

# Network Services 1

2019-2020





Licenciatura em Engenharia Informática  
Ramo de Redes e Administração de Sistemas

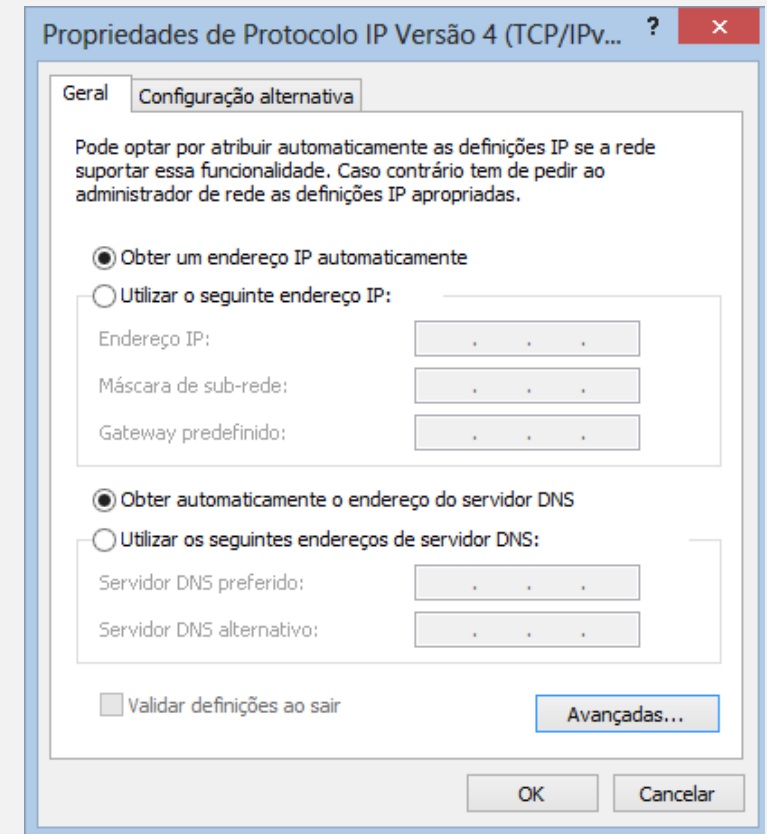
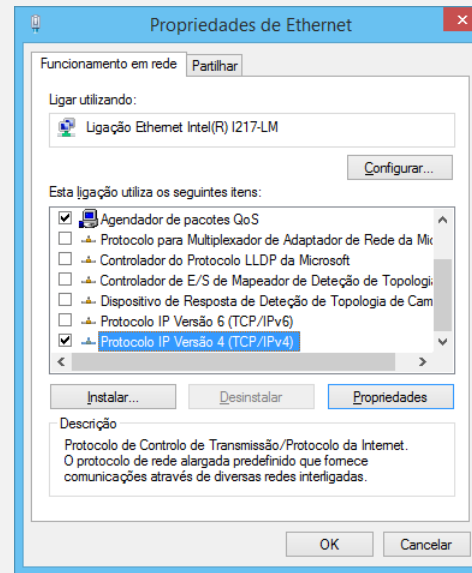
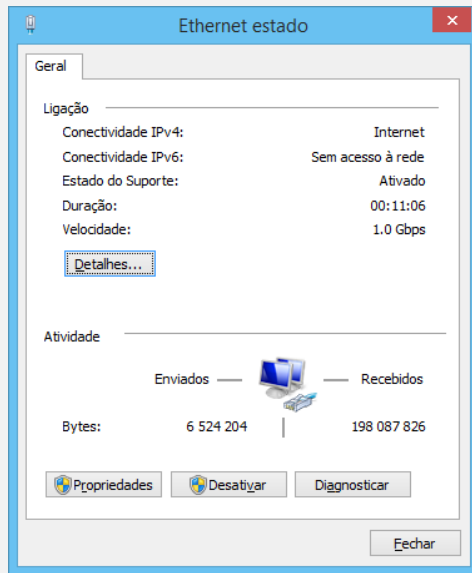
*IP Addressing*

School Year 2019-2020

© - Pedro Geirinhas

# 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

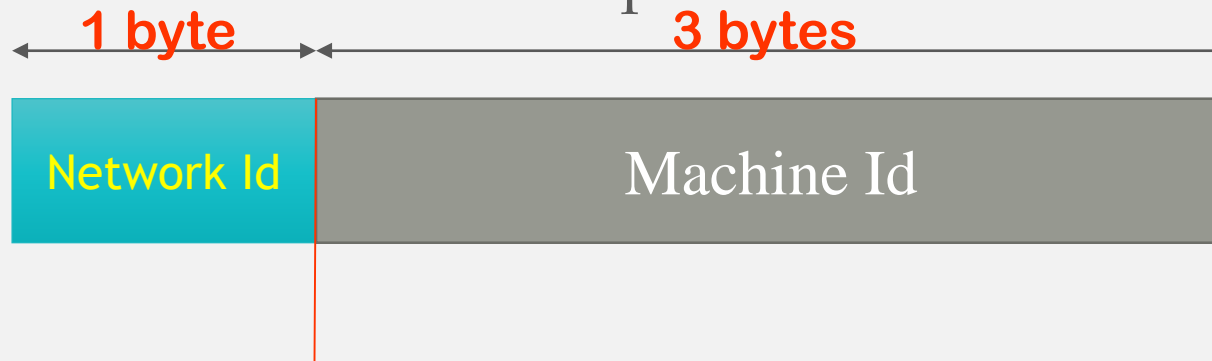


# IP Addressing

- 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**

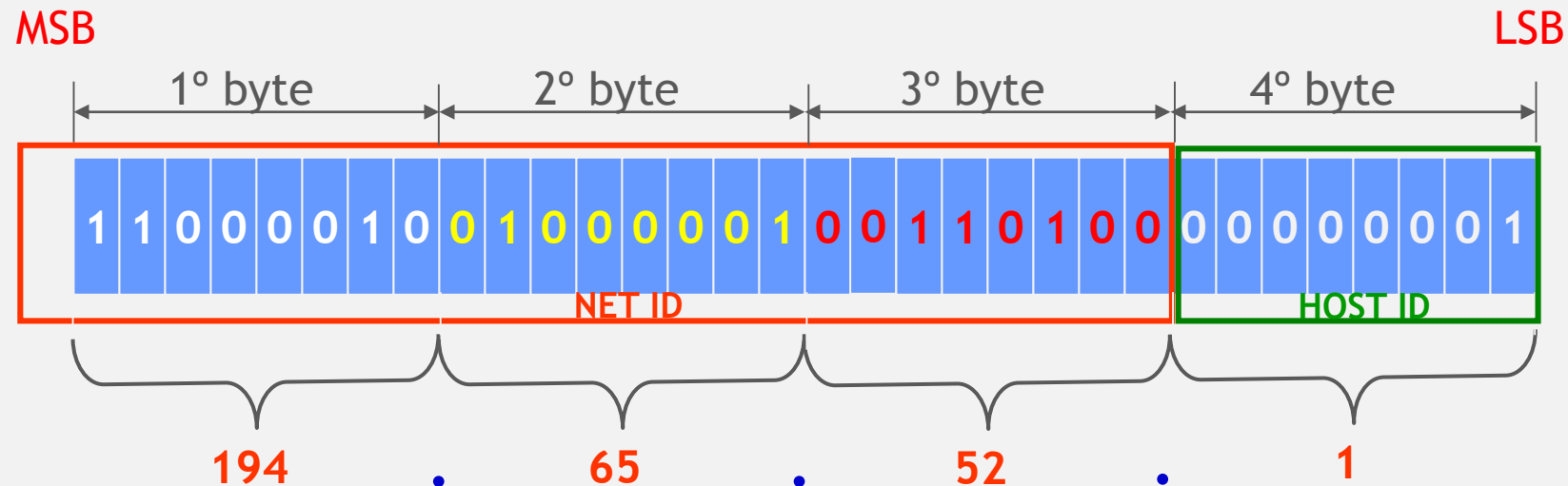
# IP Addressing v4

- IP addresses V4 have a fixed size of 4 bytes (32 bits).
  - For example 192.168.1.1
- The IPv6 addresses (2<sup>96</sup> 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.

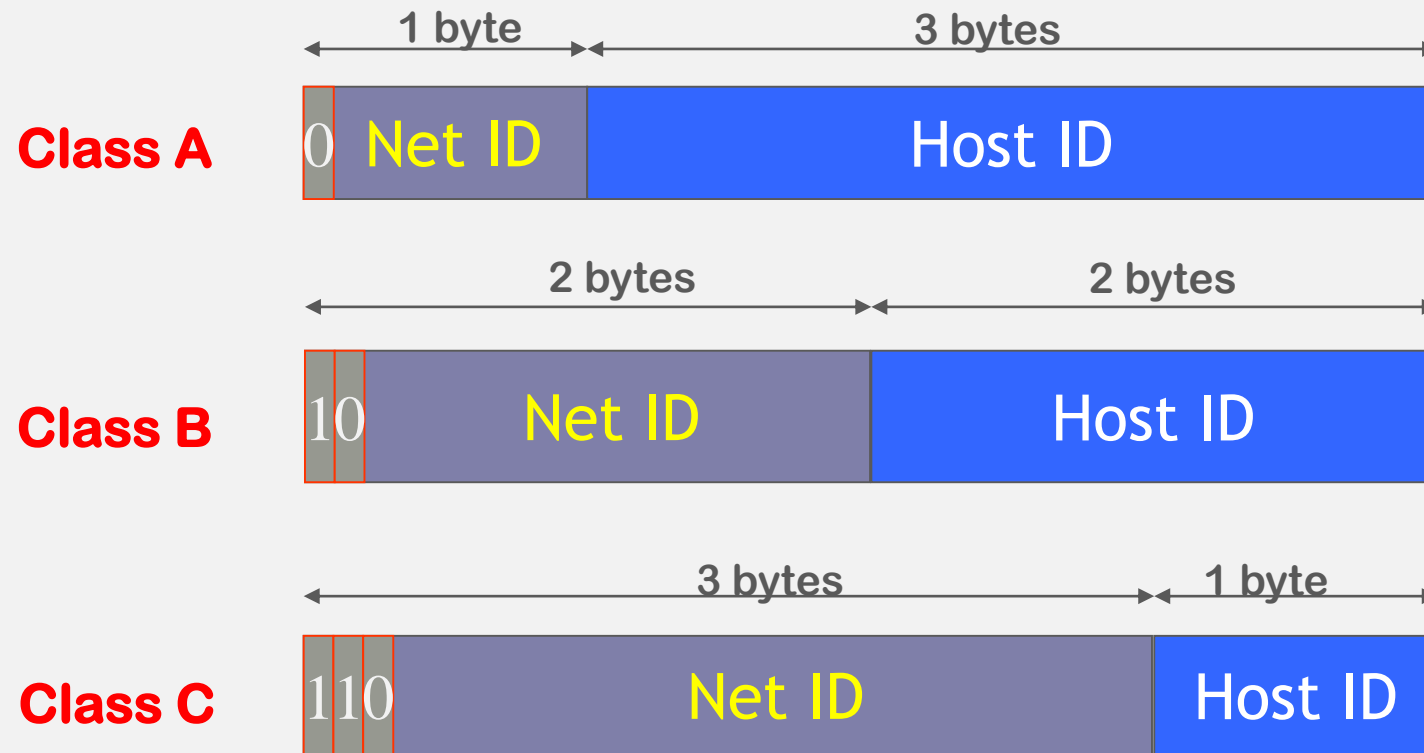


- $194 = 2^7 \cdot 1 + 2^6 \cdot 1 + 2^5 \cdot 0 + 2^4 \cdot 0 + 2^3 \cdot 0 + 2^2 \cdot 0 + 2^1 \cdot 1 + 2^0 \cdot 0 = 128 + 64 + 2 = 194$
- We can define this network as being 194.65.52.0/24 where 24 ( $3 \cdot 8$ ) defines the number of bits to be used in the network identification. Let's see this 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	N° of Networks	N° of machines in network
A	0 - 126	127 ( $2^7 - 2$ )	16.777.214 ( $2^{24}-2$ )
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	1 <sup>o</sup> Host	Last host	Broadcast
1 <sup>a</sup> subnet	192.137.78.0	192.137.78.1	192.168.78.30	192.1637.78.31
2 <sup>a</sup> subnet	193.137.78.32	193.137.78.33	193.137.78.62	193.137.78.63
3 <sup>a</sup> subnet	193.137.78.64	193.137.78.65	193.137.78.94	193.137.78.95
4 <sup>a</sup> subnet	193.137.78.96	193.137.78.97	193.137.78.126	193.137.78.127
5 <sup>a</sup> subnet	192.137.78.128	193.137.78.129	193.137.78.158	193.137.78.159
6 <sup>a</sup> subnet	192.137.78.160	193.137.78.161	193.137.78.190	193.137.78.191
7 <sup>a</sup> subnet	192.137.78.192	193.137.78.193	193.137.78.222	193.137.78.223
8 <sup>a</sup> 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

					<b>Mask</b>
	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)*

# 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)

```
Placa de rede local sem fios Ligação de rede sem fios:
Estado do suporte . . . . . : Suporte desligado
Sufixo DNS específico da ligação. :
Descrição . . . . . : Placa LAN Sem Fios 802.11n
Endereço físico . . . . . : 00-22-5F-55-91-D9
DHCP activado . . . . . : Sim
Autoconfiguração activada . . . . : Sim

Adaptador ethernet Ligação de Área Local:
Sufixo DNS específico da ligação. : ccdrc.global
Descrição . . . . . : Realtek PCIe GBE Family Controller
Endereço físico . . . . . : 00-23-54-A4-04-FD
DHCP activado . . . . . : Sim
Autoconfiguração activada . . . . : Sim
Endereço IPv6 de local de ligação : fe80::8091:72:f2ca:e150%11<Preferido>
Endereço IPv4 . . . . . : 10.9.35.199<Preferido>
Máscara de sub-rede . . . . . : 255.255.255.0
Concessão obtida. . . . . : quinta-feira, 5 de Março de 2015 08:56:39
Concessão obtida válida até . . . : quinta-feira, 5 de Março de 2015 17:26:23
```

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

```

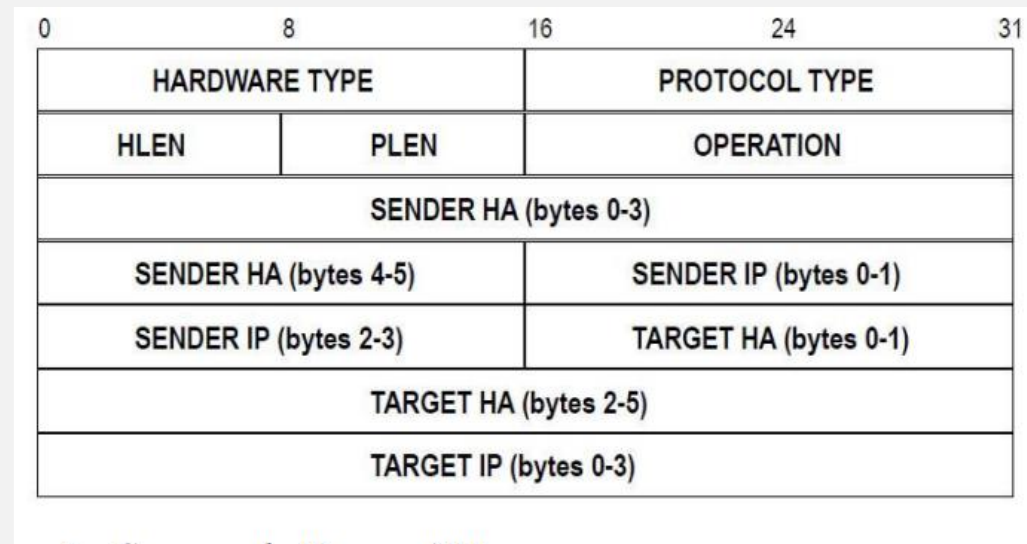
C:\Users\pgeirinhas>arp -a

Interface: 10.9.35.199 --- 0x3
Internet Address      Physical Address      Type
10.9.35.1             78-fe-3d-4f-2a-c1    dynamic
10.9.35.255           ff-ff-ff-ff-ff-ff    static
224.0.0.22            01-00-5e-00-00-16    static
224.0.0.251           01-00-5e-00-00-fb    static
224.0.0.252           01-00-5e-00-00-fc    static
239.255.255.250       01-00-5e-7f-ff-fa    static

Interface: 192.168.206.1 --- 0xa
Internet Address      Physical Address      Type
192.168.206.255       ff-ff-ff-ff-ff-ff    static
224.0.0.22            01-00-5e-00-00-16    static
224.0.0.251           01-00-5e-00-00-fb    static
224.0.0.252           01-00-5e-00-00-fc    static
239.255.255.250       01-00-5e-7f-ff-fa    static

Interface: 192.168.196.1 --- 0xc
Internet Address      Physical Address      Type
192.168.196.255       ff-ff-ff-ff-ff-ff    static
224.0.0.22            01-00-5e-00-00-16    static
224.0.0.251           01-00-5e-00-00-fb    static
224.0.0.252           01-00-5e-00-00-fc    static
239.255.255.250       01-00-5e-7f-ff-fa    static

C:\Users\pgeirinhas>
```



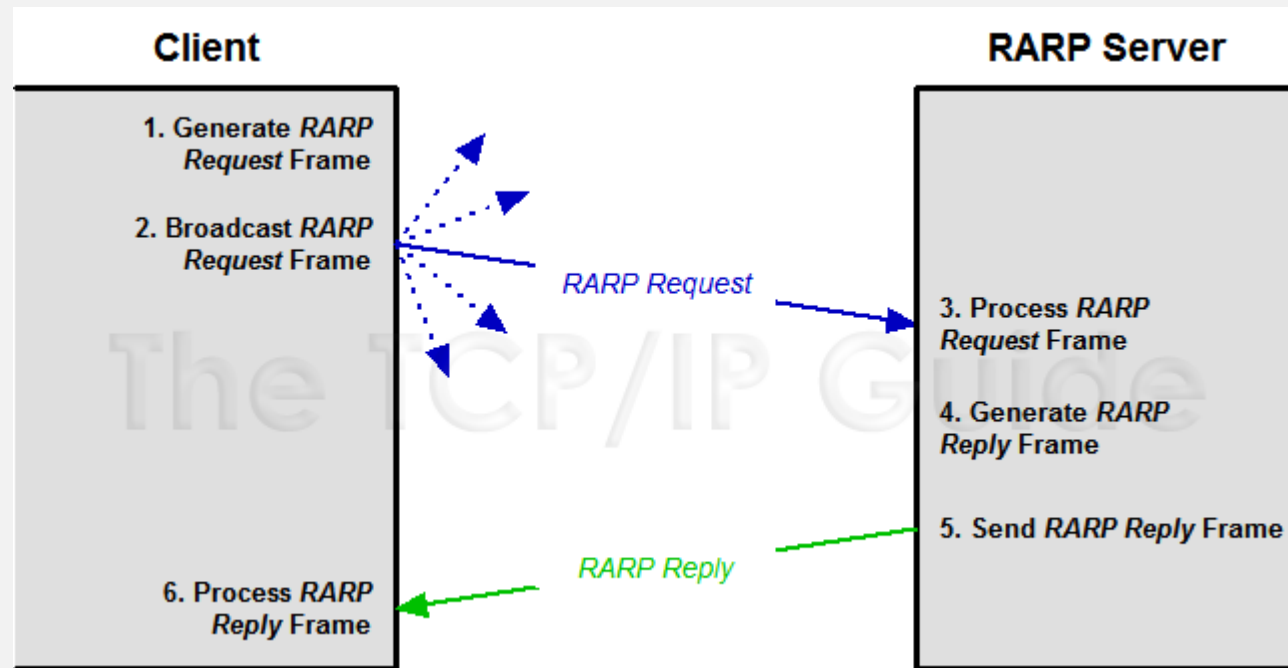
# RARP (Reverse Address Resolution Protocol)

- 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.

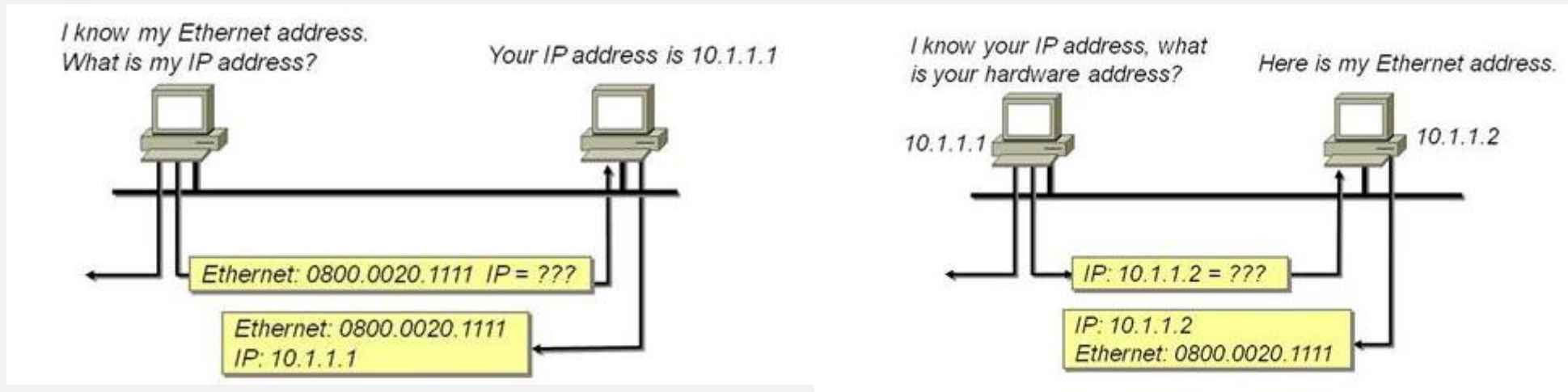
# RARP

- 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



# RARP X ARP



RARP

ARP





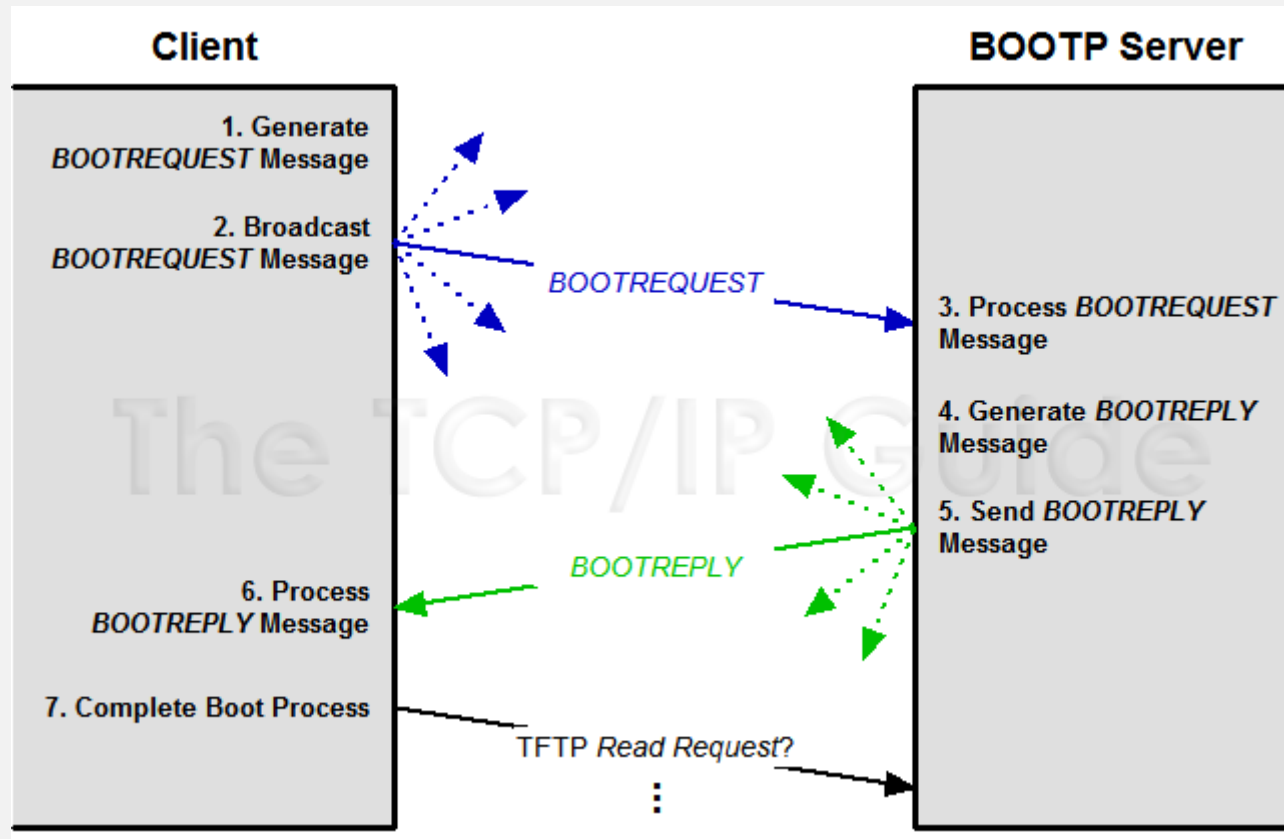
# RARP - Limitations

- 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 (*BOOTstrap Protocol*)

- 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 (*BOOT*strap Protocol)

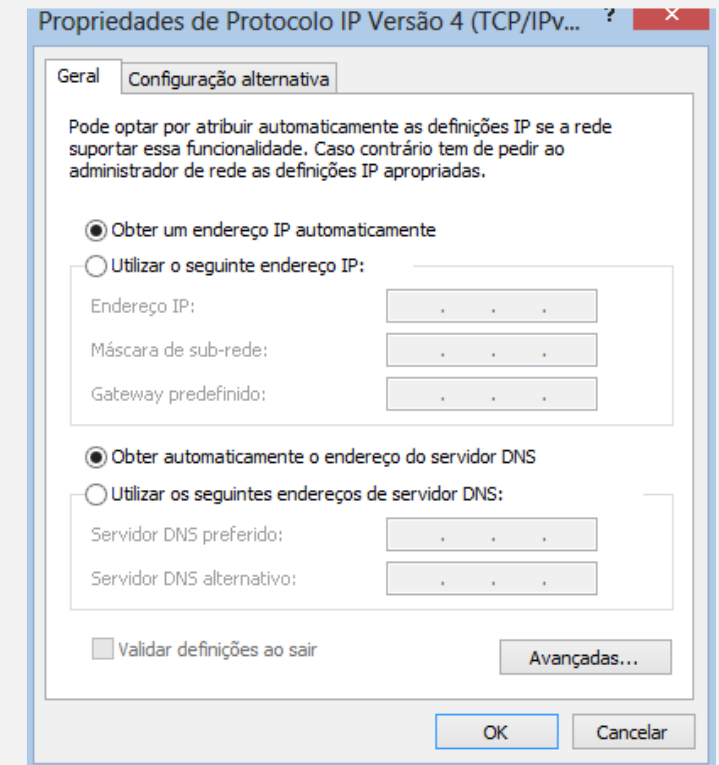


# BOOTP - Limitations

- 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.

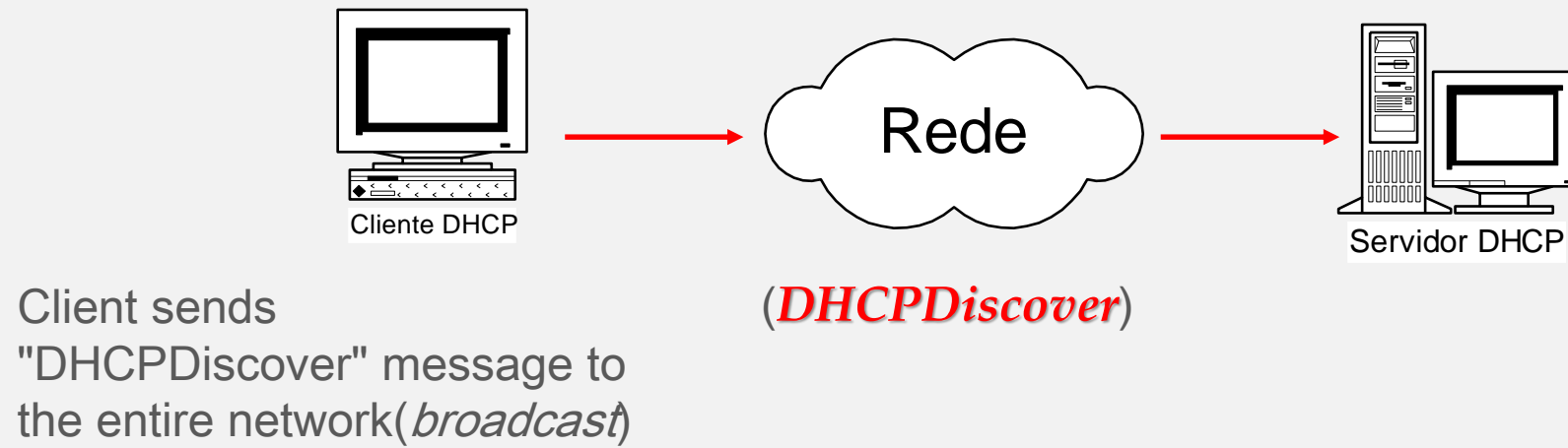
- **Reservation**

- 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

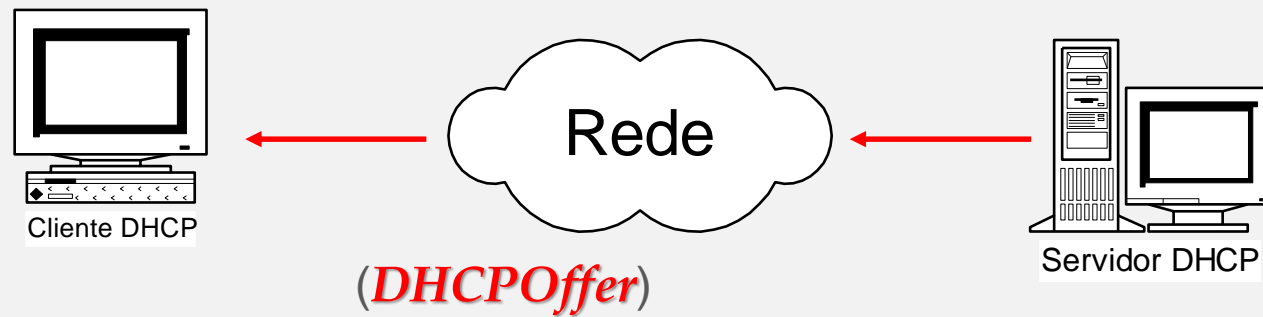
- Uses the UDP protocol on the following ports:
  - Server: port 67
  - Customer: port 68
- The messages used in the protocol for information negotiation are as follows:
  - **Discover**
    - Sent by the client to verify the existence of DHCP servers on the network.
  - **Offer**
    - Message sent 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



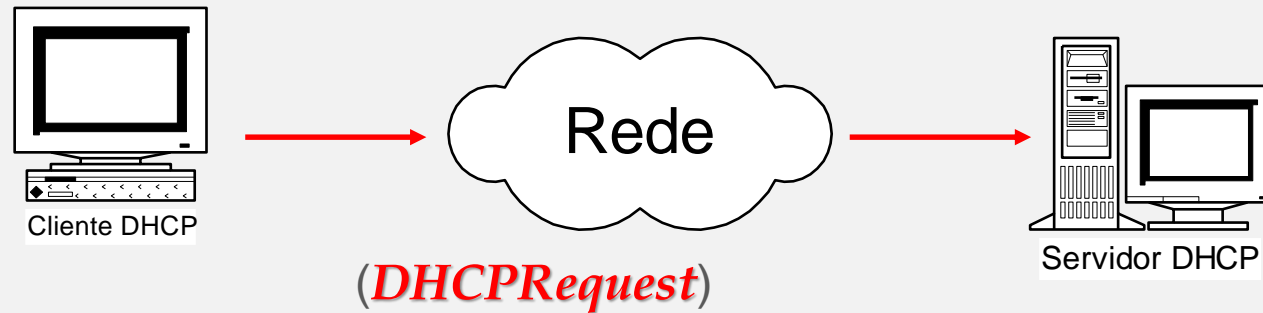
The format of this message is specific, being recognized only by the DHCP server (s) that are present in the local network.

# 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)

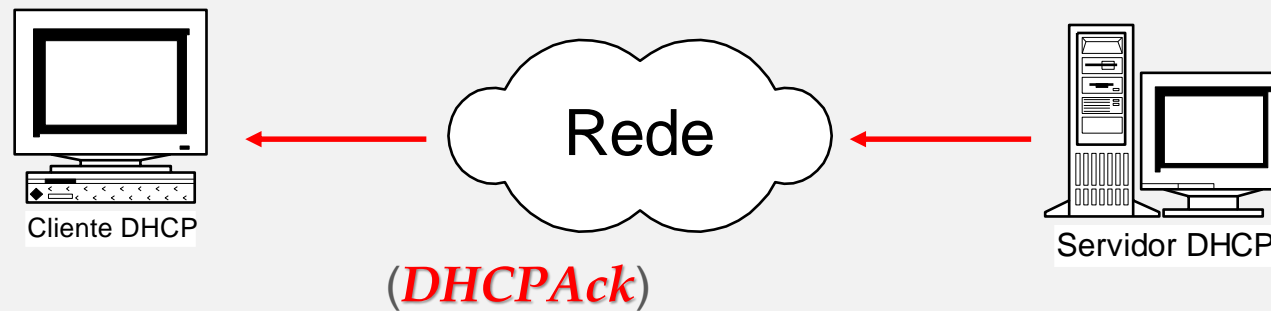
# DHCP - Initial granting procedure



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

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

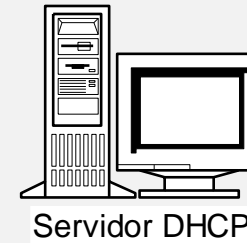
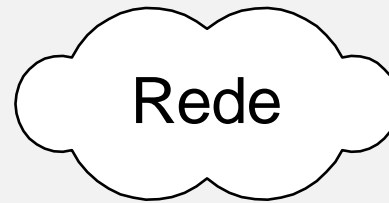
# DHCP - Initial granting procedure



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



# DHCP - Initial granting procedure



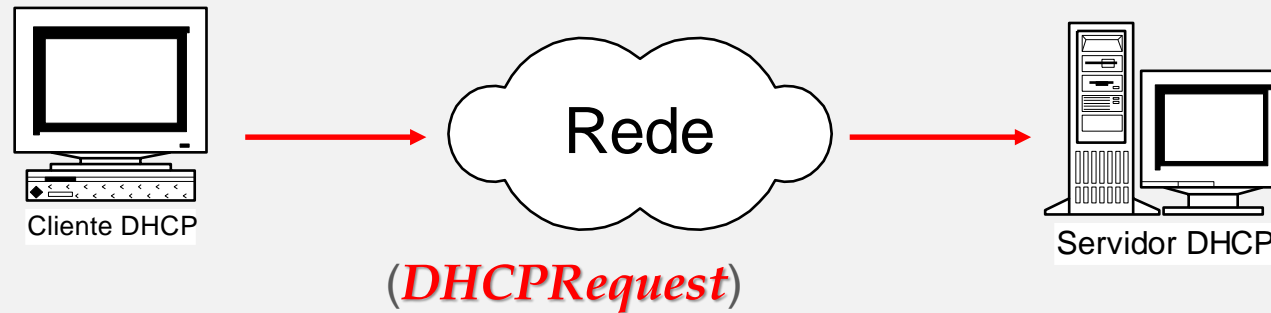
After receiving DHCPAck from the DHCP server, the client configures the d0 TCP / IP properties using the information sent by the DHCP server in the DHCPOffer message and is ready to communicate!

# Grant Renewal Process

---

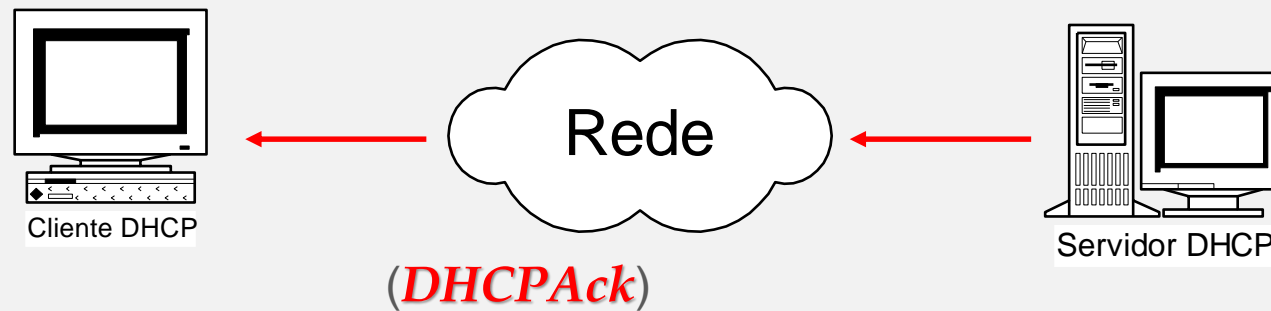
- When a DHCP client is shut down and rebooted (on the same subnet), it usually gets a lease for the same IP address it had before it was turned off.
- After half of the client lease time has elapsed, the client attempts to renew the lease with the DHCP server.

# 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

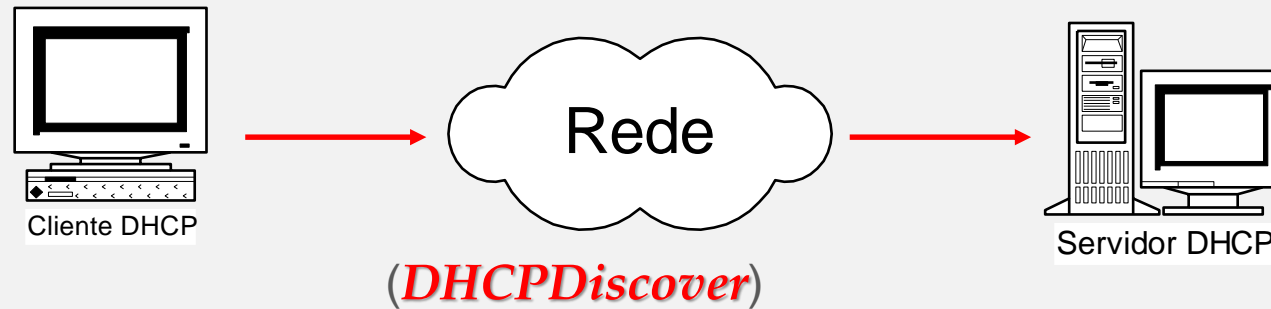
# Grant Renewal Process



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

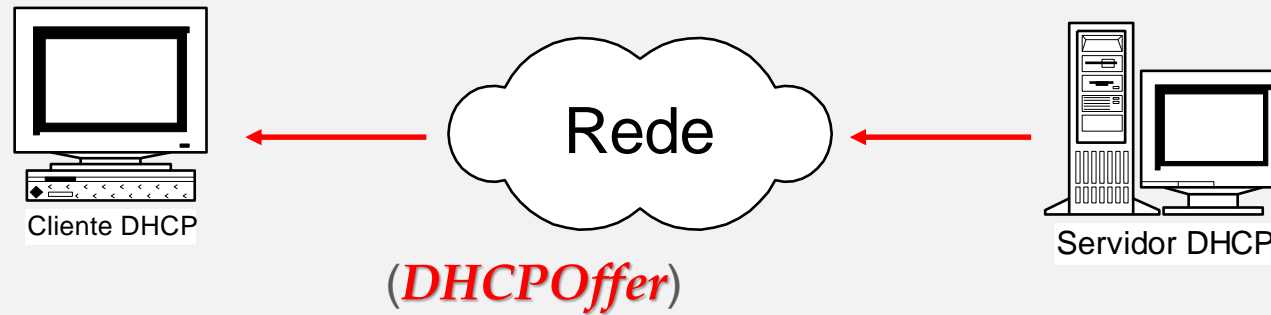
If some of the TCP-IP information used has changed, the server sends the new values so that the client can update them.

# 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 DHCP Offer 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***

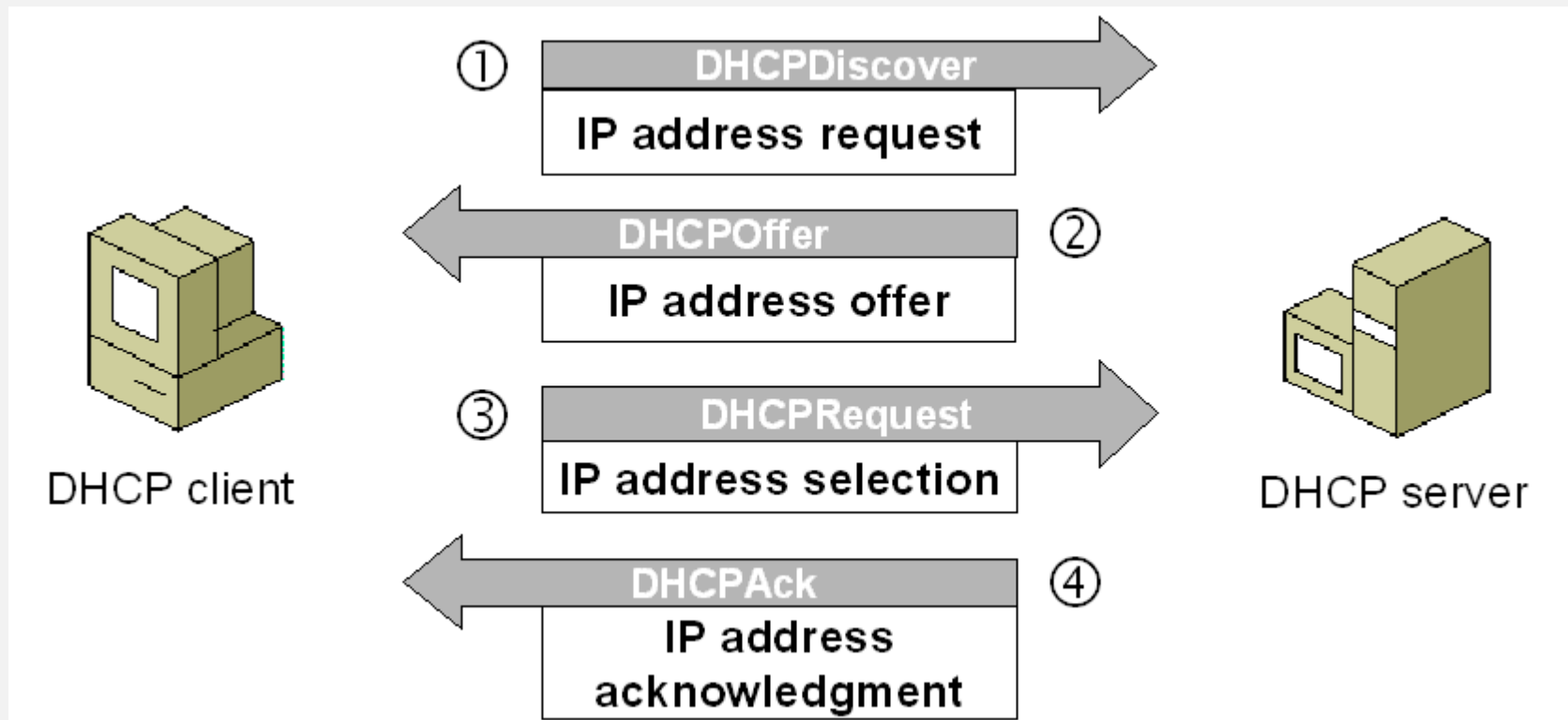
- Sent by a DHCP client to a server that provided the grant thus releasing the IP that had been assigned to it.



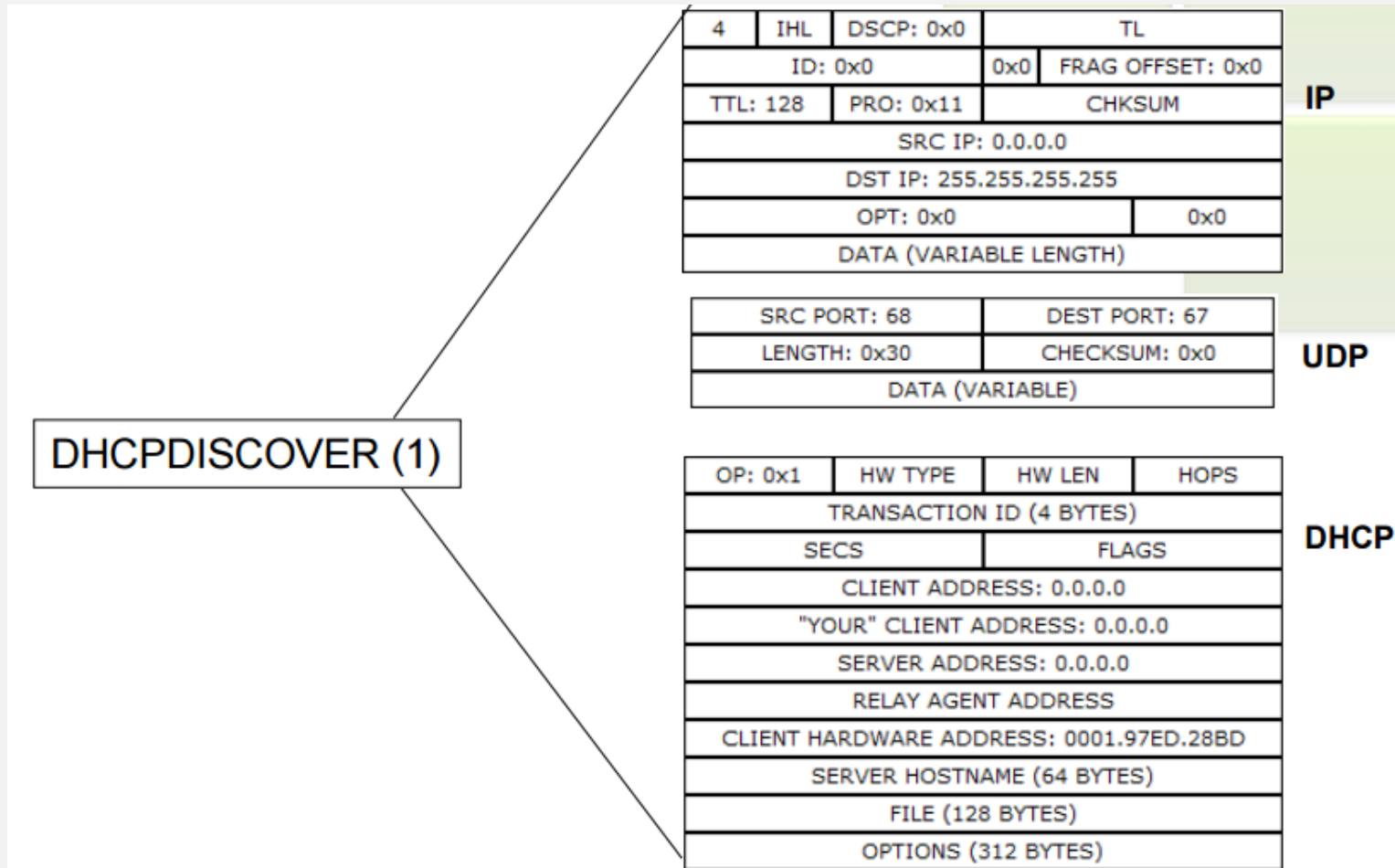
# Message format

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

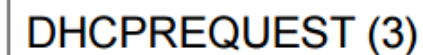
DHCPOFFER (2)

4	IHL	DSCP: 0x0	TL	
ID: 0x0		0x0	FRAG OFFSET: 0x0	
TTL: 128	PRO: 0x11	CHKSUM		
SRC IP: 192.168.10.1				
DST IP: 255.255.255.255				
OPT: 0x0			0x0	
DATA (VARIABLE LENGTH)				

SRC PORT: 67		DEST PORT: 68	
LENGTH: 0x30		CHECKSUM: 0x0	
DATA (VARIABLE)			

OP: 0x2	HW TYPE	HW LEN	HOPS
TRANSACTION ID (4 BYTES)			
SECS		FLAGS	
CLIENT ADDRESS: 0.0.0.0			
"YOUR" CLIENT ADDRESS: 192.168.10.100			
SERVER ADDRESS: 192.168.10.1			
RELAY AGENT ADDRESS			
CLIENT HARDWARE ADDRESS: 0001.97ED.28BD			
SERVER HOSTNAME (64 BYTES)			
FILE (128 BYTES)			
OPTIONS (312 BYTES)			

# Message format



4	IHL	DSCP: 0x0	TL	
ID: 0x0			0x0	FRAG OFFSET: 0x0
TTL: 128		PRO: 0x11	CHKSUM	
SRC IP: 0.0.0.0				
DST IP: 255.255.255.255				
OPT: 0x0				0x0
DATA (VARIABLE LENGTH)				

IP

SRC PORT: 68	DEST PORT: 67
LENGTH: 0x30	CHECKSUM: 0x0
DATA (VARIABLE)	

## UDP

OP: 0x3	HW TYPE	HW LEN	HOPS
TRANSACTION ID (4 BYTES)			
SECS		FLAGS	
CLIENT ADDRESS: 0.0.0.0			
"YOUR" CLIENT ADDRESS: 192.168.10.100			
SERVER ADDRESS: 192.168.10.1			
RELAY AGENT ADDRESS			
CLIENT HARDWARE ADDRESS: 0001.97ED.28BD			
SERVER HOSTNAME (64 BYTES)			
FILE (128 BYTES)			
OPTIONS (312 BYTES)			

## DHCP

# Message format

DHCPACK (4)

4	IHL	DSCP: 0x0	TL	
ID: 0x0			0x0	FRAG OFFSET: 0x0
TTL: 128	PRO: 0x11		CHKSUM	
SRC IP: 192.168.10.1				
DST IP: 255.255.255.255				
OPT: 0x0				0x0
DATA (VARIABLE LENGTH)				

IP

SRC PORT: 67	DEST PORT: 68
LENGTH: 0x30	CHECKSUM: 0x0
DATA (VARIABLE)	

UDP

OP: 0x5	HW TYPE	HW LEN	HOPS
TRANSACTION ID (4 BYTES)			
SECS		FLAGS	
CLIENT ADDRESS: 0.0.0.0			
"YOUR" CLIENT ADDRESS: 192.168.10.100			
SERVER ADDRESS: 192.168.10.1			
RELAY AGENT ADDRESS			
CLIENT HARDWARE ADDRESS: 0001.97ED.28BD			
SERVER HOSTNAME (64 BYTES)			
FILE (128 BYTES)			
OPTIONS (312 BYTES)			

DHCP

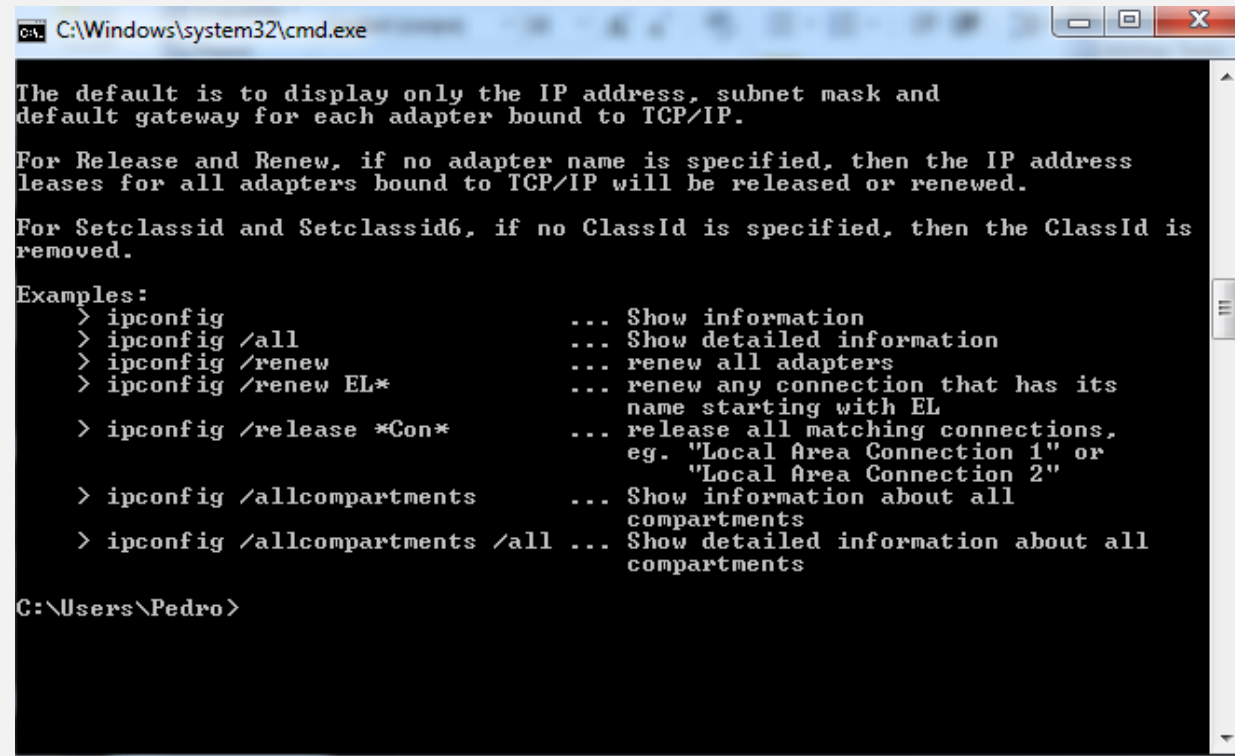
# Security

---

- 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*



```
C:\Windows\system32\cmd.exe

The default is to display only the IP address, subnet mask and
default gateway for each adapter bound to TCP/IP.

For Release and Renew, if no adapter name is specified, then the IP address
leases for all adapters bound to TCP/IP will be released or renewed.

For Setclassid and Setclassid6, if no ClassId is specified, then the ClassId is
removed.

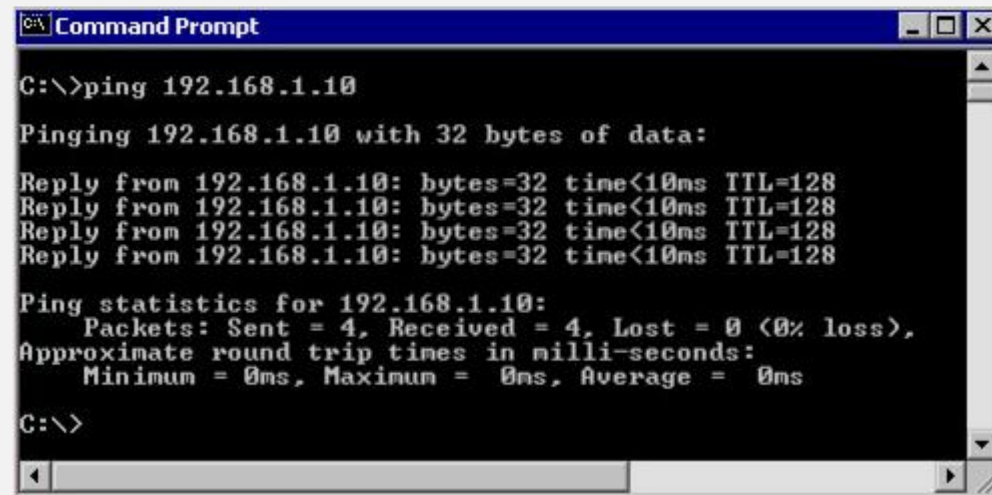
Examples:
> ipconfig                ... Show information
> ipconfig /all           ... Show detailed information
> ipconfig /renew         ... renew all adapters
> ipconfig /renew EL*     ... renew any connection that has its
                           name starting with EL
> ipconfig /release *Con* ... release all matching connections,
                           eg. "Local Area Connection 1" or
                           "Local Area Connection 2"
> ipconfig /allcompartments ... Show information about all
                           compartments
> ipconfig /allcompartments /all ... Show detailed information about all
                           compartments

C:\Users\Pedro>
```



# 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.



```
Command Prompt
C:\>ping 192.168.1.10

Pinging 192.168.1.10 with 32 bytes of data:

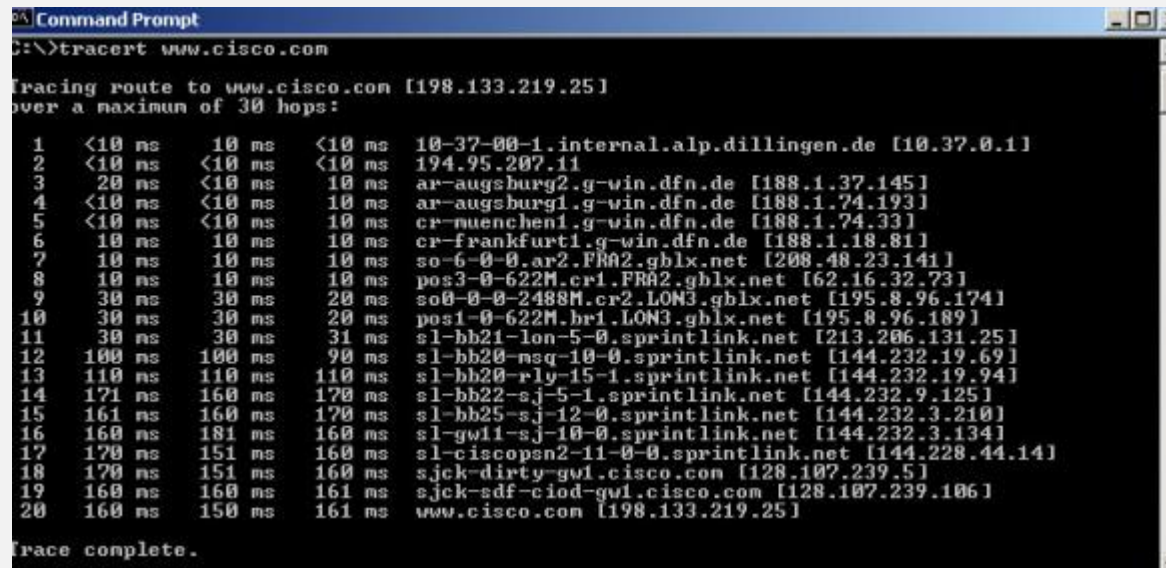
Reply from 192.168.1.10: bytes=32 time<10ms TTL=128
Reply from 192.168.1.10: bytes=32 time<10ms TTL=128
Reply from 192.168.1.10: bytes=32 time<10ms TTL=128
Reply from 192.168.1.10: bytes=32 time<10ms TTL=128

Ping statistics for 192.168.1.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

# 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.



```
Command Prompt
C:\>tracert www.cisco.com

Tracing route to www.cisco.com [198.133.219.25]
over a maximum of 30 hops:

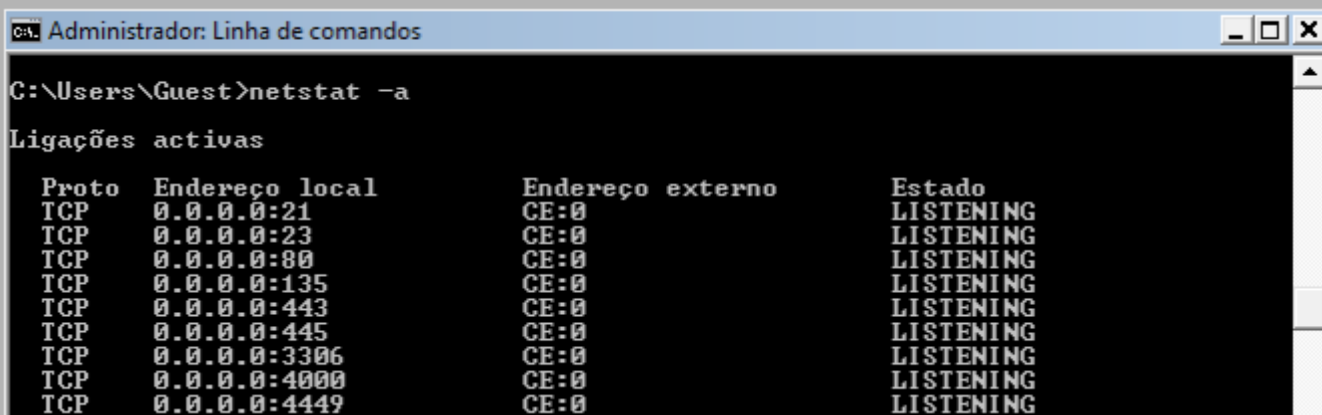
  0  <10 ns    10 ns    <10 ns    10-37-00-1.internal.alp.dillingen.de [10.37.0.1]
  1  <10 ns    <10 ns    <10 ns    194.95.207.11
  2  20 ns     <10 ns    10 ns     ar-augsburg2.g-win.dfn.de [188.1.37.145]
  3  <10 ns    <10 ns    10 ns     ar-augsburg1.g-win.dfn.de [188.1.74.193]
  4  <10 ns    <10 ns    10 ns     cr-muenchen1.g-win.dfn.de [188.1.74.33]
  5  <10 ns    <10 ns    10 ns     cr-frankfurt1.g-win.dfn.de [188.1.18.81]
  6  10 ns     10 ns     10 ns     so-6-0-0.ar2.FRA2.gblx.net [208.48.23.141]
  7  10 ns     10 ns     10 ns     pos3-0-622M.cr1.FRA2.gblx.net [62.16.32.73]
  8  30 ns     30 ns     20 ns     so0-0-0-2488M.cr2.LON3.gblx.net [195.8.96.174]
  9  30 ns     30 ns     20 ns     pos1-0-622M.br1.LON3.gblx.net [195.8.96.189]
 10  30 ns     30 ns     20 ns     sl-bb21-lon-5-0.sprintlink.net [213.206.131.25]
 11 100 ns    100 ns    90 ns     sl-bb20-nsg-10-0.sprintlink.net [144.232.19.69]
 12 110 ns    110 ns    110 ns    sl-bb20-rly-15-1.sprintlink.net [144.232.19.94]
 13 171 ns    160 ns    170 ns    sl-bb22-sj-5-1.sprintlink.net [144.232.9.125]
 14 161 ns    160 ns    170 ns    sl-bb25-sj-12-0.sprintlink.net [144.232.3.210]
 15 160 ns    181 ns    160 ns    sl-gw11-sj-10-0.sprintlink.net [144.232.3.134]
 16 170 ns    151 ns    160 ns    sl-ciscopsn2-11-0-0.sprintlink.net [144.228.44.14]
 17 170 ns    151 ns    160 ns    sjck-dirty-gw1.cisco.com [128.107.239.5]
 18 160 ns    160 ns    161 ns    sjck-sdf-ciod-gw1.cisco.com [128.107.239.106]
 19 160 ns    150 ns    161 ns    www.cisco.com [198.133.219.25]

Trace complete.
```

- 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.



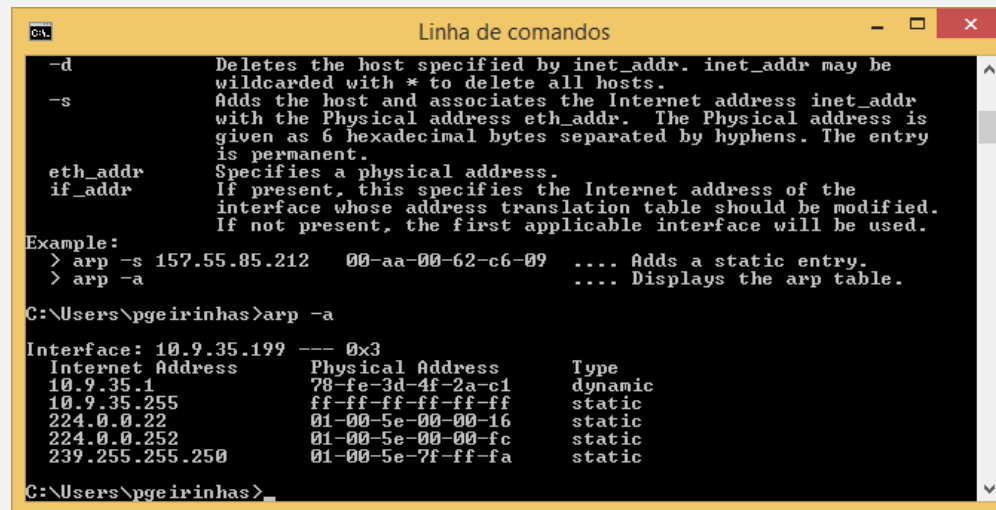
```
C:\Users\Guest>netstat -a
```

Ligações activas

Proto	Endereço local	Endereço externo	Estado
TCP	0.0.0.0:21	CE:0	LISTENING
TCP	0.0.0.0:23	CE:0	LISTENING
TCP	0.0.0.0:80	CE:0	LISTENING
TCP	0.0.0.0:135	CE:0	LISTENING
TCP	0.0.0.0:443	CE:0	LISTENING
TCP	0.0.0.0:445	CE:0	LISTENING
TCP	0.0.0.0:3306	CE:0	LISTENING
TCP	0.0.0.0:4000	CE:0	LISTENING
TCP	0.0.0.0:4449	CE:0	LISTENING

# 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`:



```
C:\>
-d      Deletes the host specified by inet_addr. inet_addr may be
        wildcarded with * to delete all hosts.
-s      Adds the host and associates the Internet address inet_addr
        with the Physical address eth_addr. The Physical address is
        given as 6 hexadecimal bytes separated by hyphens. The entry
        is permanent.
eth_addr Specifies a physical address.
if_addr  If present, this specifies the Internet address of the
        interface whose address translation table should be modified.
        If not present, the first applicable interface will be used.

Example:
> arp -s 157.55.85.212 00-aa-00-62-c6-09 .... Adds a static entry.
> arp -a .... Displays the arp table.

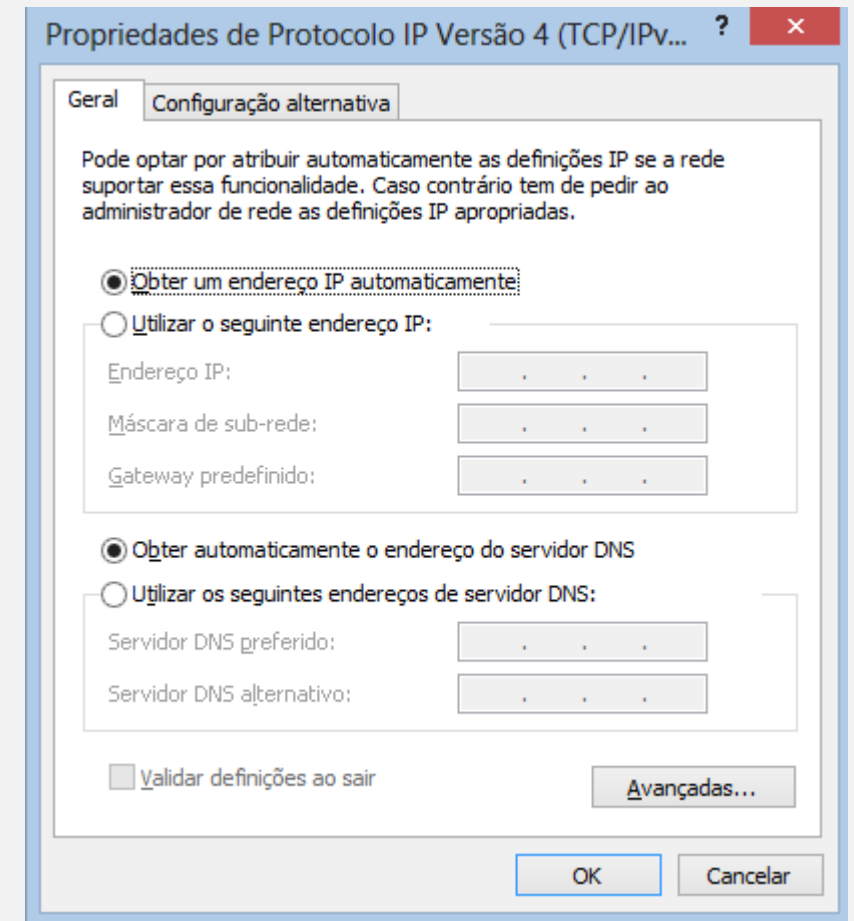
C:\Users\pgeirinhas>arp -a

Interface: 10.9.35.199 --- 0x3
Internet Address      Physical Address      Type
10.9.35.1             78-fe-3d-4f-2a-c1     dynamic
10.9.35.255           ff-ff-ff-ff-ff-ff     static
224.0.0.22            01-00-5e-00-00-16     static
224.0.0.252           01-00-5e-00-00-fc     static
239.255.255.250       01-00-5e-7f-ff-fa     static

C:\Users\pgeirinhas>
```

# 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.

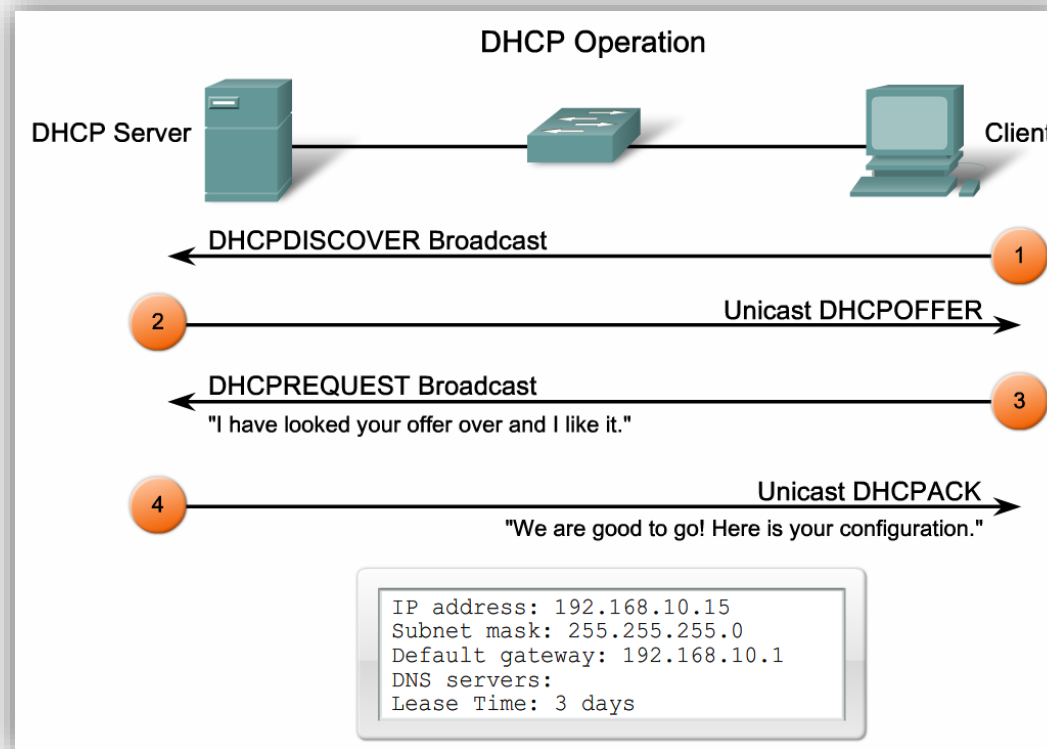


Licenciatura em Engenharia Informática  
Ramo de Redes e Administração de Sistemas

*Dynamic Host Configuration Protocol (DHCP)*  
*- Cisco*

# DHCP Configuration(Cisco)

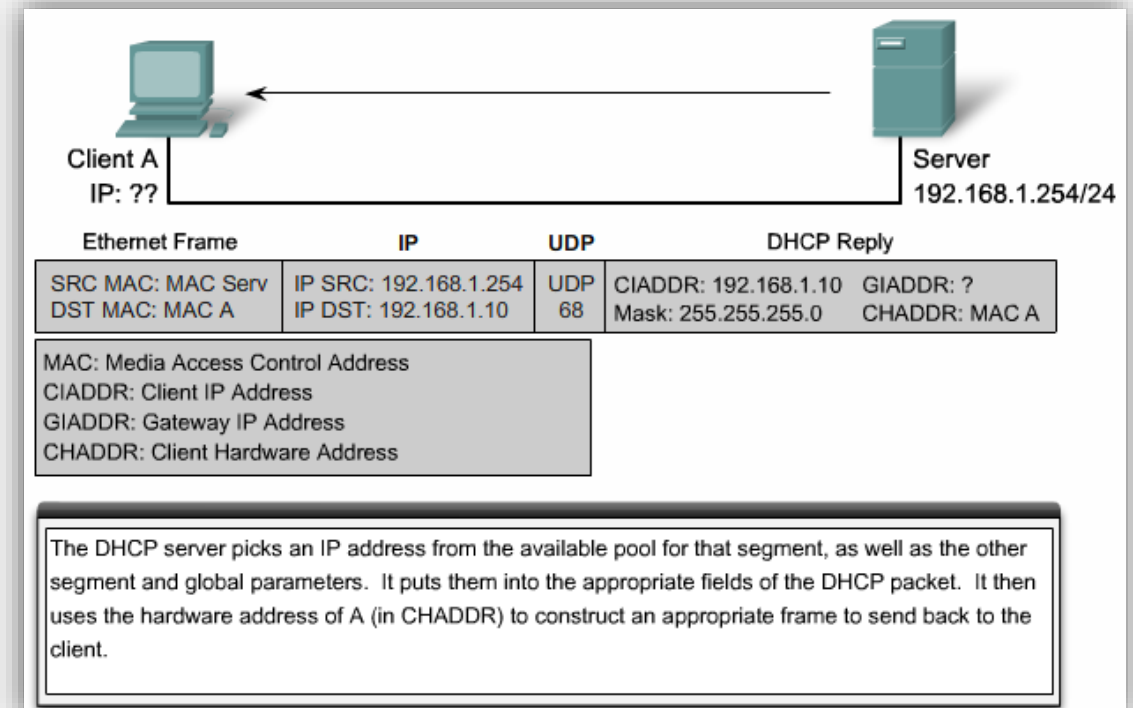
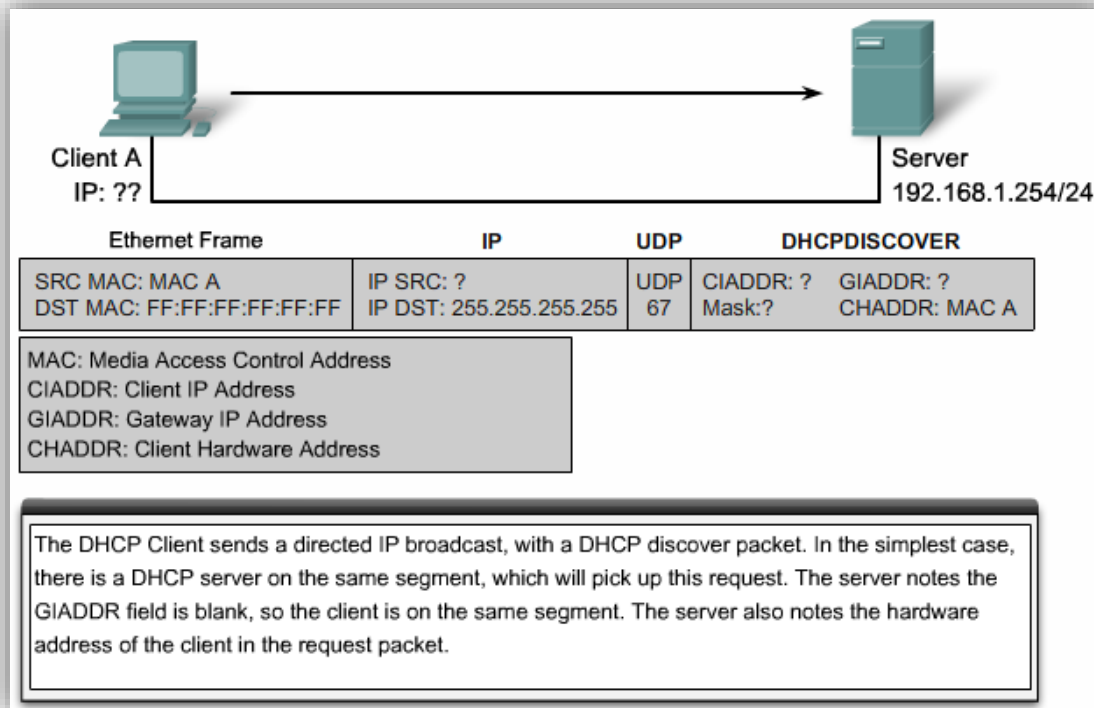
- In a cisco environment messages sent by the server are sent in unicast. The customers, and how could not fail to be in broadcast.





# 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)

## 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
```

# DHCP Configuration (Cisco)

- Give the pool a name

## 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 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	<code>network network-number [mask   /prefix-length]</code>
Define the default router or gateway	<code>default-router address [address2...address8]</code>

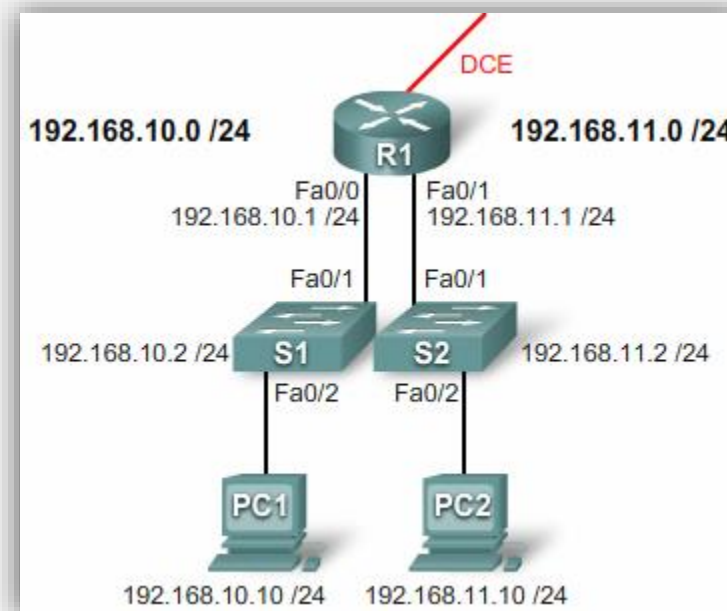
Optional Tasks	Command
Define a DNS server.	<code>dns-server address [address2...address8]</code>
Define the domain name	<code>domain-name domain</code>
Define the duration of the DHCP lease	<code>lease { days [hours] [minutes]   infinite }</code>
Define the NetBIOS WINS server	<code>netbios-name-server address [address2...address8]</code>

## 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
```

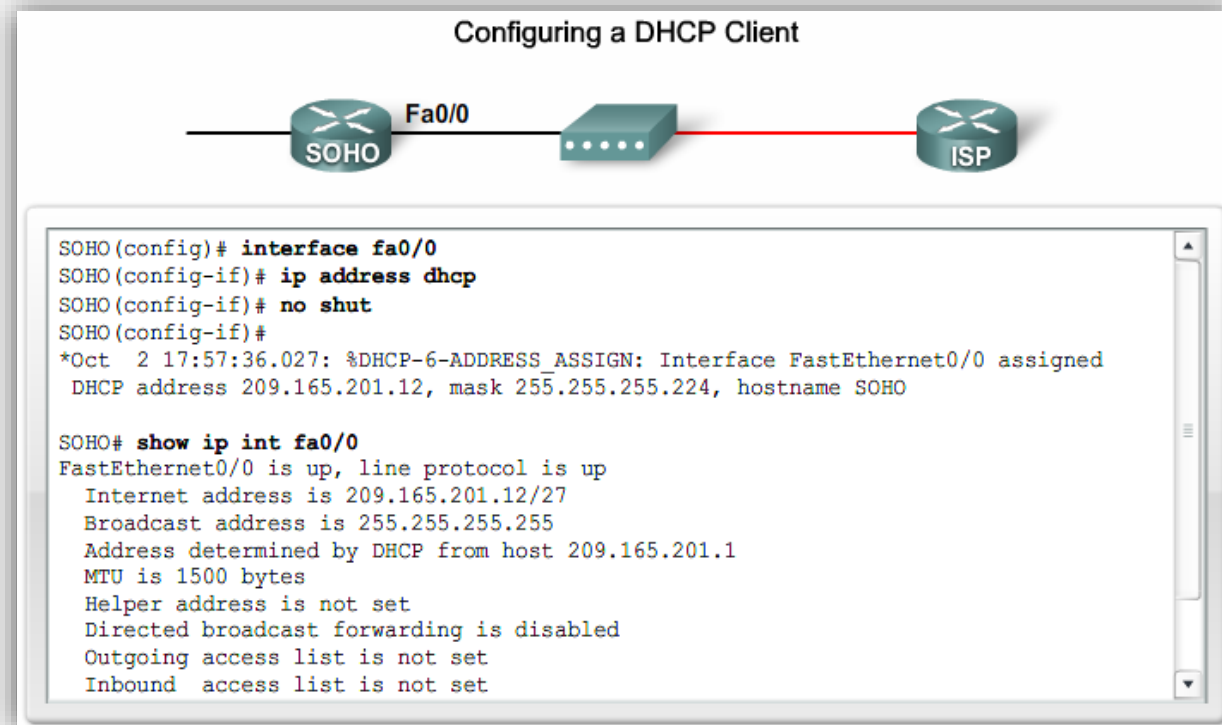
# DHCP Configuration (Cisco)

- 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 ...







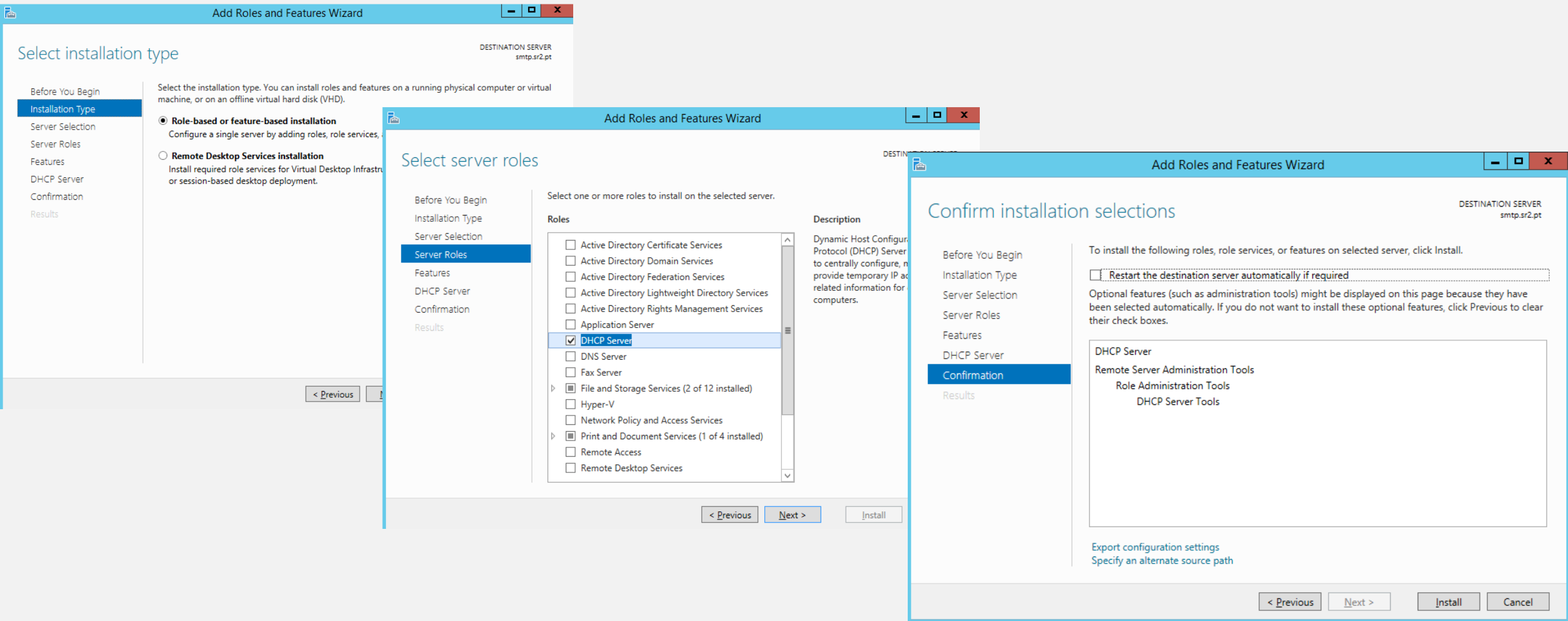
Licenciatura em Engenharia Informática  
Ramo de Redes e Administração de Sistemas

*Dynamic Host Configuration Protocol (DHCP)*  
*- Windows*

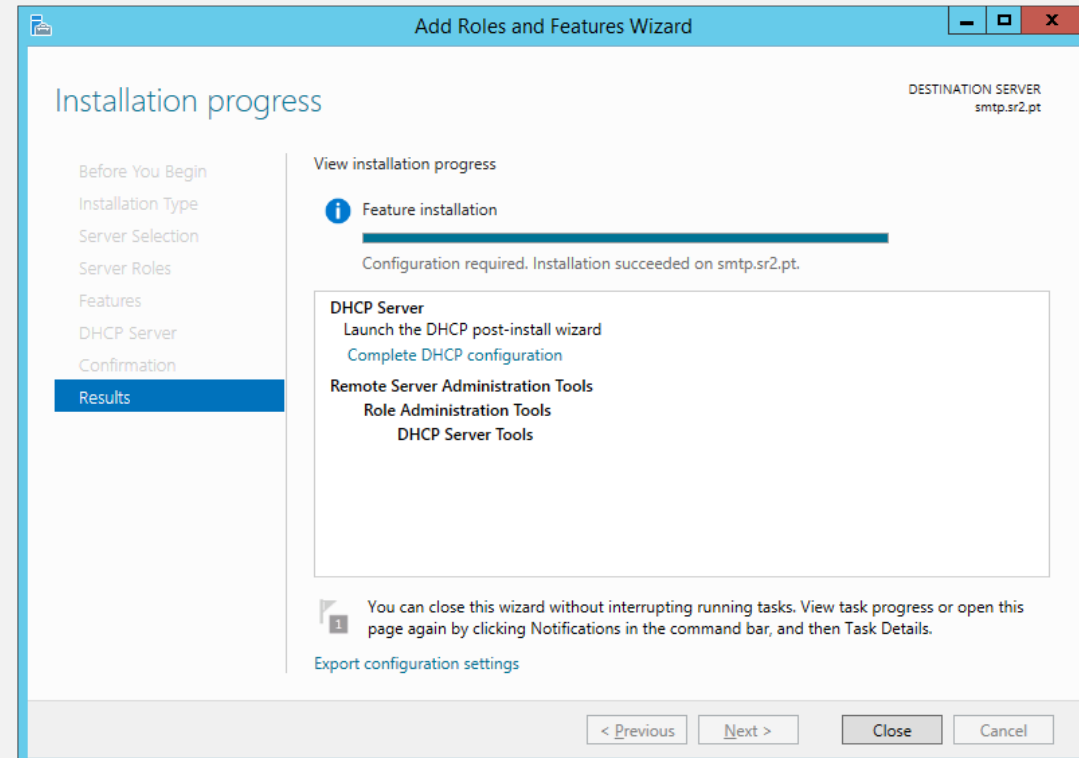
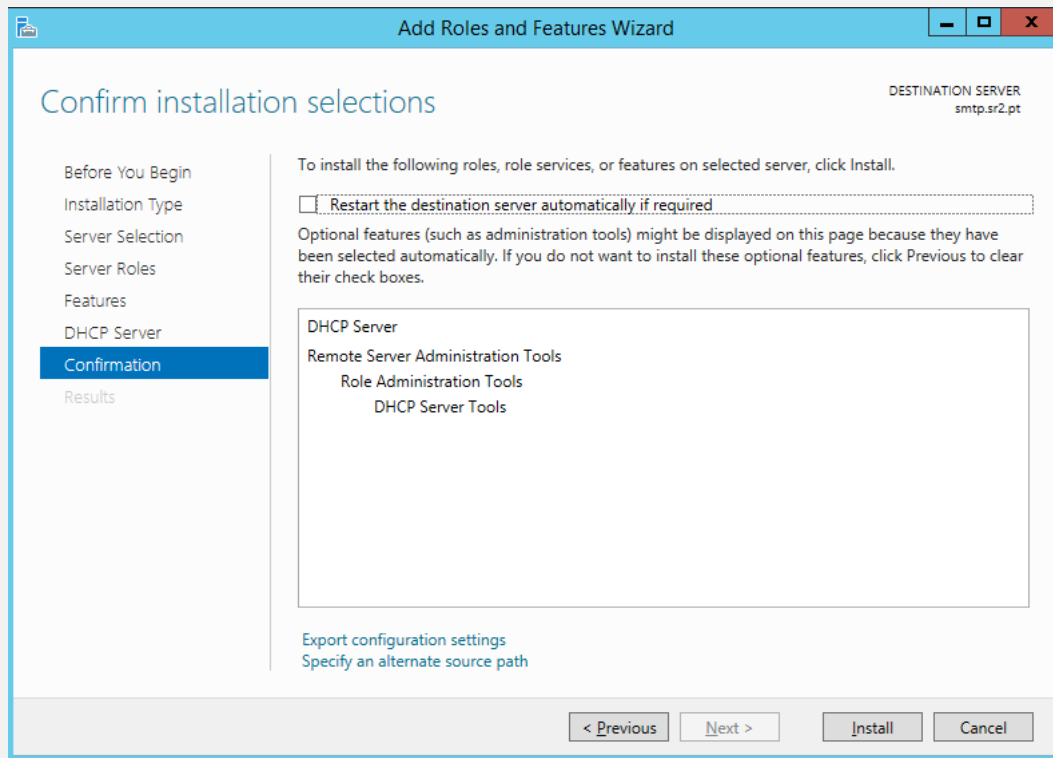
# DHCP - Service Installation

- 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.

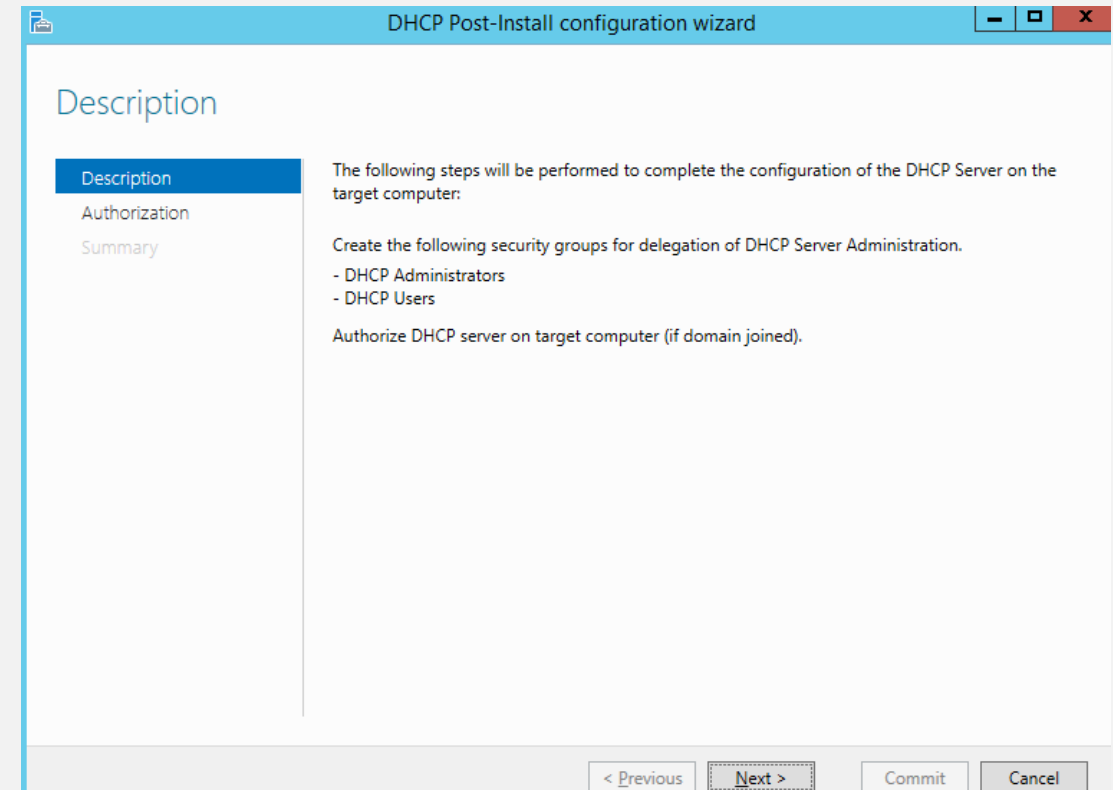
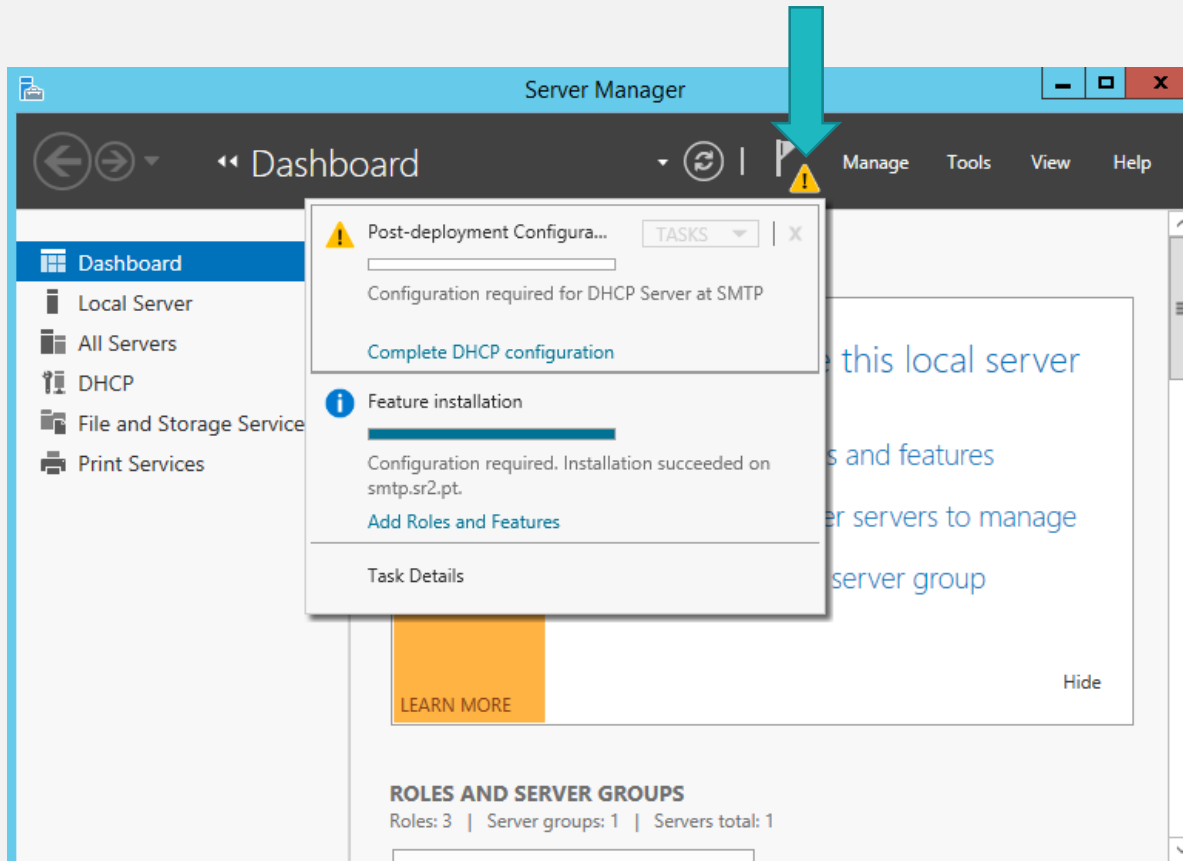
# DHCP - Service Installation



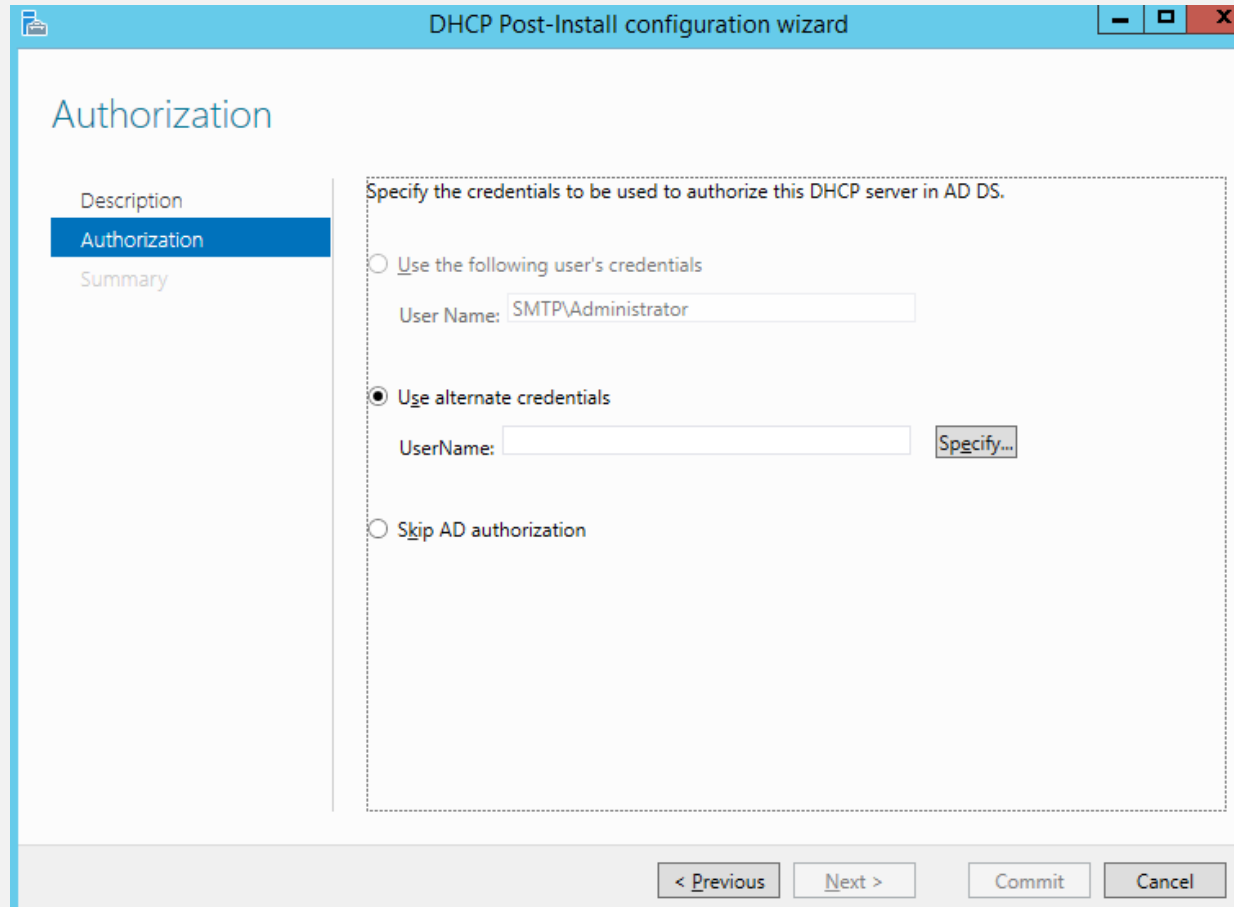
# DHCP - Service Installation



# DHCP - Service Installation



# DHCP - Service Installation



The screenshot shows the 'DHCP Post-Install configuration wizard' window. The title bar is blue with standard Windows window controls. The main content area is white. On the left, there is a vertical sidebar with three items: 'Description', 'Authorization' (highlighted in blue), and 'Summary'. The main area is titled 'Authorization' and contains a dashed border box with the text 'Specify the credentials to be used to authorize this DHCP server in AD DS.' Inside this box, there are three radio button options. The first option is 'Use the following user's credentials', with a 'User Name' field containing 'SMTP\Administrator'. The second option is 'Use alternate credentials', which is selected with a black dot; it has a 'UserName' field and a 'Specify...' button. The third option is 'Skip AD authorization'. At the bottom of the window, outside the dashed box, are four buttons: '< Previous', 'Next >', 'Commit', and 'Cancel'.

DHCP Post-Install configuration wizard

## Authorization

Description  
**Authorization**  
Summary

Specify the credentials to be used to authorize this DHCP server in AD DS.

☐ Use the following user's credentials

User Name: SMTP\Administrator

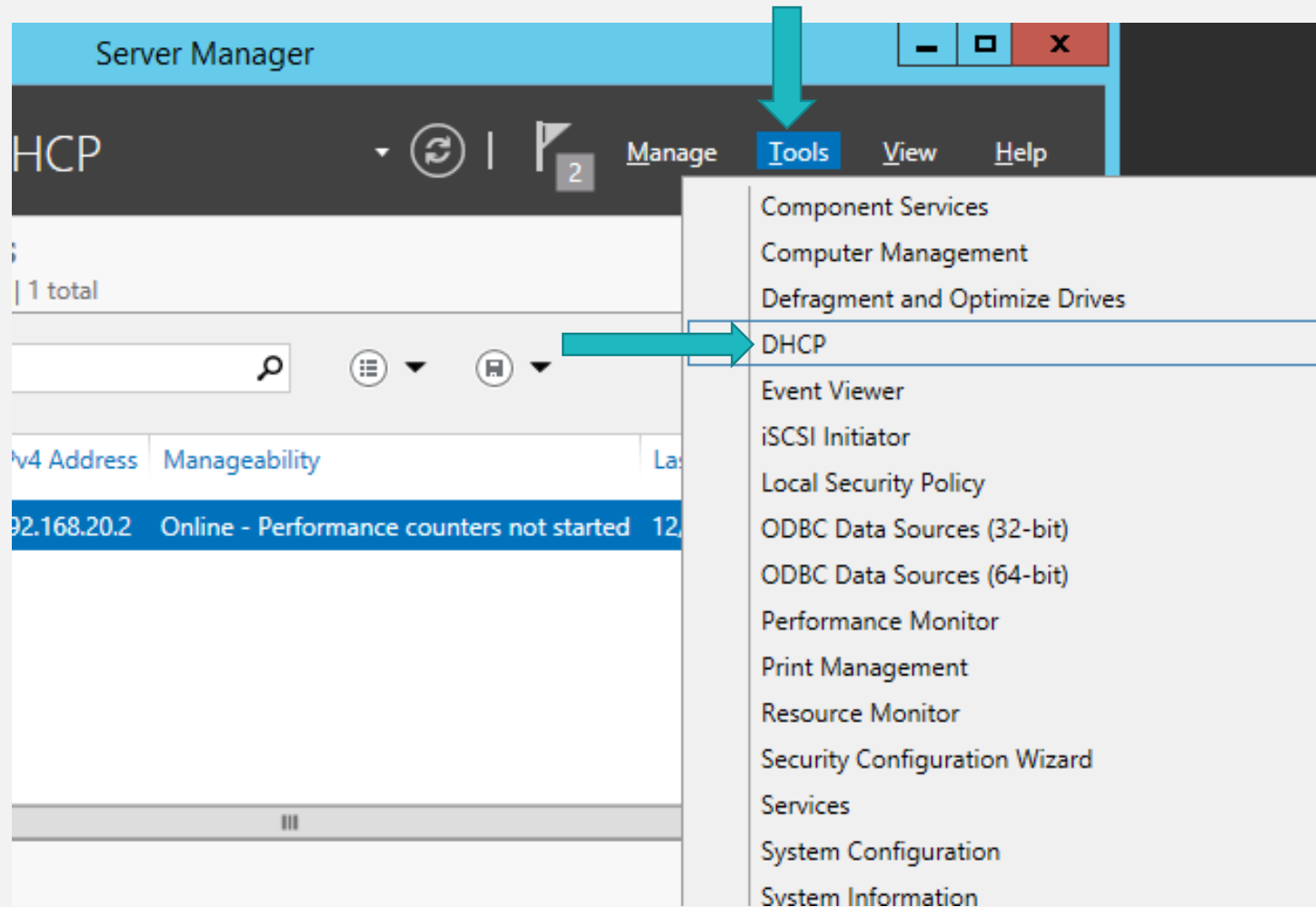
☒ Use alternate credentials

UserName:  Specify...

☐ Skip AD authorization

< Previous   Next >   Commit   Cancel

# 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

The screenshot shows the 'Specify IPv4 DNS Server Settings' window. The left sidebar lists the steps: Before You Begin, Server Roles, DHCP Server, Network Connection Bindings, IPv4 DNS Settings (selected), IPv4 WINS Settings, DHCP Scopes, DHCPv6 Stateless Mode, IPv6 DNS Settings, and DHCP Server Authorization. The main area contains instructions and input fields for DNS settings. The 'Parent Domain' is set to 'mcresolution.local'. The 'Preferred DNS Server IPv4 Address' is '10.0.0.1', which is marked as 'Valid'. There is an empty field for the 'Alternate DNS Server IPv4 Address'. A link for 'More about DNS server settings' is at the bottom. Navigation buttons at the bottom include '< Previous', 'Next >', 'Install', and 'Cancel'.

**Add Roles Wizard**

**Specify IPv4 DNS Server Settings**

Before You Begin  
Server Roles  
DHCP Server  
Network Connection Bindings  
**IPv4 DNS Settings**  
IPv4 WINS Settings  
DHCP Scopes  
DHCPv6 Stateless Mode  
IPv6 DNS Settings  
DHCP Server Authorization  
Confirmation  
Progress  
Results

When clients obtain an IP address from the DHCP server, they can be given DHCP options such as the IP addresses of DNS servers and the parent domain name. The settings you provide here will be applied to clients using IPv4.

Specify the name of the parent domain that clients will use for name resolution. This domain will be used for all scopes you create on this DHCP server.

Parent Domain:

Specify the IP addresses of the DNS servers that clients will use for name resolution. These DNS servers will be used for all scopes you create on this DHCP server.

Preferred DNS Server IPv4 Address:

Valid

Alternate DNS Server IPv4 Address:

[More about DNS server settings](#)

< Previous   Next >   Install   Cancel

The screenshot shows the 'Specify IPv4 WINS Server Settings' window. The left sidebar is identical to the previous window, with 'IPv4 WINS Settings' selected. The main area contains instructions and radio buttons for WINS settings. The first option, 'WINS is not required for applications on this network', is selected. The second option, 'WINS is required for applications on this network', is unselected. Below the second option, there are input fields for 'Preferred WINS Server IP Address' and 'Alternate WINS Server IP Address', both of which are empty. A link for 'More about WINS server settings' is at the bottom. Navigation buttons at the bottom include '< Previous', 'Next >', 'Install', and 'Cancel'.

**Add Roles Wizard**

**Specify IPv4 WINS Server Settings**

Before You Begin  
Server Roles  
DHCP Server  
Network Connection Bindings  
IPv4 DNS Settings  
**IPv4 WINS Settings**  
DHCP Scopes  
DHCPv6 Stateless Mode  
IPv6 DNS Settings  
DHCP Server Authorization  
Confirmation  
Progress  
Results

When clients obtain an IP address from the DHCP server, they can be given DHCP options such as the IP addresses of WINS servers. The settings you provide here will be applied to clients using IPv4.

☒ WINS is not required for applications on this network

☐ WINS is required for applications on this network

Specify the IP addresses of the WINS servers that clients will use for name resolution. These WINS servers will be used for all scopes you create on this DHCP server.

Preferred WINS Server IP Address:

Alternate WINS Server IP Address:

[More about WINS server settings](#)

< Previous   Next >   Install   Cancel



# 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*

The image displays two screenshots of the 'New Scope Wizard' in the Windows DHCP console. The top screenshot shows the 'IP Address Range' step, where the user defines the scope address range by identifying a set of consecutive IP addresses. It includes configuration settings for the DHCP Server, such as the Start IP address (192.168.1.1) and End IP address (192.168.1.254). The bottom screenshot shows the 'Add Exclusions and Delay' step, where the user can add exclusions (addresses or ranges not distributed by the server) and set a subnet delay in milliseconds. It includes fields for Start IP address, End IP address, and a list of excluded address ranges (e.g., 192.168.1.1 to 192.168.1.10).

**New Scope Wizard**

**IP Address Range**  
You define the scope address range by identifying a set of consecutive IP addresses.

Configuration settings for DHCP Server  
Enter the range of addresses that the scope distributes.

Start IP address: 192.168.1.1  
End IP address: 192.168.1.254

Configuration settings that propagate to DHCP Client

Length: 24  
Subnet mask: 255.255.255.0

**New Scope Wizard**

**Add Exclusions and Delay**  
Exclusions are addresses or a range of addresses that are not distributed by the server. A delay is the time duration by which the server will delay the transmission of a DHCP OFFER message.

Type the IP address range that you want to exclude. If you want to exclude a single address, type an address in Start IP address only.

Start IP address: End IP address: Add  
Excluded address range: 192.168.1.1 to 192.168.1.10 Remove  
Subnet delay in milliseconds: 0

< Back Next > Cancel

# DHCP - Service Installation

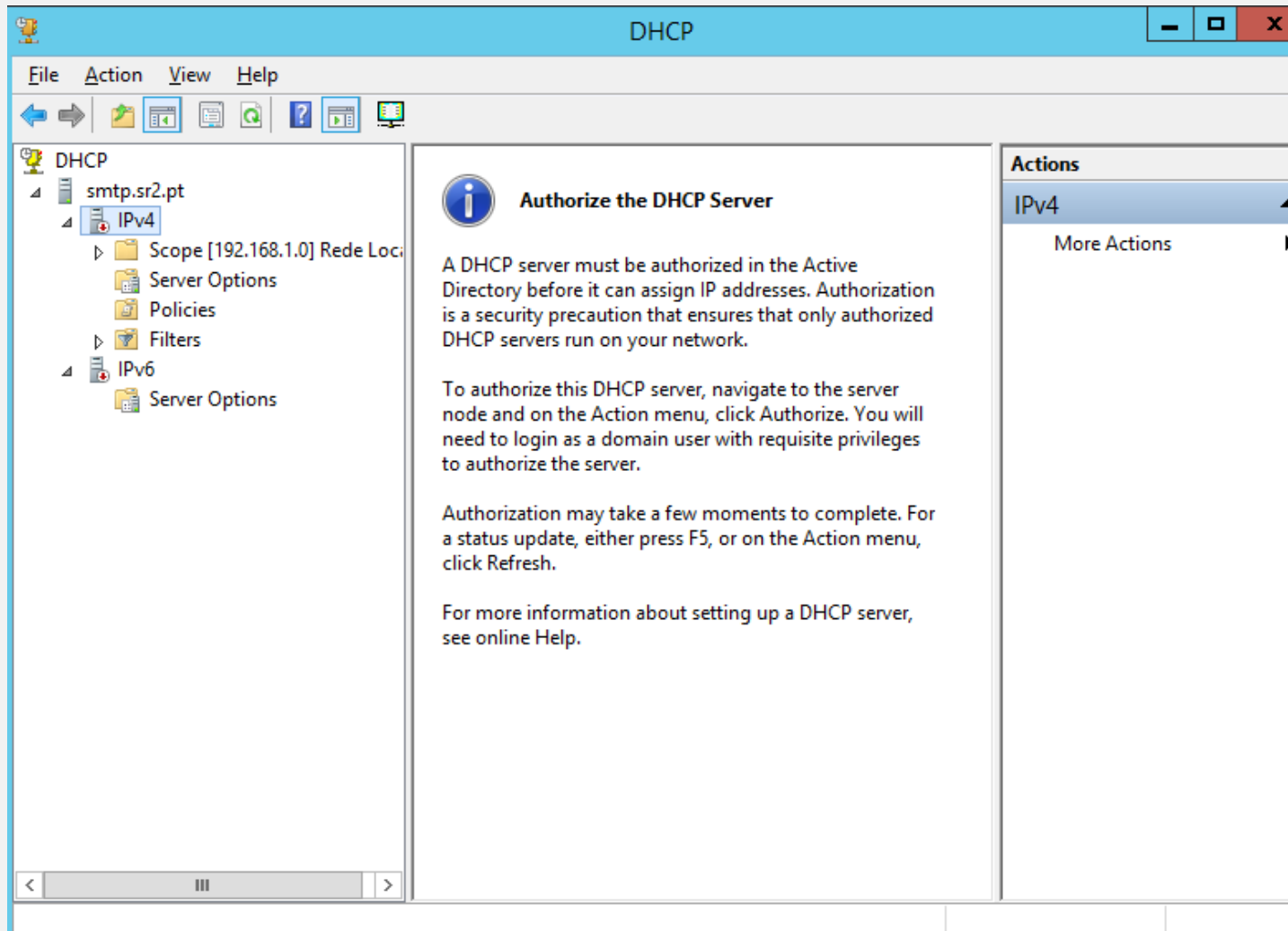
- Indicate:
  - **Scope Name:** Name
  - **Starting IP Address and Ending IP Address:** Start and End Address
  - **Subnet Mask:** Subnet mask used
  - **Default Gateway:** default router address
  - **Subnet Type:** Choose between Wired (6 days) or Wireless (8 days) to set the length of time the IP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

The screenshot displays the 'Add or Edit DHCP Scopes' wizard. The 'Add Scope' dialog box is the primary focus, containing the following configuration details:

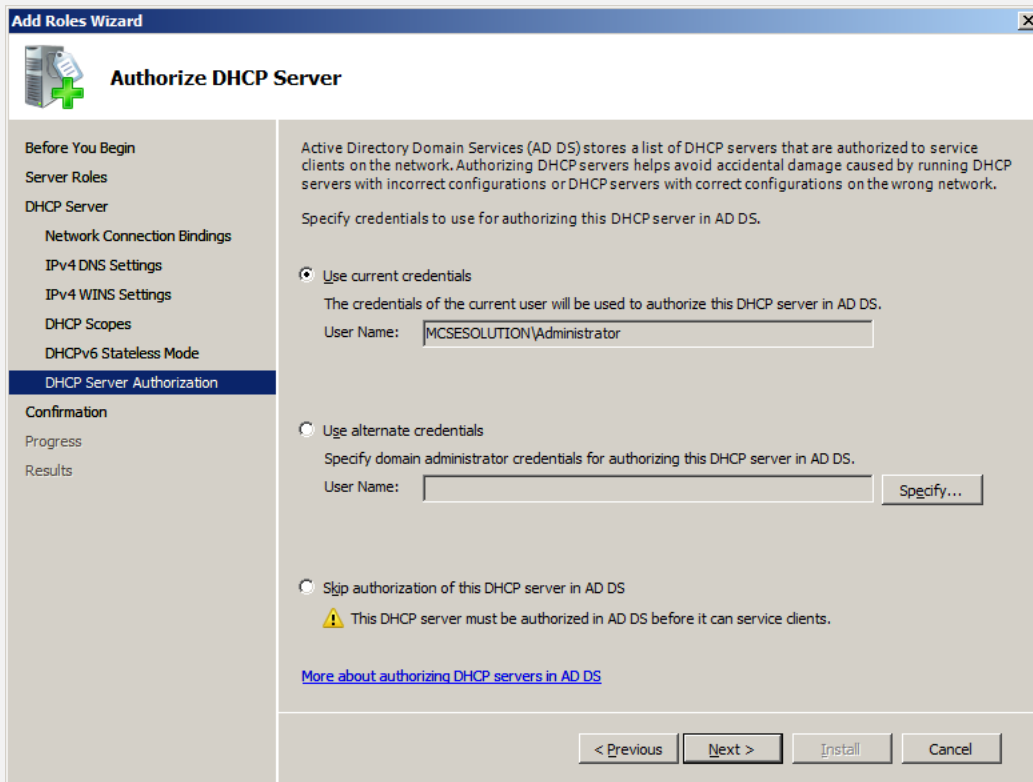
Field	Value
Scope Name	WBC-Local
Starting IP Address	192.168.1.50
Ending IP Address	192.168.1.100
Subnet Mask	255.255.255.0
Default Gateway (optional)	192.168.1.1
Subnet Type	Wired (lease duration will be 6 days)

The 'Activate this scope' checkbox is checked. The background shows the 'Add Rules Wizard' with 'DHCP Scopes' selected in the left pane.

# DHCP - Service Installation



# DHCP - Service Installation



**Add Roles Wizard**

**Authorize DHCP Server**

**Before You Begin**

**Server Roles**

DHCP Server

Network Connection Bindings

IPv4 DNS Settings

IPv4 WINS Settings

DHCP Scopes

DHCPv6 Stateless Mode

**DHCP Server Authorization**

**Confirmation**

Progress

Results

Active Directory Domain Services (AD DS) stores a list of DHCP servers that are authorized to service clients on the network. Authorizing DHCP servers helps avoid accidental damage caused by running DHCP servers with incorrect configurations or DHCP servers with correct configurations on the wrong network.

Specify credentials to use for authorizing this DHCP server in AD DS.

☒ Use current credentials

The credentials of the current user will be used to authorize this DHCP server in AD DS.


User Name:

☐ Use alternate credentials

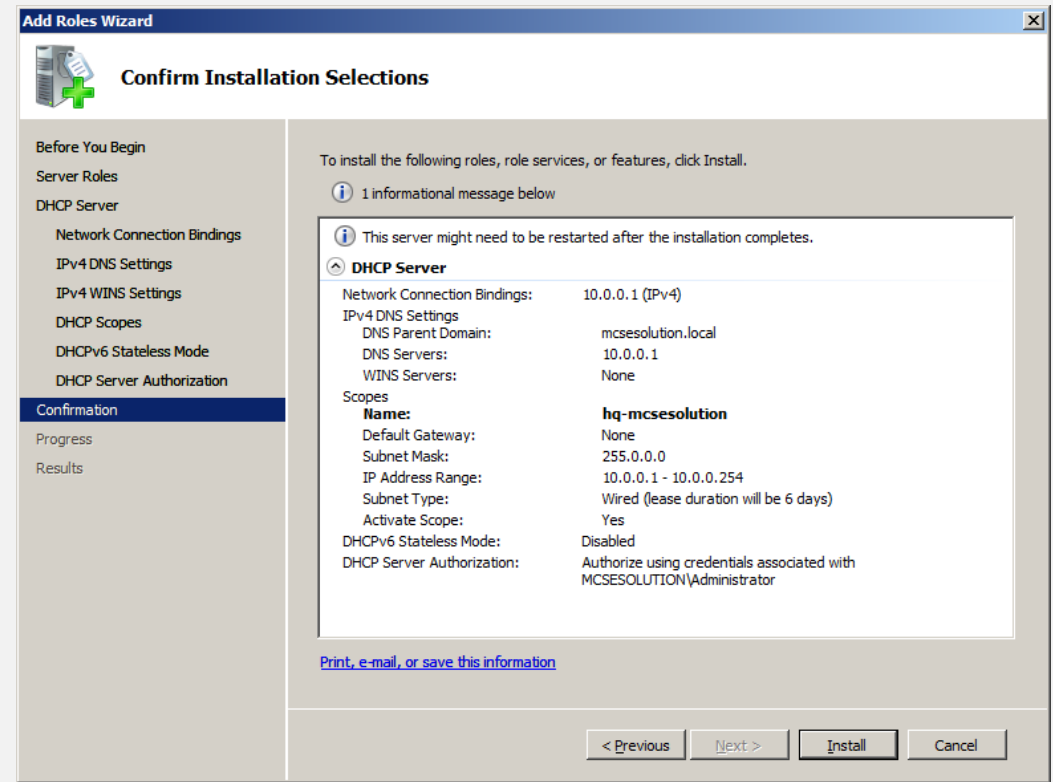
Specify domain administrator credentials for authorizing this DHCP server in AD DS.

User Name:

☐ Skip authorization of this DHCP server in AD DS

 This DHCP server must be authorized in AD DS before it can service clients.

[More about authorizing DHCP servers in AD DS](#)



**Add Roles Wizard**

**Confirm Installation Selections**

**Before You Begin**

**Server Roles**

DHCP Server

Network Connection Bindings

IPv4 DNS Settings

IPv4 WINS Settings

DHCP Scopes

DHCPv6 Stateless Mode


**DHCP Server Authorization**


**Confirmation**

Progress

Results

To install the following roles, role services, or features, click Install.

 1 informational message below

 This server might need to be restarted after the installation completes.

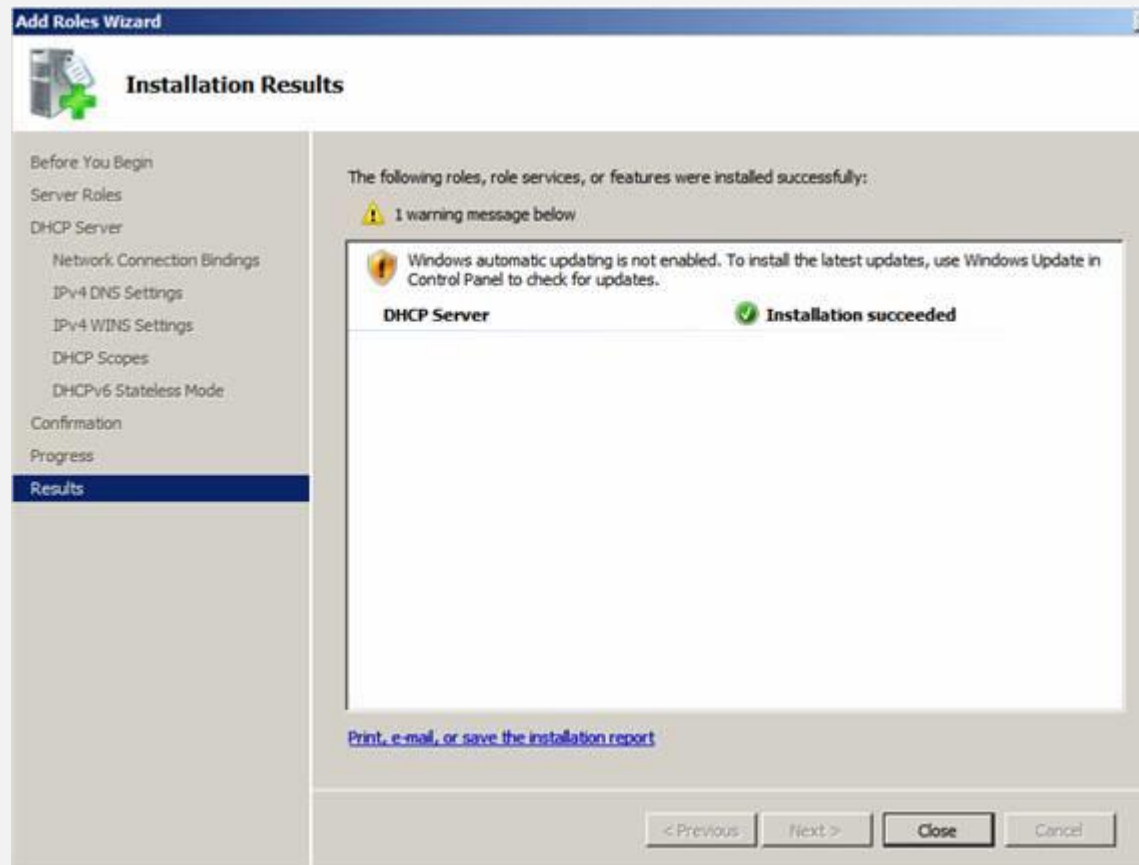
**DHCP Server**

Network Connection Bindings:	10.0.0.1 (IPv4)
IPv4 DNS Settings	
DNS Parent Domain:	mcsesolution.local
DNS Servers:	10.0.0.1
WINS Servers:	None
Scopes	
<b>Name:</b>	<b>hq-mcsesolution</b>
Default Gateway:	None
Subnet Mask:	255.0.0.0
IP Address Range:	10.0.0.1 - 10.0.0.254
Subnet Type:	Wired (lease duration will be 6 days)
Activate Scope:	Yes
DHCPv6 Stateless Mode:	Disabled
DHCP Server Authorization:	Authorize using credentials associated with MCSESOLUTION\Administrator

[Print, e-mail, or save this information](#)

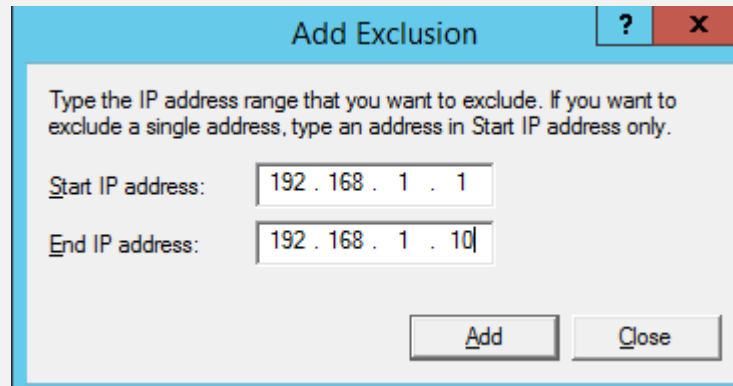
# DHCP - Service Installation

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



# DHCP - Add reservations

- A range of IPs
- A specific IP



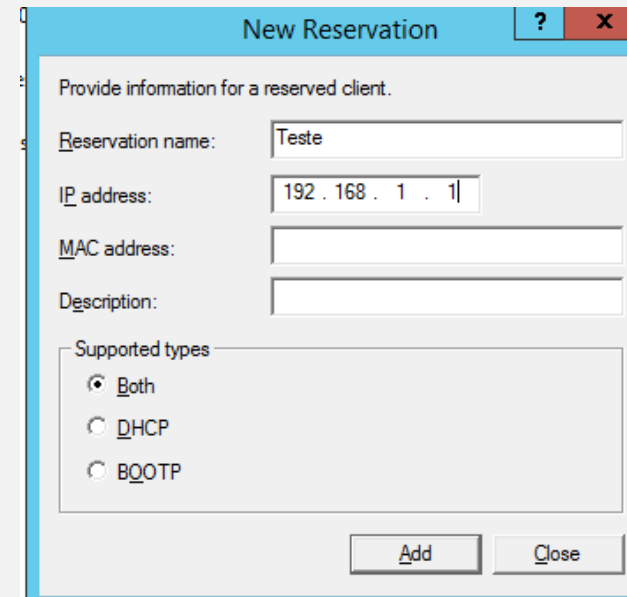
**Add Exclusion** ? x

Type the IP address range that you want to exclude. If you want to exclude a single address, type an address in Start IP address only.

Start IP address: 192 . 168 . 1 . 1

End IP address: 192 . 168 . 1 . 10

Add Close



**New Reservation** ? x

Provide information for a reserved client.

Reservation name: Teste

IP address: 192 . 168 . 1 . 1

MAC address:

Description:

Supported types

☒ Both

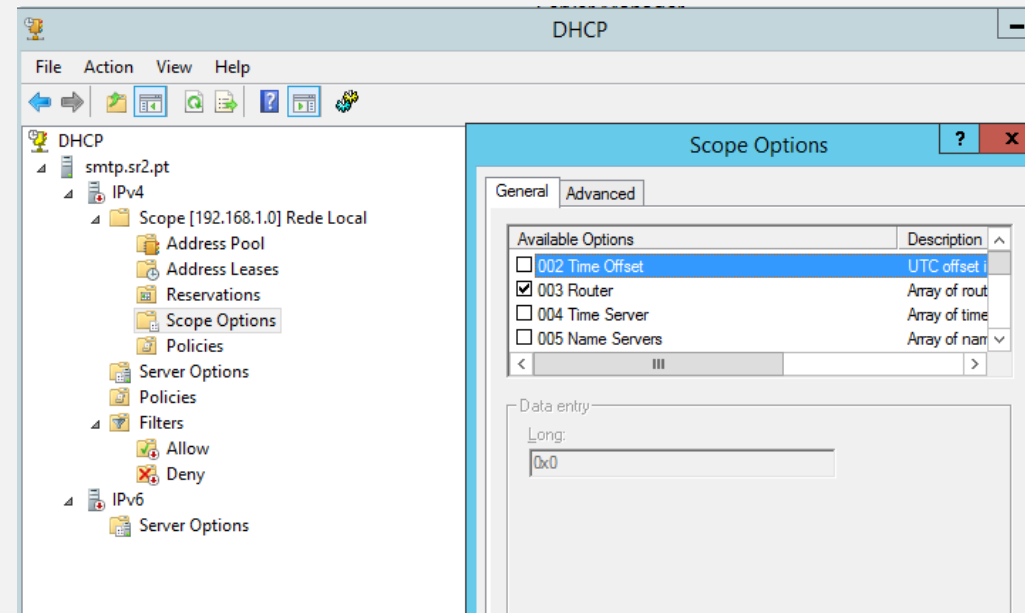
☐ DHCP

☐ BOOTP

Add Close

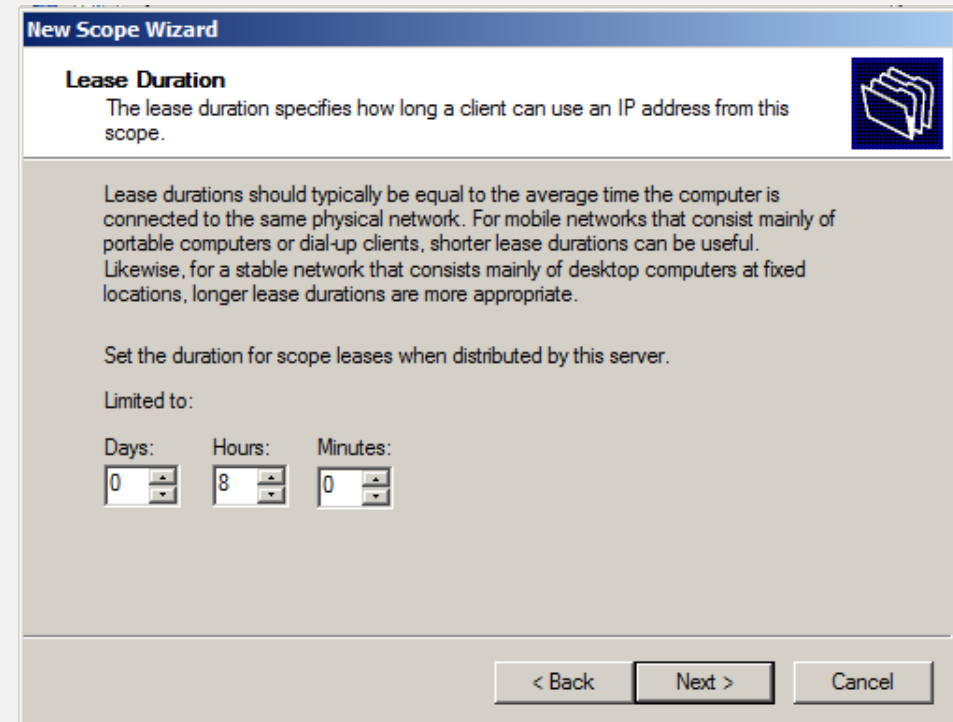
# DHCP – Server Options

- 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.



The screenshot shows the 'New Scope Wizard' window, specifically the 'Lease Duration' step. The window has a title bar 'New Scope Wizard' and a sub-header 'Lease Duration'. Below the sub-header is a description: 'The lease duration specifies how long a client can use an IP address from this scope.' To the right of this text is a folder icon. The main content area contains a paragraph explaining that lease durations should typically be equal to the average time the computer is connected to the same physical network. It also mentions that for mobile networks, shorter lease durations can be useful, and for stable networks, longer lease durations are more appropriate. Below this text is a label 'Set the duration for scope leases when distributed by this server.' followed by 'Limited to:'. There are three spin boxes for 'Days', 'Hours', and 'Minutes'. The 'Days' box is set to 0, the 'Hours' box is set to 8, and the 'Minutes' box is set to 0. At the bottom of the window are three buttons: '< Back', 'Next >', and 'Cancel'.

**New Scope Wizard**

**Lease Duration**

The lease duration specifies how long a client can use an IP address from this scope.

Lease durations should typically be equal to the average time the computer is connected to the same physical network. For mobile networks that consist mainly of portable computers or dial-up clients, shorter lease durations can be useful. Likewise, for a stable network that consists mainly of desktop computers at fixed locations, longer lease durations are more appropriate.

Set the duration for scope leases when distributed by this server.

Limited to:

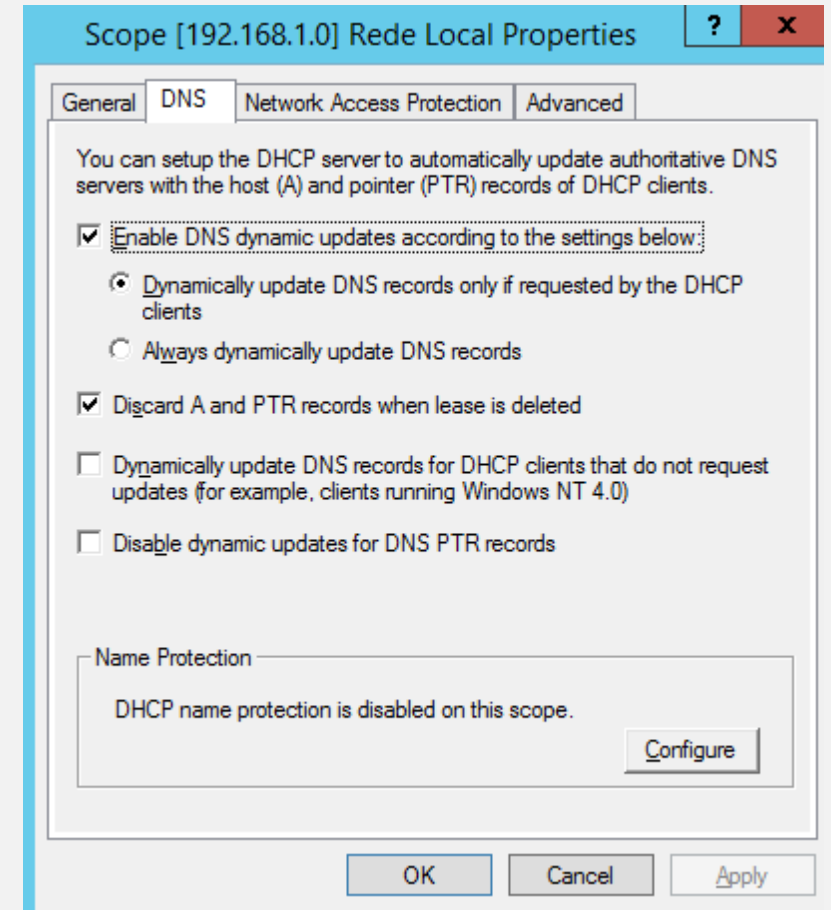
Days: 0 Hours: 8 Minutes: 0

< Back Next > Cancel



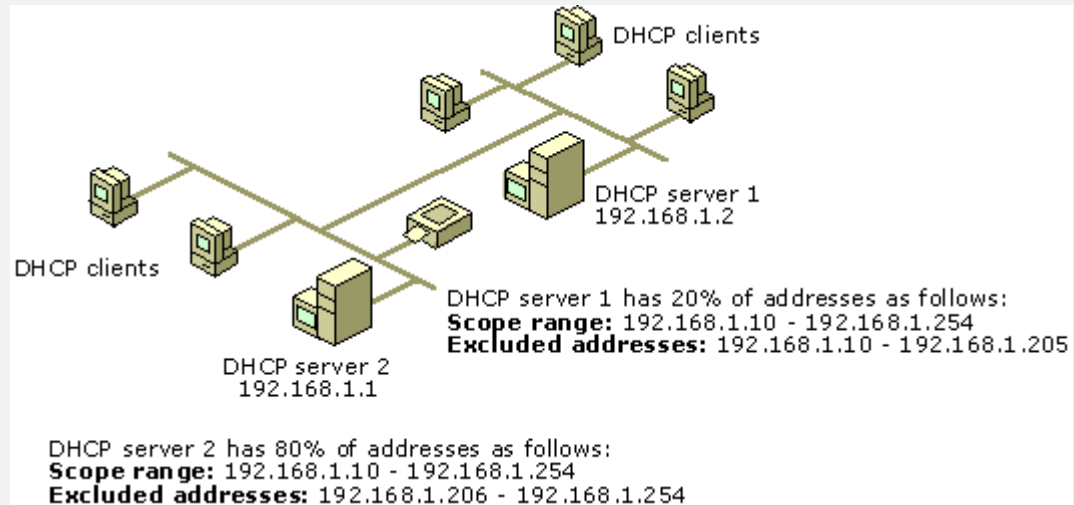
# DHCP - DNS

- In 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

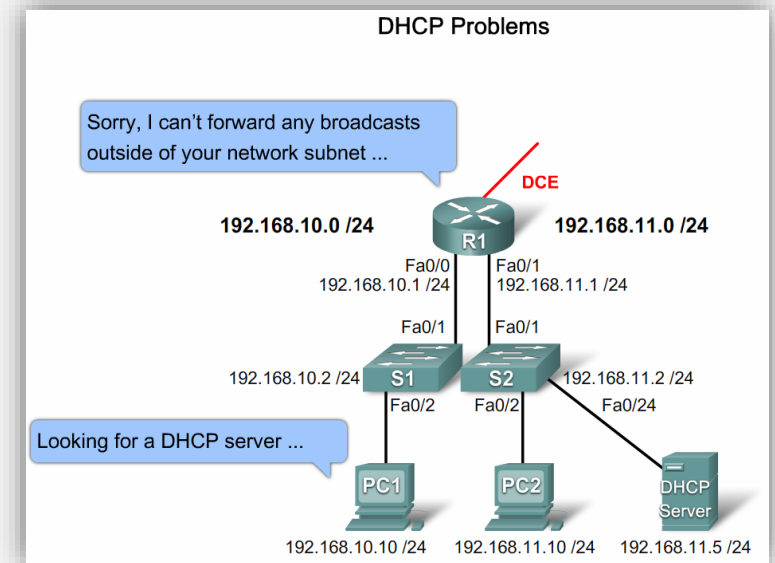
- **Multiple Device Types:** A network includes many different clients such as printers, IP phones, and desktops. Administrators can sort these devices using different IP address ranges. This allows routing and quality of service (QoS) policies based on the range of the IP address to control access or 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.

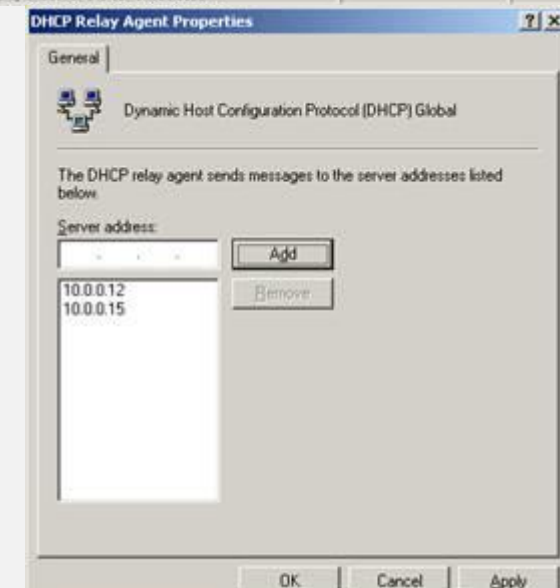
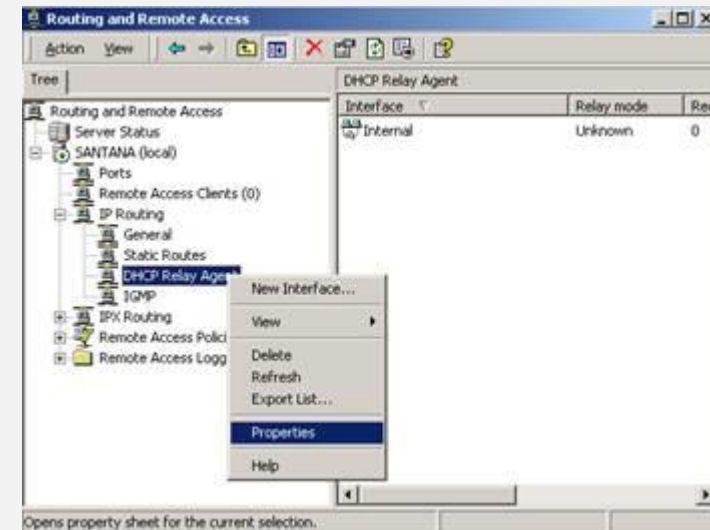
# DHCP Relay

- 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 can either forward them to the DHCP server, that is, it is an intermediary between the DHCP clients and the DHCP server.

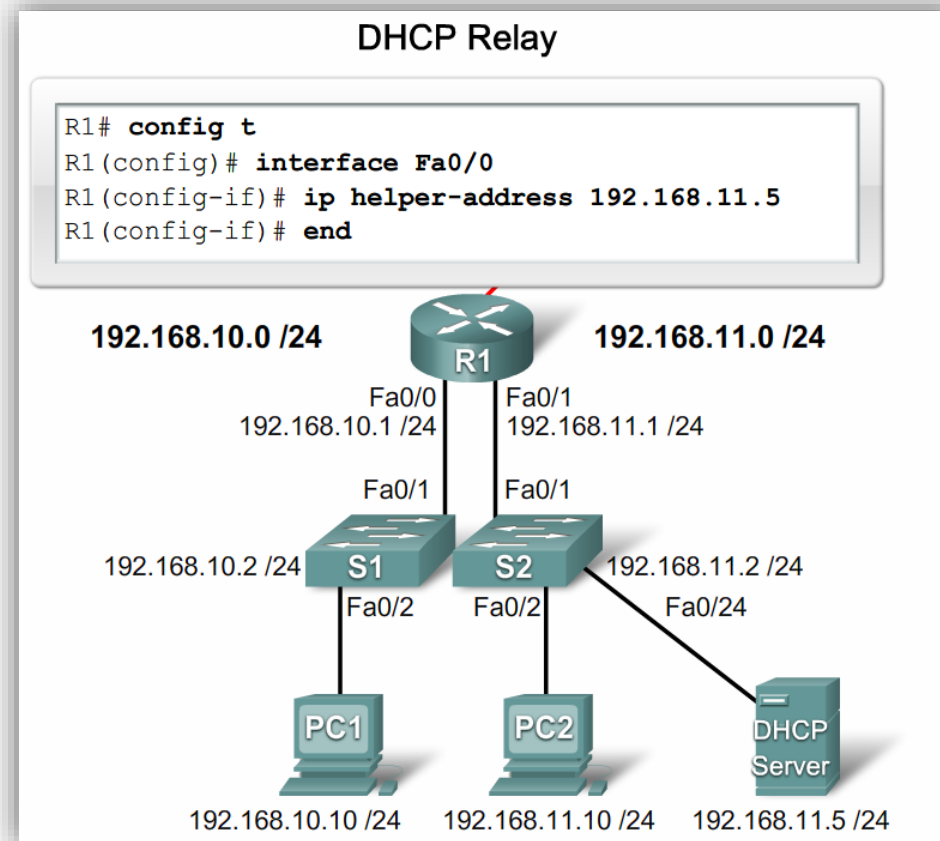


# DHCP Relay - windows

- 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://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>