ESCOLA
SUPERIOR
DE TECNOLOGIA
E GESTÃO

P.PORTO

REDES DE COMPUTADORES I – APRESENTAÇÃO DA UNIDADE CURICULAR

Network Services

- *DHCP*
- *DNS*
- *NTP*

Dynamic Host Configuration Protocol (DHCP): Ports 67/68

Bootstrap Protocol (BOOTP)

- BOOTP as a method of assigning IP address, subnet mask, and default gateway information to diskless workstations

Dynamic Host Configuration Protocol (DHCP)

- Protocol that dynamically assigns IP address information (for example, IP address, subnet mask, DNS server's IP address, and default gateway's IP address) to network devices.
- more robust solution to IP address assignment than does BOOTP

Dynamic Host Configuration Protocol (DHCP): Ports 67/68

DHCPv4 Operation

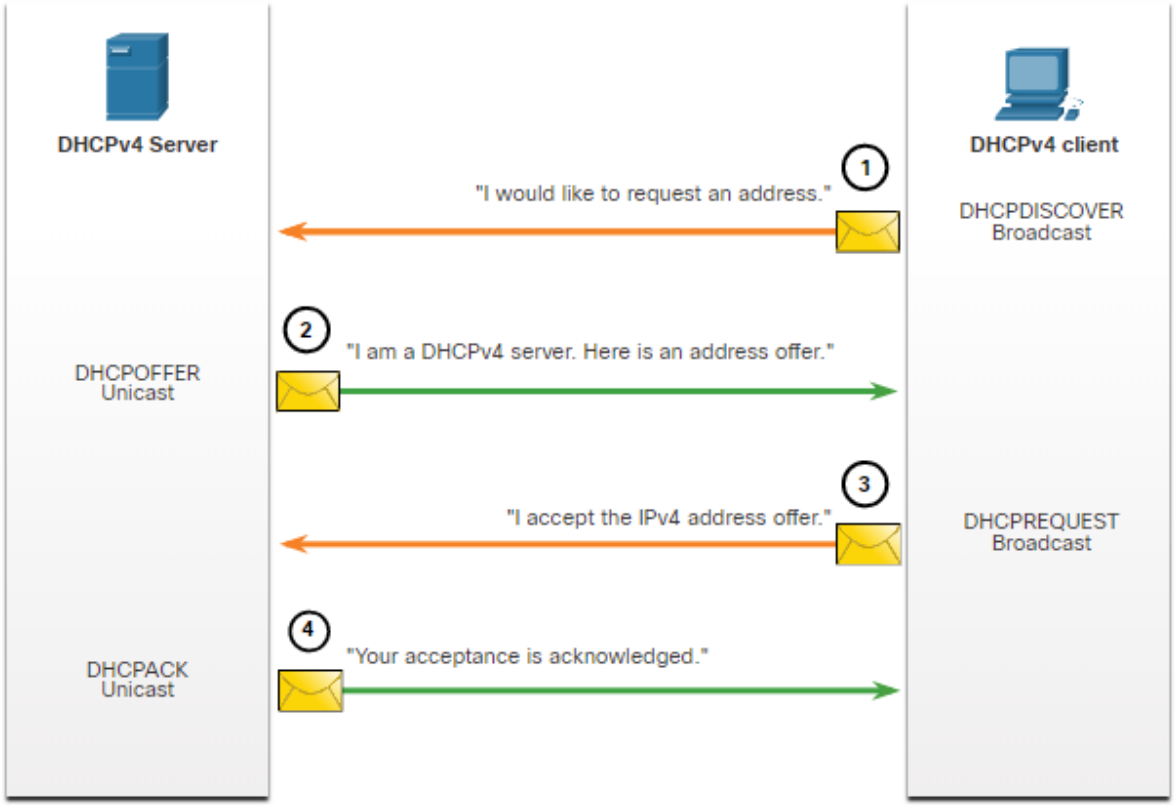
DHCPv4 works in a client/server mode. When a client communicates with a DHCPv4 server, the server assigns or leases an IPv4 address to that client.

- The client connects to the network with that leased IPv4 address until the lease expires. The client must contact the DHCP server periodically to extend the lease.
- This lease mechanism ensures that clients that move or power off do not keep addresses that they no longer need.
- When a lease expires, the DHCP server returns the address to the pool where it can be reallocated as necessary.

DHCPv4 Concepts
Steps to Obtain a Lease

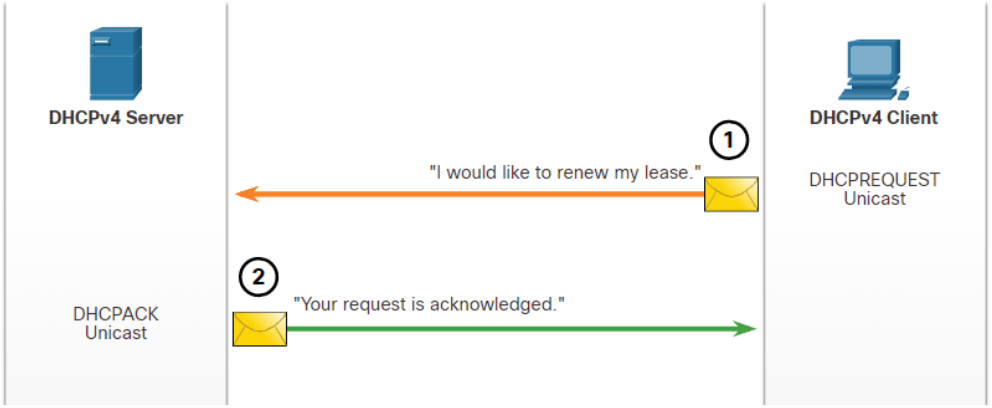
When the client boots (or otherwise wants to join a network), it begins a four-step process to obtain a lease:

1. DHCP Discover (DHCPDISCOVER)
2. DHCP Offer (DHCPOFFER)
3. DHCP Request (DHCPREQUEST)
4. DHCP Acknowledgment (DHCPACK)



DHCPv4 Concepts
Steps to Renew a Lease

Prior to lease expiration, the client begins a two-step process to renew the lease with the DHCPv4 server, as shown in the figure:



1. DHCP Request (DHCPREQUEST)

Before the lease expires, the client sends a DHCPREQUEST message directly to the DHCPv4 server that originally offered the IPv4 address. If a DHCPACK is not received within a specified amount of time, the client broadcasts another DHCPREQUEST so that one of the other DHCPv4 servers can extend the lease.

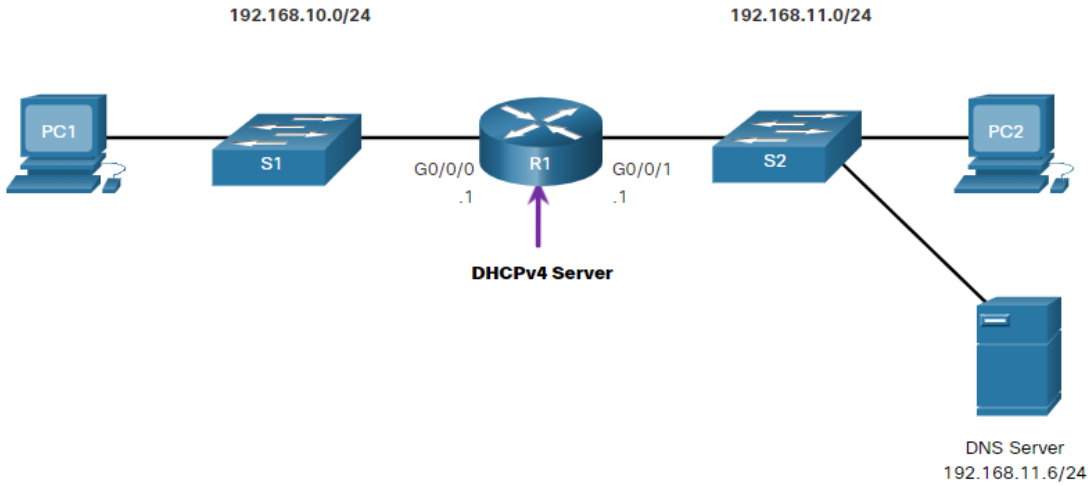
2. DHCP Acknowledgment (DHCPACK)

On receiving the DHCPREQUEST message, the server verifies the lease information by returning a DHCPACK.

Note: These messages (primarily the DHCPOFFER and DHCPACK) can be sent as unicast or broadcast according to IETF RFC 2131.

Configure a Cisco IOS DHCPv4 Server
Cisco IOS DHCPv4 Server

Now you have a basic understanding of how DHCPv4 works and how it can make your job a bit easier. A Cisco router running Cisco IOS software can be configured to act as a DHCPv4 server. The Cisco IOS DHCPv4 server assigns and manages IPv4 addresses from specified address pools within the router to DHCPv4 clients.



Configure a Cisco IOS DHCPv4 Server
Steps to Configure a Cisco IOS DHCPv4 Server

Use the following steps to configure a Cisco IOS DHCPv4 server:

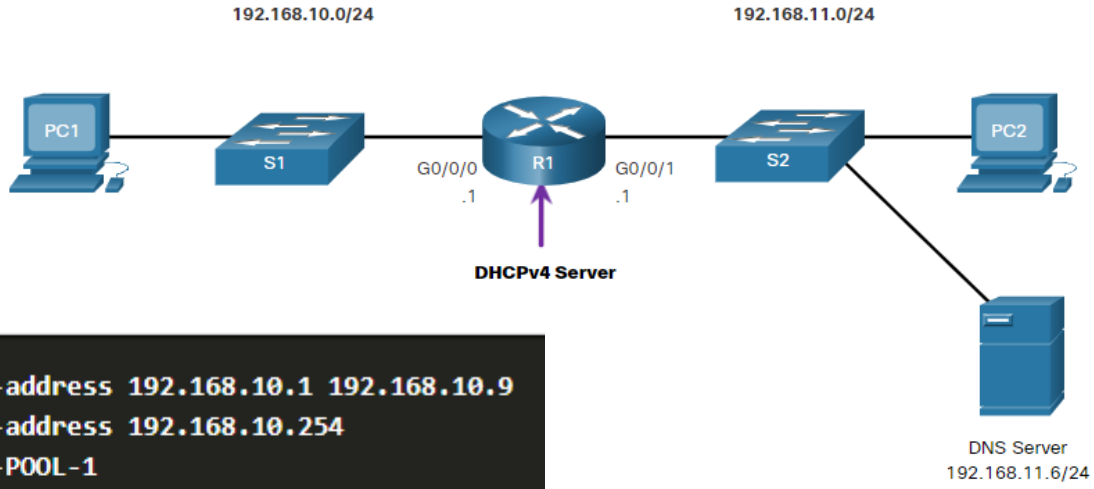
- Step 1. Exclude IPv4 addresses. A single address or a range of addresses can be excluded by specifying the *low-address* and *high-address* of the range. Excluded addresses should be those addresses that are assigned to routers, servers, printers, and other devices that have been, or will be, manually configured. You can also enter the command multiple times. The command is **ip dhcp excluded-address** *low-address [high-address]*
- Step 2. Define a DHCPv4 pool name. The **ip dhcp pool** *pool-name* command creates a pool with the specified name and puts the router in DHCPv4 configuration mode, which is identified by the prompt **Router(dhcp-config)#**.

Configure a Cisco IOS DHCPv4 Server
Steps to Configure a Cisco IOS DHCPv4 Server (Cont.)

- Step 3. Configure the DHCPv4 pool. The address pool and default gateway router must be configured. Use the **network** statement to define the range of available addresses. Use the **default-router** command to define the default gateway router. These commands and other optional commands are shown in the table.

Task	IOS Command
Define the address pool.	**network** *network-number* [*mask* | / *prefix-length*]
Define the default router or gateway.	**default-router** address [*address2....address8*]
Define a DNS server.	**dns-server** *address* [*address2...address8*]
Define the domain name.	**domain-name** *domain*
Define the duration of the DHCP lease.	**lease** {*days* [*hours* [*minutes*]] | **infinite**}
Define the NetBIOS WINS server.	**netbios-name-server** *address* [*address2...address8*]

Configure a Cisco IOS DHCPv4 Server Configuration Example




```
R1(config)# ip dhcp excluded-address 192.168.10.1 192.168.10.9
R1(config)# ip dhcp excluded-address 192.168.10.254
R1(config)# ip dhcp pool LAN-POOL-1
R1(dhcp-config)# network 192.168.10.0 255.255.255.0
R1(dhcp-config)# default-router 192.168.10.1
R1(dhcp-config)# dns-server 192.168.11.5
R1(dhcp-config)# domain-name example.com
R1(dhcp-config)# end
R1#
```

Configure a Cisco IOS DHCPv4 Server
DHCPv4 Verification

Use the commands in the table to verify that the Cisco IOS DHCPv4 server is operational.

Command	Description
show running-config | section dhcp	Displays the DHCPv4 commands configured on the router.
show ip dhcp binding	Displays a list of all IPv4 address to MAC address bindings provided by the DHCPv4 service.
show ip dhcp server statistics	Displays count information regarding the number of DHCPv4 messages that have been sent and received

Configure a Cisco IOS DHCPv4 Server
Verify DHCPv4 is Operational

Verify the DHCPv4 Configuration: As shown in the example, the **show running-config | section dhcp** command output displays the DHCPv4 commands configured on R1. The **| section** parameter displays only the commands associated with DHCPv4 configuration.

```
R1# show running-config | section dhcp
ip dhcp excluded-address 192.168.10.1 192.168.10.9
ip dhcp excluded-address 192.168.10.254
ip dhcp pool LAN-POOL-1
 network 192.168.10.0 255.255.255.0
 default-router 192.168.10.1
 dns-server 192.168.11.5
 domain-name example.com
```

Configure a Cisco IOS DHCPv4 Server
Verify DHCPv4 is Operational (Cont.)

Verify DHCPv4 Bindings: As shown in the example, the operation of DHCPv4 can be verified using the show ip dhcp binding command. This command displays a list of all IPv4 address to MAC address bindings that have been provided by the DHCPv4 service.

```
R1# show ip dhcp binding
Bindings from all pools not associated with VRF:
IP address      Client-ID/              Lease expiration        Type       State      Interface
                Hardware address/
                User name
192.168.10.10   0100.5056.b3ed.d8       Sep 15 2019 8:42 AM    Automatic  Active
GigabitEthernet0/0/0
```

Configure a Cisco IOS DHCPv4 Server
Verify DHCPv4 is Operational (Cont.)

Verify DHCPv4 Statistics: The output of the show ip dhcp server statistics is used to verify that messages are being received or sent by the router. This command displays count information regarding the number of DHCPv4 messages that have been sent and received.

```
R1# show ip dhcp server statistics
Memory usage         19465
Address pools        1
Database agents      0
Automatic bindings   2
Manual bindings      0
Expired bindings     0
Malformed messages   0
Secure arp entries   0
Renew messages       0
Workspace timeouts   0
Static routes        0
Relay bindings       0
Relay bindings active        0
Relay bindings terminated    0
Relay bindings selecting     0
Message              Received
BOOTREQUEST          0
DHCPDISCOVER         4
DHCPREQUEST          2
DHCPDECLINE          0
DHCPRELEASE          0
DHCPINFORM           0
```

Configure a Cisco IOS DHCPv4 Server
Verify DHCPv4 is Operational (Cont.)

Verify DHCPv4 Client Received IPv4 Addressing: The **ipconfig /all** command, when issued on PC1, displays the TCP/IP parameters, as shown in the example. Because PC1 was connected to the network segment 192.168.10.0/24, it automatically received a DNS suffix, IPv4 address, subnet mask, default gateway, and DNS server address from that pool. No DHCP-specific router interface configuration is required. If a PC is connected to a network segment that has a DHCPv4 pool available, the PC can obtain an IPv4 address from the appropriate pool automatically.

```
C:\Users\Student> ipconfig /all
Windows IP Configuration
   Host Name . . . . . . . . . . . . : ciscolab
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
Ethernet adapter Ethernet0:
   Connection-specific DNS Suffix  . : example.com
   Description . . . . . . . . . . . : Realtek PCIe GBE Family Controller
   Physical Address. . . . . . . . . : 00-05-9A-3C-7A-00
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv4 Address. . . . . . . . . . . : 192.168.10.10
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained  . . . . . . . . . : Saturday, September 14, 2019 8:42:22AM
   Lease Expires   . . . . . . . . . : Sunday, September 15, 2019 8:42:22AM
   Default Gateway . . . . . . . . . : 192.168.10.1
   DHCP Server . . . . . . . . . . . : 192.168.10.1
   DNS Servers . . . . . . . . . . . : 192.168.11.5
```

Configure a Cisco IOS DHCPv4 Server
Disable the Cisco IOS DHCPv4 Server

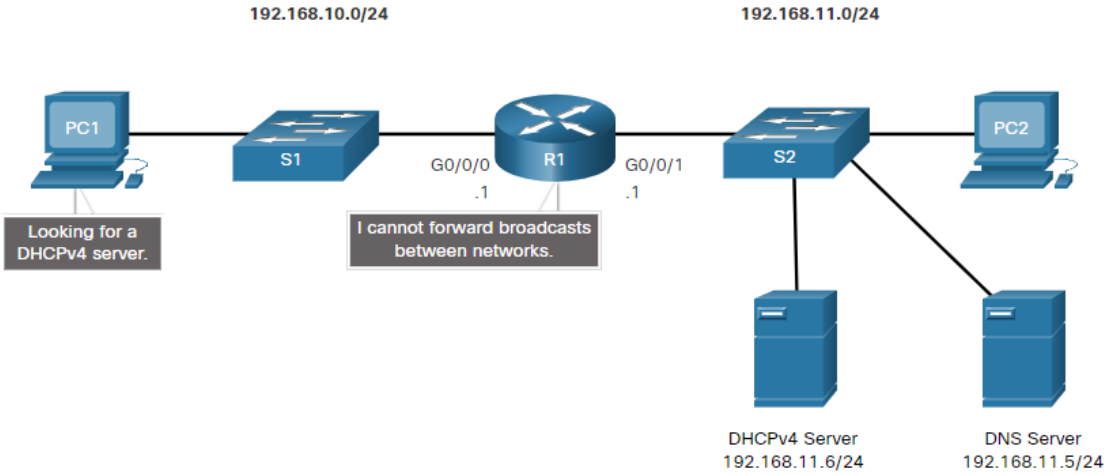
The DHCPv4 service is enabled by default. To disable the service, use the **no service dhcp** global configuration mode command. Use the **service dhcp** global configuration mode command to re-enable the DHCPv4 server process, as shown in the example. Enabling the service has no effect if the parameters are not configured.

Note: Clearing the DHCP bindings or stopping and restarting the DHCP service may result in duplicate IP addresses being temporarily assigned on the network.

```
R1(config)# no service dhcp
R1(config)# service dhcp
R1(config)#
```

Configure a Cisco IOS DHCPv4 Server
DHCPv4 Relay

- In a complex hierarchical network, enterprise servers are usually located centrally. These servers may provide DHCP, DNS, TFTP, and FTP services for the network. Network clients are not typically on the same subnet as those servers. In order to locate the servers and receive services, clients often use broadcast messages.
- In the figure, PC1 is attempting to acquire an IPv4 address from a DHCPv4 server using a broadcast message. In this scenario, R1 is not configured as a DHCPv4 server and does not forward the broadcast. Because the DHCPv4 server is located on a different network, PC1 cannot receive an IP address using DHCP. R1 must be configured to relay DHCPv4 messages to the DHCPv4 server.



Configure a Cisco IOS DHCPv4 Server
DHCPv4 Relay (Cont.)

- Configure R1 with the **ip helper-address** *address* interface configuration command. This will cause R1 to relay DHCPv4 broadcasts to the DHCPv4 server. As shown in the example, the interface on R1 receiving the broadcast from PC1 is configured to relay DHCPv4 address to the DHCPv4 server at 192.168.11.6.
- When R1 has been configured as a DHCPv4 relay agent, it accepts broadcast requests for the DHCPv4 service and then forwards those requests as a unicast to the IPv4 address 192.168.11.6. The network administrator can use the **show ip interface** command to verify the configuration.

```
R1(config)# interface g0/0/0
R1(config-if)# ip helper-address 192.168.11.6
R1(config-if)# end
R1#
```

```
R1# show ip interface g0/0/0
GigabitEthernet0/0/0 is up, line protocol is up
  Internet address is 192.168.10.1/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is 192.168.11.6
(output omitted)
```

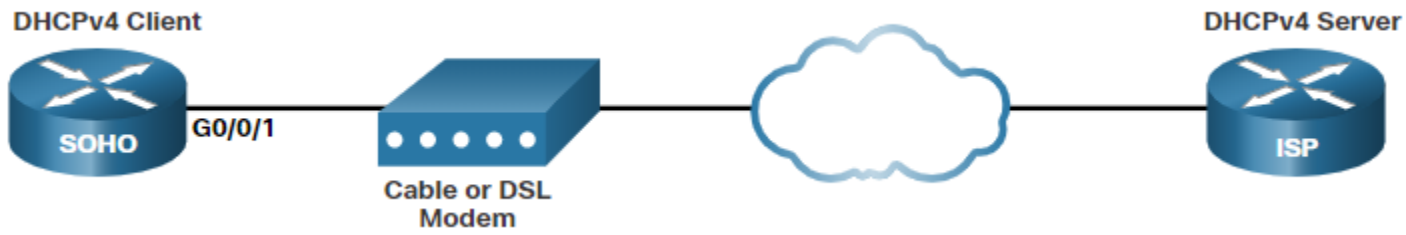
LAB

- Configure DHCPv4
  - 7.2.10 Packet Tracer - Configure DHCPv4

Configure a DHCPv4 Client
Cisco Router as a DHCPv4 Client

There are scenarios where you might have access to a DHCP server through your ISP. In these instances, you can configure a Cisco IOS router as a DHCPv4 client.

- Sometimes, Cisco routers in a small office or home office (SOHO) and branch sites have to be configured as DHCPv4 clients in a similar manner to client computers. The method used depends on the ISP. However, in its simplest configuration, the Ethernet interface is used to connect to a cable or DSL modem.
- To configure an Ethernet interface as a DHCP client, use the **ip address dhcp interface** configuration mode command.
- In the figure, assume that an ISP has been configured to provide select customers with IP addresses from the 209.165.201.0/27 network range after the G0/0/1 interface is configured with the **ip address dhcp** command.



Configure a DHCPv4 Client Configuration Example

- To configure an Ethernet interface as a DHCP client, use the **ip address dhcp** interface configuration mode command, as shown in the example. This configuration assumes that the ISP has been configured to provide select customers with IPv4 addressing information.
- The **show ip interface g0/1** command confirms that the interface is up and that the address was allocated by a DHCPv4 server.

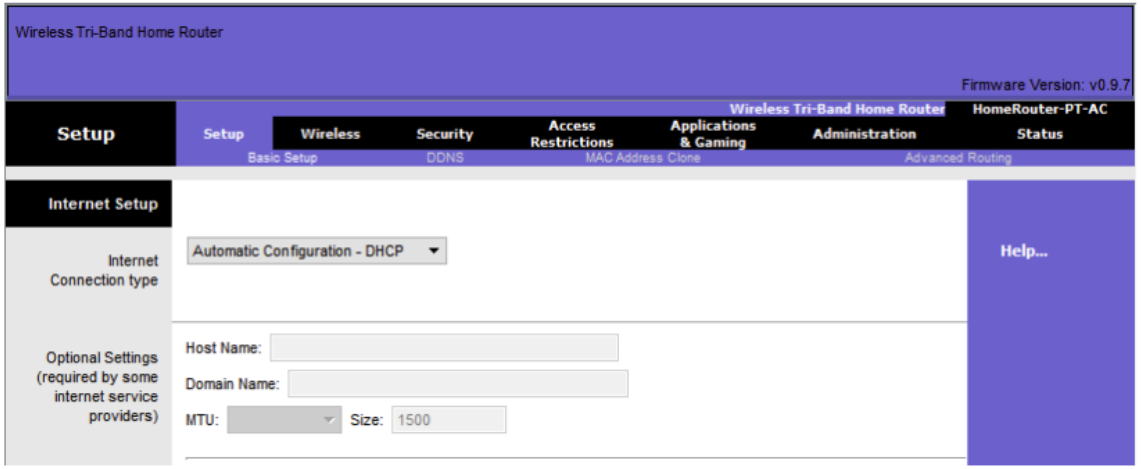
```
SOHO(config)# interface G0/0/1
SOHO(config-if)# ip address dhcp
SOHO(config-if)# no shutdown
Sep 12 10:01:25.773: %DHCP-6-ADDRESS_ASSIGN: Interface GigabitEthernet0/0/1 assigned DHCP address
209.165.201.12, mask 255.255.255.224, hostname SOHO
```

```
SOHO# show ip interface g0/0/1
GigabitEthernet0/0/1 is up, line protocol is up
  Internet address is 209.165.201.12/27
  Broadcast address is 255.255.255.255
  Address determined by DHCP
(output omitted)
```

Configure a DHCPv4 Client
Home Router as a DHCPv4 Client

Home routers are typically already set to receive IPv4 addressing information automatically from the ISP. This is so that customers can easily set up the router and connect to the internet.

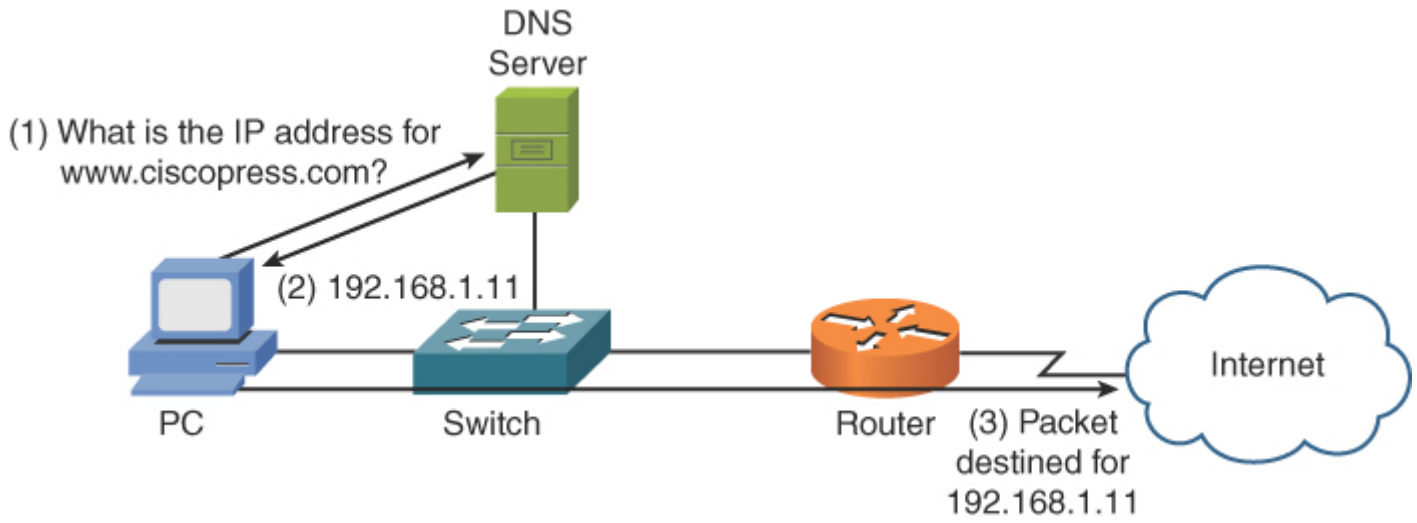
- For example, the figure shows the default WAN setup page for a Packet Tracer wireless router. Notice that the internet connection type is set to **Automatic Configuration – DHCP**. This selection is used when the router is connected to a DSL or cable modem and acts as a DHCPv4 client, requesting an IPv4 address from the ISP.
- Various manufacturers of home routers will have a similar setup.



Domain Name System (DNS): Port 53

Domain Name System (DNS):

- system that resolves a domain name (for example, www.sapo.pt) to a corresponding IP address (for example, 213.13.146.142).



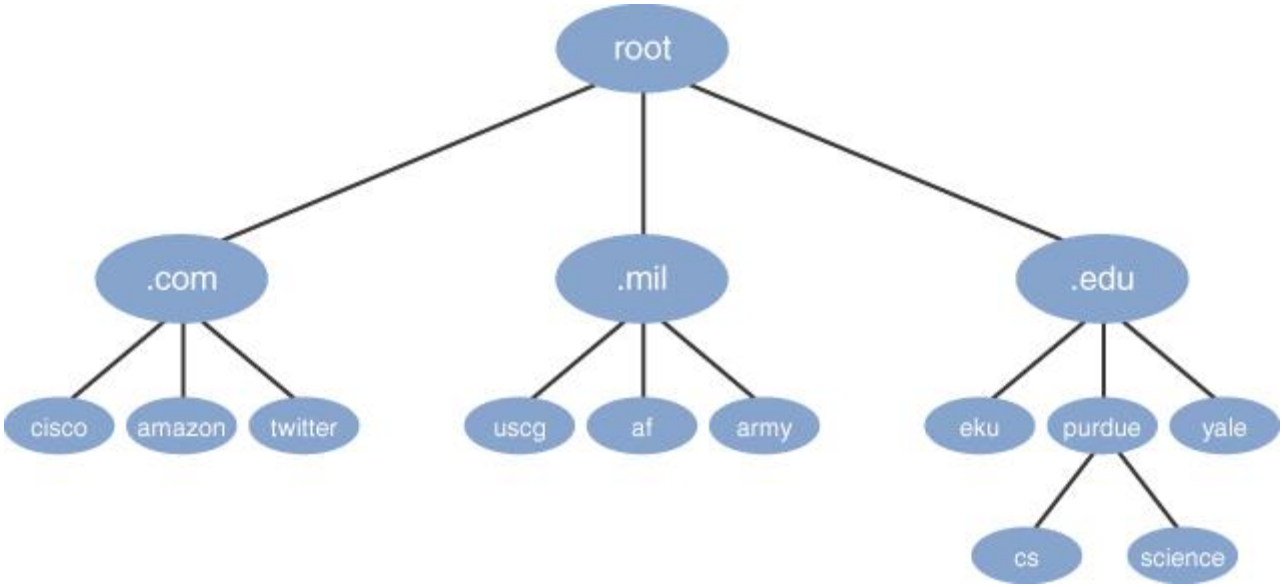
Domain Name System (DNS): Port 53

Fully Qualified Domain Name (FQDN)

- FQDN uniquely identifies a system within the Domain Name System (DNS) hierarchy, which is a globally distributed system that translates human-readable domain names into IP addresses
- FQDN consists of two main parts:
  1. Hostname: The name of the specific computer, server, or host within a domain. For example, in the FQDN "mail.example.com", the hostname is "mail".
  2. Domain name: The larger organizational structure under which the host resides. In the example "mail.example.com", the domain name is "example.com".

Domain Name System (DNS): Port 53

Fully Qualified Domain Name (FQDN)



Hierarchical Domain Name Structure

Domain Name System (DNS): Port 53

DNS server types:

- Root DNS servers: These authoritative name servers serve the DNS root zone; they are a network of hundreds of servers in many countries around the world.
- Internal DNS servers: These servers exist inside organization to resolve the names of private hosts and servers within the organizations. These servers can also forward requests for outside resources to the appropriate external DNS servers when internal clients need to access external resources.
- External DNS servers: These servers reside outside an organization (typically on the public Internet) and can resolve names of systems that are located outside the organization.
- Authoritative name server: This DNS server is usually the last step in the journey for an IP address. The authoritative name server contains information specific to the domain name it serves (for example, ajsnetworking.com). The authoritative name server is able to resolve queries thanks to the records it contains.

Domain Name System (DNS): Port 53

DNS record types

- DNS records stored in a database that include the actual DNS names and appropriate associated IP addresses.

Record Type	Description
A	An address record (that is, A record) maps a hostname to an IPv4 address.
AAAA	An IPv6 address record (that is, AAAA record) maps a hostname to an IPv6 address.
CNAME	A canonical name record (that is, CNAME record) is an alias of an existing record that allows multiple DNS records to map to the same IP address.

Domain Name System (DNS): Port 53

MX	A mail record (that is, MX record) maps a domain name to an email (or message transfer agent) server for that domain.
NS	A name server record (that is, NS record) delegates a DNS zone to use the given authoritative name server.
PTR	A pointer record (that is, PTR record) points to a canonical name. A PTR record is commonly used when performing a reverse DNS lookup to determine what domain name is associated with a known IP address.

Domain Name System (DNS): Port 53

SOA	A start of authority record (that is, SOA record) provides authoritative information about a DNS zone, such as email contact information for the zone's administrator, the zone's primary name server, and various refresh timers.
SRV	A service location record (that is, SRV record) is used for newer protocols instead of creating protocol-specific records such as MX records.
TXT	A text record (that is, TXT record) originally for arbitrary human-readable text in a DNS record. Since the early 1990s, however, this record has carried machine-readable data, such as data specified by RFC 1464, opportunistic encryption, Sender Policy Framework (SPF), or DomainKeys Identified Email (DKIM).

Domain Name System (DNS): Port 53

SOA	A start of authority record (that is, SOA record) provides authoritative information about a DNS zone, such as email contact information for the zone's administrator, the zone's primary name server, and various refresh timers.
SRV	A service location record (that is, SRV record) is used for newer protocols instead of creating protocol-specific records such as MX records.
TXT	A text record (that is, TXT record) originally for arbitrary human-readable text in a DNS record. Since the early 1990s, however, this record has carried machine-readable data, such as data specified by RFC 1464, opportunistic encryption, Sender Policy Framework (SPF), or DomainKeys Identified Email (DKIM).

Network Time Protocol (NTP): Port 123

Network Time Protocol (NTP):

- Protocol that strives to ensure that network devices (including client systems) have the correct time and date. NTP uses port 123.

NTP three main components:

- Client: Your network device is typically the NTP client and is consuming the correct time from an NTP server system.
- Server: The network node that provides the correct time to NTP clients. The most common servers these days are located regionally on the Internet.
- Stratum: The stratum is an important value in NTP operations. It is like a hop count and measures how far the client is from the accurate time source. The larger the stratum value, the more chance the time on the client could be inaccurate because it is more hops away from the accurate time source.

Bibliografia

- SEQUEIRA, Anthony. *CompTIA Network+ N10-008 Cert Guide*. Pearson IT Certification, 2021.
- ODOM, Wendell. *CCNA 200-301 Official Cert Guide, Volume 2*. Cisco Press, 2019.
- ODOM, W. CCNA 200-301, Volume 1 Official Cert Guide. 2019.
- Cisco Netacad Course Resources