NETWORKS

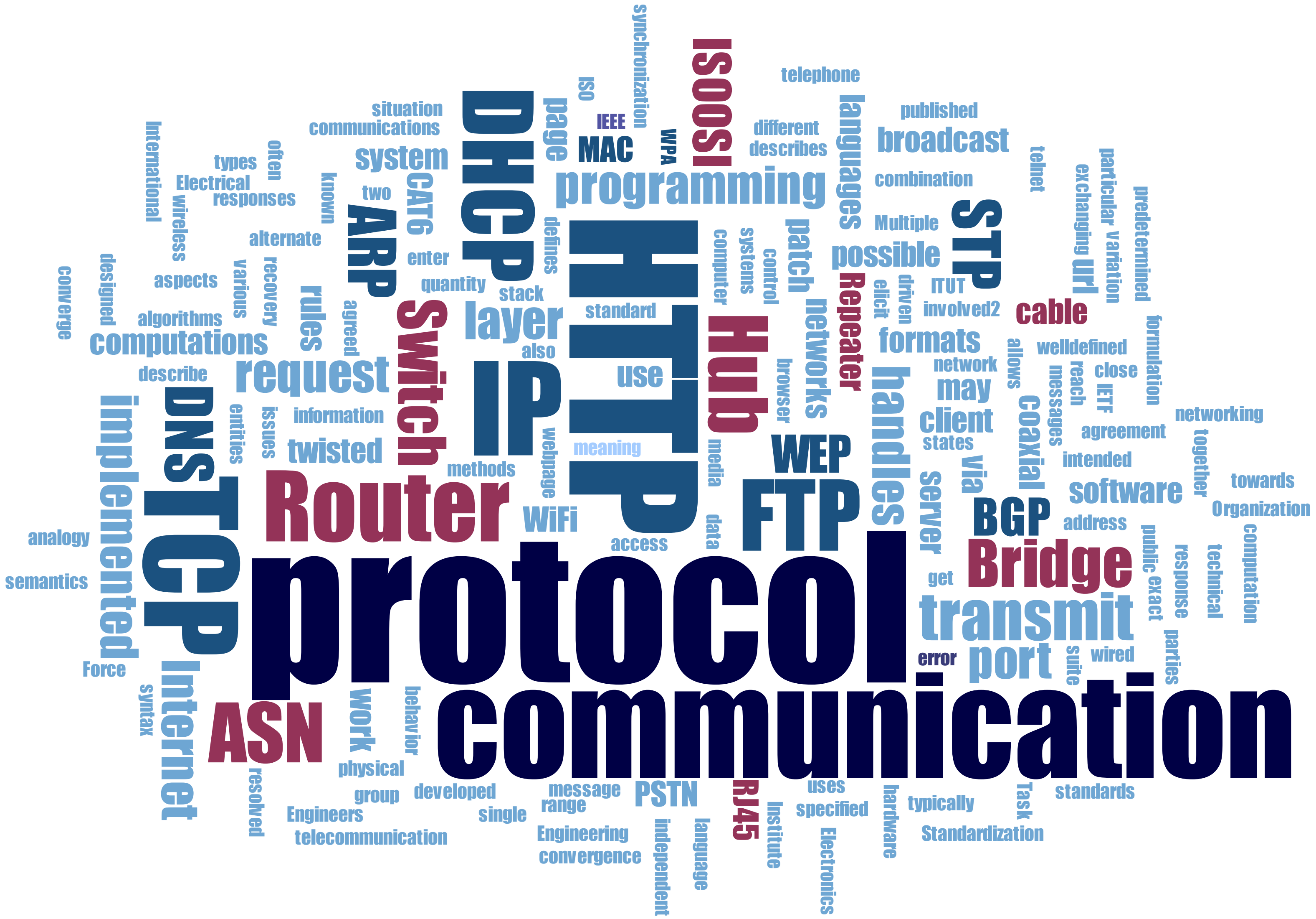
PROTOCOL & COMMUNICATION BASICS

Communication in Computer Networks
Jens Gaulke for SUSE Cloud Native Scholarship
#st_spaic
07/30/21

AGENDA

GEM MINE

AGENDA


protocol
communication
HTTP
TCP
Router
IP
DHCP
Switch
Hub
FTP
Bridge
transmit
ASN
implemented
Internet
DNS
ARP
ISOOSI
programming
request
layer
handles
WEP
BGP
STP
Repeater
port
cable
MAC
WiFi
PSTN
RJ45
IEEE
WPA
CAT6
computations
twisted
rules
languages
broadcast
possible
formats
client
may
software
coaxial
server
networks
patch
page
system
use
work
synchronization
telephone
published
different
describes
combination
Multiple
ITUT
involved2
welldefined
network
close
networking
agreement
intended
towards
Organization
address
get
error
wired
suite
parties
standards
Standardization
typically
specified
uses
hardware
Task
Electronics
Institute
language
independent
convergence
Engineering
range
message
single
developed
telecommunication
Engineers
group
physical
resolved
syntax
Force
semantics
analogy
converge
designed
algorithms
aspects
describe
information
entities
issues
methods
webpage
meaning
access
data
media
browser
standard
stack
quantity
enter
alternate
various
recovery
agreed
also
defines
computer
systems
control
elicit
driven
url
exchanging
particular
variation
predetermined
formulation
allows
messages
reach
IETF
together
states
via
public
exact
response
technical
computation
telnet
situation
communications
types
often
Electrical
responses
known
two
International
wireless
iso

AGENDA

GEM MINE

ISO OSI

REFERENCE MODEL
RELEVANT LAYER
ENCAPSULATION /
DECAPSULATION

LAYER 1

REPEATER / HUB
CROSSOVER CABLE
COLLISION DOMAIN

LAYER 2

BRIDGE/ SWITCH
IP, ARP & MAC
MAC: CSMA/CD
STP

LAYER 3

ROUTER
IP & SUBNETTING
OSPF, BGP, IBGP, EBGP
NAT

LAYER 4

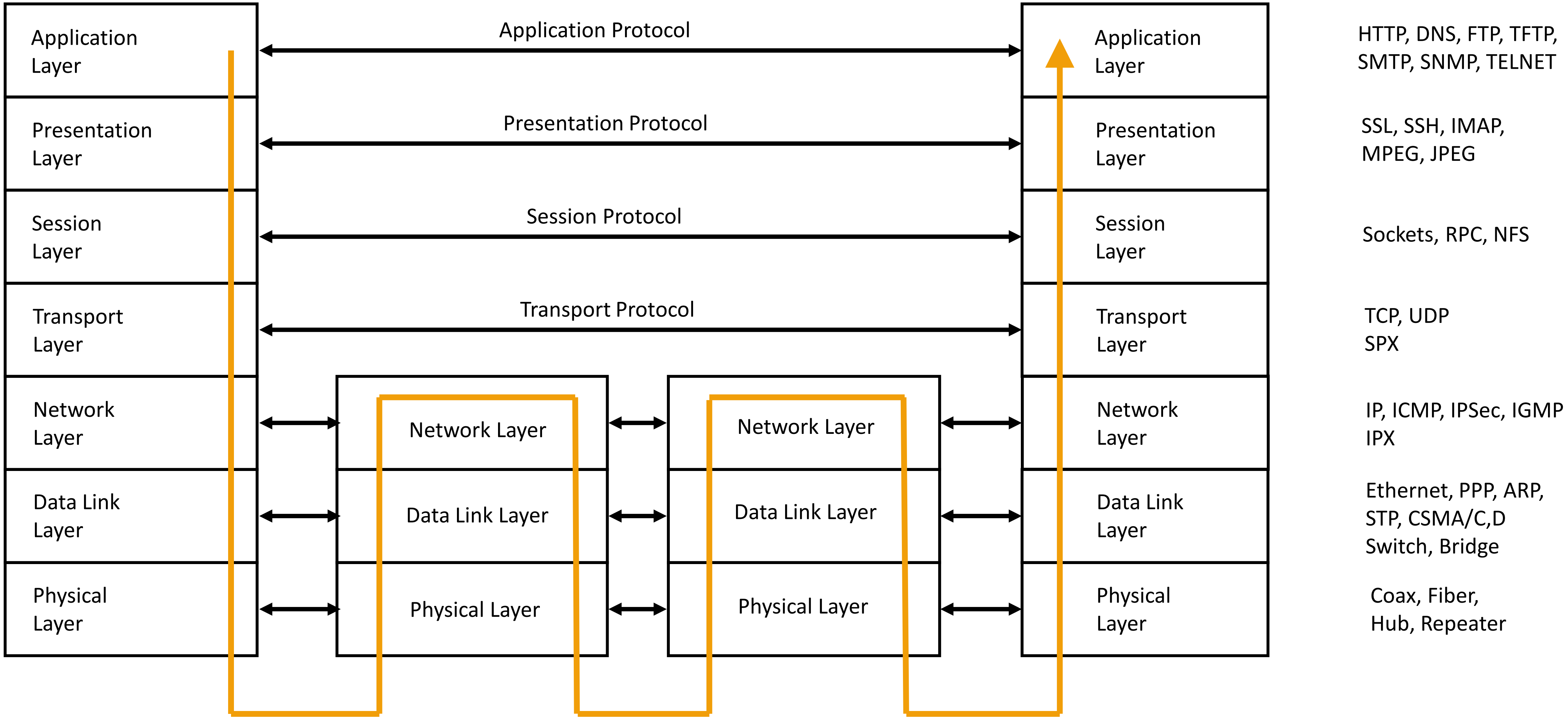
TCP
SLIDING WINDOW
PORTS
PAT

USEFUL PROTOCOLS

DHCP
DNS

ISO OSI LAYERS

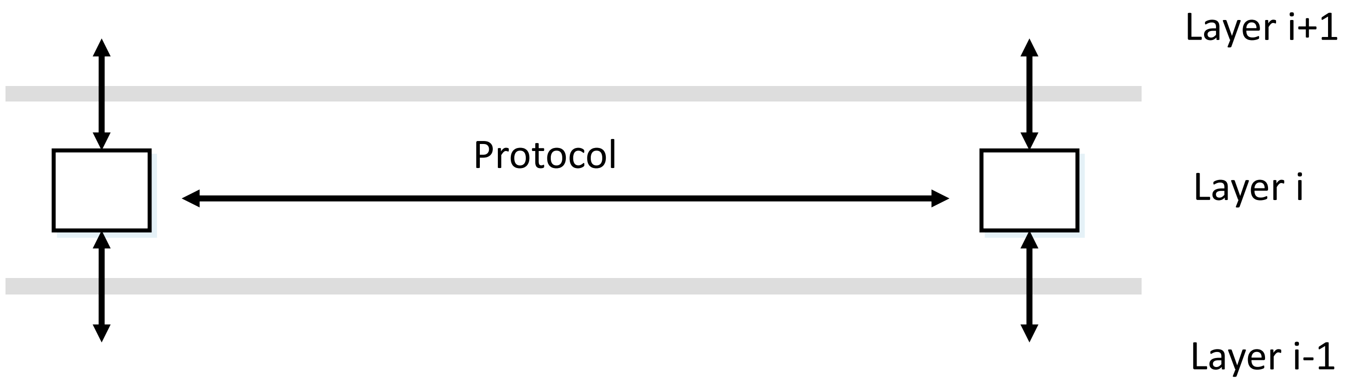
GEM MINE



ISO OSI LAYERS

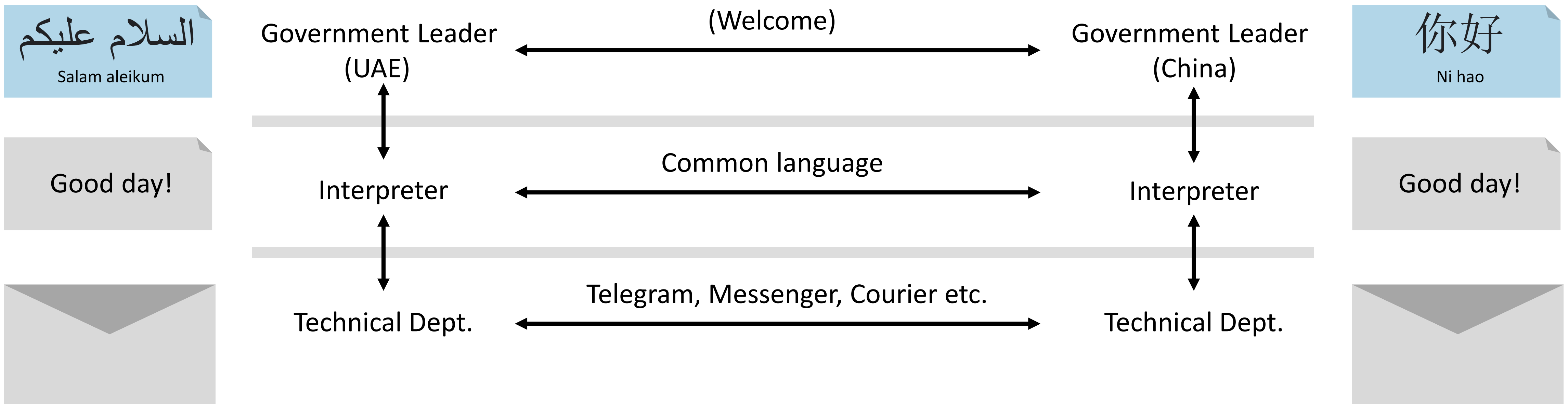
COMMUNICATION RULES

- Communication only takes place between peers on the same level

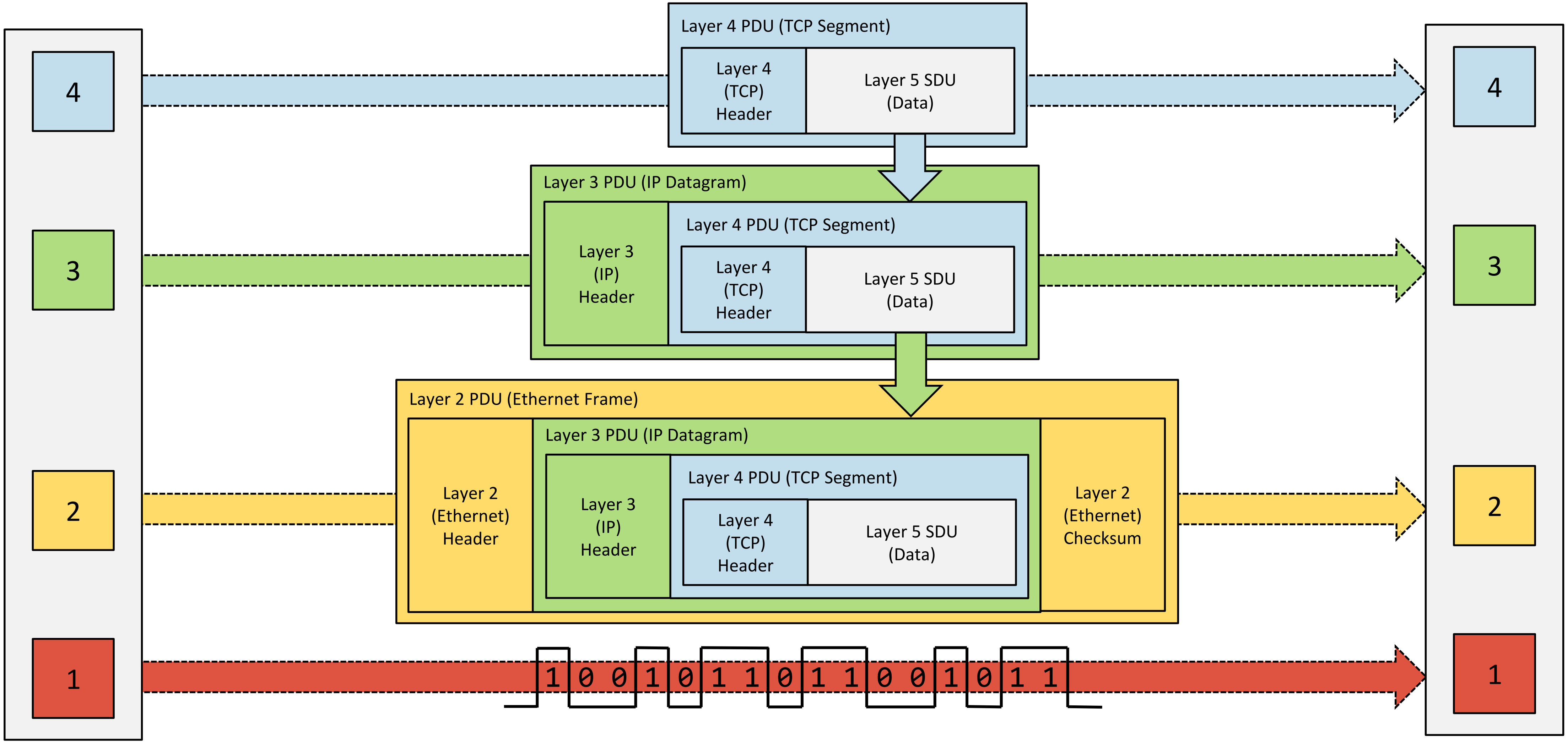


ISO OSI LAYERS

COMMUNICATION RULES



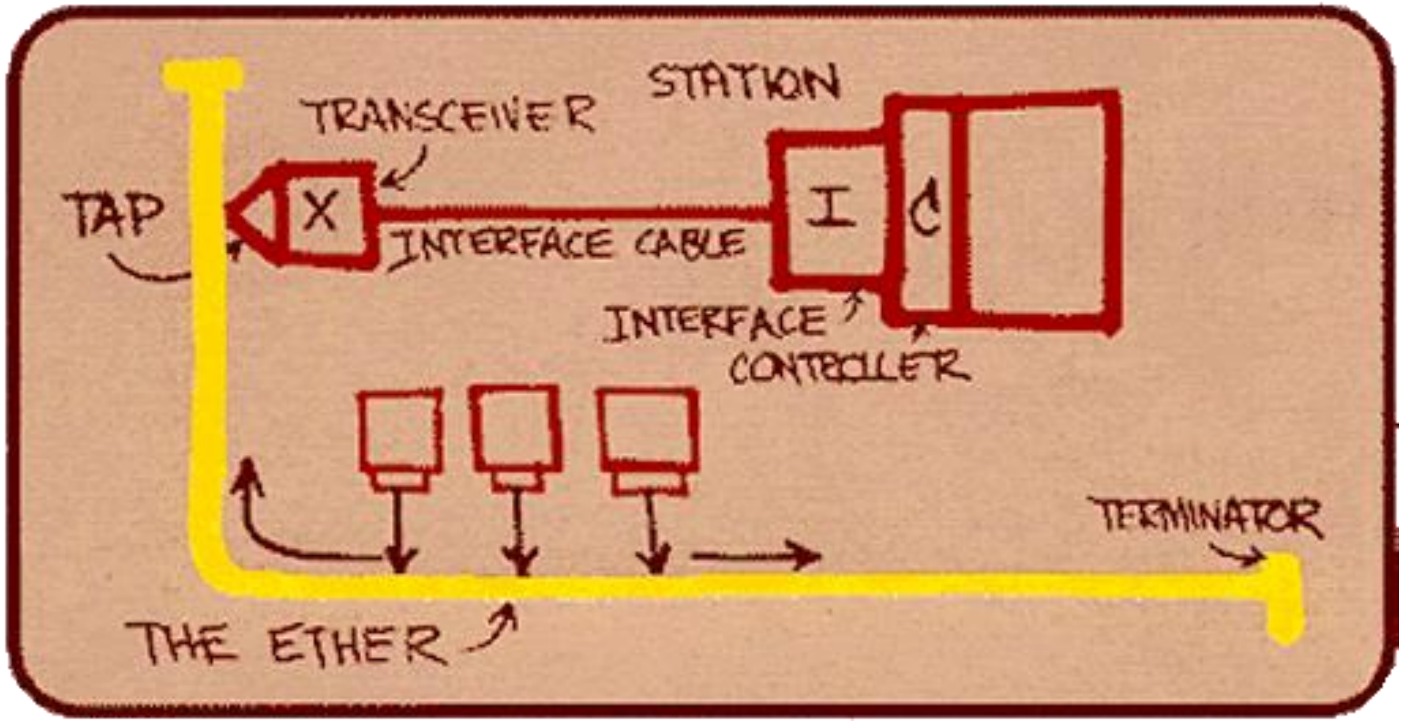
ISO OSI LAYERS



ISO OSI LAYERS

LAYER 1

Robert Metcalfe

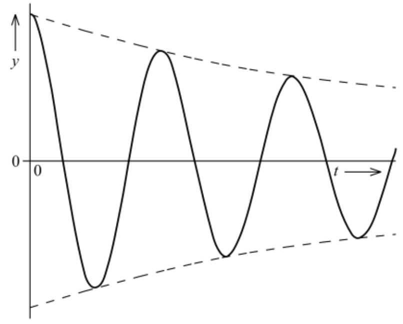


http://scihi.org/robert-metcalfe-ethernet/

ISO OSI LAYERS

GEM MINE

LAYER 1



- ***Signal damping***
  On cables, the effect of attenuation occurs at greater distance.
  The signal becomes weaker

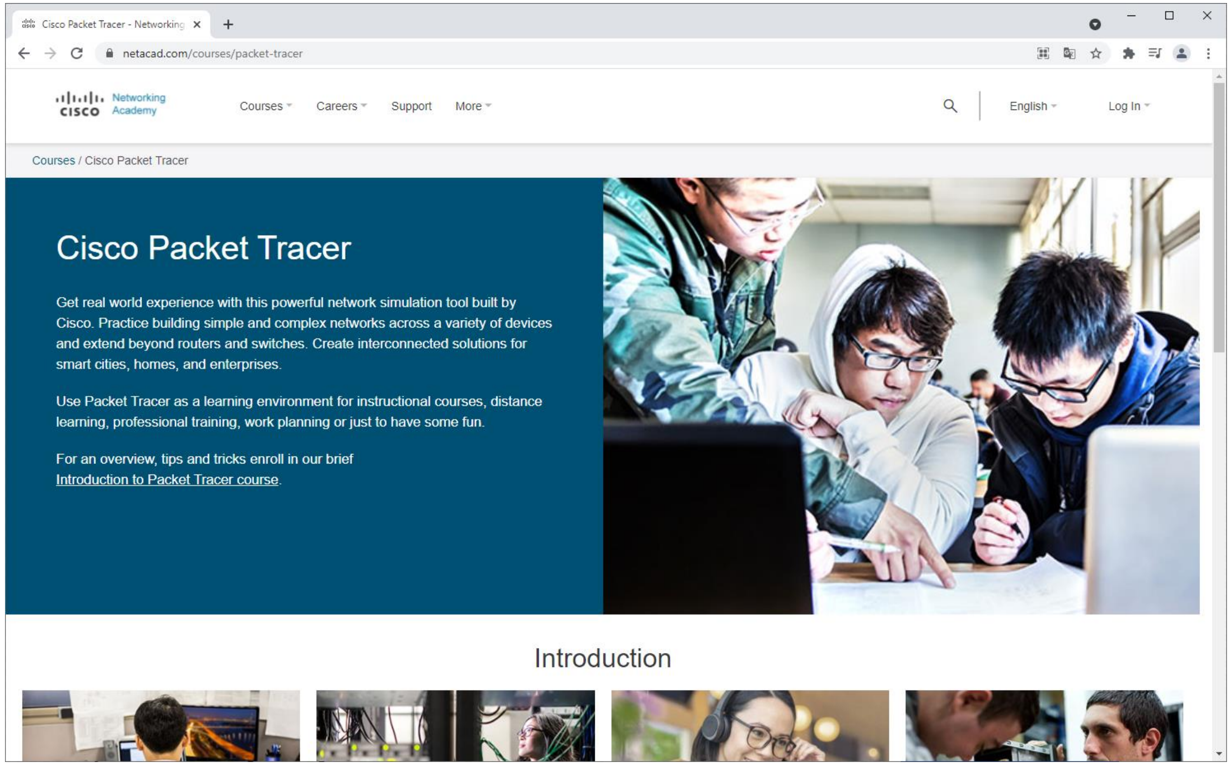
- ***Repeater***
  To increase the range, the signal must be amplified

- ***Hub***
  If a repeater has more than two ports, it is called a hub, due to the structure that results in the network – Hub and Spoke

ISO OSI LAYERS

LAYER 1

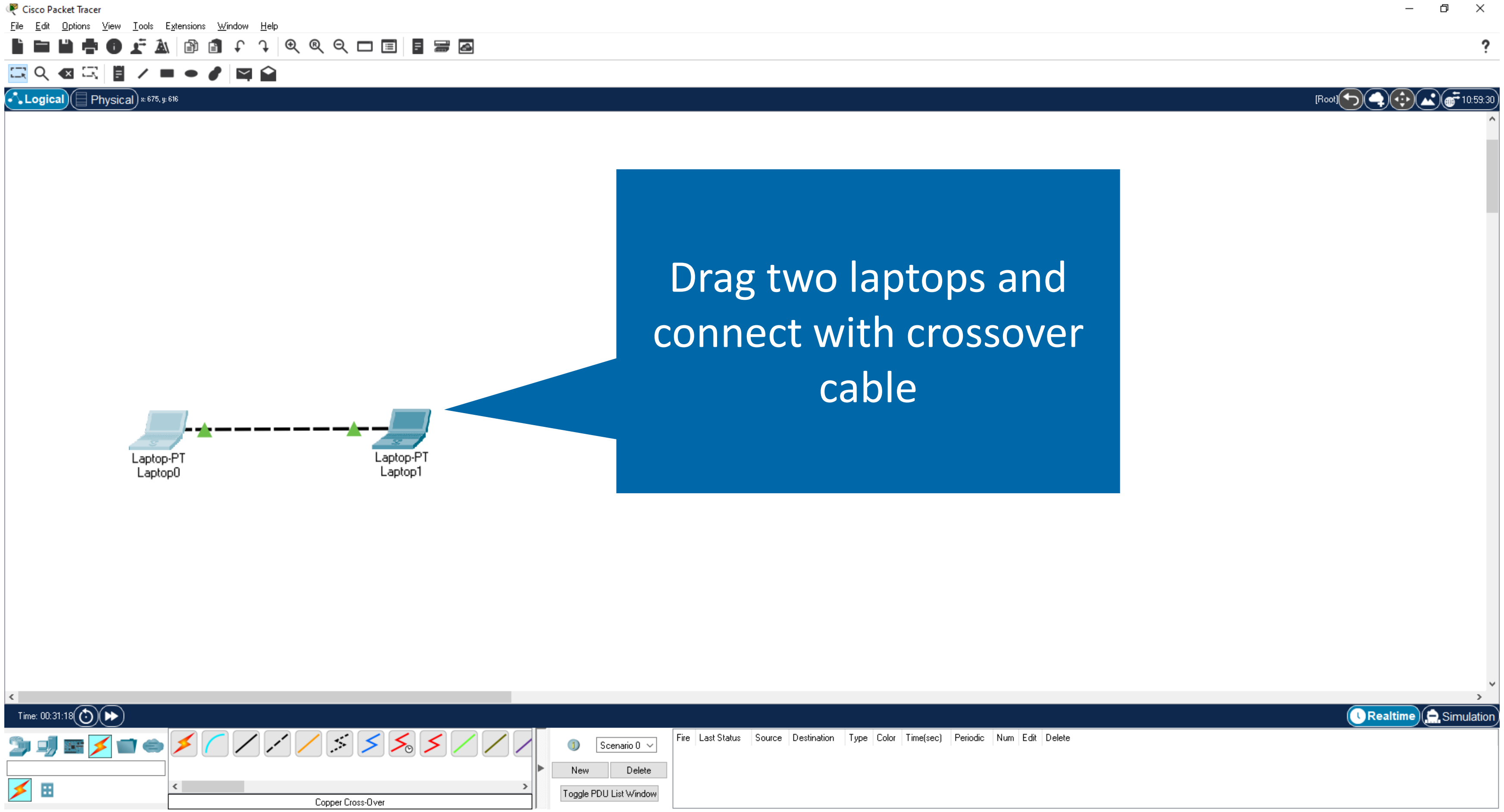
- Demo: Cisco Packet Tracer
- Enroll for free and download at https://www.netacad.com/courses/packet-tracer
- Build networks by drag and drop
- Simulate packet traces
- Easily understand what's going on in the net



ISO OSI LAYERS

GEM MINE

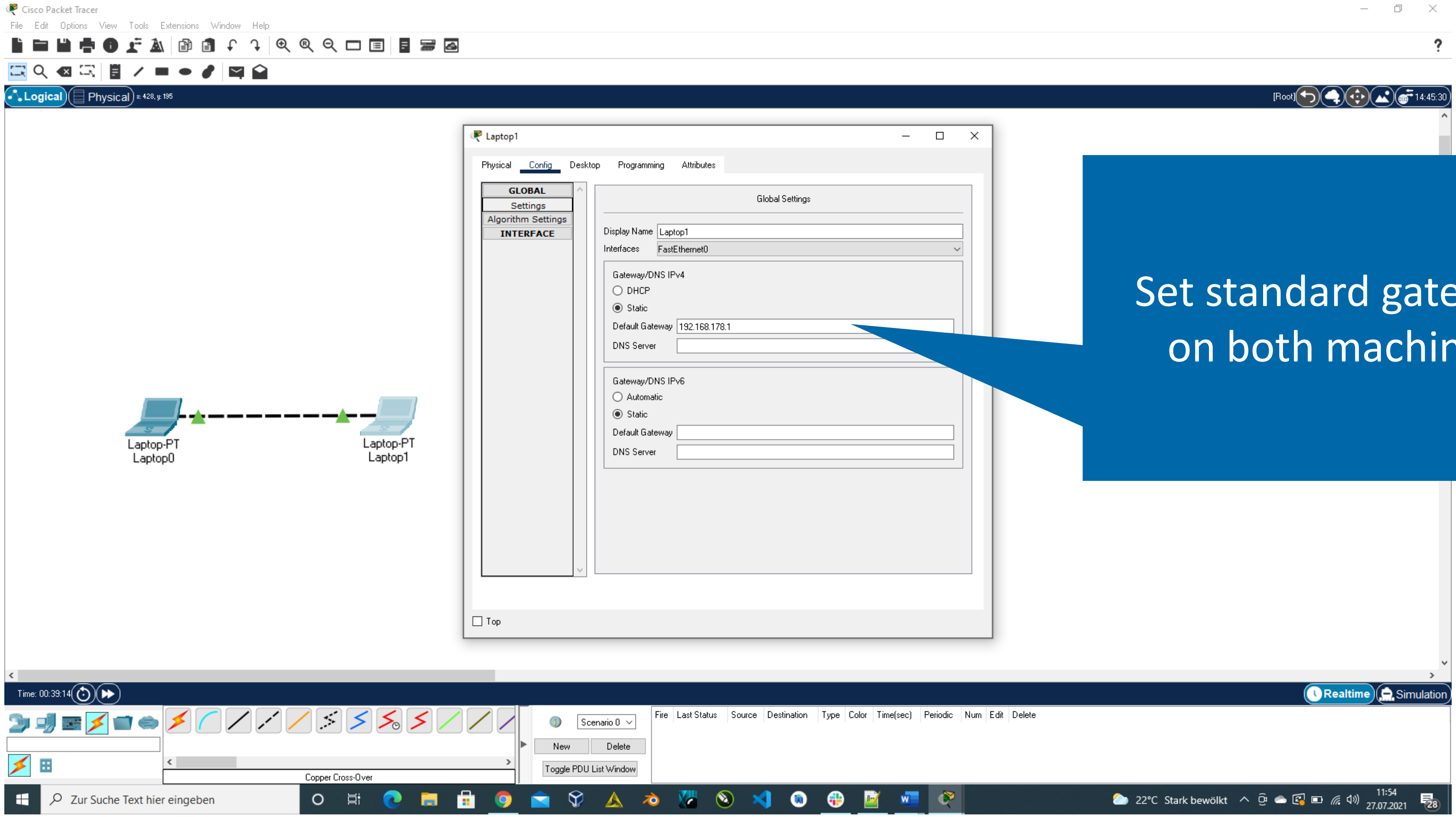
LAYER 1



ISO OSI LAYERS

GEM MINE

LAYER 1

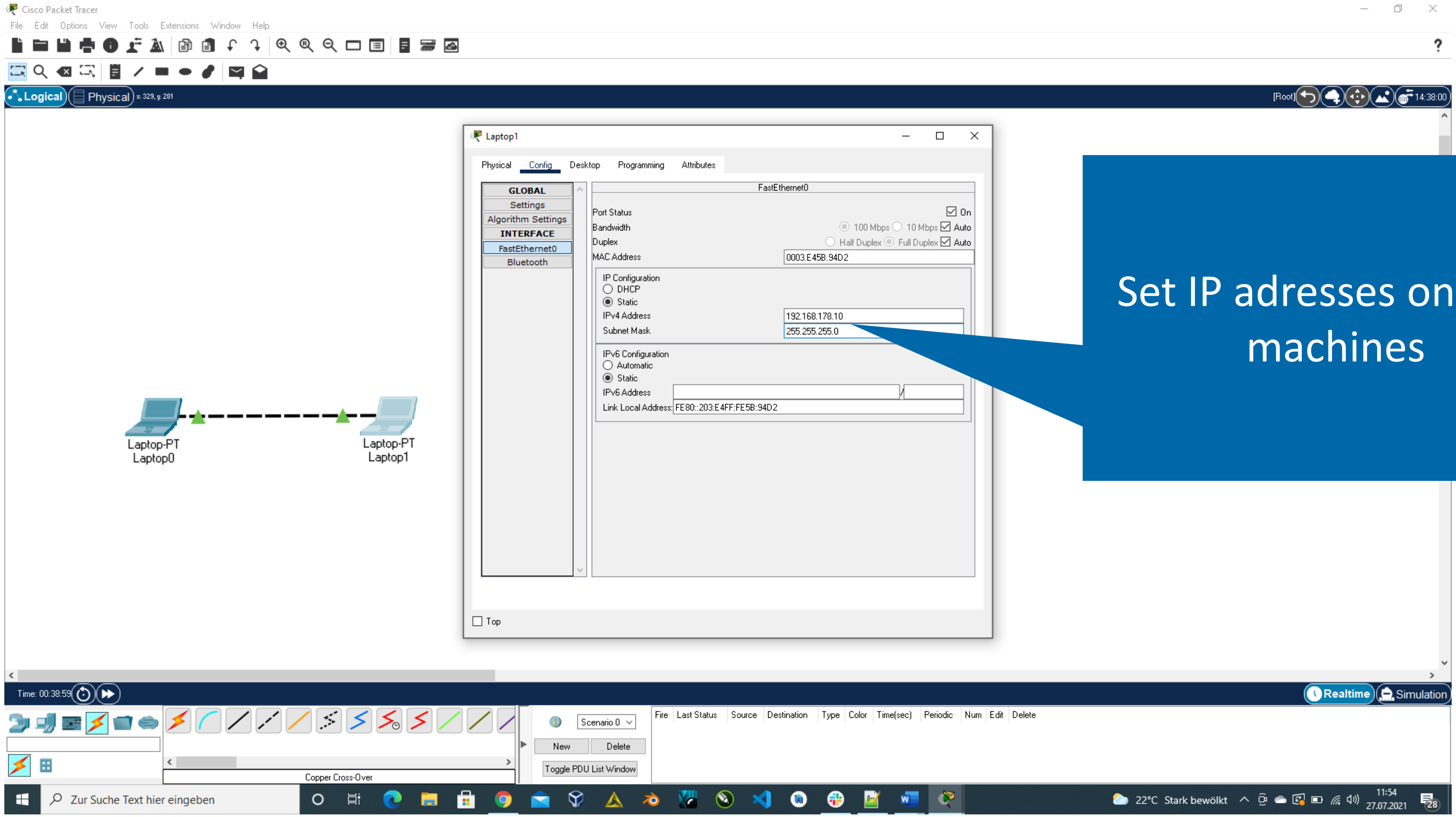


Set standard gateway on both machines

ISO OSI LAYERS

GEM MINE

LAYER 1

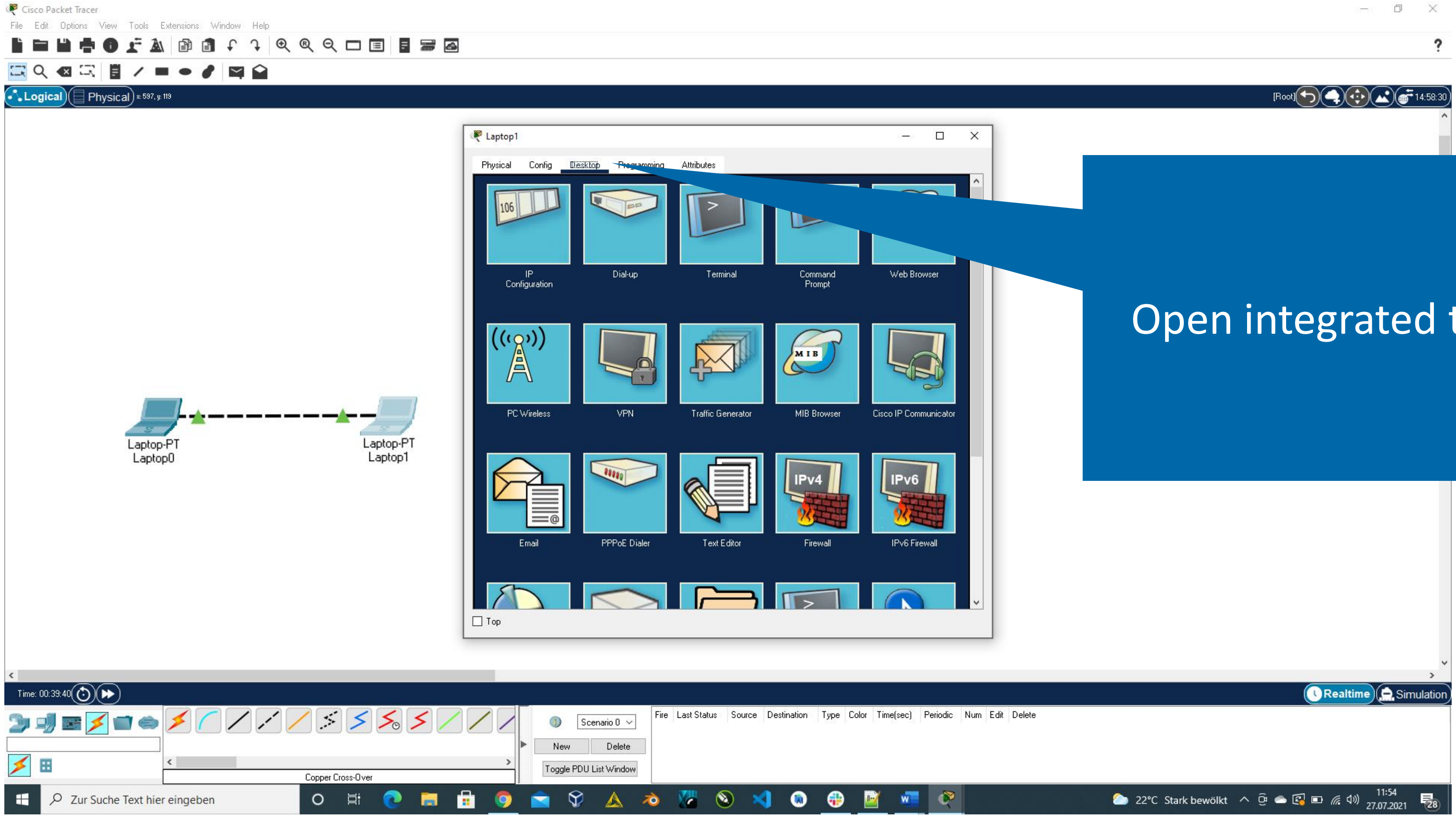


Set IP adresses on both machines

ISO OSI LAYERS

GEM MINE

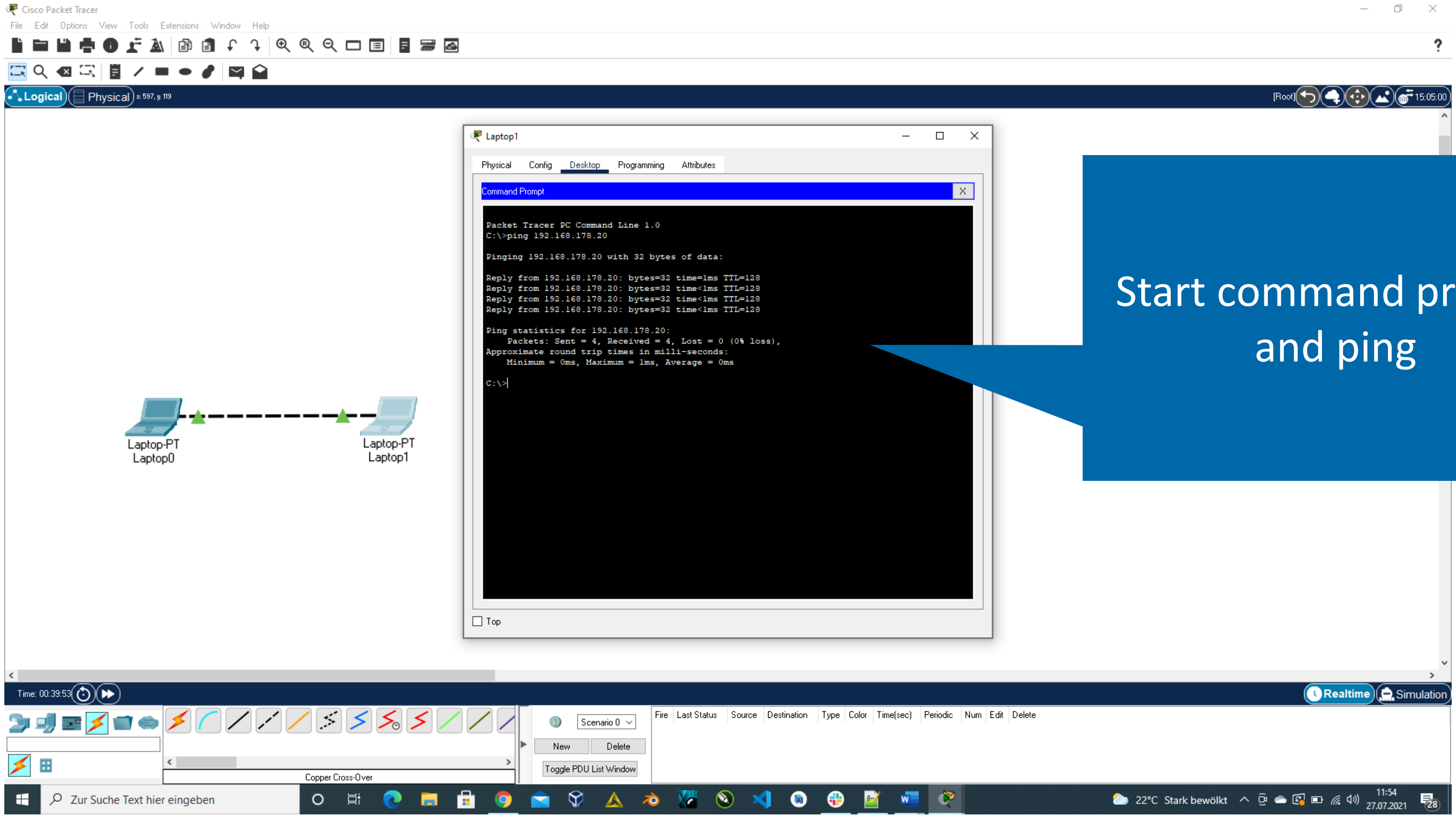
LAYER 1



Open integrated tools

GEM MINE

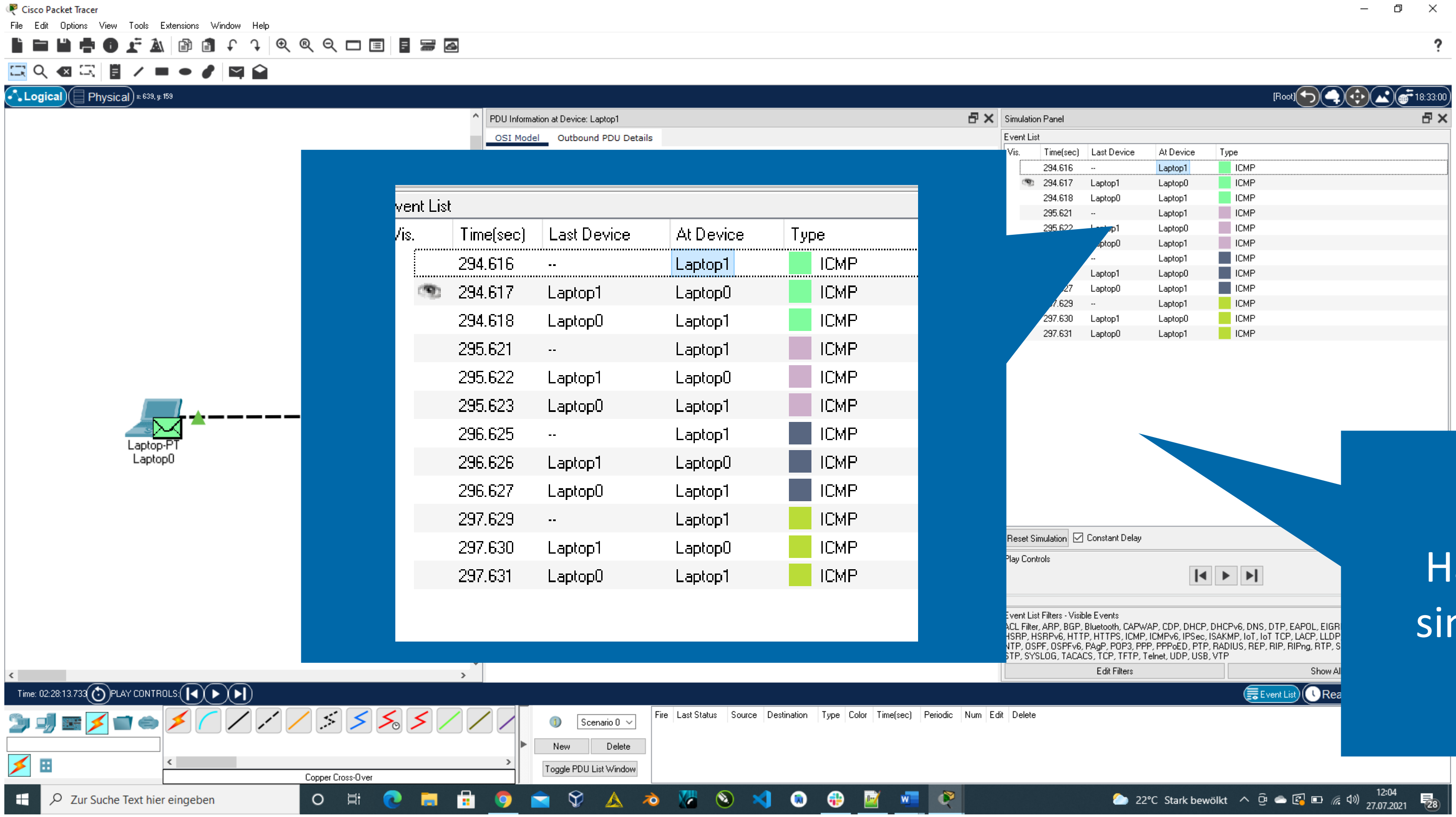
LAYER 1



Start command prompt and ping

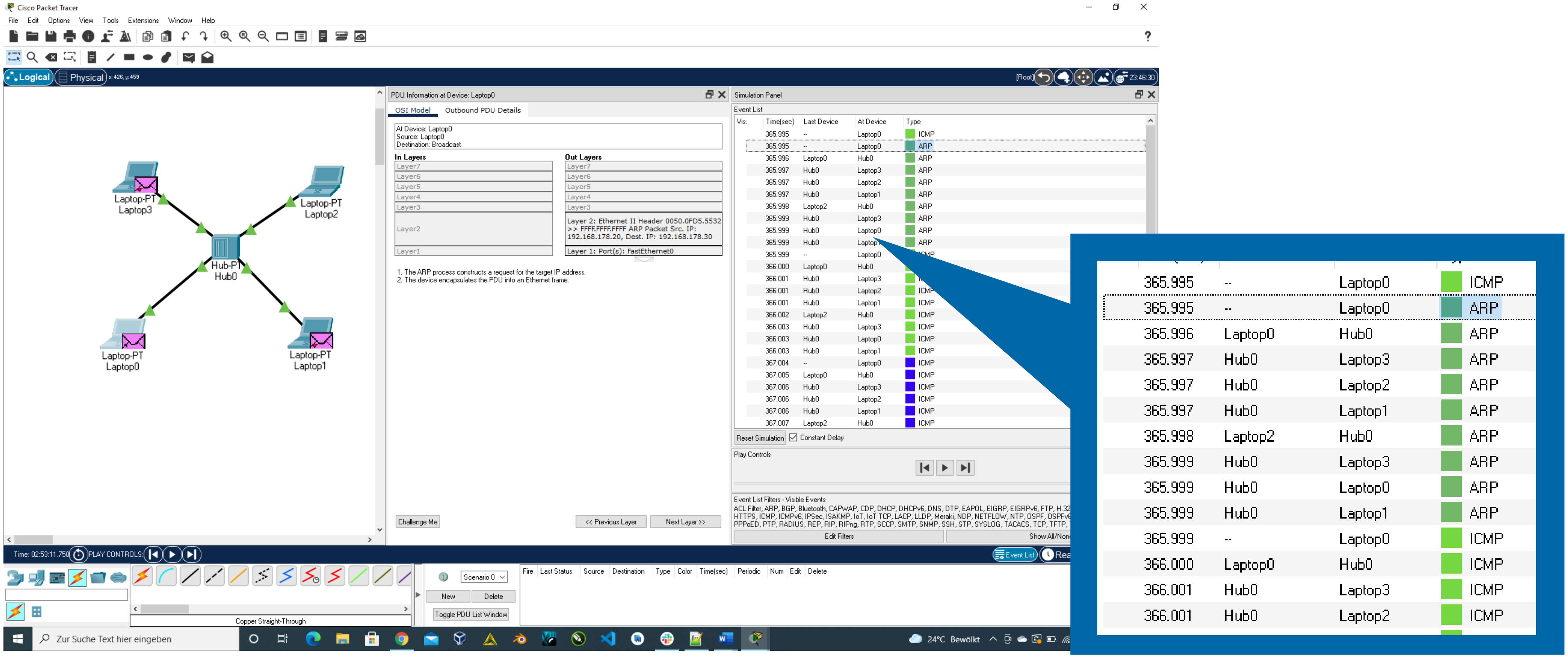
ISO OSI LAYERS

LAYER 1



Have a look at the simulation window

LAYER 1

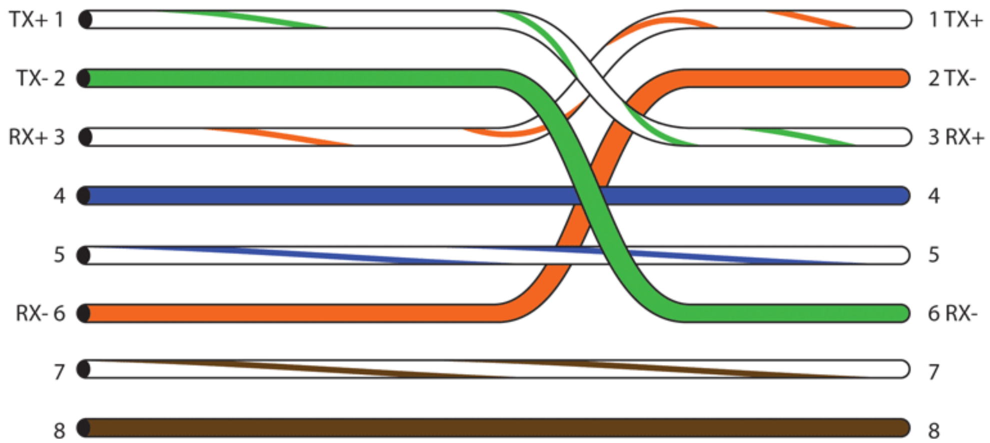


Cisco Packet Tracer
PDU Information at Device: Laptop0
OSI Model
Outbound PDU Details
At Device: Laptop0
Source: Laptop0
Destination: Broadcast
In Layers
Out Layers
Layer 2: Ethernet II Header 0050.0FD5.5532 >> FFFF.FFFF.FFFF ARP Packet Src. IP: 192.168.178.20, Dest. IP: 192.168.178.30
Layer 1: Port(s): FastEthernet0
1. The ARP process constructs a request for the target IP address.
2. The device encapsulates the PDU into an Ethernet frame.
Simulation Panel
Event List
365.995 -- Laptop0 ICMP
365.995 -- Laptop0 ARP
365.996 Laptop0 Hub0 ARP
365.997 Hub0 Laptop3 ARP
365.997 Hub0 Laptop2 ARP
365.997 Hub0 Laptop1 ARP
365.998 Laptop2 Hub0 ARP
365.999 Hub0 Laptop3 ARP
365.999 Hub0 Laptop0 ARP
365.999 Hub0 Laptop1 ARP
365.999 -- Laptop0 ICMP
366.000 Laptop0 Hub0 ICMP
366.001 Hub0 Laptop3 ICMP
366.001 Hub0 Laptop2 ICMP

ISO OSI LAYERS

LAYER 1 – OPEN QUESTIONS

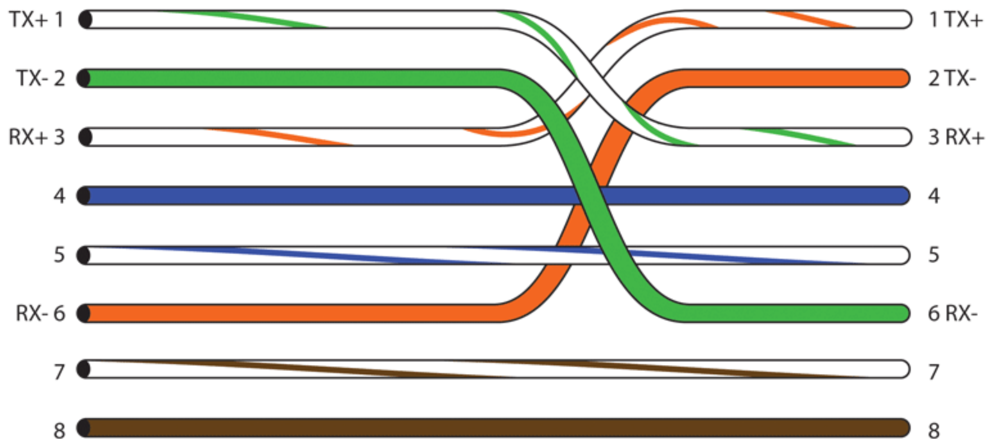
- What is a crossover cable?
- Why does a hub copy to all clients?
- What disadvantages does this create?
- What is ARP?
- What is ICMP?
- What is a Standard gateway?
- And what is it good for?



ISO OSI LAYERS

LAYER 1 – OPEN QUESTIONS

• What is a crossover cable?	
• Why does a hub copy to all clients?	
• What disadvantages does this create?	
• What is ARP?	Layer 2
• What is ICMP?	Layer 3
• What is a Standard gateway?	Layer 3
• And what is it good for?	Layer 3



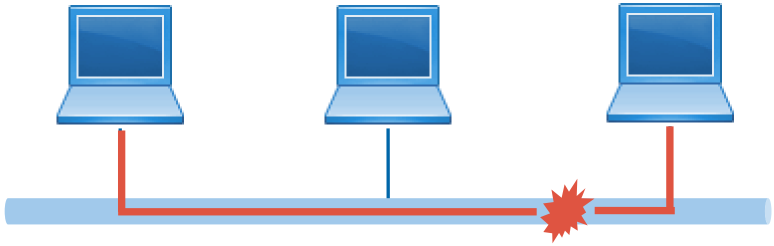
ISO OSI LAYERS

LAYER 2 – CSMA/CD

- Carrier Sense
  - Is anyone transmitting data?
  - Yes – do not transmit data
  - No – transmit data

- Multiple Access
  - Multiple devices are connected
  - Perfect for collisions

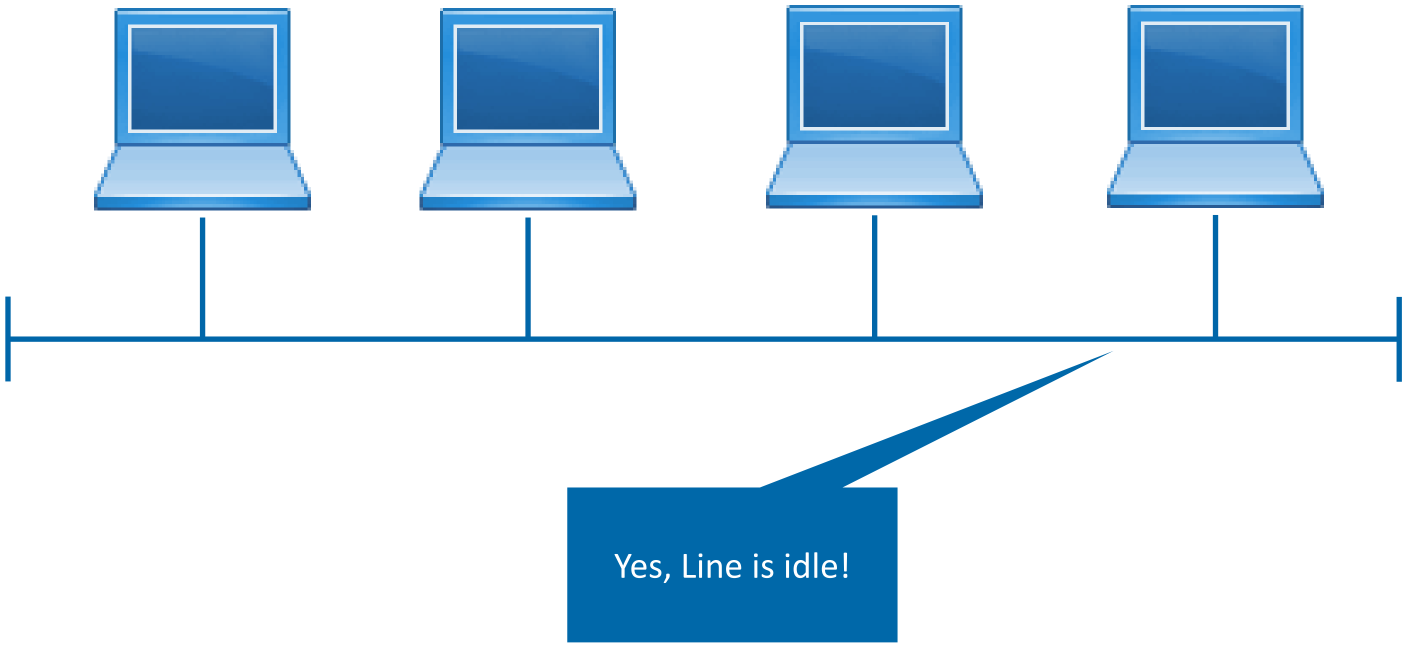
- Collision detection
  - Multiple devices send
  - Packets collide on medium



ISO OSI LAYERS

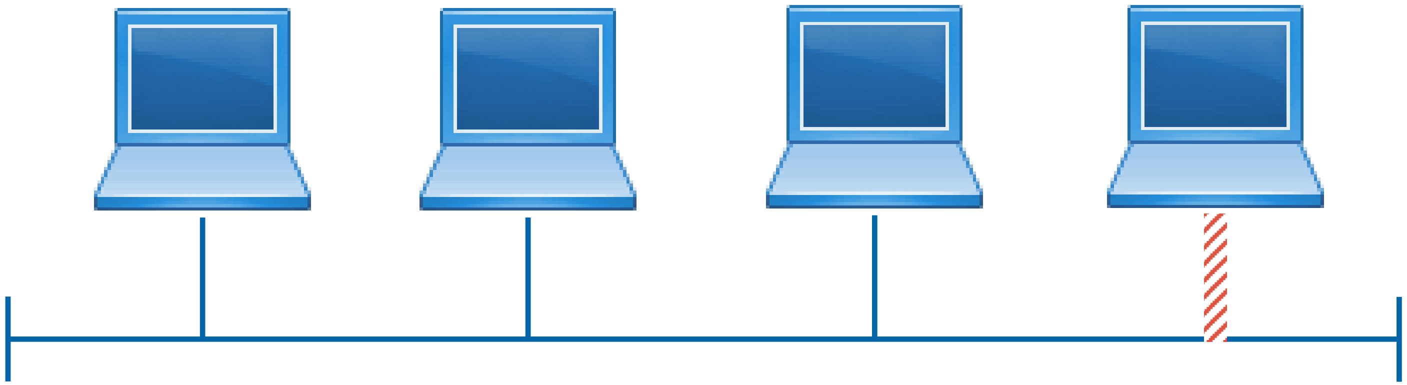
LAYER 2 – CSMA/CD COLLISION ALGORITHM

LAYER 2 – CSMA/CD COLLISION ALGORITHM



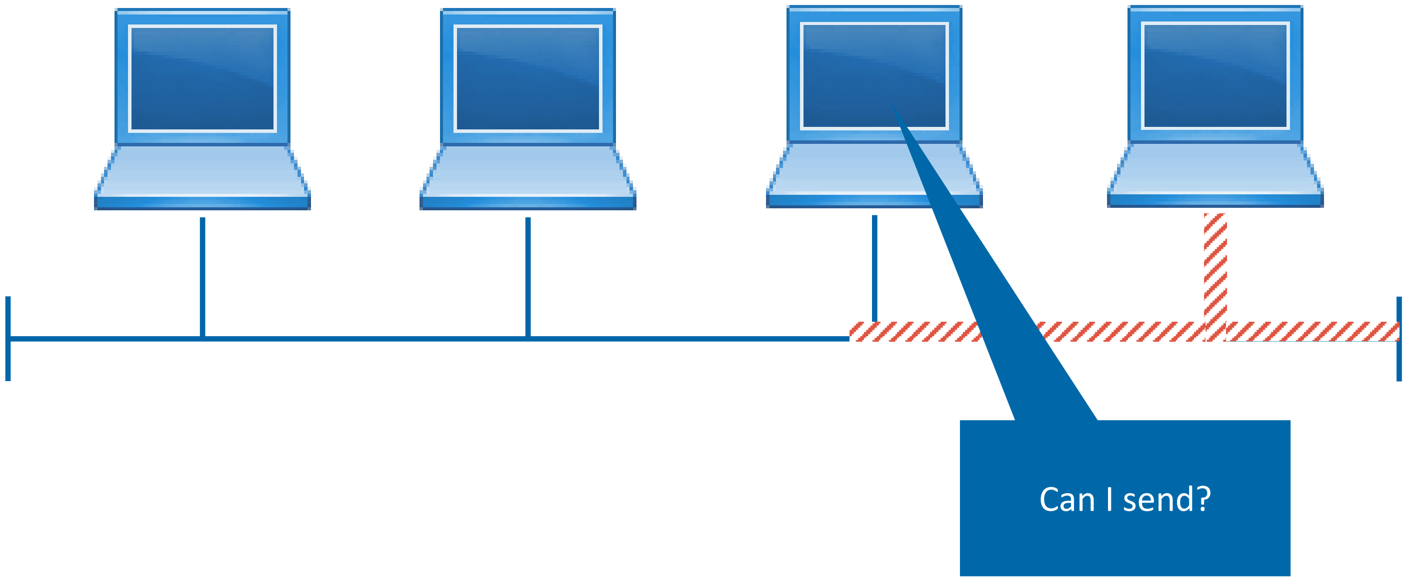
ISO OSI LAYERS

LAYER 2 – CSMA/CD COLLISION ALGORITHM

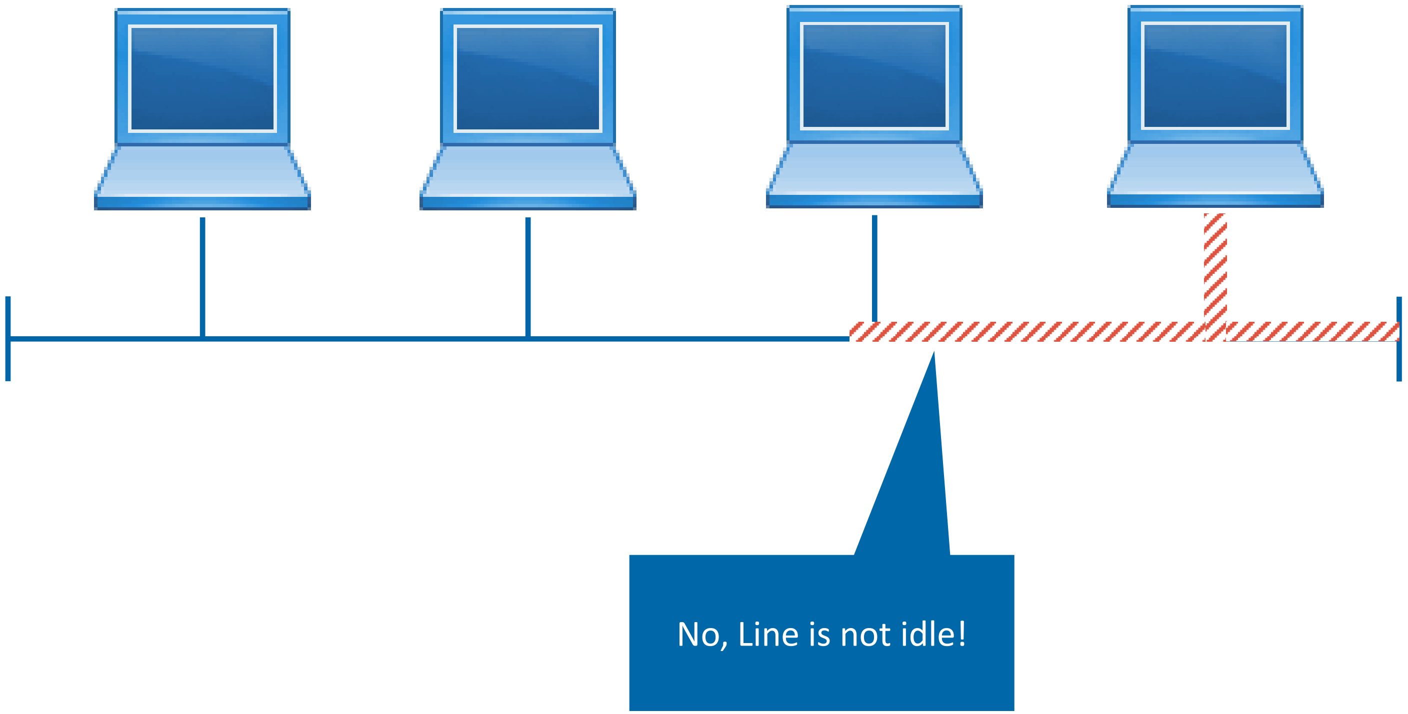


ISO OSI LAYERS

LAYER 2 – CSMA/CD COLLISION ALGORITHM

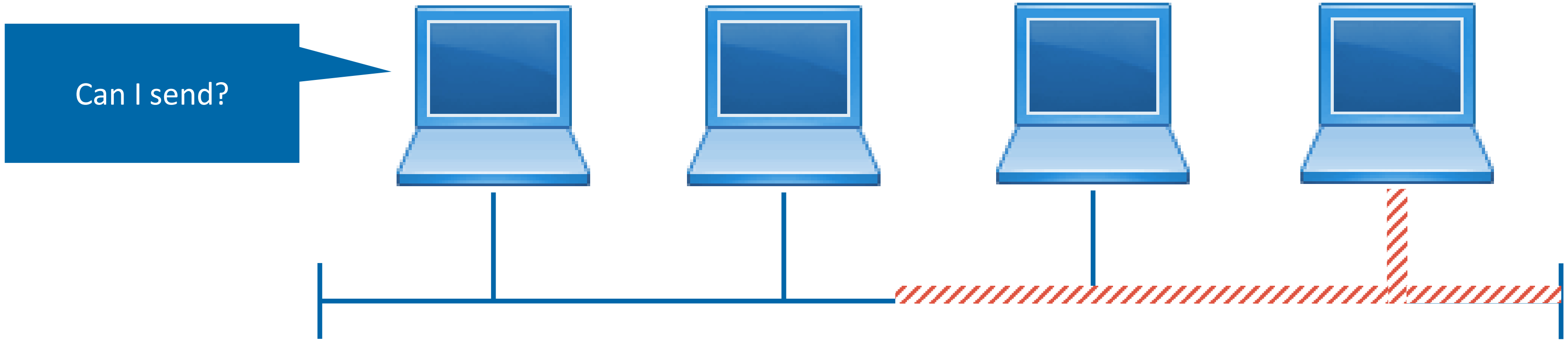


LAYER 2 – CSMA/CD COLLISION ALGORITHM

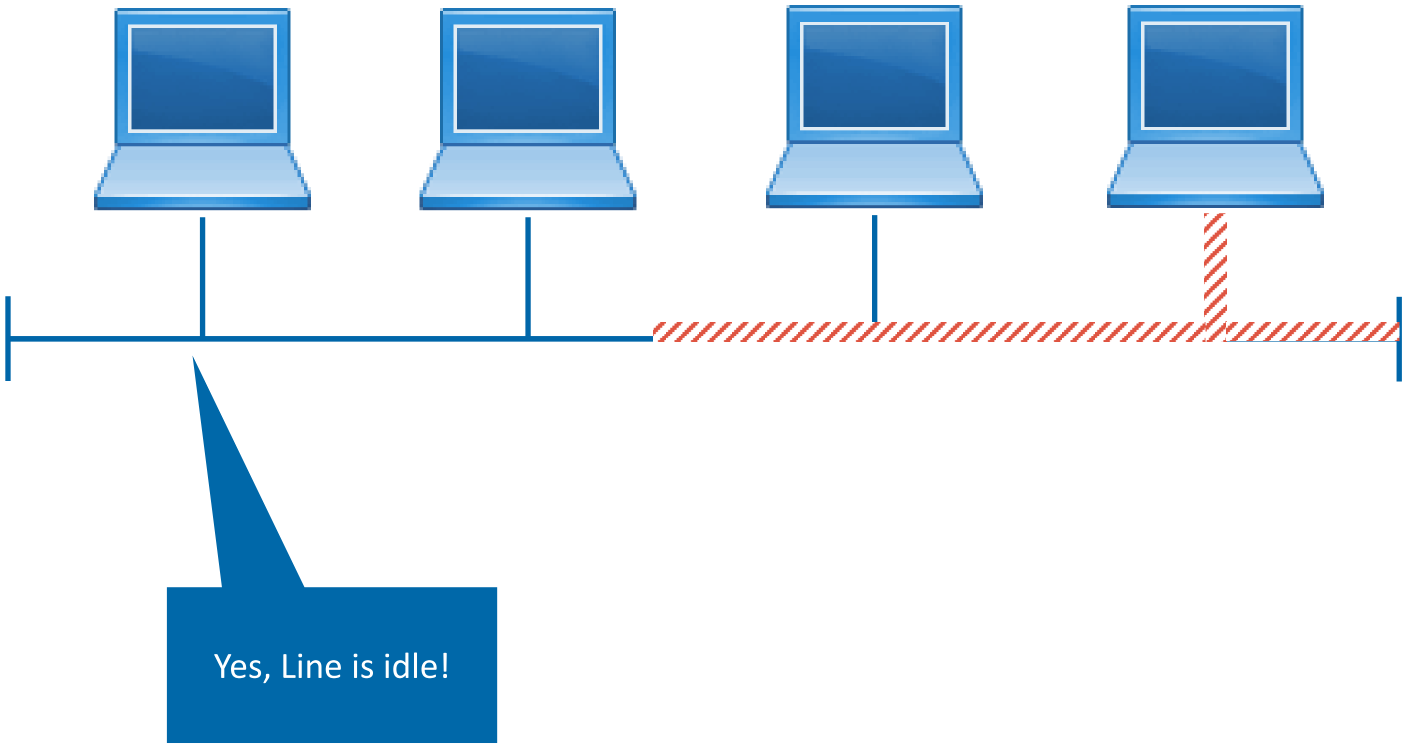


ISO OSI LAYERS

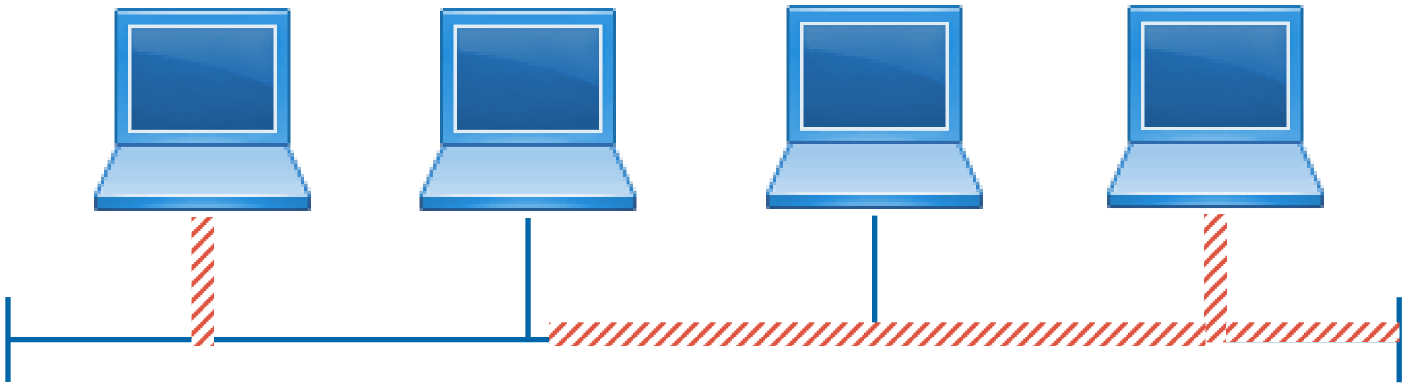
LAYER 2 – CSMA/CD COLLISION ALGORITHM



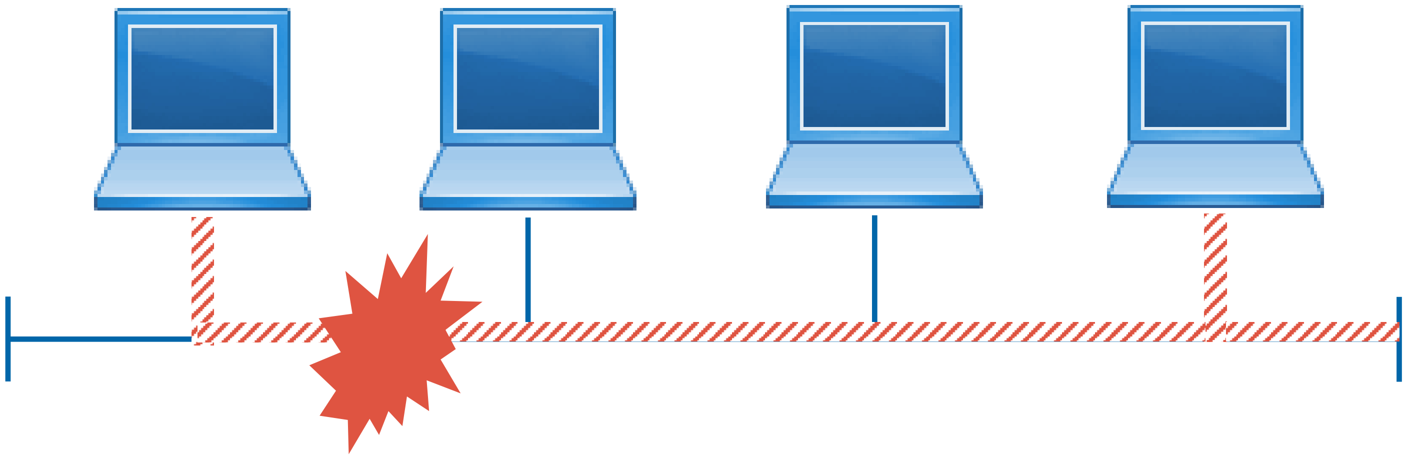
LAYER 2 – CSMA/CD COLLISION ALGORITHM



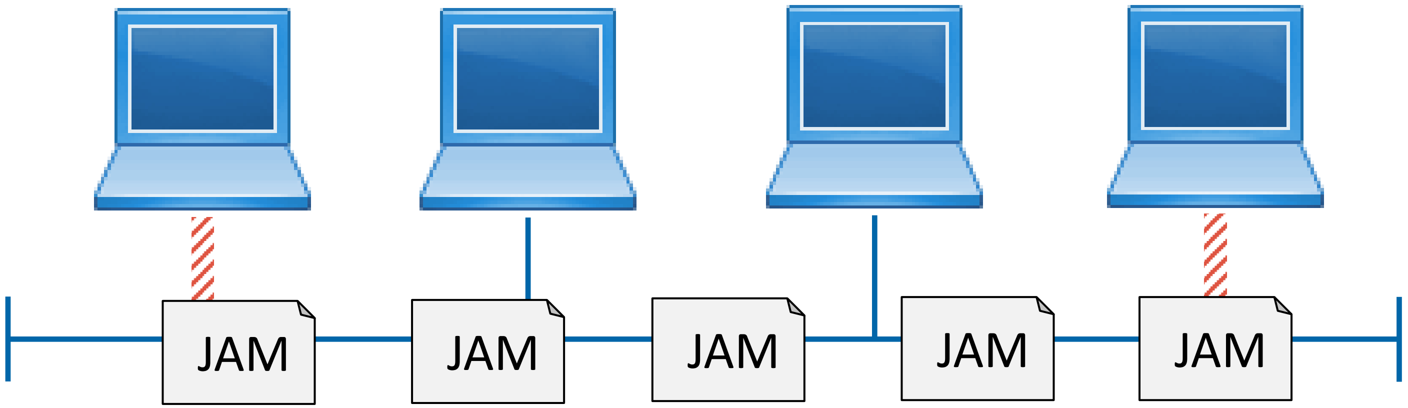
LAYER 2 – CSMA/CD COLLISION ALGORITHM



LAYER 2 – CSMA/CD COLLISION ALGORITHM

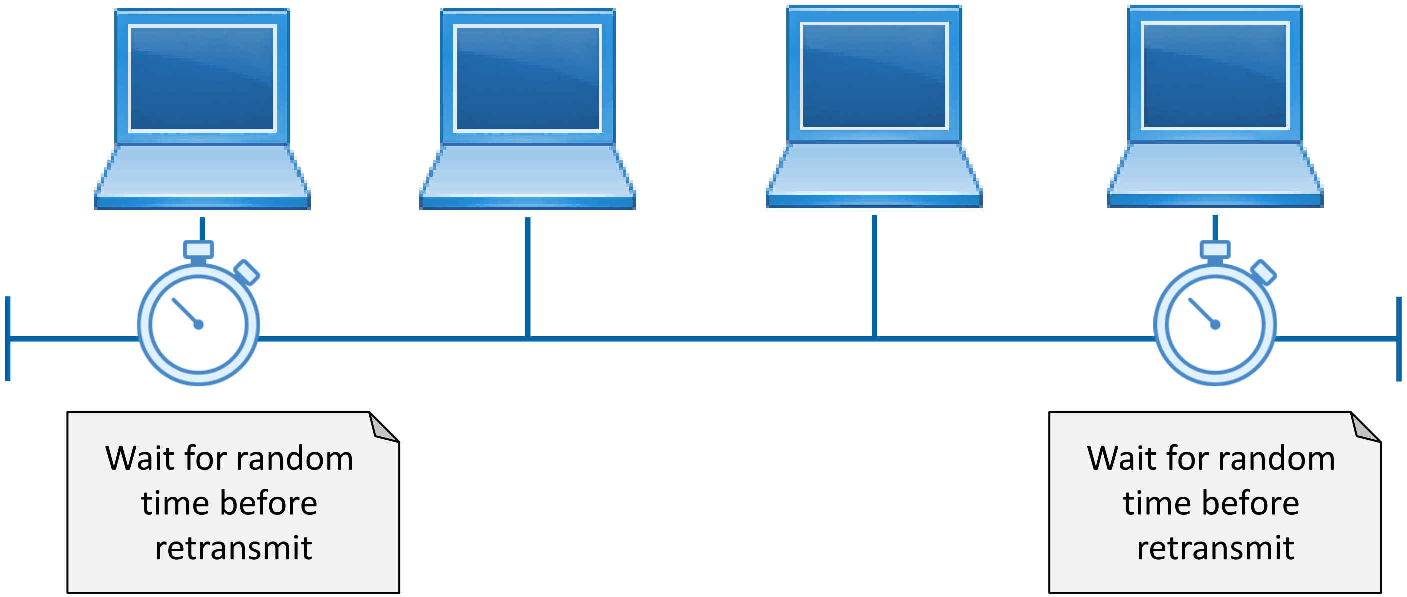


LAYER 2 – CSMA/CD COLLISION ALGORITHM



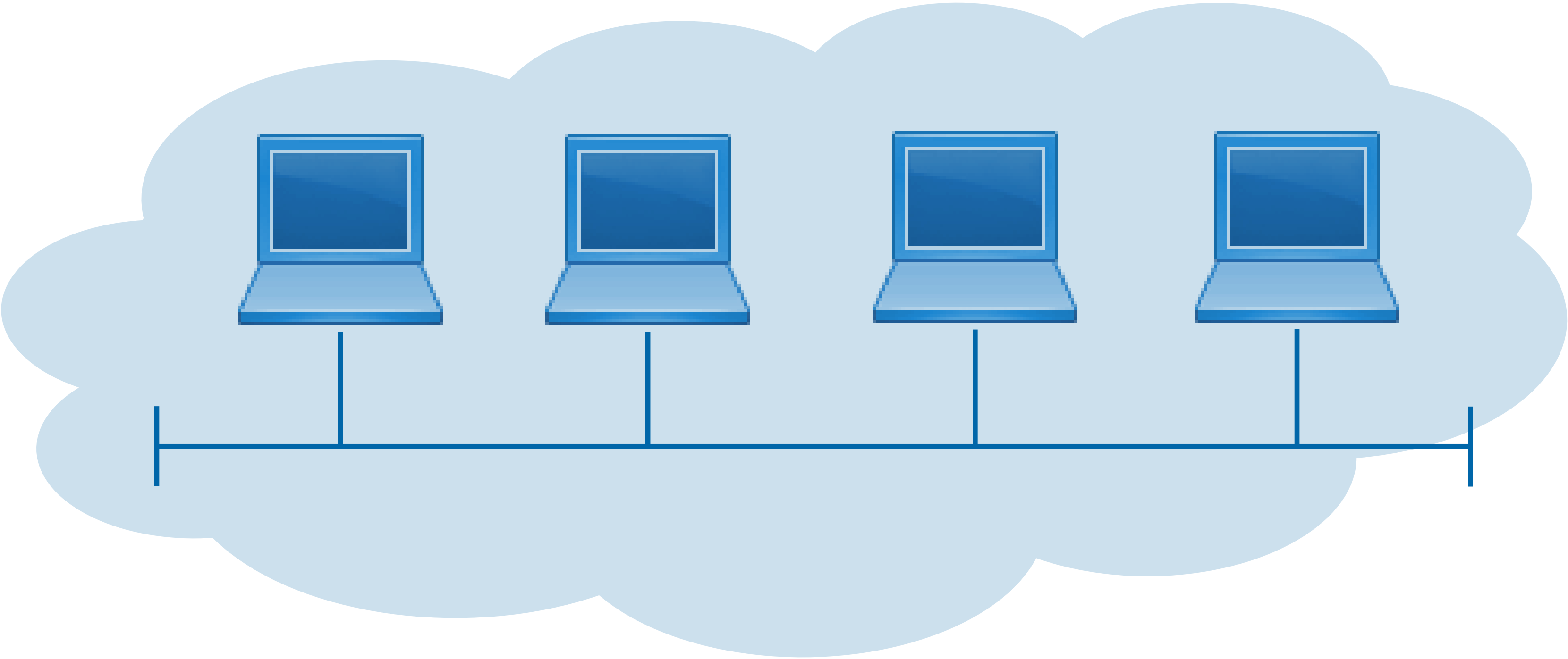
ISO OSI LAYERS

LAYER 2 – CSMA/CD COLLISION ALGORITHM



ISO OSI LAYERS

LAYER 2 – COLLISION DOMAIN

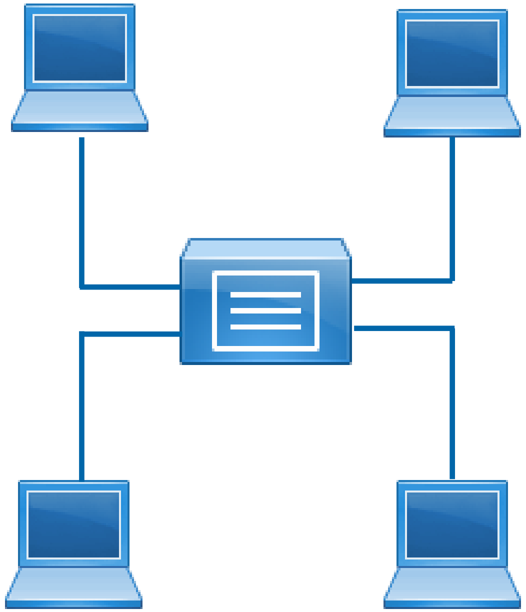


ISO OSI LAYERS

GEM MINE

LAYER 2 – COLLISION DOMAIN

- Why does a hub copy to all clients?
    - A hub is a multiport repeater
    - Its job is signal amplification
- What disadvantages does this create?
    - A hub takes the incoming signal and copies it…
    - …to all outgoing ports!
    - Thus, forming a collision domain
- Better solution: Use a switch instead!

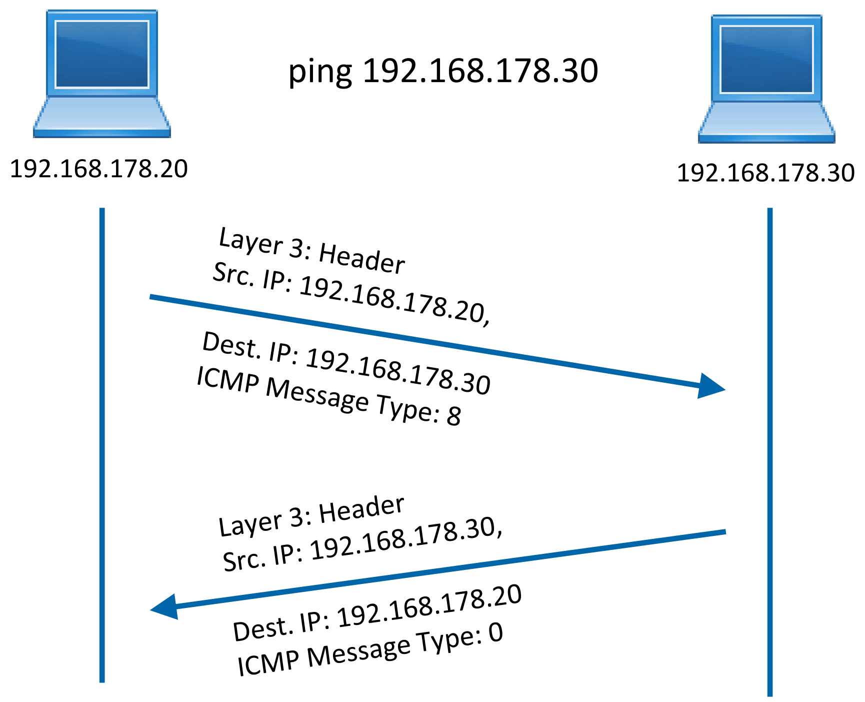


ISO OSI LAYERS

GEM MINE

LAYER 2 – ARP PROTOCOL

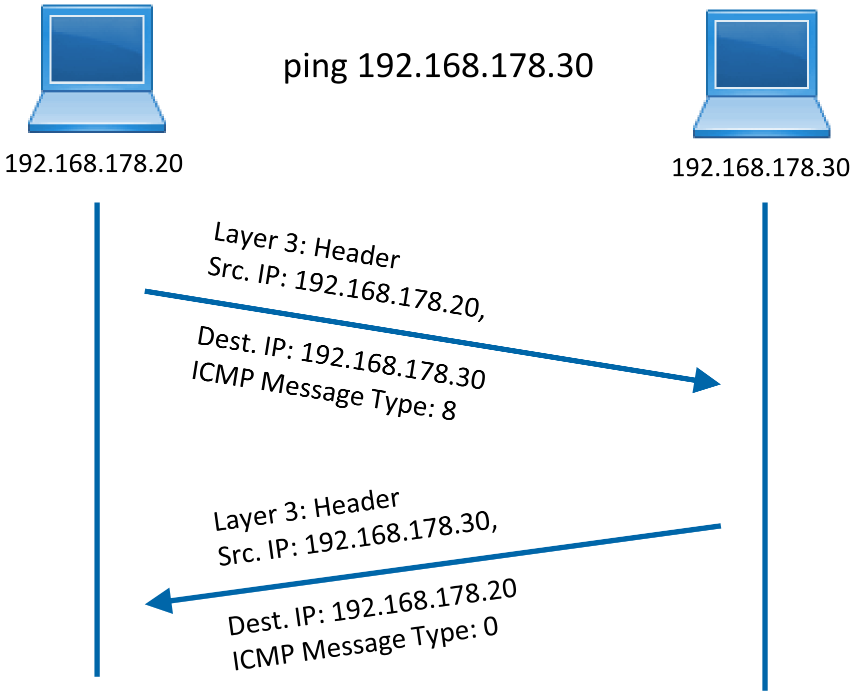
- But for a moment we believe our computer does
  - We will consider a Ping command call



ISO OSI LAYERS

LAYER 2 – ARP PROTOCOL

- But for a moment we believe our computer does
  - We will consider a Ping command call



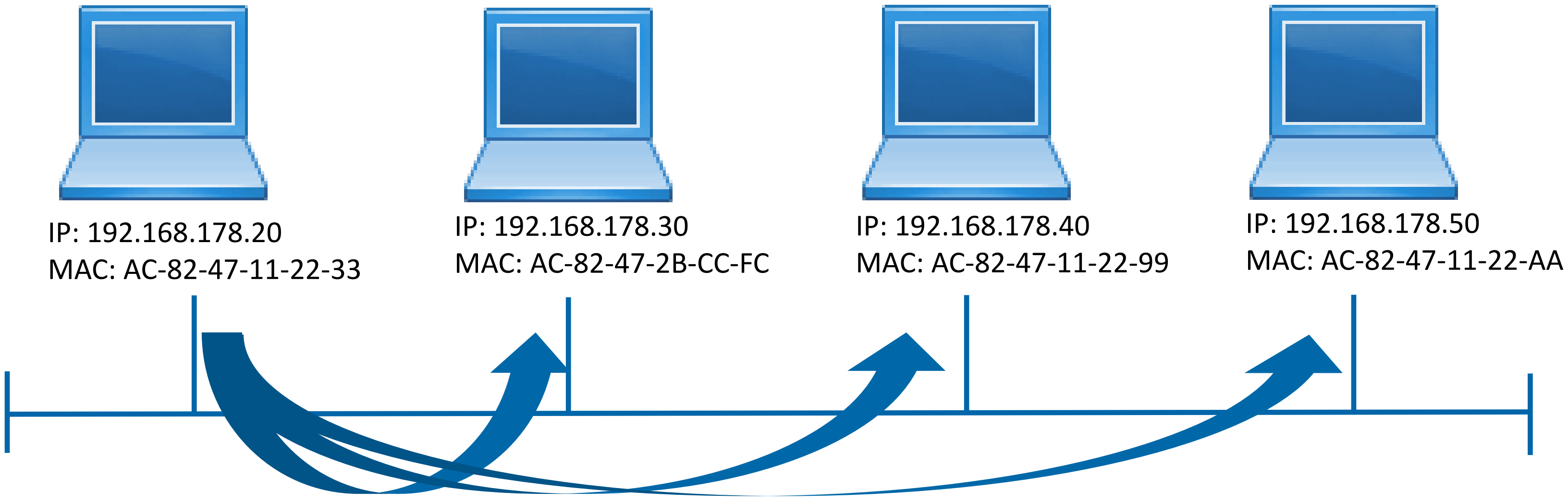

```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.178.30

Pinging 192.168.178.30 with 32 bytes of data:

Reply from 192.168.178.30: bytes=32 time=8ms TTL=128
Reply from 192.168.178.30: bytes=32 time=4ms TTL=128
Reply from 192.168.178.30: bytes=32 time=4ms TTL=128
Reply from 192.168.178.30: bytes=32 time=4ms TTL=128

Ping statistics for 192.168.178.30:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 4ms, Maximum = 8ms, Average = 5ms

C:\>arp -a
  Internet Address      Physical Address      Type
  192.168.178.30        0060.2fd0.5b0c        dynamic

C:\>
```

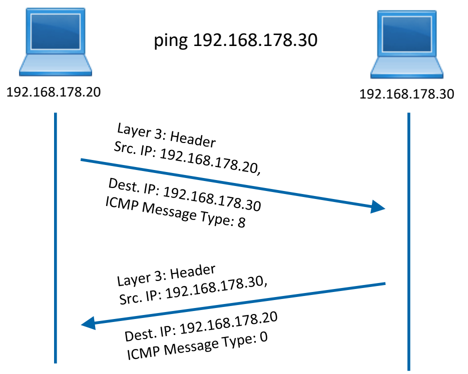
ISO OSI LAYERS

LAYER 2 – ARP PROTOCOL

ARP Table

<empty>





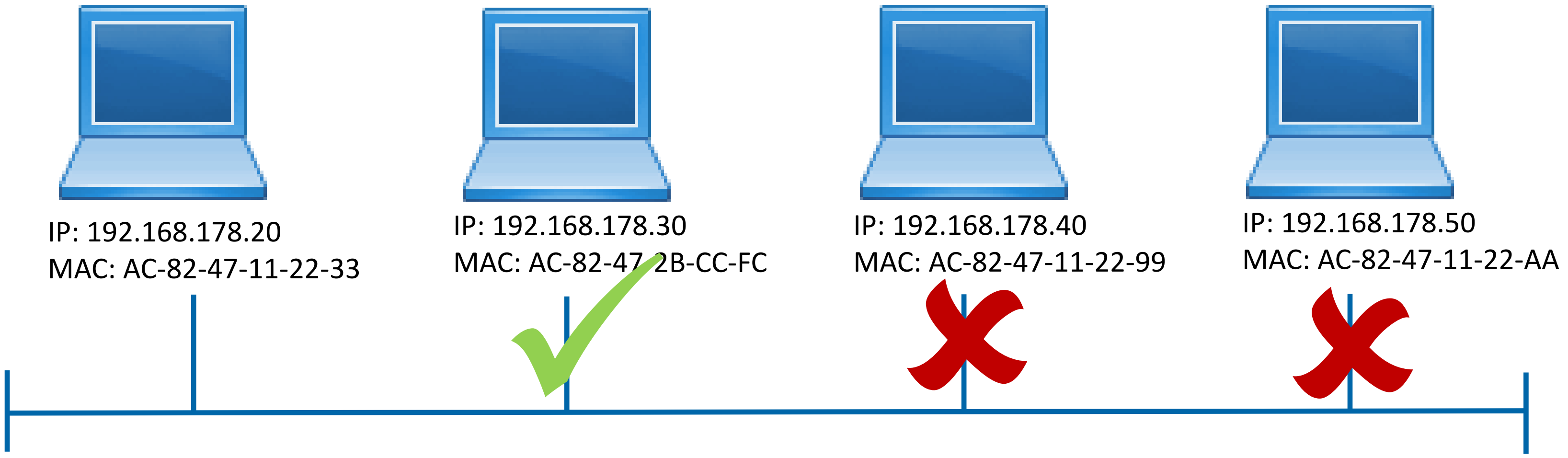
SRC MAC AC-82-47-11-22-33	DST MAC FF-FF-FF-FF-FF-FF	SRC IP 192.168.178.20	DST IP 192.168.178.30	WHAT IS YOUR MAC?

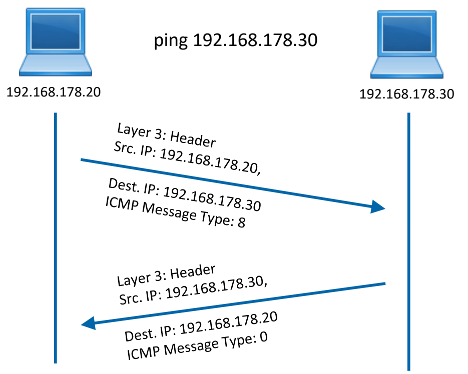
GEM MINE

LAYER 2 – ARP PROTOCOL

ARP Table

<empty>





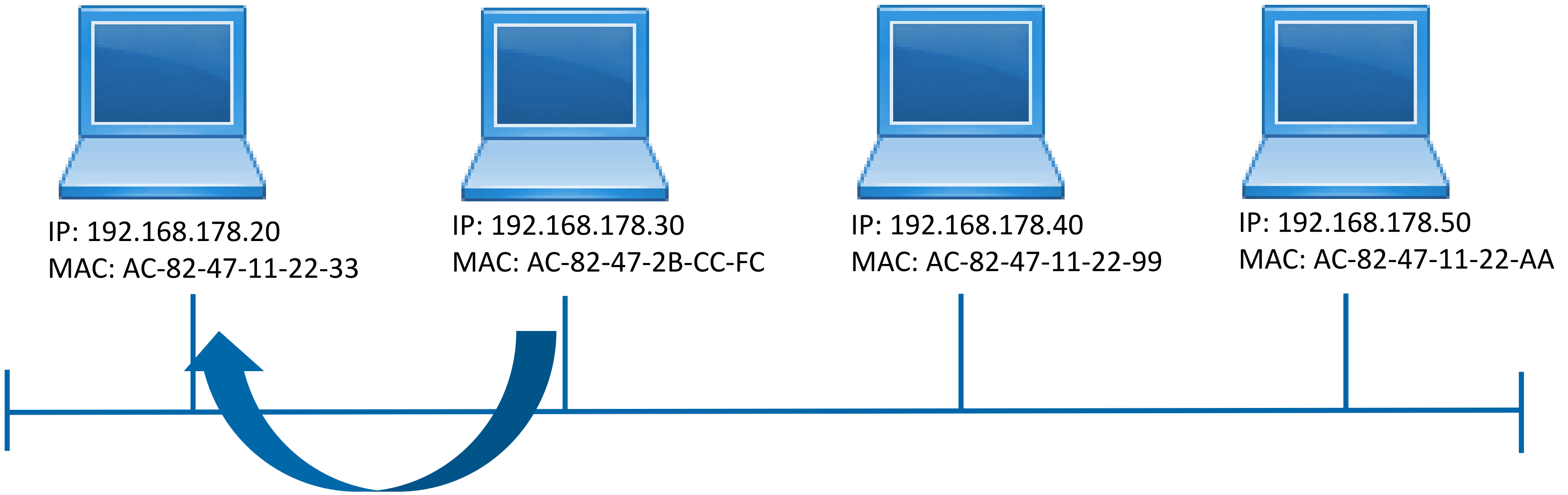
SRC MAC AC-82-47-11-22-33	DST MAC FF-FF-FF-FF-FF-FF	SRC IP 192.168.178.20	DST IP 192.168.178.30	WHAT IS YOUR MAC?

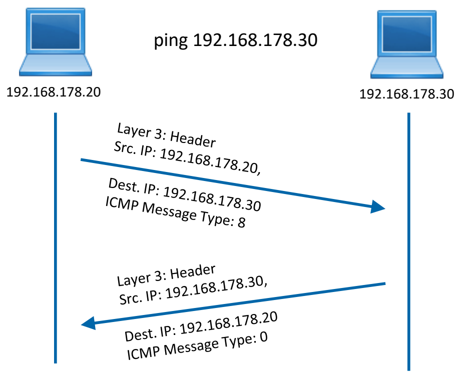
ISO OSI LAYERS

LAYER 2 – ARP PROTOCOL

ARP Table

<empty>





SRC MAC AC-82-47-11-22-33	DST MAC AC-82-47-2B-CC-FC	SRC IP 192.168.178.30	DST IP 192.168.178.20	THAT'S ME, THIS IS MY MAC.

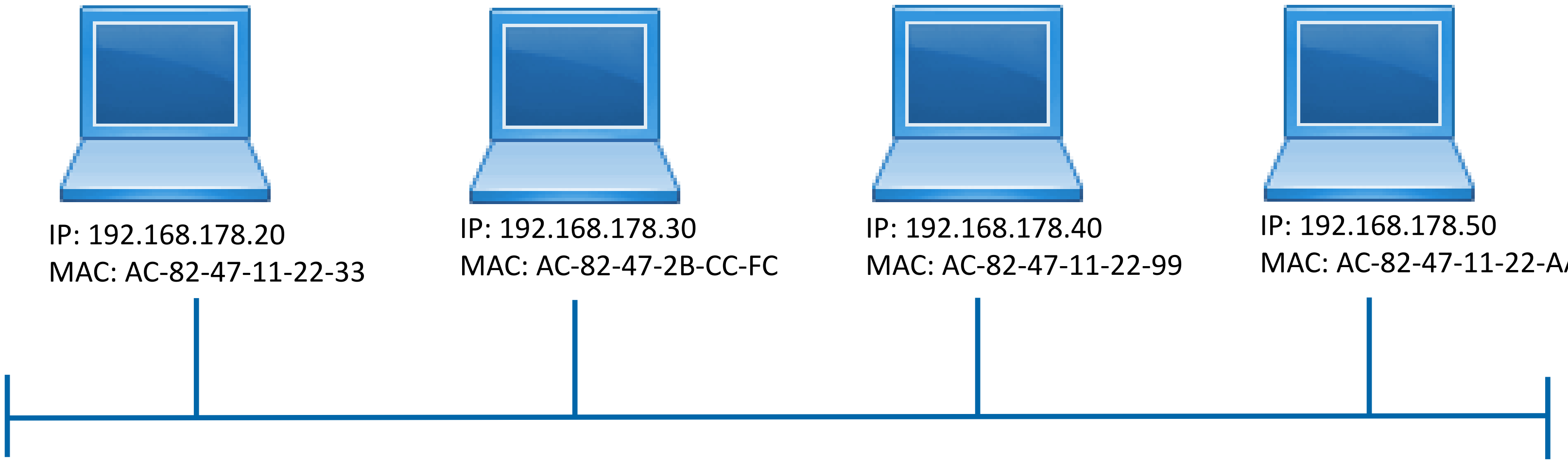
ISO OSI LAYERS

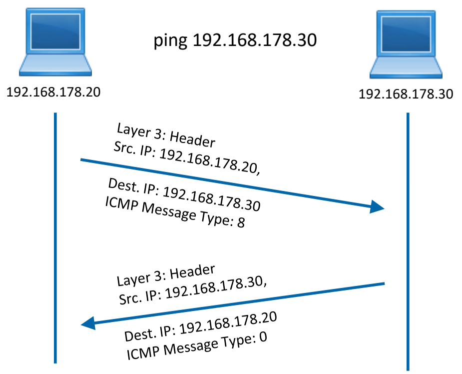
GEM MINE

LAYER 2 – ARP PROTOCOL

ARP Table

192.168.178.30	AC-82-47-2B-CC-FC





ISO OSI LAYERS

GEMMINE

LAYER 2 – ARP PROTOCOL ATTACKS

- ARP is completely unprotected
- Overwrite ARP entries (ARP poisoning)
  - ArpSpoof
  - ArpPoison
  - EtterCap
- Man in the middle attacks (MITM)

ISO OSI LAYERS

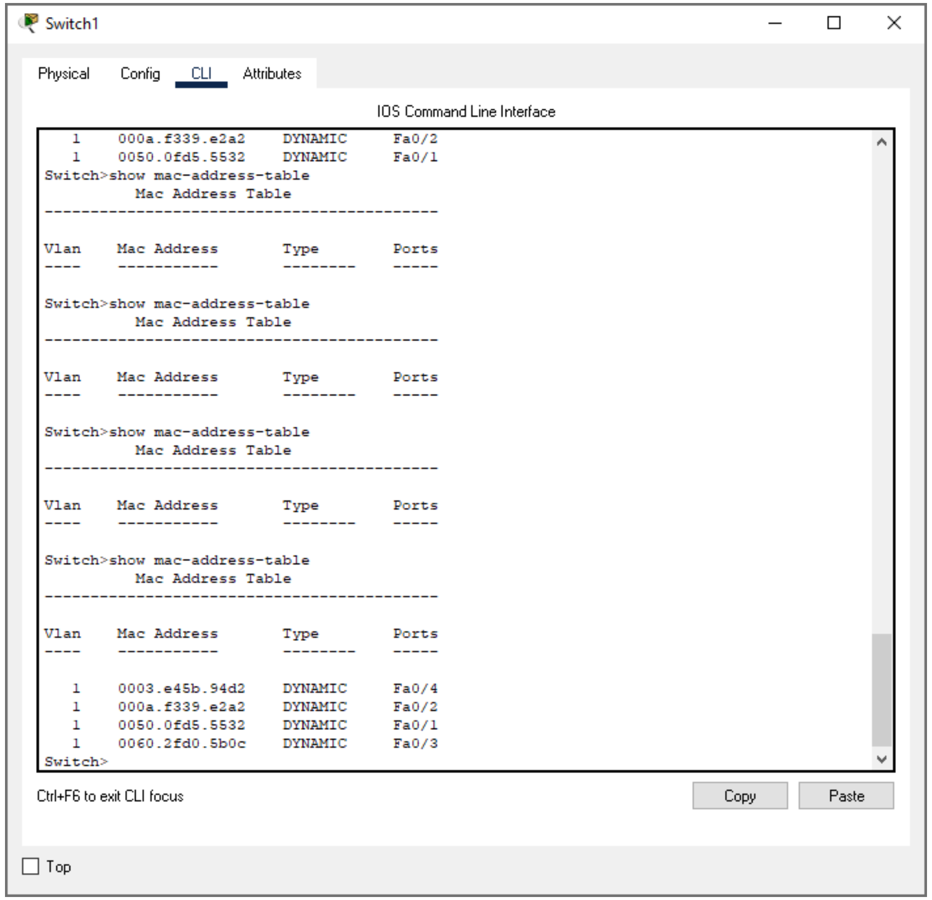
GEM MINE

LAYER 2 – HUB VS SWITCH

- Hub copies to all clients
  - Still a multiport repeater

- Switch has switch table
  - Contains MAC adresses and corresponding ports
  - Statically configurable
  - Dynamically learned
  - Thus, packets are send only to the destination

  - Switch shrinks the collision domain…
  - … but maintains the broadcast domain

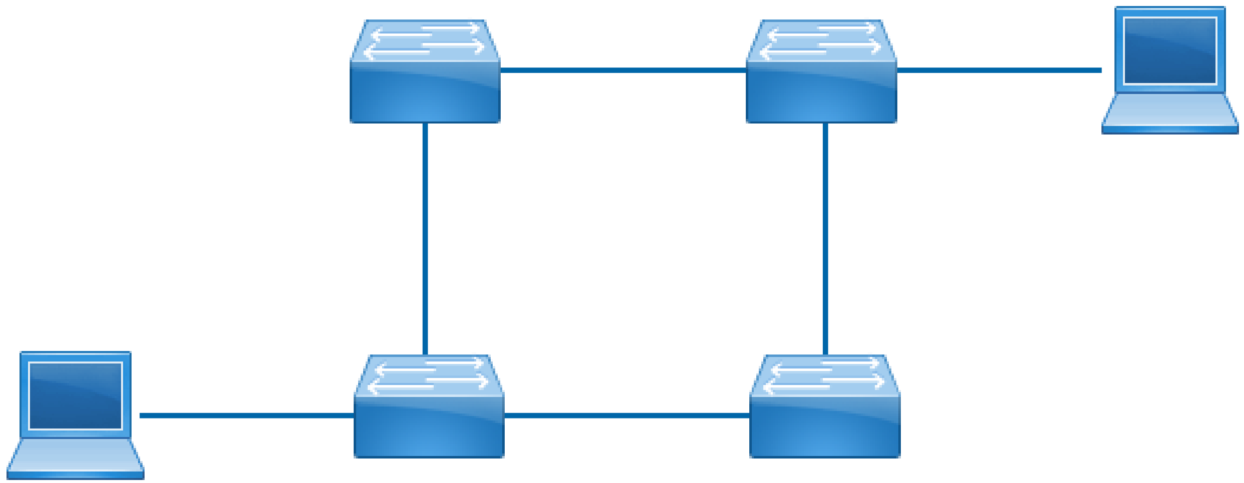


ISO OSI LAYERS

GEM MINE

LAYER 2 – SPANNING TREE PROTOCOL

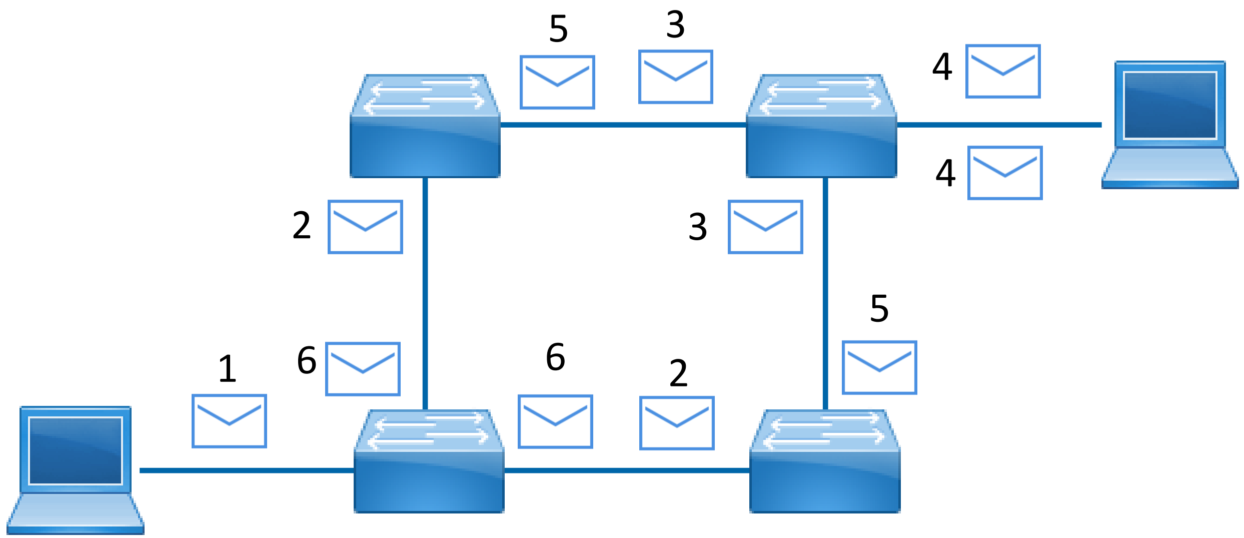
- Layer 2 network protocol
- Builds loop-free logical topology
- Prevent broadcast radiation



ISO OSI LAYERS

LAYER 2 – SPANNING TREE PROTOCOL

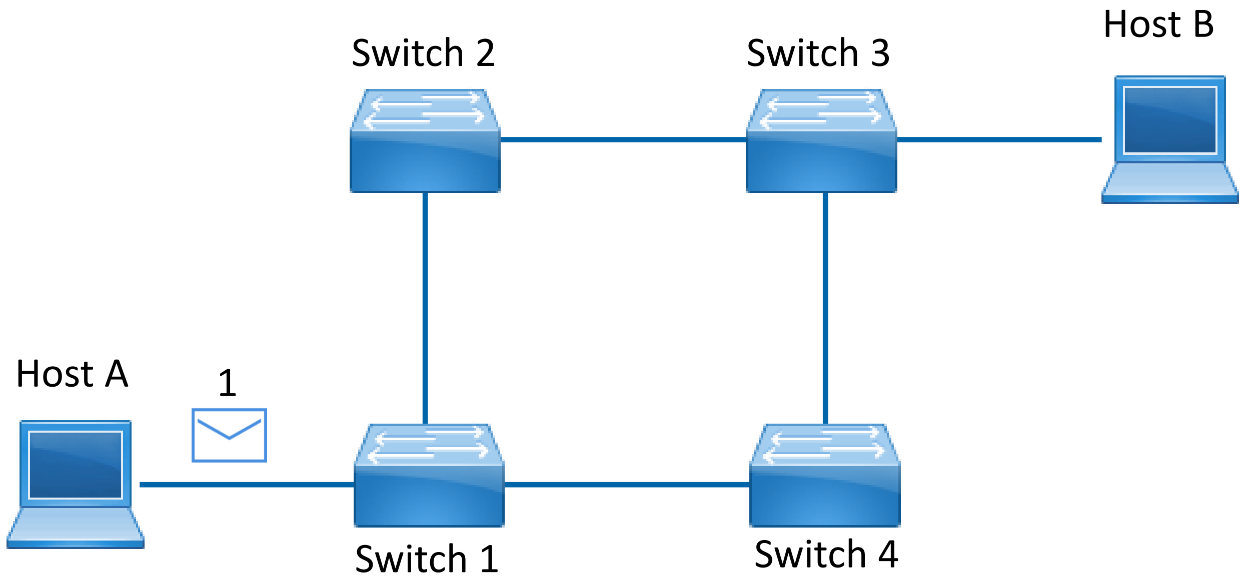
- Host A send a broadcast



ISO OSI LAYERS

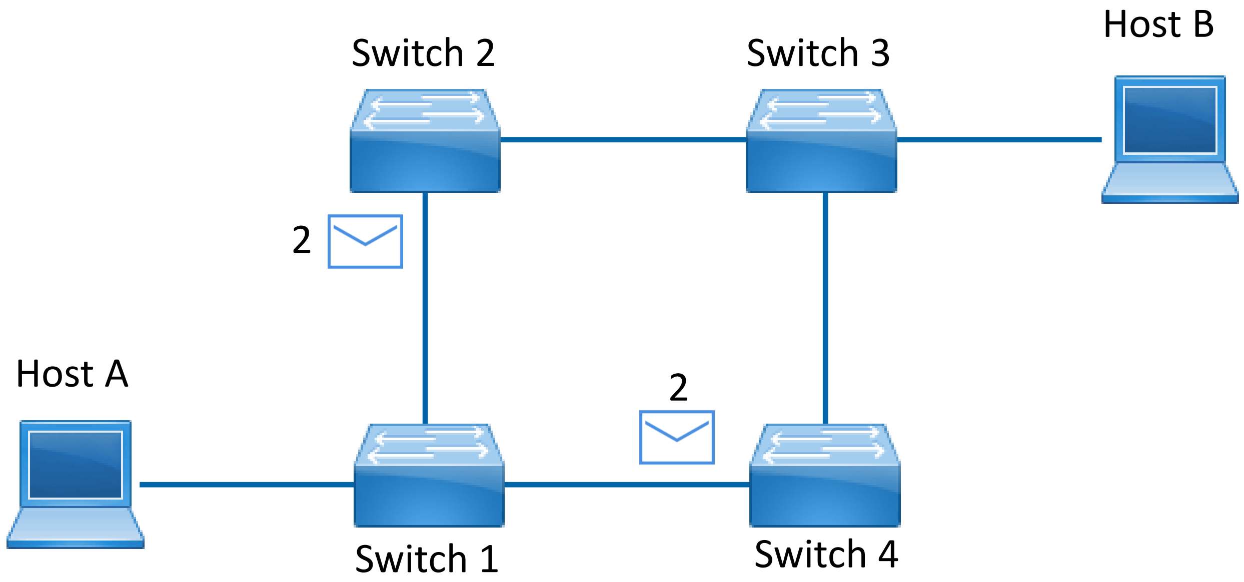
LAYER 2 – SPANNING TREE PROTOCOL

- Host A sends a broadcast



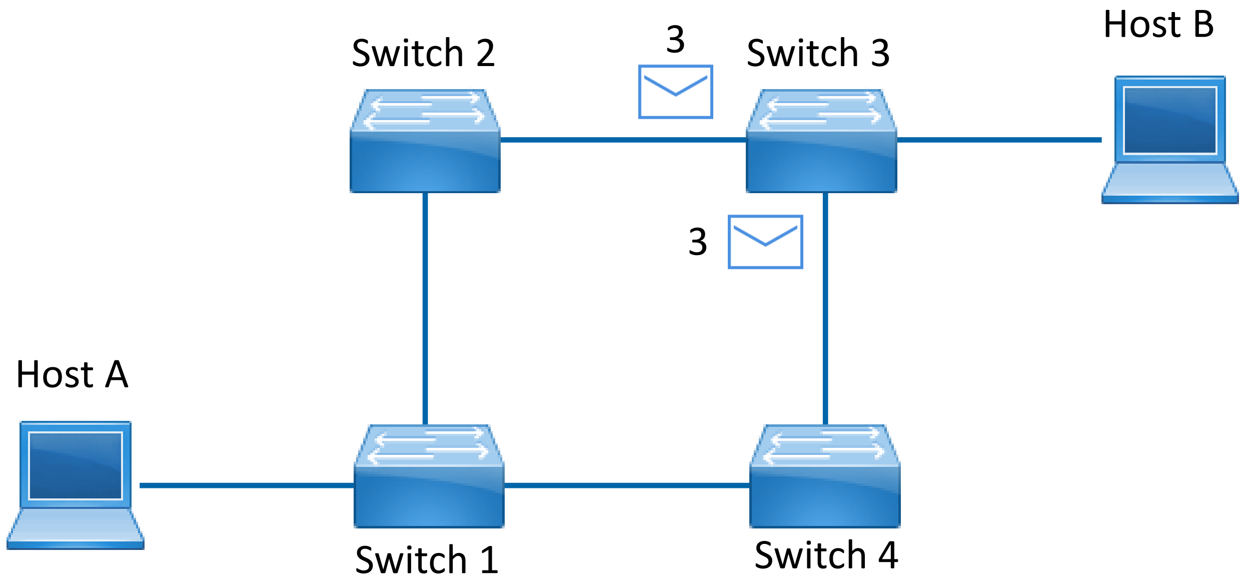
LAYER 2 – SPANNING TREE PROTOCOL

- Host A sends a broadcast
- Switch 1 receives the packet
- Switch 2 forwards the packet



LAYER 2 – SPANNING TREE PROTOCOL

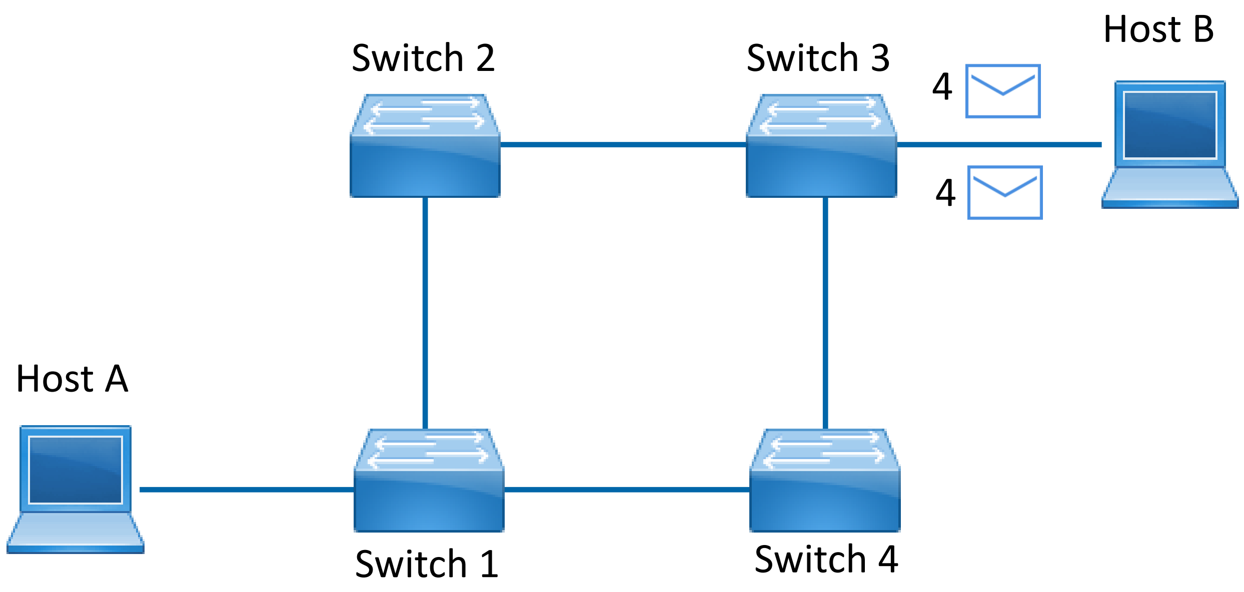
- Host A sends a broadcast
- Switch 1 receives the packet
- Switch 1 forwards the packet
- Switch 2 receives the packet
- Switch 2 forwards the packet
- Switch 4 receives the packet
- Switch 4 forwards the packet



ISO OSI LAYERS

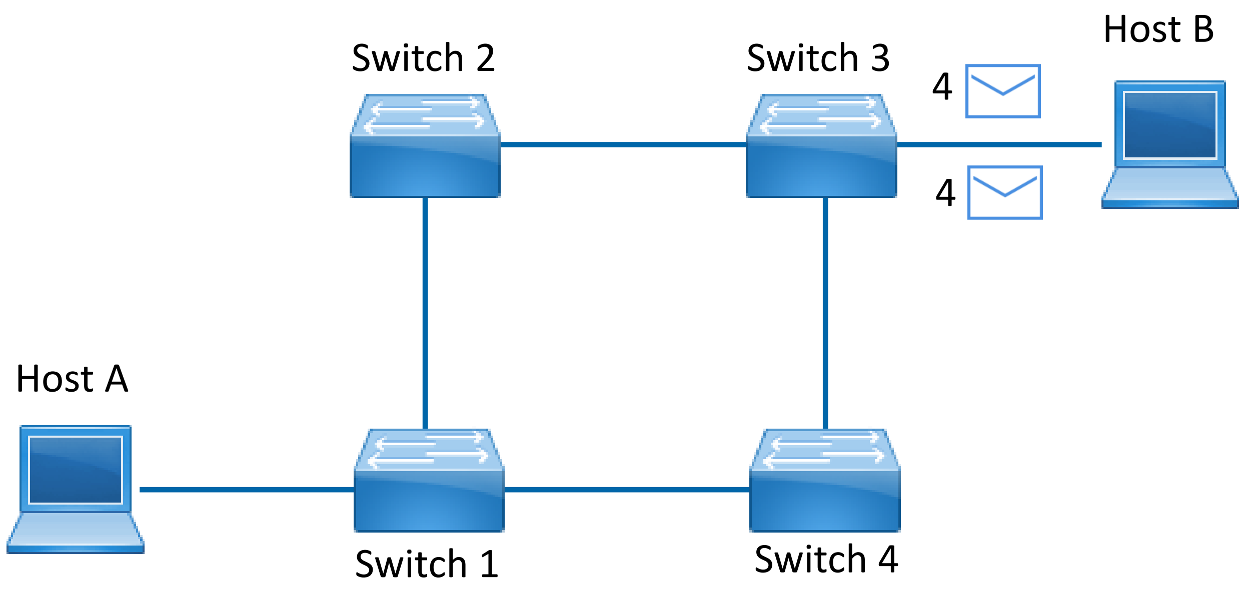
LAYER 2 – SPANNING TREE PROTOCOL

- Host A sends a broadcast
- Switch 1 receives the packet
- Switch 1 forwards the packet
- Switch 2 receives the packet
- Switch 2 forwards the packet
- Switch 4 receives the packet
- Switch 4 forwards the packet
- Switch 3 receives the packet
- Switch 3 forwards the packet
- Switch 3 receives another packet
- Switch 3 forwards the packet



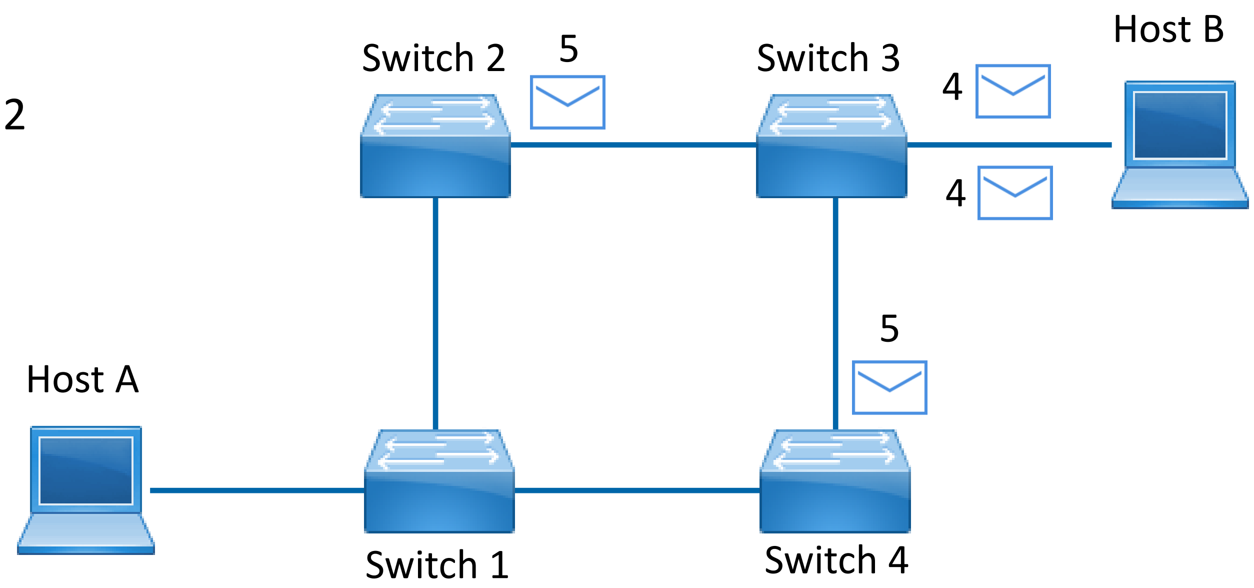
LAYER 2 – SPANNING TREE PROTOCOL

- Host A sends a broadcast
- Switch 1 receives the packet
- Switch 1 forwards the packet
- Switch 2 receives the packet
- Switch 2 forwards the packet
- Switch 4 receives the packet
- Switch 4 forwards the packet
- Switch 3 receives the packet
- Switch 3 forwards the packet
- Switch 3 receives another packet
- Switch 3 forwards the packet



LAYER 2 – SPANNING TREE PROTOCOL

- Host B gets two packets!
- Switch 3 forwards the first packet to switch 4
- Switch 3 forwards the second packet to switch 2

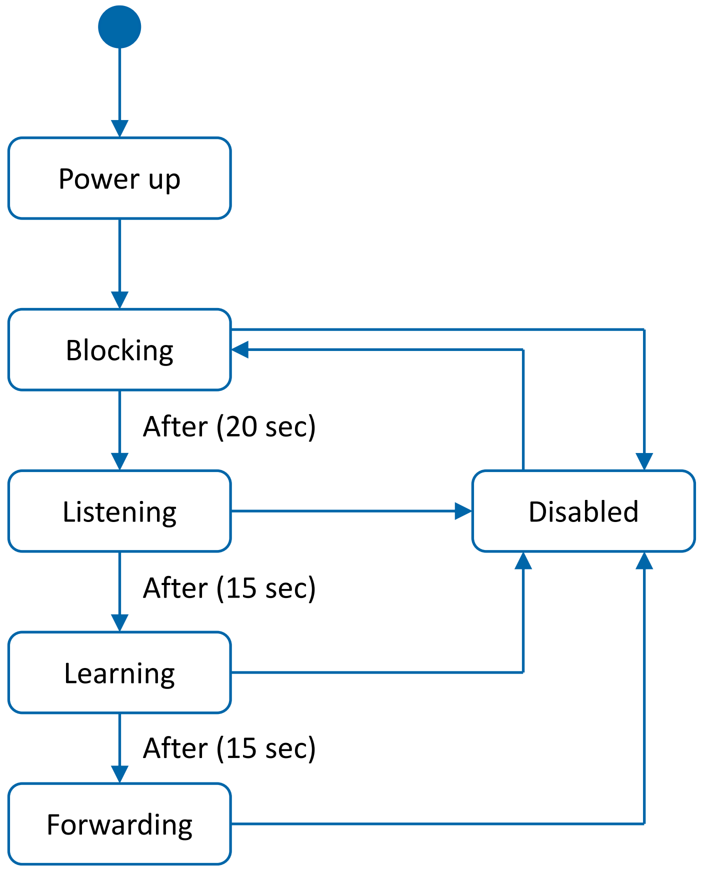


GEMMINE

LAYER 2 – SPANNING TREE PROTOCOL

- Build the topology
  - Power up all switches
  - All Switches set their ports to „Blocked“
  - Every switch assumes it is root and sends out BDPUs
  - Switch with smallest BridgeID becomes root
  - Root sends out Config-BDPUs
  - Every switch determines port with lowest costs to root
  - Ports with same costs: smallest PortID wins.

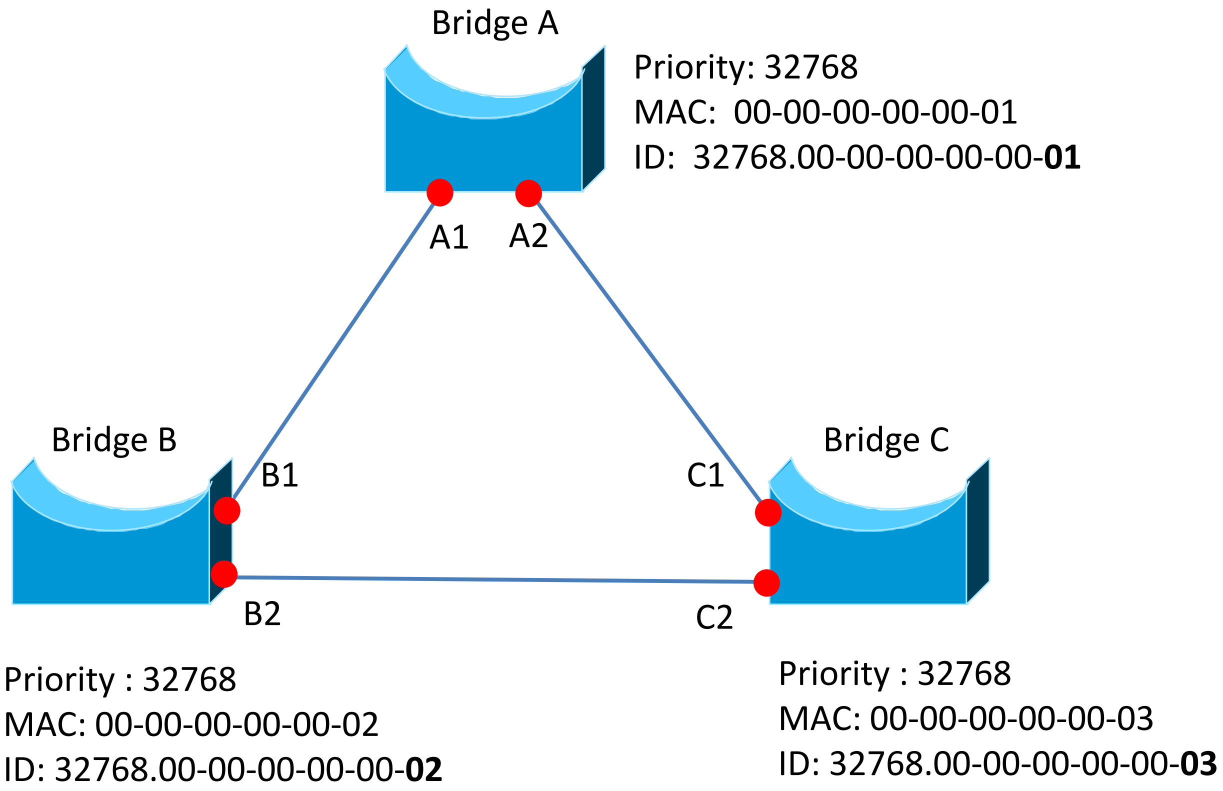
  - Cisco sets priority to 32768



ISO OSI LAYERS

LAYER 2 – SPANNING TREE PROTOCOL

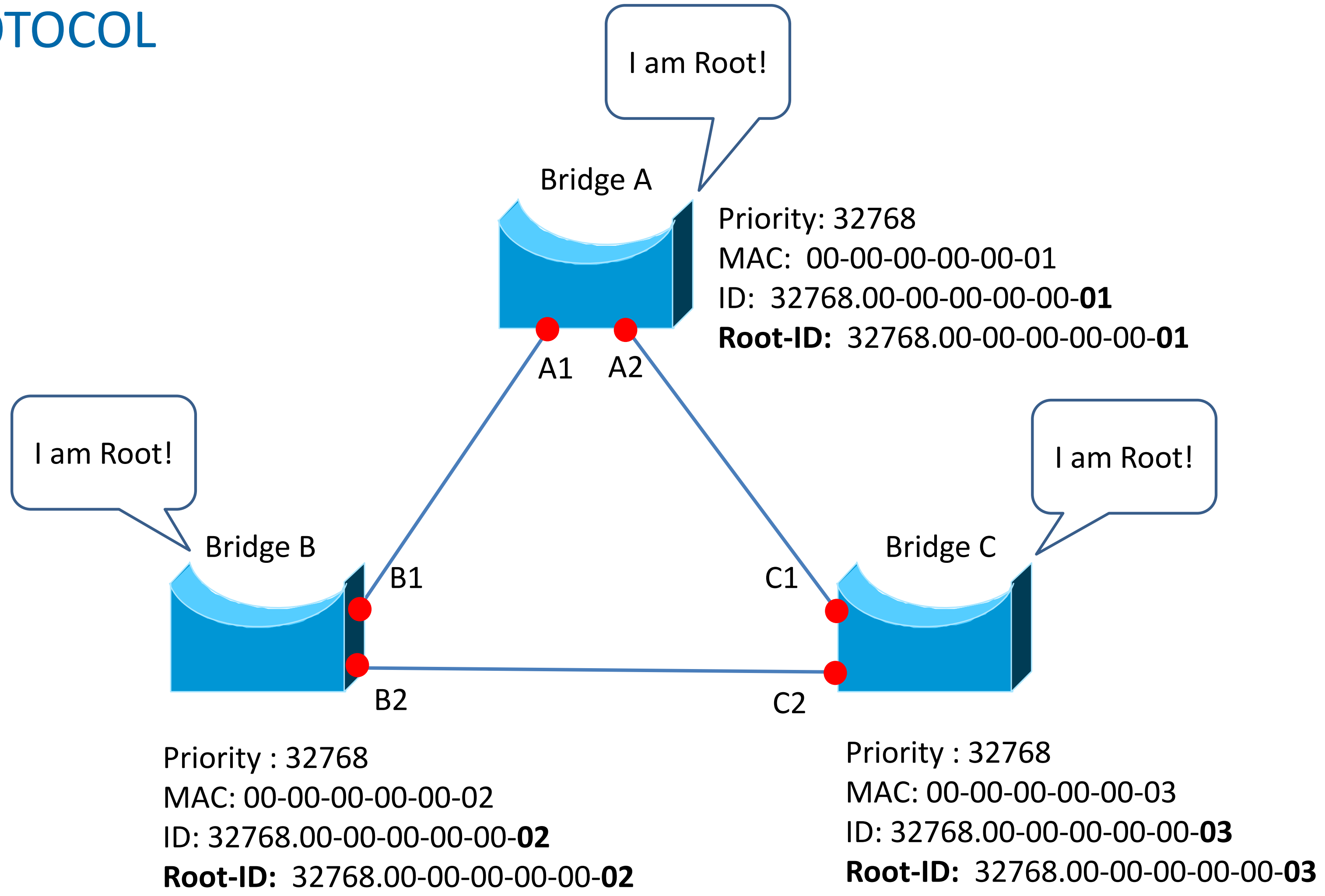
- Bridge Configuration set



GEM MINE

LAYER 2 – SPANNING TREE PROTOCOL

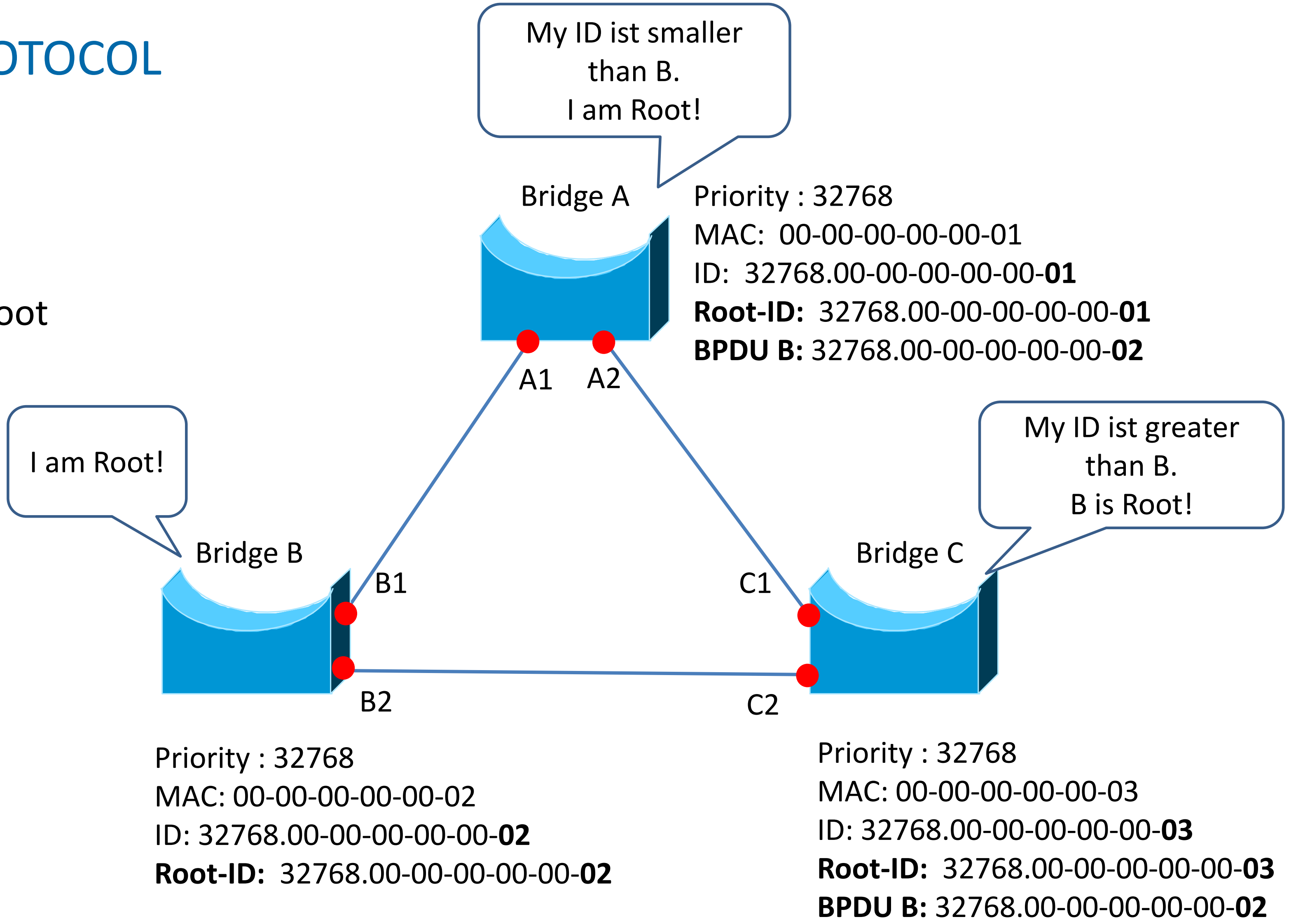
- Bridge Configuration set
- Bridges set themselves to root



GEM MINE

LAYER 2 – SPANNING TREE PROTOCOL

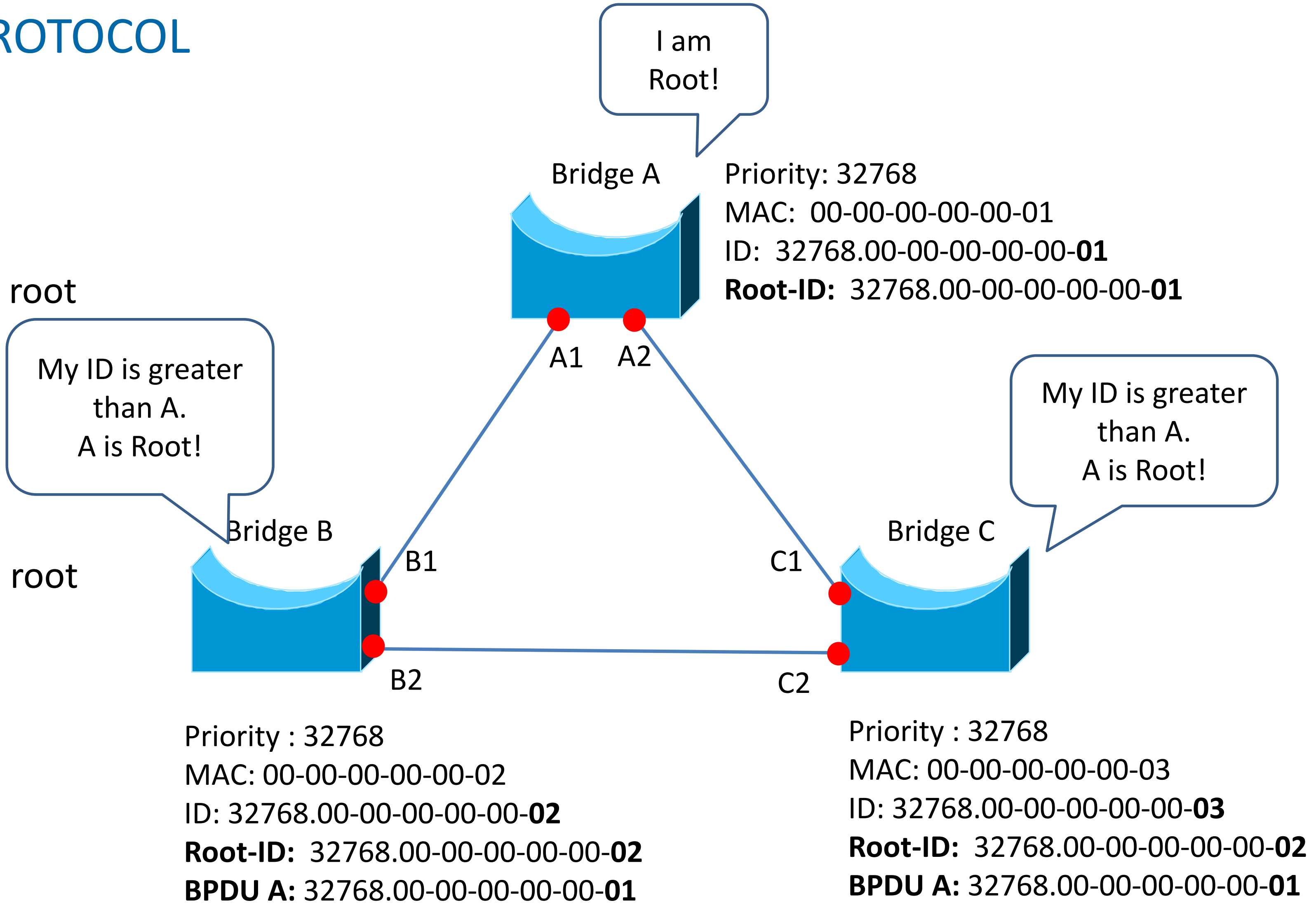
- Bridge Configuration set
- Bridges set themselves to root
- B sends a BDPU and declares to be root
- A sees its ID is smaller
- A stays root
- C sees its ID is greater
- C recognizes B as root



GEM MINE

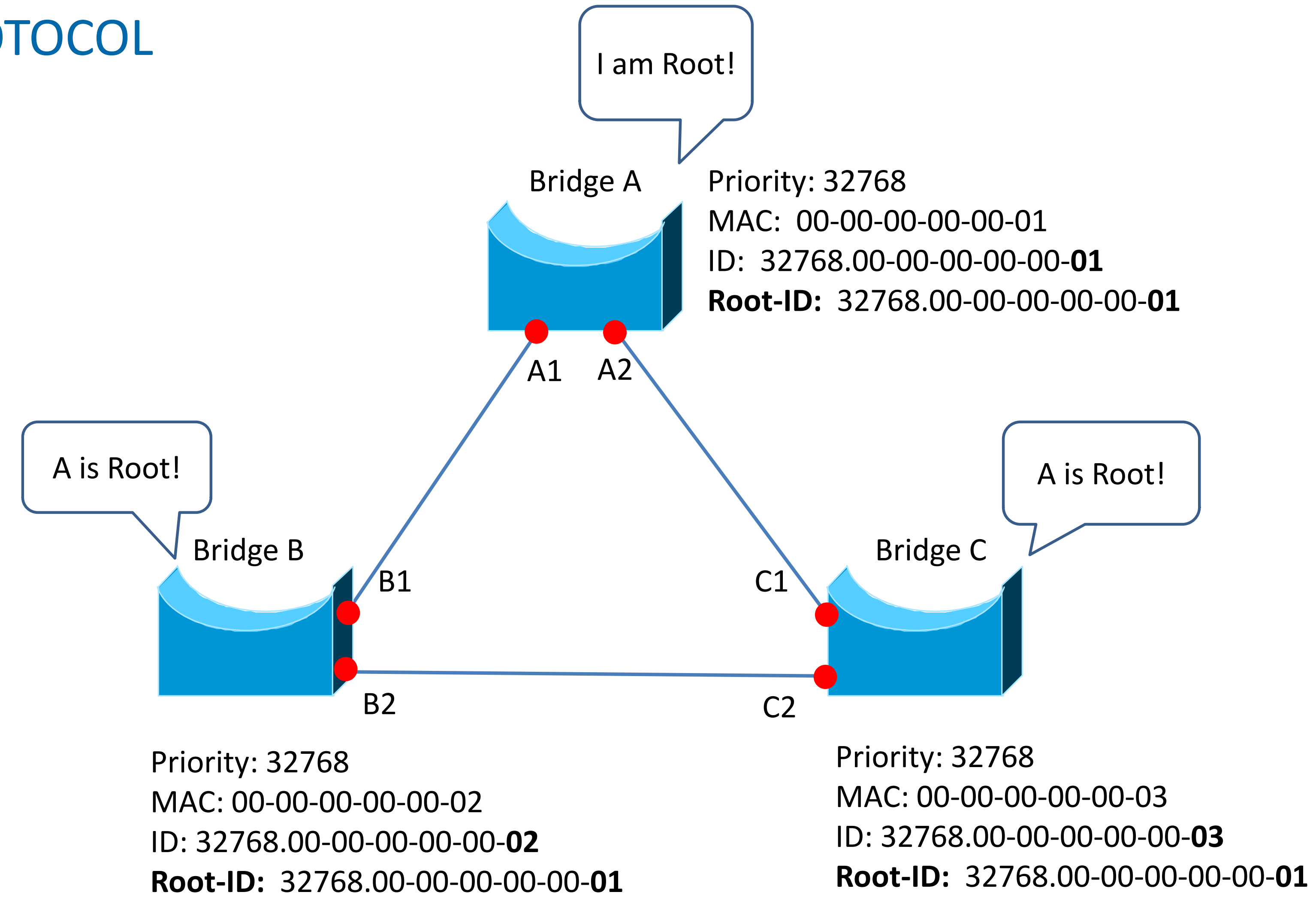
LAYER 2 – SPANNING TREE PROTOCOL

- Bridge Configuration set
- Bridges set themselves to root
- B sends a BDPU and declares to be root
- A sees its ID is smaller
- A stays root
- C sees its ID is greater
- C recognizes B as root
- A sends a BDPU and declares to be root
- C sees its ID is greater
- C recognizes A as root
- B sees its ID is greater
- B recognizes A as root



LAYER 2 – SPANNING TREE PROTOCOL

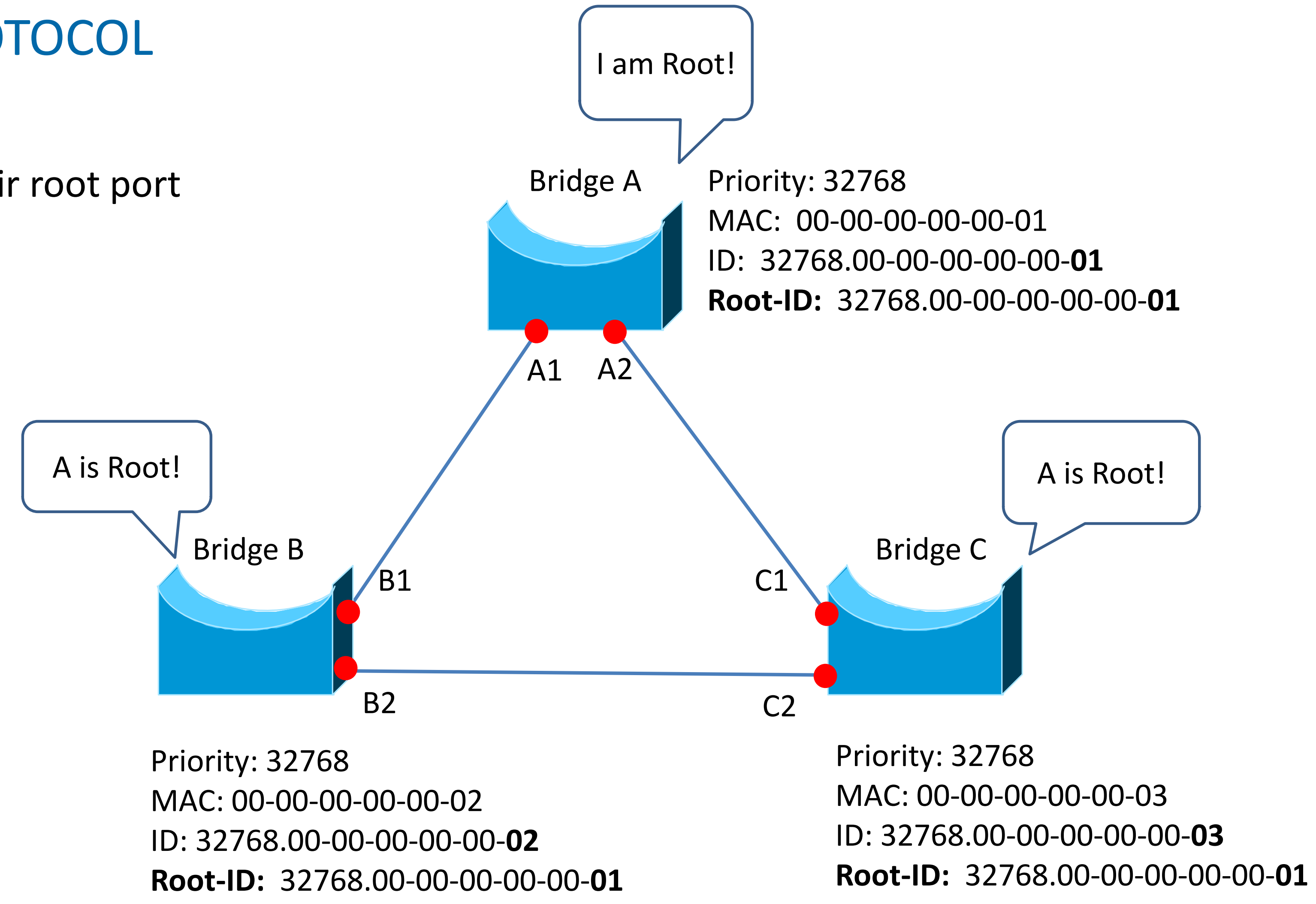
- Bridge A becomes root



LAYER 2 – SPANNING TREE PROTOCOL

- After that, the bridges determine their root port
- Done via fastest data path or
- Path with lowest cost.

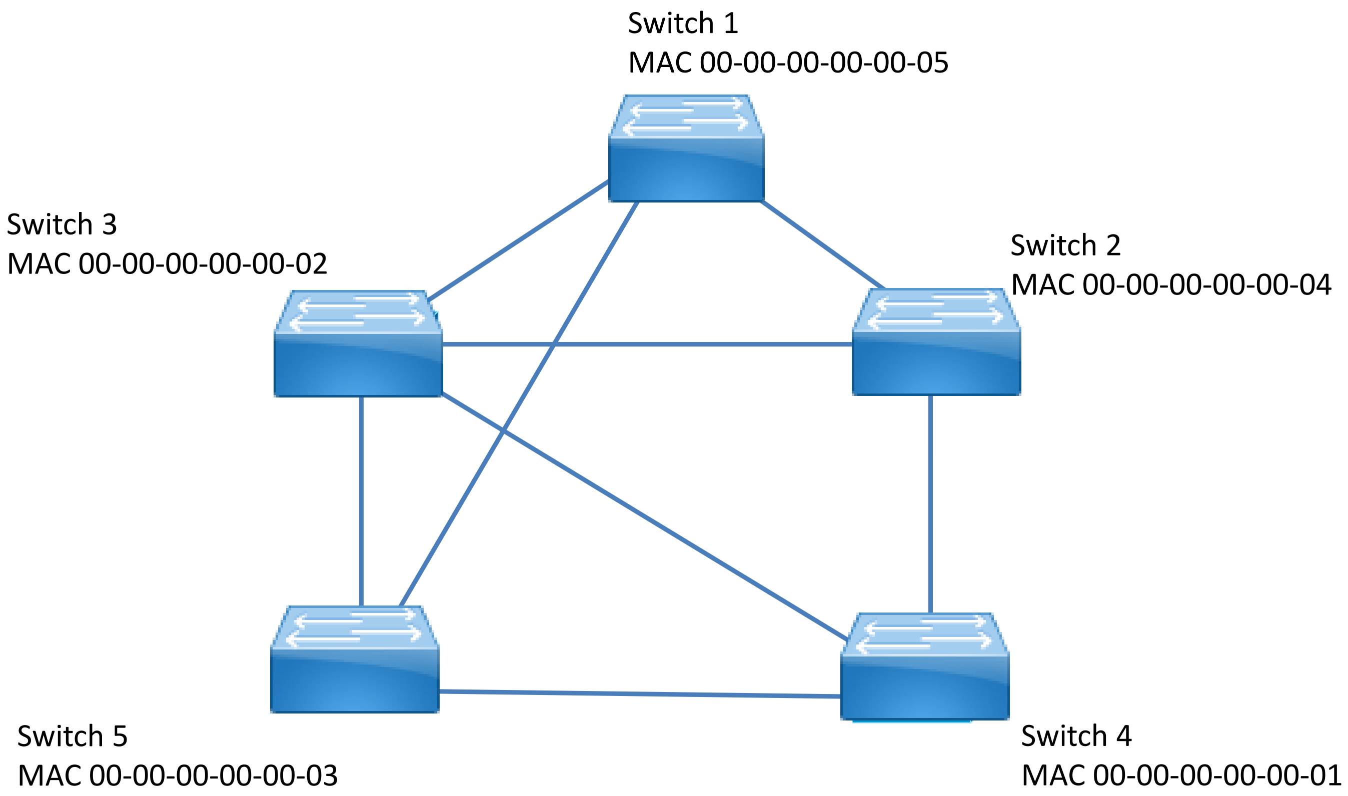
Bandwidth	STP-Cost
4 Mbit/s	250
10 Mbit/s	100
16 Mbit/s	62
45 Mbit/s	39
100 Mbit/s	19
155 Mbit/s	14
622 Mbit/s	6
1 Gbit/s	4
10 Gbit/s	2



ISO OSI LAYERS

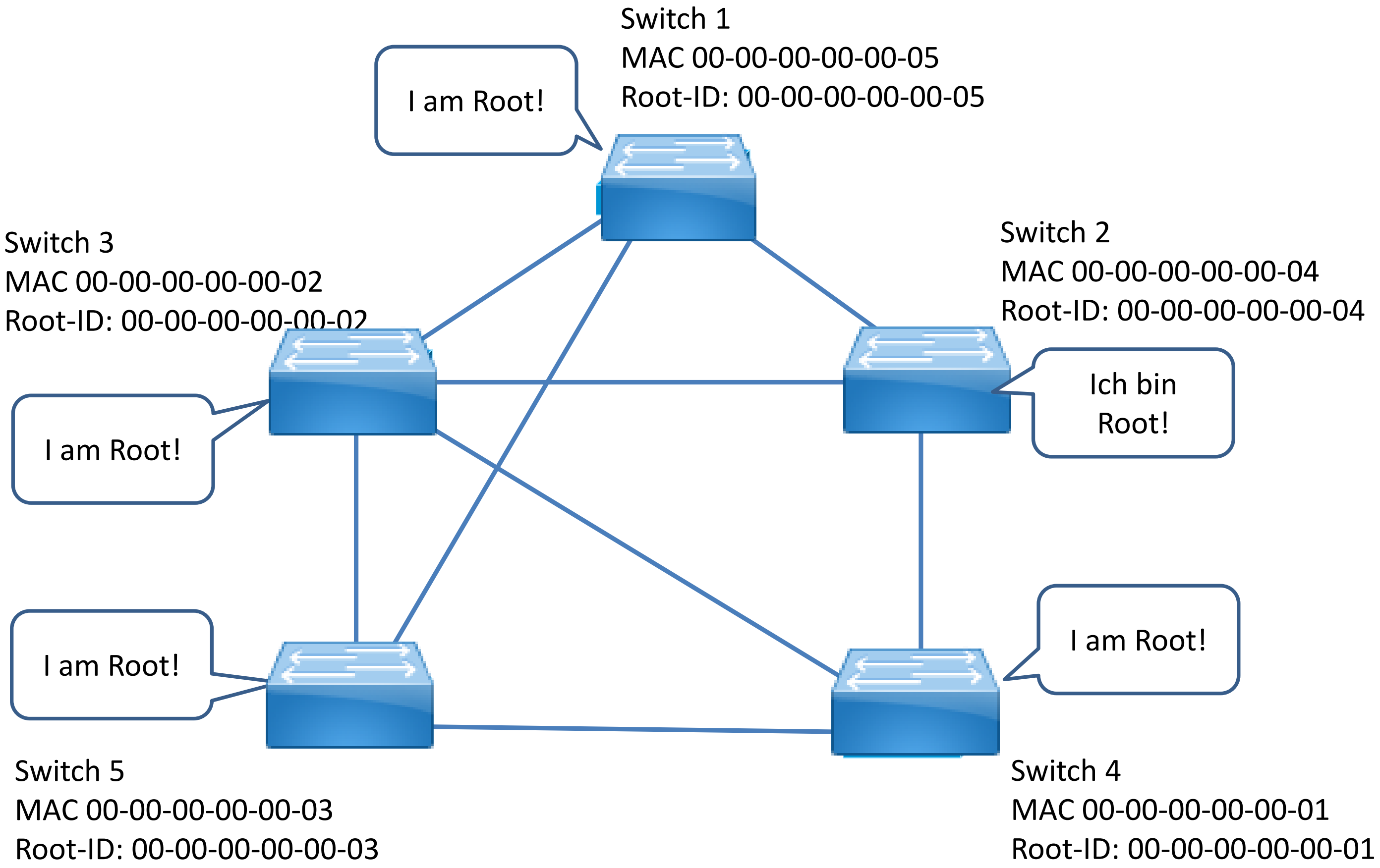
LAYER 2 – SPANNING TREE PROTOCOL

- Switch Configuration set
- All switches have same priority
- All lines are identical 100 MBit/s



LAYER 2 – SPANNING TREE PROTOCOL

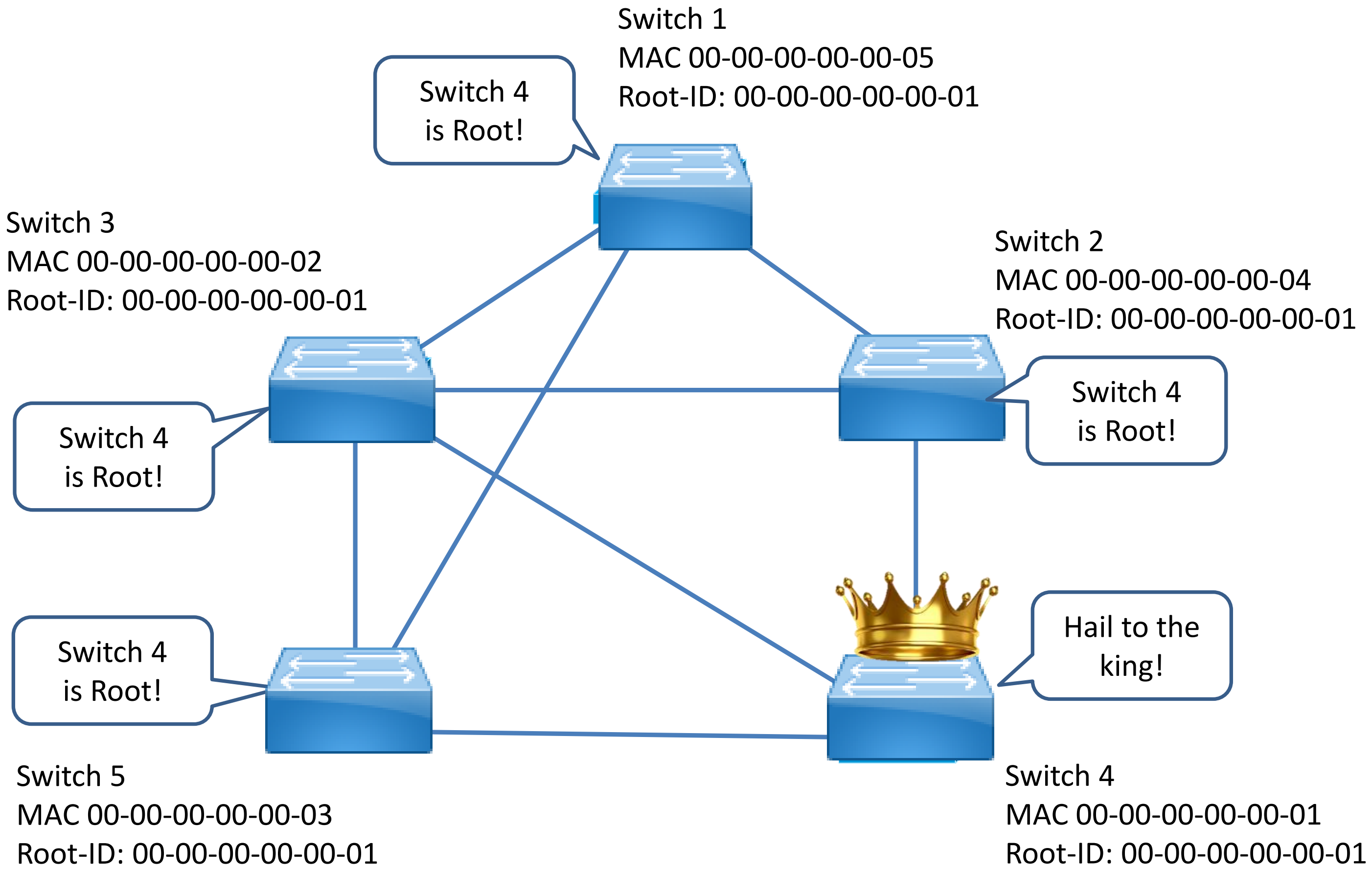
- Switch Configuration set
- Switches set themselves to root



GEM MINE

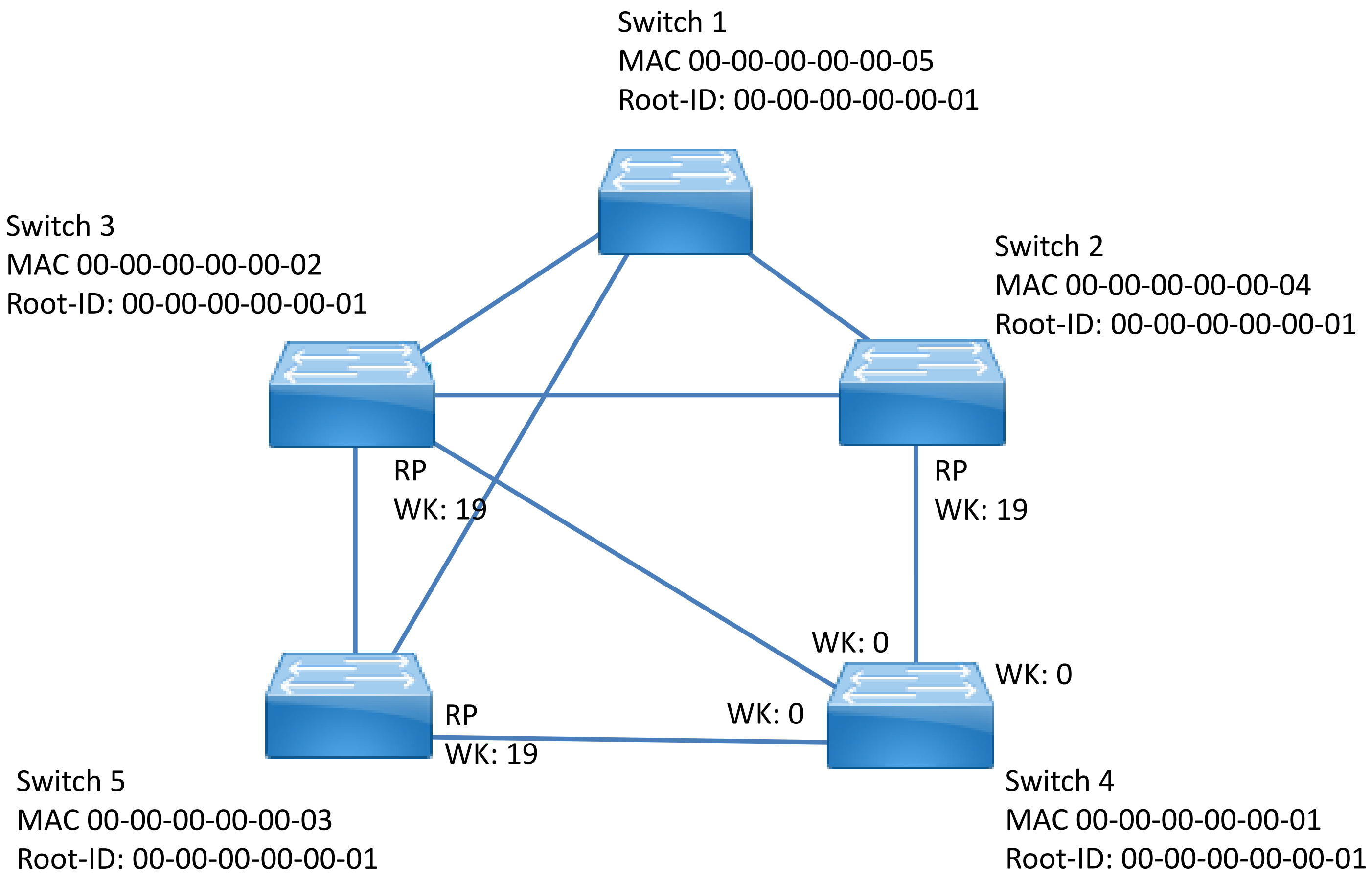
LAYER 2 – SPANNING TREE PROTOCOL

- Switch Configuration set
- Switches set themselves to root
- Switches send BDPU
- If BDPU of switch 4 arrives,
  all other switches reject the delusion
  being root



LAYER 2 – SPANNING TREE PROTOCOL

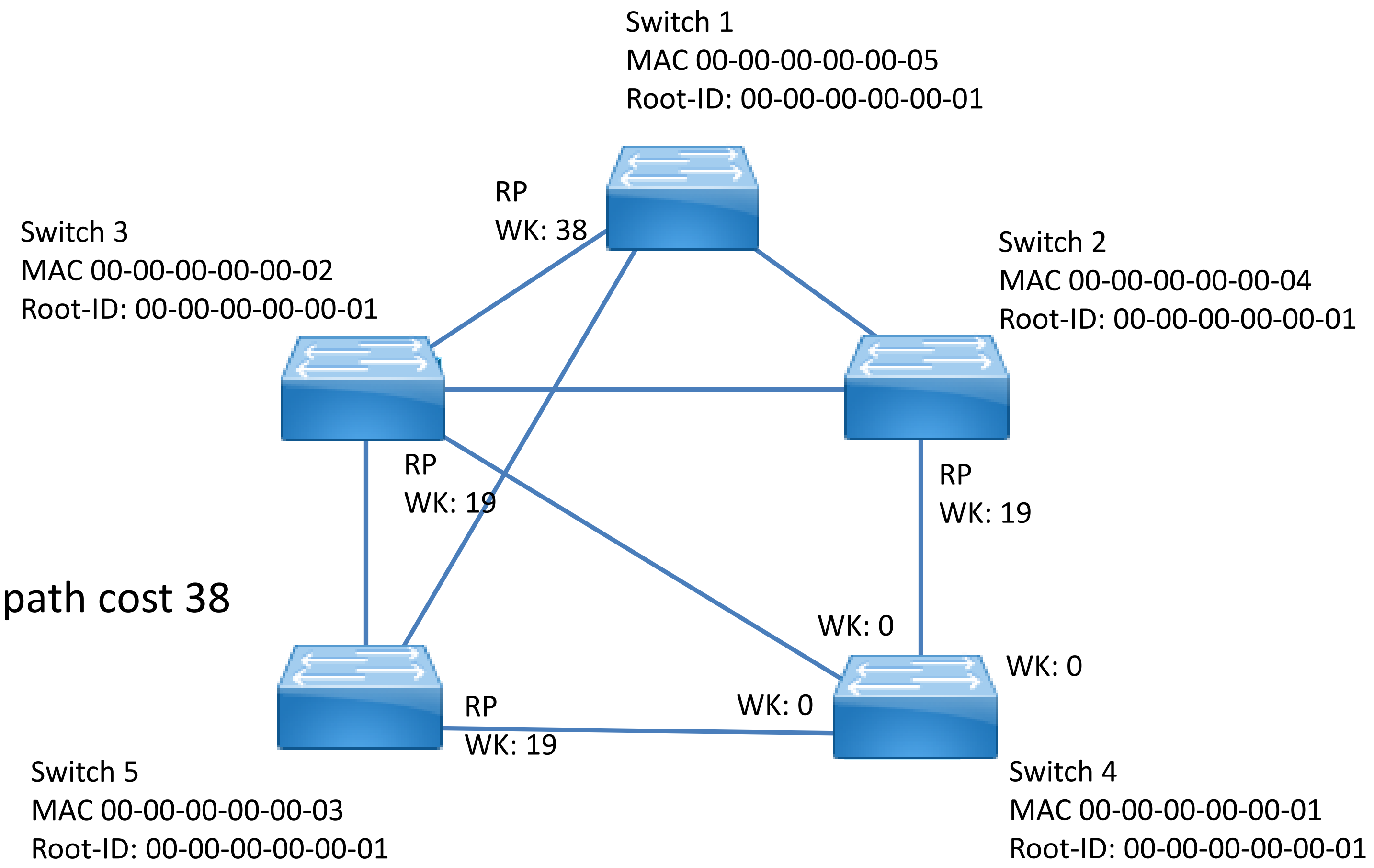
- Determine Root Ports – every Port connected with root is a Root Port (RP)
- Root Port sends BDPU with cost 0
- Switch 5, 2, 3 add costs for a 100 Mbit/S line (19) and save this value



ISO OSI LAYERS

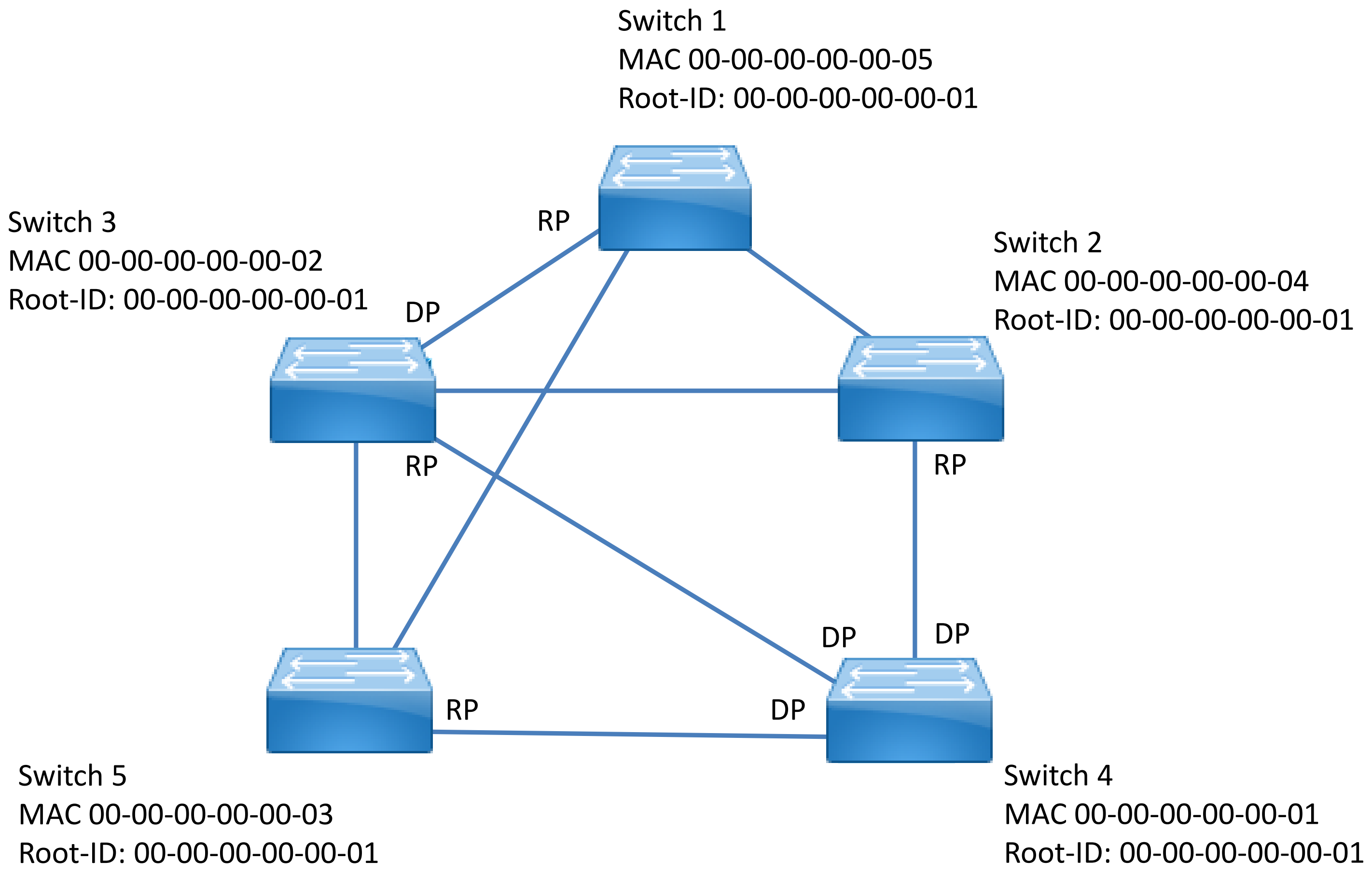
LAYER 2 – SPANNING TREE PROTOCOL

- Which Port of switch 1 becomes RP?
- The port through which root can be reached with the least cost
- Switch 5, 2, 3 modify their BDPU just obtained.
- The Message Age is increased and the cost of the line to Switch 1 is added
- Then Switch 5, 2, 3 send the BDPU on
- For all three ports, switch 1 receives the path cost 38
- So no decision can be made
- Therefore, the switch with the lowest priority is selected.
- This is switch 3



LAYER 2 – SPANNING TREE PROTOCOL

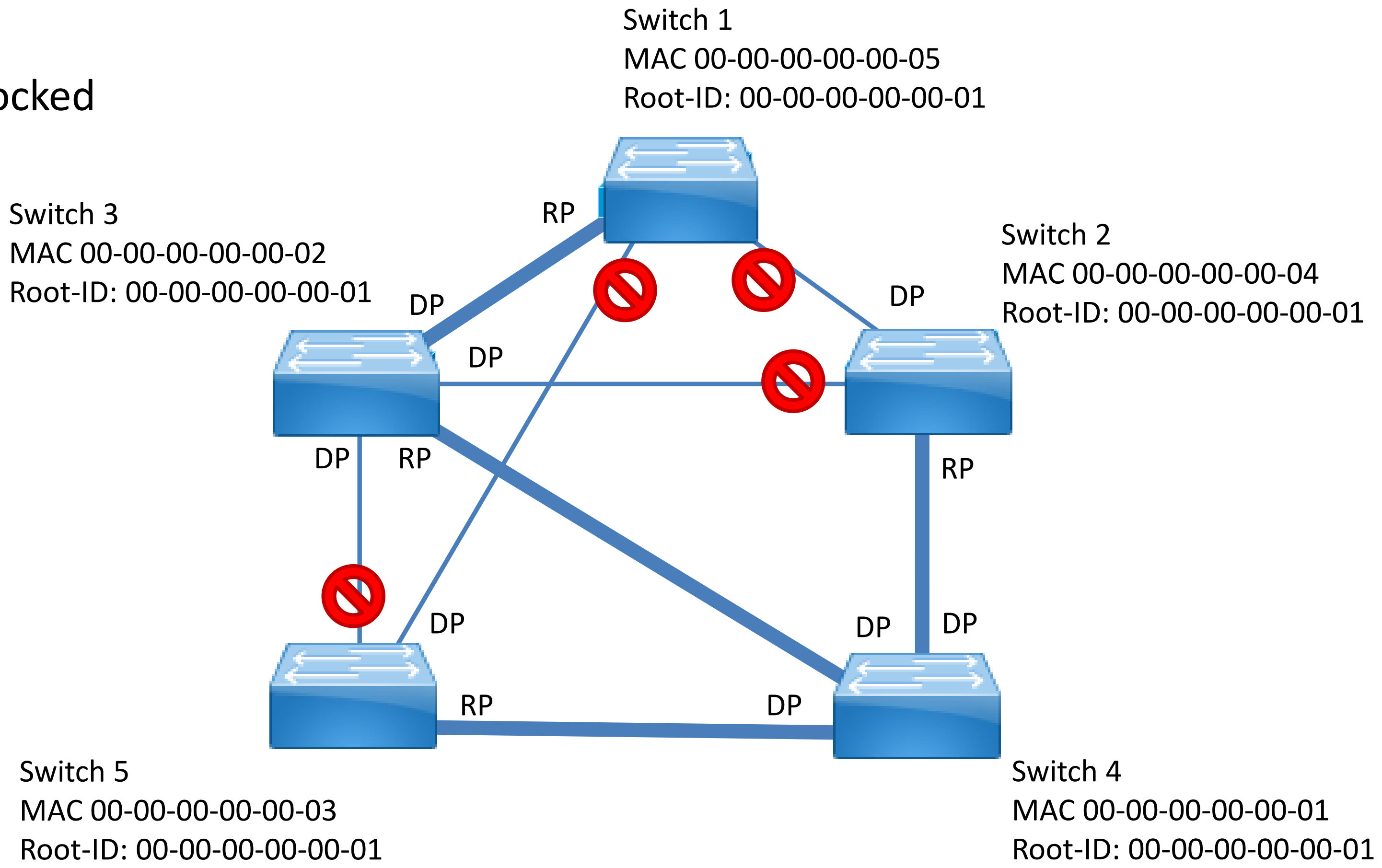
- Now each switch gets a designated port
- Simple: on the other side of the line is the root port



GEM MINE

LAYER 2 – SPANNING TREE PROTOCOL

- All other ports now get designated or blocked
- Which part of the line gets designated?
  - Search for the port with lower costs
  - If costs are identical, take the lower switch ID
  - If this also is identical, take the lower port ID
- Link 3 – 5:
  Switch 3 has smaller MAC, thus setting DP on switch 3 side
- Link 2 – 3:
  Same as above
- Switch 1: has the highest ID
  Block ports



ISO OSI LAYERS

GEM MINE

LAYER 3 – IP ADDRESSES

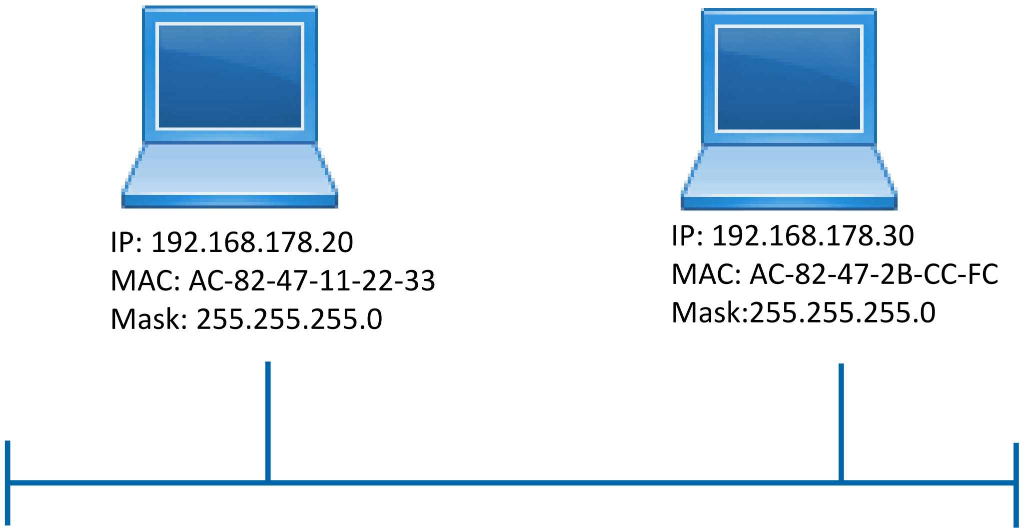
- Communication via IP
  - Why can I ping google.de / google.com?
  - Why can I not ping my neighbor‘s devices?
- Standard Gateway – Why and what for?
- Network segmentation
- Subnetting

ISO OSI LAYERS

LAYER 3 – IP ADDRESSES

- IP address consists of 32 Bit
  - 192.168.178.20
  - 11000000.10101000.10110010.00010100

  - 192.168.178.30
  - 11000000.10101000.10110010.00011110
- There is a mask !?
  - Also consists of 32 Bit
  - Here: 255.255.255.0
  - 11111111.11111111.11111111.00000000
  - Is used to divide IP address into „telephone area code“ – the net and „telephone number“ – the host ID

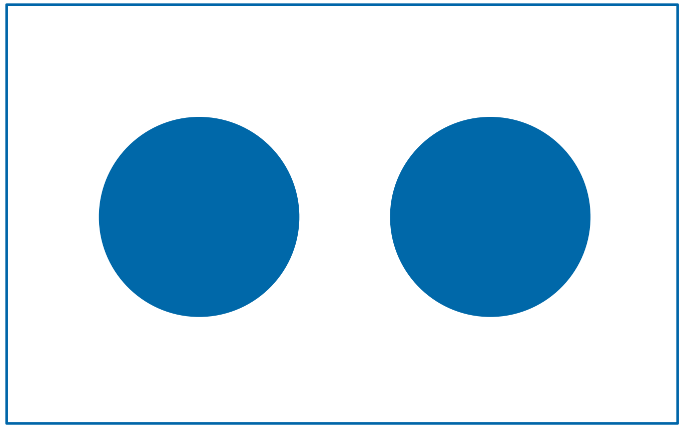


ISO OSI LAYERS

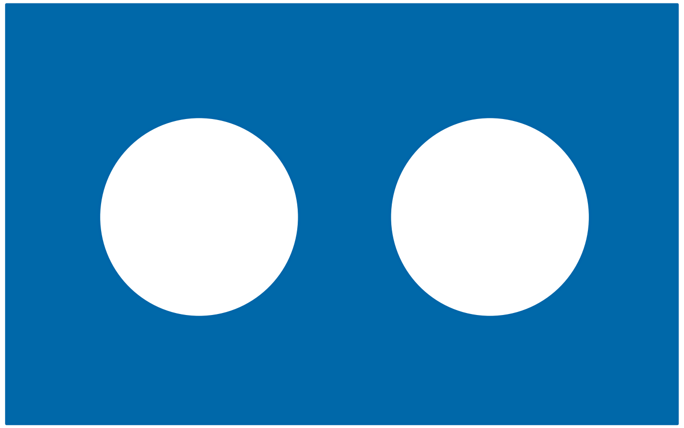
LAYER 3 – HOW A MASK WORKS

1. Define the format (32 BIT)

2. Define what to cut out



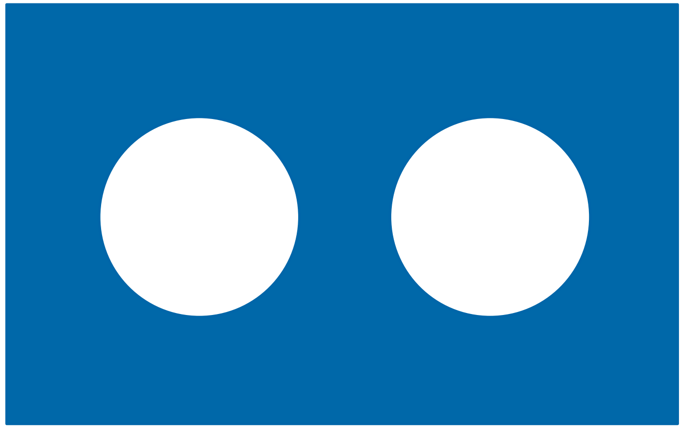
3. Generate the mask



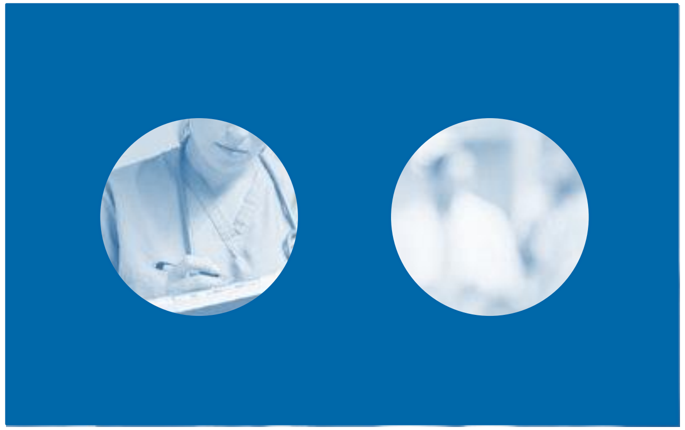
LAYER 3 – HOW A MASK WORKS

1. Take the picture (IP address)

2. Take the mask



3. Cut out irrelevant parts



GEM MINE

LAYER 3 – IP ADDRESSES

- Algorithm for communication
  - Host A wants to connect to Host B
  - Host A finds out which „area“ he is in
  - Host A finds out if Host B is in the same „area“
  - If Host A is in the same „area“ as Host B
    then communicate and send packet to Host B
    else send packet to standard gateway for routing

- Telephone example
  - I am in Berlin, my contact is in Berlin
  - I don‘t have to dial +49-30 but can dial his host number directly → No Routing

  - I am in Berlin, my contact is in NYC
  - I have to dial +1-212 to leave Berlin, leave Germany, enter USA, enter NYC (Manhattan) → Routing

ISO OSI LAYERS

GEM MINE

LAYER 3 – IP ADDRESSES

- Telephone example contd.
  - Humans can compare two phone numbers directly
  - Computers have to get the area code from number A
    - Is this Berlin?
  - Computers have to get the area code from number B
    - Is this Berlin?
    - Please note: even if the one to be called is in NYC, the question is: Is he in Berlin or not
  - Computers then have to compare both area codes to determine if routing is needed

LAYER 3 – IP ADDRESSES

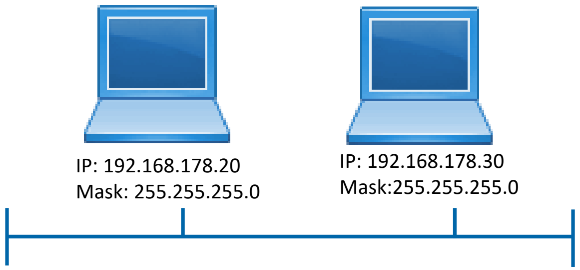
- Getting the area code
  - Host A: 192.168.178.20
  - Host B: 192.168.178.30
  - Use the AND function

A	B	X
0	0	0
0	1	1
1	0	1
1	1	0

Truth Table XOR

A	B	X
0	0	0
0	1	0
1	0	0
1	1	1

Truth Table AND



area code / Host ID

IP A	11000000.10101000.10110010.00010100
MASK A	11111111.11111111.11111111.00000000
IP-A(M)	11000000.10101000.10110010.00000000

IP B	11000000.10101000.10110010.00011110
MASK A	11111111.11111111.11111111.00000000
IP-B(M)	11000000.10101000.10110010.00000000

ISO OSI LAYERS

LAYER 3 – IP ADDRESSES

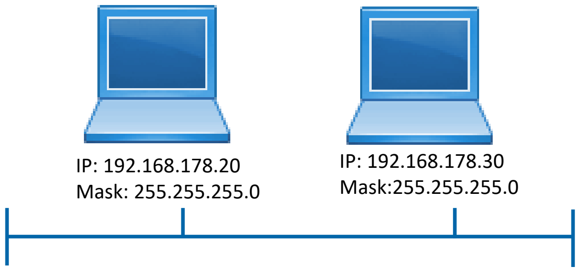
- Comparing the area code
  - Host A: 192.168.178.0
  - Host B: 192.168.178.0
  - Use the XOR function

A	B	X
0	0	0
0	1	1
1	0	1
1	1	0

Truth Table XOR

A	B	X
0	0	0
0	1	0
1	0	0
1	1	1

Truth Table AND



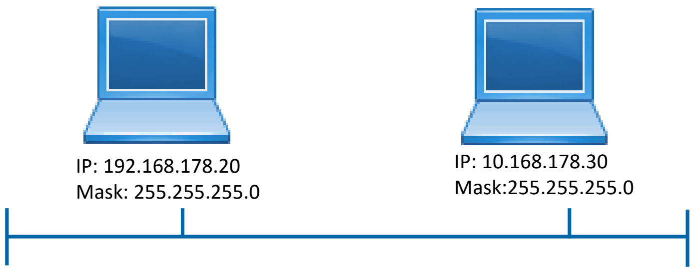
IP-A(M) 11000000.10101000.10110010.00000000
IP-B(M) 11000000.10101000.10110010.00000000

XOR 00000000.00000000.00000000.00000000

ISO OSI LAYERS

LAYER 3 – IP ADDRESSES

- Example
  - Host A: 192.168.178.20
  - Host B: 10.168.178.30



IP A 11000000.10101000.10110010.00010100
MASK A 11111111.11111111.11111111.00000000

IP-A(M) 11000000.10101000.10110010.00000000

IP B 00001010.10101000.10110010.00011110
MASK A 11111111.11111111.11111111.00000000

IP-B(M) 00001010.10101000.10110010.00000000

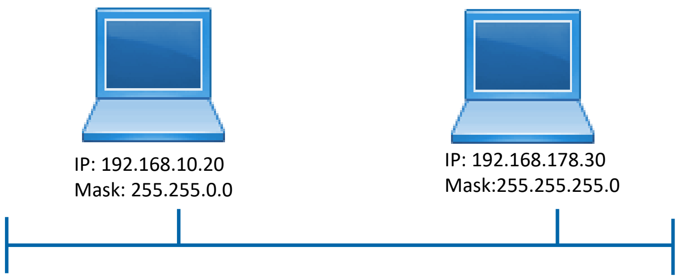
IP-A(M) 11000000.10101000.10110010.00000000
IP-B(M) 00001010.10101000.10110010.00000000

XOR 11001010.00000000.00000000.00000000

ISO OSI LAYERS

GEM MINE

LAYER 3 – IP ADDRESSES



- Consider this example – Part I
  - Host A: 192.168.10.20 / 16
  - Host B: 192.168.178.30 / 24

IP A	11000000.10101000.00001010.00010100
MASK A	11111111.11111111.00000000.00000000
IP-A(M)	11000000.10101000.00000000.00000000

IP B	11000000.10101000.10110010.00011110
MASK A	11111111.11111111.00000000.00000000
IP-B(M)	11000000.10101000.00000000.00000000

Host A
can see
Host B

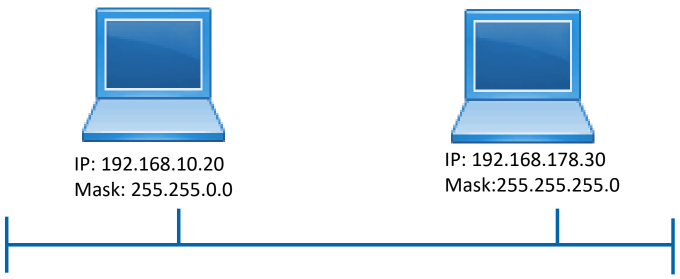
IP-A(M)	11000000.10101000.00000000.00000000
IP-B(M)	11000000.10101000.00000000.00000000
XOR	00000000.00000000.00000000.00000000

✓

ISO OSI LAYERS

GEM MINE

LAYER 3 – IP ADDRESSES



- Consider this example – Part II
  - Host A: 192.168.10.20 / 16
  - Host B: 192.168.178.30 / 24

IP A	11000000.10101000.00001010.00010100
MASK B	11111111.11111111.11111111.00000000
IP-A(M)	11000000.10101000.00001010.00000000

IP B	11000000.10101000.10110010.00011110
MASK B	11111111.11111111.11111111.00000000
IP-B(M)	11000000.10101000.10110010.00000000

IP-A(M)	11000000.10101000.00001010.00000000
IP-B(M)	11000000.10101000.10110010.00000000
XOR	00000000.00000000.10111000.00000000

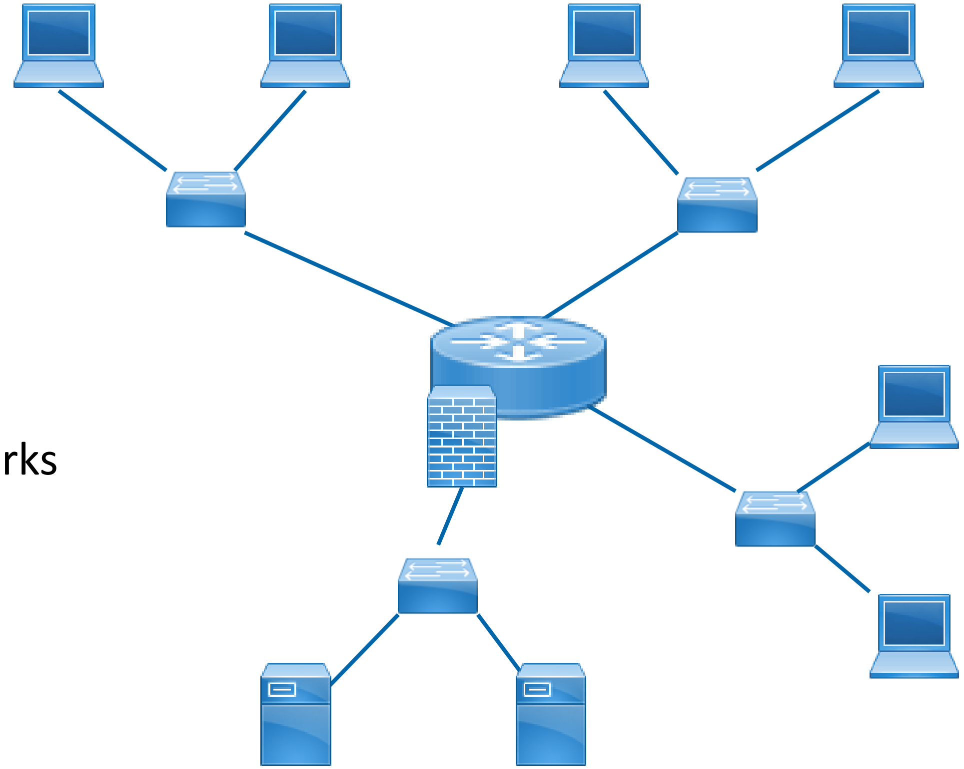
Host B
can not see
Host A

ISO OSI LAYERS

GEM MINE

LAYER 3 – STANDARD GATEWAY

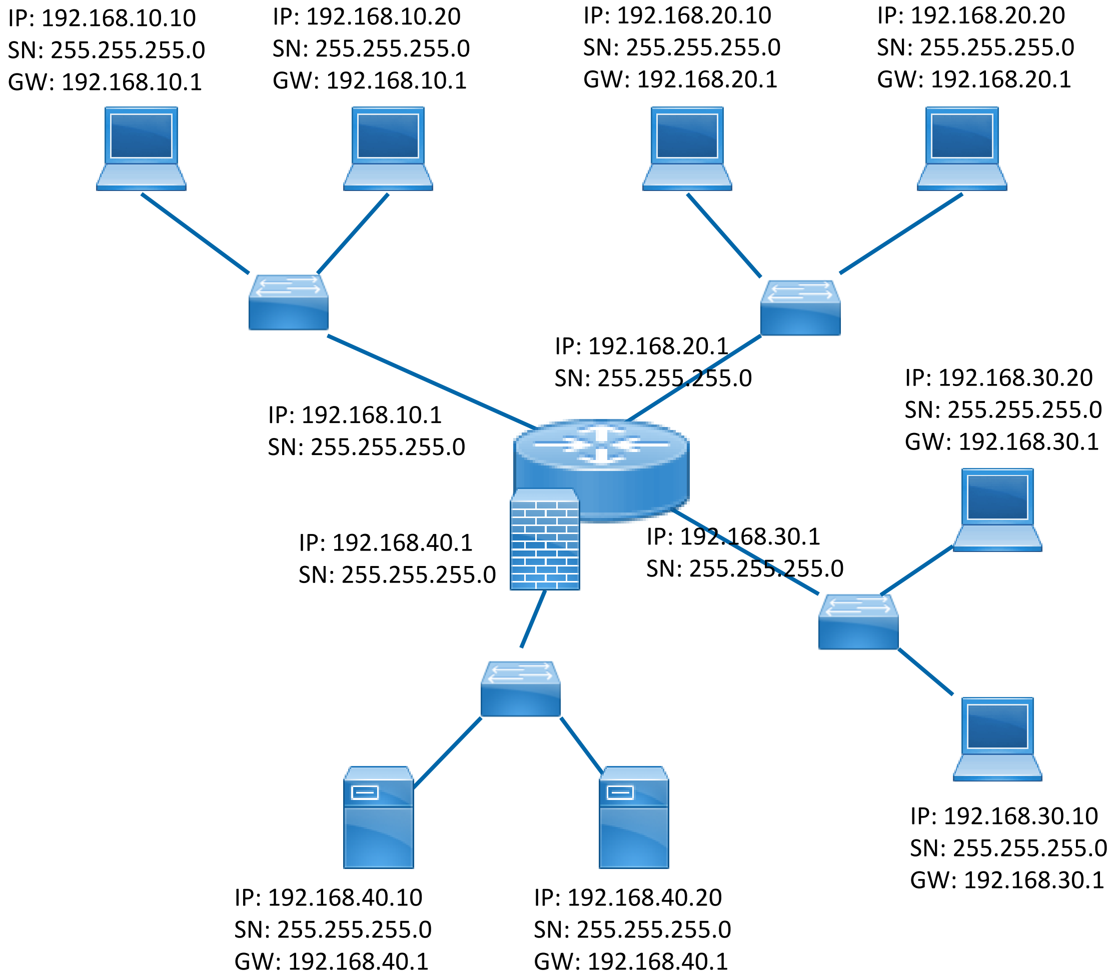
- If Host A cannot reach Host B it will send packets to the standard gateway
- Subnetting used for network segmentation
  - Restrict access to server / devices
  - Shrink collision and broadcast domain
- Router / Standard gateway used to connect segmented networks
  - Allow rules for communication
  - Firewalls



LAYER 3 – ROUTING

- Host Network Configuration
- Router Network Configuration
- Routing Tables

- In this configuration, we just have to wait
  - Router has 4 NICs
  - All NICs are the same device
  - Internal routing done automatically

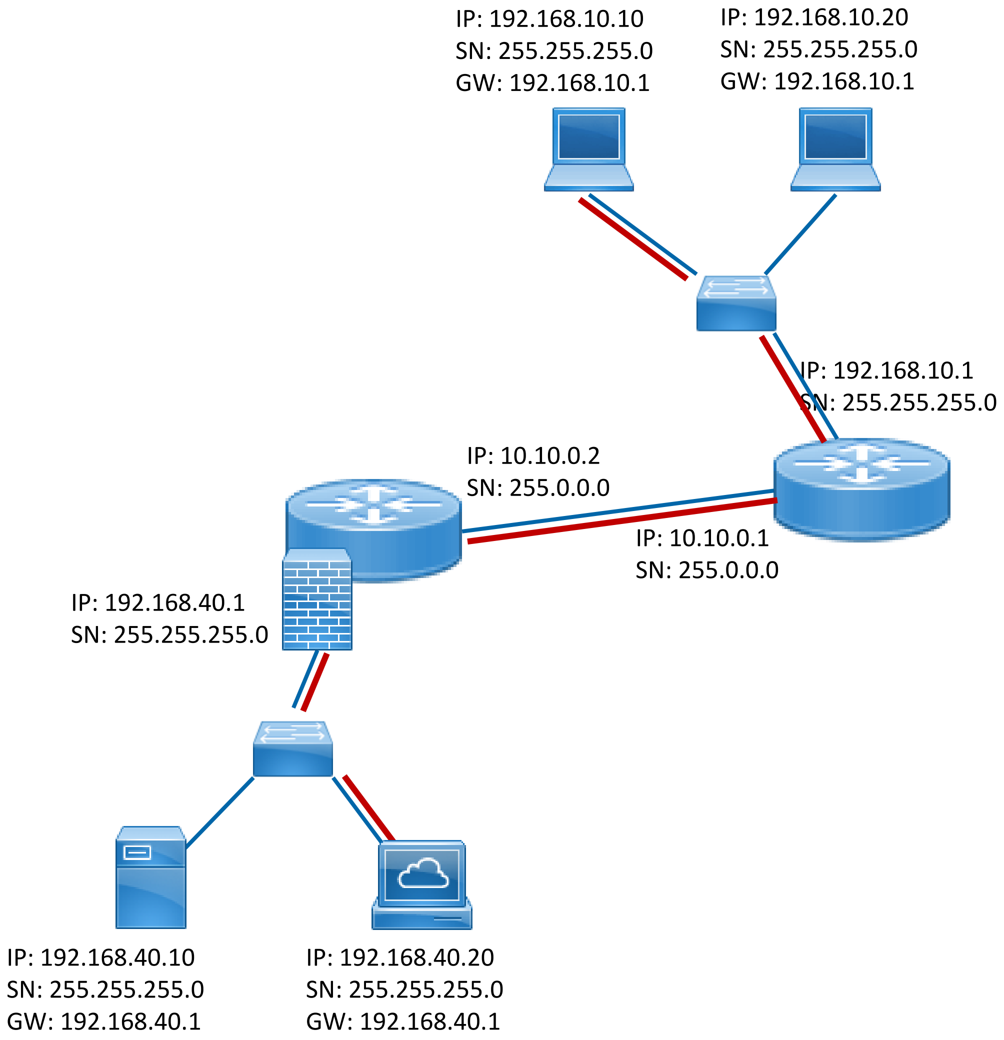


ISO OSI LAYERS

GEM MINE

LAYER 3 – ROUTING

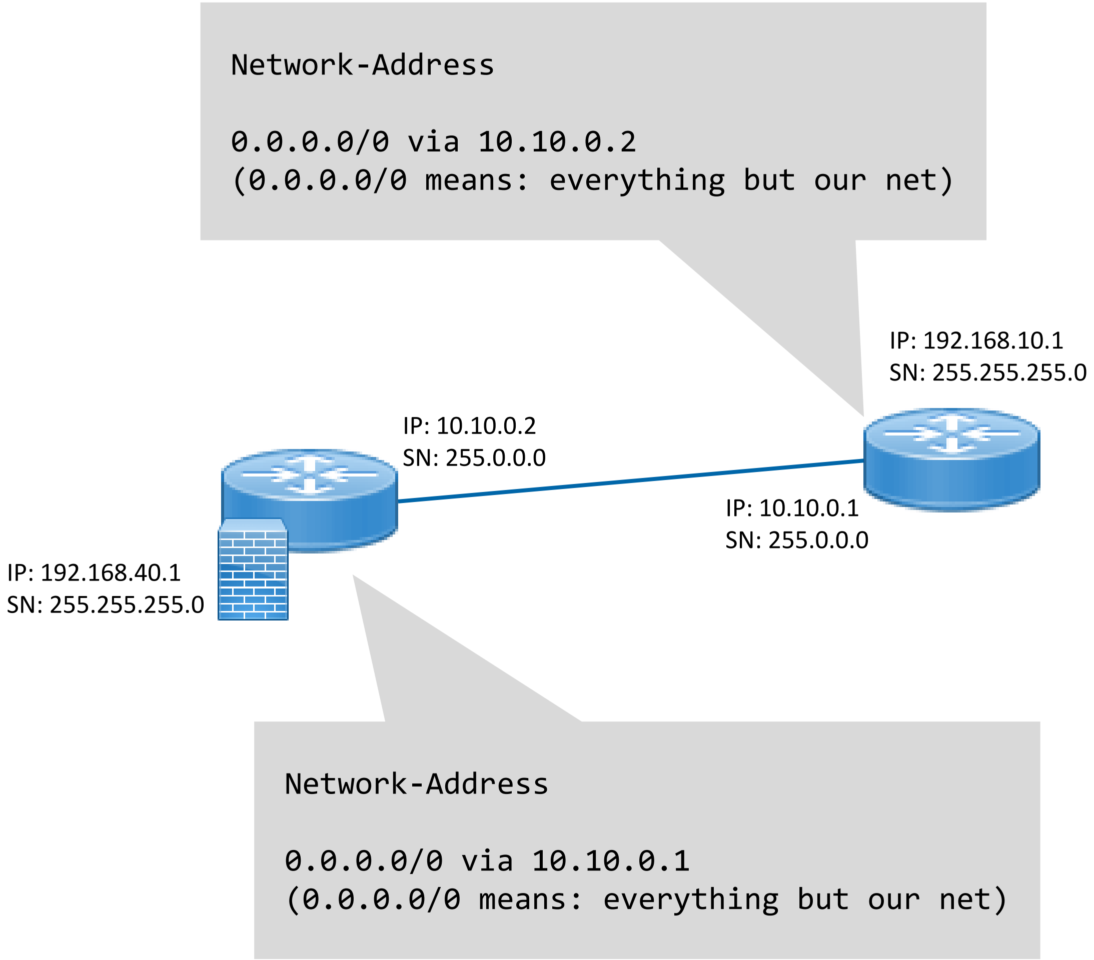
- Now we have two router
- 192.168.10.10 wants to get a HTML page from 192.168.40.20
    - He sends the request to his gateway (the right router)
    - The router has to look up where to send the packet (left router)
    - The router sends the packet to the left router
    - The left router forwards the request to the web server



ISO OSI LAYERS

LAYER 3 – ROUTING

- Rules for right router
  - Send everything what is not our net to 10.10.0.2
  - Command: „ip route 0.0.0.0 0.0.0.0 10.10.0.2“
- Rules for left router
  - Send everything what is not our net to 10.10.0.1
  - Command: „ip route 0.0.0.0 0.0.0.0 10.10.0.1“
- To show the rules set
  - Command: „show ip route“

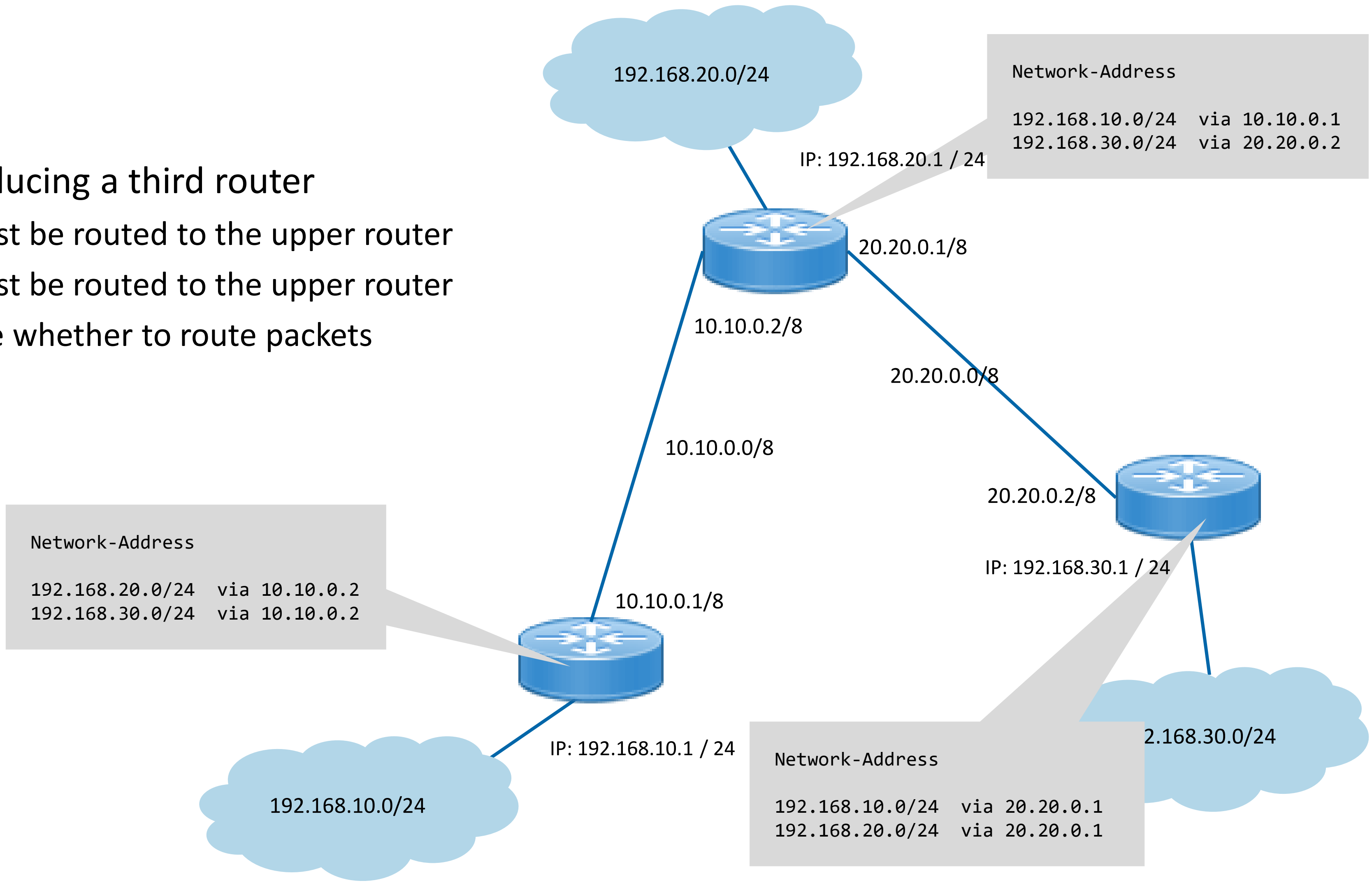


ISO OSI LAYERS

GEM MINE

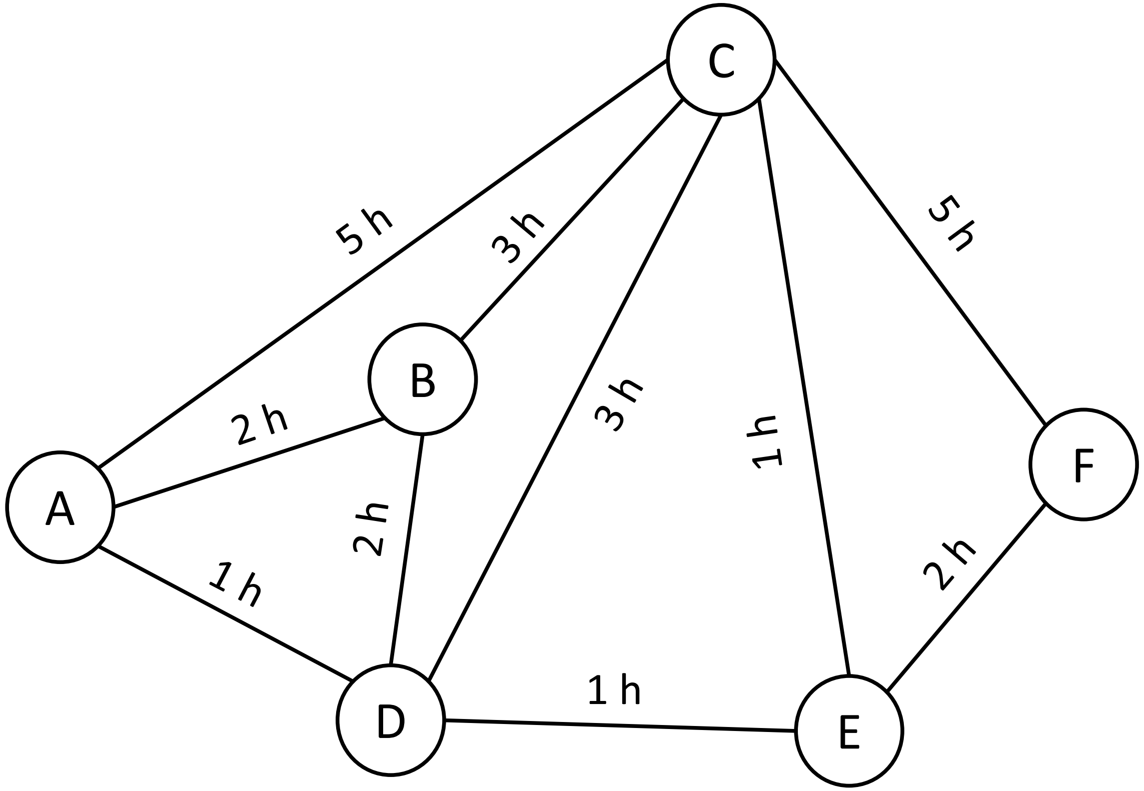
LAYER 3 – ROUTING

- Let‘s complicate thing by introducing a third router
  - Packets from 192.168.10.0 must be routed to the upper router
  - Packets from 192.168.30.0 must be routed to the upper router
  - The upper router has to decide whether to route packets to the right or to th eleft



LAYER 3 – ROUTING ALGORITHM

- I will demonstrate Dijkstra‘s algorithm
  - Algorithm for finding shortest paths between nodes
  - In this case: nodes are router
  - Algorithm produces a shortest-path tree
  - Greedy
  - OSPF (Open shortest path first)
  - IS-IS (Intermediate System to intermediate system)
  - OLSR (Optimized link state routing)



ISO OSI LAYERS

LAYER 3 – ROUTING ALGORITHM

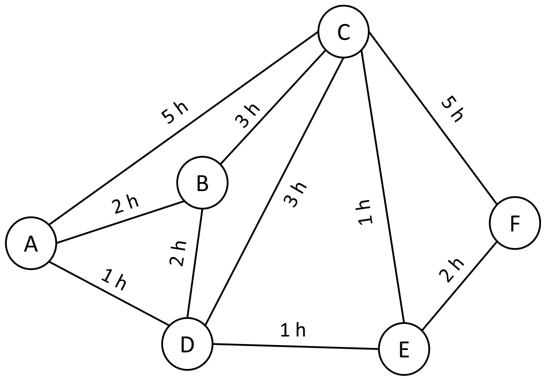
- I will demonstrate Dijkstra‘s algorithm
  1. Initialization of all nodes with distance "infinit", the one of the starting node with 0.
  2. Marking of the distance of the starting node as permanent, all other distances as temporarily.
  3. Setting of starting node as active.
  4. Calculation of the temporary distances of all neighbour nodes of the active node by summing up its distance with the weights of the edges.
  5. If such a calculated distance of a node is smaller as the current one, update the distance and set the current node as antecessor. This step is also called update and is Dijkstra's central idea.
  6. Setting of the node with the minimal temporary distance as active. Mark its distance as permanent.
  7. Repeating of steps 4 to 7 until there aren't any nodes left with a permanent distance, which neighbours still have temporary distances.

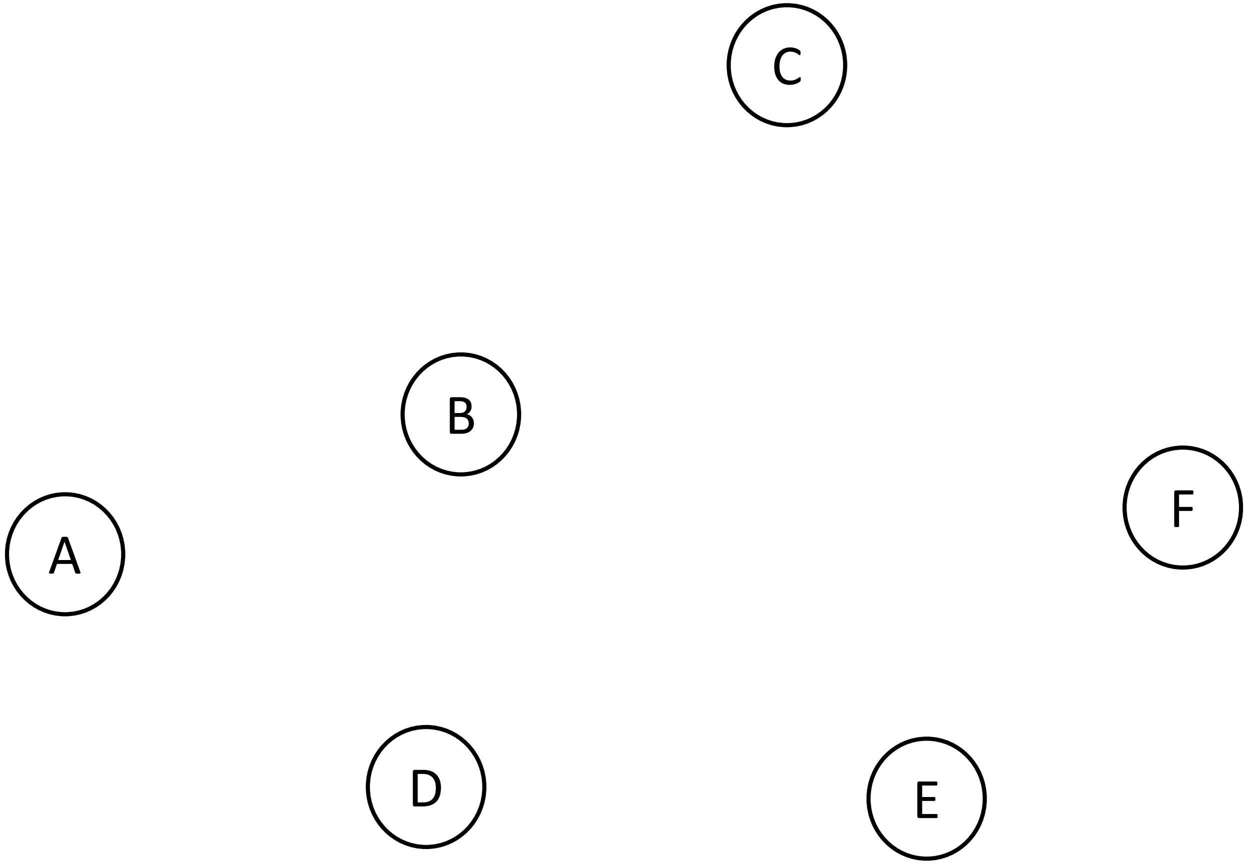
ISO OSI LAYERS

GEM MINE

LAYER 3 – ROUTING ALGORITHM

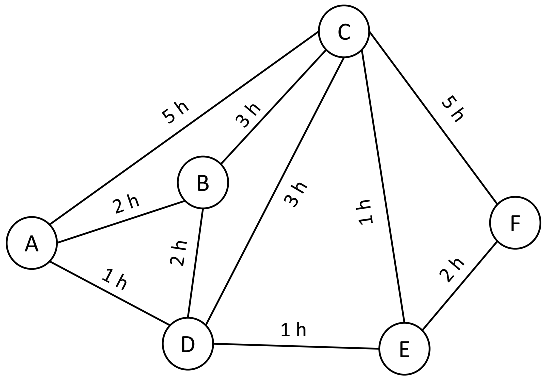
- Mark all nodes as unvisited
- Create a set of all the unvisited nodes called the unvisited set
- Assign to every node a tentative distance value
- Set it to zero for our initial node
- Set it to infinity for all other nodes

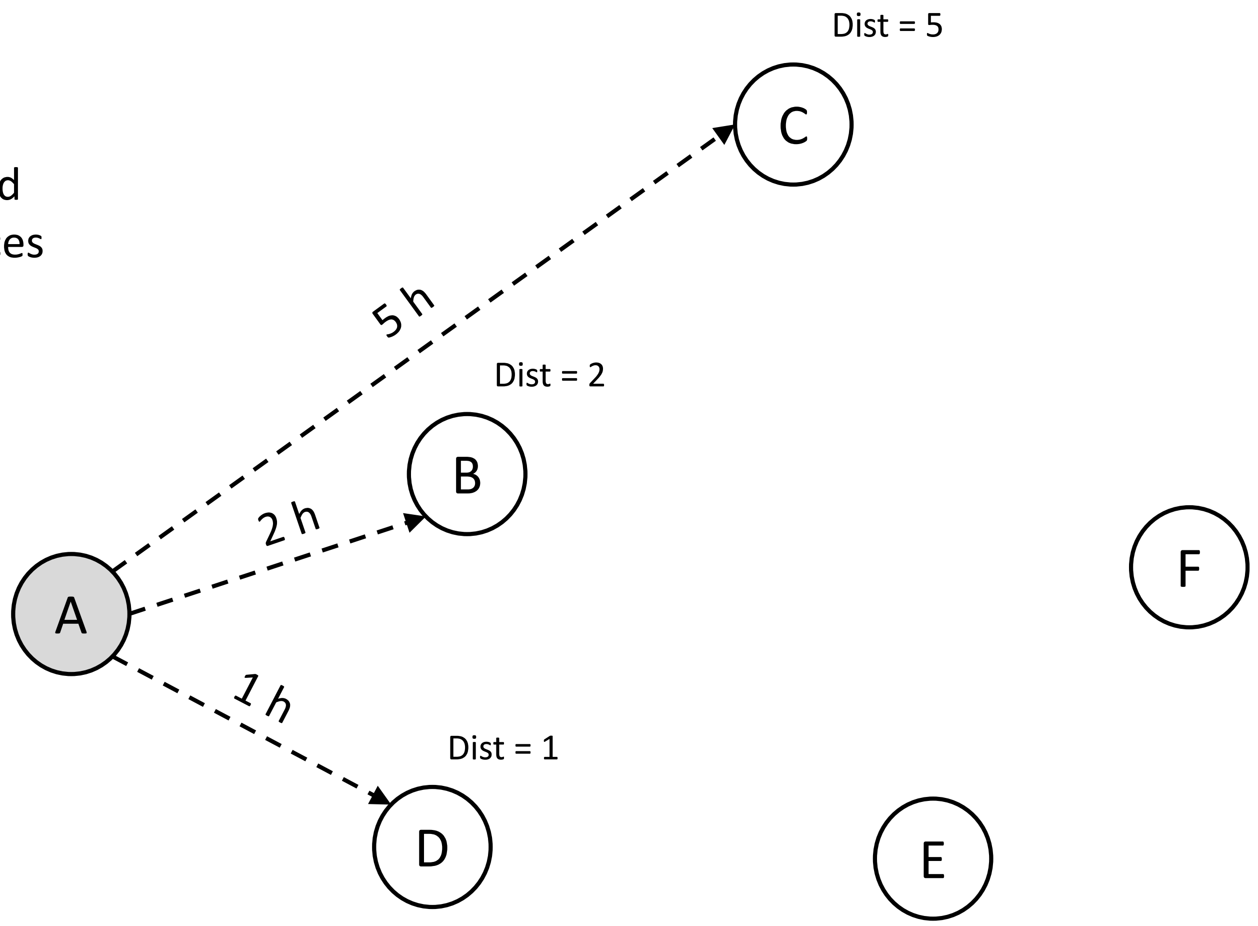




LAYER 3 – ROUTING ALGORITHM

- Set the initial node as current. (A)
- For the current node, consider all of its unvisited neighbours and calculate their tentative distances through the current node
- Compare the newly calculated tentative distance to the current assigned value and assign the smaller one



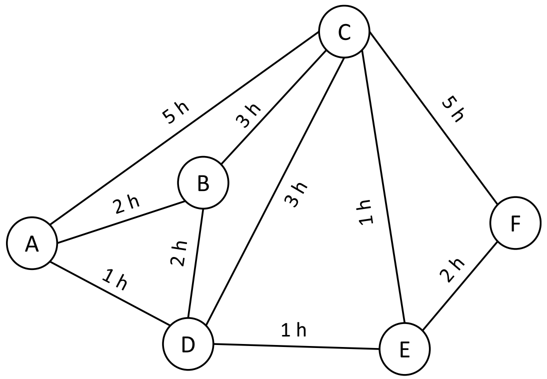


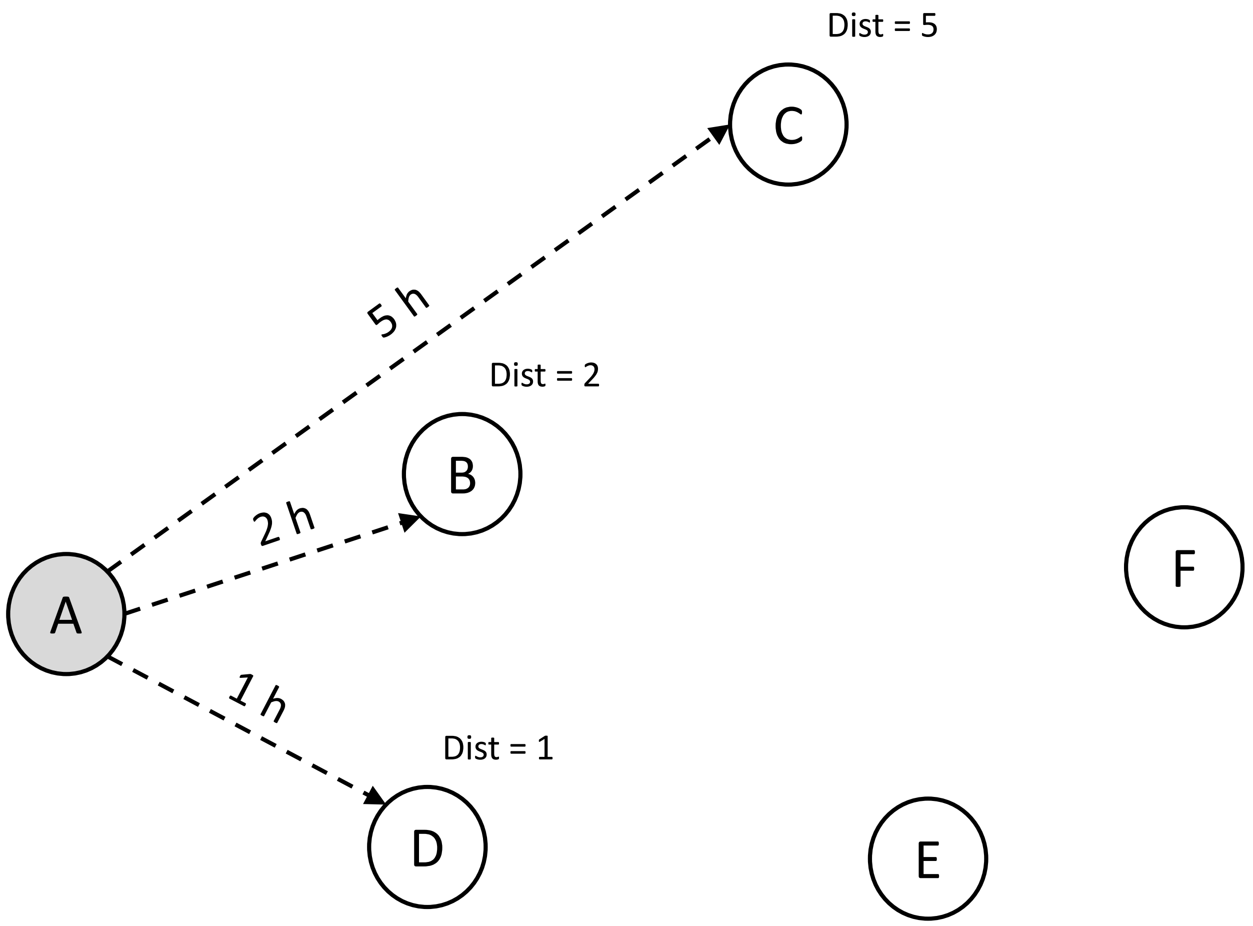
ISO OSI LAYERS

GEM MINE

LAYER 3 – ROUTING ALGORITHM

- When we are done considering all of the unvisited neighbours of the current node, mark the current node as visited and remove it from the unvisited set.
- A visited node will never be checked again

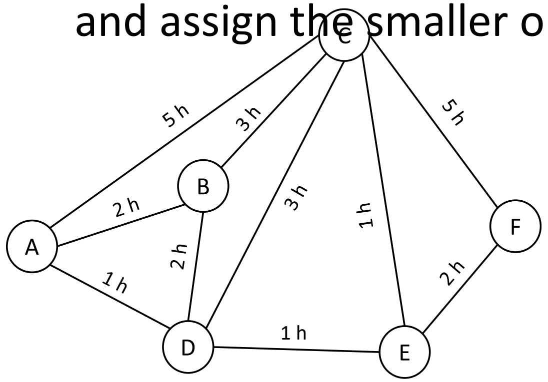


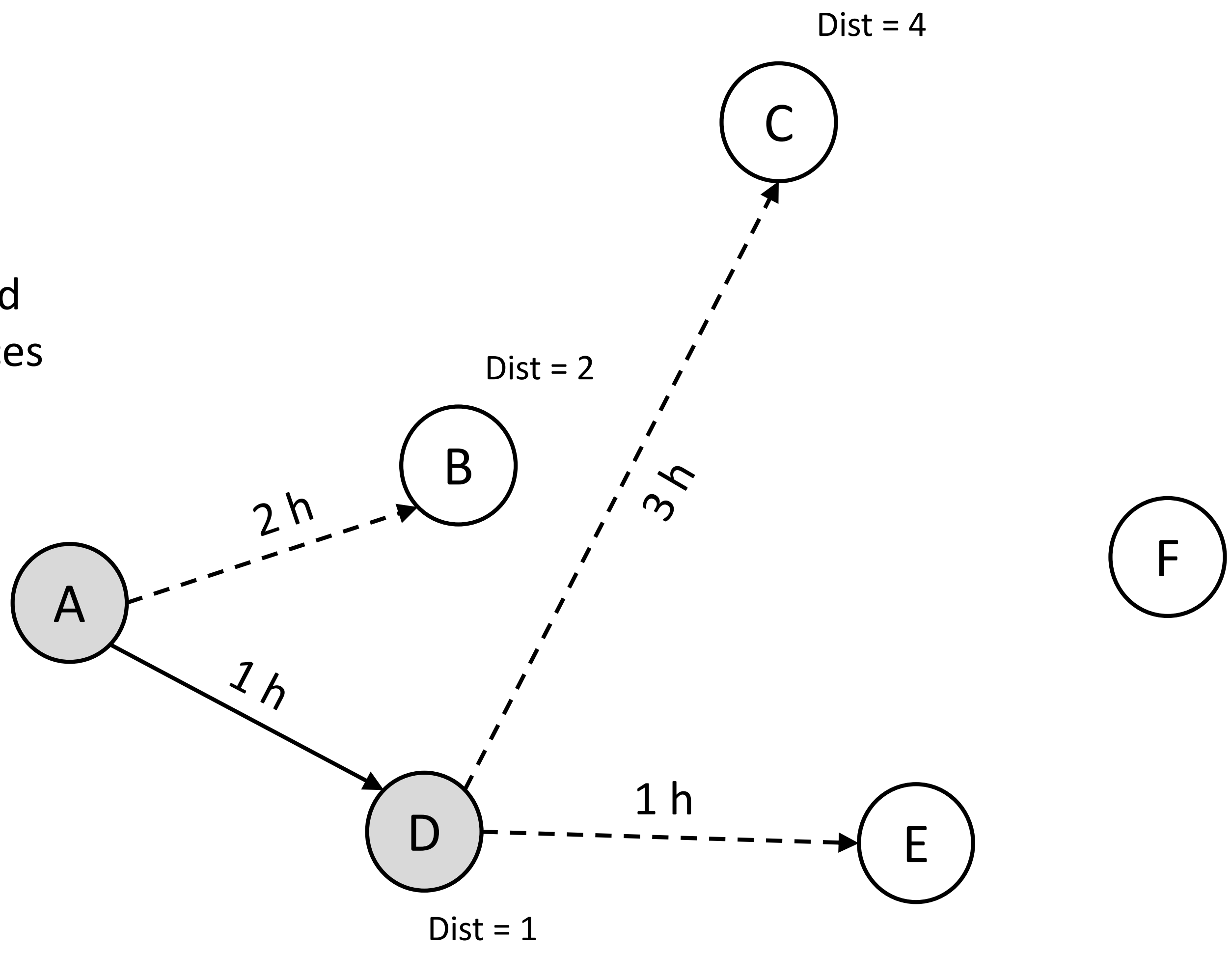


GEM MINE

LAYER 3 – ROUTING ALGORITHM

- select the unvisited node that is marked with the smallest tentative distance (D) set it as the new "current node", and repeat:
- For the current node, consider all of its unvisited neighbours and calculate their tentative distances through the current node
- Compare the newly calculated tentative distance to the current assigned value and assign the smaller one

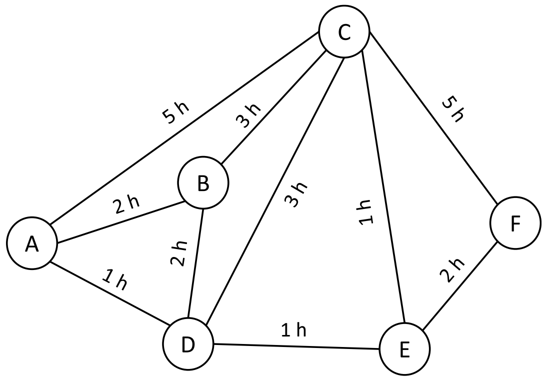


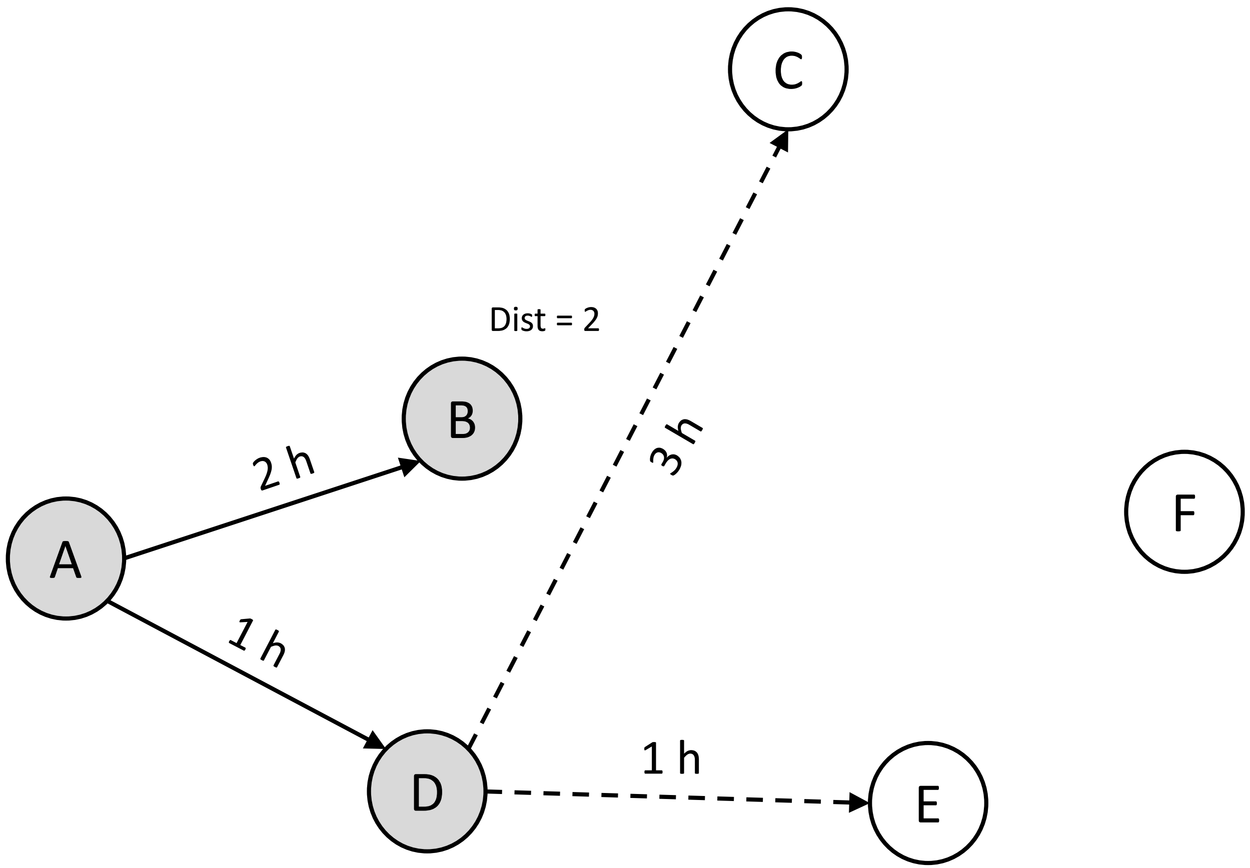


ISO OSI LAYERS

LAYER 3 – ROUTING ALGORITHM

- And again…



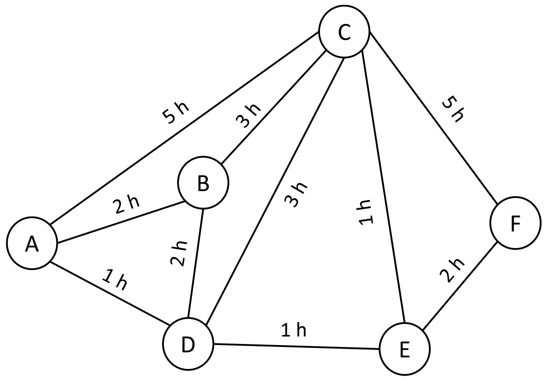


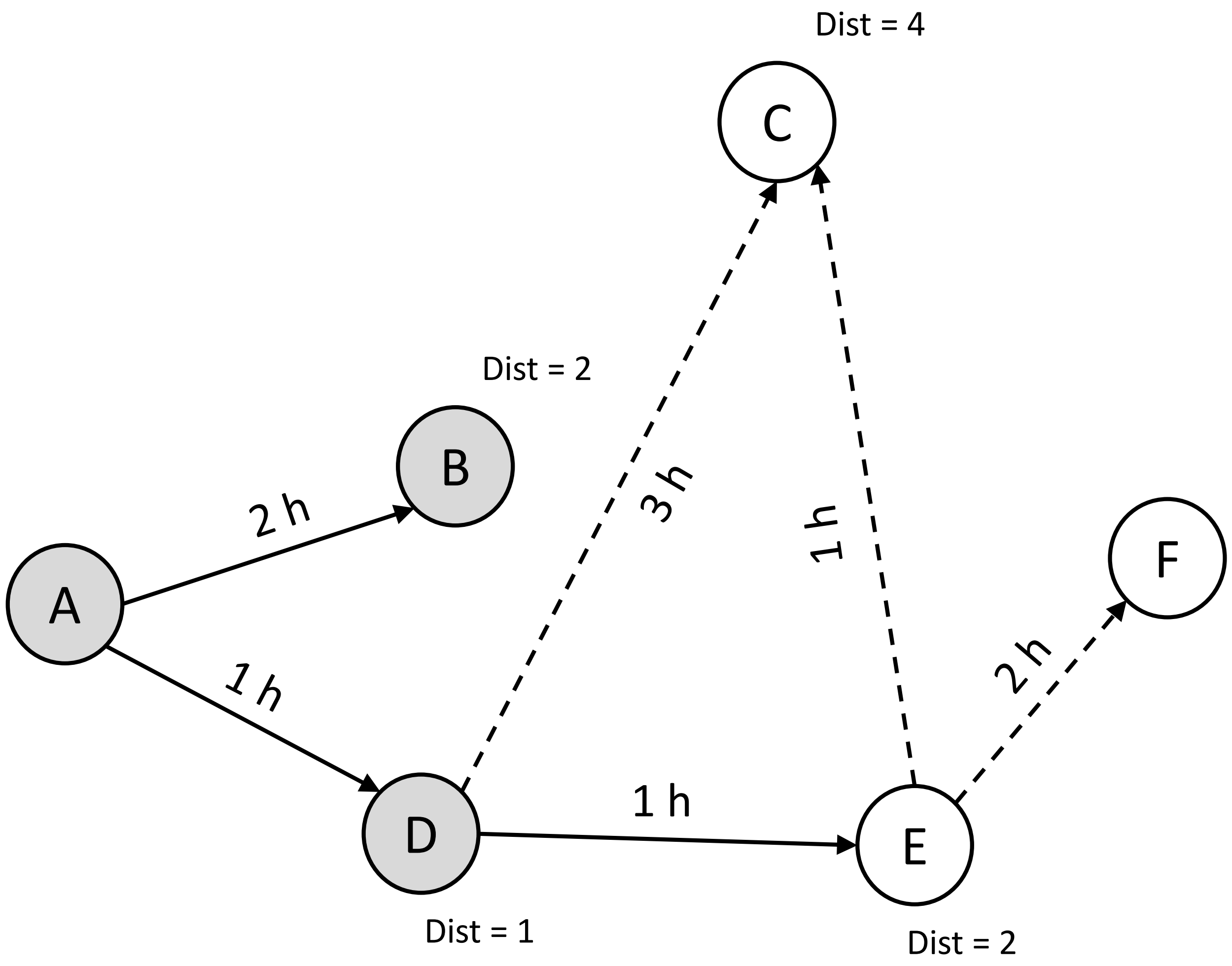
ISO OSI LAYERS

GEMMINE

LAYER 3 – ROUTING ALGORITHM

- And again…

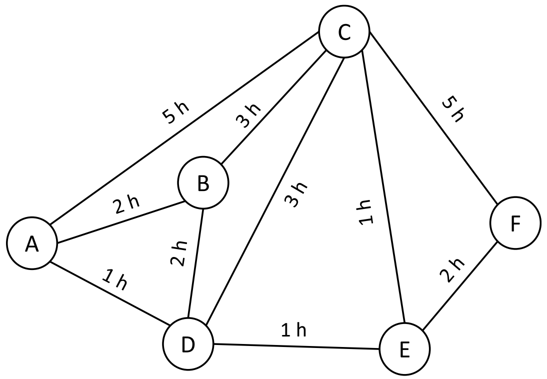


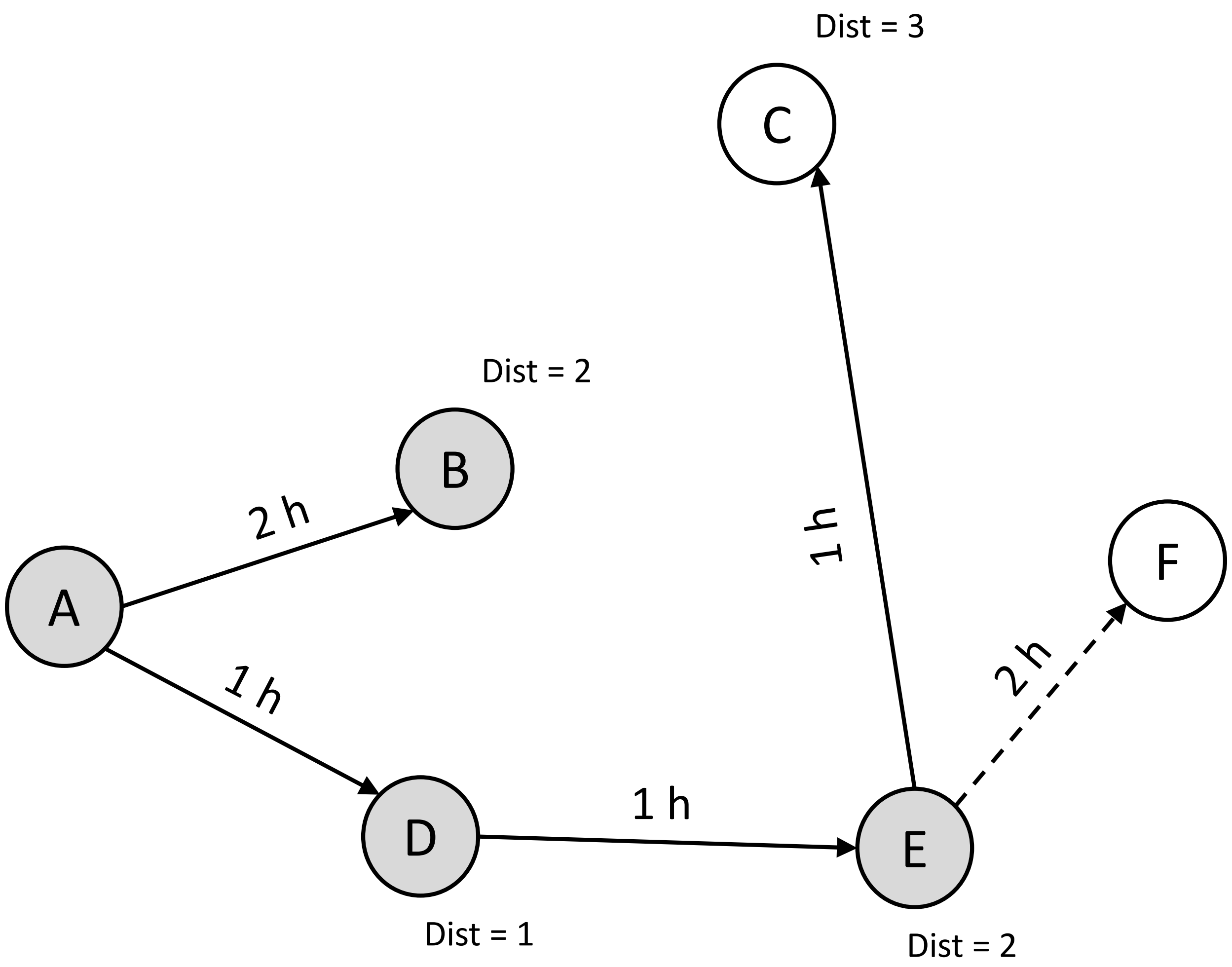


ISO OSI LAYERS

LAYER 3 – ROUTING ALGORITHM

- And again…

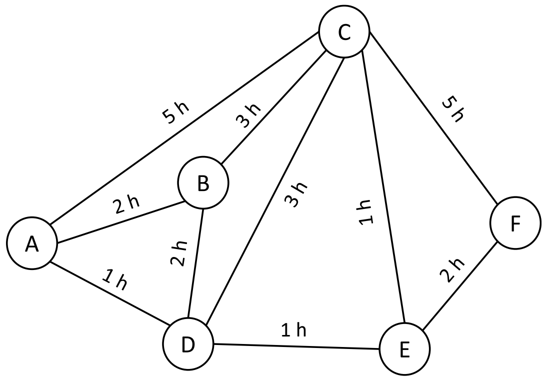


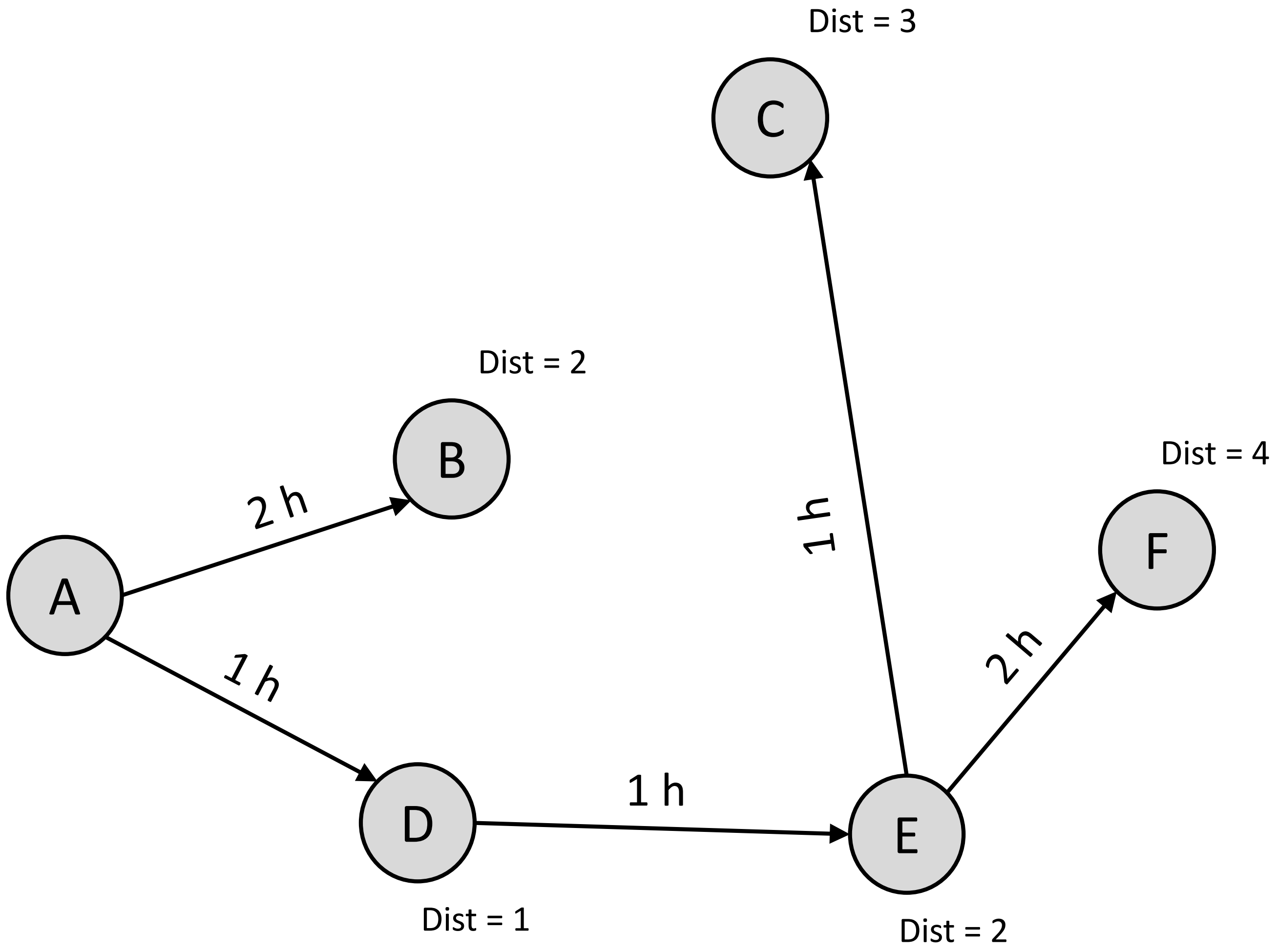


ISO OSI LAYERS

LAYER 3 – ROUTING ALGORITHM

- And again…
- … until we found the minimal spanning tree

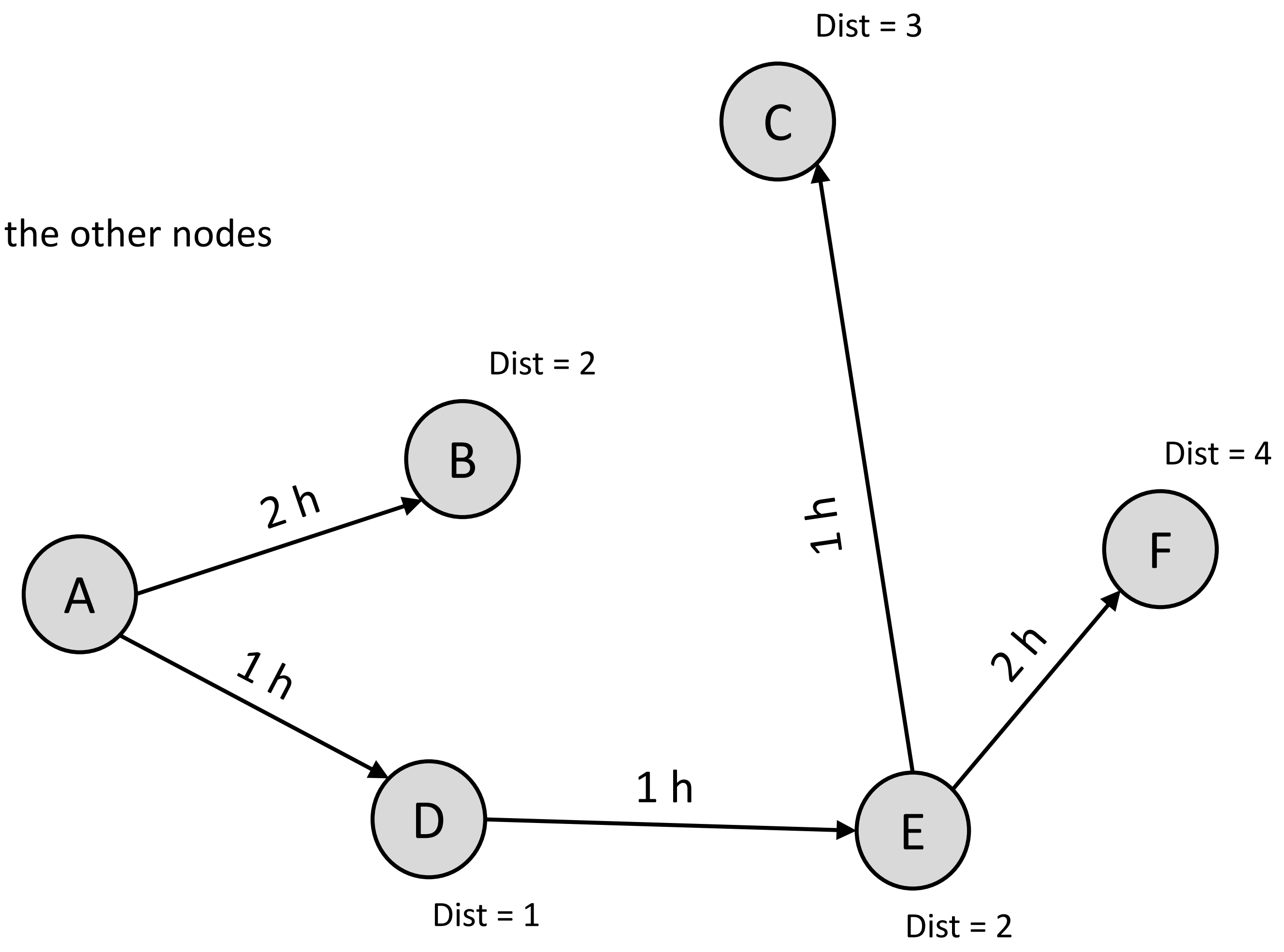




LAYER 3 – ROUTING ALGORITHM

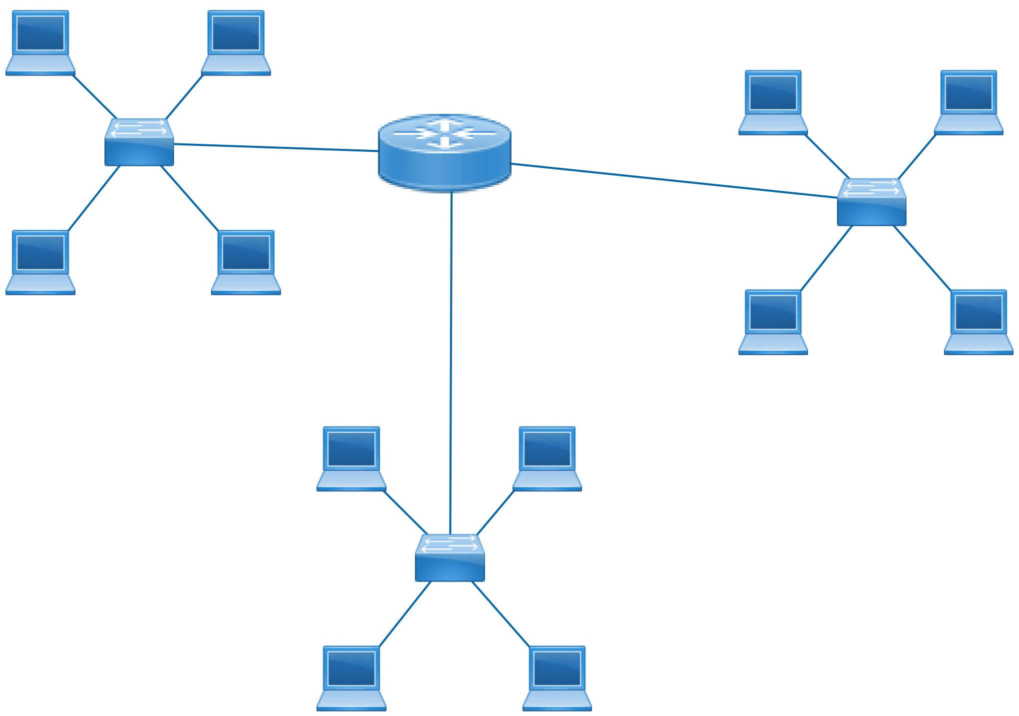
- What does this mean for us now?
  - We found the shortest paths starting from A
  - A built its routing table and knows how to get to the other nodes
  - A has a route to B
  - A has a route to D
  - A routes everything aiming to E to D
  - A routes everything aiming to F to D
  - A routes everything aiming to C to D

  - This can be done by setting the "route to last resort“ (0.0.0.0/0)
  - Or by setting three routes for the three subnets



LAYER 3 – AUTONOMOUS SYSTEMS

- Lets build our company net
  - We buy the IP range of 145.223.0.0/16
  - Routable
  - 65534 hosts
  - We do not have to rely on an ISP
  - That’s what meant by autonomous

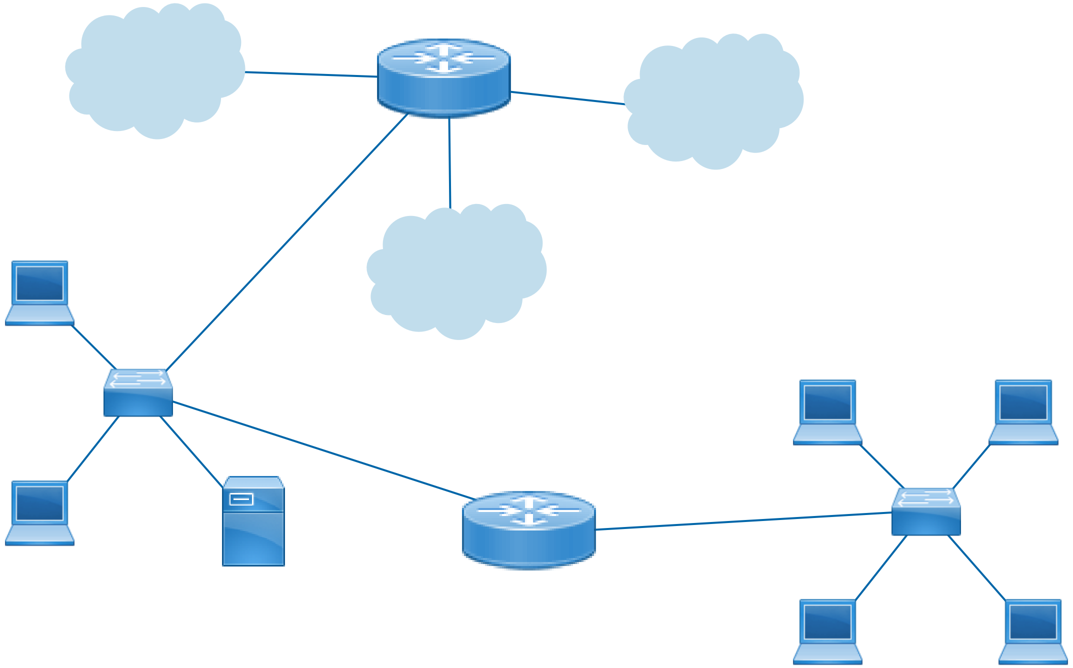


ISO OSI LAYERS

GEM MINE

LAYER 3 – AUTONOMOUS SYSTEMS

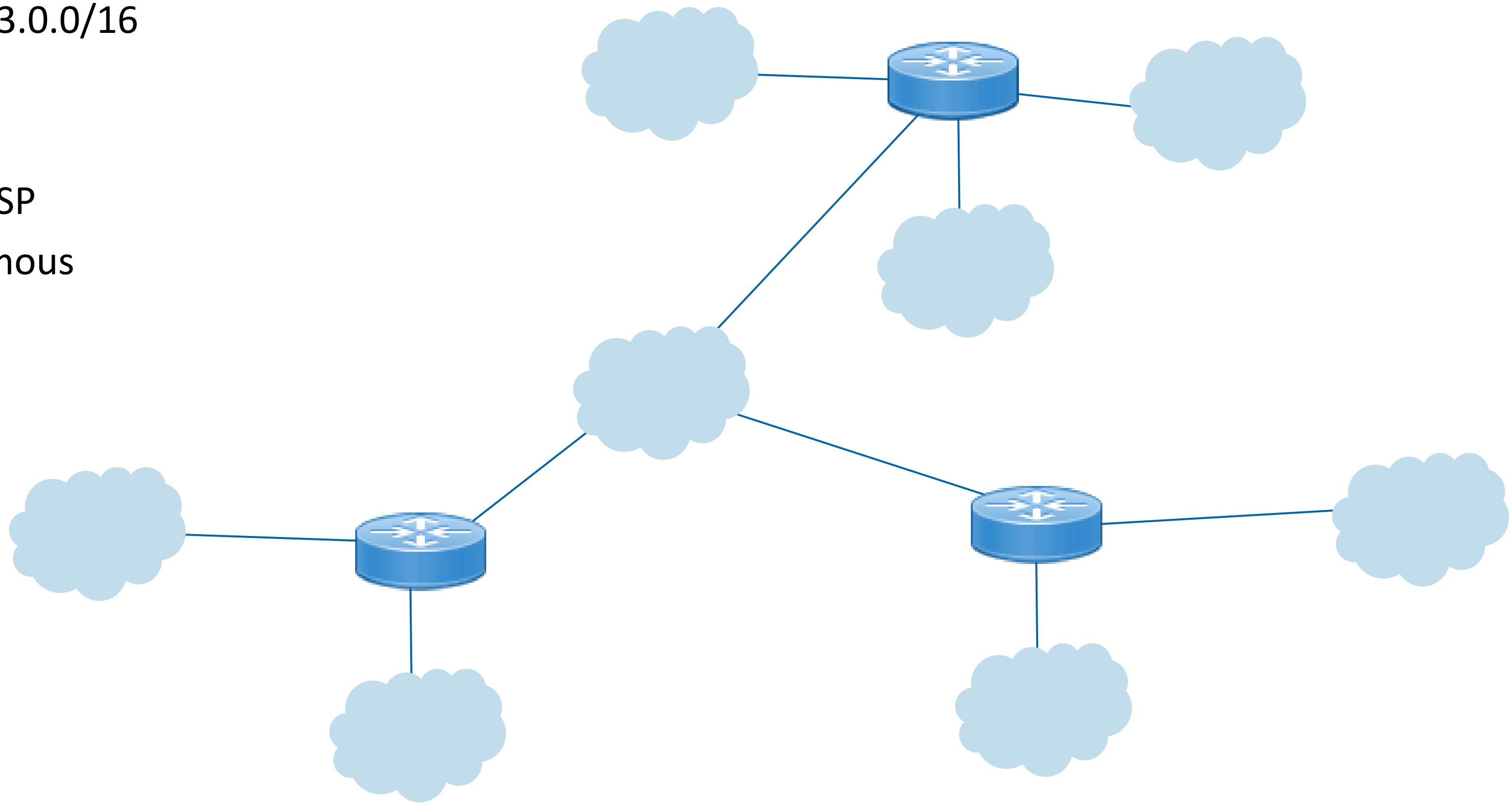
- Lets build our company net
  - We buy the IP range of 145.223.0.0/16
  - Routable
  - 65534 hosts
  - We do not have to rely on an ISP
  - That’s what meant by autonomous



GEM MINE

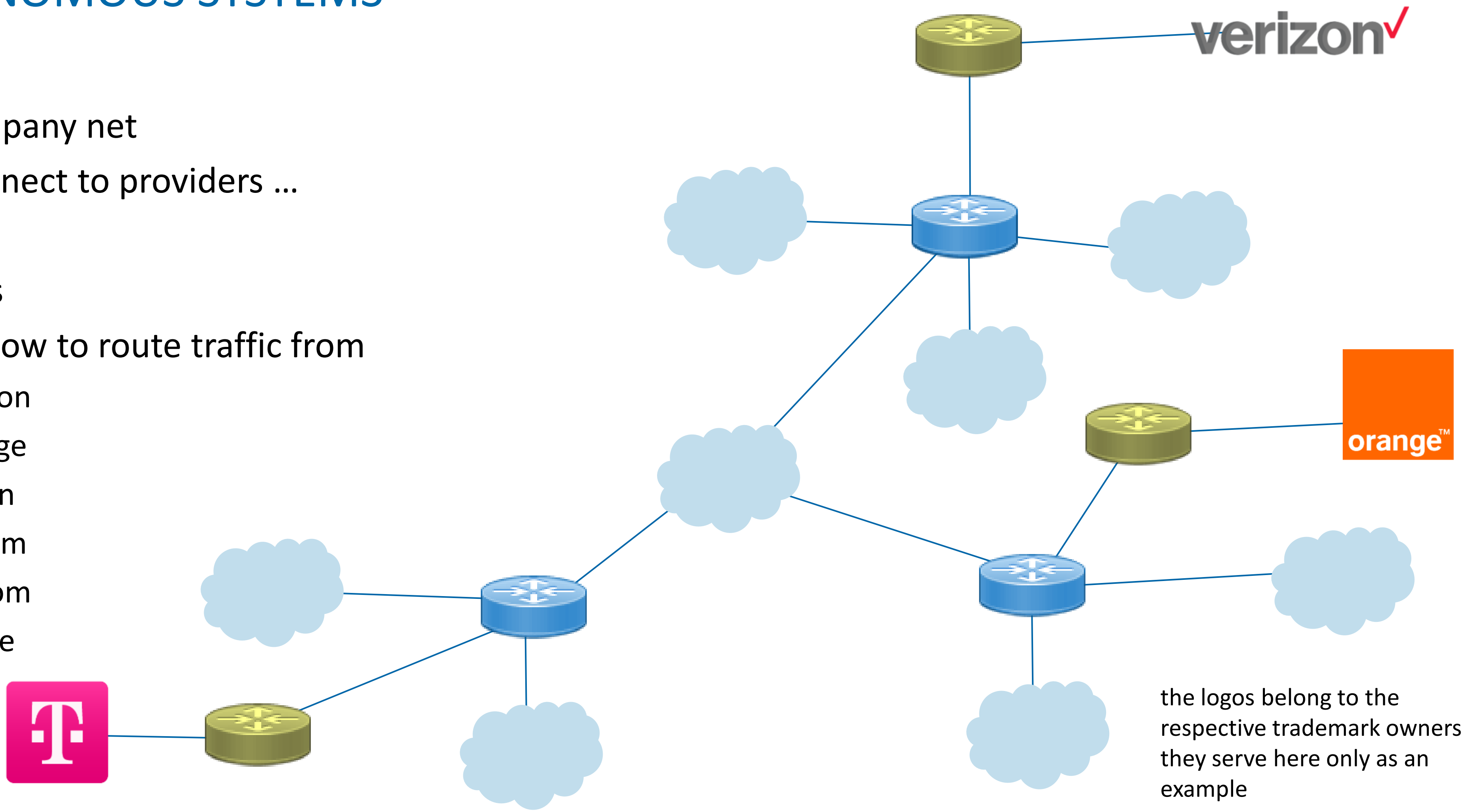
LAYER 3 – AUTONOMOUS SYSTEMS

- Lets build our company net
  - We buy the IP range of 145.223.0.0/16
  - Routable
  - 65534 hosts
  - We do not have to rely on an ISP
  - That’s what meant by autonomous



LAYER 3 – AUTONOMOUS SYSTEMS

- Lets build our company net
- OK… now let‘s connect to providers …
- … and their nets
- Redundancy for us
- Additionally we allow to route traffic from
  - telekom to verizon
  - telekom to orange
  - orange to verizon
  - orange to telekom
  - verizon to telekom
  - verizon to orange



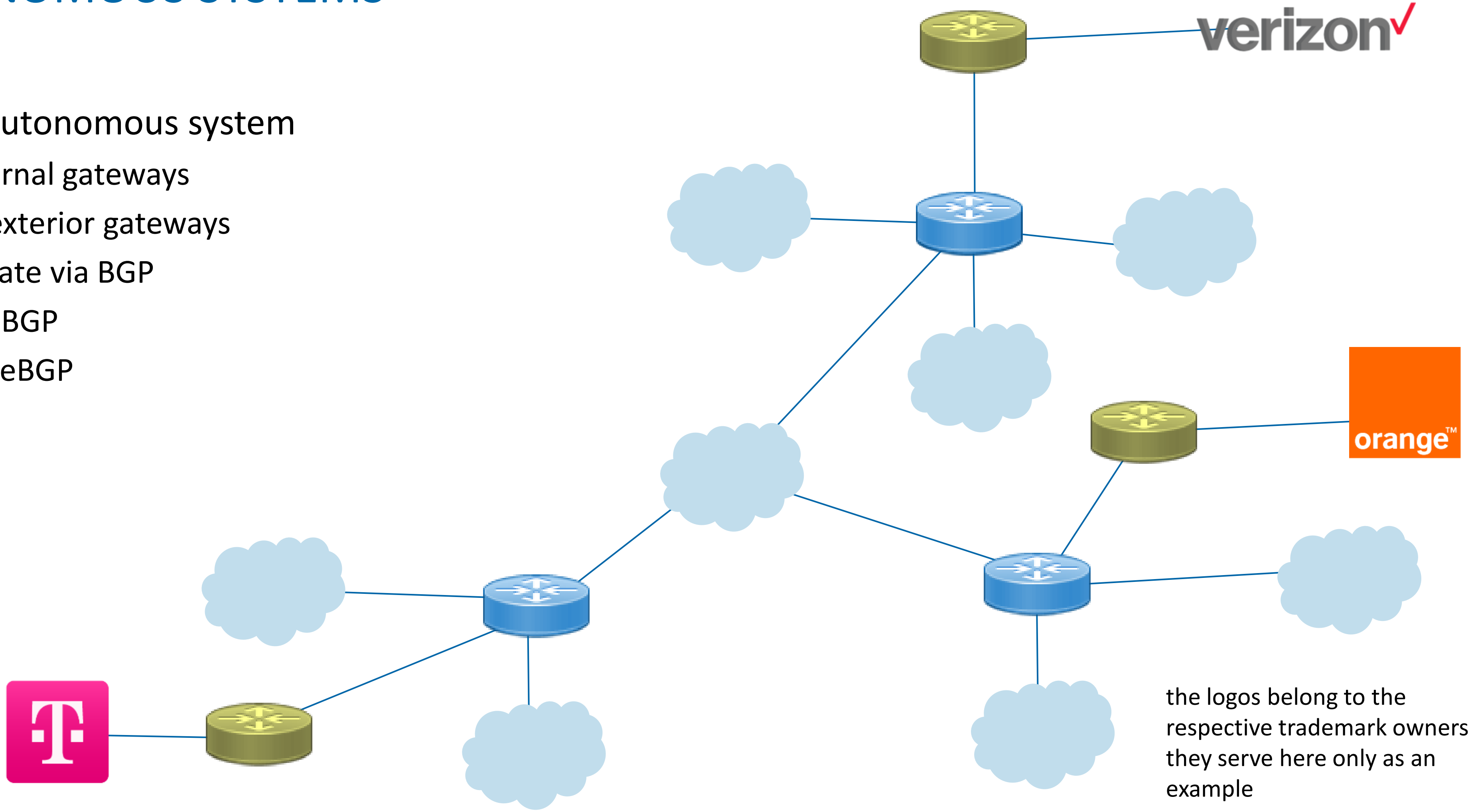
the logos belong to the respective trademark owners! they serve here only as an example

ISO OSI LAYERS

GEM MINE

LAYER 3 – AUTONOMOUS SYSTEMS

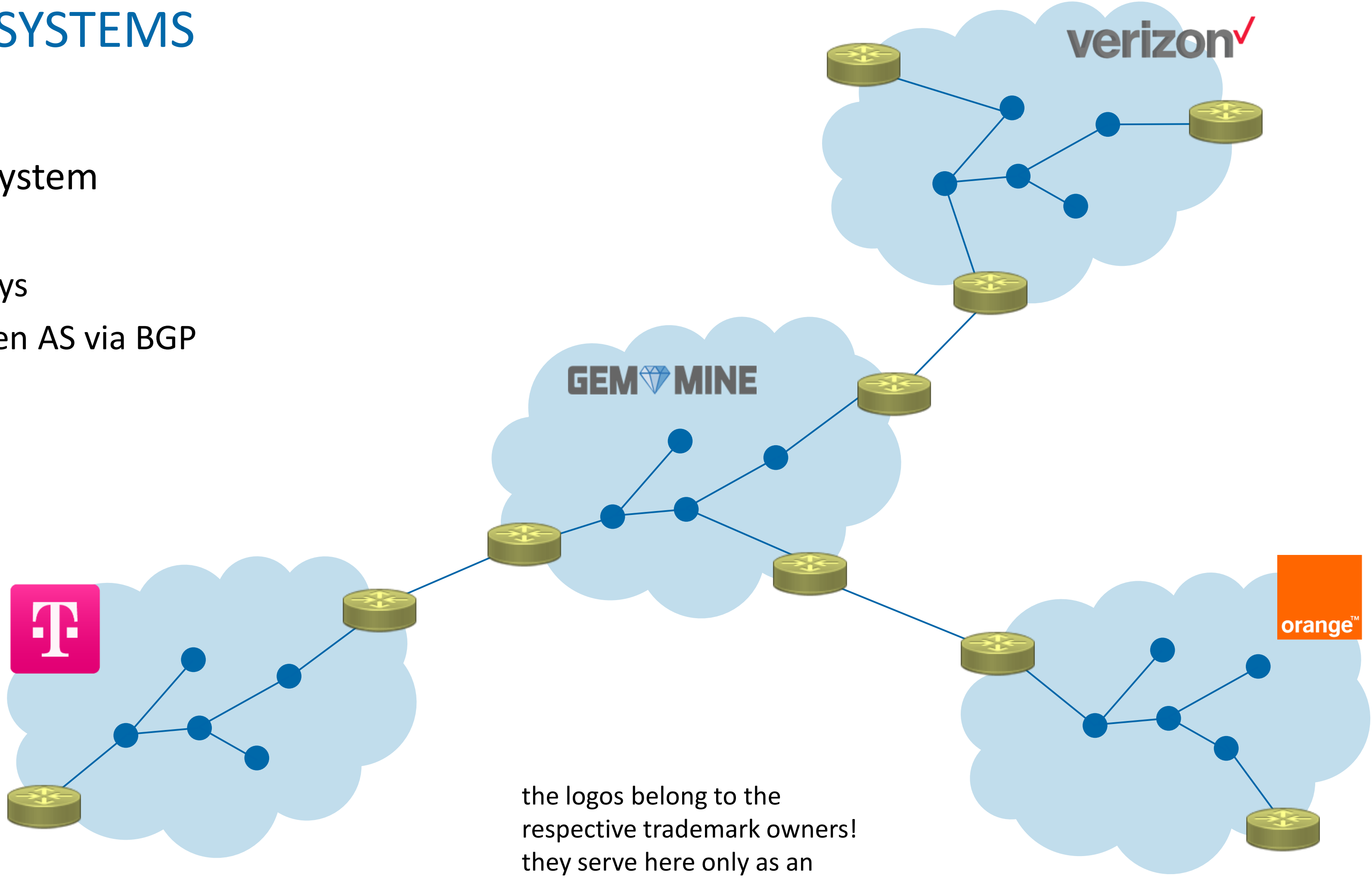
- We now have an autonomous system
  - Blue router: internal gateways
  - Golden router: exterior gateways
  - Router communate via BGP
  - internal router: iBGP
  - External router: eBGP



the logos belong to the respective trademark owners! they serve here only as an example

LAYER 3 – AUTONOMOUS SYSTEMS

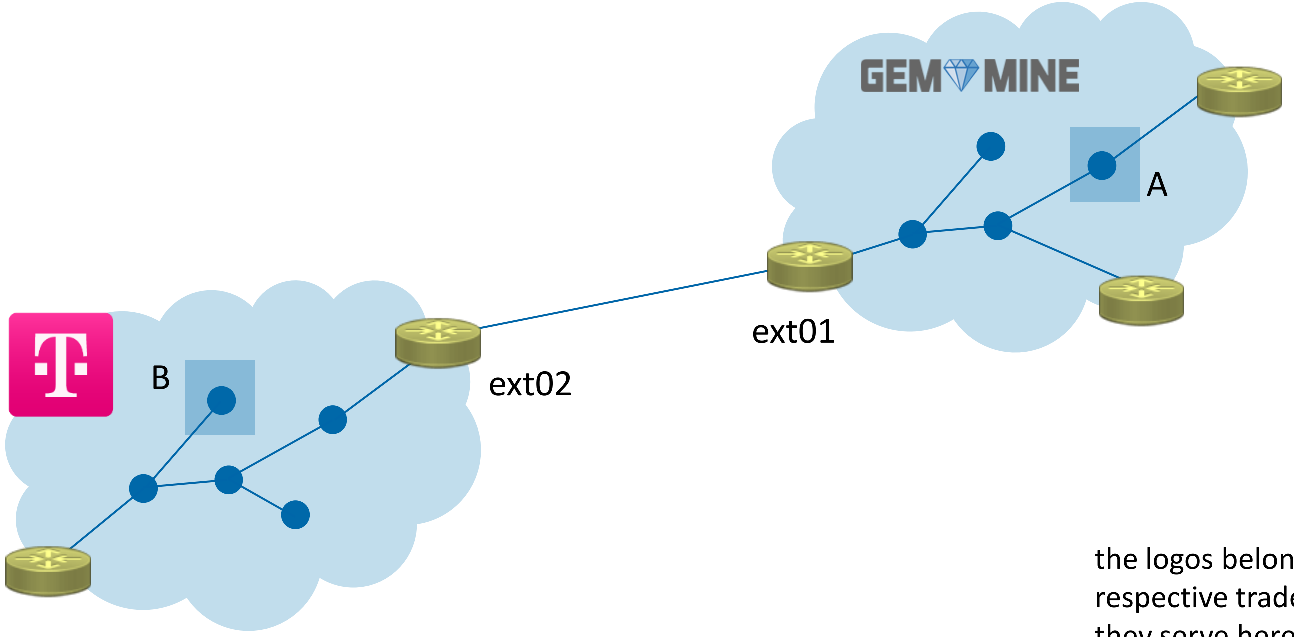
- We now have an autonomous system
  - Blue router: internal gateways
  - Golden router: exterior gateways
  - Router exchange routes between AS via BGP
  - internal router: iBGP
  - External router: eBGP



the logos belong to the respective trademark owners! they serve here only as an example

LAYER 3 – AUTONOMOUS SYSTEMS

- IGP, iBGP, eBGP
- A wants to send a packet to B
- A needs to send packet to ext01



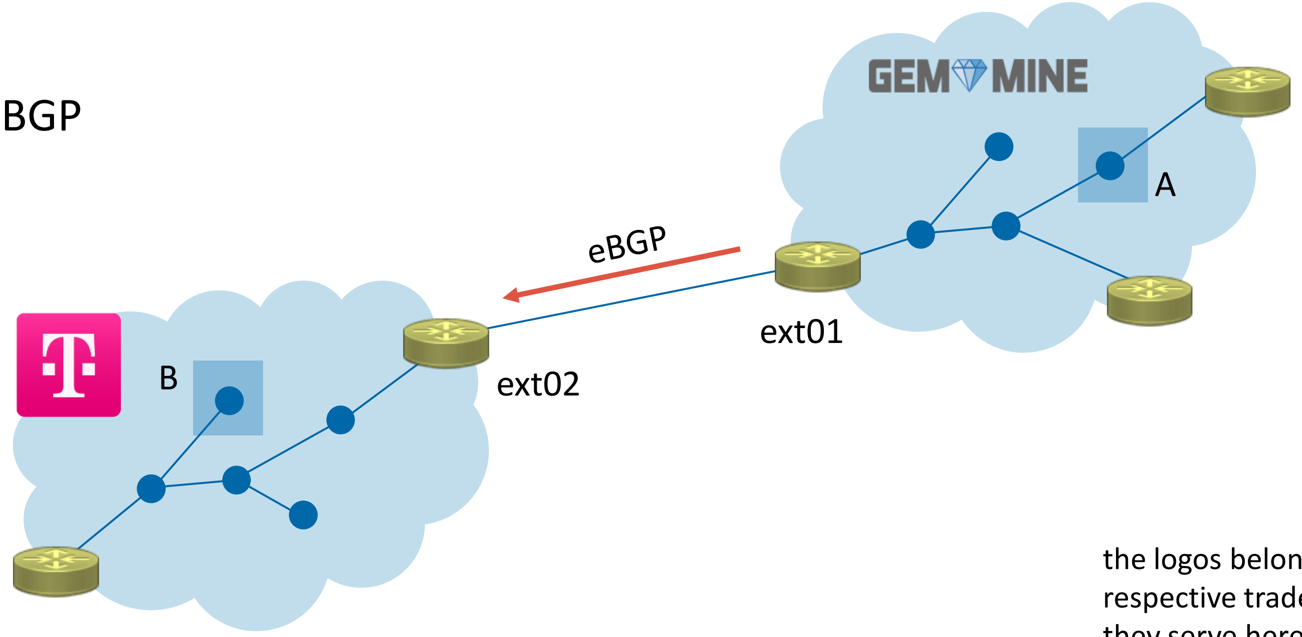
the logos belong to the respective trademark owners! they serve here only as an example

ISO OSI LAYERS

GEM MINE

LAYER 3 – AUTONOMOUS SYSTEMS

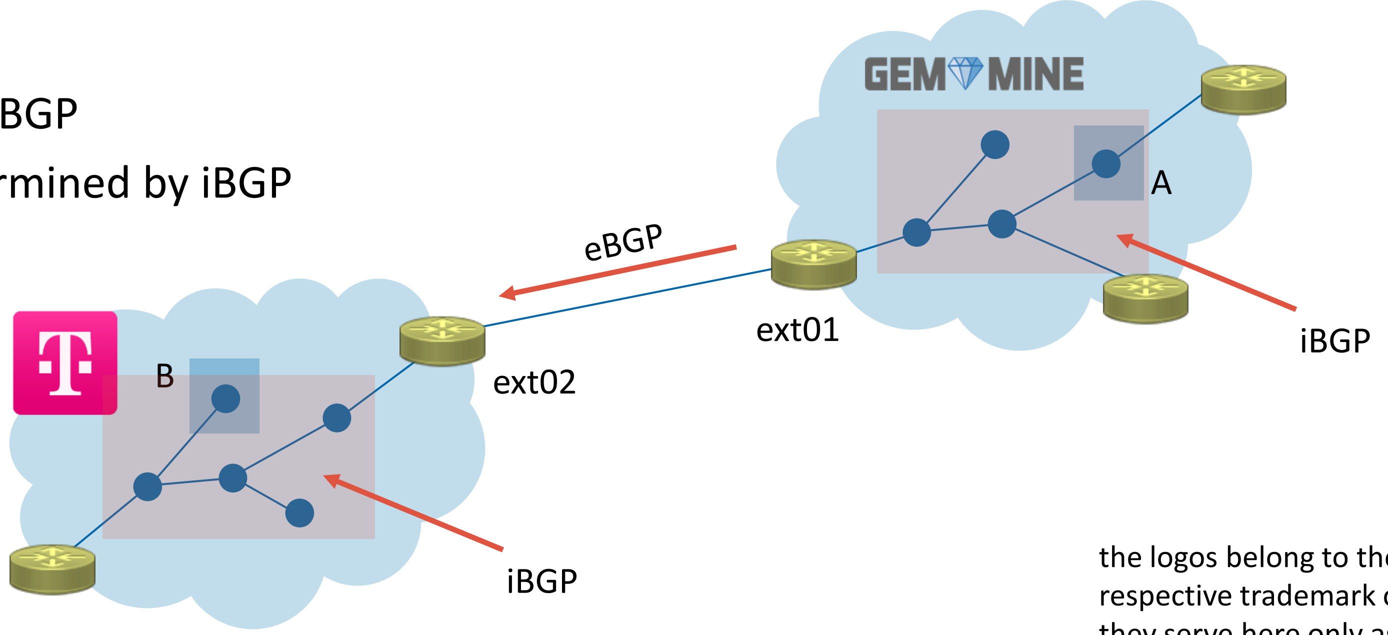
- IGP, iBGP, eBGP
- A wants to send a packet to B
- A needs to send packet to ext01
- ext01 sends packet to ext02
- ext01 knows about ext02 thanks to eBGP



the logos belong to the respective trademark owners! they serve here only as an example

LAYER 3 – AUTONOMOUS SYSTEMS

- IGP, iBGP, eBGP
- A wants to send a packet to B
- A needs to send packet to ext01
- ext01 sends packet to ext02
- ext01 knows about ext02 thanks to eBGP
- The route inside AS gemmine is determined by iBGP
- Same for route inside telekom



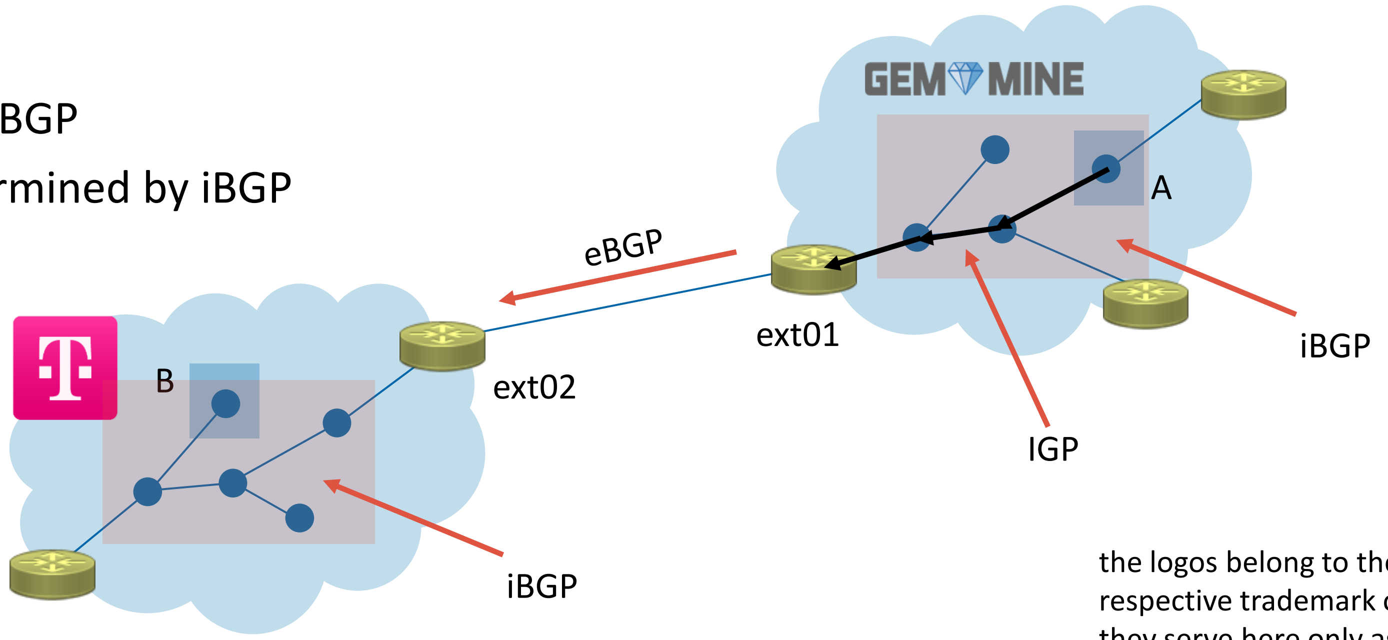
the logos belong to the respective trademark owners! they serve here only as an example

ISO OSI LAYERS

GEMMINE

LAYER 3 – AUTONOMOUS SYSTEMS

- IGP, iBGP, eBGP
- A wants to send a packet to B
- A needs to send packet to ext01
- ext01 sends packet to ext02
- ext01 knows about ext02 thanks to eBGP
- The route inside AS gemmine is determined by iBGP
- Same for route inside telekom
- Protocol to send packet to ext01 as next hop is IGP



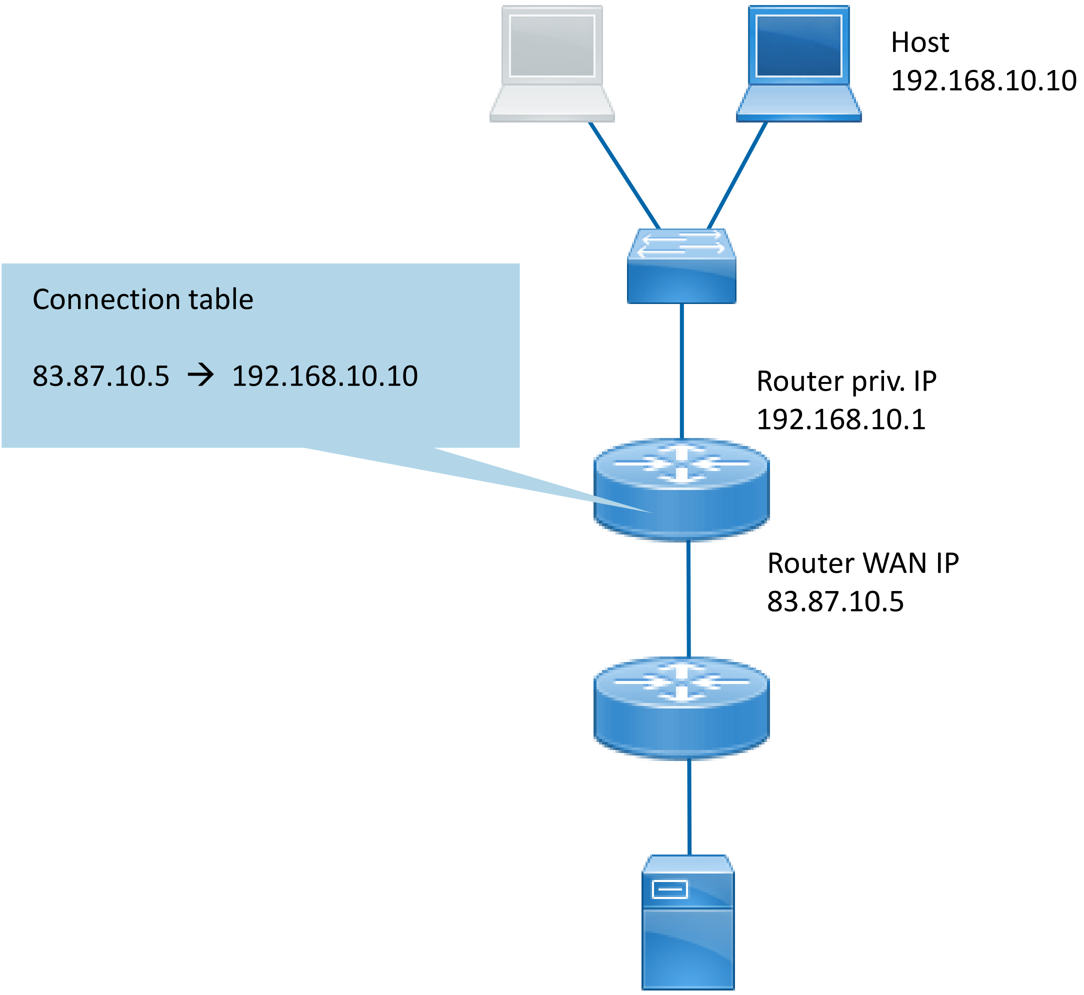
the logos belong to the respective trademark owners! they serve here only as an example

GEM MINE

LAYER 3 – ROUTING PRIVATE IP ADDRESSES

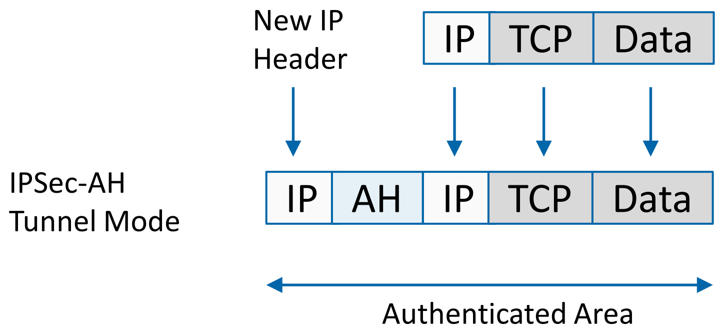
- Network Address translation
  - Host sends IP packet to router
  - Router replaces IP header
    SRC-IP: Router IP
    DST-IP: Next Hop
  - Router remembers the connection in a table
  - Router sends packet to next hop

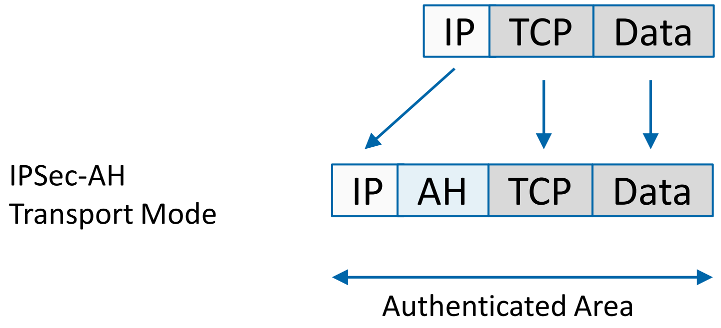
  - Response packet arrives
  - Router takes a look in connection table
  - Router replaces the IP header
    SRC-IP: Router IP
    DST-IP: Host
  - Router sends packet to Host



LAYER 3 – VPN ISSUES

- NAT and VPN is a problem is using Authentication Header (AH)
- Both in Tunnel and Transport Mode
- If router replaces IP header with his own, the Authentication Header fails

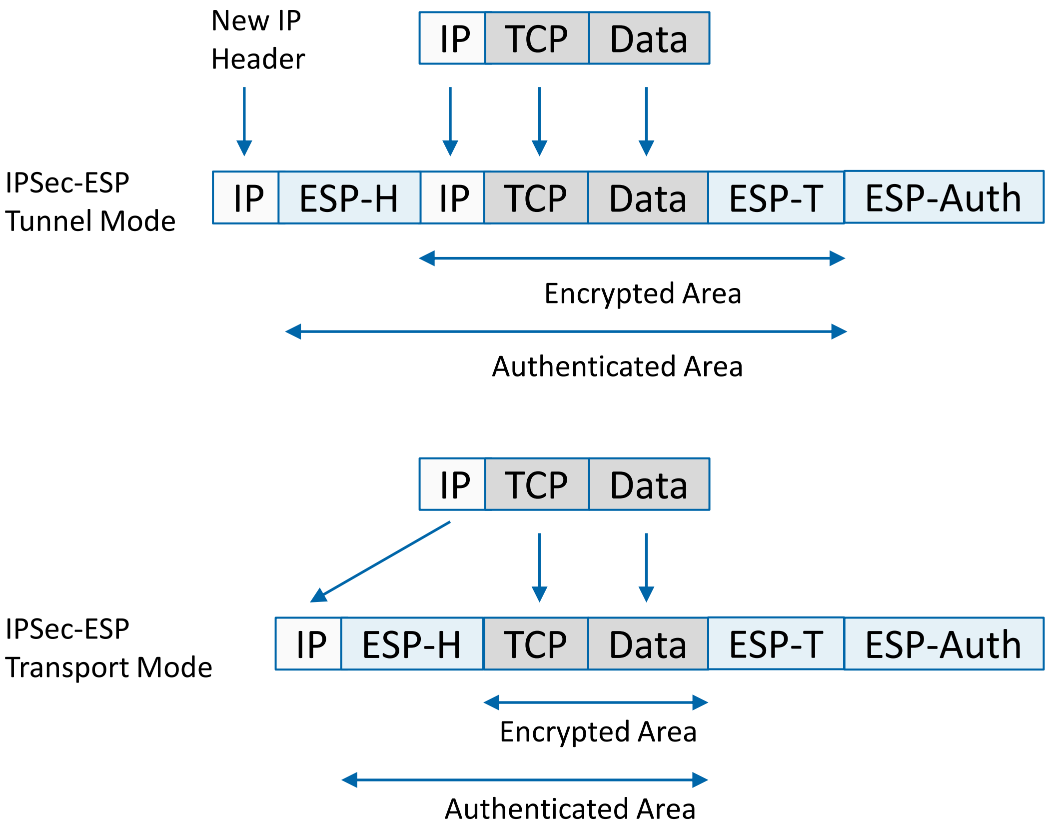




ISO OSI LAYERS

LAYER 3 – VPN ISSUES

- ESP to the rescue
- Encapsulating Security Payload
- NAT-T (Traversal)
- Both work in Tunnel and Transport Mode
- If router replaces IP header with his own, it does not matter, as the authentication does not include the IP header



ISO OSI LAYERS

LAYER 3 – NET CLASSES (BEFORE CIDR)

Net class	Prefix	Address range	Netmask	Net length	Host length	# Nets	Hosts per net	CIDR suffix
Class A	0…	0.0.0.0 – 127.255.255.255	255.0.0.0	8 Bit	24 Bit	128	16.777.214	/8
Class B	10…	128.0.0.0 – 191.255.255.255	255.255.0.0	16 Bit	16 Bit	16.384	65.534	/16
Class C	110…	192.0.0.0 – 223.255.255.255	255.255.255.0	24 Bit	8 Bit	2.097.152	254	/24
Class D	1110…	224.0.0.0 – 239.255.255.255	Reserved für Multicast Applications					
Class E	1111…	240.0.0.0 – 255.255.255.255	Reserved for future purposes					

LAYER 3 – CIDR (SOME EXAMPLES)

Notation	Addresses	Subnetmask dez	Subnet mask bin	Example	Meaning
/0	4.294.967.296	0.0.0.0	00000000.00000000.00000000.00000000	0.0.0.0/0	Full IPv4 address room
/8	16.777.216	255.0.0.0	11111111.00000000.00000000.00000000	10.0.0.0/8	10.0.0.0 – 10.255.255.255
/12	1.048.576	255.240.0.0	11111111.11110000.00000000.00000000	172.16.0.0/12	172.16.0.0 – 172.31.255.255
/16	65.536	255.255.0.0	11111111.11111111.00000000.00000000	192.168.0.0/16	192.168.0.0 – 192.168.255.255
/24	256	255.255.255.0	11111111.11111111.11111111.00000000	192.168.10.0/24	192.168.10.0 – 192.168.10.255
/28	16	255.255.255.240	11111111.11111111.11111111.11110000	192.168.10.24/28	192.168.10.16 – 192.168.10.31

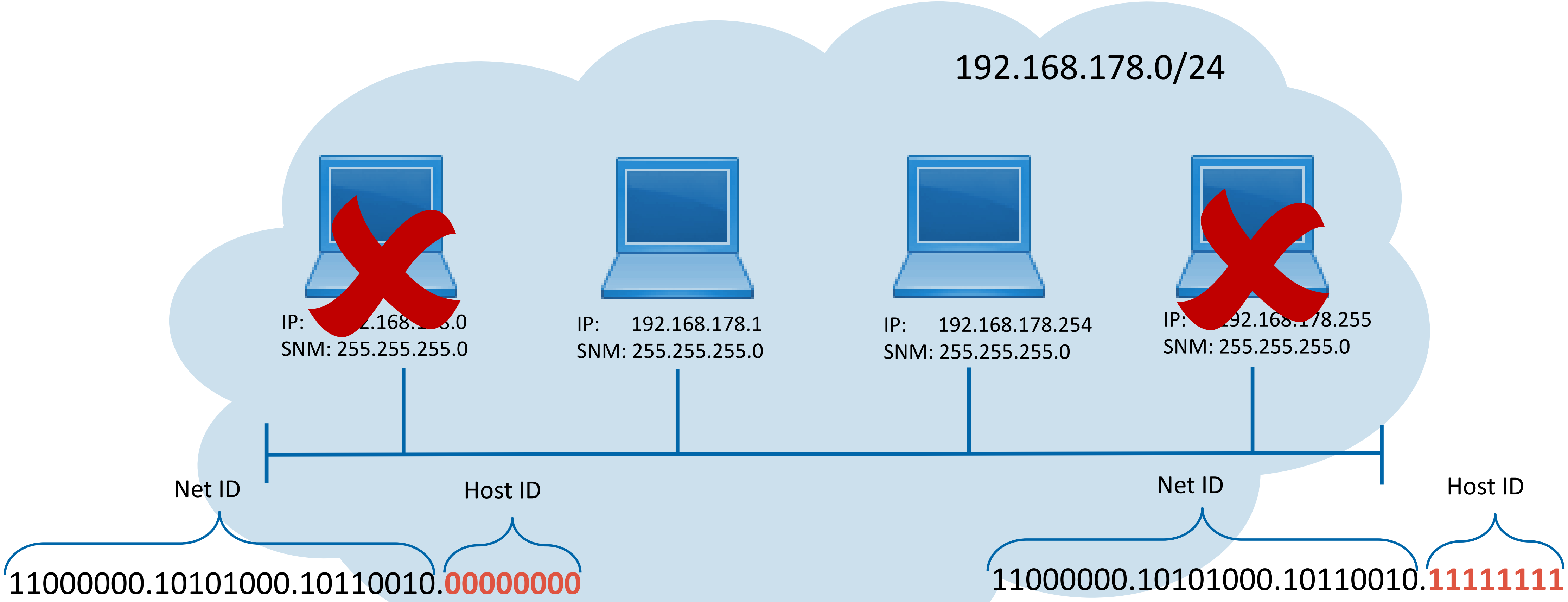
LAYER 3 – PRIVATE ADDRESS SPACE (NOT ROUTABLE)

Notation	Addresses	Subnetmask dez	Subnet mask bin	Example	Meaning
/0	4.294.967.296	0.0.0.0	00000000.00000000.00000000.00000000	0.0.0.0/0	Full IPv4 address room
/8	16.777.216	255.0.0.0	11111111.00000000.00000000.00000000	10.0.0.0/8	10.0.0.0 – 10.255.255.255
/12	1.048.576	255.240.0.0	11111111.11110000.00000000.00000000	172.16.0.0/12	172.16.0.0 – 172.31.255.255
/16	65.536	255.255.0.0	11111111.11111111.00000000.00000000	192.168.0.0/16	192.168.0.0 – 192.168.255.255
/24	256	255.255.255.0	11111111.11111111.11111111.00000000	192.168.10.0/24	192.168.10.0 – 192.168.10.255
/28	16	255.255.255.240	11111111.11111111.11111111.11110000	192.168.10.24/28	192.168.10.16 – 192.168.10.31

ISO OSI LAYERS

GEM MINE

LAYER 3 – SPECIAL IP ADDRESSES



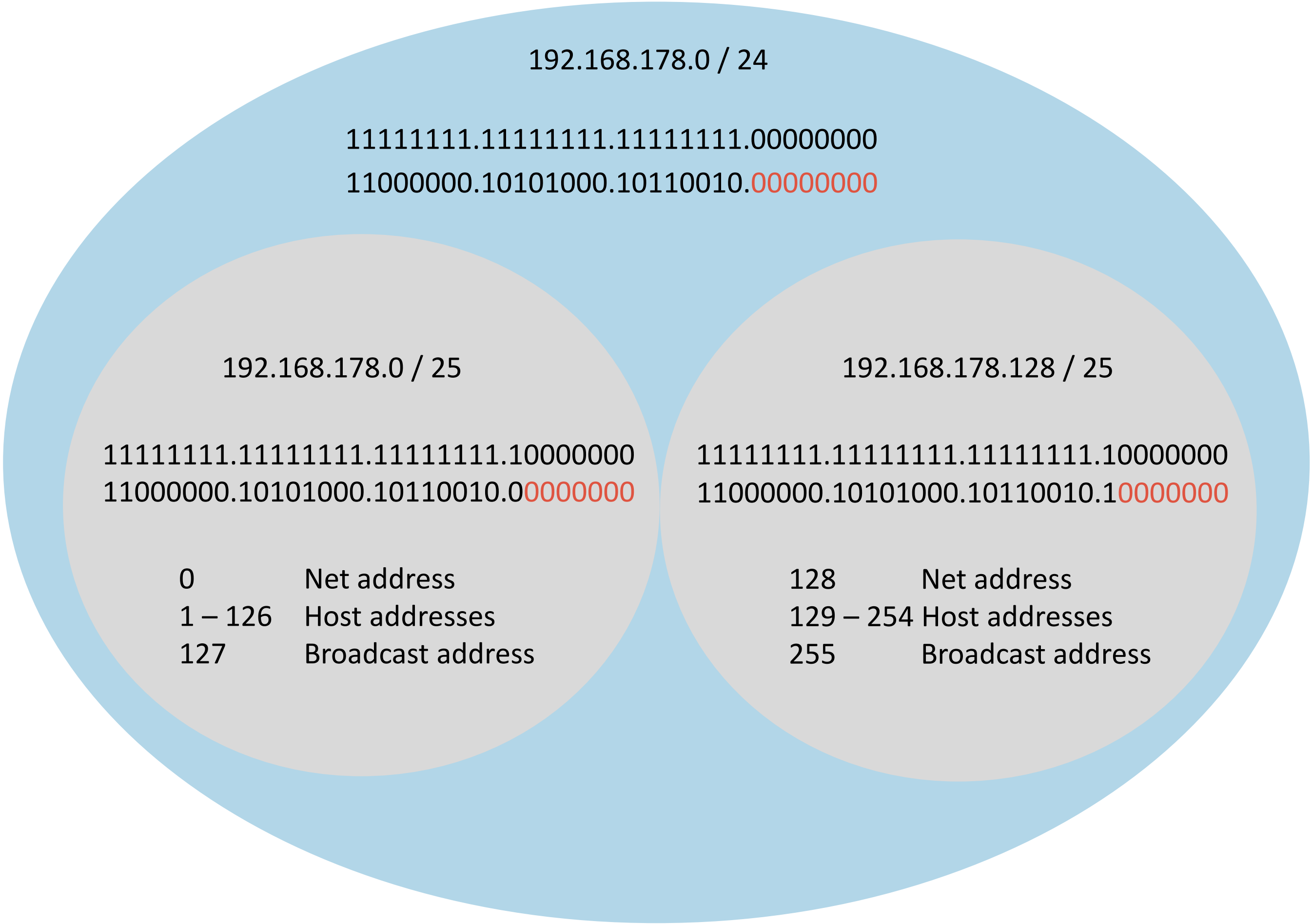
Net address, used to identify the net

Broadcast address, used to send packets to all

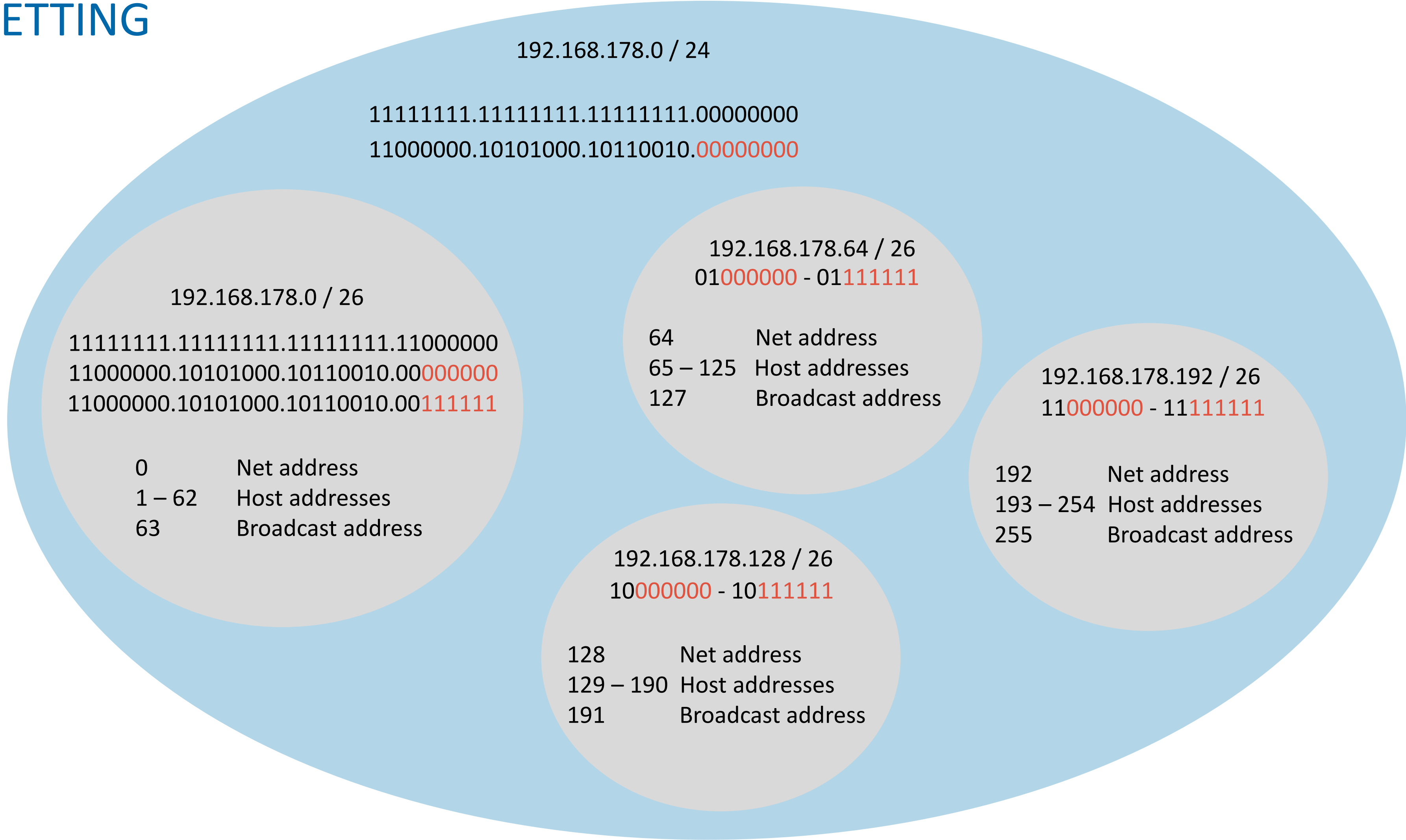
ISO OSI LAYERS

LAYER 3 – SUBNETTING

- What if we divide a net in smaller chunks?
  - 192.168.178.0 / 24
  - 254 Hosts
  - 0 – Net address
  - 255 – Broadcast address
  - 1 – 254 assignable to hosts
- What about … 192.168.178.0 / 25
  - The net part is now one bit larger
  - The host part is one bit smaller
  - Now the last seven bits are the host id
  - Dividing the net in two parts
  - 0 – 127
  - 128 - 255



LAYER 3 – SUBNETTING



GEM MINE

LAYER 3 – SUBNETTING

192.168.178.0 / 24

11111111.11111111.11111111.00000000
11000000.10101000.10110010.00000000

192.168.178.0 / 25

11111111.11111111.11111111.11000000
11000000.10101000.10110010.00000000
11000000.10101000.10110010.01111111

0	Net address
1 – 126	Host addresses
127	Broadcast address

192.168.178.128 / 26
10000000 - 10111111

128	Net address
129 – 190	Host addresses
191	Broadcast address

192.168.178.192 / 26
11000000 - 11111111

192	Net address
193 – 254	Host addresses
255	Broadcast address

GEMMINE

LAYER 3 – SUBNETTING

- In a small medium-sized company, 122 employees work in different departments.
  Your task is to set up a company network, and to form subnets for the individual departments.
  You have been assigned the IP address 200.200.200.0 by IANA. Analyze, plan, document and implement the corporate network. The following departments exist in the company:

  - Electroplating (15 employees)
  - Turning shop (11 employees)
  - Production (35 employees)
  - Shipping (9 employees)
  - Development (17 employees)
  - Warehouse (7 employees)
  - Administration (28 employees)

LAYER 3 – SUBNETTING

- In a small medium-sized company, 122 employees work in different departments.
  Your task is to set up a company network, and to form subnets for the individual departments.
  You have been assigned the IP address 200.200.200.0 by IANA. Analyze, plan, document and implement the corporate network. The following departments exist in the company:

• Electroplating (15 employees)	15 hosts + Net address + broadcast address = 17. Next power of two: 32
• Turning shop (11 employees)	11 hosts + Net address + broadcast address = 13. Next power of two: 16
• Production (35 employees)	35 hosts + Net address + broadcast address = 37. Next power of two: 64
• Shipping (9 employees)	9 hosts + Net address + broadcast address = 11. Next power of two: 16
• Development (17 employees)	17 hosts + Net address + broadcast address = 19. Next power of two: 32
• Warehouse (7 employees)	7 hosts + Net address + broadcast address = 9. Next power of two: 16
• Administration (28 employees)	28 hosts + Net address + broadcast address = 30. Next power of two: 32

GEM MINE

LAYER 3 – SUBNETTING

- In a small medium-sized company, 122 employees work in different departments.
  Your task is to set up a company network, and to form subnets for the individual departments.
  You have been assigned the IP address 200.200.200.0 by IANA. Analyze, plan, document and implement the corporate network. The following departments exist in the company:

• Production (35 employees)	35 hosts + Net address + broadcast address = 37. Next power of two: 64
• Development (17 employees)	17 hosts + Net address + broadcast address = 19. Next power of two: 32
• Electroplating (15 employees)	15 hosts + Net address + broadcast address = 17. Next power of two: 32
• Administration (28 employees)	28 hosts + Net address + broadcast address = 30. Next power of two: 32
• Turning shop (11 employees)	11 hosts + Net address + broadcast address = 13. Next power of two: 16
• Shipping (9 employees)	9 hosts + Net address + broadcast address = 11. Next power of two: 16
• Warehouse (7 employees)	7 hosts + Net address + broadcast address = 9. Next power of two: 16

GEM MINE

LAYER 3 – SUBNETTING

- In a small medium-sized company, 122 employees work in different departments.
  Your task is to set up a company network, and to form subnets for the individual departments.
  You have been assigned the IP address 200.200.200.0 by IANA. Analyze, plan, document and implement the corporate network. The following departments exist in the company:

• Production (35 employees)	200.200.200.0 / 26
• Development (17 employees)	200.200.200.64 / 27
• Electroplating (15 employees)	200.200.200.96 / 27
• Administration (28 employees)	200.200.200.128 / 27
• Turning shop (11 employees)	200.200.200.160 / 28
• Shipping (9 employees)	200.200.200.176 / 28
• Warehouse (7 employees)	200.200.200.192 / 28

ISO OSI LAYERS

GEM MINE

LAYER 4 – TCP

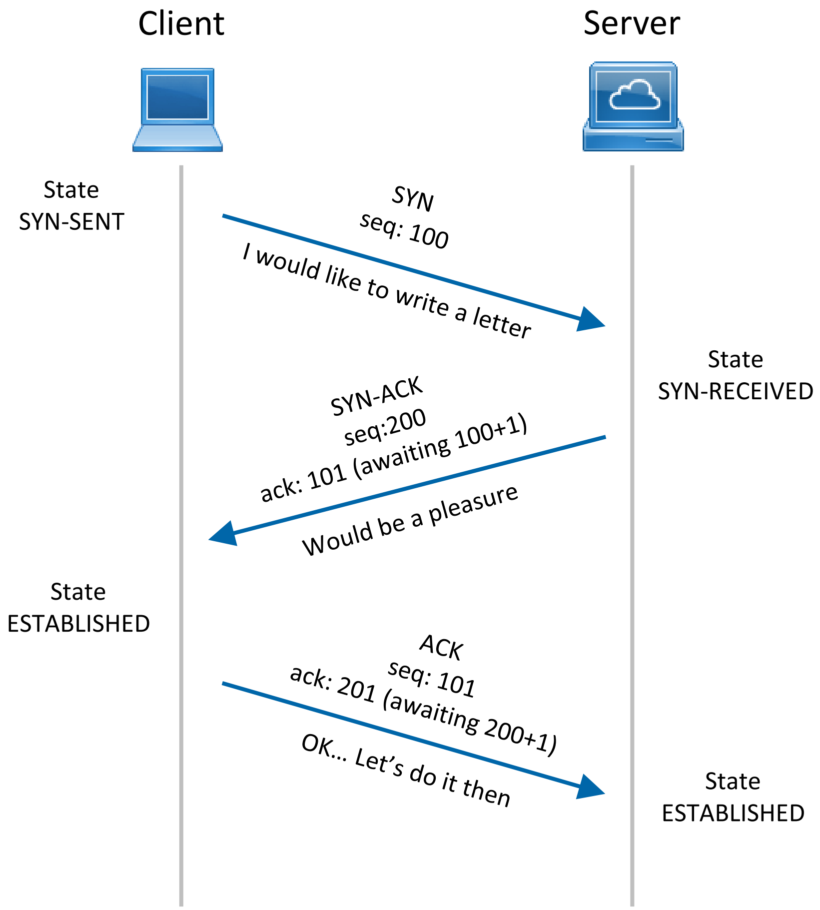
- Some Facts about IP
  - IP is a connectionless protocol - similar to writing a letter
  - You write the letter
  - You put it in the postbox and it is gone...
  - You do not know if the letter will be picked up
  - You do not know how it will be transported
  - You do not know which way it will go
  - You do not know when and if it will arrive
- America, DoD, ARPAnet needed a reliable transmission protocol
  - the korean war was almost lost
  - with russia they were in the cold war
  - in the event of a nuclear strike the network should continue to function
  - So the very normal psychosis

ISO OSI LAYERS

LAYER 4 – TCP

- A connection oriented protocol was needed
  - TCP adds a flow control layer to IP
  - Imagine you are on the phone with the person across from you
  - You tell her that you want to write a letter
  - She says she would be very happy
  - You confirm that you will write the letter
  - You write the letter
  - You send the letter ... everything as we had
  - Your counterpart tells you that the letter has arrived
  - You are happy and hang up.

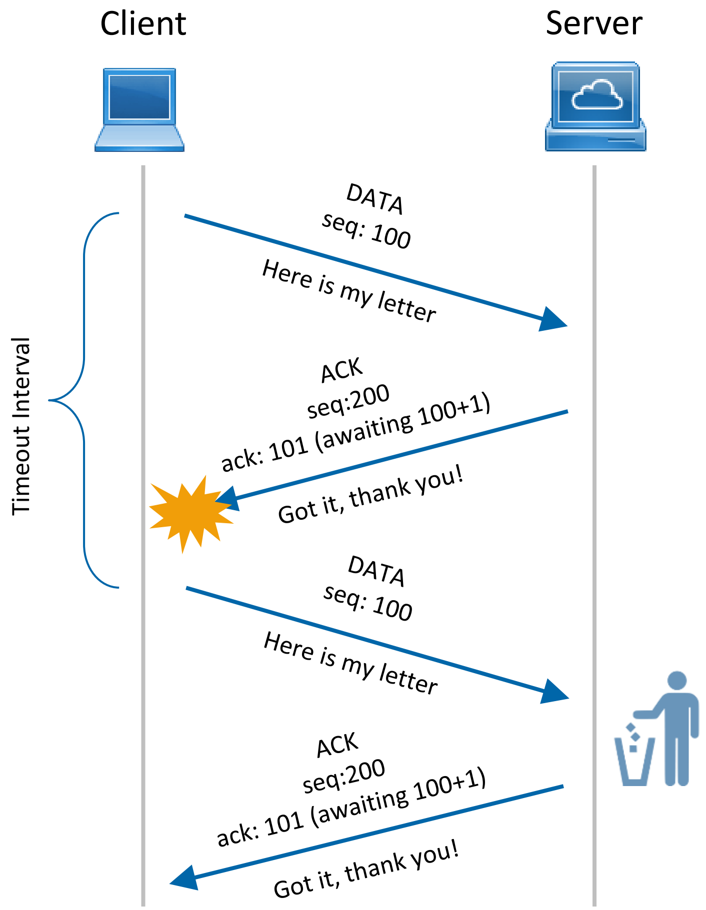
  - ...and if the letter has not arrived after an agreed time, you send it again



GEM MINE

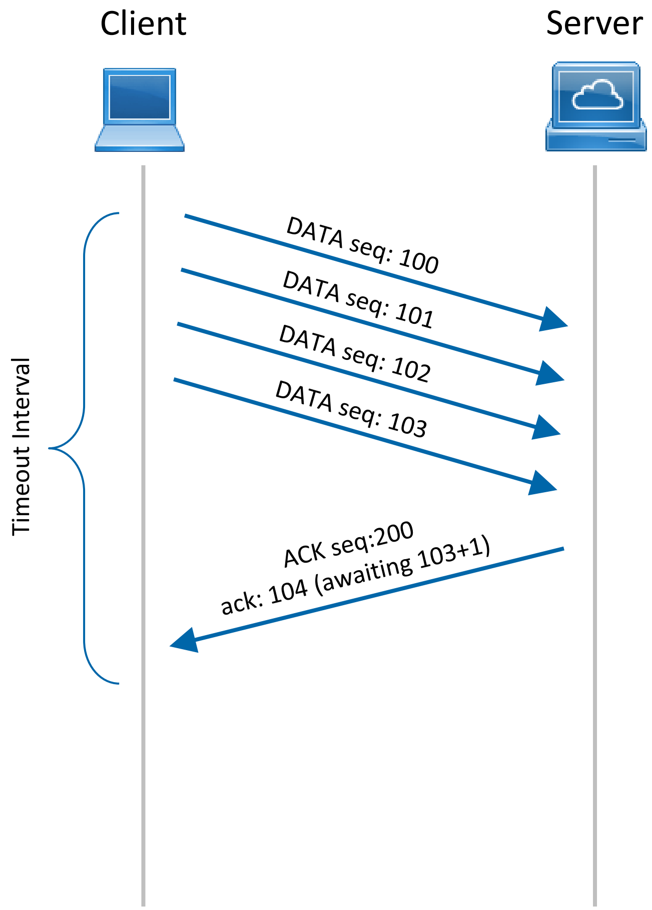
LAYER 4 – TCP DATA TRANSFER

- Stop and wait
  - The sender sends the packet and waits for the ACK
  - Once the ACK reaches the sender, it transmits the next packet in row.
  - If the ACK is not received, it re-transmits the previous packet again.



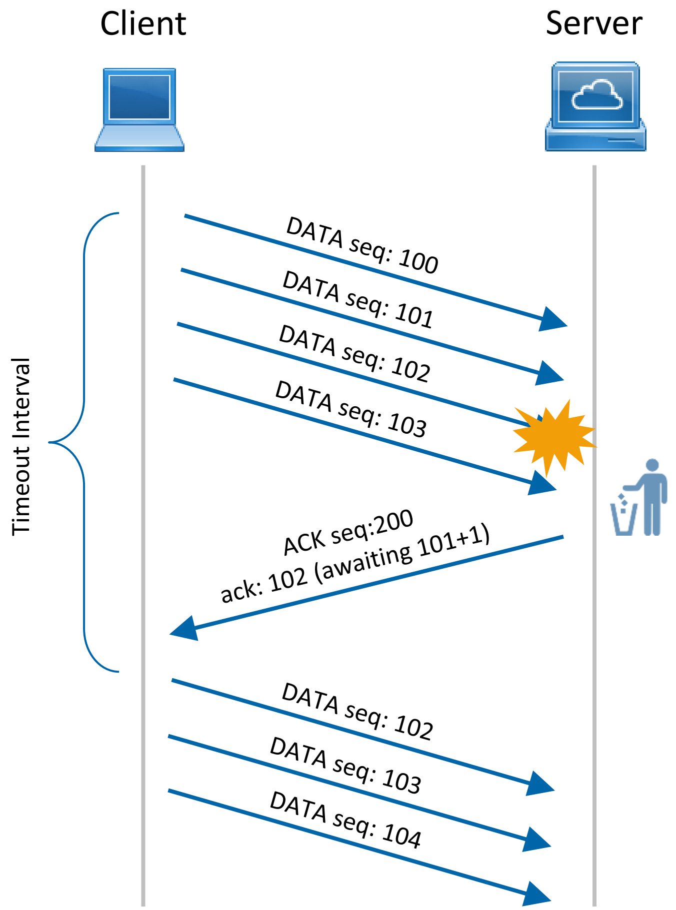
LAYER 4 – TCP DATA TRANSFER

- Go Back N
  - The sender sends N packets which is equal to the window size.
  - Once the entire window is sent, the sender then waits for a cumulative ACK to send more packets.
  - On the receiver end, it receives only in-order packets and discards out-of-order packets.
  - As in case of packet loss, the entire window would be re-transmitted.



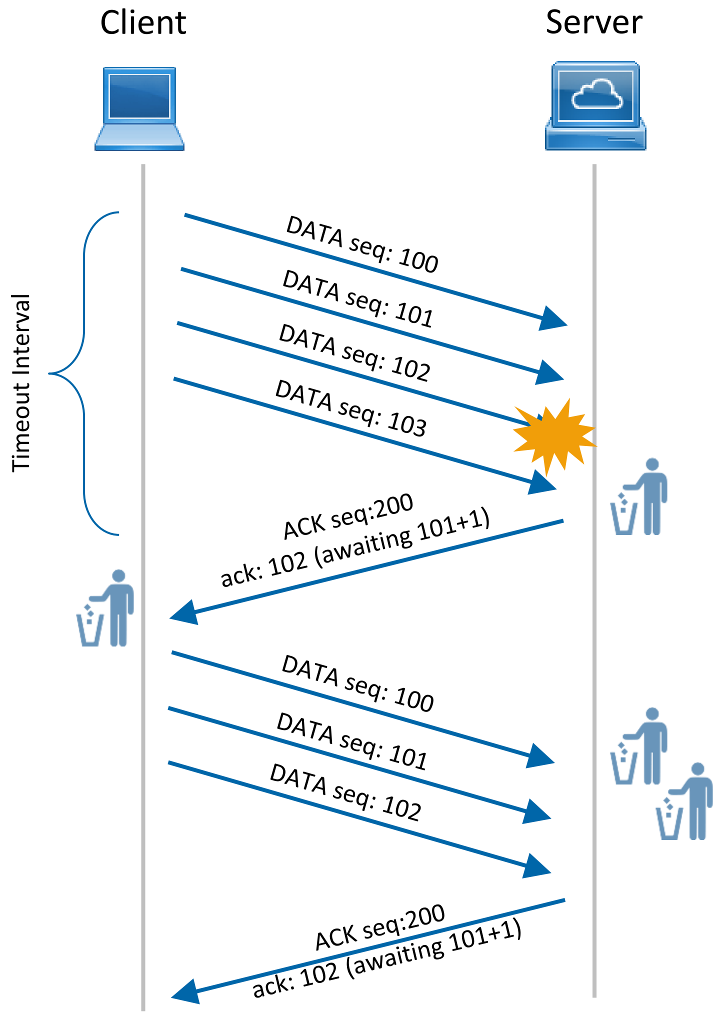
LAYER 4 – TCP DATA TRANSFER

- Go Back N
  - The sender sends N packets which is equal to the window size.
  - Once the entire window is sent, the sender then waits for a cumulative ACK to send more packets.
  - On the receiver end, it receives only in-order packets and discards out-of-order packets.
  - As in case of packet loss, the entire window would be re-transmitted.



LAYER 4 – TCP DATA TRANSFER

- Go Back N
  - The sender sends N packets which is equal to the window size.
  - Once the entire window is sent, the sender then waits for a cumulative ACK to send more packets.
  - On the receiver end, it receives only in-order packets and discards out-of-order packets.
  - As in case of packet loss, the entire window would be re-transmitted.

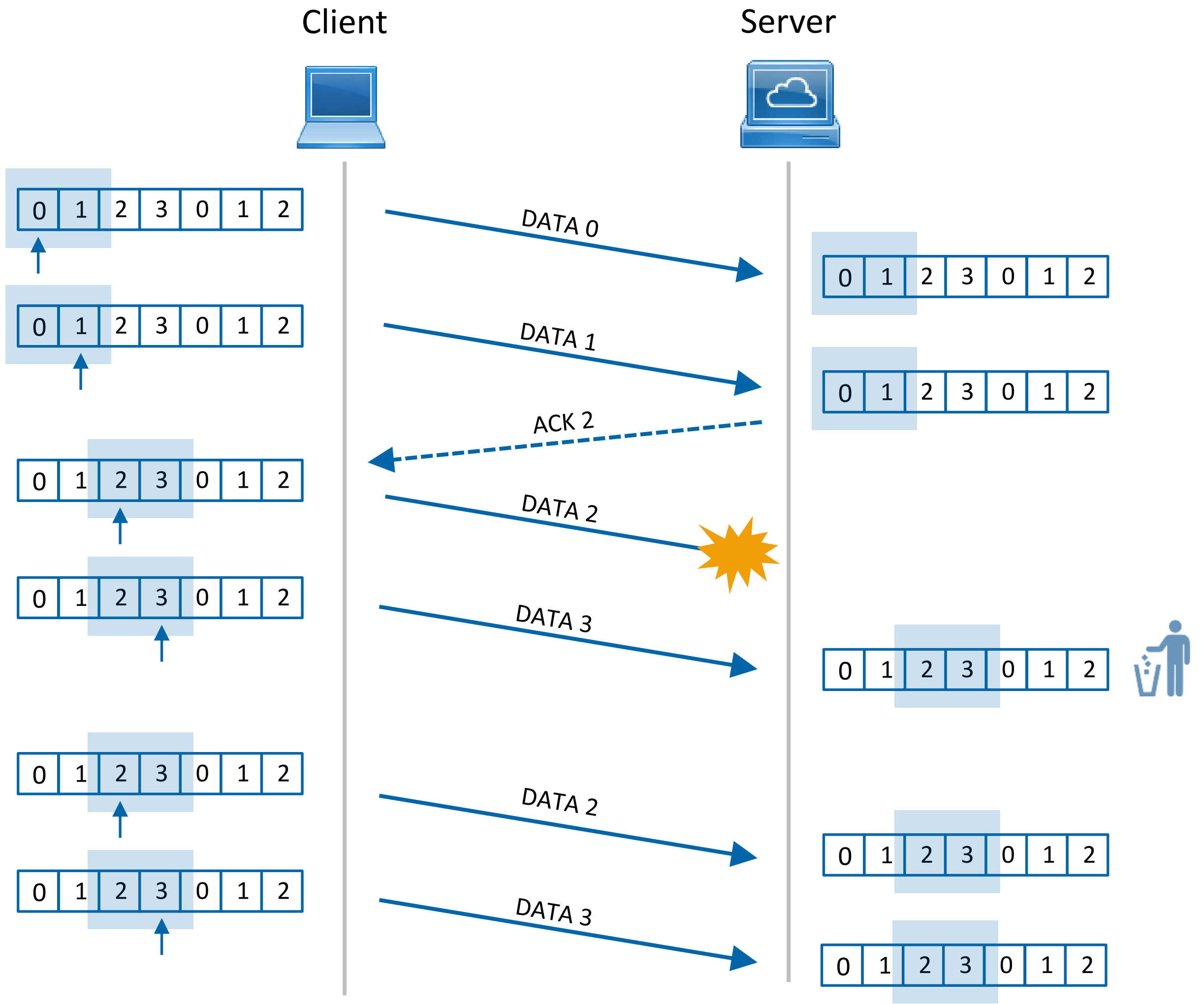


ISO OSI LAYERS

LAYER 4 – TCP DATA TRANSFER

- Sliding Window
  - Accounting of the sent packets
  - Window can vary its size
  - Gets bigger at good connection
  - Get smaller at lossy connection
  - Window slot number is not packet frame number!

  - Another implementation does not wait for the correct first packet to arrive but puts every packet in the receiver window if the slot is free, then sends accumulative ack packets



ISO OSI LAYERS

GEM MINE

LAYER 4 – TCP PORTS

- Suppose you live in a detached house
- Alone
- With your own address
- The postman can deliver a letter to your address
- Your address is here the IP

- Suppose you work in an office building
- Not alone
- In your own office on the 6th floor
- The postman can deliver a letter to the address of the office building. This is still your IP
- If the letter is to go to your office, he must also know the office number. This is the port

GEM MINE

LAYER 4 – TCP: SOME EVERYDAY PORTS

Portnumber	Protocol	Description
20	TCP	FTP
22	TCP	SSH
23	TCP	Telnet
25	TCP	SMTP
53	TCP, UDP	DNS
67	UDP	DHCP
68	UDP	DHCP
80	TCP	HTTP
123	UDP	NTP

Portnumber	Protocol	Description
443	TCP	HTTPS
666	UDP	Doom
1194	TCP, UDP	OpenVPN
1433	TCP	MSSQL
3306	TCP, UDP	MySQL, MariaDB
3389	TCP	RDP
5432	TCP	PostgreSQL
5900	TCP	VNC
8080	TCP	Alt. HTTP

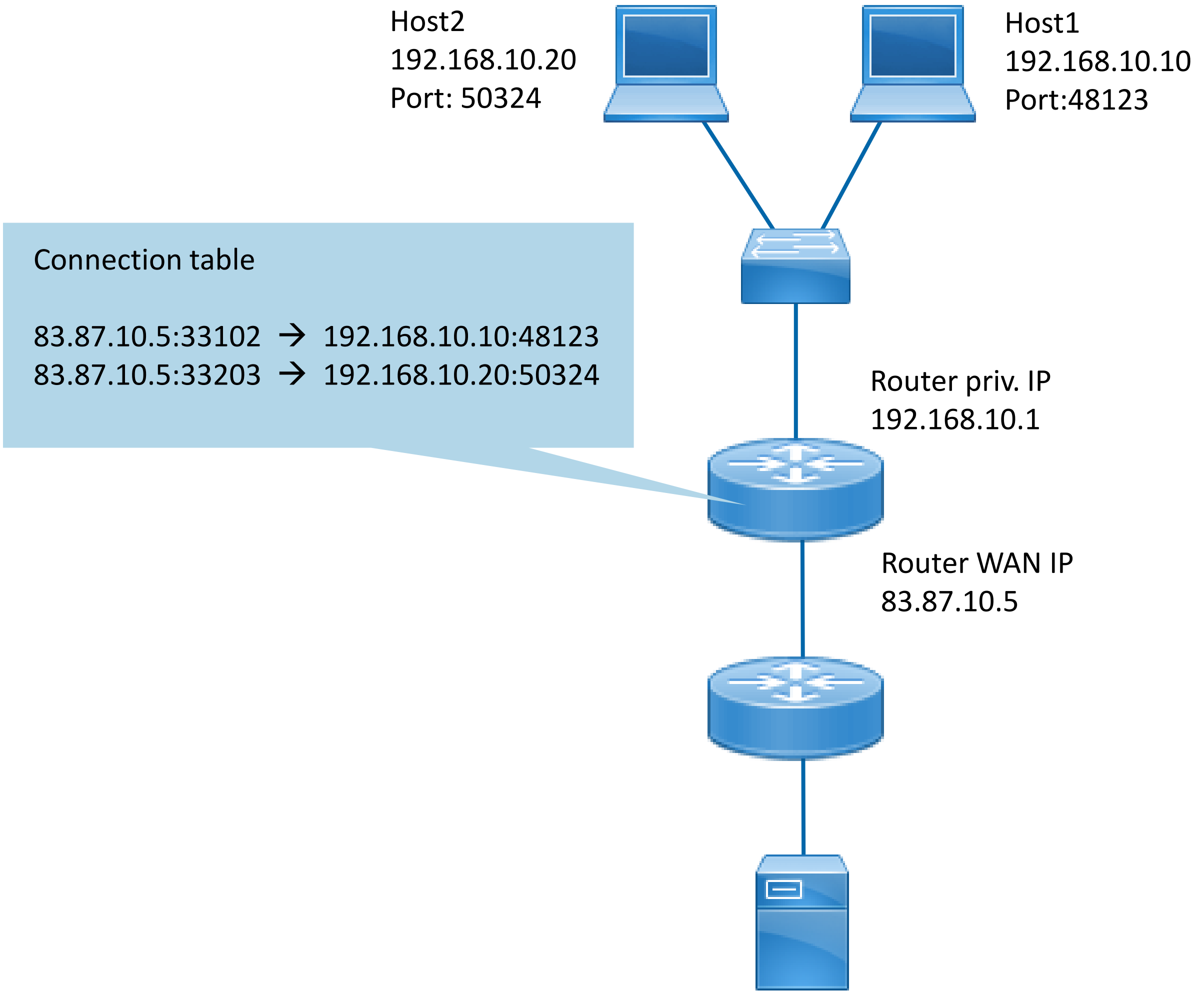
ISO OSI LAYERS

GEM MINE

LAYER 4 – ROUTING PRIVATE IP ADDRESSES

- Problems on Layer 3
  - What if… network has a second host?
  - What if… host one has multiple connections, like two browser tabs?

  - Extend NAT with a port
  - Now we have Port and Adress translation
  - This is called *Masquerading*

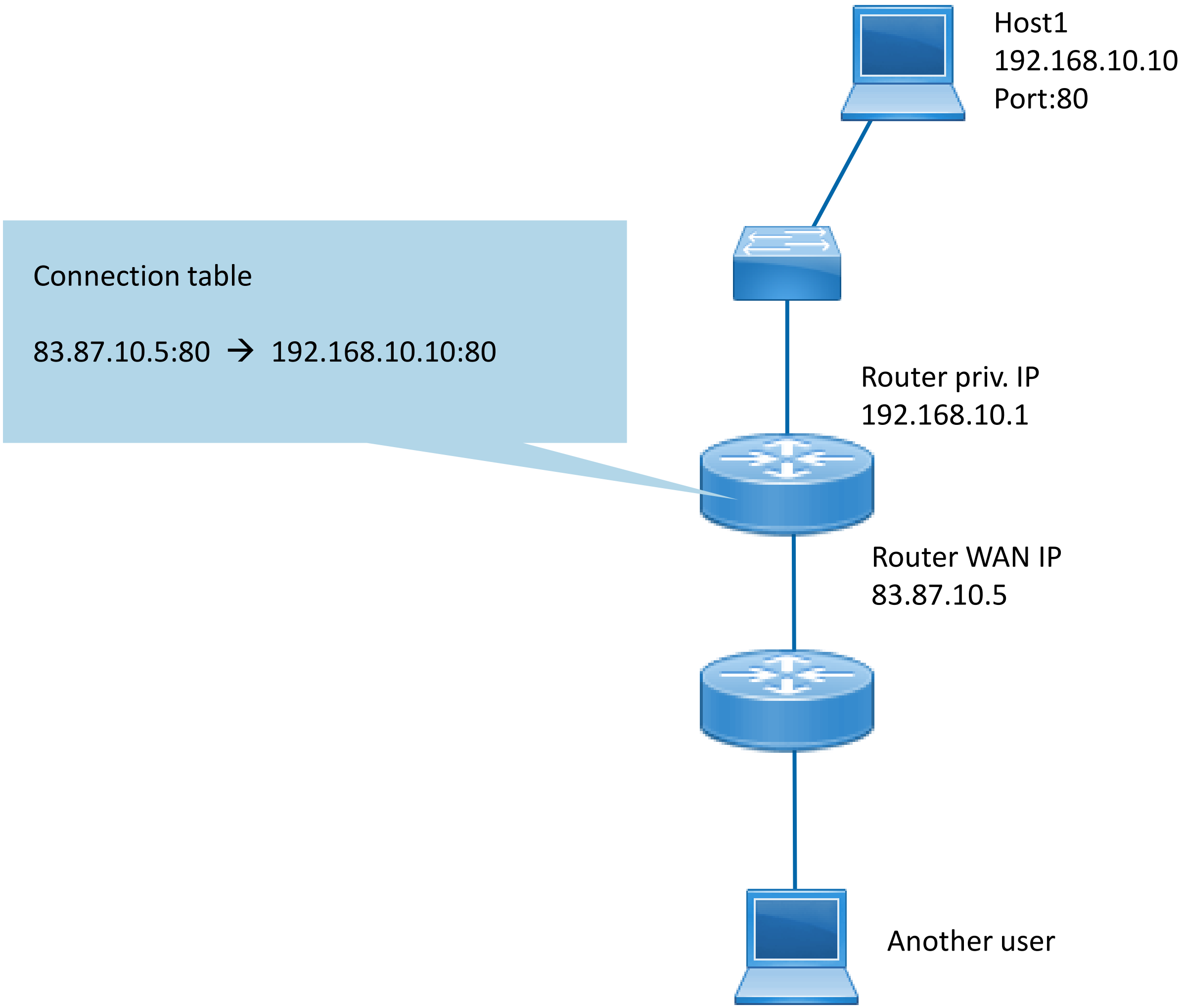


GEM MINE

LAYER 4 – ROUTING PRIVATE IP ADDRESSES

- Port forwarding
  - Basically the same like PAT / NAT
  - Another user wants to browse http://aurorafox.de
  - DNS returns 83.87.10.5 as IP
  - Another user browses 83.87.10.5 on port 80
  - Router takes request
  - Router looks in his connection table
  - Router forward request to 192.168.10.10:80
  - Another user gets website

  - DynDNS
  - ISP may offer DynDNS for one domain
  - Has to be configured at ISP and router



ISO OSI LAYERS

DHCP

- Dynamic Host Configuration Protocol
- Configuration parameters for network hosts
  - IP Address
  - Router / Standard Gateway
  - Subnet mask
  - DNS Server
  - Many more

- Benefits
  - Central and automatic TCP/IP configuration
  - Change of address of frequently moved clients is done centrally & automatically
  - No errors due to "manual configuration”
  - IP address assignment documentation

DHCP

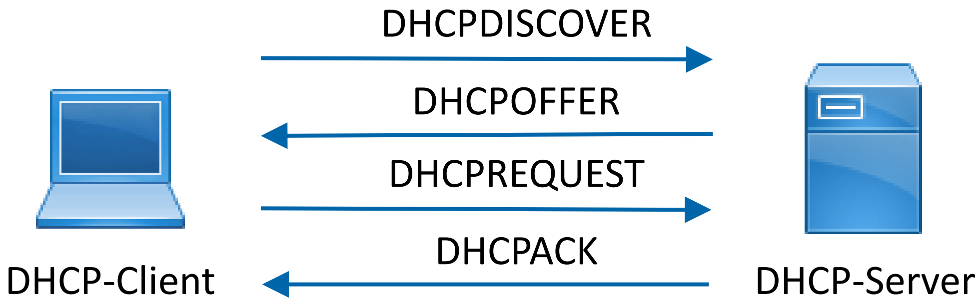
- IP assignment options
  - ***Automatic***
    Client receives a random IP address from a pool, which it uses again and again
  - ***Dynamic***
    Client receives a random IP address from a pool
    Usage is limited in time
  - ***Static***
    Client receives an IP address that was previously reserved for it
    Reservation is based on the MAC address

GEM MINE

DHCP

- IP assignment
  - Realized by broadcast messages
  - Consists of four steps

- Communication done via broadcast
- Using well-known port numbers
  - DHCP-Server: UDP port 67
  - DHCP-Client: UDP port 68



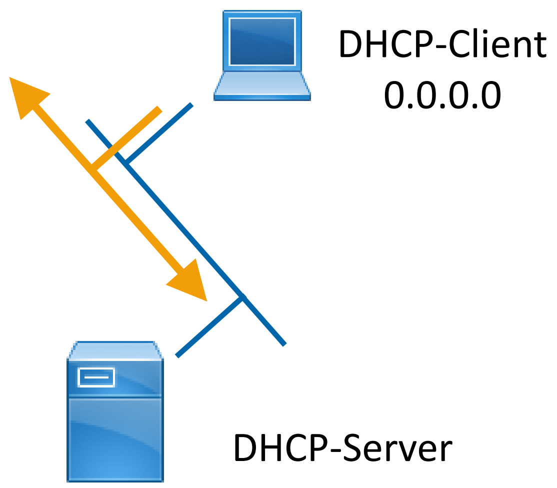
DHCP Message	Use
DHCPDISCOVER	Client broadcast to locate available servers
DHCPOFFER	Ser to client response offering conig. param.
DHCPREQUEST	Client broadcast requesting offered params-
DHCPDECLINE	Client to server notification that IP address is in use
DHCPACK	Server to client response confirming a request
DHCPNAK	Server to client response denying a request
DHCPRELEASE	Client to server request to relinquish IP address
DHCPINFORM	Client to server request for config. param.

ISO OSI LAYERS

DHCP PROCESS

- DHCPDISCOVER
  - When TCP/IP stack is initialized for the first time
  - If client is denied the requested IP address
  - When the previous IP address has been released

  - Client sends **DHCPDISCOVER** message
  - Contains the MAC address of the client and the computer name
  - The IP address of the client is 0.0.0.0 (it has none)
  - Sent to 255.255.255.255 (total broadcast, received by all)
  - Additionally the MAC is set to FF-FF-FF-FF-FF (ARP broadcast)



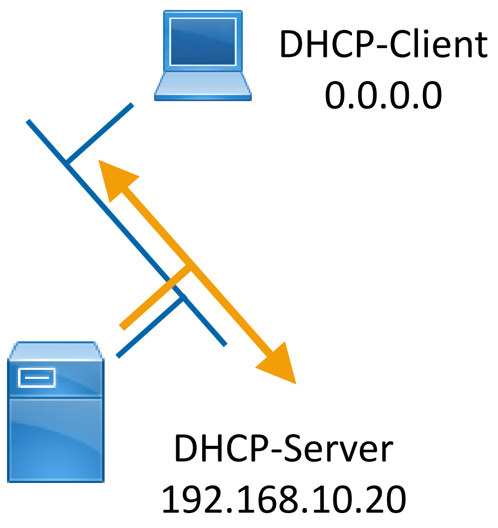
SRC-IP:	0.0.0.0
DST-IP:	255.255.255.255
SRC-MAC:	08-00-2A-3E-AC-3F
DST-MAC:	FF-FF-FF-FF-FF-FF
Client-ID:	08-00-2A-3E-AC-3F

ISO OSI LAYERS

DHCP PROCESS

- DHCPOFFER
  - All available DHCP server offer IP address

  - Server sends **DHCPOFFER** packet
  - Contains the offered IP address
    Subnetmask
    Leasetime
    Server IP address
  - Server reserves offered IP
  - Sent to 255.255.255.255
    (total broadcast, received by all)

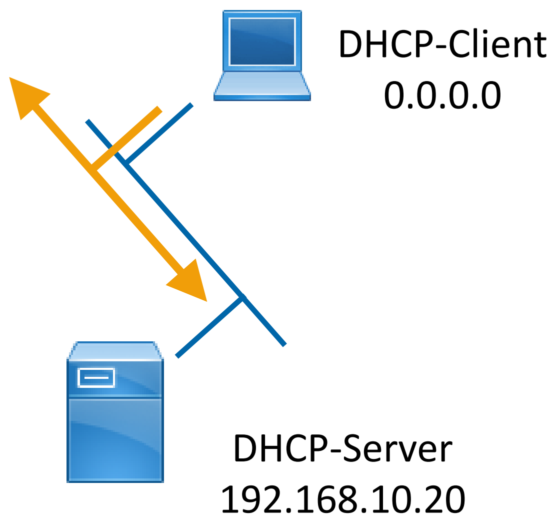


SRC-IP:	192.168.10.20
DST-IP:	255.255.255.255
SRC-MAC:	00-BC-01-12-CF-3D
DST-MAC:	FF-FF-FF-FF-FF-FF
Client-ID:	08-00-2A-3E-AC-3F
Offered IP:	192.168.10.55
Server IP:	192.168.10.20
Leasetime:	48 h

DHCP PROCESS

- DHCPREQUEST
  - Client still has no IP

  - Client sends **DHCPREQUEST** message
  - Contains the IP address of the server which responded first
  - The IP address of the client is 0.0.0.0 (it has none)
  - Sent to 255.255.255.255 (total broadcast, received by all)
  - Additionally the MAC is set to FF-FF-FF-FF-FF (ARP broadcast)
  - All DHCP server get this message and check if it is their IP.
    If not, the IP reservation is cancelled



SRC-IP: 0.0.0.0
DST-IP: 255.255.255.255

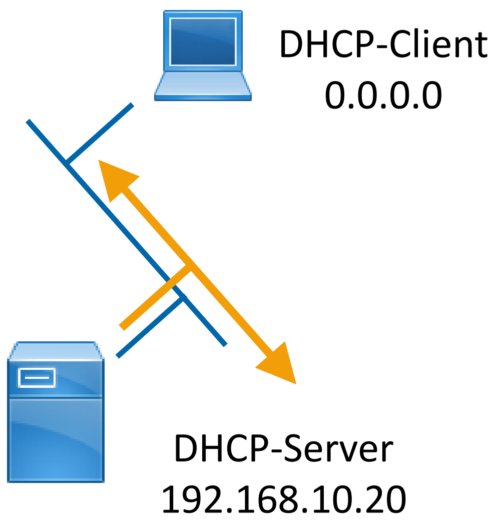
SRC-MAC:	08-00-2A-3E-AC-3F
DST-MAC:	FF-FF-FF-FF-FF-FF
Client-ID:	08-00-2A-3E-AC-3F
Offered IP:	192.168.10.55
Server IP:	192.168.10.20
Leasetime:	48 h

GEM MINE

DHCP PROCESS

- DHCPACK
  - DHCP server confirms offered IP address

  - Server sends **DHCPACK** packet
  - Contains the offered IP address
    Subnetmask
    Leasetime
    Server IP address
  - Server removes offered IP from the list of available IP addresses



SRC-IP: 192.168.10.20
DST-IP: 255.255.255.255

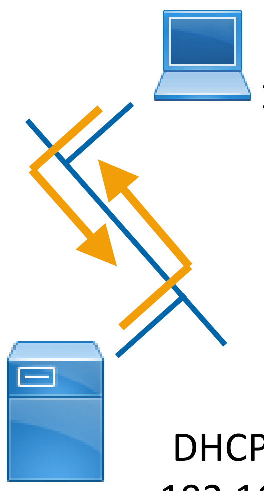
SRC-MAC: 00-BC-01-12-CF-3D
DST-MAC: FF-FF-FF-FF-FF-FF

Client-ID: 08-00-2A-3E-AC-3F
Offered IP: 192.168.10.55
Server IP: 192.168.10.20
Leasetime: 48 h

DHCP RENEWAL

- Lease get renewed by client after 50% of lease time
- If client cannot contact server, he tries again after 75%
- If he still cannot contact server, he drops his IP address and assigns an APIPA address from 169.254.0.1 to 169.254.255.254

- Clients send DHCPREQUEST unicast to DHCP server
- Server renews lease by sending DHCPACK
- If desired IP is not available, server sends DHCPNAK
- Client falls back to initial state



SRC-IP: 192.168.10.20
DST-IP: 255.255.255.255

SRC-MAC: 00-BC-01-12-CF-3D
DST-MAC: FF-FF-FF-FF-FF-FF

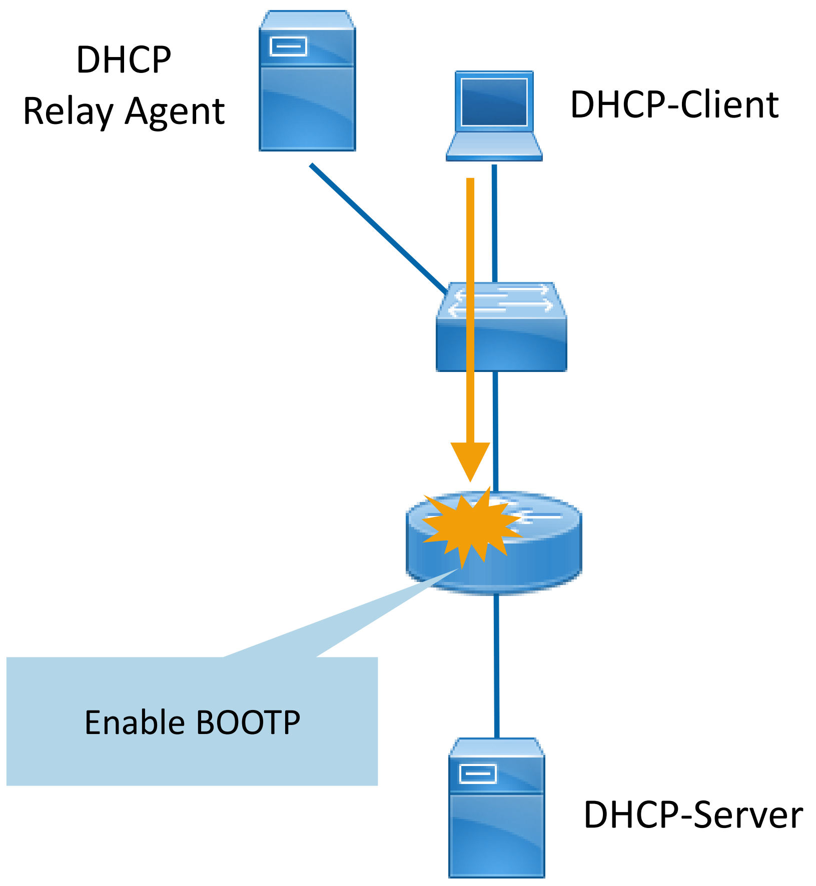
Client-ID: 08-00-2A-3E-AC-3F
Offered IP: 192.168.10.55
Server IP: 192.168.10.20
Leasetime: 48 h

DHCP DRAWBACKS

- Communication runs over broadcast
- If client and server are separated by router, DHCP will not work – Router block broadcasts

- Solution 1: enable BOOTP
  - To be configured on the router
  - Protocol used prior to DHCP
  - Enables broadcast for DHCP packets

- Solution 2: place DHCP-Relay Agent in client net
  - Agent is server with static IP
  - Agent knows DHCP server's IP
  - Agent can communicate unicast with DHCP…
  - … and client



DNS

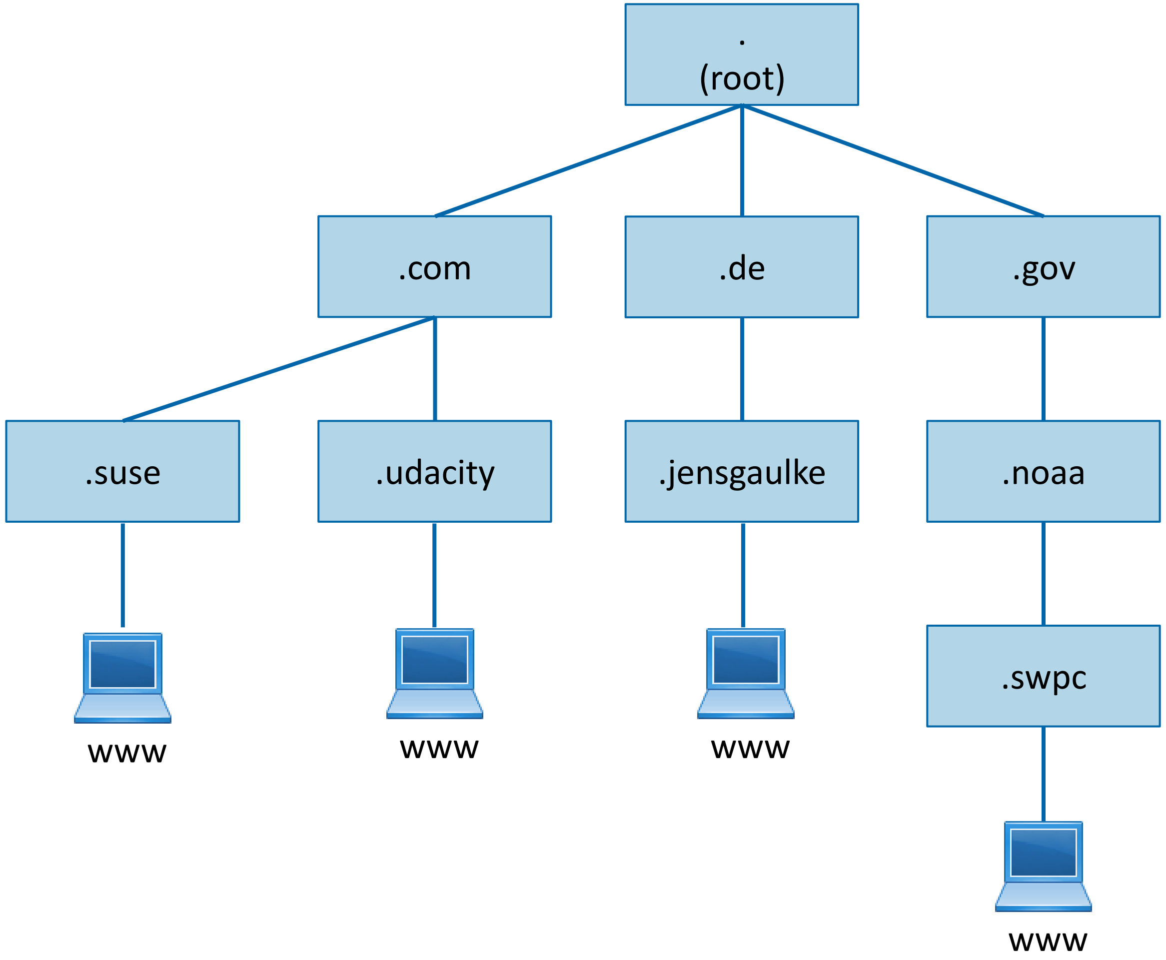
- Domain Naming System
  - Resolve names to IPs, and IPs to names
  - Internet "phonebook"

- Convenience for the user
  - Computer communicate by using IP
  - IP addresses are unique, but hard to remember
  - Names (www.udacity.com) are good to remember because of the association

- Where is it used?
  - Intranet
  - Internet
  - Active Directory Infrastructures

DNS STRUCTURE

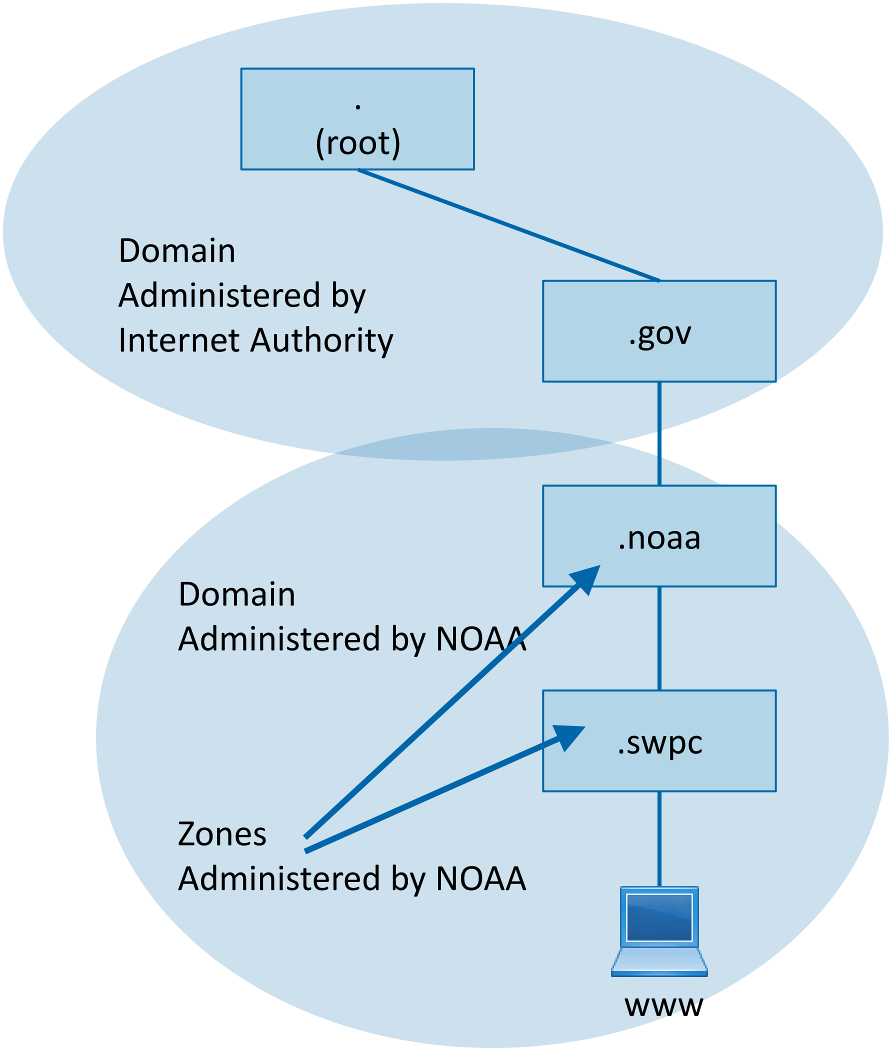
- Domain Naming System
  - Hierarchical, logical model
  - Start point: root (not freely selectable)
  - TLD: Top-Level-Domains (not freely selectable)
    Organizational domains (.com, .edu, .mil)
    Geographical domains (.de, .it, .ch, .nl)
  - Subdomains (freely selectable)
    can be registered
    Germany: DENIC
    International: INTERNIC
  - Endpoints
    Designate individual network resources



GEMMINE

DNS DOMAINS & ZONES

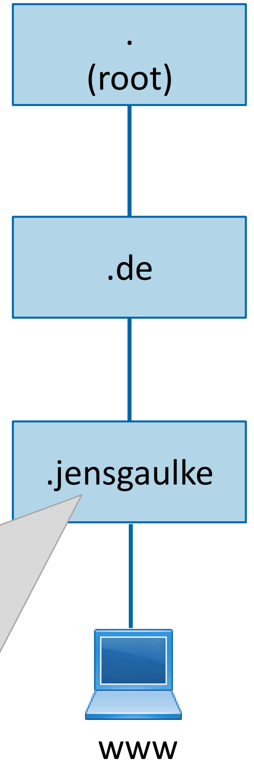
- Domain
  - A domain includes the entire subordinate DNS namespace. The term domain is also used when referring to content (what names does a domain contain?) or ownership (for whom is a domain registered?)
- Zone
  - A domain can be divided into several zones by delegating responsibility for subdomains. One also speaks of a zone if one means the physical realization - i.e. on which server and in which zone file the DNS records are located.



DNS ZONES

- Zone file
  - Part of the DNS configuration
  - Consists of a list of resource records (RR)
  - Describes a zone completely
  - must have exactly one SOA resource record …
  - … and at least one NS resource record.
- Zone vs domain
  - A zone can include an entire domain.
  - Normally subdomains are represented by their own zones.
  - Pointers - the NS Resource Records (NS-RR) - are used to refer to sub-zones, which may be located on other name servers → delegation

```
; jensgaulke.de
$TTL 3600
jensgaulke.de.   IN    SOA    ns0.iquer.net. hostmaster.iquer.net. (
                                     2018061801  ; Serial
                                     8H        ; refresh after 8 hours
                                     2H        ; retry after 2 hour
                                     168H        ; expire after 1 week
                                     1D)       ; minimum TTL of 1 day

                   ; Name Server
                   IN         NS         ns0.iquer.net.
                   IN         NS         ns2.iquer.net.
                   IN         NS         ns1.iquer.net.

                   ; Mail Exchanger
                   IN         MX         10 mx0.iquer.net.
                   IN         MX         10 mx1.iquer.net.

ns0.iquer.net.     IN         A          185.57.240.60
ns2.iquer.net.     IN         A          85.236.43.46
ns1.iquer.net.     IN         A          81.20.85.14
mx1.iquer.net.     IN         A          81.20.85.105
mx0.iquer.net.     IN         A          185.57.240.66
jensgaulke.de.     IN         A          185.57.242.34
www                IN         CNAME      jensgaulke.de.
```

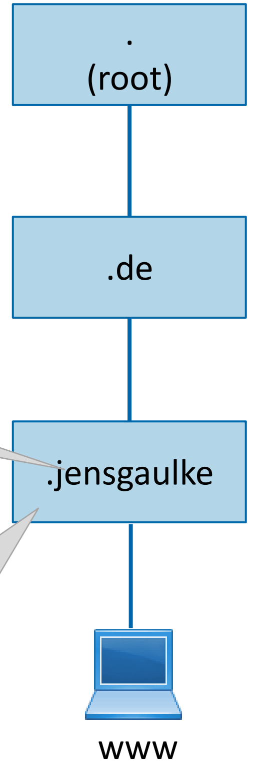


DNS ZONES

- High Availability
  - Outsource your web traffic to cloudfront
  - Do your own Load Balancing (Round Robin) (Remember my Pi-Cluster?)

ns0.iquer.net.	IN	A	185.57.240.60
ns2.iquer.net.	IN	A	85.236.43.46
ns0.iquer.net.	IN	A	81.20.85.14
mx1.iquer.net.	IN	A	81.20.85.105
mx0.iquer.net.	IN	A	185.57.240.66
www	IN	CNAME	server.cloudfront.net.
server.cloudfront.net.	IN	A	13.225.63.3
server.cloudfront.net.	IN	A	13.225.63.95
server.cloudfront.net.	IN	A	13.225.63.94
server.cloudfront.net.	IN	A	13.225.63.48

ns0.iquer.net.	IN	A	185.57.240.60
ns2.iquer.net.	IN	A	85.236.43.46
ns0.iquer.net.	IN	A	81.20.85.14
mx1.iquer.net.	IN	A	81.20.85.105
mx0.iquer.net.	IN	A	185.57.240.66
www	IN	CNAME	jensgaulke.de.
jensgaulke.de.	IN	A	185.57.242.34
jensgaulke.de.	IN	A	185.57.242.35
jensgaulke.de.	IN	A	185.57.242.36
jensgaulke.de.	IN	A	185.57.242.37



ISO OSI LAYERS

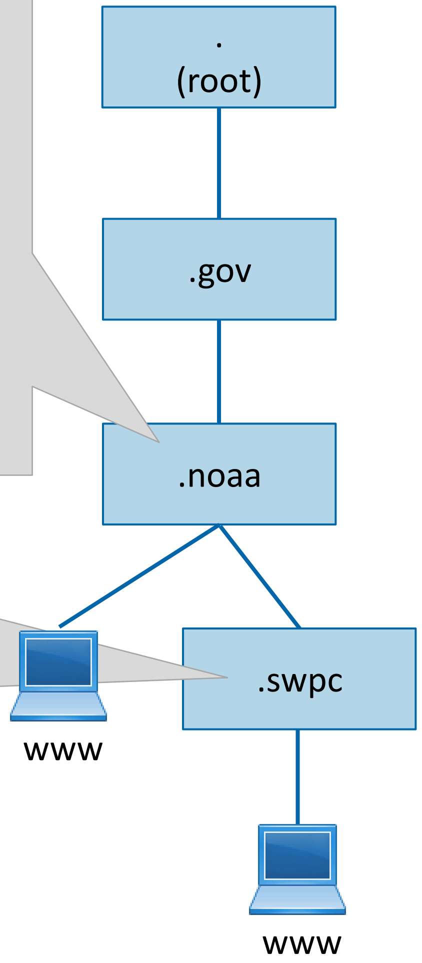
DNS ZONES

- Delegation
  - Namespace can be divided into zones
  - zone files can be stored on different servers
  - Improves performance (smaller zone files)
  - Subdomains can easily be added

- This is no real zone file!
  Example is fictitious!

```
noaa.gov.   IN    SOA   dns02.woc.noaa.gov. hostmaster.noaa.gov. (
                         2018061801  ; Serial blablabla

                         ; Name Server
                         IN          NS          dns02.woc.noaa.gov.
                         IN          NS          ns-nw.noaa.gov.
                         IN          NS          ns-e.noaa.gov.

swpc.noaa.gov.           IN          NS          dns.swpc.noaa.gov.
dns.swpc.noaa.gov.       IN          A           140.172.226.23
dns02.woc.noaa.gov.      IN          A           140.90.33.207
ns-nw.noaa.gov.          IN          A           140.172.17.237
ns-e.noaa.gov.           IN          A           140.90.33.237
www                      IN          A           65.9.77.16
...
```

```
; swpc.noaa.gov
$TTL 3600
swpc.noaa.gov.   IN    SOA   dns.swpc.noaa.gov swpc-it.noaa.gov (
                              20181801  ; Serial blablabla

                              ; Name Server
                              IN          NS          dns.swpc.noaa.gov.

dns.swpc.noaa.gov.            IN          A           140.172.226.23
www                           IN          A           13.225.63.122
```



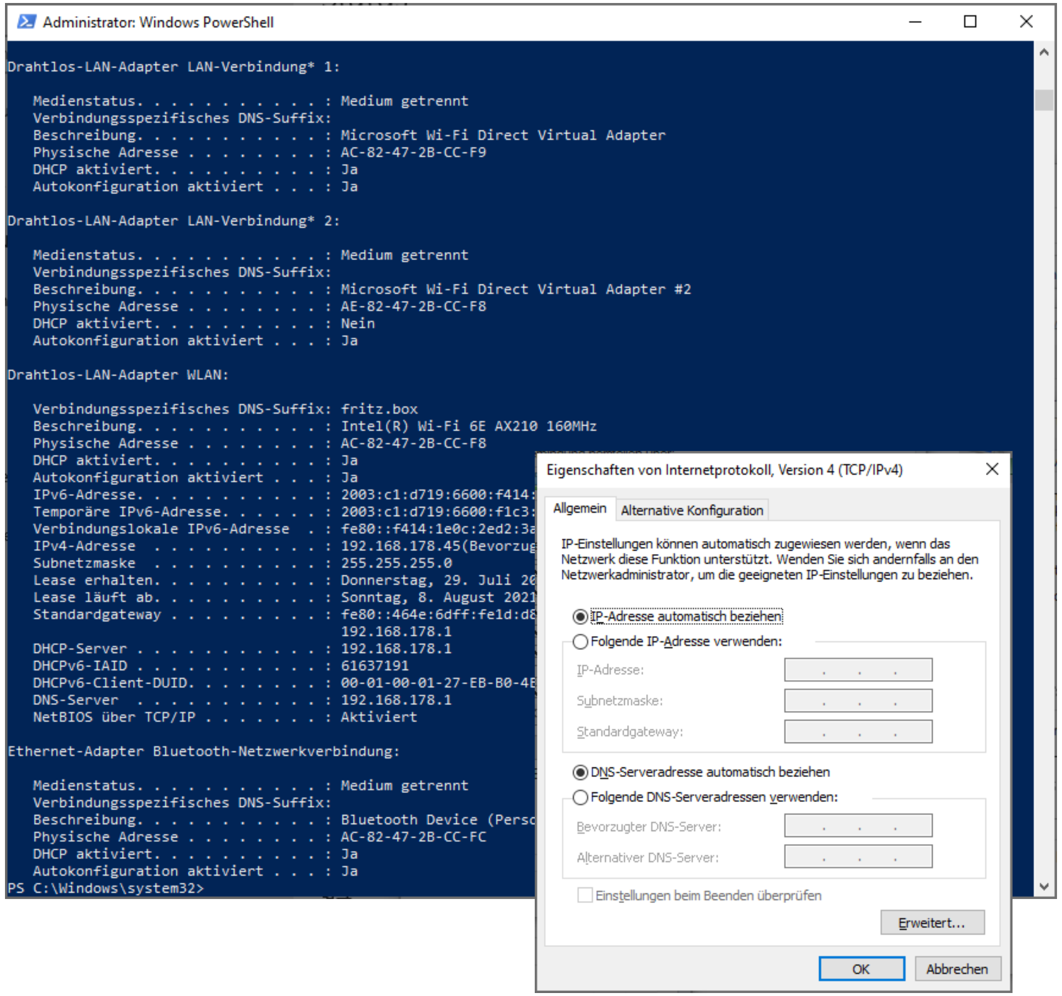
ISO OSI LAYERS

DNS NAME RESOLUTION PROCESS

- Client tries to resolve "hard coded names"
  - *Linux*: /etc/hosts
  - *Windows*: c:\windows\system32\drivers\etc\hosts
  - If name is found, client makes connection via IP address

- Client tries to resolve name from dns resolver cache
  - *Linux*: sudo /etc/init.d/dns-clean restart
  - *Windows*: clear cache with ipconfig /flushdns
  - If name is found, client makes connection via IP address

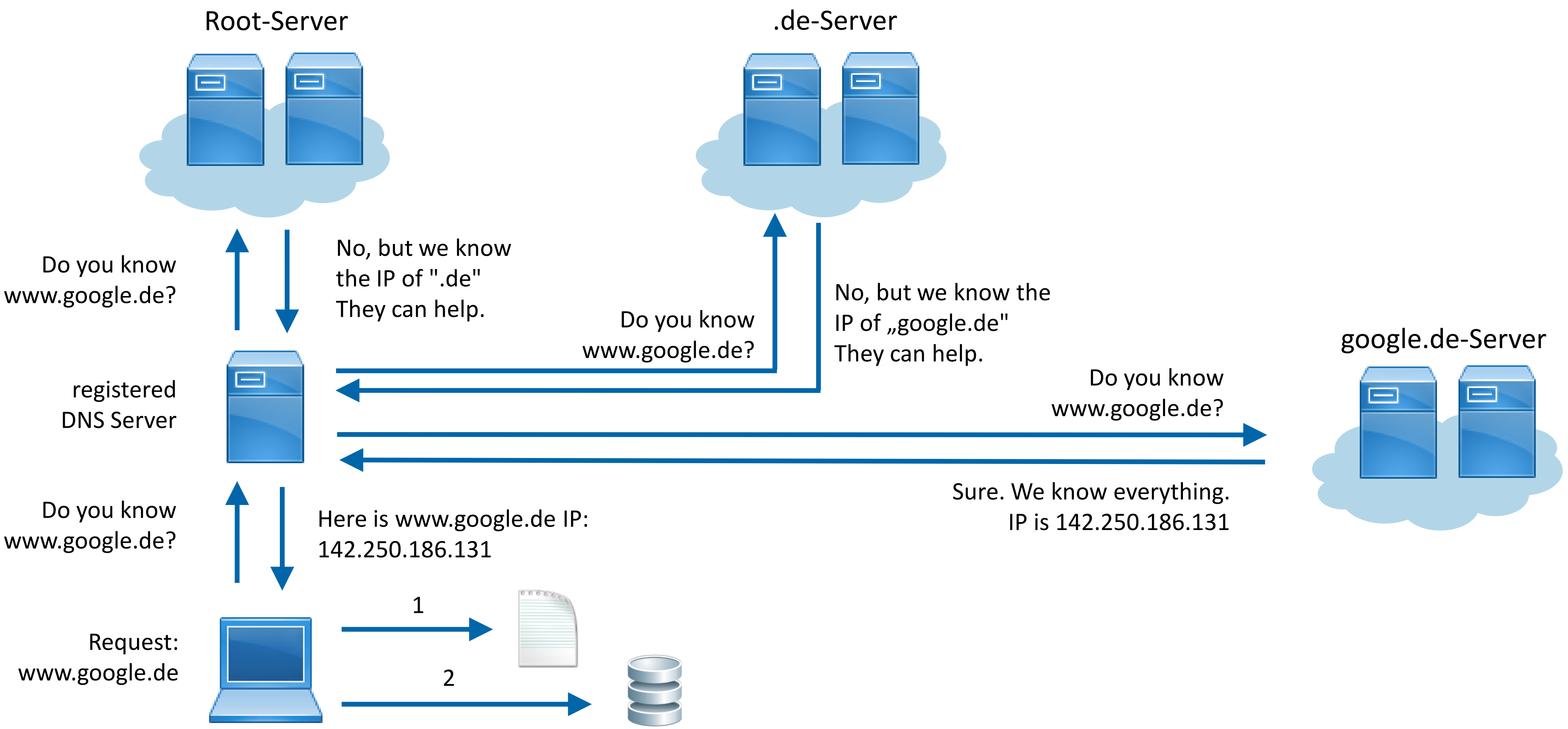
- Client tries to contact DNS server for name resolution
  - DNS Server usually part of DHCP configuration
  - Why are there two DNS entries in Windows?



ISO OSI LAYERS

GEM MINE

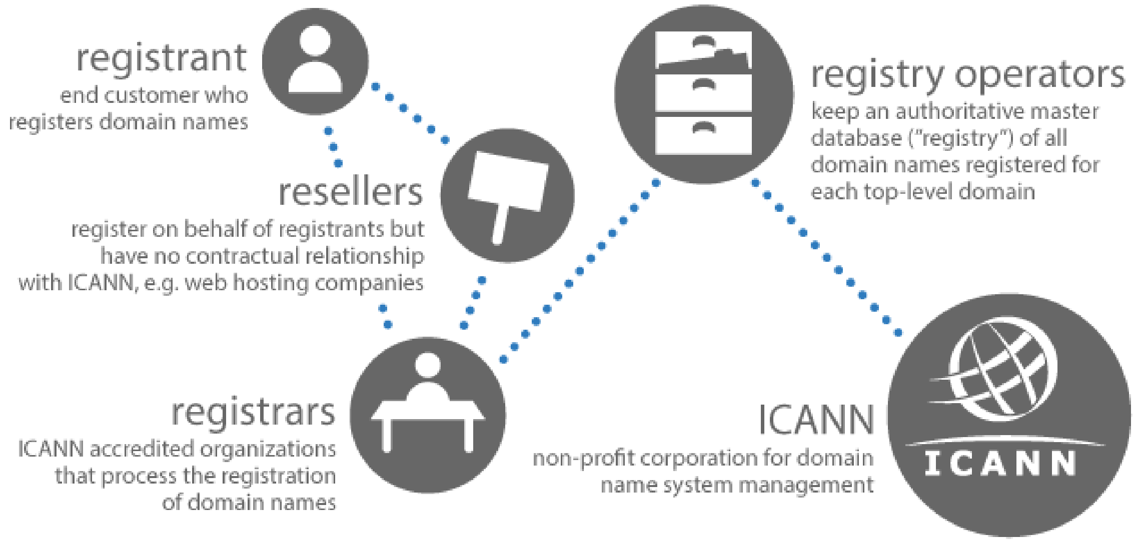
DNS NAME RESOLUTION PROCESS



GEM MINE

DNS REGISTRATION PROCESS

- Domain Registrant must register with an ICANN accredited registrar
  - Germany: DENIC
- Registrar will check if domain name is available
- Registrar creates WHOIS-entry
- Also possible: register domain through domain reseller
  - e.g. Strato



https://whois.icann.org/en/domain-name-registration-process
https://www.denic.de/ueber-denic/mitglieder/liste/

GEM MINE

DNS PROPAGATION PROCESS

- Why does it take up to 24h for a change to take effect?
  - The name servers are registered with the registry immediately after the update
  - It can take some time until other name servers have fetched the new information
  - This depends mainly on the so-called TTL (Time To Live), which each entry in the DNS has
    Depending on the size of the TTL, it can take up to 24 h (in rare cases even 72 hours) until another name server fetches the new information
  - Recommendation from RIPE NCC for small and stable zones: 86400 ≙ 24 hours.

```
; jensgaulke.de
$TTL 86400
jensgaulke.de.   IN    SOA    ns0.iquer.net.
hostmaster.iquer.net. (
                              2018061801  ; Serial
                              8H          ; refresh after 8 hours
                              2H          ; retry after 2 hour
                              168H        ; expire after 1 week
                              1D)         ; minimum TTL of 1 day

                  ; Name Server
                  IN          NS          ns0.iquer.net.
                  …

ns0.iquer.net.    IN          A           185.57.240.60
…
jensgaulke.de.    IN          A           185.57.242.34
www               IN          CNAME       jensgaulke.de.
```

DNS ZONE TRANSFER

- DNS is a distributed system
  - Primary DNS: hosts the original zone file
  - Secondary DNS: hosts a copy of the zone file
  - But: Secondary DNS may be master for another zone, therefore it is not a clear master-slave relationship

- Primary DNS changes zone file entries
  - We add a new entry
  - This requires zone record replication
  - 1 – transmit the whole zone file (AXFR)
  - 2 – transmit the changes (incremental transfer, IXFR)

DNS ZONE TRANSFER

- DNS Notify
  - Master server notifies certain secondary DNS servers that changes have occurred in the zone
  - Secondary servers then check whether a zone transfer must be initiated
  - Master server has a list of secondary DNS servers, containing IP addresses

  - Master server changes an entry in a zone
  - The "serial" field in the SOA entry is updated on the master server
  - Master server sends a notification message to the servers from the list
  - The secondary servers initiate an SOA request to the master server
  - Does the master server have a more recent version of the zone ?
  - If the master server's zone is more recent, the secondary server initiates a zone transfer (AXFR, IXFR)

  - AXFR vulnerability issues: https://www.acunetix.com/blog/articles/dns-zone-transfers-axfr/

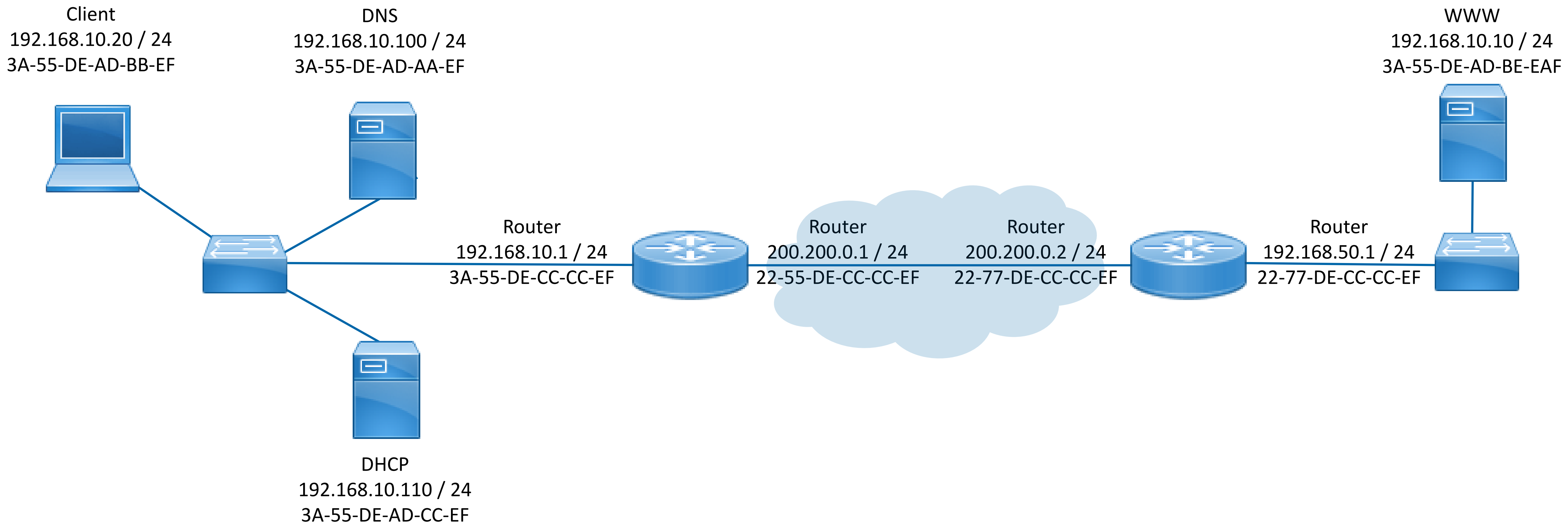
GEM MINE

DNS ZONE TRANSFER

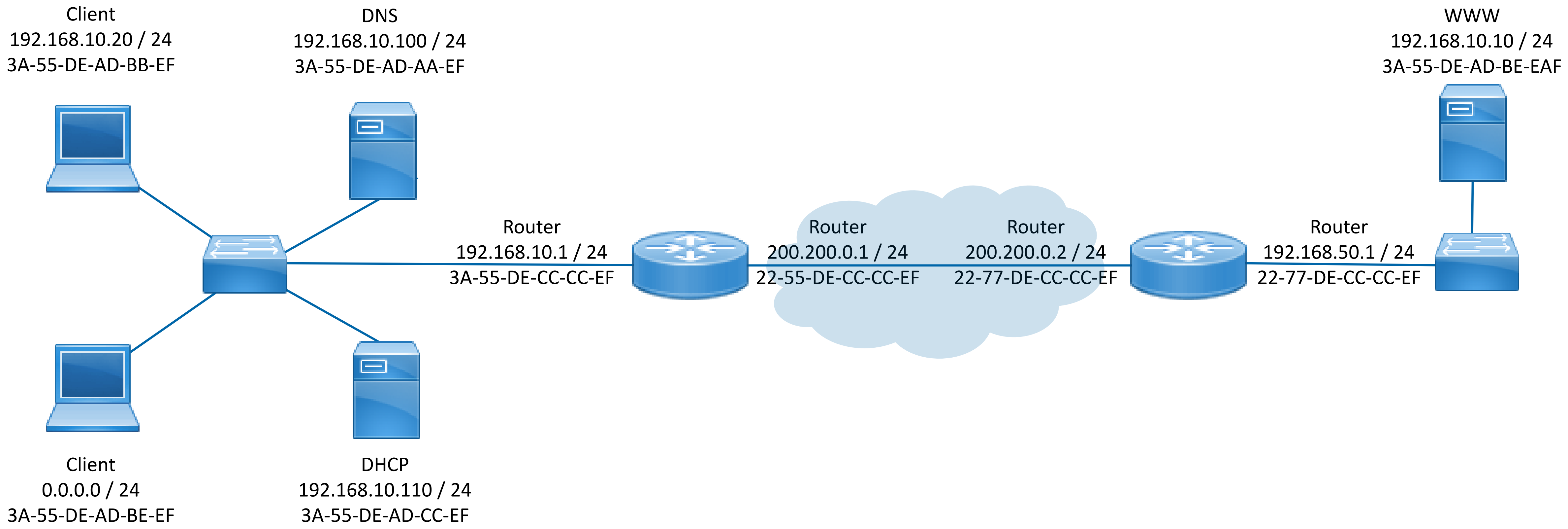
- What does SOA mean for transfers?
  - *Serial number*
    We talked about this
  - *Refresh interval*
    Specifies how often a secondary DNS server tries to update the zone
  - *Retry interval*
    If the secondary DNS server cannot reach the master server, it tries to contact it again after the interval specified here
  - *Expire interval*
    If a secondary DNS server cannot reach its master for the time interval specified here, it will no longer answer any queries for this zone anymore
  - *TTL*
    Specifies how long queries are cached on other DNS servers that are not authorized for the zone.

```
; jensgaulke.de
$TTL 86400
jensgaulke.de.   IN    SOA    ns0.iquer.net.
hostmaster.iquer.net. (
                    2018061801  ; Serial
                    8H          ; refresh after 8 hours
                    2H          ; retry after 2 hour
                    168H        ; expire after 1 week
                    1D)         ; minimum TTL of 1 day
```

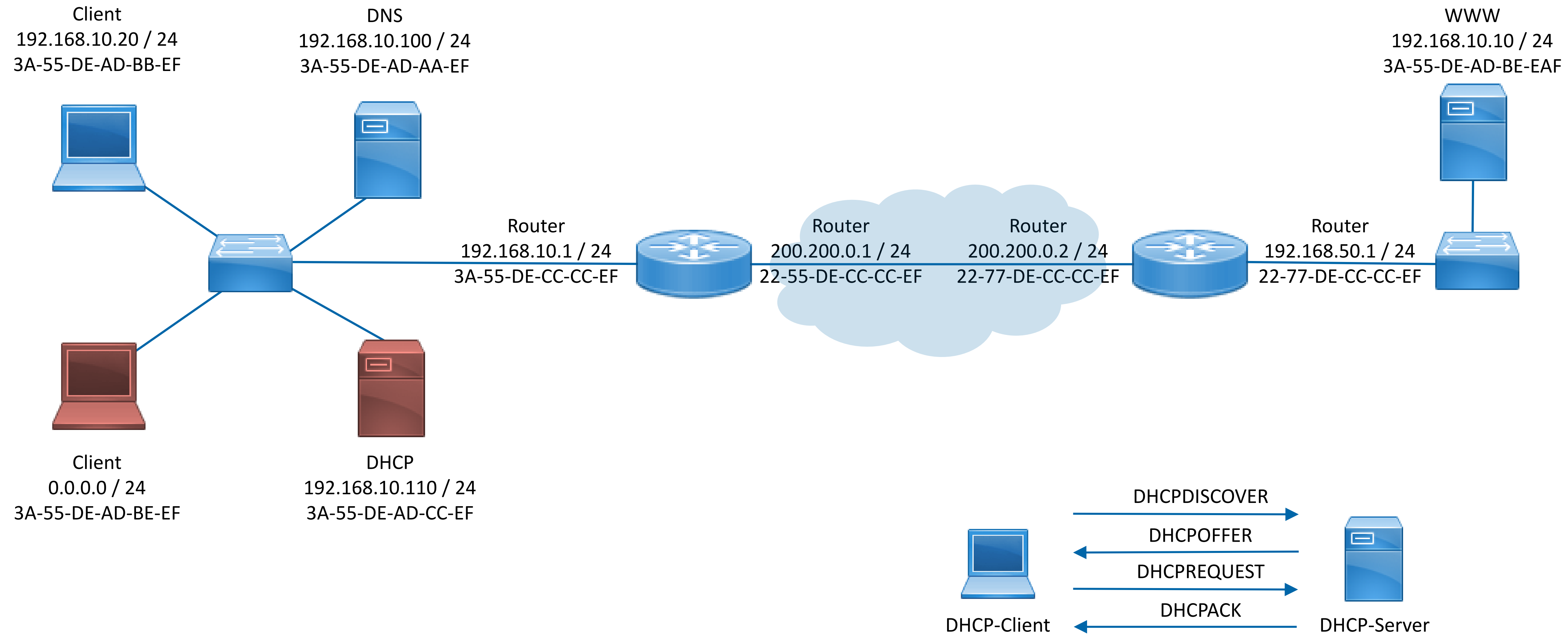
COMPLETE EXAMPLE



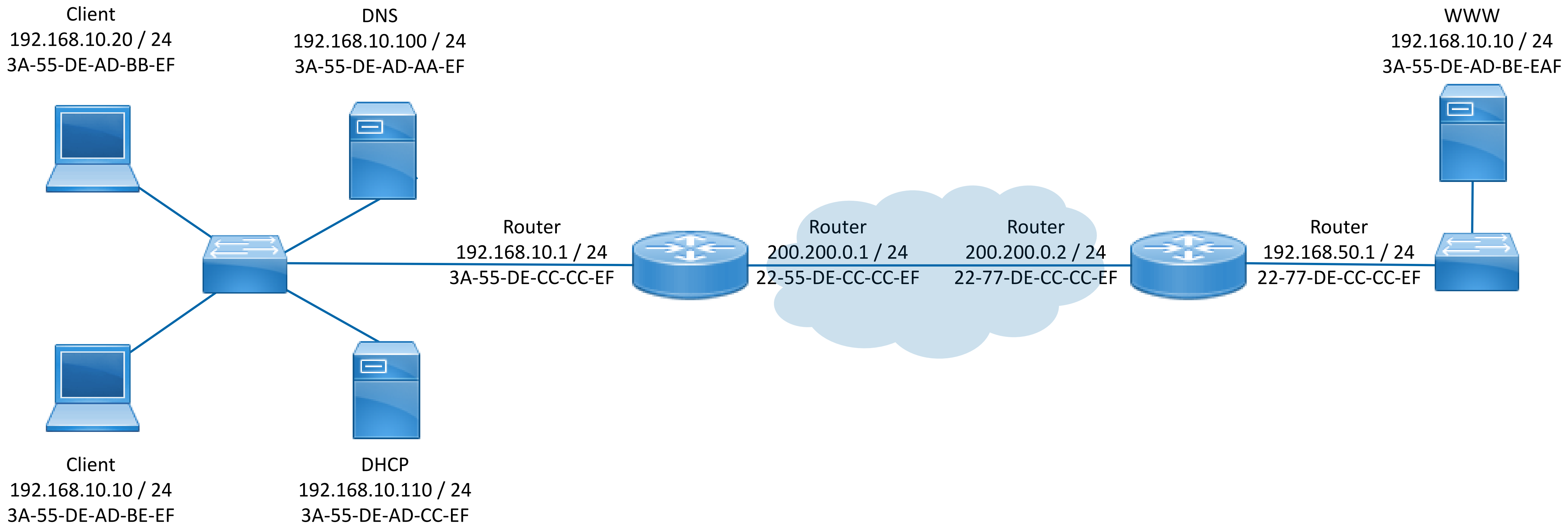
COMPLETE EXAMPLE



COMPLETE EXAMPLE

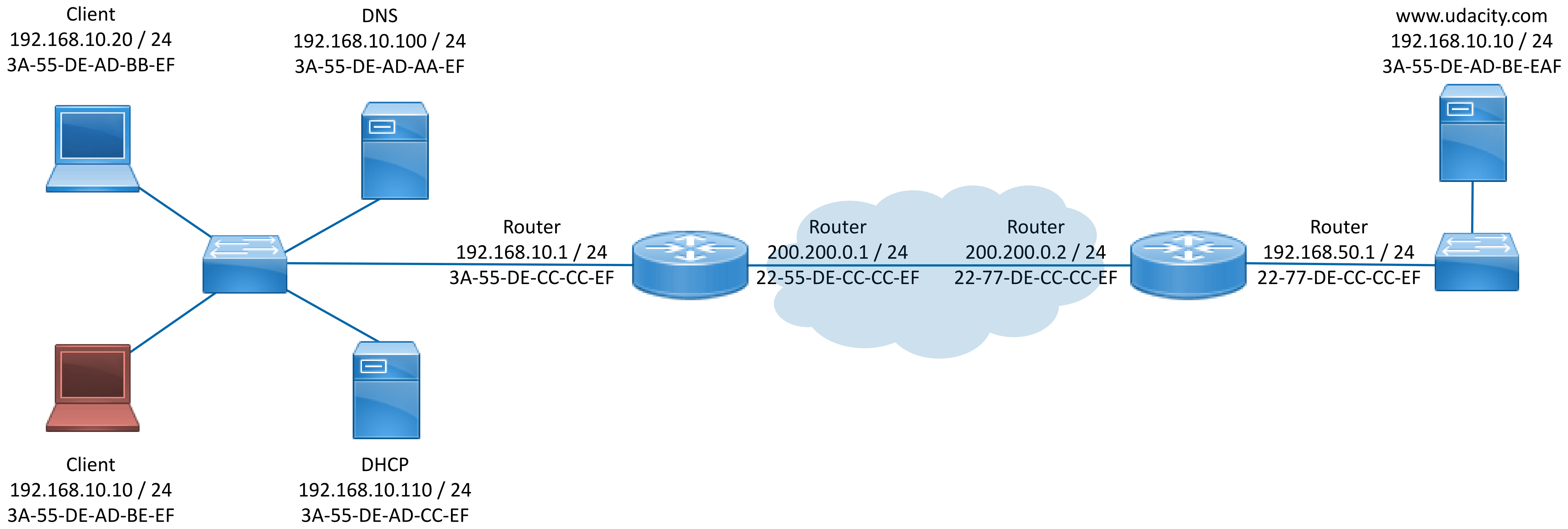


COMPLETE EXAMPLE



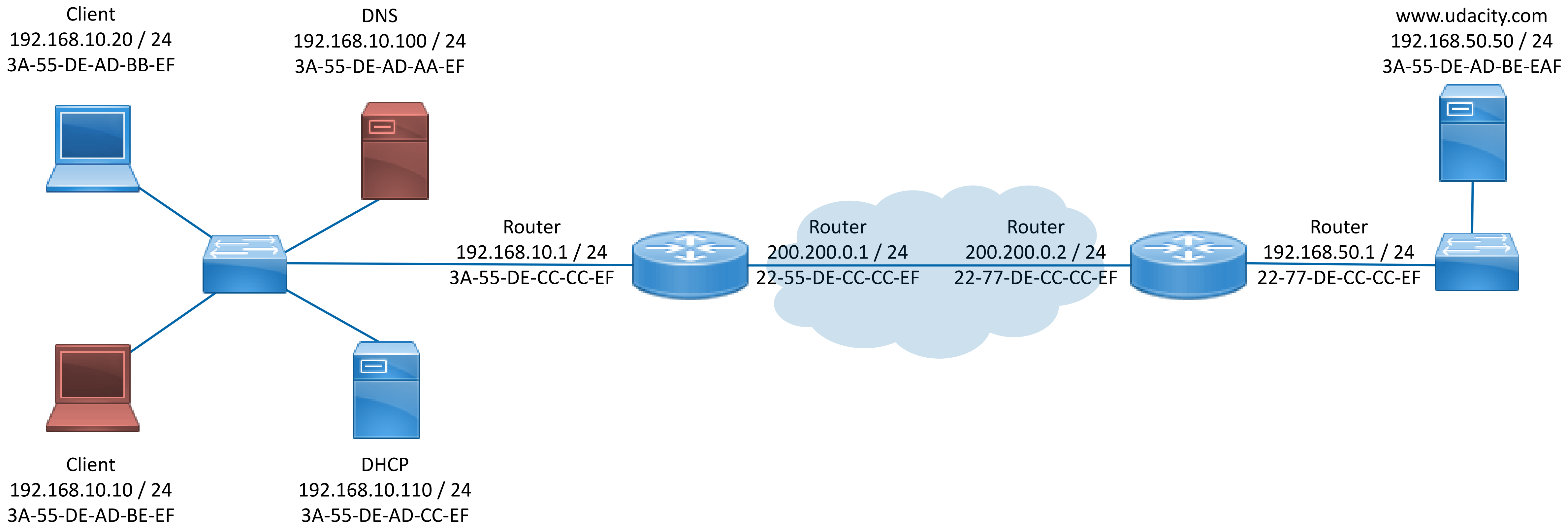
COMPLETE EXAMPLE

GEM MINE



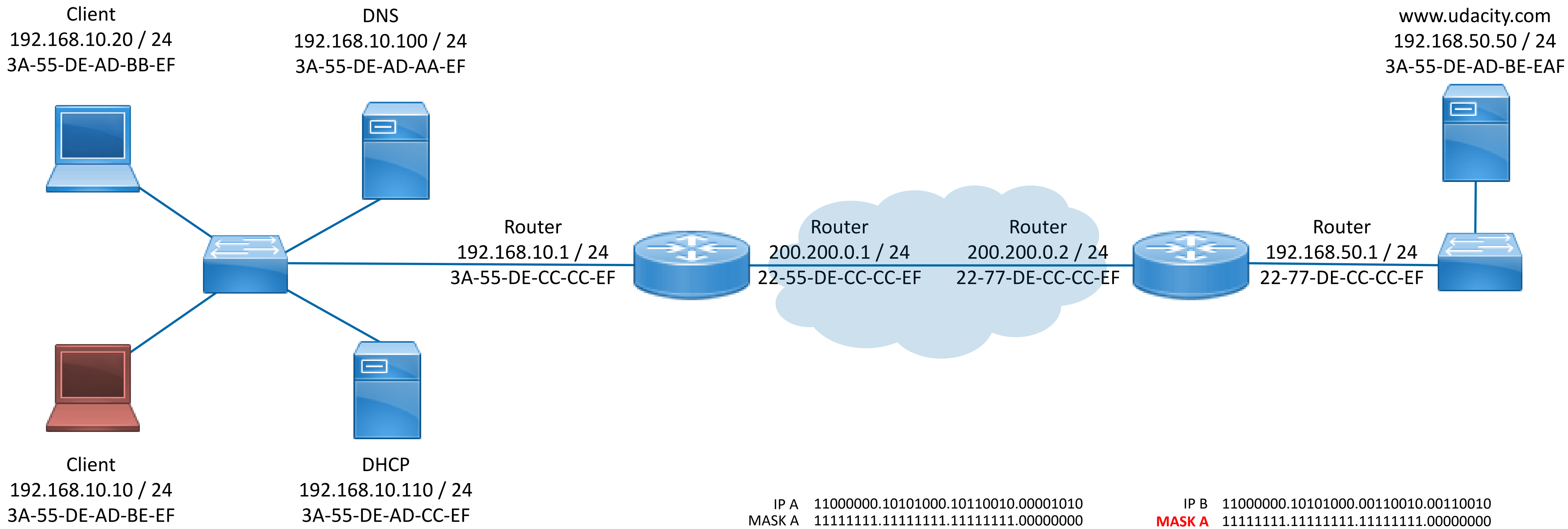
HTTP GET www.udacity.com/index.html

COMPLETE EXAMPLE



HTTP GET www.udacity.com/index.html
IP?
192.168.50.50!

COMPLETE EXAMPLE



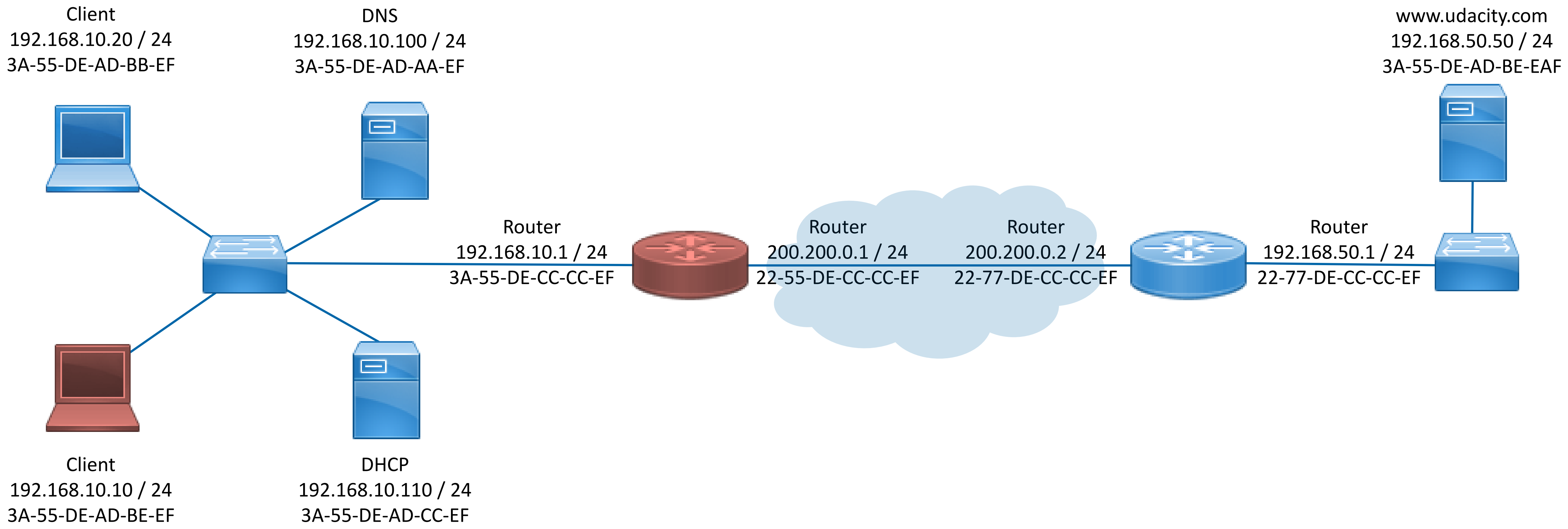
IP A	11000000.10101000.10110010.00001010
MASK A	11111111.11111111.11111111.00000000
IP-A(M)	11000000.10101000.10110010.00000000

IP B	11000000.10101000.00110010.00110010
MASK A	11111111.11111111.11111111.00000000
IP-B(M)	00001010.10101000.10110010.00000000

IP-A(M)	11000000.10101000.10110010.00000000
IP-B(M)	11001010.10101000.00110010.00000000
XOR	11001010.00000000.10000000.00000000

COMPLETE EXAMPLE

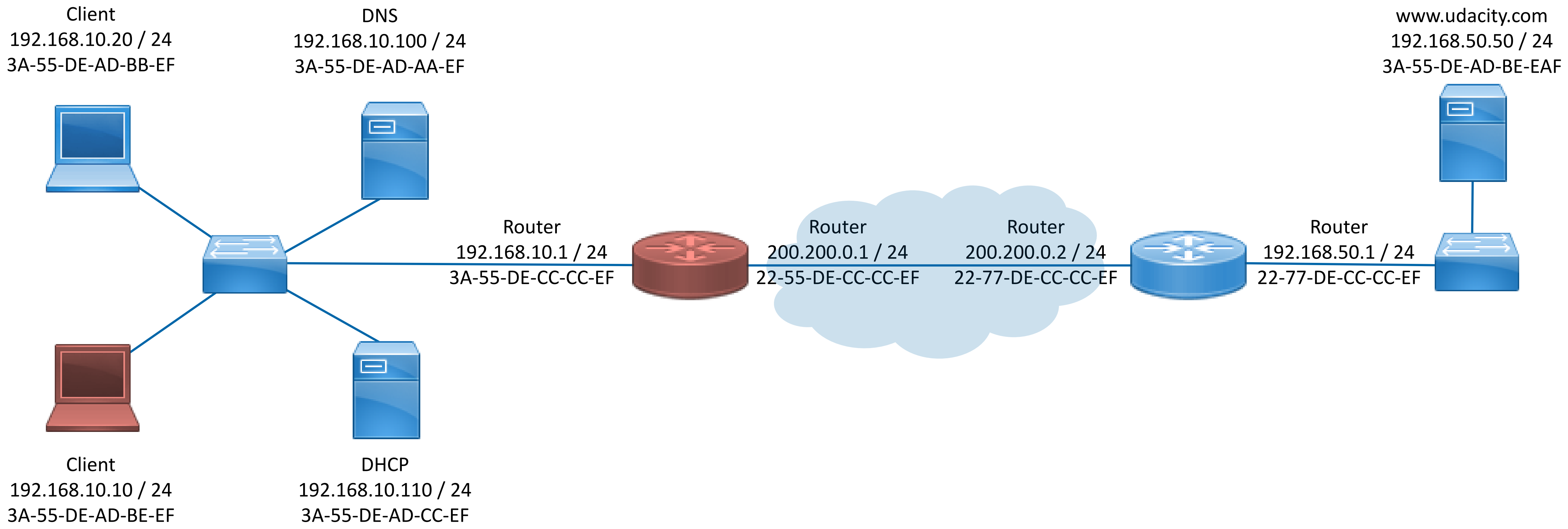
GEM MINE



Destination not in subnet.
Packet needs to be sent to
Gateway!

COMPLETE EXAMPLE

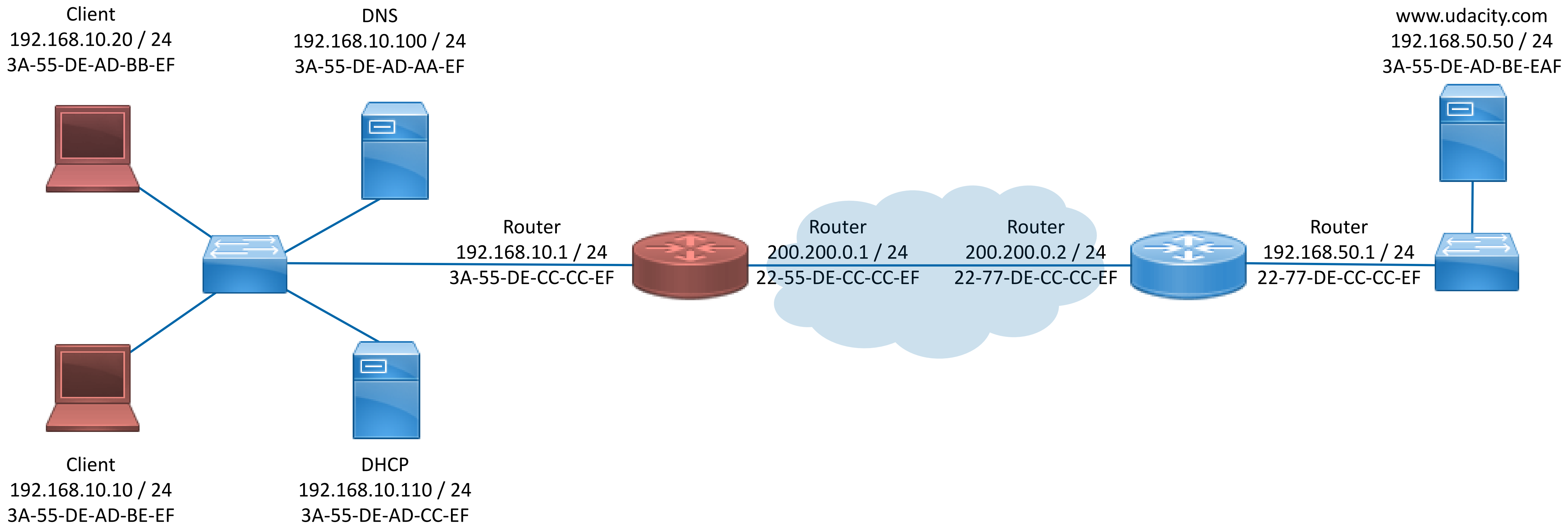
GEM MINE



Gateway address is 192.168.10.1
I need MAC!
ARP broadcast: WHO HAS?

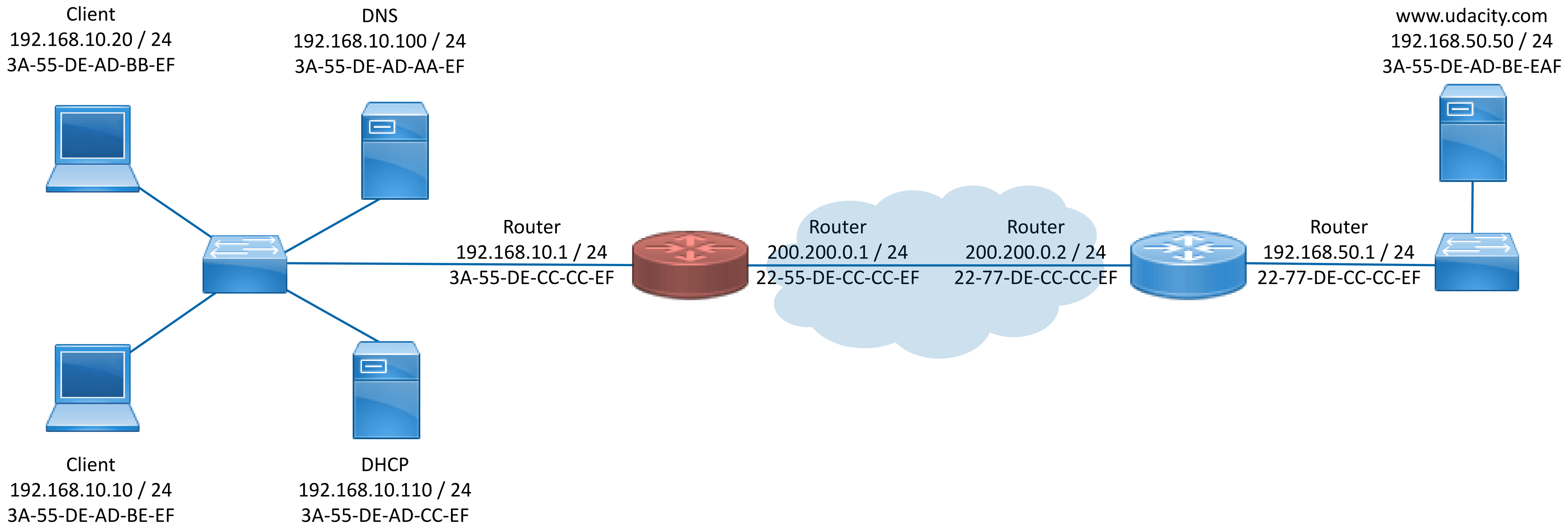
COMPLETE EXAMPLE

GEM MINE



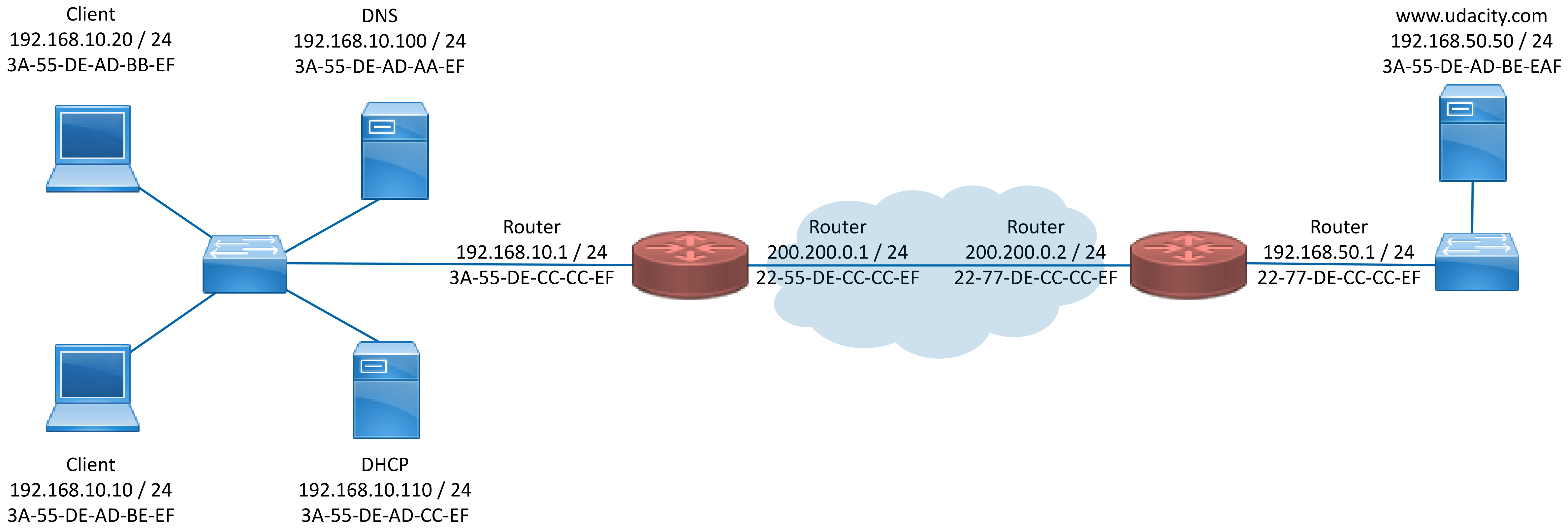
Client here: My ARP Table says:
192.168.10.1 has 3A-55-DE-CC-CC-EF
(Client was faster than router. That‘s life)

COMPLETE EXAMPLE



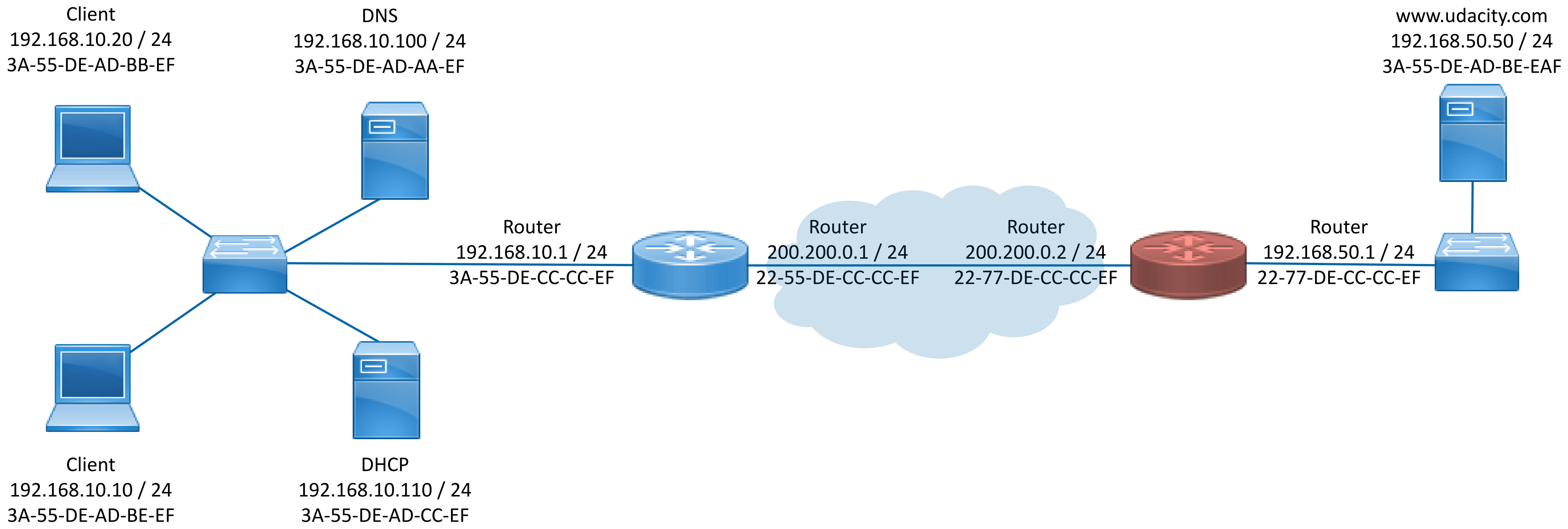
OK.
Packet sent to Router

COMPLETE EXAMPLE



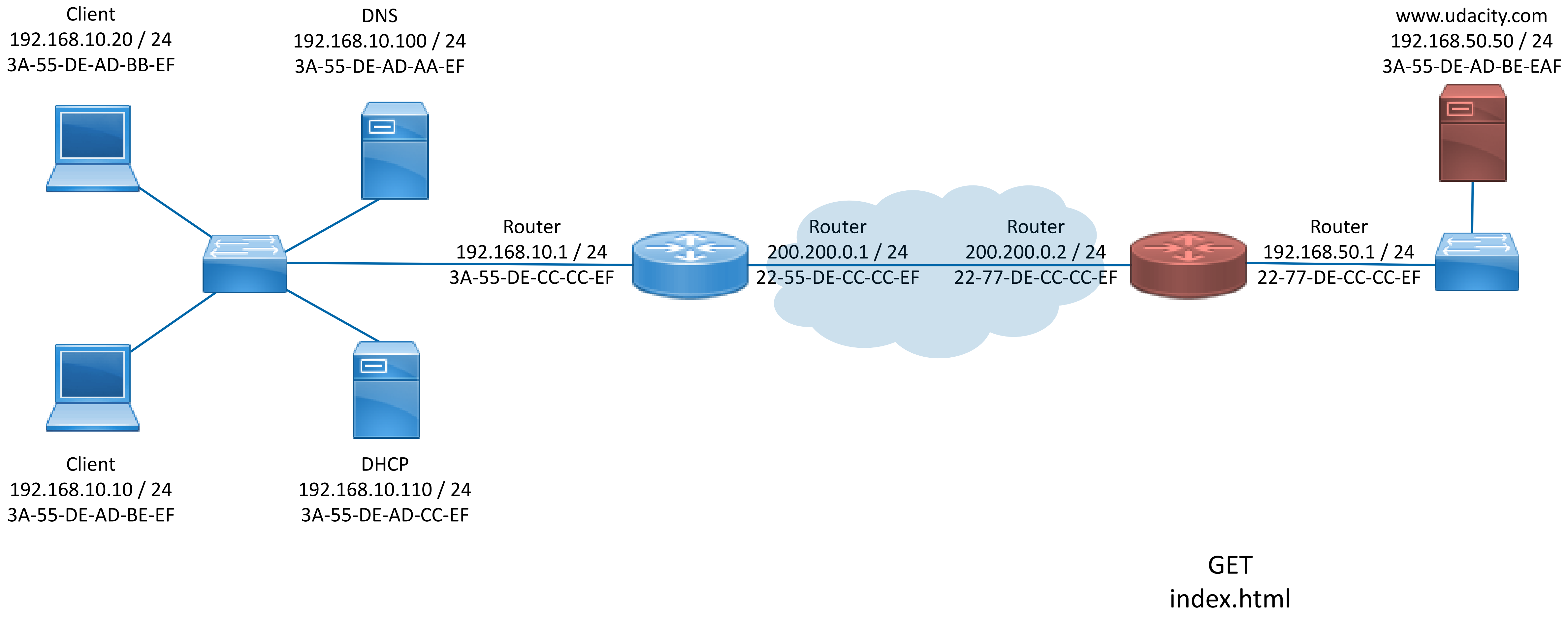
Router needs to NAT / PAT.
Sending packet to peer router

COMPLETE EXAMPLE

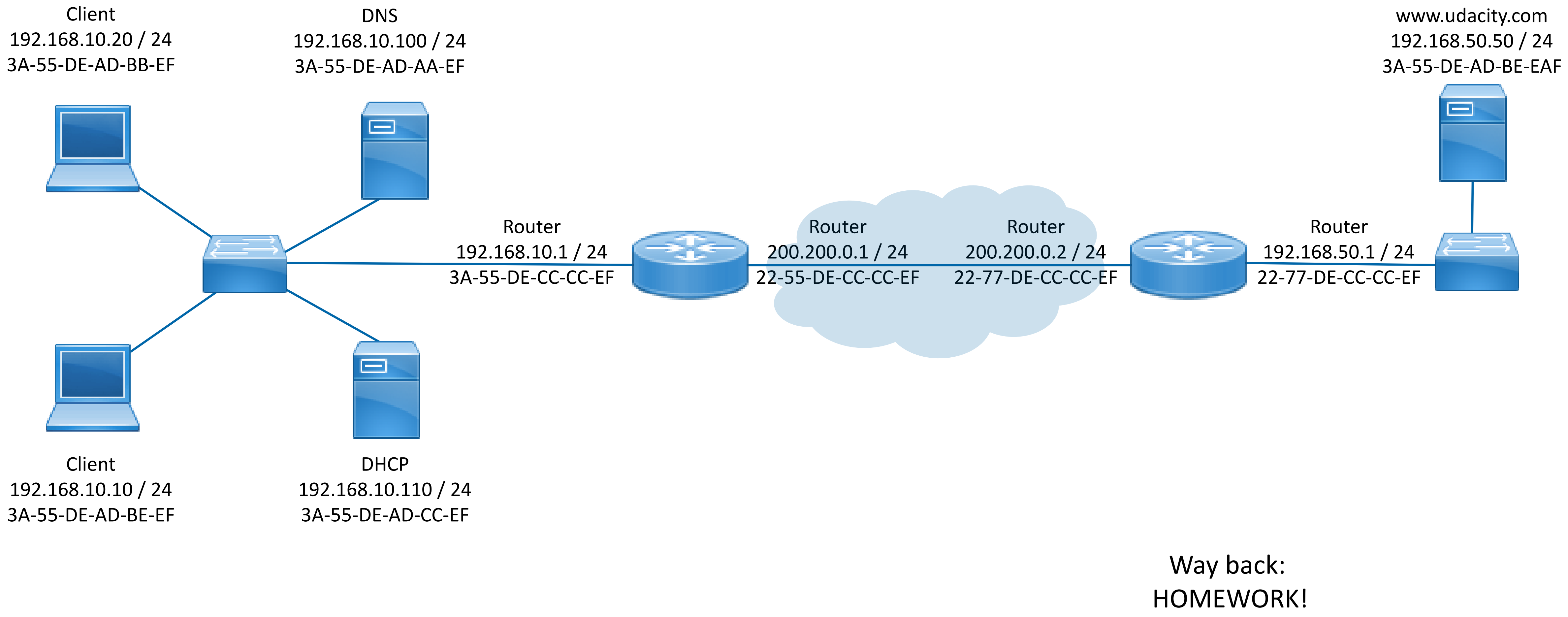


Yes…
192.168.50.50 is in my subnet

COMPLETE EXAMPLE



COMPLETE EXAMPLE

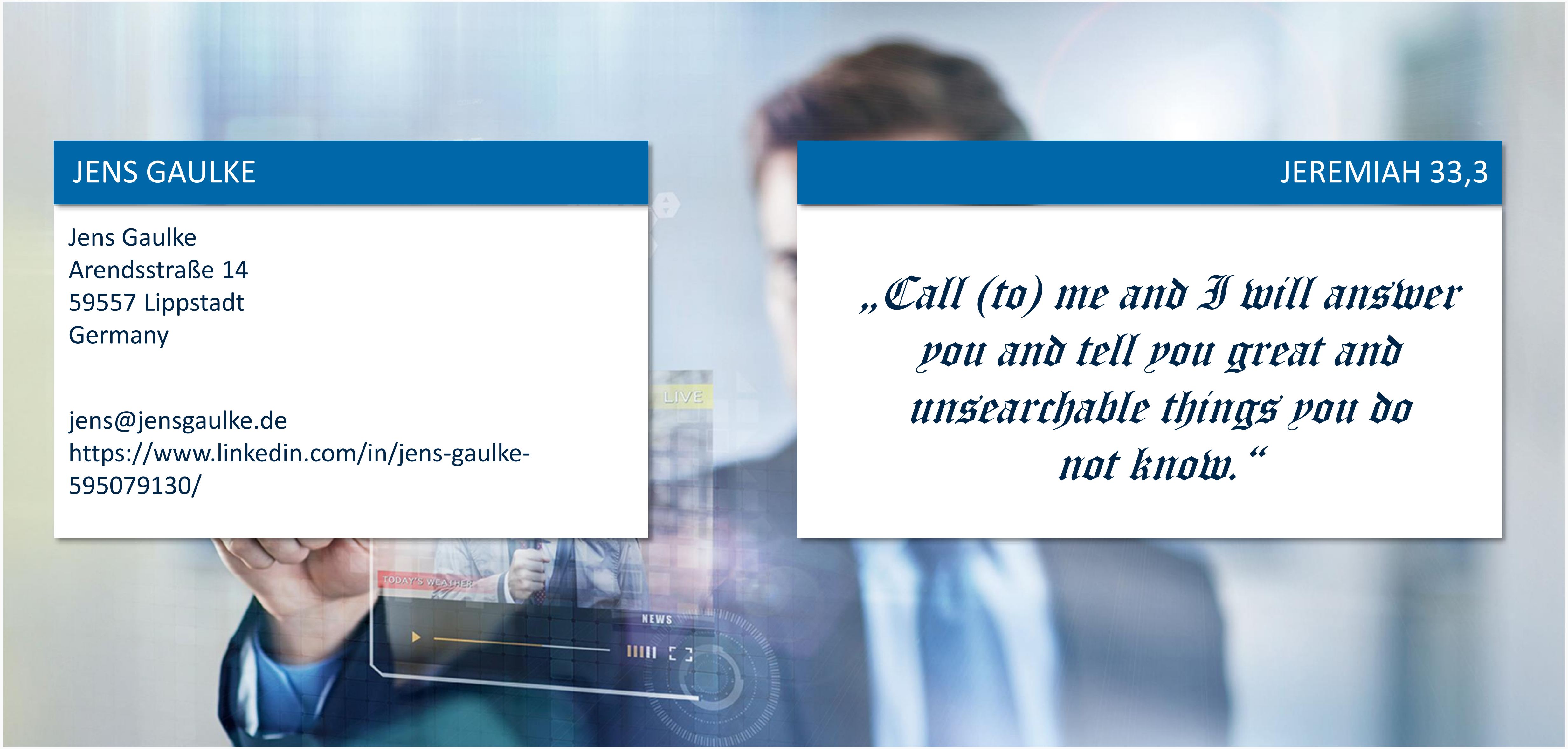


THE END

Thank you for your attention!

CONTACT

GEM MINE



JENS GAULKE

Jens Gaulke
Arendsstraße 14
59557 Lippstadt
Germany

jens@jensgaulke.de
https://www.linkedin.com/in/jens-gaulke-595079130/

JEREMIAH 33,3

„Call (to) me and I will answer you and tell you great and unsearchable things you do not know."