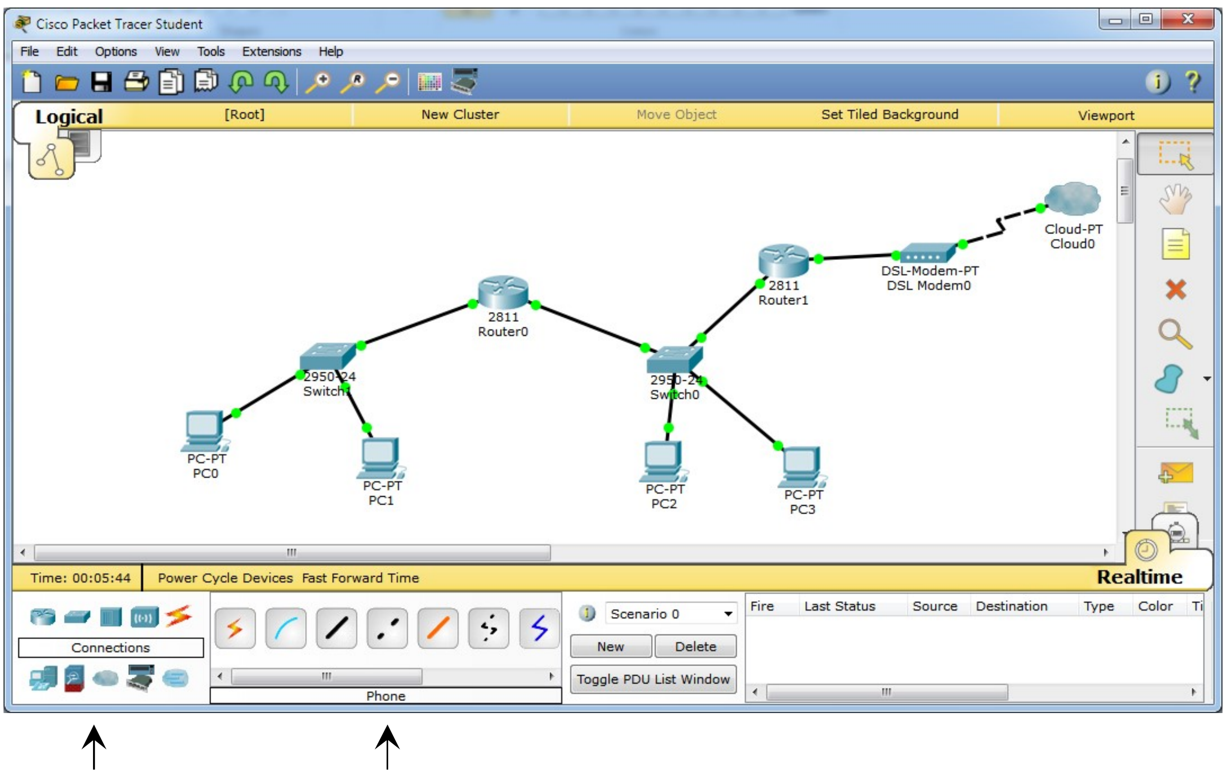
• Packet Tracer network configuration simulation tool • Shared medium networks and packet switching networks • Ethernet technology. • IPv4 basic addressing. • IPv4 connectivity testing with ICMP echo messages.	• Cisco Packet Tracer

1. 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 in 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 are able to see and follow, step by step, individual packets traveling around the created layout.

1.1. Download and install Cisco Packet Tracer (it's free)

To install **Cisco Packet Tracer** on your personal computer go to Cisco Networking Academy site and follow instructions there:

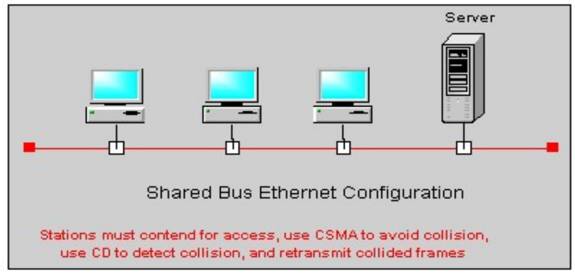
https://www.netacad.com/courses/packet-tracer-download/

2. 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 will reach every connected node. Is 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 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 will be useless, this is called a collision.



Even if collisions could be avoided the medium will 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).

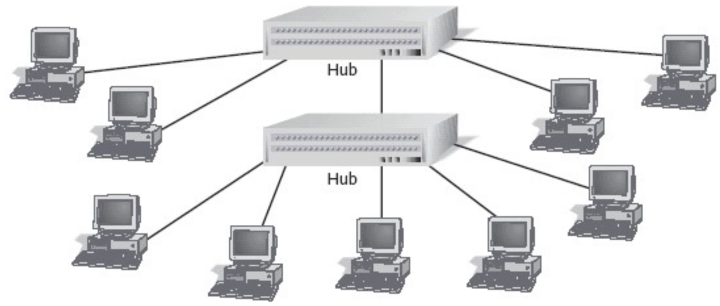
When a node is sending, it must also be listening what's going on (LWT – Listen While Talk). Listening allows the node to detect if a collision happens (CD – Collision Detection), if so, immediately stops sending data and instead sends a special signal called JAM. The JAM notifies every node a collision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

The collision detection 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 sending 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.

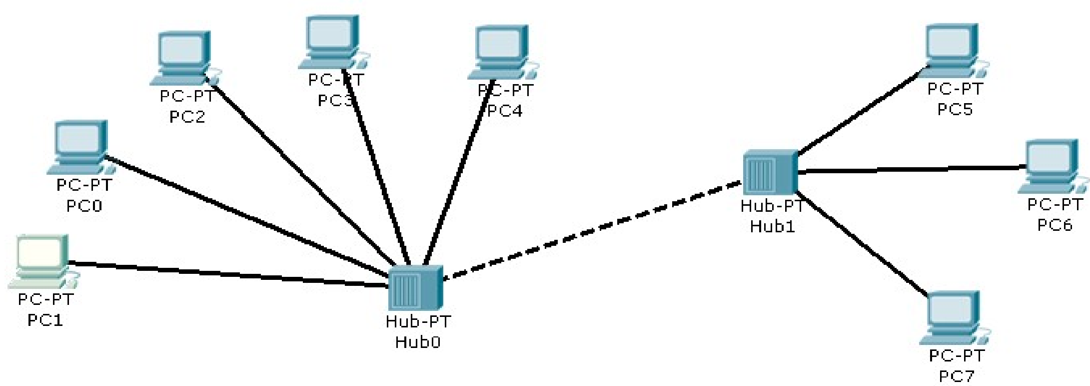
HUB (Repeating HUB) – this is a simple signal amplifier, when a signal is received on one port it's copied and emitted on all ports. This is a bus equivalent (called "bus in a box"), collisions happen as before, and thus, CSMA/CD is still required.

Network Switch – although externally similar to a hub, it works with frames (layer two), not signals (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 retransition. **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 **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 address 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.

3. 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: on Packet Tracer devices, copper ports are not auto MDI-X. Therefore to connect two intermediate devices a cross-over cable is required.

3.1 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.

3.2 Test IPv4 connectivity

The easiest way to test IPv4 connectivity is by issuing ICMP echo requests and waiting for a reply from the target node (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 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.

3.3 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.

3.4 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 IPv4 networks: 192.168.27.0/24 and 192.168.85.0/24.

4. Frame switching – 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 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.

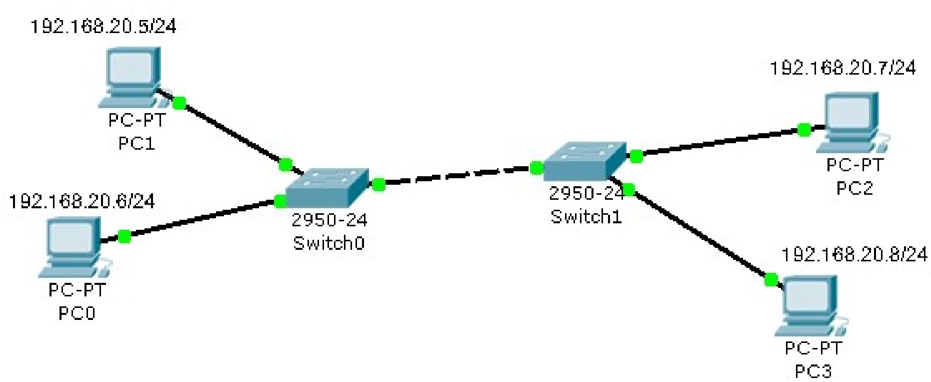
However, as frames start arriving at the switch **source node addresses** are recorded in the MAC table together with the port they are being received from. Ethernet node addresses are unique in the MAC table, if already there, the entry is refreshed with new information. Also, entries in the MAC table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

5. 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 in 3.3.

- 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
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)
Sequence number: 1
Select Periodic.
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.