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

Notas de autoria (Disclaimer) - Equipe envolvida

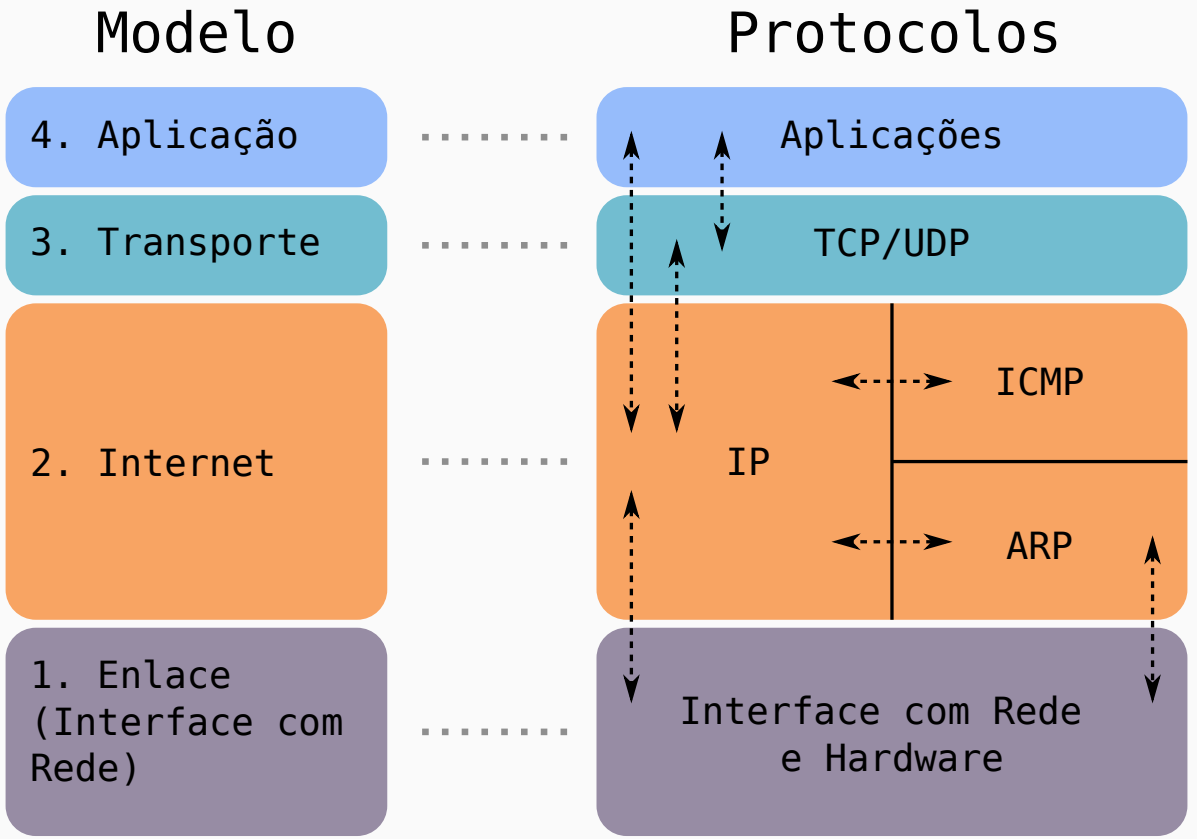
Os slides que serão utilizados nesse ano são baseados no curso desenvolvido para os anos 2020, 2021 e 2022. Participaram da concepção do curso e desenvolvimento do material os seguintes professores:

- 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

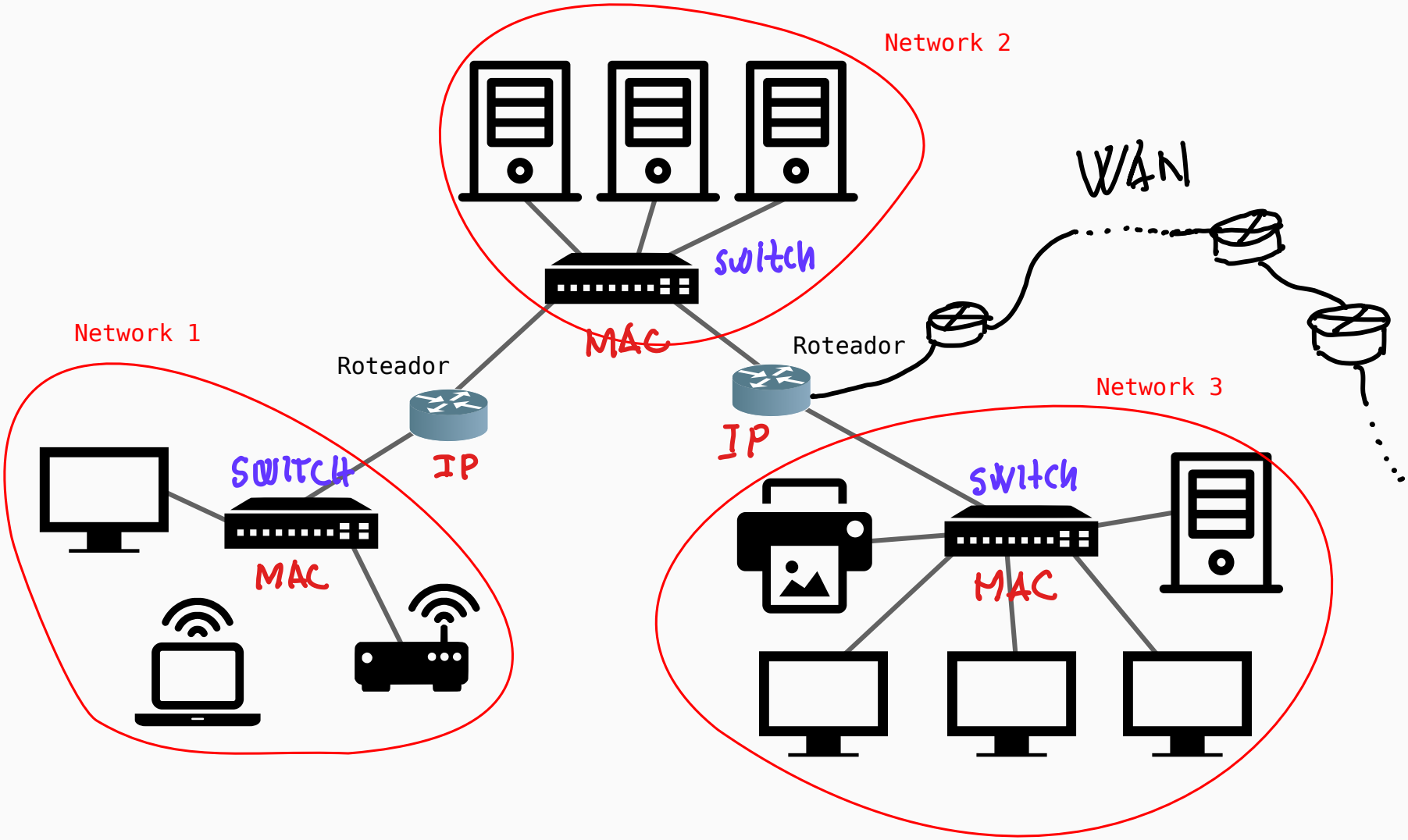
Conteúdo

Revisão

Revisão - Principais protocolos TCP / IP



Revisão - Redes e a internets



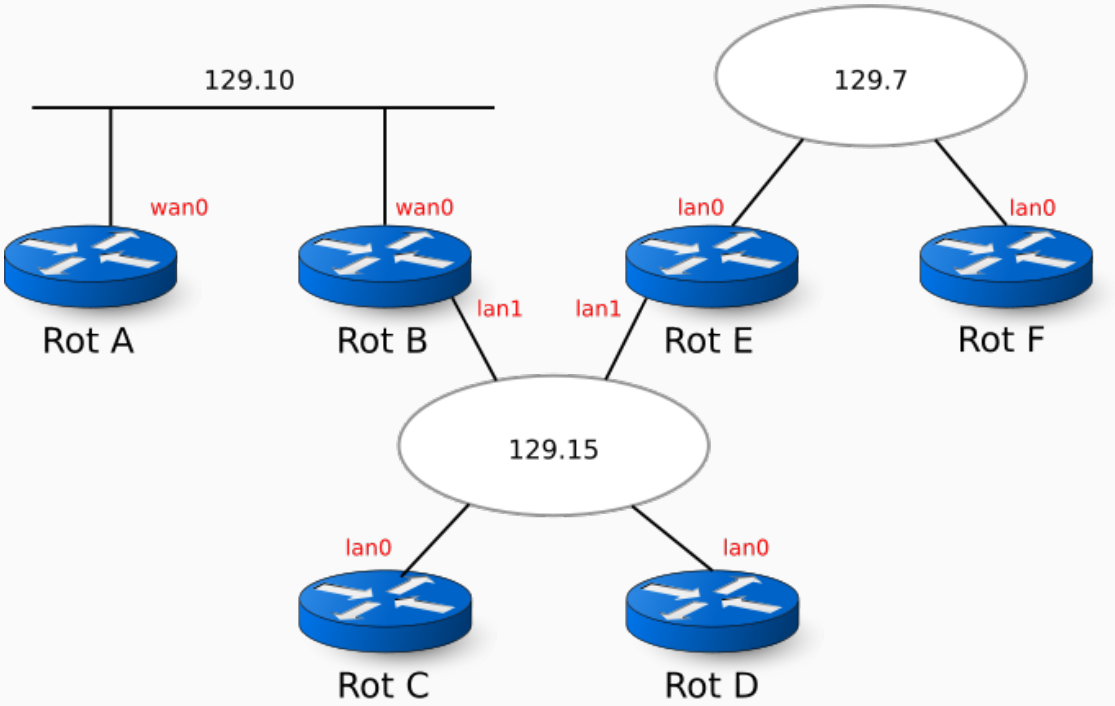
como descobrir o ip do seu computador ?

- windows: ipconfig
- linux: ifconfig

como descobrir os ips ativos da sua rede ?

nmap <CIDR ADDRESS>

Revisão - Protocolo IP



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

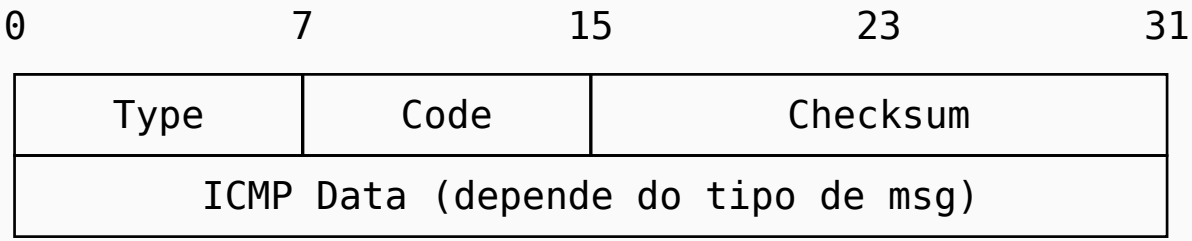
Reportando Erros - Internet Control Message Protocol (ICMP)

ICMP - Introdução

- 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.

ICMP - Mensagem

- **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

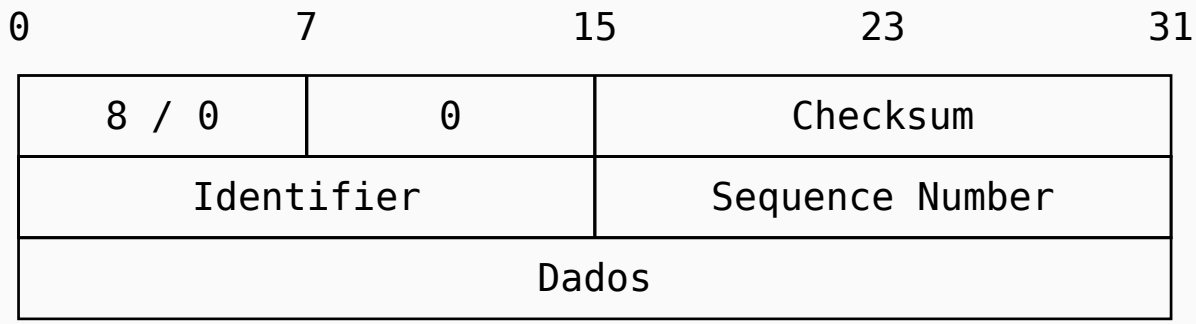
ICMP - Tipos de mensagens e códigos

- 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

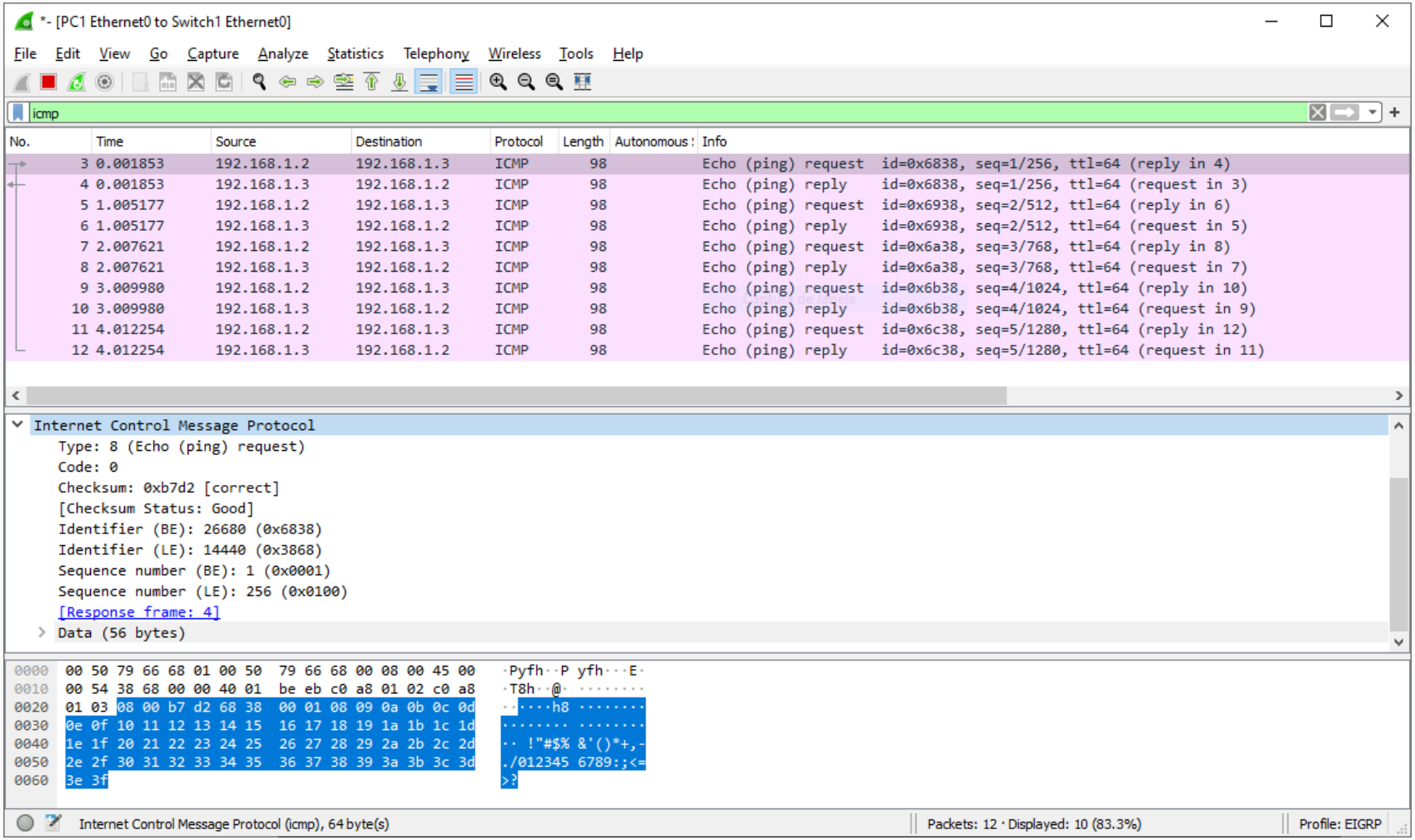
- Comando geralmente utilizado para testar se é possível acessar um destinatário.
- Utiliza mensagem ICMP tipo 8 (*Echo*) e tipo 0 (*Echo reply*)



- Formato do comando ping padrão:

```
ping <host>
```

ICMP - Aplicação ICMP: Ping (WireShark)

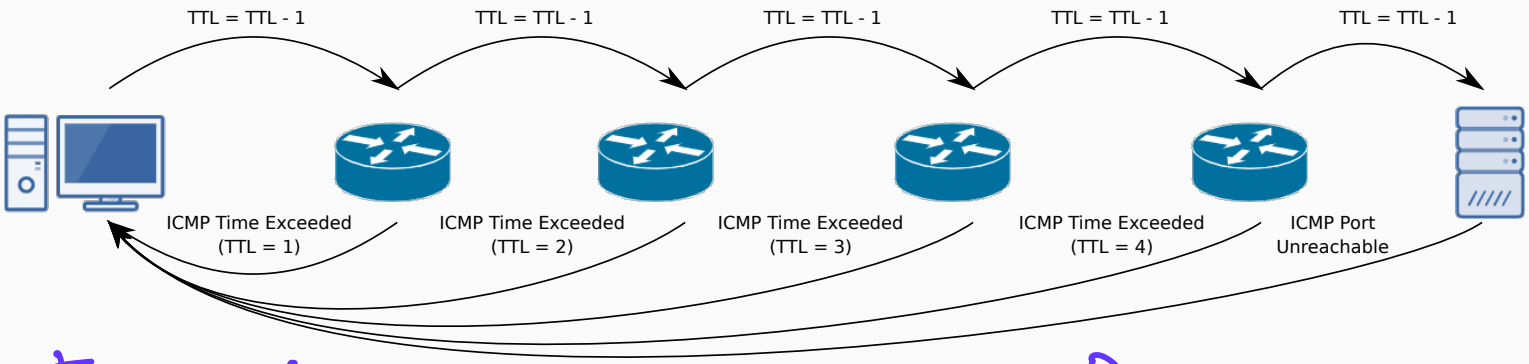


ICMP - Aplicação ICMP: Traceroute

- 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.



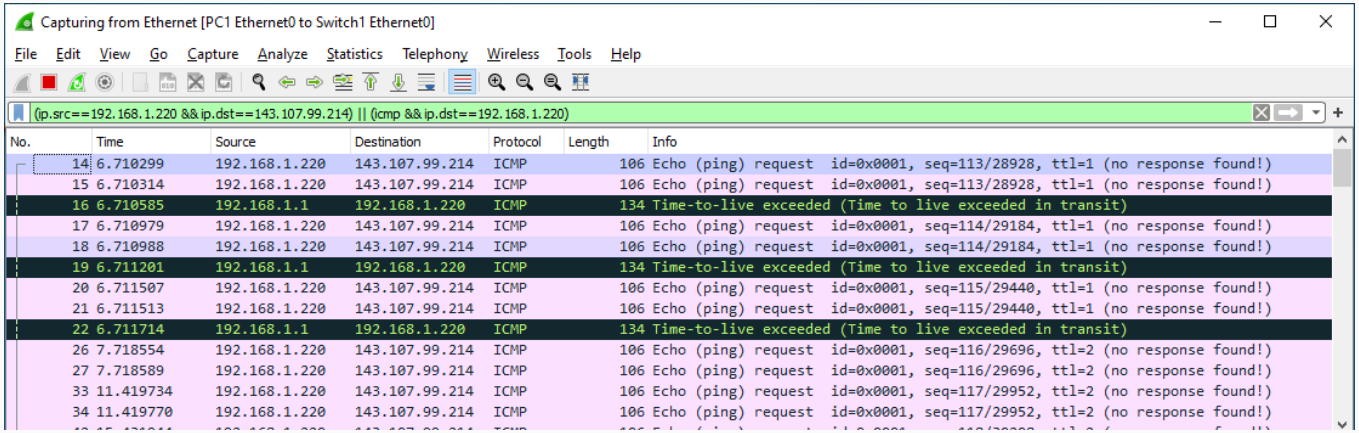
Time Exceeded : Type 11 code 0

Port Unreachable : Type 3 code 3

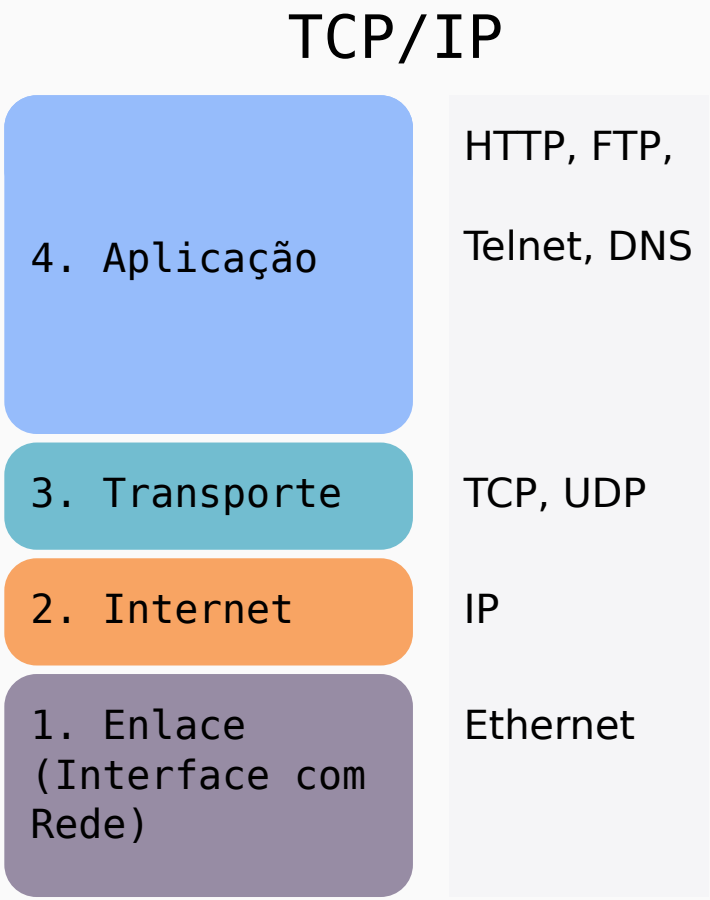
ICMP - Aplicação ICMP: Traceroute (Demonstração)

PowerShell 7

```
C:\Users\aksato> tracert 143.107.99.214

Rastreando a 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.
```



Resolução de Endereços



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 necessitamos 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

ARP - Introdução

- 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.

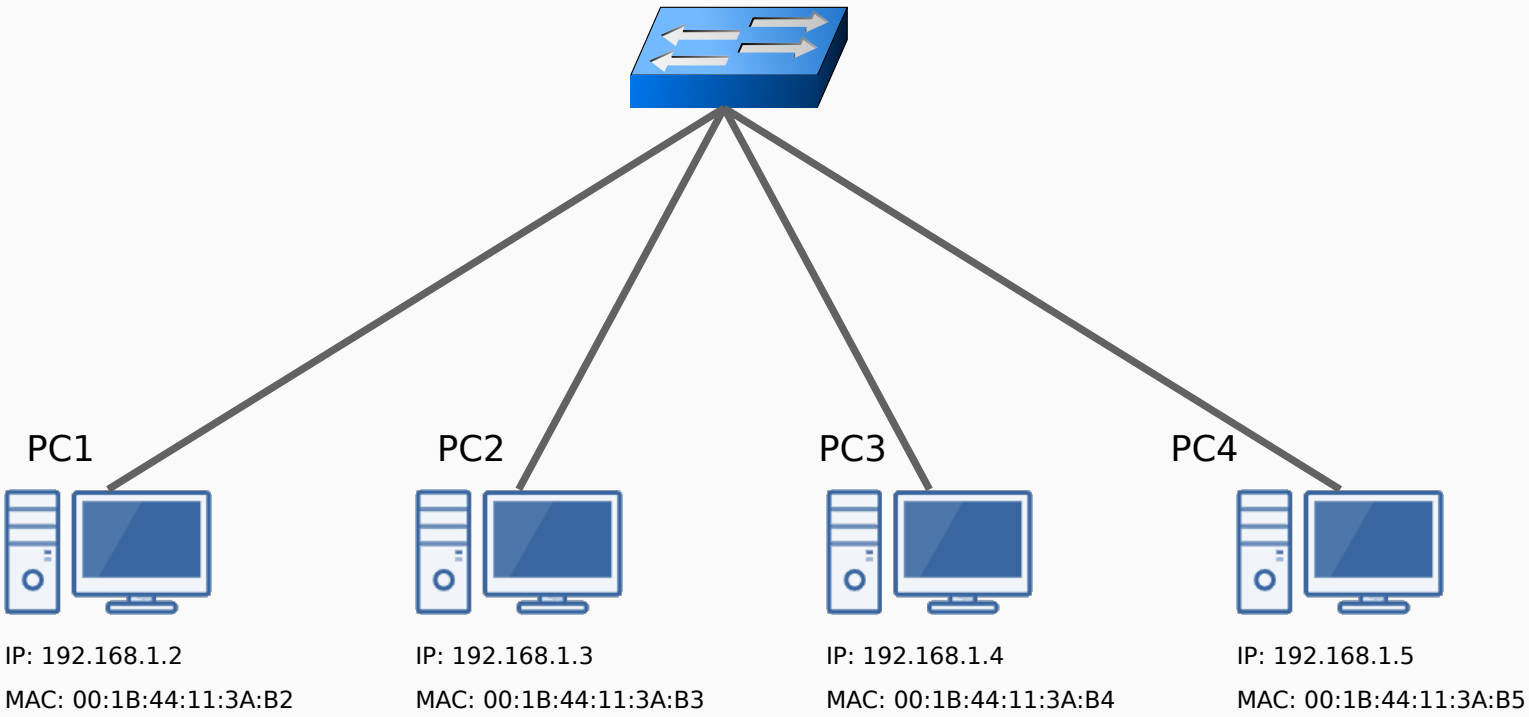
ARP - Pacote ARP

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.

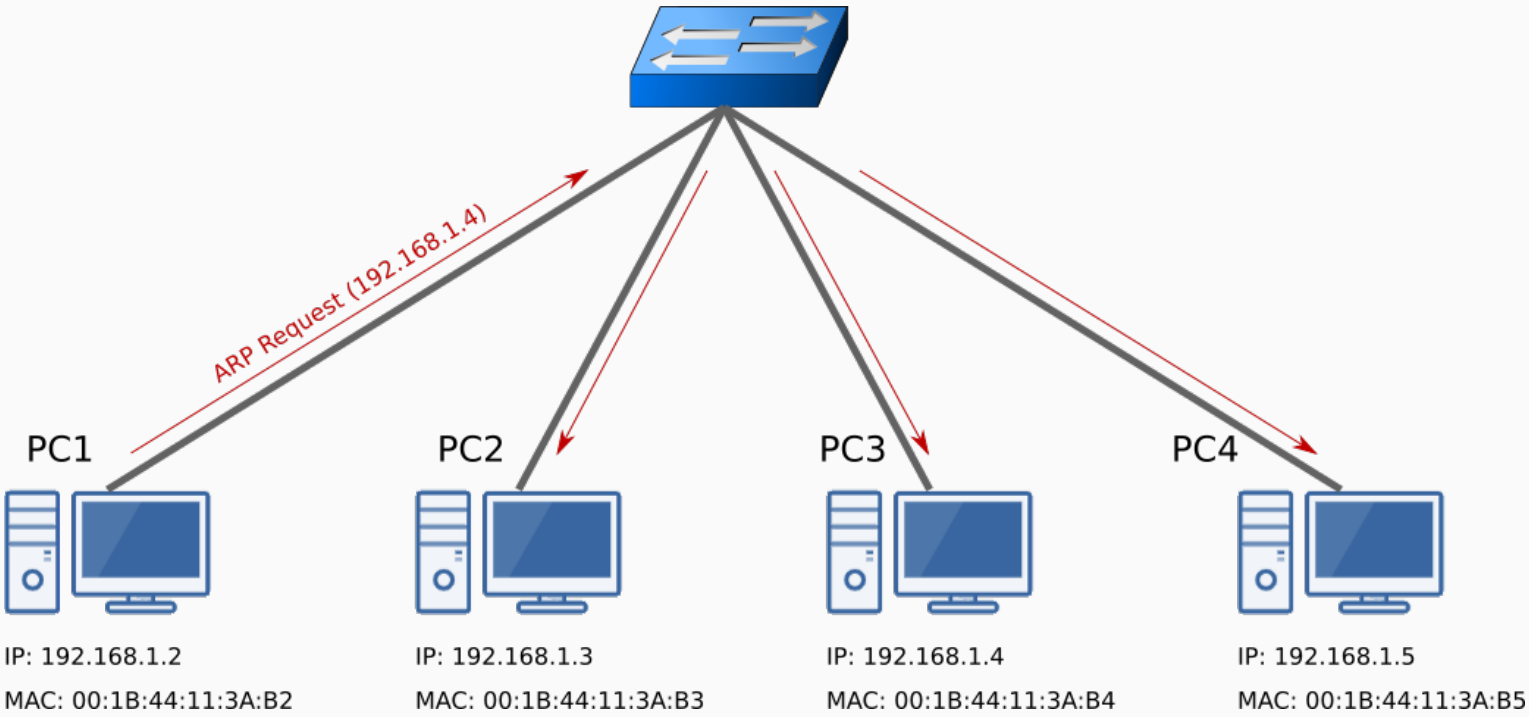
ARP - Procedimento

- PC1 deseja enviar dados para PC3



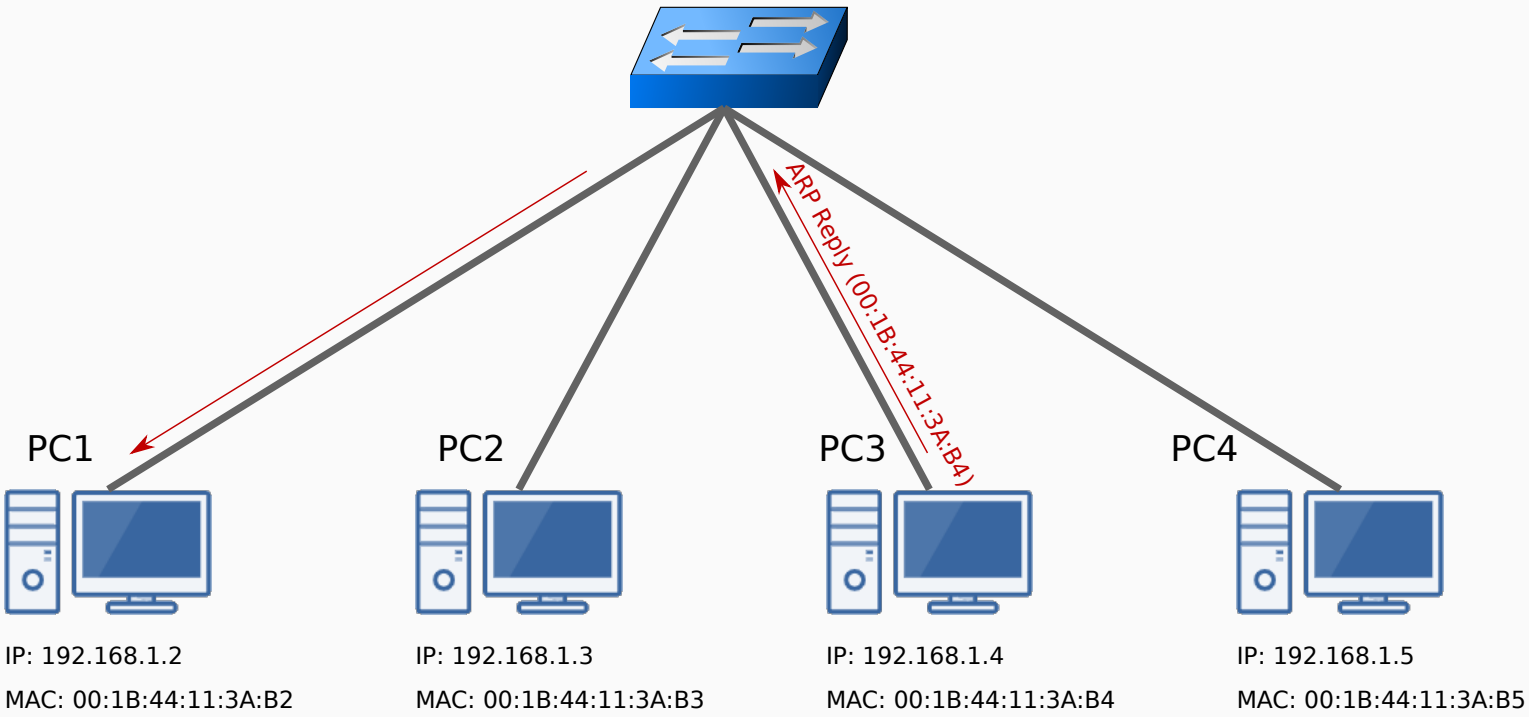
ARP - Procedimento

- PC1 deseja enviar dados para PC3

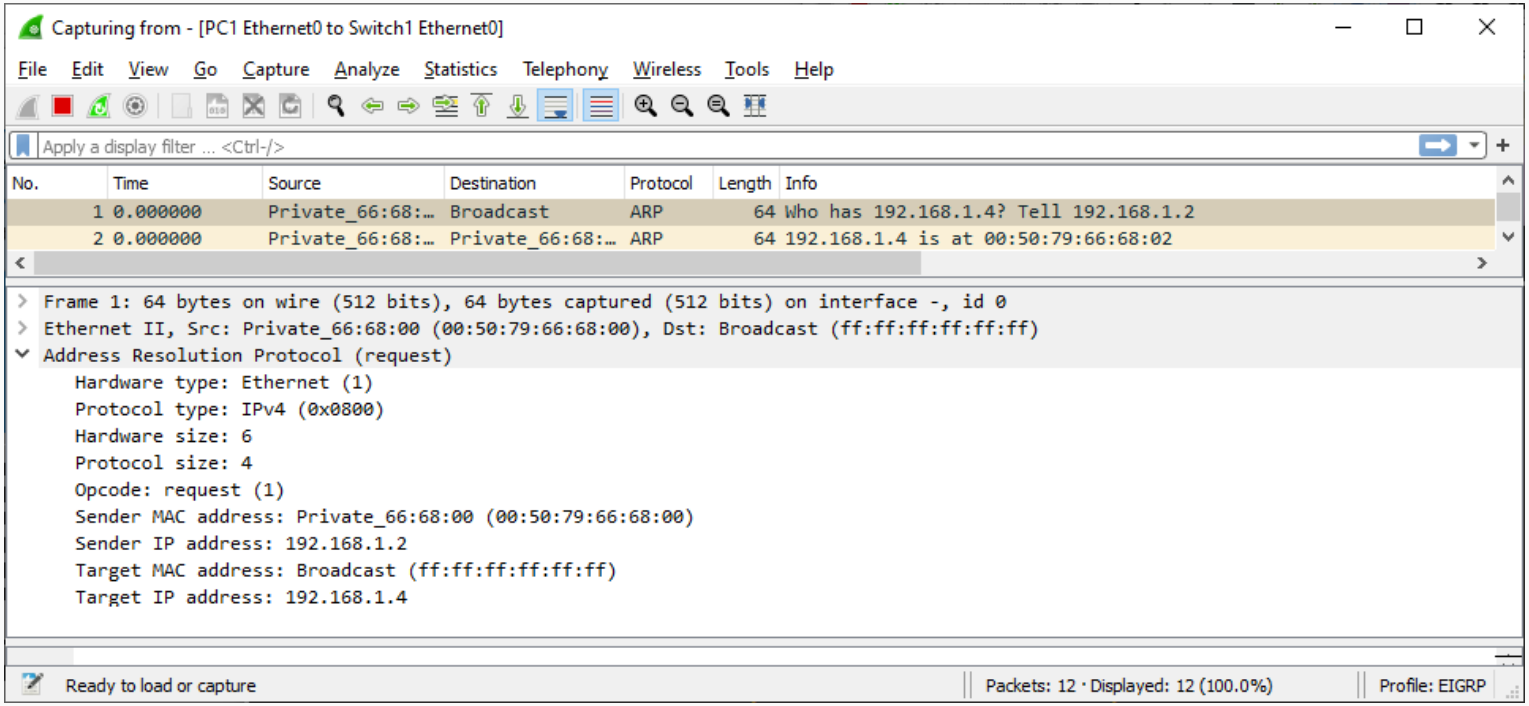


ARP - Procedimento

- PC1 deseja enviar dados para PC3



ARP - Demonstração




```
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
```

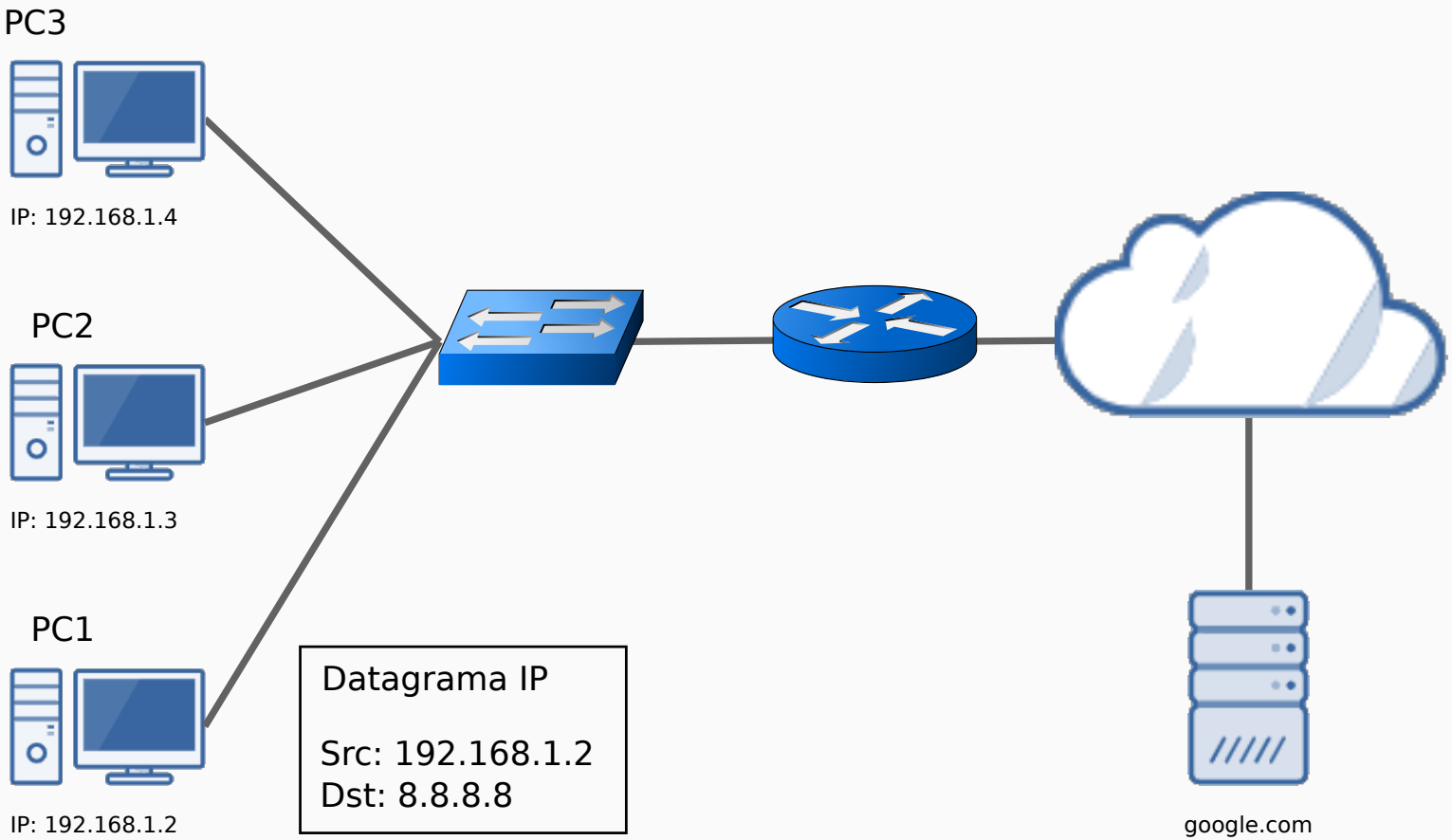
NAT

NAT - Introdução

- *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).

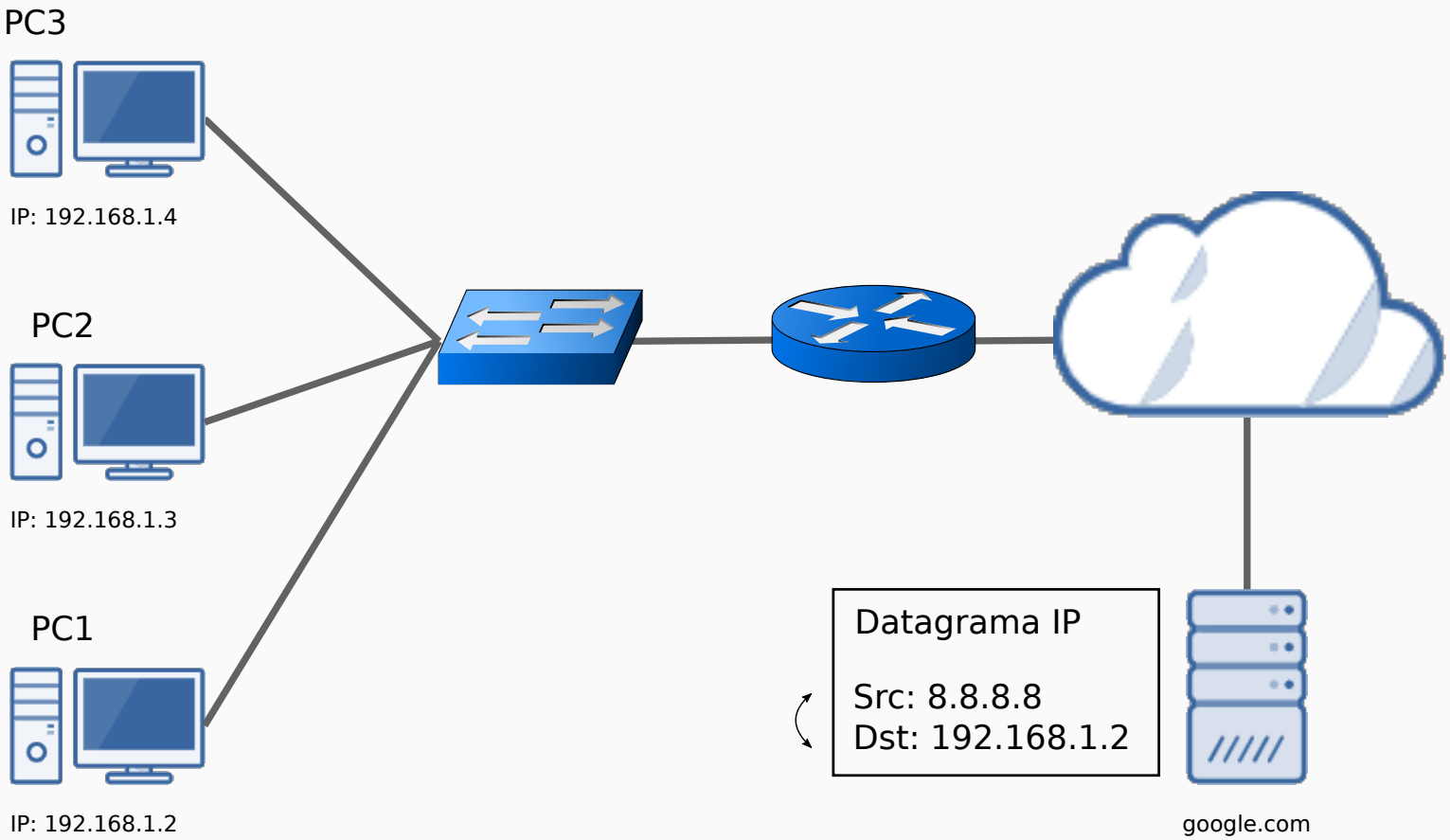
NAT - Descrição do Problema

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



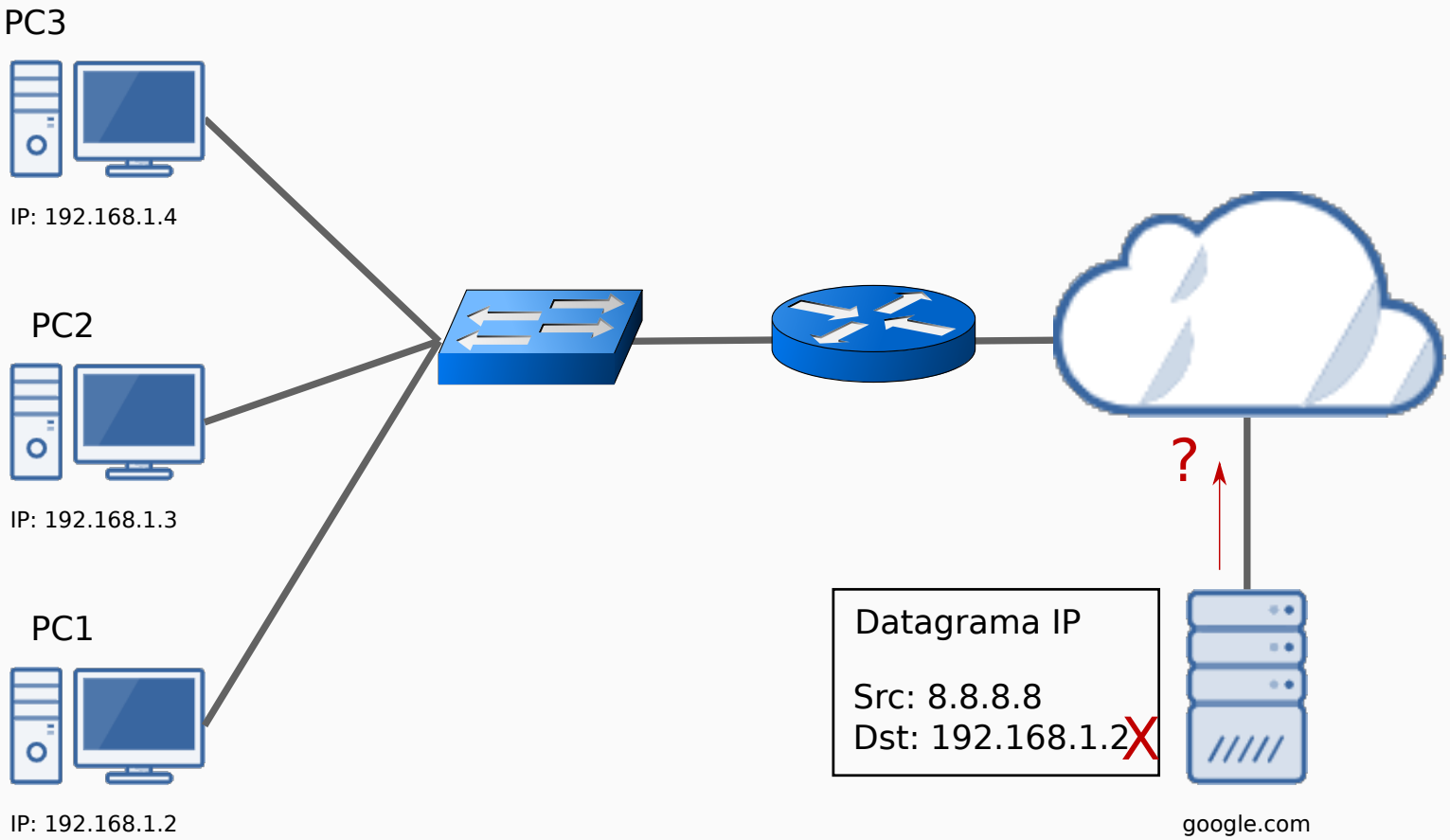
NAT - Descrição do Problema

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



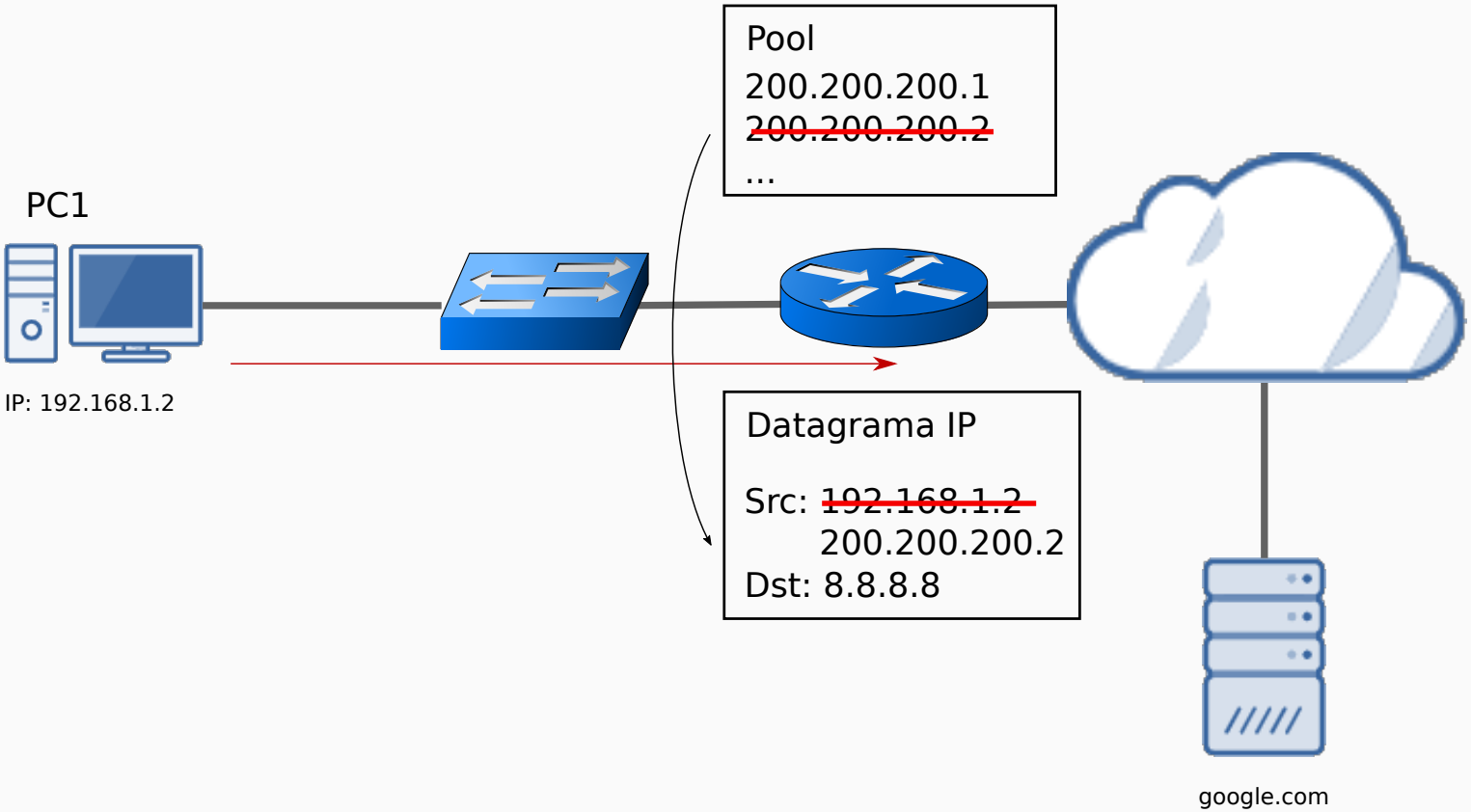
NAT - Descrição do Problema

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



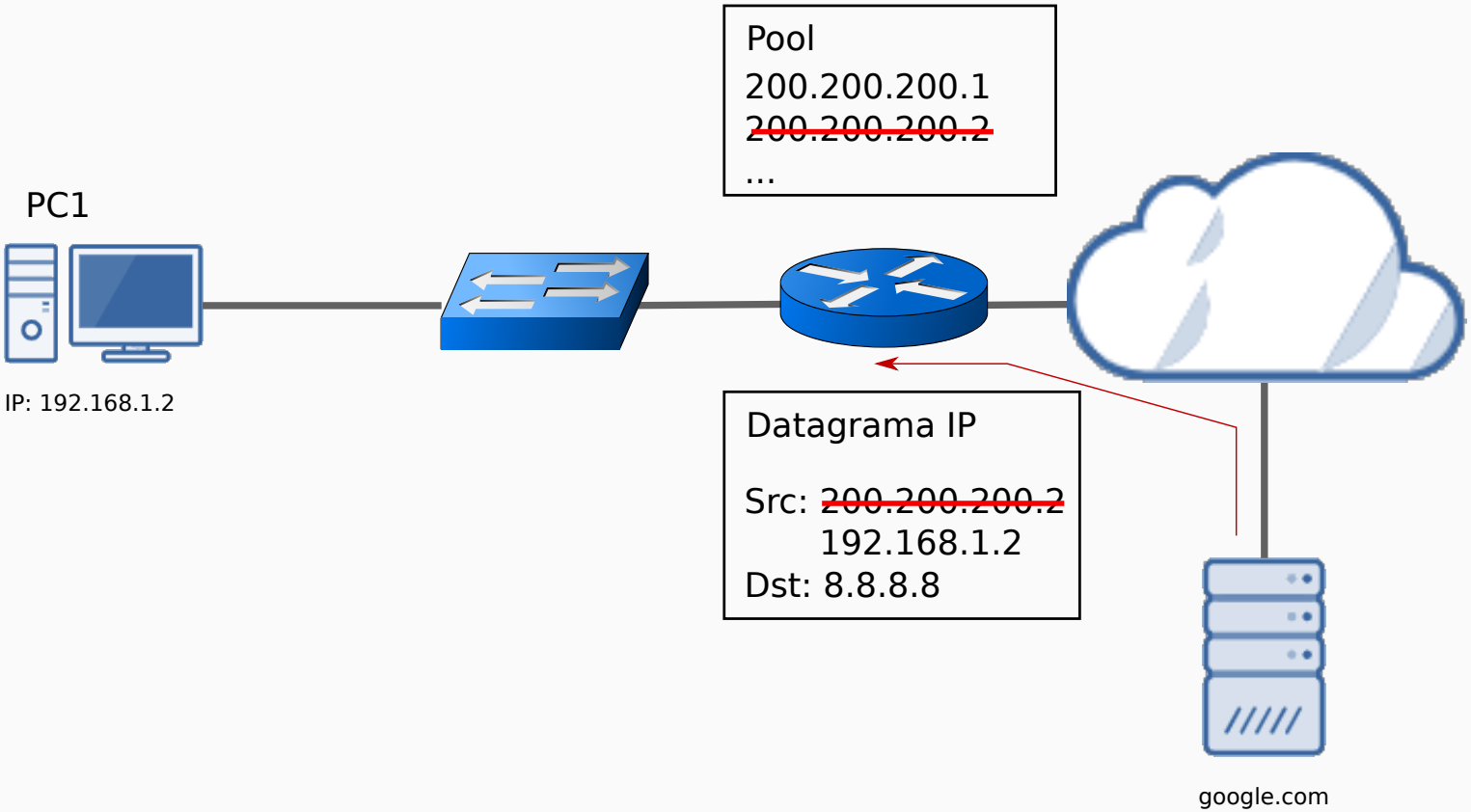
NAT - NAT Básico

- 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.

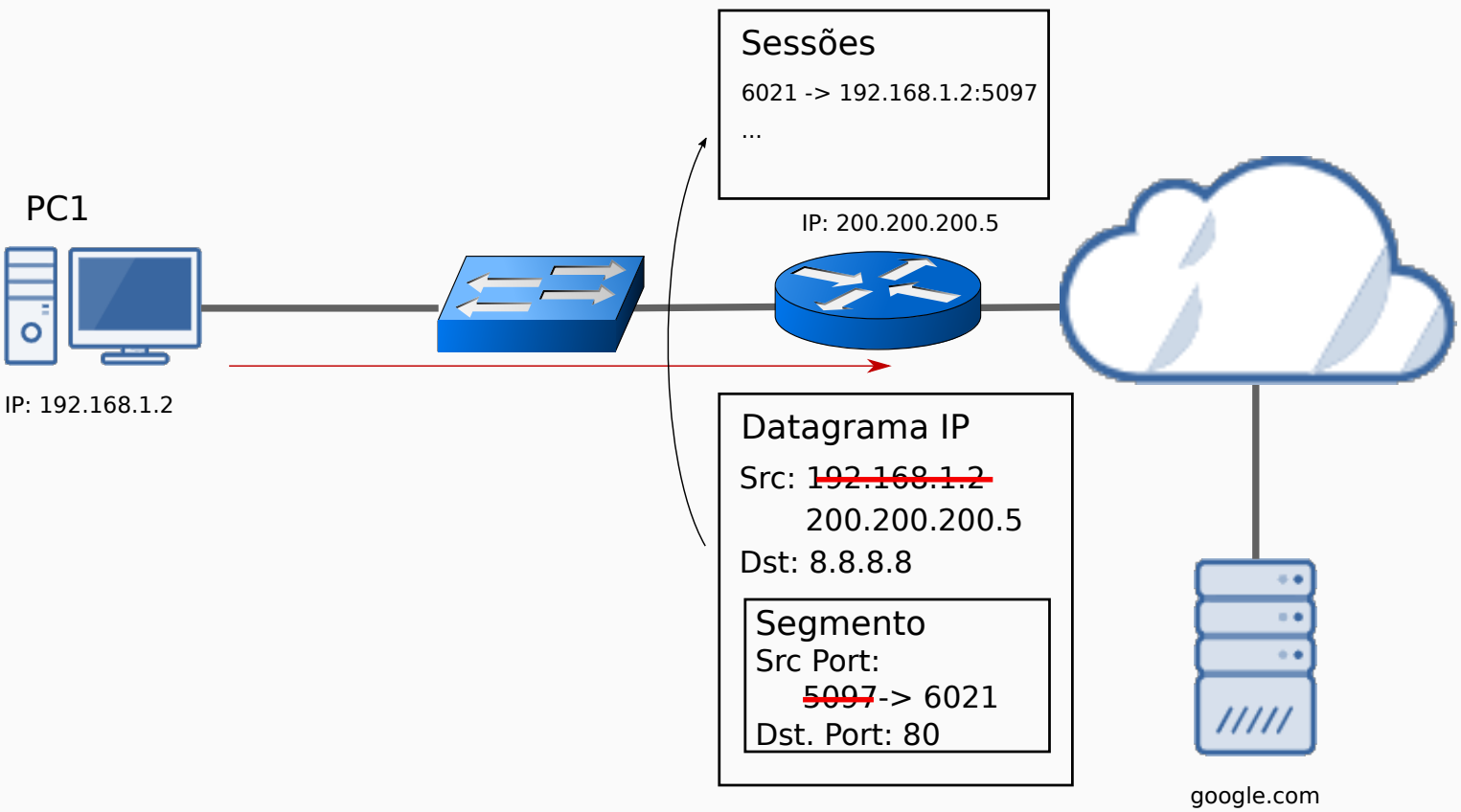


NAT - NAT Básico

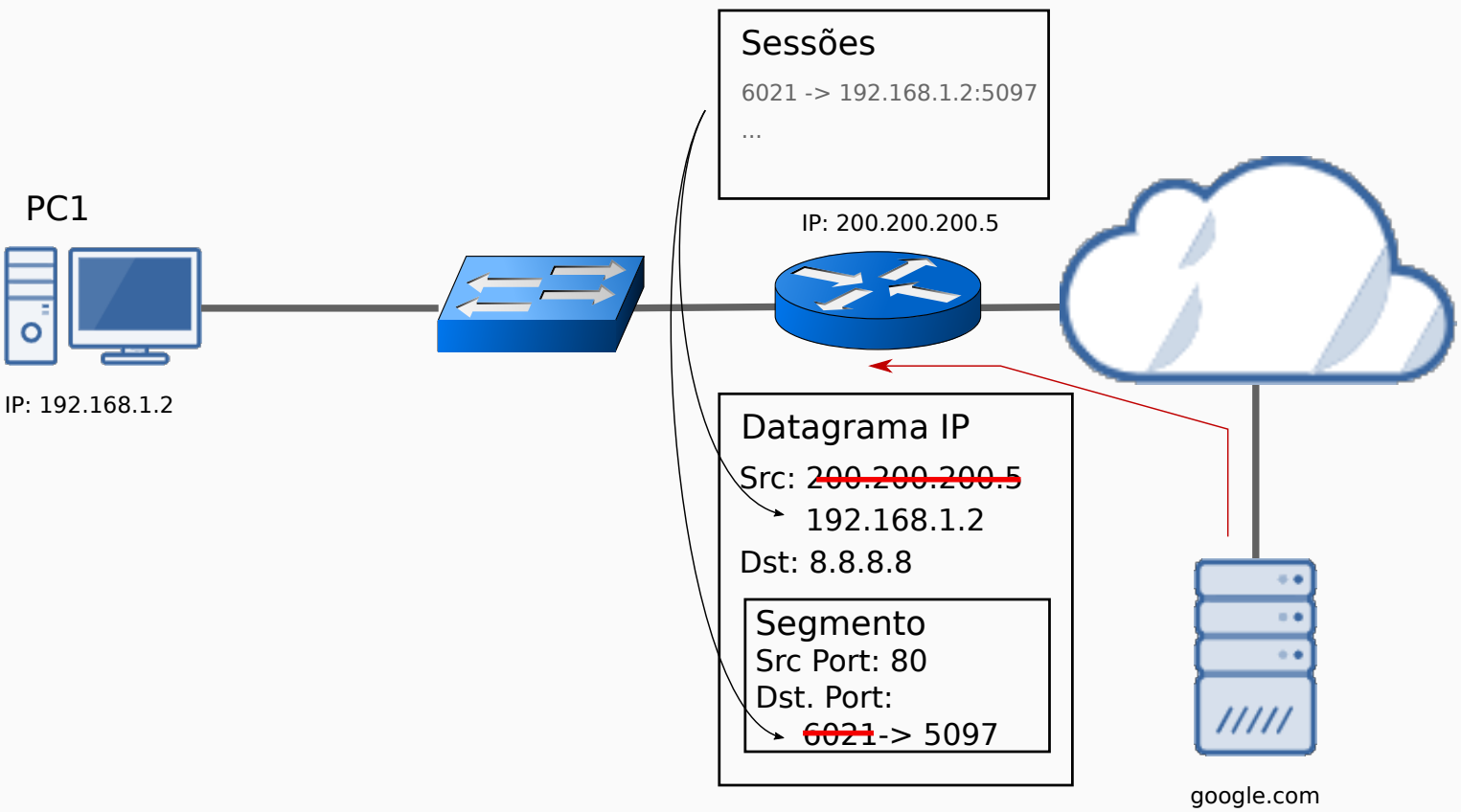
- Para pacotes enviados, o NAT traduz dinamicamente o endereço do remetente para um endereço global reservado.
- Para pacotes recebidos, o NAT traduz o endereço global para o endereço local correspondente.
- Os endereços globais são armazenados em um pool de endereços.



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



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



NAT - Limitações

- 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.

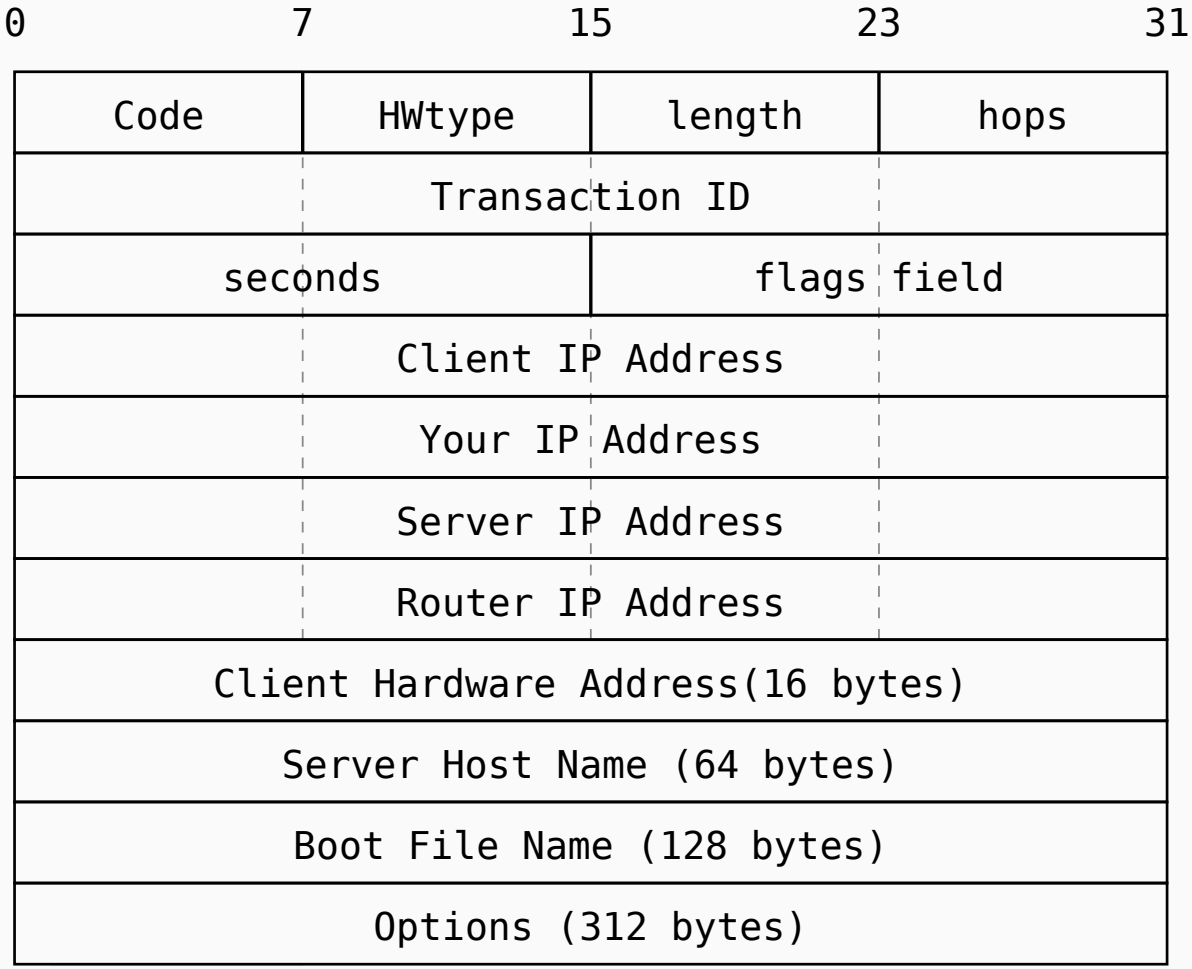
DHCP

DHCP - Introdução

- 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) inicalmente desenvolvido para o acesso a rede de terminais de computador diskless.
- Este mecanismo é bastante utilizado para servir equipamentos móveis, que recorrentemente 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.

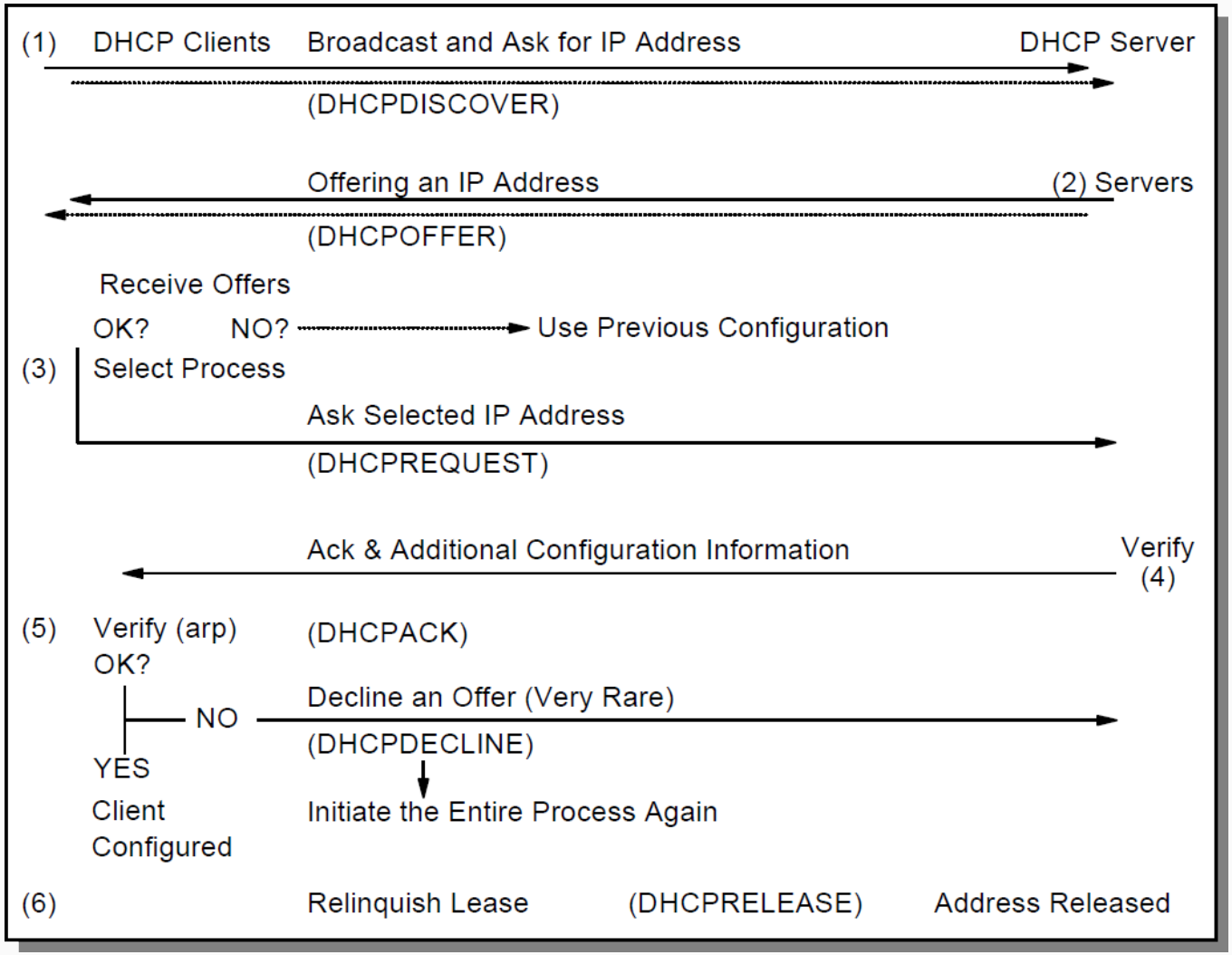
DHCP - Mensagem

- Confira subseção 3.7.1 do livro texto para mais detalhes.



DHCP - Tipos de Mensagem e Alocação de um Novo Endereço

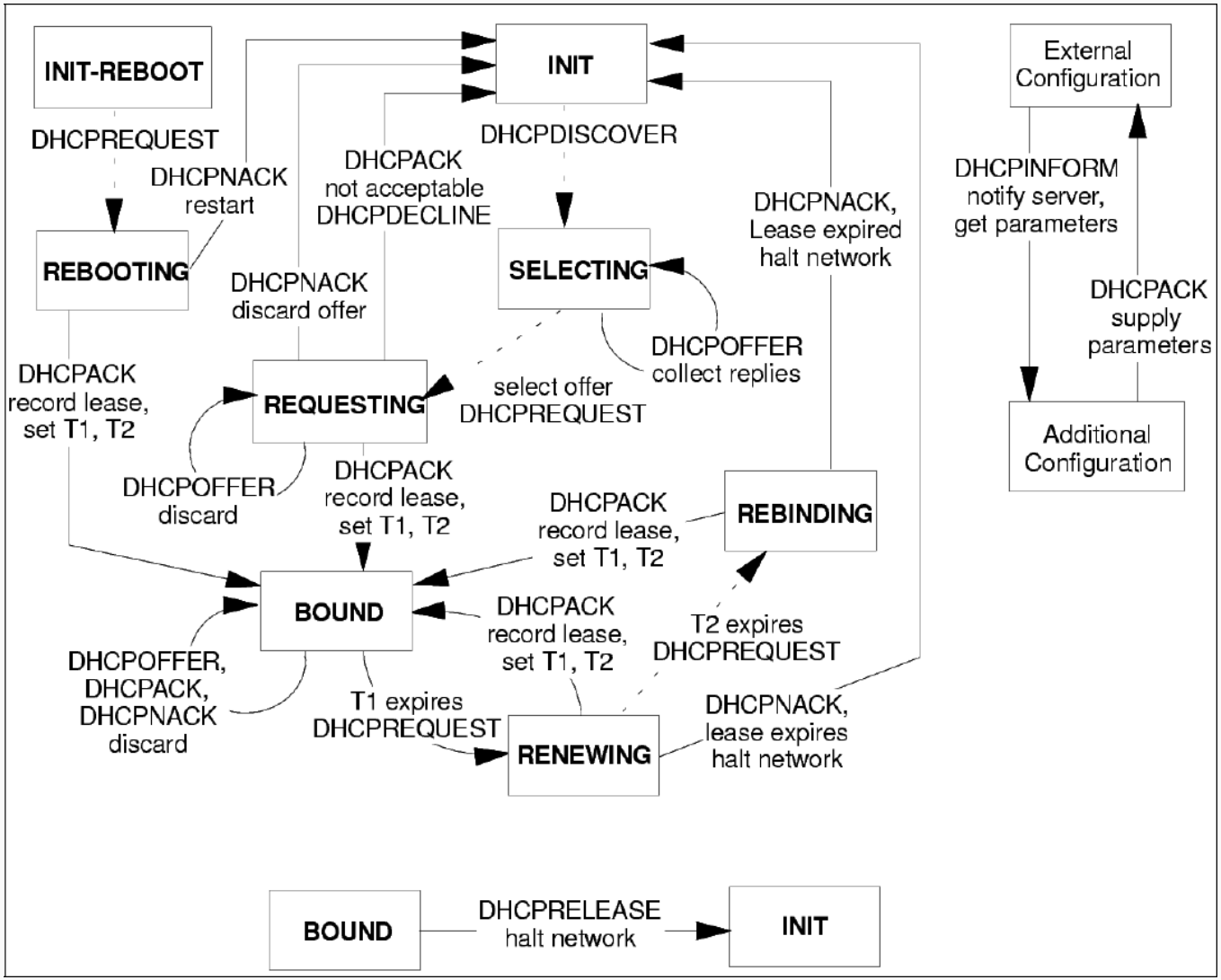
- Exemplo de alocação de um novo endereço.



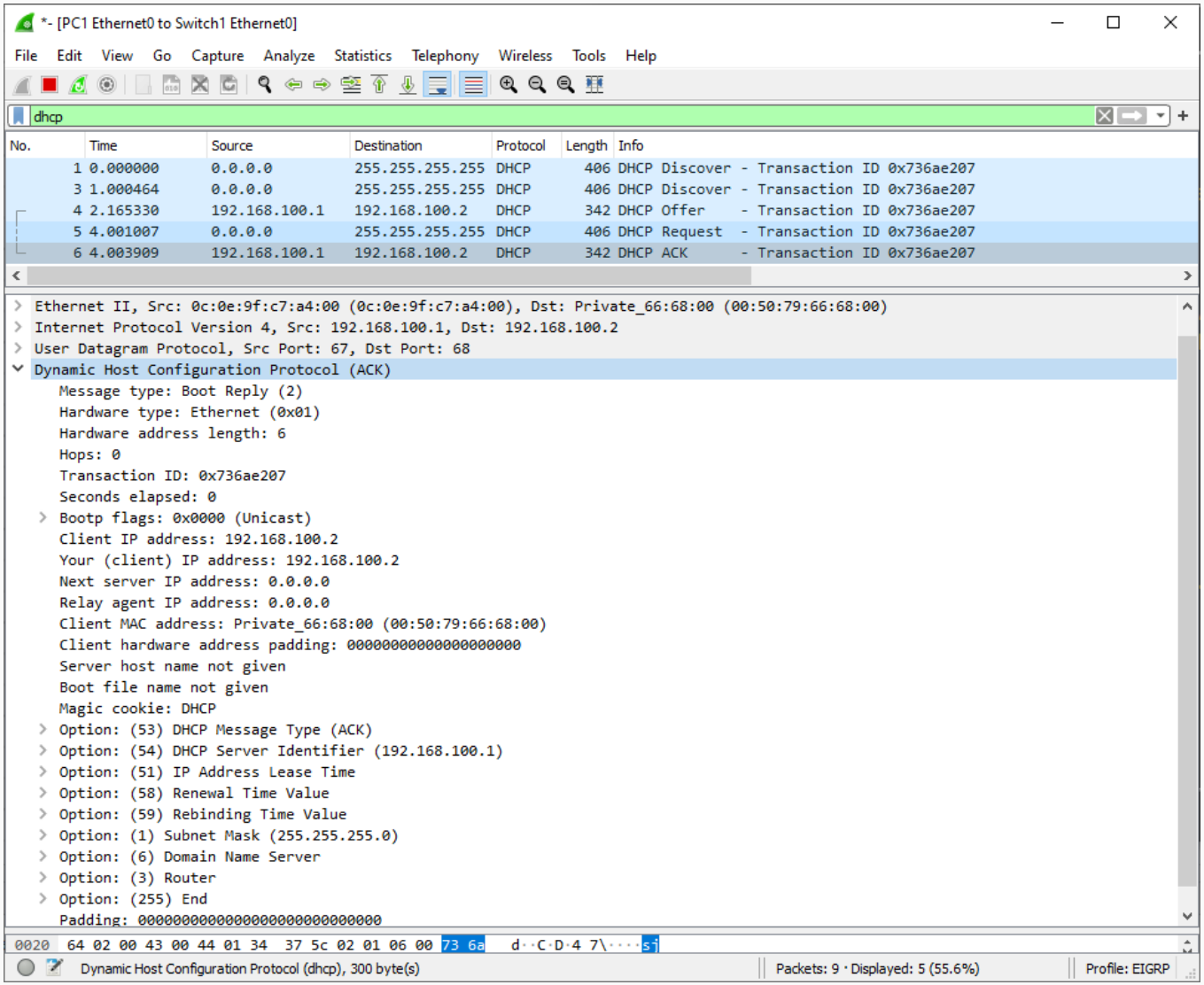
DHCP - Renovação da Concessão do DHCP

- 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



DHCP - Demonstração



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!