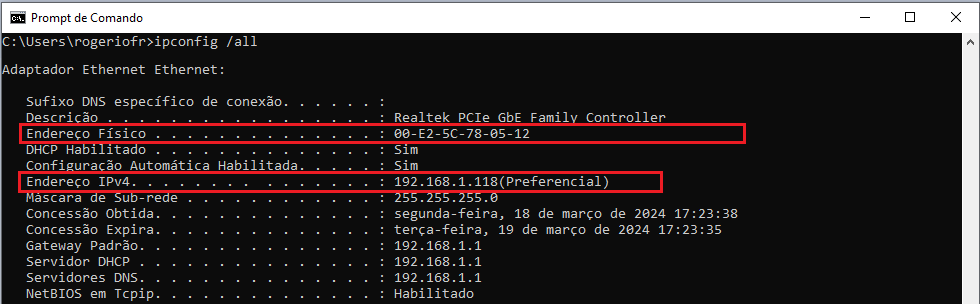
**Protocolo ARP**

Qualquer dispositivo que se conecte a uma rede de computadores possui um endereço físico e um endereço lógico.

O endereço físico é permanente (associado a placa de rede durante a fabricação) ou também conhecido como endereço de Controle de Acesso à Mídia (MAC). Já o endereço lógico ou endereço de Protocolo de Internet (IP) é um endereço aleatório que é definido quando o computador ou host qualquer é conectado a uma rede de comutadores.

Na figura a seguir, podemos ver o resultado do comando ipconfig /all executado no prompt de comando do Windows para visualizar o endereço IP e o Endereço Físico MAC.



Na imensa maioria das comunicações, o host que deseja enviar informações para um outro host precisa saber o endereço lógico (IP) e o endereço físico (MAC) do host de destino. Mas com computadores mudando os endereços IP com uma certa frequência como é descoberto qual endereço MAC está associado ao endereço IP naquele momento?

Entra em cena o ARP (Address Resolution Protocol), formalmente conhecido como Protocolo de Resolução de Endereço.

O trabalho do ARP é descobrir qual endereço MAC está associado a um determinado endereço IP. Esta é uma função bastante útil para qualquer rede. Apesar de sua utilidade, entretanto, o ARP acaba trazendo problemas de desempenho na rede quando esta possui muitos hosts na mesma sub-rede.

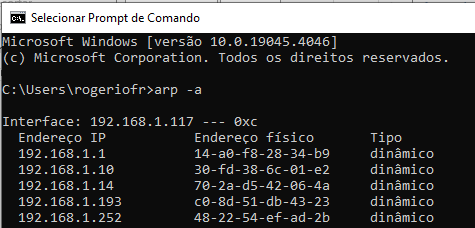
***Funcionamento do ARP:***

**Identificação do Endereço IP de Destino:** Quando um dispositivo deseja enviar dados para outro na mesma rede local, ele precisa saber o endereço MAC desse dispositivo. No entanto, ele só conhece o endereço IP do destino que normalmente é informado pelo usuário. O primeiro passo do ARP no host de origem é verificar se o endereço IP de destino consta na tabela de cache ARP. Caso o endereço IP de destino esteja na tabela de cache, é então utilizado o endereço MAC que está nesta tabela. Caso o endereço não esteja na tabela o é realizado o processo de consulta.

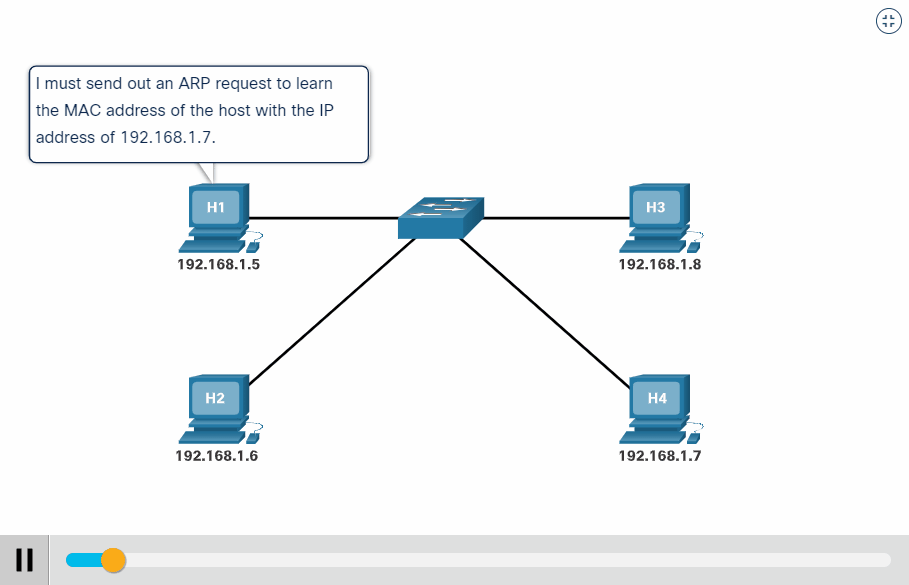
**Caching de ARP:** Cada dispositivo em uma rede mantém uma tabela de cache ARP que armazena mapeamentos de endereços IP para endereços MAC recentemente usados. Isso ajuda a melhorar a eficiência do ARP, evitando consultas repetidas para os mesmos endereços IP, pois para cada consulta ARP é gerado um tráfego de broadcast que precisa ser enviado para todos os computadores da mesma sub-rede.

A figura a seguir apresenta o comando arp -a que permite consultar no prompt de comando os registros inseridos nesta tabela. Note que se este host tentar se comunicar com o host que possui o endereço 192.168.1.10 ele não precisa utilizar o protocolo ARP, pois o MAC 30-fd-38-6c-01-e2 já consta na tabela cache.

No entanto, se este host tentar se comunicar com outro host com o endereço 192.168.1.7, será necessário acionar o protocolo ARP pois este host ainda não “aprendeu” qual é o MAC que está associado ao endereço IP 192.168.1.7.



**Consulta ARP:** Se o endereço IP de destino não estiver presente na tabela de cache ARP, o dispositivo envia uma solicitação ARP Request de broadcast (MAC FF:FF:FF:FF:FF:FF) para todos os dispositivos na rede local, perguntando quem possui o endereço IP desejado.



**Resposta ARP:** O dispositivo com o endereço IP solicitado responde à solicitação ARP com um pacote ARP Reply Unicast, fornecendo seu próprio endereço MAC. Note que apenas o dispositivo com o endereço IP de destino associado à solicitação ARP responderá com uma resposta ARP, os demais hosts que receberam o pedido ARP irão ignorar esta solicitação.

**Atualização da Tabela de Cache ARP**: Quando o dispositivo que fez a solicitação recebe a resposta, ele atualiza sua tabela de cache ARP com o mapeamento de endereço IP para endereço MAC do dispositivo de destino.

**Encaminhamento dos Dados**: Agora que o dispositivo tem o endereço MAC do destinatário, ele pode encapsular os dados em um quadro de camada de enlace contendo o endereço MAC de destino correto e enviar os dados diretamente para o dispositivo pretendido.

O protocolo ARP é essencial para a comunicação eficiente em redes locais, permitindo que os dispositivos descubram uns aos outros e se comuniquem diretamente. No entanto, como as solicitações ARP são broadcast, elas podem ser alvo de ataques de spoofing ARP, nos quais um dispositivo malicioso falsifica endereços MAC para interceptar ou redirecionar o tráfego de rede. Por isso, medidas de segurança, como o uso de ARP Spoofing Detection ou autenticação de dispositivos, são frequentemente implementadas para proteger as redes contra essas ameaças.

**Consulte o endereço para maiores informações:** https://kinsta.com/pt/base-de-conhecimento/o-que-e-arp/