Networking Technology

ADIS HODZIC – ADIS.HODZIC@HVL.NO

Need for communication between devices

Vi are sending data (information) between devices

Information is digitalized and transmitted

Networks of devices

Devices may be directly connected to one or more devices

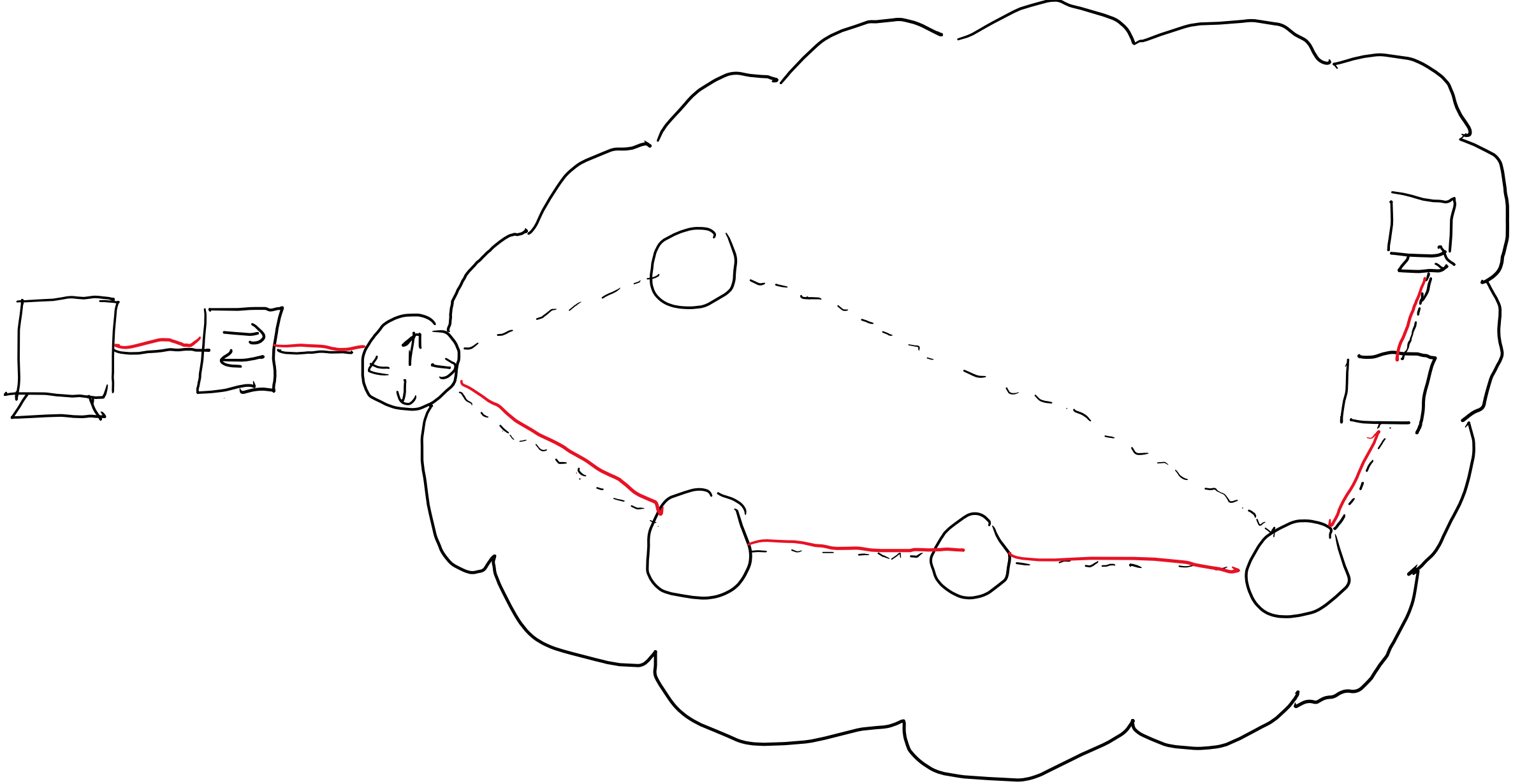
Usually, we do not have dedicated link between devices, message must pass several other devices between two endpoints – this means that we have several links between source and destination

Usually, there is more than one route to destination

Communication media between devices may vary from link to link

Communication technologies used on different links may vary

One route may be sued for message, different route may be used for reply



Communications between devices

Wired

- Electromagnetic signals transmitted over a physical medium (physical cables)
- Types: twisted pair, coaxial, optical fiber, …
- «one to one», «multiple access», …

Wireless

- Electromagnetic signals (Infrared-, Radio- or Microwave waves)
- Not bounded to physical medium (travel through air, water, vacuum, …)
- «one to one», «multiple access», …

Network topologies

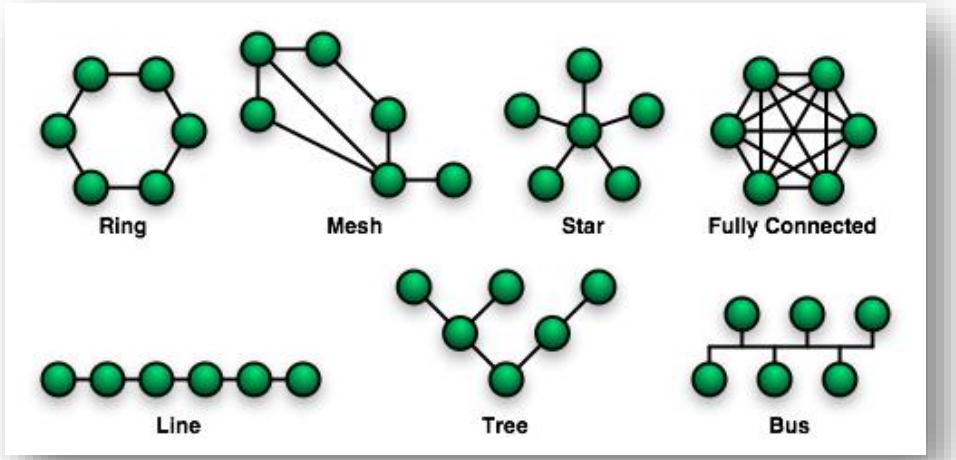
Physical or logical layout of the elements of a network

We differentiate between:

- Physical topology: physical connections and elements
- Logical topology: which devices may exchange information

Example (network 192.168.0.0/24, with no traffic filtering):

- It may be “star” with one switch at center and hosts otherwise
- Logical topology (L3) is “fully mash” (“fully connected”) between hosts



https://en.wikipedia.org/wiki/Network_topology

Network topologies

Bus: signals from one node are detected to all nodes

- Every nodes read packet destination address (Am I the recipient?). If the address match nodes address: read data, if the address doesn't match: ignore data
- Collisions/Interference/Multiplexing?

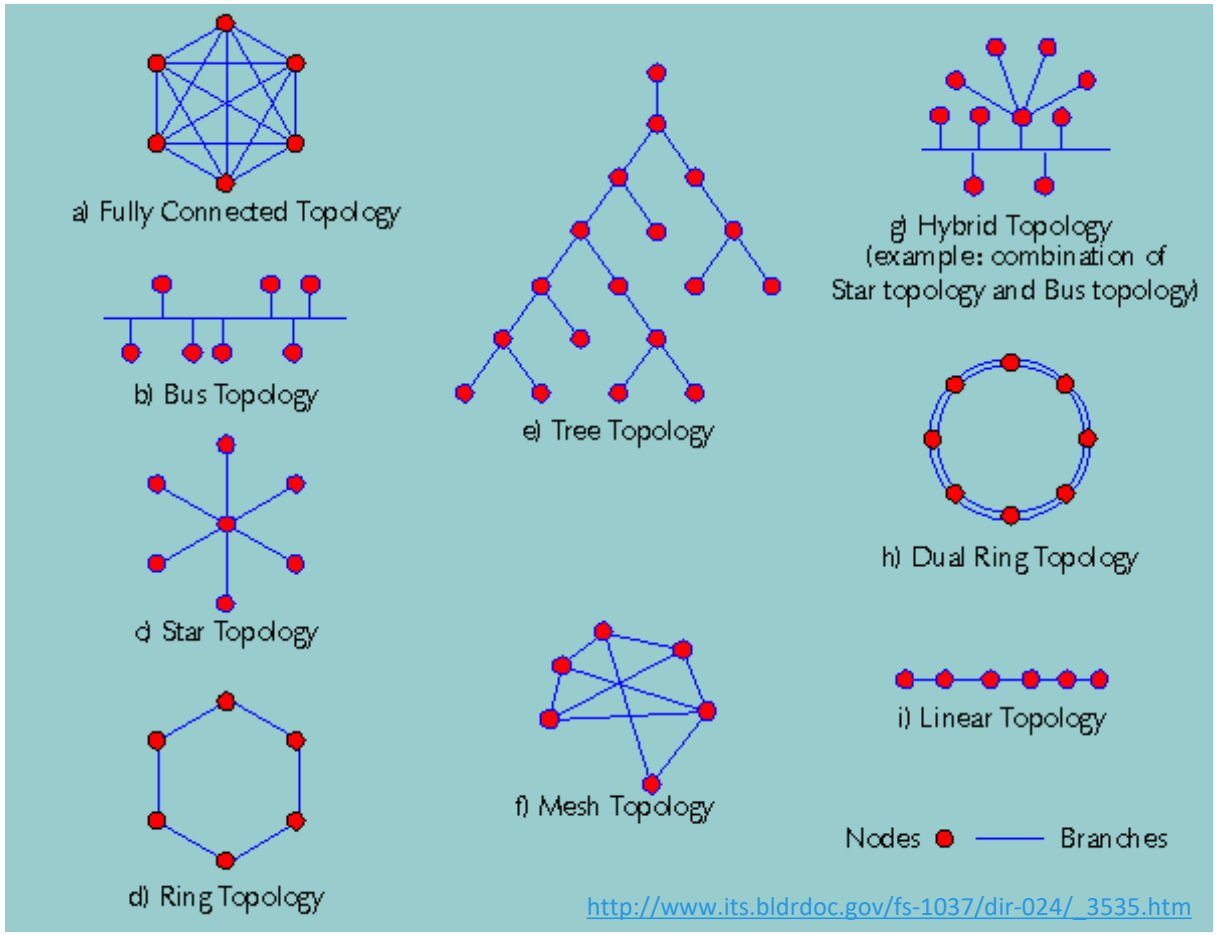
Star: all nodes connected to a central node, all traffic passes through this node (switch?)

- Links between nodes are one to one (no collision?)
- Easy to add new nodes

Ring: each node connected to two neighbors, all nodes constitute a closed loop. Signals pass through the nodes in a determined direction

- Each node has an in-interface and an out-interface in a physical ring. Usually has a "Token Passing" scheme. The node with the token can attach a message to it
- What happens if one node fails?

Network topologies



http://www.its.bldrdoc.gov/fs-1037/dir-024/_3535.htm

Communication – protocols

Multivendor devices, many devices in network:

- In order to communicate directly (one link), devices must agree how signals should be transmitted/interpreted (devices need to be able to interpret/handle receiving data)
- Two program-instances on two computers need to be in agreement which messages are OK to send which are not. In addition, if message passes through other devices (with their program-instances responsible for forwarding data) – they too need to be in agreement how to interpret parts of message that they need to interpret (how to forward message)

Protocol (networking):

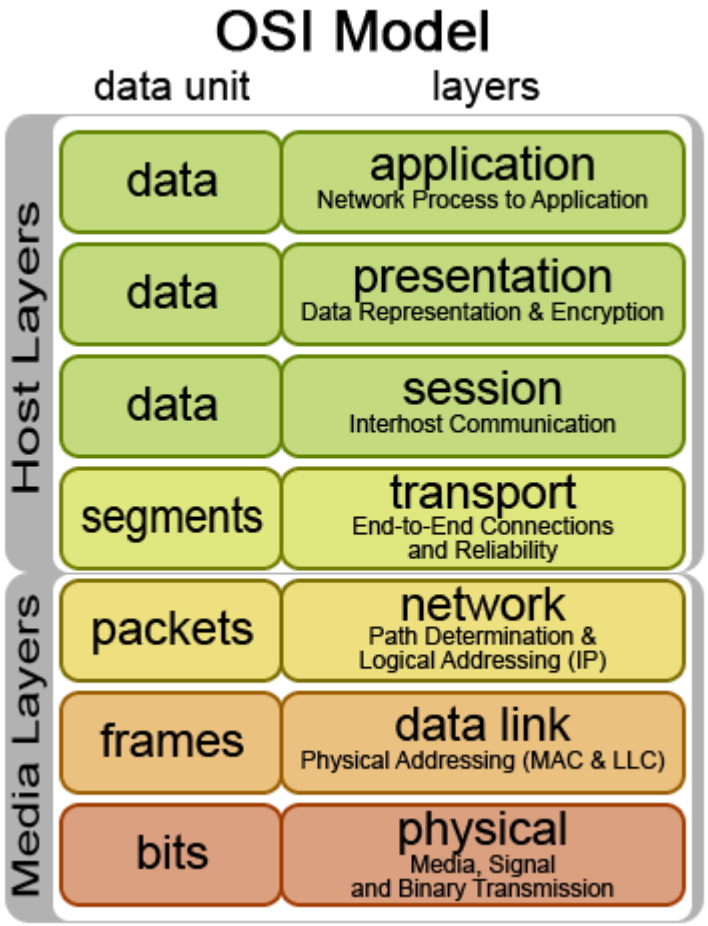
- **set of rules and/or procedures** for exchanging data between electronic devices/programs/program components
- set of rules governing communication between communication partners
- Examples:
  - RS232 – a protocol for point-to-point communication (representation of information as bits, …)
  - IPv4 – a protocol for communication in network (addressing, …)
- "Protocol" – "implementation of protocol" – "instance of implementation of protocol"

OSI model

"The purpose of this Reference Model of Open Systems Interconnection is to provide a common basis for the coordination of standards development for the purpose of systems interconnection, while allowing existing standards to be placed into perspective within the overall Reference Model." (ISO/IEC 7498-1:1994)

The model is essentially a data communications management structure, which brakes data communications down into a manageable hierarchy of seven layers. Each layer has a defined purpose and interfaces with the layers above and below

- Practical Industrial Data Communications (Reynders, Mackay, Wright)



OSI model

Reference model for (data)communication. Communications between participants are split in seven abstraction layers:

- **Application layer (L7)**: protocols within this layer ensures that programs can transfer files, send e-mails ant otherwise perform services over the network
  - HTTP, HTTPs for web-browsers, FTP fil filtransfer, SMTP – epost, Telnet, SSH - terminaler
- **Presentation layer (L6)**: if two nodes are communicating at a different format the protocols within this layer ensures proper translation to a common format. Compressing/decompressing of data. Encryption/decryption of data.
- **Session layer (L5)**: protocols within this layer enable users to create connections (sessions).
- **Transport layer (L4)**: protocols in this layer ensures that data arrives at the destination properly (segmentation, flow control, …). Large amounts of data are divided into appropriate segments and numbered.
  - Examples: TCP, UDP

OSI model

Reference model for (data)communication. Communications between participants are split in seven abstraction layers:

- **Network layer (L3)**: protocols facilitates packet addressing for transmission between multiple networks. Protocols for finding appropriate route if there are several paths for the data are alså on this level.
  - Examples: IPV4, IPV6, OSPF, BGP, …
  - (Layer 2 protocols enables addressing within one network)
- **Transport layer (L2)**: This layer produces small frames of the raw bit stream from the physical layer. These frames are labeled with the address of the receiver (and sender). The layer also defines error correction, procedures for re-sending, procedures for data rate adjustment
- **Physical layer (L1)**: The physical layer is the physical link between the devices on the network. Focuses on sending and receiving raw data bits over the physical connection. Specifies the mechanical and electrical interfaces to create and maintain the physical connection. The standards at this layer mostly defines wiring, plugs and connectors.

OSI model

A given layer in the OSI model generally communicates with three other OSI layers:

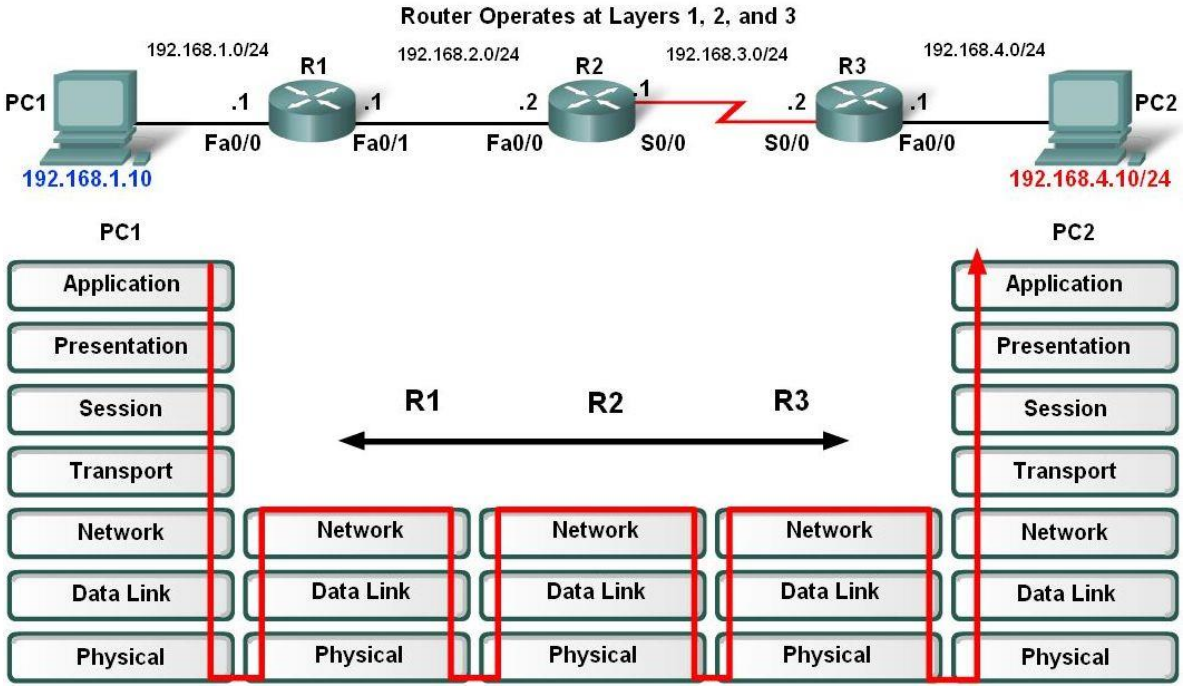
- The layer directly above it
- The layer directly below it
- Its peer layer in other networked computer systems

The Application layer in System A, for example, communicates with the network layer of System A, the physical layer of System A, and the data link layer in System B.

OSI model

An instance of a program on PC1 is sending a message to an instance of (another?) program on PC2. Data is passing several network devices (three routers in this case).

Devices are using (implementations of) different protocols that are ensuring that receiver gets the message



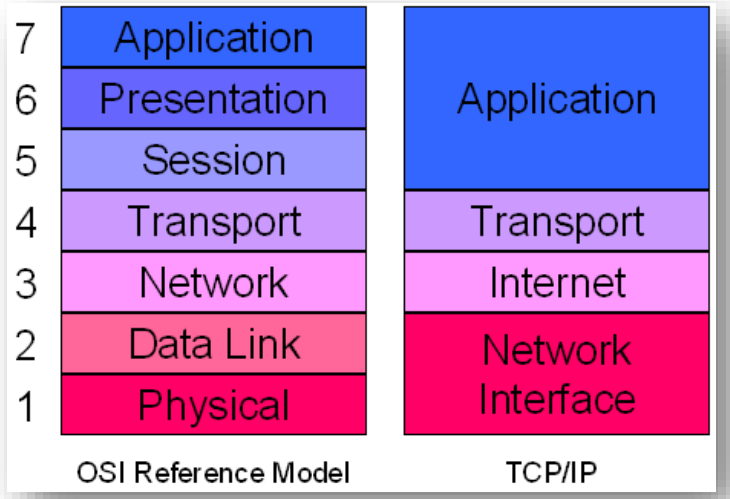
TCP-IP architecture

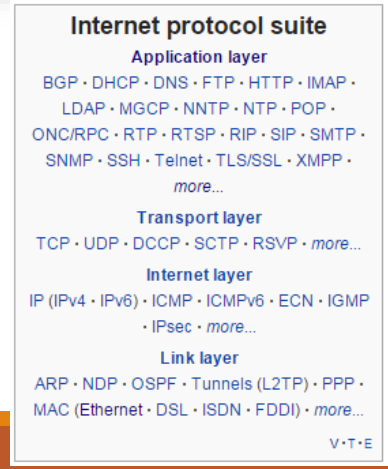
TCP-IP architecture: alternative to OSI model, partially corresponds to OSI

- TCP and IP are most significant protocols – hence name

4 layers:

- Application: application protocols used by process-to-process communication
- Transport:
  - Usually TCP – Transaction Control Protocol
  - Splitting messages into a number of packets
  - Labelling the packets with packet number
  - Request missed packages
  - Adjust transmission rate to a rate that gives an acceptable package loss
- Internet:
  - This layer holds IPv4 and IPv6
  - Addressing and network related services (security, errors during message-transit, …)
- Network interface
  - Correspond to L2 and L1 in OSI





Discussion

Look up three protocols used for data exchange

- What are they used for?
- Where in OSI model do they reside?

Types of network (by scope)

Division with respect to “geographic” scope (and often related to technologies that are used):

- Personal (PAN)
- **Local (LAN)**
- Metropolitan (MAN)
- Wide (WAN)

Other “geographic” entites exist: regional, campus, …

Need for identifiers in a network

A devices that are supposed to talk to each other may not be directly connected.

Message from device A (sent to device B) may need to pass several other devices in order to reach B. This creates necessity for some sort of identification – destination must be identified (in order to transmit data), message origin of data must be identified (if reply is to be sent and/or for other purposes)

Unique (within the network) identifier (**address**) is needed

- MAC addresses for Ethernet-networks
- IP addresses for IP networks (IPv4, IPv6)

Networks: L2 network

A (L2) network will we define as group of devices (that are connected/reachable - directly or indirectly) - that may exchange information by using L2 protocol

- Your home devices (computers, TV, streamer, …) may be L2 network
- A group of devices in a (part of a?) company/organisation/institution
  - Companies usually use many L2-networks that are connected
  - HVL networks: students, staff, management?, …'

LAN (local area networks) are L2 networks? – often but it depends on who you talk to ☺

Ethernet and ethernet networks

Ethernet:

- A family of network technologies for LANs (protocols within layer 1 and 2 in the OSI reference model)
- Standardized in IEEE 802.3 for wired networks and in IEEE 802.11 for wireless networks

Unique identifiers: 6x8bit identifiers

- First three bytes: producer (organizationally unique identifier)
- Last three bytes: unique identifier
- (Sidemark: see also universaly vs. localy adminstred)

MAC addresses are used for identifying sender/receiver in L2 (ethernet) networks

Devices in a L2 network

Computers (network adapter)

Switches (L2)

- Specialized computers
- Computers are usually connected to these
- Forwards messages (packets)
- Learning (use MAC-tables) – need for broadcast is greatly reduced
  - How does switch learn

Router (for access to Internet or other L2 networks)

- router separate L2 networks (by its operation)
- discussed later in this presentation

Hubs, Bridges and Repeaters are today largely replaced by switches/better cables

Discussion

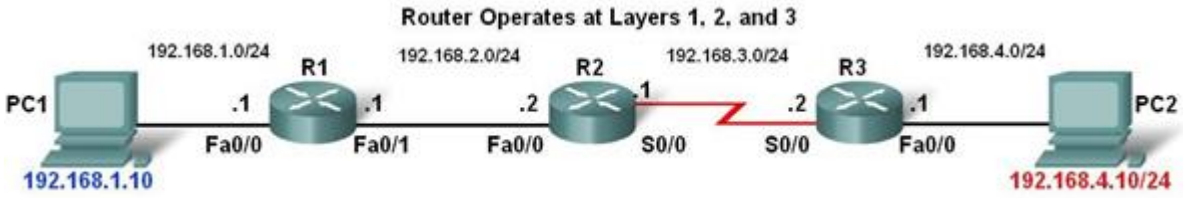
Could we use MAC-addresses as global identifiers (between ALL devices)?

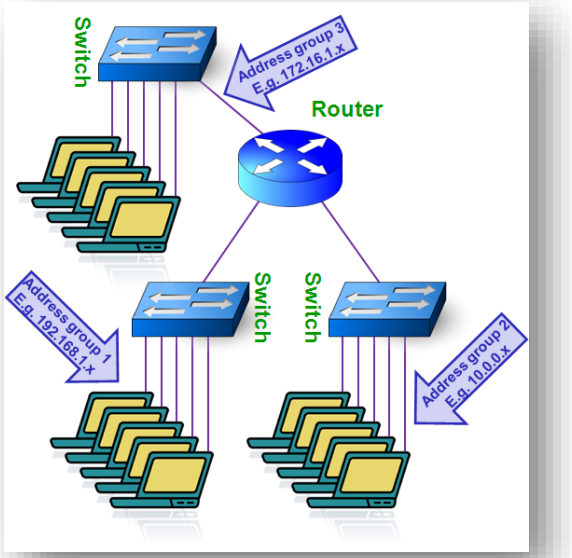
(Do we need IP addresses?)

L3 networks

A (L3) network will we define as group of devices (that are connected/reachable - directly or indirectly) - that may exchange information by using L3 protocol (that in turn use L2 protocols ☺)

L3 networks may span over multiple L2-networks



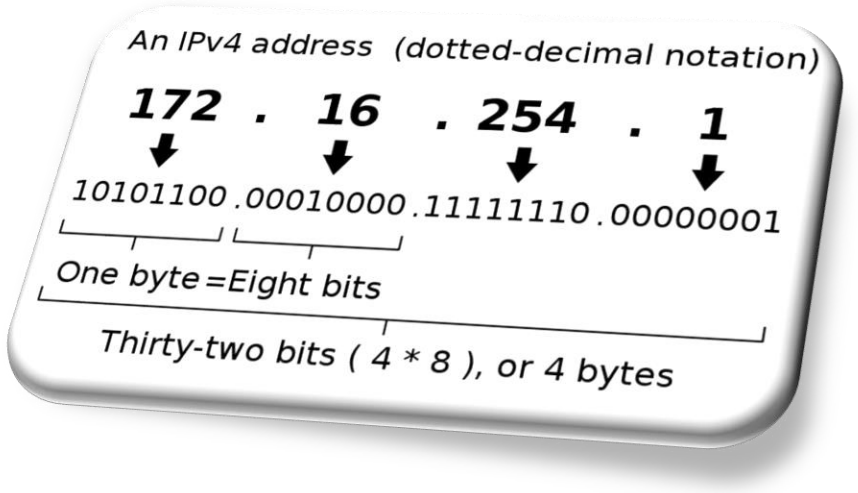


IP and networks that use IP

Provides the logical connection between network devices by providing identification for each device

IPv4:

- 32 bits identifiers, usually expressed as 4 numbers [0,255] separated by dot (.)
- 2^{32} = 4 294 967 296 addresses
  - Lack of available addresses is a problem (IPv6 is discussed later in this course)
- 0.0.0.0 – 255.255.255.255 (but some addresses are used for special purposes)



Network (L3) devices

Computers (network adapter)

Routers

- Responsible for forwarding packet, based in IP-address of destination (sending on appropriate link in order to reach destination)
- May be configured to be able to learn/update route-information
- May be configured to do additional services (packet filtering/firewalls, DHCP services, …)

L3 Switches

- Some (advanced) switches may perform (in addition to switching operation) number of responsibilities that routers do – these are called L3-switches

One may also use specialized devices that perform special operations such as security

IP - subnets

In order to make routing process (forwarding of IP-packets) manageable, IP addresses are grouped into groups that we refer to as **networks** (in some discussions) and **subnets** (in other discussions ☺).

This is done by adding **subnet mask**: 32 bits of "1-s followed by 0-s"

- Subnet mask is also written as A.B.C.D where A, B, C, D are numbers in the interval [0,255] but we will see that only some numbers in this intervals may be used: 255, 252, 224, ...
- Subnet mask is also written as /N where N is number of '1'-s in subnet mask

Example (subnet mask):

- 11111111 11111111 11111110 00000000
- 255.255.254.0
- /23

Subnet mask logically divide network-address in two parts:

- **Network identifier** part (first X bit of an address that correspond to 1-s in subnet mask)
- **Host identifier** part (last Y bit of an address that correspond to 0-s in subnet mask)

Network address

Two hosts are considered in same network if they have same network identifier

Network address (address of a network) is a number that we get when we take network identifier part of an address and fill the rest (of 32 bits) with 0-s

Network address identifies all addresses that belong to same network (same subnet).

- Use of subnet masks divides address-space in subnets
- Different organisations use different subnets/network addresses

With respect to host part of an address:

- Two devices in same network (subnet) cannot have same host identifier (we need unique identifiers)
- No host in a network may have only 0-s as its host identifier part (that would be network address)
- No host in a network may have only 1-s as its host identifier part (used for broadcast)

Routers use network addresses of destination (and not precise host addresses) when decision is made where to forward a packet – routing tables are filled with network addresses

Discussion / assignment

Find your host address (that your computer is using today) – together with subnet mask

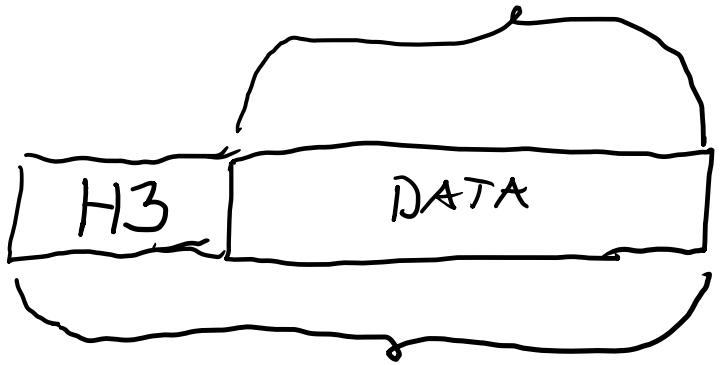
- Use `ipconfig` command in console window

Calculate

- address of your network
- address range of that network – possible addresses (used or not)

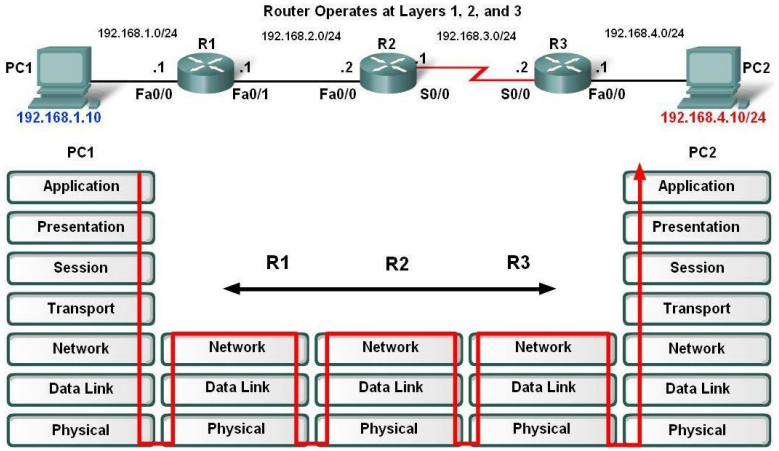
Are our computers in a same network?

FRA TRANSPORTLAGET
(L4)

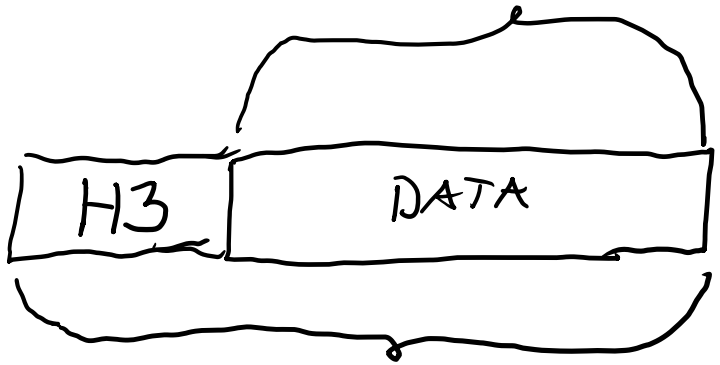


NETTVERKSLAGET
(L3)

TIL DATALINKLAGET
(L2)

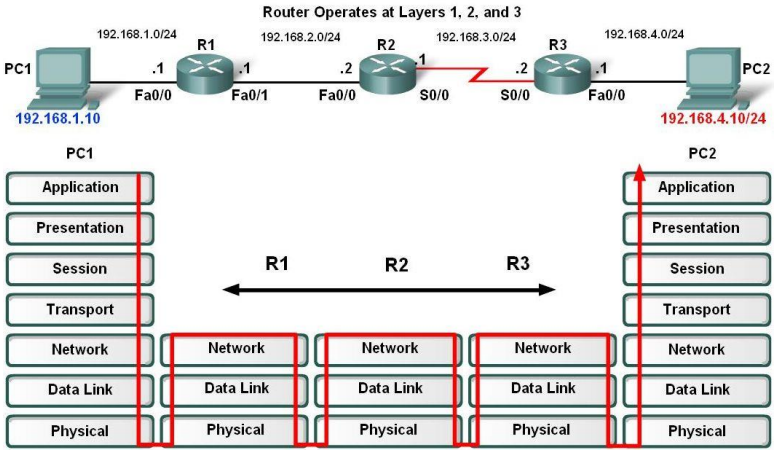


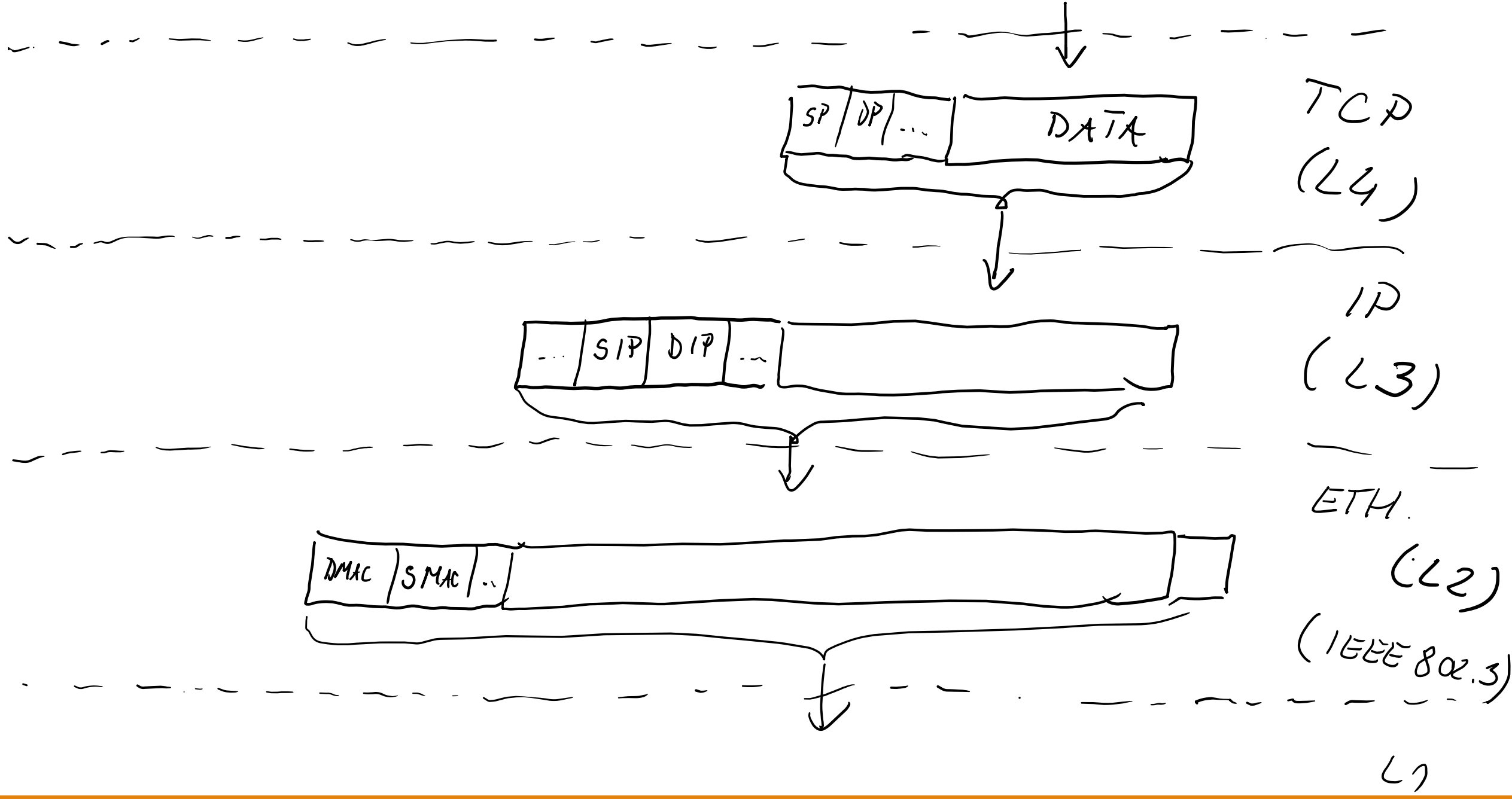
TIL TRANSPORTLAGET
(L4)

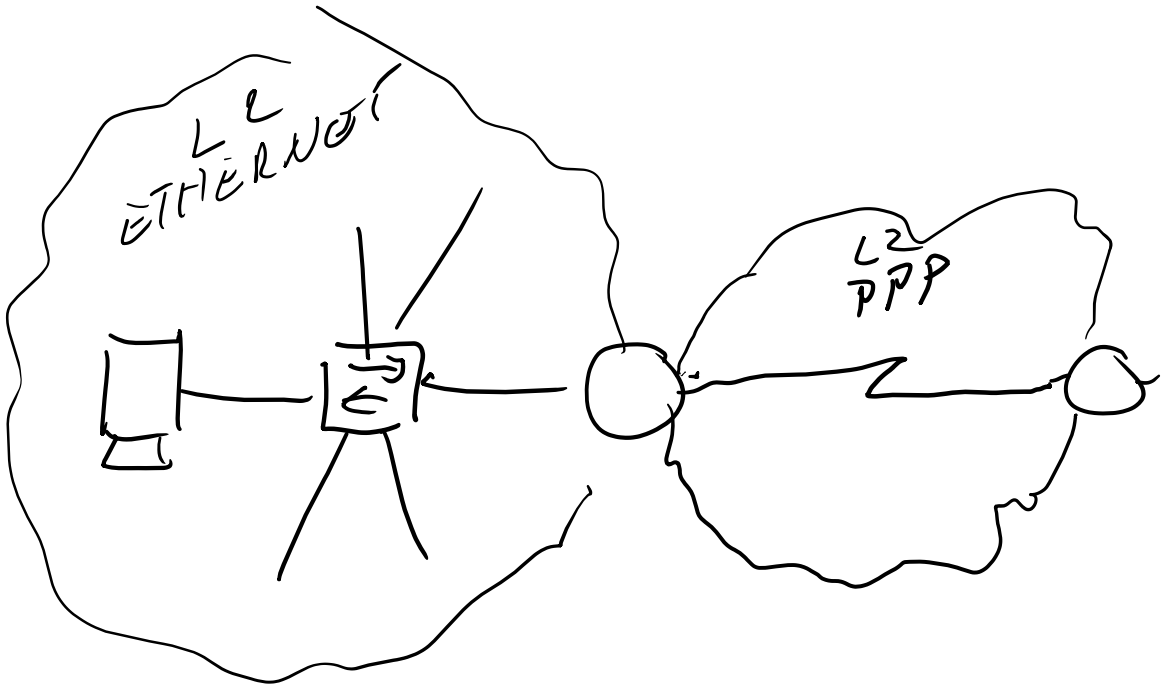


NETVERKSLAGET
(L3)

FRA DATALINKLAGET
(L2)




SP
DP
...
DATA
TCP
(L4)
...
SIP
DIP
...
IP
(L3)
DMAC
SMAC
..
ETH.
(L2)
(IEEE 802.3)
L1



A . B . C . D / X

Exercises

For given addresses (with masks), calculate

- Network and host identifier part
- address of a network
- address range of that network – possible addresses (used or not)
- Addresses:
  - 192.168.0.10 / 24
  - 192.168.1.10 / 23
  - 192.168.2.10 / 23
  - 192.168.10.10 / 22
  - 192.168.12.254 / 22

Are any of addresses in same network?

192.168.0.10 /24

192.168.0.0 – NETTVERKS ADRESSE

.1 } HOSTS / ...

.254 }

.255 – BROADCAST

192.168.1.10 /23

192.168.00000001.00001010

23

192.168.0.0

.0.1

.0.255

.1.000

.1.254

.1.255

192.168.10.10 /22

192.168.00001010.00001010

00001000.00000000

192.168.8.0/22

192.168.8.254/22

192.168.00001000.11111110

00001000.00000000

192.168.8.0/22

00001000.00000001 ~ 192.168.8.1

00001000.11111111 ~ 192.168.8.255

00001111.11111110 ~ 192.168.15.254

} HOSTS + ...

00001111.11111111 ~ BROADCAST

Discussion

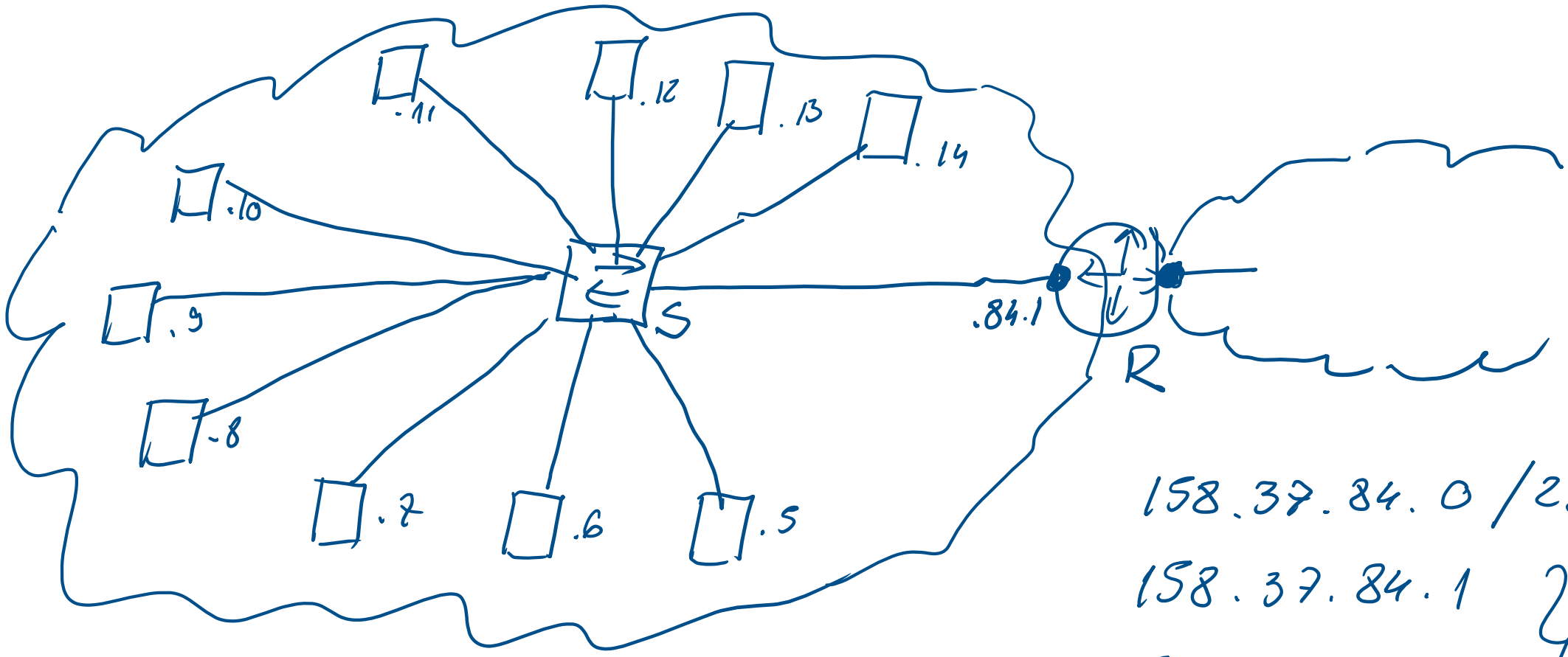
We want to connect 10 hosts in single network and connect it to Internet.

Identify devices that you need.

You are given address 158.37.84.0 / 24 but you should try to make minimum possible subnet that have enough of addresses in order to connect hosts.

Assign IP addresses to each device that needs an address

11 = 10 + 1 IP-ADRESSE



158.37.84.0 /28

158.37.84.1

158.37.84.14

(.15) - BROADC.

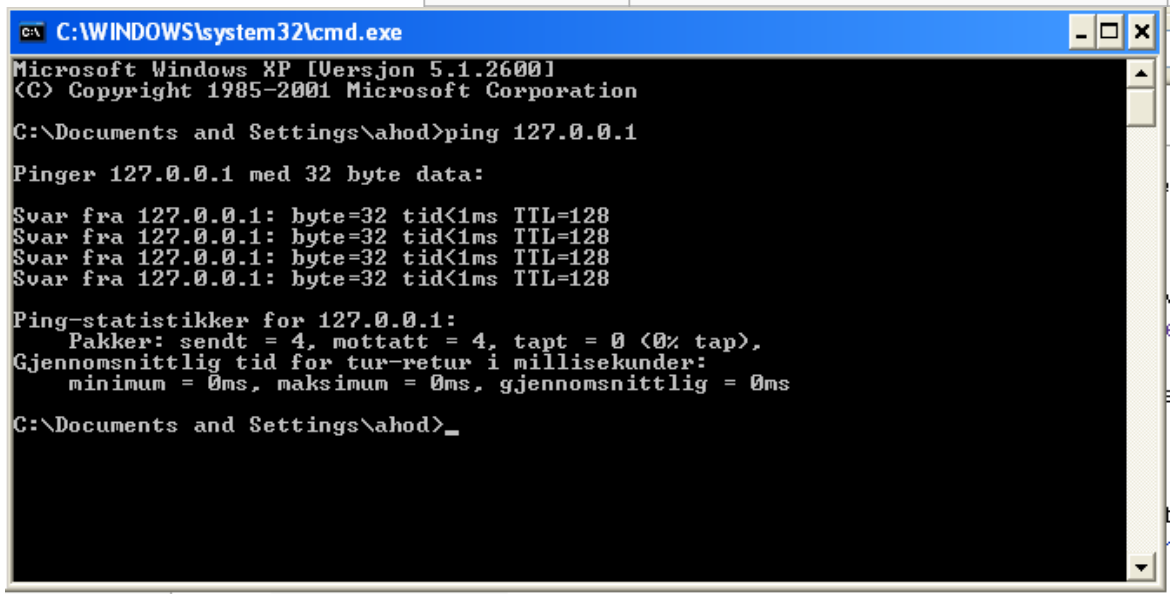
Special IPv4 adresses: **loopback**

«Localhost» adresse («loopback interface»)

Used for testing (127.0.0.1):

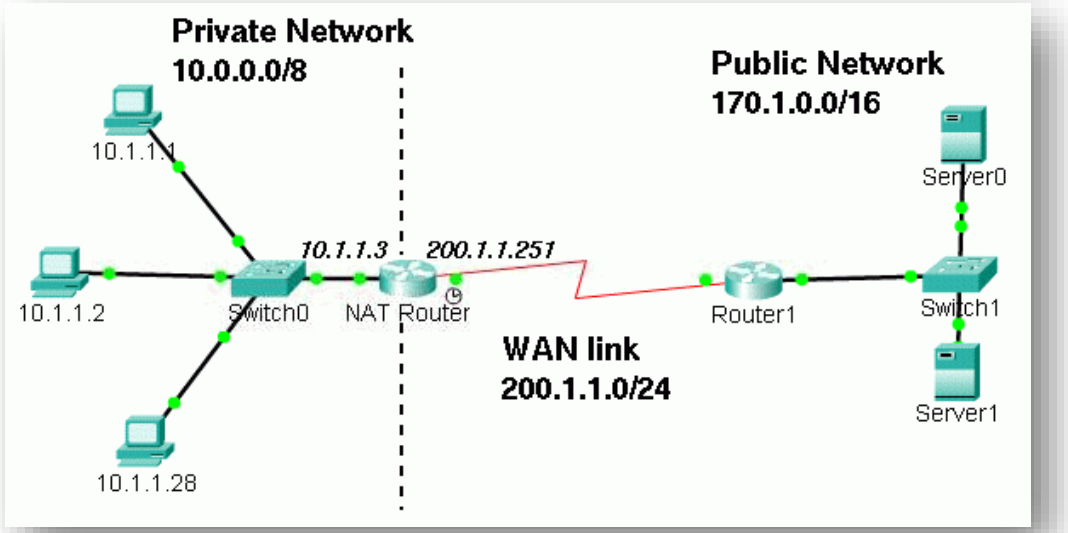
- IP stack testing («ping»)
- Programming: developing/testing of server and client applications that are run on single computer (during testing)
- Any address in 127.0.0.0/8 may be used (but still we cannot use network- and broadcast address)

CIDR address block	Description
0.0.0.0/8	Current network (only valid as source address)
10.0.0.0/8	Private network
14.0.0.0/8	Public data networks (per 2008-02-10, available for use[1])
127.0.0.0/8	Loopback
128.0.0.0/16	Reserved (IANA)
169.254.0.0/16	Link-Local
172.16.0.0/12	Private network
191.255.0.0/16	Reserved (IANA)
192.0.0.0/24	Reserved (IANA)
192.0.2.0/24	Documentation and example code
192.88.99.0/24	IPv6 to IPv4 relay
192.168.0.0/16	Private network
198.18.0.0/15	Network benchmark tests
223.255.255.0/24	Reserved (IANA)
224.0.0.0/4	Multicasts (former Class D network)
240.0.0.0/4	Reserved (former Class E network)



Special IPv4 adresses: **private adresses**

CIDR address block	Description
0.0.0.0/8	Current network (only valid as source address)
10.0.0.0/8	Private network
14.0.0.0/8	Public data networks (per 2008-02-10, available for use[1])
127.0.0.0/8	Loopback
128.0.0.0/16	Reserved (IANA)
169.254.0.0/16	Link-Local
172.16.0.0/12	Private network
191.255.0.0/16	Reserved (IANA)
192.0.0.0/24	Reserved (IANA)
192.0.2.0/24	Documentation and example code
192.88.99.0/24	IPv6 to IPv4 relay
192.168.0.0/16	Private network
198.18.0.0/15	Network benchmark tests
223.255.255.0/24	Reserved (IANA)
224.0.0.0/4	Multicasts (former Class D network)
240.0.0.0/4	Reserved (former Class E network)
255.255.255.255	Broadcast



«**private**» means that we may use addresses within an organisation (or home/company/…), but not on Internet

IPV4 – «Network Address Translation» (NAT)

"Network Address Translation (NAT) is a service that enables private IP networks to use the internet and cloud. NAT translates private IP addresses in an internal network to a public IP address before packets are sent to an external network."

[https://www.cisco.com/c/en/us/products/routers/network-address-translation.html]

May be:

- "Many → few addresses"
- "Many → one address"
- "**Many → one address (+ port number)**"
  - Port address translation (PAT)

May enhance security as additional benefit

May create additional challenges for some communication technologies (including some security technologies)

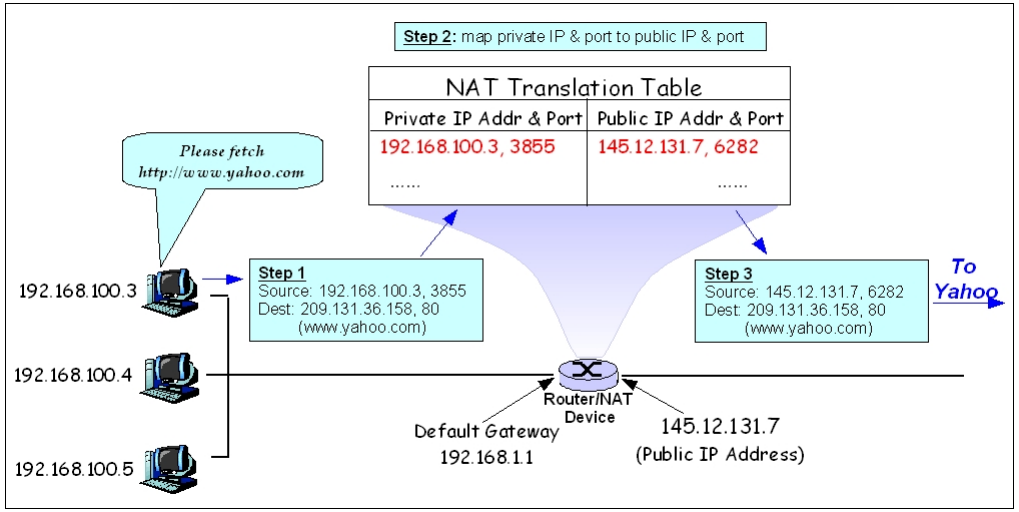


Figure from: https://en.wikipedia.org/wiki/Network_address_translation

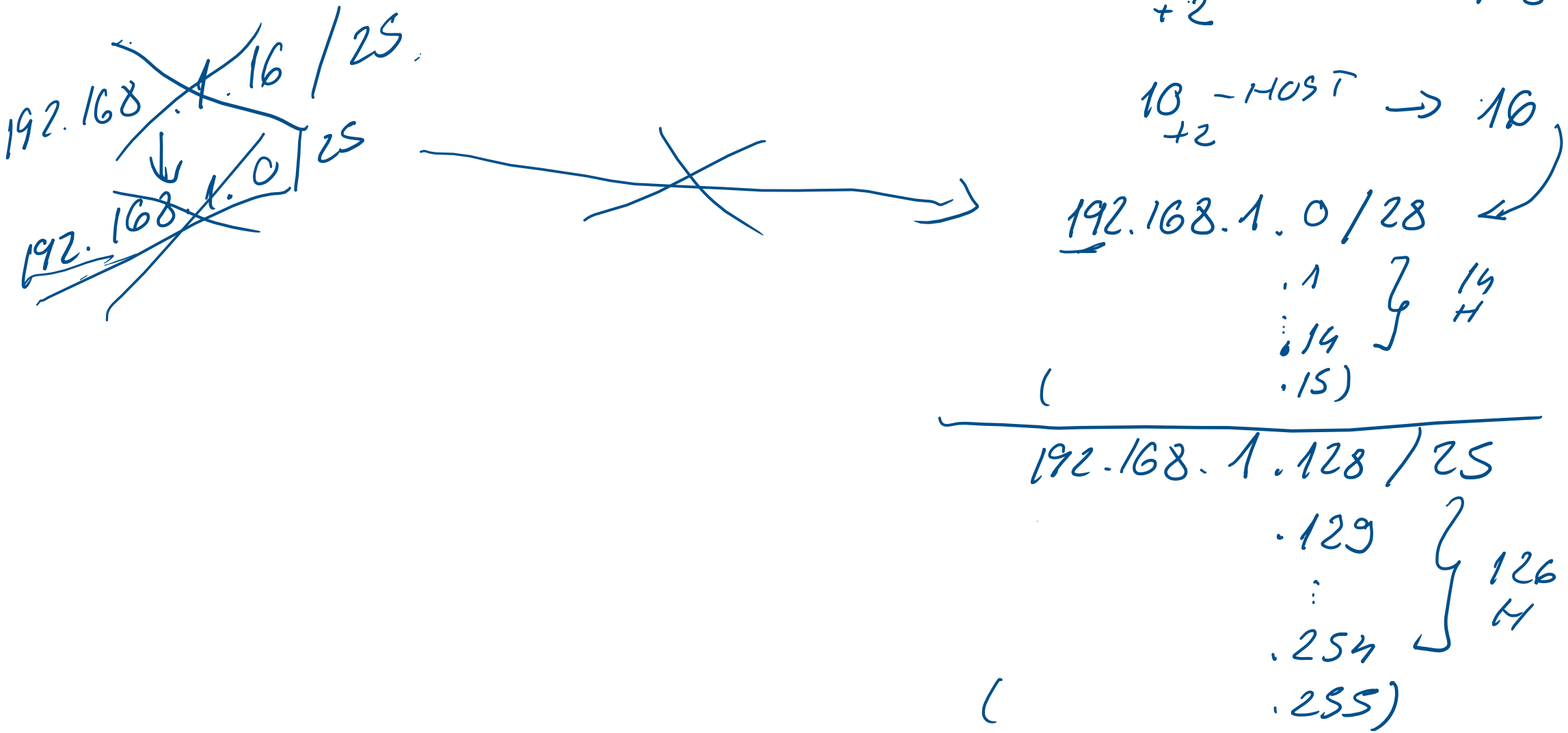
Discussion

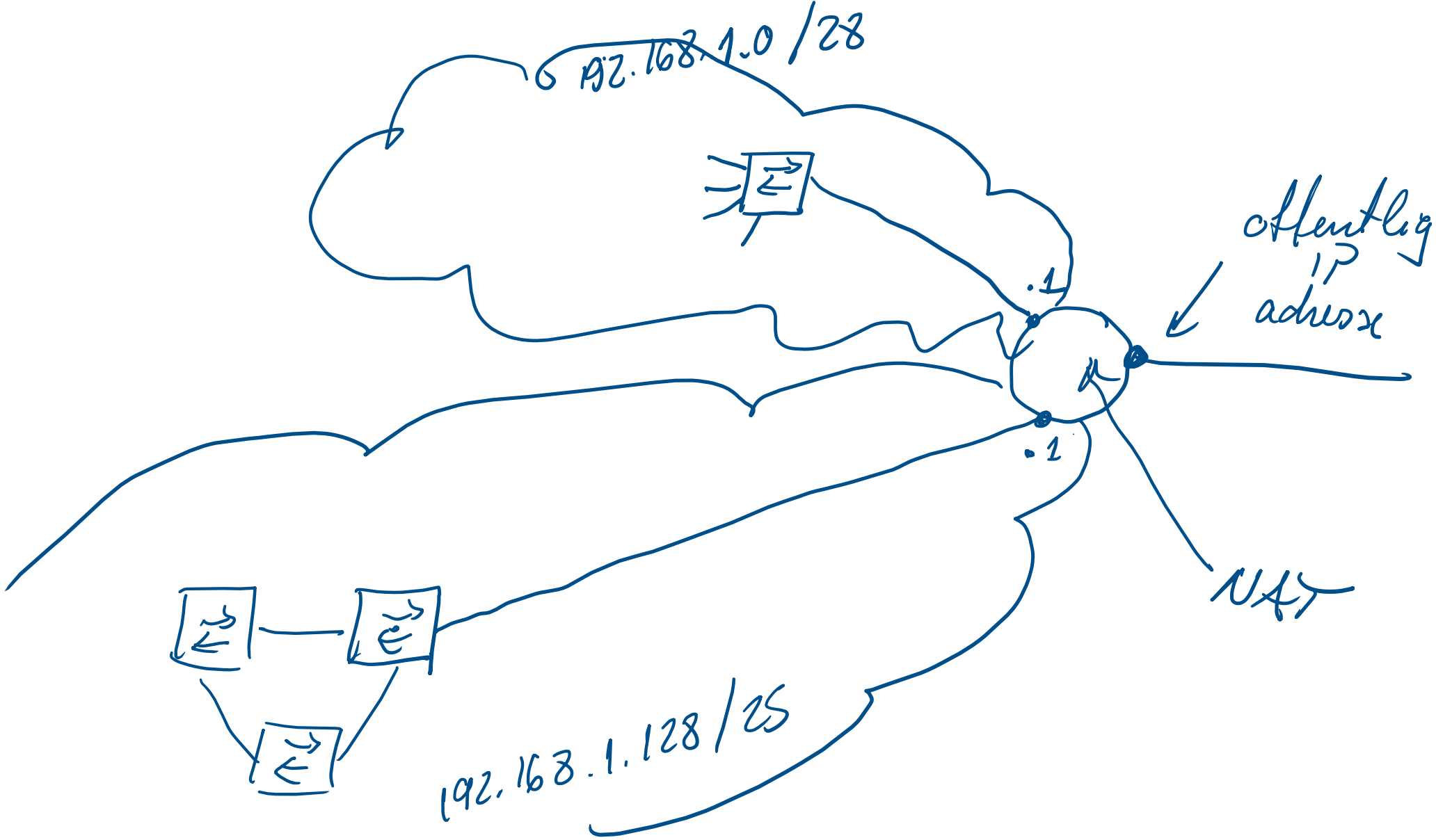
We want to connect up to 100 hosts in a network and connect it to Internet. In addition, we need additional network with up to 10 server hosts.

Identify (networking) devices that you need.

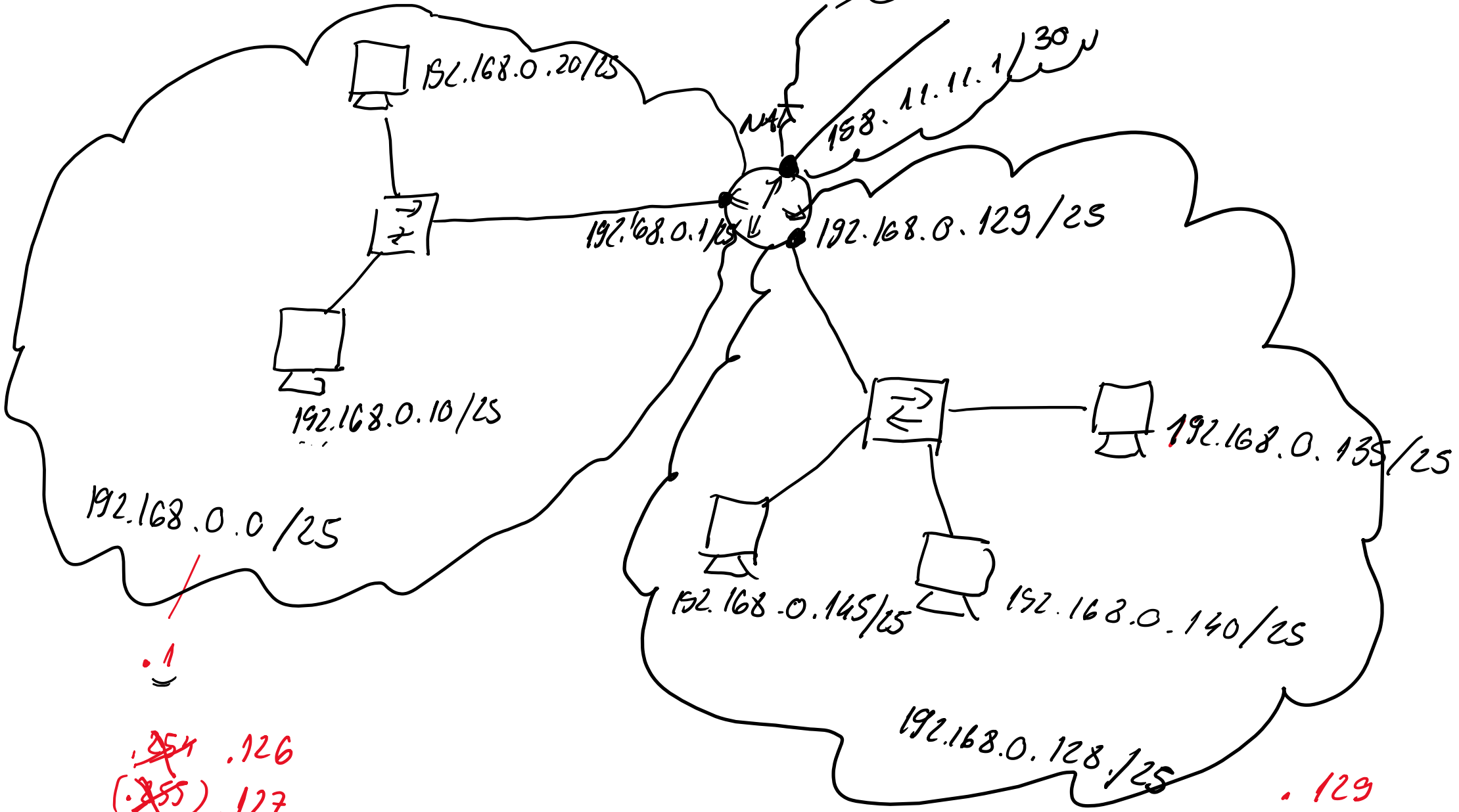
You are given address 192.168.1.0 / 24 but you should try to make minimum possible subnet that have enough of addresses in order to connect hosts.

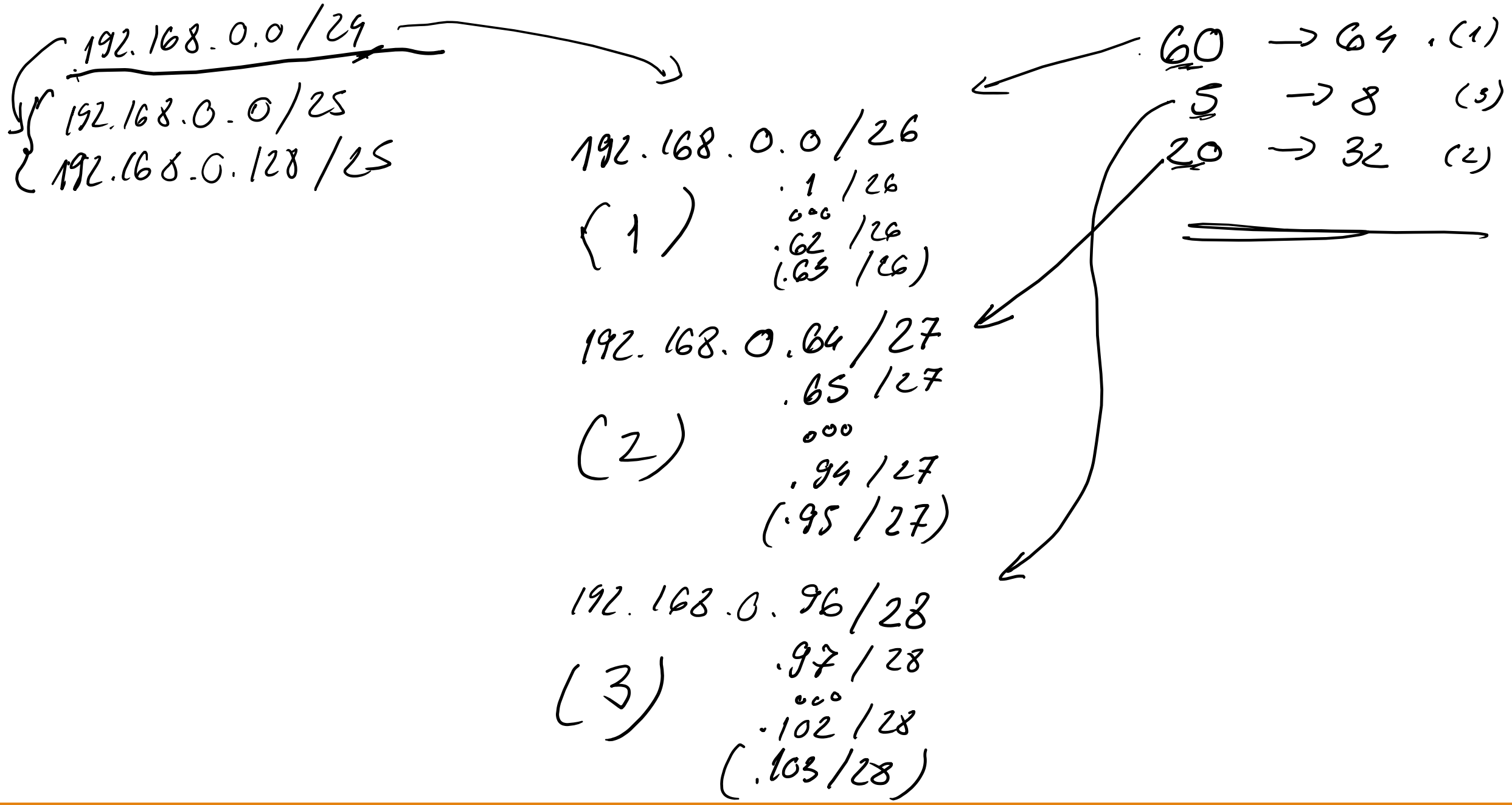
Assign IP addresses to each device that needs an address


192.168.1.0 /24
100 +2 - HOST -> 128
10 +2 - HOST -> 16
192.168.1.0/28
.1
.14
(.15)
14 H
192.168.1.128/25
.129
.254
(.255)
126 H
192.168.1.16/25
192.168.1.0/25
192.168.1.0


192.168.1.0/28
.1
offentlig IP adress
.1
NAT
192.168.1.128/25

ADA512


192.168.0.20/25
NAT
158.11.11.1/30
192.168.0.1/25
192.168.0.129/25
192.168.0.10/25
192.168.0.135/25
192.168.0.0/25
192.168.0.145/25
192.168.0.140/25
192.168.0.128/25
.1
.126
(.255).127
.129
.254
(.255)


192.168.0.0/24
192.168.0.0/25
192.168.0.128/25
192.168.0.0/26
.1/26
...
.62/26
(.63/26)
(1)
192.168.0.64/27
.65/27
...
.94/27
(.95/27)
(2)
192.168.0.96/28
.97/28
...
.102/28
(.103/28)
(3)
60 → 64 . (1)
5 → 8 (3)
20 → 32 (2)

«Domain Name System» (DNS)

Domain name: (human-friendly) string of text that may be translated into IP address

- Domain name registrar

DNS is a service that translates domain names into IP addresses

- wikipedia.org → 185.15.59.224
- wikipedia.org → 2a02:ec80:300:ed1a::1: (IPv6 address)
- vg.no → 195.88.55.16
- …

Dynamic Host Configuration Protocol (DHCP)

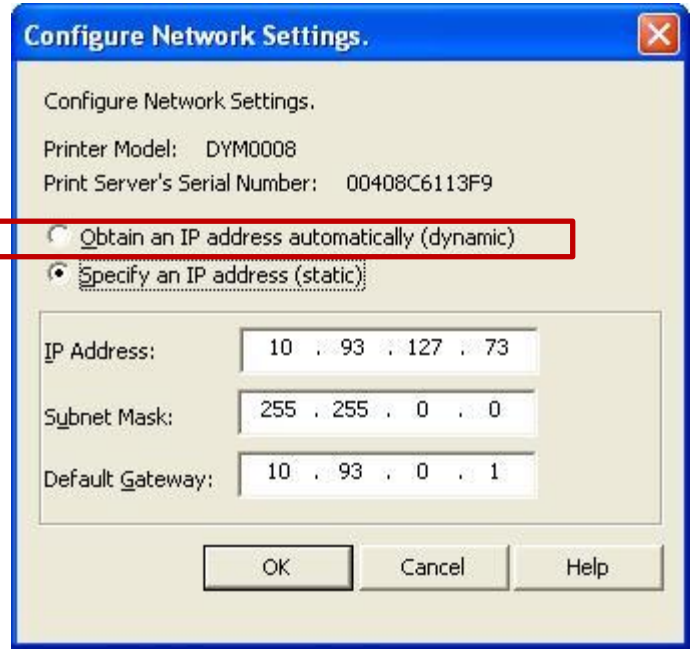
Manual configuration of IP addresses may be impractical

DHCP is client-server protocol that is used (by IP host as client) to automatically obtain available IP address (from DHCP-server) and related info (mask, default gateway, …) in network

Service may be performed by router

Lease time / renewal

// Cisco router configuration:
R1(config)#ip dhcp excluded-address 192.168.0.1 192.168.0.254
R1(config)#ip dhcp pool DHCP_GJEST
R1(dhcp-config)#network 192.168.0.0 255.255.255.0
R1(dhcp-config)#default-router 192.168.0.1
R1(dhcp-config)#dns-server 192.168.0.1



DHCP process

Figure 1: https://www.ibm.com/docs/en/i/7.1?topic=concepts-dhcp-clientserver-interaction

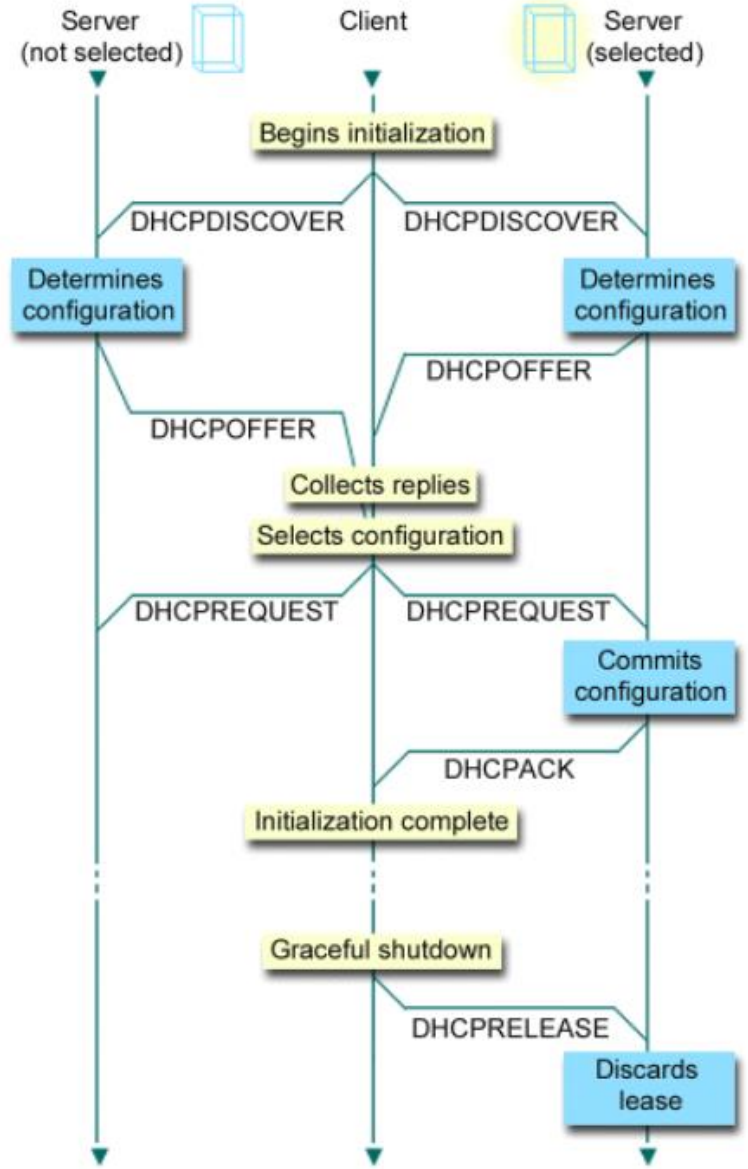
Discover: Client → Server
- L3 (and L2) broadcast (255.255.255.255, FF FF FF FF FF FF)

Offer: Server → Client
- L2 unicast or L3 broadcast

Request: Client → Server
- L3 (and L2) broadcast

Acknowledge: Server → Client
- L3 unicast

Figure 1. DHCP client-server interaction



Routing of traffic - supernets

Superneting is a process of (logically) combining of small networks in single **supernetwork**

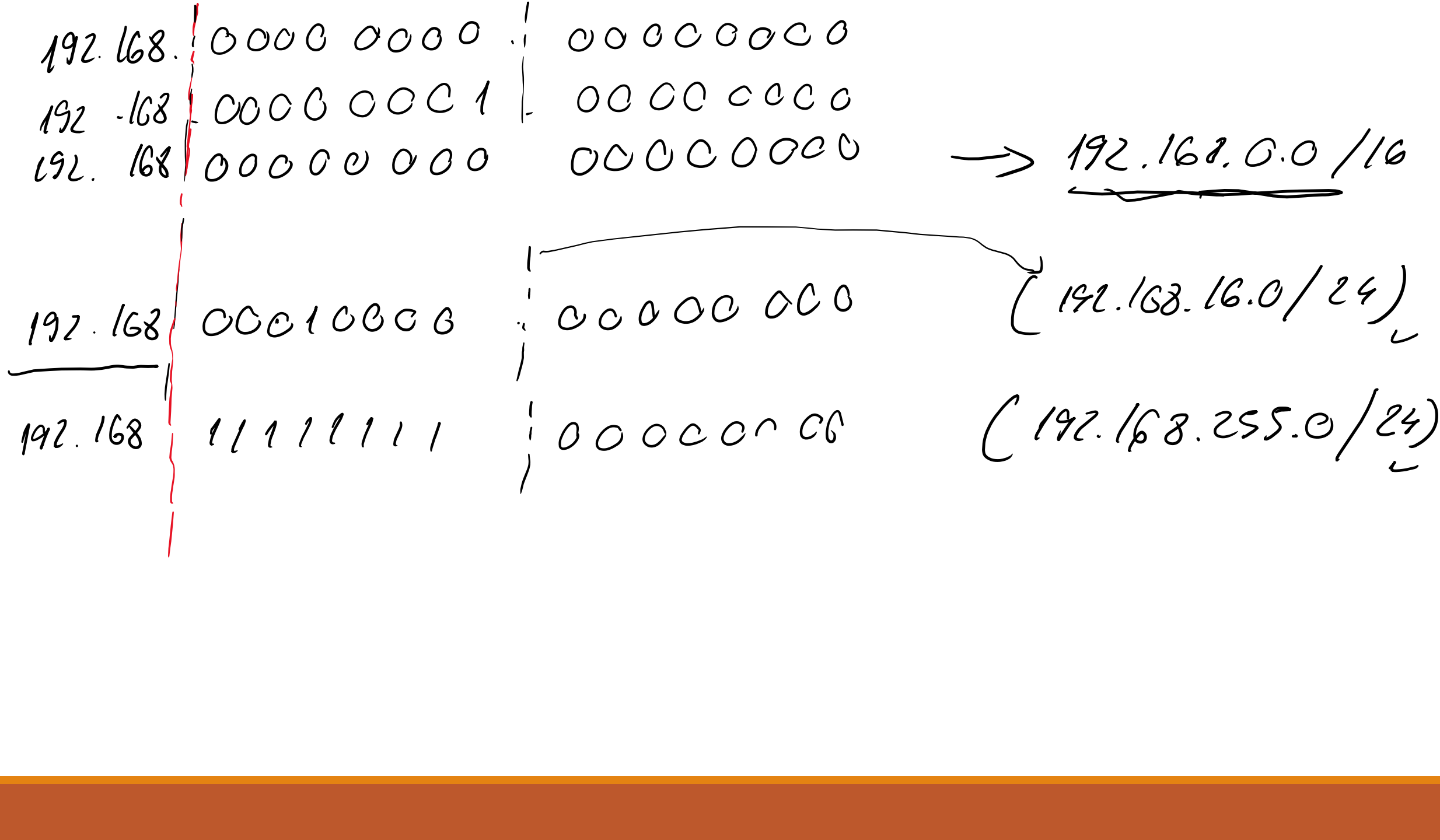
We may combine several (sub)networks in a supernet that containes subnetworks. Example:

- 192.168.0.0/24 and 192.168.1.0/24 may be combined into 192.168.0.0/23

Use of supernets may reduce length of routing tables two or more related networks may be announced as supernet for routers that are “sufficiently far away”

Notice that network 192.168.0.0 / 16 is also supernet for 192.168.0.0/24 and 192.168.1.0/24 but it also contains many other networks – some examples: 192.168.2.0/24, 192.168.16.0/20, … and many more

- Announcing “to large” supernets to routers may result in unnecessary traffic (packets being dropped later than it could have been) or packet may be sent “wrong way”
- We should attempt to introduce only supernets that do not contain additional addresses that are not part of subnets that are combined into supternet


192.168.
192.168
192.168
192.168
192.168
192.168
192.168.0.0/16
(192.168.16.0/24)
(192.168.255.0/24)

Exercise

Group networks into least possible supernet

- A: 172.16.252.0/24
- B: 172.16.253.0/24
- C: 172.16.254.0/24
- D: 172.16.255.0/24

Does supernet contains any addresses outside A, B, C, and D?

172.16.111111 00 | 00000000
-11- 111111 01 | -11-
-11- 111111 10 | -11-
-11- 111111 11 | -11-

172.16.111111 00 | 00000000

172.16.252.0/24
253.0/24
254.0/24
255.0/24

172.16.252.0/22

000 - (172.16.0.0/24)
001 (172.16.1.0/24)
010 (172.16.2.0/24)

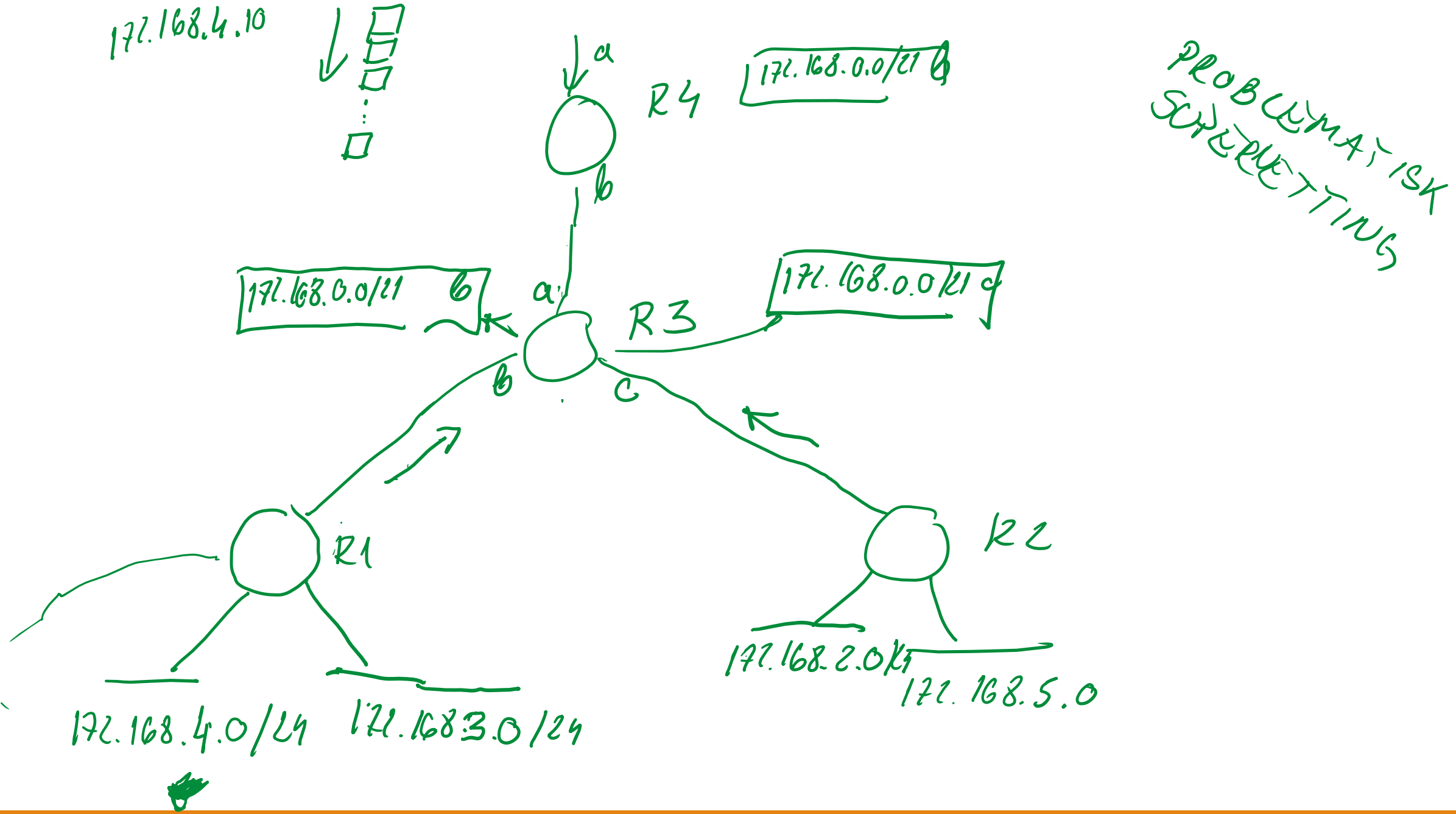
172.16: 0000000 11 | 0000 0000
-11- 000000 100 | 0000 0000
-11- 0000 0101 | -11-
-11- 0000 0110 | -11-

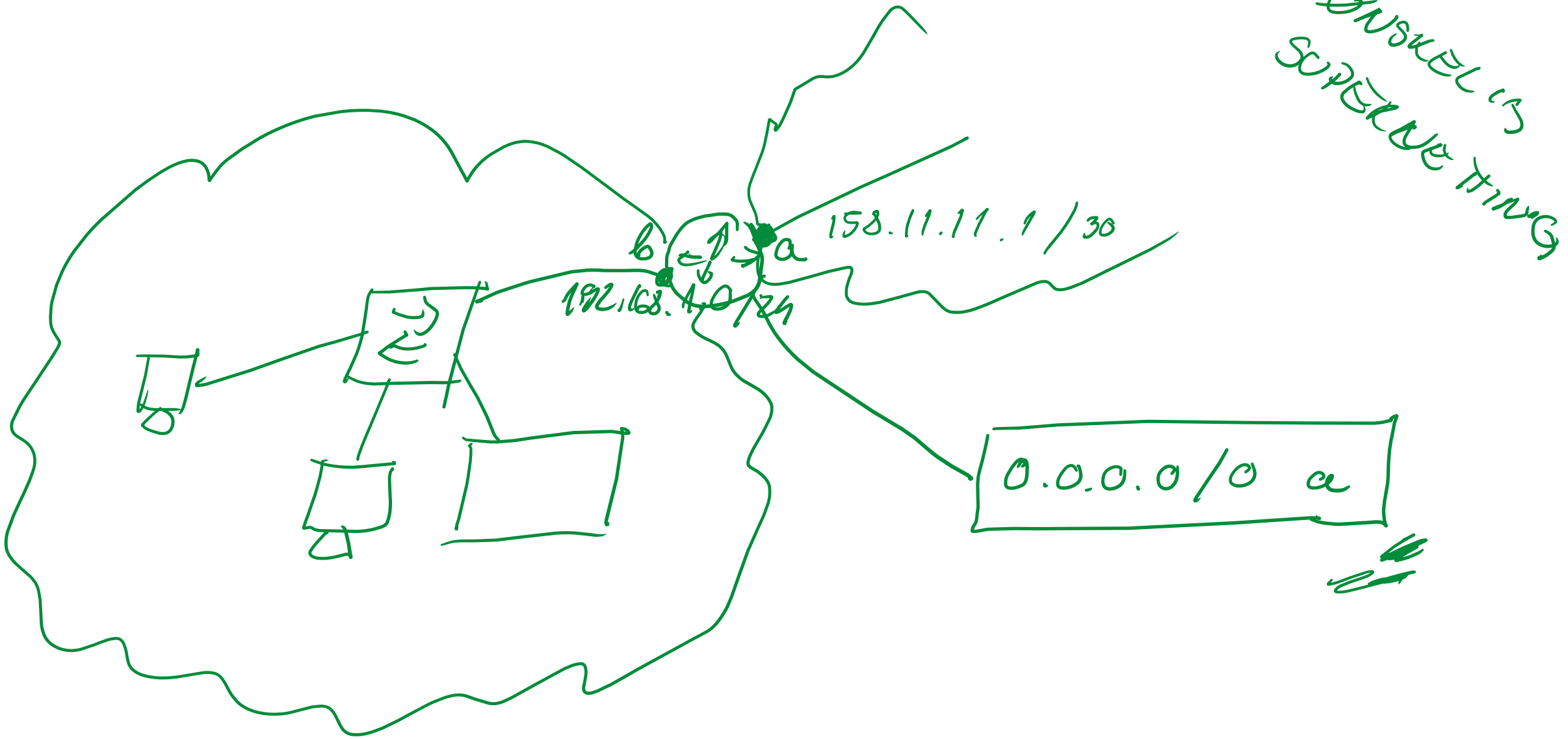
172.16.000 00000 | 000 00000000

111 (172.16.7.0/24)

172.16 .3.0/24 ✓
.4.0/24 ✓
.5.0/24 ✓
.6.0/24 ✓

172.16.0.0/21 ✓


172.168.4.10
a
R4
172.168.0.0/21
b
PROBLEMATISK SCENARIETTING
172.168.0.0/21
b
a
R3
172.168.0.0/21
c
b
c
R1
R2
172.168.4.0/24
172.168.3.0/24
172.168.2.0/24
172.168.5.0


158.11.11.1/30
b
a
192.168.1.0/24
0.0.0.0/0 a

158.11.11.10 / 0

10011100.00001011.0000 1011.00001010

00000000.00000000.00000000.00000000

00000000.00000000.00000000.00000000

0.0.0.0 / 0

Transport layer: port numbers

An IP address identifies a host but is not enough to identify the process (or activity within a process – a thread) (among many that are running) that will receive (or is sending) data

A **port number** is a number [1 – 65535] that is used in TCP and UDP – two transport layer (L4) protocols

Port numbers (together with IP addresses) are used to uniquely identify a communication between two endpoints

Port numbers 1-1024 are called «**well-known port numbers**»

- We should avoid using these for other purposes
- Examples:
  - 80 – HTTP (TCP)
  - 443 – HTTPS (TCP and UDP)
  - 20, 21 – FTP (TCP)
  - 22 – SSH
  - 32 – Telnet (TCP and UDP)
  - 53 – DNS (TCP and UDP)
  - 67, 68 – DHCP

Routers and routing tables

Primary function of router: forward packets to destination (using most suitable path – best route)

- Routing table contains routes “known” to router

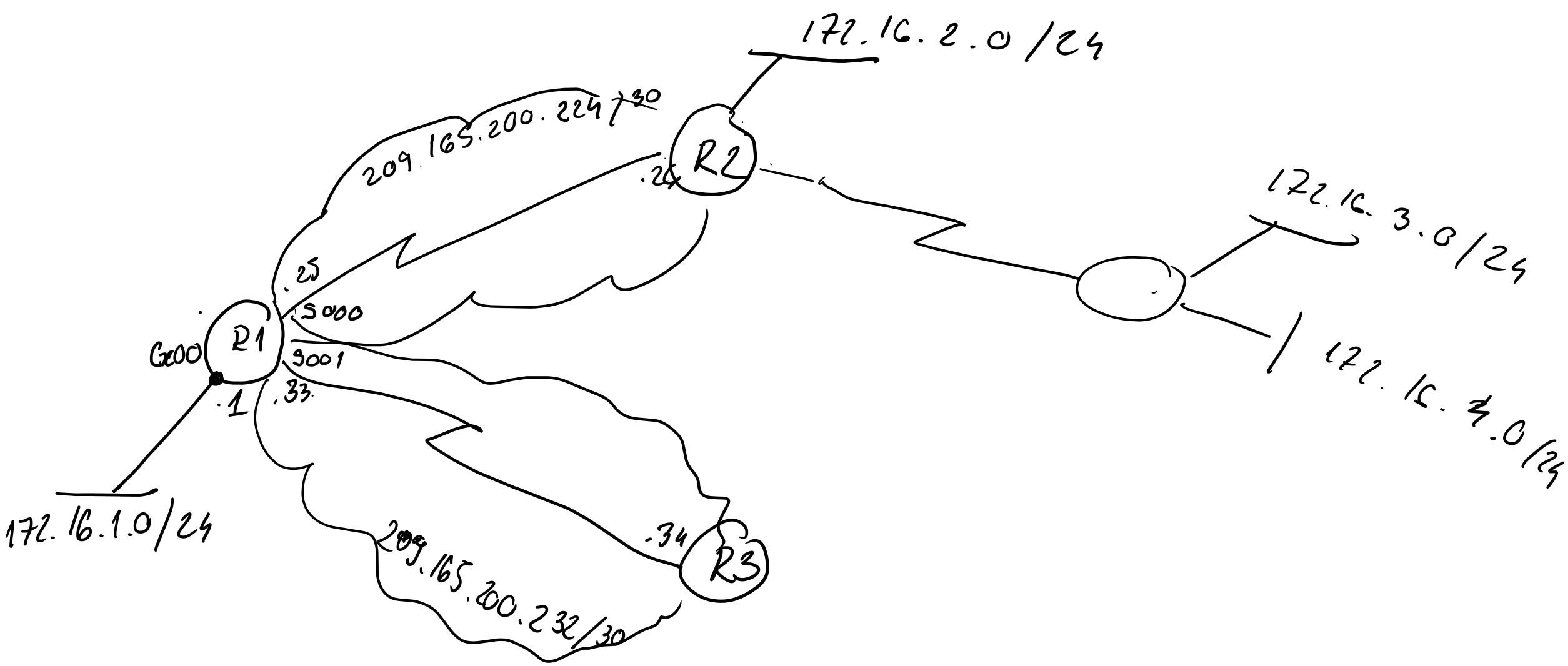
Routes may be configured statically (by administrator) and/or a routing protocol(s) may be used in order to dynamically learn/update routes

Each router interface is usually in different network (its IP address)

```
R1# show ip route | begin Gateway
Gateway of last resort is 209.165.200.234 to network 0.0.0.0

S*  0.0.0.0/0 [1/0] via 209.165.200.234, Serial0/0/1
                    is directly connected, Serial0/0/1
      172.16.0.0/16 is variably subnetted, 5 subnets, 3 masks
C     172.16.1.0/24 is directly connected, GigabitEthernet0/0
L     172.16.1.1/32 is directly connected, GigabitEthernet0/0
R     172.16.2.0/24 [120/1] via 209.165.200.226, 00:00:12, Serial0/0/0
R     172.16.3.0/24 [120/2] via 209.165.200.226, 00:00:12, Serial0/0/0
R     172.16.4.0/28 [120/2] via 209.165.200.226, 00:00:12, Serial0/0/0
R     192.168.0.0/16 [120/2] via 209.165.200.226, 00:00:03, Serial0/0/0
      209.165.200.0/24 is variably subnetted, 5 subnets, 2 masks
C     209.165.200.224/30 is directly connected, Serial0/0/0
L     209.165.200.225/32 is directly connected, Serial0/0/0
R     209.165.200.228/30 [120/1] via 209.165.200.226, 00:00:12, Serial0/0/0
C     209.165.200.232/30 is directly connected, Serial0/0/1
L     209.165.200.233/30 is directly connected, Serial0/0/1
R1#
```

Router may have “default route” configured


172.16.2.0/24
209.165.200.224/30
.26
R2
.25
S000
G000
R1
S001
.1
.33
172.16.3.0/24
172.16.4.0/24
172.16.1.0/24
.34
R3
209.165.200.232/30

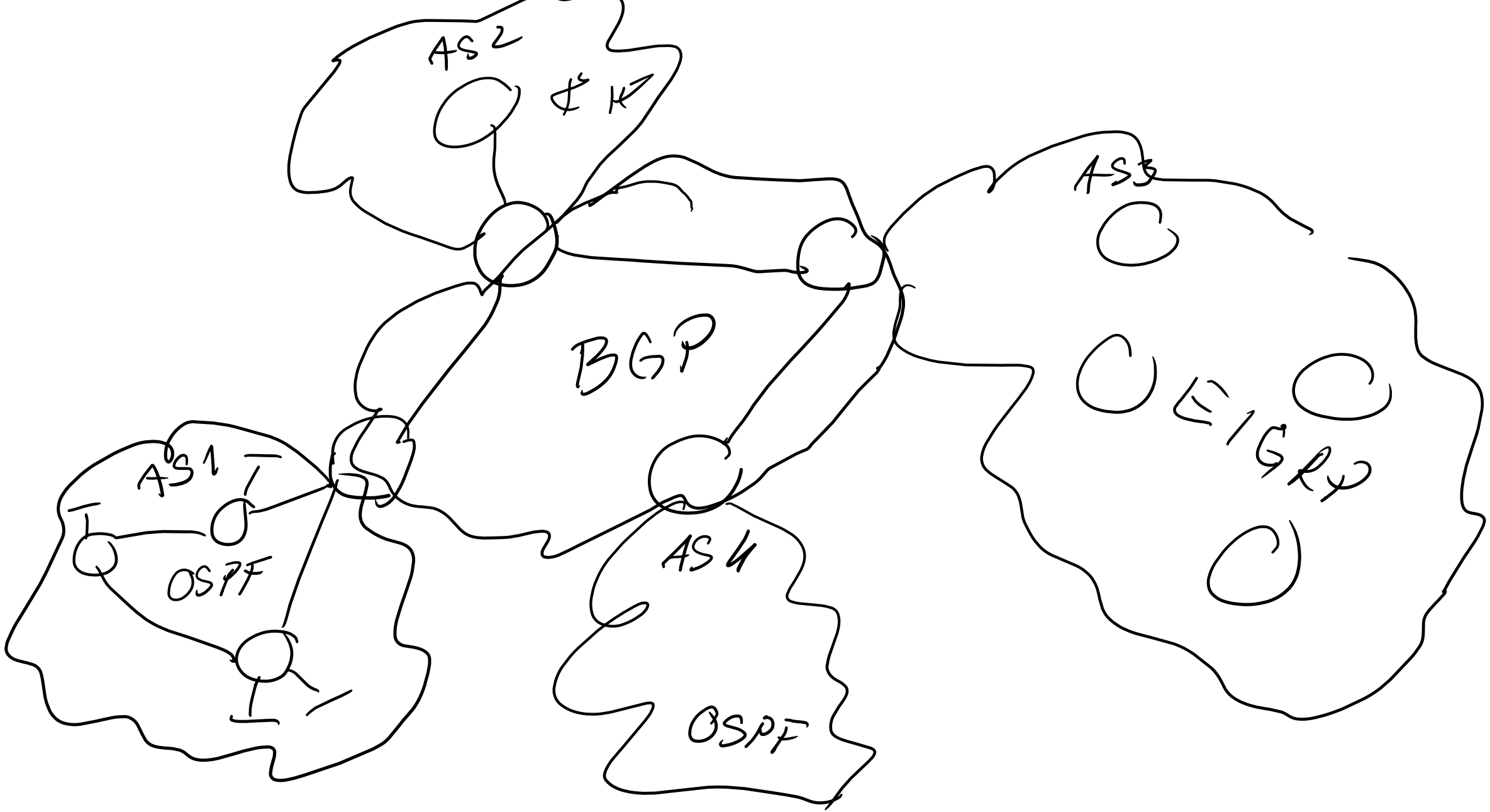
Routing protocols

Routing protocols: programs, run on routers that (dynamically) exchange routing information between routers and suggest best routes for routing table

- Examples: Open Shortest Path First (OSPF), Enhanced Interior Gateway Routing Protocol (EIGRP), Routing Information Protocol (RIP), Border Gateway Protocol (BGP)
- Metric: how "good" a route is – best route is suggested to routing table
  - OSPF: metric related to bandwidth
  - EIGRP: related to bandwidth, load, reliability, delay and MTU
  - RIP: hop count
  - BGP: complex decision process ☺ ("best path" is used instead of "metric")
- **Administrative distance** – preferred ordering with respect to the source of information
  - RIP – 120, OSPF 110, … , Static 1, Connected 0

Within an autonomous system (IGP): OSPF, EIGRP, RIP

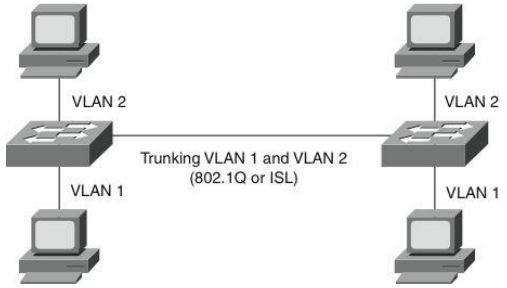
Between different autonomous systems (EGP): BGP

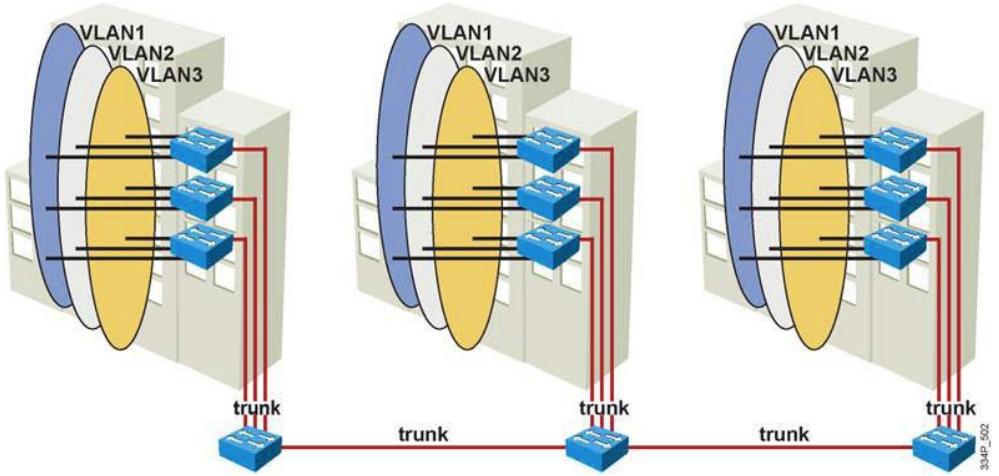

AS2
BGP
AS3
EIGRP
AS1
OSPF
AS4
OSPF

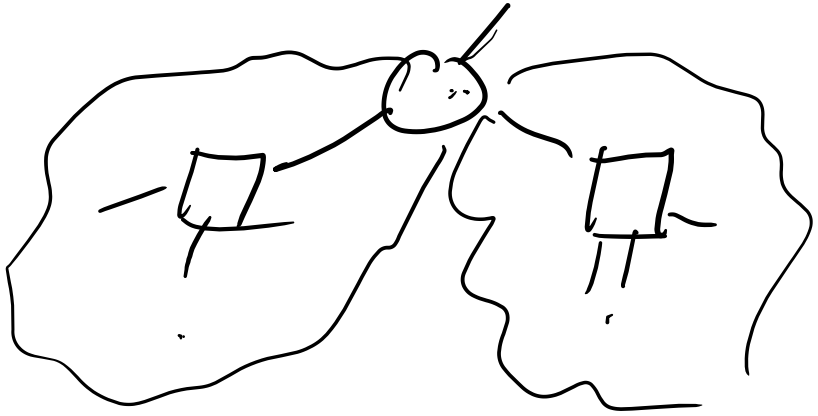
Segmentation of interconnected network: VLAN-s

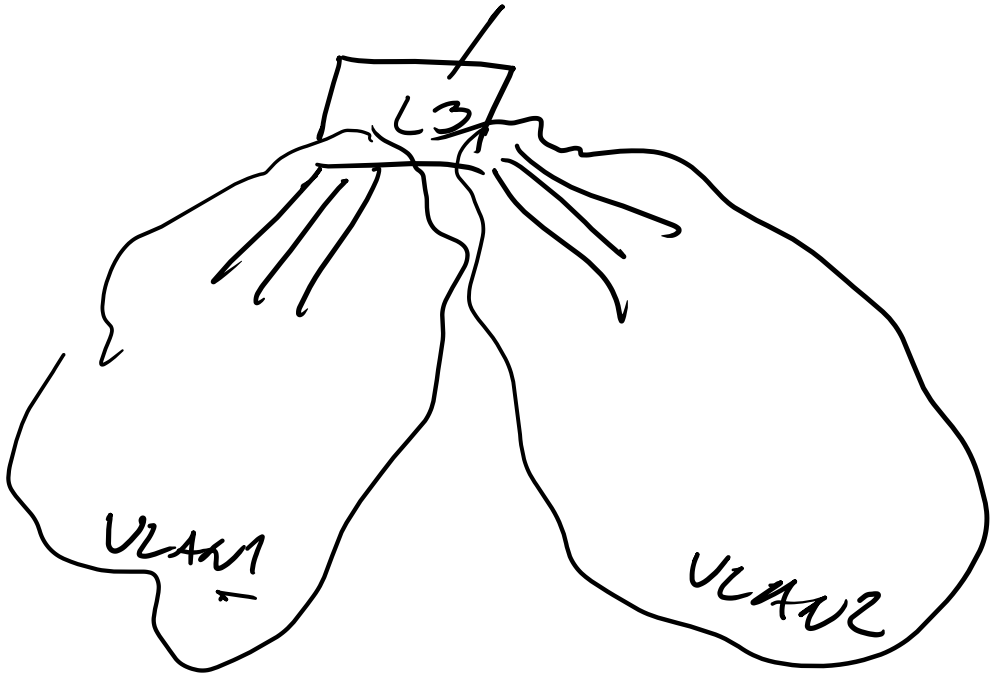
Given a network of devices - VLAN is a (logically defined) subgroup isolate subgroup-traffic (L2) from the rest of network.

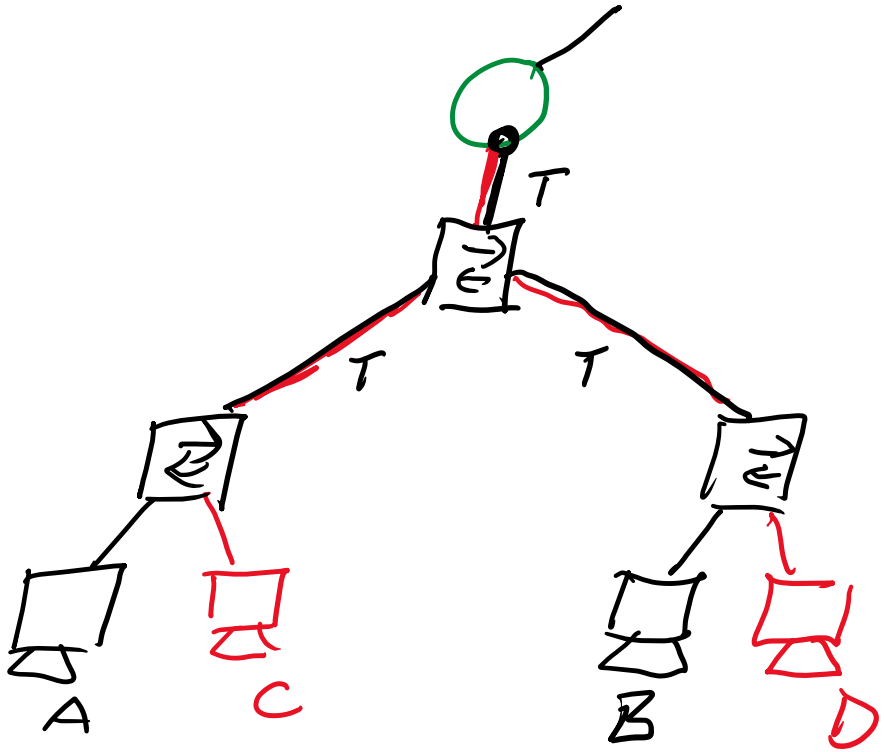
We may have different L2-network connected to same switch (or group of interconnected switches)





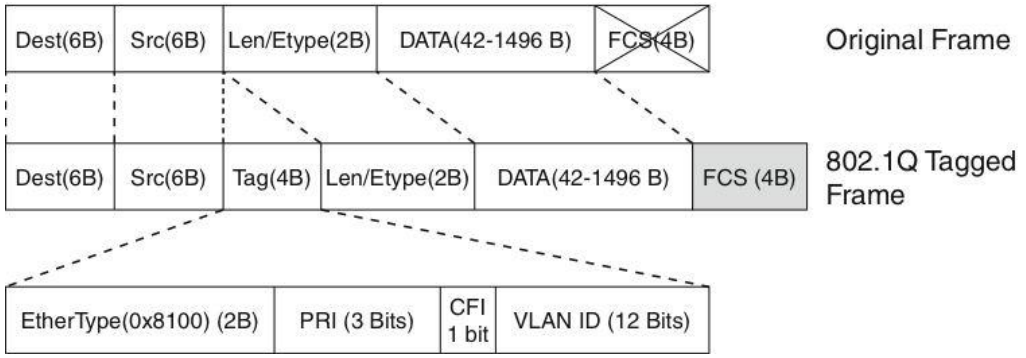



L3
VLAN1
VLAN2


T
T
T
A
C
B
D

```
Switch# show vlan brief

VLAN Name                Status    Ports
---- ------------------- --------- -------------------------------
1    default             active    Fa0/1,  Fa0/2,  Fa0/3,  Fa0/4
                                   Fa0/5,  Fa0/6,  Fa0/7,  Fa0/8
                                   Fa0/9,  Fa0/10, Fa0/11, Fa0/12
                                   Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                   Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                   Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                   Gi0/1, Gi0/2
1002 fddi-default        act/unsup
1003 token-ring-default  act/unsup
1004 fddinet-default     act/unsup
1005 trnet-default       act/unsup
```



Switch# **configure terminal**
Switch(config)# **vlan 200**
Switch(config-vlan)# **name HVL**
Switch(config-vlan)# **exit**

Switch(config)# **interface FastEthernet 0/6**
Switch(config-if)# **description ADMIN**
Switch(config-if)# **switchport host**
Switch(config-if)# **switchport access vlan 200**
Switch(config-if)# **no shutdown**
Switch(config-if)# **end**

Connecting VLANs

Router may be used

- Router on a stick
- Several interfaces on router may be used – but this does not scale well

L3 switch may be used (with SVI)

```
Switch(config)# interface vlan 10
Switch(config-if)# ip address 10.10.1.1 255.0.0.0
Switch(config-if)# no shutdown
Switch(config-if)# interface vlan 20
Switch(config-if)# ip address 10.20.1.1 255.255.255.0
Switch(config-if)# no shutdown
```

Some switch related technologies

Spanning Tree Protocol (STP): L2 protocol that ensures that we do not have loops in network that have redundant paths

- Prevents loops (broadcast storms, …)
- Some ports are placed in “blocking mode” (but status may change if necessary). No user data is sent/received on such port
- Graph → Tree
- Per-VLAN Rapid Spanning Tree (PVRST+)
  - Cisco-proprietary

VLAN Trunk Protocol (VTP): L2 protocol that automatically spread information about VLANS to remote switches

- Simplifies switch administration
- Cisco-proprietary

Transport layer: Transmission Control Protocol (TCP)

Transport Layer Protocol (TCP)

- Addressing (ports) – in order to identify higher layer activities
  - Many different application may use TCP – we need to keep data apart
- Establishment, management & termination of connection
- Data handling and packaging (segmentation, packing of segments into TCP messages with TCP header)
- Passing data to L3 protocol (IP)
- Provides for reliability and transmission (ACK of data transferred)
- Flow control and congestion avoidance – how much data may be sent without receiving ACK?

Transport layer: User Datagram Protocol (UDP)

- Addressing (ports) – in order to identify higher layer activities
  - Many different application may use TCP – we need to keep data apart
- Data handling and packaging (segmentation, packing of segments into UDP messages with UDP header)
- Passing data to L3 protocol (IP)

Note:

- booth UDP and TCP use port numbers, but they are different protocols. Same port number MAY be used at the same time by TCP and UDP simultaneously ☺

IPv6

Introduced in 1995

Some benefits:

- **Larger address space (2^128 addresses)**
- Eliminates need for NAT – and eliminates problems connected to use of NAT
- Simpler header format
- Uses extension headers if needed
  - Examples: Authentication header (AH) and Encapsulating Security Payload (ESP)
- Improved support for QoS and mobile devices

IPv6 addresses

128-bit address

Address is written using hexadecimal numbers:

- "Coloned hex format": eight 16-bit segments separated with colons between each set of four hex digits (16 bits)
- The format is `x:x:x:x:x:x:x:x`, where `x` is a 16-bit hexadecimal field (four hexadecimal digits)

Example: **`2035:0001:2BC5:0000:0000:087C:0000:000A`**

First 64 bits: Subnet prefix (network identifier: 48 + 16 bits)

Last 64 bits: Interface ID (host identifier: 64 bits)

Multiple addresses may be used:

- Link local
- Global

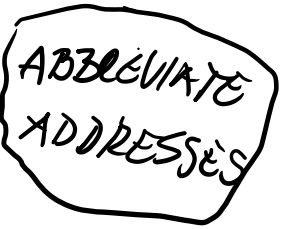
IPV6 abbreviations

Leading 0s within each set of four hexadecimal digits can be omitted

- **03AB = 3AB**
- **0001 = 1**
- **0000 = 0**

A pair of colons (“**::**”) can be used (only *once)* within an address, to represent any number of successive **0**s (as many as we are missing (not including 0-s from previous point).

FF09:0000:0000:A111:03A1:0021:0001:0011



FF09:0000:0000:0000:0000:0000:0000:0001

Special IPv6 addresses

::/0	All routes - default static route.
::/128	Unspecified address (initially assigned to a host)
::1/128	Loopback address
FE80::/10	Link-local unicast address.
FF00::/8	Multicast addresses.
Other addresses	Global unicast address.

Use of addresses:

- Unicast
- Multicast
  - FF00::/8 – an interface may
- Anycast