# UNIT 4. LOCAL AREA NETWORKS

## INTRODUCTION

Local networks can be classified by their range:

- Wide Area Network (WAN): have as objective to reach an extensive geographical area and with an unlimited number of stations. Are made to be scalable (e.g., *telephone network*).
- Local Area Network (LAN): they want to interconnect a limited number of stations in a small area, so scalability is not its main objective.

Or by the interconnection strategies:

- Switched network: formed by the interconnection of commutators that direct the information between both nodes that are communicating. Their object is similar to the one from the routers. Their main advantage is scalability due to the easiness to expand the network (just add more commutators). That's why WANs are always switched networks.
- Multi access network: the main handicap of switched networks is that the range escalates alongside its price, which makes them pretty expensive. They are formed with a shared medium so that when the emitting station sends a message, all the possible destination receive it, but all dismiss it except for the expected receiver. This way we save on commutators, but we do need a protocol (Medium Access Control, *MAC*) able handle and organize all the stations. That's why LANs use multi access networks.

## IEEE LAN ARCHITECTURE

IEEE 802.2, is a standard which defined Logical Link Control (*LLC*) as the upper portion of the data link layer of the OSI Model.

| Layer | | | Protocol Data Unit | Function |
|---|---|---|---|---|
| Host Layers | 7 | Application | Data | Protocols from apps that use the network, (i.e., *http, stmp, ftp, telnet*...) |
| | 6 | Presentation | | Provides protocols of data presentation. |
| | 5 | Session | | Manages a session among two apps. |
| | 4 | Transport | Segment, Datagram | Establishes a channel for both apps. |
| Media Layers | 3 | Network | Packet | Guides the PDUs to the correct destination. |
| | 2 | Data Link | Frame | Connection between network level and physical. |
| | 1 | Physical | Bit, Symbol | Defines the physical and electric features. |

OSI divides the Data Link layer in two sublevels:

- Logical Link Control (*LLC*): defines the interface with the upper layer. The standard has two fields; Destination SAP (*DSAP*) and Source SAP (*SSAP*). SAP identifies which upper level has to receive the content of the frame.

- Medium Access Control (*MAC*): is different for each LAN. Its objective is to regulate the access to the shared medium. The data structure (PDU) of MAC level is the frame and this is what will travel across the physical network.

## TYPES OF MAC

In order to design MAC protocols two strategies have been used:

- Token passing: the access is regulated by a token. The station that has the token is the one that can transmit and the rest of stations have to keep silent. After the transmission of a frame is completed, the station passes the token.

- Random: the stations try to transmit and if by accident two transmissions happen simultaneously (collision), they have to wait a random amount of time (backoff time) and try again. I.E., *Ethernet*.

Carrier Sense Multiple Access (*CSMA*) is a random MAC protocol where stations listen the medium before transmission. When the medium is available the station transmits immediately, if it occupied, then the station waits until it becomes free. If there is no confirmation, it means that there's been a collision and the frame will be retransmitted after a random backoff time.

## ETHERNET

Ethernet is a Random MAC protocol. Its frames use two different formats: Ethernet II and IEEE-802.3. Both are compatible and can be used simultaneously. Their frame fields are the following.

ETHERNET II (DIX)

| Preamble (8B) | Dst MAC@ (6B) | Src MAC@ (6B) | Frame Type (2B) | Payload (46-1500B) | CRC (4B) |
|---|---|---|---|---|---|

IEEE 802.3

| Preamble (8B) | Dst MAC@ (6B) | Src MAC@ (6B) | Frame Length (2B) | Payload (46-1500B) | CRC (4B) |
|---|---|---|---|---|---|

In order to make both frame formats compatible, the values of the type field of DIX frames are always higher than 1500. This way, when the driver of a station receives a frame with the value of the type field below 1500, he knows that the frame has the IEEE 802.3 format, otherwise it is the DIX format.

To solve some interoperability problems between both protocols, the standard IEEE defined an extension of LLC named Sub-Network Access Protocol (*SNAP*). When used, following the LLC header, another header is added which contains two fields: Organizationally Unique Identifier (*OUI*, 3B) represents the organism that defines the protocols and Type identifies a specific protocol (2B). It allows to encapsulate TCP/IP protocols over IEEE standard (with OUI=0x000000 and Type=RFC 1700).

The MAC protocol used by Ethernet is known as CSMA with Collision Detection (*CSMA/CD*). It is similar to CSMA, but now the station continuously listens the medium while transmitting the frame and stops transmitting when detects a collision. If there is no collision detected during the transmission it is assumed that no collision has occurred and it's not necessary for the receiver station to send a confirmation.

- Transmission: between frames, the medium doesn't receive signals during a time known as Inter Packet Gap (*IPG*), fixed in 12B. So, if a station wants to transmit consecutive frames, it has to wait an IPG after each transmission.

- Collision: when a collision occurs, the station stops transmitting immediately and a *jam signal* (32b that produce an erroneous CRC) is sent. Then the station waits a backoff time and continues transmitting.

- Backoff time is equal to $n \cdot T_{512}$ where $T_{512}$ is the transmission time of 512b (i.e., 51,2 μs at 10Mbps) and n is a random number between 0 and $2^{min(N,10)}$-1 where N is the number of retransmissions of the same frame ($N \geq 1$).

For example, at 10Mbps if there's a collision the backoff might be equal to 0 or 51,2 μs. If another collision occurs, the backoff might be equal to 0; 51,2; 102,4 or 153,6 μs. If this process is repeated 16 times, the frame is discarded.

The Ethernet standards that use different lines for transmission and reception allow both processes simultaneously. The are multiple modes of operation:

- Full Duplex: when two Ethernet NICs (Network Interface Card) are connected point-to-point, some Ethernet standards allow a full-duplex transmission. NICs deactivate CSMA/CD (no collisions can occur).

- Half Duplex: using CSMA/CD only one NIC can be simultaneously transmitting into the medium.

Ethernet NICs have an auto-negotiation mechanism to detect the full-duplex availability.

There are many physical level Ethernet standards. The following are just a few of them.

| Speed | Common Name | Informal IEEE Name | Formal IEEE Name | Cable Type, Max Length |
|---|---|---|---|---|
| 10 Mbps | Ethernet | 10BASE-T | 802.3 | Copper, 100m |
| 100 Mbps | Fast Ethernet | 100BASE-T | 802.3u | Copper, 100m |
| 1000 Mbps | Gigabit Ethernet | 1000BASE-LX | 802.3z | Fibre, 5000m |
| 1000 Mbps | Gigabit Ethernet | 1000BASE-T | 802.3ab | Copper, 100m |
| 10 Gbps | 10 Gib Ethernet | 10GBASE-T | 802.3an | Copper, 100m |

There are also Ethernet standard with optic fibre, that cover major distances. In the denomination "*XBaseY*", 'X' stands for the transmission speed in Mbps (bitrate), "Base" means that the codification is base band signal (though it can also be Broad (translated band signal)) and 'Y' has multiple meanings (maximum segment distant in hundreds of m, reference to the medium type (T: UTP, F: optic fibre, and others...).

The one more standardized is 10BaseT (is the more economic one). In this standard the stations are connected to a repeater (hub), which decodes the signal received in a port and transmits it with a delay of few bits through all the other ports. All standards use UTP or OF (except 10GBaseCX4 that operates only in full-duplex mode).

- Fast Ethernet (1995). 100BaseTX: UTP-cat 5.

- Gigabit Ethernet (1998). 1000BaseT: UTP-cat 5e.

- 10Gigabit Ethernet (2002). Uses optical fibre.

# ETHERNET SWITCHES

If there are many stations connected simultaneously in a hub, it may be inefficient due to collisions.

With the objective to segment the collision domain of an Ethernet Network in an economic manner (not router) the bridges are created. A bridge is a device with a limited number of ports and each one with its own NIC. The process is as it follows:

- The bridge has a MAC table, so that when a frame is received, the bridge knows through which port it must be sent. But before starting the transmission, the frame is stored in the transmission queue of the corresponding port. So, each port of the bridge is a different collision domain. Whenever a frame is arrives, the bridge checks whether its source address is in the MAC table, and adds it if it is not found. Then checks the destination address, and if it is unknown, duplicates the frame in all transmission queues of the ports, so that the frame will be transmitted through all ports to make sure that it reaches its destination. The entries of the MAC table have a *time-out* that triggers the deletion of the address when it expires.

And then came the switches, which have the same functionality as the bridges but with more ports and a major capability of communicating frames among the ports. It is capable of commutate frames simultaneously between different ports. Each port is a different collision domain and can have distinct bitrates. They may be full-duplex (if only one host is connected) and there can be ports simultaneously in half or full duplex mode. Bitrate can be increased by aggregating several links, which behave as a single one. Stations can only capture traffic of their collision domain, which increases the security.

Thanks to the segmenting of the collision domain, switches can increase the scalability of the LAN. Once the switches have the MAC tables initialized, the direct the frames so that they cross just the necessary links to get to their destination. But when a switch receives a broadcast frame (their objective is to arrive to all stations of the network and their destination address is FF:FF:FF:FF:FF:FF), it is sent through all ports except the one it came from. Due to this, all Ethernet stations interconnected with level 1-2 devices create a “broadcast domain”. The routers do segment the broadcast domain.

Suppose a port with a station that transmits at 100Mbps to another station with a NIC of 10Mbps. The transmission queue of the port configured at 10Mbps will quickly overflow and the switch will start losing frames. That is where the flow control appears. It is an element of the switch which consists of adapting the rate at which the switch receives the frames, and the rate at which the switch can send them. There are two techniques:

- Jabber signal (half duplex): the switch sends a signal into the port which needs to be throttled down, such that CSMA see the medium busy.
- Pause frames (full duplex): the switch sends *special pause frames*. These frames have an integer indicating the number of slow-times (512b) that the NICs receiving the frame must be silent.

But when two stations are receiving frames through the switch at different bitrates, the slow link may trigger the flow control and send pause frames towards the server, causing under-utilization of the switch-server link (which has higher bitrates).

If the hub is the bottleneck for all the active ports, the capacity is equally shared between all ports where frames are transmitted. But 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.

In a network formed by Ethernet switches, when the MAC tables are initialized, the frames go from switch to switch from de source to the destination. The switches do not admit an arbitrary topology (routers do), so when a broadcast frame is sent, each switch will transmit the frame through all ports, and some of these frames will loop indefinitely, which will saturate the network. So even though loop can sometimes come in handy, they are not allowed. To solve this problem there is the standard STP (*Spanning Tree Protocol*), which builds a loop free topology with optimal paths. The ports that do not belong to the STP tree are blocked and discard all incoming frames, so they are not in the initialization process of the MAC tables.

An Ethernet switch constitutes a broadcast domain. Sometimes is convenient due to efficiency and security motives to have servers and hosts related in different broadcast domains, each one identified by a subnetwork. With Virtual LAN (*VLAN*) we can achieve a logical distribution of the broadcast domains that do not belong to the distribution and physical connection of the commutators (switches).

Each switch port belongs to a different VLAN and all hosts connected to that port belong to the VLAN associated. For every VLAN the switch has a different MAC table. If a broadcast frame is received in a port, the switch will just retransmit it through the rest of the ports belonging to the VLAN. So, in order to go from one VLAN to another it is necessary to go through the router. This allows a greater flexibility of the physical placement of the devices, facilitates the network growth. A different STP tree is built in each VLAN.

If a port belongs to several VLANs (maybe all) it is configured as trunk (connection between two switches), so the traffic sent in one VLAN is also sent tot the trunk the VLAN belongs to. A tagging mechanism is used in the trunk to discriminate the traffic from different VLANs. There are two trunking protocols, Inter-Switch Link (*ISL*) and the IEEE-802.1Q standard, which adds 4B between the source address and the Type/Lengh fields. The field Tag Protocol Identifier (*TPID*) has the hex value 0x8100 when the tag has been added to an Ethernet frame, and the field Tag Control Information (*TCI*) contains several fields, the most important is the VLAN ID (12b), which identifies the VLAN.

## WIRELESS LANs

The wireless LANs have various advantages respecting the wired networks. No expenses in the wiring, flexibility in the deployment of the network (the network can be easily installed/uninstalled), the stations can move freely in the network.

But they also have some handicaps. High frequency modulations are needed in order to make possible the transmission through the area. When the signal is propagated though the space it is attenuated and the usable power of the received signal is really weak. The feebleness of the received signal doesn't help to get rid of interferences and noise.

The IEEE-802.11 protocol, also known as Wireless Fidelity (*WiFi*) is one of the most standardized. It uses the frequency bands Industrial, Scientific and Medical (*ISM*). There a various standards at physical level:

| Standard | 802.11 | 802.11b | 802.11a | 802.11g | 802.11n |
|---|---|---|---|---|---|
| Bitrate | 1, 2 Mbps | up to 11Mpbs | up to 54Mbps | up to 54Mbps | up to 600Mbps |
| ISM Band | 2,4 GHz | 2,4 GHz | 5 GHz | 2,4 GHz | 2,4 or 5 GHz |

802.11 has two operating modes:

- Infrastructure: all transmissions have to go through a special station known as Access Point (*AP*). AP sends beacons (special signalization) to make known their presence. The stations have to find and associate with an AP in order to access the WLAN.
- Ad-hoc: all stations access the medium the same way (no Aps).

To reduce to the maximum the number of collisions uses Carrier Sense Multiple Access with Collision Avoidance (*CSMA/CA*), which in contrast to CSMA/CD, always waits a random backoff before starting transmitting and Acks are needed to detect whether a transmission frame collided.

802.11 addresses are designed to be compatible with ethernet. Use non overlapping ranges with ethernet. The frame may have up to 4 addresses, and their meaning 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 format of an 802.11 frame

| Control (2B) | Duration (2B) | Address 1 (6B) | Address 2 (6B) | Address 3 (6B) | Seq-Ctrl (2B) | Address 4 (6B) | Payload (0-2312B) | CRC (4B) |
|---|---|---|---|---|---|---|---|---|

An important characteristic of WLAN is that uses no ISM regulated frequency band, which allows multiple independent WLANs to be inside the same radius of range. So, in order to avoid receiving unpleasant frames from another WLAN a filtering mechanism is needed. To identify stations that belong to different networks, 802.11 defines the known Basic Service Set (*BSS*), identified by a number of 48b named BSS Identifier (*BSSID*). The frames the carry a different BSSID from the one of the NIC are discarded. When a station still hasn't accessed its network and doesn't known the BSSID, it can access using the BSSID broadcast, which coincides with the address 802.11 broadcast (FF:FF:FF:FF:FF:FF).

If an 802.11 network is constituted by a single BSS, then it becomes an Independent BSS (*IBBS*). A BSS can be in infrastructure mode, where each AP forms a different BSS and the BSSID is the address 802.11 of the AP, or in ad-hoc mode (no AP). If a network has more than one BSS, then it is an Extended Service Set (*ESS*) and the part of the network that allows the interconnection of the different BSS is known as Distribution System (*DS*).

In a network with 802.11 and Ethernet, the uniqueness of the address is guaranteed. This allows 802.11 NICs to communicate with Ethernet NICs in a transparent way. But in order to make this possible, the 802.11 header has 4 address fields, the meaning of which depend on the scenario.

| Scenario | Usage | to-DS | from-DS | Address 1 | Address 2 | Address 3 | Address 4 |
|---|---|---|---|---|---|---|---|
| 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 |

In Ad-hoc mode only the STA > STA addressing mode is used. In Infrastructure mode both STA > AP and AP > STA addressing modes are used. AP > AP is only used when the DS is also wireless, this scenario is known as Wireless Distribution System (*WDS*).