SWitCH – Sistemas de Computação e Redes (SCOMRED)

2020/2021

Laboratory Script 01

Computer Networks. Packet Tracer practice.

1. The classes networking environment

In this course students will be using their own laptops. The first step is getting connected to the internet, locally at DEI premises either EDUROAM or ISEPWLAN can be used, preferably the former.

Regarding EDUROAM and ISEPWLAN, the wireless access service is provided by ISEP, so you should use your ISEP credentials to access it, the same credentials you use to access the ISEP portal (**https://portal.isep.ipp.pt/**) and the ISEP Moodle service (**https://moodle.isep.ipp.pt/**).

Once connected, a DHCP server on the network will provide the required IPv4 configuration data for your laptop:

- A unique **IPv4 node address** belonging to the local network.
- The network's **prefix length**. Together with the node address, this will establish the local network address (local network's prefix).
- The **default gateway** to be used, it's required to be able to reach IP nodes not belonging to the same local network.
- **IP addresses of DNS servers** to be used for names resolution. DNS configuration is not required for IP to work, but it allows users to specify network nodes, most often servers, by names instead of IP addresses.
- DNS domain names (local/default DNS domain and search DNS domains), to be used when the user provides an unqualified name (without the domain name, e.g. www).

PRACTICE:

Inspect your laptop's current network configuration status to see the value of each of these attributes provided by the DHCP server.

The way to view this information depends on your laptop's operating system. In MS-Windows systems, at the command line (CMD) you can type the following command:

ipconfig /all

It will present IP global configuration data, and for each network interface, specific configuration data for that interface.

If you are using other operating systems search the internet about ways to see your current network configuration.

Identify for later use:

Your own IPv4 address: ____ . ____ . ____ . ____

The IPv4 address of the default-gateway: ____ . ____ . ____ . ____

The IPv4 addresses of two local DNS servers: ____ . ____ . ____ . ____ ; ____ . ____ . ____ . ____

2. IP connectivity testing – ICMP echo requests

A network node using IP (Internet Protocol) is obliged to handle several other associated protocols. User and system applications use mostly UDP (User Datagram Protocol) and TCP (Transmission Control Protocol), however, lower level auxiliary protocols are also required, including ARP (Address Resolution Protocol) and ICMP (Internet Control Message Protocol).

ICMP is used by IP to report errors and other issues, but it can also be used to test the network. One ICMP message we can send is the **echo request**, when an IP node receives an echo request it´s obliged to reply back with one other ICMP message, the **echo reply**.

Connectivity testing stands for checking if two network nodes are able to communicate with each other, the most strait forward connectivity test we can undertake in an IP network is by using ICMP.

The round trip test usually called **ping** consist on sending one **ICMP echo request** message, and them waiting up to a maximum time (timeout) for the corresponding **ICMP echo reply** message. If this test is successful, it means **transmission is working in both directions**. This test also tell something about the network performance by measuring the round trip time (RTT).

PRACTICE:

Check IPv4 connectivity with some nodes around you. At the command prompt use the ping command:

ping {IPv4-ADDRESS-TO-TEST}

a) Ping your own address (depending on or system, the ping command may continue sending ICMP echo requests forever, press CTRL+C to stop it).

b) Ping the loopback address (127.0.0.1).

c) Ping the default gateway.

d) Ping the local DNS servers.

   Notice that some DNS servers might not respond, even though IPv4 nodes should always reply to ICMP echo requests, for security reasons, some servers may have this kind of traffic blocked by a firewall.

e) Ping **www.google.com**, instead of providing an IP address to the ping command you can also provide a DNS host name, then DNS servers are used to fetch the corresponding IP address. You may also ping some additional DNS names of the internet. This way the ping command also tell us if the local DNS resolution of names is working.

f) Ask colleagues around you for the IP node address that has been assigned to their laptop and ping them. Again, notice that some laptops may have firewalls blocking incoming ICMP echo request. There's an additional catch if you are having this class online, for this to be successful both you and your colleagues must be connected to the DEI VPN service we will talk about latter.

3. ARP tables

One protocol that is vital for IPv4 to operate **within a local network** is ARP (Address Resolution Protocol). To communicate within a local network, no routers/gateways are required, IP packets are simply placed inside layer two frames as payload and sent to the destination node address.

Yet, because IP node addresses are independent of layer two addresses (e.g. Ethernet), to get the layer two frame delivered to the correct destination node, its layer two address must be used. This layer two address is usually known as Ethernet address, MAC address or physical address and has 48 bits.

The ARP protocol is used to build and dynamically maintain an equivalences table between IPv4 address and MAC addresses called the ARP table. Entries in the ARP table persist only during a short period of time, depending on your system from 15 seconds up to a couple of minutes, if not used for that amount of time they are removed.

ARP itself uses broadcast messages within the local network to determine the MAC address of a given IPv4 address and then that information is refreshed on the node's ARP table.

PRACTICE:

a) Display your node's ARP table by issuing at command line the following command:

arp –a

b) Ping a colleague's IP node address that was not present on the ARP table.

c) Check again your node's ARP table to see that the IPv4 address has been added to your node's ARP table.

d) Repeat the previous test with other IP addresses, however, remember ARP is only for nodes belonging to the local network, don't expect remote nodes like **www.google.com** to appear on the ARP table because they a reached by using the default gateway and not directly. Thus, the default gateway will always be on the ARP table.

4. DEI networks and services

DEI manages its own networks and services, some of such services are available publicly from the Internet, but others are not. Mostly for security reasons, several services are available only within **DEI private networks infrastructure** (unreachable from the internet).

A network node (e.g. your laptop) is plugged to the **DEI private networks infrastructure** if it's either:

- Connected by a network cable to a network outlet in DEI laboratory (**physically plugged**).
- Connected through the internet to a DEI VPN service (**virtually plugged**).

In simple words, such a VPN connection is a simulated (virtual) network cable between your laptop and the **DEI private networks infrastructure.**

The **https://rede.dei.isep.ipp.pt** site contains some information in Portuguese/English about the **DEI private networks infrastructure** and several services it provides.

PRACTICE:

a) Take a while to inspect information available at this site.

b) There's a service to check what your IP node address is, in addition it also sends a couple of ICMP echo request to your IP node address.

https://rede.dei.isep.ipp.pt/myip

The IP addresses presented here are under the point of view of the **DEI private networks infrastructure**. If the node is plugged to that infrastructure they will be internal private IP addresses.

User credentials for DEI services are independent of ISEP credentials, however, every user belonging to DEI may create an account in DEI by using the ISEP credentials:

https://rede.dei.isep.ipp.pt/usersync-isep

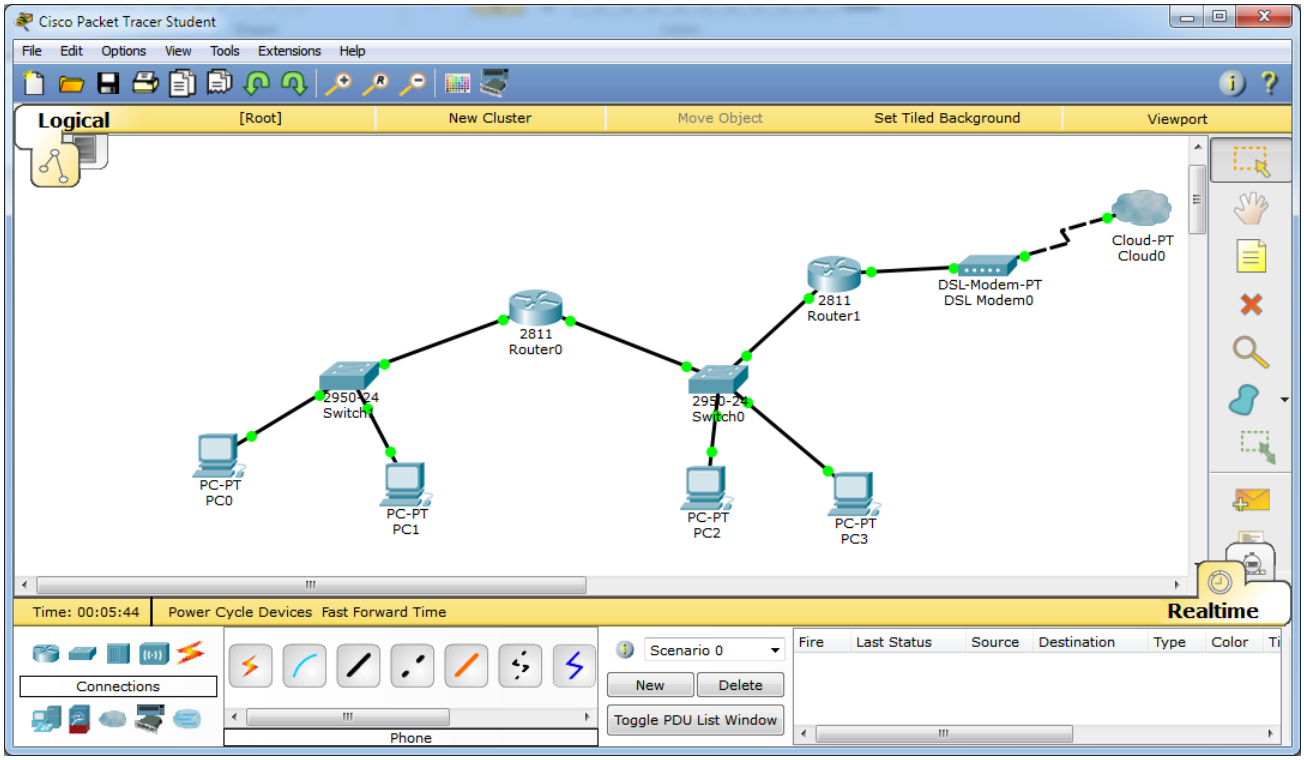
PRACTICE:

You already have an ISEP user account, if haven't already done so, create a similar DEI account by using the above link.

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

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

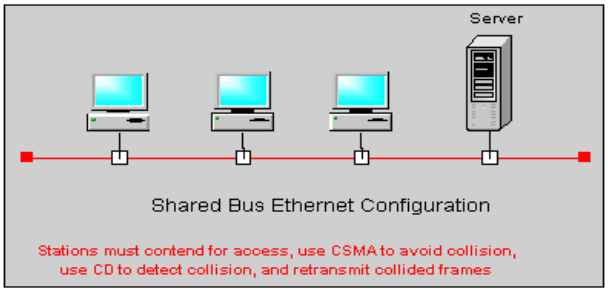
To install **Cisco Packet Tracer** on your personal computer go to Cisco Networking Academy site and follow instructions there:

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

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 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 (image on the right), 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's 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 their 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).

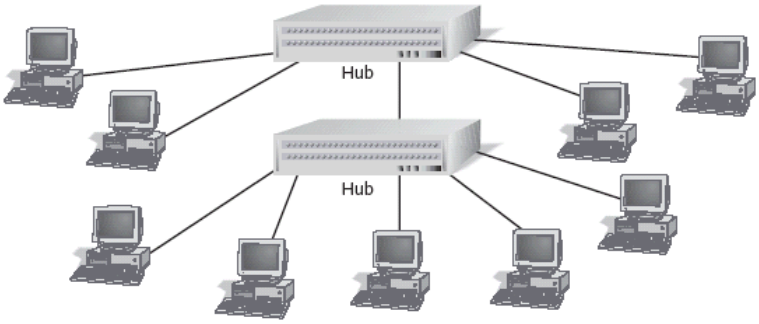
When a node is sending, it must also be listening what's going on (LWT – Listen While Talk). Listening allows the node to detect if a collision happens (CD – Collision Detection), if so, immediately stops sending data and instead sends a special signal called JAM. The JAM notifies every node a collision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



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

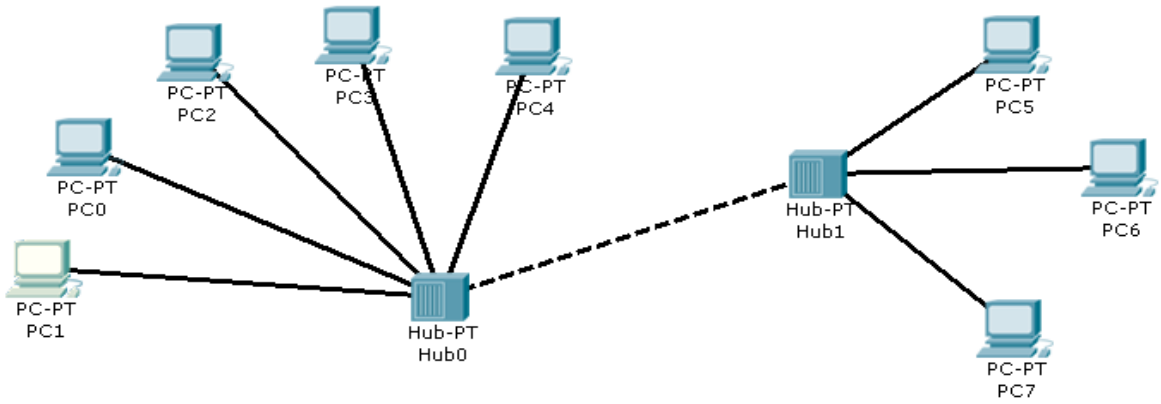
HUB (Repeating HUB) – this is a simple signal amplifier, when a signal is received on one port it's copied and emitted on all ports. This is a bus equivalent (called "bus in a box"), collisions happen as before, and thus, CSMA/CD is still required.

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.

PRACTICE:

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



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

a) 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.

b) 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 to be sent to.

Switching between real-time mode and simulation mode.

c) 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.

d) 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?

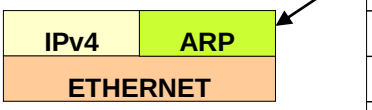
In each of the five nodes, change the network prefix length to 16 bits (255.255.0.0 mask), keeping the node addresses unchanged.

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

Changing the network's prefix length has a significant impact, 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**.

7. The ARP table

ARP is required because there´s no relation between MAC addresses and IPv4 addresses, nevertheless, to use an Ethernet network to deliver an IP packet, the MAC address is required. More exactly, when sending an IPv4 packet to some IPv4 address in the local network, the MAC address of the node having that IPv4 address is required.



ARP TABLE	
IPv4	MAC
192.168.10.5	00:0A:B3:45:34:AB
192.168.10.34	00:0A:B3:50:54:14
192.168.10.240	00:0E:F3:50:00:FA

PRACTICE:

a) **Add one additional PC (PC8) to Hub1 and assign to it IP address 192.168.85.111/16.**

b) **Show PC0's ARP table.**

Select the Inspect tool (Magnifying glass), click on PC0 and then select ARP table.

Keep the ARP table box open, check that address 192.168.85.111 isn't there.

c) **Send an ICMP echo request from PC0 to the newly added PC8.**

Check that PC8's IPv4 address has been added to the ARP table.

8. 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.

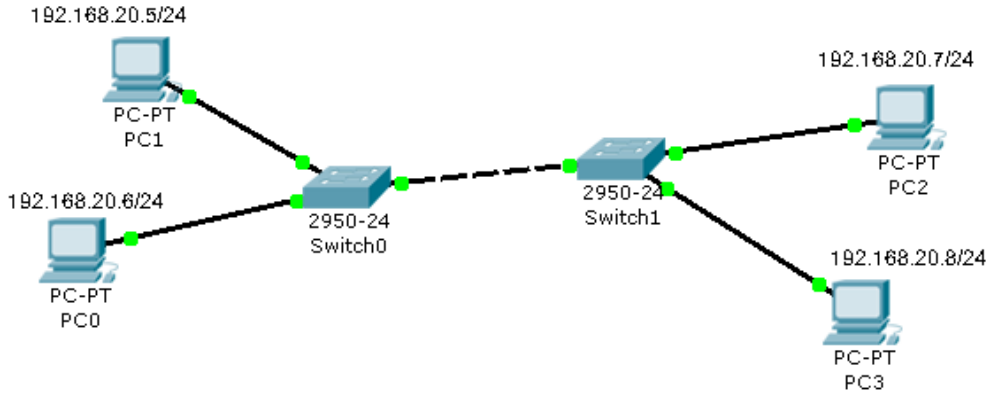
However, as frames start arriving at the switch, **source node addresses** are recorded in the MAC table together with the port they are being received from. Ethernet node addresses are unique in the MAC table, if already there, the entry is refreshed with new information. Also, entries in the MAC table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

PRACTICE:

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



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

b) **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.

c) **Switch to simulation mode, but keep the MAC table boxes visible to see changes happening.**

d) **Use the Add Simple PDU tool to create ICMP echo requests between all four nodes and watch closely what happens on MAC tables.**

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 collisions as before.

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

f) 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.

9. IPv4 routing

Two IPv4 nodes can communicate directly (without routers) only if two preconditions are meet:

A – Both are connected to the same LAN/VLAN (same broadcast domain)

B – Both nodes IPv4 addresses belong to the same IPv4 network.

We can see precondition **A** arises straight from ARP.

An IPv4 sending node must somehow know if a given destination IP address is reachable directly or not. If reachable directly it just needs to use ARP and then encapsulate it inside a layer two frame, otherwise the packet must be sent to a router.

The way a sending node decides this is by matching the given destination IP address with the local IPv4 network if the network prefix is the same we assume direct communication is possible. From here comes condition B.

9.1. Routers

Routers (aka gateways) are layer three intermediate nodes, they forward layer three packets and not layer two frame like switches do. The mission of an IP router is receiving IP packets from one LAN/VLAN and retransmitting then on another LAN/VLAN.

9.2. Using routers

When an IP sending nodes checks the IP destination address of the packet does not belong to the local IP network, it knows a router must be used, so the **router IP address** must be known.

One IP node may be aware of several routers around it, but end nodes are usually aware of only one router they can use, this is an additional required configuration parameter usually called **default-gateway** (aka default-router). If a node is not aware of any available router it will never be able to communicate with nodes beyond the local IP network.

If the destination IP address does not belong to the local IPv4 network, the IPv4 packet must be sent to the default-.gateway instead. Sending to the default-gateway works the same as before, the IPv4 packet must be encapsulated into a layer two frame, and ARP must be used to set the appropriate **Destination MAC Address**. The only difference is that now, we will be requesting ARP for the default-gateway MAC address, and not the destination IP node MAC address.

Because communications with the router use layer two encapsulation and ARP, one condition must be met for a router address to be valid:

For a given node, a router address is useful only if it belongs to a local IPv4 network.

9.3. Routing tables

The difference between a router and an end node is a router is supposed to retransmit IP packets, so it must be connected to more than one IP network. Thus the router mission is more complex, while an end node has only two options (local destination or nonlocal destination) the router has more options.

A typical end node only need to know the local IP network, if the destination address does not belong to the local network then the packet is sent to the default-gateway. This means, all other networks are reachable through the default-gateway.

A typical router is connected to several networks and has several routers available around it to be used. Each router around it will provide access to some IP networks, it needs to know which networks access is provided by each of its neighbour routers. This is the role of the routing table.

The routing table is a list of IP networks (IP address and prefix-length), and for each, the IP address of the neighbour router that should be used, the router to be used is called **next-hop**.

Take for instance a router connected to networks 192.168.10.0/24 and 192.168.20.0/20, the routing table can be something like:

Destination	Next-hop
192.168.5.0/24	192.168.10.7
192.168.8.0/24	192.168.10.7
192.168.34.0/24	192.168.20.170
192.168.38.0/24	192.168.20.200

When this router receives an IPv4 packet for forwarding it will look at its destination IPv4 address to see which network it belongs to, options are:

1º Belongs to network 192.168.10.0/24 => direct sending (layer two)

2º Belongs to network 192.168.20.0/24 => direct sending (layer two)

3º Belongs to network 192.168.5.0/20 => send to 192.168.10.7 router

4º Belongs to network 192.168.8.0/24 => send to 192.168.10.7 router

5º Belongs to network 192.168.34.0/24 => send to 192.168.20.170 router

6º Belongs to network 192.168.38.0/24 => send to 192.168.20.200 router

Once a match is found the packet is sent and processing ends. If no match is found the packet is discarded, if this happens, it means the router does not known the destination network.

Checking if an address belongs to a network is achieved by applying the network mask (bit-to-bit and) to the address and see if the network address is obtained.

Routing tables can be manually set, this is called **static routing**. There are also routing protocols that are able to build routing tables and keep them updated, this is called **dynamic routing**.

9.4. Default route

We cannot store in a single routing table all the networks being used around the internet, however, if a network is unknown to a router it will be unreachable.

The workaround is defining the special network 0.0.0.0/0 in each routing table. Because the mask is zero, it will always match any IP address, so it has to be the last entry at the routing table.

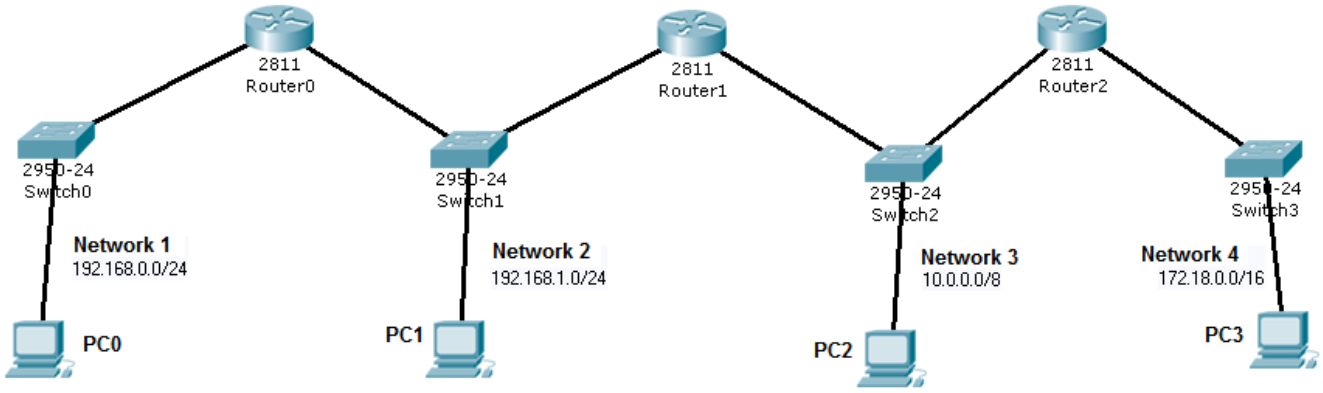
This entry is called the **default-route**, and the corresponding next-hop is called the **default-gateway**. Because is matches every IP address and is placed at the end of the table, the result will be that any packet addressed to an unknown network will be forwarded to the default-gateway.

Usually the default-route allows routing table simplifications, generally speaking, any routing table entry with a next-hop equal to the default-gateway can be removed. This is true because in its absence the table processing will continue until reaching the default-route and the result will be the same, the packet is sent to the same router.

PRACTICE:

Use the Packet Tracer tool to create the following layout

There are four IPv4 networks interconnected by three routers



a) Define all layer three nodes IPv4 addresses (routers and end nodes)

Used IPv4 addresses must belong to the represented IPv4 networks.

Check that, for now, ARP tables are empty (use the Inspect tool – Magnifying Glass).

b) Check IPv4 connectivity

Use the Add PDU tool to send ICMP echo requests between nodes.

Check that tests within each LAN are successful (from routers to local end nodes), but tests between different networks fail.

Also check that ARP tables are not empty any more.

c) Define end nodes' (PCs) default gateways

PC1 and PC2 have two alternative routers, in both cases use Router1 as default-gateway.

d) Test again communications, now only between end nodes (PCs)

Check that between PC1 and PC2 everything works fine, but not with other nodes.

Try again in simulation mode to understanding what is happening. It's related with the fact that both PC1 and PC2 are using the same default-gateway.

e) Define each router routing table to solve the issue

For each router, check the remote networks it is not aware of. For each, add a static routing entry to inform to where the packets should be forwarded to reach that network.

f) Test again IPv4 connectivity between all end nodes

Check that now every node can communicate with every other node.

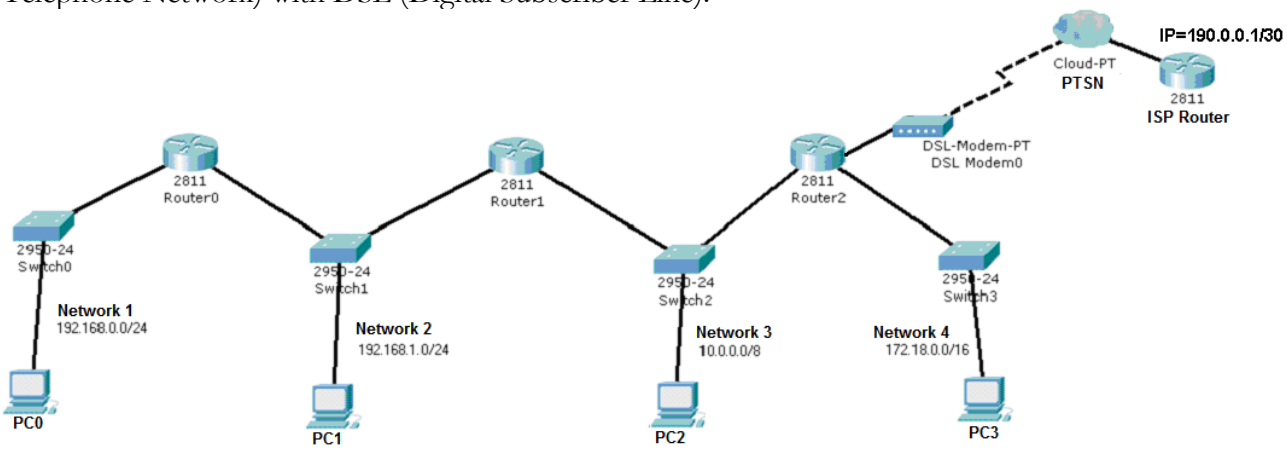
Check that ARP tables include only local addresses.

PRACTICE:

Adding a default route

a) Keep the previous layout and add an internet connection to Router 2

Router 2 will be connected to an ISP (Internet Service Provider) using the PSTN (Public Switched Telephone Network) with DSL (Digital Subscriber Line).



To establish the layer two connection, configure the cloud associating the DSL connection to the Ethernet connection

Set appropriate IPv4 addresses for the new router and for the new Router 2 interface. Because the internet connection mask has 30 bits, there are only two valid node addresses, if the ISP Router is using 190.0.0.1/30, then the only available valid node address is 190.0.0.2/30.

Before advancing, check if there is IPv4 connectivity between Router2 and the ISP Router.

b) Change the routers routing tables to represent the new reality

Now there is an internet connection, therefore you must add a default-route to each routing table, whenever the destination address of a packet is locally unknown, it should be routed to the ISP Router.

Add the necessary default-route entries in each local router.

In simulation mode use the Add Complex PDU tool to create an ICMP echo request addressed no a locally unknown address, say **172.19.1.1**. Send the request from PC0.

Check that all routers are forwarding unknown address packets in such a way they reach the ISP Router.