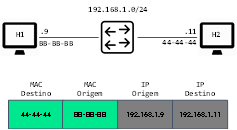
**Resolução de Endereços e Estrutura IPv4**

* **MAC e IP**

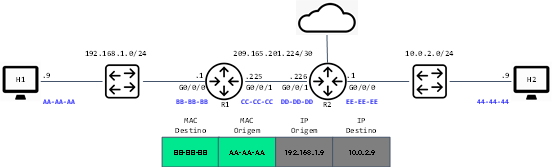
*Na mesma rede…*

Muitas vezes um host precisa enviar uma mensagem, mas só conhece o endereço IP do dispositivo de destino e necessita, também, do endereço MAC. Para isso há a resolução de endereços. Existem dois endereços principais atribuídos a um dispositivo em uma LAN Ethernet: MAC e IP (físico e lógico, respectivamente). Os endereços físicos são usados para entregar o quadro do enlace com o pacote IP encapsulado de uma NIC para outra NIC que está na mesma rede. Se o endereço IP de destino estiver na mesma rede, o endereço MAC de destino será o do dispositivo de destino. A Figura a seguir ilustra um exemplo de um quadro com destino na mesma rede.

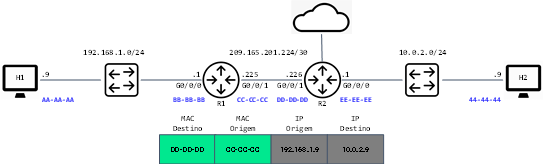


*Rede remota…*

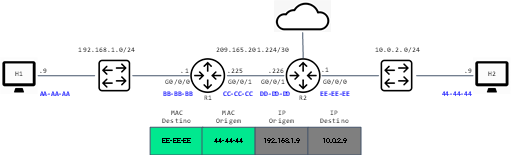
Se o endereço IP (v4 ou v6) de destino está em uma rede remota, o endereço MAC de destino será o endereço do gateway padrão do host (ou seja, a interface do roteador). A Figura a seguir mostra um exemplo de um quadro com destino em rede remota.



​Os roteadores examinam o endereço IPv4 de destino para determinar o melhor caminho para encaminhar o pacote IPv4. Quando o roteador recebe o quadro Ethernet, desencapsula as informações da camada 2. Usa o endereço IPv4 de destino para determinar o dispositivo de próximo salto e encapsula o pacote IPv4 em um novo frame do enlace (data link) para a interface de saída. O novo endereço MAC de destino é da interface R2 G0/0/1 e o novo endereço MAC de origem é da interface R1 G0/0/1.



​Ao longo de cada link do caminho um pacote IP é encapsulado em um frame específico associado à tecnologia do link, por exemplo, Ethernet. Se o dispositivo de próximo salto for o destino final, o endereço MAC de destino é da placa de rede Ethernet do mesmo.



*Como são os endereços IP dos pacotes em um fluxo de dados associados aos endereços MAC em cada link ao longo do caminho até o destino?*

* Para pacotes IPv4 é feito por meio do Protocolo de Resolução de Endereço (ARP - Address Resolution Protocol).
* Para pacotes IPv6 o processo é ICMPv6 (Internet Control Message Protocol Version 6) Neighbour Discovery (ND).

* **ARP**

*Funcionamento*

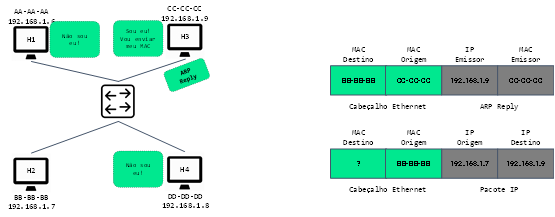
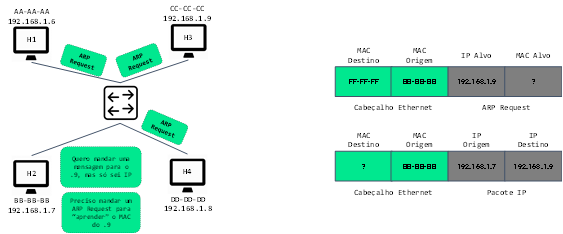
Se a rede usa o protocolo de comunicação IPv4 o ARP é necessário para mapear endereços IPv4 para endereços MAC. Lembrando que cada dispositivo IP em uma rede Ethernet possui um endereço Ethernet MAC exclusivo. Quando um dispositivo envia um frame Ethernet contém estes dois endereços:

* Endereço MAC de destino: do dispositivo de destino no mesmo segmento de rede local. Se o host de destino estiver em outra rede o endereço de destino no quadro é o do gateway padrão (ou seja, roteador).
* Endereço MAC de origem: da NIC Ethernet do host de origem.

Para enviar um pacote a outro host na mesma rede IPv4 local, o host deve saber o endereço IPv4 e o endereço MAC do dispositivo de destino. Os endereços IPv4 de destino do dispositivo são conhecidos ou resolvidos pelo nome do dispositivo. No entanto, os endereços MAC devem ser descobertos. Um dispositivo usa o protocolo de resolução de endereço (ARP) para determinar o endereço MAC de destino de um dispositivo local e já conhece o endereço IPv4 do destino. O ARP oferece duas funções básicas:

* Resolver endereços IPv4 para endereços MAC
* Manter uma tabela de mapeamentos de endereços IPv4 para MAC

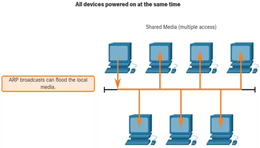
Quando um pacote é enviado à camada de enlace para ser encapsulado em um quadro Ethernet, o dispositivo consulta uma tabela em sua memória para encontrar o endereço MAC mapeado para o IPv4.  Esta tabela é armazenada temporariamente na memória RAM e é chamada de tabela ARP ou cache ARP. Se o endereço de destino do pacote estiver na mesma rede que o endereço de origem, o dispositivo pesquisará na tabela ARP o endereço destino. Se o endereço de destino estiver em uma rede diferente do endereço de origem, o dispositivo pesquisará na tabela ARP o endereço do gateway padrão. Cada entrada da tabela ARP associa um endereço IPv4 a um endereço MAC, relação chamada de mapa. A tabela ARP salva temporariamente o mapeamento.



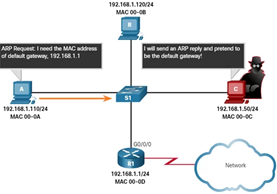
*Remoção e outras coisas…*

Em cada dispositivo há um temporizador de cache ARP para remover as entradas ARP que não foram usadas por um determinado tempo especificado. Os tempos variam conforme o sistema operacional do dispositivo. Por exemplo, o sistema operacional Windows (mais recentes) armazenam entradas da tabela ARP entre 15 e 45 segundos.

Um frame de solicitação ARP é recebido e processado por todos os dispositivos na rede local (similar a um frame de transmissão). Em uma rede comercial típica essas transmissões tem um impacto mínimo no desempenho da rede. No entanto, se um grande número de dispositivos for ligado e todos começarem a acessar os serviços de rede ao mesmo tempo, pode haver alguma redução no desempenho por um curto período de tempo.



​ARP Spoofing: em alguns casos, o uso de ARP pode levar a um risco de segurança potencial. Um ator de ameaça pode usar ARP spoofing para executar um ataque de envenenamento ARP. Esta é uma técnica usada por um ator de ameaça para responder a uma solicitação ARP de um endereço IPv4 que pertence a outro dispositivo.



* **Descoberta de IPv6**

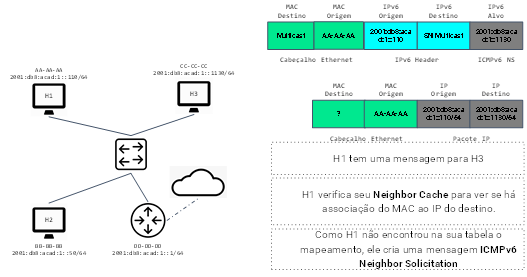
*Visão Geral*

O protocolo IPv6 Neighbour Discovery é às vezes referido como ND ou NDP (ND Protocol). O ND fornece resolução de endereço, descoberta de roteador e serviços de redirecionamento para IPv6 usando ICMPv6. O ICMPv6 ND usa cinco mensagens ICMPv6 para executar estes serviços:

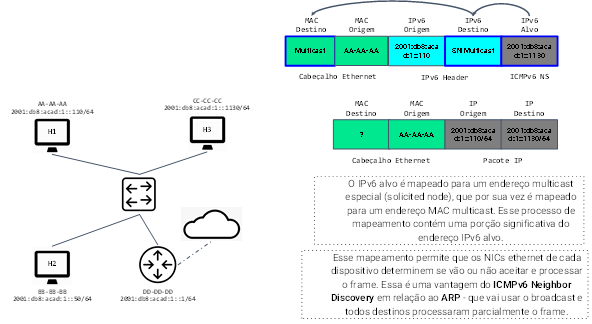
* Neighbor Solicitation messages
* Neighbor Advertisement messages
* Router Solicitation messages
* Router Advertisement messages
* Redirect Message

As mensagens de Neighbor Solicitation e Neighbor Advertisement são de dispositivo para dispositivo, como resolução de endereço (semelhante ao ARP para IPv4). As mensagens de Router Solicitation e Router Advertisement são entre dispositivos e roteadores. Geralmente, a descoberta do roteador é usada para alocação dinâmica de endereços e autoconfiguração de endereços sem estado (SLAAC - StateLess Address AutoConfiguration).

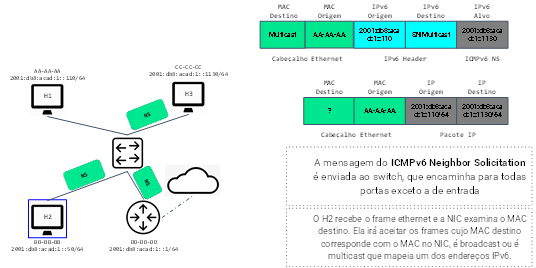
A Figura a seguir mostra um exemplo do processo de solicitação de vizinho.



A Figura a seguir ilustra um exemplo do processo de descoberta de vizinho.

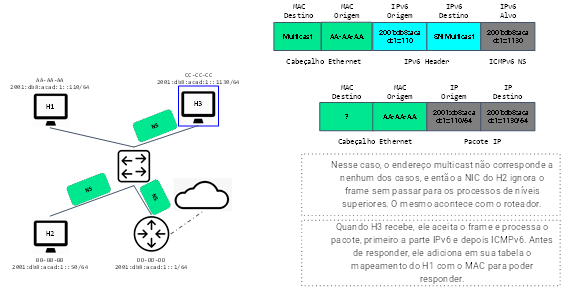


A Figura a seguir mostra um exemplo do processo de solicitação de vizinho.

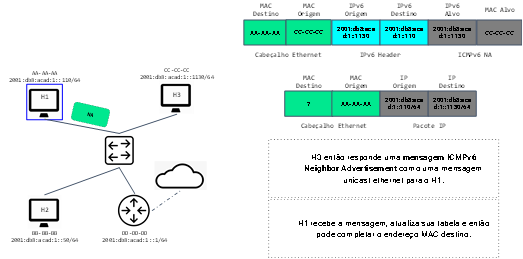


​

A Figura a seguir ilustra um exemplo do processo em que H3 aceita o frame e processa o pacote; antes de responder, adiciona em sua tabela o mapeamento do H1 com o MAC.​

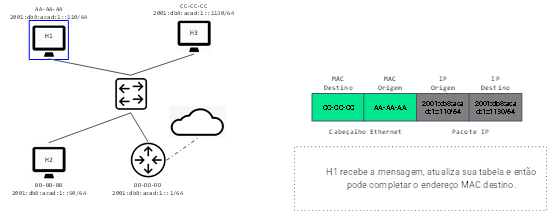


A Figura a seguir mostra um exemplo do processo de anúncio de vizinho de H3 para H1



​

A Figura a seguir ilustra um exemplo do processo em H1 recebe a mensagem, atualiza sua tabela e então pode completar o endereço MAC de destino.​



* **Estrutura do IPv4**

*Partes*

Os bits do endereço correspondentes à rede devem ser idênticos para todos os dispositivos que residem na mesma rede. Os bits do endereço da parte do host devem ser exclusivos para identificar um host específico em uma rede. Se dois hosts têm o mesmo padrão de bits na porção de rede especificada dentre os 32 bits, esses dois hosts residem na mesma rede. A Figura mostra um exemplo de endereço IPv4 com as partes rede e host.

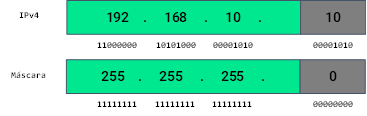
https://paperx-dex-assets.s3.sa-east-1.amazonaws.com/images/1626791281751-a2g4lapOno.png

​

Mas como os hosts sabem qual parte dos 32 bits identifica a rede e qual identifica o host? Para isso há a máscara de sub-rede! A máscara de sub-rede IPv4 é usada para diferenciar a parte da rede da parte do host de um endereço IPv4. Quando um endereço IPv4 é atribuído a um dispositivo, a máscara de sub-rede é usada para determinar o endereço de rede do dispositivo. O endereço de rede representa todos os dispositivos na mesma rede. A Figura a seguir ilustra um exemplo de máscara de sub-rede.​

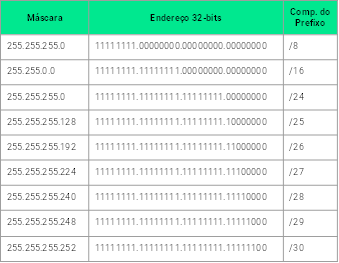
https://paperx-dex-assets.s3.sa-east-1.amazonaws.com/images/1626791365637-1KQMus1OzA.png

​A máscara de sub-rede não contém realmente a rede ou parte do host de um endereço IPv4, apenas informa ao computador onde procurar a parte do endereço IPv4 que corresponde a rede e qual ao host. O processo real para identificar a rede e o host é uma operação de AND (lógico). A Figura a seguir mostra um endereço IPv4 associado à sua máscara de sub-rede.​



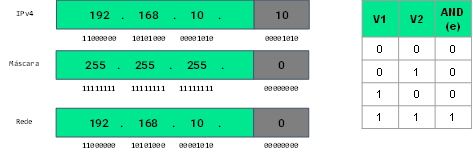
*Prefixo*

Representar endereços de rede e endereços de host com o endereço de máscara de sub-rede decimal com pontos pode não ser a melhor forma.  Existe uma maneira alternativa para identificar uma máscara de sub-rede, um método denominado comprimento do prefixo. O comprimento do prefixo é o número de bits 1s na máscara de sub-rede. É escrito por uma barra (/) seguida pelo número de bits 1s. Portanto, basta contar o número de bits 1s na máscara de sub-rede e acrescente uma barra. A Tabela a seguir ilustra exemplos de representação de máscara de sub-rede.



*AND para o endereço de Rede*

Para identificar o endereço de rede de um host IPv4, o endereço IPv4 é logicamente um AND bit a bit, com a máscara de sub-rede. Fazer o AND entre o endereço e a máscara de sub-rede produz o endereço de rede.



*Endereços importantes*

A Figura a seguir mostra exemplos de endereços importantes.

