

Protocolo ARP



Prof. Dr. Bruno Rodrigues



Protocolo de resolução de endereços (ARP)



ARP: Address Resolution Protocol

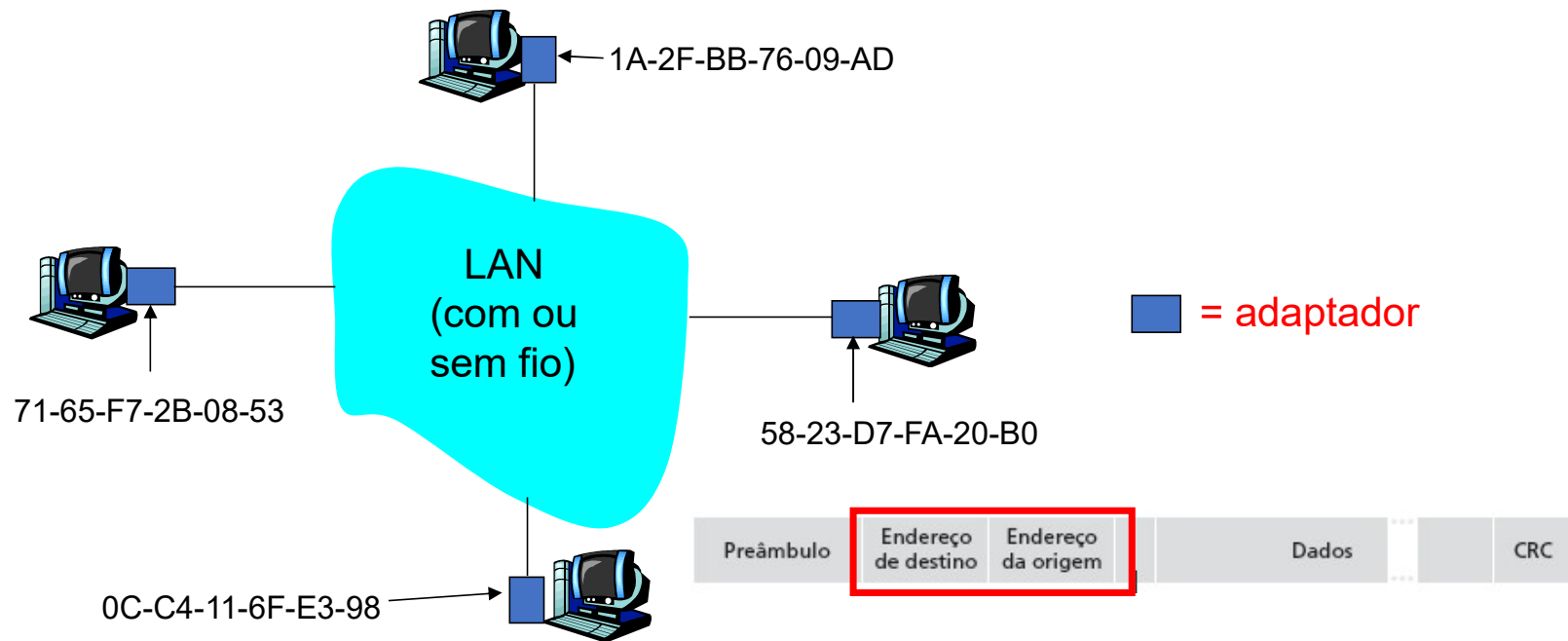
O protocolo ARP (Address Resolution Protocol) tem um papel fundamental entre os protocolos da camada Internet da suíte TCP/IP, porque permite conhecer o endereço físico de uma placa de rede que corresponde a um endereço IP.

Frame internet



ARP: Address Resolution Protocol

O protocolo ARP (Address Resolution Protocol) tem um papel fundamental entre os protocolos da camada Internet da suíte TCP/IP, porque permite conhecer o endereço físico de uma placa de rede que corresponde a um endereço IP.

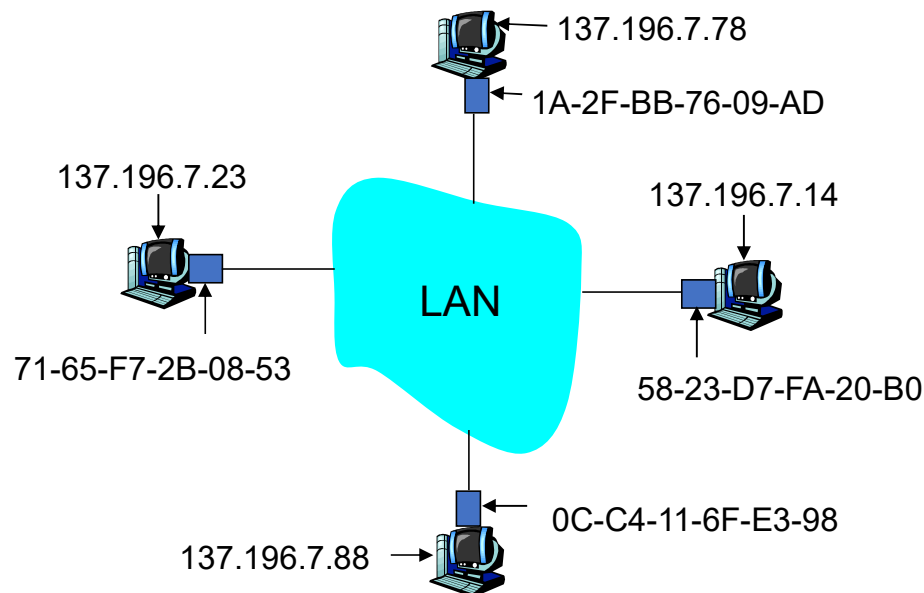


Consultas ARP



ARP: Address Resolution Protocol

Pergunta: Como determinar endereço MAC de B sabendo o endereço IP de B?



- Cada nó IP (hosp., roteador) na LAN tem tabela **ARP**
- Tabela ARP: mapeamentos de endereço IP/MAC para alguns nós da LAN

<endereço IP; endereço MAC; TTL>

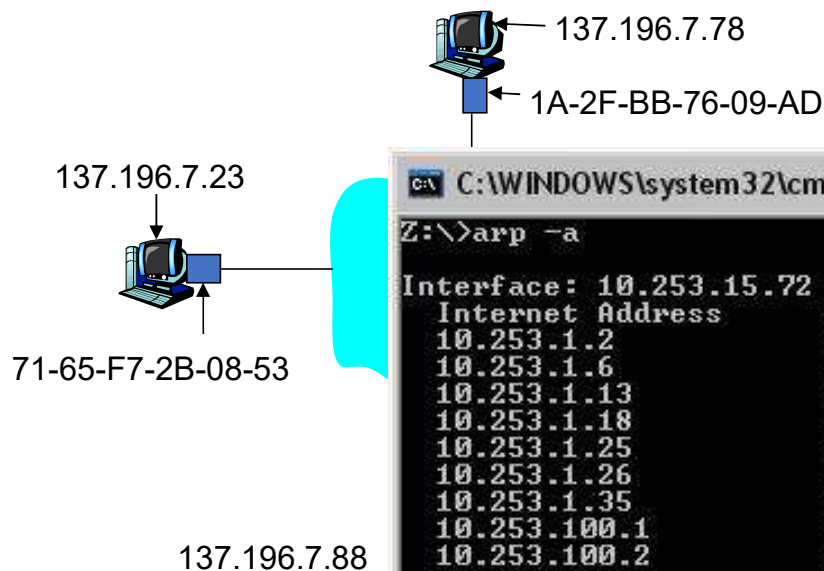
- TTL (Time To Live): tempo após o qual o mapeamento de endereço será esquecido (normalmente, 20 min)

ARP: Address Resolution Protocol

Pergunta: Como determinar endereço MAC de B sabendo o endereço IP de B?

- Cada nó IP (hosp., roteador) na LAN tem tabela **ARP**
- Tabela ARP: mapeamentos de endereço IP/MAC para alguns nós da LAN

<endereço IP; endereço MAC; TTL>

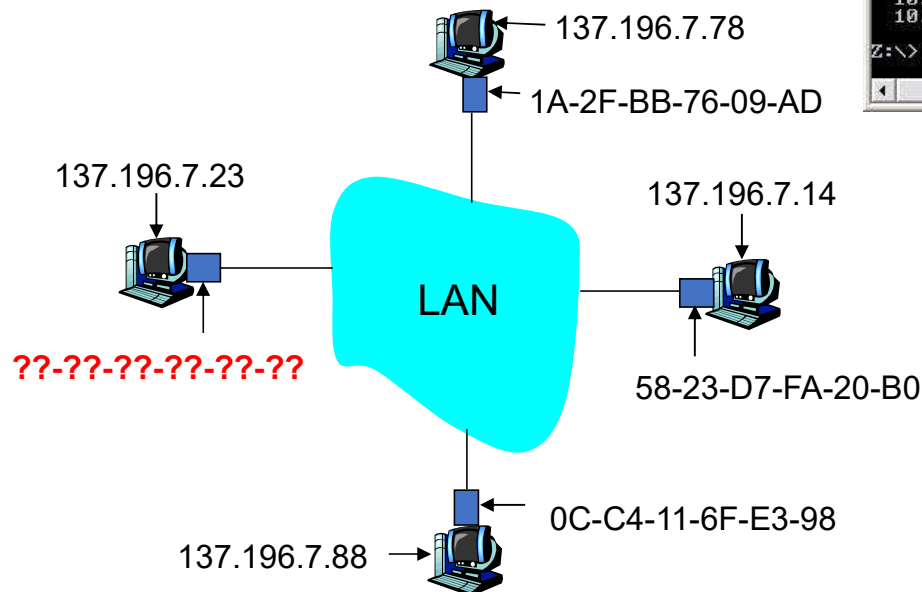


```
C:\WINDOWS\system32\cmd.exe
Z:\>arp -a

Interface: 10.253.15.72 --- 0x4
Internet Address      Physical Address      Type
10.253.1.2            00-12-3f-ed-3f-2c     dynamic
10.253.1.6            00-13-72-51-d5-a9     dynamic
10.253.1.13           00-03-ff-5b-f1-c8     dynamic
10.253.1.18           00-03-ff-36-9b-48     dynamic
10.253.1.25           00-11-43-de-91-15     dynamic
10.253.1.26           00-11-43-e7-97-fc     dynamic
10.253.1.35           00-14-22-17-c8-91     dynamic
10.253.100.1          00-15-2b-46-50-00     dynamic
10.253.100.2          00-09-0f-83-3b-8a     dynamic
```

ARP: Address Resolution Protocol

Pergunta: Como determinar endereço MAC de B sabendo o endereço IP de B?



```
C:\WINDOWS\system32\cmd.exe
Z:\>arp -a

Interface: 10.253.15.72 --- 0x4
Internet Address      Physical Address      Type
10.253.1.2            00-12-3f-ed-3f-2c    dynamic
10.253.1.6            00-13-72-51-d5-a9    dynamic
10.253.1.13           00-03-ff-5b-f1-c8    dynamic
10.253.1.18           00-03-ff-36-9b-48    dynamic
10.253.1.25           00-11-43-de-91-15    dynamic
10.253.1.26           00-11-43-e7-97-fc    dynamic
10.253.1.35           00-14-22-17-c8-91    dynamic
10.253.100.1          00-15-2b-46-50-00    dynamic
10.253.100.2          00-09-0f-83-3b-8a    dynamic
Z:\>
```

E quando não há o endereço MAC no ARP cache



Quem tem o IP 137.196.7.23

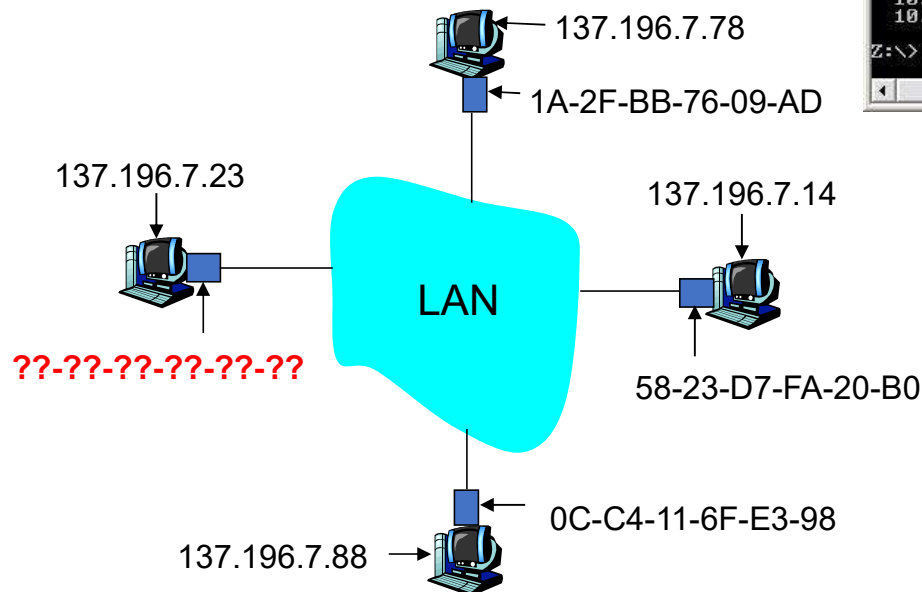
ARP: Address Resolution Protocol

Pergunta: Como determinar endereço MAC de B sabendo o endereço IP de B?

```
C:\WINDOWS\system32\cmd.exe
Z:\>arp -a

Interface: 10.253.15.72 --- 0x4
Internet Address      Physical Address      Type
10.253.1.2            00-12-3f-ed-3f-2c    dynamic
10.253.1.6            00-13-72-51-d5-a9    dynamic
10.253.1.13           00-03-ff-5b-f1-c8    dynamic
10.253.1.18           00-03-ff-36-9b-48    dynamic
10.253.1.25           00-11-43-de-91-15    dynamic
10.253.1.26           00-11-43-e7-97-fc    dynamic
10.253.1.35           00-14-22-17-c8-91    dynamic
10.253.100.1          00-15-2b-46-50-00    dynamic
10.253.100.2          00-09-0f-83-3b-8a    dynamic
Z:\>
```

E quando não há o endereço MAC no ARP cache



WHO HAS 137.196.7.23
Broadcast no enlace
FF-FF-FF-FF-FF-FF



ARP: Address Resolution Protocol

- **A** quer enviar datagrama a **B**, e endereço MAC de **B** não está na tabela ARP de **A**.
- A envia por **broadcast** pacote de consulta ARP, contendo endereço IP de **B**
 - ✓ Endereço MAC de destino = FF-FF-FF-FF-FF-FF
 - ✓ Todas as máquinas na LAN recebem consulta ARP
- **B** recebe pacote ARP, responde para A com seu endereço MAC (de B)
 - ✓ Quadro enviado ao endereço MAC de A (unicast)
- A salva em cache par de endereços IP-para-MAC em sua tabela ARP até a informação expirar

ARP: Address Resolution Protocol

Formato do protocolo ARP

Hardware Type		Protocol Type
Hardware length	Protocol length	Operation Request 1, Reply 2
Sender hardware address (For example, 6 bytes for Ethernet)		
Sender protocol address (For example, 4 bytes for IP)		
Target hardware address (For example, 6 bytes for Ethernet) (It is not filled in a request)		
Target protocol address (For example, 4 bytes for IP)		

ARP: Address Resolution Protocol

arp-storm (2).pcap

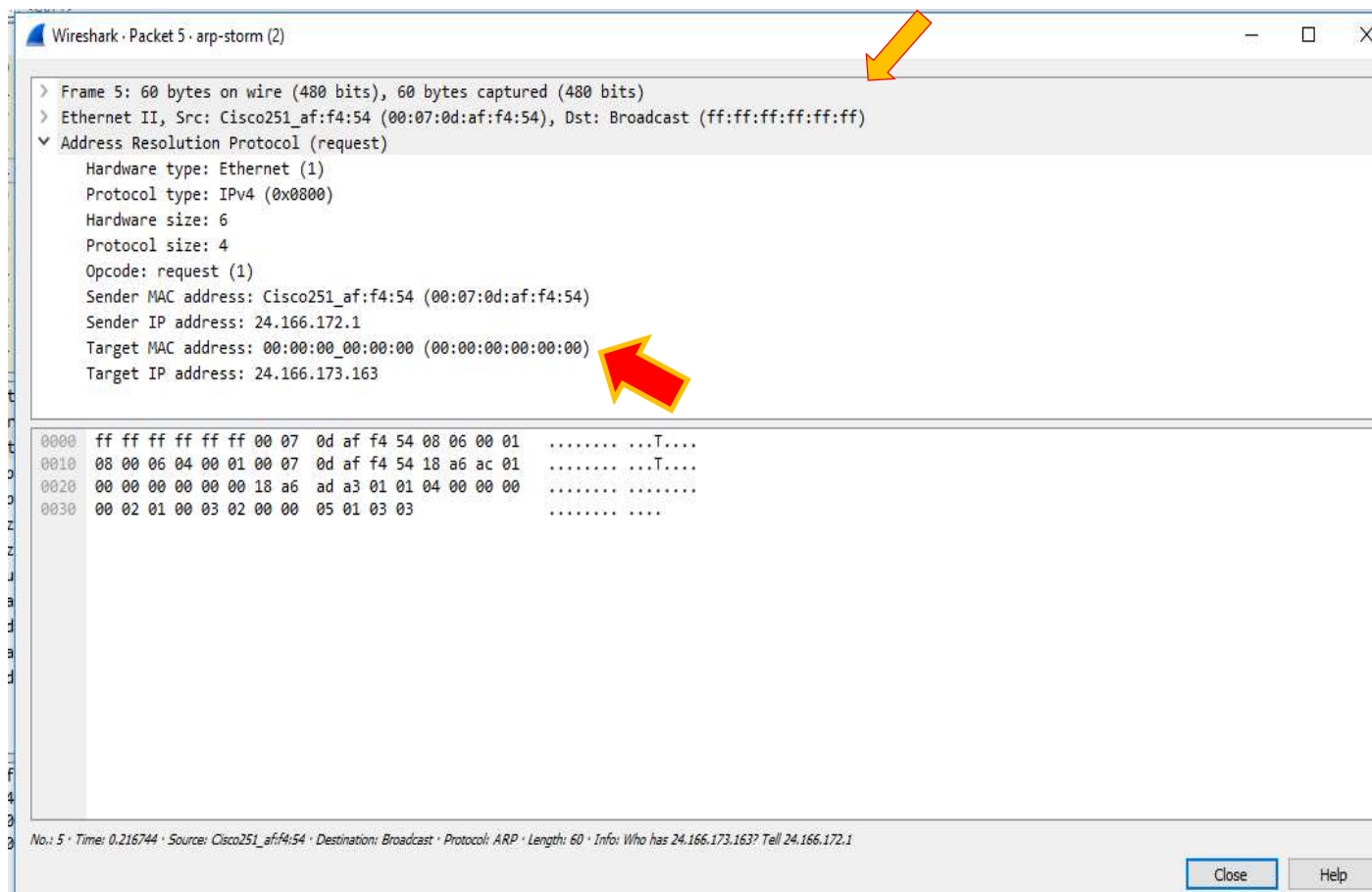
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	Cisco251_af:f4:...	Broadcast	ARP	60	Who has 24.166.173.159? Tell 24.166.172.1
2	0.098594	Cisco251_af:f4:...	Broadcast	ARP	60	Who has 24.166.172.141? Tell 24.166.172.1
3	0.110617	Cisco251_af:f4:...	Broadcast	ARP	60	Who has 24.166.173.161? Tell 24.166.172.1
4	0.211791	Cisco251_af:f4:...	Broadcast	ARP	60	Who has 65.28.78.76? Tell 65.28.78.1
5	0.216744	Cisco251_af:f4:...	Broadcast	ARP	60	Who has 24.166.173.163? Tell 24.166.172.1
6	0.307909	Cisco251_af:f4:...	Broadcast	ARP	60	Who has 24.166.175.123? Tell 24.166.172.1
7	0.330433	Cisco251_af:f4:...	Broadcast	ARP	60	Who has 24.166.173.165? Tell 24.166.172.1
8	0.408556	Cisco251_af:f4:...	Broadcast	ARP	60	Who has 24.166.175.82? Tell 24.166.172.1
9	0.455104	Cisco251_af:f4:...	Broadcast	ARP	60	Who has 69.76.220.131? Tell 69.76.216.1
10	0.486666	Cisco251_af:f4:...	Broadcast	ARP	60	Who has 24.166.173.168? Tell 24.166.172.1
11	0.504694	Cisco251_af:f4:...	Broadcast	ARP	60	Who has 69.76.221.27? Tell 69.76.216.1
12	0.510684	Cisco251_af:f4:...	Broadcast	ARP	60	Who has 24.166.174.184? Tell 24.166.172.1

ARP: Address Resolution Protocol

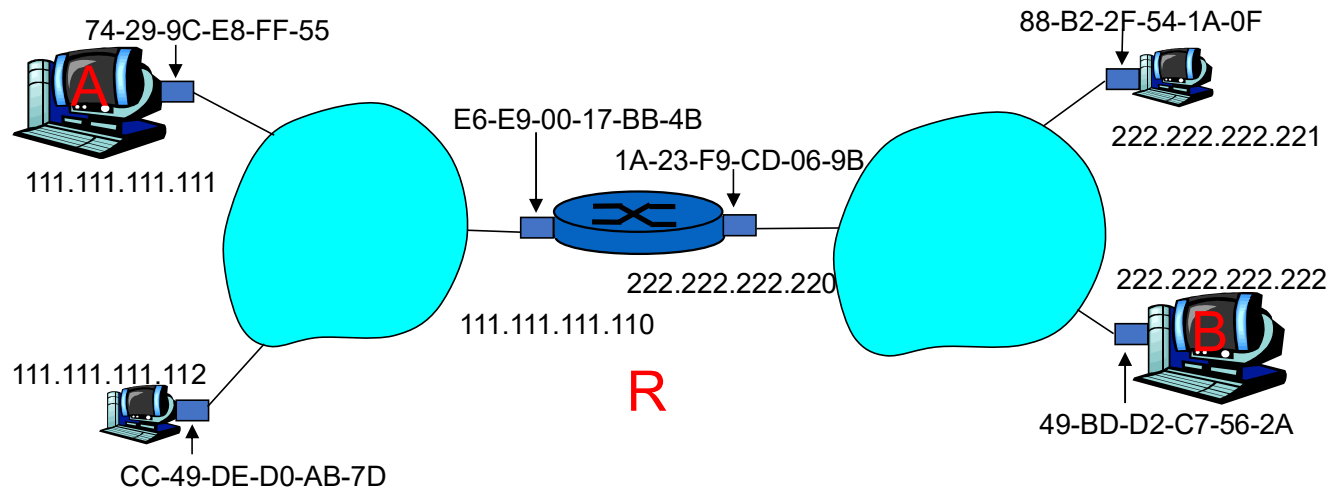
Requisição do protocolo ARP





ARP: Address Resolution Protocol

Acompanhamento: enviar datagrama de A para B via R
suponha que A saiba o endereço IP de B

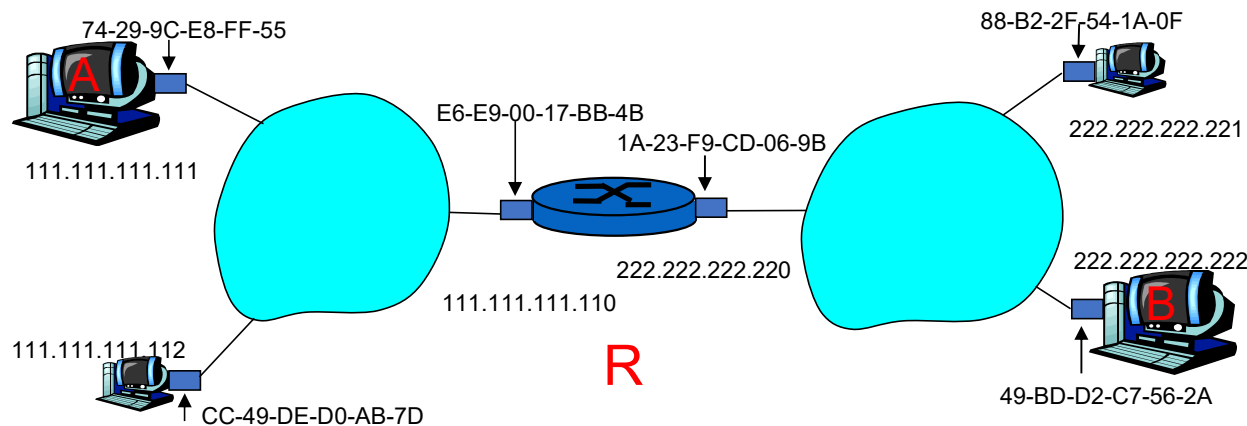


- Duas tabelas ARP no roteador R, uma para cada rede IP (LAN)

ARP: Address Resolution Protocol

- A cria datagrama IP com origem A, destino B
- A usa ARP para obter endereço MAC de R para **111.111.111.110**
- A cria quadro da camada de enlace com endereço MAC de R como destino, quadro contém datagrama IP A-para-B
- NIC de A envia quadro
- NIC de R recebe quadro
- R remove datagrama IP do quadro Ethernet, vê o seu destino a B
- R usa ARP para obter endereço MAC de B
- R cria quadro contendo datagrama IP A-para-B e envia para B

Este é um exemplo realmente importante – procure entender bem!

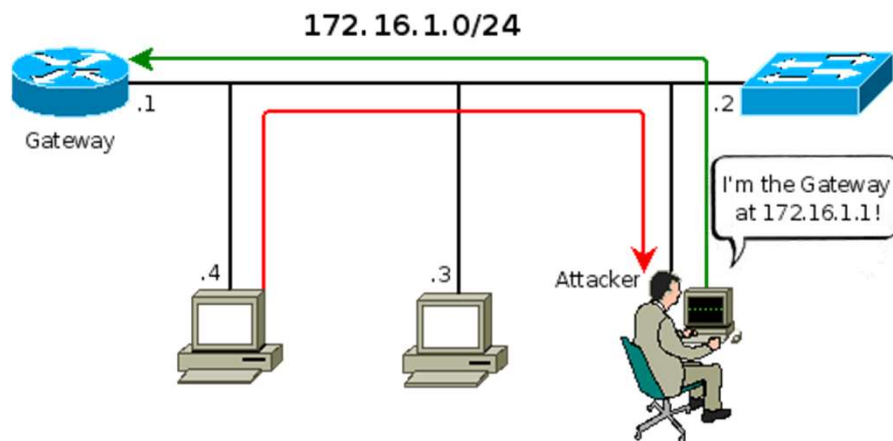




ARP: Address Resolution Protocol

ARP SPOOFING

O ataque ocorre quando o “**elemento mal intencionado**” recebe esta solicitação (broadcast) e responde como seu MAC address. Desta forma passamos a ter o “homem do meio”, que pode copiar todo o tráfego para sua máquina ou até parar a rede.





Obrigado!



Referências :

Camada de Enlace
Redes locais comutadas
Capítulo 5 - Páginas de 342 à 343



