1.ARP

Quando um pacote é enviado à camada de enlace de dados para ser encapsulado em um quadro Ethernet, o dispositivo consulta uma tabela em sua memória para encontrar o endereço MAC que é mapeado para o endereço IPv4. Esta tabela é armazenada temporariamente na memória RAM e denominada ARP. O dispositivo emissor pesquisará em sua tabela ARP um endereço IPv4 de destino correspondente a um endereço MAC. Cada entrada (linha) de tabela ARP vincula um endereço IPv4 a um endereço MAC, uma relação denominada de mapa. A tabela ARP salva temporariamente o mapeamento de dispositivos da LAN.

Se o endereço IPv4 destino estiver na mesma rede que o endereço IPv4 origem, o dispositivo pesquisará o endereço IPv4 destino na tabela ARP. Se o endereço IPv4 destino do pacote estiver em uma rede diferente do endereço IPv4 origem, o dispositivo pesquisará o endereço IPv4 do gateway padrão na tabela ARP.

Se o dispositivo localizar o endereço IPv4, seu endereço MAC correspondente será usado como endereço MAC de destino no quadro. Se nenhuma correspondência for encontrada, o dispositivo enviará uma requisição ARP.

Uma solicitação ARP é enviada quando um dispositivo precisa determinar o endereço MAC associado a um endereço IPv4 e não possui uma entrada para o endereço IPv4 em sua tabela ARP. As mensagens do ARP são encapsuladas diretamente em um quadro Ethernet. Não há cabeçalho IPv4.

A requisição é encapsulada em um quadro Ethernet usando as seguintes informações de cabeçalho.

- **Endereço MAC de destino:** Este é um endereço de broadcast FF-FF-FF-FF-FF-FF, exigindo que todas as NICs Ethernet na LAN aceitem e processem as solicitações ARP
- **Endereço MAC de origem:** Este é o endereço MAC do remetente da solicitação ARP
- **Tipo:** As mensagens ARP têm um campo de tipo 0x86. Ele informa à NIC de recebimento que a parte de dados do quadro precisa ser transferida para o processo ARP.

As solicitações ARP inundam todas as portas de switches, com exceção da porta de destino. Todas as NICs Ethernet no processo de LAN transmitem e devem entregar a solicitação ARP ao seu sistema operacional para processamento. Cada dispositivo processa a requisição, verificando se o seu endereço bate com o do pacote. Somente um dispositivo na LAN corresponde ao endereço IPv4 na requisição. Nenhum outro dispositivo responderá.

Se nenhum dispositivo responder à requisição ARP, o pacote será descartado porque não será possível criar um quadro. As entradas na tabela ARP possuem ***timestamps***. Se um dispositivo não receber um quadro de um dispositivo específico antes que o *timestamp* expire, a entrada desse dispositivo será removida da tabela ARP.

Sempre que um dispositivo de origem tiver um pacote com um endereço IPv4 em outras rede, ele encapsula esse pacote em um quadro usando o endereço MAC de destino do roteador. O endereço IPv4 gateway padrão é armazenado na configuração IPv4 dos hosts. Quando um host cria um pacote para um destino, ele compara o endereço IPv4 destino e seu próprio endereço IPv4 para determinar se os dois endereços IPv4 estão localizados na mesma rede de camada 3 OSI. Se não estiver na mesma rede, a origem irá usar a tabela ARP para obter uma entrada com endereço IPv4 do gateway padrão. Se não houver uma entrada, ele usará o processo ARP para determinar um endereço MAC do gateway padrão.

Em um rede corporativa, se um grande número de dispositivos precisasse ser ligado e todos começassem a acessar serviços de rede ao mesmo tempo, poderia haver alguma redução no desempenho por um curto período. Depois que os dispositivos enviarem os broadcasts ARP iniciais e tiverem reconhecido os endereços MAC necessários, qualquer impacto na rede é minimizado.

Um ator de ameaça pode usar falsificação ARP para realizar um ataque de envenenamento por ARP. É uma técnica usada por um ator de ameaça para responder a uma solicitação ARP de um endereço IPv4 que pertence a outro dispositivo, como o gateway padrão. O agente de ameaça envia uma resposta ARP com seu próprio endereço MAC. O destinatário da resposta ARP adicionará o endereço MAC errado à sua tabela ARP e enviará esses pacotes ao agente de ameaça. Switches de nível corporativo incluem técnicas de mitigação conhecidas como inspeção dinâmica ARP (DAI).