

Computer Networks / Retele de Calculatoare

3rd Year students (Romana, Seria A + English)

Lecturer: Prof. **Vasile Dădârlat**, PhD
Vasile.Dadarlat@cs.utcluj.ro

3rd Year students (Seria B)

Lecturer: **Assoc.Prof. Bogdan Iancu**, PhD
Bogdan.Iancu@cs.utcluj.ro

Grading Type: normal, Credits:3

No prerequisite modules required

Basic knowledge in Physics, Mathematics, Computer Architecture – feel free to ask questions anytime

MS Teams – live meetings

TUCN account

*(you were automatically enrolled; if you are not enrolled, send a message in MS Teams to **Bogdan.Iancu@campus.utcluj.ro**)*

<https://moodle.cs.utcluj.ro>

Rețele de calculatoare / Computer Networks, Sem. 2, 2023/2024

<https://moodle.cs.utcluj.ro/course/view.php?id=632>

Self-Enrolment key: ***L@b_key2024***

ASSESSMENT

- Lab test (last week) - laboratory
- Written Exam (theory, problems)
- Grading constraints: minimum of 5 (out of 10) for each:
mid-term (TBD), final, lab
- Grade policy

$$40\% \text{ Lab} + 60\% \text{ Exam}$$

- Module Credits: 3

Lecture 1

Module Description

Notions of: communications, telecommunications; Communications architecture and protocols; Introduction to computer networks; OSI Model; TCP model; analog and digital transmissions; encoding techniques; transmission media (special focus on fiber optic); synchronous and asynchronous transmissions; digital carriers; multiplexing; circuit and packet switching; Local Area Networks - systems (wired & wireless) & technologies (focus on medium access control techniques); case study: Ethernet LANs; Bridges & Switches; introduction to internetworking & routing; classic IP & IPv6; Transport level protocols; application level services.

Aim of the module

Introductory module on **data & computer communications, case study: LANs**

data comms: signal transmission, transmission media, interfacing, data link control

networking: technologies and architectures of comms networks (LANs, WANs)

computer communications –basic introduction, basic protocols

simple communications networks (LANs) & their protocols

internetworking

This is the first from a sequence of (at least) 2 modules in Computer Networks!

Why this structure?

- no more much difference between data processing (computers) and data communications (transmission & switching equipment)

- no fundamental difference in transmitting data, voice or video

- today's the metanetwork (let's say Internet), makes no difference

(reference) to single or multi processor computers, or to PAN, LAN, MAN or WAN
(access to any resource is done easily & uniformly)

Fields of Study

- data transmissions: data, signals, transmission systems, techniques (coding, multiplexing, switching)
- general aspects of networks: definition, evolution, generations, further developments; history of Internet; case study: LANs
- topologies: star, ring, bus
- introduction to internetworking
- protocols:
 - Architectures & reference models
 - Lower & higher levels
 - Study for levels 1 to 3: Physical, Data Link, Network
 - Internetworking
 - Transport & Application level services

Bibliography

Main text book for this module:

- W. Stallings – *Data and Computer Communications*, Prentice Hall, editions 2004 - 2014
- The ‘most available’ text book (Romanian) is: Vasile Teodor Dadarlat, Emil Cebuc: *Retele Locale de Calculatoare - de la cablare la interconectare*, Editura Albastra (MicroInformatica), 2005

Also you'll get good knowledge and experience reading:

- L. Peterson, B. Davie – *Computer Networks, Fifth Edition: A Systems Approach*, The Morgan Kaufmann Series in Networking, 2013
- A. Tanenbaum – *Computer Networks*, Prentice Hall, 2002,2005,2010
- D. Comer – *Computer Networks and Internets*, Prentice Hall, 2008, 2014

LAB Activity (compulsory)

TABLE OF CONTENTS

	Week
1	Introduction to Wireshark and Packet tracer
2	Cooper based transmission media and UTP cabling
3	Optical fibers and components
4	Structured Cabling
5	Connectivity to Network: IPv4 subnets and basic router configuration
6	Connectivity to Network: DHCP and IPv4 static routing
7	Connectivity to Network: IPv6 introduction and static routing
8	Transport layer: TCP/UDP and Network Programming using Socket
9	Ethernet, ARP and NDP
10	VLAN, trunking and inter-VLAN routing
11	Layer 2 networks: Spanning Tree Protocol, Link Aggregation and Etherchannel
12	Security threats in computer networks
13	Recap
14	Laboratory test

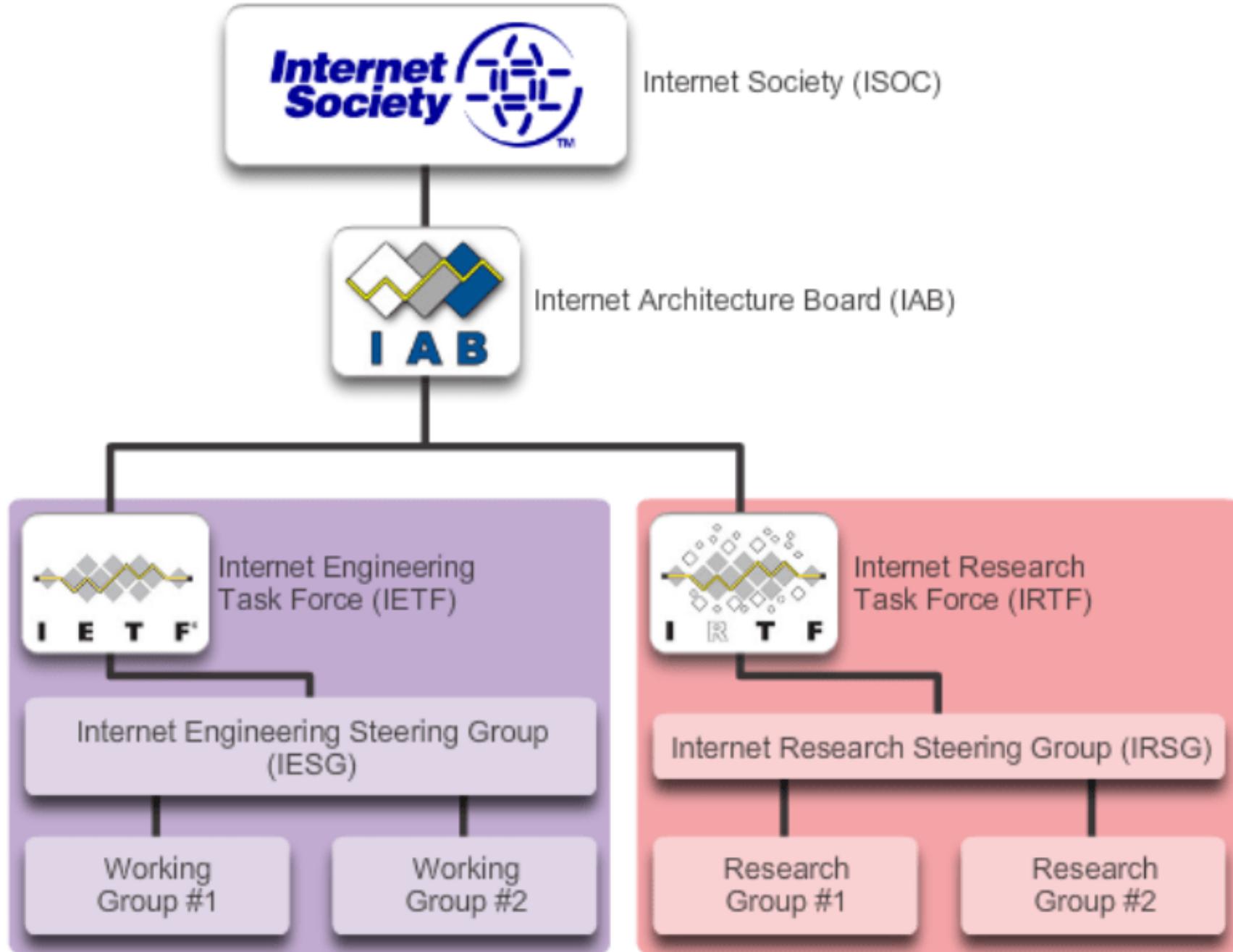
Standardization bodies

Why standards?

- for unique specifications
- for global uniformity and interoperability

What's now?

- still are proprietary networks (big companies): IBM/SNA, Digital/DECNET, Novell/Netware, Cisco
- 'de facto' standards: adopted by the market, not yet official standards: TCP/IP protocol suite
- 'de jure' standards: official standard, small market acceptance
- consortiums, forums: mix of companies (product promotion), specification & standardization bodies (standardization in progress):
 - IEEE 802.x- formal standardization group
 - Frame Relay Forum, ATM Forum, Internet Engineering Task Force (IETF) – application development, IResearchTF – further development (see structure on next page)



Standardization bodies (continued)

For proprietary standards, closed systems:

ECMA (European Computers Manufacturers Association)

EIA (European Industrials Association)

For interface standards, multi-vendor systems:

ITU-T (International Telecommunications Union, Telecommunications sector),
former CCITT (Comite Consultatif International pour telephone et telegraphe)

ANSI (American National Standards Institute)

IEEE (Institute for Electrical and Electronic Engineers)

ETSI (European Telecom Standards Institute)

For international standards, open systems:

ISO (International Organization for Standardization) – Technical Committee for
Information Processing TC 97

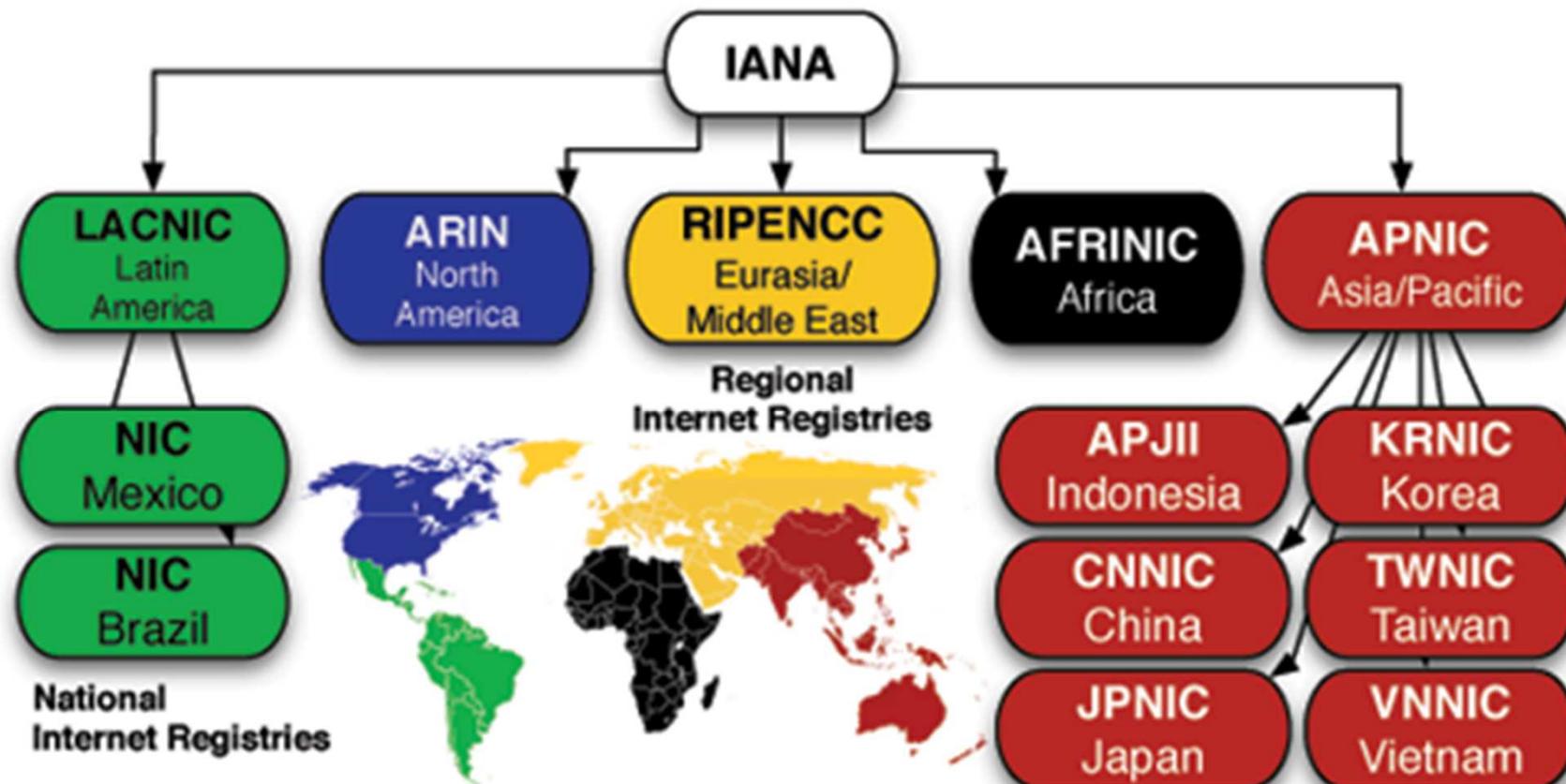
The Intersection of Media Development Principles and Internet Governance

INTERNET GOVERNANCE BODY	PRINCIPLE AT STAKE	TECHNICAL DEBATE
 ICANN	Freedom of Expression	Domain Names (gTLDs) Management of new, generic Top-Level Domains (gTLDs)
 IGF Internet Governance Forum	Media Pluralism	Social Media as News Platforms Algorithms and Media Plurality
 ITU	Access to Information	Wireless Internet 5G Cellular Networks and Unlicensed Spectrum Standards
 I E T F	Privacy	Web Browsing Privacy Encryption
 IEEE	Secure Access and Trust	Wi-Fi Security Local Area Networks (LAN) Protocols in Diverse Settings

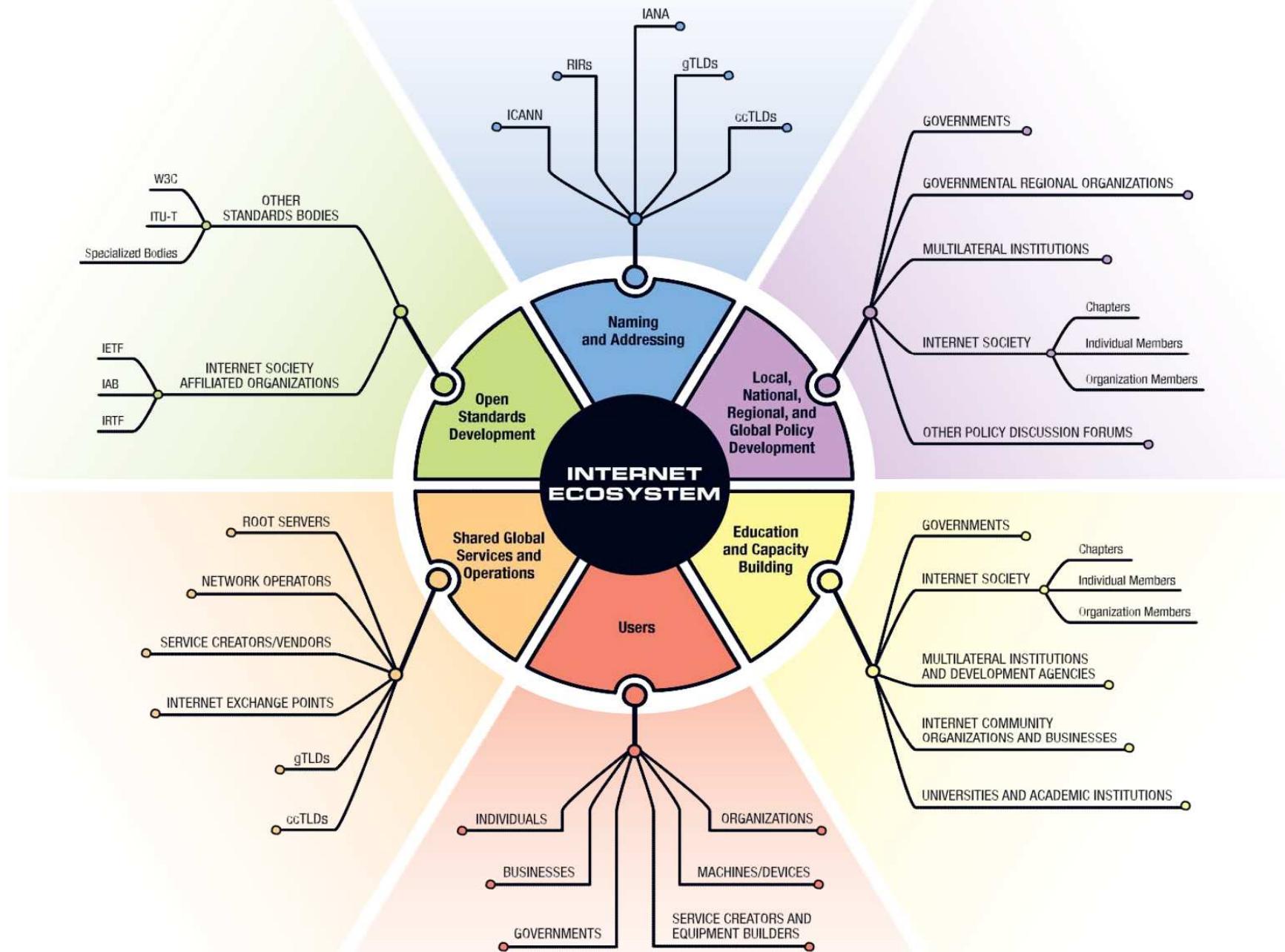
<http://www.cima.ned.org/publication/media-development-digital-age-five-ways-engage-internet-governance/>

Internet Assigned Numbers Authority

- global coordination of:
 - DNS Root, IP addressing, and other Internet protocol resources



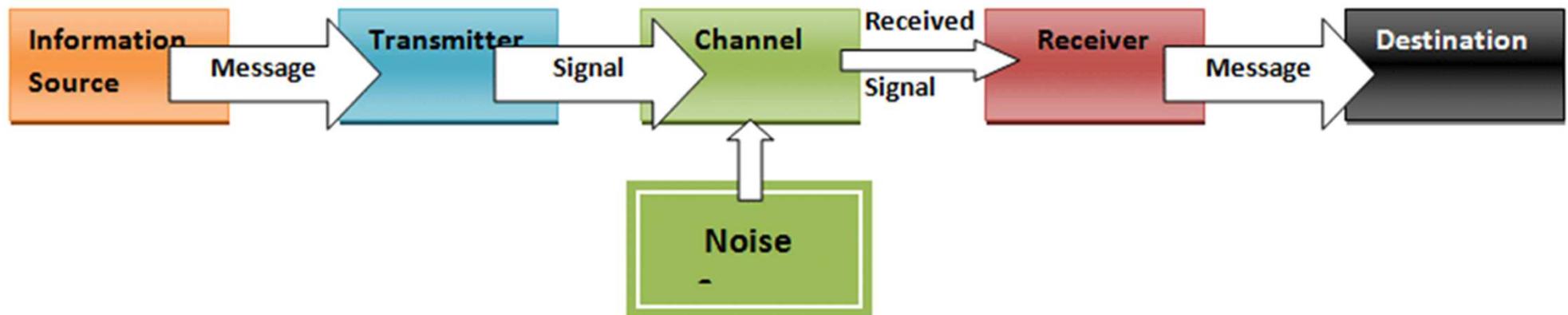
http://www.caida.org/funding/nets-ipv6/nets-ipv6_proposal.xml



Notions of: Communications, Telecommunications

The ‘old’ need to communicate: use of symbols, writing, languages

Claude Shannon’s model of communication



The Communications Model

Source

Generates data to be transmitted (the message)

Sender (transmitter)

Converts data into transmittable signals (ex. modem)

Transmission System

Simply, the **channel** - carries data, using signals; may be affected by noise; from a single transmission line to a complex network connecting the parts

Receiver

Converts received signal into data

Destination

Takes incoming data

Oral communication between two people:

Source & destination: the brain

Sender: transmitting device, the mouth

Channel: medium traversed, the air

Receiver: the receiving device, the ear

Communications

Problems (limitations) with the Shannon's model:

- one way
- no feedback
- not appropriate to group communications
- no explanation for the sending/receiving process

Questions?

- which are the formats a message is delivered?
- which are today's communications methods (radio, TV, papers, phone, Internet): one-way, two-way, multiple, interactive? Which will be preferred in the future?
- what about the teaching process?
- how to make the message secure?

Key Communications Tasks (from en engineering view)

Utilization of the Transmission System: optimal, efficient allocation of existing resources

Interfacing with the Transmission System: electromagnetic signals

Signal generation: for optimal propagation & proper interpretation at receiver

Synchronization between the communication parts

Message exchange management: rules of the conversation

Error detection and correction, flow control: part of the exchange management

Addressing and routing: more devices may share the transmission facilities

Recovery: resume of activity from the point of interruption

Message formatting: bit or character oriented

Security: data received only by intended receivers, and unaltered

Network Management: configure the system, monitor its status, detect failures & overloads, planning the future growth

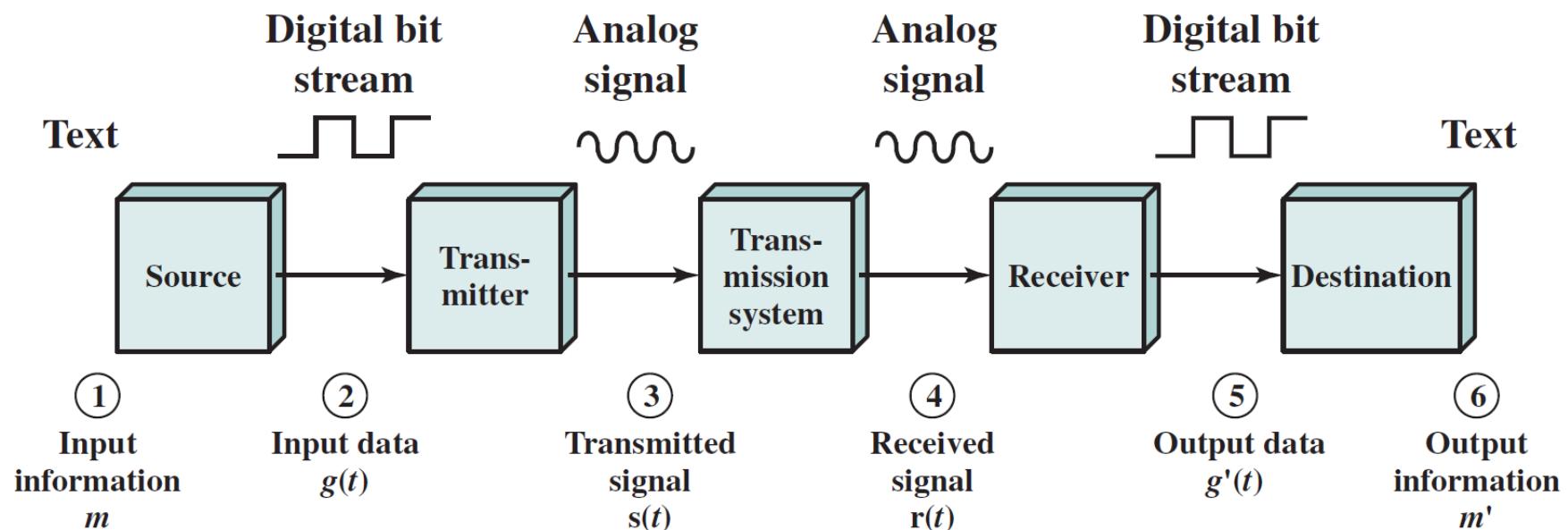
Telecommunications

Etymology: communication at a distance, as the *tele* prefix states (see television, teleaction, telecommand, telephony)

Definition: the *information transfer* between *two (or more) points*, usually at a distance, using *media* other, or perhaps including audio.

Example

Communication between two computers exchanging text files, using modems:



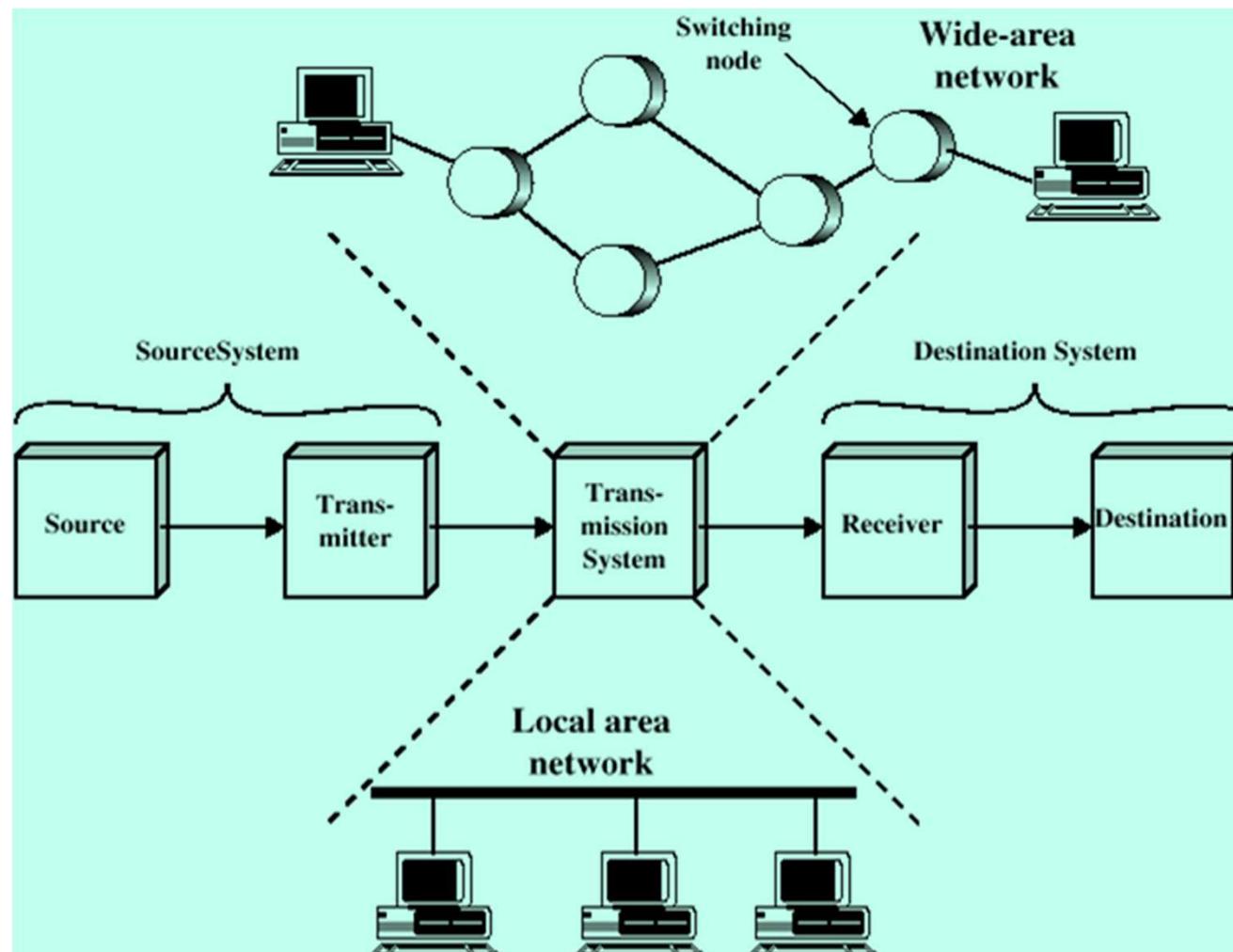
Networking

Point to point communication not usually practical

Devices are too far apart

Large set of devices would need impractical number of connections

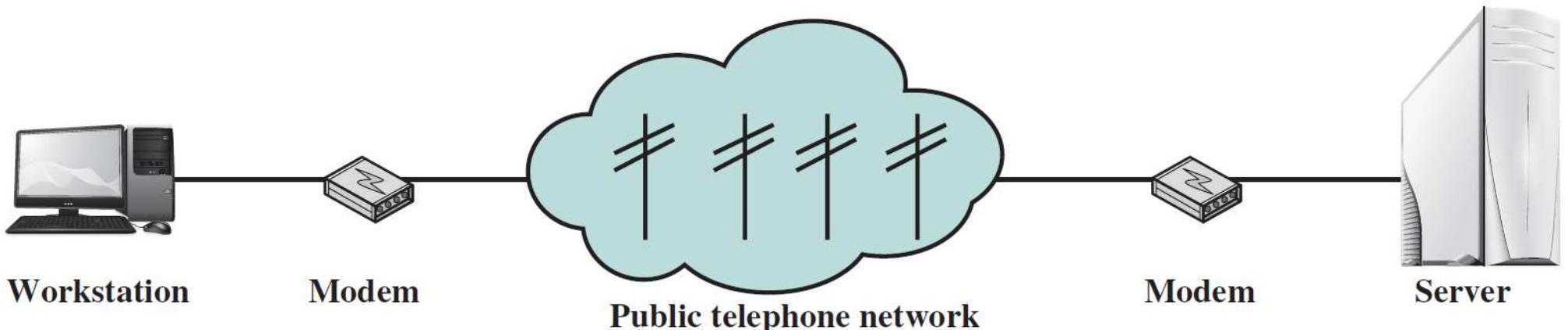
Solution is a **communications network** (see below an example)



Communications Networks

Definition: a mesh of switching nodes and links, enabling one or more ‘network hosts’ to have access to a telecommunications infrastructure which supports a range of tele-services to the network hosts or between network hosts.

Example: telecommunications connection between a computer and an e-mail server (ISP) – two network hosts – application: e-mail exchange, carrier: PSTN (Public Switch Telephone Network).



Communications Networks continued

Generally all networks are **telecommunications** (data networks, computer networks, telephony networks, mobile cellular networks, TV broadcasting networks).

In the past, a difference : computer networks carry data, telecomm networks operate with voice; no more, today's networks (let's say Internet) carry voice+data+video!

Question?

A lecture is a telecommunication activity and has the structure of a network?

Answer: a lecture has communications attributes, like: point-to-point, simplex or half duplex, symmetric in bandwidth (4KHz), unbalanced, analogue transmission, but is not telecommunication (not at distance) and there is no network (not distance transporting system).

Global Telecommunications Networks

Today we speak about **Global Networks**

Issues:

- fixed or mobiles
- application driven networks
- integrated telecommunication networks (carry data, voice, video)
- convergence of networks (in terms of access interfaces, packet size, service supply)
- seamless (network of networks, metanetwork)
- increased number of services
- need for an ordered development, based on **reference models**

Some Milestones for Communications Networks evolution

(concerning offered services)

1850: Telegraphy

1890: Telephony

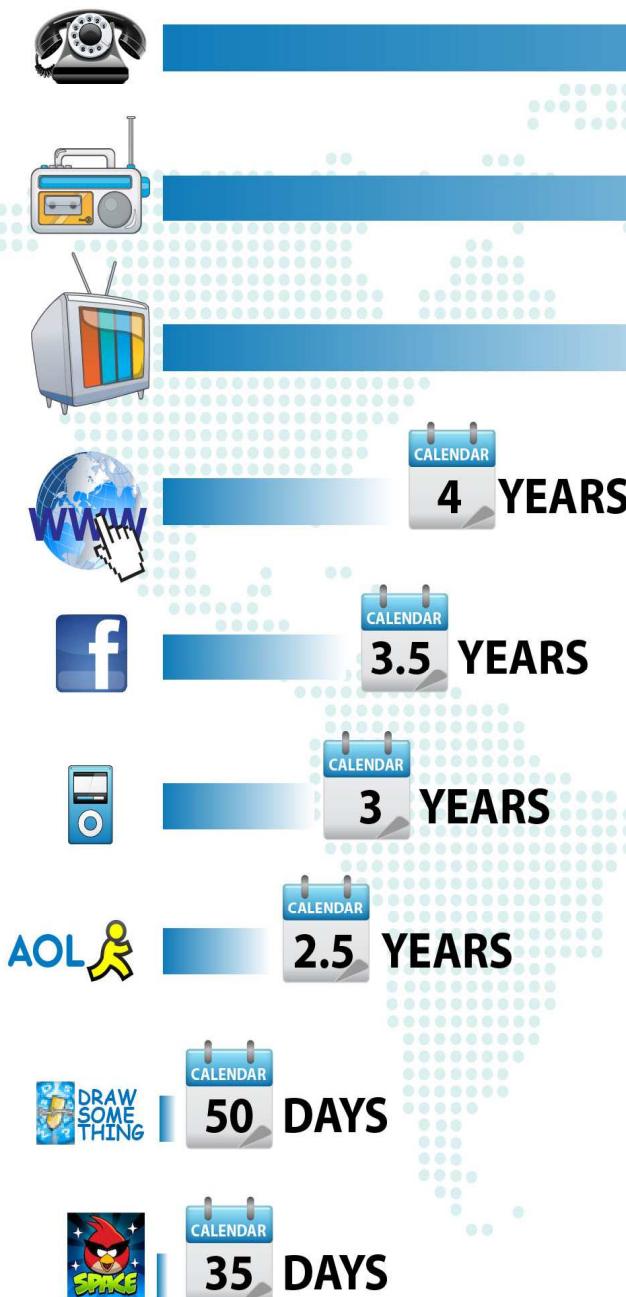
1930: Radio, Television, Facsimile, Branch Exchange

1970: Color TV, Stereo radio, low-speed data transmissions(Kbps), remote computing

1990: ISDN, medium & high speed data transmissions (Mbps), multimedia, LANs, WLANs, video...

2000: Very high speed transmissions (Gbps), mobile, home access, security, virtual reality, teleworking, banking

2010: Mobile communications, cloud computing, High Performance computing ...



Reaching 50 Million users

It took about 75 years for the telephone to connect 50 million people. Today a simple iPhone app like Draw Something can reach that milestone in a matter of days. In the past 10 years the rate of adoption of new technologies has accelerated at a dizzying speed. Can we keep up with it all?

Introduction to Computer Networks

Computer Networks are an interconnection of computers.

Two computers are said to be interconnected if they are able to exchange information (data).

The main reasons why computers are networked are:

- to share hardware resources – higher reliability (files, printers, modems, fax machines)
- to share application software (MS Office)
- to save money – downsizing process: from mainframes to a lot of small intelligent computers spread around
- to increase productivity (make it easier to share data among various users)

Types of computer networks

Different criteria:

- public (ex. educational WANs) or private (company owner)
- geographical location (coverage): Personal Area Networks (PAN), Local Area Networks (LANs), Metropolitan Area Networks (MANs), Wide Area Networks (WANs)
- type of transmission media: hard-wire (copper based wire or fiber optic), soft-wire (radio, satellite, infrared)
- topologies: mesh, star, ring, bus
- transmission type: broadcast/multicast, point-to-point, peer-to-peer
- classes of reliability
- application domains (ex. multimedia applications)
- way in which nodes exchange information: broadcast (LANs, Wireless), switched (circuit switching, packet switching (datagrams, virtual circuits))



Internet Evolution



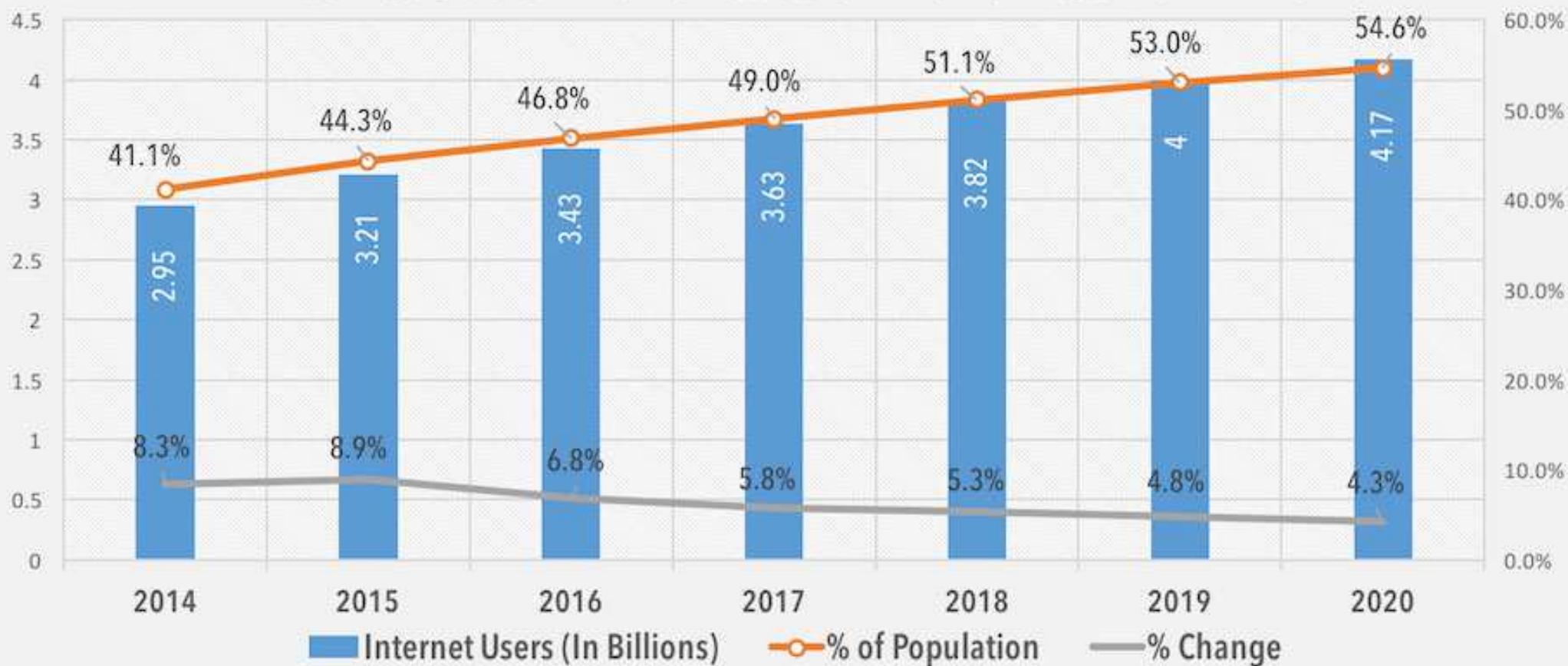
"The best predictor of future behavior is past behavior" (Dr. Phil)

Introduction

- ▶ "All Science Is Computer Science"
(New York Times, 2001)

- ▶ The Internet
 - ▶ global network connecting millions of computers
 - ▶ network of networks, a networking infrastructure

Internet Users And Penetration Worldwide 2014 - 2020



Note: Individual of any age who use the internet from any location any devices atleast once a month.

Source: eMarketer, April 2016

DAZEINFO

Internet Users in 2021



OCT
2022

COUNTRIES WITH THE LARGEST POPULATIONS

THE WORLD'S TOP 20 COUNTRIES, RANKED BY THE SIZE OF THEIR TOTAL POPULATION ON 01 OCTOBER 2022

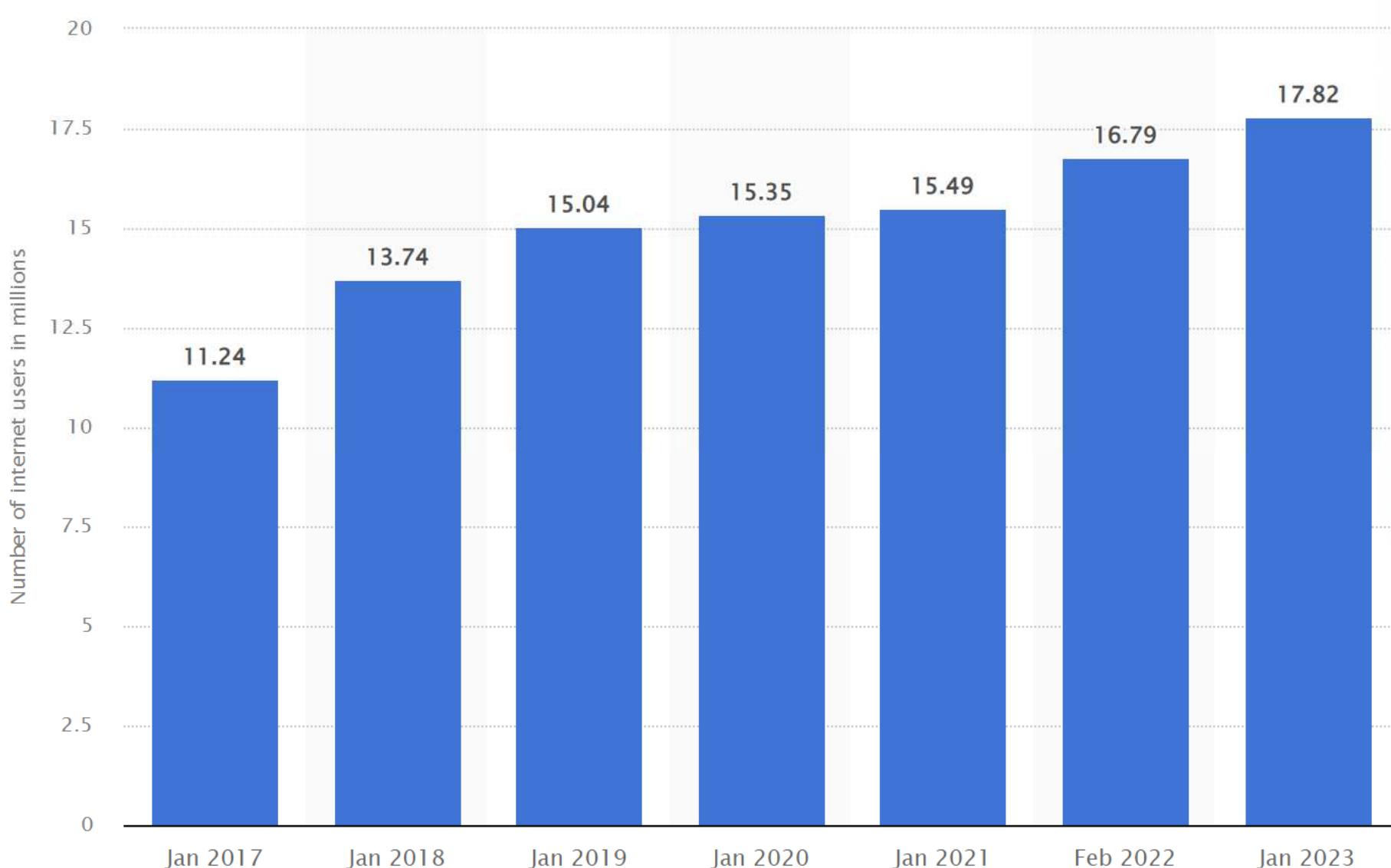


#	COUNTRY	POPULATION	#	COUNTRY	POPULATION
01	CHINA	1,425,868,312	11	ETHIOPIA	124,156,150
02	INDIA	1,419,597,776	12	JAPAN	123,788,275
03	UNITED STATES OF AMERICA	338,684,815	13	PHILIPPINES	116,004,493
04	INDONESIA	275,943,509	14	EGYPT	111,417,927
05	PAKISTAN	236,972,694	15	DEM. REP. OF THE CONGO	99,805,197
06	NIGERIA	219,843,721	16	Vietnam	98,358,992
07	BRAZIL	215,557,721	17	IRAN	88,697,412
08	BANGLADESH	171,630,186	18	TURKEY	85,465,954
09	RUSSIAN FEDERATION	144,703,713	19	GERMANY	83,341,365
10	MEXICO	127,743,896	20	THAILAND	71,725,413

18

SOURCE: EXTRAPOLATED FROM UNITED NATIONS WORLD POPULATION PROSPECTS DATA.

Romania Internet Usage

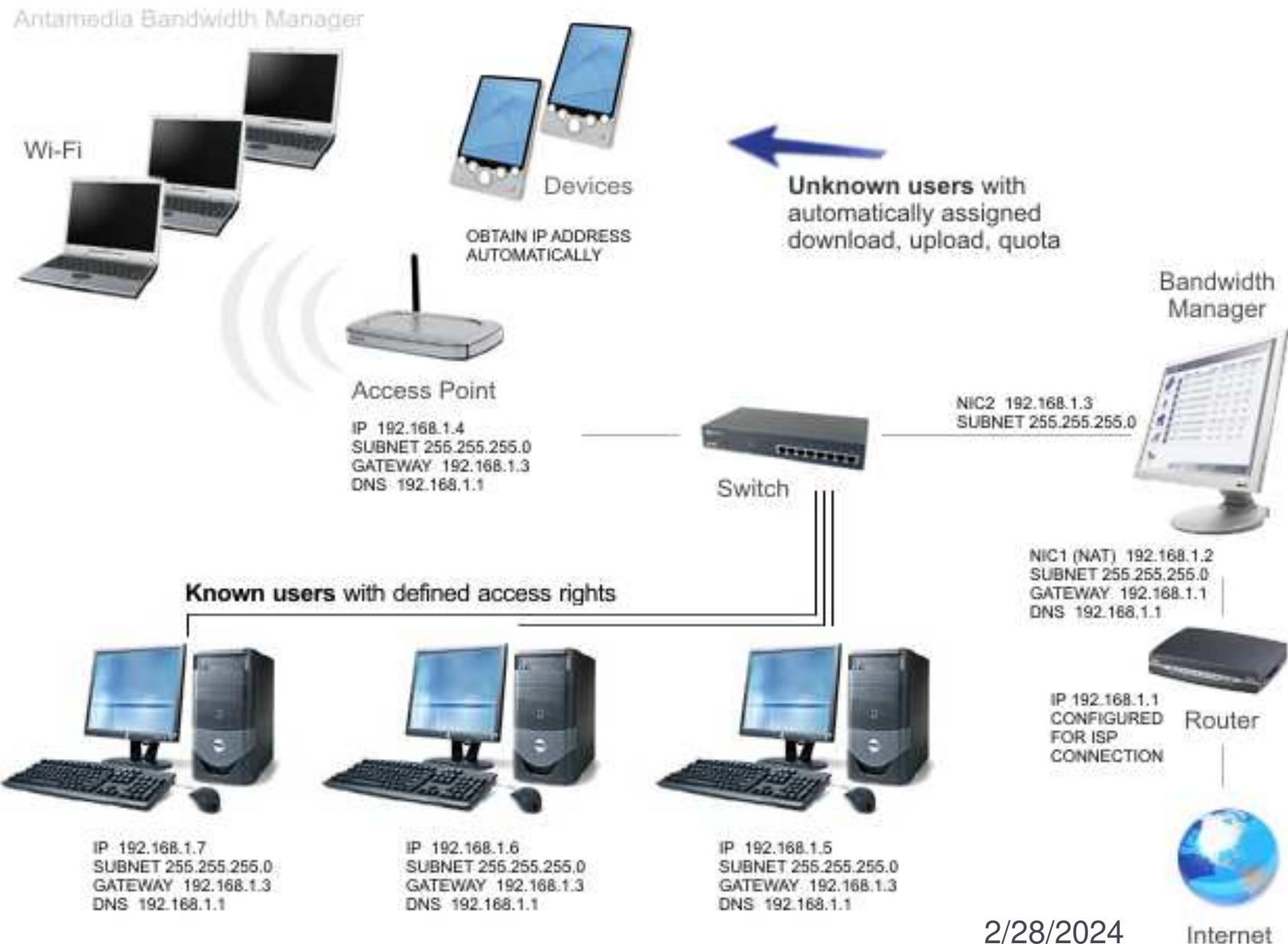




Computer Network Devices



Topologies and network devices



Physical Layer

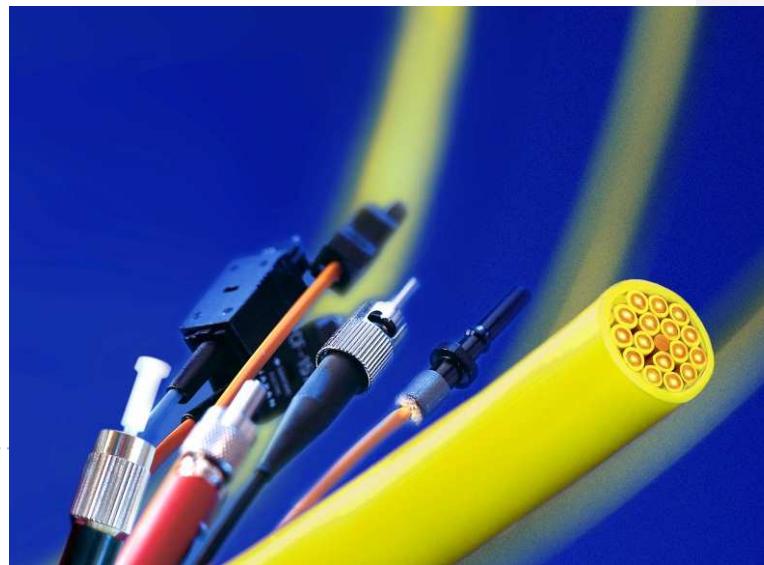
▶ Wireless

- ▶ RF
- ▶ Infrared
- ▶ Microwave



▶ Wired

- ▶ Copper: UTP, FTP, STP
- ▶ Optical fiber



Data link Layer

- ▶ Connecting devices in a LAN

- ▶ Wireless

- ▶ AP (Access Point)



- ▶ Wired

- ▶ Switch

- ▶ MAC address

- ▶ unique identifier assigned to network interfaces (48 bits)



Network Layer

- ▶ Connecting different LANs

- ▶ Wireless

- ▶ Wireless Router



- ▶ Wired

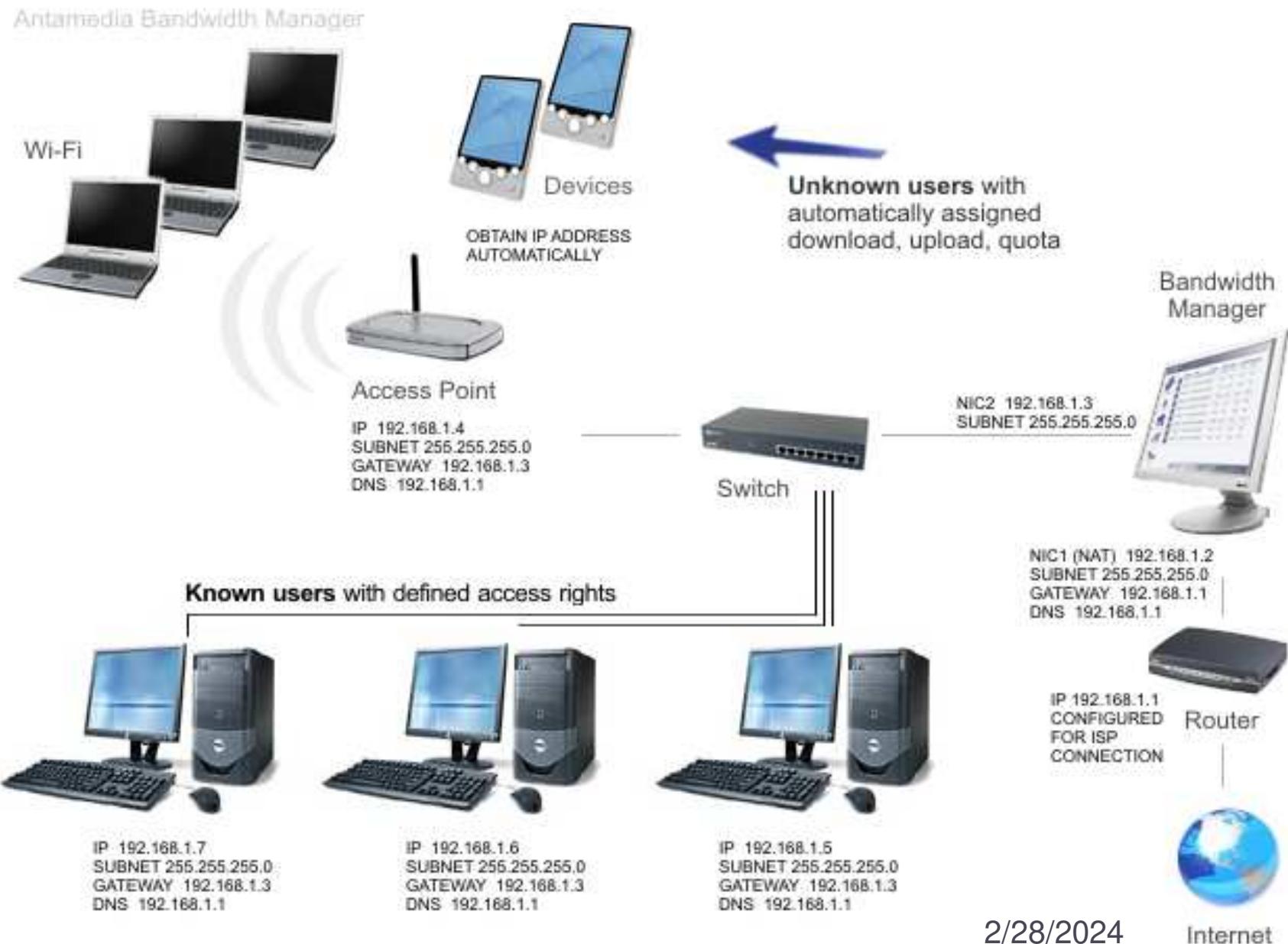
- ▶ Router

- ▶ IP address

- ▶ Version 4 (32 bits)
 - ▶ Version 6 – auto-configuration (128 bits)
(2001:0db8:3c4d:0015:0000:0000:abcd:ef12)



Topologies and network devices



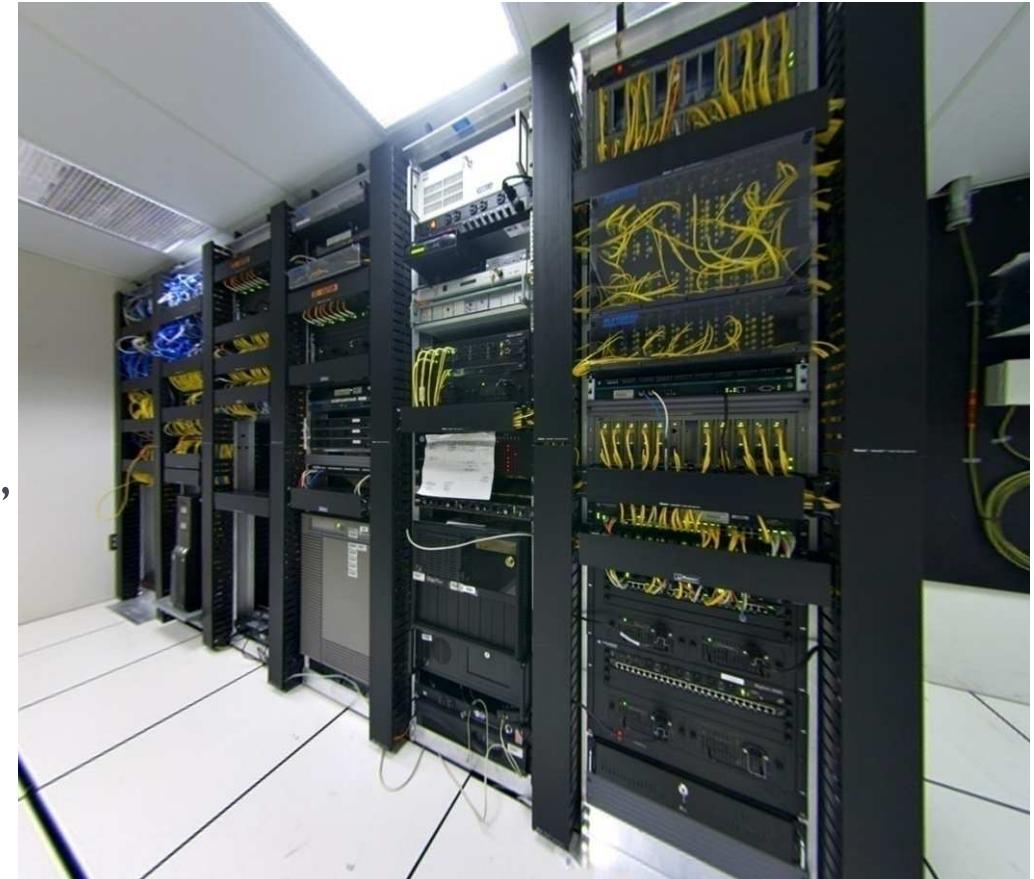


Internet and Computer Networks Evolution



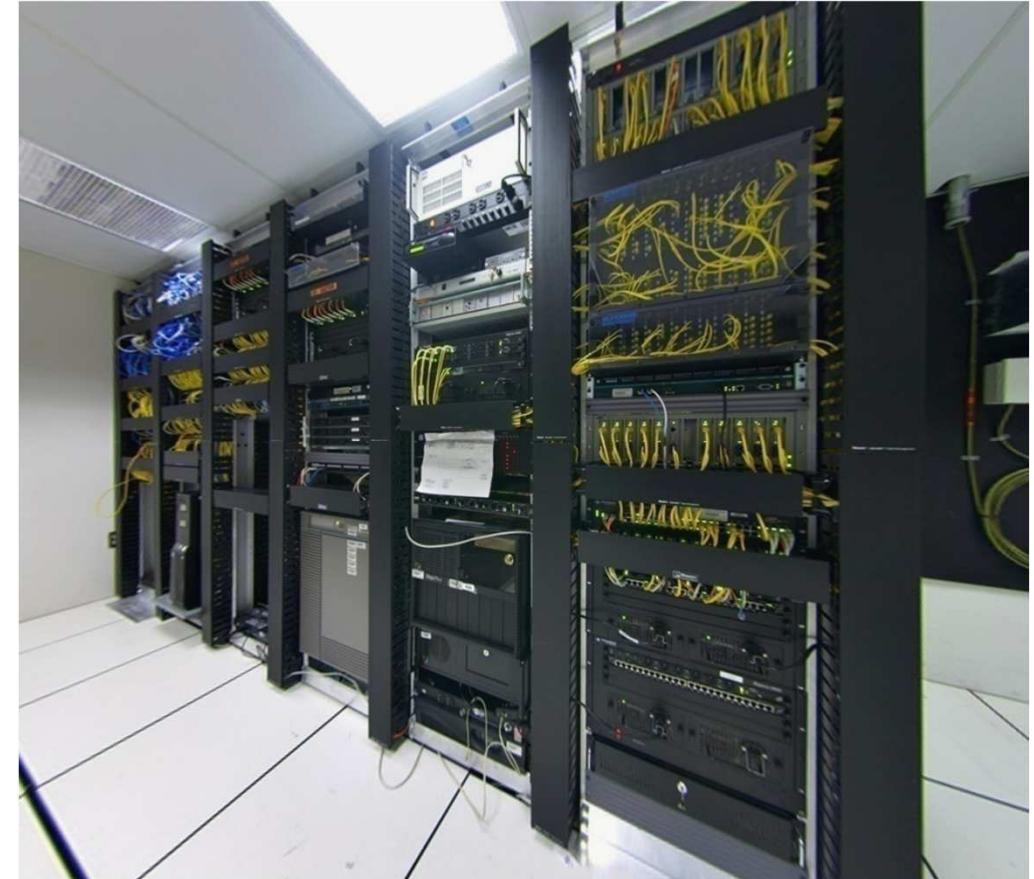
Traditional solution

- ▶ **Requirements:**
 - ▶ Office space
 - ▶ Servers
 - ▶ Cooling
 - ▶ UPS
 - ▶ Operating systems, softwares, upgrades, patches
 - ▶ Firewalls, Intrusion prevention systems, spam control, ...
 - ▶ Failover
 - ▶ Disaster recovery
 - ▶ Team of experts



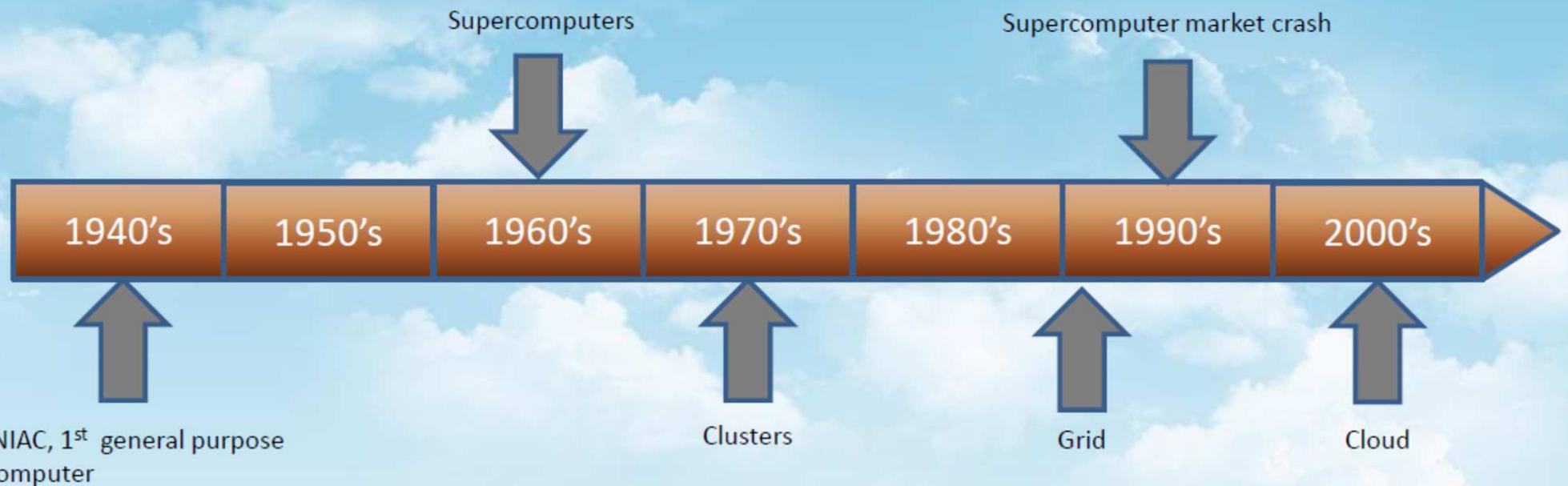
Traditional solution disadvantages

- ▶ Time consumption
- ▶ Higher costs
- ▶ Slow scaling



Evolution

Timeline:



Types of Computer Networks and their Topologies

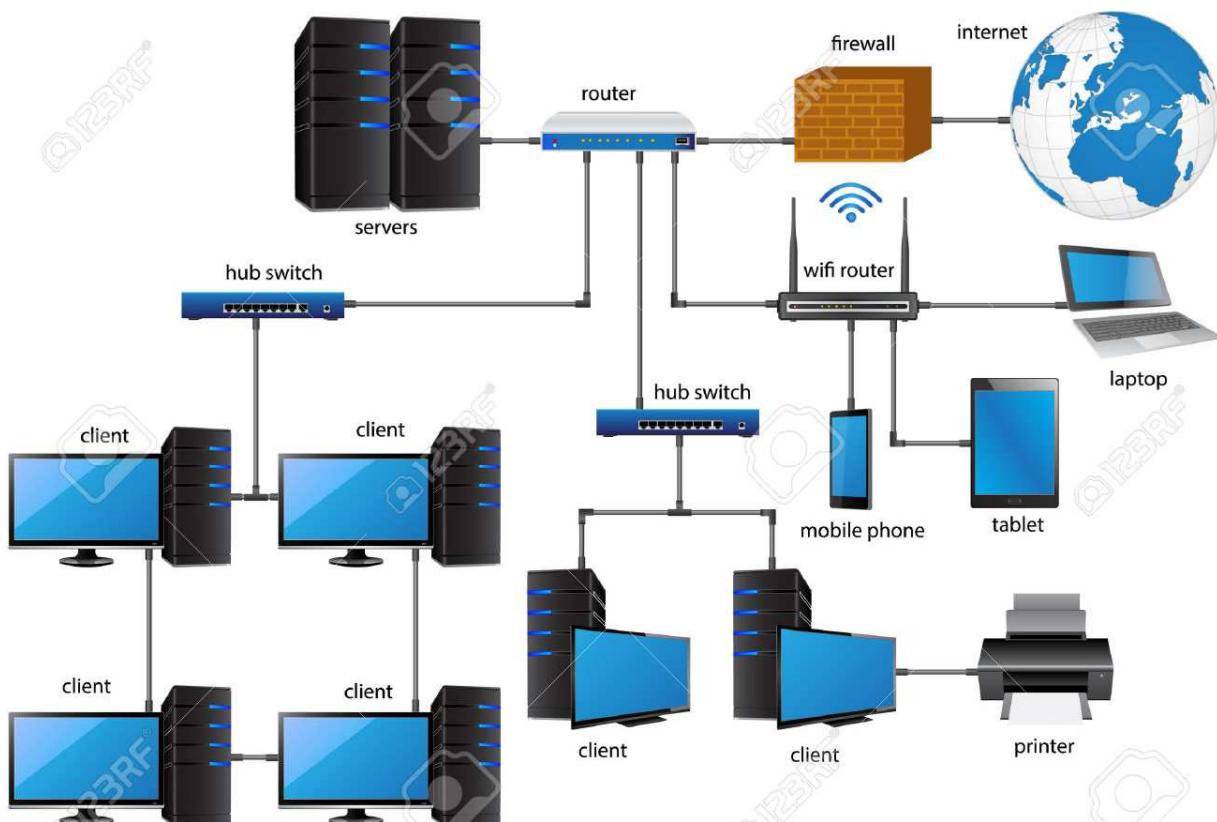
Four important groups of computer networks: PAN, LAN, MAN, WAN

PAN (Personal Area Networks)

- A network infrastructure that provides access communication between computer devices within close proximity of a user
- laptops, tablet PCs, and smartphones can communicate with each other by using a variety of wireless technologies.
- The most common technologies:
 - Bluetooth and infrared.

LAN (Local Area Networks)

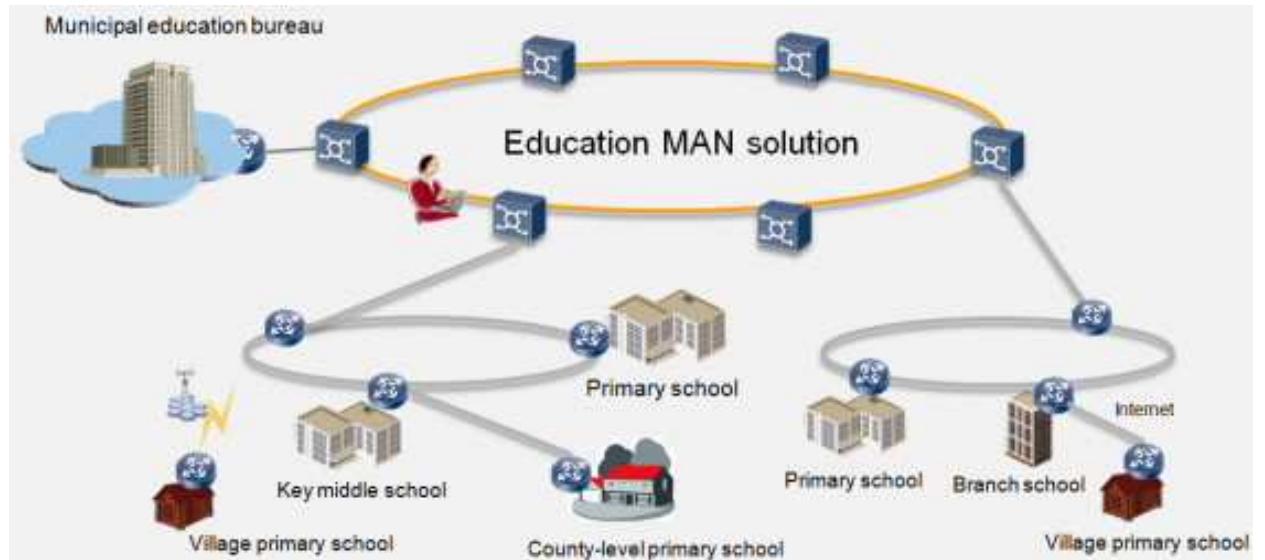
- A network infrastructure that provides access in a small geographical area:
 - enterprise, home, or small business network
 - owned and managed by an individual or IT department.
- Generally broadcast
 - Ethernet
 - Token Ring



LAN Network Diagram

MAN (Metropolitan Area Networks)

- network infrastructure that spans a physical area larger than a LAN but smaller than a WAN (e.g., a city).
- Interconnecting LANs
- MANs are typically operated by a single entity such as a large organization.
 - Different ownership, rental, sharing agreements
- e.g. FDDI, CDDI
- Own broadband infrastructure
 - transport and switching
 - Often public, 3rd party infrastructure



WAN (Wide Area Networks)

- Generally cover a large geographical area (country, continent, global)
- Interconnecting hosts, LANs, MANs
- Typically owned and managed by a telecommunications service provider
- Consists of a number of interconnected switching nodes
- Rely at least in part on circuits provided by one or more *common carriers*—companies that offer communication services to the general public
- Fixed, satellite, mobile narrowband, broadband
- ▶ Wide range of physical infrastructure

Problems to be discussed when presenting a network:

Sample network: a Wired LAN

Application domain

Standards bodies and their issues

Topologies

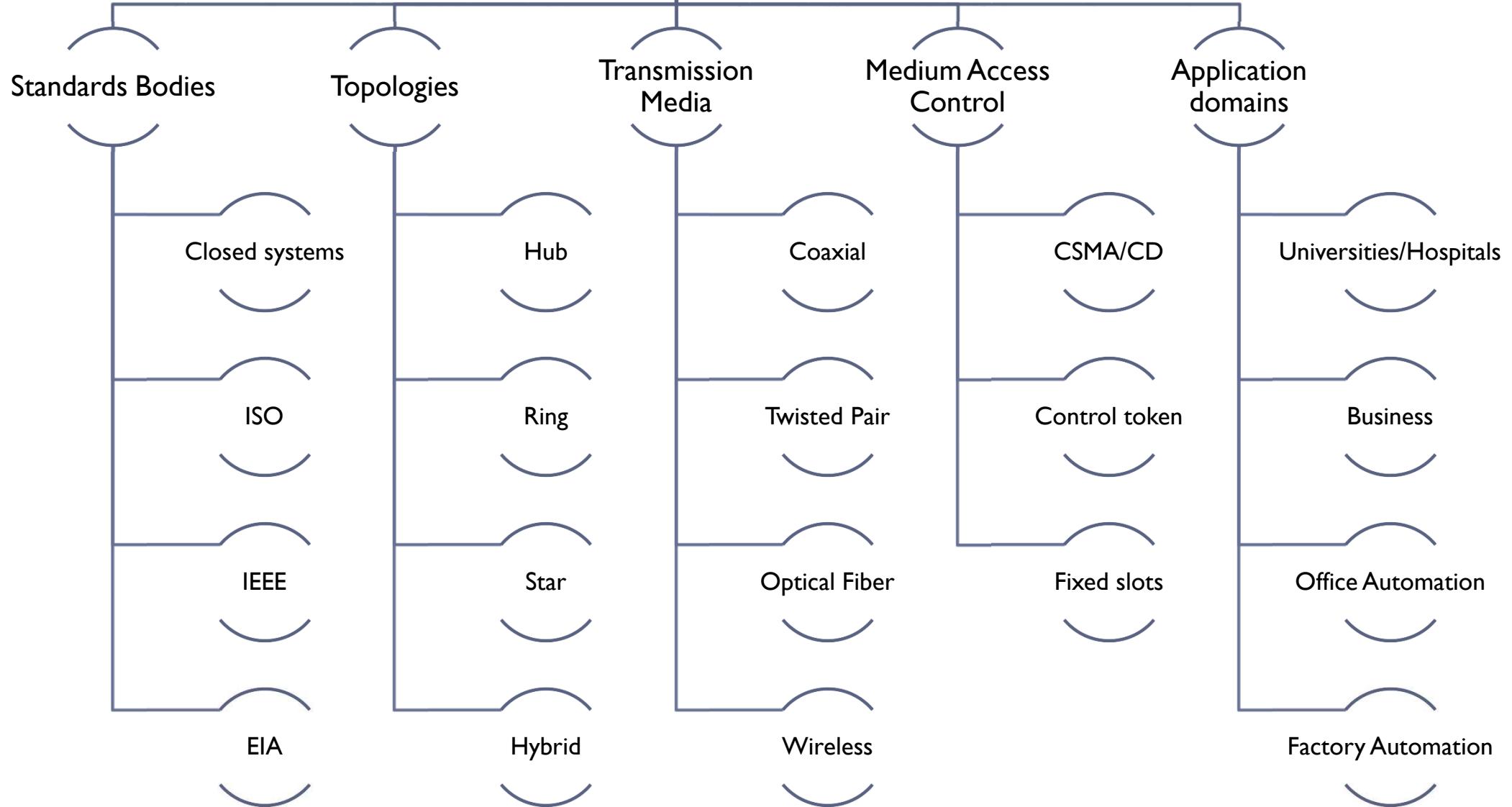
Internetworking Protocols

Medium Access Control

Transmission Media

See next slide as example:

Wired LAN



Network Topologies

Network Topology – Definition:

The specific physical, *i.e.*, real, or logical, *i.e.*, virtual, arrangement of the elements of a network.

Two networks **have the same topology** if the connection configuration is the same, although the networks *may differ* in physical interconnections, distances between nodes, transmission rates, and/or signal types.

Vertical Topology

Hierarchical

Mesh

Horizontal Topology

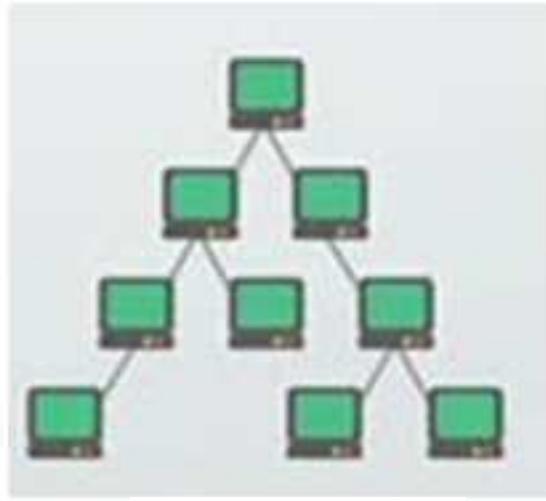
Star

Bus

Tree

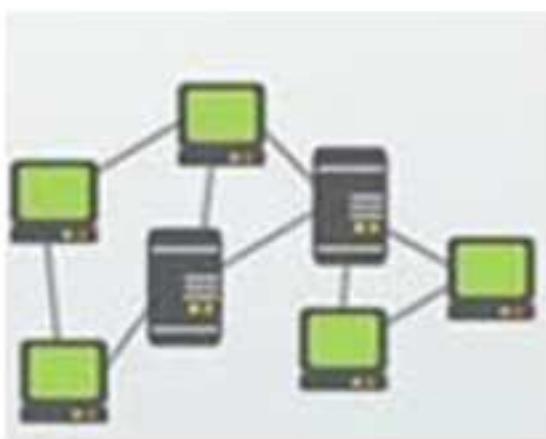
Ring

Vertical Topology



Hierarchical

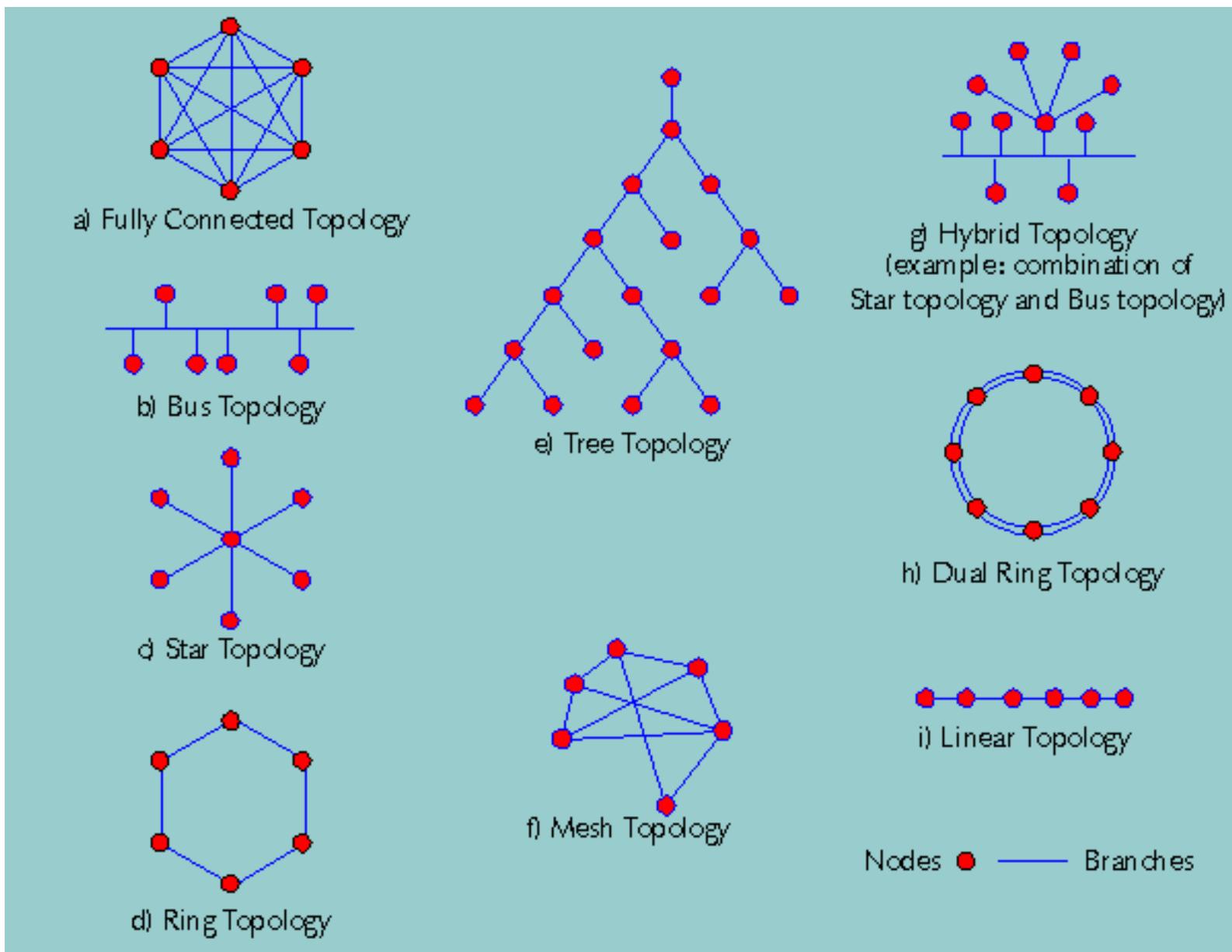
Hierarchical (tree) topology: existence of a **central node** (root) and of various sets of level organized nodes (intermediary nodes); the leaves of the tree are the workstations. The data flow between any two nodes goes up-down using the upper levels nodes.



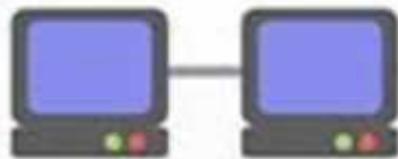
Mesh

Mesh topology: there are at least two nodes with two or more paths between them.

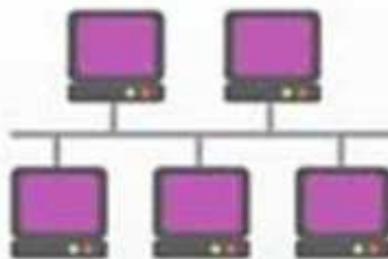
Various Topologies



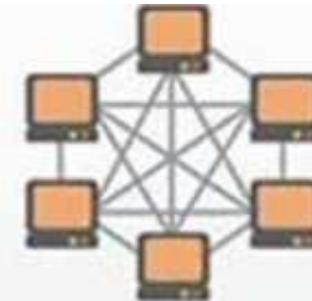
Various Topologies



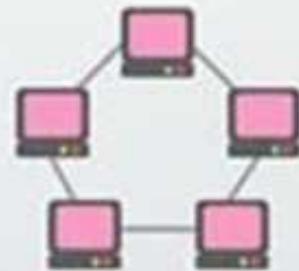
point-to-point



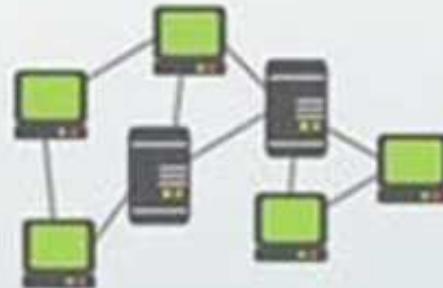
bus



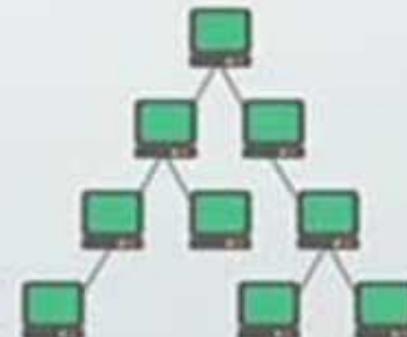
hybrid



ring



mesh



tree



star

‘Main’ Horizontal Topologies

Bus topology: all nodes, *i.e.*, stations, are connected together by a single bus (the main trunk). Stations are connected using interfaces, named transceivers or attachment units (AUI).

Ex: pure Ethernet LAN, Token Bus.

Multipoint medium

Transmission propagates throughout medium

Heard by all stations

Need to identify target station

Each station has unique address

Full duplex connection between station and AUI

Allows for transmission and reception

Need to regulate transmission

To avoid collisions and hogging

Data in small blocks - frames

Terminator absorbs frames at end of medium

Ring topology: every node has exactly two branches connected to it (a succession of point-to-point links). Stations are connected using interfaces (repeaters).

Ex: Token Ring LAN.

Repeaters joined by point to point links in closed loop

Receive data on one link and retransmit on another

Links unidirectional

Data in frames

Circulate past all stations

Destination recognizes address and copies frame

Frame circulates back to source where it is removed

Media access control determines when station can insert frame

Dual Ring – allows for a second (reserve) ring; data flow has here an opposite direction; not all stations linked to both rings

Star topology: there is a central node (switch) and peripheral nodes. The peripheral nodes are connected to the central node, which rebroadcasts all transmissions received from any peripheral nodes to all peripheral nodes on the network, including the originating node. Ex: switched Ethernet LAN.

Extended star: links individual stars together, by linking the centers (hubs/switches); also known as snowflake topology.

Need for more distance between computers => Layer 1 device **repeater**

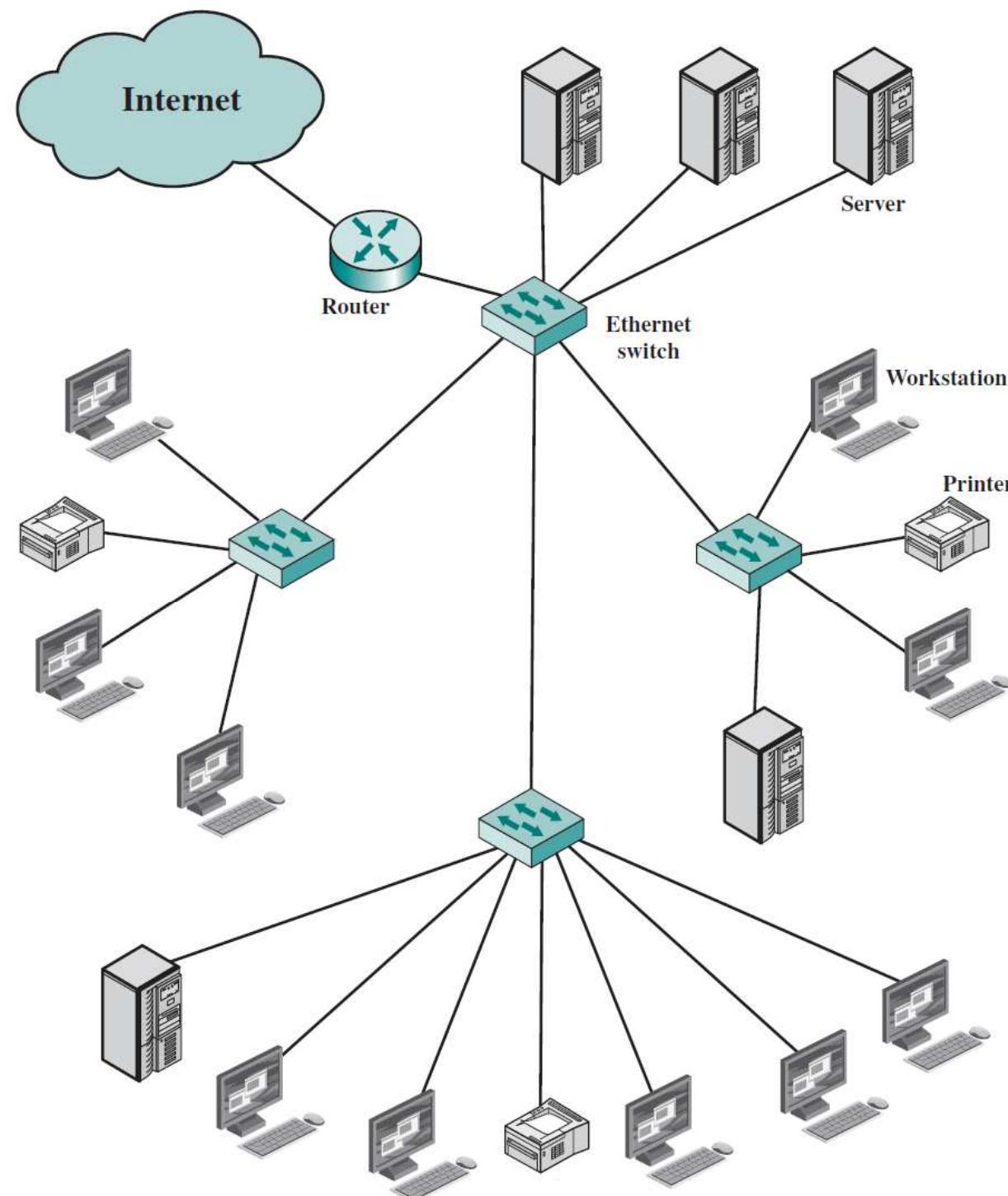
Need for more workgroup connectivity => **multiport repeater**, or **hub**.

Need for traffic filter => **bridge** as a way to filter network traffic into local and non-local traffic (Layer 2 device, based on physical address)

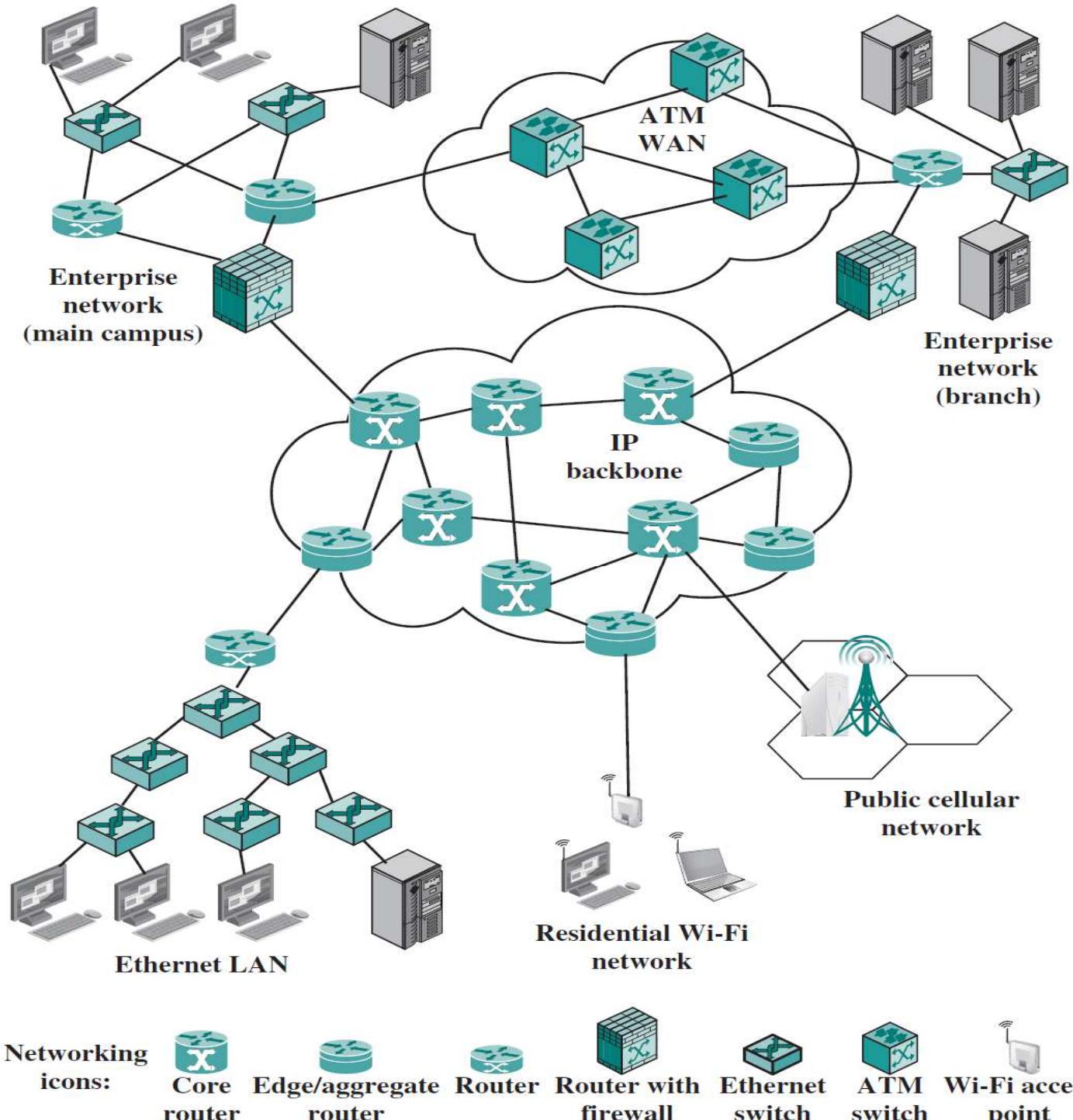
Need for Layer 2 connectivity (port-density) => a **multiport bridge**, or **switch**

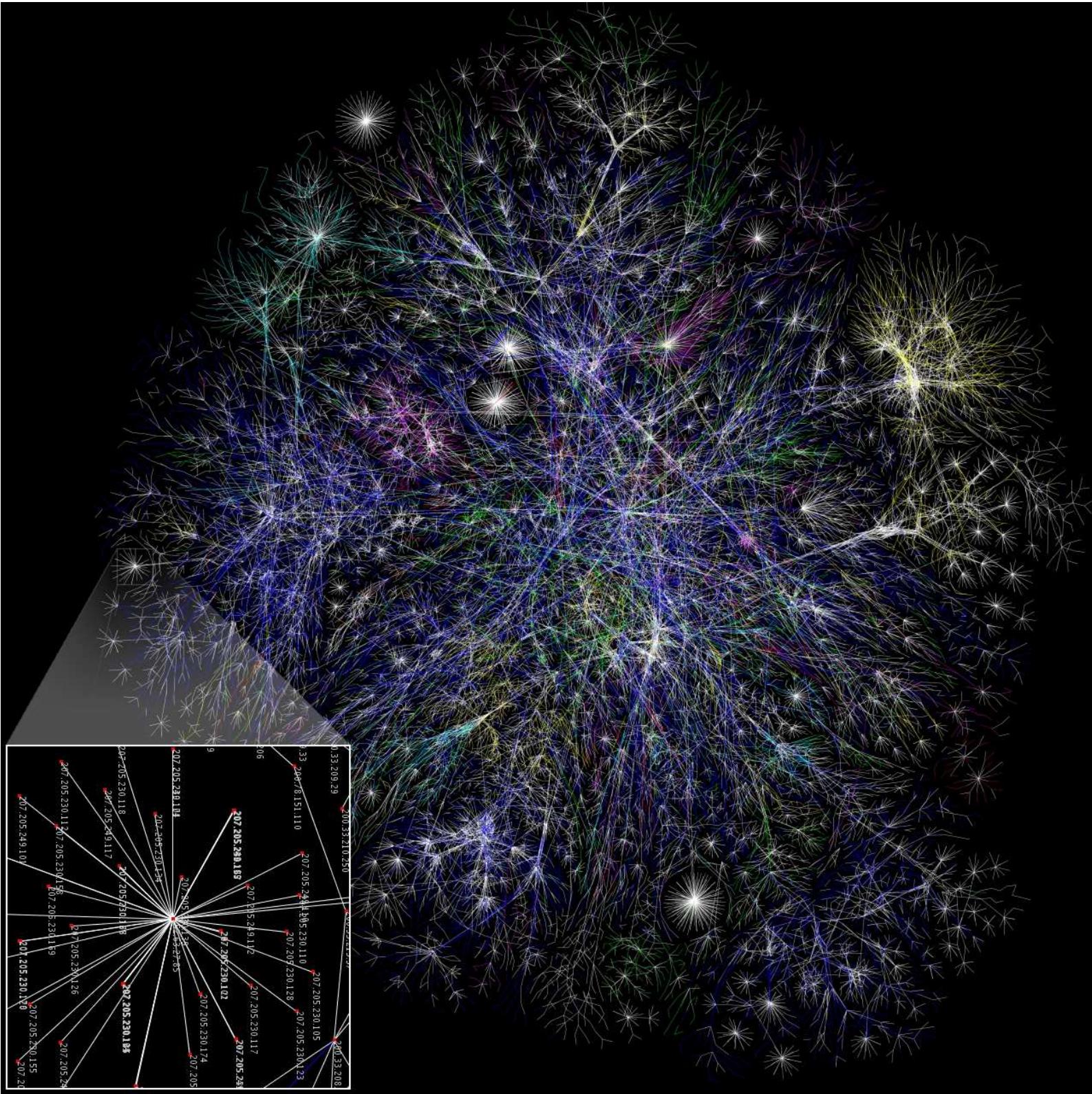
As networks grew, the diversity of platforms, protocols, and media, the geographic distance between computers, the number of computers wishing to communicate, and the dynamism inherent in large networks, all necessitated the development of the **router**. Layer 3 device which makes best path and switching decisions based on network addresses.

Example of an hierarchical, complex network



Example of an hierarchical, complex network





Lecture 2

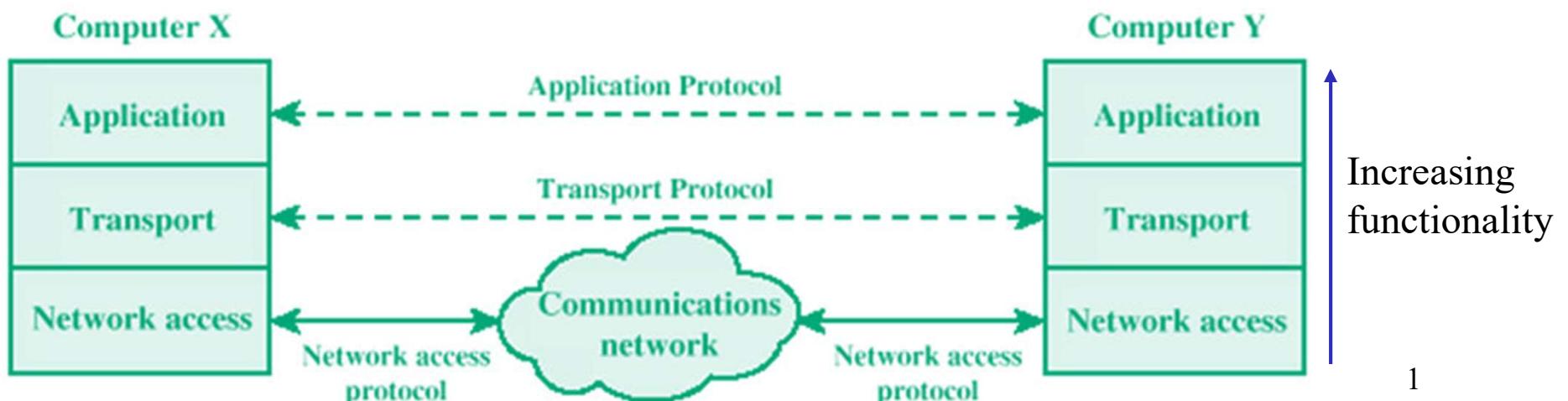
Communications Protocols & Reference models

Communications Protocol: General introduction

Communications (network) Protocols

- set of agreed procedures & languages used in those networks
- usually specified in a hierarchy of layers
- high-level layers (carry specific applications)
 - give ability for 2 systems to exchange and understand information for some particular application
- low-level (data transfer)
 - how physical data transmission media is actually used independent of application

A simplified three layer model:



Protocol Characteristics & Hierarchies

Characteristics

Direct or indirect

Direct

- Systems share a point to point link or

- Systems share a multi-point link

- Data can pass without intervening active agent

Indirect

- Switched networks or

- Internetworks or internets

- Data transfer depend on other entities

Monolithic or structured

Communications is a complex task, too complex for a single protocol unit

Structured design breaks down problem into smaller units, obtaining a layered structure

Symmetric or asymmetric

Symmetric

Communication between
peer entities

Asymmetric

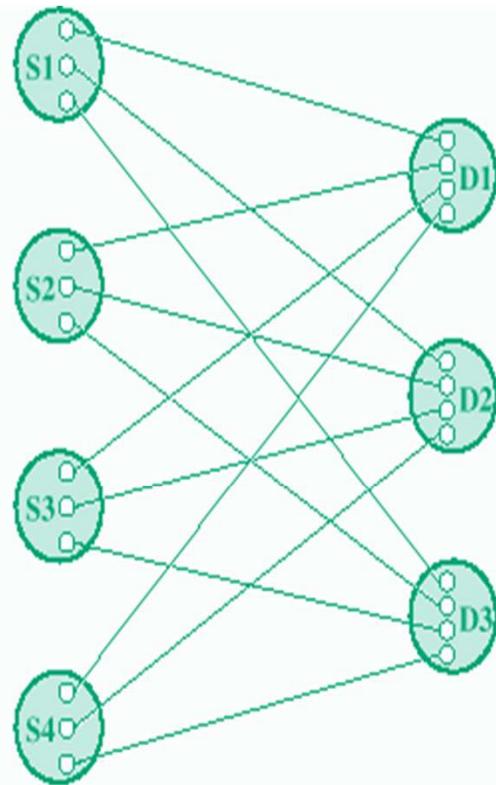
Client/server

Standard or nonstandard

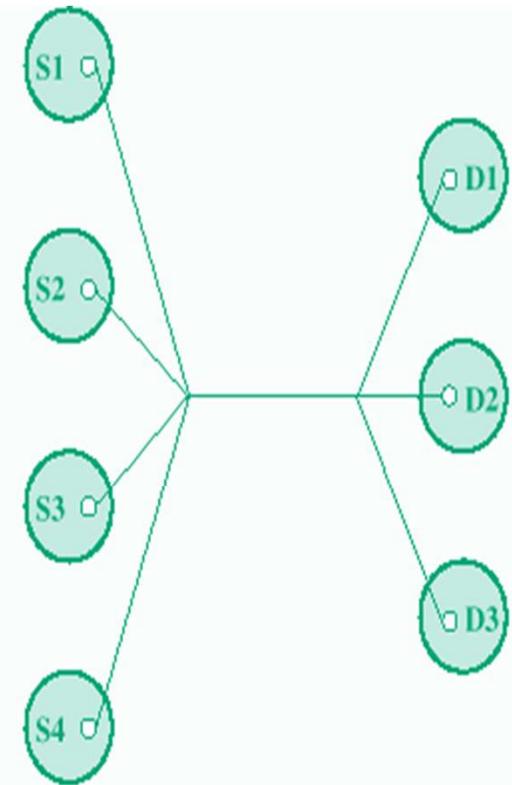
Nonstandard protocols built for specific computers and tasks

K sources and L receivers leads to $K \times L$ protocols and $2 \times K \times L$ implementations

If common communications protocol used, $K + L$ implementations needed (see figure above)



(a) Without standards: 12 different protocols;
24 protocol implementations



(a) With standards: 1 protocol;
7 implementations

Comms Protocols Main Functions (general introduction)

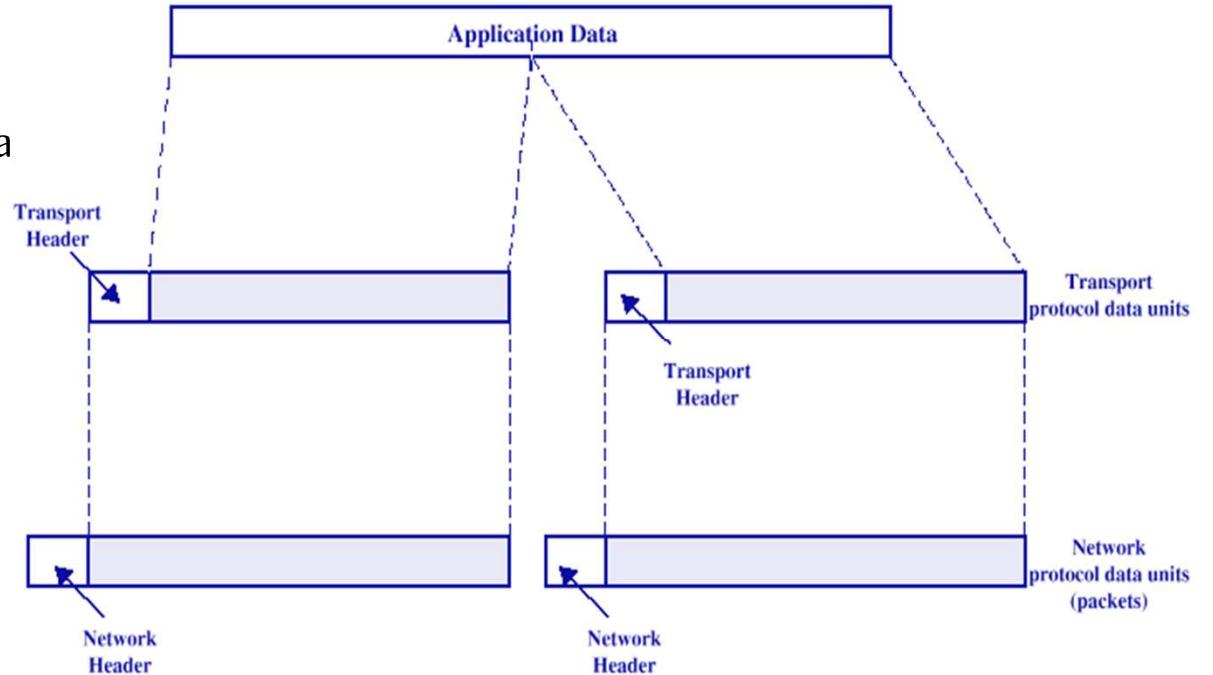
Encapsulation

Add of **control** information to data

- Address information

- Error-detecting code

- Protocol control



Segmentation (fragmentation) and reassembly

Data blocks for one protocol are of bounded size

Application layer messages may be large; Network packets may be smaller

Splitting larger blocks into smaller ones is segmentation (or fragmentation in TCP/IP)

ATM blocks (cells) are 53 octets long, Ethernet blocks (frames) are up to 1526 octets long

Use of checkpoints and restart/recovery

Allows for efficient control & resource use, but more overhead & processing time

Connection control

Three phases:

- Connection Establishment
- Data transfer
- Connection termination

Sequence numbers used for

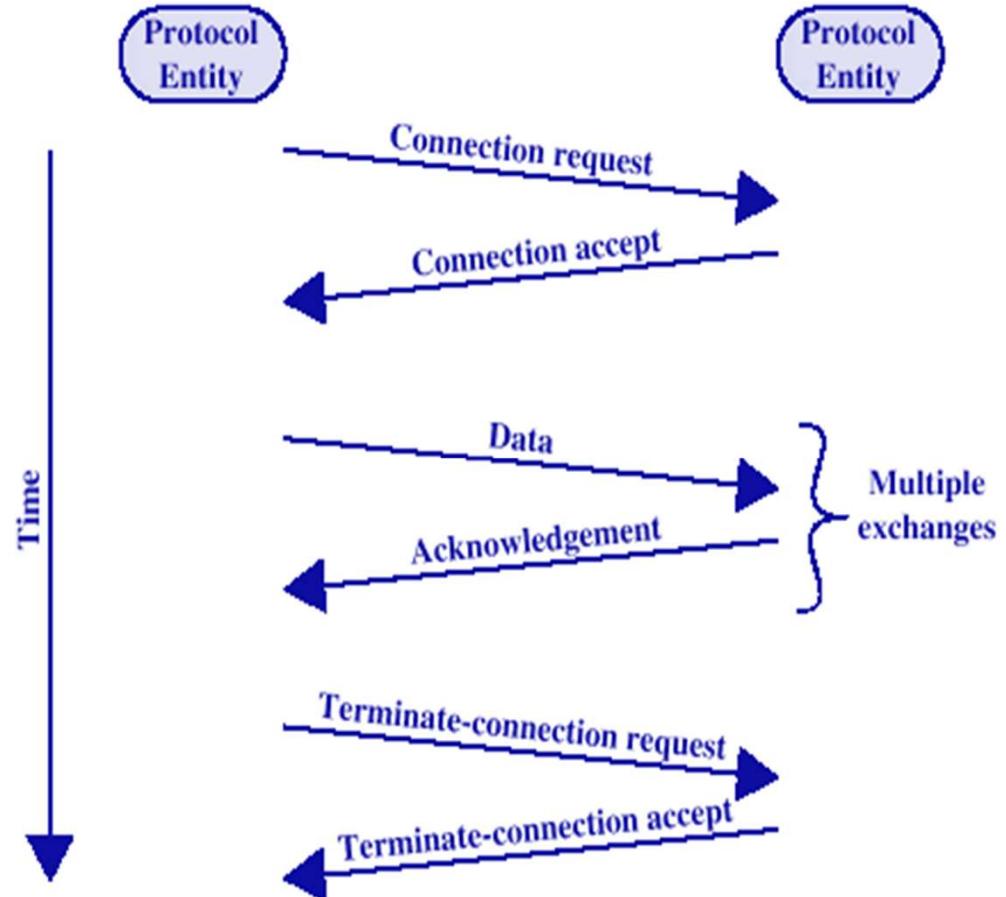
- Ordered delivery
- Flow control
- Error control

Ordered delivery

For each protocol specific data (PDUs) may traverse different paths through network

PDUs may arrive out of order

Sequentially number PDUs to allow for ordering



Flow control

Done by receiving entity: limits amount or rate of received data

- Stop and wait

- Credit systems

- Sliding window

Error control

Guard against data loss or damage

Error detection

- Sender inserts error detecting bits

- Receiver checks these bits

- If OK, acknowledge

- If error, discard packet

Retransmission

- If no acknowledge in given time, re-transmit

Performed at various levels

Multiplexing

Supporting multiple connections on one machine

Mapping of multiple connections at one level
to a single connection at another

Carrying a number of connections on
one fiber optic cable

Addressing

Addressing level

Level in architecture at which entity is named

Unique address for each computer and router

Network level address

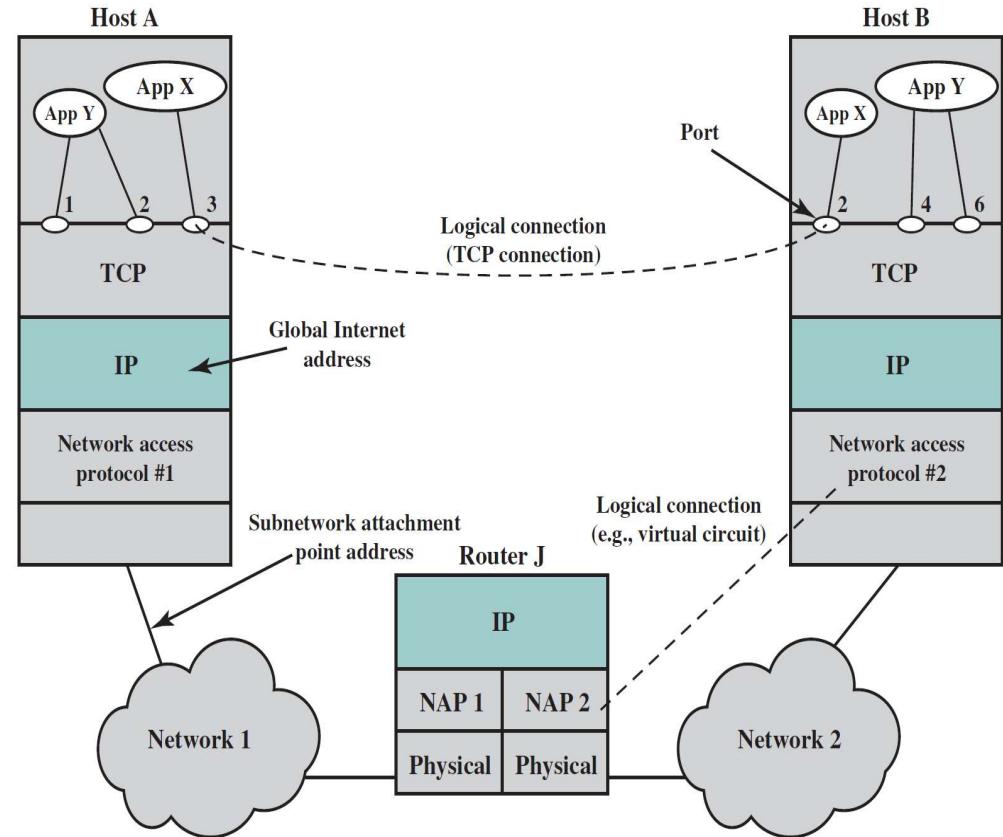
IP or internet address (TCP/IP)

OSI's Network service access point

Process within the system

Port number (TCP/IP)

Service access point or SAP (OSI) Addressing



Addressing scope

Global non-ambiguity

Global address identifies unique system

There is only one system with address X

Global applicability

It is possible at any system (any address) to identify any other system (address) by the global address of the other system

Address X identifies that system from anywhere on the network

e.g. MAC address on IEEE 802 networks

Connection identifiers

Connection oriented data transfer (virtual circuits)

Allocate a connection name during the transfer phase

Reduced overhead as connection identifiers are shorter than global addresses

Routing may be fixed and identified by connection name

Entities may want multiple connections - multiplexing

State information

Addressing modes

Usually an address refers to a single system

 Unicast address: data sent to one machine or person

May address all entities within a domain

 Broadcast: sent to all machines or users

May address a subset of the entities in a domain

 Multicast: sent to some machines or a group of users

Transmission services

Priority

 e.g. control messages

Quality of service

 Minimum acceptable throughput

 Maximum acceptable delay

Security

 Access restrictions

Comms Protocols Hierarchies (layered structure)

- organised in layers
- higher layers use services of lower layers (concepts of service user + service provider)
- each protocol layer adds value
- no similar functions in different layers
- highest layer service is exported to user
- layered organization means
 - o— cleaner operation
 - o— easier design & modification

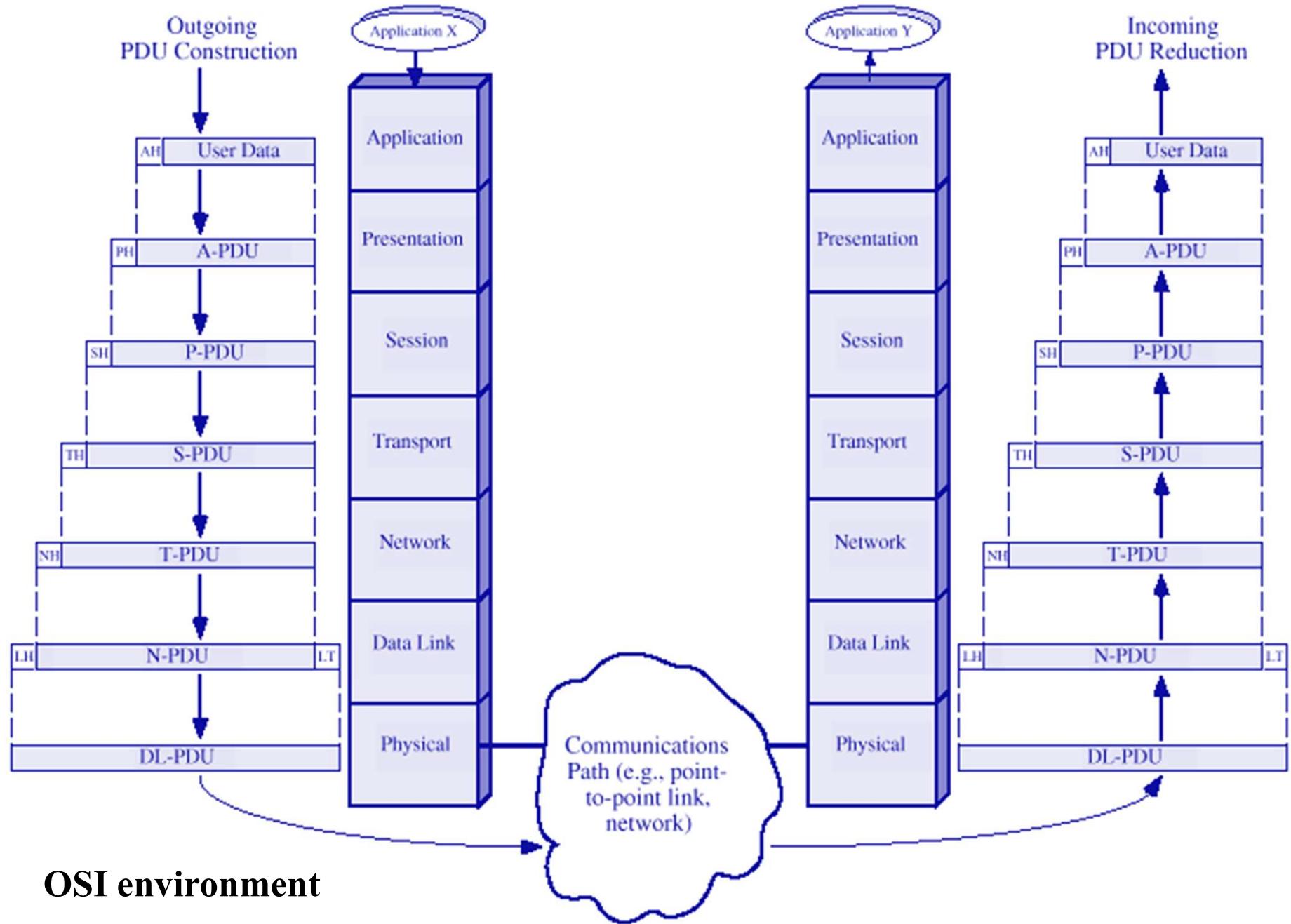
Number, name & function of layers differ from network to network (different protocol stacks)

OSI Reference Model

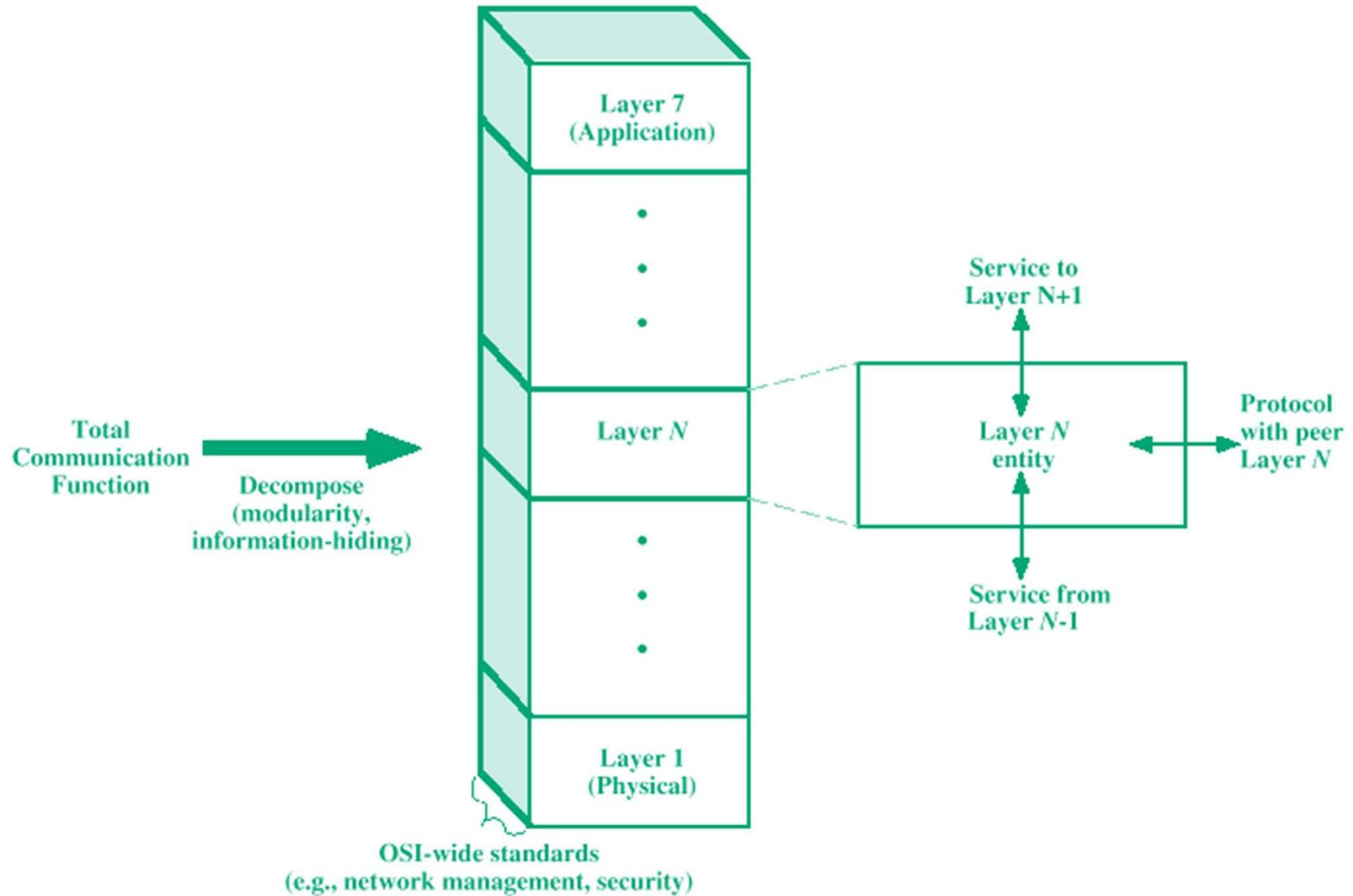
ISO Open Systems Interconnection Reference Model, ISO 7489

- a basic reference model
 - common basis for standards development
 - perspective on existing standards
 - specifies external behavior of systems, using **reference interfaces** – provide openness
- 7 layer model
- objective is to be a common base for any exchange of information
- physically info moves down - across - up
- logically each layer converses with peer
- each layer relies on the next lower layer to perform more primitive functions
- each layer provides services to the next higher layer
- changes in one layer should not require changes in other layers

(see next figure)



OSI environment



OSI as framework for standardization

Elements of Standardization

Protocol specification

Operates between the same layer on two systems

May involve different operating system

Protocol specification must be precise

Format of data units

Semantics of all fields

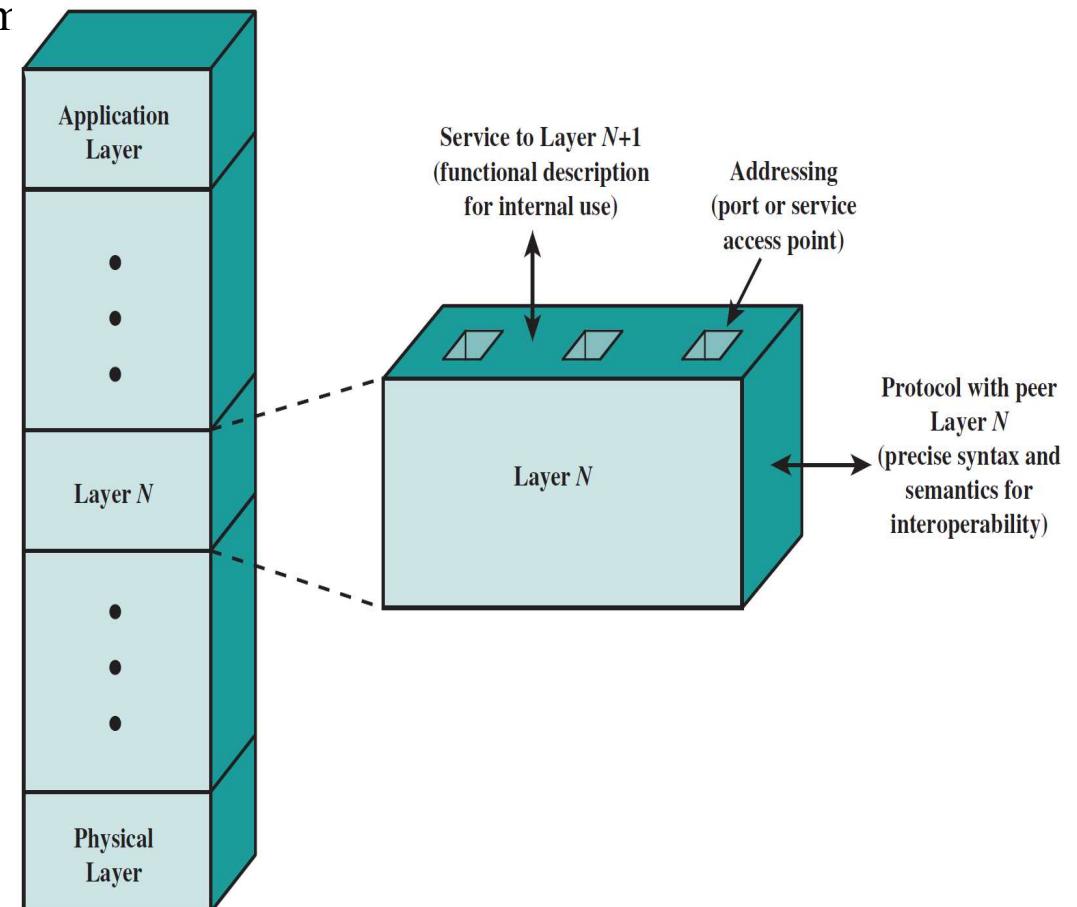
Allowable sequence of PDUs

Service definition

Functional description of what is provided

Addressing

Referenced by SAPs



Physical Layer

- “access actual media”
- Describes media interface and use
 - o— type of media
 - o— physical connection
 - o— how transmit & receive information
 - o— bit synchronisation
 - o— media dependent signals

Aplicație/Application	7
Prezentare/Presentation	6
Sesiune/Session	5
Transport	4
Rețea/Network	3
Legătură de date/Data Link	2
Fizic/Physical	1

Data Link Layer

- “manage individual (data) links between systems”
- Direct data link management
 - o— framing
 - o— addressing
 - o— sequencing & windowing
 - o— error detection & correction
 - o— access control
 - o— link management
 - o— node to node flow control

Network Layer

- “manages networks of links”
- provides for info transfer over a network
 - o— addressing
 - o— message forwarding
 - o— routing
 - o— congestion control
 - o— flow control
 - o— billing & accounting
- similar functions to Data Link / Transport layers
 - segmentation, multiplexing, sequencing, error control

Transport Layer

- “end to end data transfer”
- reliable, universal transport service
 - o— multiplexing
 - o— addressing
 - o— connection management
 - o— message segmentation
 - o— sequencing
 - o— error control
 - o— end to end flow control

Aplicație/Application	7
Prezentare/Presentation	6
Sesiune/Session	5
Transport	4
Rețea/Network	3
Legătură de date/Data Link	2
Fizic/Physical	1

Session Layer

- “dialog control”
- manages logical communication sessions
 - o— dialog discipline (half vs full duplex)
 - o— grouping
 - o— checkpoint & recovery
 - o— resource management

Only used by some applications

Aplicație/Application	7
Prezentare/Presentation	6
Sesiune/Session	5
Transport	4
Rețea/Network	3
Legătură de date/Data Link	2
Fizic/Physical	1

Presentation Layer

- “common format & language for messages”
- define format of data exchanged
 - o— data format transformation and security issues
 - code conversion
 - compression
 - encryption
 - screen formatting
 - o— protocol conversion
 - o— database management

Application Layer

- “application services & access mechanisms”
- defines interface for any applications
- defines network management functions
- defines specific general-purpose applications – VT, FTAM, X.400, X.500

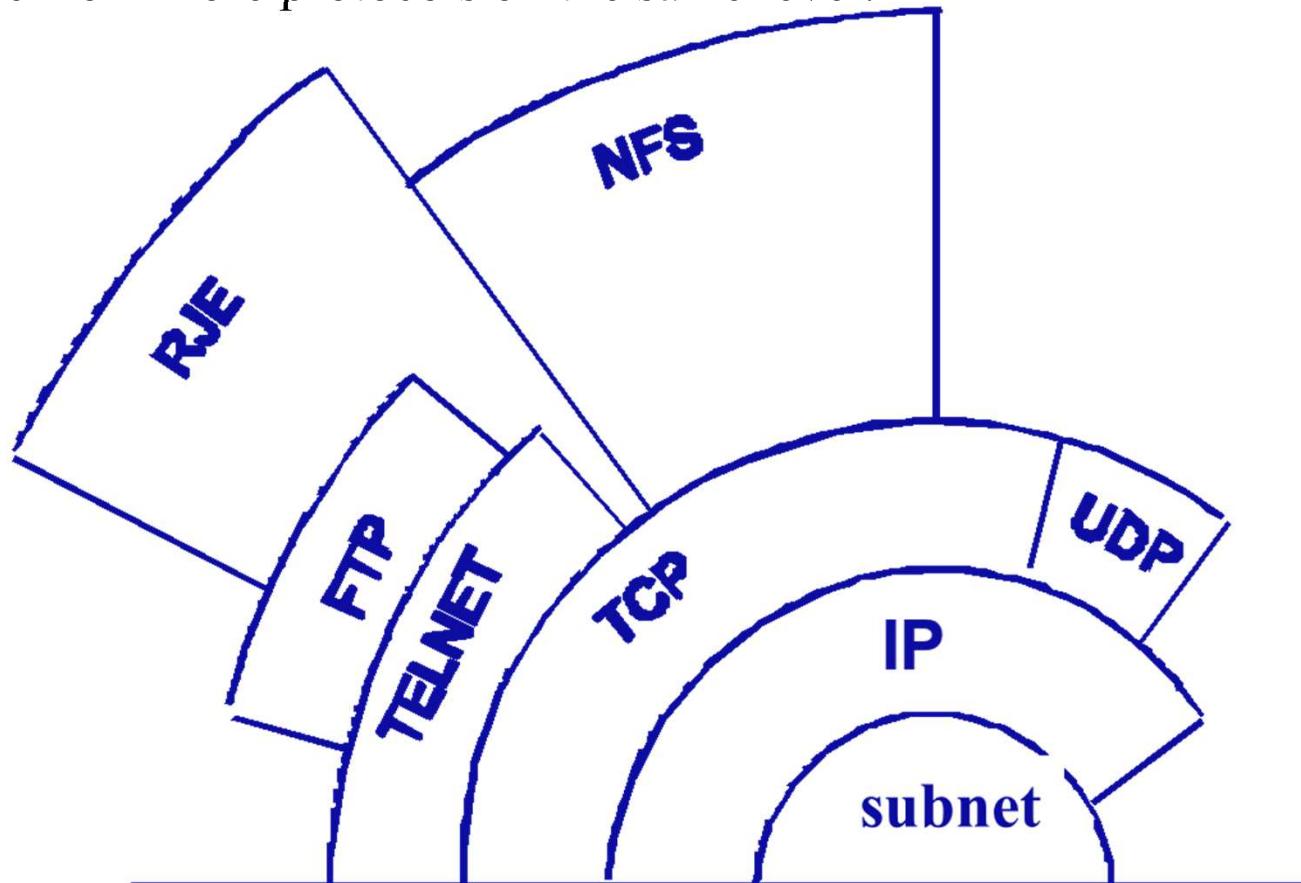
It's a Reference Model , so:

- not all functions, not all layers, need be used in an application
- “layered models are a very good way to design network protocols, but a very poor way to implement them” Van Jacobson
- in practice, often merge layer functions, see the three layer model
- are many different actual protocols in use
- but still a good reference model, excellent support for teaching

TCP/IP Reference Model (DoD DARPA)

May be considered TCP/IP a reference model? Sure it is a model, the 'de facto' standard for today implementations! Used by the Internet

A hierarchy of levels; also communications between non-adjacent levels; can choose of one from more protocols on the same level.



TCP/IP Protocol Architecture

Application Layer

Communication between processes or applications

- remote access RLOGIN
- file transfer FTP, TFTP
- electronic mail SMTP
- information retrieval NIR
- network management SNMP

End to end or transport layer (TCP/UDP/..)

End to end transfer of data

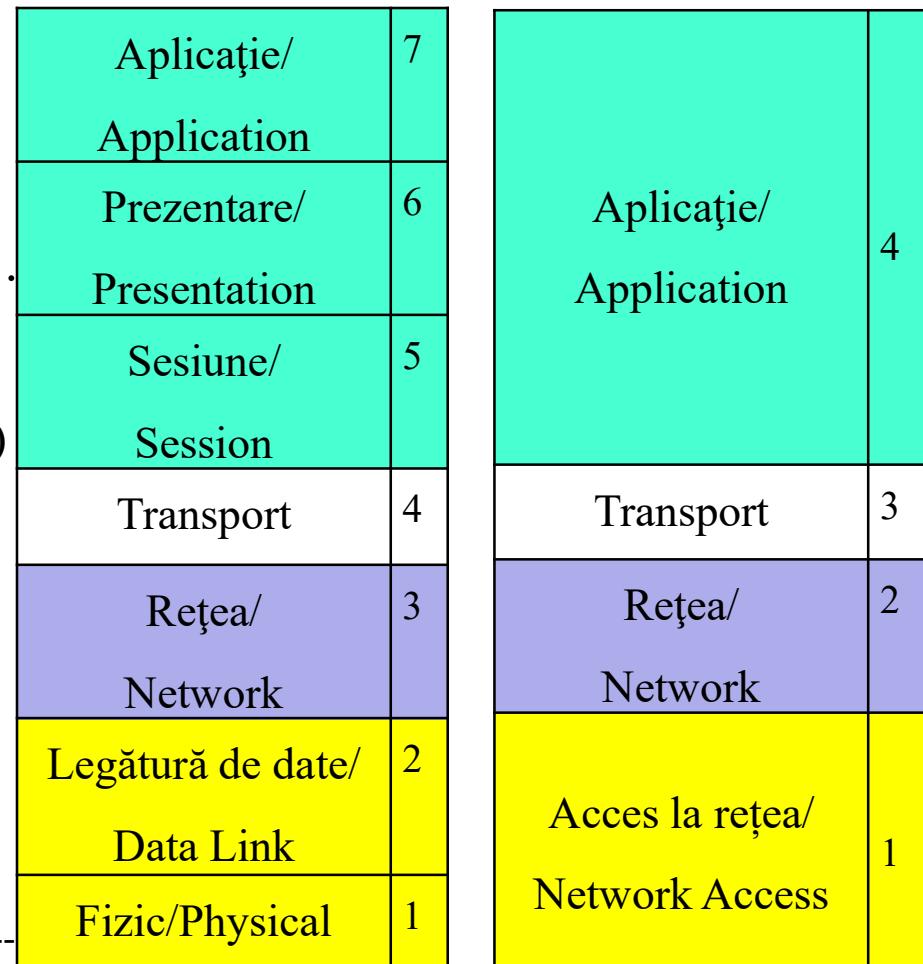
May include reliability mechanism (TCP)

Internet Layer (IP)

Routing of data

Address resolution

Routing protocols



Subnet Level

Net access

Logical interface between end system and network

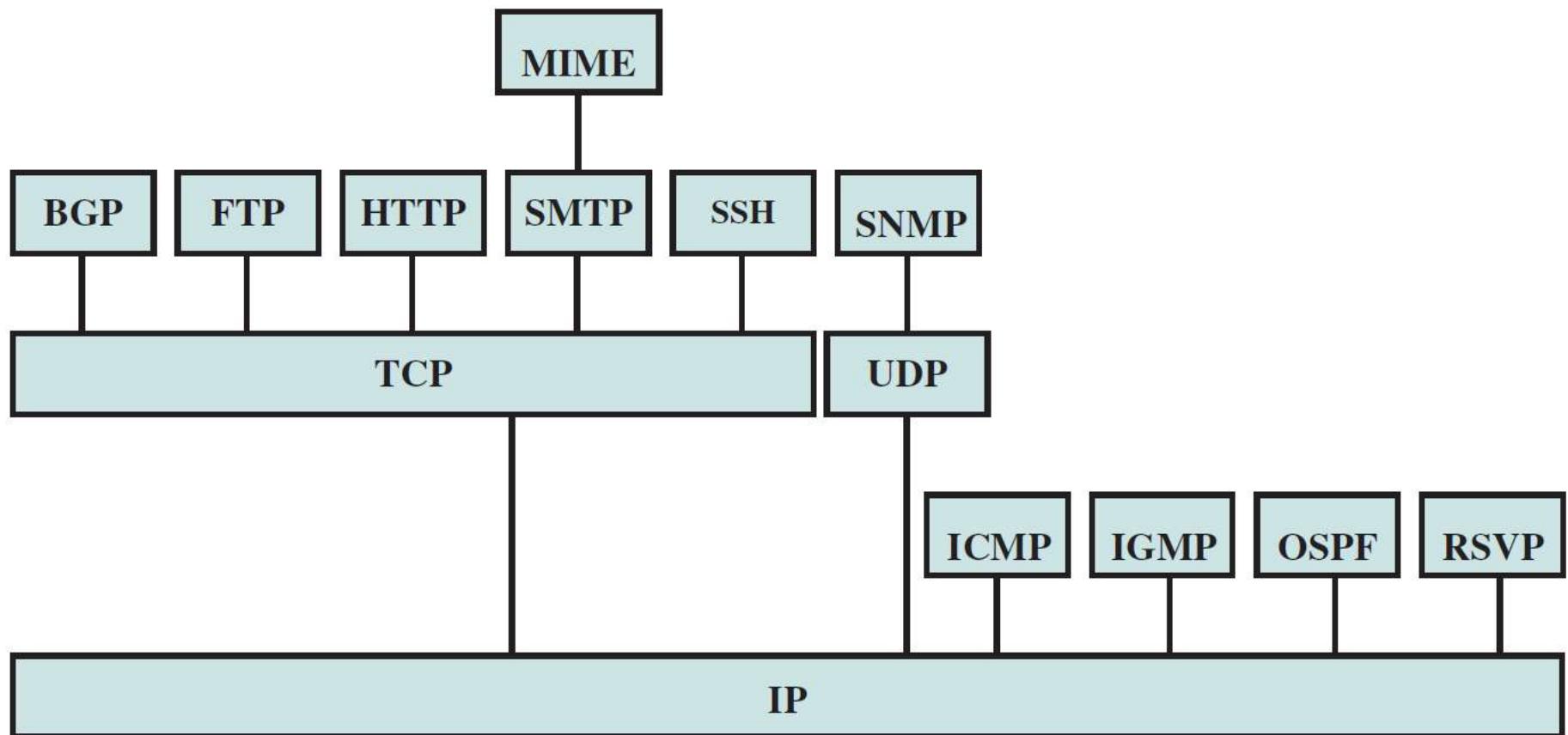
Physical access

Transmission medium

Signal rate and encoding

Aplicație/ Application	7	Aplicație/ Application	4
Prezentare/ Presentation	6		
Sesiune/ Session	5		
Transport	4	Transport	3
Rețea/ Network	3	Rețea/ Network	2
Legătură de date/ Data Link	2	Acces la rețea/ Network Access	1
Fizic/Physical	1		

Some of the components of the TCP/IP protocol suite are depicted in next slide



BGP = Border Gateway Protocol

FTP = File Transfer Protocol

HTTP = Hypertext Transfer Protocol

ICMP = Internet Control Message Protocol

IGMP = Internet Group Management Protocol

IP = Internet Protocol

MIME = Multipurpose Internet Mail Extension

OSPF = Open Shortest Path First

RSVP = Resource ReSerVation Protocol

SMTP = Simple Mail Transfer Protocol

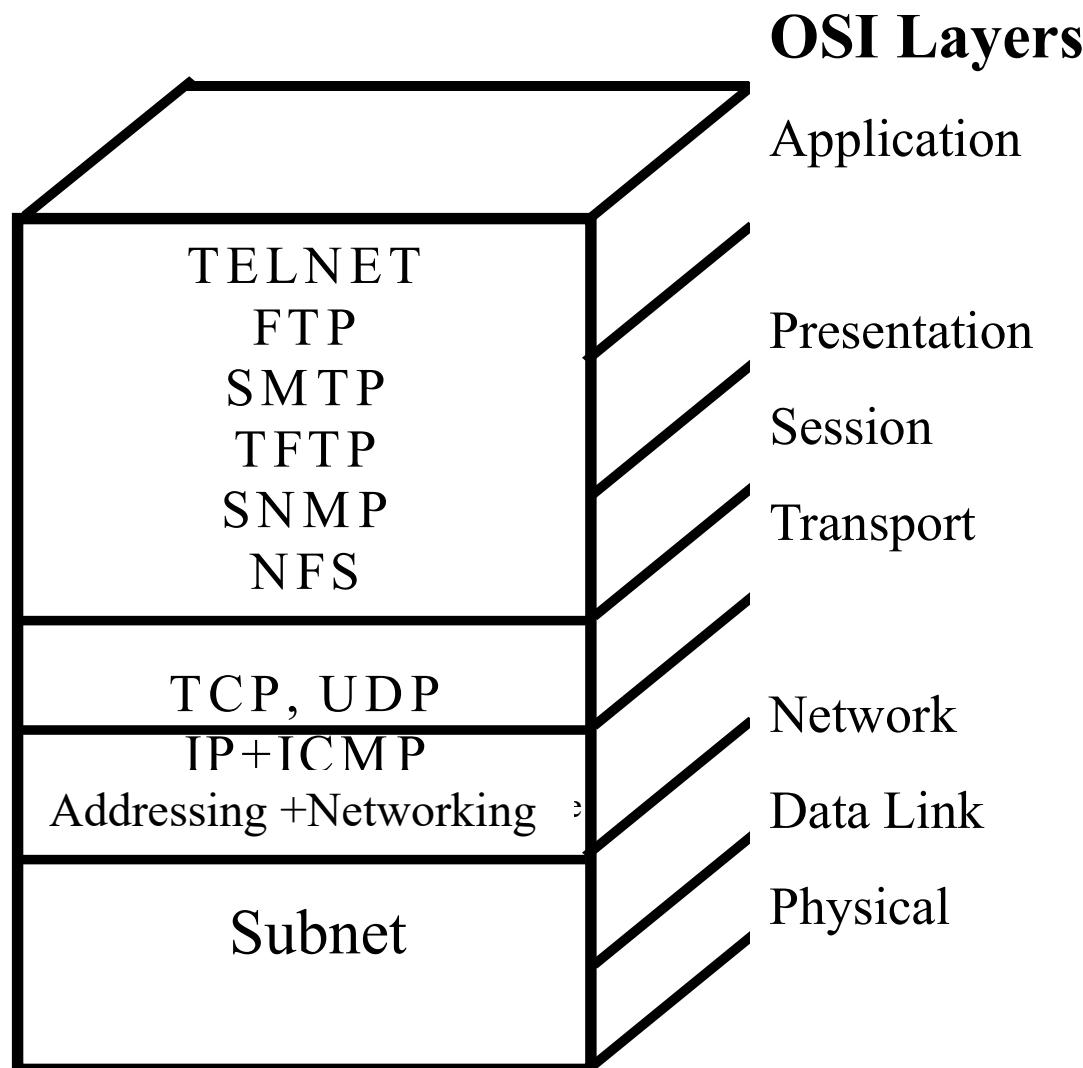
SNMP = Simple Network Management Protocol

SSH = Secure Shell

TCP = Transmission Control Protocol

UDP = User Datagram Protocol

Comparison of the protocol hierarchies



Concepts for the Data Communications and Computer Interconnection

Aim: overview of existing methods and techniques

Terms used:

- Data* – entities conveying meaning (of information)
- Signals* – data carrier; electric or electromagnetic representations of data
- Transmission* – data communications process, using the signal's propagation and processing

Main attributes of data, signals and transmission:

- digital
- analog

Towards *all digital*? Not yet!

Why? Important legacy (old telephone system); everything around (from environment) comes as analog

Today the digital technology offers:

- low cost, due to VLSI technology
- low attenuation, even in the past the analog technology led
- low noise influence
- better capacity utilization
- better data integrity
- security and privacy
- integration of digital and analog data.

Analog Data

Continuous values within some interval; e.g. sound, video.

Digital Data

Discrete values, e.g. text, integers.

Continuous signal

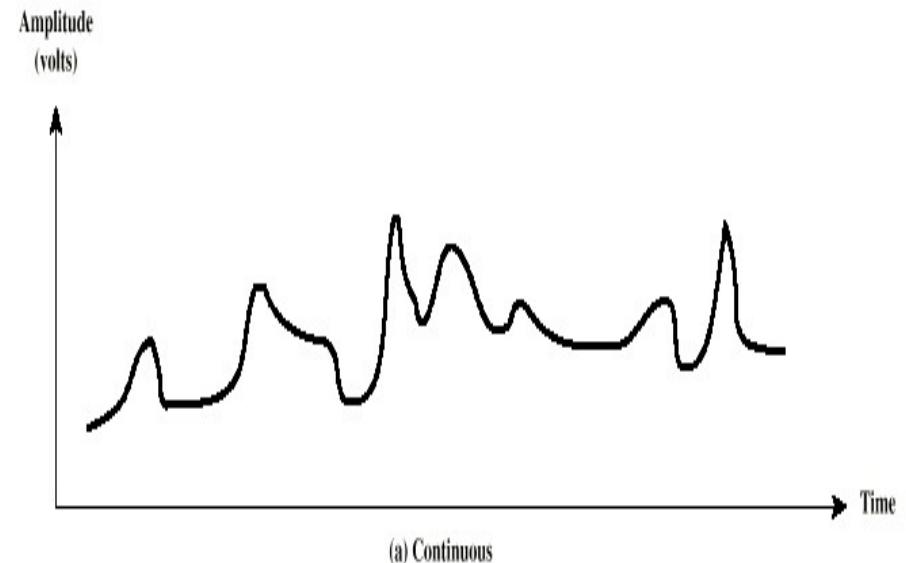
Various in a smooth way over time, may have any values.

Discrete signal

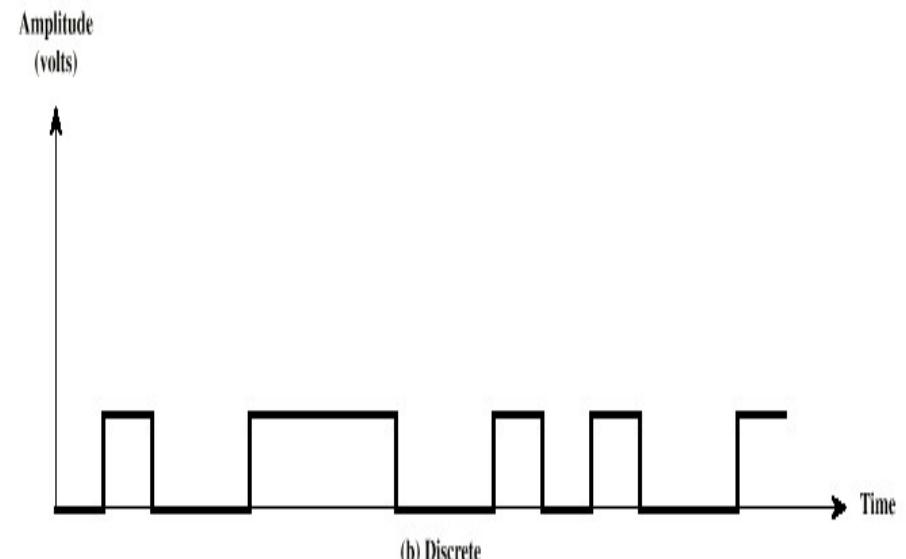
Maintains a constant level, then changes to another constant level. May have one of some (e.g. two) level values.

Mark denotes signal for ‘1’

Space denotes signal for ‘0’ data



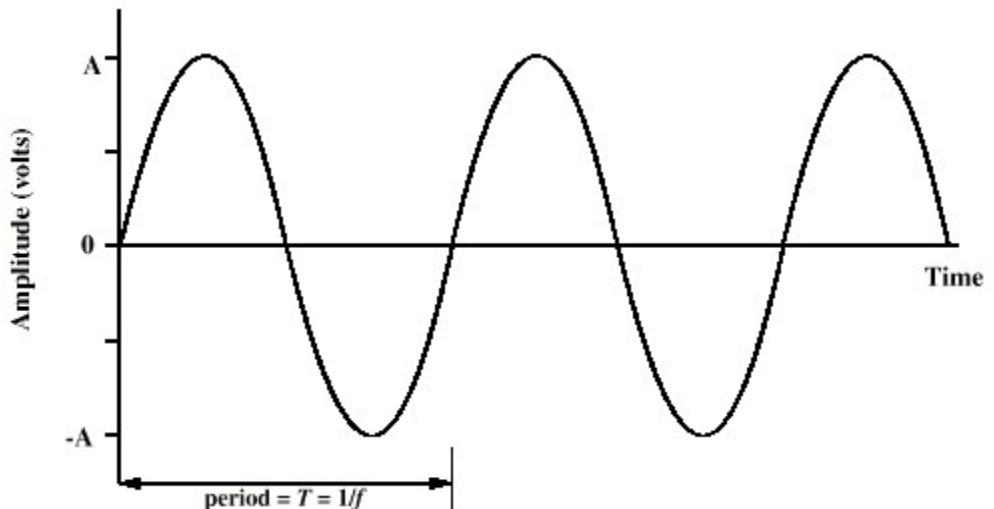
(a) Continuous



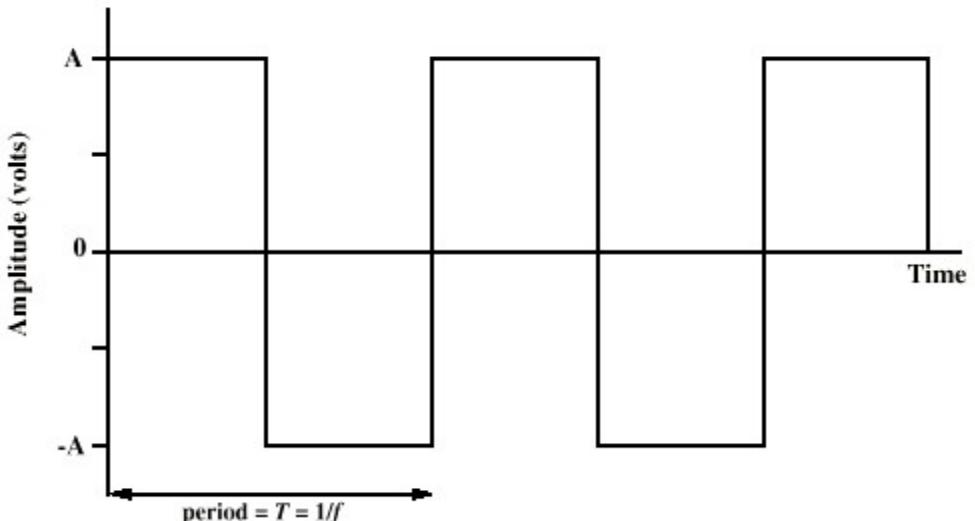
(b) Discrete

Periodic signal

Presents a pattern repeated over time.



(a) Sine wave



(b) Square wave

Parameters of the Sinus Wave (analytical, as function of time):

$$A \cdot \sin(2\pi ft + \phi)$$

Peak Amplitude (A): the maximum strength of signal, expressed in volts

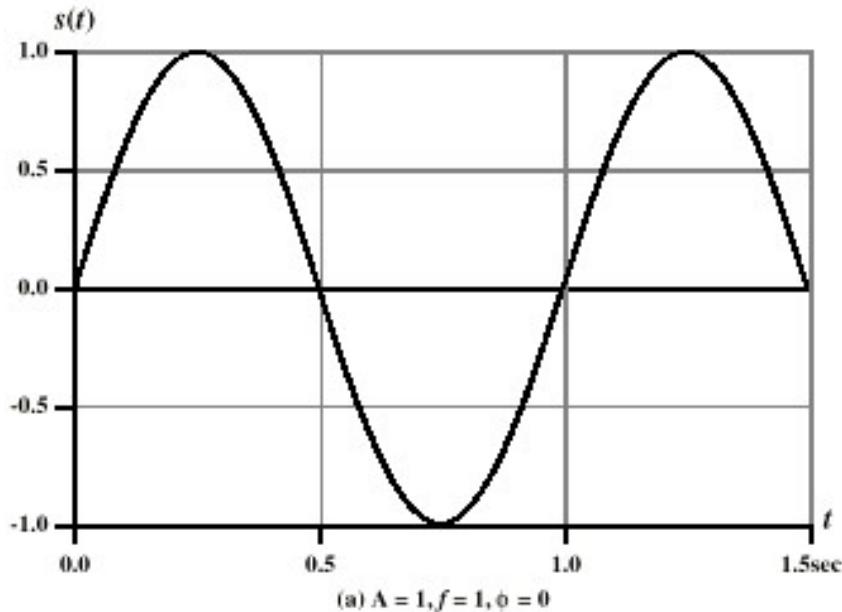
Frequency (f): the rate of change of signal, expressed in Hertz (Hz) or cycles per second

Period of the signal = time for one repetition (T)

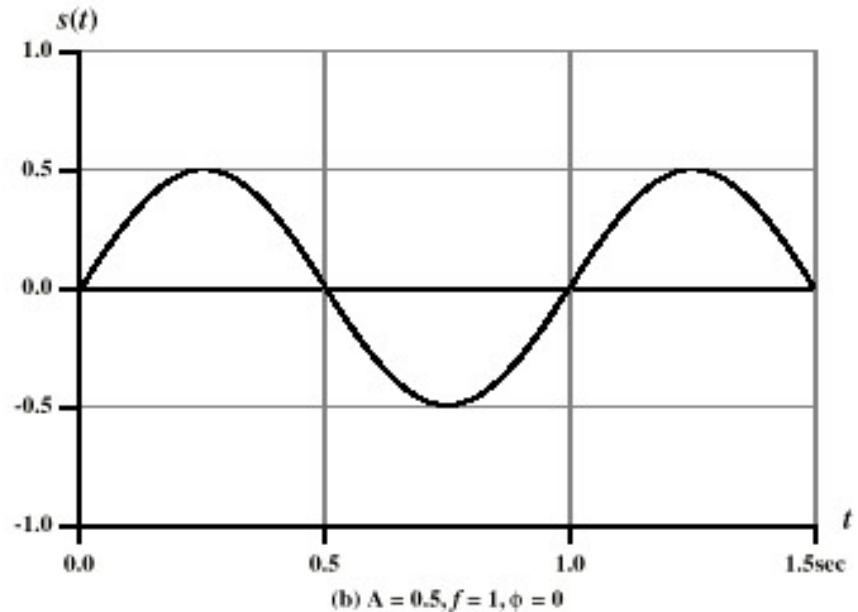
$$T = 1/f$$

Phase (ϕ): means the relative position in time

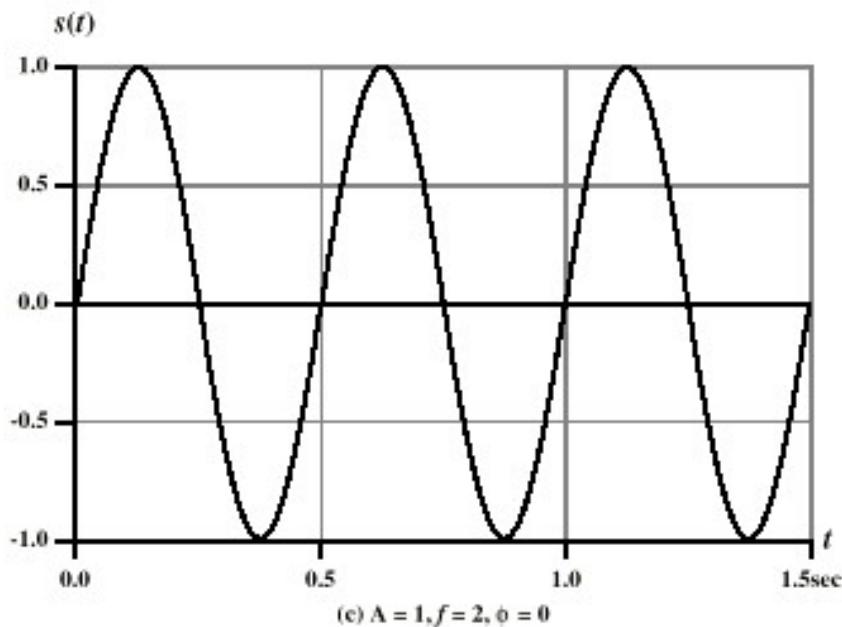
Wavelength (λ): Distance between two points of corresponding phase in two consecutive cycles. Relations: $\lambda = vT$; $\lambda f = v$, where v: signal speed expressed in m/s.



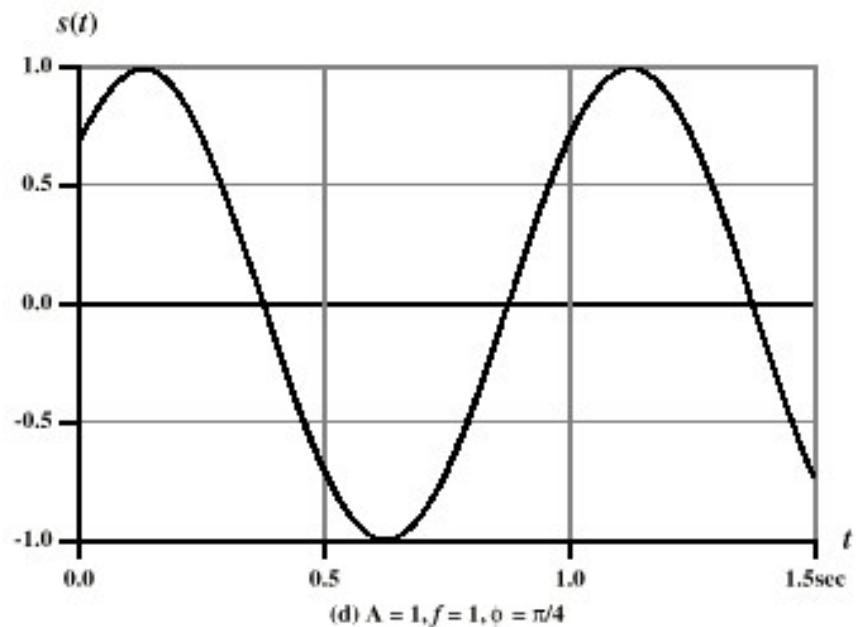
(a) $A = 1, f = 1, \phi = 0$



(b) $A = 0.5, f = 1, \phi = 0$



(c) $A = 1, f = 2, \phi = 0$



(d) $A = 1, f = 1, \phi = \pi/4$

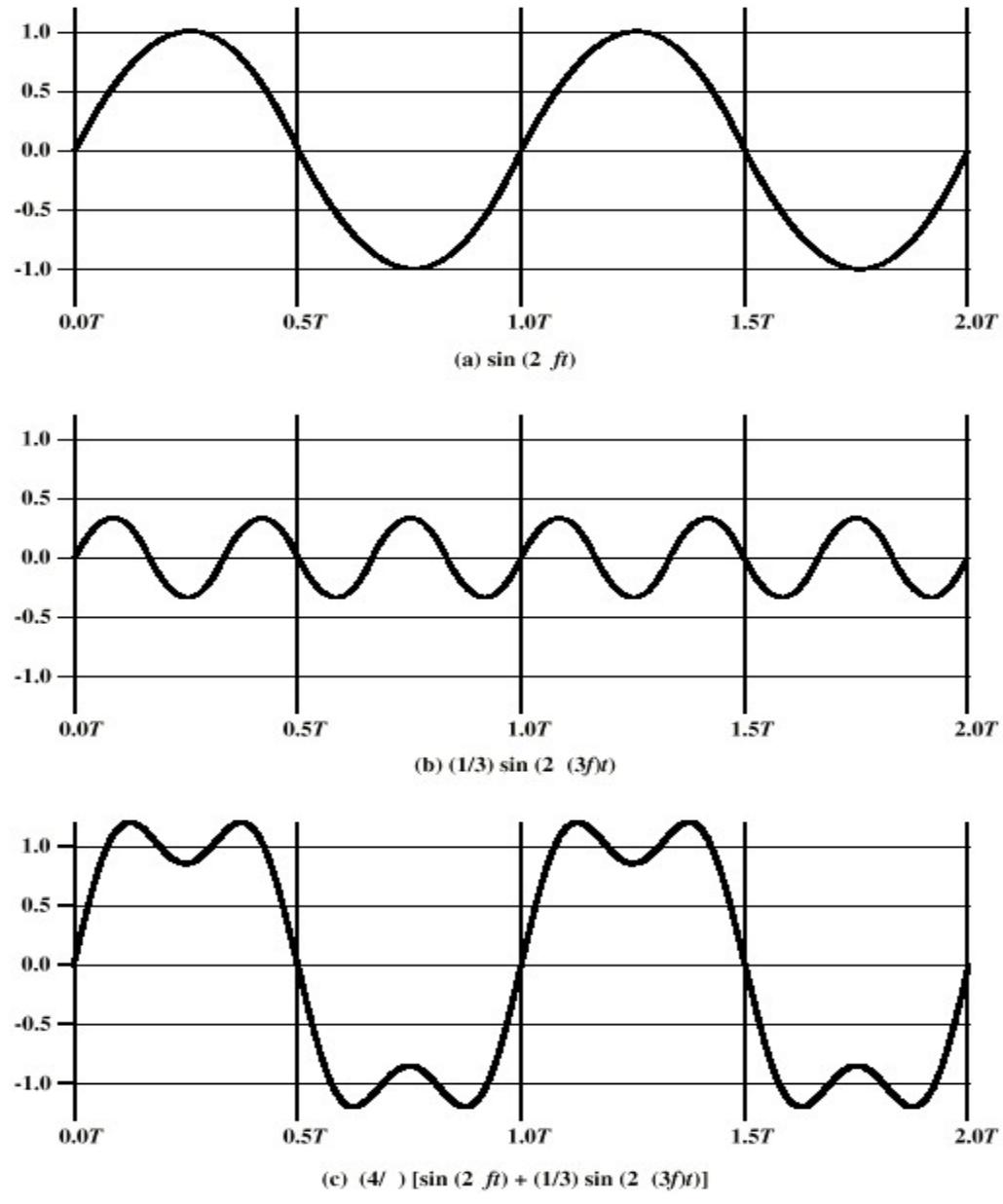
Frequency Domain

In practice, an electromagnetic signal is made up of many frequencies (has sinus components – Fourier analysis); one is the fundamental frequency, others are multiples. Spectrum – range of frequencies a signal contains.

Bandwidth – signal's width of the spectrum.

dc Component (continuous component) – component with zero frequency.

Any signal has a limited bandwidth => limited data rate!!!



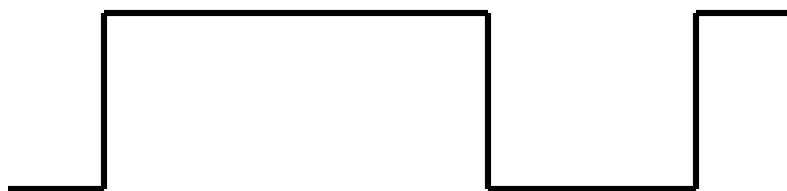
Data Coding terminology

Signal element: Pulse

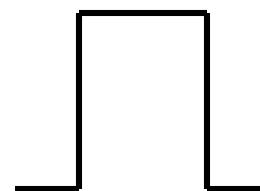
Modulation rate: 1/Duration of the smallest element or rate at which the signal level changes = Baud rate

Data rate: Number of bits per second (bps)

Data rate = $F_n(\text{Bandwidth, signal/noise ratio, encoding technique})$

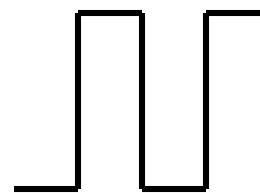


Pulse



NRZI: 1 bit = 1 signal element

Bit



Manchester: 1 bit = 2 signal elements,
Twice modulation rate required than NRZI

How to compare encoding techniques?

Various criteria:

- required bandwidth (lack of higher frequencies \Rightarrow low bandwidth)
- lack of the dc component: allows ac coupling, providing isolation
- how power is spread within the frequency spectrum (main power in the middle of the bandwidth)
- allows error detection (mechanism built in)
- avoid signals interference and allows high noise immunity
- synchronization mechanism built in (no external clock)
- cost and complexity
 - higher signal rate (data rate) \Rightarrow higher costs
 - need for a signal rate greater than data rate

Data Encoding

Digital Data, Digital Signals

Methods:

NRZ (Non Return to Zero-Level) – uses two voltage levels (H,L); may have any polarities

- difficult to find the bit margins
- no transitions between similar bits => dc component, damaging the passive connecting devices

NRZI (Non Return to Zero, Invert on Ones), also known as NRZ-M – codes data using a transition at the beginning of the bit period ('1': transition, '0': no transition).

Differential coding – compares polarities of successive signals, not their absolute values => better noise immunity

Multilevel Binary codes

Use more than two voltage levels

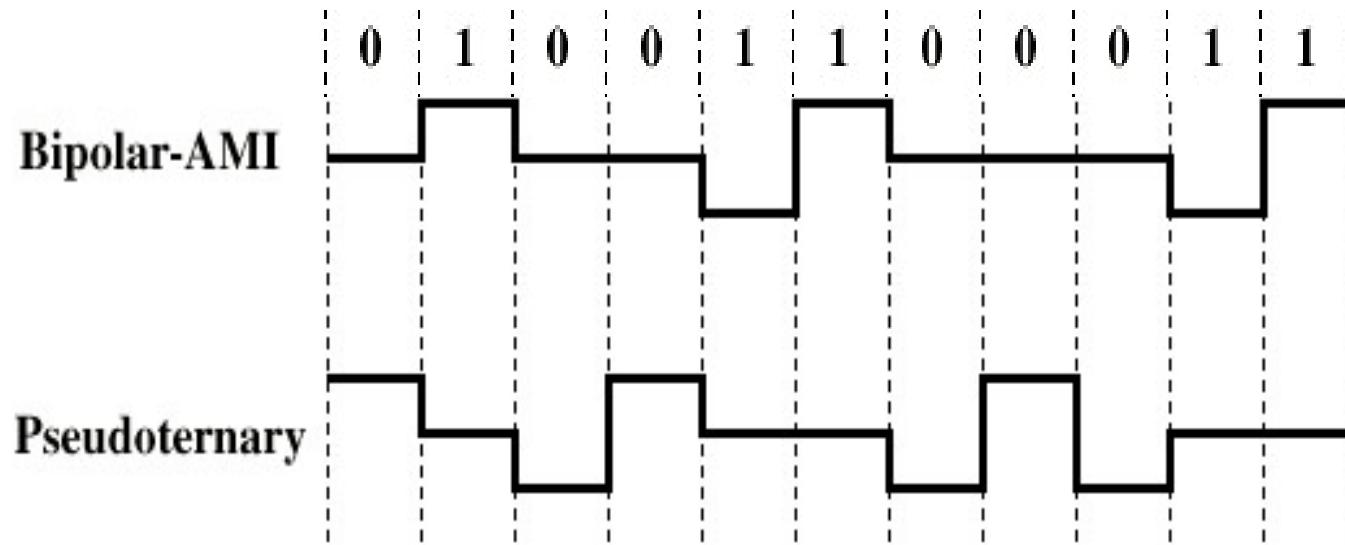
Bipolar-AMI (Alternate Mark Inversion) – ‘0’: no line signal, ‘1’: alternating positive and negative pulses => better synchronization (but avoid long ‘0’ string), lower bandwidth, improved error detection

Pseudo-ternary – reverse coding, ‘1’: no line signal, ‘0’: alternating positive and negative pulses => similar problems as for bipolar-AMI

Drawback:

Receiver must distinguish between three levels: (A, -A, 0)

Requires approx. 3dB more signal power for same probability of bit error

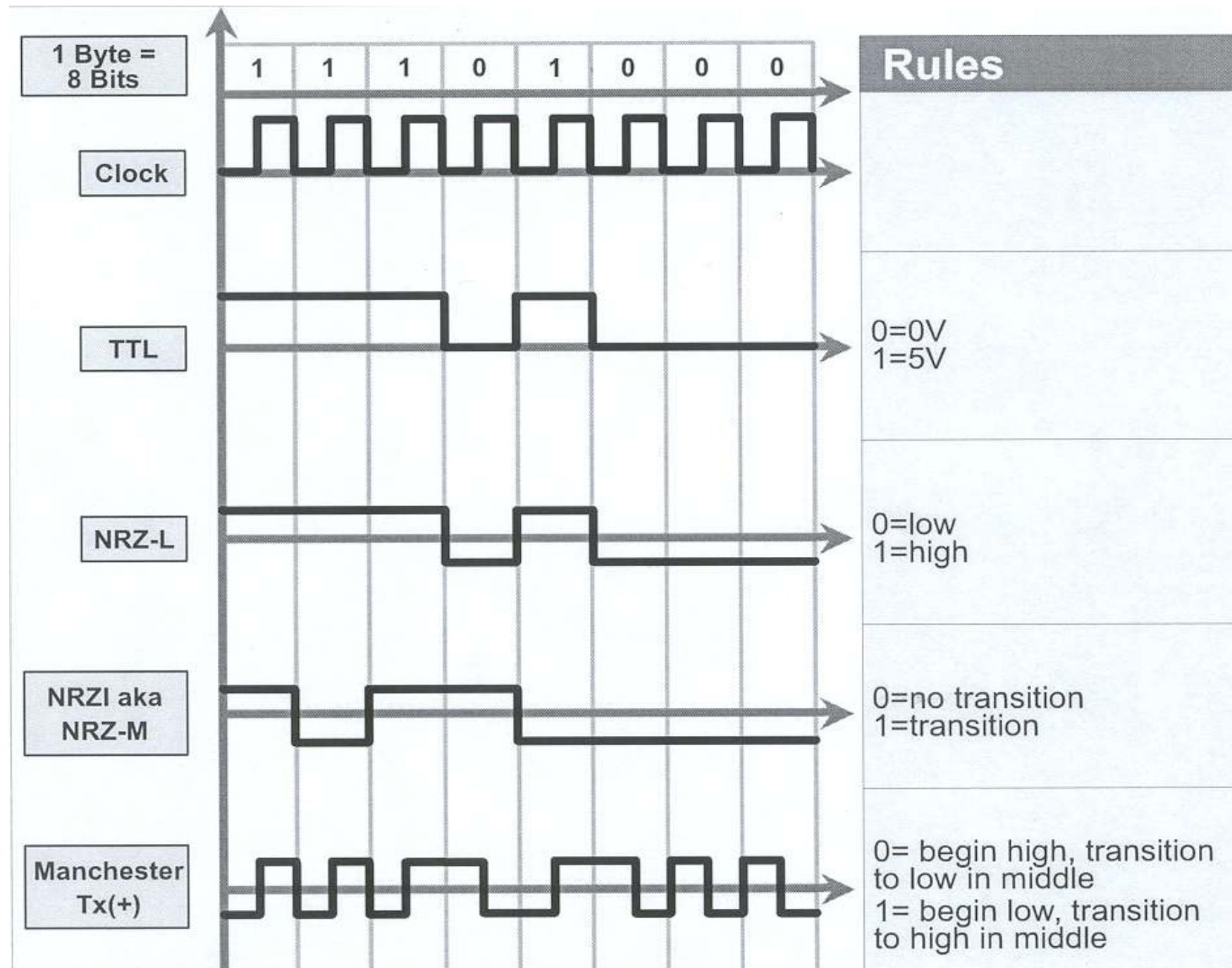


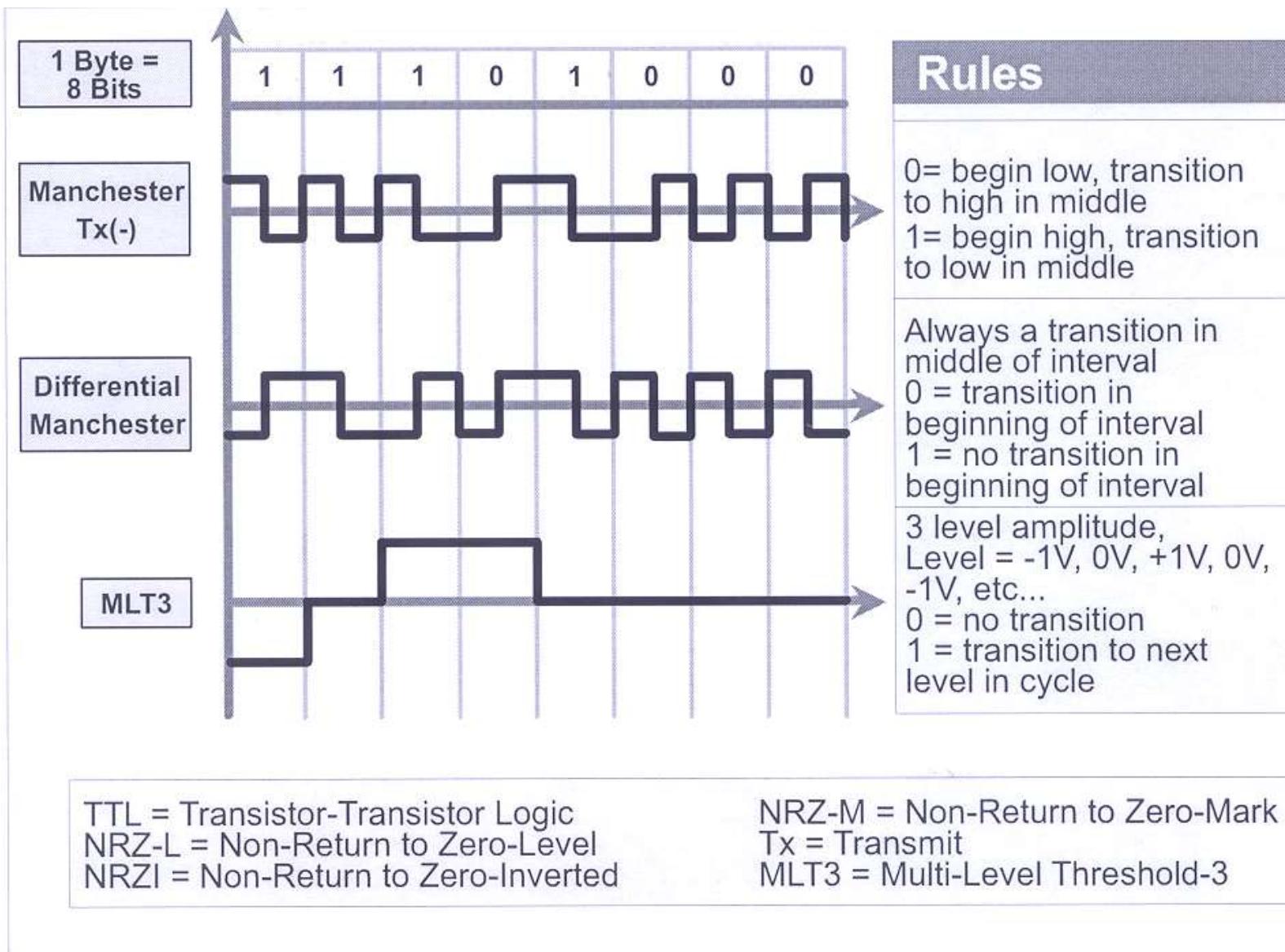
Data Encoding (continued)

Biphasic coding: one or two transitions on a bit period => higher bandwidth, but provides synchronization, better error detection, less noise influence, no dc component

Manchester – always a transition at the middle of the bit period (used as clock signal): data coding by the transition sense ('0': Low to High, '1': High to Low for Tx-, and reverse for Tx+)

Differential Manchester – middle transition as clock signal, data coding by a transition at the beginning of bit period ('0': transition, '1': no transition). Most used for twisted pair based networks.





For WANs, for sake of bandwidth costs: **scrambling techniques** (long constant data streams replaced by filling sequences):

Bipolar With 8 Zeros Substitution B8ZS

Based on bipolar-AMI, but introducing AMI code violation

IF:

Octet of all zeros and last voltage pulse preceding was positive, encode as 000+-0-+

Octet of all zeros and last voltage pulse preceding was negative, encode as 000-+0+-

Causes two violations of AMI code; Unlikely to occur as a result of noise

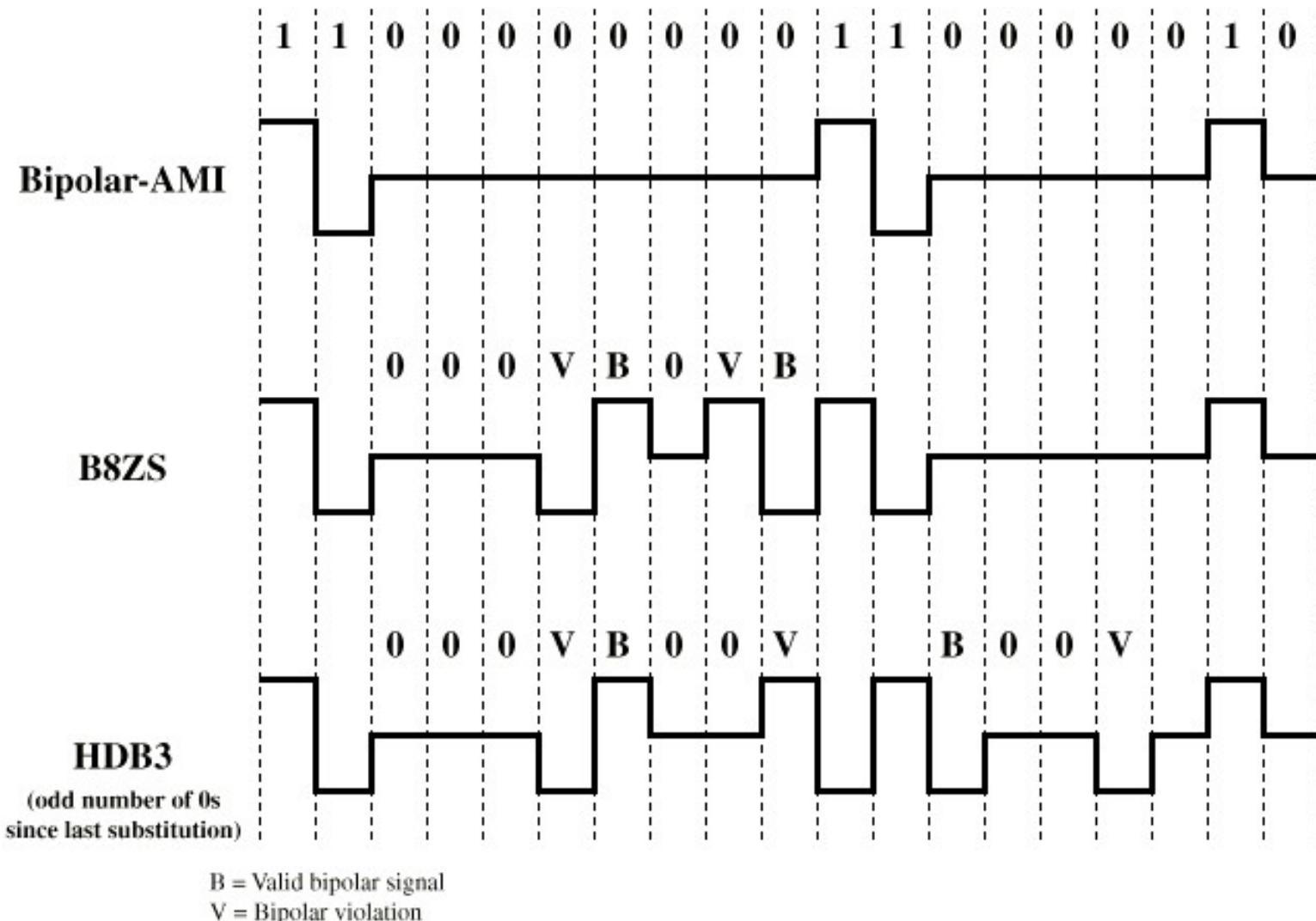
Receiver detects and interprets as octet of all zeros.

High Density Bipolar 3 Zeros HDB3

Based on bipolar-AMI, but introducing code violation (not valid AMI bipolar signal)

String of four zeros replaced with one or two pulses (the AMI code violation sequence).

Also alternation of polarities for the violation codes.



Digital Data, Analog Signals

Use of a constant frequency signal: **data carrier**, modulated conform with the data

Amplitude Shift Keying (ASK) – presence or not of the carrier, at constant amplitude; non efficient for data transmissions; variant for fiber optic transmissions: presence or absence of the light

Frequency Shift Keying (FSK) – two (symmetric) frequencies, near the carrier basic frequency

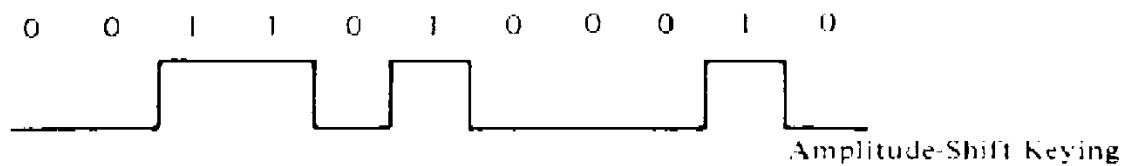
Phase Shift Keying (PSK) – short burst signals

coherent PSK: constant signals having a phase difference of 180°

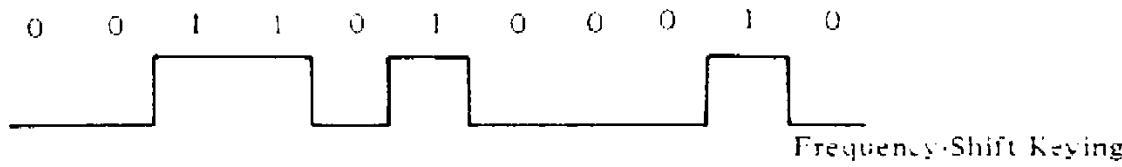
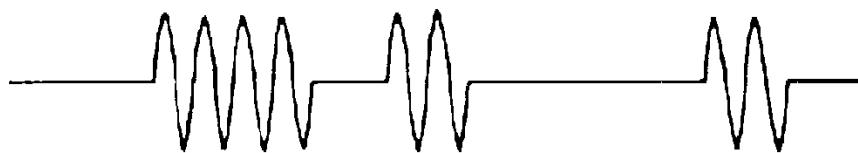
differential PSK: ‘0’ burst signal with the same phase as the previous (0° shift), ‘1’ burst signal with opposite phase as previous (shift with $0^\circ + \pi$)

best error resistant, determining the phase shift magnitude, not its absolute value.

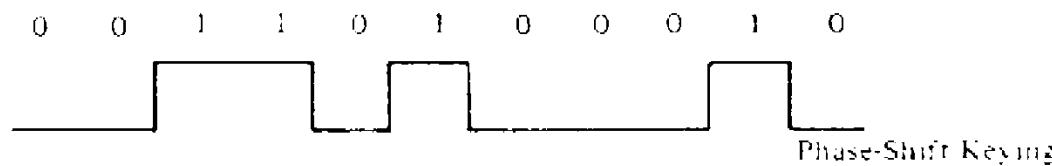
Quadrature-PSK coding – codes 2 bits by a burst signal, having more than two phase-shifts per signal: phase shifts of multiples of 90° . Possible extensions...



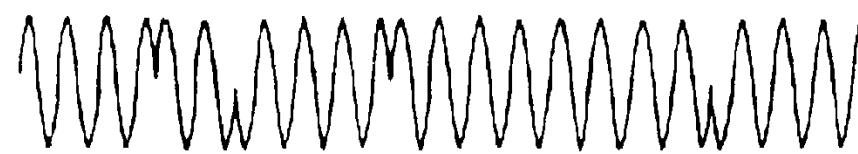
Amplitude-Shift Keying



Frequency-Shift Keying



Phase-Shift Keying



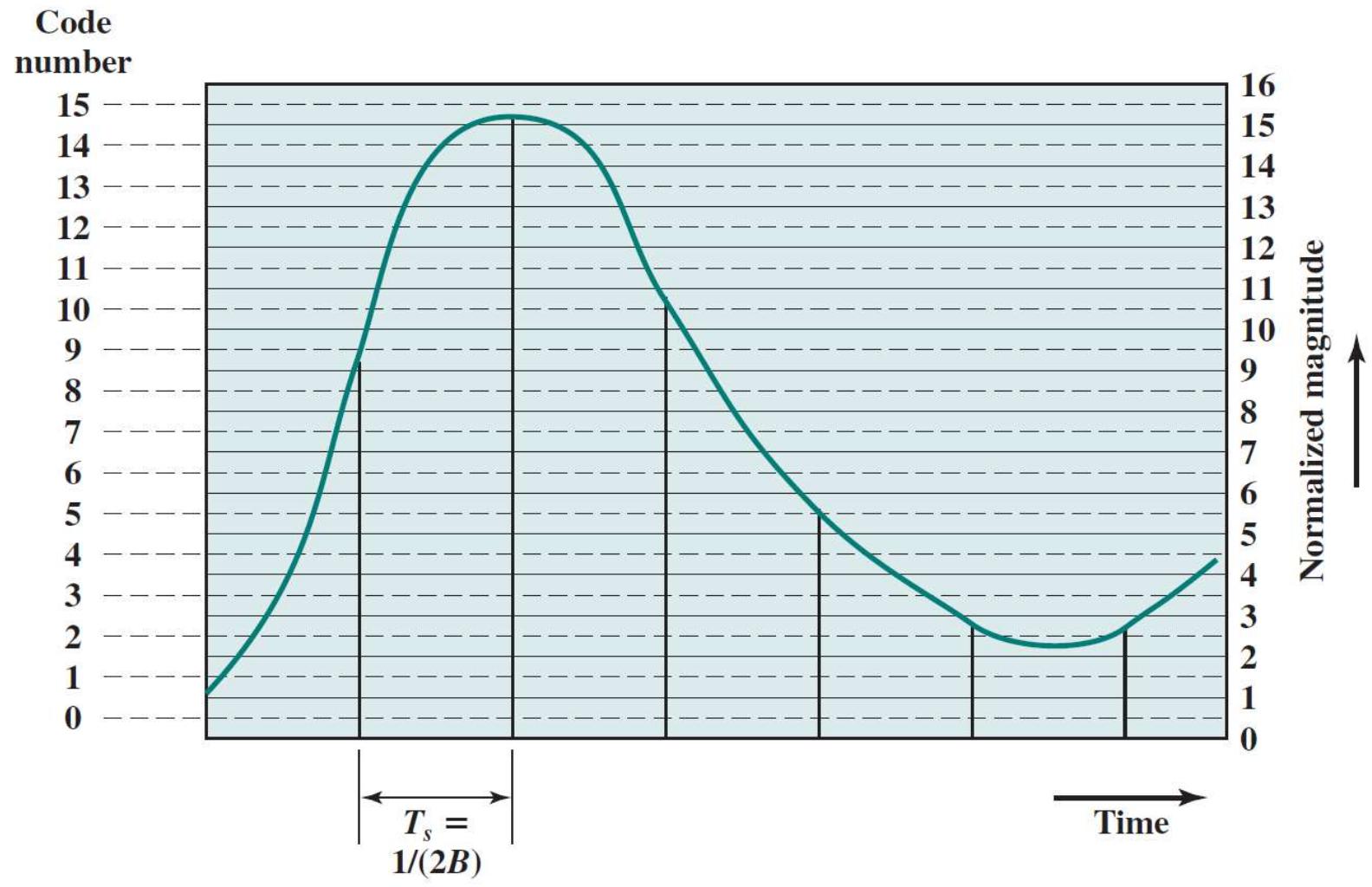
Analog Data, Digital Signals

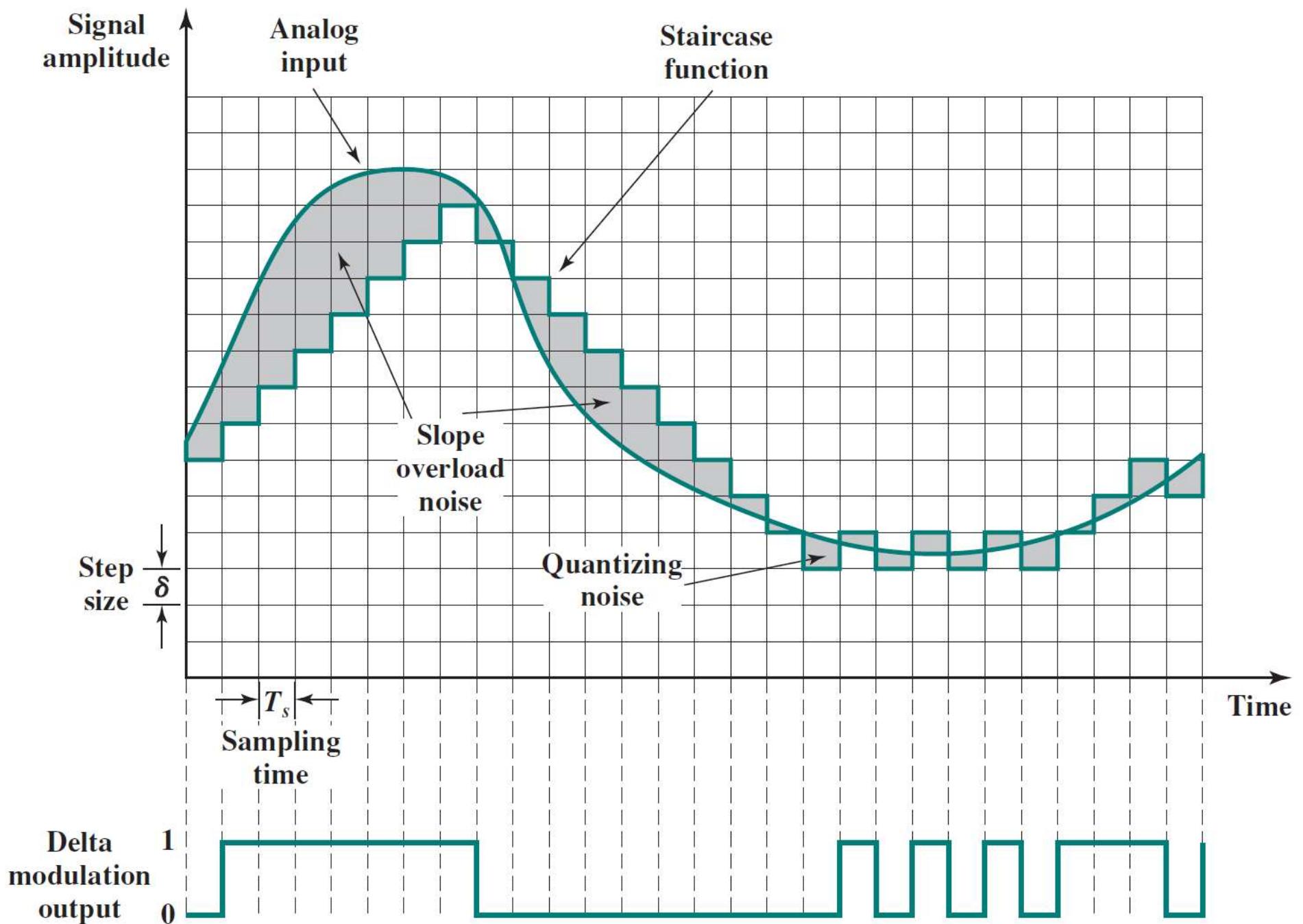
Theoretical background: Nyquist sampling theorem: sample at twice the highest signal frequency (for a voice carrying signal with bandwidth of 4kHz, sample at 8kHz, or every 125 μ sec, having 8000samples/sec)

Pulse Code Modulation (PCM), with the following 3 steps:

- signal *sampling*, using the proper sampling frequency (higher than twice the highest signal frequency); samples represented as PAM (Pulse Amplitude Modulation) pulses
- quantification* of the samples, using the available number of digits, obtaining the PCM pulses and their digital values; more digits, more accuracy, greater cost
- digital values representation as pulse trains - *coding*

Delta Modulation – approximates the analogue signal by a staircase function moving up/down by one quantization level at each sampling interval; output function has a binary behavior (moves up or down at each sample interval); method less used in computer networks





Analog Data, Analog Signals

Used when only analog facilities available.

Why analog data if the voice signals are transmitted in the baseband ?

- higher frequency may be needed for unguided transmission (impossible to transmit baseband signals), or optical
- modulation permits FDM.

Amplitude Modulation

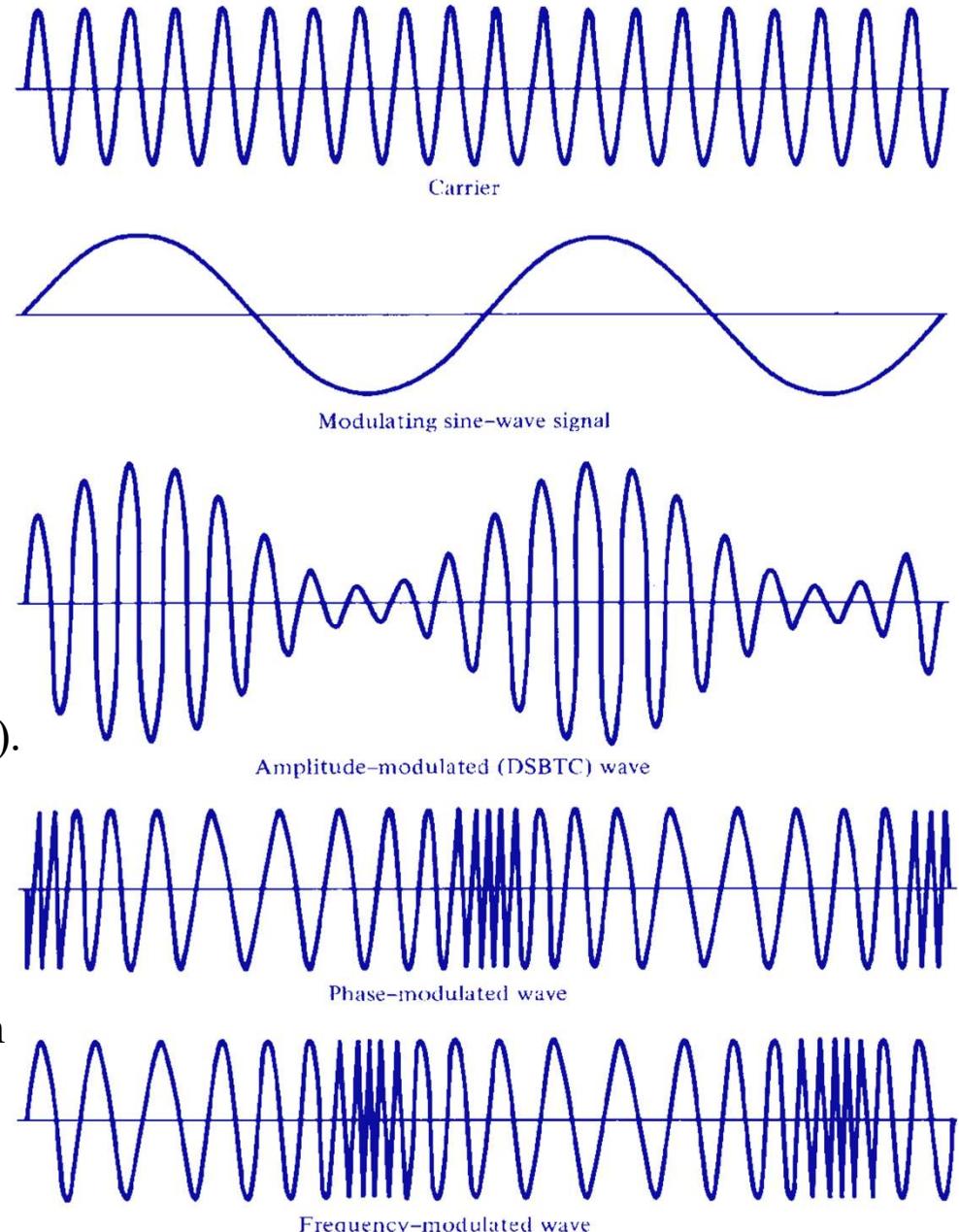
Amplitude of the carrier is varied accord. with some characteristic of the modulating signal (ex: double-sideband transm. carrier).

Phase Modulation

Data carrier's phase is varied linearly according to the data.

Frequency Modulation

Data carrier wave's frequency departs from the center frequency (carrier's) by an amount depending on the value of the modulating signal.



Spread Spectrum

Analog or digital data sent using analog signal (radio transmissions)

Spread data over wide bandwidth

Makes jamming and interception harder

Two schemes:

Frequency hopping

Signal broadcast over seemingly random series of frequencies

Hop from one frequency to other at split-second intervals

Direct Sequence

Each bit is represented by multiple bits in transmitted signal (chipping code)

Chipping code is obtaining combining original data with pseudorandom bit stream

Chipping code spreads the signal across a wider frequency band

Transmission impairments

For any communication system, the received signal will differ from the transmitted signal – not an ideal transmission!

Due to various transmission impairments, introducing signal degradation (analog transmissions), bit errors (digital); most encountered transmission impairments are:

Attenuation and attenuation distortion

Delay distortion

Noise

Attenuation

The reduction of signal's strength (power) with distance.

For guided media attenuation is logarithmic and expressed in dB/m.

For unguided media transmissions, it depends on distance and makeup of atmosphere.

$$\text{Attenuation} = 10 \cdot \log_{10} P_{\text{in}}/P_{\text{out}} \text{ [dBel]}$$

$$\text{Attenuation} = 20 \cdot \log_{10} V_{\text{in}}/V_{\text{out}} \text{ [dBel]}$$

Received signal strength:

must be enough to be detected

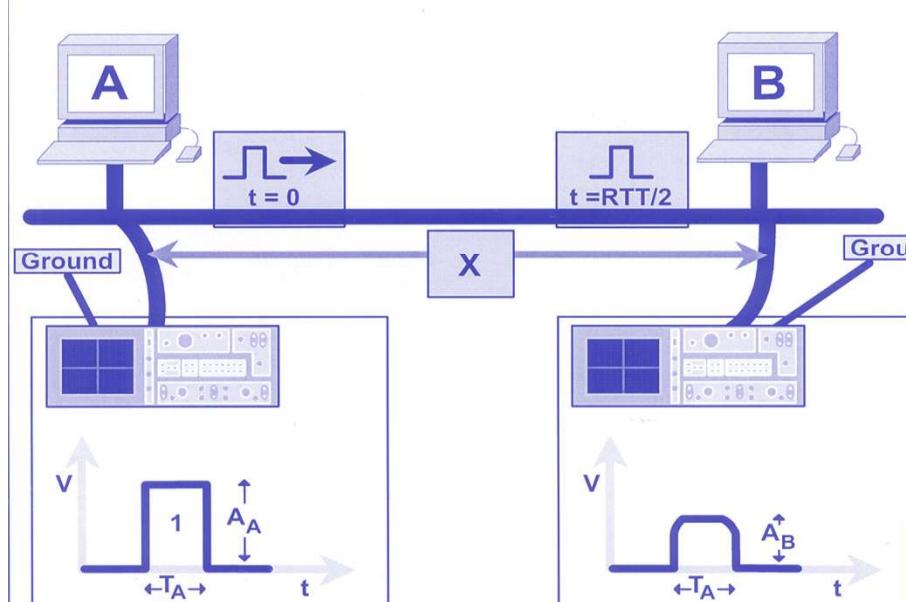
must be sufficiently higher than noise, to be received without error.

Use of amplifiers and repeaters for maintaining the signal strength.

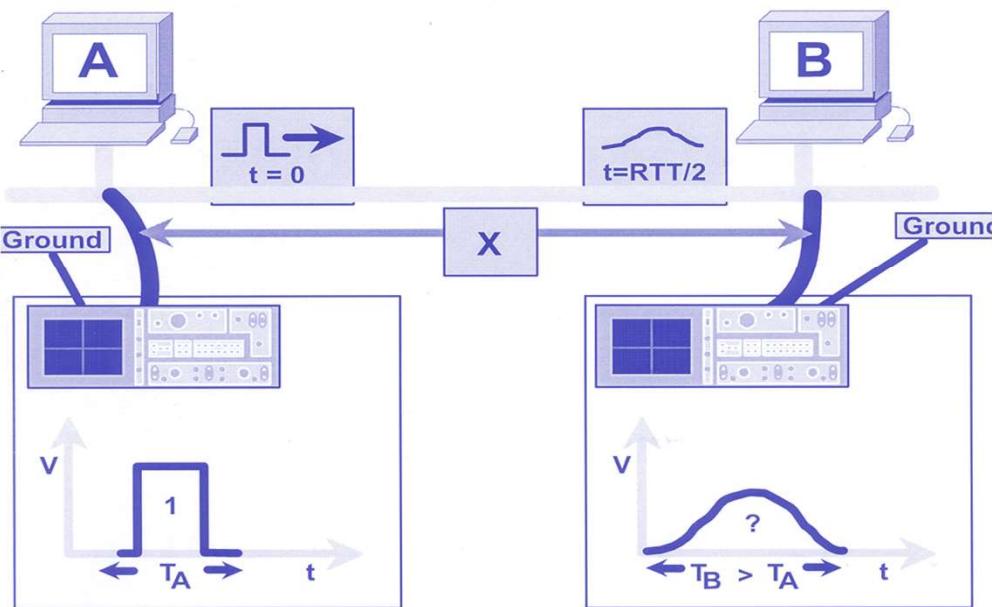
Attenuation depends increasingly of signal frequency => problems for HF transmissions, but mainly for analog transmissions, resulting signal distortions => techniques for attenuation equalization across the frequency spectrum.

Digital signal concentrates power near the fundamental frequency.

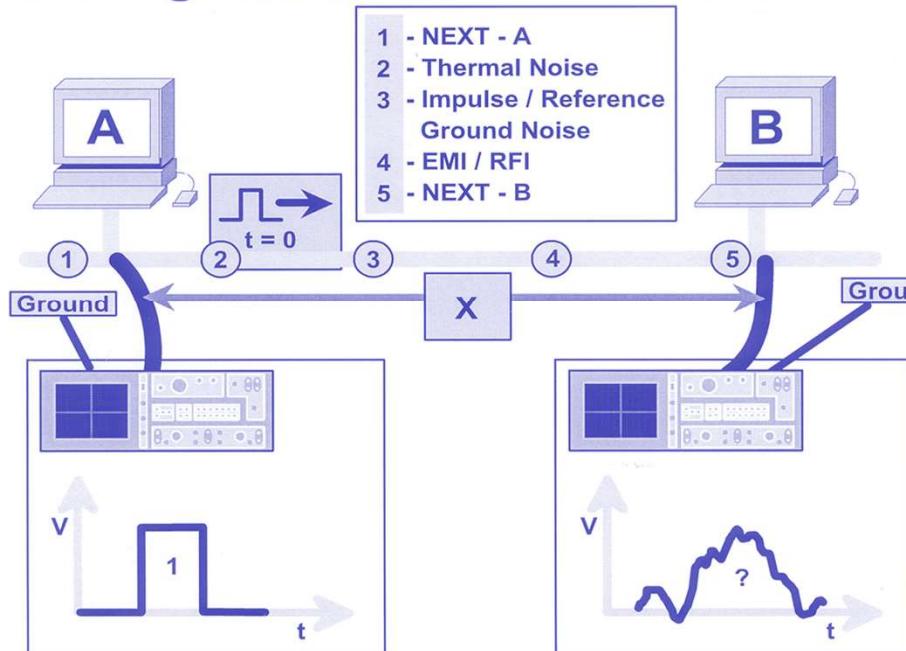
Attenuation



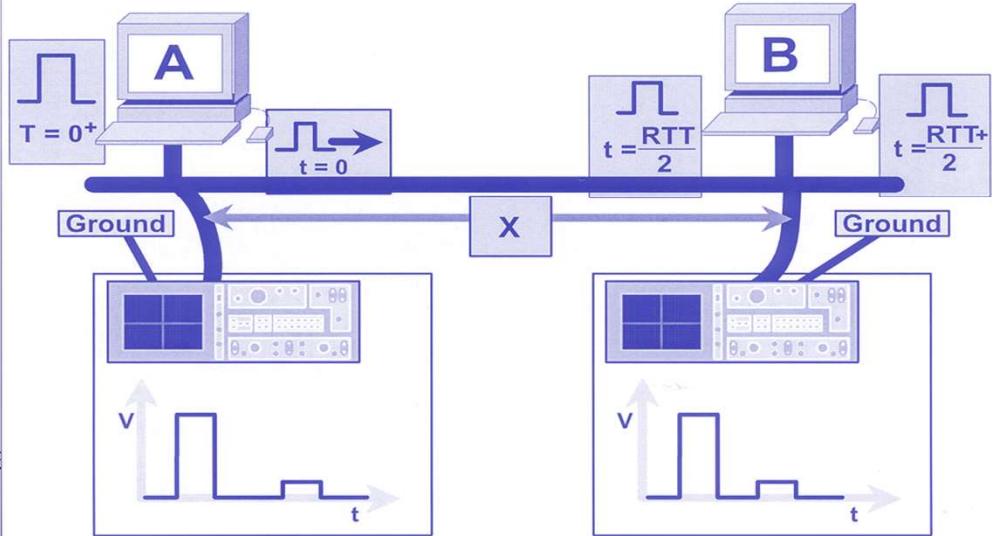
Delay Distortion (Dispersion)



Recognize and Define Noise



Reflection



Delay Distortion

Only in guided media, where the signal's propagation speed depends on frequency
=> signal distortions, centred frequency components have greater velocity than those from band edges. Use of equalizers.

Noise

Plus to above mentioned distortions: additional signals inserted between transmitter and receiver (generally called **noise**)!

Thermal noise (depends on temperature, not on frequency, intrinsic to structure):

Due to thermal agitation of electrons

Uniformly distributed across the spectrum (called white noise)

Can not be eliminated => an upper bound for communications performances.

Intermodulation noise

Noise signals that are the sum and difference of original frequencies sharing a medium, or multiples of them – due to the nonlinearities of the transmission system.

Crosstalk

A signal from one line is picked up by another (is a coupling between signal paths). Experienced by anyone with the telephone.

Impulse noise

Non predictable, caused by external electromagnetic disturbances, faults and flaws in the system; critical for digital transmissions

Irregular pulses or spikes with short duration, random amplitude (thus may be high), and spectral content.

Communications Channels

Definition: the part that connects a data source to a data sink; based on the transmission media.

Classification criteria:

-type of the link (connection):

point-to-point,

point-multipoint (master-slave configuration),

broadcast (common shared medium)

-information transfer sense:

simplex: one way

half-duplex: at a moment, data only in a sense, control may be in both

full-duplex: data and control on both ways

- maximum channel transmission speed (channel capacity), in junction with the maximum allowed bandwidth

-type of transmission

-baseband: entire bandwidth of communications media dedicated to one channel; often used for digital transmissions; cheaper, adequate for most LANs

-broadband: whole bandwidth divided into multiple independent channels; often used for analog transmissions; multiple transmissions of data, voice, video

Basic theorems used in obtaining the maximum channel speed

Nyquist theorem:

For an ideal channel (without loss, no noise), maximum channel speed (maximum data rate):

$$v=2 \cdot H \cdot \log_2 N$$

H: frequency bandwidth

N: number of levels used to encode data

(if N = 2, for the bi-level encoding, comes the well known: $v=2 \cdot H$)

Shannon's theorem:

For a ‘more realistic’ channel, affected by noise:

$$v=H \cdot \log_2(1+S/N)$$

S: power of the transmitted signal

N: power of the noise signal

S/N: signal per noise ratio, expressed usually as $10 \cdot \log_{10} S/N$ and measured in dB
(also usually understood as attenuation).

Example: Phone wire bandwidth = 3100Hz (spread between 300Hz and 3400Hz).
For an attenuation of 30dB (usual one for that type of wire), what will be the
channel capacity?

$$10 \cdot \log_{10} S/N = 30$$

$$\log_{10} S/N = 3$$

$$S/N = 10^3 = 1000$$

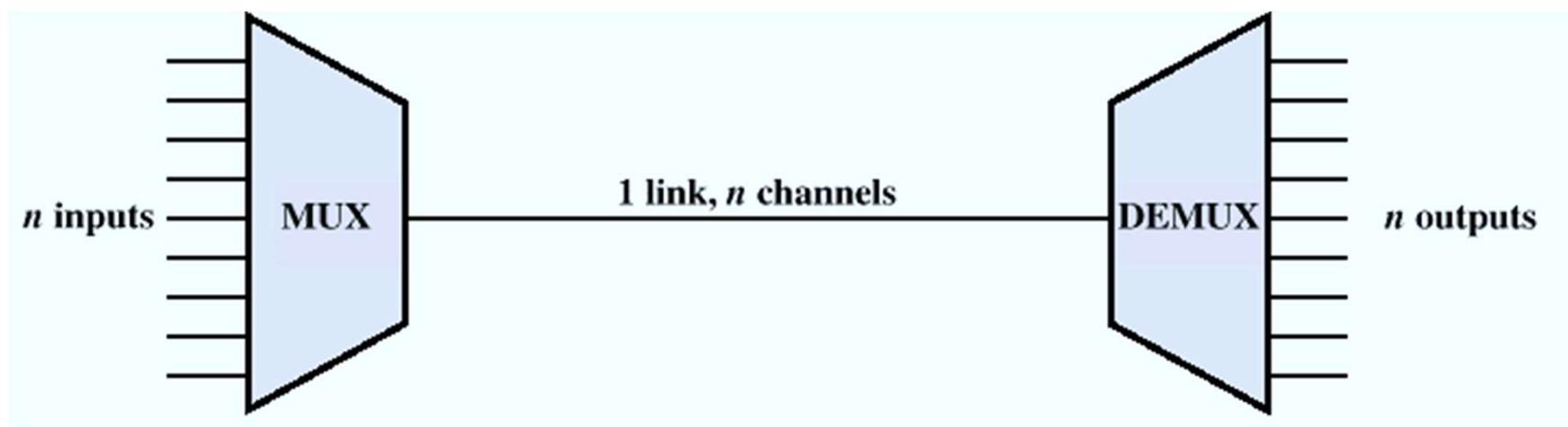
$$\begin{aligned}\text{Channel capacity no more than: } v &= 3100 \cdot \log_2(1+1000) \\ &= 30,894 \text{ bps} < 30 \text{ kbps.}\end{aligned}$$

Multiplexing techniques

Used when the total medium **transmission capacity** exceeds the channel's one => channels multiplexing for a better use of medium.
Useful for long-haul comms; trunks are fiber, coaxial, microwave high capacity links.

Higher data rate transmission => better cost-effective transmissions for a given application over a given distance.

Usually data-communicating devices require modest data rate 64kbps



Techniques:

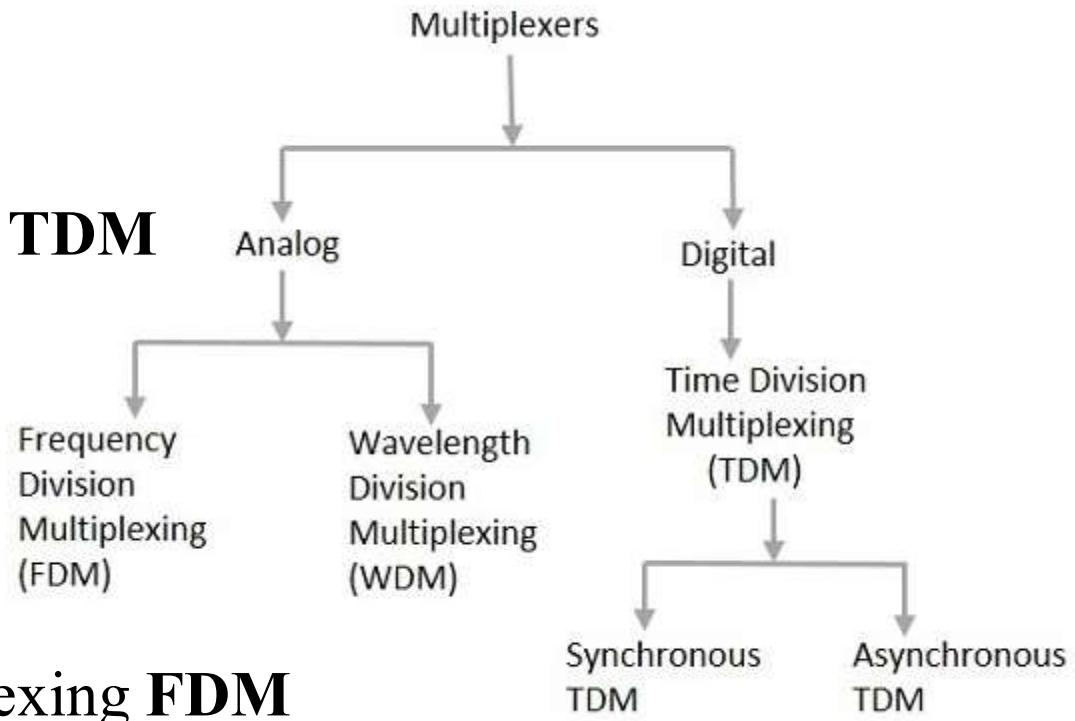
Time Division Multiplexing **TDM**

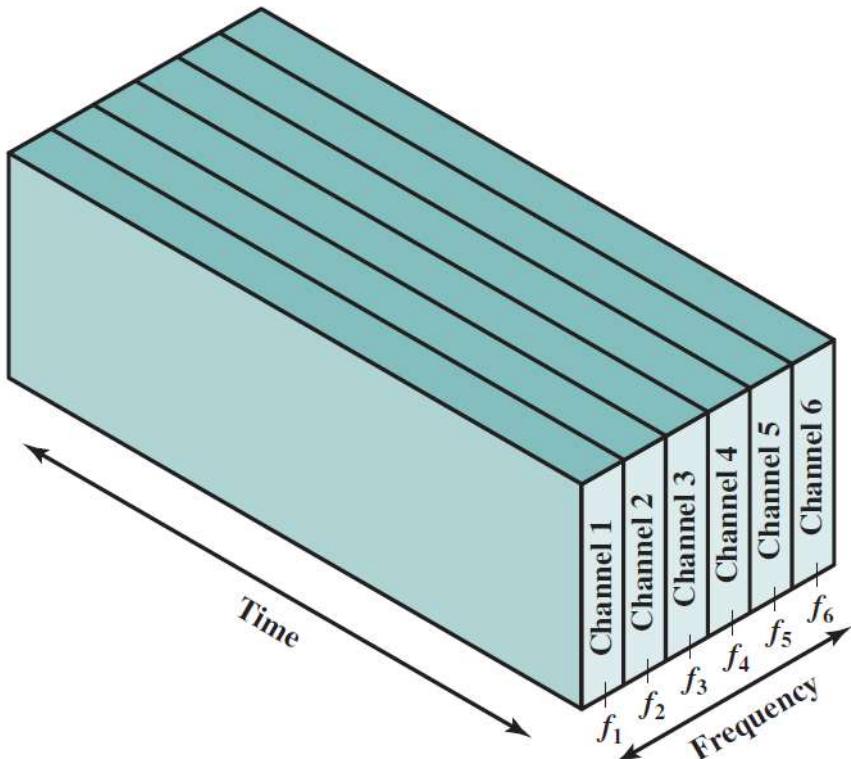
 synchronous

 statistical

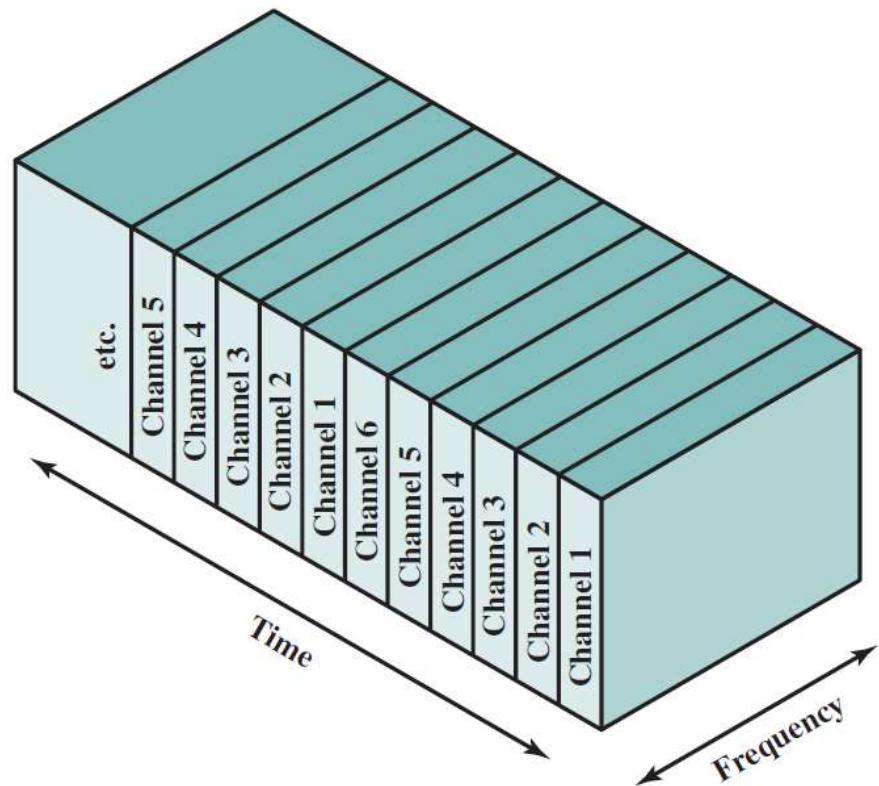
Frequency Division Multiplexing **FDM**

Wavelength Division Multiplexing **WDM** –
for optical transmissions





(a) Frequency-division multiplexing



(b) Time-division multiplexing

FDM

Total allocated bandwidth \gg that required by a single signal.

A number of signals carried simultaneously, each signal modulated onto a different carrier frequency, which are separated for avoiding signals bandwidths to overlap (use of guard bands).

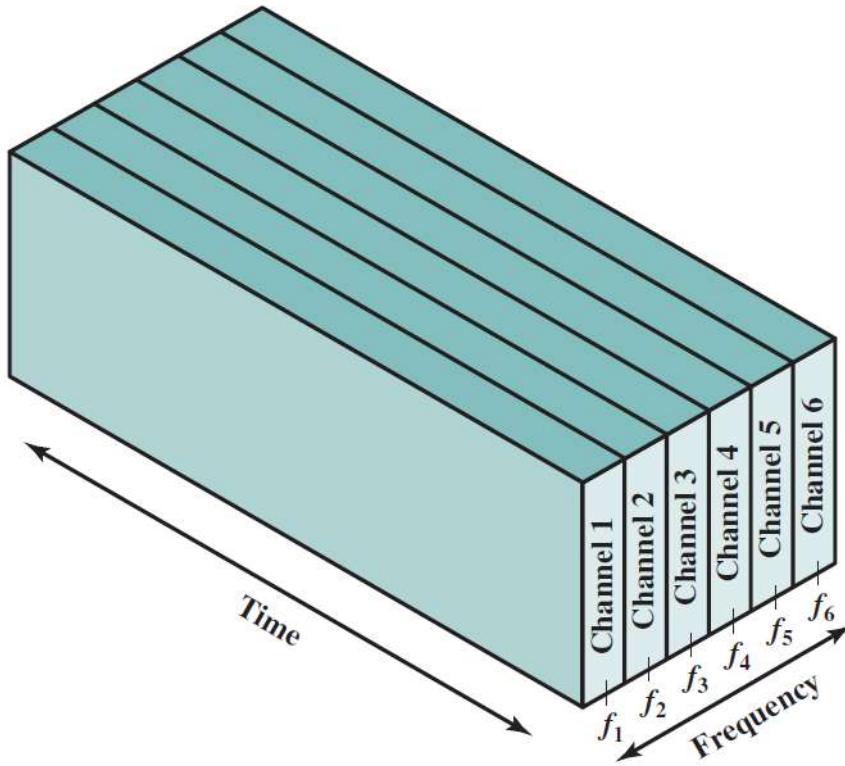
Input signals are analog or digital, converted to analog, multiplexed onto an analog composite signal.

Relevant example: broadcast television, using RF propagation or CATV (Cable Antenna TV)

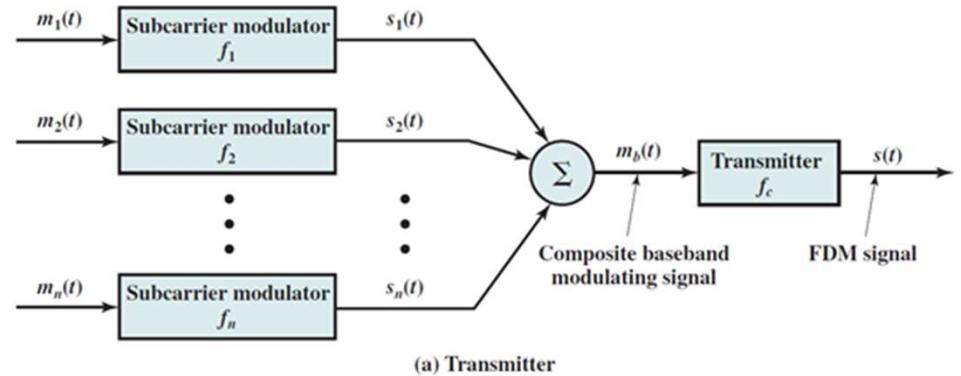
TV signal (B/W video + audio + colour) fits into 6MHz bandwidth

For a coaxial cable bandwidth of 500MHz \Rightarrow tens of TV signals

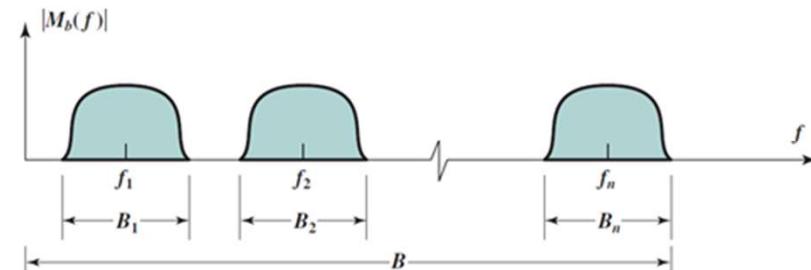
Frequency allocation: from 54-60MHz (first channel) to 800-806MHz (68th channel) – in US



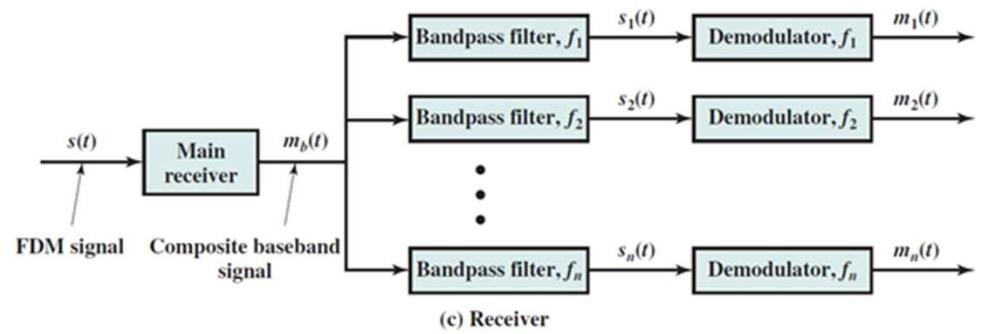
(a) Frequency-division multiplexing



(a) Transmitter



(b) Spectrum of composite baseband modulating signal



(c) Receiver

Analog Carrier System

Provides voice-band signals transmission over high capacity links.

Standard (ITU-T hierarchy) based on AT&T – but not identical!

Some levels from the hierarchy:

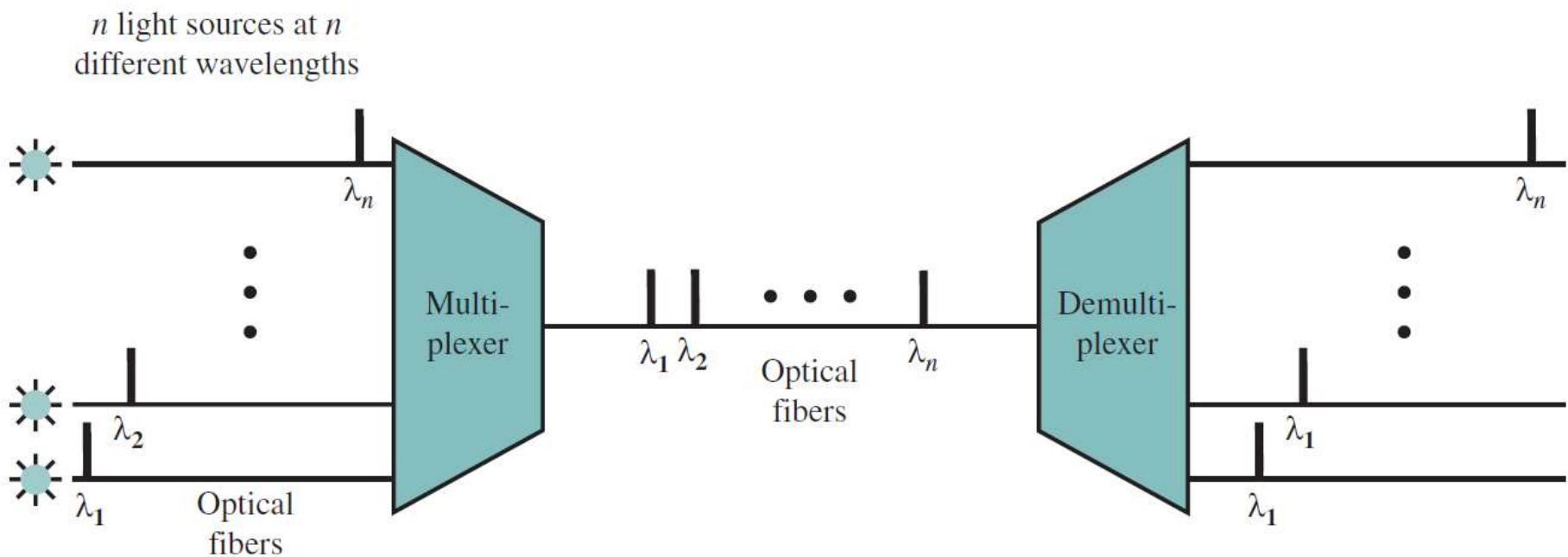
Table 8.1 North American and International FDM Carrier Standards

Number of Voice Channels	Bandwidth	Spectrum	AT&T	ITU-T
12	48 kHz	60–108 kHz	Group	Group
60	240 kHz	312–552 kHz	Supergroup	Supergroup
300	1.232 MHz	812–2044 kHz		Mastergroup
600	2.52 MHz	564–3084 kHz	Mastergroup	
900	3.872 MHz	8.516–12.388 MHz		Supermaster group
$N \times 600$			Mastergroup multiplex	
3,600	16.984 MHz	0.564–17.548 MHz	Jumbogroup	
10,800	57.442 MHz	3.124–60.566 MHz	Jumbogroup multiplex	

WDM(wavelength division multiplexing)

Multiple beams of light at different frequencies - transmitted on the same optical fiber

Dense wavelength division multiplexing (DWDM): the use of more channels, more closely spaced, than ordinary WDM (usually channel spacing of 200 GHz or less)



Synchronous TDM

Total achievable data rate of the medium \gg data rate of the signal (at least equal with the sum of signals data rate).

Method: multiple signals carried on a single path by interleaving in time portions of each (slots).

Interleaving may be at bit level or at blocks.

Time slots pre-assigned to sources and are fixed (some may be empty- slots are wasted) i.e. is synchronous.

Time slots do not have to be equally distributed among sources, depending on their own data rate.

TDM Link Control

No headers and trailers; Data link control protocols not needed

Flow control

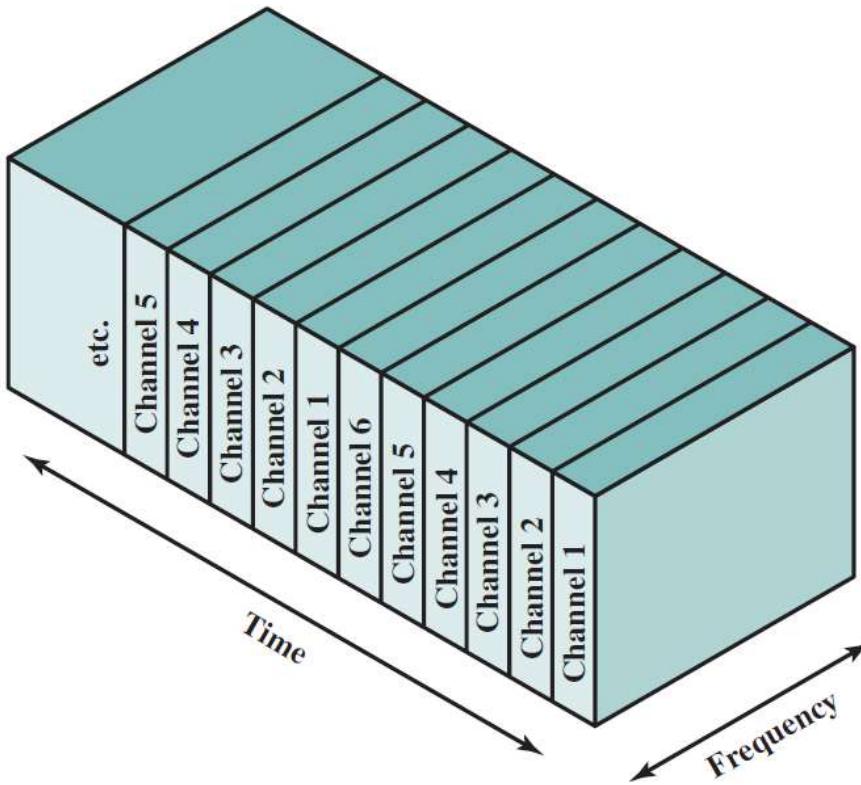
Data rate of multiplexed line is fixed

If one channel receiver can not receive data, the others must carry on

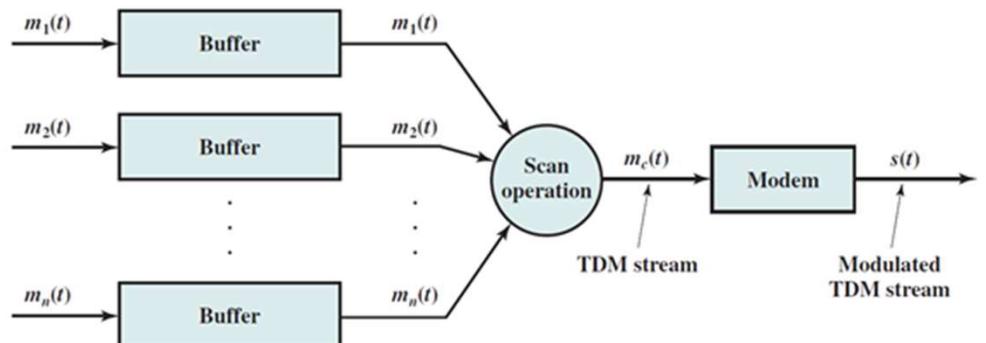
The corresponding source must be quenched; this leaves empty slots

Error control

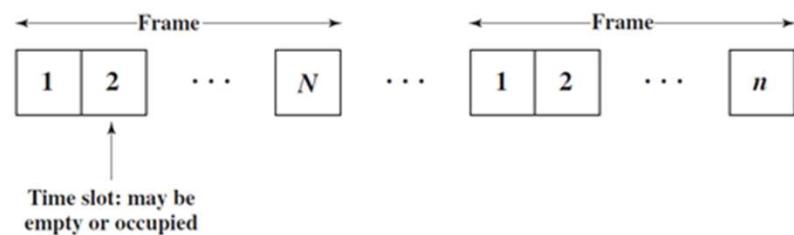
Errors are detected and handled by individual channel systems



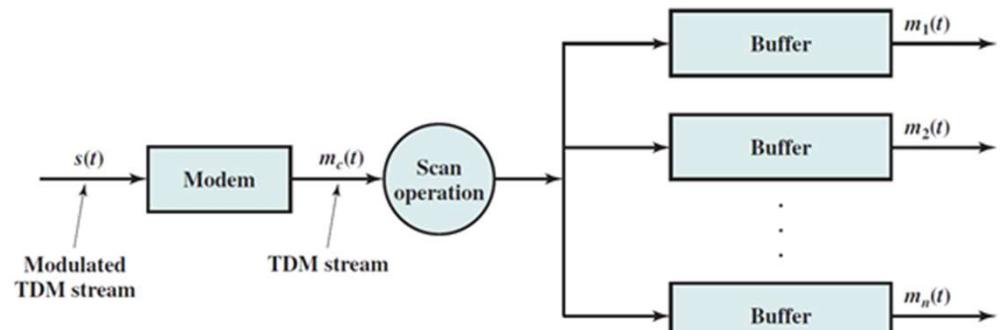
(b) Time-division multiplexing



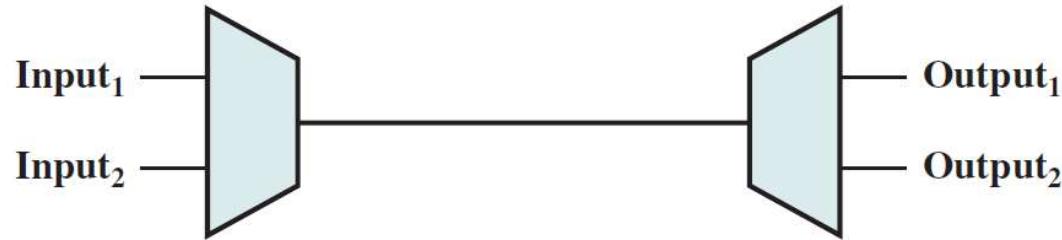
(a) Transmitter



(b) TDM frames



(c) Receiver



(a) Configuration

Input₁..... F₁ f₁ f₁ d₁ d₁ d₁ C₁ A₁ F₁ f₁ f₁ d₁ d₁ d₁ C₁ A₁ F₁

Input₂..... F₂ f₂ f₂ d₂ d₂ d₂ C₂ A₂ F₂ f₂ f₂ d₂ d₂ d₂ C₂ A₂ F₂

(b) Input data streams

... f₂ F₁ d₂ f₁ d₂ f₁ d₂ d₁ d₂ d₁ C₂ d₁ A₂ C₁ F₂ A₁ f₂ F₁ f₂ f₁ d₂ f₁ d₂ d₁ d₂ d₁ C₂ C₁ A₂ A₁ F₂ F₁

(c) Multiplexed data stream

Data Link Control on TDM

New issues:

Framing: synchronization of TDM frames, add of extra control bits per TDM frame

No flag or SYNC characters bracketing TDM frames

Must provide synchronizing mechanism

Added digit framing

One control bit added to each TDM frame

Looks like another channel - “control channel”

Identifiable bit pattern used on control channel

e.g. alternating 01010101...unlikely on a data channel

Pulse stuffing: synchronizing various data sources, adding extra bits or pulses, obtaining multiples of a basic data rate (ex. 4kHz).

Clocks in different sources drifting

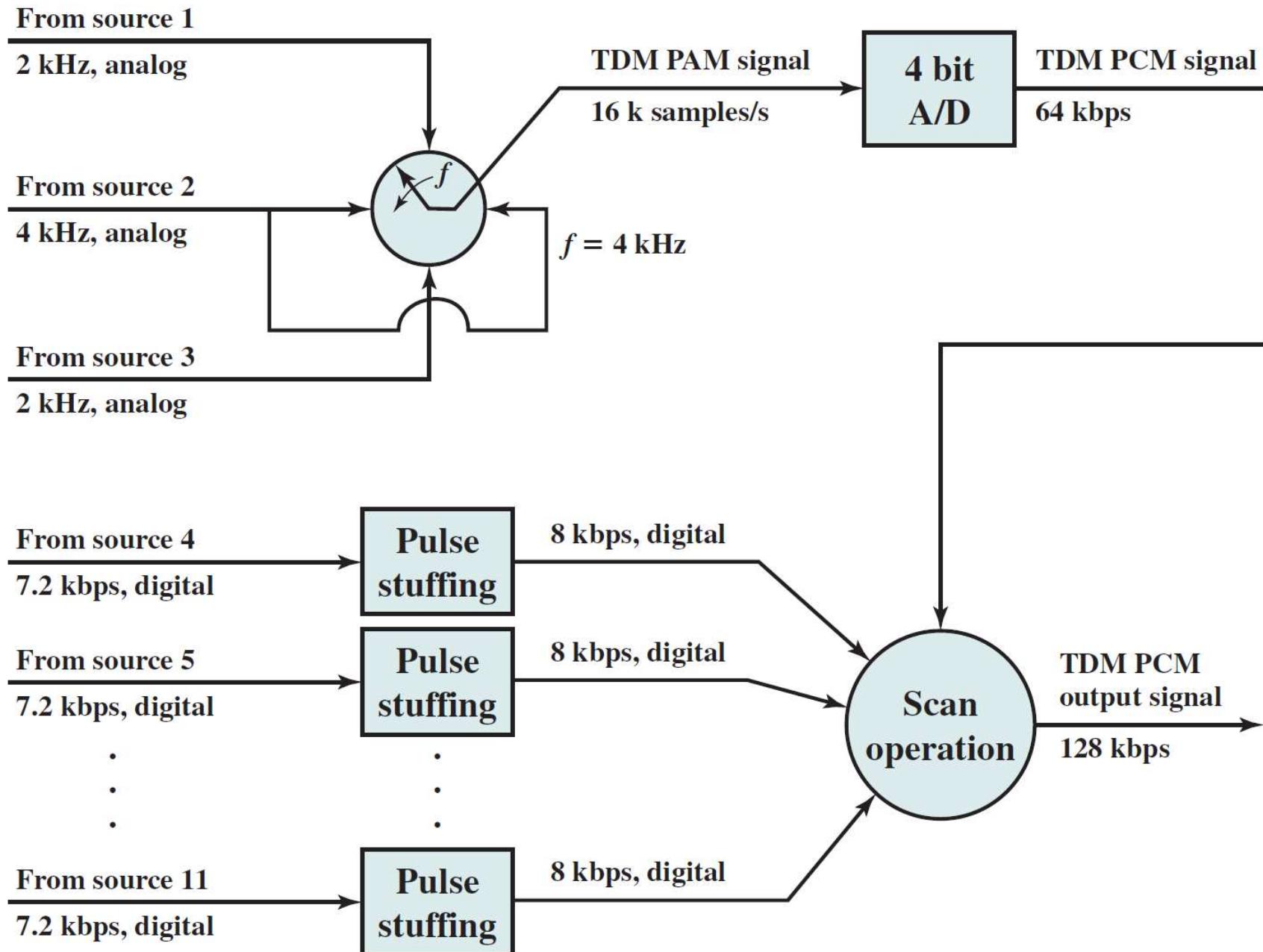
Data rates from different sources not related by simple rational number

Outgoing data rate (excluding framing bits) higher than sum of incoming rates

Stuff extra dummy bits or pulses into each incoming signal until it matches local clock

Stuffed pulses inserted at fixed locations in frame and removed at demultiplexer

TDM of Analog and Digital Sources



Digital TDM Hierarchy

Scale of the Digital Services:

North America	Europe
DS0: 64kbps	E0:64kbps
DS1:1.544Mbps	E1:2.048Mbps
DS2:6.313Mbps	E2:8.448Mbps
DS3:44.736Mbps	E3:34.368Mbps
DS4:274.176Mbps	E4:139.264Mbps
.....

Why 64kbps the basic data rate?

Bandwidth of the voice signal: 4kHz => Sample rate: 8kHz, or one sample every 125μsec

Number of bits for quantification: 8 => Needed data rate:

$$8\text{bits/sample} * 8000\text{samples/sec} = 64\text{kbps.}$$

History: In 1962 telephone carrier (cable) between Bell System offices carried approx. 1.5Mbps over a mile (distance between amplifiers – manholes in the city) $\Rightarrow 1500/64$ = approx. 24 voice channels TDM multiplexed on that carrier => Telecommunication-1 carrier or T1 carrier, in USA.

T1 – 24 channels = Digital Service 1 = DS1

T1 frame has a format of 193bits, transmitted at 125μsec each.

$193 = 24 * 8$ data bits + 1 framing (control bit) => gross data rate: 1.544Mbps, from this: 8000bps of signaling information... may be too much?

Control bit is 1 or 0, according to the synchronizing sequence 10101....

An example for **signaling**, transmission of control information.

ITU-T standard for signaling differs from US Bell's one (T versus E !)

Two major signalling methods:

- common-channel signaling (as above)

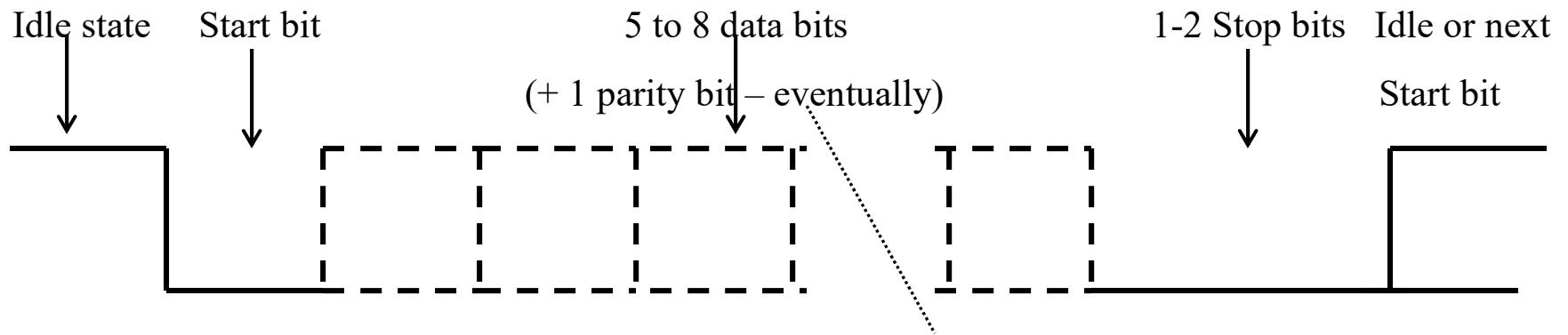
- channel associated signaling: an extra signaling subchannel provided

Synchronization

Asynchronous transmission

Data are transmitted one *character* at a time, where each character is five to eight bits in length (utile data). See ASCII code...

Timing or synchronization must only be maintained within each character; the receiver has the opportunity to resynchronize at the beginning of each new character. Samples are taken in the middle of the bit period.



Synchronous transmission

Works with blocks of bits (characters).

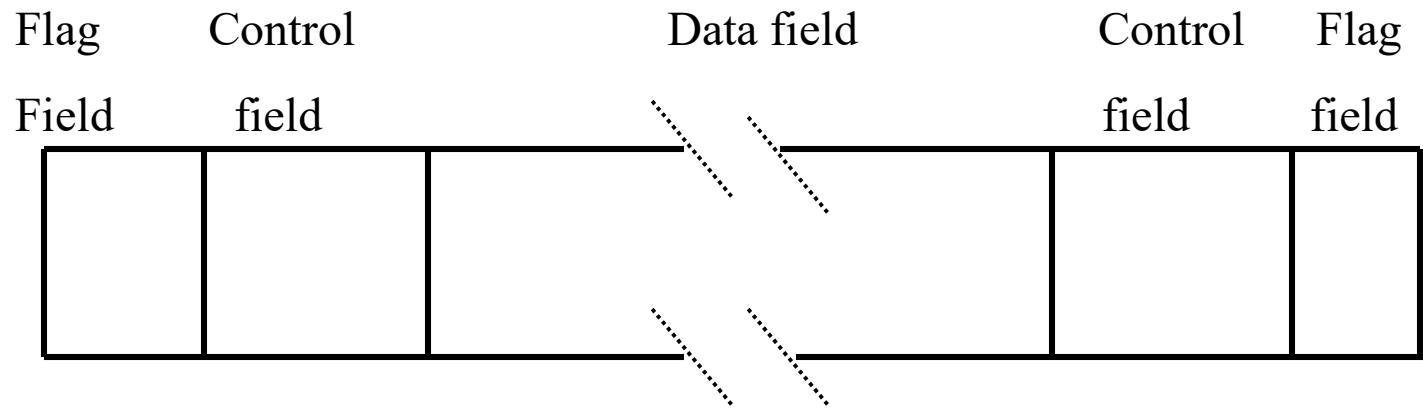
Inter-clock synchronization:

- auxiliary clock line

- biphasic coding

- + Synchronization at the block level => extra flag and control fields => data structure of **frame**

Flag fields (synchronization) fields: special bit sequences or *sync* characters; denoted as *preamble-header* and *trailer*



Comparisons

Asynchronous transmission	Synchronous transmission
Simple	Complex
Cheap	Expensive
Fixed burden (20%, 30%), depends on Stop bit number	Burden varies with block size
Fits keyboard action	Fits transmissions of blocks of data
1000 bytes takes 10000bits	1000 bytes may take 1003bytes

SOLVED PROBLEMS

#1. The human hearing system operates in the range of 2 – 20,000Hz. What sampling rate will be sufficient to preserve the information content of the signals in this range?

Solution

Cf. Nyquist theory, the sampling rate must be at least twice the bandwidth.

Requested bandwidth is: $20000 - 2 = 19998\text{Hz}$, so the necessary for sampling is $2 \cdot 19998 = 39,996$ samples/sec.

#2. In order to transmit an uncompressed video stream at 30 frames/second into a quarter size VGA window ($160 * 120$ pixels), where each pixel requires 24bits for colour, what transmission capacity is required?

Solution

Total number of pixels in a window: $160 \cdot 120 = 19,200$ pixels.

Total number of bits requested within a window: $19,200 \cdot 24 = 460,800$ bits.

Number of bits for 30 frames (number of bits sent on a second): $460,800 \cdot 30 = 13,824,000$ bits so there is a need for a transmission speed of approx. 13.8Mbps.

#3. Given a link with a signal/noise ratio of 1023, what bandwidth is required to support the transmission rate from previous problem?

At the required bandwidth, how many bits will be transmitted per Hertz?

Solution

Cf. Shannon theorem ($v=H \cdot \log_2(1+S/N)$); the transmission rate (channel speed) is 13,824,000bps.

$$H = 13,824,000 / \log_2(1+1023) = 13,824,000 / 10 = 1,382,400\text{Hz, approx. } 1,3\text{MHz.}$$

#4. A full duplex 64,000bps point-to-point data link was observed for sixty seconds. During this observation period, the following were obtained:

- 50 original data packets, each containing 24 header bytes and 1000 data bytes
- five additional data bytes observed to be retransmissions
- 100 acknowledgements , each containing 24 header bytes and no data
- 4 connection management packets, each containing 124 bytes.

What was the channel utilization?

Solution

The bytes sent with data packets: $50 \cdot (24 + 1000) = 51,200$ bytes

The bytes sent for retransmission: 5 bytes

The bytes for acknowledgements: $100 \cdot 24 = 2400$ bytes

The bytes for connection management: $4 \cdot 124 = 496$ bytes

The total of sent bytes: $51,200 + 5 + 2,400 + 496 = 54,101$ bytes

1 byte = 8 bits => a number of: $54101 \cdot 8 = 432,808$ bits

Theoretically during 60 sec, channel could carry: $64,000 \cdot 60 = 3,840,000$ bits.

**The utilisation of the channel is: number of sent bits / theoretical number =
 $432,808 / 3,840,000 \sim 9\%$**

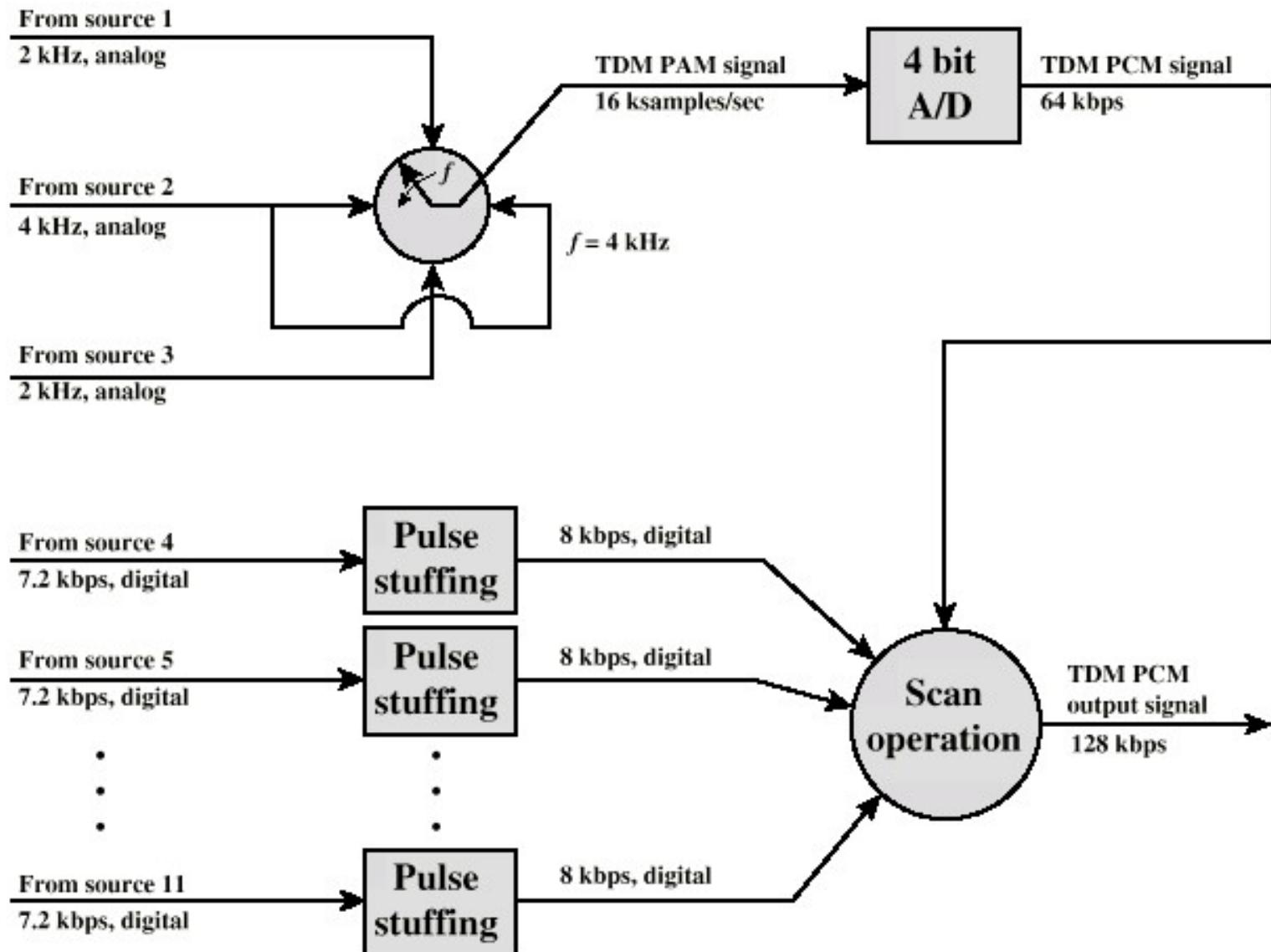
#5. Consider that there are 11 sources to be multiplexed on a single link:

-source 1: analog, 2kHz bandwidth

-Source 2: analog, 4kHz bandwidth

-Source 3: analog, 2kHz bandwidth

-Sources 4-11: digital, 7200bps synchronous.(see next slide)



Solution

Analog sources converted to digital using PCM;

Cf. Nyquist theorem, the sampling rate needs be at least twice the bandwidth, I.e. 4000samples/sec for sources 1 and 3 and 8000 samples/sec for source 2.

Sampling, we obtain analog samples (PAM) => need for quantification (be digitized); assume that 4 bits are enough. If we consider that these 3 sources are multiplexed first, at a scan rate of 4kHz, we will obtain one PAM sample for sources 1 and 3, and 2 PAM samples for source 2. These 4 samples are interleaved and converted to 4-bit PCM samples (digital values). So we need 16bit (16 bit buffer needed) to represent all PCMs, and this item is generated 4000 times/sec, so results a composite rate for the digital signal of 64kbps.

For the digital sources we will use first the *bit stuffing* to reach a rate of 8kbps, so we obtain a aggregate rate of 64kbps. For each digital source we need a 2-bit buffer (because the scan is done every 1/4000sec).

Adding all signals, it results we need a TDM composite signal of 128kbps, and the frame structure will contain 32 bits.

Proposed problems

- #1. A modem operates at 1800 baud and can encode each sample using 4 bits. What is the data rate at which the modem can transmit data?
- #2. What is the channel capacity for a teleprinter channel with a 300Hz bandwidth and a signal-to-noise ratio of 3dB?
- #3. Given a channel with an intended capacity of 20Mbps, the bandwidth of the channel is 3MHz. What signal-to-noise ratio is required to achieve this capacity?
- #4. A digital signaling system is required to operate at 9600bps. If a signal element encodes a 8-bit word, what is the minimum required bandwidth of the channel?
- #5. a). A digitized TV picture is to be transmitted from a source that uses a matrix of 480×500 picture elements (pixels), where each pixel can take one of 32 intensity values. Assume that 30 pictures are sent per second. Find the source data rate.
b). Assume that the TV picture is to be transmitted over a channel with 4.5MHz bandwidth and a 35dB signal-to-noise ratio. Find the capacity of that channel.
c). Assume that a noiseless fiber optic channel is used; how much bandwidth is needed and how many microns of wavelength are needed for this band at 1.30microns?

- #6. Deduce the maximum theoretical information rates associated with the following transmissions channels:
- Telex network with a bandwidth of 500Hz and a signal-to-noise ratio of 5dB
 - Switched telephone network with a bandwidth of 3100Hz and a signal-to-noise ratio of 20dB
- #7. A noiseless 4KHz channel is sampled every 1msec. What is the maximum data rate?
- #8. Television channels are 6MHz wide. If the channel is noiseless, what data rate may be achieved for a four-level digital signal used?
- #9. If a binary signal is sent over a 3kHz channel whose signal-to-noise ratio is 20dB, what is the maximum achievable data rate?
- #10. Why has the PCM sampling time been set at 125microsec?
- #11. Ten signals, each requiring 4000Hz, are multiplexed onto a single channel using FDM. How much minimum bandwidth is required for the multiplexed channel? Assume that the guard bands are 400Hz wide.

#12. Assuming the velocity of propagation of an electrical signal is equal with 70% of the speed of the light, determine the ratio of the signal propagation delay to the transmission delay, for the following types of data link and 1000 bits of data:

- a). 100m of UTP wire and a transmission rate of 1Mbps
- b). 0.5km of coaxial cable and a transmission rate of 10Mbps

If the signal propagates with the speed of the light, the same question for :

- c). A satellite link and a transmission rate of 512Kbps
- d). 2.5km of fiber optic and a transmission rate of 1000Mbps

#13. The maximum distance between two terrestrial microwave stations is given by the expression:

$$d = 7.14\sqrt{K \cdot h}$$

K relates to the curvature of the earth and h is the height of the dishes above.

Assuming $K = 4/3$ determine d for the following values of h : 10m, 20m, 50m, 100m.

#14. Draw a block diagram similar to figure in slide#5 for a TDM PCM system that will accommodate 4 digital synchronous inputs at 300bps, and one analog input with a bandwidth of 500Hz. The analog samples will be coded using 4bits.

#15. Find the number of the following devices that could be accommodated by a T1-type TDM line, if 3% of the line capacity is reserved for synchronization purposes:

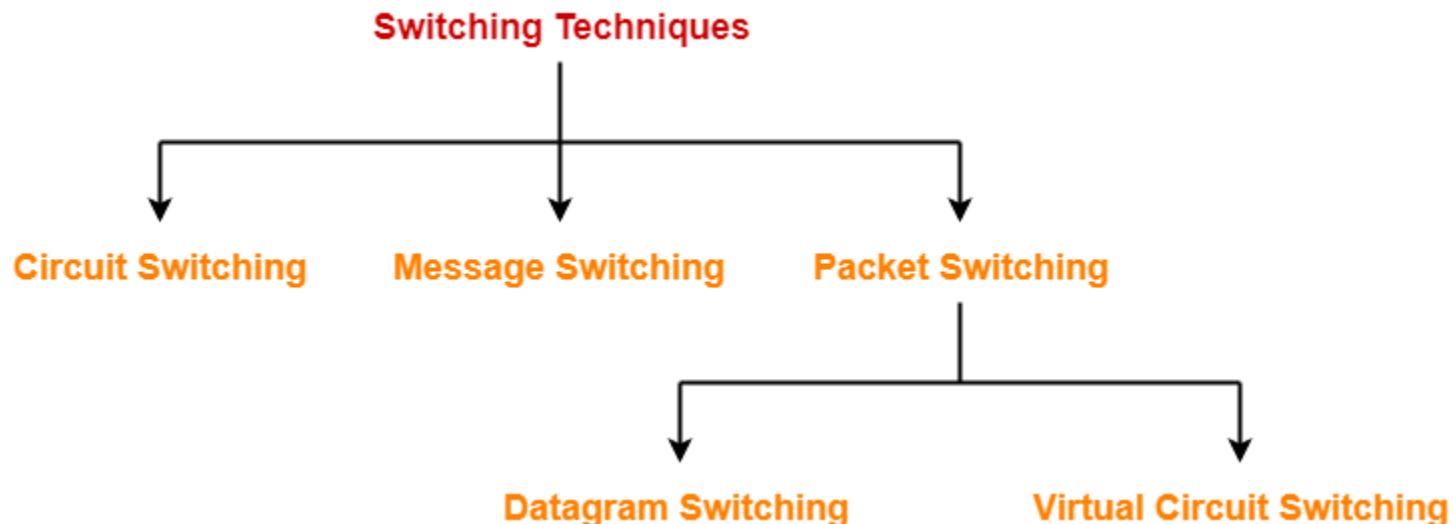
- 110bps teleprinter terminals
- 1200bps computer terminals
- 64kbps PCM voice frequency lines.

Switching techniques

Traditionally the telephonic system is based on circuit switching; is the main infrastructure for communications (computer) networks => the **switching** term remains.

Switching techniques used in information transfer are:

- circuit switching**
- message switching**
- packet switching**

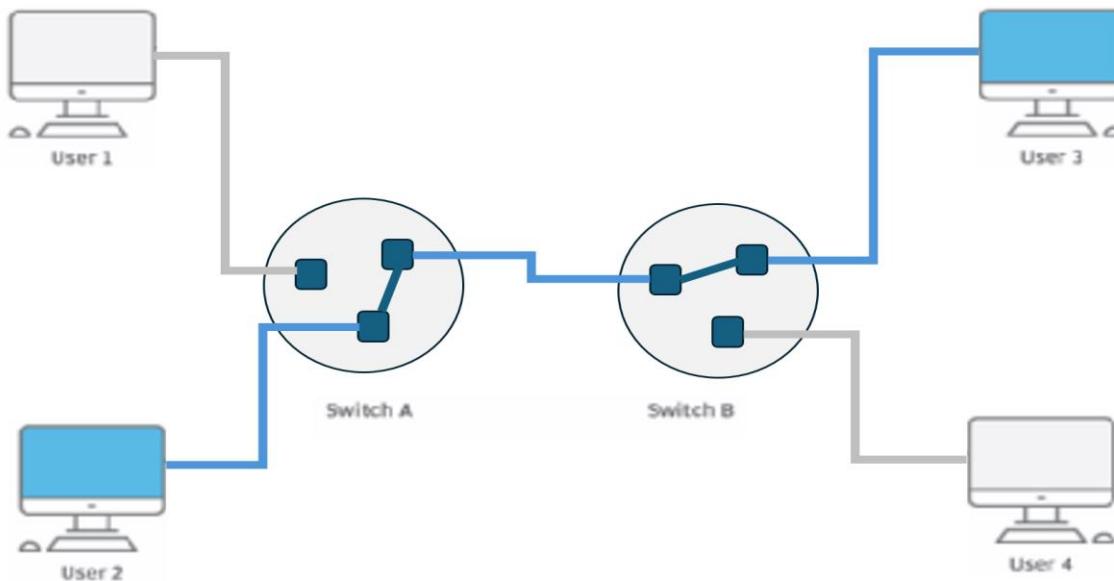


Circuit switching

Physical path between communicating parts, achieved using circuit switching –switches (relays)-in the networks nodes.

Three phase communication:

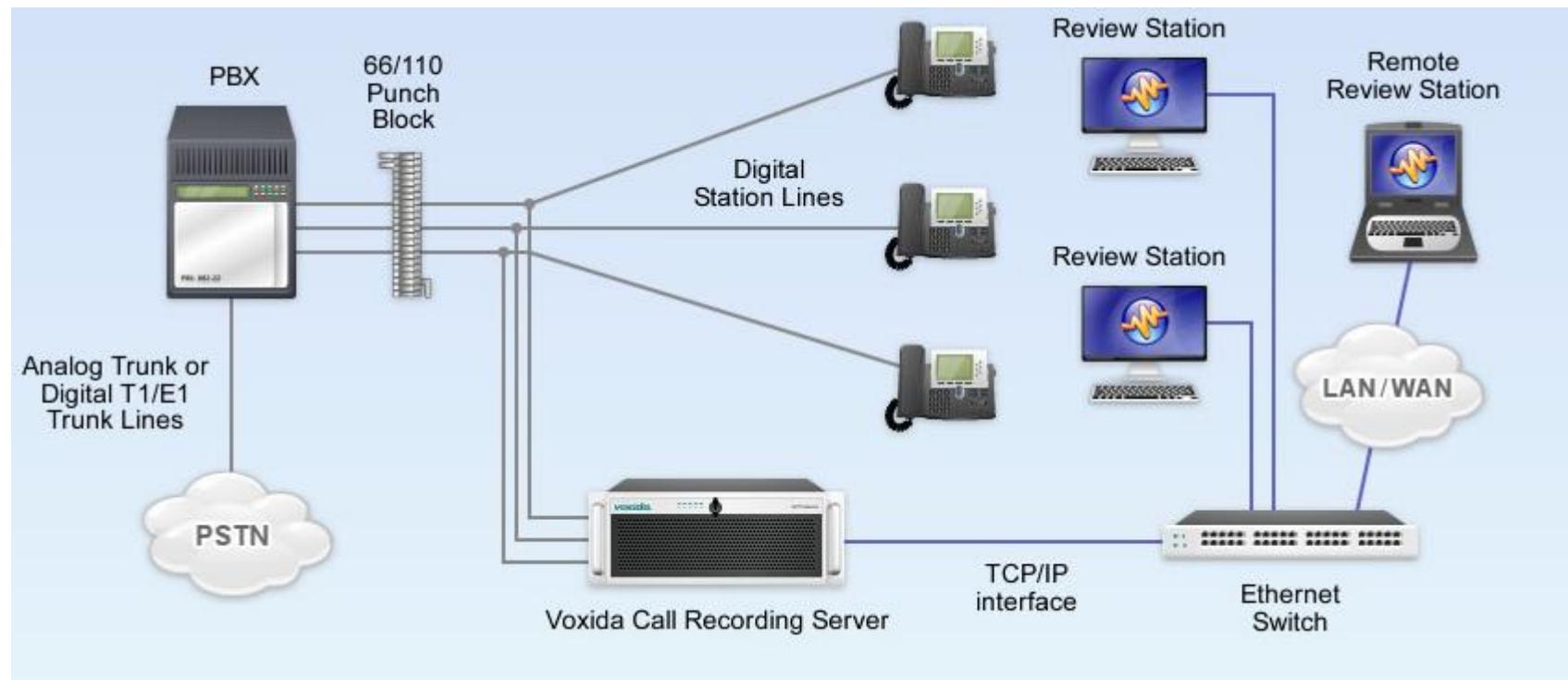
- circuit establishment (setup), establish a (optimum) path between parts; both parts agree communication
- effective data transmission (signal transfer), on this route
- circuit release (disconnection); initiative of one part.



Circuit switching

Drawbacks:

- not efficient due to existence of the first phase (it will exist even if there's no data transfer)
 - need for covering bandwidth allocation
 - important amount of cabling
 - no buffers in switches for transmission equalization
- Today use of digital **PBX** (Private Branch Exchange)



First circuit-switching: space-division switching (separated signal paths – divided in space): crossbar matrix of I/O full duplex lines

An improvement: multiple-stage switches

Today all telephony: digital time-division techniques (synchronous TDM)

Signaling in digital telephony:

-inchannel

- in-band: signals using the same band as the voice channel (as payload)
- out-band: (voice signals do not use whole 4kHz bandwidth)

-common channel – a common signal channel for a number of voice channels

Signaling may use the same (or not) path as the payload (associated/nonassociated modes)

What's signaling?

Signal = control Examples:

- connection setup request = off-hook signal from telephone to switch
- connection setup acknowledge = dial tone
- destination address = pulse or tone dialing
- destination busy = busy tone
- destination available = ringing tone

Other signaling functions: transmission of: dialed number between switches, information about a call not completed, about billing, diagnose and failure isolation

Message switching

Data transfer using **messages** (independent data units, with diff. lengths but similar structures). Types: control and data (embedding control)

Need for addressing (source & destination of message)

Communications nodes are not physical switches, but computing systems (with memory and processing units).

Philosophy is: message *store & forward* .

Not more dedicated communications path; established in an optimum way (cost, network status) by nodes (using routing tables).

Advantages:

- improvement in efficiency (path multiplexing)
- introduces message priority
- equilibrated transmissions.

Drawbacks:

- messages are too long, memory waste and difficult error recovery

Packet switching

Combines the advantages of previous methods. The **packet** has similar message structure but a lower length, up to 1000octets.

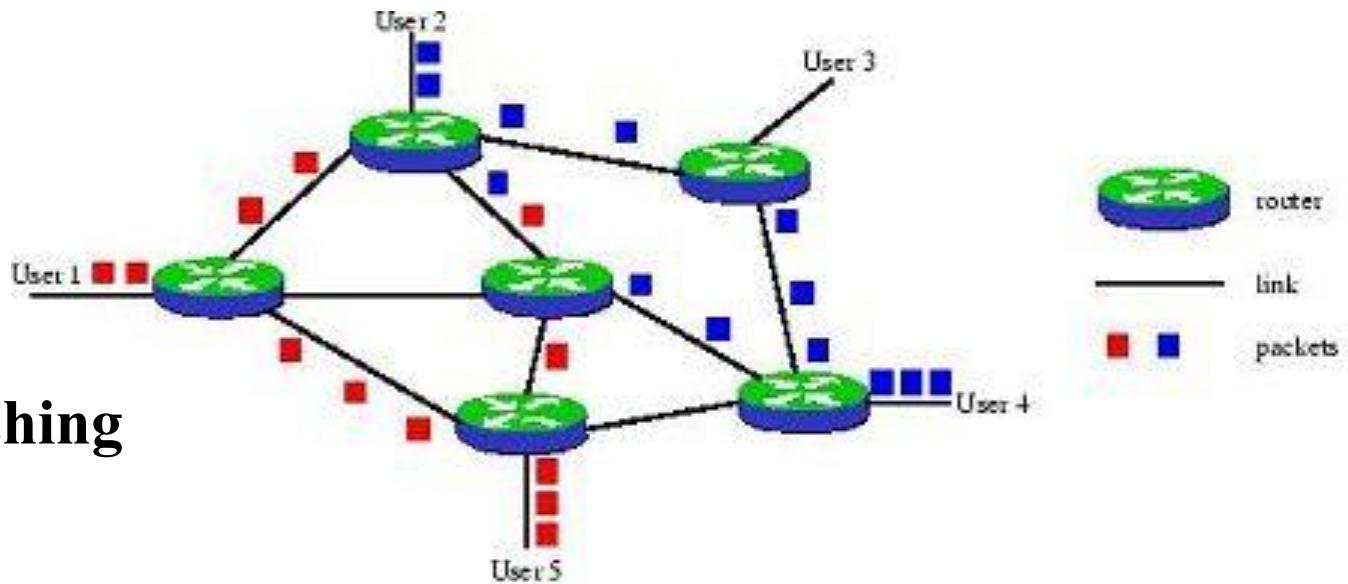
Two methods:

-use of **datagrams** (close to message switching)-more speedy and flexible method

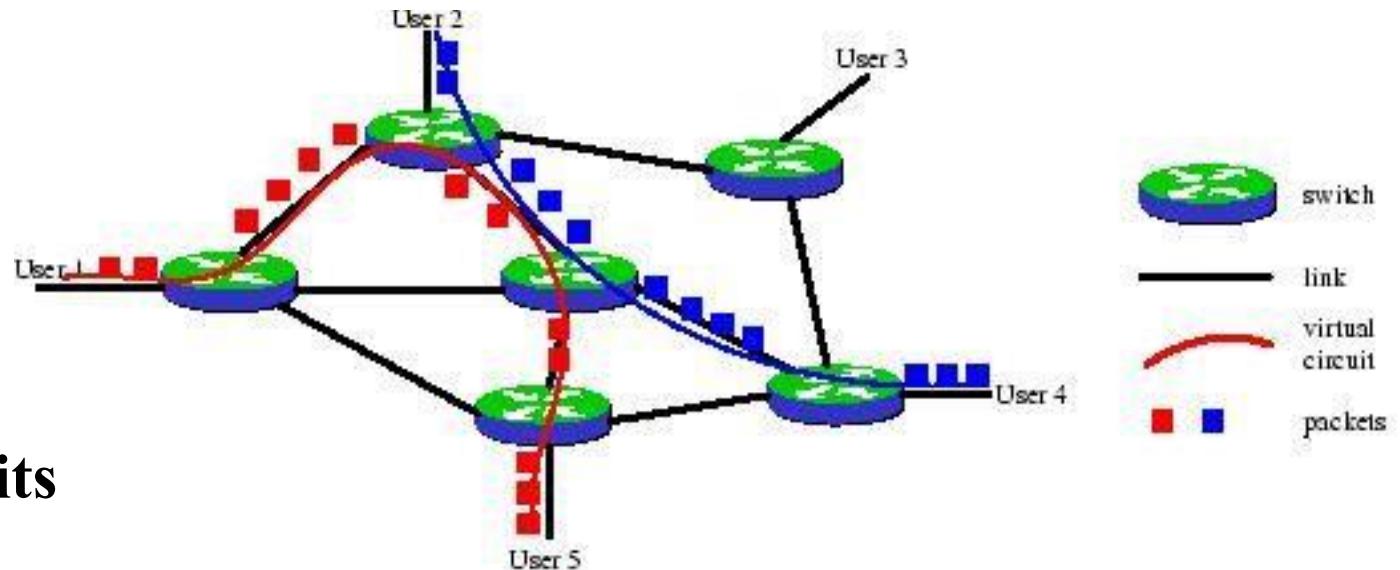
- use or not of transmission acknowledgments (ACK)

-use of **virtual circuits** (close to circuit switching)-use of the three phases (connection request, data transfer, disconnect) for a logical connection activation; use of special control packets for that. Also embedding of control information (piggybacking).

A logical connection may be implemented with more different physical connections.



Datagram switching



Virtual circuits

Routing in packet-switching networks

Circuit switching vs. Packet switching

Most of WANs based on circuit or packet switching

Circuit switching designed for voice

Resources dedicated to a particular call

Much of the time a data connection is idle

Data rate is fixed

Both ends must operate at the same rate

Packet switching - Basic Operation

Data transmitted in small packets

Typically 1000 octets

Longer messages split into series of packets

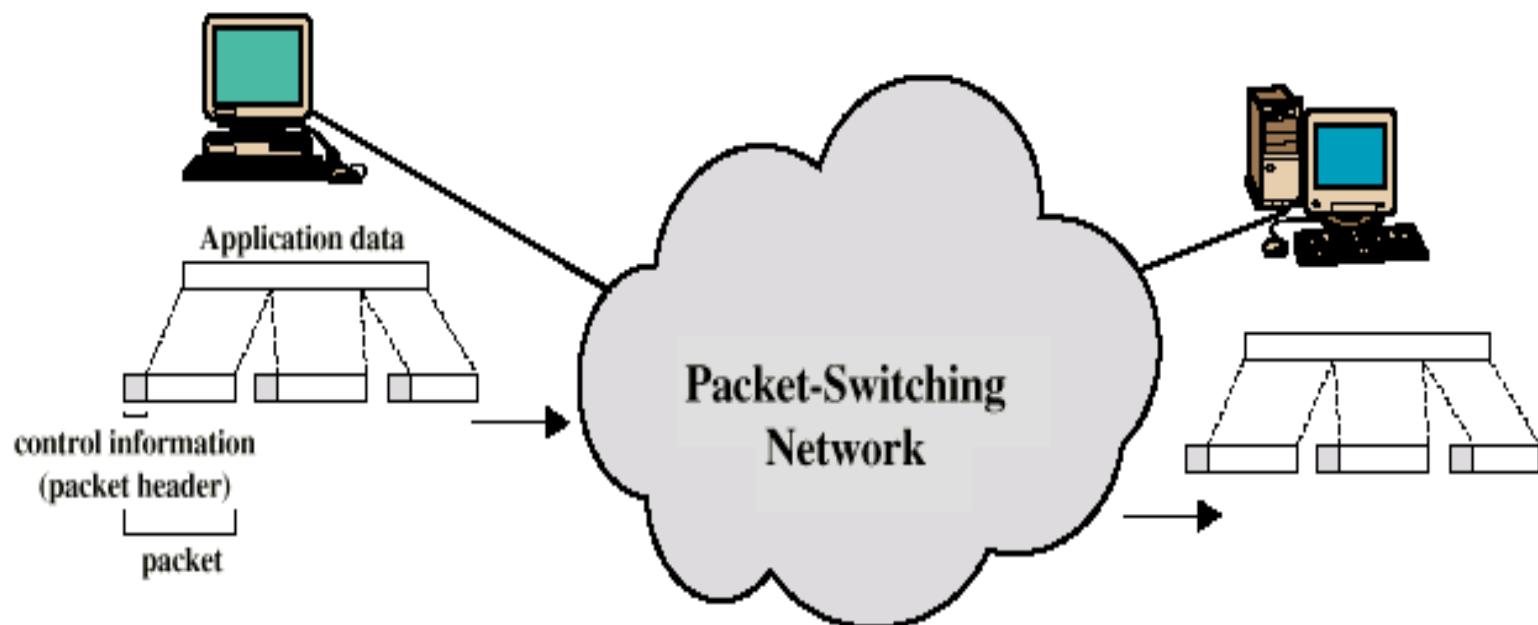
Each packet contains a portion of user data plus some control info

Use of Control info

Routing (addressing) info

Packets are received, stored briefly (buffered) and pass on to the next node

Store and forward



Advantages of packet switching

Line efficiency

Single node to node link can be shared by many packets over time

Packets queued and transmitted as fast as possible

Data rate conversion

Each station connects to the local node at its own speed

Nodes buffer data if required to equalize rates

Packets are accepted even when network is busy

Delivery may slow down

Priorities can be used

Packet Switching Technique

Station breaks long message into packets

Packets sent one at a time to the network

Packets handled in two ways: **Datagram or Virtual circuit**

Virtual Circuits v Datagram

Virtual circuits

Network can provide sequencing and error control

Packets are forwarded more quickly

No routing decisions to make

Less reliable

Loss of a node loses all circuits through that node

Datagram

No call setup phase

Better if few packets

More flexible

Routing can be used to avoid congested parts of the network

Use of variant with acknowledgements

Routing

Complex, crucial aspect of packet switched networks

Characteristics required

Correctness

Simplicity

Robustness

Stability

Fairness

Optimality

Efficiency

Performance Criteria

Used for selection of route

Minimum hop

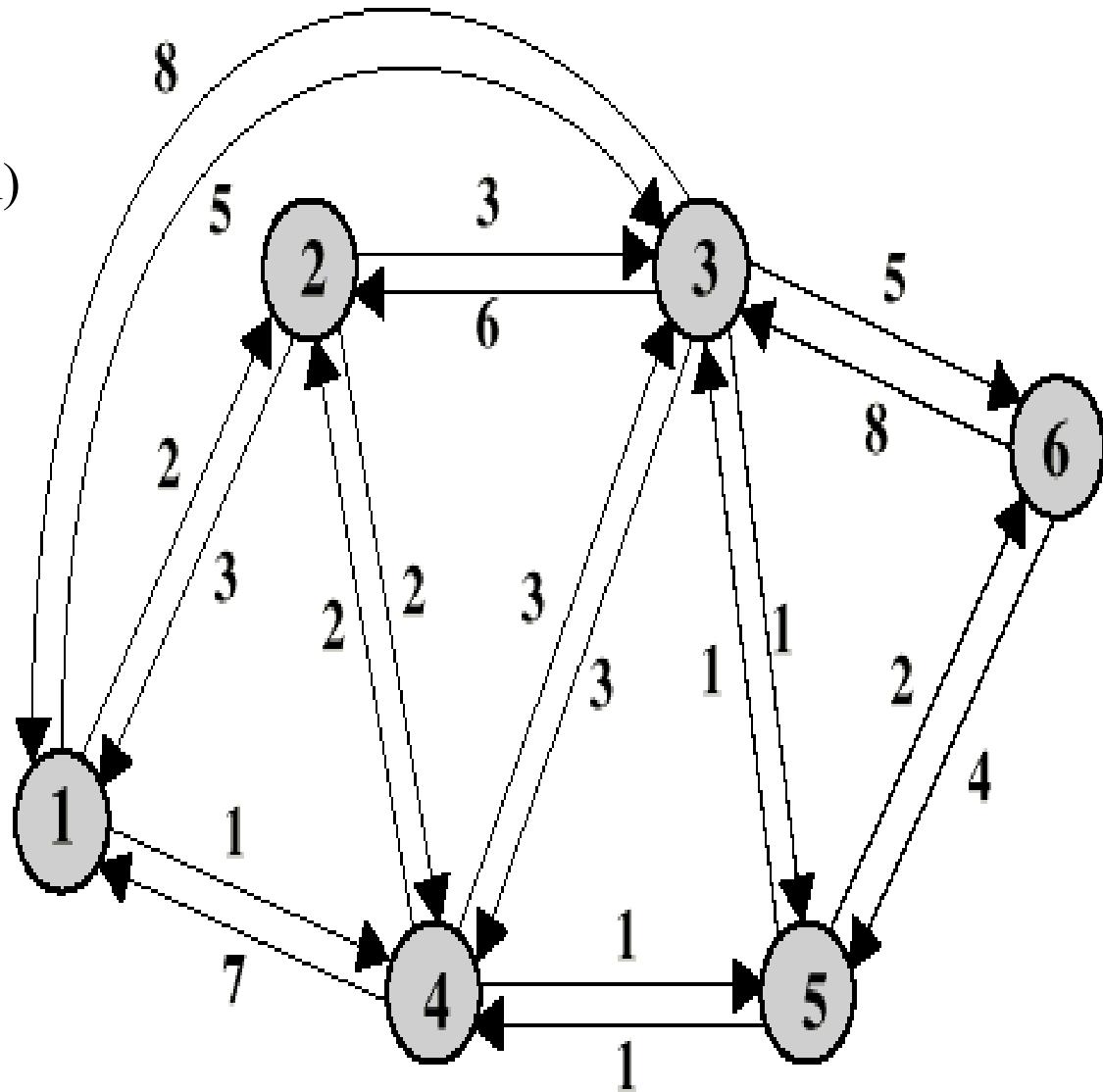
Least cost algorithms (shortest path)

Dijkstra's Algorithm

Implemented in link state packet
routing algorithms

Bellman-Ford algorithm

Used by distance vector based



Routing: Decision Time and Place

Time

On packet or virtual circuit basis

Place

Distributed routing

Made by each node

Centralized routing

Source-based routing

Network Information Source and Update Timing

Routing decisions usually based on knowledge of network (not always)

Distributed routing

Nodes use local knowledge

May collect info from adjacent nodes

May collect info from all nodes on a potential route

Central routing

Collect info from all nodes

Update timing

When is network info held by nodes updated

Fixed - never updated

Adaptive - regular updates

Routing Strategies

Fixed

Flooding

Random

Adaptive

Fixed Routing

Single permanent route for each source to destination pair

Determine routes using a *least cost algorithm*

Route fixed, at least until a change in network topology

		From Node					
		1	2	3	4	5	6
To Node	1	—	1	5	2	4	5
	2	2	—	5	2	4	5
	3	4	3	—	5	3	5
	4	4	4	5	—	4	5
	5	4	4	5	5	—	5
	6	4	4	5	5	6	—

Node 1 Directory		Node 2 Directory		Node 3 Directory	
Destination	Next Node	Destination	Next Node	Destination	Next Node
2	2	1	1	1	5
3	4	3	3	2	5
4	4	4	4	4	5
5	4	5	4	5	5
6	4	6	4	6	5

Node 4 Directory		Node 5 Directory		Node 6 Directory	
Destination	Next Node	Destination	Next Node	Destination	Next Node
1	2	1	4	1	5
2	2	2	4	2	5
3	5	3	3	3	5
5	5	4	4	4	5
6	5	6	6	5	5

Flooding

No network info required

Packet sent by node to every neighbor

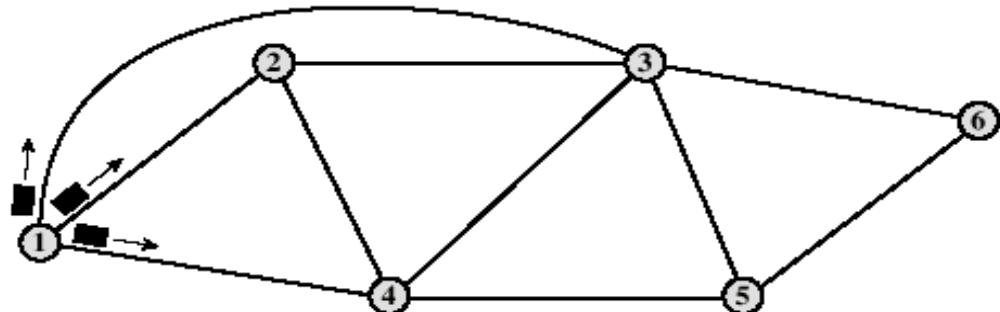
Incoming packets retransmitted on every link except incoming link

Eventually a number of copies will arrive at destination

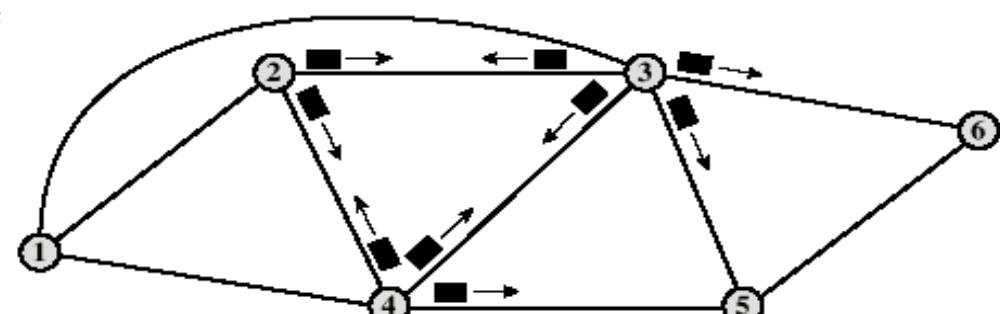
Each packet is uniquely numbered so duplicates can be discarded

Nodes can remember packets already forwarded to keep network load in bounds

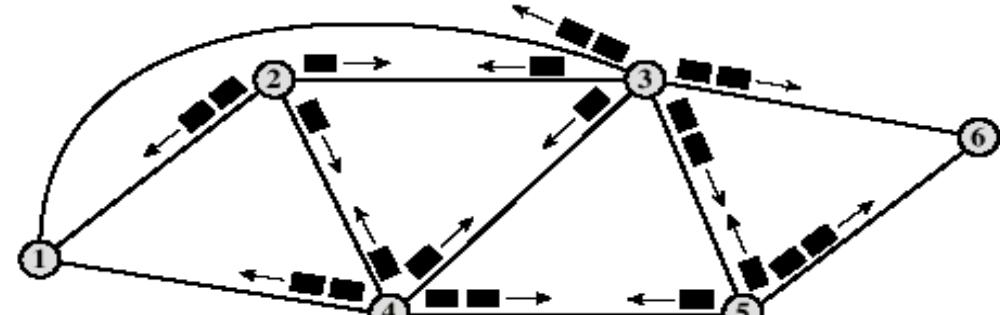
Can include a hop count in packets



(a) First hop



(b) Second hop



(c) Third hop

Properties of Flooding

All possible routes are tried

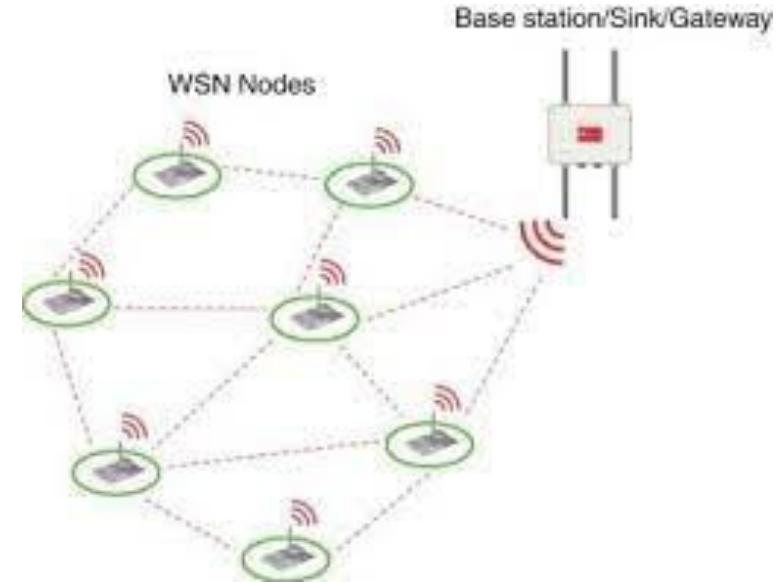
Very robust

At least one packet will have taken minimum hop count route

Can be used to set up virtual circuit

All nodes are visited

Useful to distribute information (e.g. routing)



Random Routing

Node selects one outgoing path for retransmission of incoming packet

Selection can be random or round robin

Can select outgoing path based on probability calculation

No network info needed

Route is typically not least cost nor minimum hop

Adaptive Routing

Used by almost all packet switching networks

Routing decisions change as conditions on the network change

Failure

Congestion

Requires info about network

Decisions more complex

Tradeoff between quality of network info and overhead

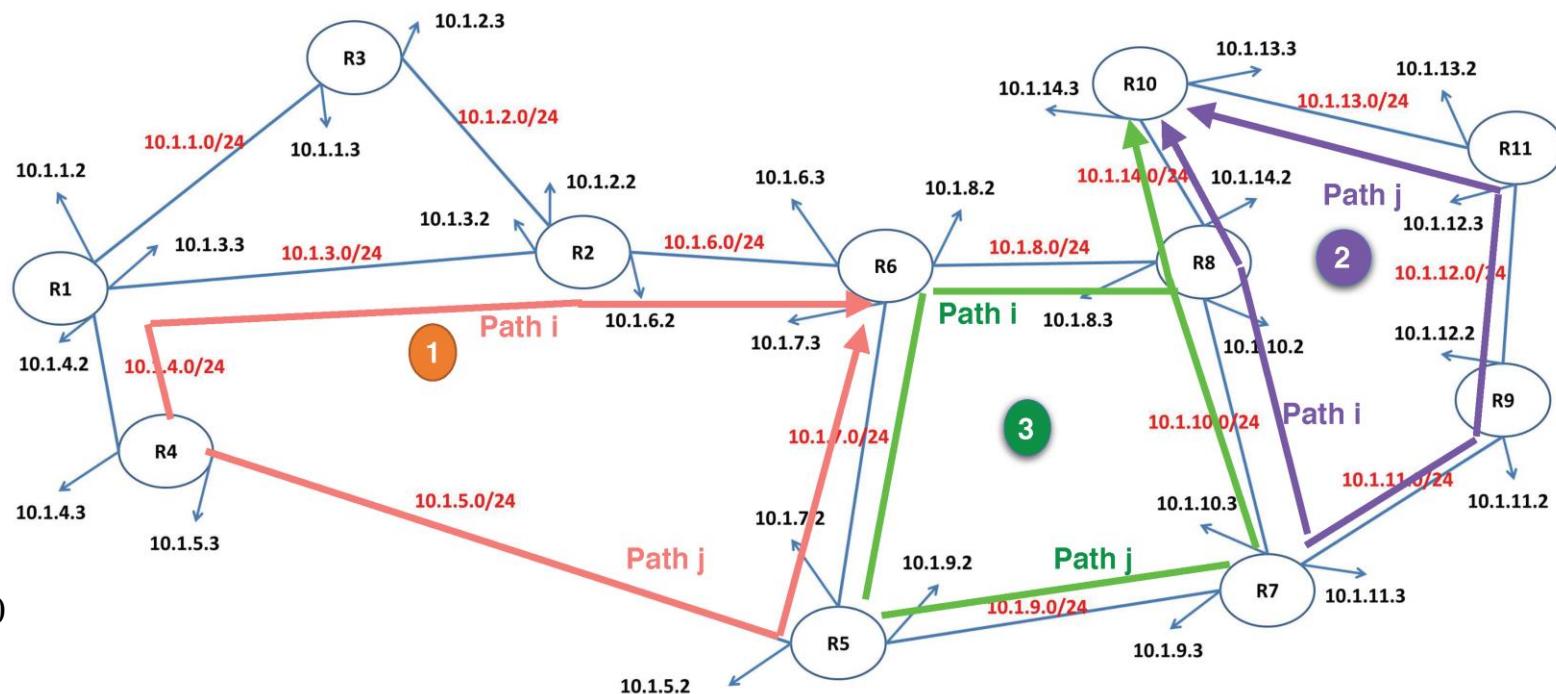
Advantages

Improved performance

Aid congestion control

Complex system

May not realize theoretical benefits



Classification

Based on information sources for network state

Local (isolated)

Route to outgoing link with shortest queue

Can include bias for each destination

Rarely used - do not make use of easily available info

Adjacent nodes – select information based on the neighbour's experience (network delays or outages)

All nodes – used for source based routing

Access to Data & Computer Networks – Physical Level

- **Terminology**
- **Serial Interface**
- **Cable Modems**
- **DSL technologies**

ISP (Internet Service Provider)

- An Internet service provider company that provides other companies or individuals with access to, or presence on, the Internet
- Individual hosts and LANs are connected to an (ISP) through a point of presence (POP).

POP (Point of Presence)

- An Internet access provider may operate several POPs distributed throughout its area of operation and represents a collection of telecommunications equipment

CPE (Customer Premises Equipment)

- is the communications equipment located onsite with the host (example: modem)

Local loop” or “last mile

- the infrastructure between a provider's installation and the site where the host is Located

NAP (Network Access Point)

- a physical facility that provides the infrastructure to move data between connected networks; serve to tie the ISPs together; ISP also connect using peering arrangements and interconnections within geographic regions

CO (Central Office)

- the place where telephone companies terminate customer lines and locate switching equipment to interconnect those lines with other networks

Common connections for SOHO (small office home office) LANs

Cable - offered by cable television service providers, where data signal is carried on television cable;

- high bandwidth, always on connection

DSL – on telephone lines (usually ADSL)

- high bandwidth, always on connection

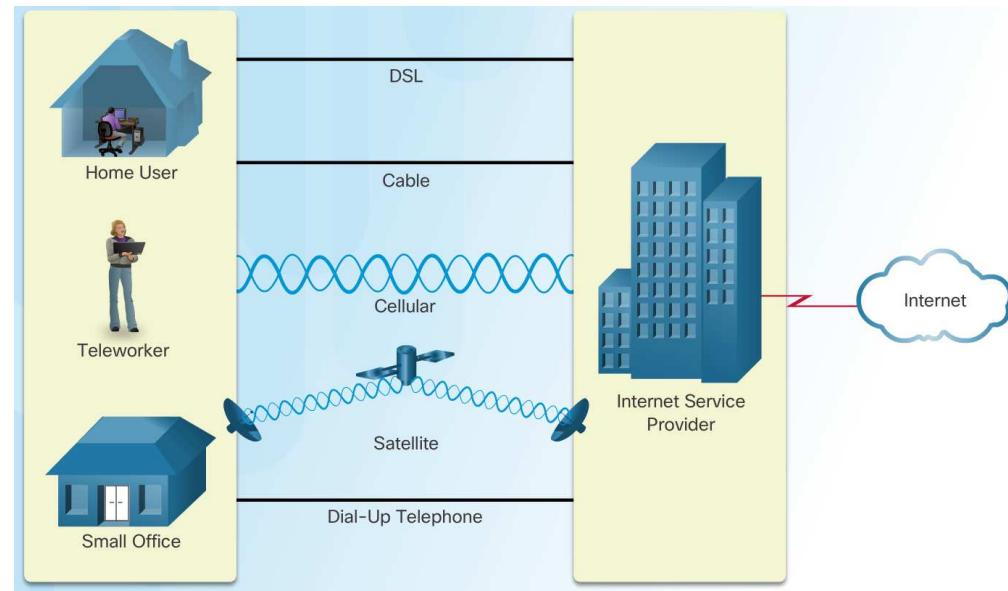
Cellular - using cell phone network; performance limited by phone and cell tower the capabilities.

Satellite – using satellite dishes

- requires a clear line of sight to the satellite.

Dial-up Telephone - inexpensive option using phone line and modems.

- low bandwidth not recommended for large data transfer.



Cisco CCNA1

Serial Interface

Serial Transmission – all bits (of an octet) are transmitted (received) on a single line

Parallel Transmission – each bit (of an octet) uses a line

Data processing devices (or **Data Terminal Equipment, DTE**, like computers, terminals, printers) do not (usually) include data transmission facilities, are stand alone equipment.

Need for an interface, called **Data Circuit terminating Equipment (DCE**, e.g. modem, NIC –Network Interface Card)

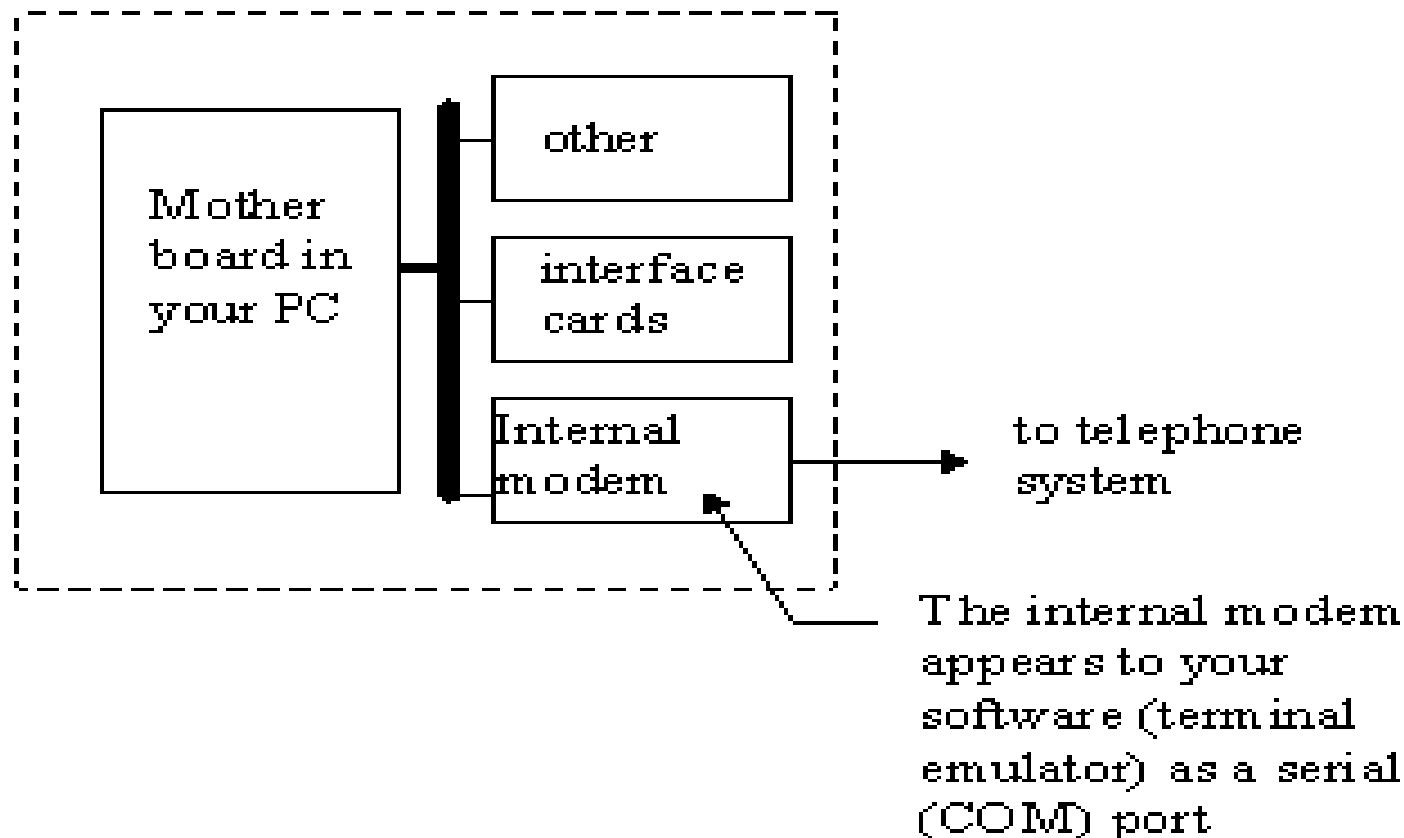
First data transmissions used the telephonic system, a normal phone and a modem, so a **dial-up line** (line established by circuit switching); takes time, unsafe =>
Use of **leased lines**, but are expensive!

Digital telephony – all signals and equipment are digital => big digital telecommunication networks, with high speed and great reliability

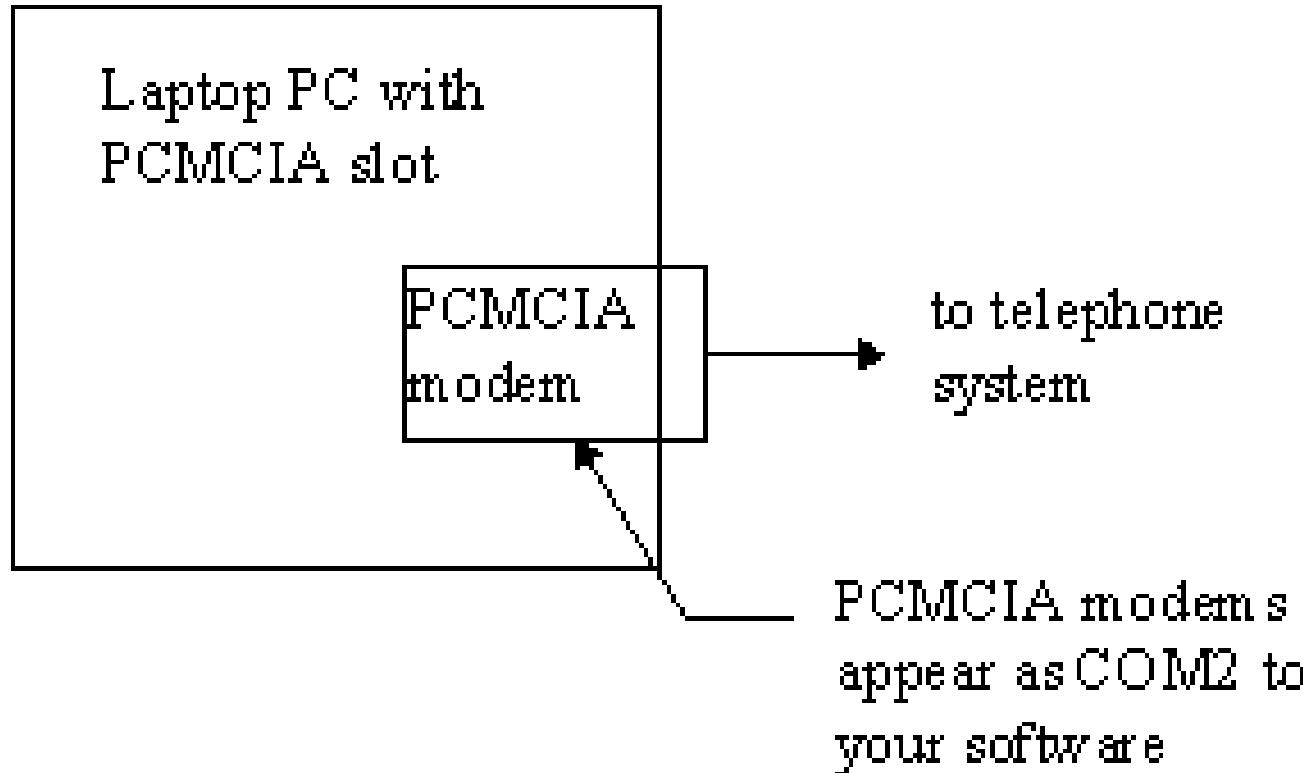
Still remains (yet) analog the **local loop**, connecting the subscriber to Telecom office
All DTEs use for connecting to telephone line (either analog or digital) the **serial interface**, so for the PCs the COM ports will be used.

For PCs the modem may be external or internal, today's internal.

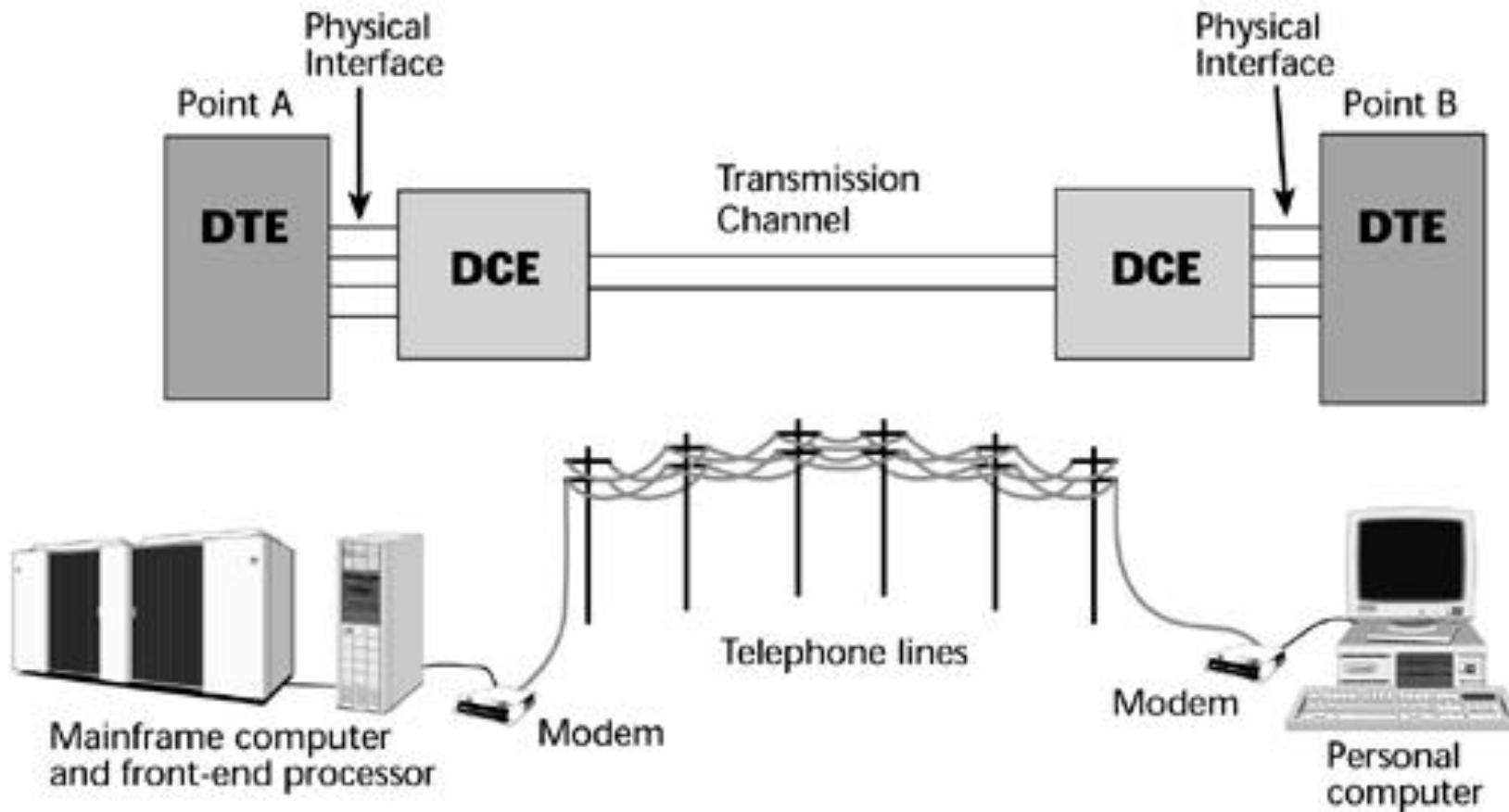
Internal view of a PC with internal modem



For your Laptop with interface adapter PCMCIA slot:



- In OSI terminology, communications interface act where data processing terminals (computers, hosts, terminals, printers) connect to the transmission system, i.e. where is the ‘end system to the network’ (data-circuit terminating equipment).
- Communications interface contains : DTE, DCE & interchange circuits.



Physical layer protocols describe this interface, in many aspects:

- electrical (voltages, currents, encoding techniques)
- electromechanical (connectors, pins location)
- functional (what circuits belongs to what pins & what signals on them mean: data, control, timing, grounding)
- procedural aspects (sequence of events, ex.: protocol of using the standard for answering calls...)

Physical aspects of connecting a DTE to a DCE – object of many standards:

EIA RS 232 (RS 232-D, from 1986, now RS 232-E, from 1991)

equivalent to ITU-T/CCITT V.24; V28 & ISO 2110

RS-449, followed by RS-530

Useful link for all kind of serial interfaces: www.arcelect.com

RS232 Serial Interface

Basics

- initial variant 232C, followed by D & E variants, improving performances and maintaining compatibility
- governs interface of DTE (computer) to DCE (modem)
- serial connection, up to 20kbaud over 15-16 m maximum (RS232C); further, data speed improved to 50kbps (versions D & E)
- originally developed for dumb terminals to modems
- good noise immunity
- handshaking not used consistently
- very cheap, single asynchronous chip
- unbalanced interface for control & data (common reference ground)
- wiring isn't set up to connect two DTEs together => use of null modem to cross several wires
- initial asynchronous, now providing synchronous capabilities

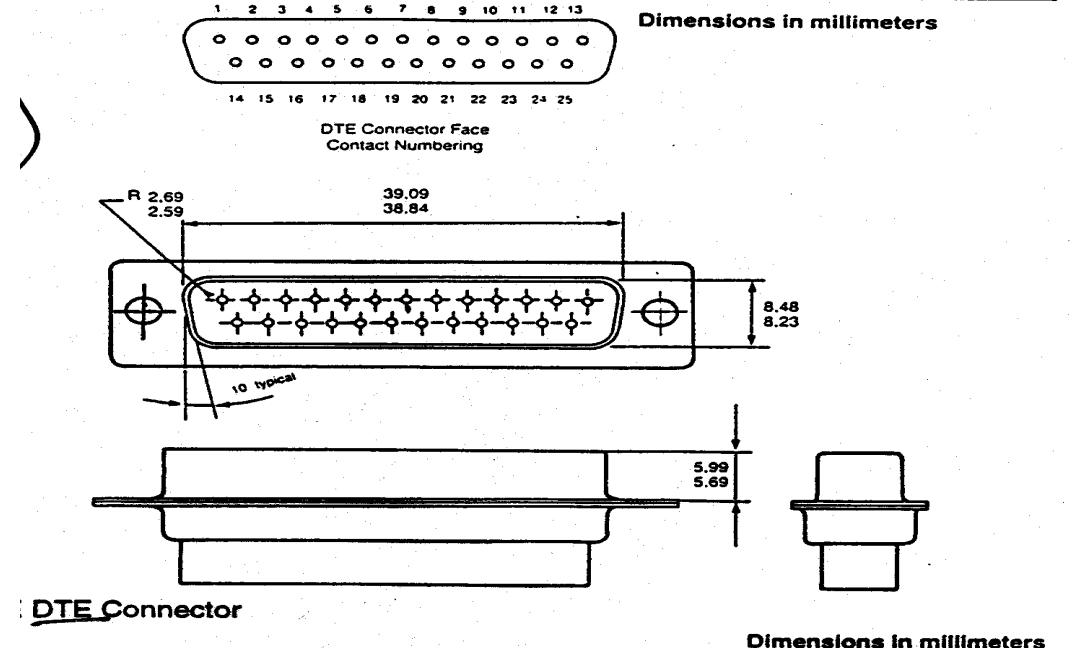
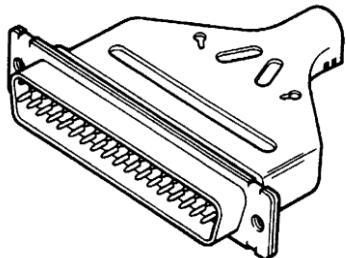
Electrical Specifications

Logic data representation by voltage transitions of min. 6V (both for data and control)

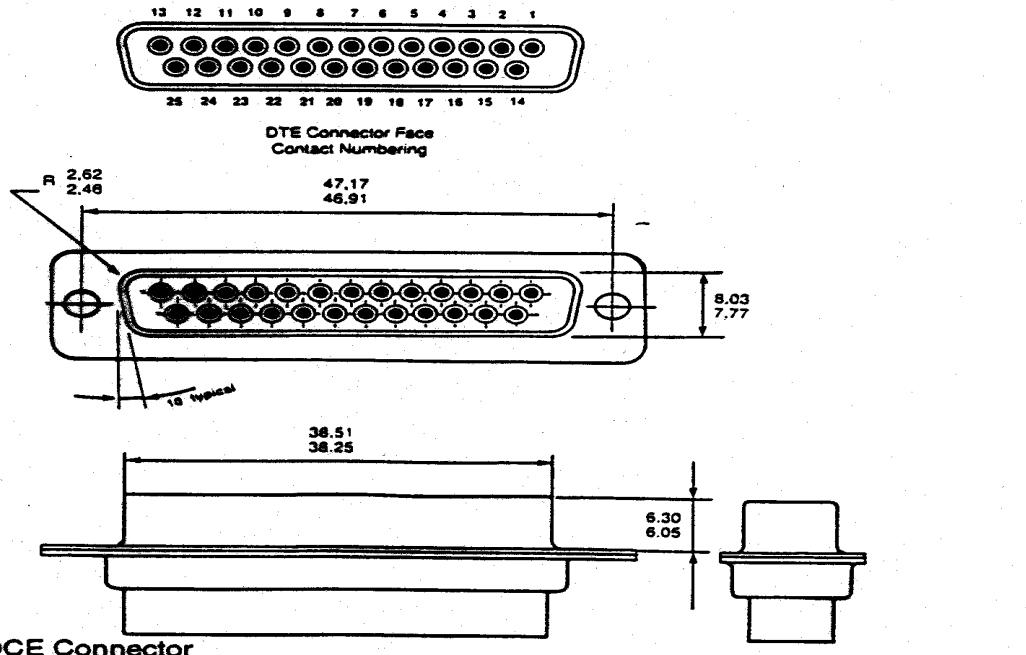
off = 0 (+3 to +15V) **on = 1 (-3 to -15V)**

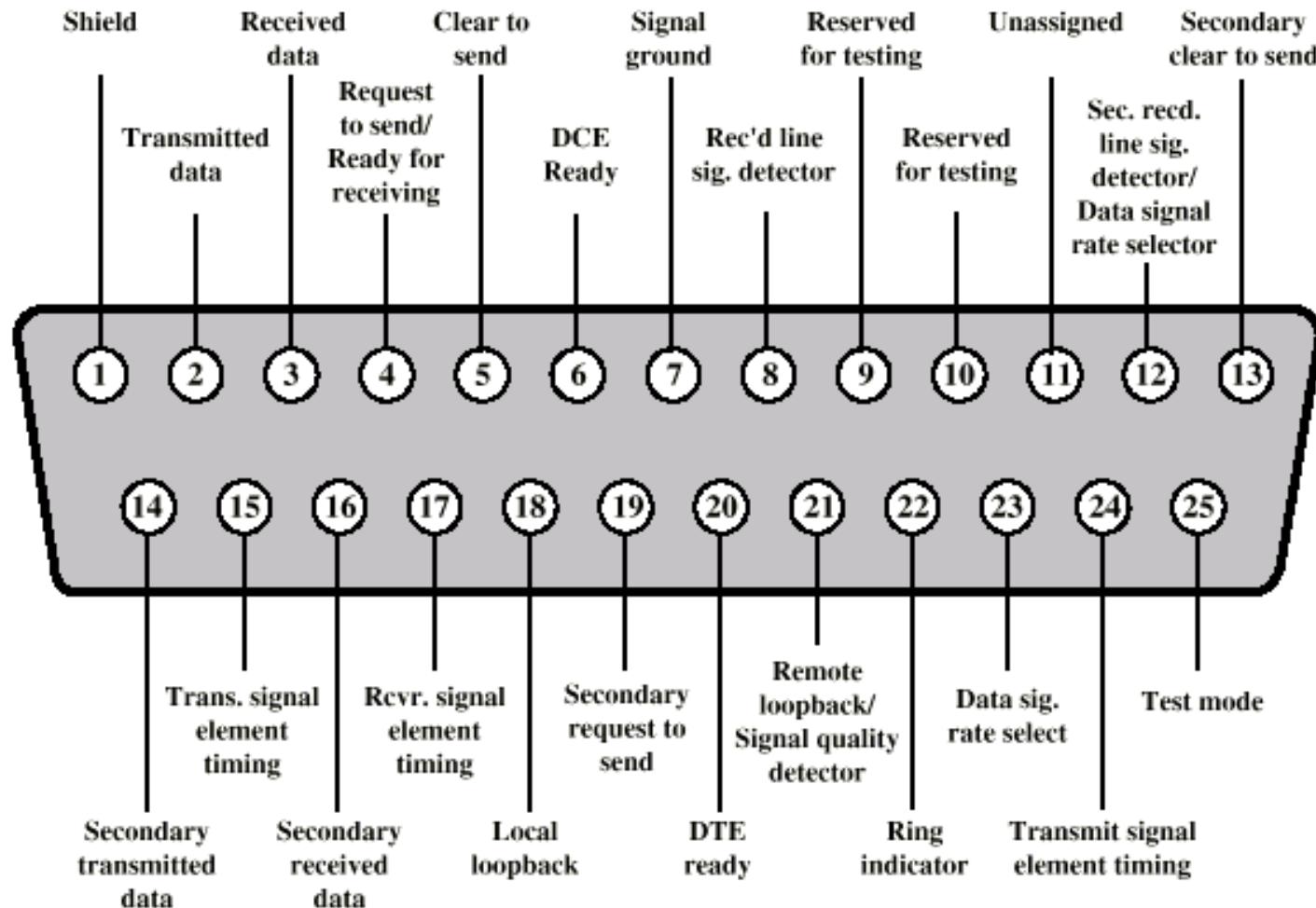
Mechanical Specifications

- connector male/female with 25 pins, 'D' shape, one 12 pins row, other with 13pins
- male connector on DTE, female connector on DCE
- mechanical specifications include: total connector's width, distance between successive pins, between pins rows, etc.



Dimensions in millimeters





Pin Assignments for V.24/EIA-232 (DTE Connector Face)

<u>Signal</u>	<u>Direction</u>	<u>Signal Name</u>	<u>Signal Name</u>	<u>Direction</u>
			Protective Ground	Both
To DCE		Secondary Transmitted Data	Transmitted Data	To DCE
To DTE		Transmit Clock	Received Data	To DTE
To DTE		Secondary Received Data		
To DTE		Receiver Clock		
		Unassigned		
To DCE		Secondary Request to Send	Request to Send	To DCE
To DCE		Data Terminal Ready	Clear to Send	To DTE
To DTE		Signal Quality Detect	Data Set Ready	To DTE
To DTE		Ring Indicate	Signal Ground	Both
Both		Data Rate Select	Carrier Detect	To DTE
To DCE		Transmit Clock	Reserved	
		Unassigned	Reserved	
			Secondary Carrier Detect	To DTE
			Secondary Clear to Send	To DTE

Functional Specifications

Functional Specifications

Define which circuits connect to each of the 25 pins (see previous slide)

9 typically used pins:

- 20: *Data Terminal Ready* (DTE to DCE): tells that DTE is powered up and ready
- 6: *Data Set Ready* (DCE to DTE): tells DTE that DCE is powered up and ready
- 8: *Carrier Detect* (DCE to DTE): tells DTE that it detects a carrier on the line
- 4: *Request to Send* (DTE to DCE): tells DCE it wants to send data (usually for half duplex)
- 5: *Clear to Send* (DCE to DTE): tells DTE that it can accept data, usually for half duplex
- 2: *Transmit* (DTE to DCE): sends data to DCE for it to transmit
- 3: *Receive* (DCE to DTE): sends received data to DTE
- 1: *Protective ground* (for safety)
- 7: *Signal Ground/Common Return* (reference voltage for detecting signal levels)

Some PCs use 9 pins connectors; pin assignment is shown in the following table.

Procedural Specifications

Gives the communication rules or how's the understanding between DTE – DCE, and between pairs.

Sample example: an asynchronous private line modem:

When turned-on and ready, modem (DCE) asserts *Data Set Ready*

When DTE ready to send data, it asserts *Request to Send*

Also inhibits receive mode in half duplex

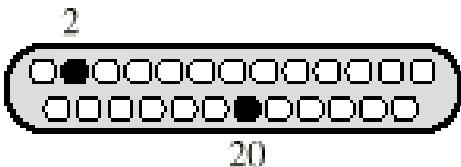
Modem responds when ready by asserting *Clear to Send*

DTE sends data

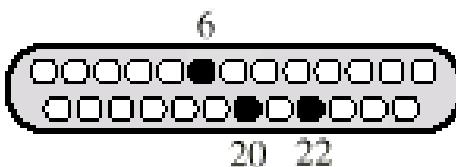
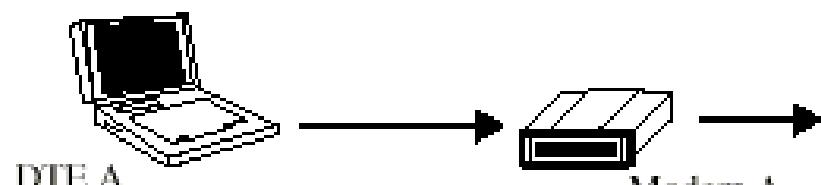
When data arrives, local modem asserts *Receive Line Signal Detector* and delivers data

9 pin	Signal	25 pins
1	Carrier Detect	8
2	Received Data	3
3	Transmitted Data	2
4	Data Terminal Ready	20
5	Signal Ground	7
6	Data Set Ready	6
7	Request To Send	4
8	Clear To Send	5
9	Ring Indicator	22

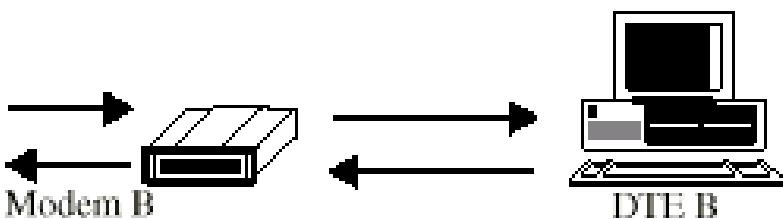
Dial Up Operation



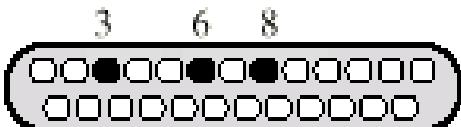
1. DTE A turns on the DTE ready pin (20) to tell its modem it wants to begin a data exchange. While this signal remains asserted, DTE A transmits a phone number via Transmitted Data (pin 2) for modem A to dial.



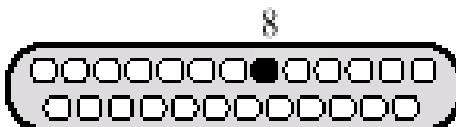
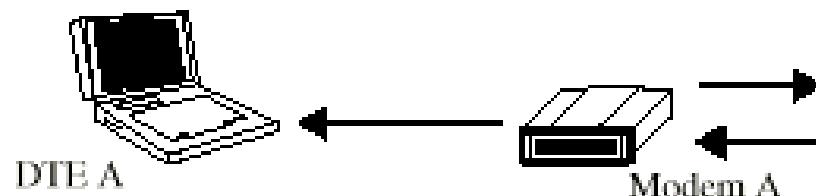
2. When modem B alerts its DTE to the incoming call via the Ring Indicator pin (22), DTE B turns on its DTE Ready pin (20). Modem B then generates a carrier signal, to be used in the exchange, and turns on pin 6, to show its readiness to receive data.



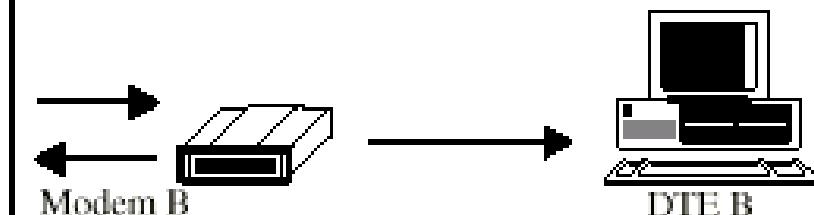
Dial Up Operation – cont.



3. When modem A detects a carrier signal, it alerts DTE A via pin 8. The modem also tells the DTE that a circuit has been established (pin 6). If the modem has been so programmed, it will also send an "on line" message to the DTE's screen via the Received Data pin (3).

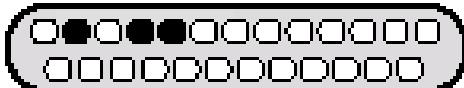


4. Modem A then generates its own carrier signal to modem B, which reports it via pin 8.

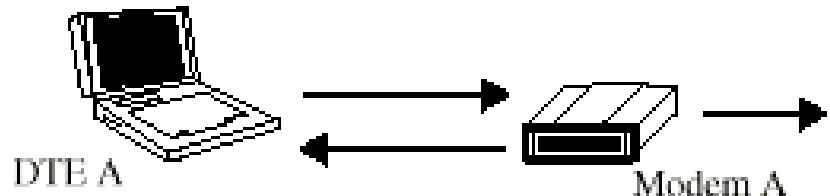


Dial Up Operation –cont.

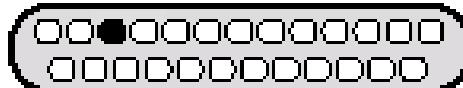
2 4 5



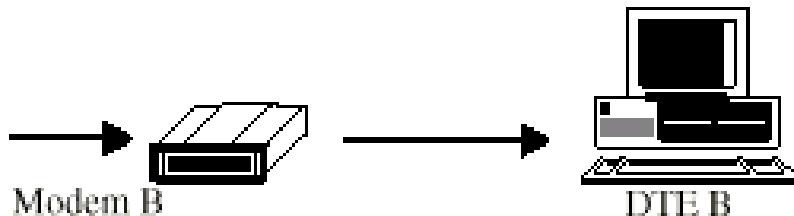
5. When it wishes to send data, DTE A activates Request to Send (pin 4). Modem A responds with Clear to Send (pin 5). DTE A sends data (pulses representing 1s and 0s) to modem A via the Transmitted Data pin (2). Modem A modulates the pulses to send the data over its analog carrier signal.



3

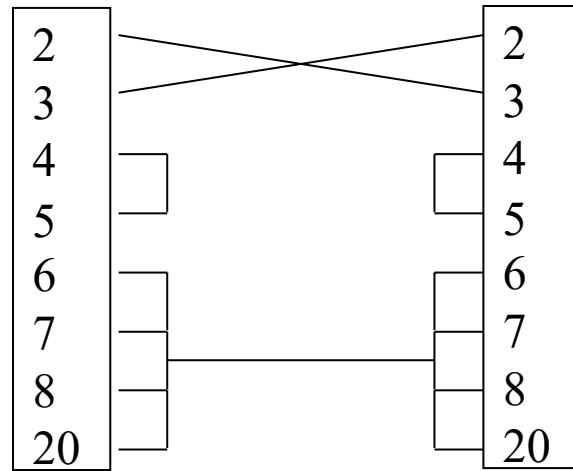


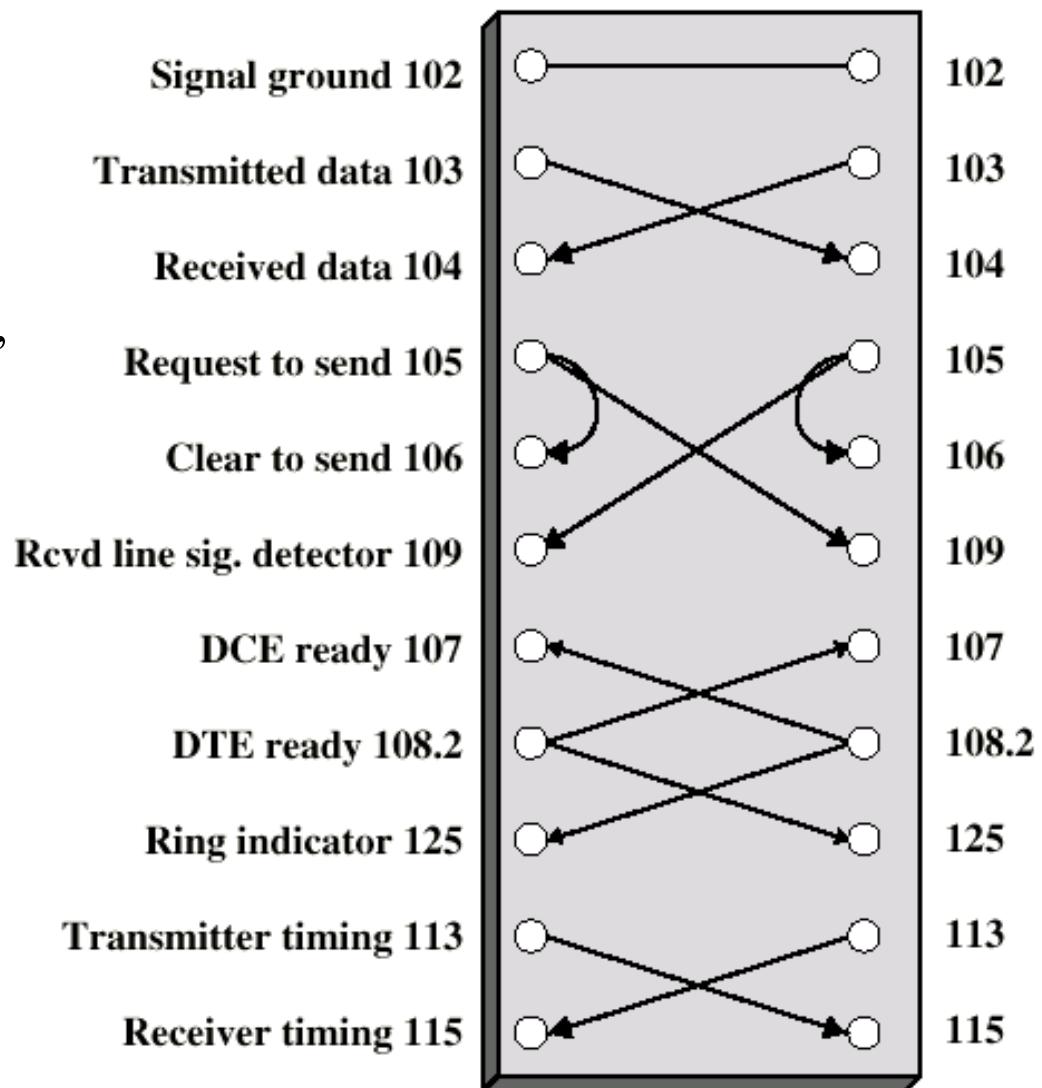
6. Modem B reconverts the signal to digital form and sends it to DTE B via the Received Data pin (3).



The wiring isn't set up to connect two DTEs together => use of **null modem** to cross several wires. Simplest case, the 3 wires short cable null modem, with the following architecture:

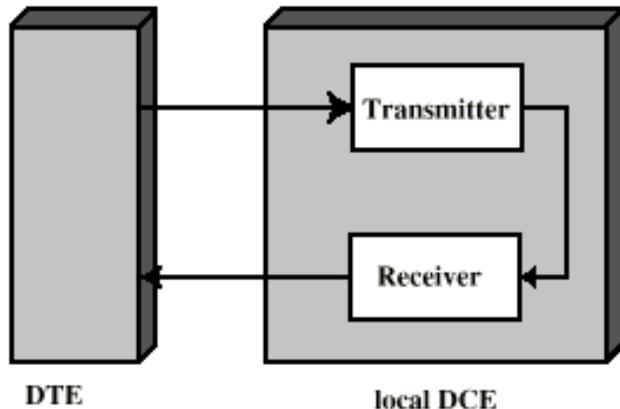
- Transmitted Data
- Received Data
- Request To Send
- Clear To Send
- Data Set Ready
- Signal Ground
- Data Carrier Detect
- Data Terminal Ready



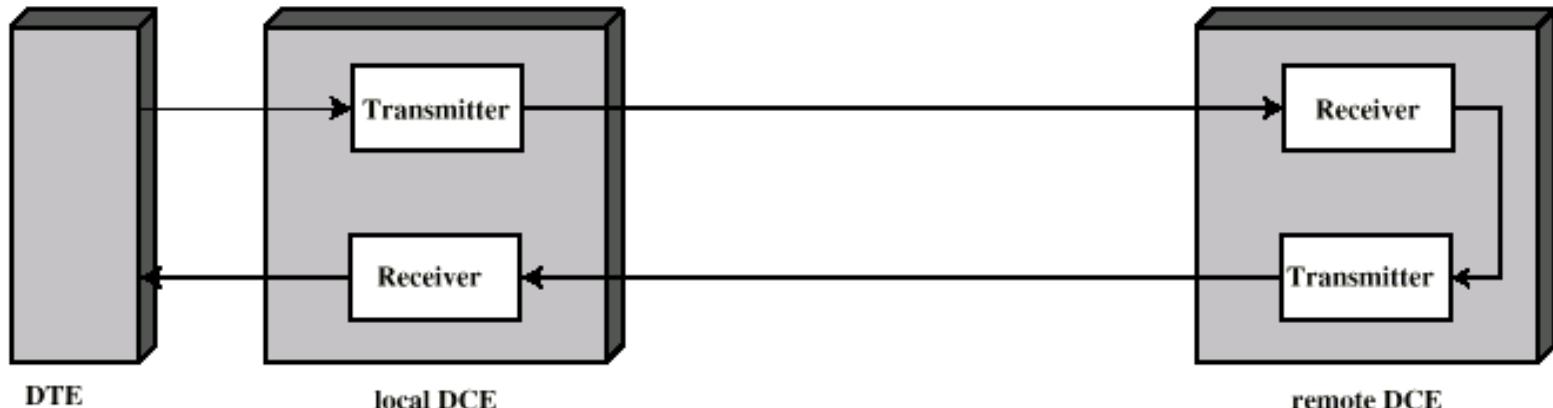


Other example of null modem,
with more wires, same effect!

For testing the serial interface (COM port), two simple tests:



(a) Local loopback Testing



(b) Remote loopback Testing

RS 449 Standard

Dates from '80s, improving the RS-232 standard, overcoming the defects.

Offers backward compatibility – very important, due to RS-232 huge usage => RS-232 can be emulated by changing various connections.

Consists in fact of three standards:

Basic RS-449, giving mechanical, functional & procedural interfaces

Electric interface given by two standards:

RS-423A, similar with RS-232, using **unbalanced** transmission
(an unique return path for all signals)

RS-422A, assigns to each signal its own grounding (or, other, for each signal is provided individual return path, isolated from other grounds); so defines a **balanced** transmission.

Gives greater DTE control over DCE, but still not exist autodialing.

Mechanical connectors: 37 pins + an additional 9 pins, if secondary channel used.

Provides synchronous & asynchronous transmissions

Offers 10Mbps for a distance of max. 12m, and 100kbps for hundreds of meters, when using RS-422A, and 3kbps @ 100m or 30kbps @ 10m length, for RS-423A. Circuit description follows; remark that there are new circuits, like those used for testing!

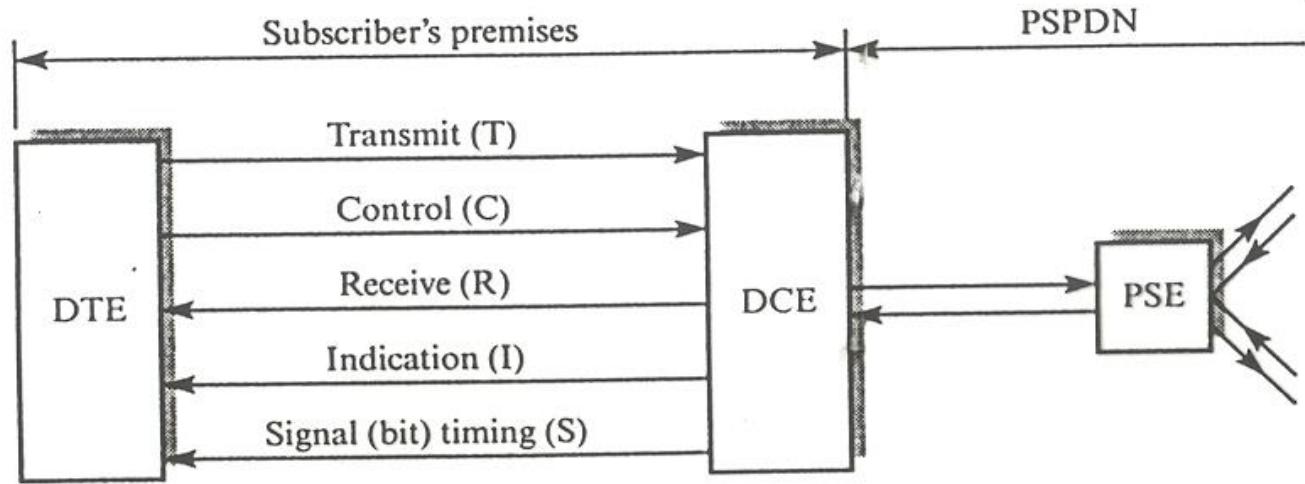
Future developments: **RS-530**, using balanced transmission, speed up to 2Mbps.

Mnemonics	Circuit Description	Mnemonics	Circuit Description
SG	Signal Ground	SC	Send Common
RC	Receive Common	IS	Terminal in Service
IC	Incoming Call	TR	Terminal Ready
DM	Data Mode	SD	Send Data
RD	Receive Data	TT	Terminal Timing
ST	Send Timing	RT	Receive Timing
RS	Request to Send	CS	Clear to Send
RR	Receiver Ready	SQ	Signal Quality
NS	New Signal	SF	Select Frequency
SR	Signaling Rate Selector	SI	Signaling Rate Indicator
SSD	Secondary Send Data	SRD	Secondary Receive Data
SRS	Secondary Request to Send	SCS	Secondary Clear to Send
SRR	Secondary Receiver Ready	LL	Local Loopback
RL	Remote Loopback	TM	Test Mode
SS	Select Standby	SB	Standby Indicator

X21 Digital interface

CCITT standard for direct digital connections to the digital telephone network.
Uses only 8 signal lines, on a 15 pin connector, allowing use of 2 channels (A, B)
Data rate from 9600bps up to 64kbps
Use of more logic, instead of more signals (RS-449)
Allows bit and byte synchronization
X21bis standard allows analog signalling (is a subset of RS-232D), developed for backward compatibility (use of analog telephone networks)
DCE provides a full-duplex, bit-serial, synchronous transmission path between the DTE and the local PSE.

Trend continued with 8-pins physical connector for **ISDN** (Integrated Services Digital Network)



Pin assignment
and functional
characteristics:

TRANSMIT B 9
CONTROL B 10
RECEIVE B 11
INDICATION B 12
SIGNAL TIMING B 13
14
15



1 FRAME GROUND
2 TRANSMIT - A
3 CONTROL - A
4 RECEIVE - A
5 INDICATION - A
6 SIGNAL TIMING - A
7
8 SIGNAL GROUND

Functional characteristics of interchange circuits.

Interchange		Direction	
Circuits	DB15	Name	
		To DCE	From DCE
G	1	Signal ground or common return.	
Ga	8	DTE common return	X
T	2 & 9	Transmit	X
R	4 & 11	Receive	X
C	3 & 10	Control	X
I	5 & 12	Indication	X
S	6 & 13	Signal element timing	X
B		Byte timing	X
X		DTE signal element timing	X

Signal Specification

Signal Ground (G): protective ground (earth).

DTE Common Return (Guard) – for the unbalanced mode, gives reference ground for receivers in the DCE interface

Transmit (T) - carry data and control from the DTE to the DCE

Receive (R) - from DCE, indicates to the DTE the type of data

Indication (I) –controlled by DTE, indicates to the DCE the meaning of the data sent on the transmit circuit

Byte Timing (B) - provides the DTE with 8-bit byte element timing

Signal Element Timing (S) - provides the DTE or DCE with timing information for sampling the Receive line or Transmit line

Control line (C) – to DCE circuit, for extra control of DTE over DCE.

ISDN Physical Interface

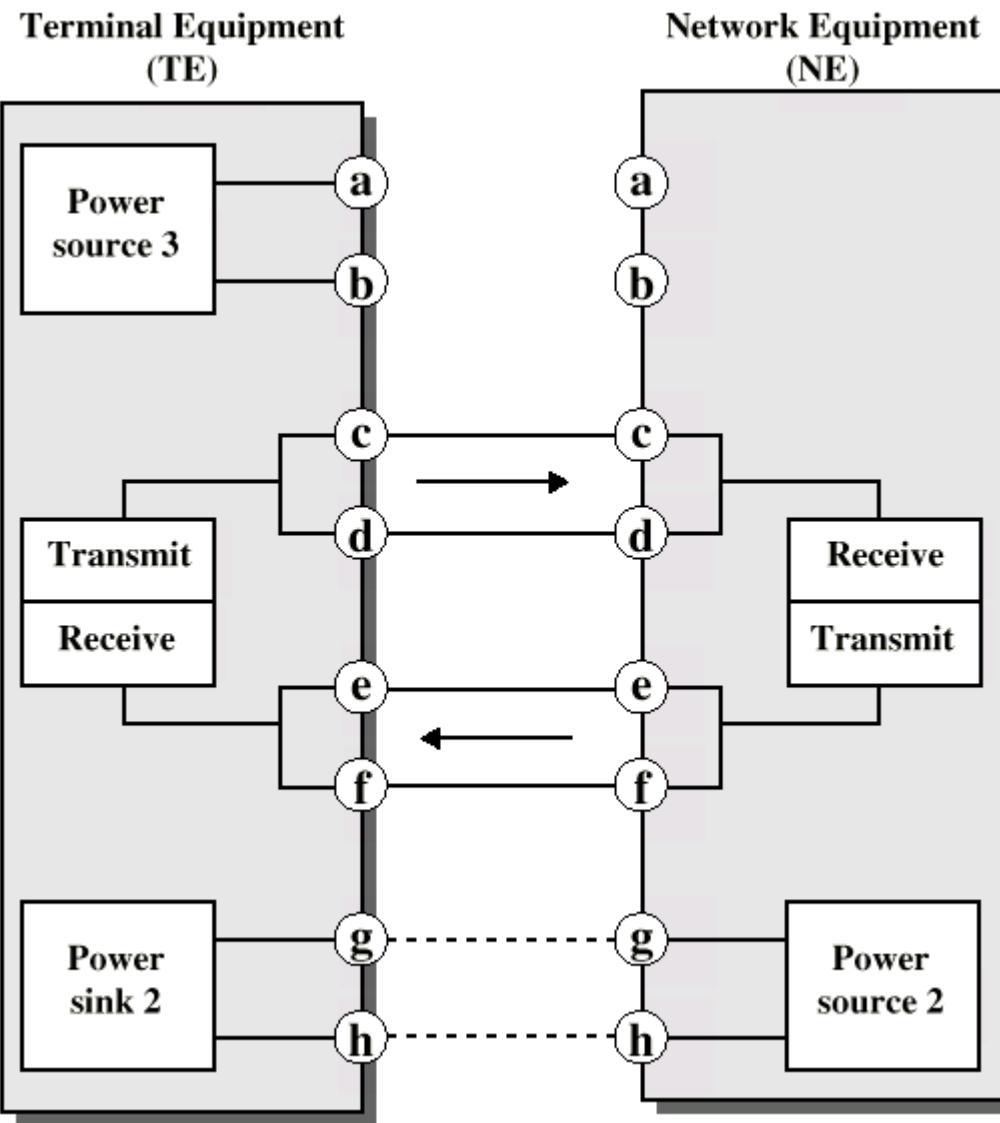
Further evolution of X21 was the specification of the ISDN physical connection

Connection between **terminal equipment TE** (c.f. DTE) and **network terminating equipment NE** (c.f. DCE)

ISO 8877

Cables terminate in matching connectors with 8 contacts

Transmit/receive lines carry both data and control



ISDN Electrical Specification

Balanced transmission

Signals carried on a channel made by two conductors, e.g. twisted pair

Signals (as currents) travel down one conductor and up the other (return way)

Differential signaling, as binary value depends on the voltage difference between lines (value depends on direction of voltage); usual differences under 1V => low power circuitry

Tolerates more noise and generates less than unbalanced transmissions, because noise affects both lines, not their voltage difference

(Unbalanced, e.g. RS-232, uses single signal line and a (common) ground)

Data encoding depends on the data rate

Basic rate 192kbps uses pseudoternary

Primary rate uses alternative mark inversion (AMI) and B8ZS or HDB3

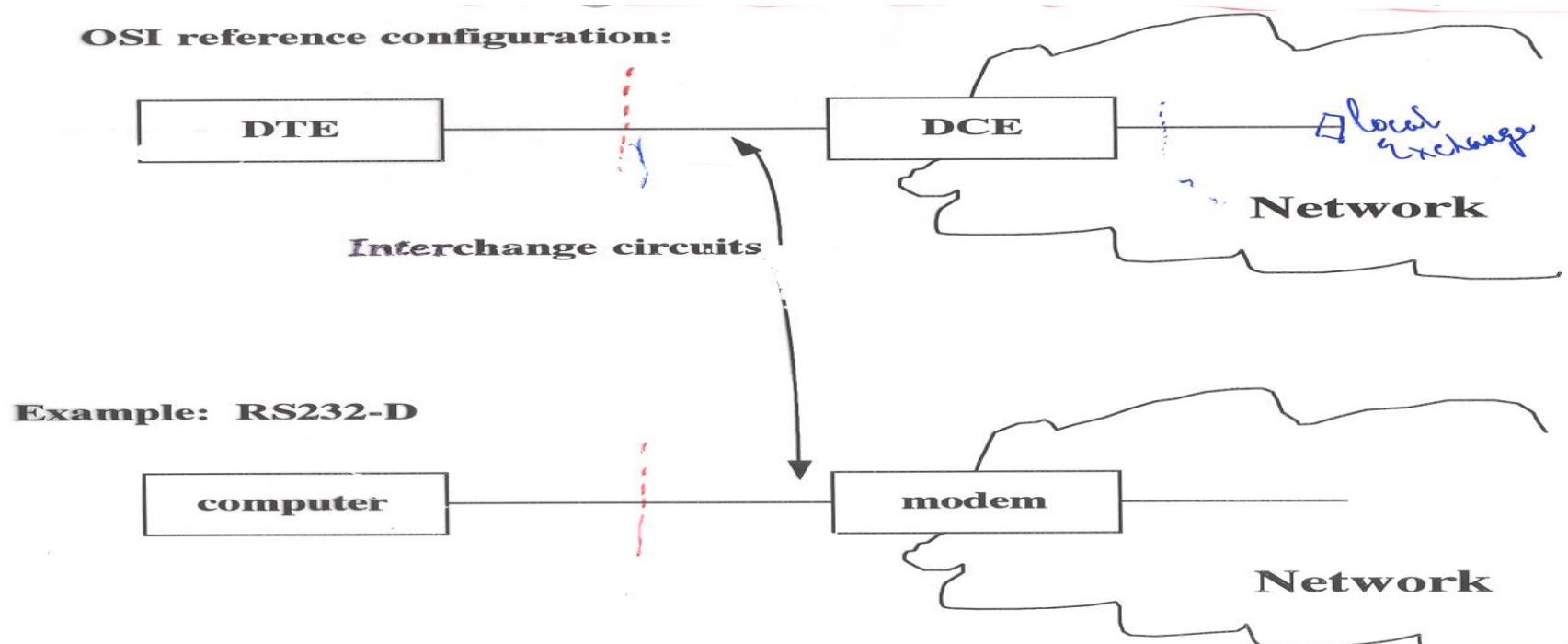
Modem

Standard modem definition:

The **modem** is the interface between a DTE (like a PC) that generates digital signals, and the telephone system that carries analog signals.

Modems encode digital signals onto analog signals by modulating an analog signal by changing the phase, frequency or amplitude of the signal, to represent 1s and 0s. The method of modulation defines the *modem standard*.

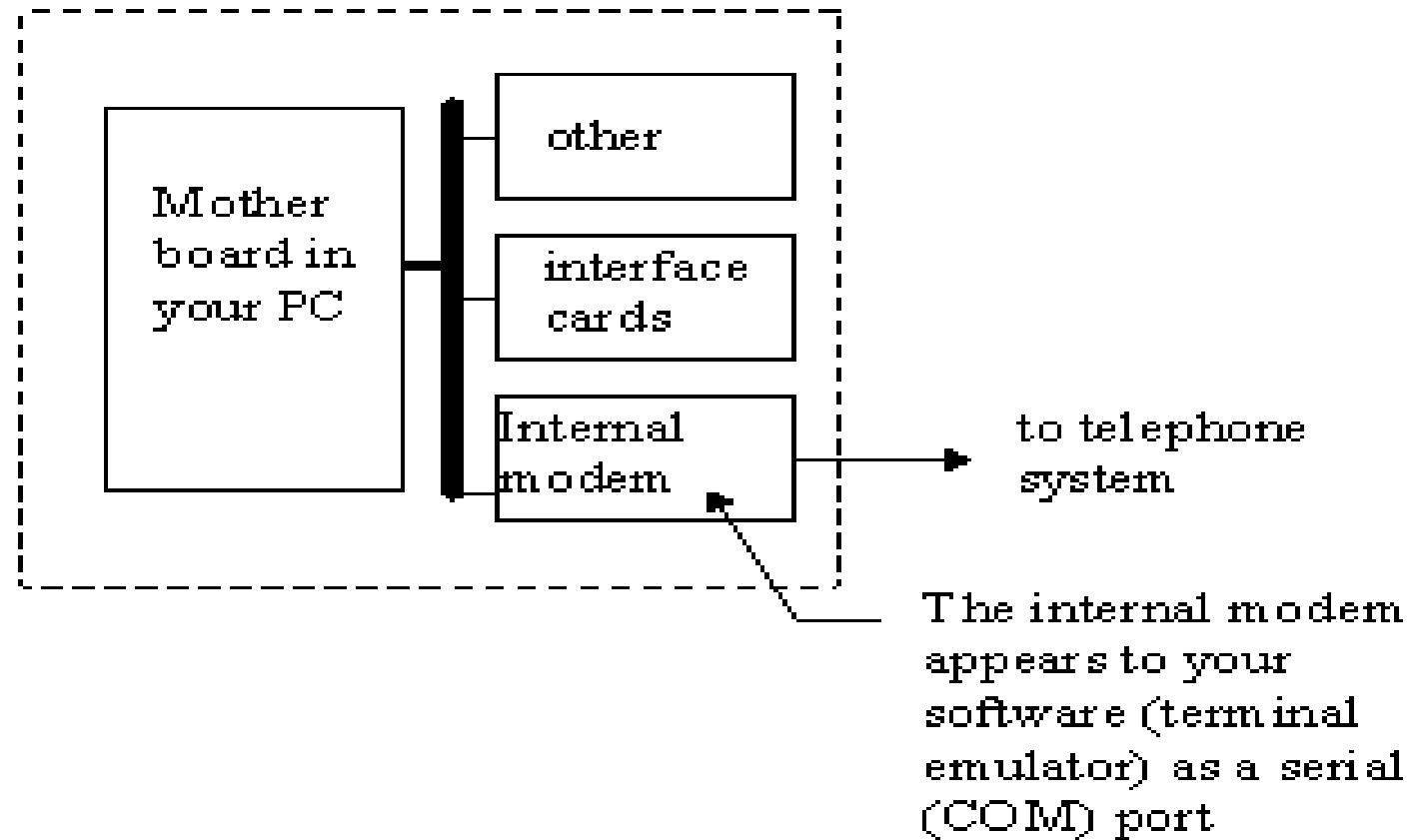
The modem receives signals from the interchange circuits, respecting the serial interface standards.



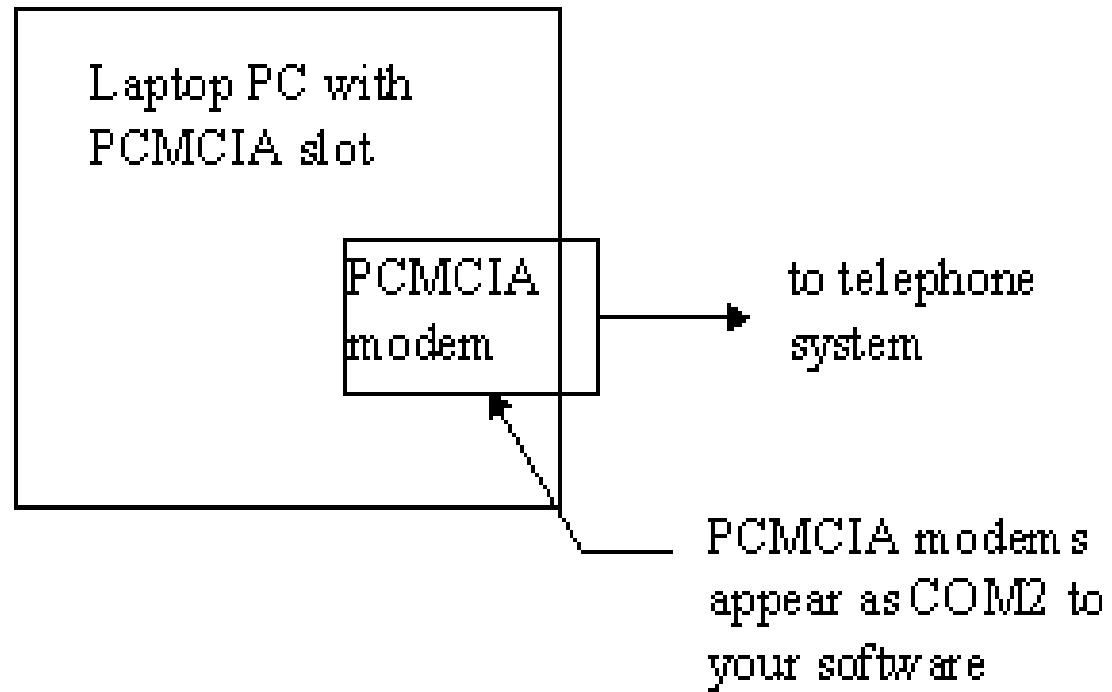
For PCs the modem may be *external* or *internal*, today's mostly internal.

Even if using an internal modem, these serial interface's signals are generated by the serial interface in the modem and are recognized by the terminal emulation software.

Internal view of a PC with internal modem



For your Laptop with interface adapter PCMCIA slot the modem appears like:



A PCMCIA modem being inserted into a laptop computer. Attached to the card is an adaptor which connects the card to a standard RJ-11 telephone line

Modem standards issued by:

- Bell standards (old standards), ITU-T (former CCITT) recommendations, concerning modulation and coding techniques
- EIA/TIA, ITU-T for interfaces

Categories of modems: (see table on next slide)

- operating speed** –low, medium & high speed
- implemented standard**
- type of transmission** (asynchronous, synchronous)
- type of modulation** (FSK, PSK, QAM)
- type of telephonic lines** (dial-up or leased)
- complexity** (traditional or smart)
- other modems** (ISDN modems, coax cable modems, LAN modems, wireless and cellular modems)

Data rate	Standard Body	Line Type	Modulation Technique	Transmission Type	Duplex Full/Half
300	Bell 103, CCITT V21	Dial-up	FSK	Asynchronous	Half+Full
600	CCITT V22	Dial-up/leased	PSK	Asynchronous	Half+Full
1200	Bell 202, CCITT V22	Dial-up/leased	PSK	Asynch/Synch	Half+Full
2400	CCITT V22bis	Leased	QAM	Asynchronous	Half+Full
4800	CCITT V27	Leased	PSK	Synchronous	Half+Full
9600	Bell 209, CCITT V32	Dial-up/leased	QAM	Asynch/Synch	Half+Full
14400	CCITT V32bis	Dial-up/leased	QAM	Asynch/Synch	Half+Full
33600	CCITT V34	Dial-up/leased	PSK	Asynch/Synch	Full
56600	CCITT V90	Dial-up/leased	QAM	Asynchronous	Full

Low speed modems

First modem operated at 300 Bauds, cf. to Bell 103A standard (repeated by CCITT V21).

A modem could be (vis-a-vis a transmission):

- transmission originate
- transmission answer

Used 2 audio frequencies, one for sending and one for receiving.

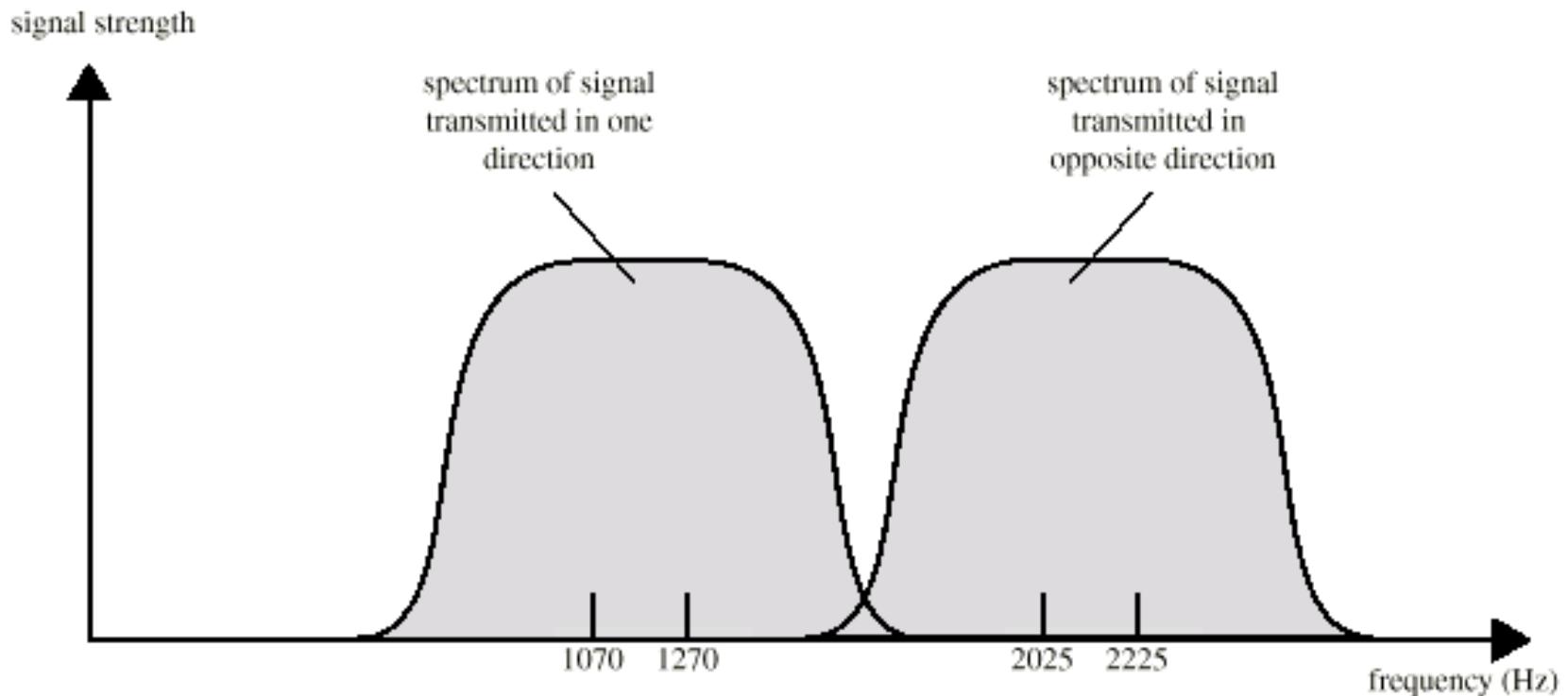
Ex. For Bell 103:

1070-1270 Hz being the frequency band for originate modem data transmission and receiving band for the answering modem

2025-2225 Hz, reception band for originate modem and emission band for answering modem.

For CCITT V21 the similar frequency bands are 980-1180 Hz and 1650-1850Hz respectively.

For this low speed ‘old’ modem, the interface signal set comprises the following signals: RTS, CTS, DSR, DTR, DCD, RI (see RS232 signal table).



Full-Duplex FSK Transmission on a Voice-Grade Line

Smartmodems (Hayes compatible)

Cf. RS232-C data and control lines are separated. Smartmodems ‘understand’ commands and status information using characters, so no more signal separation..

Modem Commands (Hayes-compatible modem)

These are commands (character strings) that the terminal emulator can send to the modem to instruct it to perform operations, such as automatic dial. Interface signal set comprises only the lines Tx (Transmit), Rx (Receive), and ground.

The modem is in one of the states:

- receive command from DTE
- on-line
- hang-up, or carrier-wait.

General format of the command:

AT *command*

Where *command* is a letter, followed (eventually) by a parameter.

The following are examples of a few of the AT (attention) commands:

ATDT n: Dial phone number <n>, using touch tone

ATDP n: Dial using pulse

ATH: Hangup

ATH1: Pick up the phone line

Introduction to: ISDN Modem

ISDN (Integrated Services Digital Network), offers services on a full digital network. ISDN modems, known as **TA** (Terminal Adapters).

An ISDN line is split in channels (see table):

B (Bearer) channel – carries (PCM coded digital) voice + data up to 64kbps

D (data signaling) channel – carries control for B channels; speed 16kbps or 64kbps

Usually B and D channels use separate paths, speeding up the transmissions

H (High speed) channel – data transport at speeds of Mbps

ITU-T defines two types of services:

BRI (Basic Rate Interface), operating at 192kbps, contains 2 B channels and one D channel at 16kbps (2B + D16)

PRI (Primary Rate Interface), signalling at 64kbps and operating at 1.544Mbps in US (23B + D64), or 2.048Mbps in Europe (30B + D64)

3/20/2024

Channel	Bit Rate	Interface
B	64kbps	Basic access
H0	384kbps	Primary rate access
H11	1536kbps	Primary rate access
H12	1920kbps	Primary rate access
D16	16kbps	Basic access
D64	64kbps	Primary rate access

Use of H channels instead of B (see table for more details):

Interface	Bit Rate	Interface Structure
Basic access	192 kbps	2B+D16
Primary rate access	1544 kbps	23B+D64 3H0+D64
	2048 kbps	30B+D64 5H0+D64 H12+D64

TA has similar functions as a normal modem, plus those for adapting the variable data rate of the DTE to the constant B channel data rate. Also transforms analog voice or fax data into digital. The commands for a TA have similar structure as for the smart Hayes modem (AT ... commands).

A little bit more about the physical level of ISDN:

ISDN: First important change from analog to digital telephony, from circuit switching telephony to packet switching based

Digital data exchanged between subscriber (user) and network terminal equipment (NTE) is Full Duplex => Separate physical line for each direction

Pseudoternary coding scheme: 1=no voltage, 0=positive or negative 750mV +/-10%

Basic rate: data rate of 192kbps, i.e. one 48 bit-long frame every 250 µs; **Basic access** uses synchronous TDM two 64kbps B channels and one 16kbps D channel (2B+D16) => This gives 144kbps multiplexed over 192kbps => Remaining capacity used for framing and synchronization.

Use of LAP-D frames (see the following data link protocol HDLC)

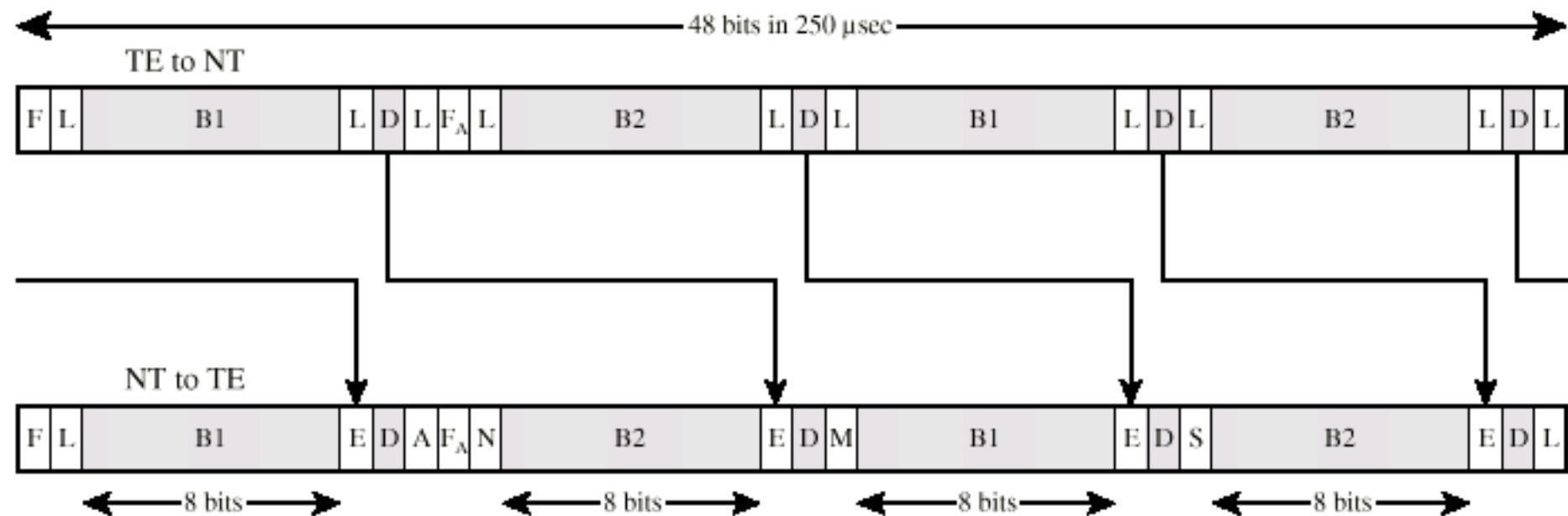
Two kind of frames: from/to subscriber to/from Terminal Equipment. Structure:

From 48 bit: 16bit for each of B channels and 4 bit for D channel.

F –framing bit (positive pulse, followed by a negative one L, for dc balance

F_A – auxiliary framing; E: D-echo channel bit (retransmission by NTE of the most received D bit; A: activation bit for NTE (allows low power-consumption mode)

ISDN LAP-D Frame Structure (basic access)



F = Framing bit

L = DC balancing bit

E = D-echo channel bit

A = Activation bit

F_A = Auxiliary framing bit

N = Set to opposite of F_A

M = Multiframing bit

B1 = B channel bits (16 per frame)

B2 = B channel bits (16 per frame)

D = D channel bits (4 per frame)

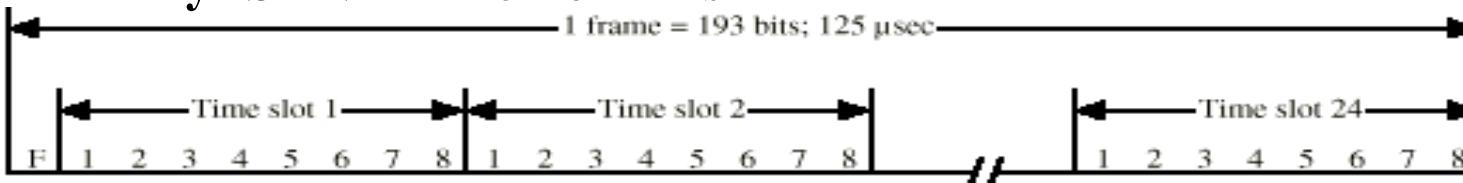
S = Spare bits

Primary ISDN Interface: synchronous TDM of multiple channels, allows point-to-point configurations; 2 data rates defined:

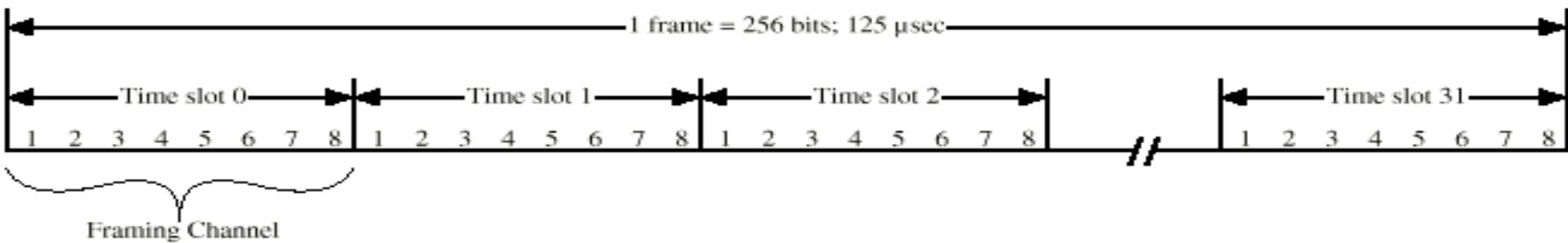
DS-1 of 1.544Mbps, based on T1 frame: 24×8 data bit + 1 framing, every 125 μ s; 8000 frames/sec \Rightarrow each channel supports 64kbps; implements 23B+D64; data encoding using AMI (alternate mark inversion) – B8ZS(bipolar-8 zeros substitution)

E1 frame, at 2.048Mbps for 30B+D64; one 256 bit frame every 125 μ s, 8000 frames/sec each channel supports 64kbps; first time slot for framing and synchronization; data coded using AMI – HDB3(high density bipolar 3zeros)

Primary ISDN Frame Formats



(a) Interface at 1.544 Mbps



(b) Interface at 2.048 Mbps

B-ISDN (Broadband ISDN)

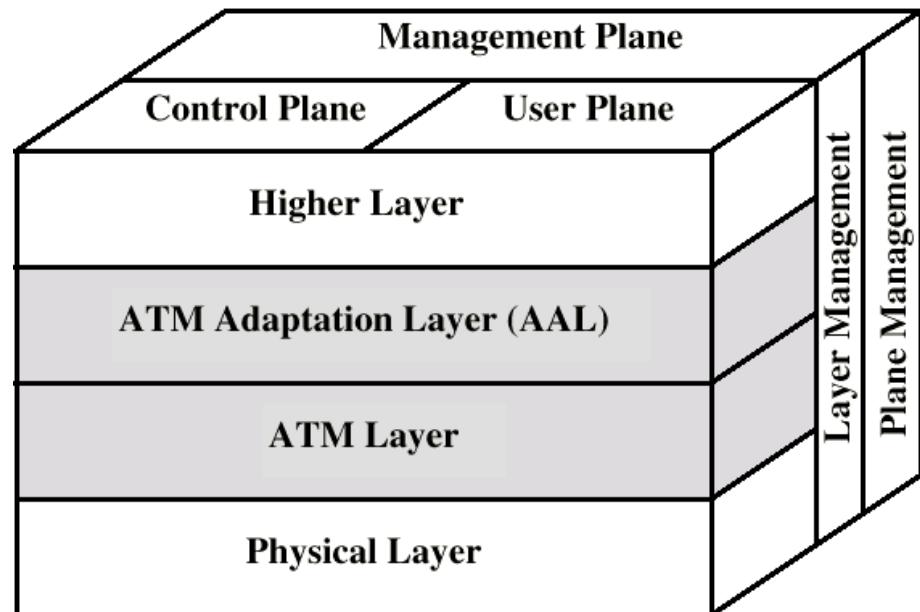
N-ISDN (Narrow – ISDN) deal with 64kbps channels (type B); with H type channels (actual H channel offers tens of Mbps) => development of B-ISDN, offering a transport of packets (cells) at a rate beginning with 155Mbps.

Transfer mode implementing B-ISDN (dealing with transmission and switching aspects) is the **ATM** (Asynchronous Transfer Mode).

The ATM transport unit is the **cell**, small packet of 53bytes, 5 octets for control and 48 bytes payload.

The protocol hierarchy of ATM is depicted below:

At the Physical level, the ATM technology is based on SONET and SDH standards.



Cable Modems

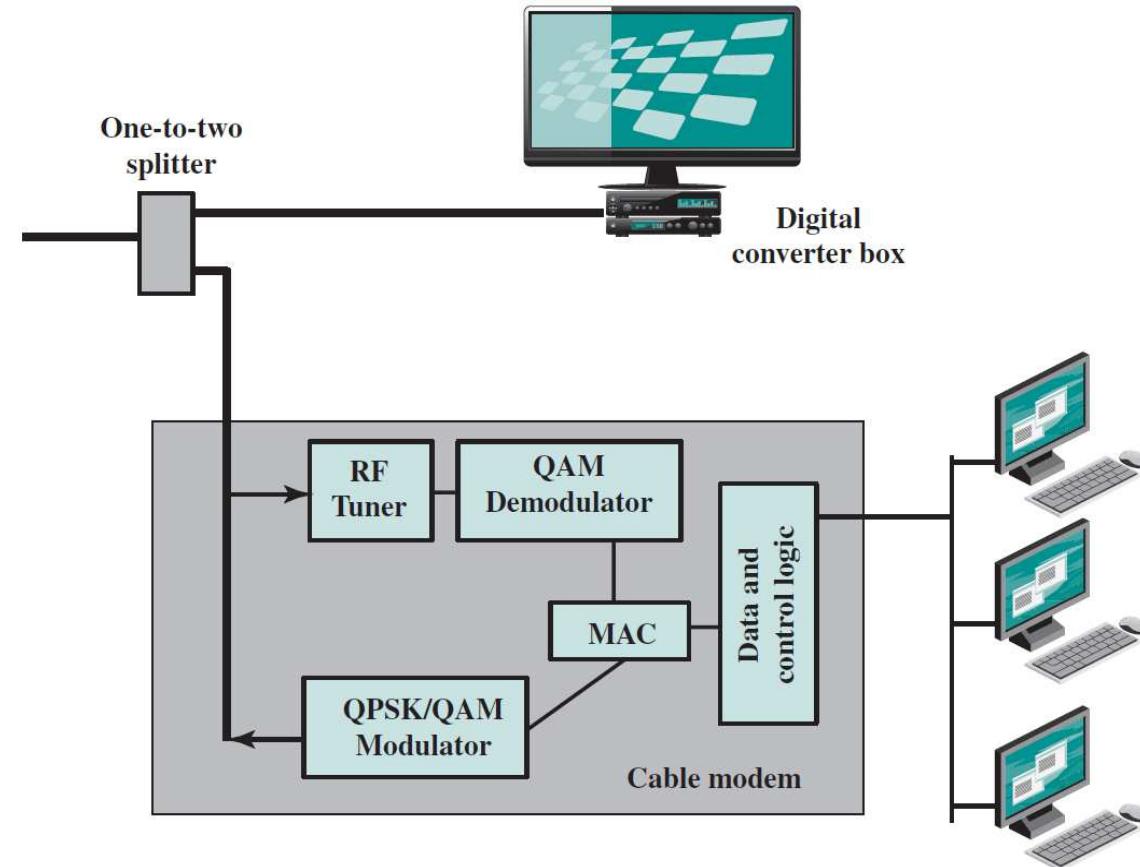
Devices allowing high-speed access to the Internet via a cable television network. Even similar with voice-band modems, more than 500 times faster. Voiceband modems operate up to 56kbps, cable modems deliver 30-40Mbps of data on a 6MHz TV channel
In a cable network:

- data from the network to the user: **downstream**
- data from the user to the network: **upstream**

Downstream and upstream bandwidths may be configured after application (domestic user - low upstream bandwidth, business office may require a higher upstream band)

Simple layout:

- one-to-two splitter for transmitting TV services to set top box, and for transmitting data through cable modem to the computer



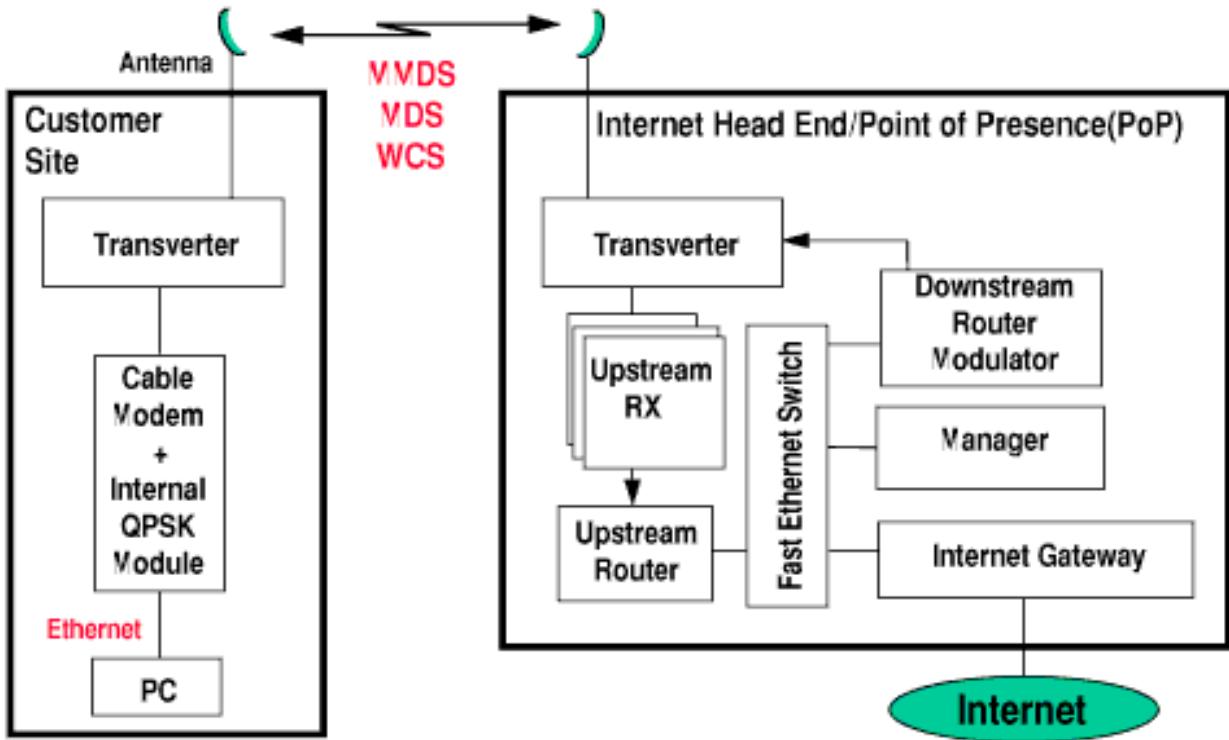
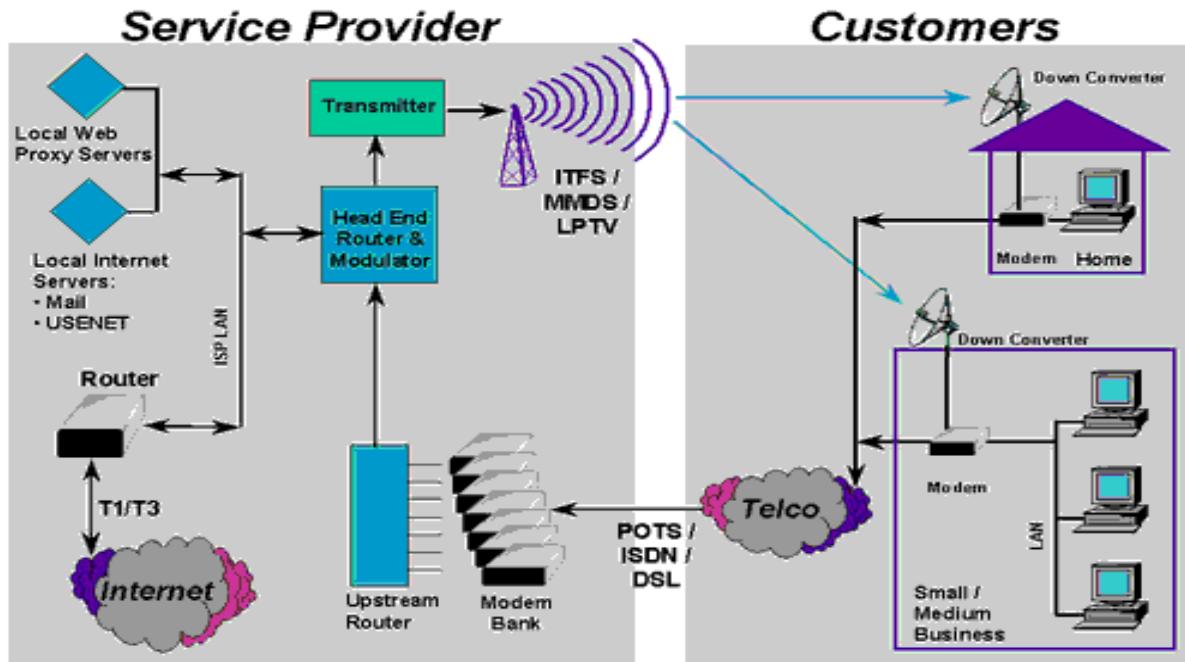
At the other end of the cable there is the head-end, may be a CATV provider or an ISP (Internet Service Provider), let's say a **head-end point-of-presence**, allowing, by use of a multiplexed network interface, the access to the Internet.

- User-to-network data (upstream): 5–40 MHz
- Television delivery (downstream): 50–550 MHz
- Network to user data (downstream): 550–750 MHz

The front of a cable modem showing its various indicators.

The back of a cable modem with standard coaxial television cable connector, telephone jacks and Ethernet jacks - connects the modem to a computer.





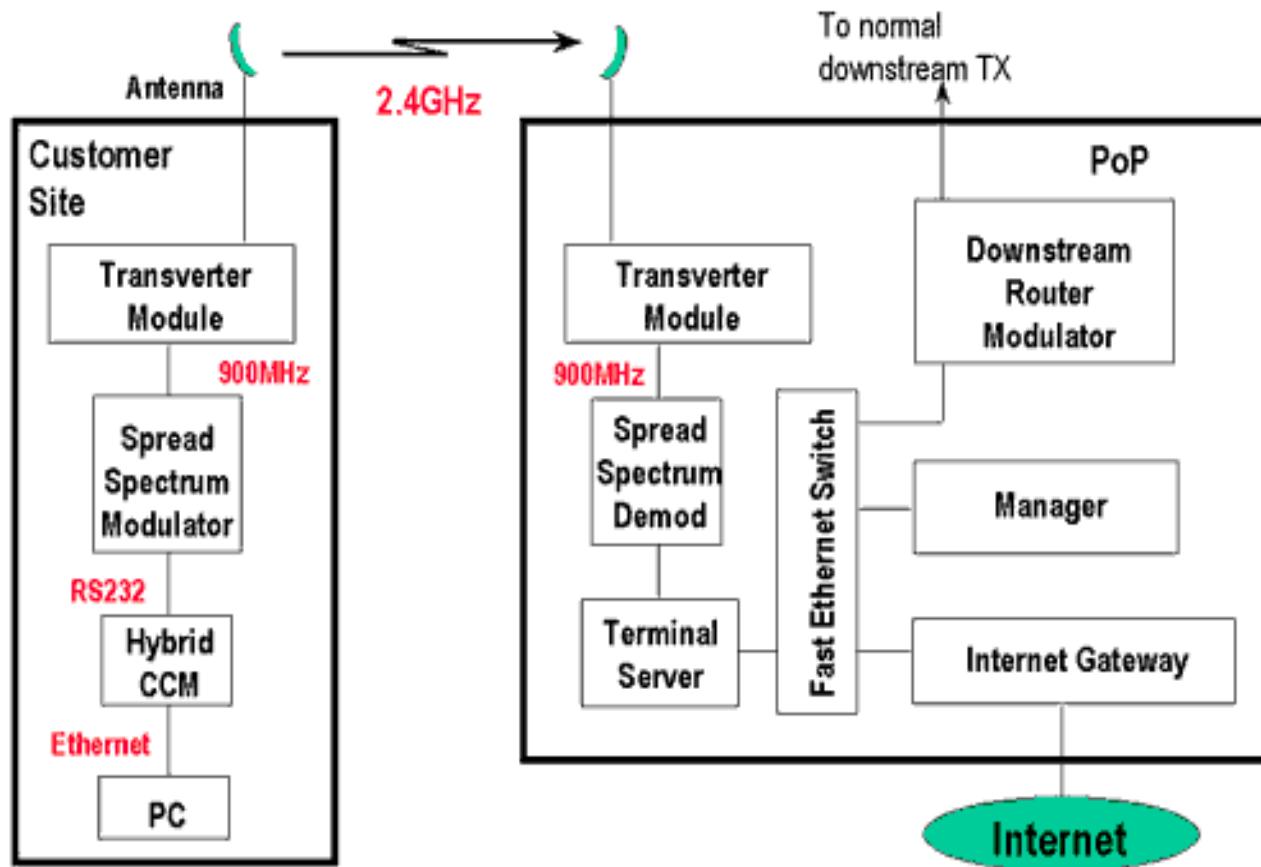
Other application with the downstream offered by CATV and upstream by cable modems.

Other application, with the use of the QPSK Signal from a Cable Modem and use of a transverter, for full wireless communications using CATC antennas.

Wireless modems

Many kinds of wireless modems:

- RF modem for a wireless network (use of ISM bands)
 - cellular modem for cellular communications, attached to the phone
- Example: use the ISM Band for Wireless Return 900 MHz/2.4 GHz:

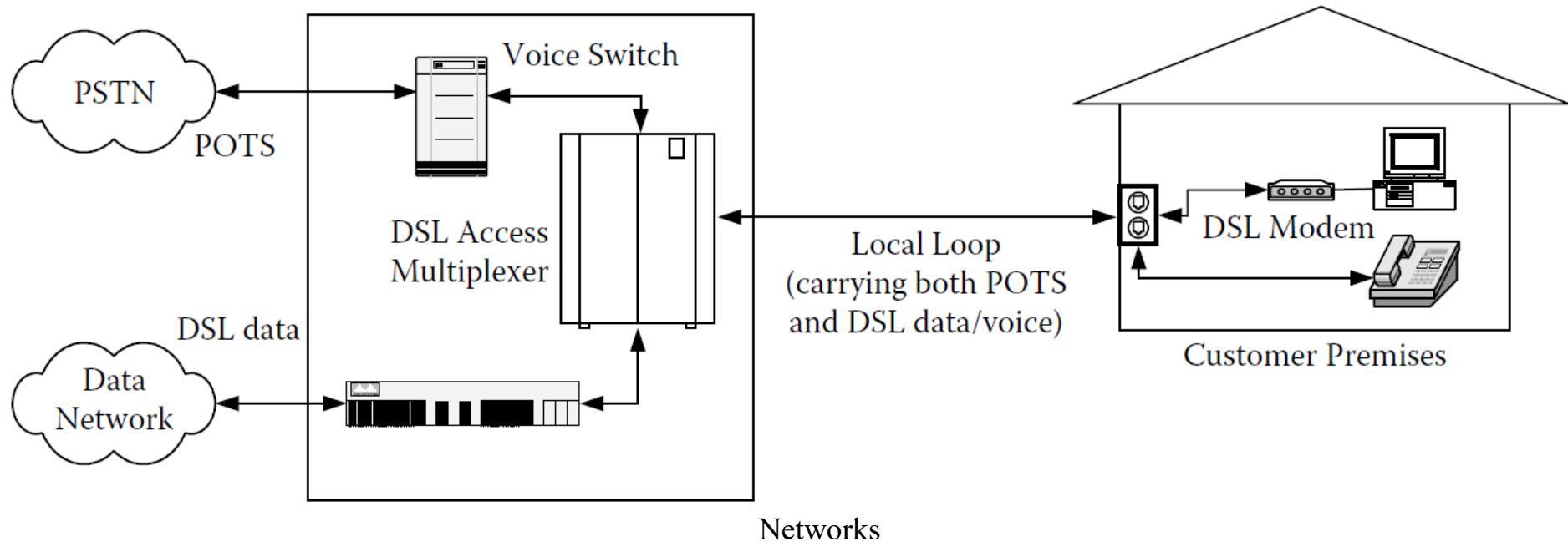


DSL (Digital Subscriber Line)

Link between subscriber and network (local loop); tens of millions installed;
Reinstall?

⇒ need for exploiting the existing base of TP wired structure; initially designed for voice-grade analog transmissions with 4kHz bandwidth, TP may carry data using signals over a spectrum of more than 1MHz => use of modems for digital high rate data transmissions, using currently installed twisted pair cable.

- DSL refers to the analog local loop between each customer premises and its local central office, and a DSL modem is required at each end of the loop



ADSL (Asymmetric Digital Subscriber Line)

ADSL initially designed for video-on-demand, now appropriate for high-speed Internet access.

Asymmetric because, from the user point, there is greater capacity downstream (from service provider to customer) than upstream.

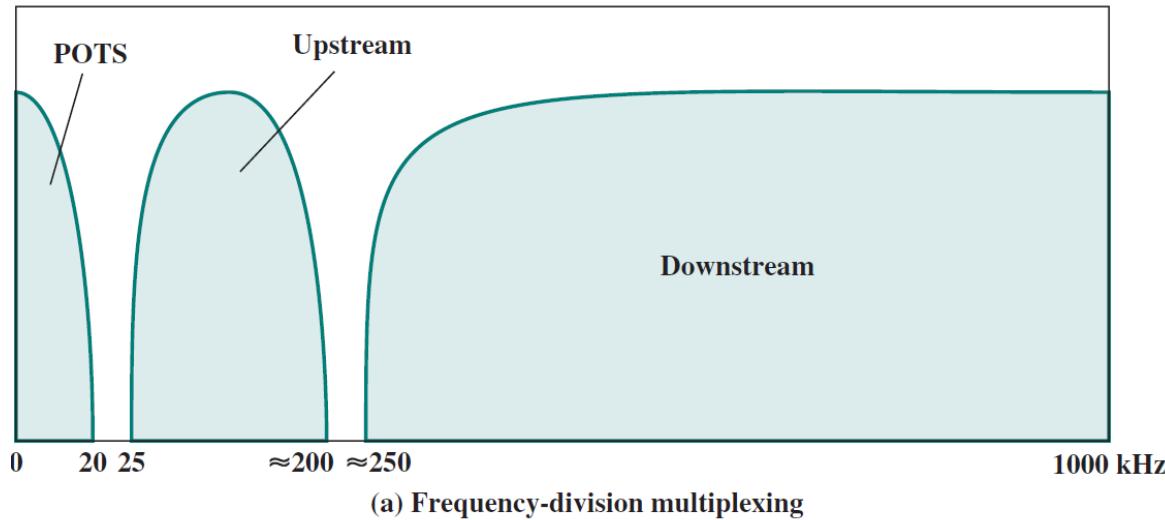
ADSL uses FDM for managing the 1MHz bandwidth:

- Lowest 25kHz for voice (Plain Old Telephone Service): 0 to 4kHz for voice, rest for guard, avoiding interference with other channels
- Use echo cancellation or FDM to give (to allocate) two bands: one for upstream , one for downstream
- Use FDM within each of two bands.

Supports loop length in the range of 5.5km.

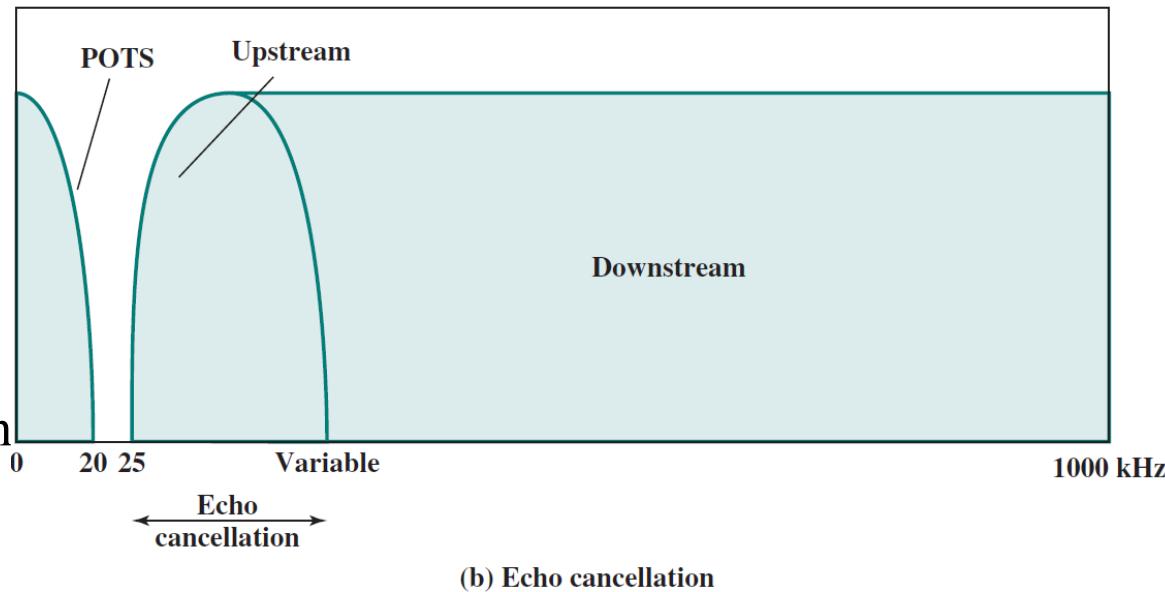
Echo Cancellation

Signal processing technique, allowing digital transmissions in both directions on a single line simultaneously. The transmitter must subtract the echo of its own transmission from the incoming signal, to recover the signal sent by the other side.



Advantages:

- more flexibility for upstream bandwidth changes, simply extending the area of overlap
- downstream bandwidth in the good part of the spectrum (not so many HFs) => a lower attenuation



DMT (Discrete Multitone)

DMT modem allows multiple carrier signals at different frequencies;

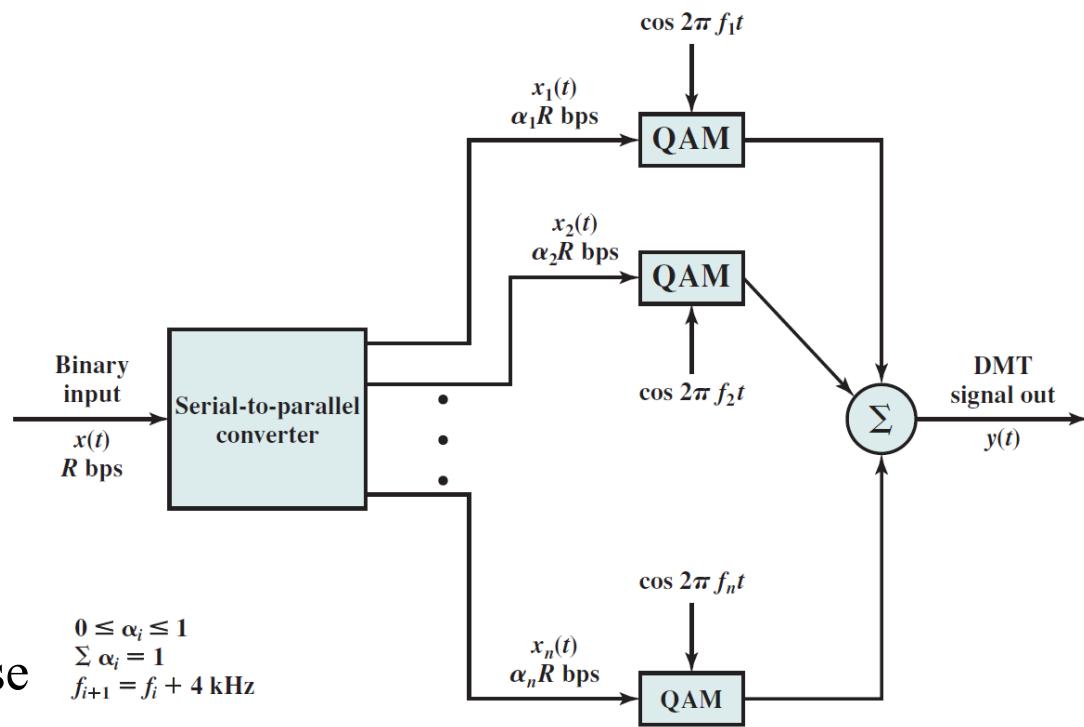
-upstream and downstream bandwidths are split in a number of 4kHz sub-channels, transmitting a number of bits on each channel.

Initially modem send test signal on each subchannel, and then use those subchannels with better signal to noise ratio.

If used 256 downstream subchannels at 4kHz, carrying data at 60kbps, will result a data rate of 15.36Mbps. Transmission impairments bring this down to 1.5Mbps to 9Mbps.

Use of **QAM (Quadrature Amplitude Modulation)** – analog signaling technique, a combination of AM and PM. May assign different number of bits/transmitted signal.

Sample example: data string is split in two sub-strings. One sub-string modulates the carrier, the other modulates the carrier shifted with 90° . The composed QAM signal is the sum: $s(t) = d_1(t)\cos 2\pi ft + d_2(t)\sin 2\pi ft$. \Rightarrow signal has 4 states, for coding 2 bits.



xDSL – recent schemes for high-data speed transmissions on ADSL

High data rate DSL

Single line DSL

Very high data rate DSL

	ADSL	HDSL	SDSL	VDSL
Data Rate	1.5–9 Mbps downstream 16–640 kbps upstream	1.544 or 2.048 Mbps	1.544 or 2.048 Mbps	13–52 Mbps downstream 1.5–2.3 Mbps upstream
Mode	Asymmetric	Symmetric	Symmetric	Asymmetric
Copper Pairs	1	2	1	1
Range (24-Gauge UTP)	3.7–5.5 km	3.7 km	3.0 km	1.4 km
Signaling	Analog	Digital	Digital	Analog
Line Code	CAP/DMT	2B1Q	2B1Q	DMT
Frequency	1–5 MHz	196 kHz	196 kHz	≥10 MHz
Bits/Cycle	Varies	4	4	Varies

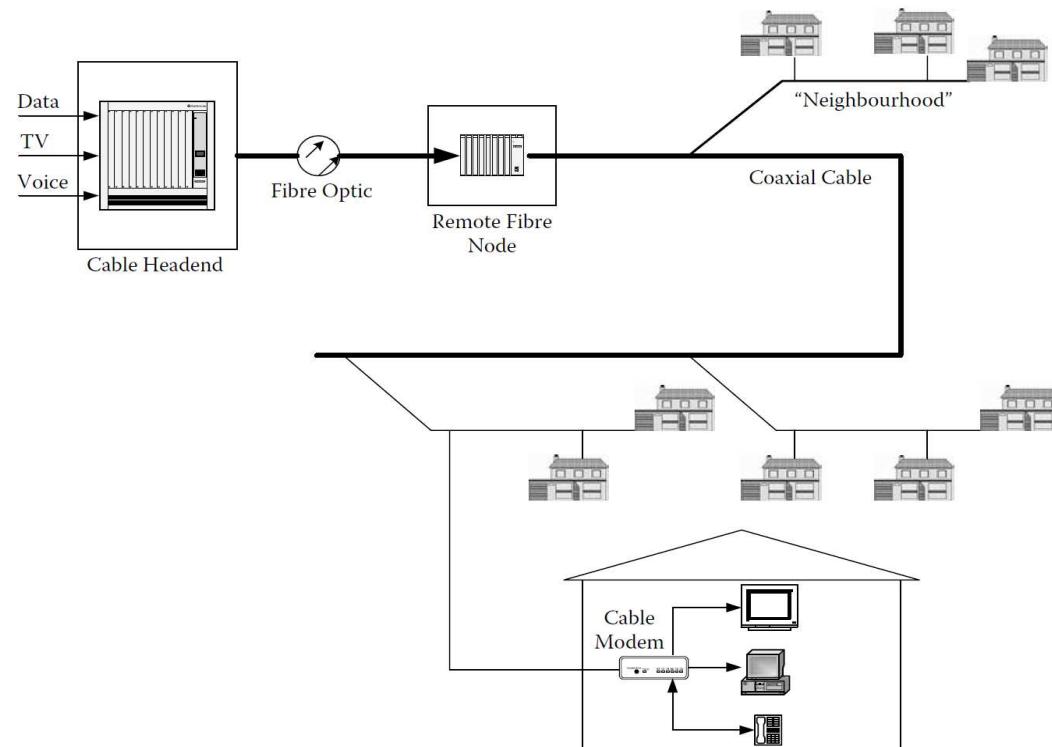
Alternative Broadband Access Technologies

Fiber-to-the-home (FTTH)

- common solution: using passive optical network (PON)
- a single transceiver in the CO serving multiple customers
- splitters and couplers to distribute the service among the different subscribers

Cable

- hybrid fiber-coax (HFC)
- fiber-optic cable carrying signals between the cable headend and fiber nodes in the network, from which existing coaxial cable is used to cover the “last mile” to the subscribers’ premises.



Alternative Broadband Access Technologies

Wireless

- wireless local loop with the advantage that it doesn't need the installation of a transmission medium
- higher frequencies systems: 20 to 40 GHz, sometimes requiring line-of-sight (LOS) availability
- Lower frequency systems: 2,4GHz– 5GHz, with non-LOS transmission

BPL (*Broadband over Power Line*)

- use of the electric power supply network for the transmission of broadband data

Example: *IEEE 1901-2010 (IEEE Standard for Broadband over Power Line Networks: Medium Access Control and Physical Layer Specifications)*

- high-speed (>100 Mbps at the physical layer) communication
- transmission frequencies below 100 MHz
- BPL devices used for the first-mile/last-mile connection (<1500 m to the premise) and BPL devices used in buildings for local area networks (LANs) and other data distribution (<100 m between devices).

Transmission Media

Two main groups:

-**Wire based media** (*hardwire*, or guided), either :

- electric*, like **twisted pair** cable TP, **coaxial** cable
- optic*, like **fiber optics**

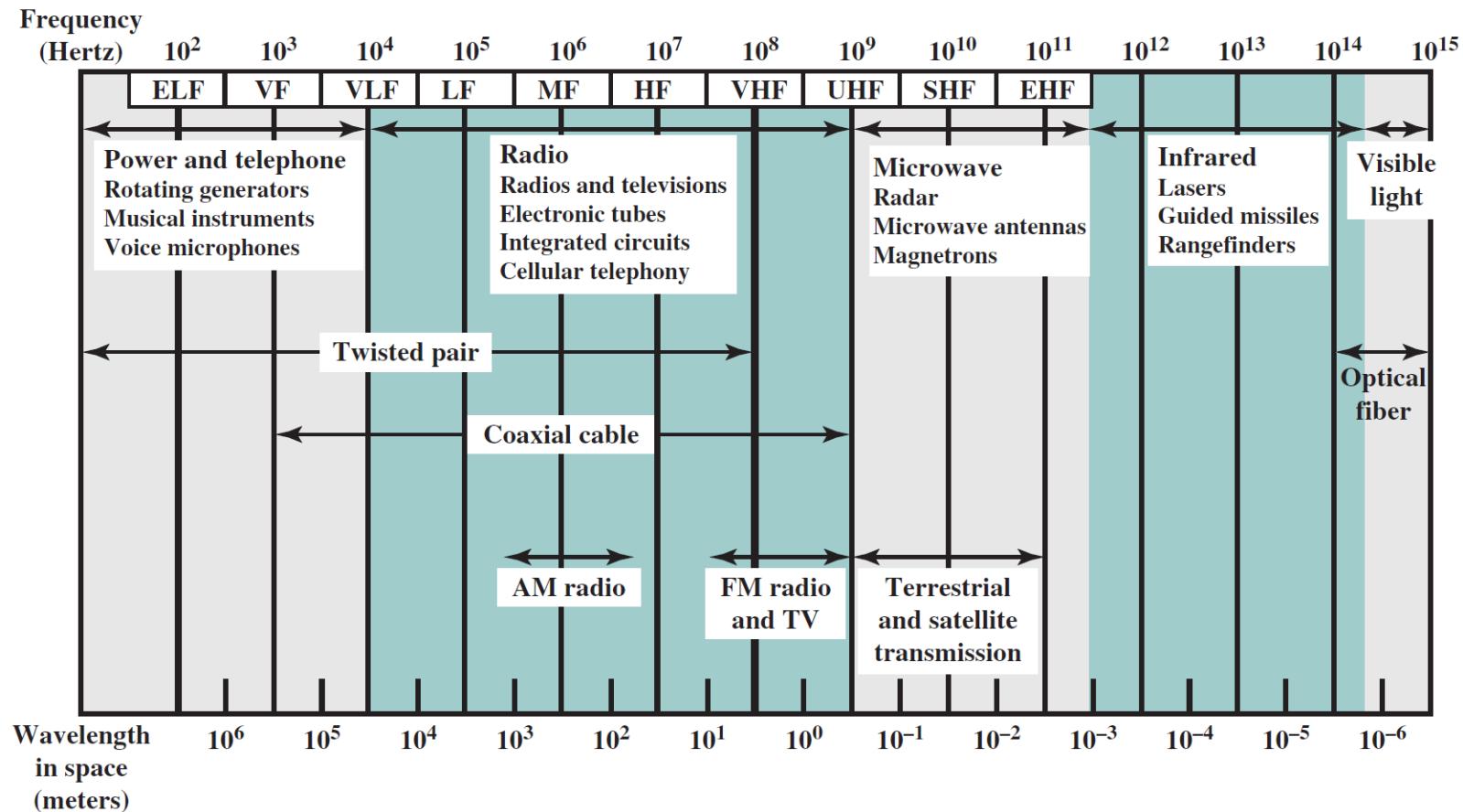
-**Wireless** (*softwire*, or unguided), like **infrared rays**, **radio waves**, **microwaves**.

Characteristics and quality determined by medium and used signal.

For guided media (wire based), the medium is more important!

For unguided media, the bandwidth produced by the antenna is more important!

Main key concerns are: **data rate & distance**



ELF = Extremely low frequency
 VF = Voice frequency
 VLF = Very low frequency
 LF = Low frequency

MF = Medium frequency
 HF = High frequency
 VHF = Very high frequency

UHF = Ultrahigh frequency
 SHF = Superhigh frequency
 EHF = Extremely high frequency

Electromagnetic Spectrum & used frequencies by each media's transmission technique

Design Factors

Bandwidth

Higher bandwidth gives higher data rate

Transmission impairments

Attenuation limits possible covered distances (acts more for guided media)

Interference (acts on both categories); for guided media use of proper shielding

Number of receivers

In guided media: more receivers (multi-point transmissions) introduce more attenuation

Hard-wire media

Specific Parameters for the Electric Cables

- Fire security*- the internal cable structure and external coating need to offer proprieties for: zero halogen emission, low smoke fume emanation, flame retardant
- Impedance* – cables for data transmission present impedance in the range of $50\text{-}150\Omega$, but usually 100Ω impedance
- Propagation speed* for the electric signal - a ratio of the light speed. An average value of $66\%\cdot c$, implying a signal speed on a copper based cable of 200.000Km/s
- Signal loss* - cable needs to allow small values for the signal loss (attenuation is measured in dB)

Hard-wire media

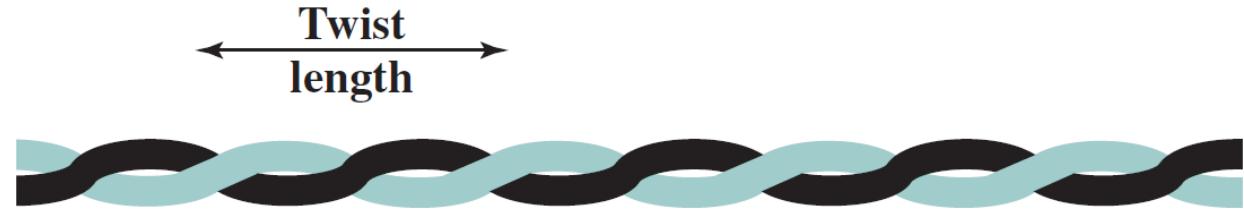
Specific Parameters for the Electric Cables

- *Cross-talk* is a measure (in dB) of how a cable affects the behavior of a neighbor cable. For effect limitation is used the shielding. Also used the balanced differential transmission
- *Section (geometry)* of the conductor – measured not in mm, but in AWG (*American Wire Gage*); 26AWG for telephony cables
- In Europe, the ISO/IEC-11801 standards family defines general and specific cabling design documents.
 - It comprises the ISO/IEC 11801-1:2017 Information technology — Generic cabling for customer premises — Part 1: General requirements and includes ISO/IEC 11801-2, ISO/IEC 11801-3, ISO/IEC 11801-4, ISO/IEC 11801-5, ISO/IEC 11801-6. The ISO/IEC 11801-1 specifies the requirements for coaxial, twisted-pair copper and optical fiber.
 - In the USA and Canada, ANSI/TIA-568-C standard is used instead of ISO/IEC 11801.

Twisted pair

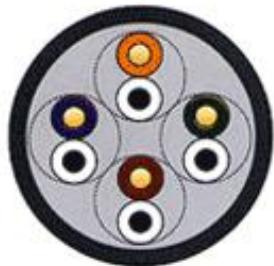
Consists of two metallic copper wires, twisted after a given step.

- Separately insulated
- Twisted together
- Often "bundled" into cables
- Usually installed in building during construction



Twisted pairs are of the following kinds:

- **STP** (*Shielded Twisted Pair*), presenting protective shield for each pair and a global shield (metal braid) for whole cable; reduces interference but increased weight
- **FTP** (*Foiled Twisted Pair*), or **ScTP** (*Screened TP*), providing an unique global shield
- **UTP** (*Unshielded Twisted Pair*), being the non-shielded variant, only the separate pair insulation



UTP



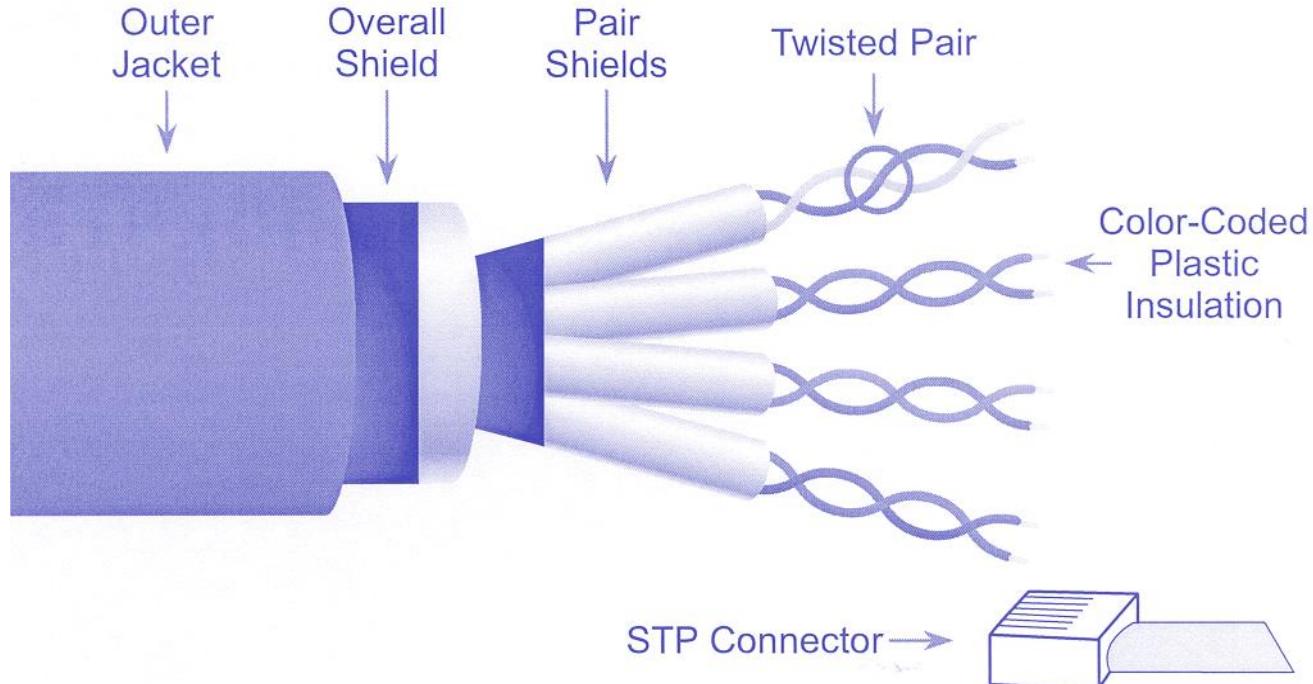
FTP



STP

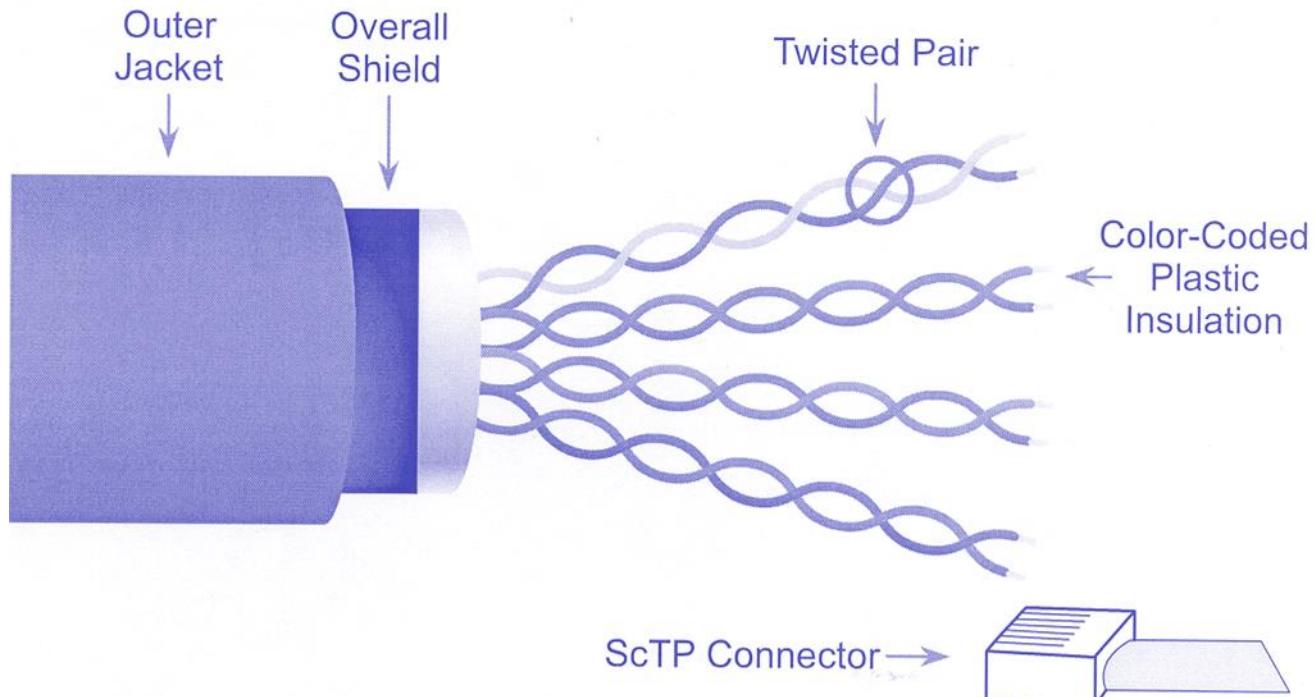


STP (Shielded Twisted Pair)



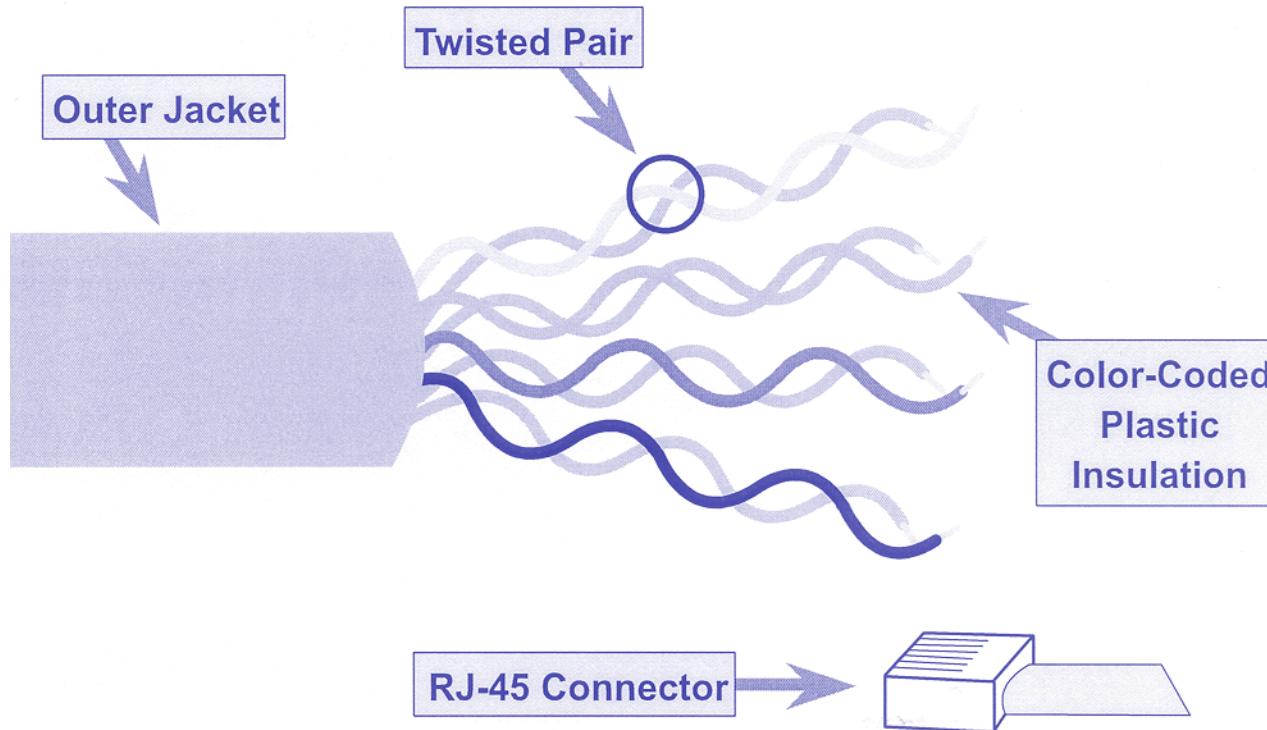
maximum cable length: 100 m (short distance)

ScTP (Screened Twisted Pair)



maximum cable length: 100 m (short distance)

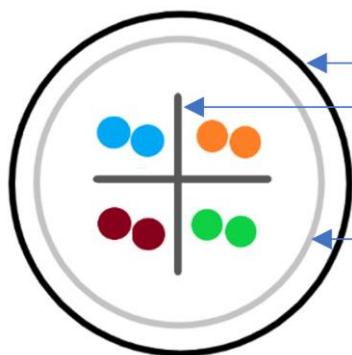
Unshielded Twisted Pair (UTP)



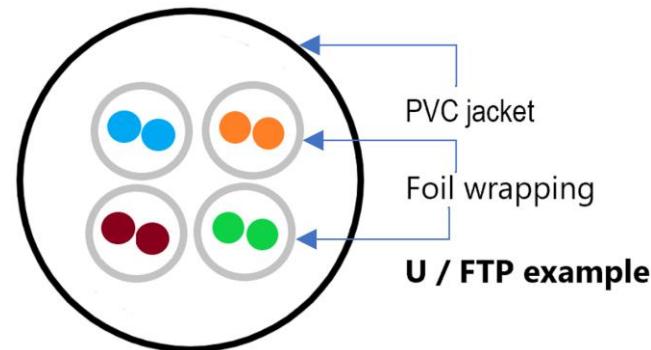
maximum cable length: 100 m (short distance)

The cable naming convention from ISO/IEC 11801 presents the different types of cable construction, based on their screening: XX / XXX. Examples of cable naming are: U/UTP, U/FTP, F/UTP, S/UTP, SF/UTP, F/FTP, S/FTP, SF/FTP etc.

XX			/	X	XX	
overall screen				element screen	balanced element	
F = foil screen	S = braid screen	SF =braid and foil screen		U = unscreened	F = foil screened	TP



PVC jacket
Plastic divider
Foil wrapping
F / UTP example



PVC jacket
Foil wrapping
U / FTP example

UTP: most common medium; used in:

-Telephone network

Between house and local exchange (subscriber loop)

-Within a company's buildings

To private branch exchange (PBX)

-For local area networks (LAN)

Ethernet at 10Mbps 100Mbps or 1Gbps

Advantages:

-cheap

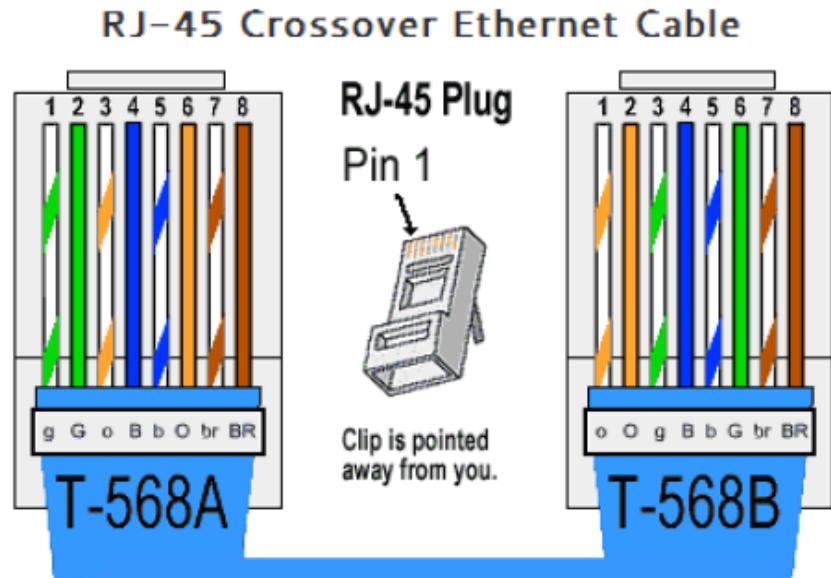
-easy to work with (to install on walls)

Problems:

-susceptible to EM interference and noise

-need for amplification (order of kilometers)

-near end crosstalk



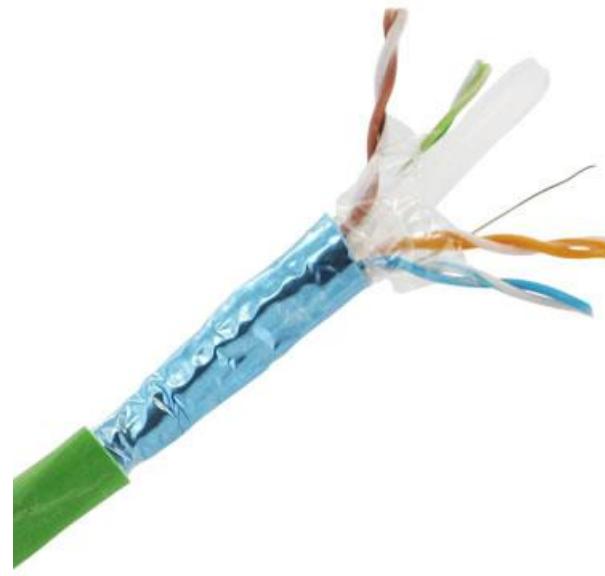
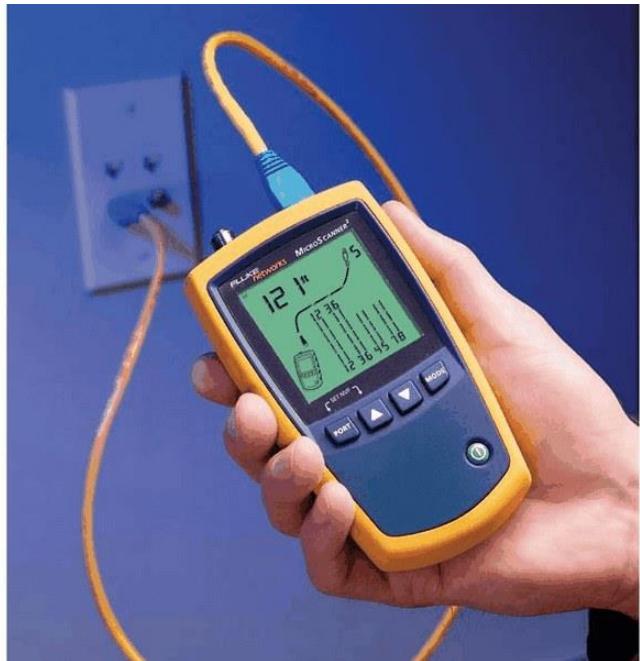
UTP Categories

- Category 1 - *Telecommunication*, the cables for the analogue telephony
- Category 2 (*Low Speed Data*), the cables for analogue and early digital telephony, offering data transmission services at low speeds
- Category 3 (*High Speed Data*) defines cables used for LANs up to 10-16Mbps; the usual voice grade
- Category 4 (*Low Loss, High Performance Data*) defines cables with higher performances, used at communication speeds of tens of Mbps (20Mbps)
- Category 5 and 5e (*Low Loss, Extended frequency, High Performance Data*), are used in today's networks working at hundreds of Mbps; Commonly pre-installed in new office buildings.
- Categories 6 and 7 (*low attenuation and higher noise immunity*); Replaces Cat5e

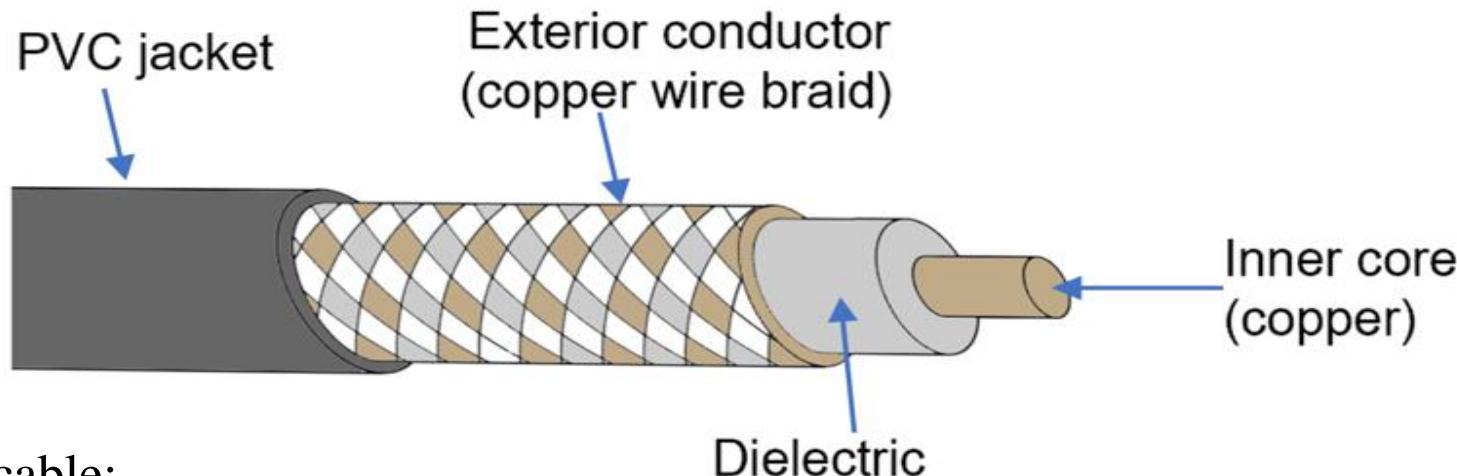
UTP Categories

Class	Bandwidth	Category
Class A	up to 100 kHz	Category1
Class B	up to 1 MHz	Category2
Class C	up to 16 MHz	Category3
Class D	up to 100 MHz	Category5e
Class E	up to 250 MHz	Category6
Class EA	up to 500 MHz	Category6a
Class F	up to 600 MHz	Category7
Class FA	up to 1000 MHz	Category7a
Class I and Class II	up to 2000 MHz	Category8.1, 8.2





Coaxial cable



Coax cable:

- base-band cable, 50Ω impedance, used in Ethernet LANs
 - thick Ethernet (RG213), difficult to install
 - thin Ethernet (RG58), excellent versatility
- broad-band cable, 75Ω impedance, used less for LANs, more for CATV or long distance telephone transmissions

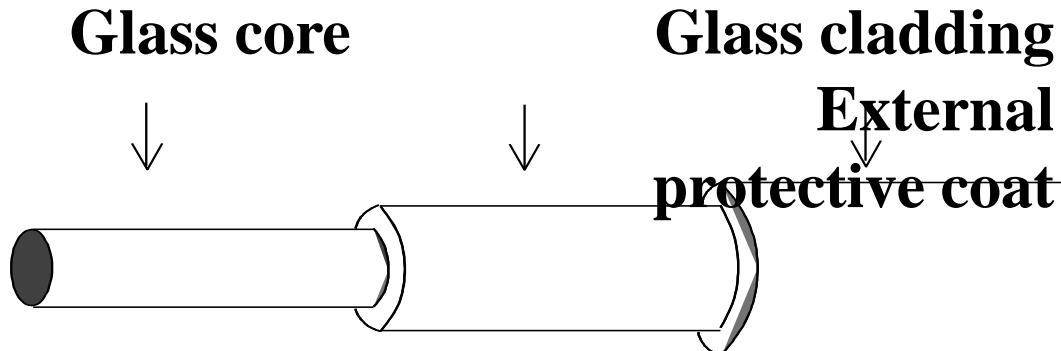
Advantages: goes up to 500MHz, repeaters every 1-2 km

Drawback: is a shared broadcast medium, not for full duplex (switched) transmissions => it is replaced by TP cables (LANs) or by fibre optics (long telephony trunks)

COAXIAL CABLE



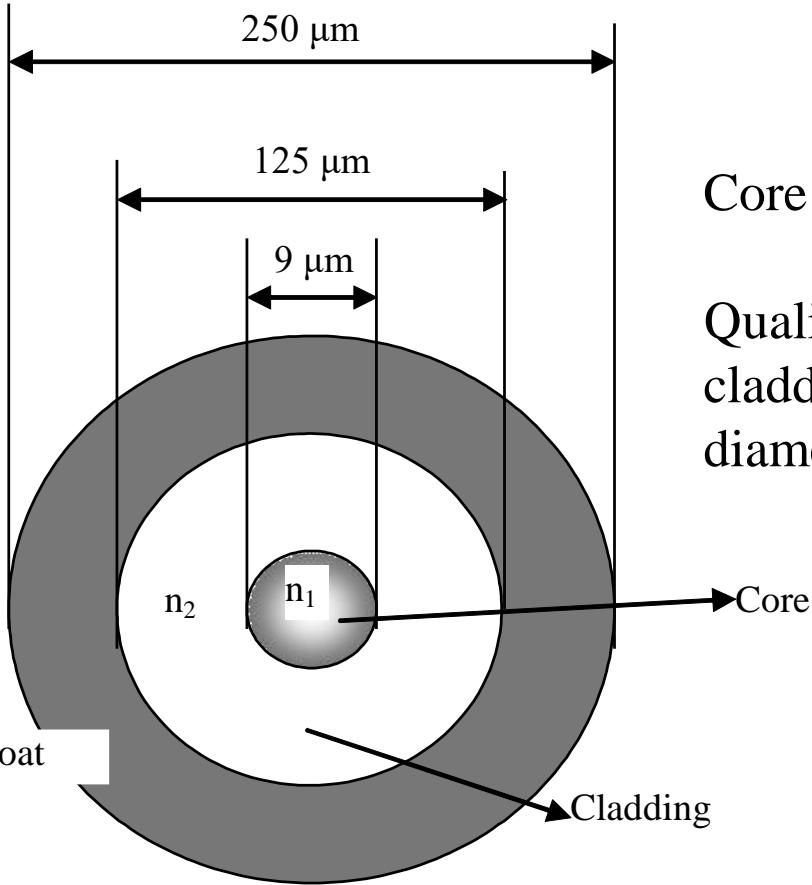
Fiber optic



An inner glass core, covered by a glass cladding *with different refractive and density properties*; for protection and easier cabling – colored plastic coat (see next slide also)

Advantages:

- low attenuation, fiber optic links with lengths in the order of ten of Kilometers
- total immunity to electromagnetic field effects (carriers are the neutral photons)
- transmission data rates in the order of Giga bps
- easy for cabling, presenting low weight, small diameter ($125/250\mu\text{m}$) and being flexible



Core diameter less than 10 microns

Quality of fiber given by ratio between
cladding diameter and whole fiber
diameter

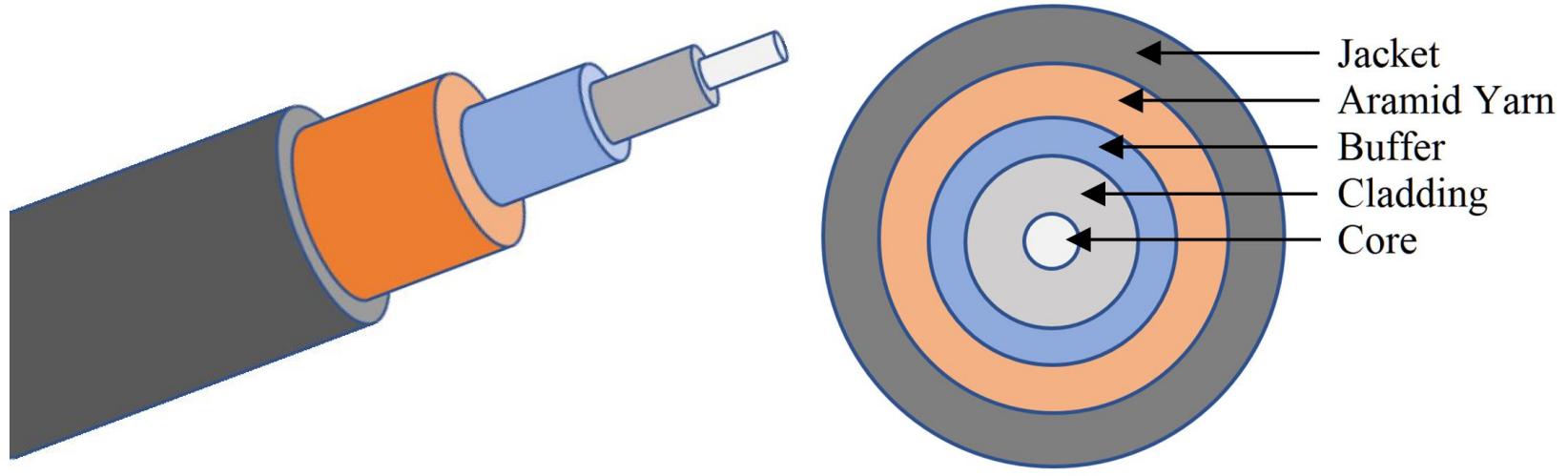


Figure 2.1 a. *Optical fiber layers*

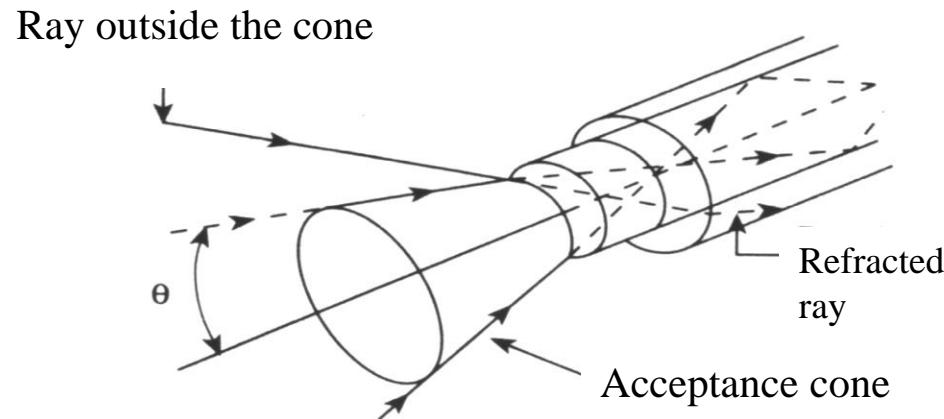
b. *Optical fiber transversal section*

Optical transmissions theoretical issues

Optical transmissions governed by Snell's law: the critical angle for an ideal transmission is: $\theta_c = \arcsin(n_2/n_1)$, n_1 and n_2 are the refractive indexes of the adjacent glass layers (core, respectively cladding);

The lower refractive index of the cladding (with respect to the core) causes the light to be angled back into the core

All attack angles for the light rays up to the critical angle will give minimum refraction and maximum of reflection => acceptance cone



Light propagation modes:

-**step-index multimode**, refraction index constant for the fibre core, doesn't matter distance to core's centre; implies different path lengths for light rays, making reception difficult; present a thicker core (hundreds of μm) => cheaper fiber

-**graded-index multimode**, refraction index decreasing from the core centre to edges; offer a better focusing of the rays, so a lower attenuation and easier reception

-**single mode** (mono-mode), the core diameter \sim light ray wavelength ($5-8\mu\text{m}$) => direct path for light ray, no loss, no attenuation, but more expensive

Condition for single-mode fiber:

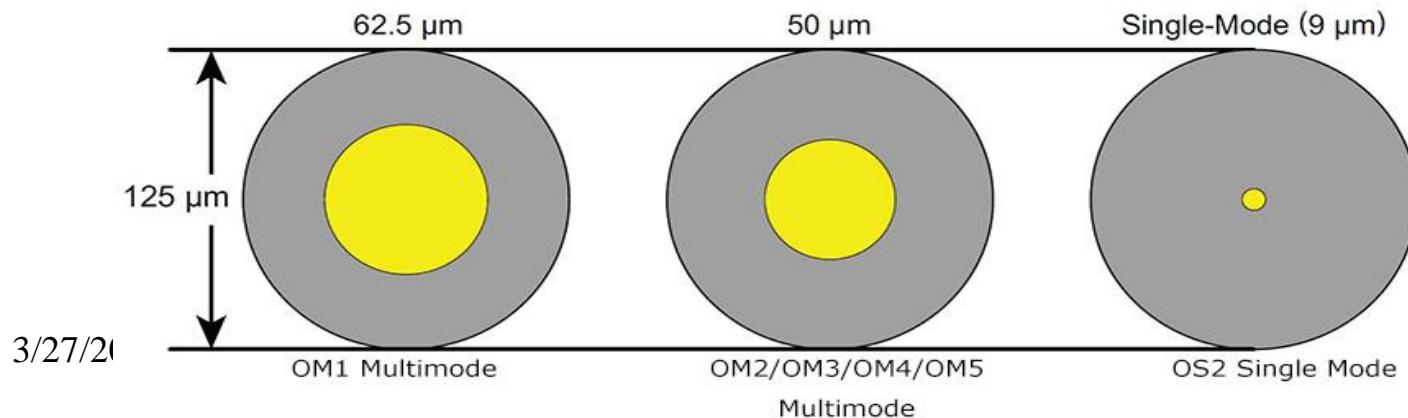
λ_c - light ray wavelength;

$2a$ – fiber diameter;

n_1 and n_2 are refractive indexes of the core, respectively cladding

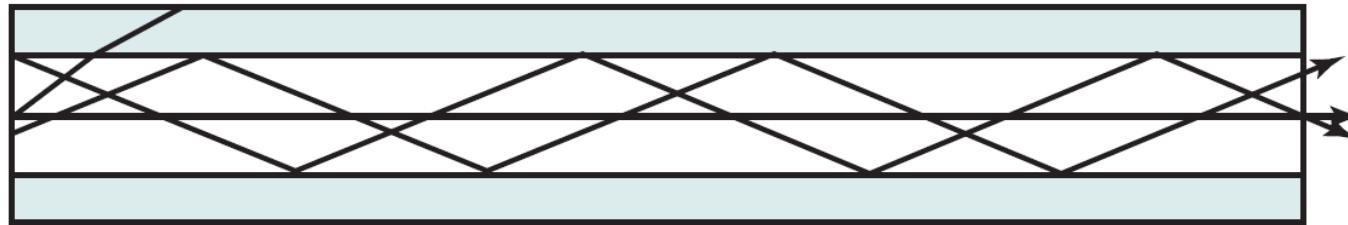
$$\lambda_c > \frac{2\pi a}{2,405} \sqrt{n_1^2 - n_2^2}$$

Optical Fiber Core Diameters

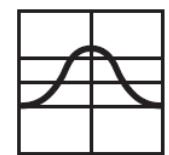


Light propagation modes

Input pulse

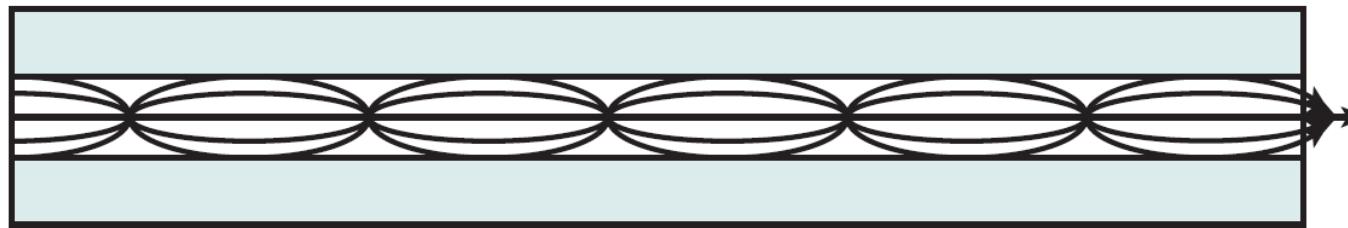
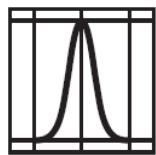


Output pulse

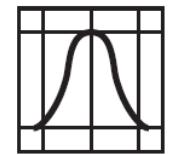


(a) Step-index multimode

Input pulse

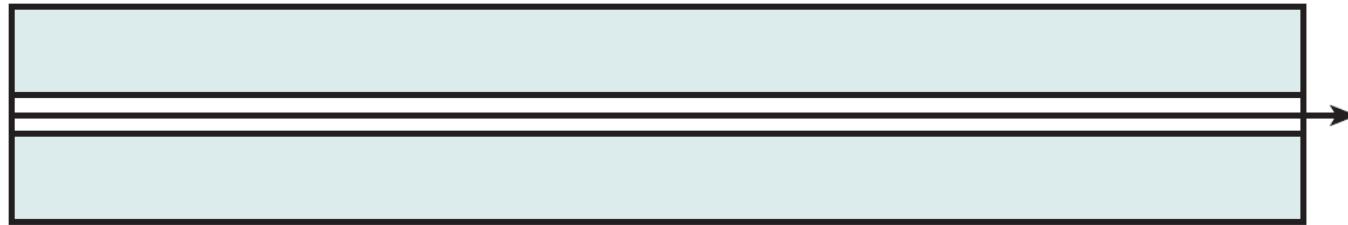


Output pulse

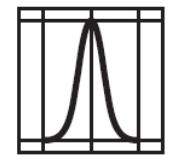


(b) Graded-index multimode

Input pulse



Output pulse



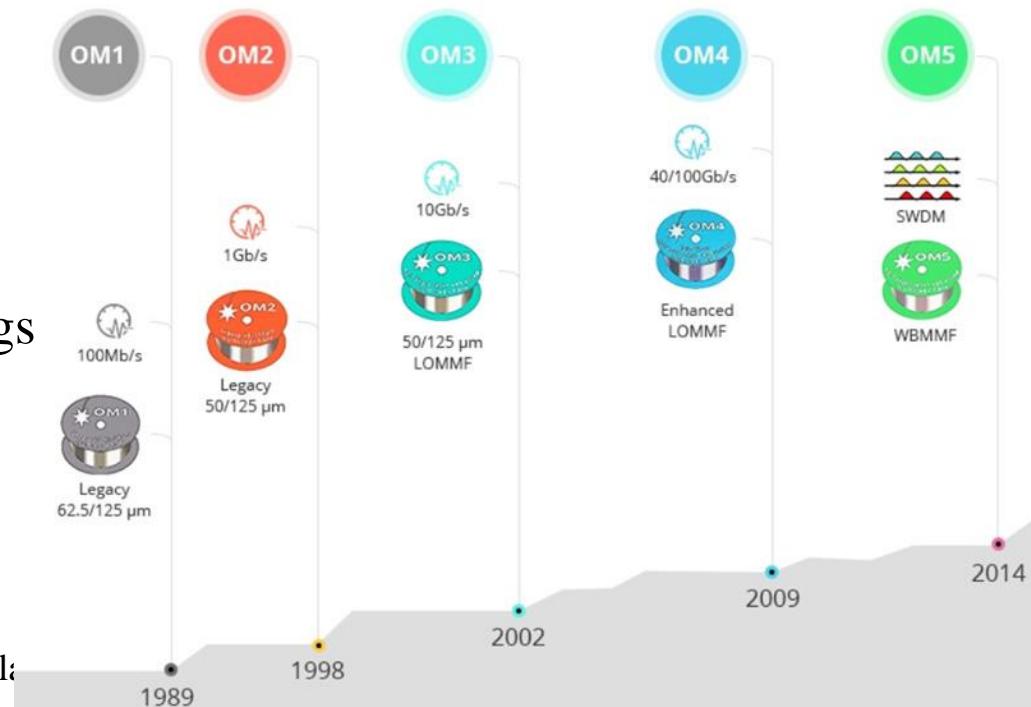
(c) Single mode

Multimode Fiber

MMF Cable Type	Diameter	Jacket Color	Optical Source	Bandwidth
OM1	62.5/125µm	Orange	LED	200MHz*km
OM2	50/125µm	Orange	LED	500MHz*km
OM3	50/125µm	Aqua	VSCEL	2000MHz*km
OM4	50/125µm	Aqua	VSCEL	4700MHz*km
OM5	50/125µm	Lime Green	VSCEL	28000MHz*km

<https://community.fs.com/blog/advantages-and-disadvantages-of-multimode-fiber.html>

- mostly used in communication over short distances (hundreds of meters):
 - inside a building or campus networks
 - backbone applications in buildings
 - enterprise and data center applications



Single-mode Fiber

Name	OS1	OS2
Standards	ITU-T G.652A/B/C/D	ITU-T G.652C/D
Cable Construction	Tight buffered	Loose tube
Application	Indoor	Outdoor
Maximum Attenuation	1.0dB/km	0.4dB/km
Distance	10 km	200 km
Price	Low	High

-used in communication over long distances (kilometers):

Advantages over multimode fiber:

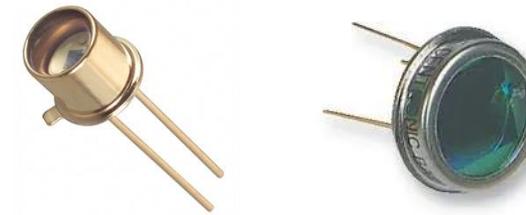
- longer transmission distance
- greater bandwidth capacity
- increased transmission speed
- limited data dispersion & external interference
- less signal attenuation

Fiber Optic Cable Type		Fiber Cable Distance					
		Fast Ethernet 100BA SE-FX	1Gb Ethernet 1000BASE-SX	1Gb Ethernet 1000BA SE-LX	10Gb Base SE-SR	40Gb Base SR4	100Gb Base SR10
Single mode fiber	OS2	200m	5000m	5000m	10km	/	/
Multi-mode fiber	OM1	200m	275m	550m (mode conditionin g patch cable required)	/	/	/
	OM2	200m	550m		/	/	/
	OM3	200m	550m		300m	100m	100m
	OM4	200m	550m		400m	150m	150m
	OM5	200m	550m		300m	400m	400m

<https://community.fs.com/blog/single-mode-cabling-cost-vs-multimode-cabling-cost.html>

Transmission devices:

- light *emission* using **LEDs** (light emitting diodes) or **laser (diodes)** (for single-mode transmissions)
- reception* of light and conversion into electrical signal using **photodiodes**



For fibers: to be used wavelengths upper than the visible light ($> 750\text{nm}$)

Attenuation depends on the light ray wavelength => definition of 3 windows for the optical transmissions:

- 850nm centred window, used for multi-mode ‘cheap’ transmissions; up to 150MHz signal frequency, attenuation of 3.5dB/km
- 1300nm centred window, used for graded-index multimode and single-mode transmissions; attenuation under 1dB/km, working frequencies: 0.5-1GHz
- 1550nm wavelength centred window, single-mode laser based transmissions, attenuation under 0.5dB/km, working frequencies up to 100GHz

Use of fiber optic cables:

- long haul trunks (10 – 100km without amplifiers)
- used also for LANs or digital subscriber loops; usually as point-to-point links, shaped as ring or star

Junctions / Splices

Points where two fibers are connected to obtain a longer link or a fibre gets attached a terminal connector (permanent connection)

Mechanical junction: fibers ends are cut, cleaned and polished, then aligned into a mechanical device

Junction by fusion: fibers ends are heated-up close to melting point, than pasted and heated-down suddenly

Junctions introduce extra attenuation (0.1 to 0.4 dB)

Connecting devices – optical connectors:

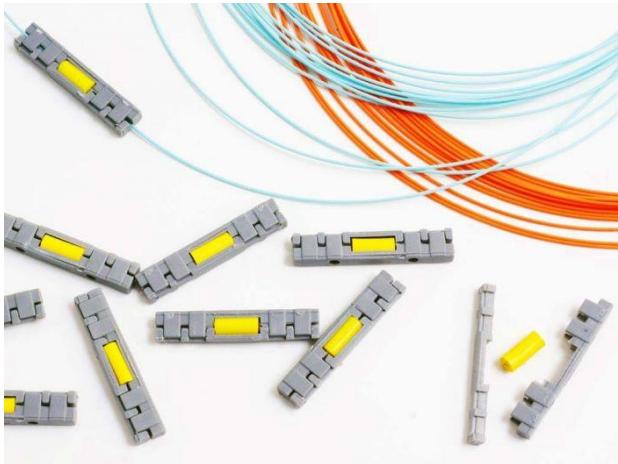
Non-permanent connections or variable configurations

Usually prefabricated connectors, one side presenting a junction with fiber, the other connector side being free

Connectors are:

- passive, using taps with LED/Photodiode; do not affect cable transmission
- active, using transformers from light/electric to electric/light signals and electric signal amplification

Connectors introduce extra attenuation, higher than junctions (0.2 to 0.5 dB)



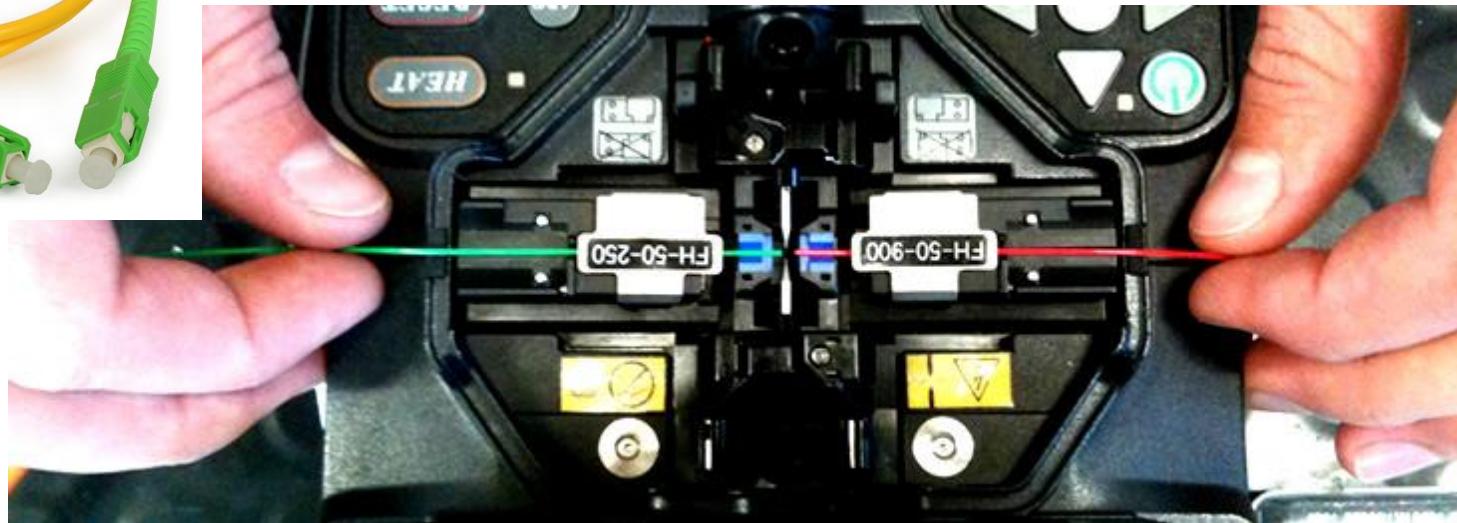
splices: (loss <= 0.3dB) mechanical and fusion



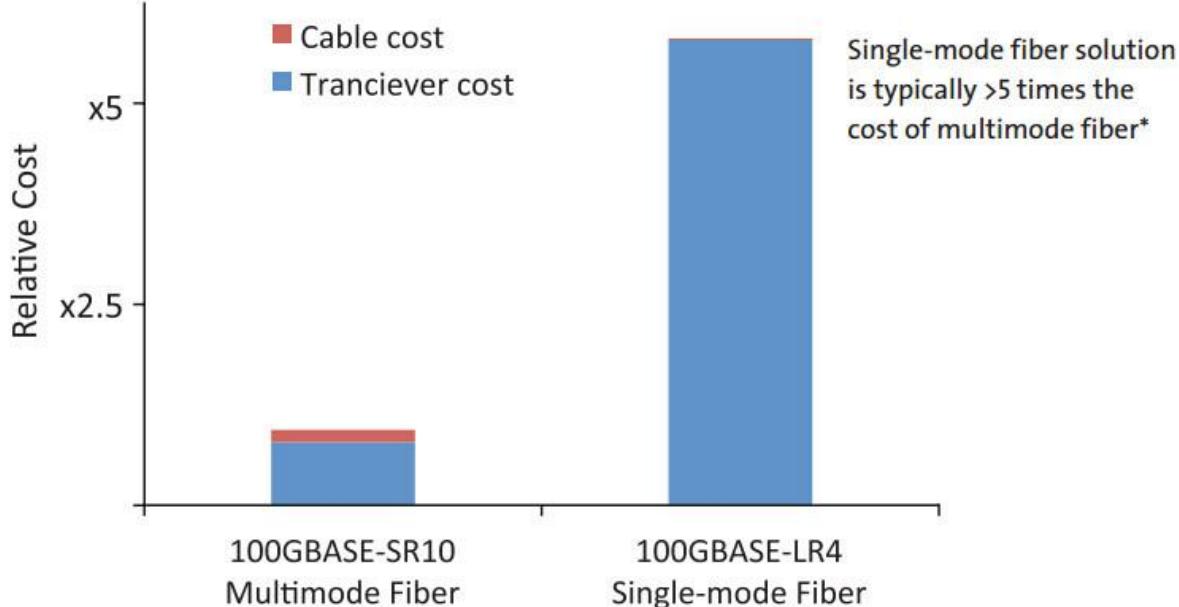
SFP



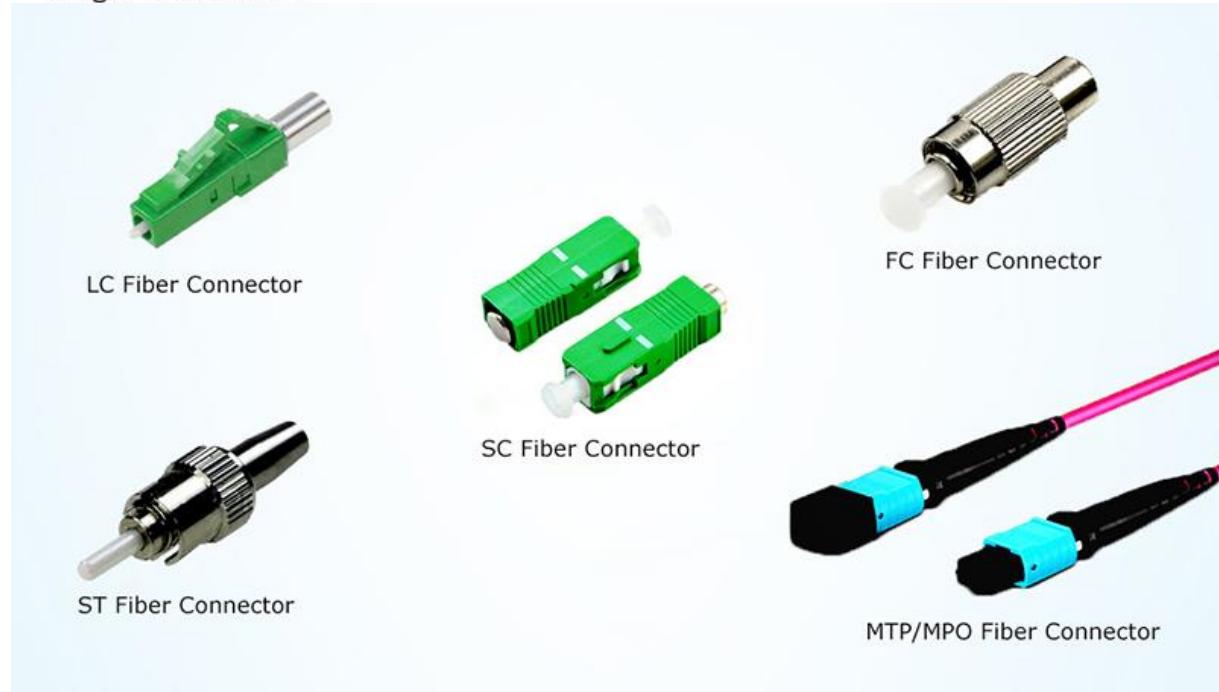
Media converter



Optical Transceiver Cost and connector types



<https://community.fs.com/blog>



Fiber Optic vs TP and Coax

Information in this table, considering especially the costs, is relative and is subject to change; so, it is purely informal

Attribute	TP	Coax	FO
Data rate	100 Mbps – 1/10 Gbps	100Mbps – 1 Gbps	n Gbps
Distance	100 m	500m	Up to 10km
Accessibility to be tapped	Easy	Easy	Difficult
Signal radiation	Yes	Yes	No
Grounding problems	Yes	Yes	No
Static problems	Yes	Yes	No
Sparkling	Yes	Yes	No
Bit error rate	10^{-9}	10^{-6}	$10^{-14} +$
Size &Weight /data rate	Medium	Large	Small
Cable cost per meter	0.5 USD	0.3 USD	0.5 USD
Installing + maintenance costs	N	N	N+

Soft-wire (wireless) media

For unguided media: higher frequencies give higher transmission data rates

Antenna based transmissions:

- directional, antenna-to-antenna focused beam, requiring antennas alignment
- omnidirectional, beam spread and may be received by many antennas

LANs using wireless media present flexibility, easiness in installing and maintenance

Main media:

- terrestrial microwaves
- satellite microwaves
- broadcast radio waves
- infrared rays

Terrestrial microwaves

Use frequency domain of 2-40GHz, offers up to 500MHz analog signal bandwidth, up to 100Mbps digital signal data rate

Use of parabolic ‘dish’ => ‘line-of-sight’ transmissions of a focused electromagnetic beam => existence of a theoretical maximum distance between antennas:

$$D = 7.14 \sqrt{K \cdot h},$$

Where **h** is antenna’s height and **K** an adjustment factor for waves reflection due to the earth curvature (a 4/3 value may be acceptable)

For long hauls => a succession of relay towers

Satellite microwave

Transmissions (directional, station – satellite – station(s)):

-optimum frequencies domain: 1-10GHz, due to low natural noise interferences (solar, wind, human devices); the most are point-to-point transmissions, referred as 4/6GHz band (the uplink based on 6GHz, the downlink frequencies centred on 4GHz). Today in use 12/14GHz (especially by small earth-stations) and 19/29GHz, offer higher bandwidth, but is need for overcoming attenuation problems.

Satellite: a **microwave relay station**, receiving on one frequency band (*uplink*) and retransmits on another (*downlink*), avoiding interferences. These frequency channels – **transponders**.

Problem: satellite remains stationary with respect to the fixed (usually) earth-stations => equal rotation period as the earth's (launched for 35,784km height)

Satellites on the same orbit, need for an angular displacement of 4° (4/6GHz band) and 3° (12/14GHz band) for no interferences between.

Applications:

-television distribution (Public Broadcasting Services – programs broadcasted to stations and then to users , also Direct Broadcast Satellite – video transmitted directly to user); today use of costless VSAT (Very Small Aperture Terminal) systems

-long distance telephone transmissions

-private networks (each using separate sub-channels)



Broadcast Radio

Being omni-directional transmission, radio antennas are not dish-shaped and may be mobile; generally radio waves use frequencies in the range of 3kHz – 300GHz; broadcast radio (telecomms radio) covers VHF and part of UHF band: 30MHz – 1GHz.

Advantages:

- good wave propagation, low reflection and refraction due to ionosphere
- line-of-sight transmission obeys same law as terrestrial microwave; an usual value for radio repeaters: 20km

Drawbacks:

- multipath interference, due to reflections from land, water, natural and human-made objects.
- radio transmissions allow up to 20Mhz analog signal bandwidth and up to 10Mbps digital signal data rate

Infrared

Infrared comms are based on modulated infrared light, using transceivers; use of THz frequency range; only line-of-sight transmissions => rigid station alignment or passive surface reflections => no interferences, due to impossibility to penetrate surfaces => good enough analog signals bandwidth or digital data rate (LANs at 16Mbps).

No licences for use of infrared channels.

Elements of Structured Cabling

A **structured cabling system** (SCS), featuring the open architecture, is a set of cabling and connectivity products that integrates the voice, data, video, and various management systems of a building.

A **BMS** (Building Management System) consists of:

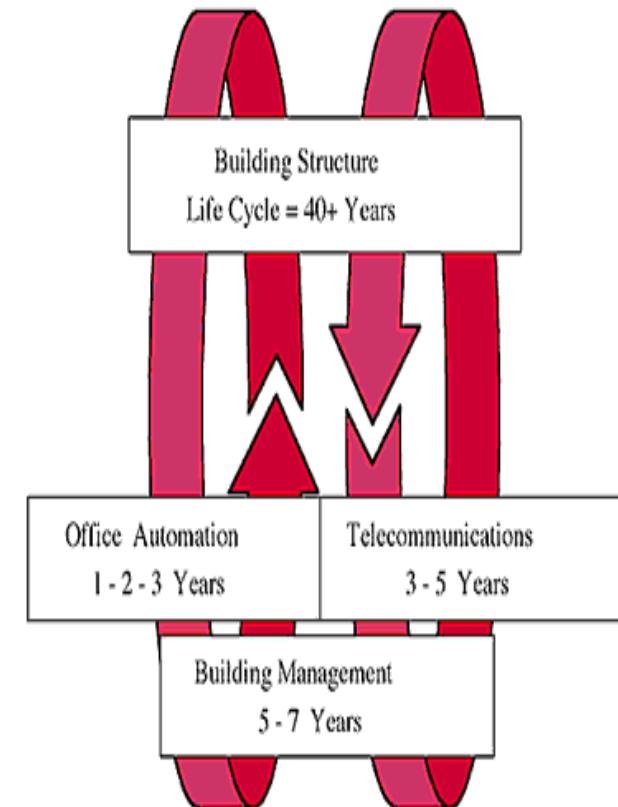
- safety, life & fire alarms
- security and access control (SAC)
- energy systems (EMS)
- heating, ventilation and air conditioning (HVAC)

Usually were cabled separately and voice & data cabling isn't addressed during construction.

Planning and installing the SCS from this phase => lower construction, labour and operational costs.

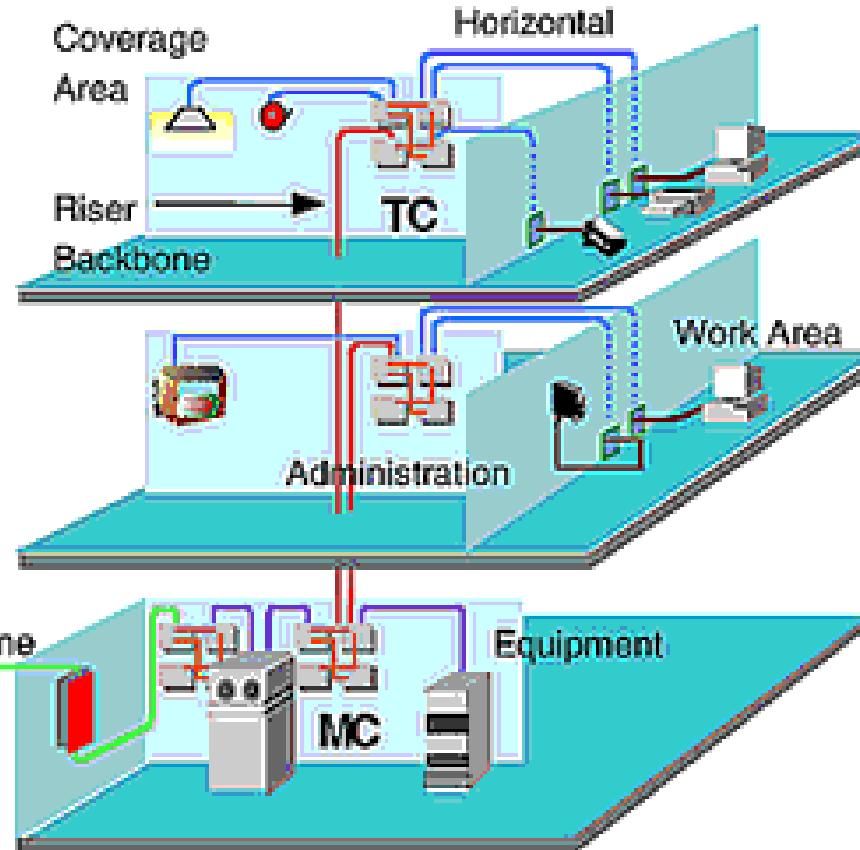
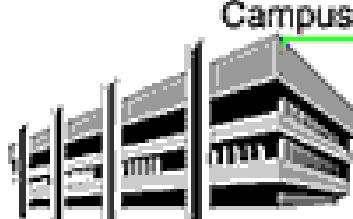
With proper planning, it is not necessary to provide new cabling every time systems are changed or upgraded.

(after International Engineers Consortium).



The Electronic Industries Association/Telecommunications Industry Association (EIA/TIA) and International Standards Organization/ International Electrotechnical Commission (ISO/IEC) have created industry standards for cabling voice and data systems (EIA/TIA 568, 570, or ISO/IEC 11801). These standards address the cabling and cable-delivery methods (pathways and spaces) and are based on a **structured subsystem architecture** of cabling elements.

Structured Cabling Subsystems



TIA/EIA Standards

TIA/EIA-568A

Commercial Building Telecommunications Cabling Standard

TIA/EIA-569A

Commercial Building Standard for Telecommunications Pathways and Spaces

TIA/EIA-570A

Residential and Light Commercial Telecommunications Wiring Standard

TIA/EIA-606

Administration Standard for the Telecommunications Infrastructure of Commercial Buildings

TIA/EIA-607

Commercial Building Grounding and Bonding Requirements for Telecommunications

Sample case study: EIA/TIA 568A (*Commercial Building Telecommunications Cabling Standard*); applicable to campus, medium companies, etc.

Used when designing a company LAN.

The standard specifications concern:

- the minimal requirements for cabling a building with a given number of offices
- -the cabling topology and the allowed distances
- -the components of the cabling system
- -the transmission media and their characteristics
- -the vertical cabling
- -the horizontal cabling
- -the cable identification manner
- -the necessary documentation of the project.

Are defined a number of subsystems:

- building entrance facilities
- equipment room
- backbone cabling (vertical cabling)
- telecommunication closet
- horizontal cabling
- work area's components

Minimum Requirement

- maximum linear covered distance of 3.000m
- maximum surface of the cabling area of 1.000.000 sqm.
- maximum number of employees of 50.000
- minimum validity of the project of 10 years.

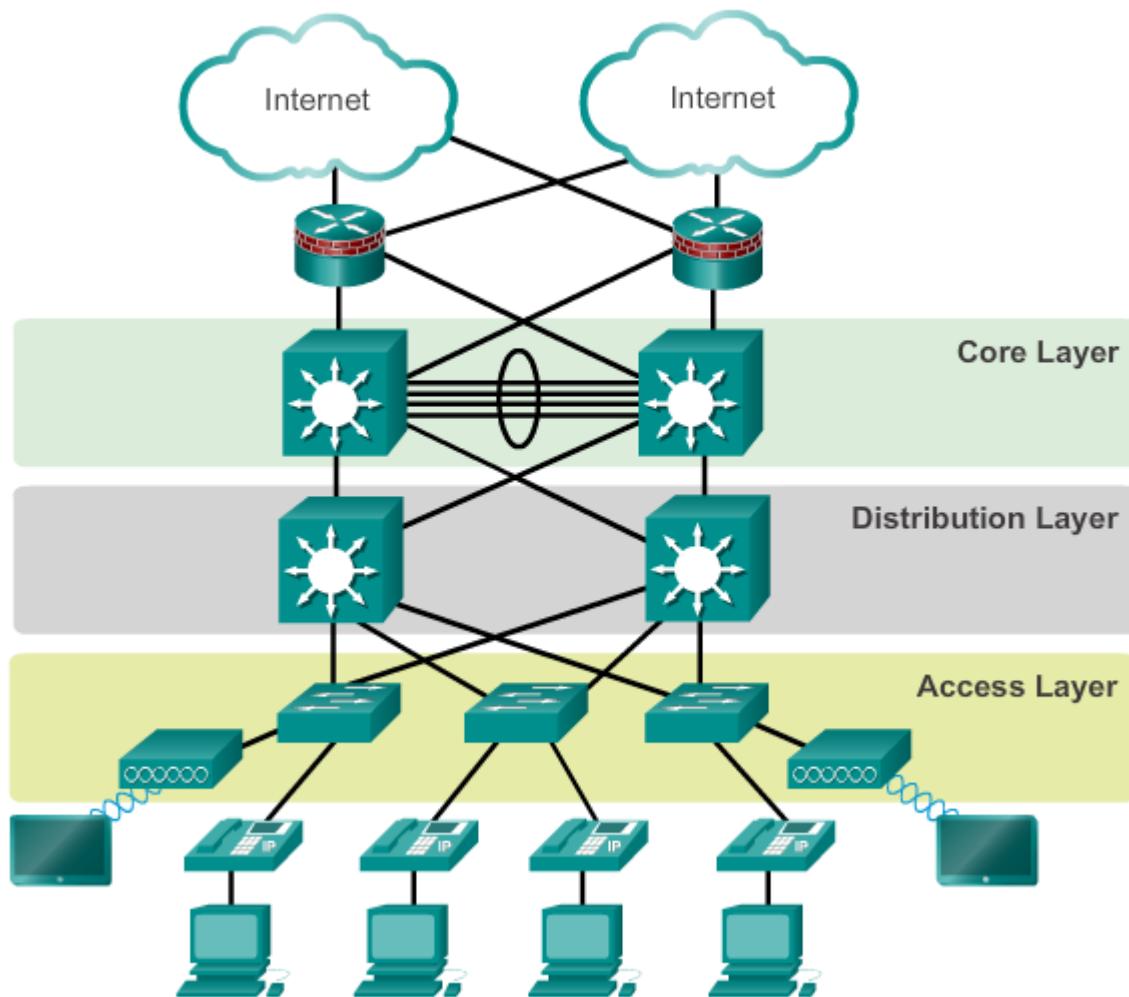
Cabling Topology

Topology: **hierarchical star** (star topology allows flexibility, the ring or bus topologies easy to be shaped as a star).

Center of the star is the **main cross connect** (MC), designed for the whole cabled area. Second hierarchical level, the **intermediate cross connect** (IC), belongs usually to one building from the cabling area.

The third level is the **telecommunication closet** (TC), associated to a floor from a building, or to a group of working rooms.

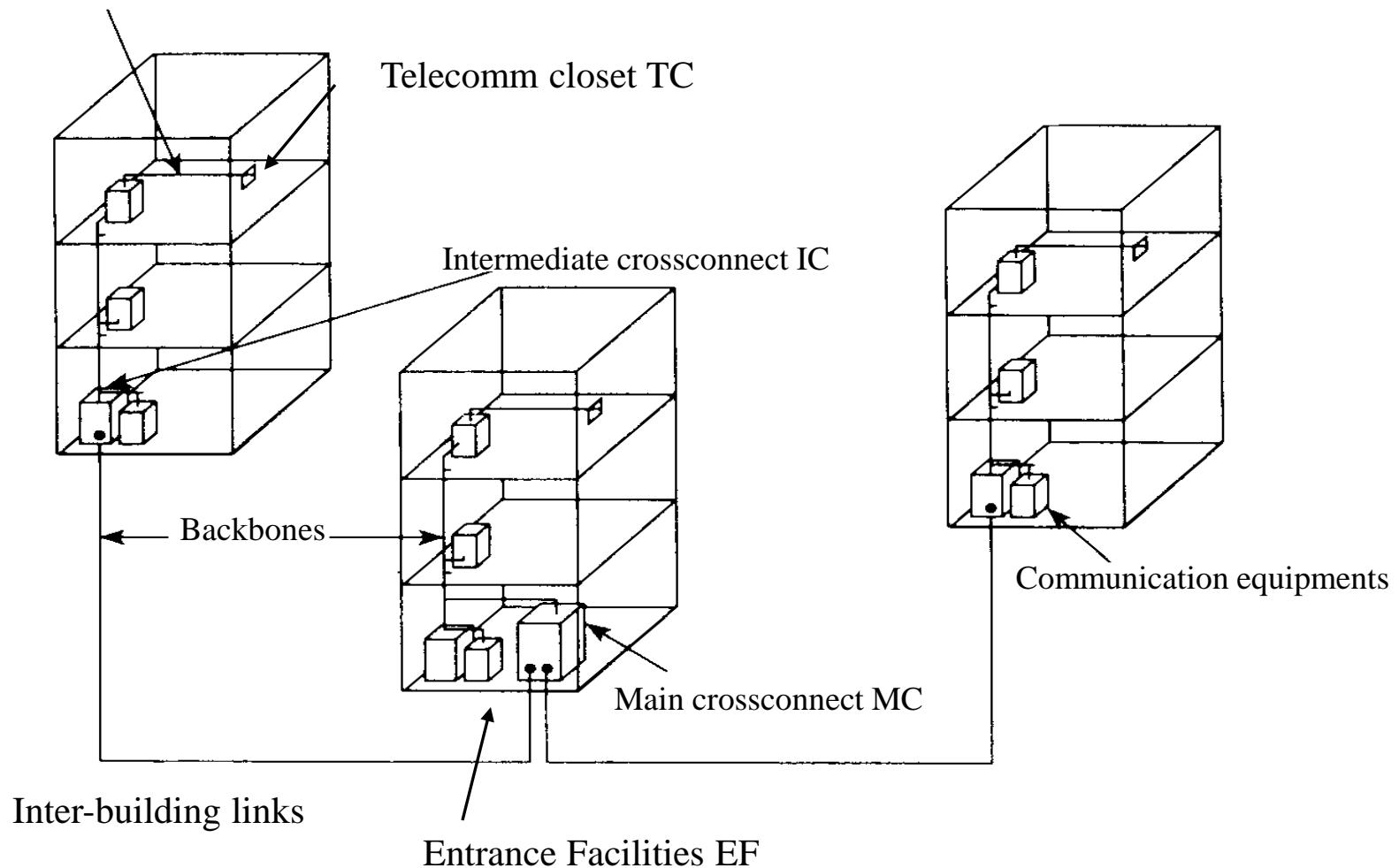
Hierarchical Design Model



Constitutive Cabling Components

- main crossconnect (MC)**-star center, a distribution center of main cables for other buildings or other cabling levels
- intermediate crossconnect (IC)**- local to each building, a ‘one by floor’ distribution closet
- telecommunication closet (TC)** – cabling toward workstations, more on a floor; contains the patch panels
- intrabuilding backbone** – cabling between ICs and local TCs
- interbuilding backbone** – cabling between MC and other buildings
- equipment room**, local to a cabling level; contains passive equipments (switching panels, cable ducts, measurement equip.), or active equip. like telephone central point, audio-video, LAN switches
- **interbuilding entrance facility**, interface between outside cabling and inside backbone, especially grounding facilities
- work area**, identifies workstations, associated patch + drop cables, adapters
- patch panels**, switching panels for coax or UTP, or barrel panels for fiber optic
- telecommunication outlets**, connect workstations to the cabling system
- cabling adapters**, both passive or active

Horizontal cabling



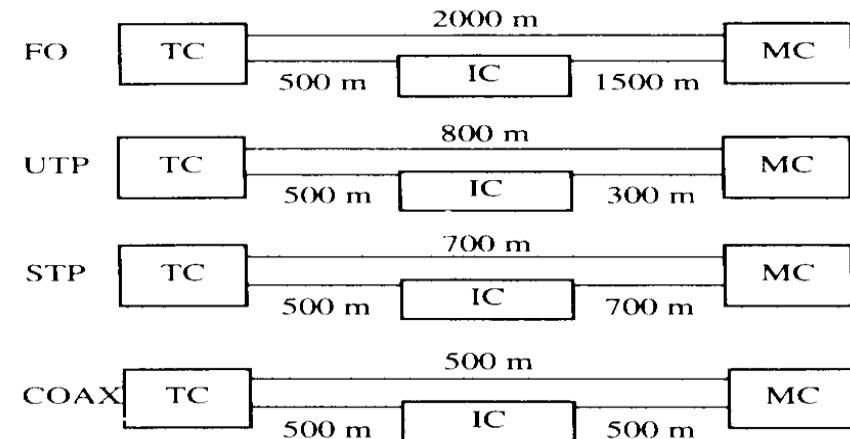
Transmission Media

Media accepted:

- coax cable** of 50ohm, known as normal Ethernet cable (less used today)
- multimode fiber** optic with the 62,5/125 μm diameters
- single-mode fiber** at 8,3/125 μm
- twisted pair cables**, either:
 - UTP (*unshielded twisted pair*) with an impedance of 100 Ω
 - STP (*shielded twisted pair*) with impedance of 150 Ω .

Vertical Cabling

Concerns inter & intra building backbones, specifying the maximum cable lengths, either directly from a TC to the MC, or using an IC

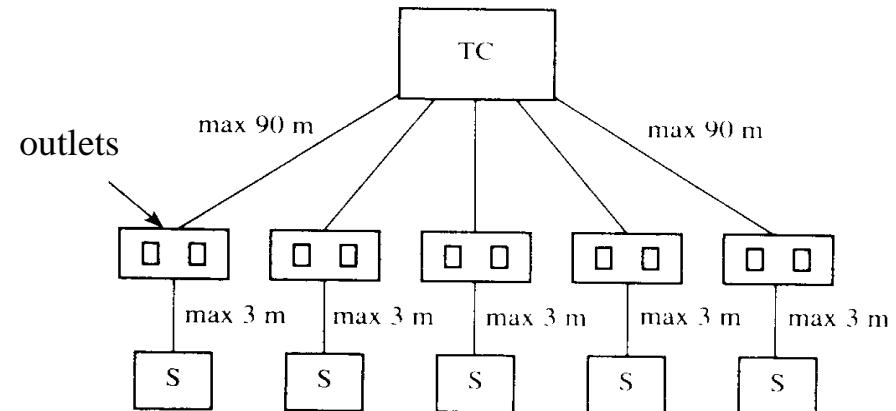


Horizontal Cabling

Specifies connections (cables, their allowed maximum lengths, connectors) between the workstations and the local distribution closet (TC); the figure shows the drop cables from the workstation to outlet and the runs from outlets to local TC.

Some types of used connectors:

- RJ45 connector for 4-wire UTP cables
- fiber optic connectors as ST and SC
- BNC connectors for coax
- hermaphrodite connector for STP



Installation Directives

- cable installation (maximum admitted force/cable, mechanical manner of connecting the wires)
 - under-carpet horizontal cabling (distance between power and data lines, necessary shielding)
 - ground protection for the electric wires or the specific protection for the fiber optics
- 3/27/2024

Cable identification

For each cable a label with an alphanumeric string, containing information about:

- the area within the building where cable is located
- the number of the floor where is located the local distribution closet
- the numerical identifier of the workstation
- the numerical identifier of the local distribution closet.

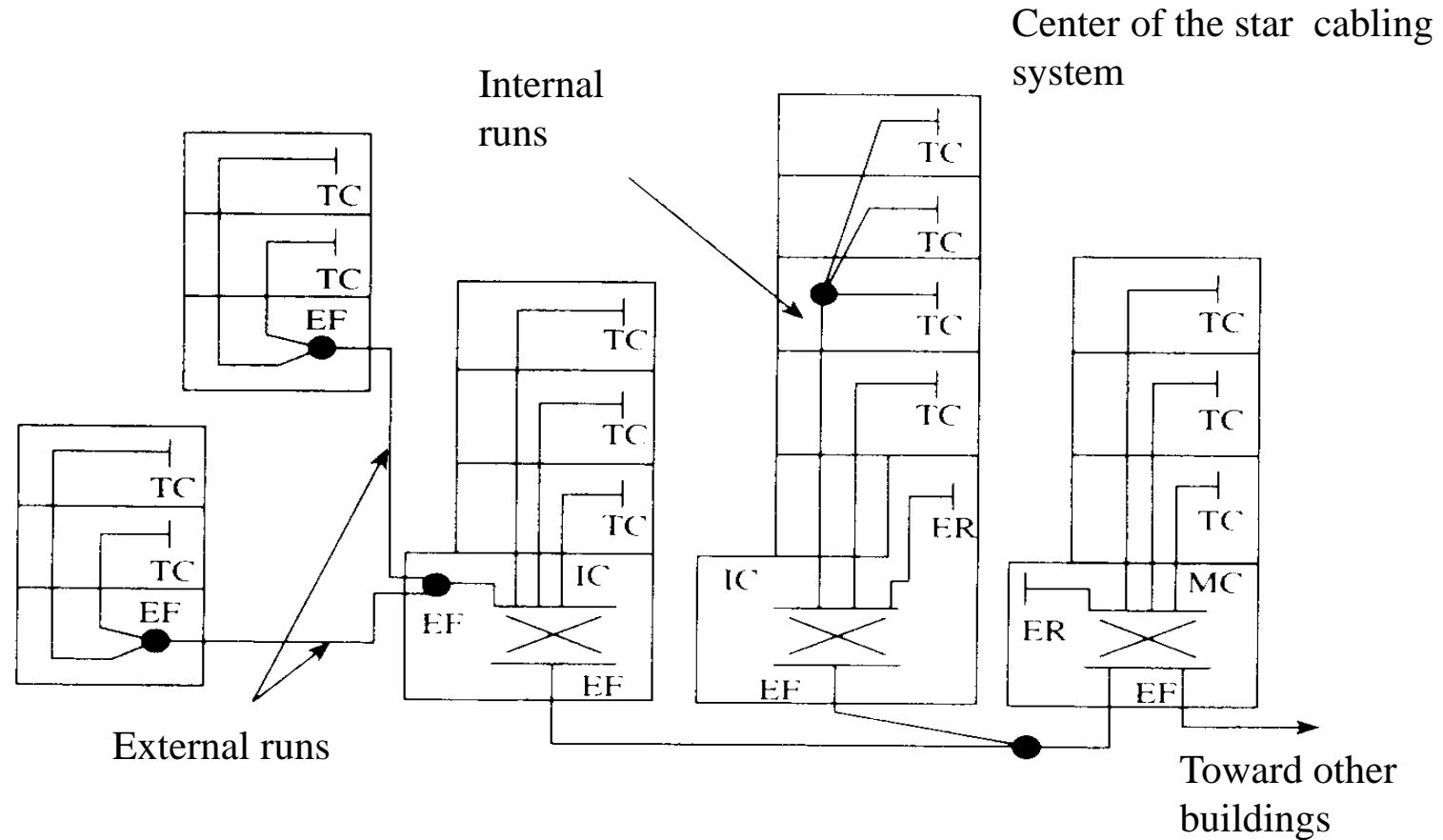
Project Documentation

Use of standard terminology and notations.

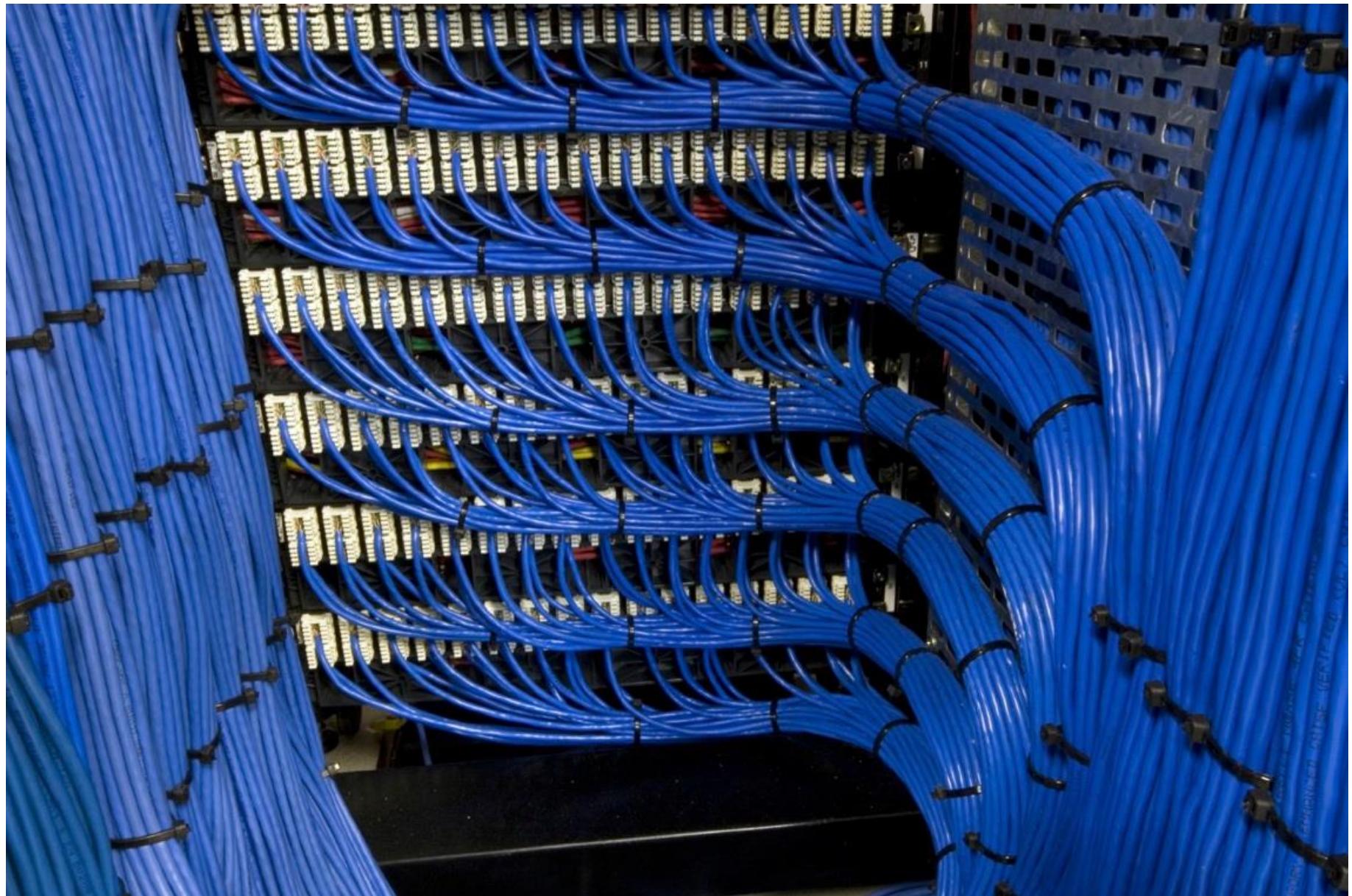
Must include:

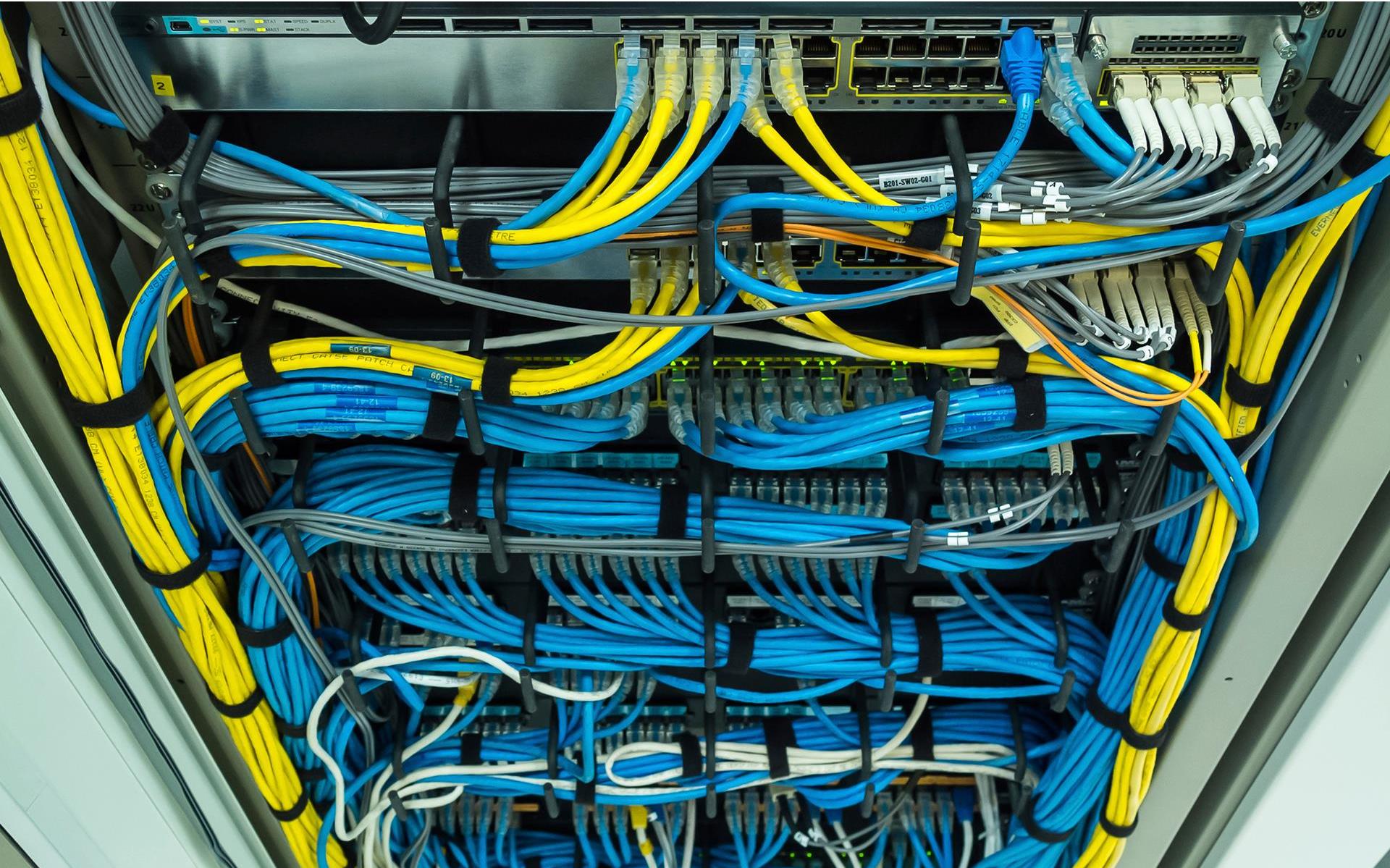
- the logic drawing of the cabling system
- the table for the vertical runs identification
- the table for each local distribution closet, for a complete cable identification.

Logic drawing of cabling

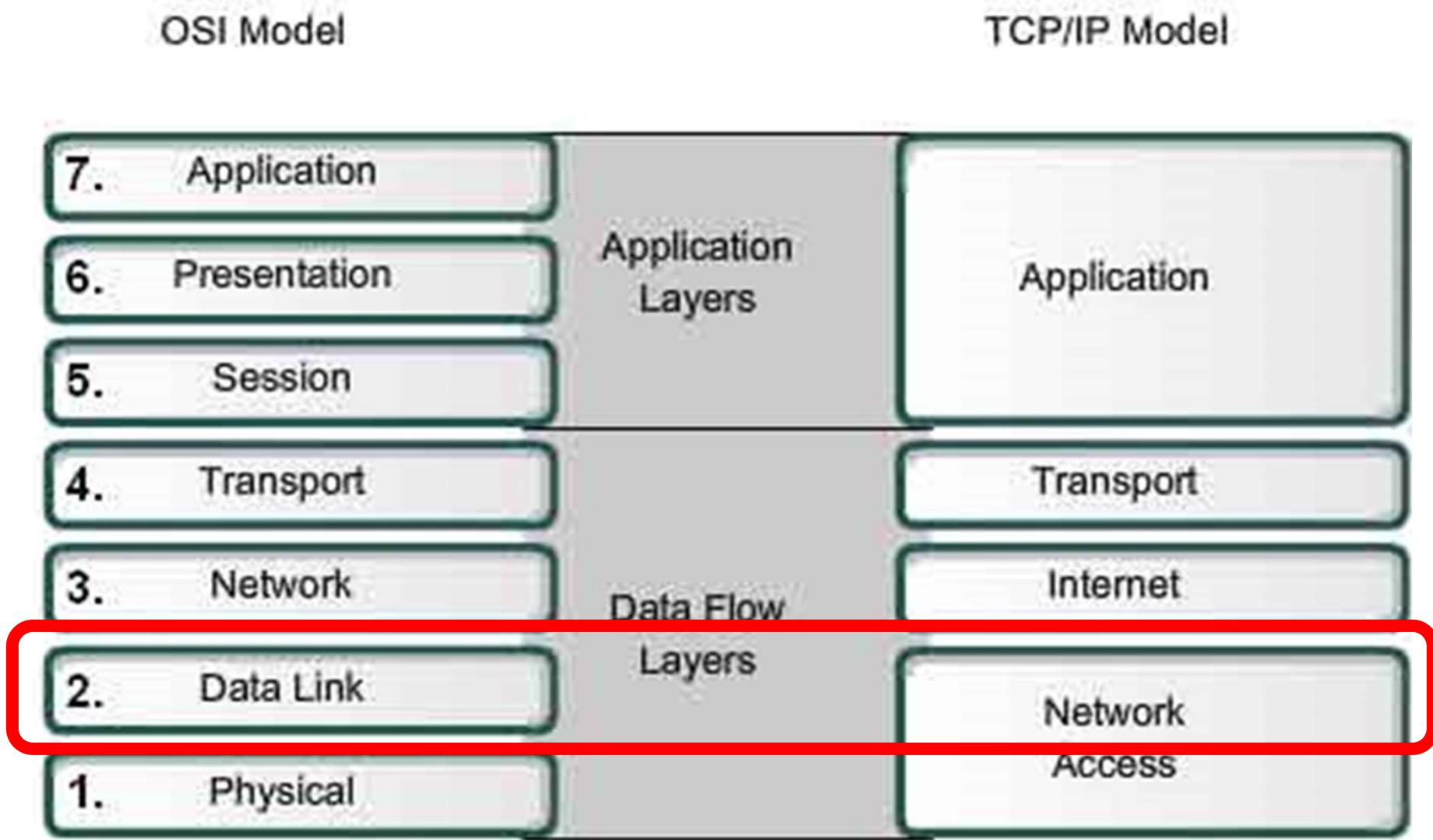






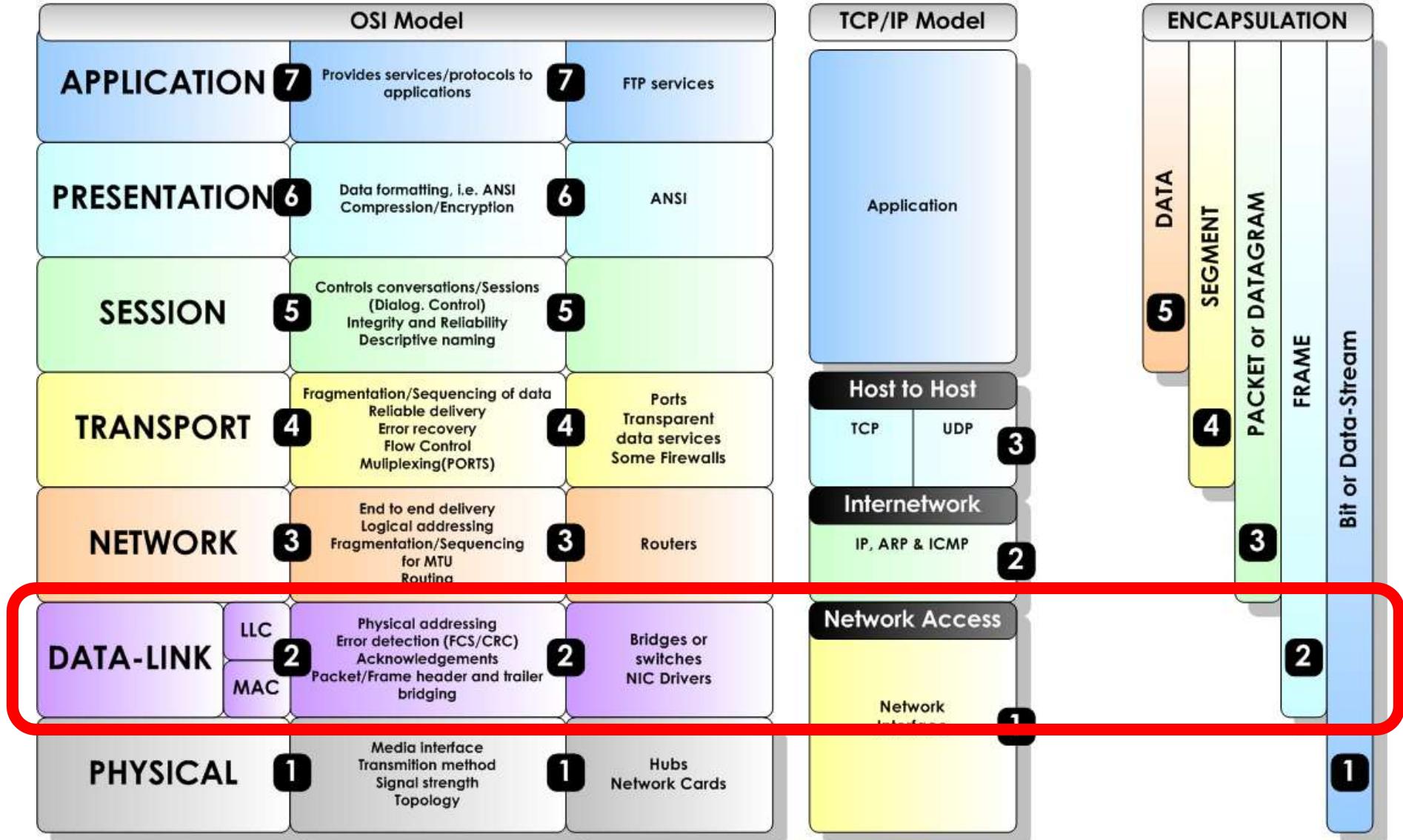






The OSI Model (Open Systems Interconnection)

© Copyright 2008 Steven Iveson
www.networkstuff.eu



Data Link Control

On layer 1 (ISO/OSI) **physical** aspects of transmissions, or **how transmit signals on a transmission link**.

How control and manage the information exchange? Adding a little logic above the physical interface!

Follows the **Data Link** layer, concerned on **how to send data over a data communication link**.

Data unit at this level: the **frame**. Problems arising with frames transmission:

-frame synchronization

-flow control

-error control

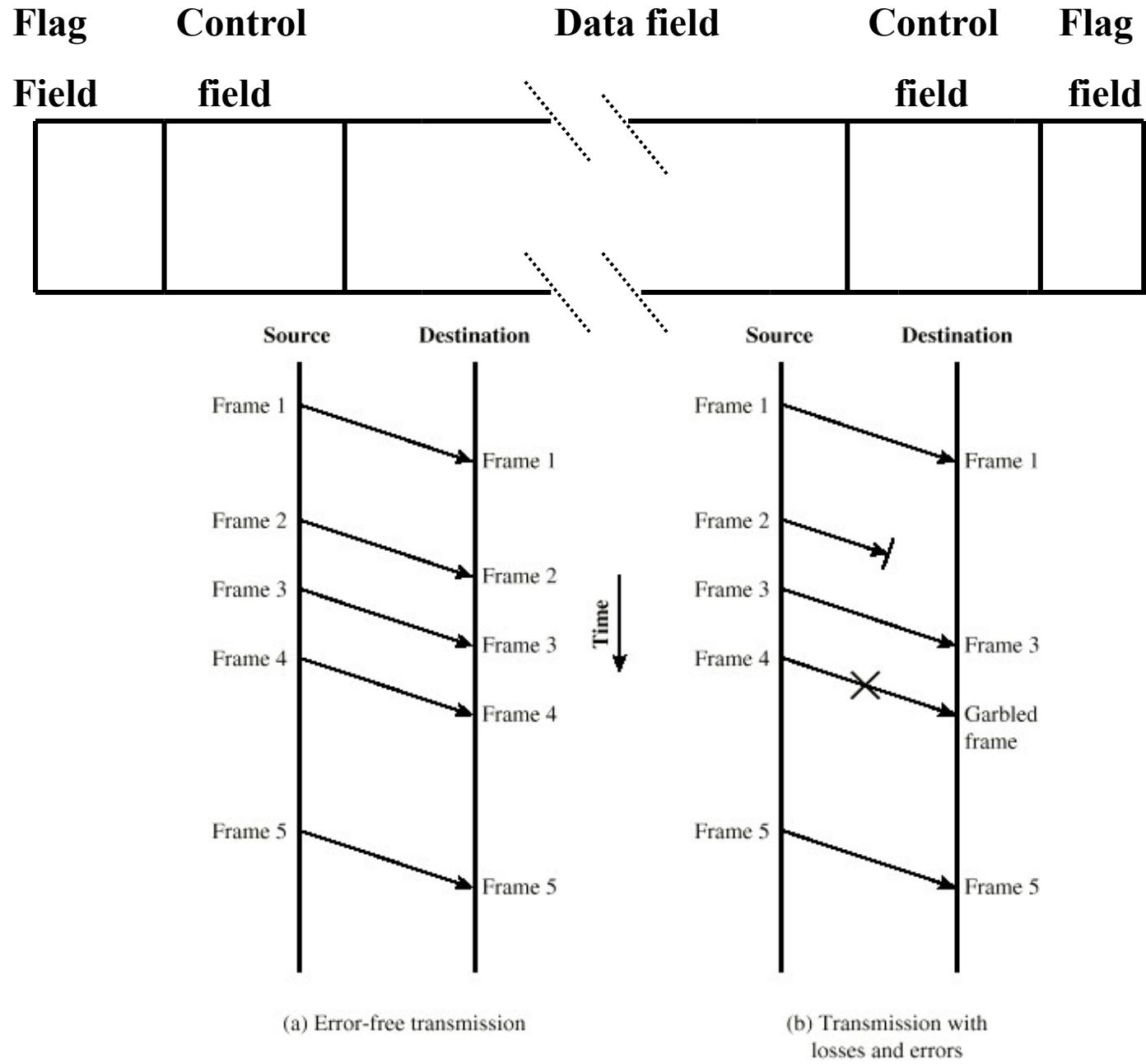
-addressing

-carrying data and control on a single link

-link management

Frame synchronization

Beginning and end of frames need be detected => special synchronization fields, **flag** fields; may exist for both parts, also may use inter-frame transmission gap, instead of end flag.



Flow Control

Technique ensuring the sending entity does not overwhelm the receiving entity, i.e. the receiver's data buffer doesn't fill up and overflow.

Temporal parameters used for transmission control:

Transmission time - time taken for a station to emit all bits into medium

Propagation time - time taken for a bit to traverse the link, from source to destination stations.

Flow Control Techniques

Stop and Wait

Sliding Window

Stop-and-Wait Flow Control Protocol

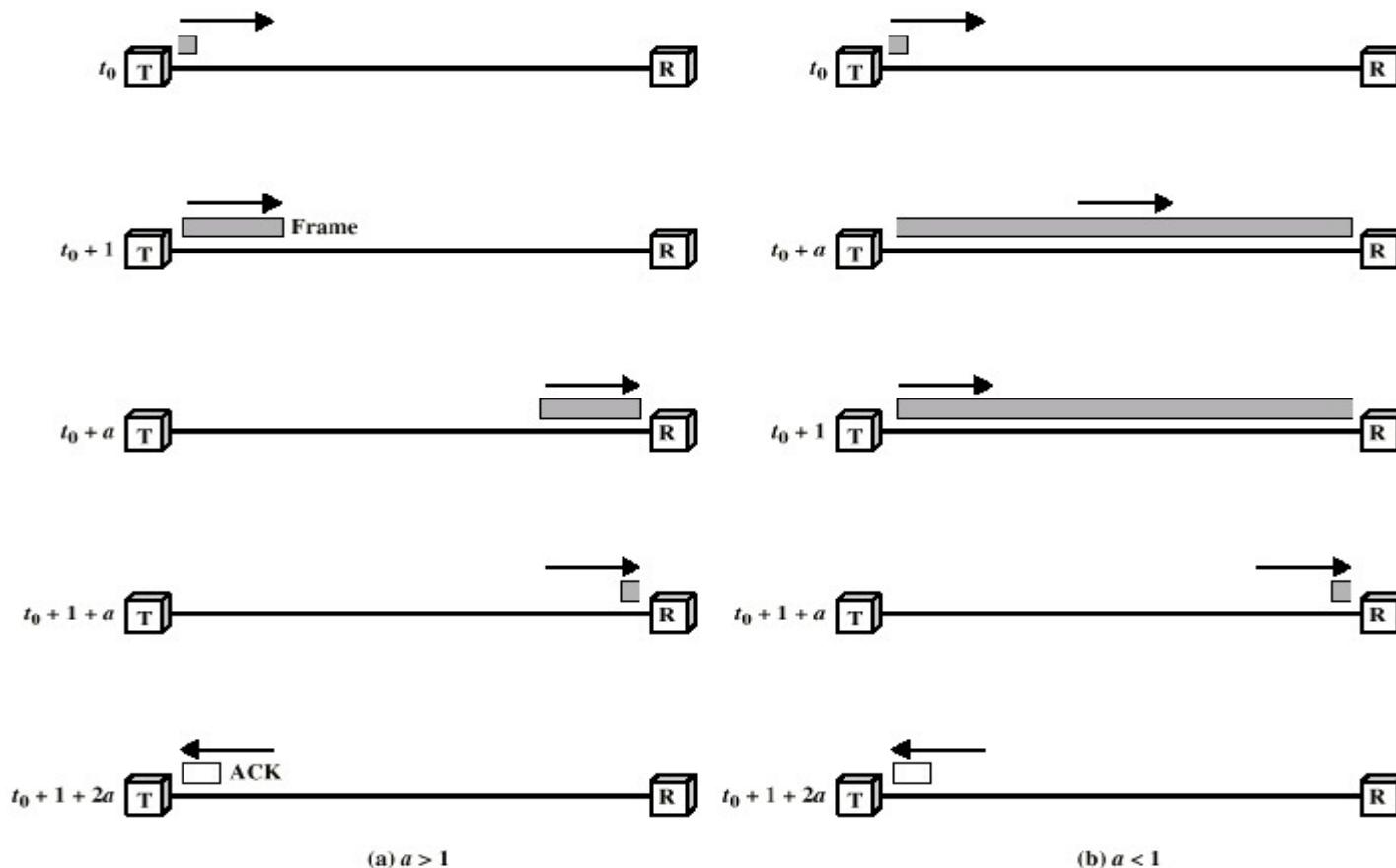
Algorithm steps:

- Source transmits a frame
- Destination receives frame and, if wants to continue, replies back with an acknowledgement (ACK) for that frame
- Source waits for ACK before sending next frame.

Protocol characteristics:

- Destination can stop the data flow by not sending ACK
- Works well for a few large frames; that's why use of frame fragmentation, i.e. large block of data may be split into small frames. It necessitates because:
 - Limited buffer size at destination
 - Errors detected sooner (when whole frame received)
 - On error, retransmission of smaller frames is needed
 - Prevents one station occupying medium for long periods (problem in LANs)

When use of multiple frames for same message, Stop and wait algorithm becomes inadequate, data link being not efficiently used. When propagation time \gg transmission time (high data transmission speed or long distance) the line is under-utilized.



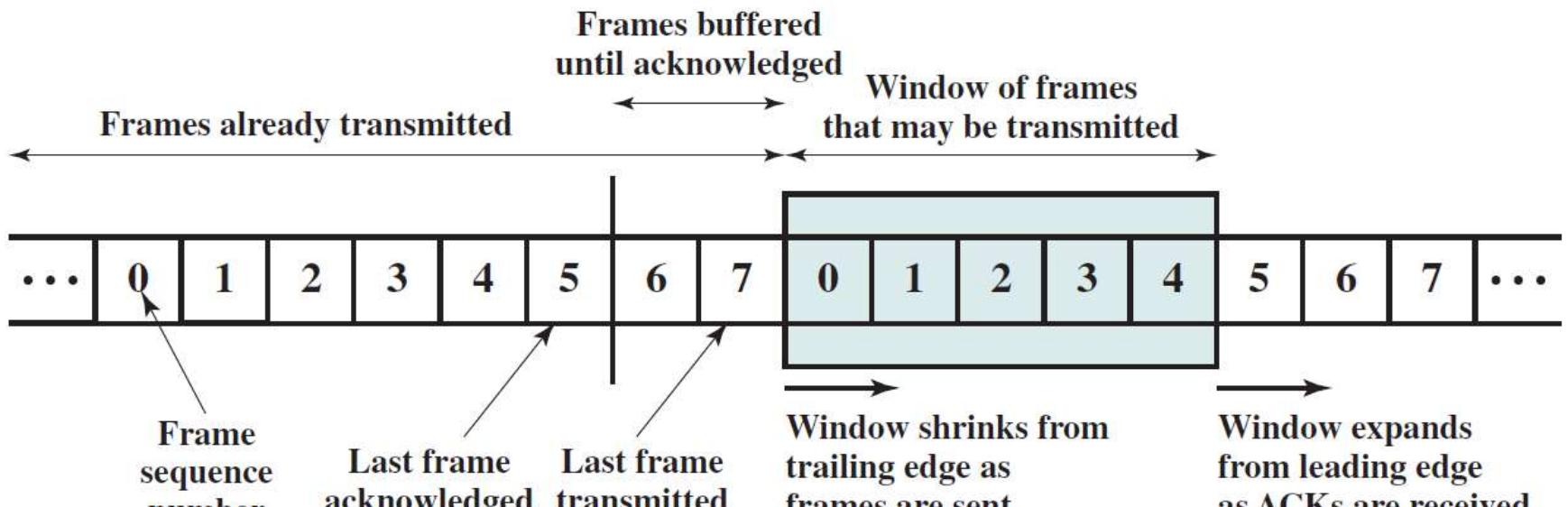
Stop-and-Wait Link Utilization (transmission time = 1; propagation time = a)

Sliding Windows Flow Control

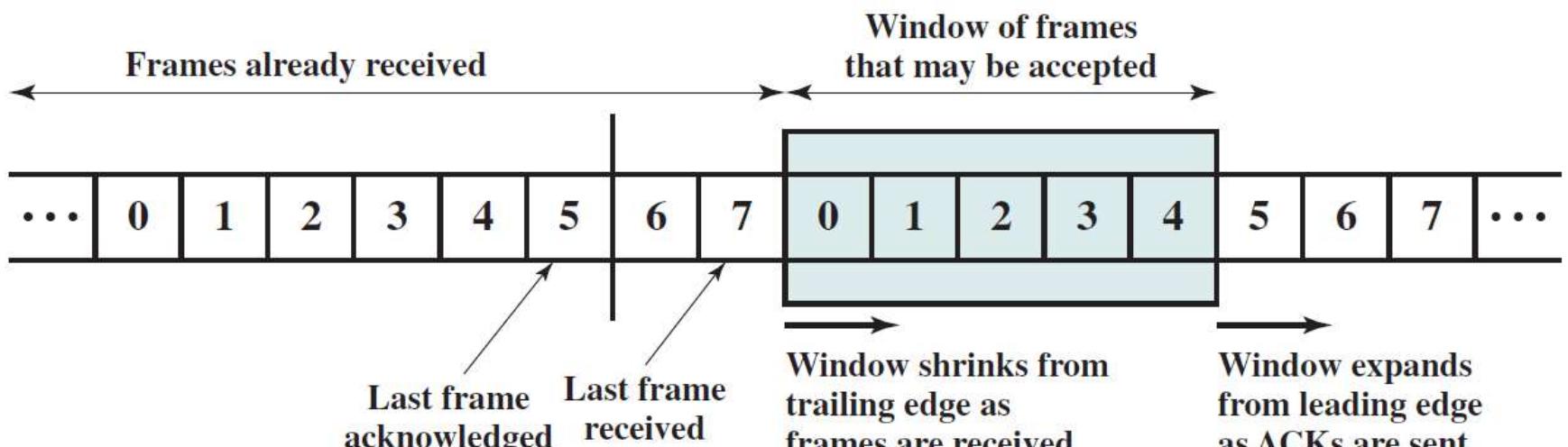
Allows for multiple frames to be in transit on the link. Efficient algorithm for full duplex links and speedy transmissions.

Main hints for algorithm:

- Receiver has buffer W long
- Transmitter can send up to W frames without waiting for ACK
- for keeping track of acknowledged frames, each frame is numbered by the sender
 - the receiver sends ACK frame, including number of *next frame expected*
 - Sequence number is bounded by the size of control field in the frame (k), so frames are numbered modulo 2^k
 - the window size usually smaller
 - Sender maintains a list with the sequence numbers it is allowed to transmit, the receiver maintains a list with the sequence numbers it is prepared to receive; so a *window* of frames; operation referred as sliding-window flow control



(a) Sender's perspective



(b) Receiver's perspective

F0 – F7: normal data frames

RRn: ack frames (Receive ready), where **n** the number of the next frame expected at receiver
A form of ‘negative acknowledgment’, like RNRn (Receive not Ready), acts as ACK for former frames, but forbidding transfer of future frames; transmission cut-off.

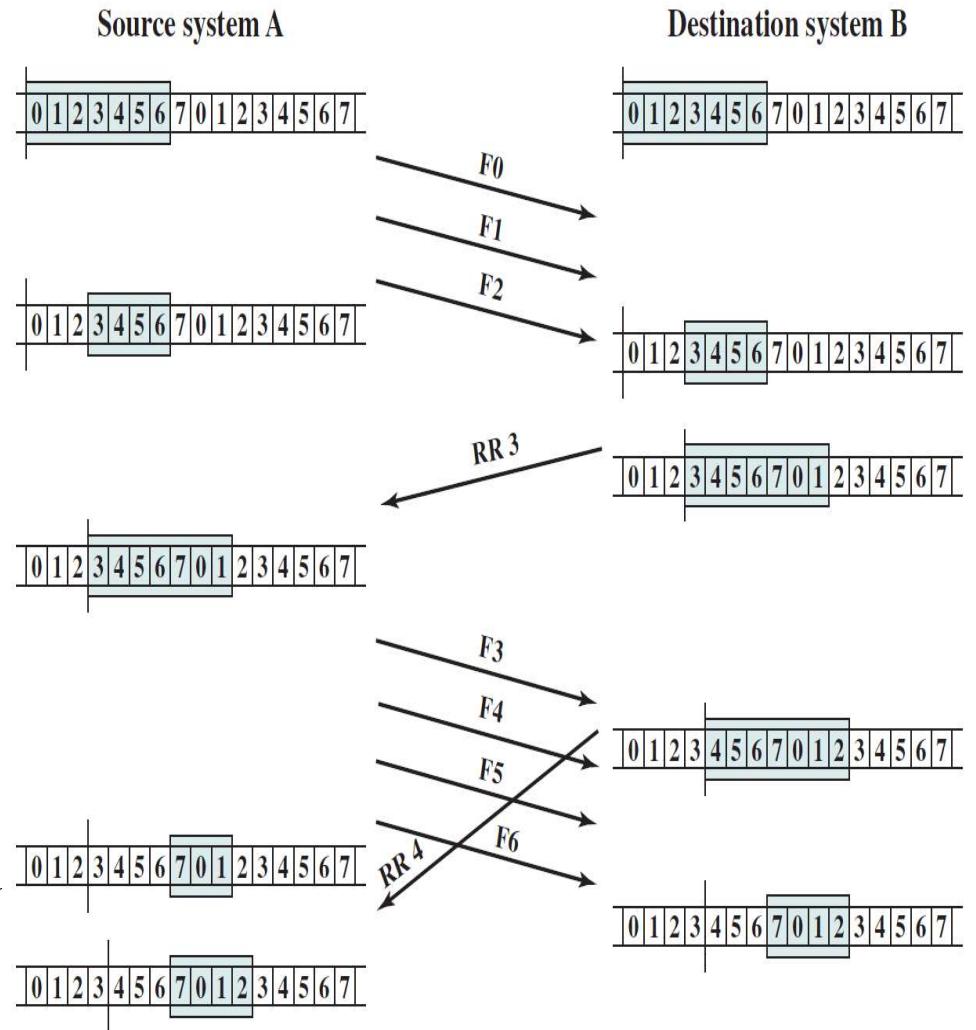
Resume with a positive ACK.

When bidirectional transmissions, both stations implement 2 windows.

The ACK information may be sent as special frames (RR, RNR), or be embedded in data frames, for transmission efficiency (piggybacking) => frame has special fields carrying it's own frame sequence number and sequence number used for counterpart acknowledgement.

2/22/2021

Vasile Dadarlat - Local Area
Computer Networks



Error Detection

Even the media is secure, data error may occur, with different probabilities. The error may affect one bit (bit error rate), affect more bits, and error may be (or not) **detected** by the receiver. ***Detection doesn't imply correction!***

Use of *additional bits*, added by transmitter, for implementing an error detection code, calculated as a function of transmitted bits. Error-detection code functions need be known by both transmission parts. Receiver performs same calculation over received bits and compares the results (its error detection code with that arrived from the sender). If mismatch, a detected error occurs!

Parity Check

Simplest method, cheap and easy to implement: append a parity bit at the end of a block of data (ex.: a character), in such that the entire block (character) – after appending- has an even (even parity) or odd (odd parity) number of ones.

Works well for one damaged bit, or an even number of them, but can't detect an odd number of damaged bits.

Odd Parity used for asynchronous transmissions, Even Parity usually for synchronous transmissions.

Cyclic Redundancy Check (CRC)

Very powerful; acts as it follows:

For a block of k bits (the original message), transmitter generates a n bit sequence, known as *frame check sequence* (FCS).

The entire frame becomes $k+n$ bits, which is exactly divisible by some number (predetermined divisor)

Receiver divides frame by that number

If no remainder, assume no error!

Predetermined divisor, represented as polynomials (variable X) is one of the CRC polynomials:

$$\text{CRC-12} = X^{12} + X^{11} + X^3 + X^2 + X + 1$$

$$\text{CRC-16} = X^{16} + X^{15} + X^2 + 1$$

$$\text{CRC-CCITT} = X^{16} + X^{12} + X^5 + 1$$

$$\text{CRC-32} = X^{32} + X^{26} + X^{23} + X^{22} + X^{16} + X^{12} + X^{11} + X^{10} + X^8 + X^7 + X^5 + X^4 + X^2 + X + 1$$

Error Control

Means not only error **detection**, but also **correction** of detected errors

In transmission of frames, there are some types of errors:

Lost frames

Damaged frames

Mechanisms for controlling frame errors: **Automatic repeat request (ARQ)**, based on:

Error detection

Positive acknowledgment

Retransmission after timeout

Negative acknowledgement and retransmission

Role of ARQ: turn a potentially unreliable data link into a reliable one

Versions of ARQ:

Stop-and-wait ARQ

Go-back-N ARQ

Stop and Wait ARQ

Based on stop-and-wait flow control. Steps:

- Source transmits one single frame
- Stops and Wait for ACK

May have two kind of errors:

If received frame is damaged, receiver discards it

- Transmitter has timeout
- If no ACK within timeout, source retransmits frame (need for a frame copy)

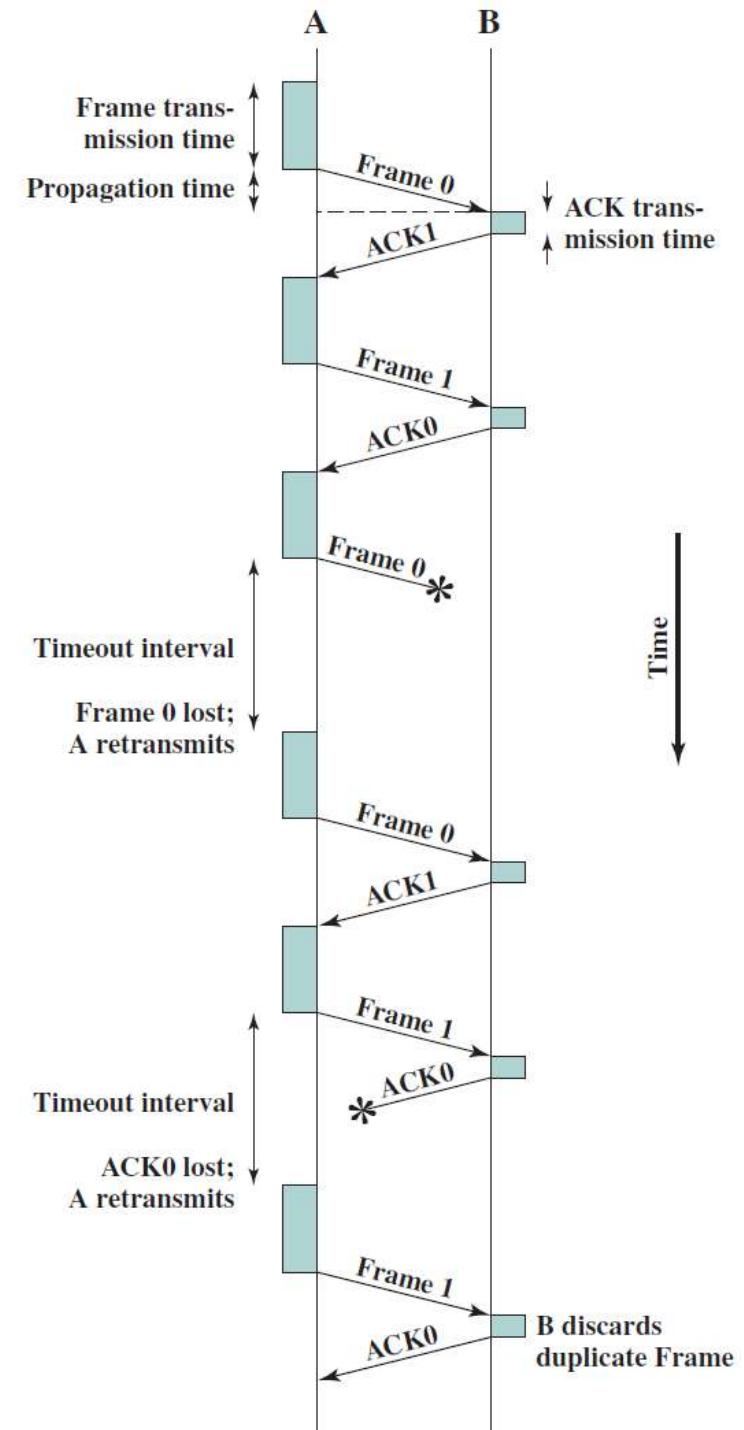
If ACK damaged, transmitter will not recognize it

- Transmitter will retransmit
- Receiver gets two copies of same frame, as if they were separated

Alternative frame labelling (1 and 0), so use of ACK0 and ACK1

2/22/2021

Vasile Dadarlat - Local Area
Computer Networks



Stop and Wait ARQ: simple but not efficient

Go Back N ARQ

Based on sliding window flow control => frames numbered sequentially modulo the window size.

Steps are:

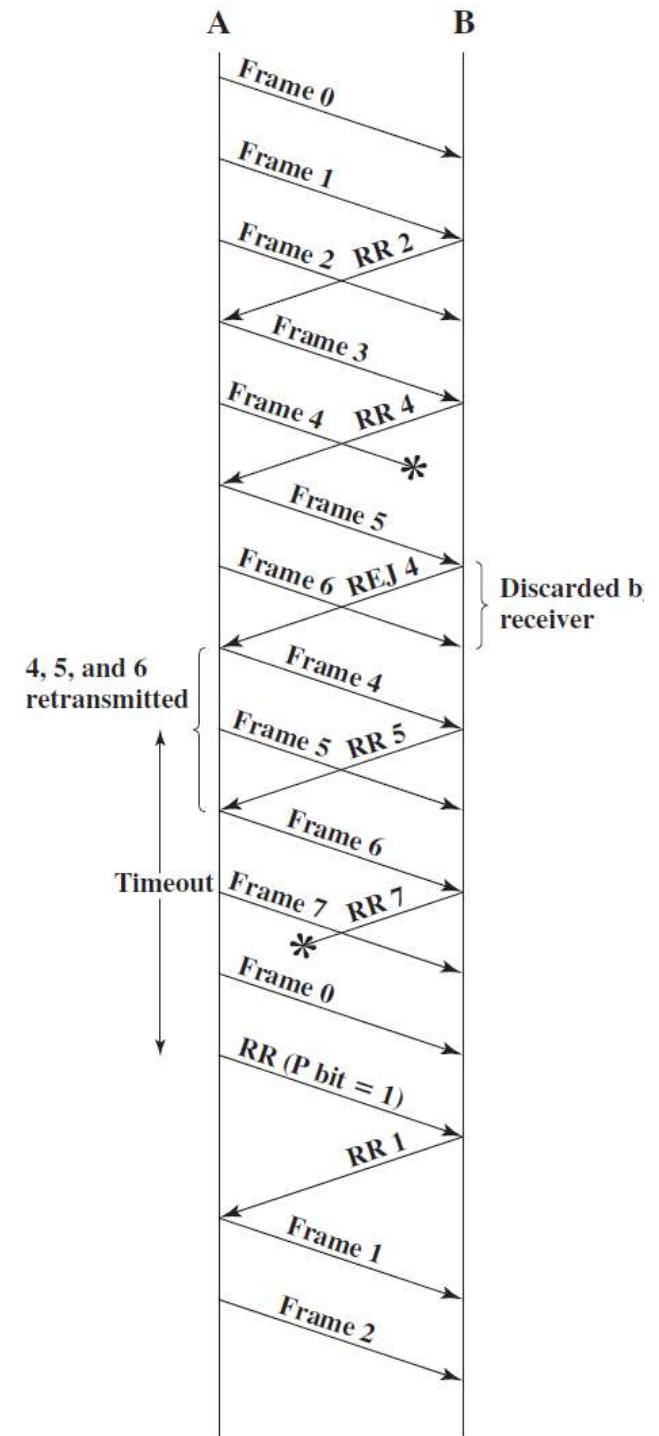
- If no error, ACK used as usual, carrying number of next frame expected (RRn, or piggybacking); use window to control number of outstanding frames

- If error, reply with rejection (RNrn or REJn, or piggybacking)

- Receiver discards that frame and all future frames, until erroneous frame received correctly

- Transmitter must go back and retransmit that frame and all subsequent frames

Need for buffers at the sender and receiver.



Go Back N - *Damaged Frame*

Receiver detects error in frame 4

Receiver sends rejection-4

Transmitter gets rejection-4

Transmitter retransmits frame 4 and all subsequent

Go Back N - *Lost Frame* – case 1

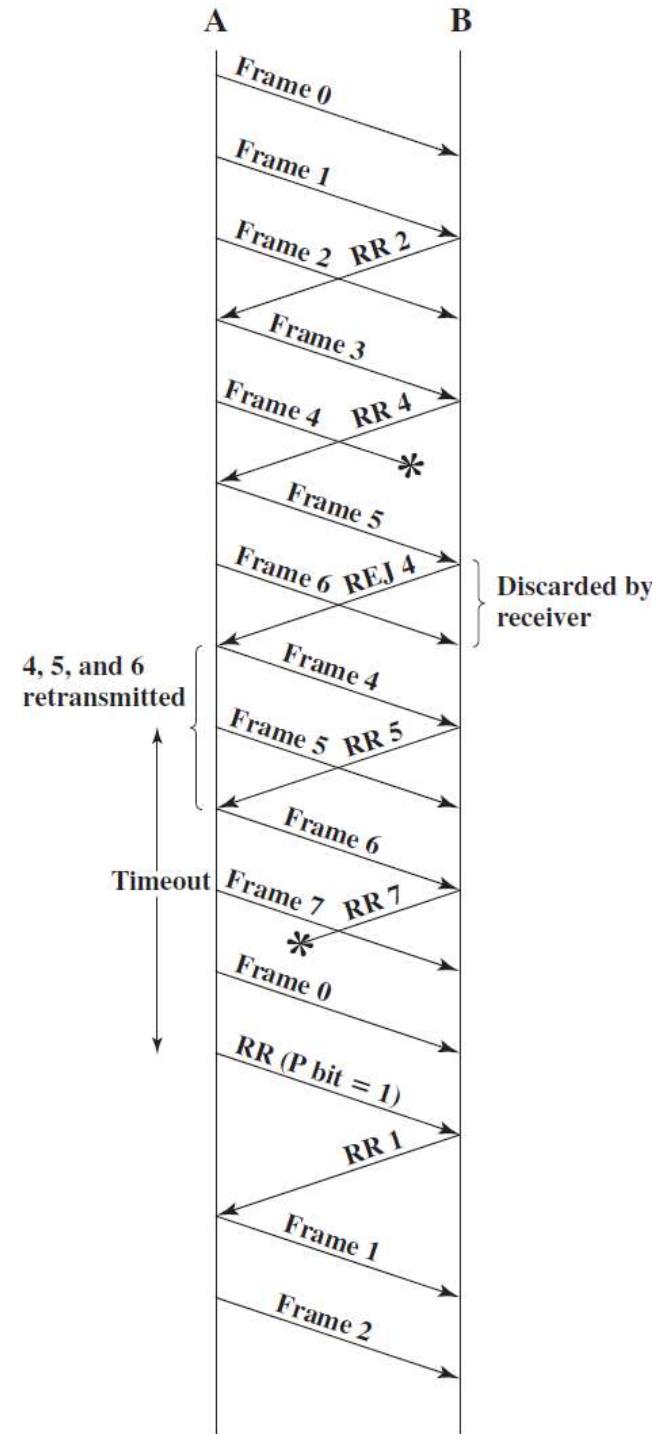
Frame i lost, so no feedback from receiver

Transmitter sends $i+1$

Receiver gets frame $i+1$ out of sequence

Receiver send reject i

Transmitter goes back to frame i and retransmits all subsequent frames



Go Back N - *Lost Frame* case 2

Frame i lost and no additional frame sent

Receiver gets nothing and returns neither acknowledgement nor rejection

Transmitter times out and sends a special acknowledgement frame with P bit set to 1

Receiver interprets this as command which it acknowledges with the number of the next frame it expects (frame i)

Transmitter then retransmits frame i

Go Back N - *Damaged Acknowledgement*

Receiver gets frame i and send acknowledgement ($i+1$) which is lost

Acknowledgements are cumulative, so next acknowledgement ($i+n$) **may arrive** before transmitter times out on frame i

If transmitter times out, it sends acknowledgement with P bit set, as before

This can be repeated a number of times before, and if successive failures, a reset procedure is initiated

Go Back N - *Damaged Rejection*

As for lost frame (2)

Selective Reject ARQ

Also called selective retransmission; Steps are:

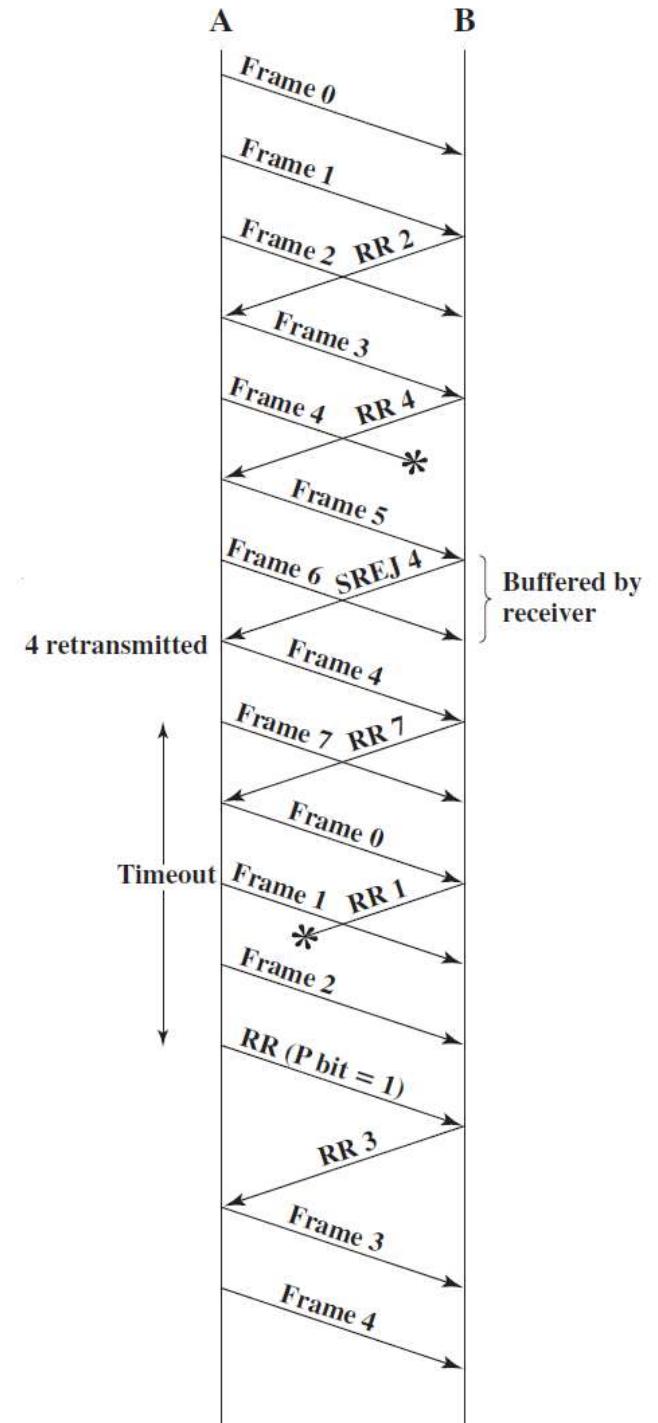
- Only rejected frames are retransmitted
- Subsequent frames are accepted by the receiver and buffered, till valid frame received
- Reordering of frames

Advantages:

- Minimizes retransmissions

Complexity:

- Receiver must maintain large enough buffer
- More complex logic in transmitter (selective choose and retransmission of erroneous frame)



Data Link Control Protocols

Early DL control protocols – character oriented: IBM's BISYNC, ARPA's IMP-IMP

Now bit-oriented protocols: IBM's **SDLC** (Synchronous Data Link Control), modified by ISO 4335 standard and becoming **HDLC** (High-level Data Link Control).

HDLC (High-level Data Link Control)

Basic characteristics:

-Station Types

-Primary station

Controls operation of link

Frames issued are called commands

Maintains separate logical link to each secondary station

-Secondary station

Under control of primary station

Frames issued called responses

-Combined station

May issue commands and responses

- Link Configurations

-Unbalanced

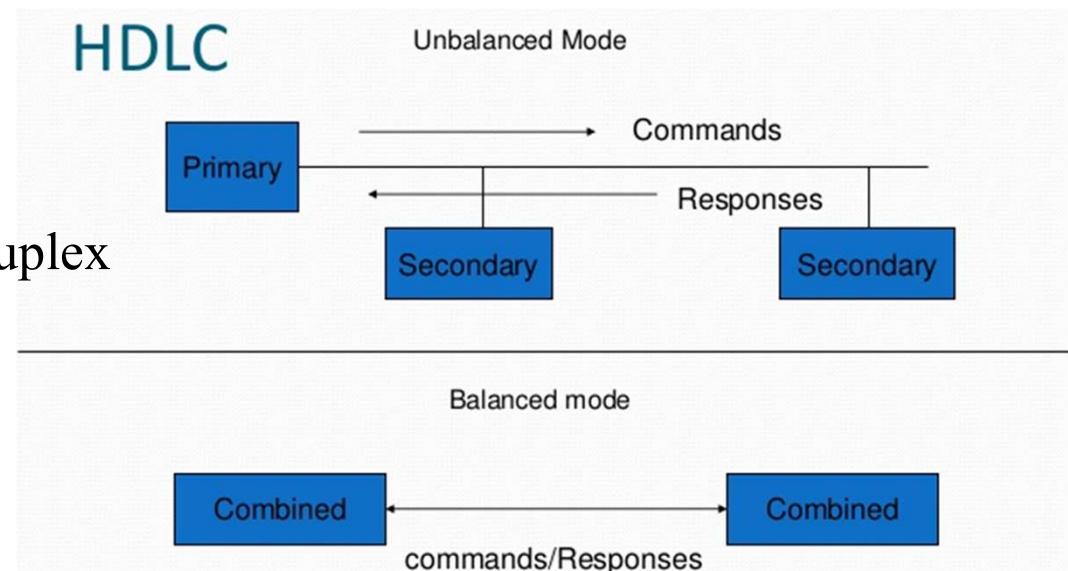
One primary and one or more secondary stations

Supports full duplex and half duplex

-Balanced

Two combined stations

Supports full duplex and half duplex



-Transfer Modes

- Normal Response Mode (NRM)
- Asynchronous Balanced Mode (ABM)
- Asynchronous Response Mode (ARM)

Normal Response Mode (NRM)

- For unbalanced configuration
- Primary station initiates transfer to secondary station(s)
- Secondary may only transmit data in response to command from primary
- Primary ***polls*** secondary for transmitting

Used on multi-drop lines and daisy-chain polling; host computer as primary, terminals as secondary

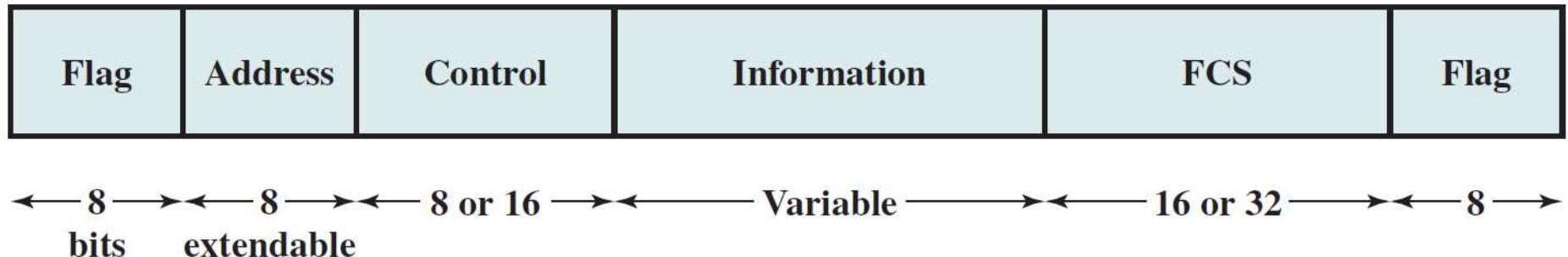
Asynchronous Balanced Mode (ABM) - *most widely used*, no polling overhead

- Balanced configuration (combined stations)
- Either station may initiate transmission without receiving permission

Asynchronous Response Mode (ARM)

- Unbalanced configuration
 - Secondary may initiate transmission without permission from primary
- Primary responsible for line management, ***rarely used*** method.

Frame Structure Diagram



HDLC uses synchronous transmission => synchronization fields

All transmissions at the DL level are done using frames

Single frame format for all data and control exchanges

Frame contains a *header* and a *trailer*, information embedded between them.

Header = **Flag + Address + Control** fields

Trailer = **FCS + Flag** fields

FCS (Frame Control Sequence), using CRC error control

Flag Fields

Delimit frame at both ends, used for frame sequence synchronization; receiver hunts for flag sequence to synchronize

Normal pattern: 0111110 (six ones between zeros)

What to do when data contains this pattern?

Bit stuffing used to avoid confusion with data containing 0111110, and to assure data transparency.

Rule:

0 inserted after every sequence of five 1s at the sender part.

If receiver detects five 1s it checks next bit:

if 0, it is deleted;

if 1 and seventh bit is 0, accept as flag

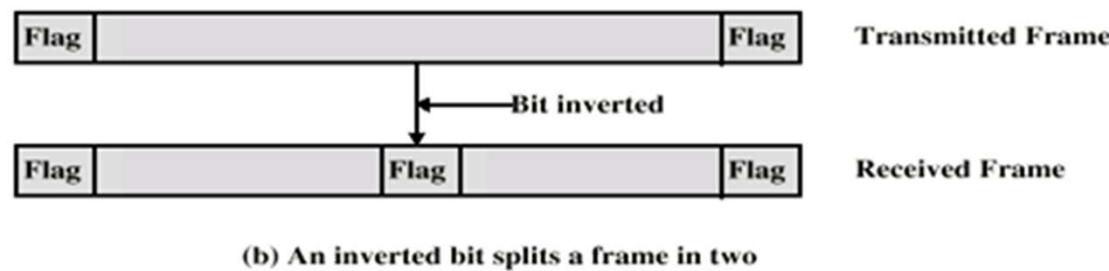
if sixth and seventh bits 1, sender is indicating abort (severe error)

Original pattern:

1111111111101111110111110

After bit-stuffing:

1111101111101101111101011111010



Address Field

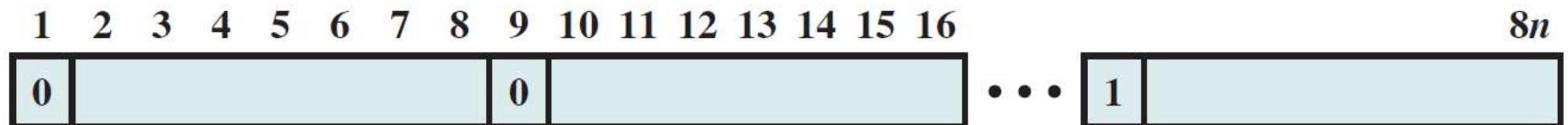
Usually 8 bits long, indicating the secondary station having transmission or to receive frame. Not useful for point-to-point links.

Usually 8 bits enough for addressing 255 secondary stations, even 127 when 7 bits used.

Address field may be extended to multiples of 7 bits, using an ‘*a priori*’ rule:

LSB of each octet indicates that it is the last octet (if 1) in the string, or not (if 0)

Special address for all stations: all ones (11111111) is **broadcast** address.



Control Field

HDLC defines three types of frames, with different control formats

Information (I-frame): data to be transmitted to user (next layer up)

Flow and error control piggybacked on information frames

Supervisory (S-frame): control for ARQ when piggyback not used

Unnumbered (U-frame): supplementary link control, if needed

Bit significance:

First one or two bits of control field identify **frame type** (bit 1, or 1 and 2)

Poll/Final Bit, used on the context:

-if Command frame, means P (Polling bit), value 1 to solicit (poll) response from peer

-if Response frame, means F (Final bit), value 1 indicates the end of the response sequence to soliciting command

Sequence bits:

$N(S)$ – frame's sequence number at transmitter

$N(R)$ – frame's sequence number at receiver, means piggybacked ACK

	1	2	3	4	5	6	7	8
I: Information	0		$N(S)$		P/F		$N(R)$	
S: Supervisory	1	0	S		P/F		$N(R)$	
U: Unnumbered	1	1	M		P/F		M	

8-bit control field format

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Information	0			$N(S)$				P/F						$N(R)$		
Supervisory	1	0	S	0	0	0	0	P/F						$N(R)$		

16-bit control field format

Supervisory bits S, coding following commands and responses:

- 00: Receive Ready – station ready for receiving or acknowledgement for N(R)
- 01: Reject – retransmission request for messages starting with sequence number N(R)
- 10: Receive Not Ready – acknowledgement for messages till N(R-1), but no more able to receive
- 11: Selective Reject – retransmission request for message N(R)

Unnumbered function bits – M fields (2+3 bits): for further developments, allowing 32 control or response functions; may suffer further extensions.

Examples of coded commands/responses:

- 11000: set ARM (Asynchronous Response Mode)
- 00001: set NRM (Normal Response Mode)
- 11100: set ABM (Asynchronous Balanced Mode)
- 11011: set NRME (Normal Response Mode Extended)

For more commands/responses see references (ex. Stallings, 6th ed., pp.218)

Information Field

Carries user data; only in information (I-frame) and some unnumbered (U) frames

Must contain an integral number of octets

Variable length

Frame Check Sequence Field (FCS)

Error detection field; applies over Control and Information field

16 bit CRC (usually CRC-CCITT)

Optional 32 bit CRC (CRC-32), if info field length and link reliability calling for.

HDLC Operation

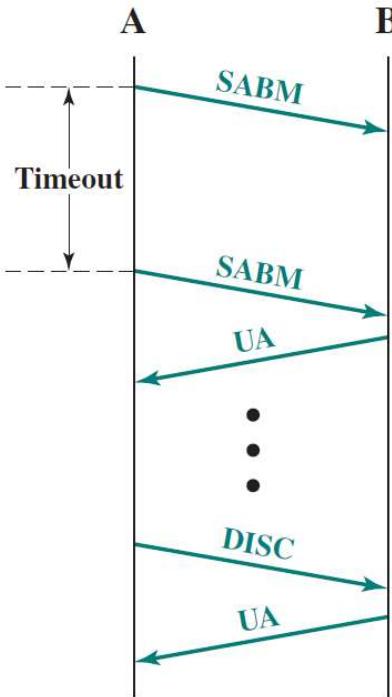
Consist in exchange of information, supervisory and unnumbered frames between the data link stations.

Any HDLC operation has three phases:

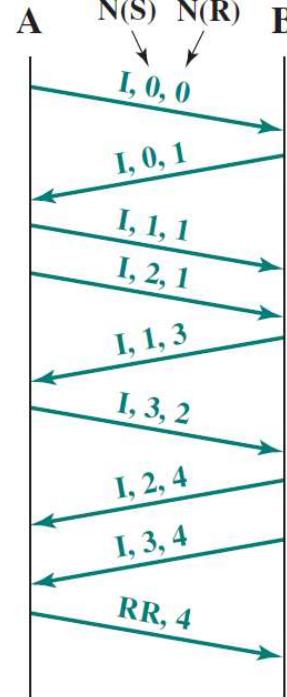
Initialization, requested by any side, using a set-mode command; after this, if operation accepted by other side, a logical connection is established

Data transfer, using data carrying I-frames, but also for flow and error control purposes, use of S-frames

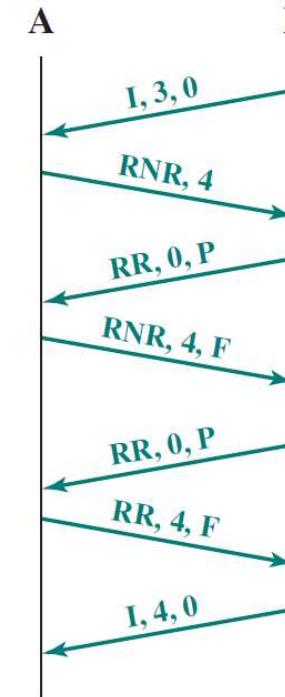
Disconnect, requested by any side, on its own initiative (if some sort of fault), or at the request of the higher level protocol (user request).



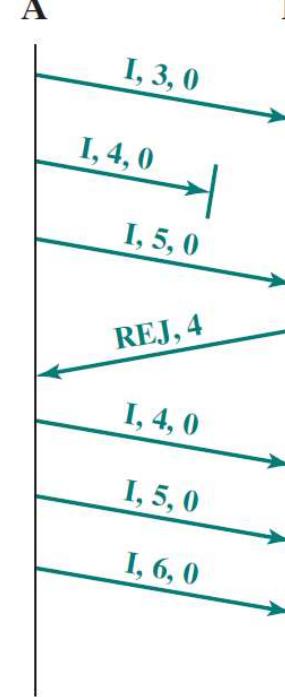
(a) Link setup and disconnect



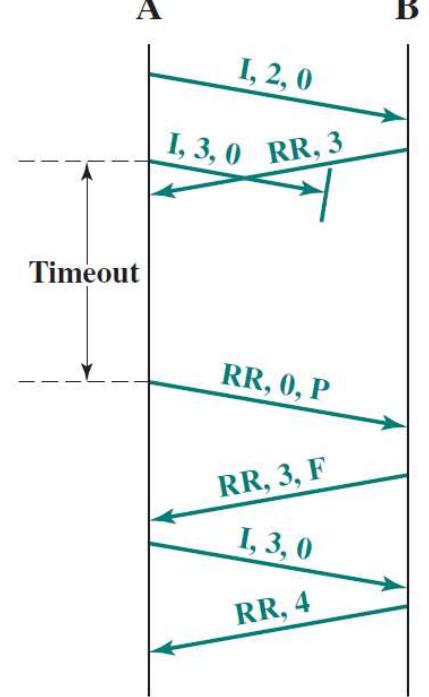
(b) Two-way data exchange



(c) Busy condition



(d) Reject recovery



(e) Timeout recovery

Examples of various operations (analysed by yourself)

Other DLC Protocols

Link Access Procedure, Balanced (LAPB)

Part of X.25 (ITU-T), as level 2 base protocol

Subset of HDLC – provides ABM

Point to point link between system and packet switching network node

Link Access Procedure, D-Channel (LAPD)

Part of the ITU-T recommendation for ISDN; data link control over D channels

Implements only HDLC- ABM, but there are differences:

Always 7-bit sequence numbers (no 3-bit)

16 bit address field, contains two sub-addresses: one for device and one for user (next layer up), allowing multiple devices for same user, or multiple logical users of LAP-D

16-bit CRC

Logical Link Control (LLC) - IEEE 802.2

Component, with MAC (Medium Access Control) of the Data Link level of LANs

Manages only the logic control of a data link

LLC frame embedded in MAC frame

Different frame format as a HDLC frame

No primary and secondary stations - all stations are peers (specific to LANs)

Two station addresses needed (appear in MAC frame):

Sender and receiver addresses

LLC deals with interaction points with upper level:

Destination and source access points (DSAP, SSAP)

Error detection done at MAC layer

Use of 32 bit CRC

LLC offers three forms of services:

- connection-oriented, similar with HDLC – ABM
- acknowledged connectionless
- unacknowledged connectionless (pure datagram service)

Frame Relay

Streamlined capability over high-speed packet-switched networks

Used in place of X.25, imposed by US

Frame Relay uses as Data Link Control the **Link Access Procedure for Frame-Mode Bearer Services (LAPF)**

In fact there are two protocols in LAPF:

Control protocol- similar to HDLC

Core protocol- subset of control protocol

Differences of control protocol vs. HDLC:

7-bit sequence numbers

16 bit CRC

2, 3 or 4 octet address field; from those bits 10, 16 and 23 respectively, implement the Data link connection identifier (DLCI); rest are flow control bits

DLCI identifies logical connection between stations.

Frame Relay **LAPP core** protocol similar with LAPF control, but allows streamlined operations, being not concerned with flow and error control

ATM (Asynchronous Transfer Mode)

Streamlined capability across high speed networks

Not HDLC based

Frame format called **cell**, providing minimum processing overhead

Fixed 53 octet (424 bit): 5 control and 48 payload.

Local Area Networks

What's a LAN?

A **transmission system**, usually **private** owned, very **speedy and secure**, covering a geographical area in the range of **kilometres**, comprising a **shared transmission medium** and a set of **hardware & software** for **interfacing** devices to the medium and regulating the **orderly access** to the medium. Generally it carries a great amount of the enterprise's internal communications load.

LAN Applications

- Personal Computer & workstation LANs: cheap, limited speed & load
- Backend Networks and Storage Area Networks: separate 'one room' network, high speed, transfer of large blocks of data, for data processing or storage (inter-connecting large systems: mainframes and large storage devices)
- High-Speed Office Networks: for modern offices requiring increased processing power & speed (image & graphical processors, fax machines, local high capacity storage devices)
- Backbone LAN: high-speed LAN interconnecting various lower cost & capacity LANs spread within buildings or departments

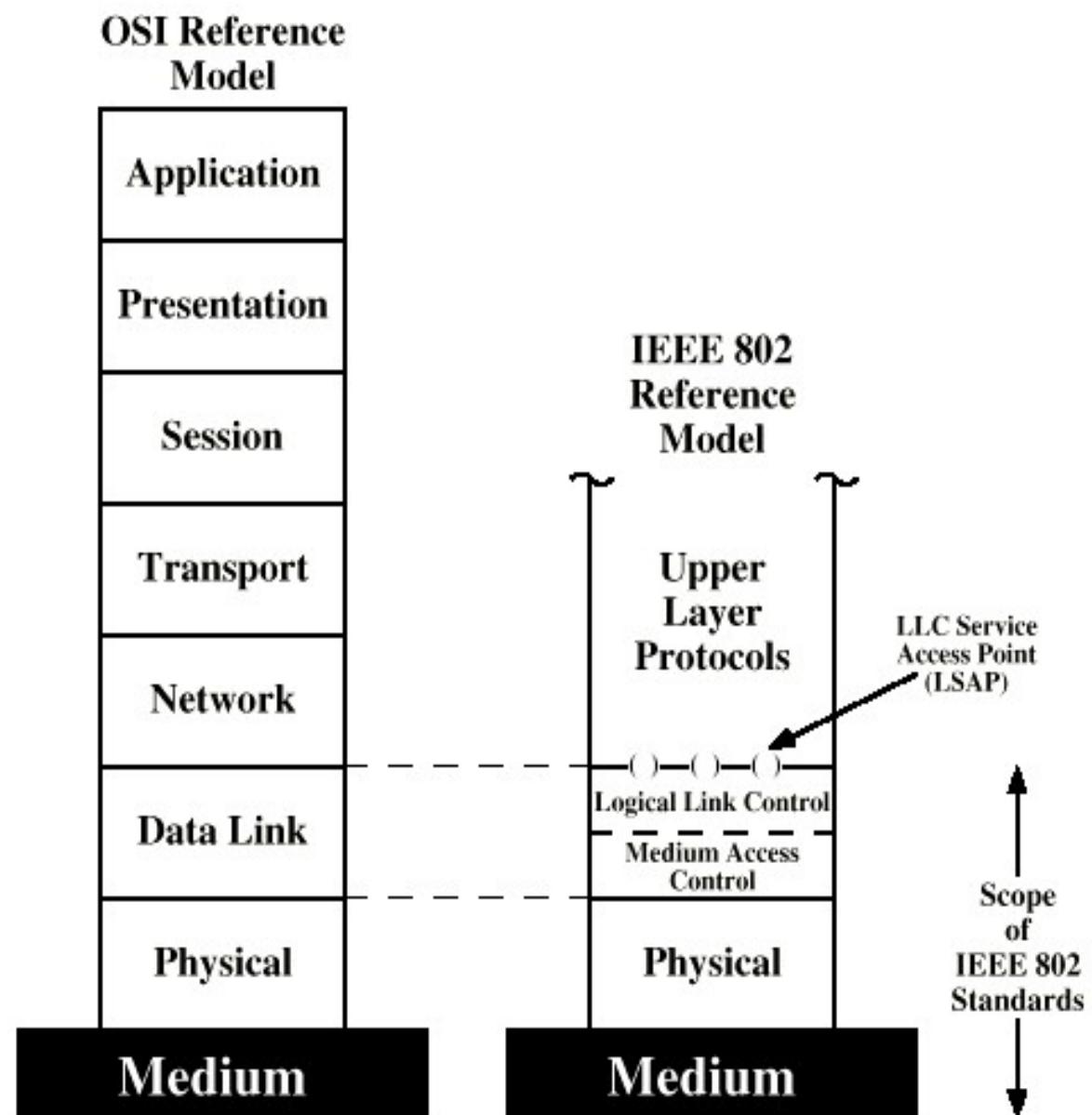
LAN Architecture

Described in terms of
Protocol architecture

Includes:

- Physical + Topologies
- Media access control
- Logical Link Control

Comparison between OSI
and LAN protocol stacks:



LAN Generations

First

CSMA/CD and Token Ring

Terminal to host and client - server

Moderate data rates (tens of Mbps)

Second

FDDI

Backbone

High performance workstations

Third

ATM-based

Aggregate throughput and real time support for multimedia applications

Wireless LANs Generations

Third Generation LANs

Support for multiple guaranteed classes of service

Live video may need 2Mbps

File transfer can use background class

Scalable throughput

Both aggregate and per host

Facilitate LAN/WAN internetworking

LANs Protocol Architecture

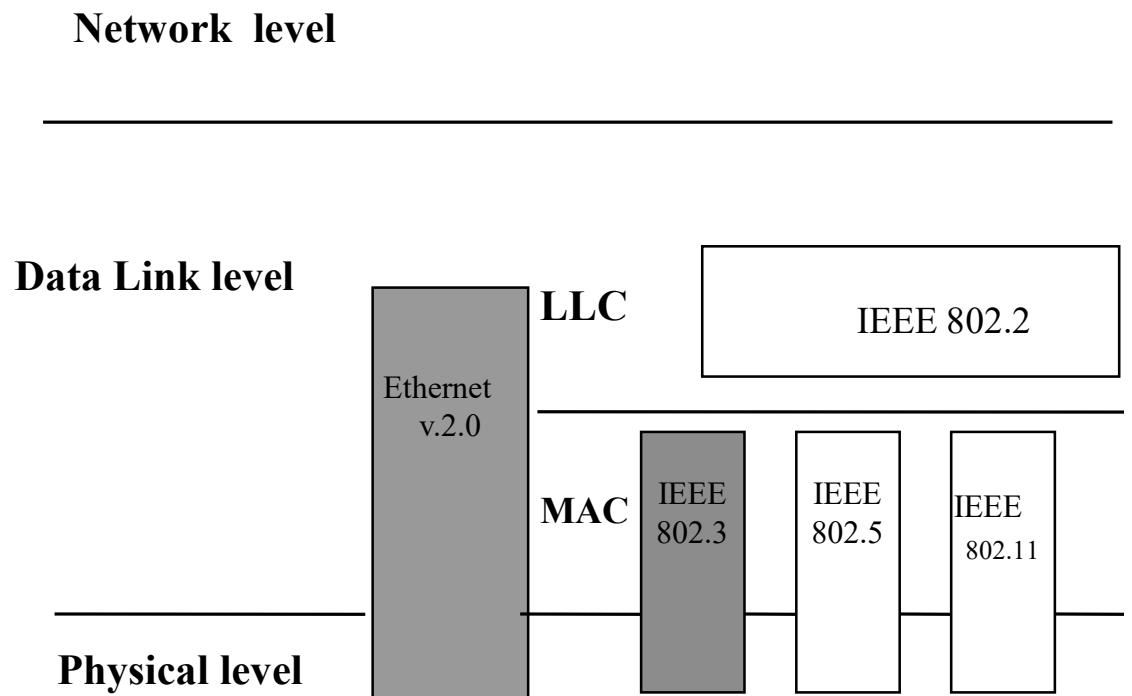
Covers lower layers of OSI
Reference model

IEEE 802.x standard suite:

LAN Reference model

Three layers:

- Physical
- Logical link control (LLC)
- Medium access control (MAC)



802.x Layers

Physical

Encoding/decoding

Preamble generation/removal

Bit transmission/reception

Transmission medium and topology

Logical Link Control

Interface to higher levels

Flow and error control

Several kind of services: connection oriented/connectionless

Media Access Control (not found in traditional layer 2 Data Link control)

Assembly of data into frames, with address and error detection fields

Disassembly of frame

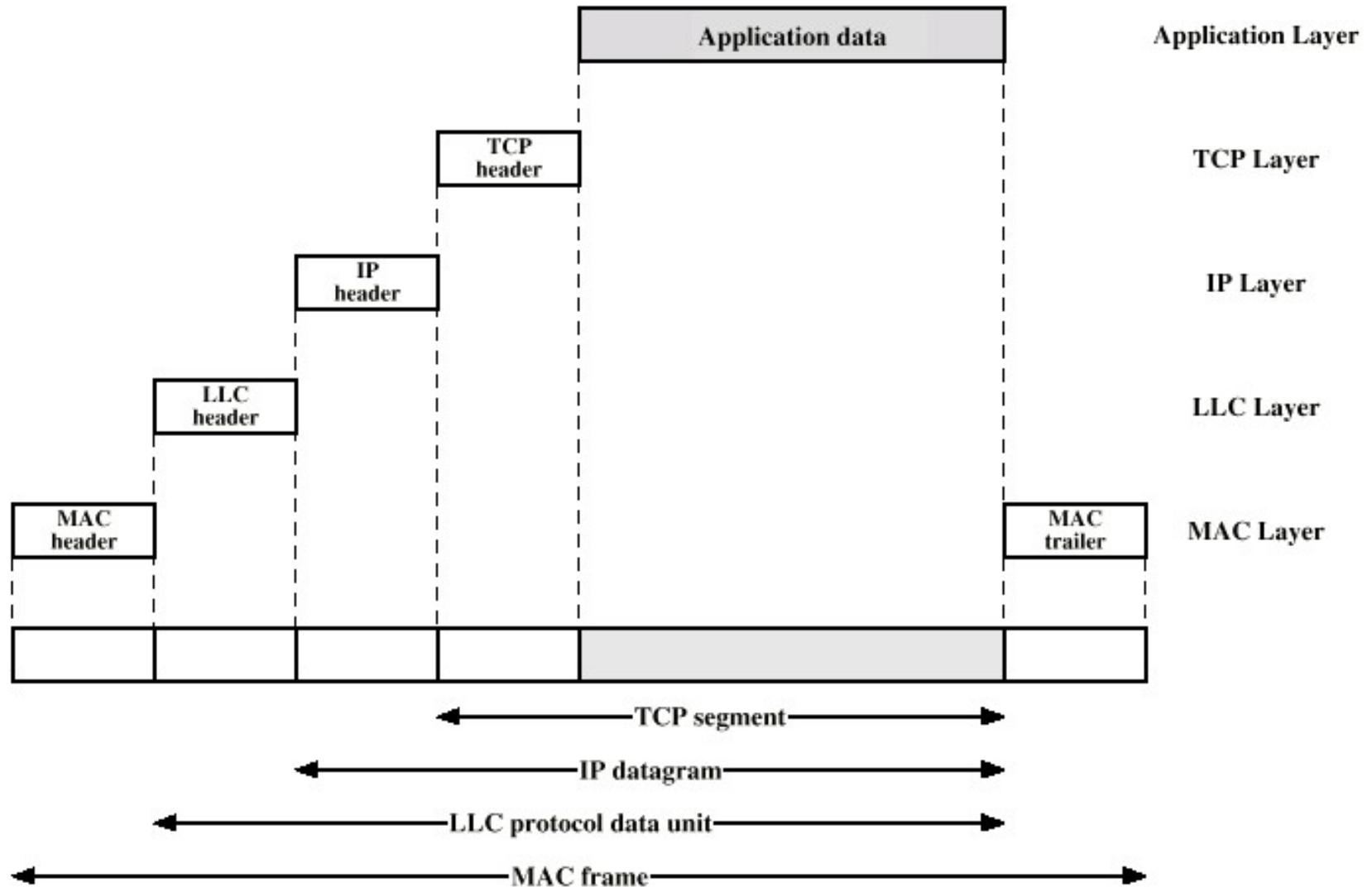
Address recognition

Error detection

Govern access to the transmission medium

For the same LLC, several MAC options may be available

Encapsulation of data at successive layers: how is obtained the MAC frame
(OSI terminology: Protocol Data Unit)



Ring Topology

Repeaters joined by point to point links in closed loop

Receive data on one link and retransmit on another

Links unidirectional

Stations attached to repeaters

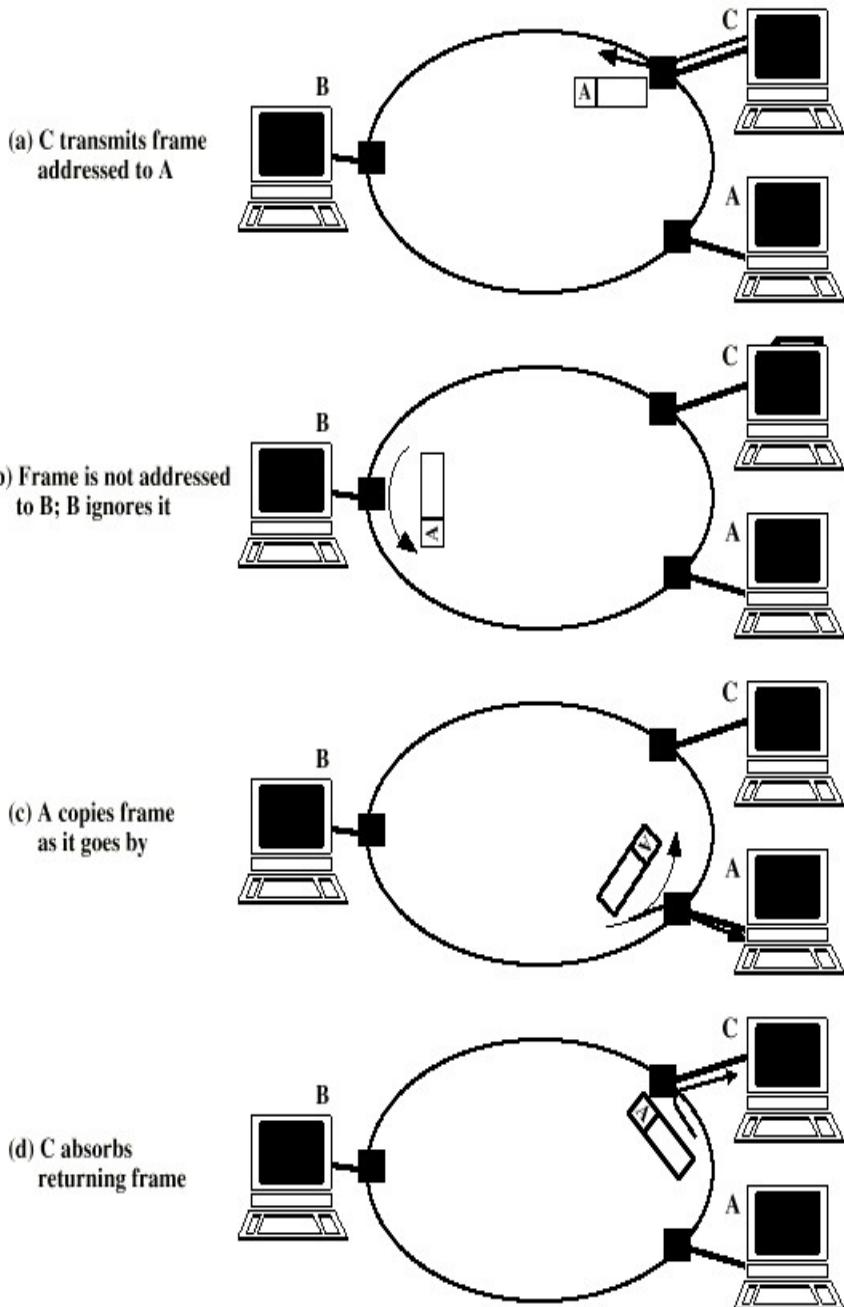
Data in frames

Circulate past all stations

Destination recognizes address and copies frame

Frame circulates back to source where it is removed

Media access control determines when station can insert frame



Advantages:

Failure of a station does not affect ring transmission

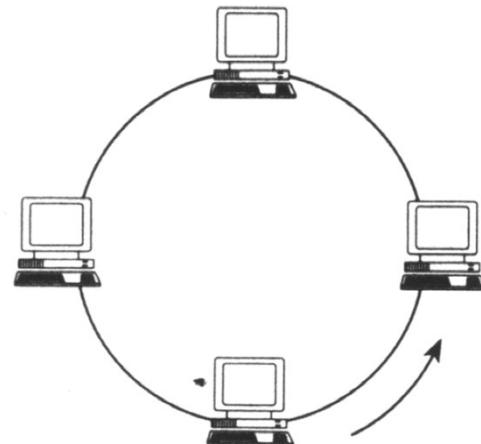
Can cover a wider area (LANs, MANs, WANs)

Disadvantages

Limited number of nodes/ring

Failure of repeater may cause failure of ring transmission

More complex operation to insert new nodes and to
manage network (clock synchronization)



Star Topology

Each station connected directly to central node

Usually via two point to point links

Central node can broadcast

Physical star, logical bus (one station transmits at a moment, all receive)

Central node can act as frame switch.

Advantages:

Easy to add devices

Easy to extend topology (extended star, snow-flake)

Possible to use existing telephonic infrastructure

ATM – friendly

Less prone to problems with connecting devices

More security (central access point – the switch)

Flexibility for customer needs

2/22/2021

Vasile Dadarlat - Computer
Networks

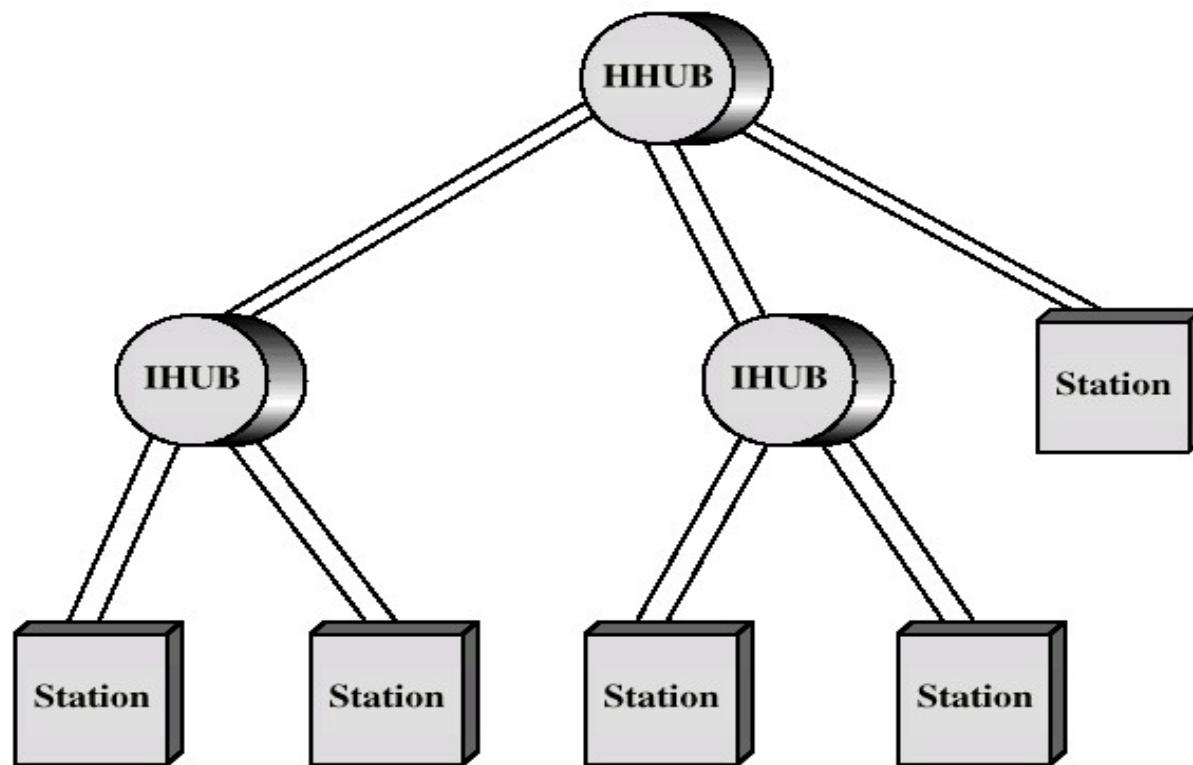
10

Disadvantages:

Central switch down => all network down

Local switch down => local network down

Wiring overhead (more ducts, cabinets, power supply)



Medium Access Control

Orderly & efficient use of the shared medium

Centralized control – one monitor (master) station

Greater control over network (priorities, guaranteed parameters, overrides)

Simple access logic at other stations

Avoids problems of co-ordination between stations

Single point of failure - monitor

Potential bottleneck – toward monitor, may reduce performance

Distributed – stations collectively perform control

-Synchronous

Specific capacity dedicated to connection (to each station) – less used in LANs – station needs are unpredictable

-Asynchronous (dynamic)

In response to (immediate) demand of each station

Asynchronous Control Approaches

Round robin

Each station in turn is given the opportunity to transmit (daisy-chain architecture)

Control: centralized (polling) or distributed.

Each station may decline to transmit or may transmit subject to some upper bound.

Good if many stations have data to transmit over extended period; less efficiency for small number of active stations (important polling overhead)

Less used for LAN control, used with terminal handling.

Reservation

Allocated time for accessing the medium (time slots). Each station for transmitting will allocate future slots. In a way similar with synchronous TDM.

Good for stream traffic

Examples: token passing based protocols

Contention

All station contend (compete) for gaining access, for an upper bounded time. Full distributed control.

Good for bursty traffic

Simple to implement

Efficient under moderate load

Tend to collapse under heavy load.

Examples: ALOHA (radio networks), CSMA (Ethernet)

MAC Frame Format

MAC layer receives data from LLC layer; this is the payload or the LLC PDU

Additional fields:

MAC control

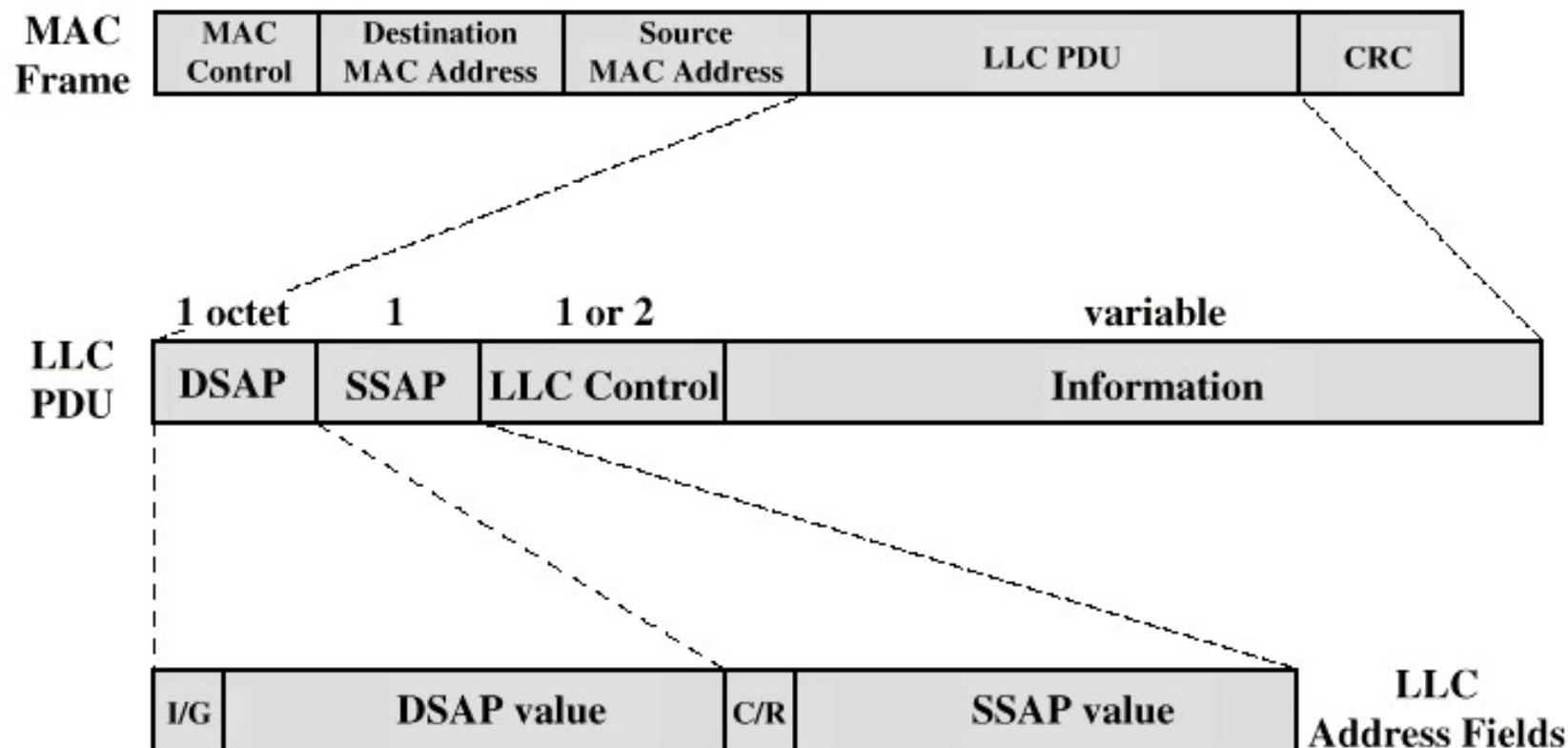
Destination MAC address

Source MAC address

CRC

MAC layer detects errors and discards frames

LLC optionally retransmits unsuccessful frames



I/G = Individual/Group

C/R = Command/Response

SAP - Service Access Point - a conceptual location at which one OSI layer can request the services of another OSI layer

MAC Frame Format + LLC Frame Content

Logical Link Control

Transmission of Data Link level PDUs between two stations having a direct data link (no switching node between)

Must support multiaccess, due to shared medium

Relieved of some link access details by the MAC layer

Addressing involves specifying source and destination LLC users (users: higher level protocol – network management)

LLC user addresses referred to as service access points (SAPs)

Allows connection multiplexing

LLC Services

Addressing stations and controlling data exchange between SAPs (users)

Based on HDLC

LLC-1:Unacknowledged connectionless service (datagram style)

LLC-2:Connection mode service (similar to HDLC)

LLC-3:Acknowledged connectionless service (trade-off)

Most used contention-based MAC techniques

ALOHA, first developed for packet radio networks (Univ. Hawaii)

Simplest protocol:

- When station has frame, it sends

- Station then listens (for a max round trip time, twice the transmission time between the most widely separated stations), plus small increment

- If ACK, fine. If not, retransmit

- If no ACK after repeated transmissions, give up

For correctness at receiver: use of frame check sequence (as in HDLC)

Each station: if frame OK and address matches receiver, send ACK

Frame may be damaged by noise or by another station transmitting at the same time (collision)

Any overlap of frames causes collision

Max. medium utilization 18%, due to the fact that increased load gives increased number of collisions.

Slotted ALOHA

Conceived to improve efficiency

Time organized in uniform slots, equal to frame transmission time

Need central clock (or other sync mechanism)

Transmission begins at slot boundary

Frames either miss collision, or overlap totally

Max utilization 37%

CSMA (Carrier Sense Multiple Access)

For 10Mbps LANs, usually the propagation time between stations is much less than frame transmission time; not true with 100 or 1000Mbps LANs – switched LANs

All stations know almost immediately that a transmission has started

CSMA algorithm based on following ideas:

- Each station first listens for clear (idle, not busy) medium (carrier sense)

- If medium idle, and has to transmit, will transmit immediate

(implementation of the 1-persistent CSMA technique)

If two stations start at the (approx.) same instant, collision of frames
Transmitter waits reasonable time (round trip, plus ACK contention)
No received ACK, collision occurred, so will retransmit

Max utilization depends on propagation time (medium length) and frame length (transmission time)

Longer frame and shorter propagation gives better utilization

CSMA/CD (CSMA / Collision Detection)

With CSMA, collision occupies medium for the durations of implied transmissions

Remedy: stations listen while transmitting, detecting collision occurrence

If medium idle, transmit

If busy, listen for idle, then transmit

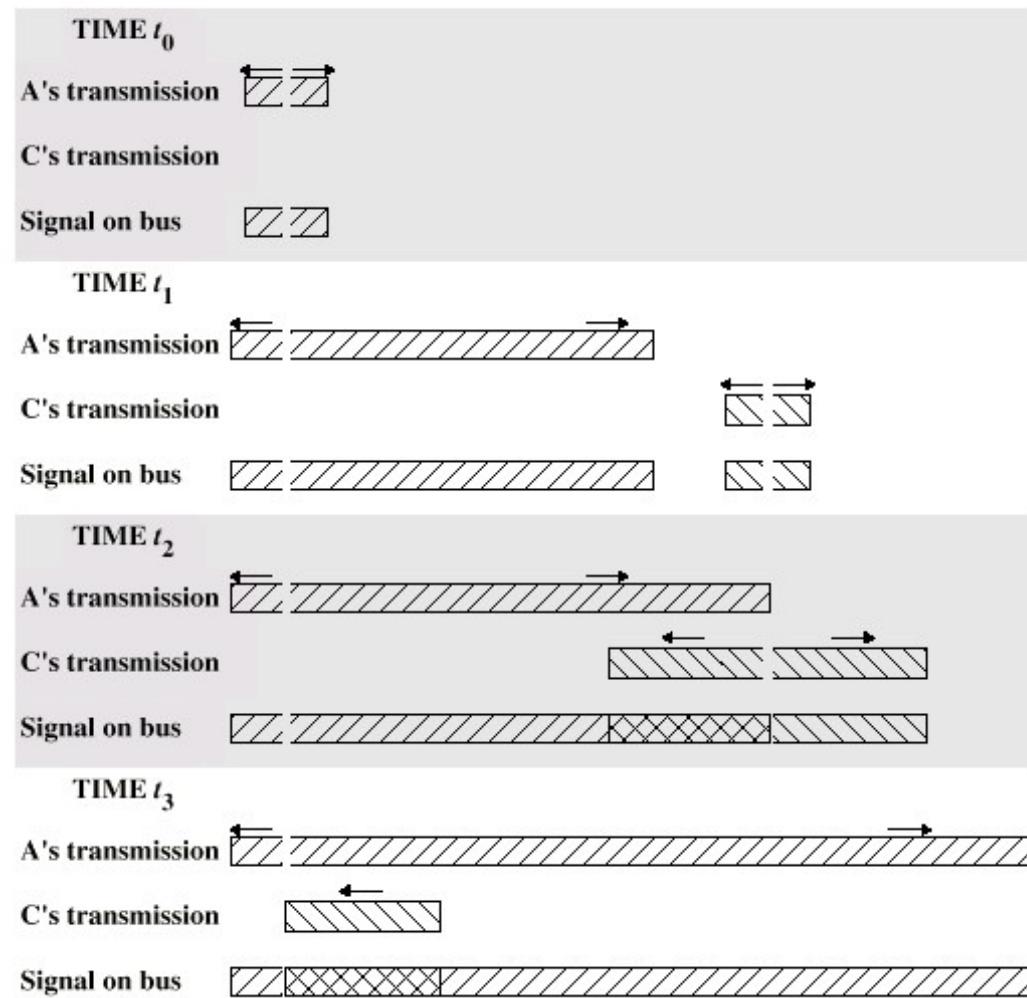
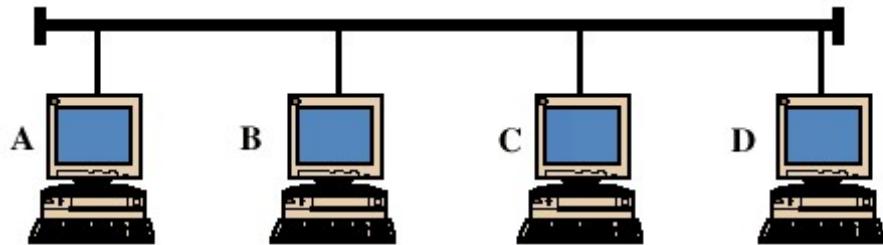
If collision detected, transmit short jamming signal, then cease transmission

After jam, wait random time then start again listening the medium

Binary exponential back-off waiting algorithm:

The time to wait t , for the n -th attempt, the value being randomly chosen in the interval $0 < t < 2^k$, where $k = \min(n, 10)$. The number of attempts is bounded (to 16).

Illustration of CSMA/CD algorithm



Token passing based protocols

Token Ring

MAC protocol

One (only) small frame (token) circulates when medium idle

Station waits for token

Changes one bit in token to make it start of frame SOF for data frame

Append rest of data frame

Frame makes round trip and is absorbed by transmitting station

Station then inserts new token when transmission has finished, and leading edge of returning frame arrives

Under light loads, some inefficiency

Under heavy loads, acts as round robin

Octets	1	1	1	6	6	0	4	1	1
	SD	AC	FC	DA	SA	Data unit	FCS	ED	FS

SD = starting delimiter
 AC = access control
 FC = frame control

DA = destination address
 SA = source address
 FCS = frame check sequence

ED = ending delimiter
 FS = frame status

(a) General Frame Format

SD	AC	ED
----	----	----

J	K	I	J	K	I	I	E
---	---	---	---	---	---	---	---

(b) Token Frame Format

J, K = non-data bits
 I = intermediate frame bit
 E = error-detected bit

P	P	P	T	M	R	R	R
---	---	---	---	---	---	---	---

PPP = priority bits M = monitor bit
 T = token bit RRR = reservation bits

(c) Access Control Field

A	C	r	r	A	C	r	r
---	---	---	---	---	---	---	---

A = Address recognized bit
 C = Frame copied bit
 rr = reserved

F	F	Z	Z	Z	Z	Z	Z
---	---	---	---	---	---	---	---

FF = frame-type bits ZZZZZZ = control bits

(d) Frame Control Field

(e) Frame Status Field

Token Ring MAC frame structure

Token Ring Operation

After seizing the token, station A transmits a frame to station C

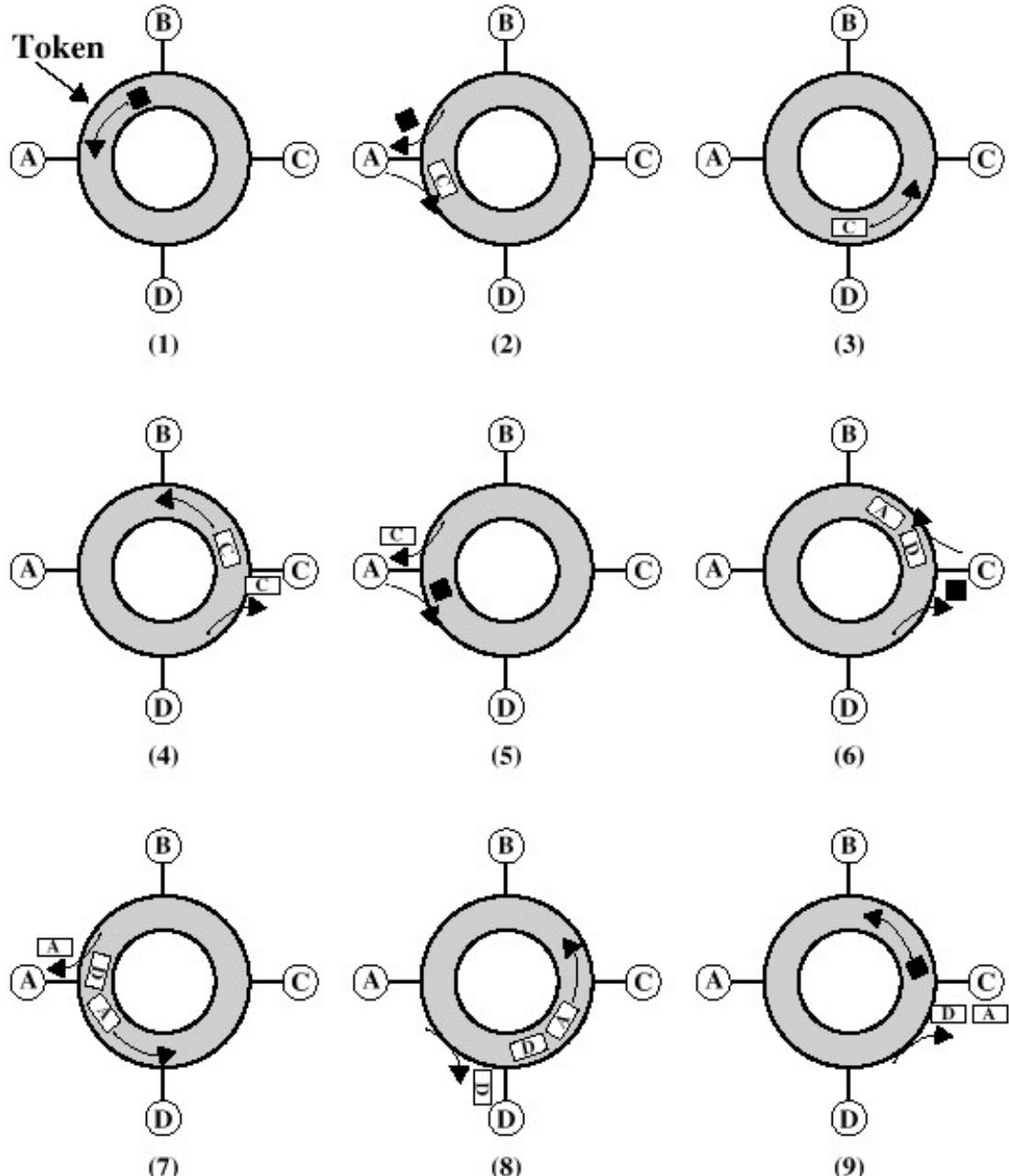
Station C copies the packet, inserts ACK

When packet back to A, it removes packet from the ring and releases token

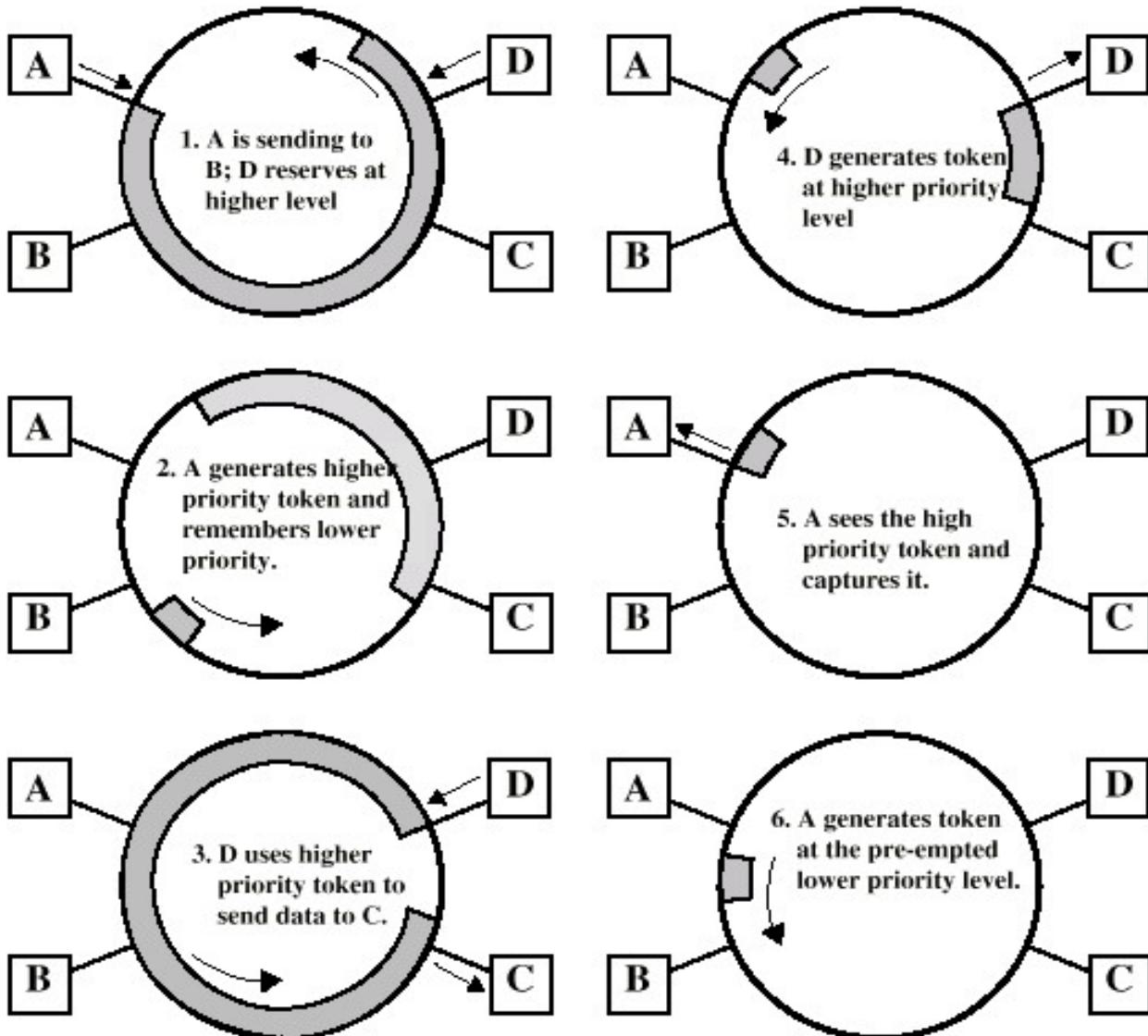
When station C seizes token, sends packets for A and D stations

Each destination stations copy packets

When packet back to C, it purges the ring and releases token



Token Ring Operation (involving priorities scheme)



Ring topology LANs

IEEE 802.5 Token Ring

Remember:

Acts at 4Mbps, 16Mbps and (will) 100Mbps, using UTP, STP and FO

Differential Manchester encoding

Each station connected using a repeater, which introduces a delay when active!

Each repeater connects to two others via unidirectional transmission links

Single closed path

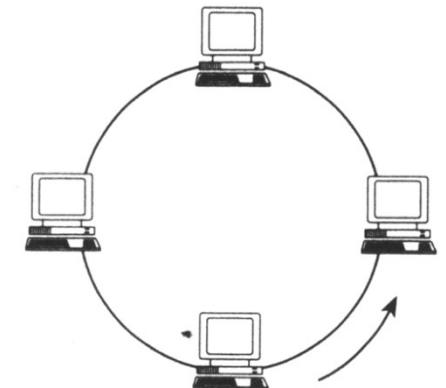
Data transferred bit by bit, from one repeater to the next

Each repeater introduces one bit delay

Repeater regenerates and retransmits each bit

Repeater performs data insertion, data reception, data removal

Packet removed by transmitter after one trip round ring



For the MAC level, *remember*:

One (only) small frame (token) circulates when medium idle

Station waits for token

Changes one bit in token to make it start of frame SOF for data frame

Append rest of data frame

Frame makes round trip and is absorbed by transmitting station

Station then inserts new token when transmission has finished, and leading edge of returning frame arrives; also allowed **early token release**

Network control – by the active **monitor**, chosen from a list of stand-by monitors

Quite complex MAC control, many ring management operations.



SD = starting delimiter

AC = access control

FC = frame control

DA = destination address

SA = source address

FCS = frame check sequence

ED = ending delimiter

FS = frame status

(a) General Frame Format



(b) Token Frame Format

J, K = non-data bits

E = error-detected bit

I = intermediate frame bit

(c) Ending Delimiter Field



PPP = priority bits M = monitor bit

T = token bit RRR = reservation bits

(d) Access Control Field

A = Address recognized bit

rr = reserved

C = Frame copied bit

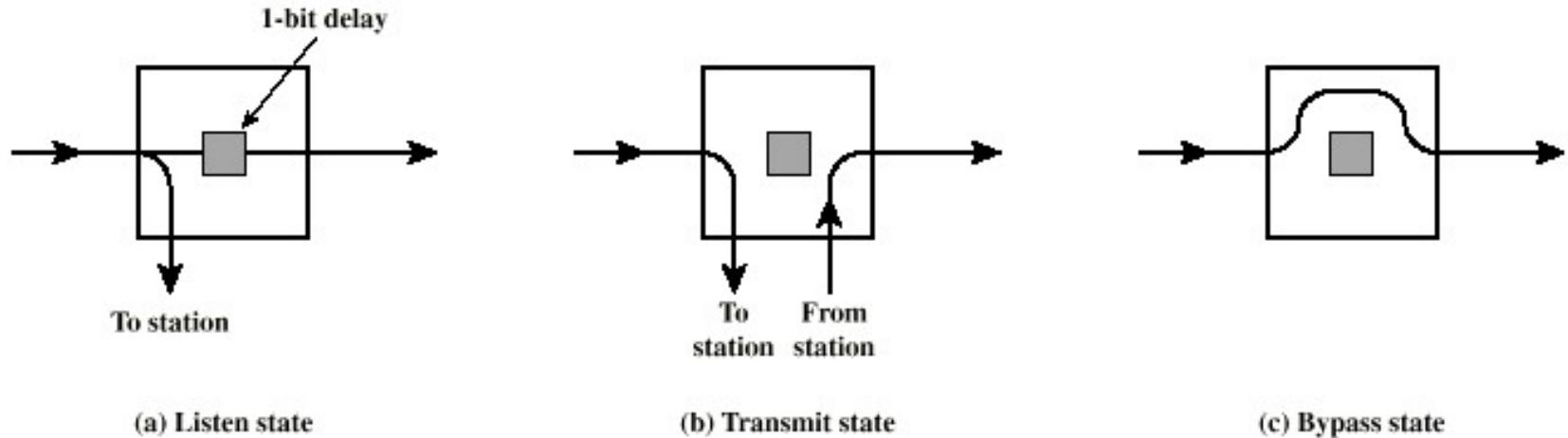


(e) Frame Status Field

FF = frame-type bits ZZZZZZ = control bits

(f) Frame Control Field

Repeater is in one of the following states:



Listen State Functions

Scan passing bit stream for pertinent patterns:

Address of attached station; if station is destination of the passing frame

Token permission to transmit

Copy incoming bit and send to attached station

Whilst forwarding each bit

Modify bit as it passes, e.g. the C bit, to indicate a packet has been copied (acts as ACK)

Transmit State Functions

Station has data to put on ring

Repeater has permission to send

Repeater receives bits from station and puts them on ring

May receive incoming bits, from the ring, on incoming line

If ring bit length is shorter than transmitted packet length

Pass back to station for checking (ACK, by example)

May be more than one packet on ring (some control strategies allow)

Buffer bits for retransmission later

Bypass State

Signals propagate past repeater with no delay (other than propagation delay)

Partial solution to reliability problem (station not in use)

Allows improved performance

Physical level problem: **Timing Jitter**

Clocking included with signal, using differential Manchester encoding

Clock recovered by repeaters, because:

- To know when to sample the signal and recover frame bits

- Use of clocking for data retransmission on the ring

Clock recovery deviates from ‘original’ midbit transmission randomly, due to

- Noise during transmissions

- Imperfections in receiving circuitry

Deviation of clock recovery is named **timing jitter**

Repeater data retransmissions obtained without distortion, but with random timing error

Cumulative effect is that the bit length varies

Timing jitter limits the number of repeaters on ring.

Solving Timing Jitter Limitations

Two methods used in combination:

Repeater uses phase-locked loop (device using feedback, minimizing the deviation from one bit time to the next)

Use buffer at one or more repeaters

Programmed to hold a certain number of bits

Buffer expands and contracts to keep bit length of ring constant

Negative result: Significant increase in maximum ring size

Other Potential Ring Problems

Break in any link disables network

Repeater failure disables network

Installation of new repeater to attach new station requires identification of two topologically adjacent repeaters (neighbour identification)

Timing jitter

Many error sources on data frames, but on token control frames

Methods of removing circulating packets required

With backup in case of errors

Mostly solved with star-ring architecture! See following DTR development.

Star Ring Architecture

Feed all inter-repeater links to a single site

Use of a concentrator acting as a multi-port repeater

Provides central access to signal on every link

Easier to find faults

Can launch message into ring and see how far it gets (beacon frames)

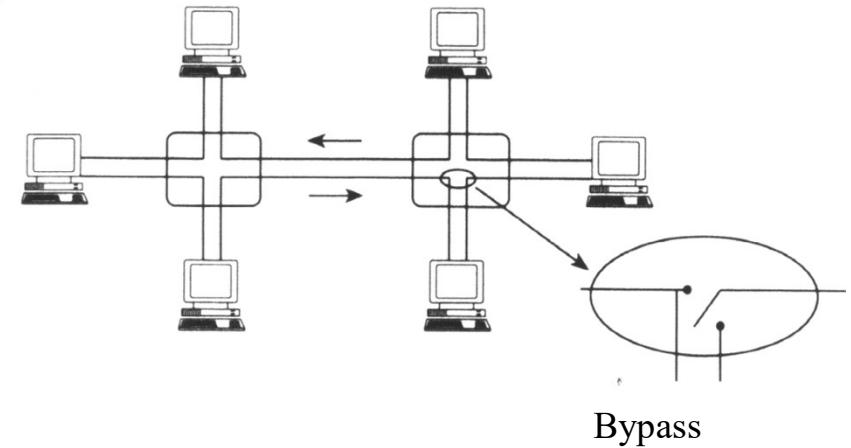
Faulty segment can be disconnected and repaired later

New repeater can be added easily

Bypass relay can be moved to concentrator

Can lead to longer cable runs

Can connect multiple rings using bridges



Dedicated Token Ring (DTR - recent development of 802.5 TR)

Operates at 16, 32 and 100Mbps, backward compatibility with 802.5

Switched Full Duplex Token Ring: star shaped ring, using a central hub (multi-port repeater) which **acts as a switch** (multi-port bridge) => means that it doesn't act at bit level like an ordinary repeater, but as frame level repeater

Full duplex point to point links between switch and stations

- Use of dedicated links at 16Mbps

- Use of full duplex links at 32Mbps

No token passing used as MAC control

- Flow-based access, or immediate access **TXI** (Transmit Immediate), e.g. communications can take place between a device and a switch at any time

FDDI (Fiber Distributed Data Interface), ISO standard 9314

100Mbps network, used for LAN & MAN applications; fiber optic based (may use short UTP links); excellent for LAN backbones

Use of Token Ring MAC algorithm, with differences (*remember?*):

- Station seizes token by aborting token transmission
- Once token captured, one or more data frames transmitted
- New token released as soon as transmission finished (early token release in 802.5)
- Allows for asynchronous & synchronous frame transmissions
- Data & control coded as **symbols**, group of 4 bits carried as 5 bits by the medium (4B/5B)
 - provide necessary clock transitions for the receiver (0000_2 contains no transitions and that causes clocking problems for the receiver)
 - ensure at least two transitions per block of bits

Data		4B5B code
(Hex)	(Binary)	
0	0000	11110
1	0001	01001
2	0010	10100
3	0011	10101
4	0100	01010
5	0101	01011
6	0110	01110
7	0111	01111
8	1000	10010
9	1001	10011
A	1010	10110
B	1011	10111
C	1100	11010
D	1101	11011
E	1110	11100
F	1111	11101

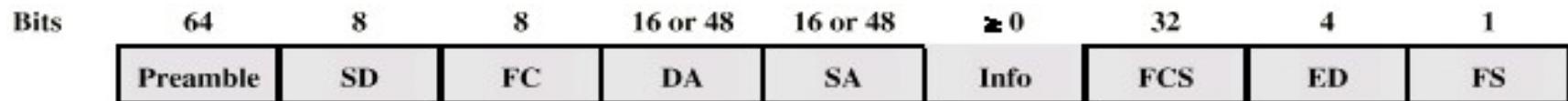
FDDI MAC Protocol

MAC protocol for FDDI (Fiber Distributed Data Interface): ss for 802.5, except:

Station seizes token by aborting token transmission

Once token captured, one or more data frames transmitted

New token released as soon as transmission finished (early token release in 802.5)



(a) General Frame Format



(b) Token Frame Format

SD = starting delimiter

FC = frame control

DA = destination address

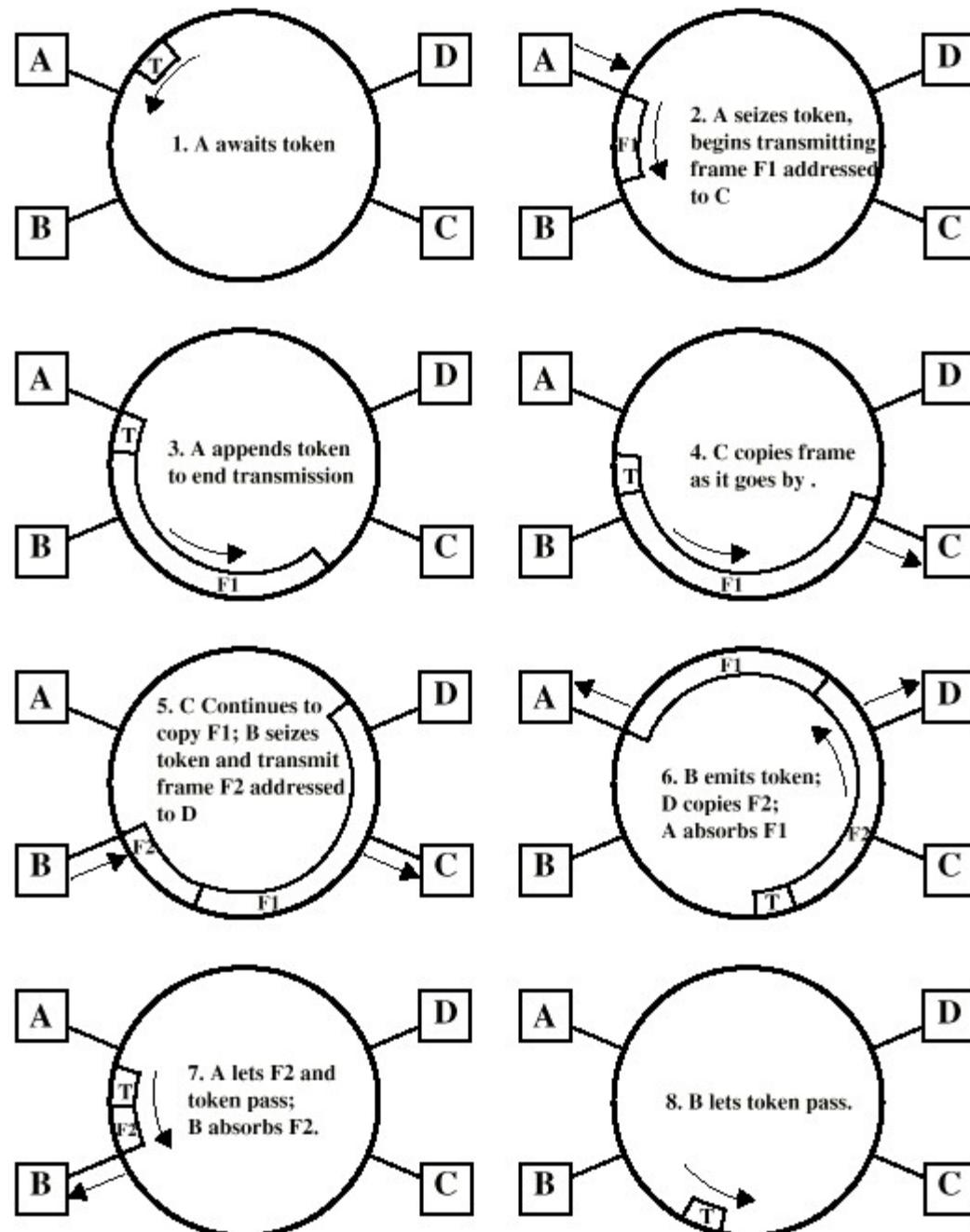
SA = source address

FCS = frame check sequence

ED = ending delimiter

FS = frame status

Example for FDDI Operation



Bits	64	8	8	16 or 48	16 or 48	≥ 0	32	4	1
	Preamble	SD	FC	DA	SA	Info	FCS	ED	FS

(a) General Frame Format



(b) Token Frame Format

SD = starting delimiter

FC = frame control

DA = destination address

SA = source address

FCS = frame check sequence

ED = ending delimiter

FS = frame status

FDDI frame

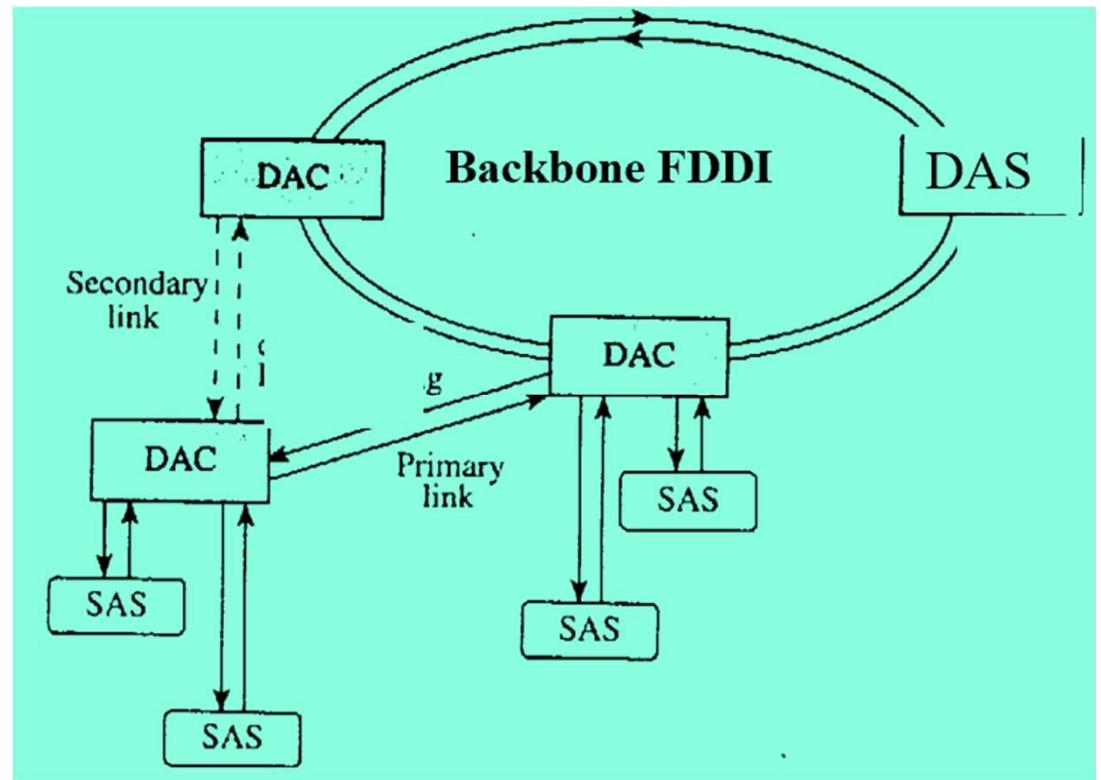
Topology – two FO rings, with opposite flows:

- Primary ring
- Back-up ring

When crash, use of attach. unit bypass and ring merger => one flow

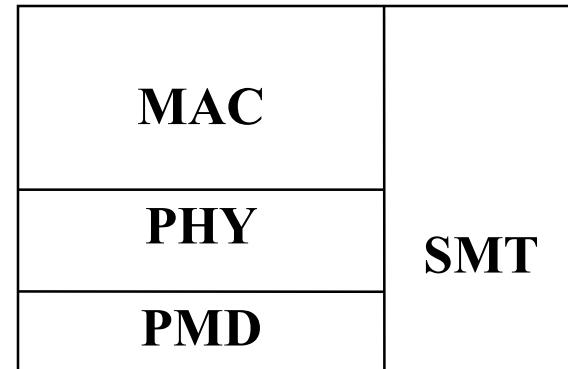
Three types of stations:

- DAS (Dual Attachment Station)
- DAC (Dual Attachment Concentrator)
- SAS (Single Attachment Station)



SAS connected only to the primary ring.
TP used to connect SAS to DAC.

Architectural levels – one more level, **Station Management**, lowering complexity of MAC level (station initialisation & management, ring management: fault detection & isolation)



FDDI Physical Layer

Extra to NRZ-NRZI coding, is used multi-level coding MLT-3, allowing lower influence of attenuation over data

Some usual parameters:

Medium	Optical Fiber	Twisted Pair
Data rate	100	100
Signaling	4B/5B/NRZI	MLT-3
Max repeaters	100	100
Between repeaters	2km	100m

Solved problem: Data Link Control Algorithms

Consider the use of 1000 bit frames on a 1Mbps satellite channel with a 270ms delay.

What is the maximum link utilization for:

Stop-and-wait protocol?

Continuous flow control with a window size of 7?

But with a window of 127?

What about a window of 255?

Bit time: $1/10^6 = 10^{-6}$ sec = 1 μ sec

Frame time: $1,000 \times 1\mu\text{sec} = 1$ ms.

Assuming no extra delay at the receiver, one bit echo will take 270ms for being received by the sender.

Continued on next slide

Assuming that all control information is under the above delay:

(Stop-and-wait): Total transmission time for a frame is: 1 (frame time) + 270 (receiving ACK delay) = 271ms. So effective utilization of the channel is $1/271 = .3\%$.

(Window of 7): Sender can send 7 messages (frames) in advance, without ACK, until an enforced wait. 7 frames transmitted in 7ms. There is a 270ms delay after first frame, for the ACK (or RR) of the first frame. Each ACK for following frames takes other 1ms. Thus 7 frames sent correctly in: $7 + 270 = 277$ ms, so an utilization of : $7/277 = 2.5\%$.

(Window of 127): 127 frames transmitted every 397ms ($127 + 270$); utilization of: $127/397 = 40\%$.

(Window of 255): $255/(255+270) = 51\%$.

CSMA/CD LANs

Solved problem:

Considering building a CSMA/CD network running at 1Gbps over a 1km cable with no repeaters. The signal speed is 200,000km/s. What is the minimum frame size?

Network transmission time: $1 / 10^9 = 10^{-9}$ s.

For detecting eventual collision, frame transmission must last at least double the propagation time within that medium (round trip delay).

Propagation time: $1 / 200,000 = 0.5 \times 10^{-5}$ s, so its double will be 10^{-5} s.

Number of bits in a minimum valid frame: $10^{-5} / 10^{-9} = 10,000$ bits.

Token Ring LANs

Solved problem:

Considering a Token Ring network at a bit rate of 4Mbps, and a signal propagation speed of 200m/ μ sec, and each interfaces introducing a delay of one bit period, find the cable length equivalent with a total of 20 interfaces on that ring.

One's interface delay = One bit period: $1/(4 \times 10^6) = 0.25 \times 10^{-6}$ sec = 250nsec.

20 interfaces delay: $20 \times 250\text{nsec} = 5\mu\text{sec}$.

Propagation speed: 200m/ μ sec, so for 5 μ sec the cable equivalence is 1,000m.

LAN Systems

Bus topology LANs

Design problems: not only MAC algorithm, not only collision domain management, but at the Physical level the signal balancing problem (signal adjustment):

Signal must be strong enough to meet receiver's minimum signal strength requirements

Give adequate signal to noise ratio

Not so strong that it overloads transmitter

Must satisfy these for all combinations of sending and receiving station on bus

Usual to divide network into small segments

Link segments with amplifiers or repeaters (operate at the physical level)

Used Transmission Media

-Twisted pair

Not practical in shared bus at higher data rates

-Baseband coaxial cable

Used by ‘pure’ Ethernet

-Broadband coaxial cable

Included in 802.3 specification but no longer made (ex.: 10Broad36)

-Optical fiber

Expensive

Difficulty with availability

Not often used, eventually as link segments

Conclusion: Few new installations, no perspectives, not allowing FD switched links

Replaced by **star based twisted pair and optical fiber.**

10Mbps CSMA/CD based LANs – IEEE 802.3 standard

MAC frame long enough to detect collision prior to transmission end

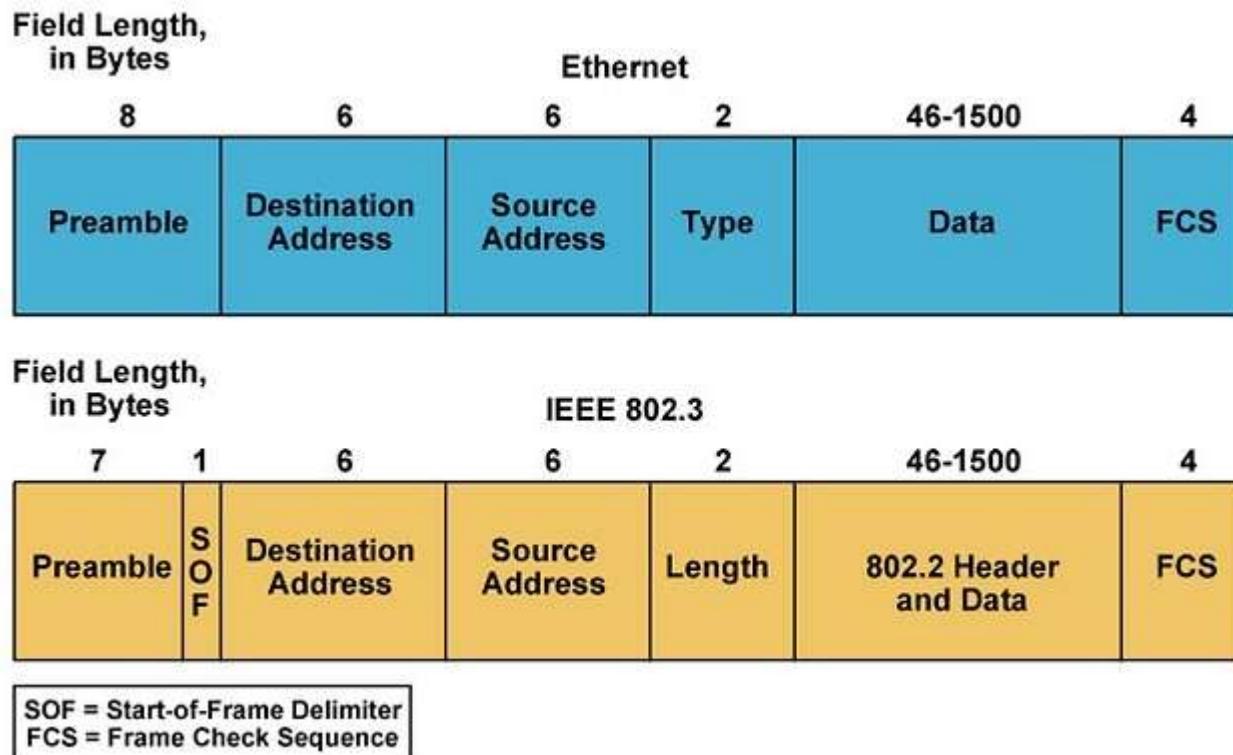
Standard 802.3 establish minimum length for the frame of 512bits, or 64bytes

Frame also upper bounded for transmission reasons

Minimum size for the Data field, if not allowed use padding (filling with *pad* char)

6 bytes for each address field: MAC address (physical address, burnt on each station network interface)

Ethernet and 802.3 frame format



10Mbps Specification (Ethernet based LANs – IEEE 802.3 standard)

Specification:

<data rate><Signaling method><Max segment length>

Example: 10Base2, 10Broad36

All implement Ethernet based CSMA/CD MAC algorithm.

Problems here: the **Round Trip Collision Delay** value, implying limitations for data format (minimum length for the frame of 512bits, or 64bytes), and maximum distance between stations (depends on link segment media).

	10BASE5	10BASE2	10BASE-T	10BASE-FP
Transmission Medium	Coaxial cable (50 Ω)	Coaxial cable (50 Ω)	Unshielded twisted pair	850-nm optical fiber pair
Signaling Technique	Baseband (Manchester)	Baseband (Manchester)	Baseband (Manchester)	Manchester/ on-off
Topology	Bus	Bus	Star	Star
Maximum Segment Length (m)	500	185	100	500
Nodes per Segment	100	30	—	33
Cable Diameter (mm)	10	5	0.4–0.6	62.5/125 μm

On baseband bus, collision produces much higher signal voltage than active signal
Collision detected if cable signal greater than single station signal; station detecting
collision will generate a burst jam signal (jabber control)

Signal attenuated over distance => limits distance to 500m (10Base5) or 200m
(10Base2)

Collision domain – given by the set of stations sensing collision when simultaneous
transmissions; for 10Mbps standard it is allowed a number of 516 bits onto the shared
medium

For higher speeds (i.e. Ethernet at 100Mbps) is kept the same minimum length,
obtained by splitting the collision domain; use of hubs or switches instead of
repeaters (they do not propagate the collision signal)

10BaseF (802.3 standard for fiber optic)

States use of fiber optics links (a pair of fibers, one for each direction) for CSMA/CD network at 10Mbps.

3 standard specifications:

10BaseFP- passive star topology (33 stations connected to a central passive optical splitter device, up to 1km segment length between two stations)

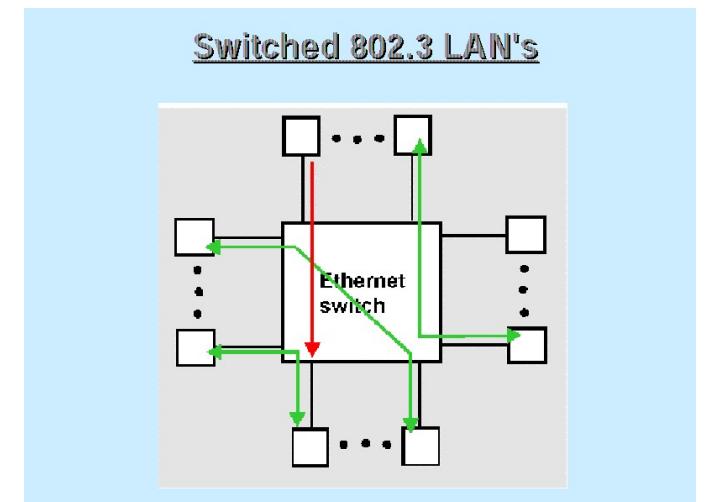
10BaseFL- point-to-point link, connecting stations & repeaters up to 2km

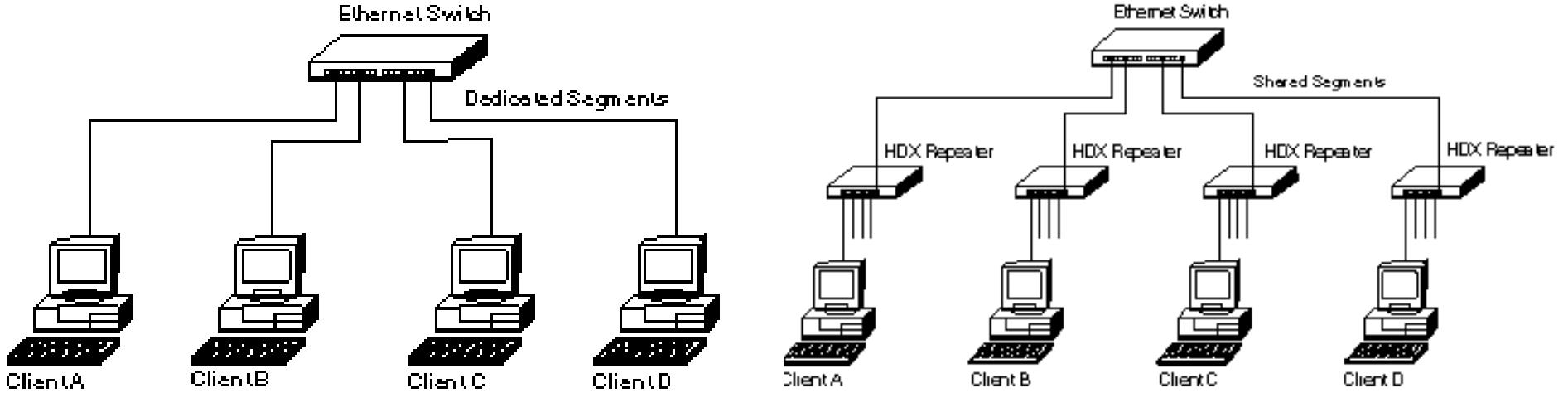
10BaseFB- backbone connecting repeaters up to 2km, using synchronous transmission (allows more repeaters cascading)

Switched Ethernet

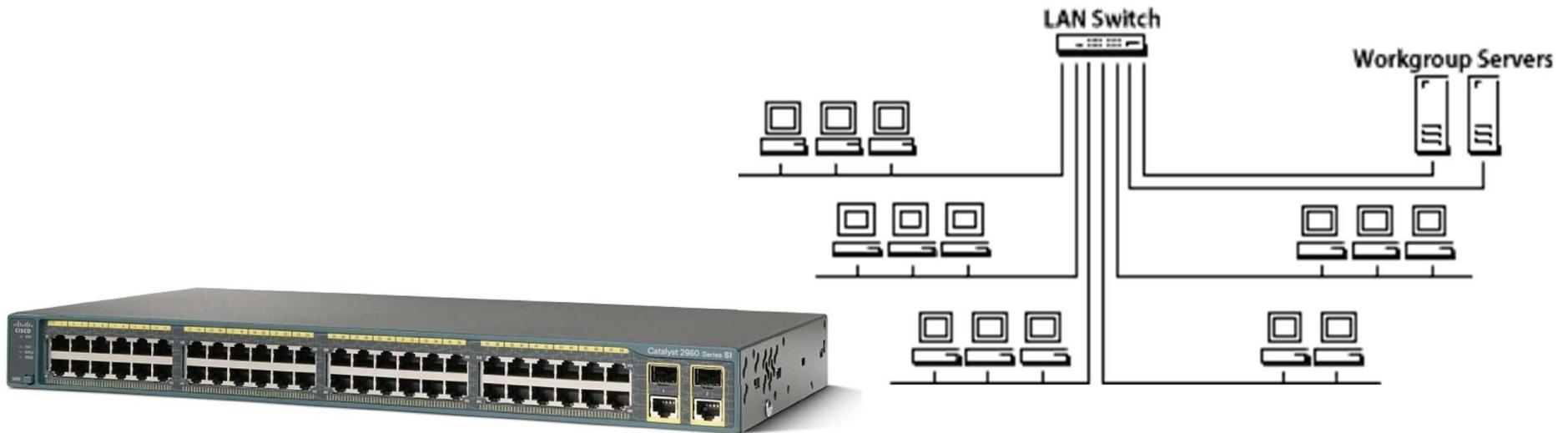
Use of *switches instead of hubs*, to join smaller LAN segments together; the switch filters and forwards the packets, in accordance with any packet protocol.

Fully Star topology.





May have dedicated segments (one per station) or shared segments (use of repeaters)



Switch device: ideal for implementing virtual LANs (for workgroup purposes)

Hubs vs. Switches

Hub: multi-port repeater, acts at Physical level

Switch: multi-port bridge, acts at Data Link level

Shared medium hub

Central hub retransmitting incoming signal to all outgoing lines

Only one station can transmit at a time

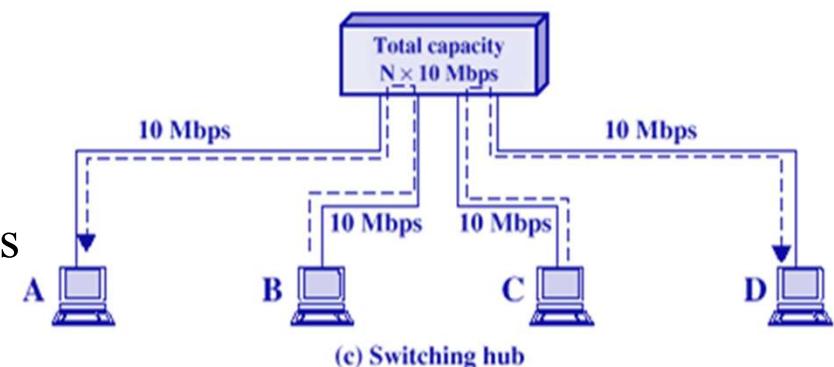
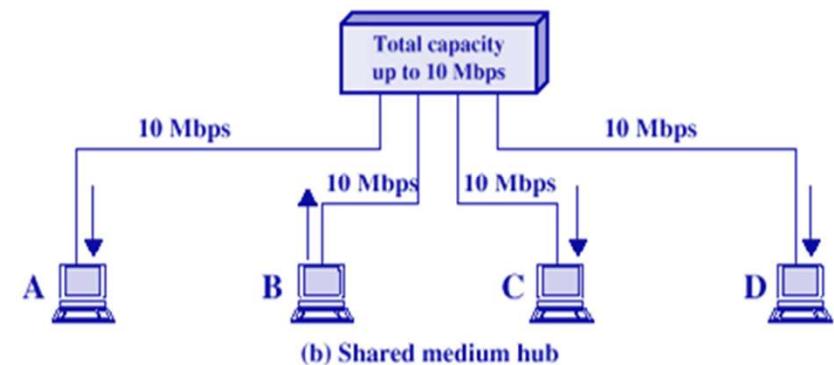
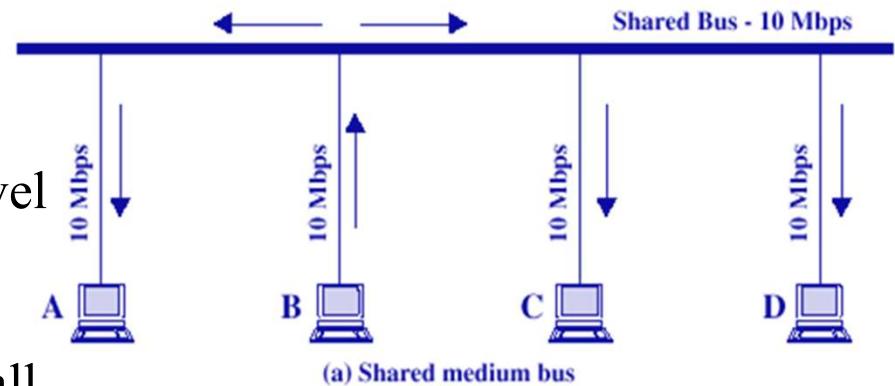
With a 10Mbps LAN, total capacity is 10Mbps

Switched LAN hub

Hub acts as switch, incoming frame switched to appropriate outgoing line

Unused lines can also be used to switch other traffic

With two pairs of lines in use, overall capacity is now multiple of line speed (20Mbps)



Switched Hubs

No change to software or hardware of devices

Each device has dedicated capacity

Scales well

Two major categories:

-Store and forward switch

Accept input, buffer it briefly, then output

-Cut through switch

Take advantage of the destination address being at the start of the frame

Begin repeating incoming frame onto output line **as soon as address recognized**

May propagate some bad frames

Switch General Problem: simultaneous transmissions to same destination:

Let first one through

Use of buffers associated with switch's ports

100Mbps specification (Fast Ethernet)

Providing low-cost Ethernet compatible LAN @ 100Mbps. Using 10Mbps legacy, development of 10/100Mbps NIC cards and devices. General specification in 100BaseX standard.

Different approaches:

100BaseT4

use of existing UTP Cat.3 networks (possible due to the signaling frequency of 25MHz), or Cat.5

achieve full-duplex 100Mbps transmissions using 4 UTP pairs, three used for data transmissions at 33,3Mbps and one for collision control

use of a ternary signaling scheme (8B6T- use of 27 symbols), allowing to transmit on three wires of a number of 4bits during a clock period

100BaseX (IEEE 802.13 standard)

Use of 100Mbps unidirectional data rate, so need for 2 pairs (Tx and Rx)

Two approaches, for different physical media:

100BaseTX for TP Cat.5 (UTP or STP)

100BaseFX for multi-mode fiber

Use of MLT-3 encoding scheme for 100BaseTX and of 4B/5B-NRZI for fiber based (as FDDI)

	100BASE-TX	100BASE-FX	100BASE-T4
Transmission Medium	2 pair, STP	2 pair, Category 5 UTP	2 optical fibers
Signaling Technique	MLT-3	MLT-3	4B5B, NRZI
Data Rate	100 Mbps	100 Mbps	100 Mbps
Maximum Segment Length	100 m	100 m	100 m
Network Span	200 m	200 m	400 m

Gigabit Ethernet (1000BaseX)

Developed by IEEE High-Speed Study Group

How to convey Ethernet packets @ Giga

Keeping backward compatibility

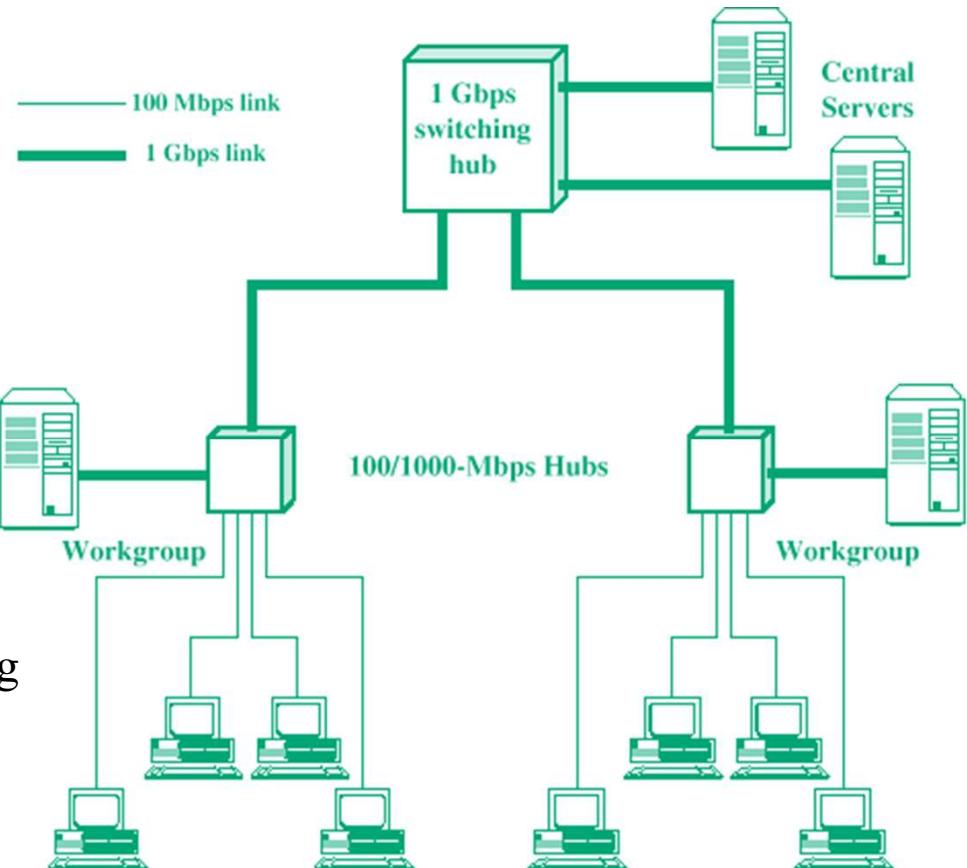
Differences vs 100Mbps at MAC level:

-**Carrier extension**, so the frame length of a transmission being longer than the propagation time at 1Gbps (principle of CSMA/CD)

Now transmission at least 4096 bit-times long
(512 bit-times for 10/100, min. frame length of 64octets)

-**Frame bursting**

Multiple short frames transmitted consecutively, without CSMA/CD control; avoids the overhead of carrier extension when a single station has a number of small frames ready to send.



Gigabit Ethernet - Physical specifications: Signaling - 8B/10B

Different approaches:

1000BaseSX

Short wavelength light, multimode fiber; duplex links @ 200-400m length

1000BaseLX

Long wavelength light, Multi or single mode fiber; duplex links @ 500 – 5000m length

1000BaseCX

Use of copper jumpers < 25m made from shielded twisted pair; cluster of stations, close situated

1000BaseT

4 pairs, cat 5 UTP

10Gigabit Ethernet (10GBaseX)

Why?

- increase in Internet and intranet traffic
- increase in the connection speed of each end-station
- increase of bandwidth-intensive applications

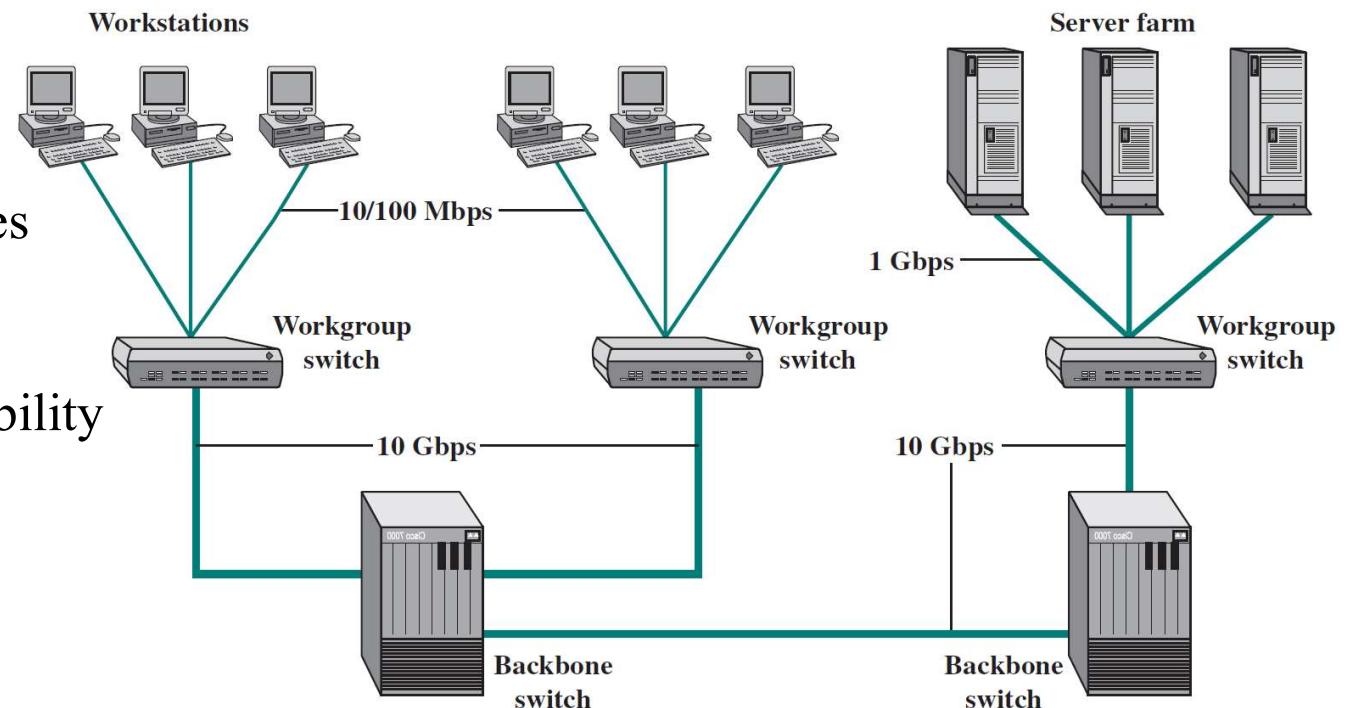
Allows the construction of MANs and WAN

Combining IP and Ethernet offers quality of service and traffic-policing capabilities

Range:

- from 300m to 40 km
- standard optical interfaces

Keeps backward compatibility



10Gigabit Ethernet

Different approaches:

10GBASE-S (short)

multimode fiber with distances up to 300 m
10GBASE-SR and 10GBASE-SW versions

10GBASE-L (long)

single-mode fiber with distances up to 10 km
10GBASE-LR and 10GBASE-LW versions

10GBASE-E (extended):

single-mode fiber with distances up to 40 km
10GBASE-ER and 10GBASE-EW versions

10GBASE-LX4:

single-mode or multimode with distances up to 10 km
uses wavelength division multiplexing (WDM) to multiplex the bit stream across four light waves.

100Gigabit Ethernet (100GBaseX)

Ethernet is the preferred carrier for bridging wireless technologies, such as Wi-Fi and WiMAX, into local networks.

Where?

Data center/Internet media providers

-to support the growth of Internet multimedia content and Web applications

Metro-video/service providers

-video on demand services

• Enterprise LANs

-converge networks (voice/video/data) and unified communications

-most enterprises still rely on 1-Gbps or a mix of 1-Gbps and 10-Gbps Ethernet,

-adoption of 100-Gbps Ethernet - slow.

• Internet exchanges/ISP core routing:

-massive amount of traffic

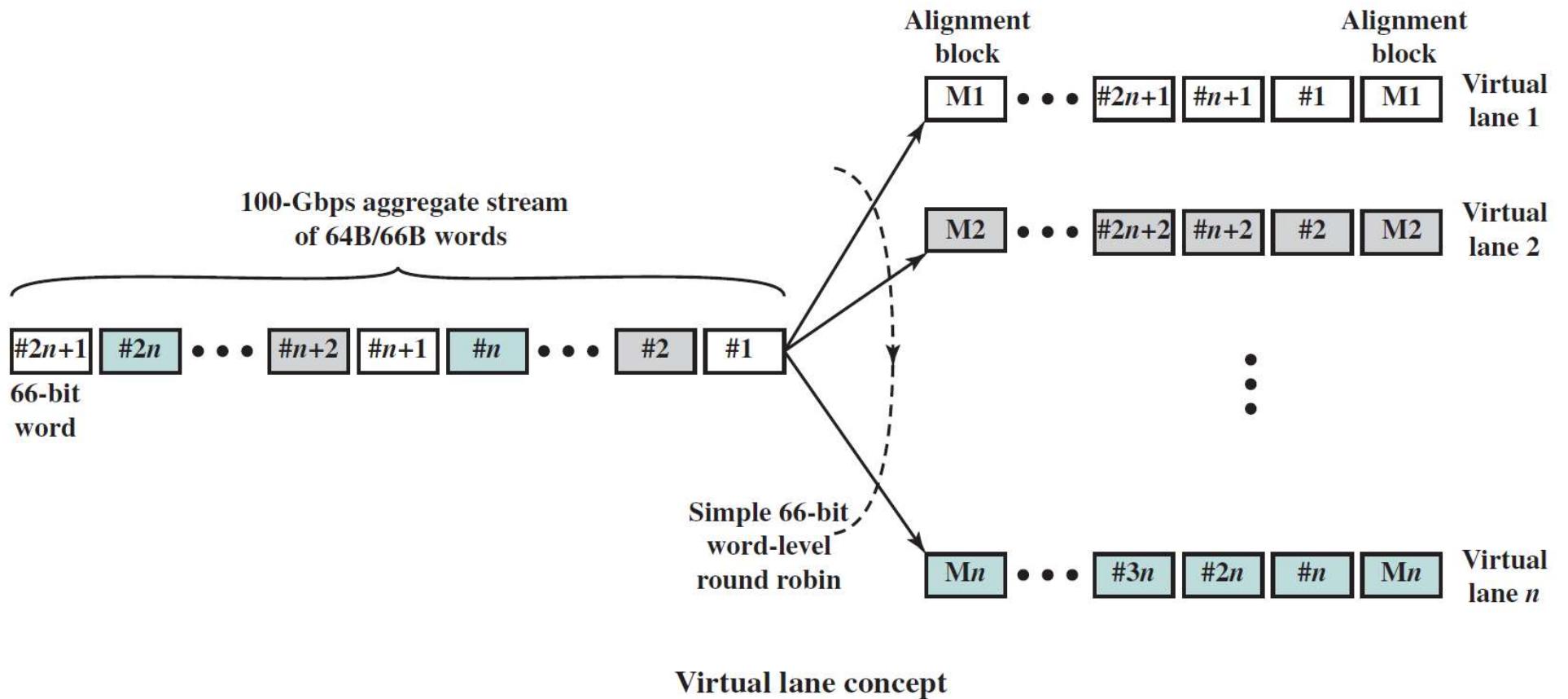
IEEE 802.3 working group: IEEE P802.3ba 40Gb/s and 100Gb/s Ethernet Task Force

-Keeps backward compatibility

New concepts: multilane distribution and virtual lanes

- **multilane distribution:**

- physical links implemented as multiple parallel channels
- separate physical wires **or** wavelength division multiplexing over a single optical fiber link



Media Options for 40-Gbps and 100-Gbps Ethernet

	40 Gbps	100 Gbps
1m backplane	40GBASE-KR4	
10 m copper	40GBASE-CR4	1000GBASE-CR10
100 m multimode fiber	40GBASE-SR4	1000GBASE-SR10
10 km single-mode fiber	40GBASE-LR4	1000GBASE-LR4
40 km single-mode fiber		1000GBASE-ER4

Naming nomenclature:

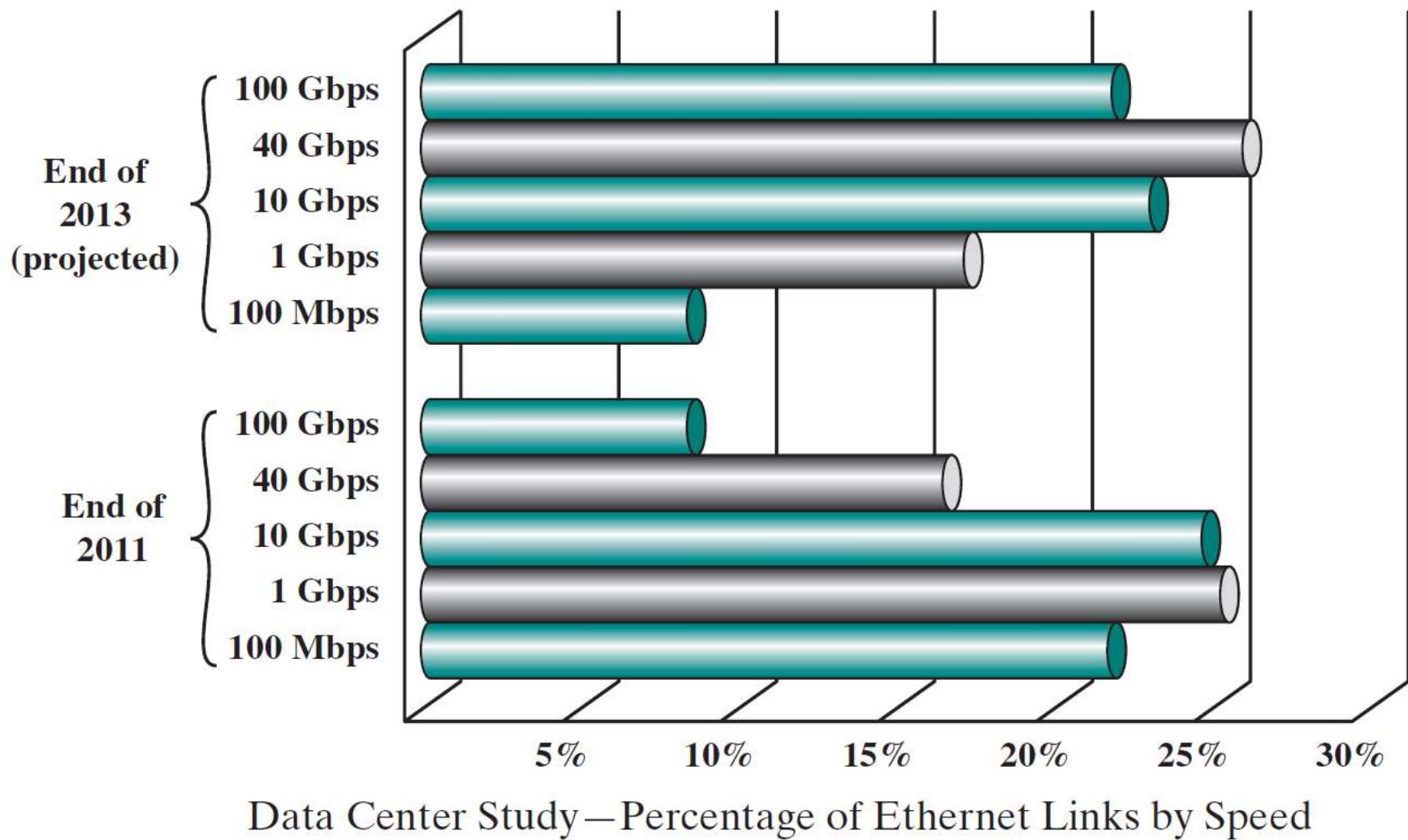
Copper: K = backplane; C = cable assembly

Optical: S = short reach (100 m); L = long reach (10 km); E = extended long reach (40 km)

Coding scheme: R = 64B/66B block coding

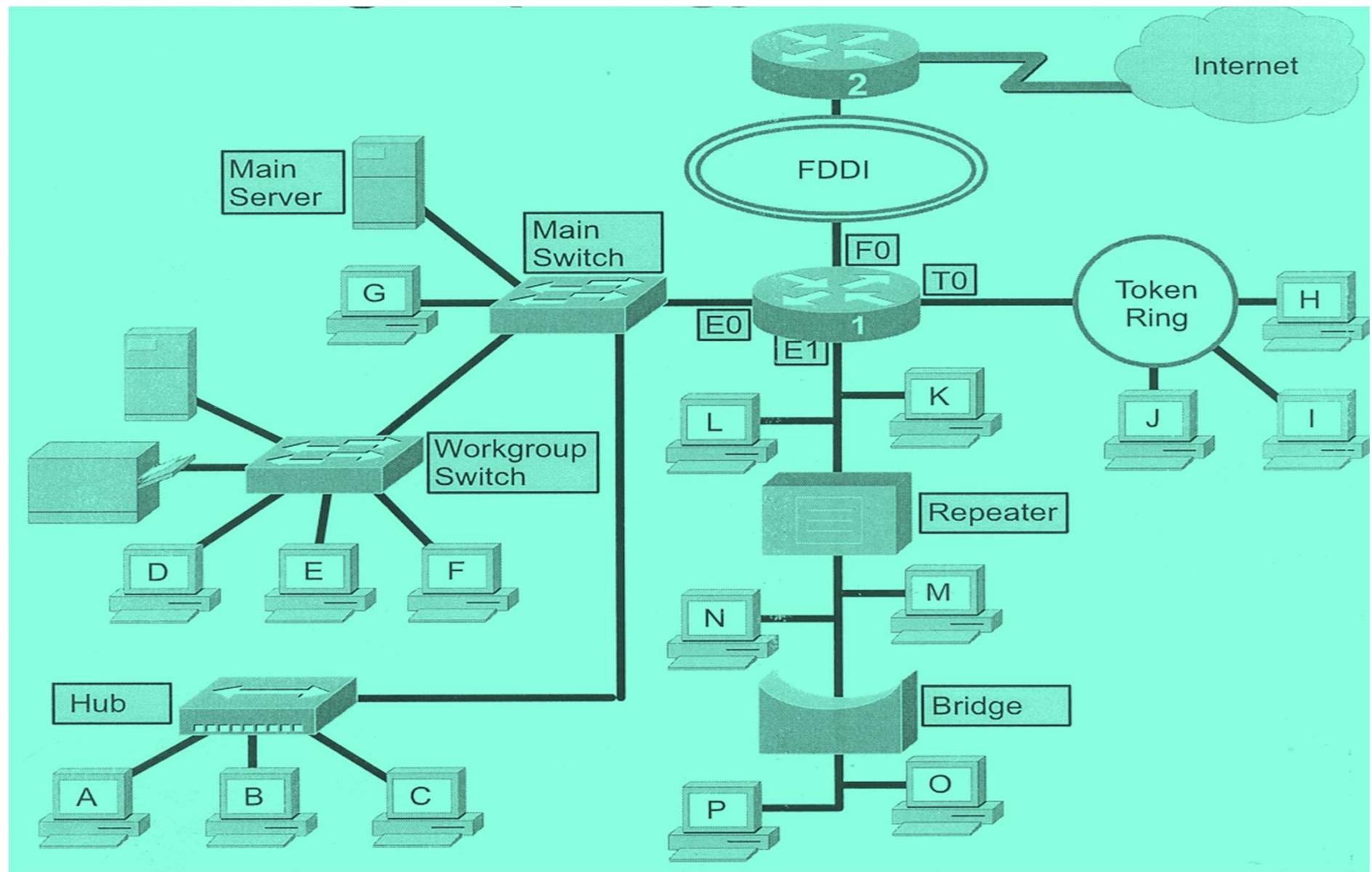
Final number: number of lanes (copper wires or fiber wavelengths)

From 100Mbps to 100Gbps Ethernet usage



LAN Interconnection

- different interconnecting devices, many approaches



Need for ability to expand beyond single LAN; appears concept of **Extended LAN**, extending the number of attached stations and maximum allowed distance between them

Provide interconnection to other LANs/WANs

Remember:

Repeater: regenerate and retime network signals at the bit level to allow them to travel a longer distance on the media

Hub: regenerate and retime network signals; process known as concentration; known as a multi-port repeater; use of a central connection point for the wiring media will increase the reliability of the network.

Bridge - a Layer 2 device designed to connect two LAN segments; filter traffic on a LAN, keep local traffic local, allow connectivity to other parts (segments) of the LAN for traffic that has been directed there

Switch - a Layer 2 device just as a bridge is; called a multi-port bridge

Router - work with that is at the OSI network layer; make decisions based on groups of network addresses (Classes), as opposed to individual Layer 2 MAC addresses



Hub



Bridge





Switch



Routers

Vasile Dadarlat- Local Area
Computer Networks

Bridges

Use Bridge or Router, but bridge is simpler (operates at Data Link level)

- Connects similar LANs

- Identical protocols for physical and data link layers

- Minimal processing

Router more general purpose: interconnect various LANs and WANs, level 3 device

Why Bridge?

Reliability – not an unique big LAN for that enterprise, but a set of small. Self contained units

Performance – avoid performance problem given by an increased number of stations

Security – may keep separately different kinds of traffic

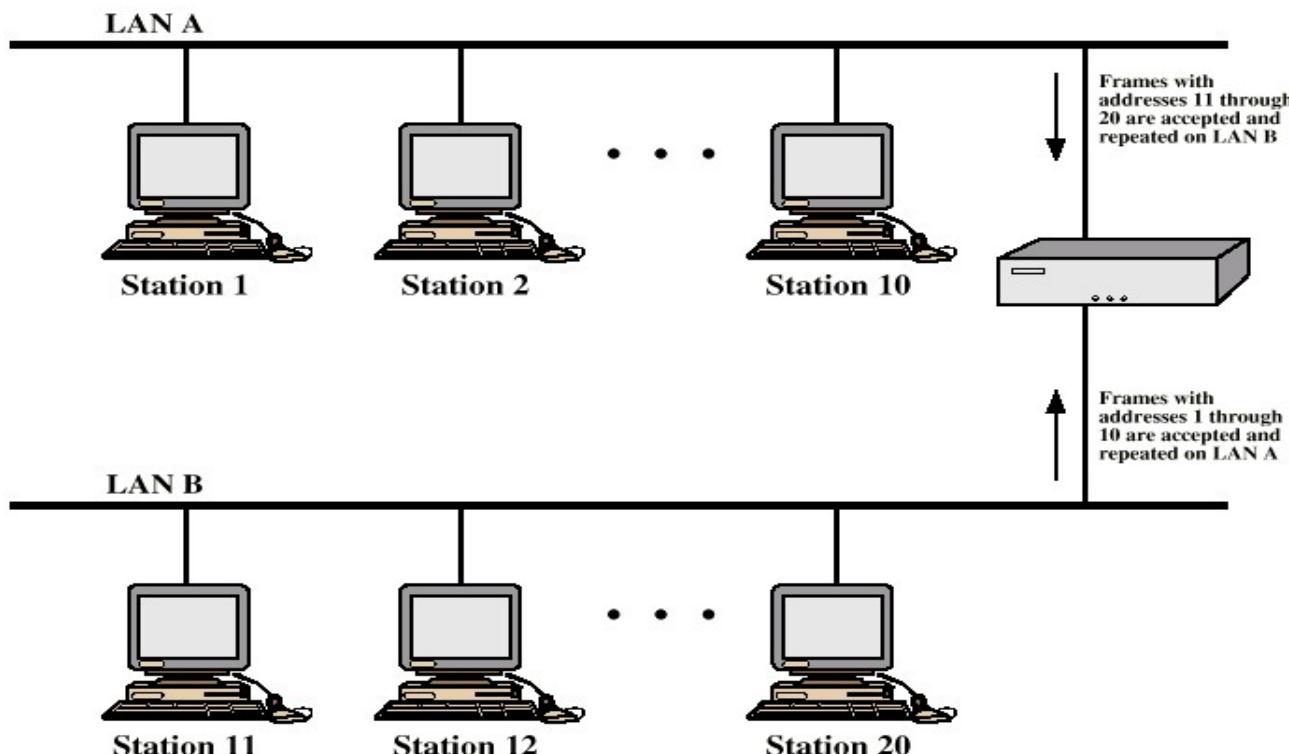
Geography – may interconnect geographically separated LANs

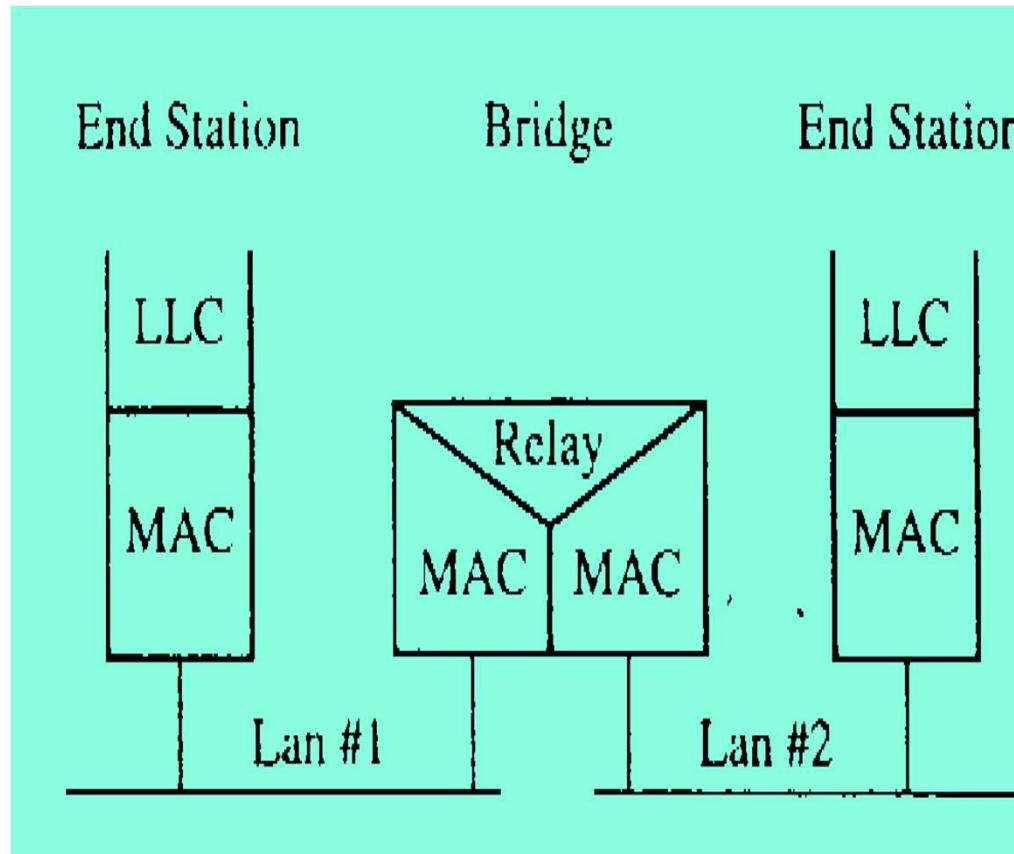
Two types of bridges:

transparent bridge – IEEE standard; operates in promiscuous mode, use of addressing tables

source-routing bridge – proposed by IBM's Token Ring, follows the route imposed by the source station

Bridge Operation





Bridge as protocol converter

Characteristics of a Transparent Bridge

Read all frames transmitted on one LAN, and accept those address to any station on the other LAN

Using MAC protocol for second LAN, retransmit each frame; acts as a **protocol relay**

Do the same the other way round

No modification to content or format of frame, no more encapsulation

Exact bitwise copy of frame

Minimal buffering to meet peak demand

Contains routing and address intelligence

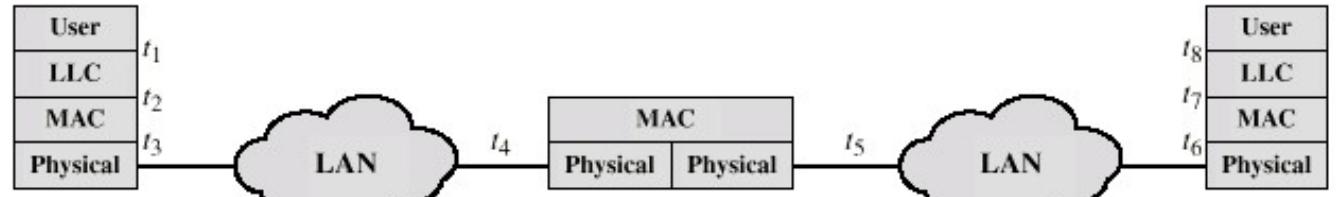
Must be able to tell which frames to pass

May be more than one bridge to cross

May connect more than two LANs

Bridging is **transparent** to stations

Appears to all stations on multiple LANs as if they are on one single LAN



Bridge Protocol Architecture

IEEE 802.1D standard

MAC level

Station address is at this level

Bridge does not need LLC layer

It is relaying MAC frames

Can pass frame over external comms system (WAN link)

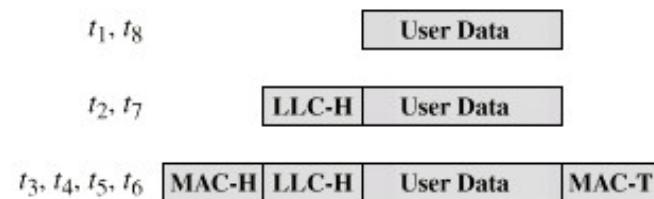
Capture frame

Encapsulate it

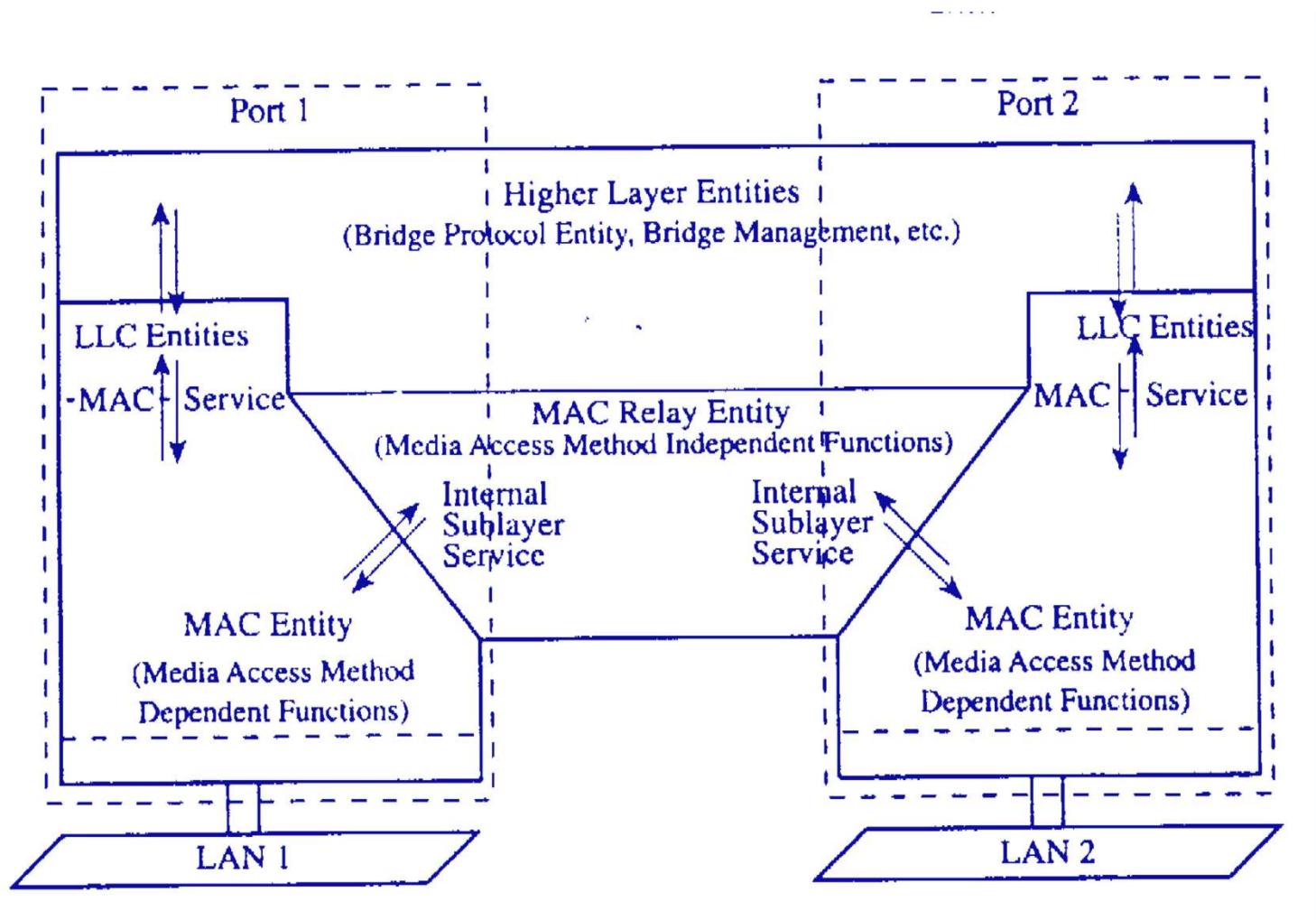
Forward it across link

Remove encapsulation and forward over LAN link

(a) Architecture



(b) Operation



Bridge Architectural Structure

Fixed Routing

Complex large LANs need alternative routes

- Load balancing

- Fault tolerance

Bridge must decide whether to forward frame

Bridge must decide which LAN to forward frame on

Routing selected for each source-destination pair of LANs

- Done in configuration

- Usually least hop route

- Only changed when topology changes

Spanning Tree

Algorithm used for:

Automatically develop **routing table**

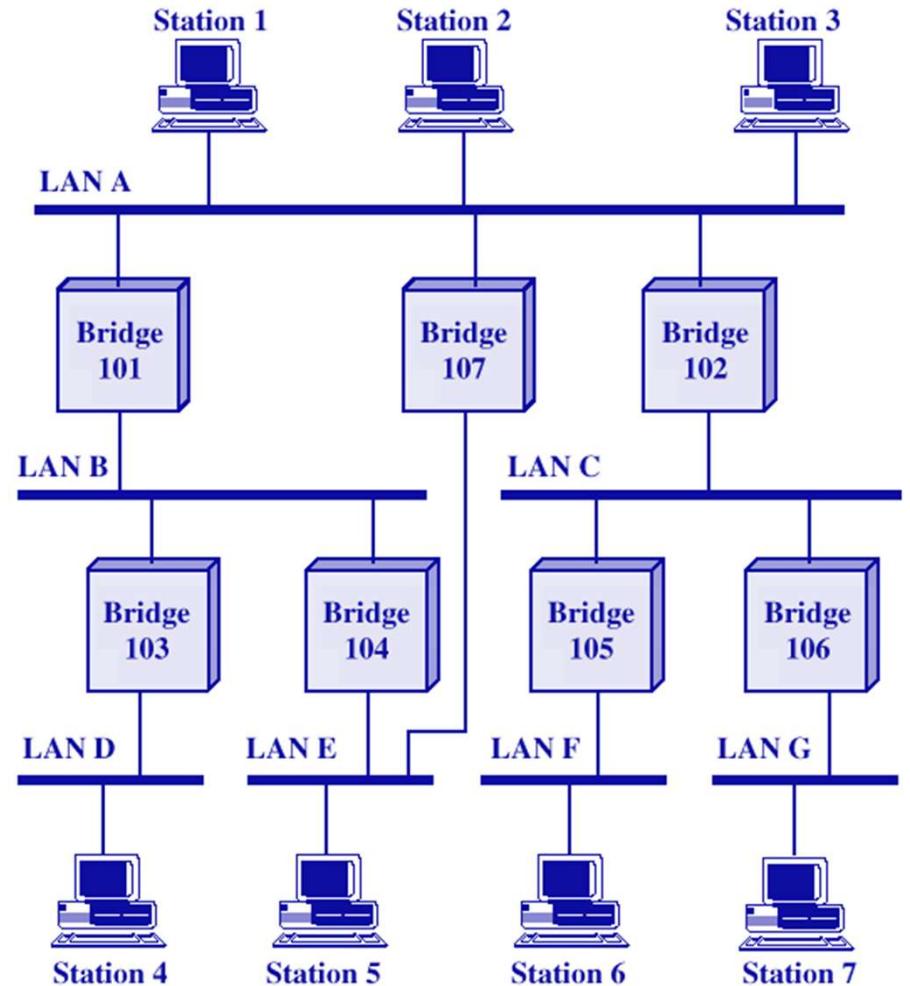
Automatically update in response to changes

Bridge Operations:

Frame forwarding

Address learning

Loop resolution



Frame forwarding

Maintain forwarding database for each port

 List station addresses reached through each port

For a frame arriving on port X:

 Search forwarding database to see if MAC address is listed for any port except X

 If address not found, forward to all ports except X

 If address listed for port Y, check port Y for blocking or forwarding state

 Blocking prevents port from receiving or transmitting

 If not blocked, transmit frame through port Y

Address Learning

Can preload forwarding database

Can be learnt

When frame arrives at port X, it has come from the LAN attached to port X

Use the source address to update forwarding database for port X to include that address

Timer on each entry in database

Each time frame arrives, source address checked against forwarding database

Loop Resolution

Use of Spanning Tree Algorithm

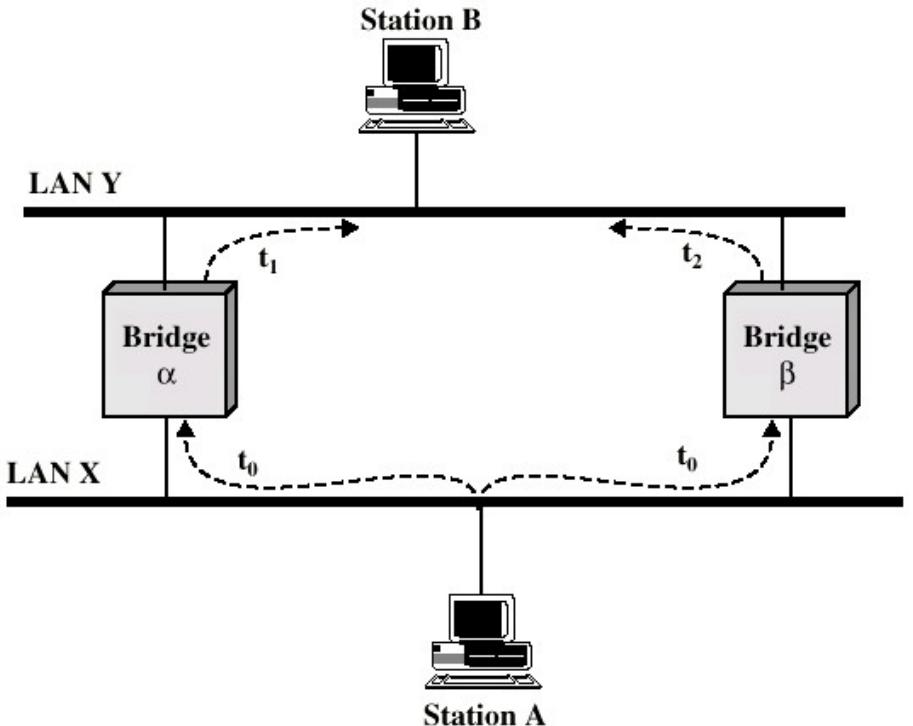
Address learning works for tree layout

i.e. no closed loops

THEORY: For any connected graph there is a spanning tree that maintains connectivity but contains no closed loops

Each bridge assigned unique identifier

Exchange between bridges of Configuration Bridge PDUs, to establish spanning tree (every 2 seconds).



IEEE 802.1d Spanning-Tree Protocol

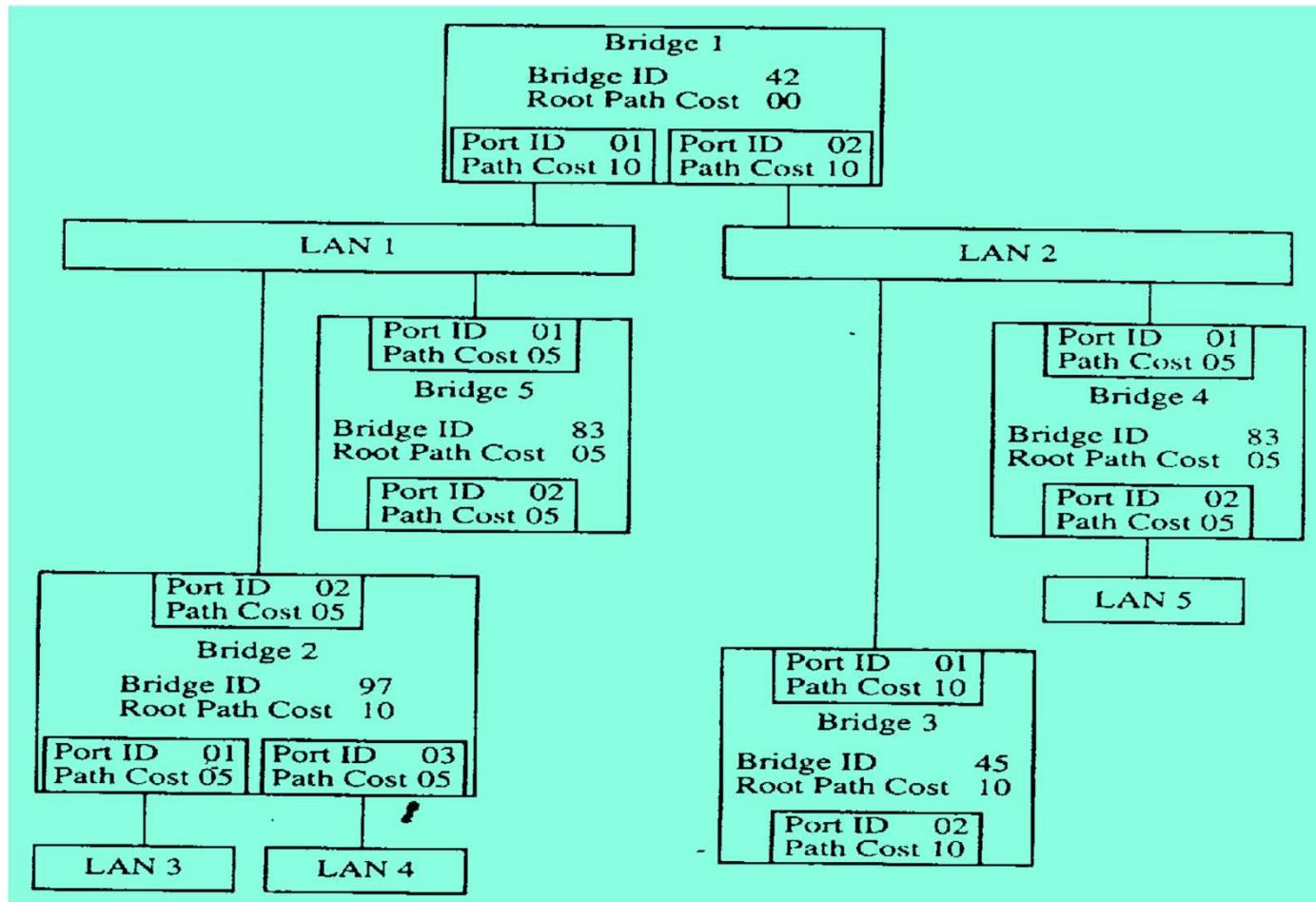
Root BID	Root Path Cost	Sender BID	Port ID
----------	----------------	------------	---------

BPDU message structure

7	6	5	4	3	2	1	0
Bridge Priority		MAC address					

BID structure

Spanning-tree algorithm used to configure the extended-LAN: sample of bridge IDs and associated costs



Link Speed	Cost
10Mbps	2000000
100Mbps	200000
1Gbps	20000
10Gbps	2000
1Tbps	20
10Tbps	2

Wireless LANs

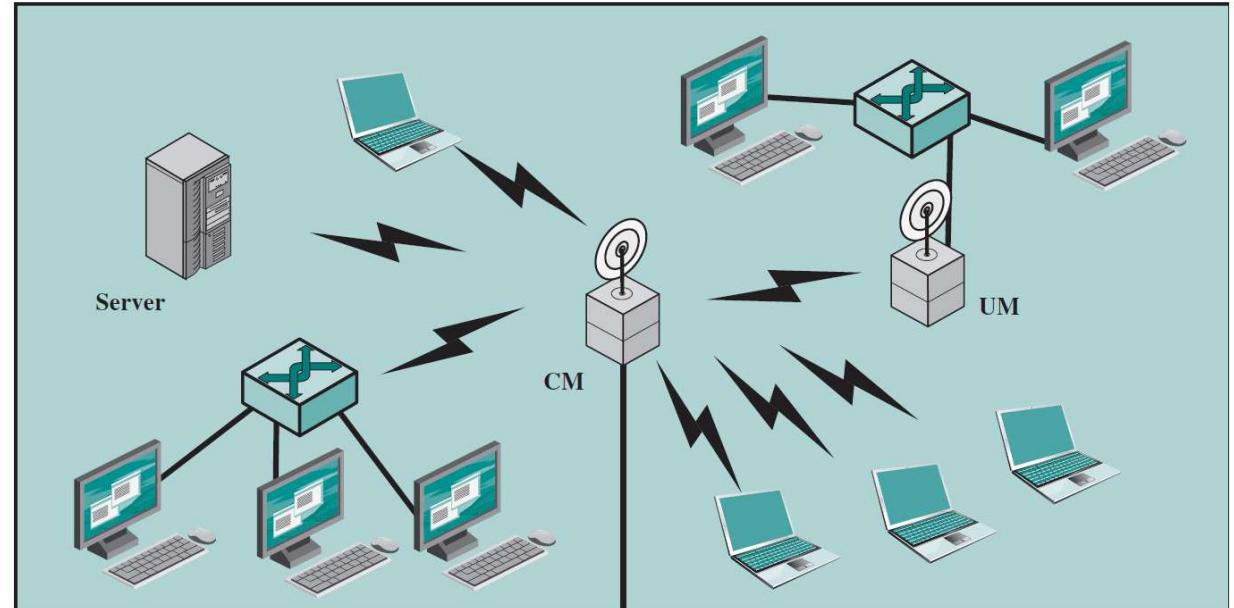
Mobility

Flexibility

Hard to wire areas

Reduced cost of wireless systems

Improved performance of wireless systems



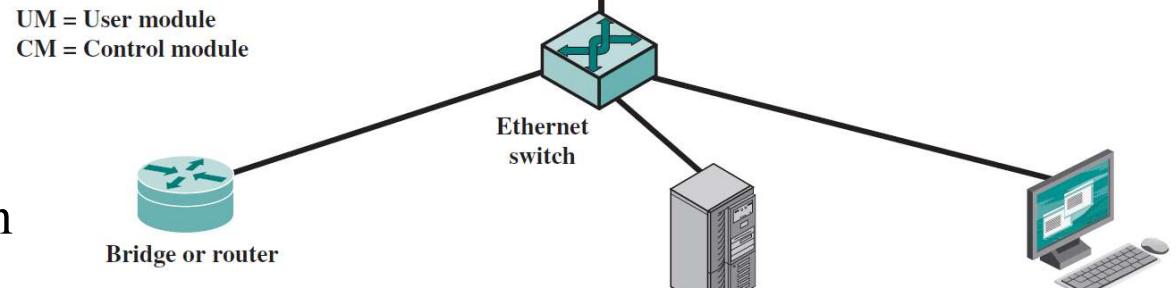
Wireless LAN Applications

LAN Extension

Cross building interconnection

Nomadic access

Ad hoc networks



Single Cell Wireless LAN

Wireless LANs (WLANs):

Use Radio Frequencies (RF) instead of cables at the physical layer and MAC sublayer of the data link layer.

Connect clients to a network through a wireless access point (AP) or wireless router, instead of an Ethernet switch.

Characteristic	802.11 Wireless LAN	802.3 Ethernet LANs
Physical Layer	Radio Frequency (RF)	Cable
Media Access	Collision Avoidance	Collision Detection
Availability	Anyone with a radio NIC in range of an access point	Cable connection required
Signal Interference	Yes	Inconsequential
Regulation	Additional regulation by country authorities	IEEE standard dictates

LAN Extension

Buildings with large open areas

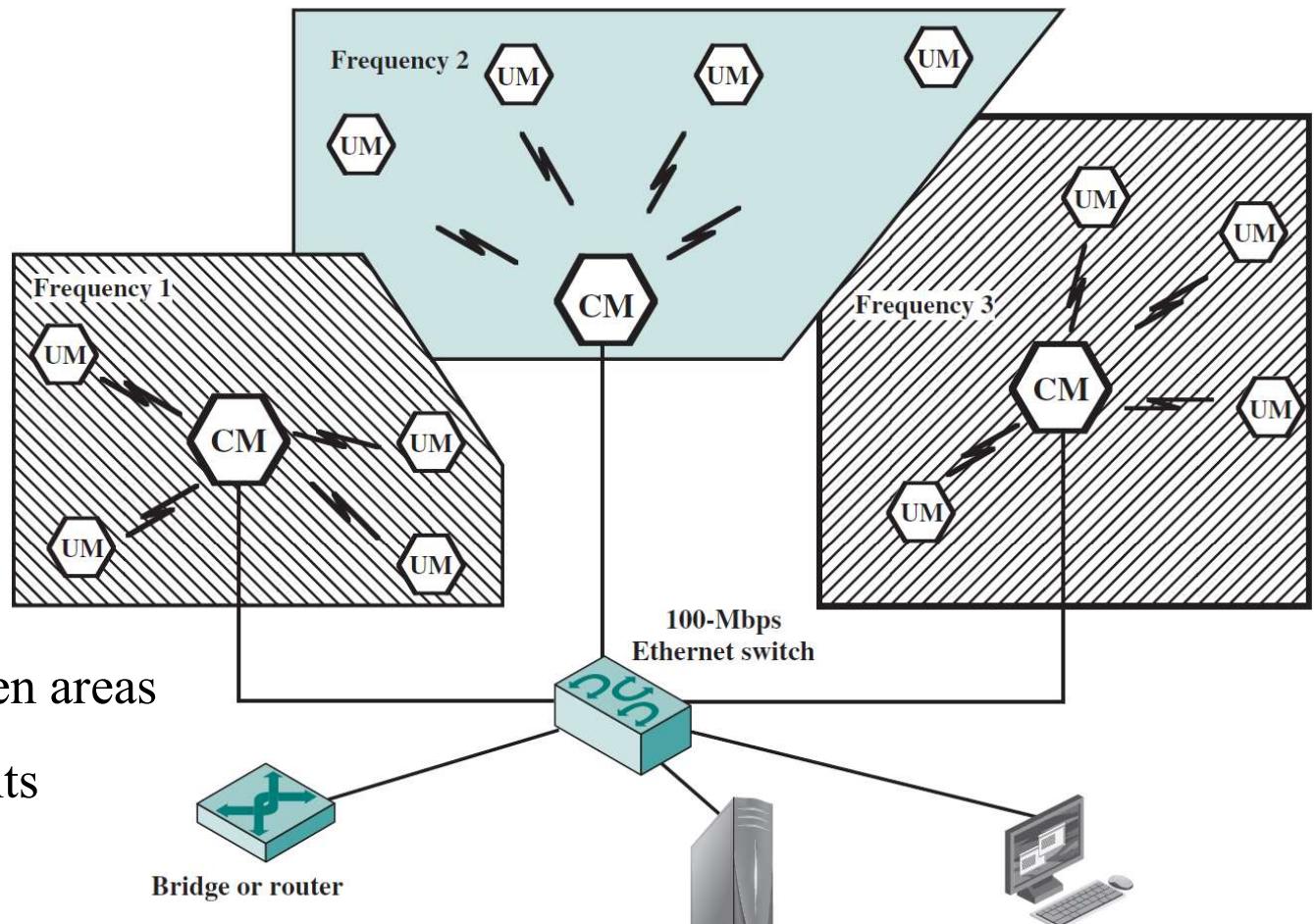
Manufacturing plants

Warehouses

Historical buildings

Small offices

May be mixed with fixed wiring system

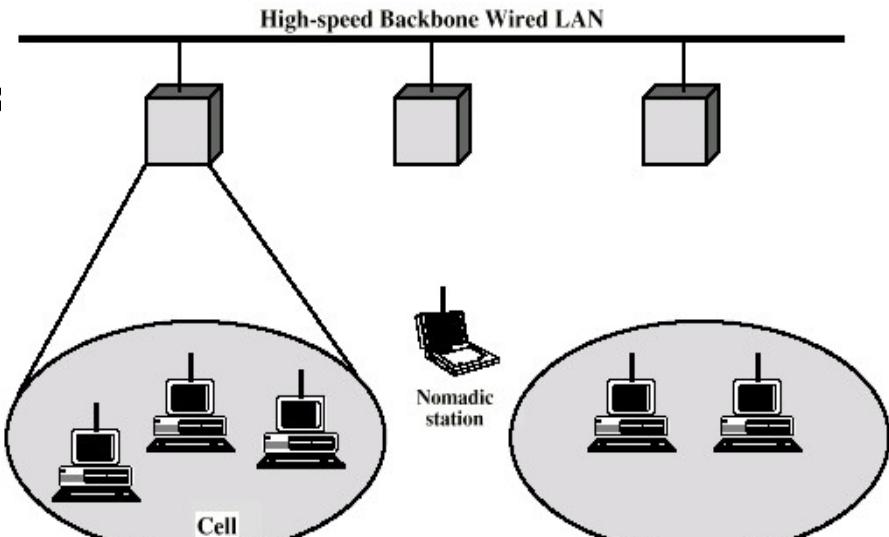


Cross Building Interconnection

Point to point wireless link between buildings

Typically connecting bridges or routers

Used where cable connection not possible,
e.g. across a street



(a) Infrastructure Wireless LAN

Nomadic Access

Mobile data terminal, e.g. laptop

Transfer of data from laptop to server

Campus or cluster of buildings



Ad Hoc Networking

Peer to peer

Temporary, e.g. conference

Wireless LAN Requirements

Throughput

Number of nodes

Connection to backbone

Service area

Battery power consumption

Transmission robustness and security

Collocated network operation

License free operation

Handoff/roaming

Dynamic configuration

Wireless LAN Technology

Infrared (IR) LANs

-Infrared Data Association: www.irda.org

Spread spectrum Radio LANs

Narrow band microwave

Comparative table

	Infrared	Spread Spectrum		Radio	
	Diffused Infrared	Directed Beam Infrared	Frequency Hopping	Direct Sequence	Narrowband Microwave
Data rate (Mbps)	1 to 4	1 to 10	1 to 3	2 to 20	10 to 20
Mobility	Stationary/mobile	Stationary with LOS	Mobile	Stationary/mobile	
Range (ft)	50 to 200	80	100 to 300	100 to 800	40 to 130
Detectability	Negligible		Little		Some
Wavelength/ frequency	λ : 800 to 900 nm		902 to 928 MHz 2.4 to 2.4835 GHz 5.725 to 5.85 GHz	902 to 928 MHz 5.2 to 5.775 GHz 18.825 to 19.205 GHz	
Modulation technique	ASK		FSK	QPSK	FS/QPSK
Radiated power	—		<1W		25 mW
Access method	CSMA	Token Ring, CSMA	CSMA		Reservation ALOHA, CSMA
License required	No		No		Yes unless ISM

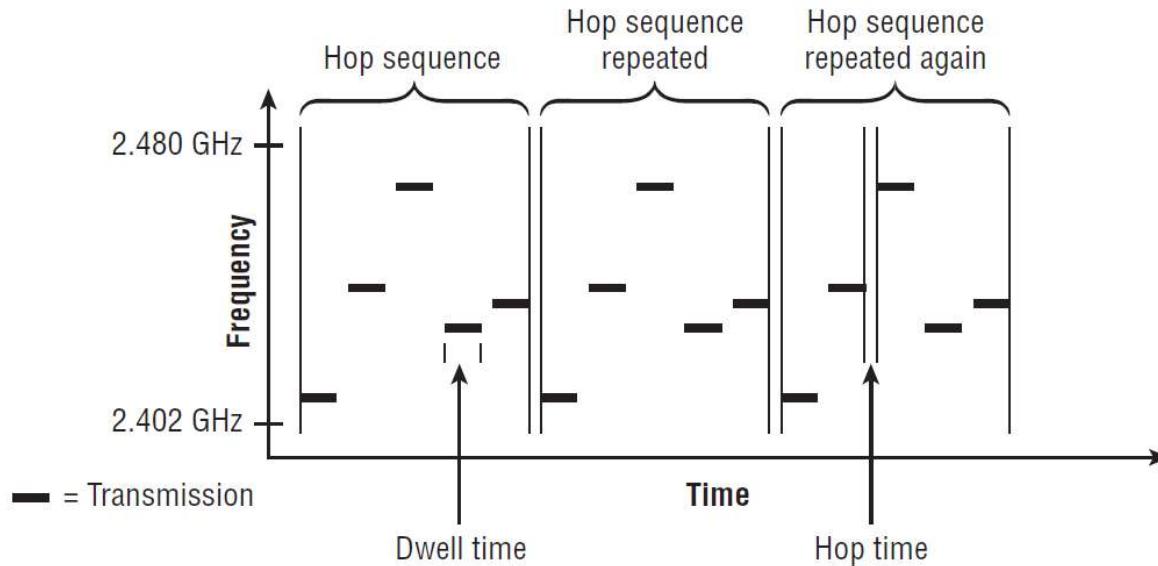
Spread Spectrum

FDM based technique using multiple carriers for the same data; improving reliability

Efficient for radio transmissions, where electromagnetic interferences or moving objects may change the optimum carrier frequency. Also energy consumption is low, so ideal for RF communications.

Spread Spectrum arranges for a sender to send signal on a set of carrier frequencies, the receiver checking all carrier frequencies. So the signal is spread over a wider bandwidth. Two techniques:

Frequency hopping (FHSS): signal is broadcast over a seemingly random series of RF carriers (use of table-derived frequencies), hopping from one frequency to another, at split-second intervals; the receiver, hopping between frequencies in synchronization with the sender, will pick-up the signal



Spread Spectrum

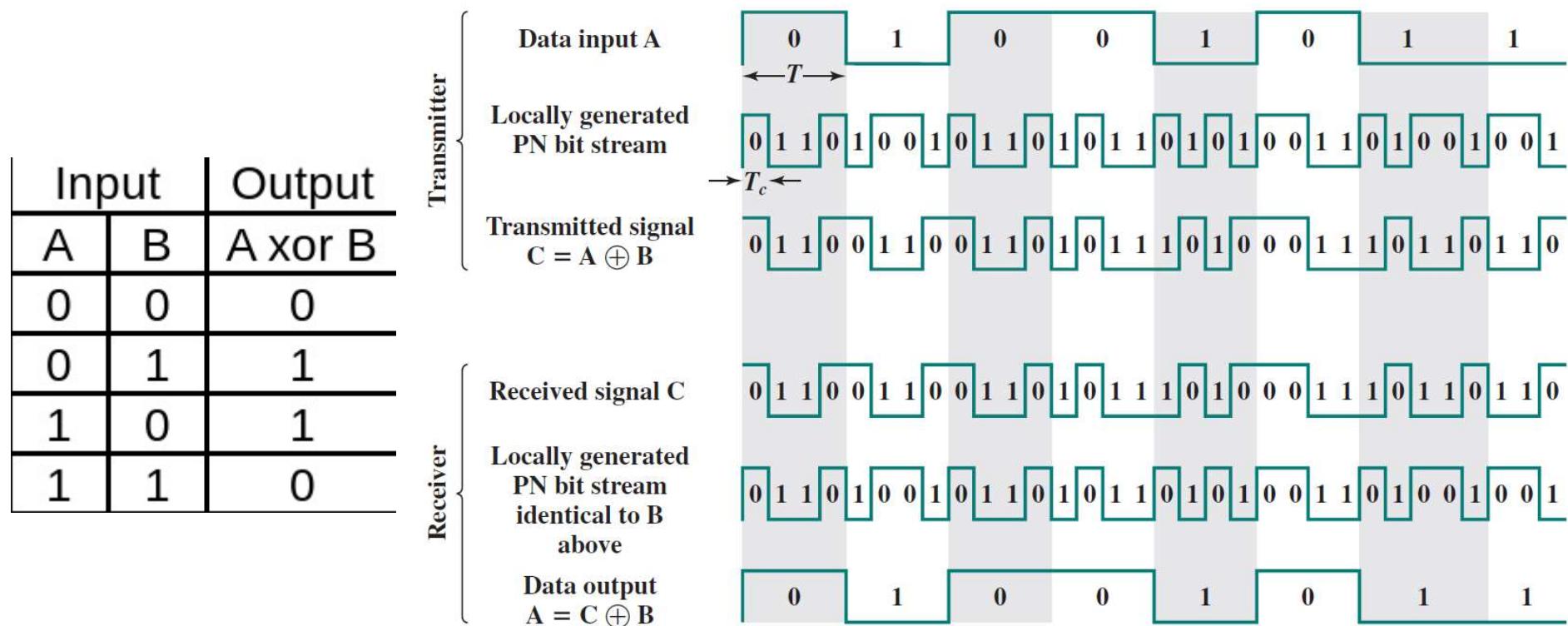
Direct sequence (DSSS): each bit in the original signal is represented by multiple bits in the transmitted signal – chipping code- (using more bits, wider bandwidth).

One technique: to combine the original digital information stream with a pseudo-random bit stream, by using a XOR function; a ‘1’ in data stream will invert the pseudorandom bit stream, a ‘0’ will pass unchanged the chipping code.

Barker code:

Binary data 1 = 1 0 1 1 0 1 1 1 0 0 0

Binary data 0 = 0 1 0 0 1 0 0 0 1 1 1



FHDS versus DSSS:

FH systems use a radio carrier that “hops” from frequency to frequency in a pattern known to both transmitter and receiver

- Easy to implement

- Resistance to noise

- Limited throughput (2-3 Mbps @ 2.4 GHz)

DS systems use a carrier that remains fixed to a specific frequency band. The data signal is spread onto a much larger range of frequencies (at a much lower power level) using a specific encoding scheme.

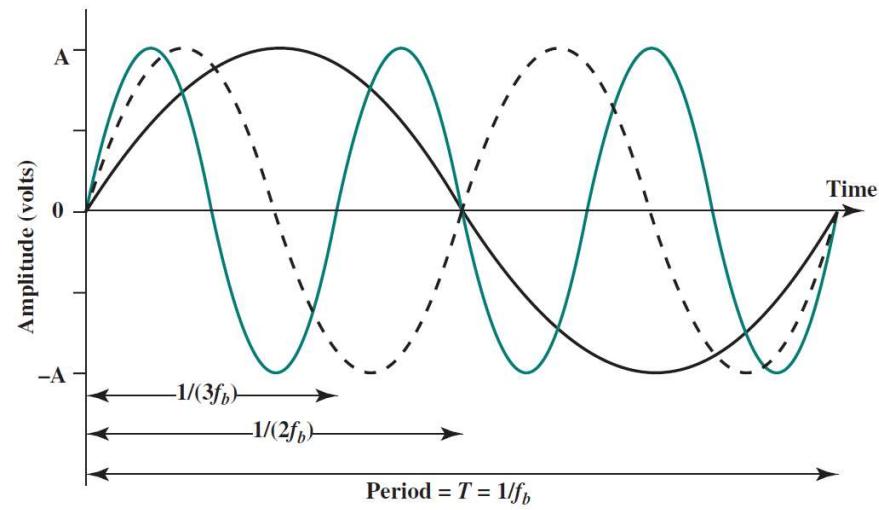
- Much higher throughput than FH (up to 11 Mbps)

- Better range

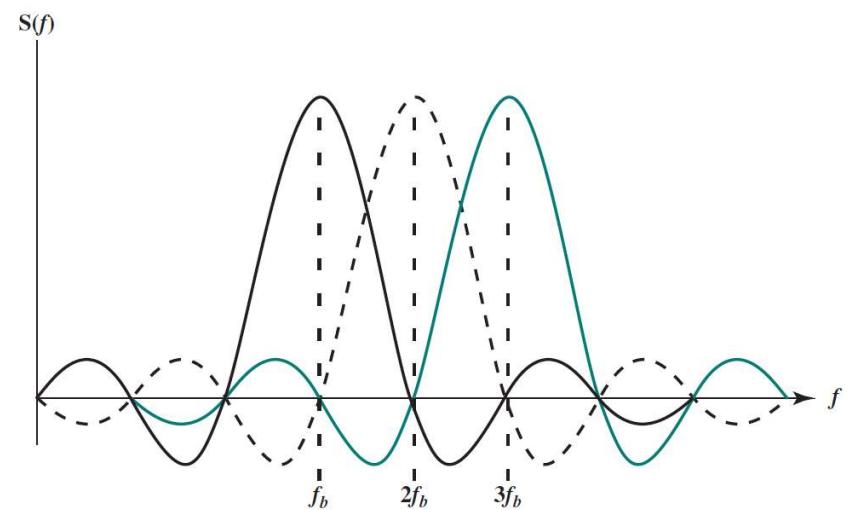
- Less resistant to noise (made up for by redundancy – it transmits at least 10 fully redundant copies of the original signal at the same time)

OFDM (Orthogonal Frequency Division Modulation)

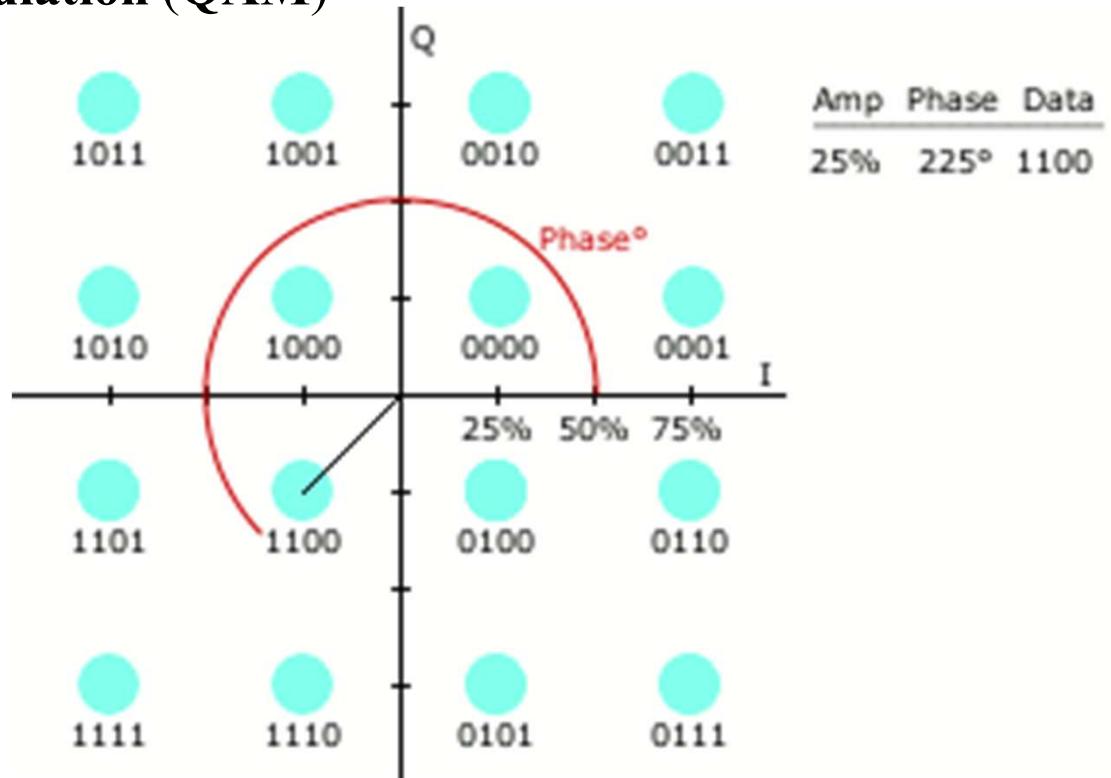
- Transmitting large amounts of digital data over a radio wave
- OFDM works by splitting the radio signal into multiple smaller sub-signals that are then transmitted simultaneously at different frequencies to the receiver
- Reduces the crosstalk (interferences) in wireless transmissions
- Use in WLANs



(a) Three subcarriers in time domain



Quadrature amplitude modulation (QAM)



Digital 16-QAM with example constellation points
(image from Wikipedia)

Example:

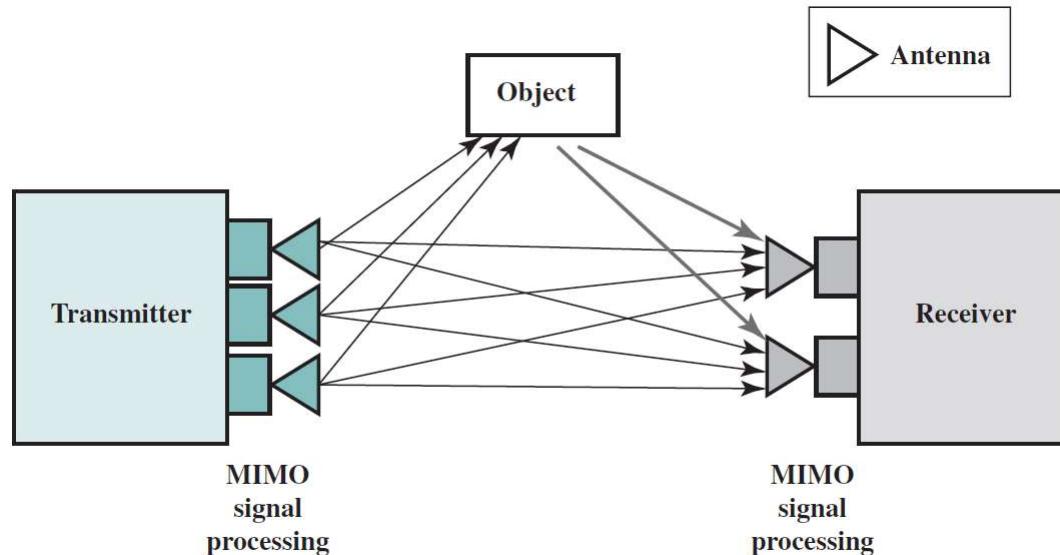
Use of a 256 QAM carrier; 1024bytes/sec would require less than 1KHz
OFDM 2000 means grouping 2000 carriers at different frequencies
For 8000 carriers QAM 256 at 1024bytes/sec, would give a throughput of
64Mbps for a spectrum band of 6MHz; extensive use in digital TV

Multiple-input-multiple-output (MIMO) antenna architecture

Key technology in evolving high-speed wireless networks => better receive signal

MIMO scheme

- the transmitter and receiver employ multiple antennas
- source
 - data stream divided into n substreams, one for each of the n transmitting antennas => multiple input
- Receiver
 - m antennas receive the transmissions from the n source antennas via a combination of line-of-sight transmission and multipath => multiple output



Industrial, scientific, and medical (**ISM**) frequency bands

- Different RF regulatory bodies

Lower Frequency MHz	Upper Frequency MHz	Comments
2400	2500	Often referred to as the 2.4 GHz band, this spectrum is the most widely used of the bands available for Wi-Fi. Used by 802.11b, g, & n. It can carry a maximum of three non-overlapping channels.
5725	5875	This 5 GHz band or 5.8 GHz band provides additional bandwidth, and being at a higher frequency, equipment costs are slightly higher, although usage, and hence interference is less. It can be used by 802.11a & n. It can carry up to 23 non-overlapping channels, but gives a shorter range than 2.4 GHz.

From: <http://www.radio-electronics.com/>

*Unlicensed National Information Infrastructure (**U-NII**) bands*

- Different RF regulatory bodies

Band	Frequency	Channels
U-NII-1	5.15 GHz – 5.25 GHz	4 channels
U-NII-2	5.25 GHZ – 5.35 GHz	4 channels
U-NII-2 Extended	5.47 GHZ – 5.725 GHz	12 channels*
U-NII-3	5.725 GHz – 5.85 GHz	5 channels

Wireless LANs – standard IEEE 802.11

A family of wireless LAN (WLAN) specifications developed by a working group at the Institute of Electrical and Electronic Engineers (IEEE)

Defines standard for WLANs using the following four technologies:

- Frequency Hopping Spread Spectrum (FHSS)

- Direct Sequence Spread Spectrum (DSSS)

- Infrared (IR)

- Orthogonal Frequency Division Multiplexing (OFDM)

Versions: 802.11a, 802.11b, 802.11g, 802.11e, 802.11f, 802.11i

802.11a offers speeds with a theoretically maximum rate of 54Mbps in the 5 GHz band; implements OFDM

- Industrial, scientific, and medical (ISM) frequency bands

802.11b offers speeds with a theoretically maximum rate of 11Mbps at in the 2.4 GHz spectrum band; implements DSSS, less power, but more noise-dependent

- Industrial, scientific, and medical (ISM) frequency bands

- much more crowded frequency space

<i>802.11a vs. 802.11b</i>	<i>802.11a</i>	<i>802.11b</i>
<i>Raw data rates</i>	<i>Up to 54 Mbps (54, 48, 36, 24, 18, 12 and 6 Mbps)</i>	<i>Up to 11 Mbps (11, 5.5, 2, and 1 Mbps)</i>
<i>Range</i>	<i>50 Meters</i>	<i>100 Meters</i>
<i>Bandwidth</i>	<i>UNII and ISM (5 GHz range)</i>	<i>ISM (2.4000— 2.4835 GHz range)</i>
<i>Modulation</i>	<i>OFDM technology</i>	<i>DSSS technology</i>

802.11g is a new standard for data rates of up to a theoretical maximum of 54 Mbps at 2.4 GHz

802.11g is a high-speed extension to 802.11b

Compatible with 802.11b

High speed up to 54 Mbps

2.4 GHz (vs. 802.11a, 5 GHz)

Using OFDM for backward compatibility

Adaptive Rate Shifting

Protocol	Frequency Band	Compatibility	Theoretical Rate	Actual Rate
802.11a	5 GHz	N/A	54 Mbit/s	About 22 Mbit/s
802.11b	2.4 GHz	N/A	11 Mbit/s	About 5 Mbit/s
802.11g	2.4 GHz	Compatible with 802.11b	54 Mbit/s	About 22 Mbit/s

802.11n

- 2.4 & 5 GHz frequency bands
- *High Throughput (HT)*, that provides PHY and MAC enhancements to support data rates of up to 600 Mbps
- 40 MHz channels
- use *multiple-input, multiple-output (MIMO)* technology in addition with OFDM technology.
 - multiple receiving and transmitting antennas
 - capitalizes on the effects of multipath as opposed to compensating for or eliminating multipath

802.11ac

5 GHz frequency bands (2.4 GHz ISM band cannot provide needed frequency space)

- *Very High Throughput (VHT)*
- 80 MHz and 160 MHz channels
- 256-QAM modulation
- designed to transmit and receive up to eight spatial streams

	802.11n	802.11n	802.11ac Wave 1	802.11ac Wave2 WFA Certification Process Continues	802.11ac
	IEEE Specification		Today		IEEE Specification
Band	2.4 GHz & 5 GHz	2.4 GHz & 5 GHz	5 GHz	5 GHz	5 GHz
MIMO	Single User (SU)	Single User (SU)	Single User (SU)	Multi User (MU)	Multi User (MU)
PHY Rate	450 Mbps	600 Mbps	1.3 Gbps	2.34 Gbps - 3.47 Gbps	6.9 Gbps
Channel Width	20 or 40 MHz	20 or 40 MHz	20, 40, 80 MHz	20, 40, 80, 80-80, 160 MHz	20, 40, 80, 80-80, 160 MHz
Modulation	64 QAM	64 QAM	256 QAM	256 QAM	256 QAM
Spatial Streams	3	4	3	3-4	8
MAC Throughput*	293 Mbps	390 Mbps	845 Mbps	1.52 Gbps- 2.26 Gbps	4.49 Gbps

* Assuming a 65% MAC efficiency with highest MCS.

Future Wi-Fi Frequencies

- Very High Throughput (VHT) technology: **60GHz**
- **White-Fi:** use of Wi-Fi technology in the unused television RF spectrum also known as TV white space

Key IEEE 802.11 Standards

Standard	Scope
IEEE 802.11a	Physical layer: 5-GHz OFDM at rates from 6 to 54 Mbps
IEEE 802.11b	Physical layer: 2.4-GHz DSSS at 5.5 and 11 Mbps
IEEE 802.11c	Bridge operation at 802.11 MAC layer
IEEE 802.11d	Physical layer: Extend operation of 802.11 WLANs to new regulatory domains (countries)
IEEE 802.11e	MAC: Enhance to improve quality of service and security mechanisms
IEEE 802.11g	Physical layer: Extend 802.11b to data rates >20 Mbps
IEEE 802.11i	MAC: Enhance security and authentication mechanisms
IEEE 802.11n	Physical/MAC: Enhancements to enable higher throughput
IEEE 802.11T	Recommended practice for the evaluation of 802.11 wireless performance
IEEE 802.11ac	Physical/MAC: Enhancements to support 0.5–1 Gbps in 5-GHz band
IEEE 802.11ad	Physical/MAC: Enhancements to support ≥ 1 Gbps in the 60-GHz band

Wireless LANs – standard IEEE 802.11continued

Basic service set (BSS - cell)

Set of stations using same MAC protocol

Competing to access shared medium

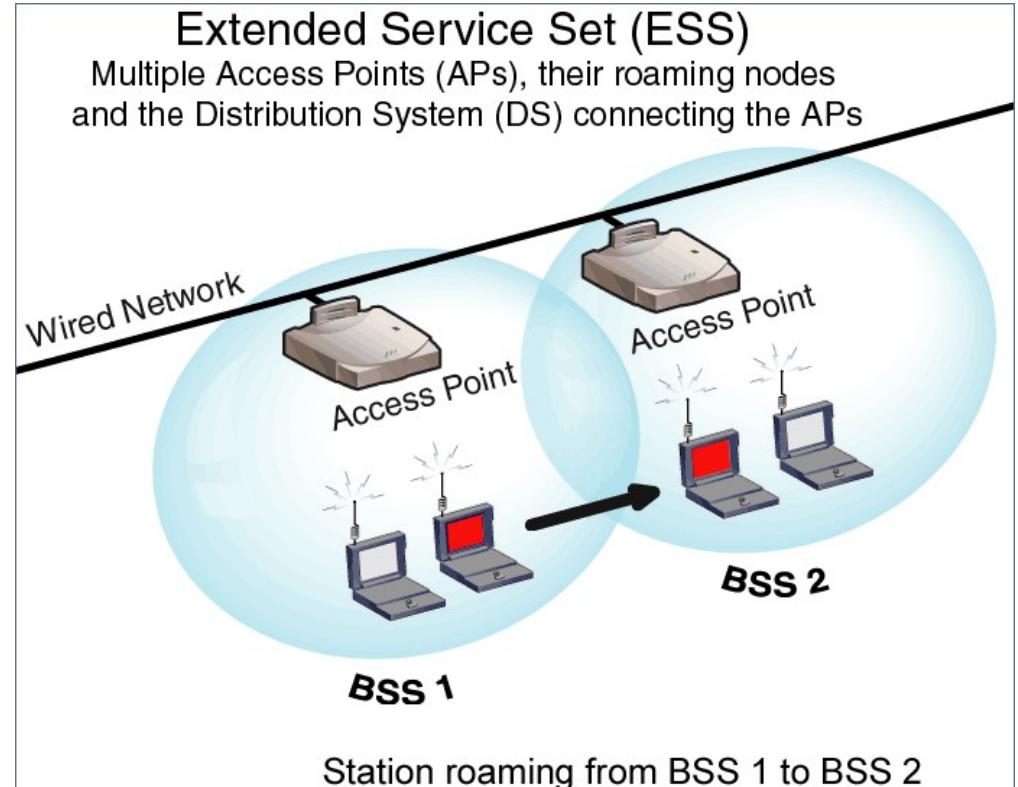
May be isolated

May connect to backbone via access point (bridge)

Extended service set (ESS)

Two or more BSS connected by distributed system

Appears as single logic LAN to LLC level



Types of station

Based on mobility:

-No transition

Stationary or moves within direct communication range of single BSS

-BSS transition

Moves between BSSs within single ESS

-ESS transition

From a BSS in one ESS to a BSS in another ESS

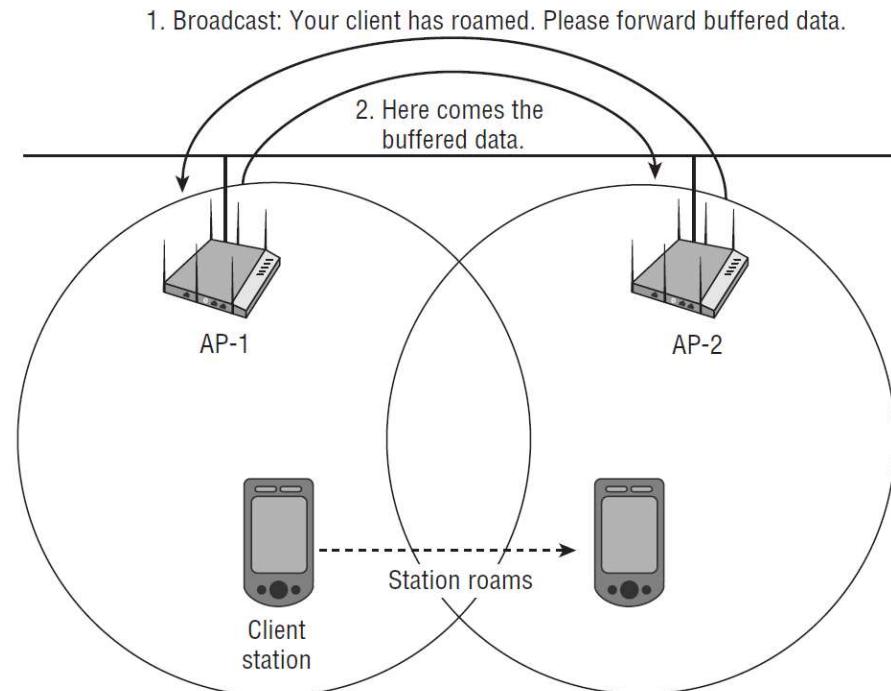
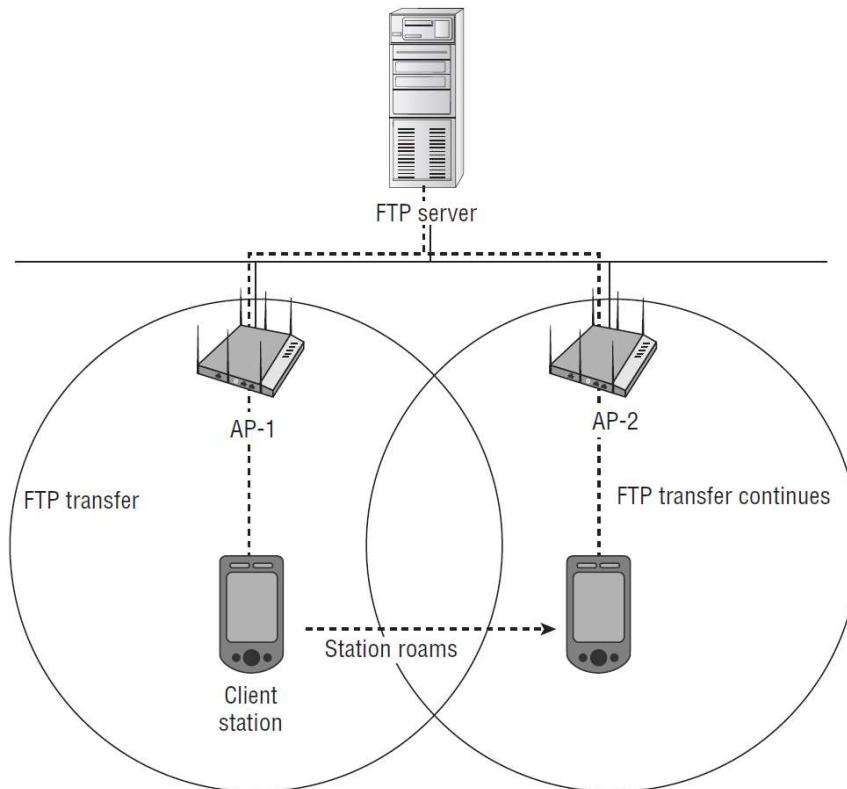
Disruption of service likely

Mobility:

802.11 standard mandated that vendor access points support **roaming**

- allow client stations communicating through one AP to move and continue communications on a new AP (coverage area overlaps).

Seamless roaming



Association-Related Services

- **Association:**

- initial association between a station and an AP
- a station must identify itself before transmitting or receiving frames on a WLAN => association with an AP within a particular BSS
- the AP can communicate this information to other APs within the ESS to facilitate routing and delivery of addressed frames.

- **Reassociation:**

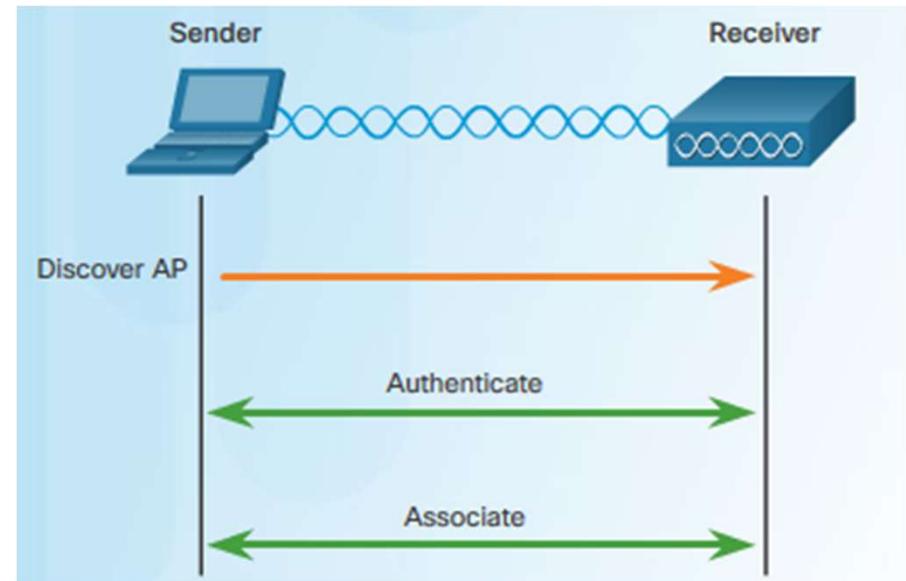
- an established association can be transferred from one AP to another, allowing a mobile station to move from one BSS to another.

- **Disassociation:**

- a station/AP notifies an existing association is terminated.
- a station should give this notification before leaving an ESS or shutting down

Wireless Network Operations

- Wireless client association process with AP includes discovering a new wireless AP, authenticating with that AP, then associating with that AP.
- Common configurable wireless parameters include:
 - **Network mode**
 - **SSID**
 - **Channel settings**
 - **Security mode**
 - **Encryption**
 - **Password**



- Wireless devices must discover and connect to an AP or wireless router. This process can be passive or active.
- The 802.11 standard was originally developed with two authentication mechanisms: **open authentication** provides wireless connectivity to any wireless device, and the **shared key authentication** technique is based on a key that is pre-shared between the client and the AP.

- Access Point (AP):
 - **Small network** – usually a wireless router that integrates the functions of a router.
 - **Large network** – can be many APs.
- Wireless LAN Controller (WLC):
 - Controls and manages the functions of the APs on a network.
 - Simplifies configuration and monitoring of numerous APs.
 - Controls Lightweight Access Points using the
 - Hardware or virtualized (cloud-based)
- Lightweight AP (LWAP):
 - Centralized management by WLC.
 - No longer acts autonomously.



Vasile Dadarlat - Local Ar
Computer Networks

Wireless LAN - Physical

Infrared

1Mbps and 2Mbps
Wavelength 850-950nm

Direct sequence spread spectrum

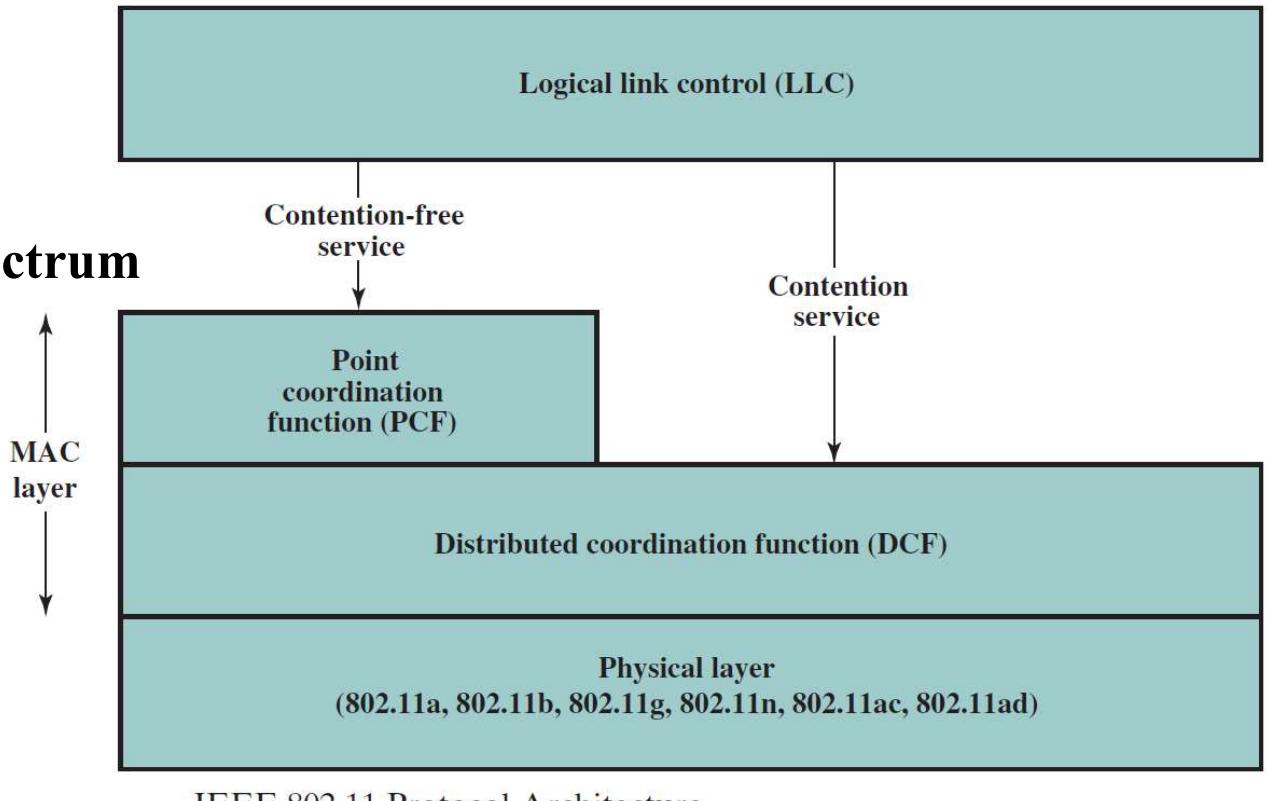
2.4GHz ISM band
Up to 7 channels
Each 1Mbps or 2Mbps

Frequency hopping spread spectrum

2.4GHz ISM band
1Mbps or 2Mbps

OFDM

Others



IEEE 802.11 Physical Layer Standards

Standard	802.11a	802.11b	802.11g	802.11n	802.11ac	802.11ad
Year introduced	1999	1999	2003	2000	2012	2014
Maximum data transfer speed	54 Mbps	11 Mbps	54 Mbps	65 to 600 Mbps	78 Mbps to 3.2 Gbps	6.76 Gbps
Frequency band	5 GHz	2.4 GHz	2.4 GHz	2.4 or 5 GHz	5 GHz	60 GHz
Channel bandwidth	20 MHz	20 MHz	20 MHz	20, 40 MHz	40, 80, 160 MHz	2160 MHz
Highest order modulation	64 QAM	11 CCK	64 QAM	64 QAM	256 QAM	64 QAM
Spectrum usage	DSSS	OFDM	DSSS, OFDM	OFDM	SC-OFDM	SC, OFDM
Antenna configuration	1×1 SISO	1×1 SISO	1×1 SISO	Up to 4×4 MIMO	Up to 8×8 MIMO, MU-MIMO	1×1 SISO

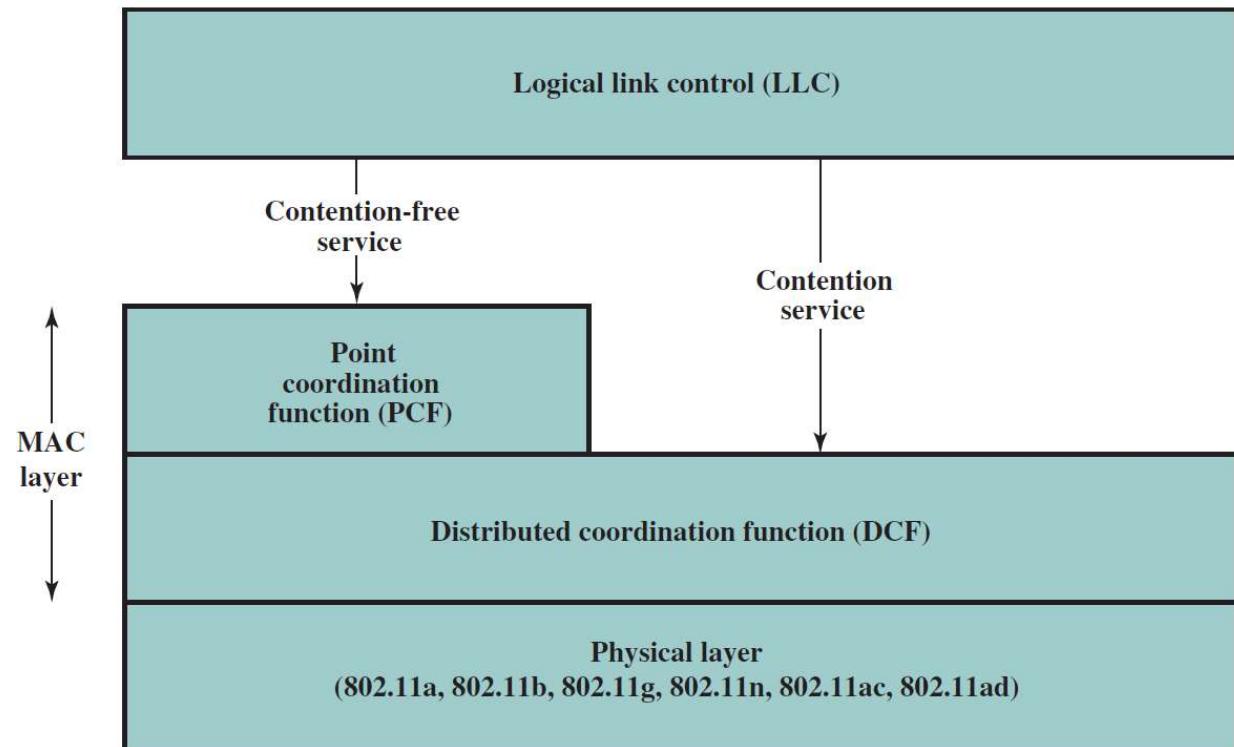
Media Access Control (IEEE 802.11)

Distributed wireless foundation MAC (DWFMAC) – MAC algorithm

Sublayers:

Distributed coordination function (DCF)

- CSMA without collision detection
- No collision detection, due to the nature of WLAN signal (dynamic range of signals in medium, some are weak or noise affected)
- Set of delays (acts as a priority scheme) – for a fair access; based on IFS (InterFrame Space)



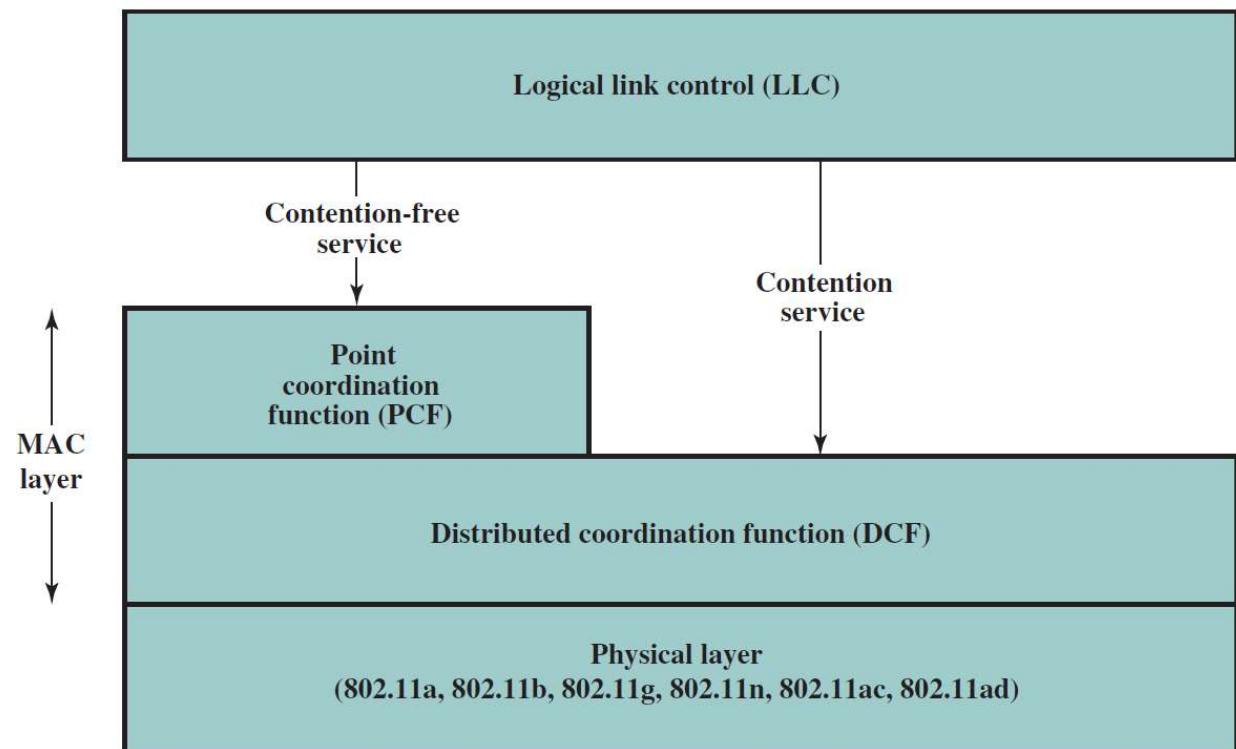
IEEE 802.11 Protocol Architecture

Media Access Control (IEEE 802.11)

Sublayers:

Point coordination function (PCF) – on top of DCF

- Polling of central master (point coordinator)
- Uses PIFS, and being shorter than DIFPS, can seize the medium and lock out traffic while issuing polls
- For preventing lock out of all traffic, use of **superframe**, allowing polling for first superframe half, and allowing contention period in the second half (see next slides)



More on DCF:

Basic delay unit **IFS** (interframe space)

Three values for IFS:

- SIFS (Short IFS) – immediate response actions, used with ACKs, or for poll responses

- PIFS (Point coordination function IFS) – used by central controller when issuing polls

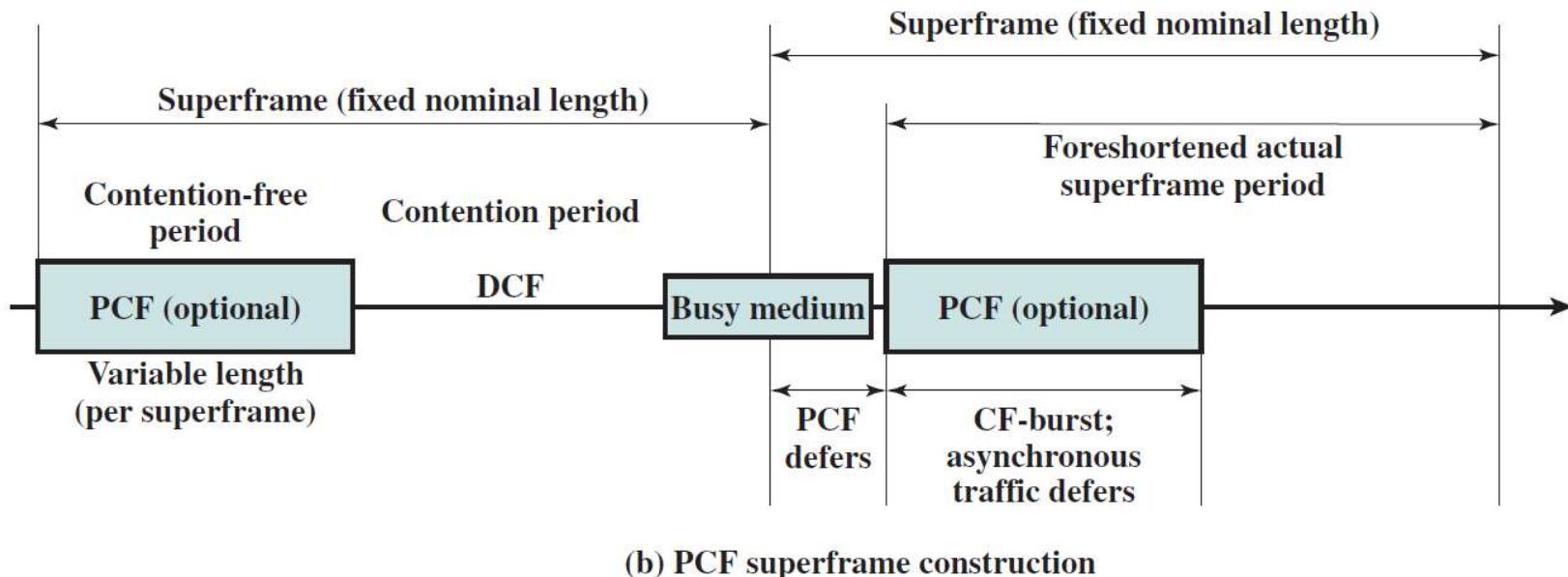
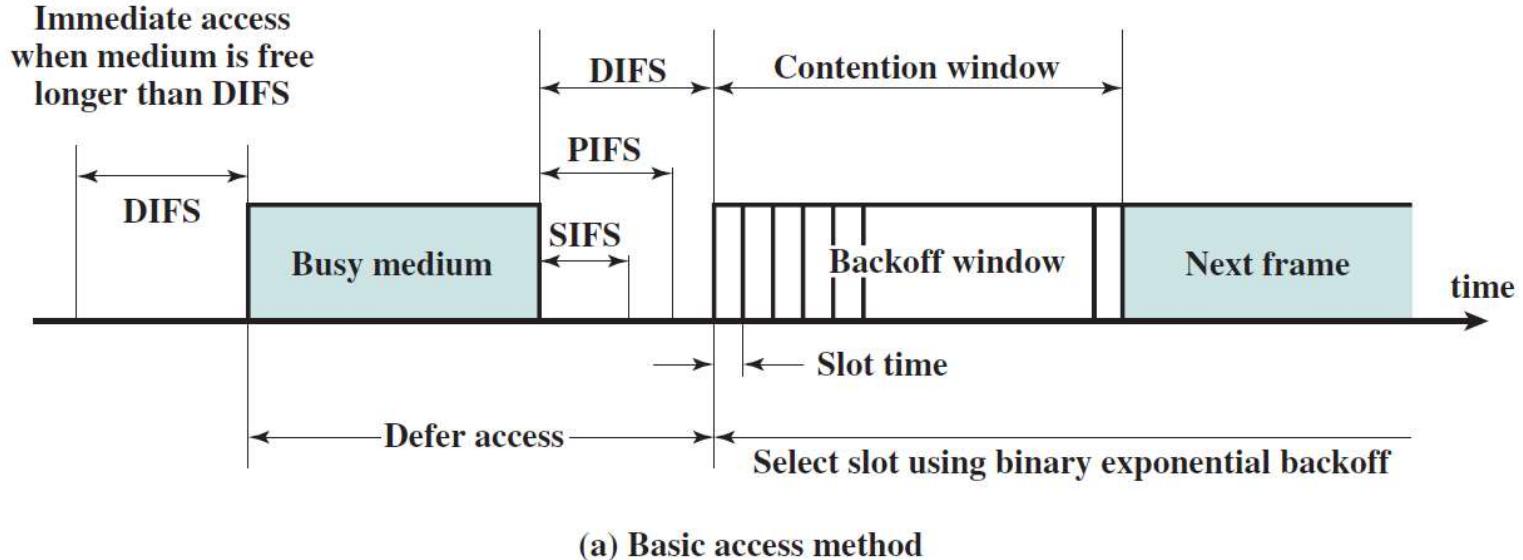
- DIFS (Distributed coordination function IFS) – minimum delay for asynchronous ordinary frames contending for access

General rules for CSMA access (802.11 MAC protocol):

- a station senses medium; if medium idle, waits for IFS seconds to see it remains idle ; then transmits

- If medium busy, waits till that transmission ends

- Current transmission over, delays own transmission with IFS; if medium idle uses a backoff algorithm waiting another period; if medium still idle, may transmit



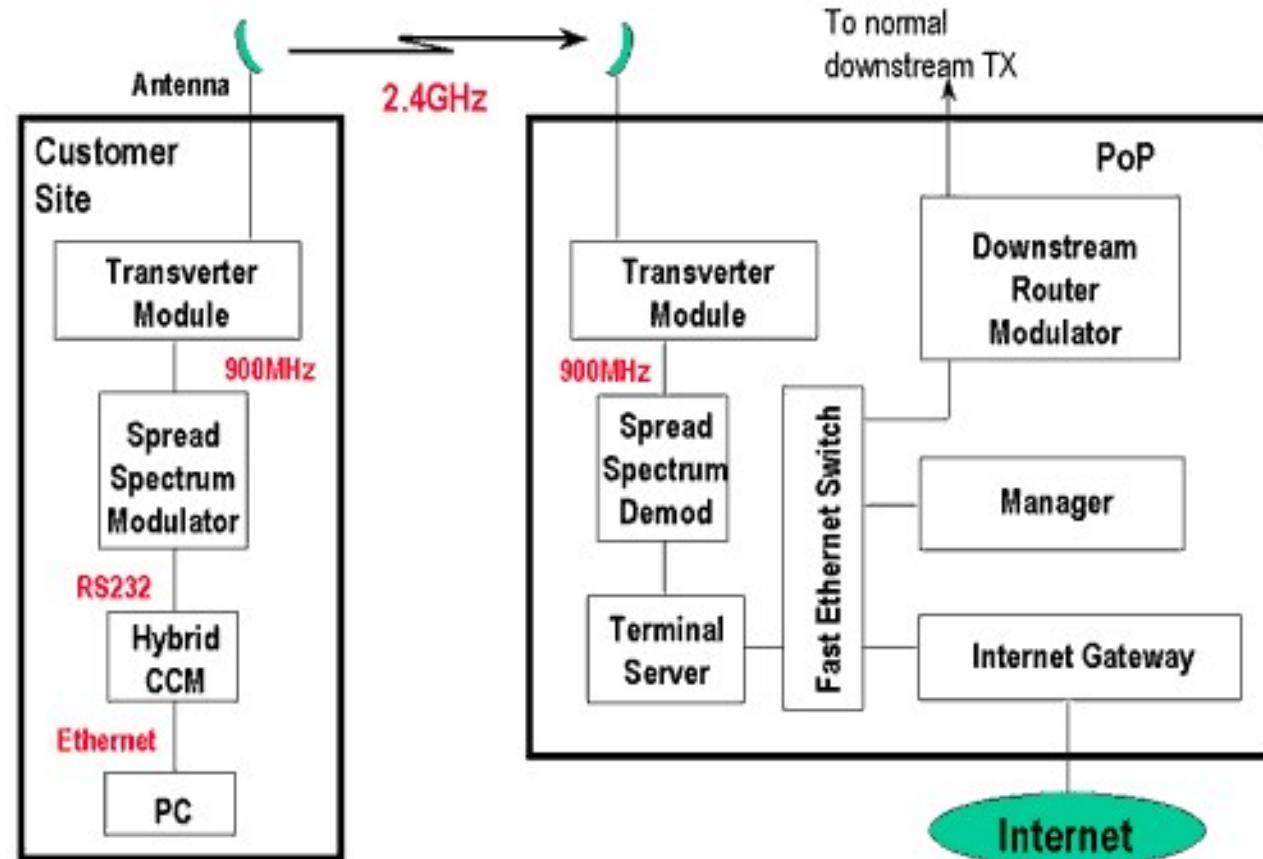
802.11 MAC Timing

Wireless modems

Many kinds of wireless modems:

- RF modem for a wireless network (use of ISM bands)
- cellular modem for cellular communications, attached to the phone

Example: use the ISM Band for Wireless Return 900 MHz/2.4 GHz:

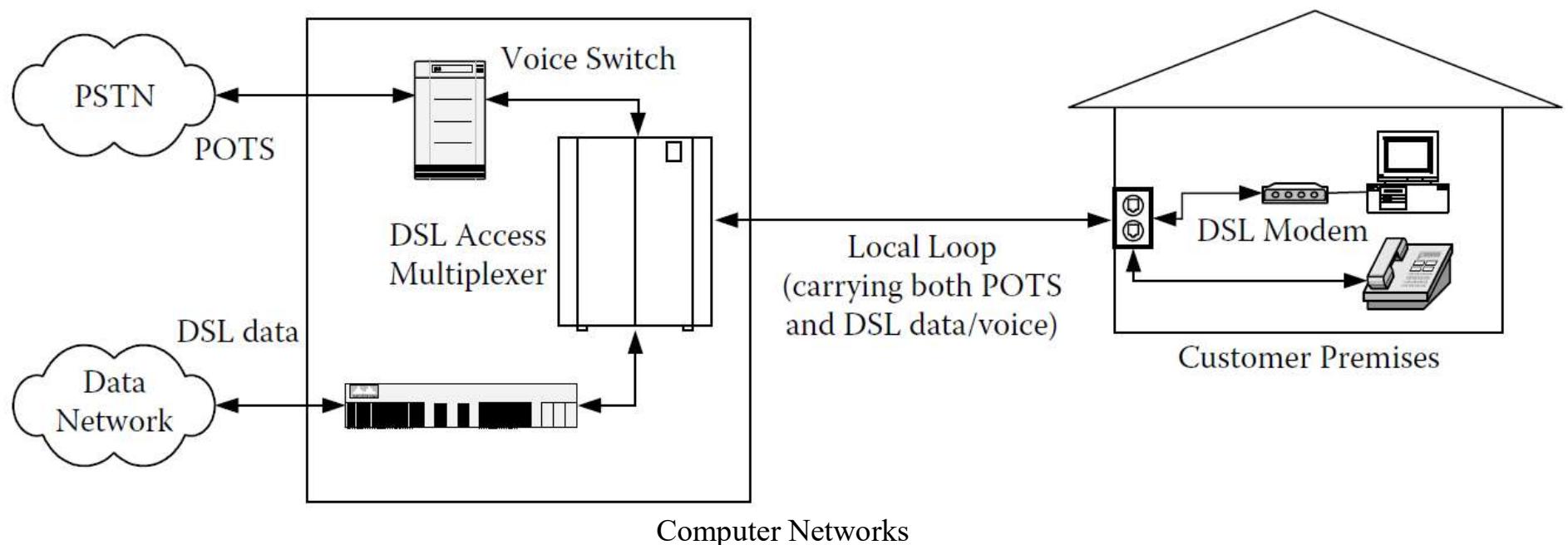


DSL (Digital Subscriber Line)

Link between subscriber and network (local loop); tens of millions installed;
Reinstall?

⇒ need for exploiting the existing base of TP wired structure; initially designed for voice-grade analog transmissions with 4kHz bandwidth, TP may carry data using signals over a spectrum of more than 1MHz => use of modems for digital high rate data transmissions, using currently installed twisted pair cable.

- DSL refers to the analog local loop between each customer premises and its local central office, and a DSL modem is required at each end of the loop



ADSL (Asymmetric Digital Subscriber Line)

ADSL initially designed for video-on-demand, now appropriate for high-speed Internet access.

Asymmetric because, from the user point, there is greater capacity downstream (from service provider to customer) than upstream.

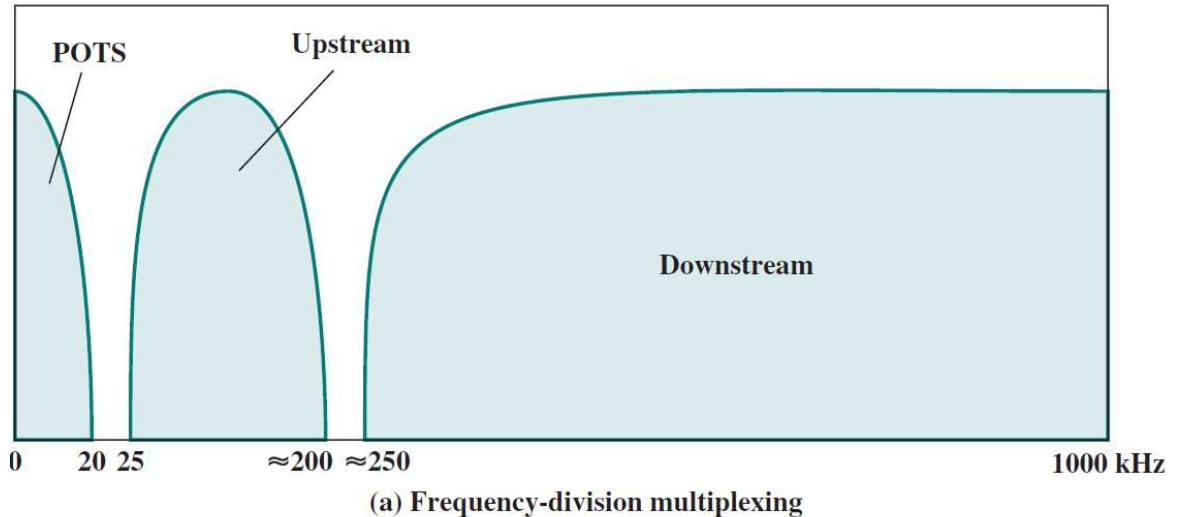
ADSL uses FDM for managing the 1MHz bandwidth:

- Lowest 25kHz for voice (Plain Old Telephone Service): 0 to 4kHz for voice, rest for guard, avoiding interference with other channels
- Use echo cancellation or FDM to give (to allocate) two bands: one for upstream , one for downstream
- Use FDM within each of two bands.

Supports loop length in the range of 5.5km.

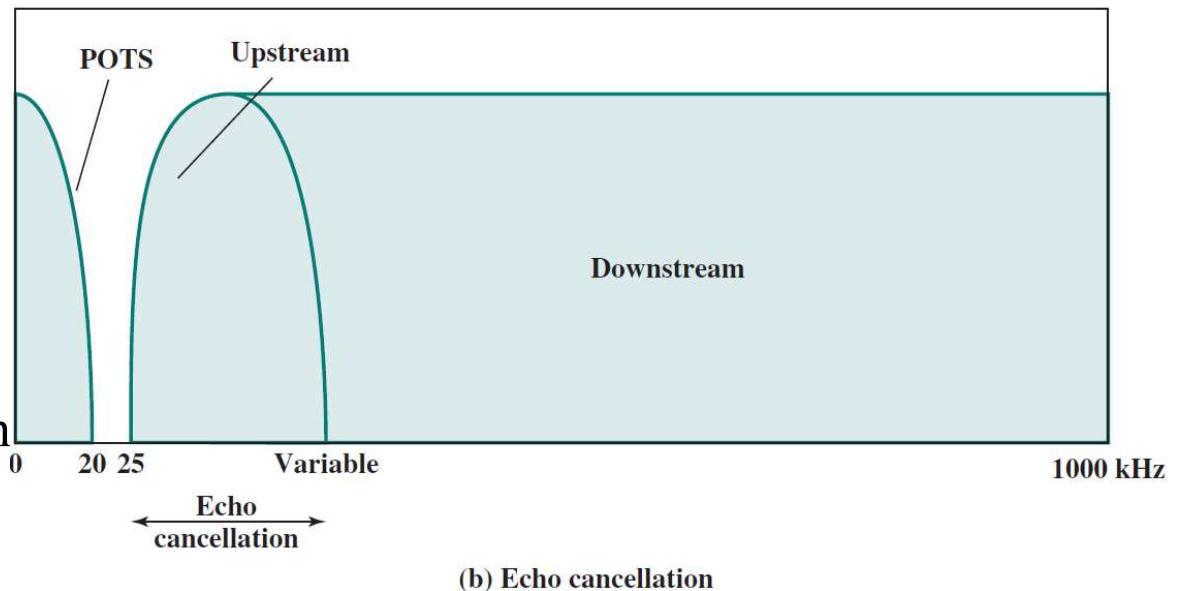
Echo Cancellation

Signal processing technique, allowing digital transmissions in both directions on a single line simultaneously. The transmitter must subtract the echo of its own transmission from the incoming signal, to recover the signal sent by the other side.



Advantages:

- more flexibility for upstream bandwidth changes, simply extending the area of overlap
- downstream bandwidth in the good part of the spectrum (not so many HFs) => a lower attenuation



DMT (Discrete Multitone)

DMT modem allows multiple carrier signals at different frequencies;

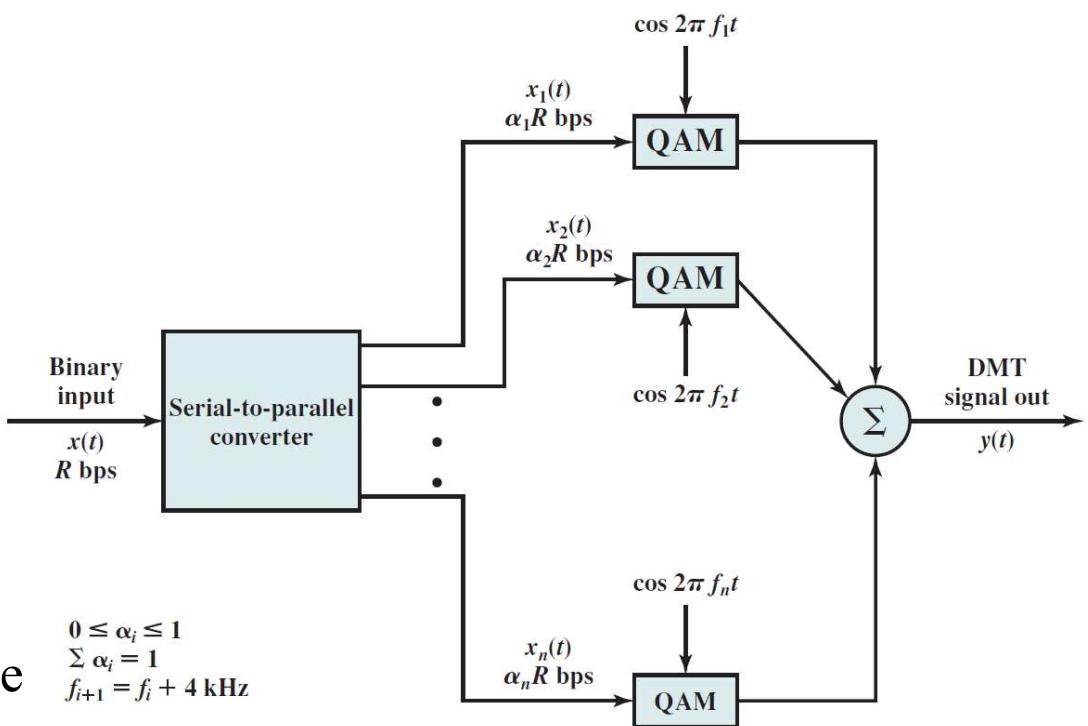
- upstream and downstream bandwidths are split in a number of 4kHz sub-channels, transmitting a number of bits on each channel.

Initially modem send test signal on each subchannel, and then use those subchannels with better signal to noise ratio.

If used 256 downstream subchannels at 4kHz, carrying data at 60kbps, will result a data rate of 15.36Mbps. Transmission impairments bring this down to 1.5Mbps to 9Mbps.

Use of **QAM (Quadrature Amplitude Modulation)** – analog signaling technique, a combination of AM and PM. May assign different number of bits/transmitted signal.

Sample example: data string is split in two sub-strings. One sub-string modulates the carrier, the other modulates the carrier shifted with 90° . The composed QAM signal is the sum: $s(t) = d_1(t)\cos 2\pi ft + d_2(t)\sin 2\pi ft$. \Rightarrow signal has 4 states, for coding 2 bits.



xDSL – recent schemes for high-data speed transmissions on ADSL

High data rate DSL

Single line DSL

Very high data rate DSL

	ADSL	HDSL	SDSL	VDSL
Data Rate	1.5–9 Mbps downstream 16–640 kbps upstream	1.544 or 2.048 Mbps	1.544 or 2.048 Mbps	13–52 Mbps downstream 1.5–2.3 Mbps upstream
Mode	Asymmetric	Symmetric	Symmetric	Asymmetric
Copper Pairs	1	2	1	1
Range (24-Gauge UTP)	3.7–5.5 km	3.7 km	3.0 km	1.4 km
Signaling	Analog	Digital	Digital	Analog
Line Code	CAP/DMT	2B1Q	2B1Q	DMT
Frequency	1–5 MHz	196 kHz	196 kHz	≥ 10 MHz
Bits/Cycle	Varies	4	4	Varies

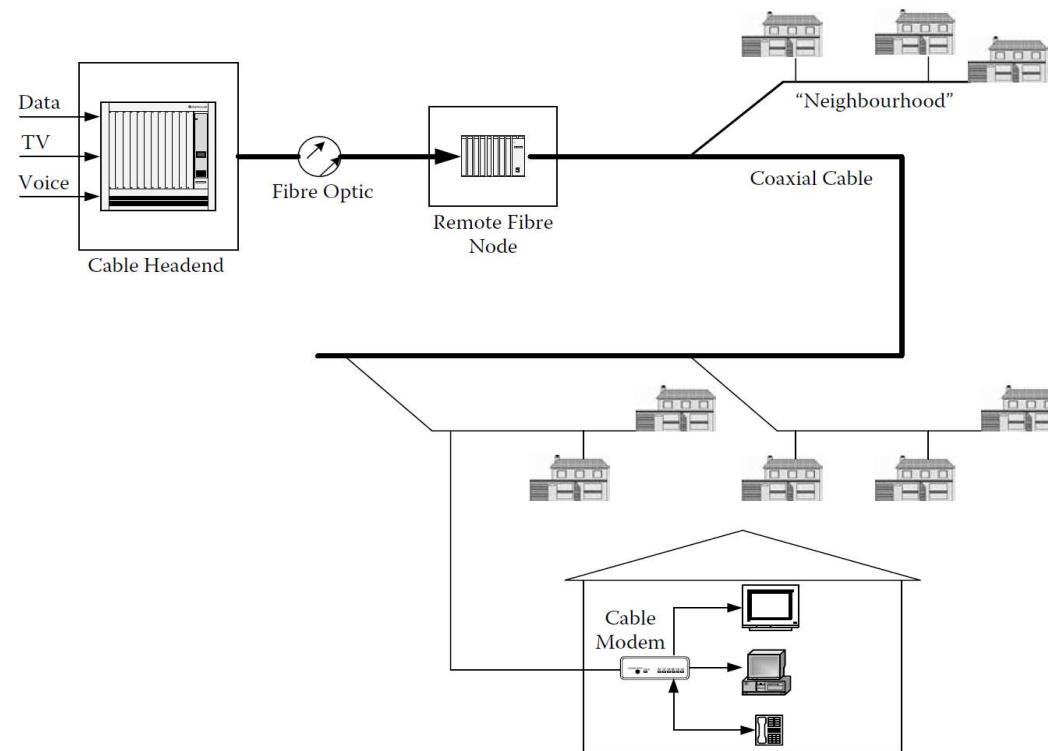
Alternative Broadband Access Technologies

Fiber-to-the-home (FTTH)

- common solution: using passive optical network (PON)
- a single transceiver in the CO serving multiple customers
- splitters and couplers to distribute the service among the different subscribers

Cable

- hybrid fiber-coax (HFC)
- fiber-optic cable carrying signals between the cable headend and fiber nodes in the network, from which existing coaxial cable is used to cover the “last mile” to the subscribers’ premises.



Alternative Broadband Access Technologies

Wireless

- wireless local loop with the advantage that it doesn't need the installation of a transmission medium
- higher frequencies systems: 20 to 40 GHz, sometimes requiring line-of-sight (LOS) availability
- Lower frequency systems: 2,4GHz– 5GHz, with non-LOS transmission

BPL (*Broadband over Power Line*)

- use of the electric power supply network for the transmission of broadband data

Example: *IEEE 1901-2010 (IEEE Standard for Broadband over Power Line Networks: Medium Access Control and Physical Layer Specifications)*

- high-speed (>100 Mbps at the physical layer) communication
- transmission frequencies below 100 MHz
- BPL devices used for the first-mile/last-mile connection (<1500 m to the premise) and BPL devices used in buildings for local area networks (LANs) and other data distribution (<100 m between devices).

Internet Protocol (IP)

Part of TCP/IP, used by the Internet

Specifies interface with higher layer, e.g. TCP

Specifies protocol format and mechanisms

IP Services

Primitives

Functions to be performed

Form of primitive implementation dependent, e.g. subroutine call

Send

Request transmission of data unit

Deliver

Notify user of arrival of data unit

Parameters

Used to pass data and control info

Source address

Destination address

Protocol

Recipient, e.g. TCP

Type of Service

Specify treatment of data unit during transmission through networks

Identification of IP packet

Source, destination address and user protocol

Uniquely identifies PDU

Needed for re-assembly and error reporting

Send only

Don't fragment indicator

Can IP fragment data

If not, may not be possible to deliver

Send only

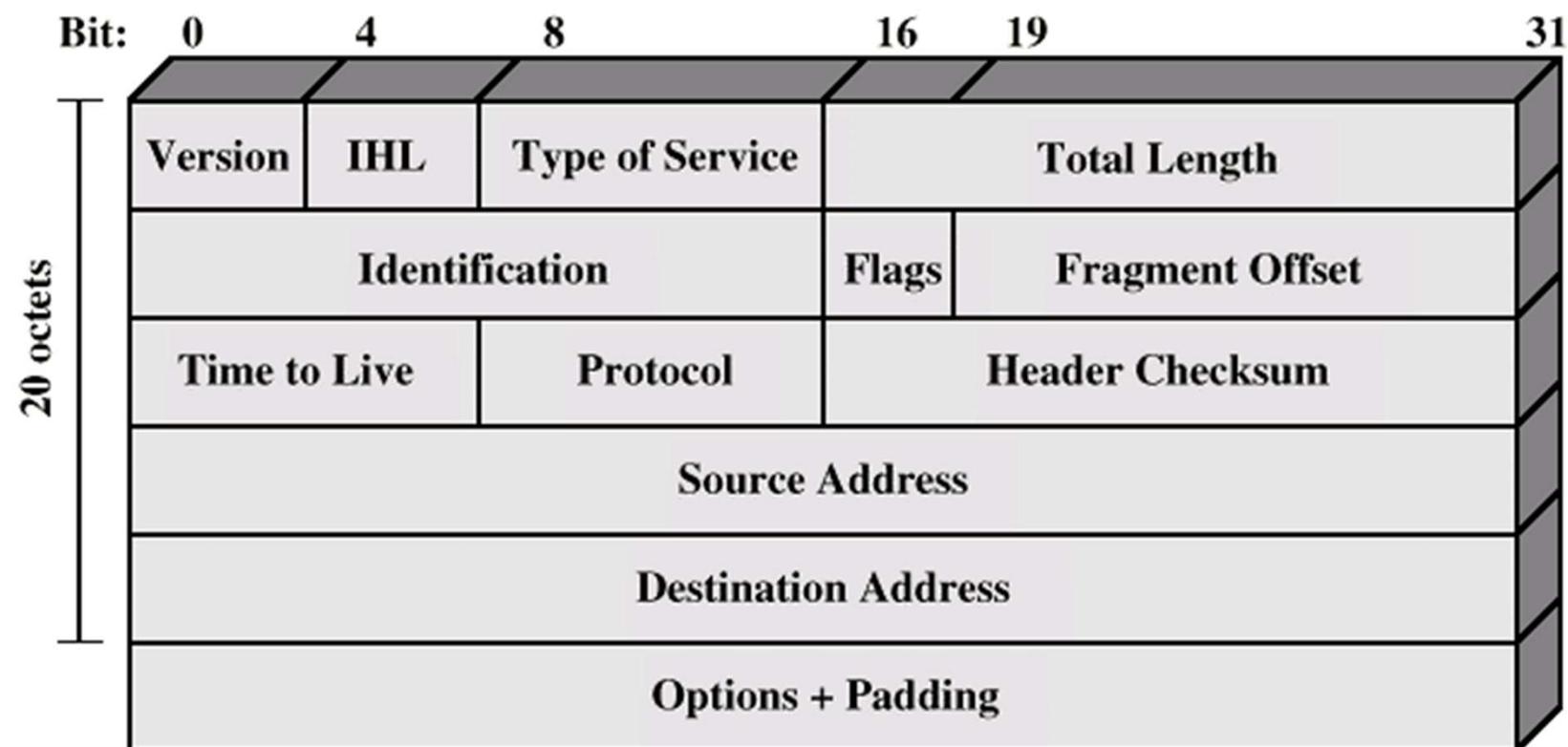
Time to live

Send only

Data length

Option data

User data



IP packet structure

Header Fields

Version

Currently 4

IP v6 - see later

Internet header length

In 32 bit words

Including options

Type of service

Total length

Of datagram, in octets

Identification

Sequence number

Used with addresses and user protocol to identify datagram uniquely

Flags

More bit

5

Don't fragment

Fragmentation offset

Time to live

Protocol

Next higher layer to receive data field at destination

Header checksum

Reverified and recomputed at each router

16 bit ones complement sum of all 16 bit words in header

Set to zero during calculation

Source address

Destination address

Options

Padding

To fill to multiple of 32 bits long

Data Field

Carries user data from next layer up

Integer multiple of 8 bits long (octet)

Max length of datagram (header plus data) 65,535 octets

IP Addresses

32 bit global internet address

Network part and host part





Class A

Start with binary 0

All 0 reserved



01111111 (127) reserved for loopback

Range 1.x.x.x to 126.x.x.x



All allocated



Class B

Start 10

Range 128.x.x.x to 191.x.x.x

Second Octet also included in network address

$2^{14} = 16,384$ class B addresses

All allocated



Class C

Start 110

Range 192.x.x.x to 223.x.x.x

Second and third octet also part of network address

$2^{21} = 2,097,152$ addresses

Nearly all allocated



Class D

Contain multicast addresses for group users

first decimal field is between 224 and 239

Class E

Reserved for research and future developments

First decimal field between 240 and 255

Class	1 st Octet Decimal Range	1 st Octet High Order Bits	Network/Host ID (N=Network, H=Host)	Default Subnet Mask	
A	1 – 126*	0	N.H.H.H	255.0.0.0	/8
B	128 – 191	10	N.N.H.H	255.255.0.0	/16
C	192 – 223	110	N.N.N.H	255.255.255.0	/24
D	224 – 239	1110	Reserved for Multicasting		
E	240 – 254	1111	Experimental; used for research		

Note: Class A addresses 127.0.0.0 to 127.255.255.255 cannot be used and is reserved for loopback and diagnostic functions.

- *Private IP addresses*

Class A: 10.0.0.0 - 10.255.255.255 /8

Class B: 172.16.0.0 - 172.31.255.255 /16

Class C: 192.168.0.0 - 192.168.255.255 /24

	172	25	114	250	AND
IP Address (B class)	10101100	00011001	01110010	11111010	0 0 0
Network Mask	11111111	11111111	00000000	00000000	0 1 0
	255	255	0	0	1 0 0
Network Address	10101100	00011001	00000000	00000000	AND
	172	25	0	0	1 1 1
Broadcast Address	10101100	00011001	11111111	11111111	
	172	25	255	255	

- Network address: all host bits = 0
- Network broadcast address: all host bits = 1
- Total number of host bits: $2^{16} = 65,536$
- Number of hosts: $2^{16} - 2 = 65,536 - 2 = 65,534$

	Binary Representation	Dotted Decimal
IP address	11000000.11100100.00010001.00111001	192.228.17.57
Subnet mask	11111111.11111111.11111111.11100000	255.255.255.224
Bitwise AND of address and mask (resultant network/subnet number)	11000000.11100100.00010001.00100000	192.228.17.32
Subnet number	11000000.11100100.00010001.001	1
Host number	00000000.00000000.00000000.00011001	25

(b) Default subnet masks

	Binary Representation	Dotted Decimal
Class A default mask	11111111.00000000.00000000.00000000	255.0.0.0
Example Class A mask	11111111.11000000.00000000.00000000	255.192.0.0
Class B default mask	11111111.11111111.00000000.00000000	255.255.0.0
Example Class B mask	11111111.11111111.11111000.00000000	255.255.248.0
Class C default mask	11111111.11111111.11111111.00000000	255.255.255.0
Example Class C mask	11111111.11111111.11111111.11111100	255.255.255.252

Subnets and Subnet Masks

Allow arbitrary complexity of internetworked LANs within organization

Insulate overall internet from growth of network numbers and routing complexity

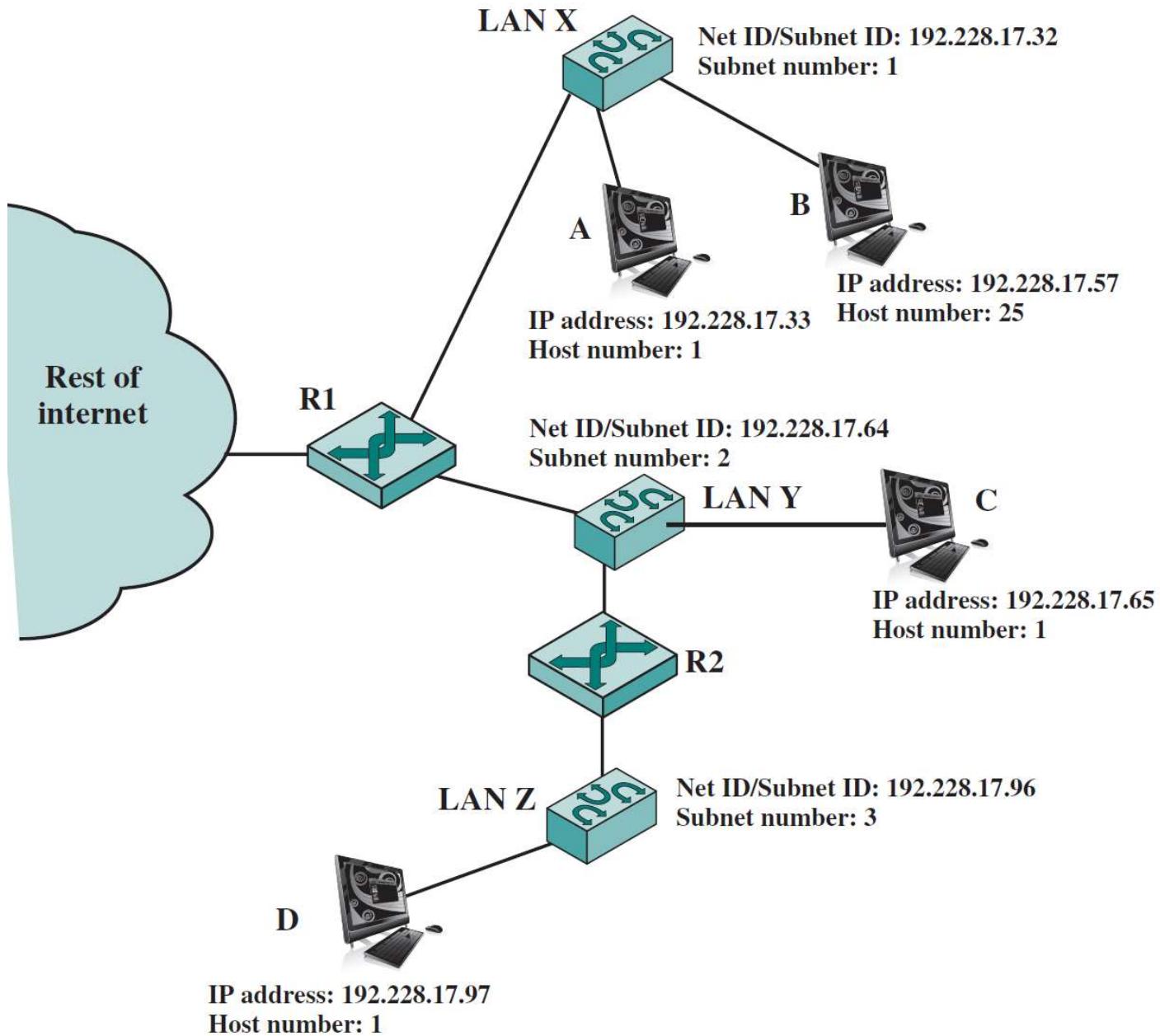
Site looks to rest of internet like single network

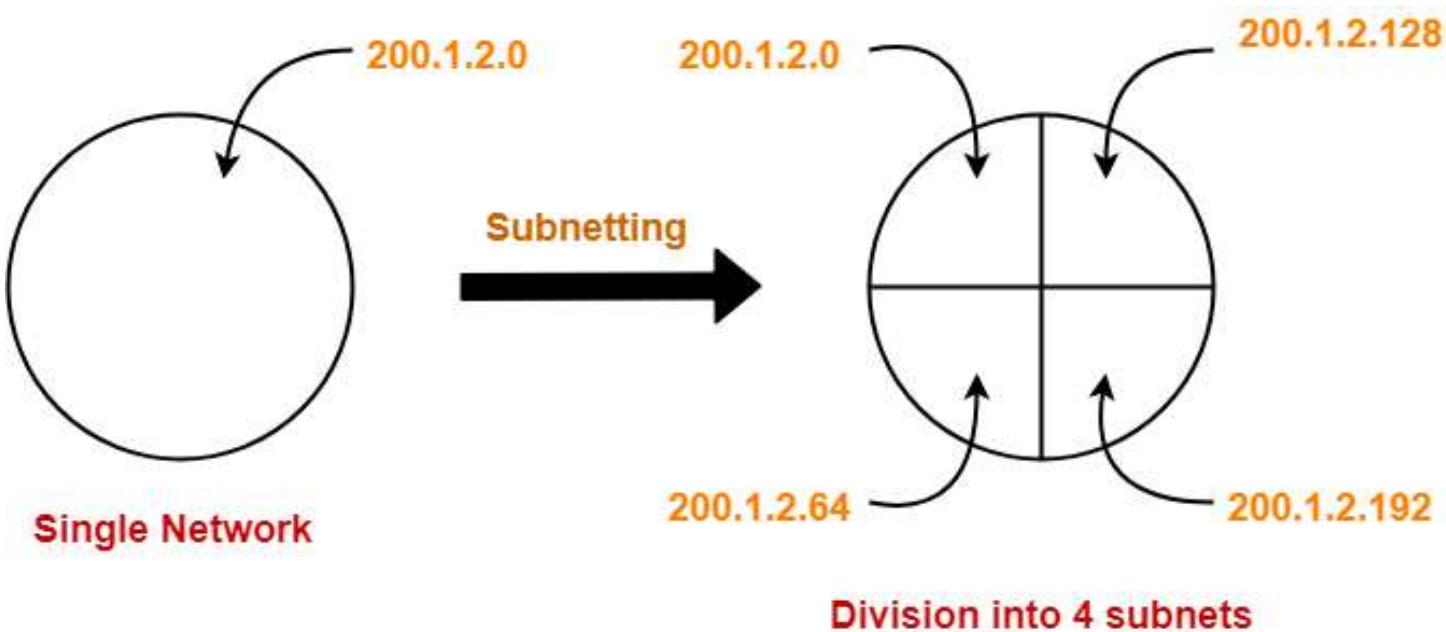
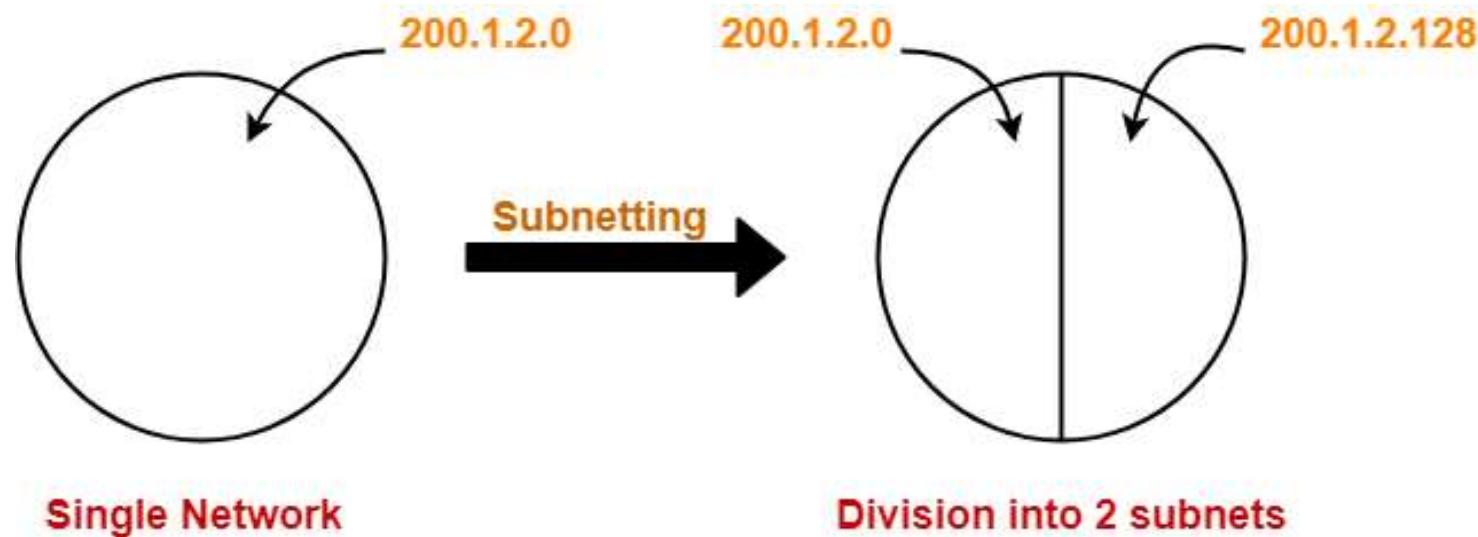
Each LAN assigned subnet number

Host portion of address partitioned into subnet number and host number

Local routers route within subnetted network

Subnet mask indicates which bits are subnet number (1s) and which are host number (0s)

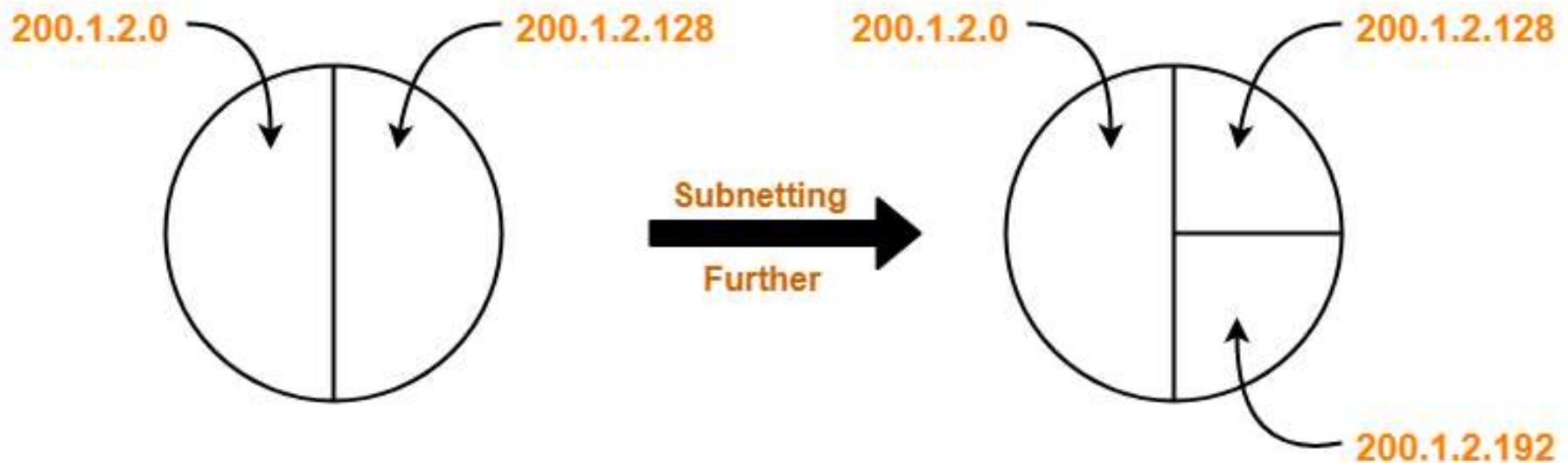
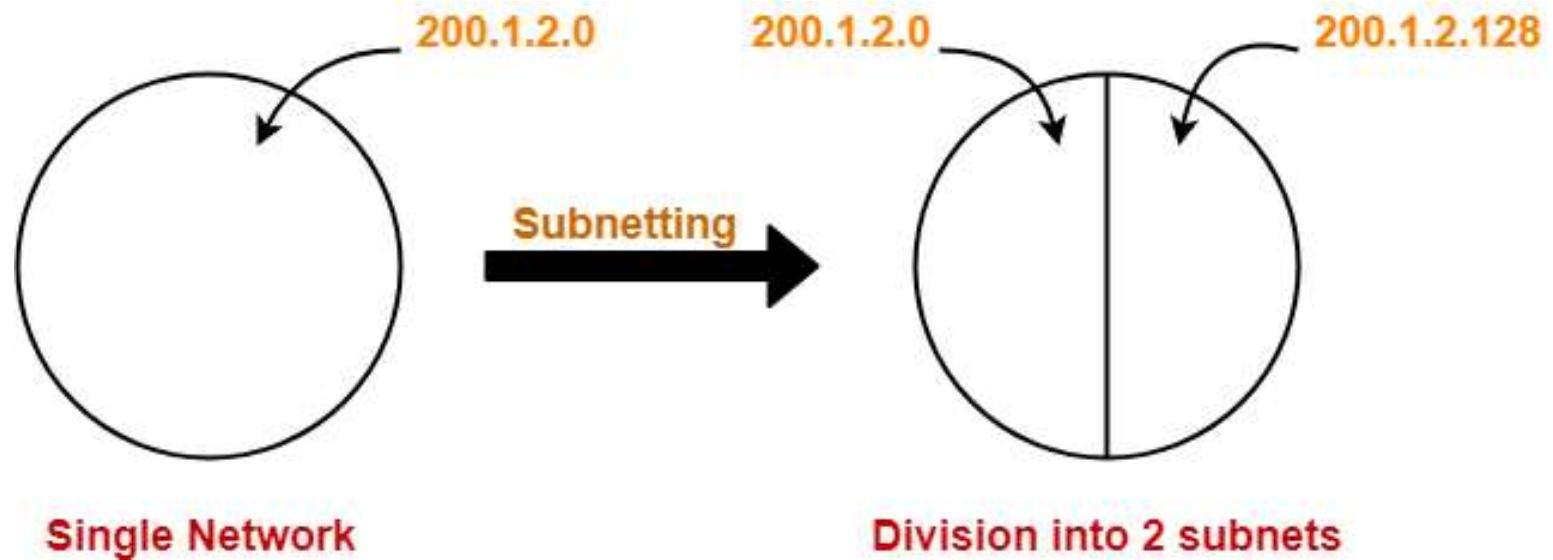




- Creating subnets:
 - borrow bits from the host ID
 - create a new Network Mask to show the new structure of the IPv4

	network ID	subnetwork ID	host ID	
	172	25	114	250
IP Address (B class)	10101100	00011001	01110010	11 111010 AND 0 0 0
Network Mask	255	255	0	0 0 /16
Subnet Mask	<u>255</u>	<u>255</u>	<u>255</u>	<u>192</u> /26 1 0 0
	11111111	11111111	11111111	11 0000000 AND 1 1 1
Subnet Address	10101100	00011001	01110010	11 0000000
	172	25	114	192
Subnet Broadcast	10101100	00011001	01110010	11 111111 172
	172	25	114	255

Total number of host bits: 2^6	
Number of hosts: $2^6 - 2 = 64 - 2 = 62$	First host IP on subnet: 172.25.114.193
Total number of subnet bits: 2^{10}	Last host IP on subnet: 172.25.114.254
Number of subnets: $2^{10} = 1024$	



ICMP

Need for appending to IP (used only for data transfer) of some **control protocols**,
e.g. ICMP, ARP, RARP, BOOTP

Internet Control Message Protocol (ICMP) provides error-reporting mechanisms

RFC 792

Transfer of (control) messages from routers and hosts, to other hosts

Feedback about problems

e.g. time to live expired

ICMP packet encapsulated in IP datagram

Not a very reliable protocol, because (see next slide):

IP provides a *best-effort delivery* (not a secure one)

Internet layer can detect a small variety of errors:

- Checksum (header only!)
- TTL expires
- No route to destination network
- Can't deliver to destination host (e.g., no ARP reply)

Internet layer discards datagrams with problems

Some - e.g., checksum error - can't trigger error messages (ICMP message)

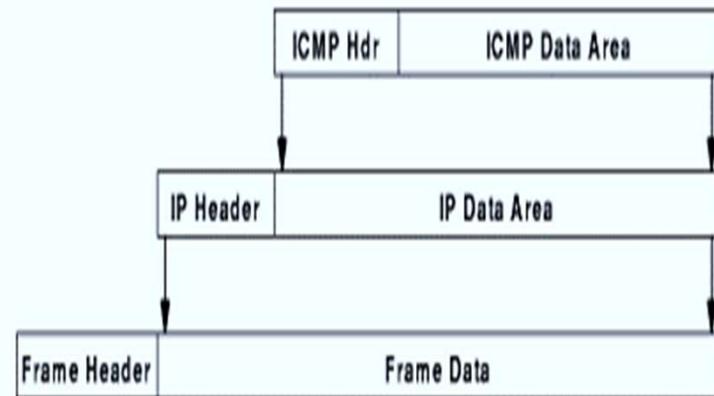
Some errors can be reported

Remember:

ICMP encapsulated in IP (see drawing)

ICMP messages sent in response to incoming
datagrams with problems

ICMP message **not** sent for ICMP message



Message type	Description
Destination unreachable	Packet could not be delivered
Time exceeded	Time to live field hit 0
Parameter problem	Invalid header field
Source quench	Choke packet
Redirect	Teach a router about geography
Echo request	Ask a machine if it is alive
Echo reply	Yes, I am alive
Timestamp request	Same as Echo request, but with timestamp
Timestamp reply	Same as Echo reply, but with timestamp

The principal ICMP message types.

ICMP and reachability

An internet host, A , is *reachable* from another host B , if datagrams can be delivered from A to B

TCP/IP *ping* program tests reachability - sends datagram from B to A , that A *echoes* back to B

Uses ICMP *echo request* and *echo reply* messages, e.g. Internet layer includes code to reply to incoming ICMP *echo request* messages

ICMP and internet routes

List of all routers on path from A to B is called the *route* from A to B

TCP/IP *traceroute* program uses UDP to non-existent port and TTL field to find route via *expanding ring* search

traceroute must accommodate varying network delays & dynamically changing routes

Sends ICMP echo messages with increasing TTL

- Router that decrements TTL to 0, sends ICMP *time exceeded* message, with router's address as source address
- First, with TTL 1, gets to first router, which discards and sends time exceeded message
- Next, with TTL 1, gets through first router to second router
- Continue until message from destination received

ICMP and path MTU (smallest accepted probe) discovery

Fragmentation should be avoided

How can source configure outgoing datagrams to avoid fragmentation?

Source determines *path MTU* - smallest network MTU (Minimum Transmission Unit) on path from source to destination

Source *probes* path using IP datagrams with *don't fragment* flag

Router responds with ICMP *fragmentation required* message

Source sends smaller probes until destination reached

ICMP and router discovery

Router can fail, causing "black-hole" or isolating host from internet

- ICMP *router discovery* used to find new route
- Host can broadcast request for router announcements to auto-configure default route
- Host can broadcast request if router fails
- Router can broadcast advertisement of existence when first connected

ICMP redirect

Default route may cause *extra hop*

- Router that forwards datagram on same interface sends ICMP *redirect*
- Host installs new route with correct router as next hop

ICMP packet format

0	8	16	31
Type	Code	Checksum	
Unused			
IP Header + 64 bits of original datagram			

(a) Destination unreachable; time exceeded; source quench

0	8	16	31
Type	Code	Checksum	
Identifier			
Sequence number			
Originate timestamp			

(e) Timestamp

0	8	16	31
Type	Code	Checksum	
Pointer	Unused		
IP Header + 64 bits of original datagram			

(b) Parameter problem

0	8	16	31
Type	Code	Checksum	
Identifier			
Sequence number			
Originate timestamp			
Receive timestamp			
Transmit timestamp			

(f) Timestamp reply

0	8	16	31
Type	Code	Checksum	
Gateway Internet address			
IP Header + 64 bits of original datagram			

(c) Redirect

0	8	16	31
Type	Code	Checksum	
Identifier			
Sequence number			
Address mask			

(g) Address mask request

0	8	16	31
Type	Code	Checksum	
Identifier			
Sequence number			
Optional data			

(d) Echo, echo reply

0	8	16	31
Type	Code	Checksum	
Identifier			
Sequence number			
Address mask			

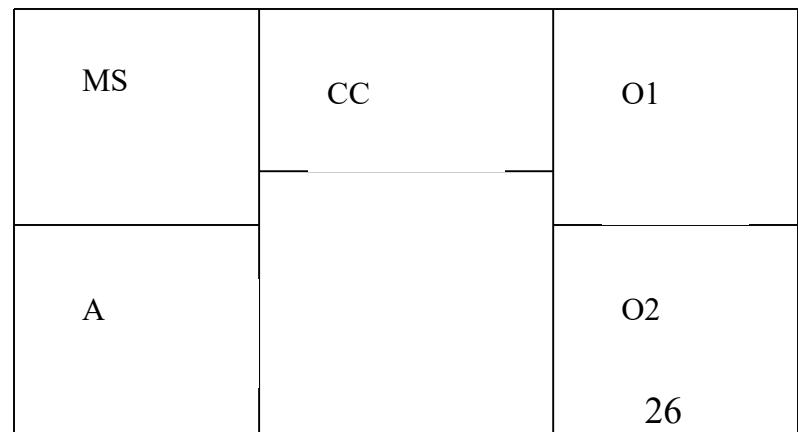
(h) Address mask reply

Proposed Problem

A company owns a building with one floor, having the following structure: **CC**-Communication Center, **O1**, **O2**-offices, **MS**-management, **A**- administration (see drawing). In room **MS** there are 2 computers, in room **A** are 5 computers, and the rooms **O1**, **O2** have 10 computers each.

The company gets for use the addresses 198.188.77.64 with the netmask 255.255.255.224.

Establish the address configuration of each subnetwork and computer located at this floor, knowing that in the both rooms **O** will be **one** subnetwork, the rooms **MS** and **A** belong to **one** other subnetwork , and **another** subnet will be setup for future applications in **CC**.



A *class C* network will be implemented.

Total number of *required subnetworks* will be 3.

Bitwise AND of address and mask values (giving the resultant network/subnet number) will be:

198.188.77.64

So the first subnet will have address: 198.188.77.64 and may serve rooms O1 and O2, with 20 stations together, filling address scheme from 198.188.77.65 to 198.188.77.84

The second subnet will have address: 198.188.77.128 and may serve rooms A+MS, with 7 computers, with addresses from 198.188.77.129 to 198.188.77.135

The third subnet with address 198.188.77.192 may serve the rest of the rooms.

Introduction to IPv6

IP v 1-3: defined and replaced

IP v4 - current version; 20+ years old

IP v5 - streams protocol

IP v6 - replacement for IP v4

During developments it was called IPng - Next Generation

Why Change IP?

32 bit Address space exhaustion

32 bit address space = millions of networks (could be enough?), BUT:

Two level addressing (network and host) wastes space: one network address used, even if not all possible associated hosts connected to Internet, or network connected to Internet

Growth of networks and the Internet (LANs, wireless LANs ...)

2^{14} Class B network addresses already almost exhausted; class C networks too low size for most companies

Extended use of TCP/IP (new applications => requests for new IP addresses)

Requirements for new types of services

Different applications have different requirements for delivery, reliability and speed

Current IP has *type of service* that's not often implemented

Multicast transmissions

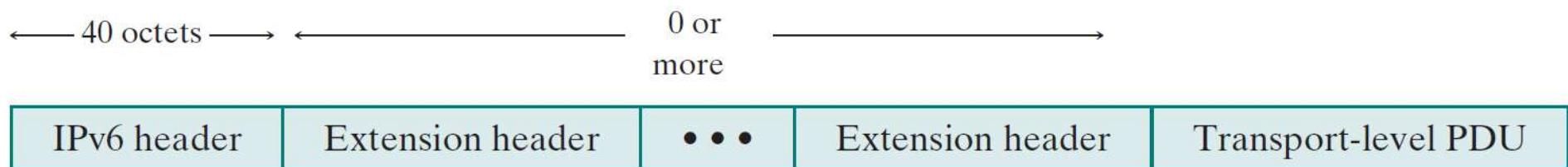
IPv6 RFCs

1752 - Recommendations for the IP Next Generation Protocol

2460 - Overall specification

4291 - addressing structure

..... Others



Enhancements over IPv4

Expanded address space: 128 bit

Improved option mechanism

Separate optional headers between IPv6 header and Transport layer header

Most are not examined by intermediate routers

Improved speed and simplified router processing of IPv6 datagrams

Easier to extend options

Address auto-configuration

Dynamic assignment of addresses

Increased address flexibility & scalability

Anycast address : packet delivered to a set of hosts

Support for resource allocation

Allow packet labeling (those belonging to a traffic flow)

General considerations

Not generally compatible with IPv4

But compatible with higher-level protocols

Longer addresses: expanded address space, 128 bit

Address auto-configuration; dynamic assignment of addresses

Traffic Priorities: 0 – 7 for variable flow rate, 8 – 15 for real time traffic

Improved option mechanism

Separate optional headers between IPv6 header and transport layer header

Most are not examined by intermediate routers

Improved speed and simplified router processing

Easier to extend options

Increased addressing flexibility

Anycast - delivered to one of a set of nodes

Improved scalability of multicast addresses

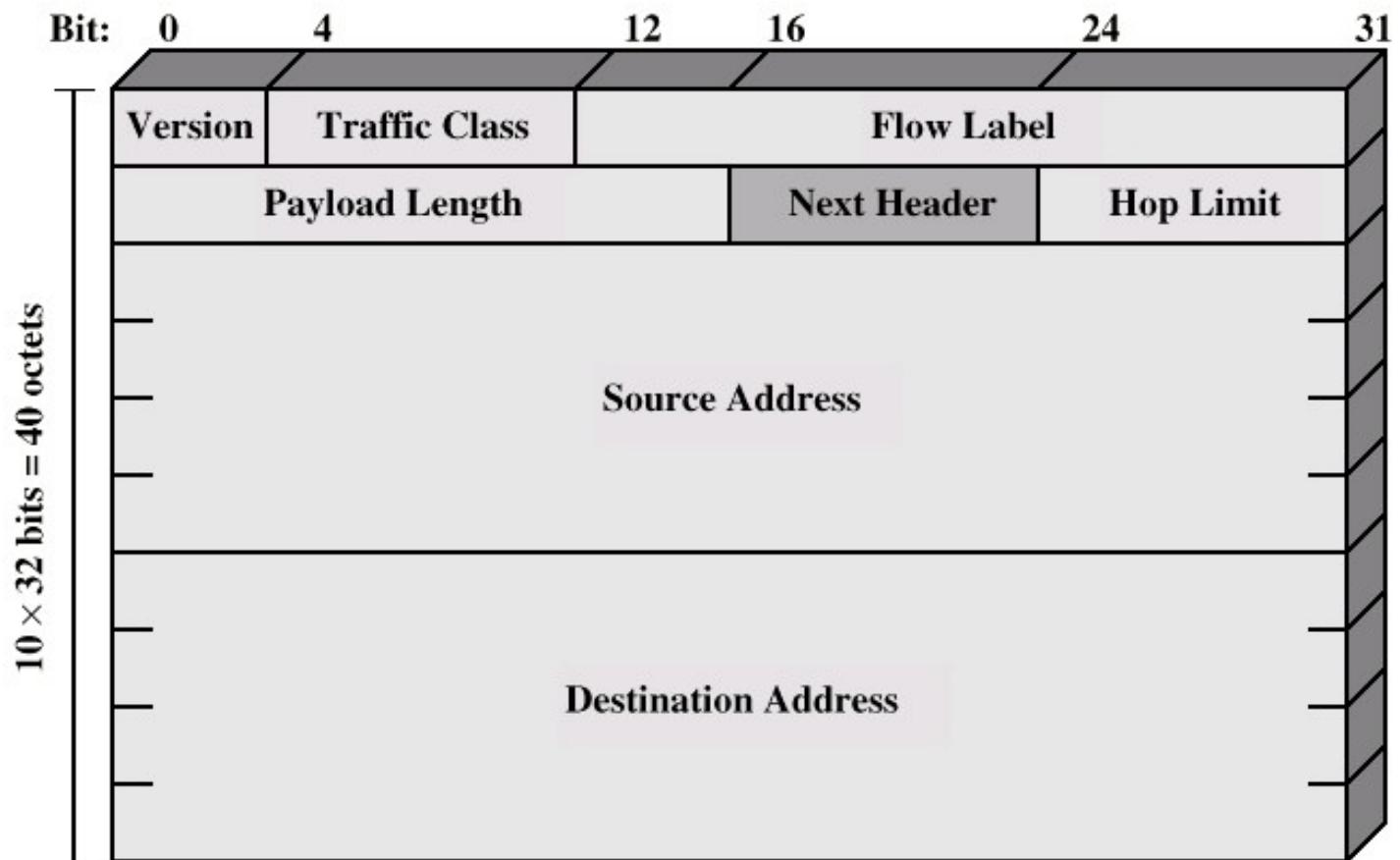
Support for resource allocation

Replaces *type of service* IPv4 field (most unused)

Labeling of packets to particular traffic flow

Allows special handling, e.g. real time video

IPv6 Header General format



IPv6 base header format

Contains less information than IPv4 header; header format - entirely different

Next Header field points to first extension header

Flow Label field used to associate datagrams belonging to a *flow* or communication between two applications (support for audio-video connections, with appropriate QoS)

Traffic class

Classes or priorities of current packet

Still under development, see RFC 2460

Advantages of the header structure

Efficiency - header only as large as necessary

Flexibility & extension - can add new headers for new features

Incremental development - can add processing for new features to testbed; other routers will skip those headers

Extension Headers

Additional information stored in optional extension headers, followed by data

Hop-by-Hop Options

Require processing at each router

Routing

Similar to IPv4 source routing

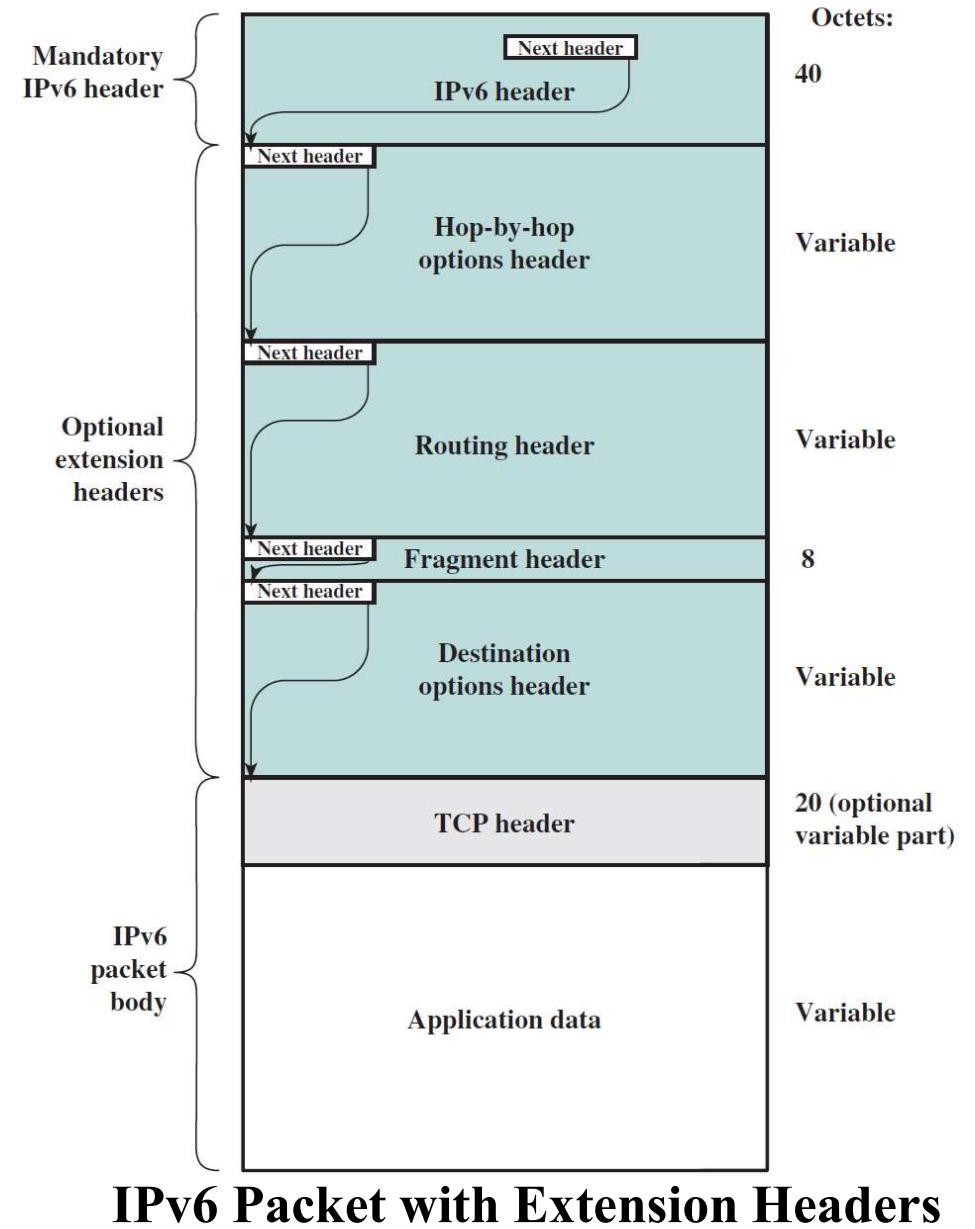
Fragment

Authentication

Encapsulating security payload

Destination options

For destination node



IP v6 Header Fields (Basic Header)

Version: 6

Traffic Class (DS/ECN)

Classes or priorities of packets

Used by originating nodes and/or forwarding routers for differentiated services and congestion functions

Flow Label

Used by routers to label packets requesting special handling within the network

Payload length

Includes all extension headers plus user (application) data

Next Header

Identifies type of header immediate following

May have another extension header or next layer up protocol header

Source Address & Destination address (128 bits)

IPv6 Addresses

128 bits long

Assigned to node's interface, not to node

One single interface may have multiple unique unicast addresses

Three types of address:

Unicast

Single interface; packet delivered there

Anycast

Set of interfaces (typically belong to different nodes)

Delivered to any **one** interface, usually the “nearest”

Multicast

Packets delivered to all interfaces identified

Prefix (binary)	Usage	Fraction
0000 0000	Reserved (including IPv4)	1/256
0000 0001	Unassigned	1/256
0000 001	OSI NSAP addresses	1/128
0000 010	Novell NetWare IPX addresses	1/128
0000 011	Unassigned	1/128
0000 1	Unassigned	1/32
0001	Unassigned	1/16
001	Unassigned	1/8
010	Provider-based addresses	1/8
011	Unassigned	1/8
100	Geographic-based addresses	1/8
101	Unassigned	1/8
110	Unassigned	1/8
1110	Unassigned	1/16
1111 0	Unassigned	1/32
1111 10	Unassigned	1/64
1111 110	Unassigned	1/128
1111 1110 0	Unassigned	1/512
1111 1110 10	Link local use addresses	1/1024
1111 1110 11	Site local use addresses	1/1024
1111 1111	Multicast	1/256

IPv6 addresses

Address Type	Description
Unicast	<p>One to One (Global, Link local, Site local)</p> <ul style="list-style-type: none"> + An address destined for a single interface.
Multicast	<p>One to Many</p> <ul style="list-style-type: none"> + An address for a set of interfaces + Delivered to a group of interfaces identified by that address. + Replaces IPv4 “broadcast”
Anycast	<p>One to Nearest (Allocated from Unicast)</p> <ul style="list-style-type: none"> + Delivered to the closest interface as determined by the IGP

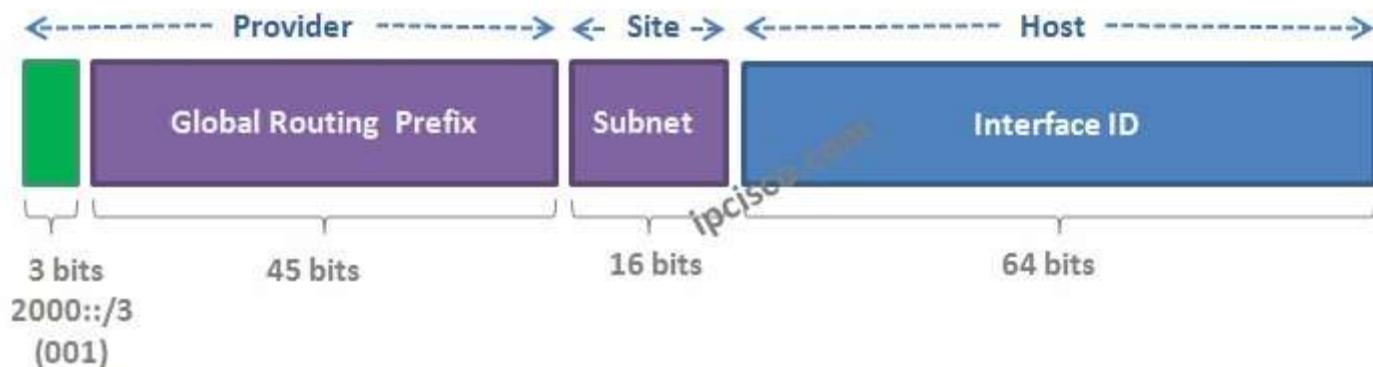
PREFIX

Interface ID

IPv6 Address Space Usage

Address Type	Binary Prefix	IPv6 Notation	Fraction of Address Space
Embedded IPv4 address	00...1111 1111 1111 1111 (96 bits)	::FFFF/96	2^{-96}
Loopback	00...1 (128 bits)	::1/128	2^{-128}
Link-local unicast	1111 1110 10	FE80::/10	1/1024
Multicast	1111 1111	FF00::/8	2/256
Global unicast	Everything else		

Global Unicast IPv6 Address



IPv6 addresses format:

- 128-bit addresses, may use dotted decimal representation; requires 16 numbers

105.220.136.100.255.255.255.255.0.0.18.128.140.10.255.255

- Groups of 16-bit numbers in hex, separated by colons - *colon hexadecimal* (or *colon hex*) representation (not case sensitive)

69DC:8864:FFFF:FFFF:0:1280:8C0A:FFFF

- Zero-compression - series of zeroes indicated by two colons

FF0C:0:0:0:0:0:B1 is equivalent with: FF0C::B1

But once in an address

- IPv6 address with 96 leading zeros is interpreted to hold an IPv4 address
- Use of “ / ” notation to denote number of bits in address represent the subnet (prefix); rest of them represent interface ID);
- /64 is common prefix length

ICANN assigns a range of IP addresses to Regional Internet Registry (RIR) organizations. The size of address range assigned to the RIR may vary but with a minimum prefix of /12 and belong to the following range: 2000::/12 to 200F:FFFF:FFFF:FFFF::/64.

Each ISP receives a /32 and provides a /48 for each site -> every ISP can provide $2^{(48-32)} = 65,536$ site addresses (note: each network organized by a single entity is often called a site).

Each site provides /64 for each LAN -> each site can provide $2^{(64-48)} = 65,536$ LAN addresses for use in their private networks.

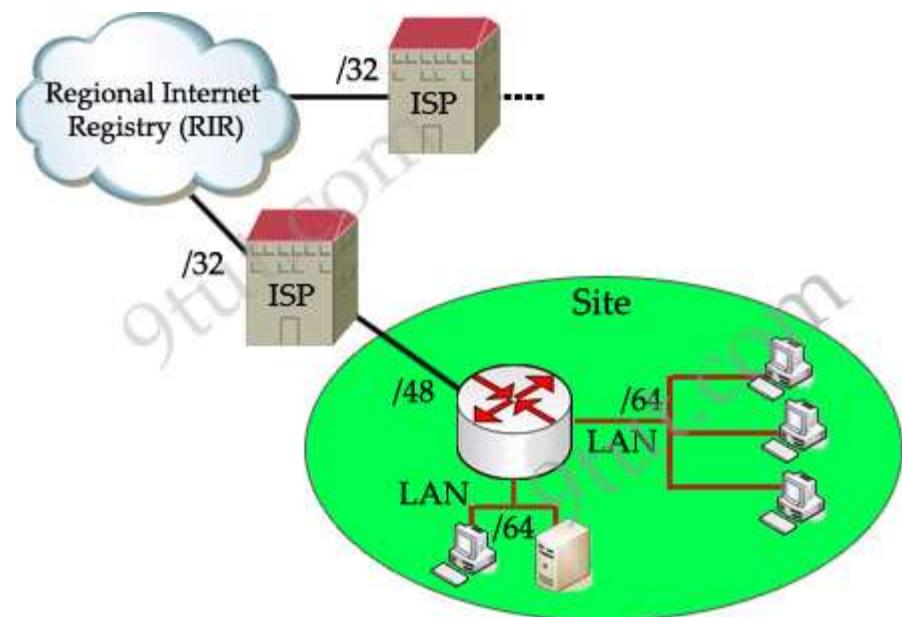
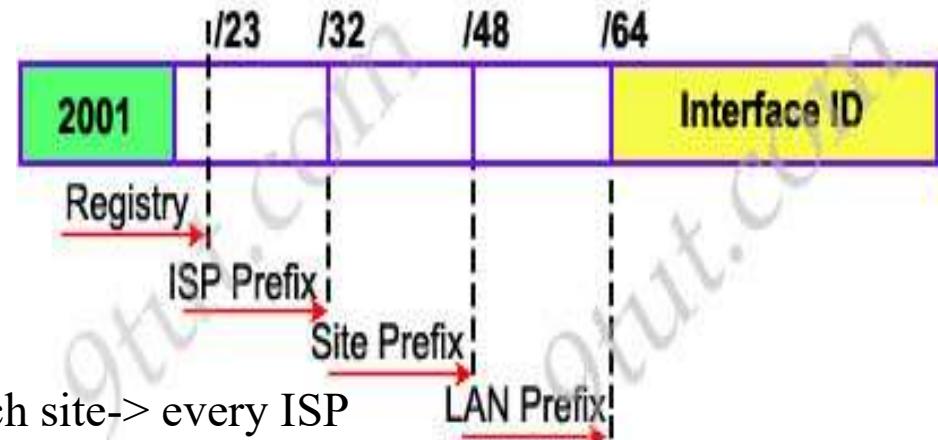
So each LAN can provide 2^{64} interface addresses for hosts.

EXAMPLE:

2001:0A3C:5437:ABCD::/64

RIR::/12 ISP::/32 Site::/48 Subnet::/64

Global Prefix (ISP-assigned) Subnet



IPv6 Address Scopes

	<i>Description</i>
Link-local address	<ul style="list-style-type: none">+ only used for communications within the local subnetwork (automatic address configuration, neighbor discovery, router discovery, and by many routing protocols). Only valid on the current subnet.+ routers do not forward packets with link-local addresses.+ are allocated with the FE80::/64 prefix -> can be easily recognized by the prefix FE80.+ is usually created dynamically using a link-local prefix of FE80::/10 and a 64-bit interface identifier (based on 48-bit MAC address).
Global unicast address	<ul style="list-style-type: none">+ unicast packets sent through the public Internet+ globally unique throughout the Internet+ starts with a 2000::/3 prefix (this means any address beginning with 2 or 3). But in the future global unicast address might not have this limitation
Site-local address	<ul style="list-style-type: none">+ allows devices in the same organization, or site, to exchange data.+ starts with the prefix FEC0::/10. They are analogous to IPv4's private address classes.

PREFIX

Interface ID

Options Headers

Carry optional information, not necessarily examined by all routers or hosts

Hop-by-Hop Options Header

Consists of the following:

Next header

Header extension length

Options

One or more option definitions

Options definition contains the following sub-fields:

Option Type – identifies option

Length – length in octets of the option's data field

Option Data – option specification

Examples for such options:

Jumbo payload option

Over $2^{16} = 65,535$ octets in an IPv6 packet

Router alert option

Tells the router that the contents of this packet is of interest to the router (to handle data accordingly)

Provides support for RSVP (Reservation Protocol), used in multimedia transmissions, for flow control

Fragmentation Header

Fragmentation only allowed at source node, no fragmentation at intermediate routers

Node must perform path discovery operation, to find the smallest MTU (Maximum Transmission Unit) of intermediate networks

Source fragments IPv6 packets to match MTU

Otherwise limits to 1280 octets, that must be supported by any network

Fragmentation Header Fields:

Next Header – type of following header

Reserved

Fragmentation offset – any fragment data is multiple of 64bits; this field indicates where in the original packet this fragment's payload belongs

Reserved

More flag – more fragments or last fragment

Identification – identify the original packet (now fragmented)

Routing Header

List of one or more intermediate nodes to be visited

Structure (see next):

Next Header

Header extension length – length of this header

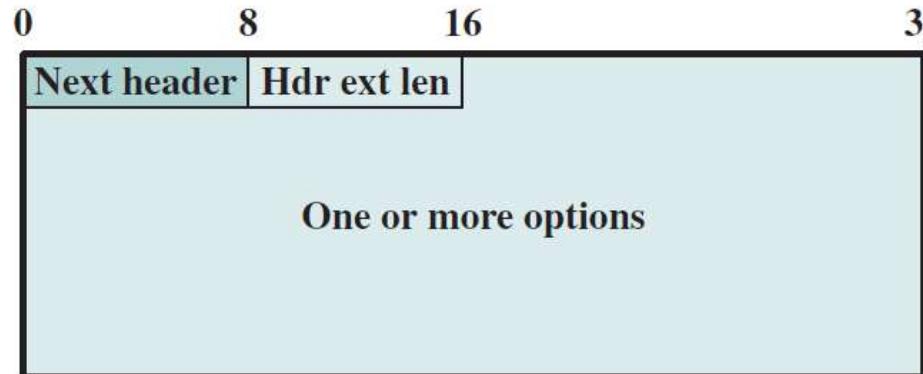
Routing type – identifies a routing protocol header variant

Segments left - number of nodes still to be visited

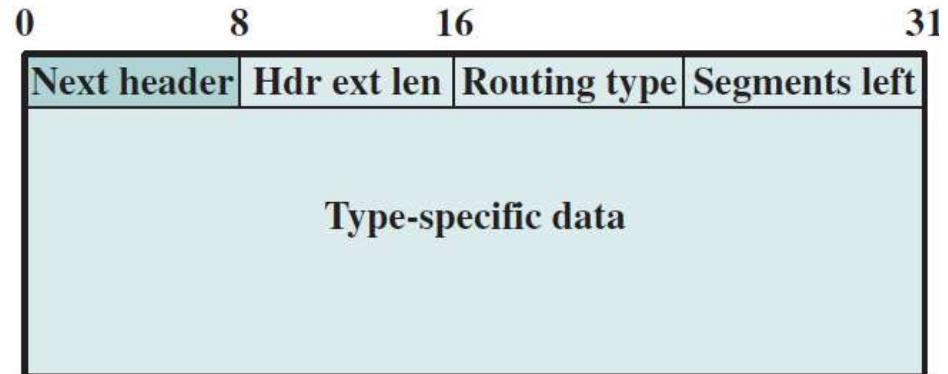
Destination Options Header

Information examined by the destination node

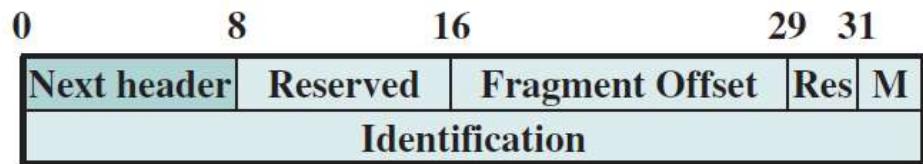
Same format as Hop-by-Hop options header



(a) Hop-by-Hop Options header;
Destination Options header



(c) Generic Routing header

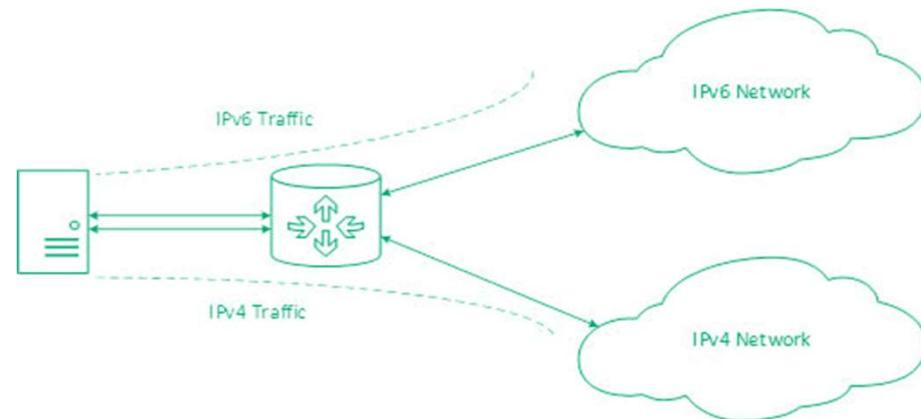


(b) Fragment header

IPv6 Extension Headers

Technologies can be used in transition from IPv4 to IPv6

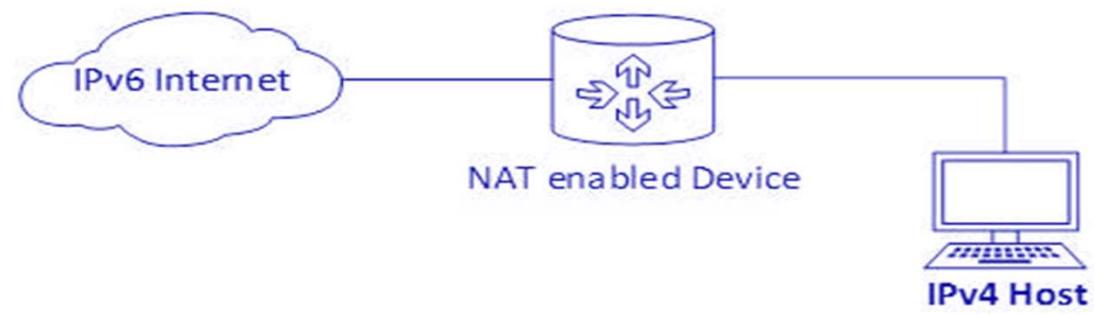
Dual Stack Routers



Tunneling



NAT Protocol Translation



Multicasting

Addresses that refer to group of hosts on one or more networks

Used in:

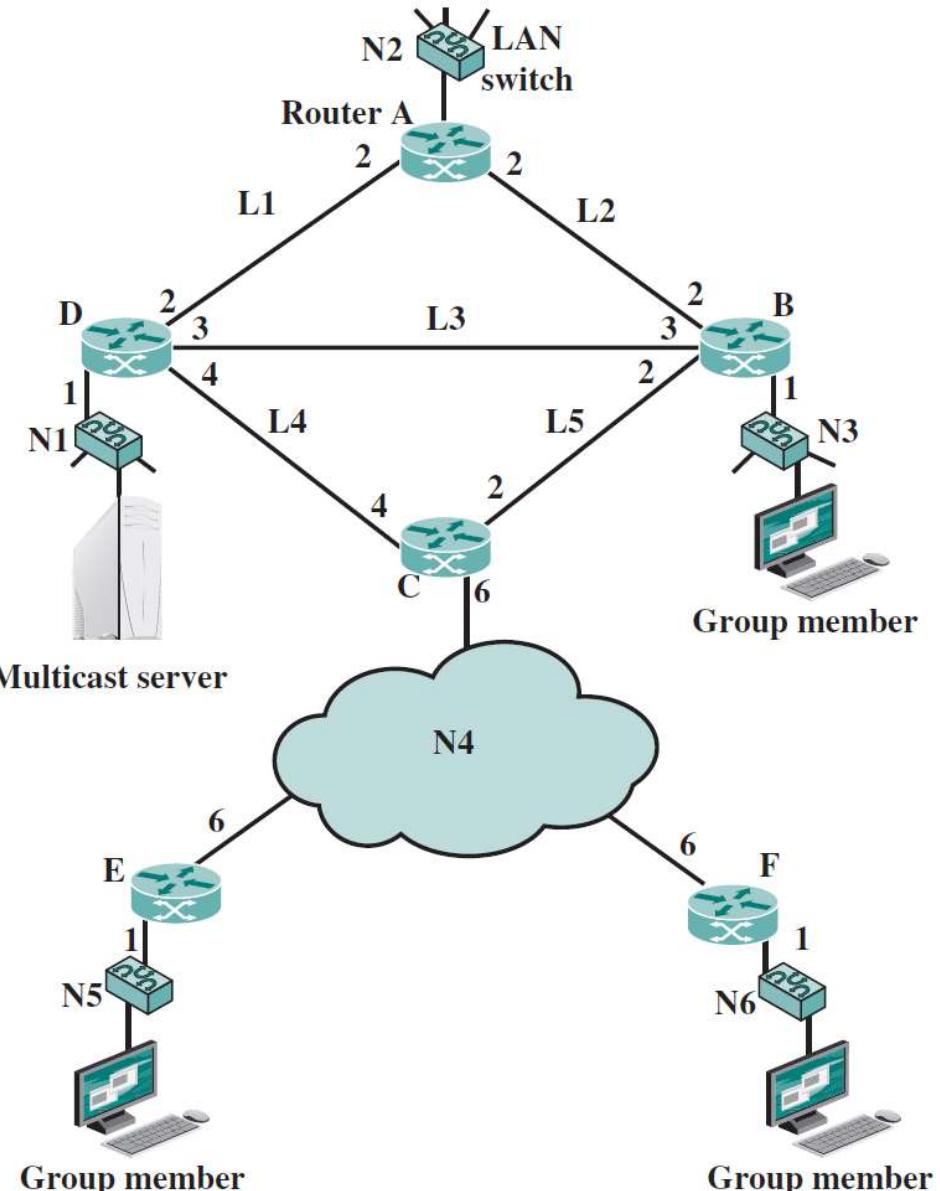
Multimedia stream “broadcasts”

Teleconferencing – a transmission from a station sent to all members

Database updating – for all copies of replicated files or databases

Distributed computing – resource sharing

Real time workgroups – real time exchange of information



Multicast Configuration

Multicast over a single Ethernet LAN segment is straightforward; provision for MAC multicast addresses, due to the broadcast nature of LAN

For Internet environment, more approaches:

Broadcast and Multiple Unicast

Broadcast a copy of packet to each network, even if does not contain group members

For figure behind, multicast server sends a packet to group hosts from networks N3, N5, N6: requires 13 copies of the packet

Multiple Unicast

Send packet only to networks that have hosts in group

Source knows location for each group member

11 packets

True Multicast

Use of following algorithm:

Determine least cost path to each network that has host in group

Gives spanning tree configuration containing networks with group members

Transmit single packet along spanning tree

Routers replicate packets at branch points of the spanning tree

8 packets required for above example

	Broadcast					Multiple Unicast				Multicast
	S → N2	S → N3	S → N5	S → N6	Total	S → N3	S → N5	S → N6	Total	
N1	1	1	1	1	4	1	1	1	3	1
N2										
N3	1	1	1				1	1		
N4			1	1	2		1	1	2	2
N5			1		1		1		1	1
N6			1	1			1	1	1	
L1	1			1						
L2										
L3		1		1		1		1		1
L4			1	1	2		1	1	2	1
L5										
Total	2	3	4	4	13	3	4	4	11	8

Multicast problems:

Router may have to forward more than one copy of packet (multiple output branches)

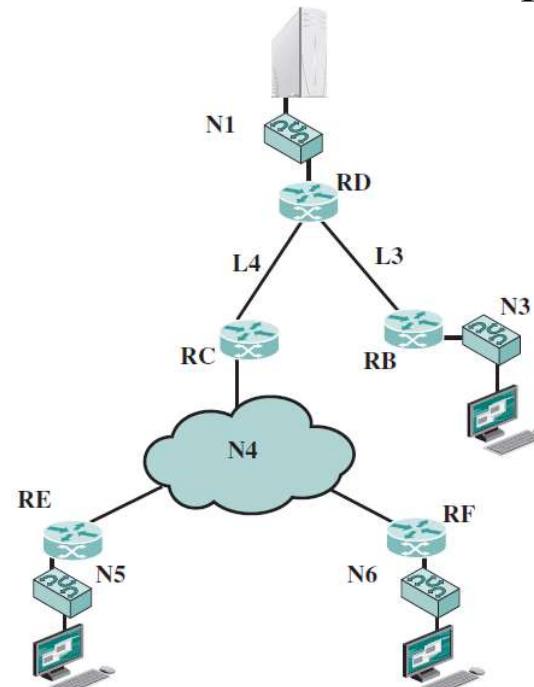
Convention needed to identify multicast addresses

IPv4 - Class D – starts with 1110 ...

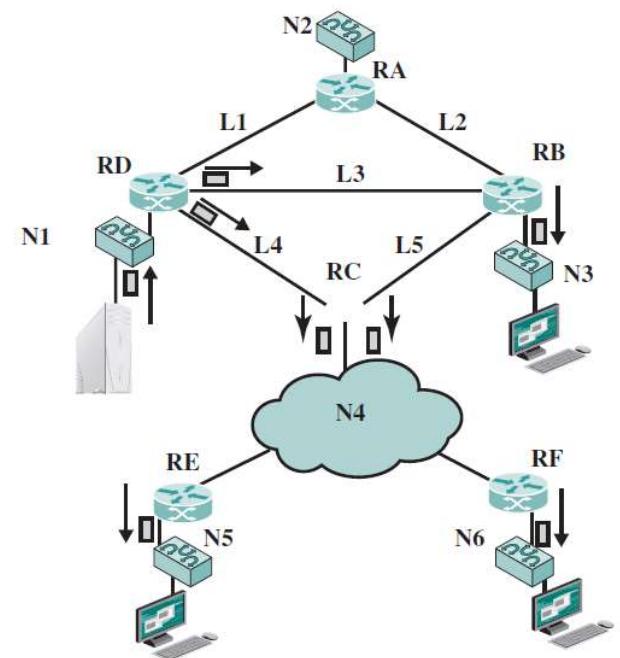
IPv6 - 8 bit prefix, all 1s, 4 bit flags field, 4 bit scope field, 112 bit group ID

Nodes (routers & source) must translate between IP multicast addresses and a list of networks containing group members; allows tree development

Multicast transmission example



(a) Spanning tree from source to multicast group



(b) Packets generated for multicast transmission

Router must translate between IP multicast address and a network LAN multicast address (at the MAC level) in order to deliver packet to that LAN

Mechanism required for hosts to dynamically join and leave multicast groups

Routers must exchange info

- Which networks include members of given group

- Sufficient info to work out shortest path to each network (spanning tree)

- Routing algorithm to work out shortest path

- Routers must determine routing paths based on source and destination addresses, for avoiding packet duplication

IGMP (Internet Group Management Protocol)

RFC 1112, initial developed for IPv4, but incorporated also in ICMPv6

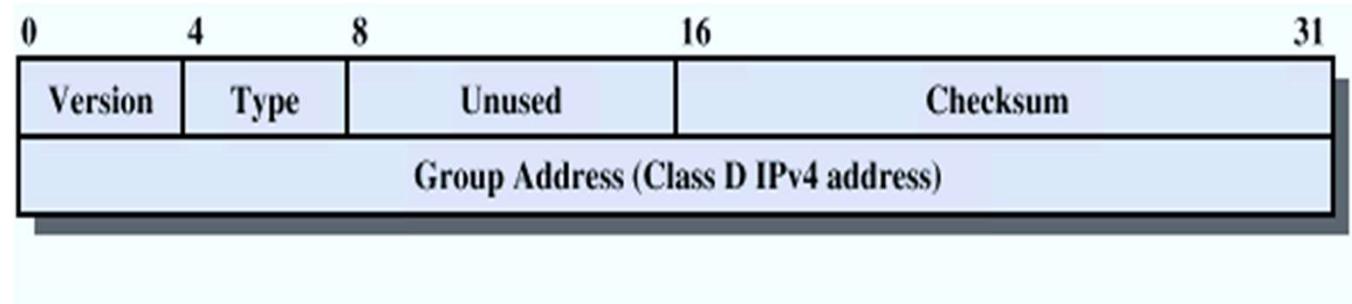
Host and router exchange of **multicast group information**

Use broadcast LAN to transfer information among multiple hosts and routers

IGMP Fields

Version - 1

Type



1 - query sent by a multicast router

0 - report sent by a host

Checksum – 16 bit ones complement addition of all the 16-bit words in the message

Group address

Zero value in a request message

Valid group address in a report message

IGMP Operation

To join a group, hosts sends report message

Group address of group to join

Sent in a IP datagram with the same multicast destination address

All hosts in group receive message and learn new member

Routers listen to all multicast addresses to hear all reports

Routers periodically issue request messages (queries)

Sent to *all-hosts* multicast address

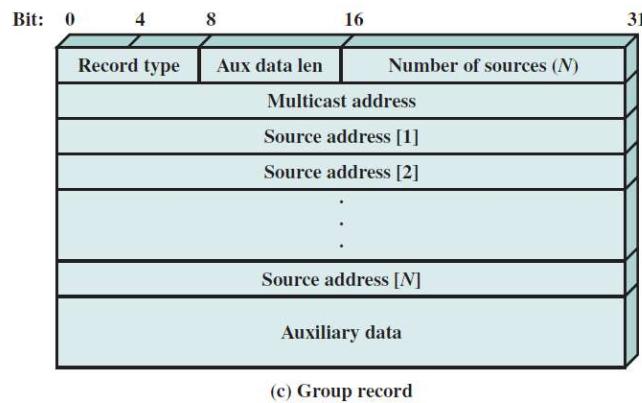
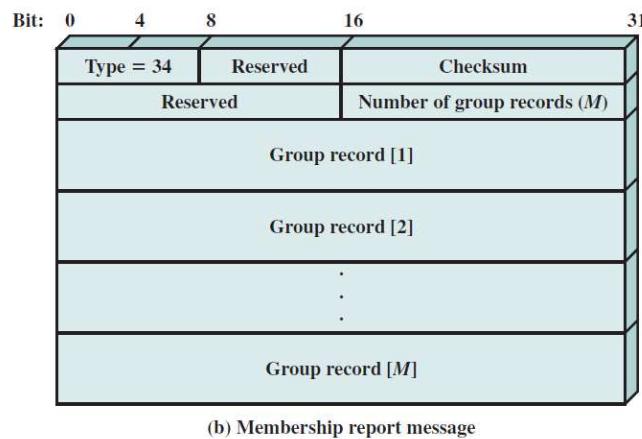
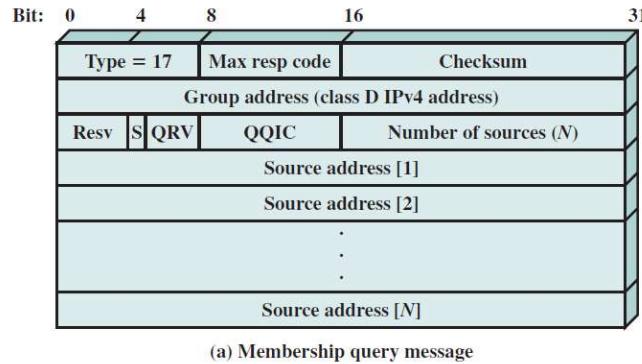
Host that want to stay in groups must read *all-hosts* messages and respond with report for each group it is in

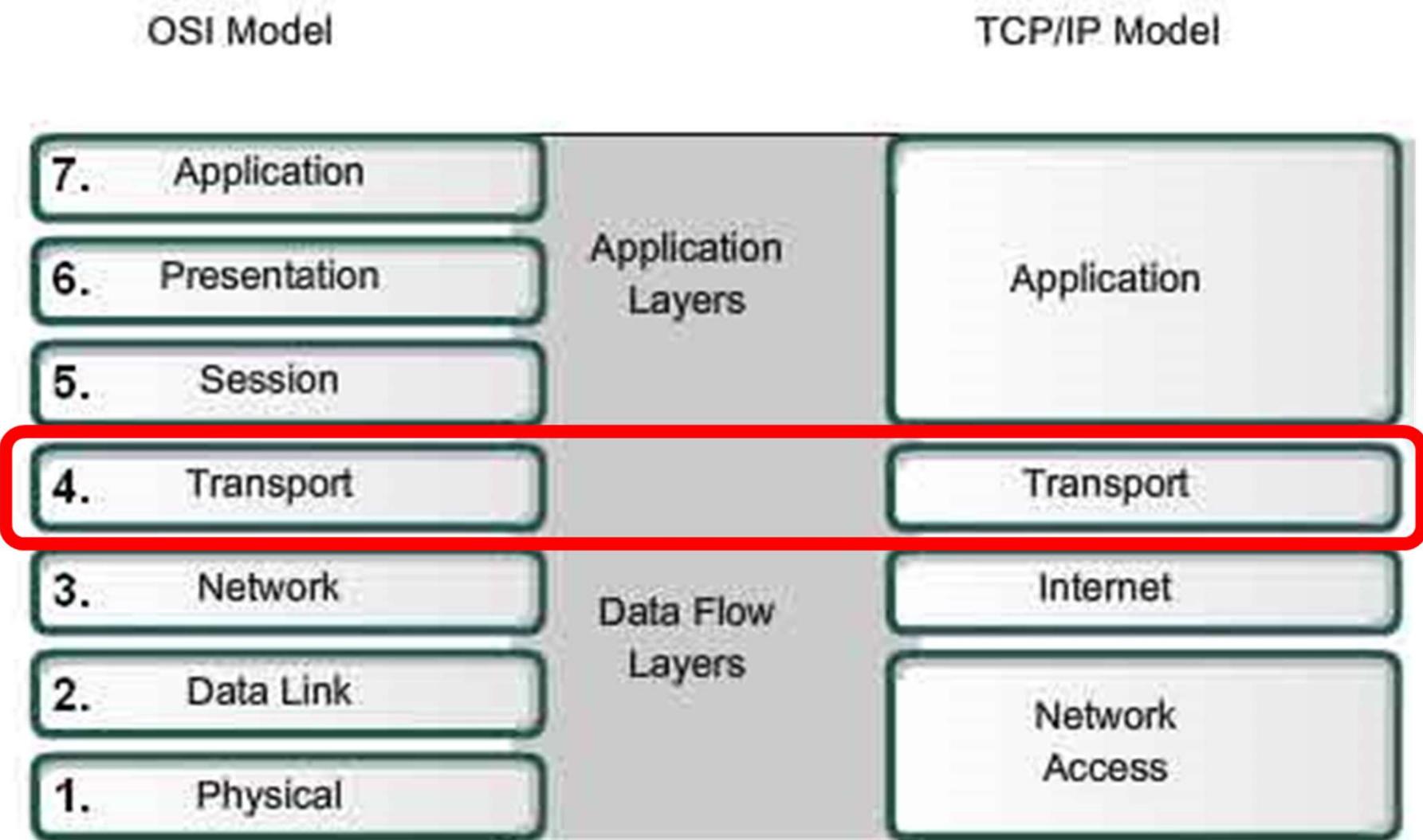
Group Membership with IPv6

Function of IGMP included in ICMP v6; ICMPv6 contains a new type of message: group membership **termination** message, to allow host to leave the group

IGMP v3

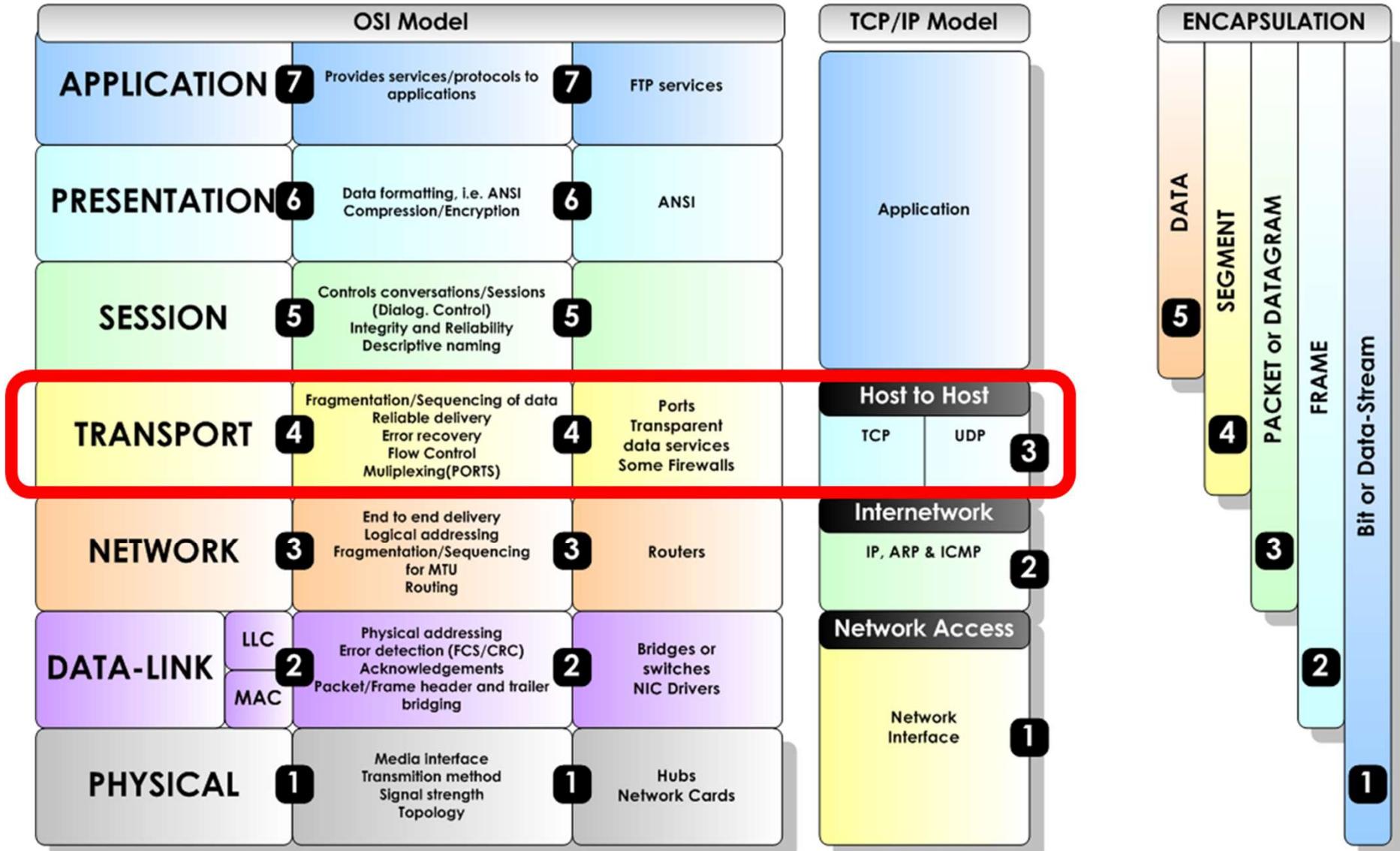
RFC 3376





The OSI Model (Open Systems Interconnection)

© Copyright 2008 Steven Iveson
www.networkstuff.eu



Transport-level Protocols

Connection Oriented

Transmission Control
Protocol (TCP)

Logical connection

Establishment

Maintenance, termination

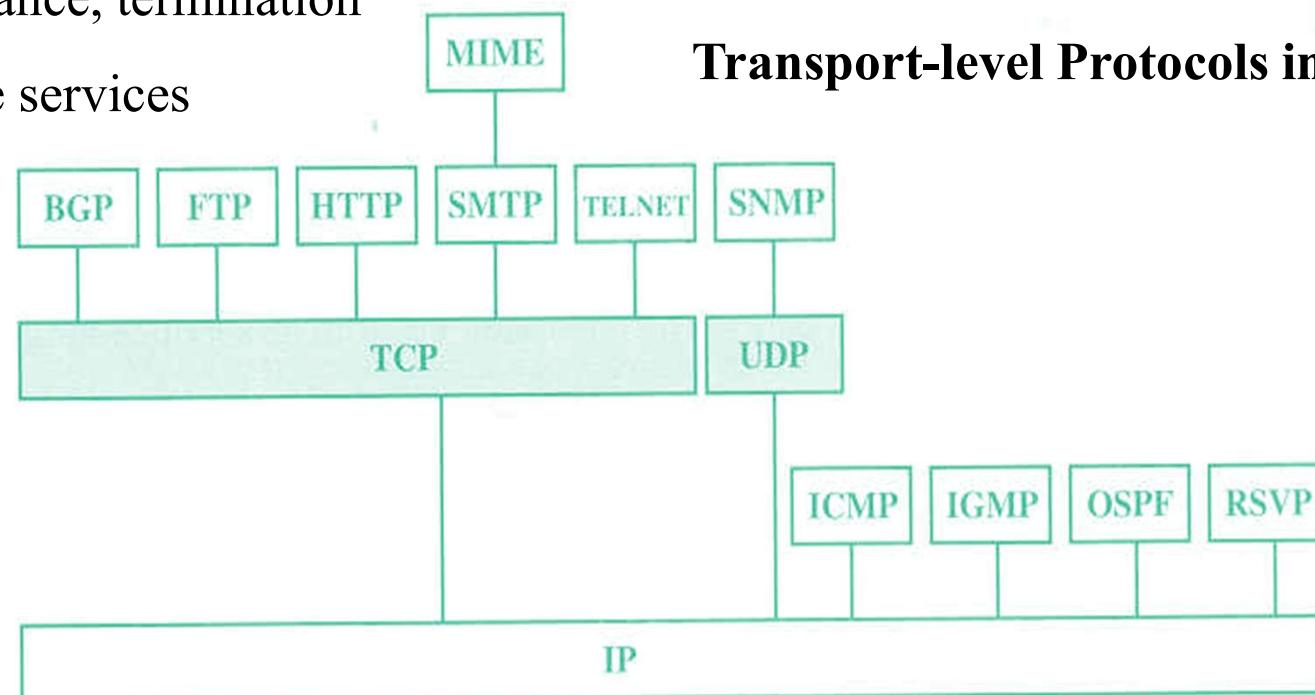
Reliable services

Connectionless

User Datagram Protocol (UDP)

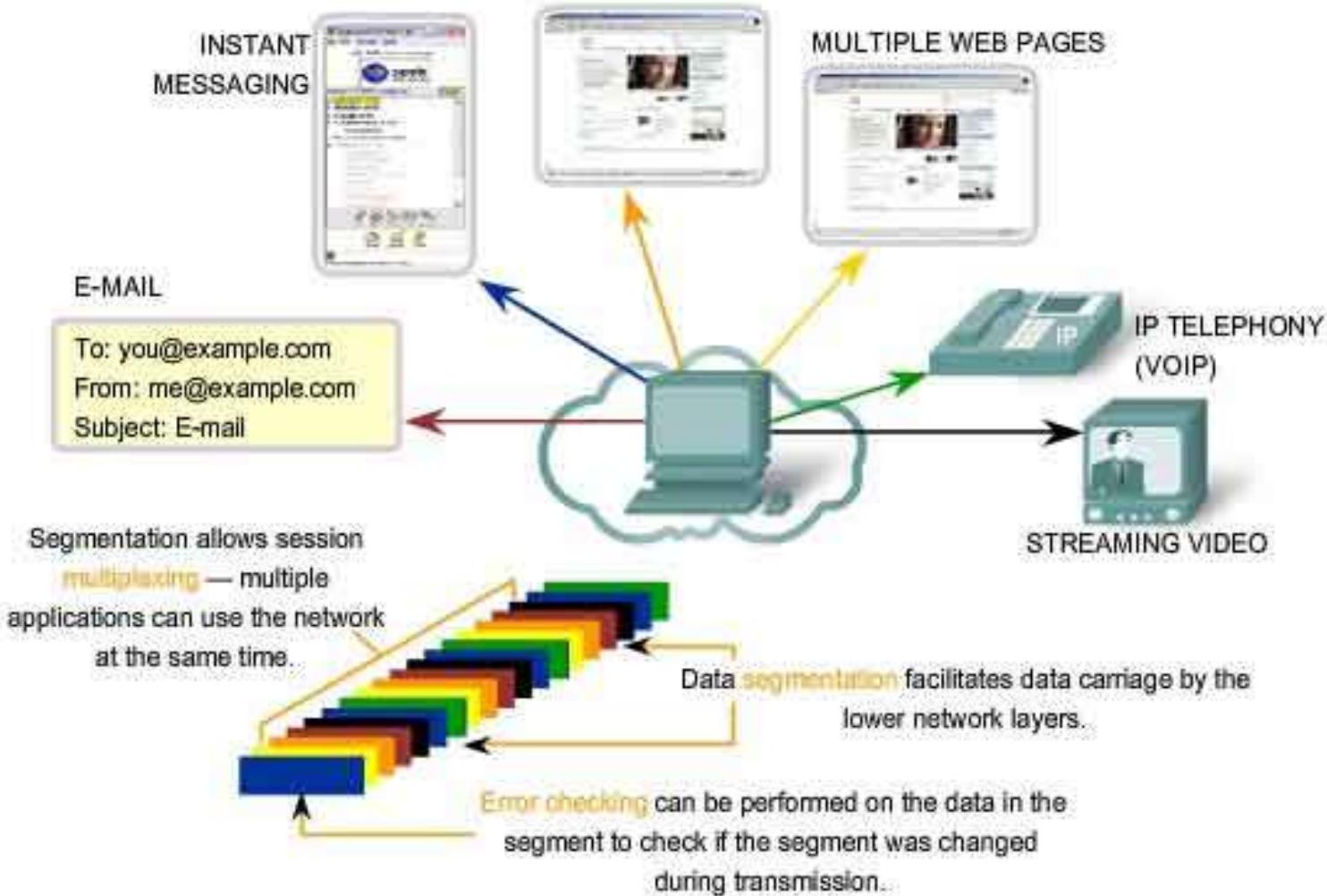
Connectionless

'Best-effort' delivery



Transport-level Protocols in Context

Transport Layer Services



Transmission Control Protocol (TCP)

Connection oriented

Reliable byte stream over unreliable IP

IP may be transported over many different network technologies

RFC 793

Each end: a socket

Socket is a pair of: IP address + port number

Multiple connections may be active on a socket

Full duplex connections

Point to point links

No multicast or broadcast

Other protocols used for these

May buffer information to increase amount sent

PUSH flag requests that buffered data be sent

Communicating computers must agree on a port number

'Server' opens selected port and waits for incoming messages

'Client' selects local port and sends message to selected port

Services provided by many computers use reserved, *well-known* port numbers:

TFTP, DNS, Echo

Other services use *dynamically assigned* port numbers

Port	Name	Description
7	echo	Echo input back to sender
9	discard	Discard input
11	systat	System statistics
13	daytime	Time of day (ASCII)
17	quote	Quote of the day
19	chargen	Character generator
37	time	System time (seconds since 1970)
53	domain	DNS
69	tftp	Trivial File Transfer Protocol (TFTP)
123	ntp	Network Time Protocol (NTP)
161	snmp	Simple Network Management Protocol (SNMP)

Transmission Control Protocol (TCP)

TCP general features

- *Connection oriented*: Application requests connection to destination and then uses connection to deliver data to transfer data
- *Point-to-point*: A TCP connection has two endpoints
- *Reliability*: TCP guarantees data will be delivered without loss, duplication or transmission errors
- *Full duplex*: The endpoints of a TCP connection can exchange data in both directions simultaneously
- *Stream interface*: Application delivers data to TCP as a continuous *stream*, with no record boundaries; TCP makes no guarantees that data will be received in same blocks as transmitted
- *Reliable connection establishment*: *Three-way handshake* guarantees reliable, synchronized startup between endpoints
- *Graceful connection termination*: TCP guarantees delivery of all data after endpoint shutdown by application

TCP Services

Reliable communication between pairs of processes (applications)

Across variety of reliable and unreliable networks and internets

Two labeling facilities:

- Data stream push

- TCP user can require transmission of all data up to push flag

- Receiver will deliver in same manner

- Avoids waiting for full buffers

- Urgent data signal

- Indicates urgent data is upcoming in stream

- User decides how to handle it

TCP uses IP for data delivery

- Endpoints are identified by ports (sockets)

- 16-bit number

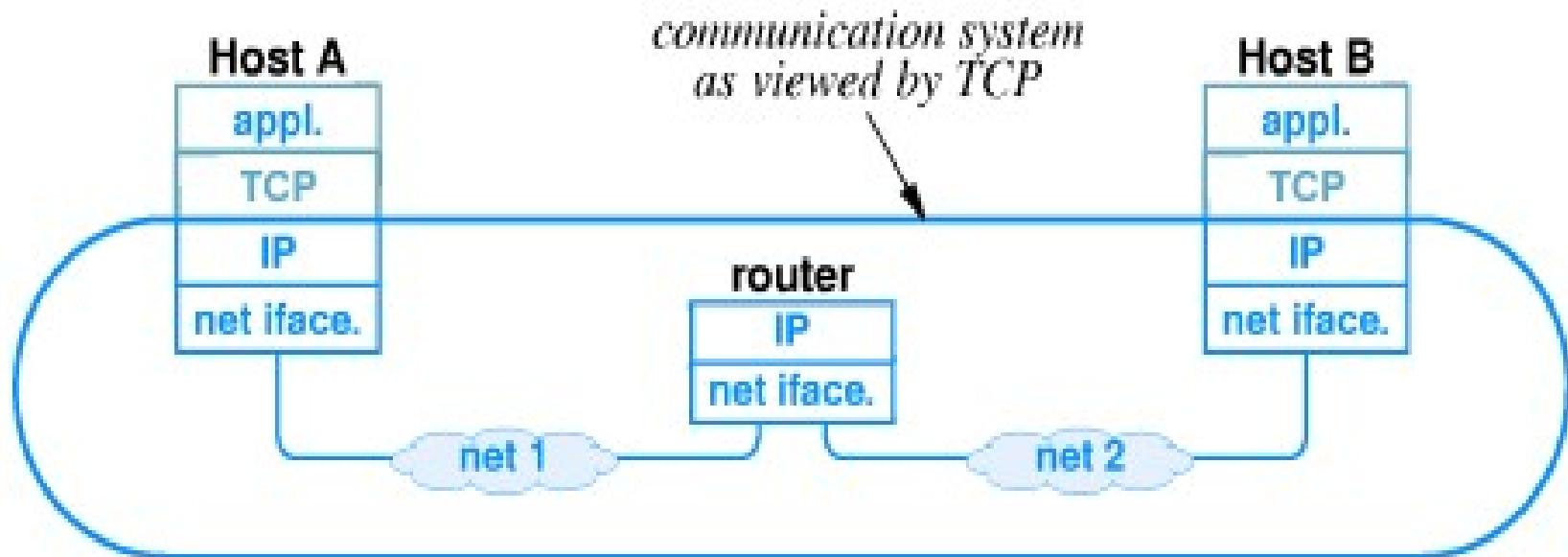
- System Ports range (0-1023): “well-known ports” which provide well-known services; assignment through IANA

<https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml>

- User Ports range (1024-49151) are available for assignment through IANA

- Dynamic Ports range (49152-65535) have been specifically set aside for local and dynamic use and cannot be assigned through IANA.

- Allows multiple connections on each host
- Ports may be associated with an application or a process
- IP treats TCP like data and does not interpret any contents of the TCP message



TCP services at the boundary with the process (application level) are defined using the concepts of abstract service primitives (TCP ASPs) and service-access points (SAPs). The primitives are implemented using the segment header fields or passing some parameters at the IP level.

Items Passed to IP

TCP passes some parameters down to IP

- Precedence of segments

- Normal delay/low delay

- Normal throughput/high throughput

- Normal reliability/high reliability

- Security

Also, TCP Protocol:

Breaks application messages into *segments* (TCP data units)

Each segment has an (at least) 20 byte header

Segments are sized based on:

being less than the 64kbytes (the path Maximum Transmission Unit (MTU))

Segments may be *fragmented* during transmission if MTU smaller than packet

TCP Header Fields

Source port – source TCP user

Destination port – destination TCP user

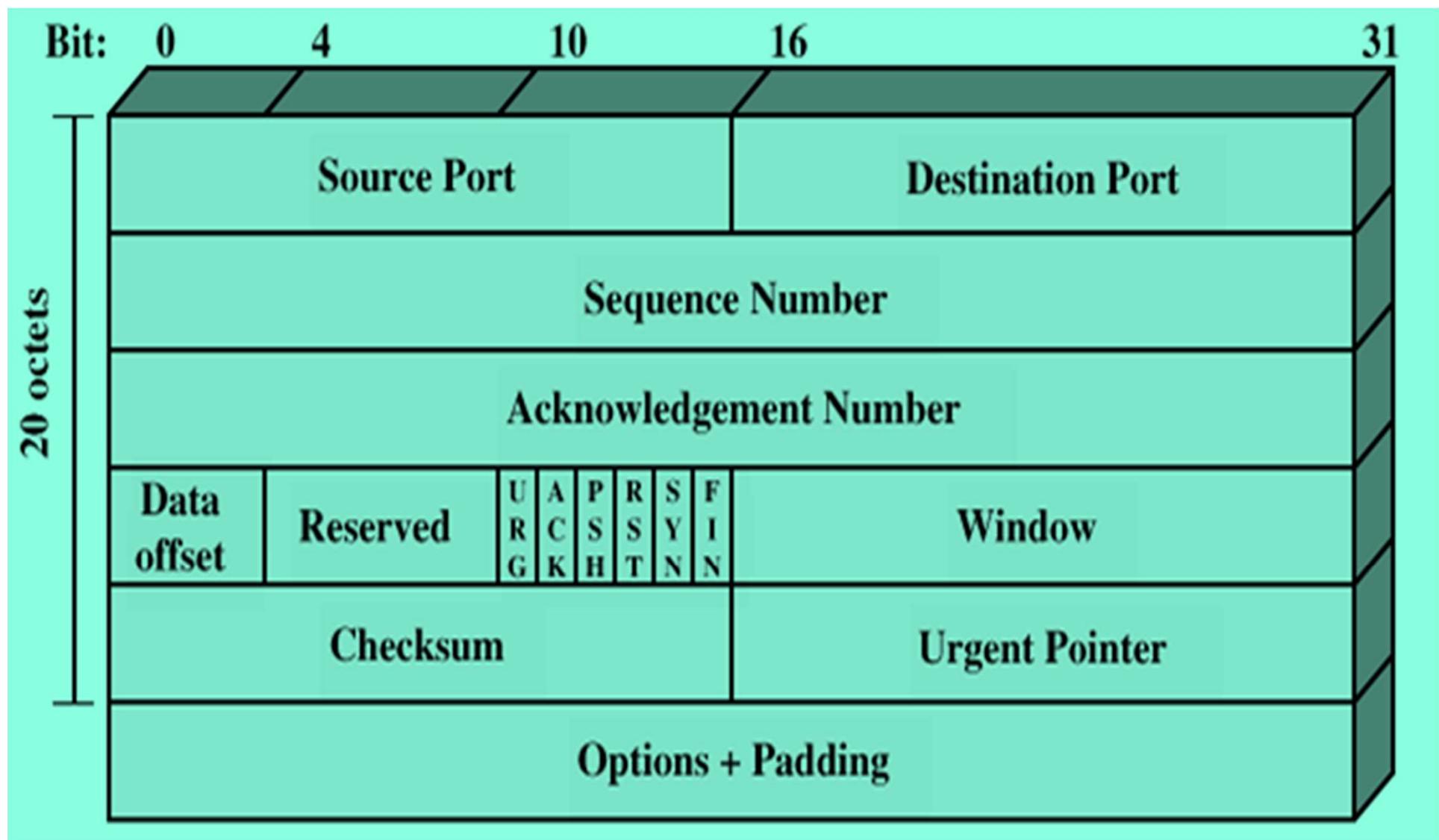
Sequence number – sequence number of the first data octet in this segment

Acknowledgement number – piggybacking acknowledgement, contains sequence number of next data octet the destination TCP entity expects to receive

Data offset – number of words (32 bit) in this header (header flexible length)

Reserved – for future use & developments

TCP Header



Flags – 6 bits:

URG – urgent pointer field significant

ACK – acknowledgement field significant

PSH – Push function

RST – reset connection

SYN – synchronize the sequence numbers (used in connection establishment)

FIN – no more data from sender (used in connection termination)

Window – flow control credit allocation in octets (window size)

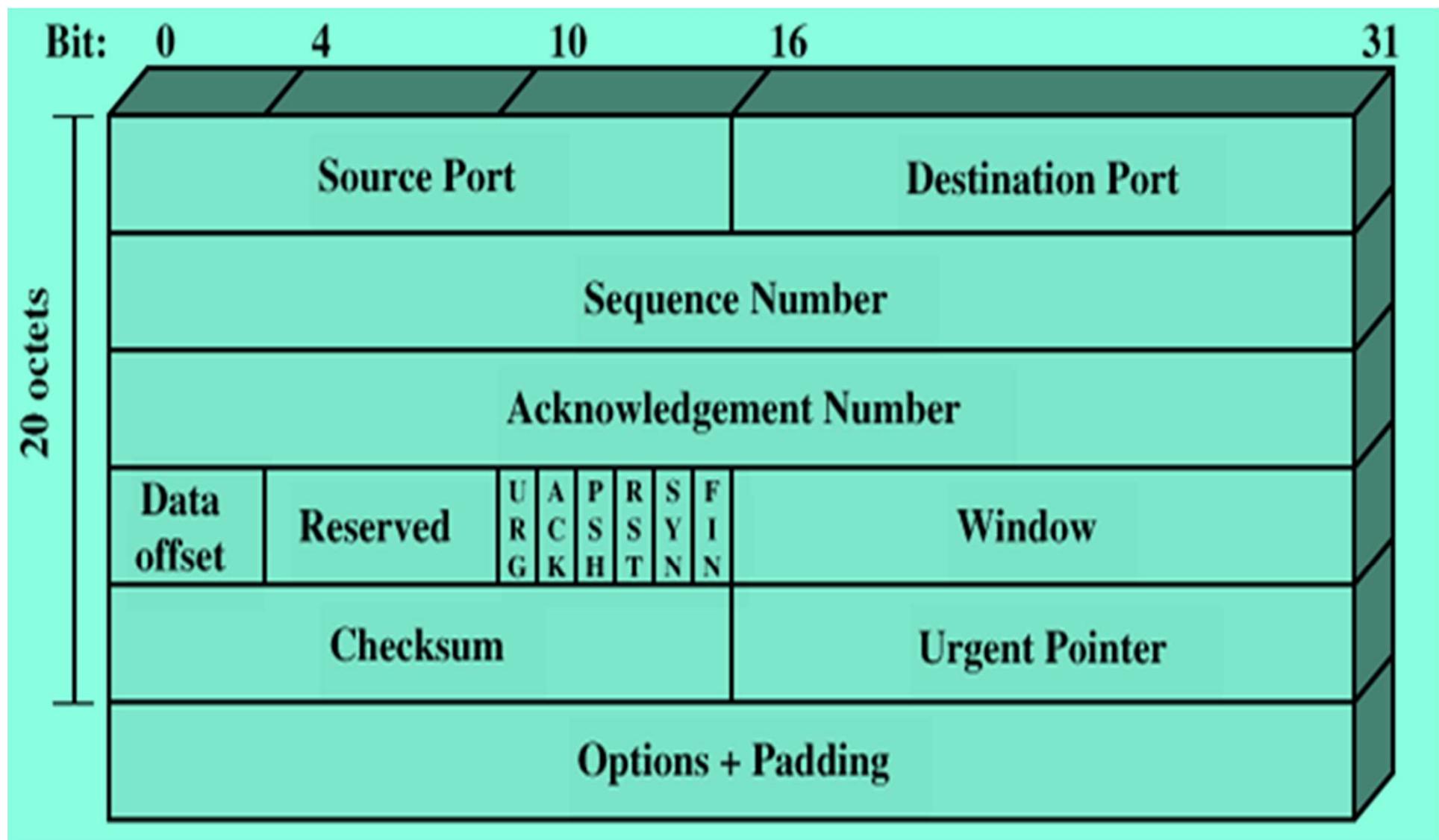
Checksum – ones complement of the sum modulo $2^{16}-1$ of all 16-bit words in the segment (plus eventually pseudo-header)

Urgent Pointer – pointer to the last octet in a sequence of urgent data

Options – variable field

Padding – to meet segment length of multiple of 32 bit

TCP Header



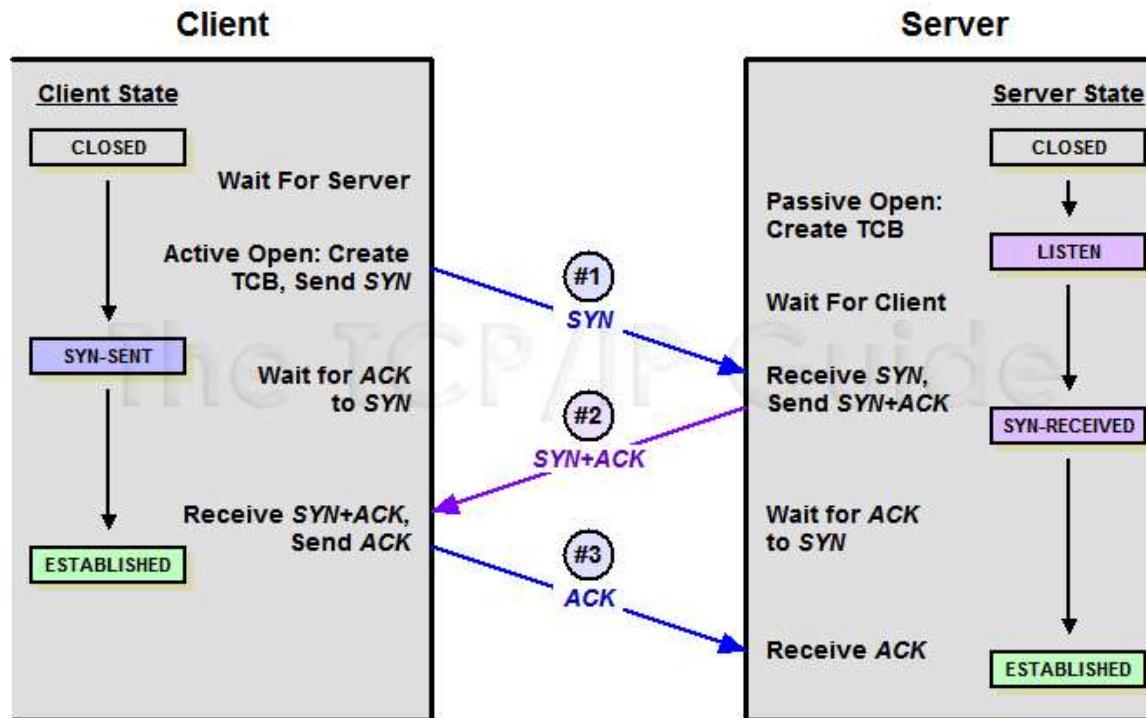
TCP Mechanisms

Connection establishment

Three way handshake used for connection establishment (exchange of SYNs)

Each TCP connection is established between pair of ports

One port can connect to multiple destinations (may support multiple connections)



TCP Mechanisms

Connection establishment

Three way handshake used for connection establishment (exchange of SYNs)

Each TCP connection is established between pair of ports

One port can connect to multiple destinations (may support multiple connections)

Data transfer

Logically, data is considered a stream of octets

Octets numbered modulo 2^{32}

Data is transferred over a TCP connection in segments

Flow control by credit allocation of number of octets

Data buffered at transmitter and receiver

Use of *PUSH* flag for forcing transmission of so far accumulated date (end-of-block function)

User may specify *urgent* data transmission

Connection termination

Graceful close (normal exchange of FIN info)

TCP users issues CLOSE primitive

Transport entity sets FIN flag on last segment sent

Abrupt termination by ABORT primitive

Entity abandons all attempts to send or receive data

RST segment transmitted (connection Reset)

Implementation Policy Options (allows for possible TCP implementations)

Send policy

Deliver policy

Accept policy

Retransmit policy

Acknowledge policy

Send policy

If no *Push* flag or CLOSE indication, a TCP entity transmits at its own convenience

- Used Data buffered at transmit buffer

- TCP entity may construct segment per data batch as provided by user

- May wait for certain amount of data

Policy depends on performance considerations (header overhead/response speed)

Delivery Policy

In absence of *Push*, receiving TCP entity may deliver data to the user at own convenience

- May deliver as each in order segment received

- May buffer data from more than one segment

Policy depends on how promptly user needs data, or how much processing involved (each delivery = application software interrupts)

Acknowledgement policy

- Immediate ACK

- Cumulative ACK

Accept policy

Segments may arrive out of order; options:

- In order

- Only accept segments in order

- Discard out of order segments

- In windows

- Accept all segments within receiver window

Retransmit policy

TCP maintains queue of segments transmitted but not acknowledged

Policy depends mainly on receiver acceptance policy (in order or in window)

TCP will retransmit if not ACKed in given time; retransmission options:

First only segment from the queue (necessary one timer for entire queue)

Batch – all segments from queue (one timer for entire queue)

Individual – one timer for each segment in queue; retransmits the individual segment

TCP Congestion Control

Basic idea in congestion avoidance: don't insert a new packet until an old one leaves

Other Basic idea: timeouts associated with retransmission are due to congestion state

Approaches based on re-transmission timer & window size management:

Timers for re-transmission: time-out management

TCP Congestion control estimate round trip delay, by observing delay pattern in recent segments, and then sets the timer to a value a little bit greater

Estimations based on:

Simple average

Average Round-Trip Time (ARTT) for a segment i , is the simple average of delays for the precedent k transmitted segments.

Exponential Average

Gives a better prediction of the next RTT value

Binary exponential Backoff algorithm (see CSMA/CD) may be used for obtaining values for the retransmission time-out values (RTOs)

Exponential RTO Backoff

Since timeout value is probably due to congestion (dropped packet or long round trip), maintaining same RTO is not a good idea

RTO increased each time a segment is re-transmitted

$$\text{RTO} = q * \text{RTO}$$

Commonly $q=2$

Known as Binary exponential backoff

Window management

TCP Window size may affect transmission parameters; need for managing size:

Used Techniques

Slow Start

If start using window size as provided by past connection, may cause excessive flow, internet conditions may differ

Solution: sender starting with a smaller window size

Two windows: allowed window and congestion window, sized in segments, no octets

$$\text{Allwd_wndw} = \min(\text{cngst_wndw}, \text{gained_credit})$$

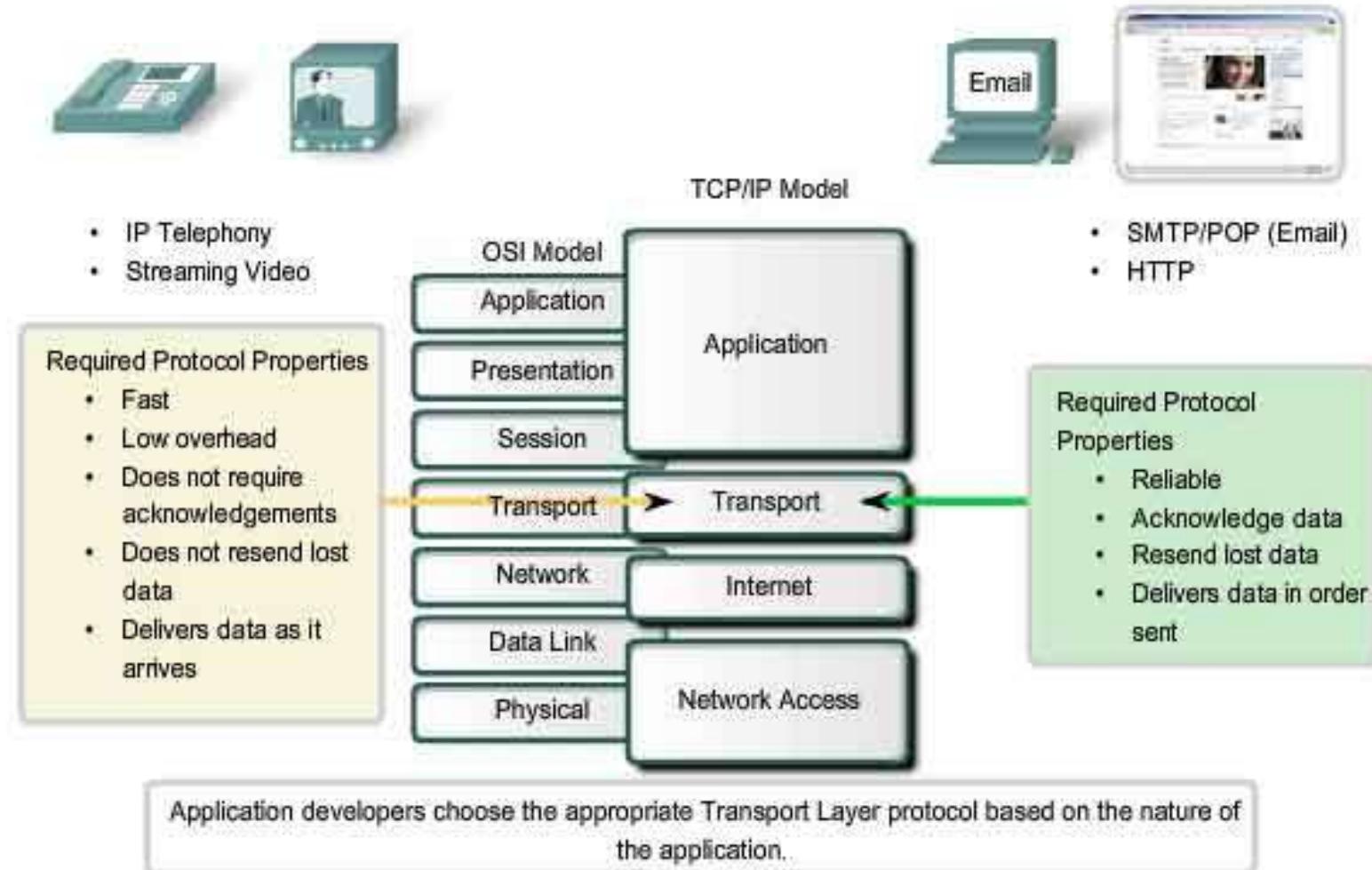
cngst_wndw starts with value 1, then increments every acknowledged segment

Dynamic window sizing on congestion

A possible scenario: When first segment lost, means collision sign, so reset value of cngst_wndw to 1 and begin ‘slow start’

There are more others

Transport Layer Protocols



User Datagram Protocol (UDP)

Connectionless

Less overhead

Used mostly for

real-time applications (voice, video, telemetry), with no need for retransmissions

non-critical functions: inward data collections (monitoring ...), outward data collections (broadcasted announcements ...)

Specified by RFC 768

Unreliable

Delivery and duplication control not guaranteed

UDP delivers independent messages, called *datagrams* between applications or processes on host computers

'Best effort' delivery - datagrams may be lost, delivered out of order, etc.

Checksum (optionally) guarantees integrity of data

For generality, endpoints of UDP are called *protocol ports* or *ports*

Each UDP data transmission identifies the internet address and port number of the destination and the source of the message (port, socket ... as TCP)

UDP header is very simple:

- Port numbers
- Message length
- Checksum (optional, if yes, use same 1s complement checksum as IP)

UDP Header



Introduction to Internetworking

Introductory terms

Communications Network

Facility that provides data transfer services

An internet

Collection of communications networks interconnected by bridges and/or routers

The Internet - note upper case I

The *global collection* of thousands of individual machines and networks

Intranet

Corporate internet operating within the organization

Uses Internet (TCP/IP and http) technology to deliver documents and resources

End System (ES)

Device attached to one of the networks of an internet

Supports end-user applications or services

Intermediate System (IS)

Device used to connect two networks

Permits communication between end systems attached to different networks

Bridge

IS used to connect two LANs using similar LAN protocols

Address filter passing on packets to the required network only

OSI layer 2 (Data Link)

Router

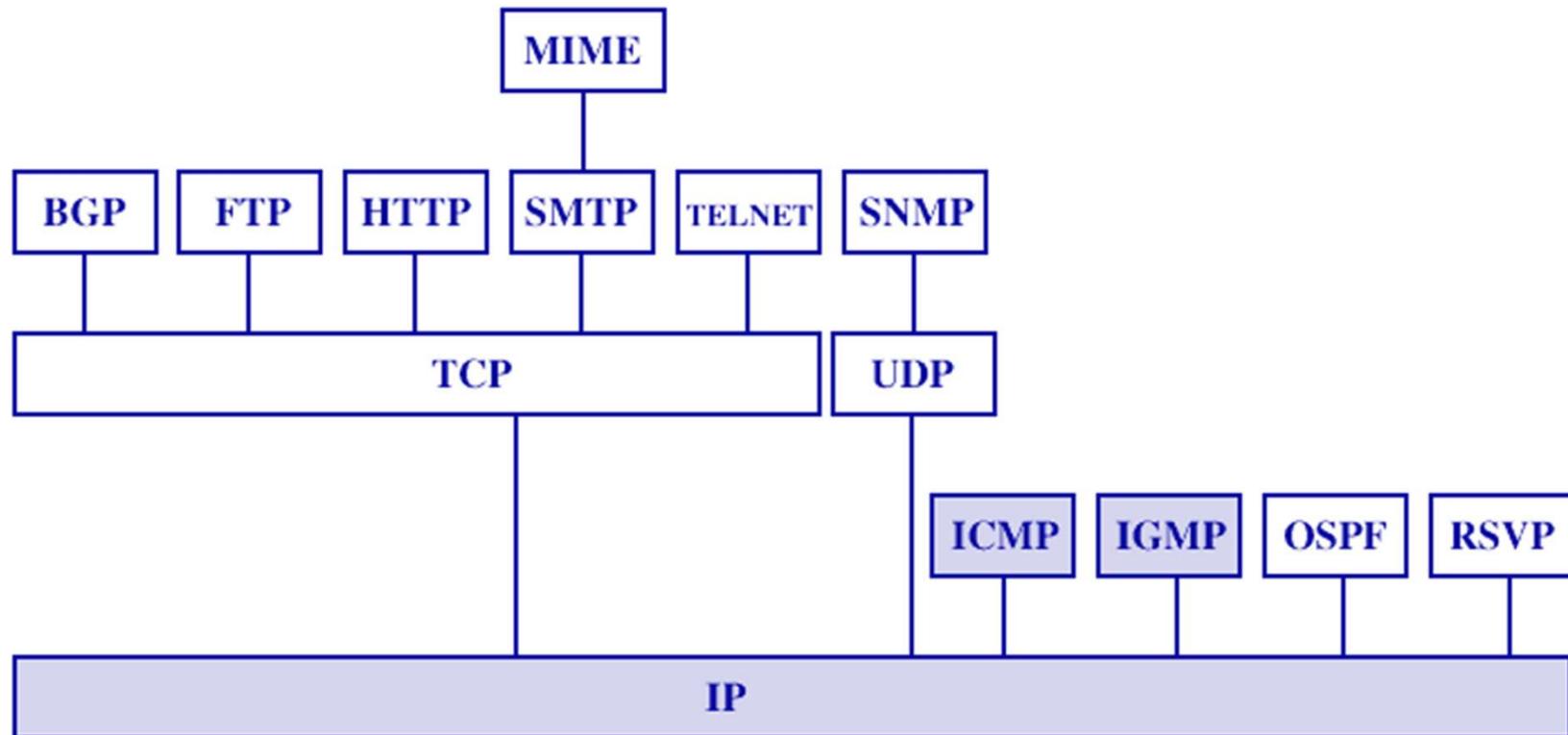
Connects two (possibly dissimilar) networks

Uses internet protocol present in each router and end system

OSI Layer 3 (Network)

Internetworking Protocols

TCP/IP stack and suite of internetworking protocols



Requirements of Internetworking

Link between networks

Minimum physical and link layer

Routing and delivery of data between processes on different networks

Accounting services and status info

Independent of network architectures

Network Architecture Specific Features

Addressing

Packet size

Access mechanism

Timeouts

Error recovery

Status reporting

Routing

User access control

Architectural Approaches

Connection oriented

Connectionless

Connection Oriented

Assume that each network is connection oriented

IS connect two or more networks

IS appear as DTE to each network

Logical connection set up between DTEs

Concatenation of logical connections across networks

Individual network virtual circuits joined by IS

May require enhancement of local network services

802, FDDI are datagram services

Connection Oriented IS Functions

Relying

Routing

e.g. X.75 used to interconnect X.25 packet switched networks

Connection oriented not often used

Connectionless Operation

Corresponds to datagram mechanism in packet switched networks

Each NPDU treated separately

Network layer protocol common to all DTEs and routers

Known generically as the internet protocol

Internet Protocol

One such internet protocol developed for ARPANET

RFC 791

Lower layer protocol needed to access particular network

Connectionless Internetworking

Advantages

Flexibility

Robust

No unnecessary overhead

Main drawback: Unreliable

Not guaranteed delivery

Not guaranteed order of delivery

Packets can take different routes

Reliability is responsibility of next layer up (e.g. TCP)

Example of an IP protocol operations, acting over a X.25 packet switched WAN network

Design Issues

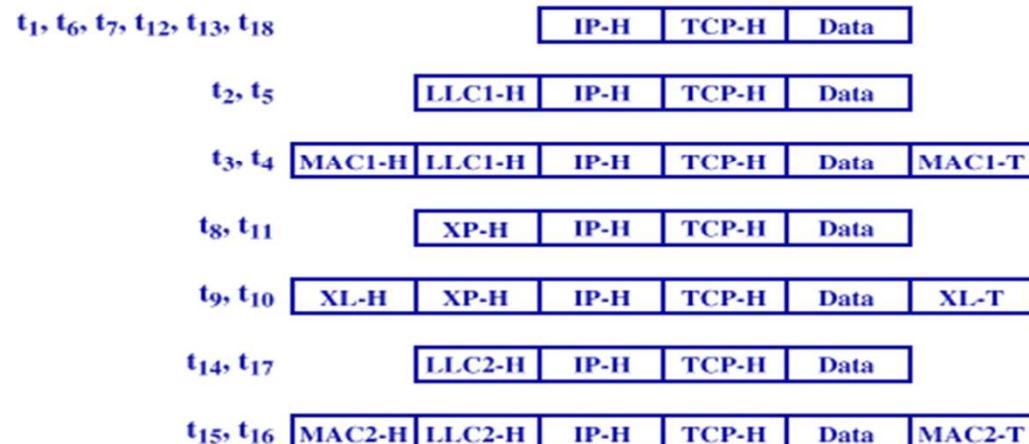
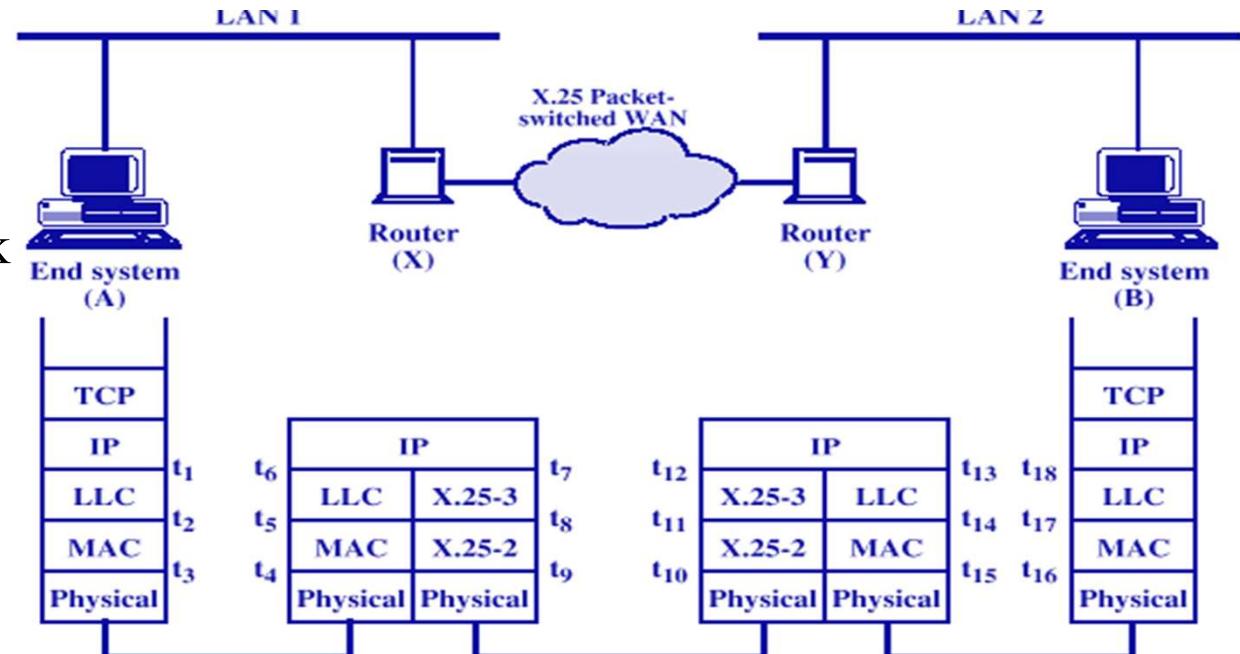
Routing

Datagram lifetime

Fragmentation and
re-assembly

Error control

Flow control



TCP-H = TCP header MACi-T = MAC trailer
 IP-H = IP header XP-H = X.25 packet header
 LLCi-H = LLC header XL-H = X.25 link header
 MACi-H = MAC header XL-T = X.25 link trailer

Routing

End systems and routers maintain routing tables

Indicate next router to which datagram should be sent

Static

May contain alternative routes

Dynamic

Flexible response to congestion and errors

Source routing

Source specifies route as sequential list of routers to be followed

Security

Priority

Route recording

Datagram Lifetime

Datagrams could loop indefinitely

Consumes resources

Transport protocol may need upper bound on datagram life

Datagram marked with lifetime

Time To Live field in IP

Once lifetime expires, datagram discarded (not forwarded)

Hop count

Decrement time to live on passing through each router

Time count

Need to know how long since last router

Fragmentation and Re-assembly

Different packet sizes

When to re-assemble

At destination

Results in packets getting smaller as data traverses internet

Intermediate re-assembly

Need large buffers at routers

Buffers may fill with fragments

All fragments must go through same router

Inhibits dynamic routing

IP re-assembles at destination only

Uses fields in header

Data Unit Identifier (ID)

Identifies end system originated datagram

Source and destination address

Protocol layer generating data (e.g. TCP)

Identification supplied by that layer

Data length

Length of user data in octets

Offset

Position of fragment of user data in original datagram

In multiples of 64 bits (8 octets)

More flag

Indicates that this is not the last fragment

Dealing with Failure

Re-assembly may fail if some fragments get lost

Need to detect failure

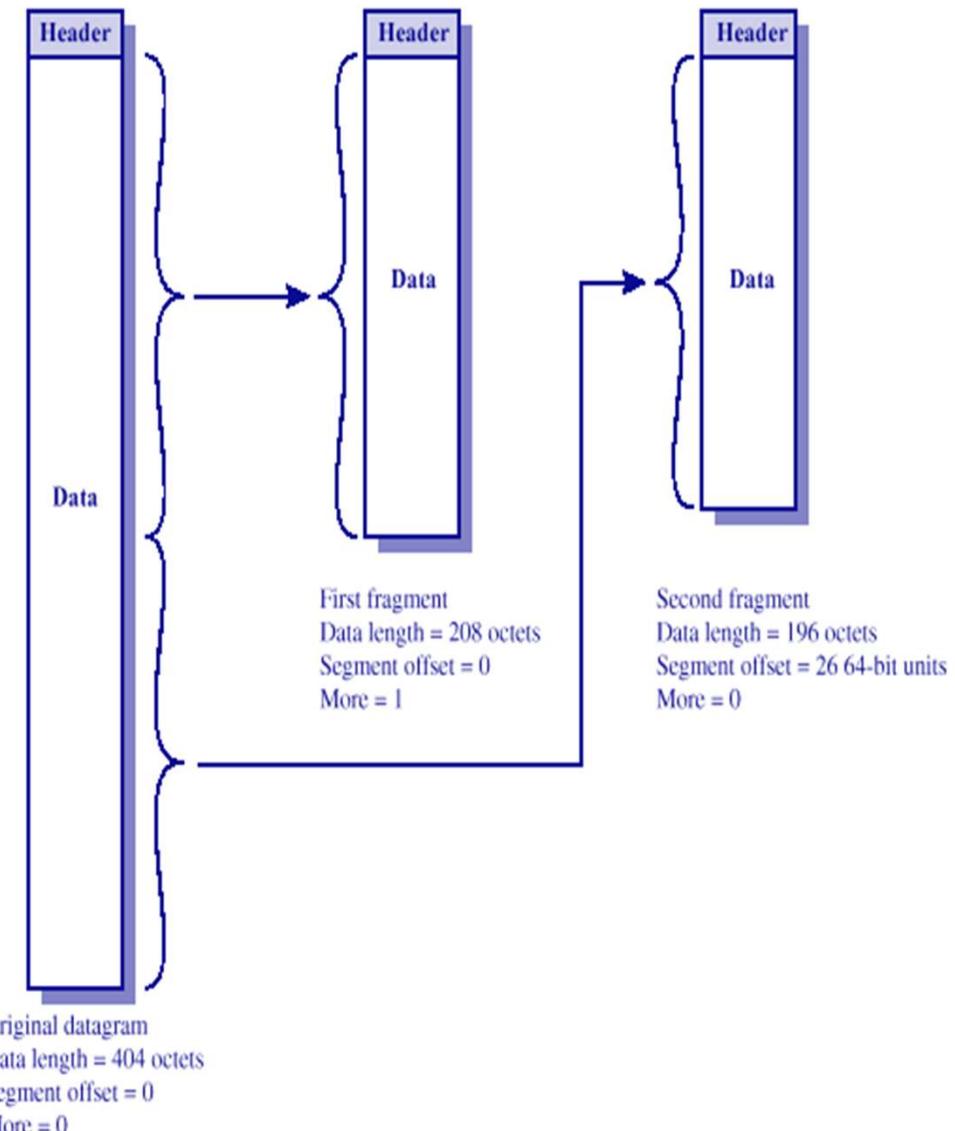
Re-assembly time out

Assigned to first fragment to arrive

If timeout expires before all fragments arrive, discard partial data

Use packet lifetime (time to live in IP)

If time to live runs out, kill partial data



Error Control

Not guaranteed delivery

Router should attempt to inform source if packet discarded

e.g. for time to live expiring

Source may modify transmission strategy

May inform high layer protocol

Datagram identification needed

(Look up ICMP)

Flow Control

Allows routers and/or stations to limit rate of incoming data

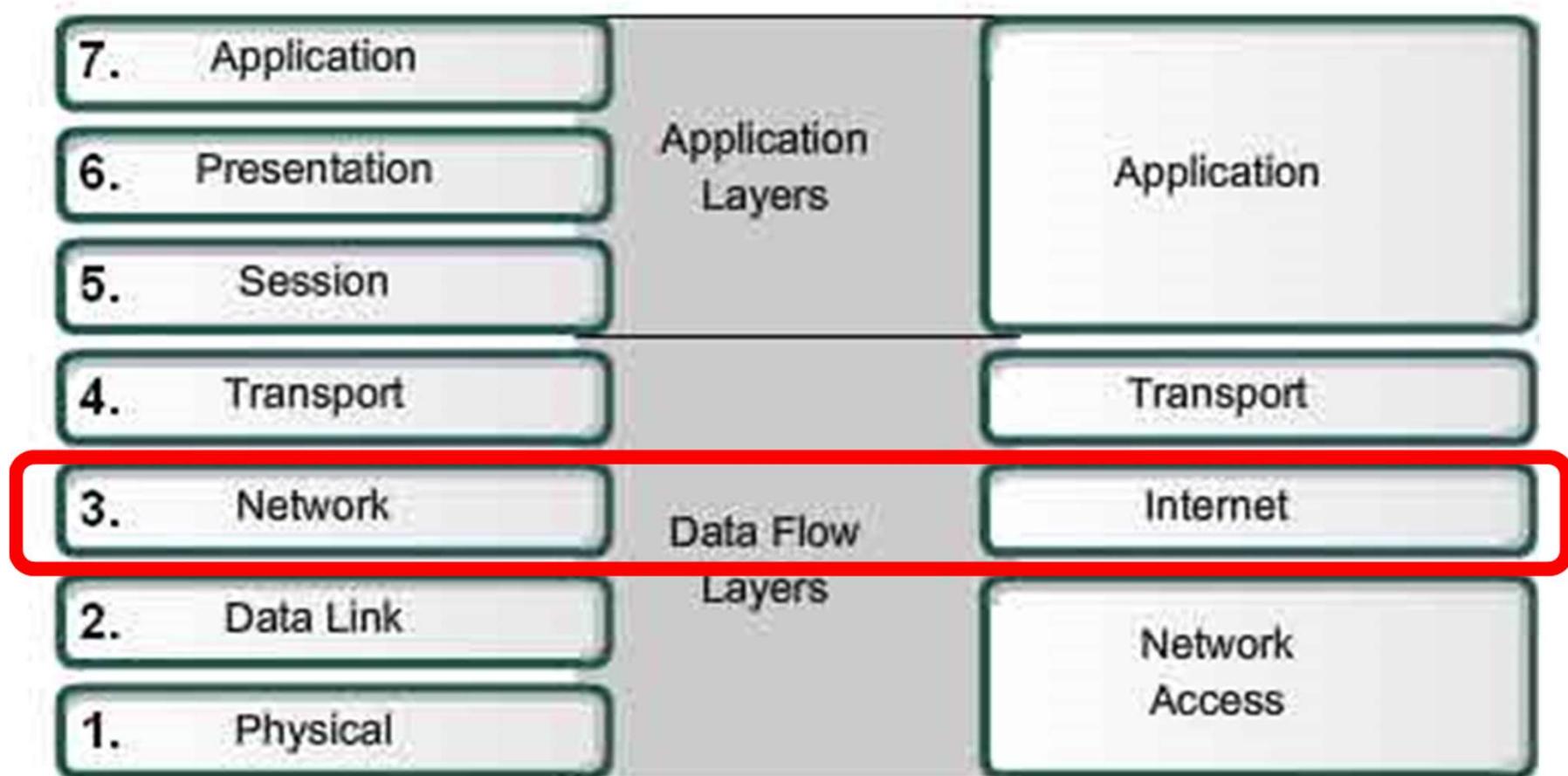
Limited in connectionless systems

Send flow control packets

Requesting reduced flow, e.g. ICMP

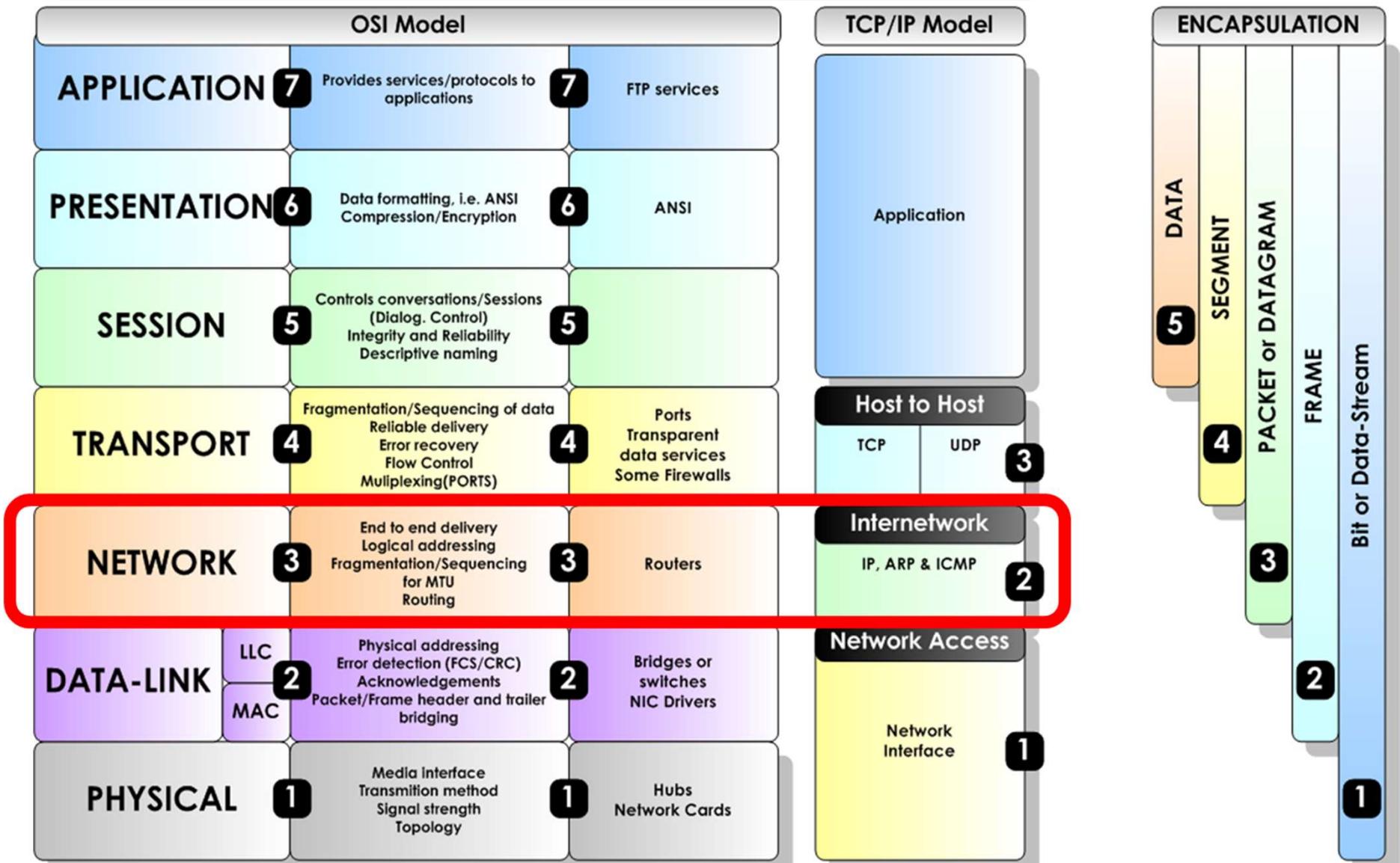
OSI Model

TCP/IP Model



The OSI Model (Open Systems Interconnection)

© Copyright 2008 Steven Iveson
www.networkstuff.eu



Application Level

Network core: routers, network of networks

Network edge: applications and hosts

end systems (hosts):

run application programs

e.g., WWW, email

client/server model:

client host requests, receives service from server

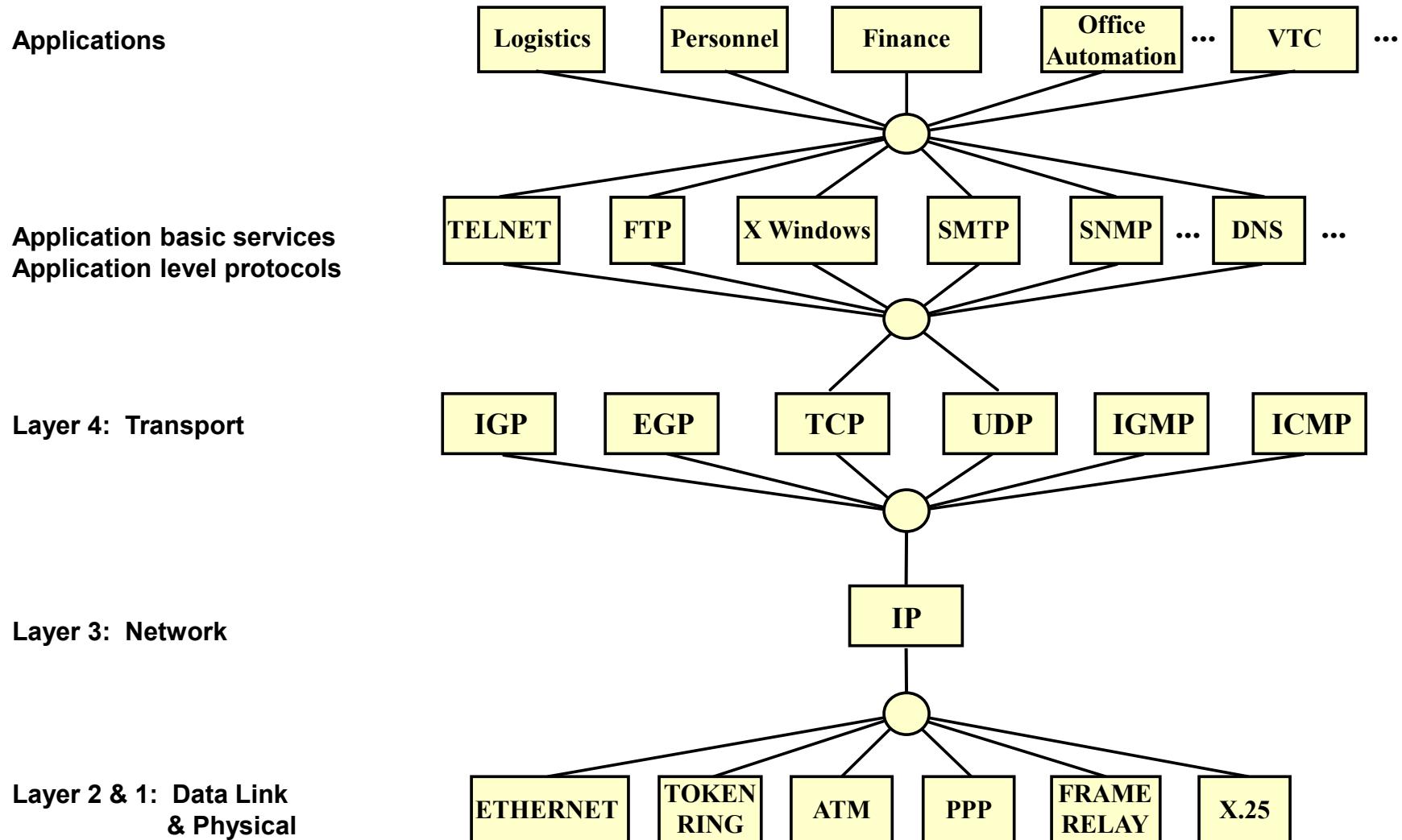
e.g., WWW client (browser)/ server; email client/server

peer-peer model:

host interaction symmetric

e.g.: teleconferencing

Everything over IP & IP over Everything



Internet protocols provide:

- General-purpose facility for reliable data transfer
- Mechanism for contacting hosts

Application-level protocols provide high-level services:

- DNS, Electronic mail, Remote login, FTP, World Wide Web

All of these applications use *client-server* architecture

Application programs

- Use internet protocols to contact other applications
- Application must interact with protocol software *before* contact is made
- *Listening* application informs local protocol software that it is ready to accept incoming messages
- *Connecting* application uses internet protocol to contact listener
- Applications exchange messages through resulting connection
- Provide *user-level* services

Application Level

Enterprise Systems:

- Engineering/Manufacturing Systems
- Business/Office Systems

Application Systems:

- User Interfaces
- Processing Programs
- Databases and files

Application Support Services:

- Client/Server support
- Distributed OS

Application: Transport Service Requirements

Data loss

- some apps (e.g., audio) can tolerate some loss
- other apps (e.g., file transfer, telnet) require 100% reliable data transfer

Timing

- some apps (e.g., Internet telephony, interactive games) require low delay to be “effective”

Bandwidth

- some apps (e.g., multimedia) require minimum amount of bandwidth to be “effective”
- other apps (“elastic apps”) make use of whatever bandwidth they get

Transport Service Requirements of Common Apps

Application	Data loss	Bandwidth	Time Sensitive
file transfer	no loss	elastic	no
e-mail	no loss	elastic	no
Web documents	loss-tolerant	elastic	no
real-time audio/video	loss-tolerant	audio: 5Kb-1Mb video:10Kb-5Mb	yes, 100's msec
stored audio/video	loss-tolerant	same as above	yes, few secs
interactive games	loss-tolerant	few Kbps up	yes, 100's msec
financial apps	no loss	elastic	yes and no

Services Provided by Internet Transport Protocols

TCP service:

- *connection-oriented*: setup required between client, server
- Client establishes connection to server
- Client terminates connection
- *reliable transport* between sending and receiving process
- *flow control*: sender won't overwhelm receiver
- *congestion control*: throttle sender when network overloaded
- *does not providing*: timing, minimum bandwidth guarantees

Some services use both

- DNS

UDP service:

- unreliable data transfer between sending and receiving process
- does not provide: connection setup, reliability, flow control, congestion control, timing, or bandwidth guarantee
- Message must fit in one UDP datagram

Internet Applications: their protocols and transport protocols

Application	Application layer protocol	Underlying transport protocol
e-mail	smtp [RFC 821]	TCP
remote terminal access	telnet [RFC 854]	TCP
Web	http [RFC 2068]	TCP
file transfer	ftp [RFC 959]	TCP
streaming multimedia	proprietary (e.g. RealNetworks)	TCP or UDP
remote file server	NFS	TCP or UDP
Internet telephony	proprietary (e.g., Vocaltec)	typically UDP

Traditional Distributed Applications

Those based on Internet: distributed applications

Have the following features:

Application logic

Application protocol support code

Example: The X protocol for transmitting graphical images

Transport interface code

Makes the appropriate network calls to send and receive the messages that make up the application protocol over a specific network transport

Usually divided into transport-independent and transport-dependent parts

Middleware provides transparency of the transport interface code

Software between application programs and OS/network.

Provides a set of higher-level distributed computing capabilities and a set of standards-based interfaces.

Interfaces allow applications to be distributed and to take advantage of other services provided over the network.

Middleware can be viewed as a set of (transport) services that are accessible to application programmers through an API (Application Programming Interface)

Example: Sockets, RPC.

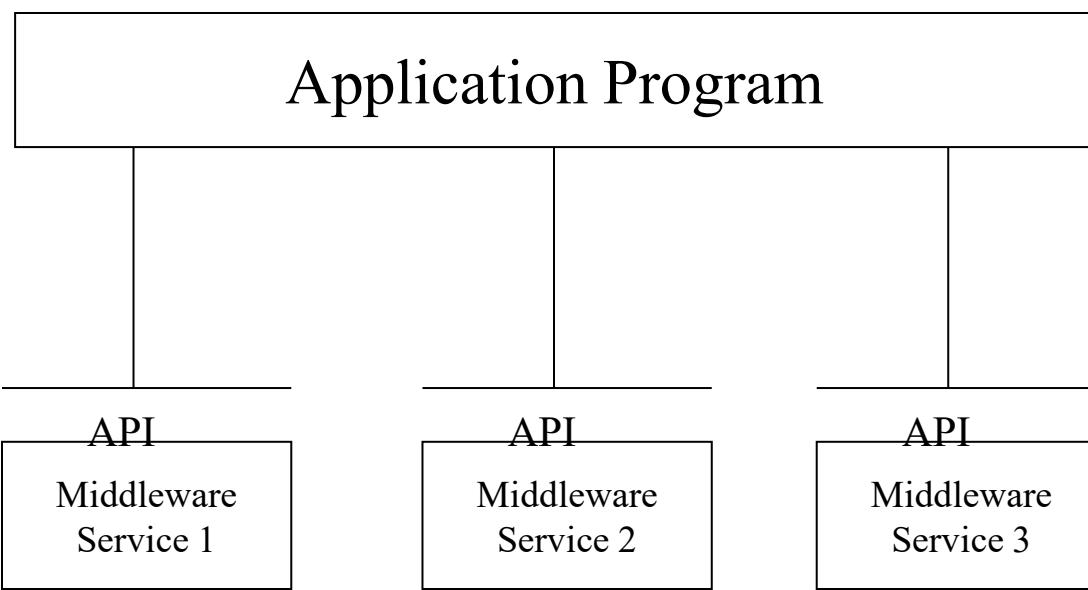
API: Application Programming Interface

Defines interface between application and transport layer

Socket API: specific Internet API

Two processes communicate by sending data into socket, reading data out of socket

- Defined by programming/operating system
- Includes collection of procedures for application program
- Protocols do not typically specify API
- API defined by programming system
- Allows greatest flexibility - compatibility with different programming systems
- Originated with Berkeley BSD UNIX, also available on Windows and other operating systems

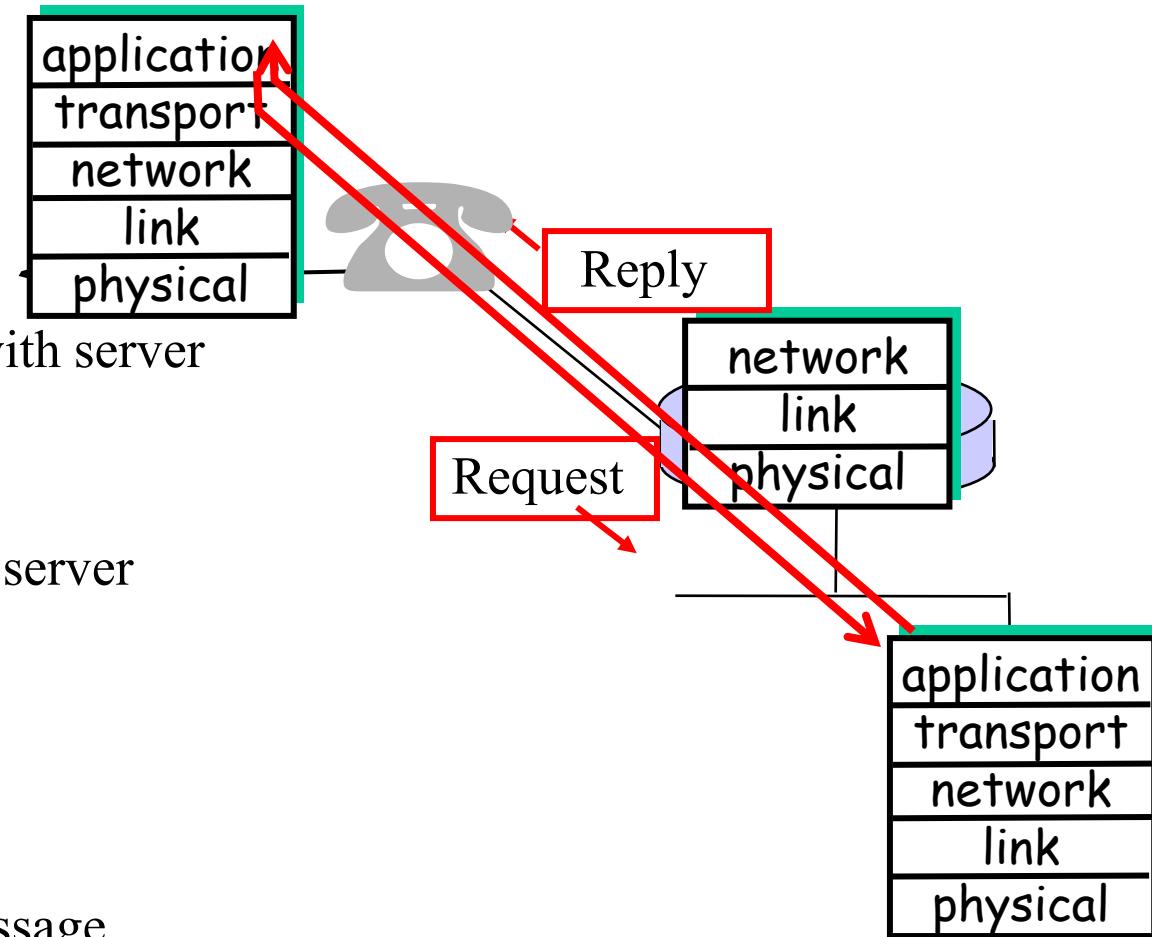


Client-server model

Typical network application has two pieces: *client* and *server*

Client application

- initiates contact (connection) with server (“speaks first”)
- Sends message to server
- typically requests service from server
- e.g.: request WWW page
- Waits for return message



Server application is “listener”

- Waits for incoming message
- Performs service
- Returns results
- e.g., sends requested WWW page.

Domain Name System

The **Domain Name System** (DNS) provides translation between symbolic names for IP hosts and their IP addresses

- People: use many identifiers: name, Passport #, ...

- Internet hosts:

- IP address (32 bit) - used for addressing in IP datagrams
- “name”, e.g., www.iitb.eirnet.ie - used by humans

Provides logical hierarchical view of the Internet

- DNS: globally *distributed database* implemented in hierarchy of many *name servers*

Functioning:

- application-layer protocol* to communicate to *resolve* names (address/name translation): application calls *resolver*

- A client/server interaction

- clients: query servers to resolve names (*nslookup* function)

- servers: run name server daemons, reply to queries (*bind, named*)

- gethostbyname*: UNIX based resolver library call that can be invoked from an application program

DNS: Example

Host named: xyz.iitb.ronet.ro wants IP address of web server: www.ibm.com

Resolver Steps:

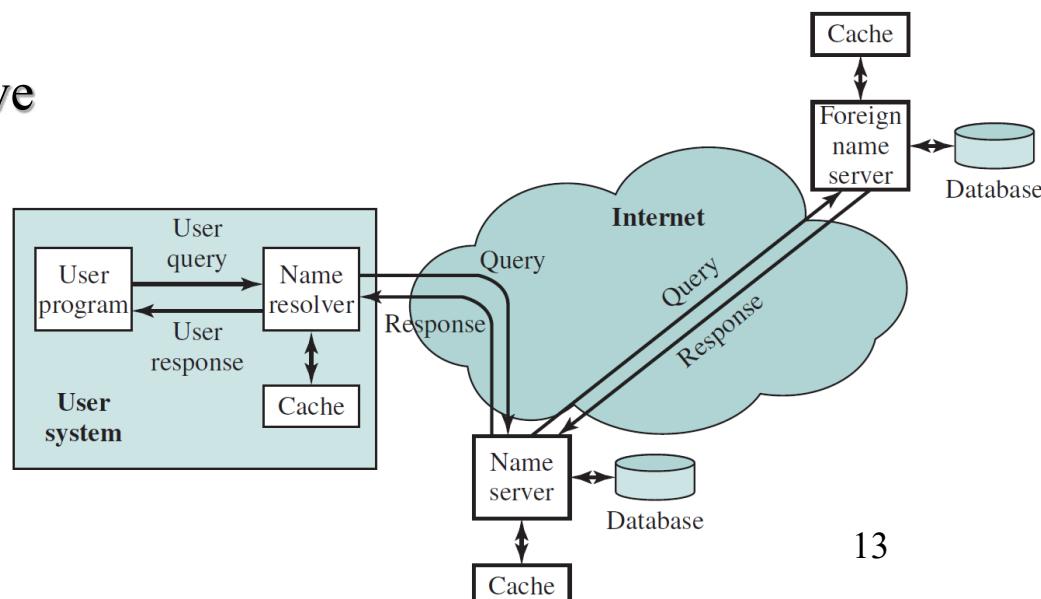
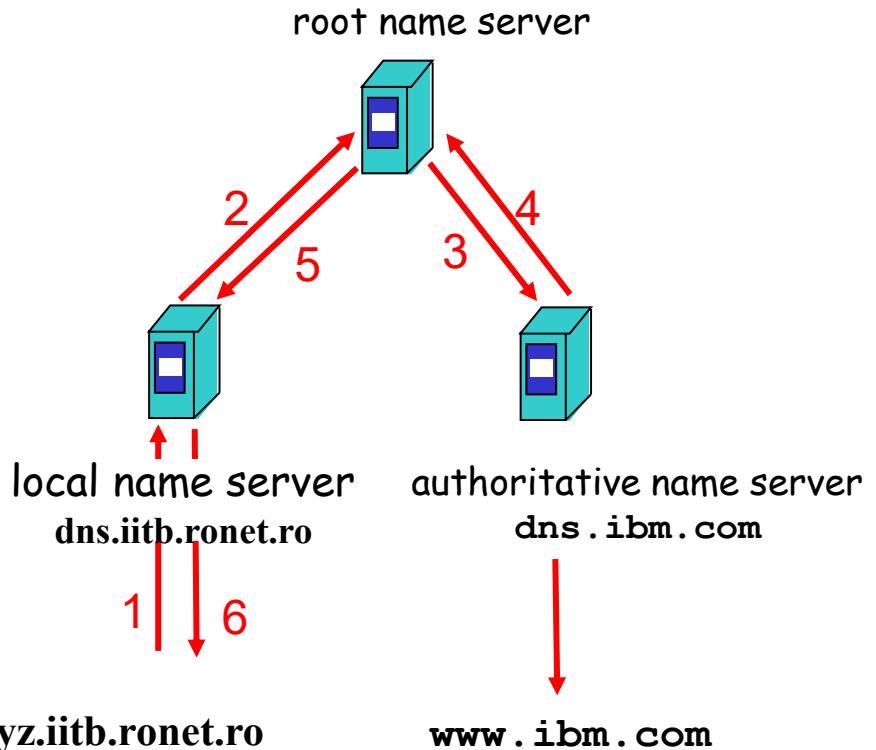
1. After checking locally, contacts its **local DNS server**:

dns.iitb.ronet.ro

2. dns.iitb.ronet.ro contacts **root name server**, if necessary

3. root name server contacts **authoritative name server** (responsible server):
dns.ibm.com, if necessary

4,5,6 Return of info



DNS Name Servers

Centralized DNS?

- single point of failure
- traffic volume
- distant centralized database
- maintenance
- doesn't *scale!*

Distributed DNS:

- no server has all name-to-IP address mappings

Local Name Servers:

- each organization/ISP has *local (default) name server*
- host DNS query first goes to local name server

Authoritative Name Server:

- for a host: stores that host's IP address & name
- can perform name/address translation for that host's name

Root Name Server:

contacts authoritative name server if name mapping not known

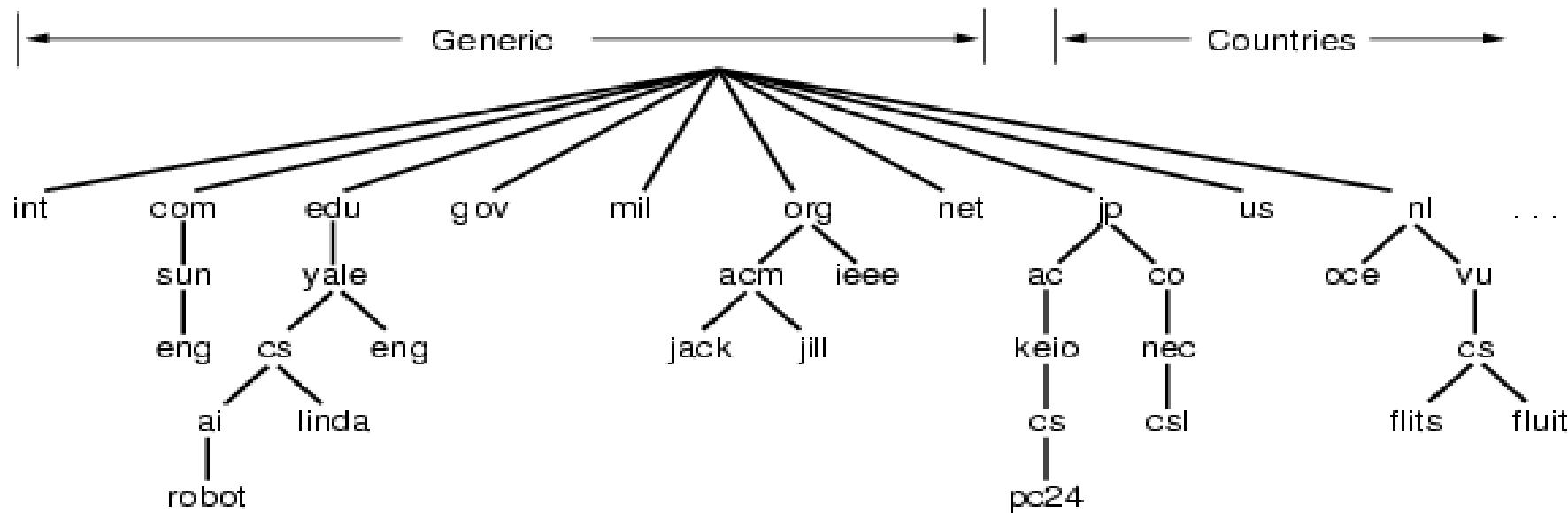
gets mapping

returns mapping to local name server

Several root name servers worldwide

Structure of DNS names

- Each name consists of a sequence of alphanumeric components separated by periods; domain names are case insensitive; each component name up to 63 characters long, entire path up to 255 characters
- Examples: www.eg.bucknell.edu www.netbook.cs.purdue.edu
charcoal.eg.bucknell.edu
- Names are hierarchical, with most-significant component on the right
- Left-most component is the computer name



A portion of the Internet domain name space.

DNS naming structure

Top level domains (right-most components; also known as *TLDs*) defined by global authority (only Internet authority, what will be for the future?)

com Commercial organization

edu Educational institution

gov Government organization

mil Military organization

Organizations apply for names in a top-level domain:

bucknell.edu macdonalds.com

Organizations determine own internal structure

csis.ul.ie cs.purdue.edu

Geographic structure

Top-level domains are US-centric (e.g., [cs.yale.edu](#) could be accessed as [cs.yale.ct.us](#)), each organization in US is under a generic domain

Geographic TLDs are used for organizations in other countries:

TLD	Country
-----	---------

.uk	United Kingdom
-----	----------------

.fr	France
-----	--------

.ch	Switzerland
-----	-------------

.ie	Ireland
-----	---------

Countries define their own internal hierarchy: [ac.uk](#) and [edu.au](#) are used for academic organizations in the United Kingdom and Australia; [ac.uk](#) or [co.uk](#) are mirrors for [.edu](#) or [.com](#)

Romania makes not (yet) that distinction, all organizations are under [.ro](#)

Choosing DNS server architecture

- Small organizations can use a single DNS server
 - Easy to administer
 - Inexpensive
- Large organizations often use multiple servers
 - Reliability through redundancy
 - Improved response time through load-sharing
 - Delegation of naming authority
- Locality of reference applies - users will most often look up names of computers within same organization

Domain names within an organization

Organizations can create any internal DNS hierarchy

- Uniqueness of TLD and organization name guarantee uniqueness of any internal name (much like file names in your directories)
- All but the left-most component of a domain name, is called the *domain* for that name:

Name	Domain
www.netbook.cs.purdue.edu	netbook.cs.purdue.edu
regulus.eg.bucknell.edu	eg.bucknell.edu
coral.bucknell.edu	bucknell.edu

Authority for creating new *subdomains* is delegated to each domain

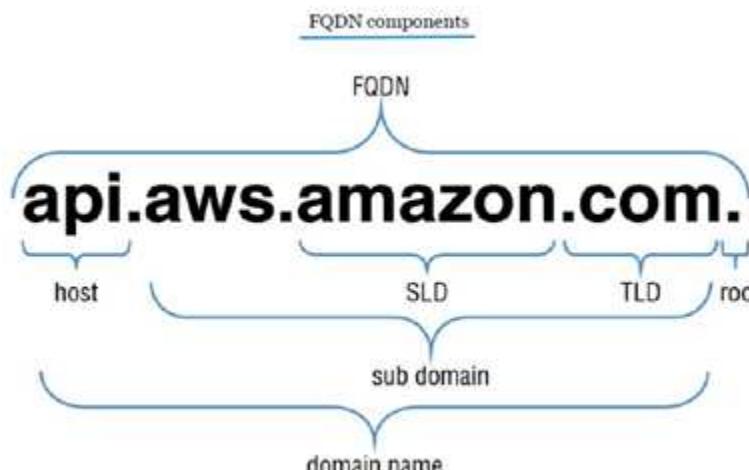
- Administrator of bucknell.edu has authority to create eg.bucknell.edu and need not contact any central naming authority

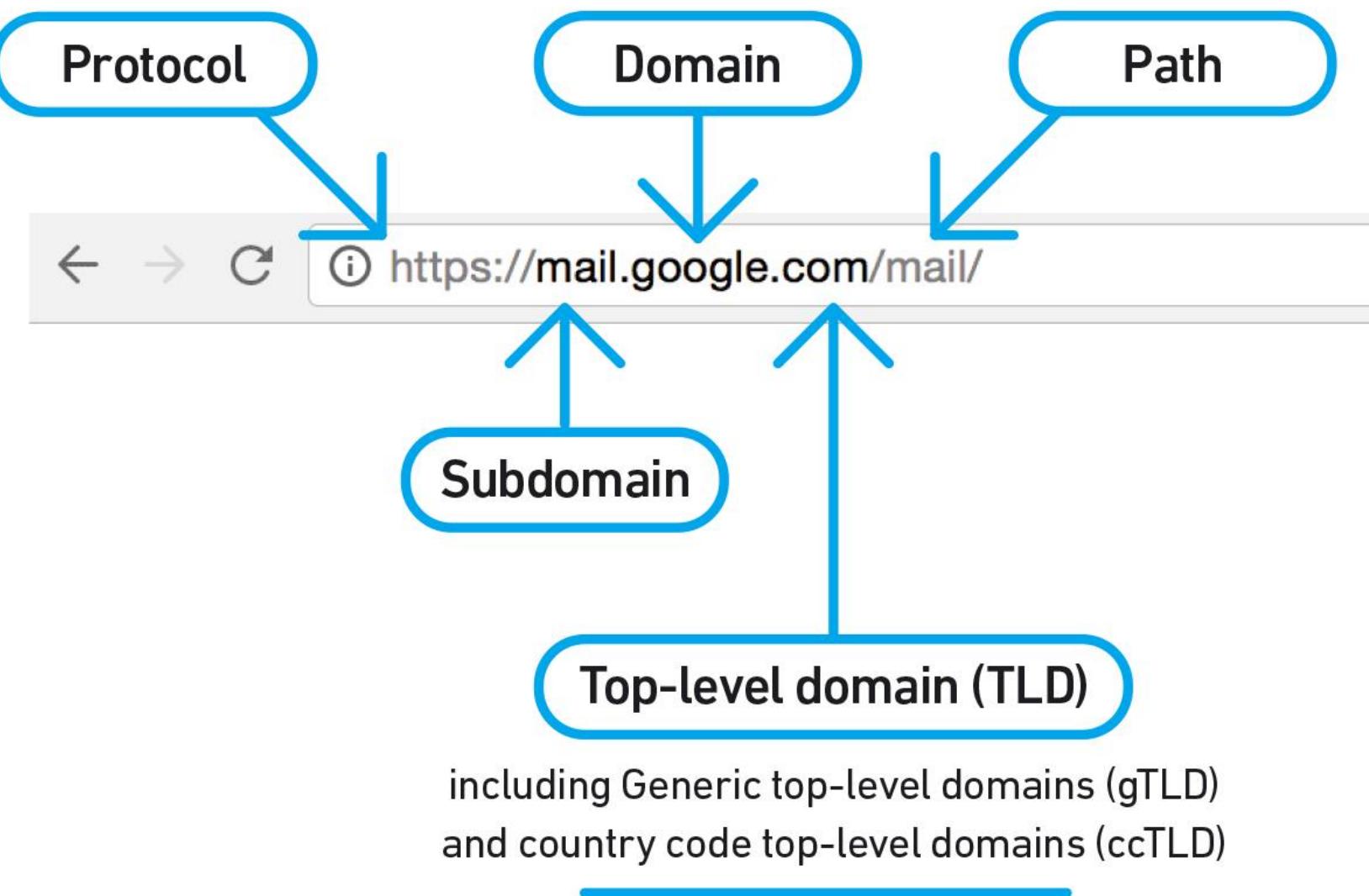
DNS names and physical location

- DNS domains are logical concepts and need not correspond to physical location of organizations
- DNS domain for an organization can span multiple networks
 - [utcluj.ro](#) covers all networks at UTCN
 - [cs.utcluj.ro](#) all from Computer Science department
 - [laptop.cs.utcluj.ro](#) could be connected to a network in ... California

Abbreviations

- May be convenient to use abbreviations for local computers; e.g. [coral](#) for [coral.bucknell.edu](#)
- Abbreviations are handled in the *resolver*; DNS servers only know *full-qualified domain names* (FQDNs)
- Local resolver is configured with list of suffixes to append
- Suffixes are tried sequentially until match found





DNS: Name Resolution

Root name server:

- may not know authoritative name server
- may know *intermediate name server* to contact to find authoritative name server
- Two ways of action:

Recursive queries:

- puts burden of name resolution on contacted name server (each server, having not requested information, goes & finds it, reporting back)
- not scalable under heavy load

Iterated queries:

- contacted server replies only with the name of next server to contact

DNS: Name Resolution (continued)

- Resolver software typically available as library procedures
 - Implement DNS application protocol
 - Configured for local servers
 - Example - UNIX *gethostbyname*
- Calling program is *client*
 - Constructs DNS protocol message - a *DNS request*
 - Sends message to local DNS server
- DNS *server* resolves name
 - Constructs DNS protocol message - a *DNS reply*
 - Sends message to client program and waits for next request

DNS: Database

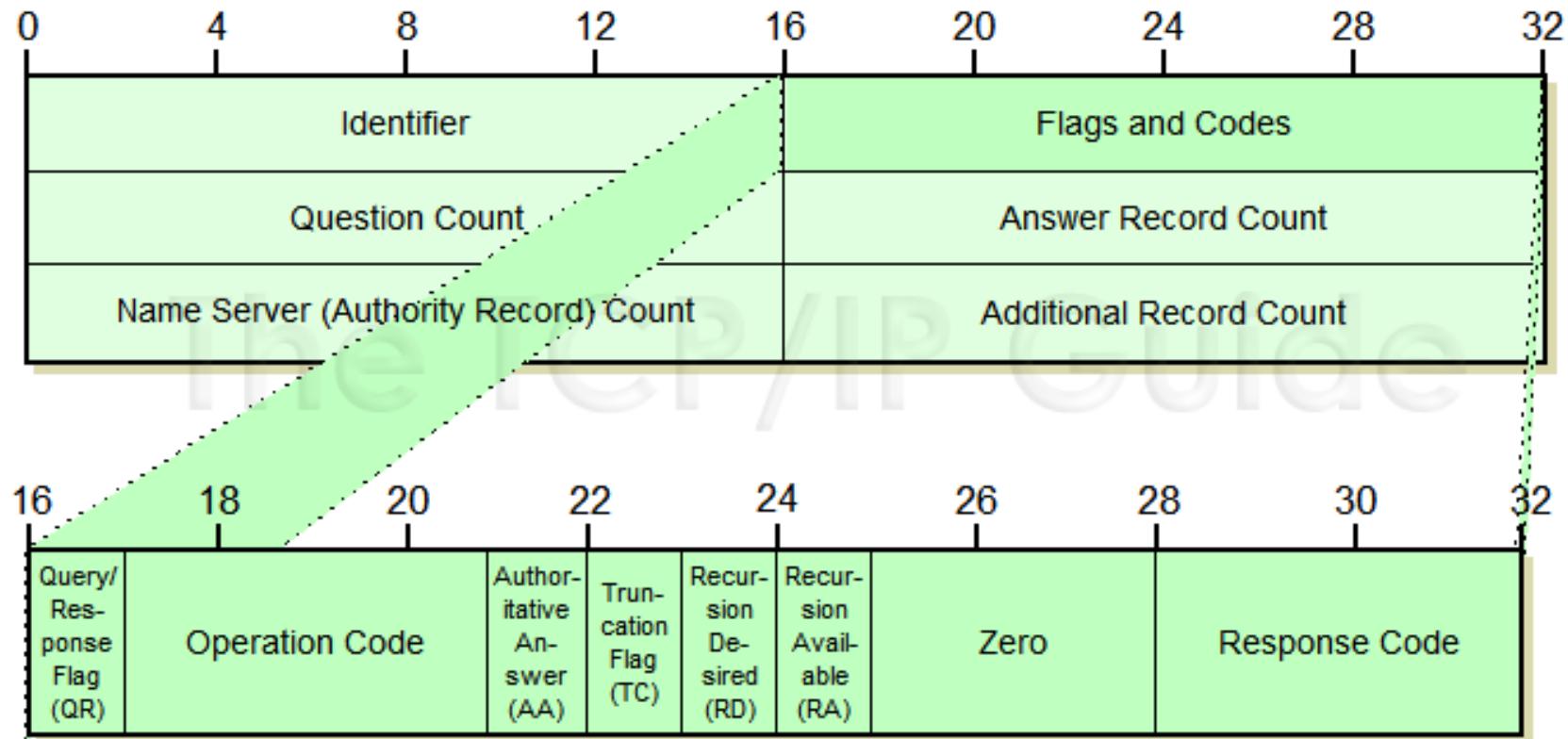
- Contains:
 - ***resource records (RRs)*** that include the name, IP address, and other information about hosts
- Key features:
 - *Variable-depth hierarchy for names*: DNS allows essentially unlimited levels and uses the period (.) as the level delimiter in printed names
 - *Distribution controlled by the database*: DNS database is divided into thousands of separately managed zones, which are managed by separate administrators. The database software controls distribution and update of records.

Type	Description
A	A host address. This RR type maps the name of a system to its IPv4 address. Some systems (e.g., routers) have multiple addresses, and there is a separate RR for each.
AAAA	Similar to A type, but for IPv6 addresses.
CNAME	Canonical name. Specifies an alias name for a host and maps this to the canonical (true) name.
HINFO	Host information. Designates the processor and operating system used by the host.
MINFO	Mailbox or mail list information. Maps a mailbox or mail list name to a host name.
MX	Mail exchange. Identifies the system(s) via which mail to the queried domain name should be relayed.
NS	Authoritative name server for this domain.
PTR	Domain name pointer. Points to another part of the domain name space.
SOA	Start of a zone of authority (which part of naming hierarchy is implemented). Includes parameters related to this zone.
SRV	For a given service, provides name of server or servers in domain that provide that service.
TXT	Arbitrary text. Provides a way to add text comments to the database.
WKS	Well-known services. May list the application services available at this host.

DNS messages (main idea)

DNS request contains name to be resolved

DNS reply contains IP address for the name in the request



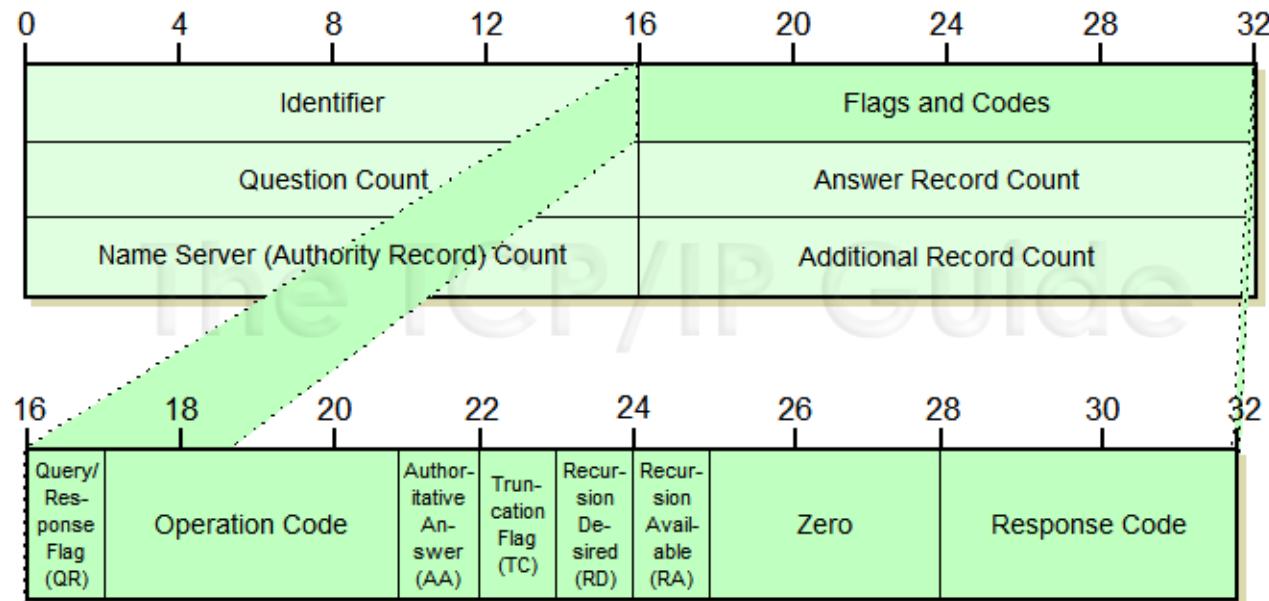
Identifier: A 16-bit identification field generated by the device that creates the DNS query. It is copied by the server into the response, so it can be used by that device to match that query to the corresponding reply received from a DNS server.

Question Count: Specifies the number of questions in the *Question* section of the message.

Answer Record Count: Specifies the number of resource records in the *Answer* section of the message.

Authority Record Count: Specifies the number of resource records in the *Authority* section of the message

Additional Record Count: Specifies the number of resource records in the *Additional* section of the message.



Email – Electronic Mail

Electronic mail paradigm

Heavily used application on any network

Electronic version of paper-based office memo

Quick, low-overhead written communication

Dates back to time-sharing systems, in 1960s

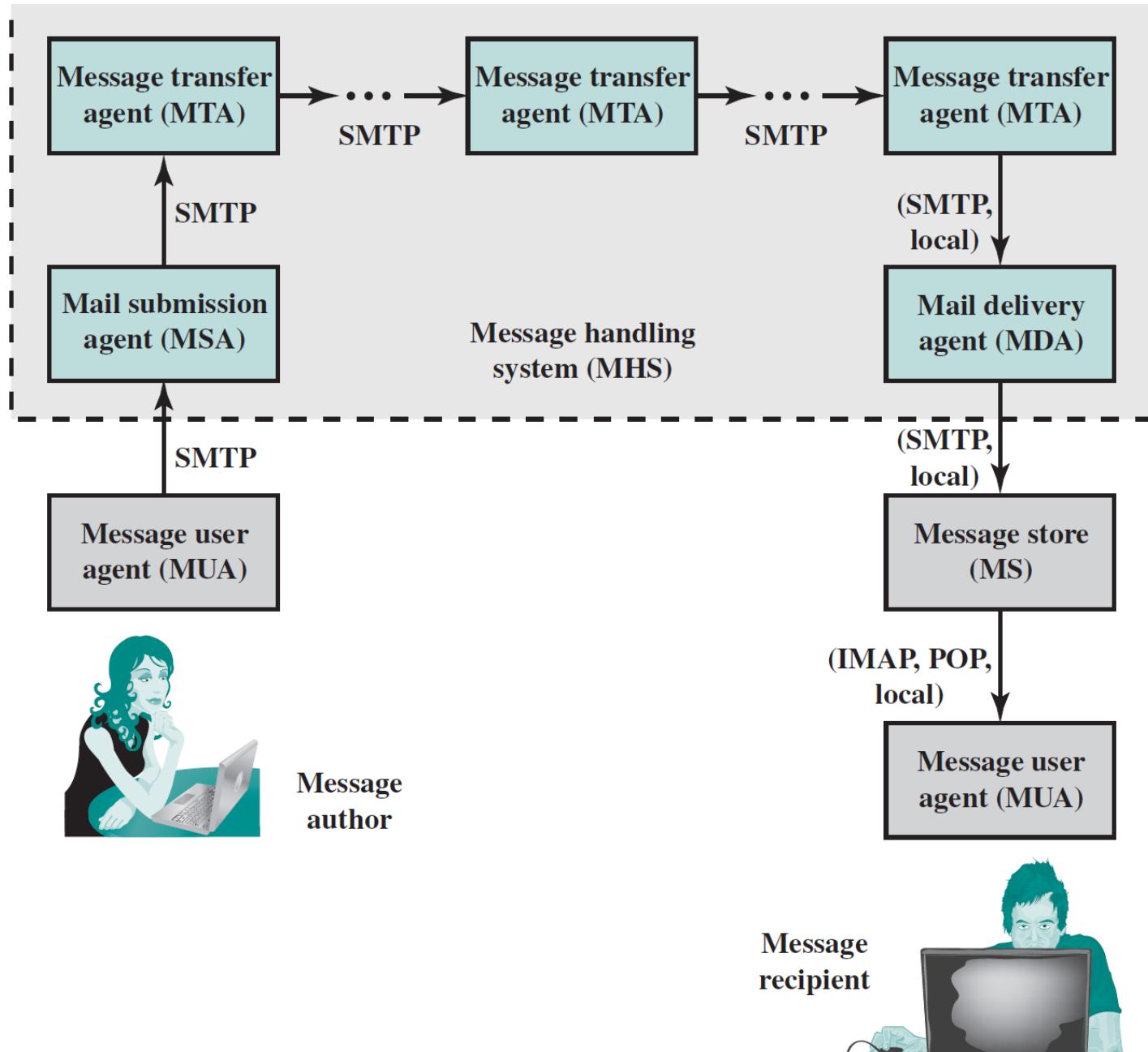
Because e-mail is encoded in an electronic medium, new forms of interaction are possible

Automatic processing - sorting, reply

Can carry other content: if basic **Simple Mail Transfer Protocol** (SMTP), based on TCP/IP, was delivering only simple text messages, by use of **Multi-purpose Internet Mail Extension** (MIME) now have delivery of other types of data (voice, images, video clips,...)

History: first standard: CCITT X.400 - too complex; base for OSI's MOTIS application; replaced by TCP/IP based standards RFC 821(transmission protocol), and RFC 822 (message format)

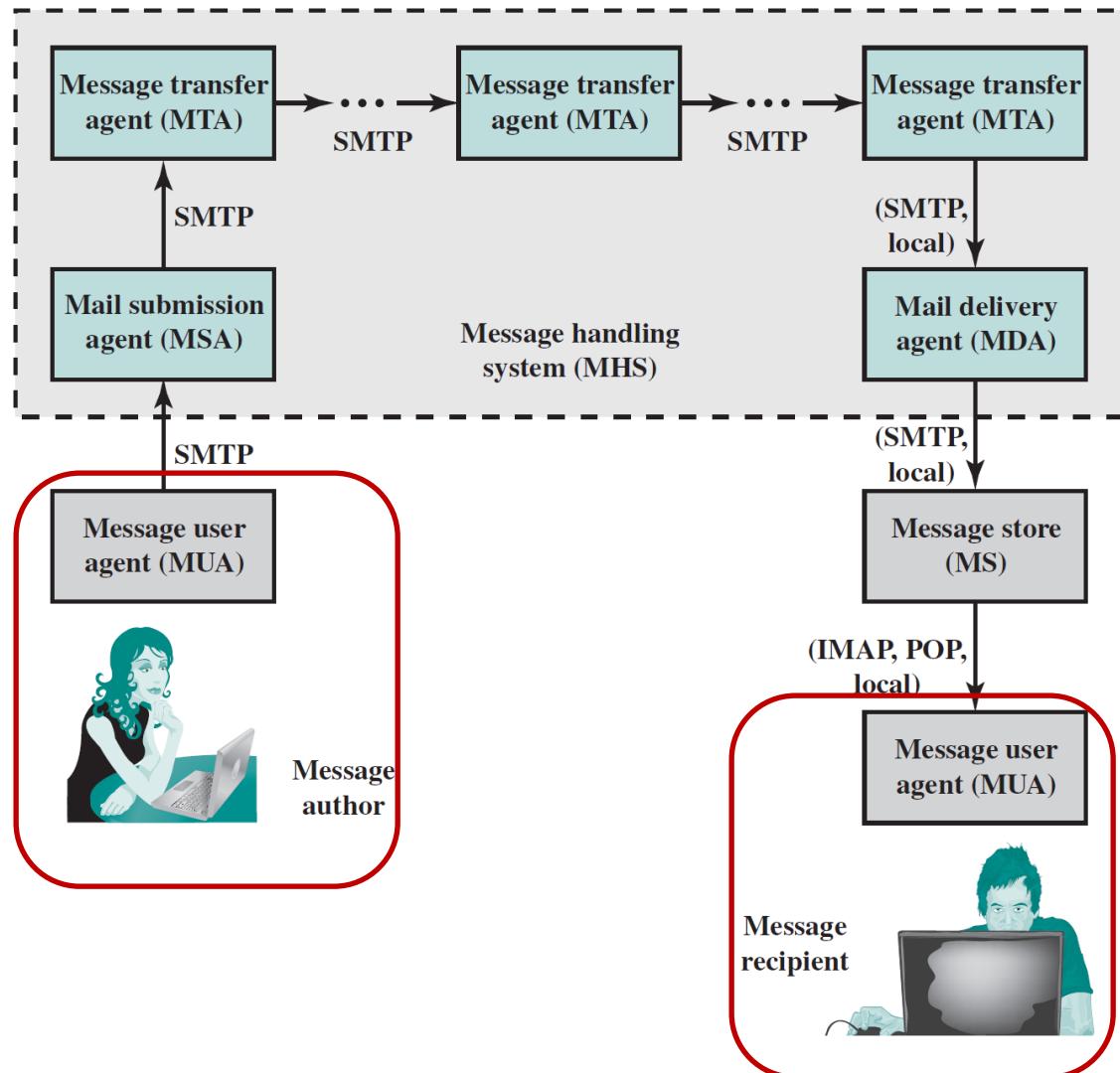
Email Architecture RFC 5598 (*Internet Mail Architecture*)



Email Architecture - components

Message User Agent (MUA)

- on behalf of user actors and user applications
- client e-mail program or a local network e-mail server
- sender MUA: formats a message and performs initial submission into the MHS via an MSA
- receiver MUA: processes receive mail for storage and/or display
- Thunderbird, Outlook, Opera Mail, Mailbird, etc



Email Architecture - components

Message Handling Service (MHS)

Mail Submission Agent (MSA) – component of MTA

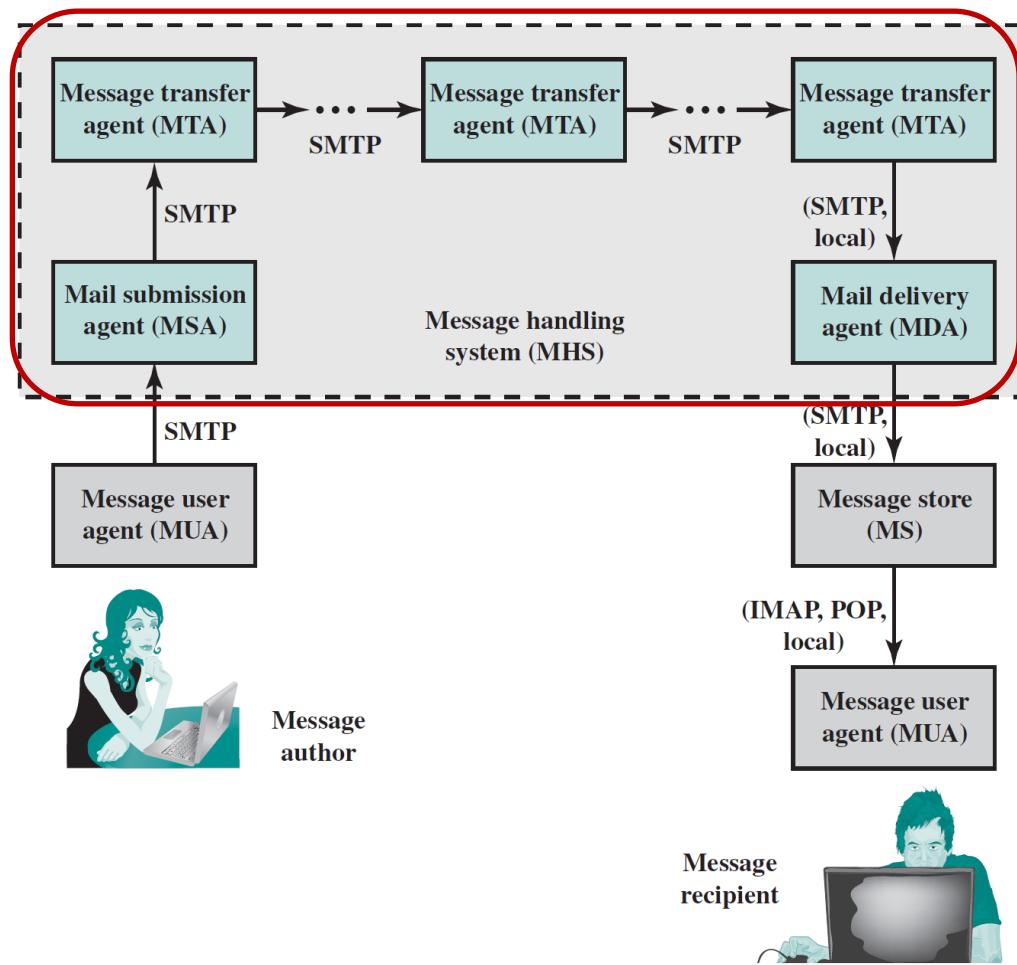
- accepts messages from MUA
- enforces the policies of the hosting domain and the requirements of Internet standards
- Simple Mail Transfer Protocol (SMTP) is used between the MUA and the MSA.

Message Transfer Agent (MTA)

- Relays mail for one application-level hop
- SMTP is used between MTAs
- client: the sending mail server, server: receiving mail server

Mail Delivery Agent (MDA) – component of MTA

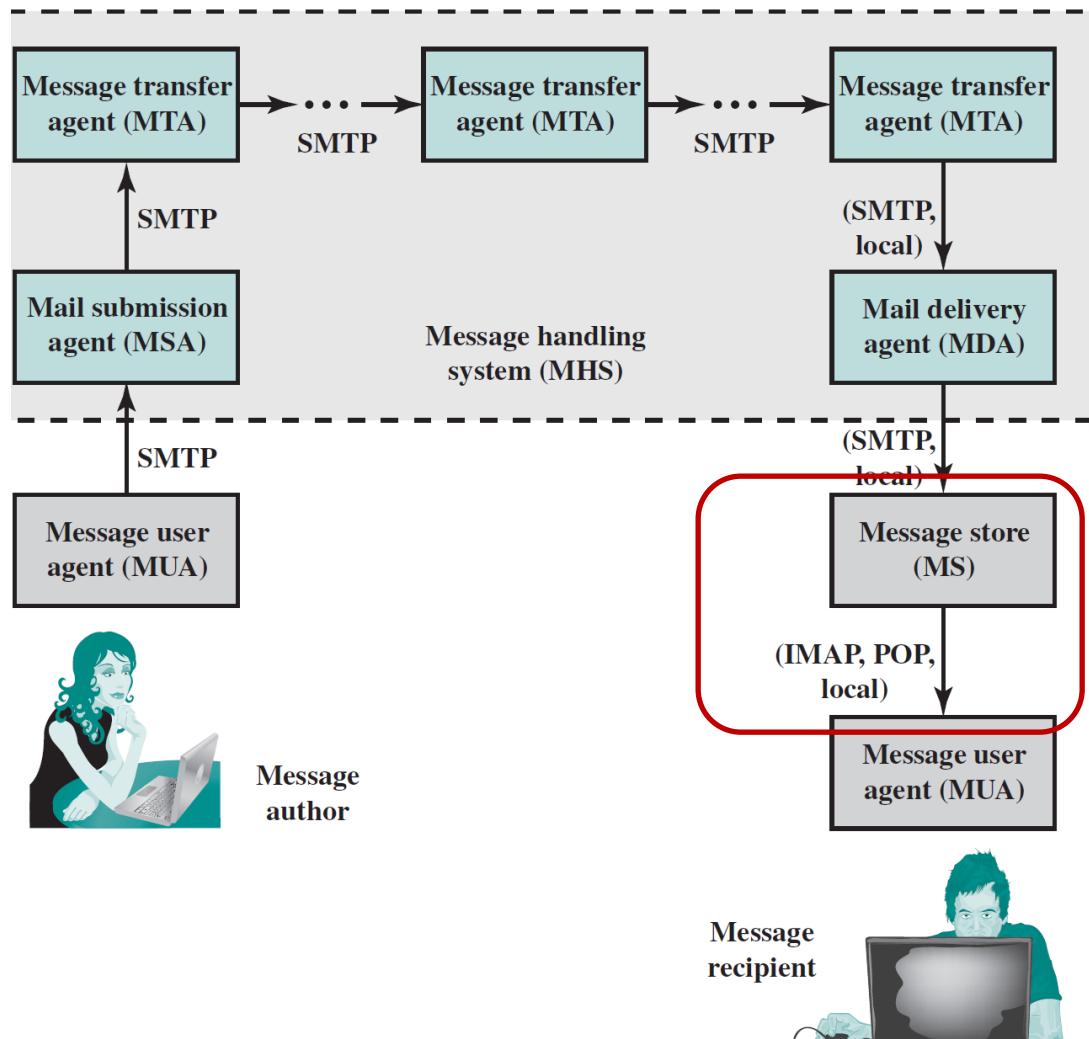
- transfers messages from the MHS to the MS



Email Architecture - components

Message Store (MS)

- located on a remote server or on the same machine as the MUA
- retrieve message from remote server using:
 - POP (Post Office Protocol) or IMAP (Internet Message Access Protocol).



Post Office Protocol (POP) and Internet Message Access Protocol (IMAP)

Role: message user agent (MUA) retrieves mail from message store (MS)

POP version 3 - RFC 1939; connection to server using TCP on port 110

- *Authentication state*: user ID/password or more sophisticated methods
- *Transaction state*: the client can access the mailbox to retrieve and delete messages
- *Update state*: the server passes all of the changes requested by the client's commands and then closes the connection

IMAP version 4 - RFC 3501; connection to server using TCP on port 143 or 993 over SSL

provides more functionality than POP3

Clients can:

- have multiple remote mailboxes
- specify criteria for downloading messages
- make changes both when connected and when disconnected (periodic re-synchronization)
- IMAP *always* keeps messages on the server and replicates copies to the clients

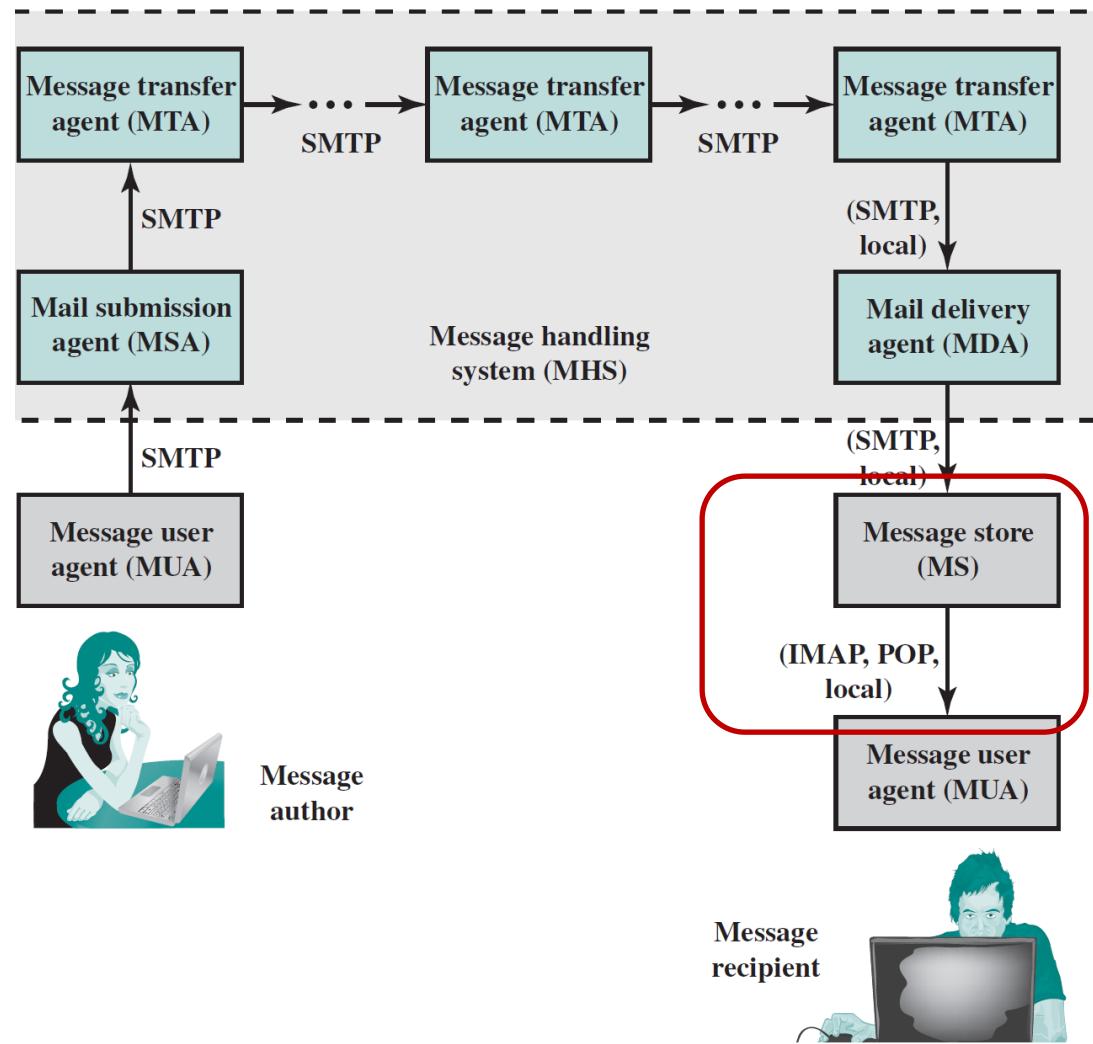
Email Architecture - components

Other components

Internet e-mail provider named also
Administrative management
domain (ADMD)

—examples:

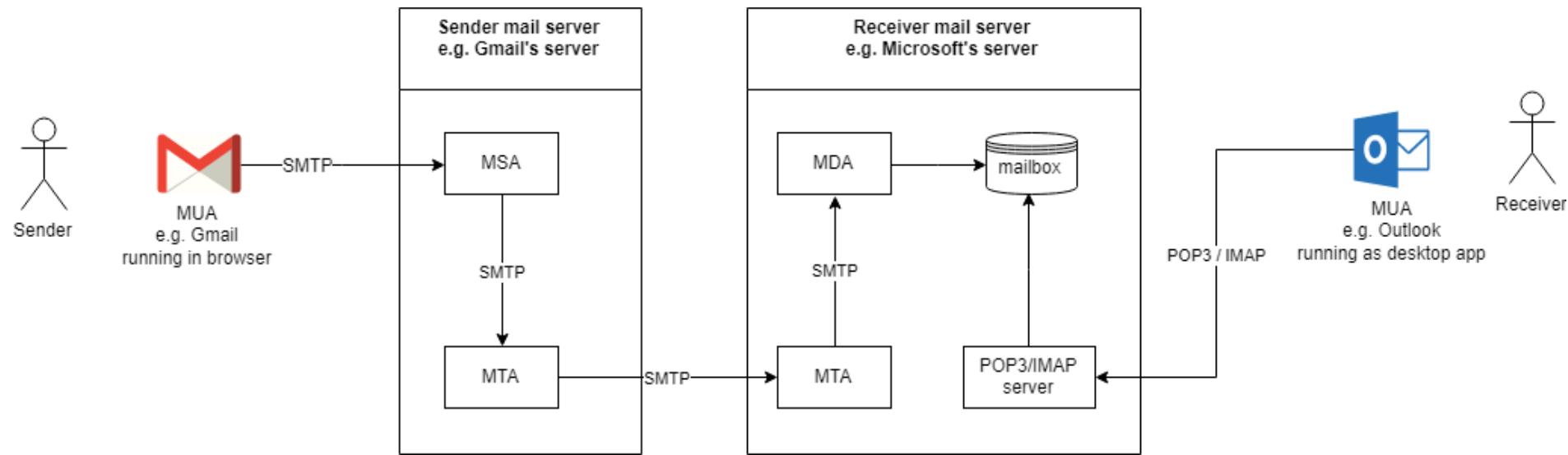
- IT department that operates a mail relay (local or enterprise)
- an ISP that operates a public shared e-mail service



Domain name system (DNS)

Example

- From Gmail user to Microsoft user
 - *also, security (Public key infrastructure)*



<https://afreshcloud.com/sysadmin/mail-terminology-mta-mua-msa-mdm-smtp-dkim-spf-dmarc>

Example – steps to send an email to *Firstname.Lastname@cs.utcluj.ro*

- Sender Message User Agent (MUA): web-based email interface (gmail)
- Mail Submission Agent (MSA): get message from MUA and sends it to MTA via SMTP
- Sender Message Transfer Agent (MTA): query MX record for *cs.utcluj.ro*
 - DNS 'mail exchange' (MX) record -> directs email to a mail server (see example below for a *nslookup of MX type*)

```
C:\Users\B>nslookup
Default Server: ro-cj01a-dns01.upcnet.ro
Address: 78.96.7.88

> set type=mx
> cs.utcluj.ro
Server: ro-cj01a-dns01.upcnet.ro
Address: 78.96.7.88

Non-authoritative answer:
cs.utcluj.ro      MX preference = 20, mail exchanger = mail.utcluj.ro
>
```

- Receiver Message Transfer Agent (MTA): responsible for *mail.utcluj.ro*
- Mail Delivery Agent (MDA): puts the email in the receiver's inbox
(Firstname.Lastname@cs.utcluj.ro vs localname@mail.utcluj.ro)
- Receiver Message User Agent (MUA): receiver's outlook client (configured for utcluj email / web interface - *intranet.utcluj.ro*)

Mailbox: Electronic mailbox

E-mail users have an *electronic mailbox* into which incoming mail is deposited; identified by an *e-mail address*

User then accesses mail with a mail reader program

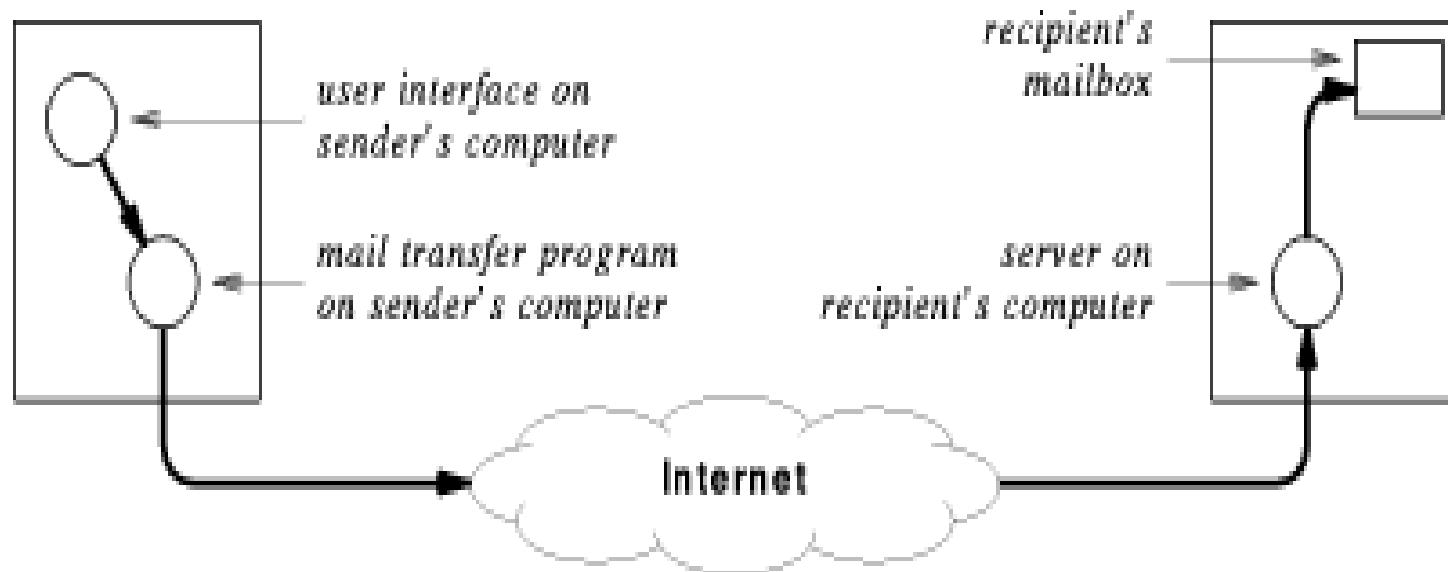
Usually associated with computer account (user's account ID); one user may have different electronic mailboxes

On networked multi-user computer, need to identify computer as well as *mailbox* :
e-mail address is composed of computer name and mailbox name

Mail transfer

- E-mail communication is really a two-part process:
 - User composes mail with an *e-mail interface* program
 - *Mail transfer* program delivers mail to destination
 - Waits for mail to be placed in outgoing message queues
 - Picks up message and determines recipient(s)
 - Becomes *client* and contacts *server* on recipient's computer
 - Passes message to server for delivery

Mail Transfer Illustration



Simple Mail Transfer Protocol (SMTP) is the standard application protocol for delivery of mail from source to destination (RFC 821)

- Provides reliable delivery of messages
- Uses TCP well-known port 25 for message exchange between client and server
- Command/Response interaction:
 - commands:** ASCII text (message character set as 7-bit ASCII)
 - response:** status code and phrase

Other functions:

E-mail address lookup & address verification

General characteristics

Three phases of transfer: handshaking, mail transfer, closure

Attempts to provide reliable service

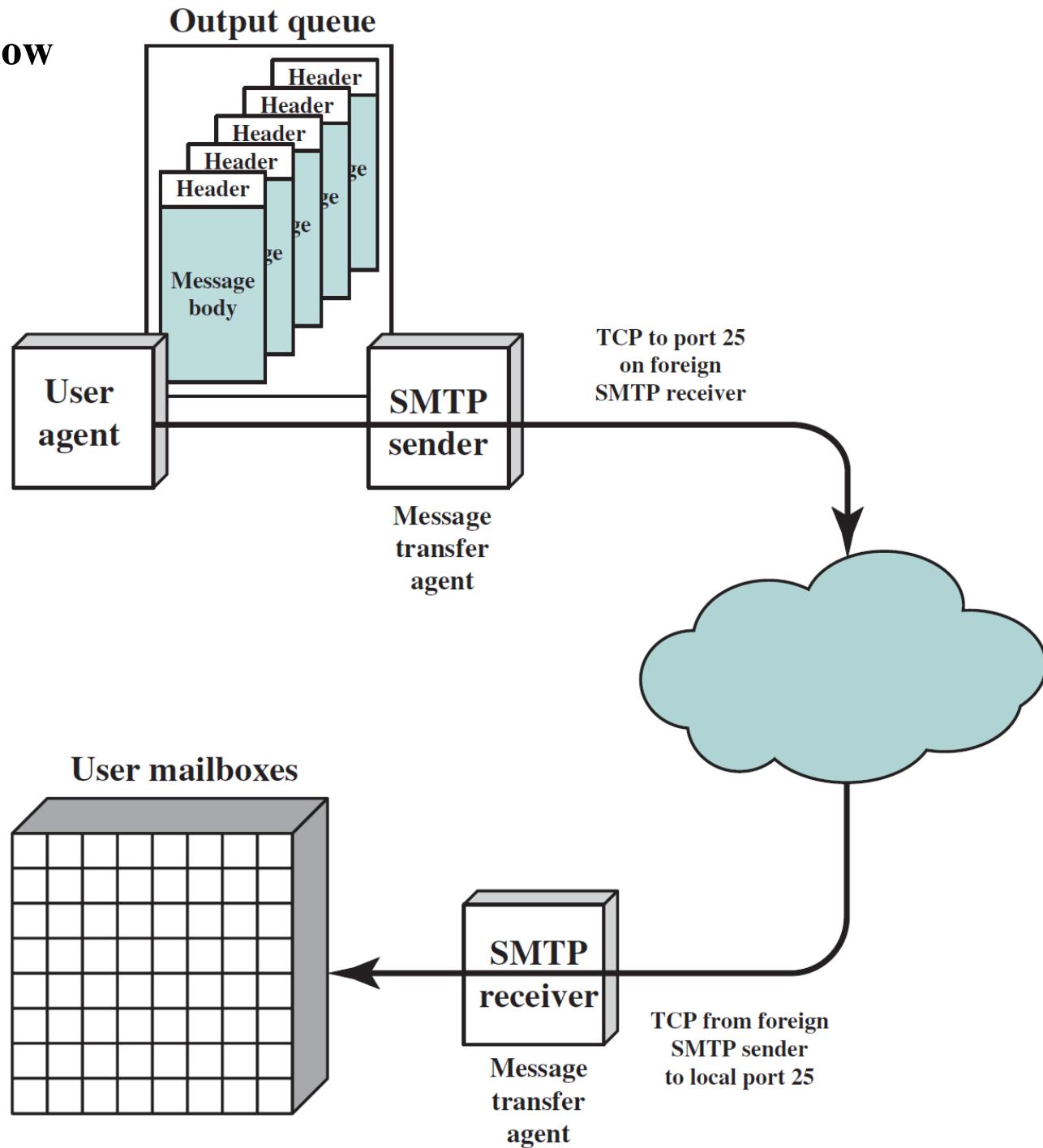
No guarantee to recover lost messages

No end to end acknowledgement to originator

Error indication delivery not guaranteed

Generally considered reliable!

SMTP Mail Flow



Mail Message Contents

Each queued message has in composition:

Message text

- RFC 822 header with: message envelope and list of recipients

- Message body, composed by user

A list of mail destinations

- Derived by user agent from header

- May be listed in header

- May require expansion of mailing lists

- May need replacement of mnemonic names with mailbox names

If **Blind Carbon Copies** (BCC) indicated, user agent needs to prepare correct message format

SMTP Sender

Takes message from queue

Transmits to proper destination host

Via SMTP transaction

Over one or more TCP connections to port 25

Host may have multiple senders active

Host should be able to create receivers on demand

When delivery complete, sender deletes destination from list for that message

When all destinations processed, message is deleted

Optimization

If message destined for multiple users on a given host, it is sent only once

Delivery to users handled at destination host

If multiple messages ready for given host, a single TCP connection can be used

Saves overhead of setting up and dropping connection

Possible Errors:

Host unreachable

Host out of operation

TCP connection fail during transfer

Sender can re-queue mail

Give up after a period

Faulty destination address

User error

Target user changed address

Redirect if possible

Inform user if not delivered

SMTP Protocol - Reliability

Used to transfer messages from sender to receiver over TCP connection

Attempts to provide reliable service

No guarantee to recover lost messages

No end to end acknowledgement to originator

Error indication delivery not guaranteed

Generally considered reliable!

SMTP Receiver

Accepts arriving message

Places in user mailbox or copies to outgoing queue for forwarding

Receiver must:

- Verify local mail destinations

- Deal with errors

- Transmission

- Lack of disk space

Sender responsible for message until receiver confirm complete transfer

- Indicates mail has arrived at host, not user

SMTP Forwarding

Mostly direct transfer from sender host to receiver host

May go through intermediate machine via forwarding capability

- Sender can specify route

- Target user may have moved

Format for Text Messages

RFC 882

Message viewed as having
envelope and contents

Envelope contains
information required to
transmit and deliver
message

Message is sequence of lines
of text

Uses general memo
framework

Header usually keyword
followed by colon
followed by arguments

Header	Meaning
To:	Email address(es) of primary recipient(s)
Cc:	Email address(es) of secondary recipient(s)
Bcc:	Email address(es) for blind carbon copies
From:	Person or people who created the message
Sender:	Email address of the actual sender
Received:	Line added by each transfer agent along the route
Return-Path:	Can be used to identify a path back to the sender

RFC 822 header fields related to message transport.

Header	Meaning
Date:	The date and time the message was sent
Reply-To:	Email address to which replies should be sent
Message-Id:	Unique number for referencing this message later
In-Reply-To:	Message-Id of the message to which this is a reply
References:	Other relevant Message-Ids
Keywords:	User chosen keywords
Subject:	Short summary of the message for the one-line display

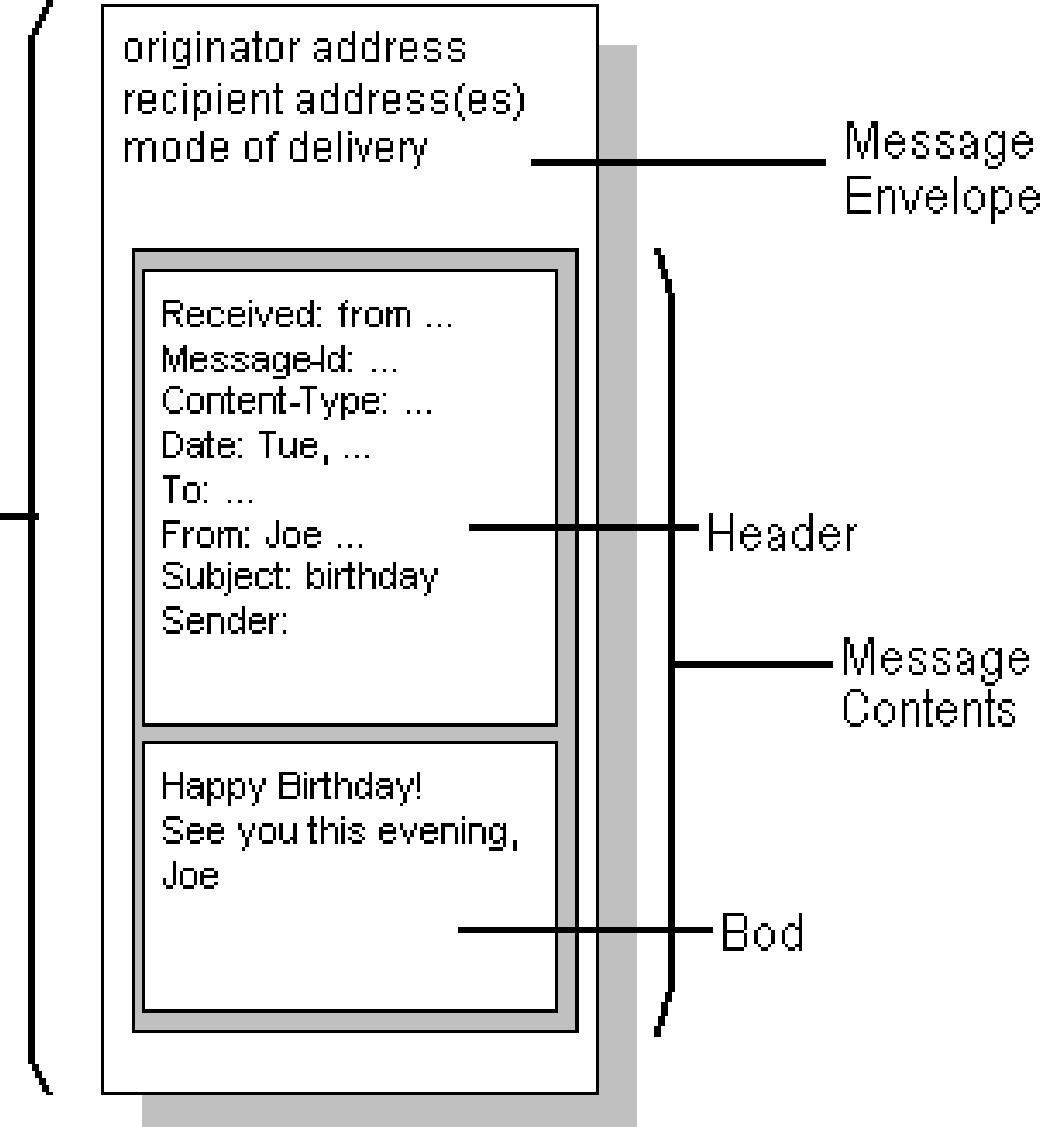
Some fields used in the RFC 822 message header.

Format for Text Messages

RFC 882

Message viewed as having
envelope and contents

RFC 822
Message



Multipurpose Internet Mail Extension (MIME)

Extension to RFC 822 for message format; given in RFC 2045, 2056

Additional lines in message header declare MIME content type

Five new message header fields

MIME version

Content type

Content transfer encoding

Content Description

Content Id

Header	Meaning
MIME-Version:	Identifies the MIME version
Content-Type:	Human-readable string telling what is in the message
Content-Id:	Unique identifier
Content-Transfer-Encoding:	How the body is wrapped for transmission
Content-Description:	Nature of the message

RFC 822 headers added by MIME.

Message Format: Multimedia Extensions

MIME version

method used
to encode data

encoded data

```
From: xyz@myServer.edu
To: abc@mailServer.iitb.edu
Subject: Picture.
MIME-Version: 1.0
Content-Transfer-Encoding: base64
Content-Type: image/jpeg
```

```
base64 encoded data .....
.....
.....base64 encoded data
.
```

- Extends and automates encoding mechanisms - *Multipart Internet Mail Extensions*
- Allows inclusion of separate components - programs, pictures, audio clips - in a single mail message (see next table)
- Sending program identifies the components, so receiving program can automatically extract and inform mail recipient
- Separator line gives information about specific encoding
- MIME is extensible - sender and receiver agree on encoding scheme
- MIME is compatible with existing mail systems
- Everything encoded as ASCII
- Headers and separators ignored by non-MIME mail systems
- MIME *encapsulates* binary data in ASCII mail envelope

MIME Content Types

Type	Subtype	Description
Text	Plain	Unformatted text; may be ASCII or ISO 8859.
Multipart	Mixed	The different parts are independent but are to be transmitted together. They should be presented to the receiver in the order that they appear in the mail message.
	Parallel	Differs from Mixed only in that no order is defined for delivering the parts to the receiver.
	Alternative	The different parts are alternative versions of the same information. They are ordered in increasing faithfulness to the original and the recipient's mail system should display the "best" version to the user.
	Digest	Similar to Mixed, but the default type/subtype of each part is message/rfc822
Message	rfc822	The body is itself an encapsulated message that conforms to RFC 822.
	Partial	Used to allow fragmentation of large mail items, in a way that is transparent to the recipient.
	External-body	Contains a pointer to an object that exists elsewhere.
Image	jpeg	The image is in JPEG format, JFIF encoding.
	gif	The image is in GIF format.
Video	mpeg	MPEG format.
Audio	Basic	Single-channel 8-bit ISDN mu-law encoding at a sample rate of 8 kHz.
Application	PostScript	Adobe Postscript.
	octet-stream	General binary data consisting of 8-bit bytes.

MIME Transfer Encodings

Reliable delivery across large range of environments

Content transfer encoding field takes on six values (see next table):

Three of them (**7bit**, **8bit**, **binary**): no encoding done

Provide some info about nature of data

SMTP transfer uses 7bit form

Quoted-printable

Data contains largely printable ASCII characters

Non-printing characters represented by hex code

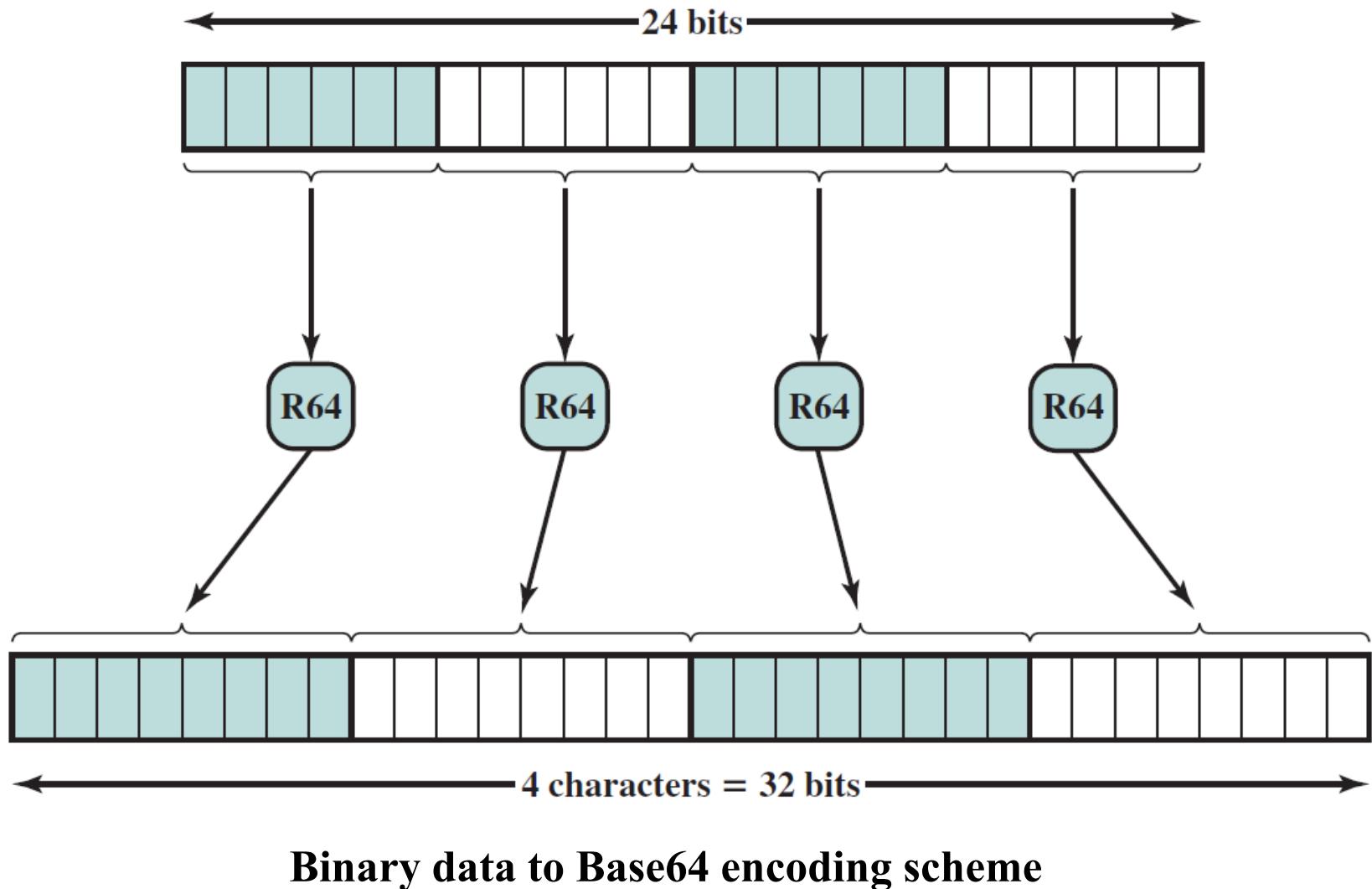
Base64 (Radix-64 Encoding)

Maps arbitrary binary input (6 bits) onto printable output 8 bit characters

X-token

Named nonstandard encoding

MIME Transfer Encodings



World Wide Web and Hypertext Transfer Protocol

World Wide Web – an architectural framework for accessing linked documents spread all over Internet

Developed at CERN (Switzerland) and MIT (USA)

<http://www.w3.org> consortium's home page

General Notions

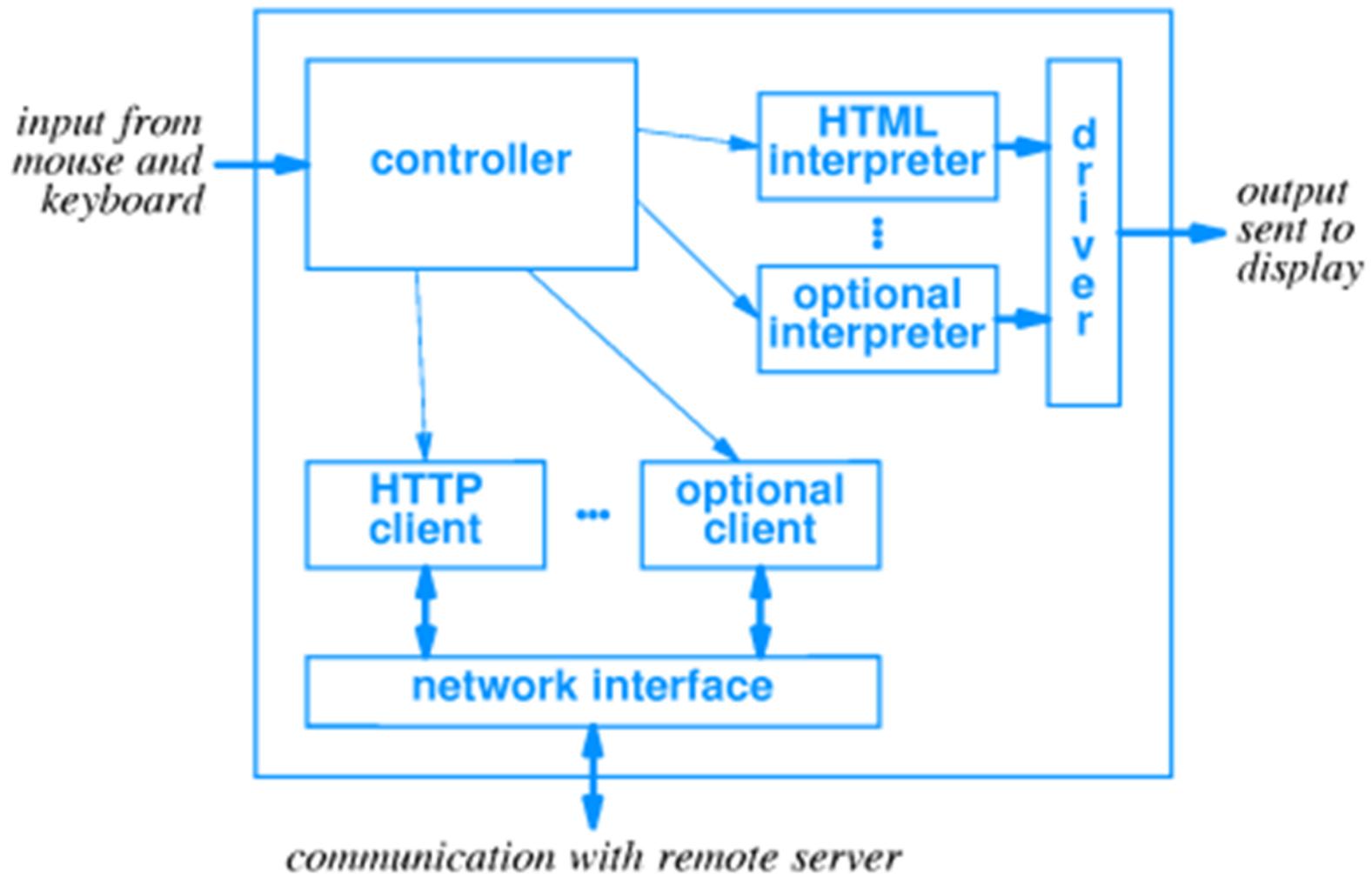
- www: basic a client/server system
- *Hypermedia* system: allows interactive access to collections of documents
- Document can hold:
 - Text (*hypertext*, if containing links to other texts)
 - Graphics
 - Sound
 - Animations
 - Video

- Documents linked together
 - Non-distributed - all documents stored locally (like CD-ROM)
 - Distributed - documents stored on remote servers
- Link represented by "active area" on screen
 - Graphic - button
 - Text - highlighted
- Selecting link will fetch referenced document for display
- Links may become invalid
- Link is simply a text name for a remote document
- Remote document may be removed while name in link remains in place
- Use of local disks for caching pages
- Pages are viewed with programs called **browsers** (Netscape, Explorer, Chrome, Mozilla)
 - interactive, "point-and-click" interface to hypermedia documents

- Browser has more components (see next figure):

- Display driver for painting screen
- HTML interpreter for HTML-formatted documents
- Other interpreters (e.g., Shockwave) for other items
- HTTP client to fetch HTML documents from WWW server
- Other clients for other protocols (e.g., ftp)
- Controller to accept input from user
- Must be multi-threaded

Browser Components



- Downloading documents from servers may be **slow**
 - Internet congested
 - Dialup connection
 - Server busy
- Returning to previous (HTML) document requires reload from server
- Local **cache** can be used to hold copies of visited pages
- Also can implement organizational *HTTP proxy* that caches documents for multiple users

Document representation

Each www document is called a *page*

- Initial page for individual or organization is called a *home page*
- Page can contain many different types of information; page must specify
 - Content
 - Type of content
 - Location
 - Links
- Rather than fixed WYSIWYG representation (e.g., Word), pages are formatted with a *mark up language* (like TeX)
- Allows browser to reformat, to fit display
- Allows text-only browser to discard graphics
- Standard is **HyperText Markup Language (HTML)**
 - **Markup:** everything in a document that is not content

- Page identified by:

Protocol used to access page, computer on which page is stored, TCP port to access page (optional) and pathname of the file on server

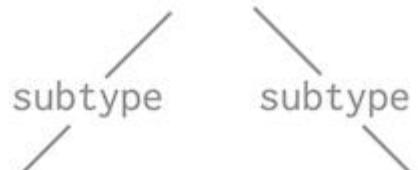
- Each link is specified in HTML
- Item on page is associated with another HTML document
- Need for mechanisms for naming, locating & accessing pages
 - Specific syntax for page's worldwide name: ***Uniform Resource Locator*** (URL): $\textit{protocol://computer_name:port/document_name}$
 - protocol* can be http, https, ftp, file, mailto
 - computer name* is DNS name
 - (Optional) *port* is TCP port
 - document_name* is path on computer to page

Generalized URL, making possible page replication (don't care where getting page)

Universal Resource Identifier (URI), allowing less resources for common pages

URI

identifier



URN

name/number

URL

protocol+
name/number

DANIEL MIESLER 2022

Uniform Resource Locator (URL)
Uniform Resource Name (URN)



URI which specifies the location is URL

URI which specified the name is URN

URI which specifies both name and location is URI

URL

URN

`http://www.example.org/index.html#date`

URI

HTML – short survey

Evolved from **Standard Generalized Markup Language (SGML)**, specialized for hypertext and adapted to the Web

HTML specifies how documents are to be formatted

- Major structure of document
- Formatting instructions
- Hypermedia links
- Additional information about document contents
- Two parts to document:
 - *Head* contains details about the document
 - *Body* contains information/content
- Page is represented in ASCII text with embedded HTML *tags* formatting instructions
- Tags have format <TAGNAME>
- End of formatted section is </TAGNAME>
- Commands inside the tags: *directives*

Main HTML Tags

Tag	Description
<html> ... </html>	Declares the Web page to be written in HTML
<head> ... </head>	Delimits the page's head
<title> ... </title>	Defines the title (not displayed on the page)
<body> ... </body>	Delimits the page's body
<h <i>n</i> > ... </h <i>n</i> >	Delimits a level <i>n</i> heading
 ... 	Set ... in boldface
<i> ... </i>	Set ... in italics
<center> ... </center>	Center ... on the page horizontally
 ... 	Brackets an unordered (bulleted) list
 ... 	Brackets a numbered list
 ... 	Brackets an item in an ordered or numbered list
 	Forces a line break here
<p>	Starts a paragraph
<hr>	Inserts a horizontal rule
	Displays an image here
> ... 	Defines a hyperlink

HTML Evolution

HTML 1.0 – one way, e.g. users could only call up pages, hard to send back information

⇒ Inclusion of **forms**, containing boxes or buttons, allowing users for info filling or make choices and sending info back to the page's owner

Form enclosed between <FORM> and </FORM> tags

One standard to handle forms' data: **Common Gateway Interface (CGI)**

Example: CGI programs (scripts) allow interface between a data base and the Web

Dynamic Web pages (higher interactivity between user & pages, continuous page updating) are designed using other methodologies, as:

-server side scripting technologies (JSP – Java Server Pages, ASP – Active Server Pages, PHP – Perl Helper Pages, ColdFusion)

-active Web documents (moves computation to the browser), using Java technologies (JavaScripts)

Hypertext Transfer Protocol (HTTP)

Underlying protocol of the World Wide Web

Not a protocol for transferring hypertext

For transmitting information with efficiency necessary for hypertext jumps
HTTP specifies commands and client-server interaction

Can transfer plain text, hypertext, audio, images, and Internet accessible information

HTTP Overview

Transaction oriented client/server protocol

Usually between Web browser (client) and Web server

Uses TCP connections

Stateless

Each transaction treated independently

Each new TCP connection for each transaction

Terminate connection when transaction complete

Client/Server model:

- *client*: browser that requests, receives, “displays” WWW objects
- *server*: WWW server daemon, sends objects in response to client requests

Functionality:

- client initiates TCP connection (creates socket) to server, port 80
- server accepts TCP connection from client
- HTTP messages (application-layer protocol messages) exchanged between browser (HTTP client) and WWW server (HTTP server)
- TCP connection closed

HTTP is “**stateless**”: server maintains no information about past client requests

HTTP1.0: RFC 1945

HTTP1.1: RFC 2068

....

HTTP/2: **RFC 7540** (May 2015) -it allows: interleaving of request and response messages on the same connection and uses an efficient coding for HTTP header fields; prioritization of requests, letting more important requests complete more quickly; longer-lived connections; further improving performance

Key Terms

Cache

Client

Connection

Entity

Gateway

Message

Origin server

Proxy

Resource

Server

Tunnel

User agent

Examples of HTTP operations:

-direct connection with origin server; client opens an end-to-end TCP connection and issues a HTTP request. It consists of a specific command (OO: method), a URL & a MIME-like message with request parameters, info about client, etc. Server receives the request, process it & return HTTP response, containing status & error info, MIME-like message with info about server, about response and the body content. Finally the TCP connection is closed.

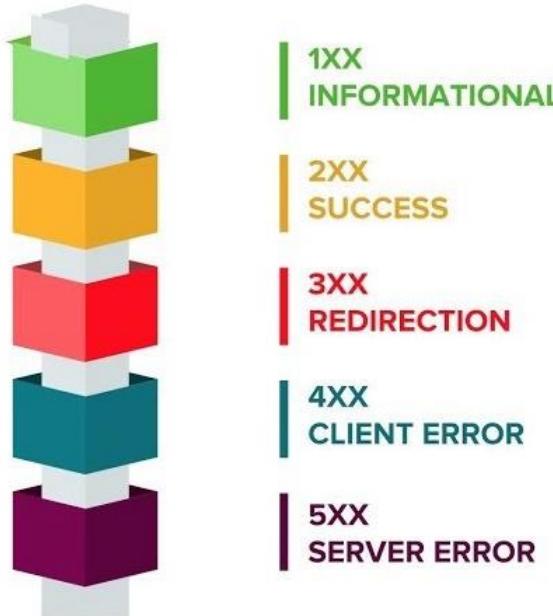
-Intermediate systems with TCP connections (relaying requests & responses)

-Example of a cache: an intermediate system stores previous requests & responses, for handling new requests; no need to access the origin server; caching time limit

HTTP methods and status codes

- GET - request data from a specified resource
- HEAD - almost identical to GET, but without the response body (useful for checking what a GET request will return before actually making a GET request)
- POST - send data to a server to create/update a resource (requests are never cached; do not remain in the browser history/cannot be bookmarked); no restrictions on data type or data length
- PUT - send data to a server to create/update a resource + idempotent characteristic (calling the same PUT request multiple times will always produce the same result)
- DELETE - deletes the specified resource
- CONNECT - requests that the recipient establish a tunnel to the destination origin server identified by the request-target; intended only for use in requests to a proxy
- TRACE - performs a message loop-back test along the path to the target resource, providing a useful debugging mechanism
- OPTIONS - requests information about the communication options available for the target resource, at either the origin server or an intervening intermediary

HTTP Status Codes



- **1xx (Informational):** The request was received, continuing process
- **2xx (Successful):** The request was successfully received, understood, and accepted
- **3xx (Redirection):** Further action needs to be taken in order to complete the request
- **4xx (Client Error):** The request contains bad syntax or cannot be fulfilled
- **5xx (Server Error):** The server failed to fulfill an apparently valid request

HTTP Messages (Protocol data units)

Implementation for:

Requests

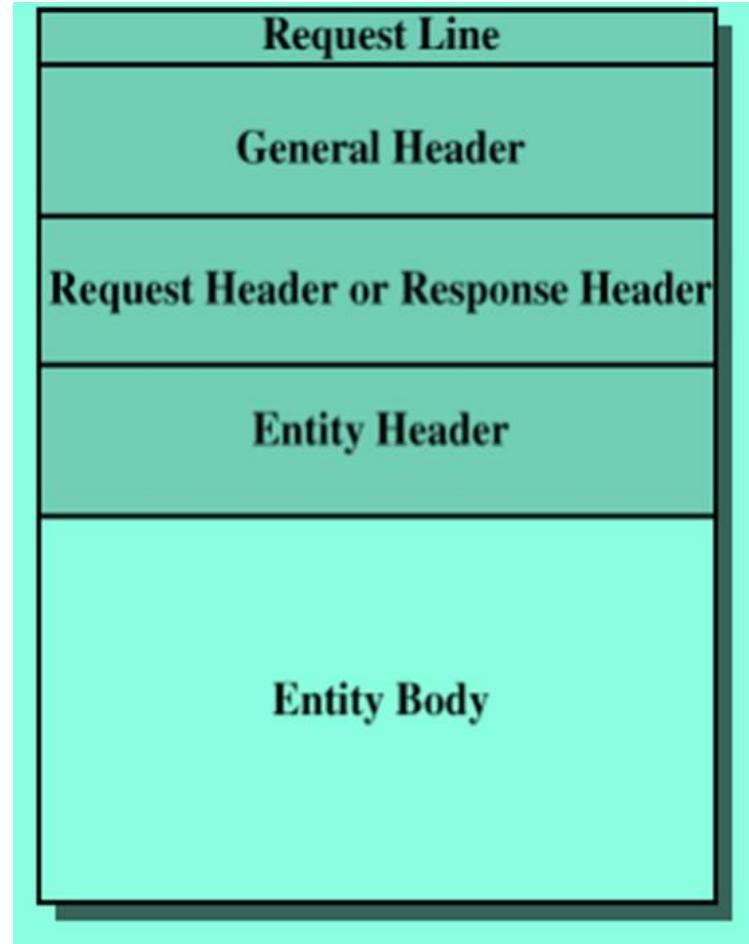
Client to server

Responses

Server to client

Structure:

- Request line – message type and requested resource
- Response line – status information about message
- General header – applies to both request/response messages
- Request header – info about request and client
- Response header – info about response and server
- Entity header – info about the resource target of the request
- Entity body – body of the message





(a) HTTP request

HTTP Message Format Example



(b) HTTP response

Example of a HTTP Get method on utcluj.ro

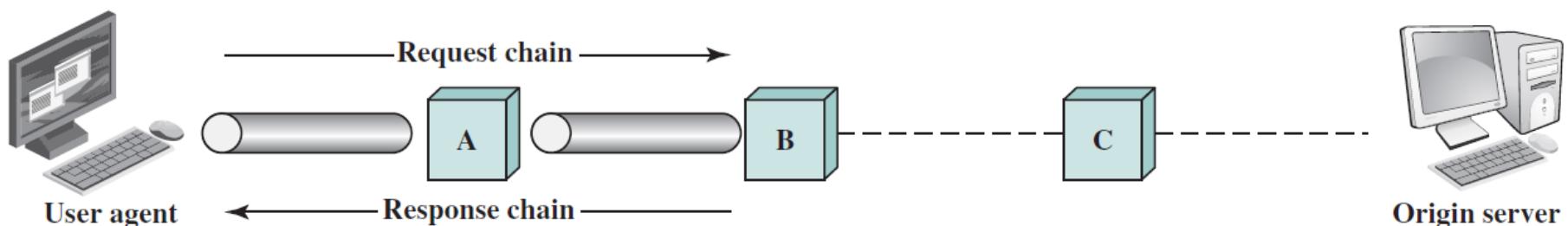
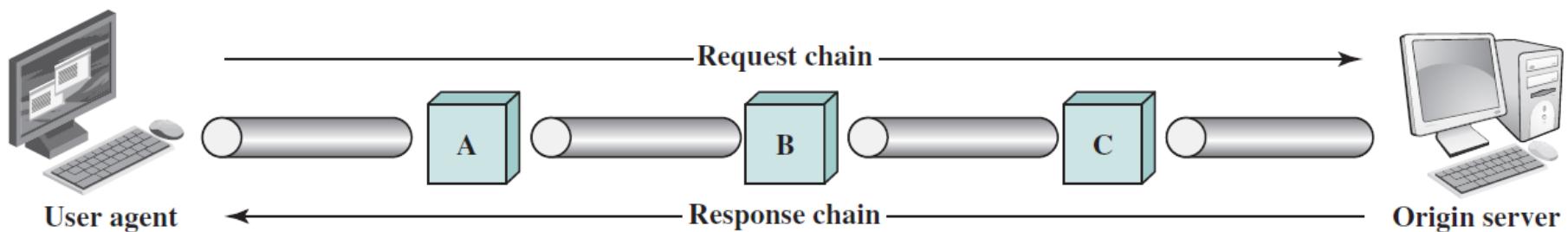
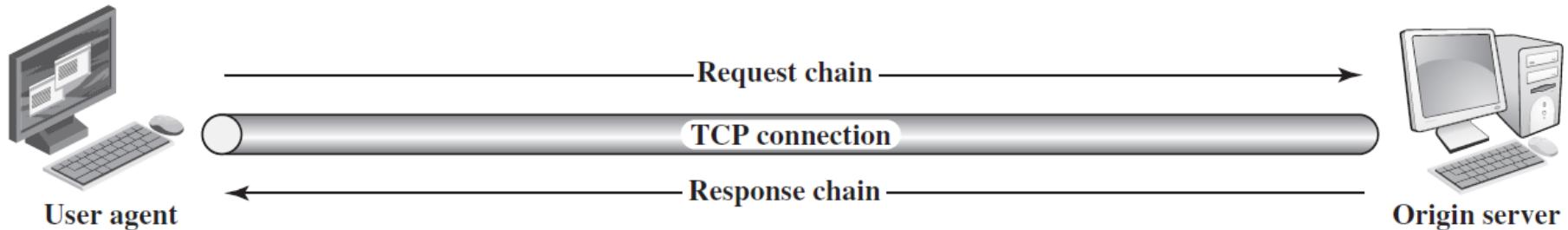
- using Chrome browser and DevTools – F12 on the keyboard

The screenshot shows a web browser window for the University of Technology Cluj-Napoca (UTN) website at [utcluj.ro](https://www.utcluj.ro). The page features a red header with the university's logo and language links (EN, FR, DE). Below the header is a map of Europe with various university logos from different countries. The main content area displays the UTN logo and some text. To the right of the browser is the Chrome DevTools Network tab, which is active. The Network tab shows a timeline of requests and a detailed list of resources. The detailed list includes:

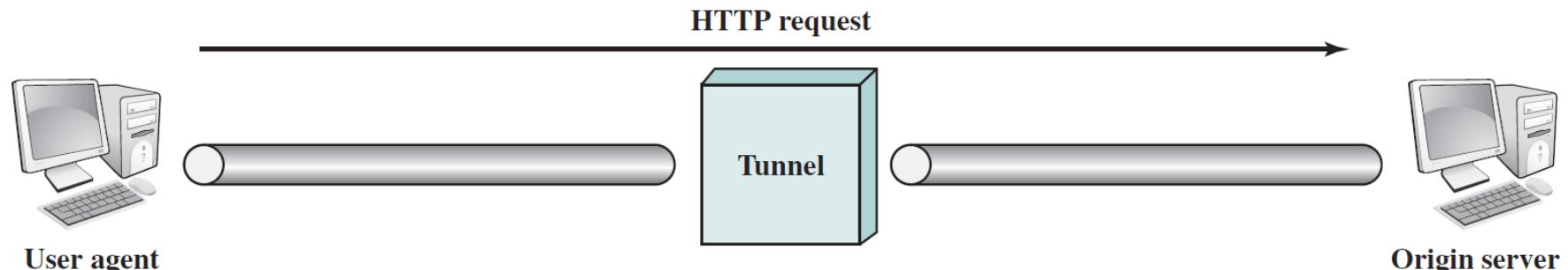
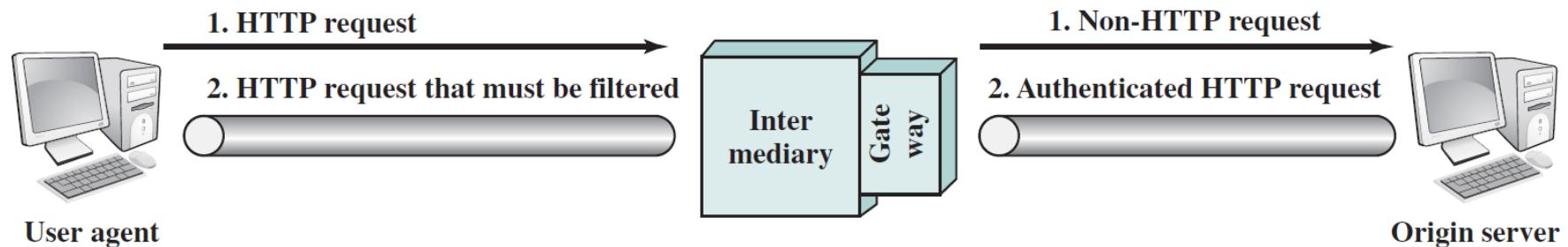
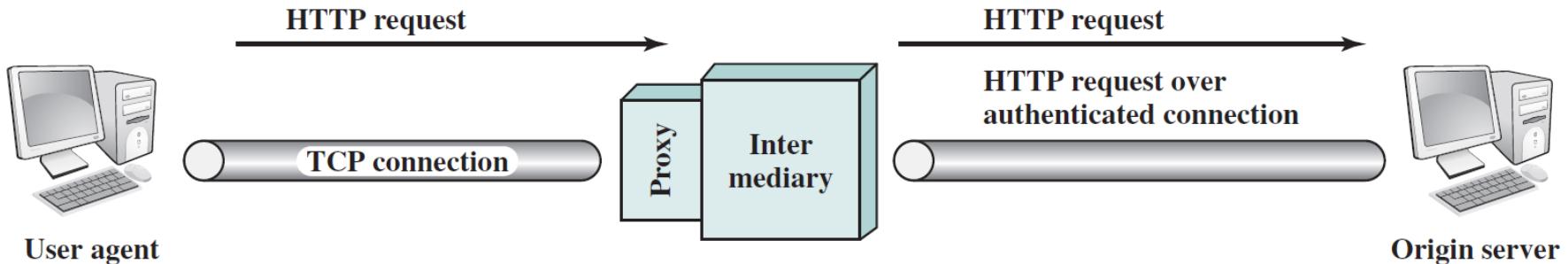
Name	Request URL	Request Method	Status Code	Remote Address	Referrer Policy
www.utcluj.ro	https://www.utcluj.ro/	GET	200 OK	193.226.5.7:443	strict-origin-when-cross-origin
bootstrap.min.css					
style.css					
skin-5.css					
template.css					
jquery.min.js					
bootstrap.min.js					
bootstrap-select.min.js					
lazyload.min.js					
waypoints-min.js					
js?id=UA-120285510-1					
counterup.min.js					
custom.nonmin.js					
serviceworker.js					
logo_site.png					
uni-overall-4star.jpg					
eut_logo_vertical_mini.png					
jquery.thememunch.tools.min.js					

Below the resource list, it shows 83 requests, 3.3 MB transferred, and 5.1 MB total.

Examples of HTTP Operation



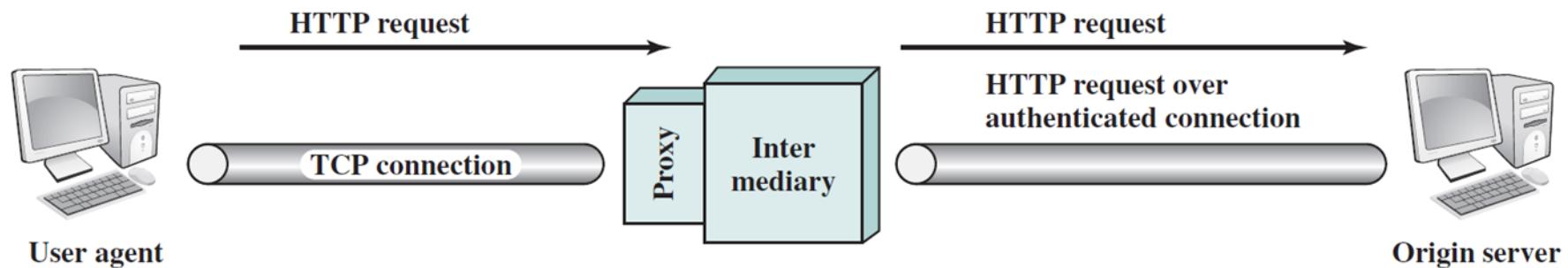
Intermediate HTTP Systems



Intermediate Systems

HTTP defines three forms of intermediate systems:

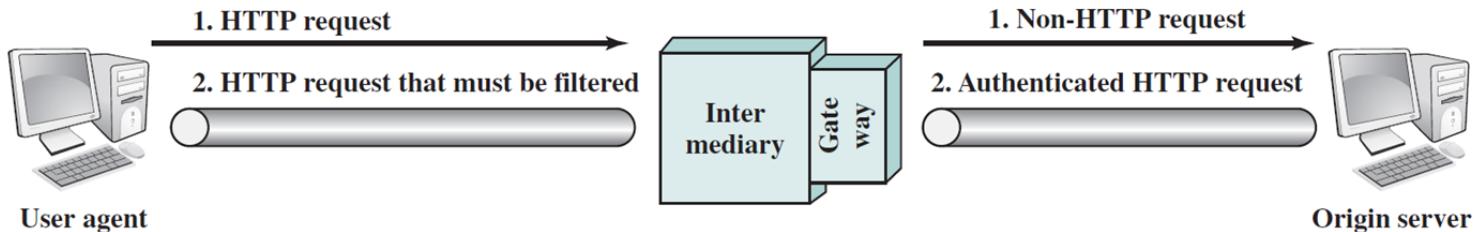
- Proxy, acting on behalf of clients, forwarding their requests;
- Security intermediary: is a server in interacting with client & client vs. server; is on the client side within a firewall; presents clients' requests to server, over an authenticated connection;
- may also implement different versions of HTTP (if the client and server are running different versions of HTTP)



Intermediate Systems

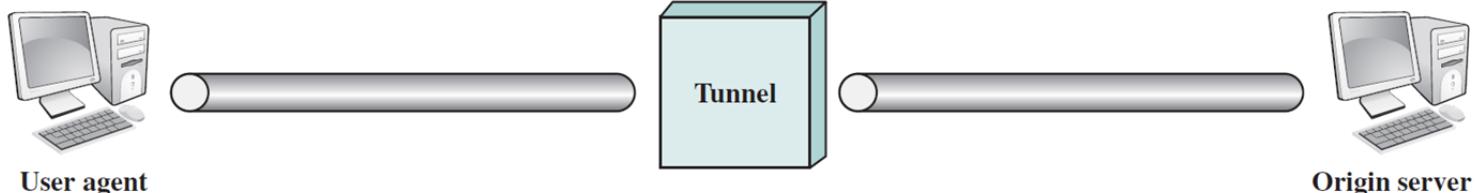
HTTP defines three forms of intermediate systems:

- Gateway, appears as server to client (acts on behalf of servers);
 - Security intermediary: is on the server part on a firewall;
 - Non-HTTP server: allows for accessing servers running other protocols than HTTP (FTP, Gopher servers)
-
- Tunnel, relay between TCP connections; no extra info check; example: a firewall in which a client & a server maintains a secure connection for purposes of HTTP transactions
-
- Cache, is a facility that may store previous requests and responses for handling new requests



HTTP request

22/05/2024



Origin server

Multimedia Networking

Impacts of multimedia networking:

- Users can choose when they want content (such as TV and radio programs) delivered, rather than needing to watch/listen when the content is broadcasted
- Telephone service and data networking will tend to converge
- Two-way video conferencing will often be used instead of telephony
- E-mail will integrate with voice mail (e-mail messages will be spoken rather than Typed)
- Voice/video e-mail: video can be included along with speech
- Multi-way video conferencing already allows virtual meetings and conferences
- As these technologies improve, the need for travel will decrease

Ingredients:

- entertainment video
- IP telephony (or voice-over-IP, VOIP)
- Internet radio
- Multimedia web sites
- teleconferencing, both 2 party and multi-party (e. g. the Access Grid Node).
- interactive games
- virtual worlds (which overlaps with interactive games)

Multimedia Application Specificity

- highly sensitive to end-to-end delay and delay variation (jitter)
- service requirements are quite different from those of traditional data applications
- attempts to extend the Internet architecture to provide explicit support for the service requirements of multimedia applications (reservation techniques, differentiated services)

How should the Internet evolve to support multimedia?

- One view: no fundamental changes are necessary

There should be more use of multicast and caching

More bandwidth should be added to links, and more router capacity should be added

- Another view: applications should be able to reserve end-to-end bandwidth

A protocol to allow applications to reserve bandwidth is needed

Router scheduling policies must take these reservations into account

Some packets will get preferential treatment, and probably the senders of those packets will have to pay more.

Applications must be able to describe the traffic that they intend to send

The network must have a means to determine whether it has the bandwidth necessary to support a reservation request

- An intermediate view: a **differentiated services** model

A small number of classes of service

IP Datagrams get different levels of service depending on their service level.

Service characteristics

- Multimedia applications are delay-sensitive and loss-tolerant
- Most data applications are delay-insensitive and loss-intolerant
- TCP/IP was designed for data applications, whereas ATM was designed for both data and multimedia; TCP/IP seems to have mostly prevailed over ATM, so we are faced with adding ATM-like features to TCP/IP (example: reserving network resources between two endpoints requires that something like a virtual circuit be set up and intermediate routers must be aware of the flow between the endpoints)
- Specific Problems
 - network-induced jitter. Some solutions: client buffering, packet sequence numbers, packet timestamps.
 - lost packets. Some solutions: forward error correction, sending periodic parity packets, sending a redundant lower-quality delayed stream
 - interleaving
 - media encapsulation: RTP and RTCP
- Real-time audio/video conferencing: H.323, an “umbrella protocol”.

Service models for the Internet

The network-layer protocol of today's Internet provides a "best-effort" service

No promises are made for end-to-end delay nor for variation in end-to-end delay (packet jitter)

Since the Internet service model is not appropriate for multimedia applications, it is challenging to develop such applications, and performance is unsatisfactory when networks are congested

Methods for overcoming these limitations:

- Use UDP rather than TCP, which avoids TCP congestion control such as slow-start.
- Delay playback at the receiver, so that late packets can be used. This is more feasible for non-interactive applications
- Timestamp packets at the sender so that the receiver knows when they should be played
- Prefetch stored data at times when extra bandwidth is available

Examples of Multimedia Applications

Streaming and stored audio and video

Distinguishing features:

- *Stored media*: The multimedia content is stored at the server
 - user may pause, rewind, fast-forward, or index through the content.
 - acceptable response time is from 1 to 10 seconds
- *Streaming*: A client begins playout of the content a few seconds after it begins receiving the file from the server.
 - client will be playing out content from one location while receiving later parts
Products include RealPlayer and Windows Media Player.
- *Continuous playout*
 - once playout begins, it should proceed according to the original timing of the recording
 - if data is received after it should be played, then the data is useless.

Streaming of Live Audio and Video

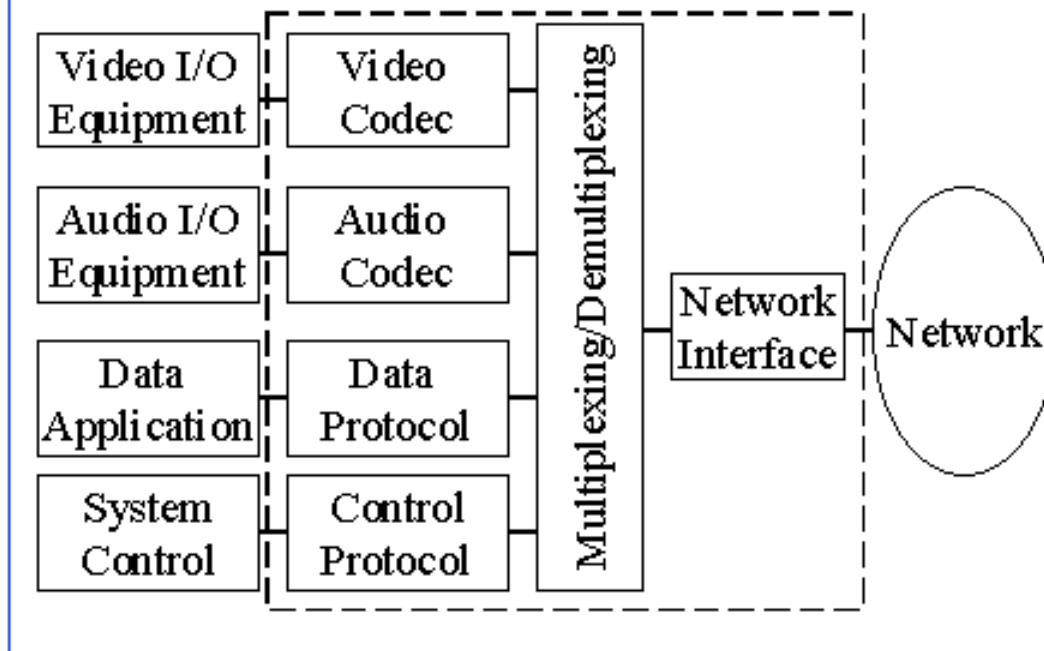
- includes radio and television broadcast over the Internet
- fast-forward is not possible
- pausing and rewinding can be implemented with local storage
- currently most often implemented using multiple unicast sessions.
- Access Grid is implemented using multicast.

Real-time Interactive Audio and Video

- includes Internet Phone
- it sets constraints on delay
 - for voice, delays smaller than 150 milliseconds are not perceived by a human listener
 - delays of 150 to 400 milliseconds are acceptable
 - delays of over 400 milliseconds tend to be unacceptable

General Architecture of Audio/Video Systems

Telephony/Conferencing Systems



Audio and Video Compression

Before sending audio and video over the network, it must be digitized and compressed

Uncompressed video is extremely large, so compression is almost a necessity

Very high compression ratios are often possible for video

Audio digitization techniques

– **Pulse code modulation (PCM)**: samples the audio signal at some fixed rate, and then represents each sample with some number of bits; standard telephone digitization samples at 8000 times per second, and then encodes each sample with 256 quantization values => an uncompressed signal of 64 Kbps

- not very good fidelity, is not suitable for music

- audio compact disks also use PCM: audio CDs sample at 44,100 samples per second, and use 16 bits per sample; results in a rate of 705.6 Kbps for mono transmissions or 1.411 Mbps for stereo.

Audio compression

- GSM issues (13 Kbps rate)
- G.729 (8 Kbps)
- MP3 (MPEG layer 3 standard): 128 or 112 Kbps - can be used for streaming audio
- Proprietary standards

Video compression

- Use of **MPEG** (Motion Picture Experts Group) standards:
 - MPEG 1 for CD-ROM quality video (1.5 Mbps)
 - MPEG 2 for DVD quality video (3-6 Mbps)
 - MPEG 4 for object-oriented video compression
- H.261, under H.323 umbrella
- Proprietary standards.

Streaming Stored Audio and Video

Clients request compressed audio/video files that are resident on servers

The server sends the file to the client over a socket, either TCP or UDP

A protocol such as **real-time protocol (RTP)** is used to encapsulate segments of the file with special headers

When the file starts to arrive at the client, typically it is played within a few seconds

A protocol such as **real-time streaming protocol (RTSP)** can be used to give interactivity, such as: pause/resume and jumps within the file

A media player application (a web-browser plugin) performs the following functions:

- *Decompression*
- *Jitter removal*: done by buffering the signal
- *Error correction*. Three techniques:

- Redundant packets and error-correcting codes

- Client requests retransmission of lost packets

- Interpolating the lost data from the received data

- provides a *GUI* (Graphic User Interface) with control knobs.

Accessing Audio and Video from a Web Server

Normally, the media will be stored as files (compressed) on the server

In the case of video, there may be separate audio and video files, or they might be interleaved in the same file

It is the responsibility of the media player to manage synchronization of the two streams

For simplicity, we assume that there is only one file

A possible architecture:

- The browser connects to the web server
- The browser requests the audio/video file with an HTTP request message
- The web server sends the file to the browser in an HTTP response message
- The browser looks at the content type, launches the media player if necessary, and forwards the file to the media player
- The media player renders the audio/video file

One drawback: the browser is an intermediary between the server and the media player => the file would need to be completely downloaded before it gets forwarded to the media player

It makes it more difficult for the media player to allow the user to control the stream.

A better method is to make use of a **meta file**, which provides information (e. g., the location and encoding) about the audio/video file => the browser passes the meta file to the media player, and the media player makes its own connection to the server

This server may be a **streaming server** rather than a web server (may be specifically designed to deliver streaming media, and may run a different protocol than HTTP)

Options for delivering the audio/video from the streaming server to the client:

1. The server sends the stream over UDP at the encoded rate of the audio/video (*drain rate*.) The client decompresses and plays the stream as it receives it.
2. Same, but the media player delays playout for 2-5 seconds in order to eliminate network-induced jitter (the client buffers the incoming stream)
3. The stream is sent over TCP, and the media player buffers the stream for 2-5 sec. It gives TCP the chance to retransmit lost packets, but the flow & congestion control of TCP might interfere with sending the stream at the drain rate.

RTSP (Real-Time Streaming Protocol)

RTSP is an **out-of-band protocol** that allows a media player to control the transmission of a media stream

- **Out-of-band protocol** means that RTSP messages are sent over a separate channel from the media itself
- RTSP does not specify how the media is compressed, encapsulated in packets, transported, or buffered

RTP (Real Time Protocol)

RTP is a protocol that provides for a standard packet structure that includes fields for sequence numbers, timestamps, etc. RTP typically runs on top of UDP.

Each source (e. g., camera or microphone) can be assigned its own independent stream of RTP packets

RTP can be sent over unicast or multicast.

Multiple RTP streams belonging to a single application can make up an **RTP session**.

The RTP header fields:

- The *payload type* gives the compression method
- The *sequence number field* is 16 bits long, and can be used to detect packet loss
- The *timestamp field* is 32 bits long, and it reflects the sampling instant of the first byte in the RTP packet
- The *synchronization source identifier (SSRC)* is 32 bits long, and identifies the source of the RTP stream

Typically, each stream in the RTP session has a distinct SSRC. The SSRC is chosen randomly.

RTCP (Real Time Control Protocol)

Typically used by participants using RTP in a multicast scenario

RTCP packets are sent periodically and contain sender and/or receiver reports and statistics than can be useful to applications

H.323

H.323 is a standard for real-time audio and video conferencing among end systems on the Internet; also covers how end systems on the Internet communicate with ordinary circuit-switched telephone networks. It means:

The products of Internet telephony and videoconferencing that use H.323 should be able to interoperate and should be able to communicate with ordinary telephones

H.323 is an umbrella specification that includes:

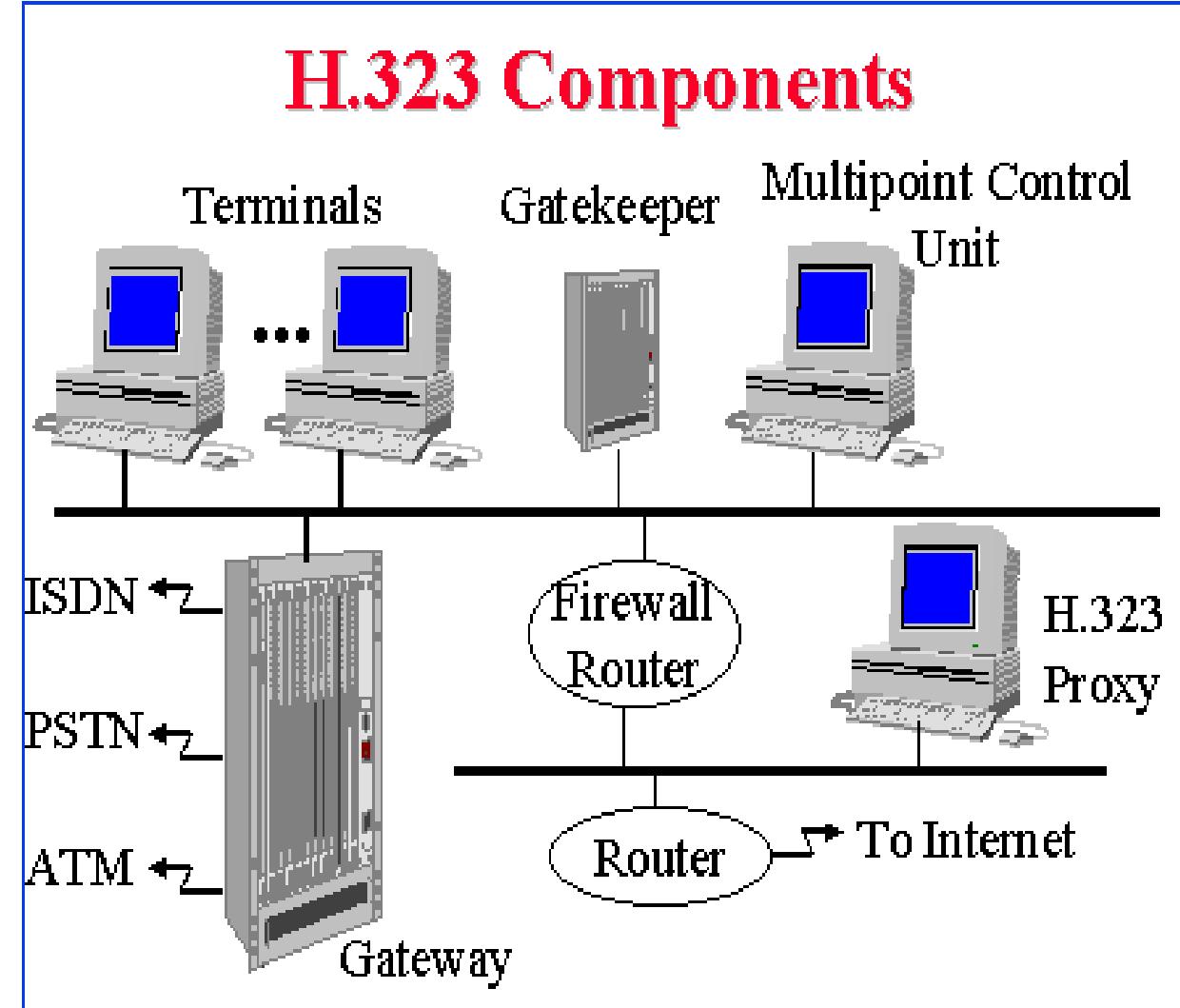
- A specification for how endpoints negotiate audio/video encodings.
- A specification for how audio and video chunks are encapsulated and sent over the network; this is done by means of RTP
- A specification for how endpoints communicate with their respective gatekeepers
- A specification for how Internet phones communicate with ordinary phones

H.323 components

End points can be standalone devices or computer applications

Gateways permit communication among H.323 endpoints and ordinary telephones

Gatekeepers (optional) provide address translation authorization, bandwidth management, and accounting for LAN terminals



H.323 endpoints must support the following protocols:

G.711 PCM (pulse code modulation) speech encoding

Real-Time Protocol

H.245: an “out-of-band” protocol for controlling media between H.323 endpoints

Q.931: a signaling protocol for establishing and terminating calls. Provides for interoperability with traditional telephones.

RAS: a protocol that allows endpoints to communicate with a gatekeeper

(see next figure)

H.323 channels

An endpoint maintains several channels

The H.245 control channel is a TCP connection that is used for capability exchanged and opening and closing media channels

H.245 is similar in purpose to RTSP (which is used for stored media and streaming sessions)

Q.931 provides traditional telephone functionality.

H.323 Protocols

- Multimedia over LANs
- Provides component descriptions, signaling procedures, call control, system control, audio/video codecs, data protocols

Video	Audio	Control and Management			Data			
H.261 H.263	G.711, G.722, G.723.1, G.728, G.729	R	H.225.0 RAS	H.225.0 Signaling	H.245 Control	T.124		
RTP		X.224 Class 0			T.125			
UDP		TCP			T.123			
Network (IP)								
Datalink (IEEE 802.3)								

Session Initiation Protocol (SIP)

Application level signaling protocol

Allows creating, modifying & terminating sessions with more participants

Supports user location, call setup, call transfers, mobility (by proxying & redirection)

Used by the gateways to setup connections

SIP works in conjunction with IP protocols:

- RSVP for reserving resources

- RTP/RTCP/RTSP for transporting real-time data

- SAP (Session Announcement Protocol) – advertise multimedia session

- SDP (Session Description Protocol)

Can use TCP/UDP

Text based