Chapter Contents

6.0 Packet Networks

6.1 System Examples
- 6.1.1 DDN
- 6.1.2 TYMNET
- 6.1.3 ARPANET†
- 6.1.4 The Internet
- 6.1.5 Nortel Packet Switches
- 6.1.6 Nortel ATM Switches
- 6.1.7 Unitel

6.2 Packets
- 6.2.1 Standards

6.3 LANs
- 6.3.1 LAN Topology
- 6.3.2 LAN Transmission Media
- 6.3.3 LAN Protocols

6.4 MANs
- 6.4.1 PDN and VAN

6.5 IEEE 802 Standards
- 6.5.1 IEEE 802.1
- 6.5.2 IEEE 802.2
- 6.5.3 IEEE 802.3 CSMA-CD Bus
- 6.5.4 IEEE 802.4 Token Bus
- 6.5.5 IEEE 802.5 Token Ring
- 6.5.6 IEEE 802.6 DQDB MAN
- 6.5.7 IEEE 802.7 BBTAG
- 6.5.8 IEEE 802.8 FOTAG
- 6.5.9 IEEE 802.9 IVD/LAN
- 6.5.10 IEEE 802.10 SILS
- 6.5.11 IEEE 802.11 Wireless LANs

6.6 Network Control and Routing
- 6.6.1 Traffic Control
- 6.6.2 Flow Control
- 6.6.3 Congestion Control
- 6.6.4 Routing

6.7 Packet Switching Protocols and Architecture
- 6.7.1 SNA
- 6.7.2 X.25
- 6.7.3 .X75
- 6.7.4 TCP/IP

6.8 MPLS Multi-Protocol Label Switching

Assignment Questions

Notes

For Further Research

6.0 Packet Networks

Objectives

This section will:

- Discuss the need for packets
- Discuss network control and routing
- Examine LANs, MANs, and WANs
- Consider Nortel's packet switch offering
- Introduce the Internet

Packet networks come in a wide variety of sizes and capabilities. They range from small LANs to worldwide WANs†.

☞ Cisco Internetworking Tutorials

Internetworking Technology Handbook by Cisco

Internetwork Design Guide by Cisco

6.1 System Examples

6.1.1 DDN

The DDN† uses a distributed adaptive algorithm. Each node measures the delay between itself and any adjacent nodes. Every 10 seconds each node calculates the average delay on each of its outgoing trunks, and sends this information out over the network by means of flooding. Each node can then perform a least cost calculation to determine the best route.

6.1.2 TYMNET

This is a centralized adaptive network, and uses a supervisor node to perform the routing function. The supervisor finds a virtual circuit using a forward search algorithm and cost per link criteria. The link cost is based on data rate, load factor, satellite vs. land link, and traffic type. This network works best with virtual circuits.

The supervisor sends a needle to the source node, containing the route as a list of nodes, The needle passes trough the designated route depositing routing

† Wide Area Networks

† Defense Data Network

______ Notes ______

information on the way. If an outage is encountered, the needle retraces the route back to the supervisor.

The advantage of the centralized system is that the controller has a better idea of the overall condition of the system, thus better able to implement flow control mechanisms, and reducing the call processing requirements on the individual nodes.

6.1.3 ARPANET†

This system uses a distributed, adaptive, delay-based, routing algorithm. Incoming packets are time stamped and the out going time noted. If a PACK is returned, the delay time is calculated as the departure time minus the arrival time plus transmission time and propagation delay. The node must therefor know the data rate and propagation delay to each other node it is connected to.

If a NACK is received, the departure time is updated, and the node tries again.

Every ten seconds the node calculates the average delay on each outgoing trunk. If there are any significant changes in delay, that information is sent out by flooding to all other nodes. Each node then updates its routing table by using a forward search algorithm.

6.1.4 The Internet

Minimum Reading

An Overview of Internet Protocols by O'Neill et. al.

For the advanced student

Internet Access by IEC

Internet Security by Sun Micro Systems

IP IN Integration by MicroLegend

IP Internetworking Transport by Newbridge

IP by Cisco

IP Multicast by Cisco

Web Hosting by PSINet

Net Socializing with Visual Communications by Connectix

Voice/Fax over IP by Micom

Intranets & VPNs by PSINet

SS7 for Internet Access by Lucent Technologies

Public Access Web Information Systems by Kambil & Ginsburg

† Advanced Research Project Agency Network

An internetwork is a network of networks and is generally classified as a WAN. The individual nets are called subnets and are linked together by high-speed backbones.

The Internet started as ARPANET in 1969. It connected government, academic, and industrial computing LANs together. Users could send Email messages, transfer files and log-on to remote hosts. The packet switched network used 56 Kbps links subdivided into 8 full duplex channels employing ABP[†]. The internet protocols were constantly evolving and in 1983 the NCP[†] became TCP/IP[†]. The current internet protocol IPv4 is expected to be upgraded to IPv6[†]. Some of the major subnetworks connected to the present Internet include:

- ARPANET - the Department of Defense ARPA network
- NSFnet - the National Science Foundation network
- MILNET - an unclassified military net
- Commercial Research Networks - many major corporations
- Government Networks - numerous government agencies

The Internet has also been called the information highway, the infobahn, the NII etc. With the advent of personal computers, modems, and networking software, any person can access from the comfort of their own home via the PSTN. By 1994 approximately 60,000 network domains and 4 million hosts were connects on this facility.[1]

One obvious problem associated with the present explosion of the Internet, is that now there is no one in charge. Consequently unscrupulous hackers can gain entry into many major computer facilities and wreck havoc with the system. A kind of undeclared anarchy presently exists.

† Alternating Bit Protocol

† Network Control Protocol

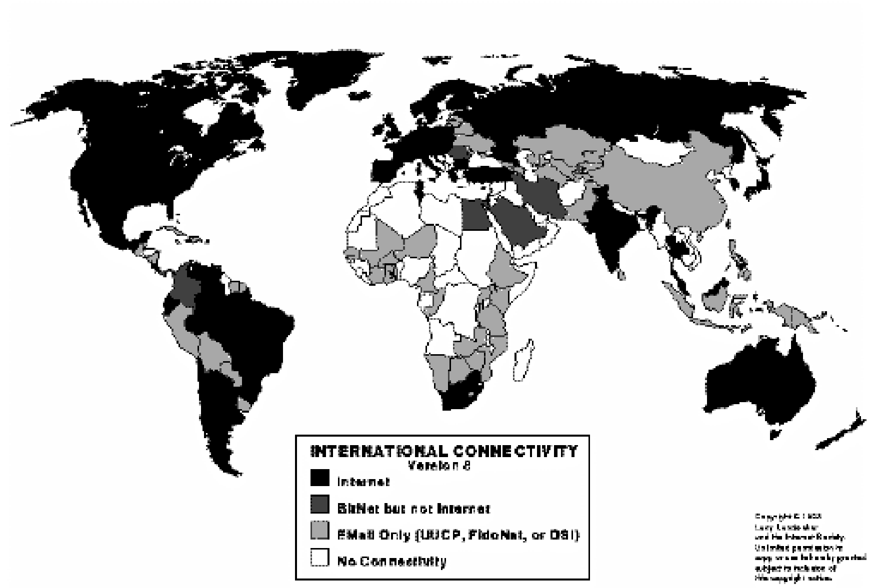
† Transmission Control Protocol/Internet Protocol

† Internet Protocol version 6

1 The State of the Internet: 1995, Telecommunications 1995, vol 29 no 1

______ Notes ______

WWW Access



MCI US Map

6.1.5 Nortel Packet Switches

☞ Minimum Reading

Packet Telephony

The Nortel DPN–100 is a packet switching system. By 1990, there were more than 3,000 switches operating in more than 90 networks in some 40 countries. Approximately 60% of these networks are privately owned.

This product, although still supported, is no longer in production.

Magellan DPN-100

The Nortel DPN–100 has enjoyed wide acceptance. It has the largest market share of any switch in its class, with nearly 5,000 switches deployed in more than 100 public and private networks in 70 countries[2]. Some of its customers include:

Bankers Trust	This organization pioneered global data networking with the first packet switching satellite bridge to Hong Kong. It currently deploys DPN–100 all over the world.

2 DPN-100: a blend of power and performance, telesis issue no. 95

Air France	Air France has more than 10,000 reservations terminals on four continents. They adopted the DPN–100 in 1991.
UPS†	UPS, the world' s largest package distribution company transports more than 3 billion parcels and documents annually. Using more than 500 aircraft, 157,000 vehicles and 1,700 facilities to provide service in more than 200 countries and territories, we have made a worldwide commitment to serving the needs of the global marketplace. It uses DPN-100.
SWIFT†	The SWIFT network handles the electronic funds transfer for 6,673 financial institutions in 193 countries. An average of 5 Trillion $US is handled every day.
SITA†	The SITA network handles the data needs of 700 companies in the air transport sector in 220 countries and territories. This is the worlds largest commercial network. There are in excess of 100 mainframe computers and 120,000 terminals connected to the system Network management centers are located in Europe, North America, and Asia.

For the advanced student

www.ups.com

www.swift.com

http://www.sita.int/

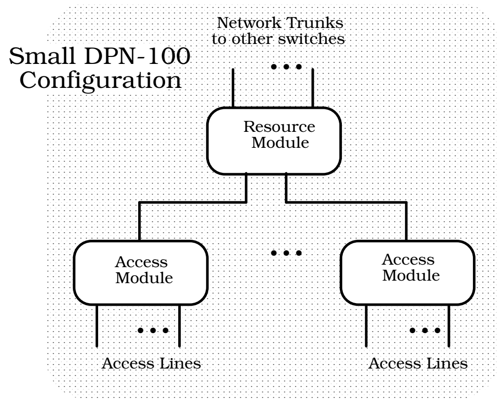
† United Parcel Service

† Society for Worldwide Interbank Financial Telecommunications

† Société Internationale de Télécommunications Aéronautiques

_____ Notes _____

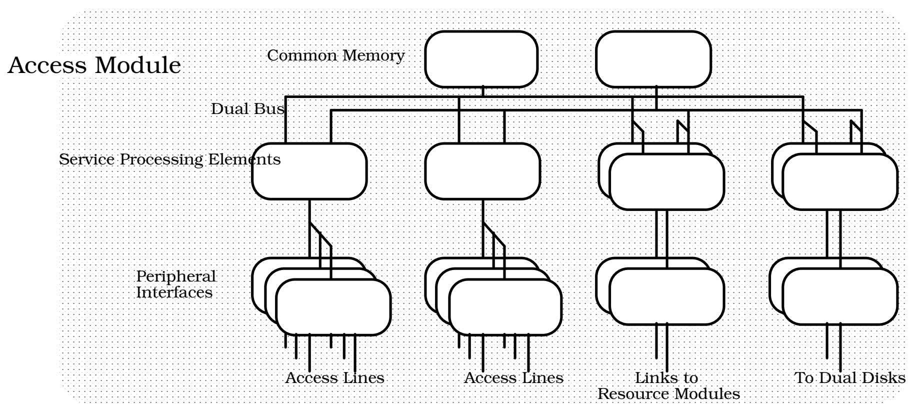
Small DPN–100 Configuration



The small DPN-100 consists of a resource module and a number of access modules.

Access Module (as of 1988)[3]

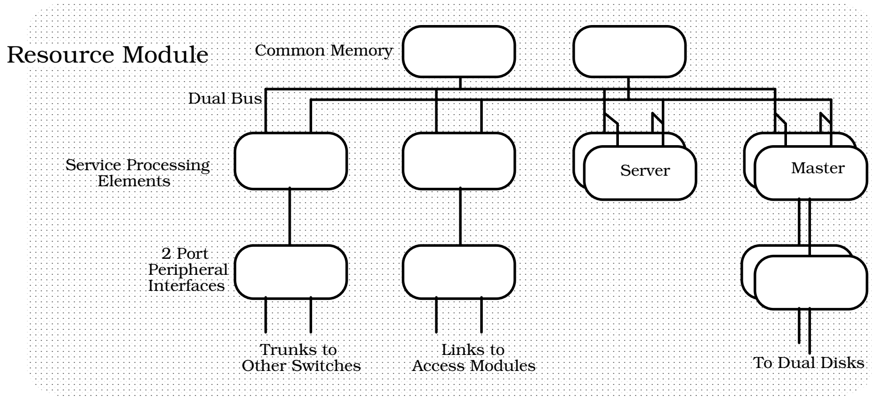
The access module is a distributed processor consisting of processing elements, a bus and memory.



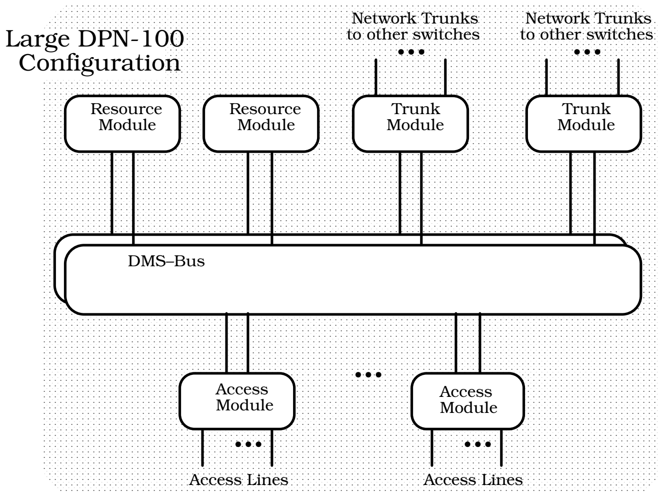
Resource Module

In large DPN–100 configurations, at least two resource modules are dedicated to switch management, network operations and server functions. Switch control is performed by one resource module designated as prime, and is backed up by an alternate resource module in the standby mode. All other functions are load shared by the remaining resource modules.

3 DPN-100: New System Architecture for DPN Packet-Switching Family, Telesis, 1988 two



Large DPN–100 Configuration



The large DPN-100 adds the same DMS–Bus found in the DMS SuperNode as well as some trunk modules.

6.1.6 Nortel ATM Switches

Some of the following information was taken from the Nortel ATM tutorial found at www.webproforum.com

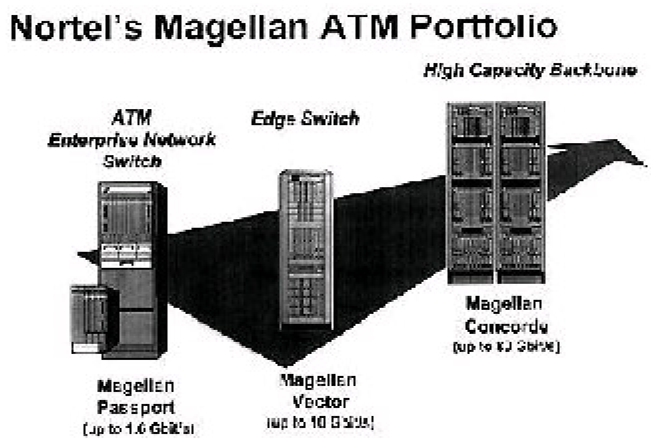
Magellan family of ATM switches developed by Nortel consists of 4 principle hardware components:

Notes

Magellan Component	Capacity [Gbps]	Function
DPN-100		Supports X.25, X.28, X.31, point-of-sale, SNA
Passport	1.6	CPE that consolidates end-user traffic and reformats it into ATM cells.
Vector	2.5 - 5	Combines ATM traffic and performs network concentrating and switching. It can be used as a smaller backbone switch.
Concorde	10 - 80	ATM backbone switch. Primarily used by long distance carriers.

This product was introduced in 1994, and by the following year more than 4000 Magellan systems had been shipped to 150 countries.[4]

Nortel's Magellan portfolio of ATM switches consisted of Magellan Passport, Vector, and Concorde.



Magellan Passport is a 1.6 Gbps ATM switch that can be deployed as a CPE-based ATM enterprise network switch or as a CO-based ATM switch. It supports ATM, frame relay, multiprotocol routing, and intelligent circuit emulation services.

There are two models: Model 50 has 5 slots; Model 160 has 16 slots. Magellan Vector is a 2.5 Gbps to 10 Gbps ATM switch. Magellan Concorde is a CO high-capacity ATM switch, scaleable to 80 Gbps, designed for use in the core of an ATM network or as part of a large-scale video-on- demand system.

Magellan Passport

For Advanced Students

Passport 6100

4 *Magellan Passport Consolidates Enterprise Networks*, Telesis issue 100, October 1995.

This device supports a wide variety of traffic types and protocols. It can switch both cell and frame based packets, allowing it to transport voice, video and LAN traffic.

Passport's key features include:

- Support interfaces including ATM UNI, frame relay UNI, LAN, channelized T-1, and synchronous links
- High-quality voice networking over VBR-RT SVCs, providing single-hop routing between PBXs in enterprise networks
- Frame-relay SVCs, frame-relay QOS support and high-density channelized interfaces
- Integrated multiprotocol routing and ATM switching
- Flexible trunking options over point-point ATM, public ATM and narrowband/wideband frame/cell trunks
- Comprehensive traffic management across the Magellan portfolio.

Magellan Vector (Discontinued)

Vector is strictly an ATM product. It consolidates lower speed ATM LAN traffic into high-speed ATM facilities. Its applications include: ATM concentration, public access switch, or LAN backbone switch.

Vector's key features include:

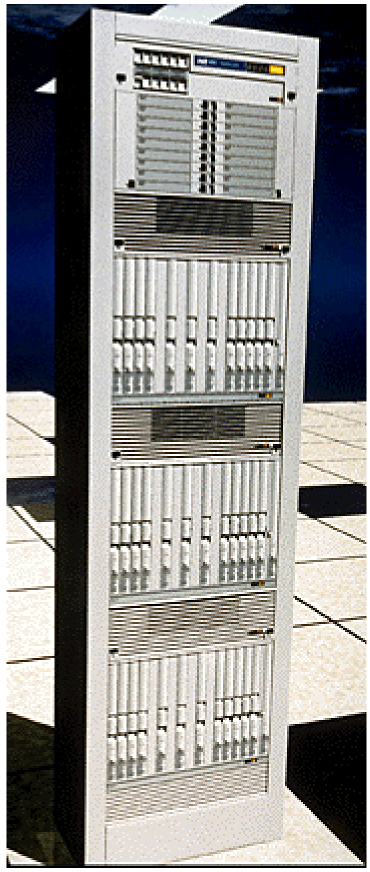
- ATM interfaces available for T-1/E-1 to OC-12
- SONET and electrical interface redundancy
- Maintains of all active VC connections on switchover
- Supports ATM SVCs and smart PVCs (SPVCs)
- Dynamic routing and VC rerouting through a pre-standard implementation of the ATM Forum's PNNI Phase 1
- Connection security and control. This allows customers to protect the network against fraudulent use, including dynamic address registration, calling-address verification, and called-address screening
- A data-collection system supporting collection and correlation of billing data for PVCs and SVCs.

Magellan Concorde (Discontinued)

The Concorde is a high speed ATM switch that is used to support OC-3 and OC-12 trunks.

Concorde's key features include:

- Scaleable hierarchical redundant switch optimized for network backbones
- Supports broadband and SONET/SDH network management
- Modular packaging with fiber management, blind-mating connectors, and self-contained line cards



The Magellan Concord system can segregate, prioritize, and manage different types of traffic. 128 QO classes are supported

6.1.7 Unitel

Unitel is generally regarded as a long distance voice carrier however, it also offers data services. Its DataVPN service is available in about 600 centers in Canada, and supported by backbone switches in Montreal, Ottawa, Toronto, Edmonton , and Vancouver.

The system consists of more than 20 Stratacom IPX cell-based frame relay switches. These are capable of supporting ATM although at the time of this writing, there were few ATM customers.[5]

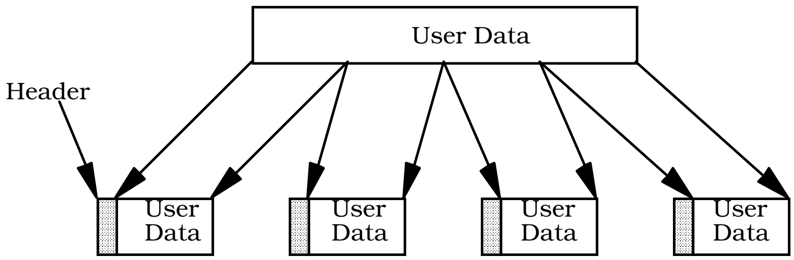
6.2 Packets

In most data applications, user data is decomposed into a string of packets. This requires that additional information be added to the user's data to ensure its safe arrival at the correct destination.

5 *Unitel turns up WAN data business*, Computing Canada, February 15, 1996

Notes

If the packets are rather long or of variable length, the system may be referred to as frame relay. If the packets are small and of fixed length, the system may be referred to as cell relay.



Dividing User Data into Packets

The user data may be organized into fixed or variable length packets depending on the type of system. In any case, additional information is appended to the customers data in the form of a header.

Some of the header contents may include:

- Source address
- Destination address
- Time stamp or packet sequence number
- Maximum allowable delay (priority)
- ACK/NACK
- Network control/billing
- Error checking etc.

However, simplex connections with transmission delays are not suitable for voice connections, but are not a concern in data transmission. Each input data packet is stored in an input buffer or queue and sent to the appropriate output queue when resources become available. If the packets and queues are sufficiently short, a virtual full duplex link may be established, and interactive transactions may be possible.

LANs can be connected to form MANs†, which in turn can be connected to form WANs. Such networks may span the country or encompass the globe.

6.2.1 Standards

In order to understand the operation of these systems, it is often necessary to resort to a standard reference model. The OSI model outlines the various functions and attributes, which are inherent in any communications system.

A further necessity is the standardization of the implementation of the OSI model. This work has largely been done by the IEEE and ITU (formerly CCITT).

† Metropolitan Area Networks

_____ Notes _____

OSI Model

Minimum Reading

OSI by Cisco

The OSI model was started in 1978 and has evolved to provide a framework for interoperability. Standardization is required in order that various types of equipment or systems can be joined in some useful way. Some of the activities, which are regulated, include:

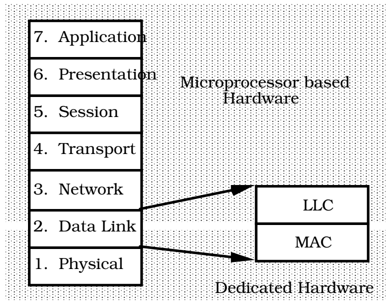
- Interprocess communications
- Data representation
- Data storage
- Resource and process management
- Security
- Program support

OSI Layers		
Level	Layer	Comments
7	Applications	Contains the management functions necessary to support such applications as file transfer and electronic mail across various types of equipment. Examples are: X.400
6	Presentation	Governs the syntax necessary to convert generic programs to specific machine types.
5	Session	Controls the dialog between applications.
4	Transport	Ensures that data are delivered in order and without errors.
3	Network	Establishes, maintains, and terminates the data link through the communications facility. Examples are: X.25, X.75, RS-366A
2	Data Link	Increases the reliability of the physical link by providing error detection and control. It is often divided into two sublayers: LLC[†], and MAC[†]. examples are: X3.28, BSC, HDLC, ADCCP, SDLC, CSMA/CD
1	Physical	Concerns the actual medium over which data is sent. Examples are: X.21, V.35, RS-232C

The majority of the OSI model is implemented in microprocessor based hardware. This means that new applications, network architectures, and protocols can generally be accommodated by making software changes. It also means that the traditional gap between the telecommunications and computer industry is being reduced.

† Logical Link Control

† Media Access Control



Significant advances have been made in the physical layer interfaces, as networks migrate from twisted pair cabling to fiber optics. These developments have introduced new applications, architectures and protocols.

Some applications for public data packet networks include:

- Electronic funds transfer
  - Banks
  - Automated tellers
  - Clearinghouses
  - Stock exchanges
- Point-of-sale terminals
- Credit card verification
- Electronic mail
- Electronic purchasing
- Inventory management
- Database interworking

IEEE

The IEEE is one of the key organizations establishing LANs standards. These standards have become more important than ever, because the large equipment suppliers have traditionally developed incompatible LAN standards. IBM for example developed the token ring concept while DEC supports Ethernet. These two systems cannot readily be interconnected until their formats are standardized and third party vendors can develop cross platform products.

Standard	Comments
802.1	HILI - higher layers and interworking
802.2	Logical Link Control
802.3	CSMA-CD Bus
802.4	Token Bus
802.5	Token Ring
802.6	DQDB MAN
802.7	BBTAG - broadband
802.8	FOTAG - Fiber
802.9	IVD LAN
802.10	SILS - interoperability of LAN security
802.11	Wireless LANs

_____ Notes _____

6.3 LANs

Minimum Reading

LAN Protocols by Cisco

For Advanced Students

BayStack Ethernet Solutions

LANs are the smallest packet networks and are used to connect a group of terminals or workstations together. These may be found in a relatively confined space such as within a building or campus setting. The attachments may be dumb or intelligent terminals, file servers, routers, and repeaters.

The majority of LANs are privately owned. They can be connected to the PSTN or some other carrier to form MANs or WANs.

LANs can be categorized in a number of ways. One method examines how information is placed on the interconnecting transmission medium. Baseband LANs directly inject logic levels of on the medium and share access by some form of TDM. Broadband LANs however, use high frequency carriers and share access by FDM.

Some authors prefer to segregate a special category, the PBX:

LAN - local area network [baseband]

HSLN - high-speed local network [may be baseband or broadband]

PBX - private branch exchange [baseband]

LAN Comparisons			
	LAN	HSLN	PBX
Transmission Media	Twisted Pair, coax, fiber	Coax, fiber	Twisted pair
Topology	Bus, tree, ring	Bus, ring	Star
Transmission Speed	1 – 20 Mbps	50 – 100 Mbps	9.6 – 64 Kbps
Maximum Range	25 Km	1 – 25 Km	1 – 10 Km
Switching Technique	Packet	Packet	Circuit
# Terminals	100 – 1000	10 – 100	100 – 10000
Attachment Cost	$500 – $5000	$40 – $50 K	$250 – $1000

Most people do not think of the telephone PBX as a LAN, since it generally does not carry digital data, but it does meet the technical definition.

There are approximately 2 million LANs in the U.S. and it is expected that there will be 6 million by the end of the decade.

The most widely used LANs today are ethernet, token ring, token bus, and Appletalk. They can be interconnected by gateways, routers, bridges, or repeaters to form MANs, which can in turn be used to create WANs.

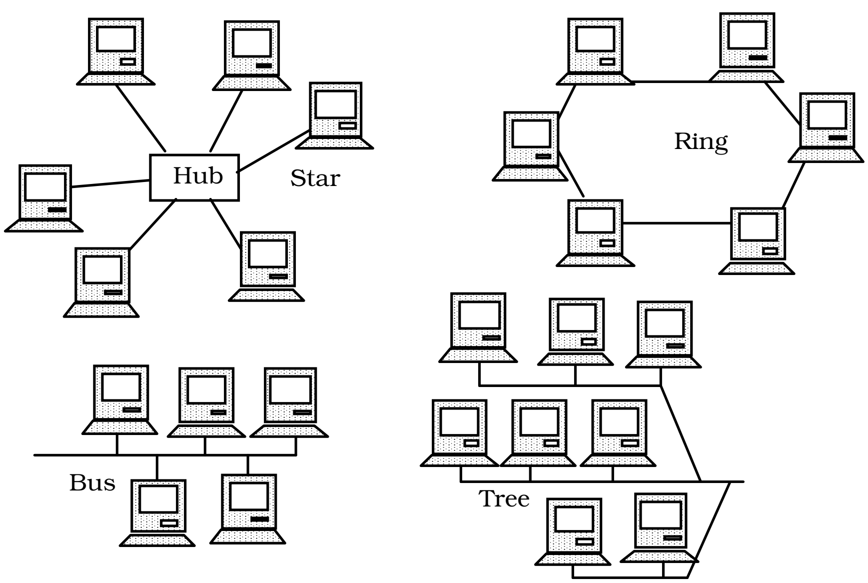
LAN Components and the OSI Model

OSI Layer	Layer Description	LAN Service Provider
7	Applications	Gateway
6	Presentation	
5	Session	
4	Transport	
3	Network	Router
2	Data Link	Bridge
1	Physical	Repeater

LANs have largely been ignored by telcos and are generally confined to relatively low speed private networks. With the advent of fiber however, new techniques such as FDDI and FDDI II are changing the way telcos view private networks.

6.3.1 LAN Topology

LANs can be configured in three basic ways, namely: as a ring, star, or bus. Another arrangement known as a tree topology is really a variation of the bus. Cable TV is an example of a tree network employing frequency division multiplexing.



Star

The end office of the PSTN is configured as a star where all lines radiate from a single location. This type of wiring is also used in all modern office buildings. This center of the star or hub may contain a network manager of some other piece of hardware that exercises control over the LAN. This type of arrangement is used in a PBX, and the most common connection media is a twisted pair of wires.

Some networks may be configured as a physical star, but may have a different logical topology, such as a ring.

Ring

A ring consists of a closed loop, where each station is connected by an active or passive tap. An active tap is one has electronic components inserted into the loop to both extract and inject signals, thus all stations are effectively connected in series. A passive tap simply comes in contact with the loop., thus all stations are effectively connected in parallel.

A station wanting to transmit waits its turn to inject a packet onto the ring. This implies some sort of distributed protocol. This is most often implemented by means of a token.

Bus

A distributed protocol arrangement or token is needed to resolve bus contention problems. Each terminal monitors the common bus for any data with their address appended, at which point it simply makes a copy. This arrangement is often found in computer systems where a number of peripheral devices may be connected on a high-speed bus.

Two important issues in this type of arrangement are access and signal level. In a baseband or digital environment, there is often a polling mechanism imposed to create order. Also, the signals degenerate as they propagate down the line, this means that some sort of compensation must be made.

RS-422 is a simple protocol that is implemented on a twisted wire bus. The system allows a couple of dozen devices to be networked as far as 1 km, with a data rate of up to 1 Mbps.

Ethernet is an example of a baseband system implemented on a bus.

6.3.2 LAN Transmission Media

Almost any type of transmission media can be used, but for higher data rate applications, coaxial or fiber optic cables are used.

Baseband coax systems use 50 Ω cable instead of the 75 Ω cable employed in TV systems. This is because digital signals cause fewer reflections at the lower impedance. In order to further reduce signal cancellation due to mismatch, the taps are spaced regular intervals depending of the data rate. If the data rate is greater than 10 Mbps, then no more than 100 taps are recommended on a 500-meter cable.

Fiber optics as a LAN medium provides a number of advantages over other transport types:

- Electromagnetic immunity
- Immune to ground loops
- Can be used in hazardous locations

_____ Notes _____

- Secure communication
- Capable of transporting all protocols and data rates
- Small size and lightweight

Transmission Media	Data Rate [Mbps]	Range [Km]	# Taps
Twisted Pair	1 – 2	2	10
Baseband Coax	10 – 50	3	100
Broadband Coax	500	30	1000
Optical Fiber	10 - 200	1	10

MAC - Media Access Control

The transmission media can be accessed by several methods, each of which has a defining standard:

CSMA/CD defined by IEEE 802.3

Token bus defined by IEEE 802.4

Token ring defined by IEEE 802.5

The various access media include twisted pair, coax, and fiber. Not all of these media types can support all access techniques.

LLC - Logical Link Control

When people communicate with each other, they generally observe certain formalities, which initiate, govern and terminate the conversation. A similar process occurs when two electronic machines communicate with each other.

Communication between two machines, such as computer terminals requires:

- Addressing (source/destination)
- Link management (setup)
- Frame synchronization (identify start & stop)
- Flow (speed) control
- Error control (detection/correction)

6.3.3 LAN Protocols

Minimum Reading

LAN Protocols by Cisco

Protocols can be either bit or byte oriented. They should adapt to a wide range of customer applications and equipment types and handle any type of code. Since the objectives of any protocol are nearly identical, it is not surprising to observe striking similarities.

The most popular bit oriented protocols are:

Protocol	Developer
HDLC	ISO
ADCCP	ANSI
LAP–B	CCITT
SDLC	IBM

For Advanced Students

HDLC

The High-level Data Link Control is formalized by the International Organization for Standardization as ISO 3309. It uses synchronous transmission and organizes customer data into a frame with the following structure:

- Start Flag - 1 octet [01111110]
- Address - 1 or more octets
- Control - 1 or 2 octets
- User Data -
- FCS - 2 or 4 octets
- End Flag - 1 octet [01111110]

6.4 MANs

Interconnected LANs form MANs. The LANs may be in different buildings on a college campus, an industrial park, or scattered across a city.

Nynex and MFS have installed a 2.4 Gbps bidirectional SONET OC-48 ring. It is a private network used to connect Citycorp offices throughout New York and New Jersey[6]. It also connects to two central offices and 3 IEC POPs. The network uses 2 fibers out of a 12 fiber ribbon cable.

Simple MANs use bridges, routers and gateways to link LANs together.

LAN Bridge [remote]

- Encases one or more LAN frames into an HDLC format for transmission
- Contains buffer space to meet peak demands
- Contains addressing and routing information so as to know which frames to pass

LAN Router

- Contains algorithms to read and translate various data link protocols
- May perform congestion control
- May fragment or reassemble frames

6 Lightwave, February 1995

LAN Gateway

- Unfortunately this is a generic term which can be used to describe any device which connects networks together [bridge, router, etc.]
- Specifically - must perform protocol conversion for all OSI layers
- Acts as a protocol converter [translator] between any two stations on different network types

More complex MANs can be created by employing high-speed data backbones, which transport only specific MAN protocols such as IEEE 802.6.

The three principle types of MANs in existence today are:

- .X25 network - the principle standard used today to create public data networks
- ISDN - already discussed as the next possible evolution of the PSTN
- SONET - a fiber based protocol being used to implement extremely high-speed backbones
- *The Internet* - an ad hoc network which has virtually no control mechanisms

Depending on where the accessed database is located, the above applications could be implemented on LANs, MANs, or WANs. However, in large business applications, they are all supported on WANs since the enormous databases involved are centralized. If the database is operated by the carrier, the network is often referred to as a VAN[†].

6.4.1 PDN and VAN

Minimum Reading

VPNs by Cisco

For Advanced Students

Virtual Private Networks

PDN[†]s or VANs have been established throughout the world. These types of networks are constructed by the public carriers to provide wide area data communications services for computer based information systems.

Extremely large organizations that require secure communications, such as international banking institutions, or the military may actually own their own private packet network.

[†] Value Added Network

[†] Public Data Networks

Nortel manufactures the DPN-100 packet switch. Its modular, flexible architecture allows corporate customers to readily adapt to market needs and establish new services.

6.5 IEEE 802 Standards

6.5.1 IEEE 802.1

This standard provides the framework for addressing issues such as: internetworking, network management, and performance measurement. It also covers end-to-end protocols, routing and bridging.

6.5.2 IEEE 802.2

This standard defines the LLC or logical link control. This corresponds to the upper half of the data link layer in the OSI model.

6.5.3 IEEE 802.3 CSMA-CD Bus

Minimum Reading

Ethernet by Cisco

For Advanced Students

http://www.lantronix.com/technology/tutorials/

http://wwwhost.ots.utexas.edu/ethernet/ethernet-home.html

http://www.gigabit-ethernet.org/

This LAN standard is most commonly known as Ethernet. Initially, the standard specified data rates up to 10 Mbps over coaxial cable or twisted copper pairs.

Learn more about the IEEE's 802.3 Ethernet standards and Working Group by visiting their website at http://grouper.ieee.org/groups/802/3/

The 802.3 standard defines the MAC and physical layer for a CSMA/CD bus. It evolved from the ALOHA packet network developed at the University of Hawaii and ethernet developed by Xerox. The standard was originally intended to operate on coaxial cable, but has since been modified to operate on UTP and fiber.

The approximate efficiency of the CSMA–CD protocol is given by:

$$\eta \approx \frac{1}{1+5a} \quad \text{where} \quad a = \frac{t_{prop}}{t_{packet}}$$

This arrangement is more efficient than pure ALOHA if $a < .89$ and more efficient than slotted ALOHA if $a < .34$. This is primarily because an Ethernet node can readily sense whether the medium is occupied before transmitting, and immediately stops once a collision is detected. The long propagation times associated with satellite based networks, reduces the effectiveness of the carrier sense technique.

IEEE 802.3 Networks[7]

	10BASE5	10BASE2	1BASE5	10BASE–T	10BROAD36
Medium	10 mm Coax	5 mm Coax	Twisted Pair	2 Twisted Pairs	Coax
Impedance	50 Ω	50 Ω	85 - 110 Ω	85 - 110 Ω	75 Ω
Bit Rate [Mbps]	10	10	1	10	10
Encoding	Manchester	Manchester	Manchester	Manchester	DPSK
Max Length [m]	500	185	500	100	1800
Nodes per Segment	100	30		2	
Max Distance [km]	2.5	.925	2.5	1	3.6
Collision Detection	Excess Current	Excess Current	2 active hub inputs	Rx & Tx	Tx ≠ Rx
Connector	DB-15	BNC		RJ-45	

MAC - Collision Detection

To minimize the number of transmission collisions, the CSMA-CD protocol requires that any unit wishing to send data, must first sense the loop and determine if it is available. However, two units may attempt to send data at the same time. This results in a collision and the data is corrupted.

There are several different collision detection schemes found in the 802.3 standard:

- Excess current - The transmitting terminal injects an average current of 18 – 24 ma into the coax. If the current exceeds this value, a collision is assumed to have occurred.
- Tx & Rx activity - A MAU[†] detects collisions by observing the activity on the Tx and Rx twisted pairs going out to each terminal. When a collision occurs, the MAU broadcasts a jam signal and both units initiate a random back off before attempting to retransmit.
- Tx ≠ Rx - This technique is used on RF networks. Each node compares what they transmit on one frequency to the signal rebroadcast by the head-end station on another frequency.

---

7 *Communications Networks*, Jean Wairand

† Media Attachment Unit

Standard	Common Name
10Base5	Ethernet
1Base5	StarLAN
10Base2	Cheapernet
10Base–T	TPE
10Base–F	Fiber optics
10Broad36	Broadband
100Base-T	Fast ethernet
1000Base-T	Gigabit ethernet

The IEEE designation has the following significance:

- Prefix [1 or 10] represents the bit rate in Mbps
- BASE means Manchester encoded baseband signals
- BROAD means broadband RF transmission using BPSK
- Numeric suffix [2, 5, 36] indicates the maximum segment length in hundreds of meters
- Alphabetical suffix [T, F] indicates the medium, twisted pair or fiber

Ethernet

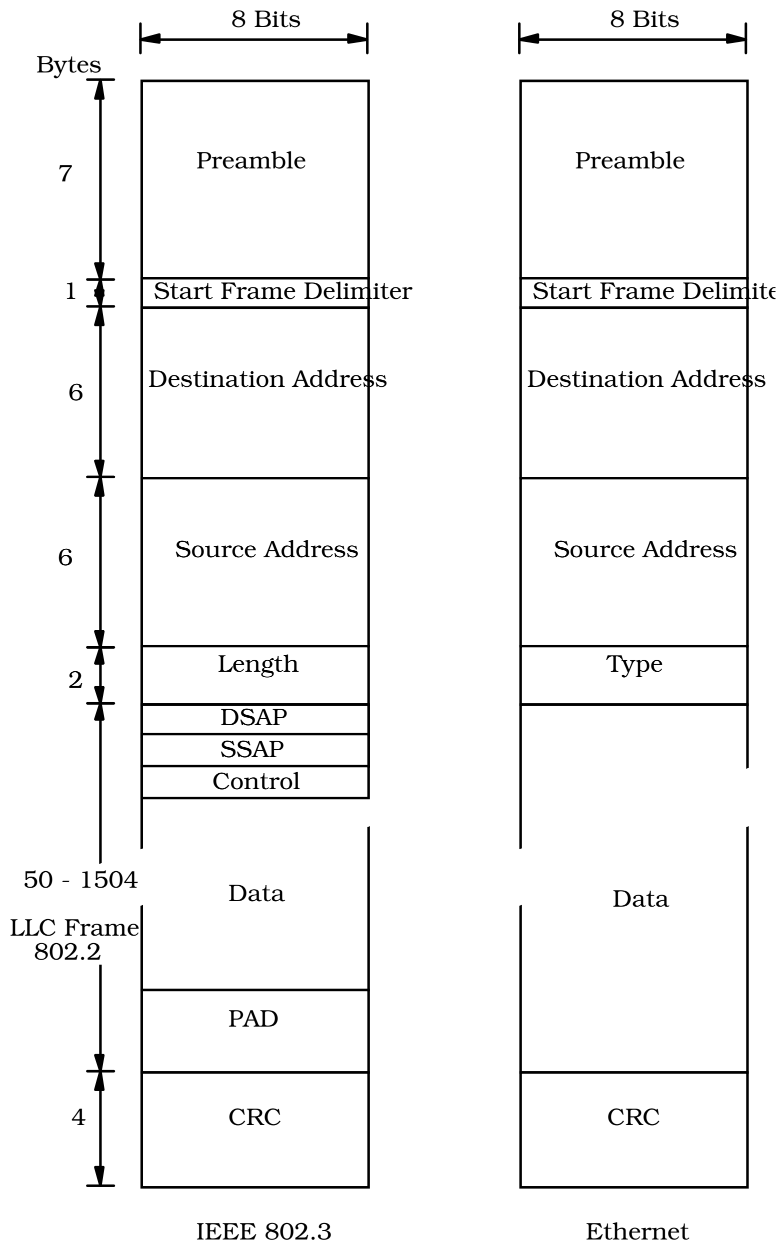
Ethernet was developed before the 802.3 standard emerged, but is very nearly identical to 10BASE5.

Three components are necessary to connect a terminal to an Ethernet:

- Interface board - this is located in the computer terminal and performs the framing and encoding functions.
- AUI[†] or Transceiver - this is connected to the interface board by a drop cable [up to 50 meters long]. It performs the collision detection and provides the electrical interface to the segment. [example: Intel 82521TA]
- Tap - this provides the electro-mechanical interface which links the transceiver to the transmission medium.

† Attachment Unit Interface

Frame Structure



The 802.3 frame is followed 96 bits of silence.

_____ Notes _____

Cable Assignments

Pin	802.3	Ethernet
1	Control In Ground	Ground
2	Control In A	Collision Presence +
3	Data Out A	Transmit +
4	Data In Ground	
5	Data In A	Receive +
6	Voltage Common	
7	Control Out A	
8	Control Out Ground	
9	Control In B	Collision Presence -
10	Data Out B	Transmit -
11	Data Out Ground	
12	Data In B	Receive -
13	Power	
14	Power Ground	
15	Control Out B	

Collision detection is determined by measuring excess current. The transmitting unit injects a jam signal comprised of a random 32 – 42 bit sequence to inform all other nodes that a collision has occurred. The colliding parties then attempt a retransmission after a random time period.

The random timer uses a binary backoff algorithm. Both devices choose a random integer *K*, between 0 and 2^N-1. *N* represents the number of times a collision has occurred [maximum of 16]. The node then waits *K* times 512 bit periods before attempting a retransmission.

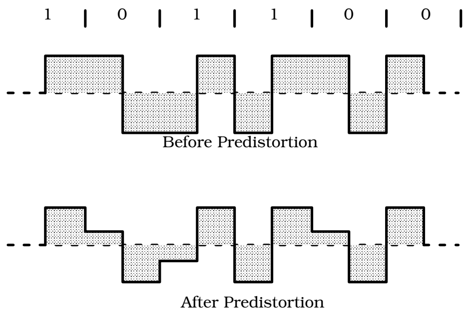
10BASE-T

10BASE-T and 1BASE5 are configured as a star, with a MAU in the center.

The MAU provides three essential functions: line driving with pre-distortion, line receiving, and collision detection. The MAU may be imbedded into a repeater or DTE.

The MAU is generally isolated from the line by means of a transformer. The transmitter must produce a differential output signal level of 2.2 to 2.8 volts into 96 Ω. The transmitted signal must be slightly modified or predistorted when driving a twisted pair loop.

Pulse width is not constant when Manchester encoding is used. As a result, the twisted pair can introduce timing jitter. To overcome this, ‘thin’ pulses [50 nSec] are driven at full amplitude. ‘Fat’ pulses [100 nSec] however, are driven in two stages: the first 50 nSec is driven at full amplitude, but the drive level is reduced to 33% during the second 50 nSec. This prevents the line from becoming ‘overcharged’ and delaying the next zero crossing.



The MAU line receiver is generally transformer coupled to the loop, and must provide an IRL of at least 15 dB. The receiver must correctly detect pulses ranging in amplitude from 0.35 volts to 2.8 volts and reject any signals below 0.25 volts. It must be able to detect pulse widths in excess of 20 nSec and detect the start of the idle condition in 1.8 bit periods.

An interesting variation of 10BaseT is iso-ethernet. It more properly falls under IEEE 802.9 since it allows a combination of both fixed rate ISDN channels and ethernet.

100BaseT Fast Ethernet

One of the more recent developments is fast ethernet, running at 100 Mbps. There are several different versions, depending on the cabling media.

Version	Cable	Length [m]	Comments
100BaseTX	2 pairs of cat 5 UTP	100	One pair operates at 125 Mbps with an 80% efficiency, and uses 4B5B coding. The second pare is used for collision detection and receive.
100BaseT4	4 pairs of cat 3, 4, or 5 UTP	100	Three pairs transmit data at 33 Mbps each while the fourth is used for collision detection.
100BaseFX	two fibers	412	One is used for transmission and the other is used for collision and receive.

IEEE 802.3z Gigabit Ethernet

Gigabit ethernet will provide a high-speed backbone to support the vast number of ethernet LANs currently in existence. It will operate at 1.25 Gbps and provide an end-user rate of 1 Gbps.

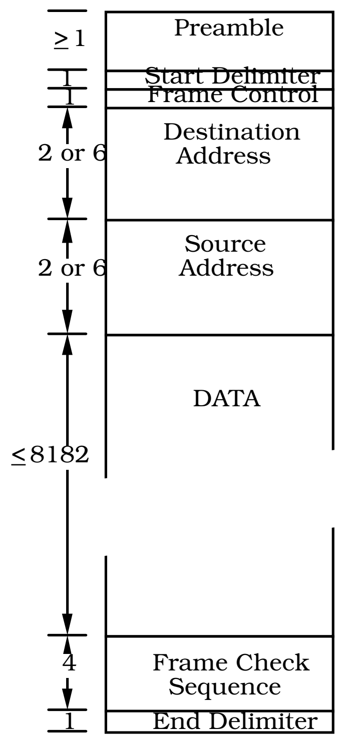
Initially, it will be supported over 780 nm single mode and 1300 nm multimode fiber, but will eventually be ported to category 5 UTP and coax. Each one of these transport mechanisms will have a different maximum range.

The present proposal relies heavily upon Fibre Channel components since these are readily available, and an 8B10B line code will be used.

6.5.4 IEEE 802.4 Token Bus

This standard defines the MAC and physical layer for a token bus arrangement. The token is passed to various terminal addresses according to a master list. GMMAP or General Motors Manufacturing Automation Protocol is based on this standard.

The bus generally operates at 1, 5, or 10 Mbps single or multichannel broadband signaling over coaxial cable. Some version of Manchester coding is used to encode the bit stream.



IEEE 802.4 Frame

The frame control byte distinguishes between three types of frames: LLC data frame, MAC control frame, and station management frame.

Since the token bus arrangement operates logically like a ring, but is physically implemented as a bus, it is more complex than token buses or standard rings. Terminals are connected to the bus by means of passive taps. When the token is broadcast, it picked up by all units attached to the bus. However, the station issuing the token addresses it to the next logical station on the bus. The receiving station can either transmit data or place a new token on the bus, addressed to the next logical station.

Notes

6.5.5 IEEE 802.5 Token Ring

☞ Minimum Reading

Token Ring by Cisco

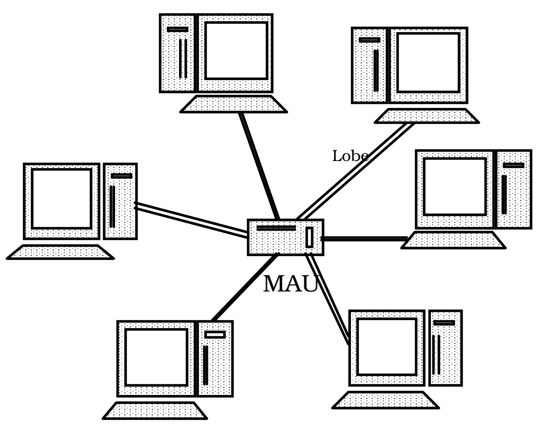
This standard defines the MAC and physical layer for a token ring. It is traditionally supported by IBM and can be implemented on twisted pair or fiber cable. When fiber is used, this technique is generally called FDDI. Copper based token rings operate at 4 or 16 Mbps with frames ranging from 4K to 16K bits. At the higher speeds, the IEEE 802.5 token ring out performs the 802.3 Ethernet. Differential Manchester encoding is used to code the bit stream.

A special bit pattern known as a token constantly circulates around the ring. Any device wishing to send information must capture the token before transmitting its packet. Once the packet is sent, the token is released to continue its orbit. This simple scheme works well for small systems but may be inappropriate for large systems with long circulation times.

One device on the ring must be designated as the active monitor in order to ensure proper operation. Some of its functions include:

- Removing unclaimed circulating data packets
- Detecting and replacing a lost or damaged token
- Maintaining ring synchronization and timing

It should be noted that the network must be connected as a logical ring but is often cabled as a physical star or hub. At the center of the hub is a MAU†, which maintains the integrity of the ring and connects to individual stations by means of lobes. The ring can be expanded by connecting more MAUs. In this way, the standard building cabling can readily be used to support a ring.



Although the most common token ring cable is STP and UTP, other cable types can be used.

† Multistation Access Unit

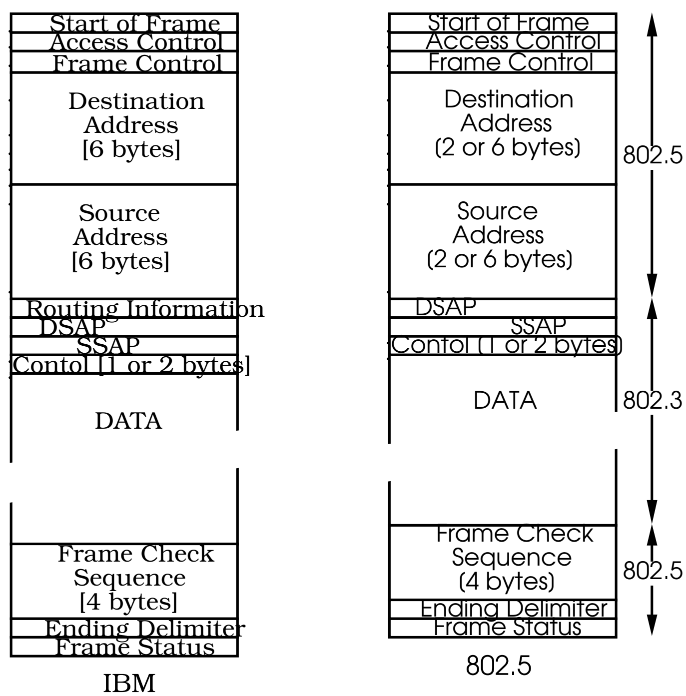
______ Notes ______

Cable Types		
Type	Max Length [meters]	Description
1	100	STP - shielded twisted pair and DB-9 connector used for lobe connections
2		Type 1 and 4 twisted pair of telephone cable
3	45	UTP - unshielded twisted pair and RJ-45 connector used for lobe connections
5		A non standard fiber optic cable used to connect repeaters
6	45	A low cost MAU to MAU cable
8	50	Used for under carpet installations
9	65	A lower cost alternative to type 1. It is a plenum jacketed data grade cable.

The token frame consists of only 3 bytes where the fourth bit in the access control field is known as the token bit.

The token ring formats developed at IBM and IEEE are nearly identical. The main difference is in the size of the address fields and routing information.

IBM and 802.5 Token Ring Formats



The token ring uses active taps. As a result, only the next station in the ring actually sees the token when it is broadcast. If a station is not going to transmit any data, it regenerates the token on its output port. If the station transmits data, that data will continue to circulate around the ring until it is removed by the originator.

6.5.5.1 FDDI

Minimum Reading

[FDDI by Cisco]

The FDDI† standard is being developed by the ANSI Accredited Standards Committee X3T9 and as an international standard by ISO/IEC/JTC1/SC 25.

The initial application for FDDI is in LANs, although there has been some speculation that it might also be suitable for MANs. FDDI is expected to dominate the high speed LAN market into the next century.[8] Some of its basic features include:[9]

- Rate: 124 Mbaud; peak data rate of 100 Mbps
- Data format: 4B/5B NRZI†
- Maximum frame size: 4,500 octets
- Addressing: 48 bits defined by IEEE 802
- Maximum number of stations: 500
- Maximum total fiber length: 100 Km
- Recommended fiber: 62.5 µm core and a cladding diameter of 125 µm with a numerical aperture of .275, with a loss < 2.5 dB/Km at a wavelength of 1.3 µm
- Optical source: 1.325 µm laser diode with a spectral width of .14 µm and an output of at least 16 dBm
- Topology: timed token dual ring

In the 4B/5B-coding scheme, 4 user bits are encoded as a 5 bit symbol. This 5-bit symbol contains at most two consecutive zeros and is transmitted using NRZI modulation. A mark is represented by a transition in the middle of the bit period, and a space by no transition. This forces at least one transition in a three bit period.

The FDDI token and frame structure is similar to 802.5.

Token

PA	SD	FC	ED

One of the major differences between 802.5 and FDDI is that the latter uses ETR†. This modification allows a station to place a token on the ring

† Fiber Distributed Data Interface

8 *The Fiber Distributed Data Interface,* Journal of Data & Computer Communications, Winter 1991

9 *An Overview of FDDI,* Journal of Data & Computer Communications, Summer 1990

† Non Return to Zero with Inversion

† Early Token Release

_____ Notes _____

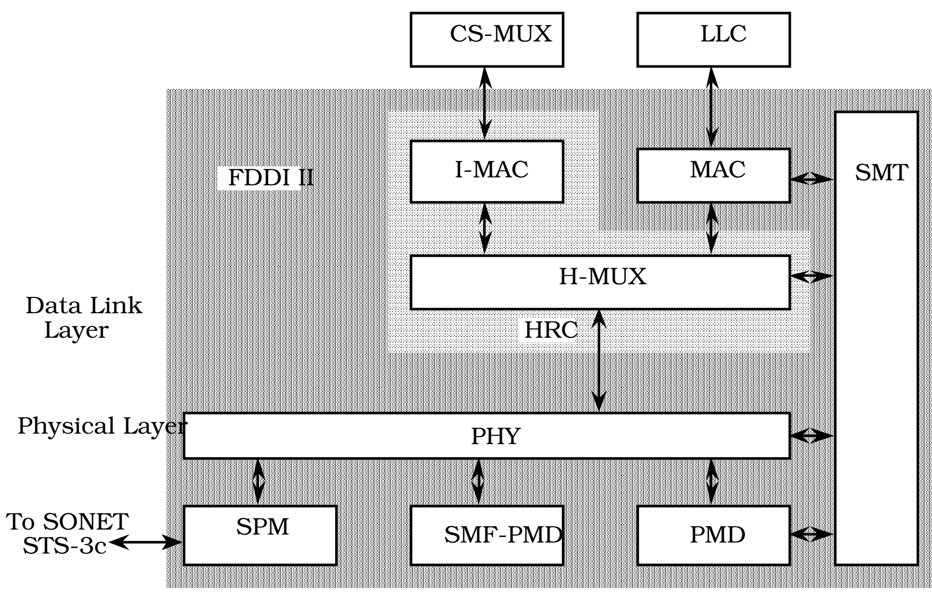
immediately after transmitting its data rather than waiting for the data to complete a circuit.

Frame

PA	SD	FC	DA	SA	DATA	FCS	ED	FS

	Segment	# of symbols [4 bits]	Function
Token Format	PA	≥ 16	Preamble
	SD	2	Starting delimiter
	FC	2	Frame control
	ED	2	Ending delimiter
Frame Format	PA	≥ 16	Preamble
	SD	2	Starting delimiter
	FC	2	Frame control
	DA	4 or 12	Destination address
	SA	4 or 12	Source address
	INFO	0 or more pairs	End-user information
	FCS	8	Frame check sequence
	ED	1	Ending delimiter
	FS	≥ 3	Frame status

FDDI is composed of two independent token rings where any terminal may communicate on either ring. A significant benefit of the dual ring is its ability to operate in a wrap around mode if a terminal fails, or to even operate as segments if there are multiple failures. An FDDI network can be configured in a number of ways, including a ring of trees.



FDDI II adds circuit switch capabilities to the packet switch nature of basic FDDI. It does this by adding a hybrid ring control [HRC] between the MAC and physical layers. The HRC is able to partition the 100 Mbps data stream into multiple streams, capable of handling packet or isochronous data. The isochronous stream can be further divided to provide up to 16 wideband channels [WBC] of 6.144 Mbps each. The WBCs can further be decomposed into multiples of 8 Kbps subchannels. This allows FDDI II to handle applications ranging from basic ISDN to high resolution video[10].

FDDI II is capable of handling a wide range of end-user and network services and can support up to 500 nodes. It is best suited for burst mode traffic. However, because of competing technologies, it remains to be seen how widely FDDI is deployed.[11]

6.5.6 IEEE 802.6 DQDB MAN

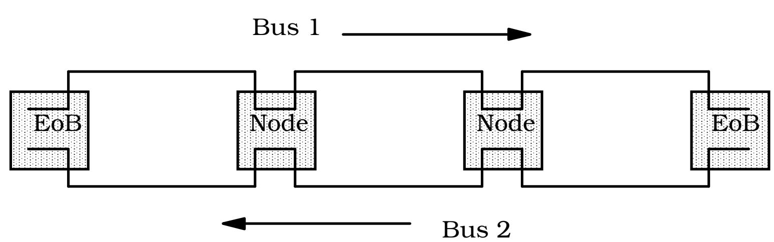
The 802.6 standard was adopted in 1990, and defines the MAC protocol for the DQDB[†] developed in Australia. It is currently being deployed in the US,[12] where it is marketed as SMDS.

The network consists of two unidirectional busses with a terminator at each end. When both ends of the dual bus are co-located, the system looks remarkably like a ring and is sometimes described as an open ring. Bridges can be used to interconnect DQDB subnets to form WANs.

A major feature of the DQDB protocol is that it can multiplex bursty LAN data, with constant bit rate traffic from PBXs. End user applications include:

- LAN to LAN interconnect
- File transfer
- Multimedia interactive computing
- Image communications

Open DQDB layout



There are two ways to access the bus:

- Pre-arbitrated access [or PA slot] - the slot is assigned by the end of bus node and is used for isochronous traffic.

10 *Fiber Distributed Data Interface an Overview,* Broadband'90

11 *FDDI finally gains backbone network prestige, but new technologies contend,* Lightwave, January, 1995

† Distributed Queue Dual Bus

12 *The IEEE 802.6 Standard for MANs, It's Scope & Purpose,* Broadband'90

- Queued arbitrated access [or QA slot] - each node implements an algorithm, which takes into account the traffic, needs of all other nodes in order to achieve some degree of fairness.

All nodes implement the arbitrated access algorithm, but only the local end of bus is able to pre-assign slots.

The BUSY bit indicates whether the cell contains user data or is idle. If a node wishes to send a packet to a node on the right, it must inform the nodes to the left of its intentions. To do this, it sets the request bit [REQ] to 1 in that direction.

Since data can be sent independently on either bus, each node contains countdown [CD] and request [RQ] counters associated with each bus.

The RQ, counts the number of requests on one bus [REQ = 1], and subtracts the number of empty slots on the other [BUSY = 0]. From this it is possible to determine the number of requests pending on that bus.

When the node wishes to enter the queue, it sets the REQ bit on the opposite bus to 1, transfers the value of the RQ to the CD, and then resets the RQ to zero. Both the RQ and CD are decremented each time an empty slot passes. Once the CD reaches zero, the node can then use the next slot to transmit. The value in the RQ then indicates the number of requests pending before transmission can begin again.

End-user data packets can be up to 9188 octets long and can use any internetworking protocol such as TCP/IP[†] and ISO IP[13]. The variable length packets are decomposed into 53 octet cells for transmission over the dual bus.

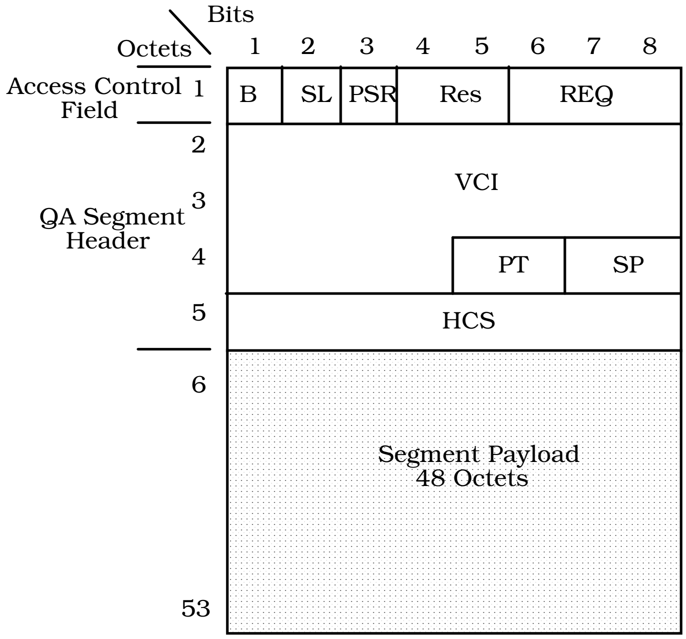
In the event of a cable break on an open dual bus network, the two segments can function independently as subnets. If the DQDB end of busses are collocated as in the looped dual bus arrangement, then a cable break forces the broken ends to assume the end of bus function, and the entire network can remain intact as an open dual bus.

---

† Transmission Control Protocol/Internet Protocol

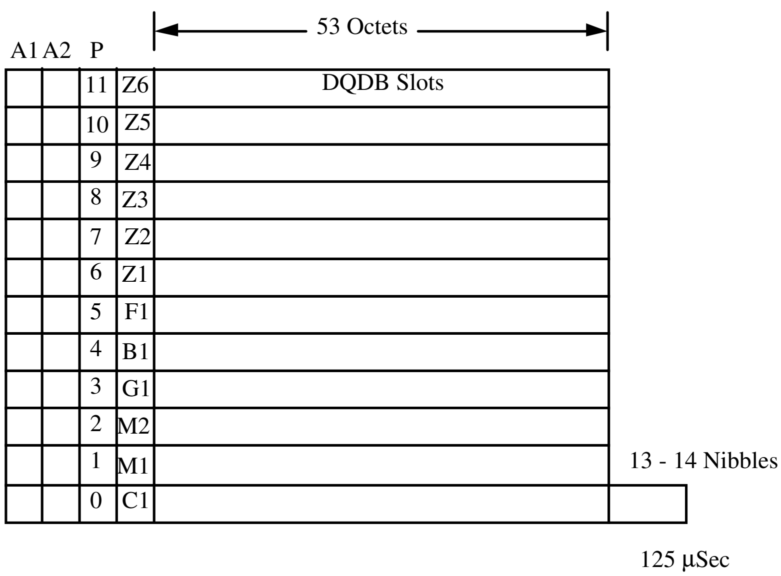
13 *Evolution of the Switched Multi-Megabit Data Service (SMDS),* Broadband (FOC/LAN)'90

DQDB Cell Structure



In order to provide isochronous [fixed rate] services, it is necessary to map these cells into a fixed 125 µSec frame. This is accomplished by defining a physical layer convergence procedure [PLCP] for DS–3 systems.

PLCP Frame Format



PLCP Bit Assignments

Bit	Function
A1	Framing Octet [11110110]
A2	Framing Octet [00101000]
P0 - P11	Path Identifier Octets
Z1 - Z6	Growth Octets
F1	PLCP Path User Channel
B1	BIP-8
G1	PLCP Path Status
M1 & M2	DQDB Layer Management Information Octets
C1	Cycle/Stuff Counter

Systems applications include:

- Public MAN
- Private backbone network
- Subscriber to network interface
- Centralized switch
- Distributed MAN switching system
- Inter-exchange carrier system

The 802.6 protocol can support three service classifications:

- Connectionless data service [datagram]
- Connection oriented data service [virtual circuit]
- Isochronous service [circuit switched]

SMDS†

SMDS by Cisco

Bellcore has taken the lead in defining SMDS standards in the form of TA†s and TS† s.

SMDS Documents & Standards	
Document	Comments
TA 1061	Procedures for LATA interconnect
TR-TSY-000 772	Subscriber network interface requirements
TR-TSY-000 773	Subscriber network interface requirements

Initially SMDS offers only connectionless service for LAN interconnect.

† Switched Multimegabit Data Service

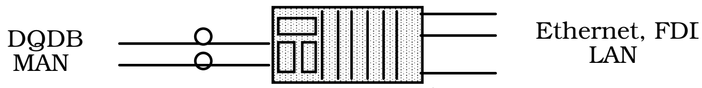
† Technical Advisory

† Technical Requirement

_____ Notes _____

In small networks, SMDS has little advantage over frame relay. But in large systems, SMDS provides better broadcast and network management capabilities. It is for this reason that telcos are considering creating cell relay SMDS backbones, and allowing the end-user to select frame or cell relay for their particular application.[14]

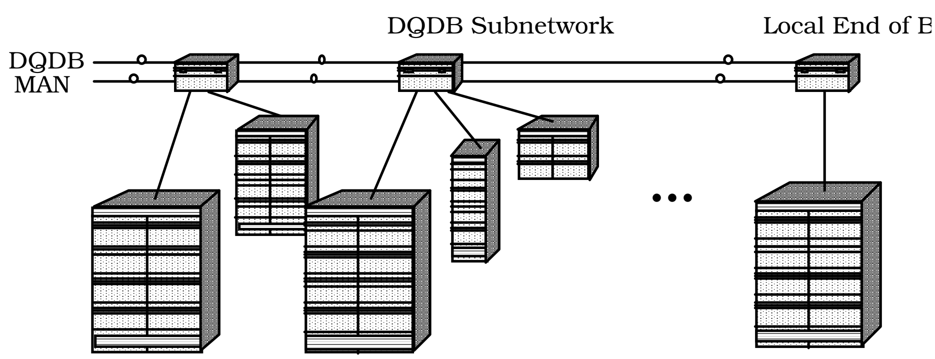
In a public SMDS network, the end-user is not compelled to using the DQDB protocol. A network access node must provide the necessary conversion to support whatever is used on the customer side.



An OC-3 link can be partitioned to provided basic services via the standard SONET TDM formats on one STS payload while offering SMDS data services on the two remaining STS payloads. This flexibility helps to protect the existing switching infrastructure, without committing equipment vendors to support any one particular transport philosophy.

The 802.6 MAN can also support DQDB subnetworks.

DQDB Subnetwork



CCITT I.121

Minimum Reading

[Sprint ATM](#)

[ATM by Cisco](#)

This standard, more commonly known as ATM, is being pioneered by CCITT Study Group XVIII as the method for providing broadband ISDN. In spite of

14 *Riding the Data Boom,* Telephony, March 18, 1991

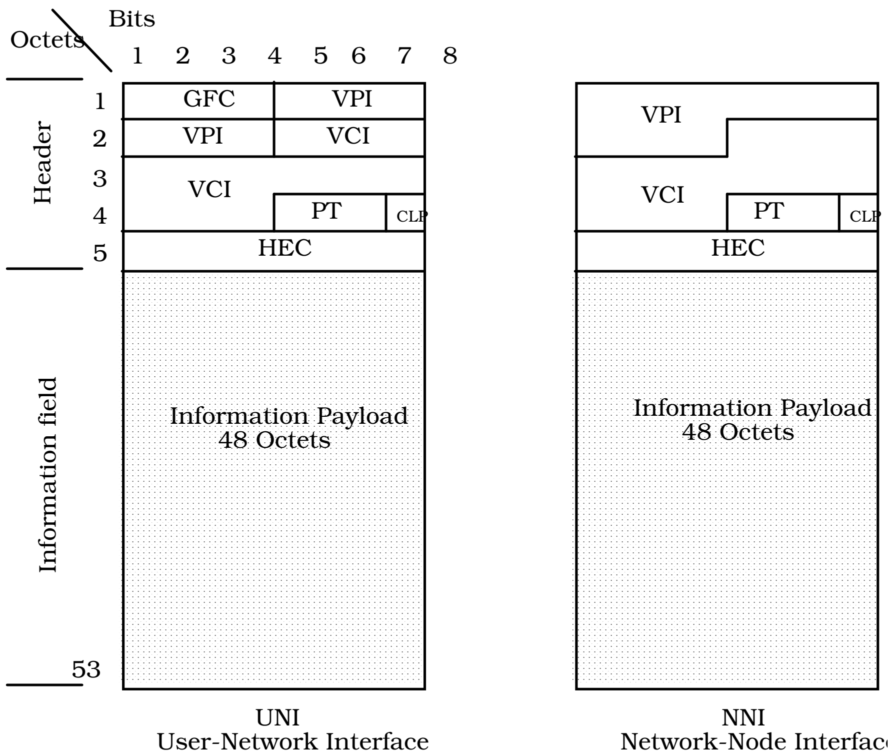
_____ Notes _____

this effort, there seems to be little consensus to create a seamless pan-European ATM network. The various PTT's are still going their own separate ways. [15]

In the US, ATM is being advocated by T1S1 and described in the MAN standard IEEE 802.6.

By definition, ATM is a connection-oriented technique utilizing fixed length packets to carry bursty information in a SONET payload. Two types of ATM cells have been defined; one for the user-network interface and the other for the network-node interface:

ATM Cell Structure[16]



Nomenclature:

GFC	generic flow control [4 bits] - regulates flow control to the customer
VPI	virtual path identifier [8 or 12 bits] - provides an explicit cell path identification
VCI	virtual channel identifier [16 bits] - provides an explicit cell channel identification

15 *European ATM Backbone: Pilot Errors*, Data Communications, January 1996

16 *Data Communications Using ATM: Architectures, Protocols, and Resource Management,* IEEE Communications August 1994, vol. 32, no. 8

PT payload type [3 bits] - distinguished between user and network information

HEC header error check [8 bits] - if a single bit header error is detected, the receiver switches into a more rigorous multi-error detect mode

CLP cell loss priority

There is currently no consensus as to how extensively ATM cells should be deployed. It may be true that as some claim, all services can be handled by this method. However, it is not intuitively obvious that a connectionless transport service should carry traditionally circuit switched narrowband services such as voice. Four basic service classes can be supported[17]:

ATM Service Categories

	Characteristics			
Class	Bit rate	Continuity	Sync	Application
A	Constant	Connection	Required	Existing services
B	Variable	Connection	Required	Variable rate video coders
C	Variable	Connection	Not required	Data communications
D	Constant	Connectionless	Not required	SMDS

There are many issues concerning ATM, which have yet to be resolved[18,19].

MAN Rings

The service provider monitors the ring and:

- Connects/disconnects users
- Removes circulating packets
- Monitors path integrity

Utilization on a fiber ring is not a great concern since:

- Fiber currently has excess bandwidth
- Unused channels can easily be stripped off
- Future services may be able to utilized the bandwidth

However, survivability is becoming a major concern, particularly for data users. Many businesses such as banks, travel agencies, stores using point of sales terminals, data banks, stock exchanges and others would come to a grinding halt if communications services were interrupted.

Accidental cable cuts are a primary cause of communications failure however; sabotage and defective software are becoming major concerns. All of these

---

17 ElectroniCast 1990

18 Conceptual Issues for ATM, IEEE 1989

19 ATM – Practical Management Issues, Br Telecom Technical Journal, vol 9 no.2 April 1991

problems can be minimized by using self-healing rings[20]. Two of the more promising methods involve:

- Diverse routing: multiple paths to the central office are provisioned
- Dual homing: a terminal homes in on two different offices. This is a much more robust, but also much more complex solution since it brings forth the question of central office sanity checking.

There are a number of different proposals to making self-healing rings.[21] Some techniques use flooding after a failure to attempt to find an alternate route, others use predefined alternate virtual paths.

Fiber rings are currently being deployed in many major cities. Sprint is planning 39 SONET rings throughout the US. To demonstrate the survivability of these rings, as a publicity stunt, Sprint deliberately cut the 4 fiber, bidirectional, line switched ring in Chicago. It took less than 60 mSec for the ring to reconfigure itself and reroute traffic.[22]

Fiber cable has often been heralded as a medium immune from eavesdropping. Unfortunately, once the cable integrity is violated and an electronic package placed in the circuit, the cable becomes very insecure.

This suggests that banks and financial institutions would prefer the more secure star structure to that of rings for telco service provisioning. The only solution to this dilemma is to encrypt the signal however; this does not address the problem of employee theft or intrusion.

6.5.7 IEEE 802.7 BBTAG

The Broadband Technology Advisory Group is helping to identify changes in broadband technology and how they affect the 802 standards.

6.5.8 IEEE 802.8 FOTAG

The Fiber Optic Technology Advisory Group is helping to identify changes in fiber optic technology and how they affect the 802 standards.

6.5.9 IEEE 802.9 IVD/LAN

This group is defining the MAC and physical layer specifications for integrated voice and data LANs, MANs, and ISDN.

---

20 *Telcos in the Trenches: Defensive Strategies for Offensive Actions,* TE&M, July 15, 1991

21 See IEEE Communications, vol. 33 no. 9, September 1995

22 Lightwave, February 1995

isoEthernet

Iso-Ethernet[23] or isochronous ethernet is being developed under the IEEE 802.9a standard. It adds a 6.144 Mbps switched ISDN C channel to the standard 10 Mbps ethernet P channel. The C channel is used to support isochronous services for multimedia applications and ISDN Q.931 signaling.

The P channel uses the same frame structure and CSMA/CD access as regular Ethernet. However, the C channel functions as a full-duplex isochronous ISDN link. Iso-Ethernet can operate in either 10Base-T mode or in all-isochronous mode.

The C channel is divided into 96, 64 Kbps ISDN B channels and one 64 Kbps ISDN D channel. Isochronous applications can request and aggregate B channels as needed but the D channel is reserved for call control and signaling.

PCs are connected to an iso-Ethernet hub or access unit (AU) via two pairs of Category 3 or Category 5 UTP wiring in a star topology. The AU, can function in a standalone LAN environment or provide the access to a private or public WAN backbone.

Iso-Ethernet uses 4B5B NRZI line coding. This enables it to achieve an average bandwidth utilization of 0.8, compared with the 0.5 afforded by Manchester encoding.

The iso-Ethernet standard defines three modes of operation:

- 10BaseT
- Multiservice
- All isochronous

10Base-T Mode

The physical layer behaves exactly like an 802.3 Ethernet, using Manchester encoding and using standard twisted pair transceivers. It provides only the 10-Mbps P channel for packet data traffic.

Multiservice Mode

Bandwidth is divided into the 10-Mbps P channel for Ethernet data packets and the ISDN C channel for 6.144 Mbps of full-duplex ISDN circuits, including the 64-kbit/s D channel for call control and signaling.

All Isochronous Mode

The total 16.144 Mbps of bandwidth is used for circuit-switched C-channel ISDN services, effectively providing 248, 64 Kbps ISDN B channels. All-isochronous mode is particularly useful for videoconferencing workgroups. It can also be used for real-time full-motion video applications.

---

[23] Data Communications, July 1995, *Iso-Ethernet: Bridging the Gap From WAN to LAN*, by Richard Brand

All three iso-Ethernet modes can run simultaneously on a common hub. However, an end-station connected to a hub port configured for all-isochronous operation can't communicate with an end-station attached to a hub port configured in 10Base-T.

6.5.10 IEEE 802.10 SILS

This group is writing the standards to address security procedures and mechanisms for security over interconnected LANs.

6.5.11 IEEE 802.11 Wireless LANs

This group is writing the MAC and physical layer specifications for radio or infrared based LANs.

_____ Notes _____

The following information comes unedited from IEEE.

Wireless Ethernet (IEEE 802.11)

This standard defines WLANs operating at 2.4 GHz. Originally 802.11 specified operation at 1 and 2 Mbps using FHSS, DSSS, and infrared. 802.11b allows operation up to 11 Mbps and 802.11a defines operation at 5 GHz with data rates up to 54Mbps.

Learn more about the IEEE's 802.11 standards and WLAN Working Groups by visiting their website at http://grouper.ieee.org/groups/802/11/

IEEE 802.11b

This extension to the 802.11 standard, adopted in 1999,allows data rates of 5.5 and 11 Mbps in the 2.4 GHz spectrum. This extension is backwards compatible to the original 802.11 standard (only DSSS systems; not FHSS or Infrared systems) but adopts a new modulation technique called Complementary Code Keying (CCK), which allows the speed increase. The 802.11b standard defines only one modulation technique for the faster speeds – CCK – unlike the original 802.11 standard that allowed DSSS, FHSS and Ir. Because CCK is the only specified technique in the 802.11b standard, any equipment, despite the brand or make, will interoperate as long as it meets the 802.11b specification. This advantage is leveraged by the creation of the Wireless Ethernet Compatibility Alliance (WECA), an organization that has set up a certification lab to test 802.11b equipment. When such equipment is certified by WECA, it can carry the Wi-Fi brand on its packaging. Additionally, 802.11b systems are backward compatible with 802.11systems.

Frequency Range:	2.4 to 2.4835 GHz
Air Access:	Direct Sequence Spread Spectrum (DSSS) using Complementary Code Keying (CCK)
Data Rate:	up to 11 Mbps
Compatibility:	Compatible to 802.11 DSSS 1 and 2 Mbps systems. Not compatible with 802.11 FHSS, Infared (Ir) systems or HomeRF
Operating Range:	depends on installation and obstacles, up to 500 m
Applications:	all LANs (wireless Ethernet)

Learn more about the IEEE's 802.11g at http://grouper.ieee.org/groups/802/11/ - Select Task Group G

IEEE 802.11g

IIEEE 802.11g brings data rates as high as 54 Mbps to the 2.4 GHz band. Of equal importance, it ensures backward compatibility with existing Wi-Fi equipment in that band. For owners of existing Wi-Fi equipment, IEEE 802.11g provides a smooth migration path to higher data rates, thus extending the life of 2.4 GHz equipment. The 802.11g Draft Standard adopted at the November, 2001 IEEE 802 meeting contains both mandatory and optional elements.

1. Mandatory: Orthogonal Frequency Division Multiplexing (OFDM) is a mandatory part of the Draft Standard. The 802.11g Draft Standard ensures that OFDM will be deployed in standards-based solutions in the 2.4 GHz band. OFDM enables the higher data rates to 54 Mbps.

2. Mandatory: Backward compatibility with existing 2.4 GHz Wi-Fi (802.11b) radios is a mandatory requirement. Use of Compementary Code Keying (CCK) ensures this to be so.

3. Optional: The 802.11g Draft Standard includes both Packet Binary Convolution Coding (PBCC) and CCK/OFDM as optional elements. CCK/OFDM means each data packet has a CCK coded preamble and header with an OFDM coded payload (message). Standards-based designs will be required to include both OFDM (#1) and CCK (#2), but need not include either option (#3).

Frequency Range:	2.4 to 2.4835 GHz
Air Access:	Mandatory Complementary Code Keying (CCK) and Orthogonal Frequency Division Multiplexing (OFDM), Optional Packet Binary Convolution Coding (PBCC) and CCK/OFDM
Data Rate:	up to 54 Mbps
Compatibility:	Backward compatible with 802.11b. Not compatible with 802.11 FHSS, Infrared (Ir), or HomeRF

Learn more about the IEEE's 802.11g Working Group by visiting their website at http://grouper.ieee.org/groups/802/11/ - Select Task Group G

5 GHz Wireless LAN/WAN (IEEE 802.11a)

IEEE 802.11a is the IEEE wireless LAN standard that applies to the 5 GHz Unlicensed National Information Infrastructure (UNII) band. This standard specifies the use of Orthogonal Frequency Division Multiplexing (OFDM) for data transmission at rates up to 54 Mbps.
There is a European standard, which is uses a very similar PHY to 802.11a, called HiperLAN2 (see more details below). Also related is work being done by the IEEE 802.11 Task Group H, which was formed to address the regulatory issues with 802.11a that prevent acceptance by European agencies. These issues are Dynamic Frequency Selection and Transmit Power Control. (DFS/TPC). Another 802.11 Study Group (the 5GSG) has formed to address interoperability between 802.11a and HiperLAN with an objective of defining anew this serious problem in an effort to make the two standards compatible and to make 802.11a into a global standard for the 5GHz band.

Frequency Ranges & Power:	5.15 to 5.25 GHz (50 mW), 5.25to 5.35 GHz (250 mW) and 5.725 to 5.825 GHz (1 W)
Air Access:	Orthogonal Frequency Division Multiplexing (OFDM)
Data Rates:	up to 54 Mbps
Compatibility:	Not compatible with 802.11, 802.11b, HomeRF, HiperLAN/2
Operating Range:	depends on installation and obstacles
Applications:	Wide Area Networks and Local Area Networks (data, voice, video)

Learn more about the IEEE's 802.11a Working Group by visiting their website at http://grouper.ieee.org/groups/802/11/ - Select Task Group A

6.5.12 IEEE 802.15

Wireless Personal Area Network (IEEE 802.15)

The 802.15 Wireless Personal Area Network (WPAN™) working group focuses on the development of consensus standards for Personal Area Networks or short distance wireless networks. WPANs are used for the wireless networking of portable and mobile computing devices such as PCs, Personal Digital Assistants (PDAs), peripherals, cell phones, pagers, and consumer electronics. The goal of this working group is to publish WPAN standards that have broad market applicability and deal effectively with the issues of coexistence and interoperability with other wired and wireless networking solutions.

Learn more about IEEE 802.15 WPAN at http://www.ieee802.org/15/

6.5.12 IEEE 802.16

Fixed Broadband Wireless Access (IEEE 802.16)

The mission of the 802.16 Working Group is to develop standards and recommended practices to support the development and deployment of fixed broadband wireless access systems. IEEE 802.16 is a unit of the IEEE 802 LAN/MAN Standards Committee.

Learn more about IEEE 802.16 at http://www.ieee802.org/16/

_____ Notes _____

European 5 GHz/54 Mbps WAN (HiperLAN2)

HiperLAN2 is being developed under the European Telecommunications Standardization Institute (ETSI) Broadband Radio Access Networks (BRAN) project. HiperLAN2 is similar to IEEE 802.11a in that both apply to the 5 GHz band and both use Orthogonal Frequency Division Multiplexing (OFDM) to attain data rates as high as 54 Mbps.

Differences between the two standards exist primarily in the medium access control (MAC) portion of the systems. HiperLAN2 is connection oriented. Air connections are time division multiplexed (TDM). Each channel, or connection, can be assigned an appropriate quality of service (QoS) based on need (type of data being transmitted such as voice or video). Because of its broadband and channel diversity/QoS capabilities, HiperLAN2 will first be used for major WAN interconnections between nodes. Currently, IEEE 802.11a does not offer channel diversity with variable QoS and is closely compared to wireless Ethernet whereas HiperLAN2 is regarded as wireless asynchronous transfer mode (ATM).

Frequency Range:	5.15 to 5.35 GHz and 5.470 to 5.725 GHz
Air Access:	Orthogonal Frequency Division Multiplexing (OFDM)
Data Rates:	up to 54 Mbps
Compatibility:	Not compatible to 802.11, 802.11b,802.11g, HomeRF
Operating Range:	depends on installation and obstacles, 150m maximum
Applications:	WAN/LAN, packetized voice, video, data

Learn more about HiperLAN2 by visiting the HiperLAN2Resource Center at http://www.palowireless.com/hiperlan2/about.asp or the HiperLAN2 Global Forum at http://www.hiperlan2.com/

Short Distance Device Interconnectivity (Bluetooth)

Bluetooth (BT) is a de facto standard established by a group of manufacturers. It was named after the 10th century Viking king, Harald Bluetooth who united his kingdoms of Denmark and Norway. In February of 1998, the Bluetooth Special Interest Group (BT-SIG) was formed to develop the standard. This standard is intended to complement, not compete with, IEEE 802.11b since BT is for personal area networking (PAN) while 802.11 applies to wide area and local area networking. BT is designed to allow laptops, PDAs, cellular phones, and other devices to exchange data in a close-range (10 m max.) ad-hoc network. BT uses quick frequency hopping at 1600 hops per second in the 2.4 GHz band and a data rate of 721 kbps. Transmitted power is limited to a very low 1 mW. Bluetooth is intended to be a replacement for Infrared (Ir) and cables.

Since both Bluetooth and IEEE 802.11b operate in the same2.4 GHz band, there can be interference between systems operating simultaneously and in close proximity. Typically, this interference will result in slower performance of the affected systems. Intersil is working with Silicon Wave on a chip solution that integrates an 802.11b and BT radio with multiplexed operation to ensure no interference.

Frequency Range:	2.400 to 2.4835 GHz
Air Access:	Frequency Hopping Spread Spectrum (FHSS)
Data Rate:	V1.1 - 721 kbps, V1.2 – 10 Mbps
Compatibility:	Not compatible with any of the other WLAN standards (802.11, HomeRF, HiperLAN/2
Operating Range:	10 meters or a little over 30 ft. maximum
Applications:	Hands-free wireless phone, PDAs, Laptops (Personal Area Network (PAN))

Learn more about Bluetooth by visiting their website at http://www.bluetooth.com/

HomeRF Wireless LAN

HomeRF is the banner name for a group of manufacturers that formed in 1998 to develop a standard for the wireless interconnection of homePCs and electronic devices. The resulting specification is called the Shared Wireless Access Protocol (SWAP). HomeRF was originally formed because these companies believed a full 802.11 radio would be too costly for home and consumer markets. In fact, this belief has been dispelled by the rapid adoption of 802.11 systems and an aggressive march down the cost curve. Furthermore, HomeRF's philosophy is that there does not need to be compatibility between home and work systems, a philosophy not shared by most systems providers. Systems based on 802.11 dominate the workspace and many believe that workers with 802.11-equipped laptops will want a compatible system at home. The original HomeRF SWAP protocol was capable of delivering only about 1.6 Mbps raw data rates. The adoption of IEEE802.11b,with 11 Mbps as a top speed, made HomeRF a hard sell. To address that, a new technique described in the HomeRF 2.0 protocol, employs what is called wide band frequency hopping (WBFH). Even so, most key supporters of HomeRF have now deployed 802.11b solutions and support for HomeRF has dwindled along with a declining market share.

Wide Band Frequency Hopping (WBFH)

Approved by the FCC in August of 2000, WBFH permits channel bandwidths as wide as 3 and 5 MHz instead of the prior 1 MHz in the 2.4 GHz band. This increased bandwidth allows data rates as high as 10 Mbps per channel as compared to the original 2 Mbps maximum per channel (roughly 2 Mbps per 1 MHz of channel bandwidth). HomeRF 2.0 products and other Frequency Hopping Spread Spectrum (FHSS) products benefit from this. However, Direct Sequence Spread Spectrum (DSSS) systems, such as promoted by Intersil and other WECA members, still dominates with 11 Mbps and possibly 54 Mbps Turbo modes. There is very limited support for WBFH technology among systems providers.

Frequency Range: 2.4 GHz

Air Access:	Frequency Hopping Spread Spectrum (FHSS)
Data Rates:	0.8 Mbps, 1.6 Mbps, 5 Mbps, 10 Mbps, (20 Mbps by2002)
Compatibility:	Not compatible with 802.11, 802.11b,802.11g, 802.11a, HiperLAN/2
Operating Range:	claims vary, depend on obstacles, up to 150 m
Applications:	Home LAN, Home networking of all electronic appliances

Learn more about HomeRF by visiting their website at http://www.homerf.org/

6.6 Network Control and Routing

For Advanced Students

- WANs by Cisco
- Bridging & Switching by Cisco
- Routing by Cisco
- Network Management by Cisco
- SNA Routing by Cisco
- OSI Routing by Cisco
- IBM Network Management by Cisco

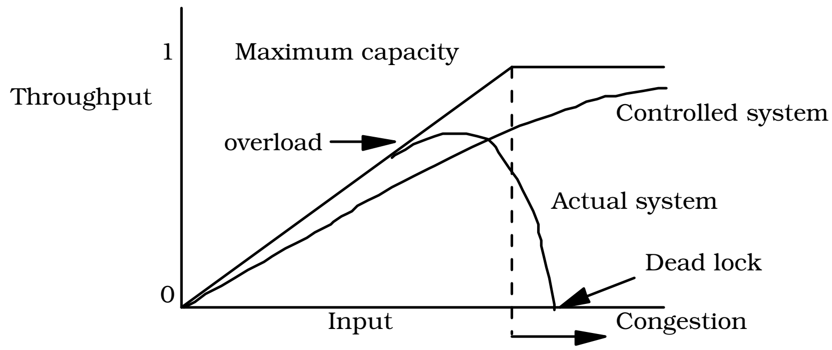
There are numerous aspects of the network which require some form of intervention or rules to ensure a fair and equitable sharing of resources. Some things requiring control include:

- Traffic
- Flow
- Congestion

6.6.1 Traffic Control

Packet switches generally have simpler call processing functions than class 5 PSTN offices. Since the packet contains some routing information, call setup and take down are often not required, and the system may not have to keep track of busy connections. However, congestion can occur when user demands exceed the system capacity. Consequently, flow and congestion control are needed.

_____ Notes _____



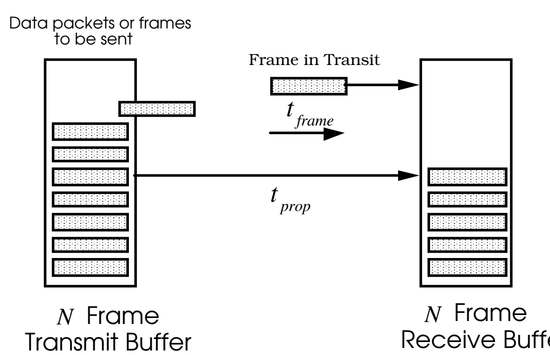
Traffic control governs the number of packets entering and using the network, and can be broken into two components, flow and congestion

6.6.2 Flow Control

The data flow between two points is controlled by the receiver. This is imposed on a link to link basis and prevents faster terminals from overloading the system, allowing transmission errors to be detected, and often corrected in route.

In some communications systems, the propagation time is quite a large and may be of the same order as the DATA period. To analyze such systems, the time taken to generate a PACK or NACK can often be ignored.

The data burst is generally organized into blocks, packets, or frames.



Utilization (U) or efficiency, can be defined as:

$$U = \frac{\text{time period of } N \text{ frames}}{\text{total transmission time for } N \text{ frames } + \text{ their ACKs}}$$

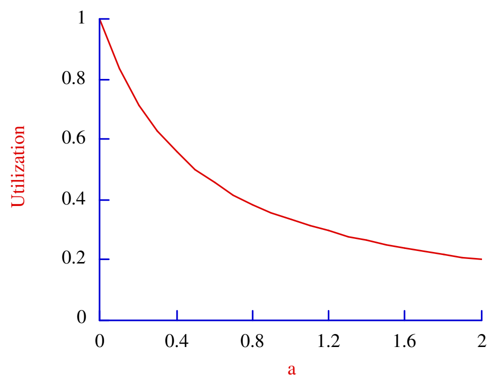
$$= \frac{Nt_{frame}}{N\left(2t_{prop} + t_{frame}\right)}$$

If the ACK time period is ignored, the time taken to transmit one frame and receive an ACK back, is equal to the frame period plus the time it takes the frame to traverse the link, plus the time it takes for the ACK to come back.

The utilization can therefore be written as:

$$U = \frac{1}{1+2a} \qquad \text{where} \qquad a = \frac{t_{propagation}}{t_{frame}}$$

Utilization vs. a



A utilization of 1, requires instantaneous communications. It can however, be nearly achieved on relatively short links. The actual propagation time is:

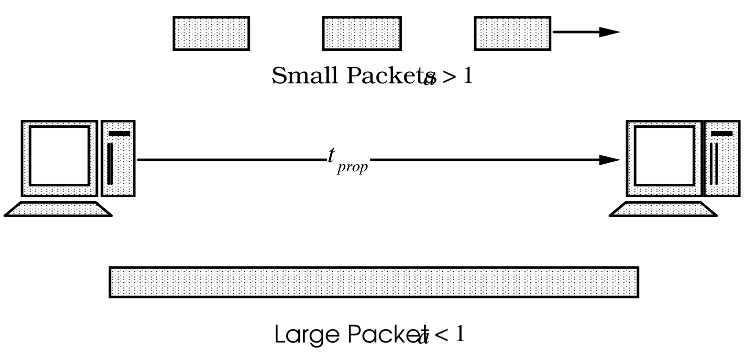
$$t_{prop} = \frac{\text{distance}}{\text{velocity of propagation}} = \frac{d}{v}$$

And since $t_{frame} = \frac{\text{frame length}}{\text{data rate}} = \frac{L}{B}$

We obtain: $a = \frac{Bd}{vL}$

If $a < 1$, the frame at some moment, occupies the entire transmission path.

If $a > 1$, the transmission path has room to spare while transmitting a frame.



Stop & Wait

In this very basic flow control protocol, the originator transmits a DATA burst and then waits for a PACK. The efficiency of a long link using this procedure is quite low.

Example: a satellite link with the following characteristics:

$t_{prop} = 0.27$ Sec

$B = 56$ Kbps

$L = 4000$ bits/frame

$v = 3\text{x}10^8$ m/sec

Has a very low utilization:

$$a = \frac{t_{prop}}{\frac{L}{B}} = \frac{0.27}{\frac{4K}{56K}} = 3.78$$

$$U = \frac{1}{1+2a} = \frac{1}{1+2(3.78)} = 0.12$$

Note what happens when the same connection is made through a local telephone loop with the following characteristics:

$d = 2$ Km

$B = 56$ Kbps

$L = 4000$ bits/frame

$v = 2\text{x}10^8$ m/sec

The utilization becomes:

$$a = \frac{Bd}{vL} = \frac{56000 \times 2 \times 10^3}{2 \times 10^8 \times 4000} = 140 \times 10^{-6}$$

$$U = \frac{1}{1+2a} = 0.99972$$

It is interesting to observe that high link utilization can be maintained even with low data rates and small frames.

Example: the utilization of a telephone link with the following characteristics:

$d = 2$ Km

$B = 9600$ bps

$L = 500$ bits/frame

$v = 2\text{x}10^8$ m/sec

is also quite high:

$$a = \frac{Bd}{vL} = \frac{9600 \times 2 \times 10^3}{2 \times 10^8 \times 500} = 0.192 \times 10^{-2}$$

$$U = \frac{1}{1+2a} = 0.9996$$

The transmitter sends a single data frame and waits for an ACK (either PACK or NACK). If it does not arrive within a predetermined interval, the frame is retransmitted.

If the transmitted data can be lost or corrupted, then it is possible that the returning ACK may also be lost or damaged. This may cause some confusion, since the transmitter will rebroadcast the frame, while the receiver assumes it is the next frame.

To overcome this situation, two slightly different ACKs may be used: ACK0 and ACK1. This allows both ends to know which frame is being acknowledged, and which is being retransmitted. This simple solution becomes inefficient for large values of a. When implemented with a sliding window protocol, it is referred to as continuous ARQ.

The utilization has to be redefined to take errors into account.

The utilization is defined as: $U = \frac{1-P}{1+2a}$

Where P = probability of a single frame being in error

Sliding Window Protocol

The utilization on long transmission paths such as satellite links, can be improved by using a sliding window protocol.

This technique increases utilization by transmitting several frames before requiring an acknowledgment. This is preferable to simply increasing the frame length since it reduces amount of DATA that would have to be retransmitted should an error occur.

Allowing the originator to send N frames before receiving a PACK also requires that it store or buffer those frames until the ACK arrives, just in case they have to be retransmitted.

The terminator sends a PACK at least once every N frames. The originator will stop transmitting if one does not arrive within that period, thus the terminator controls the rate of DATA flow, by withholding a PACK.

If the frame time is normalized to 1 ($t_{frame} = 1$) we obtain:

$$a = t_{prop}$$

If the originator starts transmission at $t = 0$, the first frame is completely received by the terminator at $t = a + 1$. If the terminator immediately sends back an ACK, it arrives back at the originator at $t = 2a + 1$.

This allows two basic situations to arise.

If $N > 2a + 1$, then the originator can send continuously since an ACK comes back before its buffer is empty.

$$\text{Consequently:} \quad U = 1$$

If $N < 2a + 1$, then the originator must pause, since an ACK will not come back before the buffer is empty.

$$\text{Consequently:} \quad U = \frac{N}{2a+1}$$

As propagation time increases, more frames must be in transit, to achieve the same utilization. For example, if the propagation time is equal to the frame length ($t_{prop} = 1$) and the terminals have a 1 frame buffer ($N = 1$), then the utilization is:

$$U = \frac{1}{2 \times 1 + 1} = \frac{1}{3}$$

However, if the link is made 10 times longer, ($t_{prop} = 10$) but the buffer size is only increased to 7 frames ($N = 7$), then the utilization is also:

$$U = \frac{7}{2 \times 10 + 1} = \frac{1}{3}$$

If the receiver detects an error, it generates an automatic repeat request (ARQ).

Go back *N* ARQ

This is a variation of continuous ARQ. When the receiver detects an error, it sends back a ACK*n* which acknowledges all data before frame *N* and disregards all subsequent ones until the error is corrected.

If an ACK*n* is lost, the next ACKm may succeed, and be received. But if all ACKs fail, then the transmitter and receiver will lose track of which group of *N* frames they are dealing with.

The utilization is define by:

$$U = \frac{1-P}{1+2aP} \qquad \text{for } N > 2a+1$$

$$U = \frac{N(1-P)}{(2a+1)(1-P+NP)} \qquad \text{for } N < 2a+1$$

Selective Repeat ARQ

If a NACK is received, only the defective frame is retransmitted. The receiver must be able to buffer all incoming frames, extract the frame in error, and reinsert it when it is retransmitted. The transmitter must also be able to transmit frames out of sequence.

To overcome possible overlap between transmit and receiving windows, and loosing N frames at a time, a valid PACK must be received within N/2 frames.

The utilization is given by:

$$U = 1 - P \qquad \text{for } N > 2a+1$$

$$U = \frac{N(1-P)}{2a+1} \qquad \text{for } N < 2a+1$$

6.6.3 Congestion Control

The number of packets must be controlled to avoid excessive queuing delays. Queue length grows dramatically if the utilization exceeds 80%.

A fundamental feature of any switching facility must be deadlock avoidance. A deadlocked system is incapable of functioning. This situation may arise in a number of ways.

Direct Store & Forward Deadlock

If a node uses the same memory space for input and output buffers, a node pair may deadlock if one node fills its buffer pool and is not able to accept any more packets. It thus prevents the originating node from being able to transmit.

Indirect Store & Forward Deadlock

This occurs if each output queue in a group of nodes connected in a loop is filled.

Reassembly Deadlock

In some systems a node must assemble all of the packets in correct sequence before delivering them to the customer. If its buffers are full but is missing part of the packet sequence, deadlock occurs.

6.6.4 Routing

There are many possible paths between source and destination in a packet network. Some attributes of a good route are:

Robustness: the ability to deliver packets when faced with localized failures and overloads.

Stability: the ability to react to changing conditions without making the situation worse.

Fairness: the ability to treat all packets or stations as equals.

Optimality: minimize a preset list of performance criteria.

Routing decisions are handled differently if the data network is implemented with a datagram or virtual circuit structure.

Datagram

In a Datagram network, the packet may be regarded as a letter, or a complete transaction in itself, thus requiring the minimum of handling. A route does not have to be established before the data packet can be sent. Since routing decisions are made on a per packet basis, a long transaction which has been broken up into datagrams, may find the various pieces taking different routes, and possibly arriving out of sequence.

Virtual Circuit

In a Virtual Circuit structure, there is the appearance of a continuous link, allowing multiple transactions, and maintaining the packet sequence. This simplifies routing since the routing decision is made only once at the start of the connection.

Another aspect to consider is where the routing decisions are made. This can be done either at a central node which acts as a master control center, or the task may be distributed to each node, providing a much more robust facility. Depending on the system, the node may be node totally ignorant of the existence of other nodes or, it may be aware of adjacent nodes, or even the entire system topology.

Routing	Comments
Fixed	All packets from one source to a given destination, follow the identical path. In the event of a node outage, an alternate route is chosen. This method has poor flexibility since it does not react to network congestion or failures in a graceful manner.
Random	A node selects only one outgoing path for retransmission, and may do so on a round robin fashion or on some probability distribution. The packet stays in the system until it is finally absorbed by the designated receiver.
Adaptive	The routing decisions become more complex as link traffic characteristics and costs are taken into account. Its variations include: isolated, distributed, and centralized adaptive routing

Each link has a cost associated with it and a route is chosen to minimize this cost. Two basic types of algorithms in use today:

Forward Search Algorithm: finds the least cost from a source node to all other nodes and is best suited to centralized routing network.

Backward Search Algorithm: finds the least cost path to a given destination from all other nodes and is best suited to a distributed routing network.

Both of these approaches converge under static topology conditions and cost. However if link costs are traffic dependent, instability may occur.

Flooding

A packet is sent by a source to each one of its neighbors. Each node then transmits the packet to all other nodes except to the one which sent it. This can cause the number of circulating packets to grow alarmingly.

To prevent blocking, the total number of times a packet is duplicated and retransmitted must be limited. This can be done if each node remembers the packets it transmitted, and discards them if they reappear. This would naturally entail a relatively large buffer space. An alternate method is to place a hop counter on the packet, and decrement it until the network diameter is reached. Each node then disregards any packet with a count of zero.

The advantage of this system is that the packet will always get through if at least one path exists, and the first packet will get through with the minimum path delay. However, since so much time is spent transmitting redundant packets, the delay may be appreciable. The main application of this type of system might be in the military where the are few nodes and the data must get through no matter how badly the system is damaged.

Flooding can also be used to gather statistical data about a system. It can also be used to implement the search algorithms to make routing decisions.

SNA[†] Routing

For Advanced Students

SNA Routing by Cisco

This arrangement defines two types of routes: explicit and virtual.

The explicit routes are fixed predetermined paths between a source and destination. There may be a number of these for each node pair.

Virtual routes are mapped onto explicit routes in a predetermined way. Only the source and destination nodes are concerned with the identity of the virtual route, since packets in transit have an explicit route number and intermediate nodes simply use a static routing table.

Virtual routes are used for real time or large file transfer applications. There are three classes of virtual routes, with up to 8 virtual routes per class, anyone of which may map onto the same explicit route. The service class is specified by the source node at the start of the session.

[†] Systems Network Architecture - developed by IBM

6.6.4.5 DNA[†] Routing

This system developed by the Digital Corporation, uses a distributed adaptive method where the user to some extent determines the cost function. The cost is based on the estimated number of hops necessary to make the connection, as well as system cost based on delay, data rate, error rate, and node capacity.

If any cost changes occur, this information is transmitted to adjacent nodes. The hop information is also used to prevent internal looping, which could conceivably occur if a node becomes unreachable because of delay information circulating in the network.

6.7 Packet Switching Protocols and Architecture

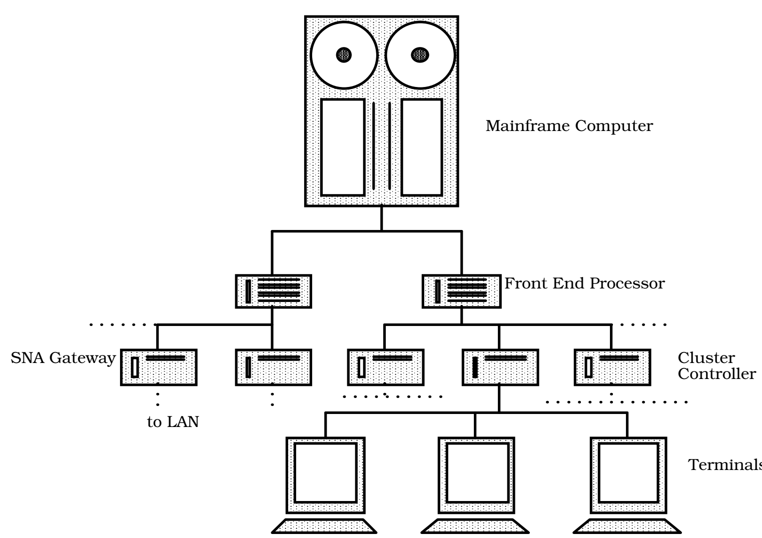
6.7.1 SNA

For Advanced Students

SNA by Cisco

SNA Routing by Cisco

The Systems Network Architecture was developed by IBM in 1974 as a way to connect an IBM host computer to a wide range of terminal types.



The majority of computer host networks in the world today are SNA based. This hierarchical structure was founded on the following assumptions:

- Computers are large, expensive, and centrally located
- Data transmission facilities are slow, expensive and unreliable
- End-user needs seldom change

[†] Digital Network Architecture

- All computing and networking equipment comes from IBM

In retrospect, it can now be readily seen that all of these assumptions proved to be false. As computing power was being down loaded to the end-user terminals, it became necessary to support direct communications without the intervention of the host mainframe. In the 1980's IBM developed APPN[†] to support better communication between end-user terminals. Unfortunately many saw this as too little too late. As a result, many corporations are now trying to either replace or modify their SNA systems to work with TCP/IP.

There are at least 3 ways to connect SNA systems to X.25 systems:

- SNA units can be encapsulated into X.25 packets by means of NPSI[†] software installed in the front end processor.
- PADs[†] are connected between the host FEP and network, and between the network and end terminal.
- If the network connecting the FEPs uses SDLC links, XI[†] can be used to do the translations

6.7.2 X.25

Minimum Reading

X.25 by Cisco

X.25 today is actually a collection of about 50 standards related to packet switching networks. It was first adopted in 1976 and has been constantly evolving. Most of the worlds X.400 messaging and E-mail services use this standard.

This network interface protocol primarily applies to the DTE - DCE interface. It is independent of user protocol, and uses asynchronous data transmission. It specifies the transmission and packet formats for establishing, maintaining, and clearing calls. This standard does not specify how a packet switch works internally, but only the format that the end-user must provide for the network.

---

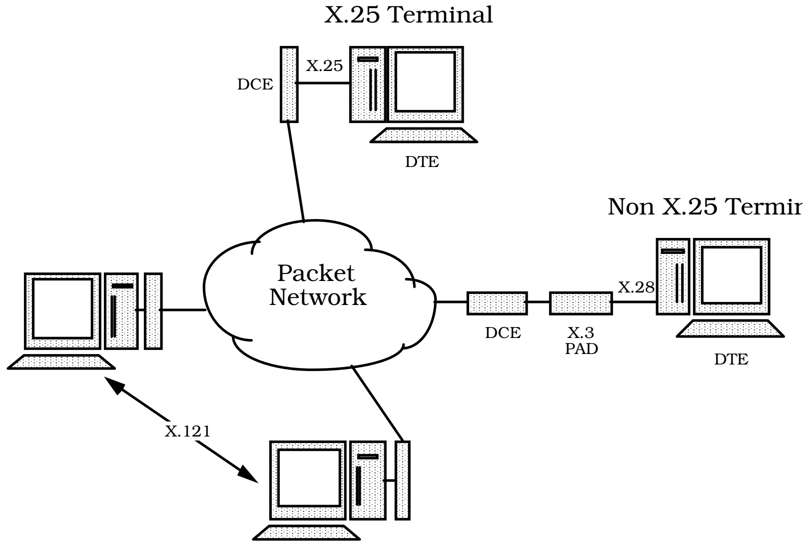
† Advanced Peer to Peer Networking

† NCP [Network Control Program] Packet Switched Interface

† Packet Assembler Disassembler

† X.25 SNA Interconnection

Notes



Standards	Contents
X.121	interconnect addressing
X.21	defines the physical interface
X.3	defines the PAD itself
X.25	defines the entry to the packet network
X.28	terminal to PAD interface
X.29	PAD to DTE interface

Two service classifications are supported:

- Virtual call service: A logical end-to-end connection is established through the packet network by means of a dial up, circuit switched path
- Permanent virtual circuit service: This is a continuous connection over a leased line facility. No call setup or clearing is required.

The X.25 standard governs the performance of layers 1, 2, & 3 in the OSI model.

Layer 1 is the physical layer. The X.25 standard recommends that the X.21 standard be used to define the physical interface. This is seldom done in practice. It is also possible to use X.26 or RS-423 for unbalanced lines, or X.27 or RS-422 for balanced lines. But RS-232 or V.35 are the most common.

Layer 2 or the data link, is implemented in a LAP-B[†] which is similar to HDLC[†]. It uses a GO BACK N protocol with both PACKs and NACKs. The window size for terrestrial links is 8, but for satellite facilities it is expanded to 128.

Error detection and correction is accomplished by means of a CRC. The binary value of the address, control, and data field is divided by a fixed number (10001000000100001 or $x^{16}+x^{12}+x^{5}+1$). The 16-bit remainder of this operation is appended to the packet. The receiver makes the same calculation and compares the two results.

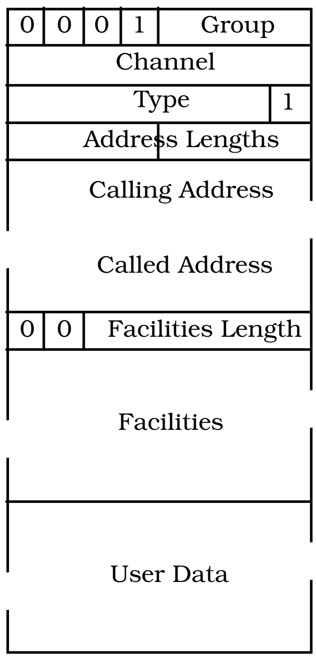
† Link Access Procedure Balanced

† High-level Data Link Control

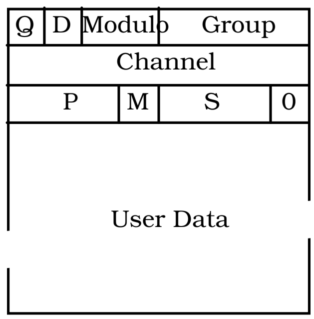
Layer 3 known as the network layer, governs the call set-up, sequencing, multiplexing, and flow control.

Flow control is implemented by means of a window whose size is determined at the time the network service is initiated. It limits the number of simultaneous packets on a given logical channel. Out-of-band signaling elements such as status inquiries, and reset or restart requests, can bypass flow control mechanisms.

X.25 Packet Format



Control Packet Format



Data Packet Format

Q - qualified data
D - delivery
P - piggyback
S - sequence
M - more

Control Packet Type Byte

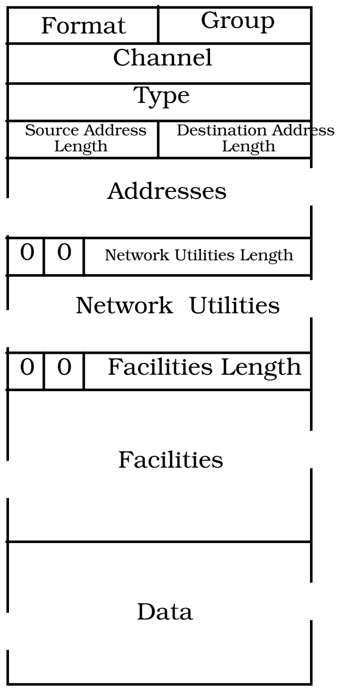
Packet Type	Bit Pattern							
	P	P	P	M	S	S	S	O
Call Request	0	0	0	0	1	0	1	1
Call Accept	0	0	0	0	1	1	1	1
Clear Request	0	0	0	1	0	0	1	1
Clear Confirmation	0	0	0	1	0	1	1	1
Interrupt	0	0	1	0	0	0	1	1
Interrupt Confirmation	0	0	1	0	0	1	1	1
Receive Ready	P	P	P	0	0	0	0	1
Receive Not Ready	P	P	P	0	0	1	0	1
Reject	P	P	P	0	1	0	0	1
Reset Request	0	0	0	1	1	0	1	1
Reset Confirmation	0	0	0	1	1	1	1	1
Restart Request	1	1	1	1	1	0	1	1
Restart Confirmation	1	1	1	1	1	1	1	1
Diagnostic	1	1	1	1	0	0	0	1

6.7.3 .X75

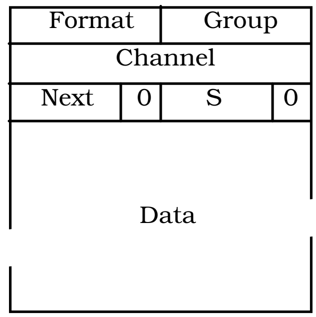
This standard specifies internetwork virtual circuit connections. It outlines the administration and management function protocols for interconnecting X.25 networks.

______ Notes ______

X.75 Packet Format[24]



Control Packet Format



Data Packet Format

A virtual circuit establishes a fixed route though a network. Call requests are broadcast along with a destination address. Each packet switching node along the way establishes a path to the next node until the destination is reached. Once data begins to flow, each node implements its part of the virtual path and translates the packet format as required.

This arrangement has a number of advantages:

- Data buffers can be reserved in advance to minimize congestion
- Data packets arrive in the correct sequence
- Short headers are used
- Delay and packet duplication are minimized

However, the system also has a few drawbacks:

- Table space is needed to remember the virtual route even when no data is being sent
- Alternate routing cannot be used to ease congestion
- Vulnerable to a single node failure
- Cannot be implemented over a data gram network

24 Based on figure 14-7, Data and Computer Communications 2nd ed., William Stallings

Fast Packet Switching

In recent years a great deal of effort has been spent in trying to improve packet performance by increasing processing and transmission speeds, reducing error rates, and reducing packet switching functions. Some of the more significant developments include:

- Introduction of RISC† processors, significantly increased processing speed
- Reduction of processing time by elimination of some networking tasks and reduced header contents
- Trellis encoding, reduces transmission error rates
- Fiber optics is less prone to interference, thus error checking requirements can be relaxed.

Two methods being considered for upgrading data networks are frame relay and cell relay. The term frame relay is unfortunate because the existing X.25 packet network is a frame relay structure.

Cell relay is also somewhat confusing since it is a generic term, but is often equated with ATM, which is specific example of cell relay.

All of these techniques fall into the broad category of fast packet and in this discussion, cell relay and frame relay will be considered generic subsets with many possible implementations. ATM will be defined specifically as CCITT I.121 in Europe and IEEE 802.6 in the United States.

6.7.3.2 Frame Relay

Minimum Reading

Frame Relay by Cisco

For Advanced Students

Frame Relay by Paradyme

Sprint Frame Relay

Frame relay is expected to increase the throughput of the existing X.25 packet switching networks by an order of magnitude, reducing the packet overhead and introducing out-of-band signaling based upon ISDN LAP-D†.

A frame relay network does not provide flow or error control, rather the end-user equipment implements these functions. The network core functions include:

- Frame delimiting

† Reduced Instruction Set Architecture

† Link Access Protocol - D channel

- Frame alignment
- Frame transparency
- Frame multiplexing & demultiplexing using DLCI
- Checking for integer number of bytes in a frame
- Checking frame length
- Detect transmission errors

Frame relay will offer connection-oriented services for LAN interconnect and high speed backbone for X.25 access.

Cell Relay

Cell relay breaks user data into small fixed length packets. Larger variable length packets, such as found in X.25 or frame relay networks can be accommodated by being segmented into cells. ATM is the preferred cell relay technique.

6.7.4 TCP/IP

Minimum Reading

IP by Cisco

TCP/IP is actually a collection of interrelated protocols, which became the first viable multi-vendor internetwork standard. IBM who had traditionally advocated its own protocols, SNA and APPN, is now also supporting the TCP/IP suite.

TCP/IP is an open environment and independent of the host hardware. Consequently it can route between different network types: Ethernet, token ring, X.25, etc. Some of its other assets include:

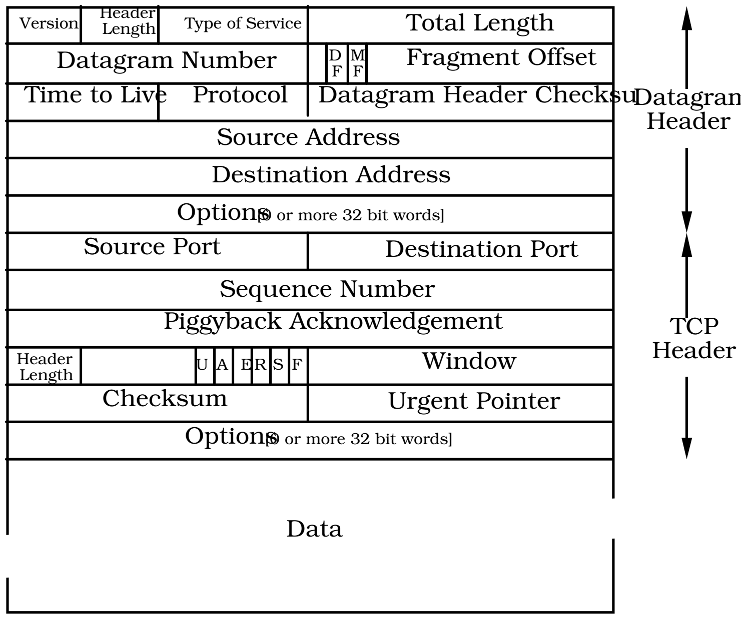
- High error tolerance in subnets
- Lower cost to operate and maintain than SNA
- Ubiquity
- Robustness

The TCP/IP protocol suite predates the OSI model. Its approximate relationship is as follows:

OSI Layer	TCP/IP and Related Protocols		
Application	File Transfer	Electronic Mail	Terminal Emulation
Presentation	FTP	SMTP	Telenet
Session			Protocol
Transport	TCP		UDP
Network	ARP	IP	ICMP
Data Link	Network Interface Cards [ethernet, token ring, etc]		
Physical	Media [twisted pair, coax, fiber, radio, etc.]		

_____ Notes _____

TCP/IP Headers[25]



DF - Don't Fragment
MF - More Fragments
U - Urgent Pointer
A - Acknowledge
E - End of Message
R - Restart
S - Connection Request
F - Finish

6.8 MPLS Multi-Protocol Label Switching

Minimum Reading

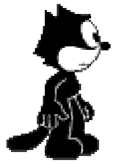
MPLS An Introduction

For Advanced Students

MPLS and ASTN
Next Generation MPLS Solutions
Using MPLS for Real-Time Services

[25] Based on figure 8-22, Computer Networks, Andrew S. Tanenbaum

Assignment Questions



Quick Quiz

1. FDDI II uses CSMA-CD. [True, False]
2. Token bus networks are used in the GM robotic assembly lines. [True, False]
3. Physical star networks [may, may not] be connected as rings.
4. Sliding window protocols are used on [long, short] links.
5. FDDI II [can, cannot] convey voice.
6. Ethernet is the same as IEEE [802.3, 802.5, 802.6]
7. At higher bit rate IEEE 802.3 out performs 802.5. [True, False]
8. Most of the world's airline reservations are currently made over the [SWIFT, SITA] network.
9. DQDB networks [can, cannot] support isochronous services.
10. Data [can, cannot] be sent independently on either bus in a DQDB system.
11. DQDB cells [can, cannot] be used on inter-exchange carrier systems.
12. A DQDB network [can, cannot] support a local end of bus in a subnetwork.
13. If the utilization of a transmission link is 0.9, the average delay is about 2 times the service time. [True, False]
14.
15. Virtual routes are used for real time file transfer applications in SNA packet networks. [True, False]
16. The [standard, slotted] ALOHA system has a peak throughput of 18%
17. The DPN-100 [does, does not] support SNA.
18. The DPN-100 comes in [1, 2, 3] product size[s].
19. The X.25 standard [is, is not] used by E-mail services.
20. Trellis coding is used by fast packet networks. [True, False]
21. While SNA continues to dominate the mainframe market, TCP/IP has taken over the internetwork market. [True, False]

Analytical Questions

1. Calculate the utilization of a fiber optic link using a Go Back N ARQ format, given the following:

Number of buffered frames:	N = 168
Bit rate:	B = 275 Mbps
Frame length:	L = 193 bits
Probability of error:	$P = 10^{-5}$
Round trip distance:	d = 8000 Km
Velocity of propagation:	$v = 2.8 \times 10^{8}$ m/Sec

   If the utilization is low, suggest how it could be improved.

2. What is the probability of 8 packets arriving in a given time interval, if the average random arrival rate during the same interval is 4? [refer to appendix 3]

Composition Questions

1. Describe the operation of a sliding window protocol.
2. Why does a system using a stop & wait ARQ protocol require two types of ACKs?
3. What are some types of routing algorithms used on packet networks?
4. List some of the things to be found in a packet header.
5. Define throughput.
6. Describe flooding as it applies to packet networks.

For Further Research

Atkins, Cooper, & Gleen, *The Evolving Art of Packet Switching*,

Gilhooly, Denis; *The Evolving Packet Network*,

Heggestad, Harold; *Telecommunications: An Overview of Packet-Switching Communications*,

Kessler, Gary C; Train, David A; *Metropolitan Area Networks: concepts, standards and services*, McGraw-Hill, New York, 1991

Marney-Petix Victoria C, *Networking and Data Communications*, Reston, 1986

Martin, James; *Systems Analysis for Data Transmission*, Prentice-Hall, (1972)

McClain ,Gary R.; *Handbook of Networking & Connectivity*, AP Professional, 1994

McDysan, David E.; Spohn, Darren L.; *ATM Theory and Application*, McGraw-Hill, New York, 1994

Ramteke Timothy; *Networks*, Prentice-Hall Career and Technology, 1994

Rosner, Roy D., Distributed Telecommunications Networks via Satellites and Packet Switching, Van Norstrand Reinhold, New York, 1982

Rosner, Roy D.; *Packet Switching: Tomorrow's Communications Today*, Van Nostrand Reinhold, New York

Saxton, Mike; Reid, Andy; *Transmission Networking: SONET and the Synchronous Digital Hierarchy*, Artech House, Boston ,1992

Stallings, William; *Data and Computer Communications* (2nd ed), Macmillan, New York, 1988

Tannenbaum, Andrew S., Computer Networks, Prentice-Hall, Englewood Cliffs, 1981

Walrand Jean, *Communication Networks: A First Course*, Irwin, Homewood, Il, 1991

Project 802 - Local & Metropolitan Area Networks, IEEE

IEEE Communications Magazine, April 1984

British Telecom Technical Journal, April 1984

"New system architecture for DPN packet switches", telesis 1988 two

ATM

http://cne.gmu.edu/~sreddiva/ATMstand.html

http://cne.gmu.edu/~sreddiva/Texttut.html

http://cell-relay.indiana.edu/cell-relay/docs/docs.html

http://www.cyberus.ca/~swanson/index.html

_____ Notes _____

Internet

http://www.merit.edu/nsf.architecture/.index.html
http://www.lidoorg.com/internetweb.htm
http://www.isoc.org/

Frame Relay

http://www.alliancedatacom.com/