Computer Networks *(Redes de Computadores - RCOMP)* – 2025/2026

Laboratory Class 01 (PL01 – 2.5 hours)

Cisco Packet Tracer tool installation. Project 1 enrolment. Project 1/Sprint 1 - structured cabling systems – development steps. Introduction to Ethernet LAN technology. Introduction to basic IPv4 addressing. ICMP – IP connectivity testing. Packet Tracer practice – shared medium networks and packet-switch networks.

1. Cisco Packet Tracer installation

In the laboratory classes we are going to use a free network simulator from Cisco known as Cisco Packet Tracer, and we are going to need it installed for today's class. The Cisco Packet Tracer tool is free, but you are required to enrol yourself in one of the free courses available at the Cisco Networking Academy.

Proceed with the installation of the **Cisco Packet Tracer** tool on your personal computer.

Go to Cisco Networking Academy site and enrol yourself in a free Cisco Packet Tracer course:

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

(proceed to the next topic while continuing with the installation)

2. First project

The first project of the RCOMP course will encompass the first three quarters of the course and is organized in three sprints, the first sprint starts in today's class.

For the first project of the RCOMP course, **teams of three or four students** must be formed. Because the first project is not linked to other courses, the only requirement is that all team members must belong to the same RCOMP laboratory class.

2.1. 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 the repository; there is a template available.
- 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.

The first sprint of the project is about planning a network cabling infrastructure for a number of buildings.

2.2. Sprint 1 - 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 the current cabling standards).

- Over dimensioning in crucial points, remarkably in backbones.

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

In Figure 1 we can see how cables are spread from irradiation points known as **cross-connects**.

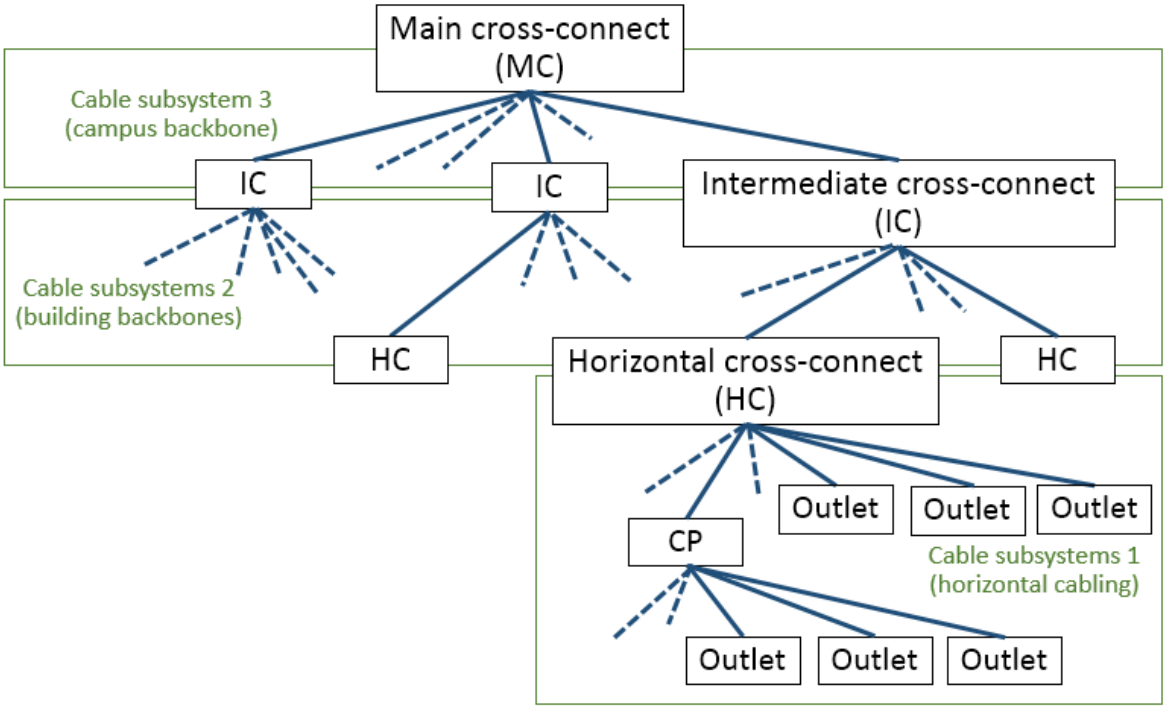

Figure 1- The structured cabling hierarchy

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.

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 (Figure 2) use a standard mechanical format known as **19-inch rack**. The mechanical specification of most networking hardware meets this format and can be stored inside these cabinets.

Figure 2 - Telecommunications enclosure

Figure 3- Copper patch panel

Under the point of view of structured cabling one key component is the patch panel, it's just a high density set of network connectors, every backbone cable terminates at a patch panel. All patch panels are housed in telecommunication enclosures. The Figure 3 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 Figure 4 shows a copper network outlet (RJ45).

Figure 4- Copper network outlet

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 Figure 5.

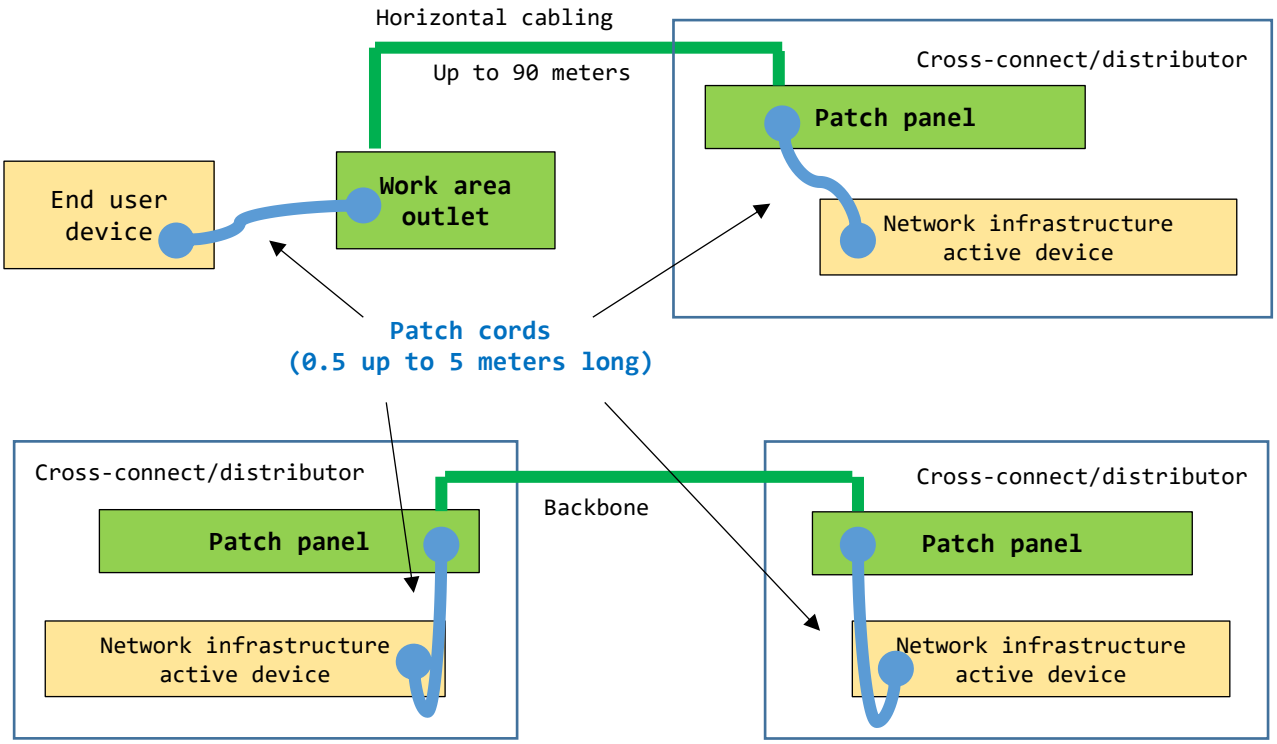

Figure 5- Connecting active equipment to the structured cabling system

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.

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.

2.3. Sprint 1 – development steps

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

Under this bottom-up approach, the 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 position 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 CAT7, 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.

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 CAT7 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 (Local Area Networking) uses Ethernet, however, when the information travels to longer distances (WAN – Wide Area Networking) the scenario is different, there is a wide range of different transmission technologies for WAN.

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

When it comes to global communications, the layer two transmission technology is not homogeneous, therefore an 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 any particular layer two implementation. It's thanks to the Internet Protocol (IP) layer three implementation that we have the Internet, a global communication platform where any node may send packets to any other node. This is achieved even when the IP packet is required to travel through several different layer two technologies to reach the destination.

To accomplish this layer 2 abstraction, 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, these are the routers, aka gateways.

4.1. 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 routing a packet, the node address itself is insufficient, a network mask must be also included.

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**
- The **192.168.10.0** address is reserved because it represents the network address.
- The **192.168.10.255** address is the network broadcast address, when an IP packet sent to this address, a packet copy is expected to be delivered to every node that belongs to the 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.

4.2. ICMP – IP connectivity testing

The IP protocol works together with some auxiliary protocol, one of them is the Internet Control Message Protocol (ICPM).

ICMP is used for error messages, for instance when the network is, for some reason, unable to deliver an IP packet at its destination address, then an **ICMP Destination Unreachable** message is sent to the source address of the packet.

ICMP is also used for a simple connectivity testing, often known as the **ping test**. This test consists of sending an **ICMP Echo Request** message to a target IP node, and then wait for an **ICMP Echo Reply** message, 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.

It's an effective test because every IP node is required to implement the ICMP protocol and respond to **ICMP Echo Requests**.

Notice however that often firewalls block ICMP traffic.

5. The Cisco Packet Tracer network simulation tool

Cisco Packet Tracer is an extensive network configuration simulation tool used at Cisco Networking Academy courses. With Cisco Packet Tracer students can create complex network layouts by simply dragging and dropping network devices at then interconnect them using different appropriate cable types.

Although a simulator, it achieves a working environment very close to real devices. Beginners may manage network devices configuration using friendly forms made available by Packet Tracer. Advanced users may also manage network devices at command-line interface (CLI) the exact same way they would do with real devices. Figure 6 shows the main window of Packet Tracer, at the bottom, on the left side, it is possible to select different devices and cable types. Once devices are connected, and configured, Packet Tracer may be run in either real-time or simulation mode.

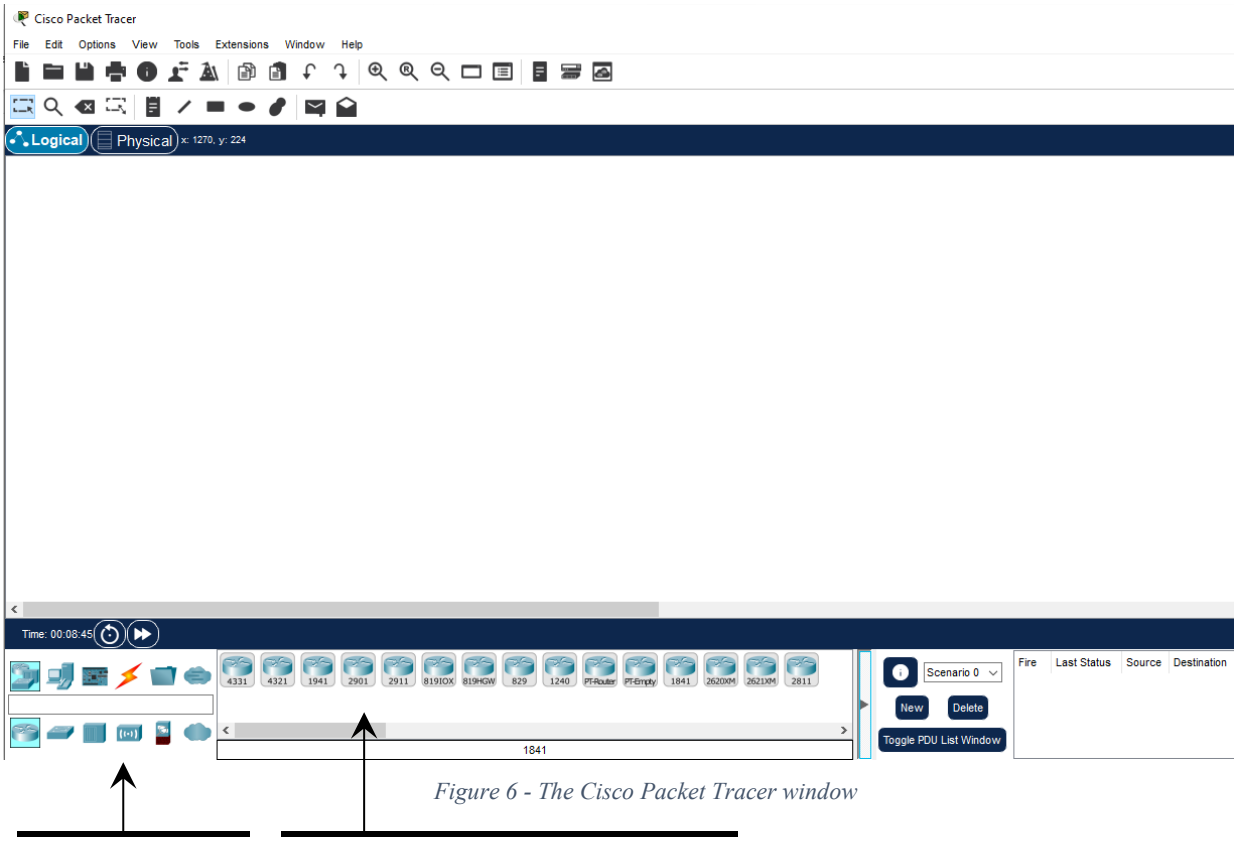

Figure 6 - The Cisco Packet Tracer window

1st Select the hardware type: router, hub, switch, cable …

2nd Select the model or cable type.

In simulation mode the user can see and follow, step by step, individual network packets traveling around the created layout.

Notice that in Packet Tracer, network packets are named as **Protocol Data Units (PDU)**, this follows the OSI (Open Systems Interconnection) standards.

6. Ethernet over shared transmission medium

Ethernet was first designed to use a shared transmission medium, on a shared transmission medium, every signal sent to the medium reaches every connected node. It's up to each node to check if the information is intended to it, otherwise, it should be discarded. Shared medium networks are also sometimes referred to as broadcast networks.

First Ethernet networks used a bus topology (Figure 7), they were made of a single cable shared among several connected nodes.

Several issues arise from shared medium networks, to start with, if two nodes send a signal at the same time, the signals get mixed and become useless, this is called a **collision**.

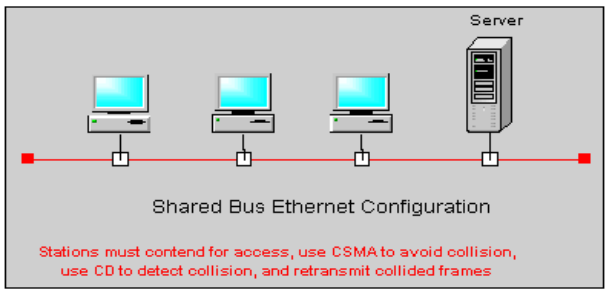

Figure 7- Ethernet shared bus

Even if collisions could be avoided, the medium would never be totally available to a node as it may be busy with another node's signal. The effective sending data rate available to a node is, therefore, the medium's nominal data rate divided by the number of active nodes.

Another issue is security. There is no privacy over transmitted data because every node receives it. It´s up to the good will of each node not looking at data that is not intended to it.

Ethernet approach to collisions is trying to avoid them, and when they happen, reduce the impact as far as possible.

For this purpose, the Ethernet layer called MAC (Medium Access Control) implements the CSMA/CD procedure, in simple words:

When a node wants to send, first it must check if the medium is idle (no signal/carrier). If the medium is idle, it may start sending, otherwise, it waits a random period of time and checks again. This part of the procedure is called CSMA (Carrier Sense Multiple Access).

When a node is sending, it must also be listening to what's going on (LWT – Listen While Talk). Listening allows the node to detect if a collision happens (CD – Collision Detection), if so, it immediately stops sending data and instead sends a special signal called JAM. The JAM notifies every node on the network that a collision has just happened, and thus data that was being sent is invalid and to be discarded.

The collision detection's role is reducing the time during which the transmission medium is unusable due to the collision, without it, the medium would be unusable until the emitter node finishes sending the frame, which may by rather long depending on the frame size.

Shared transmission medium networks with CSMA/CD become highly ineffective on heavy load, if many nodes are trying to send frames the transmission medium will be always busy and collisions rate increases to a point at which the network becomes almost unusable.

Ethernet networks would not have survived if they kept using CSMA/CD. One first improvement was a topology change from **bus to star**, this requires active hub devices capable of forwarding signals between multiple cable connections. In a star topology every node has a dedicated physical connection to a hub, moreover, each cable may support full-duplex transmission (two copper pairs or two optical fibres).

The star topology (Figure 8) introduces all the basic requirements to make collisions impossible, and thus, abandon CSMA/CD.

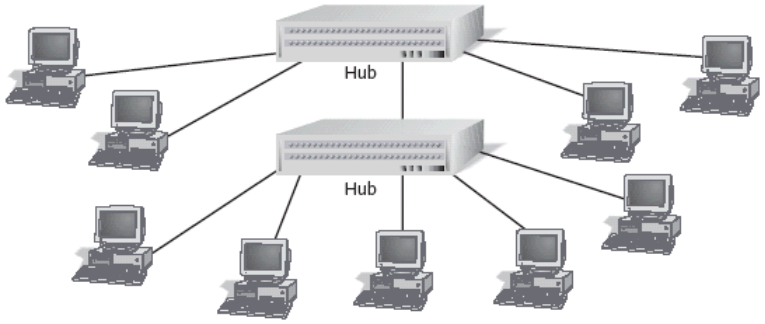

Figure 8- Ethernet star topology

The start topology by itself does not guarantee CSMA/CD can be disabled, all depends on the network intermediate devices operation mode.

HUB (repeating HUB) – this is a simple signal amplifier, when a signal is received on one port it's copied and emitted on all ports. This is a bus equivalent, often called "bus in a box" or "collapsed backbone", collisions happen as before, and thus, CSMA/CD is still required.

Network Switch – although externally similar to a hub, it works with frames (at layer two), not signals (at layer one). A switch can receive at the same time frames on every port, and additionally, at the same

time send frames on all ports. In other words, sending or receiving in any port is independent of sending or receiving in other ports. A switch is also capable of temporarily storing frames in memory for later retransmission. **These features turn collisions impossible, and CSMA/CD becomes unnecessary**. Another feature of a switch (from where the name comes), is the ability to perform frame switching. By registering each received frame's **source address** in the MAC table, a switch learns in which port each node is available. Later, when analysing a received frame´s **destination address**, the MAC table is checked, and the frame is emitted only to the port where that node is available.

Switching has immensely boosted Ethernet networks performance. Nowadays, every Ethernet network is a frame switching network and not a shared transmission medium network.
Yet, some parts of the network infrastructure may still use repeating hubs, those areas are called **collision domains** because collisions may still occur there and, therefore, CSMA/CD is still required.

7. Practical activity – shared transmission medium

Use the Cisco Packet Tracer tool to create the network layout with two **Ethernet repeating hubs** and some end nodes shown in Figure 9.

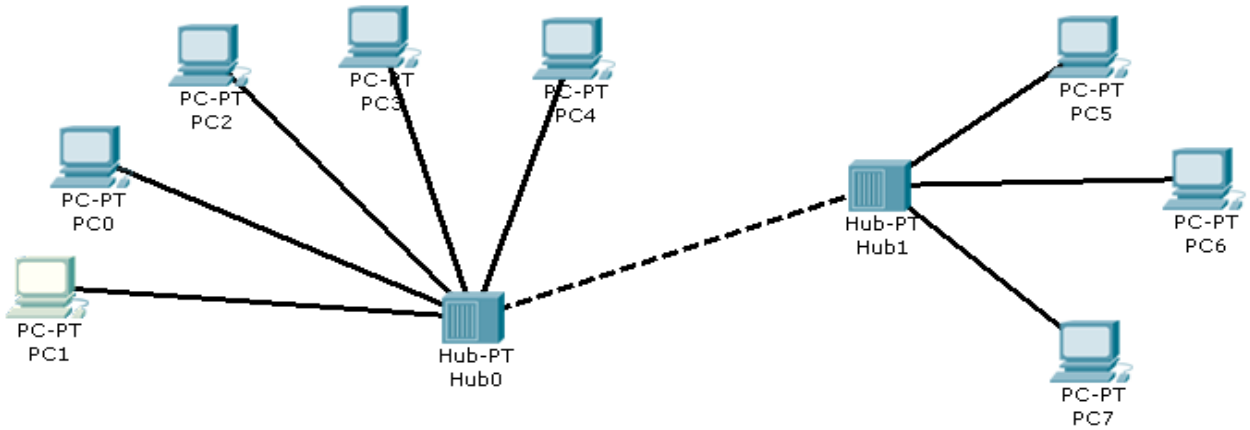

Figure 9 - Network layout with two repeating hubs

Warning: in Packet Tracer devices, copper ports are not auto MDI-X. Thus, to interconnect two intermediate layer two devices (e.g., hubs or switches) a cross-over cable is required, represented in the Packet Tracer layout by a **dashed line.**

7.1. Set IPv4 node addresses for end nodes PC1 and PC7

We will be using the **192.168.27.0/24** (255.255.255.0 mask) C class private network address.

- Assign to PC1 the first valid node address on the provided network.

- Assign to PC7 the last valid node address on the provided network.

7.2. Test IPv4 connectivity

The easiest way to test IPv4 connectivity is by sending ICMP echo requests and waiting for a reply from the target node (this is called the **ping test**). ICMP runs over IP, because we have already setup IPv4 on nodes PC1 and PC7 this test can now be performed between those two nodes.

We want to see things happening, so first switch Packet Tracer to **simulation mode**., on the right side at the bottom of the Packet Tracer window (Figure 10).

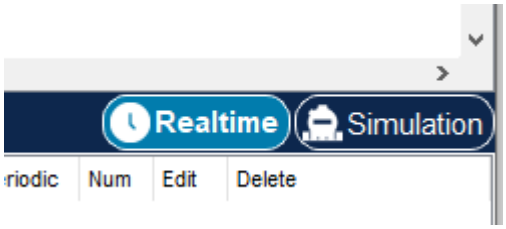

Figure 10- Switching between Realtime and Simulation

Use the **Add Simple PDU** button (Figure 11) to send an ICMP echo request from PC1 to PC7. The Add Simple PDU tool, performs a simple ping test. After selecting the tool, click on the node that will be sending the ICMP echo request and next on the node the request will be send to.

You can run the simulation step by step using **Capture/Forward** or **Auto Capture/Forward**.

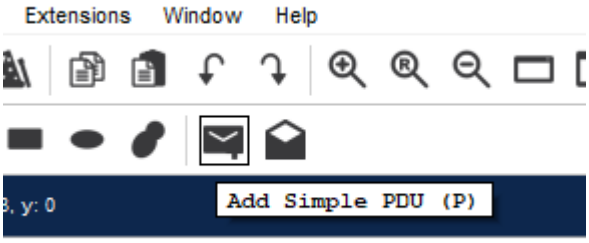

Figure 11- The Add Simple PDU button (closed envelop)

Watch closely what is happening.

Repeat the test now from PC7 to PC1.

Question: is this a shared medium network or a packet-switched network?

7.3. Collisions

Erase the previously created PDUs (NEW button), again in simulation mode, before pressing **Capture/Forward**, add two ping tests, one from PC1 to PC7 and another from PC7 to PC1.

Now start the simulation by pressing **Capture/Forward**.

As we can see the network fails because a collision happens, **definitely this is a shared medium network** that cannot cope with traffic from more than one node at a time.

7.4. Messing with IPv4 addresses and network masks

Set IPv4 node addresses for end nodes PC0, PC4 and PC6.

We will now use the 192.168.85.0/24 (255.255.255.0 mask) C class private network address.

- Assign to PC0 the first valid node address on network 192.168.85.0/24.

- Assign to PC4 the second valid node address on network 192.168.85.0/24.

- Assign to PC6 the third valid node address on network 192.168.85.0/24.

Now let us ping, we may now operate in real-time mode. One at a time, send ICMP echo requests between all five nodes with assigned IP addresses (PC0, PC1, PC4, PC6 and PC7).

Despite all nodes being connected to the same Ethernet network, they are not all able to communicate with each other's.

Why is this happening?

In each of the five nodes, change the network prefix to 16 bits (255.255.0.0 mask), keeping the node addresses unchanged.

Test again ICMP echo requests between PC0, PC1, PC4, PC6, and PC7. **Now it works. Why?**

Changing the network mask has a major effect, now all nodes belong to the same IPv4 network: 192.168.0.0/16
Before there were two different IPv4 networks: 192.168.27.0/24 and 192.168.85.0/24.

8. Frame switching and the MAC table

Unlike an Ethernet HUB, where data is always spread to every port, Ethernet switches transmit frames only to the port where each frame is needed, and that is, where the destination node stands.

Ethernet switches transform Ethernet networks from shared medium networks into packet-switched networks.

Ethernet frame switching works around the MAC table. The MAC table holds associations between Ethernet node addresses and the switch ports. The meaning of each association is: **the node with that Ethernet node address is available (connected to) that port of the switch**.

When the switch is started, the MAC table is empty, and because there is no information yet, every received frame is, for now, retransmitted to all ports (except for the incoming port itself).

However, as frames start arriving at the switch, the **source node addresses** are recorded in the MAC table together with the port through which they are being received. Ethernet node addresses are unique in the MAC table, if already there, the entry is refreshed/overwritten with the new information. Also, entries in the MAC table have a short time to live, if not refreshed they are removed within some seconds.

When the switch receives a frame, the Ethernet destination node address is searched in the MAC table (Figure 12), if present the frame is transmitted only on the associated port, otherwise, the frame is transmitted on all ports (except the port from which it was received). Frames sent to the broadcast address (FF:FF:FF:FF:FF.FF) are always transmitted on all ports.

Host MAC Address	Port
00 00 80 45 FE 21	5
00 00 80 45 DA 47	3
00 40 00 80 45 FE	2
00 40 80 10 AA 21	1
00 00 80 00 FF AB	5

Figure 12- A switch MAC table

9. Practical activity – switching Ethernet networks

Use the Cisco Packet Tracer tool to create the network layout with two **Ethernet switches** and four end nodes shown in Figure 13.

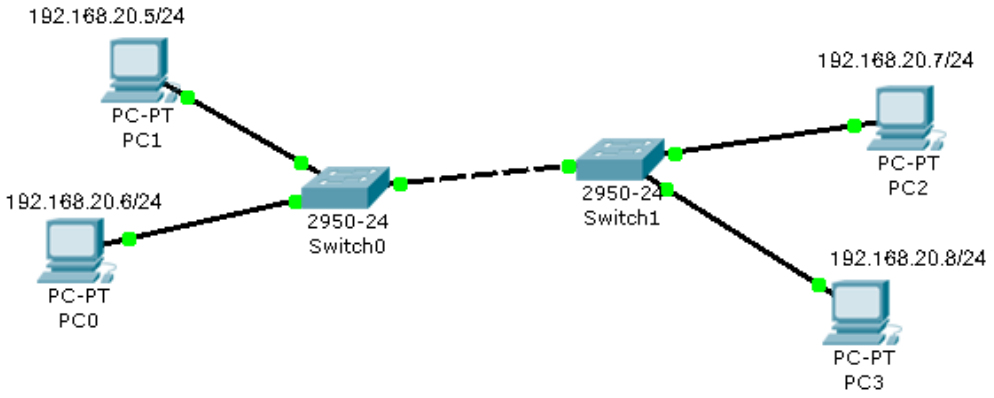

Figure 13- Network layout with two switches

- Set PC0 to PC3 IPv4 node addresses as represented on the image above (all four nodes belong to network 192.168.20.0/24).

- Display each switch MAC table (click with the Inspect tool - Magnifying glass on the switch)

Because no communications have happened yet, MAC tables should be empty.

- Switch to simulation mode but keep the MAC table windows visible.

- Use the Add Simple PDU tool to create ICMP echo requests between all four nodes and watch closely what will happen.

Why the first frame sent by each node reaches everywhere, but next frames do not?

Is this a shared medium network or a frame switching network?

Try now creating a collision as before.

- Clean the simulation (NEW button) but keep in simulation mode.

- Now let us send an ICMP echo request to the broadcast address

To do so, we must use the **Add Complex PDU** button. This button is on the right side of the Add Simple PDU button and is represented by the image of an open envelope. After selecting the tool, click on the node that will be sending the PDU, a form will popup for you to provide the details about the PDU.

Select application: PING

Set destination IP address: 192.168.20.255

(This is the IPv4 broadcast address for the network 192.168.20.0/24)

(The generic IPv4 broadcast address may also be used: 255.255.255.255)

Set sequence number: 1

Select Periodic.

Set interval: 5

Now click **Create PDU**, this will send a broadcast packet every 5 seconds.

Check that the frame reaches every node, you may repeat and send more ICMP echo requests to the broadcast address, and you will see they always reach all network nodes.

This is how switches are supposed to operate, they are to propagate broadcast (and multicast) traffic to every location, because that is what broadcast and multicast addresses are intended for.

The network areas to which broadcast traffic is propagated is frequently referred to as a **broadcast domain**. In general, **broadcast domains** match layer two networks and they also match IP networks.