Computer Networks. Unit 3: LANs

Notes of the subject *Xarxes de Computadors, Facultat Informàtica de Barcelona, FIB*

Llorenç Cerdà-Alabern

April 6, 2021

Contents

3 Unit 3: LANs

3.1 WAN vs LAN

- **LANs**:
  - **Multy-access** network with **shared media**
  - Medium Access Control (**MAC**) protocol: governs who can access the shared media
  - **Note**: Ethernet has evolved to a **switched** network

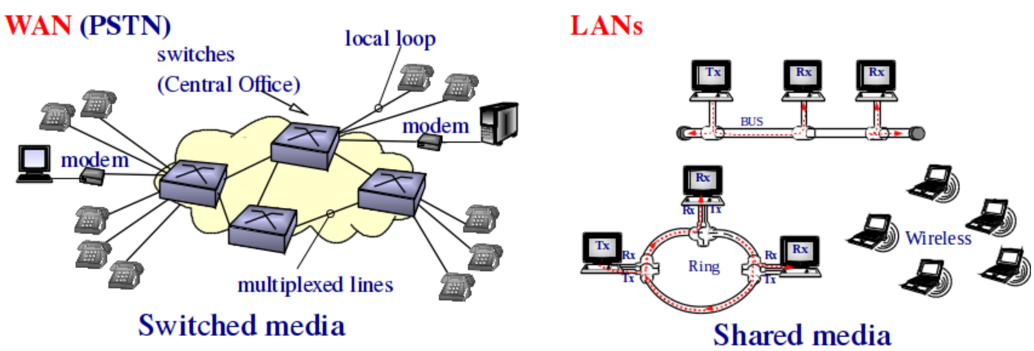


Figure 1: WAN topology (switched media) vs LAN topoloty (shared media).

Acronyms:

LAN	Local Area Network
MAC	Medium Access Control
PSTN	Public Switched Telephone Network
WAN	Wide Area Network

3.2 IEEE LAN Architecture

- **LLC** sublayer (802.2): Generic L2 layer common to all LAN standards (802.x)

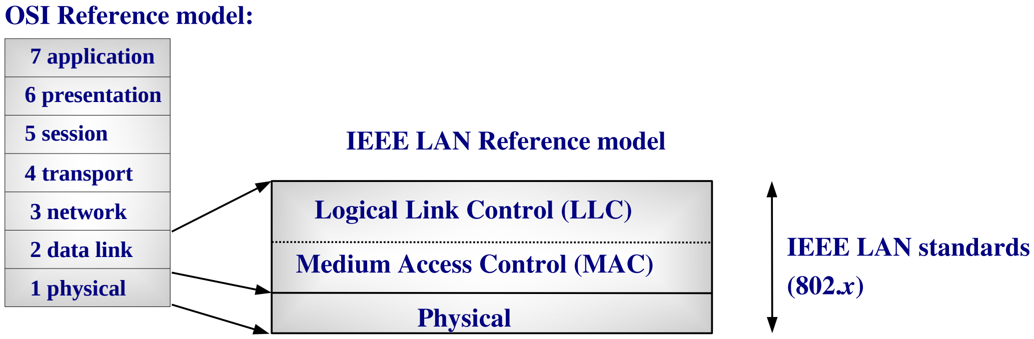


Figure 2: IEEE LAN architecture.

Acronyms:
LLC Logical Link Control

3.2.1 IEEE LAN encapsulation

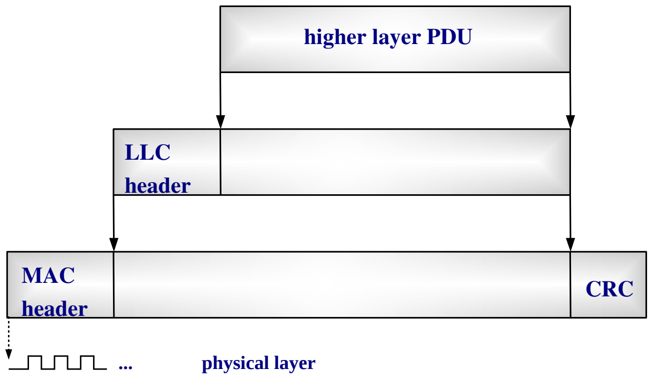


Figure 3: IEEE LAN encapsulation.

Acronyms:
PDU Protocol Data Unit
CRC Cyclic Redundancy Check

3.2.2 IEEE LLC header

3 / 4 bytes

```
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 bits
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|Destination SAP| Source SAP    | Control       /
|               |               | 8 or 16 bits  /
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 4: IEEE LAN LLC frame.

SAP: Service Access Point

- Identify the **protocols** handling the frame
- Standardized by **IEEE**
- **SNAP** allows non IEEE protocol IDs URL

SAP (hex)	Protocol
06	ARPANET Internet Protocol (IP)
08	SNA
42	3IEEE 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.

Figure 5: Table with some IEEE SAP values. SNAP is used to extend IEEE SAP values.

Acronyms:
SAP Service Access Point
SNAP Subnetwork Access Protocol

3.2.3 Ethernet with IEEE Sub-Network Access Protocol (SNAP)

- Used in **TCP/IP**
- **Type** field identifies the Ethernet frame payload.
- Values standarized by **IETF** in RFC1700 (Assigned Numbers - Ether Types)

802.3 SNAP Frame

```
+-------+------+------+------+--------+------+-----------+----------+
| MAC   | DSAP | SSAP |Contr.|  OUI   | Type |upper layer| CRC      |
| 802.3 | 0xAA | 0xAA | 0x03 |0x000000|2bytes| PDU       |(4 bytes) |
+-------+------+------+------+--------+------+-----------+----------+
```

LLC header (3 bytes) **SNAP header (5 bytes)** **≲ 1492**

Figure 6: IEEE SNAP encapsulation.

Acronyms:
DSAP Destination SAP
SSAP Source SAP
OUI Organizationally Unique Identifier

3.2.4 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 (**obsolete**)
- **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, WiFi

3.3 Ethernet

- Designed by **Bob Metcalfe** at Xerox in mid-1970s
- Original design: **random** access, **bus** topology
- Initially was commercialized by Digital, Intel and Xerox consortium (**DIX**)
- Standardized by **IEEE** (**802.3**) in 1983
- Nowadays Ethernet is the **leading** LAN technology

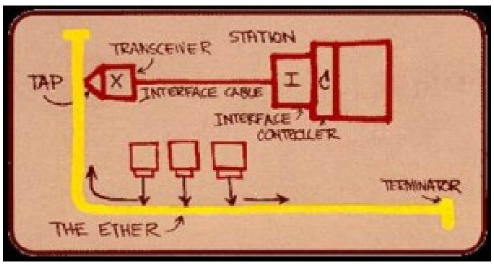


Figure 7: Original figure of Bob Metcalfe of an Ethernet LAN.

3.4 Ethernet MAC

- 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**.

Acronyms:
CSMA/CD Carrier Sense Multiple Access/Collision Detection

3.5 CSMA/CD

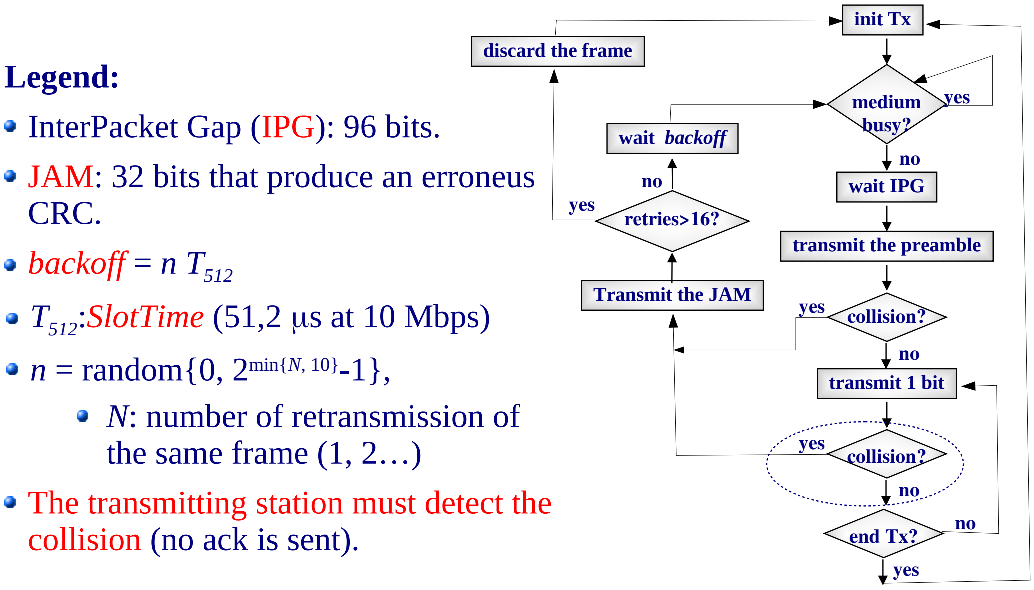


Figure 8: Flow diagram of CSMA/CD.

3.5.1 CSMA/CD: Collision example

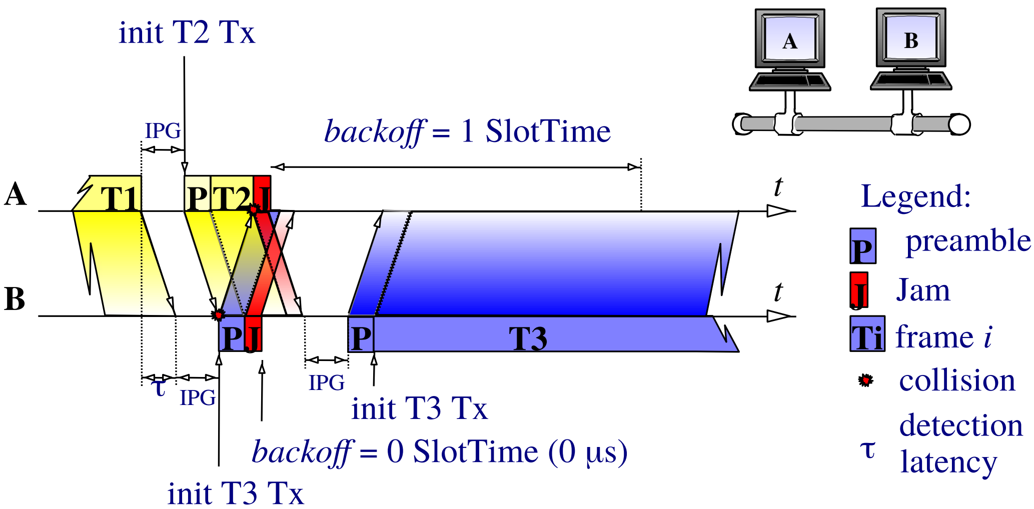


Figure 9: Time diagram of a collision with CSMA/CD.

3.5.2 Half Duplex and full-duplex

- **Half Duplex**: only one NIC can be simultaneously transmitting into the medium. **CSMA/CD** is used
- **Full Duplex**: When 2 Ethernet NICs are connected **point-to-point**, some Ethernet standards allow a full-duplex Tx. **CSMA/CD** is NOT used (no collisions can occur).
- Ethernet NICs have an **auto-negotiation** mechanism to detect the full-duplex availability and bitrate (backward compatible)

Acronyms:
Tx Transmission
Rx Reception

3.6 Ethernet Frame

There are **2 Ethernet frames** currently used: URL

- **DIX**: most common type in use today. **Do not use LLC**

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

Figure 10: DIX ethernet frame.

- **IEEE**: **use LLC**

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

Figure 11: IEEE ethernet frame.

- Minimum payload of **46** bytes when **CSMA/CD** is used
- **Length** (IEEE): Payload size (0~1500)
- **Type** (DIX): Identifies the upper layer protocol (IP, ARP, etc.) RFC1700, Assigned numbers. Always > 1500
- TCP/IP with **IEEE encapsulation uses SNAP** RFC1042

3.7 IEEE Ethernet standards

Standard: 802.3xx. Name convention:

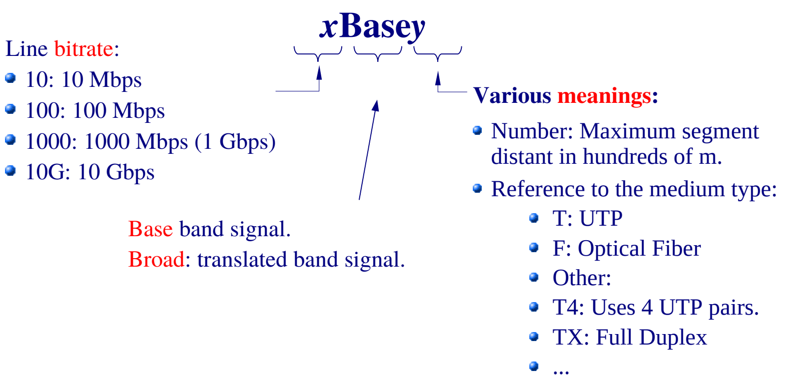


Figure 12: IEEE ethernet standards name convention.

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.

Figure 13: Table with main IEEE ethernet standards.

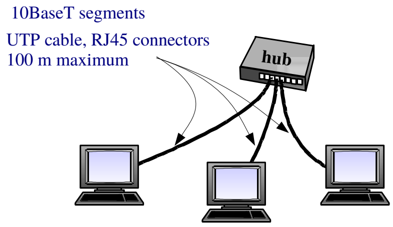


Figure 14: IEEE ethernet 10BaseT configuration.

3.8 Ethernet Switches

- CSMA/CD (hub): with many stations **collisions** are inefficient
- Solution: Ethernet **bridge**

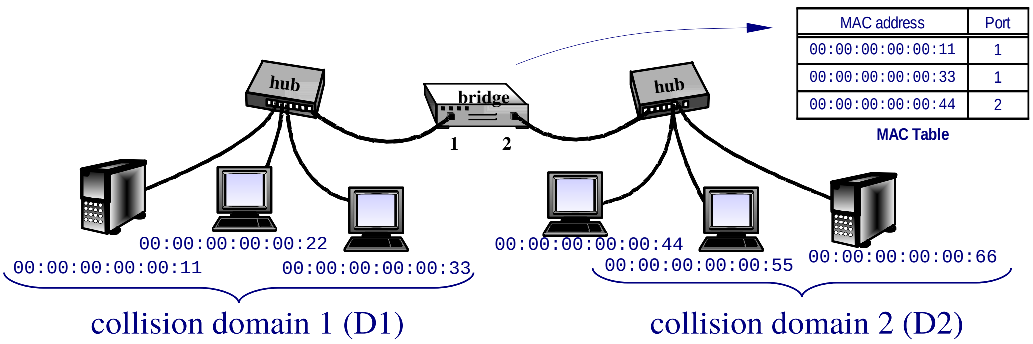
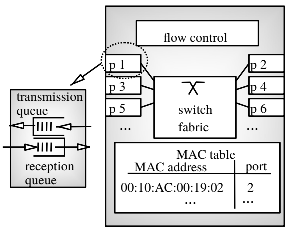


Figure 15: Ethernet bridge concept.

- In each **port** there is a NIC
- The **source address** is used to learn which MAC is in each port (**MAC table**)
- If dest. address is not in the table: **flooding** (Tx in all ports). Otherwise, Tx only in 1 port (segments the **collision domain**)
- An Ethernet switch is a **multiport bridge**




```
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.

Figure 16: Ethernet switch architecture and MAC table.

3.8.1 Ethernet switch capabilities

- Each port is different a **collision domain**
- Different ports can **Tx/Rx simultaneously**
- Ports can have **different bitrates**
- Ports can be **full-duplex**
- There can be ports **half or full duplex**
- Link **aggregation**: several links can be aggregated acting as a single link of higher capacity
- **Security**: stations see only traffic of their collision domain

3.9 Virtual LANs, VLANs

- **Motivation**: Adapt logic to physical topology
- The switch **isolates** different VLANs: Each VLAN is equivalent to a different switch

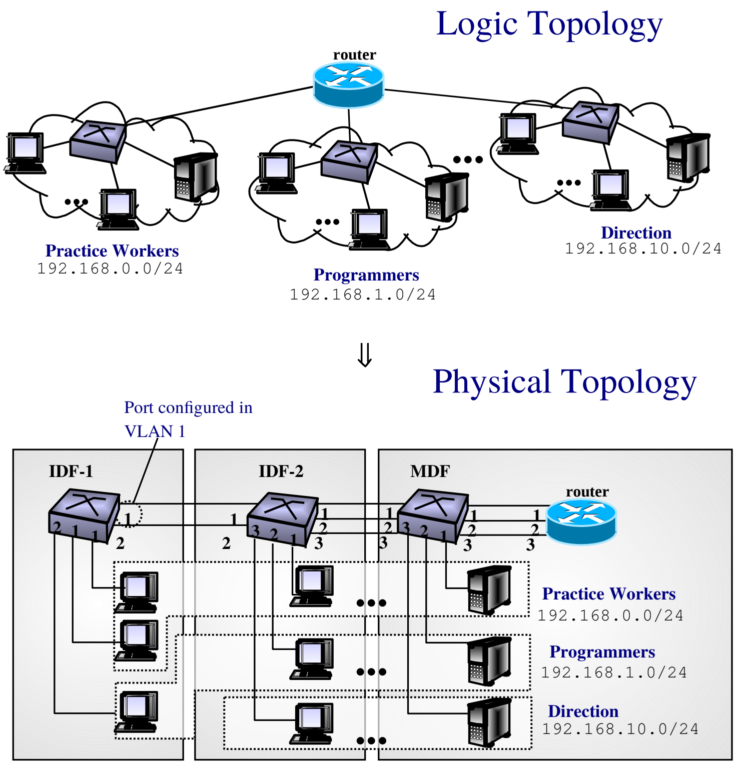


Figure 17: VLAN physical and logical topology.

3.9.1 VLAN Trunking

- The port configured as trunk belongs to **all VLANs**
- VLANs are distinguished by **tagging**

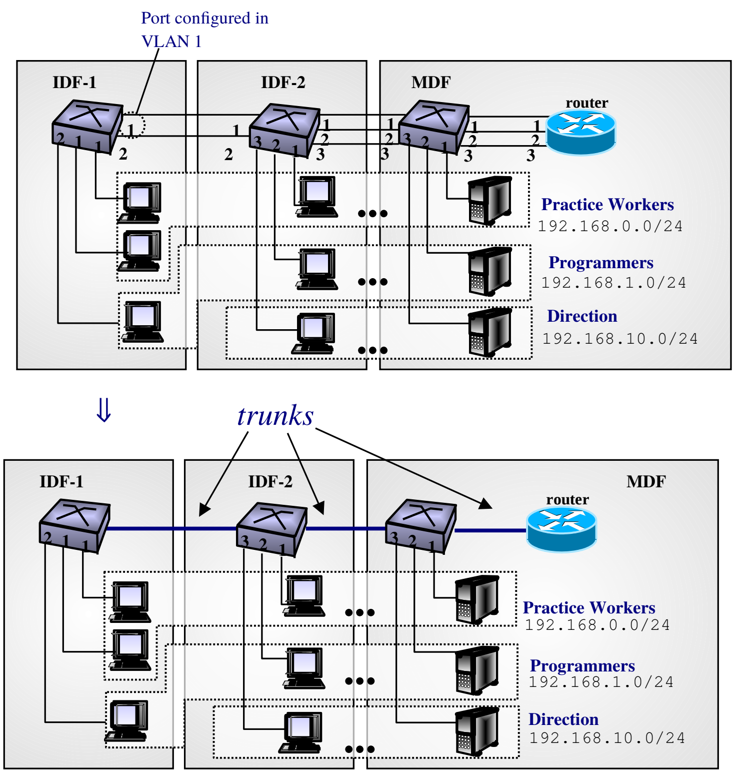


Figure 18: VLAN trunking.

- IEEE-802.1Q (VLAN tagging)

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

Figure 19: IEEE-802.3 frame with the 802.1Q tag.

- Tag Protocol Identifier (TPID): 8100 for Ethernet
- Tag Control Information (TCI): **VLAN ID** (12 bits)

3.10 Broadcast domains

- Set of stations that will received a **broadcast frame** sent by any of them
- ARP cannot solve an @IP out of the broadcast domain
- **Hubs and switches** does not partition broadcast domains
- To leave the broadcast domain a **router** is required

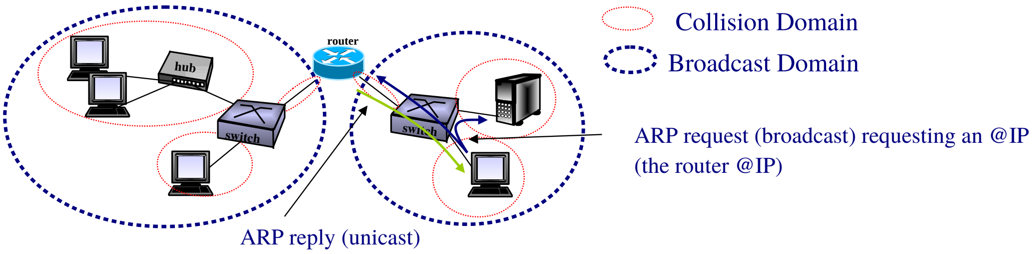


Figure 20: Broadcast domain.

3.11 Switch flow control

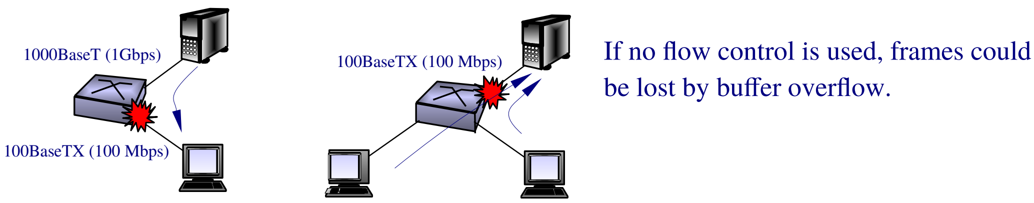


Figure 21: Flow control in ethernet switches.

- Flow control techniques
  - **Jabber signal** (**half duplex, CSMA/CD**): 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 indicating the time that the NICs receiving the frame must be silent

Flow Control head of line blocking

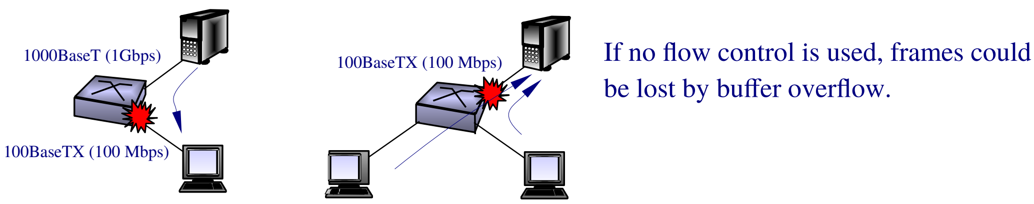


Figure 22: Flow control may be inefficient if head of line blocking occurs.

- We shall assume an **ideal flow control in the problems**, which allow achieving the maximum throughput

3.12 Spanning Tree Protocol (STP)

- loops can produce a **broadcast storm** which could block the network

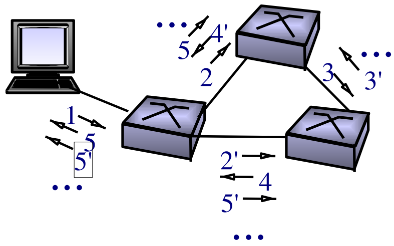


Figure 23: A broadcast storm occurs when there is a layer 2 loop.

- Solution: IEEE 802.1D **Spanning Tree Protocol (STP)**

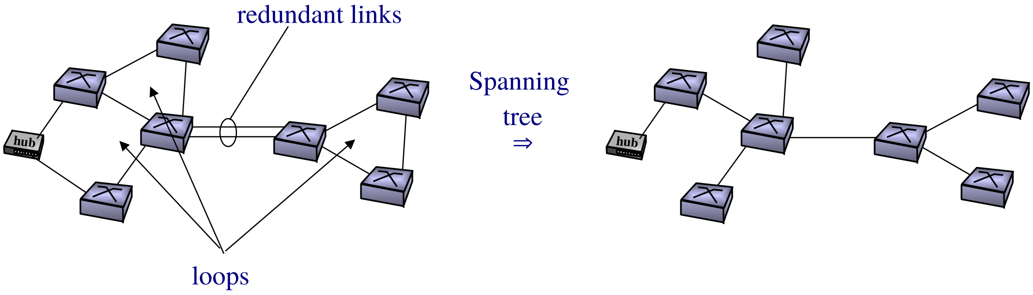


Figure 24: STP remove loops and generate a spanning tree topology.

Acronyms:
STP Spanning Tree Protocol

3.13 Evaluation of Computer Networks

- Let the **network capacity** v_t be the maximum transition rate that a connection can reach in bits per second (bps). For instance, if we have a single link, v_t would be the line bit rate

$$v_t[\text{bps}] = \frac{1}{t_b}$$

where t_b is the transmission time of a bit.

- **Throughput** (*velocidad efectiva*). It is the average transmission rate of the user data in bps:

$$v_{ef}[\text{bps}] = \frac{\text{number of information bits}}{\text{observation time}, T}$$

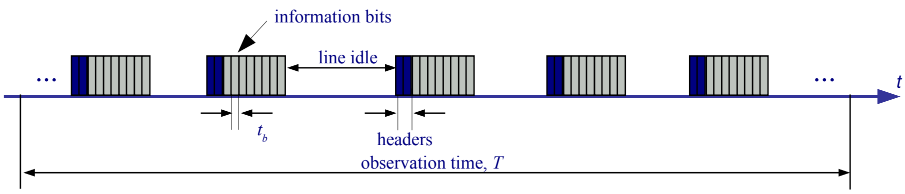


Figure 25: Definition of Throughput: information bits and observation time.

- **Efficiency**

$$E[\%] = \frac{v_{ef}}{v_t} \times 100$$

3.13.1 Practical example:

throughput with speedtest

```
tcpdump -ni wlan0 tcp
```

3.13.2 Bottleneck

- Given a network condition, the **bottleneck** of a connection is the computer component, the link or network device that limits the maximum throughput.

Example:

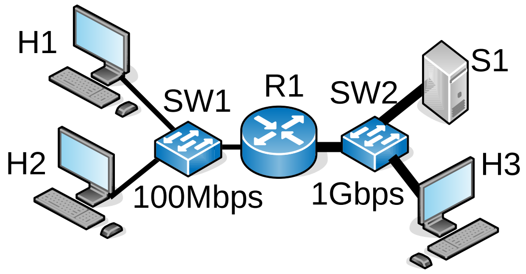


Figure 26: Router R1 connects 2 switches SW1 (100 Mpbs), and SW2 (1 Gbps). In SW1 are connected hosts H1, H2, in SW2 are connected S1 and H3.

The hosts H1, H2, H3 download a large file using TCP from the server S1 and write it to the local disc. The disc of the hosts has a writing speed of 80 Mbps. The disc of the server has a reading speed of 8 Gpbs. Identify **bottlenecks** and compute the **throughput**. **Solution**:

- **H1, H2**: The bottleneck is the link Sw1-R1. The throughput is $v_1 = v_2 = 100/2 = 50$ Mbps
- **H3**: The bottleneck is the disc. The throughput is $v_3 = 80$ Mbps

3.14 Wireless LANs (WiFi)

ISM: Industrial Scientific and Medical, **no license required**

Year	standard	max bitrate	ISM band
1997	802.11	2 Mbps	2,4 GHz
1999	802.11a	54 Mbps	5 GHz
1999	802.11b	10 Mbps	2,4 GHz
2003	802.11g	54 Mbps	2,4 GHz
2009	802.11n	600 Mbps	2,4/5 GHz
2013	802.11ac	6,9 Gpbs	5 GHz

Figure 27: Table showing WiFi stadards, maximum bitrate and ISM bands.

3.14.1 802.11 Components

- Basic Service Set, **BSS**: Identifies a WiFi Network
  - Service Set identifier (**SSID**) or Network name
  - BSS Identifier (**BSSID**): 48 bits number (MAC address of the AP)
- Distribution System (**DS**): Exchange frames with other networks. (e.g. an Ethernet switch)

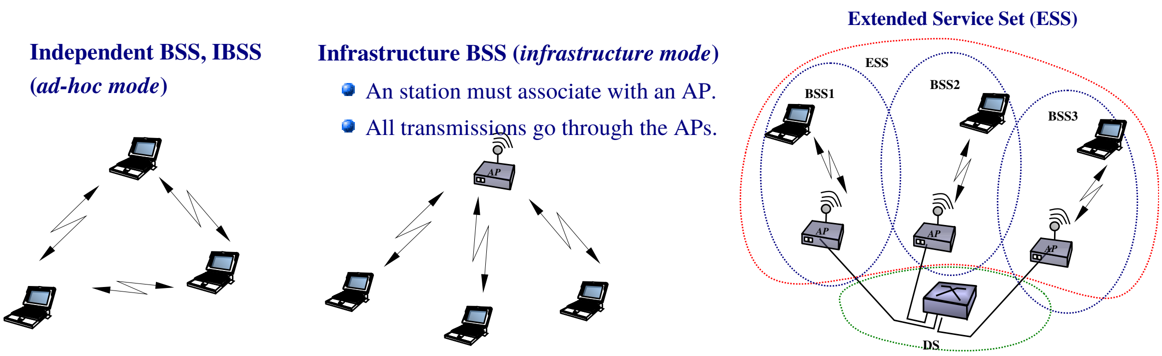


Figure 28: 3 types of WiFi configurations: ad-hoc, infrastructure and extended service set.

- Practical example:

```
sudo iw wlan0 scan
```

Acronyms:

AP	Access Point
BSS	Basic Service Set
BSSID	BSS Identifier
SSID	Service Set identifier
DS	Distribution System

3.14.2 802.11 MAC

- In WiFi collisions cannot be detected while transmitting
- Carrier Sense Multiple Access with **Collision Avoidance CSMA/CA**: In contrast to CSMA/CD, always wait a random backoff before Tx
- **Acks** are used to detect whether a unicast transmitted frame collided
- **Collisions of broadcast frames** are not detected
- **802.11 Addresses**
  - Designed to be compatible with Ethernet
  - Use non overlapping ranges with Ethernet
  - The frame may have up to **4 addresses**

2	2	6	6	6	2	6	Variable: 0-2312	4
Frame Control	Duration	**Address 1**	**Address 2**	**Address 3**	Seq Ctrl	**Address 4**	Payload	FCS

Figure 29: General data frame format.

Acronyms:
Ack Acknowledgment
CSMA/CA Carrier Sense Multiple Access/Collision Avoidance

3.14.3 802.11 Addresses

Use **3/4 addresses** depending on the **to-DS/from-DS** bits of the frame control field

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)

Figure 30: Table with Wifi addresses scenarios.

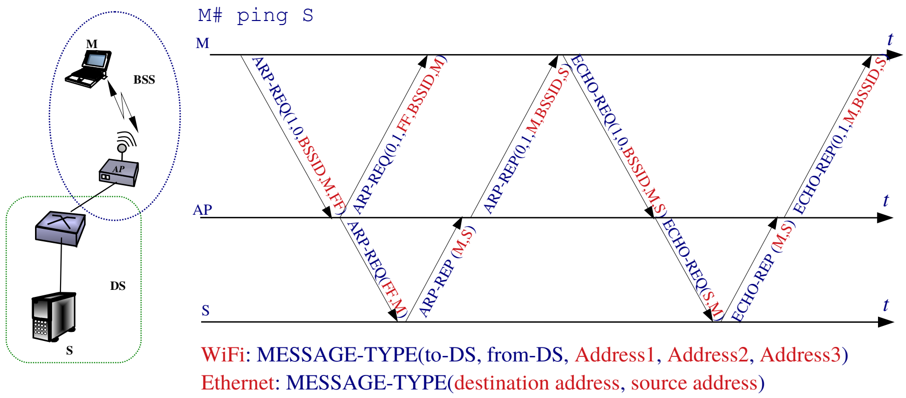


Figure 31: Transmission with an AP in bridge mode.

4 addresses

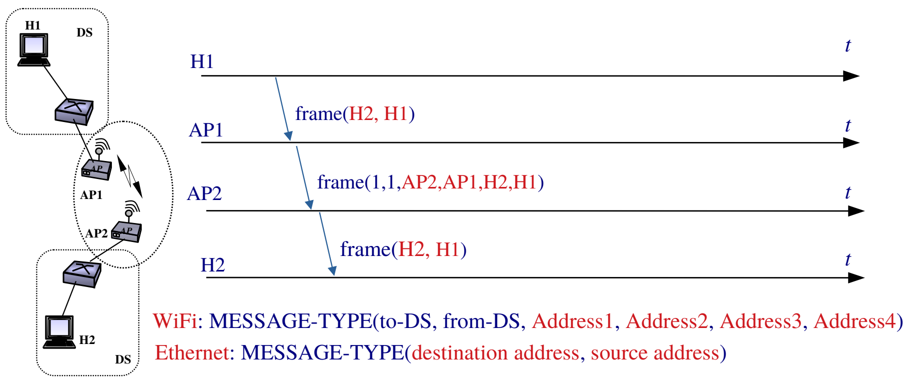


Figure 32: Transmission with APs in WDS mode.

Acronyms:
WDS Wireless Distribution System

3.14.4 Hidden Node Problem

- When **A** transmits to AP, **B** cannot detect the transmission using the carrier sense mechanism
- If **B** transmits, a **collision** will occur at AP
- Solution **802.11 RTS/CTS**

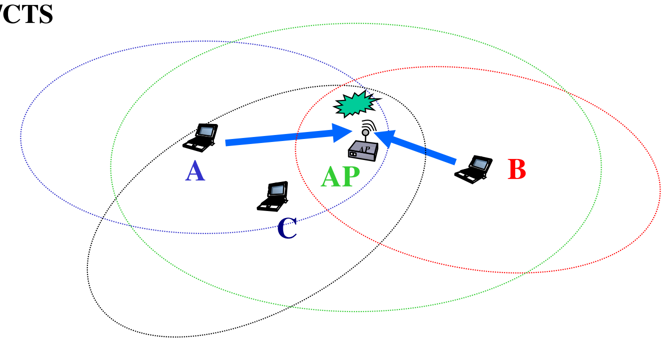


Figure 33: Hidden node problem: Stations A and B are in coverage with the AP, but are hidden from each other.

Acronyms:
RTS Request To Send
CTS Clear To Send

802.11 RTS/CTS

- Upon receiving a RTS/CTS, the station use a **virtual carrier sensing**
- RTS/CTS is only used for unicast Tx

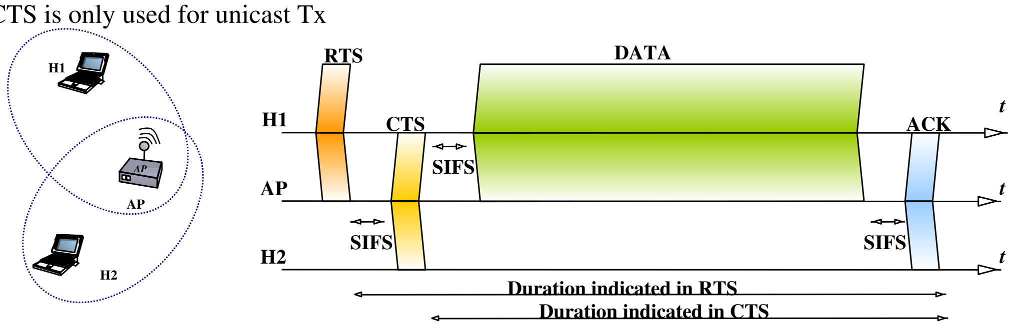


Figure 34: RTS/CTS time diagram.

Acronyms:
SIFS Short Inter Frame Space

3.15 List of Acronyms

AP	Access Point
Ack	Acknowledgment
BSS	Basic Service Set
BSSID	BSS Identifier
CRC	Cyclic Redundancy Check
CSMA	Carrier Sense Multiple Access
CSMA/CA	CSMA/Collision Avoidance
CSMA/CD	CSMA/Collision Detection
CTS	Clear To Send
DS	Distribution System
DSAP	Destination SAP
LAN	Local Area Network
LLC	Logical Link Control
MAC	Medium Access Control
OUI	Organizationally Unique Identifier
PDU	Protocol Data Unit
PSTN	Public Switched Telephone Network
RTS	Request To Send
Rx	Reception
SAP	Service Access Point
SNAP	Subnetwork Access Protocol
SSAP	Source SAP
SSID	Service Set identifier
STP	Spanning Tree Protocol
Tx	Transmission
WAN	Wide Area Network
WDS	Wireless Distribution System