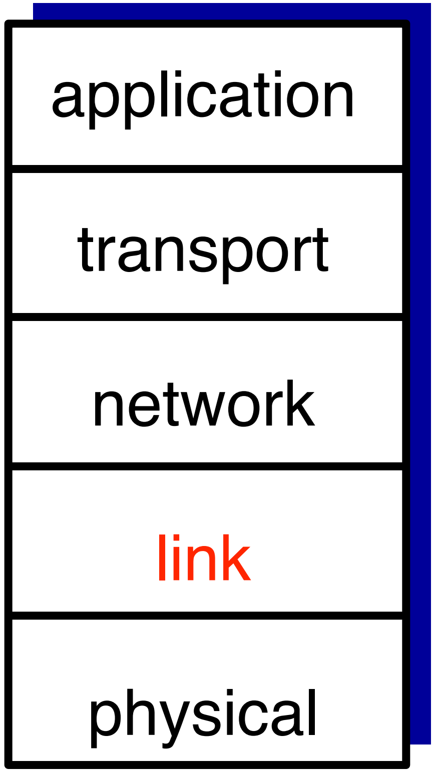
The link (ethernet) layer

Goal:

1. To understand the principles behind the link layer:
    1. Ethernet frames, MAC addresses
    2. Switching
    3. Switch security considerations



Roadmap

1. Datagrams
2. The link (ethernet) layer
   - ethernet frames, MAC addresses
3. Broadcasting
4. Switching
5. Switch security considerations

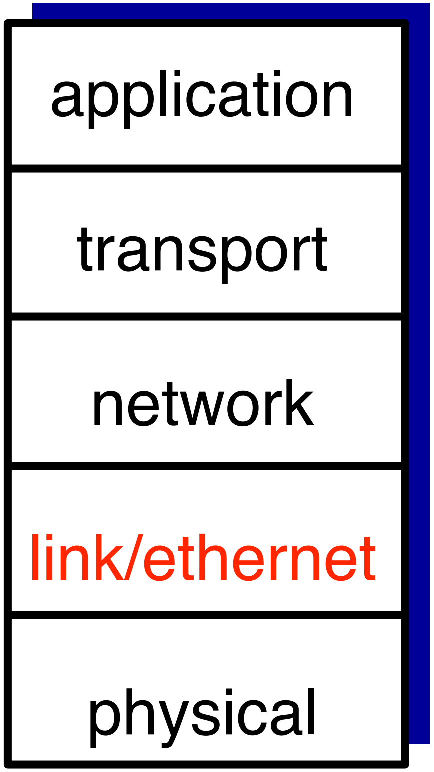
Recap: the 4-layers model

application: supporting network applications.

transport: process-process data transfer.

network: routing of datagrams from source to destination.

link: data transfer between neighbouring network elements.



application

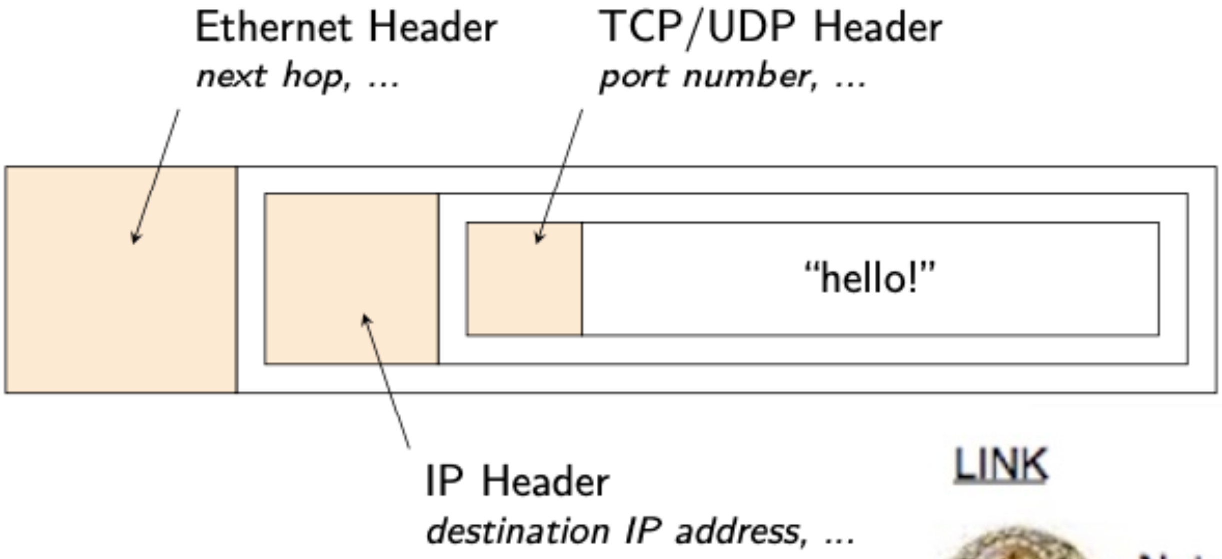
transport

network

link/ethernet

physical

Recap: datagrams

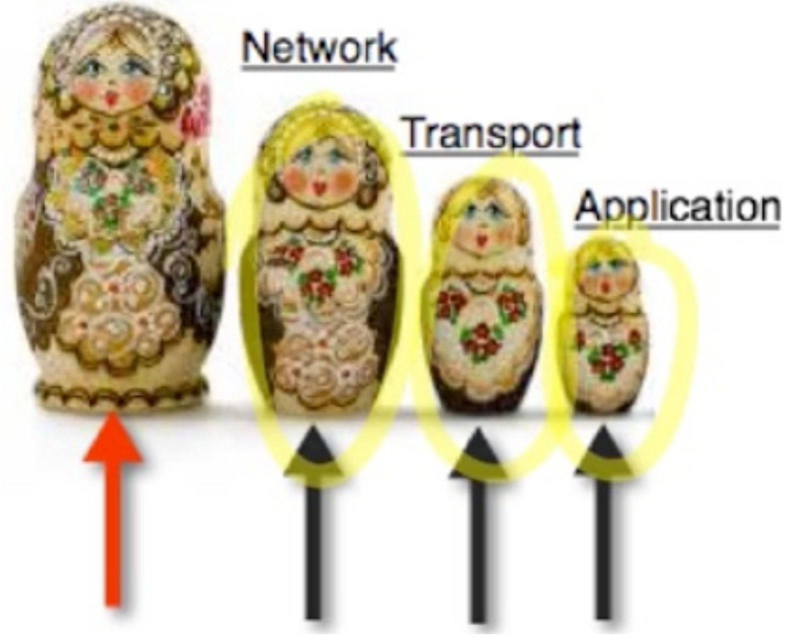


Application
HTTP, DNS, . . .

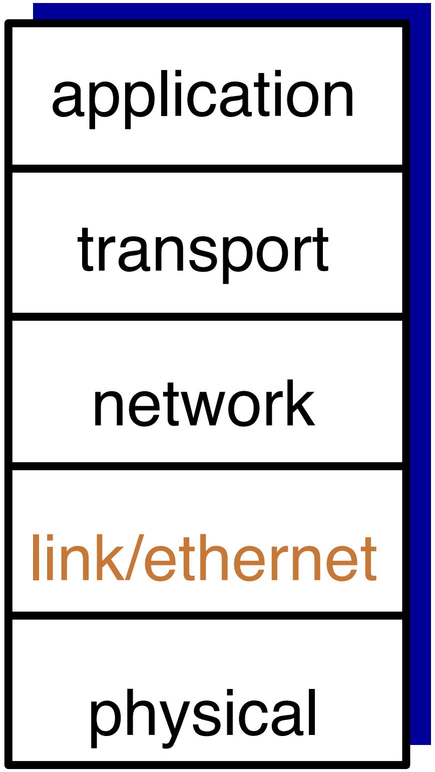
Transport
TCP, UDP

Internetwork
IP

Link
Ethernet



data transmission


application

transport

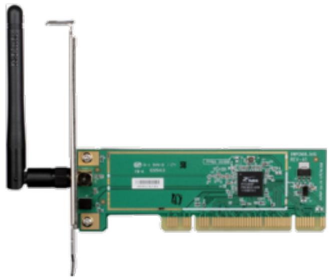
network

link/ethernet

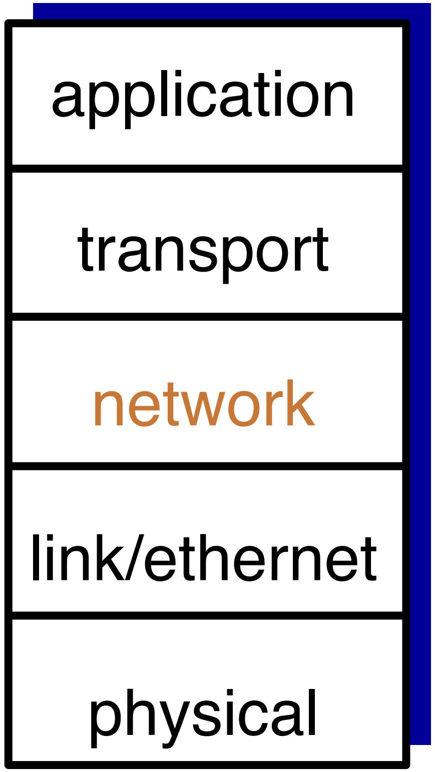
physical

Layer 2 (ethernet) is responsible for hop-to-hop delivery.

- The MAC address uniquely identifies each individual NIC (network interface controller).
- Besides your NIC, a switch also works at this level
- hop is a term that refers to the number of routers a packet (a portion of data) passes through from source to destination.



data transmission



application

transport

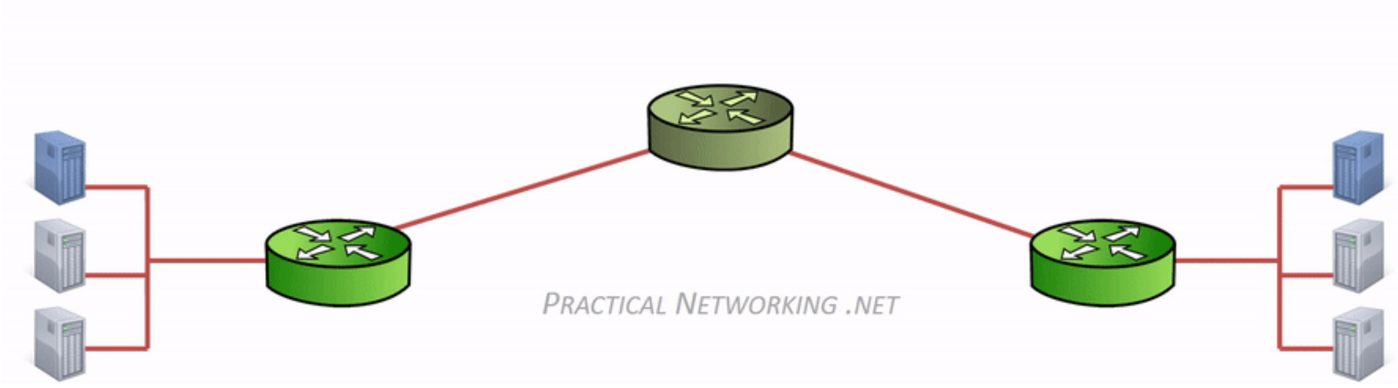
network

link/ethernet

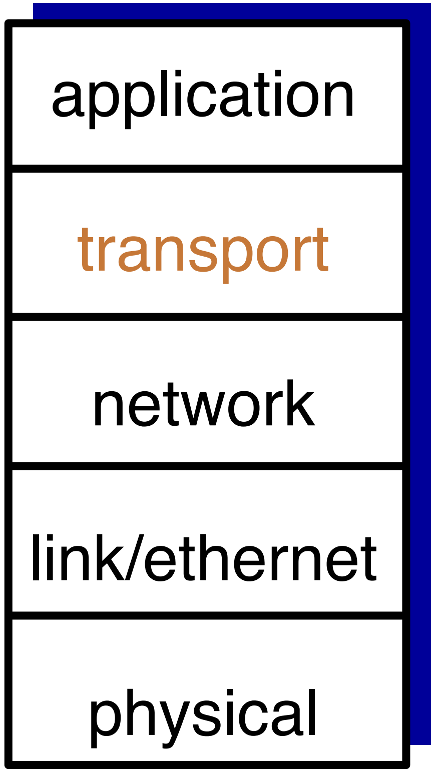
physical

Layer 3 (network) is responsible for end-to-end delivery.

- it uses IP addresses.
- when a computer has data to send, it encapsulates the data in an IP header, including information such as the Source and Destination IP address.
- between each router, the MAC address header is stripped and regenerated to get the next hop (router



data transmission


application

transport

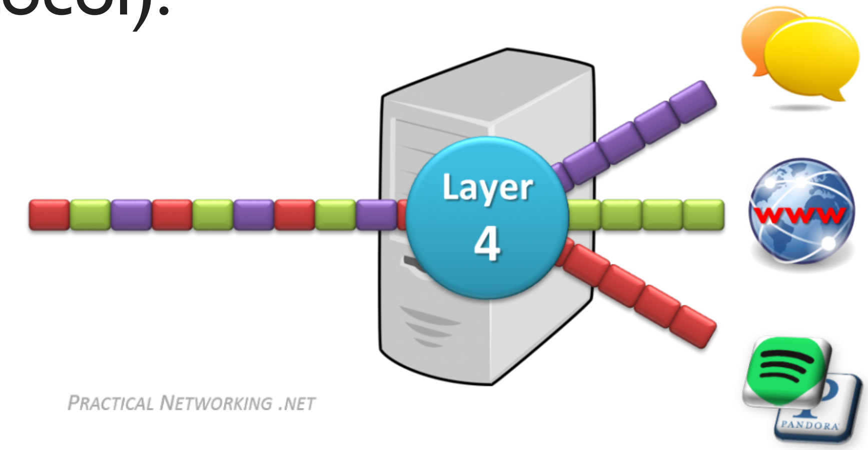
network

link/ethernet

physical

Layer 4 (transport) is responsible for service-to-service delivery.

- We need a way to distinguish data streams from the Internet, e.g. browsers, Zoom, etc.
- Protocols: TCP (transmission control protocol) and UDP (user datagram protocol).



PRACTICAL NETWORKING .NET

data transmission

When layer 4 gets data, it adds a header that facilitates service-to-service delivery, e.g., TCP or UDP ports.

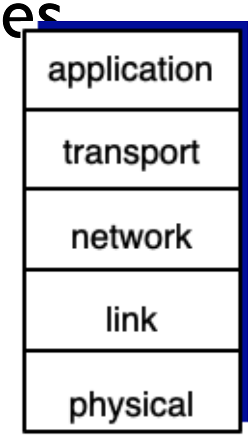
- The whole datagram is referred to as a segment.

When layer 3 gets data, it adds a header that facilitates end-to-end delivery, e.g., sure IP, destination IP, etc.

- The whole datagram is referred to as a packet.

When layer 2 gets data, it adds a header that facilitates hop-to-hop delivery, e.g., a Source MAC address.

- The whole datagram is referred to as a frame.



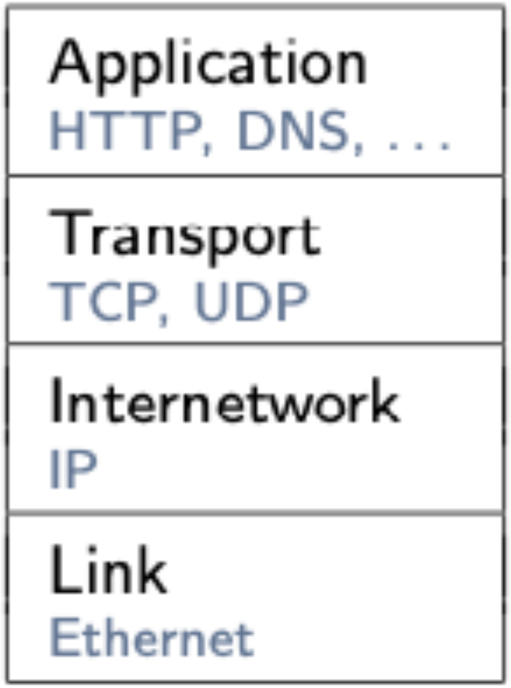
Roadmap

1. Datagrams
2. The link (ethernet) layer
    - ethernet frames, MAC addresses
3. Broadcasting
4. Switching
5. Switch security considerations

the link (ethernet) layer

What is ethernet and why do we care?

- Ethernet is a popular approach to solving the problem of transmitting data over a LAN (local area network).
- Immensely successful to this day, it continues to evolve wired, high-speed GigaBytes, wireless, etc.
- Provides link layer support for encapsulating IP datagrams.



Application
HTTP, DNS, . . .

Transport
TCP, UDP

Internetwork
IP

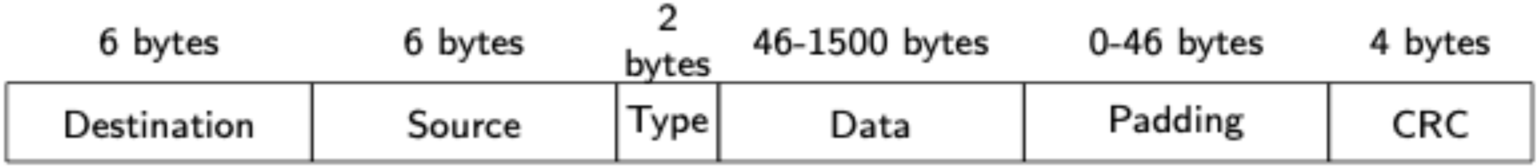
Link
Ethernet

building blocks of Ethernet

1. The frame
   - Standardised set of bits that carry data
2. The MAC (media access control) protocol
   - Set of rules for accessing Ethernet channels
3. The signaling components
   - Standardised electronic devices that send and receive signals over Ethernet channels
4. The physical medium
   - Cable carrying the signals

We will focus on 1 and 2: data frames and MAC addresses

ethernet frames



6 bytes	6 bytes	2 bytes	46-1500 bytes	0-46 bytes	4 bytes
Destination	Source	Type	Data	Padding	CRC

Destination - MAC address of the device where the packet is going

Source - MAC address from which the packet came from

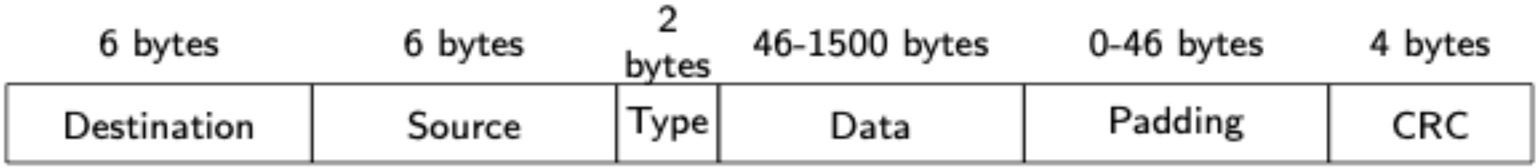
Type - it allows multiplexing (which network protocol will be used)

Data - the datagram that we are sending

Padding - to complete the minimum size of the datagram

CRC - cyclic redundant check, used to handle errors

ethernet frames



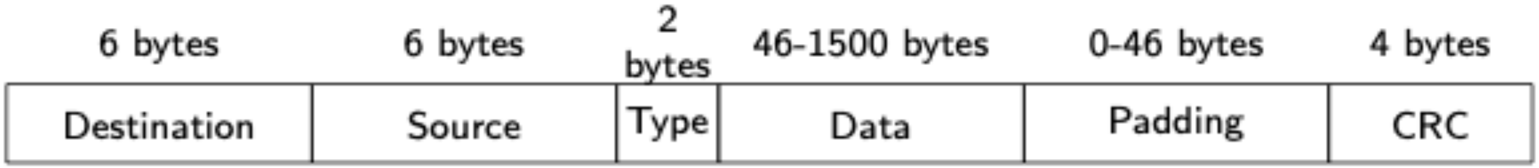
6 bytes	6 bytes	2 bytes	46-1500 bytes	0-46 bytes	4 bytes
Destination	Source	Type	Data	Padding	CRC

If we were to send 1501 bytes of data, how many frames do we need to send?

Frame 1. the Data field contains 1500 bytes.

Frame 2. the Data field contains 1 data byte plus 45 bytes of padding. Those padding bytes are the Padding field.

Quiz - example 1

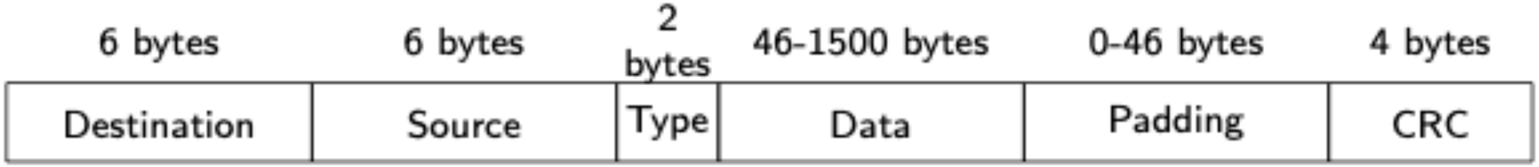


6 bytes	6 bytes	2 bytes	46-1500 bytes	0-46 bytes	4 bytes
Destination	Source	Type	Data	Padding	CRC

You are sending data over ethernet that is 5400 bytes long?

How many ethernet frames will this be?

Quiz - example 2

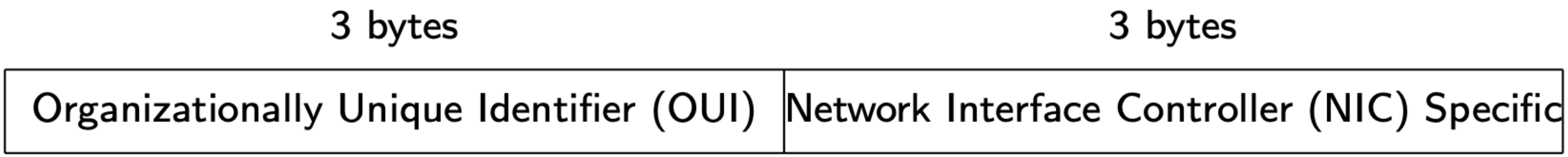


6 bytes	6 bytes	2 bytes	46-1500 bytes	0-46 bytes	4 bytes
Destination	Source	Type	Data	Padding	CRC

You are sending data over ethernet that is 3201 bytes long?

How many ethernet frames will this be?

MAC addresses



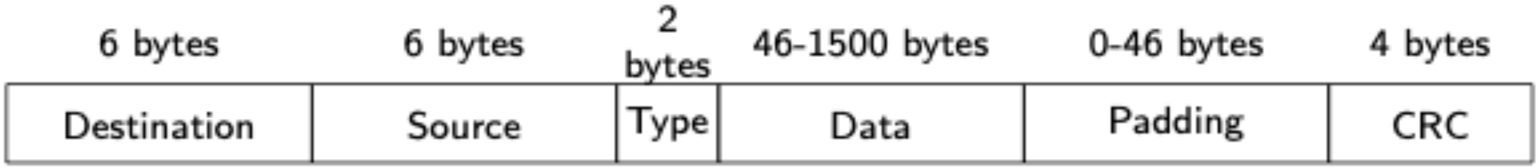
3 bytes	3 bytes
Organizationally Unique Identifier (OUI)	Network Interface Controller (NIC) Specific

1. OUI (Organization Unique Identifier), e.g. 60:45:BD for Microsoft.
2. NIC (Network Interface Controller), identifies the device.

Roadmap

1. Datagrams
2. The link (ethernet) layer
   - ethernet frames, MAC addresses
3. Broadcasting
4. Switching
5. Switch security considerations

ethernet frames - broadcasting



6 bytes	6 bytes	2 bytes	46-1500 bytes	0-46 bytes	4 bytes
Destination	Source	Type	Data	Padding	CRC

Destination is sometimes a set of physical devices, in which case we are talking about a broadcast address:

- the broadcast address is FF:FF:FF:FF:FF:FF
- In practice, this means that if a network adapter gets a broadcast address, the adapter will send the address to the network layer to translate it.

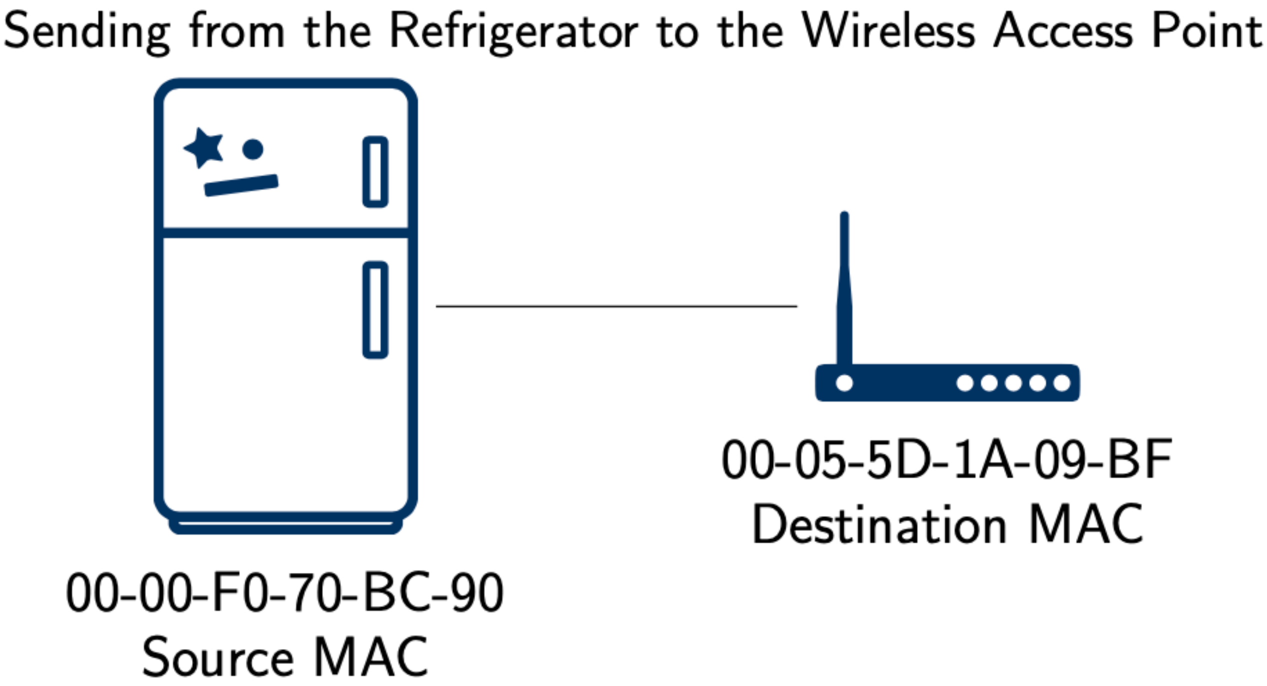
What about datagrams from other networks beyond the LAN?

- Well, that's routing, and that's the topic for next week

example 1

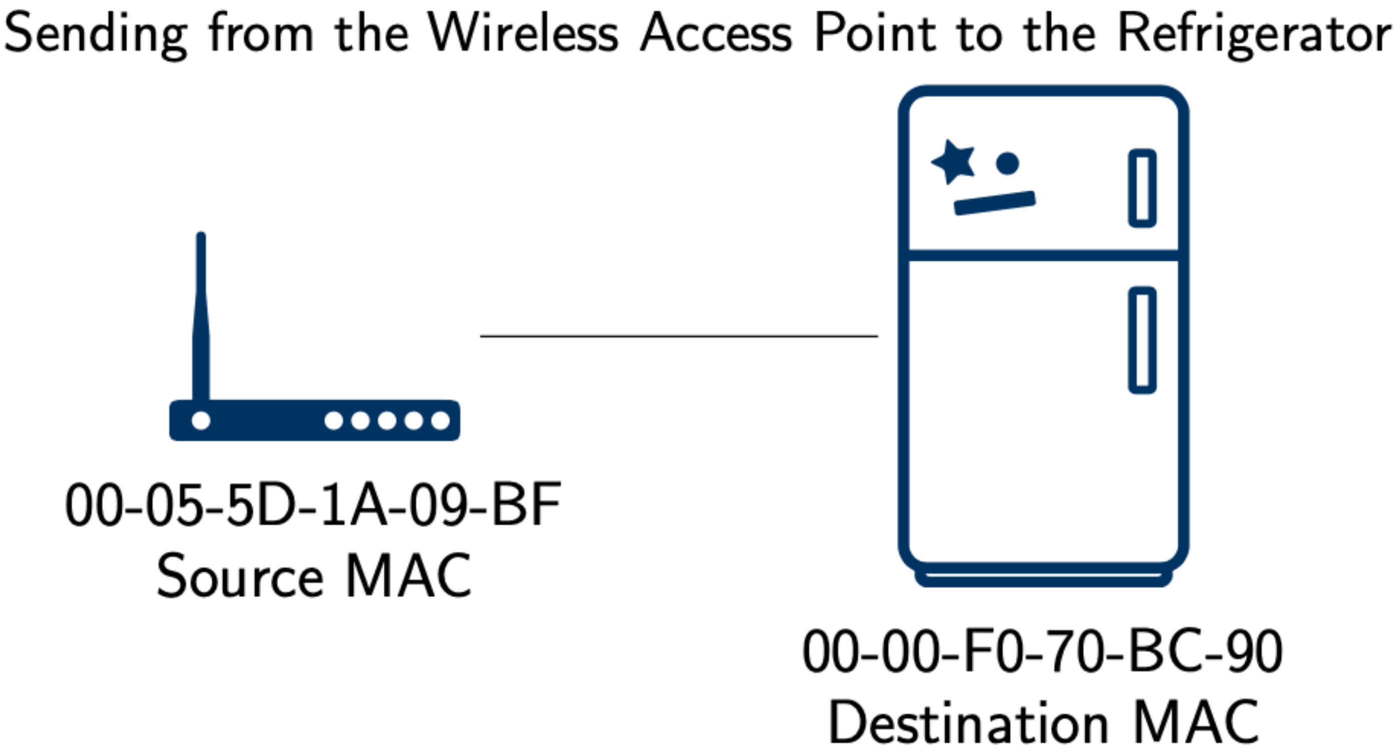
00-00-F0 equals to SAMSUNG and 00-05-5D to GUI-LINK

The refrigerator builds a frame with the Source equals to 00-00-F0-70-BC-9 and the Destination equals to 00-05-5D-1A-09-BF



example 1

00-00-F0 means SAMSUNG
00-05-5D means GUI-LINK



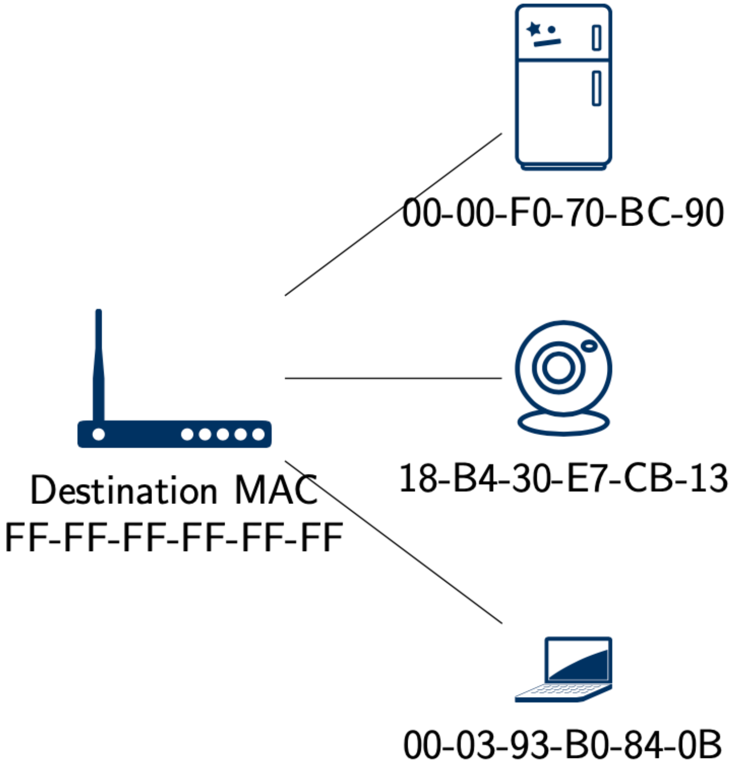
Sending from the Wireless Access Point to the Refrigerator

00-05-5D-1A-09-BF
Source MAC

00-00-F0-70-BC-90
Destination MAC

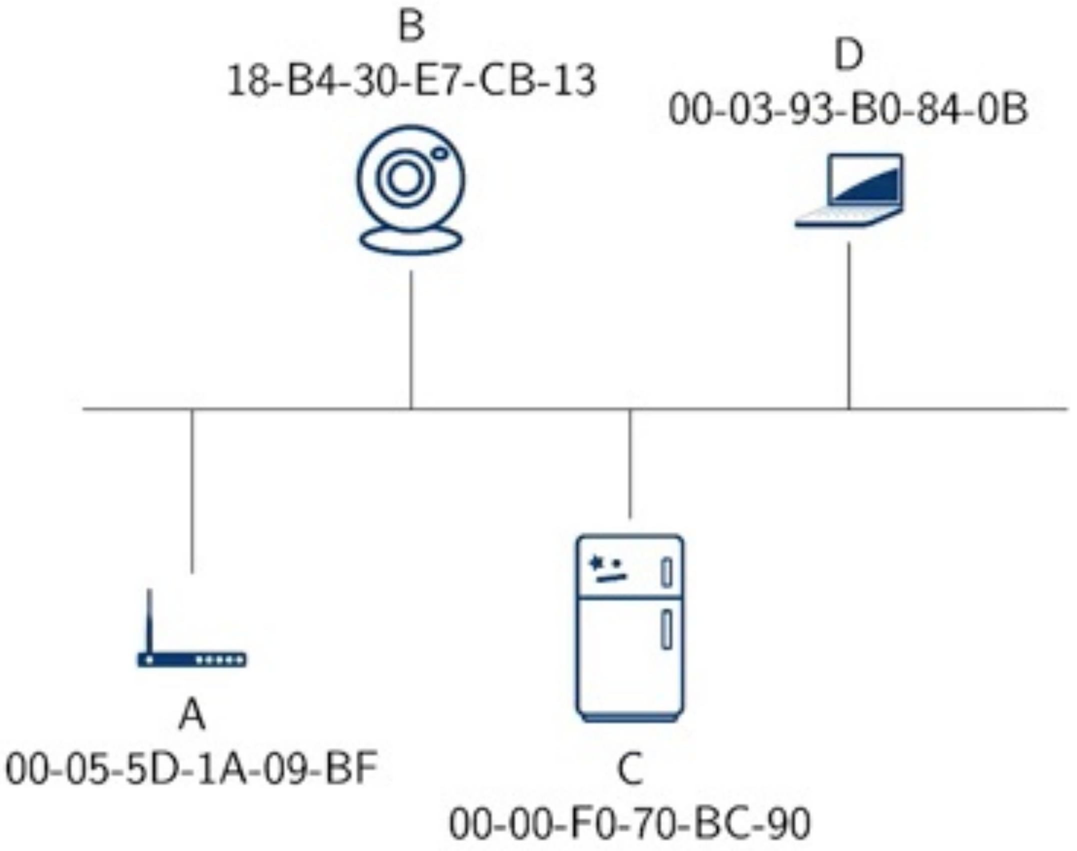
example 2 - broadcasting

- The NIC adapter broadcasts the MAC address FF: FF: FF: FF: FF:FF



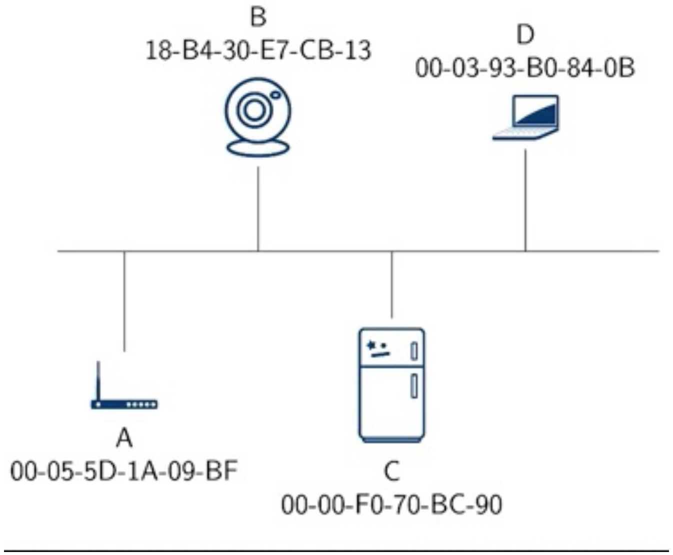
exercise - broadcasting

A is going to send a message with the destination MAC address FF:FF:FF:FF:FF:FF



exercise - broadcasting

1. What is the source address?
2. What is the destination address?
3. What devices on the network can see the ethernet frame and its contents? Check all that apply
   1. A
   2. B
   3. C
   4. D
4. What data do the devices on the network that you checked above have access to? Check all that apply
   1. Ethernet frame data field
   2. IP datagram
   3. Transport layer data
   4. Application layer data

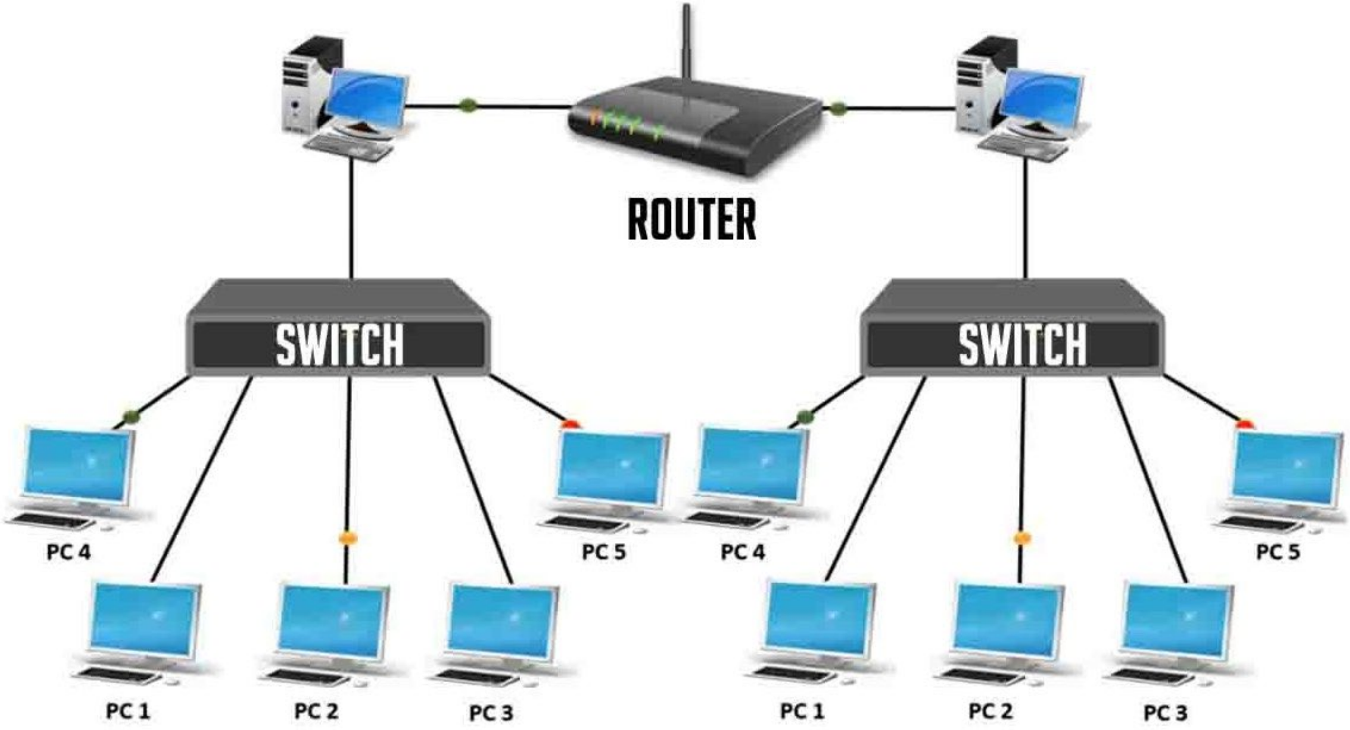


Roadmap

1. Datagrams
2. The link (ethernet) layer
   - ethernet frames, MAC addresses
3. Broadcasting
4. Switching
5. Switch security considerations

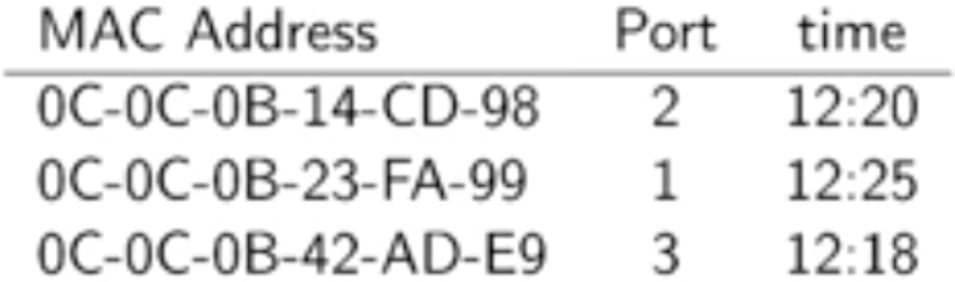
Switching vs Routing

- A switch connects multiple devices to create a network.
- A router connects multiple switches, and their respective networks, to form an even larger network



Switching and self-learning

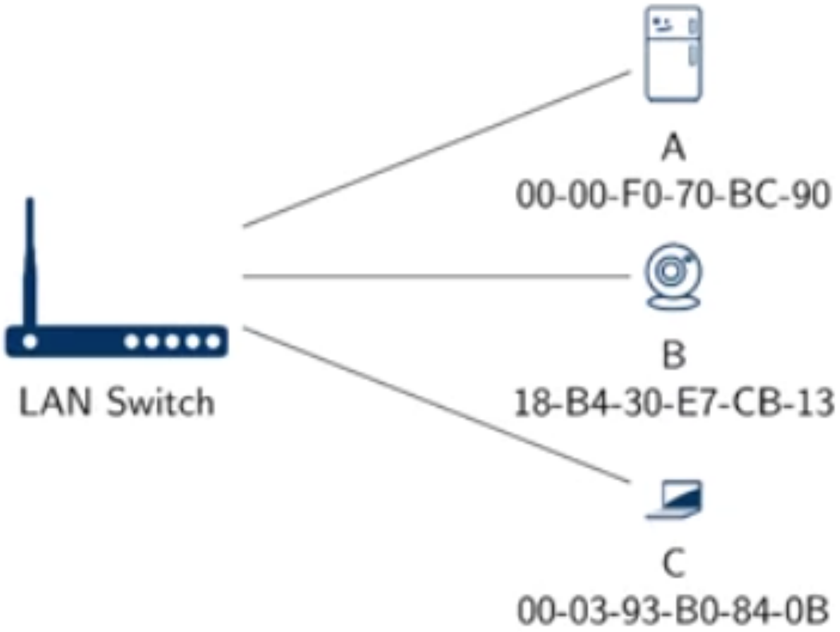
1. Switch table starts empty
2. When the ethernet frame comes in, the switch stores the source MAC address to the port it came from.
3. It records the time it received the transmission.



MAC Address	Port	time
0C-0C-0B-14-CD-98	2	12:20
0C-0C-0B-23-FA-99	1	12:25
0C-0C-0B-42-AD-E9	3	12:18

How does a switch build its table?

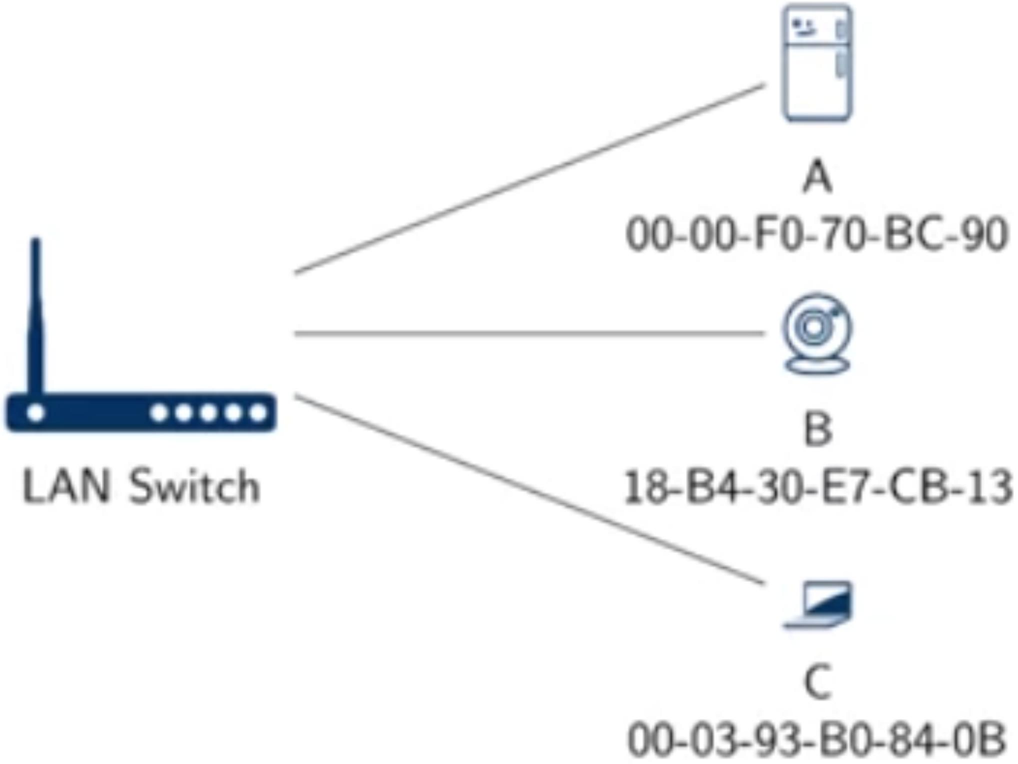
- We have a LAN with 3 devices connected to it: A, B, and C.
- At 12:20 the LAN gets a message A on port 1, and the switch adds it to the table
- At 12;35 …



MAC Address	Port	time
00-00-F0-70-BC-90	1	12:20
18-B4-30-E7-CB-13	2	12:35

How does a switch build its table?

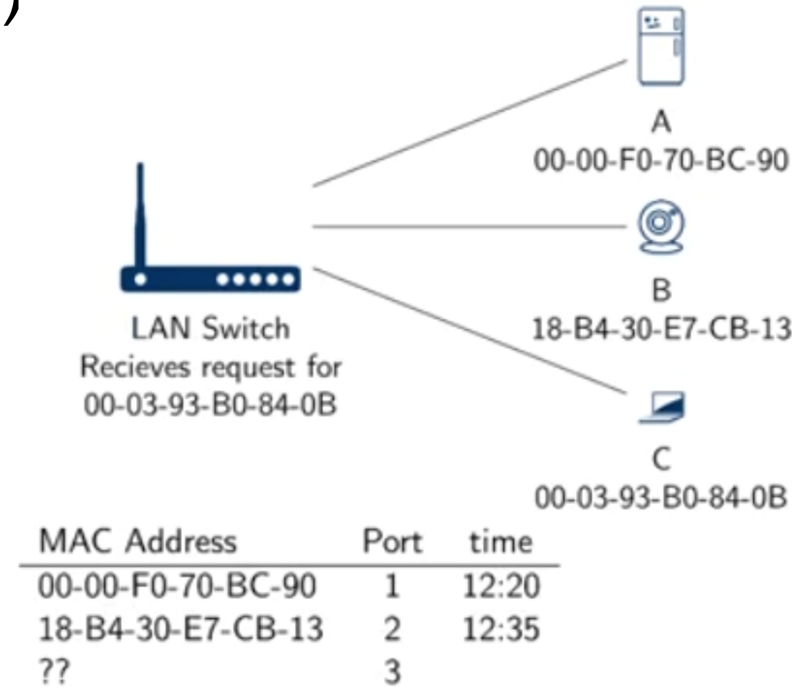
- As the LAN gets traffic sent to 00-00-F0-70-BC, it is redirected to port 1, etc.



MAC Address	Port	time
00-00-F0-70-BC-90	1	12:20
18-B4-30-E7-CB-13	2	12:35

flooding

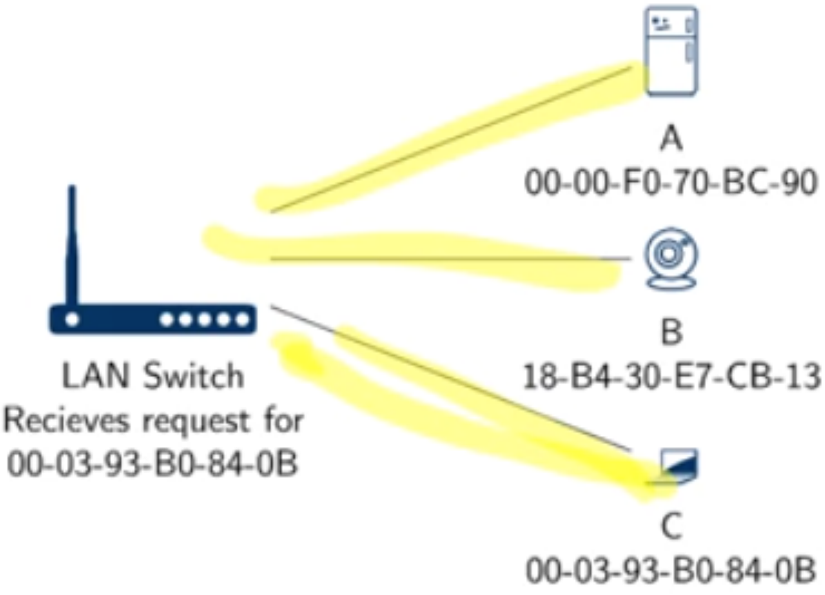
- **What happens when a switch does not know the packet destination?**
  - Suppose a message is sent to C (00-03-93-B0-84-0B), but C is not in the table.
  - In that case the switch floods all the ports (it sends messages to the ports)



MAC Address	Port	time
00-00-F0-70-BC-90	1	12:20
18-B4-30-E7-CB-13	2	12:35
??	3	

flooding

- What happens when a switch does not know the packet destination?
  - Causing the port C (and the other ports) to send a message to the LAN so this can complete the table.



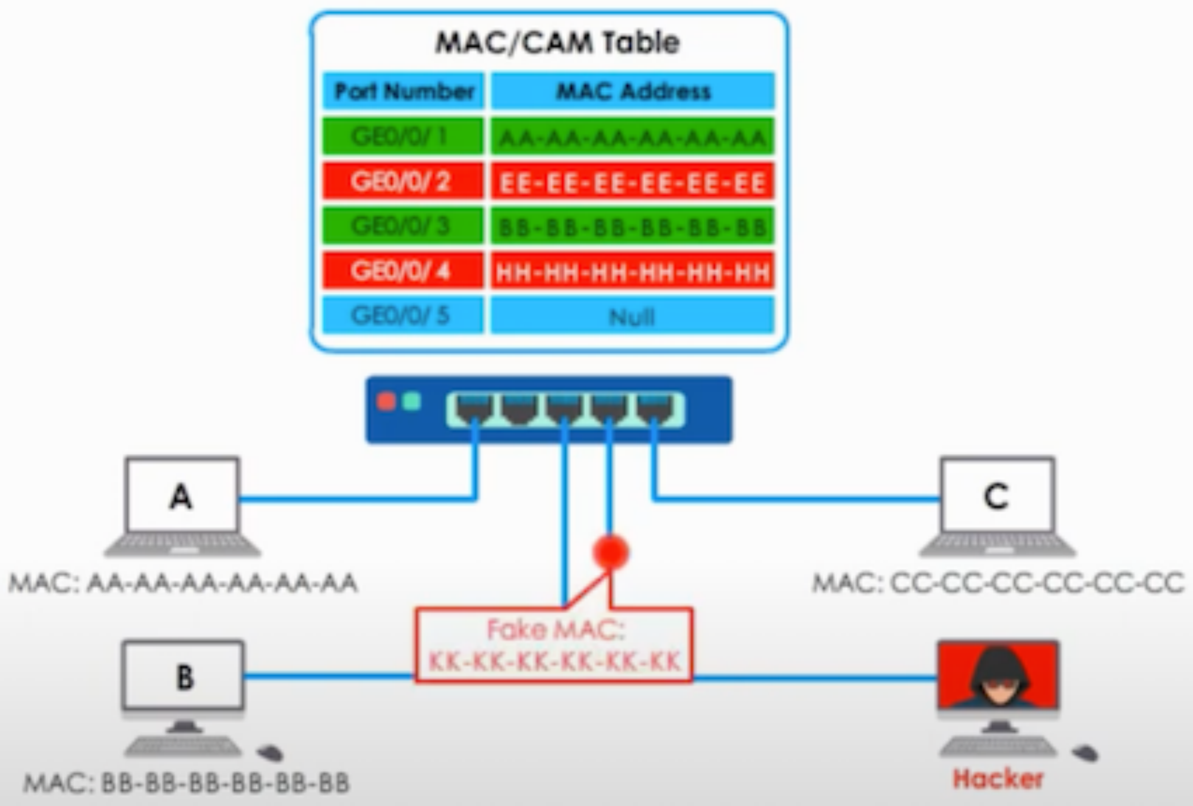
MAC Address	Port	time
00-00-F0-70-BC-90	1	12:20
18-B4-30-E7-CB-13	2	12:35
??	3	

Roadmap

1. Datagrams
2. The link (ethernet) layer
   - ethernet frames, MAC addresses
3. Broadcasting
4. Switching
5. Switch security considerations

Security - switch flooding/poisoning

- Flooding MAC ports leads to a DoS (Denial of Service) attack called MAC flooding attack.

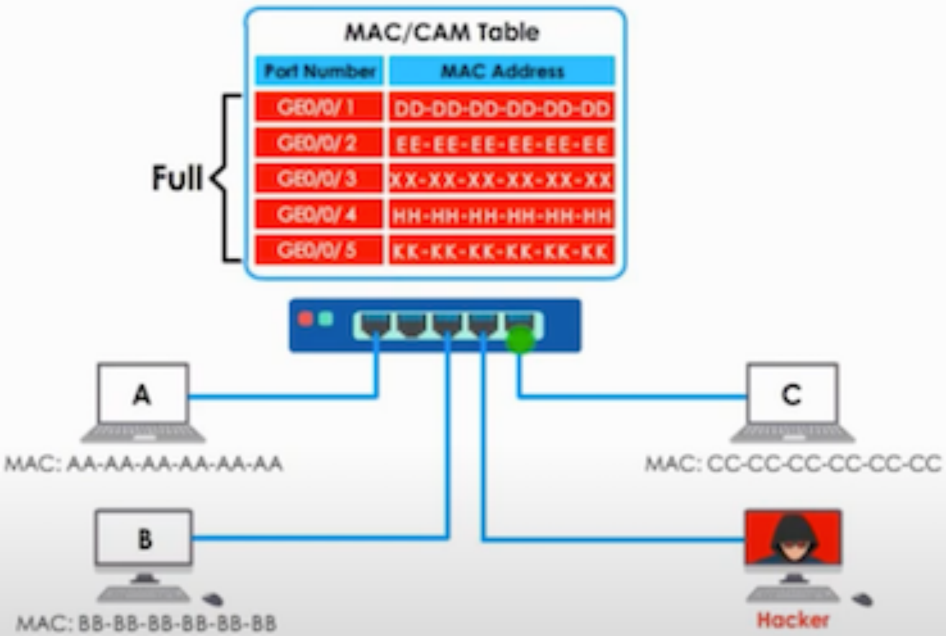


MAC/CAM Table

Port Number	MAC Address
GE0/0/ 1	AA-AA-AA-AA-AA-AA
GE0/0/ 2	EE-EE-EE-EE-EE-EE
GE0/0/ 3	BB-BB-BB-BB-BB-BB
GE0/0/ 4	HH-HH-HH-HH-HH-HH
GE0/0/ 5	Null

Security - switch flooding/poisoning

- The attacker floods the switch with fake MAC addresses until the switch table is filled.
- The switch forwards traffic to all interfaces (A, B, C), but because the addresses are fake, the switch will flood the network.
    - The network will slow down or crash

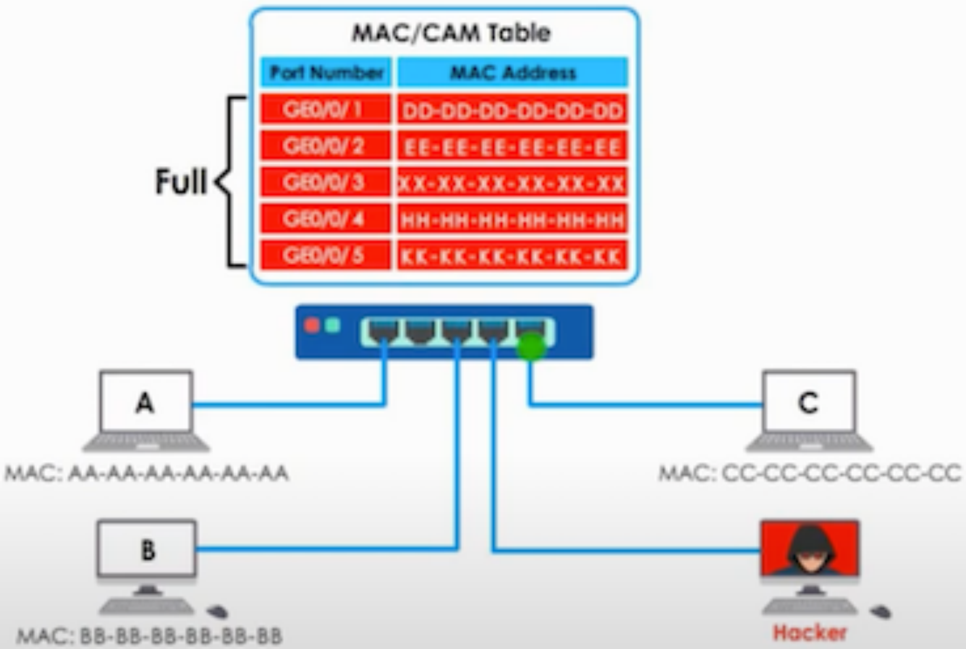


MAC/CAM Table

Port Number	MAC Address
GE0/0/1	DD-DD-DD-DD-DD-DD
GE0/0/2	EE-EE-EE-EE-EE-EE
GE0/0/3	XX-XX-XX-XX-XX-XX
GE0/0/4	HH-HH-HH-HH-HH-HH
GE0/0/5	KK-KK-KK-KK-KK-KK

Security - switch flooding/poisoning

- when a legitimate device wants to communicate with the switch, it will broadcast any received traffic to the whole network.
- once the attacker gets access to the traffic, they can carry out all types of attacks.
  - Man-in-the-middle attack
  - Eavesdropping
  - Network sniffing



MAC/CAM Table

Port Number	MAC Address
GE0/0/1	DD-DD-DD-DD-DD-DD
GE0/0/2	EE-EE-EE-EE-EE-EE
GE0/0/3	XX-XX-XX-XX-XX-XX
GE0/0/4	HH-HH-HH-HH-HH-HH
GE0/0/5	KK-KK-KK-KK-KK-KK

Mitigations for switch flooding

- by limiting the number of MAC addresses that can be learned at each port.
  - Instead of 25K addresses, you limit the number of addresses to 10 or 15.
- by checking if MAC addresses are legitimate.
  - Checking addresses w.r.t. to a set of predefined MAC addresses.

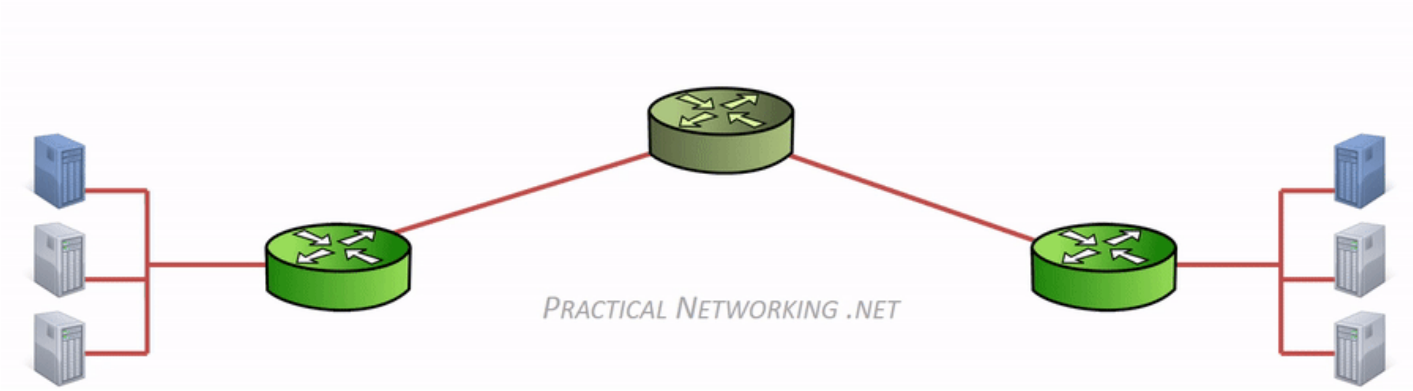
Exercise - security of MAC filtering

The uniqueness of MAC addresses means that people use them as a form of access control, for example, using MAC addresses to restrict access to wireless networks.

- How effective is this in preventing an attacker from joining the network?
  - This will prevent any unauthorised access
  - This will not prevent any unauthorised access.

Summary

- Ethernet is designed for local area networks (LANs), and carries the IP datagram.
- The datagram consists not only of an IP frame but also includes (information on) subsequent layers: TCP, UPD, HTTP
- Ethernet frames are transferred between network adapters (NICs), uniquely identified through MAC addresses.
- MAC address = OUI + NIC


PRACTICAL NETWORKING .NET