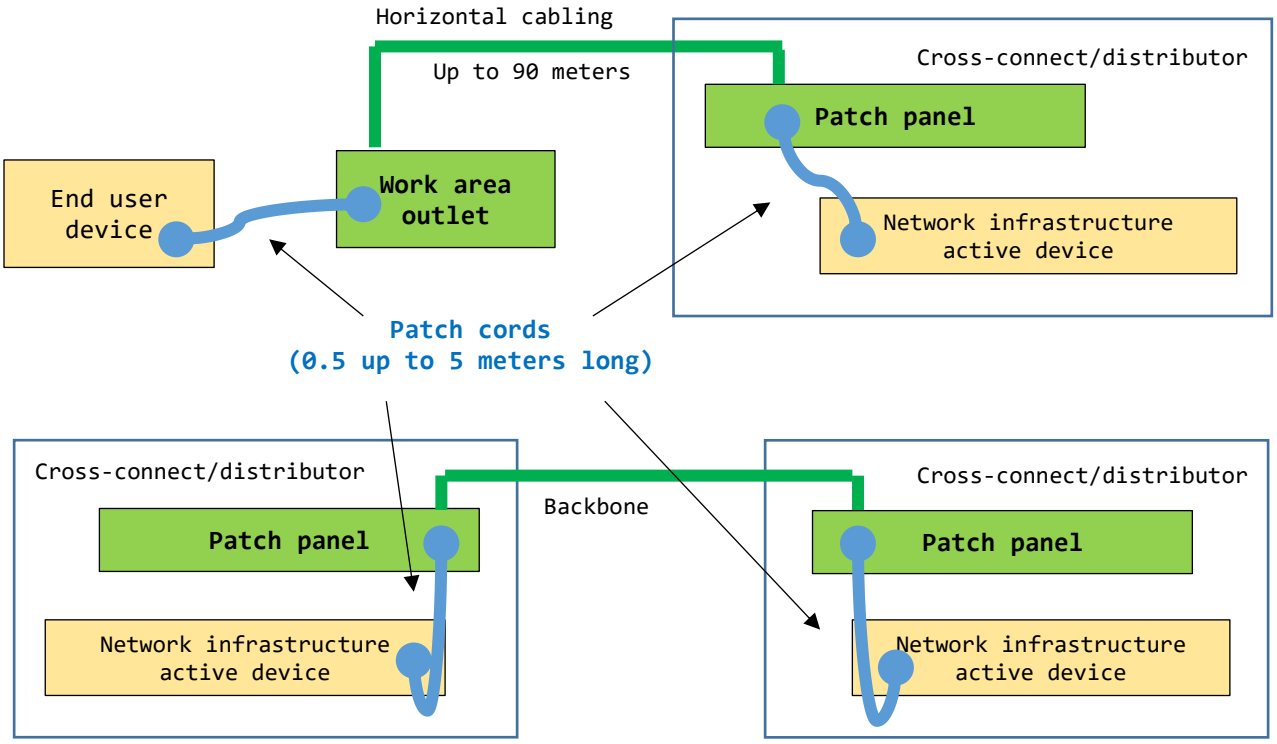
Computer Networks *(Redes de Computadores - RCOMP)* – 2021/2022 ***Laboratory Class 02 (PL02 – 3 hours)***	
Subjects	Materials
Mounting copper CAT6 patch panels. The Packet Tracer network configuration simulation tool. Shared medium networks and packet switching networks. Ethernet technology. IPv4 basic addressing. IPv4 connectivity testing with ICMP echo messages. Project - Sprint 1 support.	• 4 x RJ45 crimping plier. • 4 x Cooper patch panel punch down tool. • 2 x CAT6 copper patch panel. • 2 x CAT6 copper RJ45 sockets. • 4 x CAT6 cables.

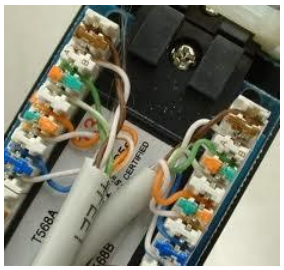
1. Patch panels and outlets

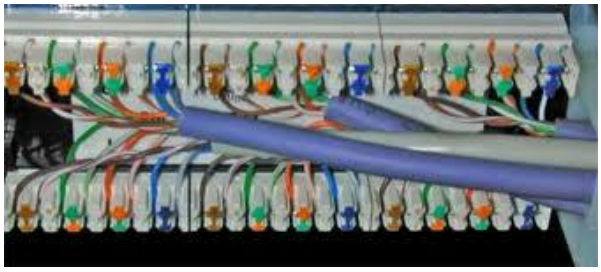
The patch cords addressed in the previous laboratory class are used to connect active devices to the cabling infrastructure of the building, meaning the wiring termination hardware used in structured cabling.

Every cable belonging to the structured cabling system is connected to either the back of a patch panel or the back of work area network outlet.

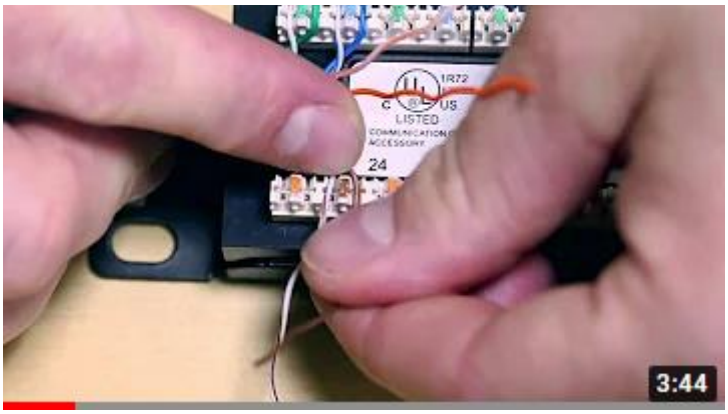


Wiring a copper cable to a patch panel is usually a simple operation, and unlike plugs crimping, it's reversible. However, details are somewhat vendor dependent. Usually, wires are forced between two metallic tabs that will drill the plastic insulation cover and establish electrical contact. For forced insertion of each wire a specialized **punch down tool**.



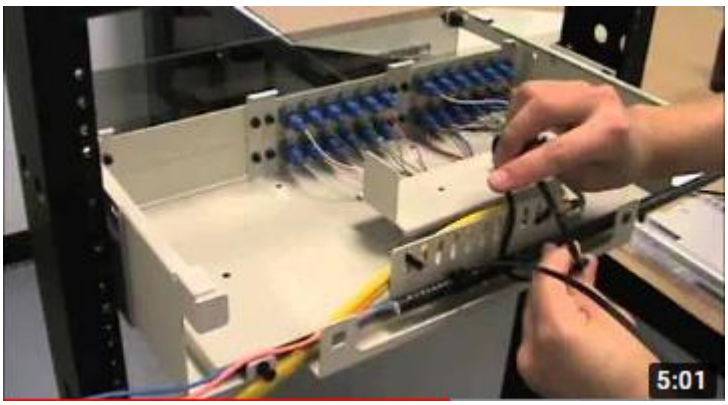


Take some minutes to see the following video:



https://www.youtube.com/watch?v=D8PnNuDbkAw

Of course, for optical fibre cabling, comparable but specific patch panels must be used instead. Check the following video:



https://www.youtube.com/watch?v=cRt-528w7ms

2. Practical activity - copper cable wiring to a patch panel and an outlet

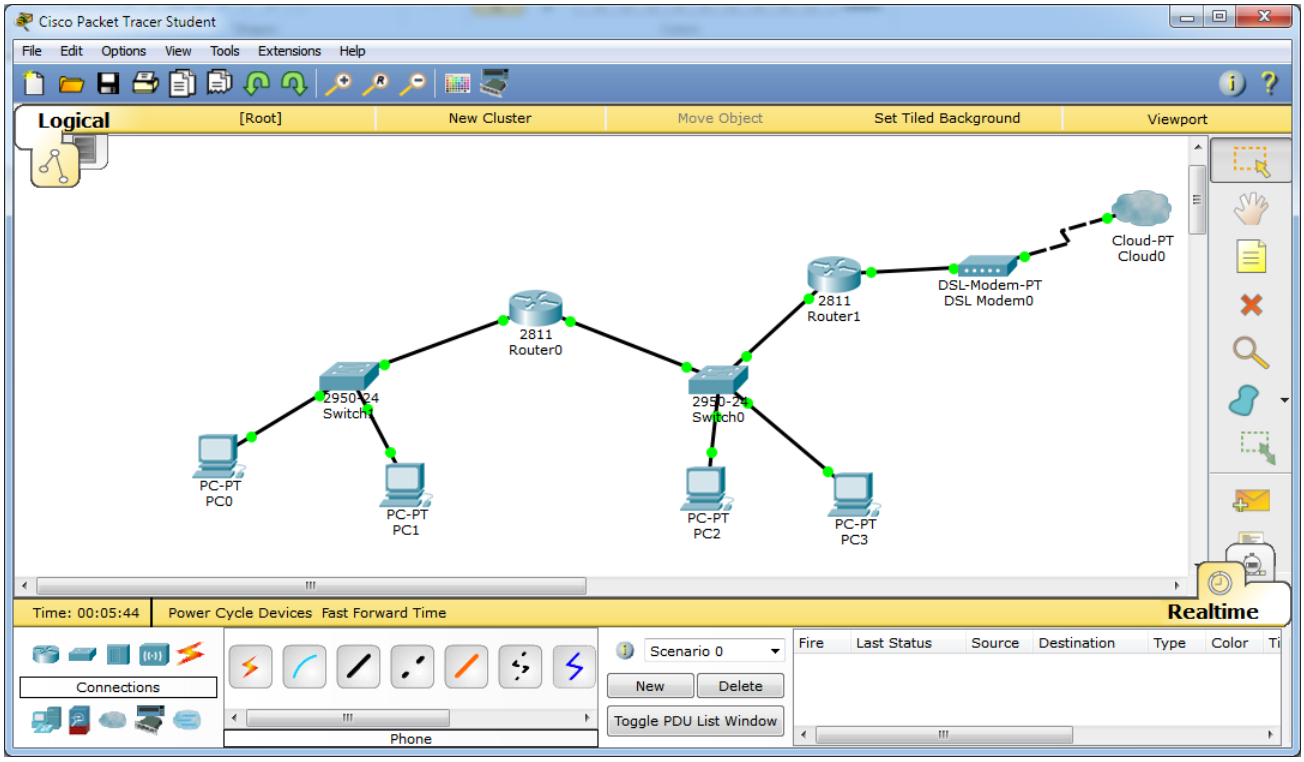
One at a time, each group of two students will:

- Wire a copper cable to a patch panel in on end.
- Wire the same copper cable to an outlet on the other end.
- Ask the teacher for comments on the job.
- When done, the group should remove the cable from both the patch panel and outlet and cut the cable ends for the next group to have a fresh start.

3. About the Cisco Packet Tracer network simulation tool

Cisco Packet Tracer is an extensive network configuration simulation tool used at Cisco Networking Academy courses. With 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.



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

2nd Select the model or cable type.

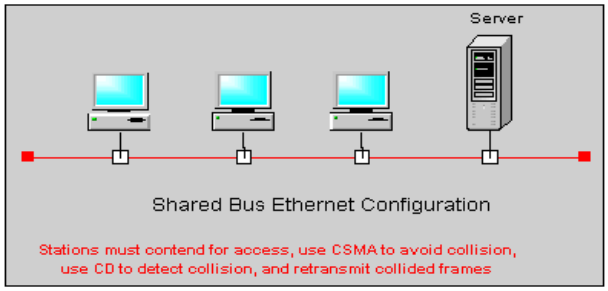
Once devices are connected and configured, Packet Tracer may be run in either real-time or simulation mode. In simulation mode the user is able to see and follow, step by step, individual packets traveling around the created layout.

4. 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, 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, signals get mixed and become useless, this is called a **collision**.



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 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).

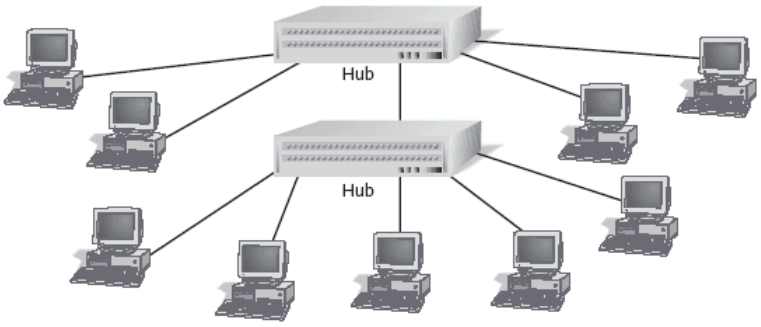
When a node is sending, it must also be listening to what's going on (LWT – Listen While Talk). Listening allows the node to detect if a collision happens (CD – Collision Detection), if so, it immediately stops sending data and instead sends a special signal called JAM. The JAM notifies every node on the network that a collision has just happened, and thus data 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 introduces all the basic requirements to make collisions impossible, and thus, abandon CSMA/CD.



The start topology by itself doesn't guarantee CSMA/CD can be disabled, all depends on the network devices operation mode.

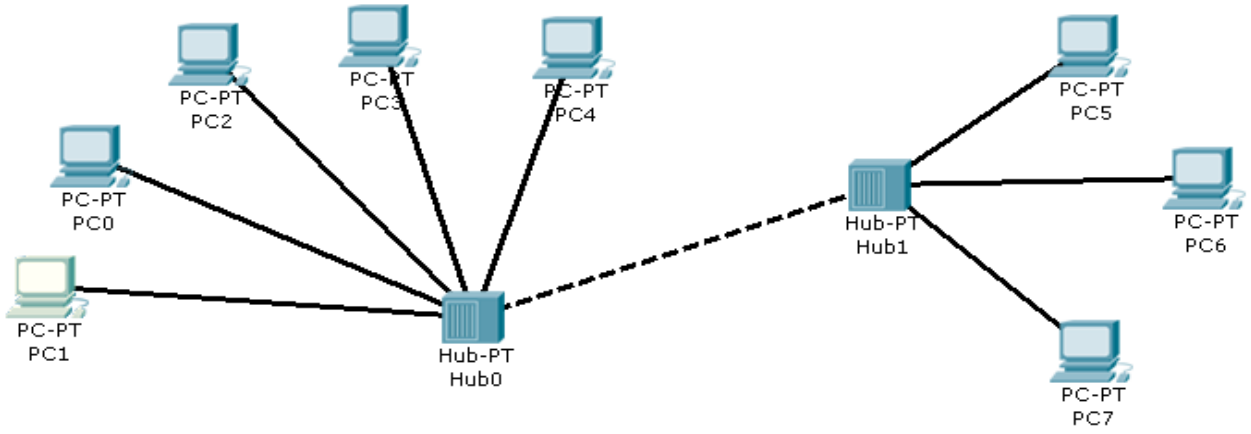
HUB (Repeating HUB) – this is a simple signal amplifier, when a signal is received on one port it's copied and emitted on all ports. This is a bus equivalent (often called "bus in a box"), collisions happen as before, and thus, CSMA/CD is still required.

Network Switch – although externally similar to a hub, it works with frames (at layer two), not signals (at layer one). A switch is capable of receiving at the same time frames on every port and additionally, at the same time sending 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, almost all Ethernet networks are frame switching networks and not shared transmission medium networks.
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.

5. Practical activity – shared transmission medium

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



Warning: in Packet Tracer devices, copper ports are not auto MDI-X. Thus to connect 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.**

5.1. 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.

5.2. 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**.

Use the **Add Simple PDU** tool to send an ICMP echo request from PC1 to PC7.

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

Watch closely what is happening.

Repeat the test now from PC7 to PC1.

Question: is this a shared medium network or a switching network?

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.

Switching between real-time mode and simulation mode.

5.3. 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 occurs, definitely this is a shared medium network than cannot cope with traffic from more than one node at a time.

5.4. Handling 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's 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.**

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.

6. 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 is.

Ethernet switches transform an Ethernet network from a shared medium network into a packet-switched network.

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

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).

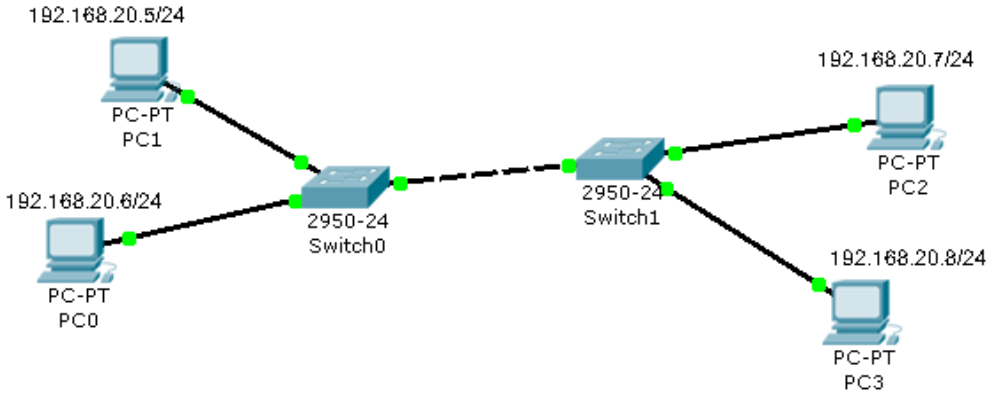
However, as frames start arriving at the switch, the **source node addresses** are recorded in the MAC table together with the port they are being received from. Ethernet node addresses are unique in the MAC table, if already there, the entry is refreshed/overwritten with the new information. Also, entries 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, 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 (again, except the incoming port).

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

7. Practical activity – switching Ethernet networks

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



- 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's send an ICMP echo request to the broadcast address

To do so, we must use the **Add Complex PDU** tool.

Add Complex PDU tool. After selecting the tool, click on the node that will be sending the PDU.

Select application: PING

Set destination IP address: 192.168.20.255

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

(The generic IPv4 broadcast address could 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 also multicast) traffic to every location because that is what these kind of 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.

8. Project - Sprint 1 support

8.1. Network outlets

Once each room's area was estimated, accordingly the number of required for each room has been established.

Concerning network outlets for indoors wireless access-points, walls, slabs, and columns disturb the signal propagation, each access-point reach is always less than about 30 meters. To maximise coverage and avoid signal propagation to outdoors, access-points should be placed in floors central locations.

For a fair coverage of an area by a set of access-points, they ought to be closer than 50 meters from each other. As far as possible, access-points in adjacent floors ought to have different positions to avoid cells overlapping. Later, Wi-Fi channels will be assigned to each access-point reinforcing this cell overlapping issue.

Each individual outlet must be pinpointed in floor blueprints.

8.2. Cross-connects, cable pathways and cables

Having all outlets locations fixed, the next step it's deciding where to place each cross-connect. Several previously studied standards and guidelines, apply here.

Concerning horizontal cabling subsystems, remember no outlet can distance more than 80 meters from the horizontal cross-connect in a straight line, also cable length cannot be above 90 meters. If required consolidation points may be created.

Cable pathways outlining comes next. As far as possible, the maximum number of cables ought to share the same pathway, or at least part of it.

Now, each cable length can be calculated. A recheck on horizontal cabling lengths is prudent for the longer cables. For lengths above 90 meters, the only available option is the optical fibre, all the same, backbones, in general, should use optical fibre. Backbone redundant connections must not be forgotten.

8.3. Patch-panels and telecommunication enclosures

Every cable entering a cross-connect is wired up to a patch panel. Being that the number of cables and cable types entering each cross-connect is now known, consistently, the number and type of required patch panels in each cross-connect can be settled.

The number of required connections at each cross-point must then be matched with patch-panel manufacturers' data, the vertical space occupied in the telecommunication enclosures is specified in U rack units. Typical 24 ports CAT6 copper patch panels take 1U and 48 ports CAT6 copper patch panels do occupy 2U on the telecommunications enclosure. Current optical fibre patch-panels have similar densities to copper patch-panels, older models are more modest: as low as four optical fibre connections for 1U.

Enforcing the previously suggested oversizing strategies, we can infer the telecommunications enclosures size by multiplying by four the amount of space required by housed patch-panels and round it up to the next commercially available size.

8.4. Inventories

In fact, the structured cabling hardware inventory is mostly done, it's just an accounting mater to establish total numbers for network outlets, each type of patch-panels, and telecommunication enclosures. One key element yet missing from the inventory are cables themselves.

Building the cable inventory over the pathways blueprint can be a fairly significant effort, previously discussed simplifications and approximations can be used.

Patch cords are not regarded as structured cabling hardware, but they are ultimately required. Copper and optical fibre patch-cords are commercially available ranging from 0.5 meters up to 5 meters long. Inside telecommunications enclosures 0.5 meters models are most appropriate to connect patch-panels to active hardware.

8.5. Global inventory (sprint master)

It's up to the sprint master creating a global inventory for all structured cabling hardware required, this is just a matter of picking each team member's inventory and sum it all. The sprint master should also start preparing the **review.md** document for the incoming sprint review meeting.