



PMR3412 - Redes Industriais - 2023

Aula 03 - Reportando Erros e Resolução de Endereços (MAC e IP)

Prof. Dr. Newton Maruyama

24 de Agosto de 2023

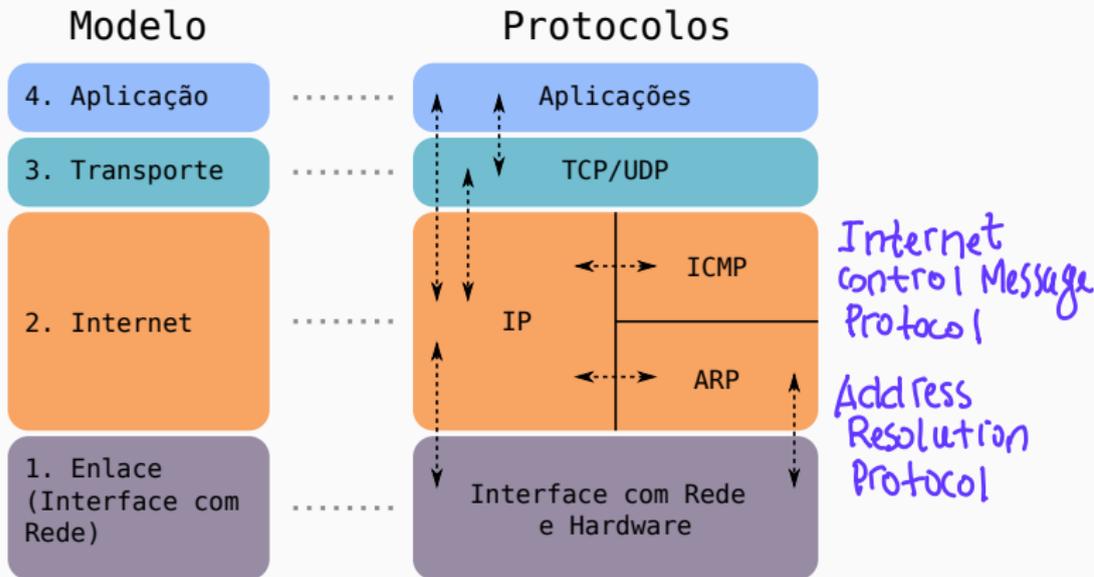
PMR-EPUSP

Os slides que serão utilizados nesse ano são baseados no curso desenvolvido para os anos 2020, 2021 e 2022. Participaram da concepção do curso e desenvolvimento do material os seguintes professores:

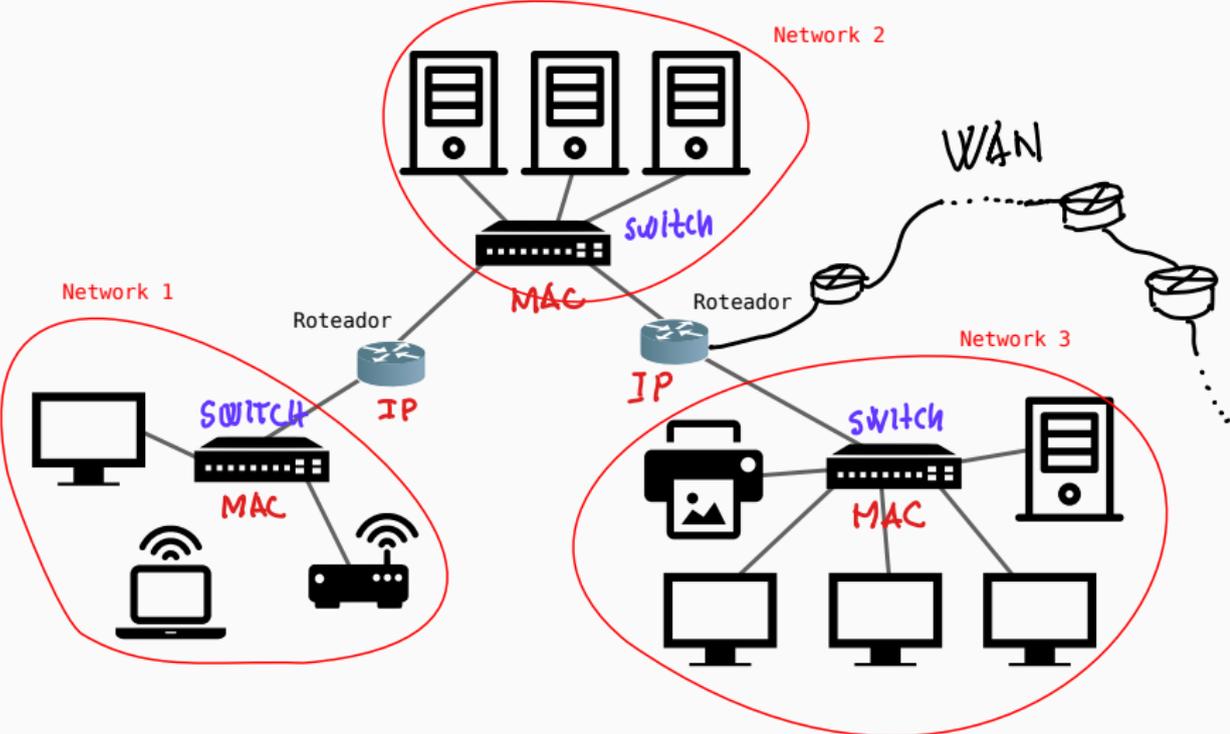
- ▶ Prof. Dr. André Kubagawa Sato
- ▶ Prof. Dr. Marcos de Sales Guerra Tsuzuki
- ▶ Prof. Dr. Edson Kenji Ueda
- ▶ Prof. Dr. Agesinaldo Matos Silva Junior
- ▶ Prof. Dr. André César Martins Cavalheiro

1. Revisão
2. Reportando Erros - Internet Control Message Protocol (ICMP)
3. Resolução de Endereços
4. ARP - Resolução de Endereços de Camada 1
5. NAT
6. DHCP
7. Referências

Revisão



Revisão - Redes e a internet

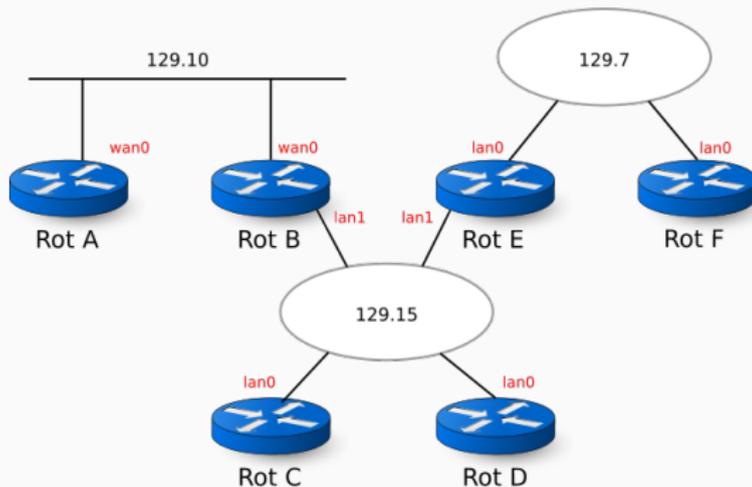


como descobrir o ip do seu computador ?

- windows: ipconfig
- linux: ifconfig

como descobrir os ips ativos da sua rede ?

nmap < CIDR ADDRESS >



Rot D

Destino	Roteador	Interface
129.7.0.0	E	lan0
129.15.0.0	D	lan0
129.10.0.0	B	lan0
default	B	lan0
127.0.0.1	loopback	loop

Rot F

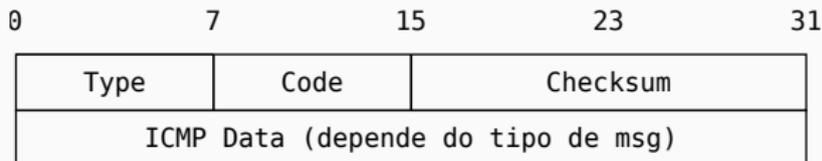
Destino	Roteador	Interface
129.7.0.0	F	lan0
default	E	lan0
127.0.0.1	loopback	lo

Reportando Erros - Internet Control Message Protocol (ICMP)

- ▶ O formato do datagrama IP é adequado para transmitir dados de camadas superiores, mas não tem um formato padrão para reportar erros.
- ▶ O protocolo ICMP foi criado para este propósito ao definir um formato padrão de mensagem de erro.
- ▶ Uma mensagem ICMP é encapsulada com o header IP padrão, como se fosse um conjunto de dados de uma camada superior (no entanto opera apenas na camada 2).
- ▶ Mensagens ICMP não são enviadas em resposta a outras mensagens ICMP para evitar repetições infinitas.

→ LIVRO TEXTO

- ▶ **Atenção:** A Figura 3.27 (Subseção 3.2.1) que trata do formato da mensagem ICMP está incorreta. A figura correta é apresentada abaixo:



- ▶ Exemplos de tipos de mensagem (Type):

- ▶ 0 - Echo reply
- ▶ 3 - Destination unreachable
- ▶ 4 - Source quench
- ▶ 5 - Redirect
- ▶ 8 - Echo
- ▶ 9 - Router advertisement
- ▶ 10 - Router solicitation
- ▶ 11 - Time exceeded
- ▶ 12 - Parameter problem
- ▶ 13 - Time stamp request
- ▶ 14 - Time stamp reply
- ▶ 17 - Address mask request
- ▶ 18 - Address mask reply
- ▶ 30 - Traceroute
- ▶ 37 - Domain name request
- ▶ 38 - Domain name reply

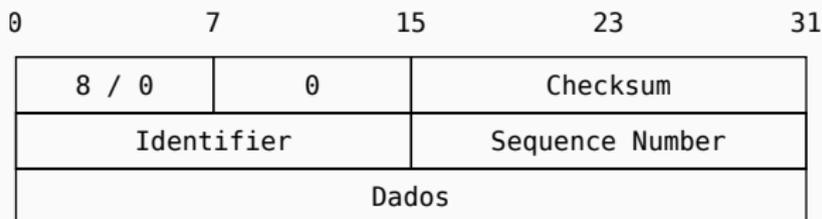
ICMP - Tipos de mensagens e códigos

- **Tabela completa** com tipos de mensagens e códigos (Fonte: James Kurose, Keith Ross. Computer Networking: A Top-Down Approach, 7th Edition, 2017, Cap. 5, pag. 448):

ICMP Type	Code	Description
0	0	echo reply (to ping)
3	0	destination network unreachable
3	1	destination host unreachable
3	2	destination protocol unreachable
3	3	destination port unreachable
3	6	destination network unknown
3	7	destination host unknown
4	0	source quench (congestion control)
8	0	echo request
9	0	router advertisement
10	0	router discovery
11	0	TTL expired
12	0	IP header bad

Figure 5.19 ♦ ICMP message types

- ▶ Comando geralmente utilizado para testar se é possível acessar um destinatário.
- ▶ Utiliza mensagem ICMP tipo 8 (*Echo*) e tipo 0 (*Echo reply*)



- ▶ Formato do comando ping padrão:

```
ping <host>
```

ICMP - Aplicação ICMP: Ping (Wireshark)

The image shows a Wireshark capture of ICMP traffic. The main pane displays a list of 12 packets, alternating between Echo (ping) requests and replies. The details pane shows the structure of an Internet Control Message Protocol (ICMP) packet, specifically an Echo (ping) request. The data pane shows the raw bytes of the packet in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Autonomous	Info
3	0.001853	192.168.1.2	192.168.1.3	ICMP	98		Echo (ping) request id=0x6838, seq=1/256, ttl=64 (reply in 4)
4	0.001853	192.168.1.3	192.168.1.2	ICMP	98		Echo (ping) reply id=0x6838, seq=1/256, ttl=64 (request in 3)
5	1.005177	192.168.1.2	192.168.1.3	ICMP	98		Echo (ping) request id=0x6938, seq=2/512, ttl=64 (reply in 6)
6	1.005177	192.168.1.3	192.168.1.2	ICMP	98		Echo (ping) reply id=0x6938, seq=2/512, ttl=64 (request in 5)
7	2.007621	192.168.1.2	192.168.1.3	ICMP	98		Echo (ping) request id=0x6a38, seq=3/768, ttl=64 (reply in 8)
8	2.007621	192.168.1.3	192.168.1.2	ICMP	98		Echo (ping) reply id=0x6a38, seq=3/768, ttl=64 (request in 7)
9	3.009980	192.168.1.2	192.168.1.3	ICMP	98		Echo (ping) request id=0x6b38, seq=4/1024, ttl=64 (reply in 10)
10	3.009980	192.168.1.3	192.168.1.2	ICMP	98		Echo (ping) reply id=0x6b38, seq=4/1024, ttl=64 (request in 9)
11	4.012254	192.168.1.2	192.168.1.3	ICMP	98		Echo (ping) request id=0x6c38, seq=5/1280, ttl=64 (reply in 12)
12	4.012254	192.168.1.3	192.168.1.2	ICMP	98		Echo (ping) reply id=0x6c38, seq=5/1280, ttl=64 (request in 11)

Internet Control Message Protocol
Type: 8 (Echo (ping) request)
Code: 0
Checksum: 0xb7d2 [correct]
[Checksum Status: Good]
Identifier (BE): 26600 (0x6838)
Identifier (LE): 14440 (0x3868)
Sequence number (BE): 1 (0x0001)
Sequence number (LE): 256 (0x0100)
[\[Response frame: 4\]](#)
Data (56 bytes)

```
0000  00 50 79 66 68 01 00 50  79 66 68 00 00 00 45 00  -P yfh...E-
0010  00 54 38 68 00 00 40 01  be eb c0 a8 01 02 c0 a8  -T8h @ .....
0020  01 a3 38 00 07 d2 68 38  00 01 00 00 00 0b 0c 0d  -...h0 .....
0030  0e 0f 10 11 12 13 14 15  16 17 18 19 1a 1b 1c 1d  -.....
0040  1e 1f 20 21 22 23 24 25  26 27 28 29 2a 2b 2c 2d  -...!*$%&'()*+,-./:;
0050  2e 2f 30 31 32 33 34 35  36 37 38 39 3a 3b 3c 3d  -.....
0060  3e 3f
```

Internet Control Message Protocol (icmp), 64 byte(s) | Packets: 12 · Displayed: 10 (83.3%) | Profile: EIGRP

- ▶ Programa que determina a rota de datagramas IPs através da rede.
- ▶ Envia n datagramas UDP com TTL (Time To Live) diferentes e uma especificação de número de porta do host fora do intervalo válido.
- ▶ Deste modo, ele determina a rota a partir das mensagens de erro ICMP (Time Exceeded e Port Unreachable).
- ▶ Na literatura encontramos duas definições de Time To Live:
 1. tempo em segundos que o datagrama pode viajar.
 2. número de dispositivos que um datagrama pode viajar.

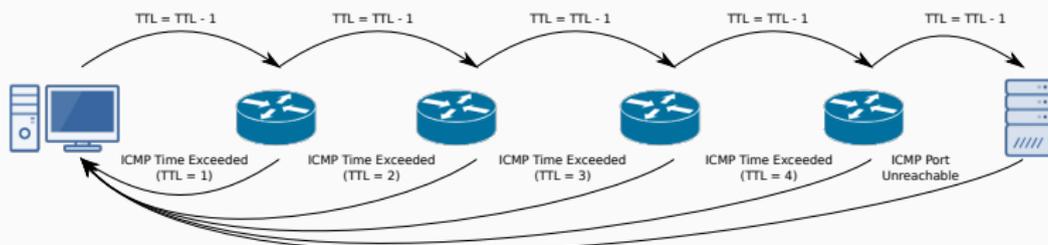


comando

linux: `traceroute IP`

windows: `tracert IP`

- ▶ Programa que determina a rota de datagramas IPs através da rede.
- ▶ Envia n datagramas UDP com TTL (Time To Live) diferentes e uma especificação de número de porta do host fora do intervalo válido.
- ▶ Deste modo, ele determina a rota a partir das mensagens de erro ICMP (Time Exceeded e Port Unreachable).
- ▶ Na literatura encontramos duas definições de Time To Live:
 1. tempo em segundos que o datagrama pode viajar.
 2. número de dispositivos que um datagrama pode viajar.



Time Exceeded: Type 11 code 0
Port Unreachable: Type 3 code 3

ICMP - Aplicação ICMP: Traceroute (Demonstração)

```
PowerShell 7
C:\Users\aksato> traceroute 143.107.99.214

Rastreamento da rota para labgeocomp.poli.usp.br [143.107.99.214]
com no máximo 30 saltos:

 1 <1 ms <1 ms <1 ms router.asus.com [192.168.1.1]
 2 * * * Esgotado o tempo limite do pedido.
 3 2 ms 1 ms 2 ms 152-255-151-82.user.vivozap.com.br [152.255.151.82]
 4 1 ms 3 ms 2 ms 187-100-197-62.dsl.telesp.net.br [187.100.197.62]
 5 3 ms 3 ms 3 ms as28571.saopaulo.sp.ix.br [187.16.216.20]
 6 3 ms 3 ms 3 ms core-cce.uspnet.usp.br [143.107.251.30]
 7 * * * Esgotado o tempo limite do pedido.
 8 * * * Esgotado o tempo limite do pedido.
 9 3 ms 3 ms 3 ms labgeocomp.poli.usp.br [143.107.99.214]

Rastreamento concluído.
```

Capturing from Ethernet [PC1 Ethernet] to Switch1 [Ethernet0]

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

(ip.src==192.168.1.220 && ip.dst==143.107.99.214) || (icmp && p.dst==192.168.1.220)

No.	Time	Source	Destination	Protocol	Length	Info
14	6.718299	192.168.1.220	143.107.99.214	ICMP	106	Echo (ping) request id=0x0001, seq=113/28928, ttl=1 (no response found!)
15	6.718314	192.168.1.220	143.107.99.214	ICMP	106	Echo (ping) request id=0x0001, seq=113/28928, ttl=1 (no response found!)
16	6.718585	192.168.1.1	192.168.1.220	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
17	6.718979	192.168.1.220	143.107.99.214	ICMP	106	Echo (ping) request id=0x0001, seq=114/29184, ttl=1 (no response found!)
18	6.718988	192.168.1.220	143.107.99.214	ICMP	106	Echo (ping) request id=0x0001, seq=114/29184, ttl=1 (no response found!)
19	6.711281	192.168.1.1	192.168.1.220	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
20	6.711587	192.168.1.220	143.107.99.214	ICMP	106	Echo (ping) request id=0x0001, seq=115/29440, ttl=1 (no response found!)
21	6.711513	192.168.1.220	143.107.99.214	ICMP	106	Echo (ping) request id=0x0001, seq=115/29440, ttl=1 (no response found!)
22	6.711714	192.168.1.1	192.168.1.220	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
26	7.718554	192.168.1.220	143.107.99.214	ICMP	106	Echo (ping) request id=0x0001, seq=116/29696, ttl=2 (no response found!)
27	7.718589	192.168.1.220	143.107.99.214	ICMP	106	Echo (ping) request id=0x0001, seq=116/29696, ttl=2 (no response found!)
33	11.419734	192.168.1.220	143.107.99.214	ICMP	106	Echo (ping) request id=0x0001, seq=117/29952, ttl=2 (no response found!)
34	11.419770	192.168.1.220	143.107.99.214	ICMP	106	Echo (ping) request id=0x0001, seq=117/29952, ttl=2 (no response found!)

Resolução de Endereços

TCP/IP

4. Aplicação	HTTP, FTP, Telnet, DNS
3. Transporte	TCP, UDP
2. Internet	IP
1. Enlace (Interface com Rede)	Ethernet

Endereços (com exemplos)

Porta	80
End. Lógico: IP	192.168.1.1
End. Físico: MAC	00:1B:44:11:3A:B7

Camadas 1 e 2 - Por que precisamos dos endereços MAC e IP?

- ▶ Tanto o endereço MAC, que é gravado no hardware físico, como o endereço IP são únicos. Por que são necessários ambos os endereços ?
- ▶ Os endereços MAC não possuem estruturas: um *host* deve inundar a rede com mensagens para obter o endereço MAC de destino. Além disso, é preciso armazenar uma tabela com todos os endereços MAC.
- ▶ Os endereços IPs são divididos de modo a facilitar a sua localização.

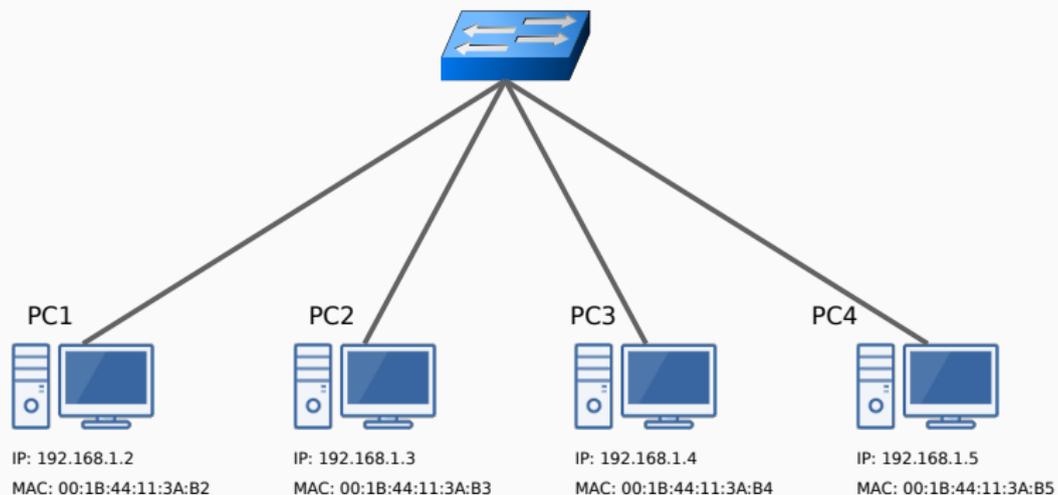
ARP - Resolução de Endereços de Camada 1

- ▶ Em uma rede física única, o endereço físico (camada 1) é utilizado para endereçar pacotes.
- ▶ No entanto, para protocolos de camadas superiores, o endereço IP é utilizado. Este endereço, no entanto, não é compreendido pelo driver do dispositivo de rede.
- ▶ O ARP (*Address Resolution Protocol*) é o protocolo responsável para traduzir endereços IP para endereços físicos (MAC).
- ▶ Uma mensagem de *ARP Request* é enviada em broadcast com o endereço IP do destinatário. Este responde com uma mensagem de *ARP reply* contendo o seu endereço físico.
- ▶ A resposta é armazenada no *ARP Cache*, para ser reutilizada em comunicações futuras.

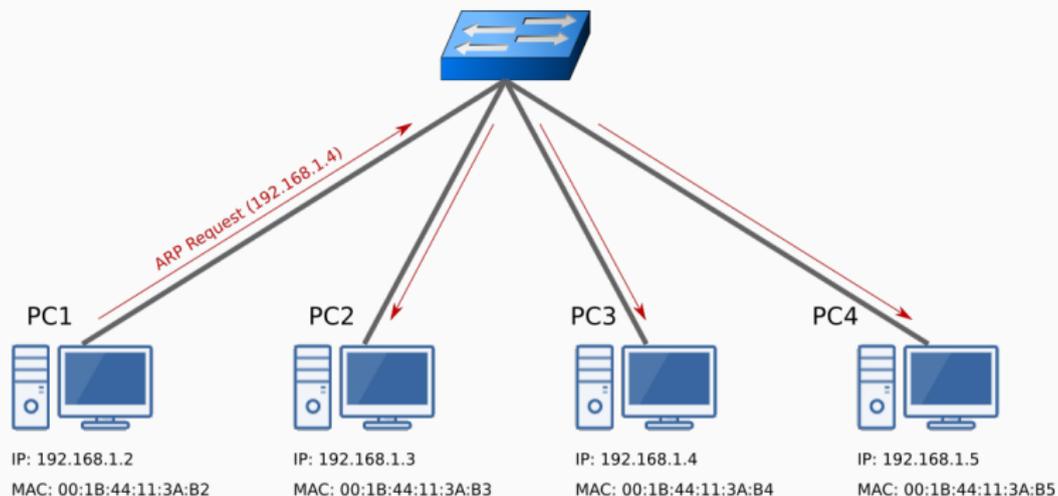
Hardware Address Space (2 bytes)	Protocol Address Space (2 bytes)
Hardware Address Byte Length (2 bytes)	Protocol Address Byte Length (2 bytes)
Operation Code: ARP request (1) or reply (2) (2 bytes)	
Hardware Address of Sender (MAC 6 bytes)	
Protocol Address of Sender (IP 4 bytes)	
Hardware Address of Target (MAC 6 bytes)	
Protocol Address of Target (IP 4 bytes)	

- ▶ ARP é um protocolo de camada 2, então o pacote ARP é encapsulado com o cabeçalho da camada 1.

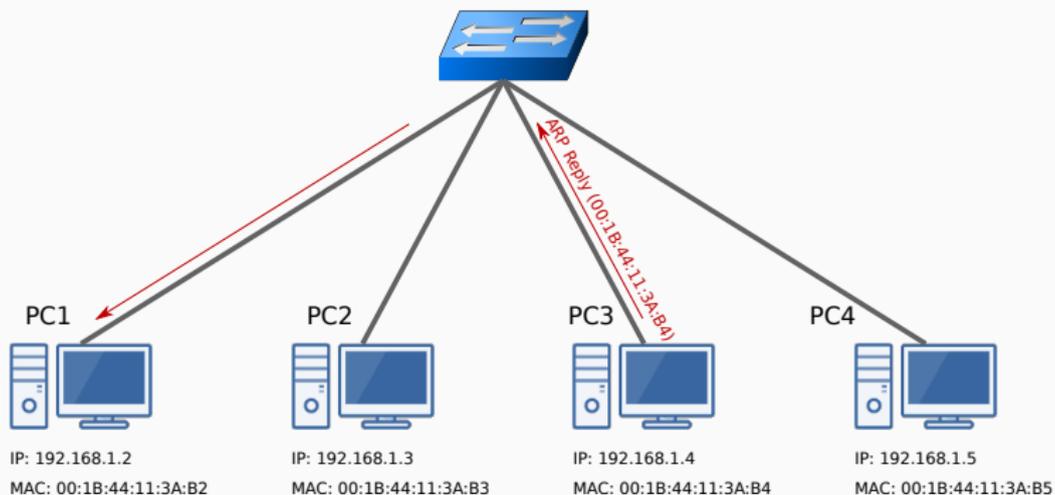
- ▶ PC1 deseja enviar dados para PC3



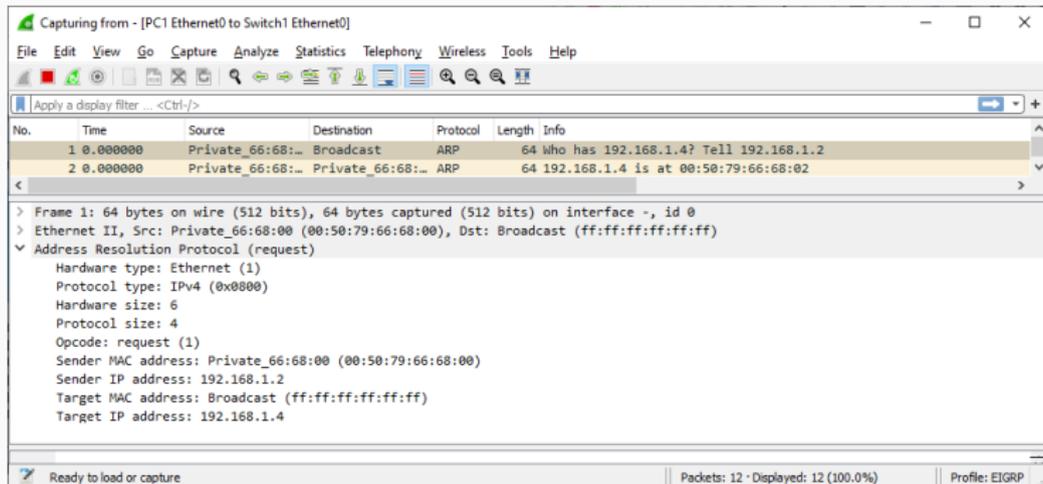
- ▶ PC1 deseja enviar dados para PC3



- ▶ PC1 deseja enviar dados para PC3



ARP - Demonstração



Capturing from - [PC1 Ethernet0 to Switch1 Ethernet0]

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	Private_66:68:...	Broadcast	ARP	64	Who has 192.168.1.4? Tell 192.168.1.2
2	0.000000	Private_66:68:...	Private_66:68:...	ARP	64	192.168.1.4 is at 00:50:79:66:68:02

> Frame 1: 64 bytes on wire (512 bits), 64 bytes captured (512 bits) on interface -, id 0
> Ethernet II, Src: Private_66:68:00 (00:50:79:66:68:00), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
▼ Address Resolution Protocol (request)
 Hardware type: Ethernet (1)
 Protocol type: IPv4 (0x0800)
 Hardware size: 6
 Protocol size: 4
 Opcode: request (1)
 Sender MAC address: Private_66:68:00 (00:50:79:66:68:00)
 Sender IP address: 192.168.1.2
 Target MAC address: Broadcast (ff:ff:ff:ff:ff:ff)
 Target IP address: 192.168.1.4

Ready to load or capture | Packets: 12 · Displayed: 12 (100.0%) | Profile: EIGRP

```
PC1> arp
```

```
00:50:79:66:68:02 192.168.1.4 expires in 83 seconds
```

```
PC3> arp
```

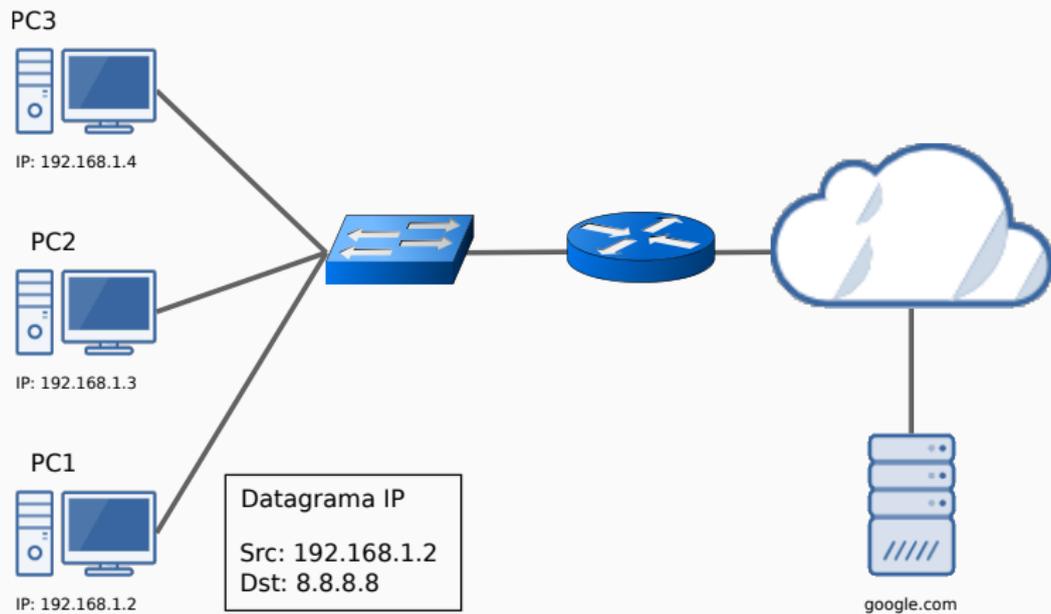
```
00:50:79:66:68:00 192.168.1.2 expires in 112 seconds
```

NAT

- ▶ *Network Address Translation* (NAT) realiza o mapeamento entre endereços IPs privado e endereços IP públicos.
- ▶ Foi sugerido como uma solução de curto prazo para o problema de esgotamento de endereços IPv4. Também permite conectar na internet redes que inicialmente eram para ser exclusivamente locais.
- ▶ Existem duas variações do NAT: o NAT básico e o NATP (também conhecido como PAT).

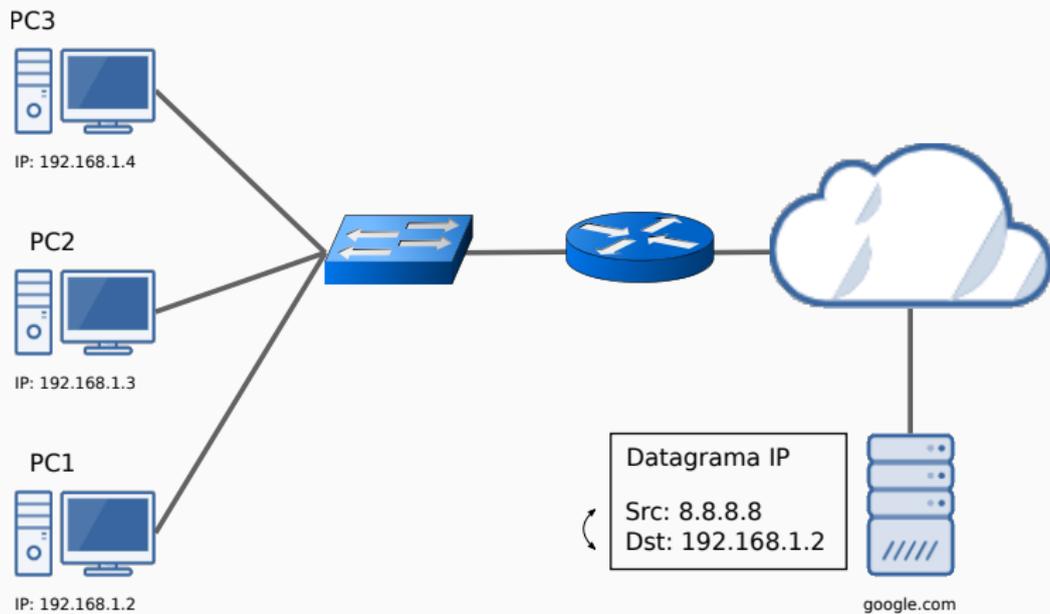
NAT - Descrição do Problema

- ▶ Como obter resposta de um pacote enviado a partir de um host de uma rede local (com end. IP privado)?



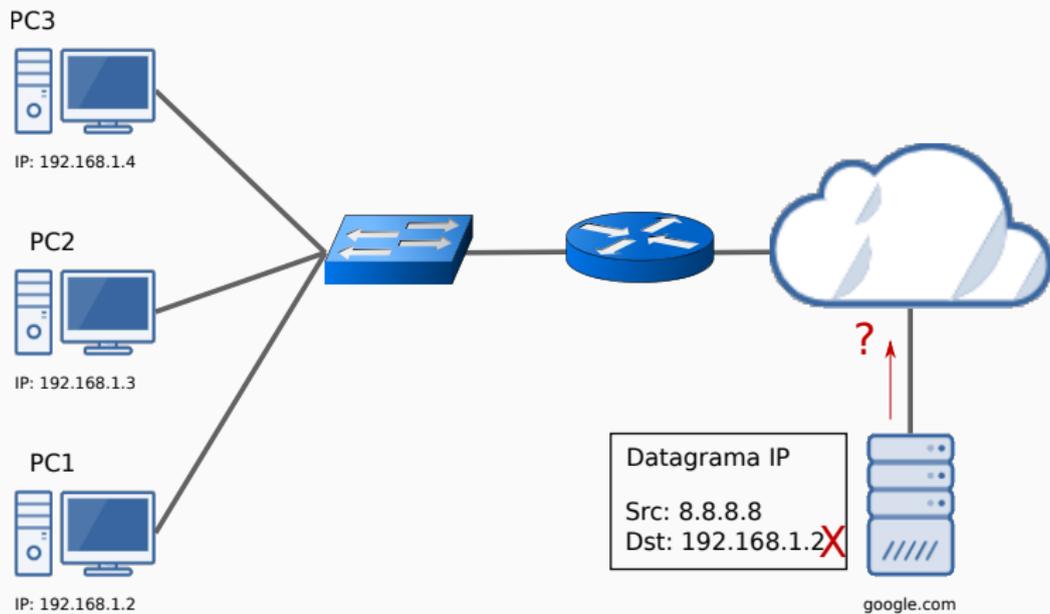
NAT - Descrição do Problema

- ▶ Como obter resposta de um pacote enviado a partir de um host de uma rede local (com end. IP privado)?

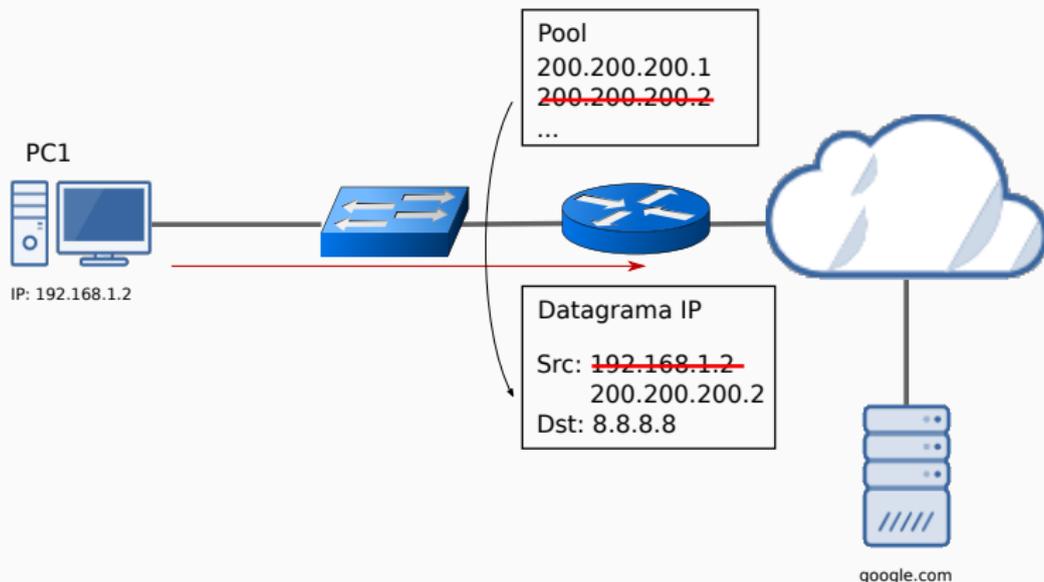


NAT - Descrição do Problema

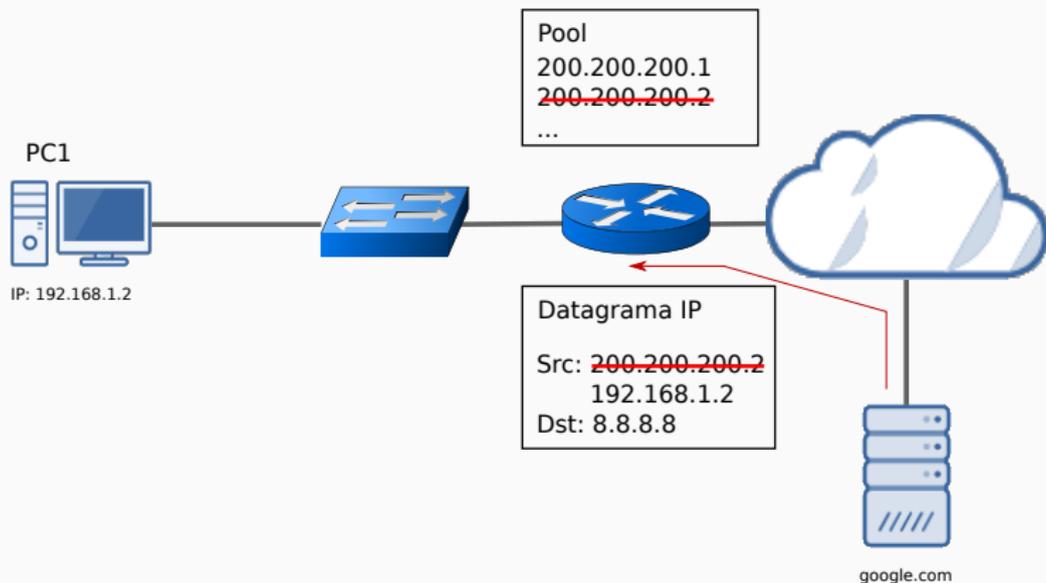
- ▶ Como obter resposta de um pacote enviado a partir de um host de uma rede local (com end. IP privado)?



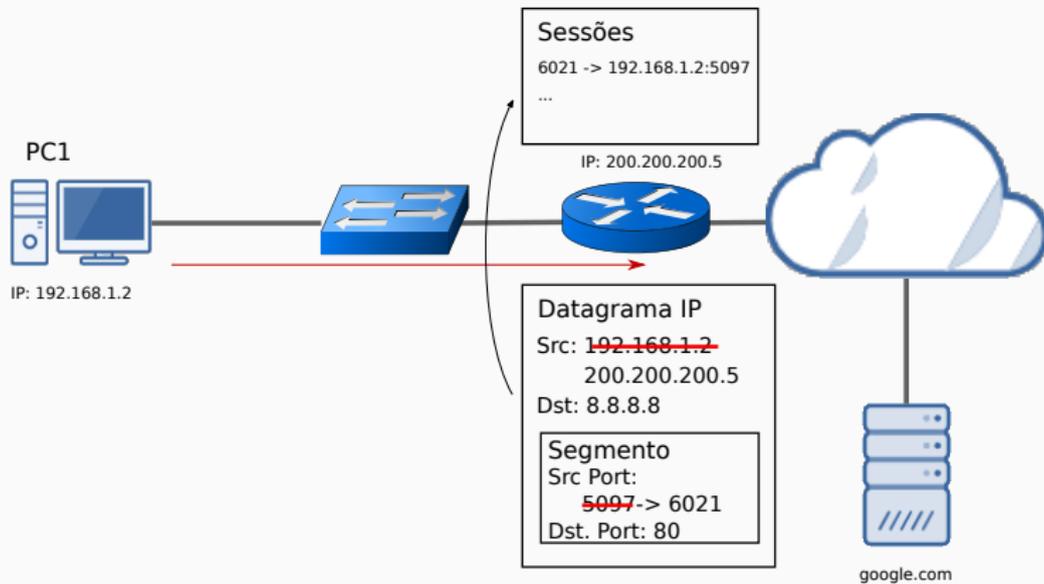
- ▶ Para pacotes enviados, o NAT traduz dinamicamente o endereço do remetente para um endereço global reservado.
- ▶ Para pacotes recebidos, o NAT traduz o endereço global para o endereço local correspondente.
- ▶ Os endereços globais são armazenados em um pool de endereços.



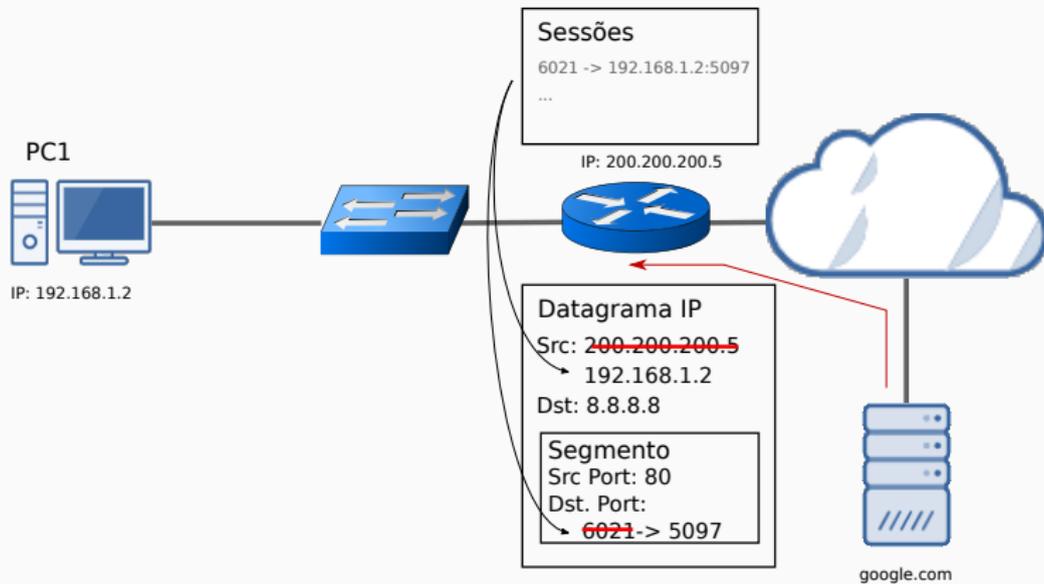
- ▶ Para pacotes enviados, o NAT traduz dinamicamente o endereço do remetente para um endereço global reservado.
- ▶ Para pacotes recebidos, o NAT traduz o endereço global para o endereço local correspondente.
- ▶ Os endereços globais são armazenados em um pool de endereços.



- ▶ O NATP utiliza informações de porta (camada 3) para mapear múltiplos endereços IP privados para um único endereço global.



- ▶ O NATP utiliza informações de porta (camada 3) para mapear múltiplos endereços IP privados para um único endereço global.



- ▶ Alguns protocolos de aplicação incluem endereços IPs dentro da mensagem da camada de aplicação, como o FTP. Implementações NAT devem levar em consideração cada uma dessas situações.
- ▶ NAT é computacionalmente custoso, uma vez que cada pacote deve ser analisado e potencialmente alterado.
- ▶ As respostas e requisições devem obrigatoriamente passar pelo mesmo roteador, que possui os mapeamentos necessários para realizar a tradução de endereços.

DHCP

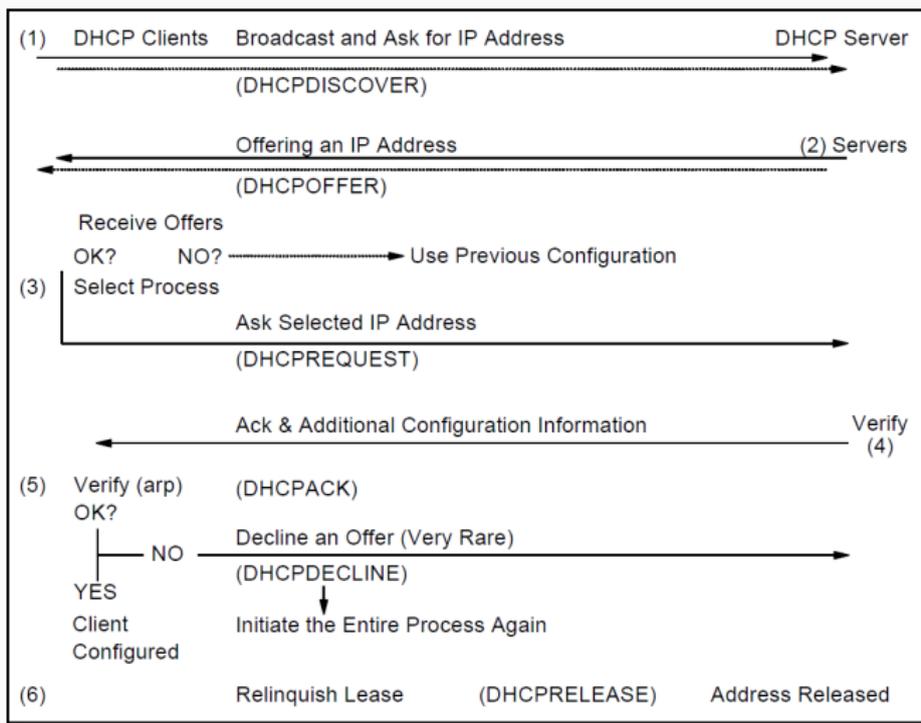
- ▶ O DHCP (*Dynamic Host Configuration Protocol*) providencia um *framework* para a transferência de informações de configuração para os hosts.
- ▶ Isto é, permite a configuração "automática" de hosts conectados à uma rede. Assim, um cliente da rede pode inicializar com uma configuração mínima e requisitar seu endereço IP, gateway padrão e máscara de subrede para um servidor DHCP.
- ▶ Utiliza o Bootstrap Protocol (BOOTP) inicialmente desenvolvido para o acesso a rede de terminais de computador diskless.
- ▶ Este mecanismo é bastante utilizado para servir equipamentos móveis, que frequentemente realizam mudança de redes.
- ▶ O DHCP possui duas funções principais: 1) providenciar um protocolo para transmissão de parâmetros de configuração e 2) gerenciar a alocação de endereços temporários e permanentes de hosts.

- Confira subseção 3.7.1 do livro texto para mais detalhes.

0	7	15	23	31
Code	HWtype	length	hops	
Transaction ID				
seconds		flags field		
Client IP Address				
Your IP Address				
Server IP Address				
Router IP Address				
Client Hardware Address(16 bytes)				
Server Host Name (64 bytes)				
Boot File Name (128 bytes)				
Options (312 bytes)				

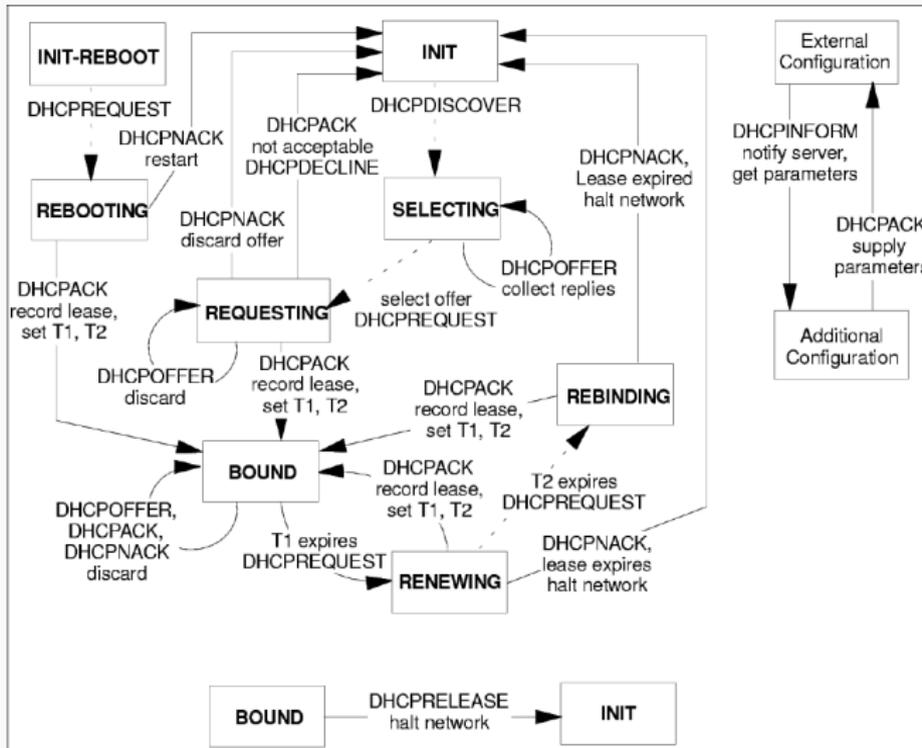
DHCP - Tipos de Mensagem e Alocação de um Novo Endereço

- ▶ Exemplo de alocação de um novo endereço.



- ▶ Ao alocar um novo endereço, o cliente recebe uma concessão para o endereço.
- ▶ Esta concessão possui um tempo de expiração; por isso, o cliente deve renovar a concessão frequentemente.
- ▶ A renovação é feita em quatro etapas:
 1. quando um cliente é configurado (recebe a mensagem DHCPACK), este é informado do tempo de concessão (*lease time*) e de mais dois tempos T1 e T2, que geralmente são 50% e 87,5% do *lease time*.
 2. quando o tempo T1 é atingido, o cliente inicia a renovação da concessão com o envio de uma mensagem DHCPREQUEST em unicast. O servidor deve responder com um DHCPACK confirmando a renovação e os tempos T1 e T2 são resetados.
 3. se o tempo T2 é atingido e o servidor ainda não respondeu a requisição, o cliente manda uma mensagem DHCPREQUEST em broadcast. Assim, qualquer servidor pode responder a renovação.
 4. se o tempo de concessão é atingido sem respostas de algum servidor, o cliente deve parar de usar a configuração TCP/IP.

DHCP - Diagrama de Estados



The image shows a Wireshark packet capture window for the interface [PC1 Ethernet0 to Switch1 Ethernet0]. The capture filter is set to 'dhcp'. The packet list pane shows six packets related to a DHCP transaction:

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	0.0.0.0	255.255.255.255	DHCP	406	DHCP Discover - Transaction ID 0x736ae207
3	1.000464	0.0.0.0	255.255.255.255	DHCP	406	DHCP Discover - Transaction ID 0x736ae207
4	2.165330	192.168.100.1	192.168.100.2	DHCP	342	DHCP Offer - Transaction ID 0x736ae207
5	4.001007	0.0.0.0	255.255.255.255	DHCP	406	DHCP Request - Transaction ID 0x736ae207
6	4.003909	192.168.100.1	192.168.100.2	DHCP	342	DHCP ACK - Transaction ID 0x736ae207

The packet details pane for the selected DHCP ACK packet (No. 6) shows the following structure:

- Ethernet II, Src: 0c:0e:9f:c7:a4:00 (0c:0e:9f:c7:a4:00), Dst: Private_66:68:00 (00:50:79:66:68:00)
- Internet Protocol Version 4, Src: 192.168.100.1, Dst: 192.168.100.2
- User Datagram Protocol, Src Port: 67, Dst Port: 68
- Dynamic Host Configuration Protocol (ACK)
 - Message type: Boot Reply (2)
 - Hardware type: Ethernet (0x01)
 - Hardware address length: 6
 - Hops: 0
 - Transaction ID: 0x736ae207
 - Seconds elapsed: 0
 - Bootp flags: 0x0000 (Unicast)
 - Client IP address: 192.168.100.2
 - Your (client) IP address: 192.168.100.2
 - Next server IP address: 0.0.0.0
 - Relay agent IP address: 0.0.0.0
 - Client MAC address: Private_66:68:00 (00:50:79:66:68:00)
 - Client hardware address padding: 00000000000000000000
 - Server host name not given
 - Boot file name not given
 - Magic cookie: DHCP
 - Option: (53) DHCP Message Type (ACK)
 - Option: (54) DHCP Server Identifier (192.168.100.1)
 - Option: (51) IP Address Lease Time
 - Option: (58) Renewal Time Value
 - Option: (59) Rebinding Time Value
 - Option: (1) Subnet Mask (255.255.255.0)
 - Option: (6) Domain Name Server
 - Option: (3) Router
 - Option: (255) End
 - Padding: 0000000000000000000000000000

The packet bytes pane shows the raw data: 0020 64 02 00 43 00 44 01 34 37 5c 02 01 06 00 73 6c d..C.D.4 71....53

Summary: Dynamic Host Configuration Protocol (dhcp), 300 byte(s) | Packets: 9 · Displayed: 5 (55.6%) | Profile: EIGRP

Referências

- ▶ Para o curso: livro da IBM “TCP/IP Tutorial and technical overview” (disponível em <https://www.redbooks.ibm.com/redbooks/pdfs/gg243376.pdf>).
- ▶ **Para esta aula: Seções 3.1.7, 3.2, 3.4, 3.7.**

The End!