

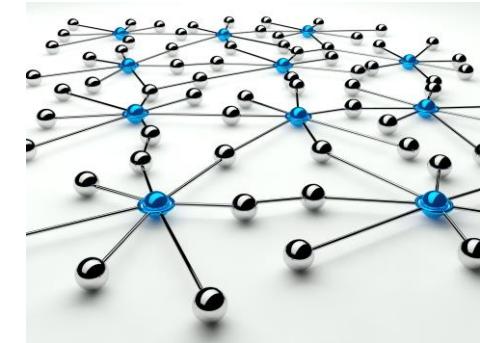
Networks Architectures and Protocols

1. INTRODUCTION

Lecturer: Zoltán Gál, PhD

Faculty of Informatics, University of Debrecen

February 05, 2018



Outline

- 1) Introduction of the computer network term
definition, goals, basic elements
- 2) Evolution of the networks, milestones
- 3) Classification criteria of the computer networks
- 4) Basic concepts of the communication
 - Node
 - Communication media, channel, collision
 - Signal, signal coding, modulation multiplexing
 - Transmission rate
 - Modulation rate
 - Data link types
 - Direction of the data transfer
 - Switching modes
 - Addressing basics
 - Elements of the communication protocol
 - Basic mechanisms of the communication

1. Introduction of the computer network term

Definition of the computer network:

- Connected system of the autonomous machines: common application.
- Connection of computer systems with a given data transmission technology (HW and SW).

Goals:

- Communication (human-human, human-machine, machine-machine)
- Resource sharing (CPU, storage, line)
- Saving of resources (optimal execution of special tasks)
- Scalability (no. of elements, capacity modification)
- Increase of reliability (data <-> hardware)
- Increase of the communication rate

Basic elements:

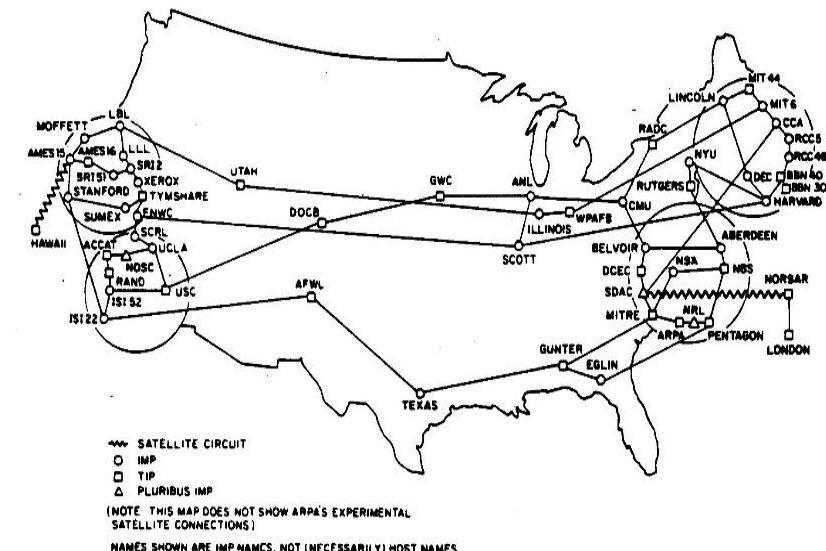
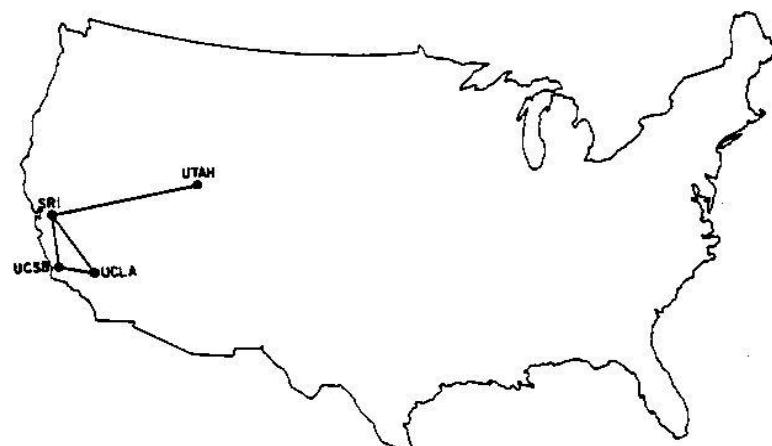
- Computers, peripheries (e.g. network printer, etc.)
- Network devices (HW: e.g. switching elements)
- Devices for physical connections (cables, lines)
- Programs for network applications (SW)

2. Evolution of the networks, milestones

Date	Event
Before 1900	Long distance communications (courier, smoke signs, galvanic/optical telegraph)
1890's	Bell: invention of the telephone, rapid penetration rate of the service
1901	Marconi: first Transatlantic wireless transmission
1920's	AM radio
1939	FM radio
1940's	Invention of the microwave
1947	Shockley, Barden, Brittain: invention of the semiconductor transistor
1948	Claude Shannon: „A Mathematical Theory of Communication”
1950's	Invention of the IC
1957	Establishment of the ARPA by DoD.

2. Evolution of the networks, milestones

Date	Event
1960's	Mainframe Computing
1962	Paul Baran: description of the packet switching theory
1967	Larry Roberts: paper in the ARPANET subject
1969	Establishment of the ARPANET: UCLA, UCSB, U-Utah, Stanford



1969

1977

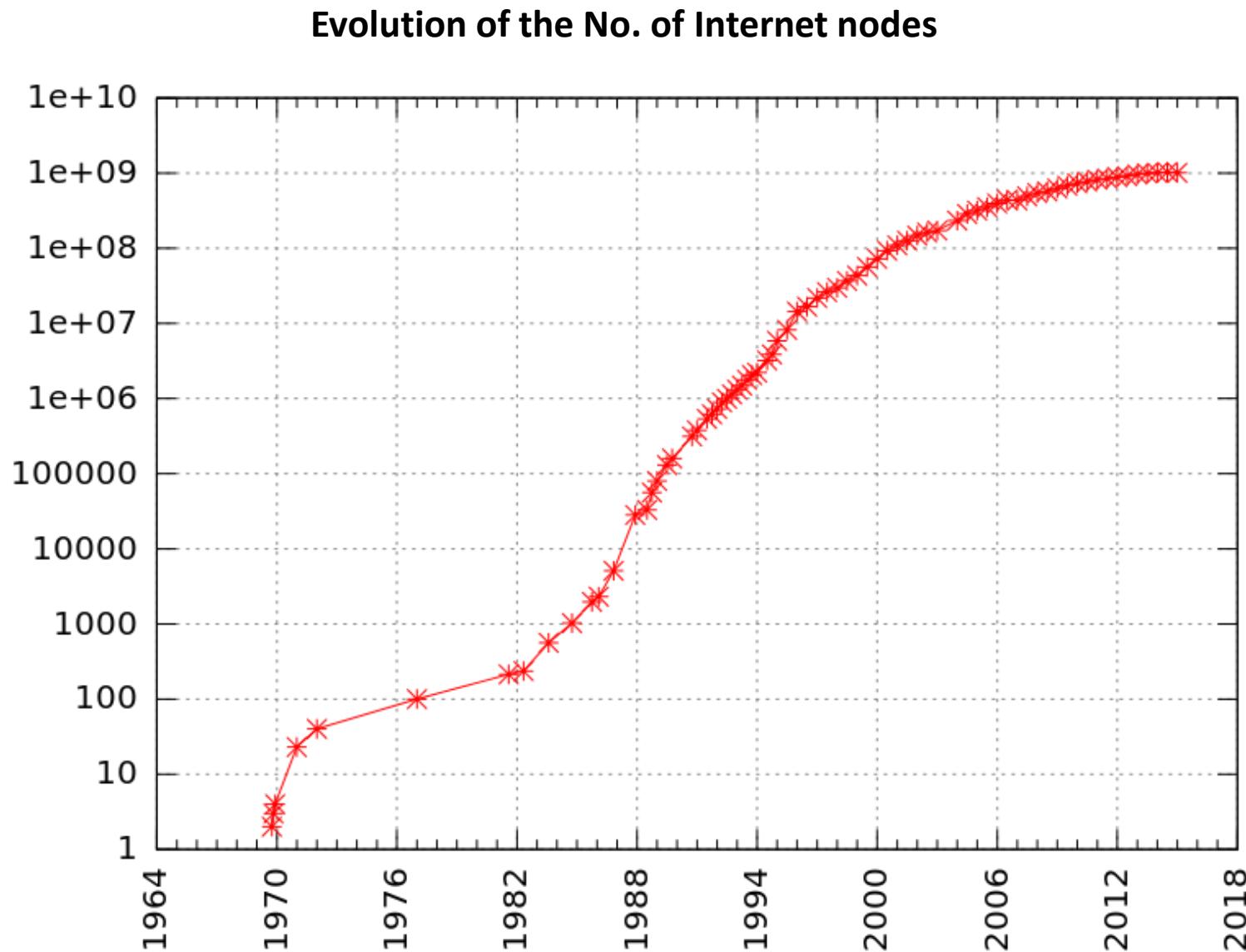
2. Evolution of the networks, milestones

Date	Event
1970	University of Hawaii: development of ALOHANET
1970's	Penetration of the digital ICs, digital PCs
1972	Ray Tomlinson: development of the E-mail program
1973	Bob Kahn, Vint Cerf: invention of TCP/IP, connection to Europe of the ARPANET
1974	BBN: development of the Telnet. Establishment of the business version of the ARPANET
1980's	Penetration of the PCs and Unix based minicomputers
1981	Setting the Internet term: network of networks
1982	ISO develops the OSI model and its protocols (these protocols are not used today, just the model)
1983	TCP/IP becomes general mechanism of the Internet. MILNET is split from the ARPANET.
1984	Establishment of the Cisco Systems, Co. (router SW). Development of the DNS, 1000 nodes.

2. Evolution of the networks, milestones

Date	Event
1986	Establishment of the NSFNET (56 kbps)
1987	No. of Internet nodes > 10 k
1988	Establishment of the CERT (Computer Emergency Response Team) by the DARPA
1990	ARPANET = Internet, (No. of nodes > 100 k)
1991	Tim Berners-Lee: invention of the World Wide Web (WWW, CERN)
1993	Development of the first web browser: Mosaic
1994	Development of the Netscape Navigator (browser)
1997	Establishment of the ARIN (American Registry for Internet Numbers), Starting Internet 2
1999	Internet 2: development of the IPv6 Setting of a purpose: integration of the voice, video and data transmission into a common infrastructure

2. Evolution of the networks, milestones



3. Classification criteria of the computer networks

1) Size of the physical area:

- BAN: Body Area Net., BCI – Brain Computer Interface
- PAN: Personal Area Network
- SOHO: Small Office/ Home Office
- LAN: Local Area Network
- MAN: Metropolitan Area Network
- WAN: Wide Area Network
- GAN/Internet: Global Area Network

2) Transmission rate:

- Classical networks: kbps ... Mbps
- High speed networks: 100 Mbps ... Tbps

3) Ownership:

- Private Network
- Public Network

4) Mobility:

- Fixed Network
- Mobile Network

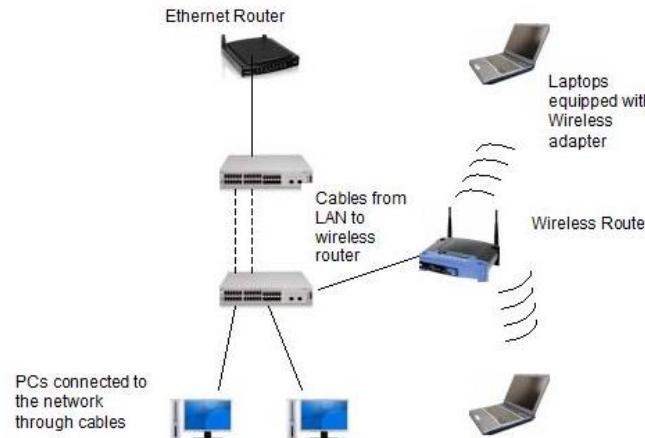
3. Classification criteria of the computer networks

A) Local Area Network (LAN):

- System of a communicating computers
- Area: $n \times \text{km}^2$, one site/institute/company/organization
- Continuous access to the network services
- Management done by the owner
- Transmission rate: 100 Mbps ... 10 Gbps ...
- High level of reliability (short distances, robust technology)

LAN types:

- Connected media (galvanic: twisted pair, coaxial cable, optical cable)
- Connectionless (wireless, radio waves)



3. Classification criteria of the computer networks

A) Local Area Network (LAN):

Basic elements of the LAN:

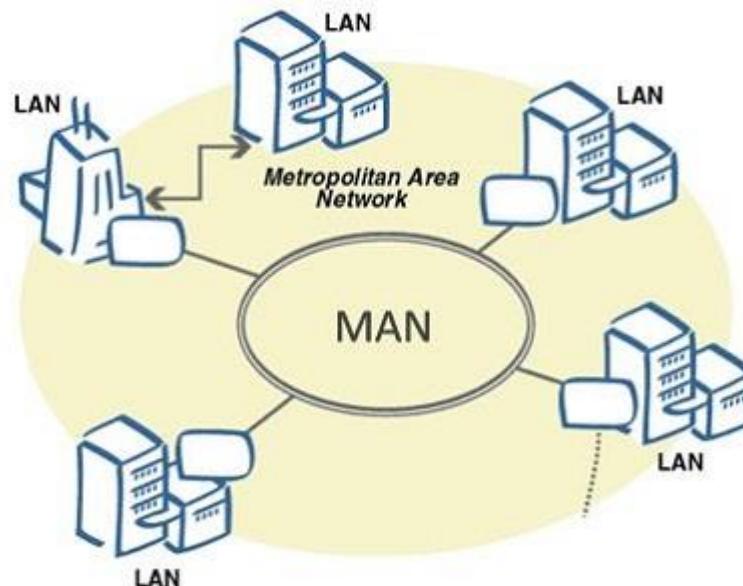
- Computers
- Network Interface Cards (NIC)
- Network media (twisted pair, coaxial cable, optical fibre, radio wave)
- Network devices:
 - Repeater/Hub, Bridge, Switch, Router



3. Classification criteria of the computer networks

B) Metropolitan Area Network (MAN):

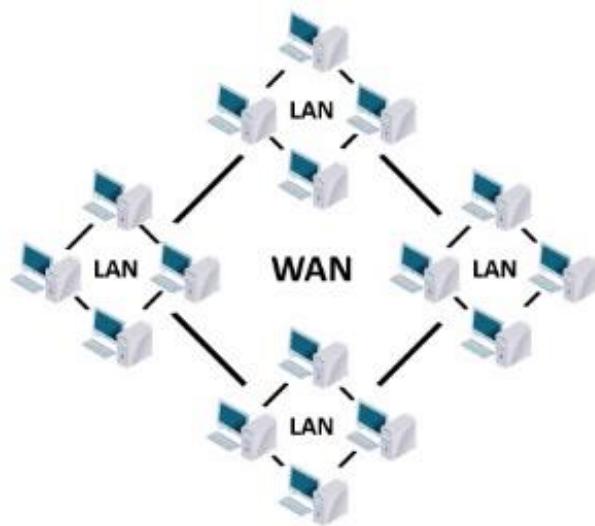
- System of LANs
- Area: $n \times 100 \text{ km}^2$, one city/region
- Connects two or more LANs
- E.g.: Bank/travel agency/university with several sites
- Leased lines of a service provider are used (usually)
- Technology: similar to the LANs
- Connection between the sites can be wired or wireless



3. Classification criteria of the computer networks

C) Wide Area Network (WAN):

- System of LANs and MANs
- Area: country, continent, World
- All users can communicate among
- Remote access of the resources
- Services: E-mail, WWW, file transfer, e-commerce, etc.



4. Basic concepts of the communication

Computer network node (communication entity) types:

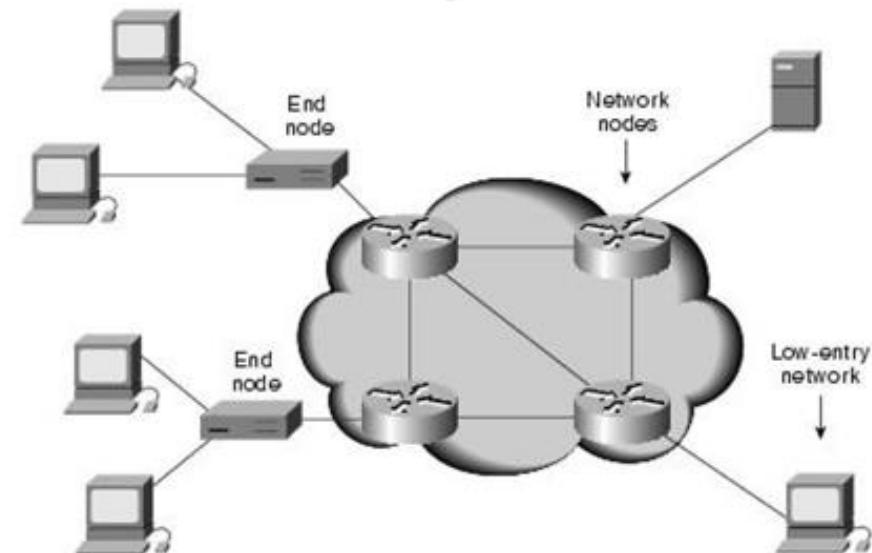
Node: Individual device with communication capability and unique network address ID (e.g. computer, printer, router). In the communication session the node can be transmitter, receiver or transmitter/receiver. The node communicates through the communication interface.

End node/User node:

Communication node able to send or receive data.

Intermediate node / Network node:

Node with transfer capability to other nodes.



4. Basic concepts of the communication

Data transfer media, channel, collision:

Data transfer media (line): Device, material to transmit signal. E.g. shielded twisted pair, coaxial cable, optical cable, air, EM space.

Data transmission channel: Path (frequency band) to transmit signals. On a given media can work more than one channel simultaneously.

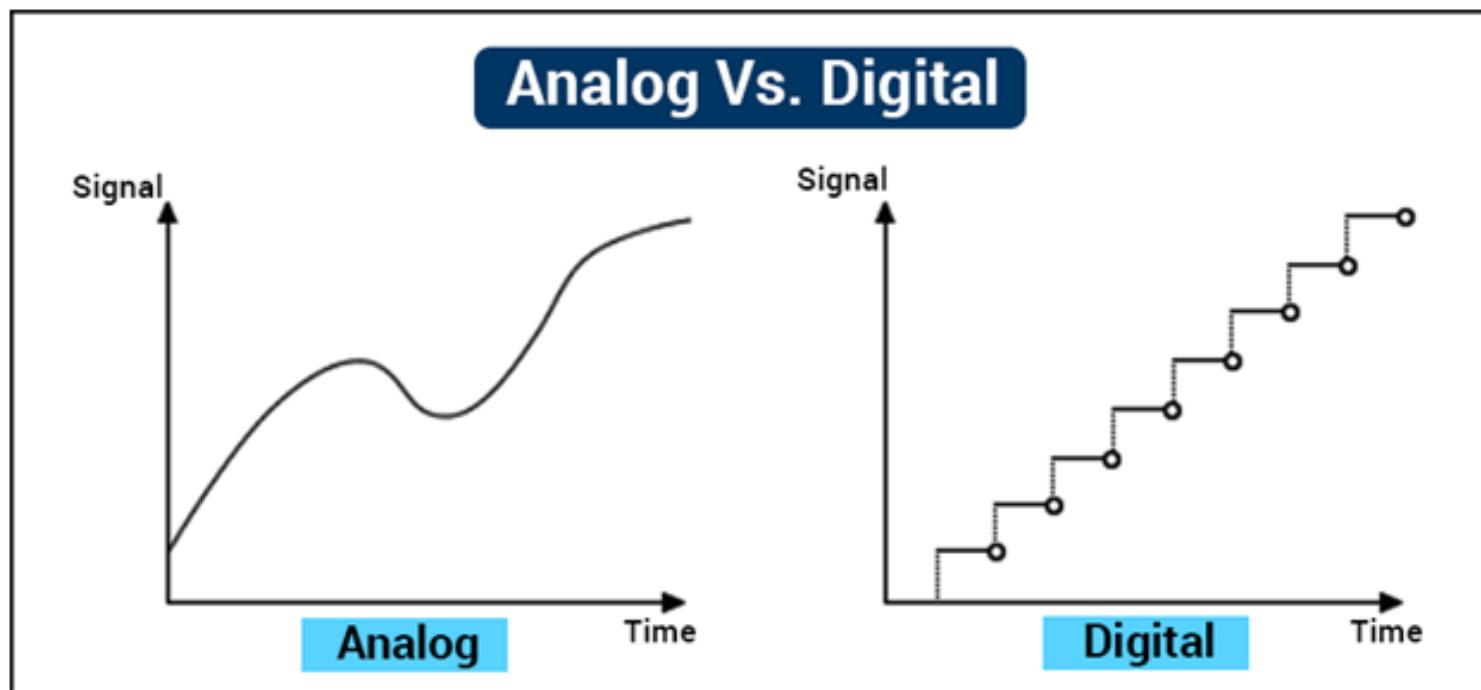
Collision: More than one sources are transmitting signals on the same moment. Classical medium allows single transmitter but multiple receivers in a given moment. Exists channels with multiple simultaneous sources, as well (e.g. CDMA).

Collision domain (bandwidth domain): Subspace of the network where the collision can be sensed. In the collision domain only one transmission is possible in a given short time interval. From logical point of view the collision domain can be represented as a common channel of the nodes for a short time duration. Here „short time” has relative meaning.

4. Basic concepts of the communication

Signal, signal coding, modulation, multiplexing:

Signal: Energy quantity dependent on space and time. It carries the data on the channel. Variants: analog, digital.



4. Basic concepts of the communication

Signal, signal coding, modulation, multiplexing:

Signal coding: Process of mapping the digital data to the analog carrier signal (e.g. voltage, voltage modification. We are discussing digital coding only, but exists analog signal coding mechanism, as well.

Modulation/Demodulation: The data transfer channel can be represented as a frequency band (carrier frequency). The digital data is mapped to the analog carrier signal. One of the parameters (e.g. amplitude, phase, etc.) of the carrier signal is modified in function of the data. The inverse process at the receiver is named demodulation. The MODEM device executes modulation task when transmits and demodulation task when receives data. These two processes can be done simultaneously on two different channels by the modem.

Multiplexing/Demultiplexing: Two or more separated transmitted flows on the same channel in the „same” time is the multiplexing. Separation process at the receiver of two or more flows from the channel is named demultiplexing.

4. Basic concepts of the communication

Data transfer rate (network speed, bit rate, bandwidth):

No. of bits transmitted on the channel per unit of time (second).

Unit of measurement:

bit/seconds,
b/s,
bps.

It is used to count the transmission capacity of the channel.

Bigger units:

1 kbps	1.000 bps				10^3 bps
1 Mbps	1.000 kbps	1.000.000 bps			10^6 bps
1 Gbps	1.000 Mbps	1.000.000 kbps	1.000.000.000 bps		10^9 bps
1 Tbps	1.000 Gbps	1.000.000 Mbps	1.000.000.000 kbps	1.000.000.000.000 bps	10^{12} bps

4. Basic concepts of the communication

Modulation rate:

No. of signal level modification on the channel per unit of time (second).

Measurement unit:

$$\text{signal change / sec} = \text{baud}$$

Measures the signal change speed. It has strong correlation with the transmission rate at a given communication mechanism.

Bigger units:

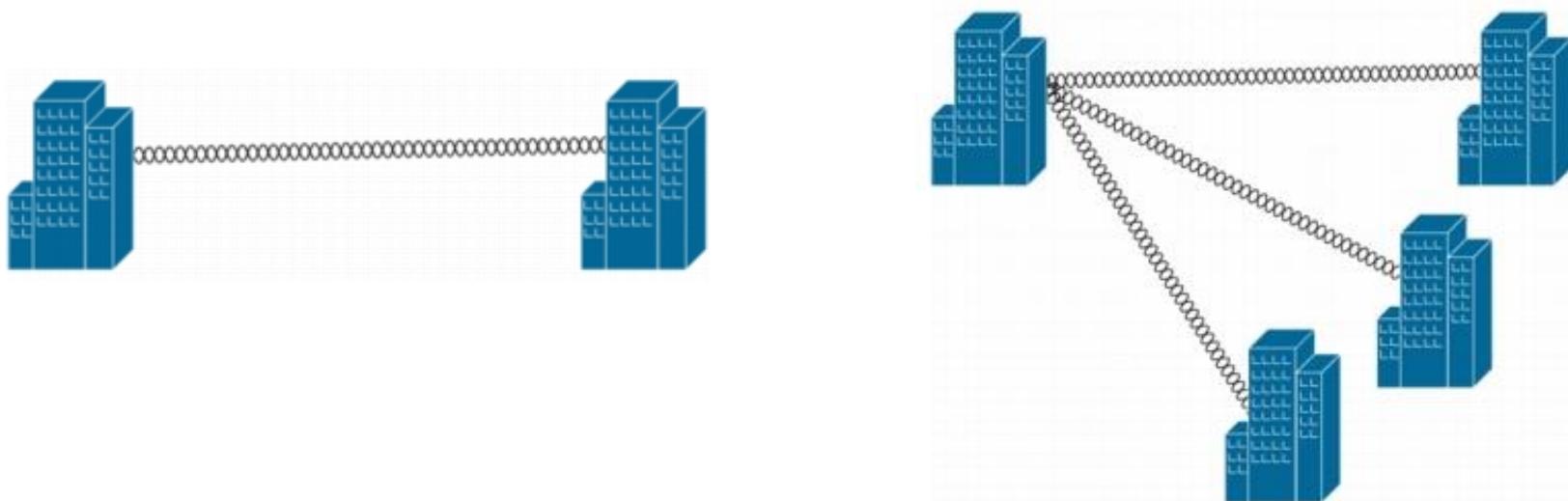
1 kbaud	1.000 baud				10^3 baud
1 Mbaud	1.000 kbaud	1.000.000 baud			10^6 baud
1 Gbaud	1.000 Mbaud	1.000.000 kbaud	1.000.000.000 baud		10^9 baud
1 Tbaud	1.000 Gbaud	1.000.000 Mbaud	1.000.000.000 kbaud	1.000.000.000.000 baud	10^{12} baud

4. Basic concepts of the communication

Data transfer (connection) types:

Point-to-Point connection: Only a pair of transmitter and receiver executes the transmission (e.g. two nodes at the both ends of a cable).

Multipoint connection (point-to-multipoint, broadcast): Only one source transmits to several destinations in a given moment. E.g.: radio transmission in the region.



4. Basic concepts of the communication

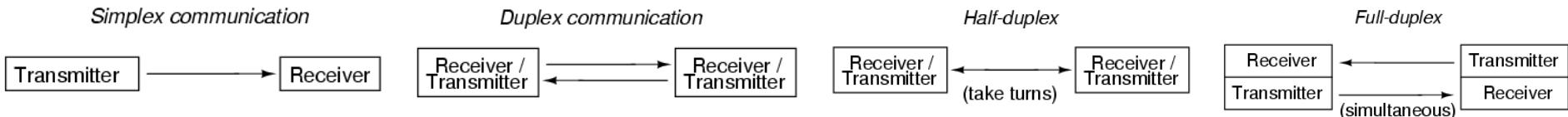
Direction of the data transfer:

Simplex connection: The communication between two nodes is possible in only one direction (e.g. A -> B). E.g.: radio broadcasting.

Duplex connection: The communication between two nodes is possible in both directions (e.g. A <-> B). E.g.: radio communication.

- **Half-duplex connection:** A -> B and A <- B but in different time intervals. E.g.: CB radio.

- **Full-duplex connection:** A -> B and A <- B simultaneously (e.g. telephone). This is logically the case of two individual simplex connections.



4. Basic concepts of the communication

Switching modes:

Circuit switched technology: Dedicated connection path is created between the end nodes before the transfer. This connection is maintained during the session.

E.g.: classic wired phone service

Message switched (store and forward) technology: Circuit is not created between the end nodes, but only on the segment between two consecutive intermediate nodes.

E.g.: Telex

Packet switched technology: The data is fragmented in packets with length < MTU and these units are forwarded separately. The method is efficient and has well manageable buffering features.

4. Basic concepts of the communication

Addressing basics:

Need unique identification of the nodes for successful delivery of the messages (like for the post office service). In the message are two address IDs: source, destination. The destination ID may be one of the following address category.

Unicast address: ID of one communication entity (interface). The source ID is unicast address. In general the communication interface has unicast ID, but exceptions exist in function of the communication technology.

Anycast address: ID of a set of communication entities (set of interfaces on different nodes). Message sent to Anycast address should arrive to at least one element of the set (usually the nearest entity).

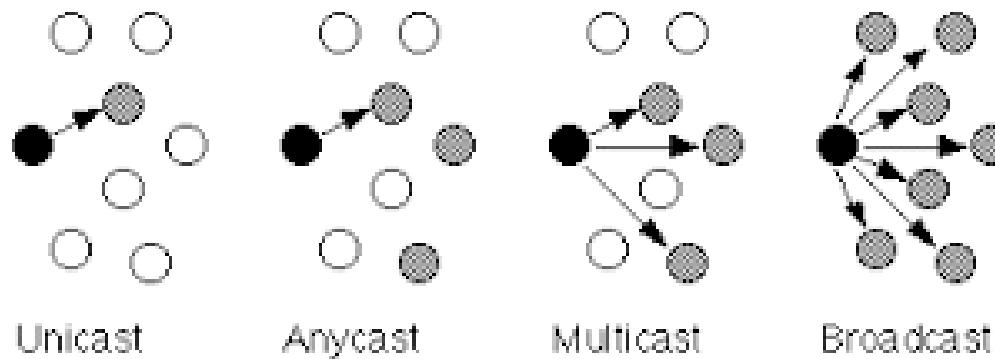
4. Basic concepts of the communication

Addressing basics (cont'd):

Multicast address: ID of the set of communication entities (usually set of interfaces on different nodes). Message sent to this ID should arrive to each entity of the set.

Broadcast address: ID of all communication entities in a given (broadcast) domain. It may be interpreted as a special multicast ID, where all entities take part in the communication.

Broadcast domain: Physical region of the network where the messages addressed to multicast or broadcast ID are sensed.



4. Basic concepts of the communication

Elements of the communication protocol:

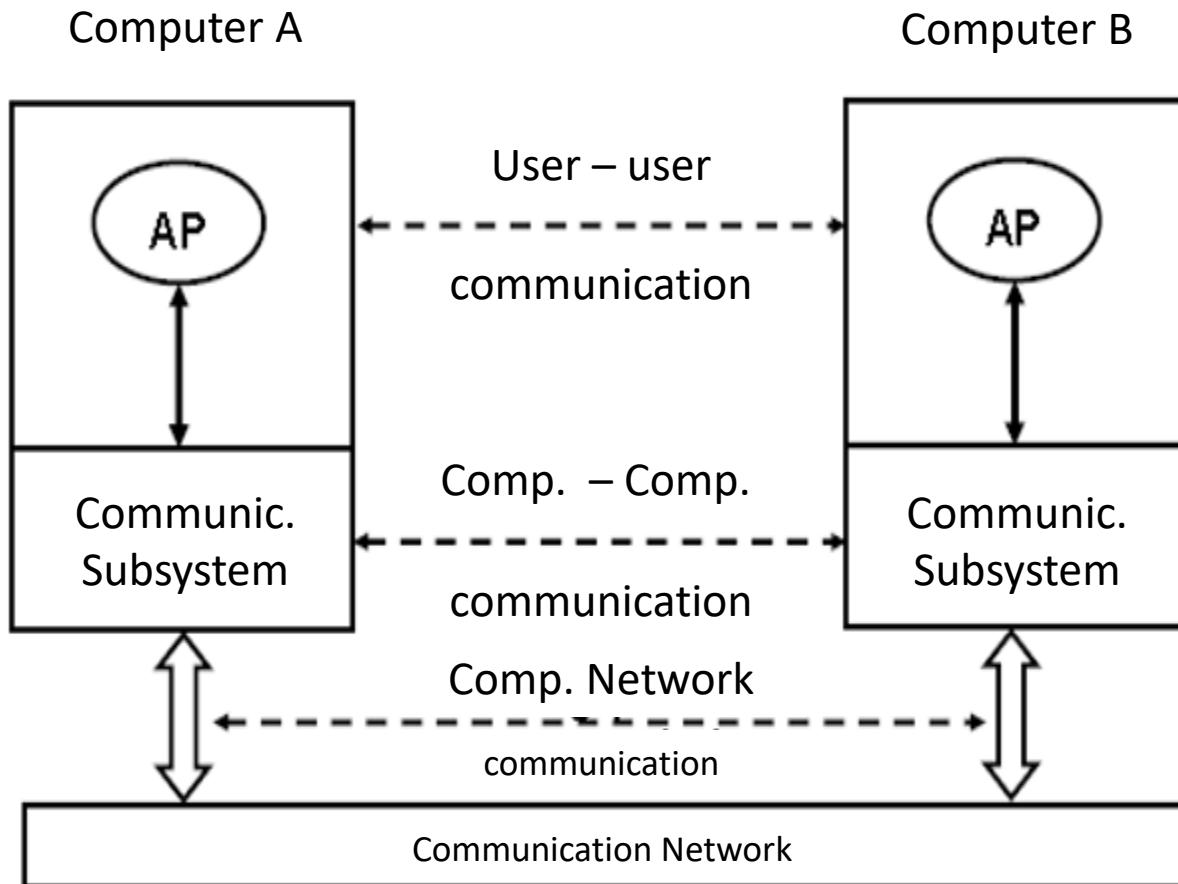
Protocol: Set of rules and conventions described formally determining the communication mechanisms between the network entities (devices, nodes). Tools used for protocol description: extended finite state automata, SDL (Specification and Description Language), high level languages.

Protocol Entity (PE): Network entity for the communication of the source and/or destination (hardware/firmware and/or software). E.g.: communication device, communication program.

Protocol Data Unit (PDU): Message record forwarded during the communication conform the rules between the protocol entities. The structure and the size of the PDU depends on the communication technology.

4. Basic concepts of the communication

Basic mechanism of the communication:



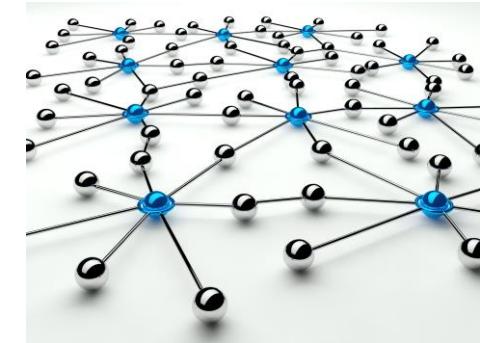
Networks Architectures and Protocols

2. LAYERED NETWORK ARCHITECTURE, LAYER MODEL

Lecturer: Zoltán Gál, PhD

Faculty of Informatics, University of Debrecen

February 05, 2018



Outline

- 1) Layered network architecture
- 2) OSI reference model and layers
- 3) Mapping of the OSI, TCP/IP and Hybrid models
- 4) Intermediate network node types
 - Repeater
 - Bridge/Switch
 - Router
 - Gateway

1. Layered network architecture

Considerations:

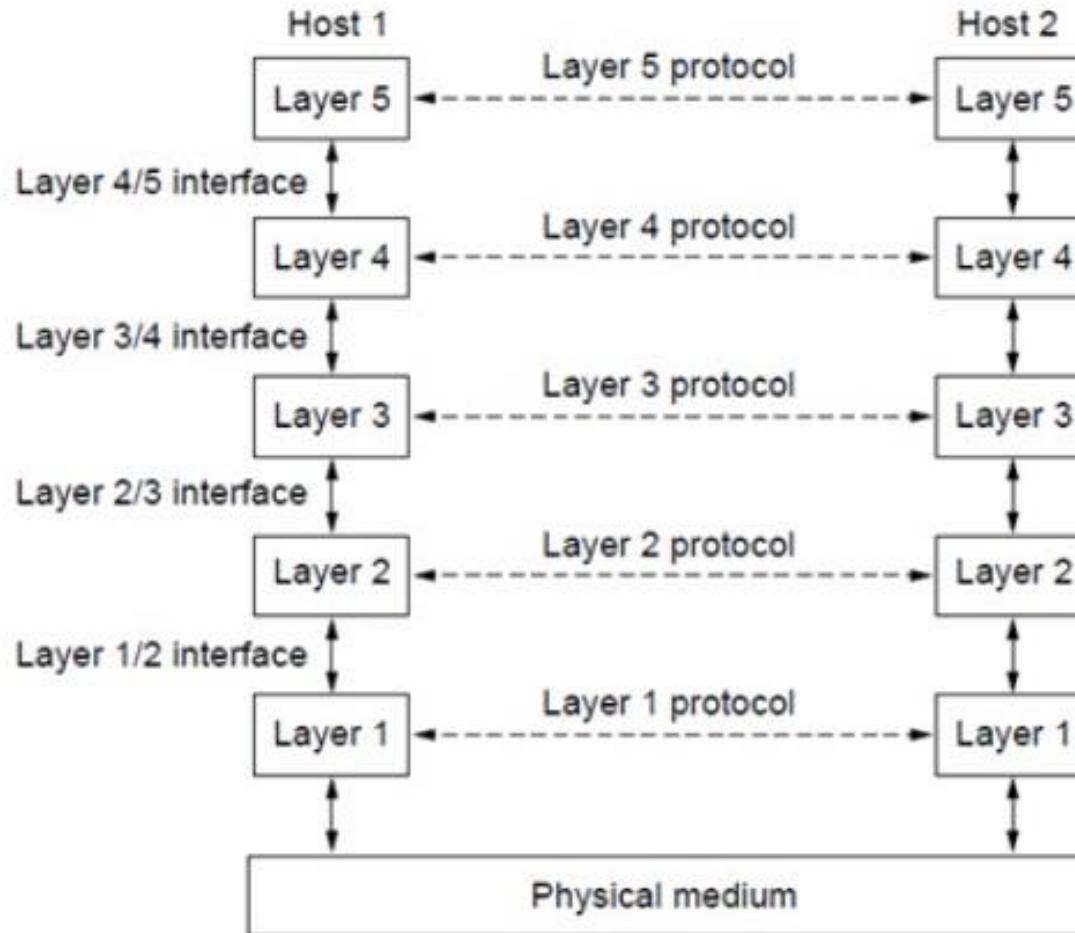
- Exact description of a protocol is a complex task.
- A protocol system developed in hierarchical structure is much more easy to understand.
- Tracking changes of such systems is relatively simple.
- Different communication products developed conform to the standards become interactive.

E.g.: Message transfer between remote users



1. Layered network architecture

Layers, protocols, interfaces:



1. Layered network architecture

Notions:

Layer N protocol:

Set of communication rules belonging to the logical layer no. N.

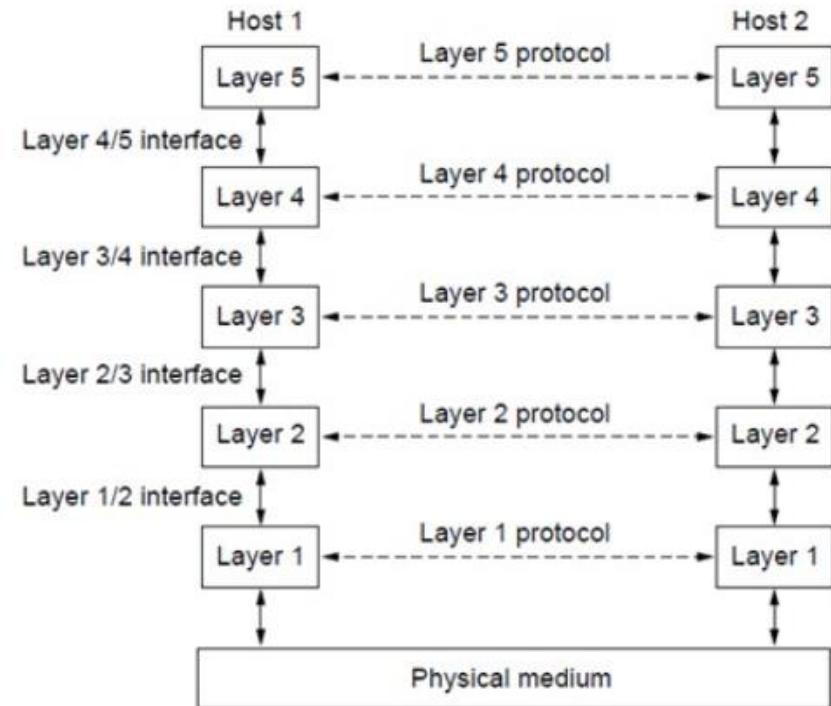
Peer entities:

Communication entities (device/module) of two communication nodes belonging to the same communication layer.

Peer entities use the communication protocol of the same logical layer.

Protocol Data Unit (PDU):

Message transmitted by the peer entities with the layer protocol. Each layer has own PDU format.



1. Layered network architecture

Notions:

Layer N/(N+1) interface:

Common border of the layer N and layer N+1 on the same communication node. Data and control messages are transmitted through this border. (E.g. formal parameter list)

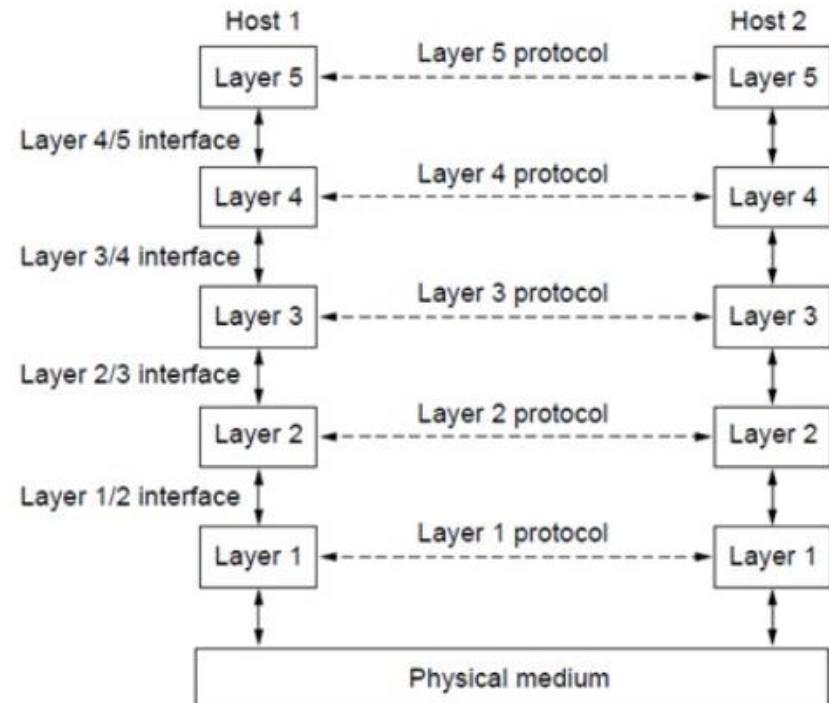
Service Data Unit (SDU):

Content transmitted through the layer interface in the same node. Each SDU is specific to the layer interface.

Peer entities:

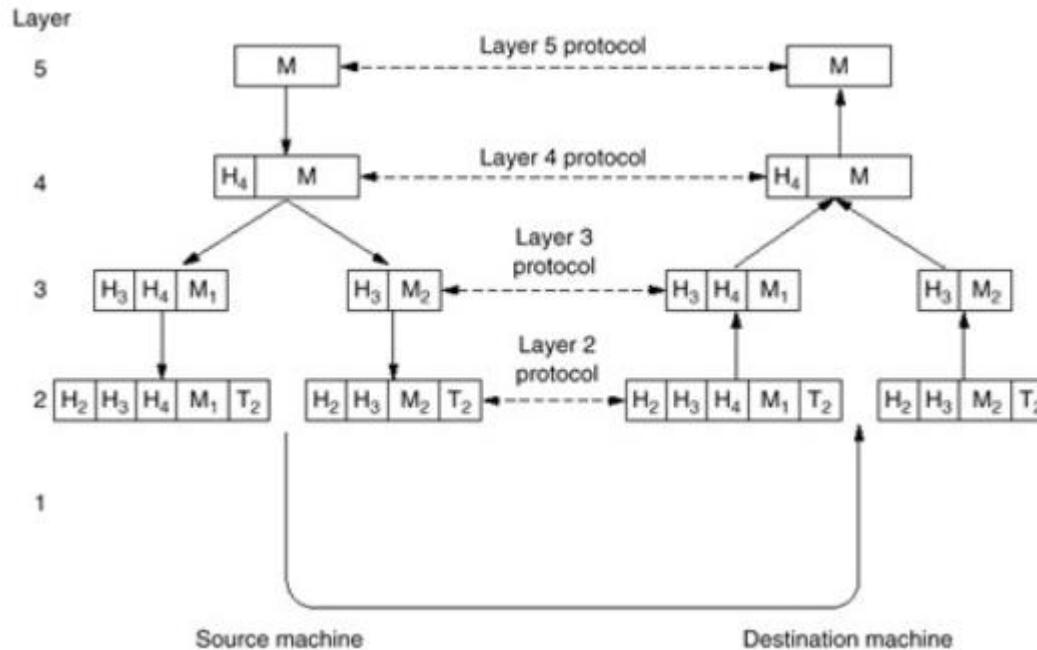
Communication entities (device/module) of two communication nodes belonging to the same communication layer.

Peer entities use the communication protocol of the same logical layer.



1. Layered network architecture

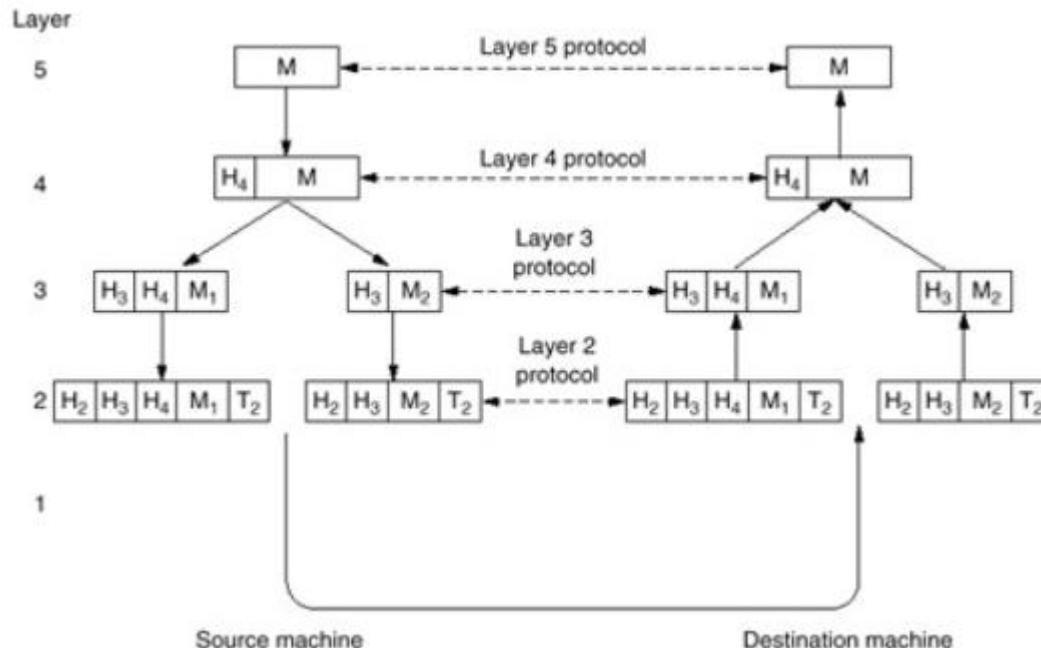
Structure of the communication mechanism:



The message is the top layer (here L5) object to be transmitted between the entities. The message is transmitted from the L5 source entity to the destination peer entity (in the same layer, L5).

1. Layered network architecture

Structure of the communication mechanism (cont'd):

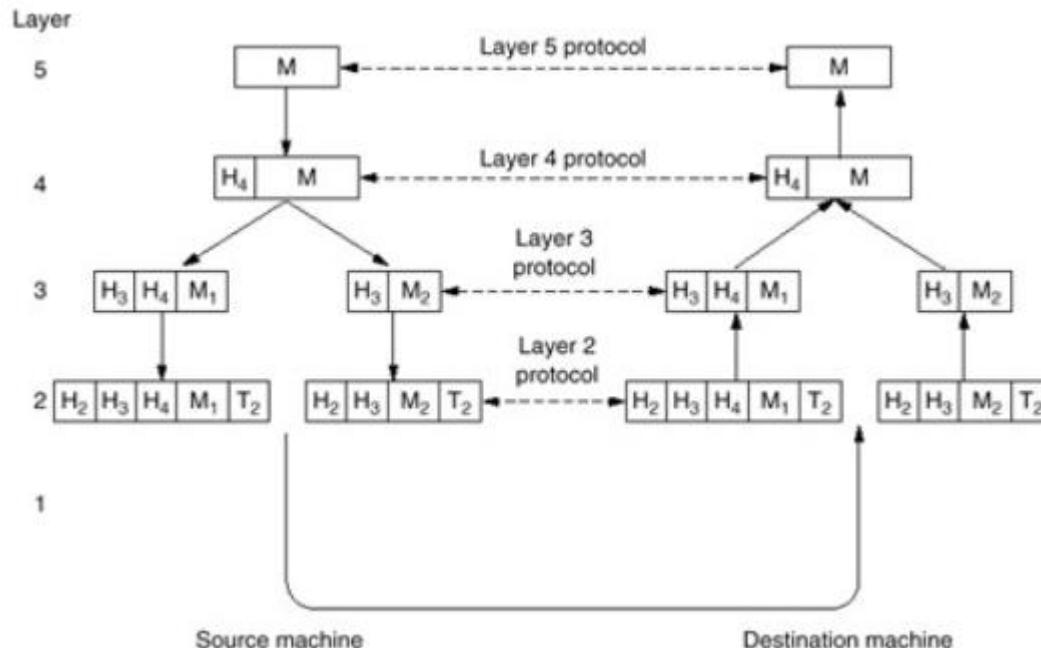


Physically the message from source L5 entity (M5) is transmitted to the source L4 entity through the L4/5 interface. L4 communication service transfers the message to the destination L4 entity. At the destination node the message is transferred from L4 entity to the L5 entity through the L4/5 interface.

Layer N entity completes the message received through LN/(N+1) interface with H (header) and eventually T (tail) fields.

1. Layered network architecture

Structure of the communication mechanism (cont'd):



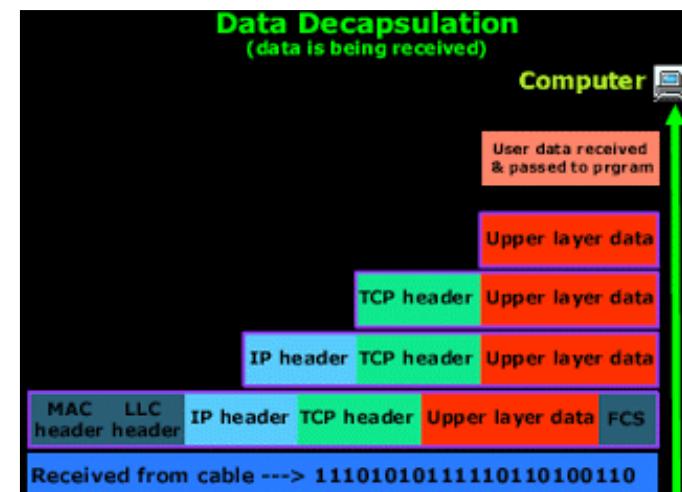
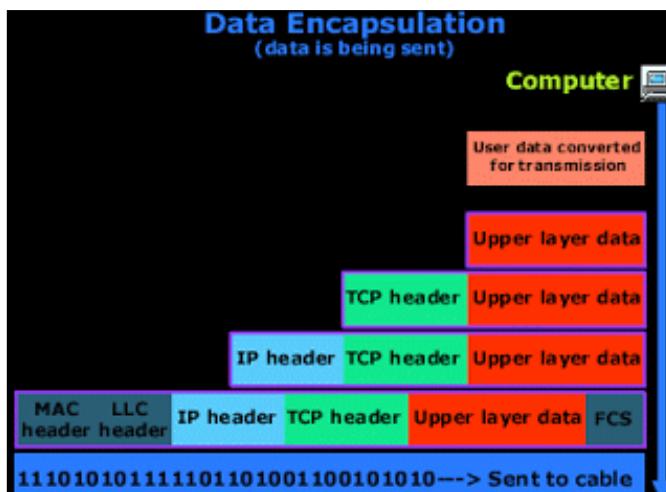
May be necessary to split the message of layer N+1 in smaller parts (fragmentation) because of the layer N message size limit (e.g. L3). Message fragments are transmitted toward the destination as individual messages. At the destination node these fragments are joined together (defragmentation) to reassemble the message of layer N+1.

1. Layered network architecture

Other communication notions:

Encapsulation, decapsulation:

The SDU received through layer N/(N+1) interface by the layer N entity is assembled (encapsulated) with header (H) and eventual tail (T) fields conform to the layer N rules. The header (H) and eventual tail (T) fields of the layer N PDU received by the destination host is disassembled (decapsulated) conform to the layer N rules. The remaining SDU is ready to be transmitted to layer N+1 entity through the interface N/(N+1) of the destination node.



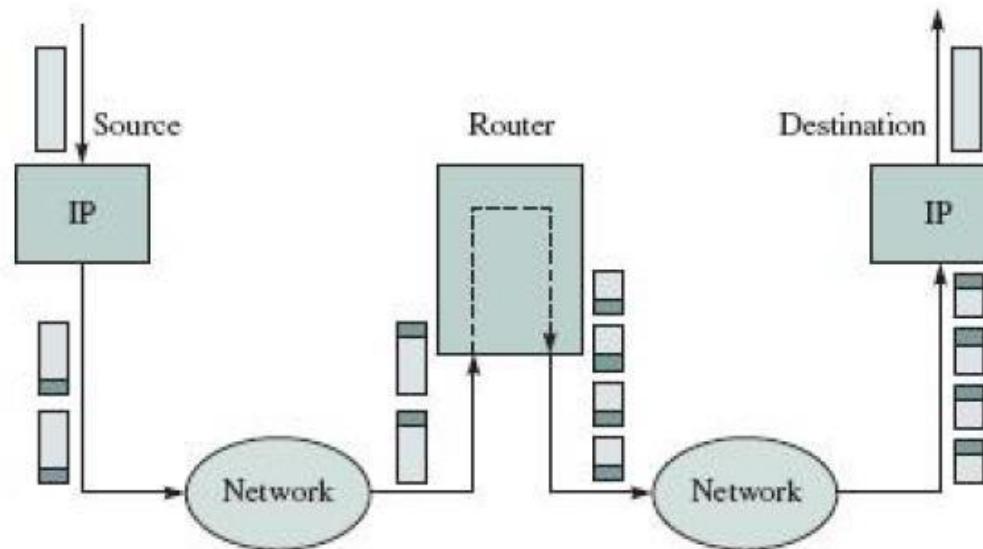
1. Layered network architecture

Other communication notions (cont'd):

Fragmentation, defragmentation (reassembly):

The SDU received through layer N/(N+1) interface is split (fragmented) into smaller pieces because of the size limit of the layer N communication service. Each SDU fragment is treated as individual SDU at the source node.

The received SDUs on layer N at the destination node are reassembled (defragmented) into the initial SDU sent by the source entity of layer N+1.

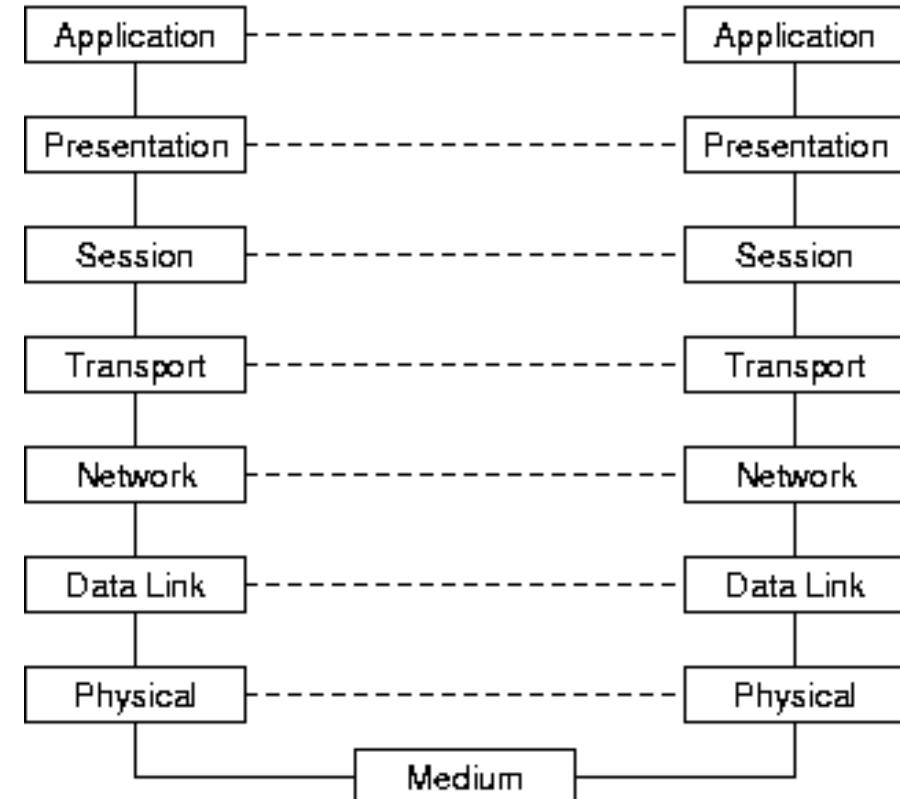


2. OSI reference model and layers

IOS OSI:

International Organisation for Standards(ISO):
Open System Interconnect (OSI)

No.	Layer name	PDU name	
7.	Application	APDU	Message
6.	Presentation	PPDU	Message
5.	Session	SPDU	Message
4.	Transport	TPDU	Segment
3.	Network	NPDU	Packet
2.	Data link	DPDU	Frame
1.	Physical	Bit	Bit



2. OSI reference model and layers

OSI Layers:

1. Physical Layer:

Electrical, mechanical, timing and geometrical characteristics of the signals, media and connectors

2. Data link Layer:

Reliable transfer of the L2 PDU (frame) between two nodes connected to the same media (wire, frequency range).

Tasks involved: physical addressing, network topology, media access control, error detection on physical layer, ordered delivery of the frames.

IEEE divided this layer into two sublayers:

- MAC: Medium Access Control sublayer (integrated into the NIC)
- LLC: Logical Link Control sublayer (device driver of the NIC)

3. Network Layer:

Provides connection and path selection (routing) between two nodes.

Tasks involved: logical addressing, routing.

2. OSI reference model and layers

OSI Layers (cont'd):

4. Transport Layer:

Provides reliable connection between two network nodes.

Tasks involved: management of the virtual circuits, detection and correction of the transmission errors, data flow scheduling.

5. Session Layer:

Sets up, schedules and releases the dialogs between the applications (session, dialog control).

6. Presentation Layer:

Conversion and alignment of the local representation of the data between different computers.

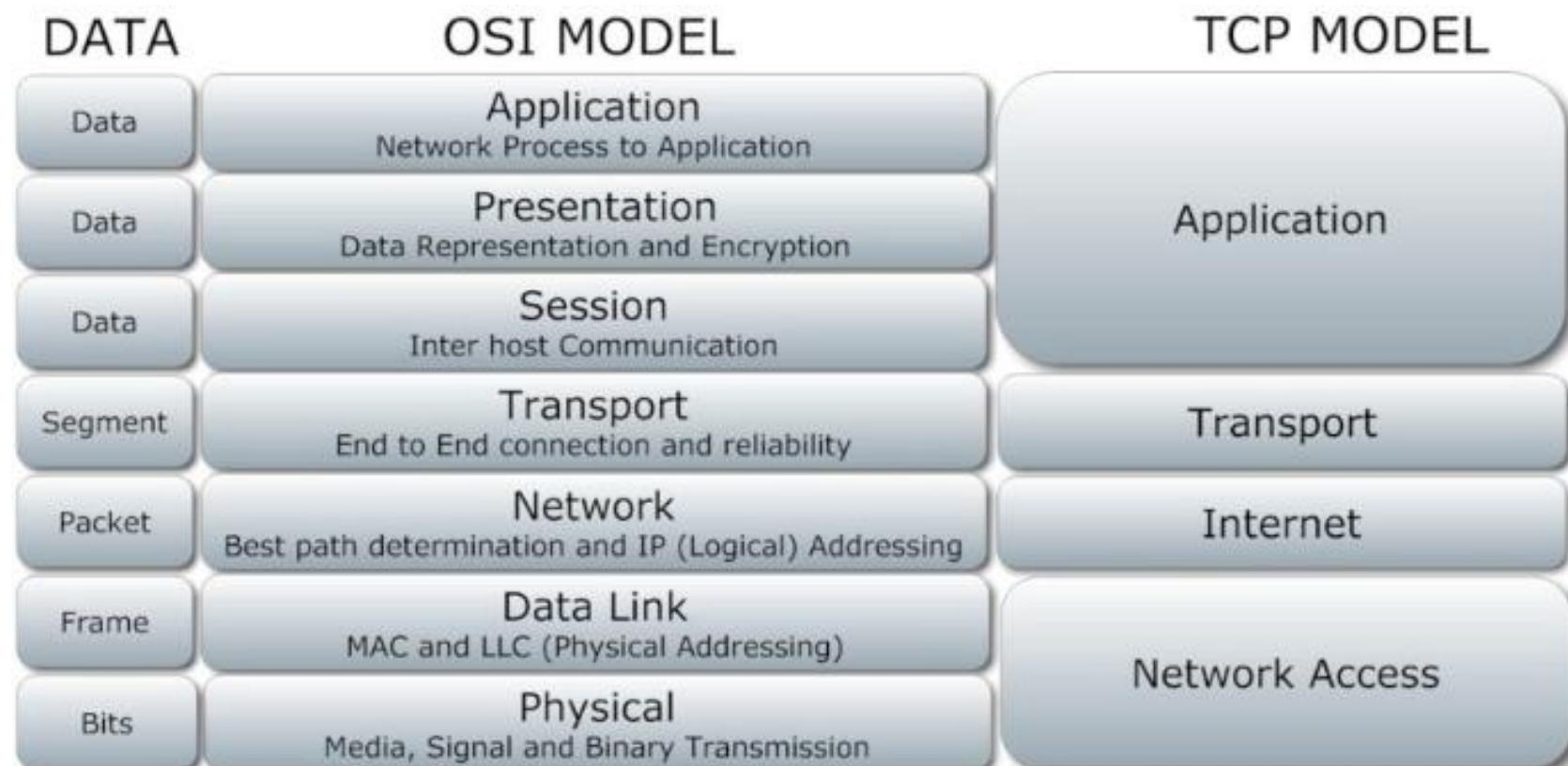
7. Application Layer:

Transfers the content between different application entities (file transfer, e-mail, etc.)

3. Mapping of the OSI, TCP/IP and Hybrid models

Considerations:

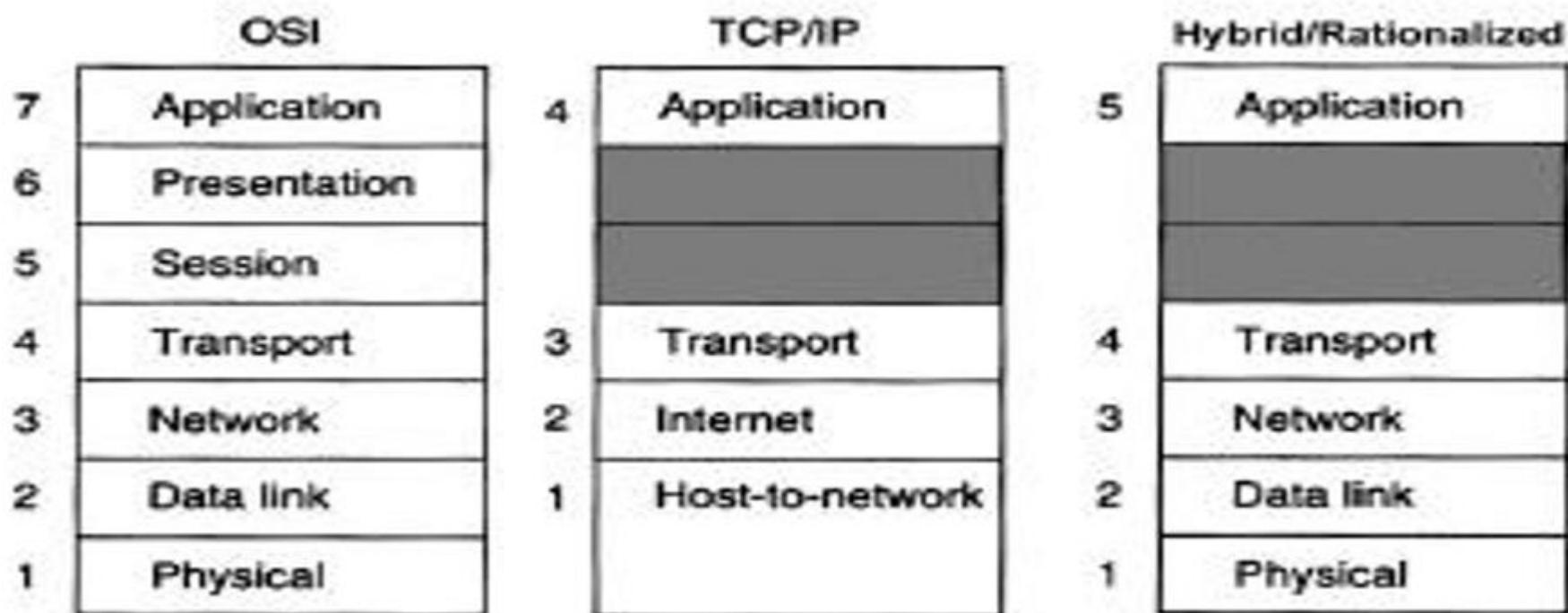
The most prevalent network technology in practice is the Internet based on the TCP/IP protocol system. The TCP/IP model differs from the OSI model.



3. Mapping of the OSI, TCP/IP and Hybrid models

Considerations:

A. S. Tanenbaum in his famous book (Computer Networks) proposes a Hybrid/Rationalized model: The lower two layers of the OSI model and the upper three layers of the TCP/IP model are used. In the rest of this course we use Hybrid/Rationalized network reference model.

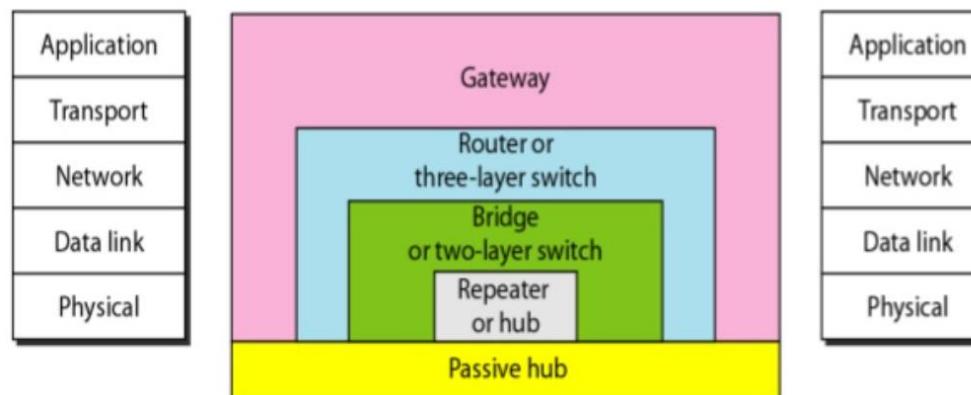


4. Intermediate node types

Considerations:

Connection of the different network component are provided by devices belonging to different OSI layers. The classification of these intermediate nodes (devices) is made by the functions of the devices.

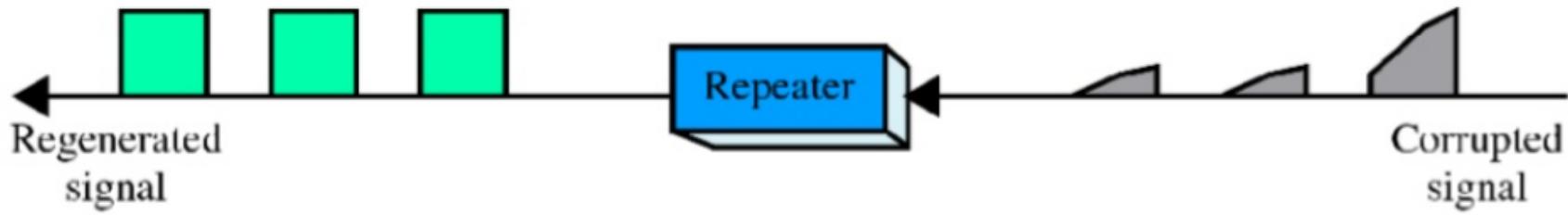
Layer	Intermediate Node (Device)
Application, Transport	Gateway
Network	Router
Data Link	Bridge, Switch
Physical	Repeater, Hub



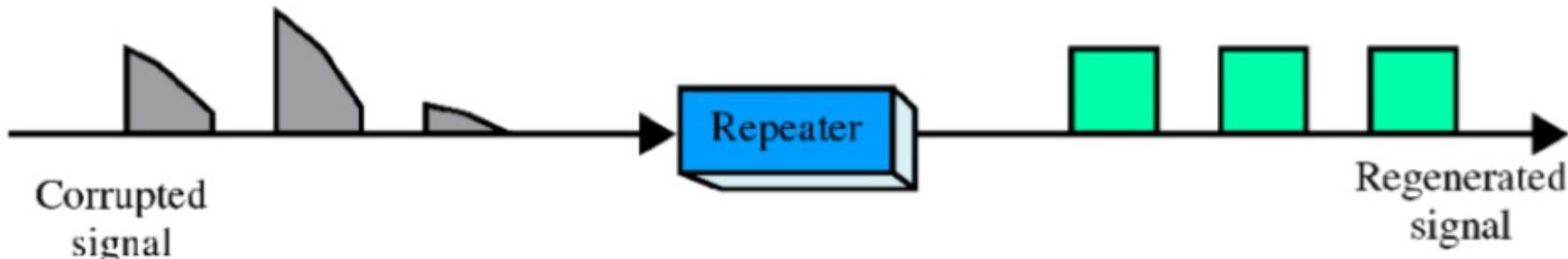
4. Intermediate node types

Repeater, Hub:

- Active Hub: transmits the signal on the media: reamplification, retiming, resynchronizing, reshaping of the pulses.
- Passive Hub: analogue amplifier without just reamplification.



(a) Right-to-left transmission.

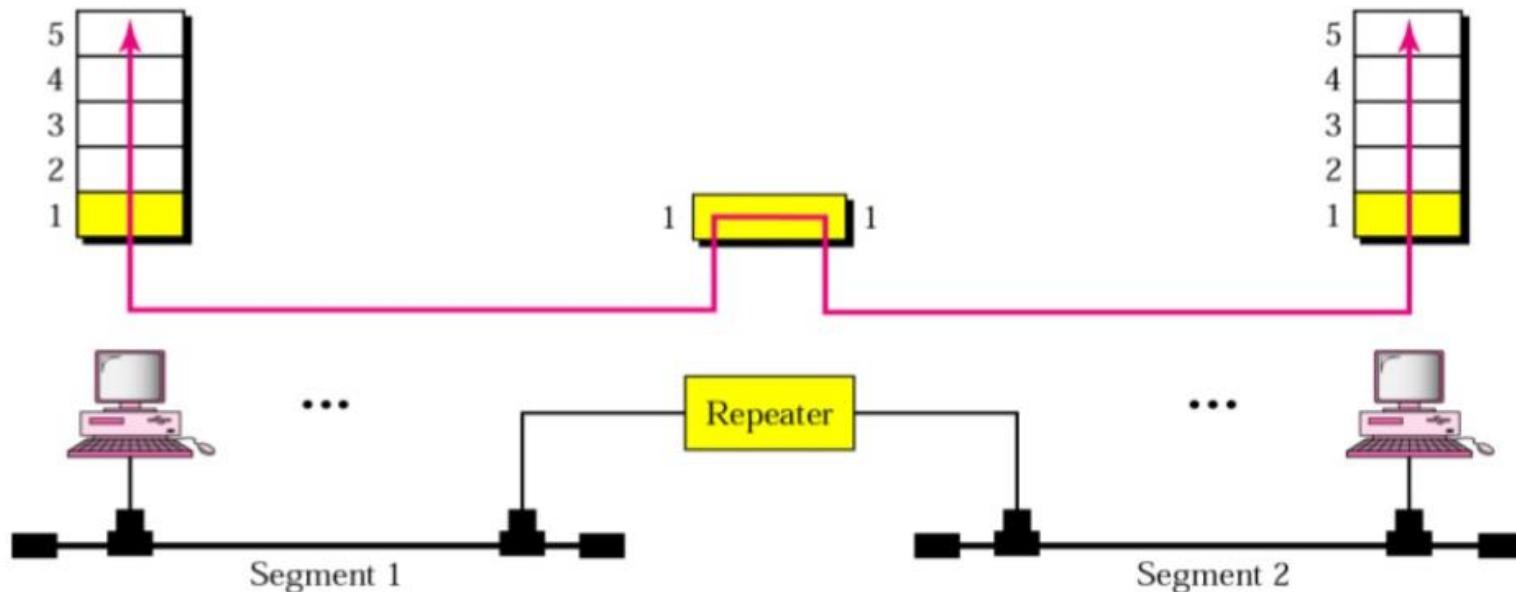


(b) Left-to-right transmission.

4. Intermediate node types

Repeater, Hub (cont'd):

- Connects multiple nodes in L1.
- Transmits the signal on the media: reamplification, retiming, resynchronizing, reshaping of the pulses.

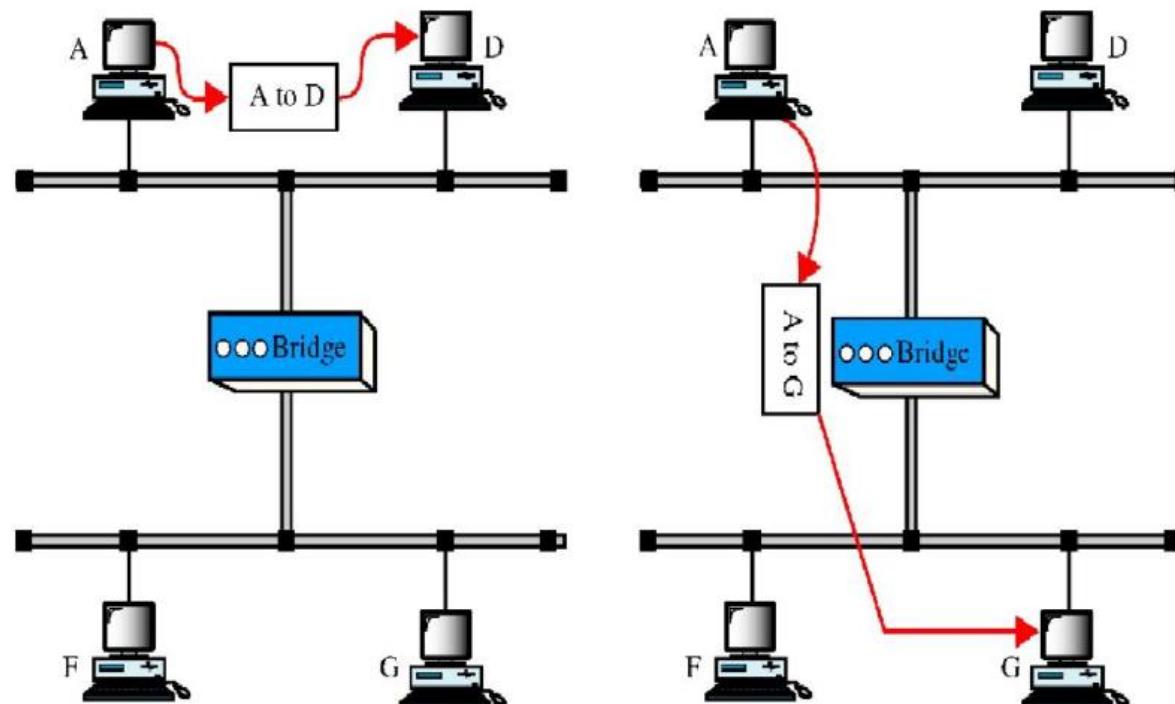


**A repeater connects segments of a LAN.
A repeater forwards every frame – there is no filtering.
A repeater is a regenerator, not an amplifier.**

4. Intermediate node types

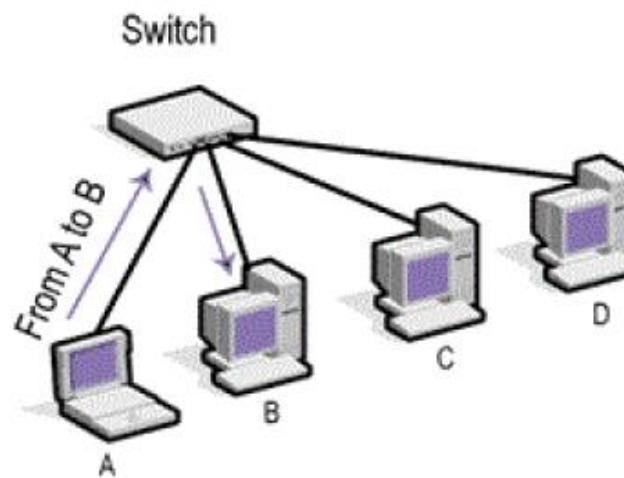
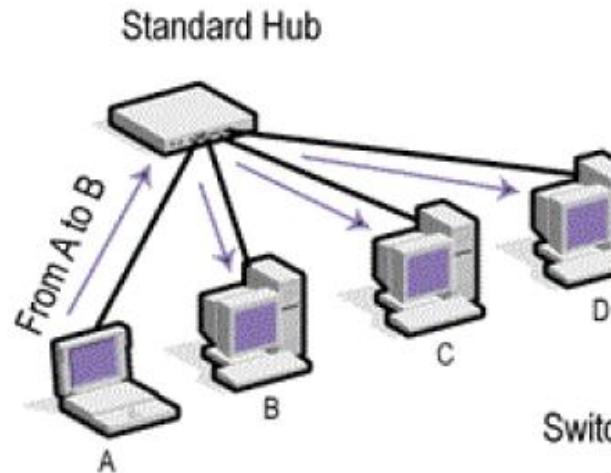
Bridge, Switch:

- Connects two or multiple nodes on different media (segments, collision domains) in L1 and L2.
- Learns transparently the source physical address of the devices and transmits the frame only to the corresponding destination node.
- Bridge: service executed by software (one CPU, old device)
- Switch: se



4. Intermediate node types

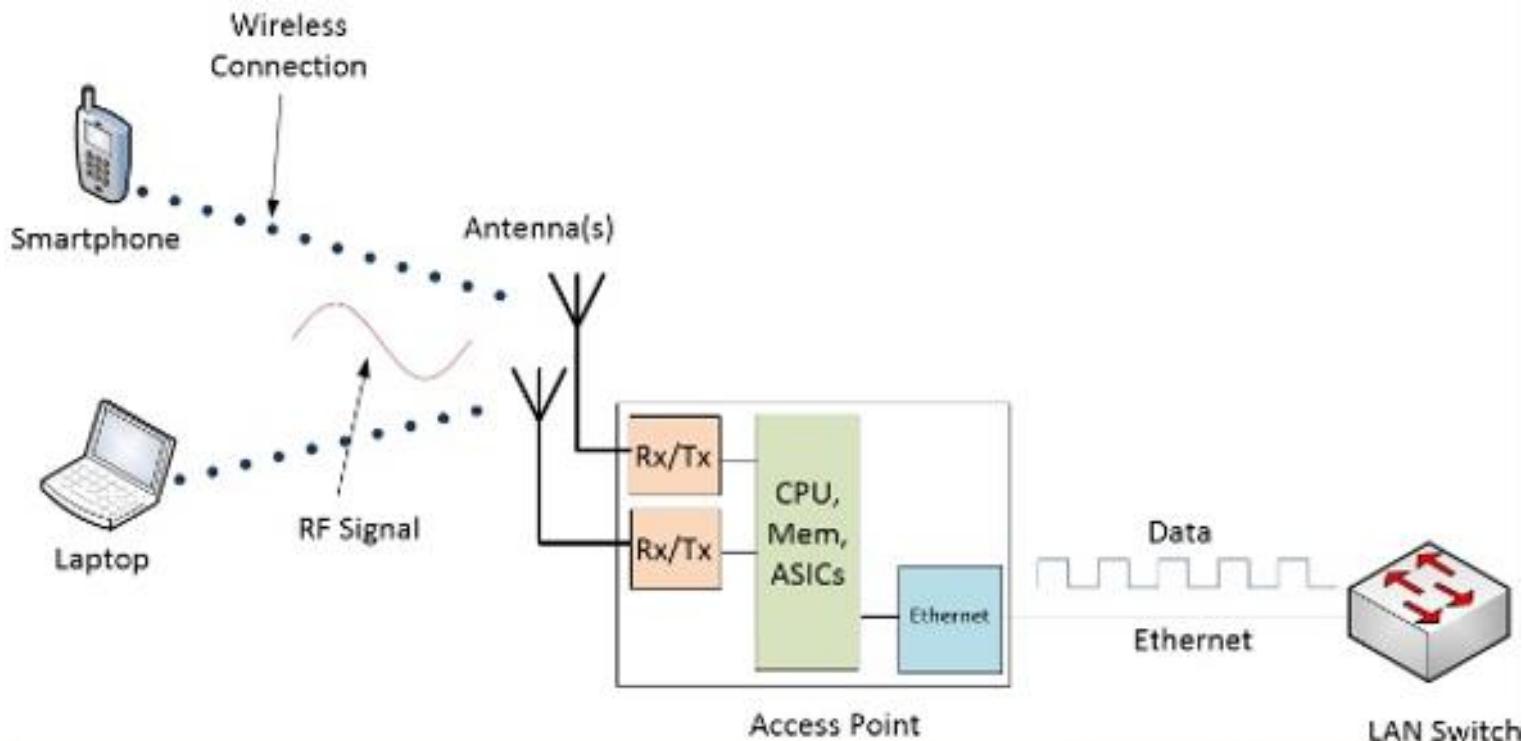
Repeater/Hub vs. Bridge/Switch:



4. Intermediate node types

Wireless Access Point (AP):

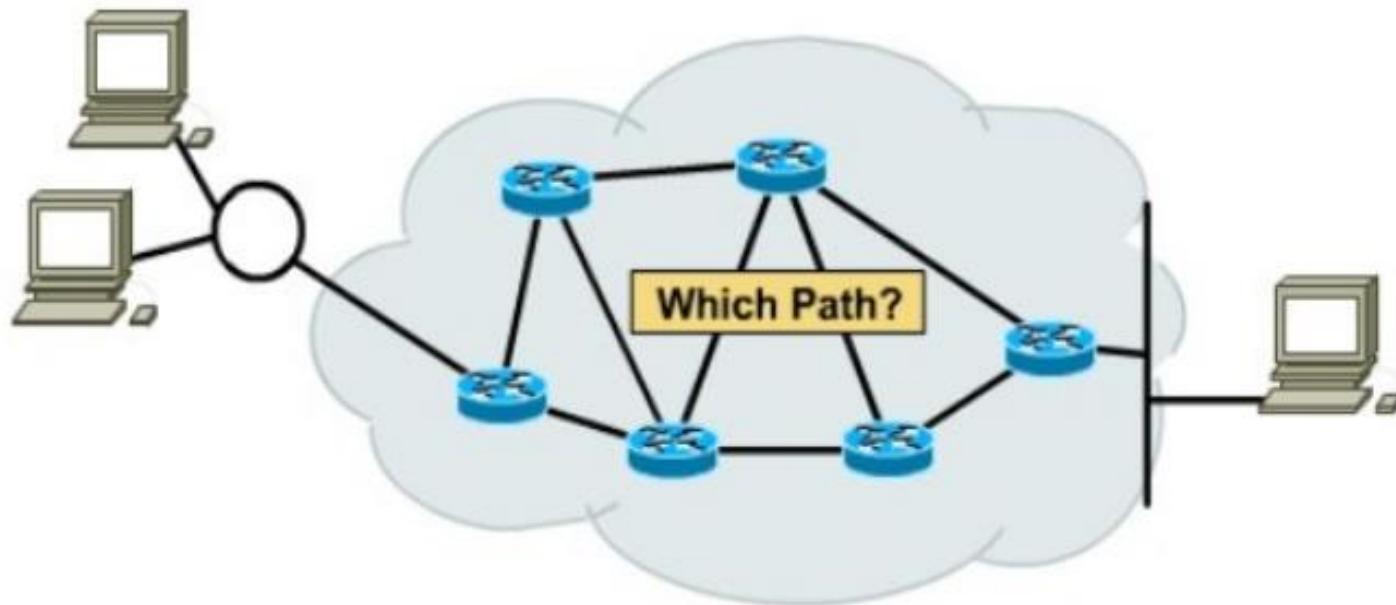
- Provides special bridging: wired port <-> wireless port.
- Forwards frames, but not bits.
- The frame is transformed during the transmission through the AP



4. Intermediate node types

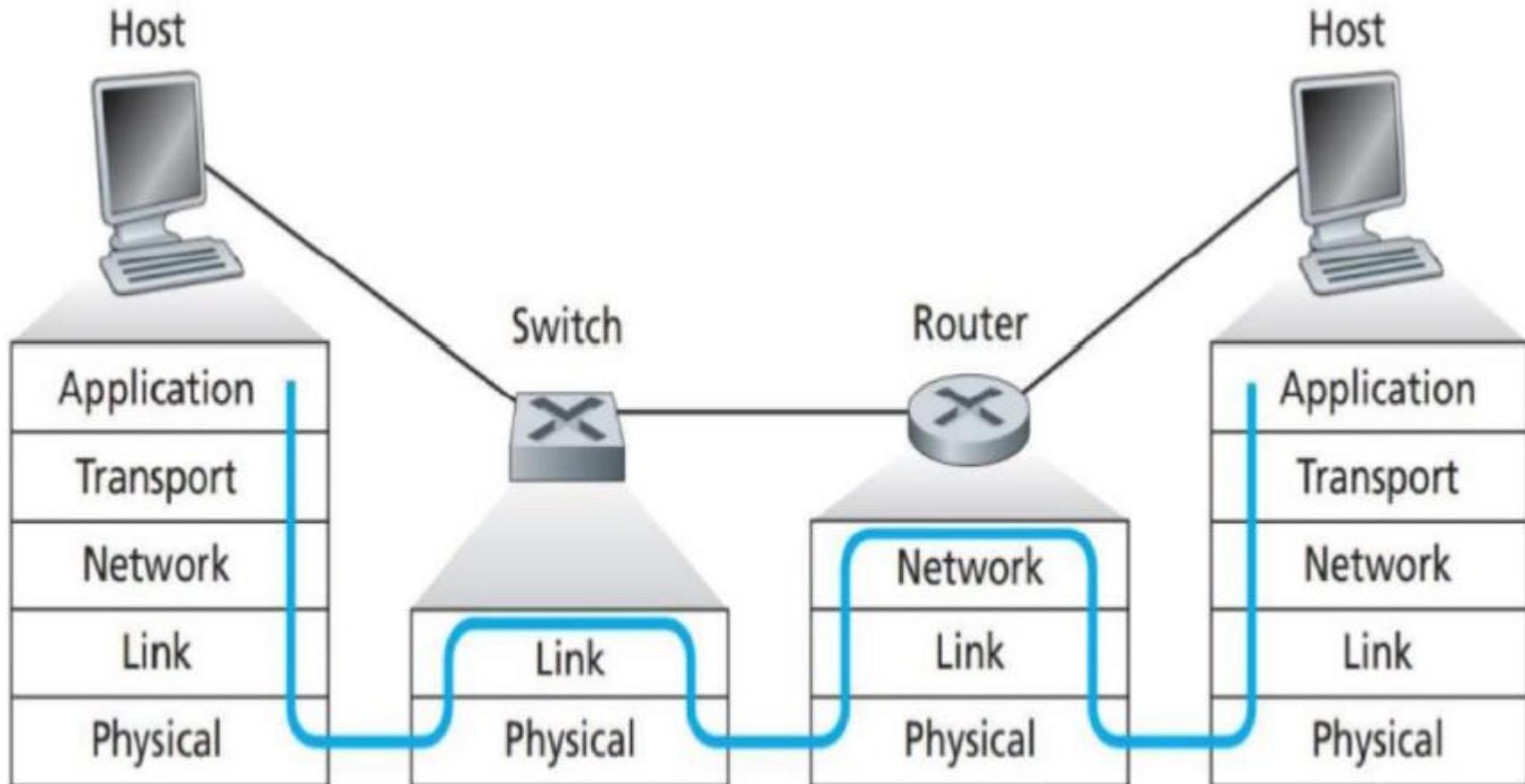
Router:

- Connects multiple nodes in L3 and L2 and L1 (broadcast domains).
- Forwards packets, does not forwards frames or bits.
- Executes routing in network layer.
- Each interface has unique physical and unique logical address.



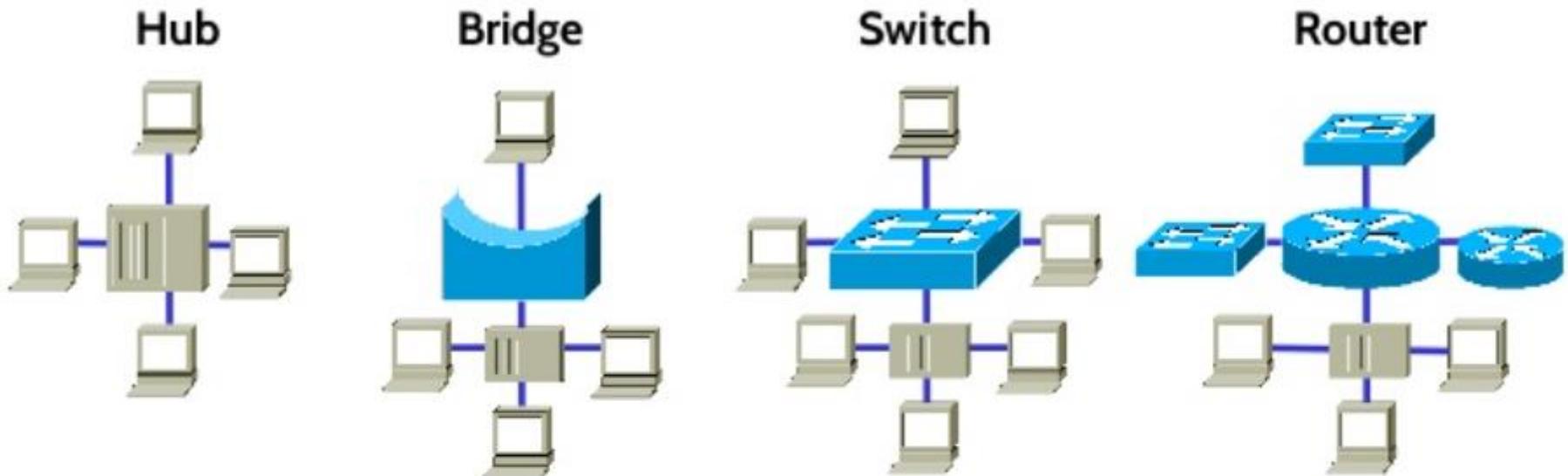
4. Intermediate node types

Switch vs. Router:



4. Intermediate node types

Hub vs. Bridge vs. Switch vs. Router:



Collision Domains:

1

2

4

4

Broadcast Domains:

1

1

1

4

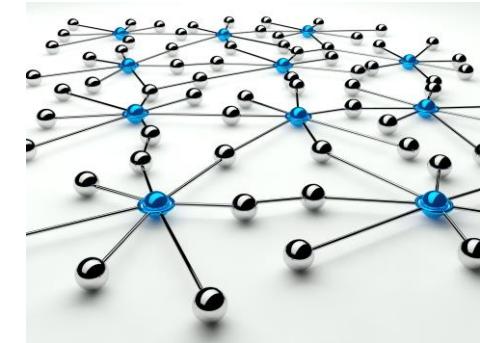
Networks Architectures and Protocols

3. PHYSICAL LAYER

Lecturer: Zoltán Gál, PhD

Faculty of Informatics, University of Debrecen

February 05, 2018



Outline

- 1) General characteristics of the Physical layer
- 2) Transmission media types
 - Wired media: twisted pair, coaxial cable
 - Wireless media: air, RF channel
- 3) Signal encoding technics
- 4) Modulation technics

1. General Characteristics of the Media

Considerations:

- Signal transmitted as a pulse on the media wastes energy during the propagation.
- The channel (media) absorbs energy (attenuates signal) depending on the frequency.
- The quality of the received signal depends on the other signals simultaneously propagated on the media.
- Each channel has upper limit of the transmission rate of the impulses (bit/sec), depending on the channel physical characteristics.

Upper limit of the channel transmission rate without noise:

Nyquist theorem of the channel upper transmission rate limit.

$$C = 2 \cdot H \cdot \log_2(V)$$

where:

C – upper limit of the transmission rate [bit/sec],
H – bandwidth (frequency domain) of the channel [Hz],
V – No. of discrete levels of the signal.

1. General Characteristics of the Media

Noise:

- Sum of the simultaneous energy impulses from other sources than the sender node is the noise.
- If the signal level is comparable with the noise level, then decoding of the information forwarded by the signal is impossible or affected by errors.
- For good reception quality the signal/noise (S/N) ratio should be as high as possible.

Upper limit of the channel transmission rate with noise:

Shannon theorem of the channel upper transmission rate limit

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

where:

- C – upper limit of the transmission rate [bit/sec],
- H – bandwidth (frequency domain) of the channel [Hz],
- S – Power of the signal [W]
- N – Power of the noise [W]

1. General Characteristics of the Media

Attenuation (A):

- Ratio of the transmitted and received signal power.
- For a signal to be received a minimum level of power is required at the sink device.
- For higher distances passive or active repeater is necessary.
- The attenuation is dependent on the frequency.
- Unit of measurement: dB (decibel)

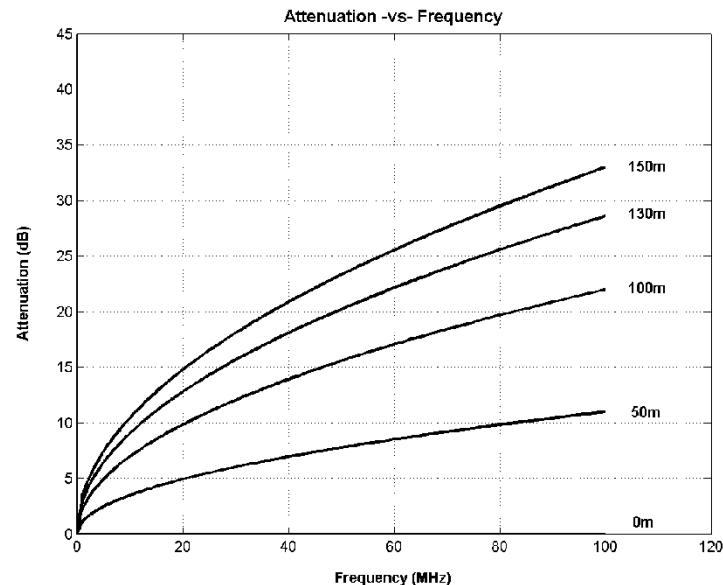
$$A = 10 \cdot \log_{10}(P_R/P_T)$$

where:

A – Attenuation [dB],

P_R – Received power [W],

P_T – Transmitted power [W]



1. General Characteristics of the Media

Signal propagation velocity (v):

- The velocity of the signal transmitted on the channel depends on the media characteristics:

$$v = \lambda \cdot f$$

where:

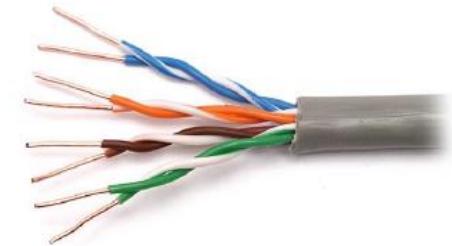
v – velocity of the signal on the media [m/s],
 λ – wavelength of the signal [m],
 f – frequency of the signal [Hz]

Media types:

Signal	Media Type	Physical aspect	v [m/s]
Electrical impulse	Galvanic wire	wire	$\sim 3 \cdot 10^8$
Optical impulse	Optical wire	wire	$\sim 3 \cdot 10^8$
Mechanical impulse	Air	wireless	~ 340
Electromagnetic wave	Electromagnetic space	wireless	$\sim 3 \cdot 10^8$

2. Transmission media types

Wired media (galvanic):



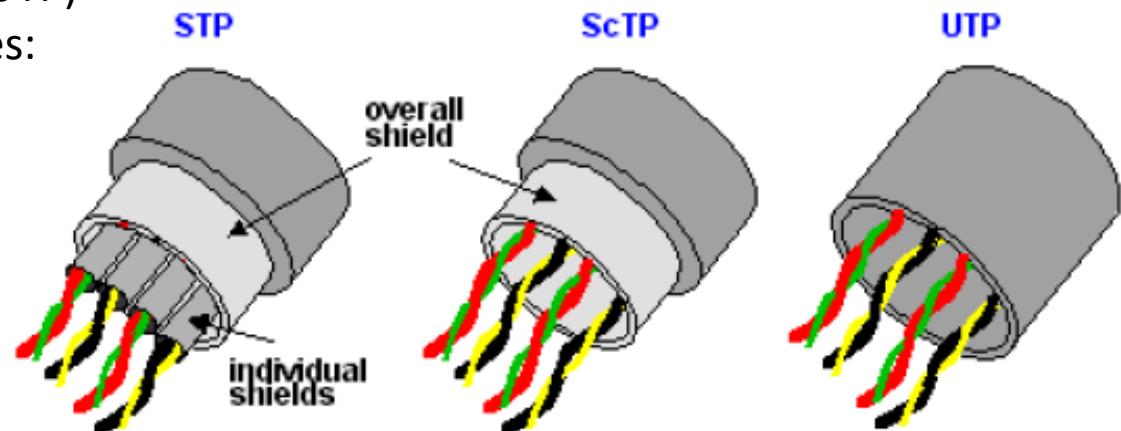
1. Twisted Pair:

- Cheap, very popular media in LAN/MAN/WAN environment.
- Pair: two conductor with own insulator twisted (wire diameter $\sim 0.4 - 0.8$ mm)



- Cable: four pairs of wire in a common insulator
- Variants:

- Unshielded Twisted Pair (UTP)
- Shielded Twisted Pair types:
 - ScTP (Screeend TP)
 - FTP (Foiled TP)
 - STP (Shielded TP)



2. Transmission media types

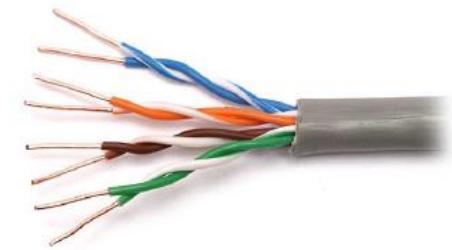
Wired media (galvanic):

1. Twisted Pair (cont'd):

- Role of the twisting: cancellation of the noises



- Influence of a given pair to other pair: crosstalk (near end, far end)
- Electric insulation between the pairs filters out the crosstalk (STP): best, but expensive
- Cable categories (classes): max. frequency, and max. transfer rate.
- Max. length in LAN environment: 100 m



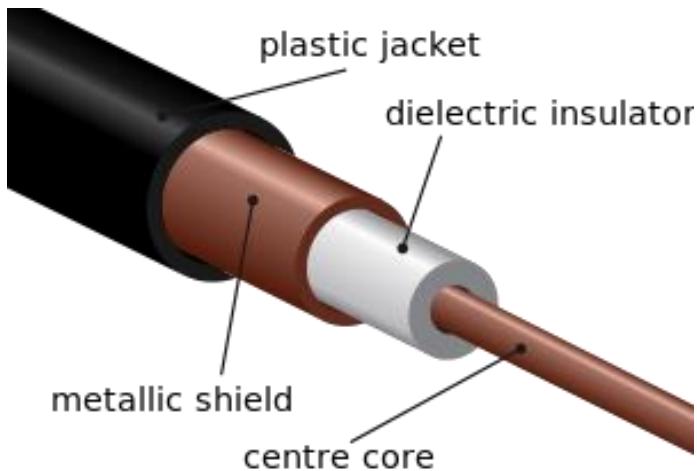
Category (USA)	Class (EU)	Frequency band [MHz]	Transmission rate [Mb/s]
Cat 3	Class C	16	100
Cat 5/5e	Class D	125	100/1,000 on 2/4 pairs
Cat 6	Class E	250	1,000 on 2 pairs
Cat 6A	Class EA	500	10,000
Cat 7	Class F	600	10,000

2. Transmission media types

Wired media (galvanic):

2. Coaxial cable:

- Concentric structure
- Role of the twisting: cancellation of the noises



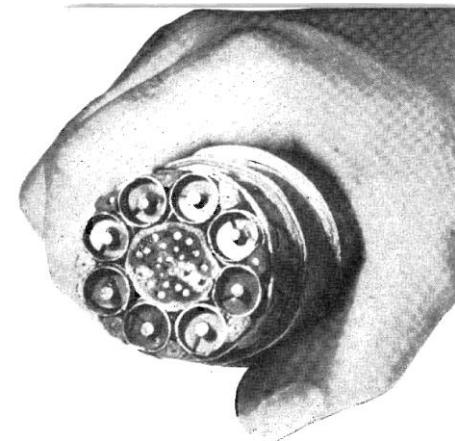
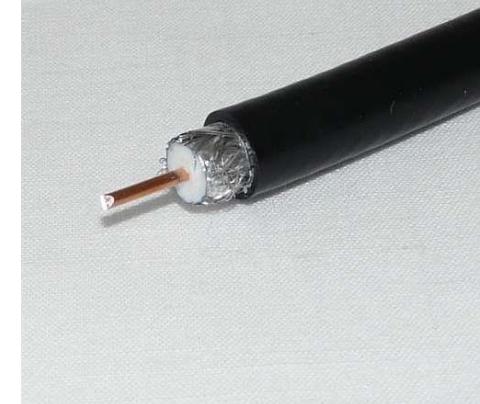
- External diameter size:
 - Thin coaxial cable: 5 mm
 - Thick coaxial cable: 25 mm (thick dielectric insulator)

2. Transmission media types

Wired media (galvanic):

2. Coaxial cable (cont'd):

- Has superior noise immunity (better than the TP)
- Can be used for higher distances, reamplification at $n \cdot km$
- Has multipoint access usage possibility
- Impedance (frequency dependent):
 - Baseband: 50Ω (digital signal transmission)
 - Broadband: 75Ω (analogue signal transmission, CATV)
- Frequency band: ~ 600 MHz
- It was used at the beginning of the LAN services, today TP is used instead:
 - RG-62: 93Ω (Arcnet, 1970's)
 - RG-58: 50Ω (Ethernet, 1980's)
- Today is used for antenna connection to the receiver or transmitter.



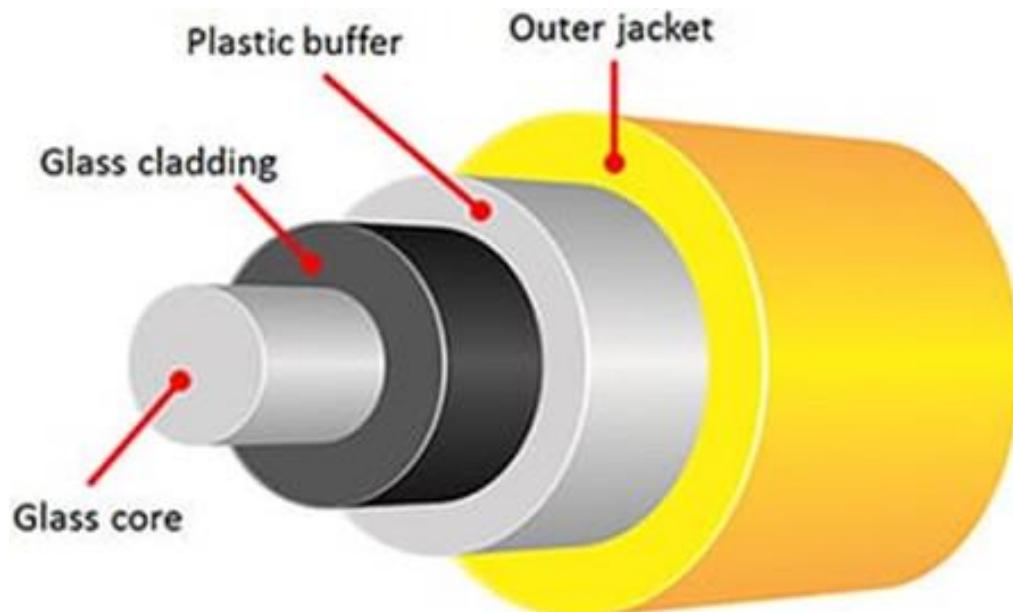
1948 (480 telephone calls,
one television channel)

2. Transmission media types

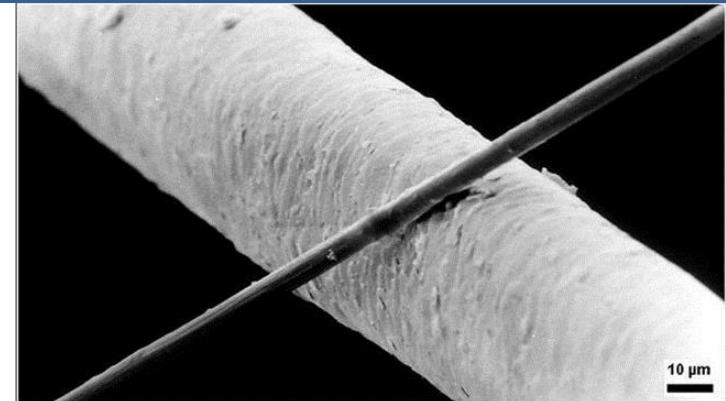
Wired media (optical):

3. Fibre cable:

- Light signal transmission
- Structure:



- Core diameter: d
- Cladding diameter: D

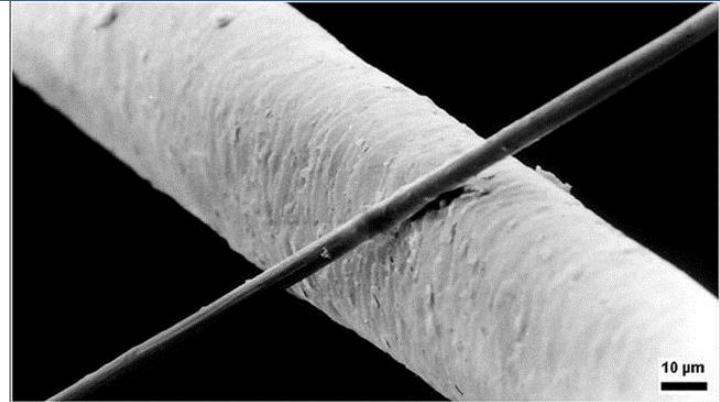


2. Transmission media types

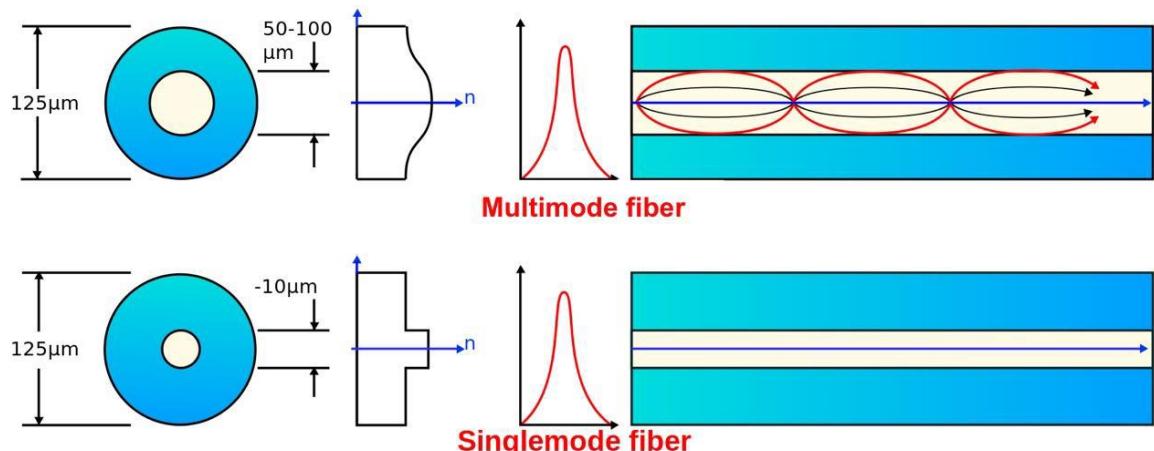
Wired media (optical):

3. Fibre cable (cont'd):

- One fibre: multiple optical simultaneous channels
- Usually pair of fibres are used for Tx and Rx
- Light transmission in the fibre
 - MMF (Multimode Fibre)
 - SMF (Single mode Fibre)



	MMF	SMF
D [μm]	125	125
d [μm]	50; 62.5	9.5
λ [μm]	0.85	1.31; 1.55

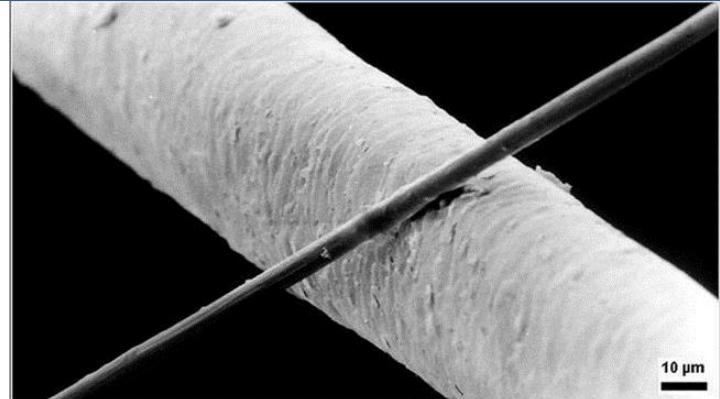


2. Transmission media types

Wired media (optical):

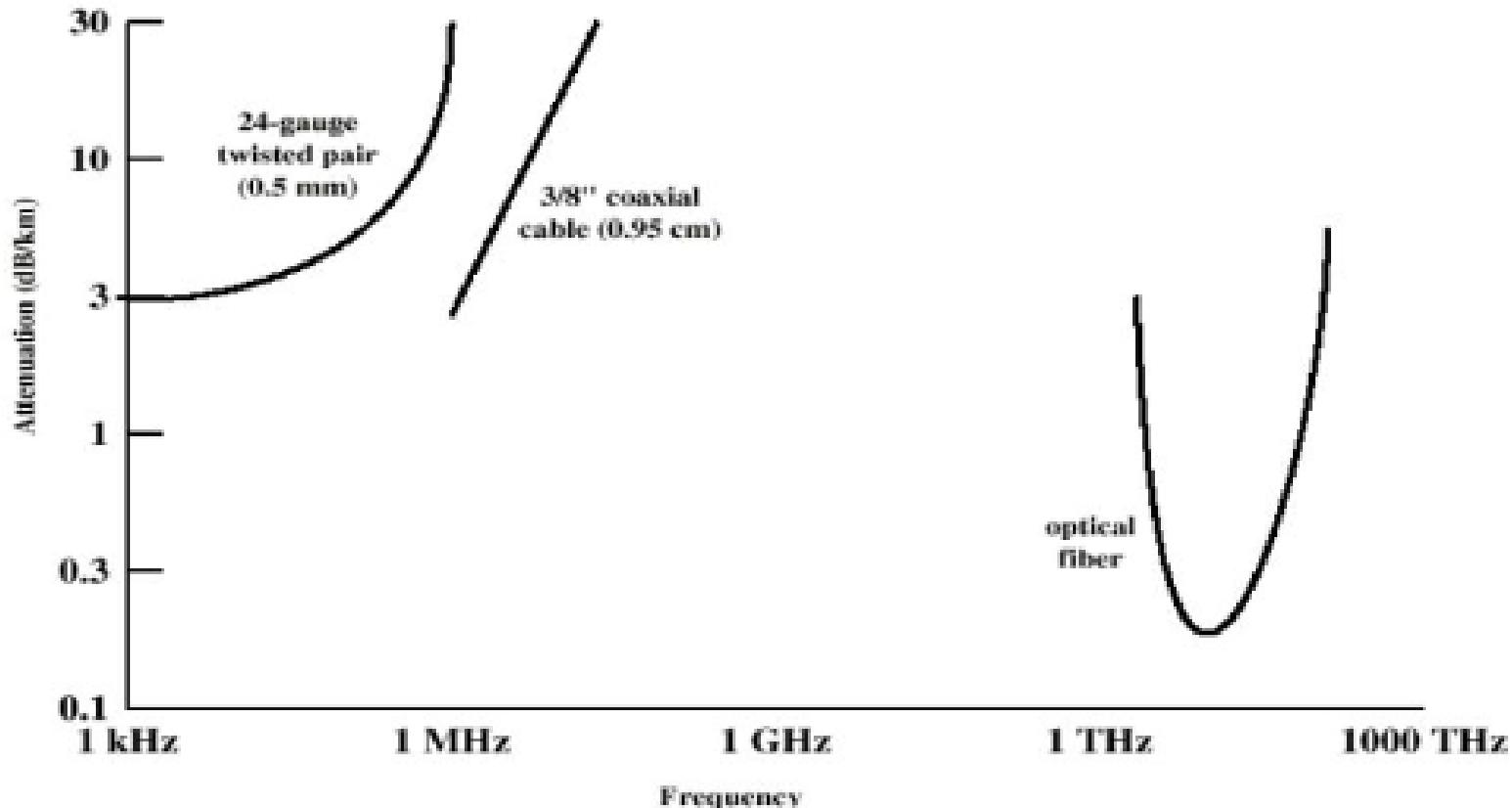
3. Fibre cable (cont'd):

- High transfer rate \times distance product:
 $n \cdot 100 \text{ Gbps} \cdot \text{km}$
- Lower mass than the galvanic cables
- Low attenuation, high frequency range
- Exterior EM noises are not collected
- EM noises are not radiated -> signals can not be intercepted
- Low error rate, low maintenance cost.



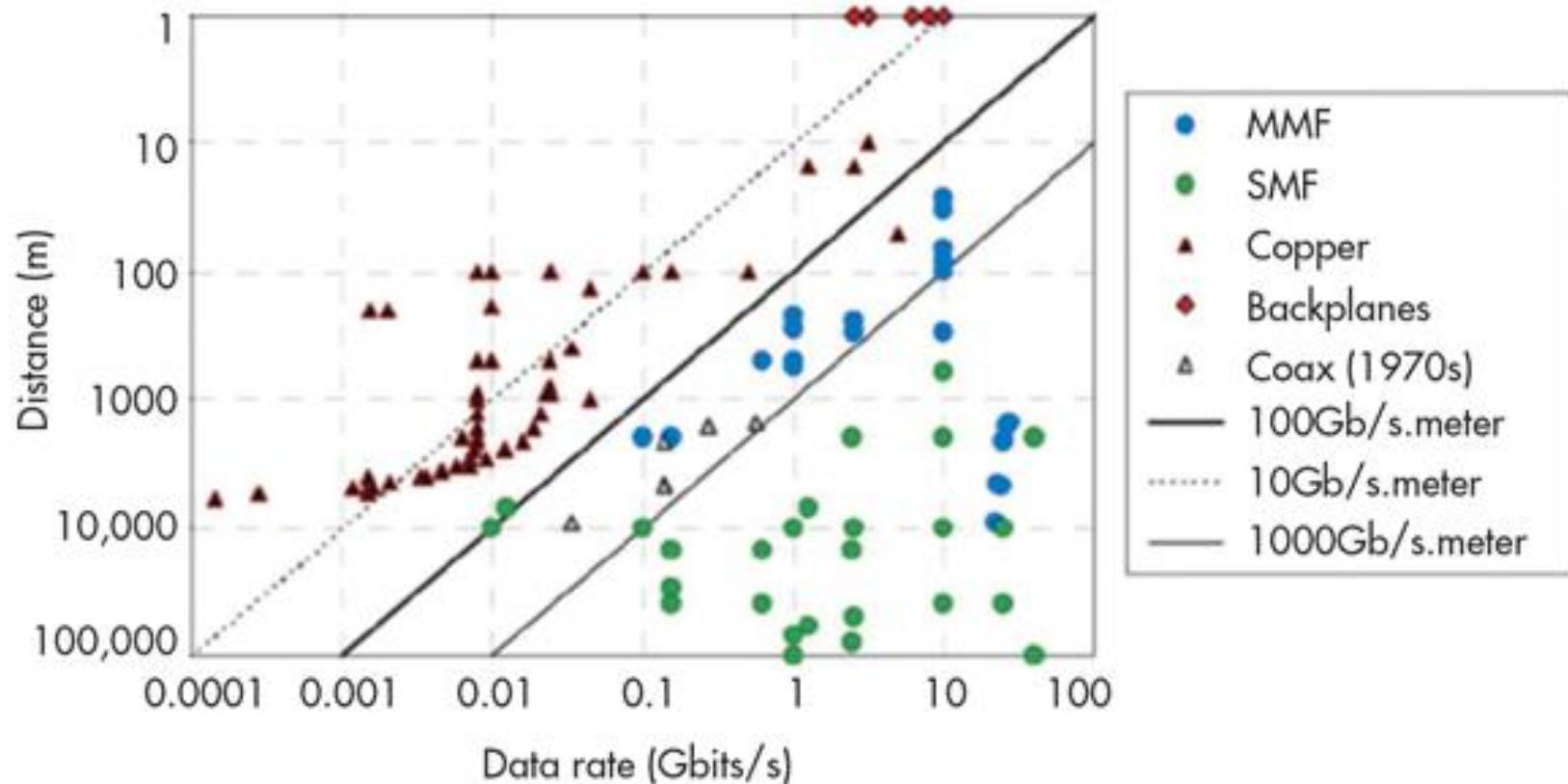
2. Transmission media types

Relative attenuation (A) of the wired media:



2. Transmission media types

Distance x Transmission Rate product of the wired media:



2. Transmission media types

Wireless media (air):

4. Air:

- Mechanical (voice) wave transmission
(movement of the gas molecules)
- Factors influencing the voice velocity:
 - Gas type
 - Pressure of the gas
 - Temperature of the gas
- Velocity of the voice in air: ~ 340 m/s
- Human ear sensing frequency range: 20 ... 20,000 Hz (300 ... 12,000 Hz)
- Human tape frequency range: 50 ... 3,520 Hz (300 ... 3,400 Hz)
- Infra frequency voice: $f < 20$ Hz (fishes, mole)
- Ultra frequency voice: $f > 20$ kHz (bat, dog)
- Application of the voice signal communication
 - Human-human,
 - Human-machine,
 - Machine-human



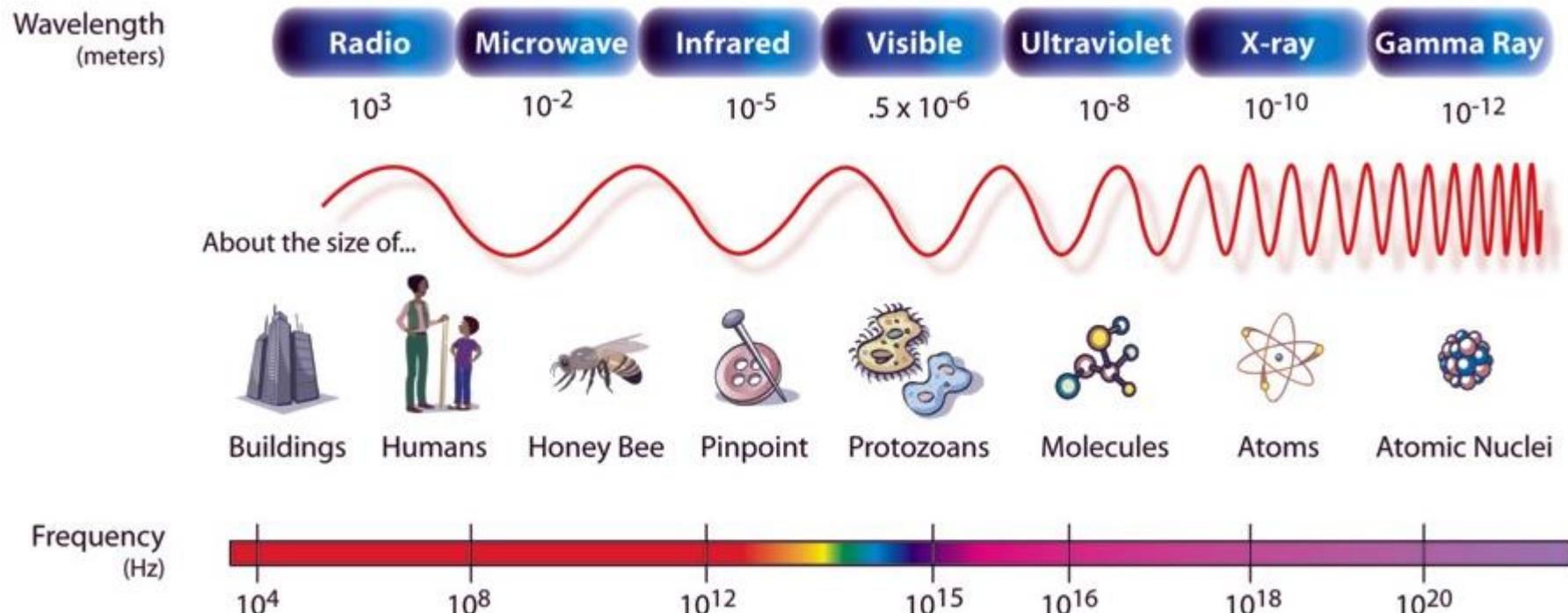
2. Transmission media types

Wireless media (RF):

5. Radio frequency wave:



$$S_i(t) = A_i \cdot \sin(2\pi \cdot f + \varphi_i), \quad S(t) = \sum_{i=0}^n S_i(t), \quad n \in \mathbb{N} \text{ and finite}$$



2. Transmission media types



Wireless media (RF):

5. Radio frequency wave (cont'd):

- Factors affecting the EM wave attenuation
 - Frequency of the signal
 - Distance
 - Physical environment geometry
- Classification in function of the covered area:
 - Unidirectional: between two antennas
 - Sector: inside of a solid angle
 - Omnidirectional: in each direction
- Classification in function of the number of frequency components:
 - Baseband: tight frequency band ($n = 1$)
 - Narrowband: small frequency band (n is small)
 - Broadband: large frequency band (n is high)
- Technologies in practice:
 - Telecommunication (GSM, LTE, 5G, ...)
 - Data networks (WiMax, WiFi, BT, RFID, NFC, ...)

3. Signal encoding technics

Signal coding:

- The bit stream on the physical layer is mapped to the digital symbol pattern of the channel (levels, level changes). The signal level depends on the media type and can be electrical voltage, light intensity, wave amplitude, etc.

Unipolar coding:

- Two signal level exist: (+V) and (0) symbols.

Bipolar coding:

- Two signal level exist: (+V) and (-V) symbols.

Synchronous/asynchronous transmission:

- The receiver receives a continuous stream of data in the form of signals accompanied by regular timing signals. The timing signals are generated by a clocking mechanism to ensure synchronization between the sender and receiver.

Asynchronous transmission:

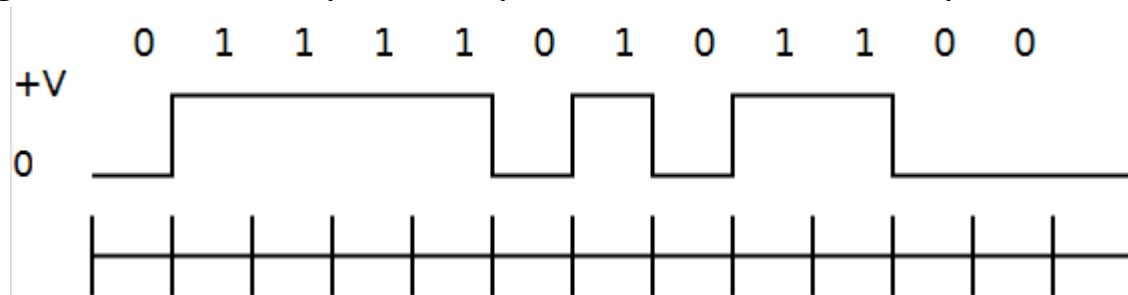
- Start and stop symbols are used at the beginning and ending of the each data. These two signals have opposite polarity. The receiver understands the new data arrival.

3. Signal encoding techniques

1. NRZ (Non-Return to Zero) Encoding: unipolar levels

„0” bit: low level during the bit time. „1” bit: high level during the bit time.
Level change is at the beginning of bit time. Simple to implement, but does not provide synchronization for a stream of identical bits.

E.g.:

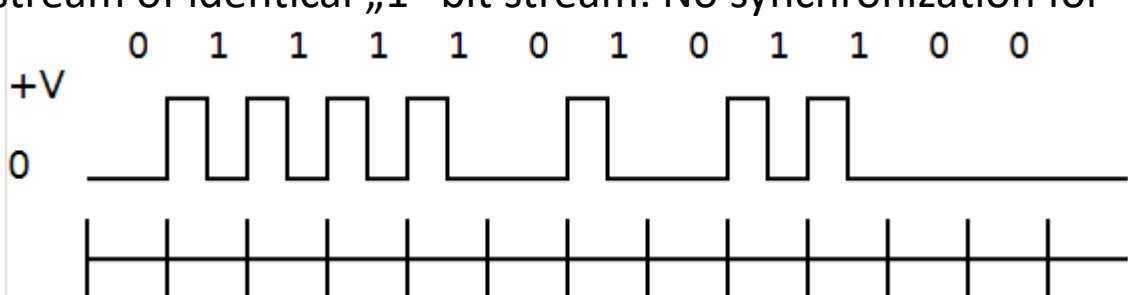


2. RZ (Return to Zero) Encoding: unipolar levels

„0” bit: low level during the bit time. „1” bit: high level during the first half of bit time, then low level for the second half of bit time.

Provides synchronization for a stream of identical „1” bit stream. No synchronization for a stream of identical „0” bit stream. Bit stuffing.

E.g.:



3. Signal encoding techniques

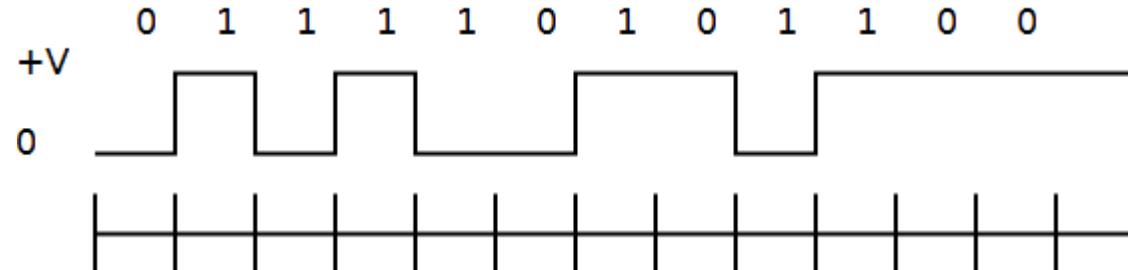
3. NRZI (Non-Return to Zero Invert on One) Encoding: unipolar levels

„0” bit: unchanged level during the bit time.

„1” bit: level change at the beginning of the bit time.

Bit stuffing/de-stuffing.

E.g.:



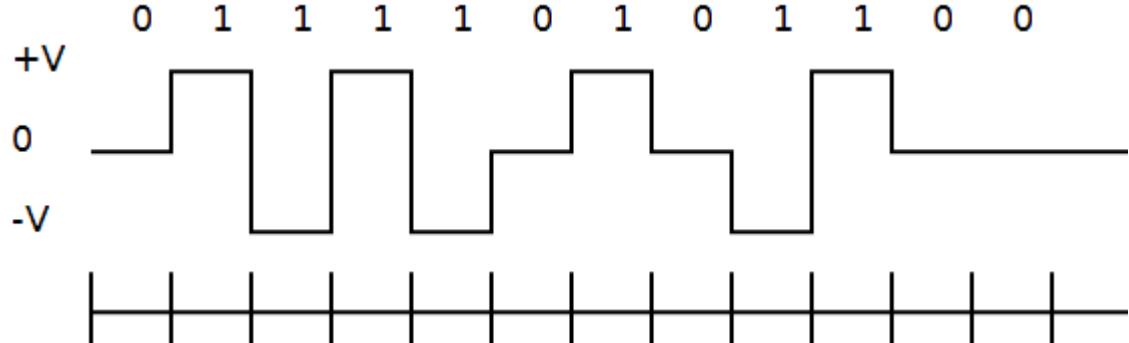
4. AMI (Alternate Mark Inversion) Encoding: bipolar levels

„0” bit: low level during the bit time.

„1” bit: following „1” bit gets opposite level during the bit time.

Bit stuffing/de-stuffing.

E.g.:



3. Signal encoding techniques

5. Manchester Encoding (PE – Phase Encoding): unipolar/bipolar levels

„0” bit: negative level change at the half of the bit time.

„1” bit: positive level change at the half of the bit time.

Provides continuous synchronization, but requires double baud.

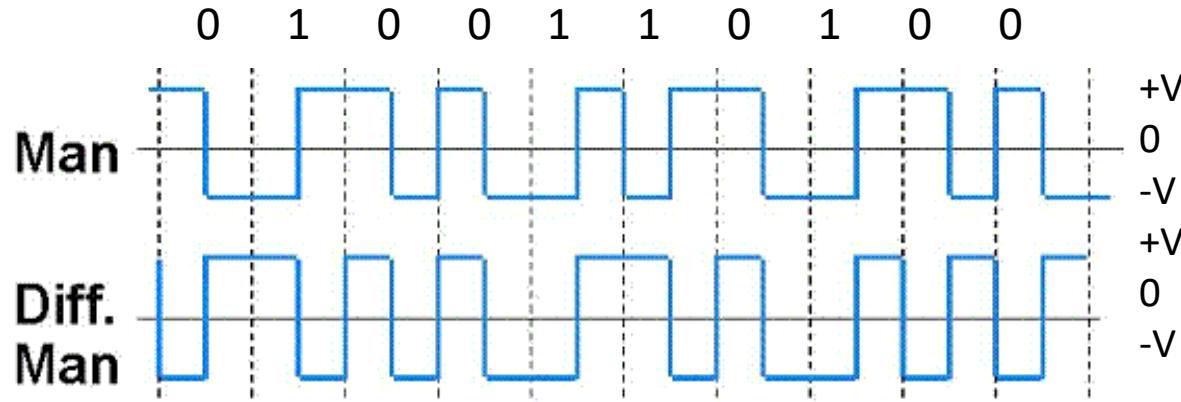
6. Differential Manchester Encoding (DME): unipolar/bipolar levels

„0” bit: change level at the beginning and at the half of the bit time.

„1” bit: change level just at the half of the bit time.

Provides continuous synchronization, with less than double baud.

E.g.:



4. Modulation technics

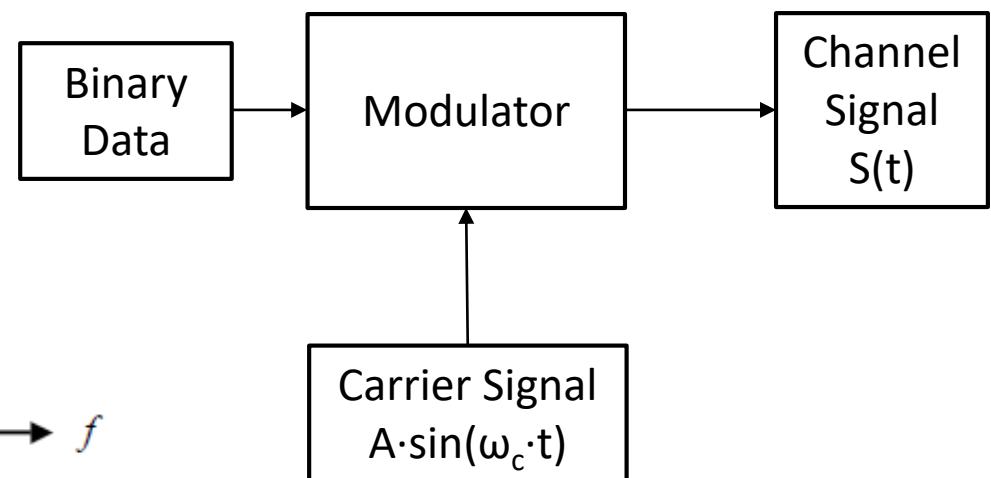
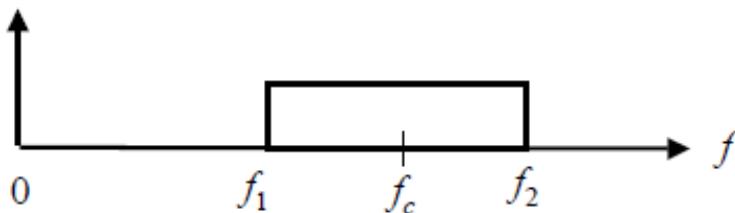
Considerations:

The binary information is transmitted through not a baseband channel, but in a given band of frequencies.

The middle value of the frequency band $[f_1, f_2]$ is the frequency of the carrier signal, f_c . This signal is modified conform to the modulation rule.

Legend:

A : Amplitude of the signal
 $\omega_c = 2 \cdot \pi \cdot f_c$ Angular frequency
t : time (continuous)



4. Modulation techniques

1. Amplitude Shift Keying (ASK) modulation:

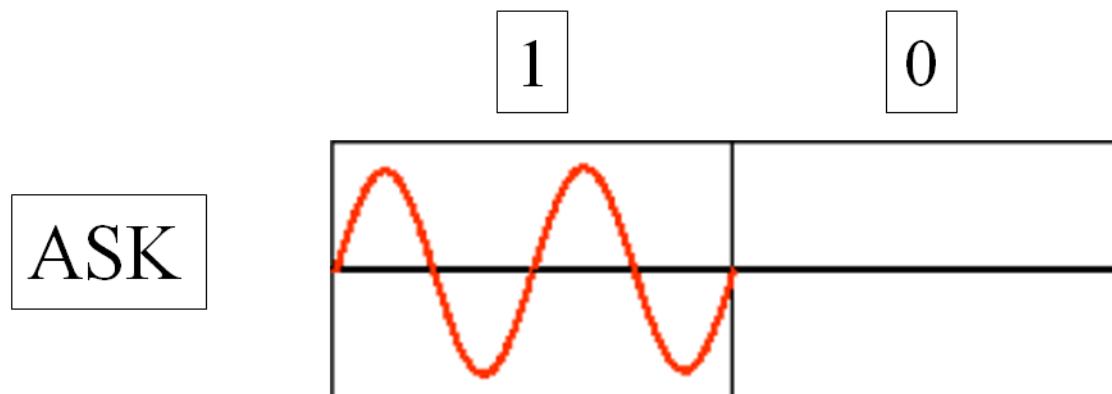
„0” bit: absence of the carrier signal ($A = 0$).

„1” bit: presence of the carrier signal ($A \neq 0$).

$$S_{(0)}(t) = 0$$

$$S_{(1)}(t) = A \cdot \sin(\omega_c \cdot t)$$

Simple to execute. Disadvantage is the presence of the constant component (energy wasting).



4. Modulation techniques

2. Frequency Shift Keying (FSK) modulation:

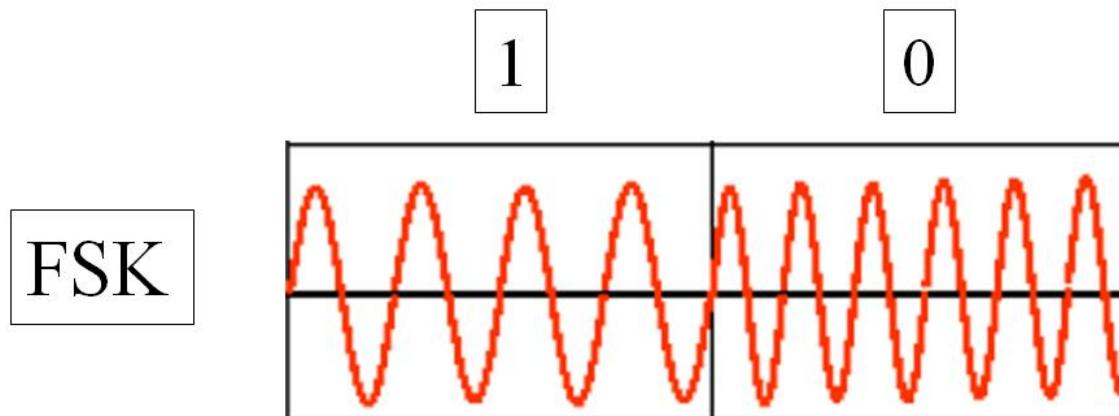
„0” bit: frequency increase by f_d (deviation) to the carrier frequency.

„1” bit: frequency decrease by f_d (deviation) to the carrier frequency.

$$S_{(0)}(t) = A \cdot \sin((\omega_c + \omega_d) \cdot t)$$

$$S_{(1)}(t) = A \cdot \sin((\omega_c - \omega_d) \cdot t)$$

In this case the bit rate and the baud is equal. The necessary spectral width is: $2 \cdot \omega_d$
It is easy to demodulate at the receiver. Disadvantage is the high frequency range.



4. Modulation technics

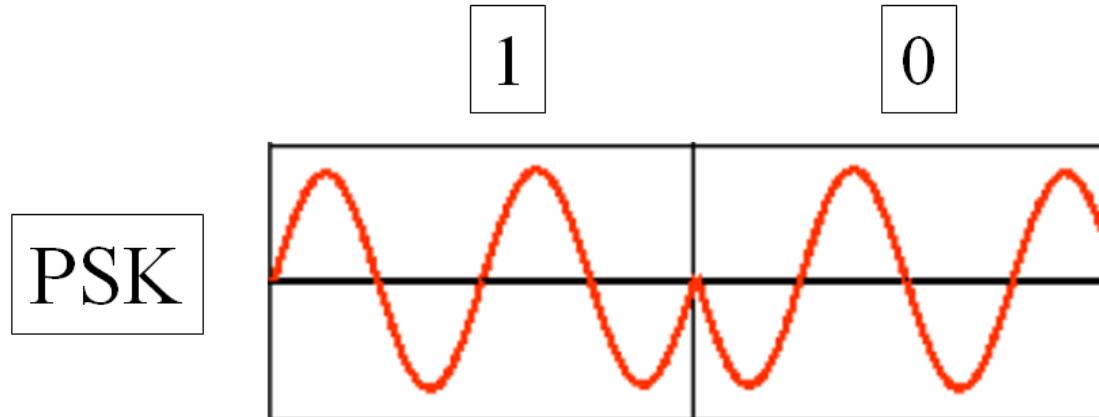
3. Phase Shift Keying (PSK) modulation:

„0” bit: inverse phase to the phase of the carrier signal.

„1” bit: identical phase with the phase of the carrier signal.

$$S_{(0)}(t) = A \cdot \sin(\omega_c \cdot t + \pi) = -A \cdot \sin(\omega_c \cdot t)$$

$$S_{(1)}(t) = A \cdot \sin(\omega_c \cdot t)$$



Multilevel PSK: In this case the bit rate and the baud is equal.

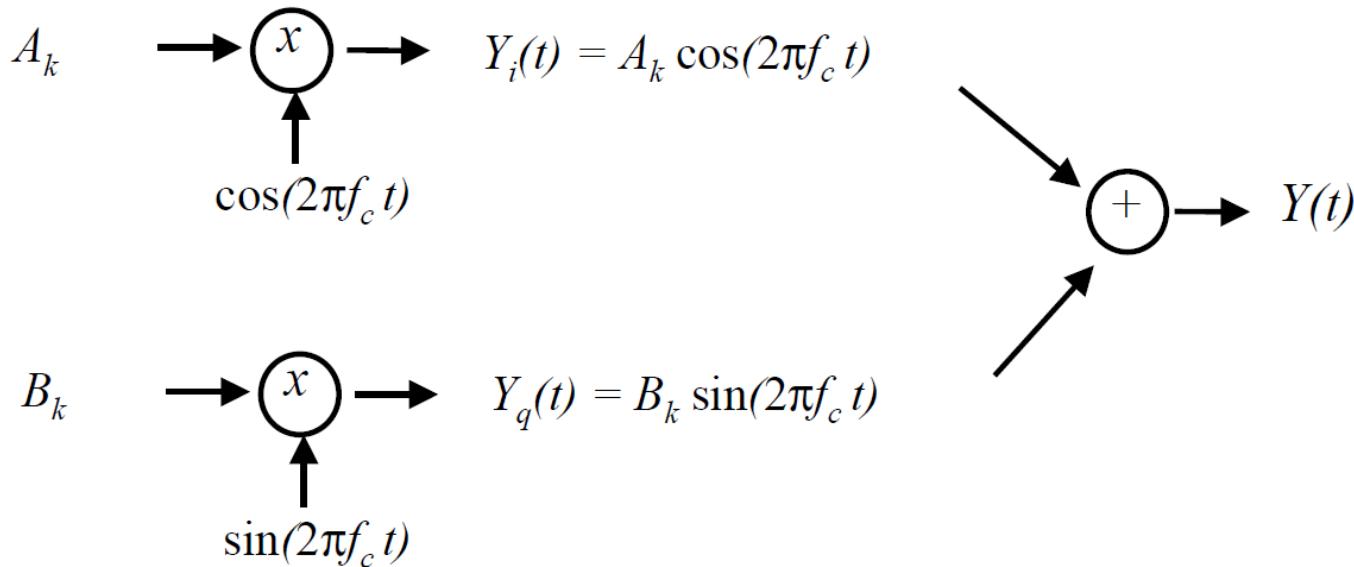
E.g.: 4 level PSK (Quadrature PSK, QPSK): phase displacements: 0°, 90°, 180° és 270°.

In this case two bits are transferred during one bit time.

4. Modulation techniques

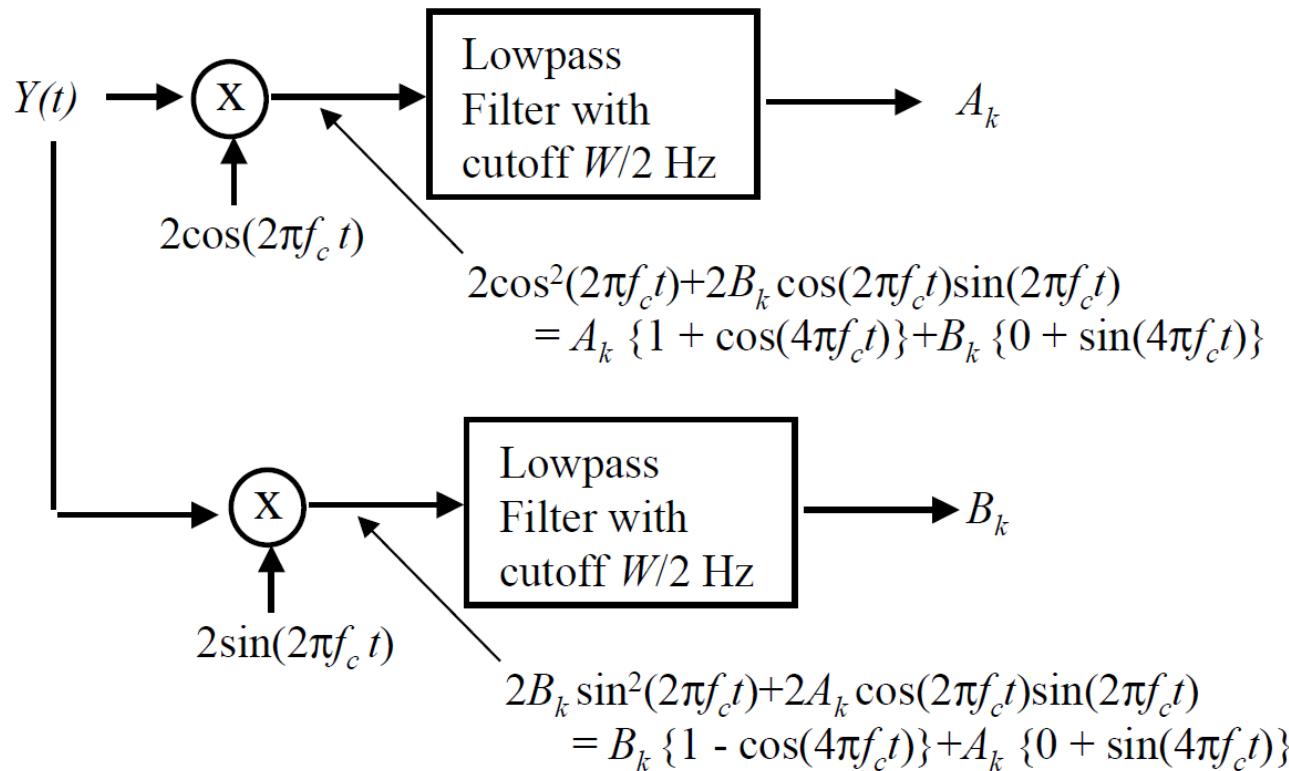
4. Quadrature Amplitude Modulation (QAM): transmitter

Modulate $\cos(2\pi f_c t)$ and $\sin(2\pi f_c t)$ by multiplying them by A_k and B_k respectively for $(k-1)T < t < kT$:



4. Modulation techniques

4. Quadrature Amplitude Modulation (QAM): receiver



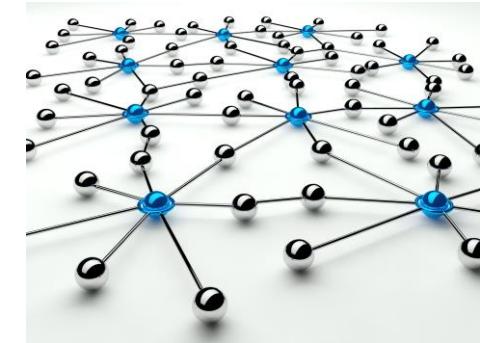
Networks Architectures and Protocols

4. TOPOLOGIES, DATA LINK LAYER

Lecturer: Zoltán Gál, PhD

Faculty of Informatics, University of Debrecen

February 05, 2018



Outline

- 1) Logical and physical topology
- 2) General functions and sublayers of the data link layer
- 3) Channel access of the MAC sublayer
- 4) Code Division Multiple Access

1. Logical and Physical Topology

Network topology:

- Connection system of the network nodes in space.
- Type of the connection graph.

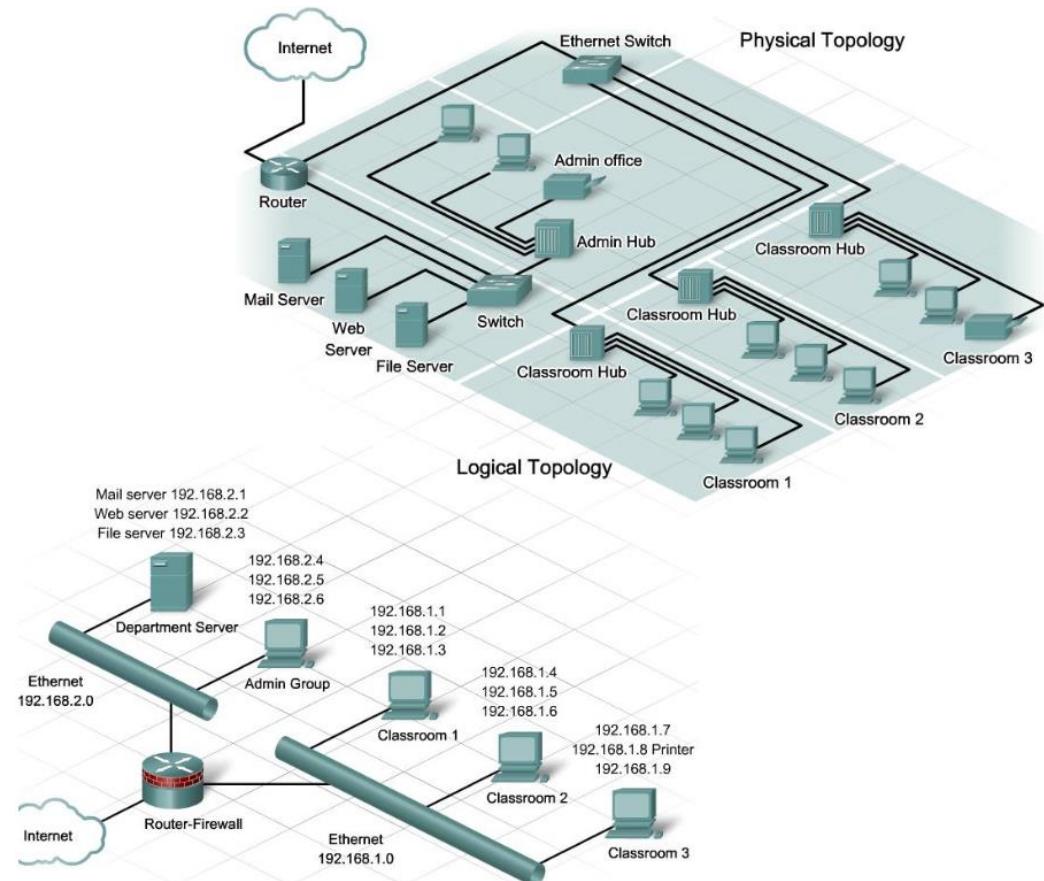
Logical topology:

- Connection system of the upper layers in the OSI model.

Physical topology:

- Connection system of the lower layers in the OSI model together with the physical path.

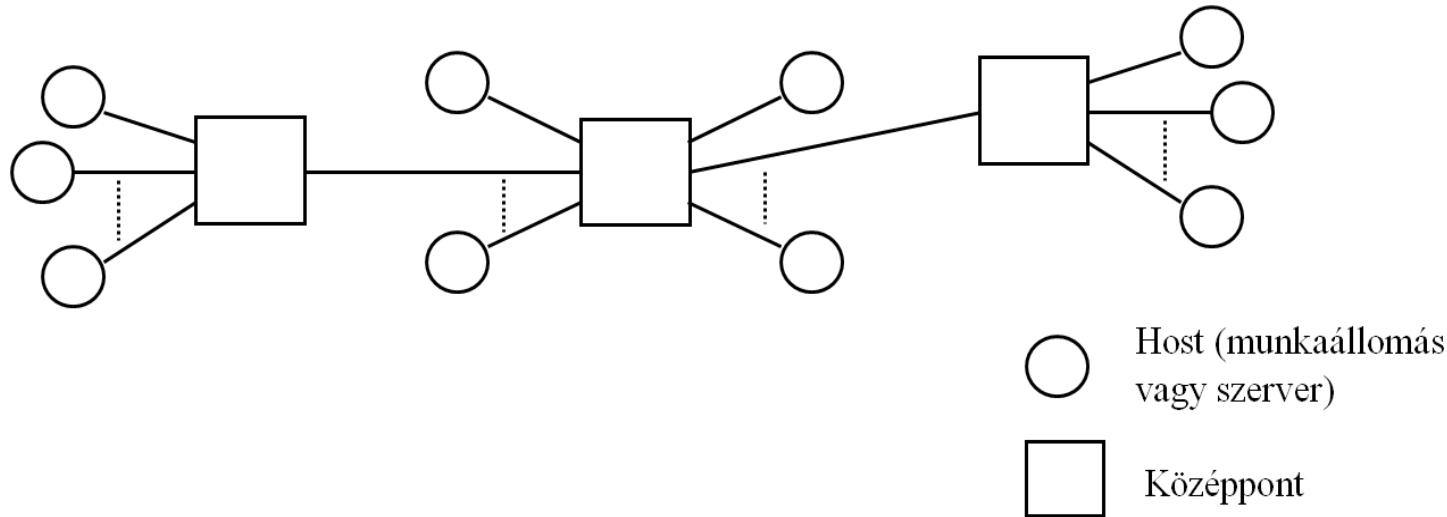
Topology type has considerable effect to the logical connection possibility in case the communication channel is affected by error (failure).



We discuss just the basic topology types.

1. Logical and Physical Topology

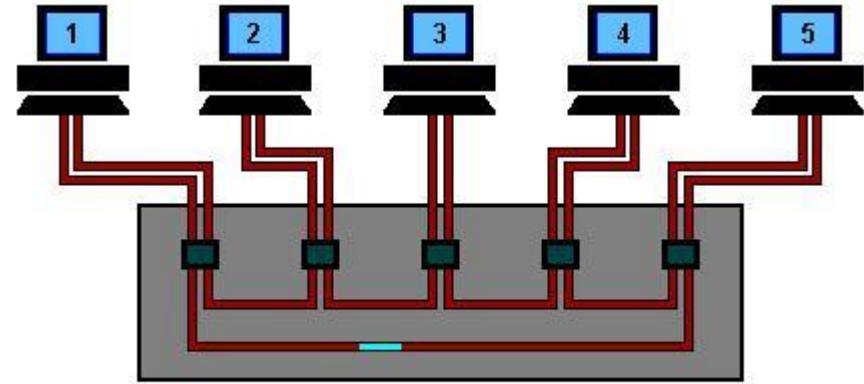
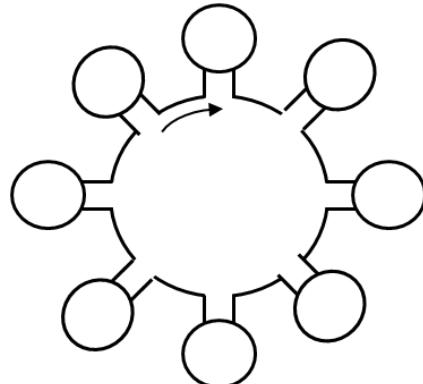
1. Star and extended star topology:



- Star: One central element (device) with end nodes.
- Extended star: Several central elements with end nodes. Extension is based on two levels, usually.
- Failure of a given central element affects the nodes and other central elements connected to this central element.

1. Logical and Physical Topology

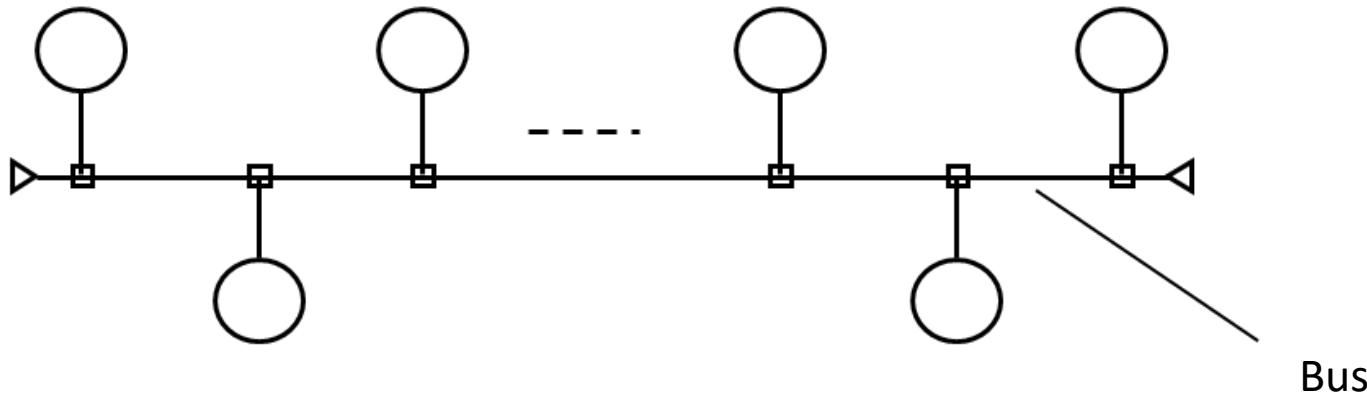
2. Ring topology:



- Each node has upside and downside neighbour.
- The ring has defined transmission direction.
- The concentrator increase the robustness, but it is a single point of failure element.
- The frame sent by the transmitted is received back from the upside neighbour and deleted from the ring by the source node.
- Secondary ring may be applied in special cases (see later).

1. Logical and Physical Topology

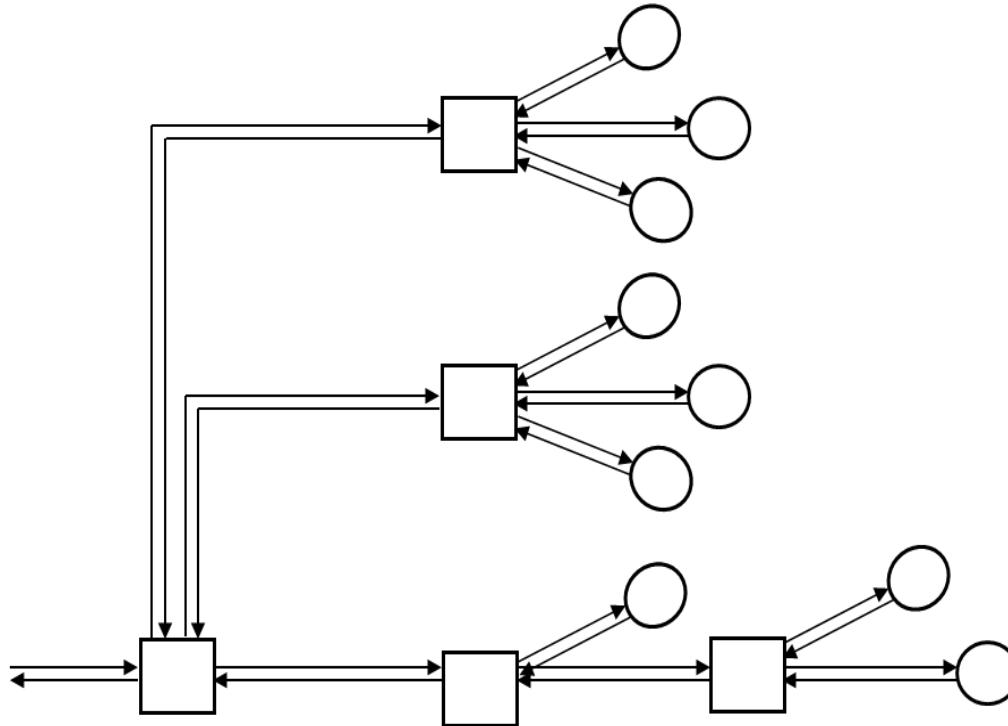
3. Bus topology:



- Several nodes are connected to the same channel (wire).
- The bus may be unidirectional or bidirectional.
- Any physical element of the wire may be single point of failure element.
- Discontinuity of the media creates reflection of the signal in that physical point. Multiple reflections produce noise.

1. Logical and Physical Topology

4. Tree topology:



- Is an extension of the extended star topology. The number of hierarchies is not limited. In practice the number of intermediate nodes and end nodes is finite.
- Any two leaves can communicate through a single path. No redundancy of the path exists.
- May appear different transmission intensities of the PDUs at different regions of the network.

2. General Functions and Sublayers of the Data Link

Service types in the data link layer:

Unacknowledged, connectionless service:

- No acknowledgement sent by the receiver after the reception of the PDU sent by the source. It is frequently used where the connection is stable (reliable).
E.g.: wire based Ethernet technology.

Acknowledged, connectionless service:

- The receiver sends acknowledgement to the source after the reception of the PDU. It is used for wireless communication technologies, where the channel is not reliable, with noise and transmission errors.
E.g.: Wireless Fidelity (WiFi) technology.

Acknowledged, connection oriented service:

- Acknowledgement is sent just for a block of PDUs. It is efficient in case of PDU stream transmission. If transmission error happens, then just the last block of PDUs should be resent by the source.

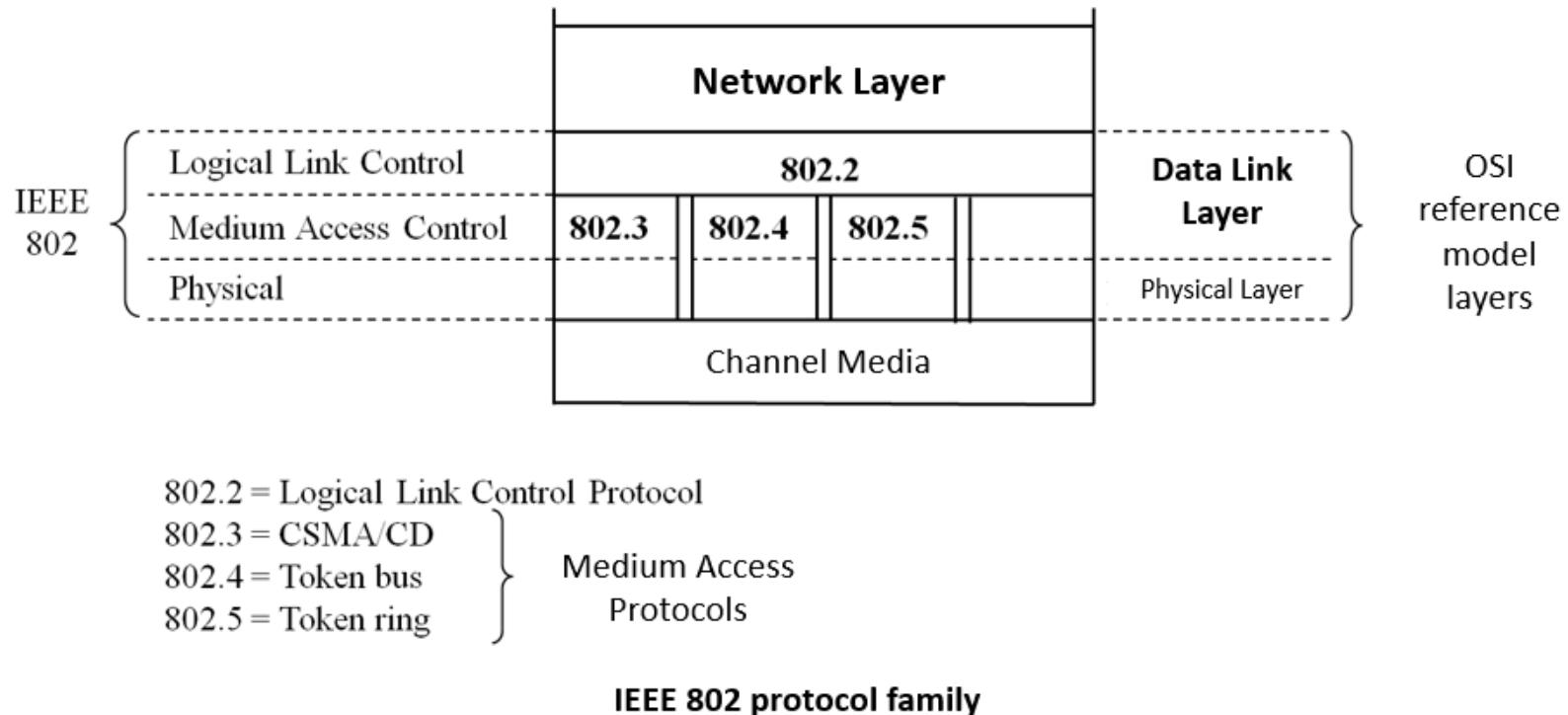
2. General Functions and Sublayers of the Data Link

Encapsulation in the Data Link layer:

- It is executed at the source node.
- The SDU (Service Data Unit) received from the network layer (L3) entity is split into frames.
- H2 and T2 fields creation and „gluing” to the payload field.
- Frame sent to the physical layer bit by bit.
- Separation methods of the consecutive frames:
 - **Timing** (IFP – InterFrame Gap): pause in sending for a given time interval, depending on the communication technology
 - **Frame size**: Frame size field in the frame header (H2) gives the size of the frame in bytes. This field affected by error makes no possible the frame decoding at the receiver.
 - **Bit pattern**: usage of DLE STX (DataLink Escape/Start of TeXt) and DLE ETX (DataLink Escape/End of TeXt) characters with character stuffing method. If DLE character should be sent in the payload, then DLE character is duplicated.

2. General Functions and Sublayers of the Data Link

IEEE LAN Data Link layer communication standards:



- Sublayers of the Data Link Layer (DLL):
 - Medium Access Control (MAC): HW/SW
 - Logical Link Control (LLC): SW

3. Channel access of the MAC sublayer

1. Static channel access methods:

Frequency Division Multiple Access (FDMA):

- The channel is split into subchannels consisting disjunctive frequency ranges to reduce the channel access contention. In idea situation each source is mapped to different subchannels eliminating the contention.

Time Division Multiple Access (TDMA):

- The access to the common channel is scheduled in consecutive time intervals (slots) for the sources in the contention. Each source has own time slot. Just one source sends in a given time slot.

Wavelength Division Multiple Access (FDMA):

- Similar to the FDMA, but the media is fibre cable or EM space, and the signal is light.

3. Channel access of the MAC sublayer

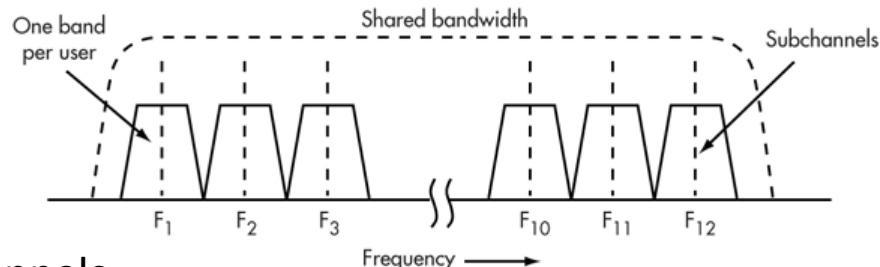
2. Dynamic channel access methods:

- Sending without carrier sensing
- Time slotting
- Carrier Sense Multiple Access (CSMA)
- Collision Detection
- Token Based Access
- Code Division Multiple Access



3. Channel access of the MAC sublayer

Frequency Division Multiple Access (FDMA):



Aspects of the channel splitting to the subchannels

- **Elimination of the collision:** No. of subchannels = No. of sources. Simple to implement, but the channel usage efficiency is slow in case when sources are not sending.
- **Minimization of the transfer time:** Communication efficiency is the main goal: minimization of the delay time during the PDU transfer.

Queueing model for channel slip in N subchannels:

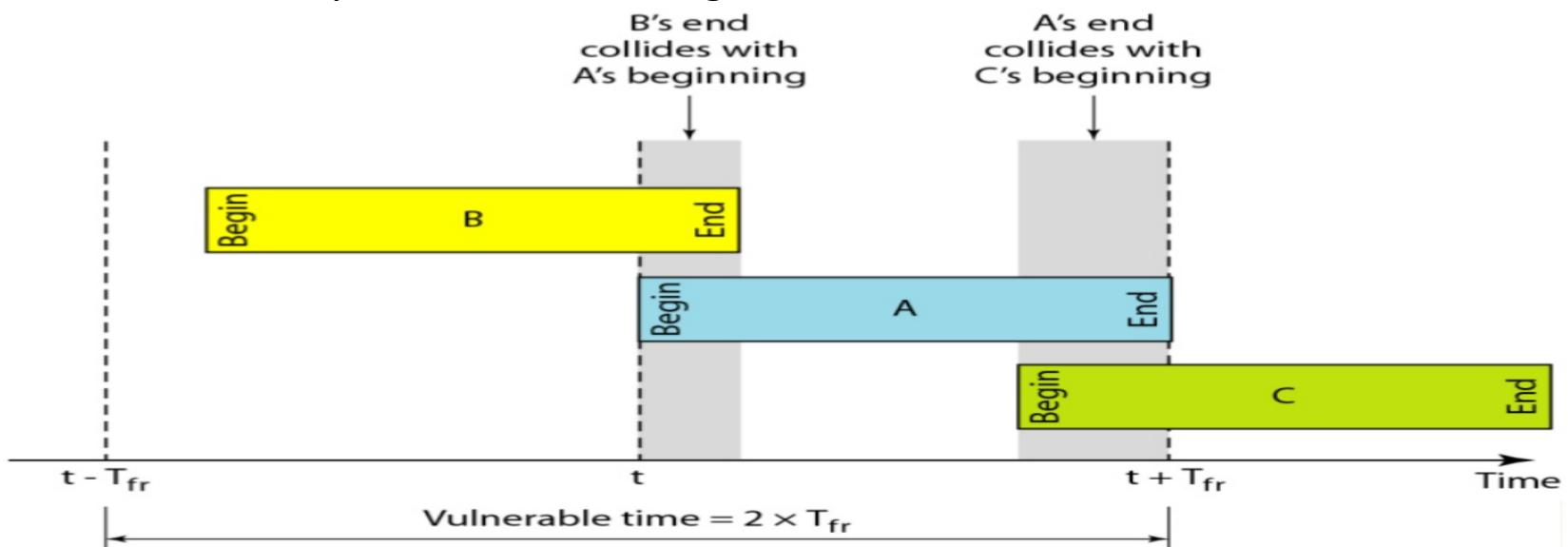
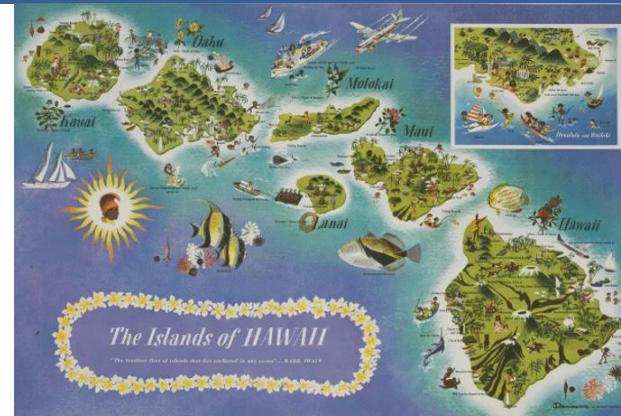
- The arrival and forwarding moments of the frames is independent and exponentially distributed. This consideration is near to the reality but not exactly.
- Transfer capacity: C/N [b/s]. Transfer time duration of one bit: C/N [s].
- Frame arrival intensity: λ/N [keret/s]. Frame arrival time intervals: N/λ [s].
- Frame size: $1/\mu$ [bit/frame].
- Token Based Access
- Transmission time of one frame: $N/(\mu \cdot C)$ [s]. Frame processing intensity: $(\mu \cdot C)/N$ [Hz].
- **Little's law:** Average response time = $1/(\text{proc. int.} - \text{arriv. int.}) = N/(\mu \cdot C - \lambda)$ [s].

Expected time duration of the frames is linear with the No. of subchannels (N).

3. Channel access of the MAC sublayer

ALOHA:

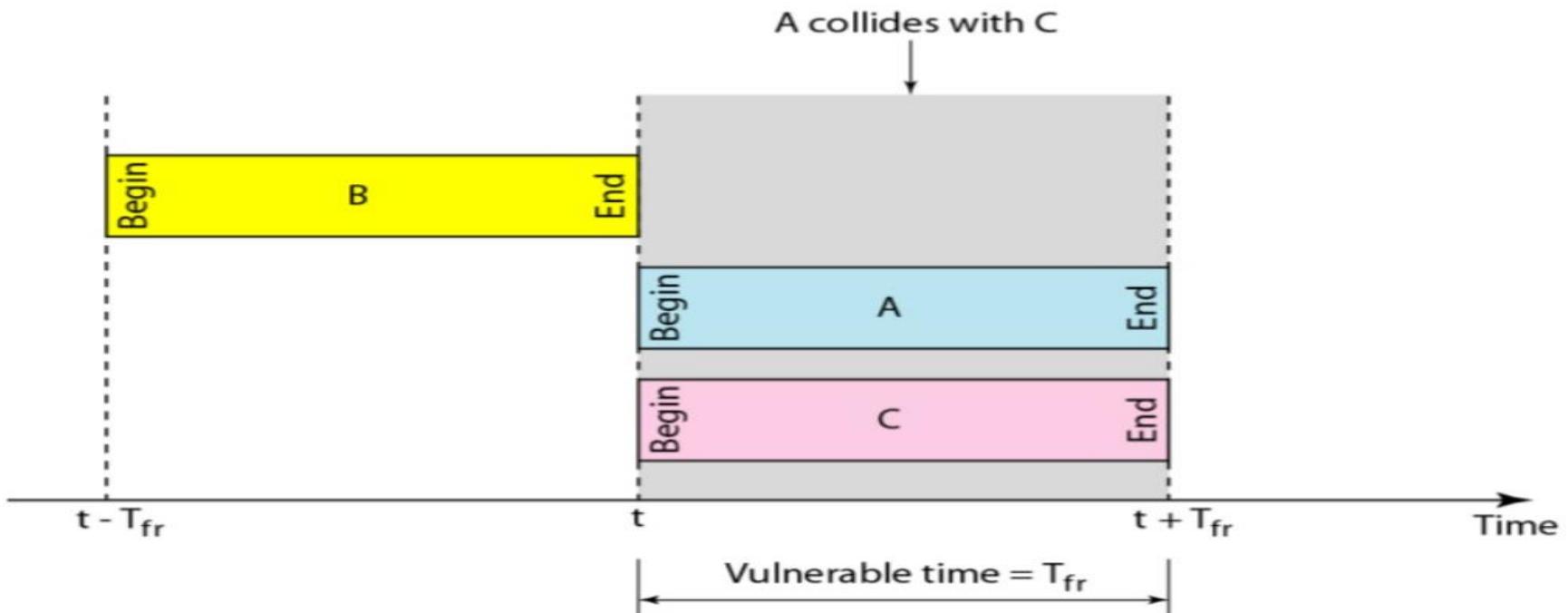
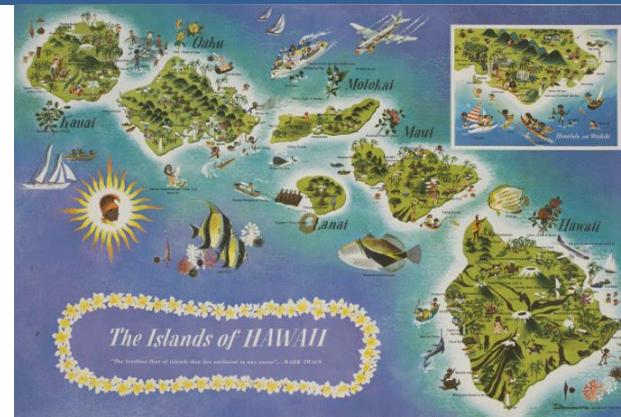
- Simplest channels access without carrier sensing.
- Source: University of Hawaii – radio channel communication between islands.
- Frame is sent on the common channel.
- Receiver send acknowledgement if no collision.
- Waiting for a random time interval and retransmission if collision is detected by the source.
- Simple to implement, simple to execute.
- Maximum efficiency of the channel usage < 18 %.



3. Channel access of the MAC sublayer

Slotted ALOHA:

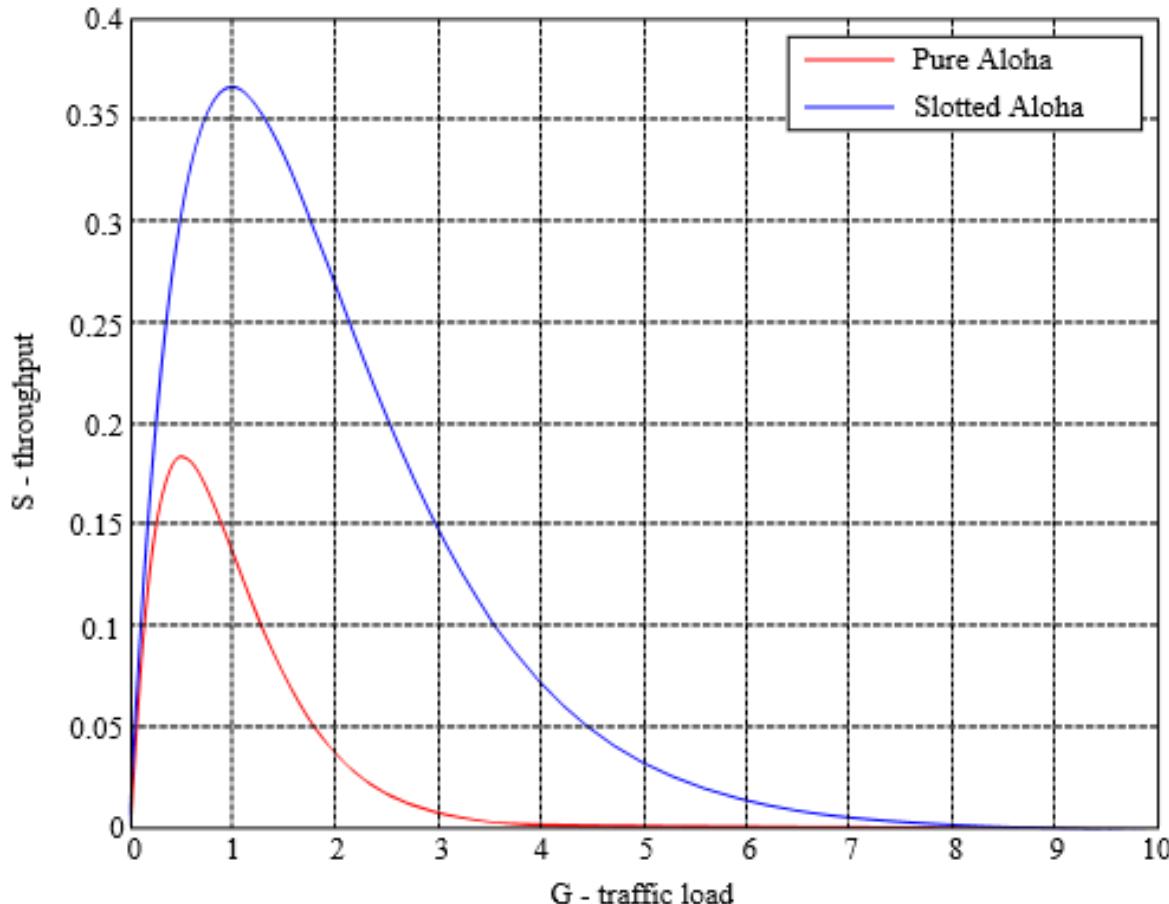
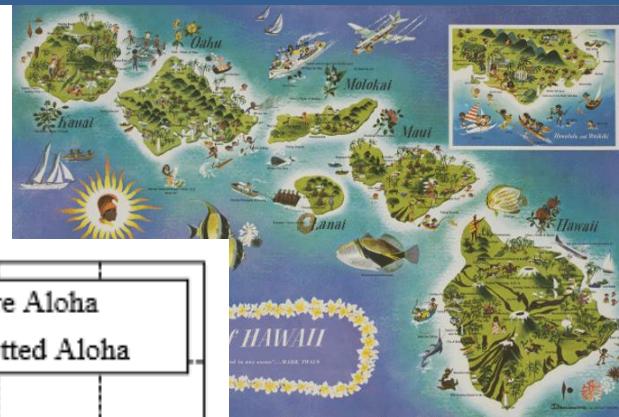
- Extension of ALOHA.
- Usage of time slot: frame transmission time
- Receiver send acknowledgement if no collision.
- Waiting for a random time interval and retransmission if collision is detected by the source.
- Maximum efficiency of the channel usage < 37 %.



3. Channel access of the MAC sublayer

Channel usage efficiency of ALOHA and S-ALOHA:

- Distribution law of the sending trials is Poisson.



4. Code Division Multiple Access (CDMA)

Considerations:

- To not have interference on the radio channel, just one radio frame is recommended to be transmitted in a given moment.
- The interference phenomenon has one positive version, when the transmission is executed on spread spectrum. This range of frequencies is significantly larger than the necessary bandwidth.
- Different sources send overlapping frames producing partial interference. Each source encodes their data bits in unique way.

Mathematical background of the CDMA:

- Each station generates chip codes having m bits. The sent code uniquely identifies the source.
- Sent data bites:

$$S_1 = (s_1, \dots, s_m)$$

$$S_0 = (-s_1, \dots, -s_m), \text{ where } s_i = +1 \text{ or } s_i = -1, \quad i = 1, \dots, m.$$

Operations with the chip codes:

Adding S and T chips: $S + T = (s_1 + t_1, \dots, s_m + t_m)$

Scalar product of chips: $S * T = (1/m) \cdot (s_1 \cdot t_1 + \dots + s_m \cdot t_m)$

4. Code Division Multiple Access (CDMA)

Mathematical background of the CDMA (cont'd):

- Because of bipolar encoding exist following relations:

$$S_1 * S_1 = S_0 * S_0 = 1,$$

$$S_1 * S_0 = -1,$$

$$S * (A+B) = (S * A) + (S * B).$$

Operation conditions:

- Chip codes belonging to different terminals are orthogonal (scalar product is zero)

$$S_1 * T_1 = S_1 * T_0 = S_0 * T_1 = S_0 * T_0 = 0$$

- Chip code length: $\log_2 m \geq \lceil \log_2 N \rceil$, where N is the population

Receiving process:

- The sum of chip bits transmitted in a given moment is received as interfered signals, but the sent chip code can be decoded.
- The receiver executes scalar product of the incoming sum and the sender chip code.
- For good reception synchronization of the chip bits is required.

4. Code Division Multiple Access (CDMA)

CDMA communication example:

- Sources ($N=3$): A, B, C.
- No. of chip bits: $m = 4$. $\log_2 4 \geq \lceil \log_2 3 \rceil$
- Orthogonal chip codes of the sources:

$$A_1 = (+1, +1, -1, -1);$$

$$A_0 = (-1, -1, +1, +1);$$

$$B_1 = (+1, -1, +1, -1);$$

$$B_0 = (-1, +1, -1, +1);$$

$$C_1 = (-1, -1, -1, -1);$$

$$C_0 = (+1, +1, +1, +1);$$

- Simultaneously sent chip bits:

A: 0 (-1, -1, +1, +1); **B: 1** (+1, -1, +1, -1); **C: 0** (+1, +1, +1, +1)

- Interfered signal on the channel: $A_0 + B_1 + C_0 = (+1, -1, +3, +1)$

A's partner: $A_1 * (A_0 + B_1 + C_0) = (+1-1-3-1)/4 = -1$. Because $A_1 * X = -1 \rightarrow X = A_0$,
Sent data bit from source A is „0”.

B's partner: $B_1 * (A_0 + B_1 + C_0) = (+1+1+3-1)/4 = 1$. Because $B_1 * X = +1 \rightarrow X = B_1$,
Sent data bit from source B is „1”.

C's partner: $C_1 * (A_0 + B_1 + C_0) = (-1-1-1-1)/4 = -1$. Because $C_1 * X = -1 \rightarrow X = C_0$,
Sent data bit from source C is „0”.

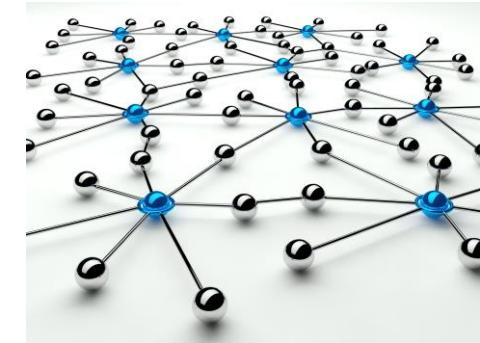
Networks Architectures and Protocols

5. LAN and MAN TECHNOLOGIES

Lecturer: Zoltán Gál, PhD

Faculty of Informatics, University of Debrecen

February 05, 2018



Outline

1) Ethernet technology

Topology, Frame structure

Characteristic parameters

MAC mechanism (CSMA/CD)

Switching, segmenting

2) Token ring technology

Topology, Frame Structure

Characteristic parameters

MAC mechanism (Token ring)

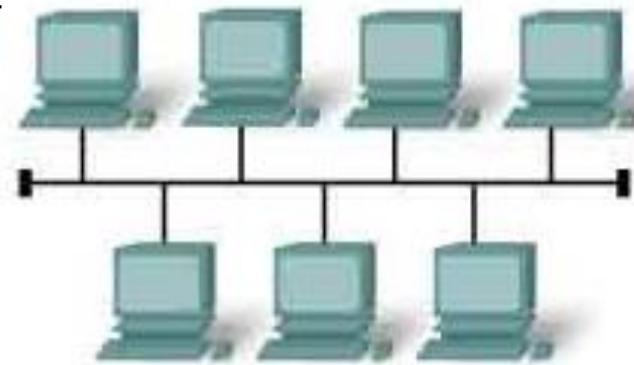
1. Ethernet technology

1. Ethernet (IEEE 802.3) communication technology:

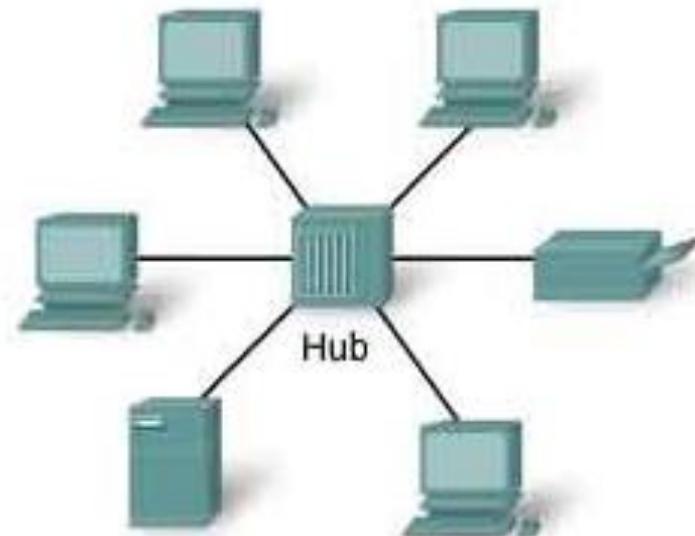
Possible topologies:

Bus

Tree (with repeater)



Star (with hub, switch)



1. Ethernet technology

1. Ethernet (IEEE 802.3) communication technology:

Frame structure of the Ethernet:

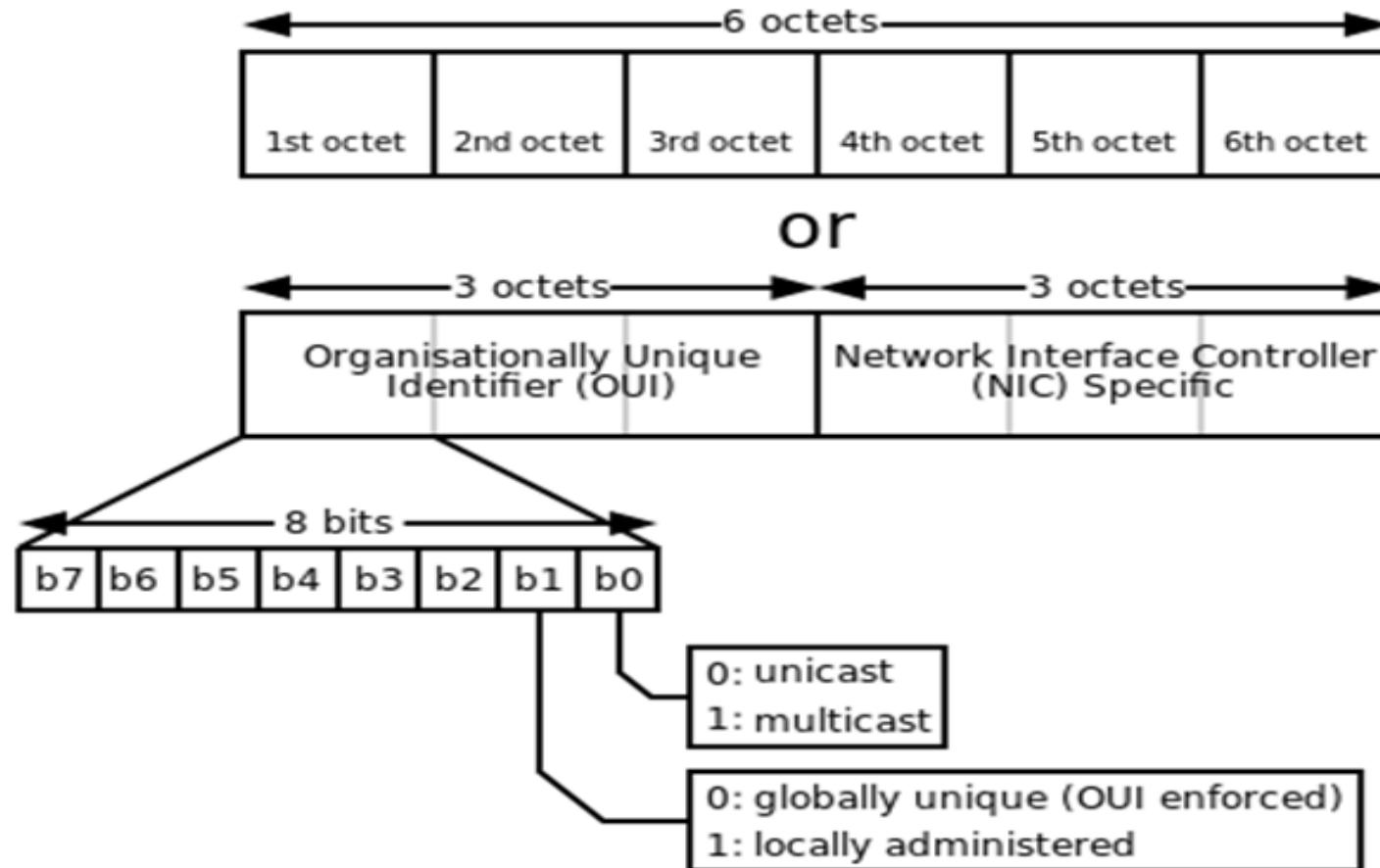


62 bits	Preamble used for bit synchronization
2 bits	Start of Frame Delimiter
48 bits	Destination Ethernet Address
48 bits	Source Ethernet Address
16 bits	Length or Type
46 -1500 bytes	Data
32 bits	Frame Check Sequence

1. Ethernet technology

1. Ethernet (IEEE 802.3) communication technology (cont'd):

Structure of the physical address:



1. Ethernet technology

1. Ethernet (IEEE 802.3) communication technology (cont'd)

Running parameters of the IEEE 802.3:

Parameter	Value
Transmission rate	10 Mbps (Manchester encoding)
Slot time	512 bit time
Inter Frame Gap (IFG)	9,6 µs
Max. no. of transmission trials	16
Duration of the Jam Signal	32 bit time
Max. length of the frame	1518 bytes
Min. length of the frame	64 bytes

Possible values of the physical address field:

- Destination address: Unicast address
- Destination address: 48 of '1' bits (broadcast) – the message is received and interpreted by all nodes on the same broadcast domain.
- Destination address: multicast (special value) – the message is received and interpreted just by the members of the group.

1. Ethernet technology

1. Ethernet (IEEE 802.3) communication technology (cont'd):

Frame transmission algorithm part (CSMA/CD):

1. Wait for SDU3 and then execute frame encapsulation.

2. Channel busy?

Yes: Goto 2.

No: Wait IFG (Inter Frame Gap) time interval, then start frame sending.

3. Is collision detected during the frame transmission?

Yes: Send Jamming signal. Frame_send_trial := Frame_send_trial+1, Goto 4.

No: End sending the frame (success). Goto 1.

4. Frame_send_trial (k) < 16 ?

Yes: Frame transmission unsuccessful. Goto 1.

No: Determine new waiting time interval and wait. Goto 2.

1. Ethernet technology

1. Ethernet (IEEE 802.3) communication technology (cont'd):

Frame transmission algorithm part (CSMA/CD) (cont'd):

Determination of the new waiting time interval:

- Slot time (T_{slot}) is the time interval for the signal to propagate in the path End_A - End_B - End_A , where End_A and End_B are the farthest points of the channel (collision domain).
- Typical propagation delay: $\sim 5 \mu\text{s}/1000 \text{ m}$.
- Slot time = $2 * (\text{channel delay} + \text{repeaters delay}) + \text{reserve time}$
 $= 51.2 \mu\text{s} = 2 * (\text{prop_delay of } 2.5 \text{ km} + 4 * \text{repeater_delay}) = 512 * T_{bit}$
- Waiting time (k), $k < 16$: Random time interval in the $[0, 2^{k*T_{slot}}]$ time interval.

Frame_send_trial (k)	Random time interval [T_{slot}]
1	$[0, 1]$
2	$[0, \dots, 3]$
3	$[0, \dots, 7]$
i	$\{0, \dots, (2^i - 1)\}$
15	$\{0, \dots, 32767\}$
16	Stop trials, send Jamming signal

1. Ethernet technology

1. Ethernet (IEEE 802.3) communication technology (cont'd):

Frame reception algorithm part (CSMA/CD):

1. Is there signal on the channel?

Yes: Execute bit synchronization. Search Starting Delimiter. Read frame.

No: Goto 1.

2. Frame Check Sequence (FCS/CRC) and frame size are OK?

Yes: Check DA physical address. Goto 3.

No: Discard frame. Goto 1.

3. Is destination physical address (DA) OK?

Yes: Decapsulate frame payload and forward SDU₂ to the L3 entity of the node.

No: Discard frame. Goto 1.

Destination physical address is OK in any of the following cases:

- DA = local physical address
- DA is broadcast or multicast address.

1. Ethernet technology

2. Fast Ethernet (IEEE 802.3u) communication technology:

Goal of the technology development:

- 10x faster transmission rate than IEEE 802.3
- Usage of the existing structured cabling system for IEEE 802.3
- Same MAC algorithm and same frame structure

Cabling system: structured galvanic (UTP/SFT/FTP), optical.

Variants of the standard:

- 100BASE-TX: Half-Duplex mode - 100 Mb/s, Full-Duplex mode – 200 Mb/s.
- 100BASE-FX: separated channels for Tx and Rx – 200 Mb/s.

Channel coding mechanism: 4B/5B, NRZI.

- Data (hexa digit): 5 bits symbol.
- No. of different symbols: $2^5 = 32$.
- 16 special symbols for data: no more than 3 neighbouring symbol zeros for any order of data.

1. Ethernet technology

2. Fast Ethernet (IEEE 802.3u) communication technology (cont'd):

4B/5B coding (cont'd):

Data (Hexa)	Data (Binary)	4B/5B code
0	0000	11110
1	0001	01001
2	0010	10100
3	0011	10101
4	0100	01010
5	0101	01011
6	0110	01110
7	0111	01111

Data (Hexa)	Data (Binary)	4B/5B code
8	1000	10010
9	1001	10011
A	1010	10110
B	1011	10111
C	1100	11010
D	1101	11011
E	1110	11100
F	1111	11101

1. Ethernet technology

3. Gigabit Ethernet (IEEE 802.3ab, IEEE 802.3z) communication technology:

1000BASE-TX:

- Cat5e UTP (IEEE 802.3ab), four pairs of wire, 125 MHz/wirepair.
- Duplex transmission is provided by hybrid circuits, transmission rate: 250 Mb/s on pair.
- Slot time: $4096 T_{\text{bit}}$ (512 bytes).

1000BASE-SX:

- Multimode (MM) optical fibre: $\lambda = 850 \text{ nm}$ laser.
- Distance: 550 m.
- Tx and Rx on different fibre: Full-Duplex mode.

1000BASE-LX:

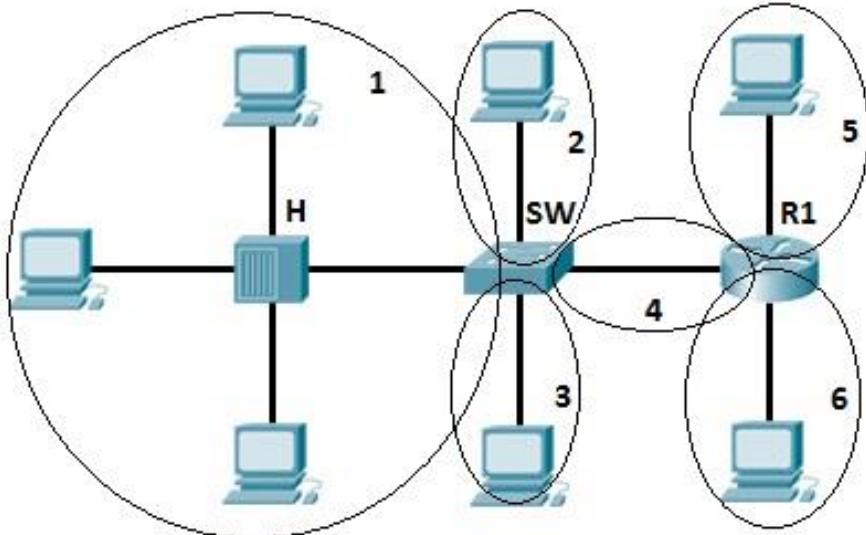
- Singlemode (SM) or multimode (MM) optical fibre: $\lambda = 1310 \text{ nm}$ laser.
- Distance (SM): 5,000 m.
- Tx and Rx on different fibre: Full-Duplex mode.

1. Ethernet technology

4. Ethernet switching, segmenting:

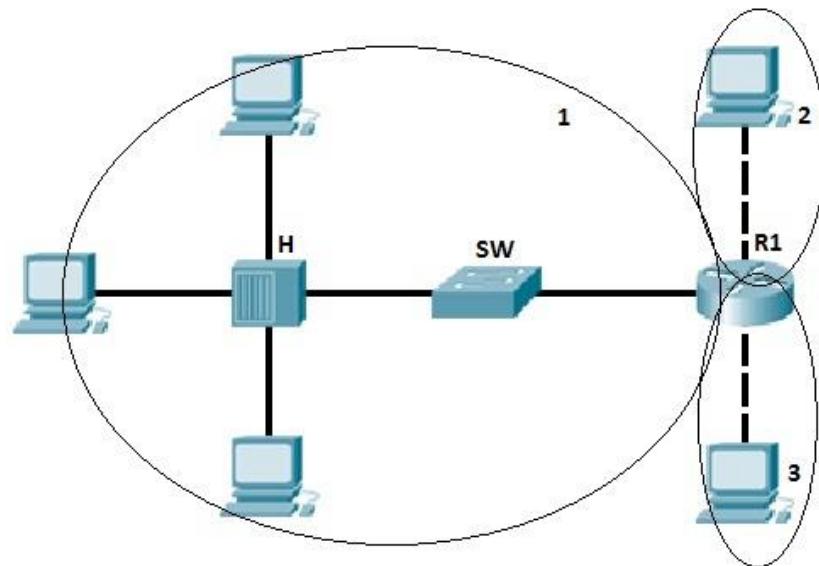
Collision domain:

Channel media connected physically by repeaters, hubs.



Broadcast domain:

L3 PDU delivery without router.
Segments connected by switches.



- L2 devices (bridge, switch) separate the collision domains between the interfaces, but forward frames transparently based on the destination MAC address.
- L2 and L3 devices do not forward collisions.

1. Ethernet technology

4. Ethernet switching, segmenting (cont'd):

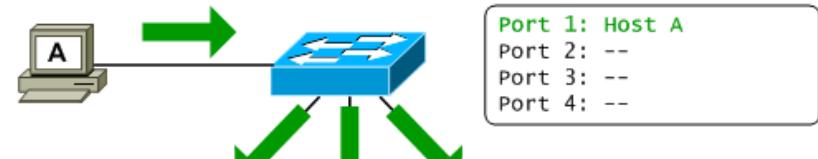
- CAM table contains records with the fields:

- Physical address value
 - Interface ID of the switch
 - Usage timer

- Switch searches the destination physical address of the incoming frame in the local CAM.

- If destination physical address is broadcast, multicast or unknown unicast address, then change the function of the switch to repeater mode and forwards this frame on all interfaces of the switch except the receiver interface.

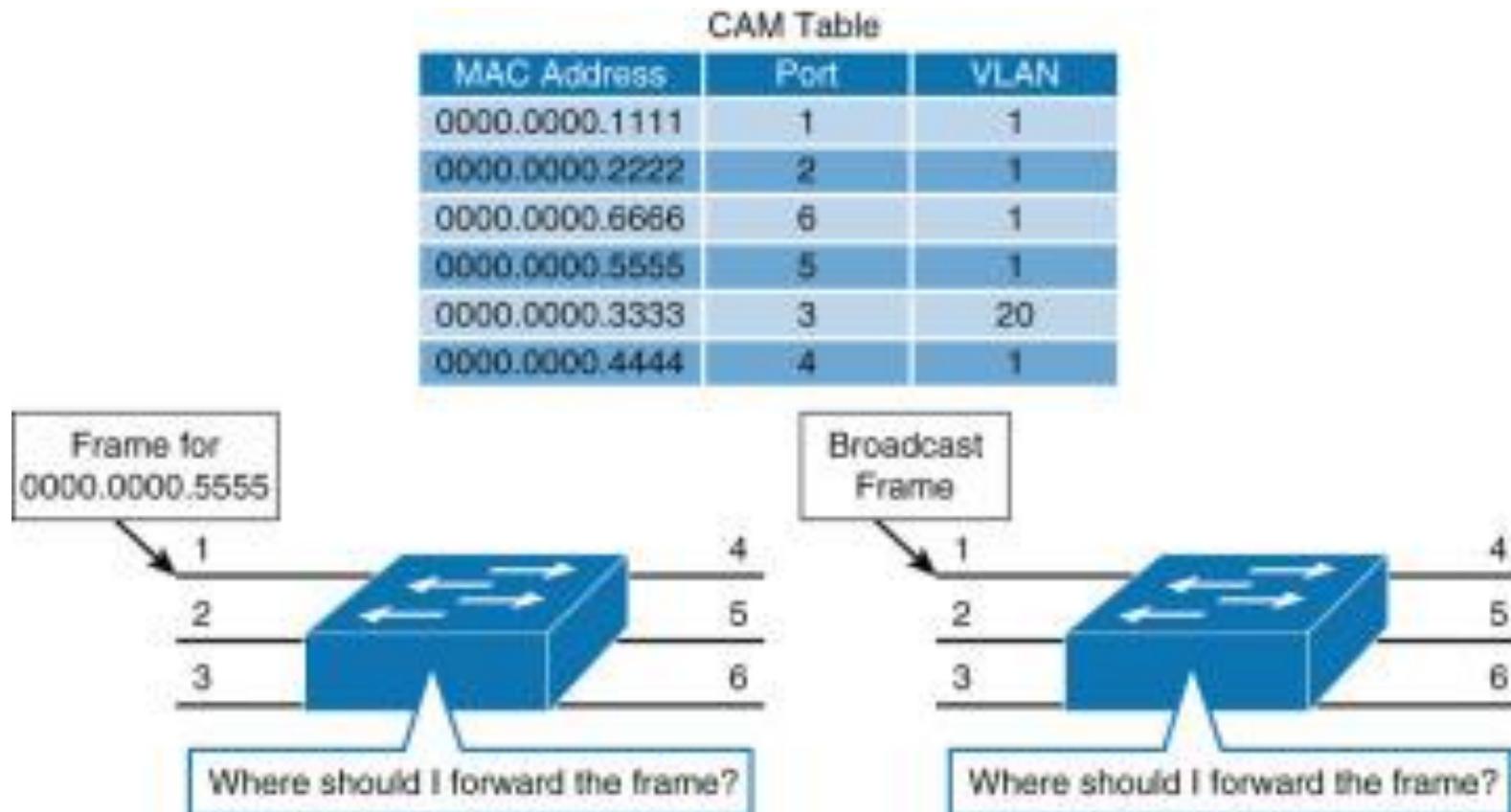
- If destination physical address is unicast and is found in the local CAM, then forwards this frame on the corresponding interface of the switch.



1. Ethernet technology

4. Ethernet switching, segmenting (cont'd):

Unicast/Broadcast forwarding:



1. Ethernet technology

4. Ethernet switching, segmenting (cont'd):

Ethernet switching types:

Store and Forward switching:

- The switch receives the whole frame. Checks the CRC code. If error is detected, then discards the frame. If no error is detected, then executes forwarding. High delay time in the switch.

Fast Forward switching:

- Based on the value of the first 6 bytes (DA) the frame forwarding is executed immediately. Very low delay in the switch, but frame fragment may be forwarded.

Fragment free switching:

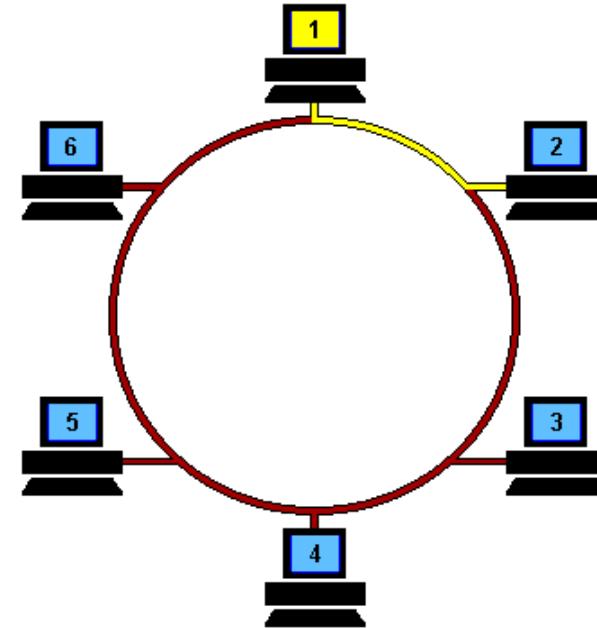
- Forwarding is started just when the first 64 bytes (minimum frame length) of the frame are received by the switch. No frame fragment is forwarded, reasonable delay in the switch.

2. Token ring technology

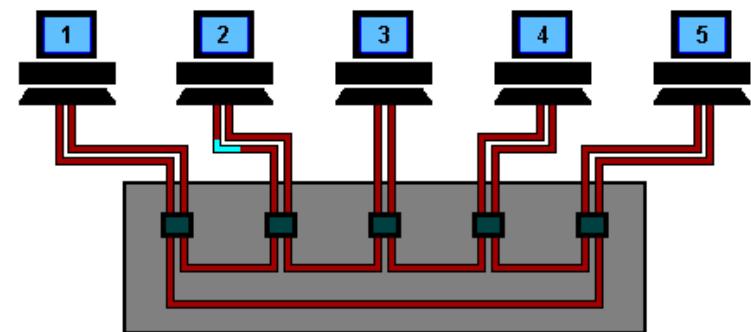
Token Ring (ISO/IEEE 802.5):

Possible topologies:

Ring (repeater)



Physical star, logical ring (repeater, switch)



2. Token ring technology

Token Ring (ISO/IEEE 802.5) (cont'd):

Token structure:

Start Delimiter (SD)	Access Control (AC)	End Delimiter (ED)
1 B	1 B	1 B

Frame structure:

SD	AC	FC	DA	SA	Data	CRC	ED	FS
1 B	1 B	1 B	6 B	6 B	max. 4500 B	4 B	1 B	1 B

FC – Frame Control

ED - Ending Delimiter

FS – Frame Status

2. Token ring technology

Token Ring (ISO/IEEE 802.5):

- Token eliminates the collision.
- Token: special frame forwarded in the ring hop-by-hop conform to the direction.
- Owning time of the token is possible for one frame transmission.
- After the actual frame is sent by the source node, the token should be forwarded to the next node.
- Topology: ring (logical), star (physical).
- Star centre device: TCU (Trunk Coupling Unit) isolates any link failure, but it is a single point of failure device.

2. Token ring technology

Token Ring (ISO/IEEE 802.5) (cont'd):

MAC algorithm:

- Source node waits for the token.
- Token owner node sends the frame to the destination physical node through the downside neighbour node.
- Each node forwards the incoming frame and compares the destination physical address field with the own MAC address.
- If the destination address of the incoming frame is OK, then interprets the content of the frame. If no matching exist, then the frame is just forwarded without interpretation.
- The destination node sets the status filed of the frame tail. This signal is used as acknowledgement to the source from the destination.
- Ending source node forwards the token to the next node.

2. Token ring technology

Token Ring (ISO/IEEE 802.5) variants:

TR (4 Mbps):

- Just one frame in the ring.
- The token is forwarded after the sent frame is received by the source.
- Max. no. of nodes: 72.

ETR (Early TR, 16 Mbps):

- Several frames in the ring.
- The token is forwarded immediately the frame is sent by the source (early token release).
- Max. no. of nodes: 125.

FTR (Fast TR, 100 Mbps): IEEE 802.5t (2000)

GTR (Gigabit TR, 1 Gbps): IEEE 802.5v (2003)

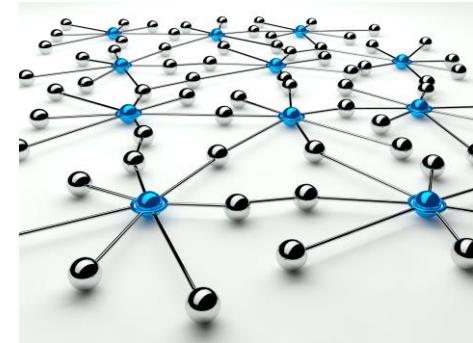
Networks Architectures and Protocols

6. INTERNET PROTOCOL - IP

Lecturer: Zoltán Gál, PhD

Faculty of Informatics, University of Debrecen

February 05, 2018



OUTLINE

1. IP Protocol Mechanism

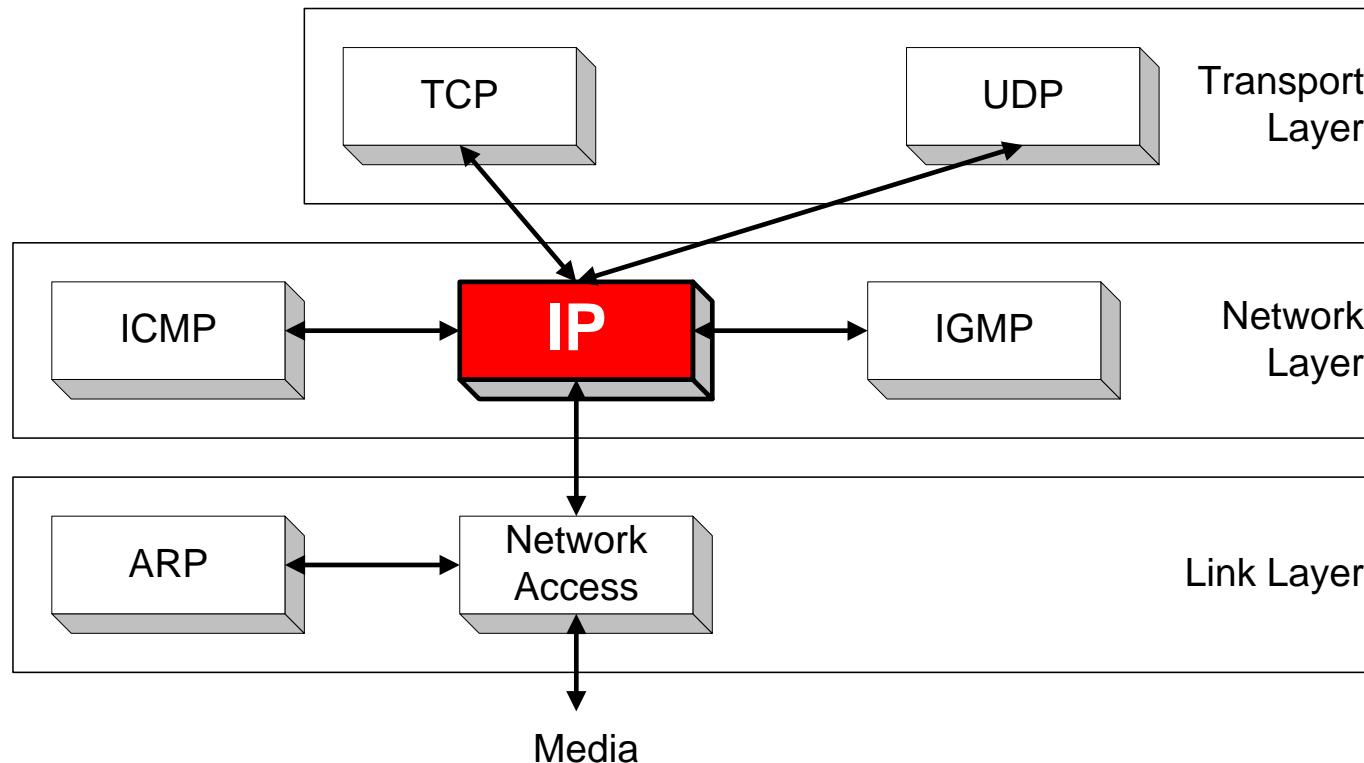
2. Addressing in IP

- Address Space, Mask/Prefix
- Class Based Addressing
- Classless Addressing
- Subnetting
- Supernetting
- CIDR

1. IP Protocol Mechanism

Orientation

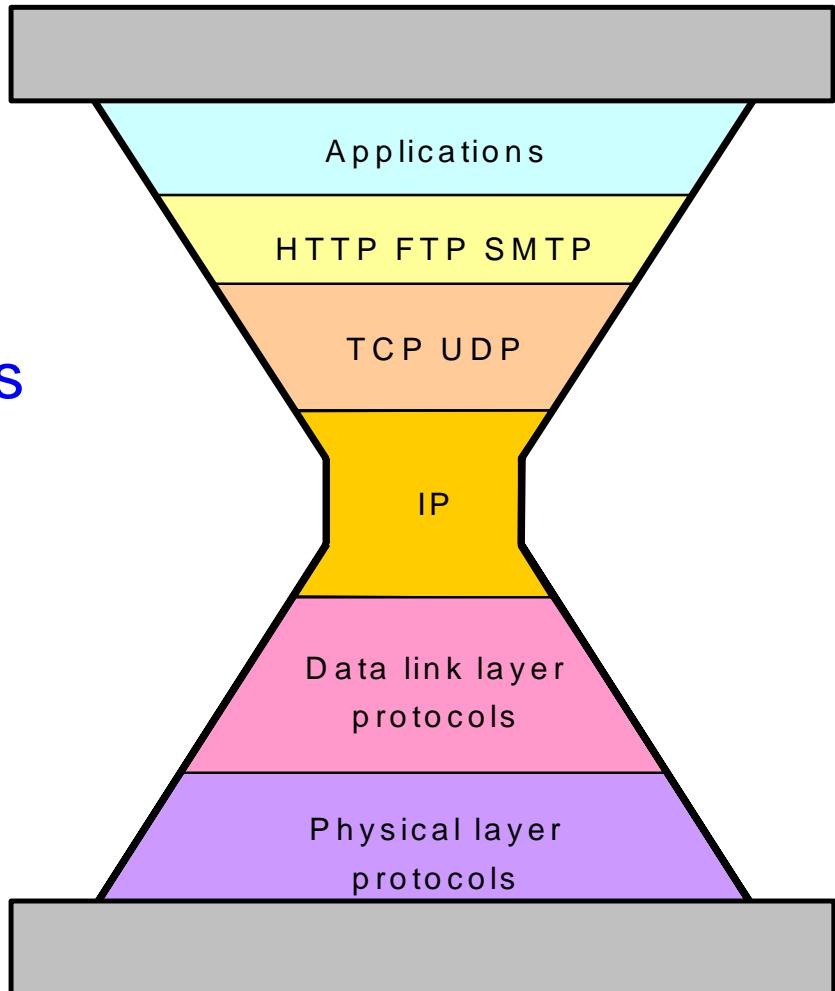
- IP (Internet Protocol) is a Network Layer Protocol.



- IP's current version is Version 4 (IPv4). It is specified in RFC 891.

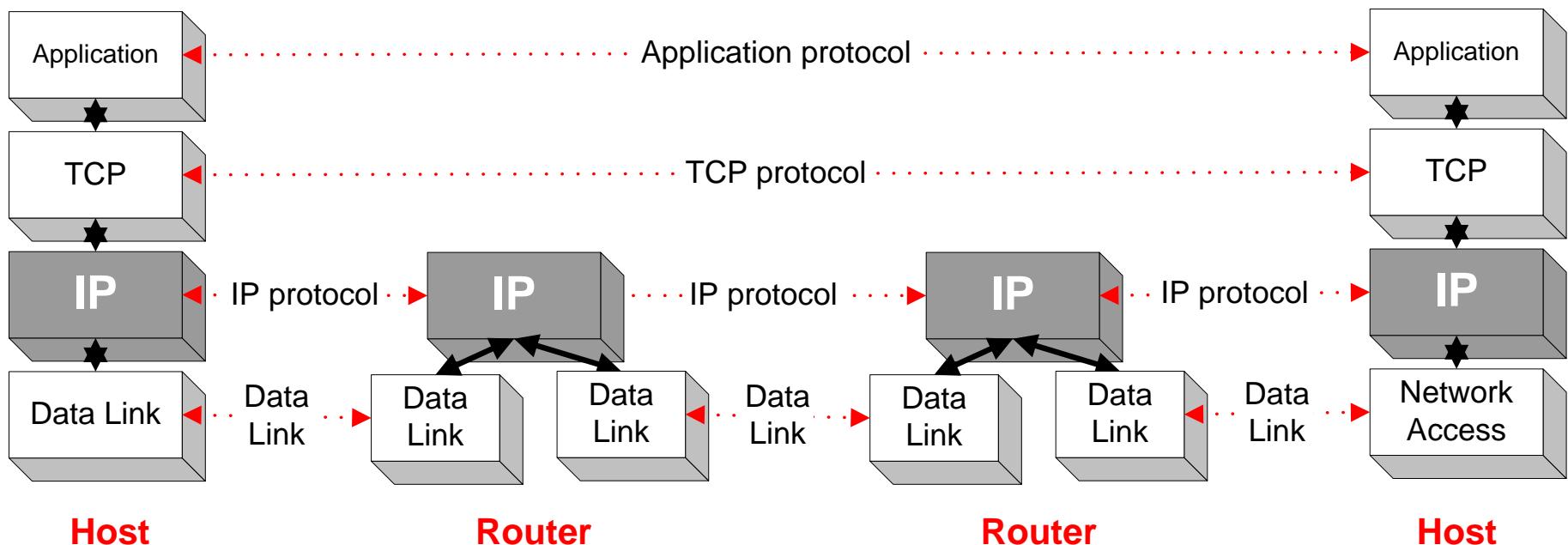
IP: The waist of the hourglass

- IP is the waist of the hourglass of the Internet protocol architecture
- Multiple higher-layer protocols
- Multiple lower-layer protocols
- Only one protocol at the network layer.



Application protocol

- IP is the highest layer protocol which is implemented at both routers and hosts

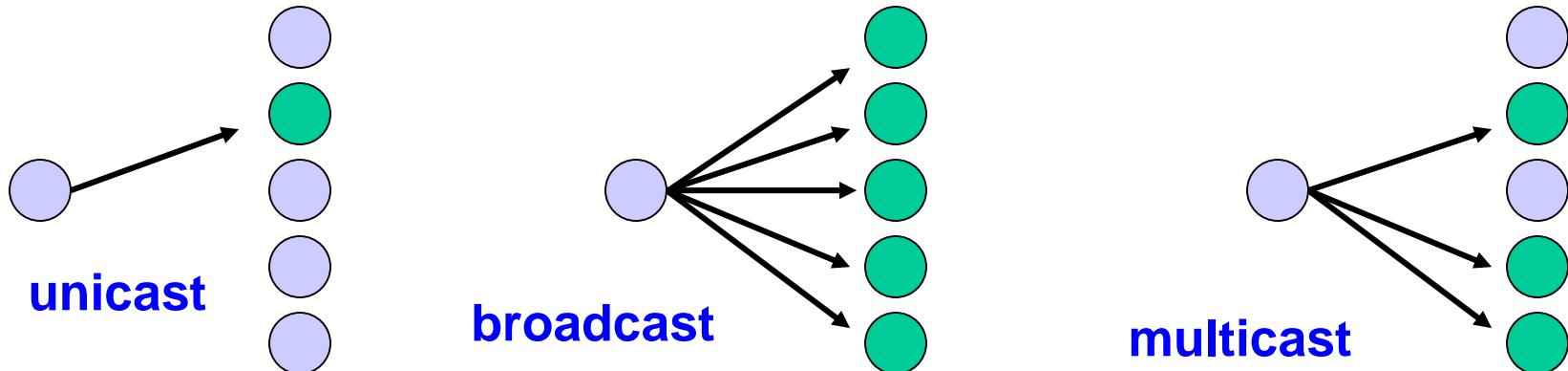


IP Service

- Delivery service of IP is minimal
- IP provides an **unreliable connectionless** best effort service (also called: “datagram service”).
 - **Unreliable:** IP does not make an attempt to recover lost packets
 - **Connectionless:** Each packet (“datagram”) is handled independently. IP is not aware that packets between hosts may be sent in a logical sequence
 - **Best effort:** IP does not make guarantees on the service (no throughput guarantee, no delay guarantee,...)
- Consequences:
 - Higher layer protocols have to deal with losses or with duplicate packets
 - Packets may be delivered out-of-sequence

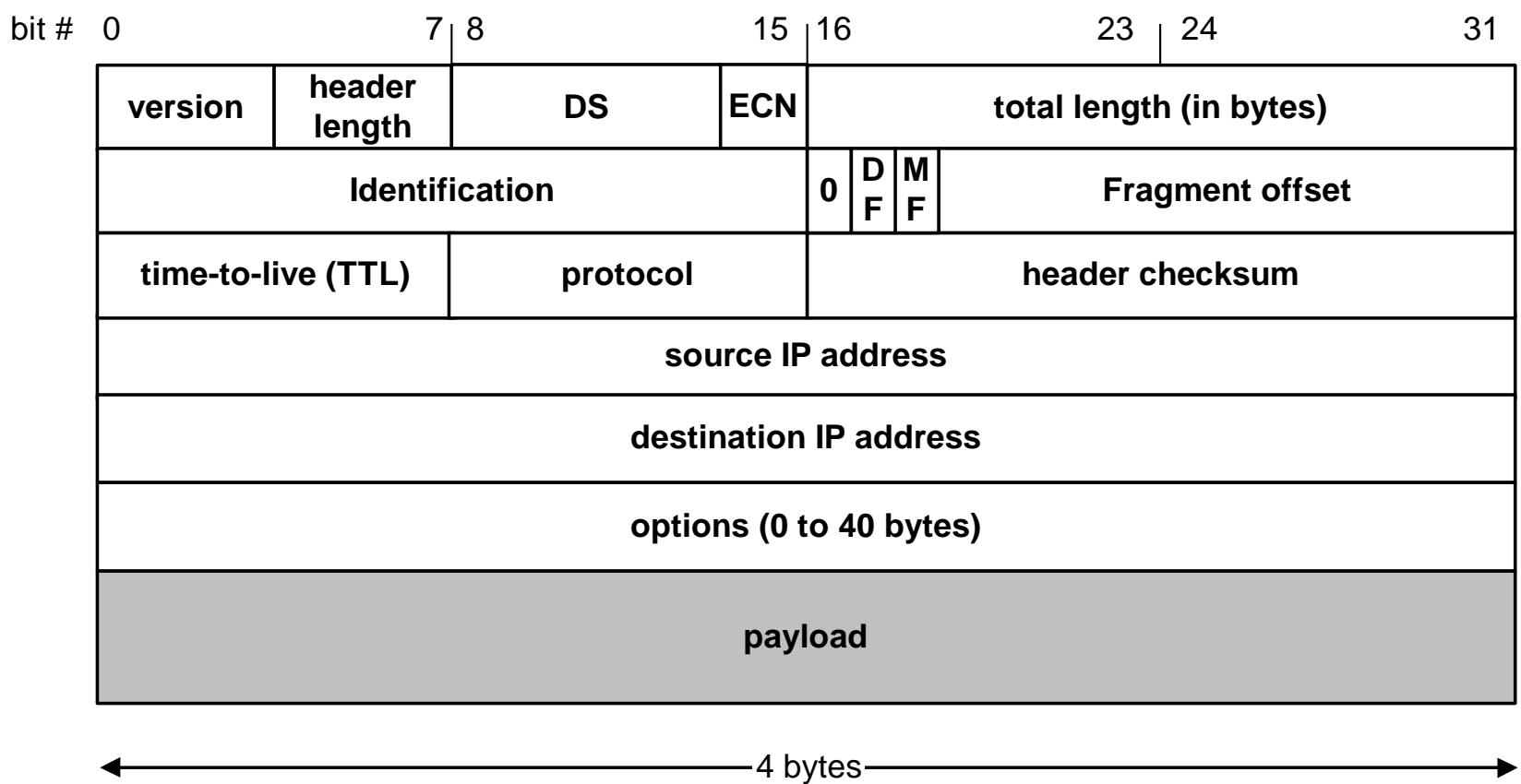
IP Service

- IP supports the following services:
 - one-to-one (unicast)
 - one-to-all (broadcast)
 - one-to-several (multicast)



- IP multicast also supports a many-to-many service.
- IP multicast requires support of other protocols (IGMP, multicast routing)

IP Datagram Format



- $20 \text{ bytes} \leq \text{Header Size} < 2^4 \times 4 \text{ bytes} = 60 \text{ bytes}$
- $20 \text{ bytes} \leq \text{Total Length} < 2^{16} \text{ bytes} = 65536 \text{ bytes}$

IP Datagram Format

- **Question:** In which order are the bytes of an IP datagram transmitted?
- **Answer:**
 - Transmission is row by row
 - For each row:
 1. First transmit bits 0-7
 2. Then transmit bits 8-15
 3. Then transmit bits 16-23
 4. Then transmit bits 24-31
- This is called **network byte** order or **big endian** byte ordering.
- **Note:** Many computers (incl. Intel processors) store 32-bit words in little endian format. Others (incl. Motorola processors) use big endian.

Big endian vs. small endian

- Conventions to store a multibyte word
- Example: a 4 byte Long Integer **Byte3 Byte2 Byte1 Byte0**

LittleEndian

- Stores the low-order byte at the lowest address and the highest order byte in the highest address.

Base Address+0 Byte0

Base Address+1 Byte1

Base Address+2 Byte2

Base Address+3 Byte3

BigEndian

- Stores the high-order byte at the lowest address, and the low-order byte at the highest address.

Base Address+0 Byte3

Base Address+1 Byte2

Base Address+2 Byte1

Base Address+3 Byte0

- Intel processors use this order

Motorola processors use big endian.

Fields of the IP Header

- **Version (4 bits)**: current version is 4, next version will be 6.
- **Header length (4 bits)**: length of IP header, in multiples of 4 bytes
- **DS/ECN field (1 byte)**
 - This field was previously called as Type-of-Service (TOS) field. The role of this field has been re-defined, but is “backwards compatible” to TOS interpretation
 - **Differentiated Service (DS) (6 bits)**:
 - Used to specify service level (currently not supported in the Internet)
 - **Explicit Congestion Notification (ECN) (2 bits)**:
 - New feedback mechanism used by TCP

Fields of the IP Header

- **Identification (16 bits):** Unique identification of a datagram from a host. Incremented whenever a datagram is transmitted
- **Flags (3 bits):**
 - First bit always set to 0
 - DF bit (Do not fragment)
 - MF bit (More fragments)

Will be explained later → Fragmentation

Fields of the IP Header

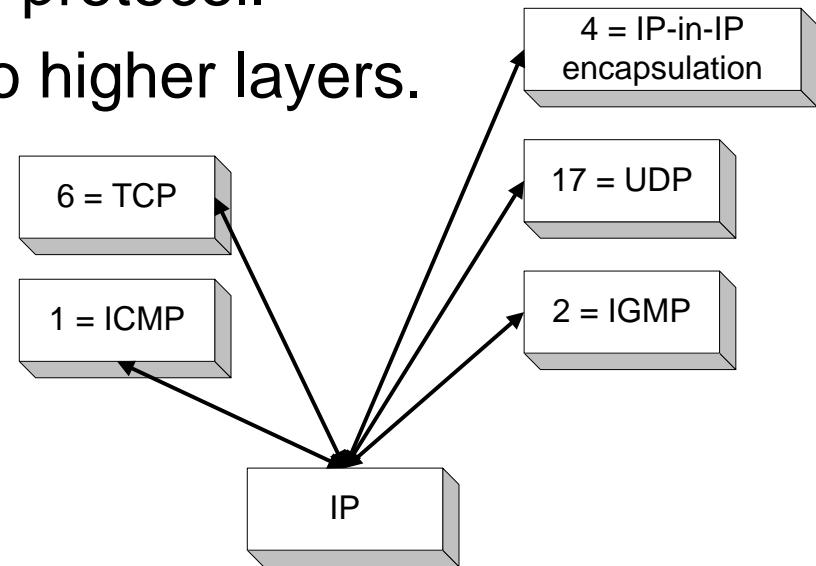
- **Time To Live (TTL) (1 byte):**
 - Specifies longest paths before datagram is dropped
 - Role of TTL field: Ensure that packet is eventually dropped when a routing loop occurs

Used as follows:

- Sender sets the value (e.g., 64)
- Each router decrements the value by 1
- When the value reaches 0, the datagram is dropped

Fields of the IP Header

- **Protocol (1 byte):**
 - Specifies the higher-layer protocol.
 - Used for demultiplexing to higher layers.



- **Header checksum (2 bytes):** A simple 16-bit long checksum which is computed for the header of the datagram.

Fields of the IP Header

- **Options:**
 - Security restrictions
 - Record Route: each router that processes the packet adds its IP address to the header.
 - Timestamp: each router that processes the packet adds its IP address and time to the header.
 - (loose) Source Routing: specifies a list of routers that must be traversed.
 - (strict) Source Routing: specifies a list of the only routers that can be traversed.
- **Padding:** Padding bytes are added to ensure that header ends on a 4-byte boundary

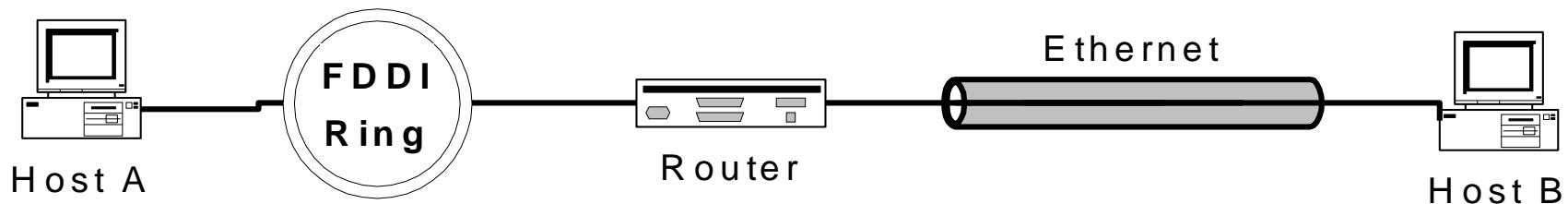
Maximum Transmission Unit

- Maximum size of IP datagram is 65535, but the data link layer protocol generally imposes a limit that is much smaller
- Example:
 - Ethernet frames have a maximum payload of 1500 bytes
→ IP datagrams encapsulated in Ethernet frame cannot be longer than 1500 bytes
- The limit on the maximum IP datagram size, imposed by the data link protocol is called **maximum transmission unit (MTU)**
- MTUs for various data link protocols:

Ethernet:	1500	FDDI:	4352
802.3:	1492	ATM AAL5:	9180
802.5:	4464	PPP:	negotiated

IP Fragmentation

- What if the size of an IP datagram exceeds the MTU?
IP datagram is fragmented into smaller units.
- What if the route contains networks with different MTUs?



MTUs:

FDDI: 4352

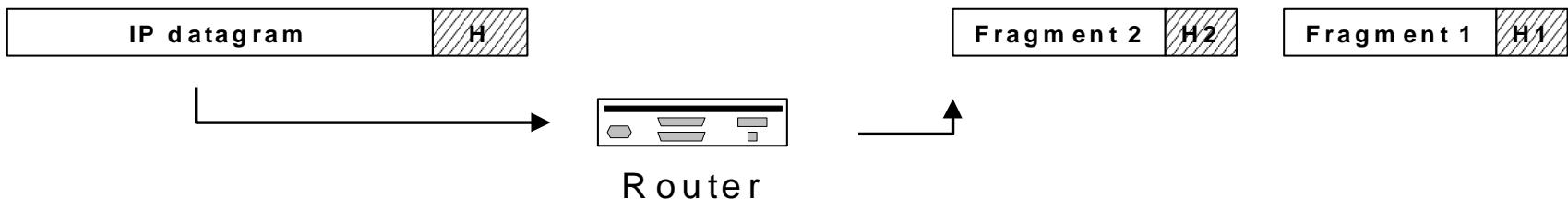
Ethernet: 1500

- **Fragmentation:**

- IP router splits the datagram into several datagram
- Fragments are reassembled at receiver

Where is Fragmentation done?

- Fragmentation can be done at the sender or at intermediate routers
- The same datagram can be fragmented several times.
- Reassembly of original datagram is only done at destination hosts !!



What's involved in Fragmentation?

- The following fields in the IP header are involved:

version	header length	DS	ECN	total length (in bytes)			
Identification				0	D	M	
				F	F		Fragment offset
time-to-live (TTL)	protocol	header checksum					

Identification

When a datagram is fragmented, the identification is the same in all fragments

Flags

DF bit is set: Datagram cannot be fragmented and must be discarded if MTU is too small

MF bit set: This datagram is part of a fragment and an additional fragment follows this one

What's involved in Fragmentation?

- The following fields in the IP header are involved:

version	header length	DS	ECN	total length (in bytes)			
Identification				0	D	M	
				F	F		Fragment offset
time-to-live (TTL)	protocol		header checksum				

Fragment offset

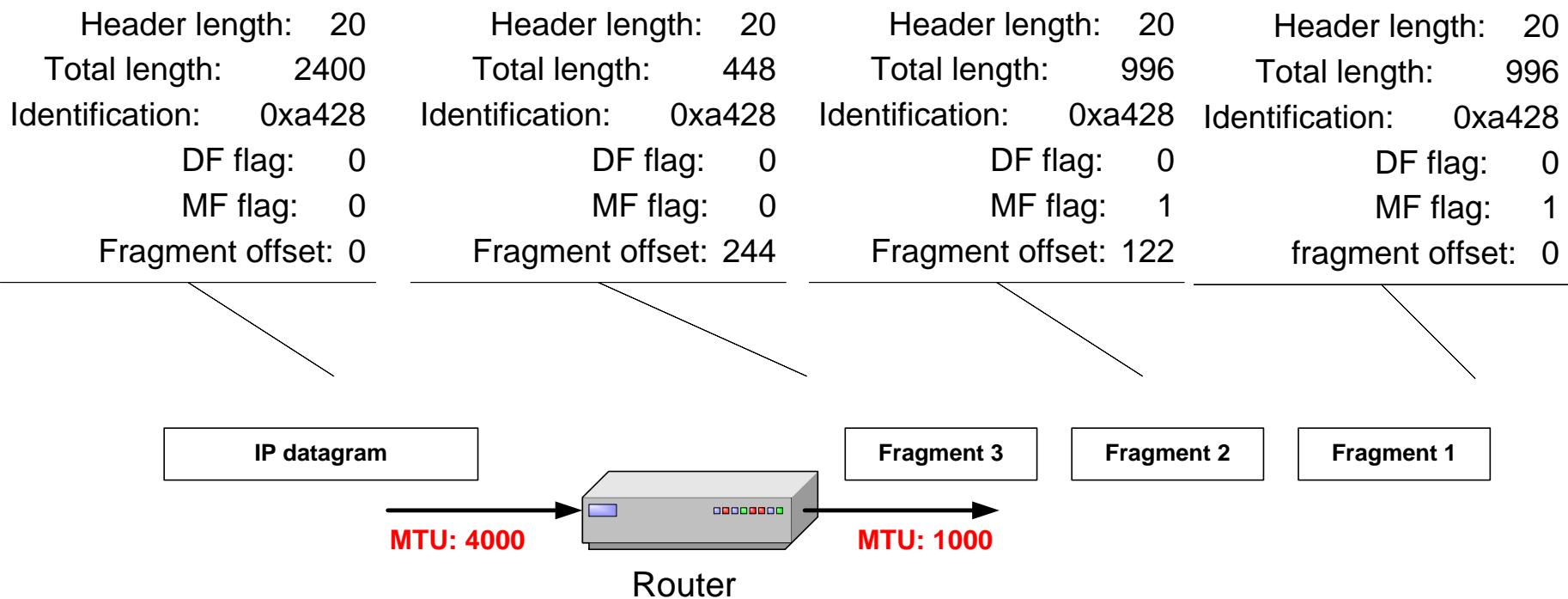
Offset of the payload of the current fragment in the original datagram

Total length

Total length of the current fragment

Example of Fragmentation

- A datagram with size 2400 bytes must be fragmented according to an MTU limit of 1000 bytes



2. Addressing in IP

CONTENTS

- INTRODUCTION
- CLASSFUL ADDRESSING
 - Different Network Classes
 - Subnetting
- Classless Addressing
 - Supernetting
- CIDR (Classless Interdomain Routing)

What is an IP Address?

*An IP address is a
32-bit
address.*

Note

*The IP addresses
are
unique.*

Address space rule

The address space in a protocol that uses N-bits to define an address is:

$$2^N$$

IPv4 address space

The address space of IPv4 is

2^{32}

or

4,294,967,296.

Binary Notation

01110101 10010101 00011101 11101010

Dotted-decimal notation

10000000

00001011

00000011

00011111

128.11.3.31

Hexadecimal Notation

0111 0101 1001 0101 0001 1101 1110 1010

75

95

1D

EA

0x75951DEA

Example 1

Change the following IP address from binary notation to dotted-decimal notation.

10000001 00001011 00001011 11101111

Solution

129.11.11.239

Example 2

Change the following IP address from dotted-decimal notation to binary notation:

111.56.45.78

Solution

01101111 00111000 00101101 01001110

Example 3

Find the error in the following IP Address

111.56.045.78

Solution

There are no leading zeroes in
Dotted-decimal notation (045)

Example 3 (continued)

Find the error in the following IP Address

75.45.301.14

Solution

In decimal notation each number ≤ 255
301 is out of the range

Example 4

Change the following binary IP address
Hexadecimal notation

10000001 00001011 00001011 11101111

Solution

0X810B0BEF or 810B0BEF16

CLASSFUL ADDRESSING

Occupation of the address space

Address space



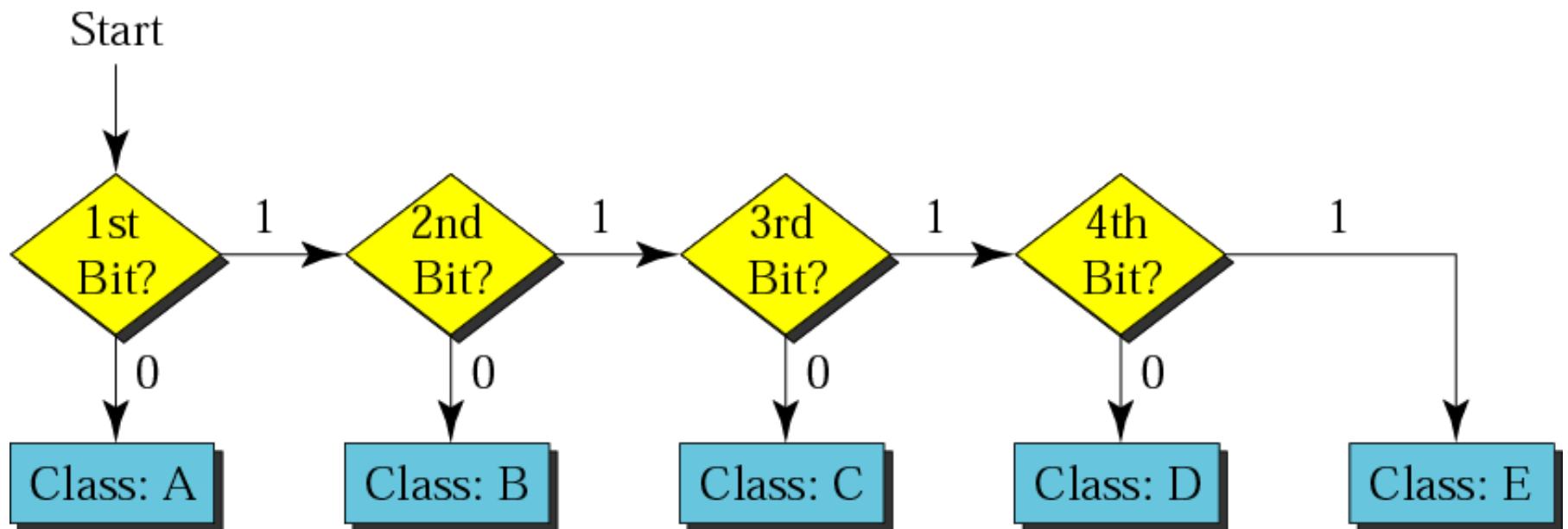
In classful addressing the address space is divided into 5 classes:

A, B, C, D, and E.

Finding the class in binary notation

	First byte	Second byte	Third byte	Fourth byte
Class A	0			
Class B	10			
Class C	110			
Class D	1110			
Class E	1111			

Finding the address class



Example 5

Show that Class **A** has
 $2^{31} = 2,147,483,648$ addresses

Example 6

Find the class of the following IP addresses

00000001 00001011 00001011 11101111
11000001 00001011 00001011 11101111

Solution

- 00000001 00001011 00001011 11101111
1st is 0, hence it is Class A
- 11000001 00001011 00001011 11101111
1st and 2nd bits are 1, and 3rd bit is 0 hence, Class C

Finding the class in decimal notation

	First byte	Second byte	Third byte	Fourth byte
Class A	0 to 127			
Class B	128 to 191			
Class C	192 to 223			
Class D	224 to 239			
Class E	240 to 255			

Example 7

Find the class of the following addresses

158.223.1.108

227.13.14.88

Solution

- 158.223.1.108

1st byte = 158 (128<158<191) class B

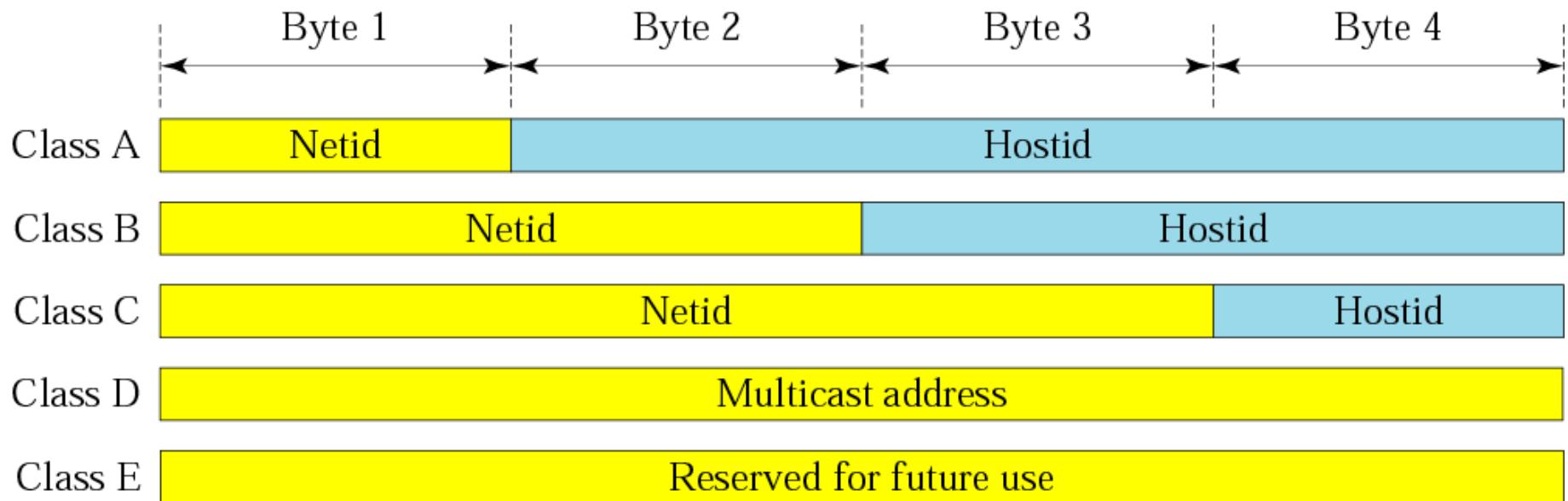
- 227.13.14.88

1st byte = 227 (224<227<239) class D

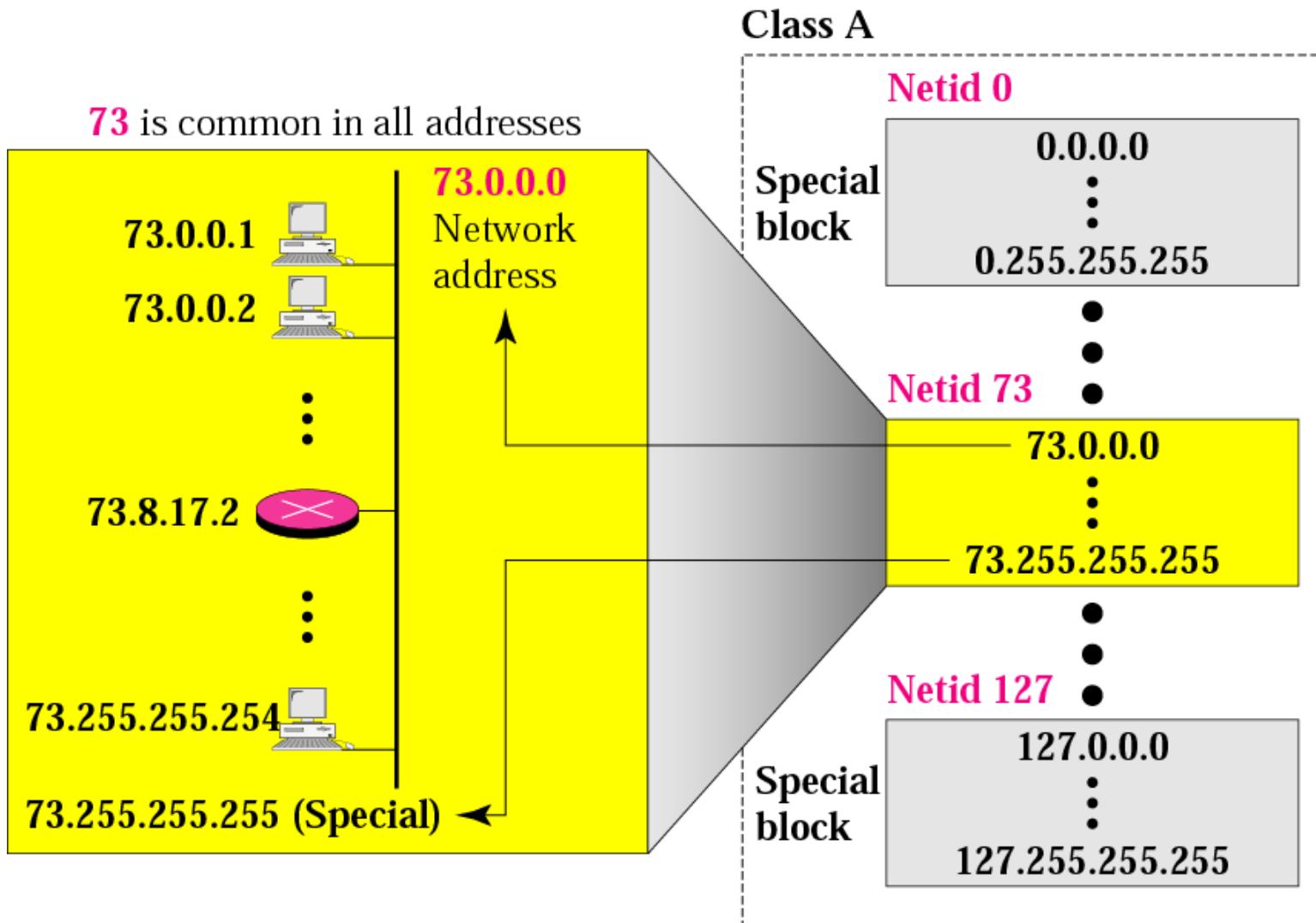
IP address with appending port number

- 158.128.1.108:25
- the first octet before colon is the IP address
- The number after colon (25) is the port number

Netid and hostid



Blocks in class A

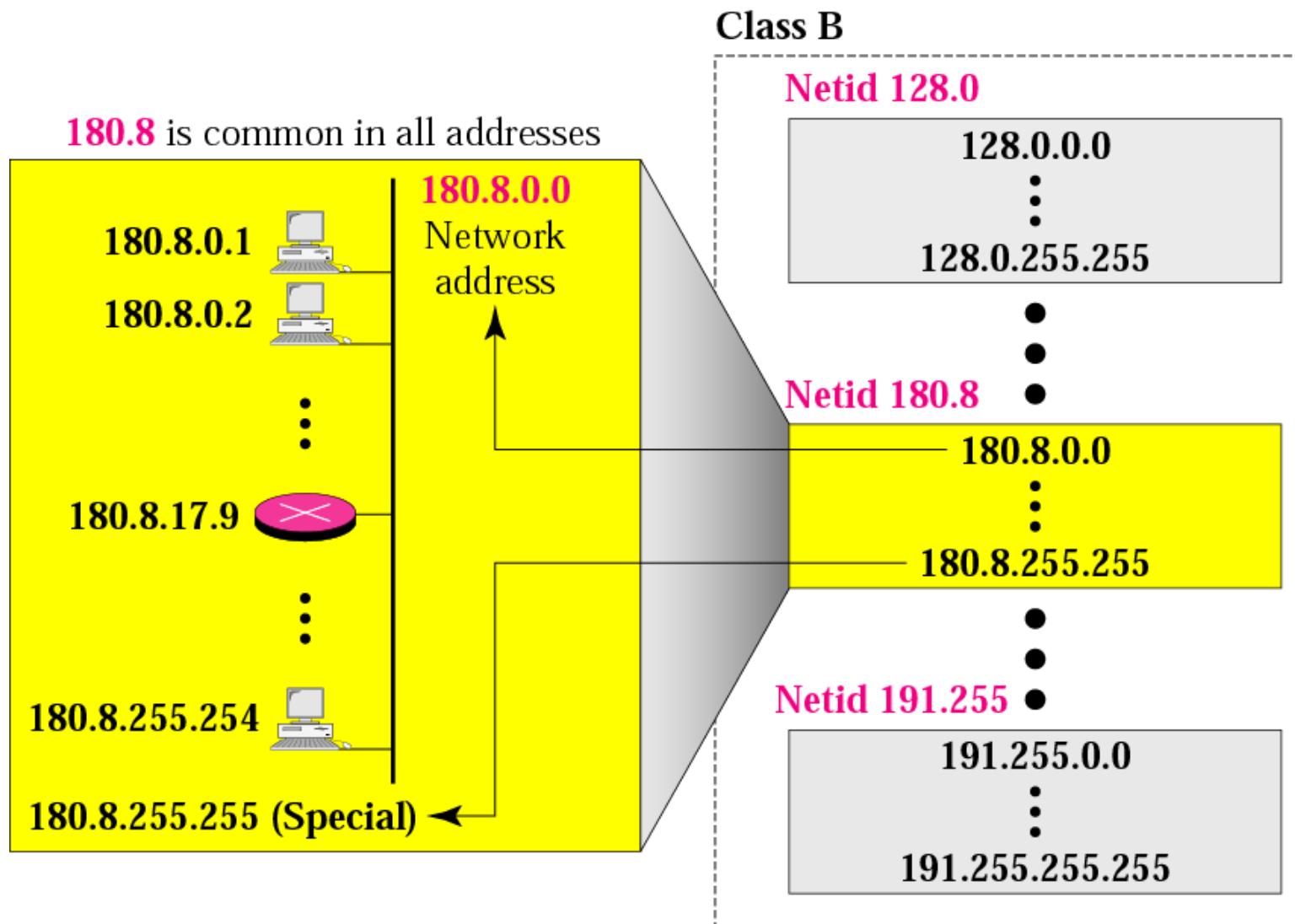


128 blocks: 16,777,216 addresses in each block 47

Note

*Millions of class A addresses
are wasted.*

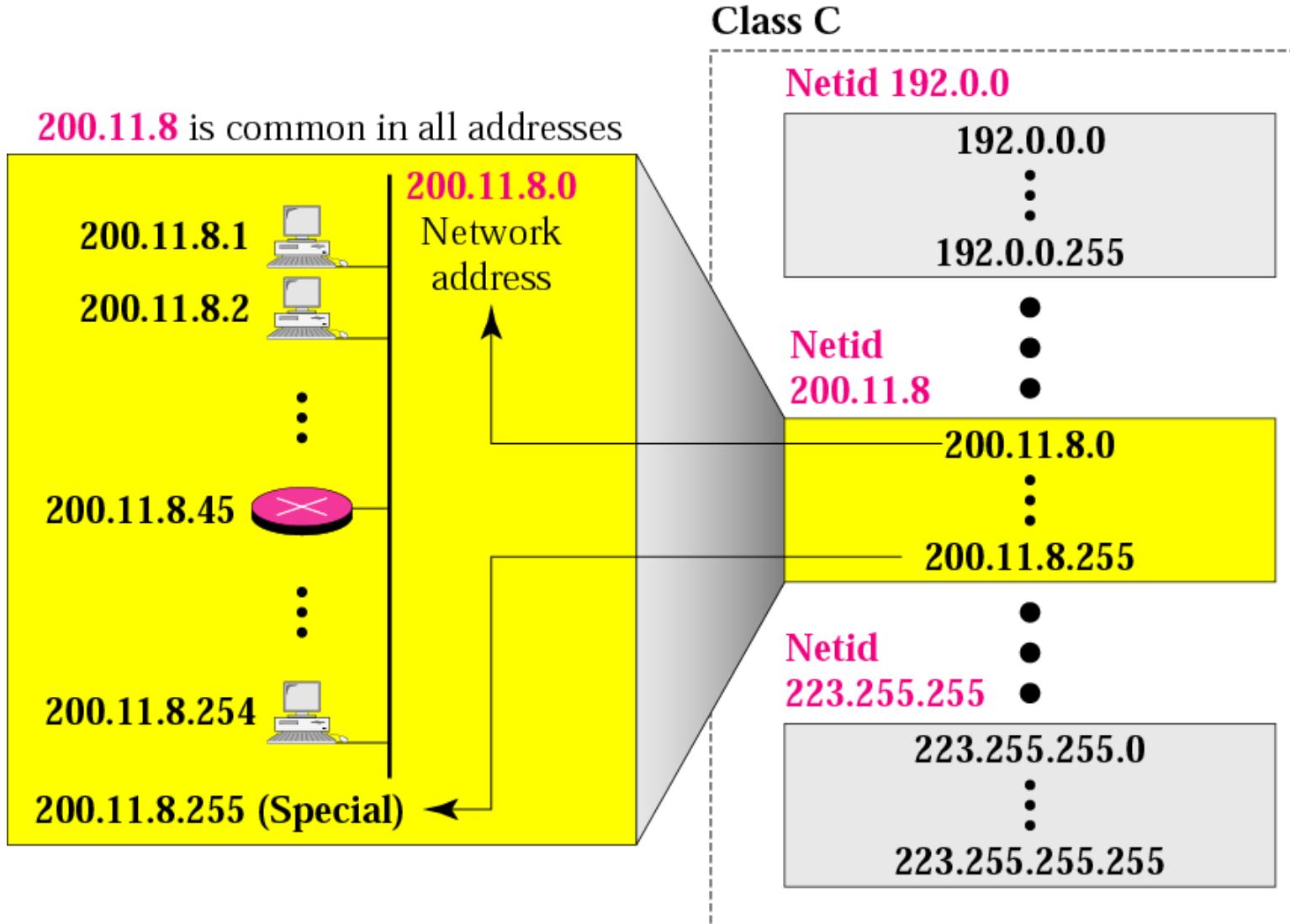
Blocks in class B



Note

*Many class B addresses
are wasted.*

Blocks in class C



Note

***The number of addresses in
a class C block
is smaller than
the needs of most organizations.***

Note

*Class D addresses
are used for multicasting;
there is only
one block in this class.*

Note

*Class E addresses are reserved
for special purposes;
most of the block is wasted.*

Network Addresses

The network address is the first address.

The network address defines the network to the rest of the Internet.

Given the network address, we can find the class of the address, the block, and the range of the addresses in the block

Note

*In classful addressing,
the network address
(the first address in the block)
is the one that is assigned
to the organization.*

Example 8

Given the network address 132.21.0.0, find the class, the block, and the range of the addresses

Solution

The 1st byte is between 128 and 191.

Hence, Class B

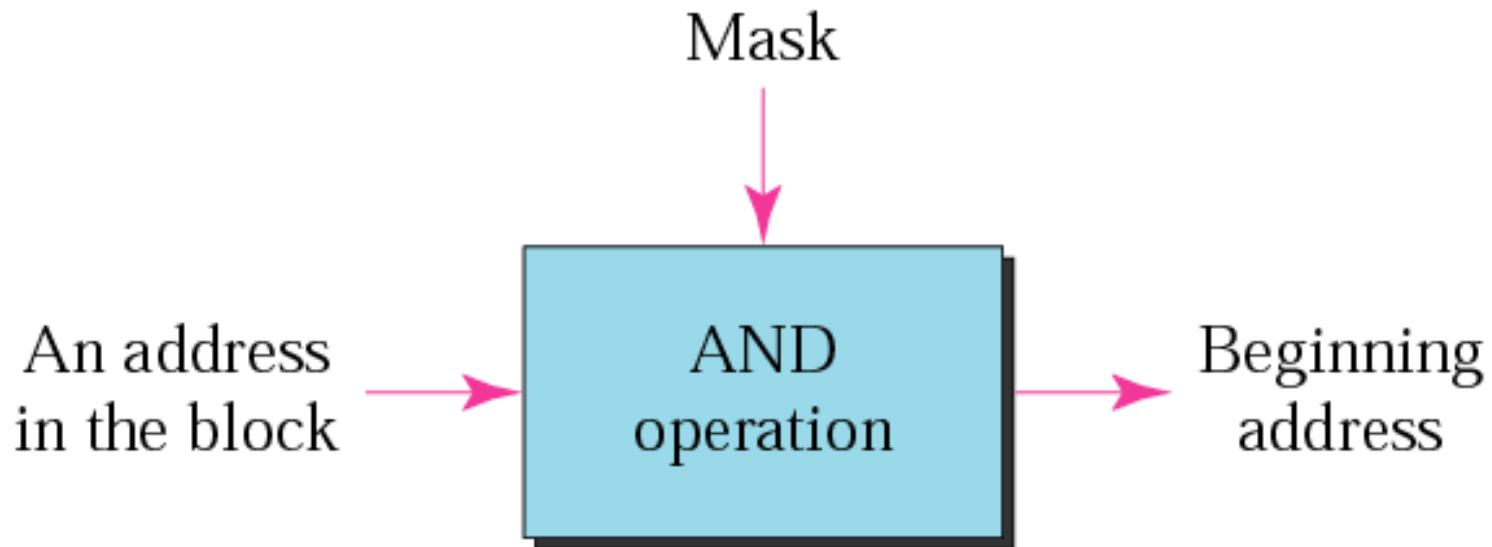
The block has a netid of 132.21.

The addresses range from
132.21.0.0 to 132.21.255.255.

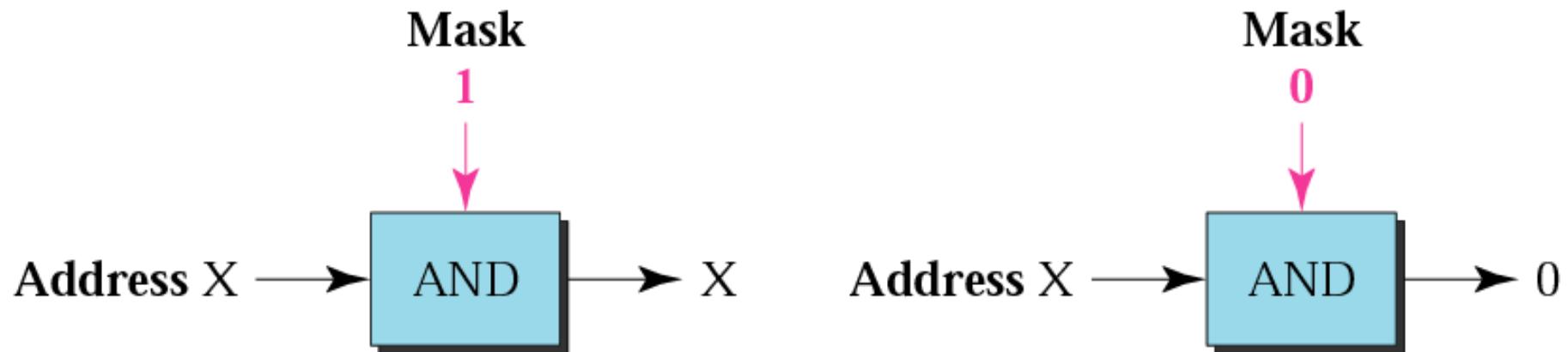
Mask

- A mask is a 32-bit binary number.
- The mask is **ANDeD** with IP address to get
 - The bloc address (Network address)
 - **Mask And IP address = Block Address**

Masking concept



AND operation



Note

*The network address is the beginning address of each block. It can be found by applying the default mask to any of the addresses in the block (including itself). It retains the **netid** of the block and sets the **hostid** to zero.*

Default Mak

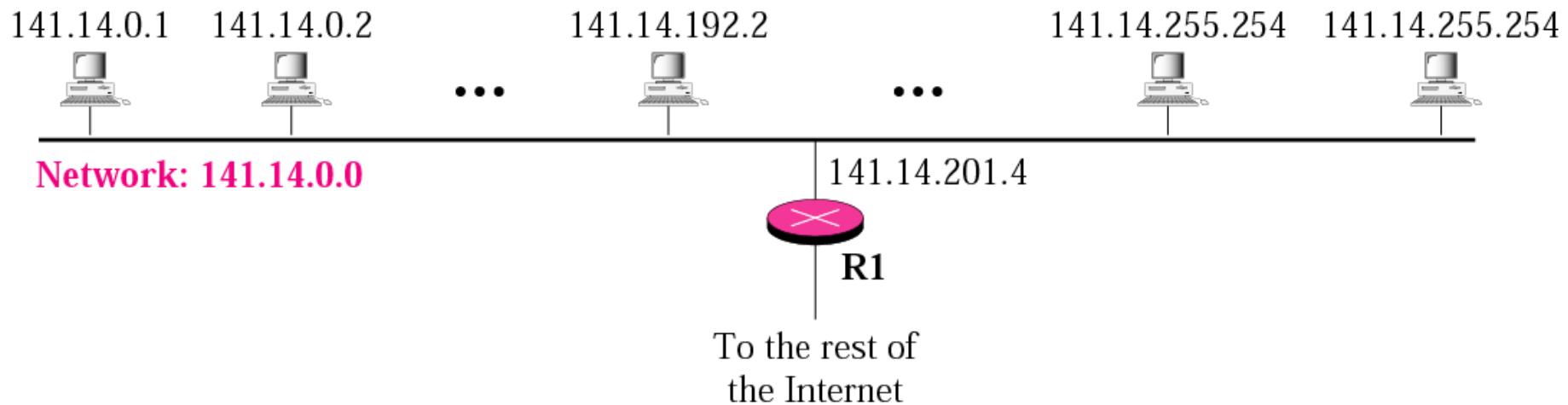
- Class A default mask is 255.0.0.0
- Class B default mask is 255.255.0.0
- Class C Default mask 255.255.255.0

SUBNETTING

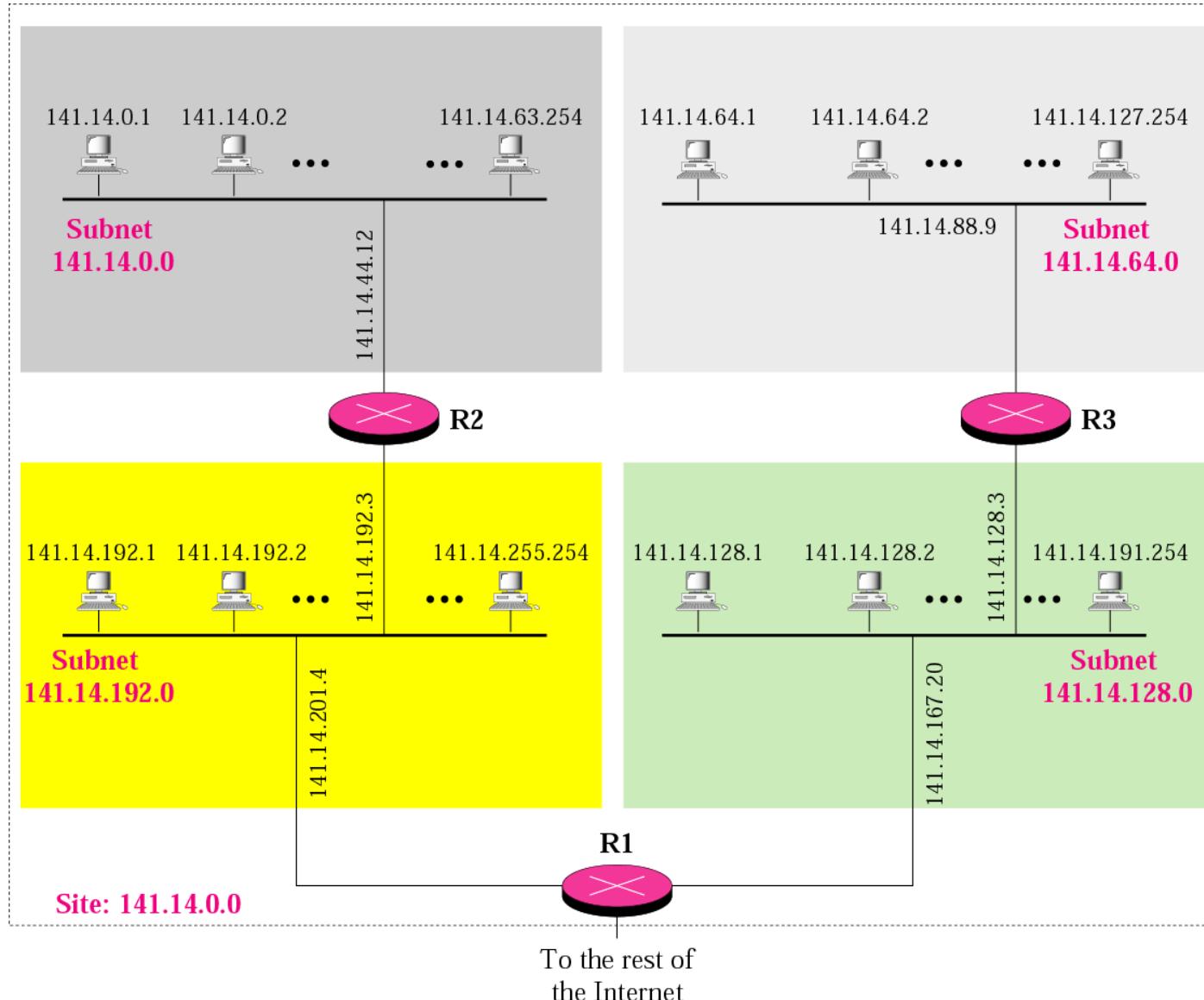
Note

*IP addresses are designed with
two levels of hierarchy.*

A network with two levels of hierarchy (not subnetted)



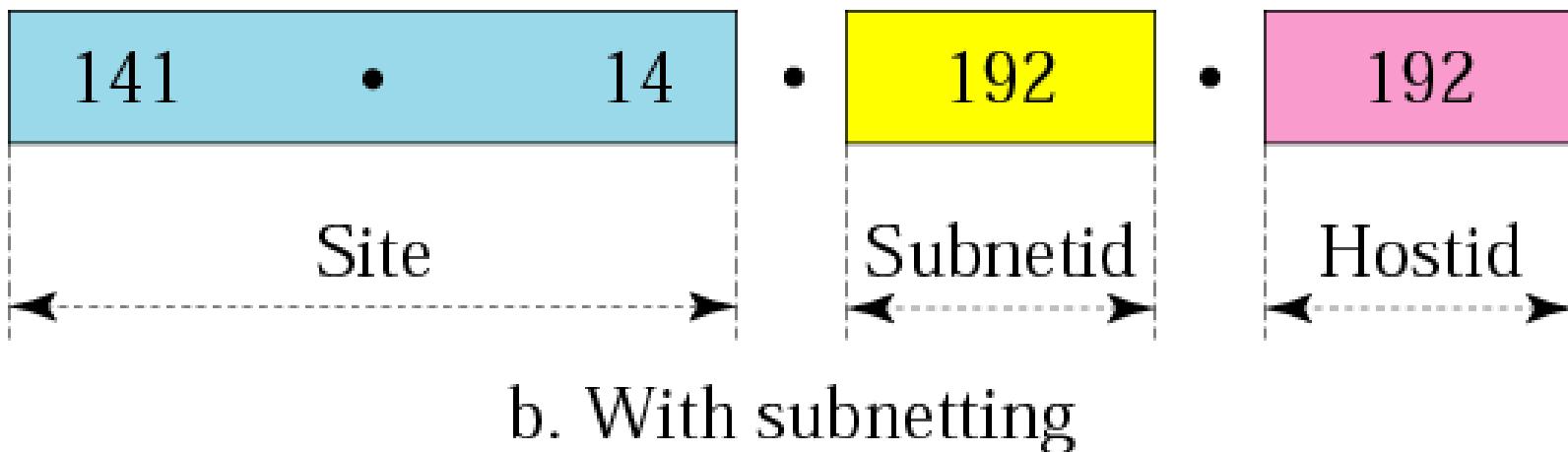
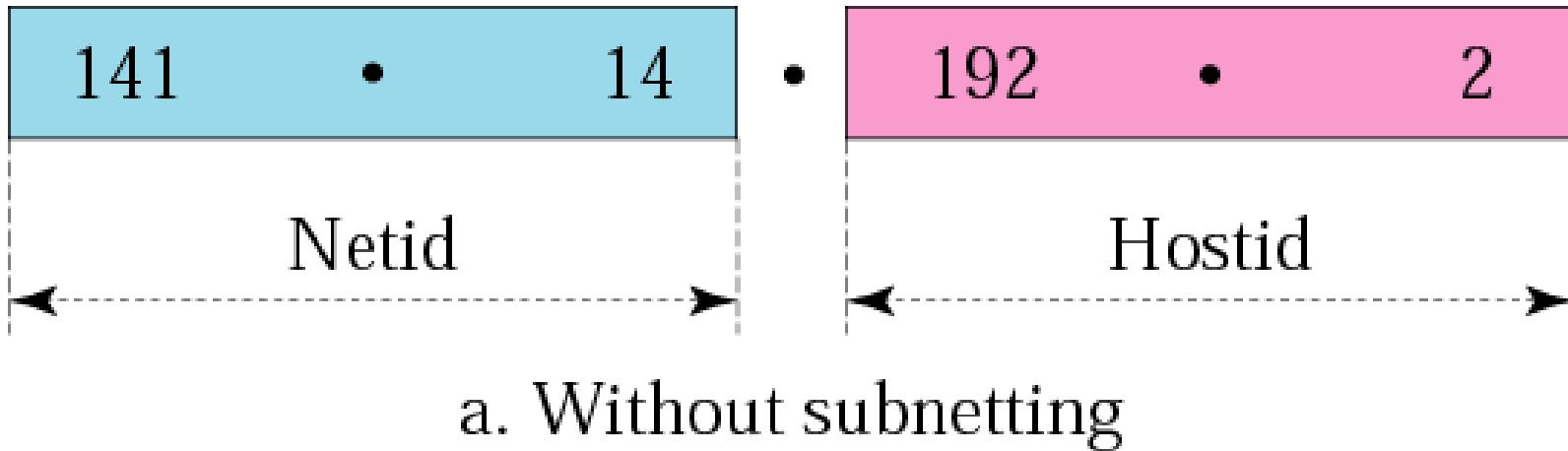
A network with three levels of hierarchy (subnetted)



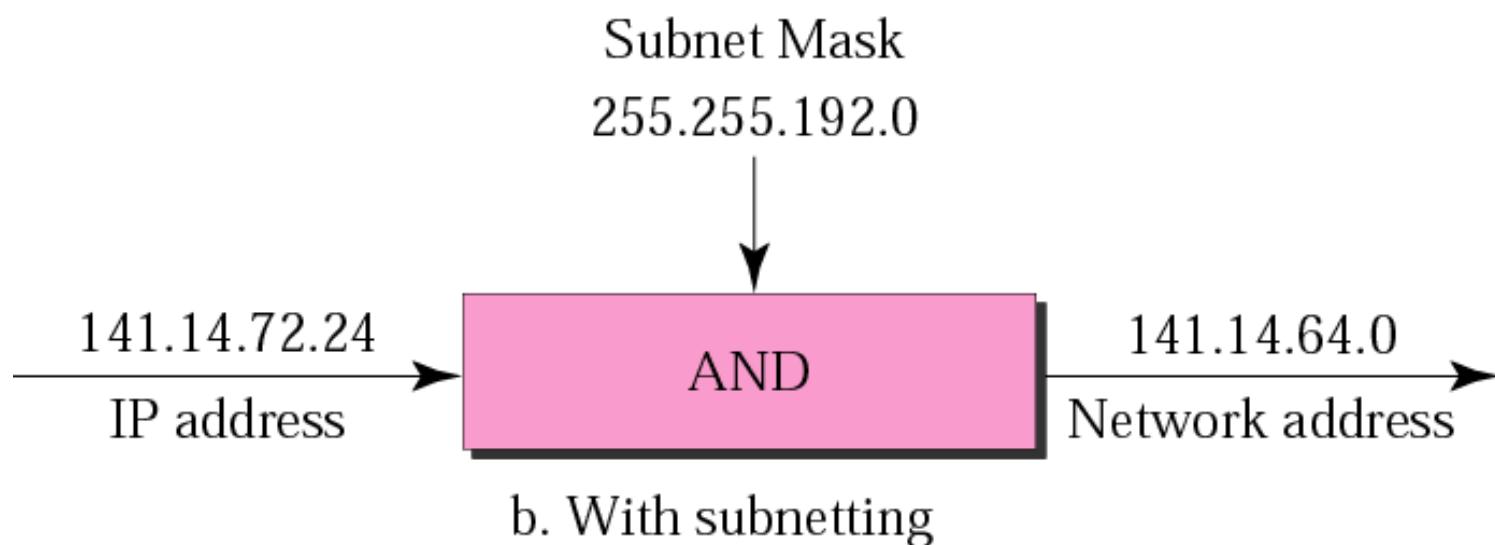
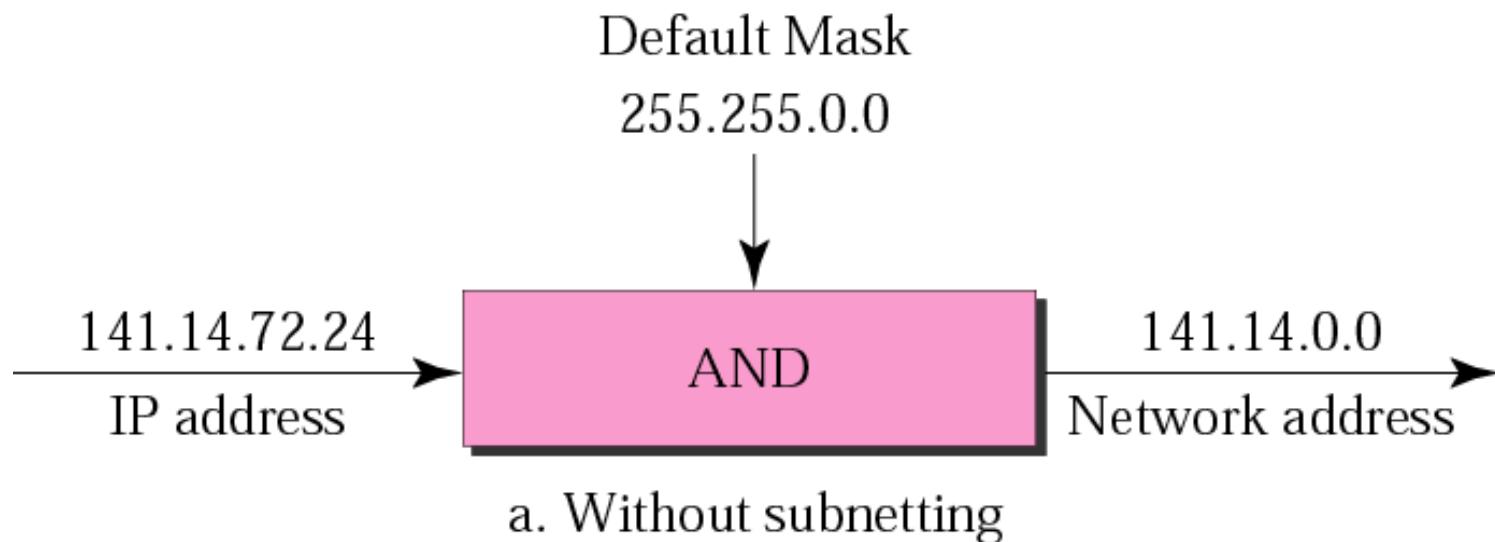
Note

Subnetting is done by borrowing bits from the host part and add them the network part.

Addresses in a network with and without subnetting



Default mask and subnet mask



Finding the Subnet Address

Given an IP address, we can find the subnet address the same way we found the network address. We apply the mask to the address. We can do this in two ways: straight or short-cut.

Straight Method

In the straight method, we use binary notation for both the address and the mask and then apply the AND operation to find the subnet address.

Example 9

What is the subnetwork address if the destination address is 200.45.34.56 and the subnet mask is 255.255.240.0?

Solution

11001000 00101101 00100010 00111000

11111111 11111111 11110000 00000000

11001000 00101101 00100000 00000000

The subnetwork address is **200.45.32.0**.

Short-Cut Method

- ** If the byte in the mask is 255, copy the byte in the address.
- ** If the byte in the mask is 0, replace the byte in the address with 0.
- ** If the byte in the mask is neither 255 nor 0, we write the mask and the address in binary and apply the AND operation.

Example 10

What is the subnetwork address if the destination address is 19.30.80.5 and the mask is 255.255.192.0?

Solution

See next slide

Solution

IP Address

19	•	30	•	84	•	5
----	---	----	---	----	---	---

Mask

255	•	255	•	192	•	0
-----	---	-----	---	-----	---	---

19	•	30	•	64	•	0
----	---	----	---	----	---	---

Subnet Address

84	0	1	0	1	0	0	1	0	0
192	1	1	0	0	0	0	0	0	0
<hr/>									
64	0	1	0	0	0	0	0	0	0

Comparison of a default mask and a subnet mask

255.255.0.0

Default Mask	11111111	11111111	00000000	00000000
--------------	----------	----------	----------	----------

16

255.255.224.0

Subnet Mask	11111111	11111111	111	00000	00000000
-------------	----------	----------	-----	-------	----------

3

13

Note

*The number of subnets must be
a power of 2.*

Example 11

A company is granted the site address 201.70.64.0 (class C). The company needs six subnets. Design the subnets.

Solution

The number of 1s in the default mask is 24 (class C).

Solution (Continued)

The company needs six subnets. This number 6 is not a power of 2. The next number that is a power of 2 is 8 (2^3).

We need 3 more 1s in the subnet mask. The total number of 1s in the subnet mask is 27 ($24 + 3$).

The total number of 0s is 5 ($32 - 27$). The mask is

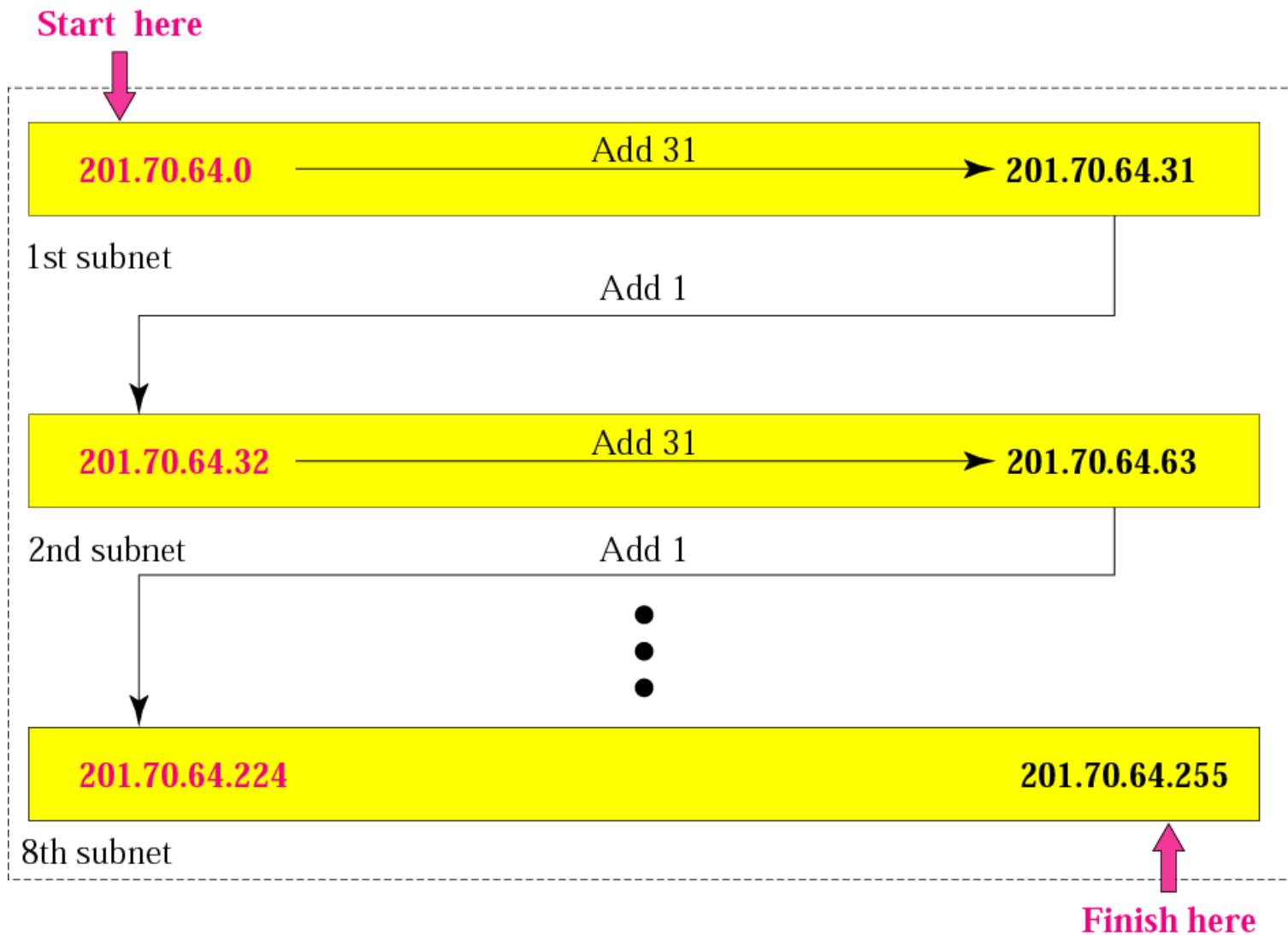
11111111 11111111 11111111 11100000

or

255.255.255.224

The number of subnets is 8. The number of addresses in each subnet is 2^5 (5 is the number of 0s) or 32.

Example 3



Example 12

A company is granted the site address 181.56.0.0 (class B).

The company needs 1000 subnets. Design the subnets.

Solution

The number of 1s in the default mask is 16 (class B).

Solution (Continued)

The company needs 1000 subnets. This number is not a power of 2. The next number that is a power of 2 is 1024 (2^{10}). We need 10 more 1s in the subnet mask.

The total number of 1s in the subnet mask is 26 ($16 + 10$).

The total number of 0s is 6 ($32 - 26$).

Solution (Continued)

The mask is

11111111 11111111 11111111 11000000

or

255.255.255.192.

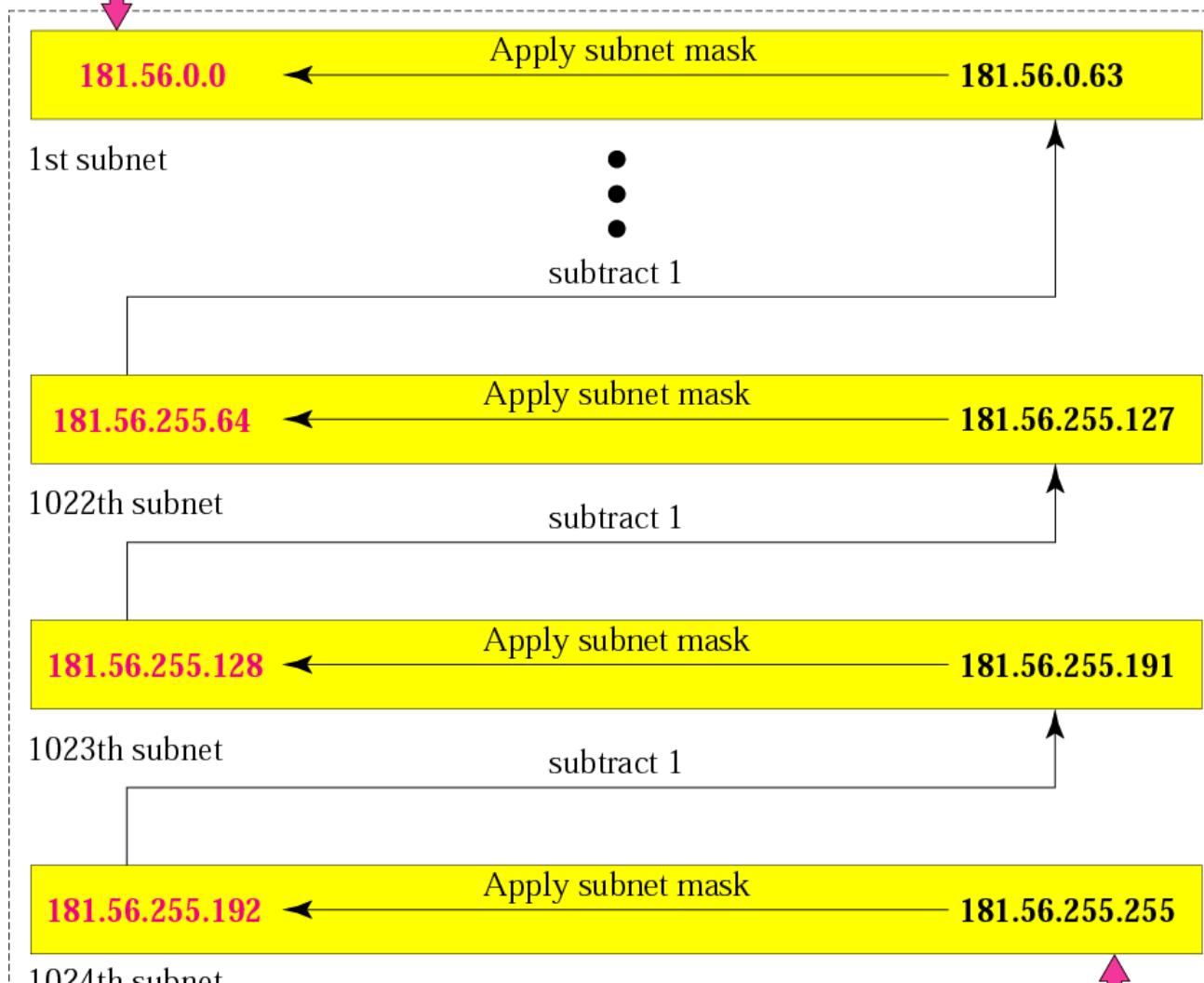
The number of subnets is 1024.

The number of addresses in each subnet is 2^6 (6 is the number of 0s) or 64.

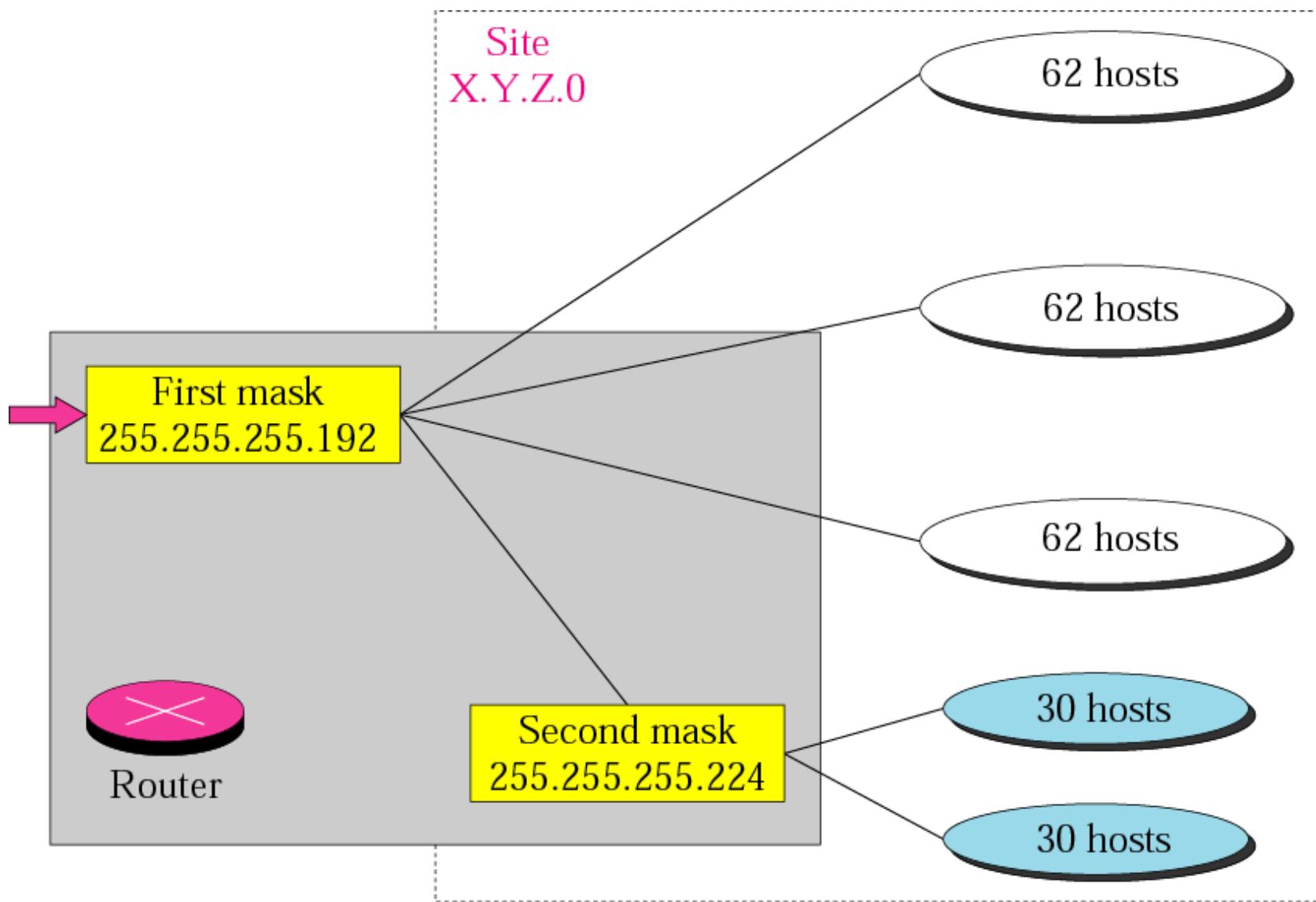
See next slide

Example 4

Finish here



Variable-length subnetting

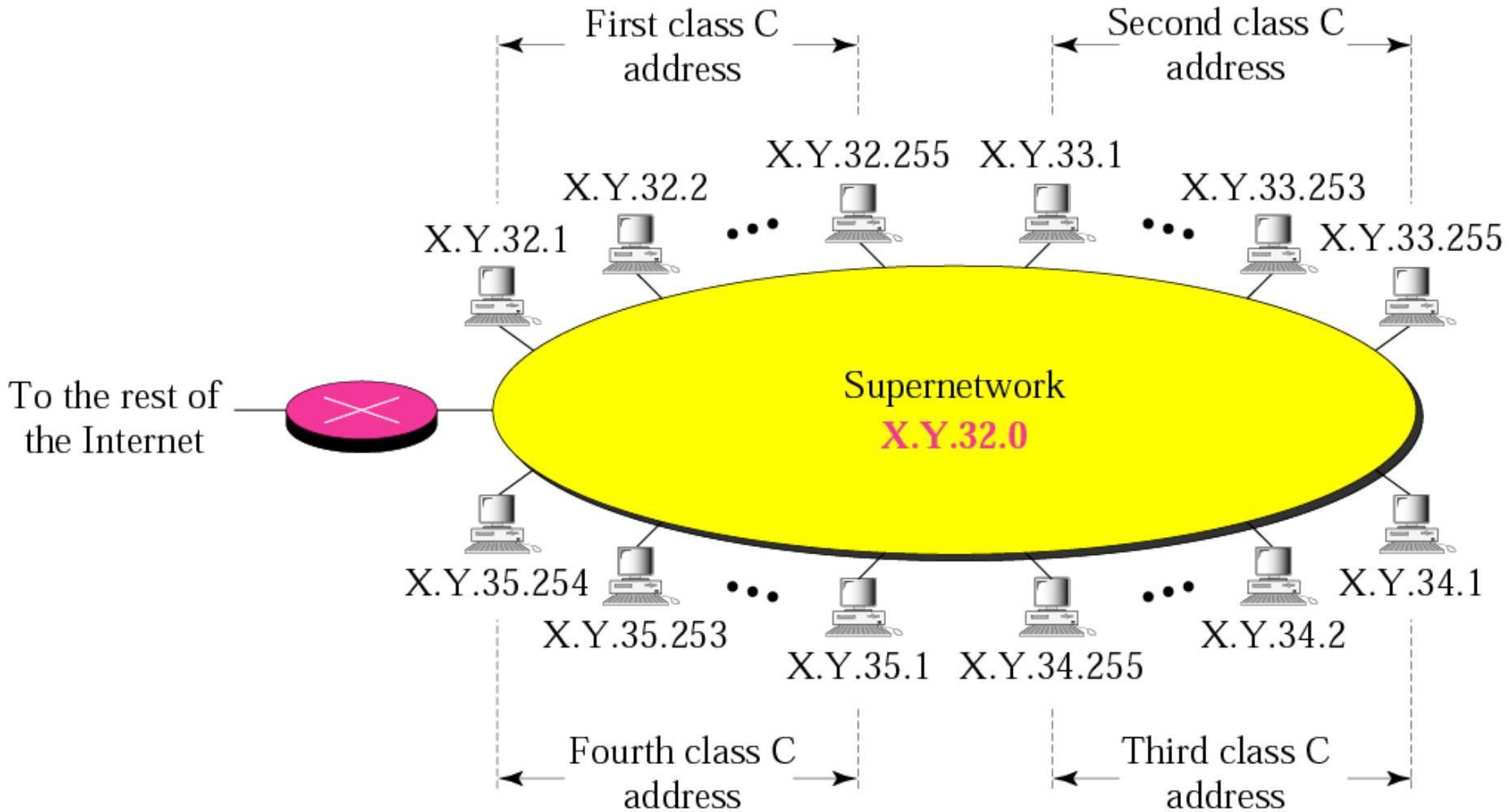


SUPERNETTING

What is supernetting?

- Supernetting is the opposite of subnetting
- In subnetting you borrow bits from the host part
- Supernetting is done by borrowing bits from the network side.
- And combine a group of networks into one large supernet.

A supernet



Rules:

- ▲ The number of blocks must be a power of 2 (1, 2, 4, 8, 16, . . .).
- ▲ The blocks must be contiguous in the address space (no gaps between the blocks).
- ▲ The third byte of the first address in the superblock must be evenly divisible by the number of blocks. In other words, if the number of blocks is N , the third byte must be divisible by N .

Example 5

A company needs 600 addresses.

Which of the following set of class C blocks can be used to form a supernet for this company?

198.47.32.0 198.47.33.0 198.47.34.0

198.47.32.0 198.47.42.0 198.47.52.0 198.47.62.0

198.47.31.0 198.47.32.0 198.47.33.0 198.47.52.0

198.47.32.0 198.47.33.0 198.47.34.0 198.47.35.0

Solution

- 1: No, there are only three blocks.**
- 2: No, the blocks are not contiguous.**
- 3: No, 31 in the first block is not divisible by 4.**
- 4: Yes, all three requirements are fulfilled.**

Note

*In subnetting,
we need the first address of the
subnet and the subnet mask to
define the range of addresses.*

Note

**In supernetting,
we need the first address of
the supernet
and the supernet mask to
define the range of addresses.**

Comparison of subnet, default, and supernet masks

Subnet Mask

Divide 1 network into 8 subnets

1 1 1 1 1 1 1 1	1 1 1 1 1 1 1 1	1 1 1 1 1 1 1 1	1 1 1	0 0 0 0 0
-----------------	-----------------	-----------------	-------	-----------

↑
Subnetting

3 more
1s →

Default Mask

1 1 1 1 1 1 1 1	1 1 1 1 1 1 1 1	1 1 1 1 1 1 1 1	0 0 0 0 0 0 0 0
-----------------	-----------------	-----------------	-----------------

↓
Supernetting

3 less
1s ←

Supernet Mask

1 1 1 1 1 1 1 1	1 1 1 1 1 1 1 1	1 1 1 1 1	0 0 0 0 0 0 0 0
-----------------	-----------------	-----------	-----------------

Combine 8 networks into 1 supernet

Example 13

We need to make a supernet out of 16 class C blocks.

What is the supernet mask?

Solution

We need 16 blocks. For 16 blocks we need to change four 1s to 0s in the default mask. So the mask is

11111111 11111111 1111**0000** 00000000
or

255.255.240.0

Example 14

A supernet has a first address of 205.16.32.0 and a supernet mask of 255.255.248.0. A router receives three packets with the following destination addresses:

205.16.37.44

205.16.42.56

205.17.33.76

Which packet belongs to the supernet?

Solution

We apply the supernet mask to see if we can find the beginning address.

205.16.37.44 AND 255.255.248.0 → 205.16.32.0

205.16.42.56 AND 255.255.248.0 → 205.16.40.0

205.17.33.76 AND 255.255.248.0 → 205.17.32.0

Only the first address belongs to this supernet.

Example 15

A supernet has a first address of 205.16.32.0 and a supernet mask of 255.255.248.0.

How many blocks are in this supernet and what is the range of addresses?

Solution

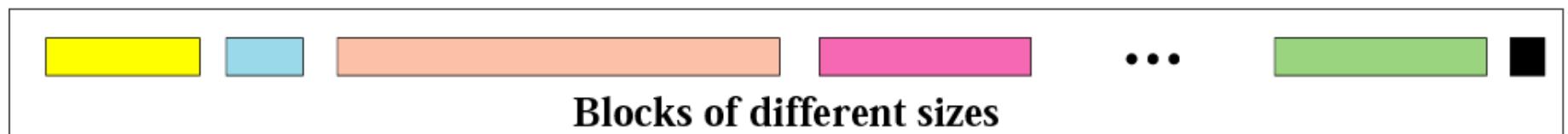
The supernet has 21 1s. The default mask has 24 1s. Since the difference is 3, there are 2^3 or 8 blocks in this supernet.

The blocks are 205.16.32.0 to 205.16.39.0. The first address is 205.16.32.0. The last address is 205.16.39.255.

CLASSLESS ADDRESSING

Variable-length blocks

Address Space



Number of Addresses in a Block

There is only one condition on the number of addresses in a block; it must be a power of 2 (2, 4, 8, . . .). A household may be given a block of 2 addresses. A small business may be given 16 addresses. A large organization may be given 1024 addresses.

Beginning Address

The beginning address must be evenly divisible by the number of addresses. For example, if a block contains 4 addresses, the beginning address must be divisible by 4. If the block has less than 256 addresses, we need to check only the rightmost byte. If it has less than 65,536 addresses, we need to check only the two rightmost bytes, and so on.

Example 16

Which of the following can be the beginning address of a block that contains 1024 addresses?

205.16.37.32

190.16.42.0

17.17.32.0

123.45.24.52

Solution

To be divisible by 1024, the rightmost byte of an address should be 0 and the second rightmost byte must be divisible by 4.

Only the address 17.17.32.0 meets this condition.

Slash notation

A.B.C.D/*n*

Note

*Slash notation is also called
CIDR
notation.*

Example 17

A small organization is given a block with the beginning address and the prefix length **205.16.37.24/29** (in slash notation).

What is the range of the block?

Solution

- The beginning address is 205.16.37.24. To find the last address we keep the first 29 bits and change the last 3 bits to 1s.
- Beginning: 11001111 00010000 00100101 00011000
- Ending : 11001111 00010000 00100101 00011111
- There are only 8 addresses in this block.

Example 17 cont'd

We can find the range of addresses in Example 17 by another method.

We can argue that the length of the suffix is $32 - 29$ or 3. So there are $2^3 = 8$ addresses in this block.

If the first address is 205.16.37.24, the last address is 205.16.37.31 ($24 + 7 = 31$).

Note

A block in classes A, B, and C can easily be represented in slash notation as **A.B.C.D/ *n*** where *n* is either 8 (class A), 16 (class B), or 24 (class C).

Example 18

What is the network address if one of the addresses is 167.199.170.82/27?

Solution

- The prefix length is 27, which means that we must keep the first 27 bits as is and change the remaining bits (5) to 0s.
- The 5 bits affect only the last byte.
- The last byte is 01010010. Changing the last 5 bits to 0s, we get 01000000 or 64.
- The network address is 167.199.170.64/27.

Example 19

An organization is granted the block 130.34.12.64/26. The organization needs to have four subnets. What are the subnet addresses and the range of addresses for each subnet?

Solution

- The suffix length is 6.
- This means the total number of addresses in the block is 64 (2⁶).
- If we create four subnets, each subnet will have 16 addresses.

Solution (Continued)

Let us first find the subnet prefix (subnet mask). We need four subnets, which means we need to add two more 1s to the site prefix. The subnet prefix is then /28.

Subnet 1: 130.34.12.64/28 to 130.34.12.79/28.

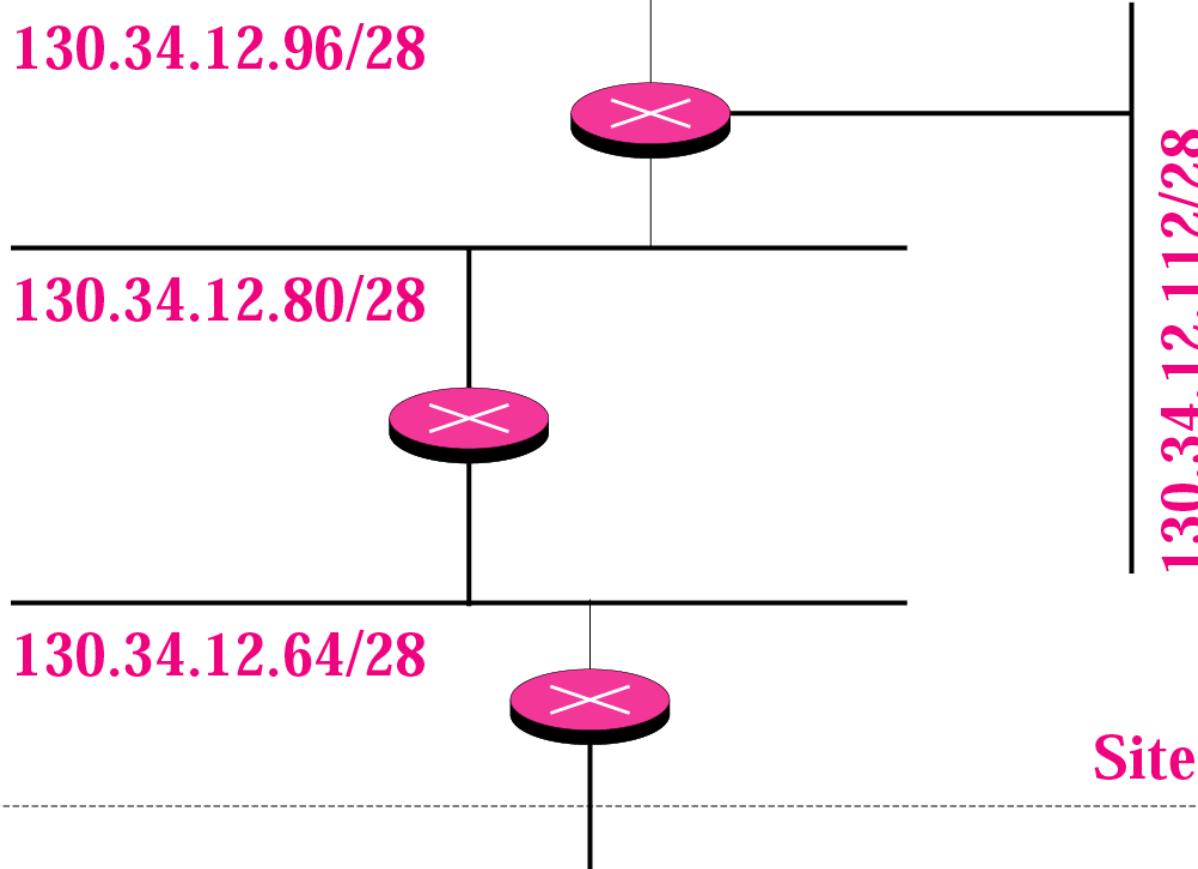
Subnet 2 : 130.34.12.80/28 to 130.34.12.95/28.

Subnet 3: 130.34.12.96/28 to 130.34.12.111/28.

Subnet 4: 130.34.12.112/28 to 130.34.12.127/28.

See next Fig.

Example 19 cont'd



To and from the
rest of the Internet

Example 20

An ISP is granted a block of addresses starting with 190.100.0.0/16. The ISP needs to distribute these addresses to three groups of customers as follows:

1. The first group has 64 customers; each needs 256 addresses.
2. The second group has 128 customers; each needs 128 addresses.
3. The third group has 128 customers; each needs 64 addresses.

Design the subblocks and give the slash notation for each subblock. Find out how many addresses are still available after these allocations.

Solution

Group 1

For this group, each customer needs 256 addresses. This means the suffix length is 8 ($2^8 = 256$). The prefix length is then $32 - 8 = 24$.

01: 190.100.0.0/24 **→** 190.100.0.255/24

02: 190.100.1.0/24 **→** 190.100.1.255/24

.....

64: 190.100.63.0/24 **→** 190.100.63.255/24

Total = $64 \times 256 = 16,384$

Solution (Continued)

Group 2

For this group, each customer needs 128 addresses. This means the suffix length is 7 ($2^7 = 128$). The prefix length is then $32 - 7 = 25$. The addresses are:

001: 190.100.64.0/25 \rightarrow 190.100.64.127/25

002: 190.100.64.128/25 \rightarrow 190.100.64.255/25

.....

128: 190.100.127.128/25 \rightarrow 190.100.127.255/25

Total = $128 \times 128 = 16,384$

Solution (Continued)

Group 3

For this group, each customer needs 64 addresses. This means the suffix length is 6 ($2^6 = 64$). The prefix length is then $32 - 6 = 26$.

001:190.100.128.0/26 →190.100.128.63/26

002:190.100.128.64/26 →190.100.128.127/26

.....

128:190.100.159.192/26 →190.100.159.255/26

Total = $128 \times 64 = 8,192$

Solution (Continued)

Number of granted addresses: 65,536

Number of allocated addresses: 40,960

Number of available addresses: 24,576

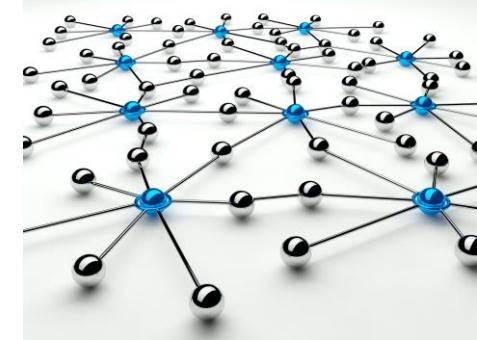
Networks Architectures and Protocols

7. ROUTING PROTOCOLS

Lecturer: Zoltán Gál, PhD

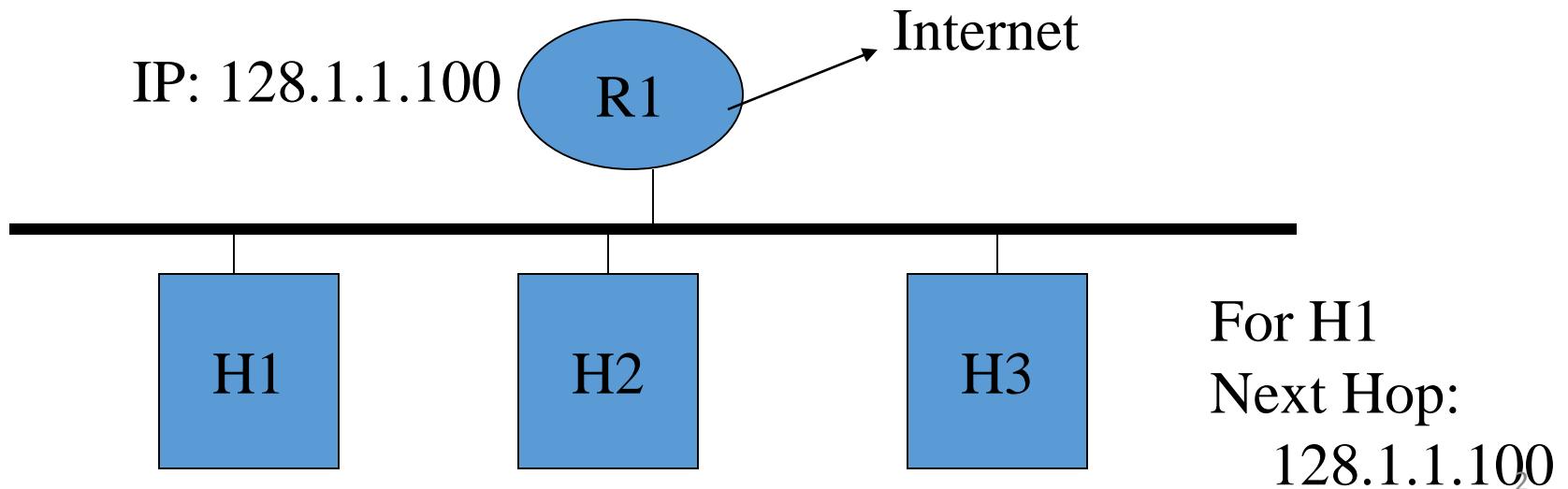
Faculty of Informatics, University of Debrecen

February 05, 2018



Static Routing

- Typically used in hosts
 - Enter subnet mask, router (gateway), IP address
 - Perfect for cases with few connections, doesn't change much
 - E.g. host with a single router connecting to the rest of the Internet



Dynamic Routing

- Most routers use dynamic routing
 - Automatically build the routing tables
 - As we saw previously, there are two major approaches
 - Link State Algorithms
 - Distance Vector Algorithms
- First some terminology
- AS = Autonomous System
 - Contiguous set of networks under one administrative authority
 - Common routing protocol
 - E.g. University of Alaska Statewide, Washington State University
 - E.g. Intel Corporation
 - A connected network
 - There is at least one route between any pair of nodes

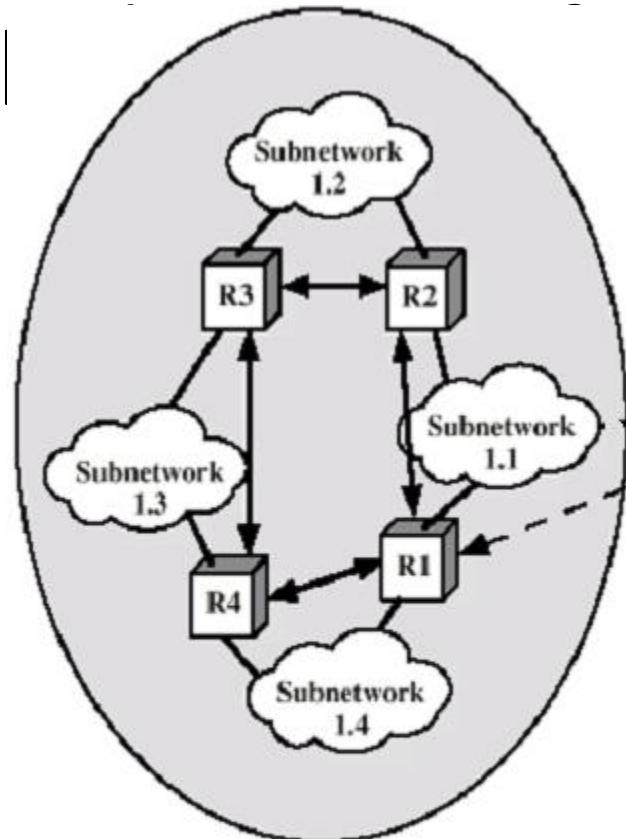
Routing in an AS

- IRP = Interior Routing Protocol
 - Also IGP ; Interior Gateway Protocol
 - Passes routing information between routers within AS
 - Can use routing metric, e.g. hop count or administrative cost
 - E.g. two paths from accounting to payroll, a 2 hop path for customers, and a 3 hop path for internal corporate
 - Shortest path violates corporate policy for internal employees, so administrator can override the actual cost to 4 hops
 - Customers still get the 2 hop path so they pick this route

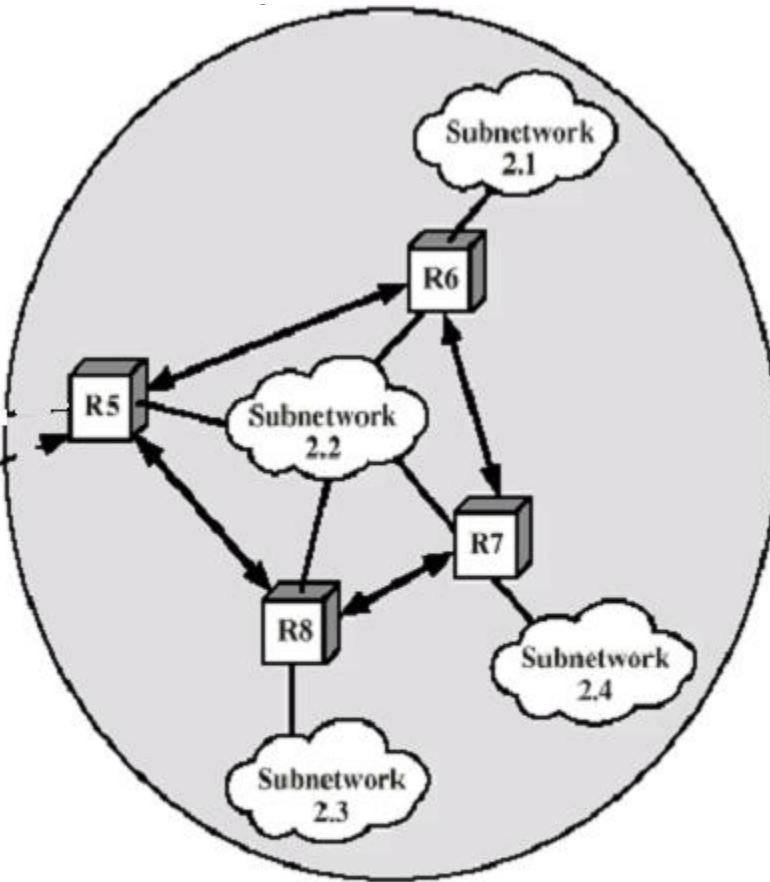
Routing in an AS

- ERP = Exterior Routing Protocol
 - Also EGP; Exterior Gateway Protocol
 - Passes routing information between routers across AS
 - May be more than one AS in internet
 - Routing algorithms and tables may differ between different AS
 - Finds a path, but can't find an optimal path since it can't compare routing metrics via multiple AS

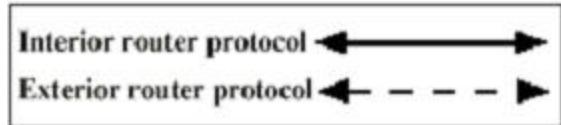
A



Autonomous System 1



Autonomous System 2



Hierarchical Routing

Our routing study thus far - idealization

- all routers identical
- network “flat”
- ... *not* true in practice

scale: with 50 million destinations:

- can't store all dest's in routing tables!
- routing table exchange would swamp links!

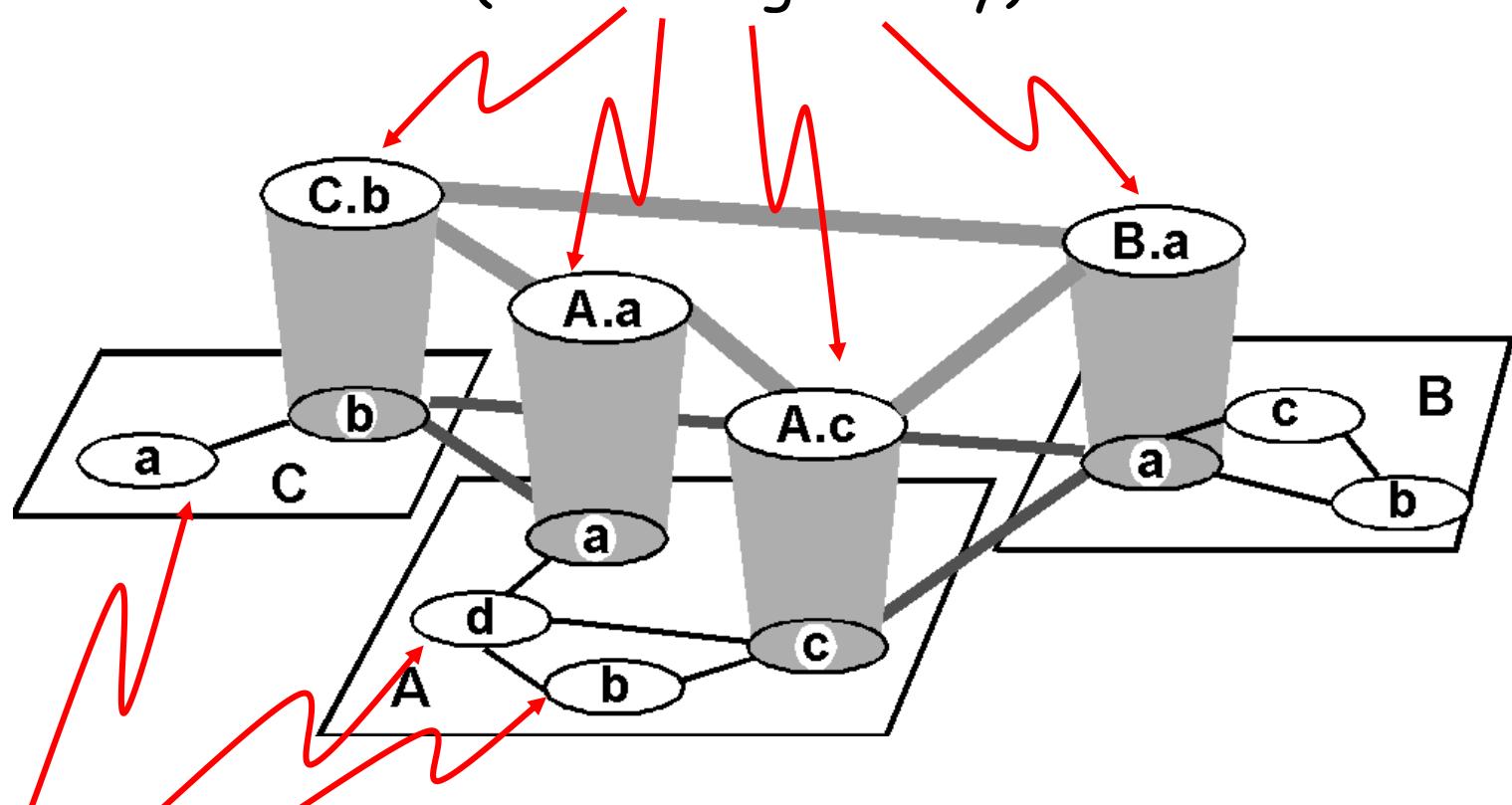
administrative autonomy

- internet = network of networks
- each network admin may want to control routing in its own network

Internet consists of Autonomous Systems interconnected with each other!

Internet AS Hierarchy

Inter-AS border (exterior gateway) routers



Intra-AS interior (gateway) routers

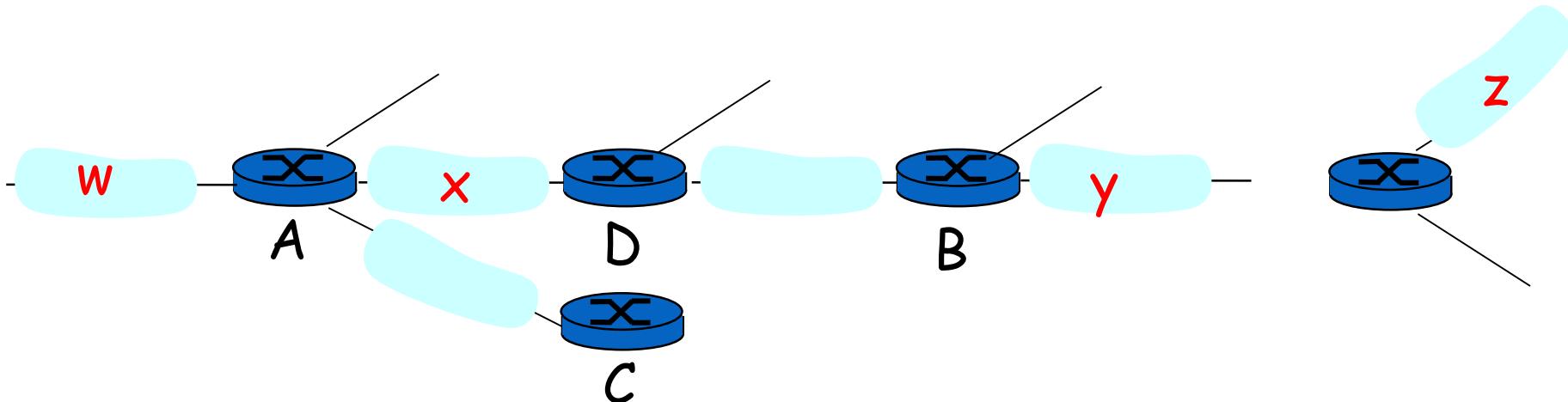
Intra-AS Routing

- Also known as Interior Router Protocols (IRP) or Interior Gateway Protocols (IGP)
- Most common:
 - RIP: Routing Information Protocol
 - OSPF: Open Shortest Path First
 - IGRP: Interior Gateway Routing Protocol (Cisco proprietary)

RIP (Routing Information Protocol)

- Distance vector algorithm
- Included in BSD-UNIX Distribution in 1982
 - routed
- Distance metric: # of hops (max = 15 hops)
 - *Can you guess why?*
- Distance vectors: exchanged every 30 sec via Response Message (also called **advertisement**)
- Each advertisement: route to up to 25 destination nets

RIP (Routing Information Protocol)



Destination Network	Next Router	Num. of hops to dest.
W	A	2
Y	B	2
Z	B	7
X	--	1
....

Routing table in D

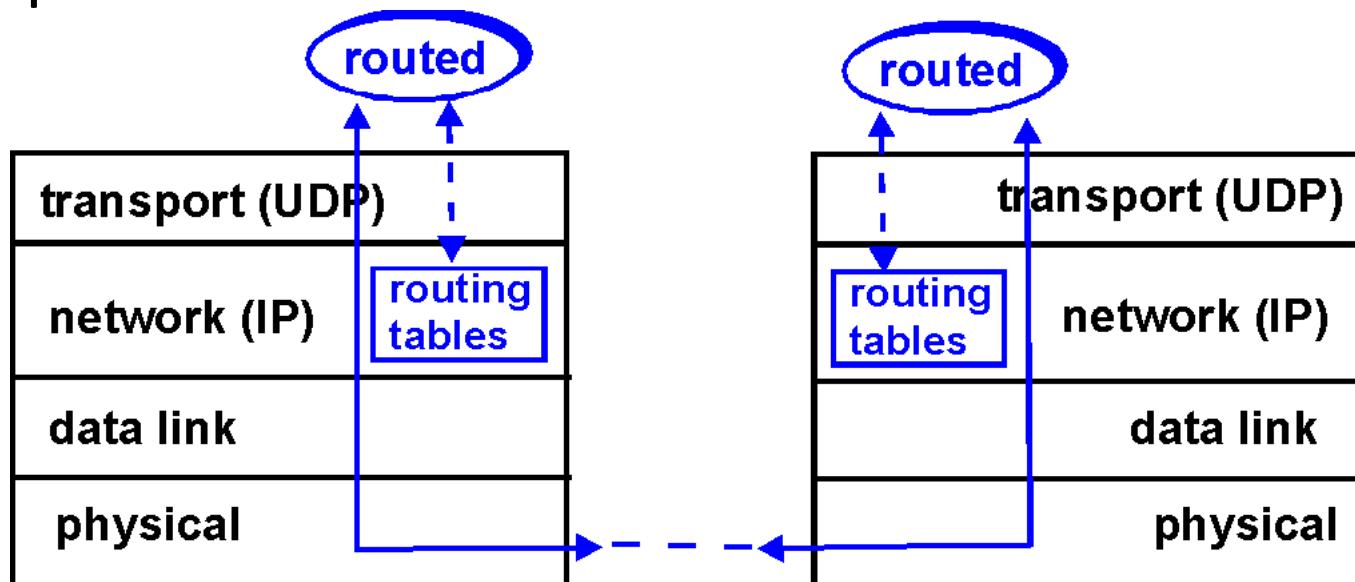
RIP: Link Failure and Recovery

If no advertisement heard after 180 sec → neighbor/link declared dead

- routes via neighbor invalidated
- new advertisements sent to neighbors
- neighbors in turn send out new advertisements (if tables changed)
- link failure info quickly propagates to entire net

RIP Table processing

- RIP routing tables managed by **application-level** process called route-d (daemon)
- advertisements sent in UDP packets, periodically repeated



RIP Table example (continued)

Router: *giroflee.eurocom.fr* via: netstat -rn

Destination	Gateway	Flags	Ref	Use	Interface
127.0.0.1	127.0.0.1	UH	0	26492	lo0
192.168.2.	192.168.2.5	U	2	13	fa0
193.55.114.	193.55.114.6	U	3	58503	1e0
192.168.3.	192.168.3.5	U	2	25	qaa0
224.0.0.0	193.55.114.6	U	3	0	1e0
default	193.55.114.129	UG	0	143454	

- Three attached class C networks (LANs)
- Router only knows routes to attached LANs
- Default router used to “go up”
- Route multicast address: 224.0.0.0
- Loopback interface (for debugging)

RIP

- Advantages

- Simplicity ; little to no configuration, just start routed up
- Passive version for hosts
 - If a host wants to just listen and update its routing table

- Packet Format

- This is in the payload of a UDP packet

0	8	16	24	31
Command(1-5)	Version(2)	Must be Zero		
Family of Net 1		Route Tag for Net 1		
IP Address of Net 1				
Subnet Mask for Net 1				
Next Hop for Net 1				
Distance to Net 1				
Family of Net 2		Route Tag for Net 2		
IP Address of Net 2				
...				

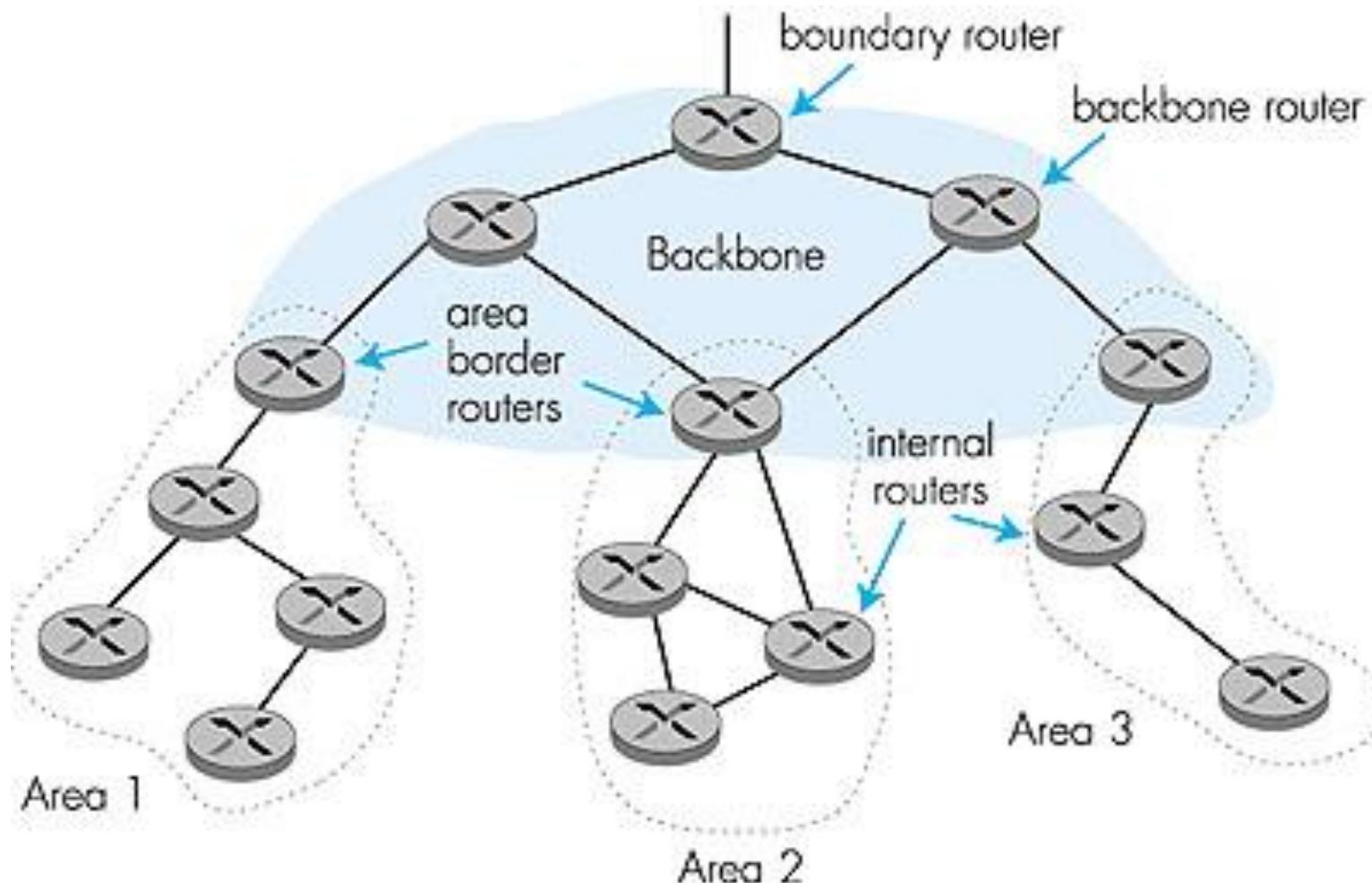
OSPF (Open Shortest Path First)

- “Open”: publicly available
 - RFC 2328
- Uses Link State algorithm
 - LS packet dissemination
 - Topology map at each node
 - Route computation using Dijkstra’s algorithm
- OSPF advertisement carries one entry per neighbor router
- Advertisements disseminated to **entire** AS (via flooding)
- Conceived as a successor to RIP

OSPF “advanced” features (not in RIP)

- Security: all OSPF messages authenticated (to prevent malicious intrusion); TCP connections used
- Multiple same-cost paths allowed (only one path in RIP)
- For each link, multiple cost metrics for different Type Of Service (e.g., satellite link cost set “low” for best effort; high for real time)
- Integrated uni- and multicast support:
 - Multicast OSPF (MOSPF) uses same topology data base as OSPF
- Hierarchical OSPF in large domains.

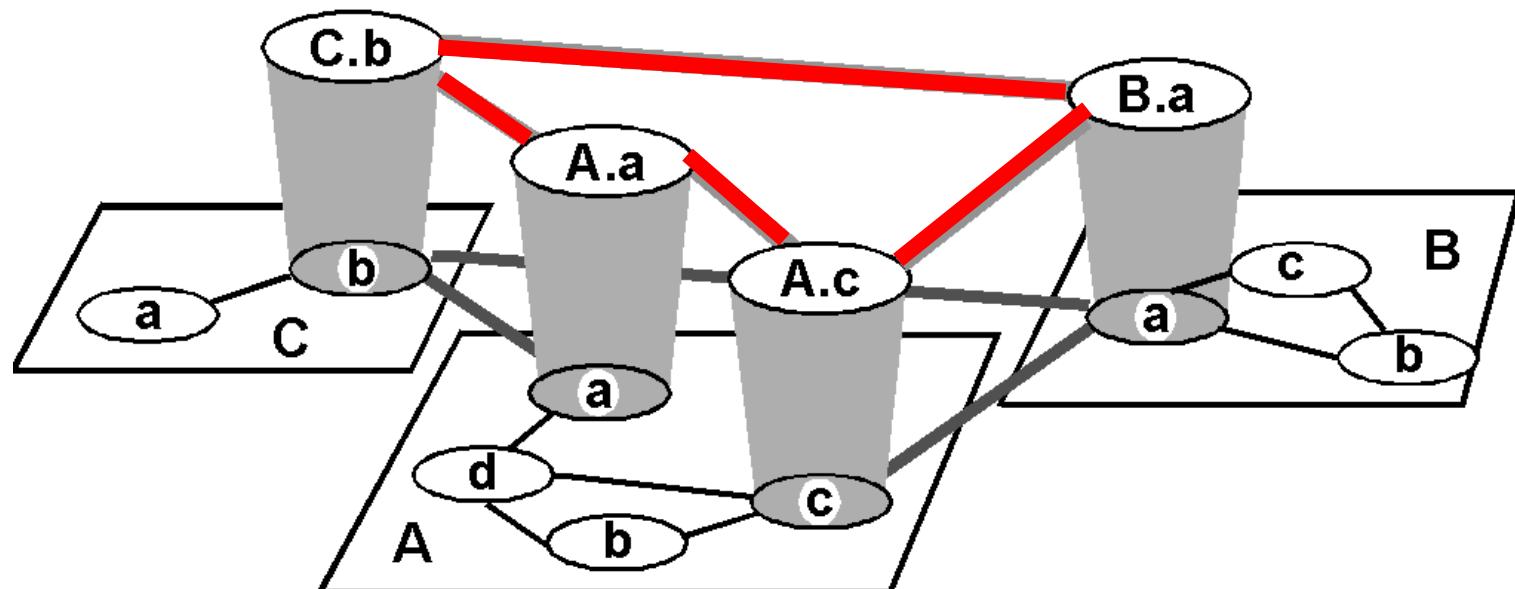
Hierarchical OSPF



IGRP (Interior Gateway Routing Protocol)

- CISCO proprietary; successor of RIP (mid 80s)
- Distance Vector, like RIP
- Several cost metrics (delay, bandwidth, reliability, load etc)
- Uses TCP to exchange routing updates
- Loop-free routing via Distributed Updating Alg. (DUAL) based on *diffused computation*

Inter-AS routing / Exterior Route Protocols



Internet inter-AS/ERP routing: BGP

- BGP (Border Gateway Protocol): *the de facto standard*
 - Version 4 the current standard
- **Path Vector** protocol:
 - similar to Distance Vector protocol
 - each Border Gateway broadcast to neighbors (peers) *entire path* (i.e, sequence of ASs) to destination
 - E.g., Gateway X may send its path to dest. Z:

Path (X,Z) = X,Y₁,Y₂,Y₃,...,Z

Internet inter-AS routing: BGP

Suppose: router X send its path to peer router W

- W may or may not select path offered by X
 - cost, policy (don't route via competitors AS), loop prevention reasons, many other metrics
- E.g. X advertises path to Z: $XY_1Y_2Y_3Z$
 - If W selects path advertised by X, then:
$$\text{Path (W,Z)} = WXY_1Y_2Y_3Z$$
- Note: X can control incoming traffic by controlling its route advertisements to peers:
 - e.g., don't want to route traffic to Z -> don't advertise any routes to Z

Internet inter-AS routing: BGP

- BGP messages exchanged using TCP.
- BGP messages:
 - OPEN: opens TCP connection to peer and authenticates sender
 - UPDATE: advertises new path (or withdraws old)
 - KEEPALIVE keeps connection alive in absence of UPDATES; also ACKs OPEN request
 - NOTIFICATION: reports errors in previous msg; also used to close connection

Why different Interior/Exterior routing ?

Policy:

- Inter-AS / Exterior: admin wants control over how its traffic routed, who routes through its net.
- Intra-AS / Interior: single admin, so no policy decisions needed

Scale:

- hierarchical routing saves table size, reduced update traffic, hierarchical scheme allows different interior routing protocols

Performance:

- Intra-AS / Interior: can focus on performance, customization
- Inter-AS / Exterior: policy may dominate over performance

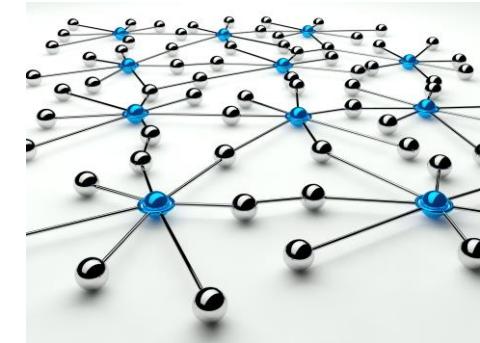
Networks Architectures and Protocols

8. NETWORK LAYER PROTOCOLS: IPv4 & IPv6

Lecturer: Zoltán Gál, PhD

Faculty of Informatics, University of Debrecen

February 05, 2018



Outline

- IPv4 Protocol Mechanism
- IPv6 Addressing and Protocol Mechanism

Internet Protocol

- Provides best effort, connectionless packet delivery
 - motivated by need to keep routers simple and by adaptability to failure of network elements
 - packets may be lost, out of order, or even duplicated
 - higher layer protocols must deal with these, if necessary
- RFCs 791, 950, 919, 922, and 2474.
- IP is part of Internet STD number 5, which also includes:
 - Internet Control Message Protocol (ICMP), RFC 792
 - Internet Group Management Protocol (IGMP), RFC 1112

IPv4 Protocol

IPv4 Packet Header

0	4	8	16	19	24	31					
Version	IHL	Type of Service	Total Length								
Identification			Flags	Fragment Offset							
Time to Live	Protocol		Header Checksum								
Source IP Address											
Destination IP Address											
Options					Padding						

- Minimum 20 bytes
- Up to 40 bytes in options fields

IPv4 Packet Header

0	4	8	16	19	24	31					
Version	IHL	Type of Service	Total Length								
Identification			Flags	Fragment Offset							
Time to Live	Protocol		Header Checksum								
Source IP Address											
Destination IP Address											
Options				Padding							

Version: current IP version is 4.

Internet header length (IHL): length of the header in 32-bit words.

Type of service (TOS): traditionally priority of packet at each router. Recent Differentiated Services redefines TOS field to include other services besides best effort.

IPv4 Packet Header

0	4	8	16	19	24	31					
Version	IHL	Type of Service	Total Length								
Identification			Flags	Fragment Offset							
Time to Live	Protocol		Header Checksum								
Source IP Address											
Destination IP Address											
Options					Padding						

Total length: number of bytes of the IP packet including header and data, maximum length is 65535 bytes.

Identification, Flags, and Fragment Offset: used for fragmentation and reassembly (More on this shortly).

IPv4 Packet Header

0	4	8	16	19	24	31									
Version	IHL	Type of Service	Total Length												
Identification			Flags	Fragment Offset											
Time to Live	Protocol		Header Checksum												
Source IP Address															
Destination IP Address															
Options					Padding										

Time to live (TTL): number of hops packet is allowed to traverse in the network.

- Each router along the path to the destination decrements this value by one.
- If the value reaches zero before the packet reaches the destination, the router discards the packet and sends an error message back to the source.

IPv4 Packet Header

0		4		8		16		19		24		31											
Version	IHL	Type of Service	Total Length																				
Identification				Flags	Fragment Offset																		
Time to Live	Protocol		Header Checksum																				
Source IP Address																							
Destination IP Address																							
Options							Padding																

Protocol: specifies upper-layer protocol that is to receive IP data at the destination. Examples include TCP (protocol = 6), UDP (protocol = 17), and ICMP (protocol = 1).

Header checksum: verifies the integrity of the IP header.

Source IP address and **destination IP address:** contain the addresses of the source and destination hosts.

IPv4 Packet Header

0	4	8	16	19	24	31					
Version	IHL	Type of Service	Total Length								
Identification			Flags	Fragment Offset							
Time to Live	Protocol		Header Checksum								
Source IP Address											
Destination IP Address											
Options					Padding						

Options: Variable length field, allows packet to request special features such as security level, route to be taken by the packet, and timestamp at each router. Detailed descriptions of these options can be found in [RFC 791].

Padding: This field is used to make the header a multiple of 32-bit words.

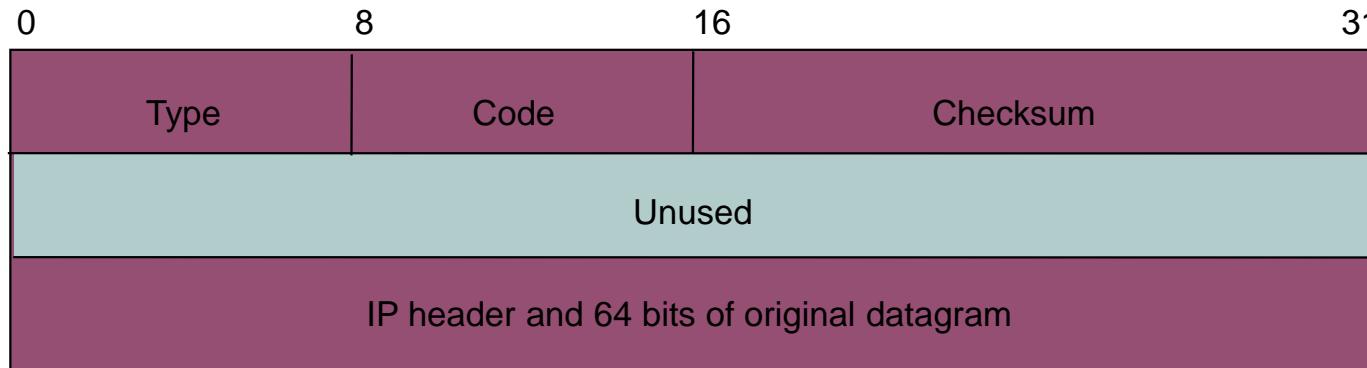
IPv4 Header Checksum

- IP header uses check bits to detect errors in the *header*
- A checksum is calculated for header contents
- Checksum recalculated at every router, so algorithm selected for ease of implementation in software
- Let header consist of L, 16-bit words,
 $\mathbf{b}_0, \mathbf{b}_1, \mathbf{b}_2, \dots, \mathbf{b}_{L-1}$
- The algorithm appends a 16-bit *checksum* \mathbf{b}_L

IPv4 Header Processing

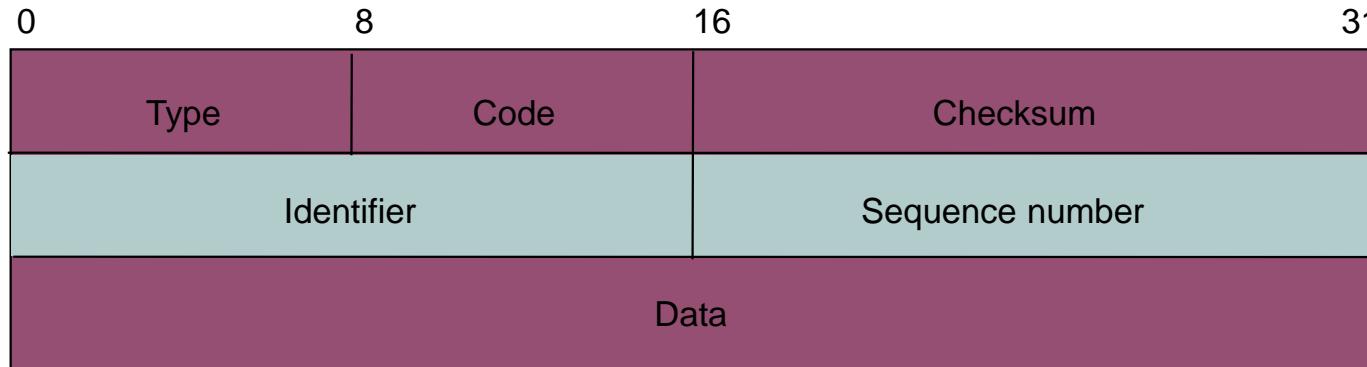
1. Compute header checksum for correctness and check that fields in header (e.g. version and total length) contain valid values
2. Consult routing table to determine next hop
3. Change fields that require updating (TTL, header checksum)

ICMP Basic Error Message Format



- *Type* of message: some examples
 - 0 Network Unreachable; 3 Port Unreachable
 - 1 Host Unreachable
 - 2 Protocol Unreachable
 - 11 Time-exceeded, code=0 if TTL exceeded
- Code: purpose of message
- IP header & 64 bits of original datagram
 - To match ICMP message with original data in IP packet

Echo Request & Echo Reply Message Format



- Echo request: type=8; Echo reply: type=0
 - Destination replies with echo reply by copying data in request onto reply message
- Sequence number to match reply to request
- ID to distinguish between different sessions using echo services
- Used in PING

Example – Echo request

Screenshot of the Ethereal network traffic analyzer showing captured frames related to an echo request.

File Edit Capture Display Tools Help

No.	Time	Source	Destination	Protocol	Info
1	0.000000	00000000.0001031dccf7	Broadcast	IPX SAP	Nearest Query
2	13.526454	192.168.2.18	192.168.2.1	DNS	Standard query A tesla.comm.utoronto.ca
3	13.534545	192.168.2.1	192.168.2.18	DNS	Standard query response A 128.100.11.1
4	13.541026	192.168.2.18	128.100.11.1	ICMP	Echo (ping) request
5	13.555913	128.100.11.1	192.168.2.18	ICMP	Echo (ping) reply
6	14.542842	192.168.2.18	128.100.11.1	ICMP	Echo (ping) request
7	14.567211	128.100.11.1	192.168.2.18	ICMP	Echo (ping) reply
8	15.547669	192.168.2.18	128.100.11.1	ICMP	Echo (ping) request
9	15.586209	128.100.11.1	192.168.2.18	ICMP	Echo (ping) reply
10	16.552528	192.168.2.18	128.100.11.1	ICMP	Echo (ping) request
11	16.565526	128.100.11.1	192.168.2.18	ICMP	Echo (ping) reply
12	22.941534	192.168.2.18	192.168.2.255	BROWSER	Domain/workgroup Announcement @HOME, windows for wor

Frame 4 (74 bytes on wire, 74 bytes captured)

Ethernet II, Src: 00:01:03:1d:cc:f7, Dst: 00:04:e2:29:b2:3a

Internet Protocol, Src Addr: 192.168.2.18 (192.168.2.18), Dst Addr: 128.100.11.1 (128.100.11.1)

Internet Control Message Protocol

Type: 8 (Echo (ping) request)
Code: 0
Checksum: 0xf05b (correct)
Identifier: 0x0200
Sequence number: 5b:00
Data (32 bytes):
.....
0000 00 04 e2 29 b2 3a 00 01 03 1d cc f7 08 00 45 00 ...).:.E.
0010 00 3c 19 8a 00 00 20 01 33 18 c0 a8 02 12 80 64 .<.... 3.....d
0020 0b 01 08 00 f0 5b 02 00 5b 00 61 62 63 64 65 66[. [.. abcdef
0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 ghijklmn opqrstuv
0040 77 61 62 63 64 65 66 67 68 69 wabcdeFG hi

Filter: / Reset Apply File: pingtesla

15

Example – Echo Reply

pingtesla - Ethereal

File Edit Capture Display Tools Help

No.	Time	Source	Destination	Protocol	Info
1	0.000000	00000000.0001031dccf7	00000000.Broadcast	IPX SAP	Nearest Query
2	13.526454	192.168.2.18	192.168.2.1	DNS	Standard query A tesla.comm.utoronto.ca
3	13.534545	192.168.2.1	192.168.2.18	DNS	Standard query response A 128.100.11.1
4	13.541026	192.168.2.18	128.100.11.1	ICMP	Echo (ping) request
5	13.555913	128.100.11.1	192.168.2.18	ICMP	Echo (ping) reply
6	14.542842	192.168.2.18	128.100.11.1	ICMP	Echo (ping) request
7	14.567211	128.100.11.1	192.168.2.18	ICMP	Echo (ping) reply
8	15.547669	192.168.2.18	128.100.11.1	ICMP	Echo (ping) request
9	15.586209	128.100.11.1	192.168.2.18	ICMP	Echo (ping) reply
10	16.552528	192.168.2.18	128.100.11.1	ICMP	Echo (ping) request
11	16.565526	128.100.11.1	192.168.2.18	ICMP	Echo (ping) reply

Frame 5 (74 bytes on wire, 74 bytes captured)
Ethernet II, Src: 00:04:e2:29:b2:3a, Dst: 00:01:03:1d:cc:f7
Internet Protocol, src Addr: 128.100.11.1 (128.100.11.1), Dst Addr: 192.168.2.18 (192.168.2.18)
Internet Control Message Protocol
Type: 0 (Echo (ping) reply)
Code: 0
Checksum: 0xf85b (correct)
Identifier: 0x0200
Sequence number: 5b:00
Data (32 bytes)

0000	00	01	03	1d	cc	f7	00	04	e2	29	b2	3a	08	00	45	00).	..E.
0010	00	3c	99	88	00	00	f0	01	e3	18	80	64	0b	01	c0	a8	.<.....d....	
0020	02	12	00	00	f8	5b	02	00	5b	00	61	62	63	64	65	66[..	[.abcdef	
0030	67	68	69	6a	6b	6c	6d	6e	6f	70	71	72	73	74	75	76	ghijklmn	opqrstuvwxyz	
0040	77	61	62	63	64	65	66	67	68	69							wabcdefghijklm	hi	

Filter: File: pingtesla

IPv6 Protocol

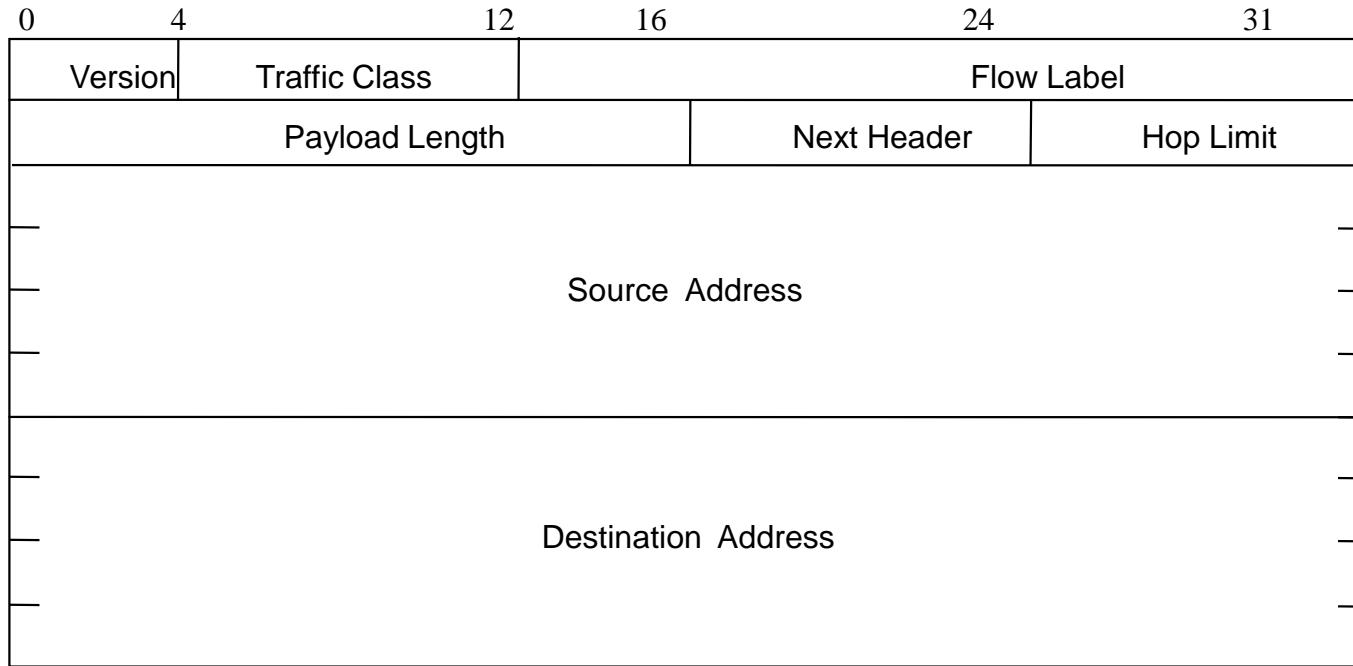
IPv6

- **Longer address field:**
 - 128 bits can support up to 3.4×10^{38} hosts
- **Simplified header format:**
 - Simpler format to speed up processing of each header
 - All fields are of fixed size
 - IPv4 vs IPv6 fields:
 - Same: Version
 - Dropped: Header length, ID/flags/frag offset, header checksum
 - Replaced:
 - Datagram length by Payload length
 - Protocol type by Next header
 - TTL by Hop limit
 - TOS by traffic class
 - New: Flow label

Other IPv6 Features

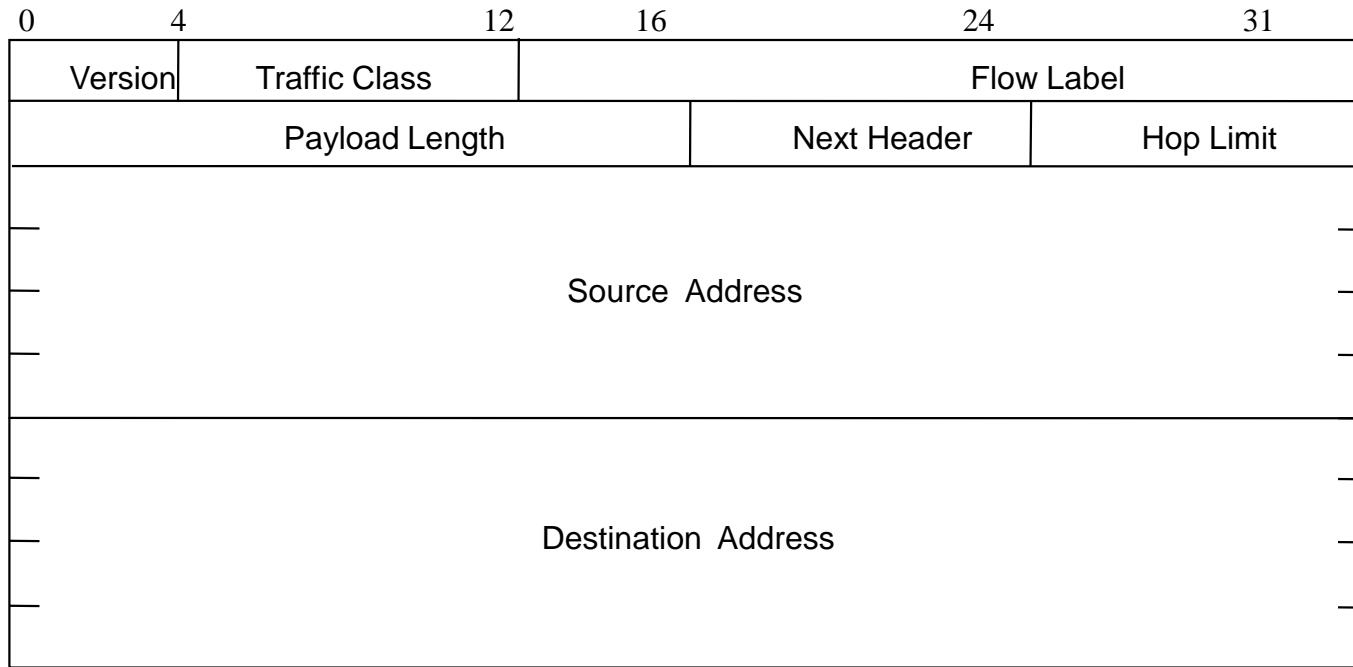
- **Flexible support for options:** more efficient and flexible options encoded in optional *extension headers*
- **Flow label capability:** “flow label” to identify a packet flow that requires a certain QoS
- **Security:** built-in authentication and confidentiality
- **Large packets:** supports payloads that are longer than 64 K bytes, called *jumbo* payloads.
- **Fragmentation at source only:** source should check the minimum MTU along the path
- **No checksum field:** removed to reduce packet processing time in a router

IPv6 Packet Header Format



- Version field same size, same location
- Traffic class to support differentiated services
- Flow: sequence of packets from particular source to particular destination for which source requires special handling

IPv6 Packet Header Format



- Payload length: length of data excluding header, up to 65535 B
- Next header: type of extension header that follows basic header
- Hop limit: # hops packet can travel before being dropped by a router

IPv6 Addressing

- Address Categories
 - Unicast: single network interface
 - Multicast: group of network interfaces, typically at different locations. Packet sent to all.
 - Anycast: group of network interfaces. Packet sent to only one interface in group, e.g. nearest.
- Hexadecimal notation
 - Groups of 16 bits represented by 4 hex digits
 - Separated by colons
 - 4BF5:AA12:0216:FEBC:BA5F:039A:BE9A:2176
 - Shortened forms:
 - 4BF5:0000:0000:0000:BA5F:039A:000A:2176
 - To 4BF5:0:0:0:BA5F:39A:A:2176
 - To 4BF5::BA5F:39A:A:2176
 - Mixed notation:
 - ::FFFF:128.155.12.198

Example

v6.pcap - Ethereal

File Edit Capture Display Tools Help

No.	Time	Source	Destination	Protocol	Info
1	0.000000	3ffe:507:0:1:200:86ff	3ffe:501:4819::42	DNS	Standard query ANY itojun.org
2	0.073515	3ffe:501:4819::42	3ffe:507:0:1:200:86ff	DNS	Standard query response NS coconut.itojun.
3	5.352508	fe80::200:86ff:fe05:8	fe80::260:97ff:fe07:6	ICMPv6	Neighbor solicitation
4	5.352839	fe80::260:97ff:fe07:6	fe80::200:86ff:fe05:8	ICMPv6	Neighbor advertisement
5	5.478595	3ffe:507:0:1:260:97ff	3ffe:507:0:1:200:86ff	ICMPv6	Neighbor solicitation
6	5.479045	3ffe:507:0:1:200:86ff	3ffe:507:0:1:260:97ff	ICMPv6	Neighbor advertisement
7	6.617560	3ffe:507:0:1:200:86ff	3ffe:501:4819::42	DNS	Standard query MX www.yahoo.com
8	6.752573	3ffe:501:4819::42	3ffe:507:0:1:200:86ff	DNS	Standard query response MX 0 mr1.yahoo.com
9	10.364948	3ffe:507:0:1:200:86ff	3ffe:507:0:1:260:97ff	ICMPv6	Neighbor solicitation
10	10.365231	3ffe:507:0:1:260:97ff	3ffe:507:0:1:200:86ff	ICMPv6	Neighbor advertisement
11	10.490052	fe80::260:97ff:fe07:6	fe80::200:86ff:fe05:8	ICMPv6	Neighbor solicitation
12	10.490554	fe80::200:86ff:fe05:8	fe80::260:97ff:fe07:6	ICMPv6	Neighbor advertisement
13	12.297384	fe80::260:97ff:fe07:6	ff02::9	RIPng version 1 Response	
14	16.109457	3ffe:507:0:1:200:86ff	3ffe:501:4819::42	DNS	Standard query AAAA kiwi.itojun.org
15	16.121831	3ffe:501:4819::42	3ffe:507:0:1:200:86ff	DNS	Standard query response AAAA 3ffe:501:410:
16	16.124364	3ffe:507:0:1:200:86ff	3ffe:501:410:0:200:df	TCP	1022 ~ 22 [SYN] seq=2598119713 ack=0 win=8

Frame 7 (93 on wire, 93 captured)

Ethernet II

Internet Protocol version 6

- Version: 6
- Traffic class: 0x00
- Flowlabel: 0x00000
- Payload length: 39
- Next header: UDP (0x11)
- Hop limit: 64
- Source address: 3ffe:507:0:1:200:86ff:fe05:80da
- Destination address: 3ffe:501:4819::42

User Datagram Protocol, Src Port: 2397 (2397), Dst Port: domain (53)

Domain Name System (query)

0000 00 60 97 07 69 ea 00 00 86 05 80 da 86 dd 60 00 . . . i
0010 00 00 00 27 11 40 3f fe 05 07 00 00 00 01 02 00 @?
0020 86 ff fe 05 80 da 3f fe 05 01 48 19 00 00 00 00 ? . . H . . .
0030 00 00 00 00 00 42 09 5d 00 35 00 27 46 b7 00 06 B .] 5 . F . .
0040 01 00 00 01 00 00 00 00 00 00 03 77 77 77 05 79 www.y

Filter: File: v6.pcap

23

IPv6 Address Types based on Prefixes

Binary prefix	Types	Percentage of address space
0000 0000	Reserved	0.39
0000 0001	Unassigned	0.39
0000 001	ISO network addresses	0.78
0000 010	IPX network addresses	0.78
0000 011	Unassigned	0.78
0000 1	Unassigned	3.12
0001	Unassigned	6.25
001	Unassigned	12.5
010	Provider-based unicast addresses	12.5
011	Unassigned	12.5
100	Geographic-based unicast addresses	12.5
101	Unassigned	12.5
110	Unassigned	12.5
1110	Unassigned	6.25
1111 0	Unassigned	3.12
1111 10	Unassigned	1.56
1111 110	Unassigned	0.78
1111 1110 0	Unassigned	0.2
1111 1110 10	Link local use addresses	0.098
1111 1110 11	Site local use addresses	0.098
1111 1111	Multicast addresses	0.39

IPv6 Special Purpose Addresses

	n bits	m bits	o bits	p bits	(125-m-n-o-p) bits
010	Registry ID	Provider ID	Subscriber ID	Subnet ID	Interface ID

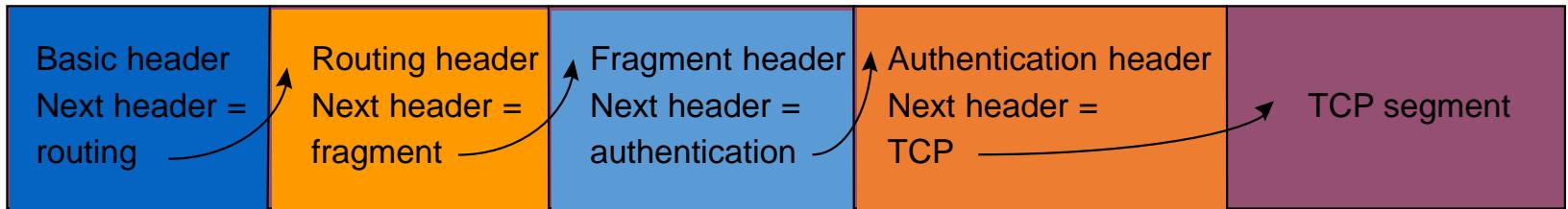
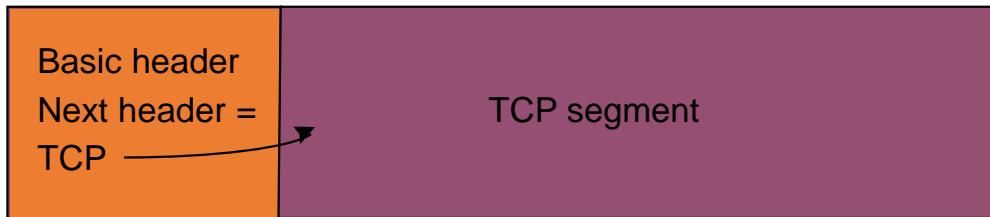
- *Provider-based Addresses:* 010 prefix
 - Assigned by providers to their customers
 - Hierarchical structure promotes aggregation
 - Registry ID: ARIN, RIPE, APNIC
 - ISP
 - Subscriber ID: subnet ID & interface ID
- *Local Addresses:* do not connect to global Internet
 - Link-local: for single link
 - Site-local: for single site
 - Designed to facilitate transition to connection to Internet

IPv6 Special Purpose Addresses

- *Unspecified Address:* 0::0
 - Used by source station to learn own address
- *Loopback Address:* ::1
- *IPv4-compatible addresses:* 96 0's + IPv4
 - For tunneling by IPv6 routers connected to IPv4 networks
 - ::135.150.10.247
- *IP-mapped addresses:* 80 0's + 16 1's + IPv4
 - Denote IPv4 hosts & routers that do not support IPv6

IPv6 Packet Extension Headers

Daisy chains of extension headers



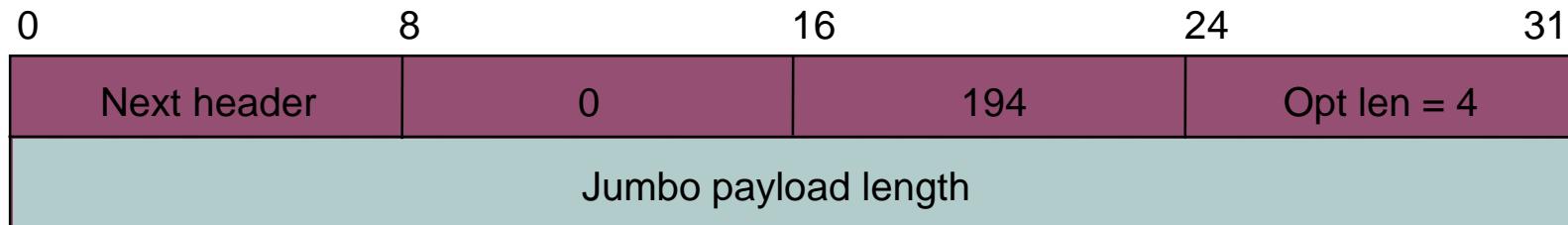
- Extension headers processed in order of appearance

IPv6 Six Extension Headers

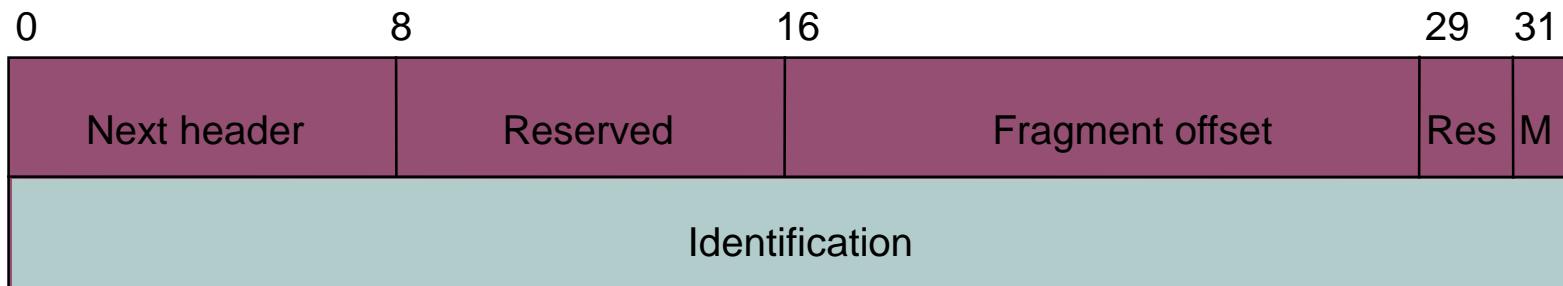
Header code	Header type
0	Hop-by-hop options header
43	Routing header
44	Fragment header
51	Authentication header
52	Encapsulating security payload header
60	Destination options header

IPv6 Extension Headers

- Large Packet: payload>64K

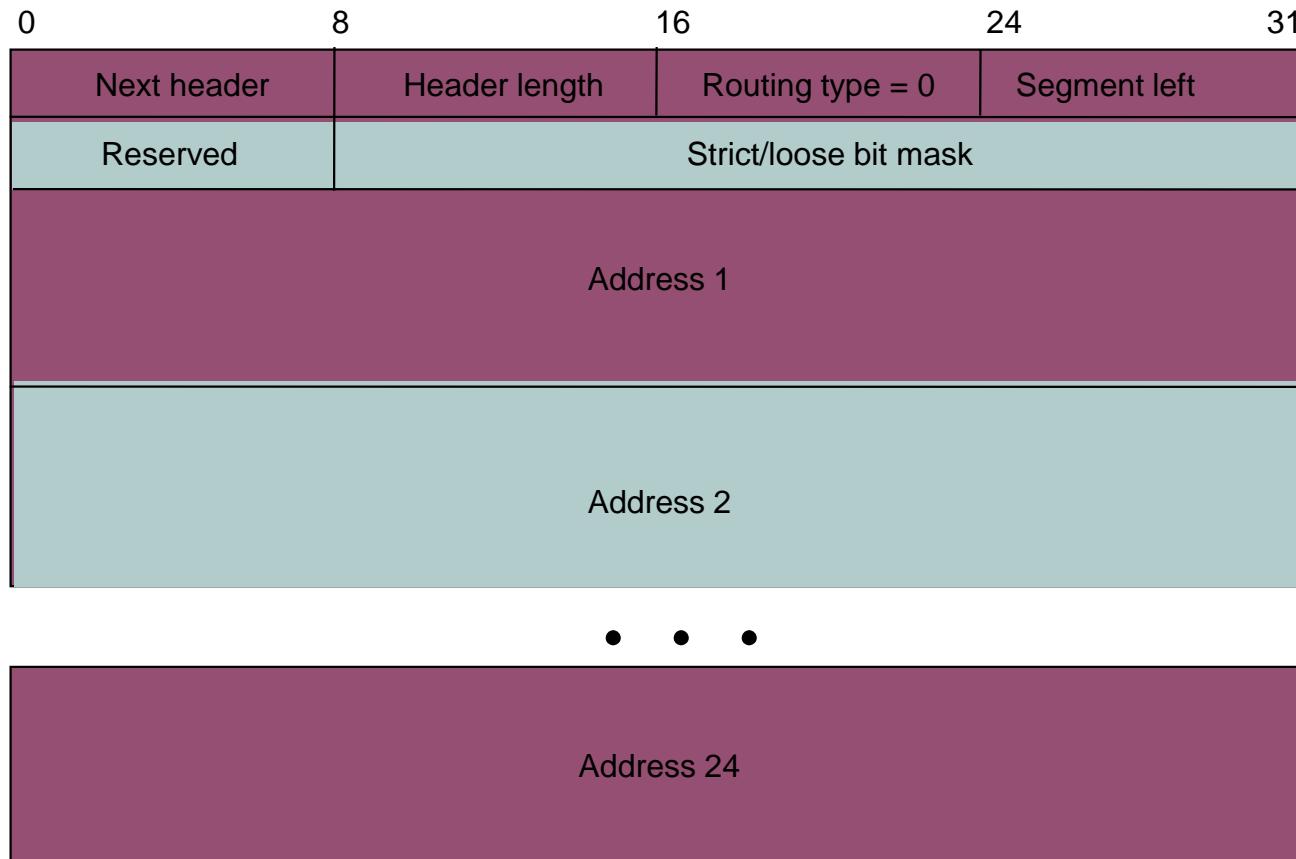


- Fragmentation: At source only



IPv6 Extension Headers

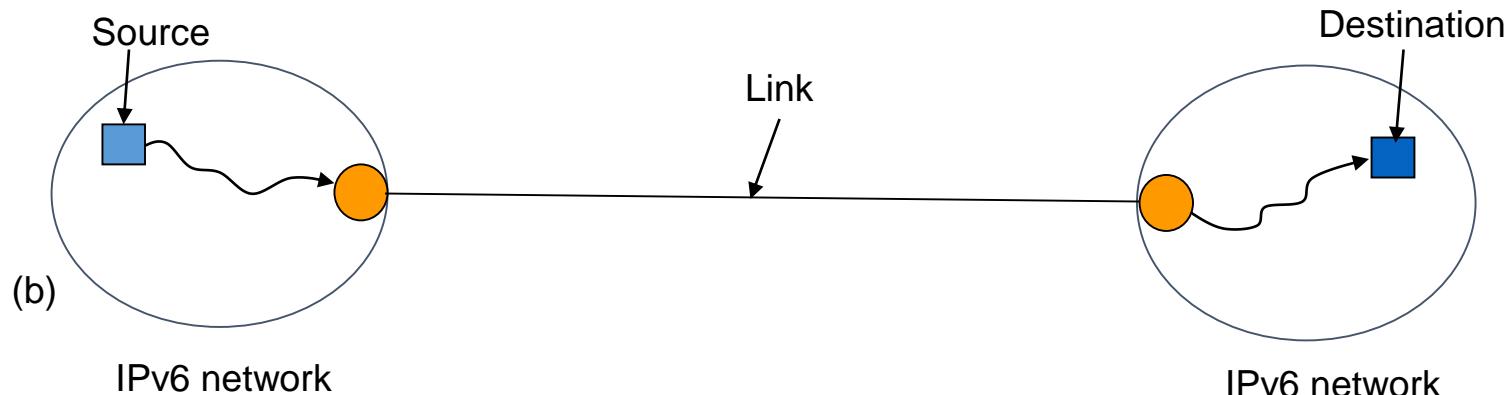
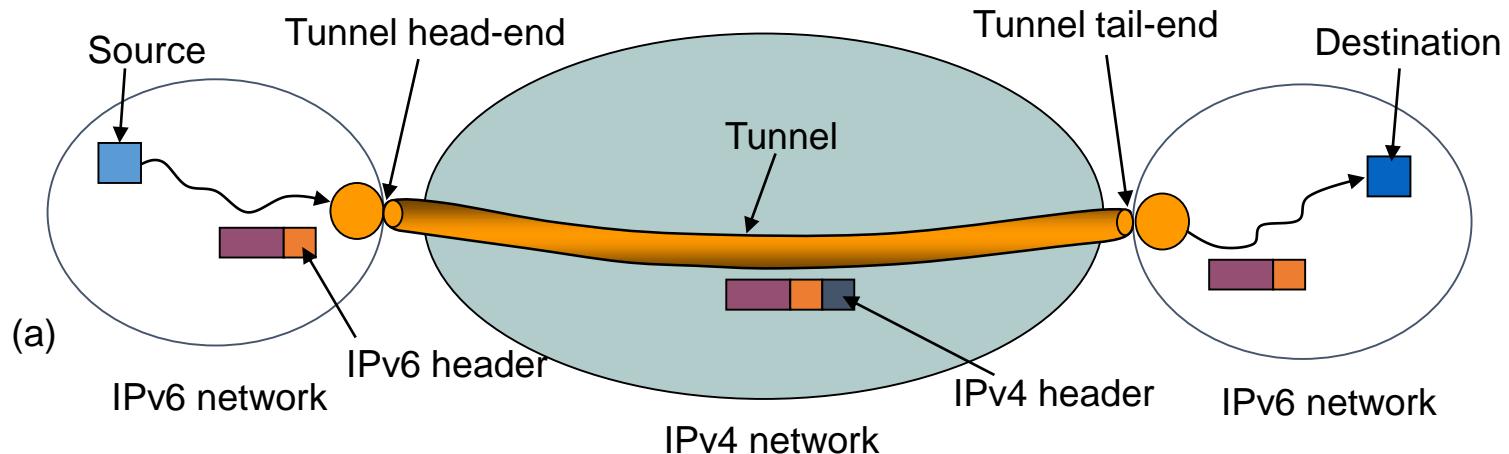
- Source Routing: strict/loose routes



Migration from IPv4 to IPv6

- Gradual transition from IPv4 to IPv6
- Dual IP stacks: routers run IPv4 & IPv6
 - Type field used to direct packet to IP version
- IPv6 islands can tunnel across IPv4 networks
 - Encapsulate user packet inside IPv4 packet
 - Tunnel endpoint at source host, intermediate router, or destination host
 - Tunneling can be recursive

Migration from IPv4 to IPv6



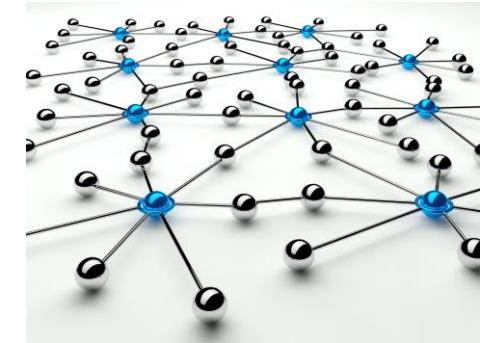
Networks Architectures and Protocols

9. TRANSPORT LAYER PROTOCOLS TCP & UDP

Lecturer: Zoltán Gál, PhD

Faculty of Informatics, University of Debrecen

February 05, 2018



Outline

- UDP Protocol
- TCP Protocol
 - Reliable Stream Service
 - TCP Connection Management
 - TCP Flow Control
 - TCP Congestion Control

Our goals:

- Understand principles behind transport layer services:
 - multiplexing, demultiplexing
 - reliable data transfer
 - flow control
 - congestion control
- Learn about Internet transport layer protocols:
 - UDP: connectionless transport
 - TCP: connection-oriented reliable transport
 - TCP congestion control

Encapsulation

TCP Header contains source & destination port numbers

IP Header contains source and destination IP addresses; transport protocol type

Ethernet Header contains source & destination MAC addresses; network protocol type

HTTP Request

TCP header HTTP Request

HTTP Request

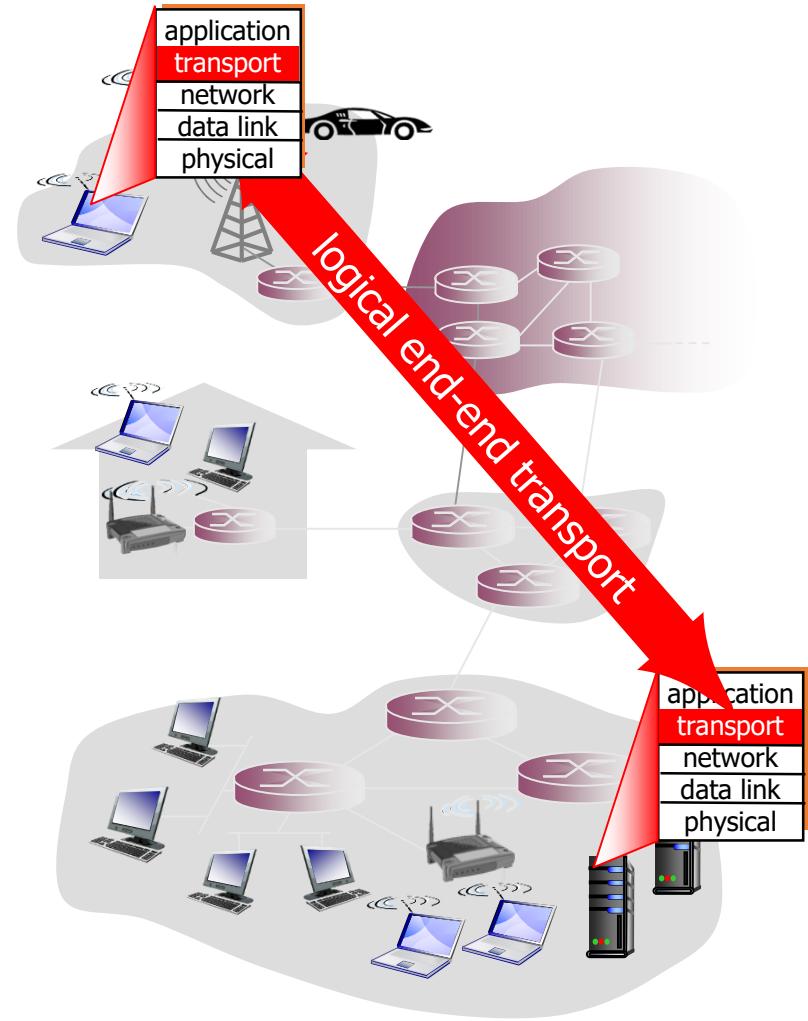
IP header TCP header HTTP Request

HTTP Request

Ethernet header IP header TCP header HTTP Request FCS

Transport services and protocols

- provide *logical communication* between app processes running on different hosts
- transport protocols run in end systems
 - send side: breaks app messages into *segments*, passes to network layer
 - rcv side: reassembles segments into messages, passes to app layer
- more than one transport protocol available to apps
 - Internet: TCP and UDP



Transport vs. network layer

- *network layer:*
logical communication between hosts
- *transport layer:*
logical communication between processes
 - relies on, enhances, network layer services

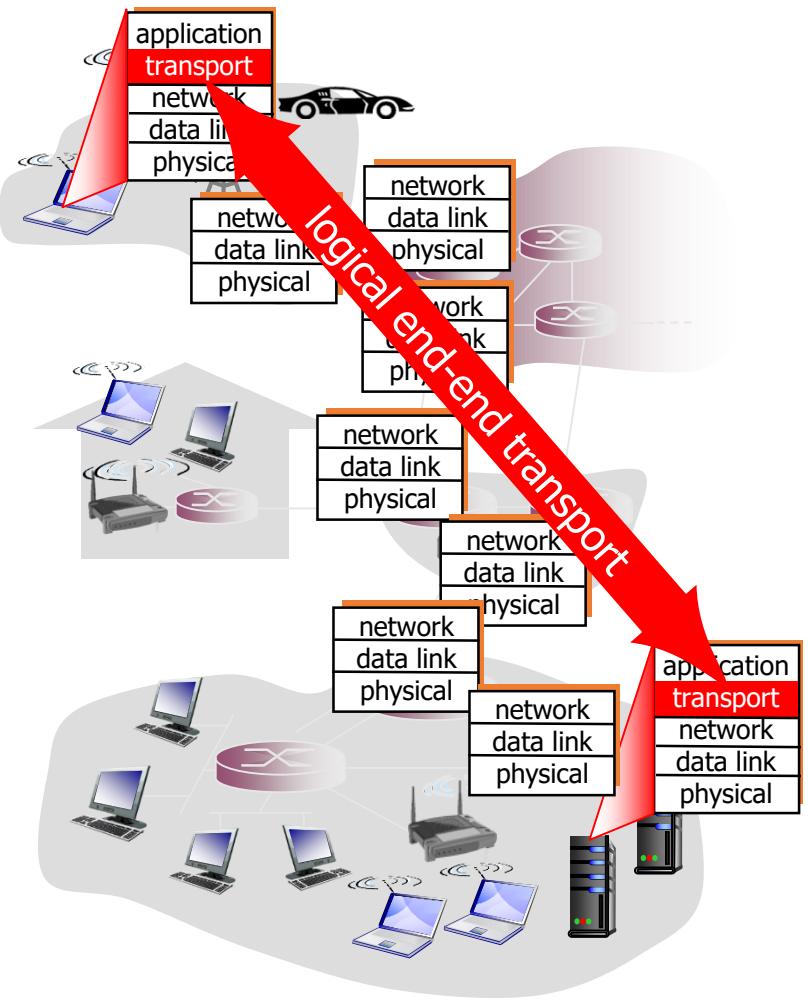
household analogy:

12 kids in Ann's house sending letters to 12 kids in Bill's house:

- hosts = houses
- processes = kids
- app messages = letters in envelopes
- transport protocol = Ann and Bill who demux to in-house siblings
- network-layer protocol = postal service

Internet transport-layer protocols

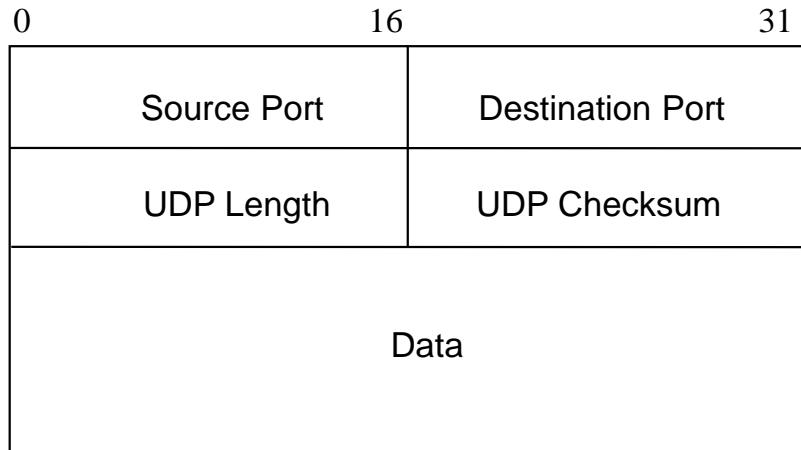
- reliable, in-order delivery (TCP)
 - congestion control
 - flow control
 - connection setup
- unreliable, unordered delivery: UDP
 - no-frills extension of “best-effort” IP
- services not available:
 - delay guarantees
 - bandwidth guarantees



UDP: User Datagram Protocol

- Best effort datagram service
- Multiplexing enables sharing of IP datagram service
- Simple transmitter & receiver
 - Connectionless: no handshaking & no connection state
 - Low header overhead
 - No flow control, no error control, no congestion control
 - UDP datagrams can be lost or out-of-order
- Applications
 - multimedia (e.g. RTP)
 - network services (e.g. DNS, RIP, SNMP)

UDP Datagram



Ports:

0-255: Well-known ports

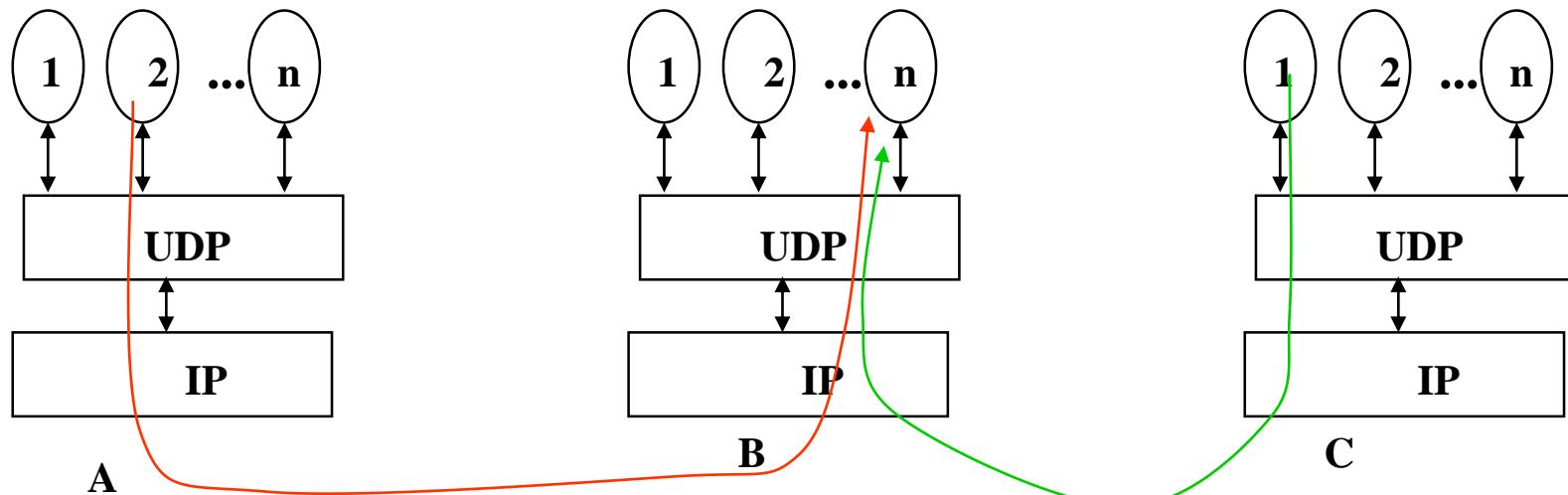
256-1023: Less well-known ports

1024-65536: Ephemeral client ports

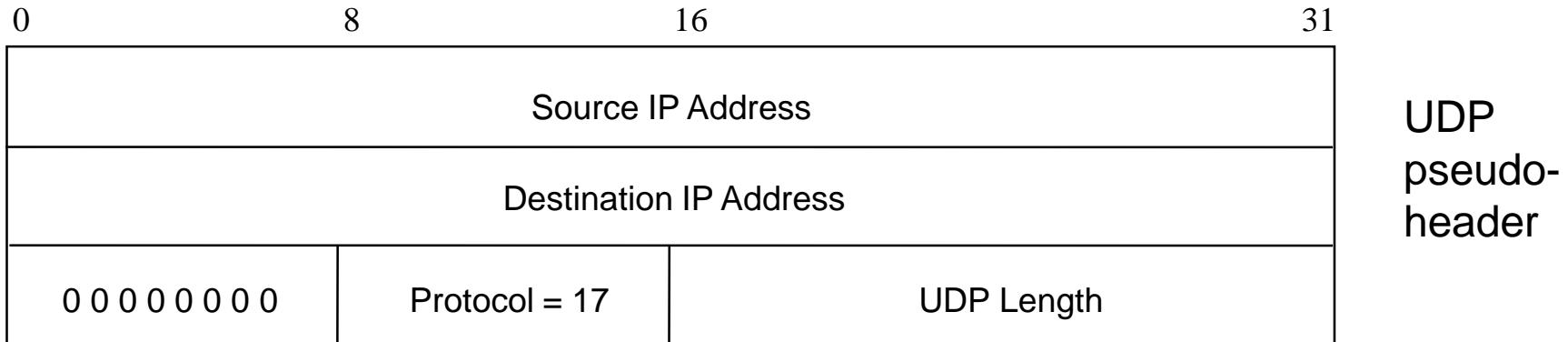
- Source and destination port numbers
 - Client ports are ephemeral
 - Server ports are well-known
 - Max number is 65,535
- UDP length
 - Total number of bytes in datagram (including header)
 - $8 \text{ bytes} \leq \text{length} \leq 65,535$
- UDP Checksum
 - Optionally detects errors in UDP datagram

UDP Multiplexing

- All UDP datagrams arriving to IP address B and destination port number n are delivered to the same process
- Source port number is not used in multiplexing



UDP Checksum Calculation



- UDP checksum detects for end-to-end errors
- Covers pseudoheader followed by UDP datagram
- IP addresses included to detect against misdelivery
- IP & UDP checksums set to zero during calculation
- Pad with 1 byte of zeros if UDP length is odd

UDP Receiver Checksum

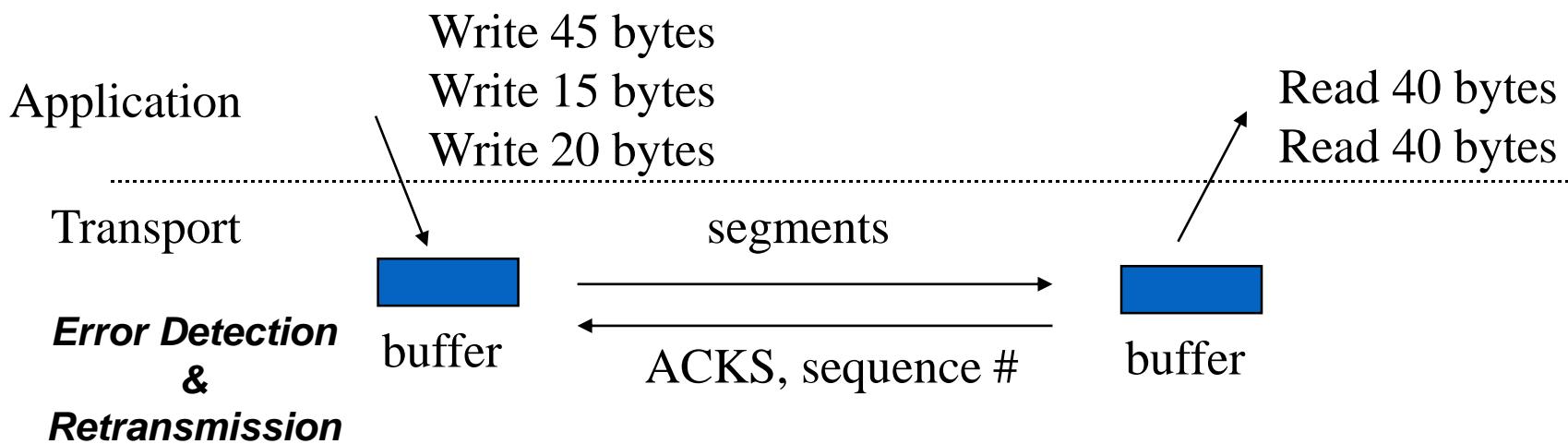
- UDP receiver recalculates the checksum and silently discards the datagram if errors detected
 - “silently” means no error message is generated
- The use of UDP checksums is optional
- But hosts are required to have checksums enabled

TCP: Transmission Control Protocol

- Reliable byte-stream service
- More complex transmitter & receiver
 - Connection-oriented: full-duplex unicast connection between client & server processes
 - Connection setup, connection state, connection release
 - Higher header overhead
 - Error control, flow control, and congestion control
 - Higher delay than UDP
- Most applications use TCP
 - HTTP, SMTP, FTP, TELNET, POP3, ...

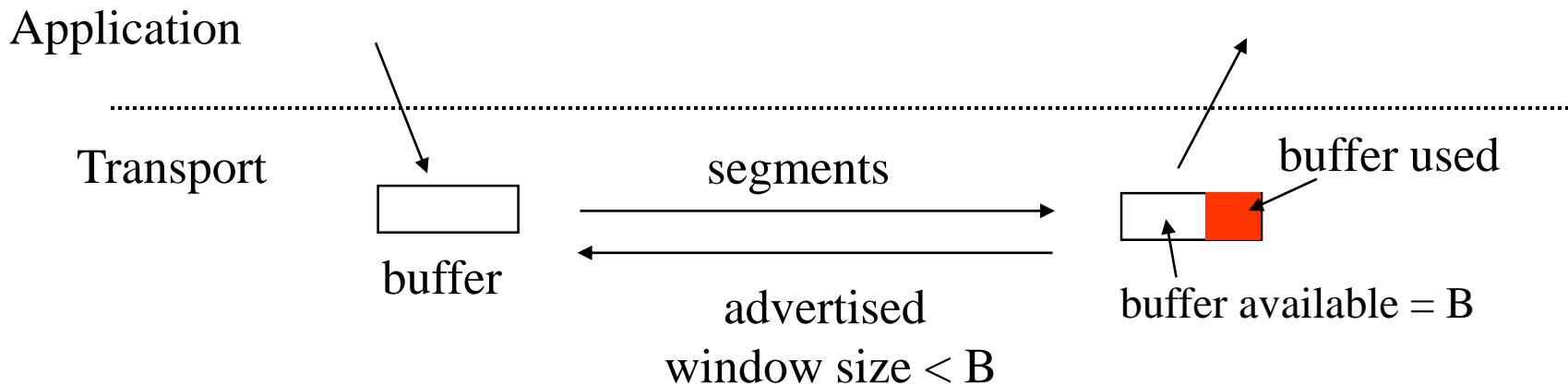
TCP Reliable Byte-Stream Service

- Stream Data Transfer
 - transfers a contiguous stream of bytes across the network, with no indication of boundaries
 - groups bytes into segments
 - transmits segments as convenient (Push function defined)
- Reliability
 - error control mechanism to deal with IP transfer impairments



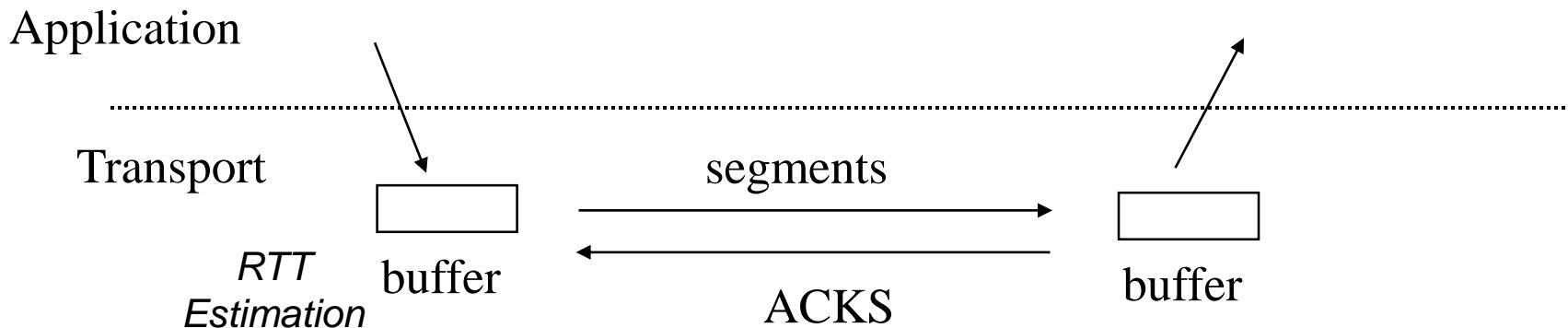
Flow Control

- Buffer limitations & speed mismatch can result in loss of data that arrives at destination
- Receiver controls rate at which sender transmits to prevent buffer overflow



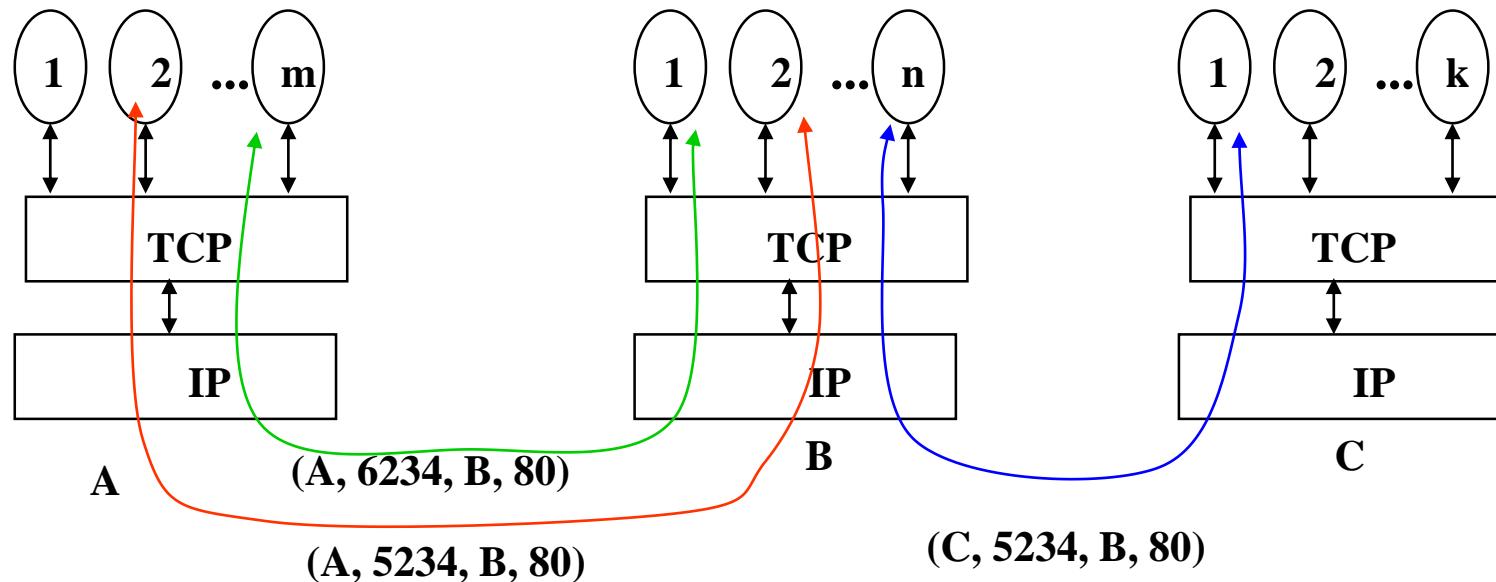
Congestion Control

- Available bandwidth to destination varies with activity of other users
- Transmitter dynamically adjusts transmission rate according to network congestion as indicated by RTT (round trip time) & ACKs
- Elastic utilization of network bandwidth

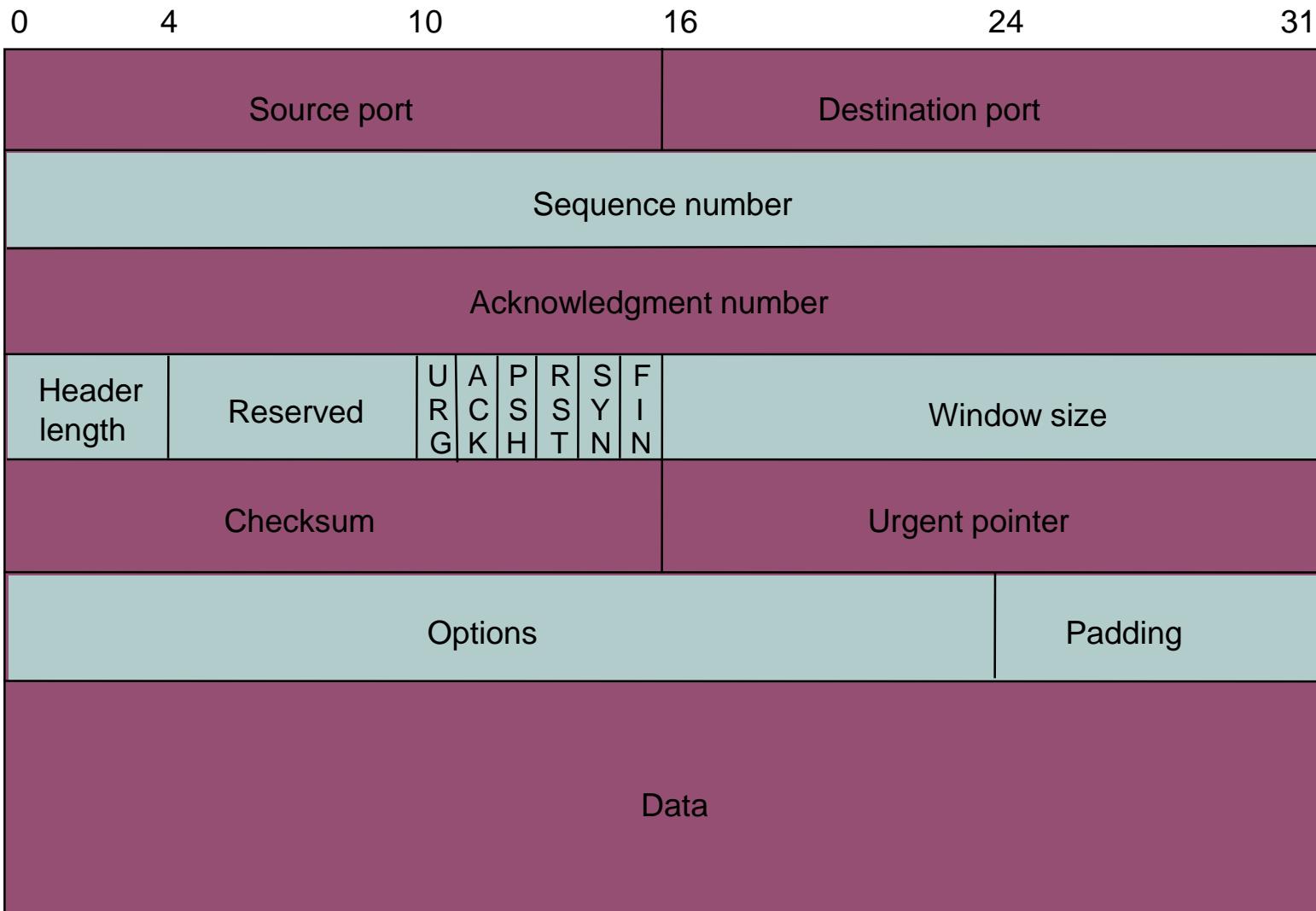


TCP Multiplexing

- A *TCP connection* is specified by a *4-tuple*
 - (source IP address, source port, destination IP address, destination port)
- TCP allows multiplexing of multiple connections between end systems to support multiple applications simultaneously
- Arriving segment directed according to connection 4-tuple



TCP Segment Format



- Each TCP segment has header of 20 or more bytes + 0 or more bytes of data

TCP Header

Port Numbers

- A socket identifies a connection endpoint
 - IP address + port
- A connection specified by a *socket pair*
- Well-known ports
 - FTP 20
 - Telnet 23
 - DNS 53
 - HTTP 80

Sequence Number

- Byte count
- First byte in segment
- 32 bits long
- $0 \leq SN \leq 2^{32}-1$
- Initial sequence number selected during connection setup

TCP Header

Acknowledgement Number

- SN of next byte expected by receiver
- Acknowledges that all prior bytes in stream have been received correctly
- Valid if ACK flag is set

Header length

- 4 bits
- Length of header in multiples of 32-bit words
- Minimum header length is 20 bytes
- Maximum header length is 60 bytes

TCP Header

Reserved	Control
• 6 bits	<ul style="list-style-type: none">• 6 bits• URG: urgent pointer flag<ul style="list-style-type: none">• Urgent message end = SN + urgent pointer• ACK: ACK packet flag• PSH: override TCP buffering• RST: reset connection<ul style="list-style-type: none">• Upon receipt of RST, connection is terminated and application layer notified• SYN: establish connection• FIN: close connection

TCP Header

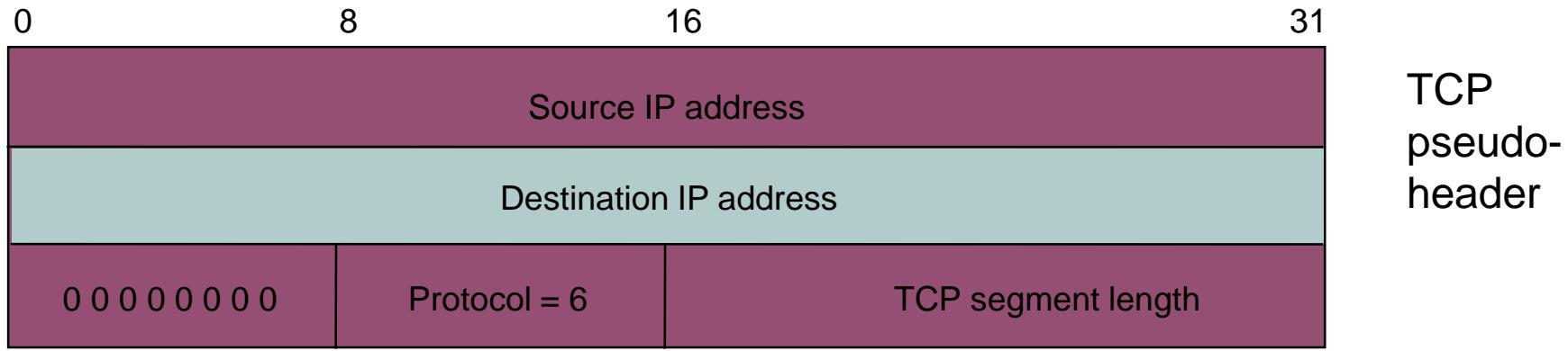
Window Size

- 16 bits to advertise window size
- Used for flow control
- Sender will accept bytes with SN from ACK to ACK + window
- Maximum window size is 65535 bytes

TCP Checksum

- Internet checksum method
- TCP pseudoheader + TCP segment

TCP Checksum Calculation



- TCP error detection uses same procedure as UDP

TCP Header

Options

- Variable length
- NOP (No Operation) option is used to pad TCP header to multiple of 32 bits
- Time stamp option is used for round trip measurements

Options

- Maximum Segment Size (MSS) option specifies largest segment a receiver wants to receive
- Window Scale option increases TCP window from 16 to 32 bits

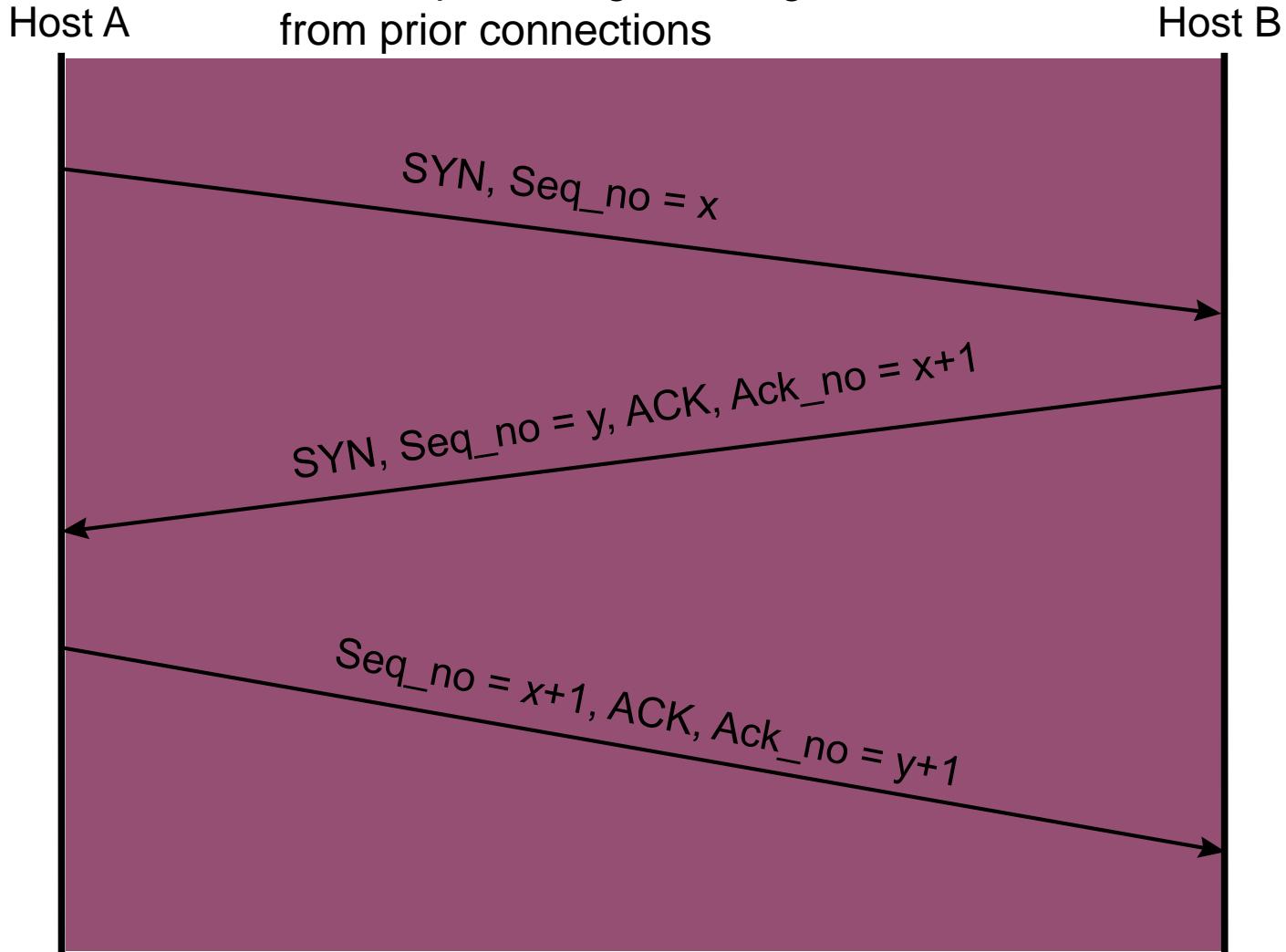
TCP Connection Management

Initial Sequence Number

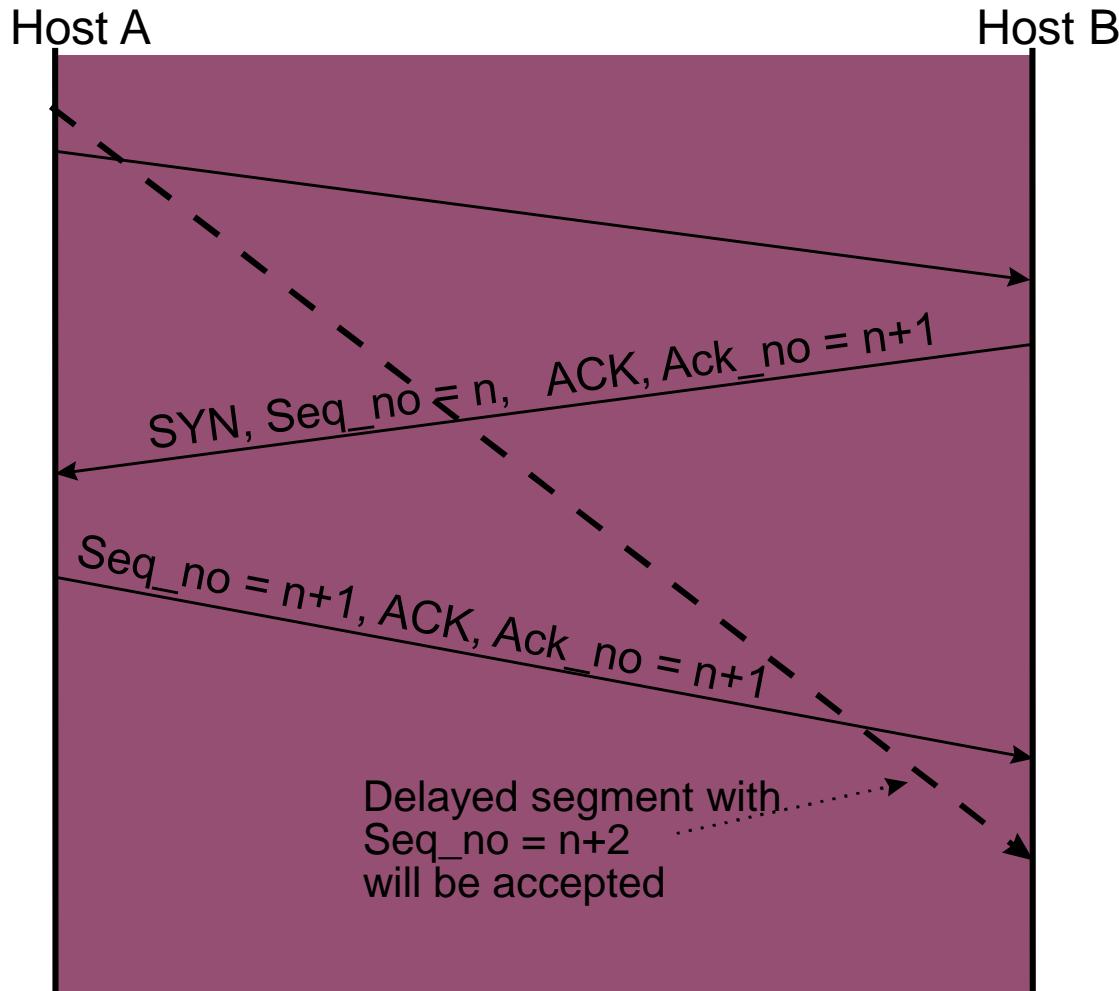
- Select initial sequence numbers (ISN) to protect against segments from prior connections (that may circulate in the network and arrive at a much later time)
- Select ISN to avoid overlap with sequence numbers of prior connections
- Use local clock to select ISN sequence number
- Time for clock to go through a full cycle should be greater than the maximum lifetime of a segment (MSL); Typically MSL=120 seconds
- High bandwidth connections pose a problem
- $2^n > 2 * \text{max packet life} * R \text{ bytes/second}$

TCP Connection Establishment

- “Three-way Handshake”
- ISN’s protect against segments from prior connections



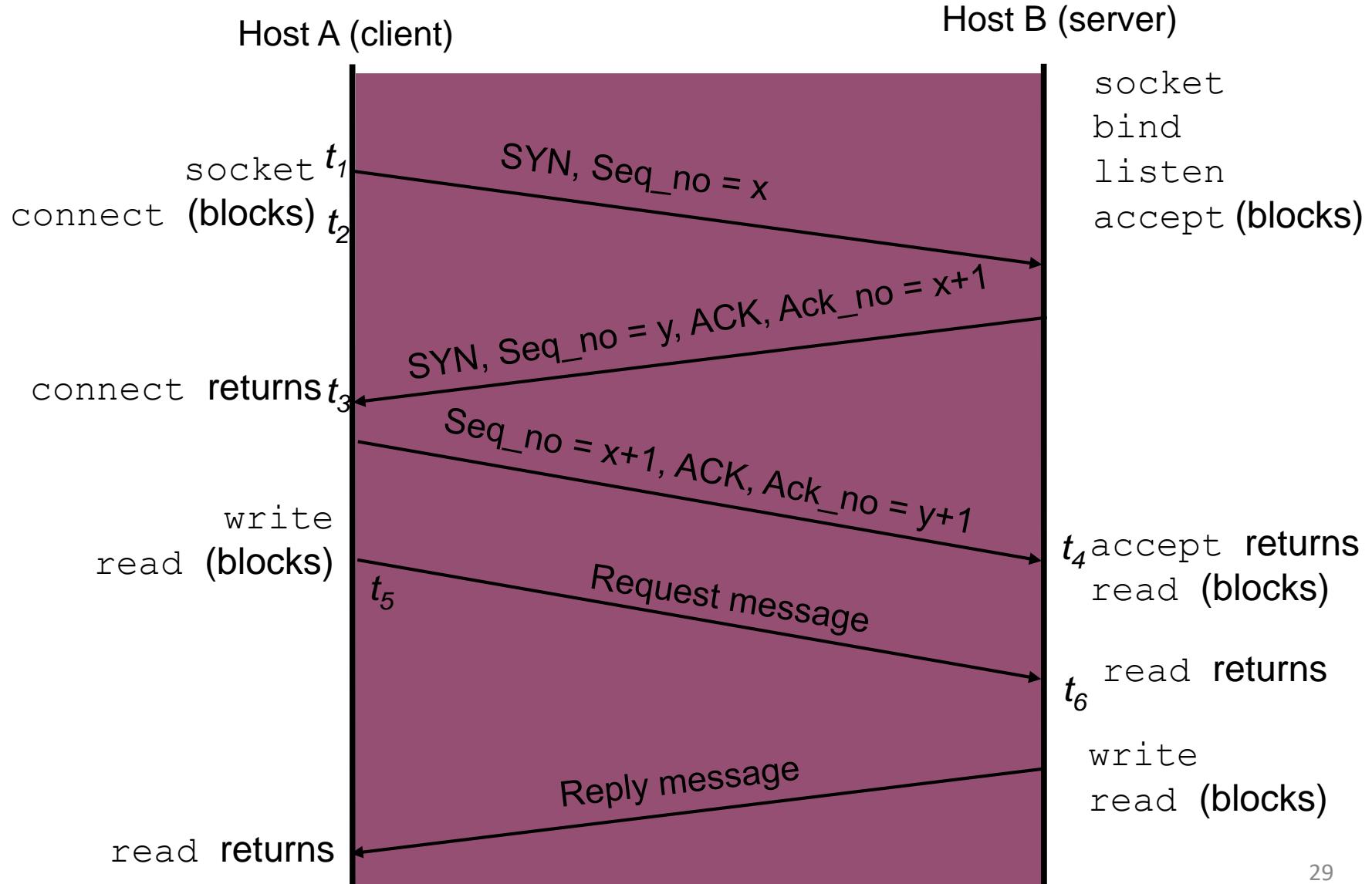
If host always uses the same ISN



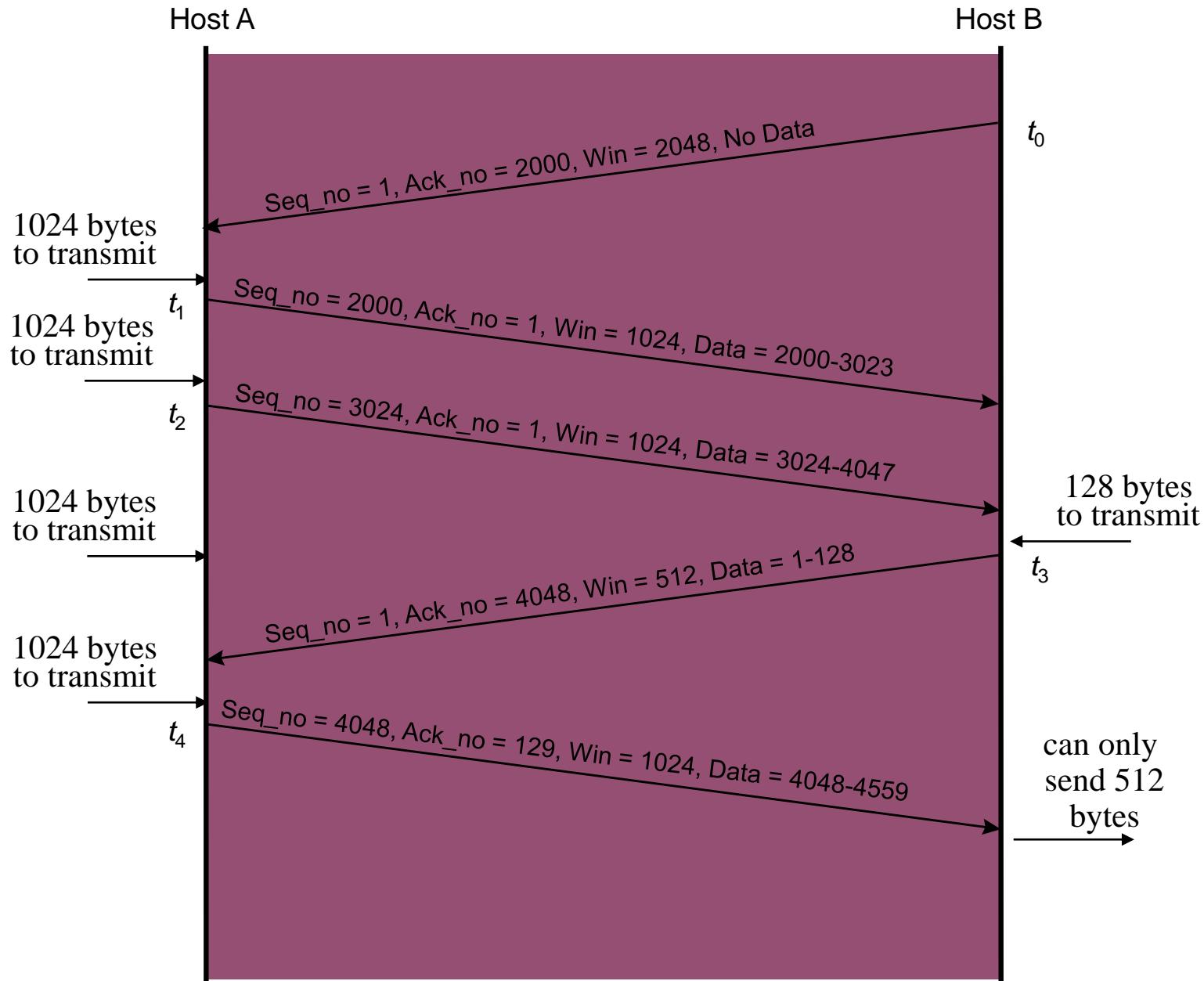
Maximum Segment Size

- Maximum Segment Size
 - largest block of data that TCP sends to other end
- Each end can announce its MSS during connection establishment
- Default is 576 bytes including 20 bytes for IP header and 20 bytes for TCP header
- Ethernet implies MSS of 1460 bytes
- IEEE 802.3 implies 1452

Client-Server Application



TCP Window Flow Control



Sequence Number Wraparound

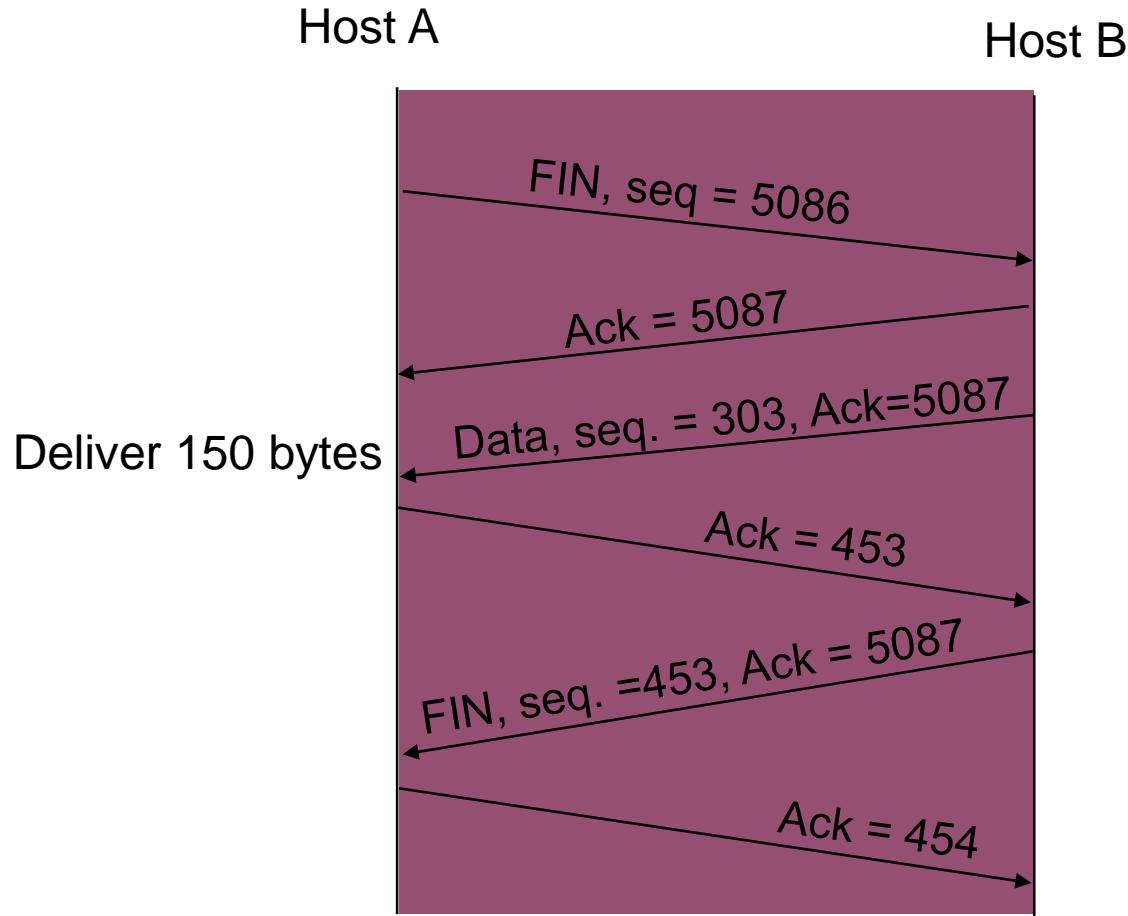
- $2^{32} = 4.29 \times 10^9$ bytes = 34.3×10^9 bits
 - At 1 Gbps, sequence number wraparound in 34.3 seconds.
- Timestamp option: Insert 32 bit timestamp in header of each segment
 - Timestamp + sequence no → 64-bit seq. no
 - Timestamp clock must:
 - tick forward at least once every 2^{31} bits
 - Not complete cycle in less than one MSL
 - Example: clock tick every 1 ms @ 8 Tbps wraps around in 25 days

Delay-BW Product & Advertised Window Size

- Suppose RTT=100 ms, R=2.4 Gbps
 - # bits in pipe = 3 Mbytes
- If single TCP process occupies pipe, then required advertised window size is
 - RTT x Bit rate = 3 Mbytes
 - Normal maximum window size is 65535 bytes
- Solution: Window Scale Option
 - Window size up to $65535 \times 2^{14} = 1$ Gbyte allowed
 - Requested in SYN segment

TCP Connection Closing

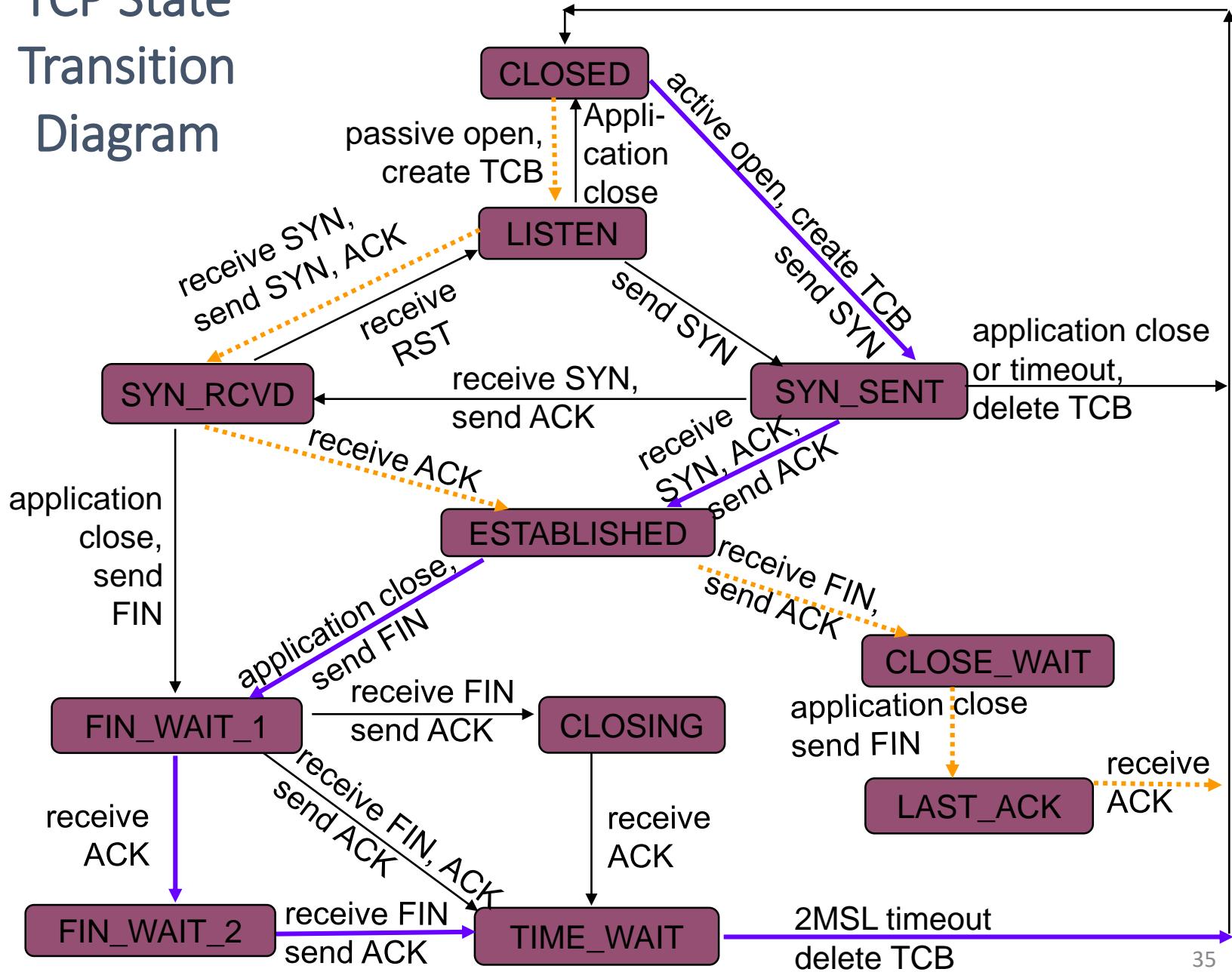
“Graceful Close”



TIME_WAIT state

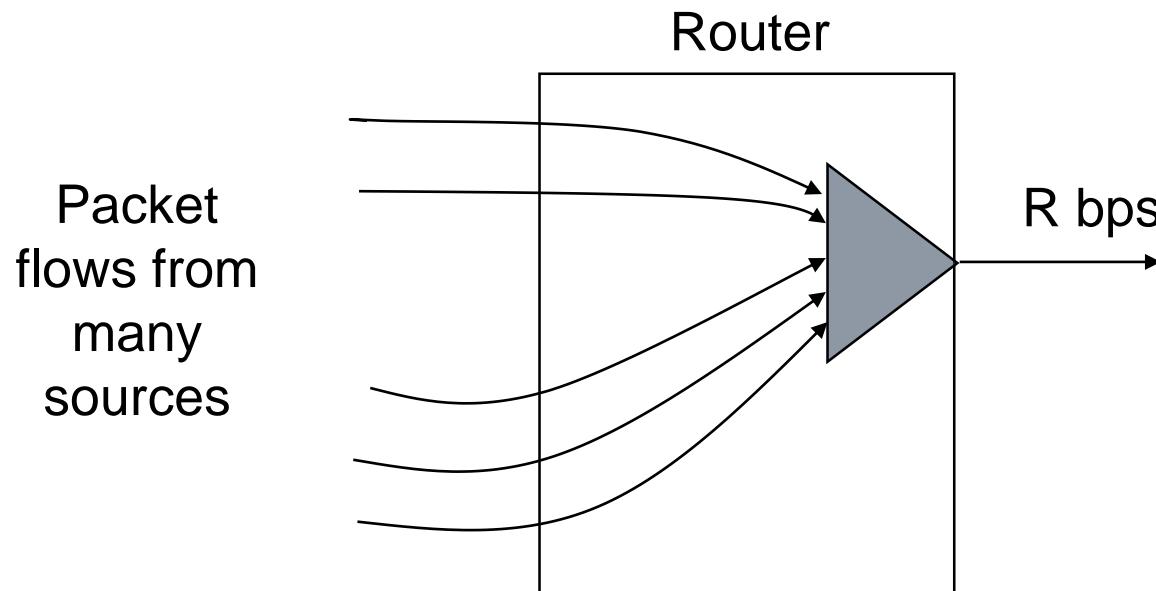
- When TCP receives ACK to last FIN, TCP enters TIME_WAIT state
 - Protects future incarnations of connection from delayed segments
 - $\text{TIME_WAIT} = 2 \times \text{MSL}$
 - Only valid segment that can arrive while in TIME_WAIT state is FIN retransmission
 - If such segment arrives, resend ACK & restart TIME_WAIT timer
 - When timer expires, close TCP connection & delete connection record

TCP State Transition Diagram



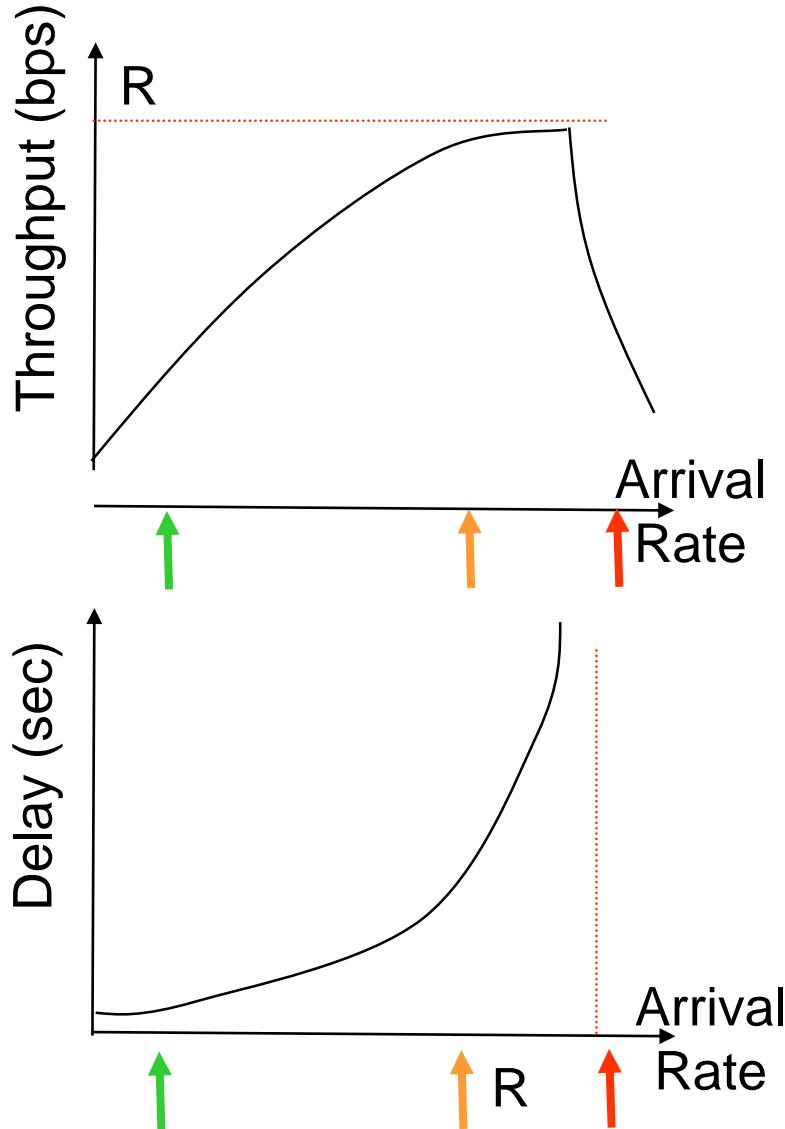
TCP Congestion Control

- *Advertised window size* is used to ensure that receiver's buffer will not overflow
- However, buffers at intermediate routers between source and destination may overflow



- Congestion occurs when total arrival rate from all packet flows exceeds R over a sustained period of time
- Buffers at multiplexer will fill and packets will be lost

Phases of Congestion Behavior



1. Light traffic

- Arrival Rate $<< R$
- Low delay
- Can accommodate more

2. Knee (congestion onset)

- Arrival rate approaches R
- Delay increases rapidly
- Throughput begins to saturate

3. Congestion collapse

- Arrival rate $> R$
- Large delays, packet loss
- Useful application throughput drops

Window Congestion Control

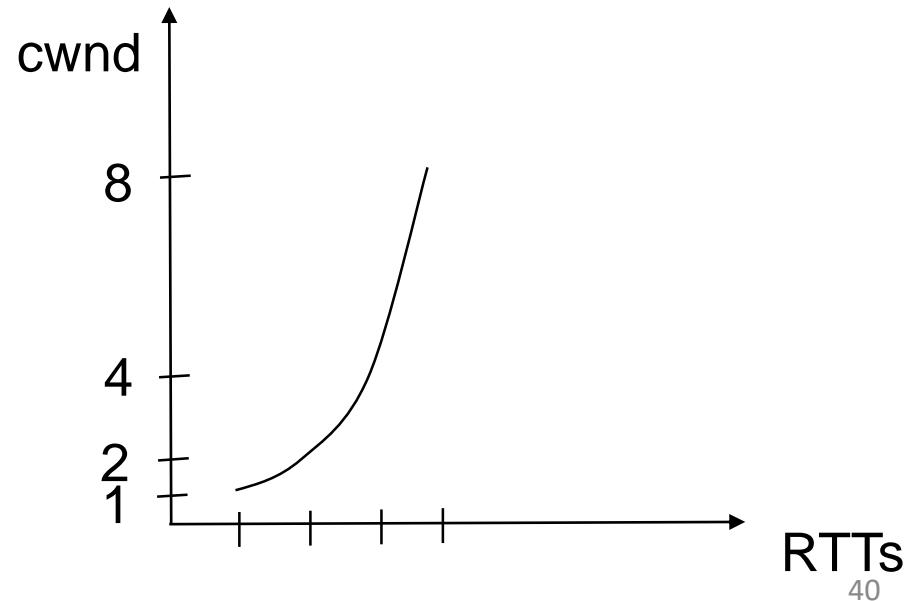
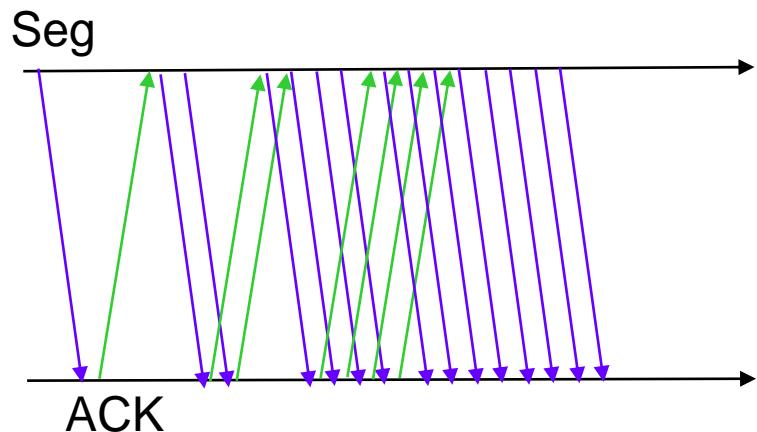
- Desired operating point: just before knee
 - Sources must control their sending rates so that aggregate arrival rate is just before knee
- TCP sender maintains a *congestion window* cwnd to control congestion at intermediate routers
- Effective window is minimum of congestion window and advertised window
- Problem: source does not know what its “fair” share of available bandwidth should be
- Solution: adapt dynamically to available BW
 - Sources probe the network by increasing cwnd
 - When congestion detected, sources reduce rate
 - Ideally, sources sending rate stabilizes near ideal point

Congestion Window

- How does the TCP congestion algorithm change congestion window dynamically according to the most up-to-date state of the network?
- At light traffic: each segment is ACKed quickly
 - Increase cwnd aggressively
- At knee: segment ACKs arrive, but more slowly
 - Slow down increase in cwnd
- At congestion: segments encounter large delays (so retransmission timeouts occur); segments are dropped in router buffers (resulting in duplicate ACKs)
 - Reduce transmission rate, then probe again

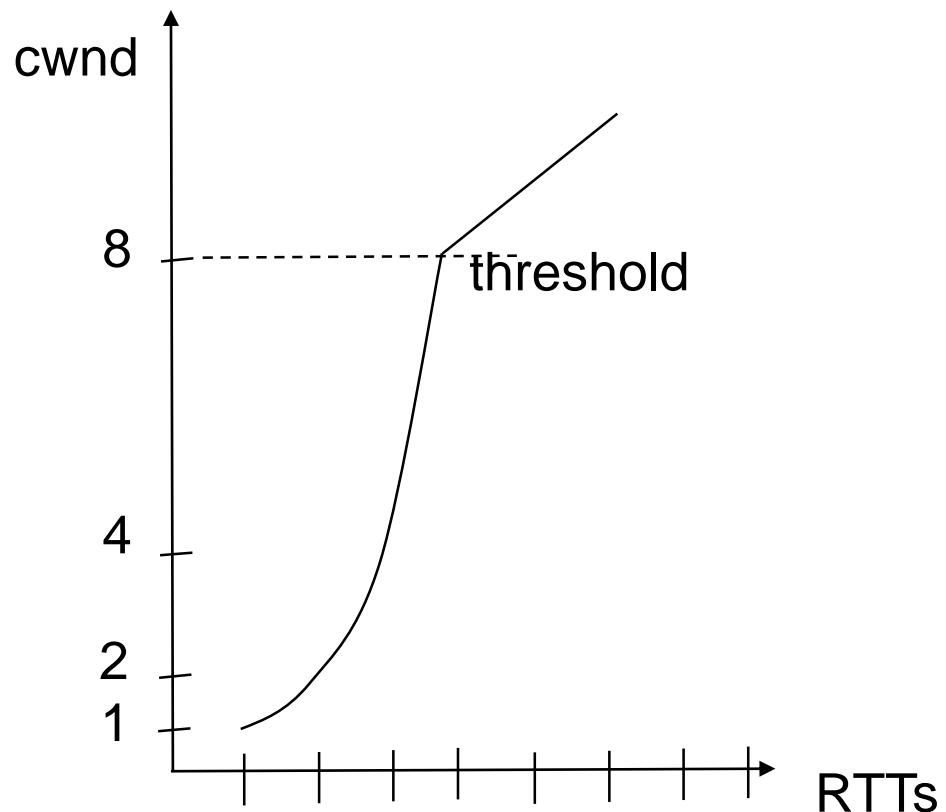
TCP Congestion Control: Slow Start

- **Slow start:** increase congestion window size by one segment upon receiving an ACK from receiver
 - initialized at ≤ 2 segments
 - used at (re)start of data transfer
 - congestion window increases exponentially

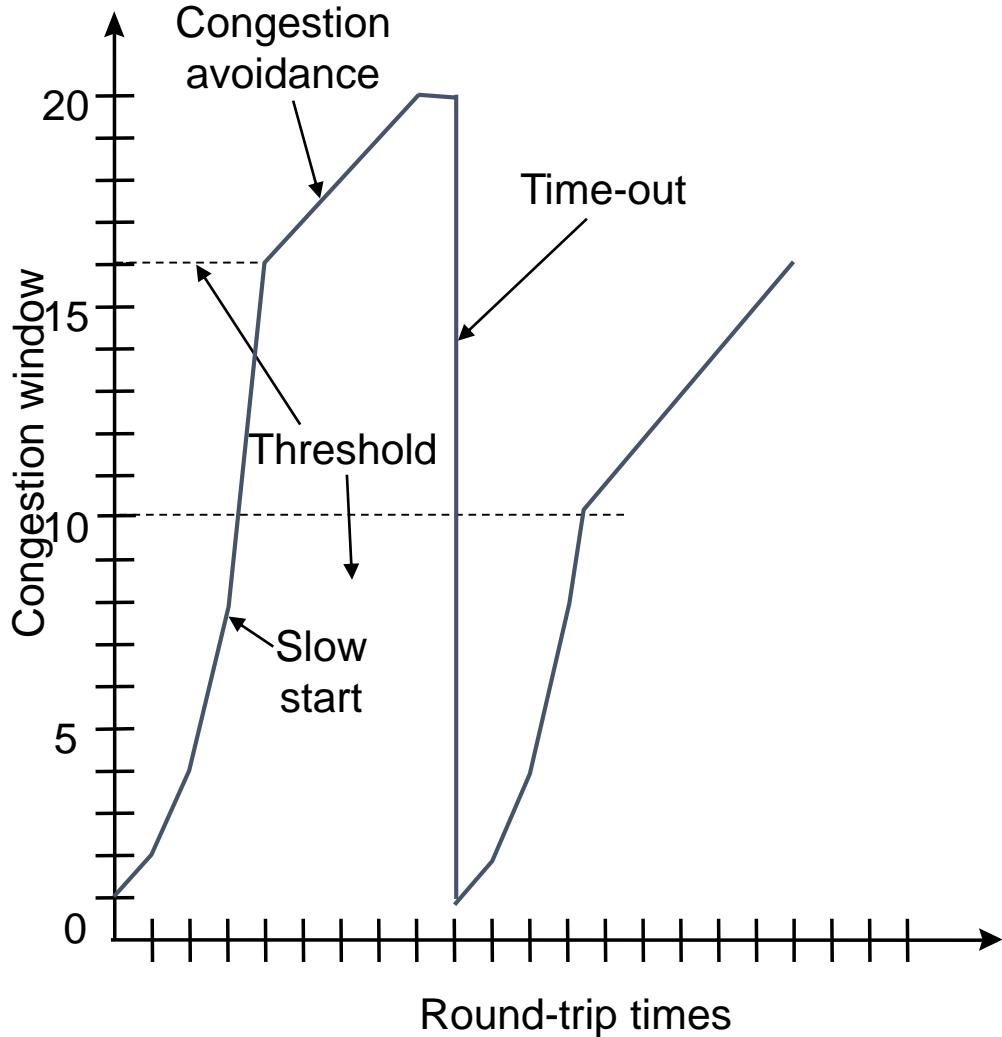


TCP Congestion Control: Congestion Avoidance

- Algorithm progressively sets a *congestion threshold*
 - When $cwnd > \text{threshold}$, slow down rate at which $cwnd$ is increased
- Increase congestion window size by one segment per round-trip-time (RTT)
 - Each time an ACK arrives, $cwnd$ is increased by $1/cwnd$
 - In one RTT, $cwnd$ segments are sent, so total increase in $cwnd$ is $cwnd \times 1/cwnd = 1$
 - $cwnd$ grows linearly with time



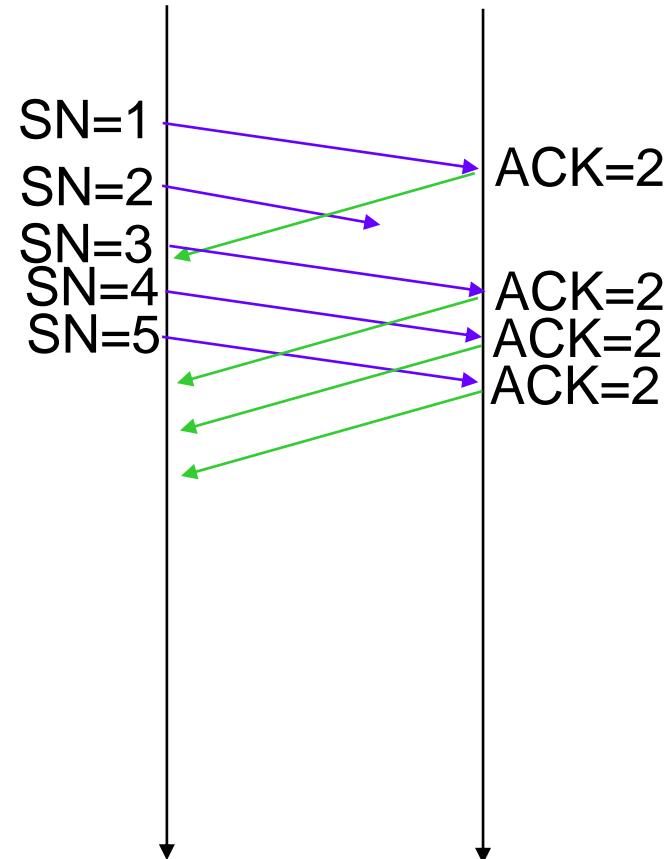
TCP Congestion Control: Congestion



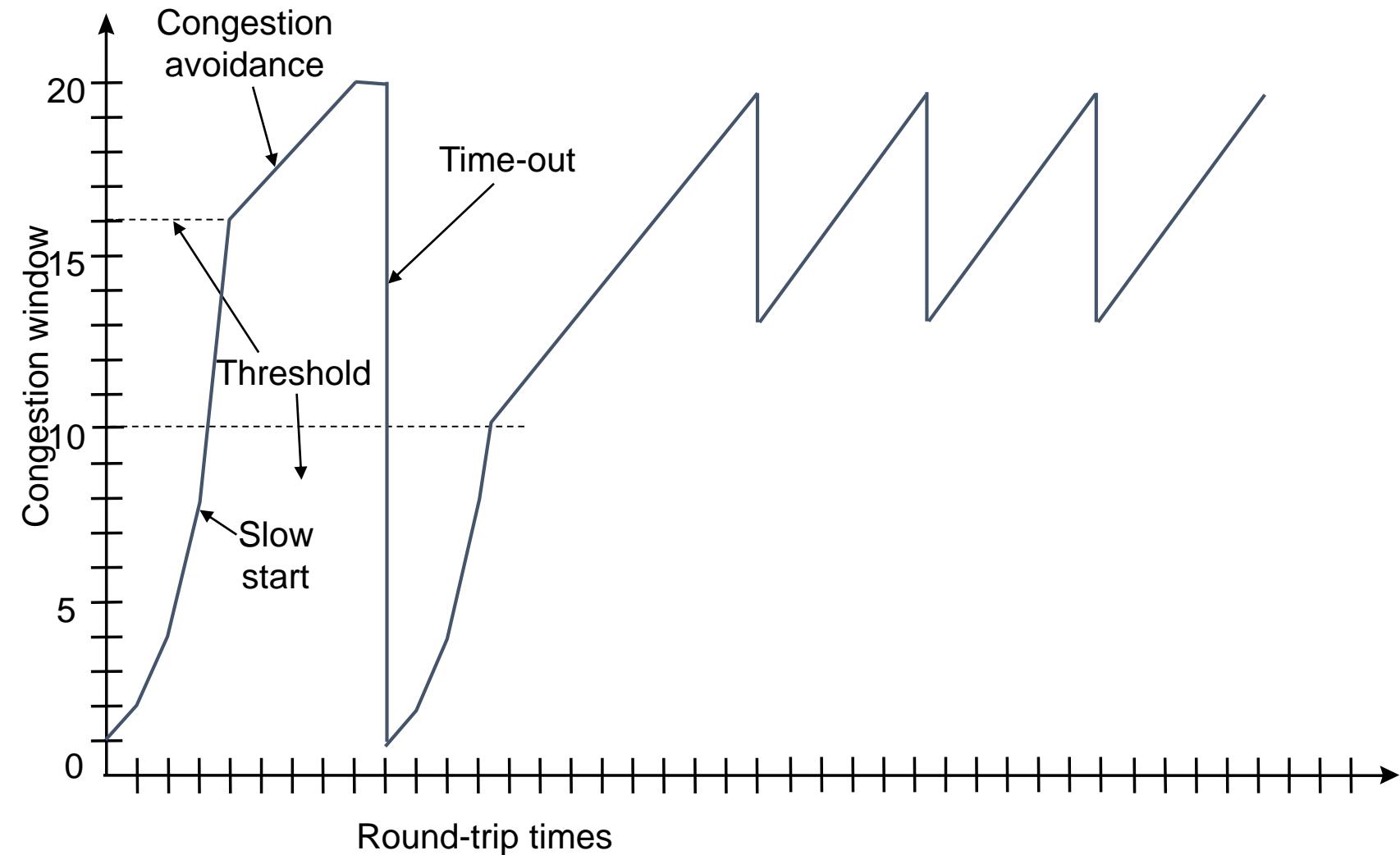
- Congestion is detected upon timeout or receipt of duplicate ACKs
- Assume current cwnd corresponds to available bandwidth
- Adjust congestion threshold = $\frac{1}{2} \times$ current cwnd
- Reset cwnd to 1
- Go back to slow-start
- Over several cycles expect to converge to congestion threshold equal to about $\frac{1}{2}$ the available bandwidth

Fast Retransmit & Fast Recovery

- Congestion causes many segments to be dropped
- If only a single segment is dropped, then subsequent segments trigger duplicate ACKs before timeout
- Can avoid large decrease in cwnd as follows:
 - When three duplicate ACKs arrive, retransmit lost segment immediately
 - Reset congestion threshold to $\frac{1}{2}$ cwnd
 - Reset cwnd to congestion threshold + 3 to account for the three segments that triggered duplicate ACKs
 - Remain in congestion avoidance phase
 - However if timeout expires, reset cwnd to 1
 - In absence of timeouts, cwnd will oscillate around optimal value



TCP Congestion Control: Fast Retransmit & Fast Recovery



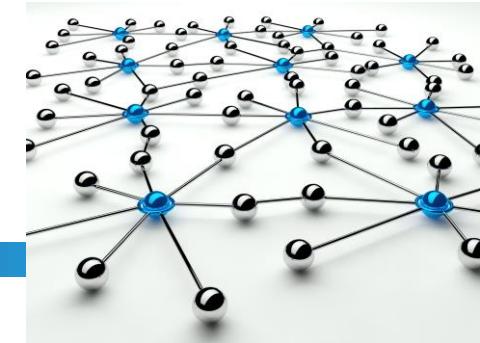
Networks Architectures and Protocols

10. APPLICATION LAYER PROTOCOLS

Lecturer: Zoltán Gál, PhD

Faculty of Informatics, University of Debrecen

February 05, 2018



Outline

1. Introduction

- 1.1. Application, Presentation, and Session**
- 1.2. How Application Protocols Interact with End-User Applications**

2. Application Layer Protocols and Well-Known Application Services

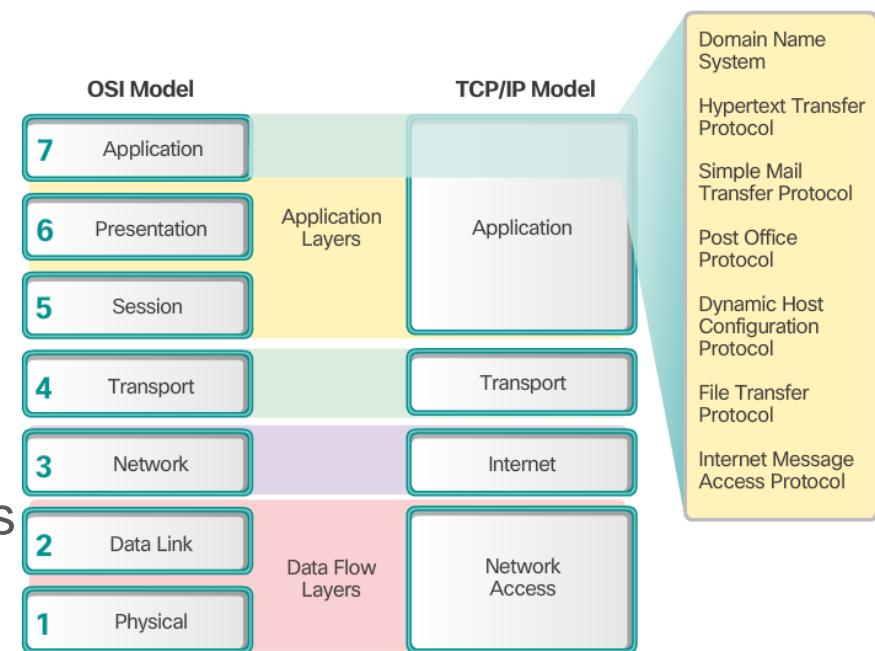
- 2.1. Web and Email Protocols**
- 2.2. IP Addressing**
- 2.3. File Sharing Services**

Section 1: Application Layer Protocols

Topic 1.1: Application, Presentation, and Session

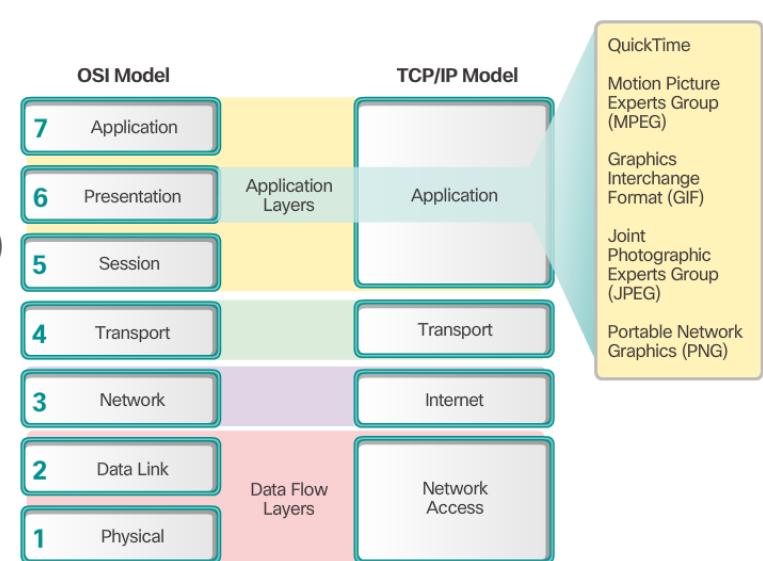
Application Layer

- The application layer is closest to the end user.
- Network applications enable users to send and receive data with ease.
- The application layer acts as interface between the applications and the underlying network.
- Application layer protocols help exchange data between programs running on the source and destination hosts.
- The TCP/IP application layer performs the functions of the upper three layers of the OSI model.
- Common application layer protocols include: HTTP, FTP, TFTP, DNS.



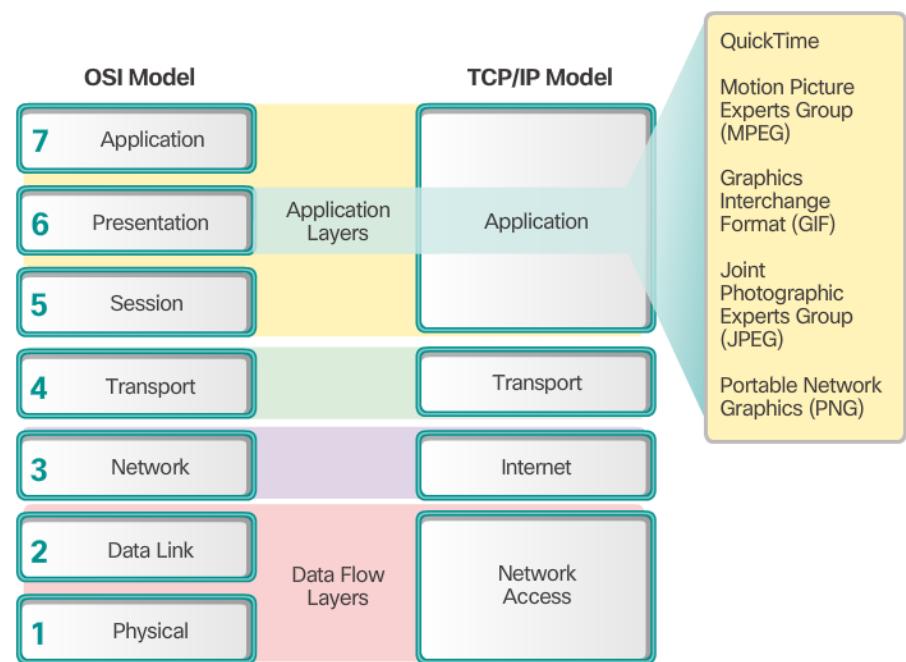
Presentation and Session Layer

- The presentation layer has three primary functions:
 - Format data
 - Compress data
 - Encrypt data
- Common standards for video include QuickTime and Motion Picture Experts Group (MPEG).
- Common graphic image formats are:
 - Graphics Interchange Format (GIF)
 - Joint Photographic Experts Group (JPEG)
 - Portable Network Graphics (PNG) format



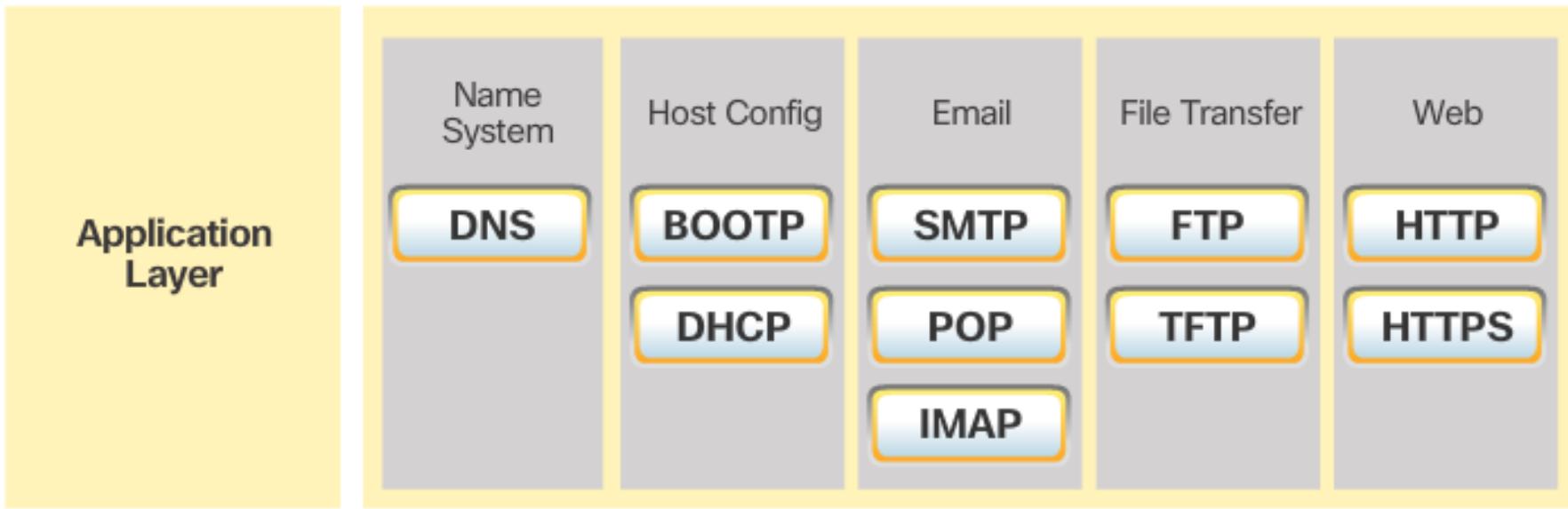
Presentation and Session Layer (cont.)

- The session layer creates and maintains dialogs between source and destination applications.
- The session layer handles the exchange of information to initiate dialogs, keep them active, and to restart sessions that are disrupted or idle for a long period of time.



TCP/IP Application Layer Protocols

- TCP/IP application protocols specify the format and control information necessary for common Internet functions.
- Application layer protocols must be implemented in both the source and destination devices.
- Application layer protocols implemented on the source and destination host must be compatible to allow communication.



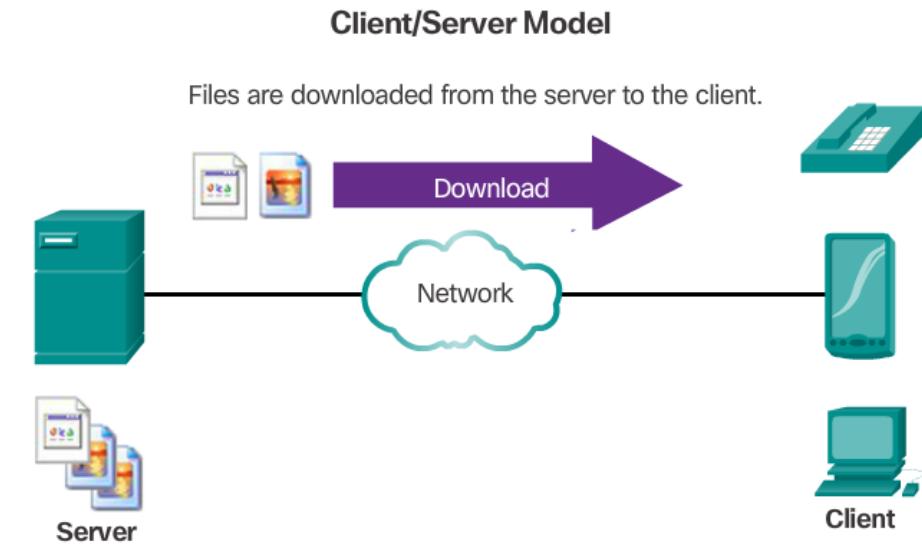
Topic 1.2:

How Application Protocols Interact with End-User Applications



Client-Server Model

- The device requesting the information is called a client.
- The device responding to the request is called a server.
- Client and server processes are considered to be in the application layer.
- The client initiates the exchange by requesting data from the server.
- The server responds by sending one or more streams of data to the client.
- Application layer protocols describe the format of the requests and responses between clients and servers.
- The contents of the data exchange will depend of the application in use.
- Email is an example of a Client-Server interaction.

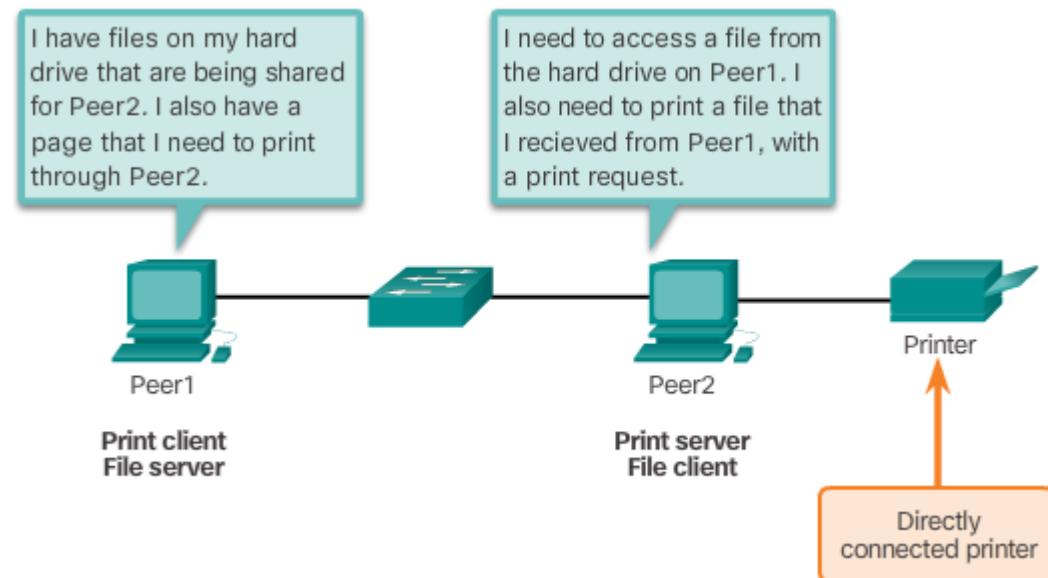


Resources are stored on the server.

A client is a hardware/software combination that people use directly.

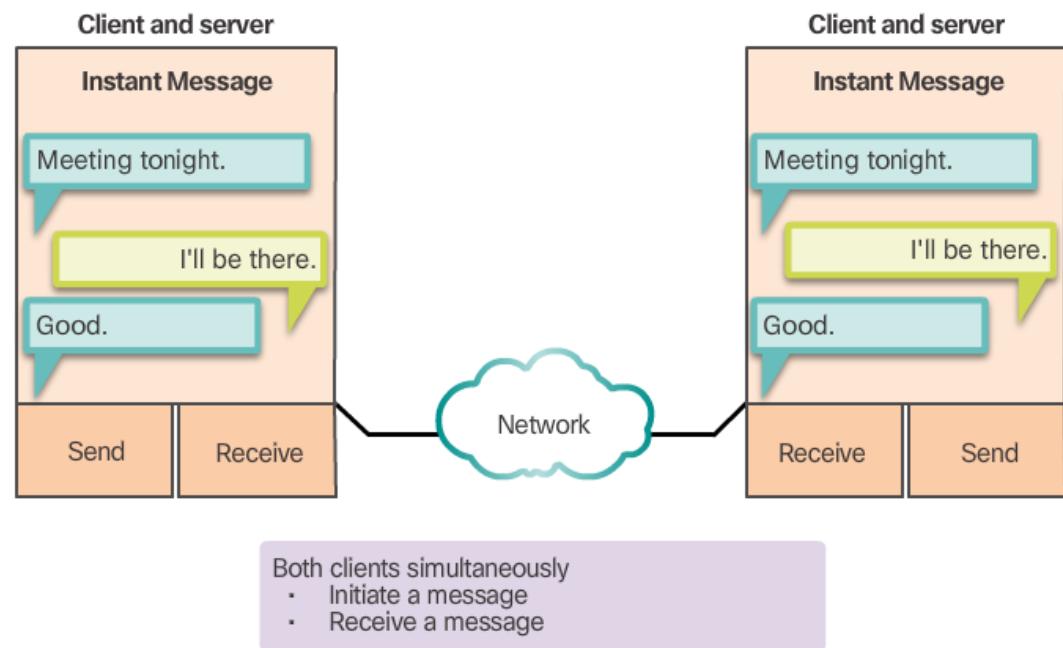
Peer-to-Peer Networks

- In the peer-to-peer (P2P) networking model, the data is accessed without the use of a dedicated server.
- Two or more computers can be connected to a P2P network to share resources.
- Every connected end device (a peer) can function as both a server and a client.
- The roles of client and server are set on a per request basis.



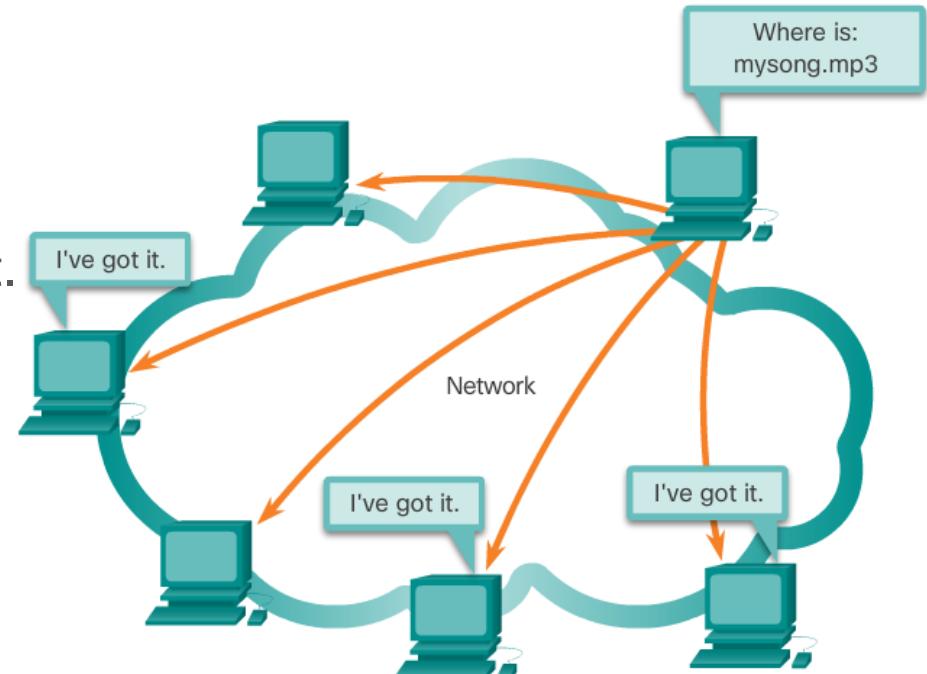
Peer-to-Peer Applications

- Some P2P applications use a hybrid system.
- In hybrid P2P, resource sharing is decentralized.
- Indexes that point to resource locations are stored in a centralized directory.
- In a hybrid system, each peer accesses an index server to get the location of a resource stored on another peer.



Common P2P Applications

- Common P2P networks include: eDonkey, G2, BitTorrent, Bitcoin.
- Many P2P applications allow users to share pieces of many files with each other at the same time.
- A small torrent file contains information about the location of other users and tracker computers.
- Trackers are computers keeping track of the files hosted by users.
- This technology is called BitTorrent.
- There are many BitTorrent clients, including BitTorrent, uTorrent, Frostwire, and qBittorrent.

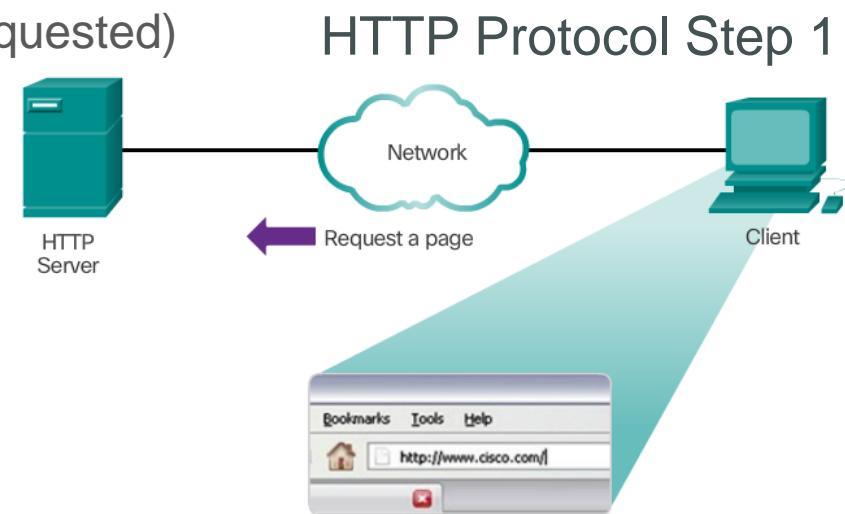


Section 2: Well-Known Application Layer Protocols and Services

Topic 2.1: Web and Email Protocols

Hypertext Transfer Protocol (HTTP) and Hypertext Markup Language (HTML)

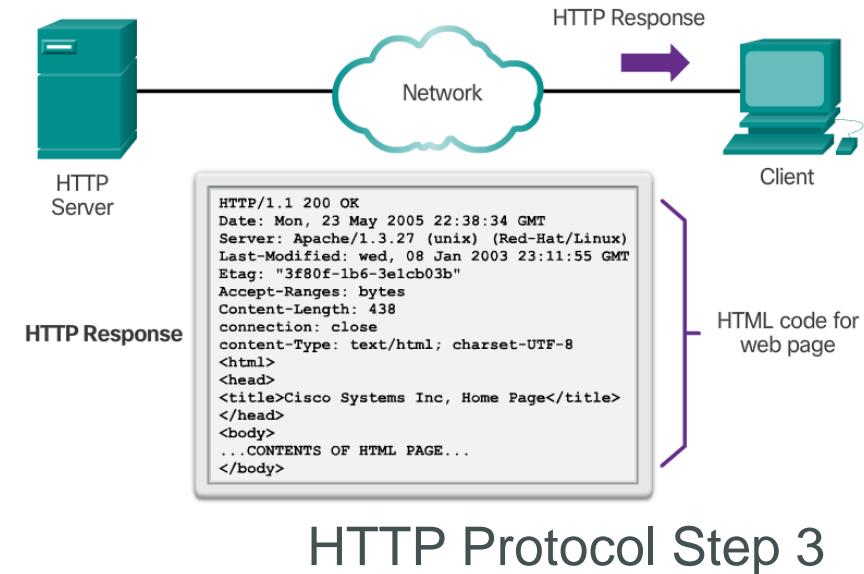
- A web address or uniform resource locator (URL) is a reference to a web server. A URL allows a web browser to establish a connection to that web server.
- URLs and Uniform Resource Identifier (URIs) are the names most people associate with web addresses.
- The URL <http://cisco.com/index.html> has three basic parts:
 - **http** (the protocol or scheme)
 - **www.cisco.com** (the server name)
 - **index.html** (the specific filename requested)
- Using DNS, the server name portion of the URL is then translated to the associated IP address before the server can be contacted.



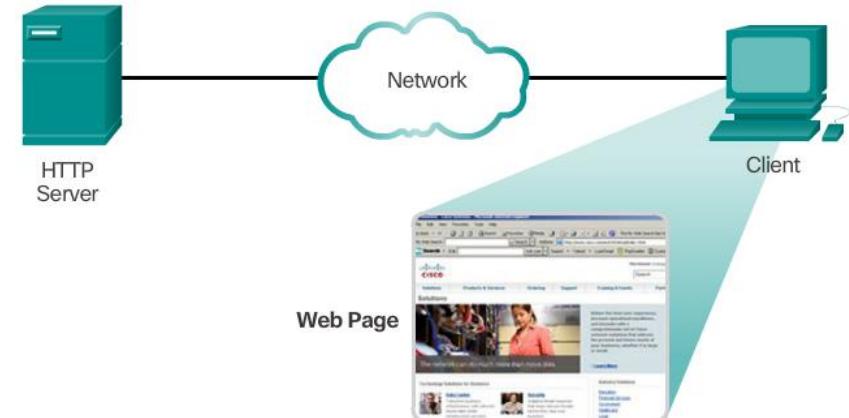
Hypertext Transfer Protocol (HTTP) and Hypertext Markup Language (HTML)

HTTP Protocol Step 2

- The browser sends a GET request to the server's IP address and asks for the **index.html** file.
- The server sends the requested file to the client.
- The **index.html** was specified in the URL and contains the HTML code for this web page.
- The browser processes the HTML code and formats the page for the browser window based on the code in the file.

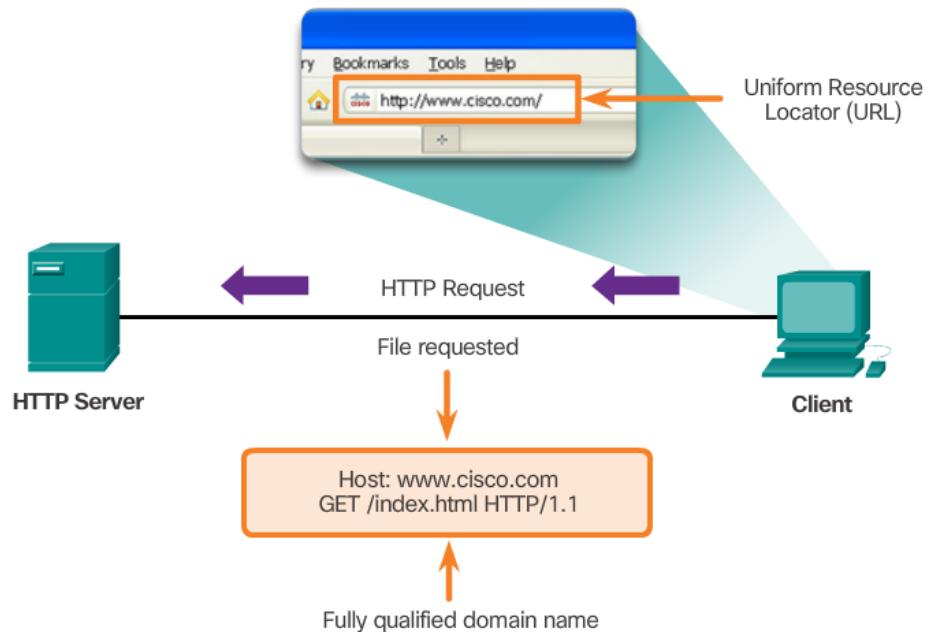


HTTP Protocol Step 3



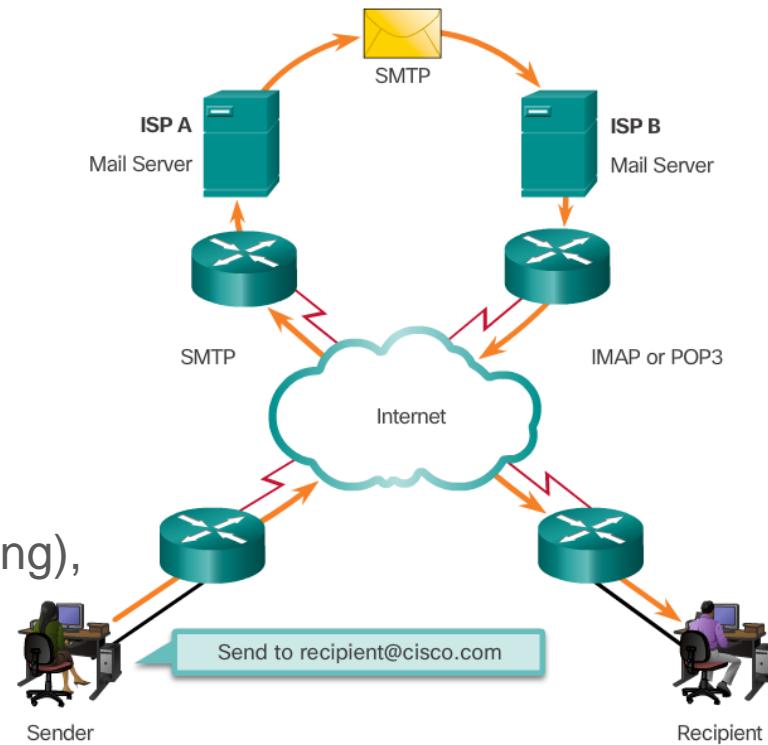
HTTP and HTTPS

- HTTP
 - Is a request/response protocol.
 - Has three common message types: GET, POST, PUT.
 - Is not secure. Messages can be intercepted.
- HTTPS uses authentication and encryption to secure data.



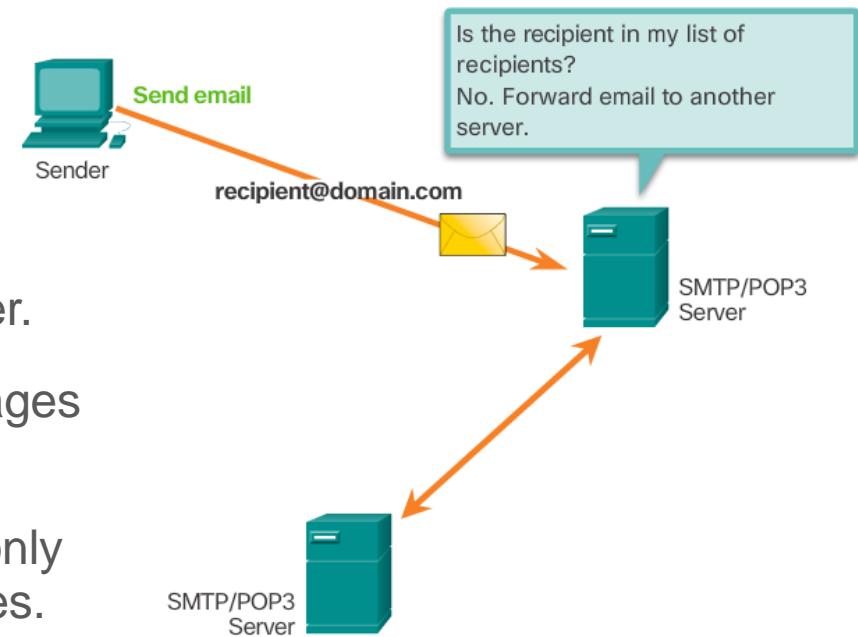
Email Protocols

- Email is a store-and-forward method of sending, storing, and retrieving electronic messages.
- Email messages are stored in databases on mail servers.
- Email clients communicate with mail servers to send and receive email.
- Mail servers communicate with other mail servers to transport messages from one domain to another.
- Email clients do not communicate directly when sending email.
- Email relies on three separate protocols for operation: SMTP (sending), POP (retrieving), IMAP (retrieving).



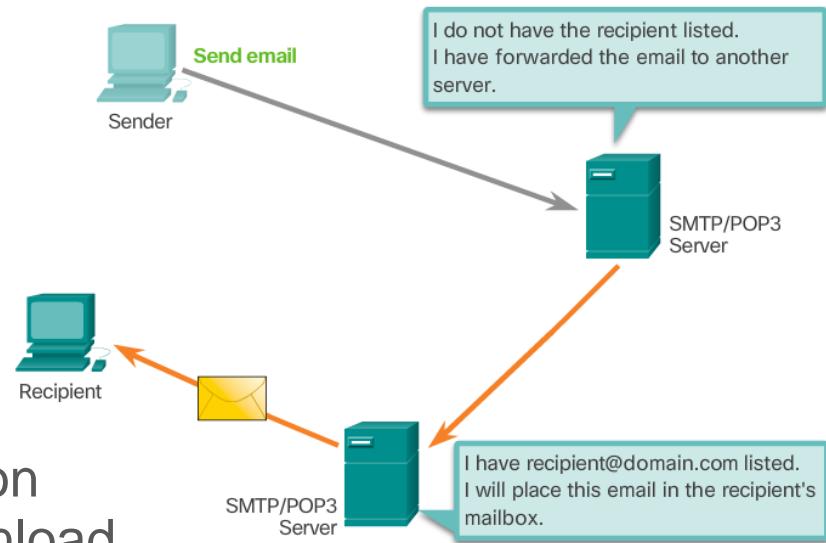
SMTP Operation

- SMTP message formats require a message header and body.
- The body can contain any amount of text.
- The header must have a properly formatted recipient email address and a sender address.
- An SMTP client sends an email by connecting to a SMTP server on port 25.
- The server receives the message and stores it message in a local mailbox or relays the message to another mail server.
- Users use email clients to retrieve messages stored on the server.
- IMAP and POP are two protocols commonly used by email clients to retrieve messages.



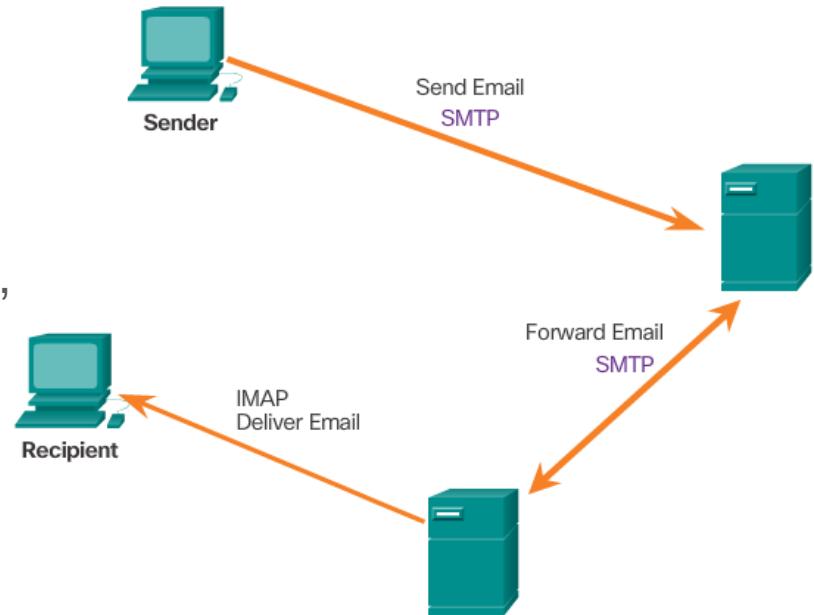
POP Operation

- Messages are downloaded from the server to the client.
- The server listens on port 110 TCP for client requests.
- Email clients direct their POP requests to mail servers on port TCP 110.
- The POP client and server exchange commands and responses until the connection is closed or aborted.
- POP allows for email messages to be downloaded to the client's device (computer or phone) and removed from the server.
- There is no centralized location where email messages are kept.
- A downloaded message resides on the device that triggered the download.



IMAP Operation

- IMAP is another protocol used to retrieve email messages.
- Allows for messages to be displayed to the user rather than downloaded.
- The original messages reside on the server until manually deleted by the user.
- Users view copies of the messages in their email client software.
- Users can create a folder hierarchy on the server to organize and store mail.
- That file structure is displayed on the email client.
- When a user decides to delete a message, the server synchronizes that action and deletes the message from the server.

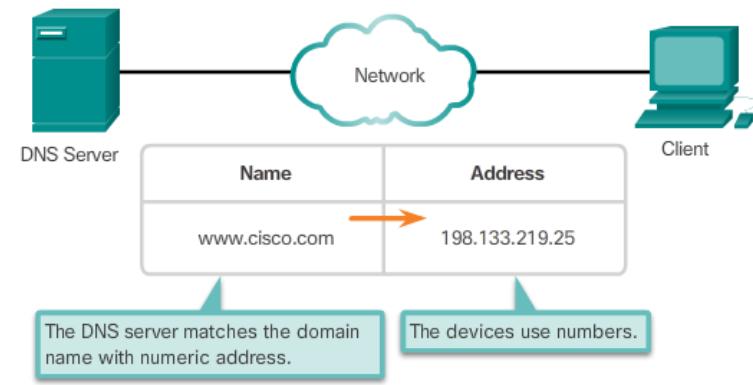
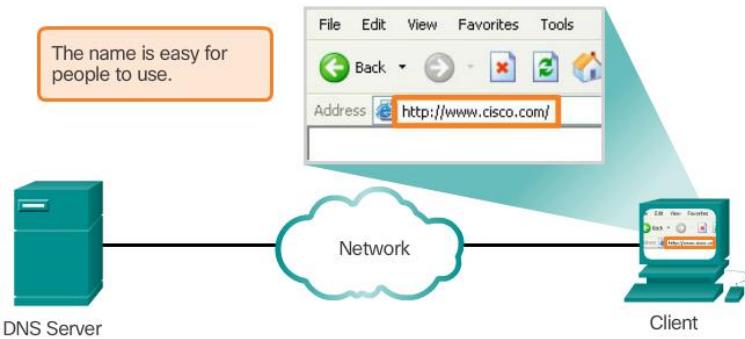


Topic 2.2: IP Addressing



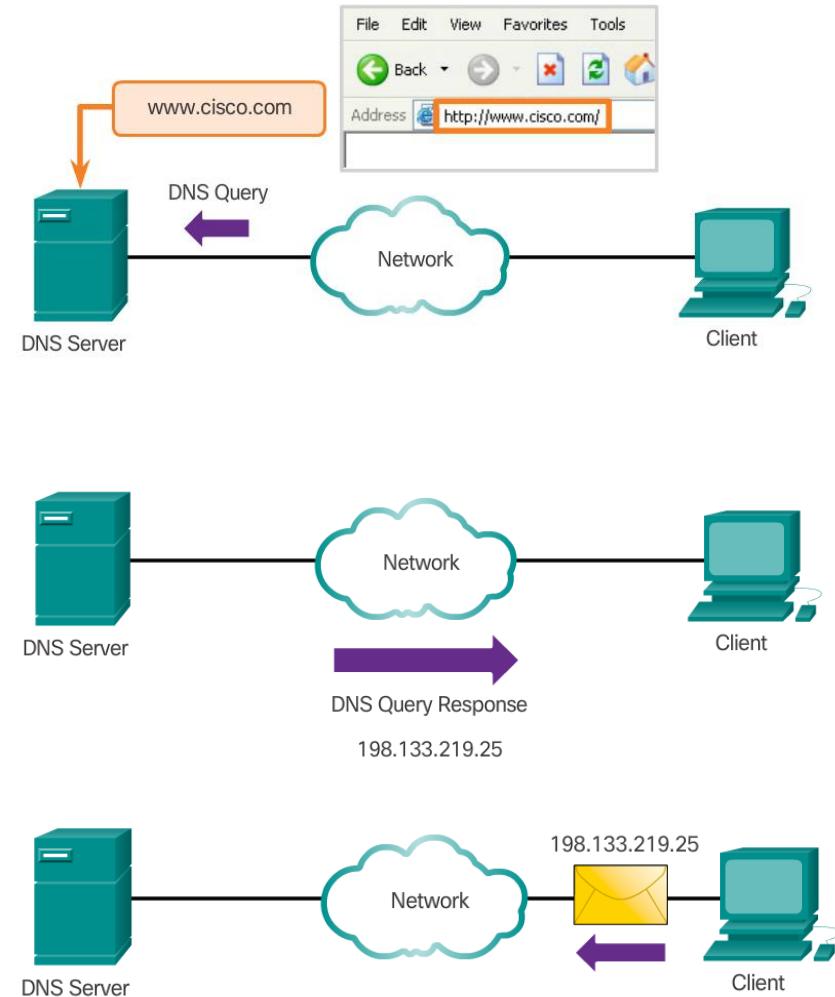
Domain Name Service

- While IP addresses are crucial for network communication, they are not easy to memorize.
- Domain names are created to make server addresses more user-friendly.
- Domain names such as <http://www.cisco.com> are user-friendly addresses associated with the IP address of a specific server.
- However, computers still need the actual numeric address before they can communicate.



Domain Name Service (cont.)

- The DNS protocol allows for the dynamic translation of a domain name into the correct IP address.
- The DNS protocol communicates using a single format called a message.

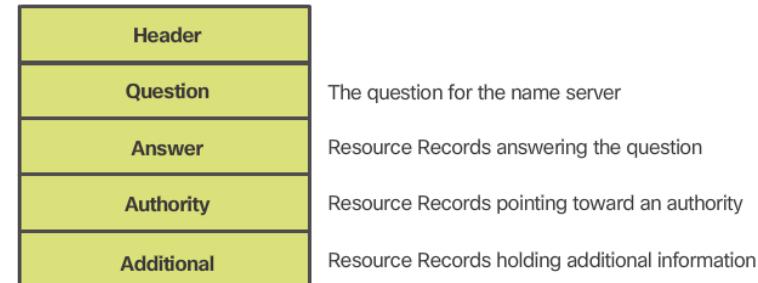


DNS Message Format

- DNS supports different types of records. Some of these record types are:
 - **A** - An end device IPv4 address
 - **NS** - An authoritative name server
 - **AAAA** - An end device IPv6 address (pronounced quad-A)
 - **MX** - A mail exchange record
- DNS servers will first look at its own records to resolve the name. If the server is unable to resolve the name using its locally stored records, it relays the query to other servers.
- The response is then forwarded to the requesting client.
- The DNS Client service on Windows PCs also stores previously resolved names in memory.
- **ipconfig /displaydns** displays all of the cached DNS entries on Windows.

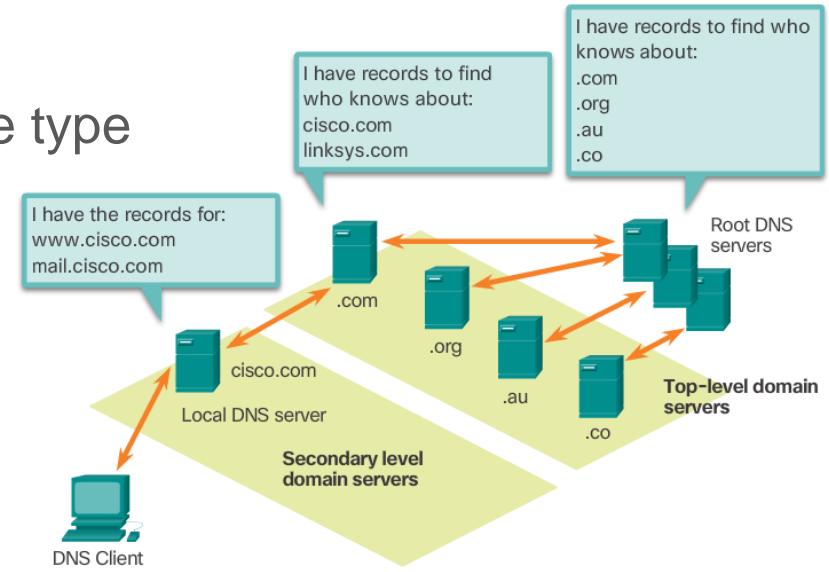
DNS uses the same message format for:

- all types of client queries and server responses
- error messages
- the transfer of resource record information between servers



DNS Hierarchy

- The DNS protocol uses a hierarchical system, with the root at the top and branches below. The naming structure is broken down into small, manageable zones.
- Each DNS server is only responsible for managing name-to-IP mappings for that small portion of the DNS structure.
- Requests for zones not stored in a specific DNS server are forwarded to other servers for translation.
- Top-level domains represent either the type of domain or the country of origin.
Examples of top-level domains are:
 - .com - a business or industry
 - .org - a non-profit organization
 - .au - Australia
 - .co - Colombia



The nslookup Command

- Allows the user to manually place DNS queries.
- It can also be used to troubleshoot name resolution issues.
- Has many options available for extensive testing and verification of the DNS process.

```
C:\WINDOWS\system32\cmd.exe - nslookup
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\bradfjoh>cd..

C:\Documents and Settings>nslookup
Default Server: dns-sj.cisco.com
Address: 171.70.168.183

> www.cisco.com
Server: dns-sj.cisco.com
Address: 171.70.168.183

Name: www.cisco.com
Address: 198.133.219.25

> cisco.netacad.net
Server: dns-sj.cisco.com
Address: 171.70.168.183

Non-authoritative answer:
Name: cisco.netacad.net
Address: 128.107.229.50

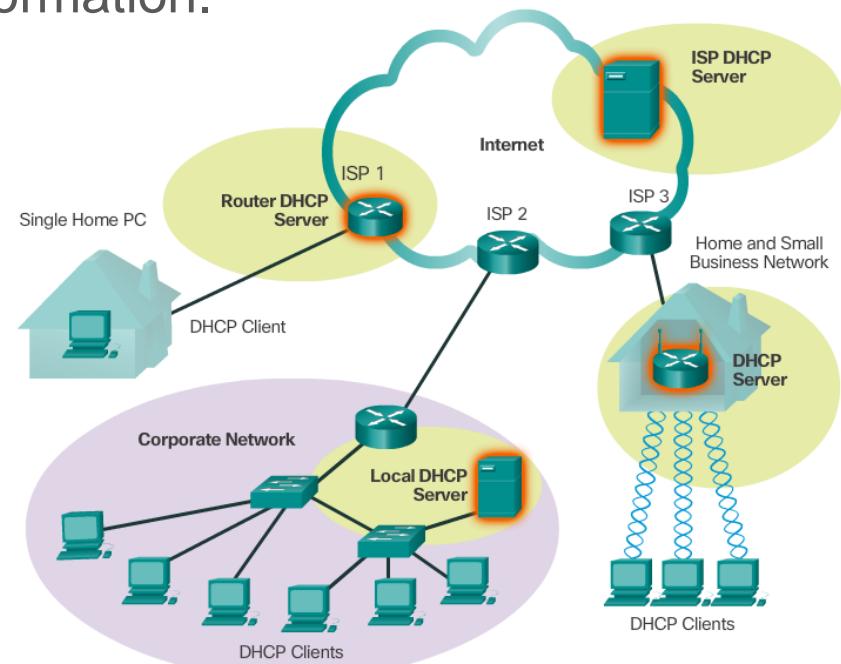
>
```

Topic 2.3: File Sharing Services



Dynamic Host Configuration Protocol

- Computers need network addresses to communicate over a network.
- Additional crucial information includes gateway address, subnet mask, and DNS server.
- Manually configuring end devices is not scalable. DHCP allows for automated distribution of network information.
- DHCP-distributed addresses are leased for a set period of time.
- Addresses are returned to the pool for reuse when no longer in use.
- DHCP supports IPv4 and DHCPv6 supports IPv6.



DHCP Operation

- A DHCP client goes through the following basic steps to request an IP:
 - The client broadcasts a DHCPDISCOVER.
 - A DHCP server replies with a DHCPOFFER message
 - The client sends a DHCPREQUEST message to the server it wants to use (in case of multiple offers).
- A client may also choose to request an address that it had previously been allocated by the server.
- The server returns a DHCPACK message to confirm the lease has been finalized.



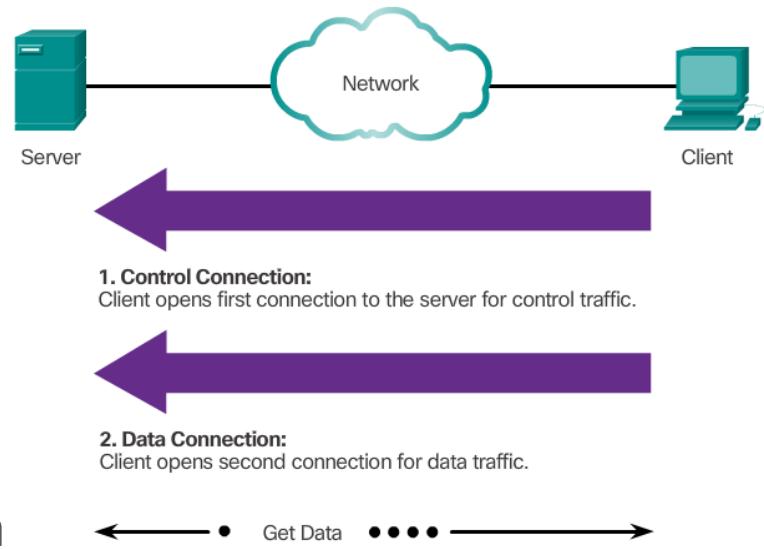
DHCP Operation (cont.)

- The server would respond with a DHCPNAK if the offer is no longer valid
- Leases must be renewed before its expiration through another DHCPREQUEST.
- DHCPv6 has a similar set of messages:
 - SOLICIT
 - ADVERTISE
 - INFORMATION REQUEST
 - REPLY



File Transfer Protocol

- FTP was developed to allow the transfer of files over the network.
- An FTP client is an application that runs on a client computer used to push and pull data from an FTP server.
- FTP requires two connections between the client and the server: one connection for commands and replies and another connection for the actual file transfer.
- The client initiates and establishes the first connection to the server for control traffic on TCP port 21.
- The client then establishes the second connection to the server for the actual data transfer on TCP port 20.
- The client can download (pull) data from the server or upload (push) data to the server.



Server Message Block

- SMB is a client/server file sharing protocol.
- All SMB messages share a common format.
- SMB file-sharing and print services have become the mainstay of Windows networking.
- Microsoft products now support TCP/IP protocols to directly support SMB resource sharing.
- After the connection is established, the user of the client can access the resources on the server as if the resource is local to the client host.
- The Mac, LINUX, and UNIX operating systems have their own implementation of SMB.

