Chapter Contents

7.0 Networking Infrastructure

Objectives

The purpose of this section is to:

- Examine the various transmission types
- Consider switched network issues
- Consider packet network structures

http://www.cisco.com/univercd/cc/td/doc/cisintwk/idg4/nd2013.htm

http://www.cit.rcc.on.ca/

http://

Most types of networks can support a limited amount of multimedia traffic however; few can support real-time full duplex multimedia communication. Applications such as videoconferencing are most often used as a benchmark.

Some of the basic videoconferencing requirements are:

A bi-directional throughput of about 1.5 Mbps

A maximum transmission delay of about 100 mSec

Multicast

Guaranteed QoS [quality of service]

Some LANs can meet these requirements. It is much more difficult to meet this criteria in WANs. As a result, videoconferencing is not readily available.

Nortel - Video Supertrunk Solutions

7.1 LAN Characteristics

LANs and WANs route information using packet switching techniques. However, circuit switching is more appropriate for voice and video formats. Circuit switching provides a fixed delay, and since it uses a dedicated link, does not compete for network resources.

The H.324 standard specifies how the circuit switched telephone system can support a low-grade videoconference connection over a POTS line, using. The H.320 standard defines video links over ISDN lines.

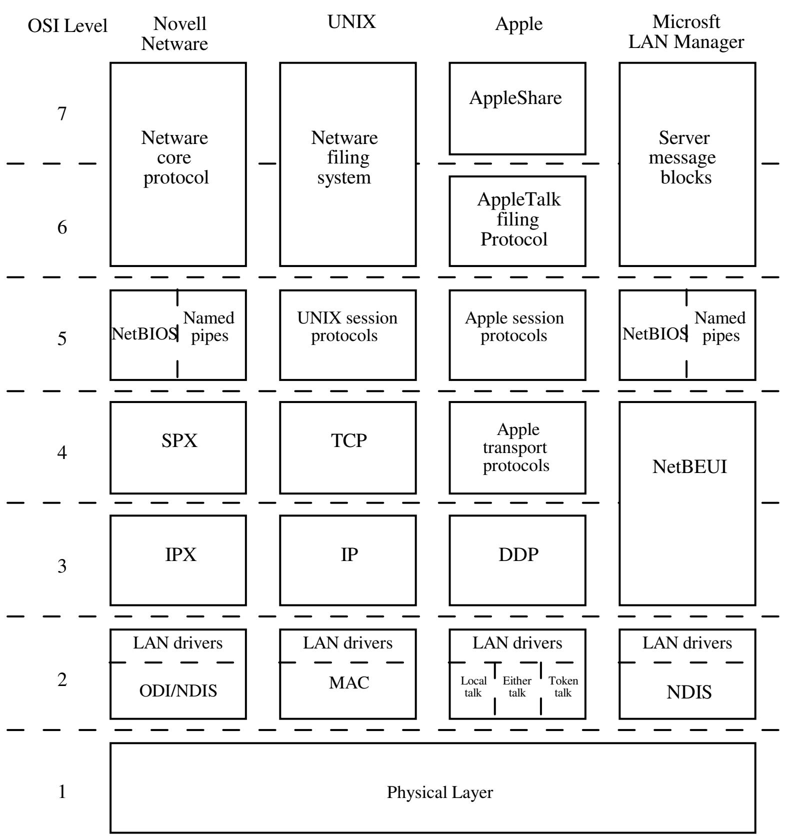
7.1.1 OSI Model

Cisco - Internetworking Basics

The OSI model provides a framework for establishing interoperability between various network types.

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

Most of the OSI model can be implemented in microprocessor-based hardware. This allows new applications, network architectures and protocols to be implemented by making software changes.

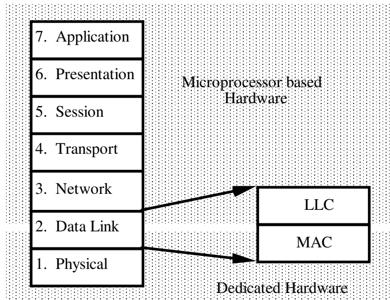


† Logical Link Control

† Media Access Control

Notes

The data link layer bridges the gap between hardware and firmware.



Significant advances have been made in physical layer interfaces. Networks are migrating from twisted pair to fiber optics. This development has introduced a host of new applications, network architectures and protocols.

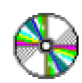
The most widely used LANs today are Ethernet, token ring, token bus, and Appletalk. They can be interconnected by gateways, routers, bridges, or repeaters to form MANs[†], which can be used to create WANs[†].

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

7.1.2 Topology

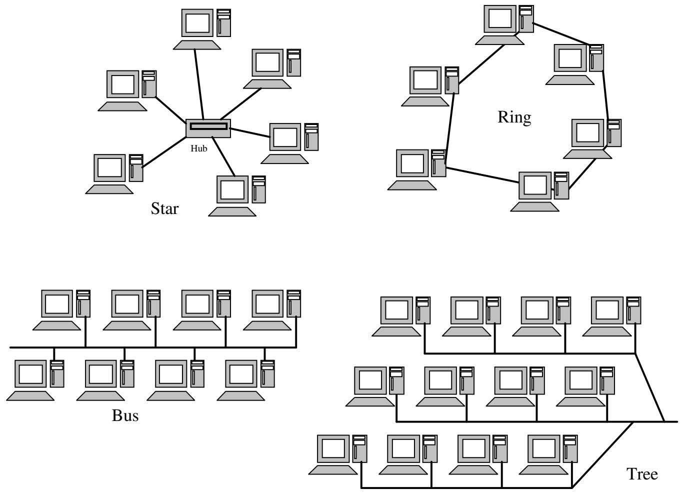
[Cisco - Introduction to LAN Protocols]



LANs can be configured in three basic ways, namely: as a ring, star, or bus. The tree topology is a variation of the bus. Cable TV is deployed over a tree network.

† Metropolitan Area Networks

† Wide Area Networks



7.2 IEEE LAN Standards

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

LAN standards have not been developed to transport video. However, a number can be used for this purpose.

7.2.1 IEEE 802.3

Cisco - Ethernet Technologies

The 802.3 standard defines the MAC and physical layer for a CSMA/CD bus. The standard was originally intended to operate on coaxial cable, but has since been modified to operate on UTP and fiber. Because of the long propagation times, it is not used on satellite networks. However, it is interesting to note that the technique was pioneered as ALOHA on satellite systems, and is widely used as a random access method on wireless data networks.

Notes

IEEE 802.3 Networks[1]

	Comments
10BASE5	10 mm, 50 Ω, coax, 500m segment
10BASE2	5 mm, 50 Ω, coax, 185m segment
10BASE-T	2 twisted pairs, 100m segments
1BASE5	Twisted pair, 500m segment
10BROAD36	Coax, 1800 m segment
10BASE-F	Fiber optics, 4 km segment
100BASE-TX	2 Twisted pair, 4B5B, NRZ-I
100BASE-FX	2 Fibers, 4B5B, NRZ-I
100BASE-T4	4 Twisted pair, 8B6T, NRZ
100VG-AnyLAN	Twisted pair

The IEEE designation has the following meaning:

- 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 computer terminal to Ethernet:

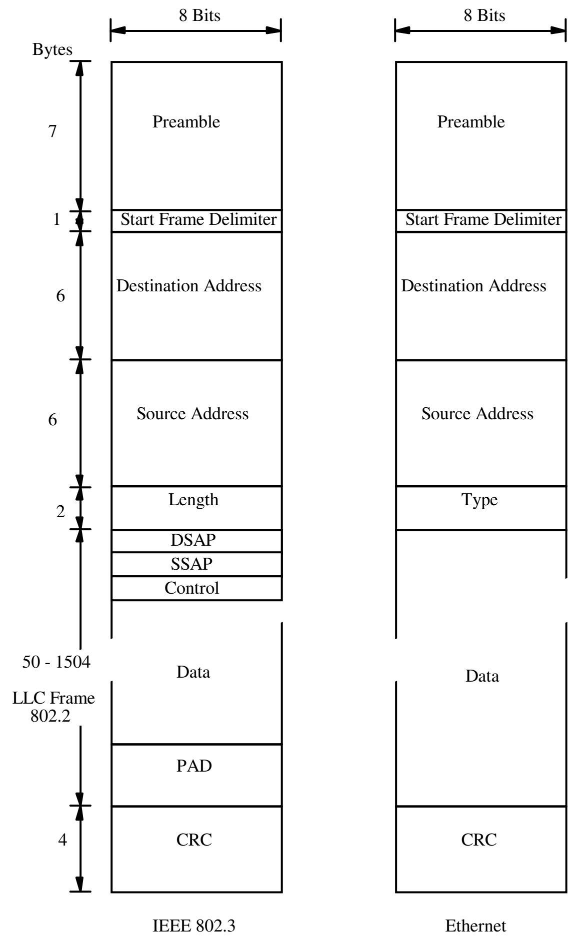
- Interface board - this is located in the computer and performs the framing and encoding functions.
- AUI[†] or Transceiver - this is connected to the interface board by a drop cable [up to 50 meters long]. It performs the collision detection and provides the electrical interface to the local segment.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

1 *Communications Networks*, Jean Wairand

† Attachment Unit Interface

Notes

Frame Structure



The 802.3 frame is followed by silence lasting 96 bit periods.

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 [a random 32 – 42 bit sequence] to alert other nodes of the collision. The colliding parties then attempt a retransmission after a random period.

The random timer uses a binary back-off algorithm. Both devices choose an 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.

100Base-T can be used to support limited video conferencing. However, since it uses CSMA, delay and bandwidth requirements cannot be guaranteed.

IsoEthernet

See IsoEthernet by Ross et. al.

IsoEthernet is variation of ethernet. Each terminal is assigned part of a dedicated 10 Mbps channel containing several isochronous 64 Kbps channels. A hub switches these channels between terminals. The 64 Kbps channels can also be routed through the ISDN.

The isochronous channels can support multimedia communications.

100VG AnyLAN

The term means:

- 100 - 100 Mbps
- VG – voice grade lines (UTP-3)
- AnyLAN – supports multiple frame types (802.3, 802.5)

This system generally uses 4 pairs of wires and 5B6B NRZ coding.

Switched Ethernet

This enhancement shares a switch rather than sharing the transmission media. The switching hub may support a throughput of 9 Mbps, thus making it usable for multimedia communications.

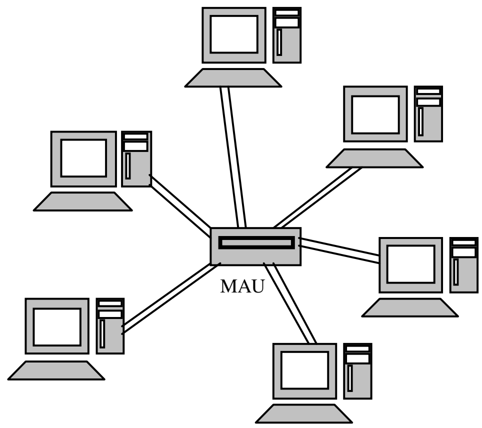
7.2.2 IEEE 802.5 Token Ring

- Cisco - FDDI
- Cisco - Token Ring

This standard defines the MAC and physical layer for a token ring over UTP or fiber. 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. Differential Manchester encoding is used to code the bit stream.

Any terminal wishing to send information must capture the token before transmission. Once the packet is sent, the token is released to continue its orbit. This arrangement works reasonably well for data transmission, but for multimedia communications, delay sensitive packets have to be given some sort of priority.

Logical rings are most often cabled as a physical star or hub. At the center of the hub is a MAU[†] that 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.

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.

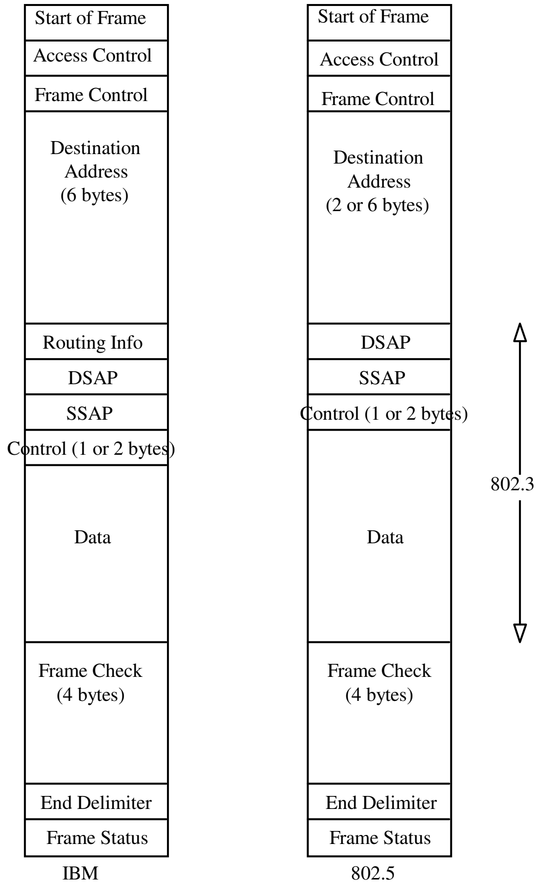
The token frame consists of only three bytes where the fourth bit in the access control field is known as the token bit.

Start of Frame
Access Control
End Delimiter

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.

† Multistation Access Unit

IBM and 802.5 Token Ring Formats



The token ring uses active taps. Therefore, 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 terminal transmits data, it circulates around the ring until it is removed by the originator.

A 16 Mbps token ring is capable of supporting video conferencing. Unfortunately, if is not very scalable.

FDDI

The FDDI[†] standard is being developed by the ANSI Accredited Standards Committee X3T9 and as an international standard by ISO/IEC/JTC1/SC 25. Some of its basic characteristics are:[2]

- Rate: 124 Mbaud; peak data rate of 100 Mbps
- Data format: 4B/5B NRZI[†]
- Maximum frame size: 4,500 octets

---

† Fiber Distributed Data Interface

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

† Non Return to Zero with Inversion

- 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 0.275, 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

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

Frame

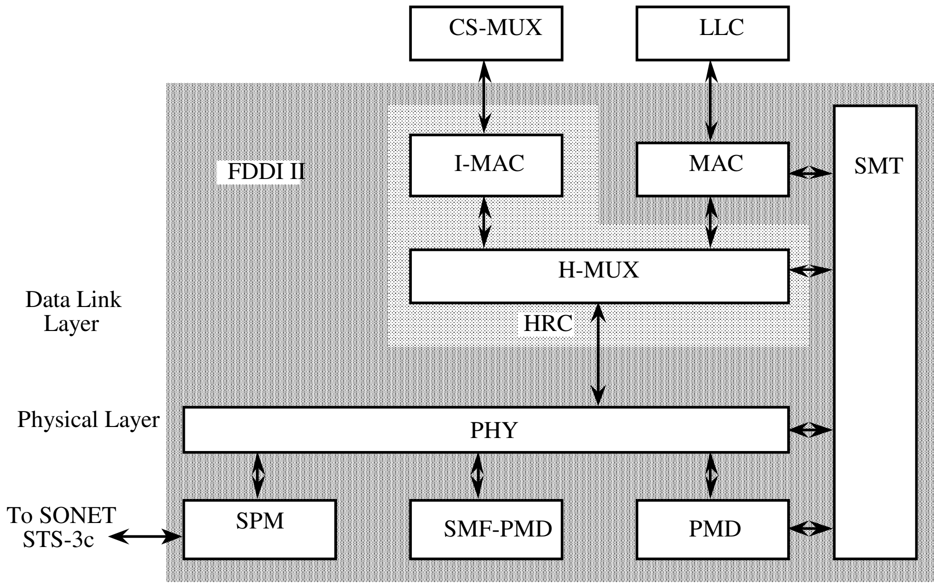
PA	SD	FC	DA	SA	DATA	FCS	ED	FS

	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.

† Early Token Release

FDDI II



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 sub-channels. This allows FDDI II to handle applications ranging from basic ISDN to high-resolution video[3].

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.[4]

7.2.3 IEEE 802.6 DQDB MAN

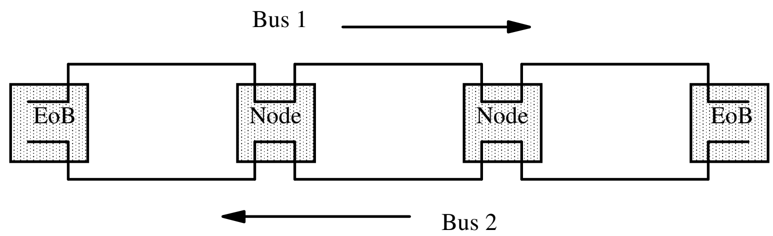
Cisco - SMDS

An 802.6 DQDB[†] network has two unidirectional busses with a terminator at each end. When both ends of the dual bus are co-located, the system is called an open ring.

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

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

† Distributed Queue Dual Bus



There are two ways to access the bus:

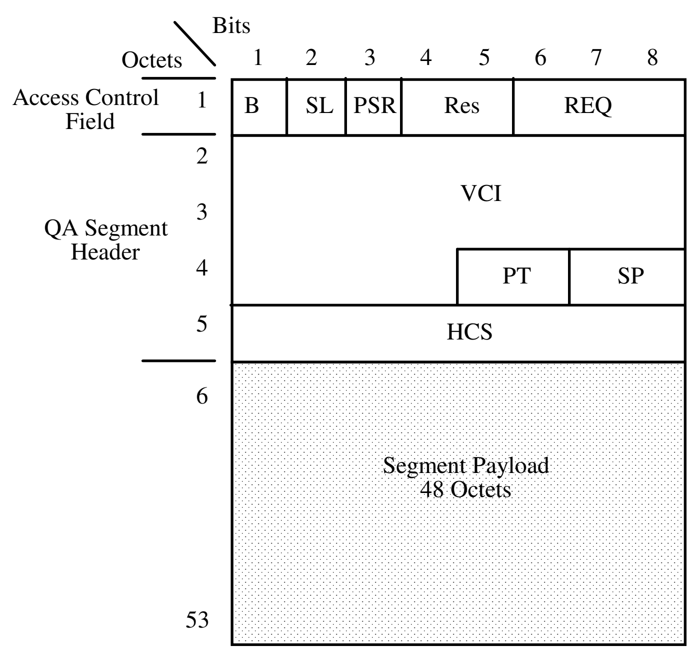
- Pre-arbitrated access [or PA slot] - the slot is assigned by the end of bus node and is used for isochronous traffic.
- Queued arbitrated access [or QA slot] - each node implements an algorithm which takes into account the traffic needs of all other nodes in order to achieve some degree of fairness.

Broadcasting or multicasting isochronous channels requires allocating symmetrical up and down stream channels. This is not currently available.

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

End-user data packets can be up to 9188 octets long and can use any internetworking protocol such as TCP/IP[†] and ISO IP[5]. The variable length packets are decomposed into 53 octet cells for transmission over the dual bus.

DQDB Cell Structure

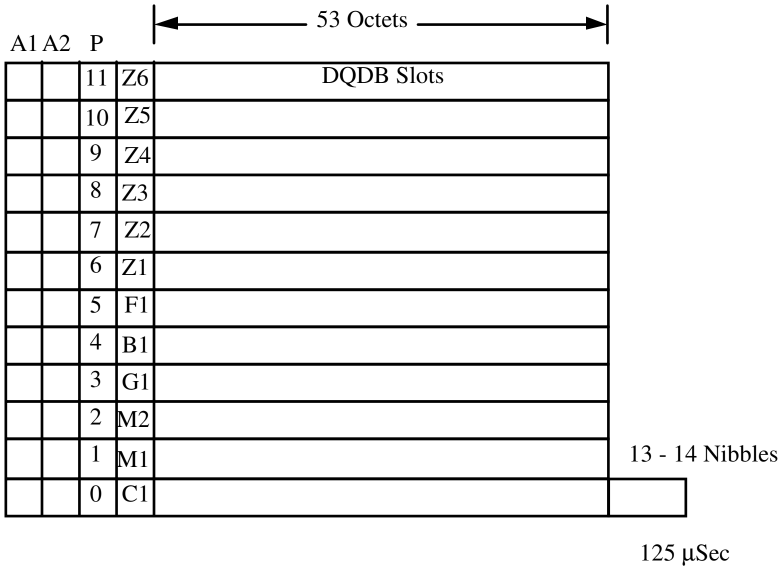


† Transmission Control Protocol/Internet Protocol

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

These cells are mapped into a 125 µSec frame to provide isochronous [fixed rate] services. This requires defining a 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

The 802.6 protocol can support three service classifications:

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

With the present digital video compression techniques, it is possible to deliver 6 broadcast quality channels over a 45 Mbps SMDS connection. Since it also supports multicast, SMDS can also convey near video on demand.

However, since there are no QoS guarantees, real-time interactive multimedia communication is not readily supported.

† Physical Layer Convergence Procedure

7.3 The Internet

For a comprehensive discussion of Internetworking Technologies, refer to:

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

Cisco has published a number of articles dealing with internetworking protocols:

Cisco - About This Manual

Cisco - Internetworking Basics

Cisco - Internetworking Design Basics

Cisco - Large-Scale IP Internetworks

7.3.1 IPv4

The current version of the Internet Protocol, TCP/IP, is called IPv4. It was not specifically designed to support multimedia. In spite of this however, it has been possible to transport the various classes of multimedia signals and formats. Still pictures for example, can simply be thought of as a particular data type.

Moving and real-time images as well as real-time voice have presented much more of a problem. These data formats require constant transmission rates and a minimum quality of service. Furthermore, multiparty video and audio conferencing requires broadcast capabilities. Business applications require a high degree of security. None of these concerns is specifically addressed in IPv4.

One of the most interesting programs developed to transport multimedia signals over IPv4 is CUSeeMe.

CUSeeMe

CUSeeMe is a software package developed at Cornel University, to transport audio and video signals across the internet. Multiparty conferences can be held if all of the participants log in to a reflector site. This site will rebroadcast each incoming signal to all participants as well as keep track of transmission statistics.

7.3.2 IPv6[6]

Bay Networks - The Case For IPv6

Internet EDGAR Project

Voice Fax Over IP

Cisco - Internet Protocols

Cisco - IP Multicast

The next version, IPv6 is currently being developed under the supervision of the Internet Engineering Steering Group, and is specifically designed to address most of the issues related to supporting multimedia.

6 Information in this section is based upon *IP Next Generation Overview*, by Robert M. Hinden and is available on the Internet

IPv6 will simply be a software upgrade and backward compatible with IPv4. Its wide range of capabilities will allow it to support transport facilities ranging from high performance ATM networks to low bandwidth wireless networks.

Since computers have been the driving force behind the growth of the Internet, IPv4 primarily serves the computer sector. Its purpose is to interconnect the computers in large business, government agencies, and educational institutions. Most computers in these organizations are also connected to LANs.

Further expansion will probably be driven by growth in: nomadic personal computing, wireless networks, networked entertainment, controllers for lighting and HVAC systems, etc.

The major differences between IPv4 and IPv6 are:

- Expanded routing and addressing capabilities
- New address types
- Header simplification
- Improved support
- Quality of service features
- Improved authentication and privacy

IPv6 increases the address size from 32 bits to 128 bits, to support more levels of hierarchy and nodes, and to simplify auto-configuration of addresses.

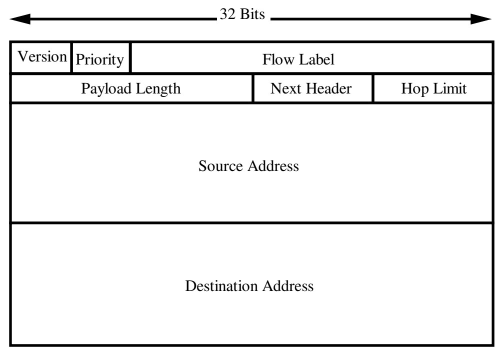
A new address type, the anycast address, has been created to identify sets of nodes where a packet can be sent to anyone of the nodes. The use of anycast addresses in the source route allows nodes to control the traffic flow path.

Some IPv4 header fields have been dropped or made optional, to reduce the packet processing costs and to minimize bandwidth. Although the addresses are four times longer than in IPv4, the header is only twice the size.

Changing the IP header option increases efficiency and flexibility. Among other things, this will allow the end user to determine the quality of service. New extension definitions provide support for authentication, data integrity, and confidentiality.

The IPv6 protocol consists of two parts, the basic header and extension headers.

IPv6 Header Format



Version	4-bit Internet Protocol version number = 6
Priority	4-bit field indicating priority value
Flow Label	24-bit field defining Quality of Service
Payload Length	16-bit unsigned integer indicates the payload length in octets
Next Header	8-bit selector identifying the header type following the IPv6 header
Hop Limit	8-bit unsigned integer. Decremented by 1 at each forwarding node. The packet is discarded when it reaches zero.
Source Address	128 bits. The address of the packet originator
Destination Address	128 bits. The address of the intended recipient

IPv6 Extensions

Routers in IPv4 examine all header options. In IPv6, the options are placed in separate extension headers located between the IPv6 header and the transport layer header. Most of these are examined only at the destination and not along the route.

IPv6 extension headers can be of arbitrary length and the total number of options is not limited to 40 bytes. This feature permits new options such as authentication and security encapsulation. Options are always an integer multiple of 8 octets.

The current extension headers include:

- Routing — Extended Routing (like IPv4 loose source route)
- Fragmentation — Fragmentation and Reassembly
- Authentication — Integrity, Authentication, and Security
- Encapsulation — Confidentiality
- Hop-by-Hop Option — Special options that require hop by hop processing

- Destination Options — Optional information to be examined by the destination node

IPv6 Addressing

The addresses are 128 bits long and are identifiers for both interfaces and nodes. This provides for thousands of addresses to be assigned for every square meter of the earth. Consequently, vast groups of addresses can be reserved for specific functions or a single interface may be assigned multiple address types.

There are three types of addresses:

- Unicast — a single interface
- Anycast — identify a set of interfaces where a packet will be delivered to any one member of the set
- Multicast — identify a group of interfaces where a packet will be sent to all of the interfaces in the group. This is the same as a broadcast address.

The specific address type is indicated by the leading bits in the address. This variable length field is called the FP†. These prefixes are:

Address Type	Format Prefix	Fraction of Address
Reserved	0000 0000	1/256
Unassigned	0000 0001	1/256
Reserved for NSAP	0000 001	1/128
Reserved for IPX	0000 010	1/128
Unassigned	0000 011	1/128
Unassigned	0000 1	1/32
Unassigned	0001	1/16
Unassigned	001	1/8
Provider-Based Unicast	010	1/8
Unassigned	011	1/8
Neutral-Interconnect Unicast	100	1/8
Unassigned	101	1/8
Unassigned	110	1/8
Unassigned	1110	1/16
Unassigned	1111 0	1/32
Unassigned	1111 10	1/64
Unassigned	1111 110	1/126
Unassigned	1111 1110 0	1/512
Local Link	1111 111010	1/1024
Local Site	1111 1110 11	1/1024
Multicast	1111 1111	1/256

The unassigned address space is reserved for future use. Note that anycast addresses are allocated out of the unicast address space. Approximately 15% of the address space is allocated and the balance is reserved for future use.

Unicast Addresses

There are several forms of unicast address in IPv6:

- Global provider based unicast address
- Neutral-interconnect unicast address
- NSAP address
- IPX hierarchical address

† Format Prefix

- Site-local-use address
- Link-local-use address
- IPv4-capable host address

Provider Based Unicast Addresses

These addresses are used for global communication and are similar to IPv4 addresses under CIDR. Their format is:

010	Registry ID	Provider ID	Subscriber ID	Subnet ID	Interface ID

The first 3 bits are the provider-oriented unicast identifier. The balance describes the exact interface and its hierarchy.

Local-Use Addresses

A local-use address is a unicast address used within the subnet or subscriber network. They are intended for plug and play, local communication and for bootstrapping up to use the global addresses.

Two types of local-use unicast addresses are presently defined:

- Link local use — is for use on a single link such as an auto-address configuration
- Site local use — is for use in a single site

Local link addresses have the following format:

	n bits	118 - n bits
1111111010	0	Interface ID

Site local use addresses have the following format:

	n bits	m bits	118 - n - m bits
1111111011	0	Subnet ID	Interface ID

In both cases, the local address must be unique within the domain. In most cases, this will correspond to the node's IEEE-802 48 bit address.

The subnet ID identifies a specific subnet in a site. This in combination with the interface ID, allows a large private internet to be constructed without any other address allocation.

Local addresses allow organizations that are not yet connected to the Internet to operate without an Internet address prefix. If the organization later connects to the Internet, it can use is subnet ID and interface ID in conjunction with a global prefix [e.g. registry ID + provider ID + subscriber ID] to create a global address.

IPv6 Addresses with Embedded IPv4 Addresses

There are two types of IPv6 addresses that can contain the IPv4 address:

- IPv4-compatable IPv6 address — IPv6 nodes are assigned special unicast addresses containing the IPv4 address in the low-order 32 bits
- IPv4 mapped IPv6 address — this address contains an embedded IPv4 address for those nodes that do not support IPv6

The IPv4-compatible IPv6 address has the format:

80 bits	16 bits	32 bits
all 0s	all 0s	IPv4 Address

IPv4-mapped IPv6 address has the format:

80 bits	16 bits	32 bits
all 0s	all 1s	IPv4 Address

Anycast Addresses

Anycast addresses are assigned to more than one interface. An anycast address is routed to the nearest interface having that address.

Using anycast addresses as part of a route sequence allows a node to select internet service providers. It can be implemented by making the anycast address the same as the internet service provider router chain.

Since anycast addresses are allocated from the unicast address space, they are indistinguishable from them. The assigned nodes must be explicitly configured to identify anycast address.

Multicast Addresses

A multicast address identifies a group of interfaces and any interface may belong to any number of groups. This addresses type has the following format:

8 bits	4 bits	4 bits	112 bits
all 1s	Flags	Scope	Group ID

The first 8 bits identifies a multicast address.

The next 4 bits are flags of which only the last one [T] is assigned:

- T = 0 indicates a permanently assigned multicast address
- T = 1 indicates a temporary multicast address

The next 4 bits define the scope of the multicast address, most of which are undefined:

Scope Value	Comment
0	Reserved
1	Local node
2	Local link
5	Local site
8	Local organization
E	Global
F	Reserved

The 112-bit group ID identifies the multicast group within the scope.

IPv6 Routing

The routing is almost identical to IPv4 routing under CIDR. With extensions, all of IPv4's routing algorithms such as: OSPF, RIP, IDRP, and ISIS can used. IPv6 also supports new routing extensions with increased capabilities including:

- Provider Selection — based on policy, performance, cost, etc.
- Host Mobility — route to current location
- Auto-Readdressing — route to new address

New routing functionality is obtained by creating address sequences to list the intermediate nodes defining the route. For a full duplex connection, the host simply reverses the address sequence.

Address sequencing can be used for provider selection. mobility, and readdressing.

Quality of Service Capabilities

Cisco - QoS

The flow label and priority fields in the header are used to support applications that require some degree of consistent throughput, delay, and jitter. These include multi-media and real-time applications. This will allow the Internet to support reasonable quality video.

Flow Labels

This aspect of IPv6 is subject to change as the requirements for flow support in the Internet become clearer. Hosts or routers that do not support the flow label field are required to set the field to zero when originating a packet, pass the field on unchanged when forwarding a packet, and ignore the field when receiving a packet.

A flow label is assigned to a flow by the source node. New flow labels must be chosen pseudo randomly and uniformly from the range 1 to FFFFFF hex. The purpose of the random allocation is to make any set of bits within the flow label field suitable for use as a hash key by routers, for looking up the state associated with the flow.

All packets in a given flow have the same source and destination address, same non-zero flow label, hop-by-hop options and routing header. If a violation is detected, it is reported to the source by an ICMP parameter problem message, code 0, pointing to the high-order octet of the flow label field (i.e., offset 1 within the IPv6 packet)

Routers are free to set up flow handling state even when no explicit flow establishment information has been provided.

Priority

The 4-bit priority field identifies the relative packet priority from a given source. The priority values are divided into two ranges:

- 0 to 7 — specify traffic when the source provides congestion control, and backs off in response to congestion. This is typical in TCP traffic.
- 8 to 15 — used to specify traffic that does not back off in response to congestion, as in constant rate or real time applications.

Congestion Control Traffic Priority	
Category	Comment
0	Uncharacterized traffic
1	Filler traffic (netnews)
2	Unattended data transfer (Email)
3	Reserved
4	Attended bulk transfer (FTP, HTTP, NFS)
5	Reserved
6	Interactive traffic (telnet, X)
7	Internet control traffic (routing protocols, SNMP)

For non-congestion-controlled traffic, the lowest priority value is used for packets that the sender is most willing to have discarded. The highest value is used for packets that the sender is least willing to have discarded. There is no relative ordering implied between congestion and non-congestion controlled priorities.

Security

Cisco - Security Technology

Security concerns are a major issue for business applications over the Internet. It is essential that bankcard numbers and other private information not be available to anyone other than the intended recipient. The current PSTN has a quite high degree of security since only those persons actually employed by the telephone companies can access the system. However, on the Internet, signals travel to all sorts of non-secured locations where any number of non-bonded persons may have access.

IPv6 has two security service options. These may be used separately or together:

- Authentication Header — an extension header that provides datagram authentication and integrity without confidentiality. While the extension is algorithm-independent and supports many different authentication techniques, keyed MD5 is recommended.
- Encapsulating Security Header — This provides integrity and confidentiality to datagrams. It is algorithm independent but, DES CBC is recommended

7.3.3 FireWire

Kodak - IEEE-1394

The IEEE-1394 high performance serial bus is on its way to becoming the standard method of connecting digital audio and video electronic devices to personal computers. IEEE-1394 is the industry-standard implementation of Apple's FireWire. It supports video and audio via low-cost cables.

More than 50 video equipment manufacturers have adopted the DV format and IEEE-1394.

The IEEE-1394 standard defines three layers:

- Physical — provides the signals required by the FireWire bus
- Link — takes the raw data from the Physical layer and formats it into recognizable 1394 packets
- Transaction — takes the packets from the Link layer and presents them to the application

Link chips provide all link functions as well as a limited number of transaction functions. The remainder of the transaction function is performed in software.

Consumer audio/video applications use logical plugs and sockets, which are similar to RCA phono jacks and mini-DIN S-video connectors. A plug corresponds to an audio or video output and a socket represents an input connector.

The implementation of logical plugs and sockets is defined by the Digital Interface for Consumer Electronic Audio/Video Equipment specification. This is an extension of the IEEE-1394 standard proposed by members of the Japanese Digital Video Consortium (DVC).

7.4 ISDN

Cisco - ISDN
Cisco - ISDN Internetworks

There are two types of ISDN lines used to convey multimedia signals: the basic rate and primary rate access. It is unfortunate that the systems developed in Europe and North America are not identical.

7.4.1 Basic Access Rate [2B+D]

This is sometimes referred to as narrowband ISDN and is conveyed over a standard telephone loop. Thus, advanced services can be supported over existing wires. The link consists of:

- 2B = 2 x 64 Kbps channels for voice/data
- D = 1 x 16 Kbps data/signaling channel
- 48 Kbps for framing and synchronization

Some applications include:

- Telecommuting - For those people whose livelihood depends upon PCs, there is little if any need for them to go to the office, if they can be interconnected on high speed links via the PSTN.
- Remote file sharing - PCs connected over a LAN can share information or even the same screen. ISDN would allow this to be extended to anywhere in the world.
- Videophone
- Fax and E-mail - Either of these could be much more cost effective than the postal system.

In those areas where the telephone networks cannot support the entire basic rate channel, two lower rate access structures have been defined:

- B+D [64 Kbps + 16 Kbps]
- B [64 Kbps]

Frame Structure

The bits are organized into a 250 µSec, 48 bit frame.

The bit definitions within a frame change slightly according to the signal direction. The four D bits in positions 12, 25, 36, and 47 form the D channel with an effective bit rate of 16 Kbps.

2B+D Frame Composition		
Bit	TE to NT	NT to TE
1 & 2	Framing bit	Framing bit
3 - 10	B1 Channel 1st octet	B1 Channel 1st octet
11	Balancing bit	E, D-echo channel bit
12	D Channel bit	D Channel bit
13	Balancing Bit	Bit A, used for activation
14	F_A auxiliary framing bit	F_A auxiliary framing bit
15	Balance bit	N bit
16 - 23	B2 Channel 1st octet	B2 Channel 1st octet
24	Balancing bit	E, D-echo channel bit
25	D Channel bit	D Channel bit
26	Balancing bit	M multiframing bit
27 - 34	B1 Channel 2nd octet	B1 Channel 2nd octet
35	Balancing bit	E, D-echo channel bit
36	D Channel bit	D Channel bit
37	Balance bit	S bit, future
38 - 45	B2 Channel 2nd octet	B2 Channel 2nd octet
46	Balancing bit	E, D-echo channel bit
47	D Channel bit	D Channel bit
48	Balance bit	Frame balance bit

Since multiple ISDN terminals can share the same loop, a peer-to-peer protocol is necessary to:

- Activate and deactivate terminals
- Allocate D channel resources
- Perform diagnostic and maintenance functions
- Code, multiplex, and synchronize signaling

Information States

Signal	Comment
I0	An absence of signal denotes deactivation between NT and TE
I1	A pattern +-000000 from TE to request activation of NT
I2	Signals activation of NT or request activation of TE. All B, D, and echo bits, plus A are set to logical zero
I3	A properly synchronized frame with operational data in the B and D location transmitted from TE to NT
I4	The same as I3 but in the opposite direction. The A bit is set to zero.

Terminal States

Signal	Comment
F1	Inactive. TE is powered down
F2	Sensing. Powered up but not receiving
F3	Deactivated
F4	Awaiting signal. TE has responded to an activation request.
F5	Identifying Input. An unidentified signal has been received
F6	Synchronized. TE is active and waiting for normal frames
F7	Activated. Normal operating mode.
F8	Lost Framing.

Network States

Signal	Comment
G1	Deactivated
G2	Pending Activation
G3	Active
G4	Pending Deactivation

Basic Rate Line Code [2B+D]

North America [2B1Q]

Two binary symbols are mapped into a single quaternary symbol or quat, which can take the values of ±1 and ±3. This arrangement does not provide any redundancy, but does lower the baud rate by 50%.

Binary Value	Quat Level
00	-3
01	-1
10	3
11	1

7.4.2 Primary Access Rate [23B+D]

This is also called BISDN or Broadband ISDN.

The primary access link is expected by some to eventually displace the 24-channel DS1 format. It has the same bit rate as DS1, and is therefor somewhat backward compatible with existing facilities. However, the S bit is redefined as an F bit and has a increased functionality. Since A & B bit signaling is not employed, a clear 64 Kbps channel can be given to the end-user.

F Bit Designation	Frame	Use
m	all odd frames	Operation & Maintenance
e1, e2, e3, e4, e5, e6	2, 6, 10, 14, 18, 22	Error checking
FAS [001011]	4, 8, 12, 16, 20, 24	Frame Alignment Signal

North American version: 23B+D

- 23 x 64 Kbps B channels
- 1 x 64 Kbps D channel
- 8 Kbps for framing bits
- Total bit rate 1.544 Mbps
- Uses B8ZS coding

Applications for BISDN center on video conferencing and high-speed data transfer. There are numerous opportunities for providing both connection and connectionless services.

7.5 New Line Technologies[7]

Many new line technologies are under development. Some may never see the light of day while others may enjoy a limited degree of success. It remains to be seen whether any particular technology will dominate.

3 Com - xDSL

AG - ADSL

xDSL

	Max Rate	Max Distance [24 AWG UTP]	Applications
ADSL/ RADSL	1.5 - 8 Mbps Down 16 - 640 Kbps Up	18 Kft 12 Kft above 1.5 Mbps	Internet/intranet access, VoD, database access, remote LAN, lifeline phone service
HDSL	Full-duplex T1 or E1	15 Kft	T1/E1, PBX interconnection, frame relay, traffic aggregation
SDSL	Full-duplex T1 or E1	10 Kft	T1/E1, PBX interconnection, frame relay, traffic aggregation
VDSL	13 - 52 Mbps Down 1.5 - 2.3 Mbps Up	1 – 4.5 Kft	HDTV, multimedia Internet access

ADSL Asymmetric digital subscriber line

RADSL Rate-adaptive digital subscriber line

SDSL Single-pair digital subscriber line

UTP Unshielded twisted pair

VDSL Very high bit-rate digital subscriber line

7 Most of the information in this section comes from *xDSL Supercharges Copper*, by Robyn Abner, Data Communications, March 1997

xDSL

All DSL technologies run on existing copper telephone lines and use modulation to boost transmission rates. The basic differences are signal distance, speed, and transmission symmetry.

7.5.1 ADSL

The asymmetrical digital subscriber line uses FDM to convey a 1.536 to 8 Mbps downstream depending on line quality, distance, and wire gauge. Upstream rates range between 16 and 640 Kbps. The link contains a16 Kbps upstream control channel, and full duplex POTS or 2B+D channel.

ADSL has three information channels; two for data and one for voice. Thus, data performance is not hampered by voice calls.

ADSL has already been standardized by both ANSI†, which is now working on a revised version, and ETSI†. The rollout of ADSL services will begin this in 1997, and widespread availability is expected during 1998 and 1999.

ADSL modems divide the bandwidth using one of two methods: FDM and echo cancellation.

FDM assigns one band for upstream data and another for downstream data. The downstream path is further divided by TDM into one or more high-speed channels for data and one or more low-speed channels, one of which is for voice. The upstream path is multiplexed into several low-speed channels.

The upstream and downstream band can and be separated by means of echo cancellation. This uses bandwidth more efficiently, but at increased complexity and cost.

7.5.2 RADSL

RADSL has the same transmission limits as ADSL. However, it adjusts transmission speed according to the length and quality of the local line. Connection speed is established when the line is set by a signal from the central office.

7.5.3 HDSL

High-speed digital subscriber lines used 2B1Q coding to transmit 800 Kbps over a standard 5.5 km copper loop. Using two of these loops, full duplex DS1 or BISDN can be supported.

HDSL over two twisted pairs is capable of operating at T1 speeds, and over three pairs, can operate at E1 speeds.

† American National Standards Institute

† European Telecommunications Standards Institute

At 15,000 feet, the operating distance is less than ADSL, but carriers can install signal repeaters to extend its useful range by 3 – 4 Kft.

7.5.4 SDSL

SDSL is essentially the same as HDSL with two notable exceptions: It uses a single wire pair and has a maximum operating range of 10,000 feet. Since it's symmetric and needs only one twisted pair SDSL is suitable for applications like videoconferencing or collaborative computing with identical downstream and upstream speeds. Standards for SDSL are still under development.

7.5.5 VDSL

VDSL is the fastest DSL technology. It delivers downstream rates of 13 to 52 Mbps and upstream rates of 1.5 to 2.3 Mbps over a single wire pair. But the maximum operating distance is only 1 - 4.5 Kft. In addition to supporting the same applications as ADSL, VDSL, with its additional bandwidth, could potentially enable carriers to deliver HDTV. VDSL is still in the definition stage, and a standard isn't expected before late 1998.

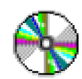
7.6 Switching Architecture

Cisco - ATM Switching

Cisco - Data Link Switching

Cisco - LAN Switching

Cisco - Tag Switching



7.7 Protocols

Port Numbers

Port numbers are virtual ports, which allows access to different service types. In most cases, the end-user does not have to set the port number.

Port Number	Comments
20	FTP data path
21	FTP control path
23	Telenet
25	SMTP
53	Domain Name Server
70	Gopher
79	Finger
80	WWW
110	Post Office Protocol version 3
119	Network News Transfer Protocol
123	Network Time Protocol
194	Internet Relay Chat Protocol

7.8 Broadband

7.8.1 SONET

Nortel SONET 101

SDH by Marconi

SONET by Nortel

SONET by tektronix

OC Level	Bit Rate [Mbps]	Payload Rate [Mbps]
OC-1	51.84	
OC-3	155.52	149.760
OC-9	466.56	
OC-12	622.08	600.768
OC-18	993.12	
OC-24	1244.16	1202.112
OC-36	1866.24	
OC-48	2488.32	2404.800
OC-96	4976.64	
OC-192	9953.28	

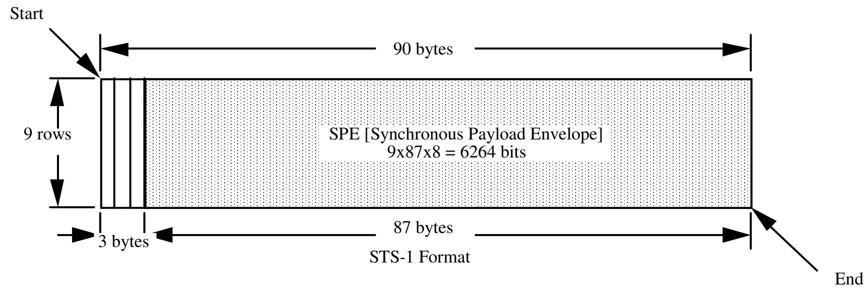
7.8.2 OC-1

This is the lowest level of optical carrier defined. It can carry all of the existing multiplexing structures in virtual tributaries.

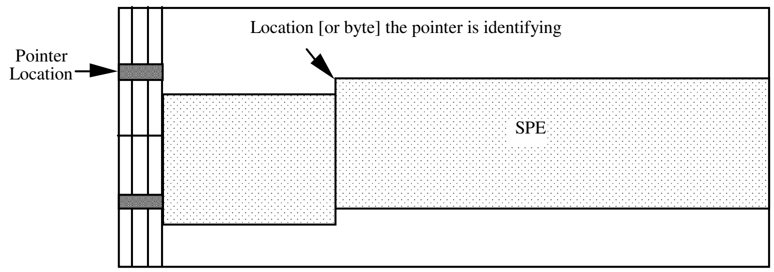
Many end-users will want to continue using existing DS-1 service. When this is mapped into an OC-n signal, is called a VT1.5 [since the bit rate is approximately 1.5 Mbps]. The VT stands for virtual tributary. Each OC-1 component can carry 28, VT1.5s [or 672, DS-0s].

Higher order SONET signals can be obtained by byte interleaving frame aligned STS-1 signals or by concatenation. Concatenation occurs when the payload is treated as a single unit. This is denoted by placing the letter c after the rate designation. [i.e. STS-3c]

STS-1 Format



STS-1 Format



STS-1 with Floating SPE Payload

SONET Overhead Channel Byte Allocation[8]

	Transport Overhead				Path Overhead
	Row	Byte 1	Byte 2	Byte 3	
Section Overhead	1	A1	A2	C1	J1
	2	B1	E1	F1	B3
	3	D1	D2	D3	C2
Line Overhead	4	H1	H2	H3	G1
	5	B2	K1	K2	F2
	6	D4	D5	D6	H4
	7	D7	D8	D9	Z3
	8	D10	D11	D12	Z4
	9	Z1	Z2	E2	TC

Nomenclature:

A1 & A2	Framing bits indicating the start of the frame
B1 - B2	8 bit Interleaved Parity
C1	STS-1 identification byte
D1 - D12	Line data communications channel
E1 & E2	Orderwire for network maintenance personnel
F1	Reserved for network operation user applications
H1 - H3	Header pointer
K1 & K2	Automatic protection switching message channel
Z1 & Z2	Reserved for future growth

8 *SONET: Now It's The Standard Optical Network,* IEEE, 1989

In addition to these overhead bytes, SONET carries a number of STS-1 path overhead bytes, which are processed at the payload terminating equipment:

J1	Trace
B3	8 bit interleaved parity
C2	Signal label indicating payload type
G1	Path status for maintenance purposes
F2	User channel
H4	Multiframe alignment byte
Z3 & Z4	Reserved for future growth
TC	Tandem connection

Standardization of these bit patterns is necessary to ensure the interoperability of SONET at the network level.

7.8.3 OC-3

A SONET OC-3 signal is composed of three OC-1 signals. An OC-3 can carry 84, VT1.5s [or 2016 DS-0s]. Of the 155.52 Mbps available on the OC-3 link, about 129 Mbps will be offered to end-users in North American.

It has been suggested that both ATM and STM can be mixed in the same STS envelope and separated by the CO at a broadband cross-connect.[9] An alternative would be to segregate ATM and STM in their own STS envelopes.

7.8.4 ATM

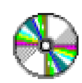
Nortel ATM Tutorial

Cisco ATM Internetworking

Ch 8 Designing ATM Internetworks by Cisco

http://www.cisco.com/univercd/cc/td/doc/cisintwk/idg4/nd2008.htm

http://www.cisco.com/univercd/cc/td/doc/cisintwk/idg4/nd2012.htm#28092



This standard, I.121, is being developed by ITU Study Group XVIII, is nearly identical to the IEEE 802.6 MAN standard. One of its main applications will be to supply bandwidth on demand. This naturally is very attractive to videoconferencing developers.

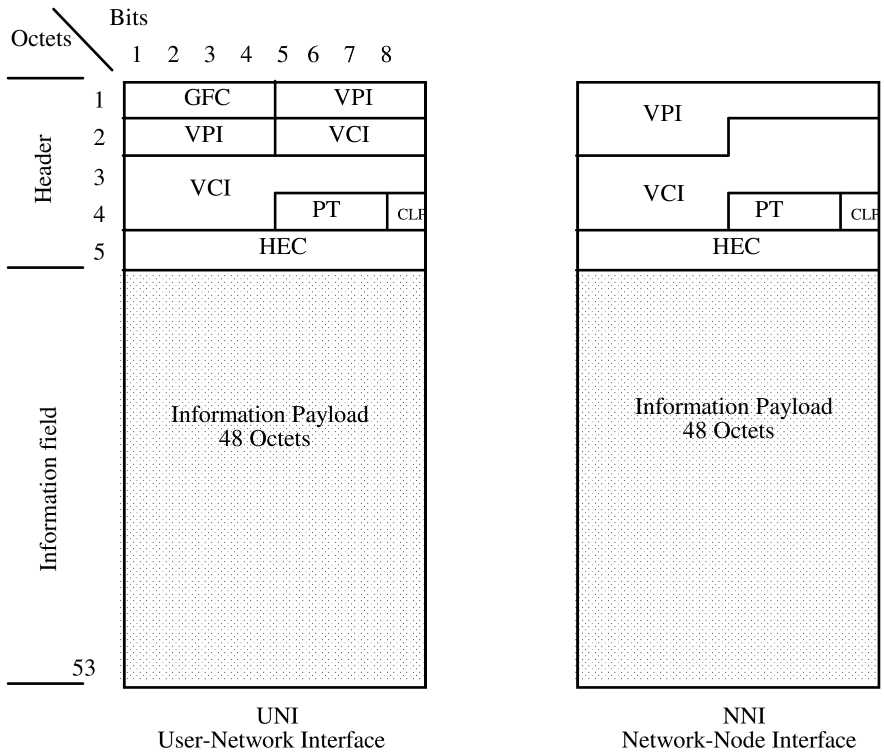
ATM Service Categories

Class	Bit rate	Continuity	Application
A	Constant	Connection	Existing services
B	Variable	Connection	Videoconferencing
C	Variable	Connection	Data communications
D	Constant	Connectionless	SMDS

[9] *Telesis* 1990 One/Two

Notes

ATM Cell Structure[10]



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
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

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

Assignment Questions

Quick Quiz

1. The per segment delay on a videoconferencing circuit should be no more than 15 mSec. [True, False]
2. Videoconferencing is easier to support on [packet, circuit] switching networks.
3. The H.324 standard does not allows a low-grade videoconference to be established over a POTS line. [True, False]
4. All network types conform exactly to the OSI model. [True, False]
5. A physical star LAN can be logical ring. [True, False]
6. Ethernet is the same as IEEE [802.3, 802.5, 802.6]

Composition Questions

To answer these questions, it may be necessary to do some additional research.

1. What are the basic requirements any network should meet in order to support videoconferencing, and why are they important?
2. What Nortel products currently support video conferencing?
3. How does LAN topology influence the ability to support videoconferencing?
4. Which versions of Ethernet are suited to handling multimedia communications, and why?
5. What is the principle benefit of the ring topology over the bus topology?
6. Why does SMDS not readily support multimedia communications?
7. Why is IPv6 better suited to handling multimedia communications than IPv4?
8. Find out what version of ADSL is available locally.

For Further Research

S. Bradner, A. Mankin, RFC 1752, The Recommendation for the IP Next Generation Protocol, January 1995.

ADSL Forum TR-001, ADSL Forum System Reference Model

1394 High Performance Serial Bus: The Digital Interface for ATV, Adam J. Kunzman, Alan T. Wetzel, Texas Instruments

1394-based Digital Camera Specification, Version 1.04, 1394 Trade Association

1394 Technical Overview, Texas Instruments

The facts about FireWire, Ingrid J. Wickelgren, IEEE Spectrum April 1997

ISDN

http://public.pacbell.net/ISDN/connect.html

http://alumni.caltech.edu/~dank/isdn/

http://www.teles-usa.com/teles.www/isdn/e_isdn.htm

Multimedia Internetworking

http://web.mis.ccu.edu.tw/ip/idgmulti.html

FireWire

www.ti.com/sc/docs/msp/1394/tech.htm

www.1394TA.org

www.ddx.com/fibre.html

http://www.firewire.org/

ADSL

http://www.adsl.com/adsl_home.html

http://www.ee.ubc.ca/home/comlab1/irenek/etc/www/techpaper/adsl/adsl.html

http://www.analog.com/publications/whitepapers/products/back_adsl/

http://www.dqnet.com/apps/adsl.html

http://alumni.caltech.edu:80/~dank/isdn/adsl.html

http://pilot.msu.edu/user/hsuhsuni/adsl.htm

DWMT

http://bugs.wpi.edu:8080/EE535/hwk97/hwk3cd97/suska/suska.html

http://www.analog.com/publications/whitepapers/whitepaper_html/content.html

Cable Modem

http://www.cablemodem.com/

http://www.cablelabs.com/

http://www.davic.org/

http://www.cocom.dk/

http://www.ncta.com/modem.html

ftp://ftp.ietf.org/internet-drafts/draft-ietf-ipcdn-cable-device-mib-02.txt

http://www.rhk.com/index.htm

http://www.catv.org/modem/

DVB

http://www.dvb.org/

HFC

http://bugs.wpi.edu:8080/EE535/hwk97/hwk3cd97/murti/murti.html

http://www.ericsson.com/Connexion/connexion3-97/techno.htm

http://conquest.oakridge.com/STel/modchip.html

http://www.dqnet.com/apps/hfc.html

Dijkstra demonstration applet
http://www.dcss.mcmaster.ca/~ea97c1/steve/dgraph.htm

Cisco Documentation
http://www.cisco.com/univercd/home/home.htm
http://www.cisco.com/warp/public/784/packet/