

Comando arp

Comando ARP – O ARP (Address Resolution Protocol) estabelece uma ligação entre o endereço físico (MAC Address) da placa de rede e o endereço lógico (Endereço IP). A placa de rede de um computador contém uma tabela onde faz a ligação entre os endereços físicos e lógicos dos computadores presentes na rede.

Quando um computador quer comunicar com o outro, vai verificar nessa tabela se o computador está presente na rede. Se estiver, envia os dados e o tráfego na rede é diminuído, caso contrário envia um sinal designado por pedido ARP para determinar o seu endereço.

Como funciona o protocolo ARP?

Vamos supor que tem uma máquina com o IP 192.168.1.69 e quer se conectar à máquina 192.168.1.3. A sua máquina, primeiro irá verificar se a máquina com o IP 192.168.1.3 está na mesma rede, se se confirmar ele pode conversar diretamente via Ethernet. Então ele irá procurar 192.168.1.3 na sua tabela ARP, para ver se este endereço já é conhecido. Caso seja conhecido, o sistema irá adicionar um cabeçalho Ethernet, e enviar o pacote. Mas vamos supor que esta máquina não esteja na tabela ARP. Sendo assim não há como enviar o pacote, porque você precisa do endereço físico. Então o seu sistema usa o protocolo ARP para enviar uma requisição ARP. Basicamente uma requisição ARP diz 'Eu preciso o endereço físico para o IP 192.168.1.3.

Todas as máquinas escutam as requisições ARP. Quando uma máquina vê uma requisição ARP para ele mesmo, ele é requisitado a responder. Então 192.168.1.3 verá a requisição e responderá com uma resposta ARP dizendo como resultado para o IP 192.168.1.3 é D0-67-E5-40-B5-3F. Tenha em conta que o resultado obtido é o endereço físico (MAC Address).

A sua máquina irá salvar esta informação na sua tabela ARP, então os futuros pacotes para esse mesmo endereço poderão ir diretamente. Muitos sistemas tratam a tabela ARP como uma cache, e limpam suas entradas se estas não forem usadas em um determinado período de tempo. Existe uma cache ARP em separado para cada placa de rede.

UTILIZANDO O COMANDO ARP:

É possível verificar a cache ARP através do comando arp. Para visualizar a cache ARP, escreva arp -a numa linha de comandos.

C:\arp -a

Interface: 10.3.2.235 --- 0x9

Endereço IP	Endereço físico	Tipo
10.3.0.2	58-49-3b-50-81-00	dinâmico
10.3.0.10	58-49-3b-50-81-10	dinâmico
10.3.0.16	00-0c-29-c2-72-08	dinâmico
10.3.7.255	ff-ff-ff-ff-ff-ff	estático
224.0.0.2	01-00-5e-00-00-02	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
255.255.255.255	ff-ff-ff-ff-ff-ff	estático

Comando ARP

Para verificar as opções da linha de comandos para o comando ARP, escreva `arp /?` na linha de comandos.

Opções para o comando ARP:

-a : Mostra todas as entradas ARP correntes lidas da tabela de um arquivo `kmem` baseada no arquivo núcleo do `unix`

-d : Apaga uma entrada para o host chamado. Esta opção só poder ser usado pelo super usuário

-f : Le o arquivo chamado `filename` e marca diversas entradas na tabela ARP

-s : Criar uma entrada ARP para o host chamado `hostname` com o endereço físico. O endereço físico (MAC Address) é mostrado com 6 bytes hexadecimais separados por pontos.

Exemplos de execução para o comando ARP:

- Mostra o endereço físico e o endereço lógico de uma máquina presente na rede

`arp -a`

Interface: 192.168.1.69

Internet Address Physical Address Type

192.168.1.3 D0-67-E5-40-B5-3F Dynamic

- Apaga os endereços das máquinas especificado pelo `inet_addr`

`arp -d 192.168.1.3`

- Adiciona uma entrada na tabela de mapeamento do arp até o restart do sistema

`arp -s 802.3 host2 0:dd:0:a:85:0 temp`