Computer Networks

Lecture 1:

Introduction to the Course
and to the Domain of Computer Networks

What for Do We Learn the *Computer Networks*?

Basic course

- terminology
- reference models
- data transmission
  - problems
  - mechanisms
- communication protocols
  - those widely used in the Internet
  - their functionality
- administration & monitoring of network devices

Advanced courses

- programming communicating applications
- programming network devices
- network and systems security
- radio networking
- and others more specific

To be able to

- understand technical documentation
- talk with professionals
- to solve problems in network communication
- design a small network

Jobs

- network administrator
- network architect/designer
- communicating application developer
- network device designer/programmer
- security auditor

Plan of the Course

# hours	Subject
1	L1: Introduction to the course and to the domain of computer networks
2	L1&2: Basic terms and network reference models
2	L2&3: Review of today's network technologies
	Tutorial 1: Forwarding tables, transmission time
1	L3: Computer links (signals, coding, framing)
2	L4: Addressing (MAC, EUI, IPv4, IPv6, port numbers, DNS, URL)
	Tutorial 2: Bit coding, representation of IP addresses
1	L5: Packet transmission issues (fragmentation, reliability, network congestion)
	Tutorial 3: Frame synchronisation, error rate, CRC
2	L5&6: ARP, IPv4, ICMP, DHCP, IPv6
4	L6&7: Routing (taxonomy, mechanisms, protocols)
	Tutorial4: Routing tables
1	Test 1
2	L8: Queuing, scheduling, quality of service
2	L9: Ethernet

	Tutorial 5: Learning switch tables, Spanning Tree Protocol
2	L10: TCP
	Tutorial 6: TCP state machine, retransmissions, congestion control
1	L11: Other transport protocols (MTCP, UDP, RUDP, SCTP, RTP, Wireless TCP)
1	L11: DNS
2	L12: Multicast solutions
1	L13: MPLS, GMPLS
1	L13: Software Defined Networking
	Tutorial 7: Flow tables
1	L14: Network management
2	L14&15: Network security issues
1	Test 2

Supplementary Documents

Lecture slides

- S3-Other_LANs_2h — Token Ring, Token Bus, WiFi
- S6-Pictures-of-routers
- S10-BSD_sockets_1h
- S11-Application_protocols_4h — TFTP, FTP, HTTP, Electronic mail protocols

Tutorial slides

- T1-Forwarding_transmission-time
- T2-Bit-coding_IP-addresses
- T3-FrameSync_BitErrors_CRC
- T4-Routing
- T5-Switch-tables_STP
- T6-TCP
- T7-Flow_tables

Grading and Evaluation

There will be

- 2 tests – max. 20 points for each
- 10 laboratory exercises – max. 6 point for each

The maximum score is 100 points

Who reaches more than 90 points can classify ECONE without writing the exam

There will be 2 exams

- If you write two of them, then the second result will overwrite the first one
- The final score is: exam_points + 0.5 * semester_points

To classify ECONE:

- more than 50 points as the final score **and**
- at least 37 points from laboratory exercises

Final score	Mark
< 50	2
51 - 60	3
61 -70	3.5
71 - 80	4
81 -90	4.5
91 - 100	5

Bibliography

1. Peter Dordal, *An Introduction to Computer Networks*, Loyola University Chicago (2014). https://open.umn.edu/opentextbooks/textbooks/353
2. Olivier Bonaventure, *Computer Networking: Principles, Protocols and Practice*, Universite catholique de Louvain (2011). https://open.umn.edu/opentextbooks/textbooks/computer-networking-principles-protocols-and-practice
3. L. Peterson, B. Davie, *Computer Network: A Systems Approach*, 5th Edition, Elsevier (2011). http://booksite.elsevier.com/9780123850591/index.php
4. D. U. Comer, *Internetworking with TCP/IP,* 6th Edition, Pearson (2014).
5. D. U. Comer, *Computer Networks and Internets,* 6th Edition, Pearson (2015).
6. J. F. Kurose, K. W. Ross, *Computer Networking A top-Down Approach Featuring the Internet*, 6th Edition, Addison Wesley (2012).
7. W. R. Stevens, *TCP/IP Illustrated*, Volume 1, *The Protocols*. Addison Wesley (2011).
8. A. S. Tanenbaum, D. J. Wetherall, *Computer Networks*, 5th ed. Prentice Hall (2011).

What Is a Computer Network?

It is a digital telecommunications network that allows nodes

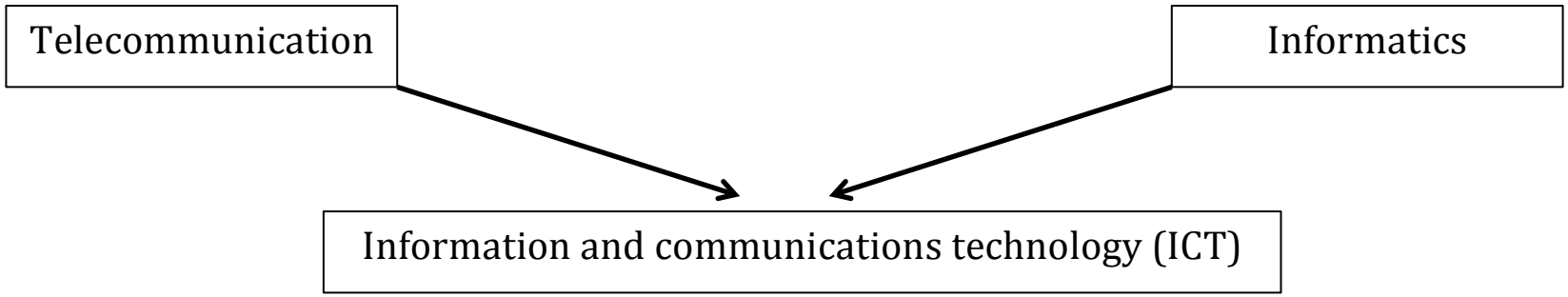
- to exchange information
- to share resources
- to cooperate

The traditional telecommunication – was about signals

The modern telecommunication – is about transmission of

- signs and signals
- messages
- words and writings
- images and sounds
- information of any nature

by wire, radio, optical or electromagnetic systems



Summary

The lecture

- points the knowledge you should master
- explains techniques you should understand

You should

- learn and repeat
- discuss the issues

There are questions at the end of each lecture slides

use them for repetitions ☺

Questions

1. What is a computer network?
2. What is it ICT?
3. What for do we learn the computer networks?
4. What jobs can you do if you master the computer networks?

Computer Networks

Lecture on

Basic Terms and Network Reference Models

Plan of This Lecture

- Communication issues
- Network classifications
- Network **r**eference **m**odels
  - ISO OSI RM
    International **O**rganization for **S**tandardization, **O**pen **S**ystems **I**nterconnection
  - TCP/IP RM
    Transport **C**ontrol **P**rotocol/ **I**nternet **P**rotocol
  - IEEE LAN/MAN RM
    Institute of **E**lectrical and **E**lectronics **E**ngineers

Communication Issues

The communicating nodes have to know or agree on

- what they want to do
- what they can
- what information they are going to exchange
- what is the coding (representation) for transmission
- how to synchronise their activities

An item of information

- is something abstract
- has semantics and structure
- can have many representations –on different machines, on storage, on transmission channel
- can have metadata

Communication between nodes has to

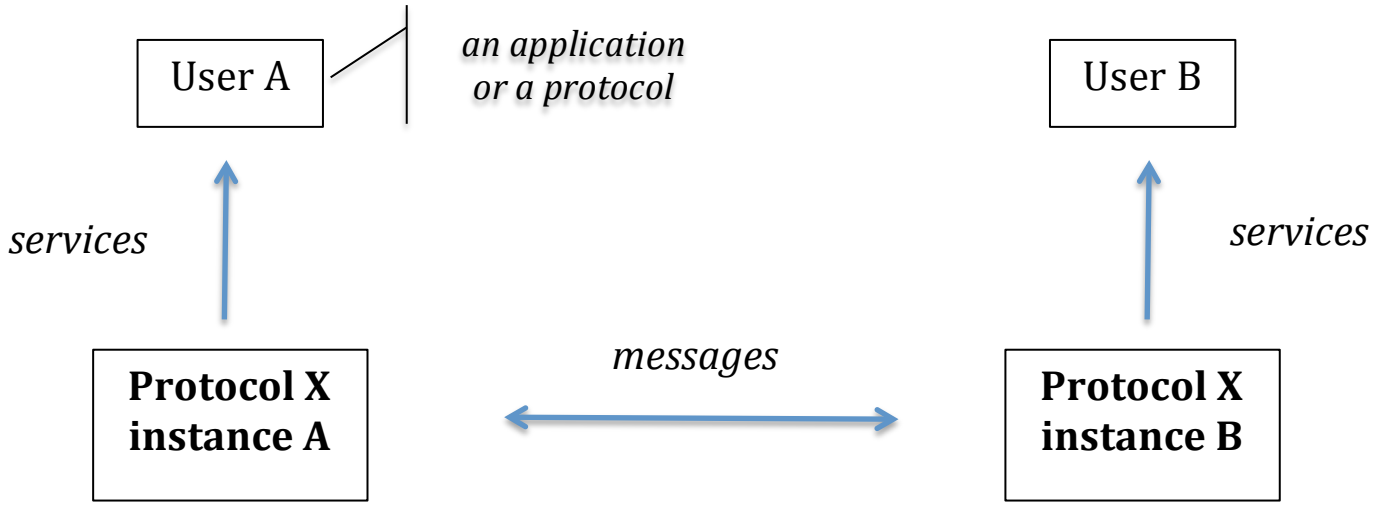
- tolerate transmission errors
- recover from node's failures
- adapt to network capabilities (speed, delay, jitter, availability, error rate)

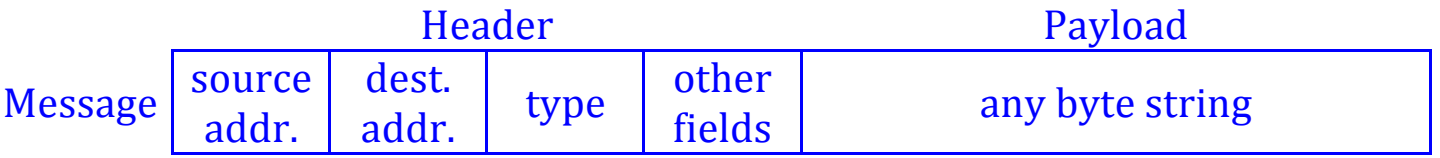
To enable communication – standard rules must be defined

A communication protocol

A **communication protocol** is a system that realizes a set of rules,
which governs cooperation between autonomous entities

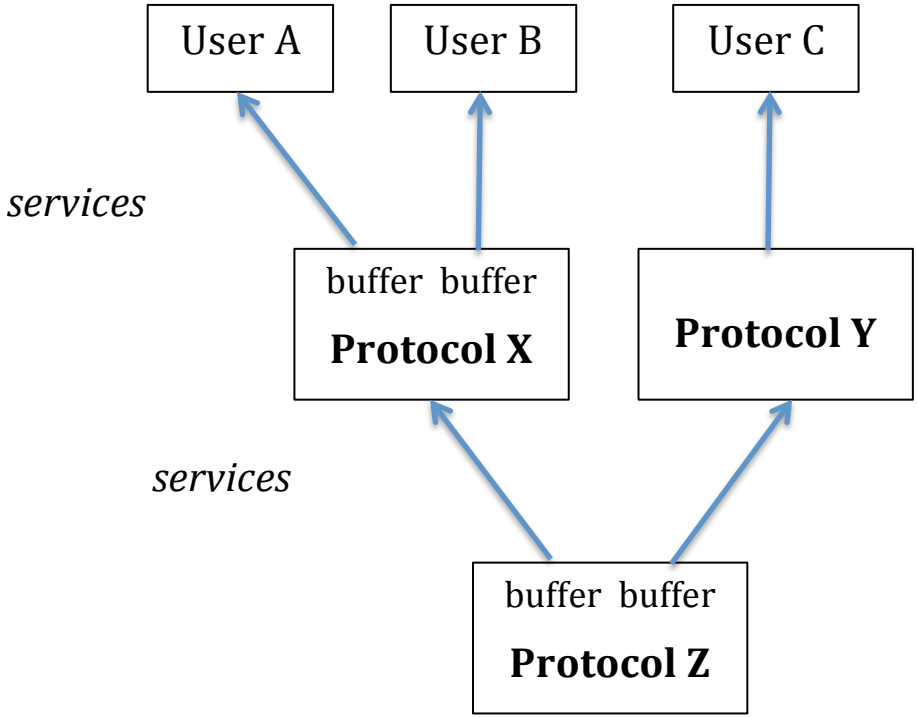
To deal with complex problem – we split it to sub-problems – here to different protocols





Protocol service multiplexing

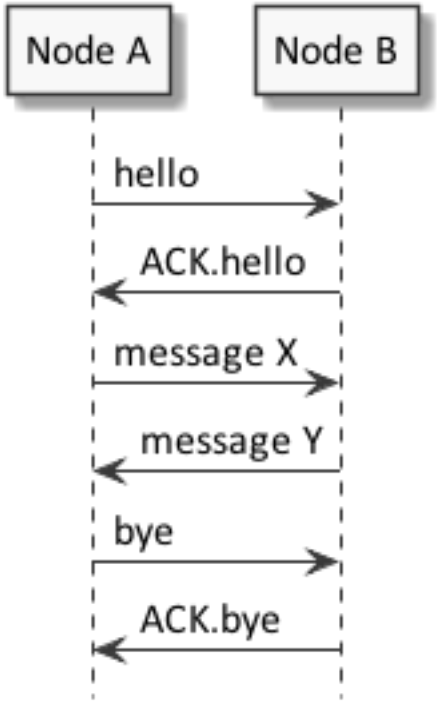
Provided by **X** and **Z** on this example:



Connection-Full & Connectionless Communication

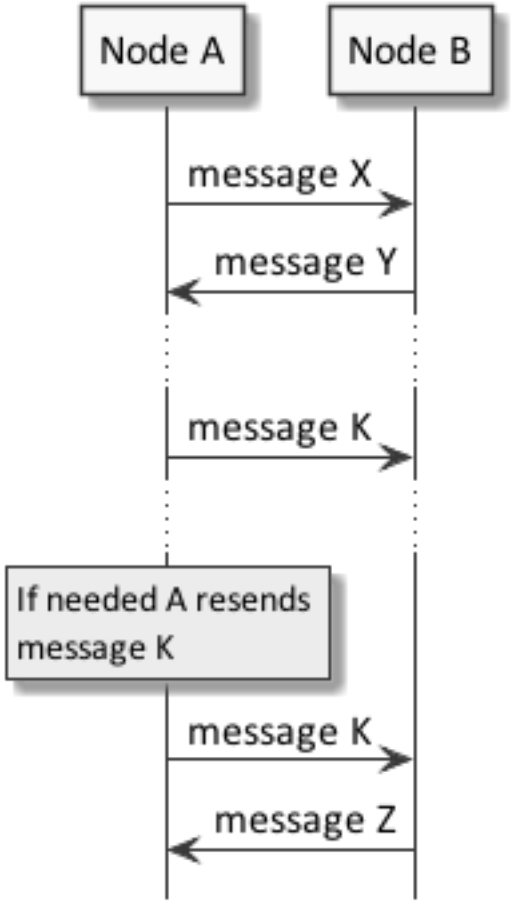
- Connection full, can be:
  - reliable
  - unreliable

  Provided by X.25, Frame Relay, ATM

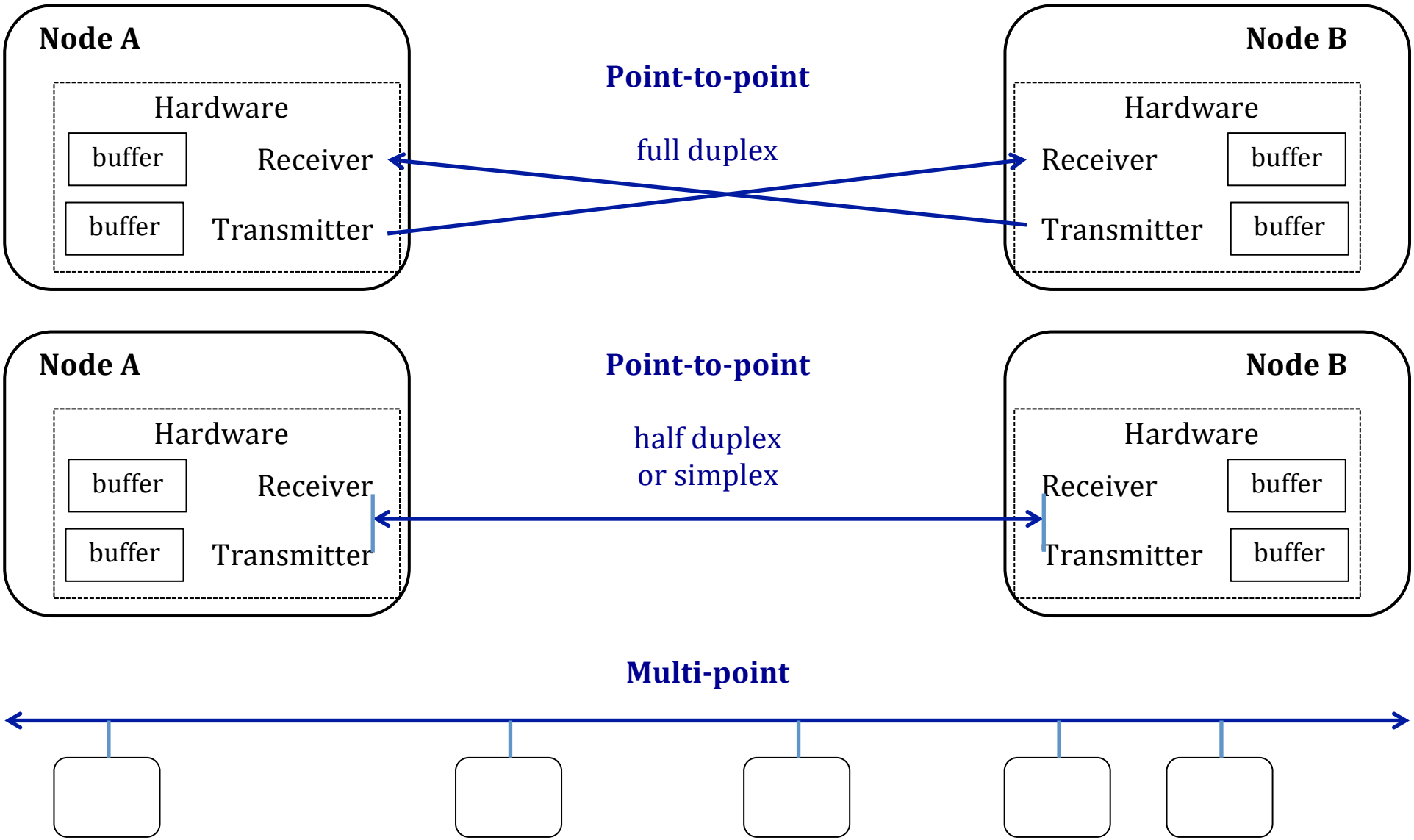


- Connectionless, can be:
  - reliable
  - unreliable

  E.g. Internet protocol



Simplex & Duplex Links



Link Rate, Bandwidth, Throughput and Goodput

Link Rate ≡ Data Rate

– the rate at which bits are transmitted

Throughput

– the overall effective transmission rate,
taking into account things like transmission overhead & protocol inefficiencies

- usually in kilo (10^3), mega (10^6) or giga (10^9) bits per second – kb/s, Mb/s, Gb/s

Bandwidth

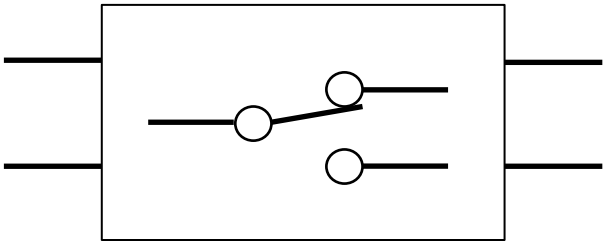
– depending on author or context, can be link rate or throughput

Goodput

– the amount of usable data delivered to the receiving application

- usually in Kilo (2^{10}) or Mega (2^{20}) bytes per second – kB/s, MB/s
- rarely in kilo (10^3) or mega (10^6) bytes per second – kB/s, MB/s

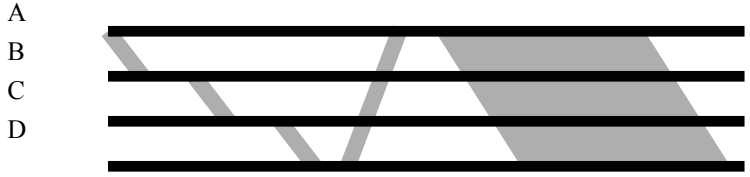
Switching



Switch types

- direct connection (galvanic, capacitive or inductive coupling, mirrors for light beams)
- TDMA – Time Division Multiple Access
- FDMA – Frequency Division Multiple Access
- packet switching

Circuit Switching



e.g. traditional telephone communication

Efficient for:

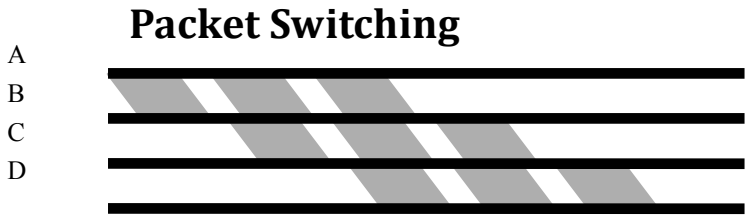
- real time applications
- large chunk data transfer

Message Switching

e.g. email

- short messages transfer

Packet Switching



e.g. IP

- any kind of messages

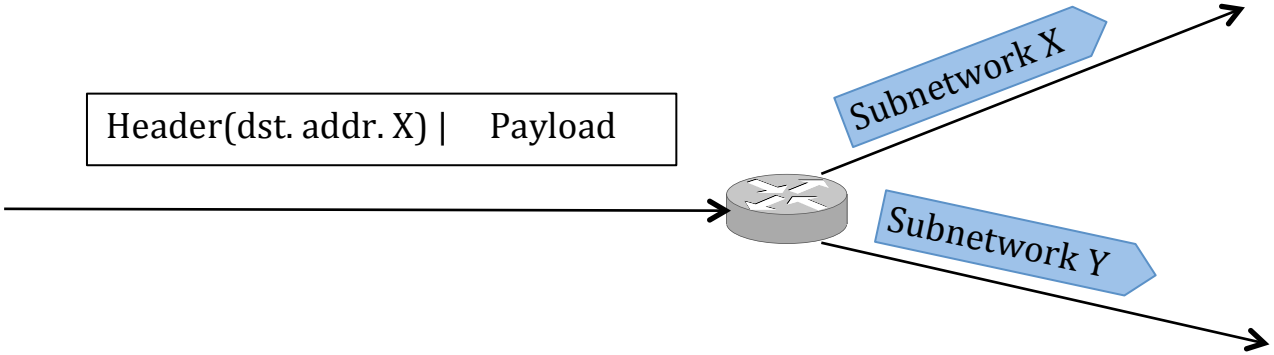
Efficient usage of network links!

Permanent Virtual Circuits
– predefined path in a packet network

e.g. X.25, Frame Relay, ATM

- for real time applications e.g. live video streams

Datagram Packet Switching



Every sent packet contains a destination address

Advantages

- simple implementation
- efficient for short data exchanges

Disadvantages

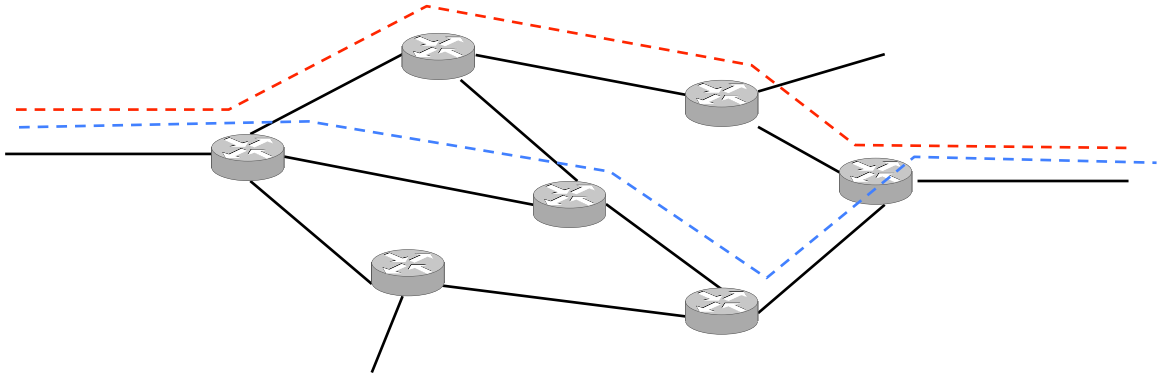
- destination addresses are long due to the number of possible destinations
- switch should process the address to find output queue for every packet !

IP routers apply this method

Virtual Circuit Packet Switching

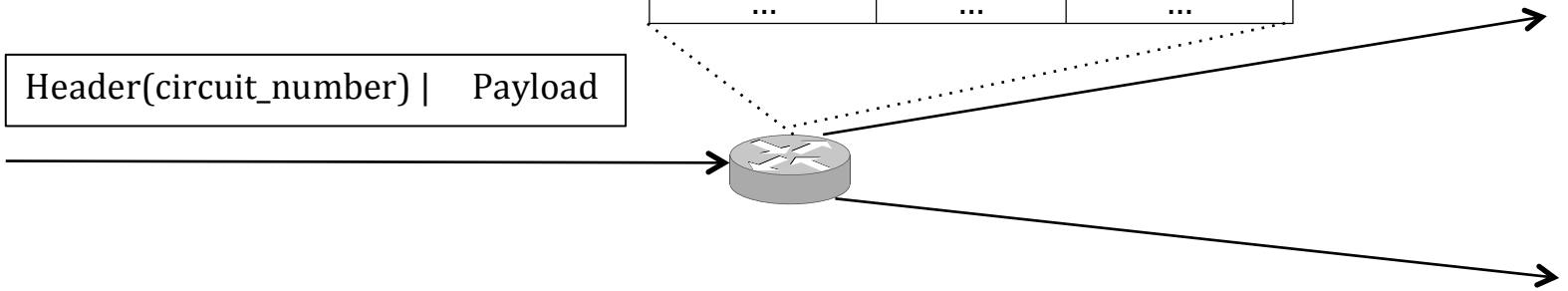
Every data packet contains a circuit number

The circuits are set before transmission of data packets



Index of attributed bandwidth on the output port

Input Circuit_Num	Output port	Output Circuit_Num
1	1	5
2	1	3
3	2	1
...	...	...



The circuit can be set

- When a terminal starts the communication session
  - Connect_request message creates the circuit
  - Connect_confirmation message confirms it
- Permanently by network admin

Advantages

- circuit number are short – due to limited number of circuits over one interface
  - the number points information in circuit table – fast forwarding
  - packet header is short – efficient payload / packet length ratio
- efficient for long data exchanges
- possible to guarantee bandwidth and delays for connections

Disadvantages

- complex implementation

X.25, Frame Relay, ATM switches apply this method

Addressing

Unicast

- only one destination node

Multicast

- group of destination nodes
- all of them should obtain the messages

Anycast

- group of destination nodes
- one of them should obtain the messages

Broadcast

- every node in the network should obtain the messages

The sender is always distinguished by its unicast address

Fragmentation & Grouping

Fragmentation

- Every network and link limits max. message size
- Too big message must be fragmented
- Recipient defragments the message

Grouping

- Messages can be grouped to optimise communication cost or time
  - e.g. telephone dial-up connections
  - e.g. satellite links between ground stations
- Sender groups the messages
- Recipient regroups them

Network Classifications

By coverage

- WAN – Wide Area Network
- MAN – Metropolitan Area Network
- LAN – Local Area Network
- PAN – Personal Area Network

By types of communication medium

- wireless – radio, optical, acoustic
- wired – optical, electrical

By mobility

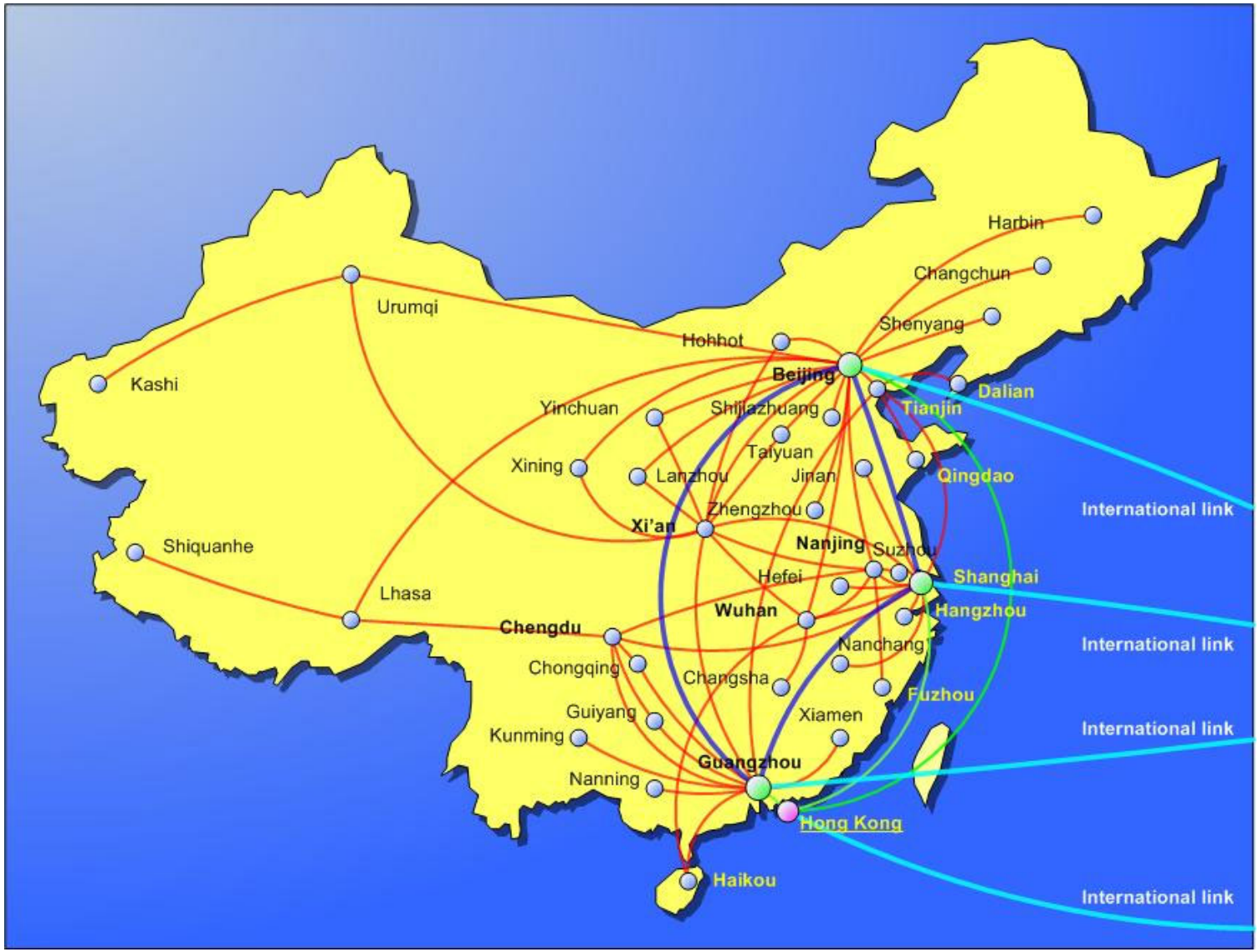
- fixed
- mobile

By topology

- star
- bus
- ring
- mesh
- tree

- Nanoscale
- NFC – Near-field
- BAN – Body
- PAN – Personal
- NAN – Near-me
- LAN – Local
  - HAN – Home
  - SAN – Storage
  - WLAN – Wireless
- CAN – Campus
- Backbone
- MAN – Metropolitan
- WAN – Wide
- IAN – Cloud (Internet area network)
- Internet
- Interplanetary Internet

WAN example: ChinaNet



Source: www.ctamericas.com/resource/chinanet-network-map/chinanet-network-map-2

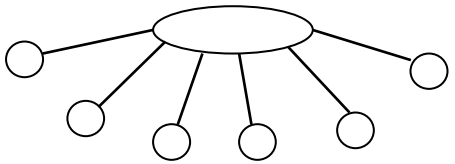
Topology

Distinguish!

- Physical (tubes) topologies
- **Signal topologies**
- Logical topologies

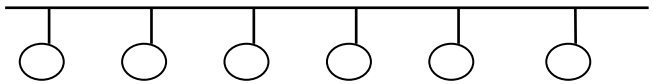
Star

- Size limited by efficiency of the main node
- Easy implementation and management
- Reliability of the main node!
- Time consuming broadcast



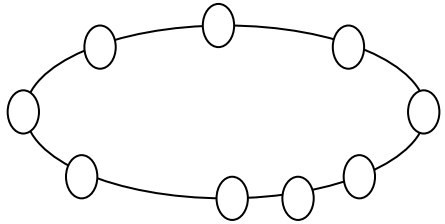
Bus

- Network size limited by the bus throughput
- Broadcast is very fast



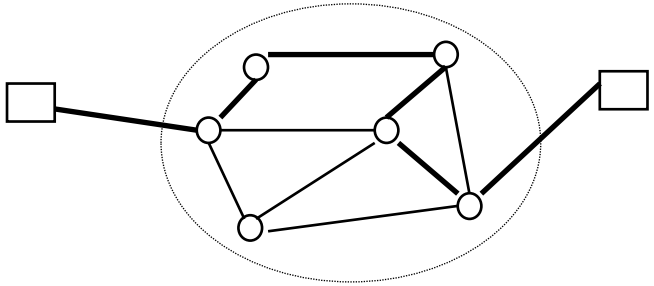
Ring – Nodes retransmit a received stream of bits

- Congestion resistant
- Easy management
- Sensible for a node failure



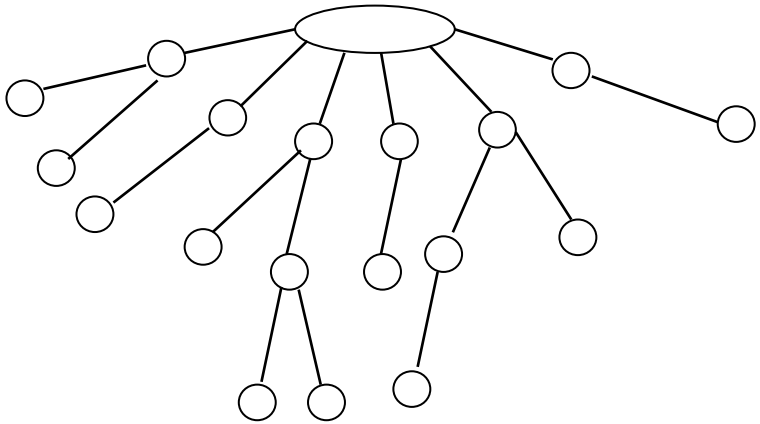
Mesh

- Good reliability
- Possibility of load balancing – for congestion reduction
- Routing problems



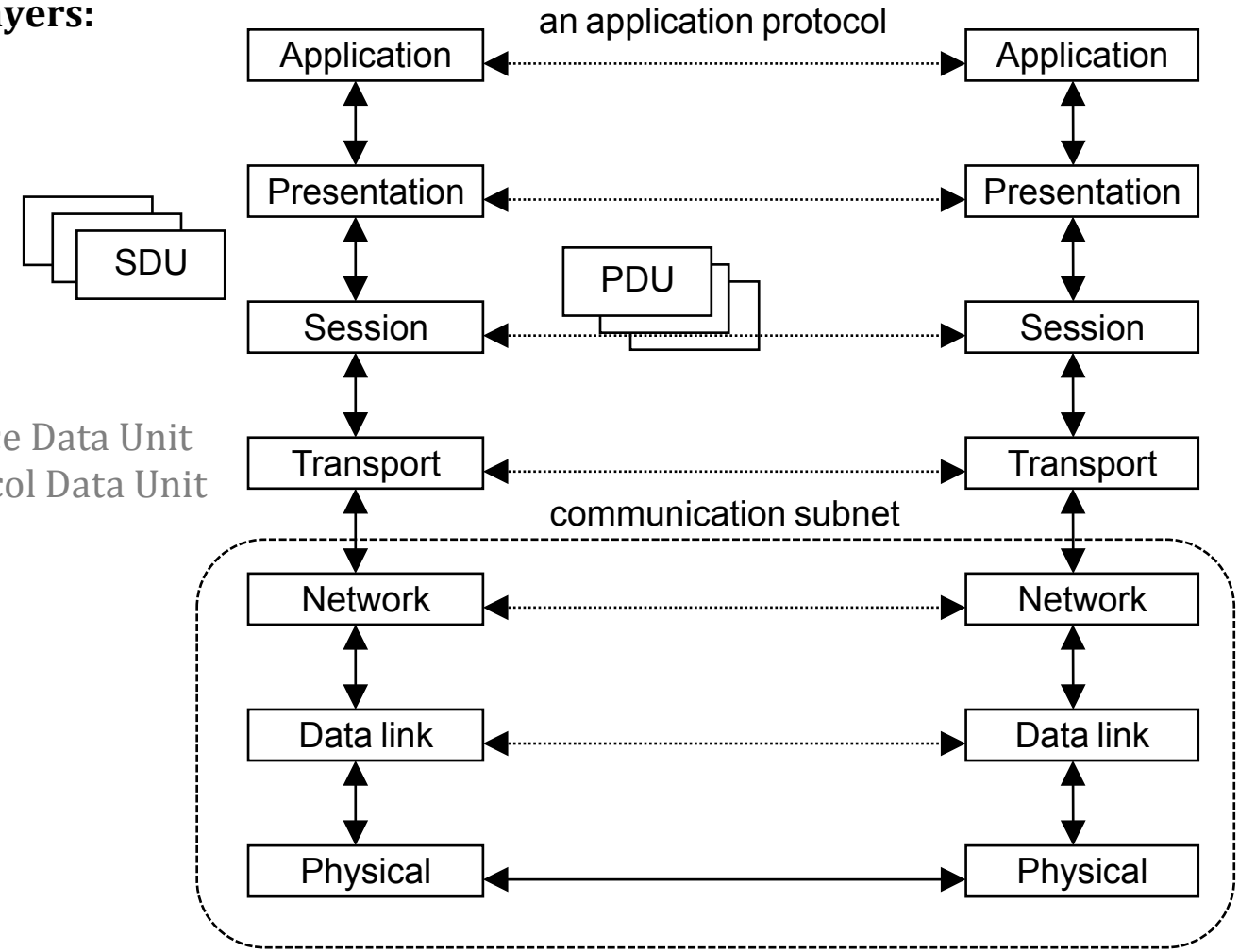
Tree – Hierarchical distribution of transmission control

- Relatively easy management
- Risk of root node congestion



ISO 7498, Open Systems Interconnection Reference Model

7 protocol layers:



SDU – Service Data Unit
PDU –Protocol Data Unit

L4-7 messages
L3 packets
L2 frames
L1 signals

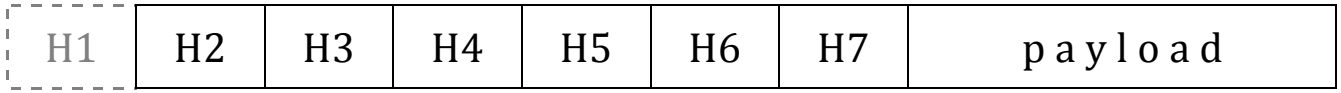
OSI defines:

- Functionality of communication protocols for every layer
- Rules of naming, description and co-operation between layers

OSI does not define:

- Any implementation aspects

Headers encapsulation:



Examples of ISO protocols and not ISO:

L7 FTAM, DTP, X.400, X.500, Virtual Terminal
L6 ISO Presentation Protocol
L5 ISO Session Protocol
L4 ISO TP4, TCP, UDP
L3 ISO Network Protocol, IPX, IP
L2 HDLC, Ethernet, Wi-Fi
L1 RS-232, RS-485

Protocol Functionalities

1. Physical Layer

- mechanical, electrical details
- coding, signals

2. Data link Layer

- bit, frame synchronization
- bit error detection/correction
- control of data flow

3. Network Layer

- node addressing
- multiplexing of higher layer data streams
- fragmentation, defragmentation
- grouping, regrouping
- network and users administration
- error detection/correction
- control flow

4. Transport Layer

- transport addressing
- connection quality negotiation
- fragmentation, defragmentation
- grouping, regrouping
- error detection/correction, control flow

5. Session Layer

- synchronization points
- activity management

6. Presentation Layer

- data context negotiation
- data translation: host-network representation
- compression, ciphering

7. Application Layer

- email, file transfer
- distributed transactions
- directory services
- …

TCP/IP Reference Model

<table>
<tr><th>TCP/IP model</th><th>ISO model</th><th colspan="2">Example protocols</th><th></th></tr>
<tr><td rowspan="3">Application</td><td>L7</td><td>NFS</td><td rowspan="3">Telnet, FTP, SMTP, DNS, …</td><td rowspan="3">user processes</td></tr>
<tr><td>L6</td><td>XDR</td></tr>
<tr><td>L5</td><td>RTP</td></tr>
<tr><td>Transport</td><td>L4</td><td colspan="2">TCP, UDP, …</td><td rowspan="2">kernel modules</td></tr>
<tr><td>Internet</td><td>L3</td><td colspan="2">IP, ICMP, RIP, …</td></tr>
<tr><td>Network Interface</td><td>L1, L2</td><td colspan="2">Ethernet, PPP, Wi-Fi, …</td><td>hardware drivers</td></tr>
</table>

TCP/IP is a shortcut for a bunch of related protocols

Network devices

L1 ÷ L7	gateway	
L1 ÷ L3	router	(intermediate system – in ISO standards) (gateway – in many IETF documents)
L1, L2	bridge	– can translate a frames of different L2 protocols
L1	hub	_ can be passive or active
L1	signal amplifier	
L1	cross-panel	
?	switch:	

- layer 2 switch
- layer 3 switch
- layer 4 switch
- layer 7 switch

– layer X address determines the output

Layer 2 switch – process and forward data at the data link layer

Layer 3 switch

- can be a hardware switching router (CISCO definition)
- can by just a router
- can combine switching in layer 2 and 3

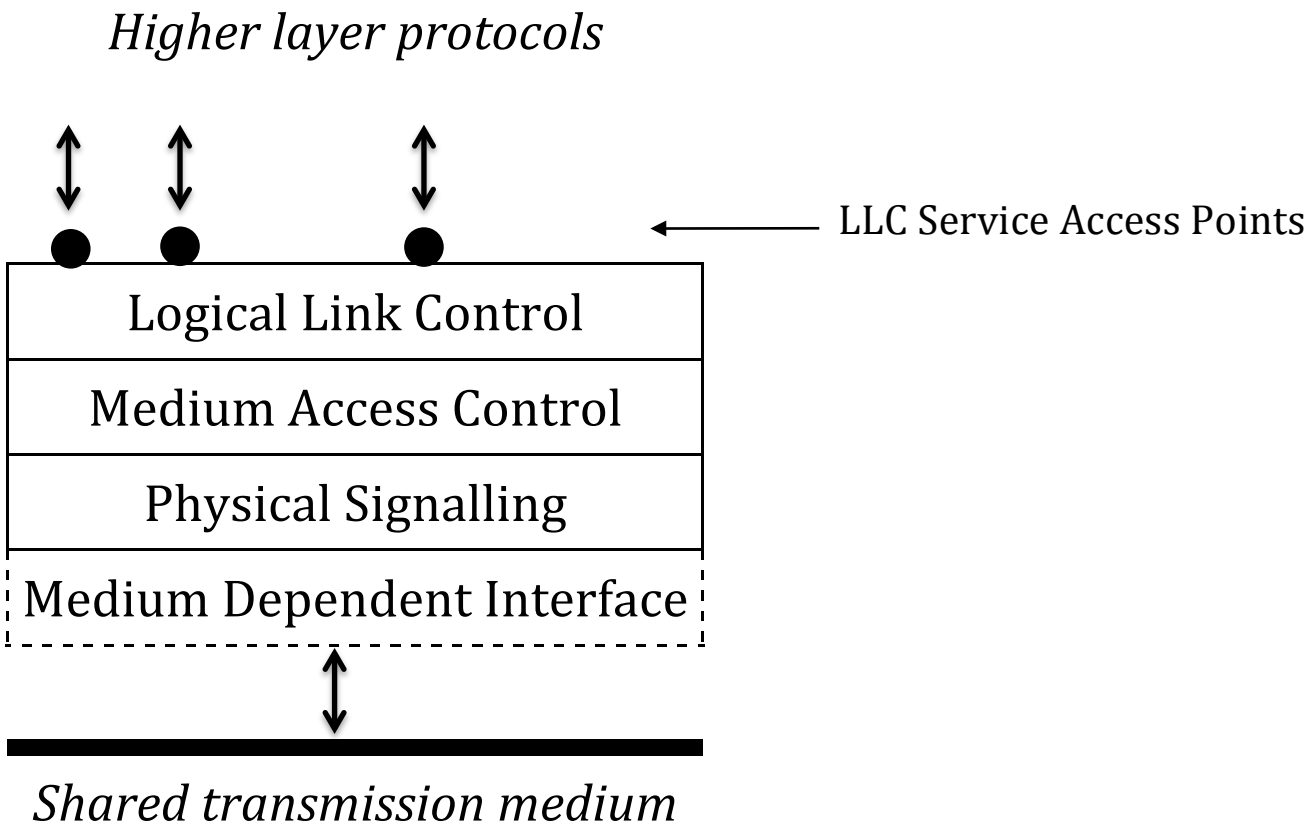
Layer 4 switch can

- perform network address translation
- perform load distribution – depending on layer 4 address
- combine a firewall
- support VPNs

Layer 7 switch can

- perform load distribution – depending on layer 7 address
  based on uniform resource locators (URLs)
- support WWW caching
- support content delivery network

IEEE 802.1, LAN/MAN Reference Model

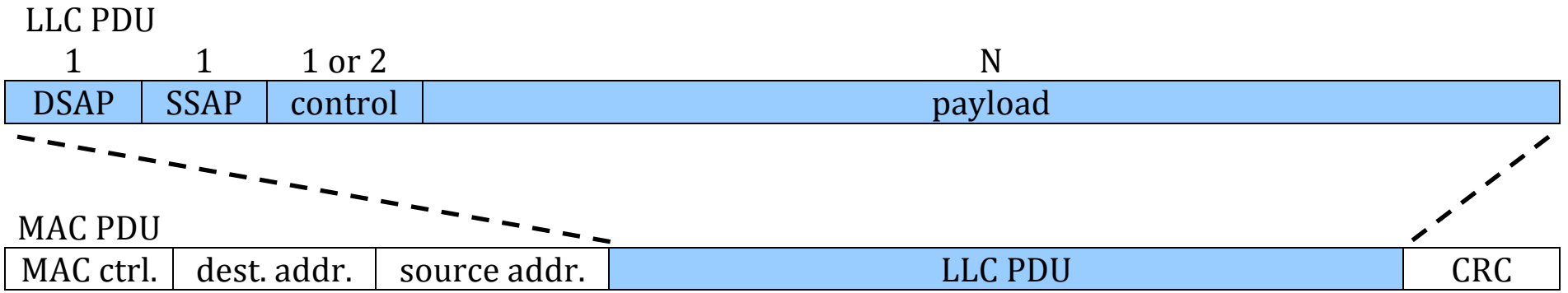


Logical Link Control Protocol

- Common interface independent from different MAC protocols

  Medium Access Control

- Data streams multiplexing
- Control flow for every SAP *Service Access Points*
- Duplicated and lost frames treatment



Summary

- Communication issues
  - Communication protocol
  - Connection-full & connectionless communication
  - Simplex, half-duplex, full-duplex links
  - Link rate, bandwidth, throughput and goodput
  - Switching
    - Datagram packet switching
    - Virtual circuit packet switching
  - Types of addresses
  - Message fragmentation & grouping
- Network classifications
  - by coverage area
  - by topology
- Network **r**eference **m**odels
  - ISO OSI RM
  - TCP/IP RM
  - IEEE LAN/MAN RM

Questions

1. What is a communication protocol?
2. Why throughput can be lower than link rate of the same communication channel?
3. Can we set a full duplex communication over a multi-point link?
4. What means circuit switching?
5. What means packet switching?
6. In which case packet switching is more efficient than message switching?
7. What are virtual circuits in packet networks?
8. What is the meaning of unicast, mulicast, anycast and broadcast?
9. What is the reason for packet fragmentation?
10. What is the reason for packet grouping?
11. Characterize different network topologies.
12. What is the topology of a simple broadcasting radio network?
13. List the principal functions of all OSI ISO protocol layers.
14. Characterize the layers defined by the TCP/IP protocol stack model.
15. What is the difference between the 2nd layer switch and the 3rd layer switch?
16. In which ISO OSI layers do the devices: hub, bridge, router, switch, gateway, firewall work?
17. Characterize Local & Metropolitan Area Network Reference Model defined by IEEE.
18. What are the functions of Logical Link Control layer?
19. What are the functions of Medium Access Control layer?

Computer Networks

Lecture on

Review of Today's Network Technologies

Plan of This Lecture

- Word Wide Web
- Internet
- Other WAN technologies
- Access networks
- Passive networks
- Wavelength-Division Multiplexing
- Special purpose networks

Word Wide Web

- Is an information space where documents and services – called resources
  - are identified by Uniform Resource Locators (URLs)
  - are interlinked by hypertext links
- Works over the Internet – precisely over the Hypertext Transfer Protocol (HTTP)
  - for security HTTPS – i.e. HTTP over Transport Layer Security (TLS) protocol
- Is standardised by Word Wide Web Consortium (W3C)

The W3C standards define a collection of technologies for application development

- Web Design and Applications – for building and Rendering Web pages
- Web of Devices – to enable Web access anywhere, anytime, using any device
  - e.g. mobile phones, interactive television, automobiles
- Web Architecture
- Semantic Web
- Web of Services
- Browsers and Authoring Tools

Internet

Interconnected networks or internetwork – origin of the term “internet”

Next the Internet protocol was standardised (1982)

The Internet – a global public network where devices communicate over the Internet protocol (IP)

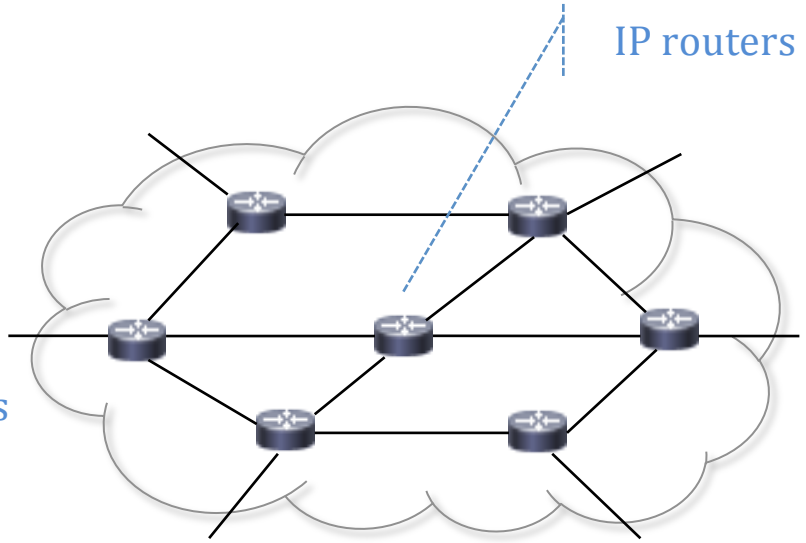
- A proper noun – to distinguish it from other public WANs
- An internet – a common noun as a computer communication medium, like radio, television
- See: en.wikipedia.org/wiki/Capitalization_of_Internet

An intranet – a private network where devices communicate over IP

All over the Internet

- digital documents
- remote processing
- telephone calls VoIP – Voice over IP
- TV programs IPTV
- commercial and financial services

IP header contains destination address
Router use it to select output interface



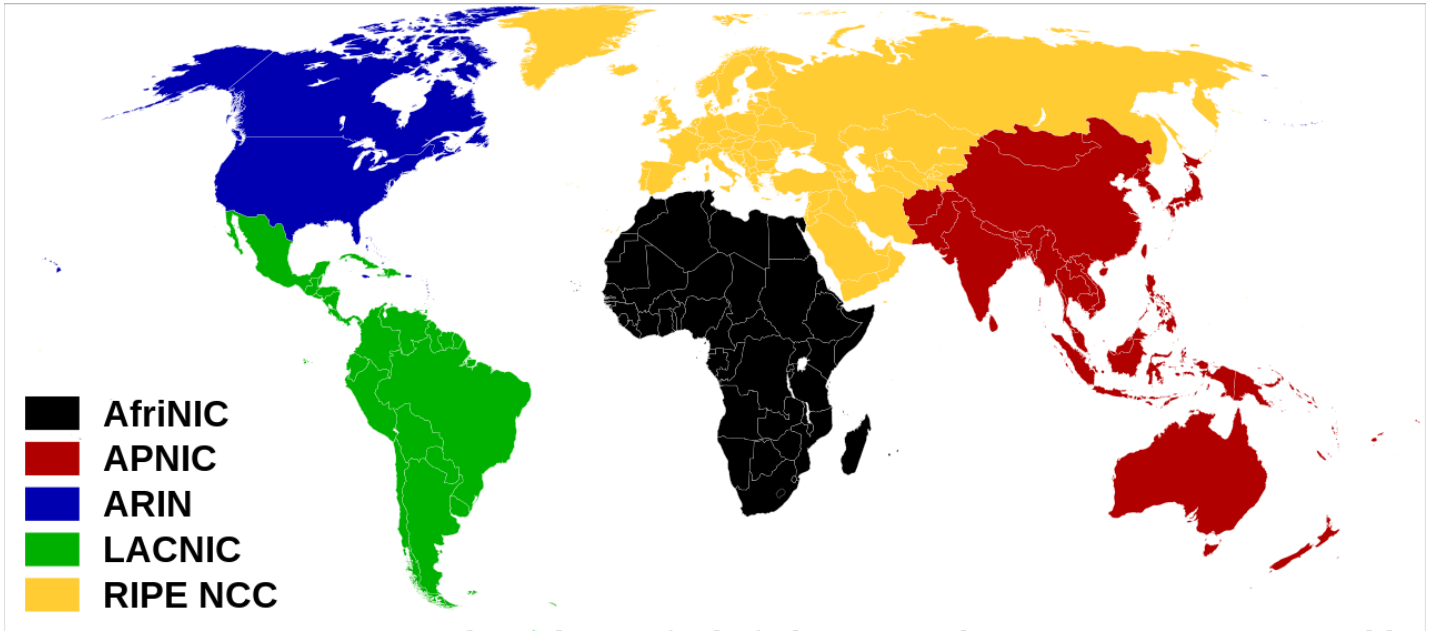
Institutions related to the Internet

IRTF Internet Research Task Force

IETF Internet Engineering Task Force – publishes RFCs *Request For Comments*

IANA Internet Assigned Numbers Authority – e.g. IP addresses

- RIPE Réseaux IP Européens
- ARIN American Registry for Internet Numbers
- APNIC Asia-Pacific Network Information Centre
- LACNIC Latin American and Caribbean Internet Addresses Registry
- AfriNIC African Network Information Centre



Source: commons.wikimedia.org/wiki/File:Regional_Internet_Registries_world_map.svg

Brief Internet History

1962 first memos about packet switching
from Bolt Beranek and Newman - a high-technology company

1966 Advanced Research Projects Agency of USA DoD started the ARPANET project

1968 BBN started its deployment

1969 public distribution of RFC - *Request For Comments* !!!
nic.ddn.mil ftp telnet (guest anonymous)
www.rfc-editor.org/rfcsearch.html – today
datatracker.ietf.org
tools.ietf.org/html/ See RFC 2549 – have some fun

1971 ARPANET opened to the public use NCP – *Network Control Protocol*

- remote login
- file transfer
- email

1981 TCP/IP – It is a shortcut for a bunch of related protocols
National Transport Control Protocol / Internet Protocol, Version 4 Specification

1983 UNIX 4.2 BSD with TCP / IP - public domain !!!

rise of DNS !!!

1984 MILNET - separation of the military portion of ARPANET

1985 Creation of NSFNET *National Science Foundation Network*

1989 100 000 computers in the Internet

1990 Dismantling of ARPANET

First web server !!! – non qualified people can use the Internet

1992 1 000 000 computers in the Internet

1994 Creation of W3C *World Wide Web Consortium*

1994 NAT *The IP Network Address Translator* – connects to Internet nodes with private addresses

1996 IPv6 *Internet Protocol, Version 6 Specification* – huge IP address space

1998 CIDR *Classless Inter-Domain Routing* – more efficient IP address assignments

2002 200 000 000 computers in the Internet

2004 Root DNS servers support both IPv6 and IPv4

2008 DNS support IPv4 & IPv6 in IANA IP core – users mustn't deal with IP addresses

Other WAN Technologies

	X.25	Frame Relay (FR)	Asynchronous Transfer Mode (ATM)	Multiprotocol Label Switching (MPLS)
Massive deployments from	1980	1990	1995	2000
In use	no	yes	yes	still new deployments
Max. speed	64 kb/s – access 2 Mb/s – net.	45 Mb/s	1,54 ... 622 Mb/s, 2.5, 10 Gb/s	100 Gb/s
Packets	variable length	variable length	53 bytes length	variable length

Quality of services	Basic, i.e.:
	• delay
	• delivery ratio availability
	• time to repair
		Basic +
		CIR – Committed Information Rate
		EIR – Excess Information Rate
			Basic +
			traffic categories:
			• **C**onstant **B**it **R**ate
			• Real-Time
			  • **V**ariable **B**it **R**ate
			• Non-Real-Time
			  • **V**ariable **B**it **R**ate
			• Unspecified Bit Rate
			• Available Bit Rate
				Basic +
				a few forwarding classes (class of services)

- X.25, FR, ATM switches are layer 3 devices
  - Addressing – International numbering plan for public data networks ITU-T X.121
  - Path identifier is used to switch data packets
- ATM QoS parameters

	CBR	nrt-VBR	rt-VBR	ABR	UBR
Cell Loss Ratio	+	+	+	+	
Cell Transfer Delay	+		+		
Cell Delay Variation	+	+	+		
Peak Cell Rate	+	+	+		+
Sustained Cell Rate		+	+		
Burst Tolerance @ PCR		+	+		
flow control				+	

  - ATM connection can manage some QoS parameters
- MPLS switches are considered layer 2.5 devices
  - Path identifier is used to switch data packets
  - Packet flows are bound to forwarding classes – Class of Services
    - Bandwidth is statically allocated to the classes

Telephony Technologies

All of them can carry data, so IP packets too

Analog telephony networks via modems

Digital

- ISDN – Integrated Services Digital Network
  - N x 64 kb/s
- SONET / SDH – Synchronous Optical Networking / Synchronous Digital Hierarchy in USA / in Europe
  - reliable transmission channels of fixed bit rate – TDM
  - STM-1 – 155.52 Mb/s … STM-256 – 39.813120 Gb/s
- Cellular Networks
  - GSM
  - IS-95
  - UMTS
  - CDMA2000
  - LTE
- Satellite phone networks

Access networks

DSL – Digital Subscriber Line

- family of technologies used to transmit digital data over copper telephone lines
- different down- and up-link speeds, e.g. 24 Mbit/s and 3.5 Mbit/s
- speed strongly depends on distance and cable quality

DOCSIS – Data Over Cable Service Interface Specification

- data transfer over existing cable television systems (hybrid fiber-coaxial)
- speeds from 10 Mb/s to 10 Gb/s

Ethernet

- wired network
- big variety of interfaces
- speeds: 10, 100 Mb/s, 1, 10, 40, 100, 400 Gb/s

Wi-Fi

- wireless network
- numerous versions
- speed strongly depends on distance and radio noise

Generation	Supported version	Max. link rate
Wi-Fi 6	802.11ax	600–9608 Mbit/s
Wi-Fi 5	802.11ac	433–6933 Mbit/s
Wi-Fi 4	802.11n	72–600 Mbit/s

Passive Networks

Passive network infrastructure

- telecommunication pipes
- telecommunication cables

Laid by

- telephone and cable-TV companies
- energy (electro- and heat), water, gas, oil distribution companies
- railway and highway companies
- municipalities
- building developers

for

- their own purposes
- lease

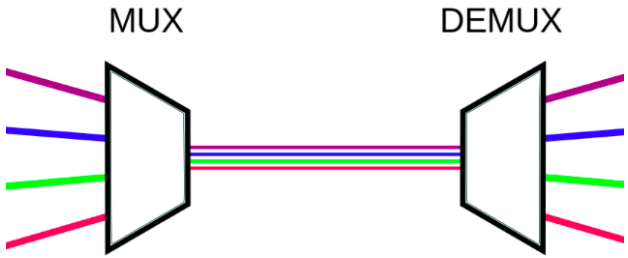
Optical cables replace copper cables

Wavelength-Division Multiplexing

Multiplexes a number of optical carrier signals onto a single optical fiber

Wavelengths are colors of laser light

- Coarse WDM
  - 60 km span
  - up to 16 colors
- Dense WDM
  - 100-140 km span
  - 40, 80 and more colors



Overlay Networks

- VPN – Virtual Private Network
  - e.g. enterprise intranet connecting remote departments and workers

- Content addressable
  - to unbind resources from their locations
  - e.g. for distributed data storage

- Anonymous Internet – TOR (The Onion Routing)
  - intended to protect the personal privacy – e.g. visits to Web sites, instant messages
  - does not hide the fact that someone is using TOR

Special Purpose Networks

- Delay tolerant (disruption tolerant)
  - lack of continuous connectivity due to
    - limits of wireless radio range
    - sparsity of mobile nodes
    - energy resources
    - attack
    - noise
  - mobile or extreme terrestrial environments
  - planned networks in space
- Ad hoc networks
  - e.g. between moving vehicles
- Sensor networks
  - for energy and computation constrained devices
  - can be connected to the Internet via gate devices

Bandwidth

Offered by interfaces

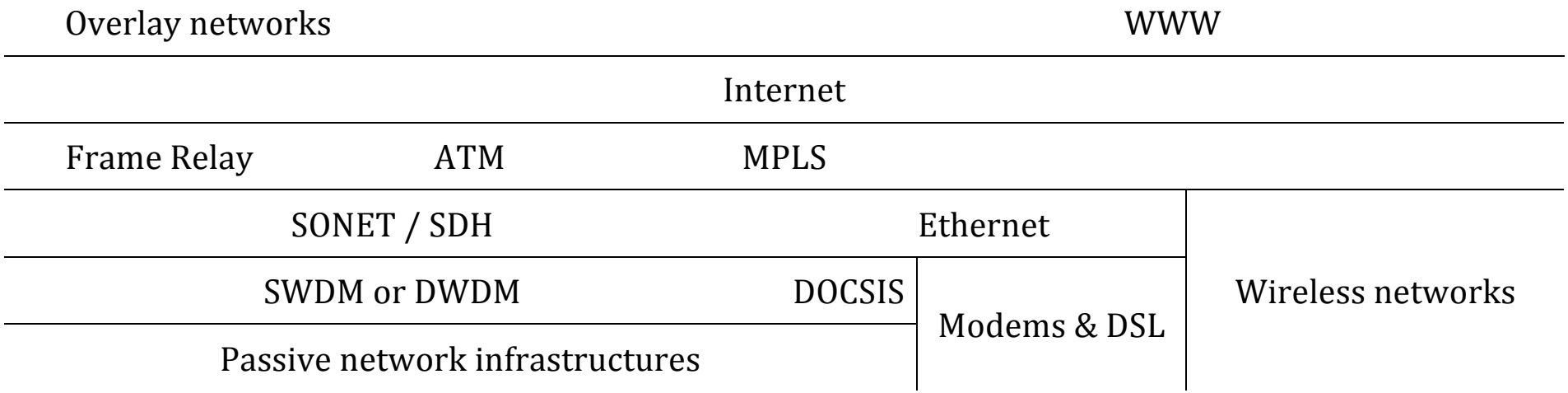
- analog modem 28.8 ÷ 56 kb/s
- ISDN 64 kb/s ÷ 2 Mb/s
- DSL 115 kb/s ÷ 1 Gb/s – distance and cable quality dependent
- Ethernet 10 Mb/s ÷ 100 Gb/s
- optical fiber 34 Mb/s ÷ 40 Gb/s
- DWDM 800 Gb/s ÷ 10 Tb/s (!)
- radio link 128 kb/s ÷ 1 Gb/s

Needed by applications

- voice channel 64 kb/s
- SDTV (MPEG-2) 3 ÷ 8 Mb/s
- SDTV (MPEG-4) 1.4 ÷ 2 Mb/s
- HDTV (MPEG-2) 14 ÷ 20 Mb/s
- HDTV (MPEG-4) 4 ÷ 18 Mb/s

Summary

Data transmission services or infrastructure for lease:



Owners of passive network infrastructures:

- municipal companies that distribute: electricity, water, heat, gas
- country wide distributors of: electricity, gas, oil
- rail roads and highway companies

- Word Wide Web
- Internet
  - Institutions related to the Internet
  - Brief internet history
- Other WAN technologies
- Access networks
- Passive networks
- Wavelength-Division Multiplexing
- Overlay networks
  - Virtual private network
  - Content addressable
  - Anonymous Internet
- Special purpose networks
  - Delay tolerant
  - Ad hoc & sensor networks
- Offered and needed bandwidth

Questions

1. What is WWW (World Wide Web)?
2. What are the aims of IETF, IANA and APNIC?
3. Describe the history of Internet evolution.
4. What were the most important reasons for Internet grow and be world widely used?
5. What was the reason for introduction of NAT (Network Address Translation) into Internet?
6. What was the main reason for IPv6 construction?
7. What was the reason for introduction of CIDR (Classless Inter-Domain Routing)?
8. Compare Frame Relay, ATM and MPLS technologies.
9. What are the telephony technologies used for data transmission?
10. What are today's network access technologies?
11. Who builds passive network infrastructures?
12. What for do we use wavelength-division multiplexing devices?
13. What is the difference between SWDM and DWDM?
14. Give 2 examples of overlay networks.
15. Give 2 examples of special purpose networks.

Computer Networks

Lecture on

Computer Serial Links

Plan of This Lecture

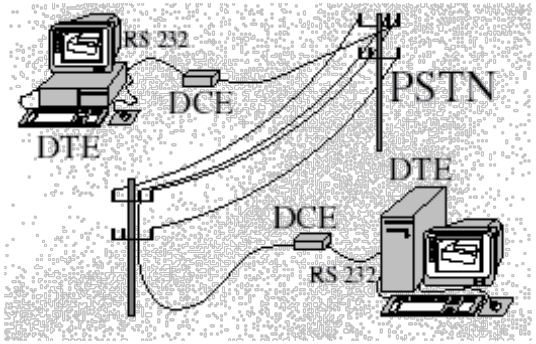
- Common computer wired interfaces
- Transmission media
- Data representations on a transmission line
- Bit error correcting code
- Framing
- Point-to-Point Protocol

Common Computer Wired Interfaces

Ethernet	Thunderbolt	USB	FireWire (IEEE 1394)
0.1 1 10 40 100 400 Gb/s	10 20 40 Gb/s	1.5 12 480 Mb/s 5 10 20 Gb/s	100 200 400 800 Mb/s 3.2 Gb/s
100 m - CAT5 100 km - fiber	copper 3 m fiber 30, 100 m	5 m; can be 50 m - CAT5 10 km - fiber	4.5 m; can be 100 m also fiber and coax

- Ethernet is dominant for any distance communication
- Any older interfaces can be find in data centers
- VPN over Internet is the cheapest solution to set a new link between remote devices

Asynchronous commuted lines



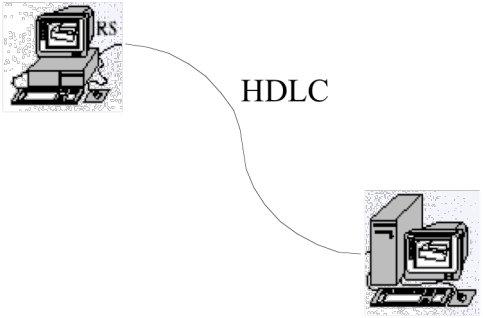
- Modems over PSTN are still in use for:
  - dialup remote control

    PSTN – Public Switched Telephone Network

- Synchronous HDLC over telephone leased lines are still in use for:
  - backup communication

    HDLC – High-Level Data Link Control

Synchronous leased lines



- xDSL technologies are widely used
  - DSL modem can be built in the home router
  - or connected via USB or Ethernet

    DSL – Digital subscriber line

- Optical cables replace copper cables – Ethrnet interfaces are dominant

Transmission Media

Cable media:

- Unshielded Twisted Pair (UTP) & Shielded Twisted Pair (STP)

Category	Bandwidth
3	16 MHz
5e	100 MHz
…	…
8.2	2000 MHz

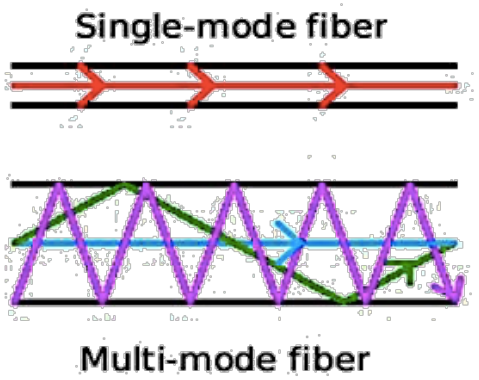
- Coaxial Cable
  - Wide standards range
  - Higher attenuation than twisted pairs

- Optical Fibre
  - Single-mode fibre core 8-10 μm

No degradation of signal	Manufacturing and handling is difficult
Low dispersion	Higher price
Well suited for long distance	Coupling light into the fibre is difficult
Used in MANs and WANs	

  - Multi-mode fibre core 50-200 μm

High attenuation	Manufacturing and handling is easy
High dispersion	Lower price
Well suited for short distance	LED transmitters can be used
Used in LANs and inside devices	



Why do fibre cables replace copper ones?

- Insensible for electromagnetic noises
- Junctions are humidity resistant
- Enable much higher transmission speed
  which is limited by electro-optic interfaces
- Enables much longer transmission distances without signal amplifiers
- Optical cables weight less than copper cables
- Installations are less expensive

Non-cable transmission media:

- Radio waves
- Visible light
- Infrared light
- Ultrasound waves

Data Representations on a Transmission Line

There is huge number of line codes

Prominent examples are:

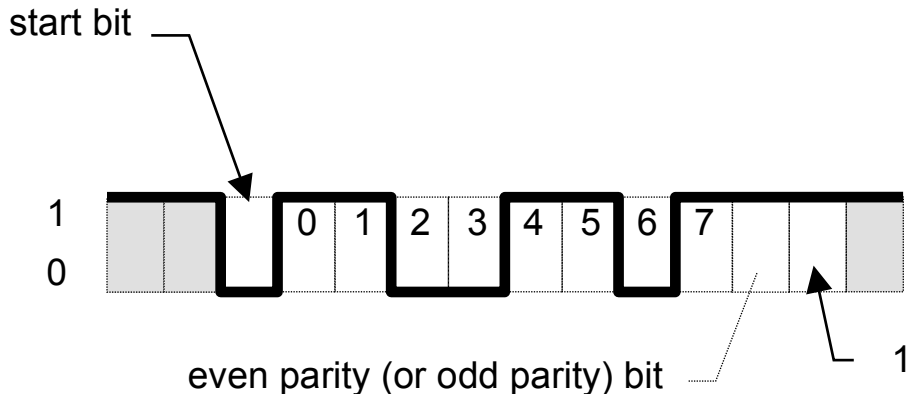
- Asynchronous transmission schema
- Manchester code aka. Phase Encoding
- Miller code aka. Modified Frequency Modulation
- MLT-3 *Multi-Level Transmit*
- 4B5B
- 8b/10b
- 64b/66b

Expected features of line codes

- clock recovery
- special symbols e.g. start of frame
- DC-balance – no direct current
  - non-galvanic coupling possible – no risk of ground loop courent
- lower bandwidth

Asynchronous Transmission

The signal carries only data bits

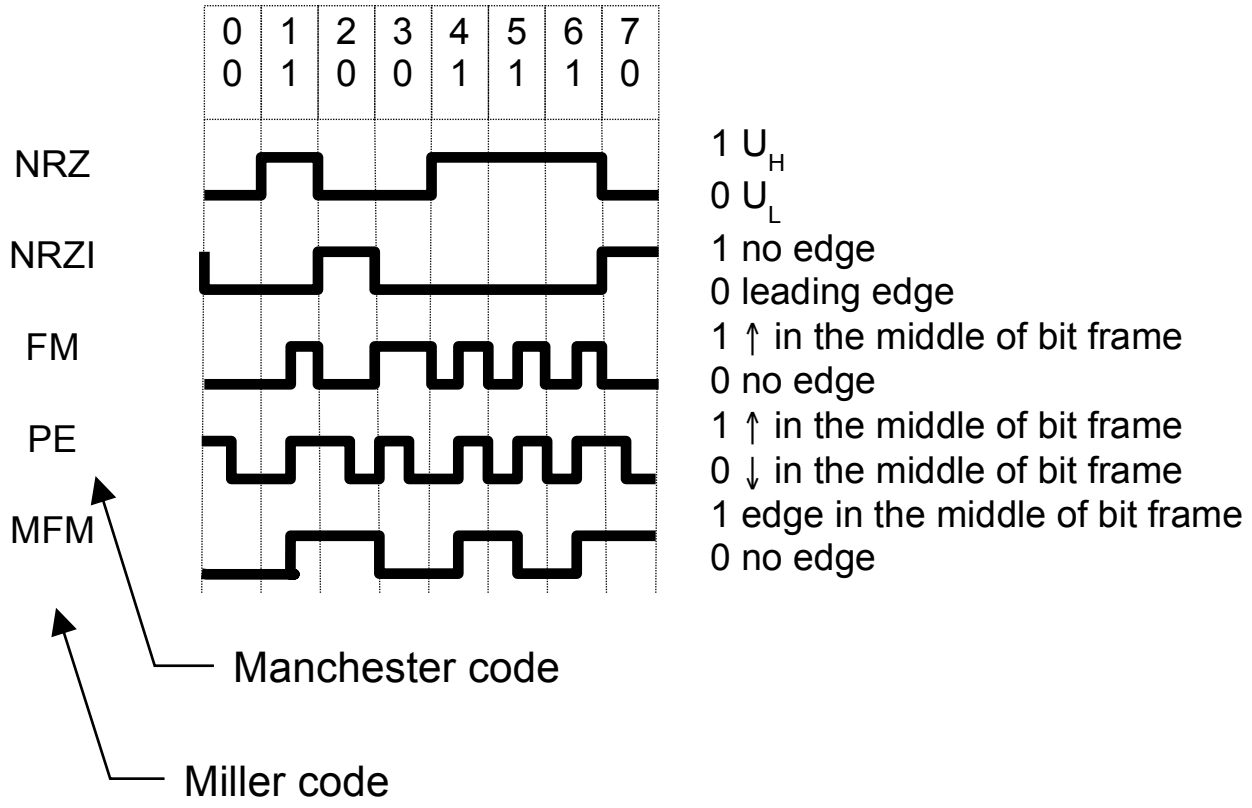


5 data bits – teletypewriter code
7 data bits – ASCII code
8 data bits – for octet stream

‘0’ for 20 ms it is a brake signal

Synchronous Transmission

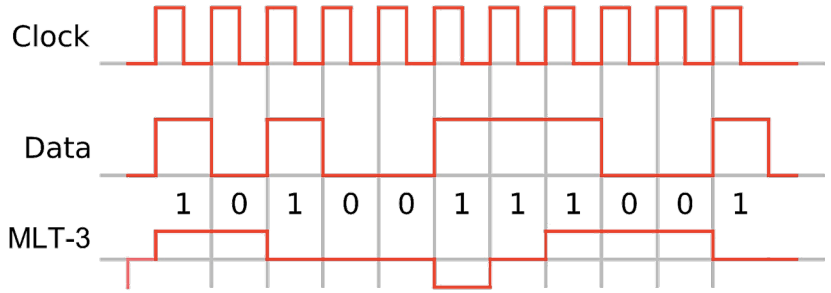
The signal carries clock and data bits



MLT-3 encoding

Multi-Level Transmit

- cycles sequentially through −1, 0, +1, 0



4B5B encoding

- Used in FDDI, Fast Ethernet and others
- There are 16 special purpose codes
  - e.g. start of the frame
- On optical fiber is NRZI encoded
- On copper is MLT-3 encoded

Data		4B5B code
(Hex)	(Binary)	
0	0000	11110
1	0001	01001
2	0010	10100
3	0011	10101
4	0100	01010
5	0101	01011
6	0110	01110
7	0111	01111

Data		4B5B code
(Hex)	(Binary)	
8	1000	10010
9	1001	10011
A	1010	10110
B	1011	10111
C	1100	11010
D	1101	11011
E	1110	11100
F	1111	11101

8b/10b encoding

- Used in DVI, HDMI, USB 3.0 and others

64b/66b encoding

- Used in 10, 100 Gigabit Ethernet and others

Cyclic Redundancy Check (CRC)

Bit error-detecting code

- is based on the remainder of a polynomial division
- has proved efficiency of detecting strength
- is simple to implement in binary hardware

A binary polynomial:

$$X=10011011 \quad \rightarrow \quad w(X)=x^7+x^4+x^3+x+1$$

Popular divisors

CRC-16 (BISYNC)	$x^{16}+x^{15}+x^2+1$
SDLC (IBM, CCITT)	$x^{16}+x^{12}+x^5+1$
CRC-16 reverse	$x^{16}+x^{14}+x+1$
SDLC reverse	$x^{16}+x^{11}+x^4+1$
LRCC-16	$x^{16}+1$
CRC-12	$x^{12}+x^{11}+x^3+x^2+x+1$
LRCC-8	x^8+1
ETHERNET CRC	$x^{32}+x^{26}+x^{23}+x^{22}+x^{16}+x^{12}+x^{11}+x^{10}+x^8+x^7+x^5+x^4+x^2+x+1$

How it works:

frame s(x) = w(x).FCS – *Frame Check Sequence*

FCS = reminder of polynomials division $2^G * w(x) : g(X)$

s(x) = $2^G * w(x) : g(X) + r(x)$

CRC code

e.g.. G=3 w(x)= 0111

$2^3 * w(x)$ g(X)

0111000 : 1011 = 0110 ← '0' if shift, '1' if subtraction modulo-2

1011

1010 ← exor

1011

0010 ← exor

010 = **r(x)** => **s(x)** = 0111 010

CRC

See: http://www.ee.unb.ca/cgi-bin/tervo/calc.pl

Mathematically proved efficiency

e.g. for CRC-16 and frame length ≤ 32 767 bits

- All detected errors
  - single bit
  - two bit
  - three bit
  - all odd bits
- Probability of detection of serial bit errors
  - 100% for ≤ 16 consecutive bits
  - 99,997 % for 17 consecutive bits
  - 99,998 % for 18 consecutive bits

Bit Error Correction Codes

There are many such correction codes

Hamming codes are widely used

- simple implementation
- can correct one-bit error

m – message length
r – number of parity bits
n – number of transmitted bits $n = m + r$
Condition of one bit correction $m + r + 1 \leq 2^r$

m	16	32	64	128	…
r	5	6	7	8	…

How it works:

Bit position		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	
Encoded data bits		p1	p2	d1	p4	d2	d3	d4	p8	d5	d6	d7	d8	d9	d10	d11	p16	d12	d13	d14	d15	
Parity bit coverage	p1	✗		✗		✗		✗		✗		✗		✗		✗		✗		✗		...
	p2		✗	✗			✗	✗			✗	✗			✗	✗			✗	✗		
	p4				✗	✗	✗	✗					✗	✗	✗	✗					✗	
	p8								✗	✗	✗	✗	✗	✗	✗	✗						
	p16																✗	✗	✗	✗	✗	

P = 0 then no error, otherwise P is the number of bit to be corrected

Hamming codes with additional parity allow

- to detect and correct a single error
- and at the same time detect (but not correct) a double error

Framing – Protocols Using Asynchronous Links

- BISYNC (IBM) - based on ASCII characters

SYNC	SOH	**Header**	STX	**Payload**	ETX	CRC	SYNC	SOH

- Other methods:
  - SOH and ESC injection
  - min/max delays between frames and characters in a frame
- DDCMP (DEC) - for binary data
  - fixed length header carries payload counter

Protocols Using Synchronous Links

- SDLC (IBM)
  - synchronization byte: 01111110
  - after every 5 ones a zero bit is injected/removed
  - silence byte: 11111111
  - ring release byte: 11111110

- Token Ring (IBM)
  - coding disturbance: J and K symbols in Manchester code

- HDLC - High Level Data Link Control (ISO) - for binary data

- HDLC subsets:
  - LAP Link Access Procedure X.25
  - LAPB Link Access Procedure Balanced, X.25
  - LAPD Link Access Procedure, D-channel, ISDN
  - LAPX LAPB extended, teletex
  - LAPM ITU V.24 for modems
  - LLC LOGICAL Link Control IEEE 802

Serial Line IP (SLIP)

- RFC 1055 A Nonstandard for Transmission of IP Datagrams over Serial Lines
  "SLIP END" = 192 (219 220) → 192
  "SLIP ESC" = 219 (219 221) → 219
  - no means for control information
  - no bit error detection, correction, nor compression mechanisms
  - no means for dynamic IP address assignment
  - no authorization mechanisms
  - can carry bytes of any protocol (up to 1006 octets)
- CSLIP *Compressed SLIP* RFC 1144
  IP header 20 B + TCP header 20 B → 3-5 octets
  - can handle up to 16 connections

Point-to-Point Protocol (PPP)

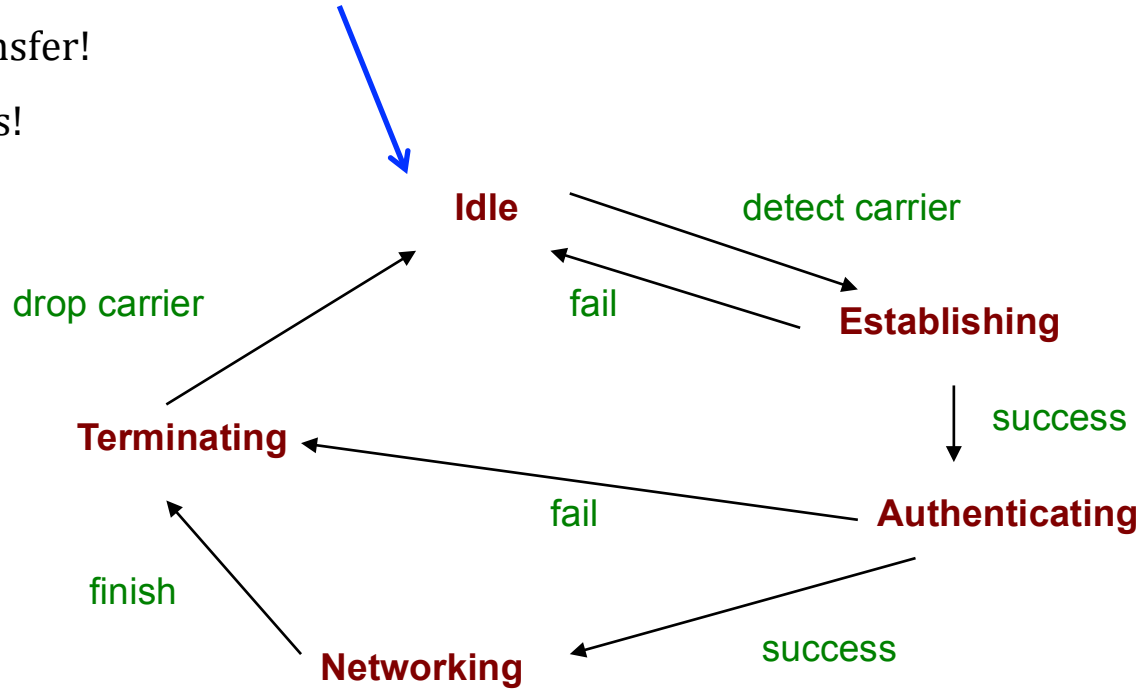
RFC 1171, RFC 1172, ...

Set of protocols organized in 3 layers

- Physical layer - any ANSI standard
- Data link layer - modified HDLC
- **LCP Link Control Protocol**

Reliable data transfer!

It can link routers!

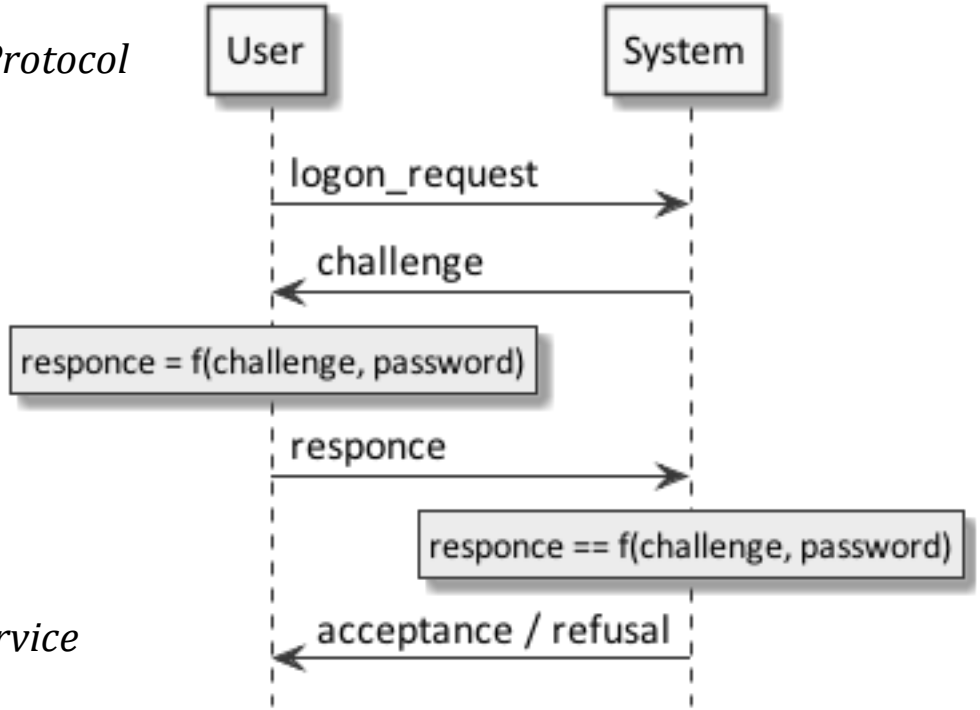


PPP General Features

- Control of connection parameters
- Flow control
- Means for diagnostic mechanisms
- Means for authentication mechanisms
- Compression possibilities
- Max. datagram size = 1500 octets

PPP Support Many Authentication Mechanisms

- PAP *Password Authentication Protocol*
  - name & password plain text transfer – easy to sniff
  - confirmation plain text transfer
- CHAP *Challenge Handshake Authentication Protocol*
  - No password transfer!



- RADIUS *Remote Authentication Dial-In User Service*
- IPSec

PPP Network Control Protocols

They work at **networking state of LCP**

Different instances for divers 3rd layer protocols

i.e.: DECNET, IP, OSI NP, IPX, AppleTalk

IPCP

- It provides IP addresses for: host, network mask, DNS servers
- Support header compression
- ...

PPP Usage

- Over asynchronous or synchronous serial links see: man pppd
- Over broadband connections:
  - PPPoE *Point-to-Point Protocol over Ethernet*
  - PPPoATM *Point-to-Point Protocol over ATM*
  - PoS *Packet over SONET/SDH*
  - PPTP *Point-to-Point Tunneling Protocol*
    between two hosts via IP

Summary

- Common computer wired interfaces
- Transmission media
- Data representations on a transmission line
  - asynchronous transmission
  - synchronous transmission
- Cyclic redundancy check
- Hamming codes
- Framing on
  - asynchronous links
  - synchronous links
- Point-to-Point Protocol
  - general features
  - authentication mechanisms
  - IP Network Control Protocol
  - usage

Questions

1. What for we use modems over PSTN in today network applications?
2. What for we use synchronous links over leased telephone lines in today network applications?
3. What is the difference between multi-mode and single-mode optical fibres?
4. Why do fibre cables replace copper ones?
5. What are the expected features of line codes?
6. What is the principle of asynchronous serial communication?
7. What is the principle of Manchester encoding?
8. What is the principle of MLT-3 encoding?
9. What is it CRC and what for is it used?
10. How many parity bits are needed to correct one bit in a frame of 256-bit length?
11. How frame synchronization can be done in serial asynchronous links?
12. How frame synchronization can be done in serial synchronous links?
13. Give an example of the SLIP (Serial Line IP) protocol usage.
14. Give an example of PPP (Point-to-Point Protocol) usage.
15. Why PPP is better than SLIP?
16. How can be done authentication in PPP?

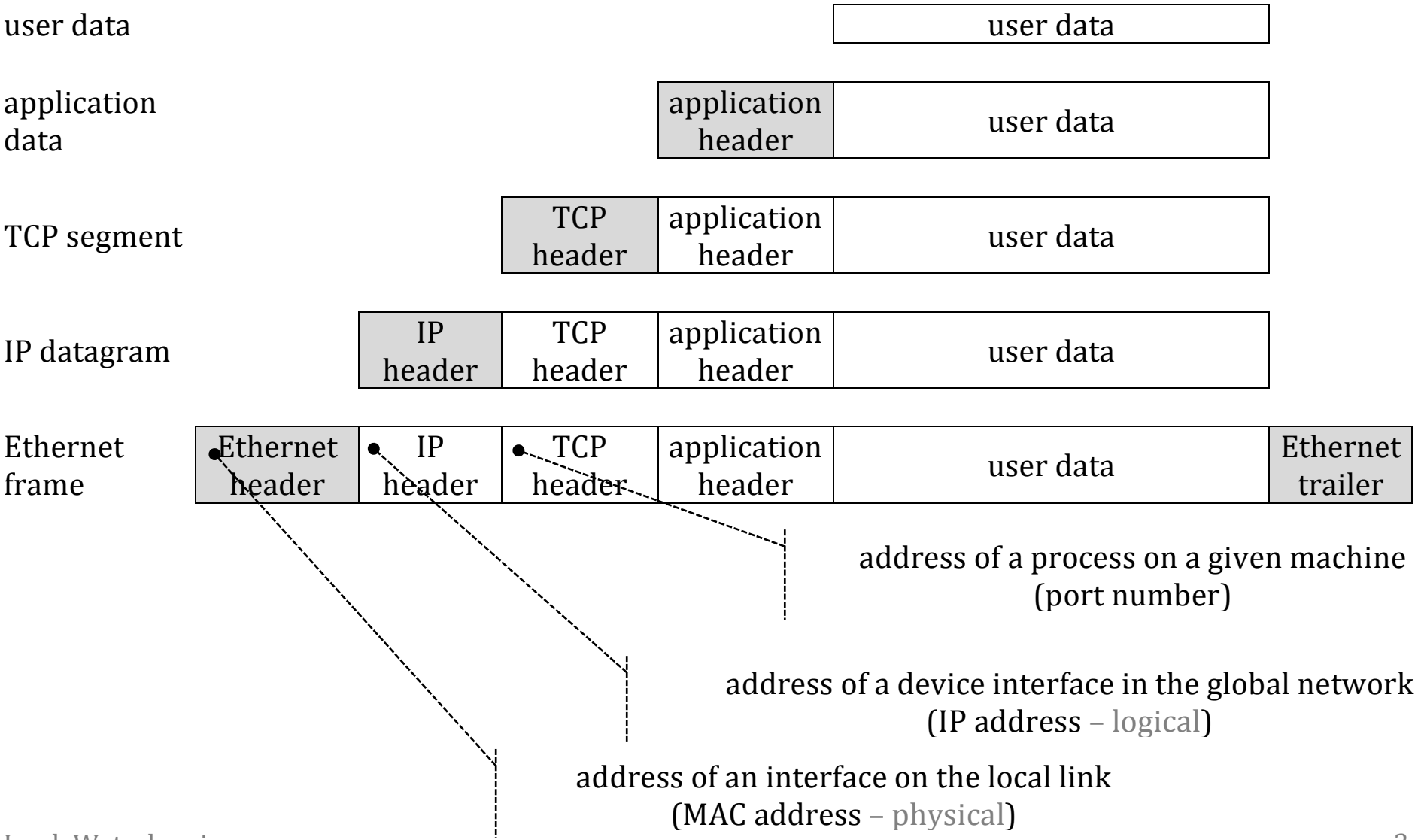
Computer Networks

Lecture on
Addressing – MAC, EUI, IPv4, IPv6, port numbers, URL

Plan of This Lecture

- Encapsulation of packet headers
- 2nd layer addresses – IEEE 802 addresses
- 3rd layer addresses – Internet addresses
- 4th layer addresses – port numbers
- Web addresses – Uniform Resource Locators (URLs)

Encapsulation of Packet Headers



Address Notations – Examples

		Numerical		Symbolic
Transport	address	25, 80	/etc/services	SMTP, HTTP
Network	type of payload	6, 17	/etc/protocols	TCP, UDP
	address	139.159.208.110 2607:f8b0:4000:813::200e	→ DNS ← RevDNS	www.qzhu.edu.cn ipv6.google.com
	ARP ↓ ↑ RARP or ICMPv6			
Data Link	type of payload	0x0800, 0x86DD		IPv4, IPv6
	address	00-20-AF-9A-10-E1		

2nd Layer Addresses – IEEE 802 Addresses

MAC-48 (Medium Access Control address, 48-bits length)

- Was defined to distinguish hardware interfaces
- IEEE considers the term as obsolete

EUI-48 (Extended Unique Identifier, 48-bits length)

- Indistinguishable from MAC-48
- Was defined to distinguish hardware or software instances
  – not necessarily a network address
- Users still use the name MAC-48
- Used by: Ethernet, WiFi, Bluetooth, ATM, Token Ring, SCSI, FDDI, Fibre Channel, most other IEEE 802 networks

EUI-64 (64-bits length)

- Used by: FireWire, 802.15.4 PAN, ZigBee

MAC address

2-byte format

- for simple devices working in local isolated networks
- address is assigned by network administrator

6-byte format

- for general usage
- address
  - is assigned by interface manufacturer
    - 3-byte Organizational Unique Identifier (OUI)
    - 3-byte Network Interface Card (NIC)
  - can be cloned by administrator
  - can by assigned by administrator

    bit1: U/L =0 => universal, =1 => local
- unicast, multicast and broadcast

  bit0: I/G =0 => individual, =1 => group

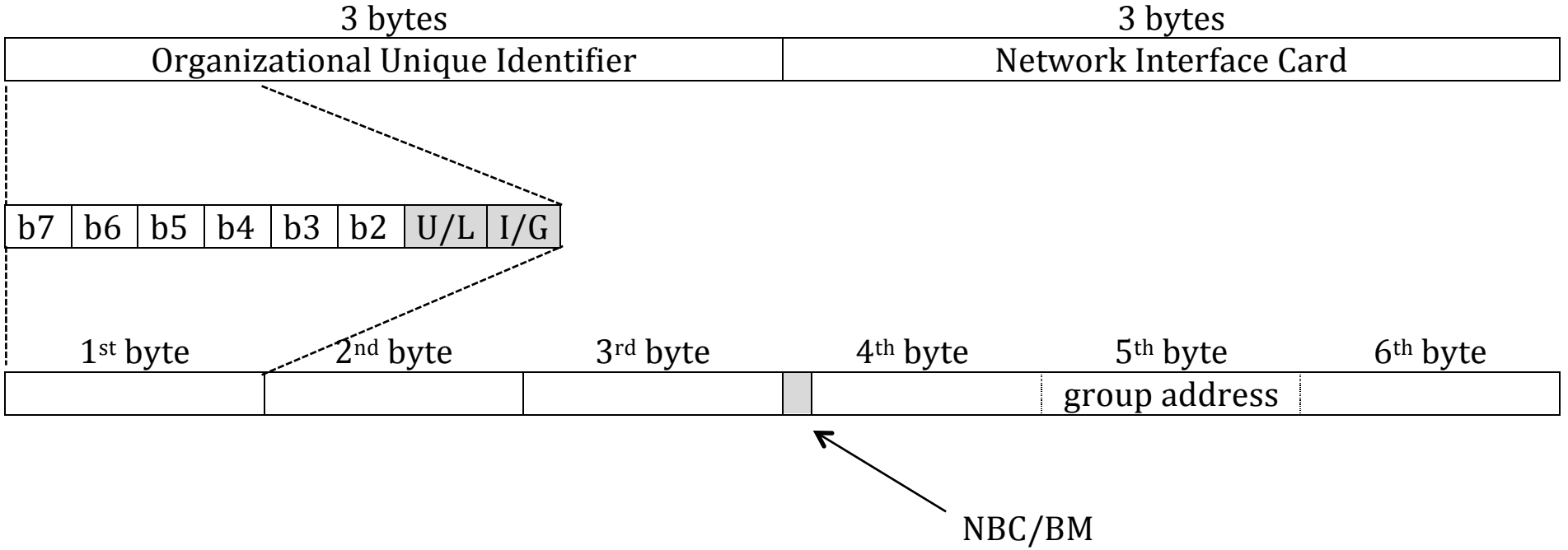
  NBC/BM bit24: =0 => Natural Binary Code, =1 => bit mask

  FF-FF-FF-FF-FF-FF – broadcast

  00-00-00-00-00-00 – NULL or uninitialized value

IEEE defined logical format of addresses

- physical structure (transferred order of bits and bytes) is not the same in different networks
  e.g. MSB first in Ethernet, Ring LSB first in Token



EUI-64

64 bit identifier

Organizational Unique Identifier lengths:

- 24, 28 and 36 bits, so the organisations have 40, 36, and 28 bits for numbering

00-00-00-00-00-00-00-00 – NULL or uninitialized value

FF-FF-FF-FF-FF-FF-FF-FF – broadcast

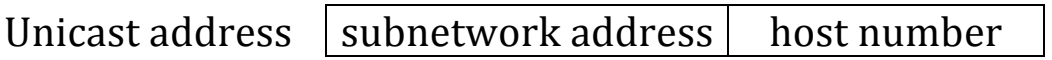
Address translation is deprecated, historically it was:

MAC-48 → EUI-64: OUI + 0xFFFF + NIC

EUI-48 → EUI-64: OUI + 0xFFFE + NIC

3rd Layer Addresses – Internet Addresses

	IPv4	IPv6
Length	32 bits	128 bits
Notation	decimal, e.g.: 139.159.208.110	hexadecimal, e.g.: 2607:f8b0:4000:813::200e :: is a shortcut for string of 0s
Type	unicast, multicast, broadcast in subnets special (e.g. loopback)	unicast, multicast, anycast no broadcast special (e.g. loopback) IPv4 mapped
Range	global and private	global, unique-local (private), link-local
Subnetwork addressing	class-full classless	classless



Several IP addresses can be assigned to one interface!

IPv4 Addresses

Class	First Octet	Leading Bits	Network Address	Host Index
			address (effective) #bits	*#bits*
A	0-127	0…	8 (7)	24
B	128-191	10…	16 (14)	16
C	192-223	110…	24 (21)	8
D	224-239	1110…	multicast	
E	240-255	11110…	reserved	

e.g. 127.0.0.1 is a loopback address

Host index = 0 – unknown source address or default destination
Host index = all 1s – broadcast inside the subnetwork

Number of hosts = $2^H - 2$ H – number of index bits
Number of networks = $2^N - 2$ N – number of effective bits

Dotted decimal notation e.g. 192.168.16.4 → 11000000 10100000 00001000 00000010

Private address pools

1	class A network:	10.0.0.0/8
16	class B networks:	172.16.0.0/12
256	class C networks:	192.168.0.0/16

Automatic Private IP Addressing (APIPA) 169.254.0.0/16

– for configuration of link-local addresses in IPv4

Prefixes, VLSM, CIDR

Prefix notation

194.29.168.0 255.255.255.0 = 194.29.168.0/24

11111111.11111111.11111111.00000000

10.2.3.4 255.255.255.252 = 10.2.3.4/30

11111111.11111111.11111111.11111100

Variable Length Subnet Mask

#ISP level 1	…	# organization	# host

Subnetwork address = 0 – unknown source address or default destination

Subnetwork address = all 1s – broadcast inside the subnetworks

Classless Inter-Domain Routing

- Routers can aggregate routing records for subnets reachable form the same output
- Routers have to store IP addresses and subnet masks

Subnetwork Mask

IP address: 11000101.11001010.11101001.01010100

197 . 202 . 233 . 84

Subnet mask 11111111.11111111.11111111.11000000

255 . 255 . 255 . 192

Subnet address IP address AND mask

11000101.11001010.11101001.01000000

197 . 202 . 233 . 64

Host Index IP address AND (NOT subnetwork mask)

00000000.00000000.00000000.00010100

20

IPv6 Addresses

- Optimistically around 4,000 trillions of addresses per 1 m^2 of the earth (considering different types of allocations)
- Most pessimistically, at least 1,564 addresses per 1 m^2 of the earth
- Hexadecimal notation

  e.g. 2001:0DB8:AC10:FE01:: *:: – indicates omitted zeroes*

  2a00:1450:401b:804::200e

  2001:0db8::0001 = 2001:db8::1 *leading zeroes can be omitted too*

Hierarchy of IPv6 addressing

# Regional Internet Registry	#ISP level 1	# ISP level 2	#ISP level N	#organi zation	#locali zation	# host
		64 bits				64 bits

Anycast addresses

- Selected from the unicast address space
- Assigned to more than one interface / nodes

Domain Names

- Symbolic representation of IP addresses
- Hierarchical structure
- Can reflect:
  - geographical dependences
    e.g. www.ztm.waw.pl bip.warszawa.pl
  - organizational dependences
    e.g. www.ii.pw.edu.pl
- Can use national characters
  e.g.: .中国 кц.рф
- One domain name can be attributed to many IP addresses
- One IP address can have many domain names

4th Layer Addresses – Port Numbers

Port identifies a process, participating in a communication

It is a 16-bit natural number

3 scopes

- Permanent ports – used by server processes
  - Well-known services (<1024)
    - defined by Internet Assigned Numbers Authority
    - system processes
  - Registered ports (1024 ÷ 49151)
    - assigned by IANA
    - can be used without superuser privileges
- Private or ephemeral (dynamic) ports (49152 ÷ 65535)
  - used for private or customized services, for temporary purposes
  - used by client processes – automatic allocation of ephemeral ports

Web Address – Uniform Resource Locator

Is a reference to a web resource

Is a specific type of Uniform Resource Identifier (URI)

Often URI and URL are used interchangeably

URI = scheme:[//authority]path[?query][#fragment]

Popular schemes: http, https, ftp, mailto, file, data, irc

authority = [userinfo@]host[:port]

Examples:

http://en.qzhu.edu.cn/list.jsp?urltype=tree.TreeTempUrl&wbtreeid=1069

https://john.doe@www.example.com:123/forum/questions/?tag=networking&order=newest#top

https://en.wikipedia.org/wiki/URL#Syntax

http://[::FFFF:129.144.52.38]:80/index.html

hkp:// 192.0.2.16:80/

sftp://wytrebowicz@ www.example.com/ftpdir

file:///path/resource.txt <-- *It is not a web address*

Summary

- Encapsulation of packet headers
- 2nd layer addresses – IEEE 802 addresses
  - MAC addresses
  - Extended Unique Identifiers
- 3rd layer addresses – Internet addresses
  - IPv4 addresses
  - IPv6 addresses
  - Domain Names
- 4th layer addresses – port numbers
- Web addresses – Uniform Resource Locators (URLs)

Exercises

See content of the following files:

- /etc/services (see: man services)
- /etc/protocols (see: man protocols)
- /etc/hosts (see: man hosts)

Run in a terminal window the following commands:

- ifconfig (ipconfig on a MS Windows OS; or the newer ip addr list on Linux)
  and figure out the output (see: man ifconfig)
- host www.ii.pw.edu.pl (similar commands: dig, nslookup)
- host www.qzhu.edu.cn
- host -t AAAA en.wikipedia.org
- wget http://staff.ii.pw.edu.pl/~jwt/4you.html

Check the manufacturer name of the network interface of your computer. Use the MAC Address Lookup tool: https://www.macvendorlookup.com

Questions

1. What is the difference between multicast and anycast addressing?
2. Give an example of anycast address usage?
3. What is the structure of the MAC-48 address?
4. What is the difference between MAC-48 and EUI-48 addresses?
5. Describe the types of addresses defined by IEEE (2^{nd} layer addresses).
6. What is the host number pointed by the IPv4 address 197.202.233.64/24?
7. What is the host number pointed by the IPv4 address 197.202.32.64/16?
8. What is the meaning of the 197.202.255.255/16 IPv4 address in the subnet?
9. What is the meaning of the 0.0.0.0 IPv4 address in a subnet?
10. What is the meaning of the 255.255.255.255 IPv4 address in a subnet?
11. What for can we use the 127.0.0.1 address?
12. How many hosts can we address in the subnet 192.168.6.00/9?
13. How many IP addresses can be bind to a domain name?
14. How many domain names can be attributed to an IP address?
15. What for is the port number field in the TCP header?
16. What are permanent and ephemeral port numbers?
17. Characterize the addressing in the Internet (distinguish addresses related to 2^{nd}, 3^{rd}, and 4^{th} OSI layers).
18. Describe the structure of URL.

Computer Networks

Lecture on

Packet Transmission Issues

Plan of This Lecture

- How to achieve communication reliability?
- Network congestion problem
- Packet delay

Communication Reliability

Problems

- Corrupted message
  - Noise at transmission medium
- Lost message
  - Noise at transmission medium
  - Buffer overload in network switches or in the terminal device
- Duplicated messages
  - Due to retransmissions or bad configuration of communication protocols
- Modified message order
  - Due to multipath propagation in switched networks

Solutions

- Corrupted message
  - Bit error detection
  - Bit error correction – using an error correcting code, e.g. Hamming code
- Lost message
  - Flow control mechanisms
  - Message numbering
  - Positive or negative acknowledgments (ACKs or NACKs)
  - Retransmission timers
- Duplicated messages
  - Message numbering

How long the number should be?

- Modified message order
  - Message numbering

Bit Error Detection

- Bit parity check for every byte sent – used in asynchronous lines
- Cyclic Redundancy Check codes – used in synchronous lines
- Check sum of all bytes of a message
  - supplementary check on network & transport layers

Longer frame

- Higher probability of bit errors
- Better efficiency, i.e. $(\frac{\text{payload bits}}{\text{transmitted bits}})$ rate

Shorter frame

- Lower probability of bit errors
- Lower efficiency

Radio links – higher probability of serial bit errors

- Parallel transmission of several frames can change a serial error to several single-bit errors

b0	b1	b2	…	bN	CRC_B
c0	c1	c2	…	cN	CRC_C
…	…	…	…	…	…
x0	x1	x2	…	xN	CRC_X

Transmission order: b0, c0, …, b1, c1, …, b2, c2, …

Message Repetition

- Each message is sent two or three times or with error-correcting code – in very noisy networks
- Using positive acknowledgement ACK
  - Sender sets a timer for each message sent
  - Arriving ACK cancels the respective timer
  - When a timer fires the message is retransmitted and the timer is set
  - Number of retransmissions is limited

How to set the timer?

- Using negative acknowledgement NACK
  - Recipient sends NACK when it gets a message out of sequence
  - Recipient sets a timer for each sent NACK
  - Sender retransmit the message pointed by NACK

How long to store the message?

ACKs

- Needlessly take bandwidth in reliable links
- Slower retransmission
- Recommended for unreliable links

NACKs

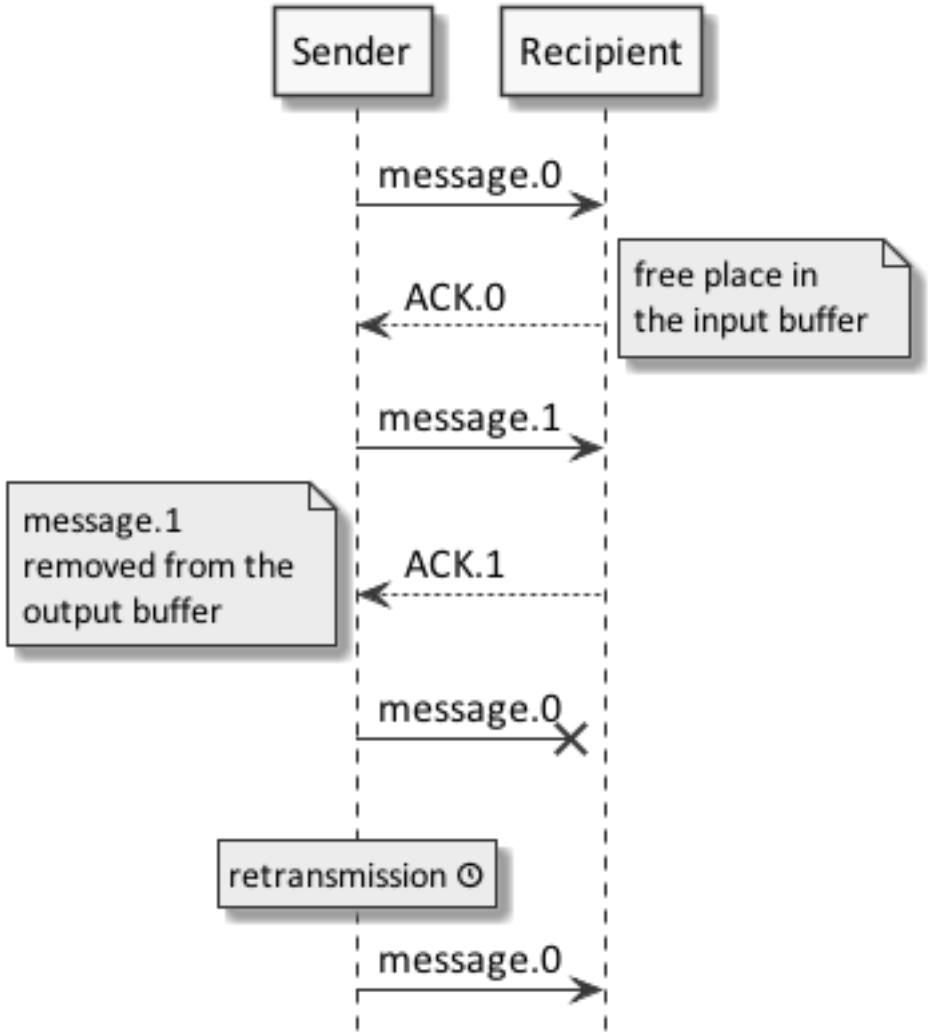
- Can be frequent in unreliable links
- Faster retransmission
- Recommended for reliable links
- Periodic ACKs help to free buffers

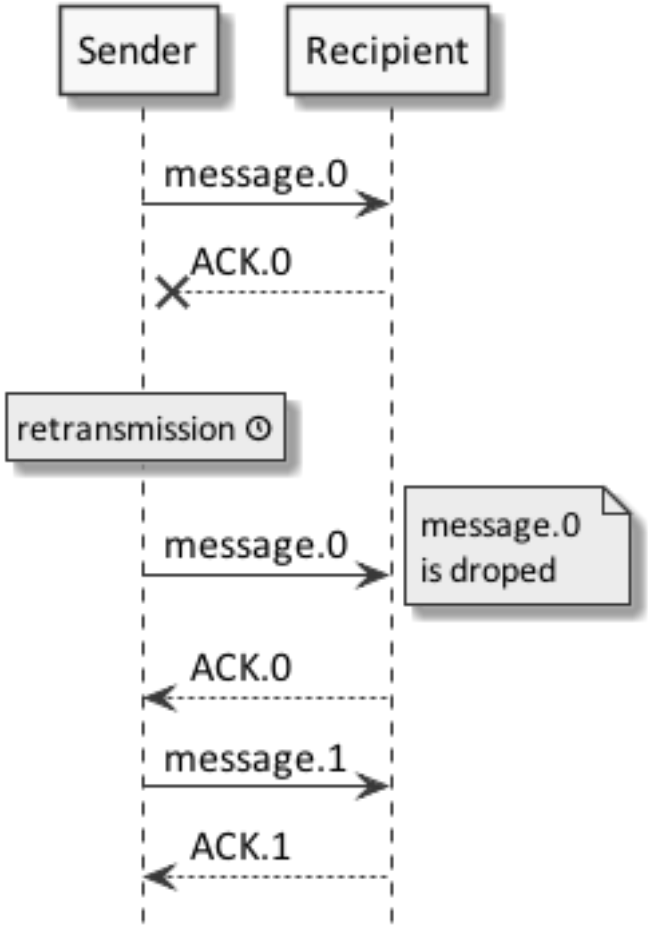
A retransmission can be too late – if long delay

- then forward error correction or even multiple-transmission of the same packet

Flow control – Send and Wait (Bit Alternate Protocol)

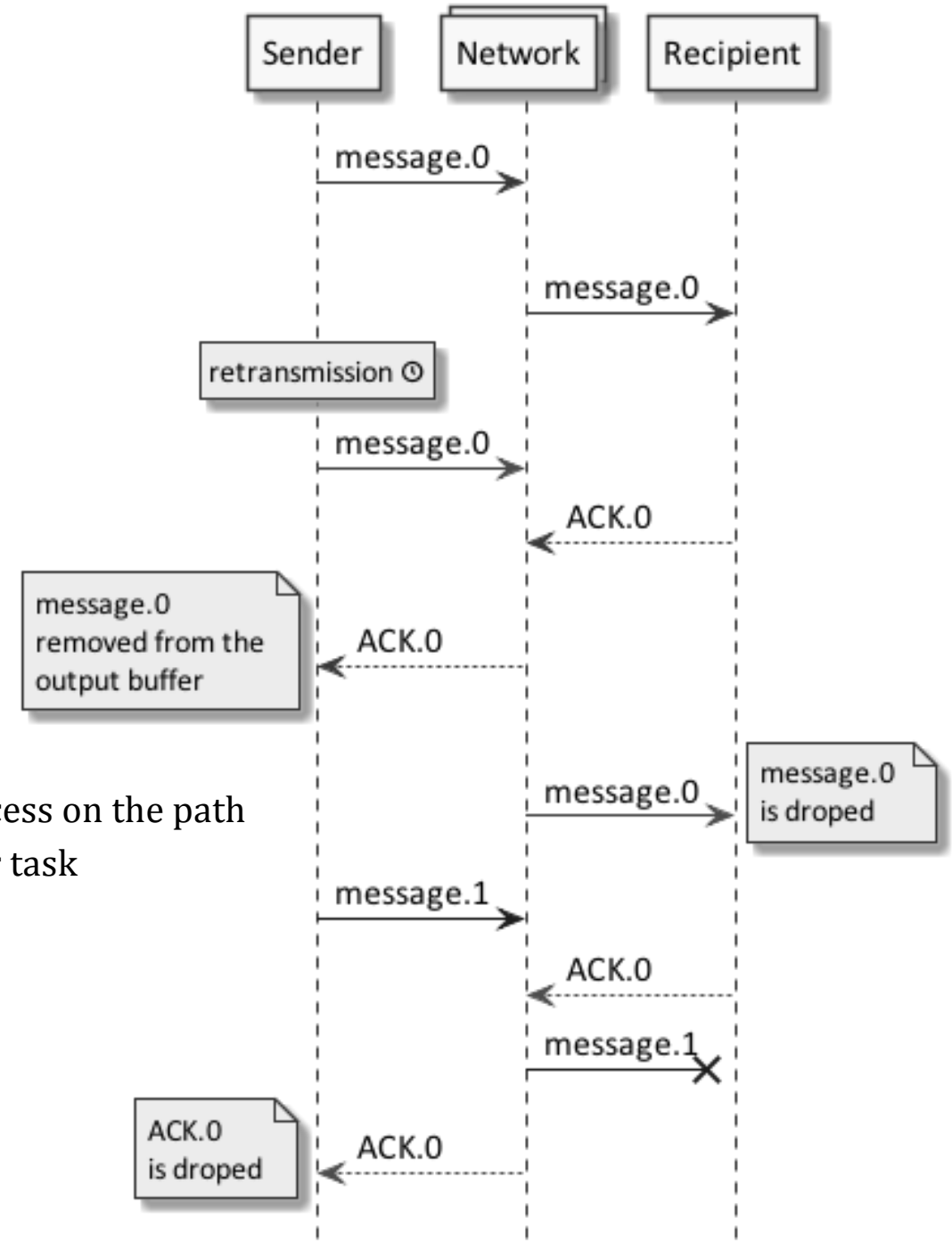
There is 1 output and 1 input buffer





This is why messages must be numbered

This is why
ACKs must be numbered



Reasons for ACK delay:

- Transmission time
- Signal propagation time
- Buffering time by every process on the path
- Recipient processed another task

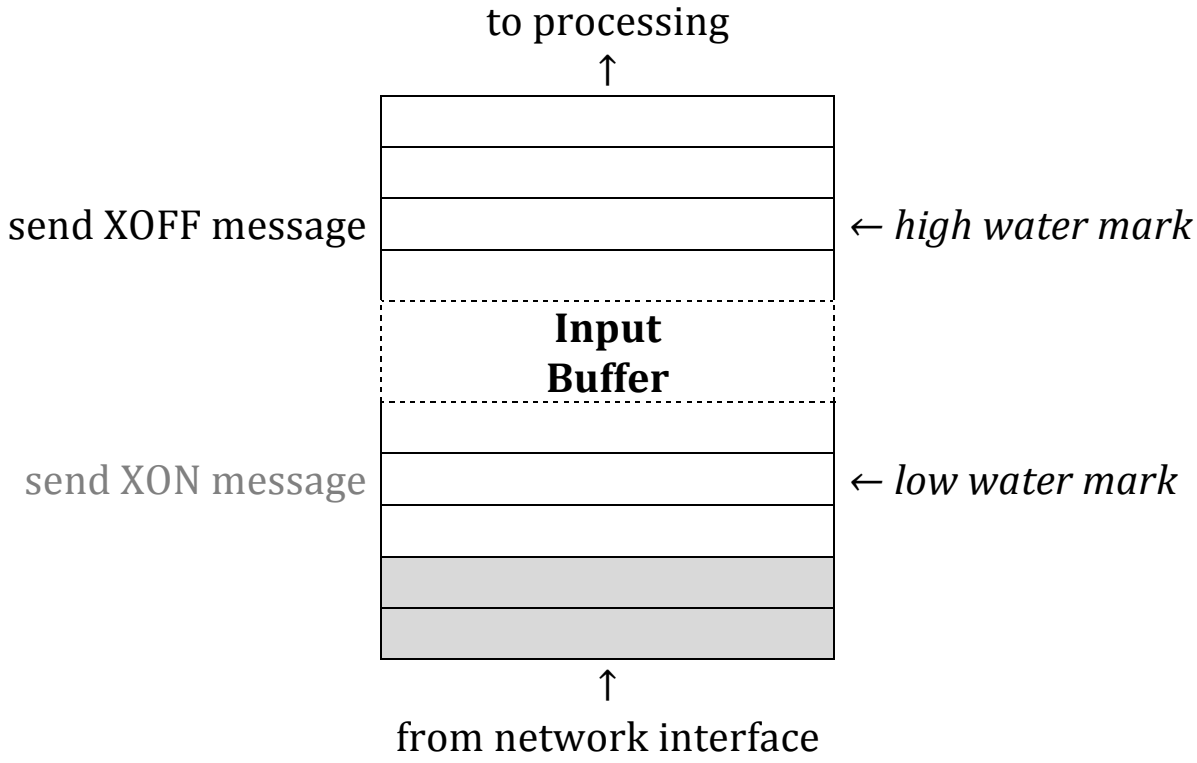
Messages are buffered by:

- operating systems
- communication hardware

Flow control – XON/XOFF Protocol

- Is efficient – while processing a message, the next are transmitted
- Do not guarantee message delivery (by itself)

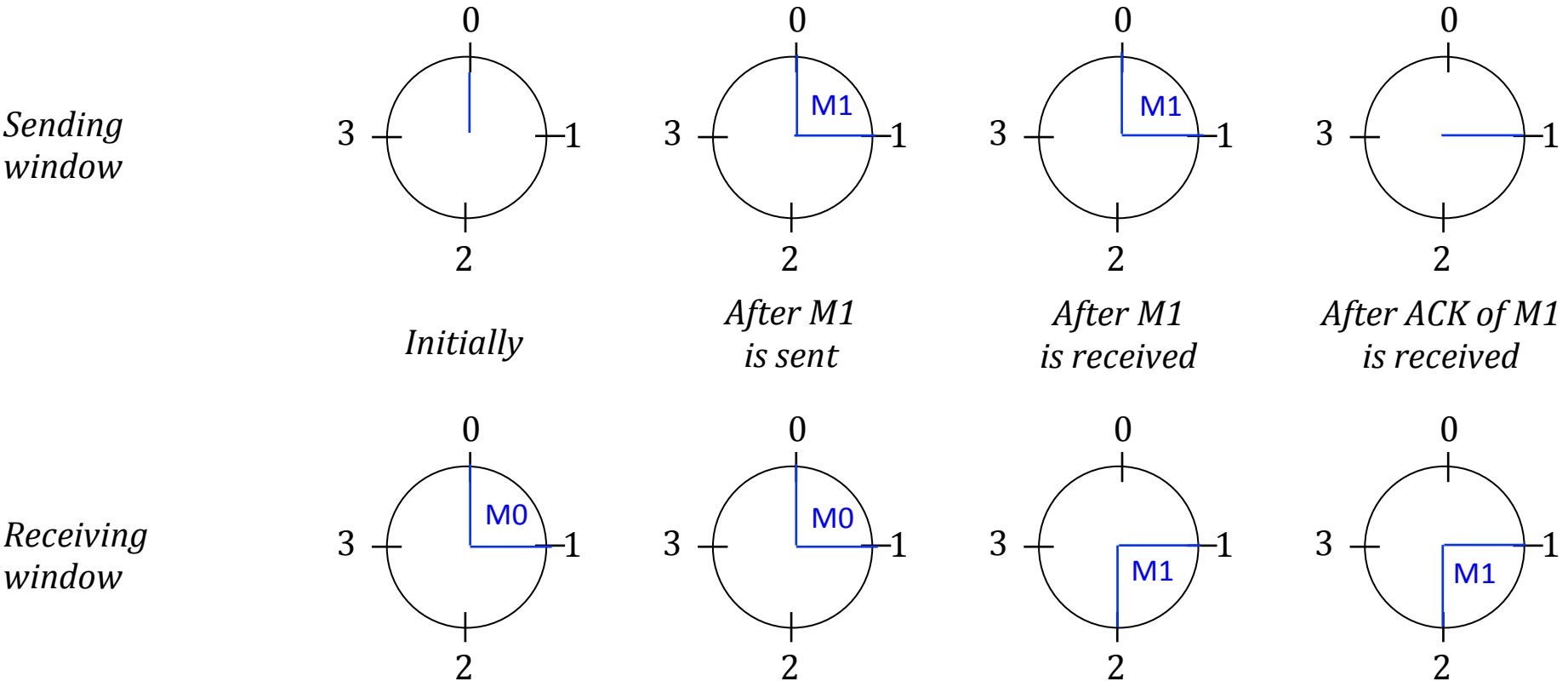
Input buffer can store N messages



A message size can be 1 byte

Flow control – Sliding Window Mechanism

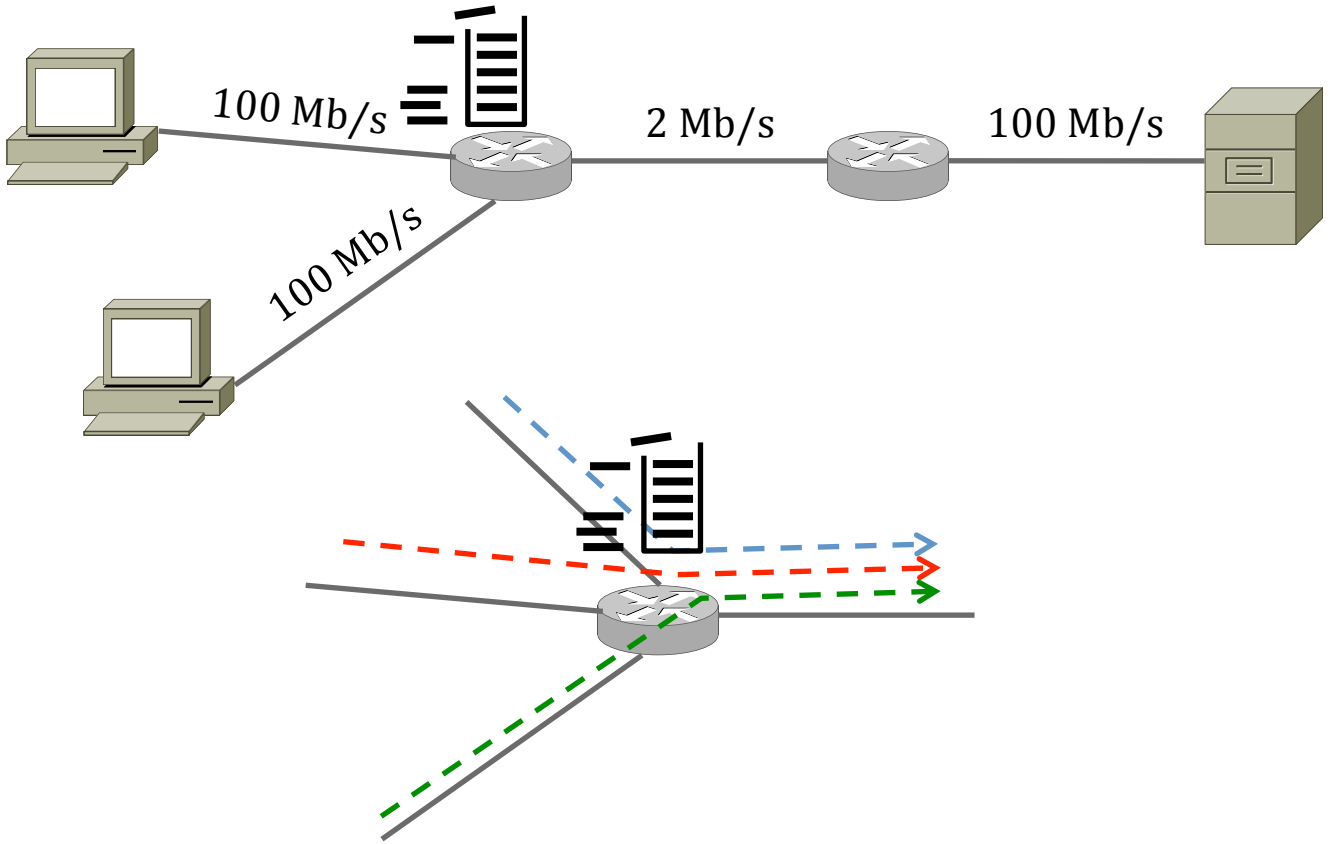
- Is efficient – while processing a message, the next are transmitted
- Guarantee message delivery



Parameters to be set: window size and number of messages to be sent without ACK

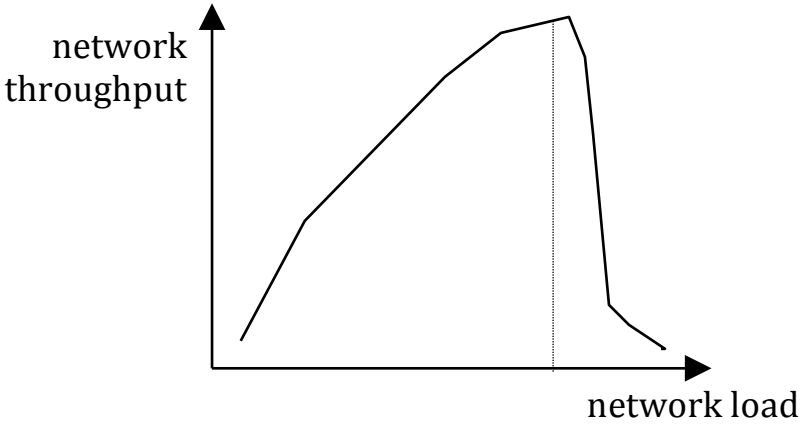
Network Congestion

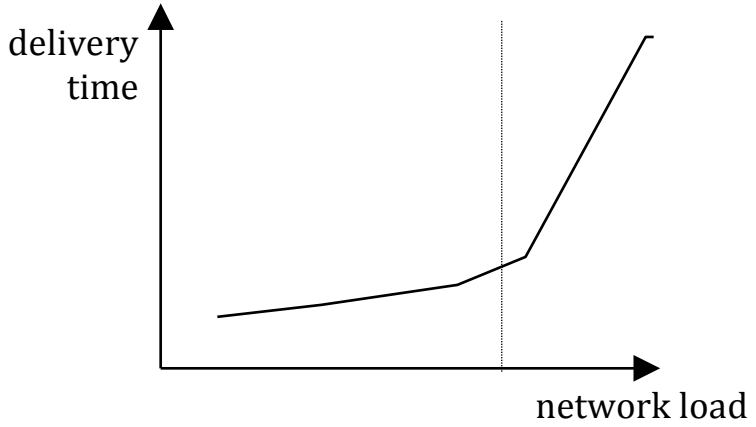
Source of the problem:

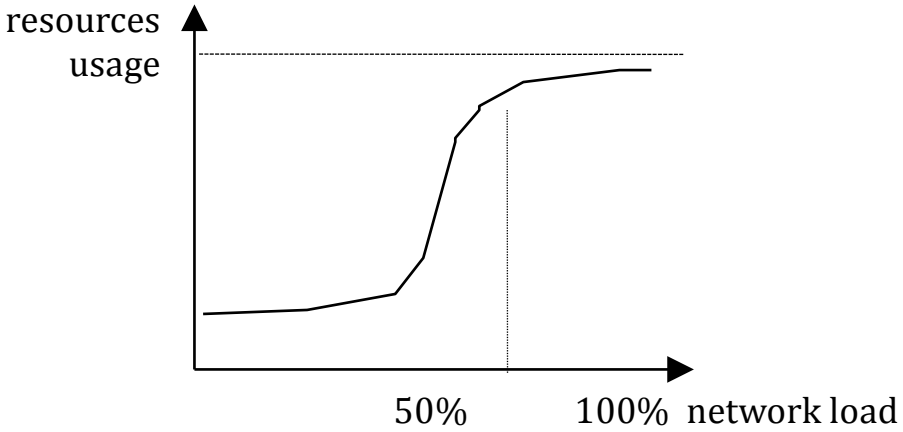


Retransmissions of dropped packets can lead to the *congestion collapse*

Effects of the Congestion Collapse







Communication suffers from

- queueing delay
- packet loss
- blocking of new connections

Techniques Used to Avoid the Collapse

- Congestion control – reactive
  helps the network to recover from the congestion state
  - exponential backoff
    - as in CSMA/CD Ethernet & Wi-Fi
  - transmission window reduction in TCP
  - explicit notifications
  - some queuing & scheduling mechanisms with active queue management

- Congestion avoidance – proactive
  allows a network to operate in the region of low delay and high throughput
  - admission control
  - some queuing & scheduling mechanisms

Packet Delay

Delay	Where	Example
Bandwidth	per-transmitter	Sending 1 Mb at 10 Mb/s will take 100 ms
Propagation	per-link	At twisted pair wire, coax, fibre: ≃ 2/3 of the light speed, thus ≃ 200 km/ms
Store-and-forward	per-switch	Transmission time of the frame
Queuing	per-switch	Generally less than 10 ms and often is less than 1 ms; at bad moments this can exceed 1 s
Total packet from sender to receiver	per-path	Sum of the above for each switch and link

Store-and-forward

– A switch receives entire packet, checks its CRC, and then decides to retransmit it

Fast-forward

– A switch receives header with addresses, and then decides to retransmit the packet

Summary

- Reliability problems & solutions
  - Bit error detection
  - Message repetition
  - Flow control mechanisms
    - Send and wait
    - Xon/Xoff
    - Sliding window
- Network congestion
  - Effects of the congestion collapse
  - Techniques used to avoid the collapse
- Packet delay

Questions

1. What are the causes of communication reliability problems?
2. What are the mechanisms used to make communication reliable?
3. Which frames are better long or short and why?
4. What size of frames is more efficient in transmission over noisy radio channels?
5. What size of frames is more efficient in transmission over reliable fibre cables?
6. What are pros & cons of positive and negative acknowledgements?
7. Under which conditions error-correcting codes or repeated frames should be used?
8. Why Bit Alternate Protocol is inefficient?
9. What is the aim of XON/XOFF protocol?
10. What for we define low and high water marks for data buffers?
11. Explain sliding window mechanism.
12. Why do we need congestion control and avoidance mechanisms?
13. Why the ring network topology is congestion resistant?
14. What techniques are used to avoid the congestion collapse?
15. What are the elements of total packet delay?
16. Explain the fast-forward technique.

Computer Networks

Lecture on

ARP, IPv4, ICMP, DHCP, IPv6, NAT

Plan of This Lecture

- ARP & RARP – Address Resolution Protocol & Reverse ARP
- IPv4
- ICMP – Internet Control Message Protocol
- DHCP – Dynamic Host Configuration Protocol
- IPv6
- ICMPv6
- NAT – Network Address Translation

ARP & RARP – Address Resolution Protocol & Reverse ARP

ARP answers to:

„What is the physical address
of a station with a given network address?"

RARP answers to:

„What is the network address
of a station with a given physical address?"

The questions are broadcasted to the LAN segment

ARP

Who is asking?

- Every node sending a network packet

Who is answering?

- Owner of the network address – if exists in the LAN
- Router – if the address do not belong to the LAN

Answers are collected in the ARP table See it with: `arp -a`

RARP

Who is asking?

- Diskless station during a booting process: – What is my network address?

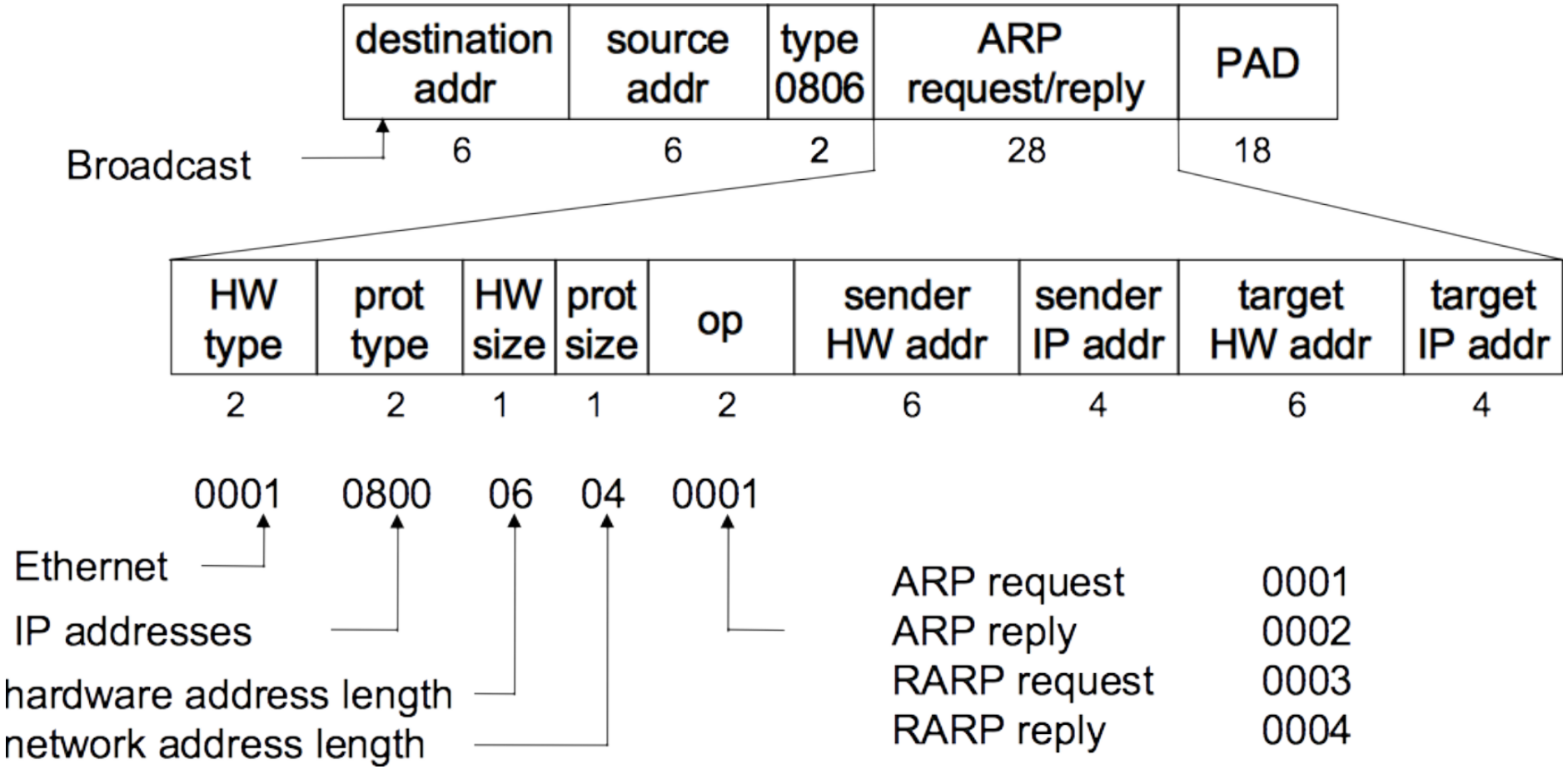
Who is answering?

- RARP server

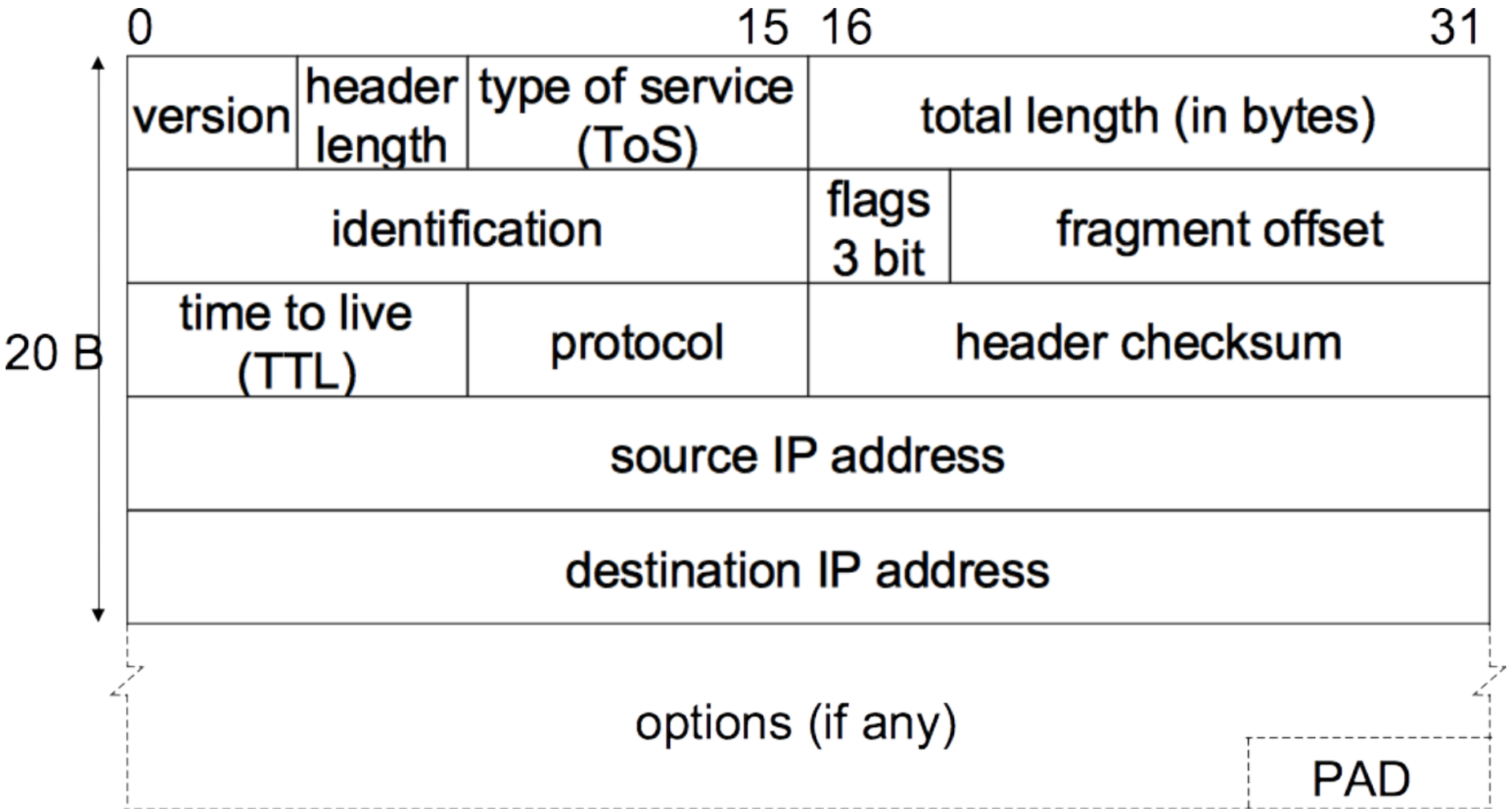
ARP & RARP were conceived for any kind of networks

They support any 2nd & 3rd layer protocols

PAD is needed to get the minimum payload size of 46 octets



IPv4


0
15
16
31
version
header length
type of service (ToS)
total length (in bytes)
identification
flags 3 bit
fragment offset
time to live (TTL)
protocol
header checksum
source IP address
destination IP address
20 B
options (if any)
PAD

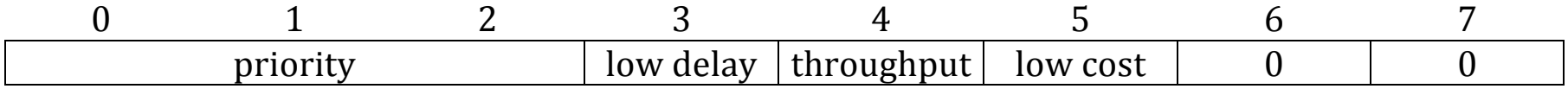
Version = 4

Header length = (5 + N) 32-bit words

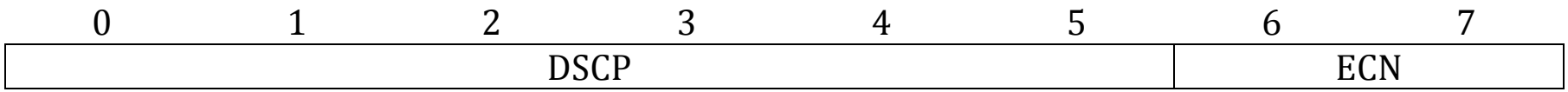
for this reason **PAD**ding can be needed

ToS – Type of Service

- originally defined as



- not used in most past networks
- in today's network it is replaced by



DSCP – Differentiated Services Code Point

specifies differentiated services (DiffServ)

– priorities assigned to well defined services

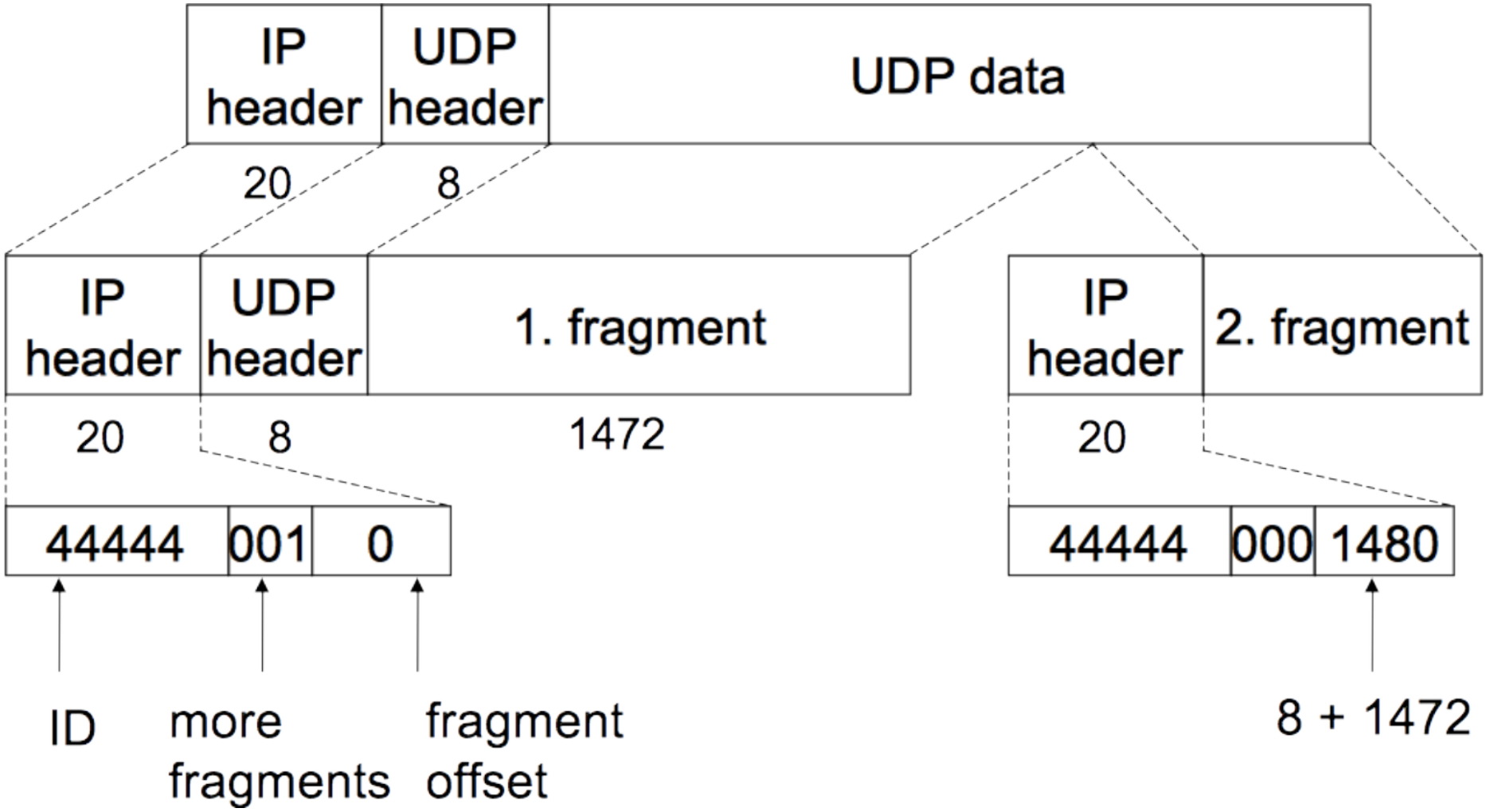
ENC – Explicit Congestion Notification

stamped by a congested router

Flags

- bit 0: Reserved; must be zero
- bit 1: Don't Fragment (DF)
- bit 2: More Fragments (MF)

IP fragmentation



Time-to-live

nowadays it is number of hops

every router decrement it by 1

if =0 then packet is dropped

Protocol

defines payload – what is the next header

e.g.: 6 – TCP, 17 – UDP, 1 – ICMP

Options

- rarely used
- for control, testing, probing, experimentation
- some considered as unsecure & are blocked by some routers, e.g.:
  - loose source routing
  - strict source routing

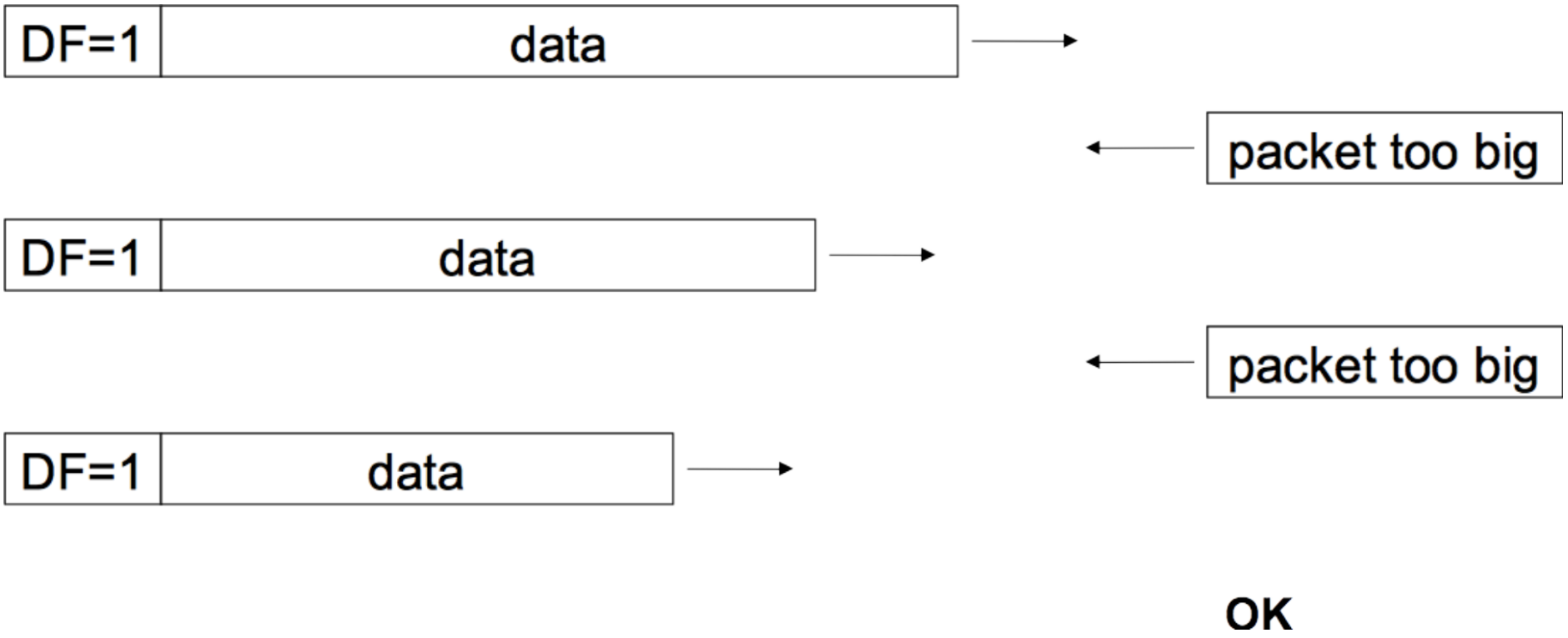
ICMP – Internet Control Message Protocol

Aim: self-recovery from errors in the network

PDU types:

- echo request, echo response Try: `ping host` host – IP addr. or domain name
- destination unreachable
- packet too big
- stop packet source
- need to change the route
- TTL expired
- error in the IP header
- timestamp request, timestamp response
- subnet mask request, subnet mask response
- router solicitation, router advertisement
- …

Path MTU Discovery



DHCP – Dynamic Host Configuration Protocol

Aim: to assign an IP address and other network configuration parameters to each device in the LAN

DHCP server delivers:

- IP address & mask – for the asking interface
- Other addresses
  - default router
  - DNS servers
  - time servers
  - WINS servers
  - ...
- Other parameters
  - Domain name
  - Host name
  - File server & path to the operating system for booting
  - ...

Examples of DHCP clients

- workstations
- lightweight WiFi access points
- IP phones
- ...

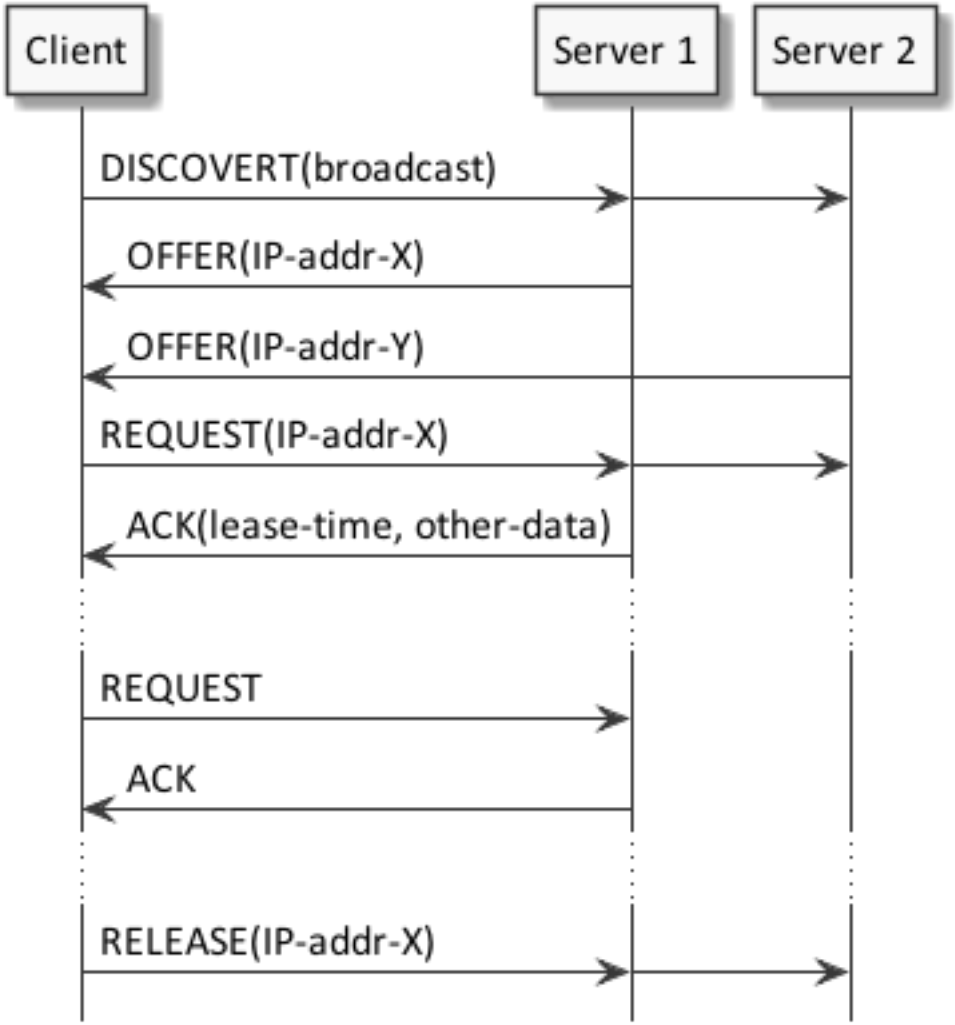
DHCP works over UDP

Address allocation methods

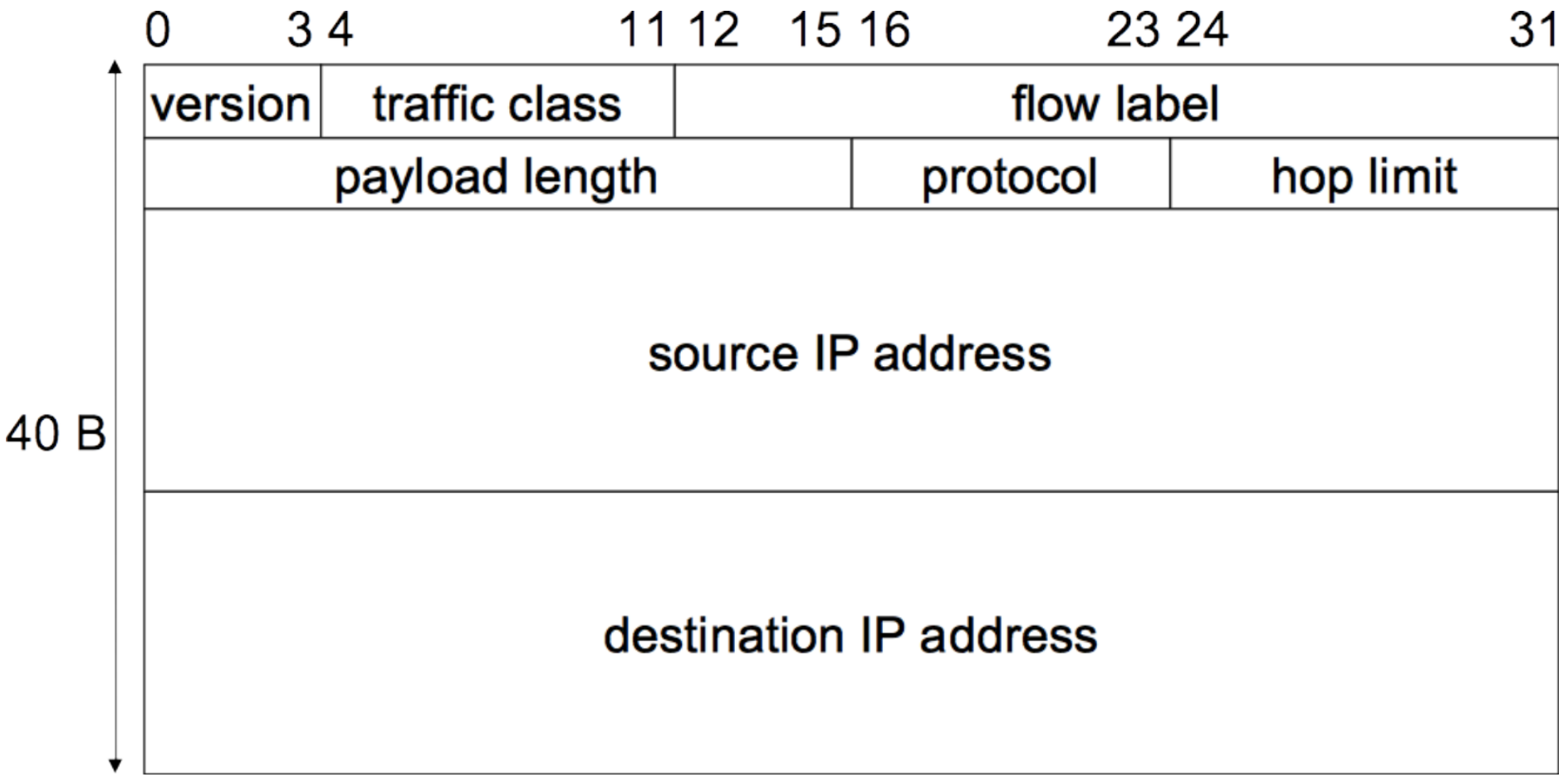
- Manually
  - MAC addr. to IP addr. mapping
- Automatically – permanently — e.g. for servers
  - from a given address range, set by an admin
- Dynamically – for a finite time (lease period) — e.g. for workstations
  - from a given address range, set by an admin
  - client may also request its last known IP address

After the lease period

- The address can be returned to the free addresses pool
  and allocated to the other client
- The client can also “refresh” the lease and retain the allocated address
- The client can be suspend from the network — e.g. after the end of a laboratory class


Client
Server 1
Server 2
DISCOVERT(broadcast)
OFFER(IP-addr-X)
OFFER(IP-addr-Y)
REQUEST(IP-addr-X)
ACK(lease-time, other-data)
REQUEST
ACK
RELEASE(IP-addr-X)

IPv6


0
3 4
11 12
15 16
23 24
31
version
traffic class
flow label
payload length
protocol
hop limit
source IP address
destination IP address
40 B

Version = 6

Header length is constant = 40 B

Traffic class

- 6 bits – Differentiated Services (DS) field
  - well defined priorities for known services
- 2 bits – Explicit Congestion Notification

Flow label – with src. addr. allow to recognize packet flows

- Routers can use it
  - to speed-up forwarding
  - to direct a flow via the same path

Main Features

- Huge address space
  - Optimistically around 4,000 trillions of addresses per 1 m^2 of the earth (considering different types of allocations)
  - Most pessimistically, at least 1,564 addresses per 1 m^2 of the earth
- End-to-end connectivity without NATs
- Efficient autoconfiguration – ad hoc & mobile networks
- Routers work faster
  - 1st header is simple and has constant length
  - No checksums
  - Simple subnetwork address aggregation
  - Flow label enables efficient packet processing

- Jumbograms
  - Can be as large as 4 GiB
  - Since both TCP and UDP include fields limited to 16 bits

    transport-layer tweaks are needed – RFC 2675
- Simple multihoming – access to the Internet via several ISPs
- Built in mobility mechanisms
- Built in security (IPSec)
- Header chain concept allows for future evolution
- Mechanism to co-work with IPv4 networks and to evolutionary migration from IPv4 to IPv6

IPv6 Addresses

Hierarchy of IPv6 addressing

64						64
# Regional Internet Registry	# ISP level 1	# ISP level 2	# ISP level N	# organization	# localization	# host

- Address autoconfiguration
  - Important for mobility & ad hoc networking
  - Stateless (obtained IPv6 prefix, own EUI-64 address)
    LAN submask has constant length = 64 bits
  - Stateless (obtained IPv6 prefix, randomly generated address)
  - Stateful – address from DHCPv6

- No broadcast addresses e.g. ARP broadcast load is replaced by ICMPv6 multicast
- Anycast addresses
  - Used by routing protocols, network security systems, …
  - Selected from the unicast address space
  - Assigned to more than one interface
    Typically belonging to different nodes
  - Routed to the nearest interface having that address
    According to the routing protocols' measure of distance
- Addressing scopes

unicast	**multicast**
loopback	interface-local
link-local	link-local
	realm-local
	admin-local
	site-local
unique-local	organization-local
global	global

IPv6 Header Extensions

IP options have been moved to a set of optional Extension Headers

Extension Headers are chained together and placed between IPv6 and transport layer headers

IPv6 Header Next = TCP H.	TCP Header	Application Data

IPv6 Header Next = Routing H.	Routing Header Next = TCP	TCP Header	Application Data

IPv6 Header Next = Security H.	Security Header Next = Fragmentation	Fragmentation Header Next = TCP	TCP Header	Application Data

IPv4 to IPv6 Transition Mechanisms

- Dual stack – supports both IPv4 and IPv6
  - Modern OSs do it

- Stateless IP/ICMP Translation translates packet header formats IPv6 ↔ IPv4
  - Address prefix ::ffff:0:0:0/96 ::ffff:0:a.b.c.d ↔ a.b.c.d
  - IPv4 net can connect 2 IPv6 nets
  - IPv6-only hosts can communicate with IPv4-only hosts

- Tunnelling – encapsulating IPv6 packets within IPv4
  tunnel broker is a service which provides a network tunnel
  - encapsulated within IPv4 packets using protocol number 41
  - encapsulated within UDP packets e.g. in order to cross a router or NAT device
  - use generic encapsulation schemes, such as AYIYA or GRE
  - SATAP – treats the IPv4 network as a virtual IPv6 local link
  - **Teredo** – an automatic tunnelling technique that uses UDP encapsulation
    (is claimed to be able to cross multiple NAT boxes)
  - **6in4** – configured tunnelling – used by enterprises

- Proxying and translation
  - dual-stack application-layer proxy
  - **464XLAT** allows clients on IPv6-only networks to access IPv4-only Internet services
    e.g. Skype
  - …

ICMPv6

Supports IPv6 addresses

Covers functionalities of diverse IPv4 related protocols and adds more, e.g.:

- ICMP
- ARP & RARP – here is called Neighbour Discovery Protocol
- Internet Group Management Protocol – here is called Multicast Listener Discovery
- Multicast Router Discovery
- …

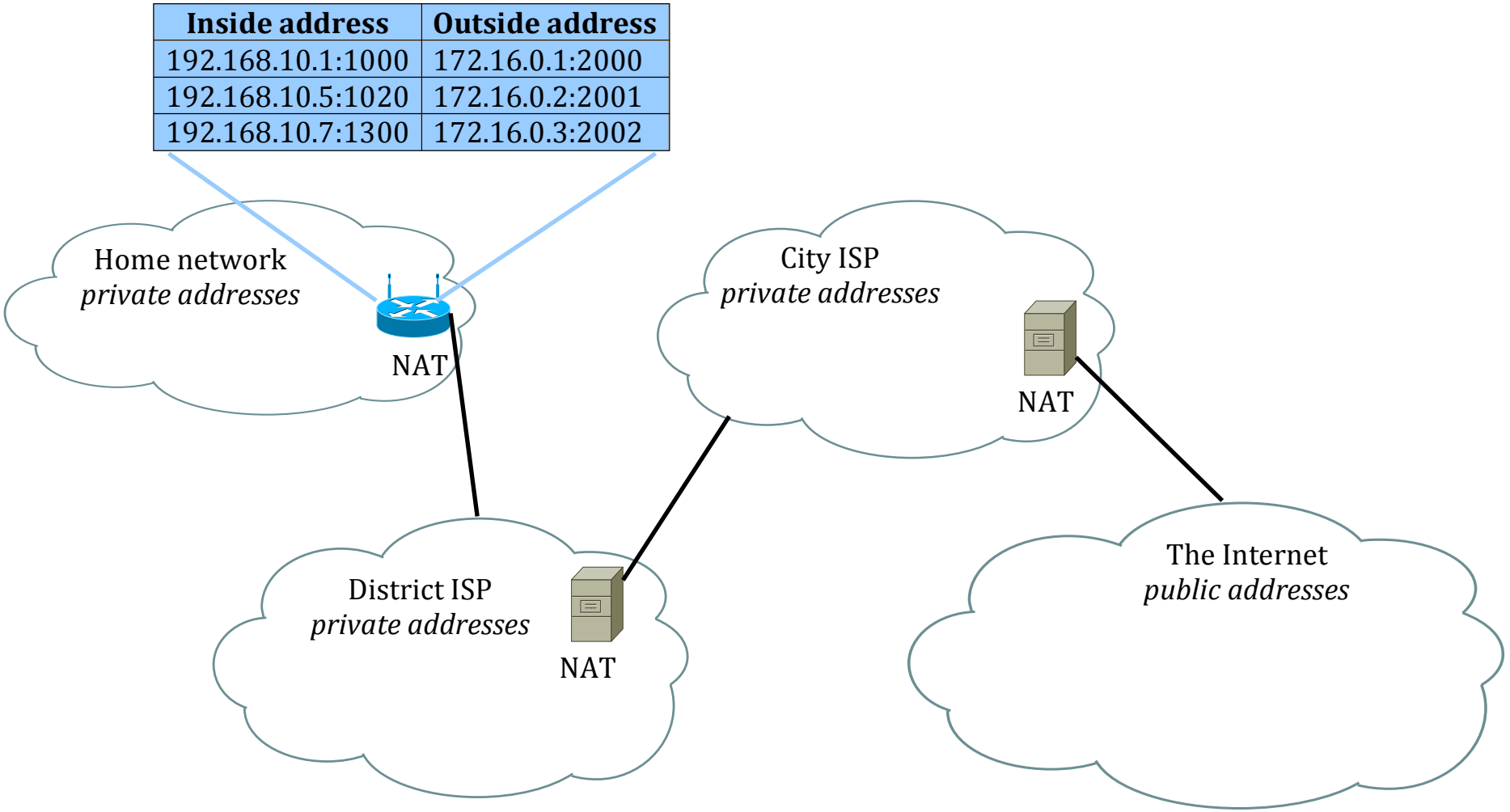
Try: `ping6 host`

NAT – Network Address Translation

- Conceived as a short term solution for IPv4 address shortage
- Enables hosts an a private network to communicate with hosts on the Internet
- IP addresses and possibly port numbers

  are replaced at the boundary of a private network
- NAT server has address translation table
- Often installed on routers

Example Chain of NAT Servers



NAT Problems

- Outside IP address pool is smaller than inside pool
- How long to keep a translation record?
  - Many protocols are connectionless
- How to deal with
  - protocols that do not carry a port number, e.g. ICMP?
  - protocols that carry embedded IP addresses or port numbers?
    - e.g. in order to redirect responses or queries
  - IP multicast?

NAT Advantages

- Public addressing space savings
- Elimination of need for LAN(s) readdressing when changing an ISP
- Elimination of need for ISP access readdressing when changing an ISP
- Local network security improvement is illusory
  even thought stated in many publications
  - Many attacks starts from internal network, from infected computers
  - Internal host which started communication with an outside one is visible from outside
    and can be attacked from outside
    - If it is not TCP communication, then if it ends, then the host is still visible until timeout
      – can be a few seconds

NAT Disadvantages

- Main Internet concept is broken – the same visibility of every communication point
  - difficulties for applications demanding full network visibility
    (e.g., IP telephony, network games) – mitting point or proxy servers are needed
  - difficulties with server placing behind NATs – dynamic DNS services are needed
  - difficulties with sensor networks placement
- NAT server is a bottleneck for network throughput
  - have to keep state of every connection
  - cannot support many servers on local side
    - many users want to expose theirs HTTP servers
  - implementation in hardware is impossible
- Battery save terminals (e.g., portable phones) cannot be placed behind a NAT
- Disable integrity verification of IP headers (IPSec)
- Application that use several ports usually needs a proxy installed on NAT server (e.g., FTP)
- Integration of two networks, which use the same private address space, is difficult

Summary

- ARP & RARP – Address Resolution Protocol & Reverse ARP
- IPv4
  - IP fragmentation
- ICMP – Internet Control Message Protocol
  - Path MTU discovery
- DHCP – Dynamic Host Configuration Protocol
- IPv6
  - Main features
  - Addressing
  - Header Extensions
  - IPv4 to IPv6 transition/coexistence mechanisms
- ICMPv6
- NAT – Network Address Translation
  - Problems
  - Advantages
  - Disadvantages

Exercises

Run in a terminal window the following commands and figure out the output

```
arp -a
ping -c3 www.qzhu.edu.cn
ping6 -c3 en.wikipedia.org
traceroute www.ii.pw.edu.pl
```

Take a look into `man tcpdump`

To do the following exercises, you need to have the root permissions

1st terminal window	2nd terminal window
Run `sudo tcpdump -vl icmp` Observe and explain the output Stop it by pressing Ctrl-C	Run `ping -c1 www.qzhu.edu.cn`
Run `sudo tcpdump -vl icmp6` Observe and explain the output Stop it by pressing Ctrl-C	Run `ping6 -c1 en.wikipedia.org`

Questions

1. What for a host uses ARP and RARP (Reverse Address Resolution Protocol)?
2. How does ARP (Address Resolution Protocol) work?
3. What for is the hop count field in the IP header?
4. What for is the protocol field in the IP header?
5. What for is the Type of Service / Traffic Class field in the IP header?
6. What is the aim of the Time to Live field in IPv4 header (hope limit in IPv6)?
7. What is the aim of ICMP?
8. What for a host uses DHCP (Dynamic Host Configuration Protocol)?
9. How many DHCP servers can work in a network segment?
10. What are main advantages of IPv6?
11. What is it anycast address, and for what is it used (example of applications)?
12. What are the purposes of local-link and unique local IPv6 addresses?
13. Mention principal transition mechanism to use IPv6 in IPv4 world.
14. What is the IPv6 tunnel broker service?
15. How an IPv4 address is mapped into IPv6?
16. What is the difference between ICMPv4 and ICMPv6?
17. Why is better to process fragmentation/defragmentation on terminal devices than on routers?
18. What was the reason for introduction of NAT (Network Address Translation) into Internet?
19. What are main disadvantages of NAT?

Computer Networks

Lecture on

Routing

Plan of This Lecture

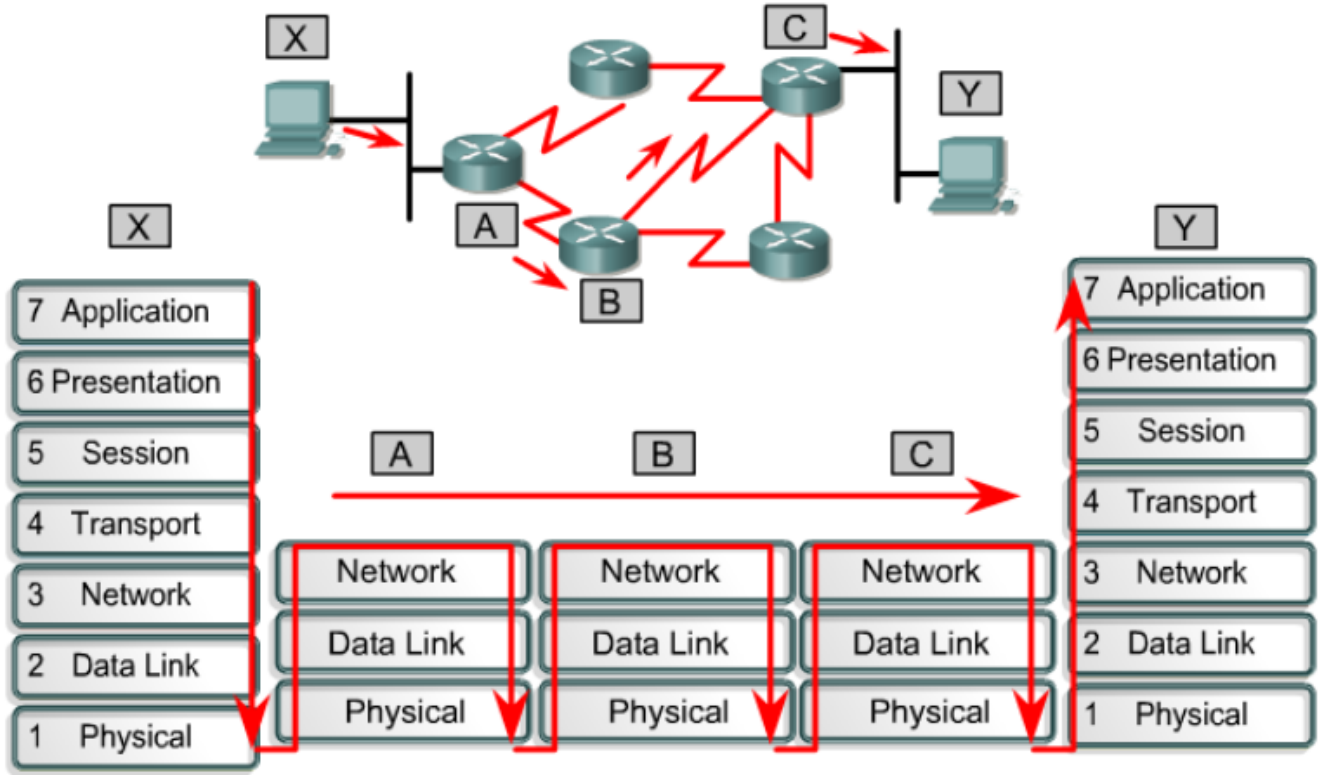
- Terminology
- Mechanisms
- Protocols

What is Routing?

Process of selecting an **optimal** data path through a network,
from sender to recipient

Metrics in routing

- Hop count
- Bandwidth
- Delay
- Load
- Reliability
- Cost
- ...



Different protocols use different metrics

Routing Taxonomies

static	vs.	dynamic
interior	vs.	exterior
distance-vector	vs.	link-state
classfull	vs.	classless
reactive	vs.	proactive
single-path	vs.	multipath
flat	vs.	hierarchic

Routing protocols route routed protocols

- routed (routable) protocols – forward data
- routing protocols – maintain routing tables

Static vs. Dynamic Routing

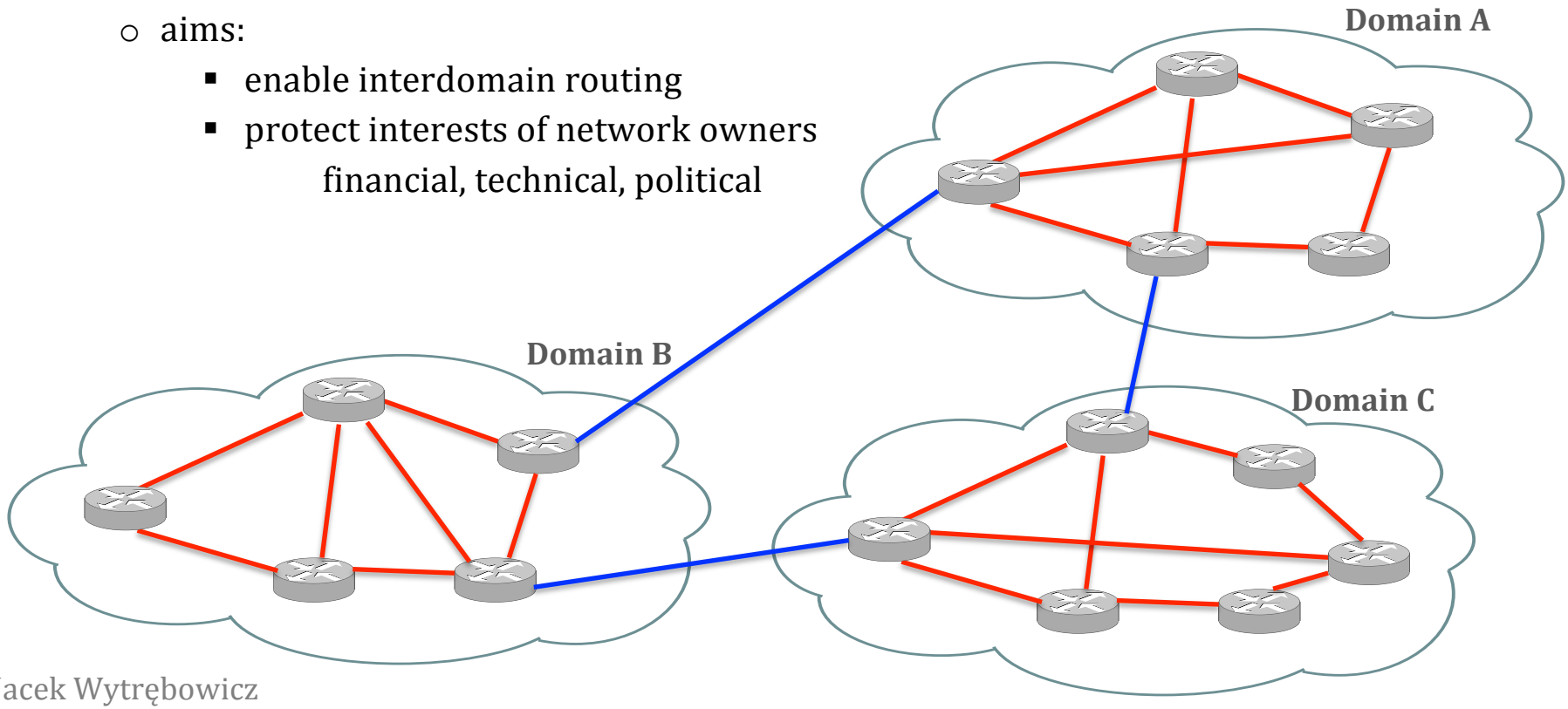
- Static
  - More predictable
  - Less load to the network
  - Can be used in a small network
    - highly secure network — e.g. a military one
    - to minimize energy consumption — e.g. in fixed sensor network

- Dynamic
  - Automatically adjust to changes in topology and load
  - Commonly used

IGP vs. EGP Routing

AS Autonomous system – administrative domain

- IGP Interior Gateway Protocols (Intradomain)
  - inside the AS
  - aim – efficient updating of routing tables
- EGP Exterior Gateway Protocols (Interdomain)
  - between AS's
  - aims:
    - enable interdomain routing
    - protect interests of network owners
      financial, technical, political



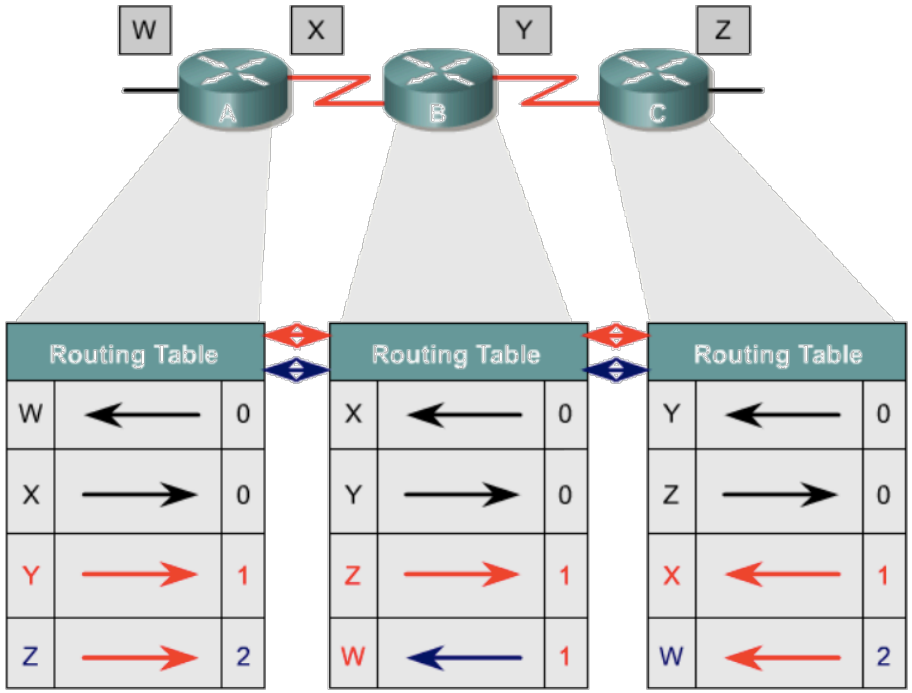
Distance-Vector vs. Link-State Protocols

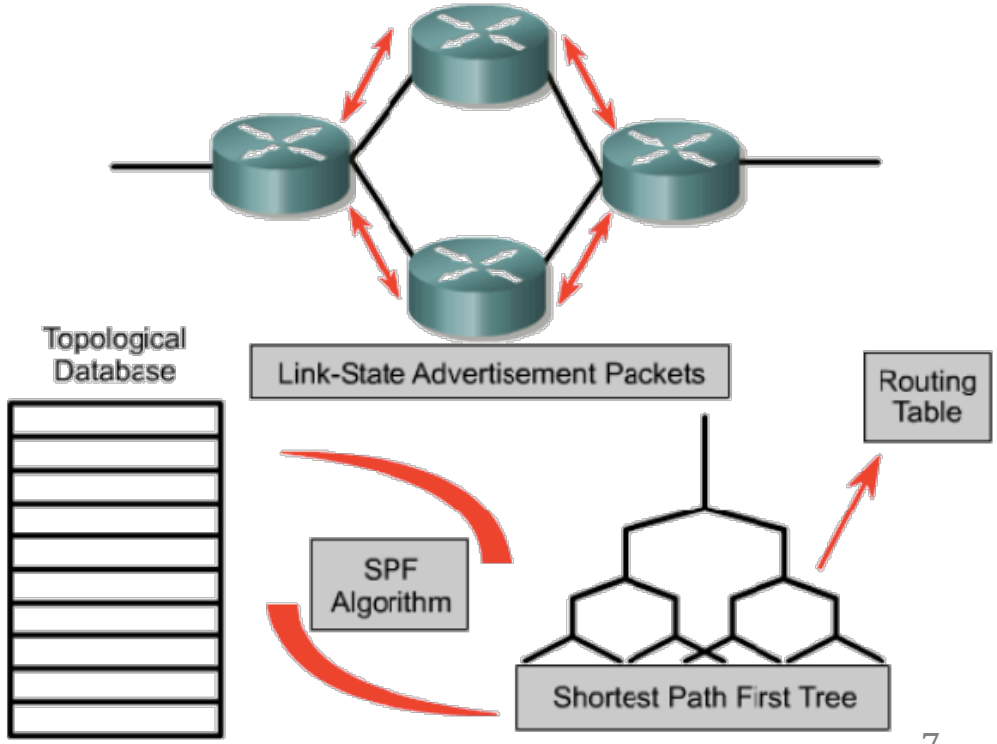
Distance-Vector

- about the neighbours
- to neighbours
- only distance
- ~ periodically
- simple
- slow-converging

Link-State

- about whole topology
- to all routers
- link state
- ~ after changes
- complex
- fast-converging





Reactive vs. Proactive

- Reactive – routers discover a path when it is needed
  - mobile ad hoc radio networks (MANETs) aka. wireless ad hoc networks (WANETs)
    e.g. Ad Hoc On-Demand Distance Vector (AODV) RFC 3561
- Proactive – routers discover all paths in advance
  - fixed cable and radio networks
- Hybrid – both proactive and reactive
  e.g. Hybrid Wireless Mesh Protocol IEEE 802.11s

Other Routing Types

Classfull vs. Classless

- Classfull – routers recognize subnet addresses by IPv4 address prefix
  - no more in use
- Classless – routers recognize subnet addresses by subnet mask value

Single-path vs. Multipath

- Multipath – routers discover two or more paths for each pair of end-points
  - for fast rerouting in case of failure
  - for higher transmission efficiency

Flat vs. Hierarchic

- Hierarchic routing is a must for big networks – provides scalability

Router Internals

Routers tasks

- Forwarding packets to the recipient
- Maintaining routing tables
- Informing other routers about changes in:
  - network topology
  - link states

Routing table content

- Source (routing protocol)
- Prefix (destination network, network mask)
- Outgoing interface / next hop
- Administrative distance
- Metrics

Routing table on PCs

`netstat -r` (Unix, MS Windows)

`route print` (MS Windows)

`nslookup`

`nettop -r`

`netstat -nr -f inet` – shows the existing routing table (IPv4 only)

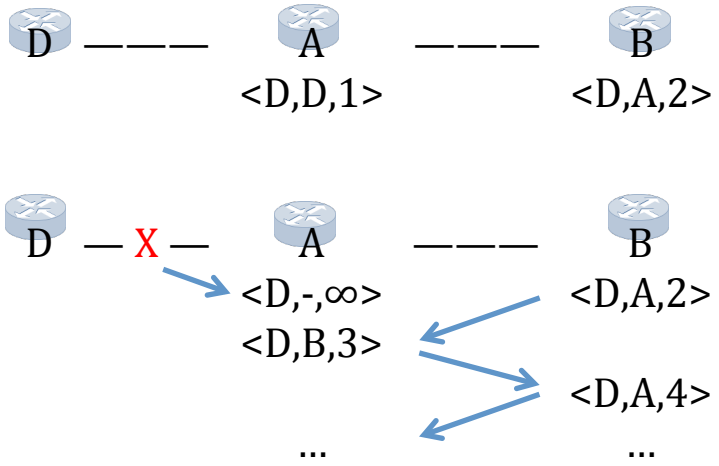
`route get HOSTNAME_OR_IP` – shows how a specific host will get routed

Desirable Features of Routing Protocols

- Quality of route optimization
- Simplicity
- Little overhead
- Robustness and stability, e.g.
  - Support for multipath routing
  - Support for different forward and backward paths
- Flexibility
- Fast convergence

Distance-Vector Slow-Convergence Problem

How a loop can arise:



Hold down – the simplest solution

- Do not use & advertise new alternative routes for two router-update cycles
- Widely adopted for small networks (RIP)
- Legitimate new routes are also delayed – disadvantage

Originator sequence number

- Vector contains a sequence number issued by the router directly connected to the subnet

Equal-Cost MultiPath Routing

Two or more routes of the same cost can be calculated and used by each router
i.e. more than 1 output interface is used to reach a given destination

- Most routing protocols support ECMP
  - administrator can enable and configure it
- Equal-cost ≠ equal-propagation-delay
- Round-robin
  - per-packet
    - better load-balancing between the paths
  - per-flow
    - TCP friendly
- Variants for radio networks
  - link-disjoint paths
  - node-disjoint paths

Most Popular Routing Protocols

- RIP Routing Information Protocol
- EIGRP Enhanced Interior Gateway Routing Protocol
- OSPF Open Shortest Path First
- IS-IS Intermediate System-to- Intermediate System
- BGP Border Gateway Protocol

There are numerous routing protocols for radio networks

	IGP	**EGP**
Distance-Vector	RIP	BGP
Hybrid	EIGRP	
Link-State	OSPF IS-IS	

All of them evolve

RIP

Main features

- Interior gateway protocol
- Open standard from IETF
- Distance-Vector
- Simple
- Metrics: hop count
- Broadcasts every ~30 s content of the routing table
  - Random delay eliminates risk of message synchronization
    i.e. all routers exchange tables at the same time
- Little max. hop count (15)
- One RIP message can carry up to 20 route entries – for IPv4 or IPv6 subnets
- Slow convergence (minutes)
- For little networks

EIGRP – Enhanced Interior Gateway Protocol

- Interior gateway protocol
- Once-proprietary Cisco protocol RFC 7868 in 2016
- Hybrid (distance-vector and link-state features)
- Max hop count: 224
- No risk of routing loops
- Flexible but complex 32-bit metrics
- Fast (because of backup routes)
- Mainly used in enterprise networks
- Metrics

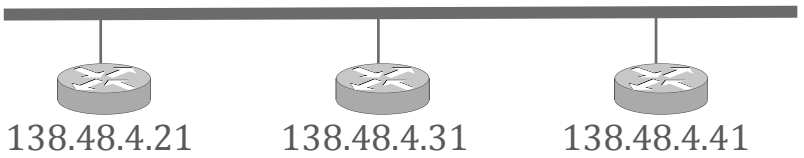
  [K1*bandwidth + (K2*bandwidth)/(256-load) + K3*delay] * [K5/reliability + K4]

  - Weighting constants K1-K5 (for tuning)
  - Default: K1=1, K2=0, K3=1, K4=0, K5=0
    thus: [Bandwidth, +Delay]

OSPF – Open Shortest Path First

Main features

- Interior gateway protocol from IETF
- Open standard
- Link-state
- Hierarchical architecture – areas
- Scalable
- Designated Routers on multi-access segments – DR represents its segment
  - minimize the number of routing messages
  - failure of the bus is processed correctly
- Areas allow for
  - summarization
  - containment of changes propagation
  - ⇒ scalability



- Frequently used in enterprise networks and in many ISP networks

OSPF – Basic Concepts

- Area
  - set of routers sharing the same knowledge
  - backbone area (#0)
  - non-backbone areas (#!0)
  - path between 2 non-backbone areas must pass by the backbone area
- Cost
  - feature of a link
- Adjacency database
  - contains information about all directly connected neighbours
- Topological database
  - detailed info about all routers and links in the area
  - summarized info about other areas and external networks – by distance vectors

OSPF – Operation

↓ Hello packets

- Adjacency database

↓ Initial Database Exchange

↓ Link state updates by flooding

- Topology database

↓ Dijkstra algorithm

- Shortest path first tree

↓ Best path selection

- Routing table

IS-IS Intermediate System-to-Intermediate System

Open standard from ISO

IS-IS & OSPF do the same

- Both establish a two level hierarchy among the areas
- Both have similar stability and convergence properties.
- Differ in many aspects, e.g.: tuning parameters, timeouts, data structure size & granularity
- Main differences:

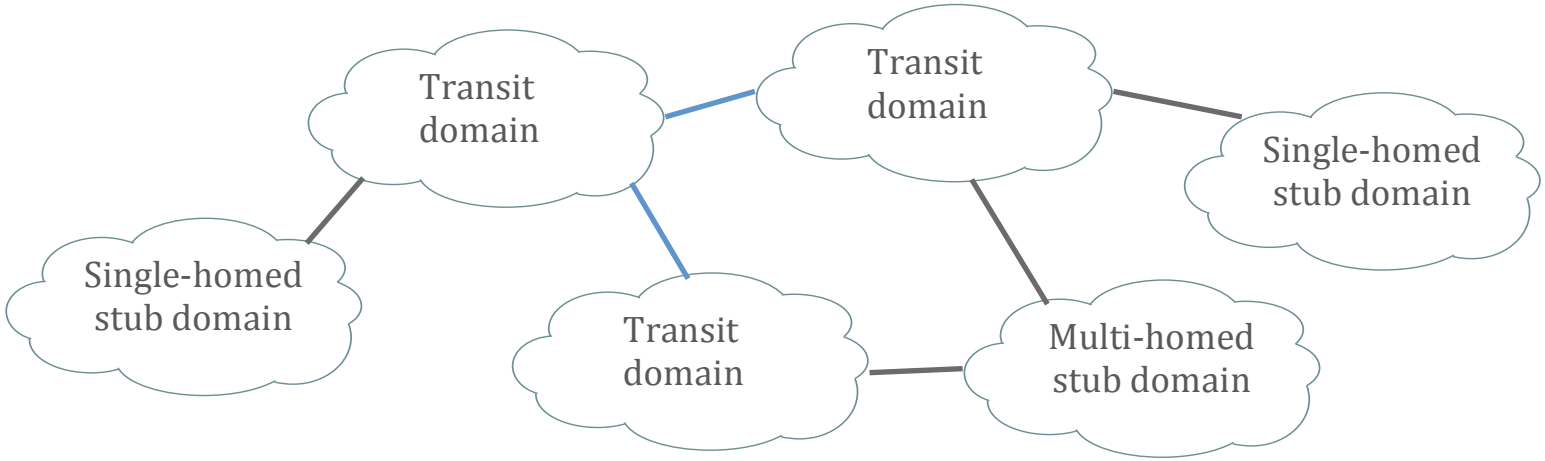
IS-IS	OSPF
Designed for any kind of networks • uses Type-Length-Value encoding	for IPv4 later IPv6
Works over data-link layer e.g. Ethernet • uses short messages • resistant against IP level attacks	over IP • can profit from IP fragmentation • can use virtual links
Area boundaries intersect on links	on routers

Large ISPs prefer IS-IS than OSPF

Autonomous Systems

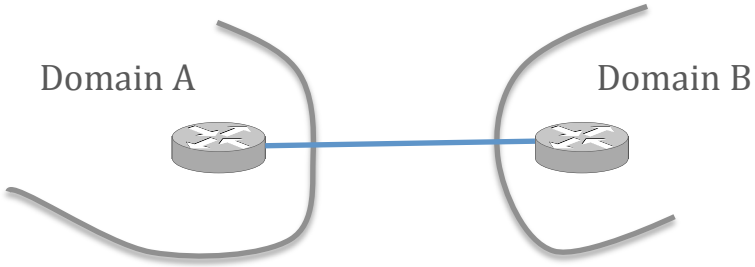
- Set of networks with a common administrative policy
- Seen from outside as a „black box”
- AS numbers are assigned by IANA & next by RIRs

Total number of active AS domains 63 520 April 2019
source: http://www.potaroo.net/tools/asn32/



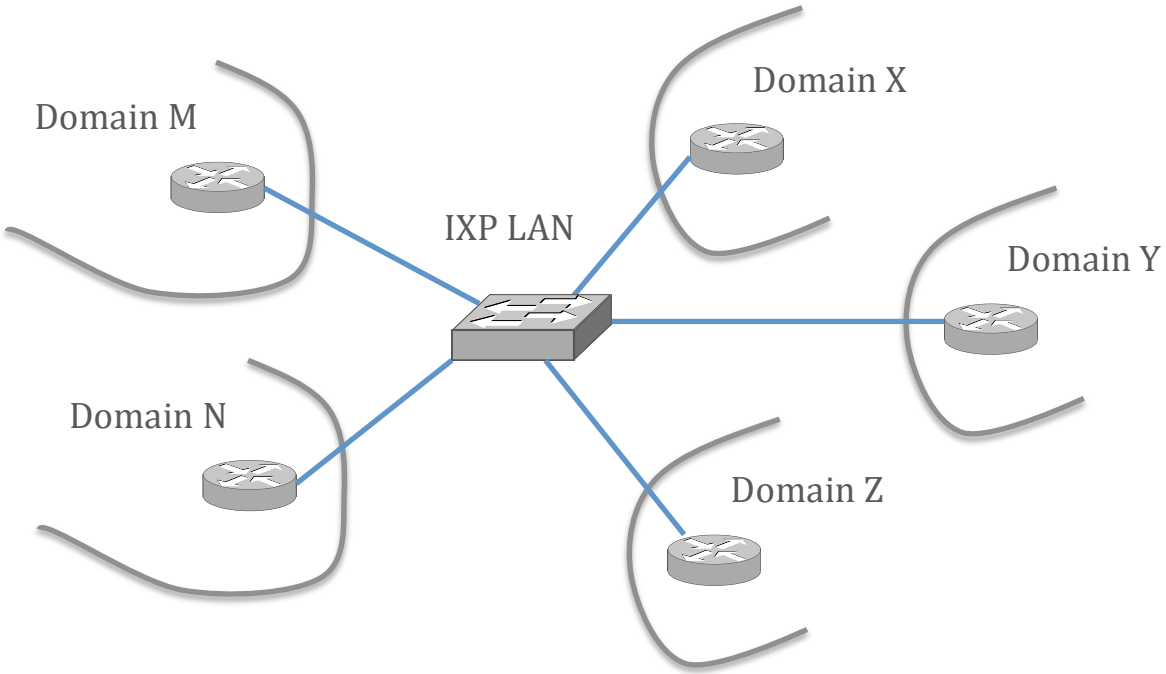
Domain Interconnections

- Private link



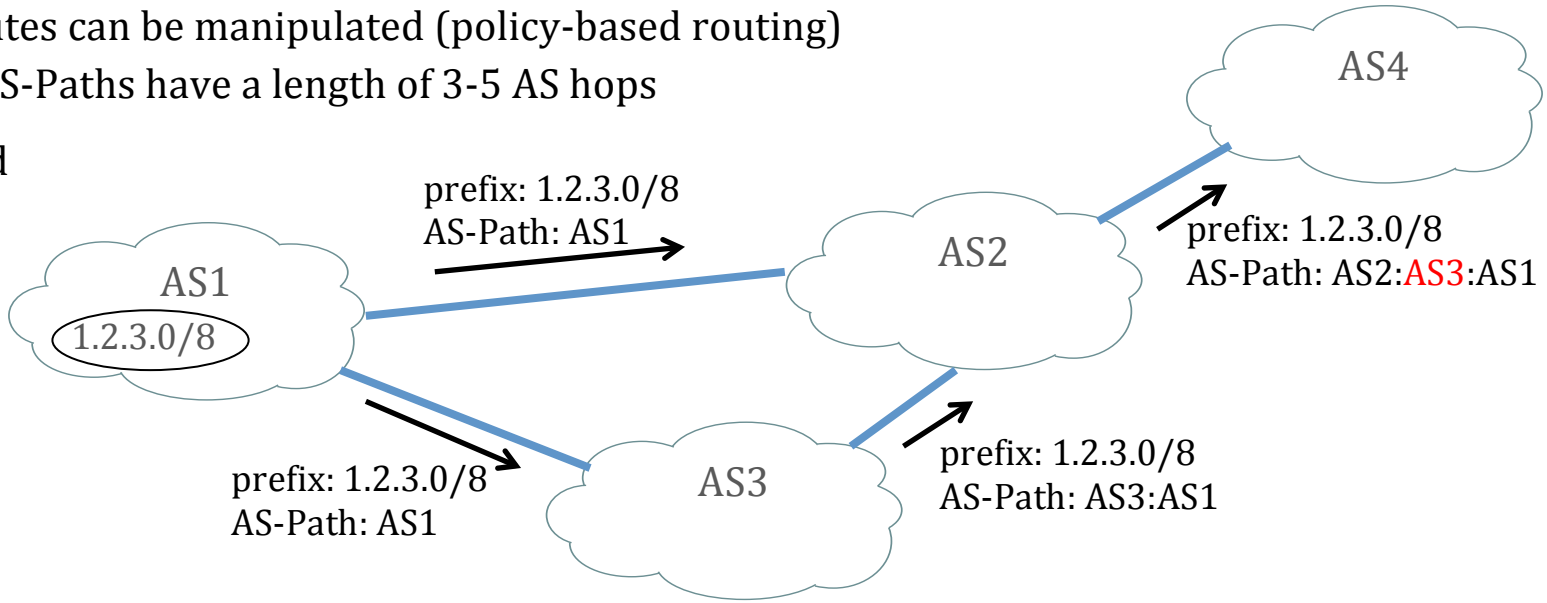
- Internet eXchange Point

  Datacentre hosting routers belonging to many domains – tens, hundreds



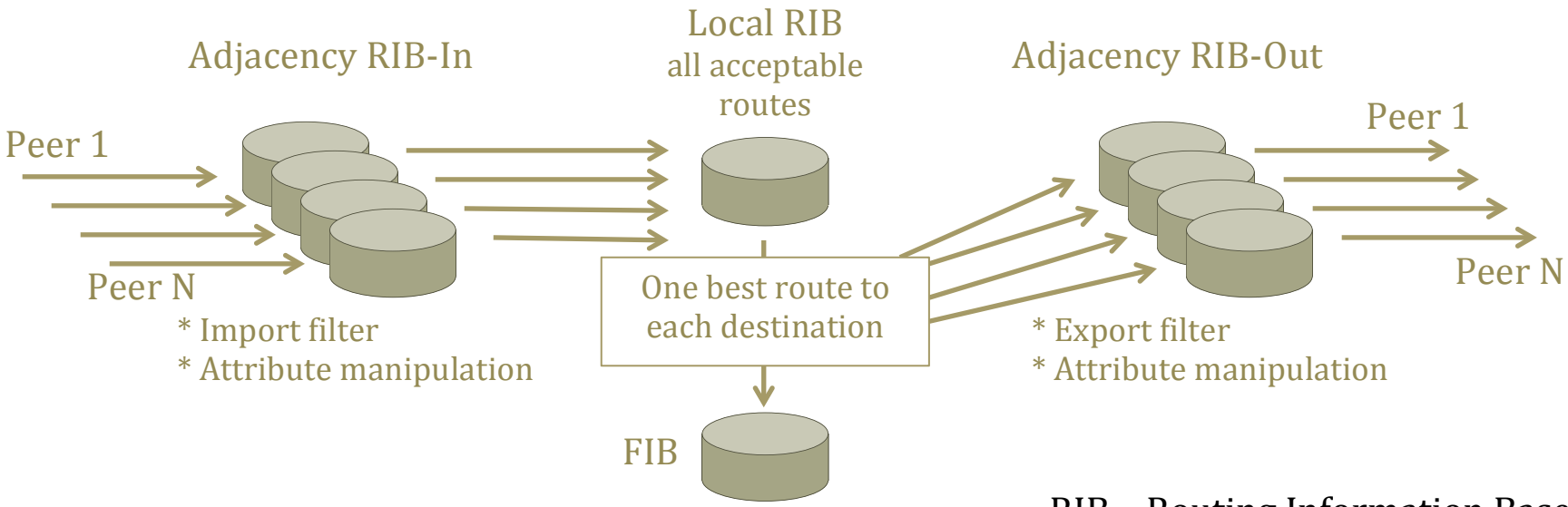
Border Gateway Protocol

- The sole Exterior Gateway Protocol used in the today's Internet
- Path-Vector
  - BGP path: a sequence of autonomous system numbers
  - Path attributes decide on route selection order
  - Attributes can be manipulated (policy-based routing)
  - Most AS-Paths have a length of 3-5 AS hops
- Policy-based



- Reduces transit traffic – according to defined policies

- Databases

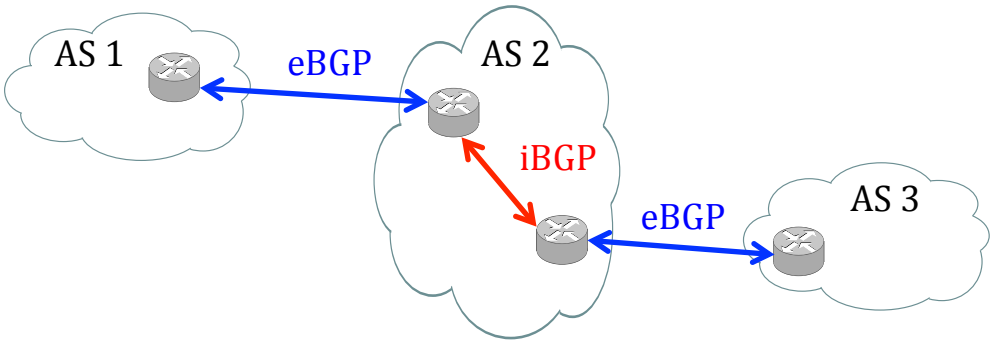


RIB – Routing Information Base

FIB – Forwarding Information Base

- Scalable
  - Incremental updates – it only announces the routes that have changed to its neighbours
- Update message
  - list of IP prefixes that are withdrawn
  - list of IP prefixes that are (re-)advertised
  - set of attributes (e.g. AS-Path) associated to the advertised prefixes
- Keep-alive message every 30 s

- Internal BGP carries
  - AS-paths and their attributes
  - only those allowed for transit



- Route aggregation (summarization)
  - With aggregation:
    - Neighbouring networks described with a single entry
    - Router knows details about it's directly connected networks
      the other routers – don't
  - Without aggregation:
    - Every network / subnetwork described with separate entries

- Route selection – complicated!
  - no metrics as in IGP

- Administration – complicated!
  - Route Policy Specification Language
    Several tools help to easily convert a RPSL policy into router commands
  - Inattentive configuration can lead to oscillation of routes

Summary

- What is Routing?
- Routing taxonomies
  - Static vs. dynamic routing
  - IGP vs. EGP routing
  - Distance-Vector vs. Link-State Protocols
  - Reactive vs. Proactive
  - Other routing types
- Router internals
  - Desirable features of routing protocols
  - Distance-Vector slow-convergence problem
  - Equal-cost multipath routing
  - Most popular routing protocols
- RIP
- EIGRP
- OSPF
  - OSPF – basic concepts
  - OSPF – operation
- IS-IS
- Autonomous Systems
  - Domain interconnections
- Border Gateway Protocol

Questions

1. What are the functionalities of routing protocols?
2. Give a short classification of routing protocols.
3. What metrics can be used by a routing protocol?
4. Characterize Distance-Vector and Link-State routing.
5. What kind of networks uses reactive routing protocols?
6. What metrics are possible in configuration of EIGRP?
7. What are the important features of the OSPF protocol?
8. How scalability is achieved by OSPF?
9. Why convergence of OSPF is much faster than convergence of RIP?
10. Why fast failover is possible in an OSPF cloud?
11. What are the main differences
12. Why RIP, OSPF and EIGRP are not suitable for radio ad hoc networks?
13. In which kind of networks are RIP, EIGRP, OSPF and IS-IS mainly used?
14. What is Internet eXchange Point?
15. What does it mean that BGP is a path-vector protocol?
16. What is the difference between EBGP and IBGP routers?
17. What databases does BGP router contain?