Redes de Computadores (RCOMP) – 2017/2018 Laboratory Class Script – PL08	
• IPv4 addressing and static routeing. • DHCP service configuration on Cisco routers. • Project 1 – VLAN based layer two platform. • VLAN Trunking Protocol (VTP).	• Cisco Packet Tracer

1. About DHCP (Dynamic Host Configuration Protocol)

Thanks to DHCP, when a node is plugged into a network it gets all required IPv4 configuration information automatically. This only works if the network has at least one running DHCP service.

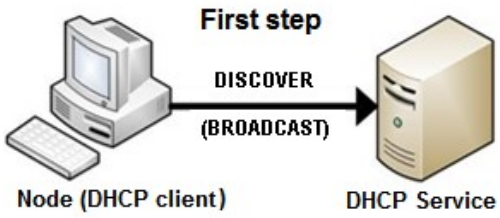
Among others, most relevant data provided by the DHCP service to the client node are a unique IPv4 address for the node to use, the network mask, the default gateway and DNS configuration data.

The DHCP service can manage static and dynamic IPv4 addresses. Static IPv4 addresses are manually assigned by the service administrator to specific client nodes (identified by their MAC addresses). Dynamic IPv4 addresses are automatically assigned by the DHCP service from an address pool provided by the service administrator. The DHCP service identifies client nodes by their MAC address and ensures assigned IPv4 addresses are unique.

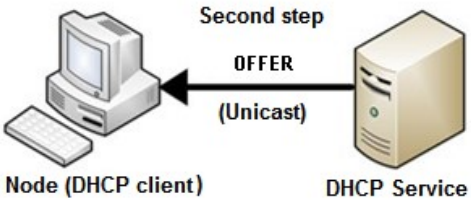
DHCP itself uses UDP over IPv4 for messages transport. At first glance, this would result in a cyclic dependency for the client node: needs DHCP to get the IPv4 configuration and DHCP requires IPv4 to be operating.

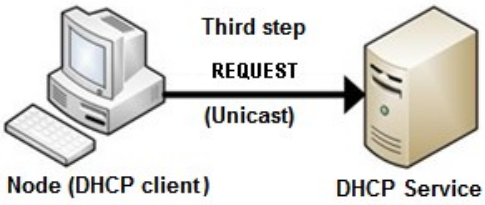
Nevertheless, this is overcome by using some special-purpose IPv4 addresses. The first message sent by the client node (DHCP Discover) is transported by an IPv4 packet with source address 0.0.0.0 (unknown IPv4 source address) and destination address 255.255.255.255 (local network IPv4 broadcast address).

Because the first contact from the client node to the DHCP service is made using broadcast, **it will only work if both the node and the service are in the same broadcast domain** (LAN/VLAN).

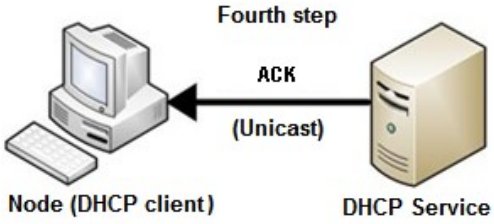


Every DHCP service within the broadcast domain will receive the discover message and reply with an offer message. The client can then select one and send a unicast request to start using the provided configuration data.





Finally, the DHCP service sends back an ACK (acknowledgement) message.



The configuration assigned to the client node is valid during the **lease time** period, if the node wants to keep using the same data it must send a new request before the lease time expires.

2. Setting up the DHCP service on Cisco routers

Several types of network nodes can be used to supply a DHCP service to a network, including Windows and Linux servers, however, a Cisco router can also provide this service.

Because broadcast is used, one requirement to be meet is that the node providing the service must have a direct interface connection to the network. Although this requirement is generally true, a **DHCP Relay Agent** can be used to work around it. The DHCP Relay Agent must be directly connected to the network, but it will retransmit local DHCP messages to a remote DHCP service.

Although Cisco routers support static IPv4 addresses assignment as well, we usually want dynamic assignment. To achieve that on a Cisco router, one **DHCP pool** must be defined for each IPv4 network we want to offer the service on.

The DHCP pool is identified by an arbitrary administrative name, the **ip dhcp pool POOL-NAME** command can be used to create a new DHCP pool or edit an existing one. In will enter a specific sub-configuration level to manage that pool configuration, for instance:

```
(config)# ip dhcp pool NETWORK1
(dhcp-config)# network 192.168.5.0 255.255.255.0
```

The **network** command shown above associates the pool to a directly connected IPv4 network (192.168.5.0/24 on the example). The service assumes every valid node address within this network is available to be dynamically assigned to clients, addresses already in use on the network must be explicitly excluded.

With this information, the DHCP service is already capable of dynamically assigning IPv4 node addresses to clients and also inform them about the network address and network mask. Additional data is, nevertheless, required by clients, the **default-router** command settles the default gateway to be used by clients. The following example also shows how to set the default DNS domain, and DNS servers the clients should use.

```
(config)# ip dhcp pool NETWORK1
(dhcp-config)# network 192.168.5.0 255.255.255.0
(dhcp-config)# default-router 192.168.5.1
(dhcp-config)# domain-name dei.isep.ipp.pt
(dhcp-config)# dns-server 192.168.20.4
```

Node addresses that are being used for other purposes must be excluded from DHCP management, starting with the router own address, but including servers and other devices with manual IPv4 address configuration.

If fact, before assigning a new address, the DHCP service tests if anyone is replying to ICMP echo requests on that address, and skips that address if so.

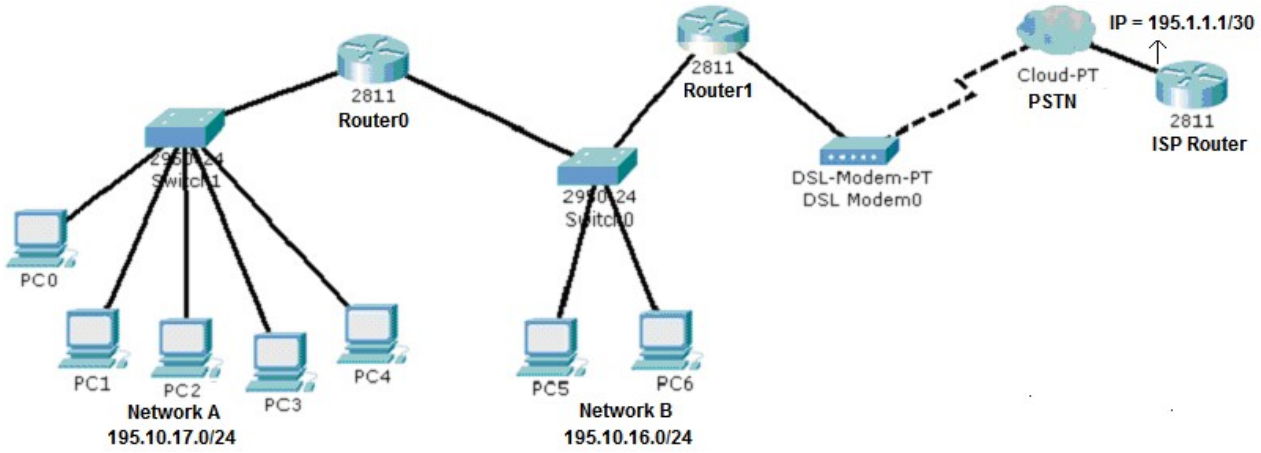
At general configuration-level, the **ip dhcp excluded-address** command allows the definition of one IPv4 address or a range of IPv4 addresses that should never be assigned to clients by DHCP, for instance:

```
(config)# ip dhcp excluded-address 192.168.5.1 192.168.5.100
```

Used together with the previous commands, this will make the DHCP service assign to clients only addresses between 192.168.5.101 and 192.168.5.254.

The **ip dhcp excluded-address** command may be used several times to exclude different addresses, possibly belonging to different DHCP pools.

3. Use Packet Tracer to create the following scenario



3.1. Define all routers connected interfaces IPv4 addresses

You can use any valid node address as far as it belongs to the connected IPv4 networks shown on the image. By tradition the network's first addresses are assigned to routers.

Do not assign IPv4 addresses to end nodes, they will be assigned by the DHCP service running in Router0.

3.2. Configure the DHCP service on Router0 to assign IPv4 address to all end nodes

Because nodes are spread in two networks, two DHCP pools are required.

Within each pool, set the correct default gateway each node must use (default-router command).

Don't forget to exclude from DHCP already in use addresses.

3.3. Create the required static routeing tables on each router

This scenario has an internet connection, thus, default routes must be settled in a way that will lead to the ISP Router all packets with locally unknown destination IPv4 addresses.

At ISP Router do default route can be defined, it should forward packets to next router on the internet side and we are not aware of it.

Notice that networks A and B can be aggregated into a single network address and mask.

3.4. Test ICMP echo requests between all nodes, including the ISP Router

They should all work.

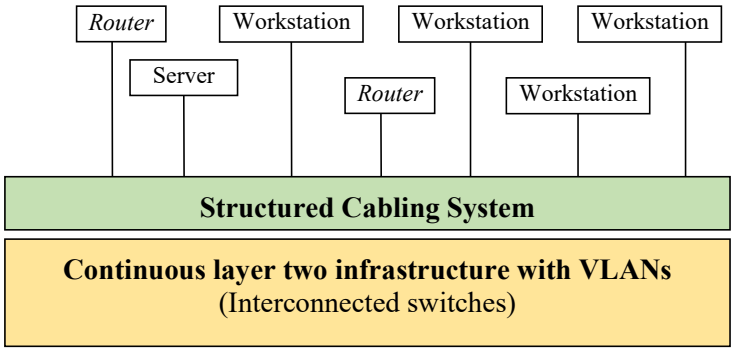
3.5. In simulation mode, send an ICMP echo request to a locally unknown IPv4 addresses

If everything is working as it is supposed to, those requests will reach the ISP Router and be rejected there.

4. Project 1 – VLAN based layer two platform

This project includes the need for a continuous layer two implementation covering the whole infrastructure. To achieve this, the layer two infrastructure is made of all the switches directly interconnected in trunk mode, with no breaks between them.

A continuous layer two guarantees the maximum flexibility because any point within the infrastructure can be assigned to any VLAN. In other words, VLANs can be drawn freely over the entire infrastructure.

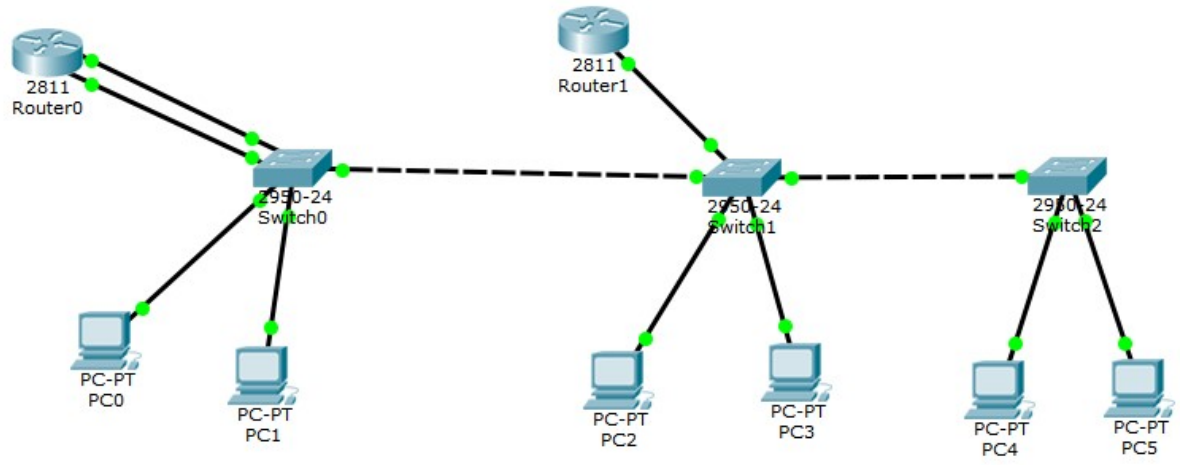


Under this perspective, the structured cabling system role is connecting switches to layer three devices like routers and end-nodes. Each layer three device connection is managed at layer two by using VLANs, thus, no physical handling of patch cords is required. Changing the VLAN a layer three device is connected to it's simply a matter of changing the VLAN assigned to a switch port.

If the layer two implementation is split into two or more areas with no layer two connection between them, then a VLAN defined in one area can never be propagated to the other area. This introduces a restriction to the desired flexibility in VLAN design over the infrastructure.

To better illustrate these concepts, let's perform a small practical exercise. **Concepts introduced in this class are to be deployed on Project 1 development.**

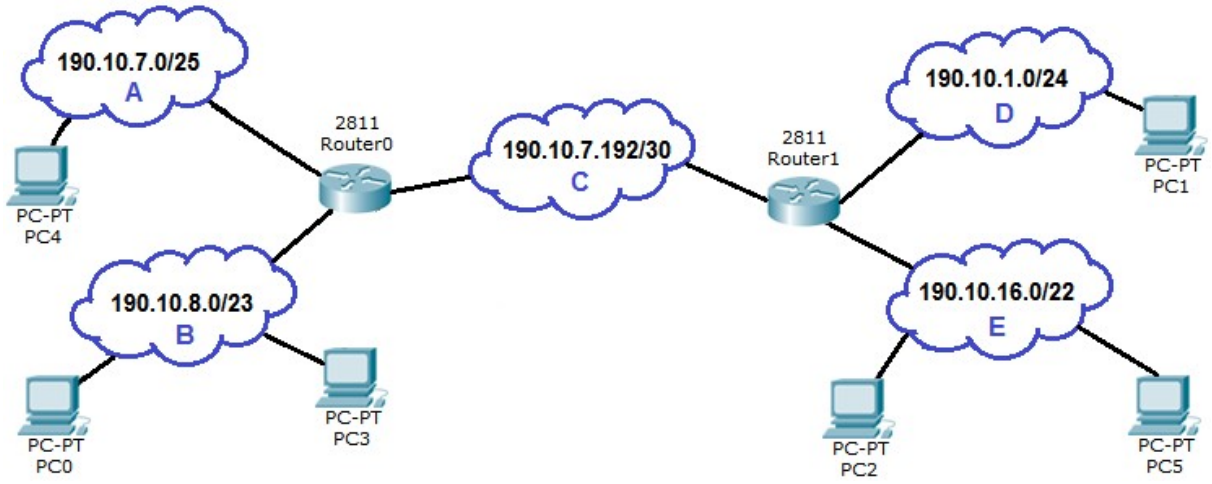
4.1. Use Packet Tracer to implement the following physical infrastructure



It looks rather odd! Router 1 has a single connection? Router 0 has two connections to the same switch?

The point is, physical connections don't mean much, as it all depends on VLANs.

4.2. Over the preceding infrastructure, use VLANs to define the following IPv4 networks



4.2.1. Define de required VLANs using VTP

There's not much to wonder about, for each independent IPv4 network a VLAN is required, so a total of five VLANs are necessary. From the image above we can establish the following table:

VLAN name	VLANID	IPv4 network
VLAN-A	100	190.10.7.0/25
VLAN-B	101	190.10.8.0/23
VLAN-C	102	190.10.7.192/30
VLAN-D	103	190.10.1.0/24
VLAN-E	104	190.10.16.0/22

Assigned VLANIDs are arbitrary, as far as they are unique and don't overlap others in use.

Here there are only three switches, the five VLANs could be manually created on each. However, VLAN Trunking Protocol (VTP) offers a better solution. By using VTP we can define all VLANs in a single switch (the VTP server) and spread them to all other switches (VTP clients). To works together, both the **VTP server** and the **VTP clients** must belong to the same **VTP domain**.

One switch must be elected to be the VTP server, say **Switch0**. Enter Switch0 CLI and set it as the VTP server for a VTP domain, say **rcomp** VTP domain.

```
(config)# vtp domain rcomp
(config)# vtp mode server
```

The other switches will be VTP clients on the **rcomp** VTP domain.

```
(config)# vtp domain rcomp
(config)# vtp mode client
```

From now on, any change on VLANs defined in Switch0 (VLAN database) gets propagated to Switch1 and Switch2.

So you can now use the Packet Tracer form to define the VLAN database on Switch0.

4.2.2. Ensure all VLANs are available on all switches

Every switch port connected to another switch must be in trunk-mode, so that corresponding VLANs are effectively interconnected between switches. On Cisco switches, ports are by default in dynamic mode, thus, if one end of the connection is manually changed to trunk-mode, the other end will automatically also change to trunk-mode.

4.2.3. Assign VLANs to switch ports connected to end nodes

These end nodes (PCs) are not VLAN-aware, for each PC check to which switch port it's connected to and assign to that port the appropriate VLAN in access-mode.

4.2.4. Assign VLANs to switch ports connected to routers

Router1 has a single connected physical interface, however, we need three network connections. The connected switch port must, therefore, be in trunk-mode.

Assuming **Router1** physically connected interface is **FastEthernet0/0** and addresses to be assigned to the router are **190.10.7.193/30** for VLAN-C, **190.10.1.1/24** for VLAN-D and **190.10.0.1/22** for VLAN-E. Configuration commands are:

```
(config)# interface FastEthernet0/0.1
(config-subif)# encapsulation dot1Q 102
(config-subif)# ip address 190.10.7.193 255.255.255.252

(config)# interface FastEthernet0/0.2
(config-subif)# encapsulation dot1Q 103
(config-subif)# ip address 190.10.1.1 255.255.255.0

(config)# interface FastEthernet0/0.3
(config-subif)# encapsulation dot1Q 104
(config-subif)# ip address 190.10.16.1 255.255.252.0
```

Concerning **Router0**, it has two connected physical interfaces and, as with **Router1**, three network connections are required. If physically connected interfaces are **FastEthernet0/0** and **FastEthernet0/1**, we can for instance use one interface for one VLAN and the other interface for the other two VLANs. Use the following commands:

```
(config)# interface FastEthernet0/0
(config-if)# ip address 190.10.7.194 255.255.255.252

(config)# interface FastEthernet0/1.1
(config-subif)# encapsulation dot1Q 100
(config-subif)# ip address 190.10.7.1 255.255.255.128

(config)# interface FastEthernet0/1.2
(config-subif)# encapsulation dot1Q 101
(config-subif)# ip address 190.10.8.1 255.255.254.0
```

Establish the correct configuration for each switch port these routers' interfaces are connected. Both in trunk-mode? Apply the correct VLAN configurations to the connected switch.

4.2.5. Use the two routers to offer the DHCP service on networks A, B, D, and E

Each router can serve only directly connected networks, so, for Router0 networks A and B, and for Router1 networks D and E.

On **Router0**:

```
(config)# ip dhcp excluded-address 190.10.7.1
(config)# ip dhcp excluded-address 190.10.8.1

(config)# ip dhcp pool NET-A
(dhcp-config)# default-router 190.10.7.1
(dhcp-config)# network 190.10.7.0 255.255.255.128

(config)# ip dhcp pool NET-B
(dhcp-config)# default-router 190.10.8.1
(dhcp-config)# network 190.10.8.0 255.255.254.0
```

On **Router1**:

```
(config)# ip dhcp excluded-address 190.10.1.1
(config)# ip dhcp excluded-address 190.10.16.1

(config)# ip dhcp pool NET-D
(dhcp-config)# default-router 190.10.1.1
(dhcp-config)# network 190.10.1.0 255.255.255.0

(config)# ip dhcp pool NET-E
(dhcp-config)# default-router 190.10.16.1
(dhcp-config)# network 190.10.16.0 255.255.252.0
```

Check that all end nodes receive their configuration from the DHCP service. Confirm the IPv4 network each node belongs to.

4.3. Move end nodes between VLANs

Let's move PC0 to network A and PC2 to network D.

Thanks to VLANs no physical connections changes are necessary, all is required is changing the VLAN assigned to the corresponding switch port.

Force DHCP clients on PC0 and PC2 to request new configuration data and confirm they have moved to the desired IPv4 network.