INTRODUÇÃO A REDES DE COMPUTADORES

CAPÍTULO 4 - QUE PADRÕES E TECNOLOGIAS SÃO ESSENCIAIS PARA O FUNCIONAMENTO DAS TELECOMUNCAÇÕES E REDES DE COMPUTADORES?

Josiane Boeira Kirinus Fernandes

Introdução

No mundo das redes de computadores, a comunicação ocorre constantemente entre equipamentos ou dispositivos em sistemas diferenciados. Equipamentos e dispositivos são dotados de capacidade para receber e lidar com informações. No entanto, esses equipamentos ou dispositivos não podem simplesmente enviar fluxos de *bits* para outros equipamentos ou dispositivos, esperando que sejam prontamente compreendidos. Para que a comunicação seja realizada, são necessárias tecnologias, processos, protocolos e padrões. Você sabe quais são essas tecnologias e padrões? Como elas funcionam? Qual é o seu papel para que redes de computadores e telecomunicações funcionem de forma adequada e eficiente?

Os protocolos realizam a definição de como, o que e quando deve acontecer a comunicação. Já os padrões são de extrema importância no desenvolvimento e na manutenção de um mercado aberto, que proporcione competitividade para os fabricantes de equipamentos ou dispositivos. Isso é essencial para se garantir a interoperabilidade nacional e internacional de dados e de tecnologias.

Este capítulo tem como objetivo apresentar, de forma mais detalhada, tecnologias pertencentes à camada de rede, que é a responsável pela entrega de pacotes desde o *host* de origem até o *host* de destino, como a fragmentação, NAT e endereços IPv6, com seu formato e funcionamento básico.

Também apresentará princípios e fundamentos básicos da camada de enlace de dados, transformando a camada física, de um meio de transmissão bruto em um *link*, que fornece confiabilidade. A camada de enlace de dados também é responsável por fazer a camada física parecer livre de erros para a camada superior, camada de rede.

Descreverá também protocolos auxiliares, como o ARP, utilizado para descobrir o endereço físico do nó, quando o endereço internet for conhecido e RARP, usado quando um computador é conectado a uma rede pela primeira vez.

E finalizando, será possível conhecer de forma mais detalhada a ethernet, tecnologia muito utilizada, pode-se dizer até preponderante nas LANs com fios.

Vamos conhecer esses novos fundamentos na área de redes de computadores?

Bons estudos!

4.1 NAT e Fragmentação

Para começar, vamos entender dois conceitos importantes de forma um pouco mais detalhada. Pense na seguinte situação: cada vez mais aumenta o número de usuários domésticos e de pequenas empresas que querem fazer parte da internet. Tempos atrás, para fazer parte da internet, um usuário fazia uso de uma linha discada, o que o deixava conectado por um tempo determinado. Clique na interação a seguir para continuar lendo.

A seguir, falaremos mais da tradução de endereços de rede. Acompanhe!

Um ISP (*Internet Service Provide*), ou seja, provedor de internet com um grupo de endereços, poderia fazer a alocação de um endereço, de forma dinâmica, a esse usuário. Um endereço era atribuído, ou seja, alocado a um usuário, quando era necessário. Agora a situação mudou.

Os usuários domésticos e empresas de porte menor podem ser conectadas por meio de uma linha ADSL (*Assymetrical Digital Subscriber Line*) ou *modem*. Além do mais, alguns usuários desenvolviam pequenas redes com vários computadores e necessitavam de um endereço IP para cada um desses computadores. Com a questão de falta de endereços, isso se tornou um problema sério. Qual a solução então?

A NAT (*Network Address Translation*), ou seja, tradução de endereços de redes, ela possibilita que um usuário tenha (de forma interna) um conjunto de endereços e de forma externa, um endereço apenas, ou um conjunto pequeno de endereços. E o que isso significa? Que o tráfego interno pode fazer uso do conjunto grande, já o tráfego externo faz uso do conjunto pequeno. Vamos entender isso melhor e também abordar a fragmentação.

4.1.1 Tradução de endereços de rede

Para que ocorra uma separação dos endereços usados internamente, em casa ou na empresa, os provedores de internet se baseiam em um conjunto chamado de endereços privados, que vemos na figura a seguir.

Intervalo	Total
10.0.0.0 a 10.255.255.255	2^{24}
172.16.0.0 a 172.31.255.255	2^{20}
192.168.0.0 a 192.168.255.255	2^{16}

Tabela 1 - Demonstração de endereços para redes privadas.
Fonte: FOROUZAN, 2008, p. 563.

Toda a organização ou instituição que desejar, pode usar um endereço desse conjunto sem necessidade de obter permissão dos seus provedores de internet. Esses endereços reservados são para redes privadas. Esses endereços são únicos dentro da empresa,

porém não são únicos de forma global. Um roteador não teria como encaminhar um pacote de dados que tenha esse endereço como endereço de destino.

VOCÊ QUER VER?

O filme *O quinto poder* (SINGER, 2013) é baseado na história do *site* Wikileaks e aborda a polêmica sobre o vazamento de documentos secretos dos Estados Unidos na internet. O filme mostra como funciona o prisma do funcionamento da internet, seus endereçamentos e da sua importância, para compartilhamento de informações.

A figura a seguir mostra o processo de utilização de uma NAT por um roteador. Esse roteador está localizado na casa de um usuário qualquer e tem uma interface, que faz parte da rede residencial, que se encontra do lado direto da figura. No endereçamento da rede residencial, observa-se que todas as quatro interfaces da rede têm o mesmo endereço de sub-rede, ou seja, 10.00.0/24. O espaço de endereço 10.0.0.0/8 representa uma das três partes do espaço de endereço IP, reservado para uma rede privada ou então um domínio com endereços privados, exatamente como a rede residencial da imagem.

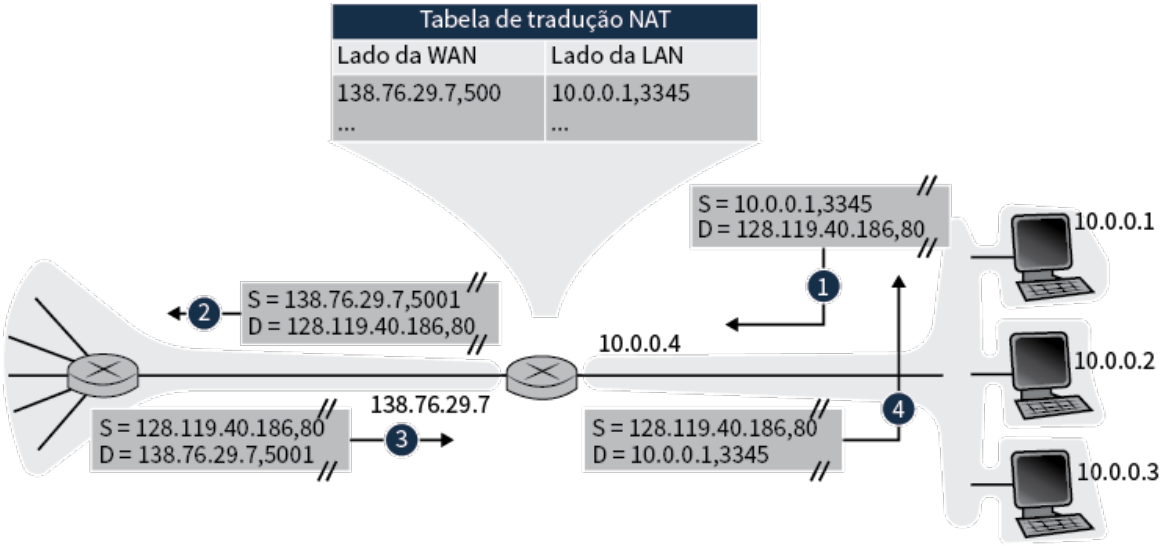


Figura 1 - Demonstração da operação de um roteador que faz uso da NAT, tradução de endereços de rede.
Fonte: KUROSE; ROSS, 2014, p. 261.

Um domínio com endereços privados está relacionado a uma rede onde os endereços somente podem ser compreendidos para equipamentos que fazem parte dessa rede.

VOCÊ SABIA?

Um domínio com endereços privados está relacionado a uma rede, e somente os endereços que fazem parte dela possuem significado para equipamentos e dispositivos. Já os endereços públicos são de unicidade global.

Segundo Forouzan (2008), o *site* deve ter somente uma única conexão para a internet global por meio de um roteador que executa o *software* NAT, como mostra a figura a

seguir, implementação simples da NAT.

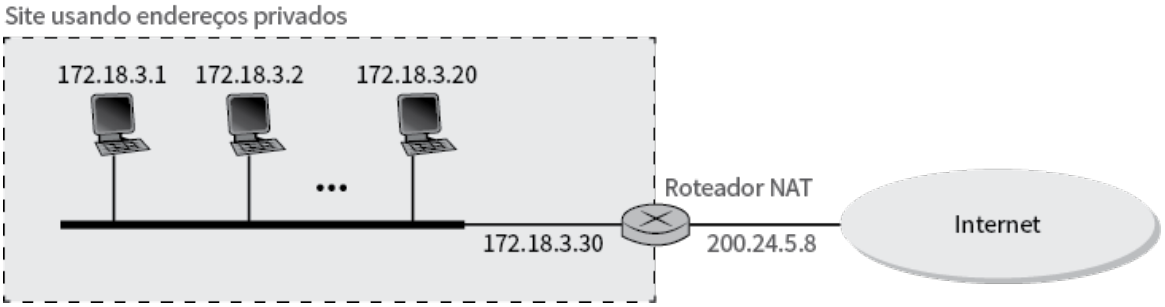


Figura 2 - Demonstração da implementação NAT (Networking Address Translation), ou seja, tradução de endereços de rede.
Fonte: FOROUZAN, 2008, p. 564.

Assim, na figura acima, vemos uma rede privada que faz uso de endereços privados. O roteador que faz a interligação da rede ao endereço global faz uso de um endereço privado e de um endereço global. A rede privada aparece de forma transparente para o restante da internet, já o restante dela consegue enxergar somente o roteador NAT com o endereço 200.24.5.8.

4.1.2 Fragmentação

Um datagrama consegue trafegar por diversas redes diferenciadas. Em cada roteador ocorre um desencapsulamento do datagrama IPv4, a partir do *frame* recebido por ele, ocorre o processamento e, então, o encapsula em um outro *frame*. Quanto ao formato e tamanho do *frame* recebido ocorre a dependência em função do protocolo usado pela camada física por meio do qual, o *frame* acabou de passar. Já o formato e o tamanho do *frame* irão depender do protocolo usado na camada física pela qual o *frame* realiza o tráfego. Para facilitar a compreensão, se por ventura um roteador faz a interligação de uma LAN a uma WAN, ele receberá um *frame* no formato da LAN e faz a transmissão no formato da WAN.
Cada protocolo da camada de enlace de dados possui seu próprio formato de *frame* e um dos campos estabelecidos no formato é o tamanho máximo do campo de dados, ou seja, no momento que o datagrama é encapsulado em um *frame*, o tamanho total do datagrama deve ser menor que esse tamanho máximo o qual é estabelecido pelas restrições exigidas pelo *hardware* e *software* utilizados na rede (figura a seguir).

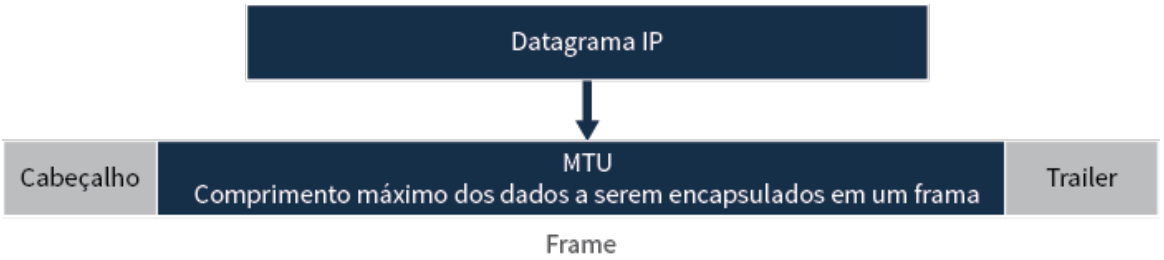


Figura 3 - Demonstração da Unidade de transferência máxima (MTU), campo.
Fonte: FOROUZAN, 2008, p. 590.

O valor da MTU (Unidade de Transferência Máxima) depende do protocolo associado à camada física (tabela a seguir).

Protocolo	MTU
HyperChannel	65.535
Token Ring (16 Mbps)	17.914
Token Ring (4 Mbps)	4.465
FDDI	4.352
Ethernet	1.500
X.25	576
PPP	296

Tabela 2 - Demonstração de unidades de transferência máxima para alguns tipos de redes.
Fonte: FOROUZAN, 2008, p. 590.

Para que o IPv4 fosse independente da rede física, o comprimento máximo de um datagrama IPv4 é equivalente a 65.535 *bytes*, tornando a transmissão eficientemente se for usado um protocolo com um MTU equivalente a esse tamanho. No entanto, o datagrama pode ser dividido para outras redes físicas, possibilitando sua passagem. Esse processo é chamado de fragmentação.
Normalmente, a origem não realiza a fragmentação de um pacote IPv4. Cabe à camada de transporte segmentar os dados num tamanho que fique adequado e, de certa forma, acomodado pelo IPv4 e a camada de enlace de dados em utilização.
No momento que um datagrama é fragmentado, cada um dos fragmentos tem seu

próprio cabeçalho com a grande maioria dos campos em repetição, porém alguns deles modificados. Um datagrama que já foi fragmentado pode sofrer fragmentação novamente no momento que ele se deparar com uma rede com MTU ainda menor. Um datagrama pode sofrer fragmentação diversas vezes, até que chegue no seu destino final.

Como ocorre a fragmentação no IPv4? Ele é fragmentado pelo *host* de origem ou então por qualquer roteador pertencente a rota, mesmo que exista uma tendência em limitar a fragmentação somente na origem. O processo de remontagem do datagrama é realizado apenas pelo *host* de destino, porque cada fragmento se tornou independente.

Um datagrama que foi fragmentado pode trafegar por diversas rotas diferenciadas e isso é algo sem um controle ou garantia de qual rota ele deve trafegar, entretanto, todos os fragmentos pertencentes ao mesmo datagrama chegam ao *host* de destino. Em função disso, que a remontagem ocorre no destino final. Existe um fator importante que pode impactar a remontagem dos pacotes durante a transmissão que é a perda de eficiência por ela.

No momento que um datagrama é fragmentado, partes necessárias do cabeçalho devem ter uma cópia em todos os fragmentos. Existe um capo de opção que pode ou nãos ser copiado. Quando um *host,* ou então, um roteador, fragmenta um datagrama, devem alterar os valores de três campos, são eles: *flags*; *offset* de fragmentação; e comprimento total. Os demais campos são copiados. O valor relacionado ao *checksun* é recalculado independentemente da fragmentação. Clique nas abas para saber mais sobre os campos.

- **Identificação**

  Esse campo possui 16 *bits* destinados à identificação do datagrama oriundo de um *host* de origem. É pela combinação da identificação e do endereço de origem do IPv4, que se define de maneira única e exclusiva um datagrama já que ele deixa o *host* de origem. Segundo FOROUZAN (2008), para que se tenha garantia dessa exclusividade, o protocolo IPv4 faz uso de um contador que realiza a identificação dos datagramas. Esse contador tem sua inicialização em um número positivo. No momento que o protocolo IPv4 faz o envio de um datagrama, ele faz a cópia do valor atual contido no contador para o campo de identificação e faz a incrementação do contador em 1. Se o contador for mantido na memória principal, a exclusividade também será garantida. No momento que um datagrama é fragmentado, o valor no campo de identificação é copiado para todos os fragmentos.

- ***Flags***

  Em um campo de 3 *bits*, sendo o primeiro reservado, o segundo é chamado de *bit* de não fragmentação. Caso o valor for igual a 1, o dispositivo não poderá fragmentar o datagrama. Segundo FOROUZAN (2008), se não for possível passar o datagrama por uma rede disponível, ele descarta o datagrama e realiza o envio de uma mensagem de erro ao *host* de origem. Agora se o valor for iguala 0, o datagrama pode ser fragmentado. O terceiro *bit* é denominado

de *bit* mais fragmentos, que se tiver valor 1 isso indica que esse datagrama não é o último fragmento e que existem mais após ele. Agora se seu valor for 0, significa que esse fragmento é o último ou então é o único fragmento.

- ***Offset* de fragmentação**

  É um campo de tamanho 13 *bits* com o objetivo de mostrar a posição relativa desse fragmento relacionado ao datagrama inteiro. É o *offset* dos dados no datagrama original medido em unidades de 8 *bytes*. Os bytes do datagrama original possuem numeração de 0 a 3.999. Segundo FOROUZAN (2008), o primeiro fragmento transporta os bytes 0 a 1.399, o offset para esse datagrama é 0/8=0; o segundo fragmento transporta os *bytes* 1.400 a 2.799, o valor de *offset* para esse fragmento é 1.400/8=175 e o terceiro fragmento transporta os *bytes* 2.800 a 3.999 e o valor de *offset* para esse fragmento é 2.800/8=350.

É importante lembrar que o valor de *offset* tem sua medida em unidades de 8 *bytes* em função que o comprimento do campo de *offset* ser de apenas 13 *bits* e não conseguir realizar a representação de uma sequência de *bytes* maior do 8.191, forçando *hosts* e roteadores que realizam a fragmentação de datagramas escolham um tamanho de fragmento no qual o número do primeiro *byte* possa ser dividido por 8.

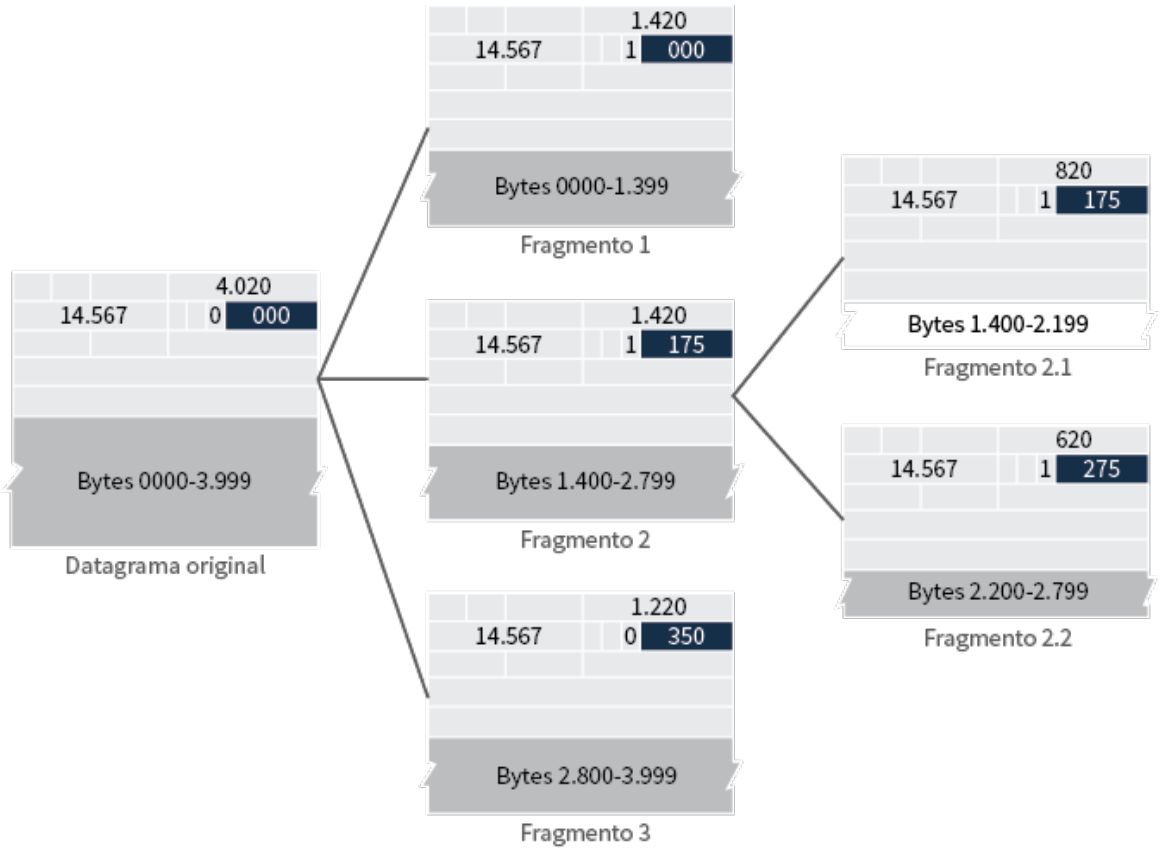


Figura 4 - Visão detalhada dos fragmentos onde o campo identificação é o mesmo em todos os fragmentos. O valor do campo flags com o bit mais ativo em todos os fragmentos, menos no último.
Fonte: FOROUZAN, 2008, p. 592.

Observe que a figura acima demonstra, também, o que acontece se o próprio fragmento for fragmentado novamente, aí o valor do campo *offset* é relacionado ao datagrama original. Para facilitar o entendimento, observe que, na figura, o segundo fragmento é dividido em dois fragmentos, de 800 e 600 *bytes*, entretanto o *offset* apresenta sua posição relacionada aos dados originais.
O próximo tópico explorará o protocolo IPv6, desenvolvido para superar deficiências do IPv4. Na versão 6 o IP foi modificado de forma extensa ara que a acomodação do crescimento da internet fosse possível.

4.1 IPv6

Segundo Kurose e Ross (2014), no início dos anos 1990, a IETF iniciou estudos para o desenvolvimento do sucessor do IPv4, que tinham como entendimento que o espaço de endereços IP de 32 *bits* estava ficando limitado, ou seja, ficando escasso, com novas sub-redes e nós IP sendo inseridos à internet e ainda recebendo endereços IP únicos e exclusivos, a uma velocidade muito acelerada. Então, para que essa necessidade de

maior espaço para endereços IP fosse atendida, um protocolo novo foi desenvolvido, o IPv6.

VOCÊ QUER LER?

O livro IPv6: o novo protocolo da internet (BRITO, 2013), abrange conceitos e fundamentos acerca da nova versão do protocolo IP, o IPv6, com endereços de 128 *bits*, expandindo o espaço de endereços para possibilitar o crescimento da internet, apresentando também vantagens, em relação ao IPv4.

Os desenvolvedores do IPv6 também realizaram ajustes e ampliaram outros fundamentos e aspectos do IPv4.
Quando todos os endereços IPv4 estivessem locados, ou seja, nenhuma sub-rede conseguiria se conectar à internet, foi o que impulsionou o debate em torno do assunto. Segundo Kurose e Ross (2014), o grupo de estudos da IETF tinha como estimativa que os endereços se esgotariam em 2008 e 2018, respectivamente. Em outra análise, a estimativa era que esgotassem em 2010. Embora essas estimativas e análises apontassem um tempo próximo para que esses endereços fossem exauridos, estava muito claro que era necessária uma nova tecnologia e o resultado é a especificação IP versão 6.

4.2.1 Formato do datagrama

O formato do IPv6 pode ser observado na figura a seguir. Mudanças foram acrescentadas nessa versão IPv6.

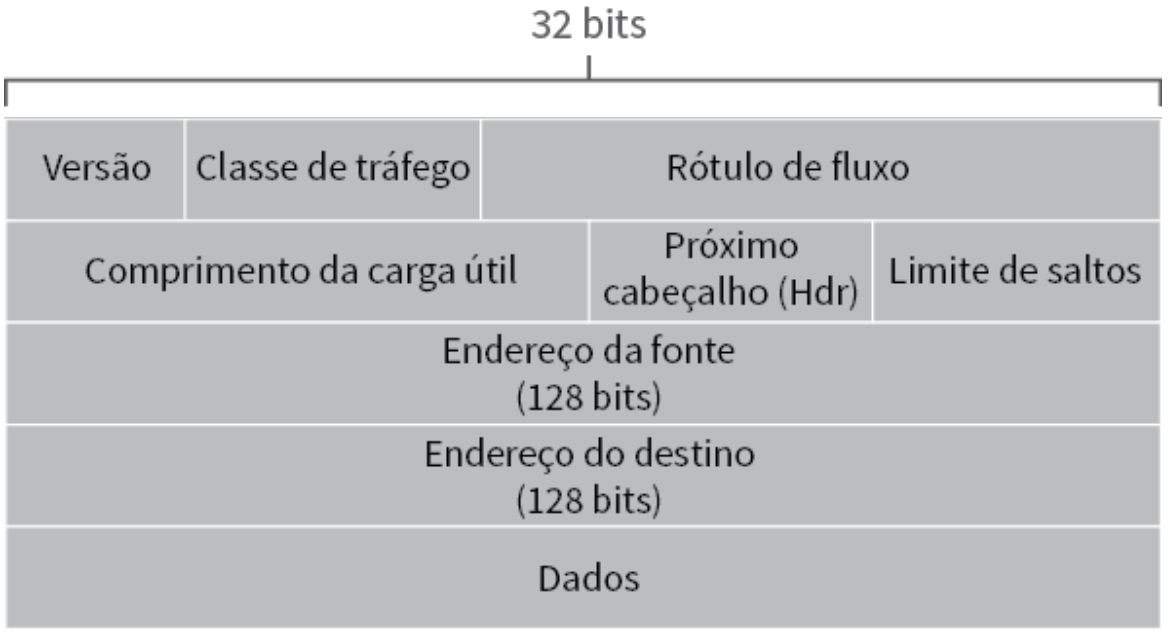


Figura 5 - Demonstração do formato do datagrama IPv6 de tamanho, no qual são acrescentados alguns campos.
Fonte: KUROSE; ROSS, 2014, p. 265.

As mudanças ocorridas na versão IPv6 são relacionadas a alguns pontos, como a capacidade de endereçamento ampliada. Por meio do IPv6 é possível o aumento do tamanho do endereço de 32 *bits* pata 128 *bits*. Isso permite que o planeta não fique sem endereços IP. Além de endereços *multicast* e *unicast*, o IPv6 consegue introduzir um tipo novo de endereço, chamado *anycast*. O *anycast* possibilita que um datagrama seja entregue a qualquer hospedeiro dentro de um conjunto.

VOCÊ SABIA?

Um endereço *unicast* faz a definição de um único computador. O pacote que é enviado a um endereço *unicast* deverá ser entregue somente a este computador determinado. Já o endereço *multicast* são utilizados para a definição de um conjunto de computadores, ao invés de somente um. Um pacote enviado para um endereço *multicast* deverá ser entregue a cada componente do conjunto.

Outra mudança está relacionada ao cabeçalho de 40 *bytes*. Campos do IPv4 foram descartados ou então tornaram-se opcionais. O cabeçalho de tamanho fixo de 40 *bytes* estipulado, proporciona processamentos mais acelerados do datagrama IP.
E, por fim, a rotulação de fluxo e prioridade, que no IPv6 tem uma definição ambígua de fluxo. Os desenvolvedores do IPv6 preveem uma necessidade possível de realizar a diferenciação de fluxos, ainda que o conceito de fluxo não tenha sido determinado. O cabeçalho IPv6 também possui um campo de 8 *bits* para a classe de tráfego. Esse campo, assim como o campo TOS do IPv4 pode ser utilizado para fornecer prioridade a determinados datagramas dentro de um fluxo ou a datagramas de determinadas aplicações, em relação a datagramas de outras aplicações.
A seguir são definidos os campos do IPv6. Clique para conhecê-los.

Versão	Campos de 4 *bits*, que é responsável por identificar o número da versão do IP. Para Kurose e Ross (2014, p. 266) “não é surpresa que o IPv6 tenha o valor 6 nesse campo, se colocar 4 nesse campo não criará um datagrama IPv4 válido”.
Classe de tráfego	Campo de 8 *bits* tem função semelhante à função do

	campo TOS do IPv4.
Rótulo de fluxo	É um campo com tamanho de 20 *bits* e é utilizado para a identificação de um fluxo de datagramas.
Comprimento de carga útil	Campo onde o valor de 16 *bits* é tratado como um número inteiro sem sinal que fornece o número de *bytes* no datagrama IPv6, que é seguido ao cabeçalho, que tem tamanho fixo de 40 *bytes*.
Próximo cabeçalho	A este campo é dotada a responsabilidade de identificação do protocolo al qual o conteúdo, ou seja, campo de dados do datagrama será entregue. Esse campo faz uso dos mesmos valores do campo de protocolo no cabeçalho IPv4.
Limite de dados	Este campo tem seu conteúdo decrementado de um para cada roteador que repassa o datagrama. Quando a contagem do limite de saltos for igual a zero, esse datagrama é descartado.

Endereços de fonte e de destino	Campo destinado a variados formatos do endereço de 128 *bits* do IPv6.
Dados	É o campo responsável pela carga útil do datagrama IPv6. No momento que o datagrama alcança seu destino, a carga útil pode ser retirada do datagrama IP e entregue adiante para o protocolo especificado no campo próximo cabeçalho.

Sabe-se que o protocolo da camada de rede no conjunto de protocolos TCP/IP é ainda hoje o IPv4, que fornece comunicação *host-host* entre sistemas na internet. De acordo com Forouzan (2008), ainda que o IPv4 tenha sido bem projetado, a comunicação dos dados implicou em uma evolução desde o surgimento do IPv4 nos anos 1970. Claro que, como foi mencionado anteriormente, o IPv4 apresenta algumas deficiências. E para que essas deficiências fossem sanadas é que o IPv6 foi estudado, proposto e atualmente é um padrão.

4.2.2 Funcionamento básico

Alguns conceitos são fundamentais para o entendimento do funcionamento do IPv6. O Campo *prioridade* em um pacote IPv6 faz a definição da prioridade de cada pacote em relação a outros pacotes de uma mesma origem. Para facilitar a compreensão, imagine se dois datagramas em sequência tiverem de ser descartados em função do congestionamento, o datagrama que foi sinalizado com a prioridade de pacote menor terá sua eliminação.

De acordo com Forouzan (2008), o tráfego do IPv6 possui duas categorias bastante amplas: controlado por congestionamento; e não controlado por congestionamento.

O tráfego controlado por congestionamento ocorre se a máquina origem consegue fazer a adaptação de um tráfego mais devagar, quando existe congestionamento. O TCP, que faz uso do protocolo de janela deslizante, pode fornecer resposta de forma fácil ao tráfego. No tráfego controlado por congestionamento é necessário ter o entendimento que os pacotes poderão, mesmo que de forma eventual, chegarem atrasados, sem estar na ordem correta ou até mesmo serem perdidos.

VOCÊ SABIA?

Os dados controlados por congestionamento recebem prioridades de 0 a 7. A prioridade 0 tem significado de menor prioridade e a prioridade 7 é a maior: 0 – nenhum tráfego específico; 1 – dados de segundo plano; 2 – tráfego de dados não atendido; 3 – reservado; 4 – tráfego de dados pesado atendido; 5 – reservado; 6 – tráfego interativo; 7 – tráfego de controle.

Já o tráfego não controlado por congestionamento faz referência a um tipo de tráfego que possui expectativa bastante reduzida de atraso. O descarte de pacotes é indesejável. Na maioria das vezes, a retransmissão é impossível de acontecer. O que isso significa? Clique na interação a seguir para saber a resposta desta pergunta!

Que a origem não faz a adaptação a situações de congestionamento. Exemplos desse tipo de tráfego são os vídeos e áudios em tempo real. Nele existe também as prioridades, que são baseadas na qualidade dos dados recebidos em relação a eliminação de pacotes. Os pacotes contendo menos redundância como áudios e vídeos de baixa fidelidade, podem receber prioridade 15. Já os dados contendo maior redundância como vídeos e áudios de alta fidelidade recebem prioridade 8. A tabela de referência para essas prioridades varia de 8 (dados com maior redundância) a 15 (dados com menor redundância).

Existe um processo chamado *Flow Label*, no qual uma sequência de pacotes, enviada de certa origem até um determinado destino necessita de tratamento especial da parte dos roteadores. É necessária a combinação do endereço de origem com o valor do rótulo de fluxo, ou seja, o *flow label* que faz a definição de forma exclusiva de um fluxo de pacotes.
Na visão de um roteador, fluxo é uma sequência de pacotes compartilhando as mesmas características, como tráfego pela mesma rota, uso dos mesmos recursos, possuir o mesmo nível de segurança, entre outras coisas.

Um roteador que consegue oferecer suporte e tratar os rótulos de fluxo,

disponibiliza uma tabela de referência de rótulos de fluxo, que apresenta uma entrada para cada rótulo de fluxo ativo e cada entrada faz a definição dos serviços requisitados pelo rótulo de fluxo correspondente. No momento em que o roteador faz o recebimento de um pacote, ele realiza uma consulta em sua tabela de rótulo de fluxo, para encontrar a entrada que corresponde ao valor de rótulo de fluxo que foi definido no pacote. Logo, o fornecimento ao pacote dos serviços disponibilizados na entrada. No entanto, se é possível notar, o rótulo de fluxo em si não realiza o fornecimento de informações para as entradas de sua tabela, essas informações são fornecidas por meio de outras formas, como opções nó a nó ou outros protocolos.

Até aqui, foi possível conhecer o funcionamento básico do IPv6. O próximo tópico apresentará fundamentos importante relacionados a camada de enlace de dados, responsável pela transformação da camada física.

4.3 Camada de enlace de dados

Na camada de enlace de dados existem dois tipos de canais de camada de enlace muito diferentes. O primeiro tipo se refere aos canais de *broadcast*, bastante comuns e conhecidos nas redes locais, as LANs, LANs sem fio, redes por satélite e as redes de acesso híbrido de cabo coaxial e de fibra. Relacionado ao canal de *broadcast*, hospedeiros são conectados no mesmo canal de comunicação e é necessário um protocolo que permita acesso ao meio para a coordenação de transmissões e para que se consiga evitar possíveis colisões entre quadros que são transmitidos. O outro tipo de canal de camada de enlace é o enlace de comunicação ponto a ponto, exatamente como o que existe entre dois roteadores ou, então, entre um *modem* residencial que funciona com uma linha discada e um roteador do provedor. Realizar a coordenação do acesso a um enlace ponto a ponto é simples, entretanto existem questões relevantes relacionadas ao enquadramento, transferir de forma confiável os dados, detectar de erros e controlar o fluxo.
Este tópico tem por objetivo apresentar fundamentos importantes do funcionamento da camada de enlace de dados.

4.3.1 Princípios da camada de enlace

Segundo Lima Filho (2015), a camada de enlace tem o propósito de prover uma maneira de realizar a ligação entre dois *hosts* para o envio e recebimento de datagramas. Também tem a função de prestar alguns serviços à camada superior, como detecção e correção de erros; endereçamento de datagramas após o encapsulamento de quadros, de acordo com o tipo de interface física usada; provimento de entrega confiável, quando o meio físico usado está sujeito a perdas de *bits* de informação; e controle de fluxo, para que o envio e o recebimento dos dados sejam compatibilizados, de acordo com as restrições de cada *host*.
A camada de enlace de dados tem como papel a transformação da camada física, que se trata de um recurso de transmissão bruto em um *link* com responsabilidade pela comunicação de dados nó a nó. Ela possui algumas responsabilidades entre elas o *framing*, endereçamento, controle de fluxo, controle de erros e controle de acesso ao

meio de transmissão.

Segundo FOROUZAN (2008), a camada de enlace de dados faz a divisão do fluxo de *bits* recebidos da camada de rede em unidades de dados gerenciáveis que são chamadas de *frame*s. A camada de enlace faz o acréscimo de um cabeçalho ao *frame* para a definição dos endereços de quem envia e de quem recebe. Se, por ventura, a velocidade com que os dados podem ser sorvidos na recepção for menor que a velocidade na qual os dados são gerados na emissão, a camada de enlace faz uma imposição de mecanismos para controlar o fluxo para que se evite que o receptor possa sofrer uma sobrecarga.

A camada de enlace de dados também consegue acrescentar confiabilidade à camada física incorporando mecanismos para detectar e retransmitir *frame*s que posam ser corrompidos, ou então duplicados e até perdidos. No momento que dois ou mais equipamentos são conectados a um mesmo *link*, se faz necessário protocolos para a determinação de qual equipamento vai possuir o controle sobre o *link* em determinado instante.

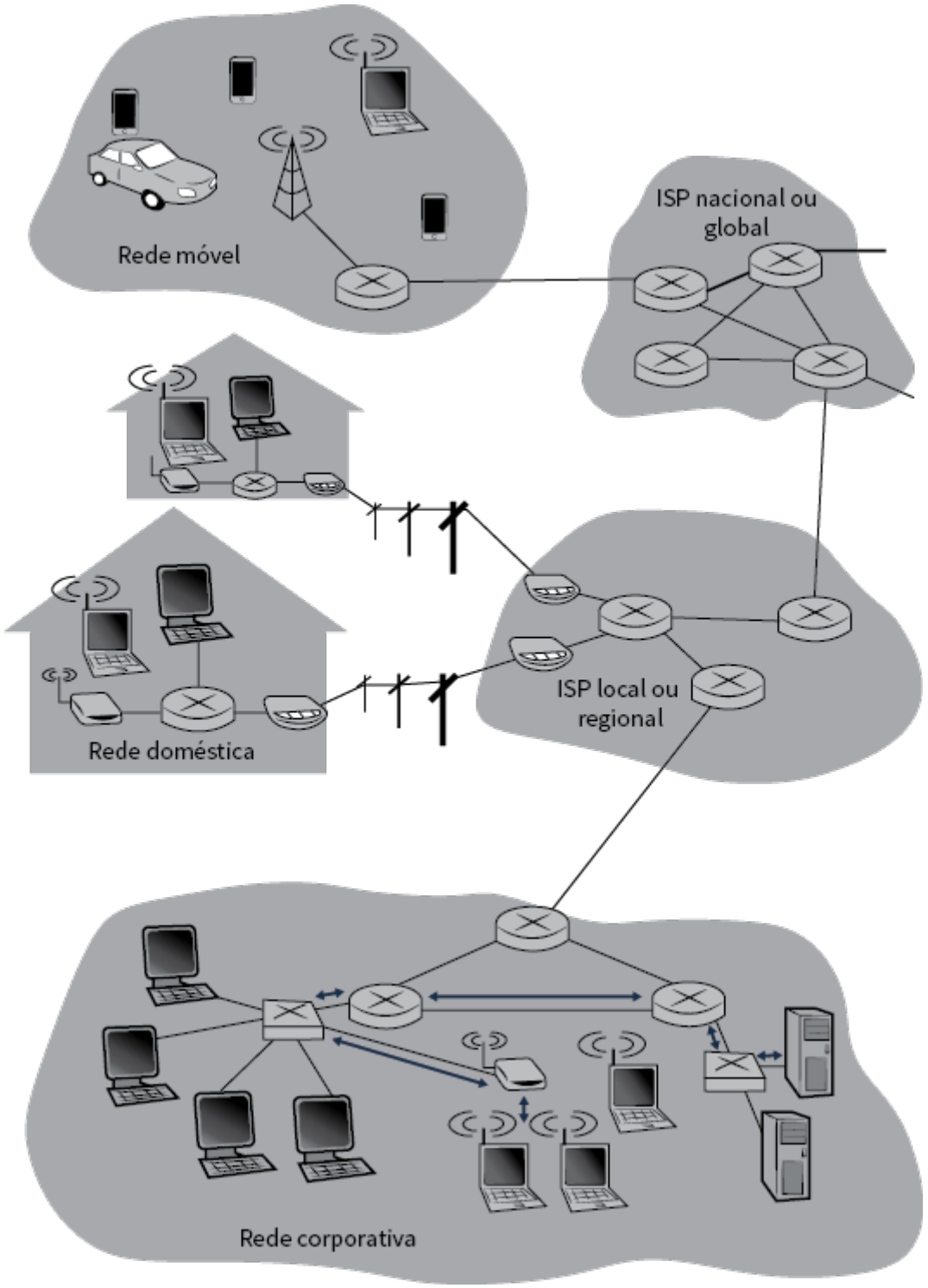


Figura 6 - A camada de enlace de dados.
Fonte: KUROSE; ROSS, 2014, p. 323.

Antes de prosseguir, é importante analisar alguns termos para o bom andamento da leitura deste tópico. Hospedeiros e roteadores terão como referência o termo “nós” e os

canais de comunicação que fazem a conexão entre os nós no decorrer dos caminhos de comunicação serão chamados de “enlaces”. Para que um datagrama vá de um hospedeiro origem, até um hospedeiro destino, esse datagrama precisa ser transportado sobre cada um dos enlaces individuais, que estiverem ao longo do caminho fim a fim. Se for considerado um determinado enlace, um nó faz o encapsulamento do datagrama em um quadro de camada de enlace e realiza a transmissão do quadro para dentro do enlace e um nó receptor faz o recebimento do quadro e também a extração do datagrama.

Um protocolo pertencente à camada de enlace é utilizado para o transporte de um datagrama por um enlace individual. O protocolo de camada de enlace realiza a definição do formato dos pacotes trocados entre os nós que estão nas extremidades do enlace, assim como as ações realizadas por esses nós ao fazer o envio e recebimento de pacotes.

Sabe-se que a camada de rede tem como objetivo o movimento dos segmentos da camada de transporte fim a fim, desde o hospedeiro de origem até o hospedeiro de destino já um protocolo de camada de enlace é responsável pelo movimento de datagramas de camada de rede nó a nó por meio de um único enlace no caminho. A camada de enlace possui uma característica importante que é que se refere a um datagrama que pode ser transportado por diferenciados protocolos de enlace nos diferentes enlaces no caminho. Para facilitar a compreensão, Kurose e Ross (2014) apresentam um exemplo, um datagrama pode ser transportado pelo protocolo Ethernet no primeiro enlace, pelo PPP no último enlace e por um protocolo WAN de camada de enlace nos enlaces intermediários. Os referidos autores também ressaltam que é importante notar que os serviços que são fornecidos pelos protocolos de camada de enlace podem ser diferentes.

Um protocolo de camada de enlace pode prover, ou não, entrega confiável. Portanto, a camada de rede deve ter a capacidade de realização de sua tarefa fim a fim, em face de um grupo heterogêneo de serviços individuais de camada de enlace.

4.3.2 ARP e RARP

Existem endereços de camada de rede como os endereços IP da internet e endereços de camada de enlace, os endereços MAC (*Media Access Control*) se fazem necessários na realização da tradução de um para o outro. E para a internet está é a atribuição do protocolo denominado protocolo de resolução de endereços, o ARP (*Address Resolution Protocol*).

Para o entendimento da necessidade de utilização de um protocolo, tal qual o ARP, considere a figura a seguir.

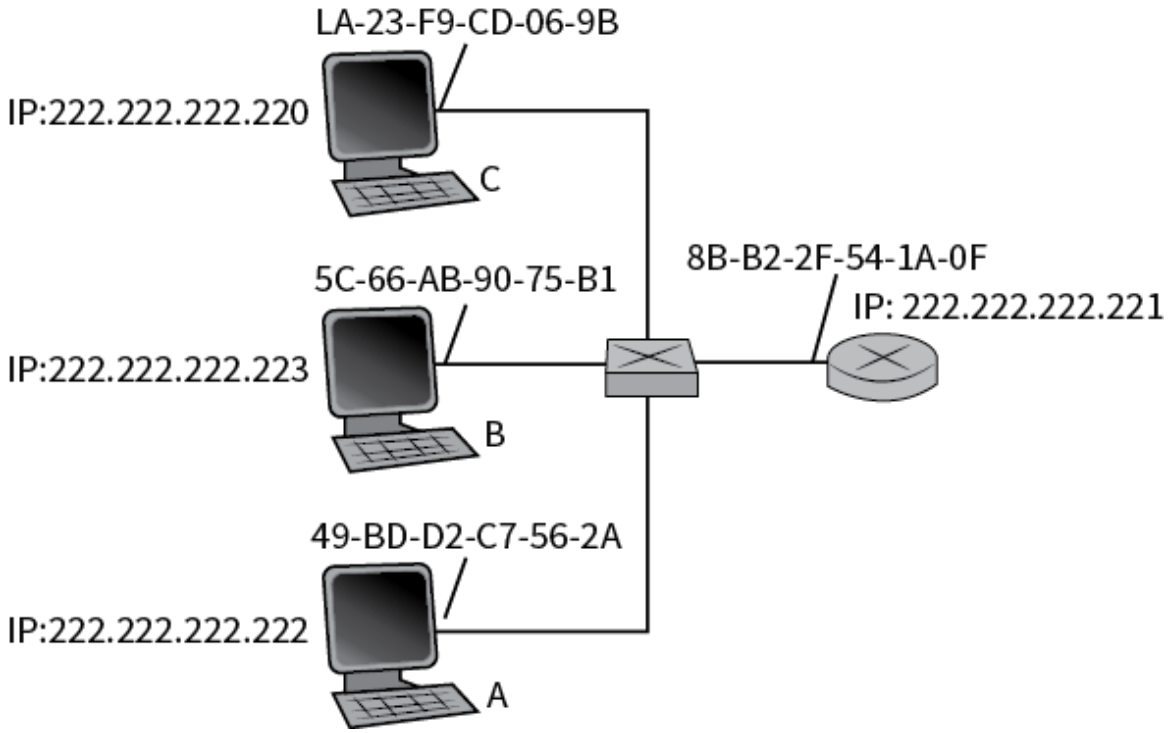


Figura 7 - Demonstração onde cada nó em uma LAN tem um endereço IP e o adaptador de cada nó tem um endereço MAC.
Fonte: KUROSE; ROSS, 2014, p. 345.

Observe que na figura acima, cada nó apresenta seu endereço IP único e o adaptador de cada nó apresenta seu endereço MAC único. Os endereços IP não apresentados em notação decimal com pontos e endereços MAC, em notação hexadecimal. Imagine que o nó 222.222.222.220 precise enviar um datagrama IP para o nó 222.222.222.222. Nesta situação, apresentada na figura acima, tanto o nó de origem, quanto o nó de destino pertencem à mesma rede (LAN). Para que o envio de um datagrama ocorra, o nó de origem deve fornecer a seu adaptador o endereço IP e o endereço MAC para o nó de destino 222.222.222.222. O adaptador do nó que envia, faz a montagem de um quadro de camada de enlace, no qual contém o endereço MAC de quem recebe e faz o envio desse quadro para dentro da rede. Uma questão importante de se ressaltar é relacionada ao modo, ou seja, a forma como o nó que faz o envio determina o endereço MAC para o nó de endereço IP 222.222.222.222, por meio da ARP. E como é realizado esse processo? Clique na interação a seguir para ler!

Segundo Forouzan (2018), a máquina pode obter seu endereço físico localmente exclusivo. Logo depois, pode usar seu endereço físico para a obtenção de endereço lógico, fazendo uso do protocolo RARP. Para tanto, será criada e transmitida uma solicitação RARP na rede local. Outra máquina de rede local, que conheça todos os endereços, retornará com uma resposta RARP. A máquina requisitante deve executar um programa RARP *Client*; a máquina que retorna com a resposta tem que executar um programa RARP *Server*.

Um módulo ARP que fica no nó de quem faz o envio toma como entrada qualquer endereço IP na mesma rede e faz o retorno do endereço MAC equivalente. No mesmo exemplo acima, que foi citado por Kurose e Ross (2014), o nó de quem envia 222.222.222.220 disponibiliza, a seu módulo ARP, o endereço IP 222.222.222.222 e o módulo ARP regressa o endereço MAC equivalente, ou seja, 49-BD-D2-C7-56-2A.

O RARP (*Reverse Address Resolution Protocol*), ou seja, protocolo de resolução de endereço reverso, tem como propósito o mapeamento do endereço lógico de uma máquina partindo de seu endereço físico. Cada *host* ou roteador recebe um ou mais endereços lógicos, IP, que são endereços únicos, exclusivos e independentes do endereço físico, ou seja, *hardware* da máquina. Para a criação de um datagrama IP, um *host* ou roteador necessita ter o conhecimento do seu próprio endereço IP. O endereço IP de uma máquina quase sempre pode ser lido de um arquivo de configuração armazenado em um arquivo em disco.

s MAC, eles não conseguiriam suportar com facilidade outros protocolos de camada de rede, como, por exemplo, o IPX ou DECNet.

Em segundo lugar, se os adaptadores usassem endereços de camada de rede, ao invés de endereços MAC, o endereço de camada de rede teria de ser armazenado na RAM do adaptador e reconfigurado, toda vez

que o adaptador mudasse de local ou, mesmo, fosse ligado.

Uma outra alternativa seria não usar nenhum endereço nos adaptadores e fazer com que cada um deles passe os dados, caracteristicamente, datagrama IP, de cada quadro que recebe para cima da pilha de protocolos. A camada de rede poderia, então, verificar se o endereço

combina com o endereço da camada de rede. No entanto, existe um problema com essa alternativa que é que o nó pai seria interrompido por cada quadro enviado à rede (LAN), bem como por quadros destinados a outros nós na mesma LAN *broadcast* (KUROSE; ROSS, 2014).

Sintetizando, para que as camadas sejam blocos construtivos em grande parte independentes na arquitetura de uma rede, muitas delas precisam ter seu próprio

esquema de endereços.
Foi possível, neste tópico, perceber que a ARP consegue converter um endereço IP para um endereço MAC. Em alguns pontos, a ARP é semelhante ao DNS, que faz a conversão de nomes de hospedeiros para endereços IP. Entretanto, existe uma diferença importante entre os dois conversores é que o DNS realiza a conversão de nomes de hospedeiros para máquinas que estejam em qualquer lugar da internet, já a ARP faz a conversão de endereços IP somente para os nós na mesma sub-rede.
Neste tópico foi possível conhecer um pouco mais da camada de enlace de dados e dos serviços/recursos por ela fornecidos. O próximo tópico abordará uma tecnologia predominante nas redes locais com fios, a ethernet.

4.4 Ethernet

Pode-se dizer que a ethernet praticamente invadiu o mercado de LANs com fio. Segundo Kurose e Ross (2014), na década de 1980 e início da década de 1990, havia muitos desafios de outras tecnologias LAN, entre elas *token ring*, FDDI e ATM. Algumas dessas tecnologias conseguiram conquistar uma parte do mercado das LANs durante alguns anos. Porém, desde seu desenvolvimento, nos anos 1970, a ethernet continuou se desenvolvendo, cresceu e continuou sua posição de destaque no mercado. Atualmente ela é a tecnologia predominante de LAN com fio e, provavelmente, continue sendo. A ethernet é para rede local o que a internet é para rede global.
A LAN Ethernet original foi projetada na década de 1970 pelos engenheiros Bob Metcalfe e David Boggs.

VOCÊ O CONHECE?

O engenheiro Bob Metcalfe nasceu em 1946 nos Estados Unidos e foi um pioneiro no desenvolvimento de tecnologias como a ethernet, da qual foi co-inventor junto com o colega David Boggs. Recebeu vários prêmios durante sua carreira. Quando fazia doutorado na Universidade Harvard, no início dos anos 1970, ele trabalhava na ARPANET, no M.I.T. A ethernet original de Metcalfe e Boggs executava a 2,94 *Mbps* e interligava até 256 hospedeiros em uma distância de até 1,5 km.

Alguns motivos pelos quais persiste o sucesso da ethernet tem a ver com ela ter sido a primeira LAN de alta velocidade amplamente difundida e com disseminação. Quando uma nova tecnologia de rede surgia, os gerentes preferiam não mudar pois elas tinham maior complexidade de custo mais alto, como *token ring*, FDDI e ATM. Mas a ehternet surgiu como uma alternativa mais simples e barata que suas concorrentes.
Nos próximos tópicos vamos conhecer um pouco mais a fundo o formato e o funcionamento básico da ethernet.

4.4.1 CSMA/CD

No momento em que os nós estão interconectados em dispositivo como o *hub*, a LAN ethernet é uma LAN de *broadcast*, ou seja, quando um adaptador realiza a transmissão de um quadro, todos os adaptadores na LAN conseguem receber o quadro. Empregando o *broadcast*, a ethernet necessita de um protocolo capaz de realizar acesso múltiplo, isto é, ela faz uso de um protocolo de acesso múltiplo denominado CSMA/CD. E como ele trabalha? De acordo com Kurose e Ross (2014), realiza os passos a seguir.

- Um adaptador está apto a iniciar a transmissão a qualquer momento, ou seja, não existe noção de compartilhamentos de tempos.
- Um adaptador nunca transmitirá um quadro, quando faz a percepção que algum outro adaptador está realizando a transmissão, isto é, ele faz uso de detecção de portadora.
- Um adaptador que está realizando a transmissão faz o abortamento de sua transmissão no momento que percebe que algum outro adaptador está realizando a transmissão, isto é, faz uso de detecção de colisões.
- Antes de realizar a tentativa de uma retransmissão, um adaptador aguarda um certo espaço de tempo que de certa forma é pequeno, se comparado com o tempo de uma transmissão de um quadro.

Cada adaptador realiza a execução do protocolo CSMA/CD, sem a necessidade de coordenação ou combinação com demais adaptadores na ethernet. Internamente, um determinado adaptador realiza o funcionamento do protocolo CSMA/CD de uma forma que podemos listar a seguir. Clique nos números.

1

O adaptador faz a obtenção de um datagrama de camada de rede de seu nó pai e realiza a preparação de um quadro ethernet e o insere no *buffer* do adaptador.

2

Caso o adaptador realize a percepção de que o canal está em ociosidade, ele inicia a transmissão do quadro. Caso o adaptador consiga perceber que o canal está em ocupação, faz a espera até que consiga perceber que não existe nenhuma energia de sinal.

3

Durante o tempo que realiza a transmissão, o adaptador faz um monitoramento da presença de energia de sinal que vem de outros adaptadores. Caso o adaptador realize a transmissão do quadro inteiro sem detecção de energia de sinal, que vem de outros

adaptadores, ele faz a consideração de conclusão da operação com o quadro.

4

Caso o adaptador consiga detectar energia de sinal que vem de outros adaptadores, no momento que está transmitindo, ele para de transmitir seu quadro e, no lugar dele, realizará a transmissão de um sinal de reforço de colisão de 48 horas.

5

Após o abortamento, o adaptador passa para a fase de *backoff* exponencial. De forma específica, no momento que está realizando a transmissão de um determinado quadro, depois de passar pela enésima colisão em seguida para esse quadro, o adaptador realiza a escolha de um valor para K de forma aleatório de (0, 1, 2, ..., $2^m - 1$), onde m = min (n, 10). O datagrama faz uma espera de k . 512 tempos de *bits* e então faz o retorno à etapa 2.

Questões importantes sobre o CSMA/CD necessitam ser abordadas. Existe um intuito do sinal de reforço de colisão como garantia de que todos os outros adaptadores que estejam em transmissão tenham consciência da colisão.

4.4.2 Formato do quadro ethernet

O *frame* ethernet possui sete campos. De acordo com Forouzan (2008), são eles: preâmbulo, SFD, endereço de destino, endereço de origem, comprimento ou tipo de PDU, Dados e preenchimento e CRC. A ethernet não disponibiliza mecanismos capazes de realizar reconhecimento de *frame*s recebidos, tornando-a um meio conhecido como não confiável. As confirmações devem ser implementadas nas camadas superiores. O formato do *frame* MAC é apresentado na figura a seguir.

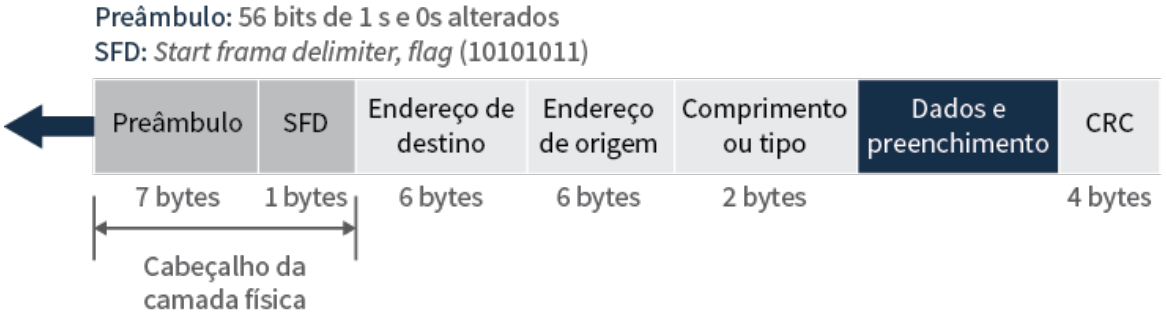


Figura 8 - Demonstração do formato do frame ethernet e seus sete campos: preâmbulo, SFD, endereço de destino, endereço de origem, comprimento, dados e preenchimento e CRC.
Fonte: FOROUZAN, 2008, p. 398.

Veja a descrição de todos os campos a seguir, clicando nas abas.

Preâmbulo

O campo Preâmbulo é o primeiro campo de um *frame* MAC 802.3 possui 7 *bytes*, ou seja, 56 *bits*, que são formados por *bits* 0s e 1s, de forma alternada, que são responsáveis por alertar o receptor sobre o *frame* que está chegando e também habilitar a realização da sincronização do seu *clock* de entrada. O padrão de 56 *bits* permite que as estações possam perder alguns *bits* do início do *frame*. Esse campo preâmbulo é, na verdade, adicionado à camada física e, de forma formal, não pertence ao *frame*.

SFD

O segundo campo é SFD (*Start Frame Delimiter*) de tamanho de 1 *byte*: 10101011 e é capaz de anunciar o início de um *frame*. O SFD (delimitador de início de *frame*) consegue emitir alerta à estação ou estações, quanto à última oportunidade para a realização da sincronização. Os dois últimos *bits*, ou seja, 11 avisam o receptor que o próximo campo será o endereço de destino.

Endereço de Destino

O campo de Endereço de Destino (DA – *Destination Address*) possui 6 *bytes* de comprimento e possui o endereço físico da estação ou, então, estações de destino que deverão receber o pacote.

Endereço de Origem

O Campo de Endereço de Origem (SA – *Source Address*) também possui tamanho de 6 *bytes* e é responsável por conter o endereço físico de quem envia o pacote.

Comprimento

O campo comprimento, ou tipo, é determinado como o campo de tipo ou de comprimento. A ethernet-padrão fazia uso desse campo para a definição do protocolo da camada superior que foi encapsulado pelo *frame* MAC.

Dados

O campo dados tem o papel de realizar o transporte de dados encapsulados, oriundos dos protocolos das camadas superiores. Esse campo apresenta um mínimo de 46 *bytes* e um máximo de 1.500 *bytes* de tamanho.

CRC

O campo CRC é o último campo e tem a capacidade de conter as informações para a realização da detecção de erros.

Após a apresentação dos campos que compõem um *frame* ethernet, é importante ressaltar que ele necessita ter um comprimento mínimo de 512 *bits*, ou seja, 64 *bytes*, que parte desse comprimento é destinado ao cabeçalho e ao trailer.

4.4.3 Funcionamento básico da ethernet

A LAN Ethernet original fazia uso de barramento coaxial para a interconexão dos nós. As topologias de barramento da ethernet permaneceram por todos os anos 1980 até meados dos anos 1990. Com uma topologia de barramento, a ethernet é uma transmissão LAN de *broadcast*, ou seja, todos os quadros em transmissão movimentam-se para, e são executados por todos os adaptadores que estão conectados nesse barramento.

Já para o final dos anos 1990, grande parte das empresas e universidades já tinha realizada a substituição de suas LANs com instalação ethernet, fazendo uso da topologia estrela, aquela em que um *hub*, repetidor. Nesse tipo de topologia os hospedeiros e também o roteador estão conectados de forma direta a um *hub* por meio de um cabo de pares de cobre. Mas o que é um *hub*? É um equipamento de camada física que consegue agir em *bits* de forma individual e não em quadros. No momento que um *bit*, representando 0 ou 1, faz a chegada em uma interface, o *hub* faz a recriação do *bit*, faz um aumento da energia e realiza a transmissão do *bit* para todas as outras interfaces. Desta forma, ethernet com uma topologia estrela baseada em um *hub* também é uma LAN de *broadcast*, sendo assim, toda vez que um *hub* faz o recebimento de um *bit* de uma das interfaces, ela faz o envio de uma cópia para todas as outras interfaces. No caso de um *hub* receber quadros de duas interfaces diferenciadas ao mesmo tempo, acontece uma colisão e os nós que tinham criado os quadros precisam realizar a retransmissão.

VOCÊ QUER LER?

O livro “Novas Tecnologias de Redes Ethernet” (ENNE; WANDERLEI; FERRAZ, 2017) foi desenvolvido por engenheiros de telecomunicações com enorme experiência em redes. Se você quer se aprofundar em conceitos e fundamentos necessários para a compreensão da tecnologia ethernet, esse é o livro indicado.

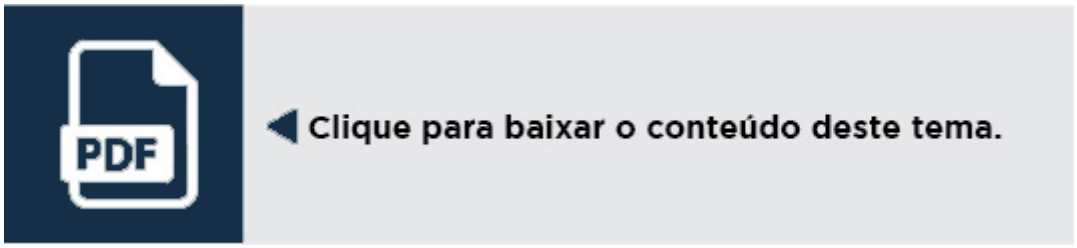
Kurose e Ross (2014) enfatizam que, no início dos anos 2000, a ethernet sofreu uma grande transformação, suas instalações continuaram no formato estrela, entretanto, um comutador (*switch*) substituiu o *hub* no núcleo. Esse dispositivo comutador é preparado para que não ocorra colisões. O comutador difere dos roteadores na questão de

operação, ou seja, roteadores operam até a camada três e os comutadores operam até a camada dois.

Síntese

Chegamos ao final deste capítulo! Vimos conteúdos fundamentais para os estudos sobre redes, como a NAT, Tradução de Endereços de Redes, tecnologia capaz de permitir que usuários possuam, internamente, um grande conjunto de endereços e, externamente, um endereço ou, então, um conjunto pequeno de endereços, e a fragmentação, na qual, dependendo do tipo de rede física é necessária a divisão do datagrama, para que seja possível sua passagem. Também foi possível conhecer de forma um pouco mais detalhada o funcionamento do IPv6, cuja motivação para essa nova versão surgiu para lidar com o esgotamento do espaço de endereços IP.
Outro ponto de destaque foi a camada de enlace de dados, com seus princípios de funcionamentos bem como os protocolos ARP e RARP.
E, finalmente, a apresentação da ethernet e redes de acesso múltiplo, tecnologia que domina o mercado de redes locais e que possibilita que um conjunto de nós consiga enviar e receber quadros por meio de um enlace compartilhado.
Neste capítulo, você teve a oportunidade de:

- introduzir termos, terminologias e conceitos básicos sobre telecomunicações e redes;
- fornecer ao aluno uma visão geral sobre a arquitetura OSI e TCP/IP;
- identificar e compreender todas as camadas e as suas funções no modelo de referência OSI e na arquitetura TCP/IP.



Bibliografia

BRITO, S. H. B. **IPv6: o novo protocolo da internet.** São Paulo: Novatec, 2013.
ENNE, A. J. F.; WANDERLEY, B. L.; FERRAZ, C. H. **Tecnologias de Redes Ethernet.** Rio de Janeiro: Elsevier, 2017.
FOROUZAN, B. A. **Comunicação de dados e redes de computadores**. 4. ed. São Paulo: McGraw-Hill, 2008.
KUROSE, J. F.; ROSS, K. W**. Redes de Computadores e a Internet - Uma Abordagem Top-Down**. 6. ed. São Paulo: Pearson, 2014.
LIMA FILHO, E. C. **Fundamentos de Redes e Cabeamento Estruturado**. São Paulo: Pearson, 2015.

SINGER, J. **O quinto poder**. Direção: Bill Condon. Produção: Bard Dorros; Steve Golin; Michael Sugar; DreamWorks Pictures; Participant Media; Anonymous Content; Reliance Entertainment. Cor (128 Min). Estados Unidos, 2013.
TANENBAUM, A. S. WETHERALL, D. **Redes de Computadores**. 5. ed. São Paulo: Pearson, 2011.