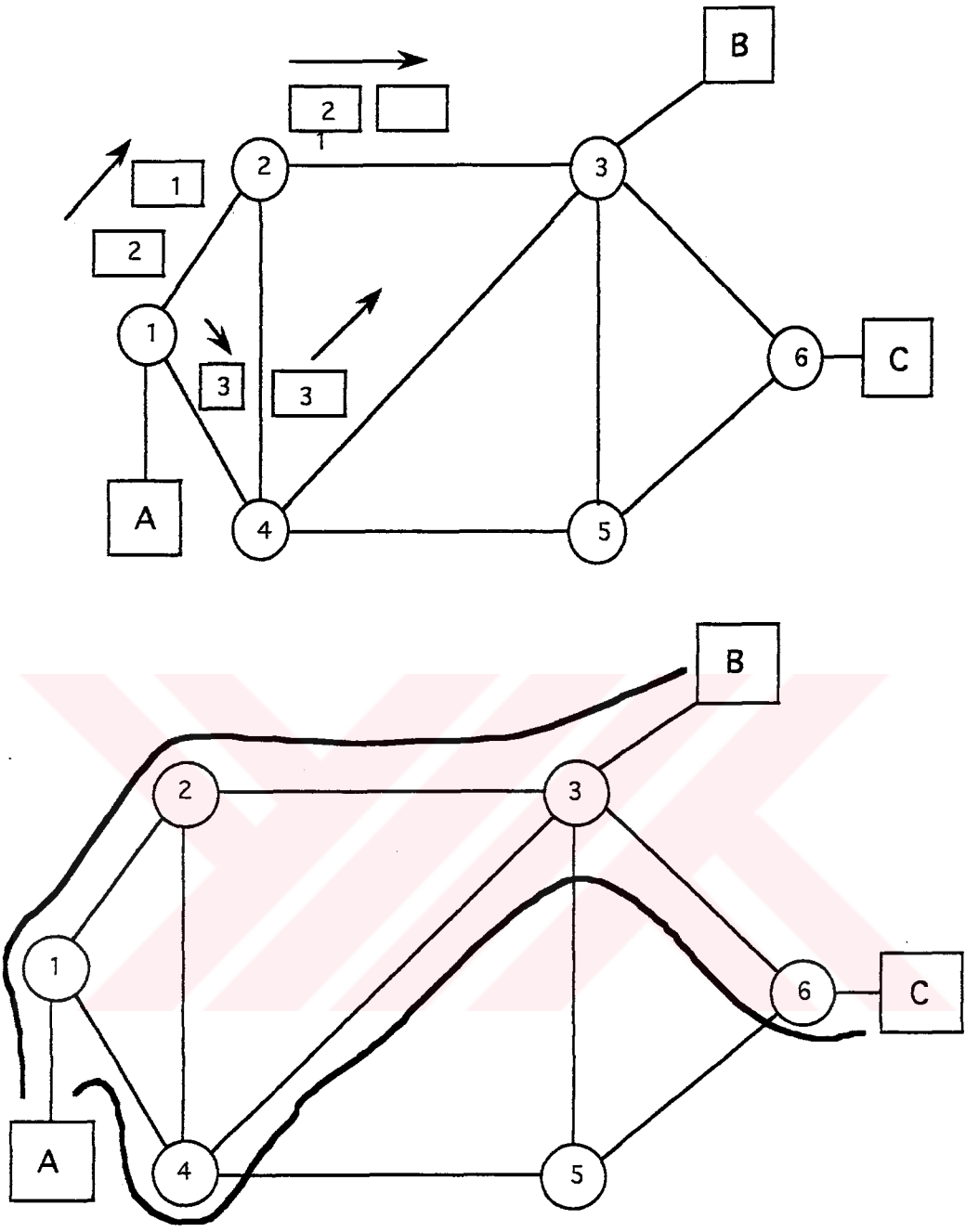
Kullanıcı açısından da, network açısından da her paket ayrı ayrı değerlendilir.

- External datagram, internal virtual circuit:

Bu kombinasyonun herhangi bir anlamı yoktur, çünkü birbirinden ayrı değerlendirilmesi gereken paketler için network içinde bu işe ayrılmış bir virtual circuit kurmak kaynakların boşa harcanması anlamına gelecektir.


A
B.3
B.2
B.1
C.3
C.2
C.1
PACKET
SWITCHED
NETWORK
B.3
B.2
B.1
B
C.1
C.2
C.3
C
A
1.3
1.2
1.1
2.3
2.2
1.1
PACKET
SWITCHED
NETWORK
1.1
1.2
1.3
B
2.3
2.2
2.1
C

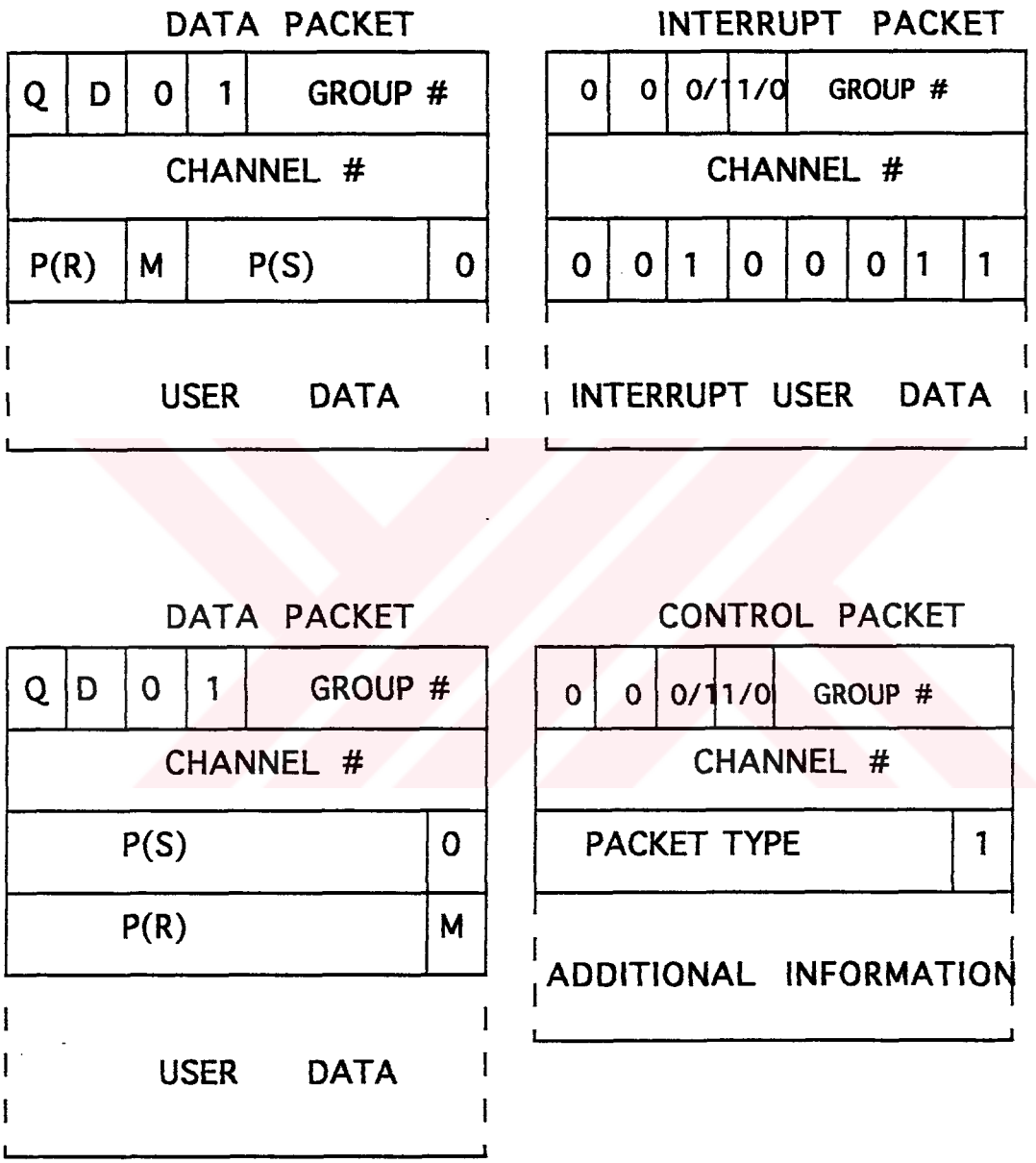
Şekil 4-5a



Şekil 4-5b

IV.2.2 X.25 Paket Seviyesi

X.25 paket seviyesinde bilgiler, paket adı verilen yapılarla taşınmaktadırlar. Pek çok değişik paket tipi olmasına rağmen, bunlar bir iki adet temel paketformatının basit değişikliklere uğramış halleridir. Değişik paket tipleri şekil 4-6 da gösterilmiştir.

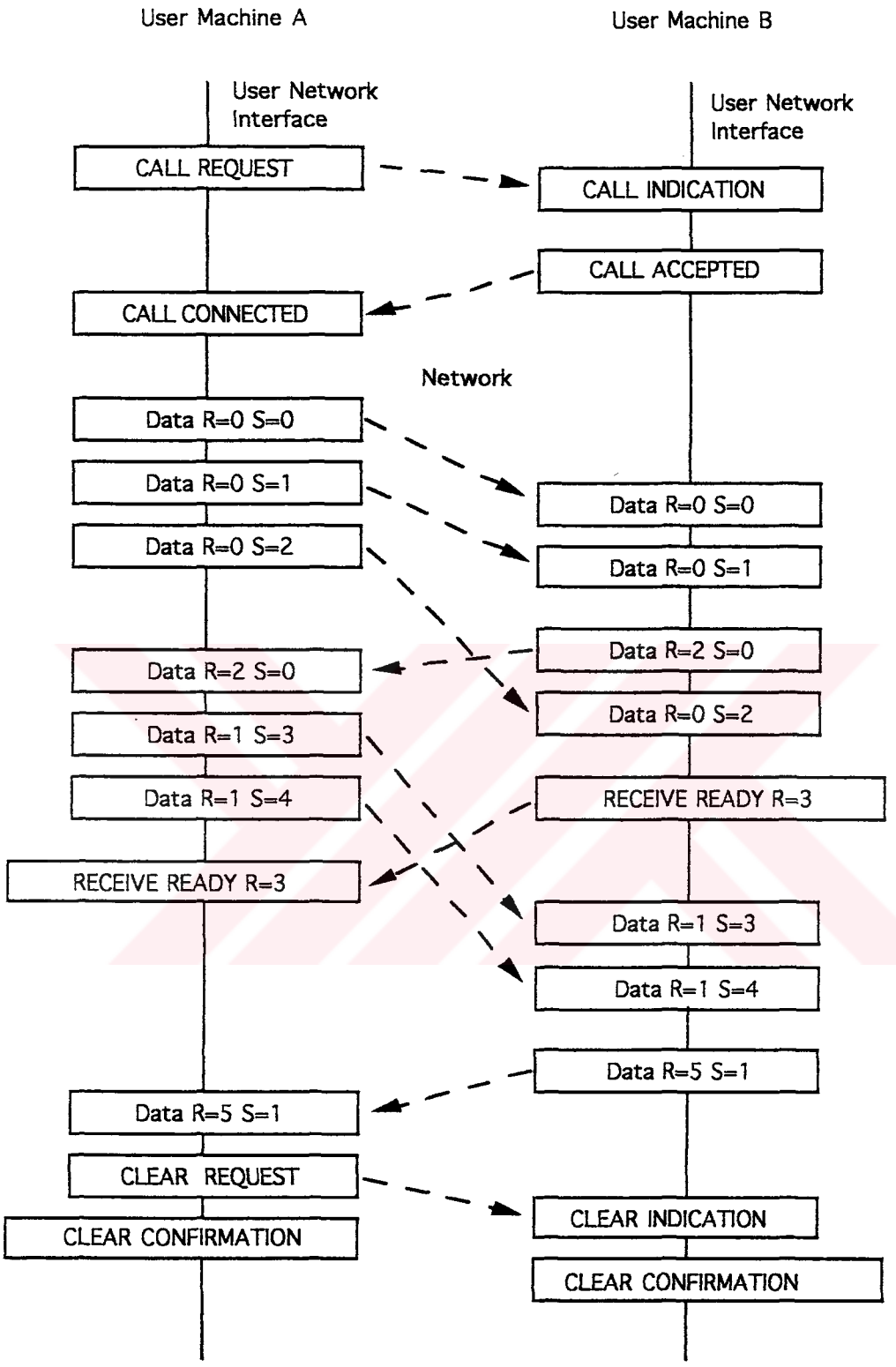


Şekil 4-6

X.25 standartı, kullanıcı cihazlarına, bilgisayar, terminal gibi, 'Data Terminal Equipment' DTE (Veri Terminal Cihazı) olarak , network'e bağlantı yapılmasını sağlayan cihazlara ise 'Data Circuit-Terminating Equipment' DCE (Veri Devresi Sonlandırma Cihazı) olarak isim vermektedir.

X.25 standartının sağladığı virtual circuit hizmetinin iki türü bulunmaktadır. Biri virtual call (sanal cağrı) , diğeri ise permanent virtual circuit (kalıcı sanal devre). Virtual call, dinamik olarak çalışma sırasında birbirine bağlanmak isteyen DTE'ler arasında, call setup (çağrı kurulması) ve call clearing (cağrı sonlandırılması) yöntemlerine uygun olarak kurulur veya sonlandırılır. Buna karşın permanent virtual circuit'ler network tarafından atanmış sürekliliği olan bağlantılardır ve call setup veya call clearing işlemlerine gerek duymazlar.

Şekil 4-7 de A ve B olarak isimlendirilmiş iki DTE arasında X.25 aracılığıyla haberleşme olabilmesi için her iki DTE'nin yerine getirmesi gereken işlemler ve bu işlemlerin sonucunda bilgi alışverişinin nasıl yapıldığı ve en son olarak da iki DTE'nin aralarındaki bağlantıyı nasıl sonlandırdıkları gösterilmiştir.


User Machine A
User Machine B
User Network Interface
User Network Interface
CALL REQUEST
CALL INDICATION
CALL ACCEPTED
CALL CONNECTED
Network
Data R=0 S=0
Data R=0 S=1
Data R=0 S=2
Data R=0 S=0
Data R=0 S=1
Data R=2 S=0
Data R=0 S=2
Data R=2 S=0
Data R=1 S=3
Data R=1 S=4
RECEIVE READY R=3
RECEIVE READY R=3
Data R=1 S=3
Data R=1 S=4
Data R=5 S=1
Data R=5 S=1
CLEAR REQUEST
CLEAR INDICATION
CLEAR CONFIRMATION
CLEAR CONFIRMATION

Şekil 4-7

IV.2.3 X.25 Paket Yapısı

Gönderilecek bilgiler, maximum uzunluğu belirlenmiş olan paketlere bölünürler ve her paketin başına 24 bit uzunluğunda bir header (başlık) eklenir. Böylece data paketi meydana getirilmiş olur. Header içinde 12 bit uzunluğunda virtual circuit number (sanal devre numarası) ve P(S) ile P(R) alanları mevcuttur.

Kullanıcı bilgisinin gönderilmesinin yanısıra, X.25 ,kontrol amacına yönelik, bağlantı kurulması ve sonladırılması gibi, paketler de yollayabilmelidir. Bu cins paketlere kontrol paketi adı verilir. Her kontrol paketinde bir virtual circuit number ve paket tipini belirten bir alan mevcuttur. Örnek vermek gerekirse call request (çağrı isteği) paketinde aşağıda belirtilen bilgiler mevcuttur:

- Aranan DTE adresi
- Arayan DTE adresi
- Facilities (istenen özellikler)

Maximum paket uzunluğu bulunulan X.25 networküne bağlı olarak, diğer bir değişle ülkeden ülkeye,değişmekle beraber minimum 128 byte maximum 4096 byte olabilir.

IV.2.4 Akış ve Hata Kontrolü

Akış ve hata kontrolü X.25' de, HDLC protokolünde olduğu gibi, gönderilen paketlere bir numara verilmesi yöntemiyle gerçekleştirilmiştir. Akış kontrolunün temelini yine sliding-window tekniği meydana getirmektedir. Paket aktarımı sırasında oluşabilecek hatalarda go-back-N yöntemi kullanılmaktadır. Her paketi açık bir şekilde belirleyebilmek için P(S) değeri mevcuttur ve bu değer 8 modülüne göre arttırılmaktadır. Bu sayede hiç bir zaman yedi taneden fazla paket, gönderilen ilk paket için onay gelmeden networke aktarılamaz. Aynı şekilde P(R) değeri de bir sonraki adımda alınması beklenen paketin numarasını belirtmektedir. Aynen HDLC protokolünde uygulandığı gibi X.25 de de birden fazla paket, gönderilecek tek bir P(R) değeri ile onaylanabilir. Bu olaya daha önce belirtildiği gibi piggbacked acknowledgement adı verilir.

IV.2.5 Sıfırlama ve Yeniden Başlama

X.25 hatalardan kurtulmak için iki temel yöntem kullanmaktadır. Reset (sıfırlama) virtual circuit'ı başlangıç koşullarına getirmek için kullanılır. Reset paketi geldiğinde, o virtual circuit'a ait olan P(S) ve P(R) değerleri sıfırlanır. Reset paketi, data paketi kaybolması, numaralandırma hatası meydana gelmesi veya network içinde oluşabilecek daha ciddi hatalar sonucunda hem DTE hem de DCE tarafından gönderilebilir. Daha ciddi durumlarda ise restart (yeniden başlama) paketi kullanılır. Bu paket, var olan tüm virtual circuit'lere reset paketi uygulanması ile eşdeğerdir.

IV.2.6 Interrupt (Kesme) Paketleri

Zaman zaman network içinde, diğer bilgilere göre önceliği olan bilgilerin gönderilmesi gereklidir. X.25, interrupt paketlerini bu amaç için kullanmaktadır. Bu paketler normal akış kontrol mekanizmalarının dışındadırlar ve bu sebeple P(S) veya P(R) değeri içermezler. Interrupt paketlerindeki kısıtlama ise paket içindeki data alanının 32 byte ile sınırlı olmasıdır. Herhangi bir virtual circuit üzerinde sadece bir adet onaylanmamış interrupt paketi olabilir.

V.1 IP Router (Yönlendirici) Uygulaması

V.1.1 Amaç

Bu proje, akademik ortamlarda kullanılmak üzere, çok özel hardware (donanım) gerektirmeyen ve olabildiğince programa yönelik yapıda olacak bir IP router tasarlanması düşüncesi sonucunda ortaya çıkmıştır. Bilgisayar dünyasında bulunan IP router'lar incelendiklerinde, bunların çoğu zaman akademik ortam için aslında gerekli olmayan pek çok ticari özelliğe sahip olmaları sonucu oldukça pahalı oldukları ortaya çıkmaktadır. Aslında sadece temel fonksiyonlara sahip bir yapıda çalışan ve bir veya iki farklı haberleşme ortamı arasında geçişi sağlarken sadece belli bir protokolü destekleyen router'lar akademik ortamlarda yeterli olmaktadır. Bu noktalar göz önünde bulundurularak Yıldız Teknik Üniversitesi, Elektrik Elektronik Fakültesi Bilgisayar Bilimleri ve Mühendisliği Bölümü bünyesinde bulunan IP protokolünü de destekleyen network'de kullanılmak üzere bu projenin gerçekleştirilmesine karar verilmiştir. Değişikliklere açık ve ileriye dönük bir yapıya sahip olması da planlan bu IP router daha sonraki lisans veya lisans üstü çalışmaları için de bir temel oluşturabilecektir.

V.1.2 Kullanılan Kaynaklar

IP router iki farklı haberleşme ortamını destekleyecek şekilde tasarlanmıştır. Bunlardan birincisi ethernet tipi local area network bağlantısı, diğeri ise X.25 standartı üzerinden mainframe (anabilgisayar) bağlatısıdır. IP router, Intel 80x86 serisi mikroişlemcileri temel alan PC (Kişisel Bilgisayar) ler üzerinde ve DOS (Disk Operating System) işletim sistemi kullanılarak geliştirilmiştir. Ethernet bağlantısı için bilgisayar piyasasında kolayca elde edilebilen NE2000 serisi ethernet kartı ve bu kartla beraber satılan software kullanılmıştır. Mainframe ile X.25 protokolü üzerinden bağlantıyı sağlamak üzere Bilgisayar Bilimleri ve Mühendisliği Bölümü hardware laboratuarında, AMD (Advanced Micro Devices) firması tarafından üretilen AMD85C30 entegresi kullanılarak geliştirilmiş olan SDLC/HDLC/BSC/Asynch protokollerini destekleyen IBM compatible AT-BUS uyumlu multiprotocol kartı kullanılmıştır. Multiprotocol kartı için gerekli yazılım ise proje kapsamında MASM 6.0 (Macro Assembler) derleyicisi kullanılarak assembler dilinde yazılmıştır. Bu yazılımın temel özelliği hem X.25 standartının bir alt seviyesi olan HDLC protokolü ile ilgili işlemleri yerine getirmek hem de IP router'in X.25 üzerinden bilgi alışverişi yapabilmesi için gerekli X.25 primitive'lerini sağlamaktır. Ethernet kısmı ile ilgilenen yazılımda olduğu gibi X.25 kısmının yazılımı da TSR (Terminate and Stay Resident) yöntemine uygun çalışmaktadır. Daha üst seviyede yer alan ve gerçek IP router fonksiyonlarını gerçekleştiren kısımlar ise

Turbo Pascal 6.0 derleyicisi kullanılarak Pascal programlama dilinde hazırlanmıştır. Bu birimler temel olarak, ethernet üzerinde internet adresleri ile hardware adresler arasında dönüşümü sağlayan ARP modülü, diğer hostlardan gelen kontrol mesajlarına cevap veren ve IP'nin temel parçalarından olan ICMP modülü ile iki bağlantı arasında bilgilerin gidiş gelişini sağlayan IP modülü olarak sıralanabilir.

V.2 IP Router için Oluşturulan Data Yapıları

V.2.1 X.25 Virtual Circuit (Sanal Devre) Kontrol Blokları

Projenin X.25 standartını destekleyen kısmı hem esnek yapı sağlaması hem de gerektiğinde performans dengelemesi yapılabilmesi için birden fazla virtual circuit destekleyecek şekilde tasarlanmıştır. Bu durumda birden fazla virtual circuit bilgisinin birbirlerine karışmadan değerlendirilebilmesi ve işlemleri spesifik olarak hangi virtual circuit üzerinde yapıldığının belirlenebilmesi için 'Virtual Circuit Control Block' adı verilen kontrol blokları kullanılmıştır. Bu kontrol bloklar herhangi bir anda ait olduğu virtual circuit'in durumunu göstermeleri açısından programın işleyişi için büyük önem taşımaktadırlar.

V.2.2 Ethernet Queue (Kuyruk) Yapısı

Ethernet bağlantısının 10 Mbit, X.25 bağlantısının ise şu anki yapıda 19.2 Kbit ile çalıştığı göz önüne alınacak olursa X.25 tarafından gelip ethernet tarafına gidecek bilgiler normal şartlar altında herhangi bir tıkanmaya neden olmazlarken, ethernet tarafından gelip X.25 tarafına aktarılacak bilgilerin arada oldukça fazla olan hız farkı sebebiyle bir birikmeye sebebiyet verecekleri aşikardır. Bu birikmeyi dengeleyebilmek ve oluşabilecek bilgi kayıplarını ortadan kaldırmak için ethernet'den X.25'e geçiş yönünde bir queue (kuyruk) mekanizması geliştirilmiştir. Bu queue yapısına 'Ethernet Queue' adı verilmiştir.

V.3 IP Router Uygulamasının Sonucu

Öncelikle uygulamanın geliştirildiği işletim sistemi olan DOS'un aynı anda birden fazla process (işlem) çalıştırma, timer (zamanlama) servisleri konusunda yeterince sistem hizmetine sahip olmaması sonucunda uygulamanın değişik aşamalarında problemler ile karşılaşılmış, fakat lokal olarak geliştirilen çözümler ile bu problemlerin üstesinden gelinmiştir. Yine aynı sebepten ötürü X.25 kısmını destekleyen ve assembler dili kullanılarak yazılan modülün tasarımı sırasında, modülün reenterant (kendi kendini değiştirmeyen ve birden fazla process tarafından çağrılabilen) yapıda olup olmayacağı konusunda projenin genelini ilgilendiren kritik bir karar verilmesi durumu ortaya çıkmıştır. Yapılan araştırma ve inceleme sonucunda, X.25 haberleşme hızının 19.200 bps ile sınırlı olduğu ve bu hızın kullanılan bilgisayarın hızı yanında ihmal edilebilecek bir seviyede bulunduğu tesbitiyle, reenterant yapı kullanılmaktan vazgeçilmiştir. Ayrıca haberleşme konularında oldukça önem taşıyan ve çoğu zaman oluşan dead-lock (kısır döngü) durumlarını çözmeyi sağlayan time-out (zamanın dolması) mekanizmalarının da geliştirilmesinde DOS'un gerekli desteği yeterince sağlamaması sonucunda program içinde özel kodlamaların uygulanması gerekli olmuştur.

Sonuç olarak, haberleşme konusunda önemli bir yeri olan ve bilgisayar piyasasında da ticari değeri bulunan bu cins bir cihazın tamamen akademik imkanlar kullanılarak Türkiye'de de gerçekleştirilebileceği ve hem teknoloji uygulaması hem de geliştirilmesi açısından dünyadaki diğer eş seviyedeki kurumlar ile başabaş bir yarış içinde olunabileceği görülmüştür.

KAYNAKLAR

1- Tanenbaum, S. A., "Computer Networks, Second Edition", Prentice-Hall International Editions,1989

2- Comer, D., "Operating System Design-Volume II: Internetworking with Xinu", Prentice Hall International Editions, 1987

3- Schwartz, M. "Telecommunication Networks, Protocols, Modeling and Analysis", Addison Wesley,1988

4- Stallings, W. "Local Networks", Maxwell Macmillan International Editions, 1990

5- Stallings, W. "ISDN an Introduction", Maxwell Macmillan International Editions,1990

6- CCITT, "Recommendation X.25, Interface between Data Terminal Equipment (DTE) and Data Circuit Terminating Equipment (DCE) for Terminals OPerating in the Packet Mode on Public Data Networks", 1980

ÖZGEÇMİŞ

Soyadı:	YAVUZ
Adı:	A. Gökhan
Doğum Yeri:	İstanbul
Doğum Tarihi:	07/07/1969

1975-1979	Pilot Cengiz Topel İlkokulu
1979-1986	İstanbul Erkek Lisesi
1986-1990	Yıldız Üniversitesi Mühendislik Fakültesi Bilgisayar Bilimleri ve Mühendisliği Bölümü
1991-	Yıldız Üniverstitesi Fen Bilimleri Enstitüsü Bilgisayar Bilimleri Mühendisliği Anabilim Dalı