

Computer Networks - *Xarxes de Computadors*

Outline

- Course Syllabus
- Unit 1: Introduction
- Unit 2. IP Networks
- **Unit 3. LANs**
- Unit 4. TCP
- Unit 5. Network applications

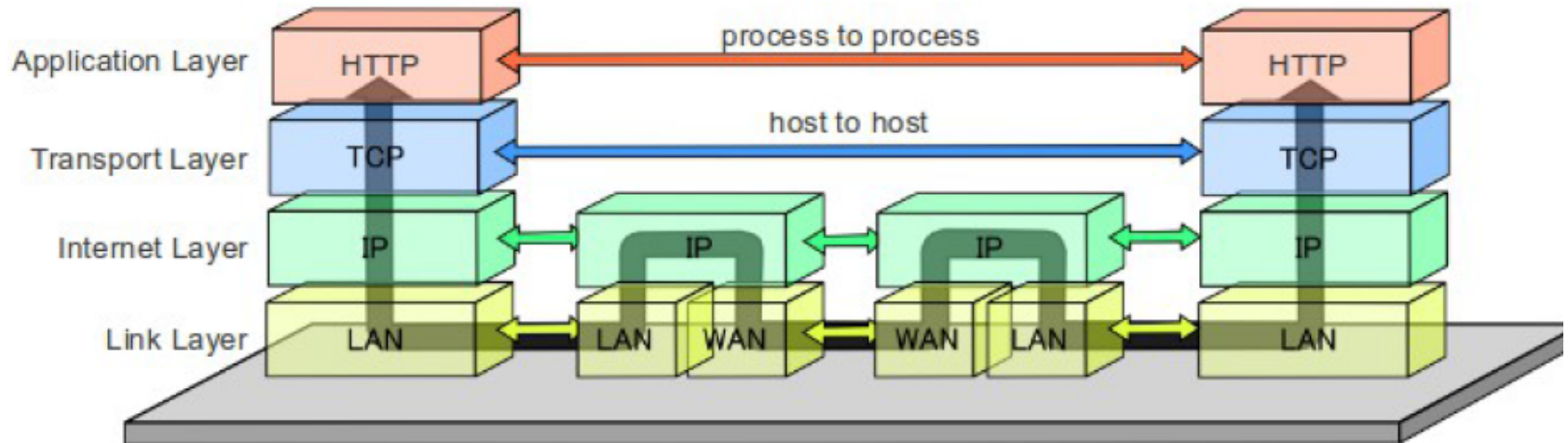
These slides are based on the set of slides provided by Llorenç Cerdà for this course. They include some modifications and some new slides.

Local Area Networks, LANs

Outline

- **Introduction**
- IEEE LAN Architecture
- Ethernet
- Ethernet Switches
- Wireless LANs

Data Flow of the Internet Protocol Suite



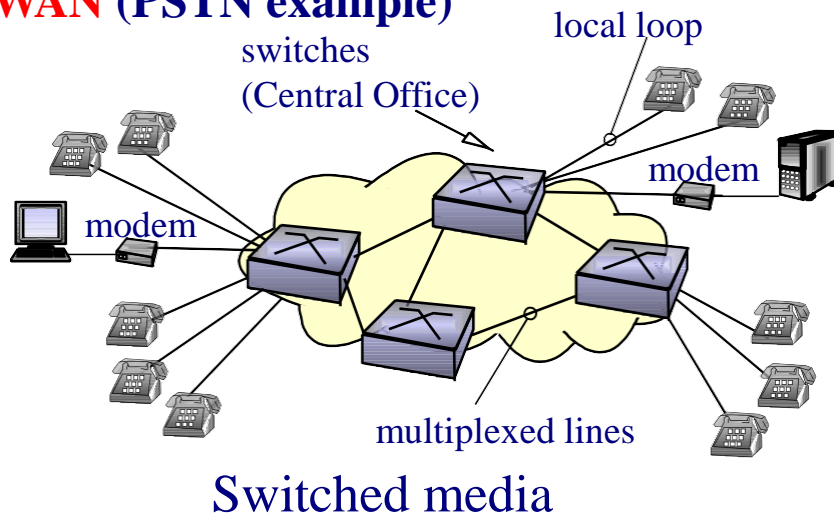
Outgoing E-mail Frame

Destination MAC Address	Source MAC Address	Destination IP Address	Source IP Address	Destination TCP Port	Source TCP Port		
00:0C:78:52:F3:A5	0E:11:81:F2:C3:98	216.93.82.9	172.16.20.57	25	58631	Hi Mom	101101
MAC address of default gateway router's interface	Your NIC's MAC address	IP address of the SMTP server at your mom's ISP	IP address of your PC	Standard port number for SMTP	Randomly generated by your PC's TCP/IP stack		

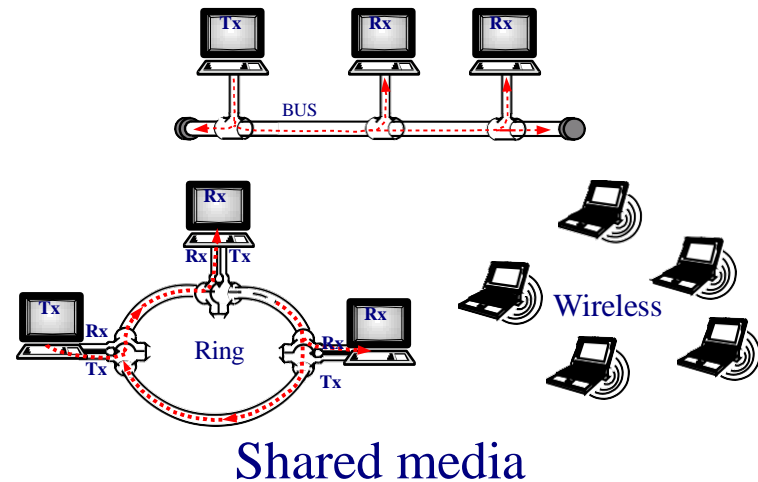
Introduction – WAN and LAN differences

- **WANs (Wide Area Network):**
 - Main goal: scalability.
 - Switched network with mesh topology.
- **LANs (Local Area Network):**
 - Multi-access network with shared media.
 - A Medium Access Control (MAC) protocol is needed.

WAN (PSTN example)



LANs

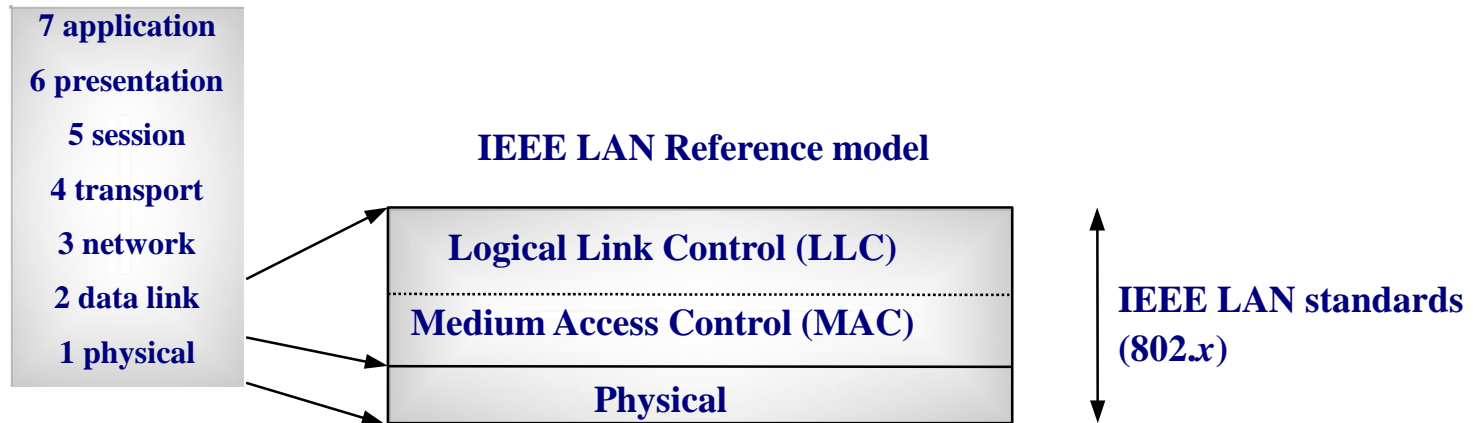


Outline

- Introduction
- **IEEE LAN Architecture**
- Ethernet
- Ethernet Switches
- Wireless LANs

IEEE LAN Architecture

OSI Reference model:



- **LLC** sublayer (802.2):
 - Common to all 802.x MAC standards.
 - Define the interface with the upper layer and specifies several services (operational modes):
 - (i) **unacknowledged connectionless**, (ii) connection oriented, (iii) acknowledged connectionless.
- **MAC** sublayer:
 - Define the medium access protocol. It is different for each LAN technology.

IEEE LAN Architecture – IEEE 802 standards (some)

802.1 LAN/MAN architecture

802.2 Logical Link Control (LLC)

802.3 Ethernet

802.4 Token Bus

802.5 Token Ring

802.6 MAN (DQDB)

802.8 FDDI

802.11 WiFi: Wireless LANs.

802.15 Personal Area Networks or short distance wireless networks (WPAN)

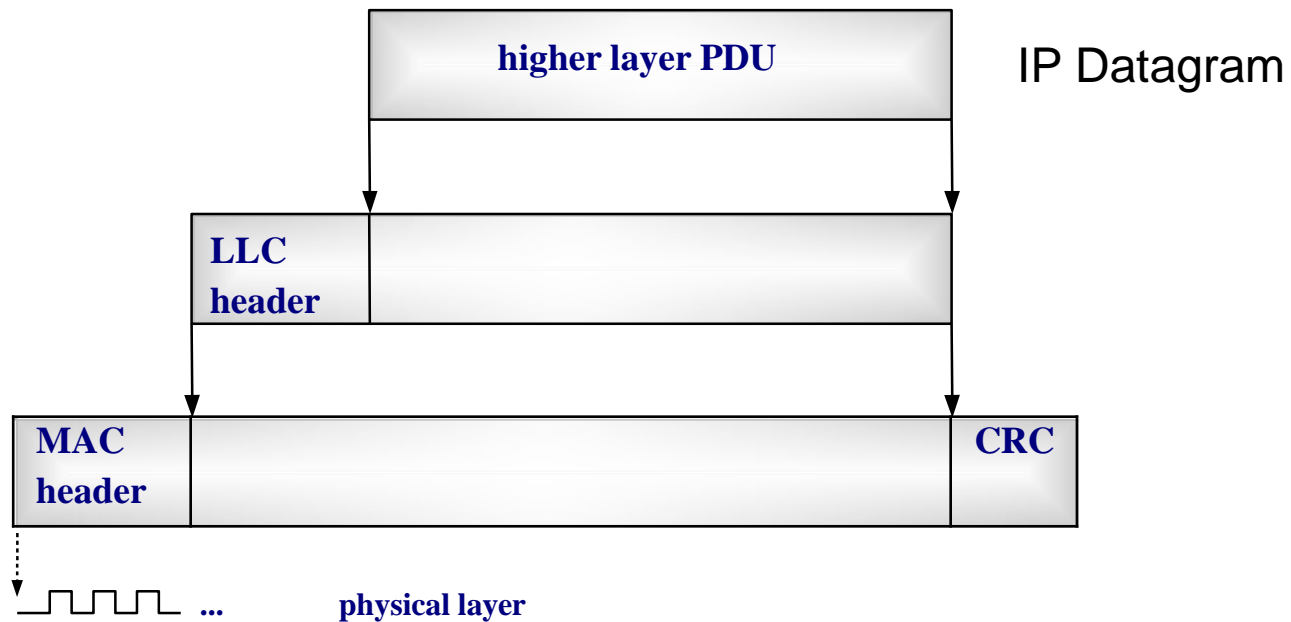
802.15.1 Bluetooth

802.15.4 Low data rate and low cost sensor devices

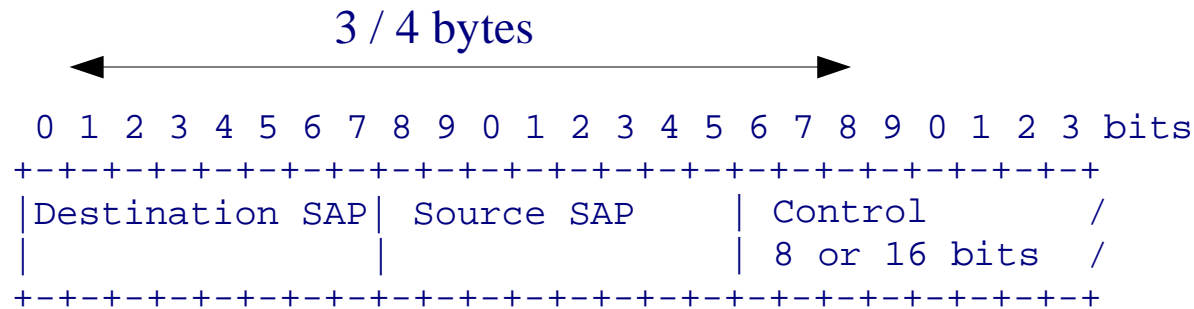
802.16 WiMAX: broadband Wireless Metropolitan Area Networks.

See: <http://grouper.ieee.org/groups/802/1, 2, ...>

IEEE LAN Architecture – LAN encapsulation



IEEE LAN Architecture – LLC header



- Service Access Point (**SAP**): Identifies the upper layer protocol.
- **Control**: Identifies the frame type. It can be 8 or 16 bits long, 8 bits for unnumbered frames (used in connectionless modes).

SAP (hex)	Protocol
06	ARPANET Internet Protocol (IP)
08	SNA
42	IEEE 802.1 Bridge Spanning Tree Protocol
98	ARPANET Address Resolution Protocol (ARP)
AA	SubNetwork Access Protocol (SNAP)
E0	Novell Netware
F0	IBM NetBIOS
FF	Global LSAP

SNAP: used in TCP/IP

Example of some IEEE SAP values.

Ethernet – Frames

- Ethernet II (DIX):

Preamble (8 bytes)	Destination MAC Address (6 bytes)	Source MAC Address (6 bytes)	Frame type (2 bytes)	Payload (46 to 1500 bytes)	CRC (4 bytes)
-----------------------	---	------------------------------------	-------------------------	----------------------------------	------------------

- IEEE 802.3

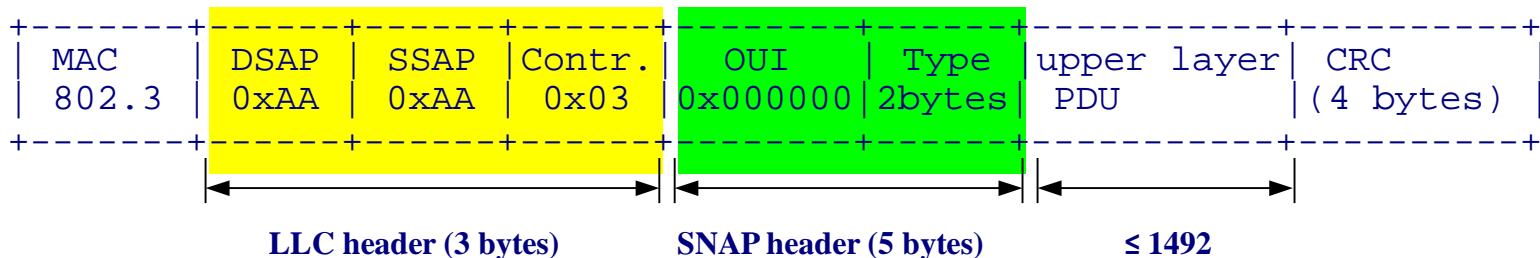
Preamble (8 bytes)	Destination MAC Address (6 bytes)	Source MAC Address (6 bytes)	Length of the frame (2 bytes)	Payload (46 to 1500 bytes)	CRC (4 bytes)
-----------------------	---	------------------------------------	-------------------------------------	----------------------------------	------------------

- Preamble:** Give time to detect, synchronize and start reception.
- Type:** Identifies the upper layer protocol (IP, ARP, etc.) (RFC 1700, Assigned numbers). This value is always > 1500 .
- Length:** Payload size (0~1500).

Ethernet – IEEE Sub-Network Access Protocol (SNAP)

- Allows the specification of protocols, and vendor-private identifiers, not supported by the 8-bit 802.2 Service Access Point (SAP) field.
- It is used to encapsulate **TCP/IP** protocols over IEEE 802.2 (LLC) with OUI=0x000000 and Type equal to the RFC 1700 (used for DIX).

802.3 SNAP Frame



- The **MSS** used by TCP would be of 1460 if DIX encapsulation is used, and 1452 if IEEE is used.

Outline

- Introduction
- IEEE LAN Architecture
- **Ethernet**
- Ethernet Switches
- Wireless LANs

Ethernet – Introduction

- Designed by **Bob Metcalfe** at Xerox in mid-70s.
- Initially was commercialized by Digital, Intel and Xerox consortium (**DIX**).
- Ethernet was standardized by IEEE (**802.3**) in 1983.
- Nowadays Ethernet is the **leading LAN technology**.
There are numerous Ethernet standards with different transmission mediums, and line bitrates.

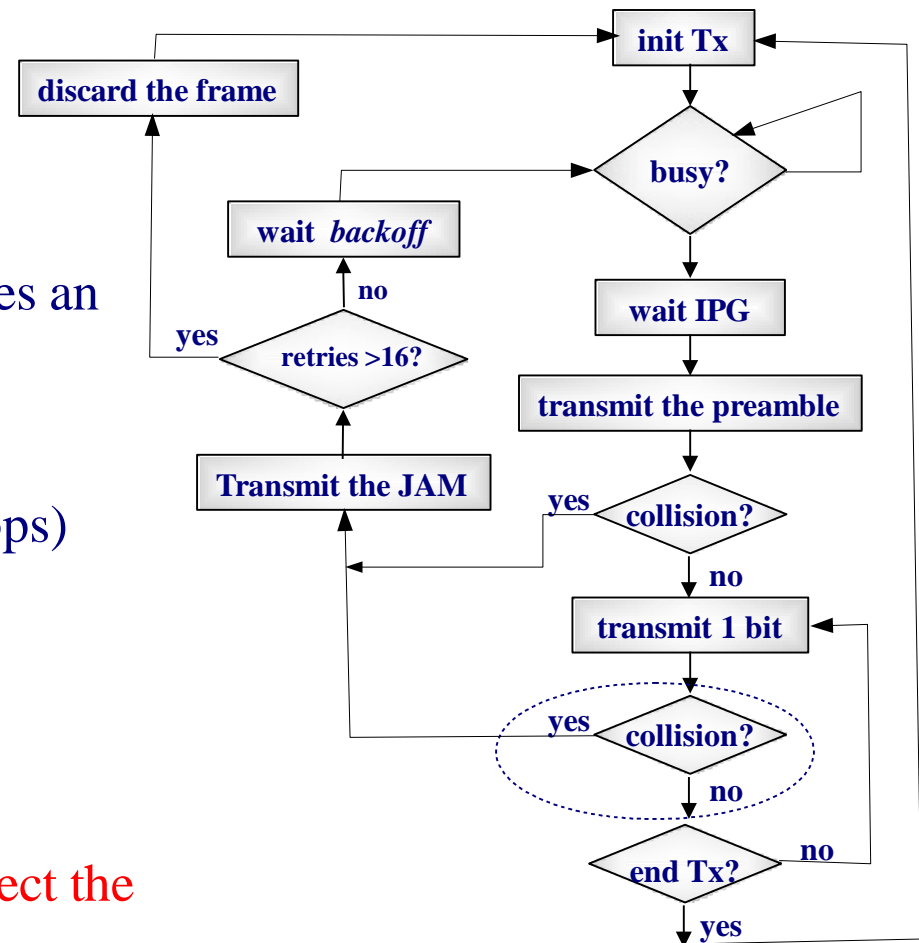
Types of MACs

- **Token Passing:**
 - Only the station having the token can transmit. After transmission the token is passed to another station.
 - Examples: FDDI and Token-Ring
- **Random:**
 - There is no token. Instead, there is a non null collision probability. In case of collision, the frame is retransmitted after a random *backoff* time.
 - Examples: **Ethernet**

Carrier Sense Multiple Access/Collision Detection (CSMA/CD)

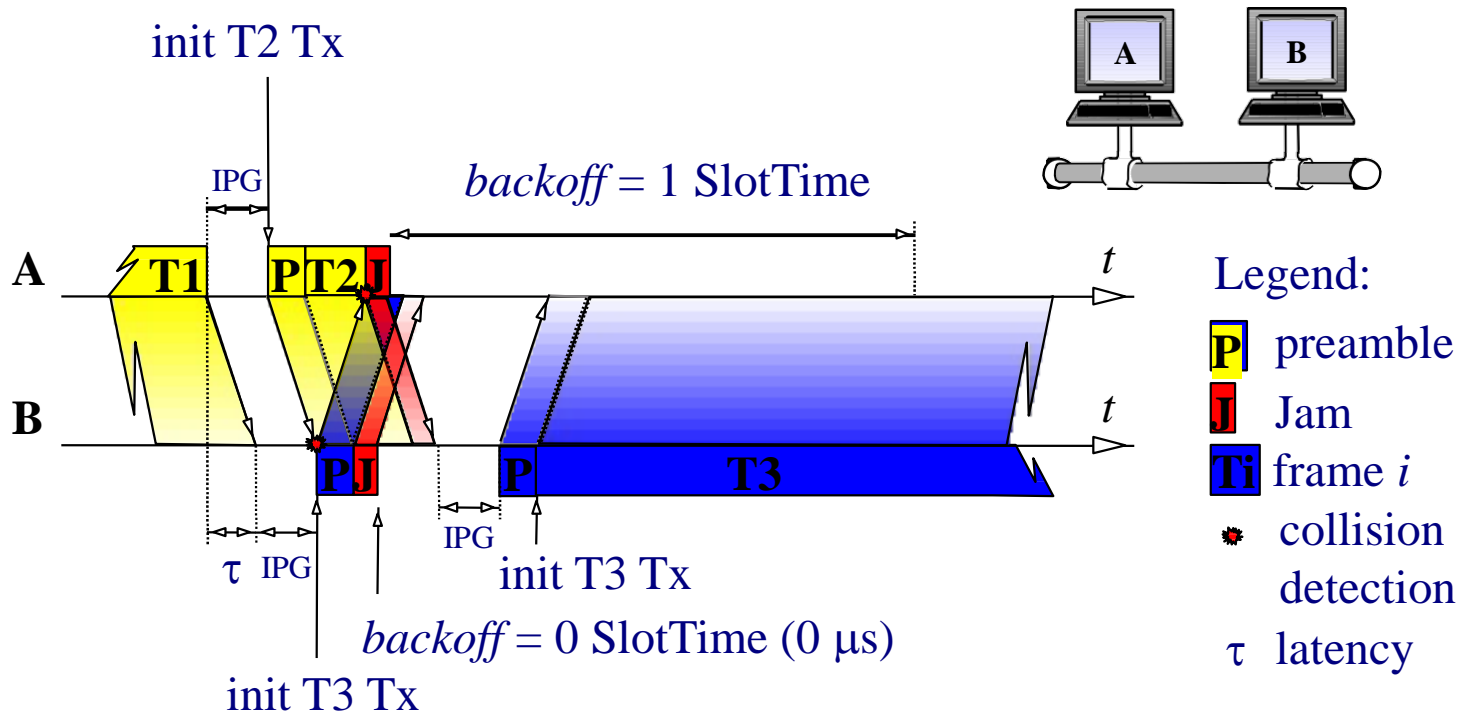
- Is a random MAC where the stations “**listen**” the medium (*carrier sense*) before transmission.
- When the medium is becomes **free** the frame is transmitted immediately, and the medium is listened to detect collisions.
- In case of **collision**, the frame is retransmitted after a **random backoff** time.

- Inter Packet Gap (**IPG**): 96 bits.
- **JAM**: 32 bits pattern that produces an erroneous CRC.
- $\text{backoff} = n T_{512}$
- T_{512} : **Slot Time** (51,2 μs at 10 Mbps)
- $n = \text{random}\{0, 2^{\min\{N, 10\}} - 1\}$,
 - N : maximum number of retransmission of the same frame (1, 2...)
- The transmitting station must detect the **collision** (no ack is sent).



Ethernet – Collision example

- Stations A y B have frames ready to Tx:



NOTE: The preamble is not interrupted in case of collision, and the JAM is Tx immediately after.

xBasey



Line **bitrate**:

- 10: 10 Mbps
- 100: 100 Mbps
- 1000: 1000 Mbps (1 Gbps)
- 10G: 10 Gbps

Base band signal.

Broad: translated band signal.

Various meanings:

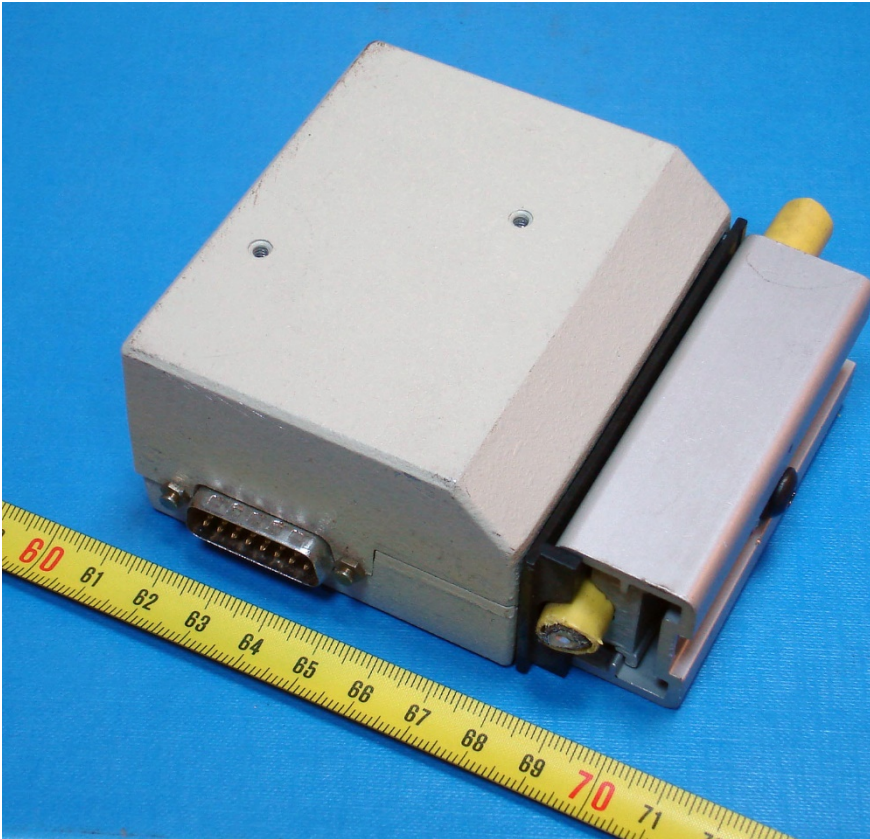
- Number: Maximum segment distant in hundreds of m.
- Reference to the medium type:
 - T: UTP
 - F: Optical Fiber
 - Other:
 - T4: Uses 4 UTP pairs.
 - TX: Full Duplex

...

Ethernet – Different Ethernet Standards (some)

Commercial name	bps	Standard	year	Name	Cabling	UTP/OF Pairs	Connector	Codification	segment distance*	
									Half duplex	Full duplex
Ethernet	10Mbps	802.3	1983	10Base5	Coax-thick	-	AUI	Manchester	500m	n/a
		802.3a	1985	10Base2	Coax-thin	-	BNC	Manchester	185m	n/a
		802.3i	1990	10BaseT	UTP-cat.3	2	RJ45	Manchester	100m	100m
		802.3j	1993	10BASE-FL	FO	2	SC	on/off Manchester	2000m	>2000m
Fast Ethernet	100Mbps	802.3u	1995	100BaseTX	UTP-cat.5	2	RJ45	4B/5B	100m	100m
		802.3u	1995	100BaseFX	FO	2	SC	4B/5B	412m	2000m
		TIA/EIA-785	1999	100BaseSX	FO/led	2	SC	4B/5B	300m	300m
Gigabit-Eth.	1Gbps	802.3z	1998	1000BaseSX	FO	2	SC	8B/10B	275-316m	275-550m
		802.3z	1998	1000BaseLX	FO	2	SC	8B/10B	316m	550-10000m
		802.3z	1998	1000BaseLH	FO	2	SC	8B/10B	n/a	100km
		802.3ab	1999	1000BaseT	UTP-cat. 5e	4	RJ45	PAM5	100m	100m
10Gigabit-Eth.	10Gbps	802.3ae	2002	10GBASE-CX4	InfiniBand	4	CX4	8B/10B	n/a	15m
		802.3ae	2002	10GBASE-SR	FO	2	SC	64B/66B	n/a	26-300m
		802.3ae	2002	10GBASE-LR	FO	2	SC	64B/66B	n/a	10km
		802.3ae	2002	...	FO	2	SC	...	n/a	...

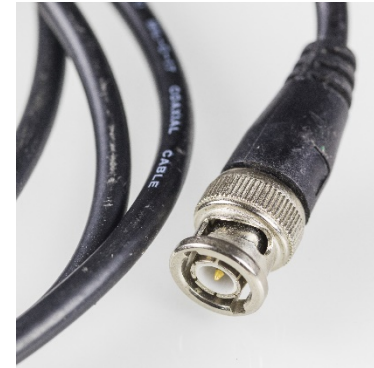
*With OF the distance depends on the OF type.



10Base5 connector (thick coaxial)

AUI connector

CC BY-SA 2.5,
<https://commons.wikimedia.org/w/index.php?curid=426337>



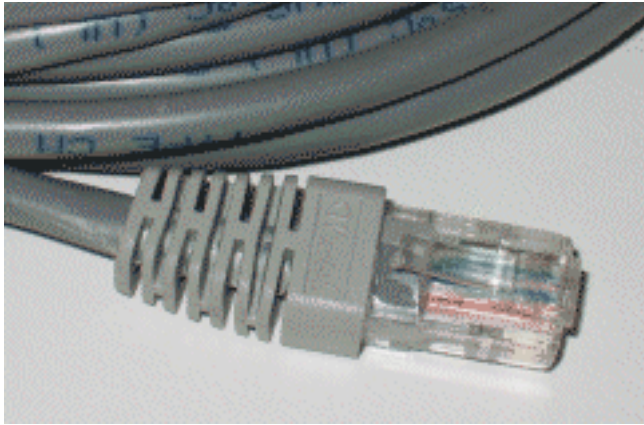
By © Raimond Spekking / CC BY-SA 4.0 (via Wikimedia Commons),
 CC BY-SA 4.0, <https://commons.wikimedia.org/w/index.php?curid=69527040>



By © Raimond Spekking / CC BY-SA 4.0 (via Wikimedia Commons),
 CC BY-SA 4.0, <https://commons.wikimedia.org/w/index.php?curid=69527036>

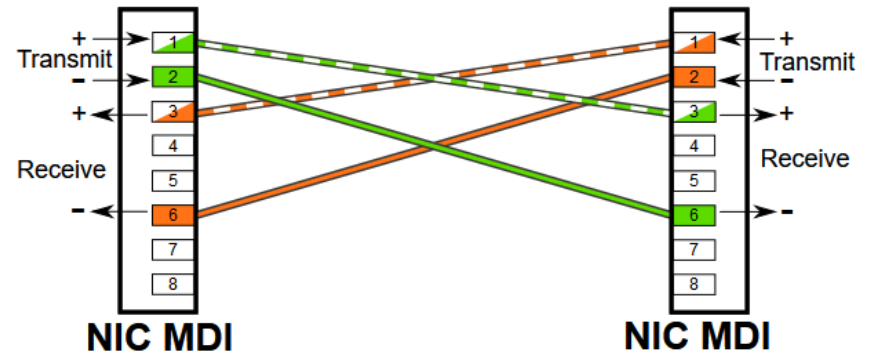
10Base2 (thin coaxial)

BNC connector



RJ45 connector

By Dflock at English Wikipedia
 Later versions were uploaded by Zcrayfish at en.wikipedia. –
 Transferred from en.wikipedia to Commons. Public Domain,
<https://commons.wikimedia.org/w/index.php?curid=1752537>



Crossover cable

By W Nowicki - Own work, CC BY-SA 3.0,
<https://commons.wikimedia.org/w/index.php?curid=15551059>

Ethernet – Different Ethernet Standards: after 10BaseT

All standards use UTP or OF (except 10GBaseCX4):

- **Fast** Ethernet (1995). 100BaseTX: UTP-cat 5
- **Gigabit** Ethernet (1998). 1000BaseT: UTP-cat 5e
- **10Gigabit** Ethernet (2002). Uses optical fiber. The only copper standard is Infiniband with segment size $\leq 15\text{m}$.



NIC 10/100 – RJ45
10BaseT-100BaseTX
\$11.99



NIC 10/100/1000 - SC
10BaseFL-100BaseFX-
1000Base-SX
\$151



NIC 10Gbps – CX4
10GBaseCX4
\$795



Infiniband cable with
CX4 connectors

Outline

- Introduction
- IEEE LAN Architecture
- Ethernet
- **Ethernet Switches**
- Wireless LANs

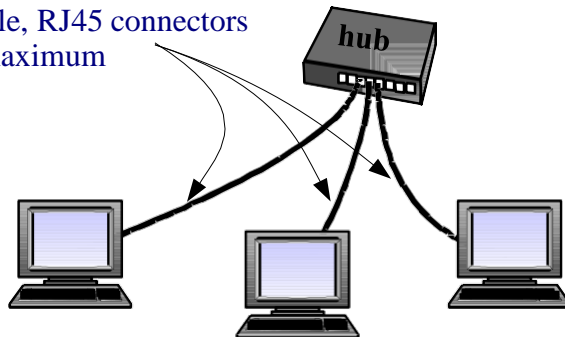
Ethernet – Different Ethernet Standards: 10BaseT

1990. Cable UTP-cat 3.

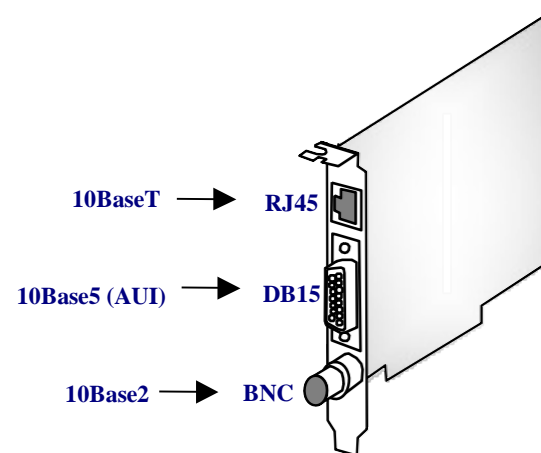
- **Hub**: Is a multi-port repeater (layer 1).
- The signal received in 1 port is retransmitted by all the others.

10BaseT segments

UTP cable, RJ45 connectors
100 m maximum



Transceivers
AUI-BNC/AUI-RJ45

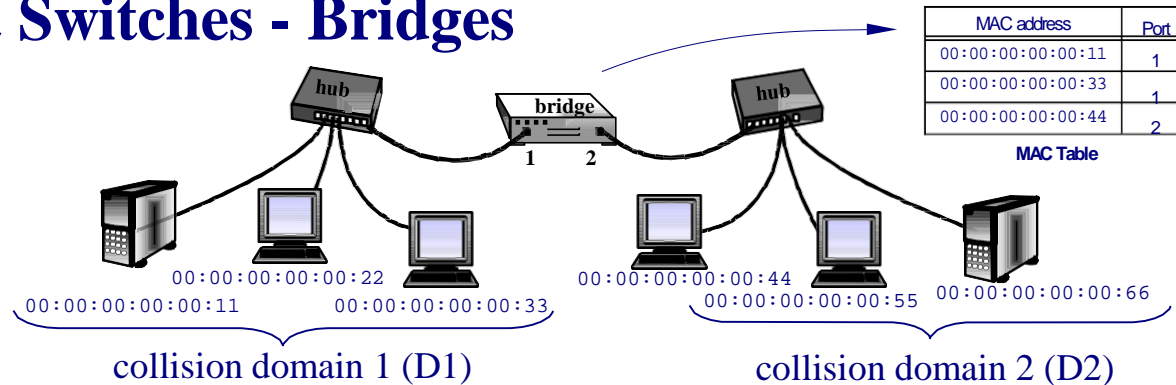


NIC “combo”:
Supports 10Base5, 10Base2, 10BaseT

Ethernet Switches - Introduction

- Hub problem: If many stations are connected, may be inefficient due to **collisions**.
- Solution: bridges and switches.
- **Ethernet bridge**:
 - “plug and play” layer 2 device. Retransmits Ethernet frames
 - In each port there is a **NIC** in “promiscuous” mode: Capturing all frames.
 - The source address is used to “**learn**” which MAC is present in each port (MAC table). Each entry has the MAC and the port numbers.
 - The destination MAC is used to decide whether the frame needs to be retransmitted by another port.
 - Isolates the “**collision domain**”.

Ethernet Switches - Bridges



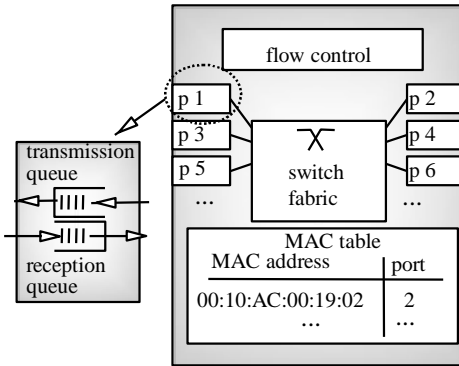
How the bridge works:

- If a frame is received with a **source address not in the MAC table**, it is added (*learning bridge*).
- If a frame from D1 is received with a **destination address that**: (i) is in D2, (ii) it is not in the table, (iii) it is broadcast: It is **sent into D2** (*flooding*).
- If it is received a frame from **D1 addressed to another station from D1**, it is **discarded** (*filtering*).
- The entries have an **aging timer**. Each time an entry is used, it is refreshed. If the aging timer expires, the entry is removed.

Advantages:

- **Segments the collision domain** (less collisions).
- Clients in **D1 and D2 can simultaneously send frames** to their servers.

Ethernet Switches - Switch Architecture



```
Switch#show mac-address-table
Address          Dest Interface
-----
00D0.5868.F583   FastEthernet 2
00E0.1E74.6ADA   FastEthernet 1
00E0.1E74.6AC0   FastEthernet 1
0060.47D5.2770   FastEthernet 3
00D0.5868.F580   FastEthernet 5
```

MAC Table in a CISCO Switch

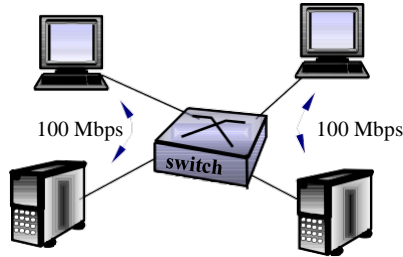


Edge and backbone CISCO switches.

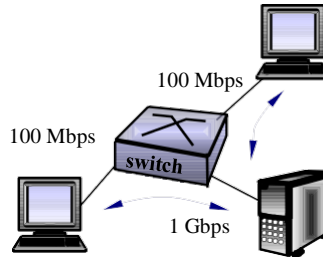
How the switch works:

- It is equivalent to a “**multiport bridge**”.
- When a frame is received with a **source address** not in the table, it is added.
- If a frame is received with a **destination address**: (i) not in the table, (ii) broadcast or multicast: copy the frame in all transmission buffer of the other ports (**flooding**).
- If a frame is received with the address from another port: It is **switched** as fast as possible the the transmission buffer of that port.
- If receives a frame addressed to another station from the same port, it is discarded (**filtering**).

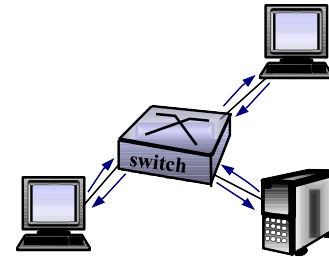
Ethernet Switches - Switch Capabilities



Simultaneous Transmissions



Ports with Different bitrates



Full Duplex Ports

- Each port is different a **collision domain** (less collisions).
- Different ports can be simultaneously **Tx/Rx**.
- Ports can have different **bitrates**.
- Ports may be **full-duplex** (if only one host is connected).
- There can be ports in **half or full** duplex mode simultaneously.
- **Link aggregation**: Bitrate can be increased by aggregating several links, which behave as a single one (*etherchannel* in CISCO).
- **Security**: Stations can only capture the traffic of their collision domain.

Ethernet – Half Duplex and full-duplex

- **Half Duplex**: Using CSMA/CD only one NIC can be simultaneously transmitting into the medium.
- **Full Duplex**: When 2 Ethernet NICs are connected point-to-point, some Ethernet standards allow a full-duplex Tx, .
- Ethernet NICs have an **auto-negotiation** mechanism to detect the full-duplex availability.
- **In full-duplex mode Ethernet NICs deactivate CSMA/CD** (no collisions can occur).



Home WiFi Router

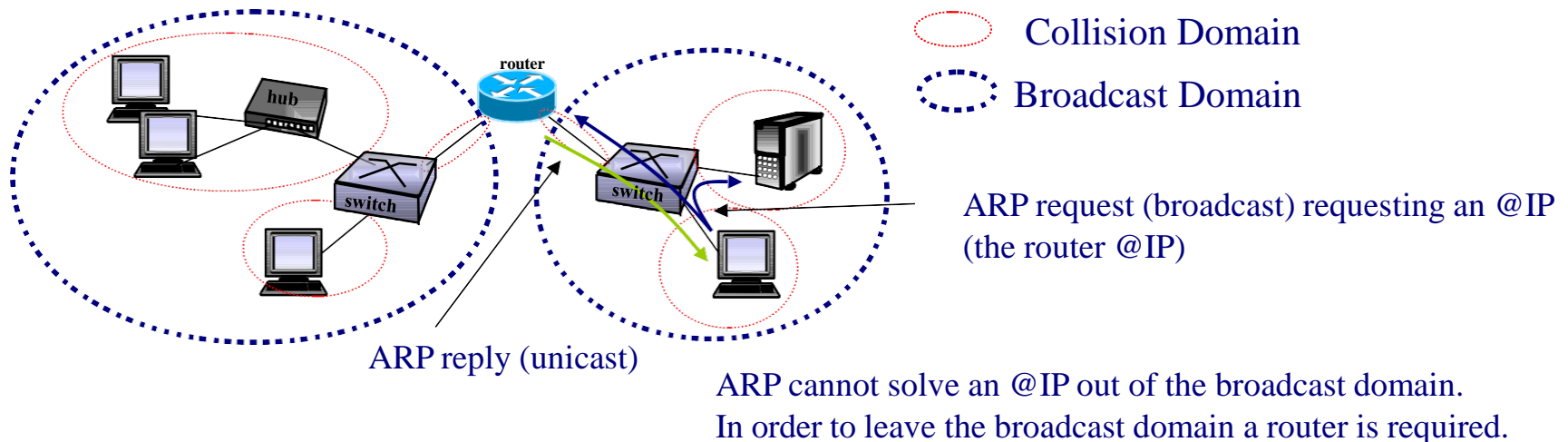
Yellow port: uplink to/from ISP

Ethernet switch with 4 ports

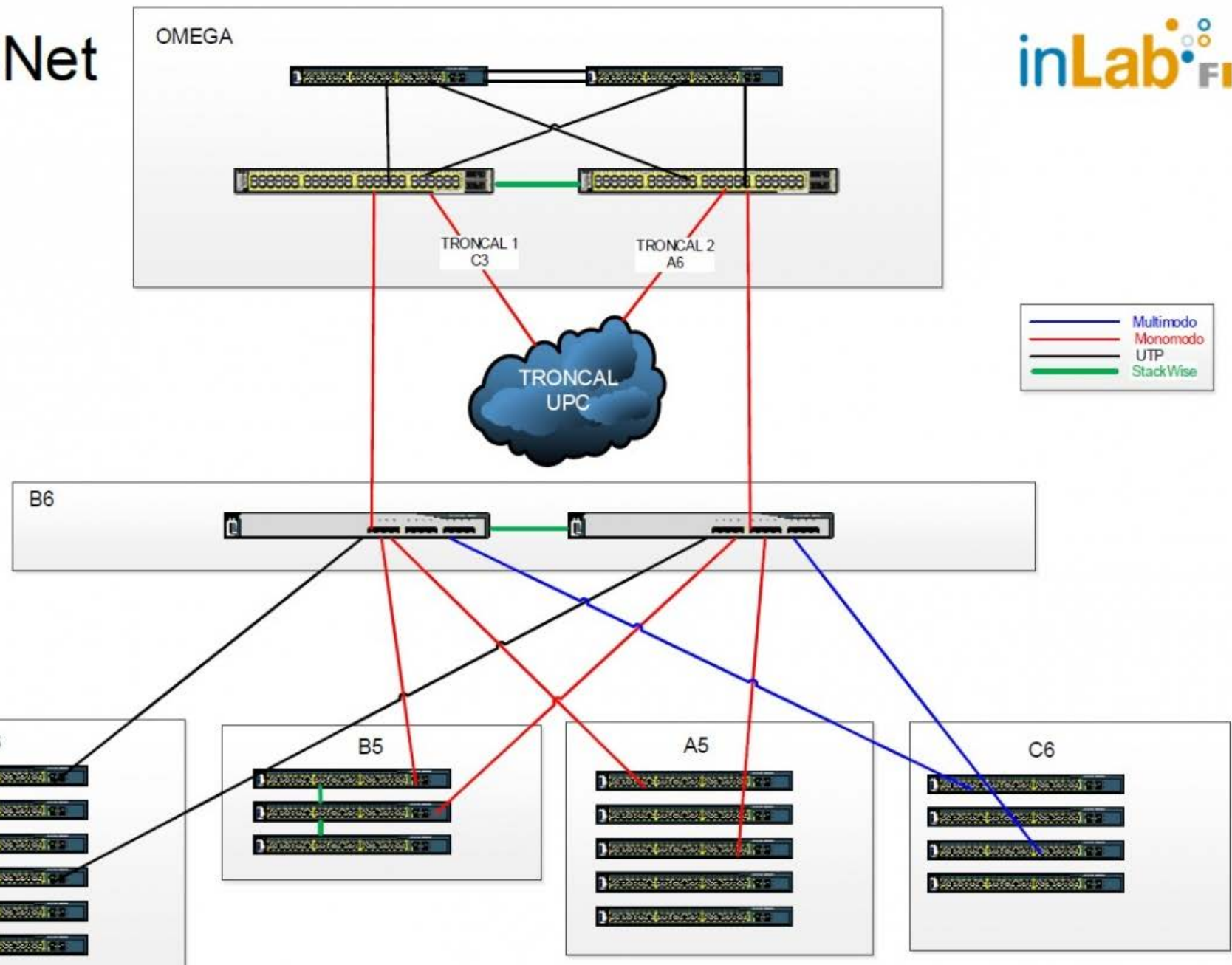
WiFi antennae

Ethernet Switches - Broadcast and Collision Domains

- **Broadcast Domain:** Set of stations that will receive a broadcast frame sent by any of them.
- Unless Virtual LANs are used, a switch does not segment the broadcast domain.
- A router segments the broadcast domain.
- The broadcast reachability is important because allows reaching stations having one hop connectivity (with ARP).

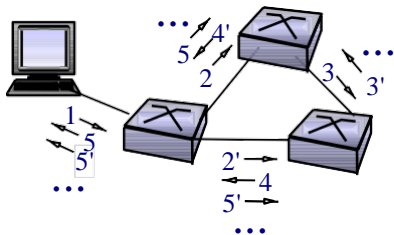


FIBNet



Ethernet Switches – Spanning Tree Protocol (STP)

- The basic principle of the “layer 2 routing” done by Ethernet switches is based on having a unique path to forward the frame towards the destination. Therefore, **loops are not allowed**.
- In practice loops can appear because:
 - They are introduced by accident.
 - They are desirable to have redundant path (fault tolerance).
- If loops are introduced without protection a **broadcast storm** is produced, and the network blocks:



Frames multiply and remain turning indefinitely in the loop!

Other problems:

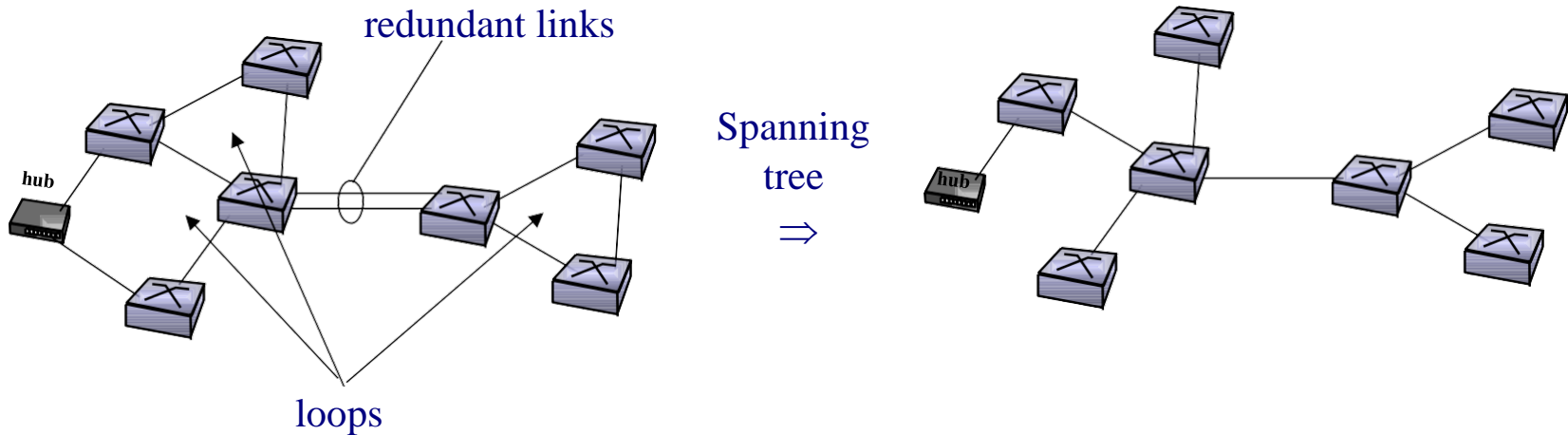
- Reception of duplicated frames
- MAC Tables instability



Solution: IEEE 802.1D Spanning Tree Protocol (STP)

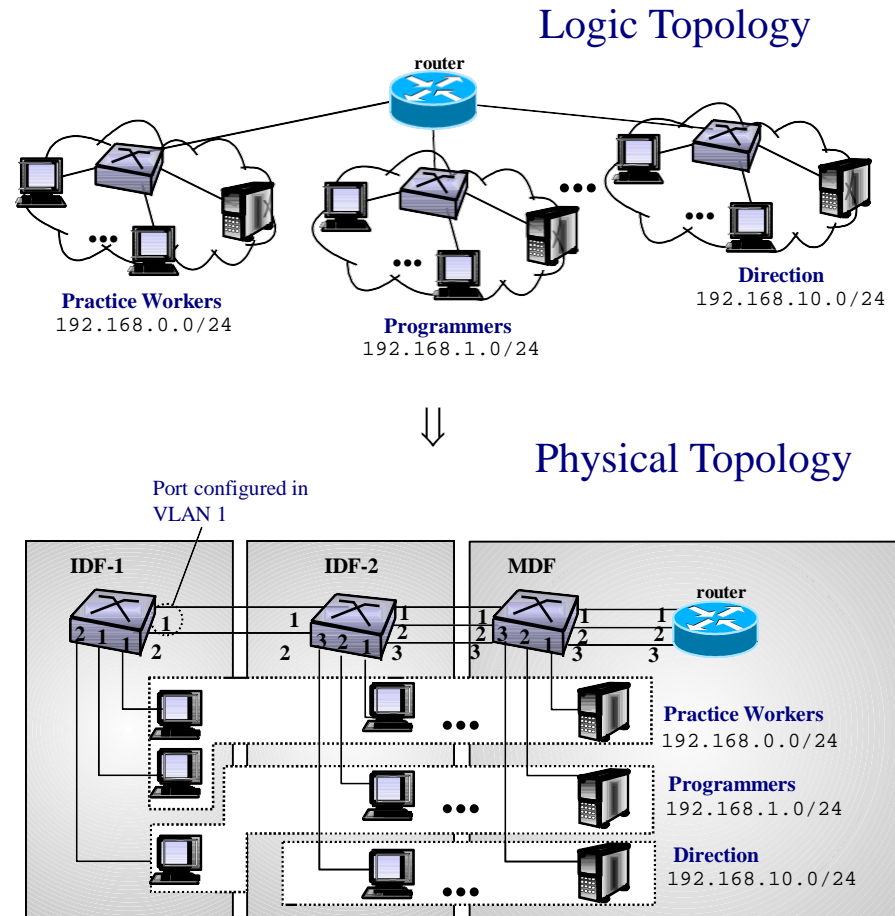
Ethernet Switches – Spanning Tree Protocol (STP)

- STP goal: Build a loop free topology (**STP-tree**) with optimal paths. The ports that do not belong to the STP tree are **blocked**.
- The switches send **802.1D messages** to their neighbors to build up the STP-tree. If the topology changes (e.g. due to a link failure), a new STP-tree is setup.



Ethernet Switches – Virtual LANs, VLANs

- Motivation:
- Grouping related servers and hosts in different broadcast domains.
- How VLANs work:
- Each switch port belongs to a VLAN.
- The switch **isolates different VLANs**: The switch flooding is done only towards the ports of the same VLAN. Each VLAN is equivalent to a different physical switch.
- A **router** is needed to send traffic to a different VLAN.

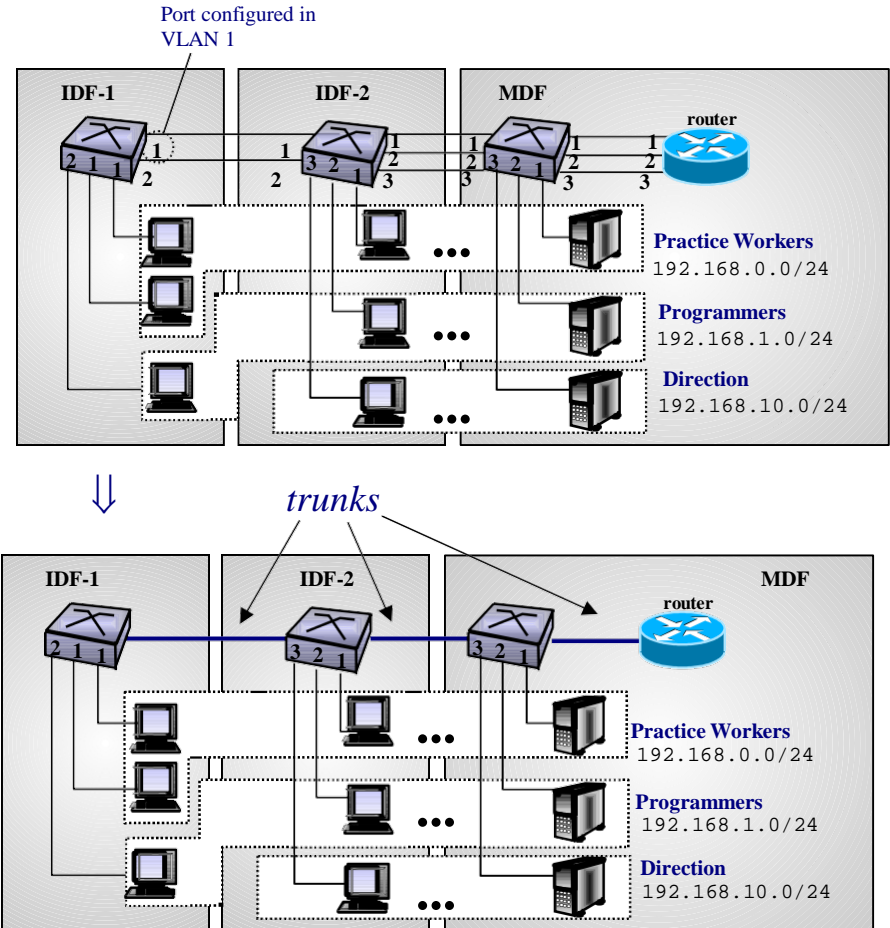


Ethernet Switches – Virtual LANs, VLANs

- **Advantages:**
- Flexibility of the physical placement of the devices.
- Facilitates network growth.
- Facilitates the network management: Changing the topology, adding new subnetworks, moving ports from one network to another.
- **NOTE:** Since each VLAN is a different broadcast domain, usually a different **STP** instantiation is used **for each VLAN**. Thus, a different STP-tree is build in each VLAN.

Ethernet Switches – VLAN Trunking

- Problem:
- Why connecting several ports between the same devices?
- **Trunking:**
- The port configured as trunk belongs to several VLANs (maybe all).
- The traffic sent in one VLAN is also sent to the trunk the VLAN belongs to.
- A **tagging** mechanism is used in the trunk to discriminate the traffic from different VLANs.



Ethernet Switches – VLAN Trunking

- Trunking Protocols: **IEEE-802.1Q**

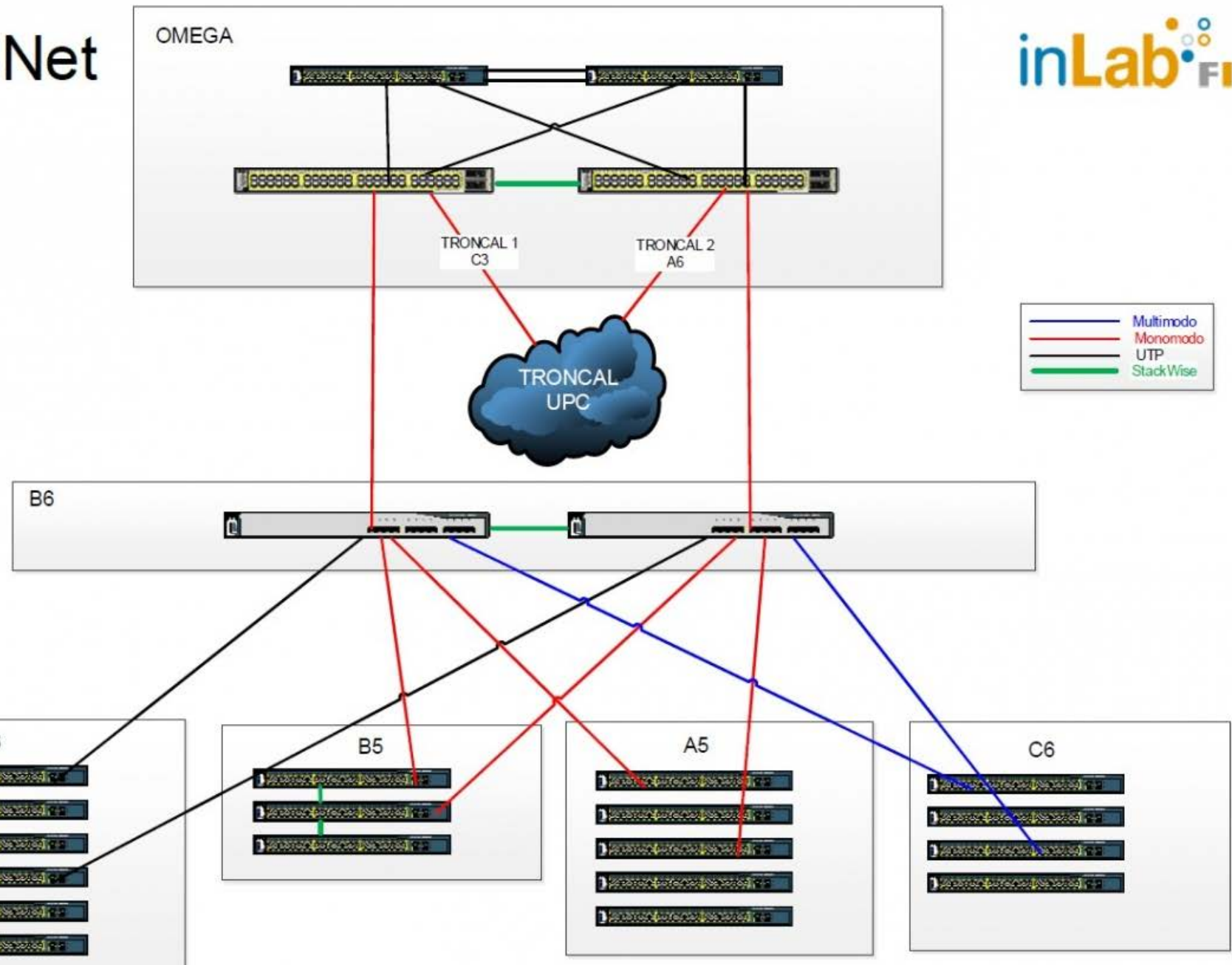
Preamble (8 bytes)	Destination MAC Address (6 bytes)	Source MAC Address (6 bytes)	TPID (2 bytes)	TCI (2 bytes)	Length of the frame (2 bytes)	Payload (46 to 1500 bytes)	CRC (4 bytes)
-----------------------	---	------------------------------------	-------------------	------------------	-------------------------------------	----------------------------------	------------------

IEEE-802.3 frame with the 802.1Q *tag*.

Legend:

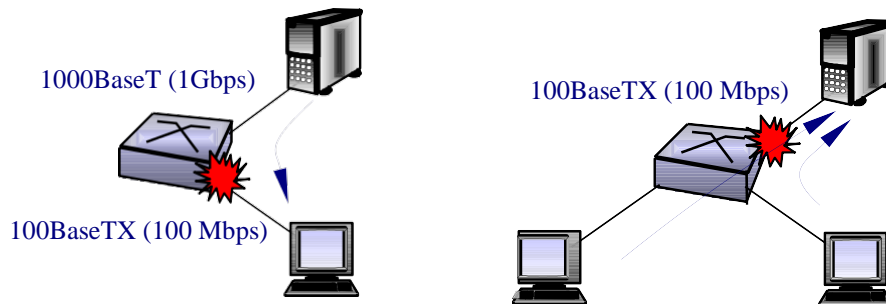
- *Tag Protocol Identifier* (TPID): Field with the hexadecimal value 8100 for an Ethernet frame.
- *Tag Control Information* (TCI): Contains several fields. The most important is the **VLAN ID (12 bits)**, which identifies the VLAN.

FIBNet



Ethernet Switches – Flow Control

- Switch **Flow Control**: Consists of adapting the rate at which the switch receives the frames, and the rate at which the switch can send them.
- Examples:

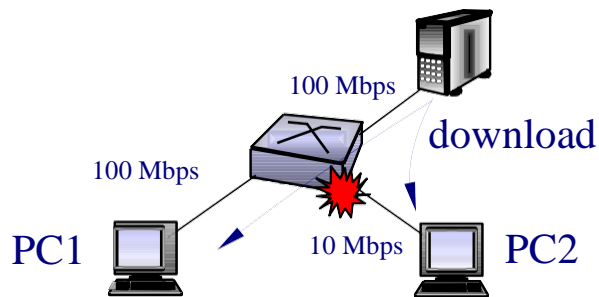


If no flow control is used, frames could be lost by buffer overflow.

- Flow control techniques (back pressure):
 - **Jabber** signal (**half duplex**): The switch sends a signal into the port which need to be throttled down, such that CSMA see the medium busy.
 - **Pause frames** (**full duplex**): The switch send special *pause frames*. These frames have an integer (2 bytes) indicating the number of slot-times (512 bits) that the NICs receiving the frame must be silent.

Ethernet Switches – Problems of Flow Control

- Flow Control can introduce inefficiencies (*head of line blocking*):

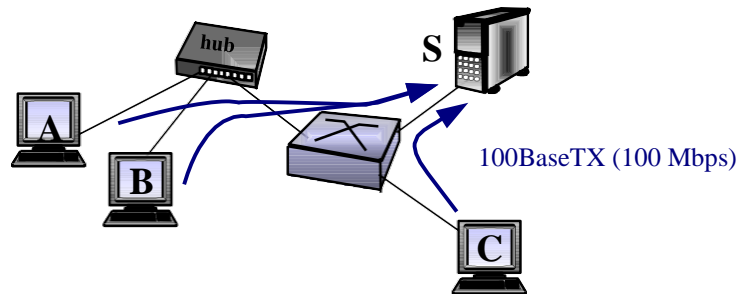


The **slow link** may trigger the flow control and send pause frames towards the server, causing under-utilization of the switch-server link.

- We would expect a download of approximately 90 Mbps for PC1 and 10 Mbps for PC2. However, the flow control can make the PC1 throughput to be significantly lower. **Switches allow disabling the flow control** in a link. If **flow control is disabled**, traffic is assumed to be controlled by **TCP**.
- If not otherwise stated, we shall assume an **ideal flow control** in the problems, which allow achieving the maximum throughput.

Ethernet Switches – Line bitrate sharing

- **Hub**: If the hub is the bottleneck for all the active ports, the capacity is equally shared between all ports where frames are transmitted.
- **Switch**: If one congested port is the bottleneck for all ports sending traffic to it, the port bit rate is equally shared between all ports sending traffic to it.
- Example:



- If A, B and C simultaneously transmit to S:
throughput C $\approx 100 \text{ Mbps} / 2 = 50 \text{ Mbps}$
throughput A = throughput B $\approx (100 \text{ Mbps} / 2) / 2 = 25 \text{ Mbps}$

Outline

- Introduction
- IEEE LAN Architecture
- Ethernet
- Ethernet Switches
- **Wireless LANs**

Wireless LANs (WLANs) – Brief WLAN History

- 1971: Prof. Norman **Abramson** develops ALOHNET for the University of Hawaii
- 1990: many companies develop proprietary WLANs products.
- 1996: ETSI approves HIPERLAN/1 and
- 1997: IEEE approves **802.11**
- Late 90 and 2000: Wi-Fi Alliance, tremendous growth of 802.11 products.
- 1999: 802.11a, 802.11b. 2003: 802.11g. 2009: 802.11n...



802.11 indoor APs

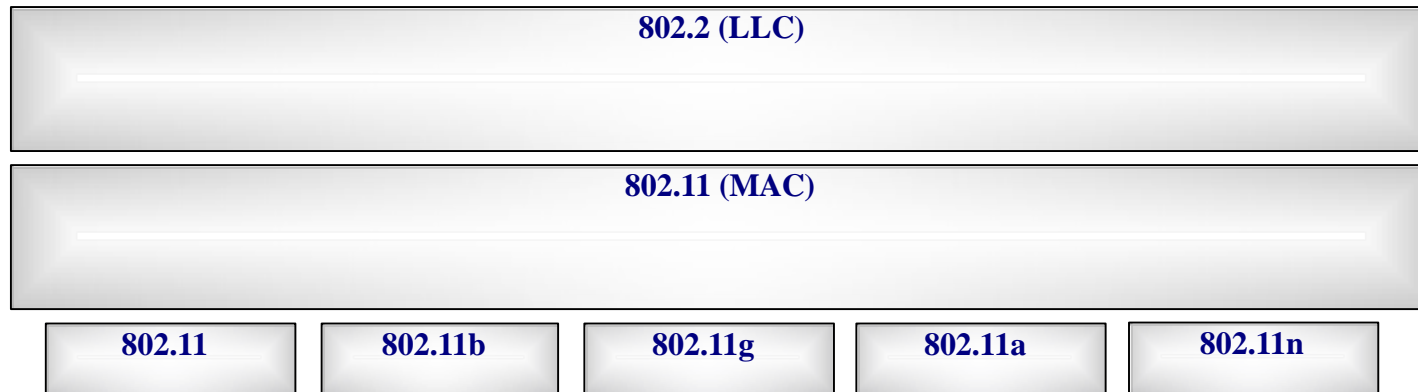


802.11 NICs



802.11 outdoor

Wireless LANs (WLANs) – 802.11

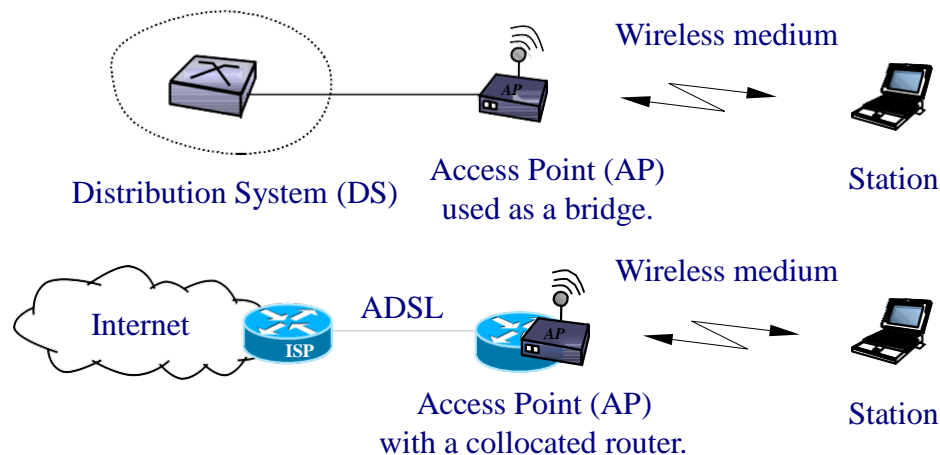


<u>Standard</u>	<u>Bitrate</u>	<u>ISM band</u>
802.11	1, 2 Mbps	2.4 GHz
802.11b	up to 11 Mbps	2.4 GHz
802.11a	up to 54 Mbps	5 GHz
802.11g	up to 54 Mbps	2.4 GHz
802.11n	up to 600 Mbps	2.4 or 5 GHz

- **ISM:** Industrial Scientific and Medical. No licence required for non commercial usage.

Wireless LANs (WLANs) – 802.11 Components

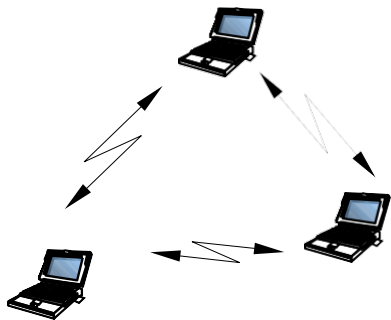
- Distribution System (DS):
 - Used by APs to exchange frames with one another and with wired networks. (e.g. an ethernet switch).
- Access Point (AP)
 - Simplify communication between stations.
 - All transmissions go through the AP.
 - APs are bridges and may have a collocated router.



Wireless LANs (WLANs) – 802.11 Components

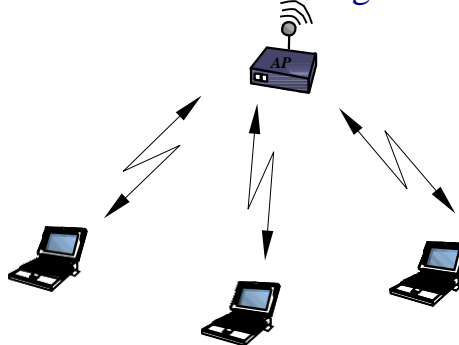
- Basic Service Set (**BSS**)
 - Set of stations communicating with each other.
 - Are identified by: (i) a Service Set identifier (**SSID**), or Network name: String with <32 characters; and (ii) a BSS Identifier (**BSSID**): 48 bits number.
 - If the network is composed of more than 1 BSS it is called Extended Service Set (**ESS**).

Independent BSS (IBSS) (*ad-hoc mode*)

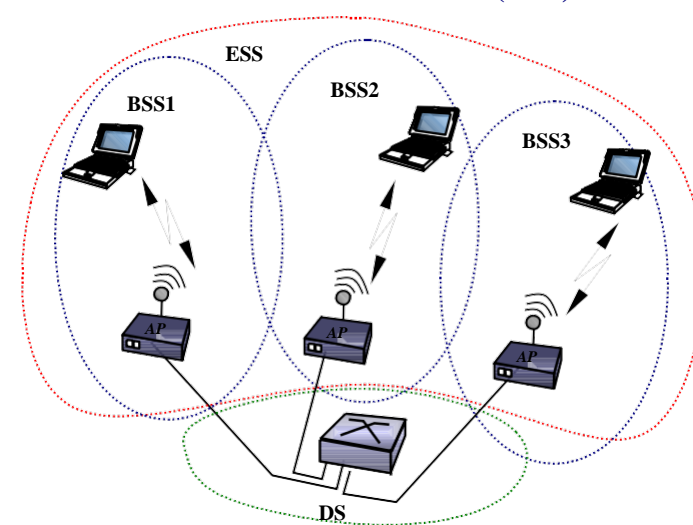


Infrastructure BSS (*infrastructure mode*)

- An station must associate with an AP.
- All transmissions go through the APs.



Extended Service Set (ESS)



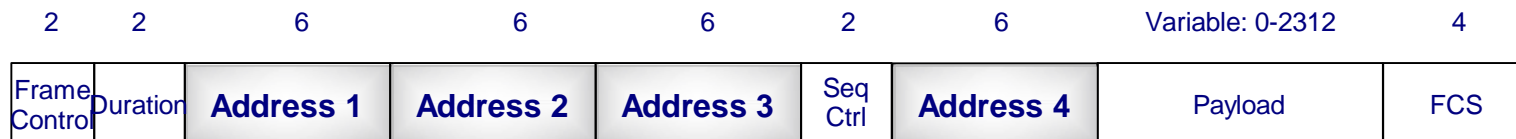
Wireless LANs (WLANs) – 802.11 MAC

- Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA):
In contrast to CSMA/CD, **always waits a random backoff before Tx.**
Acks are needed to detect whether a transmitted frame collided.
- CSMA/CD is not used because collisions can hardly be detected in wireless (because in the antenna the Tx power is orders of magnitude higher than Rx power).

A mobile device must associate with an AP (SSID)
All frames go through the AP
Frames must be acknowledged (no collision detection)

Wireless LANs (WLANs) – 802.11 Frame and Addresses

- Designed to be **compatible with ethernet**.
- Use non overlapping ranges with ethernet.
- The frame may have **up to 4 addresses**. The meaning of the addresses is specified by the bits **to-DS** and **from-DS** of the control.
- The **BSSID** is always present to identify frames belonging to the BSS



Generic frame format

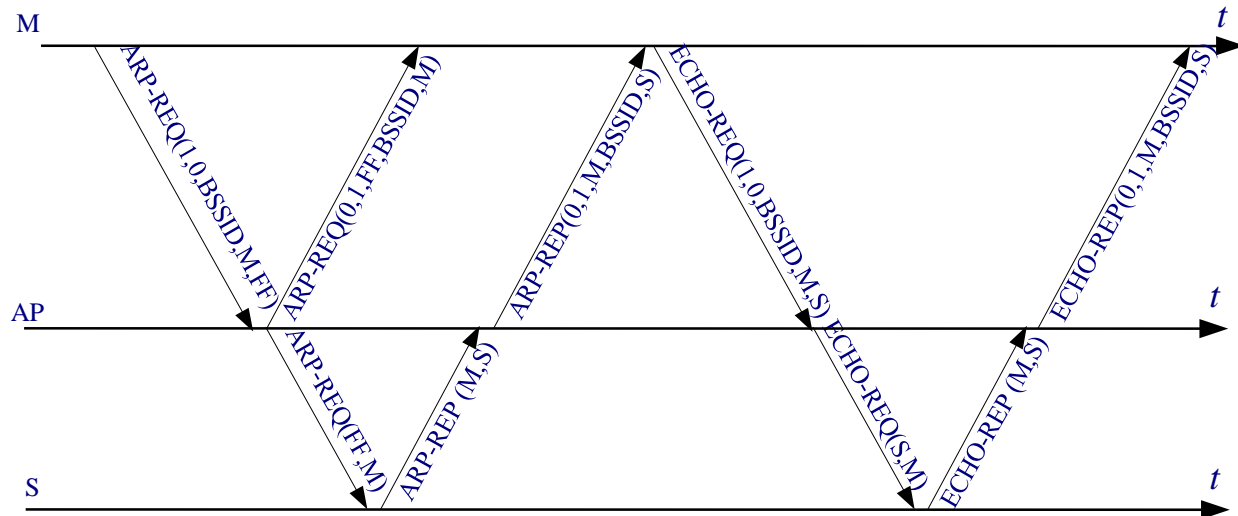
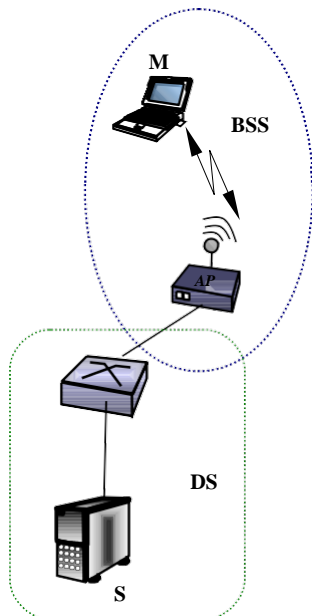
Wireless LANs (WLANs) – 802.11 Addresses

Scenario	Usage	to-DS	from-DS	Address1	Address2	Address3	Address4
STA→STA	Ad-hoc	0	0	DA	SA	BSSID	-
STA→AP	Infrastructure	1	0	BSSID	SA	DA	-
AP→STA	Infrastructure	0	1	DA	BSSID	SA	-
AP→AP	WDS	1	1	RA	TA	DA	SA

Legend: Destination Address (DA), Source Address (SA), Receiver Address (RA), Transmitter Address (TA), Wireless Distribution System (WDS)

Example:

M# ping S



Legend, frames 802.11:

MESSAGE-TYPE(to-DS, from-DS, Address1, Address2, Address3)

Legend, frames ethernet:

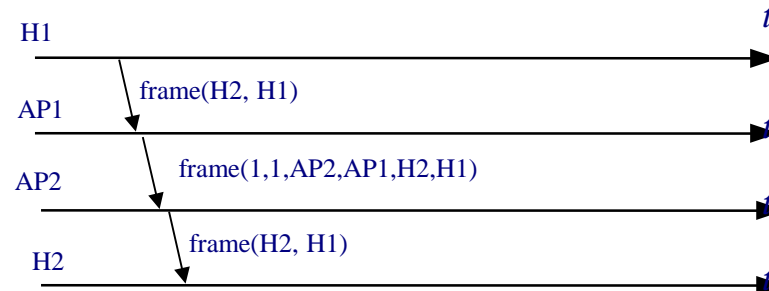
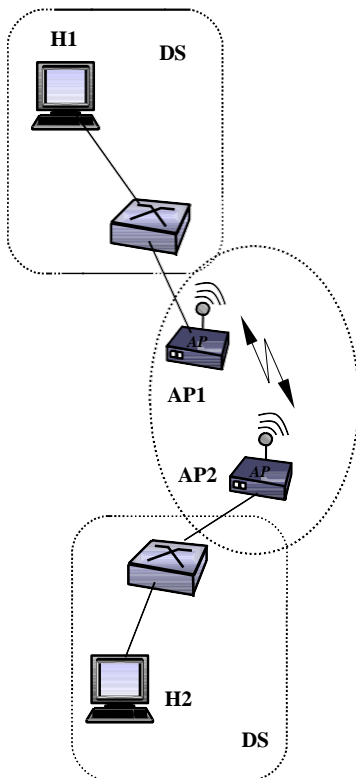
MESSAGE-TYPE(destination address, source address)

FF is the broadcast address

Wireless LANs (WLANs) – 802.11 Addresses

Scenario	Usage	to-DS	from-DS	Address1	Address2	Address3	Address4
STA→STA	Ad-hoc	0	0	DA	SA	BSSID	-
STA→AP	Infrastructure	1	0	BSSID	SA	DA	-
AP→STA	Infrastructure	0	1	DA	BSSID	SA	-
AP→AP	WDS	1	1	RA	TA	DA	SA

Legend: Destination Address (DA), Source Address (SA), Receiver Address (FA), Transmitter Address (TA) , Wireless Distribution System (WDS)



Legend, frames 802.11:

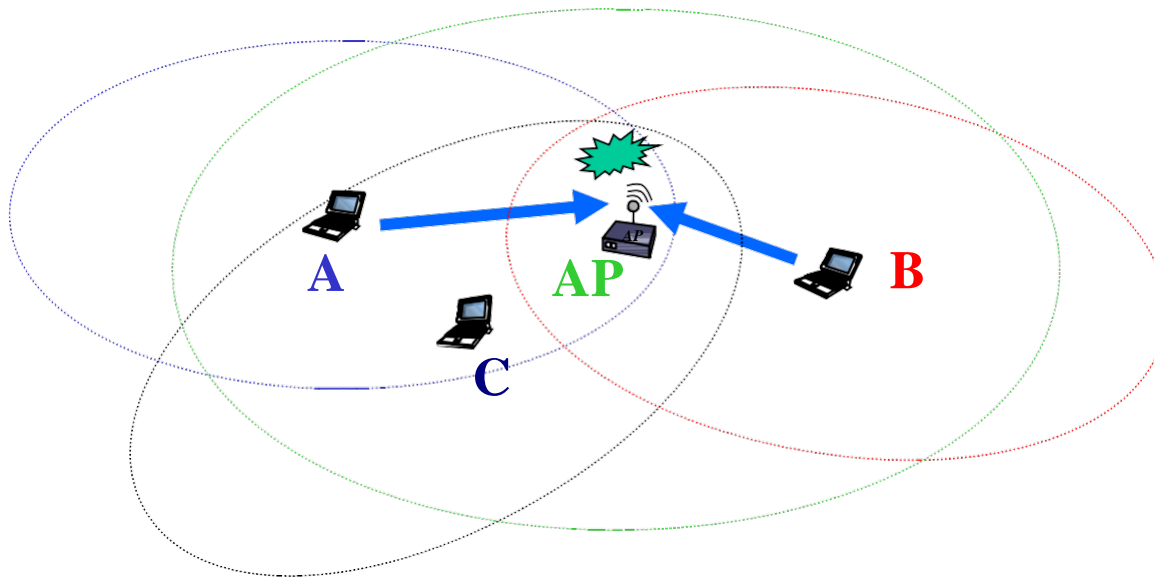
frame(to-DS, from-DS, Address1, Address2, Address3, Address4)

Legend, frames ethernet:

frame(destination address, source address)

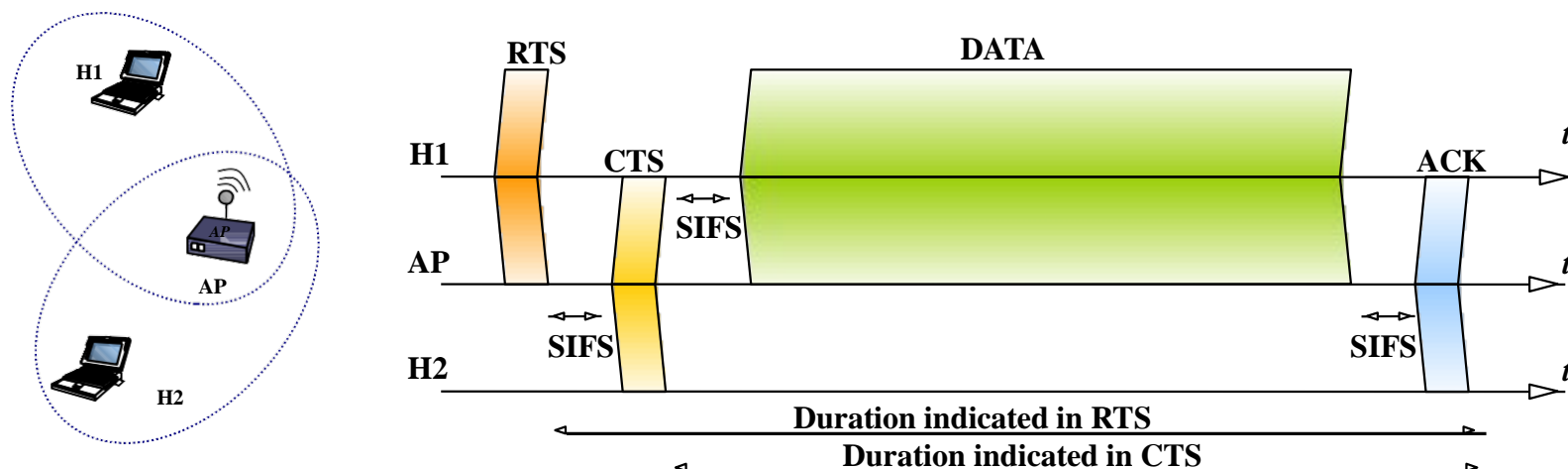
Wireless LANs (WLANs) – Hidden Node Problem

- Node A is in coverage with AP and C
- A and B cannot hear each other
- When A transmits to AP, B cannot detect the transmission using the carrier sense mechanism
- If B transmits, a collision will occur at AP



Wireless LANs (WLANs) – 802.11 RTS/CTS

- Optional mechanism to solve the hidden node problem.



- RTS** is sent using the basic access mechanism.
- Upon receiving a RTS/CTS, the station set the **Network Allocation Vector (NAV)** to the indicated duration. While the NAV is non zero, the virtual carrier sensing indicates that the medium is busy.
- RTS/CTS is **only used for unicast Tx**.
- There is a **threshold** indicating the minimum frame size for using RTS/CTS.