# Communication Networks

## Spring 2024

Lukas Röllin

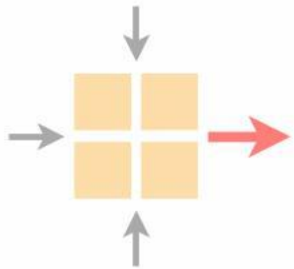
https://comm-net.ethz.ch/

ETH Zürich

March 14, 2024

# Communication Networks

## Exercise 2



- Last week's exercise
- Important lecture topics
- Introduction to this week's exercise
- Time to solve the exercise

# AS Classification

Tier 1: Provider of at least one AS and never a customer

Tier 2: Provider of at least one AS
and the customer of at least one AS

Tier 3: Customer of at least one AS and never a provider

IXP: Only Peering connections

Peering can in theory happen between any two types of AS

A peering connection between a Tier 1 and a Tier 3 is possible, however unlikely in the real world

Hint: Ignore peering connections at first when solving this exercise and only use them to find the IXPs

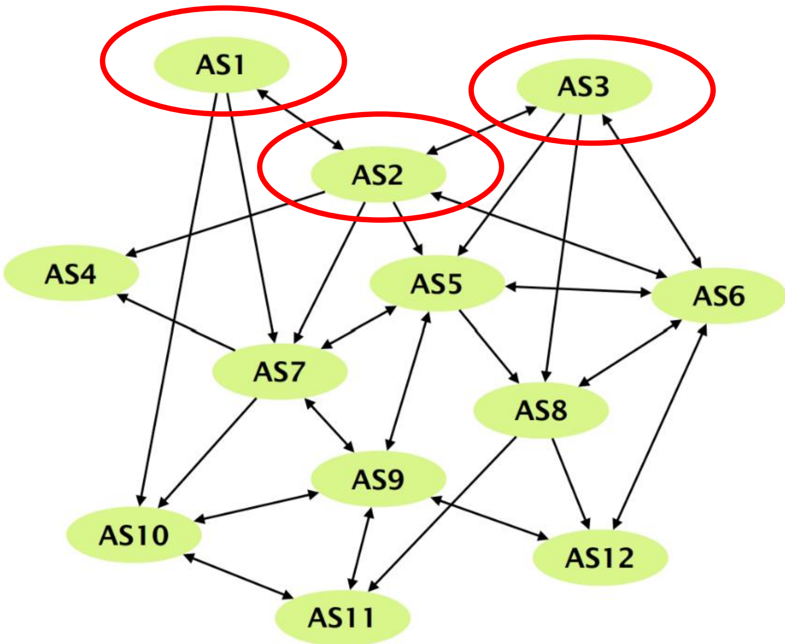
# AS Classification

Tier 1: Provider of at least one AS and never a customer

Tier 2: Provider of at least one AS
and the customer of at least one AS

Tier 3: Customer of at least one AS and never a provider

IXP: Only Peering connections



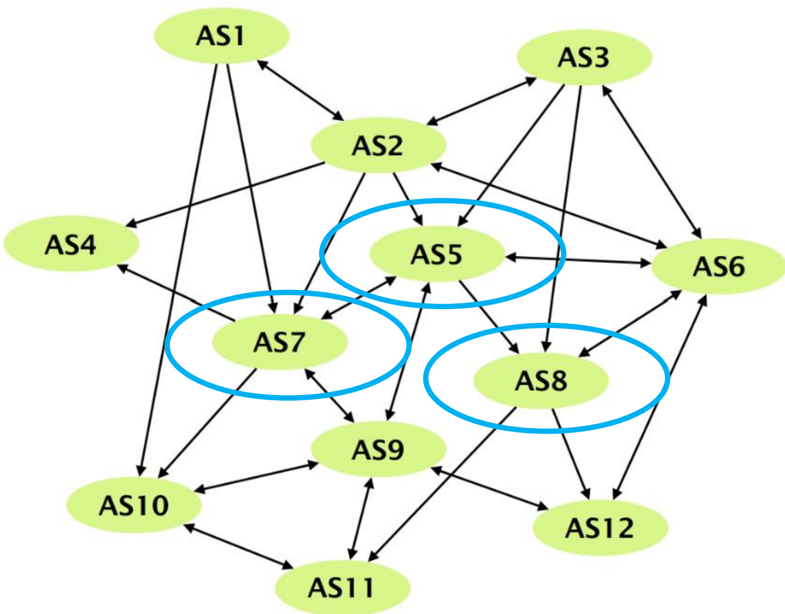
# AS Classification

Tier 1: Provider of at least one AS and never a customer

Tier 2: Provider of at least one AS
and the customer of at least one AS

Tier 3: Customer of at least one AS and never a provider

IXP: Only Peering connections



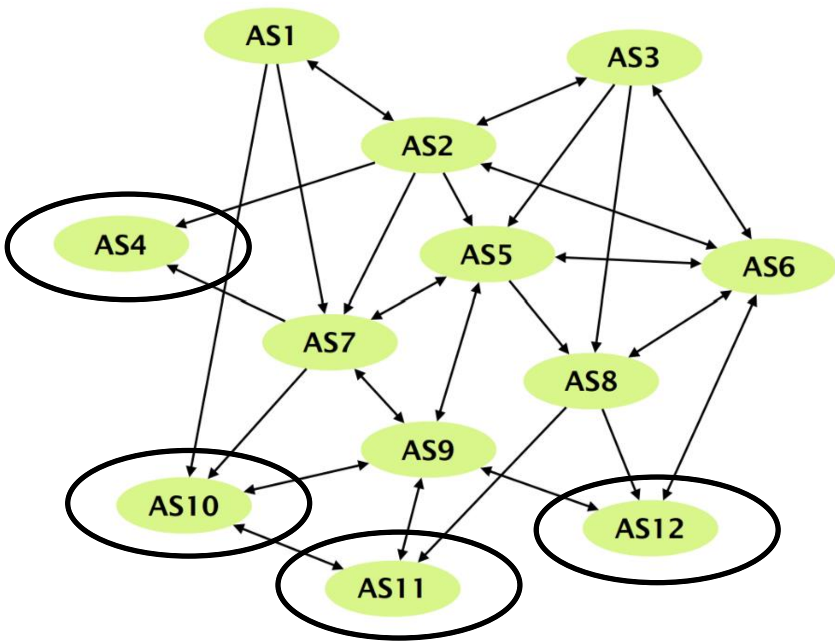
# AS Classification

Tier 1: Provider of at least one AS and never a customer

Tier 2: Provider of at least one AS
and the customer of at least one AS

Tier 3: Customer of at least one AS and never a provider

IXP: Only Peering connections



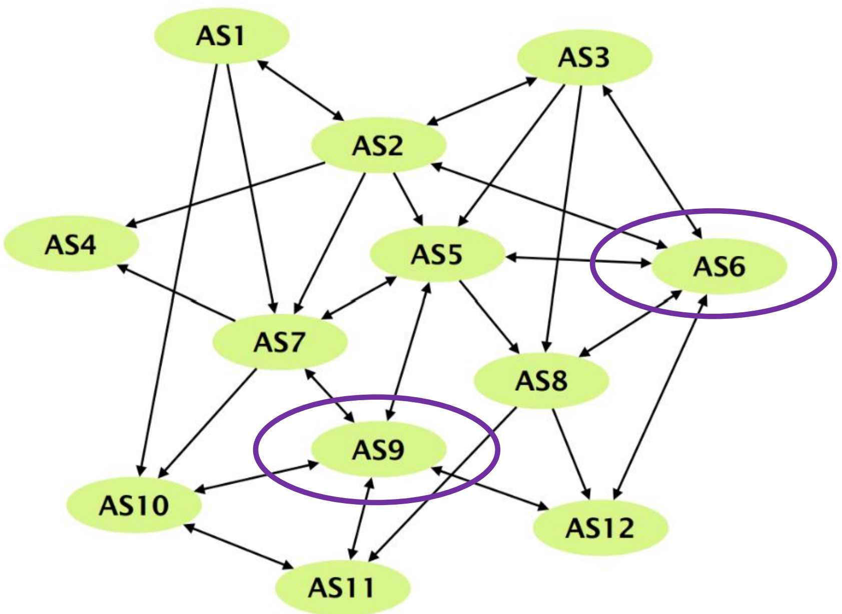
# AS Classification

Tier 1: Provider of at least one AS and never a customer

Tier 2: Provider of at least one AS and the customer of at least one AS

Tier 3: Customer of at least one AS and never a provider

IXP: Only Peering connections



# The problem with traceroute

When running a traceroute from within the ETH network we get outputs like this

```
roellinl@roellinl-nsg:~$ traceroute www.princeton.edu
traceroute to www.princeton.edu (104.18.4.101), 30 hops max, 60 byte packets
 1  roellinl-nsg.mshome.net (172.29.48.1)  0.865 ms  0.784 ms  0.704 ms
 2  rou-ref-hsrp-staff-net-core-vpn-1-a.ethz.ch (10.6.192.1)  6.162 ms  6.130 ms  6.022 ms
 3  rou-bgw-hci-staff-net.intern.ethz.ch (10.1.2.54)  5.943 ms  5.893 ms  9.220 ms
 4  104.18.4.101 (104.18.4.101)  5.576 ms  6.618 ms  6.806 ms
 5  104.18.4.101 (104.18.4.101)  6.938 ms  6.860 ms  6.827 ms
 6  104.18.4.101 (104.18.4.101)  6.413 ms  5.900 ms  5.883 ms
 7  104.18.4.101 (104.18.4.101)  5.817 ms  7.460 ms  7.070 ms
 8  104.18.4.101 (104.18.4.101)  7.915 ms  7.906 ms  7.901 ms
 9  104.18.4.101 (104.18.4.101)  7.027 ms  6.989 ms  12.322 ms
10  104.18.4.101 (104.18.4.101)  12.298 ms  12.308 ms  12.283 ms
11  104.18.4.101 (104.18.4.101)  12.277 ms  12.268 ms  12.261 ms
```

Possible Reasons?

# The problem with traceroute

When running a traceroute from within the ETH network we get outputs like this

```
roellinl@roellinl-nsg:~$ traceroute www.princeton.edu
traceroute to www.princeton.edu (104.18.4.101), 30 hops max, 60 byte packets
 1  roellinl-nsg.mshome.net (172.29.48.1)  0.865 ms  0.784 ms  0.704 ms
 2  rou-ref-hsrp-staff-net-core-vpn-1-a.ethz.ch (10.6.192.1)  6.162 ms  6.130 ms  6.022 ms
 3  rou-bgw-hci-staff-net.intern.ethz.ch (10.1.2.54)  5.943 ms  5.893 ms  9.220 ms
 4  104.18.4.101 (104.18.4.101)  5.576 ms  6.618 ms  6.806 ms
 5  104.18.4.101 (104.18.4.101)  6.938 ms  6.860 ms  6.827 ms
 6  104.18.4.101 (104.18.4.101)  6.413 ms  5.900 ms  5.883 ms
 7  104.18.4.101 (104.18.4.101)  5.817 ms  7.460 ms  7.070 ms
 8  104.18.4.101 (104.18.4.101)  7.915 ms  7.906 ms  7.901 ms
 9  104.18.4.101 (104.18.4.101)  7.027 ms  6.989 ms  12.322 ms
10  104.18.4.101 (104.18.4.101)  12.298 ms  12.308 ms  12.283 ms
11  104.18.4.101 (104.18.4.101)  12.277 ms  12.268 ms  12.261 ms
```

## Possible Reasons?

- The packet loops on the same device
- The endpoint network tries to obfuscate the path
- ETH itself is messing with the packets
- Etc..

# The problem with traceroute

What is most likely?

Since it happens only in the ETH network and it happens to different targets that are independent of each other option 3 is most likely.

# The problem with traceroute

What is most likely?

Since it happens only in the ETH network and it happens to different targets that are independent of each other option 3 is most likely.

What are they doing?

Rewrite the source IP of incoming packets to the one that was requested before

# The problem with traceroute

What is most likely?

Since it happens only in the ETH network and it happens to different targets that are independent of each other option 3 is most likely.

What are they doing?

Rewrite the source IP of incoming packets to the one that was requested before

Why?

This is where it gets tricky. There is no one answer traceroute will never give you the full picture.

Possible answers:

- Security (stateful Firewall)
- Saving IP addresses (some form of NAT)
- Misconfiguration

# The problem with traceroute

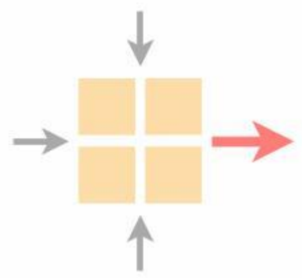
Following up with the ETH network admins

It turns out that this is the expected behavior of the Cisco firewall, it is done to save on NAT resources

If you are curious:
https://networkdirection.net/articles/firewalls/icmpinspection/

# Communication Networks

## Exercise 2



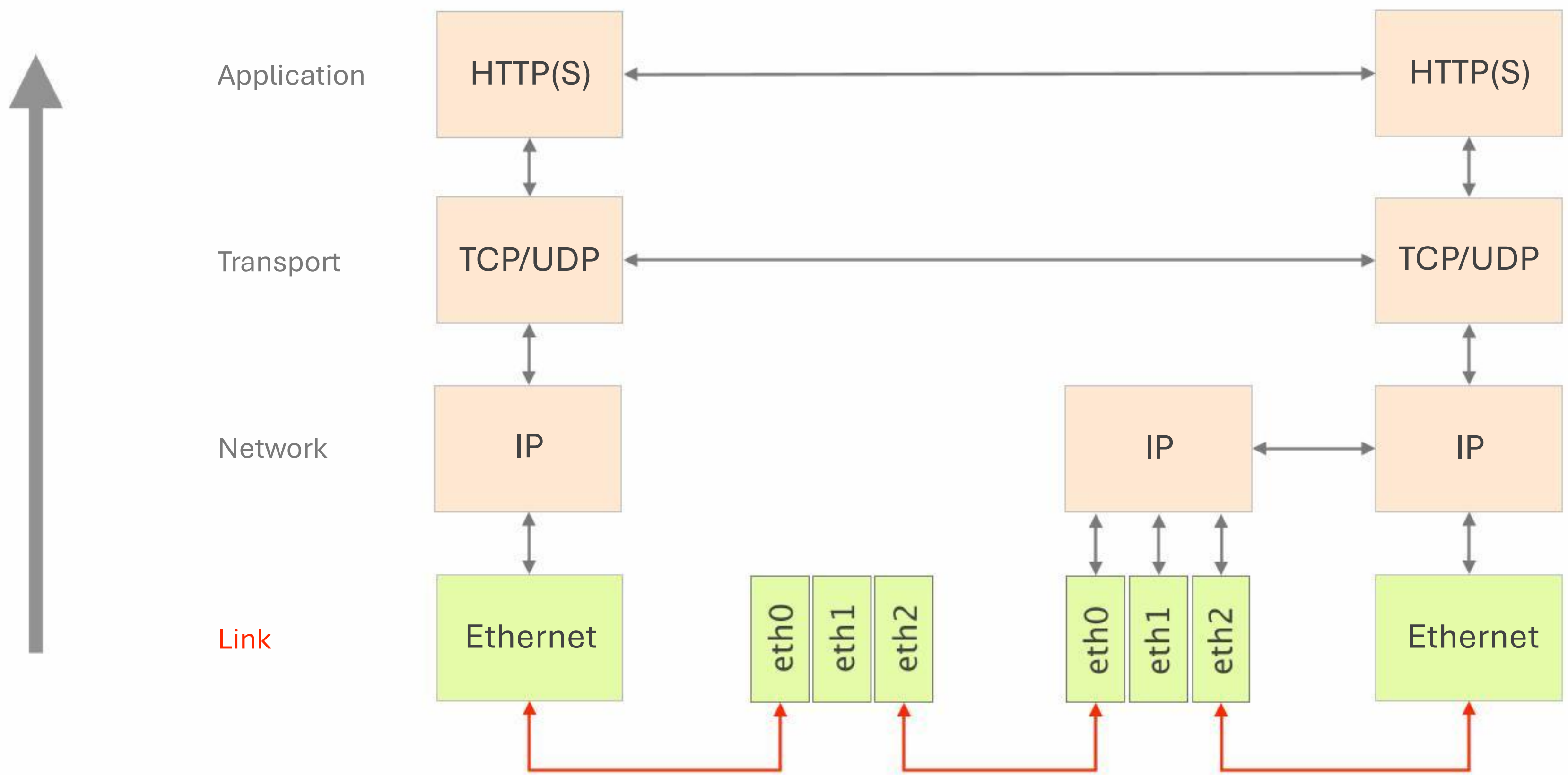
Last week's exercise

Important lecture topics

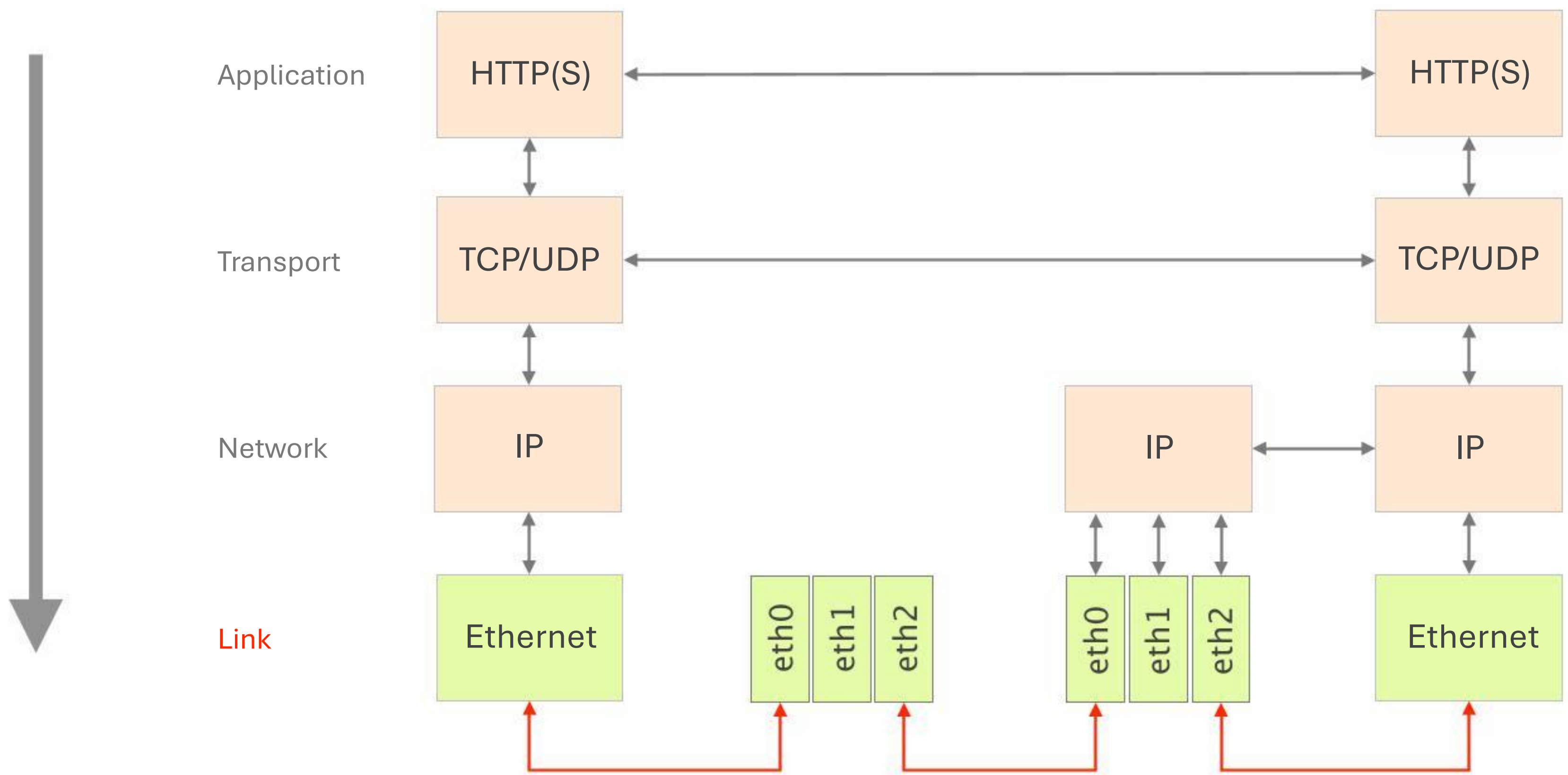
Introduction to this week's exercise

Time to solve the exercise

# In the lecture we go through the layers bottom-up



# Another possible approach would be top-down



# We face a common problem

No matter the direction, often concepts of other layers are needed to understand the current one

Unfortunately, we cannot prevent that completely

We saw that when speaking about MAC addresses, suddenly we also care about IP addresses

MAC addresses identify sender and receiver adapters

used on a "single" link

# MAC addresses identify sender and receiver adapters

↓ used on a "single" link

In general, we therefore use IP addresses (L3)
to address arbitrary hosts

MAC addresses are then used on a hop-by-hop basis
to eventually reach the corresponding host

In fact, for humans domain names are even easier to remember

domain name of destination → DNS (L5) → IP (L3) of destination → ARP → MAC (L2) of next hop

# We currently only consider IP addresses which are reachable over a given link

That simplifies the whole process, we only need to be able to translate from IP to MAC address

IP (L3) of destination → ARP → MAC (L2) of destination

Who are you?

IP-to-MAC binding

Given an IP address reachable on a link,

How do I find out what MAC to use?

Address Resolution Protocol

# That can only work if hosts can get an IP address

Who am I?

MAC-to-IP binding

How do I acquire an IP address?

Dynamic Host Configuration Protocol

We will explore both concepts
(ARP and DHCP) in today exercise

# Communication Networks

## Exercise 2

Last week's exercise

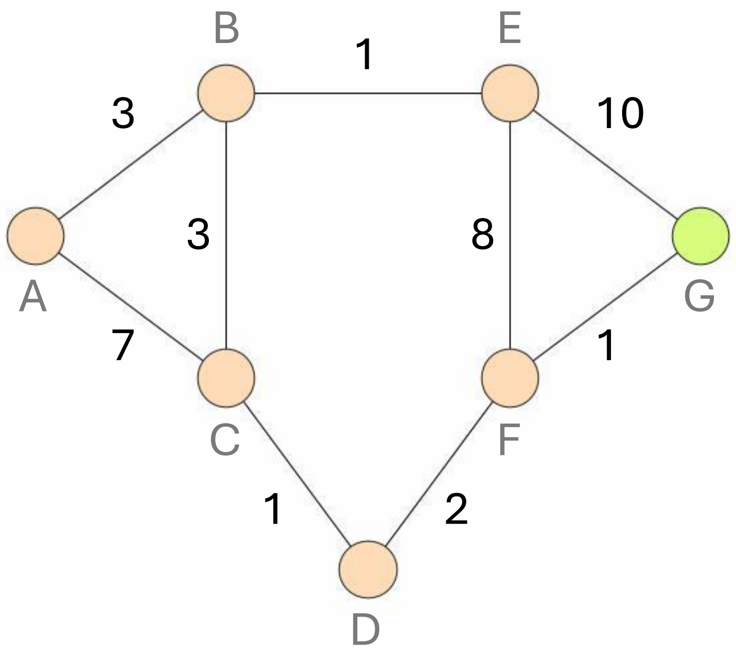
Important lecture topics

Introduction to this week's exercise

Time to solve the exercise

# Two more questions related to routing concepts

# Task 3.1 Distance Vector

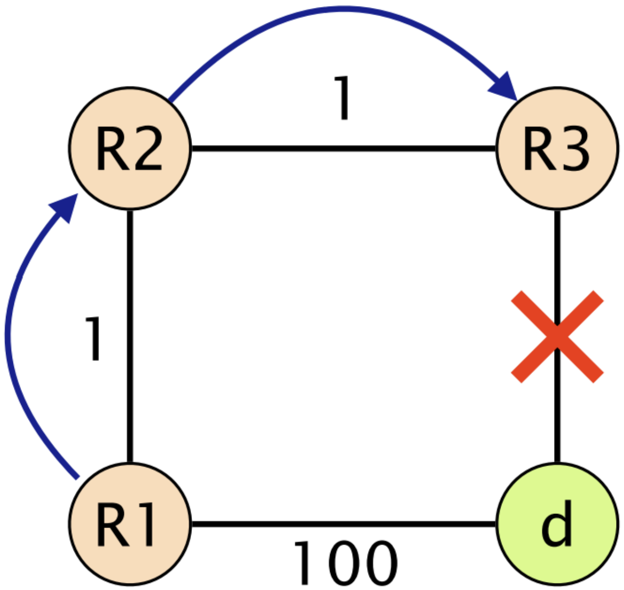



Compute shortest-paths using a distance vector algorithm

Tie-breaking: path with lower amount of links

Compared to link-state algorithms, paths are now computed in a distributed fashion

# Task 3.2 Dijkstra's Algorithm with Link Failure




Back to Dijkstra (link-state)

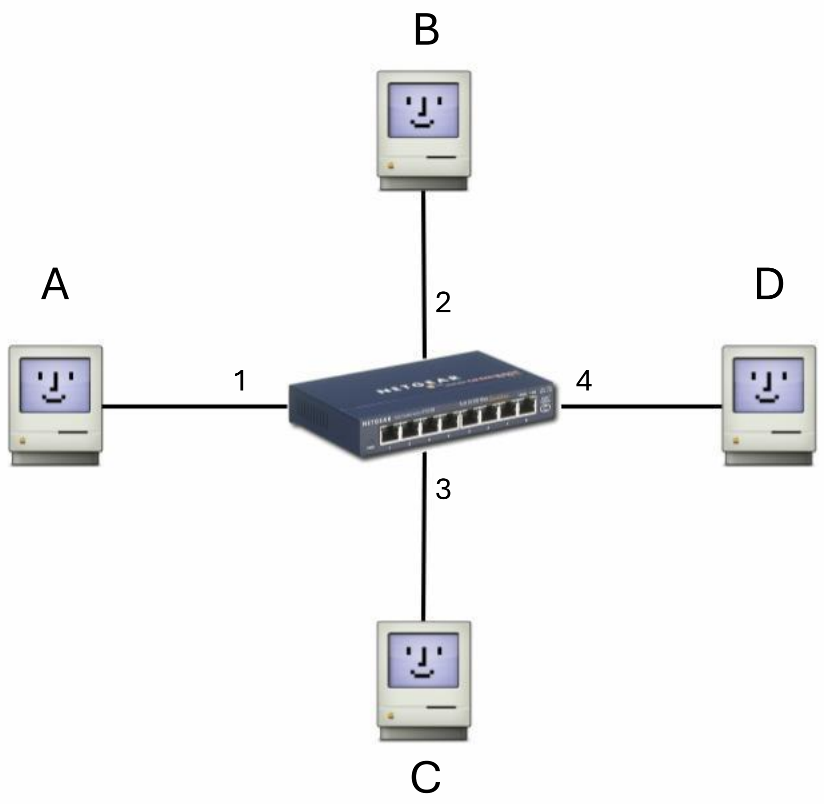
We assume that the link between d and R3 fails

R3 detects that quickly but what about the other nodes?

What happens if the local network view does not match with the reality?

# And three questions related to Ethernet & Switching

# Task 3.3: Duplicate MAC Address

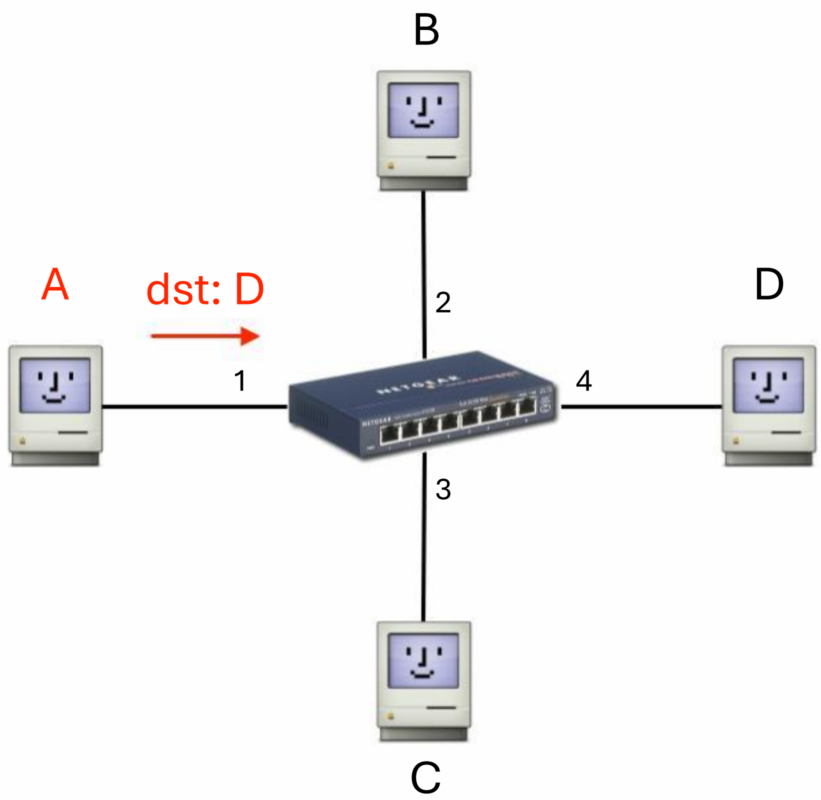



| dst | port |
|---|---|

As a reminder, let's look at this simple example

A switch learns how to map MACs to ports

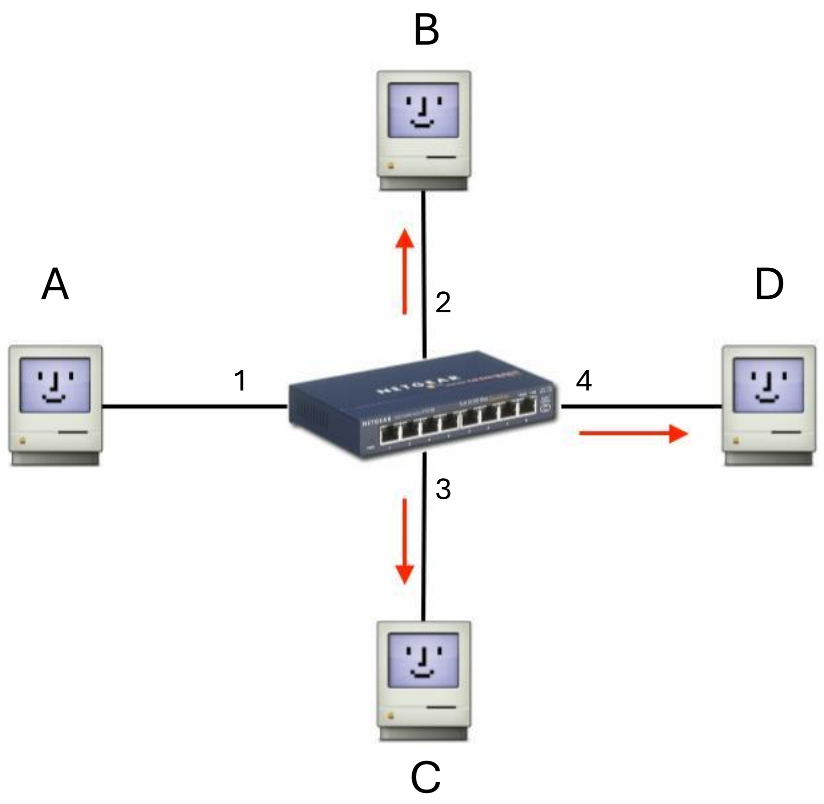
# Task 3.3: Duplicate MAC Address




| dst | port |
| --- | --- |
| A | 1 |

Switch learns how to map A to port 1

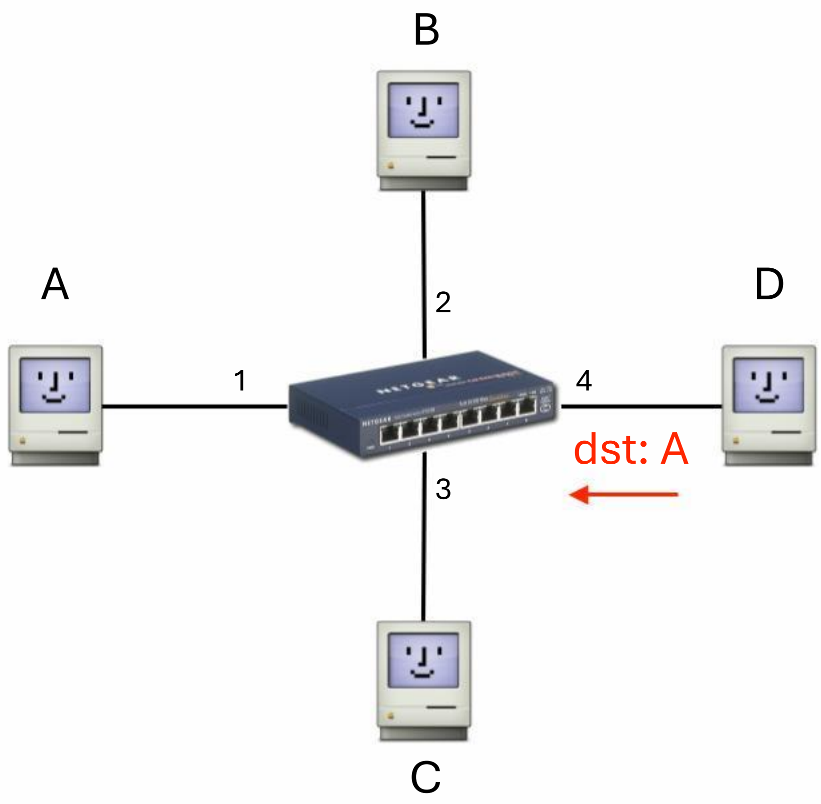
# Task 3.3: Duplicate MAC Address




| dst | port |
|---|---|
| A | 1 |

Dst D unknown: broadcast

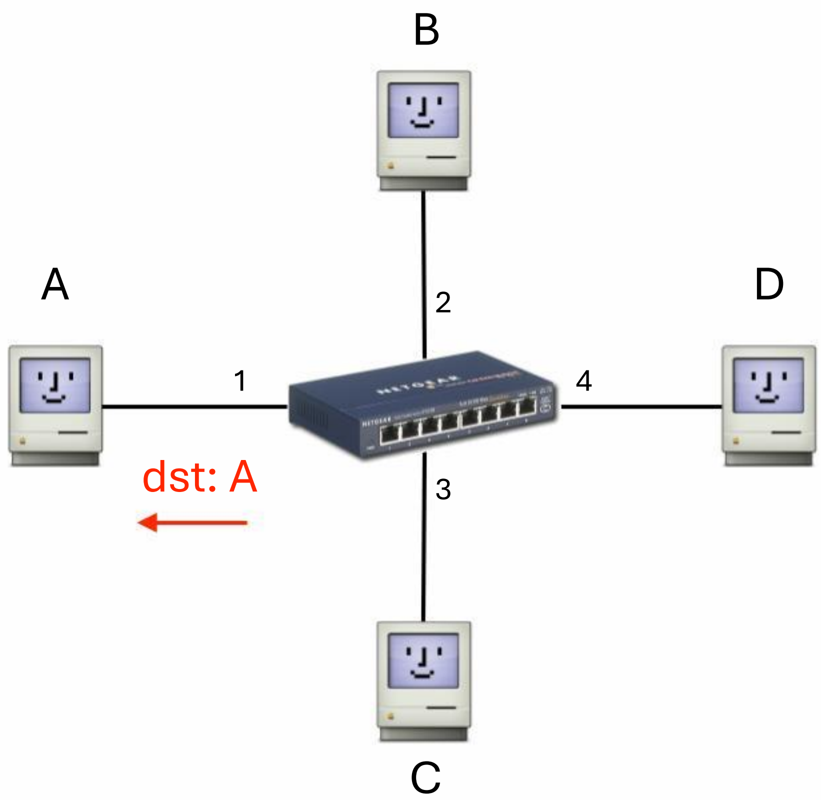
# Task 3.3: Duplicate MAC Address




| dst | port |
|---|---|
| A | 1 |
| D | 4 |

Switch learns how to map D to port 4

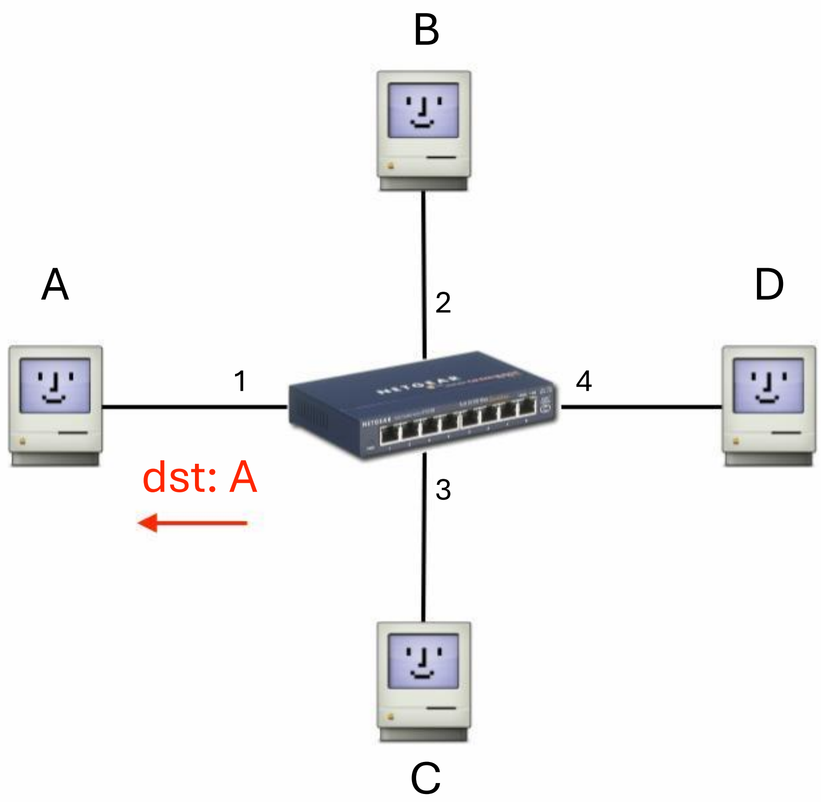
# Task 3.3: Duplicate MAC Address




| dst | port |
|---|---|
| A | 1 |
| D | 4 |

Dst A known, no broadcast required

# Task 3.3: Duplicate MAC Address




| dst | port |
|---|---|
| A | 1 |
| D | 4 |

What happens if you have duplicated MAC addresses?

# Task 3.4: Imposter

Put your knowledge about DHCP and ARP together

| | |
|---|---|
| Who am I? | How do I acquire an IP address? |
| MAC-to-IP binding | Dynamic Host Configuration Protocol (DHCP) |
| Who are you? | Given an IP address reachable on a link, how do I find out what MAC to use? |
| IP-to-MAC binding | Address Resolution Protocol (ARP) |

# Task 3.5: MAC-Learning (exam question 2021)

We asked this question in the summer exam of 2021

Use your knowledge from task 3.3 to solve this one

# Communication Networks

## Exercise 2

Last week's exercise

Important lecture topics

Introduction to this week's exercise

Time to solve the exercise