Network Services 1

2019-2020

Licenciatura em Engenharia Informática

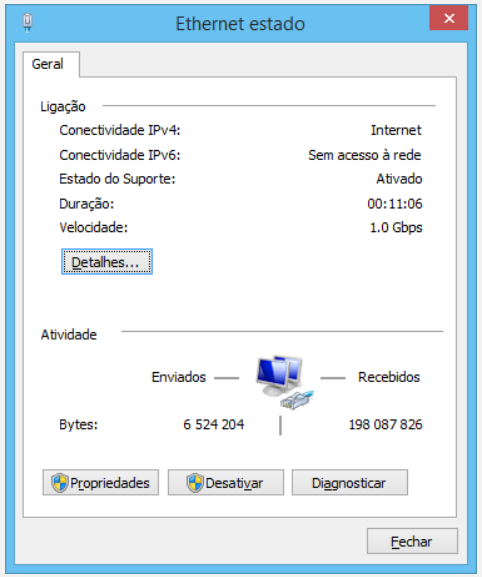
Ramo de Redes e Administração de Sistemas

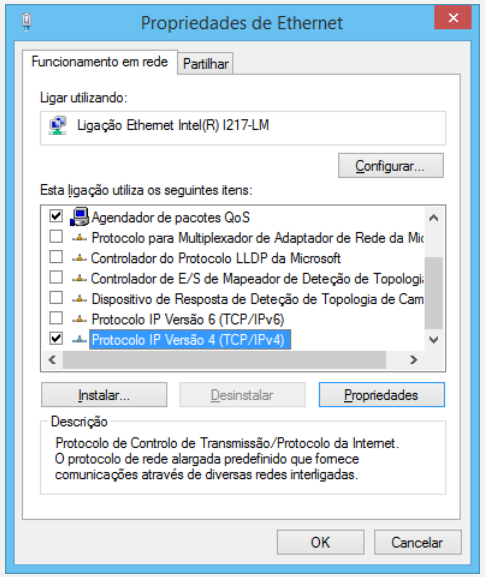
IP Addressing

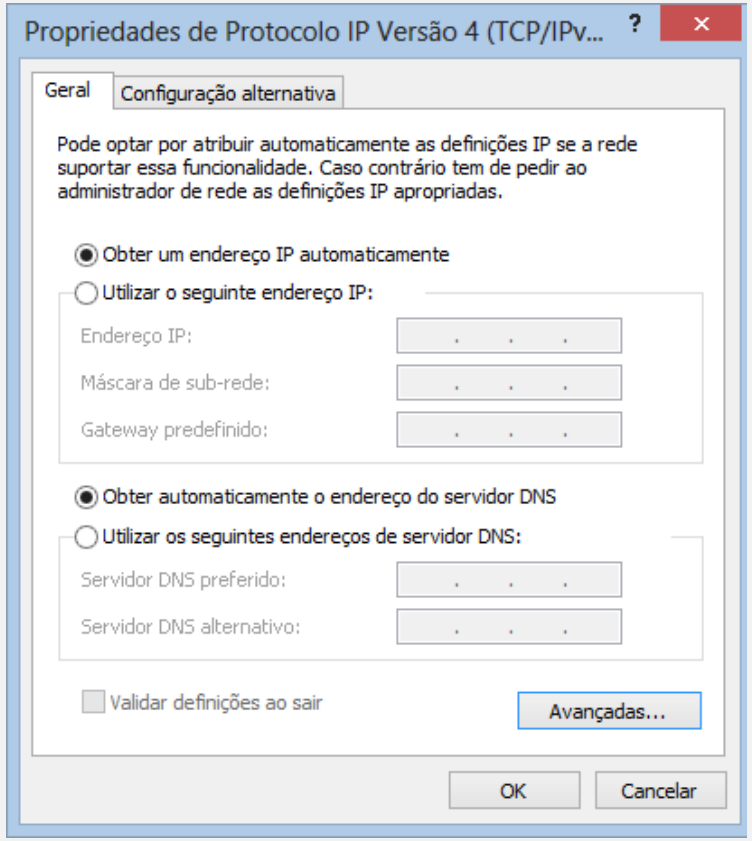
School Year 2019-2020

IP Addressing

- The main parameters that must be configured for the TCP / IP protocol to work correctly are:
  - IP Address
  - Subnet Mask
  - Default Gateway
  - IP address of one or more DNS servers





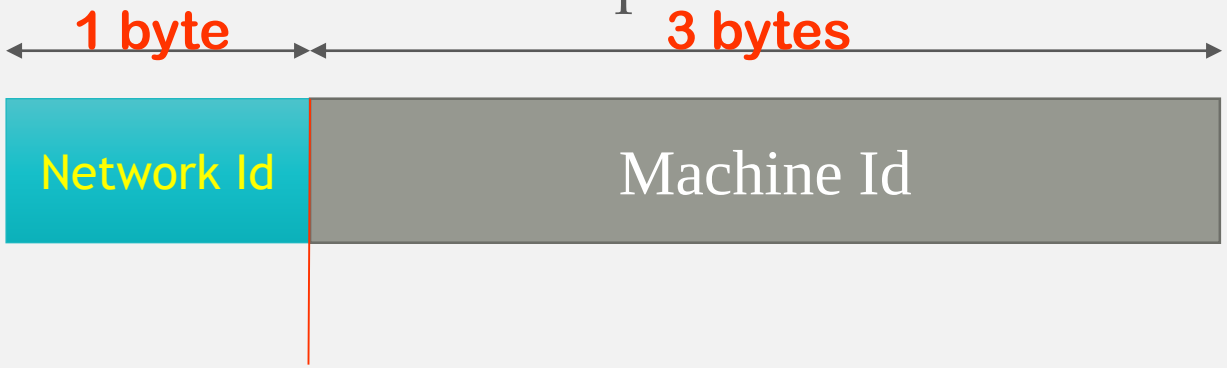


IP Addressing

- Each machine is identified by an IP address.
- In the same network, this address is **unique** to each machine and therefore can not duplicate this identification.
- As a residential postal address that has a standard format consisting of two parts (street name and house number), each IP address is separated internally into two parts:
  - **network identification**
  - **machine identification**

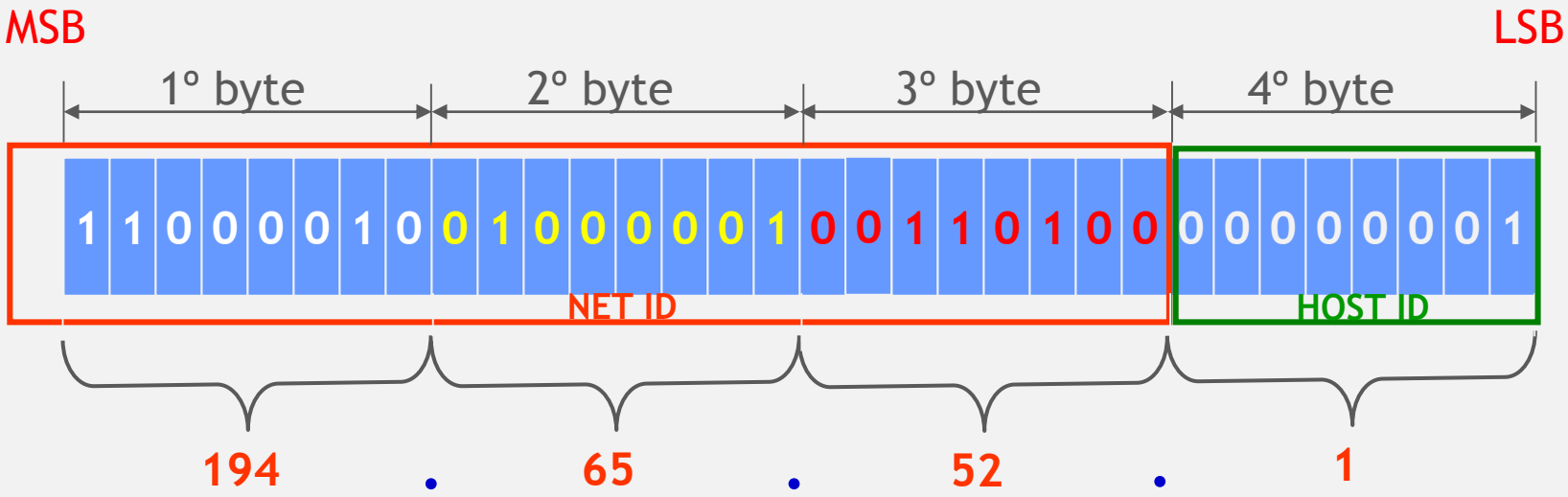
IP Addressing v4

- IP addresses V4 have a fixed size of 4 bytes (32 bits).
  - For example 192.168.1.1
- The IPv6 addresses (296 times the IPv4 address space) consist of 128 bits and are presented in 8 groups of 4 hexadecimal digits separated by ':'.
  - For example. 1234: 5678: 90AB: CDEF: FEDC: BA09: 8765: 4321.
- In the case of IP V4 there is a rigid division of network and machine identification. Consider the example:



IP Addressing v4

- The "dotted decimal" notation of the IP address is based on four decimal numbers from 0 to 255, separated by dots.
- Each number corresponds to the decimal representation of one of the 4 bytes of the IP address.

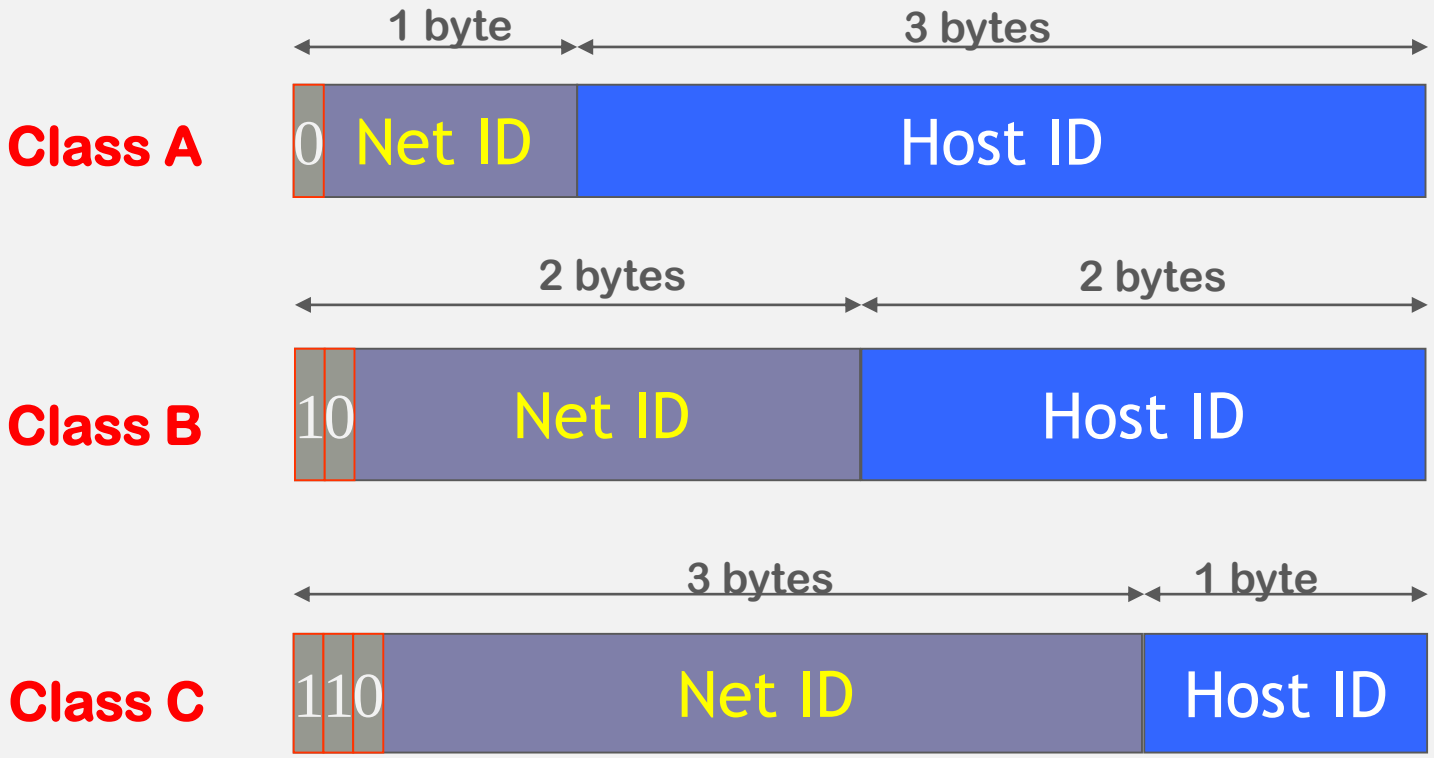


- $194 = 2^7*1+2^6*1+2^5*0+2^4*0+2^3*0+2^2*0+2^1*1+2^0*0 = 128+64+2=194$
- We can define this network as being 194.65.52.0/24 where 24 (3 * 8) defines the number of bits to be used in the network identification. Let's see this in more detail ...

IP Addressing v4

- Division of the address space in 3 classes:
  - Class A
  - Class B
  - Class C
- Purpose for this division is the need for **scalability** and **flexibility** of the addressing structure to use.
- The viral growth of the Internet implied a more structured analysis of the addressing to use and the first step was its division into classes.

IP Addressing v4



IP Addressing v4

- There are reserved addresses for special effects that can not be assigned to hosts:
  - All bits of the host id a 1 - Broadcast address (when a device sends a message to all devices on the network)
  - All bits of the host id to 0 - Address that identifies the network
- For example:
  - in network 192.168.1.0 (class C) there are 256 available addresses. From 192.168.01.0 to 192.168.1.255. As the first is used to designate the network and the last one is the broadcast address are only available for machines from 192.168.0.1 to 192.168.0.254 ie 254.
- Thus we can say that in a network we have $2^{\text{No of host bits}} - 2$ addresses available for peripheral machines / equipment.

IP Addressing v4

- Address space by class:

Class	1 byte	Nº of Networks	Nº of machines in network
A	0 - 126	127 (2^7 – 2)	16.777.214 (^{24}-2)
B	128 - 191	16.384 (2^{14})	65.534 (2^{16}-2)
C	192 - 223	2.097.152 (2^{21})	254 (2^8-2)

IP Addressing v4

- What network does 192.168.200.225 belong to? Can we say it to a class C. But if it has subnets? Is the answer so easy?
- For an address to be correctly defined, you must indicate how many bits are part of the network and devices. This is done by the **netmask**!
- The netmask:
  - Indicates the boundary between the network and host ID.
  - Generally, 255 indicates the IP address portion of the network, and a value of 0 indicates the address part for the host.
  - It also consists of 32 bits grouped together in 1 byte each.

IP Addressing v4

- The binary 1 in the network mask indicates that this bit belongs to the network ID and the binary 0 indicates that it belongs to the device.
- Here's how:
  - Class A - 255.0.0.0
  - Class B - 255.255.0.0
  - Class C - 255.255.255.0
- The mask can be represented in the same format as the four-byte IP address separated by dots, or in the slash (/) format. In this format we explain the number of bits used in the network identification.
- Here's how:
  - Class A - / 8
  - Class B - / 16
  - Class C - / 24

Public Address vs. Private Address

- Problem "*With the growth of the Internet, there are not enough addresses to connect all the machines*."
- One way to solve this problem was to establish a set of private use addresses to put on machines without Internet access (private addresses).
- The addresses used on the Internet are public addresses.

Private Address

- Private networks use a specific set of addresses. Here's how:

Class	From…	…To
A	10.0.0.0	10.255.255.255
B	172.16.0.0	172.31.255.255
C	192.168.0.0	192.168.255.255

Private Address

- Private addresses can not be "passed" to the Internet.
- So can not internal network devices communicate over the Internet?

- Yes!!! And one of the possible solutions is ...

Private Address

- Its use is not subject to licensing.
- Routers should not propagate information about these networks to the Internet.
- Traffic with private origin and destination should not use the Internet.
- Reference to private addresses should not be advertised (DNS public).
- Use of NAT to guarantee access to the Internet (this solution will be studied in future classes).

Sub-Addresses

- Another solution to "save" addresses is sub-addressing which is no more than the subdivision of an IP addressing class into a smaller set of networks.
- How many subnets can we have?
  - $N = 2^X$ where X represents the number of bits that were used by host id.
- How many hosts do we have for each subnet?
  - $N = 2^X-2$ where X represents the number of bits at "0" of the netmask. In each network everything at 0 indicates the network and all at 1 the broadcast, hence the ratio of -2.
- What is the broadcast address of the subnetworks?
  - This is the address that precedes the next subnet. From the address of the subnet put all hosts bits to "1"
- What are the valid hosts on a subnet?
  - Those whose host id does not have all the bits neither "1" nor "0"

Sub-Addresses

N° bits Network Id	Subnet mask	N° of networks	N° os hosts
25 (24+1)	255.255.255.128	2 (2^1)	126 (2^7-2)
26 (24+2)	255.255.255.192	4 (2^2)	62 (2^6-2)
27 (24+3)	255.255.255.224	8 (2^3)	30
28 (24+4)	255.255.255.240	16 (2^4)	14
29	255.255.255.248	32	6
30	255.255.255.252	64	2
31	255.255.255.254	128	0

Sub-Addresses

- Consider now the example (193.137.78.0 255.255.255.224) we have:

Number of bits for the host	5 (32-27)
Number of bits for the network	27 (24+3)
Network	193.137.78.0/27
Number of subnets	2^3=8
No. of hosts per network	2^5-2=30

Network	Subnet	1º Host	Last host	Broadcast
1ª subnet	192.137.78.0	192.137.78.1	192.168.78.30	192.1637.78.31
2ª subnet	193.137.78.32	193.137.78.33	193.137.78.62	193.137.78.63
3ª subnet	193.137.78.64	193.137.78.65	193.137.78.94	193.137.78.95
4ª subnet	193.137.78.96	193.137.78.97	193.137.78.126	193.137.78.127
5ª subnet	192.137.78.128	193.137.78.129	193.137.78.158	193.137.78.159
6ª subnet	192.137.78.160	193.137.78.161	193.137.78.190	193.137.78.191
7ª subnet	192.137.78.192	193.137.78.193	193.137.78.222	193.137.78.223
8ª subnet	192.137.78.224	193.137.78.225	193.137.78.254	193.137.78.255

Sub-Addresses

- To determine the network of a given machine just have to do the AND of the address with the netmask.
- Consider the machine with address 10.20.237.15 and mask 255.255.248.0 (ie 10.20.237.15/21), your network is

	10	20	237	15
AND	255	255	248	0
	10	20	232	0

				Mask
	00001010	00010100	11101101	00001111
AND	11111111	11111111	11111000	00000000
	00001010	00010100	11101000	00000000

Licenciatura em Engenharia Informática

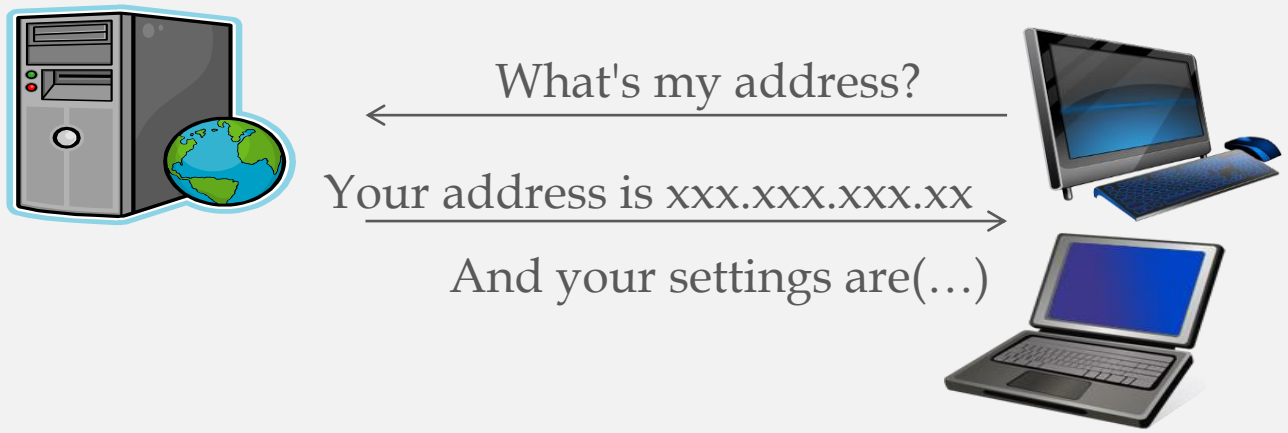
Ramo de Redes e Administração de Sistemas

Dynamic Host Configuration Protocol (DHCP)

Ano Letivo 2019-2020

Dynamic allocation of IP

- If your network has 5 computers, the work and errors you can commit in manually assigning and configuring the addresses are few.
- But if your network has 300 or more machines? With portable machines always entering and leaving the network? It would not be easy to manually configure all addresses.
- Solution: arrange a centralized service that does this function automatically.



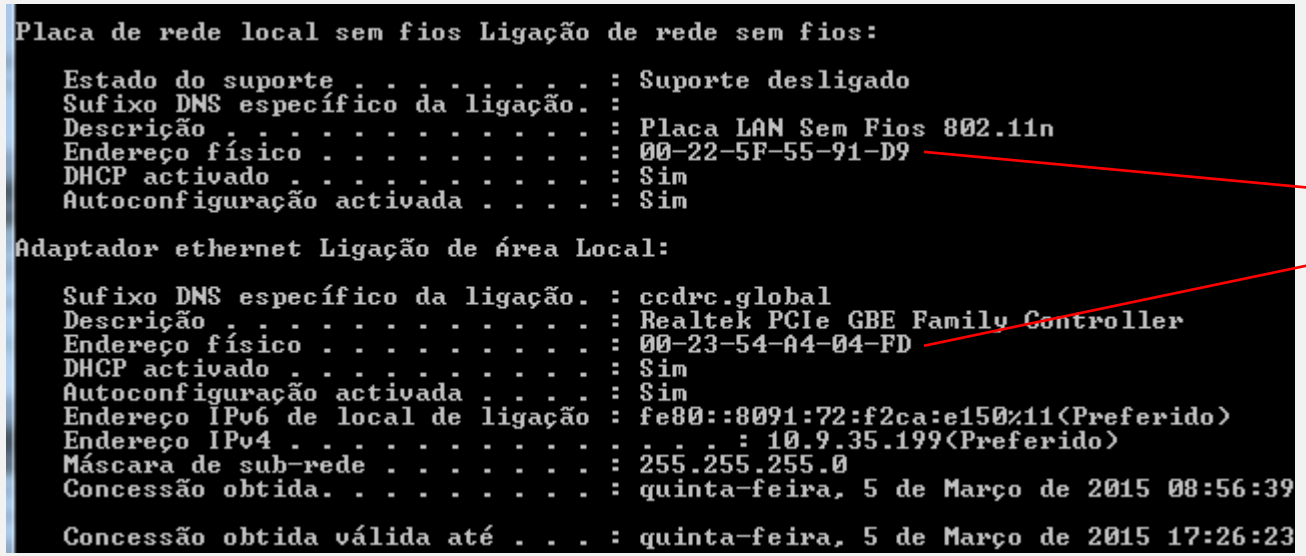
MAC (*Media Access Control*)

- Each machine with a network card has a unique and non-repeating identification.
- This identification is a sequence of bits, which is called the physical address on the network (**MAC address**).
- The MAC address consists of a set of 6 bytes separated by a colon (":") or hyphen ("-"), each byte being represented by two digits in the hexadecimal form, for example: "00: 19: B9: FB: E2: 58 ". Each digit in hexadecimal corresponds to a binary word of four bits, in this way, the 12 digits that form the address totalize 48 bits.

MAC (*Media Access Control*)

- There is a standard for MAC addresses that is administered by the IEEE (Institute of Electrical and Electronics Engineers) which defines:
  - The first three bytes - called OUI (Organizationally Unique Identifier), and which are intended for manufacturer identification are provided by IEEE itself.
  - The last three bytes are defined by the manufacturer, which is responsible for controlling the numbering of each board it produces.
- The MAC address is unique in the world for each network card (although there are tools that allow it to be changed), and it is kept in the ROM, and later this information is copied to the RAM memory when the card is started.

MAC (*Media Access Control*)



MAC address of two network cards of one machine

ARP - *Address Resolution Protocol*

1) When we want to communicate with another machine, what do we need to know?

IP address (or the name that is then translated into an IP address).

2) What information is inserted in a frame relative to the recipient?

The MAC Address of the destination PC (physical address) is included in the frame.

3) But if I only know the IP, how to find out the MAC of the target PC?

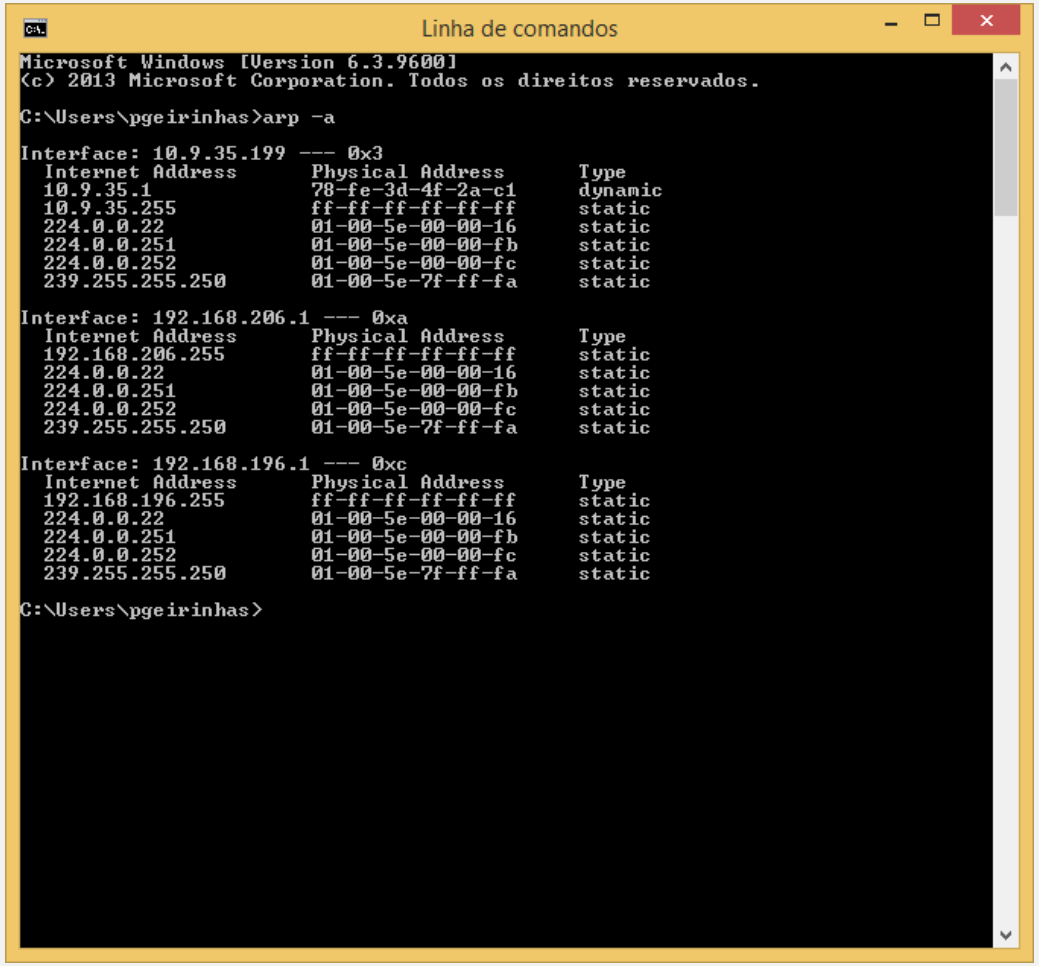
Using the ARP protocol, which allows obtaining the MAC address (from the destination PC) using the IP address (from the destination PC).

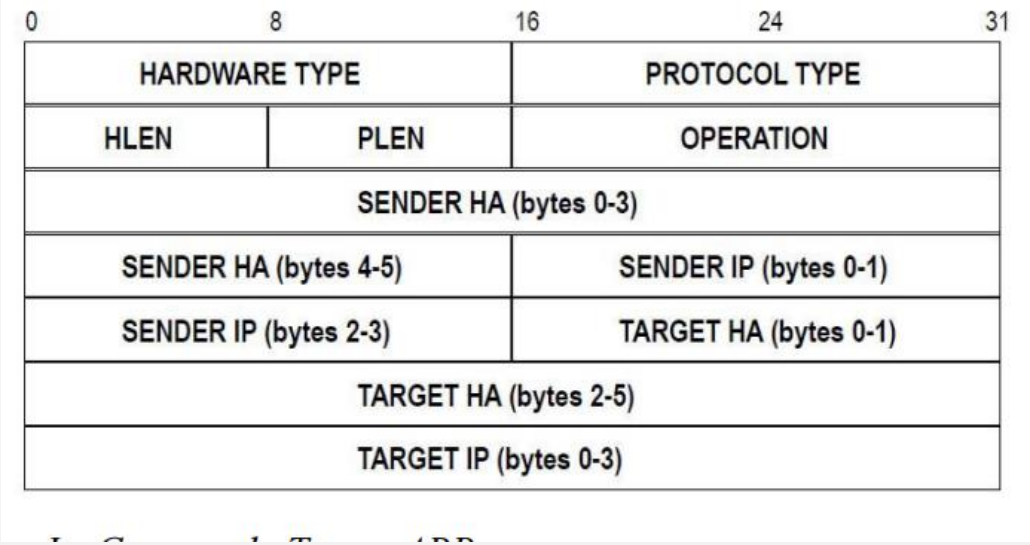
4) In the case of sending information outside the domain of the local network, the physical address to be registered in the ARP table of a local PC will be the physical address of the gateway.

ARP - *Address Resolution Protocol*

- Every time a machine starts communicating with another, its ARP table is queried.
- If the requested address is not in the table, the ARP protocol issues a request to the network (ARP Request).
- The machines connected in the network will compare the IP address (logical address) of the request.
- If any of the machines recognize the IP address in the request it will respond by sending an (ARP Reply).
- This response will contain the physical address (MAC) of the target machine, which will be stored in the ARP table of the source machine.

ARP - *Address Resolution Protocol*





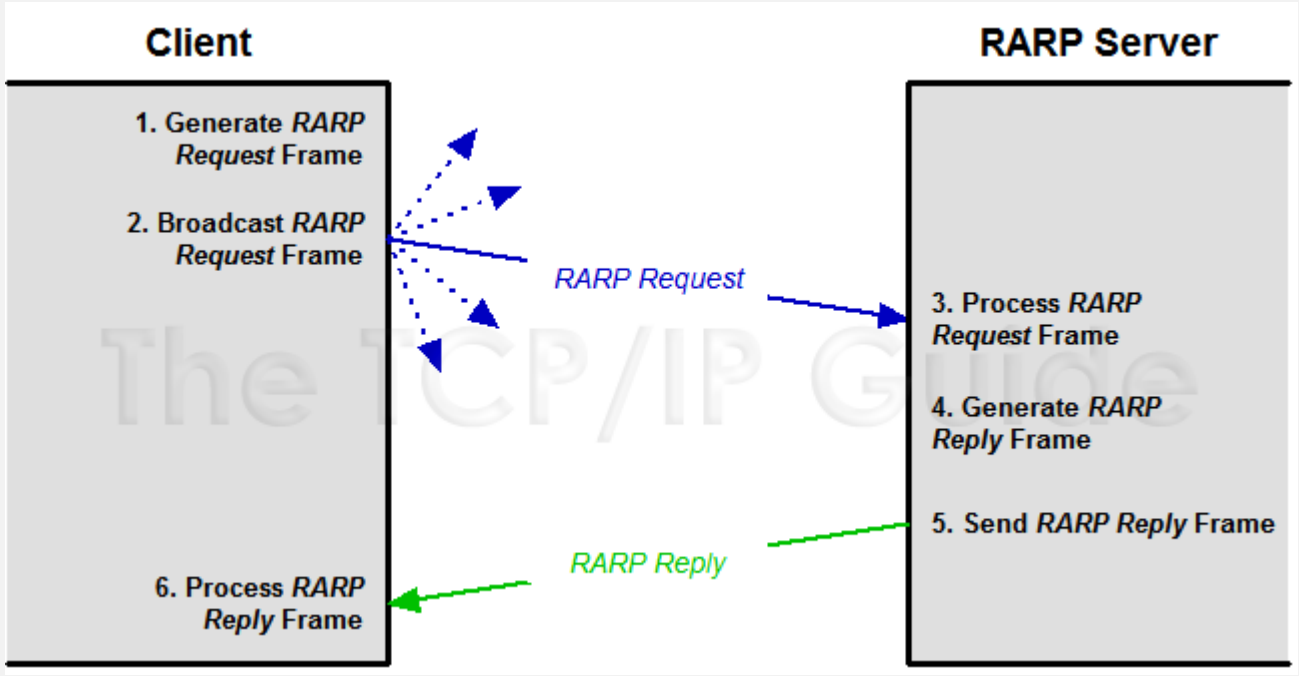
RARP (Reverse Address Resolution Protocol)

- The equipment must use a protocol that allows obtaining the IP address making use of the physical address of the board.
- This protocol is **RARP**.
- RARP associates a MAC address with an IP address. This allows network devices to encapsulate the data before sending it to the network.
- For an equipment to send and receive information on a network, it needs to have an IP address. But before that you need to be able to exchange information.
- A network device, such as a diskless workstation, for example, may know its MAC address but not its IP address. RARP allows the device to make a request to know its IP address.Os dispositivos que usam este protocolo exigem que haja um servidor RARP presente na rede para responder as estas solicitações.

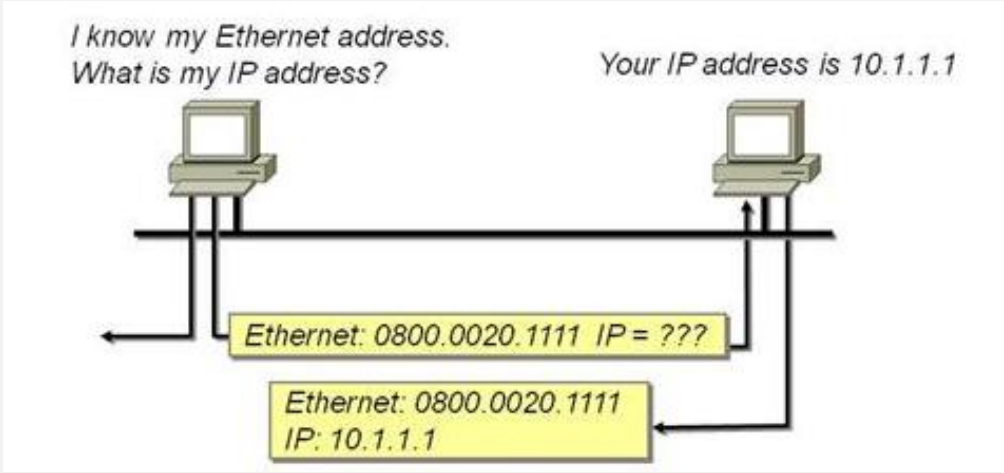
RARP

- The communication is made from the diffusion of the request of a station in the local network to acquire an IP address. The station sends the MAC address in the target HA field in the message.
- Only RARP servers will process the sent message.
- Servers respond to requests by populating the protocol type field by changing the operation field from request to response and by sending the message directly to the machine.
- It receives responses from all RARP servers, even though it accepts the first one.
- From this moment the machine will only use RARP again if a system reboot is done.

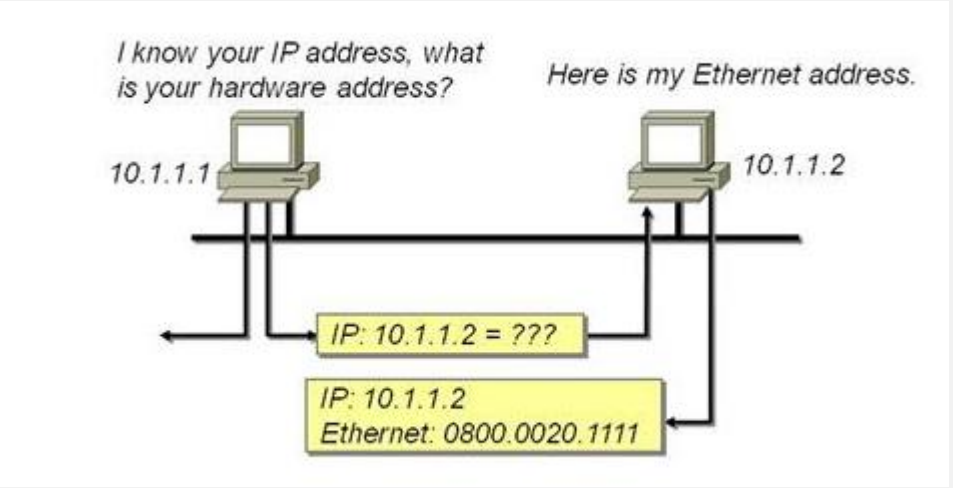
RARP


Client
RARP Server
1. Generate *RARP Request* Frame
2. Broadcast *RARP Request* Frame
RARP Request
3. Process *RARP Request* Frame
4. Generate *RARP Reply* Frame
5. Send *RARP Reply* Frame
RARP Reply
6. Process *RARP Reply* Frame
The TCP/IP Guide

RARP X ARP



RARP



ARP

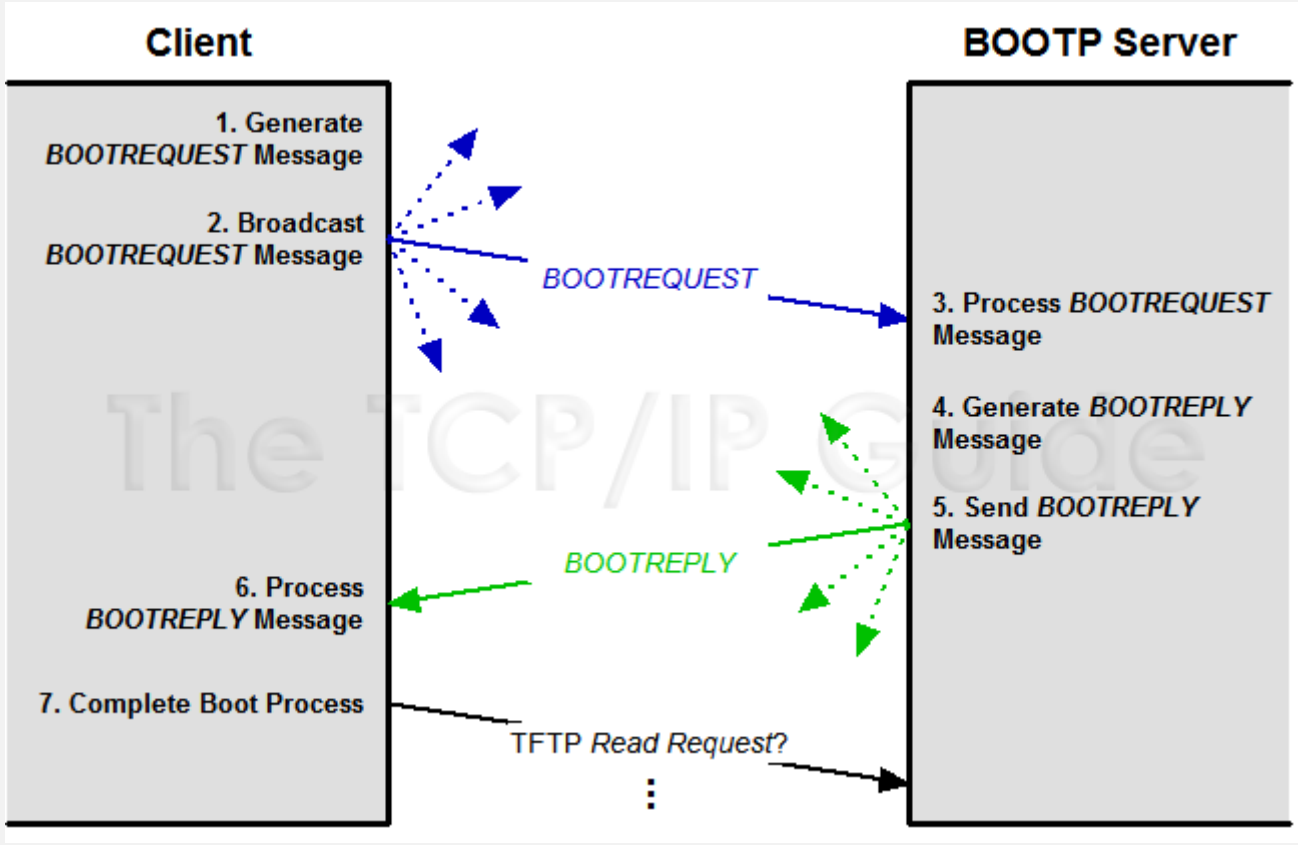
RARP - Limitations

- RARP servers need to be on the same network as your clients.
- By operating so close to the hardware of the machine complicate the development of client-server applications.
- They could not have automatic address assignment mechanisms.
- The exchange of information between the clients and the server was limited only to an IP address.
- It was thus replaced by **BOOTP** (BOOTstrap Protocol).

BOOTP (***BOOT****strap* ***P****rotocol)*

- BOOTP is a server configuration protocol developed prior to DHCP.
- BOOTP is defined by RFC 951.
- It is based:
  - In a single exchange of messages.
  - Transfers much more information than in RARP.
  - How to use UDP is much easier to program.
  - It provides only a static mapping between a machine identifier and a set of parameters for those machines.

BOOTP (*BOOTstrap Protocol*)

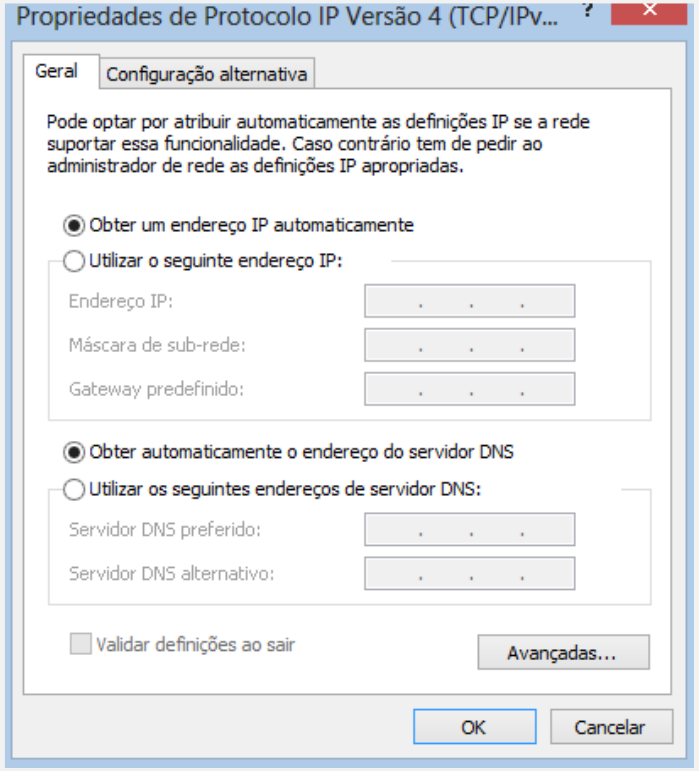


BOOTP - Limitations

- Limitations:
  - Static configuration of machine identifier for parameters to be configured.
  - Does not allow the dynamic configuration of machines.
  - It does not allow the reuse of IP addresses for different machines.
- With the laptops and mobile networks it was necessary to find another initialization protocol.
- This is how the **Dynamic Host Configuration Protocol**

DHCP (*Dynamic Host Configuration Protocol*)

- DHCP stands for Dynamic Host Configuration Protocol. It is a protocol used in networks of terminal equipment that allows them to obtain an IP address automatically.
- Provides dynamic configuration of terminals, granting host IP addresses and other configuration parameters to network clients.



DHCP (*Dynamic Host Configuration Protocol)*

- It emerged by default in October 1993.
- RFC 2131 and RFC 2131 contain the most current specifications (March 1997).
- The last standard for specifying DHCP over IPv6 (DHCPv6) was published in July 2003 as RFC 3315.
- DHCP is essentially an improved and extended version of BOOTP, running, such as this one, in client-server mode and enabling automatic retrieval of IP addresses, server names, subnet mask, and default gateway.

DHCP - Benefits

- Automation of the TCP / IP protocol configuration process on network devices.
- Ease of changing parameters such as Default Gateway, DNS Server, etc., on all devices in the network, through a simple change in the DHCP server.
- Elimination of configuration errors, such as incorrectly typing a subnet mask or using the same IP number on two different devices, generating an IP address conflict.
- IP addresses are refreshed at predefined time intervals on the server. You can also configure that the IP will be free when the host disconnects from the network.

DHCP

- Address Allocation Mechanisms
  - **Manual**
    - The administrator configures in the DHCP server the IP to assign to each machine through the use of the MAC.
  - **Automatic**
    - The DHCP service automatically assigns a static IP to an equipment, among a set of available addresses.
    - The equipment uses this information without limiting its use.
  - **Dynamics**
    - The DHCP service assigns IP addresses to an equipment between a set of available addresses for a predefined time interval.
    - The equipment can use this information for a certain time.

DHCP

- **Server:**
  - It must be configured by your network administrator to make IP addresses available to customers in one of the three forms of delivery described.
  - It is important to leave fixed addresses on some machines their IP addresses (for example routers and servers).
  - The time limit for the rental of an address must also be established. This can range from hours to days or simply be unlimited.
- **Client:**
  - A DHCP client is a device that is configured to request a server an IP address.
- **Scope:**
  - Full consecutive range of possible IP addresses for a network eg the address range from 10.10.10.100 to 10.10.10.150 on the network 10.10.10.0 255.255.255.0

DHCP

- **Exclusion interval**
  - Limited sequence of IP addresses within a given scope, excluded from addresses to be provided by DHCP
  - For example, within the range 10.10.10.100 to 10.10.10.150 (network 10.10.10.0 / mask 255.255.255.0), an exclusion range is created from 10.10.10.120 to 10.10.10.130
- **Address Pool**
  - These are the remaining addresses of the scope after defining the exclusion range.
  - In the previous example the address pool is formed by the addresses from 10.10.10.100 to 10.10.10.119, plus the addresses from 10.10.10.131 to 10.10.10.150

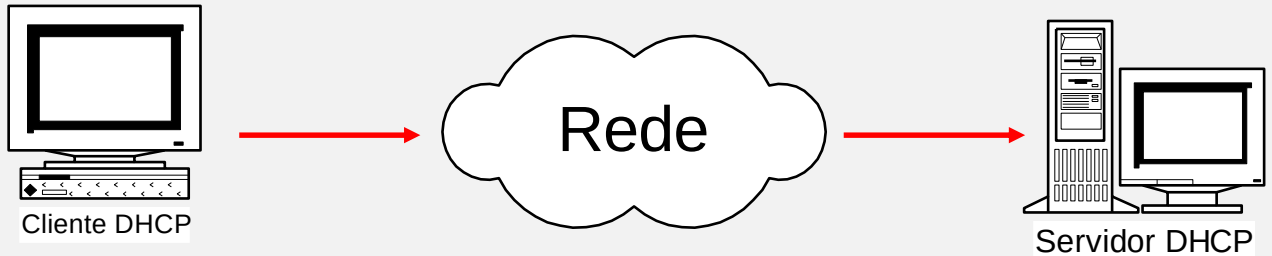
DHCP

- **Concession**
  - The period of time specified by a DHCP server during which a client computer can use an IP address that it received from the DHCP server.
- **Reservation**
  - Providing permanent address by the DHCP server, ensuring that a hardware device specified in the subnet can always use the same IP address.

DHCP - Operation

- Uses the UDP protocol on the following ports:
  - Server: port 67
  - Customer: porto 68
- The messages used in the protocol for information negotiation are as follows:
  - **Discover**
    - Sent by the client to verify the existence of DHCP servers on the network.
  - **Offer**
    - Message sent by the servers with the information proposal.
  - **Request**
    - Message sent by the customer in which he chooses the offer (usually the first one sent to him).
  - **Ack**
    - Confirmation message from the server that "won the deal".
  - Other messages: **Inform**, **Decline**, **Nack**, **Release**

DHCP - Initial granting procedure

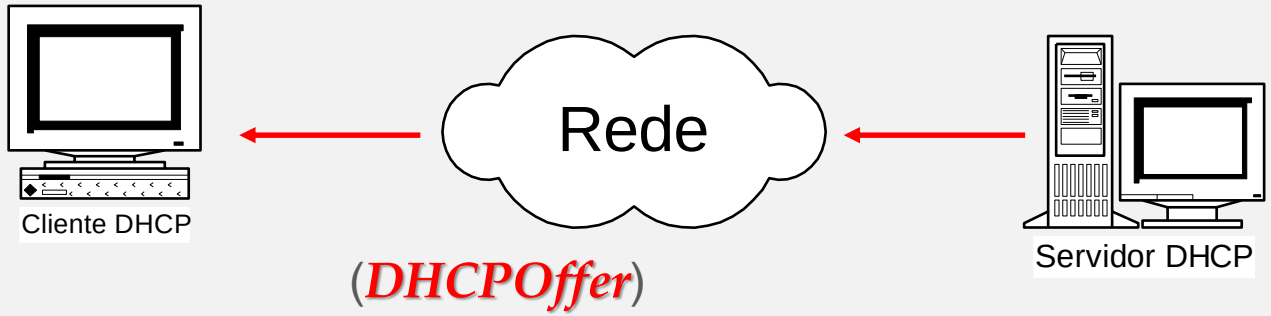


Client sends "DHCPDiscover" message to the entire network(*broadcast*)

(***DHCPDiscover***)

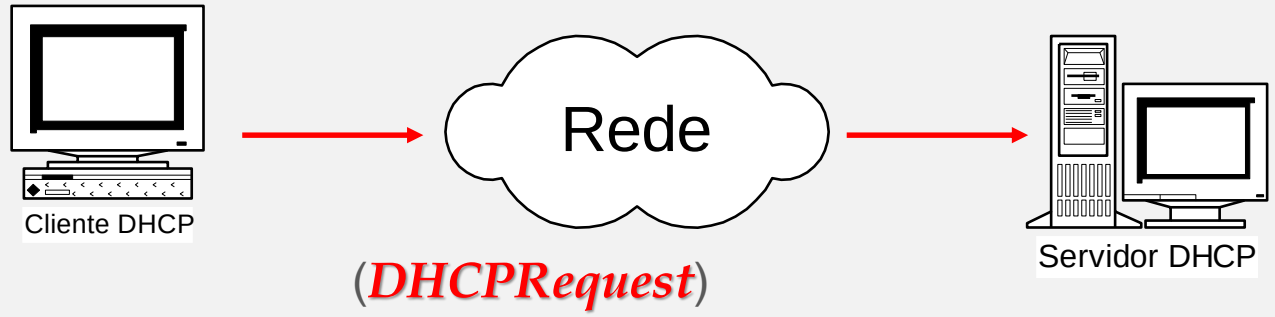
The format of this message is specific, being recognized only by the DHCP server (s) that are present in the local network.

DHCP - Initial granting procedure



The DHCP server "hears" the message sent by the client and responds by offering an IP address and other settings (subnet mask, gateway, and DNS)

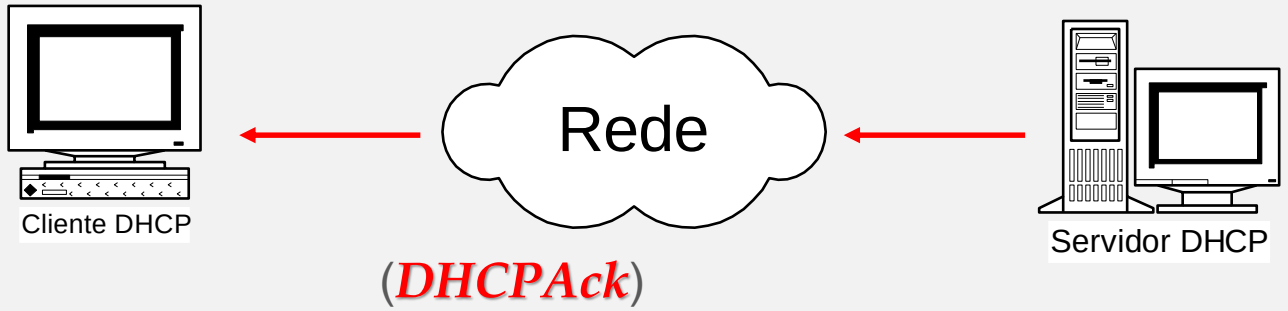
DHCP - Initial granting procedure



As soon as the DHCPOffer message is received, the client selects the offered address responding to the server with a "DHCPRequest" DHCP request, stating that the offer was accepted

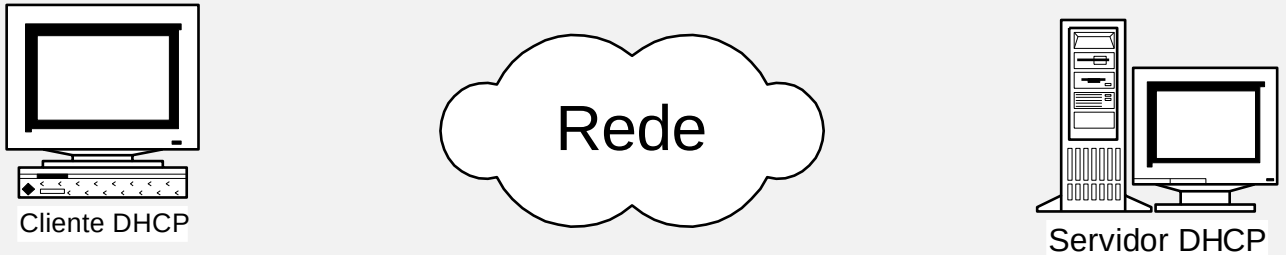
This message is broadcast because the client does not yet have TCP / IP protocol settings

DHCP - Initial granting procedure



After receiving the client's DHCPRequest message, the DHCP server sends a acknowledgment message ("DHCPAck"), approving the lease.

DHCP - Initial granting procedure

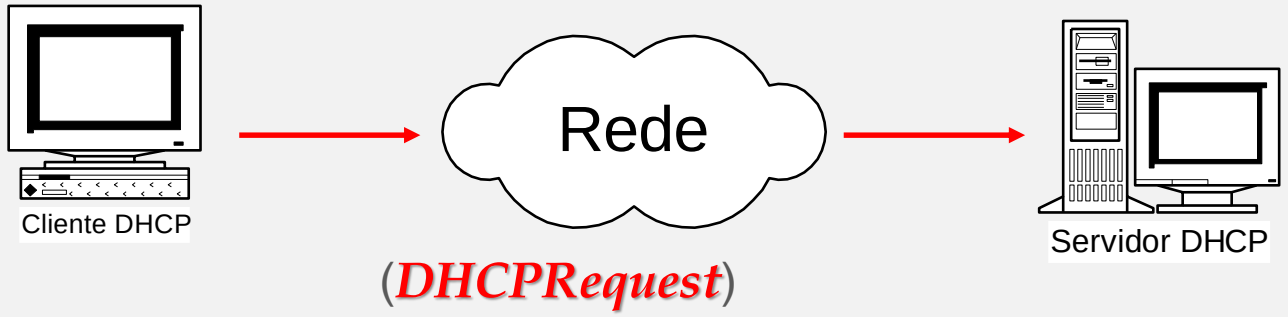


After receiving DHCPAck from the DHCP server, the client configures the d0 TCP / IP properties using the information sent by the DHCP server in the DHCPOffer message and is ready to communicate!

Grant Renewal Process

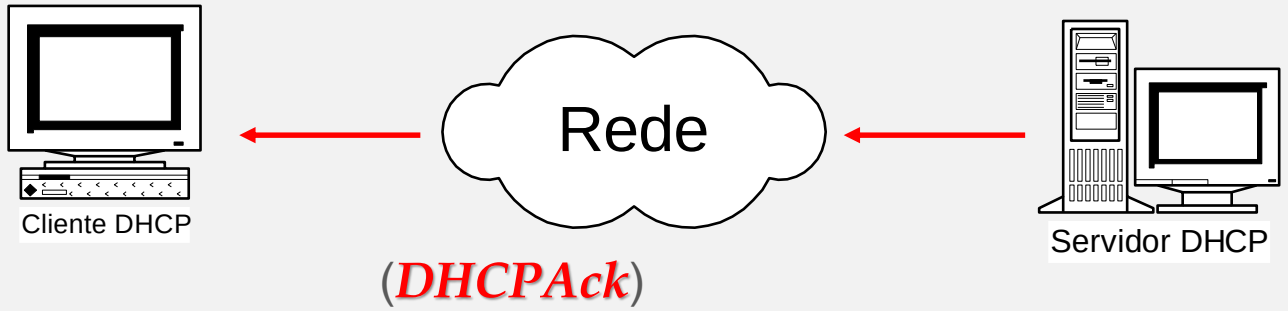
- When a DHCP client is shut down and rebooted (on the same subnet), it usually gets a lease for the same IP address it had before it was turned off.
- After half of the client lease time has elapsed, the client attempts to renew the lease with the DHCP server.

Grant Renewal Process



The client sends a DHCPRequest message directly to the server that previously granted the grant (since the client now has an IP address and knows the IP address of the DHCP server), to renew and extend the current address lease

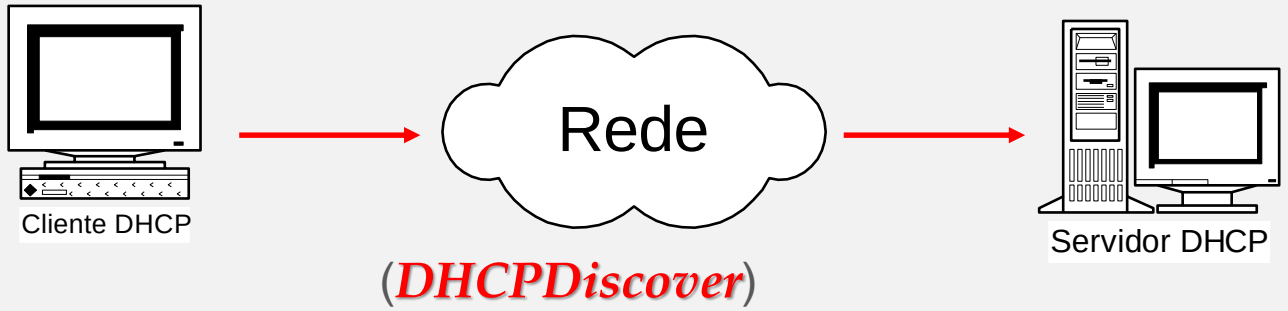
Grant Renewal Process



f the original DHCP server is active, it sends a DHCPAck message, which means that the current lease has been renewed

If some of the TCP-IP information used has changed, the server sends the new values so that the client can update them.

Grant Renewal Process



If the client can not communicate with the original DHCP server, it attempts to renew the current lease with any other available DHCP server by sending a DHCPDiscover in broadcast

Grant Renewal Process

If any server responds with a DHCPOffer to update the current lease, the client can renew the lease based on the DHCP server offer, and continue to work normally on the network

Grant Renewal Process

- If the lease expires and has not been able to establish any connection with any DHCP server, the client should immediately stop using the granted IP address.
- The customer then repeats the entire process of obtaining a new lease.
- The DHCP client uses the UDP "Checksum" field to ensure the integrity of the received packet.
- In case the UDP message is lost, the protocol uses the conventional retransmission timeout technique.

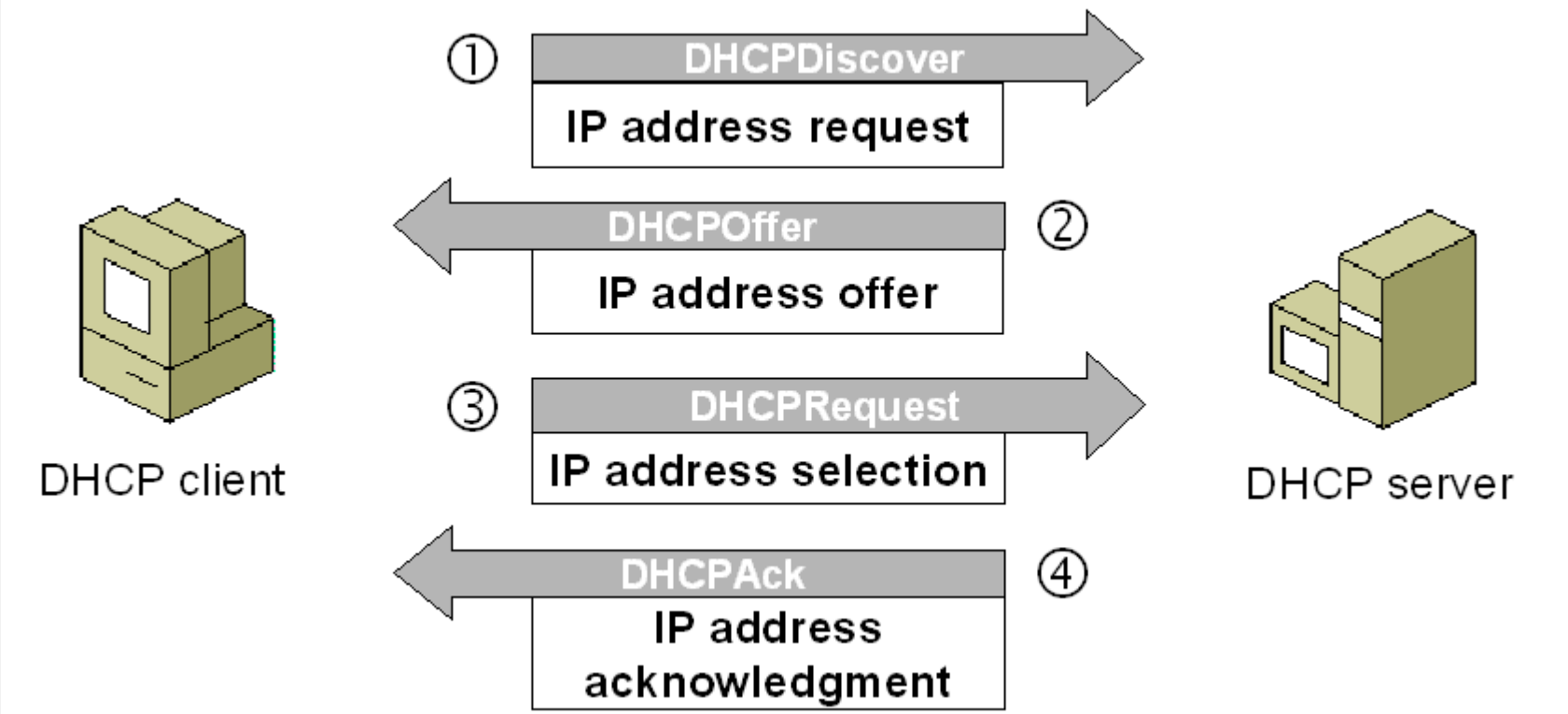
Other Commands

- ***DHCPNack***
  - Sent by a DHCP server to a client denying the DHCPRequest message. This can occur if the requested address is incorrect because the client has been moved to a new subnet or lease and can not be renewed.
- ***DHCPDecline***
  - Sent by a DHCP client to a server, stating that the server that the IP address offered was refused because it appears to be in use by another computer.
- ***DHCPInform***
  - Sent from a DHCP client to a DHCP server, requesting only additional local configuration parameters;
  - the client already has a configured IP address. This type of message is also used by DHCP servers running Windows Server 2008 to detect unauthorized DHCP servers.
- ***DHCPRelease***
  - Sent by a DHCP client to a server that provided the grant thus releasing the IP that had been assigned to it.

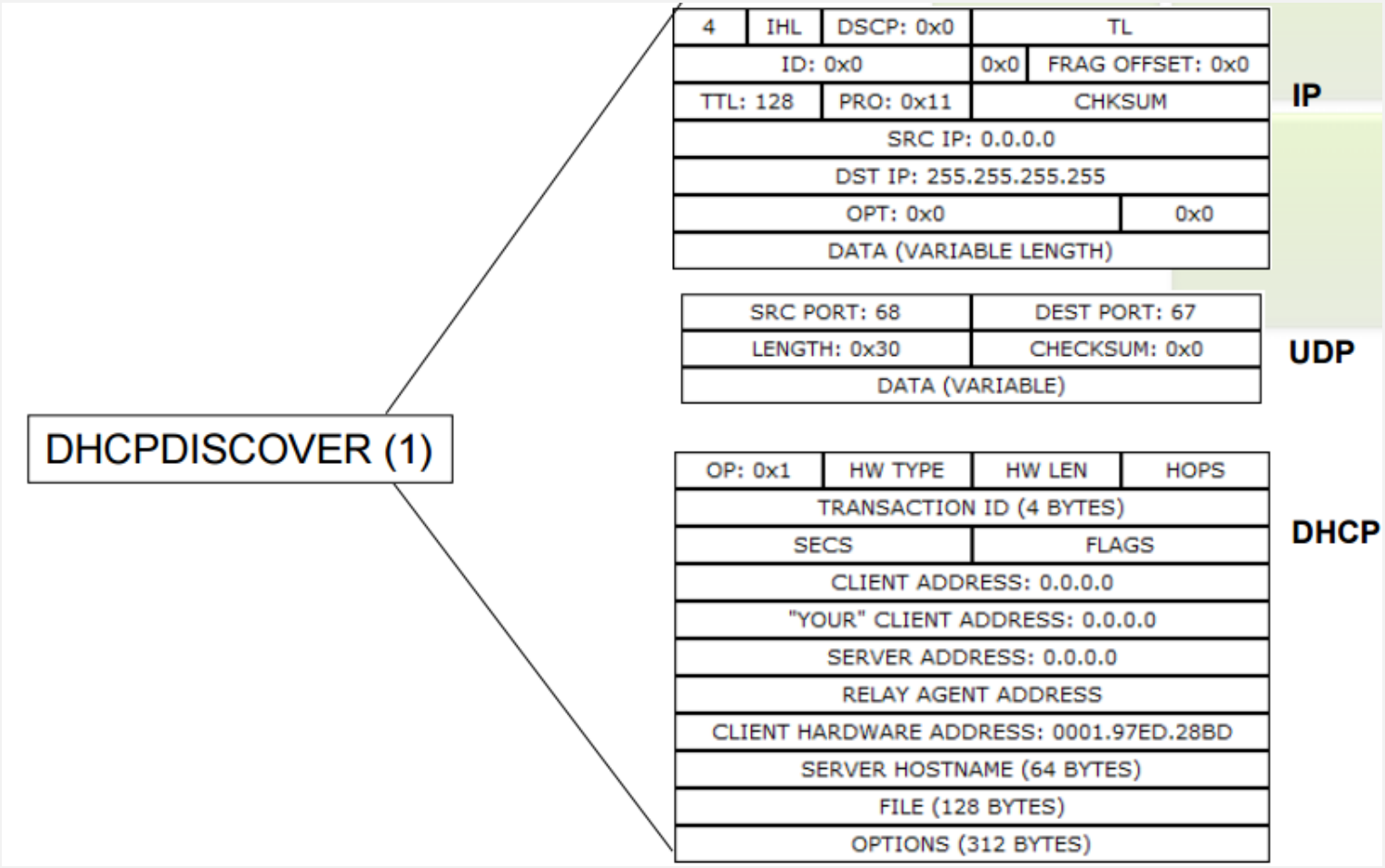
Message format

8	16	24	32
OP Code (1)	Hardware type (1)	Hardware address length (1)	Hops (1)
Transaction Identifier			
Seconds – 2 bytes		Flags – 2 bytes	
Client IP Address (CIADDR) – 4 bytes			
Your IP Address (YIADDR) – 4 bytes			
Server IP Address (SIADDR) – 4 bytes			
Gateway IP Address (GIADDR) – 4 bytes			
Client Hardware Address (CHADDR) – 16 bytes			
Server name (SNAME) – 64 bytes			
Filename – 128 bytes			
DHCP Options – variable			

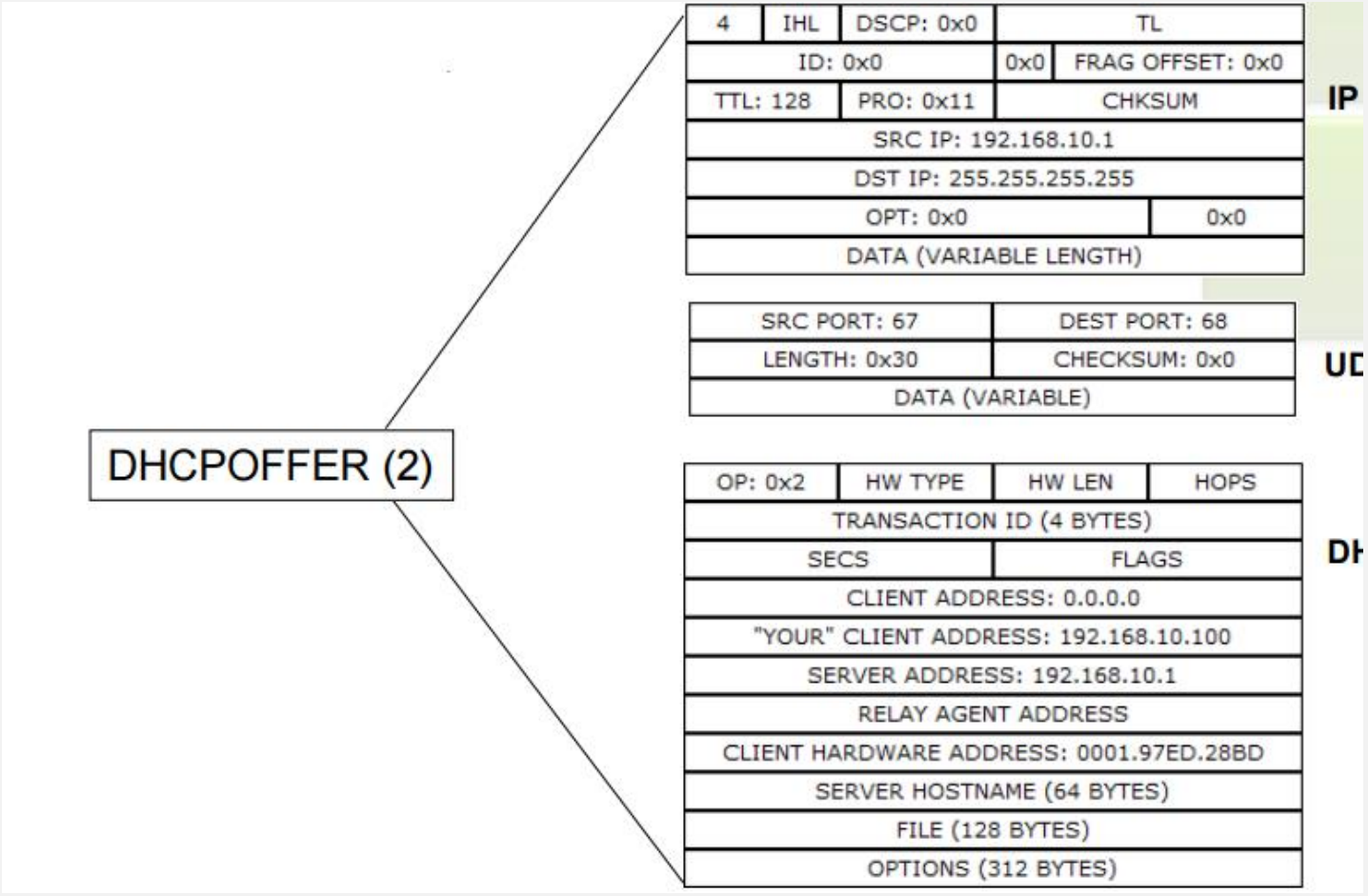
Message format



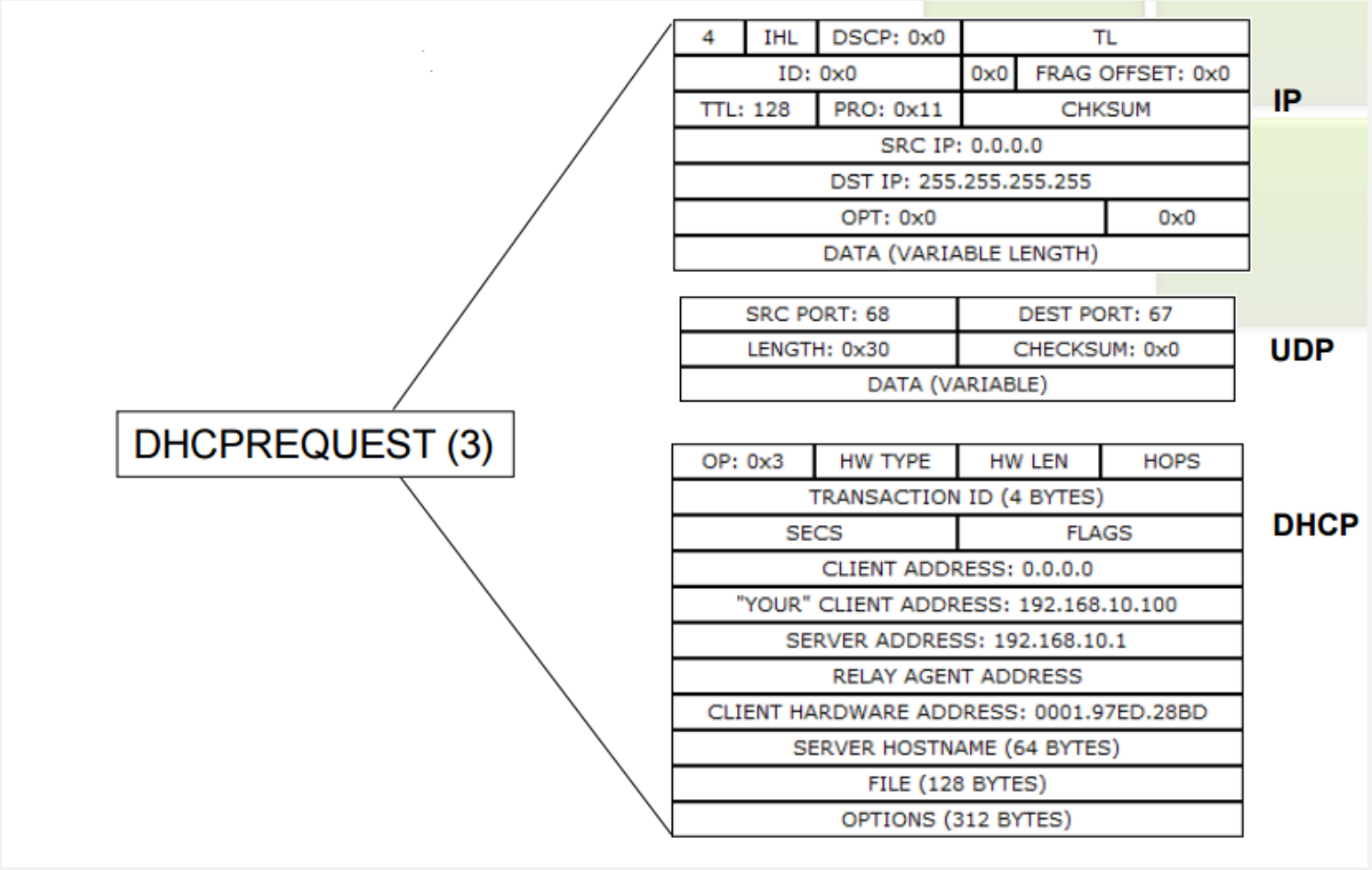
Message format



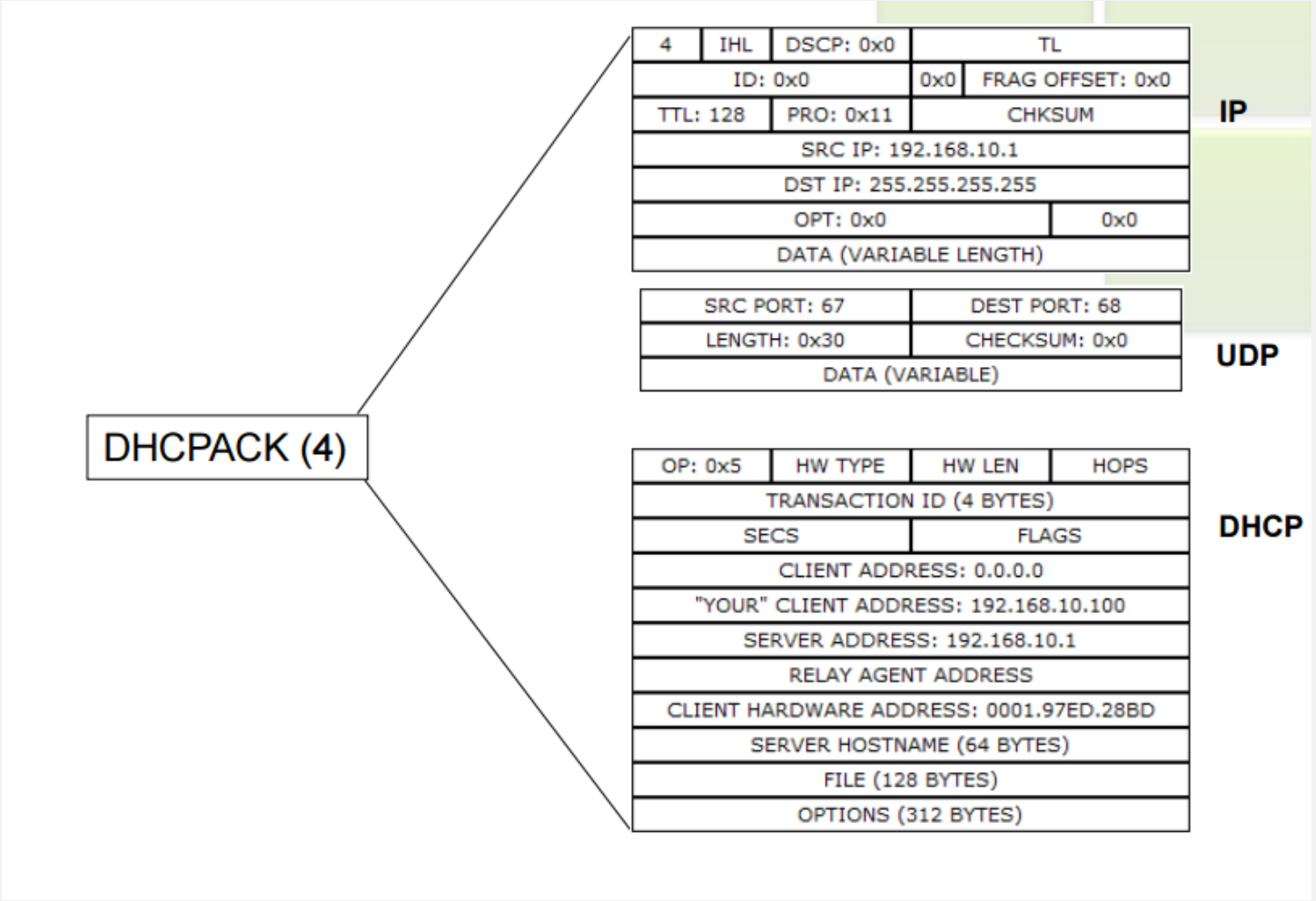
Message format



Message format



Message format

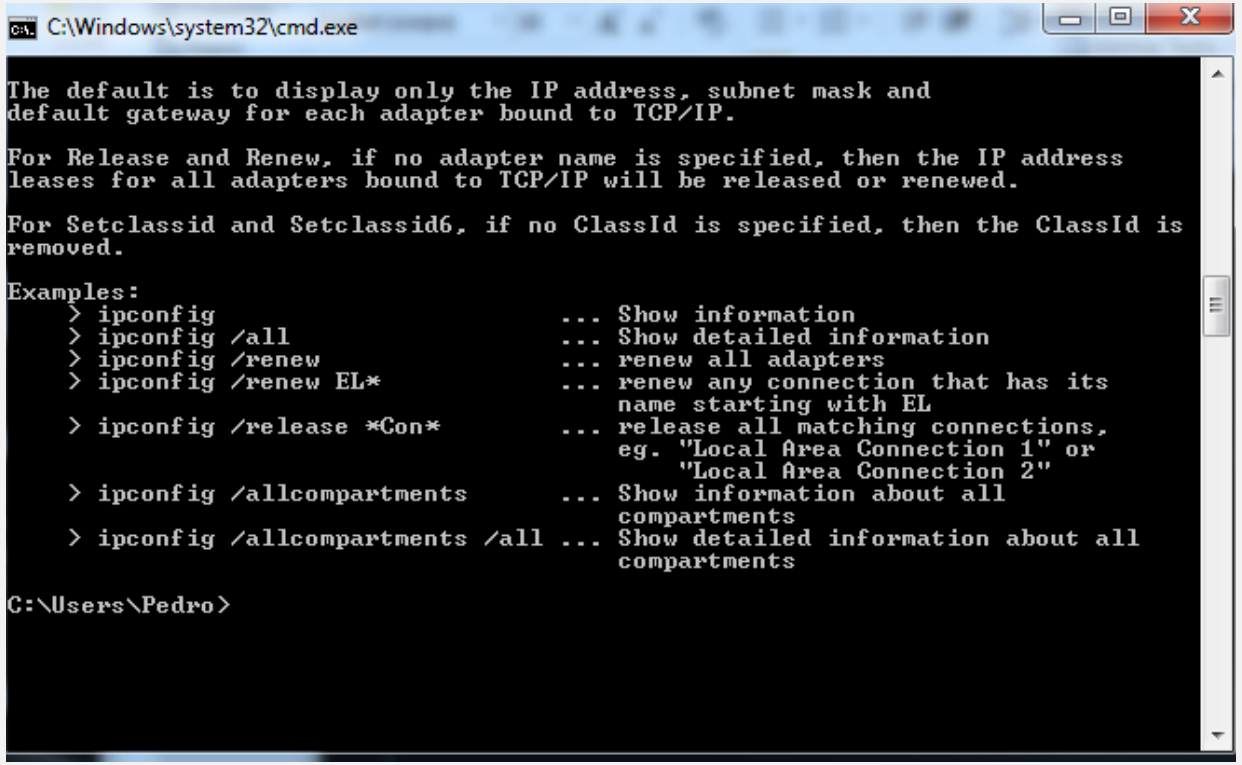


Security

- DHCP does not include any authentication mechanism. This is why it is vulnerable to a variety of attacks.
- These can be divided into three fundamental groups:
  - Provision of erroneous information to clients by unauthorized DHCP servers
  - Unauthorized clients with access to resources.
  - Exhaustion of customer resources.

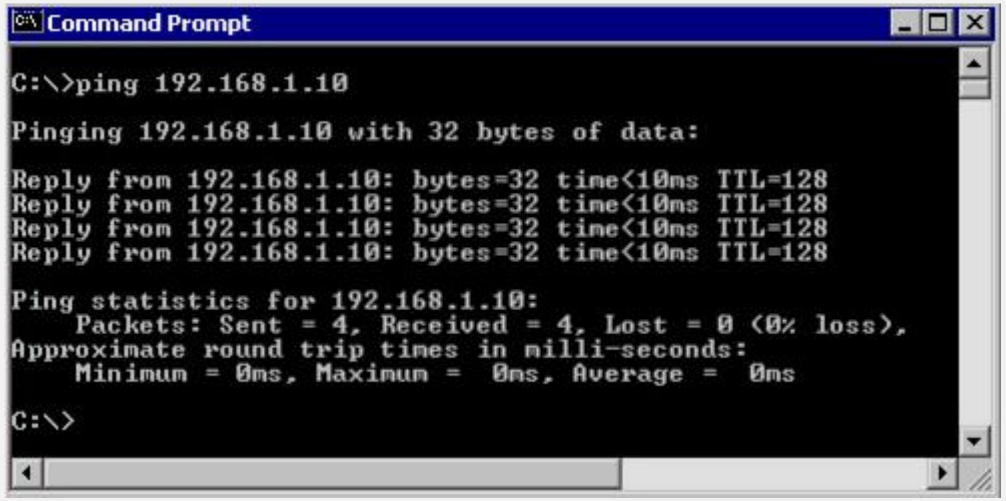
DHCP (Client)

- In a client and to know / change your IP configuration you can use these commands:
  - *Ipconfig / all*
  - *Ipconfig / renew*
  - *Ipconfig / release*



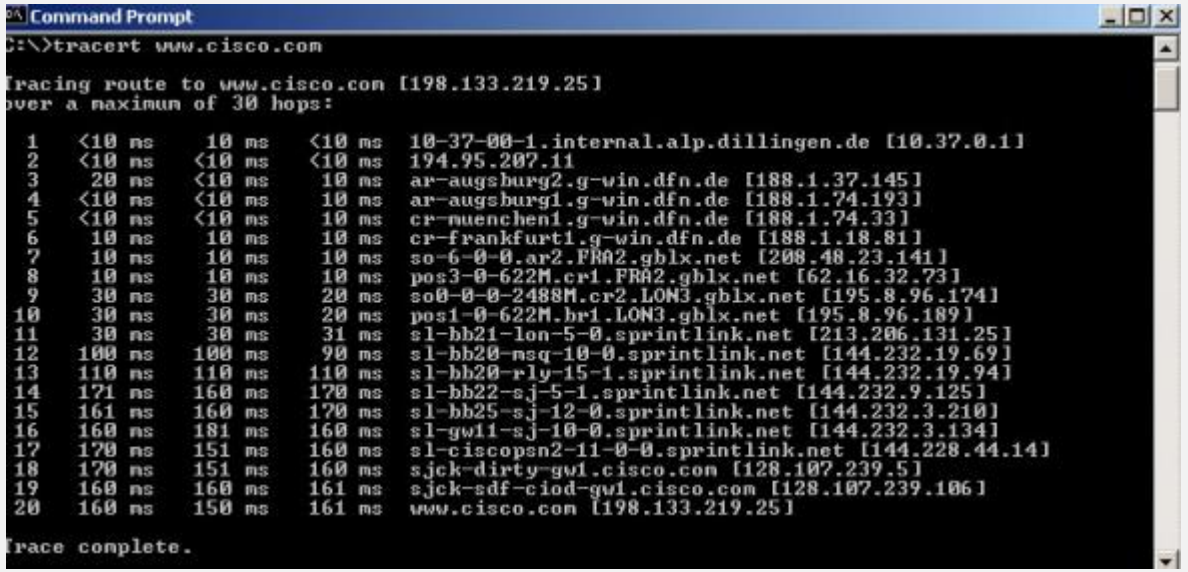
DHCP (Client)

- The **ping** command tests the physical connectivity between two extremes, providing an indication of the reliability of the connection as it presents the result of four attempts at communication.



DHCP (Client)

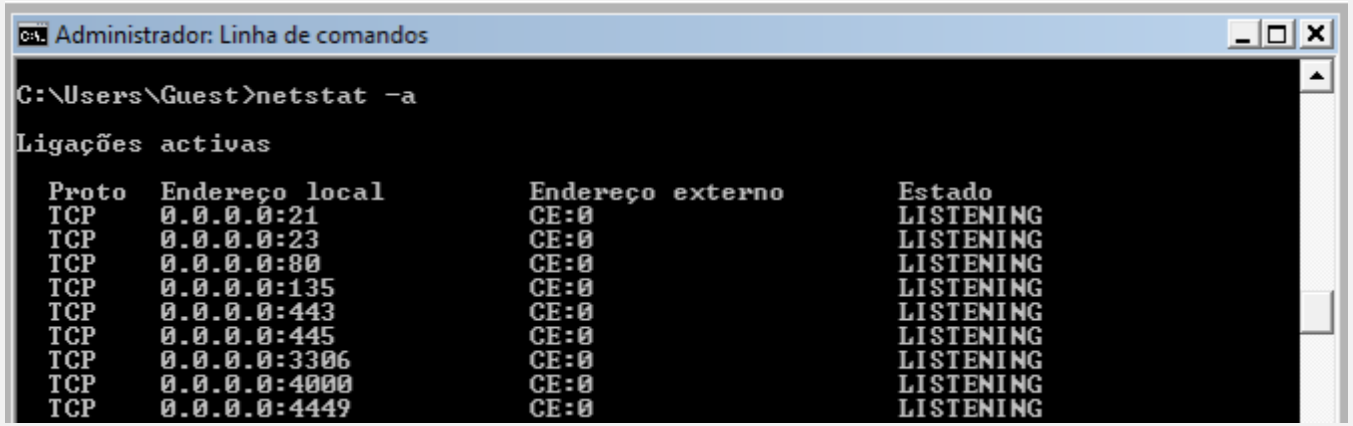
- The **tracert** command is the TCP / IP abbreviation for trace route. The command uses IP datagrams to display the routers that are found on the path to the destination.



- The first line of the output shows the destination name followed by its IP address. Following are the listings of all the routers through which the tracert had to pass to reach the destination

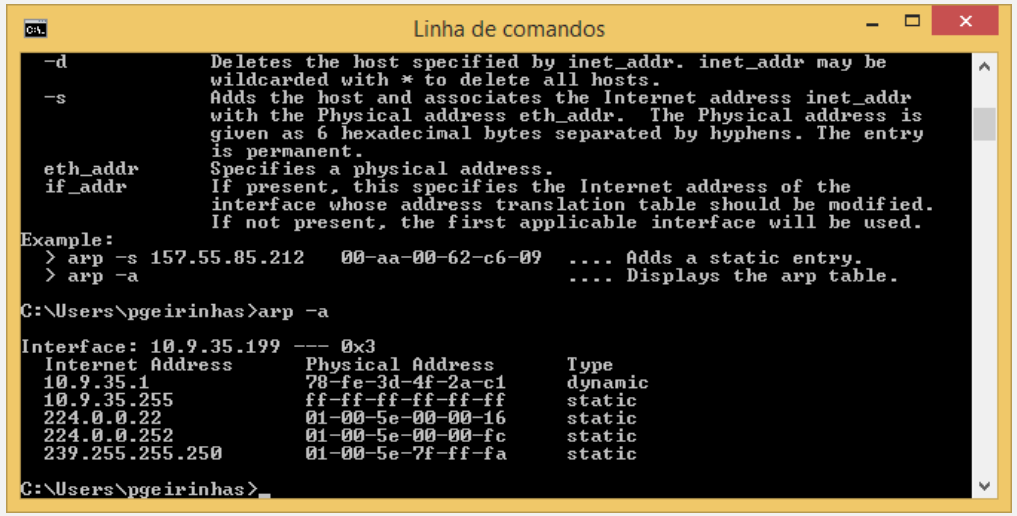
DHCP (Client)

- The **netstat** command allows you to view information about TCP / IP network connections on the local machine and statistics about the protocols used.



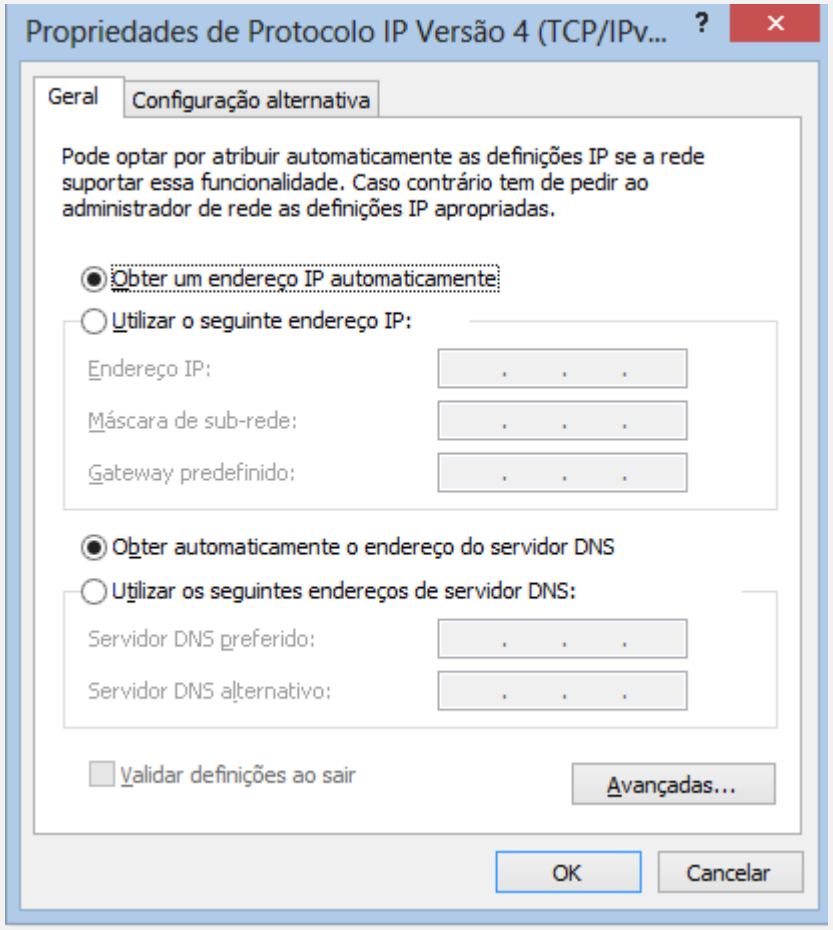
DHCP (Client)

- Each machine is responsible for dynamically maintaining a table of correspondence between physical addresses and recently used IP addresses (ARP table), this procedure reduces the frequency of using the ARP protocol. To see this table do arp -a):



DHCP (Client)

- In the client configuration you can define which parameters are obtained automatically (DHCP) or manual.
- It is also possible for the W8 to define an alternative configuration for the use of the board in multi-environments.



APIPA

- Microsoft has registered with iana.org, an entity in charge of distributing IPs worldwide, a range of addresses for use on networks that do not have DHCP. This range is:
  - **169.254.0.0 to 169.254.255.255**

- When a Windows computer concludes that there is no DHCP on the network, it will automatically use an IP starting with 169.254 ending with two numbers that are generated based on the hardware configuration of the computer. This ensures that computers will have "compatible" IPs.
- APIPA stands for Automatic Programmed IP Address.

Licenciatura em Engenharia Informática

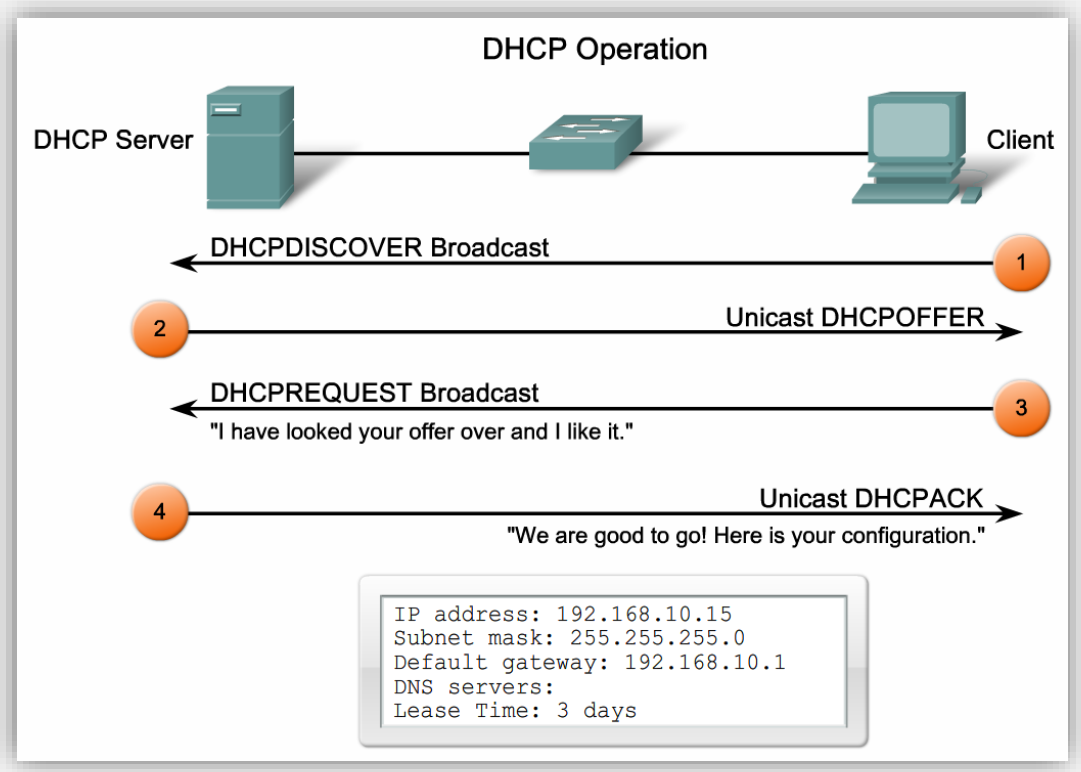
Ramo de Redes e Administração de Sistemas

Dynamic Host Configuration Protocol (DHCP) - Cisco

Ano Letivo 2019-2020

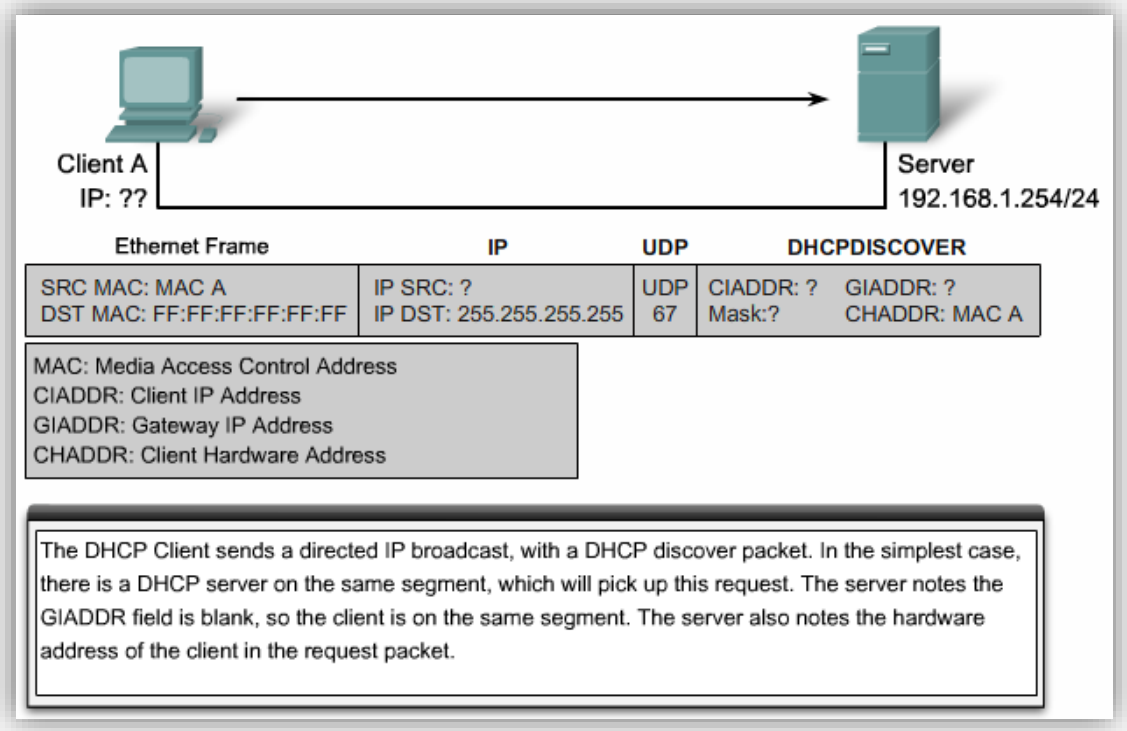
DHCP Configuration(Cisco)

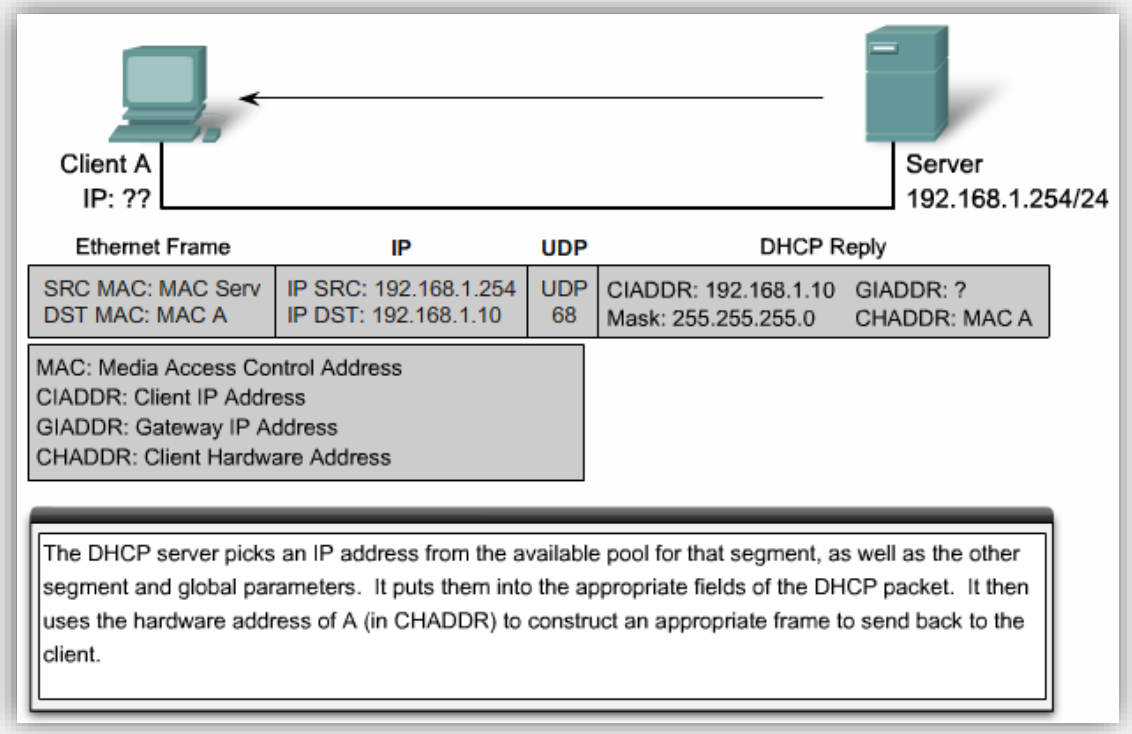
- In a cisco environment messages sent by the server are sent in unicast. The customers, and how could not fail to be in broadcast.



DHCP Configuration (Cisco)

- Operation

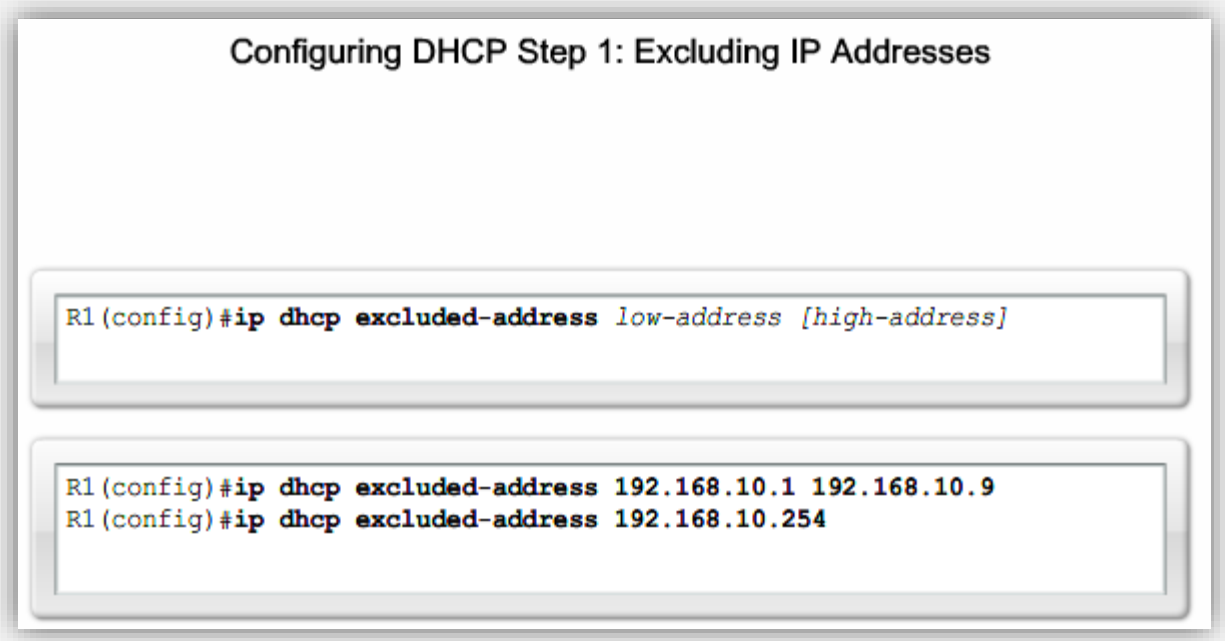




DHCP Configuration (Cisco)

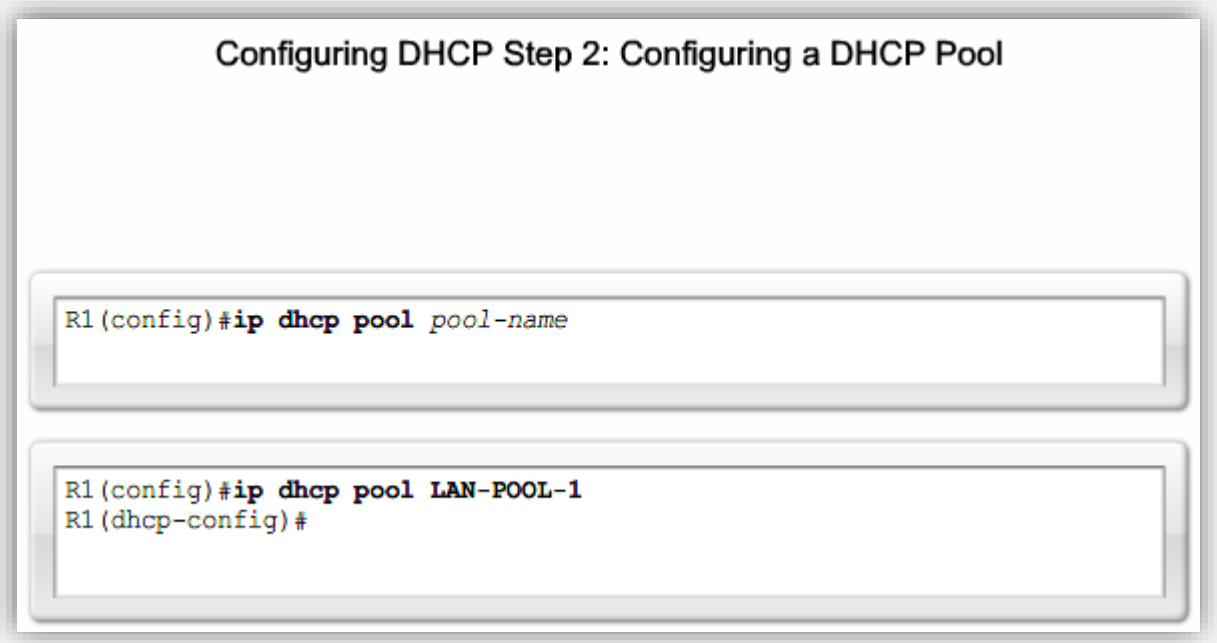
- Configuration steps
  - Activate service: **service dhcp**.
  - By default, it is active.
- Define an address range to use for dynamic allocation
  - Exceptions may be indicated - addresses or set of addresses belonging to the range but not assigned
- Create a pool
  - Use **the ip dhcp pool** command
  - Configure pool-specific parameters

DHCP Configuration (Cisco)



DHCP Configuration (Cisco)

- Give the pool a name



DHCP Configuration (Cisco)

Configuring DHCP Step 1: Excluding IP Addresses

```
R1(config)#ip dhcp excluded-address low-address [high-address]
```

```
R1(config)#ip dhcp excluded-address 192.168.10.1 192.168.10.9
R1(config)#ip dhcp excluded-address 192.168.10.254
```

Configuring DHCP Step 2: Configuring a DHCP Pool

```
R1(config)#ip dhcp pool pool-name
```

```
R1(config)#ip dhcp pool LAN-POOL-1
R1(dhcp-config)#
```

DHCP Configuration (Cisco)

Configuring DHCP Step 3: Specific Tasks

Required Tasks	Command
Define the address pool	`network network-number [mask | /prefix-length]`
Define the default router or gateway	`default-router address [address2...address8]`

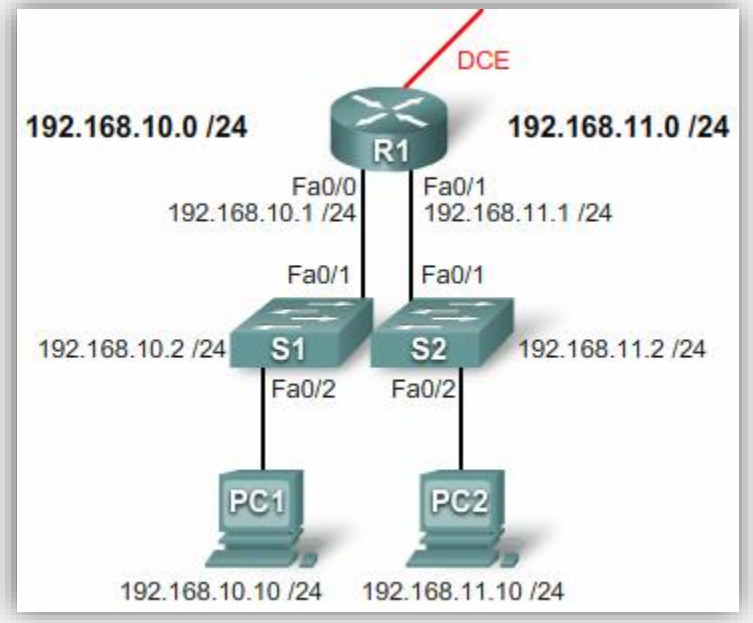
Optional Tasks	Command
Define a DNS server.	`dns-server address [address2...addre`
Define the domain name	`domain-name domain`
Define the duration of the DHCP lease	`lease { days [hours] [minutes] | infi`
Define the NetBIOS WINS server	`netbios-name-server address [address`

DHCP 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)# domain-name span.com
R1(dhcp-config)# end
```

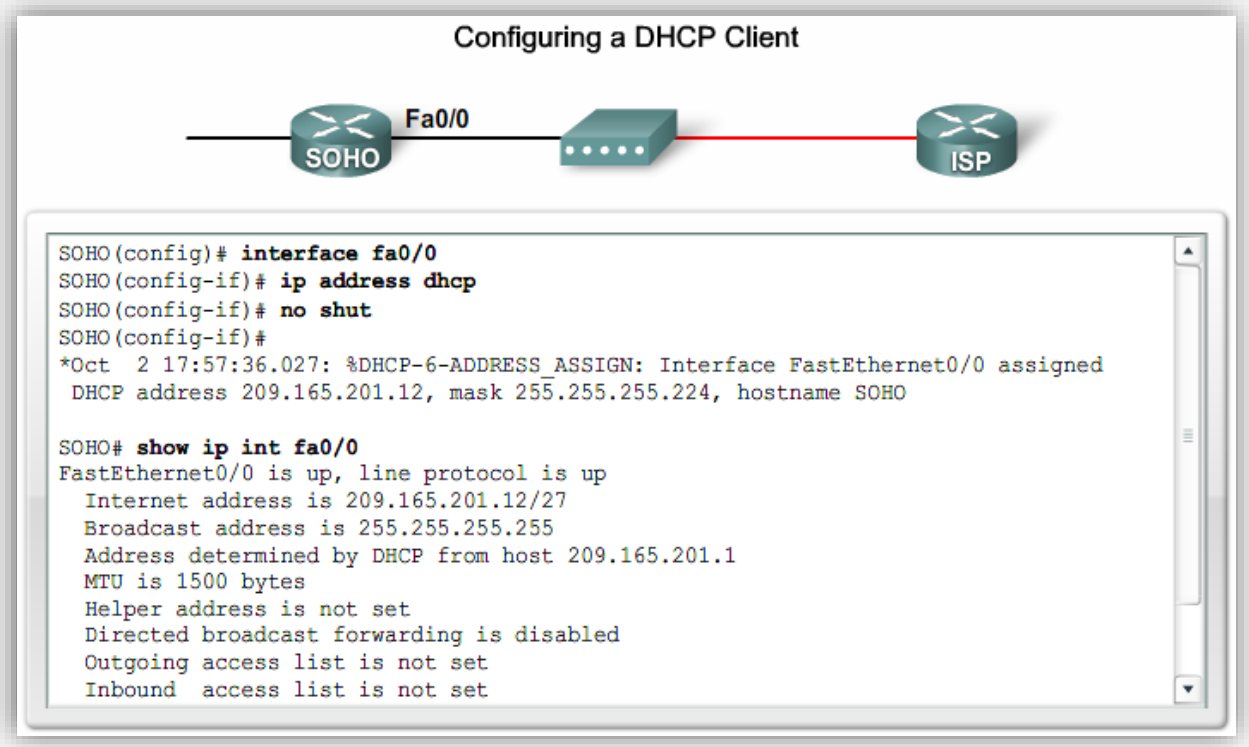
DHCP Configuration (Cisco)

- Um router pode possuir várias '*pools*' configuradas
  - A escolha da '*pool*' a usar para a atribuição dinâmica de informação IP é efectuada tendo por base o interface que recebe o pedido de DHCP (mensagem DHCPDISCOVER)



Router as DHCP client

- You can configure the router to be a DHCP client.
- It is not a usual situation and can cause some problems …



Licenciatura em Engenharia Informática

Ramo de Redes e Administração de Sistemas

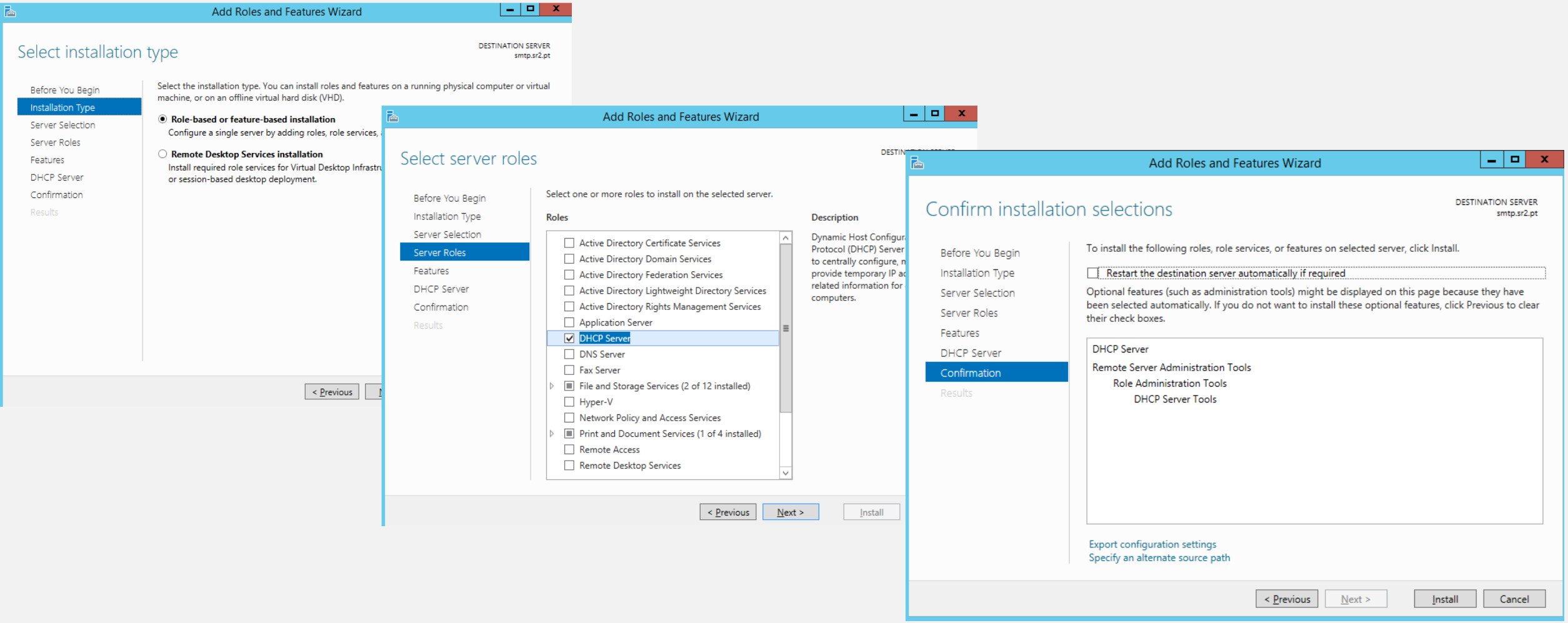
Dynamic Host Configuration Protocol (DHCP) - Windows

Ano Letivo 2019-2020

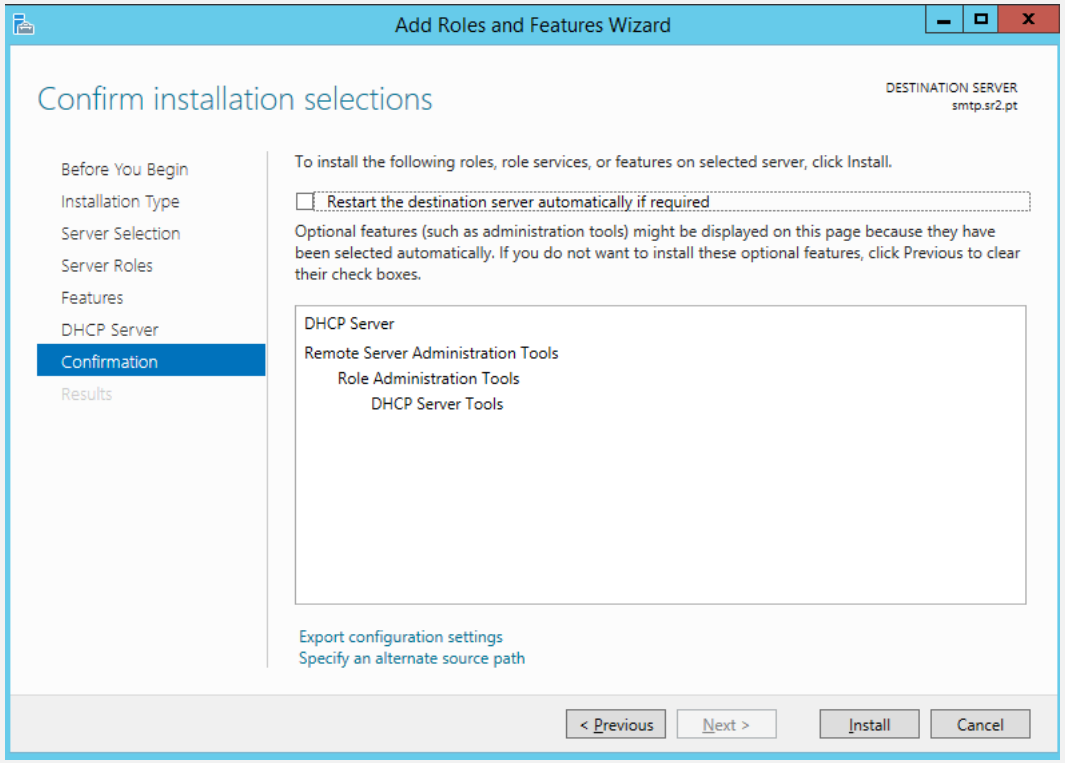
DHCP - Service Installation

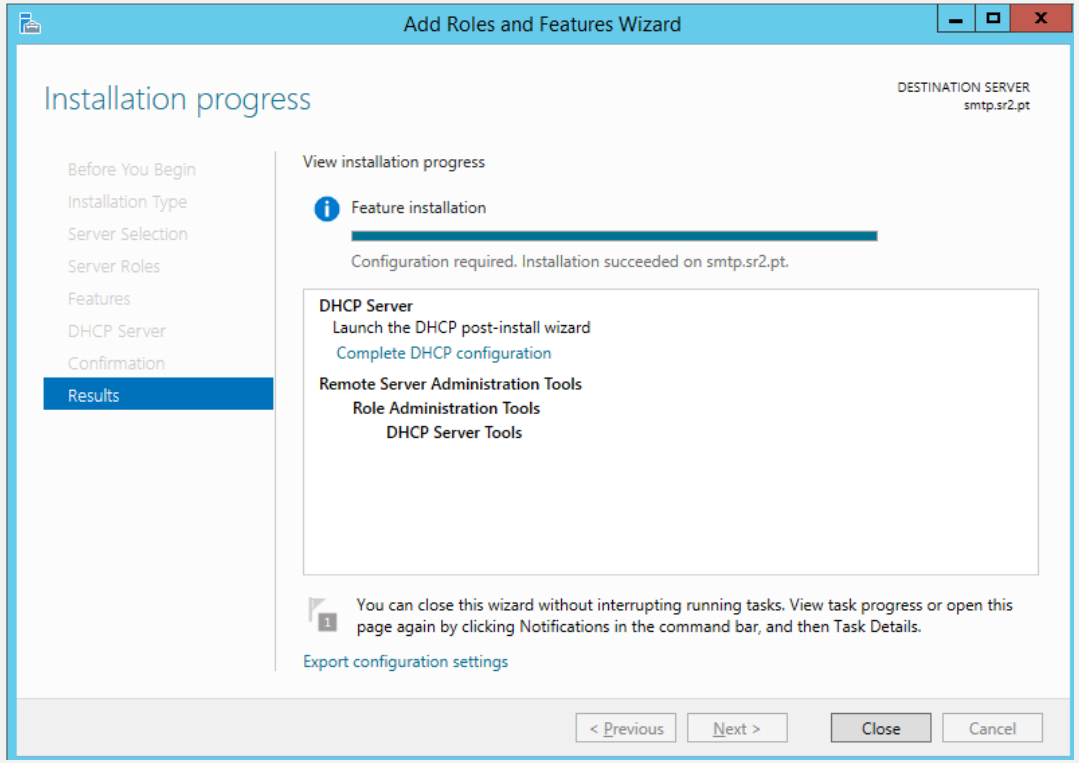
- The installation of the DHCP service in Windows Server 2012 is performed through the Server Manager application, choosing the option "Add roles“.
- At the end of the installation a new DHCP entry is added in the "Administrative Tools" menu.
- You should not use a server / machine with a dynamic address for this type of service.

DHCP - Service Installation

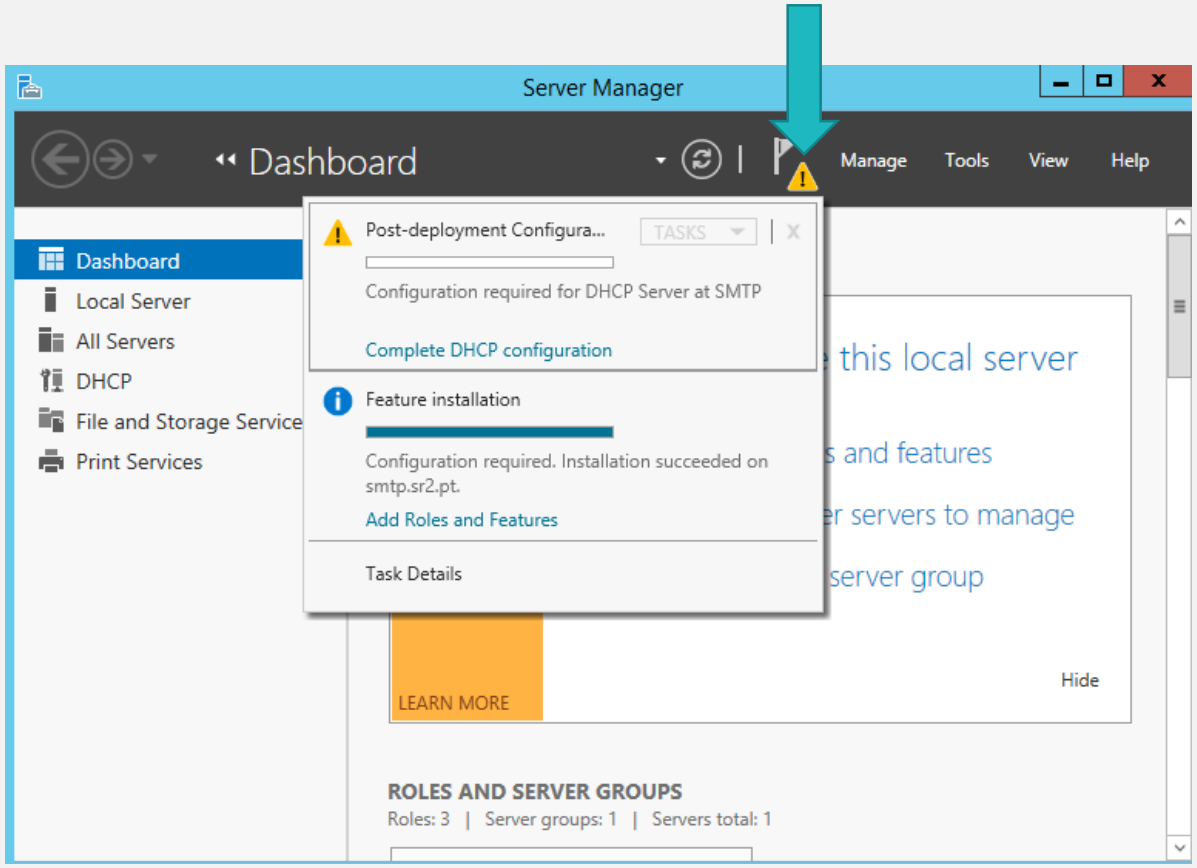


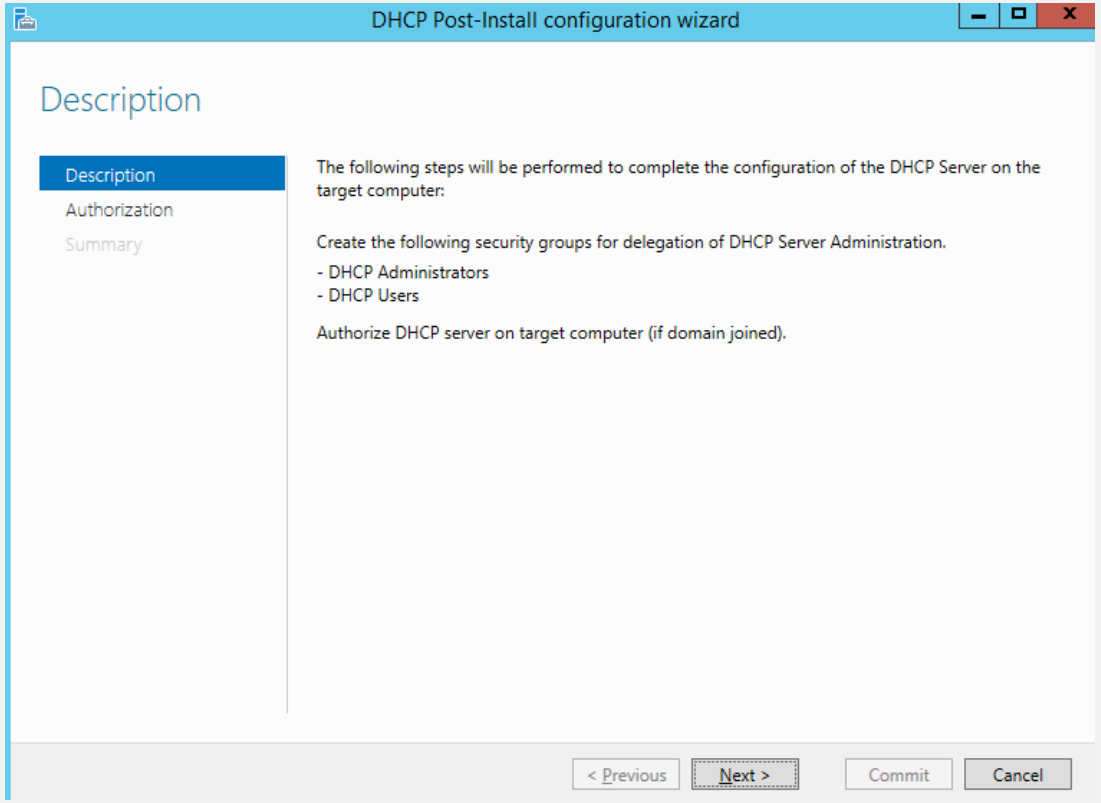
DHCP - Service Installation



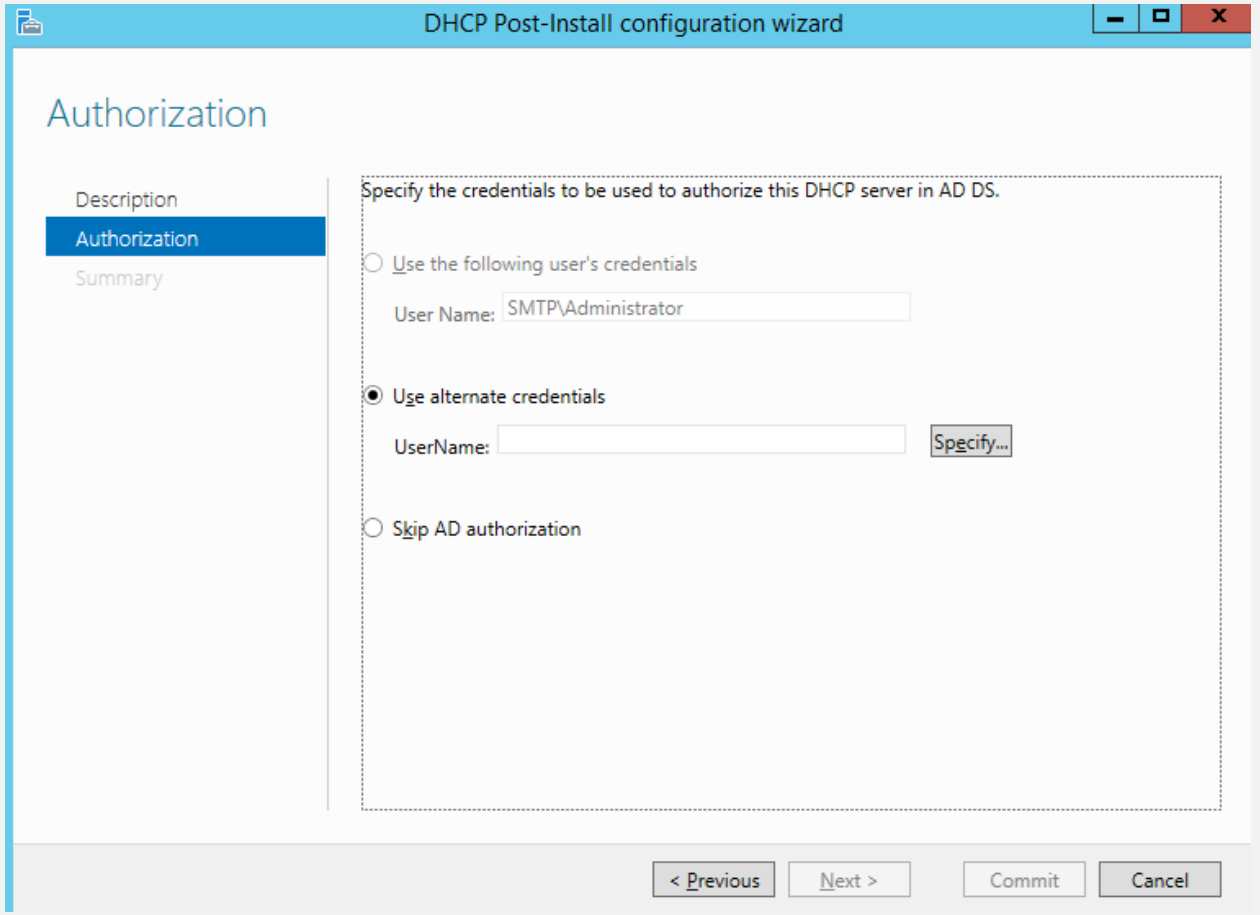


DHCP - Service Installation

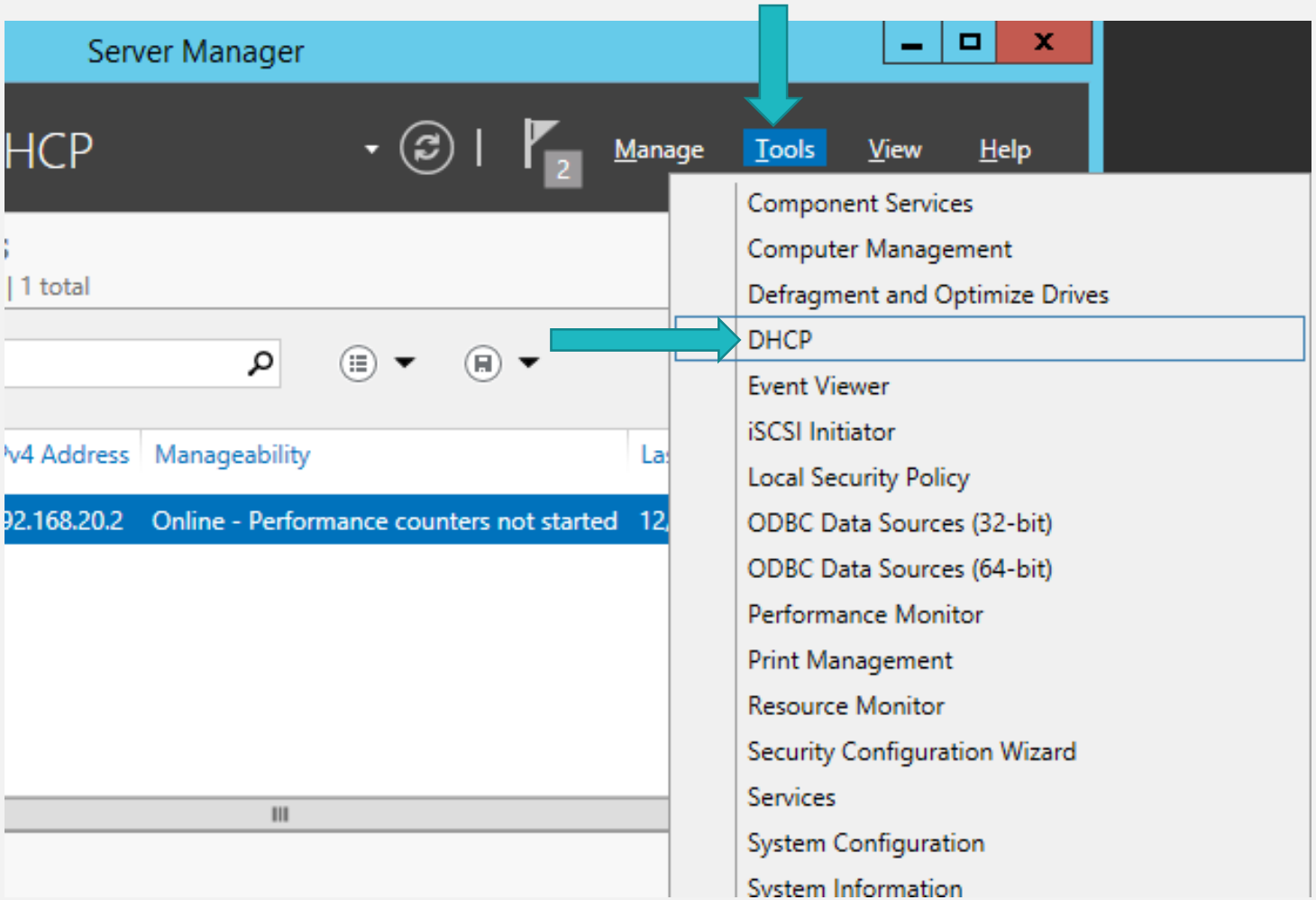




DHCP - Service Installation

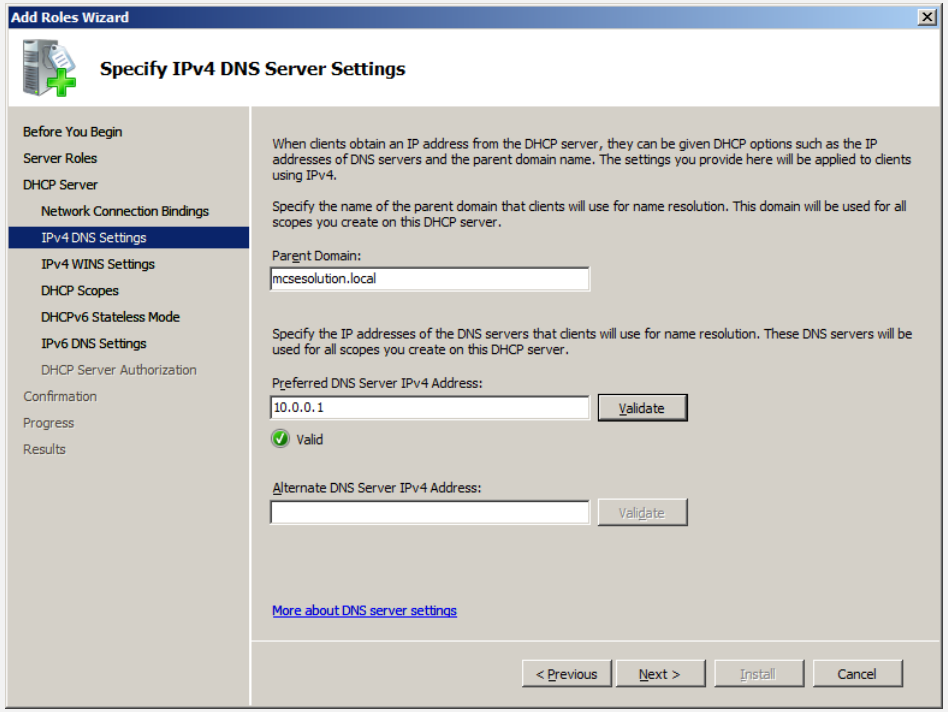


DHCP - Service Installation

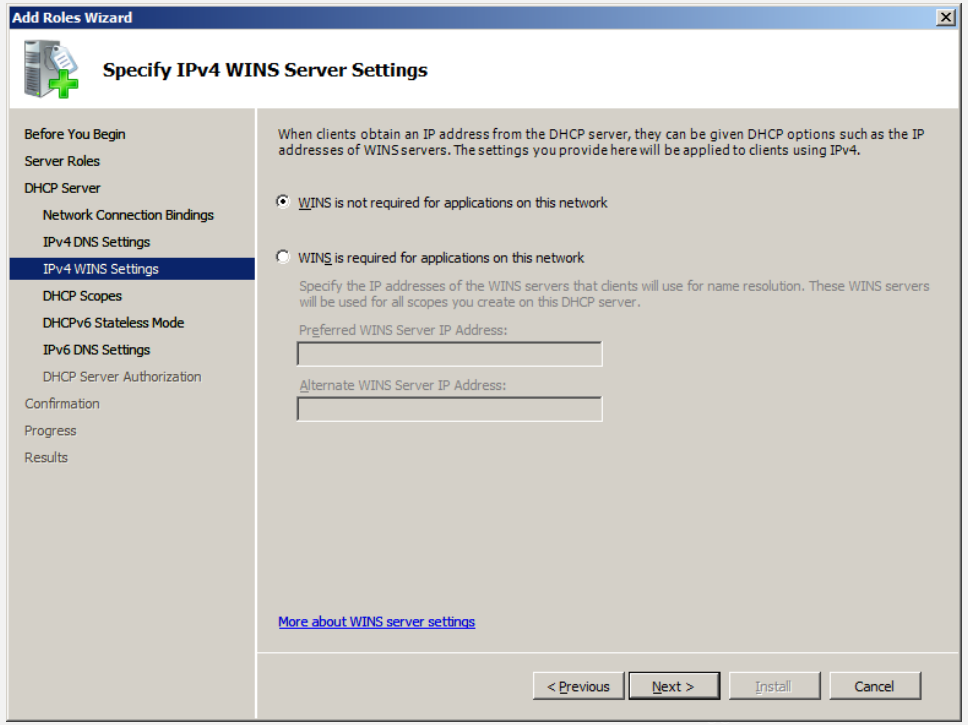


DHCP - Service Installation

- Enter the DNS options (you can then change this setting):
  - Domain Name
  - Primary and alternate DNS server addresses

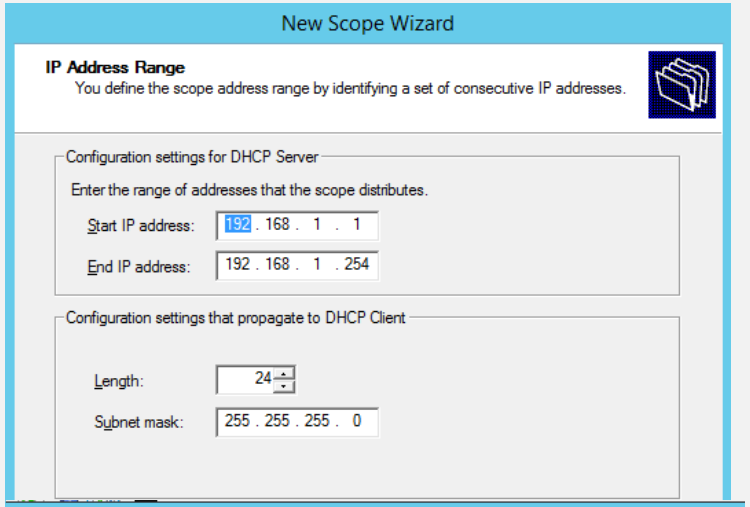


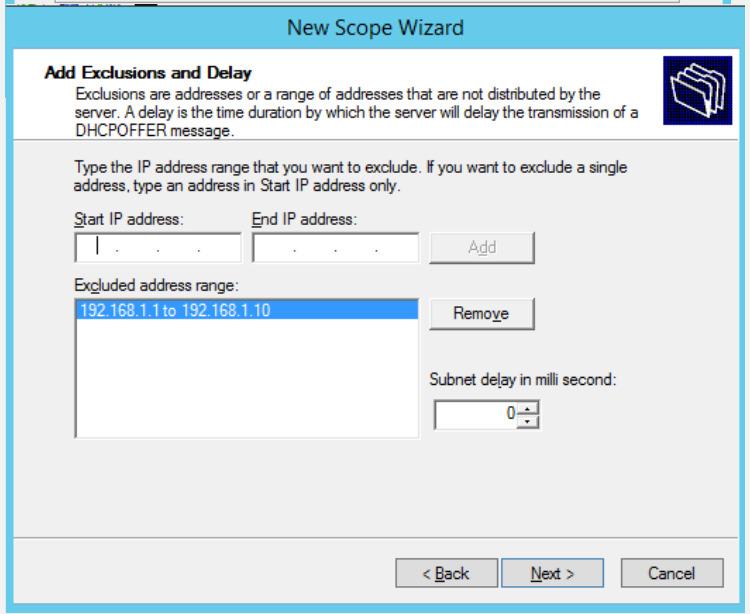
- If your network has a WINS server you can put the IP address of this server here



DHCP - Service Installation

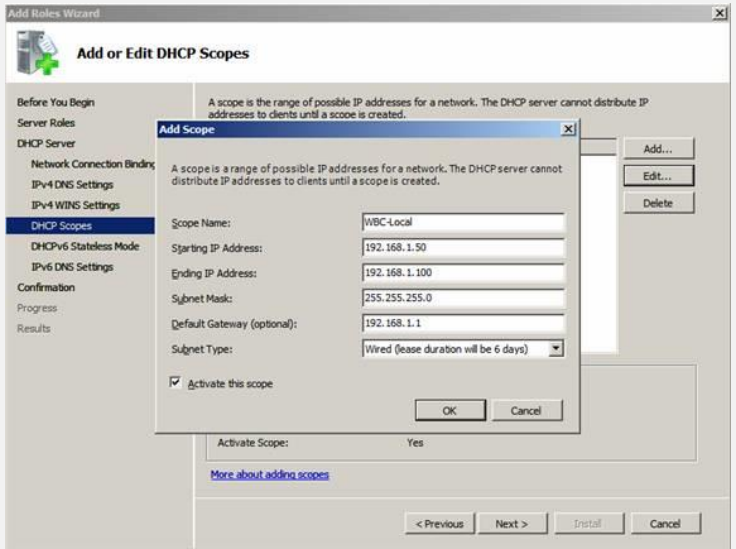
- *Scope*
  - *Set of IP addresses belonging to a logical subnet*
    - *Example: 192.168.1.1-192.168.1.254*
- *Lease*
  - *The act of assigning an IP address to a client*
    - *When the assignment is made it is said that the lease is active*
- *When the lease is carried out, the maximum duration is*
  - *Two base settings (later can be changed)*
    - *Wired networks (6 days)*
    - *Wireless networks (8 hours)*
- *The customer must make the renewal and can be:*
  - *Automatically (operation performed by OS)*
    - *On Windows systems the renewal request is made when half the loan time is reached (information from the server)*
  - *Manually*
    - *ipconfig / release (for release - optional)*
    - *ipconfig / renew*



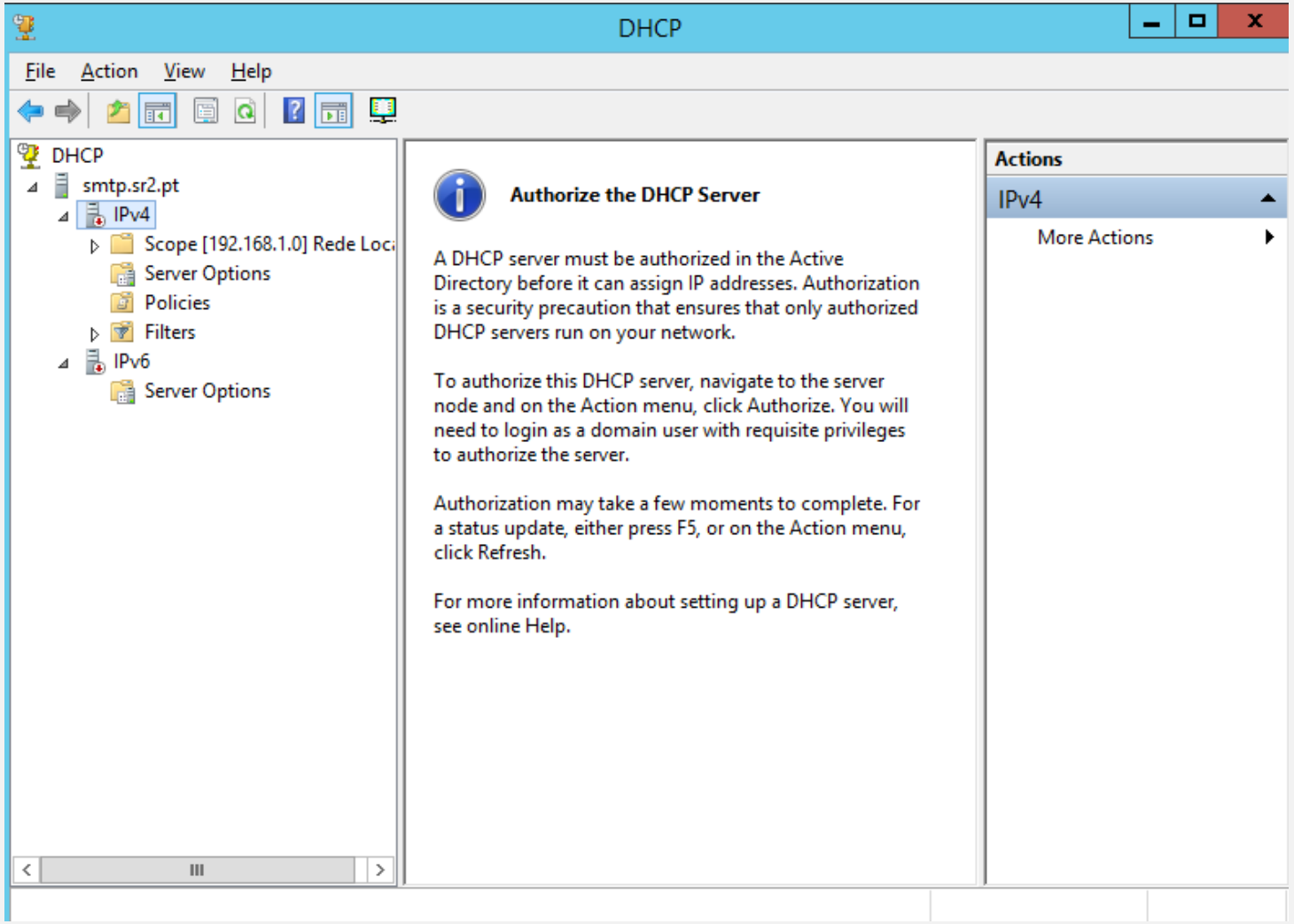


DHCP - Service Installation

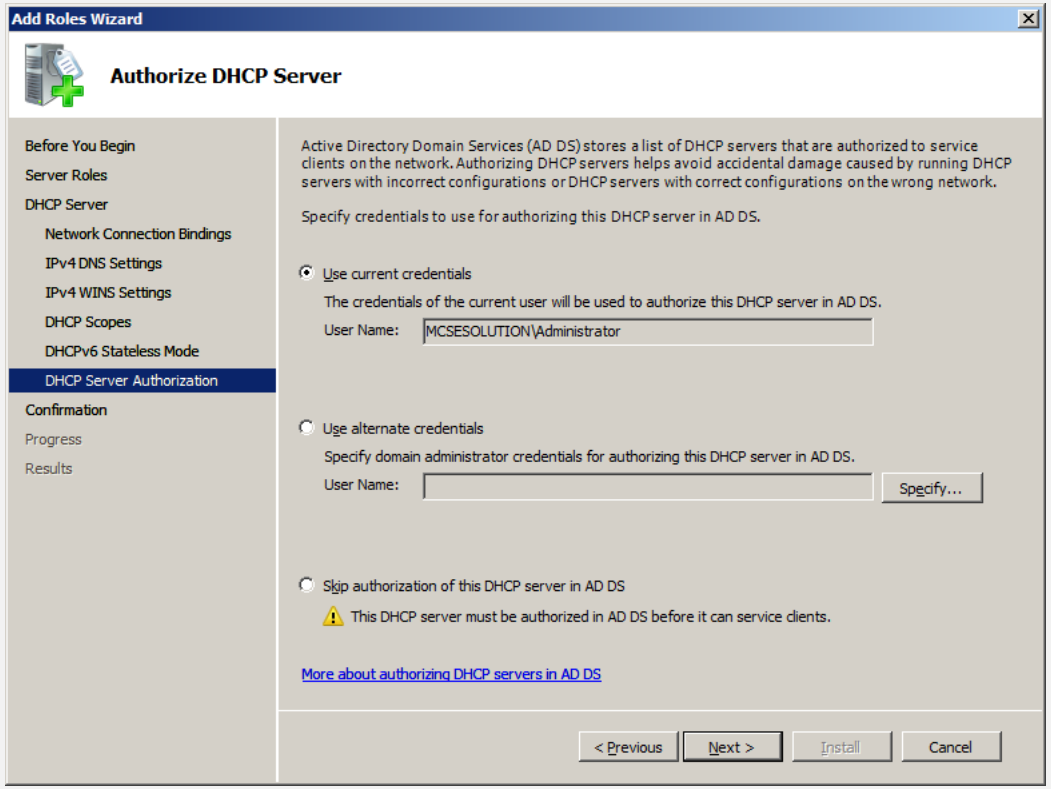
- Indicate:
  - **Scope Name**: Name
  - **Starting IP Address and Ending IP Address**: Start and End Address
  - **Subnet Mask**: Subnet mask used
  - **Default Gateway**: default router address
  - **Subnet Type**: Choose between Wired (6 days) or Wireless (8 days) to set the length of time the IP address is granted.
- Check the Activate this scope option to enable scope when configuration is complete.

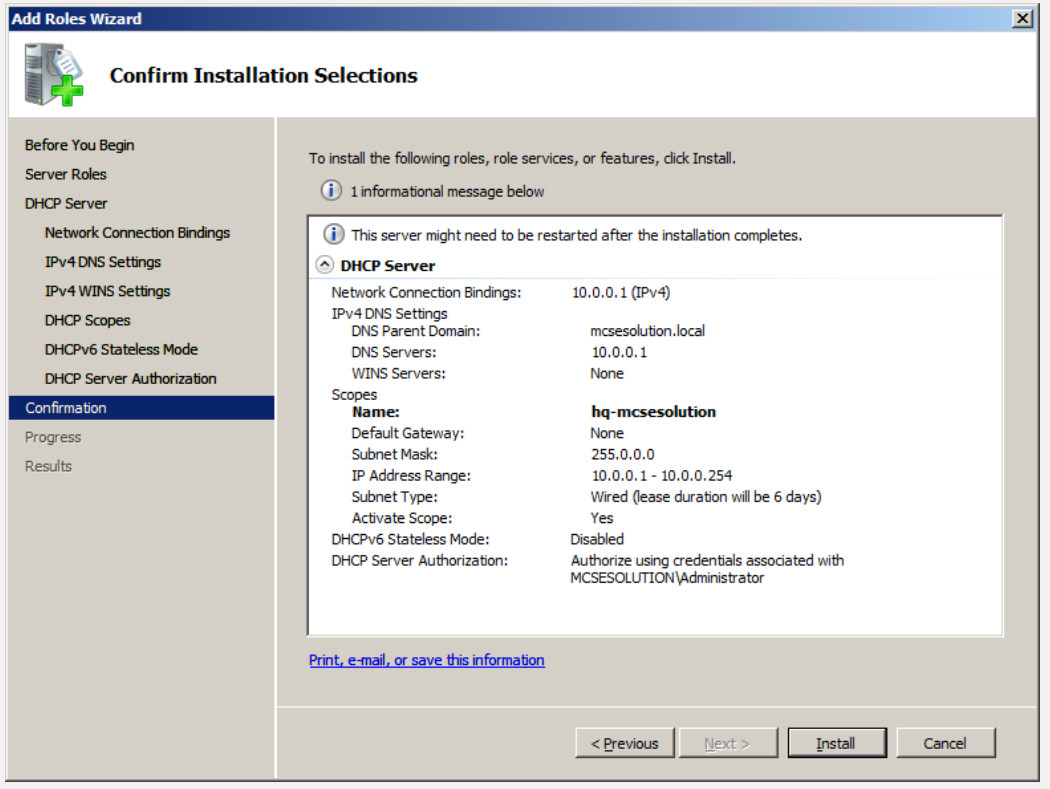


DHCP - Service Installation



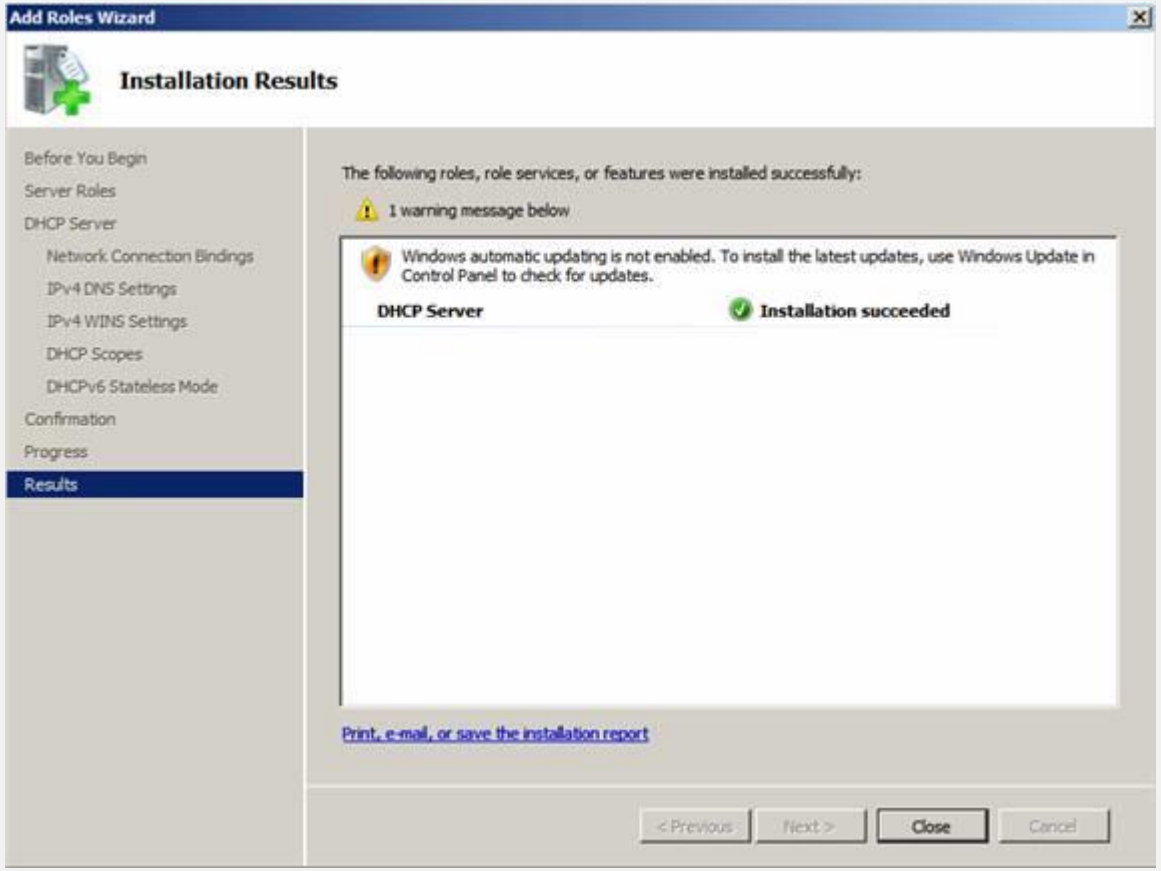
DHCP - Service Installation





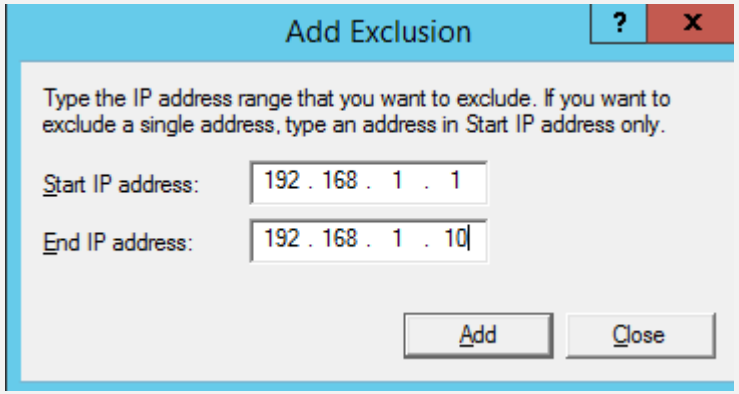
DHCP - Service Installation

- And if everything is well configured your service should be installed and functional.

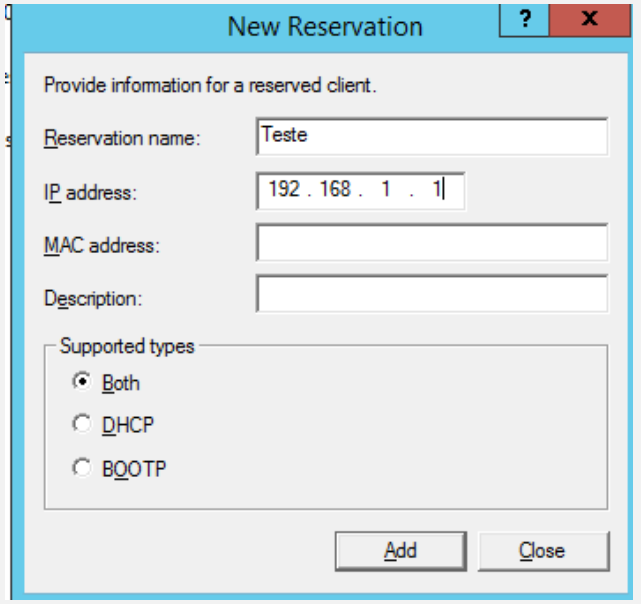


DHCP - Add reservations

- A range of IPs

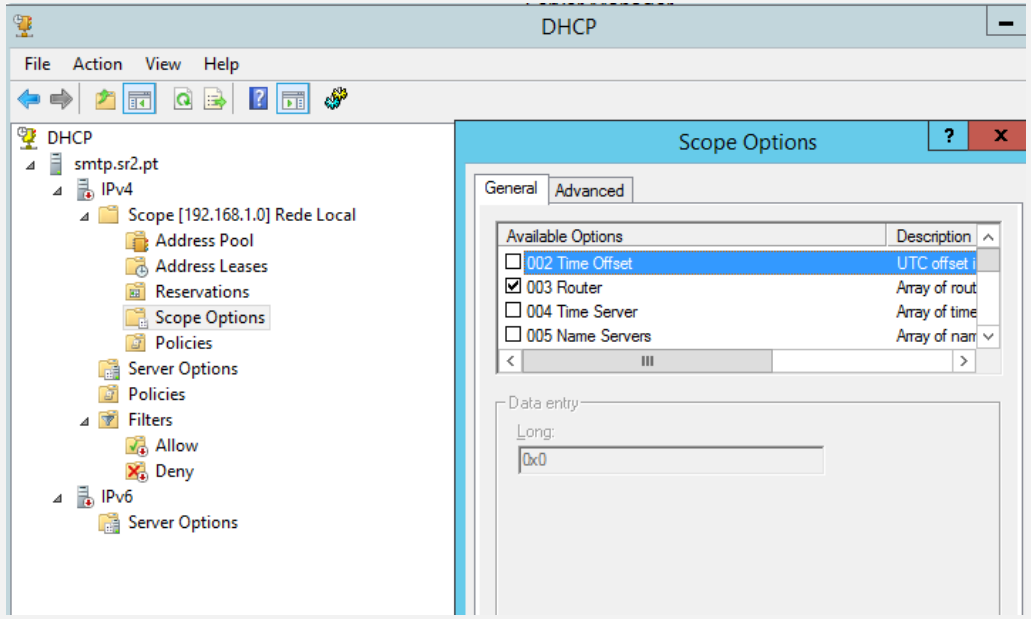


- A specific IP



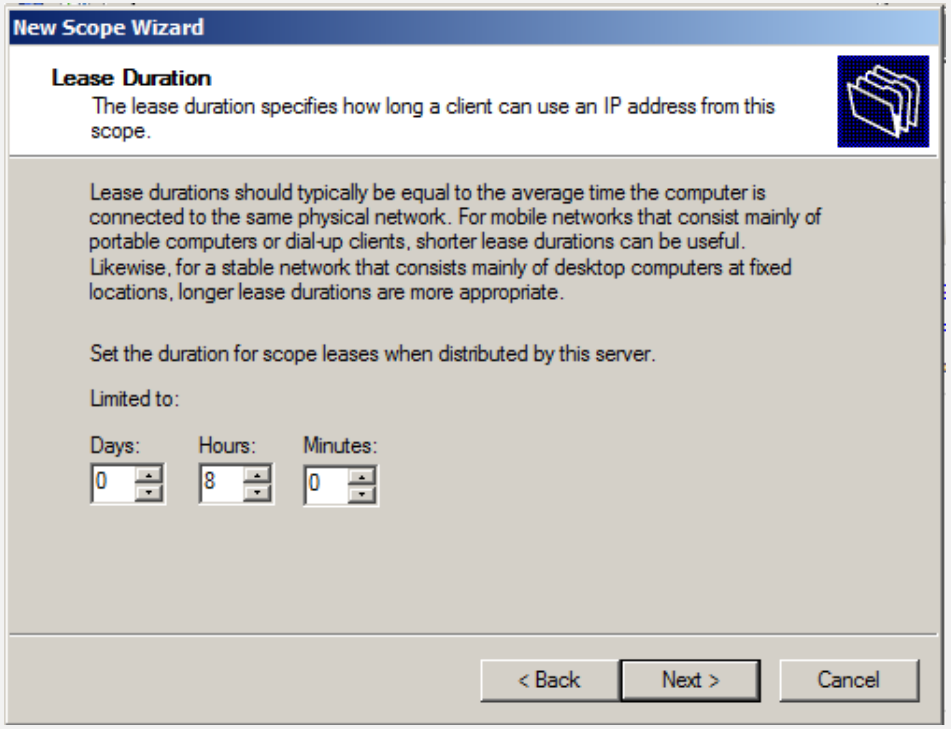
DHCP – *Server Options*

- Here you can configure TCP options and settings common to all scopes.
- Right-click and choose Configure options-> General tab and choose the desired option.
- Afterwards the settings made will appear in the "Server Options", as shown below.



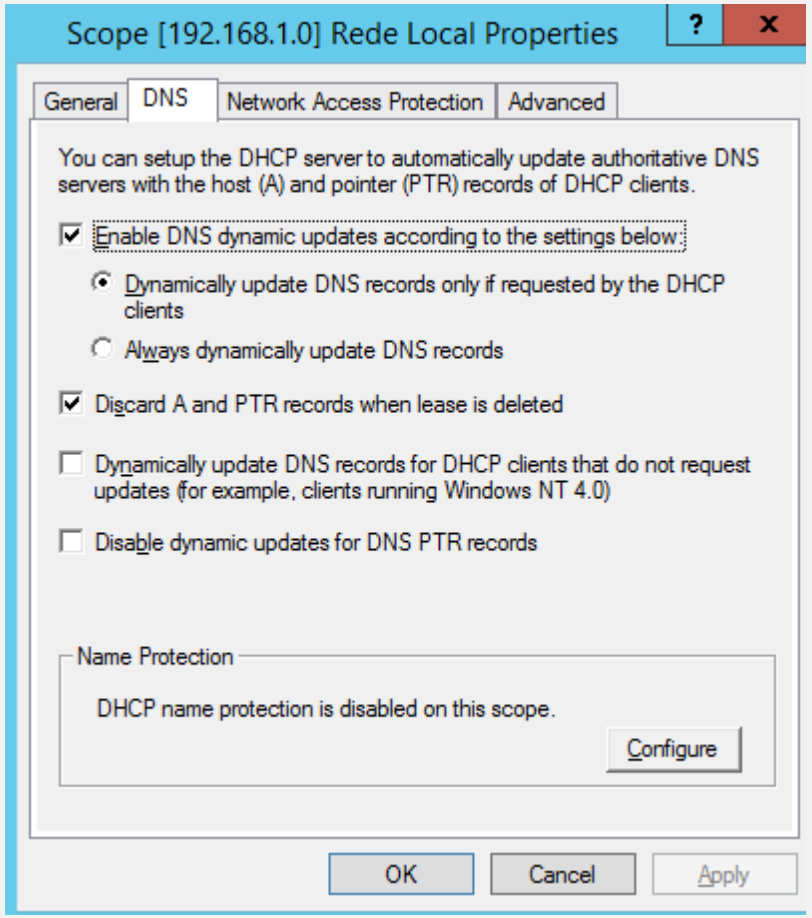
DHCP - Options

- Lease Duration must be adjusted according to the type of network in place so that there are no address safeguards that could affect the assignment of new IP's.
- If the network is more static, a larger value should be assigned, if the network is more dynamic (for example, use of many external portable clients), it should have a smaller value.



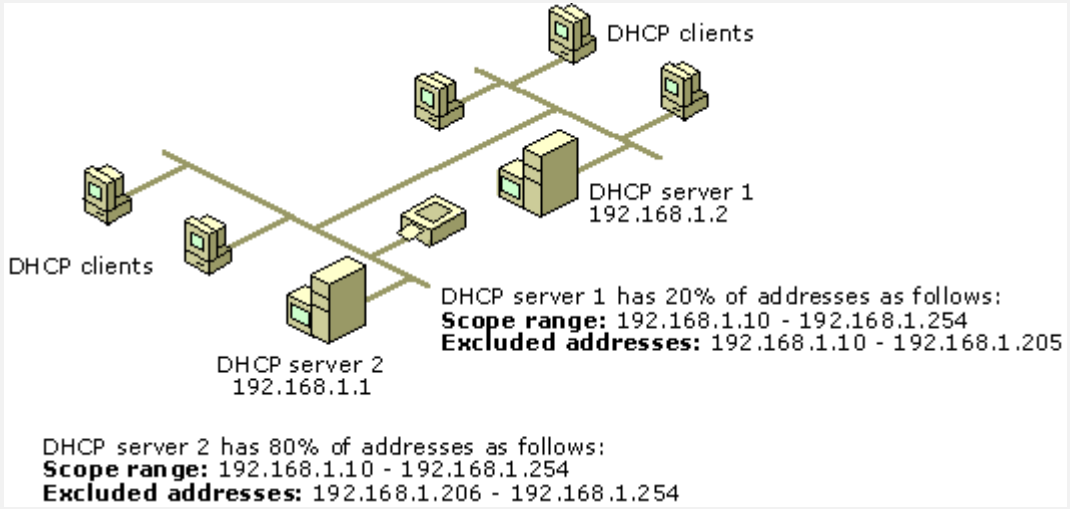
DHCP - DNS

- n windows server it is possible to put DHCP to automatically update DNS.
  1. Go Start | Administrative Tools and choose DHCP
  2. Left-click the scope DHCP scope you want to configure and choose Properties.
  3. Click on the DNS Tab and enable this possibility.
  4. Then you have to go to the DNS server and accept this possibility



DHCP - Redundancy

- Having more than one DHCP server on the same subnet provides greater fault tolerance to meet customer request.
- A common practice for balancing the two DHCP servers on a single network is to have 80% of the addresses distributed by one DHCP server and the remaining 20% to be delivered by a second server.
- The 80-20 rule



Policy-based assignment

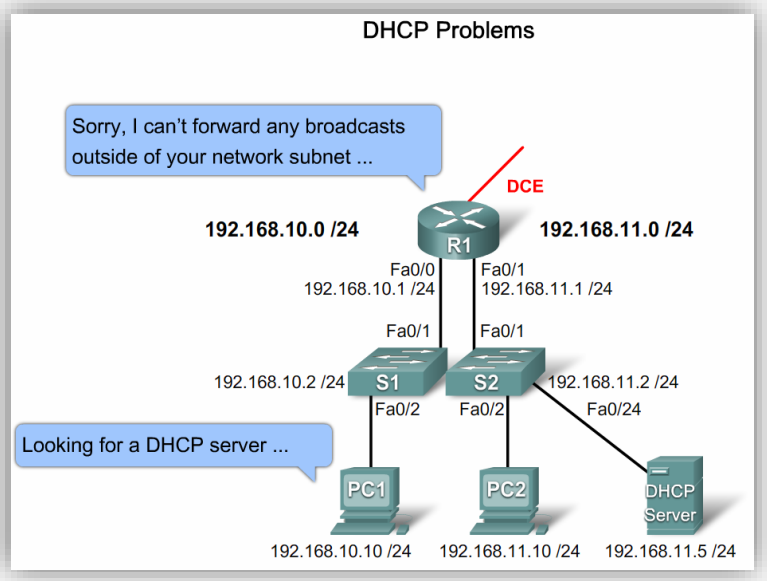
- **Multiple Device Types:** A network includes many different clients such as printers, IP phones, and desktops. Administrators can sort these devices using different IP address ranges. This allows routing and quality of service (QoS) policies based on the range of the IP address to control access or traffic on the network.
- **Multiple functions:** A network includes different types of computers, and servers on the same subnet. Depending on the type of customer, the administrator may want to provide different lease duration settings. All wireless clients that connect through a specific agent can receive a four-hour grant duration. Dynamic DNS updates can be disabled for clients that match this policy.

Policy-based assignment

- **Virtualization:** Virtual machines are added and removed dynamically depending on the load requirements at a given time. The administrator can routing network traffic differently to virtual machines by creating a policy based on the MAC address prefix to assign a short lease duration, a specific IP address range, and a different default gateway.

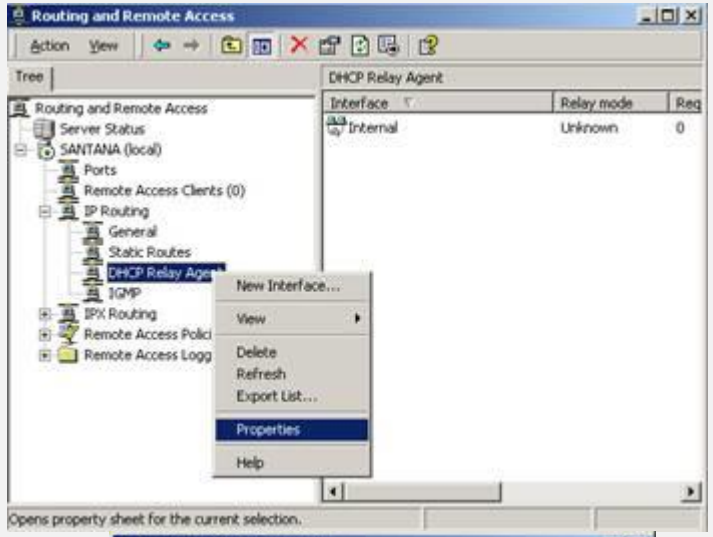
DHCP Relay

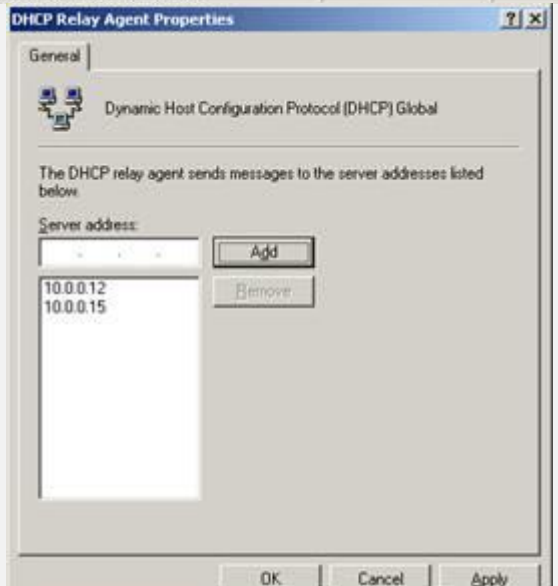
- A DHCP client uses broadcast mechanisms to locate DHCP and request TCP / IP settings.
- The default routers do not route this type of traffic. That is, clients can only obtain TCP / IP settings if the DHCP server is located on the same local network.
- There may be situations in which the DHCP server is located on another subnet, that is, located on another LAN. In this case, we must configure a DHCP Relay Agent on the network where the DHCP server does not exist.
- The DHCP Relay Agent picks up packets sent by DHCP clients, transforms these packets into a format that rr can either forward them to the DHCP server, that is, it is an intermediary between the DHCP clients and the DHCP server.



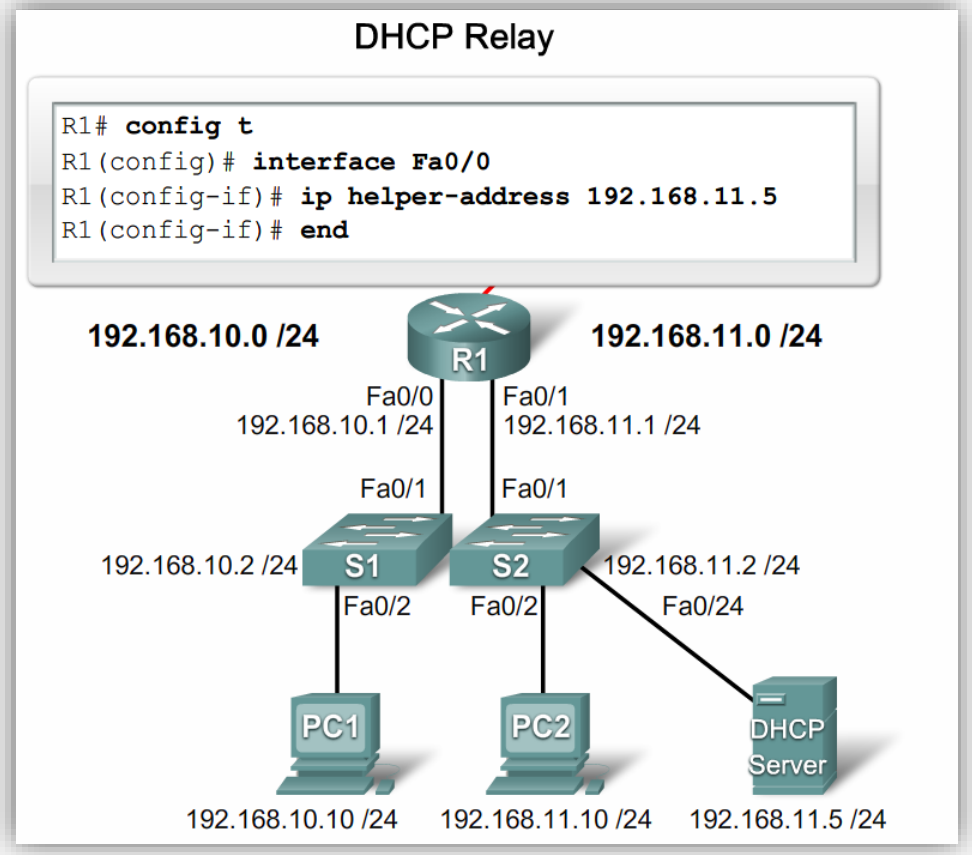
DHCP Relay - windows

- The DHCP Relay Agent is part of the RRAS service. Therefore, in order for us to configure a DHCP Relay Agent we must enable the RRAS service:
  - Log on with an admin account;
  - Open the Routing and Remote Access console
  - Start, -> Administrative Tools, -> Server Manager;
  - Open Roles, and Network Policy and Access Services, and click Routing and Remote Access RRAS;
  - Click the + sign next to the IP Routing option;
  - Right-click on the DHCP Relay Agent option and click on Properties;
  - Type the address of the DHCP server





DHCP Relay - Cisco



Questions

References

- Windows Server 2012, António Rosa, FCA
- www.cisco.com
- http://pt.wikipedia.org
- http://pt.scribd.com/doc/22021856/Apresentacao-DHCP-Rosario
- http://pt.scribd.com/doc/22021986/DHCP-Apresentacao-no-power-point
- http://www.ccc.ipt.pt/~ricardo/ficheiros/RedesComputadores.pdf