**Comutação Ethernet**

* **Objetivo e Estrutura**

**Ethernet – relembrando**: A tecnologia Ethernet é usada em LAN tanto com fio quanto sem fio (WLANs). A Ethernet com fio pode utilizar par trançado (UTP ou STP), fibra óptica ou cabo coaxial (este último considerado legado). Opera nas camadas de enlace e física. É uma família de tecnologias de rede definida nos padrões IEEE 802.2 e 802.3. Suporta as seguintes larguras de banda (taxas de bit):

* 10 Mbit/s
* 100 Mbits
* 1000 Mbit/s (1 Gbit/s)
* 10.000 Mbit/s (10 Gbit/s)
* 40.000 Mbit/s (40 Gbit/s)
* 100.000 Mbit/s (100 Gbit/s)

**Subcamadas – relembrando**: A subcamada MAC é responsável pelo encapsulamento de dados e acesso ao meio.

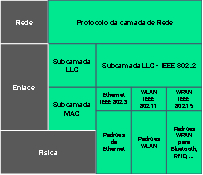
**O encapsulamento de dados IEEE 802.3 inclui:**

* Frame Ethernet - É a estrutura interna
* Endereçamento Ethernet - O frame Ethernet inclui um endereço MAC de origem e de destino para entregar o frame de Ethernet NIC para Ethernet NIC na mesma LAN.
* Detecção de erro Ethernet - O frame Ethernet inclui um trailer de sequência de verificação de frame (FCS) usado para detecção de erro.

**Acesso ao meio:**

* A subcamada IEEE 802.3 MAC inclui as especificações para diferentes padrões de comunicação Ethernet em vários tipos de mídia, incluindo cobre e fibra.
* A subcamada LLC pega os dados do protocolo de rede e adiciona informações de controle da Camada 2 para ajudar a entregar o pacote ao nó de destino.

A Figura a seguir ilustra as subcamadas LLC e MAC.



**Comunicação e Acesso:** A Ethernet legada, usando uma topologia de barramento ou hubs, é um meio *half-duplex* compartilhado. A Ethernet em meio *half-duplex*usa um método de acesso baseado em contenção (CSMA/CD) - garante que apenas um dispositivo esteja transmitindo por vez. O CSMA/CD permite que vários dispositivos compartilhem o mesmo meio *half-duplex*, detectando uma colisão quando mais de um dispositivo tenta transmitir simultaneamente. Também fornece um algoritmo de *back-off* para retransmissão. As LANs Ethernet de hoje usam *switches* que operam em *full-duplex*. As comunicações *full-duplex* com *switches* Ethernet não requerem controle de acesso por CSMA/CD.

***Frame*:** O tamanho mínimo do quadro Ethernet é 64 bytes e o máximo esperado é 1518 bytes. O campo do preâmbulo não é incluído ao descrever o tamanho do quadro. O tamanho do quadro pode ser maior se requisitos adicionais forem incluídos, como VLAN *tagging*. Qualquer quadro com menos de 64 bytes de comprimento é considerado um “fragmento de colisão” ou “*runt frame*” e é automaticamente descartado pelas estações receptoras.  Quadros com mais de 1.500 bytes de dados são considerados “jumbo” ou “quadros gigantes”. Os quadros jumbo são geralmente suportados pela maioria dos *switches* e NICs *Fast Ethernet* e *Gigabit Ethernet*. A Figura a seguir mostra os campos do quadro Ethernet.

https://paperx-dex-assets.s3.sa-east-1.amazonaws.com/images/1626725404243-EKYSU12Mu1.png

**Os campos Preâmbulo (7 bytes) e *Start Frame Delimiter* – SFD, também chamado de *Start of Frame,* (1 byte):** São usados para a sincronização entre os dispositivos de envio e recebimento. Esses primeiros oito bytes do quadro são usados pelos nós receptores. Essencialmente, os primeiros bytes sinalizam aos receptores para se prepararem para receber um novo quadro.

***Destination MAC Address***: Este campo de 6 bytes é o identificador do destinatário. Esse endereço é usado pela camada 2 para ajudar os dispositivos a identificar a quem o quadro é endereçado. O endereço no quadro é comparado ao endereço MAC no dispositivo. Se houver uma correspondência, o dispositivo aceita o quadro. Pode ser um endereço *unicast*, *multicast* ou *broadcast*.

***Source MAC Address***: Este campo de 6 bytes identifica a NIC de origem ou interface do quadro.

***EtherType*:** Este campo de 2 bytes identifica o protocolo da camada superior encapsulado no quadro Ethernet. Os valores comuns são, em hexadecimal, 0x800 para IPv4, 0x86DD para IPv6 e 0x806 para ARP.

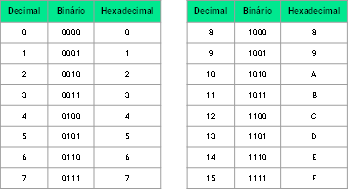
Nota: este campo também pode ver referido como Tipo ou Comprimento.

***Data*:** Este campo (46-1500 bytes) contém os dados encapsulados de uma camada superior, que é uma PDU da camada 3 genérica ou, mais comumente, um pacote IPv4. Todos os quadros devem ter pelo menos 64 bytes. Se um pequeno pacote for encapsulado, bits adicionais chamados de *pad* são usados para preenchimento do quadro até completar o tamanho mínimo.

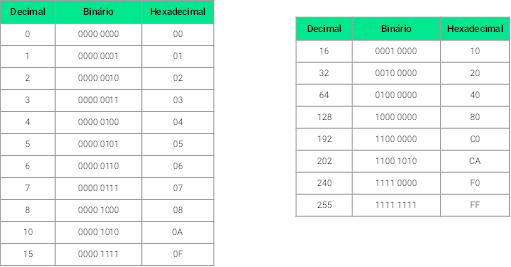
**FCS:** O campo *Frame Check Sequence* - FCS (4 bytes) é usado para detectar erros em um quadro. Usa uma verificação de redundância cíclica (*Cyclic Redundancy Check* - CRC). O dispositivo de transmissão inclui os resultados de um CRC no campo FCS do quadro. O dispositivo receptor recebe o quadro e recalcula o CRC. Se o resultado do cálculo corresponde ao transmitido, nenhum erro ocorreu. Cálculo que não corresponde são uma indicação de que os dados foram alterados durante a transmissão e o quadro é descartado.

* **Endereço MAC**

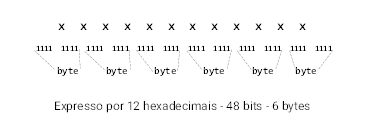
**Relembrando Hexadecimal**: A Tabela a seguir ilustra os valores decimais e hexadecimais equivalentes para o binário 0000 a 1111.



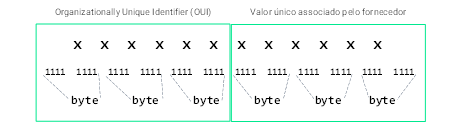
**Equivalências - exemplos 8 bits**: A Tabela a seguir mostra os valores equivalentes em decimal e hexadecimal para os binários 0000000 a 11111111.



A Figura a seguir ilustra um exemplo de endereço MAC Ethernet.

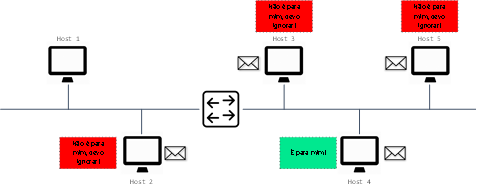


​Todos os endereços MAC devem ser exclusivos para o dispositivo Ethernet ou interface Ethernet. Para garantir isso, **todos os fornecedores que vendem dispositivos Ethernet devem se registrar no IEEE para obter um código hexadecimal exclusivo de 6 (ou seja, 24 bits ou 3 bytes) denominado identificador organizacional exclusivo (OUI).** A Figura a seguir mostra a composição do endereço MAC Ethernet.​



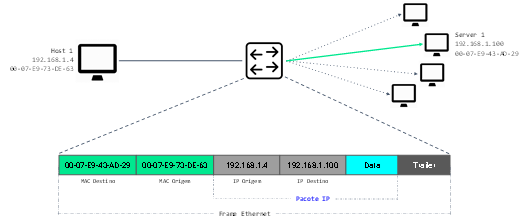
É responsabilidade do fornecedor garantir que nenhum de seus dispositivos receba o mesmo endereço MAC. Podem existir endereços MAC duplicados por erros cometidos durante a fabricação, erros em alguns métodos de implementação de máquina virtual ou modificações feitas ao usar ferramentas de *software*.

**Processamento do *Frame*:** O endereço MAC é também conhecido como “endereço gravado” (BIA - *Burned-in Address*) porque o endereço é codificado na memória ROM permanentemente na NIC. Em sistemas operacionais de PC modernos e NICs, é possível alterar o endereço MAC no *software*. Isso é útil ao tentar obter acesso a uma rede que filtra com base em BIA. Logo, filtrar ou controlar o tráfego com base no endereço MAC não é mais tão seguro. Quando o computador é inicializado, a NIC copia seu endereço MAC da ROM para a RAM. Quando um dispositivo encaminha uma mensagem para uma rede Ethernet, o cabeçalho Ethernet inclui o MAC de origem e o MAC de destino. Quando uma NIC recebe um *frame* Ethernet, examina o endereço MAC de destino para ver se corresponde ao endereço MAC físico armazenado na RAM. Se não houver correspondência, o dispositivo descarta o *frame*. Se houver uma correspondência, aceita o *frame* que passa pelas camadas OSI, onde ocorre o processo de desencapsulamento. A Figura a seguir ilustra o processo de encaminhamento de uma mensagem em uma rede Ethernet.



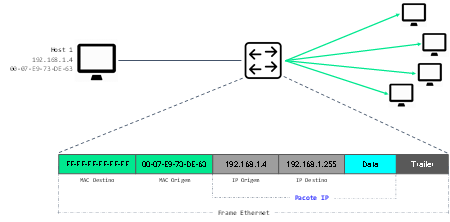
As placas de rede Ethernet também aceitarão quadros se o endereço MAC de destino for um *broadcast* ou um grupo *multicast* do qual o*host* é membro. Qualquer dispositivo que seja a origem ou destino de um *frame* Ethernet, terá uma placa de rede Ethernet e, portanto, um endereço MAC. Isso inclui estações de trabalho, servidores, impressoras, dispositivos móveis e roteadores.

***Unicast*:** Um endereço MAC *unicast* é o endereço exclusivo usado quando um quadro é enviado de um único dispositivo de transmissão para um único dispositivo de destino. A Figura a seguir mostra um exemplo de endereço MAC *unicast.*



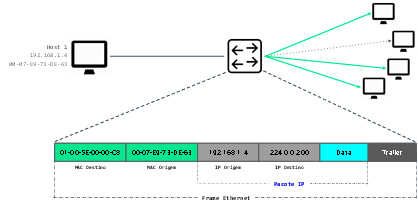
O processo que um *host* de origem usa para determinar o endereço MAC de destino associado a um endereço IPv4 é conhecido como protocolo de resolução de endereço (ARP – *Address Resolution Protocol*). O processo que um *host* de origem usa para determinar o endereço MAC de destino associado a um endereço IPv6 é conhecido como descoberta de vizinho (*Neighbour Discovery* - ND).

***Broadcast*:** Um quadro de transmissão Ethernet é recebido e processado em cada dispositivo na LAN Ethernet. Tem um endereço MAC de destino de FF-FF-FF-FF-FF-FF em hexadecimal que é “inundado” para todas as portas do *switch* Ethernet, exceto a porta de entrada. Não é encaminhado por um roteador. Se os dados encapsulados forem um pacote de broadcast IPv4, isso significa que o pacote contém um endereço IPv4 de destino que possui tudo um (1s) na parte referente ao *host*. Essa numeração no endereço significa que todos os *hosts* nessa rede local (domínio de *broadcast*) recebem e processam o pacote. A Figura a seguir ilustra um exemplo de endereço MAC de *broadcast*.



O DHCP (*Dynamic Host Configuration Protocol*) para IPv4 é um exemplo de protocolo que usa endereços de transmissão Ethernet e IPv4. No entanto, nem todos os *broadcasts* Ethernet carregam um pacote de *broadcast* IPv4. Por exemplo, as solicitações ARP não usam IPv4, mas a mensagem ARP é enviada como uma transmissão Ethernet.

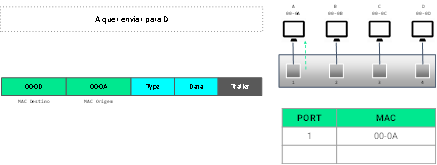
***Multicast:*** Há um endereço MAC de destino de 01-00-5E (pacote *multicast* IPv4) e um endereço MAC 33-33 (pacote multicast IPv6). Existem outros endereços MAC de destino de *multicast* reservados sem ser IP, como *Spanning Tree Protocol* (STP) e *Link Layer Discovery Protocol* (LLDP). É “inundado” por todas as portas do *switch* Ethernet, exceto a porta de entrada, a menos que o *switch* esteja configurado para *snooping multicast.*Não é encaminhado por um roteador, a menos que o roteador esteja configurado para rotear pacotes *multicast*. Se os dados encapsulados forem um pacote *multicast* IP, os dispositivos pertencentes a um grupo *multicas*t são atribuídos a um endereço IP do grupo *multicast***. O intervalo de endereços *multicast* IPv4 é de 224.0.0.0 a 239.255.255.255.  O intervalo de endereços *multicast* IPv6 começa com ff00 ::/8.** Como os endereços multicast representam um grupo de endereços (às vezes chamado de grupo de *hosts*), só podem ser usados como destino de um pacote. A fonte sempre será um endereço *unicast*. A Figura a seguir mostra um endereço MAC *multicast*.



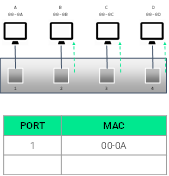
* **Tabela MAC**

***Switching*:** Um *switch* Ethernet da camada 2 usa endereços MAC da camada 2 para tomar decisões de encaminhamento. Ignora completamente os dados (protocolo) sendo transportados na parte de dados do quadro, como um pacote IPv4, uma mensagem ARP ou um pacote IPv6 ND. O *switch* toma suas decisões de encaminhamento com base exclusivamente nos endereços MAC Ethernet da camada 2. Um *switch* Ethernet examina sua tabela de endereços MAC para tomar uma decisão de encaminhamento para cada quadro, ao contrário de *hubs* Ethernet legados que apenas repetem os bits em todas as portas, exceto na porta de entrada.

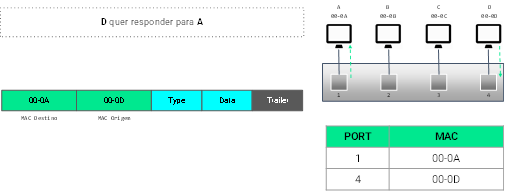
**Aprendendo**: O *switch* constrói dinamicamente a tabela de endereços MAC examinando o endereço MAC de origem dos *frames* recebidos em uma porta.  O *switch* encaminha os quadros procurando uma correspondência entre o endereço MAC e a porta na tabela. Cada quadro que entra em um *switch* é verificado para novas informações a serem aprendidas. Faz isso examinando o endereço MAC de origem do quadro e o número da porta onde o *frame* entrou no *switch* -  se o endereço MAC de origem não existir, então será adicionado à tabela junto com o número da porta de entrada; se existir, o *switch* atualizará o temporizador (cronômetro) para essa entrada na tabela (por padrão, a maioria dos *switches* Ethernet mantém uma entrada na tabela por 5 minutos). A Figura a seguir ilustra um exemplo do processo de aprendizagem do switch.



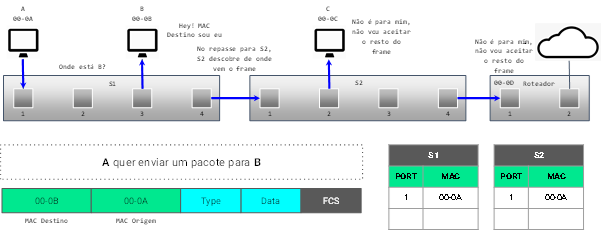
**Encaminhando:** Se o endereço MAC de destino for um endereço *unicast*, o *switch* procurará uma correspondência entre o endereço MAC de destino do quadro e uma entrada em sua tabela de endereços MAC. Se o endereço MAC de destino estiver na tabela, encaminhará o quadro pela porta especificada. Se o endereço MAC de destino não estiver na tabela, o *switch* encaminhará o quadro por todas as portas, exceto a porta de entrada. Isso é chamado de *unicast* desconhecido. Se o endereço MAC de destino for um *broadcast* ou *multicast*, o quadro também é inundado por todas as portas, exceto a porta de entrada.



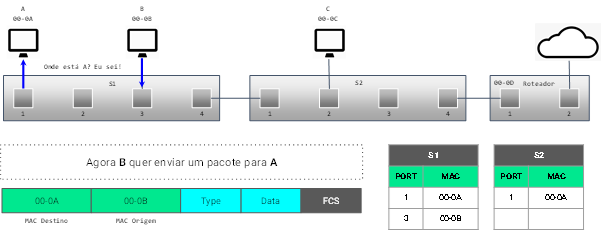
**Filtrando:** À medida que um *switch* recebe quadros de diferentes dispositivos é capaz de preencher sua tabela de endereços MAC examinando o endereço MAC de origem de cada *frame*. Quando a tabela de endereços MAC do *switch* contém o endereço MAC de destino é capaz de filtrar o *frame* e encaminhar para uma única porta.



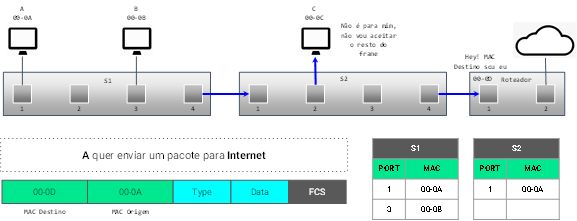
**Exemplificando:** *A Figura a seguir mostra um exemplo do processo de enviar um pacote do PC A para o PC B em uma rede local com acesso à Internet.*



A Figura a seguir ilustra um exemplo do processo de enviar um pacote do PC B para o PC A.



​Quando um dispositivo está em uma rede remota o quadro Ethernet não pode ser enviado diretamente ao dispositivo de destino. Em vez disso, o quadro Ethernet é enviado ao endereço MAC do *gateway* padrão, o roteador. A Figura a seguir mostra um exemplo do processo de enviar um pacote do PC A para Internet.​



A Figura a seguir ilustra um exemplo do processo de enviar um pacote da Internet para o PC A.

