

Tecnologias de Redes



Cruzeiro do Sul Virtual
Educação a distância

Material Teórico



Rede *Ethernet*

Responsável pelo Conteúdo:

Prof. Esp. Antonio Eduardo Marques da Silva

Revisão Textual:

Prof. Esp. Claudio Pereira do Nascimento

UNIDADE

Rede *Ethernet*



- Redes Ethernet e Subcamadas LLC e MAC;
- MAC - Controle de Acesso ao Meio;
- Processamento de um Quadro (Frame);
- Tipos de Endereços MAC.



OBJETIVO DE APRENDIZADO

- Compreender e apresentar a tecnologia de rede local (LAN) baseada no protocolo Ethernet / IEEE 802.3 e suas funcionalidades.

Orientações de estudo

Para que o conteúdo desta Disciplina seja bem aproveitado e haja maior aplicabilidade na sua formação acadêmica e atuação profissional, siga algumas recomendações básicas:



Assim:

- ✓ Organize seus estudos de maneira que passem a fazer parte da sua rotina. Por exemplo, você poderá determinar um dia e horário fixos como seu “momento do estudo”;
- ✓ Procure se alimentar e se hidratar quando for estudar; lembre-se de que uma alimentação saudável pode proporcionar melhor aproveitamento do estudo;
- ✓ No material de cada Unidade, há leituras indicadas e, entre elas, artigos científicos, livros, vídeos e sites para aprofundar os conhecimentos adquiridos ao longo da Unidade. Além disso, você também encontrará sugestões de conteúdo extra no item **Material Complementar**, que ampliarão sua interpretação e auxiliarão no pleno entendimento dos temas abordados;
- ✓ Após o contato com o conteúdo proposto, participe dos debates mediados em fóruns de discussão, pois irão auxiliar a verificar o quanto você absorveu de conhecimento, além de propiciar o contato com seus colegas e tutores, o que se apresenta como rico espaço de troca de ideias e de aprendizagem.

Redes Ethernet e Subcamadas LLC e MAC

O protocolo de rede local (LAN) Ethernet é atualmente a tecnologia mais utilizada na interconexão de hosts. Ela opera na camada de enlace de dados e na camada física em relação ao modelo de referência OSI/ISO. É um conjunto de tecnologias de redes de comutação definida nos padrões IEEE 802.2 (LLC) e IEEE 802.3 (Ethernet descrita no IEEE). Tal rede pode suportar algumas vazões de dados como segue:

- 10 Mb/s;
- 100 Mb/s;
- 1000 Mb/s (1 Gb/s);
- 10.000 Mb/s (10 Gb/s);
- 40.000 Mb/s (40 Gb/s);
- 100.000 Mb/s (100 Gb/s).

Os padrões de rede ethernet definem os protocolos de Camada 2 e as tecnologias físicas de Camada 1. Em relação ao protocolo de Camada 2 (enlace) a ethernet nessa camada é dividida em duas subcamadas, a subcamada de controle lógico de link (LLC) e a subcamada de controle de acesso ao meio (MAC). (TANENBAUM, A. S., 2011)

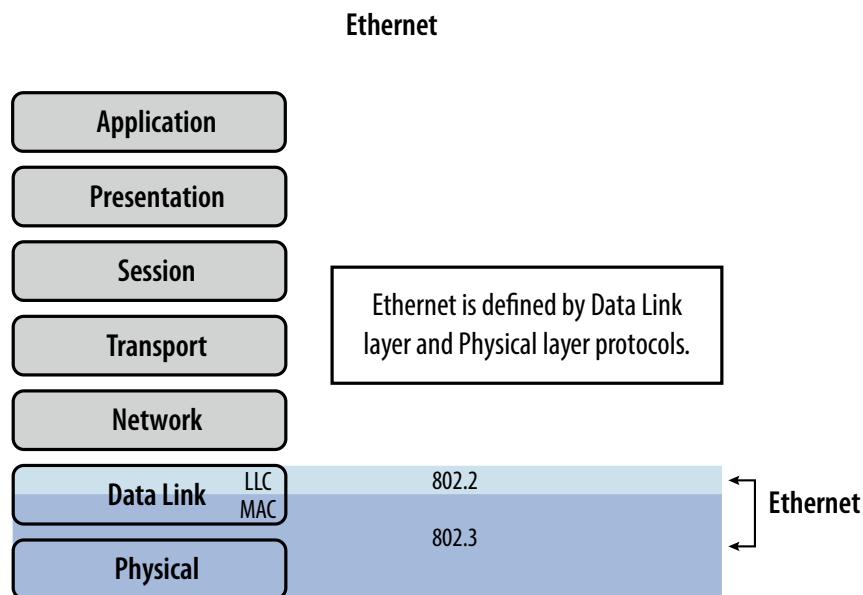


Figura 1 – Rede Ethernet

A Subcamada LLC

A subcamada de controle lógico de link da rede ethernet trata da comunicação entre as camadas superiores e as camadas inferiores do modelo de referência de rede. Isso é normalmente entre o software de rede e o hardware do dispositivo a ser estudado. A subcamada LLC obtém os dados do protocolo de rede, que normalmente é um pacote IPv4, e adiciona informações de controle para ajudar a entregar o pacote no host destino.

Esse tipo de controle é usado para comunicar com as camadas superiores do aplicativo e mover os pacotes de dados para as camadas inferiores. (TANENBAUM, A. S., 2011)

O controle lógico de link é implementado no software de rede, e sua implementação independe do hardware do dispositivo utilizado. Em um computador, o LLC pode ser considerado o driver de uma placa de rede por exemplo. A função desse programa de driver é interagir diretamente com o hardware na placa afim de transmitir os dados entre a subcamada de controle de acesso ao meio (MAC) e os meios físicos, tais como um cabo UTP e uma fibra Óptica.

A Subcamada MAC

A subcamada MAC constitui uma inferior da camada de enlace de dados. É implementada pelo hardware do dispositivo, normalmente na placa de rede do computador por exemplo. Os detalhes estão especificados nos padrões IEEE 802.3, que o padrão ethernet descrito no IEEE. A subcamada MAC possui duas responsabilidades principais:

- Encapsulamento dos dados a serem transmitidos;
- Controle de acesso ao meio.

É na subcamada MAC que é representado o conhecido endereço físico adotado pelos hosts em uma rede ethernet, o MAC address.

O Encapsulamento de Dados

O processo de encapsulamento de dados é a forma como os dados são montados em quadros antes da transmissão ser enviada e a desmontagem dos dados que são carregados no quadro recebido por um determinado destino, chamamos de desencapsulamento. Ao formar o frame, a camada MAC adiciona um cabeçalho e um trailer à PDU de camada de rede, que conhecemos por pacote.

O encapsulamento e desencapsulamento de dados fornecem três funções:

- **Delimitação de Quadro:** o processo de encapsulamento oferece delimitadores importantes que são utilizados para identificar um grupo de bits que formam um frame. Esse processo oferece sincronização entre os nós transmissor e receptor.
- **Endereçamento:** o processo de encapsulamento fornece o endereçamento de camada de enlace de dados, que no caso da ethernet, é o endereço MAC. Cada cabeçalho de Ethernet adicionado ao frame possui esse endereço físico que possibilita que um frame seja entregue a um host destino.
- **Detecção de Erros:** cada frame ethernet possui um finalizador (trailer) que pode realizar a verificação de redundância cíclica (CRC) do conteúdo do frame. Depois do recebimento de um frame, o host de destino cria uma CRC para comparar com a que está dentro do frame. Se estes dois cálculos de CRC de ambos os frames se corresponderem, pode-se afirmar que os dados com certeza foram recebidos sem erros.

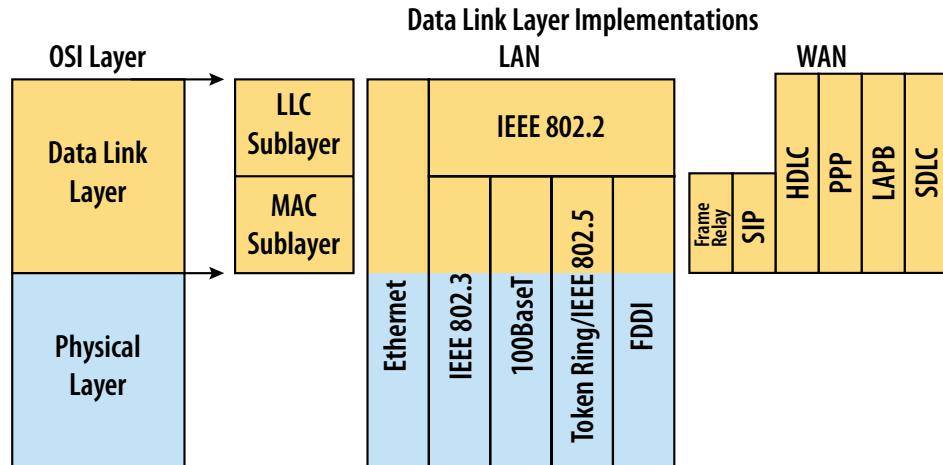


Figura 2 – Subcamadas LLC e MAC

MAC - Controle de Acesso ao Meio

A segunda responsabilidade da subcamada MAC é o controle de acesso à mídia ou ao meio. Tal controle é responsável pela colocação e remoção dos frames no meio físico utilizado, para que os dados possam ser transportados. Tal subcamada se comunica diretamente com a camada física de rede.

A topologia lógica da rede ethernet é um barramento de multiacesso; portanto, todos os dispositivos de rede em um único segmento de rede são compartilhados com o meio físico. A rede ethernet é um método baseado em contenção de rede, também conhecido como método não determinístico, que significa que qualquer dispositivo de rede poderia tentar transmitir os dados através do meio físico compartilhado sempre que tiver dados para enviar, desde que aguarde a portadora ficar livre. Nesse caso, é possível que dois dispositivos tentem compartilhar esse meio físico ao mesmo tempo, pois como foi dito a rede possui um processo de concorrência. Caso isso ocorra, os frames transmitidos poderão se colidir gerando dados corrompidos e inutilizáveis. Por esse motivo a rede ethernet fornece um método de acesso para controlar como os hosts podem compartilhar o acesso à rede, através de uma tecnologia conhecida como Portadora Sensível a Múltiplos Acessos (CSMA). (TANENBAUM, A. S., 2011)

O método de acesso CSMA é utilizado para detectar primeiro se o meio físico está transportando um sinal e utilizando o meio concorrente. Se um sinal de um determinado host for detectado na portadora, significa que alguém está utilizando o recurso e nesse caso, mais ninguém na rede pode transmitir. Até que depois de um curto período ele tente novamente e identifique que o canal está livre e nesse caso possa transportar o dado. É possível que o esse processo de CSMA falhe e dois dispositivos acabem transmitindo os dados ao mesmo tempo. O que vai ocorrer também a colisão de dados. Caso essa colisão ocorra, os dados enviados por ambos os dispositivos serão corrompidos e precisarão ser reenviados depois de um tempo de envio aleatório. (STALLINGS, W. e ROSS K., 2010)

Esses métodos de controle de acesso ao meio físico baseados em contenção não possuem mecanismos para rastrear de quem é o dado a ser enviado no meio físico; portanto, eles não têm a sobrecarga dos métodos de acesso controlado. No entanto, os sistemas baseados em contenção não escalam bem sob uso intenso do meio físico, pois à medida que o uso e o número de hosts aumentam, a probabilidade de acesso bem-sucedido ao meio físico sem colisão diminui muito. Além disso, os mecanismos de recuperação necessários para corrigir erros devido a tais colisões ainda diminuem a taxa de transferência. O CSMA é geralmente implementado em conjunto com um método para resolver a contenção do meio físico. (CISCO NETACAD, 2017)

Os dois métodos frequentemente usados são:

- **O Processo de Detecção de Colisão (CD)** – Na Detecção de Colisão do CSMA ou conhecida como CSMA/CD, o dispositivo de rede monitora o meio físico para verificar a presença de um sinal de dados. Se um sinal de dados estiver ausente, indicando que o meio físico está livre, o dispositivo transmitirá os dados sem problemas. Caso forem detectados sinais que presentam que outro dispositivo de rede estava transmitindo o dado em um canal, todos os dispositivos da rede param de enviar dados e tentam aguardar o canal ficar livre, para que possam novamente tentar mais tarde. Por esse motivo foram desenvolvidas outras formas tradicionais de ethernet afim de auxiliar esse método.

A ampla utilização de tecnologias de comutação em redes modernas retirou em grande parte a necessidade original do CSMA/CD em redes locais. Quase todas as conexões com fio entre dispositivos em uma rede local atualmente são conexões em full-duplex, um dispositivo pode enviar e receber simultaneamente os dados e ficarem livres de colisão em um mesmo cabo. No entanto, as conexões de rede sem fio em um ambiente de rede local (WLAN) ainda precisam levar em consideração as colisões que podem ocorrer. Os dispositivos de rede local sem fio utilizam o método de acesso ao meio físico com previsão de colisão, conhecido pela sigla CSMA/CA.

- **O Processo de Prevenção de Colisão** – No método de acesso de CSMA/CA, o host origem examina o meio físico para verificar a presença de sinal de dados no canal de transmissão. Se o meio físico estiver livre, o dispositivo enviará uma notificação pelo meio físico com sua intenção de poder utilizá-lo para transmitir uma determinada informação. O dispositivo então envia os dados sem problemas. Esse método é usado por tecnologias de rede sem fio descritas no IEEE 802.11, também conhecida popularmente como redes Wi-Fi.

Endereço Físico MAC

A topologia lógica subjacente da Ethernet é um barramento de multiacesso, como já vimos em outros tópicos. Cada host de rede é conectado ao mesmo meio físico compartilhado, e todos os hosts estão recebendo todos os quadros transmitidos por um host de origem da informação, esse processo de envio para todas as máquinas de um segmento, é conhecido como broadcast. (STALLINGS, W. e ROSS K., 2010)

O problema é: se todos os dispositivos estiverem recebendo cada quadro, como cada dispositivo individual poderá identificar se é o destinatário pretendido sem a sobrecarga de ter que processar e desencapsular o quadro para chegar ao endereço IP? A questão se torna ainda mais problemática em grandes redes, com alto volume de tráfego, em que os quadros são encaminhados. (CISCO NETACAD, 2017)

Para evitar essa sobrecarga em excesso envolvida no processamento de cada frame, um identificador ou endereço exclusivo conhecido como endereço MAC foi desenvolvido para identificar os dispositivos de rede origem e destino dentro de uma rede ethernet. Um endereço MAC Ethernet é composto por um valor binário de 48 bits expresso em 12 dígitos hexadecimais (4 bits por dígito hexadecimal) e é dessa forma que ele é representado. (STALLINGS, W. e ROSS K., 2010)

Estrutura do Endereço MAC

Os endereços MAC devem ser globalmente exclusivos e seus valores são um resultado direto de regras impostas pelo IEEE a fornecedores para garantir endereços globalmente exclusivos identifiquem dispositivos de rede na Ethernet. Tais regras estabelecidas pelo IEEE exigem que todos os fornecedores e fabricantes que vendam dispositivos de rede Ethernet sejam registrados no IEEE.

O IEEE atribui a cada fabricante / fornecedor um código de 3 bytes (24 bits), chamado Identificador organizacionalmente exclusivo (OUI), exigindo que siga duas regras simples:

- Todos os endereços MAC atribuídos a uma placa de rede de um dispositivo Ethernet devem usar os três primeiros bits para identificar o OUI atribuído ao fornecedor.
- Todos os endereços MAC com o mesmo OUI, ou seja, fabricados pelo mesmo fornecedor, devem receber um valor exclusivo (código do fornecedor ou número de série) nos últimos 3 bytes, que identifica características próprias de quem fabrica.

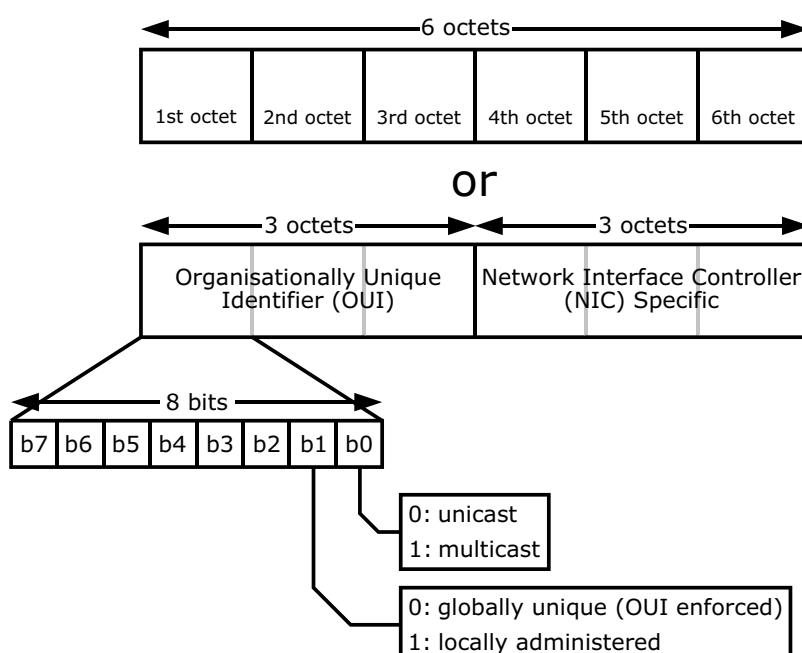


Figura 3 – Estrutura do endereço MAC

Processamento de um Quadro (Frame)

O endereço de enlace MAC também costuma ser conhecido como endereço gravado (BIA, burned-in address) por ser, historicamente, armazenado na memória ROM (Read-Only Memory – Memória Somente de Leitura) que está situada na placa de rede do host. Isso significa que o endereço é codificado no chip da ROM de uma forma permanente e ele não pode ser alterado por software.

Em Sistemas Operacionais e Placas de Rede instalada em alguns sistemas modernos, é possível alterar o endereço MAC via software. Isso é útil ao tentar obter acesso a uma rede que filtra dados com base no BIA; logo, filtrar ou controlar o tráfego com base no endereço MAC não é uma técnica tão segura e por esse motivo, não é visto com muita frequência. (TANENBAUM, A. S., 2011)

Os endereços MAC são atribuídos em vários dispositivos de rede, tais como servidores, estações de trabalho, impressoras, switches, pontos de acesso, roteadores e muitos outros. Todos os dispositivos conectados a uma rede LAN Ethernet têm uma ou várias interfaces identificadas com endereços MAC. Nesse caso, diferentes fabricantes de hardware e software podem representar o endereço MAC em diferentes formatos hexadecimais, que é a forma como tal endereço é apresentado. Os formatos do endereço MAC podem ser semelhantes aos seguintes exemplos:

- 00-05-9A-3C-78-00
- 00:05:9A:3C:78:00
- 0005.9A3C.7800

Quando um computador é inicializado, a primeira coisa que a placa de rede faz no processo de boot é copiar o endereço MAC da ROM na memória de trabalho RAM. Quando um dispositivo está encaminhando uma mensagem para uma rede Ethernet, ele anexa as informações do cabeçalho ao pacote. As informações do cabeçalho contêm o endereço MAC de origem e destino.

Cada placa de rede na rede exibe as informações na subcamada MAC, para ver se o endereço MAC destino no quadro corresponde ao endereço MAC físico do dispositivo armazenado na RAM. Se não houver correspondência, o dispositivo descartará o quadro. Quando o quadro chega ao destino onde o MAC da placa de rede corresponde ao MAC destino do quadro, a placa de rede passa o quadro para as camadas OSI, onde ocorre o processo de desencapsulamento. (CISCO NETACAD, 2017)

Encapsulamento Ethernet

Desde a criação do protocolo Ethernet no ano de 1973, os padrões evoluíram para especificar versões mais rápidas e flexíveis dessa tecnologia. A capacidade de a rede Ethernet melhorar sua evolução ao longo do tempo e sua característica de podem interligar dispositivos independentemente do tipo de hardware ou sistema ope-

racional utilizado, são um dos principais fatores de ela ter se tornado tão popular no mercado de tecnologia de informação. As primeiras versões da rede Ethernet eram relativamente lentas, com uma vazão de dados que não ultrapassava 10 Mbps. Já nas versões mais recentes desse protocolo podem operar a velocidades de vazão de 10 gigabits por segundo e 40 gigabits por segundo e ainda mais rápido, com o desenvolvimento das tecnologias de 100 gigabits por segundo. O cabeçalho e o finalizador do quadro Ethernet possui várias seções de informações usadas por tal protocolo, cada seção do frame é chamada de campo. (TANENBAUM, A. S., 2011)

Como mostrado na figura, há dois estilos de enquadramento de frames Ethernet:

- O padrão IEEE 802.3 Ethernet que foi atualizado várias vezes para incluir novas tecnologias de rede;
- O padrão DIX Ethernet que praticamente deu origem a este protocolo e que é conhecido como Ethernet II.

As diferenças entre os dois estilos de enquadramento Ethernet são mínimas. Sendo que a diferença mais significativa entre os dois padrões é a adição de um delimitador de início de quadro (SFD) e a alteração do campo Tipo que é indicado no Ethernet II e que muda para o campo de Comprimento no IEEE 802.3.

Tamanho do Quadro Ethernet

Ambos os padrões Ethernet II e IEEE 802.3 definem o tamanho mínimo de quadro como 64 bytes e o tamanho máximo como 1518 bytes. Isso incluía todos os bytes do campo Endereço MAC destino e origem, o campo controle e o campo Frame Check Sequence (FCS). Os campos Preâmbulo de 7 bytes e o campo Delimitador inicial de quadro de 1 byte, não são incluídos nessa conta total quando se descreve o tamanho de um frame. (TANENBAUM, A. S., 2011)

Todos os frames com comprimento inferior a 64 bytes são considerados um “fragmento de colisão” ou um “quadro desprezível” e por esse motivo são automaticamente descartados pelos dispositivos de rede na recepção.

O padrão IEEE 802.3ac, lançado em 1998, ampliou o tamanho máximo permitido de quadro para 1522 bytes. O tamanho do quadro aumentou para acomodar uma tecnologia chamada Rede de Área Local Virtual (Virtual Local Area Network - VLAN). As VLANs são criadas dentro de uma rede comutada e além disso, muitas tecnologias, como técnicas de Qualidade de serviço (QoS) aproveitam o campo de prioridade do usuário para executar vários níveis de serviço, como o serviço de prioridade para tráfego de voz, dados e outros.

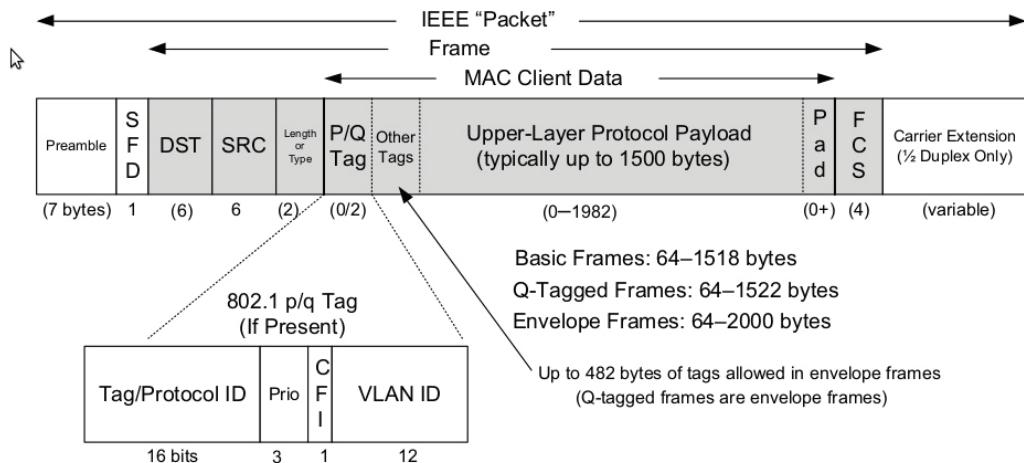


Figura 4 – Tamanho do quadro Ethernet

Na camada de enlace de dados, a estrutura do frame é praticamente idêntica aos protocolos estudados e na camada física, versões diferentes de Ethernet variam em seu método para detectar e colocar dados no meio físico utilizado.

Formato do Quadro Ethernet

Os campos principais no frame Ethernet são:

- **Campos Preâmbulo e Delimitador de Início de Quadro:** os campos Preâmbulo (7 bytes) e Delimitador de Início de Quadro (SFD), também conhecido como Início de Quadro (1 byte), são utilizados para a sincronização entre os dispositivos que participam do processo de transmissão. Esses primeiros oito bytes do quadro são usados para chamar a atenção dos dispositivos receptores da comunicação, fazendo com que se preparem para receber as informações de um novo frame.
- **Campo Endereço MAC Destino:** esse campo possui 6 bytes é o identificador de endereço de enlace do dispositivo destinatário. O endereço no quadro é comparado ao endereço MAC no dispositivo destino e se houver correspondência no endereçamento, o dispositivo aceitará o frame transmitido.
- **Campo Endereço MAC Origem:** esse campo possui 6 bytes identifica a placa de rede ou a interface do dispositivo de origem do frame, ou seja, o host que transmitiu a informação na rede.
- **Campo Comprimento:** em qualquer padrão IEEE 802.3 antes do ano de 1997, o campo Comprimento tem o objetivo de definir o comprimento exato do campo de dados do frame. Isso é usado posteriormente como parte do

FCS para garantir que a mensagem foi recebida corretamente. Caso contrário, o propósito do campo é descrever qual é o protocolo de camada superior existente. Se o valor de dois octetos for igual ou superior a 0x0600 hexadecimal ou 1536 decimal, o conteúdo do campo Dados será decodificado de acordo com o protocolo EtherType indicado. Considerando que, se o valor for igual a ou menor que 0x05DC hexadecimal ou 1500 decimal, o campo Comprimento será usado para indicar o uso do formato de quadro IEEE 802.3. É assim que os quadros Ethernet II e 802.3 são diferenciados. (CISCO NETACAD, 2017)

- **Campo Dados (Payload):** esse campo de tamanho variável de 46 a 1500 bytes, contém os dados encapsulados de um nível superior, que é uma PDU genérica conhecida como pacote IPv4 e que identifica o encapsulamento de Camada 3. Todos os frames a serem transmitidos precisam ter ao menos 64 bytes de comprimento mínimo, considerando os valores de overhead. Se um pacote com tamanho menor que o estabelecido for encapsulado, os bits adicionais chamados de pad serão utilizados e incluídos no campo de dados, afim de aumentar o tamanho do frame até seu tamanho mínimo para que o mesmo possa ser enviado.
- **Campo Sequência de Verificação de Quadro:** o campo Sequência de verificação de quadro (FCS) de tamanho de 4 bytes é utilizado para detectar erros em um frame. Ele utiliza uma verificação de redundância cíclica (CRC), sendo que o dispositivo emissor inclui os resultados calculados de uma CRC no campo FCS do frame. Já o dispositivo receptor recebe o frame e gera novamente um cálculo de CRC para buscar erros. Se o cálculo corresponder com o CRC incialmente enviado, significa que não ocorreu erro na transmissão. Já se os cálculos não corresponderem, é uma indicação de que os dados transmitidos foram alterados, e nesse caso o quadro será descartado.

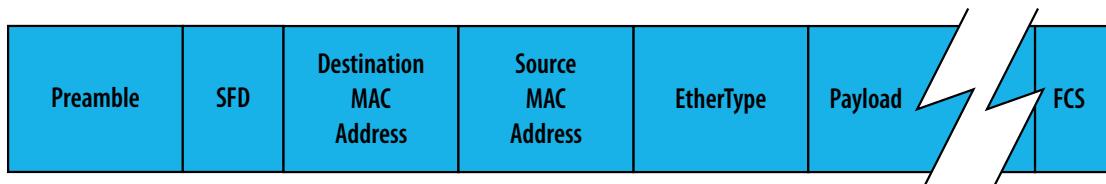


Figura 5 – Frame Ethernet genérico

Tipos de Endereços MAC

Em uma rede Ethernet utilizamos alguns tipos específicos de endereços, para que possamos transmitir dados a apenas um host, um grupo de hosts ou até mesmo todos os dispositivos de rede interligados em uma mesma rede.

Vamos conhecer esses tipos de endereços MAC:

- **Endereço de Unicast** – Um endereço MAC unicast é um tipo de endereço exclusivo utilizado quando um frame é enviado de um único dispositivo de rede transmissor para um único dispositivo de rede destino. Ou seja, de um para um equipamento.

No exemplo mostrado na figura, um host com endereço IP 192.168.1.5 (origem) solicita uma página Web do servidor no endereço IP 192.168.1.200. Para que um pacote unicast seja enviado e recebido, um endereço IP destino deve estar no cabeçalho do pacote IP. Um endereço MAC destino correspondente também deve estar presente no cabeçalho do quadro Ethernet. O endereço IP e o endereço MAC combinam para entregar dados a um host destino específico. (CISCO NETACAD, 2017)

- **Endereço de Multicast** – Os endereços de multicast permitem que um dispositivo origem envie um frame a um grupo de dispositivos dentro de uma rede. Dispositivos que pertencem a um grupo multicast recebem um endereço IP de grupo de multicast definido pelo órgão de administração da Internet conhecido como IANA. O intervalo de endereços de multicast IPv4 está entre os valores 224.0.0.0 a 239.255.255.255.

Como exemplo da utilização de endereços de multicast, poderíamos citar as aplicações de jogos remotos, em que muitos jogadores se conectam remotamente em uma mesma rede e reproduzem o mesmo jogo. Uma outra atividade seria a utilização de endereços multicast nas aplicações de ensino à distância com videoconferência, em que muitos alunos se conectam à mesma sala virtual de aula.

O endereço IP multicast exige um endereço MAC multicast correspondente para realmente entregar quadros em uma rede local. O endereço MAC multicast é um valor especial que começa com 01-00-5E em hexadecimal. A parte restante do endereço MAC multicast é criada pela conversão dos 23 bits inferiores do endereço IP do grupo multicast em 6 caracteres hexadecimais. Um exemplo, como mostrado na figura, é o endereço multicast hexadecimal 01-00-5E-00-00-C8. (CISCO NETACAD, 2017)

- **Endereço de Broadcast** – Um pacote que é enviado a todos os dispositivos em uma mesma rede, é conhecido como broadcast e possui um endereço IP destino que possui todos os valores 1 (um) na parte do host. Essa numeração no endereço significa que todos os hosts naquela rede local (domínio de broadcast) receberão e processarão o pacote enviado. Muitos protocolos de rede, como o DHCP e o Protocolo de Resolução de Endereços (ARP), utilizam envio em broadcasts.

Como mostrado na figura, um endereço IP de broadcast para uma rede necessita de um endereço MAC de broadcast correspondente no quadro Ethernet. Em redes Ethernet, o endereço MAC de broadcast é 48 valores uns exibidos como hexadecimal FF-FF-FF-FF-FF-FF. (CISCO NETACAD, 2017)

O Protocolo ARP

Como sabemos, cada host em uma rede IP tem um endereço MAC e um endereço IP origem e destino. Para que possamos enviar dados, os hosts devem utilizar esses dois endereços. O host deve usar seus próprios endereços MAC e IP nos campos origem e necessita identificar um endereço MAC e um endereço IP para

o destino. Enquanto o endereço IP destino será fornecido por uma camada OSI superior, como por exemplo um provedor de serviços ISP, o host origem precisará ter uma maneira para identificar o endereço MAC destino para um determinado link de Ethernet ou conectividade local. Essa é a finalidade do protocolo ARP na rede. Esse protocolo baseia-se em determinados tipos de mensagens de broadcast e mensagens unicast Ethernet, chamadas solicitações ARP e respostas ARP. O protocolo ARP fornece duas funções básicas:

- Resolver endereços de IPv4 para endereços MAC;
- Manter uma tabela de mapeamentos de endereços MAC.

Resolver Endereços IPv4 para Endereços MAC

Para que um frame seja adicionado no meio físico da rede local para ser transmitido, ele deverá possuir um endereço MAC de destino. Quando um pacote é enviado para a camada de enlace de dados para ser encapsulado em um frame, o nó se refere a uma tabela em sua memória RAM para encontrar o endereço de camada de enlace de dados mapeada para o endereço IPv4 destino. Essa tabela é chamada de Tabela ARP ou de cache ARP e tem a principal função de armazenada na RAM do dispositivo esses endereços por um tempo determinado pelo Sistema Operacional usado. (TANENBAUM, A. S., 2011)

Cada entrada, ou linha, da tabela ARP vincula um endereço IP a um endereço MAC. Chamamos o relacionamento entre os dois valores de mapa – isso significa simplesmente que você pode localizar um endereço IP na tabela e descobrir o endereço MAC correspondente. A tabela ARP salva temporariamente o mapeamento (coloca em cache) nos dispositivos na rede local, esse tempo depende do SO instalado e utilizado no dispositivo. (CISCO NETACAD, 2017)

Para iniciar o processo, um host de transmissão tenta localizar o endereço MAC mapeado para um destino IPv4. Se esse mapa for encontrado na tabela do equipamento, o host usará o endereço MAC como o MAC destino no quadro que encapsula o pacote IPv4. Em seguida, o quadro é codificado no meio físico da rede. (CISCO NETACAD, 2017)

Manutenção da Tabela ARP

A tabela ARP é mantida dinamicamente em um dispositivo de rede e existem duas formas para um host reunir e gravar endereços MAC nessa tabela. Uma forma é monitorar o tráfego que ocorre no segmento de rede local, como um host que recebe quadros do meio físico, nesse caso, ele pode registrar o IP origem e o endereço MAC relacionado como um mapeamento na tabela ARP, e a medida que os quadros são transmitidos, esse dispositivo preenche a tabela ARP com pares de endereços aprendidos. Outra forma de um dispositivo de rede adquirir um par de endereços é ao se enviar uma solicitação ARP, que é feita em broadcast de Camada 2 para todos os dispositivos de rede dentro de uma rede de área local Ethernet. (STALLINGS, W. e ROSS K., 2010)

A solicitação ARP contém o endereço IP do host destino e o endereço MAC de broadcast, FFFF.FFFF.FFFF. Como se trata de um broadcast, todos os nós em uma LAN Ethernet o receberemos e consultaremos seu conteúdo. O nó com o endereço IP que corresponde ao endereço IP da solicitação ARP responderá. A resposta será um quadro unicast que inclui o endereço MAC correspondente ao endereço IP da solicitação. Essa resposta é usada para fazer uma nova entrada na tabela ARP do nó emissor. As entradas na tabela ARP são carimbadas com data e hora da mesma forma que as entradas da tabela MAC são carimbadas com data e hora em switches. Se um dispositivo não receber um quadro de um dispositivo específico antes de o carimbo expirar, a entrada para esse dispositivo será removida da tabela ARP. (CISCO NETACAD, 2017)

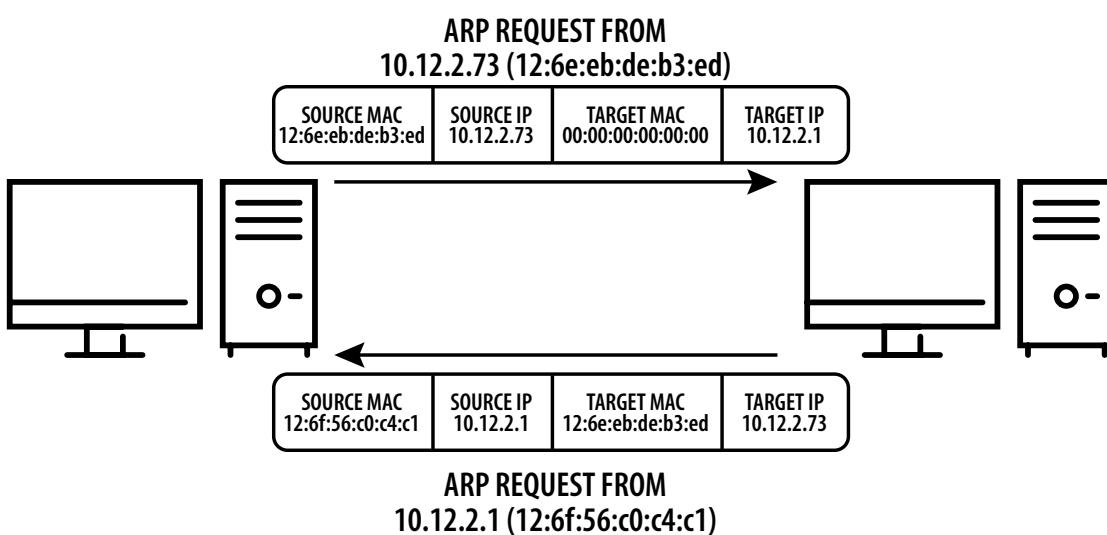


Figura 6 – ARP na conexão local

Além disso, as entradas de endereços estáticos (manualmente incluídos) podem ser inseridas em uma tabela ARP, apesar de não ser muito comum. Caso isso seja realizado, essas entradas não expiram com o tempo e devem ser removidas manualmente, da mesma forma que foram incluídas.

Função do ARP na Comunicação Remota

Todos os frames devem ser entregues a um host no segmento de rede local, caso esse host IPv4 esteja na mesma rede local. Se isso ocorrer, o host IPv4 usará o endereço MAC desse dispositivo como o endereço MAC destino. Se o host IPv4 destino não estiver na mesma rede local, o host origem precisará entregar o frame à interface do roteador que é o gateway ou o próximo salto da rede usado para alcançar o determinado destino. O host origem usará o endereço MAC do gateway como o endereço destino para quadros que contêm um pacote IPv4 endereçado aos hosts em outras redes. (CISCO NETACAD, 2017)

O endereço do gateway da interface de roteador, também é armazenado na configuração IPv4 dos hosts. Quando um host cria um pacote para um destino, ele compara o endereço IP destino e seu próprio endereço IP para determinar se os dois endereços IP estão localizados na mesma rede de Camada 3. Se o host de recebimento não estiver na mesma rede, a origem usa o processo ARP para determinar um endereço MAC para a interface do roteador servindo como o gateway. (CISCO NETACAD, 2017)

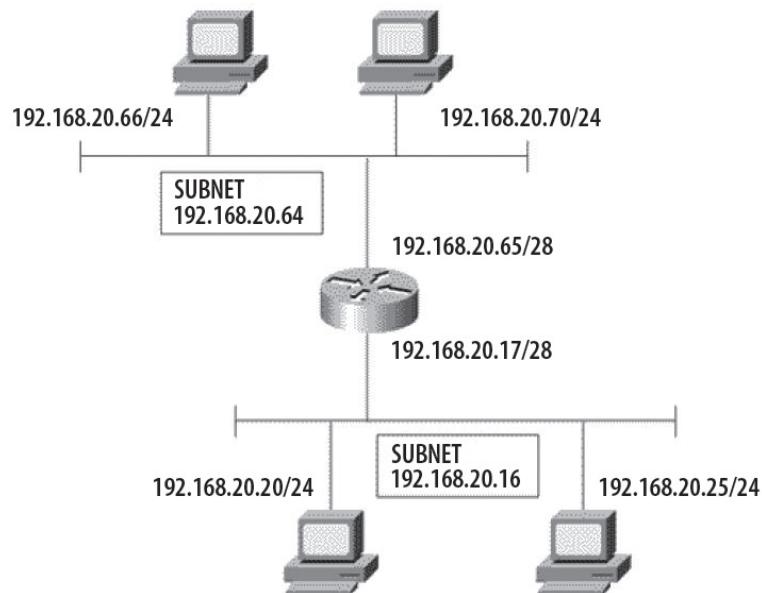


Figura 7 – ARP na conexão remota – ProxyARP

Caso a entrada do gateway não esteja na tabela de MAC, o processo ARP normalmente enviará uma solicitação ARP para recuperar o endereço MAC associado ao endereço IP da interface do roteador.

Material Complementar

Indicações para saber mais sobre os assuntos abordados nesta Unidade:

Sites

Curso WEB: CISCO NETACAD

Curso WEB: CISCO NETACAD – Módulo de Introdução a Redes – Capítulo 5: Ethernet.

<https://goo.gl/kSQz1K>

Livros

Redes de Computadores e a Internet

STALLINGS, W. e ROSS K. – Redes de Computadores e a Internet - 5^a Ed., Pearson, 2010.

Redes de Computadores

TANENBAUM, A. S. – Redes de Computadores – 5^a Ed., Pearson, 2011.

Referências

CISCO NETACAD – **Módulo de Introdução a Redes (CCNA1)** – 6^a Versão, Cisco Systems, 2017. (material on-line). Disponível em: <<https://www.netacad.com/pt-br>>

STALLINGS, W. e ROSS K. – **Redes de Computadores e a Internet** - 5^a Ed., Pearson, 2010.

TANENBAUM, A. S. – **Redes de Computadores** – 5^a Ed., Pearson, 2011.



Cruzeiro do Sul
Educacional