

02 - Prati-Protocolo ARP

Davi Ventura Cardoso Perdigão - 82148

1. Use o comando “arp -a” (na linha de comando) para trabalhar com o cache ARP. Verifique quais são os endereços que estão no cache de cada PC e identifique o endereço físico ou MAC de cada um por meio do comando ipconfig /all.

```
C:\Users\davi.perdigao>arp -a

Interface: 20.103.0.79 --- 0x3

Endereço IP      Endereço físico    Tipo
20.103.0.7       b8-af-67-9b-1f-00  dinâmico
20.103.0.8       b8-af-67-54-c8-a8  dinâmico
20.103.0.13      1c-39-47-5e-65-26  dinâmico
20.103.0.24      b8-ca-3a-fe-e9-59  dinâmico
20.103.0.42      84-2b-2b-7c-f8-e8  dinâmico
20.103.0.69      20-47-47-75-51-a6  dinâmico
20.103.0.254     00-0c-42-c0-2b-da  dinâmico
20.103.0.255     ff-ff-ff-ff-ff-ff  estático
224.0.0.22       01-00-5e-00-00-16  estático
224.0.0.251      01-00-5e-00-00-fb  estático
224.0.0.252      01-00-5e-00-00-fc  estático
239.255.255.250  01-00-5e-7f-ff-fa  estático
239.255.255.253  01-00-5e-7f-ff-fd  estático
255.255.255.255  ff-ff-ff-ff-ff-ff  estático
```

```
C:\Users\davi.perdigao>ipconfig/all

Configuração de IP do Windows

Nome do host. . . . . : GPA-TI-13
Sufixo DNS primário . . . . . : interno.grupoalfa.local
Tipo de nó. . . . . : híbrido
Roteamento de IP ativado. . . . . : não
Proxy WINS ativado. . . . . : não
Lista de pesquisa de sufixo DNS . . . . . : interno.grupoalfa.local

Adaptador Ethernet Ethernet:

Estado da mídia. . . . . : mídia desconectada
Sufixo DNS específico de conexão. . . . . : interno.grupoalfa.local
Descrição . . . . . : Realtek PCIe FE Family Controller
Endereço Físico . . . . . : 54-BF-64-F4-DC-A2
DHCP Habilitado . . . . . : Sim
Configuração Automática Habilitada. . . . . : Sim

Adaptador desconhecido OpenVPN Wintun:

Estado da mídia. . . . . : mídia desconectada
Sufixo DNS específico de conexão. . . . . :
Descrição . . . . . : Wintun Userspace Tunnel
Endereço Físico . . . . . :
DHCP Habilitado . . . . . : Não
Configuração Automática Habilitada. . . . . : Sim

Adaptador Ethernet Ethernet 2:

Sufixo DNS específico de conexão. . . . . :
Descrição . . . . . : TP-LINK Gigabit Ethernet USB Adapter
Endereço Físico . . . . . : 1C-61-B4-D8-07-A3
DHCP Habilitado . . . . . : Sim
Configuração Automática Habilitada. . . . . : Sim
Endereço IPv6 de link local . . . . . : fe80::9530:f3c6:1413:3e0c%3(Preferencial)
Endereço IPv4. . . . . : 20.103.0.79(Preferencial)
Máscara de Sub-rede . . . . . : 255.255.255.0
Concessão Obtida. . . . . : quarta-feira, 22 de março de 2023 19:11:31
Concessão Expira. . . . . : sábado, 25 de março de 2023 19:11:31
Gateway Padrão. . . . . : 20.103.0.254
Servidor DHCP . . . . . : 20.103.0.254
IAID de DHCPv6. . . . . : 941384116
DUID de Cliente DHCPv6. . . . . : 00-01-00-01-2B-35-02-00-54-BF-64-F4-DC-A2
Servidores DNS. . . . . : 177.52.96.3
                          177.52.96.4
NetBIOS em Tcpip. . . . . : Habilitado
```

2. Execute o “ping -t 200.131.3.3” para o endereço ip 200.131.3.5. Verifique a tabela arp por meio do comando arp -a em cada máquina. Verifique os pacotes ARP capturados. Verifique quais são os endereços MAC. Pacotes ICMP's estão sendo capturados?

[illegible]

```
C:\Users\davi.perdigao>ping -t 200.131.3.3, 200.131.3.5
A solicitação ping não pôde encontrar o host 200.131.3.3,. Verifique o nome e tente novamente.
```

```
C:\Users\davi.perdigao>arp -a

Interface: 20.103.0.79 --- 0x3

    Endereço IP           Endereço físico          Tipo
    20.103.0.7            b8-af-67-9b-1f-00      dinâmico
    20.103.0.8            b8-af-67-54-c8-a8      dinâmico
    20.103.0.13           1c-39-47-5e-65-26      dinâmico
    20.103.0.24           b8-ca-3a-fe-e9-59      dinâmico
    20.103.0.42           84-2b-2b-7c-f8-e8      dinâmico
    20.103.0.69           20-47-47-75-51-a6      dinâmico
    20.103.0.254          00-0c-42-c0-2b-da      dinâmico
    20.103.0.255          ff-ff-ff-ff-ff-ff      estático
    224.0.0.22            01-00-5e-00-00-16      estático
    224.0.0.251           01-00-5e-00-00-fb      estático
    224.0.0.252           01-00-5e-00-00-fc      estático
    239.255.255.250       01-00-5e-7f-ff-fa      estático
    239.255.255.253       01-00-5e-7f-ff-fd      estático
    255.255.255.255       ff-ff-ff-ff-ff-ff      estático
```

3. Repita os mesmos procedimentos. Foram capturados pacotes agora (ICMP e ARP)? Por quê?

```
Adaptador Ethernet Ethernet 2:

Sufixo DNS específico de conexão. . . . . :
Descrição . . . . . : TP-LINK Gigabit Ethernet USB Adapter
Endereço Físico . . . . . : 1C-61-B4-DB-D7-A3
DHCP Habilitado . . . . . : Sim
Configuração Automática Habilitada. . . . . : Sim
Endereço IPv6 de link local . . . . . : fe80::9530:f3c6:1413:3e0c%3(Preferencial)
Endereço IPv4. . . . . : 20.103.0.79(Preferencial)
Máscara de Sub-rede . . . . . : 255.255.255.0
Concessão Obtida. . . . . : quarta-feira, 22 de março de 2023 19:11:31
Concessão Expira. . . . . : sábado, 25 de março de 2023 19:11:31
Gateway Padrão. . . . . : 20.103.0.254
Servidor DHCP . . . . . : 20.103.0.254
IAID de DHCPv6. . . . . : 941384116
DUID de Cliente DHCPv6. . . . . : 00-01-00-01-2B-35-02-0D-54-BF-64-F4-DC-A2
Servidores DNS. . . . . : 177.52.96.3
                          177.52.96.4
NetBIOS em Tcpip. . . . . : Habilitado
```

Os pacotes foram capturados pois, ao dar um “ping” ele conseguiu trafegar pela rota, trazendo esses pacotes consigo.

[illegible]

4. Remove entradas da tabela ARP com o comando “arp -d”. Execute esse comando. Agora os pacotes ARP foram capturados? Por quê?

```
C:\Windows\system32>arp -a

Interface: 20.103.0.79 --- 0x3

Endereço IP      Endereço físico    Tipo
20.103.0.7        b8-af-67-9b-1f-00  dinâmico
20.103.0.8        b8-af-67-54-c8-a8  dinâmico
20.103.0.13       1c-39-47-5e-65-26  dinâmico
20.103.0.24       b8-ca-3a-fe-e9-59  dinâmico
20.103.0.42       84-2b-2b-7c-f8-e8  dinâmico
20.103.0.69       20-47-47-75-51-a6  dinâmico
20.103.0.254      00-0c-42-c0-2b-da  dinâmico
20.103.0.255      ff-ff-ff-ff-ff-ff  estático
224.0.0.22        01-00-5e-00-00-16  estático
224.0.0.251       01-00-5e-00-00-fb  estático
224.0.0.252       01-00-5e-00-00-fc  estático
239.255.255.250   01-00-5e-7f-ff-fa  estático
239.255.255.253   01-00-5e-7f-ff-fd  estático
255.255.255.255   ff-ff-ff-ff-ff-ff  estático

C:\Windows\system32>arp -d 20.103.0.13

C:\Windows\system32>arp -a

Interface: 20.103.0.79 --- 0x3

Endereço IP      Endereço físico    Tipo
20.103.0.7        b8-af-67-9b-1f-00  dinâmico
20.103.0.8        b8-af-67-54-c8-a8  dinâmico
20.103.0.24       b8-ca-3a-fe-e9-59  dinâmico
20.103.0.42       84-2b-2b-7c-f8-e8  dinâmico
20.103.0.69       20-47-47-75-51-a6  dinâmico
20.103.0.254      00-0c-42-c0-2b-da  dinâmico
20.103.0.255      ff-ff-ff-ff-ff-ff  estático
224.0.0.22        01-00-5e-00-00-16  estático
224.0.0.251       01-00-5e-00-00-fb  estático
224.0.0.252       01-00-5e-00-00-fc  estático
239.255.255.250   01-00-5e-7f-ff-fa  estático
239.255.255.253   01-00-5e-7f-ff-fd  estático
255.255.255.255   ff-ff-ff-ff-ff-ff  estático
```

Eles foram capturados pois, como acabará de ser trafegado pela rota, ele consegue capturar esses pacotes.