U.PORTO
FEUP FACULDADE DE ENGENHARIA
UNIVERSIDADE DO PORTO

Arquitecturas da Computação Industrial

Industrial Computing Architectures

2020/2021 – 1st Semester

3rd lab assignment

Ethernet & Wireless LANs and IP protocol

Pedro Santos

(based on slides by Paulo Portugal and Luís Almeida)

Learning objectives

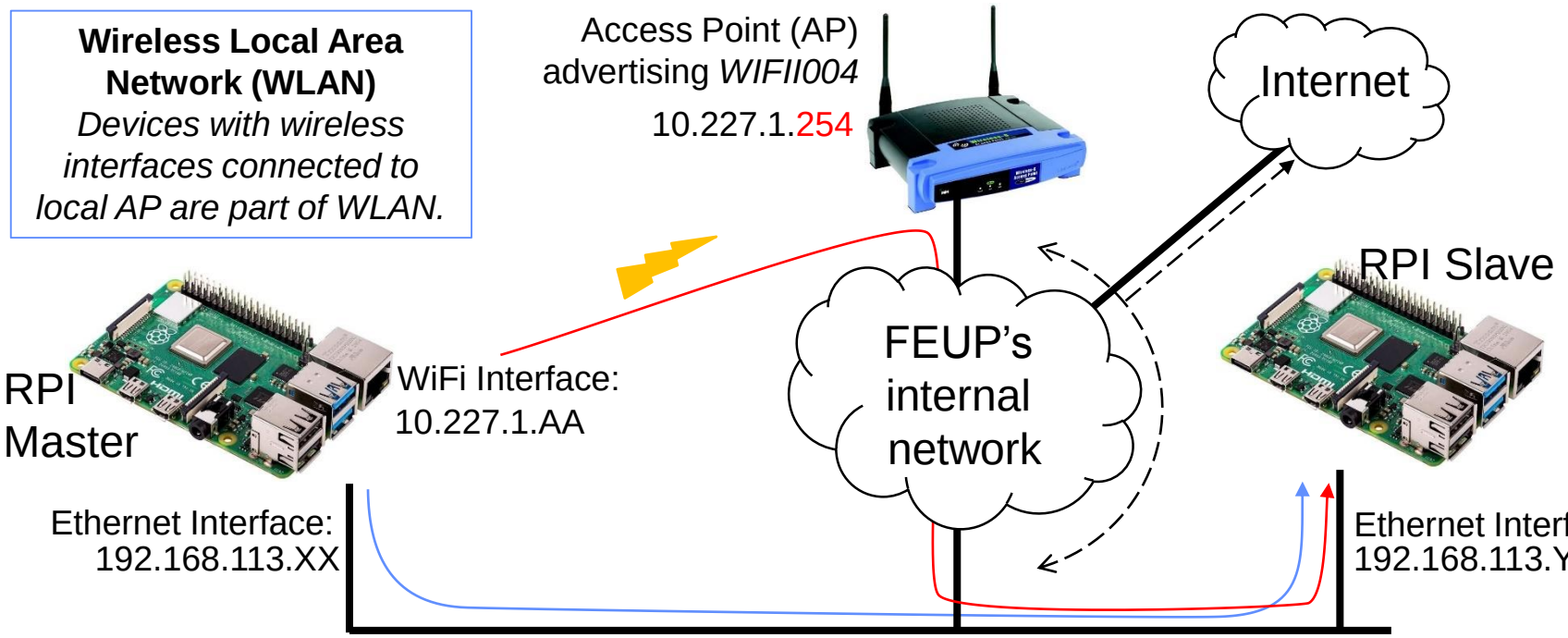
- Understand the operation of Ethernet/Wi-Fi networks and IP protocol in practice and their configuration.
- To do and learn:
  - observe network traffic in Ethernet & Wi-Fi networks,
  - understand routing in Local Area Networks (LAN) and to other networks,
  - observe differences in temporal response of traffic exchanged over different media (Ethernet or Wi-Fi) and to networks outside LAN,
  - learn the structure of Ethernet packets,
  - understand forwarding in Ethernet Local Area Networks (LAN),
  - carry out MAC address resolution,
  - understand IP addresses assignment via DHCP.
- Acquire the capacity to use Ethernet & Wi-Fi networks and IP protocols.

1st Part of Assignment: WLAN vs. Ethernet

- Set up Modbus connection between Modbus Master (RPI Master) and Modbus Slave (RPI Slave)
- Connect RPI Master to WLAN (*WIFII004*) and to LAN (Ethernet); compare TRR times
- Through Ethernet, both devices are in the same network (lab's subnet)
- Through Wi-Fi, traffic from AP is routed to the lab's wired LAN

TCP= freewheeling
TCR=5,20,40,60ms

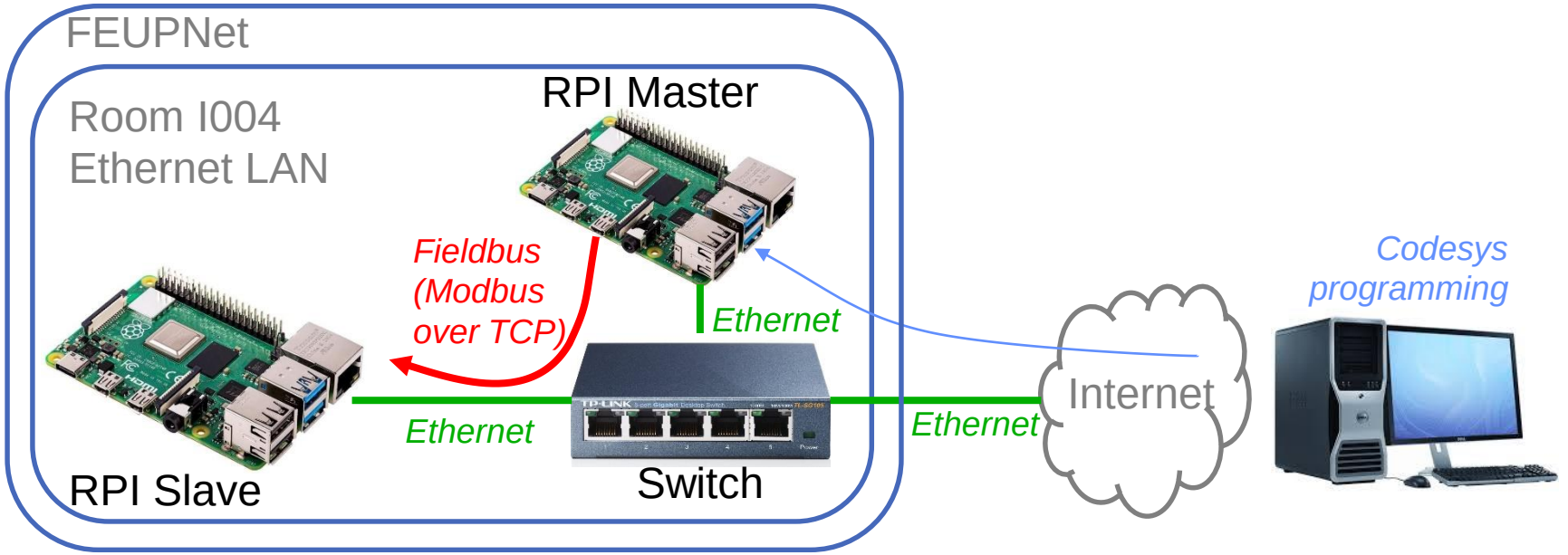
Wireless Local Area Network (WLAN)
Devices with wireless interfaces connected to local AP are part of WLAN.



(Ethernet) Local Area Network (LAN)
Lab's devices connected through Ethernet and with similar subnet (192.168.113.x).

2nd Part of Assignment: Ethernet & IP Protocols

- Set up Modbus connection between Modbus Master (RPI Master) and Modbus Slave (RPI Slave)
- Inspect Ethernet & IP headers
- Inspect switches' MAC forwarding tables and understand MAC to physical port associations
- Understand operation of the Address Resolution Protocol (ARP)
- Observe IP assignment via Dynamic Host Configuration Protocol (DHCP)



U.PORTO
FEUP FACULDADE DE ENGENHARIA
UNIVERSIDADE DO PORTO

Arquitecturas da Computação Industrial

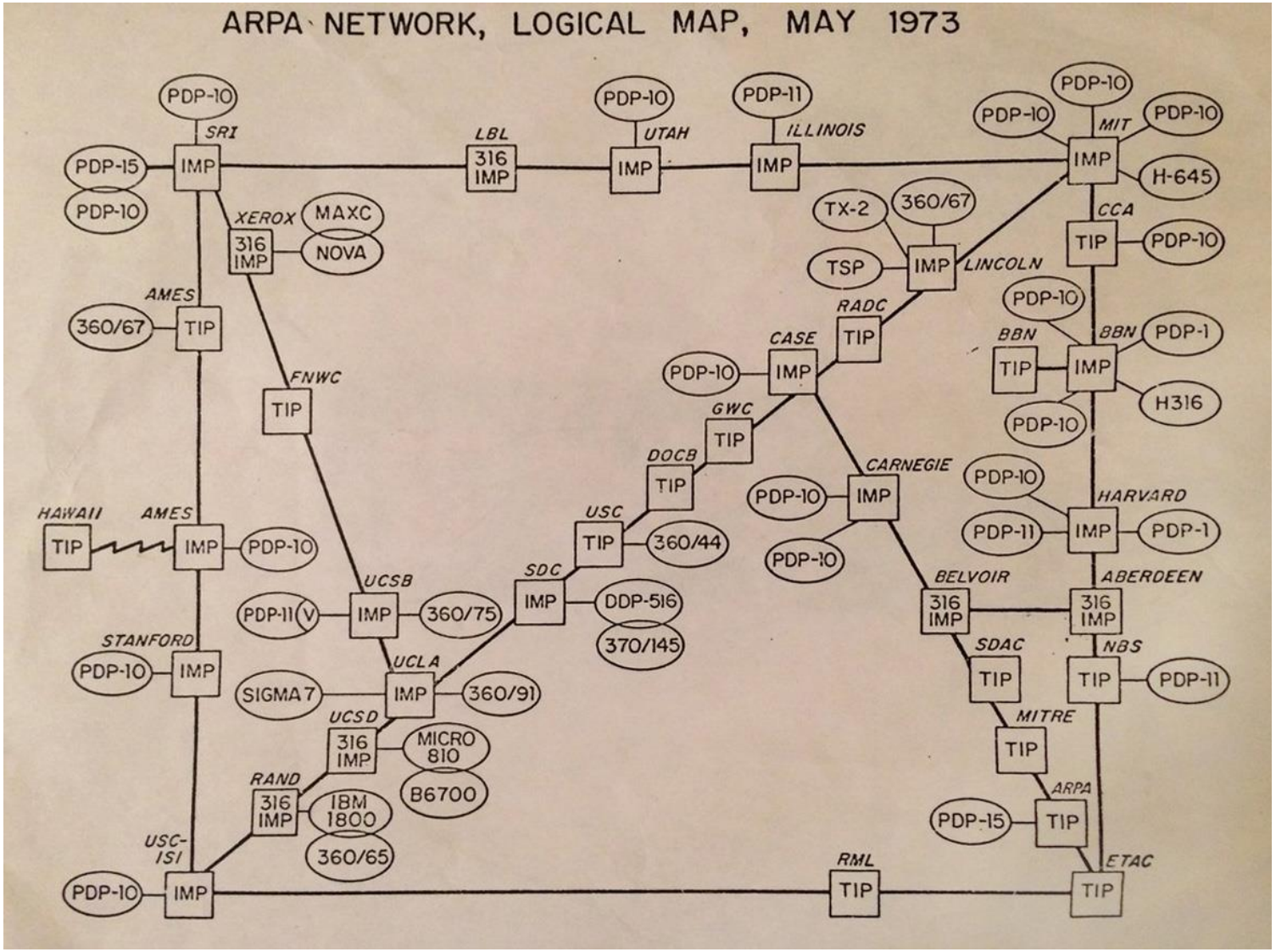
Industrial Computing Architectures

2020/2021 – 1st Semester

Ethernet and TCP/IP protocols

Background

An historical perspective…

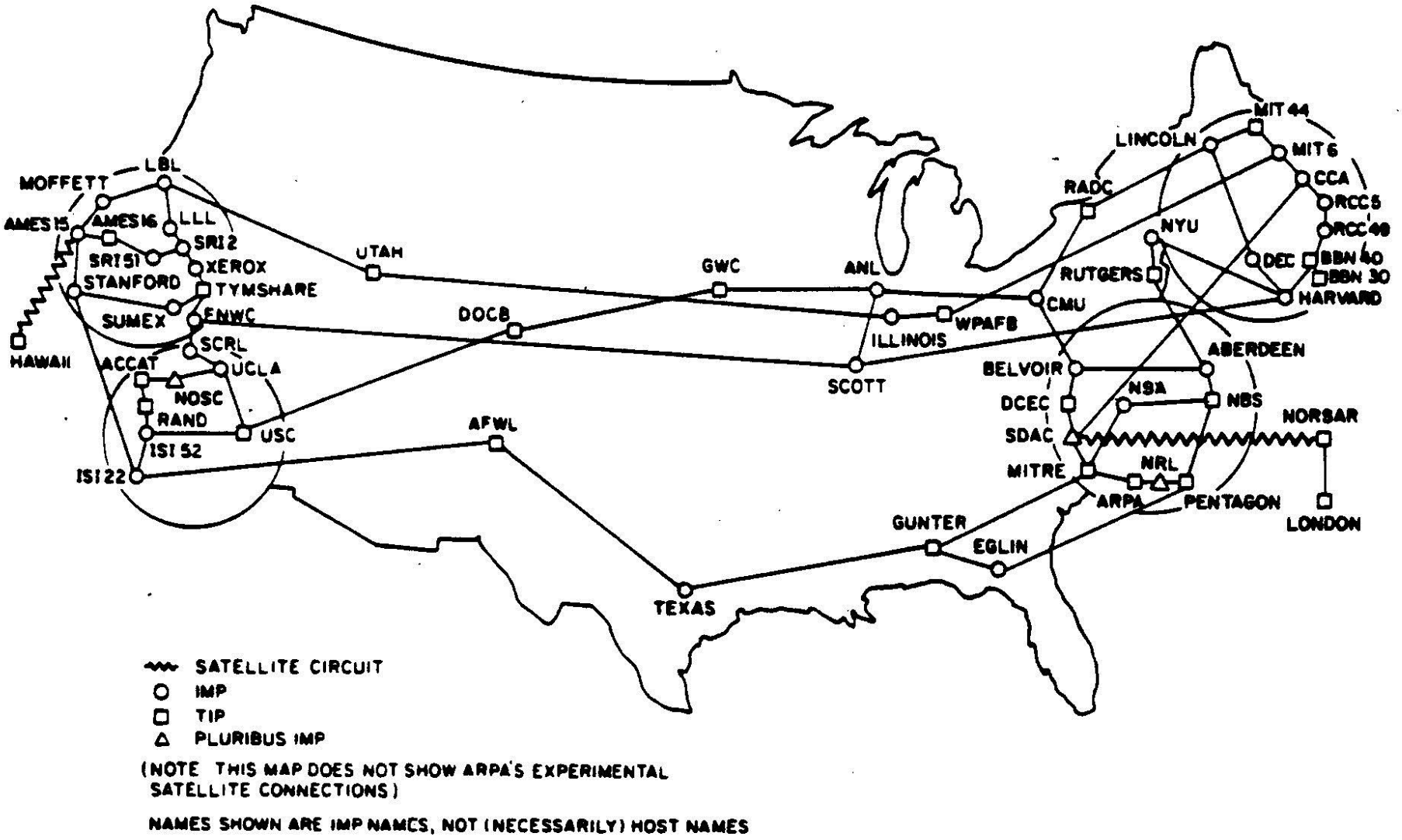


Public Domain

An historical perspective…

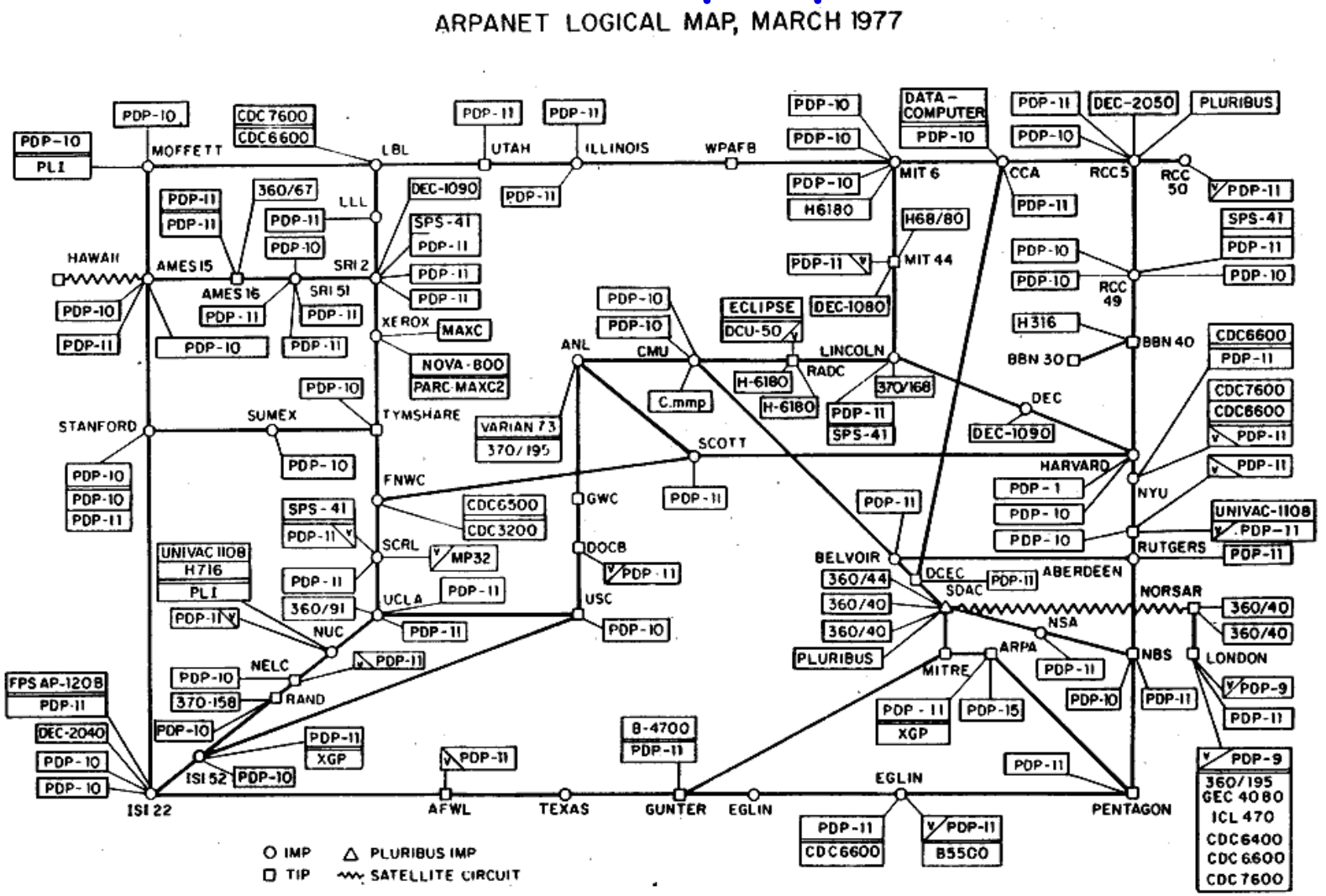
By Retro-Computing Society of Rhode Island - Own work, CC BY-SA 3.0.

An historical perspective…



Public Domain

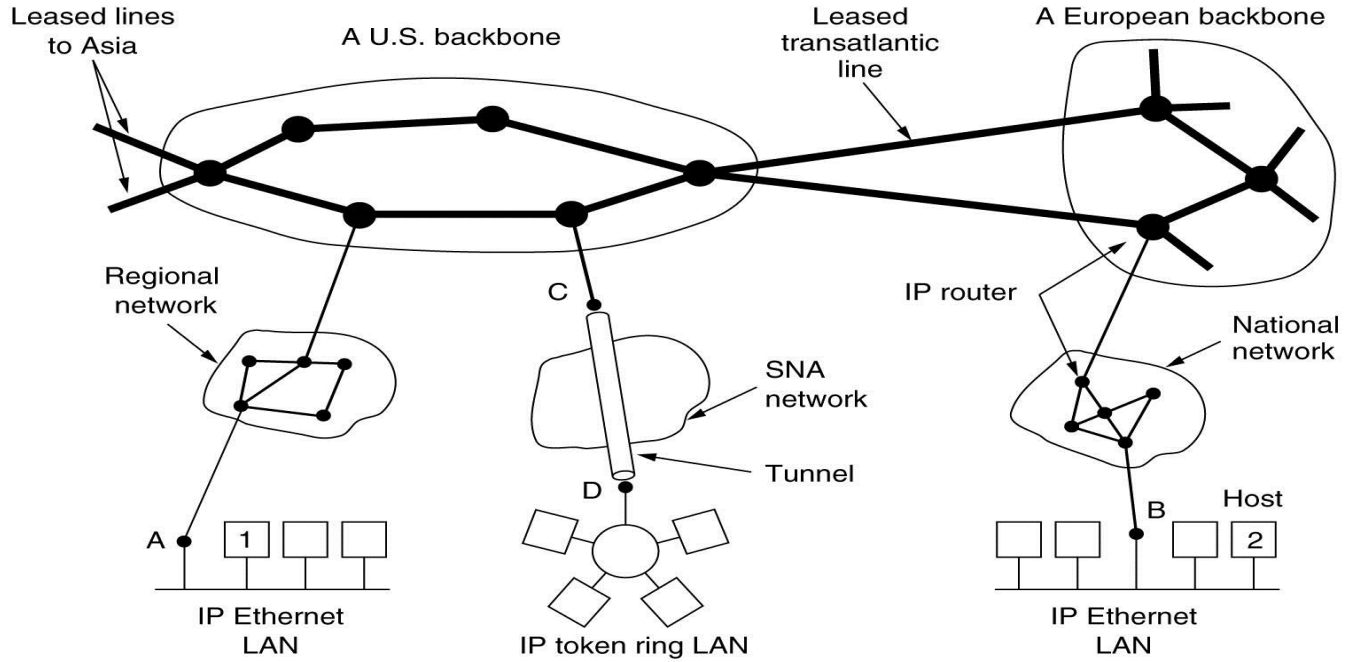
An historical perspective…



Public Domain

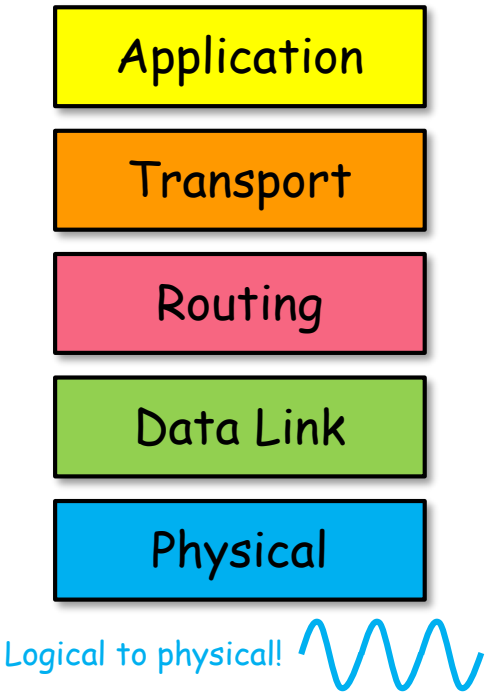
The Internet Now

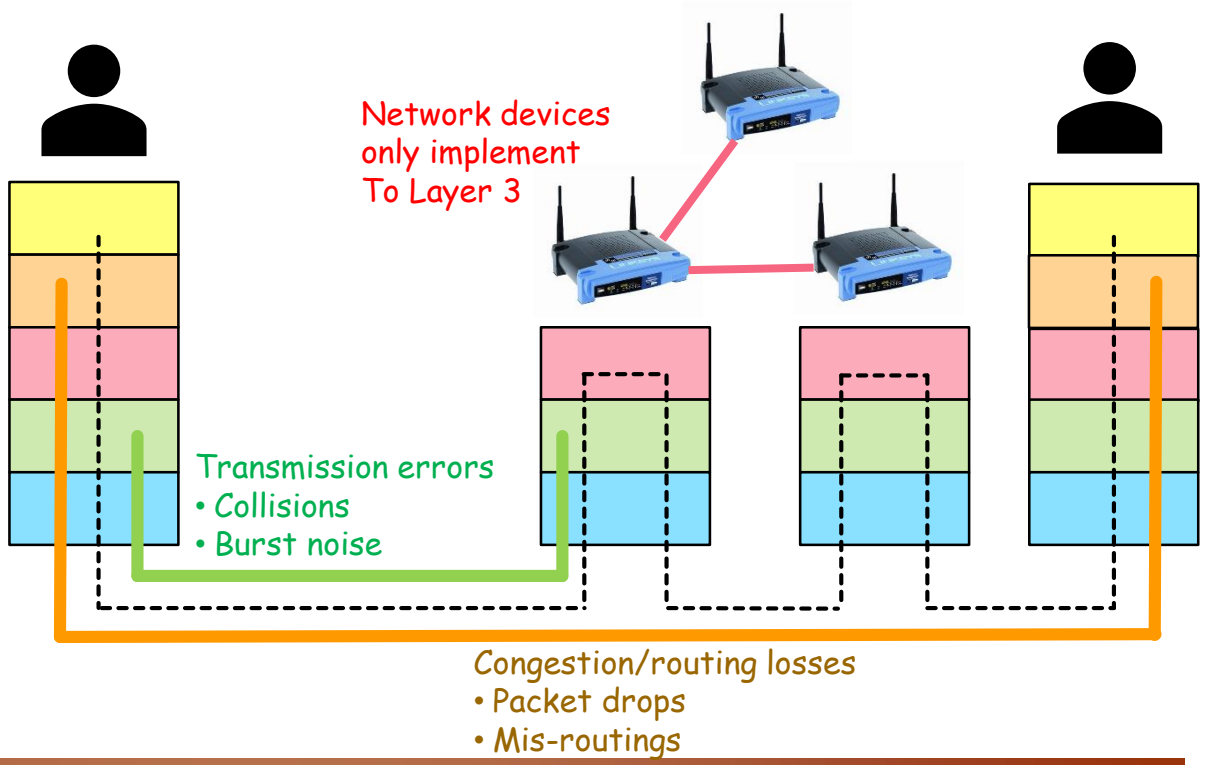
- A collection of networks, all interconnected and the backbone networks behind!
  1. Your home network connects to your ISP (Internet Service Provider)
  2. Your ISP connects to the national network, that links other ISPs, companies, government institutions, etc.
  3. The local network connects to continental and transcontinental backbones, so that you can access a computer in China



The TCP/IP Stack

- The TCP/IP stack was built ad hoc – ***people proposed solutions and incorporated them***
- The two main problems to be solved gave the name to the stack
  - How do I route my packets from A to B? → **Internet Protocol (IP)**
  - How do I guarantee all my packets arrive to B? → **Transport Control Protocol (TCP)**

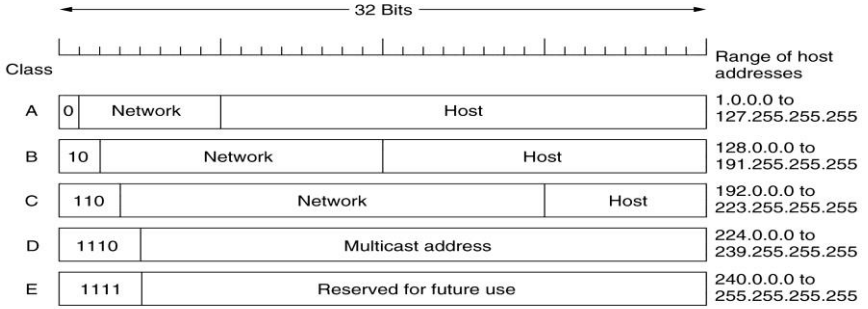




A few words about Internet Protocol - IP

- The Internet Protocol <u>does not mandate any routing protocol!</u> It sets:
  - Common format for addressing (IP addresses)
  - Management/control messages

- IPv4 addresses use 32 bits. Structure:
  - **Classes:** network category. Somewhat outdated.
  - **Network:** number of bits is inversely proportional to number of devices on network.
    - » **'Many small networks', 'Few large networks'**

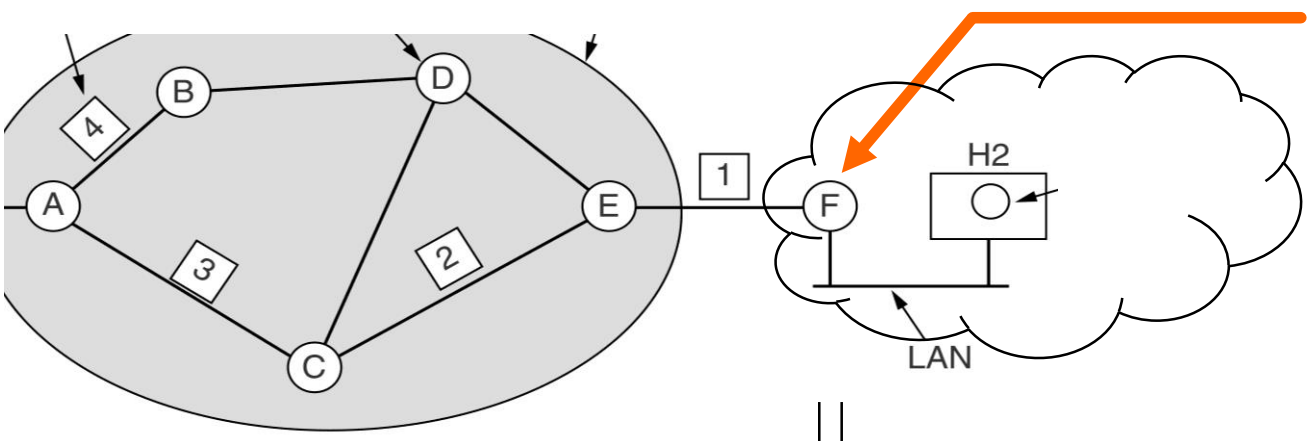


  - Due to this initial assignment, most small LANs (e.g., your home network) have IP of class C (e.g. **192.168.0.xxx)**, but you are free to change it!

- What about IPv6?
  - IPv4 provides 2^32 addresses = 4,294,967,296 *[vide world population: **7,700,000,000**]*
  - So, not enough IP addresses for every person/device/machine → **IPv6 uses 128 bits!**

Default Gateway

- **Local communications**
  - Destination address AND network mask = Source address AND network mask
  - Ex: 192.168.113.28 && 255.255.255.0 = 192.168.113.50 && 255.255.255.0
- **External communications**
  - Destination address AND network mask ≠ Source address AND network mask
    - » **Destination is in a different network ➔ send packet to *Default Gateway***



Gateway:
router that connects a network to the Internet

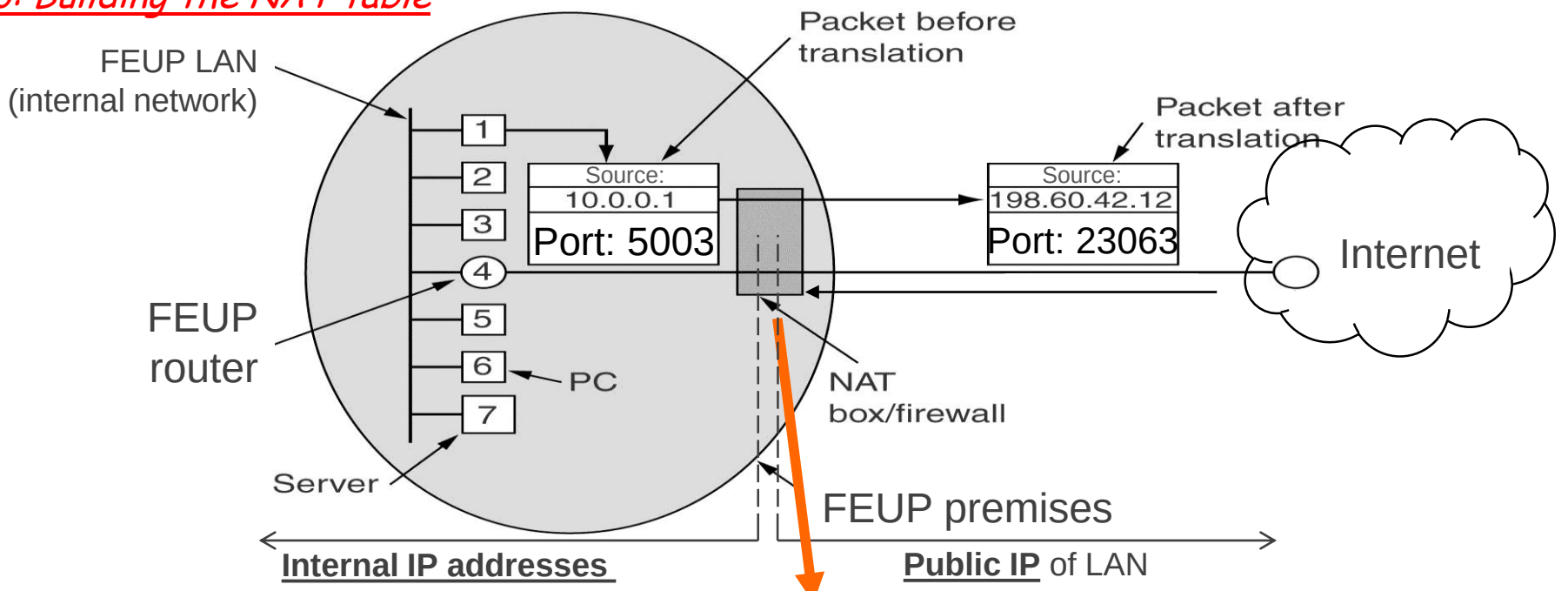
Public IP of LAN

Internal IP addresses
(separate from rest of Internet)

NAT - Network Address Translation

- With a **gateway**, all computers in an internal network have, to the Internet, the same IP.
- Then, how to know who are inbound packets destined to? → **NAT**
- NAT relies on internal machines initiating connection to the outside, to learn their IP and ports
- Also, very hard for outside/Internet nodes to access internal machines → **SECURITY!!!**

1. Setup: Building the NAT table



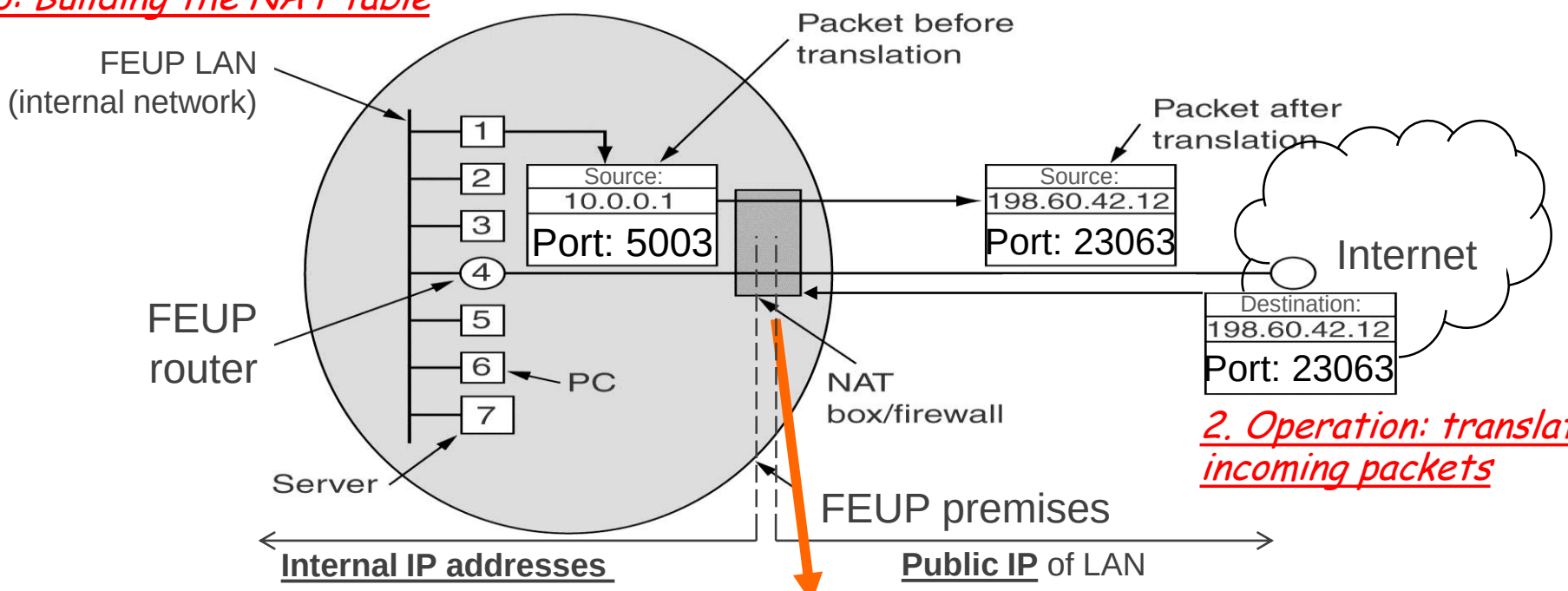
NAT Translation table

Internal Src IP	Internal Src Port	↔	Public IP	Public Port
10.0.0.1	5003	↔	198.60.42.12 (**FEUP's public IP**)	23063

NAT - Network Address Translation

- With a **gateway**, all computers in an internal network have, to the Internet, the same IP.
- Then, how to know who are inbound packets destined to? → **NAT**
- NAT relies on internal machines initiating connection to the outside, to learn their IP and ports
- Also, very hard for outside/Internet nodes to access internal machines → **SECURITY!!!**

1. Setup: Building the NAT table



2. Operation: translating incoming packets

NAT Translation table

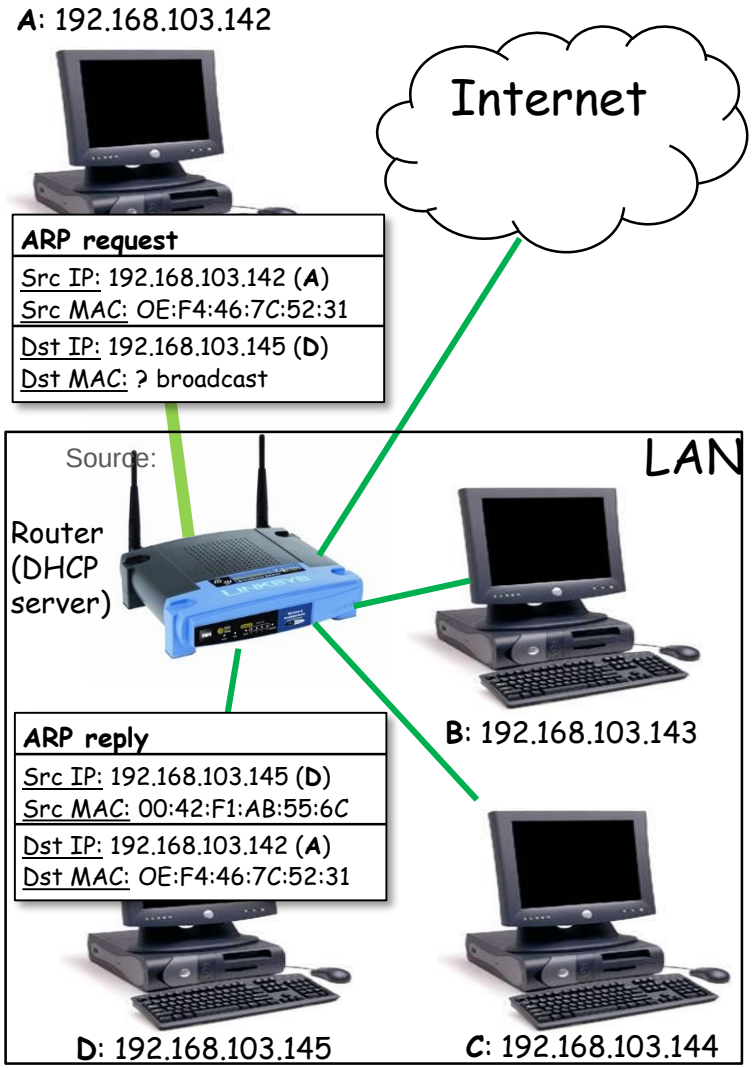
Internal Src IP	Internal Src Port	↔	Public IP	Public Port
10.0.0.1	5003	↔	198.60.42.12 (**FEUP's public IP**)	23063

ARP – Learning Layer 2 Addresses in the LAN

- Motivation
  1. Great! Your machine now has a local IP address!
  2. Now you want to start talking to someone in this LAN. And you know its IP address.
  3. But! Because I'm in the same LAN/sharing the same medium *, I actually need the **Layer 2 address - the MAC address!**
  4. Because I just arrived, I don't know any L3 addresses! **Gotta ask!**

- **ARP - Address Resolution Protocol**
  1. **Machine A**, wishing to talk to **machine D**, sends an ARP packet addressed to 192.168.103.145 but using a MAC broadcast
  2. **Machine D** replies back with its MAC address, in a packet addressed to A

* Note:
- If destination machine is outside the local network (LAN), you're not sharing the same medium.
- The packet has to be routed to the local gateway for forwarding.
- Address resolution must be made at EVERY network the packet goes through, until reaching the destination.



DHCP – Getting a Layer 3 Address

- **DHCP – Dynamic Host Configuration Protocol**
  - Layer 3 addresses (IP addresses) are not unique per machine (unlike Layer 2 addresses, MACs)
  - When a machine arrives to LAN, it needs an IP address to communicate with LAN and Internet machines
  - The DHCP server (typically hosted by the router)
    - » **provides this address**
    - » **controls the pool of available and assigned addresses**
- Example:
  1. Suppose a machine A arrives to a local network (e.g., your laptop connecting to Eduroam)
  2. Machine A sends an IP and MAC **broadcast** packet requesting assignment of an IP address by DHCP server
  3. DHCP server replies with IP address and lease time (for how long the address is valid)