Computer Networks (*Redes de Computadores - RCOMP*) – 2021/2022 ***Laboratory Class 01 (PL01 – 3 hours)***	
Subjects Shielded and unshielded twisted pairs copper cables. CAT6 copper patches wiring. Ethernet technology. IPv4 basic addressing. IPv4 connectivity testing with ICMP echo messages. Structured cabling systems. Team project guidelines. **Sprint 1 planning meeting.**	Materials • 10 x RJ45 crimping pliers • 10 x pieces of CAT6 cable • 20 x RJ45 CAT6 male crimping plugs • 2 x Ethernet Switches • 1 x RJ45 CAT6 cable tester • Students' own personal computers

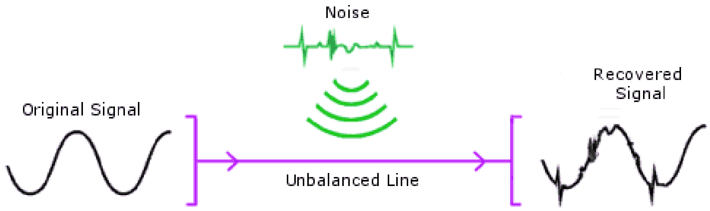
1. Twisted pairs (TP) copper cables

1.1. Transmission of electrical signals through balanced copper pairs.

In an unbalanced transmission, the electrical signal is sent through a single copper line. The receiver measures the signal relative to an absolute reference (ground).

As we already know, one important issue when using electrical signals is external noise. There is a wide range of external sources for electromagnetic noise, the external electromagnetic noise transforms itself into electrical noise in the copper line. This phenomenon is called EMI (*Electro Magnetic Interference*).

Because the receiver measures the signal relative to an absolute reference, what it gets is the signal mixed with a lot of external noise.

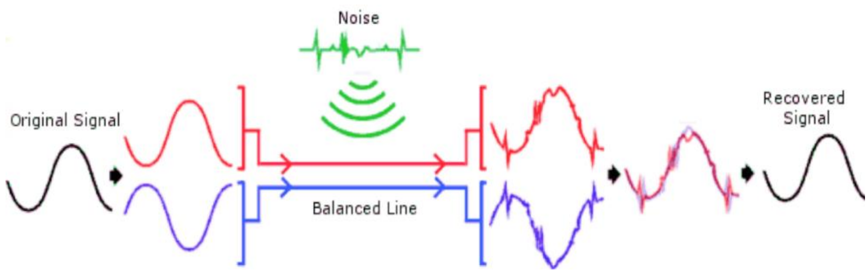


Of course, EMI also works the other way around, the signal being sent through the copper line causes electromagnetic radiation that will be regarded as noise by other nearby electric signals transmission systems.

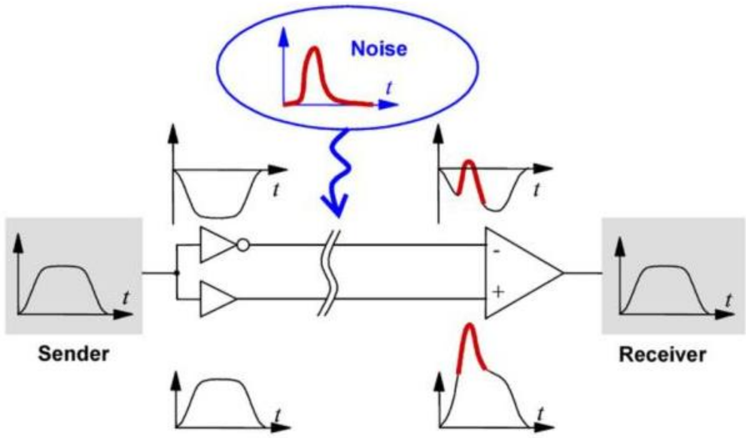
Most current copper transmission systems, including local area networks, use *balanced lines with symmetrical differential transmission*.

Balanced lines differential transmission means two lines (a pair) are used to transmit a single signal, one line holds the signal, and the other line is used as reference. At the receiver the signal is measured as being the difference between the two lines, the big advantage is that external noise will be the same on both lines, and thus it's eliminated when the receiver measures the difference. Although this removes external noise at the receiver, is does nothing to prevent electromagnetic radiation of the transmitted signal.

In *balanced lines with symmetrical differential transmission*, a symmetrical copy of the signal is placed on the second line. Therefore, each line this produce symmetrical electromagnetic radiation cancelling each other. To make the most of this electromagnetic radiation annulation effect, the two lines are twisted on each other, making what is called a *twisted pair*.



The next image shows a key device on the receiver side, it's called a *differential amplifier*, this device has two inputs (+) and (-) and amplifies the difference between them.

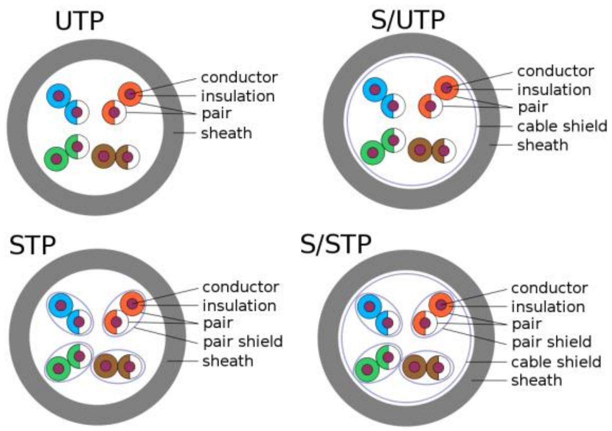


1.2. Shielding

In order to improve external noise and electromagnetic radiation suppression, twisted pair cables may also be shielded. Electric shielding is achieved by surrounding the pairs with an electric conductor material connected to ground, usually an aluminium foil or a copper mesh.

UTP – Unshielded Twisted Pairs

STP – Shielded Twisted Pairs



1.3. CAT5E, CAT6 and CAT7 copper cables

Current structured cabling systems standards require at least the use of category 5E (CAT5E) copper cables, however, category 6 (CAT6) or CAT7 are recommended. All these cables have four twisted pairs, making a total of eight connections.

Each CAT5E (CAT5 Enhanced) twisted pair can cope with signals up to 100 MHz, 1000baseT Ethernet technology can use this type of cable to transmit up to 1 Gbps data rate. CAT6 twisted pairs can cope with up to 250 MHz signals, and CAT6A (CAT6 Augmented) up to 500 MHz, 10GbaseT Ethernet technology uses category 6 cables to transmit up to 10 Gbps data rate.

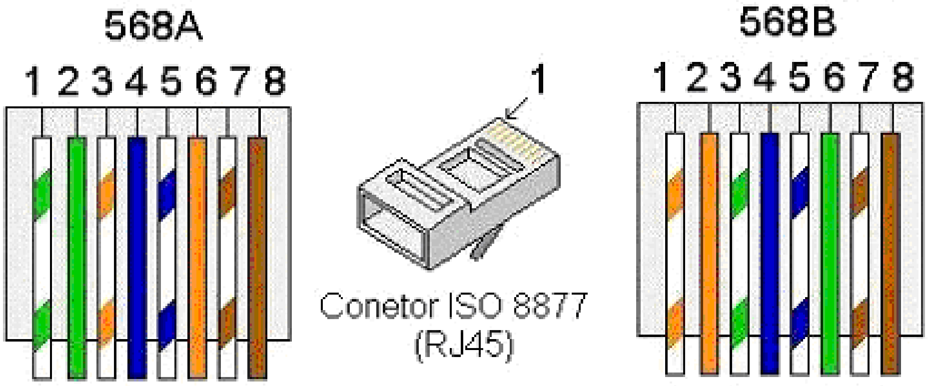
Category 7 copper cables (CAT7) are S/STP and may be used with signals up to 600 MHz.

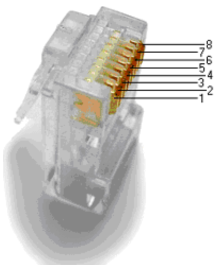
1.4. ISO8877 connectors (RJ45) and pairs' colours

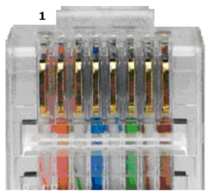
TIA/EIA-568 standards require the described copper cables to be terminated with ISO8877 connectors, they are usually known as RJ45 (Registered Jack) or 8P8C (8 position 8 contact).

RJ45 connectors have eight metallic contacts numbered from 1 to 8 that provide electric connection. In addition, they may have a shielding connection to be used for shielded cables. On the right image, male connectors or plugs are shown, below a female connector or jack also known as socket.

To make assembly easier, each cable pair is identified by a different colour: green, orange, blue and brown. Each pair assignment to connector pins may follow two alternative standards: 568A or 568B.







<u>The purpose of each pair depends upon the upper layer technology using the cable</u>, the cabling infrastructure should be independent of specific technologies and thus in any cabling infrastructure **one standard must be adopted (568A or 568B) and enforced everywhere in the infrastructure**.

1.5. Copper pairs usage (historical background)

During several years there were two major dominant technologies using these cables: 10baseT and 100baseTX, Ethernet at 10 Mbps and 100 Mbps. Both these Ethernet implementations use only two pairs, one for sending data and the other for receiving, thus supporting full-duplex (simultaneous transmission in both directions). The signal is emitted in the pair corresponding to connector pins 1 and 2 (TX pair) and received in the pair corresponding to pins 3 and 6 (RX pair). Thus, only the green and orange pairs were used.

To directly interconnect two 10baseT or 100baseTX nodes through a cable, TX and RX pairs must be swapped. Two types of port connection (MDI - Medium Dependent Interface) were established:

MDI ports	RX/TX pairs not swapped	End nodes ports.
MDI-X ports	RX/TX pairs swapped	Intermediate nodes (hubs and switches) ports.

On those days, any cable connection was required to be made between an MDI port and an MDI-X port, this is guaranteed because intermediate devices have MDI-X ports and end devices have MDI ports. However, to be possible to interconnect intermediate devices, those intermediate devices were also provided with an MDI port, commonly known as uplink port. Frequently it was a shared port (internally a single port with two external connectors, one MDI and other MDI-X), other vendors provided a single port and a small switch to change the port behaviour between MDI and MDI-X.

As last resort, the interconnection of two intermediate devices could also be made between two MDI-X ports by using a specially assembled cable itself swapping the TX and RX pairs, that is called a cross-over cable. A cross-over cable is assembled by using different standards (568A/568B) in each cable end. A cross-over cable would also be required to directly interconnect two end devices MDI ports.

Nowadays, every Ethernet MDI port has the ability to automatically detect and negotiate the pairs to be used, this is called *auto MDI-X*. Also, the current Ethernet technologies make different use for each of the four available pairs. So, **cross-over cables are now historical, and the entire cabling infrastructure should be assembled using the same standard.**

2. Practical activity – mounting a copper patch cable

(Groups of two students)

Patch cables, also called ***patch cords***, are needed to connect active devices to a cabling system. Copper patch cords may be from **0.5 meters up to 5 meters long** and have an RJ45 (ISO8877) male connector (plug) assembled on both ends.

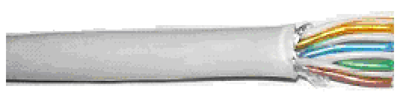
Active devices and cabling systems are provided with RJ45 female connectors (aka **jacks** or **sockets**).

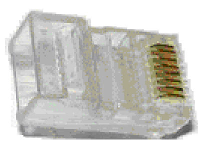
The easiest option is buying a ready to be used patch cord like the one we can see on the right image; they are available with several different lengths. Nevertheless, copper patch cords can be mounted with a suitable **RJ45 crimping plier**.

Before using the plier to crimp the connector to the cable, wires must be prepared. Common RJ45 crimping pliers provide features for external jacket removal and wire cutting.

- The external jacket must be removed to an extent that will allow the handling of individual wires of each pair. However, the external jacket must be inserted into the connector for appropriate crimping, therefore only the appropriate length should be removed.

- **Individual wires jacket removal is not required**.
- All wires must be parallel to each other and in the correct positions for insertion into the connector.
- All wires must fully reach the crimping zone of the connector, if one wire is shorter it will be missed by crimping and no electrical contact will exist.





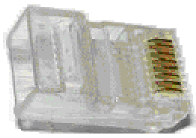
Take some minutes to watch the following video:

https://www.youtube.com/watch?v=noRk8jYAbSg

Students are encouraged to perform the cable end preparation several times before crimping the connector. Crimping is irreversible; if the cable was inadequately prepared the connector will be wasted.

<u>TO AVOID UNNECESSARY CONNECTORS WASTE, CRIMPING SHOULD BE PERFORMED ONLY AFTER INSPECTION BY THE CLASS TEACHER</u>

There are two assembly standards: 568A e 568B. Adopting one or another is irrelevant, however once one is adopted it must be used everywhere in the infrastructure. Therefore, in this activity, **the same standard must be used on both ends of the patch cord**.

1st	
2nd	 
3rd	  right wrong

Use a copper cable tester to check the freshly assembled patch cord. Basic copper cable testers are simple electric continuity testers for each of the eight wire connections and for the shield (if available and connected). Each circuit is tested at a time so any wrong connection or short circuit will be visible.
More sophisticated cable testers are used for cabling certification, they can measure the cable length and signal propagation properties for each pair.

3. Introduction to Ethernet LAN technology

Ethernet is the most widespread technology used over local area twisted pairs copper networks and Local Area Networks (LAN) in general. Several categories of copper cables and optical fibres can be used by Ethernet. Depending on the available physical medium, different data rates can be achieved.

Ethernet technology matches OSI layers one (physical link) and two (logical link), the physical layer is dependent on the transmission medium, however, the logical layer is not. This means different transmission mediums share the same logical link layer, and thus data transmission between nodes attached to different transmission mediums is guaranteed by Ethernet.

Ethernet logical link layer (historically know as MAC – Media Access Control) implements packets transmission, at this layer, packets are usually called **frames**. Ethernet frames are a long burst of bits send through the wire, each will have a destination node address, a source node address, a data type identifier, the data itself (usually up to 1500 bytes) and an error detection code.

Ethernet node addresses are 48 bits numbers used to uniquely identify nodes within the Ethernet network. Ethernet addresses are also known as MAC addresses, physical addresses, or hardware addresses. For human readable representation, the 48 bits are split into six sets of eight bits (octets), each represented in hexadecimal separated by a colon or a hyphen. Examples:

```
1b-23-45-6c-f9-5b        1b:23:45:6c:f9:5b
AA:B3:34:00:08:CA
```

The first half of the address (24 more significant bits) is called OUI (Organizationally Unique Identifier), they are used to identify the device vendor. Each vendor has a unique OUI assigned and is up to the vendor ensuring the remaining 24 bits are unique. So, we can expect there will never be two devices with the same MAC address.

Some ethernet addresses are reserved for special purposes, the most notable is the broadcast address where all 48 bits have the one value:

```
ff-ff-ff-ff-ff-ff        ff:ff:ff:ff:ff:ff
FF-FF-FF-FF-FF-FF        FF:FF:FF:FF:FF:FF
```

When a frame is sent to the broadcast address (the frame's destination address is the broadcast address) all Ethernet intermediate devices will forward it, thus it will reach every node in the network (the broadcast domain).

Ethernet technology may use different physical mediums, each will support some types of Ethernet transmission modes and rates, for instance CAT6 twisted pair copper cables can be used by Ethernet to transmit at 10 Mbps (10baseT), 100 Mbps (100baseTX), 1 Gbps (1000baseT), and up to 10 Gbps (10GbaseT).

When two Ethernet devices are connected through a twisted pair cable, they start a negotiation procedure to settle the transmission mode, including useable data rate and the support for full-duplex transmission.

4. The network layer

Although nowadays almost every local area network uses Ethernet, when information travels through the internet the scenario is different, there is a wide range of diverse transmission technologies.

Therefore, network final applications cannot use Ethernet directly, if they were to do so they could only communicate with other applications connected to the same local Ethernet network.

In other words, globally speaking, the layer two transmission technology is not homogeneous. To work around the layer two diversity one additional layer is required, this is called the network layer or layer three.

The network layer has an abstraction role, it may operate over any existing layer two technology, but it is not dependent on a particular layer two implementation. Thanks to the Internet Protocol (IP) layer three implementation we have now a global communication platform where any node connected to it may send packets to any other node. This is achieved even if the packet is required to travel through several different layer two technologies to reach the destination.

To accomplish this abstraction level the network layer must:

- Define a universal (abstract) packet format. (The IP packet)

- Define a universal (abstract) node addressing scheme. (The IP node addresses)

- Implement devices capable of using different layer two technologies for IP packet transport, and forward IP packets between different layer two technologies. (Routers, aka gateways)

5. Introduction to basic IPv4 addressing

Currently two IP versions coexist over the internet: IPv4 and IPv6. Although a gradual transition from version four to version six is in progress, version four is still most widely used. Both IPv4 and IPv6 define a universal packet format and addressing scheme, the most notorious difference is that IPv4 uses 32 bits node addresses while IPv6 uses 128 bits node addresses.

IPv4 node addresses are 32 bits numbers used to uniquely identify a node, for human representation they are split into four eight bits sets (octets) represented in decimal notation and separated by a dot. This is known as the **dot-decimal notation**. For instance: **192.168.10.5**.

Because the network layer must handle with different layer two networks (and route packets between them) beyond the node addresses layer three also defines network addresses.

Network addresses make routing easier, to operate routers are not required to know every node location, knowing every network location is enough.

In IPv4 and IPv6 the network address is integrated in the node address; the most significant bits of the node address are in fact the network address. The number of bits used to represent the network address (and accordingly the number of bits left no identify the node address) is known as **the network prefix length** and is settled by the network mask.

Nodes belong to the same network if their node addresses have the same network prefix (same bits within the network prefix length), otherwise, they belong to different networks. In the former case, direct communication is possible, in the latter case, the use of a router will be required to transfer packets between different networks.

Of course, if two nodes belong to the same network, then the bits left to identify each node must be different because node addresses must be unique. When two nodes belong to the same network, they expect to be able to communicate directly, so they should be connected to the same layer two network (LAN).

Two nodes may be connected to the same layer two network (LAN), however if they belong to different layer three networks (different network prefixes) they will never even try direct communication.

Network masks (network prefix lengths) define the number of most significant bits being used to identify the network a node belongs to. For the purpose of routing a packet, the node address itself is insufficient, a network mask must be also added.

One common prefix length is 24 bits, this means the first three octets are for network identification (network prefix) and only the rightmost octet identifies the node within that network, this is also called a C class IPv4 network. The traditional way to specify a network mask is through a dot-decimal representation of an address where network bits have value one, and node bits have value zero. Thus, for a C class IPv4 network the network mask is **255.255.255.0**.

The maximum number of nodes a C class IPv4 network can hold is 254, this is because the first and last possible node addresses in each IPv4 network are always reserved. The first is used to represent the network address, the last is used for the purpose of broadcasting (sending to all nodes in that network).

Take for instance node address **192.168.10.0** with the network mask **255.255.255.0**:

- This defines a C class IPv4 network, it can also be represented as **192.168.10.0/24** (/24 stands for a 24 bits prefix length).

- There are 254 valid node addresses on this network, from **192.168.10.1** up to **192.168.10.254**

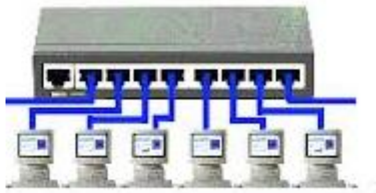
- Address **192.168.10.0** is reserved because it represents the network address.

- Address **192.168.10.255** is the network broadcast address, when an IP packet sent to this address, a packet copy is expected to be received by all nodes that belong to this network.

Each network address must be unique, over the internet (public addresses) this is enforced by IANA (Internet Assigned Numbers Authority). Once a network address is assigned to an organization is up to the local network administrators assigning unique node addresses within the network.

Some network addresses are reserved for private local use and ignored by the internet; they are convenient for local testing purposes. Among others, there are 255 C class IPv4 private networks, from 192.168.0.0/24 up to 192.168.255.0/24.

6. Practical activity – setting up a private IPv4 network



For this activity the class is divided into two groups of students, for each group an Ethernet switch is provided. **Students will be using their own personal computers to perform this activity.** Depending on the number of available personal computers, the class may be reduced to a single group.

First create the layer two LAN. Use the assembled patch cord (previously tested) to connect a personal computer to the switch.

Both the switch and the personal computer ports are auto MDI-X, so, after negotiation the link led (usually green) should be on at both sides.

The link led means everything is ok at layer one, to perform further testing of real data transmission we are going to use the **ping** test command. The ping command sends an **ICMP echo request** and waits for an **ICMP echo reply**, in other words it performs a **round-trip communication test**.

If node A successfully "pings" node B, this means the packets sent by node A are being received by node B, and also, that packets sent by node B are being received by node A. If either fails, the ping test will fail.

ICMP (*Internet Control Message Protocol*) runs over IP, so we must first setup an IPv4 network over the Ethernet network we have already operating.

ping command
ICMP
IPv4
Ethernet

Now test how IPv4 operates:

1 – Setup your own personal computer Ethernet interface to use an IPv4 node address belonging to the 192.168.100.0/24 (255.255.255.0 mask) private network. The node part of the address must be different for each connected node. Valid node addresses are 192.168.100.1, 192.168.100.2, up to 192.168.100.254.

2 – Test the IPv4 network by using the command line ping command. For each personal computer connected to the same switch use the commands:

ping 192.168.100.1

ping 192.168.100.2

…

ping 192.168.100.254

Important: personal computer firewalls may block incoming ICMP echo requests, for a successful test the target personal computer may be required to temporarily disable the firewall.

3 – For roughly half the personal computers connected to each switch change the network address to be **192.168.101.0/24**, you may keep the node number unchanged.

4 – Now let's test again, we will notice nodes belonging to different IPv4 networks are not able to communicate with each other. Nodes with addresses started by 192.168.100 are not able to communicate with nodes with addresses started by 192.168.101. Despite being connected to the same layer two network (switch).

However, it all depends on the network mask

5 – For every node connected to each switch lets change the network mask to 16 bits prefix length (255.255.0.0), keeping the address unchanged. This will make all nodes belong to network 192.168.0.0/16. Valid nodes on network 192.168.0.0/16 go from 192.168.0.1 up to 192.168.255.254, so they include both network 192.168.100.0/24 and network 192.168.101.0/24.

6 – Test again, now nodes using addresses started by 192.168.100 can communicate with nodes using addresses started by 192.168.101, with the 255.255.0.0 mask they all belong to the same IPv4 network.

7. Structured cabling

Unlike active devices, cabling systems replacement is an overwhelming and costly task, therefore, cabling systems must be planned to be usable for a reasonable time.

A cabling system design can't merely meet the current requirements for present usage and network devices, it must also be able to support technological upgrades and future usage requirements.

To achieve these goals two principles must be applied:

- Respect the structured cabling standards (because new technologies are developed based on for current cabling standards).

- Over dimensioning in crucial points, like backbones.

A structured cabling system is a hierarchical set of cables interconnection points known as cross-connects or distributors.

The structured cabling system is made of **passive equipment only: cables, connectors, and suitable mechanical supports.**

Each cable termination is provided with the appropriate connector, in the case of copper cables, RJ45 (ISO8877) sockets. Active equipment can later be connected to the cabling system through **patch cords**.

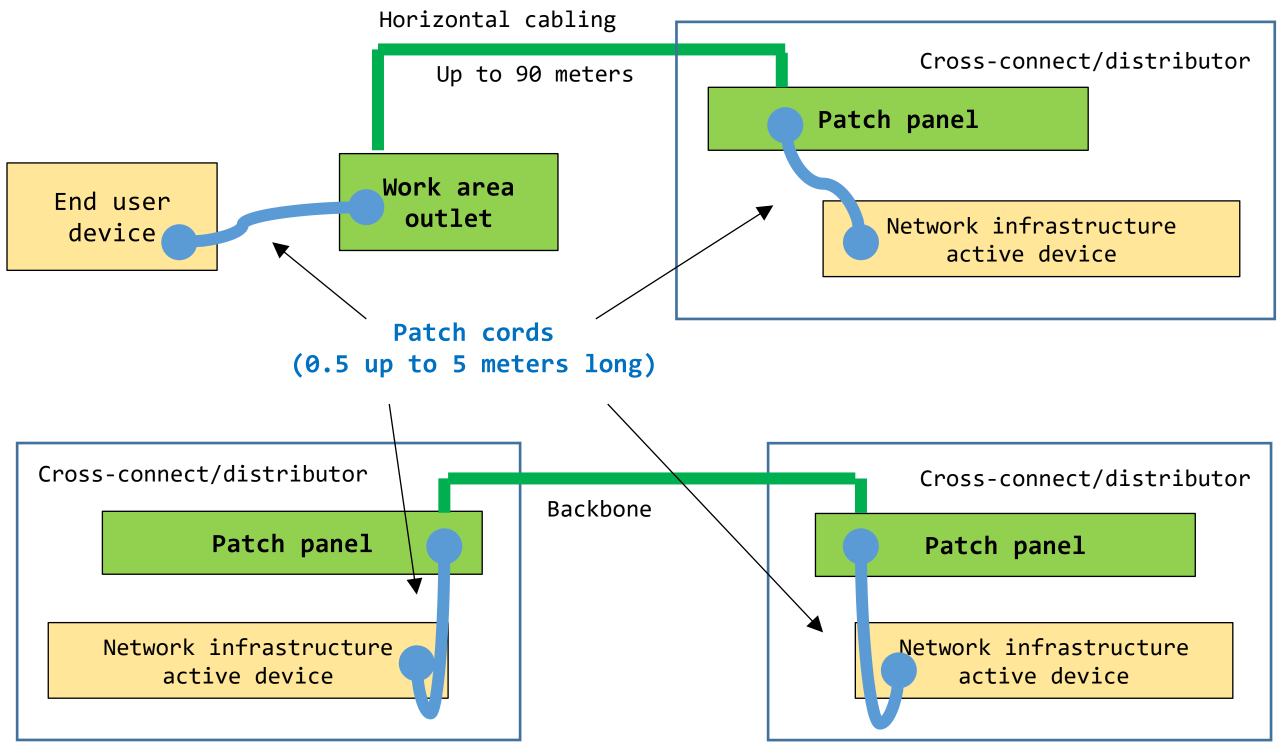
Backbone cable termination points (cross-connects/distributors) are housed in telecommunication enclosures.

Telecommunication enclosures or cabinets use a standard mechanical format known as **19-inch rack**. The mechanical specifications of most hardware meet this format and can be stored inside these cabinets (image on the right).

Under the point of view of structured cabling one key component is the patch panel, it's merely a high density set of network connectors, every backbone cable terminates at a patch panel. All patch panels are housed in telecommunication enclosures. The left image shows a copper patch panel made of a set of RJ45 sockets.

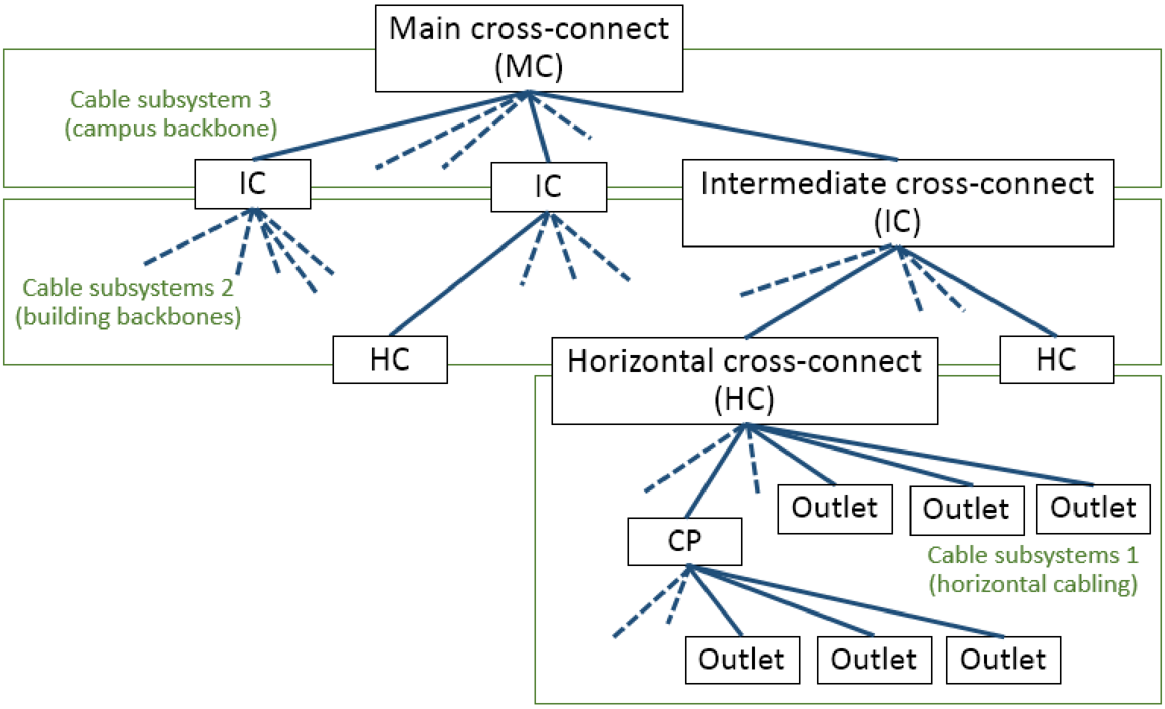
At the lower hierarchical level of the structured cabling system (horizontal cabling) each cable ends in a user network socket (outlet). The right image shows a copper network outlet (RJ45).

Every cable is ended by either two patch panels, one on each edge, or, for horizontal cabling, a patch panel on one edge and a work area outlet on the other edge. Both scenarios are shown in the images below.



Patch cords (from half a meter long, up to 5 meters long) are used to connect active devices to the cabling system. Within the same distributor, active devices can be directly interconnected by a patch cord, elsewhere, they are interconnected as shown below.

The next image represents the general hierarchy of a standard structured cabling system.



The campus backbone makes sense when there are several buildings to be covered, in such a scenario, in each building there will be an intermediate cross-connect (IC).

The building backbone connects the intermediate cross-connect to each horizontal cross-connect (usually one per floor). The horizontal cross-connect is the starting point for the horizontal cabling leading to outlets for users. In places with very high outlets density, a Consolidation Point (CP) can be created.

Telecommunication enclosures capacity is measured in U rack units (1U represents 1.75 inches/44.45 mm in height), typical telecommunication enclosures capacity goes from 6U up to 42U. A typical patch panel or active device requires 1U or 2U.

All sorts of required active equipment like hubs, switches, routers, servers, and uninterruptable power supplies (UPS) are also housed inside telecommunication enclosures at cross-connects. Telecommunication enclosures dimensioning must take all that into account.

8. Project enrolment

- Student's analysis of the documents available at Moodle.
- Teacher's briefing - comments and clarifications.
- Within the lab class, a unique one-digit number is assigned by the teacher to each team.
- Each team creates a BITBUCKET repository (fork of the provided template).
- Teams assure the repository is private and that all team members have the required write access permissions granted. The class teacher must have read access.
- Teams edit the project's **README.md** file and insert correct membership information.
- All team members can now clone the repository to their personal workstations.

9. Project - Sprint 1 development guidelines

The best strategy for a structured cabling project development is **bottom-up**, this means starting at the delivery point, the <u>network outlets</u>.

Under this bottom-up approach, steps are:

1st – Rooms area measurement and a resulting standard number of network outlets

On this specific project, areas are to be estimated from the in-scale provided plans (accuracy is not a key factor in this sprint assessment). Specific project requirements (client needs) must be taken into account. Some rooms or locals may require no outlets, others may require an abnormally high number of outlets.

2nd – Pinpoint outlets positions over the provided floor plans

Distributing the previously calculated number of outlets inside a room is mostly a common-sense issue, they are supposed to cover the whole area. Network outlets, required at special locations (e.g., access-points) can't be forgotten.

3rd – Decide cross-connects locations

Concerning cross-connects housing rooms, if not described in the project requirements, they should be negotiated and agreed with the client/owner. As far as possible cross-connects housing rooms should be out of public reach, they may be dedicated rooms or shared with other usages like services storage.

Keeping the bottom-up approach, we first handle the horizontal cross-connects. Desirably a horizontal cross-connect location should be central to served outlets, no outlet can distance more than 80 meters in a straight line, also cable length cannot be above 90 meters. If required consolidation points may be created.

A cross-connect for each floor is not mandatory, for a very low number of outlets, a single cross-connect can serve more than one floor.

Once horizontal cross-connects are placed, intermediate cross-connects can be handled, one for each building is required. The housing room and telecommunication enclosure for the intermediate cross-connect can be shared with the horizontal cross-connect for that same floor.

Finally, the main cross-connect is to be housed in some building, likewise, the housing room and telecommunication enclosure can be shared with that building's intermediate cross-connect.

Of course, all cross-connects positioning must also take in account pre-existing cable passing points and pathways.

4th – Define cable pathways and cable types

At this stage, all outlets and cross-connects are already placed on schematic plans. The next step is setting pathways to interconnect then and connect horizontal cross-connects to outlets. Again, remember each horizontal cable length cannot go beyond 90 meters.

Once defined, pathways must also be represented on plans, either together with outlets and cross-connects or in separate plans.

Redundant backbone cable connections are desirable, they provide fault-tolerance (failover) and can also be used to increase the bandwidth (network load balancing). As far as there are redundant cables, these features may be later enabled at layer two switches (Spanning Tree Protocol and Link Aggregation Control Protocol) or at layer three routers (Dynamic Routing Protocols).

Under the fault-tolerance point of view, redundant cable connections ought to follow different pathways, this ensures a local disaster is less likely to disrupt all cables.

5th – Select cable types

All copper cables should be at least CAT6, they are limited to up to 90 meters long, for longer cables optical fibre must be used.

On horizontal cabling, the use of optical fibre is for now somewhat unpopular because typical end-user devices lack an optical network interface, thus, transceivers would be required to connect optical outlets to most workstations.

On backbones cabling, the scenario is rather different, even if the optical fibre is not imposed due to the cable length, it should always be enforced. Optical fibre grants higher bandwidth and better compatibility with future layer two technologies.

Mind that, depending on the selected cable types, different types of patch panels, outlets, and patch cords are required.

6th – Structured cabling hardware inventory

We already know the total number of outlets. Achieving a good estimate of total cables lengths required is a heavy task, special for horizontal cabling. Some common-sense approximations can be used:

- When a high number of cables share the same segment of a pathway, measure the segment pathway length and multiply by the number of cables.
- When a high number of cables irradiates from the same point, we can estimate the average cable length and multiply by the number of cables. This will be accurate if the cables length distribution is symmetrical. For instance, we can estimate the average cable length based on the two longest cables and two shortest cables.

Each cable reaching a cross-connect it attached to an appropriate type (copper or fibre) patch panel, the number of patch panels needed at each cross-connect depends on the number of connections supported by each.

Typical copper patch panels have 24 or 48 connections, taking 1U or 2U respectively, fibre patch panels are more vendor specific. Patch panel models must be selected, and conformingly, the number of patch panels required at each cross-connect is determined.

Layer two hardware and other active equipment are not part of structured cabling project; however, they impact on telecommunications enclosures dimensioning, which are part of the project.

Roughly, the space required for layer two switching hardware is the same amount required for corresponding patch panels. Because structured cabling infrastructure is supposed to bear future hardware upgrades and additions, an extra 100% over-dimensioning should be applied.

In engineering dimensioning, when some value is reached through calculations, then the commercially available solutions that supports that value must be selected.

Examples:

- If the telecommunications enclosure is housing a single 1U patch panel, then we add another 1U for the expected corresponding switch, making 2U, and an additional 100% over dimensioning, this will make 4U total. Commercially available telecommunications enclosures start at 6U, so we will use one of those.

- If the telecommunications enclosure is housing 2U of patch panels, then we add another 2U for the expected corresponding switches, making 4U, and an additional 100% over dimensioning, this will make 8U. Commercially available size above 6U is usually 12U, so we will use one.

On the other hand, telecommunications enclosure dimensioning is not that critical. If required, as far as there is physical space available, an additional telecommunications enclosure can be mounted side-by-side with existing ones.

10. Important: please, install in advance for the next week

Starting in next week laboratory class the **Cisco Packet Tracer** networks simulation tool is going to be used in this course.

Even though **Cisco Packet Tracer** is already installed in the workstations available in DEI laboratories, many students may rather have it installed in their laptops, it's not acceptable that such software installation activities are undertaken in the laboratory class itself.

For the next week laboratory class, it's expected that students will have Cisco Packet Tracer installed and ready to be used.

To install **Cisco Packet Tracer** on your personal computer, go to Cisco Networking Academy site and enrol yourself in a free Packet Tracer course:

`https://www.netacad.com/courses/packet-tracer`