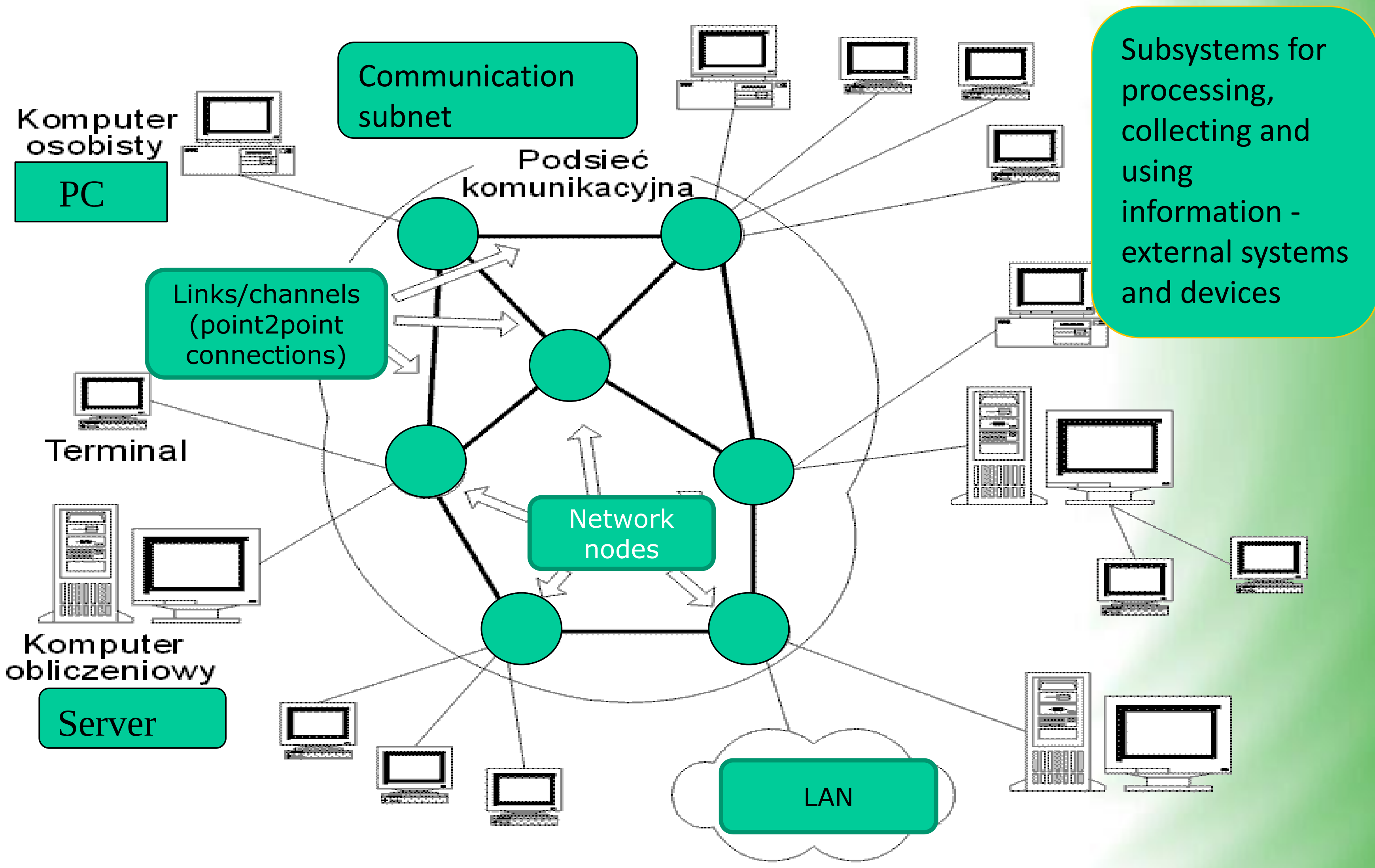
Computer networks

WAN networks
IP networks
Routing concepts (IGP type)
IP addressing schemes

Józef Woźniak
Katedra Teleinformatyki
Wydział Elektroniki, Telekomunikacji i Informatyki
Politechniki Gdańskiej
jowoz@eti.pg.gda.pl

POLITECHNIKA
GDAŃSKA

An exemplary structure of a computer network



Basic features of WAN networks

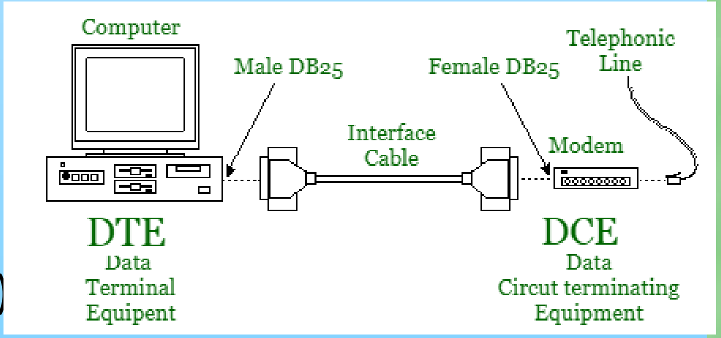
- **Significant propagation delays** - up to hundreds of milliseconds - in the case of using satellite links,
- **Transmission speeds usually lower than those obtained in LAN and MAN** networks (often from a few to several hundred kb/s),
- **Higher error rates than those observed in LAN** networks (procedures for their detection and removal become necessary),
- **Influence of many institutions and organizations on the standards** used in the network: interfaces and protocols, as well as types of end devices and computers,
- **Greater complexity of network management and maintenance** procedures,
- **Greater susceptibility of transmission links and switching devices on failures** than in LAN networks,
- **Necessity to convert protocols and/ or data formats** when connecting networks with different requirements, including different technologies,
- **WAN service costs are usually related to the volume of messages** being transferred (in packet-switched networks).

Features and functions of wide area networks

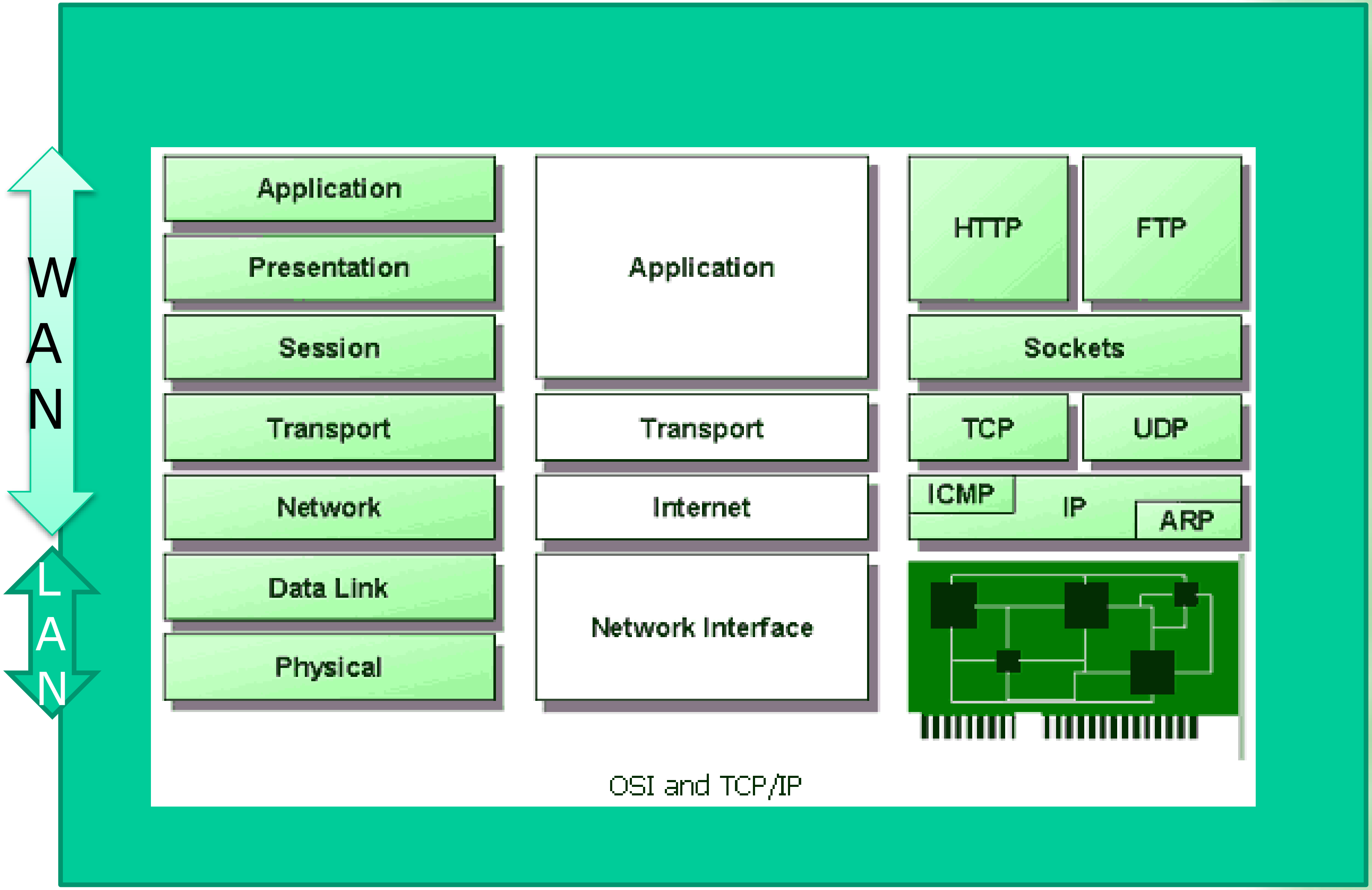
- **Data transfer between end systems -** according to the switching (commutation) concept it requires setting up routes (cascade connections) with the use of existing point-2-point inter-node transmission links (tl). This means that a particular transmission link may (simultaneously or at different times) constitute a common route segment for many different "relations" - source and destination stations.

- **Separation (administrative and physical) of network hardware and software, and user hardware and software.** For example, a network is subject to a specific administration (e.g. network public operator), constituting a Public Data Network (PDN). So we define two components: **DTE** - which stands **for Data Terminal Equipment**, and **DCE** - which stands for **Data Communications (Circuit terminating) Equipment**. PC or NIC cards are generally considered as DTE devices while Modems and **CSU/DSU** (**channel service unit/data service unit**) are considered as DCE devices.

- There are also separated/private networks (industrial, corporations, banks, academia), which often use transmission links provided by the public operator (the so-called leased lines).

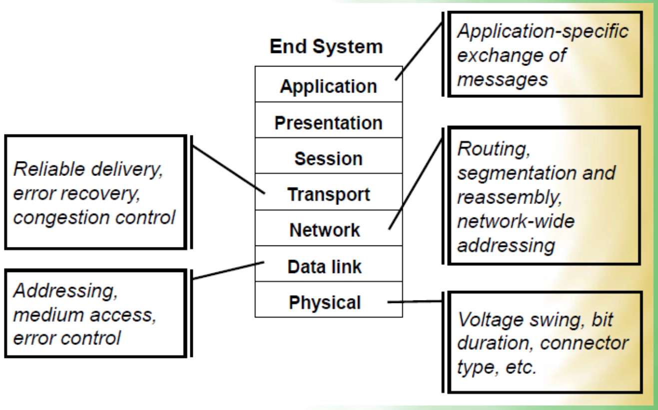


Layered architectures for WANs



Basic functions of the network layer

Techniques for setting up routes (switching/commutation):
Switching of physical circuits (links/channels);
Packet switching:
Packet switching in networks with logical/virtual connections.
Packet switching - Datagram technique.



Routing mechanisms (route selection):
Device location methods;
Methods of exchanging information
(and gathering information)
about network topology and load;
Route selection algorithms (optimal - least cost – shortest path).

Network protection against overloads and transmission deadlocks.

Communication protocols:
Internet Protocol IP (data structures, addressing schemes !!!!!);
PSPDN: X25 / FR; ATM; Ethernet End –to – End.

Route selection problems

Note: **Selection of links (channels) and intermediate devices (routers) forming the route (path) for the connection (e.g. paths for transmitted datagrams) should be made with a view to ensuring high quality of service and efficient use of network resources.**

Examples of criteria and postulates for route selection:

High network throughput ,S, i.e. a large number of completed connections and/ or packages/ datagrams delivered per time unit,

Low end-to-end delay, T,

Low traffic losses - quick response to changes in network topology and traffic conditions, i.e. creating bypass routes,

Stability of routes - routes should not change too often (in order to reduce the costs of setting up/ disconnecting, restoring the order of packets – to aviod the „flutter effect”),

Fairness - any pair of end systems - should be able to transfer data with the same rights,

Postulated priority (privilege) of handling time-related applications (e.g. multimedia)

NOTE: Too rapid response to changes in operational conditions may result in: increase in delays (longer and sub-optimal routes), or "oscillation" of routes (massive escape from congested routes, causing congestion of bypass routes and the need to re-route).

In turn, striving to increase the flow of S (throughput) in the network may lead to: the increase delay times T and unfairness in access to the network.

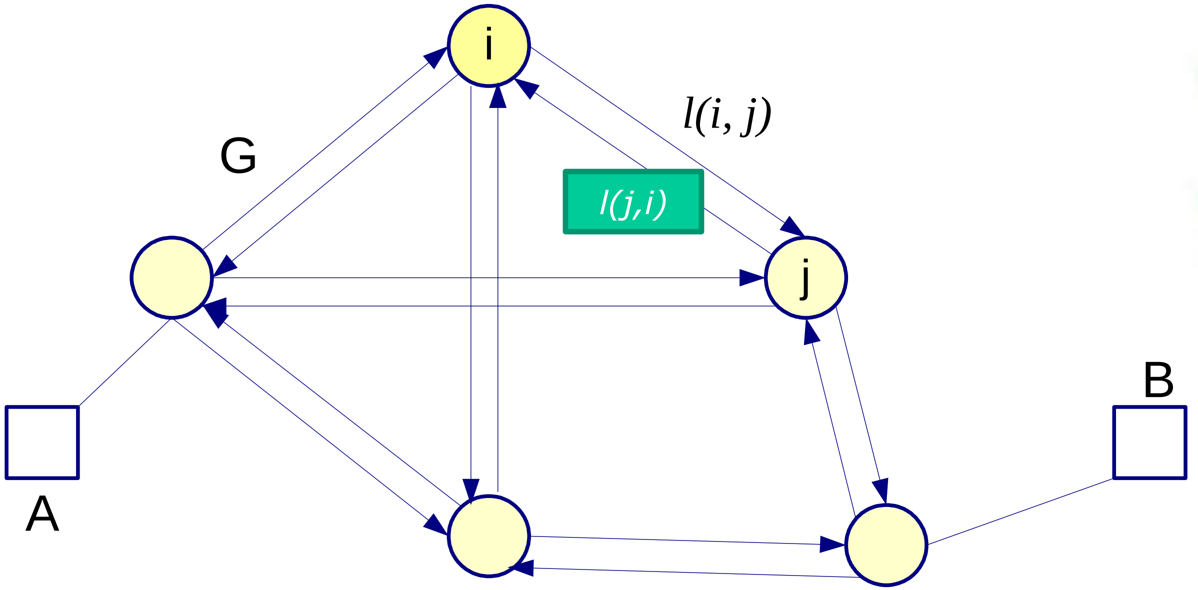
Route selection problems

Path selection in packet-switched networks is a more complex issue than in channel/circuit-switched networks.

WARNING! Acceptance of a new connection affects the quality of service of already established routes, especially when the network topology is non-hierarchical.

The necessity to select a criterion function and branch metrics >>> in order to optimize the route selection

Route selection problems



Network topology in the form of a directed, weighted graph (G)

The "length" l (i, j) of the arc (i, j) represents the contractual "cost" of transmitting the data unit over the link (arc) between nodes (vertices) i and j the link metric „l”.

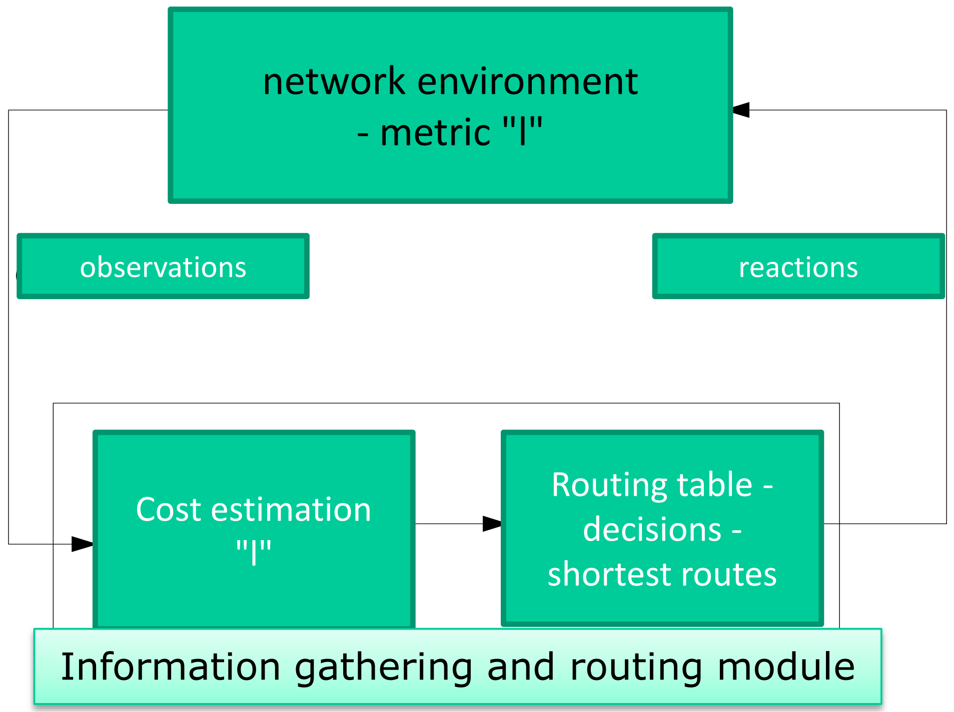
l (i, j) may be interpreated as:

-packet delay (due to: buffering, transmission, propagation, processing) in time units.

- **the number of hops to a destination**
- the number of occupied logical sub-channels in the link,
- the link capacity or transmission speed,

as well as: reliability, link operating costs, type of data transferred, etc.

Route selection problems
Adaptive routing mechanisms



The optimal (in terms of metric „l”) route selection consists in finding the shortest route (shortest routes) in graph G for each "relation" A - B in the sense of the adopted criterion function, where the "length" of the route can be expressed in various ways, e.g.:

Σ(ij)l(ij) (sum of delays, number of hops or intermediate nodes, total costs or geographical distance)

Π(ij)l(ij) (reliability),

max(ij)l(ij) ("bottleneck" – minimum throughput).

Route selection problems

Information gathering and routing module

Developing assessments (estimates) for the route metric or its parts (link metrics) based on available network observations and/or information exchange between network nodes.

Choosing the shortest routes (with the least-cost) - based on the developed estimates.

For additive metrics:

Route/path cost (source – destination) =
min Σ (costs of individual links along the entire route/path)

Route selection problems

Classification of adaptive route selection mechanisms

Such a classification can be made taking into account:

- **unambiguous /ambiguous decision:**

- without branches, ie. a single-path routing or
- with branches – bifurcated or multipath routing,

- **location of the decision making routing module:**

- centralized - the Control Center selects the A-B route, or
- distributed
    - the source node selects the A-B route, or
    - each node selects only the next section of the route.

- *Interior vs exterior methods (inside of an AS system or between AS systems)*

POLITECHNIKA GDAŃSKA

Route selection problems

Distributed mechanisms

Taxonomy

Cooperative – Routing module (RM) uses the estimates developed by other RMs, in particular in neighboring nodes,

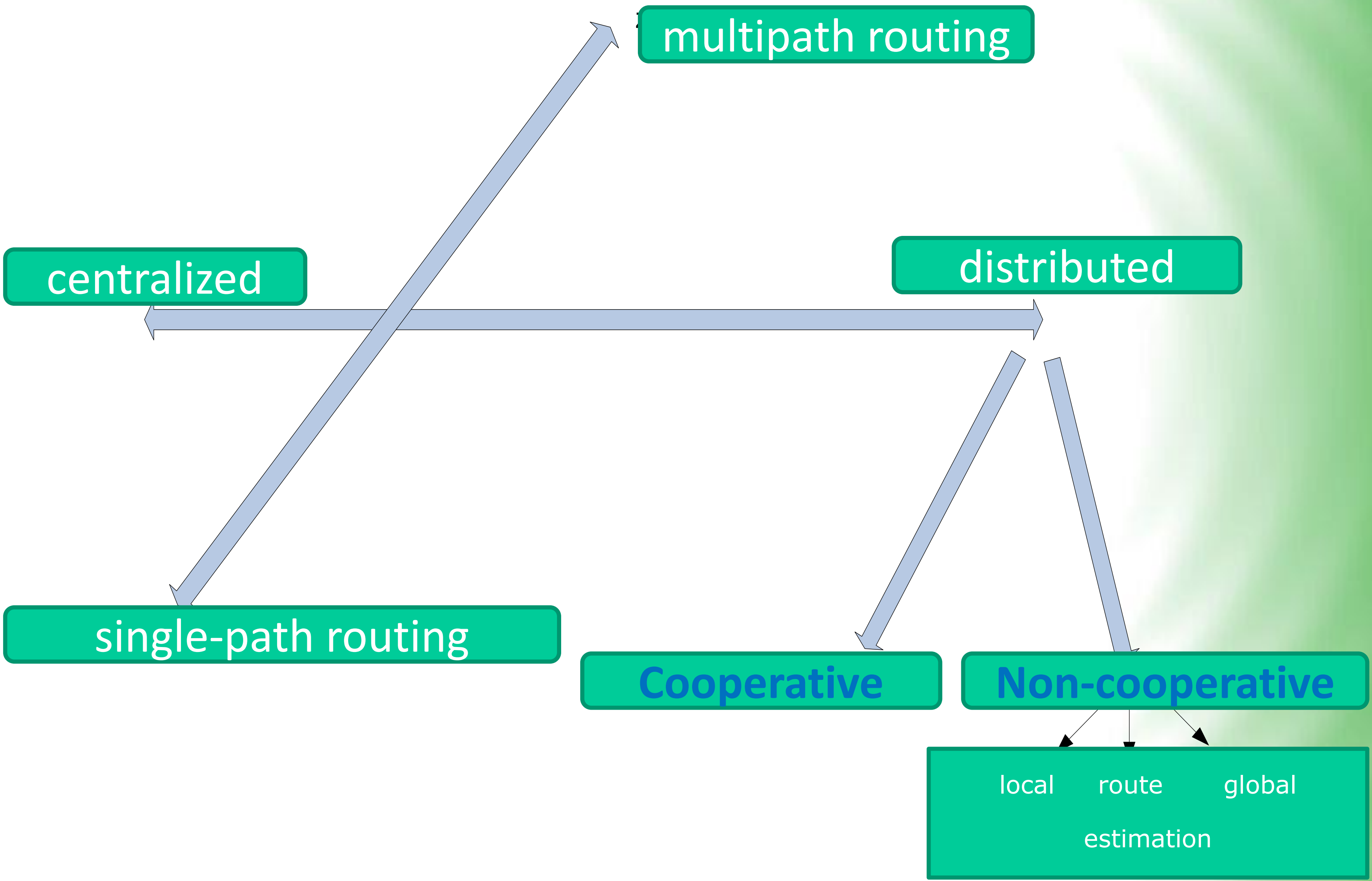
Non-cooperative - RM relayes on its own observations (or those sent by other RM).

In turn, non-cooperative mechanisms are divided, due to the range of the developed estimates, into:

- local estimates,
- state estimates of routes passing through the node,
- global estimates.

Additionally: dynamic vs static

Route selection problems



Network overload - congestion

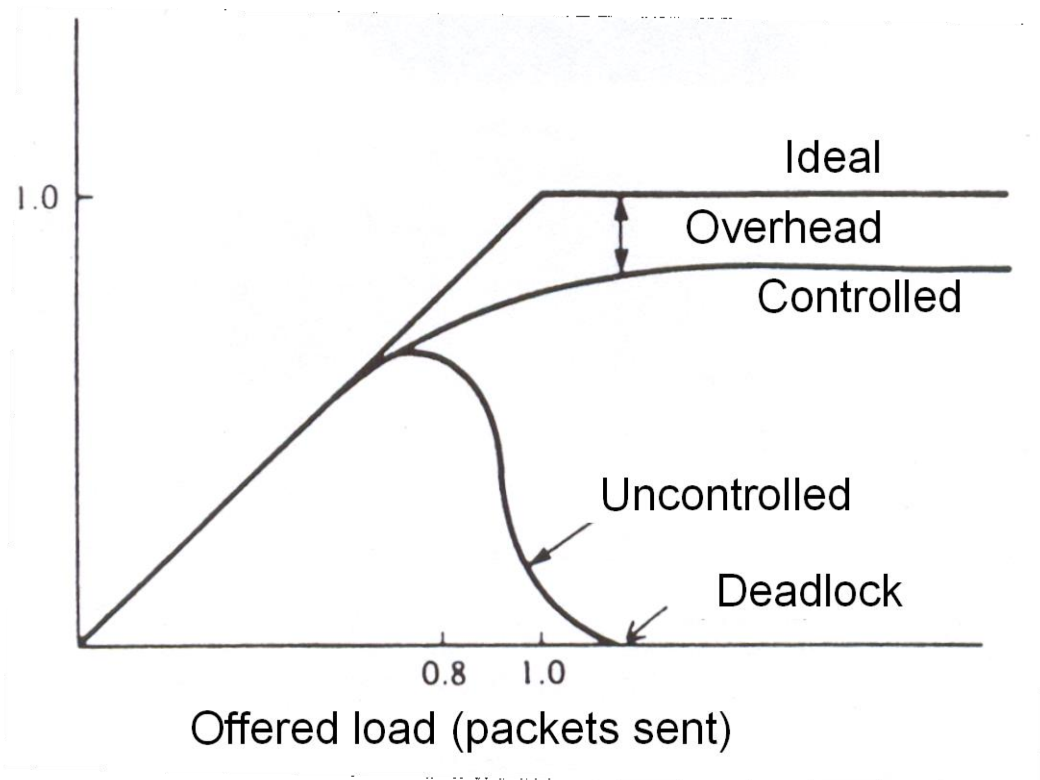
Flow control in the A-B "relation" does not eliminate the possibility of network congestion (local or global).
Traffic control is needed - through a set of mechanisms limiting packet access to the network or its fragments.
Several groups of mechanisms are distinguished here:
due to the range of impact:
-- at the network access level,
-- at the node level,
-- at the level of "relation" A -B,
due to the way of operation:
--threshold,
--reservation,
due to the way of „starting” to solve the problem:
--preventive,
--reactive.

An important role is played by methods of active traffic management in networks

Basic goals: fairness in access to network resources (available bandwidth) and guarantees of service quality (delay, packet loss, delay variability).

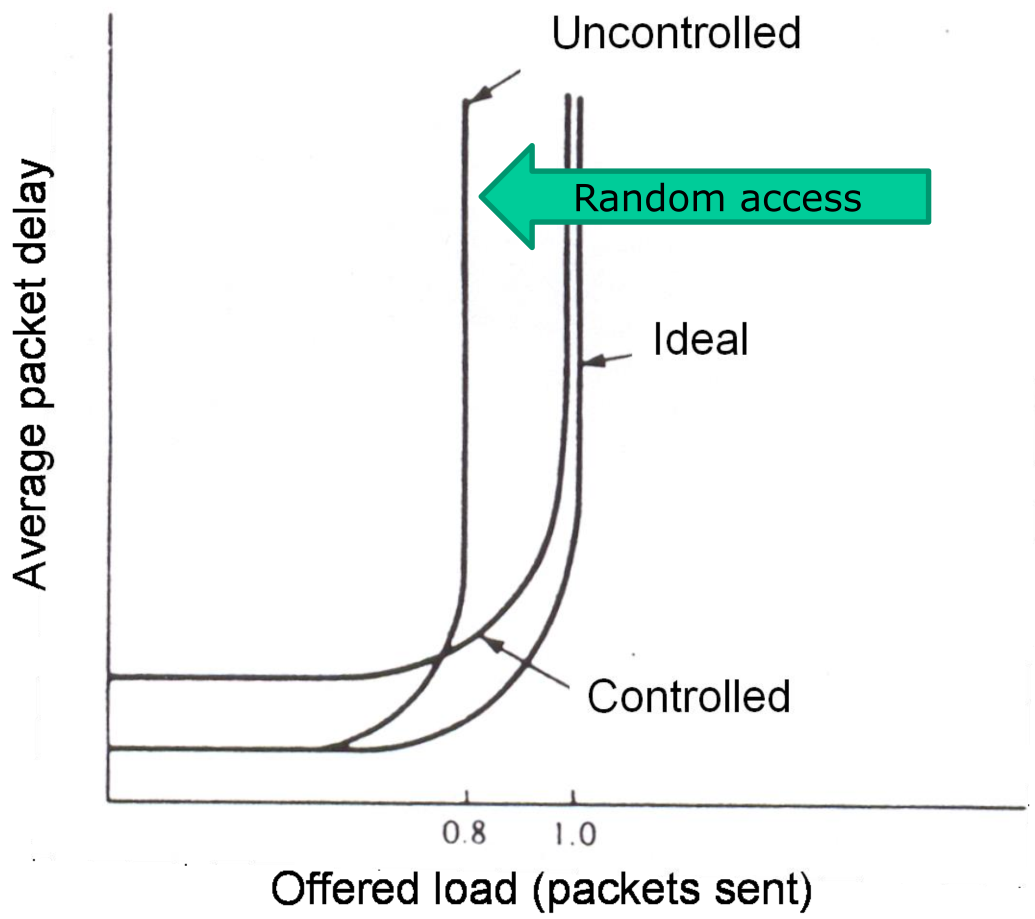
Management methods include:
queue management: drop-tail, RED (Random Early Drop/Detection),
queuing disciplines: FIFO (First In First Out), PRIO, fair queuing - W(weighted)FQ, D(deficit)RR/W(weighted)RR),
bandwidth management : CBQ - Class Based Q, HTB - Hierarchical Token Bucket.

Network overload - congestion



Change in the normalized network capacity with increasing network load

Network overload - congestion



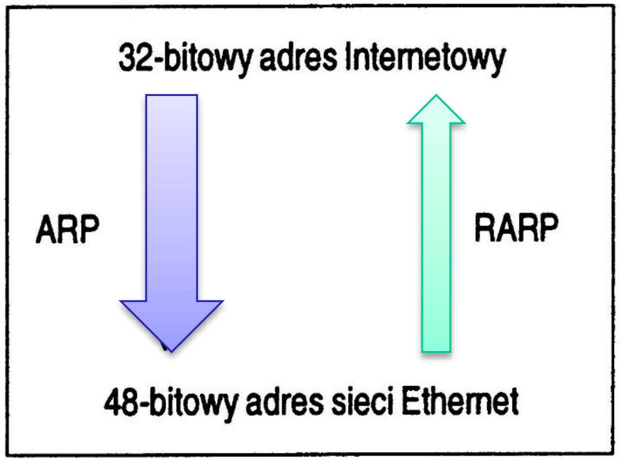
Packet delay changes with increasing network load

IP networks
Basics of routing
Intradomain routing concepts (Interior Gateway Protocol type)

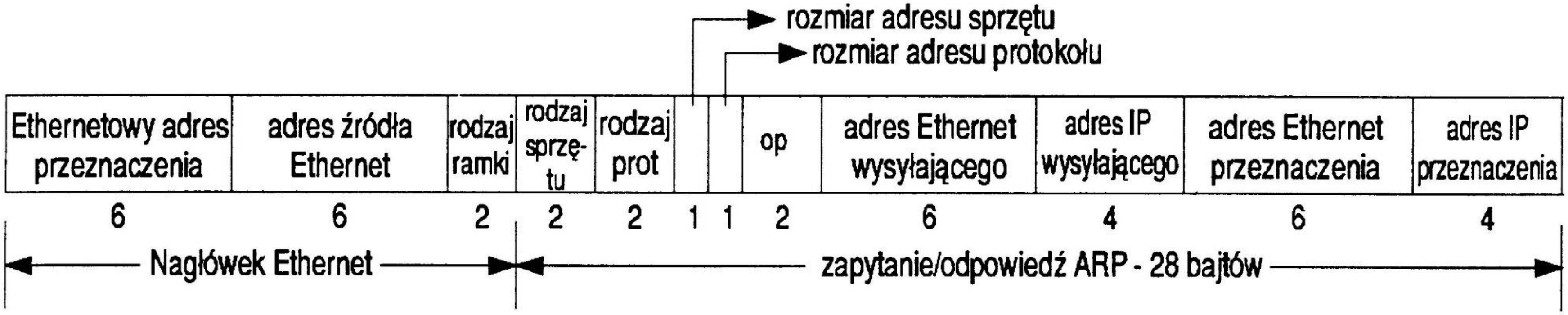
Józef Woźniak
Katedra Teleinformatyki
Wydział Elektroniki, Telekomunikacji i Informatyki
Politechniki Gdańskiej
jowoz@eti.pg.edu.pl

POLITECHNIKA GDAŃSKA

ARP – RARP Protocols

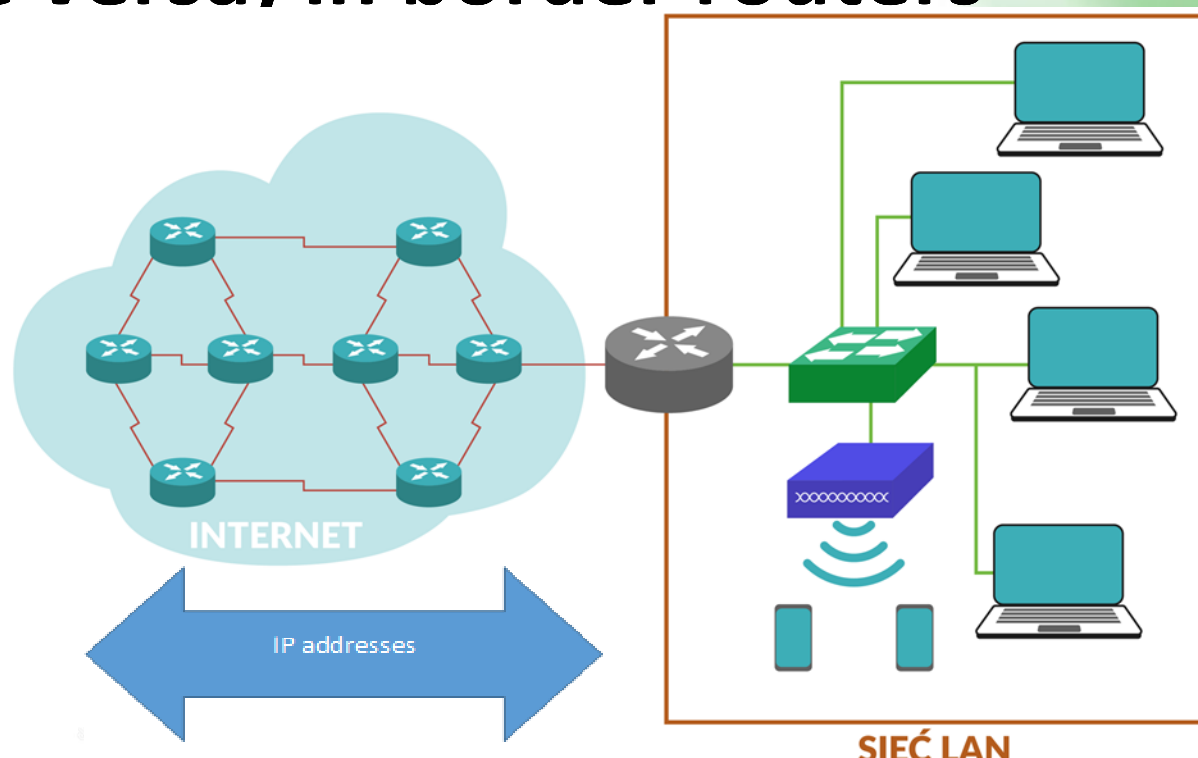


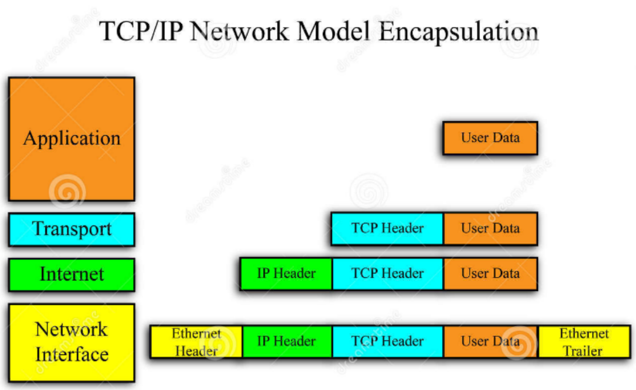
RFC 826 - ARP Specification
RFC 903 - RARP Specification
ARP - Address Resolution Protocol
the protocol enables the **conversion of logical network layer IP addresses to physical MAC addresses** of the data link layer.
RARP - Reverse Address Resolution Protocol
reverse procedure MAC Adr > IP Adr



Format pakietów zapytania i odpowiedzi ARP, kiedy używane są w sieci Ethernet

Converting IP addresses to MAC addresses (and vice versa) in border routers





Port numbers

IP addresses
MAC addresses

MAC addresses

IP addressing

In IP networks, the IP address (Net ID+HostID):

- Indicates the location of the station - by locating the user's network - the NetID part is responsible for this (the so-called network identifier)
- Uniquely identifies the station - this is provided by the HostID part;
- Routing tables in routers use NetID only, while datagrams must contain the full IP address.

Routing concepts

- **Routers are network nodes responsible for efficient packet forwarding through an assembly of network components;**

  \- **We often have many paths to a destination**;

  -- Routers should select (indicate) optimal paths (in the sense of the adopted criterion);

  \- **There are situations when we have to deal with different network protocols**.

  -- Routers should repackage packets, similarly to bridges;
- **„Least/Lowest Cost" Routing is usually applied**

  \- Routers tend to send packets along the shortest path for performance reasons.

  \- **But what makes us say that one path is shorter (better) than the other?**

  -- Is it the number of stages? Or maybe the cost of the transmission? Or maybe a delay? Relatively greater reliability? Or maybe security?
- **It will often be a path that takes into account a combination of these factors.**

Routing concepts

Static vs Adaptive Routing

- For static routing, the selected path from router "A" to the destination node is used for all transmissions;
  - Routing tables are usually created "manually" by the network administrator.
- For adaptive (*dynamic*) routing, router "A" path selection depends on network conditions (*e.g. changes in network topology*). The routing tables can change "automatically" with changes in topology and/or network load.

Routing concepts
Concepts of dynamic routing

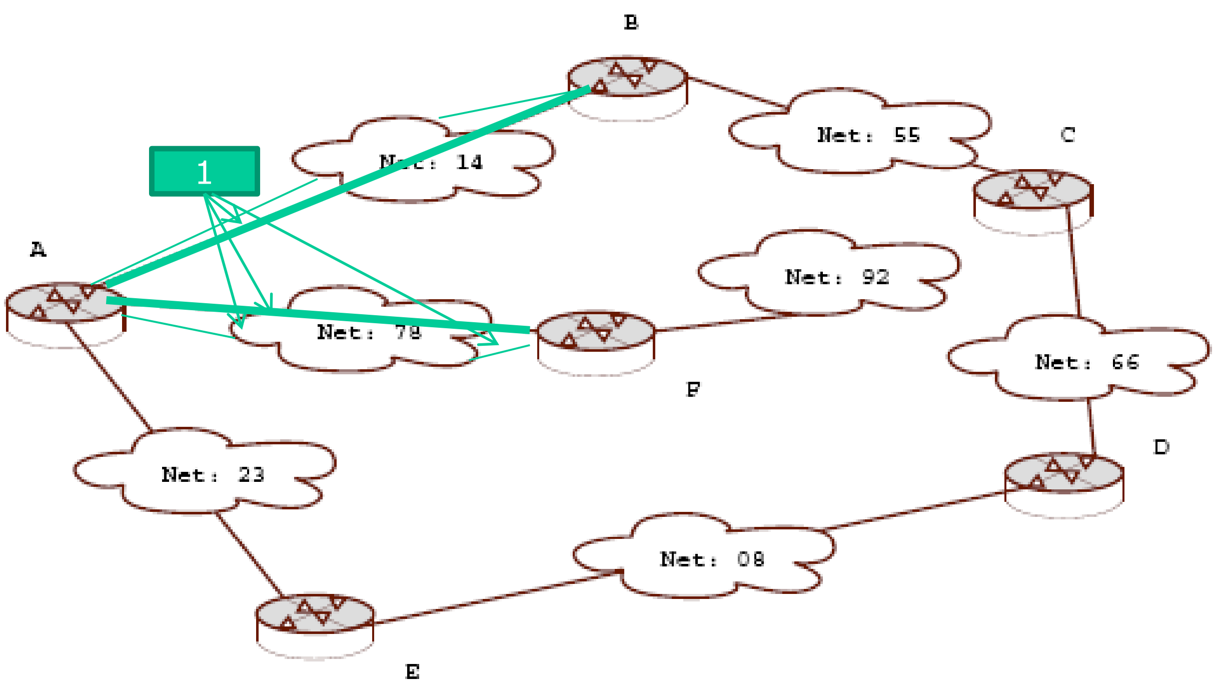
- As long as the cost associated with each transmission step is known (link metric value), routers can determine optimal routes for each transmission.
  - There are several (dozen) routing algorithms that work out such decisions - the two basic methods are:
- **distance vector routing** - and
- **link state routing.**

- **Distance Vector Routing:**
  Each node periodically "shares" knowledge about the state of the network with its neighbors.
- **Link State Routing**

  Each node occasionally "shares" knowledge about the state of the network, however with all other network nodes.

Routing concepts
Distance Vector Routing (DVR)

- Each node periodically exchanges knowledge about the state of the network (***its routing table***) with its neighbors;
- The key elements of the distance vector algorithm are:
  -- Knowledge of the entire network (about all subnets);
  -- Transmission of routing information only to neighbors;
  -- Exchange routing information at regular intervals.



Routing concepts (DVR)

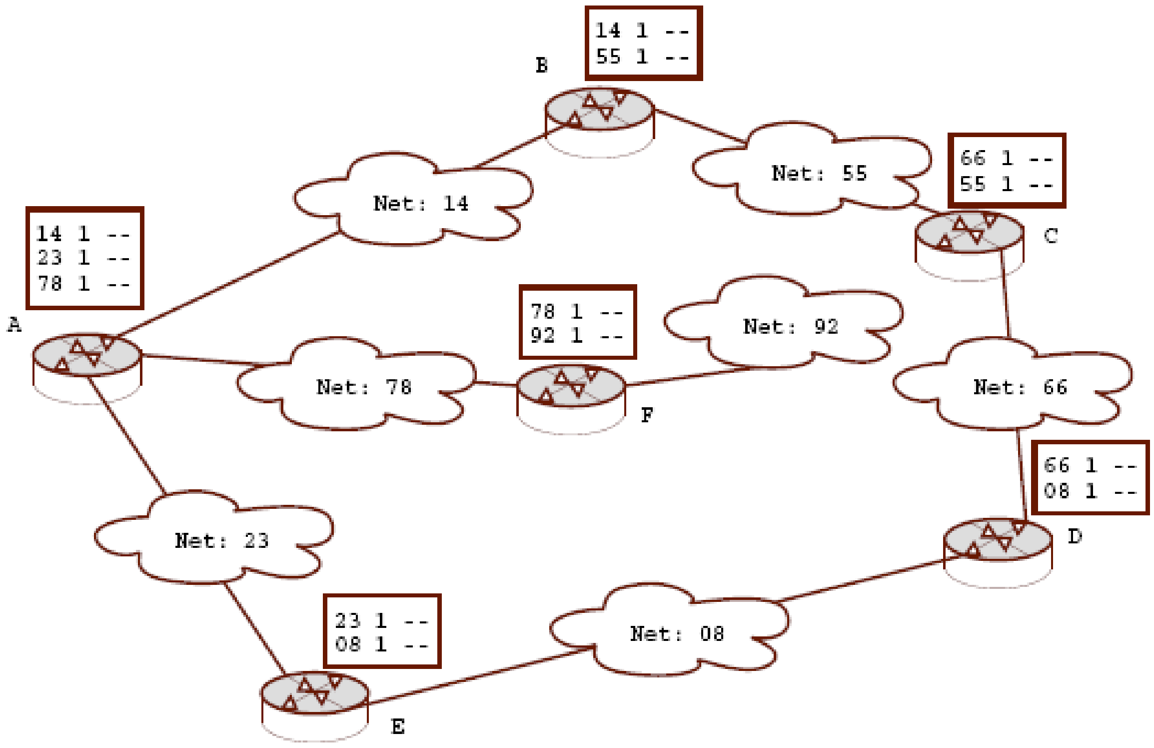
- **The distance vector algorithm assumes (most often) the cost of each single stage of transmission as a unit cost (equal to 1, in general);**
- **Information about the entire network (all routers and nodes) reaches all network nodes (routers) after a certain number of exchanges of "tables„. We are then talking about the process of convergence.**
- The initial content of the array (routing table) includes only the closest networks
  (for example for node A we have):

Network ID	Cost	Next Hop
14	1	–
23	1	–
78	1	–

- **The routing table is updated at regular intervals to include tables from neighbors.**
- If router A can "reach" router B in one hop, then it can reach all the nodes in router B's table in the number of hops one more (than is possible from B)

Routing concepts (DVR)

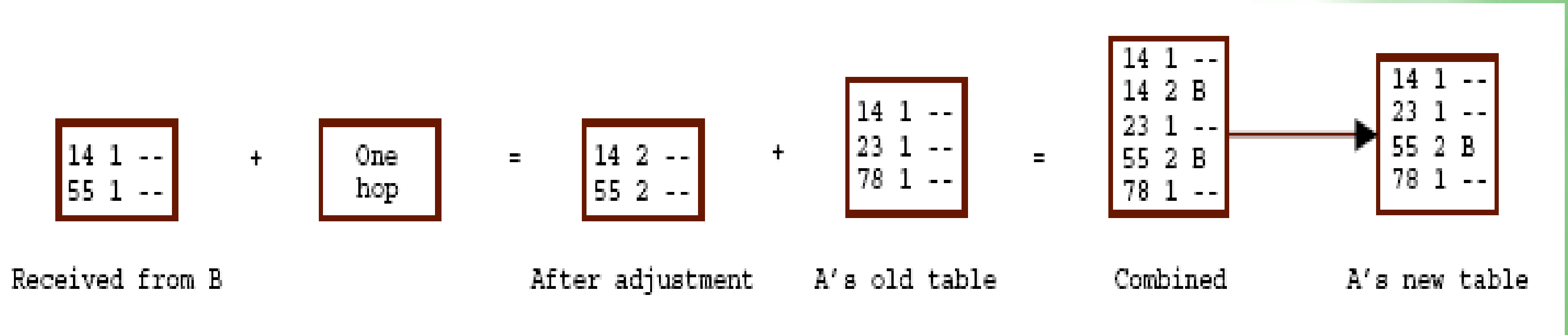
- **Initial routing tables:**



- In our example, each router will have full network knowledge after 3 updates.

Routing concepts (DVR)

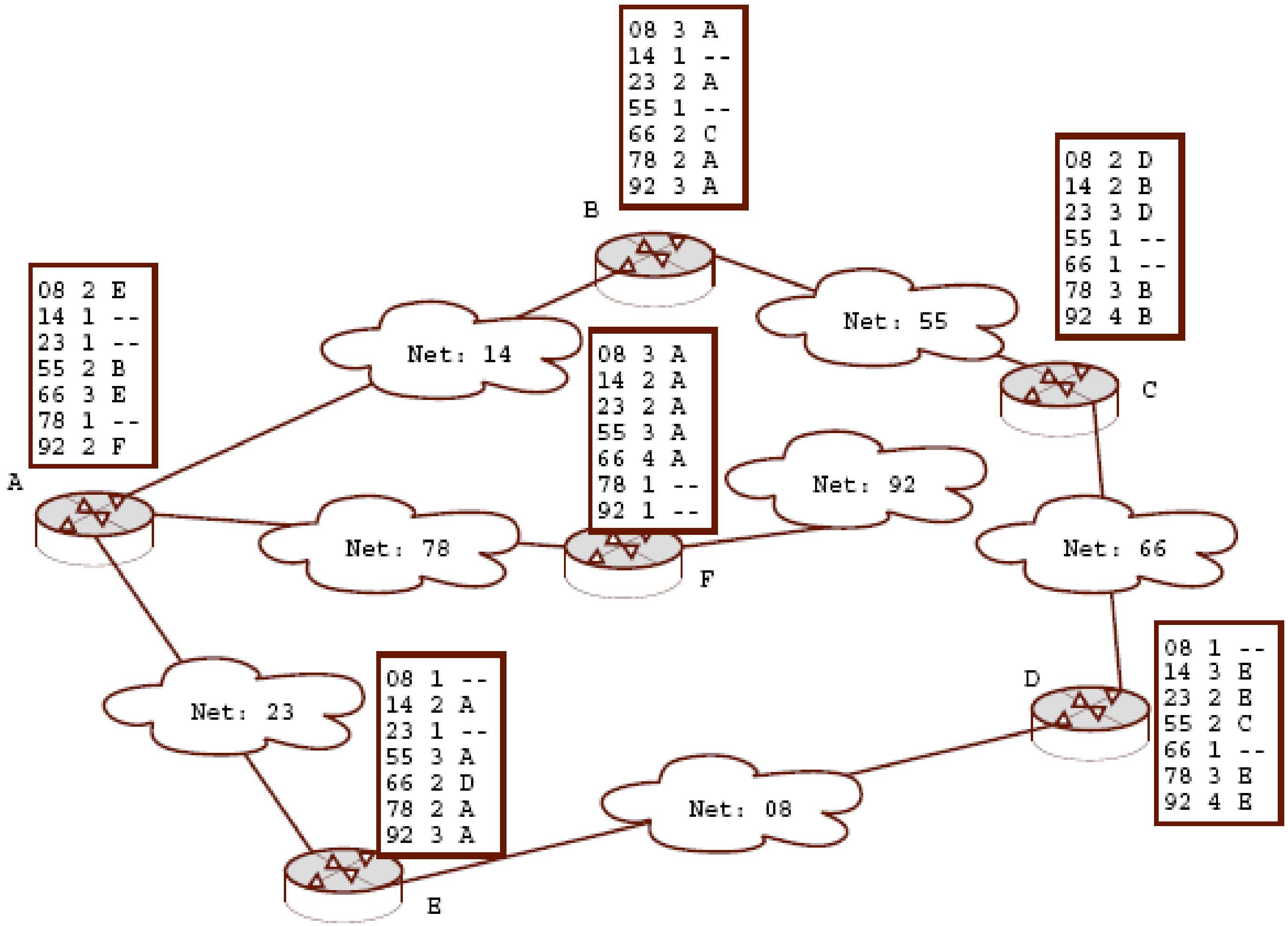
Updating the routing tables



Upgrade Algorithm:

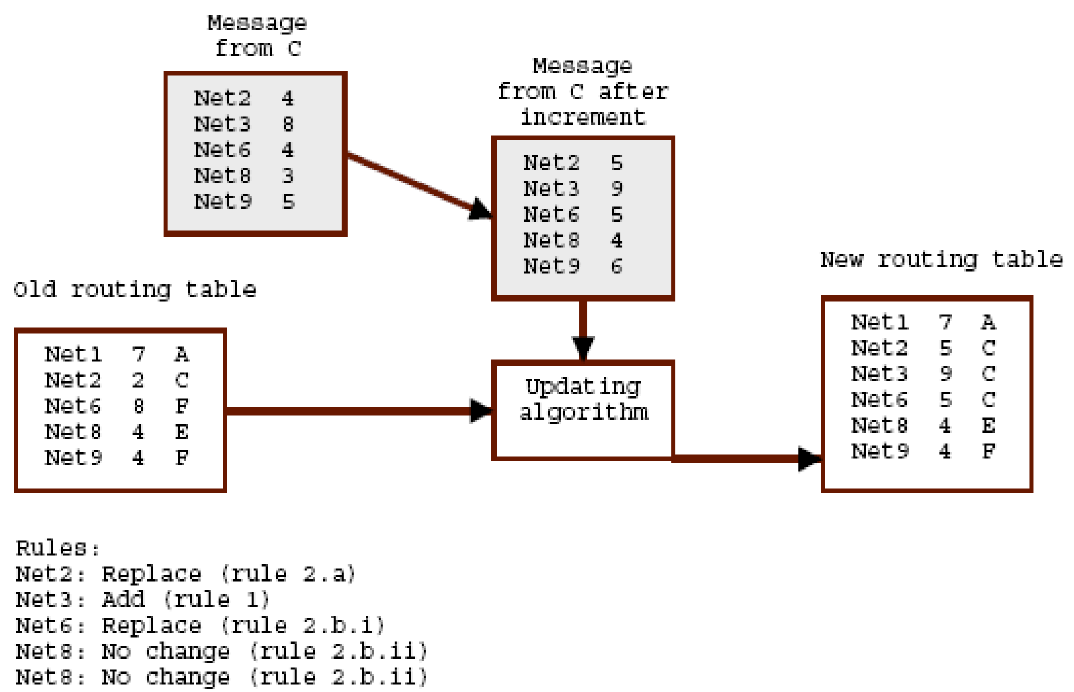
1. If "destination" is not included in the table -> add;
2. If "destination" is included in the table:
2.a. If the next hop is the same for the destination -> replace old entry;
2.b. If the next hop is different:
-- 2.b.i. If the new number of hops is smaller -> replace the entry;
-- 2.b.ii. If the new hop count is greater -> do not change anything.

Routing concepts (DVR)
Final routing tables



Routing concepts

An example of updating routing tables



Note: Net1 was not announced in an update packet from C, so none of the previous rules apply in this case.

In the case of Net 2, on the other hand, there is an "unfavorable" change. Nevertheless, node C remains the only one providing access to this network in this step.

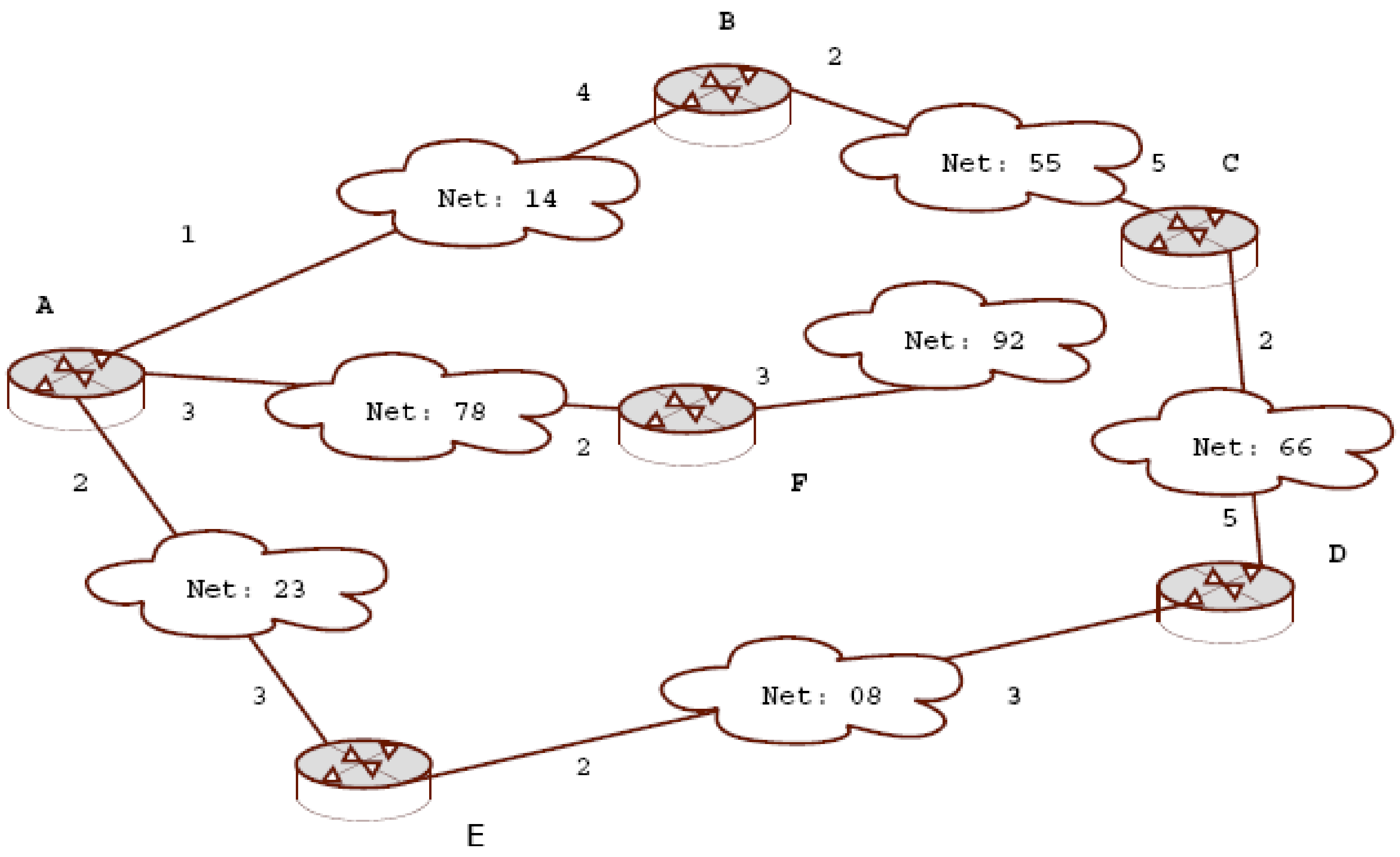
Routing concepts

Link State Routing (LSR)

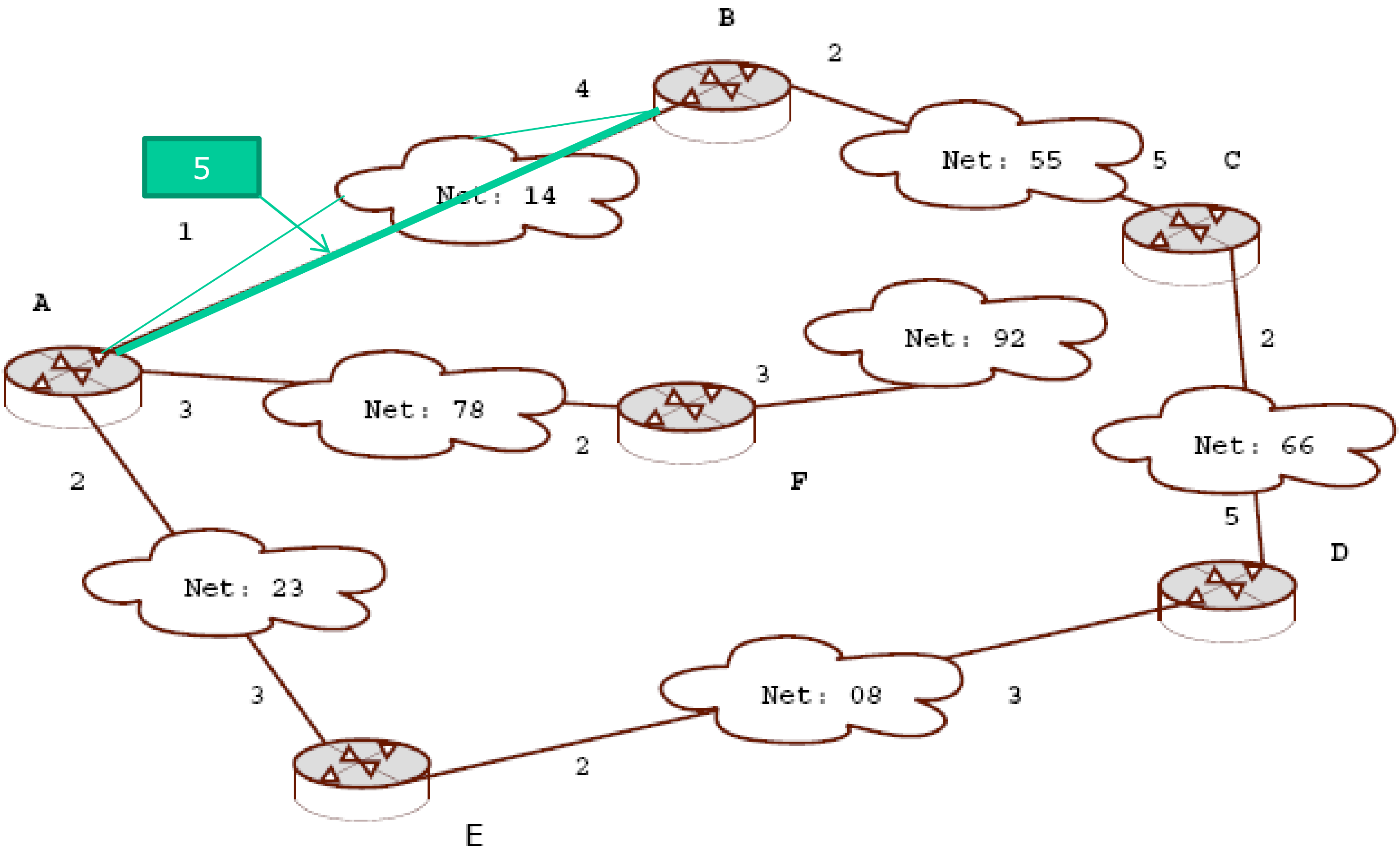
- **Link State Routing:**
  The key components of the link state algorithm are:
  - Maintaining direct connections to neighboring routers;
  - Broadcasting routing information about known subnets and routers to all routers. This means that every router has full information about the network (its topology - although it requires much more effort on data processing).
  - **Exchange of routing information only when significant changes occur in the network.**

  Link State routing properties:
  The the metric used is usually inversely proportional to the channel/link bandwidth/capacity - thus favoring links with lower delays

Routing concepts (LSR)
Cost of paths in LS routing



Routing concepts (LSR)
Cost of paths in LS routing



Routing concepts (LSR)

Link State Routing

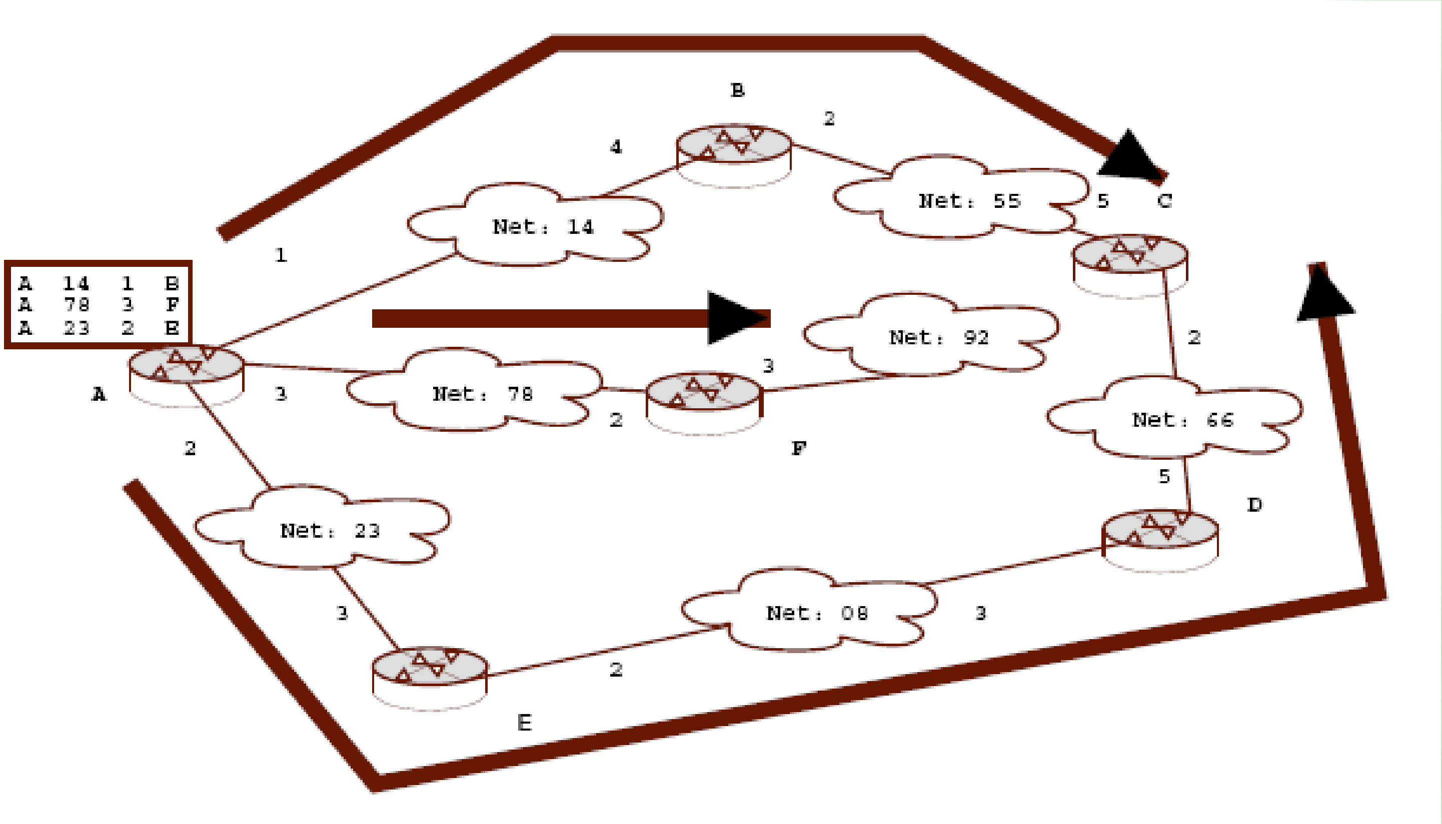
- **Link State Packets (LSP) are broadcast**.
- The router broadcasts LSP packets ("floods" the network) to all its neighbors.
  LSP packet format:

Advertiser	Network	Cost	Neighbour
...	...	...	...
...	...	...	...

- Periodically, short "Hello" packets are exchanged between neighbors to test connectivity between neighbors:
  -- The neighbor's answer signifies his normal functioning;
  -- In the absence of a response, a set of new data in the LSP is sent, indicating a disabled or damaged router.

Routing concepts (LSR)

Router A broadcasts information using LSP



- Each router receives each LSP and updates its routing database - link state database

Routing concepts (LSR)

metrics – costs - link state table

Advertiser	Network	Cost	Neighbour
A	14	1	B
A	78	3	F
A	23	2	E
B	14	4	A
B	55	2	C
C	55	5	B
C	56	2	D
D	66	5	C
D	08	3	E
E	23	3	A
E	08	2	D
F	78	2	A
F	92	3	–

Routing concepts (LSR)
Dijkstra algorithm

- State - metrics - cost table link state table
  Dijkstra algorithm;
- To derive the routing tables, routers use the Dijkstra algorithm;
- This algorithm makes it possible to determine the shortest paths between each pair of nodes in the network;
- The amount of memory and CPU time required to determine the shortest paths in the root tree on a given router increases with the number of nodes;
  -- Surprisingly, however, most networks use the link state algorithm without any special problems;
  -- For example, the Internet commonly uses OSPF (Open Shortest Path First) routing using the link state algorithm.

POLITECHNIKA GDAŃSKA

Routing concepts (LSR)
Dijkstra algorithm

- Each router computes the routing tables using a tree of the shortest paths

  Link state routing table for router A:

Sieć Network	Koszt Cost	Kolejny router Next hop
08	7	E
14	1	-
23	2	-
55	7	B
66	14	B
78	3	-
92	8	F

  – The shortest path trees will vary from router to router

Task to be developed

- In the case of determining the optimal routes in distance-vector algorithms and link state algorithms, either Bellman-Ford or Dijkstra algorithms are used.
- Present the basic assumptions and example applications of both algorithms (B-FA/DA) (short presentation in ppt).

Computer Networks

Internet - IP networks – IPv4

Józef Woźniak
Katedra Teleinformatyki
Wydział Elektroniki, Telekomunikacji i Informatyki
Politechniki Gdańskiej
jowoz@eti.pg.edu.pl

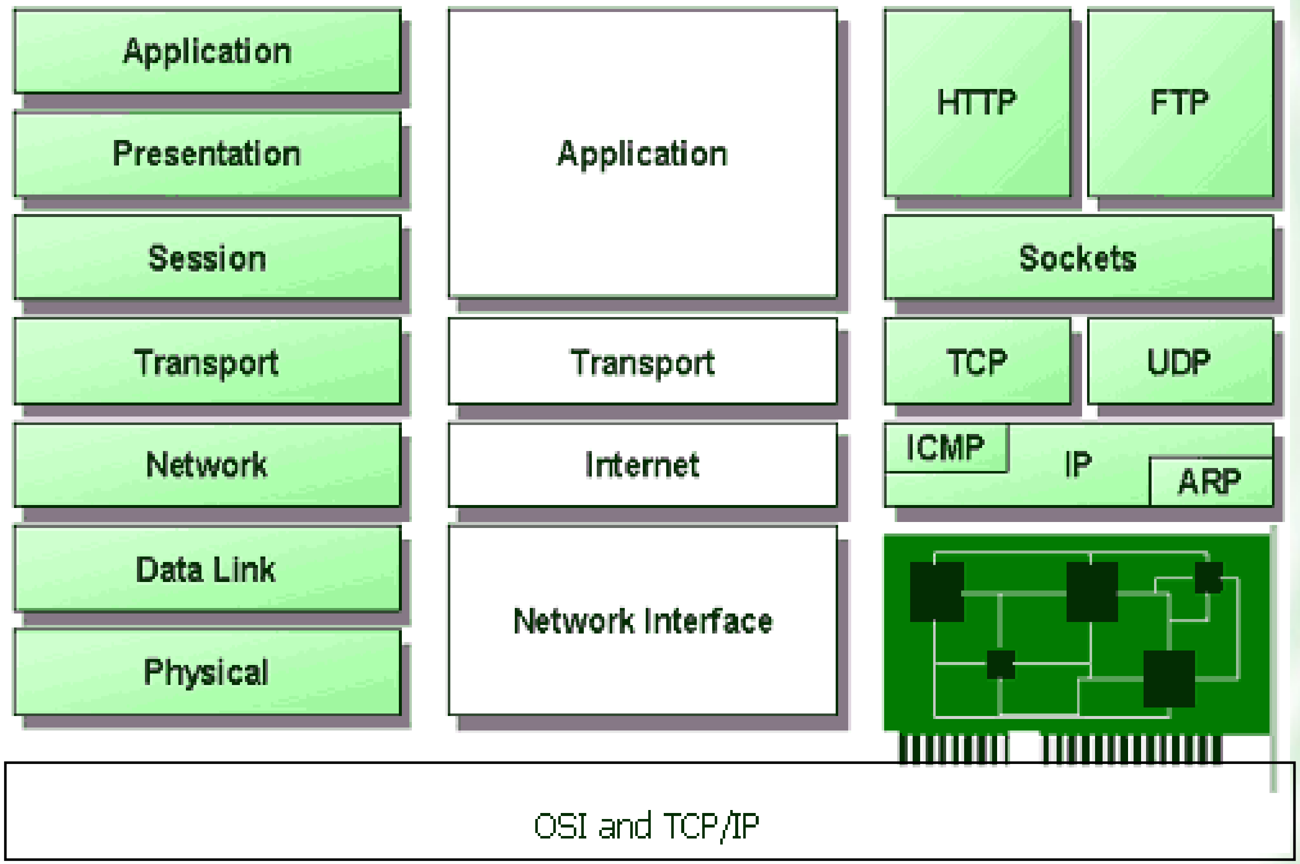
POLITECHNIKA
GDAŃSKA

Internet

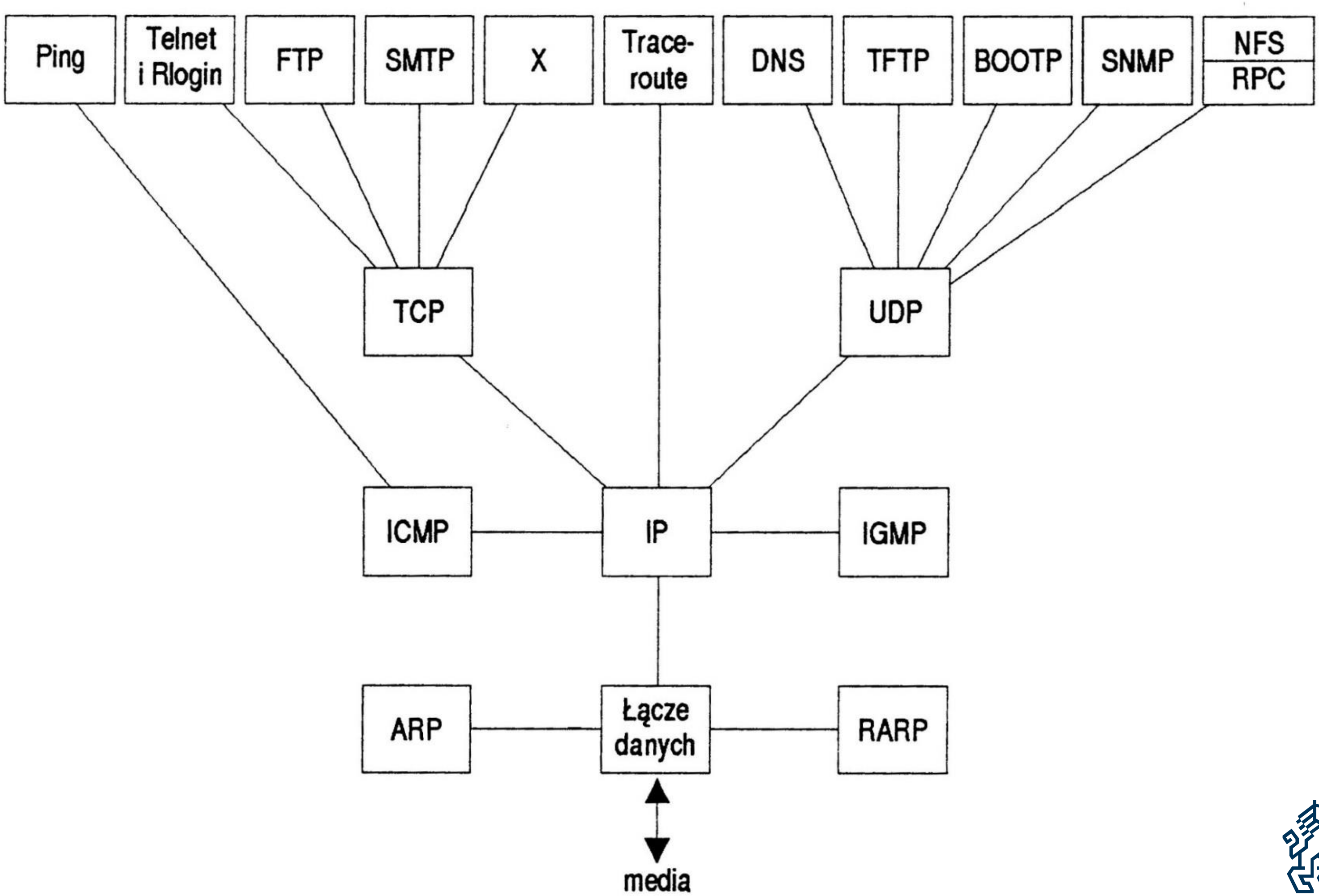
Entities coordinating the activities of the Internet

- ISOC (Internet Society, http://www.isoc.org),
- IAB (Internet Activity Board, http://www.iab.org)
- IETF (Internet Engineering Task Force, http://www.ietf.org)
- IESG (Internet Engineering Steering Group, http://www.ietf.org/iesg.html)
- **ICANN (Internet Corporation for Assigned Names and Numbers, http://www.icann.org)** is an institution currently responsible for assigning Internet domain names, structuring them, and for overall supervision of DNS servers around the world. Established on September 18, 1998 to oversee the technical aspects of the Internet).
- **IANA (Internet Assigned Numbers Authority), http: /www.iana.org** is responsible for the global coordination of zone DNS servers (DNS Root), IP addressing (also AS numbers) and other Internet protocol resources - it is an autonomous part of ICANN.

ISO-OSI and TCP/IP architectures
A rough comparison

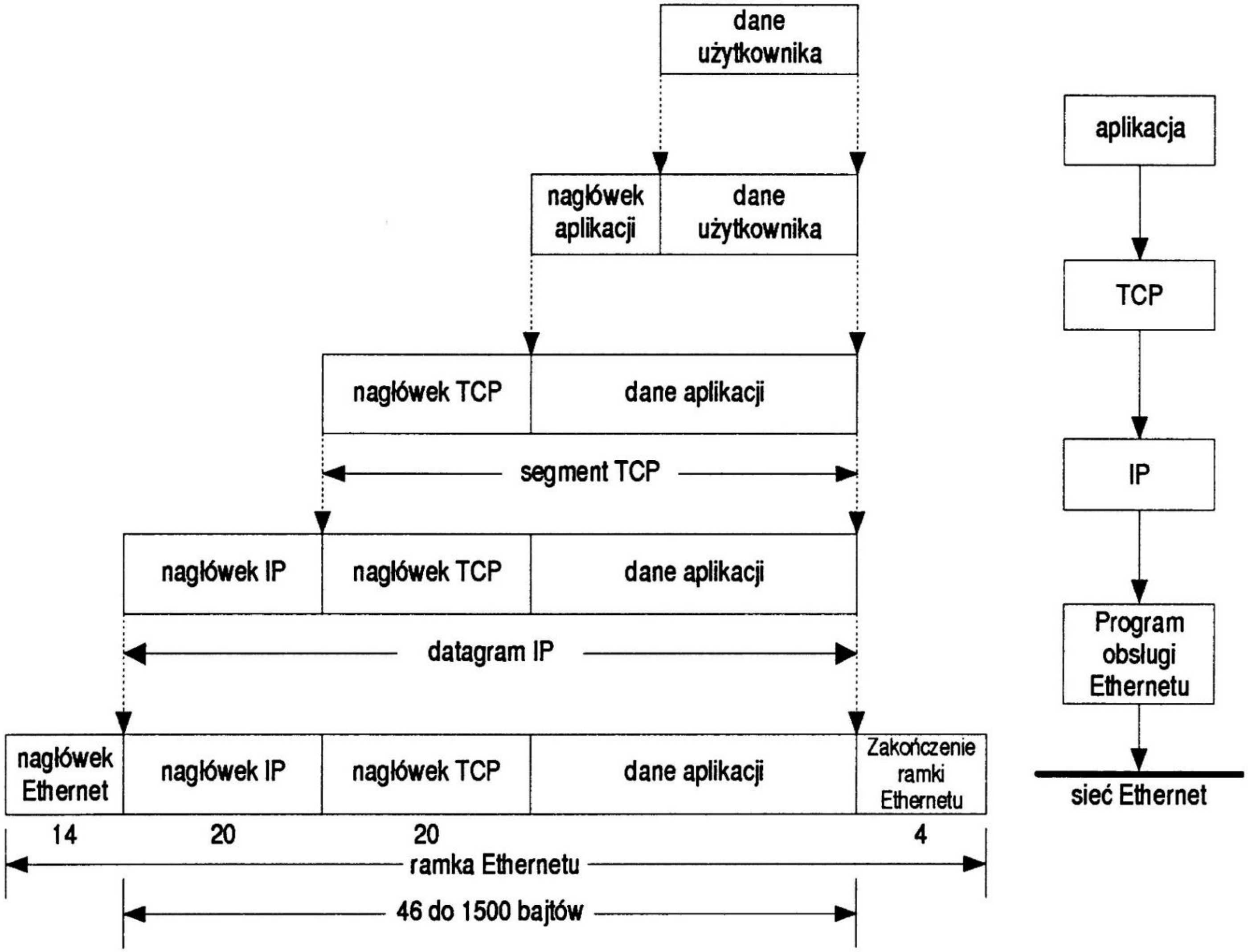


Internet
Protocols from the IPv4 family



POLITECHNIKA GDAŃSKA

Internet
IPv4 encapsulation



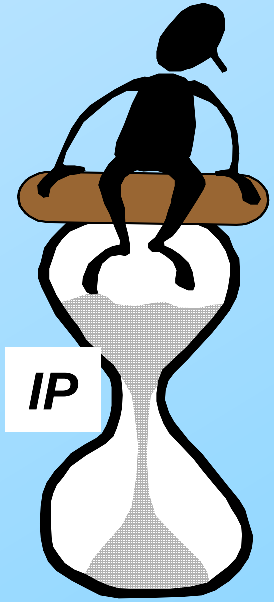
Internet
IP protocol

- The IP protocol was developed for ARPANET networks for communication between remote end systems;
- IP networks (Internet components) are located in many dispersed locations;
- **IP networks were designed to improve resistance to failures and intentional attacks;**
- IP enables remote systems to work as a single organism;
- When the OSI model was developed, the IP protocol was assigned to the network layer;
- **IP is a datagram protocol that offers a simple but unreliable means of transmission.**

Internet

Why is IP so popular?

- **A "minimal" hourglass-like form of the TCP / IP architecture protocol suite**
  -- Many protocols work "over" IP;
  -- IP works over everything.



- **Architecture and IP principles**
  -- Minimalism and autonomy of nodes;
  -- Universal service (best effort service);
  -- Stateless routers;
  -- Decentralized control.

Internet

IPv4 Protocol/IP addresses

- Each network-layer object in an IP network has at least one unique IP address
- IP address formats:
  4 bytes: 132.181.10.9
  32 bit: 10000100.10110101.00001010.00001001
  Hex: 0x84 0xB5 0x0A 0x09
- Number of available (theoretically) IP addresses:
  $2^{32} \approx 4.3$ billion
- Is this a sufficient number? No!!!
  -There are many inefficiencies in the IP address distribution policy:
  -- Certain IP addresses are reserved for special purposes;
  -- IP addresses are allocated in relatively large blocks (part of them stay unused).
- Some stations require multiple IP addresses.
- Urgent need of a huge number of addresses for IoT (Internet of Things).

Internet

IPv4 addressing problems - "short-term" solutions

- **The original IPv4 address concept was related to the division of addresses into 5 classes: Classes A, B, and C were allocated to networks of various sizes, while classes D and E were used for other purposes. This solution proved to be highly ineffective.**
- **In the following years, further (still 4 byte) solutions were proposed:**
- **CIDR (Classless Inter-Domain Routing) – RFCs 1517, 1518, 1519, 1520**
- VLSM (Variable Length Subnet Mask) – RFC 1009
- Private Addressing - RFC 1918
- NAT/PAT (Network Address Translation / Port Address Translation) – RFC 1631, RFC 2766.

Internet
IPv4/6

- The current version of IP is still IPv4.
- **New version, IPv6, more and more widely used, expands the address space (128 bit addresses).**
- **IPv6 offers new functionalities and a completely modified header structure (much less mandatory and many optional fields). This allows the processing of datagrams in routers to be faster.**
- However, the installation problem is significant (still valid…).

  -- What strategy? - Globally and at the same time, or rather double stacks.
  -- Who maintains information on station IP address mapping?

No central management: IP is a decentralized architecture.

IP has very limited functionality… but that is not its real weakness

What will the Internet of the Future be like ????

Internet

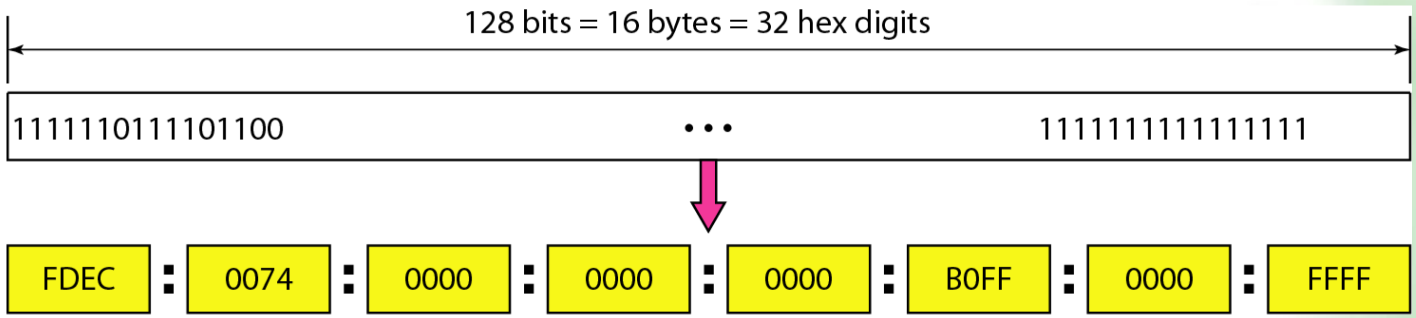
"Long-term" address solution: IPv6

- IPv6 uses the 128-bit address space with 340,282,366,920,938,463,463,374,607,431,768,211,456 possible addresses.
- IPv4 addresses went through a series of "refreshes", which meant that the full rollout of IPv6 did not progress quickly.
- IPv6 requires new software and preparation of IT administrators.
- IPv6 will coexist with IPv4 for several years to come.

Internet

IPv6 addresses - example

- The IPv6 address is 128 bits (16B).
  Hexadecimal notation:



- **Abbreviated notation**: