Redes de Computadores II

Universidade do Algarve

Aulas Teóricas 3 e 4
Semana 2

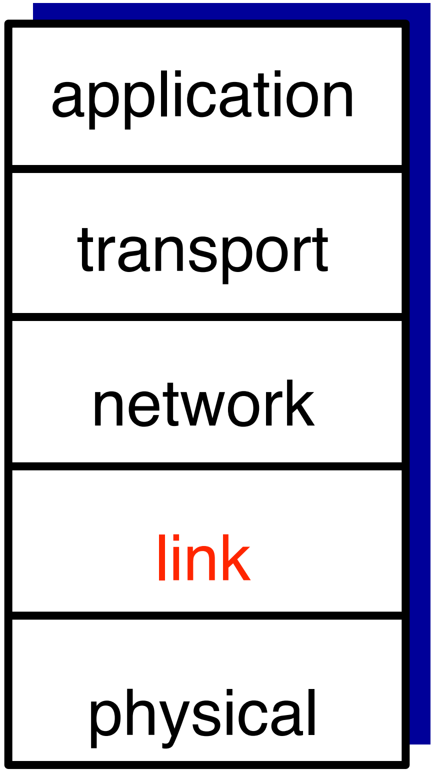
https://github.com/ncatanoc/redes_algarve

Néstor Cataño
nestor.catano@gmail.com

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
6. Error detection and correction

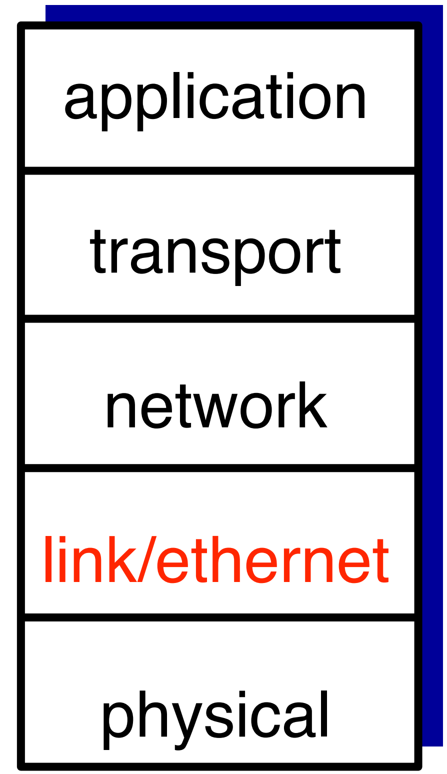
Recap: the 4-layers model

application: supporting network applications.

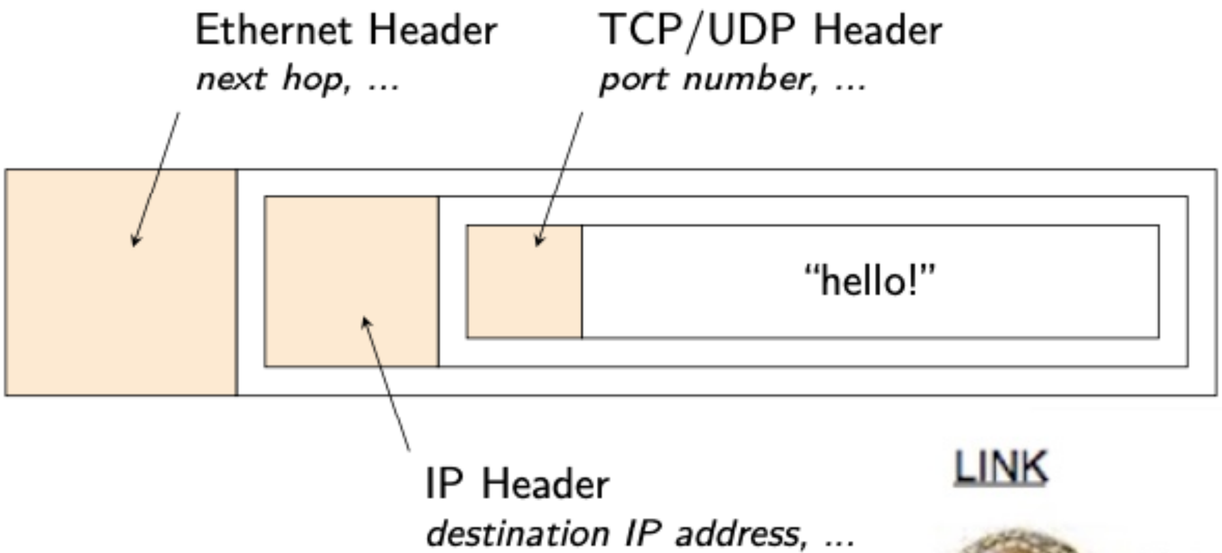
transport: process-process data transfer.

network: routing of datagrams from source to destination.

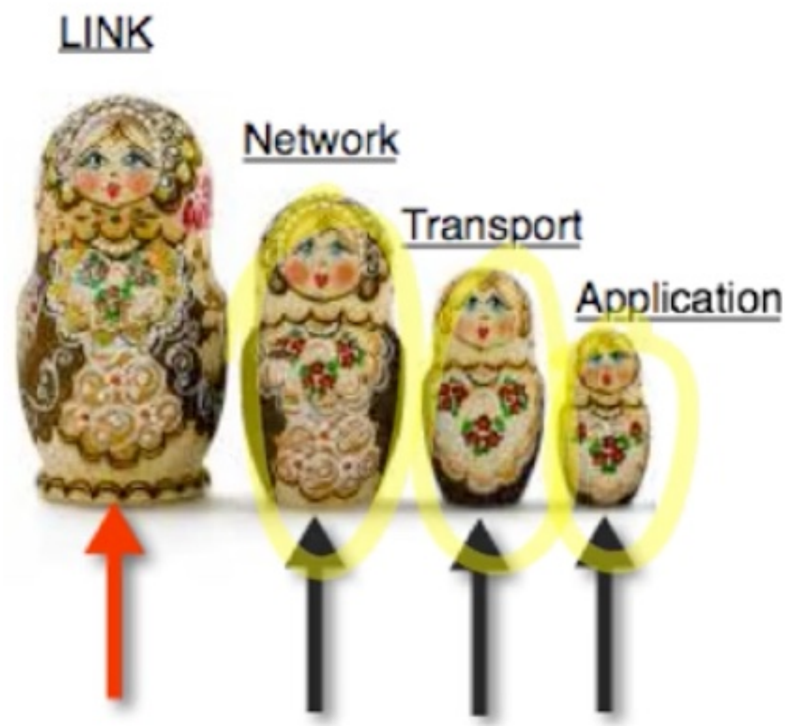
link: data transfer between neighbouring network elements.



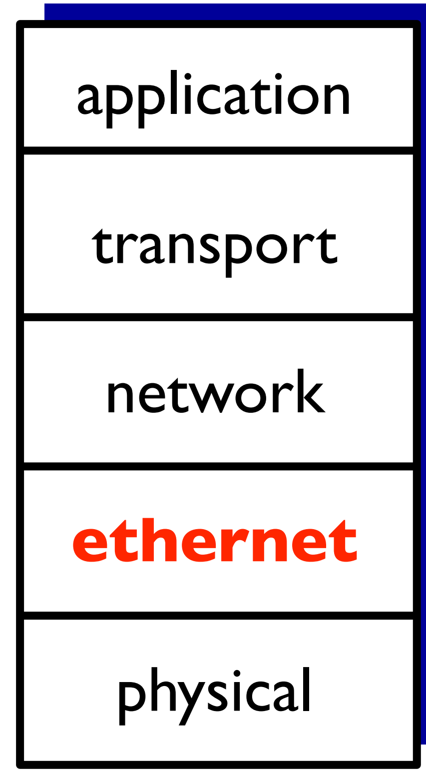
Recap: datagrams



Application HTTP, DNS, ...
Transport TCP, UDP
Internetwork IP
Link Ethernet



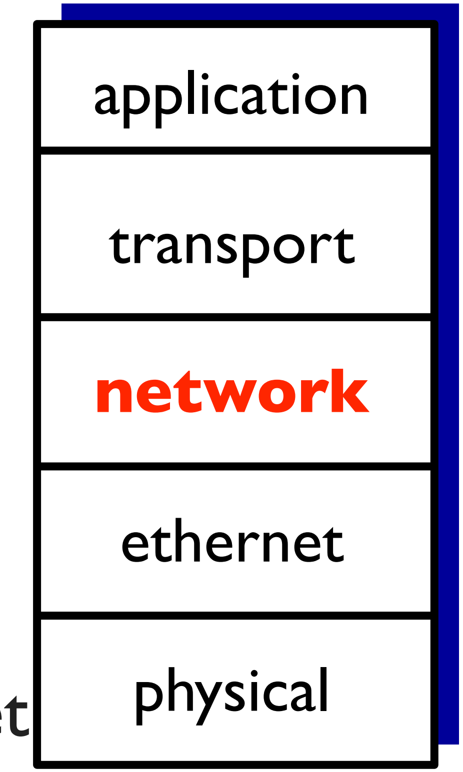
ethernet - data transmission



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

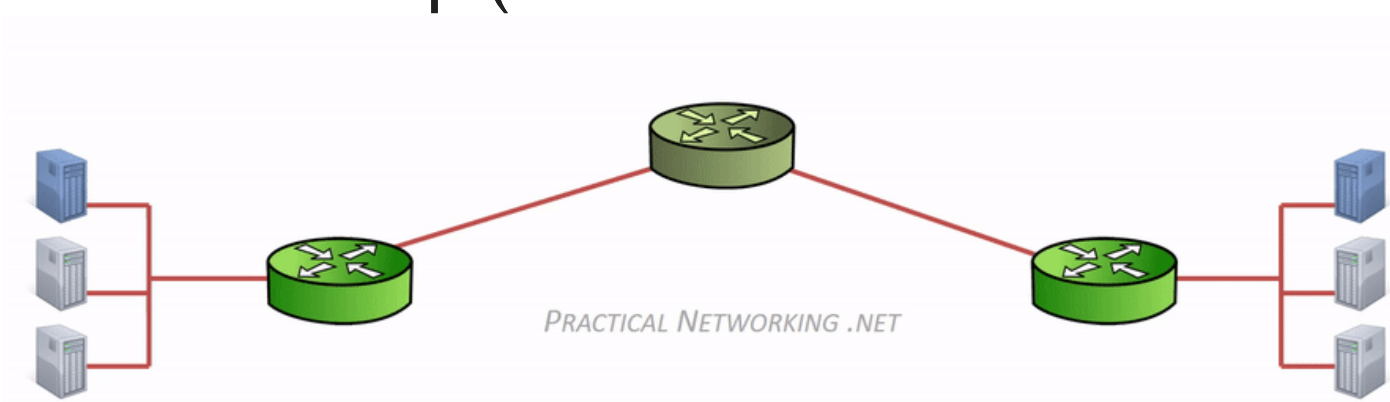
- The MAC address uniquely identifies each individual NIC (network interface controller).
- Besides your NIC, a switch also works at this level
- **hop** is a term that refers to the number of routers a packet (a portion of data) passes through from source to destination.

network - data transmission



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

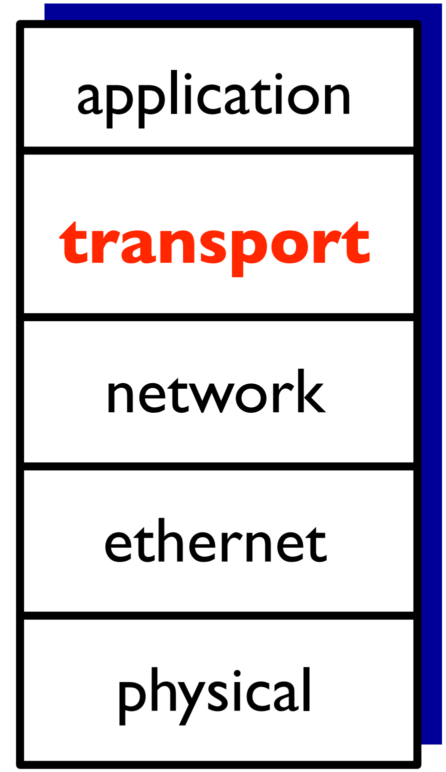
- it uses IP addresses.
- when a computer has data to send, it encapsulates the data in an IP header, including information such as the Source and Destination IP address.
- between each router, the MAC address header is stripped and regenerated to get the next hop (router

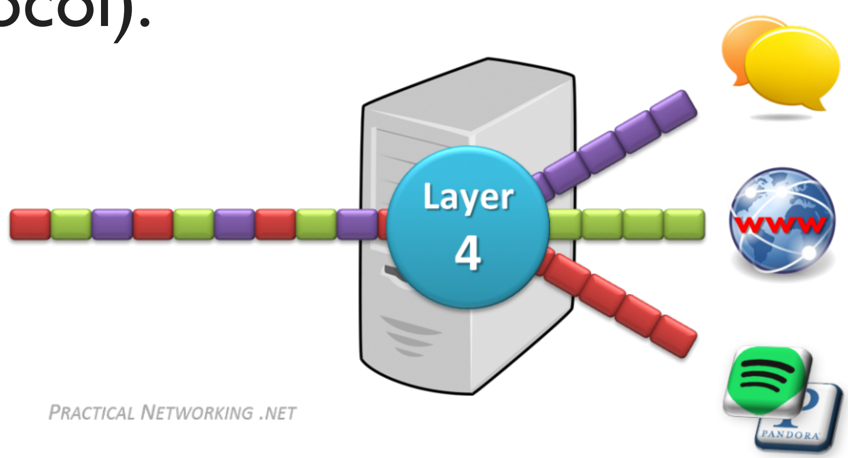


data transmission

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).





data transmission

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

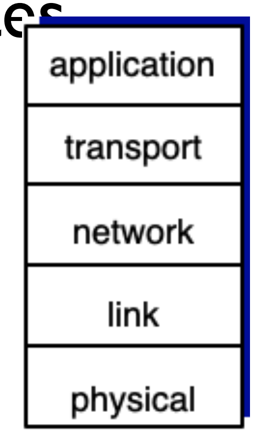
- The whole datagram is referred to as a **segment**.

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**.



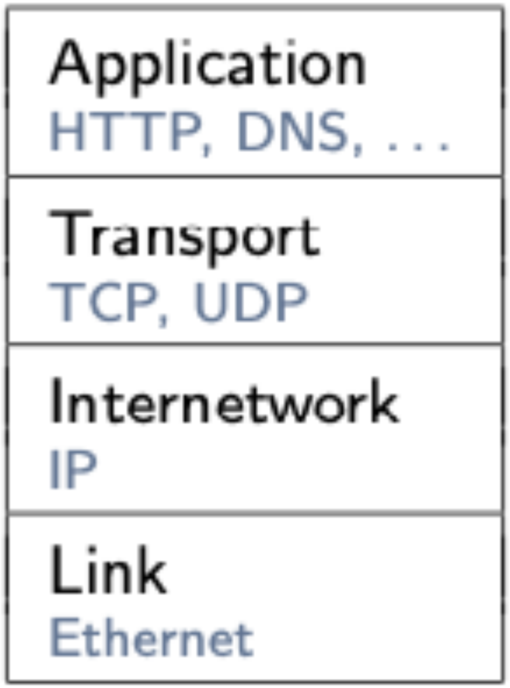
Roadmap

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

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.



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 signalling 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 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?

3 frames x 1500 bytes = 4500 bytes
1 frame of 900 bytes

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?

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?

3021

How many ethernet frames will this be?

2 frames x 1500 bytes = 3000 bytes
1 frame of 21 bytes plus 25 bytes of padding

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
   1. security considerations
5. Error detection and correction

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.

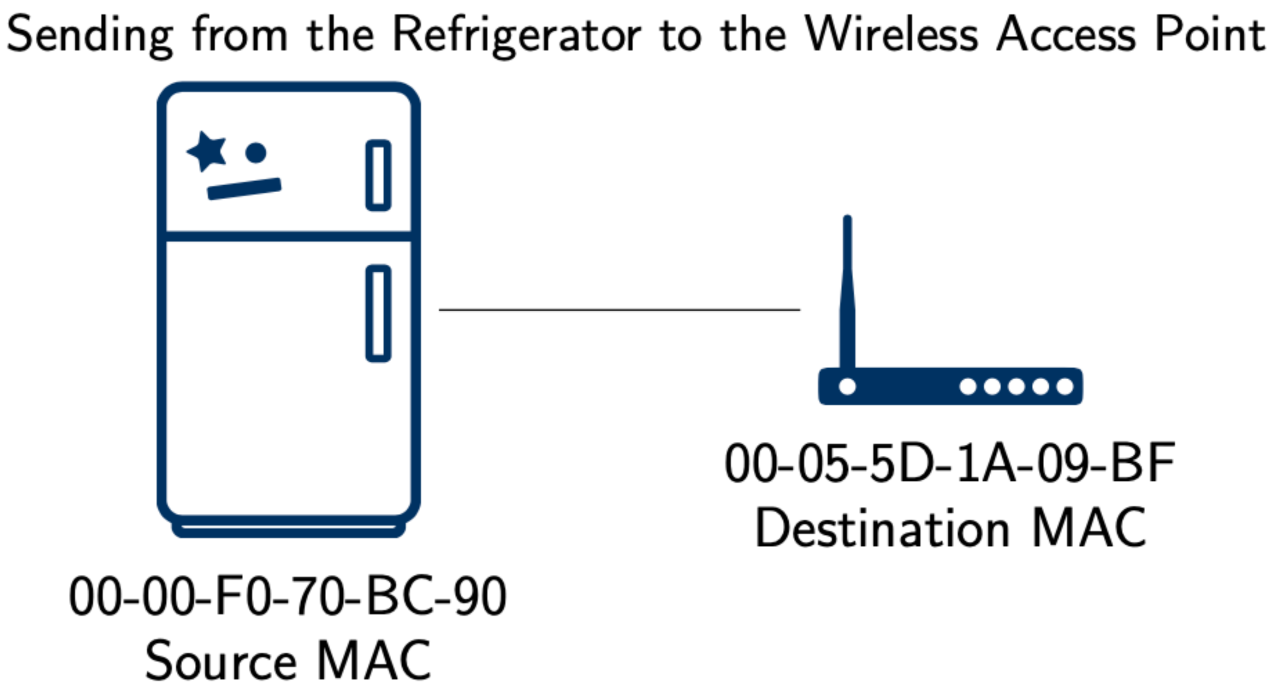
What about datagrams from other networks beyond the LAN?

- 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

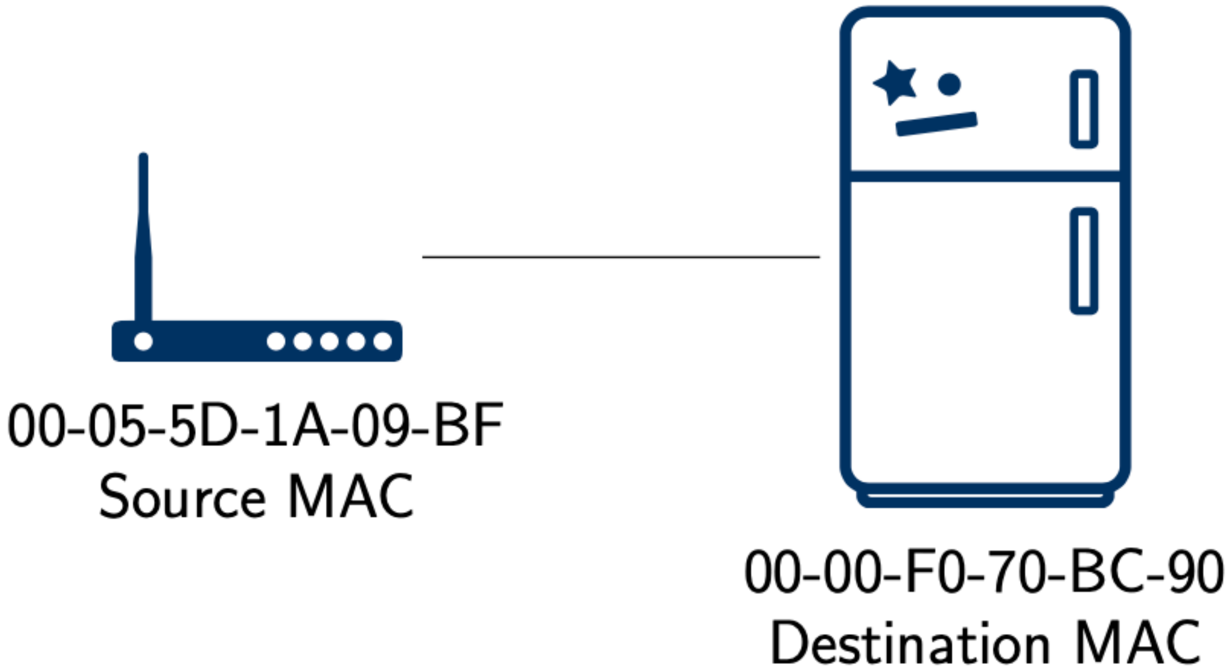
The refrigerator builds a frame with the Source equals to 00-00-F0-70-BC-9 and the Destination equals to 00-05-5D-1A-09-BF



example 1

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

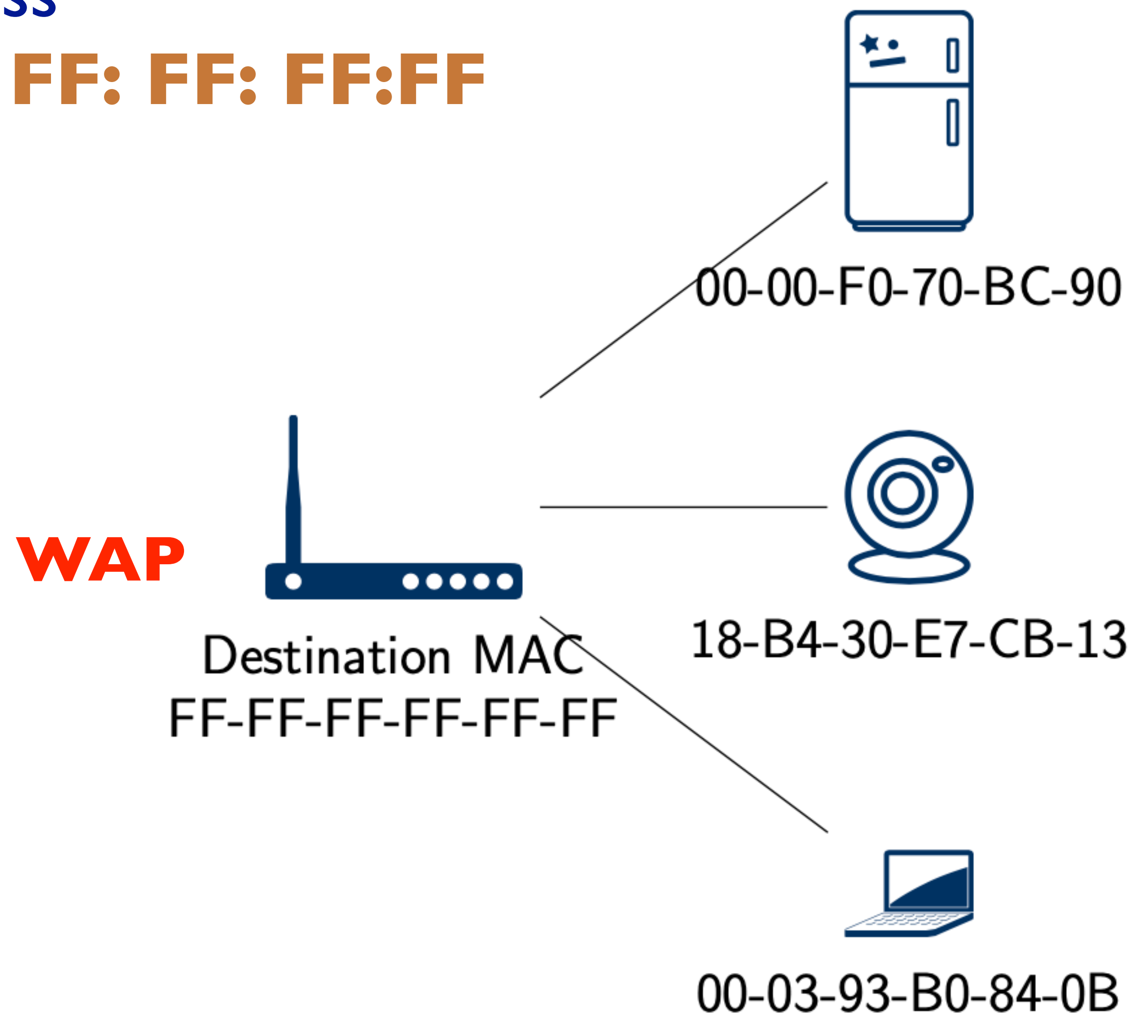
Sending from the Wireless Access Point to the Refrigerator



example 2 - broadcasting

- The Wireless Access Point (WAP) broadcasts the MAC address

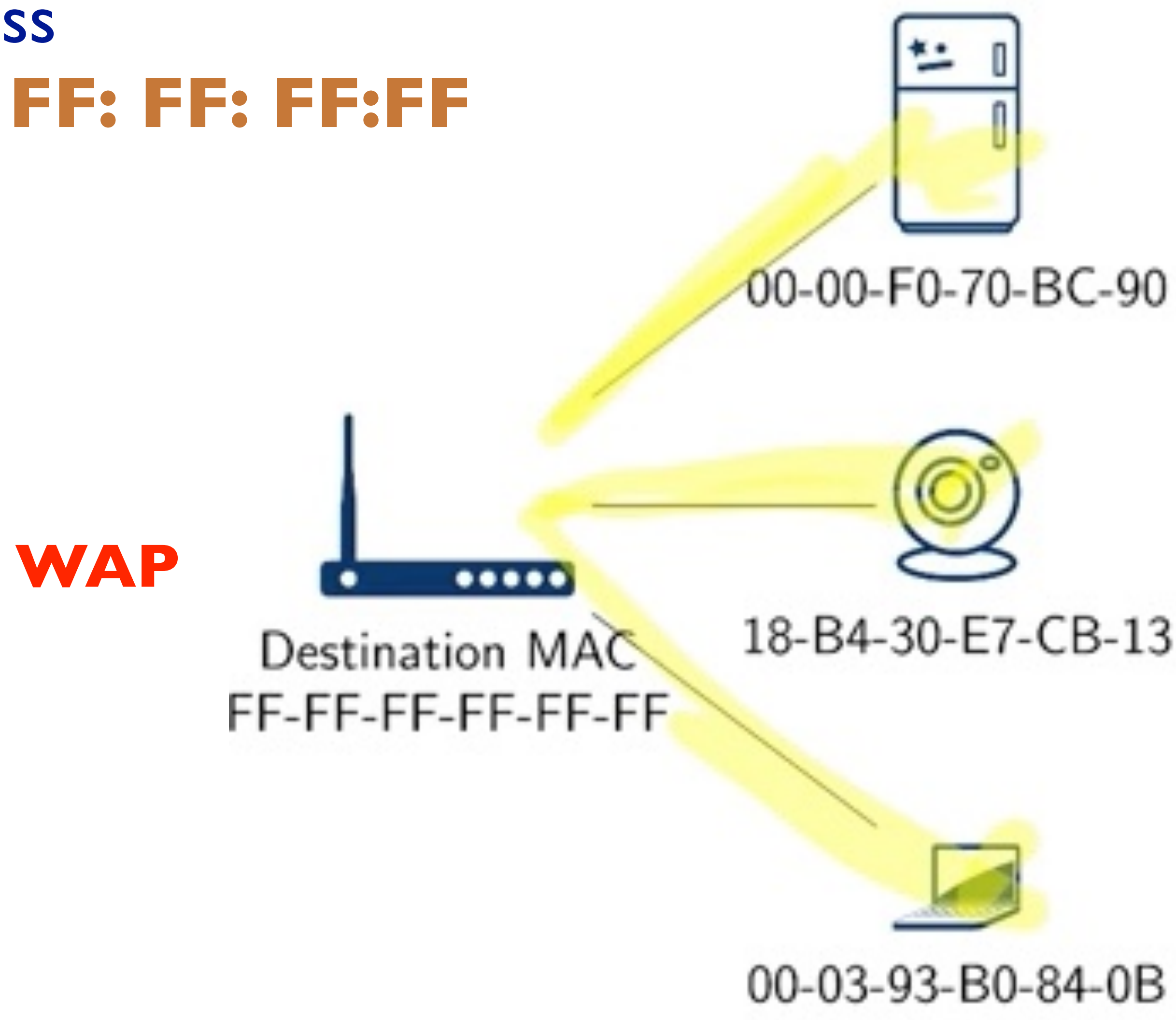
    FF: FF: FF: FF: FF:FF



example 2 - broadcasting

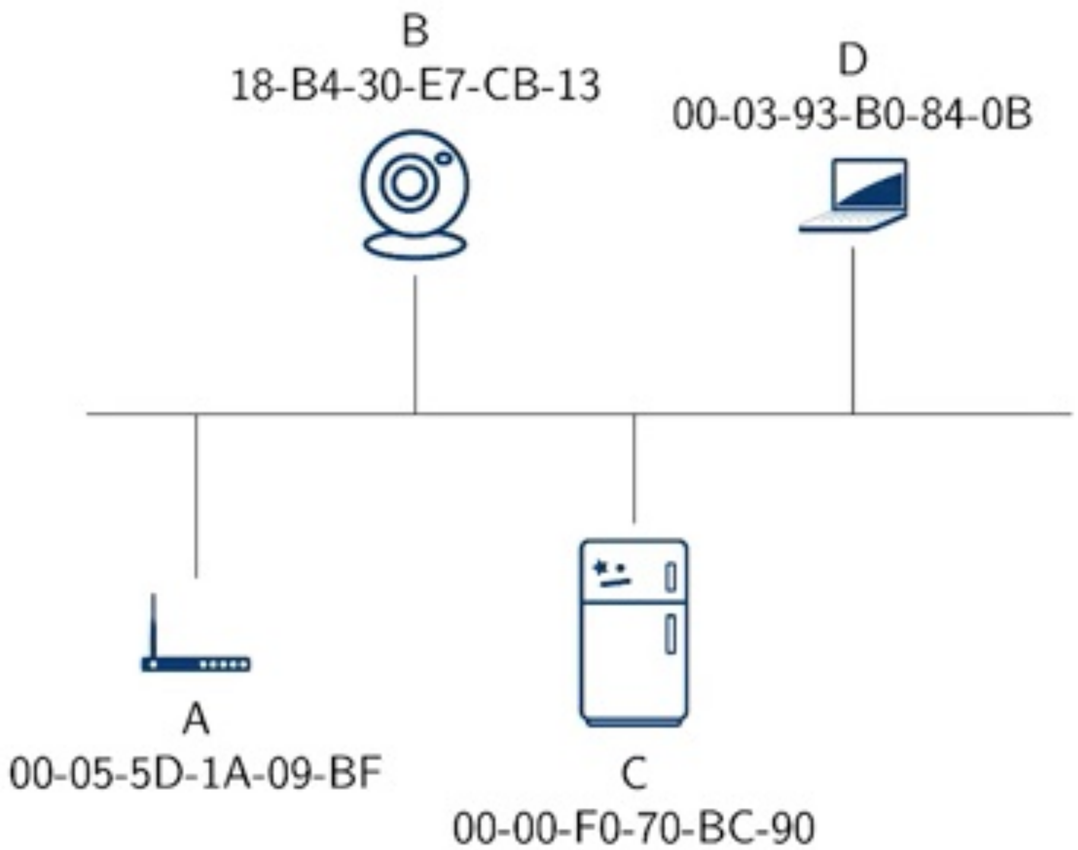
- The Wireless Access Point (WAP) broadcasts the MAC address

  FF: FF: FF: FF: FF:FF



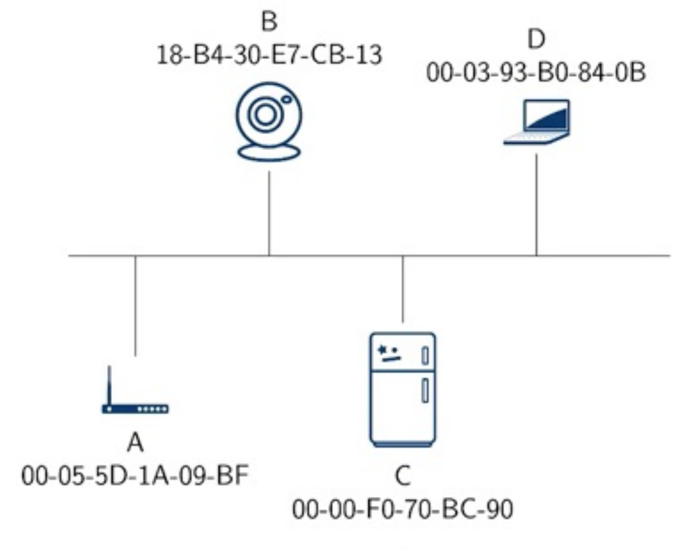
exercise - broadcasting

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

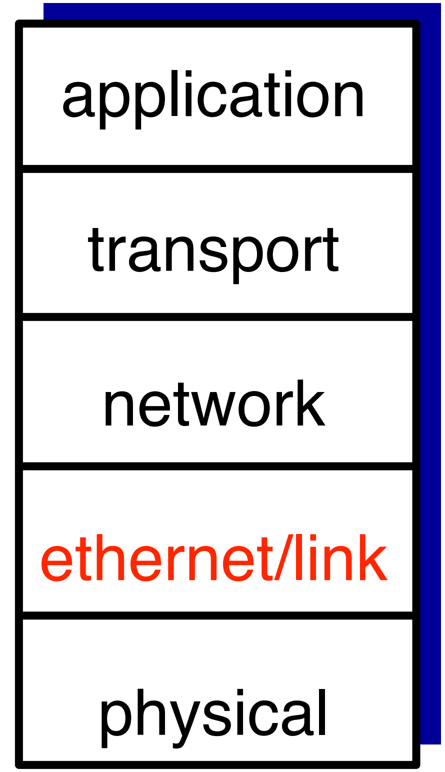


exercise - broadcasting

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



Summary



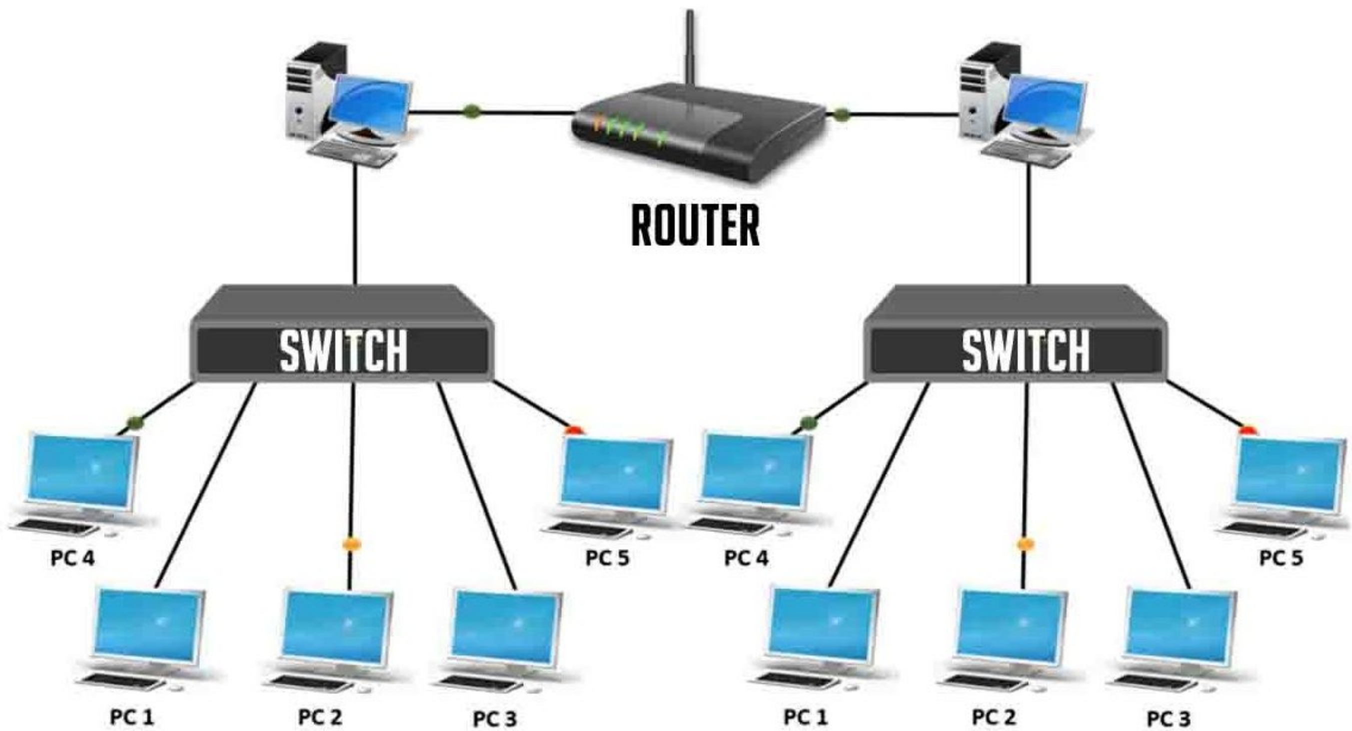
1. Ethernet is designed for local area networks and carries the IP datagram.
2. Ethernet addresses are MAC addresses
3. MAC addresses have a specific format, including an **OUI**.
4. **Next**: transferring data through **switching**

Roadmap

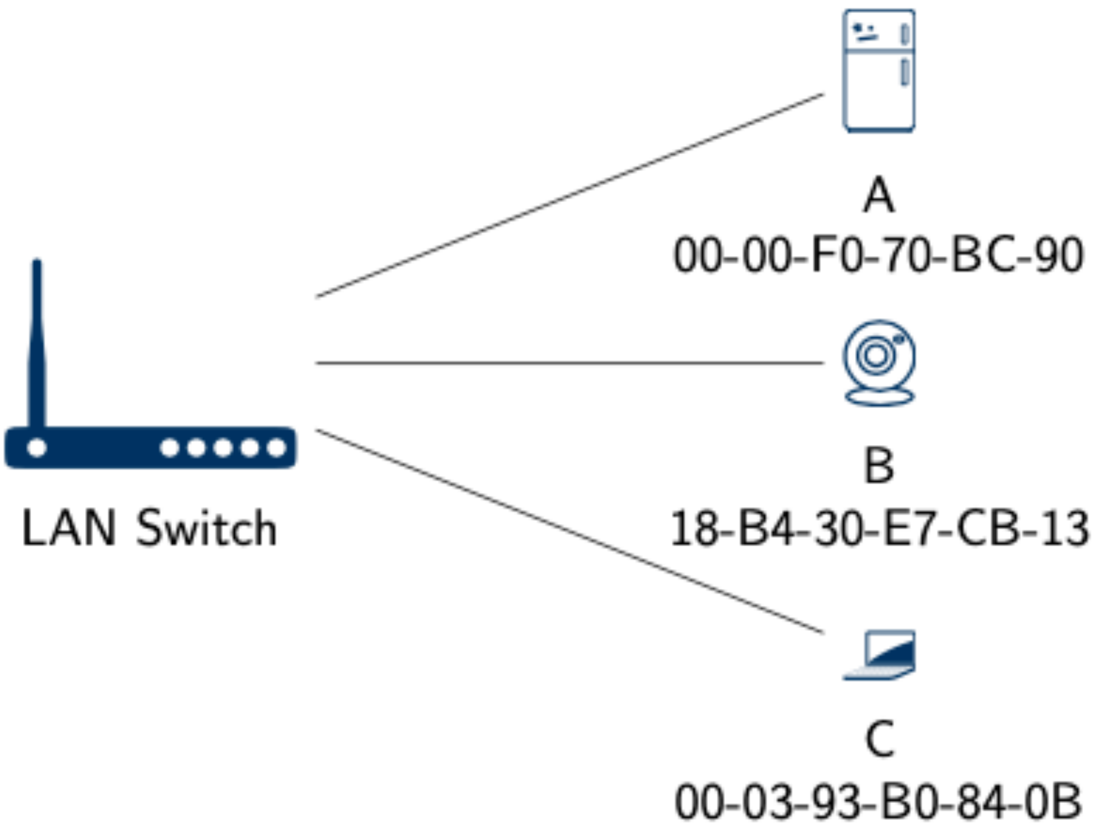
1. Datagrams
2. The link (ethernet) layer
   - ethernet frames, MAC addresses
3. Broadcasting
4. Switching
   1. security considerations
5. Error detection and correction

Switching and 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.



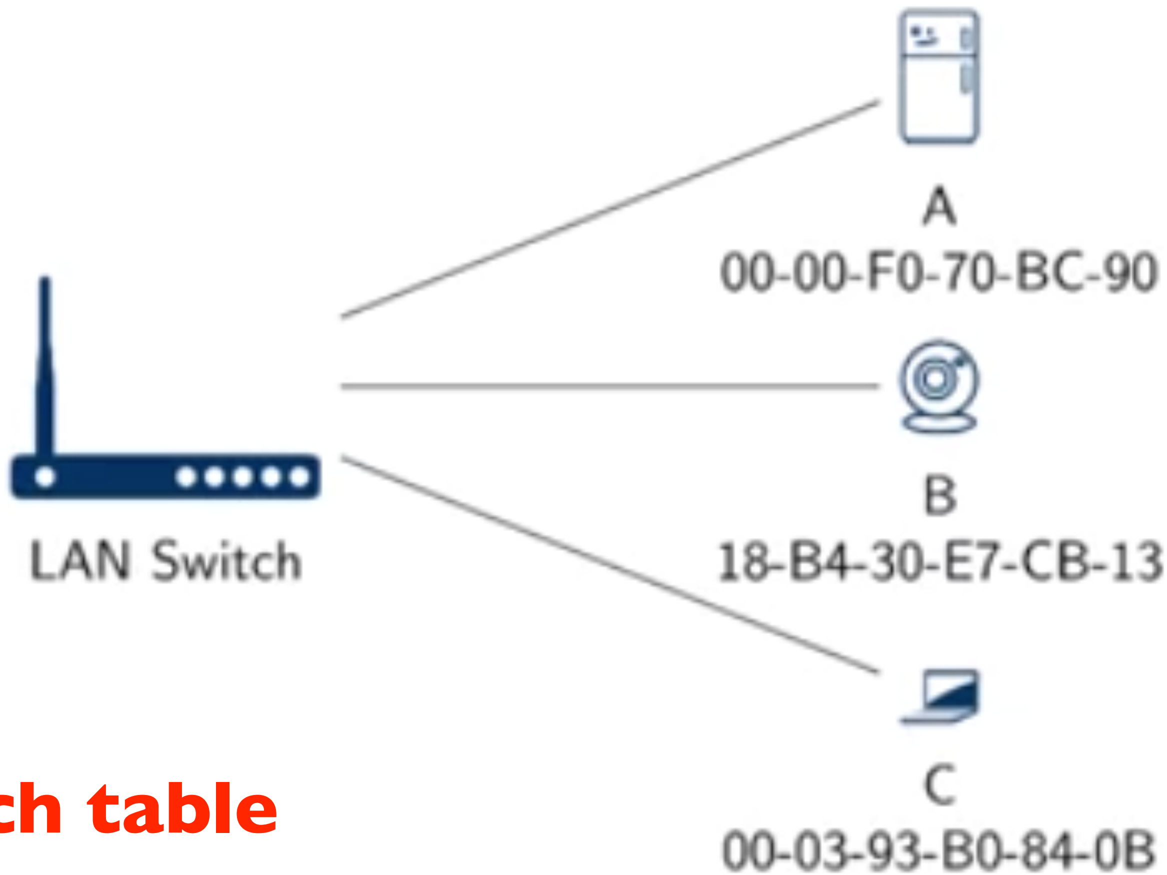
Switching example



Switch table

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

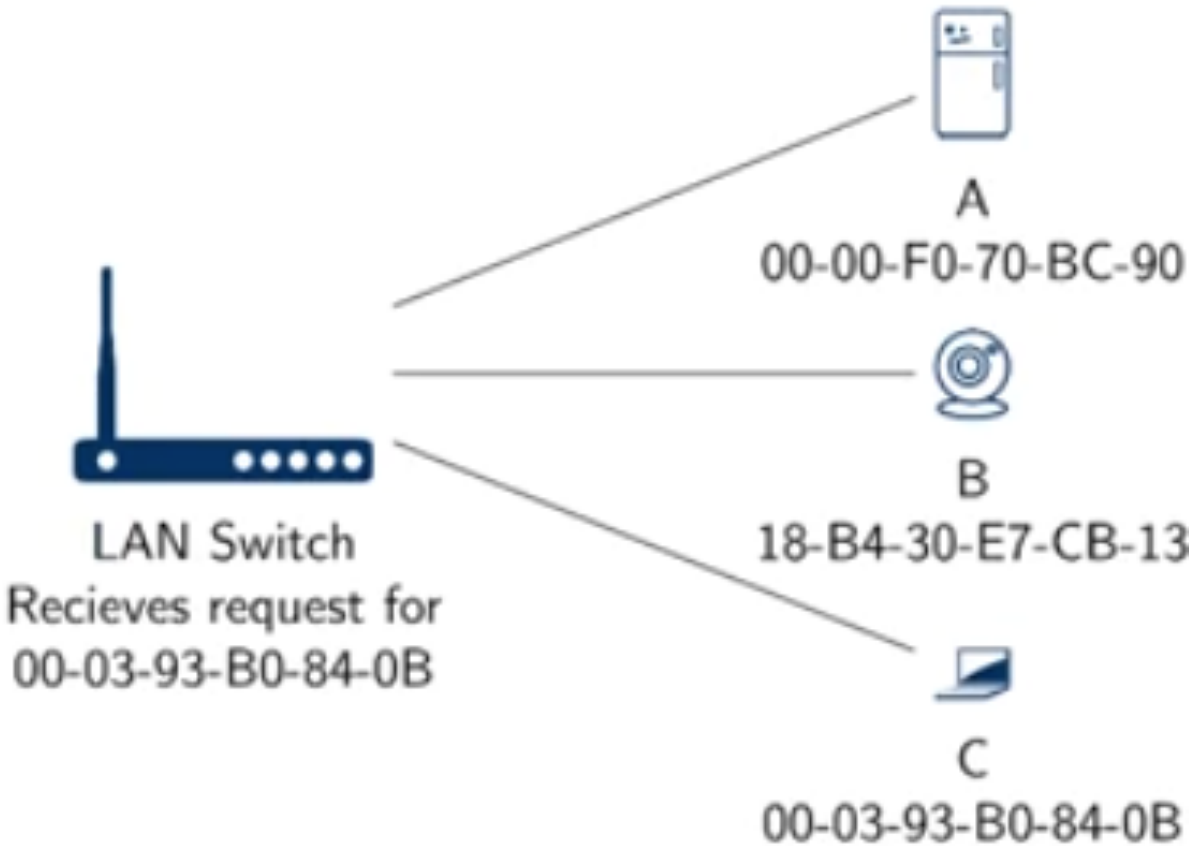
How does the switch build its table?



Switch table

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

How does the switch build its table?



Switch table

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

How does the switch build its table?

1. The 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 also records the time it received the transmission.
4. Aging: entries are allowed for a fixed time.

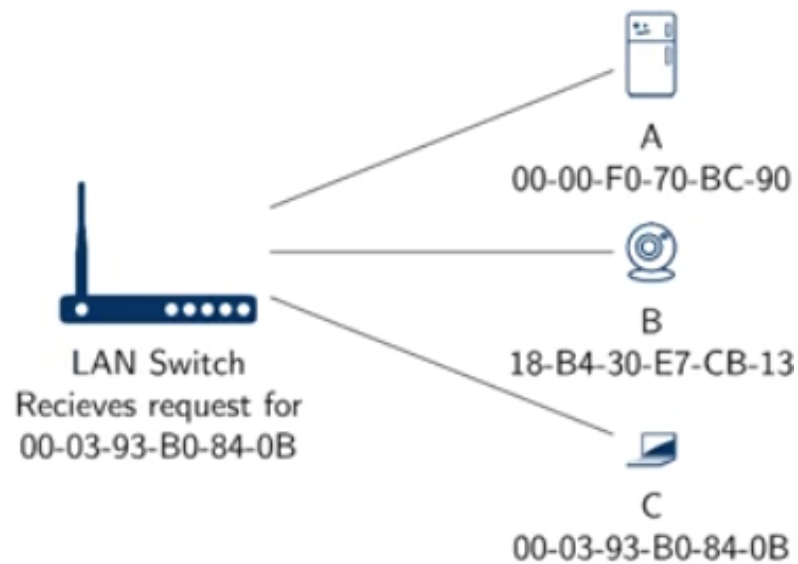
Switch table

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

A message sent to 0C:0C:0b:14:cd:98 is transmitted over port 2

flooding

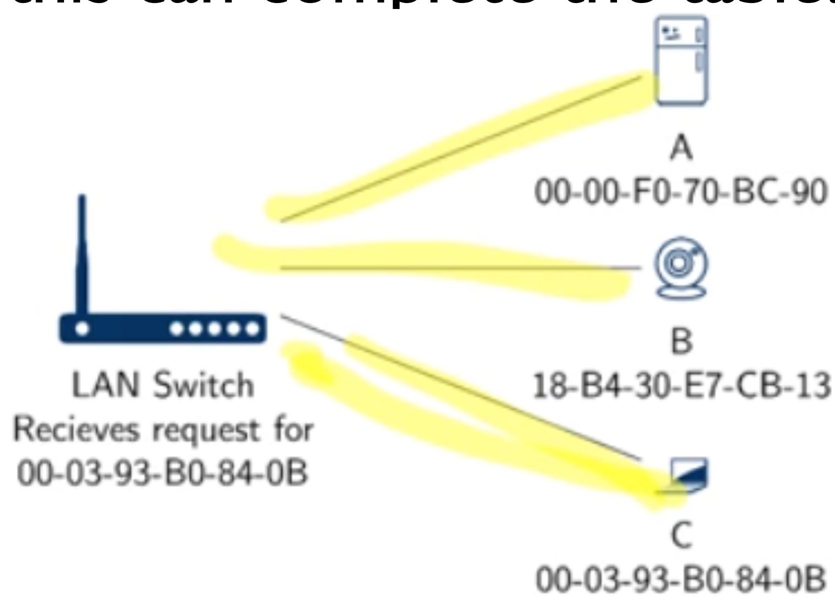
- **What happens when a switch does not know the packet destination?**
    - Message is sent to C (00-03-93-B0-84-0B), but C is not in the switch table.



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

flooding

- In that case the **the switch floods** all the ports
  - it sends a message to each port
- This causes port C (and the other ports) to send a message to the LAN so this can complete the table.



Switch table

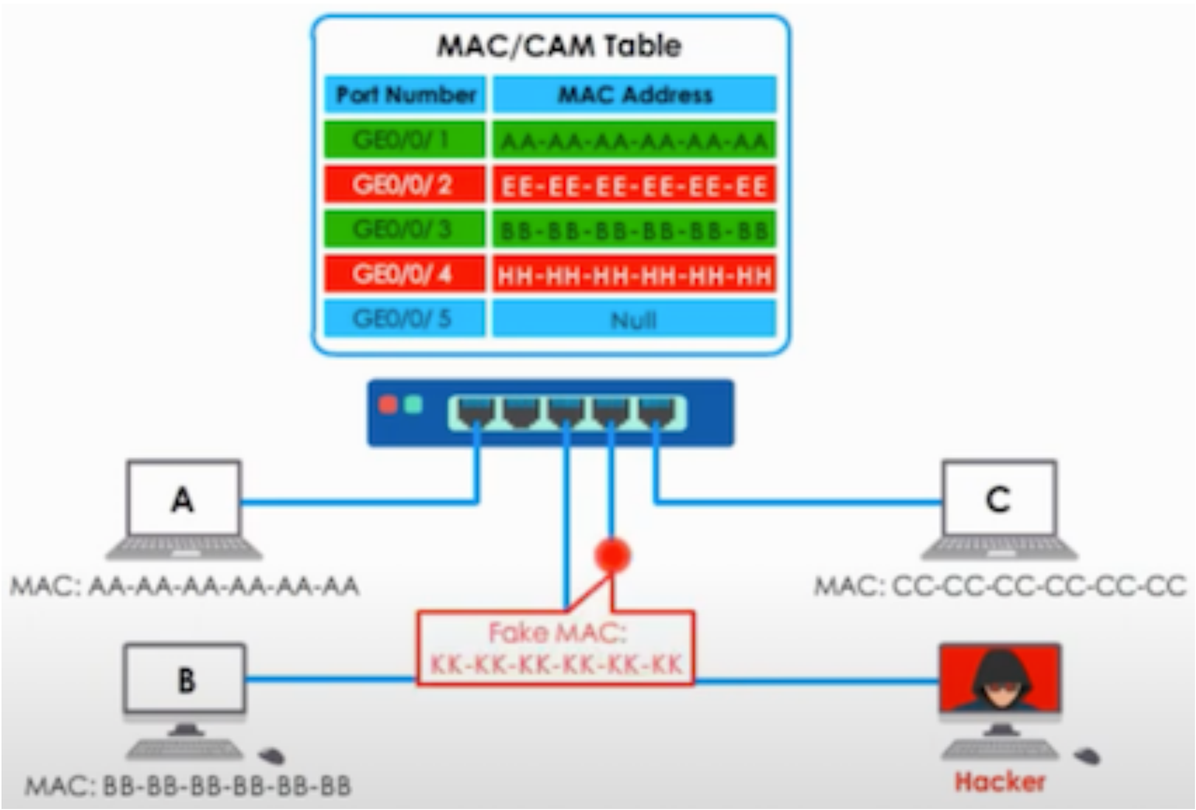
MAC Address	Port	time
00-00-F0-70-BC-90	1	12:20
18-B4-30-E7-CB-13	2	12:35
??	3	

Roadmap

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

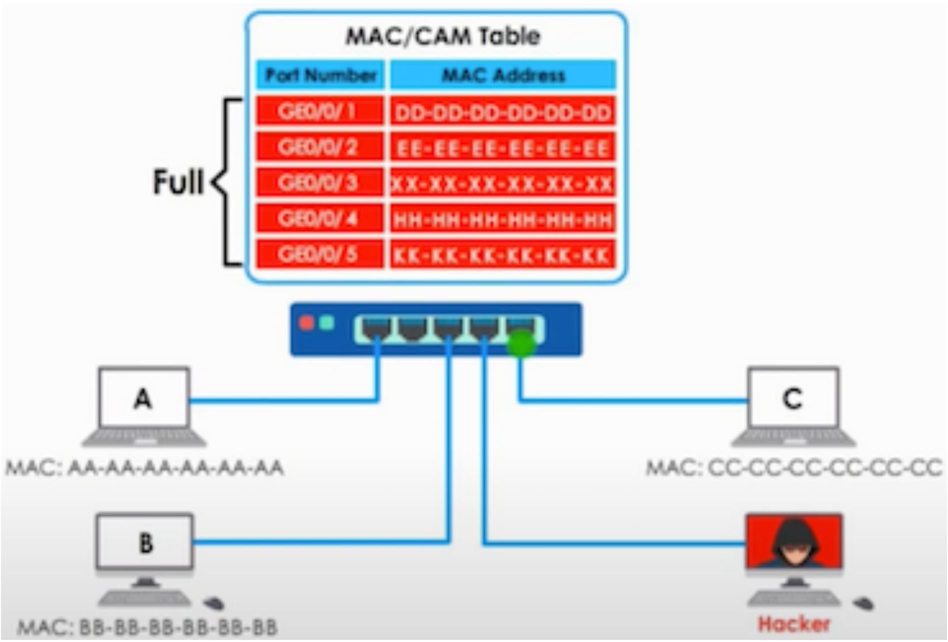
Security - switch flooding/poisoning

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



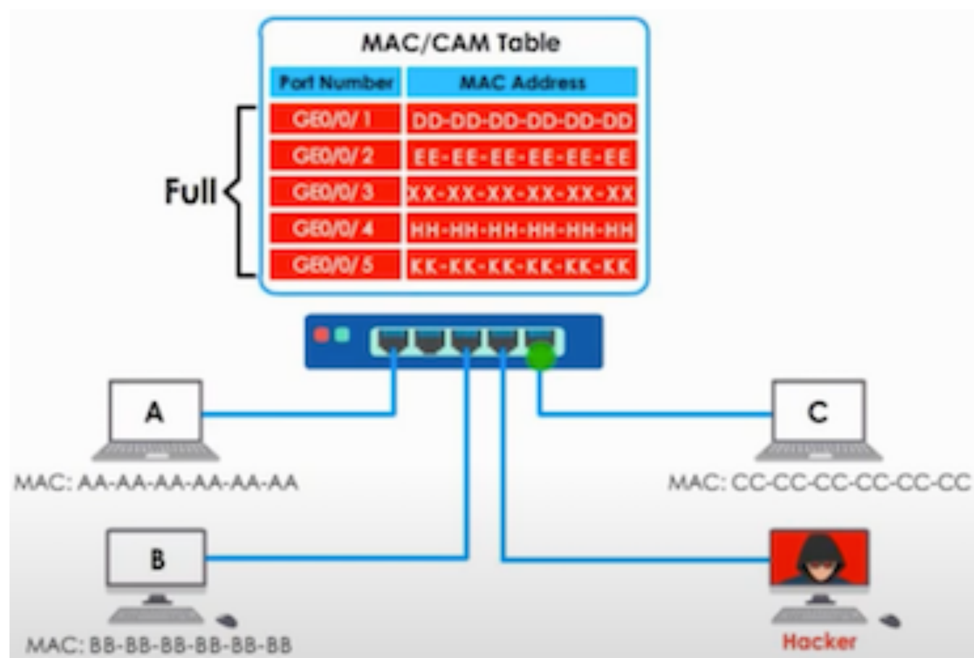
Security - denial of service attack

- 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

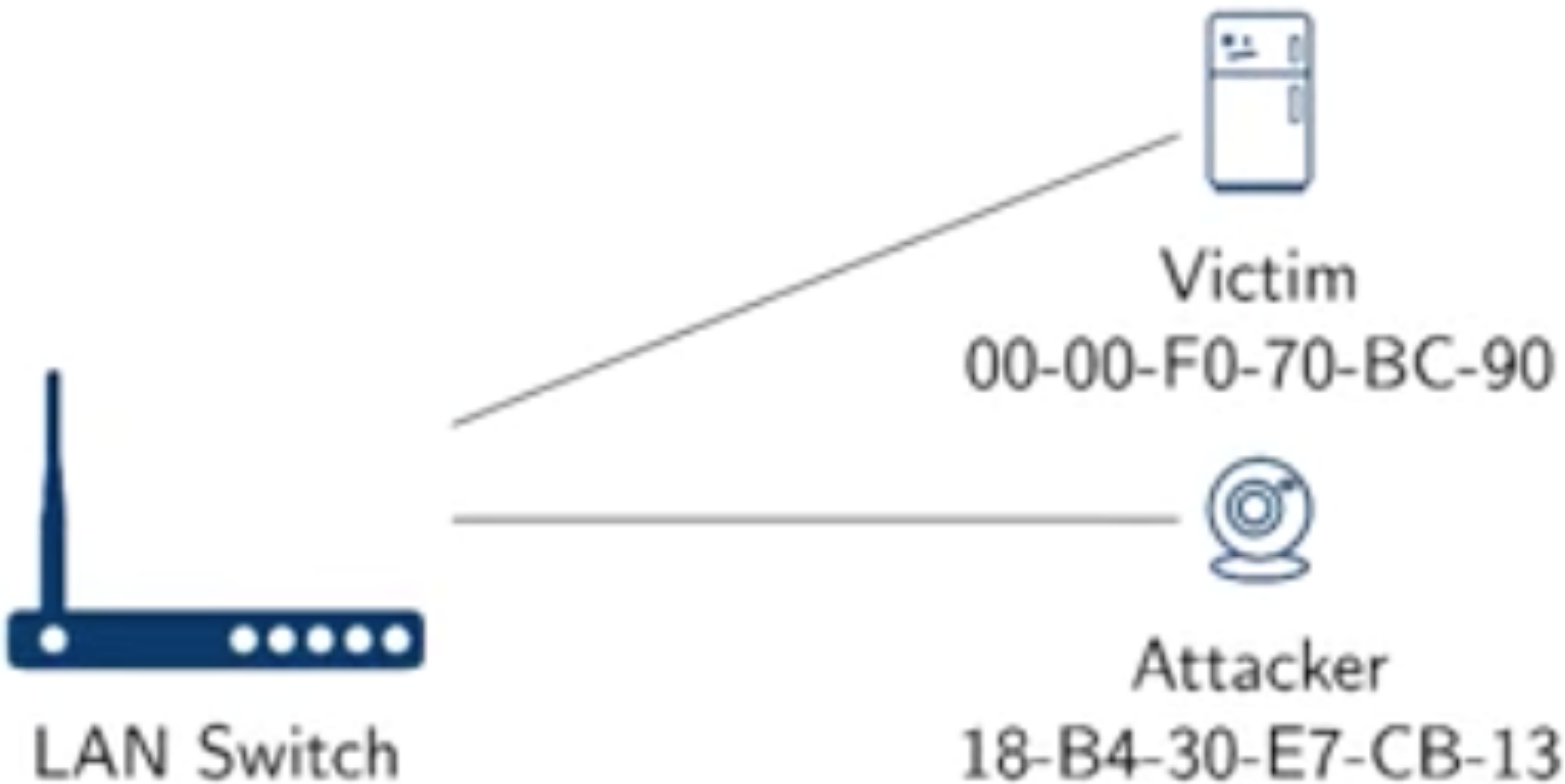


Security - network sniffing

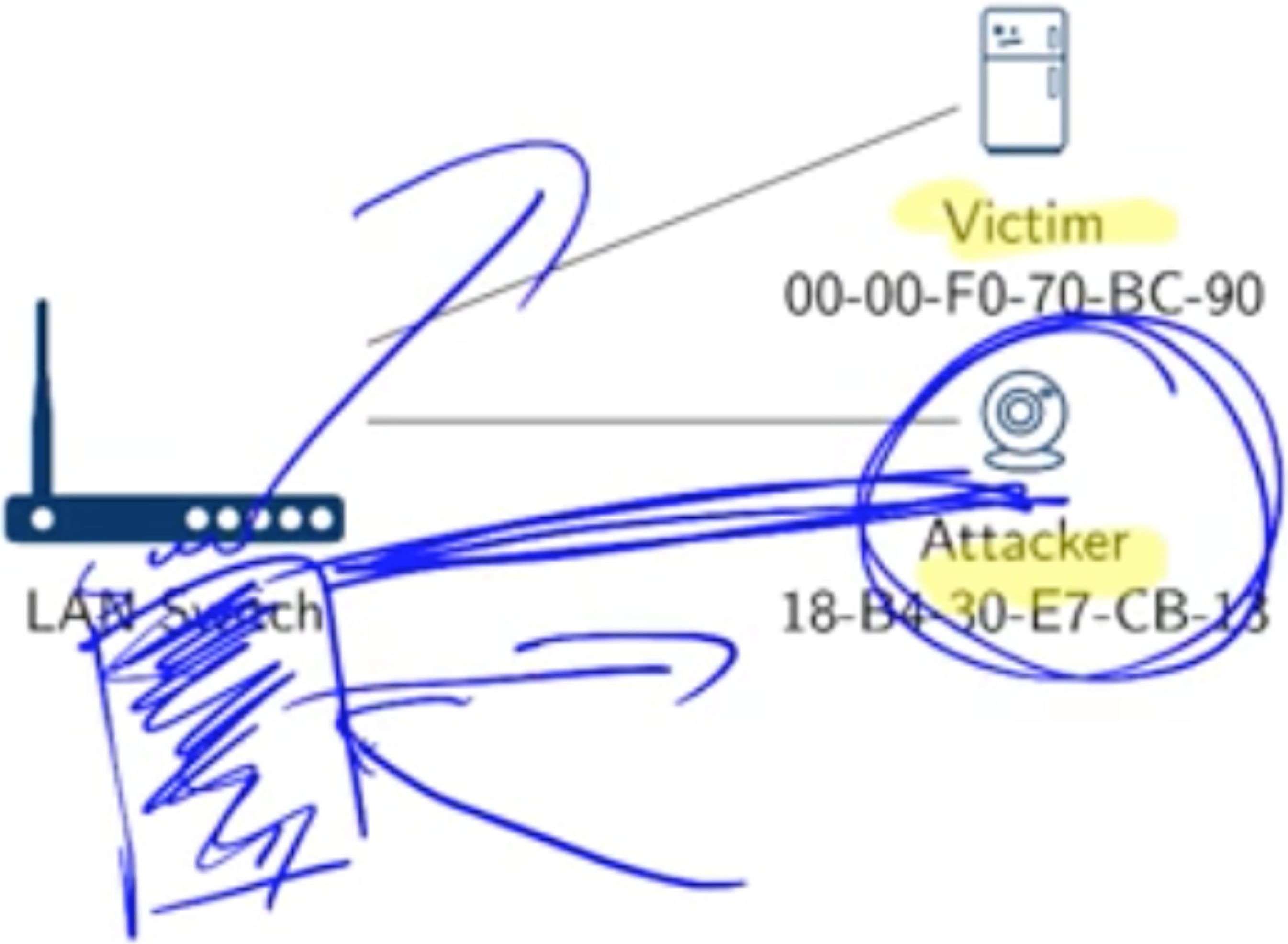
- when a legitimate device wants to communicate with the switch, it will broadcast any received traffic to the whole network.
- once the attacker gets access to the traffic, they can carry out all types of attacks.
  - Man-in-the-middle attack
  - Eavesdropping
  - Network sniffing



Security attack



Security attack



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.

Quiz - security

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.

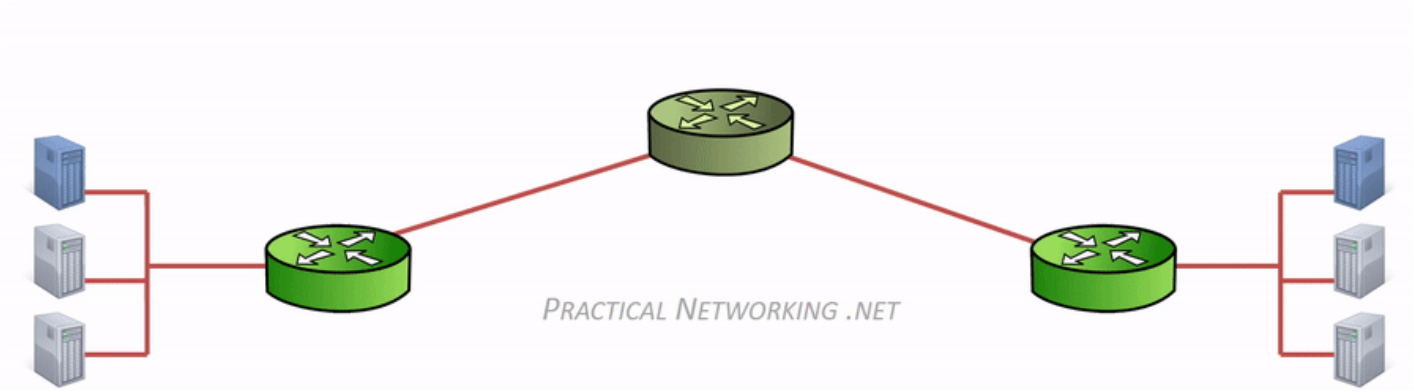
http://menti.com
Code = 1867 6956

Quiz - security

Answer: MAC addresses can be changed and spoofed so they are not a very form of access control.

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



Roadmap

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

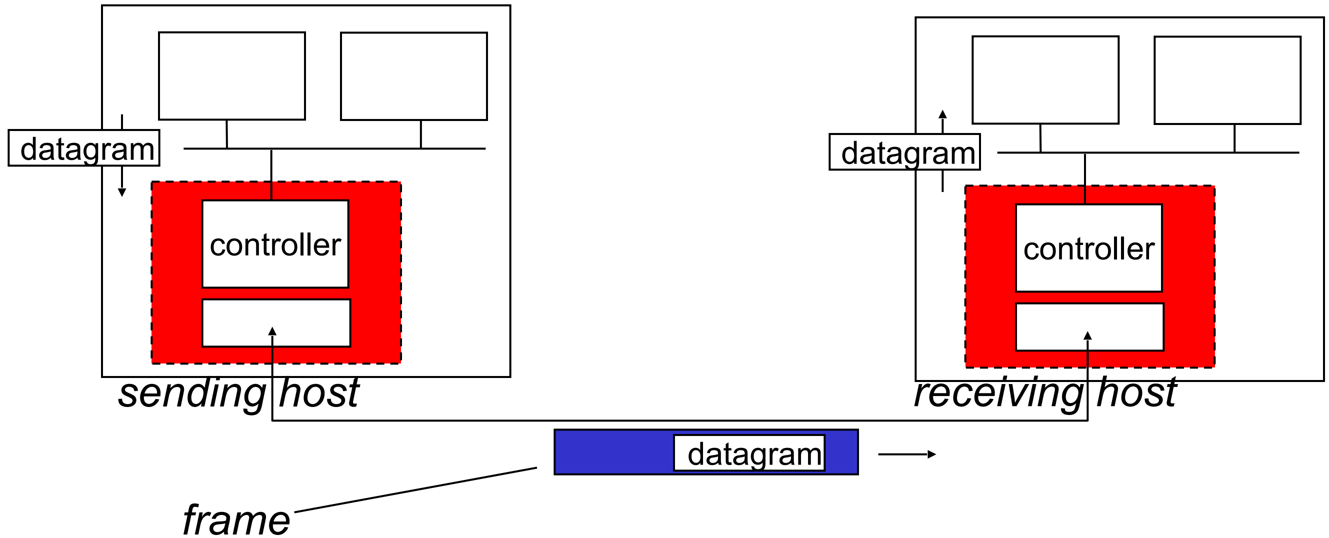
Link layer services

- **framing, link access:**
  - encapsulate datagram into frame, adding header, trailer
  - channel access if shared medium
  - “MAC” addresses used in frame headers to identify source, destination
    - different from IP address!
- **reliable delivery between adjacent nodes**
  - we learned how to do this already (chapter 3)!
  - seldom used on low bit-error link (fiber, some twisted pair)
  - wireless links: high error rates
    - Q: why both link-level and end-end reliability?

Link layer services (more)

- flow control:
  - pacing between adjacent sending and receiving nodes
- error detection:
  - errors caused by signal attenuation, noise.
  - receiver detects the presence of errors:
    - signals sender for retransmission or drops frame
- error correction:
  - receiver identifies and corrects bit error(s) without resorting to retransmission
- half-duplex and full-duplex
  - with half duplex, nodes at both ends of link can transmit, but not at same time

Adaptors communicating

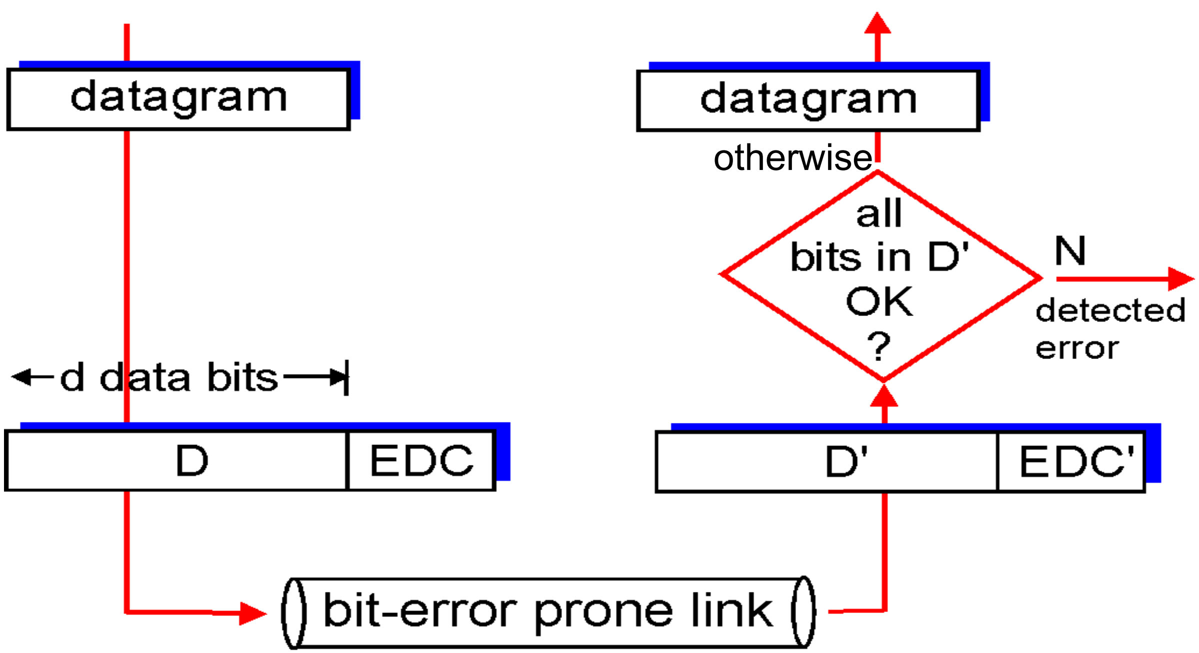


- sending side:
  - encapsulates datagram in frame
  - adds error checking bits, rdt, flow control, etc.
- receiving side
  - looks for errors, rdt, flow control, etc.
  - extracts datagram, passes to upper layer at receiving side

Error detection

EDC= Error Detection and Correction bits (redundancy)
D = Data protected by error checking, it may include header fields

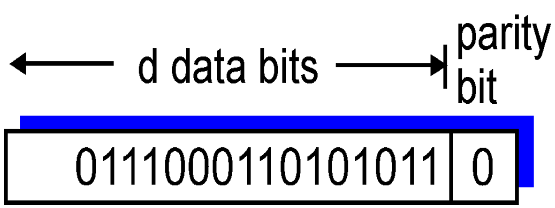
- Error detection is not 100% reliable!
    - protocol may miss some errors, but rarely
    - larger EDC field yields better detection and correction



Parity checking

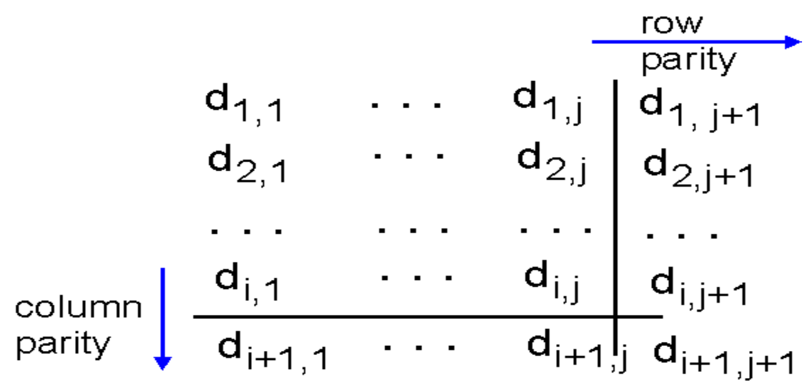
single bit parity:

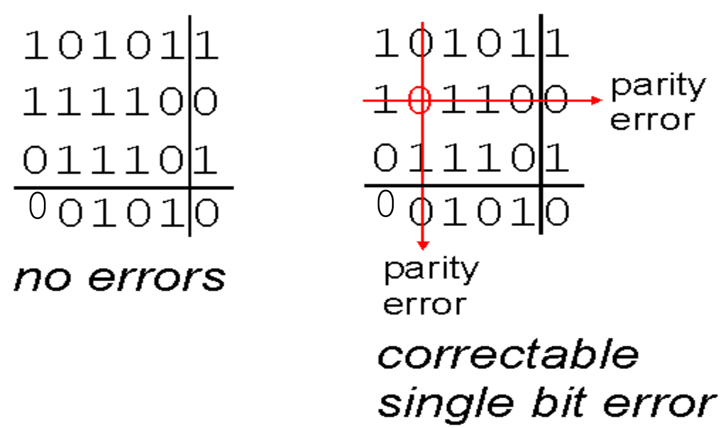
- detect single-bit errors



two-dimensional bit parity:

- detect and correct single-bit errors





Internet checksum (review)

goal: detect "errors" (e.g., flipped bits) in the transmitted packet (note: used at transport layer only)

sender:

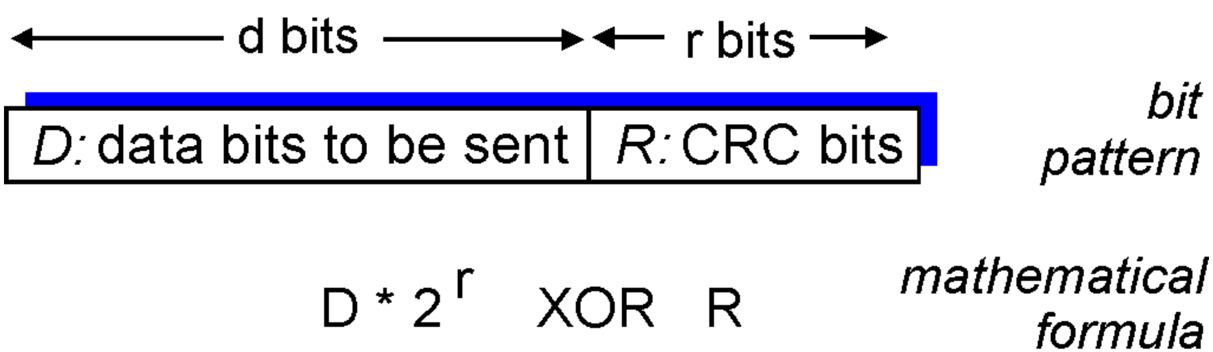
- treat segment contents as sequence of 16-bit integers
- checksum: addition (1's complement sum) of segment contents
- sender puts checksum value into UDP checksum field

receiver:

- compute checksum of received segment
- check if computed checksum equals checksum field value:
  - NO - error detected
  - YES - no error detected. But maybe errors nonetheless?

Cyclic redundancy check

- more powerful error-detection coding
- view data bits, D, as a binary number
- choose r+1 bit pattern (generator), G
- goal: choose r CRC bits, R, such that
  - <D,R> exactly divisible by G (modulo 2)
  - receiver knows G, divides <D,R> by G. If non-zero remainder: error detected!
  - can detect all burst errors less than r+1 bits
- widely used in practice (Ethernet, 802.11 WiFi, ATM)



CRC example

want:

$D \cdot 2^r$ XOR R = nG

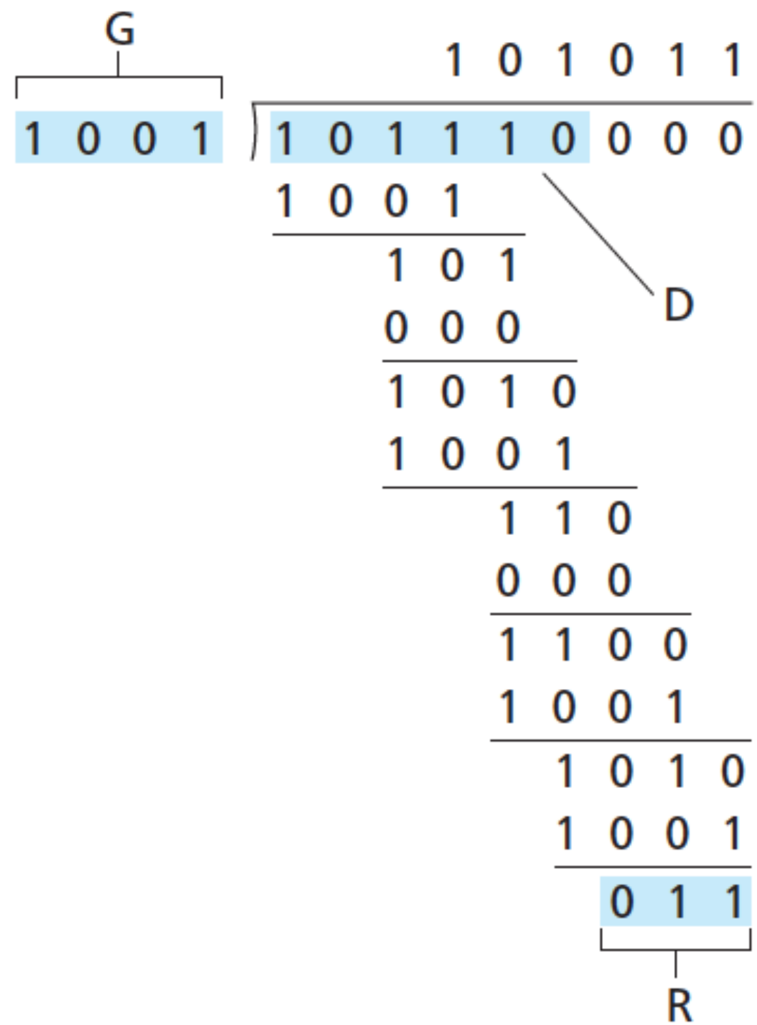
equivalently:

$D \cdot 2^r$ = nG XOR R

equivalently:

if we divide $D \cdot 2^r$ by G, want remainder R to satisfy:

$$R = remainder\left[\frac{D \cdot 2^r}{G}\right]$$



* Check out the online interactive exercises for more examples: http://gaia.cs.umass.edu/kurose_ross/interactive/

Summary

- Error detection
- Error correction