

FUNDAMENTOS DE REDES DE COMPUTADORES

AUTOR

SIDNEY NICOLAU VENTURI FILHO



FUNDAMENTOS DE REDES DE COMPUTADORES

FUNDAMENTOS DE REDES DE COMPUTADORES - CCT0457

Transmission versus Propagation Delay

Queuing Delay

http://media.pearsoncmg.com/aw/aw_kurose_network_2/applets/queuing/queuing.html

AUTOR

SIDNEY NICOLAU VENTURI FILHO

1^a EDIÇÃO

SESES

RIO DE JANEIRO 2016



Estácio

Conselho editorial REGIANE BURGER, SIMONE MARKENSON, ROBERTO PAES; GLADIS LINHARES

Autor do original SIDNEY NICOLAU VENTURI FILHO

Projeto editorial ROBERTO PAES

Coordenação de produção GLADIS LINHARES

Projeto gráfico PAULO VITOR BASTOS

Diagramação BFS MEDIA

Revisão linguística BFS MEDIA

Revisão de conteúdo SERGIO ALVES

Imagem de capa AREK_MALANG | SHUTTERSTOCK.COM

Todos os direitos reservados. Nenhuma parte desta obra pode ser reproduzida ou transmitida por quaisquer meios (eletrônico ou mecânico, incluindo fotocópia e gravação) ou arquivada em qualquer sistema ou banco de dados sem permissão escrita da Editora. Copyright SESES, 2016.

Diretoria de Ensino — Fábrica de Conhecimento
Rua do Bispo, 83, bloco F, Campus João Uchôa
Rio Comprido — Rio de Janeiro — RJ — CEP 20261-063

Sumário

Prefácio	7
1. Modelo de Referência OSI e a Arquitetura TCP/IP	9
1.1 Redes de computadores	11
1.2 Classificação das redes de computadores	12
1.3 Modelo de referência OSI (<i>open systems interconnection - RMOSI</i>)	13
1.3.1 Encapsulamento dos dados	17
1.3.2 Transmissão de dados	19
1.3.3 Terminologia do modelo OSI	19
1.4 Arquitetura TCP/IP	20
1.5 Organizações de padronização	21
2. Camada de Acesso a Rede da Arquitetura TCP/IP	25
2.1 Sistemas de comunicação de dados	27
2.2 Camada física	28
2.3 Cabeamento de cobre	29
2.4 Sem fio (<i>wireless</i>)	32
2.5 Tipos de fluxo de transmissão	33
2.6 Topologias de redes	34
2.7 Topologias físicas	35
2.8 Camada de enlace	39
2.9 Acesso ao meio	39
2.10 Métodos de acesso ao meio (topologia lógica)	41
2.11 Acesso controlado	42
2.12 Acesso baseado em contenção	43

3. Arquitetura Ethernet	47
3.1 Ethernet	49
3.2 Encapsulamento de dados	50
3.3 O Controle de acesso ao meio físico	50
3.4 Endereçamento de camada de enlace	51
3.5 Transmissão na camada de enlace	53
3.6 Evolução da Ethernet	56
3.7 CSMA/CD (<i>carrier sense multiple access with collision detection</i>)	58
3.8 Ethernet comutada	60
3.9 Endereços MAC e IP	61
3.10 Address resolution protocol – ARP (protocolo para resolução de endereços)	61
4. Camada de Rede da Internet	69
4.1 Camada de rede	71
4.1.1 Circuito virtual (CV)	72
4.1.2 Datagrama	73
4.2 Protocolo IP	73
4.3 Endereço IP	74
4.4 Endereçamento por classes (<i>classfull</i>)	77
4.5 Endereçamento sem classes (<i>classless</i>)	83
4.6 Roteamento IP	93
5. Camadas de Transporte e de Aplicação da Internet	103
5.1 Camada de Transporte	105
5.1.1 Protocolo UDP	105
5.1.2 Portas	106
5.1.3 Protocolo TCP	108
5.2 Camada de aplicação	112
5.2.1 DNS	115
5.2.2 Correio eletrônico	117

5.2.3 Telnet	121
5.2.4 FTP (<i>file transfer protocol</i>)	121
5.2.5 HTTP	122
6. Redes SOHO	127
6.1 Redes SOHO	129
6.2 Soluções de acesso à Internet	129
6.2.1 Endereçamento IP privado	129
6.2.2 Equipamentos de acesso	130
6.2.2.1 Modo ponte (<i>bridge</i>)	132
6.2.2.2 Modo roteador (router)	132
6.3 Ativos de redes	134
6.3.1 Placa de rede	134
6.3.2 Switch	136
6.3.3 Roteador	142
6.4 Configuração de host	144
6.4.1 DHCP - Dynamic Host Configuration Protocol (Protocolo de Configuração Dinâmica de Host)	146
6.5 NAT	149
6.6 VPN	153
7. Redes Sem Fio	157
7.1 Redes sem fio	159
7.2 Características de enlace sem fio	160
7.3 WI-FI: LANS sem fio 802.11	161
7.4 Arquitetura 802.11	162
7.5 Associação	164
7.6 O protocolo MAC 802.11	165
7.7 Prevenção de colisão	166
7.8 Reconhecimento/Retransmissão (ARQ)	167
7.9 Segurança	168
7.10 Configurando o roteador integrado	169

Prefácio

Prezados(as) alunos(as),

A globalização e a criação da grande rede (Internet) levou as organizações e as pessoas a adotarem cada vez mais hábitos ligados à utilização de tecnologias de redes de computadores.

As empresas implementam soluções de e-commerce, sistemas distribuídos e compartilhamento de recursos. Já os usuários realizam o acesso à Internet praticamente ao longo de todo o dia, seja por smartphones, seja por redes domésticas, acessando seus e-mail e redes sociais.

O conhecimento das tecnologias das redes de computadores permitem aos profissionais das áreas de tecnologia da informação configurar os diversos serviços e compartilhar os recursos , otimizando as comunicações e propiciando maior interação entre os usuários.

A disciplina de fundamentos de redes de computadores visa apresentar a vocês estes conhecimentos básicos e permitir-lhes utilizá-los para implementar soluções de redes domésticas e de pequenas empresas.

Com essa preocupação, o conteúdo da disciplina é organizado do seguinte modo:

Capítulo 1 – Conheceremos os conceitos básicos de redes, o modelo de referência OSI e a arquitetura TCP/IP.

Capítulo 2 – Serão apresentados os princípios de funcionamento das camadas de acesso à rede da arquitetura TCP/IP.

Capítulo 3 – Será apresentada a arquitetura Ethernet.

Capítulo 4 – Entenderemos o funcionamento da camada de rede da Internet.

Capítulo 5 – Veremos os funcionamentos das camadas de transporte e de aplicação da Internet.

Capítulo 6 – Conheceremos os equipamentos utilizados em redes SOHO.

Capítulo 7 – Exploraremos as redes sem fio.

Bons estudos!

1

Modelo de Referência OSI e a Arquitetura TCP/IP

Imagine duas pessoas conversando através de ondas sonoras: elas estão trocando informações, ou seja, realizando um processo de comunicação.

Neste processo de comunicação, podemos notar a existência de dois polos: o emissor, pessoa que está falando, o receptor, pessoa que está ouvindo, e de um meio de transmissão, no caso o ar que transmite as ondas sonoras.

Os computadores também necessitam trocar informações, mas, para que isso ocorra, deve existir um meio de transmissão que faça a ligação entre eles. É nesse cenário que aparecem as redes de computadores.

Este capítulo irá abordar aspectos básicos das redes de computadores e apresentar os fundamentos de seu funcionamento.



OBJETIVOS

- Definir redes de computadores.
 - Conhecer a classificação das redes.
 - Conhecer o funcionamento do modelo OSI.
 - Conhecer a arquitetura TCP/IP.
 - Identificar as organizações de padronização.
-

1.1 Redes de computadores

No início da informática, os computadores eram máquinas enormes, normalmente conhecidas como **Mainframe**, que trabalhavam de forma isolada e centralizavam o processamento dos dados da organização. Estas máquinas eram acessadas em **terminais**, sem capacidade de processamento, formando as **redes de teleprocessamento**.



CONCEITO

Mainframe é um computador de grande porte, dedicado normalmente ao processamento de um volume grande de informações. Os mainframes são capazes de oferecer serviços de processamento a milhares de usuários por meio de milhares de terminais conectados diretamente ou através de uma rede. Disponível em: < [wikipedia](#)>.

O desenvolvimento tecnológico levou à redução de custos do *hardware*, o que conduziu ao desejo de distribuir o poder computacional, que até então ficava centralizado. Esta evolução inseriu os microcomputadores no cenário das empresas. Nessa nova estrutura, os computadores não se comunicavam uns com os outros, o que acarretava uma série de problemas com duplicação de recursos e dificuldades para o compartilhamento de informações.

Nesse cenário, visando sanar as dificuldades apresentadas, surgiram as **redes de computadores**, em que um **sistema de comunicação** foi introduzido para interligar os equipamentos de processamentos de dados (estações de trabalhos), antes operando isoladamente, com o objetivo de permitir o compartilhamento de recursos. O **sistema de comunicação** é constituído de enlaces físicos (meio de transmissão) e de um conjunto de regras (protocolo) que permite a interligação dos vários módulos processadores.



CONCEITO

Rede de computadores: Conjunto de equipamento com capacidade de processamento, interligado por um sistema de comunicação, com capacidade de compartilhar recursos e trocar mensagens.

A diferença básica entre um **rede de computadores** e uma **rede de teleprocessamento** é que cada nó (dispositivo conectado à rede) na primeira tem capacidade de processamento, enquanto na segunda todo processamento é realizado na máquina central (*mainframe*).



CURIOSIDADE

Teleprocessamento é uma junção de "telecomunicações" e "processamento", representando a capacidade de se promover à distância o processamento de dados.

1.2 Classificação das redes de computadores

Uma redes de comutadores, quanto à sua abrangência geográfica, pode ser classificada como:

- **Rede Local** (LAN – *Local Area Network*) – é uma rede privada que interliga equipamentos em uma região geográfica bem definida, como um escritório, um prédio, uma sala etc. São projetadas para permitir o compartilhamento de recursos entre os usuários. Possuem normalmente grande velocidade de transmissão e podem ser com fio (cabeadas) ou sem fio (WiFi). Veja figura 1.1, parte a.
- **Rede metropolitana** (MAN – *Metropolitan Area Network*) – cobrem a área de um distrito ou até de uma cidade. É projetada para fornecer alta velocidade aos clientes como, por exemplo, as redes que as empresas de telecomunicações montam para permitir o acesso à Internet para seus clientes, seja via **ADSL** (Velox, GVT) seja por cabo (virtual). Veja figura 1.1, parte b.
- **Rede de longa distância** (WAN – *Wide Area Network*) – normalmente interligam redes locais e abrangem uma grande área geográfica como um país, um continente ou até o mundo todo.

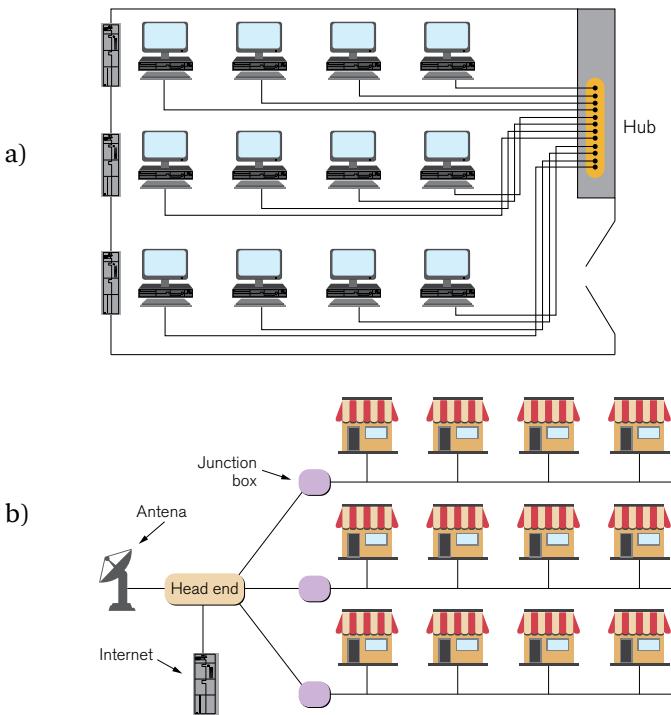


Figura 1.1 – Redes quanto à abrangência: a) Computadores em uma rede local - Fonte: Forouzan (2008). b) Rede metropolitana utilizando cabo - Fonte Tanenbaum (2007).

1.3 Modelo de referência OSI (*open systems interconnection* - RMOSI)

O aumento na quantidade e no tamanho das redes ao longo dos anos 1980 ocorreu quando as empresas perceberam o quanto podiam economizar e aumentar a produtividade com esta tecnologia. Na metade da década de 1980, começaram a surgir problemas causados pela falta de padronização de equipamentos e **protocolos**, o que dificultava ou até mesmo impedia a comunicação entre redes que usavam especificações e implementações diferentes.



CONCEITO

Protocolo: é definido como um conjunto de regras. No caso das redes de computadores, os protocolos definem o seu funcionamento. Para que dois computadores possam se comunicar em rede, eles devem usar os mesmos protocolos. Fonte: autor

Visando prover a comunicação entre as redes de diferentes tecnologias, a *International Organization for Standardization* (ISO) pesquisou esquemas de redes como, por exemplo, DECNET, SNA e TCP/IP, para tentar padronizar um conjunto de regras que balizassem seu funcionamento. Como resultado dessa pesquisa, a ISO criou um **modelo em camadas** visando permitir que soluções de redes de diferentes fabricantes pudessem se comunicar.



ATENÇÃO

Um modelo em camada funciona da seguinte forma:

1. Cada camada funciona independentemente da outra e busca resolver uma parte do problema.
 2. Cada camada tem um conjunto de funções e oferece à camada superior um conjunto de serviço por meio de uma interface bem definida.
 3. A camada superior não precisa saber como a camada inferior implementa o seu serviço, apenas tem que saber utilizar a interface.
-

O modelo de referência OSI da ISO, lançado em 1984, é composto de 7 camadas em que cada uma executa uma função específica da rede, proporcionando as seguintes vantagens:

- Decompõe as comunicações de rede em partes menores e mais simples, facilitando sua aprendizagem e compreensão.
- Padroniza os componentes de rede, permitindo o desenvolvimento e o suporte por parte de vários fabricantes.
- Possibilita a comunicação entre tipos diferentes de hardware e de software de rede.
- Evita que as modificações em uma camada afetem as outras, possibilitando maior rapidez no seu desenvolvimento.



ATENÇÃO

ISO é a organização, OSI é o modelo.

Cada camada do modelo OSI possui um grupo de funções que cabe a ela executar para que os pacotes de dados trafeguem na rede entre a origem a e o destino. A seguir, veremos uma breve descrição de cada camada do RM OSI como mostrado na figura 1.2.

Camada 7: A camada de aplicação

A camada de aplicação é a mais próxima do usuário, fornecendo serviços de rede a seus aplicativos como navegadores, clientes de correio eletrônico, aplicativos bancários e outros.

Camada 6: A camada de apresentação

Sua função é realizar transformações adequadas nos dados, tais como a compressão de textos, a criptografia, a conversão de padrões de terminais e arquivos para padrões de rede e vice-versa.

Camada 5: A camada de sessão

O nível de sessão fornece mecanismos que permitem estruturar os circuitos oferecidos pelo nível de transporte, ordenando a conversação entre equipamentos.

Camada 4: A camada de transporte

O nível de rede, dependendo da tecnologia utilizada, pode ou não garantir que um pacote chegue a seu destino. Desta forma, a camada de transporte pode também implementar a confirmação de entrega.

No nível de transporte, a comunicação é fim a fim, isto é, a entidade do nível de transporte da máquina origem comunica-se com a entidade do nível de transporte da máquina destino. Isto pode não acontecer nos níveis físico, de enlace e de rede, onde a comunicação se dá entre máquinas adjacentes (vizinhos) na rede.

Camada 3: A camada de rede

A camada de rede provê conexão entre dois hosts que podem estar localizados em redes diferentes e, eventualmente, distantes do ponto de vista geográfico. Para tal, inclui entre os seus serviços o endereçamento lógico e o roteamento, ou seja, a seleção de caminhos entre a rede de origem e a rede de destino.

Camada 2: A camada de enlace

A camada de enlace pode fornecer trânsito seguro de dados através de um link físico. Fazendo isso, a camada de enlace trata do endereçamento físico (em oposição ao endereçamento lógico), da topologia de rede, do acesso à rede, da notificação de erro, da entrega ordenada de quadros e do controle de fluxo.

Camada 1: A camada física

A camada física define as especificações elétricas, mecânicas, funcionais e de procedimentos para ativar, manter e desativar o link físico entre sistemas finais. Características como níveis de voltagem, temporização de alterações de voltagem, taxas de dados físicos, distâncias máximas de transmissão, conectores físicos e outros atributos similares são definidas pelas especificações da camada física.



ATENÇÃO

O modelo OSI não define a arquitetura de uma rede, nem especifica com exatidão os serviços e protocolos. Ele divide os processos de comunicações em camadas e determina o que cada camada deve fazer.

Desta forma, dois sistemas distintos podem se comunicar desde que obedeçam aos padrões em cada uma das camadas predeterminadas.

É importante notar que nem todas as arquiteturas de rede implementam as sete camadas do modelo OSI separadamente. Cada arquitetura implementa as funções de cada camada por meio de protocolos específicos.



Figura 1.2 – Modelo OSI. Fonte: elaborado pelo autor.



MULTIMÍDIA

Assista ao vídeo sobre o modelo OSI disponível no link <https://www.youtube.com/watch?v=9iZmAq0lsI0>

1.3.1 Encapsulamento dos dados

No processo de comunicação entre elementos na rede, a informação sai da aplicação do usuário e atravessa as diversas camadas funcionais apresentadas no modelo OSI, sob a forma de uma unidade de informação, denominada **PDU** (*Protocol Data Unit*).

Cada camada funcional possui o seu **PDU** que, genericamente, é chamado de pacote. Com base na camada de transporte, cada PDU recebe um nome específico, identificando-o conforme as funções que devem ser executadas em cada camada.

- O PDU da camada de transporte, no caso da pilha TCP/IP, recebe o nome de segmento quando utilizado o protocolo TCP ou de datagrama de usuário no caso do protocolo UDP.
- O PDU da camada de rede é chamado de **datagrama IP**, no caso da pilha TCP/IP ou pacote, no caso do modelo OSI.

- O PDU da camada de enlace é chamado de quadro (*frame*), como, por exemplo, *frame Ethernet*.
- Na camada física, a informação a ser transportada é codificada como uma sequência de *bits*.



ATENÇÃO

A pilha TCP/IP é composta pelo conjunto de protocolos que atuam na Internet e que será estudada mais à frente neste livro.

UDP e TCP são protocolos de transporte utilizados na Internet e fazem parte da pilha TCP/IP.

De acordo com a aplicação do usuário, a informação a ser transmitida será submetida a funções em cada camada do modelo OSI, podendo receber um cabeçalho que adiciona instruções para orientar a camada funcional equivalente no equipamento destino.

Este processo é denominado de **encapsulamento dos dados** e ocorre até que o quadro da camada de enlace seja encaminhado por meio do meio físico, serializado pela camada física, para o equipamento destino. (figura 1.3)

Quando o pacote chega ao destino, as instruções (contidas no cabeçalho) são lidas e o desencapsulamento é realizado à medida que o pacote "sobe" pelas camadas do modelo OSI, até sua chegada à camada de **aplicação**.

Este é o processo de **desencapsulamento dos dados**.

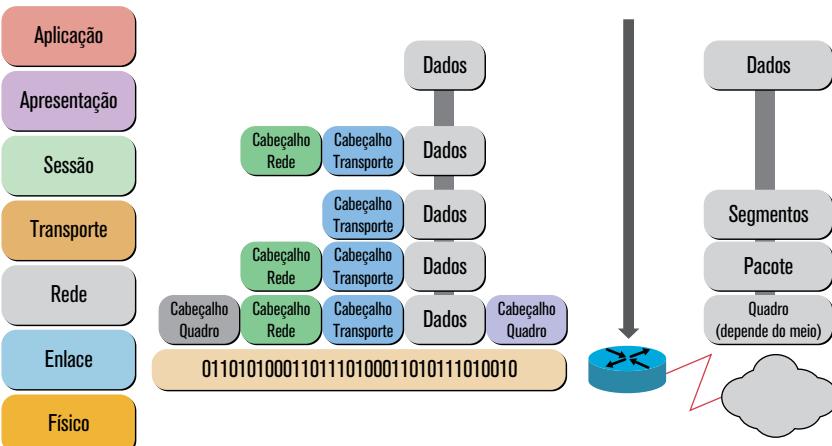


Figura 1.3 – Encapsulamento. Fonte: elaborado pelo autor.

1.3.2 Transmissão de dados

Para que os pacotes de dados trafeguem da origem para o destino, cada camada do modelo OSI na origem deve se comunicar com sua camada par no destino. Esta forma de comunicação é chamada de comunicação virtual entre camadas pares, quando os protocolos destas trocam PDUs como ilustrado na figura 1.4.

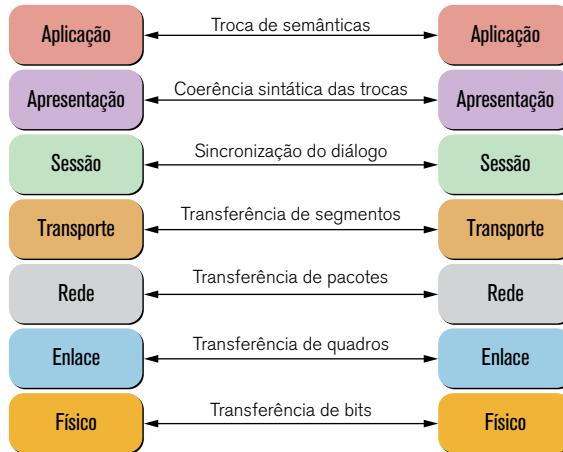


Figura 1.4 – Transmissão de dados. Fonte: elaborado pelo autor.

1.3.3 Terminologia do modelo OSI

- **Camada ou nível**

Reúne um conjunto de serviços relacionados que serão oferecidos para as camadas superiores.

- **Protocolo**

Regras e convenções usadas no diálogo entre as camadas pares de duas máquinas.

- **Interface**

Define as operações e serviços que a camada inferior tem a oferecer para a camada superior.

- **Entidade**

Elemento ativo das camadas, que pode ser um software ou hardware.

- **Entidades pares (ou parceiras)**

Entidades de mesma camada em máquinas diferentes

- **Serviço**

Conjunto de funções oferecidas a um usuário por uma camada

- **SAP (*service access point*)**

Ponto de acesso ao serviço oferecido pela camada.

1.4 Arquitetura TCP/IP

O TCP/IP é um conjunto de protocolos hierárquicos que embasa o funcionamento da Internet e, atualmente, o funcionamento de praticamente todas as redes locais.

A arquitetura TCP/IP, assim como o OSI, realiza a divisão de funções do sistema de comunicação em estruturas de camadas, porém, como foi desenvolvida antes do modelo OSI, as camadas não correspondem exatamente às do RMOSI, conforme mostrado na figura 1.5.

Conforme podemos notar na figura 1.5, o TCP/IP é formado por 4 camadas:

- **Aplicação:** corresponde aproximadamente às 3 camadas superiores do OSI e tem por função tratar de questões de representação, codificação e controle de diálogo. O TCP/IP combina todas as questões relacionadas a aplicações em uma camada e presume que esses dados estejam empacotados corretamente para a próxima camada. Exemplos de protocolos desta camada são: FTP, HTTP, Telnet, SMTP, POP3 e IMAP.

- **Transporte:** corresponde aproximadamente à camada de transporte do OSI e reúne os protocolos que realizam as funções de transporte de dados fim a fim, ou seja, considera apenas a origem e o destino da comunicação, sem se preocupar com os elementos intermediários. A camada de transporte possui dois protocolos principais que são o UDP (*user datagram protocol*) e TCP (*transmission control protocol*).

- **Inter-rede:** corresponde aproximadamente à camada de rede do OSI e tem como finalidade enviar pacotes da origem de qualquer rede e fazê-los chegar ao destino, independentemente do caminho e das redes. O protocolo específico que governa essa camada é chamado de protocolo de Internet (IP). A determinação do melhor caminho e a comutação de pacotes acontecem nessa camada.

- **Intra-rede:** é também chamada de camada *host-rede* ou rede de acesso. É a camada que se relaciona a tudo aquilo de que um pacote IP necessita para

realmente estabelecer um *link* físico. Isso inclui detalhes de tecnologia de LAN e WAN e todos os detalhes nas camadas física e de enlace do OSI.

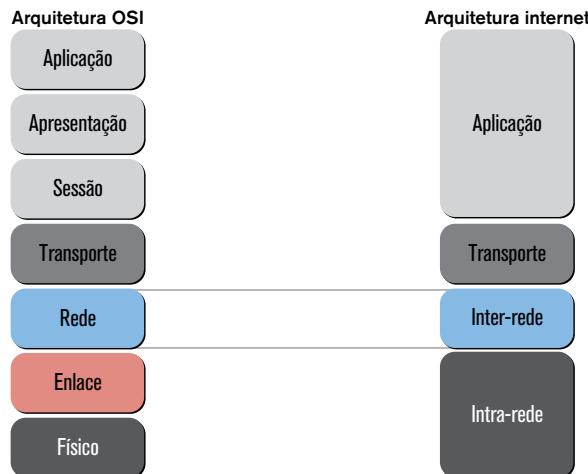


Figura 1.5 – Comparação OSI X TCP/IP. Fonte: elaborado pelo autor.

1.5 Organizações de padronização

Padrões de redes são fundamentais para a manutenção da interoperabilidade dos equipamentos de diversos fabricantes, pois fornecem diretrizes para a construção e interação dos diversos equipamentos.

As organizações de padronização foram estabelecidas por convênios entre governos e instituições voluntárias. Grande parte destas instituições já tinham envolvimento com padronizações em várias outras áreas de conhecimento e passaram a se preocupar e a se ocupar com definições de padrões aplicáveis às redes de computadores. Entre estas instituições, merecem destaque:

- **ANSI** – *American National Standards Institute* (Instituto Americano de Padrões Nacionais)
- **BSI** – *British Standards Institute* (Instituto Ingles de Padrões)
- **DIN** – *Deutsches Institut for Normung* (Instituto Alemão de Normas)
- **ABNT** – Associação Brasileira de Normas Técnicas
- **ISO** – *International Standards Organization* (Organização Internacional de Padrões)

- **ITU** – *International Telecommunications Union* (União Internacional de Telecomunicações). A ITU-T, especificamente, está voltada para comunicações, interfaces e outros padrões relativos a telecomunicações. É a antiga CCITT – *Consultative Committee for International Telephony and Telegraphy*.
- **EIA** – *Electronic Industries Association* (Associação das Indústrias Eletrônicas)
- **TIA** – *Telecommunication Industries Association* (Associação das indústrias de telecomunicações)
- **IEEE** – *Institute of Electrical and Electronic Engineers* (Instituto de Engenheiros Elétricos e Eletrônicos)
- **IETF** – *Internet Engineering Task Force* (Grupo de Trabalho de Engenharia da Internet)

Por detrás de todas estas organizações, há empresas, pesquisadores, governos, ONGs e um grande número de voluntários. Da grande maioria destas organizações saem “recomendações” que acabam se transformando em regras gerais aceitas pelo consenso dos usuários.



ATIVIDADES

Pesquise na internet como funciona o software *Wireshark*, instale-o em sua máquina e realize a captura de pacotes de sua rede.

Responda às seguintes perguntas:

01. Uma LAN é:
 - uma rede que conecta estações de trabalho e outros dispositivos em uma área geographicamente limitada.
 - uma rede que cobre uma área maior que uma MAN.
 - uma rede que conecta usuários em uma grande área metropolitana.
 - uma rede que interconecta outras redes.
02. O conjunto formado pelos meios de transmissão e pelos protocolos constituem:
 - uma rede de computadores.
 - um sistema de comunicações.

- c) um sistema de cabeamento.
- d) uma rede física.

03. No encapsulamento de dados, a informação de controle que é colocada antes dos dados denomina-se:

- a) quadro.
- b) cabeçalho.
- c) cápsula.
- d) informações de roteamento.

04. A ordem correta das camadas no modelo OSI é:

- a) física, enlace rede, transporte, sessão, apresentação, aplicação.
- b) física, sessão, dados, rede, aplicação, transporte, apresentação.
- c) física, enlace, rede, sessão, transporte, apresentação, aplicação.
- d) física, enlace, rede, sessão, aplicação, transporte, apresentação.

05. A camada do modelo OSI em que os pacotes são encapsulados em quadros é o(a):

- a) enlace.
- b) rede.
- c) transporte.
- d) sessão.

06. O conjunto de regras que determina o formato e a transmissão de dados denomina-se:

- a) padrão.
- b) modelo.
- c) representação.
- d) protocolo.

07. Uma rede em barramento:

- a) compartilha meios de transmissão.
 - b) utiliza ligação ponto a ponto.
 - c) depende de um nó central.
 - d) tem transmissão unidirecional.
-



REFLEXÃO

Você viu nesta aula o que é uma rede de computadores, como ela se organiza em camadas e suas topologias.

Conheceu ainda os principais componentes de um sistema de comunicações.



LEITURA

Leia os capítulos 1 e 2 do Livro **Comunicação de dados e redes de computadores**, de Behrouz A. Forouzan.

Saiba mais

Assista aos seguintes vídeos:

- Funcionamento da internet

Disponível em: <https://www.youtube.com/watch?v=O9tg_gr_ilY>.

Disponível em: <<https://www.youtube.com/watch?v=E4gcWJaw8aQ>>.

Disponível em: <https://www.youtube.com/watch?v=_axG2fUpUCs>.

- História da Internet

Disponível em: <<https://www.youtube.com/watch?v=b3iZnC652Yo>>.

Disponível em: <<https://www.youtube.com/watch?v=CU0mEufdExE>>.



REFERÊNCIAS BIBLIOGRÁFICAS

FOROUZAN, Behrouz A. **Comunicação de dados e redes de computadores**. 4. ed. São Paulo: McGraw-Hill, 2008.

KUROSE, James F. e ROSS, Keith W. **Redes de computadores e a Internet**: uma abordagem top-down. 4. ed. São Paulo: Addison Wesley, 2009.

Tanenbaum, Andrew S. **Redes de computadores**. 5. ed. Rio de Janeiro: Campus, 2007.

2

Camada de Acesso a Rede da Arquitetura TCP/IP

Conforme vimos no capítulo 1 o modelo OSI é composto de 7 camadas, enquanto a Arquitetura TCP/IP define 4 camadas.

A camada inferior do TCP/IP é chamada de intra-rede ou acesso à rede e corresponde às camadas 1 física e 2 enlace do modelo OSI.

Em nosso estudo, a partir deste ponto consideraremos um modelo híbrido composto de cinco camadas: física, enlace, rede, transporte e aplicação

Este capítulo irá abordar características do funcionamento das duas camadas inferiores.



OBJETIVOS

- Identificar os meios físicos de transmissão.
 - Conhecer o UTP.
 - Descrever as topologias físicas de redes.
 - Identificar os métodos de acesso ao meio.
-

2.1 Sistemas de comunicação de dados

Comunicação é o ato de dois indivíduos trocarem mensagens ou informações. No caso de computadores, os dados enviados de uma forma acordada entre as partes constituem o objeto da comunicação.

Um **sistema de comunicação de dados** provê um meio de transmissão para que os computadores possam realizar seu intercâmbio.

Para ter eficácia, segundo Forouzan(2008), um sistema de comunicações de dados depende dos seguintes fatores:

1. **Entrega:** o sistema deve entregar os dados no destino correto. Os dados devem ser recebidos exclusivamente pelo dispositivo ou usuário pretendidos.

2. **Precisão:** o sistema deve entregar os dados de forma precisa. Dados alterados durante a transmissão e deixados sem correção são inúteis.

3. **Sincronização:** o sistema deve entregar dados no momento certo. Dados entregues com atraso são inúteis. No caso de vídeo e áudio, a entrega em tempo significa fornecer os dados à medida que eles são produzidos e sem atrasos consideráveis. Este tipo de entrega é denominado transmissão em tempo real.

4. **Jitter:** refere-se à variação do tempo de chegada do pacote. É o atraso desigual na entrega de pacotes de áudio ou vídeo.

Os componentes de um sistema de comunicação de dados, segundo Forouzan(2008), são cinco:

1. **Mensagem:** são as informações (dados) a serem transmitidos. Entre as formas populares de informação, temos texto, imagens e vídeos.

2. **Emissor:** é o dispositivo que envia a mensagem de dados. Pode ser um computador, uma estação de trabalho, um aparelho telefônico, televisão e assim por diante.

3. **Receptor:** é o dispositivo que recebe a mensagem. Pode ser um computador, uma estação de trabalho, um aparelho telefônico, televisão e assim por diante.

4. **Meio de transmissão:** é o caminho físico pelo qual uma mensagem trafega do emissor para o receptor. Alguns exemplos de meio de transmissão são: cabo de par trançado, cabo coaxial, fibra ótica e o ar.

5. **Protocolo:** é um conjunto de regras que controla a comunicação de dados. Representa um acordo entre os dispositivos de comunicação. Sem o

protocolo, dois dispositivos podem estar conectados, mas não conseguem se comunicar.

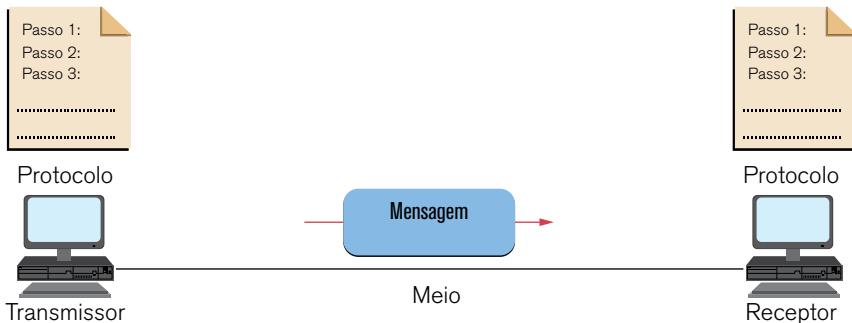


Figura 2.1 – Componentes de um sistema de comunicações de dados. Disponível em: <<http://www.brasilescola.com/upload/e/img1.jpg>>.

2.2 Camada física

A camada física fornece os requisitos para transportar pelo meio físico de transmissão o **quadro** da camada de enlace de dados. Essa camada aceita um quadro completo da camada de enlace de dados e codifica-o como uma série de sinais que serão transmitidos para o meio físico local. Os *bits* que formam um quadro são recebidos por um dispositivo final ou por um dispositivo intermediário.



ATENÇÃO

A camada física entende o quadro com uma sequência de *bits* que são codificados e transmitidos como uma série de sinais. Ela não “enxerga” o quadro.

A entrega de quadros pelo meio físico local exige os seguintes elementos da camada física:

- Meio físico e conectores ligados
- Representação de bits no meio físico
- Codificação de dados e informações de controle
- Circuito transmissor e receptor nos dispositivos de rede



ATENÇÃO

Lembre-se: quadro é o nome da PDU da camada de enlace de dados.

Os dois meios físicos mais utilizados em redes de pequeno porte são:

- Cabo de cobre
- Sem fio (*wireless*)

Diferentes meios físicos suportam a transferência de bits em velocidades diferentes. A transferência de dados normalmente é discutida em termos de **largura de banda** e **throughput**.

A **largura de banda** é a capacidade de um meio transportar dados. A largura de banda digital mede a quantidade de dados que pode fluir de um lugar para outro durante um determinado tempo. A largura de banda normalmente é medida em *quilobits* por segundo (kbps) ou *megabits* por segundo (Mbps)

O **throughput** é a medida da transferência de *bits* pelo meio físico durante um determinado período.



ATENÇÃO

O **throughput** efetivo que você obtém em uma rede normalmente é menor que a largura de banda disponível devido a fatores como volume de dados sendo trafegados e congestionamento na rede.

2.3 Cabeamento de cobre

Ao longo dos anos, foram utilizados vários tipos de cabeamento de cobre como coaxial grosso, coaxial fino e par trançado.

Nos dias atuais, o tipo mais utilizado em redes locais é o UTP (*unshielded twisted-pair*), em português denominado par trançado não blindado com conectores RJ45 (figura 2.2), usado para interconectar dispositivos de redes como computadores com dispositivos intermediários como *switch* ou roteadores.

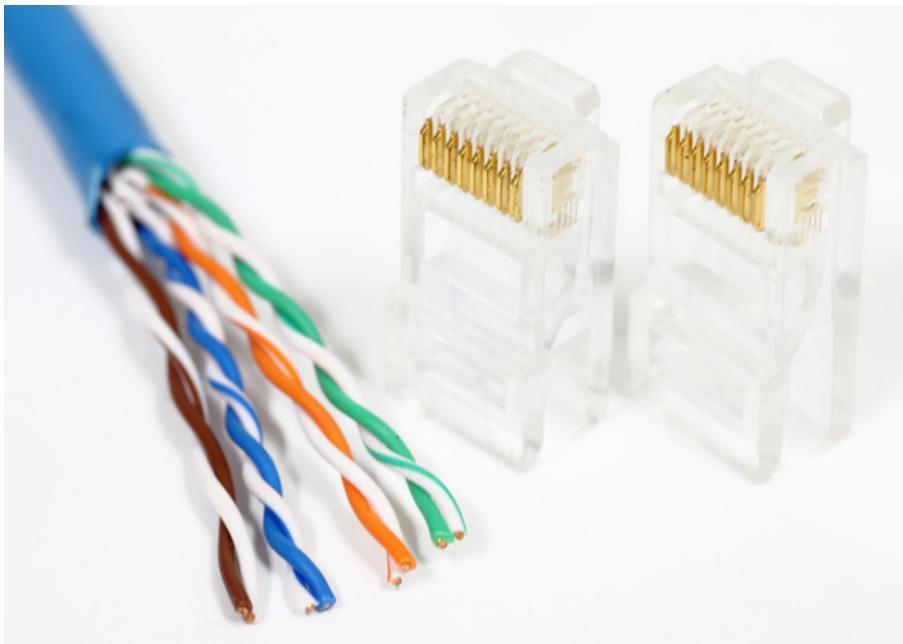


Figura 2.2 – Cabo UTP e conectores RJ 45.

Para conectar o cabo UTP, devemos seguir os padrões estabelecidos pela norma TIA/EIA 568, que define duas ordens diferentes para os fios:

Padrão T568A:

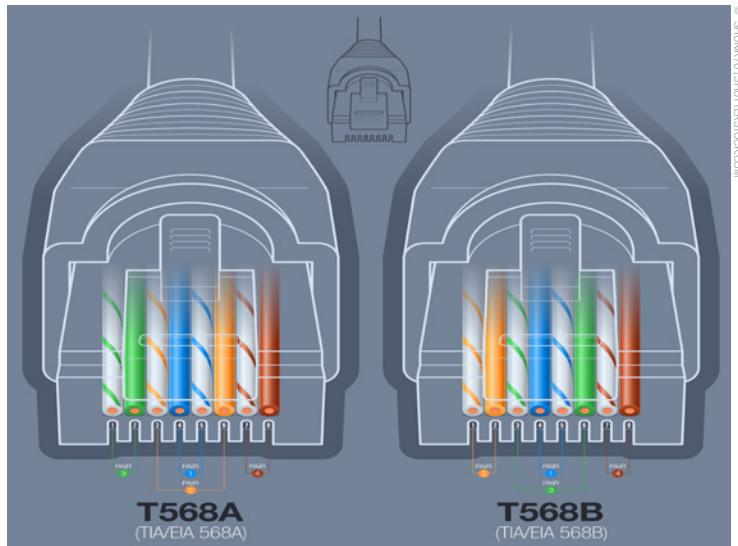
Pino

- 1** branco do verde (transmissão)
- 2** verde (transmissão)
- 3** branco do laranja (recepção)
- 4** azul
- 5** branco do azul
- 6** laranja (recepção)
- 7** branco do marrom
- 8** marrom

Padrão T568B:

Pino

- 1** branco do laranja (recepção)
- 2** laranja (recepção)
- 3** branco do verde (transmissão)
- 4** azul
- 5** branco do azul
- 6** verde (transmissão)
- 7** branco do marrom
- 8** marrom



© SHUTTERSTOCK.COM

Figura 2.3 – Padrão T568.

Situações diversas podem exigir que os cabos UTP sejam conectados de acordo com diferentes padrões de conexão de fios. Isso significa que os fios do cabo precisam ser conectados em uma ordem diferente para conjuntos diferentes de pinos nos conectores RJ-45.

A seguir estão os principais tipos de cabo obtidos pelo uso de padrões específicos de conexão de fios:

- **Cabo direto ou straight-through** (Ethernet): são usados quando utilizamos o mesmo padrão nas duas pontas (T568A ou T568B).
- **Cabo cruzado ou crossover** (Ethernet): são usados quando utilizamos o padrão T568A em uma ponta e o T568B na outra.

O **cabo direto** é o tipo "normal" de cabo, usado para ligar os micros ao *switch*. Já o **cabo cruzado** permite ligar diretamente dois micros, sem precisar do *hub* ou *switch*. Ele é uma opção mais barata quando você tem apenas dois micros.



MULTIMÍDIA

Assista ao vídeo sobre como montar cabos de redes no link:
<<https://www.youtube.com/watch?v=wmxiV0hQUGE>>.

2.4 Sem fio (*wireless*)

O meio físico sem fio conduz sinais eletromagnéticos nas frequências de rádio que representam os dígitos binários de comunicação de dados. Como um meio de rede, o sem fio não é restrito aos condutores ou caminhos, como é o meio físico de cobre.

As tecnologias de comunicação de dados sem fio funcionam bem em ambientes abertos, entretanto, em ambientes fechados, têm sua cobertura prejudicada por determinados materiais de construção utilizados em prédios e estruturas sendo, ainda, suscetíveis à interferência de telefones sem fio, lâmpadas fluorescentes e fornos micro-ondas, entre outros equipamentos.

Além disso, pelo fato de a cobertura da comunicação sem fio não exigir acesso físico ao meio, os dispositivos e usuários que não são autorizados a acessar a rede poderão ter acesso à transmissão. A segurança de rede, portanto, é o principal componente da administração de uma rede sem fio.

O IEEE e os padrões da indústria de telecomunicações para a comunicação de dados sem fio abrangem as camadas física e enlace de dados. Os padrões de comunicação de dados comuns que se aplicam ao meio físico sem fio são:

- **Padrão IEEE 802.11:** geralmente conhecido como “*Wi-Fi*”, é uma tecnologia *wireless LAN* (WLAN), que utiliza a contenção ou sistema não determinístico com o processo de acesso ao meio físico Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA).
- **Padrão IEEE 802.15:** padrão *Wireless Personal Area Network* (WPAN), conhecido como “*bluetooth*”, utiliza um dispositivo de processo em pares para se comunicar a distâncias entre 1, 10 ou 100 metros, dependendo da classe do equipamento.



ATENÇÃO

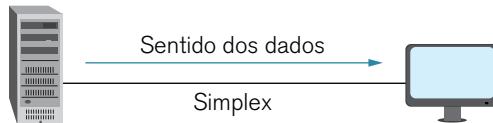
Bluetooth é o tipo de rede utilizado quando pareamos dois celulares, o celular e um fone de ouvido ou o celular e o kit multimídia do automóvel.

2.5 Tipos de fluxo de transmissão

A forma de utilização do meio físico que conecta estações dá origem à seguinte classificação sobre comunicação no enlace:

- **Simplex**

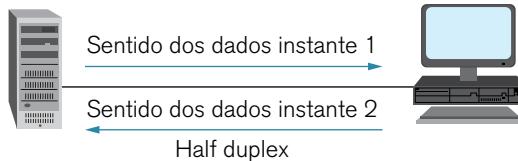
O enlace é utilizado apenas em um dos dois possíveis sentidos de transmissão. Teclados, monitores e radio comerciais (AM, FM) são exemplos de transmissão simplex.



Fonte: elaborado pelo autor.

- **Half-duplex**

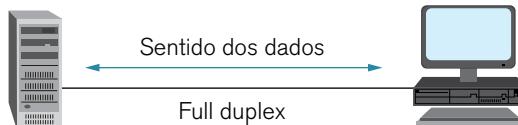
O enlace é utilizado nos dois possíveis sentidos de transmissão, porém apenas um por vez, como, por exemplo, rádios portáteis de comunicação, *walk-talk* e redes sem fio.



Fonte: elaborado pelo autor.

- **Full-duplex**

O enlace é utilizado simultaneamente nos dois possíveis sentidos de transmissão como, por exemplo, a telefonia fixa e celular, redes cabeadas com *switch*.



Fonte: elaborado pelo autor.

Enlaces como os classificados serão utilizados pelas diferentes topologias que, por sua vez, irão variar de acordo com o tipo de rede, seus equipamentos e sua configuração.

2.6 Topologias de redes

O sistema de comunicação vai se constituir num arranjo topológico interligando os diversos **nós** através de enlaces físicos (meios de transmissão) e de um conjunto de regras com o fim de organizar a comunicação (protocolos).



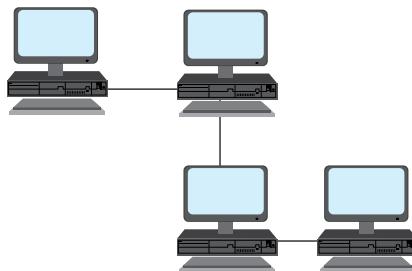
ATENÇÃO

Lembre-se: um nó de rede é um computador, celular ou outro tipo de dispositivo ligado à rede.

Uma das questões vitais na construção de qualquer sistema de comunicação é verificar qual arranjo topológico deve ser utilizado e quais as alternativas. Essas alternativas dependerão do tipo de rede. A topologia de uma rede irá, muitas vezes, caracterizar o seu tipo, eficiência e velocidade. A topologia de uma rede de comunicação refere-se à forma como os enlaces físicos e os nós de comutação estão organizados, determinando os caminhos físicos existentes e utilizáveis entre quaisquer estações conectadas a essa rede.

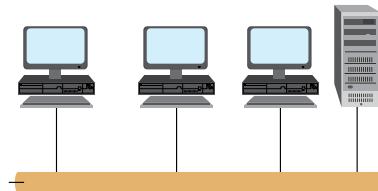
Ao organizar os enlaces físicos num sistema de comunicação, várias são as formas possíveis de utilização das linhas de transmissão. As ligações podem ser de dois tipos:

- **Ponto a ponto (*point to point*)**: caracterizam-se pela presença de somente dois pontos de comunicação, um em cada extremidade do enlace.



Fonte: elaborado pelo autor.

- **Multiponto (Multipoint)**: presença de três ou mais dispositivos de comunicação com possibilidade de utilização do mesmo enlace.



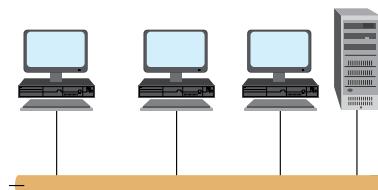
Fonte: elaborado pelo autor.

Existem duas partes na definição da topologia: a **topologia física**, que é o *layout* atual do fio (meio) e os **métodos de acesso ao meio (topologia lógica)**, que define como os meios são acessados pelos *hosts* ou nós de rede e é padronizada por protocolos da camada de enlace.

2.7 Topologias físicas

Barramento ou barra

Usa um único segmento de *backbone* (comprimento do cabo), ao qual todos os *hosts* ou nós de rede se conectam diretamente



Fonte: elaborado pelo autor.

Características

- Todas as estações se ligam a um mesmo meio de transmissão.
- Usa uma configuração multiponto.
- Cada nó pode ouvir todas as informações transmitidas.
- Única decisão necessária em cada nó é a identificação das mensagens que lhe são destinadas.

- As *interfaces* não fazem parte do meio de transmissão, portanto, se falharem, não causam a parada total do sistema.
- O poder de crescimento vai depender do meio de transmissão utilizado, da taxa de transmissão e da quantidade de ligações ao meio.
- Não há necessidade de roteamento.
- O meio de transmissão é um segmento multiponto, compartilhado pelas diversas estações.
- Exige mecanismos que disciplinem o acesso das estações ao meio compartilhado.

Vantagens

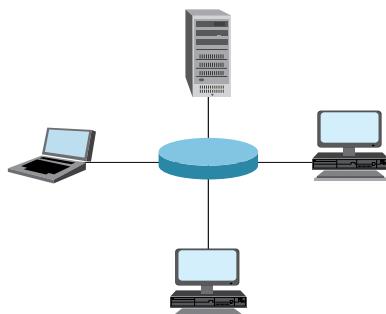
- Facilidade de instalação
- Simples e barato
- Minimiza a quantidade de cabo utilizado nas ligações à rede.

Desvantagens

- Quanto maior a distância coberta por um sinal ao longo da linha de comunicação, maior será o calor produzido, devido ao fato de a energia ser transformada para aquecer tornando o sinal mais fraco, à medida que ele se desloca.
- Uma falha ao longo da linha de comunicação comum afeta todas as transmissões na rede.

Anel

Conecta um *host* ou nó de rede ao próximo até retornar ao primeiro. Isso cria um anel físico do cabo.



Fonte: elaborado pelo autor.

Características

- Estações conectadas através de um caminho fechado
- Série de repetidores ligados por meio físico
- Usualmente unidirecionais
- Mensagens circulam por todo o anel.
- Cada repetidor possui um relé que pode removê-lo mecanicamente da rede, o que faz com que a confiabilidade aumente.

Vantagens

- A rede propicia maior distância entre as estações.
- Performance superior à topologia barramento

Desvantagens

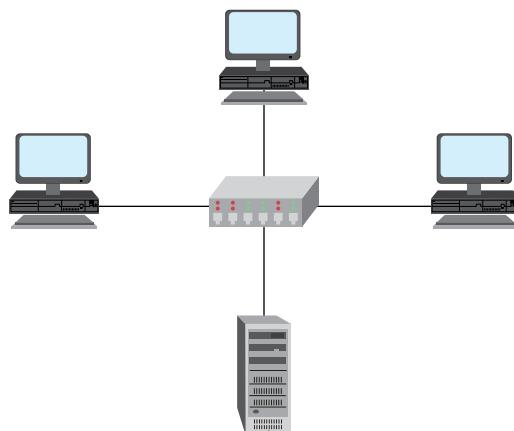
- Como cada ponto é necessário para a transmissão ou retransmissão, se houver um problema num determinado ativo de rede, a transmissão será interrompida.
- Essa topologia pode ser encarada como uma ligação de pontes entre várias ilhas (pontos), sendo preciso passar por dentro de uma ilha para alcançar a próxima. Dessa maneira, se houver um problema qualquer e interditarem uma ilha, o "carteiro" não terá como atingir a próxima ilha.

Uma solução de rede baseada na topologia em anel que foi adotada comercialmente pela IBM (Rede *Token Ring*) é manter o anel somente para os aspectos lógicos e utilizar uma topologia em estrela na ligação física.

A utilização de concentradores (*ring wiring concentrators*) deu grande poder de expansão, em razão da capacidade regenerativa dos sinais e da interconexão de concentradores.

Estrela

Conecta todos os cabos ao ponto central de concentração. Esse ponto é normalmente um *hub* ou *switch*.



Fonte: elaborado pelo autor.

Características

- Utiliza ligação ponto a ponto (estação-concentrador).
- O nó central, cuja função é o chaveamento (comutação), é denominado comutador (*hub*) ou *switch*.
- No nó central, ocorre a comutação e/ou gerência de comunicações;
- Podem atuar por difusão (*broadcasting*).
- O fluxo de comunicação é centralizado.
- O nó central pode realizar a compatibilidade de velocidade entre os nós ou atuar como conversor de protocolos se o equipamento for de camada 2 (*switch*).
- Necessita uso de processador relativamente grande para atuar como nó de comunicação central se o equipamento for de camada 2 (*switch*);
- O desempenho depende da quantidade de tempo requerido pelo nó central, para processar e encaminhar mensagem e tráfego.

Vantagens

- Simplificação do processo de gerenciamento dos pedidos de acesso
- A existência de um nó central para o controle facilita a manutenção e a detecção de erros.

Desvantagens

- Limita a quantidade de pontos que podem ser conectados, devido até mesmo ao espaço físico disponível para a conexão dos cabos.

- Ocorre degradação acentuada da performance quando existem muitas solicitações simultâneas à máquina centralizadora.
- Se o concentrador tiver alguma falha, toda a rede para de funcionar.

2.8 Camada de enlace

A camada de enlace é responsável pela troca de quadros entre nós sobre o meio de uma rede física.

Termos específicos da camada de enlace:

- **Quadro:** a PDU da camada de enlace
- **Nó:** a notação da camada 2 para dispositivos de rede conectados a um meio comum
- **Meio/Mídia (físico):** o meio físico para transferência de informação entre dois nós
- **Rede (física):** dois ou mais nós conectados a um meio comum



ATENÇÃO

Uma rede física é diferente de uma rede lógica. Redes lógicas são definidas na camada de rede pelo arranjo do esquema de endereçamento hierárquico. Redes físicas representam a interconexão de dispositivos sobre um meio comum. Às vezes, uma rede física também é relatada como um segmento de rede.

A camada de enlace realiza dois serviços básicos:

- Permite às camadas superiores acessarem o meio usando técnicas como enquadramento.
- Controla como o dado é colocado sobre o meio e é recebido do meio usando técnicas como o controle de acesso ao meio e a detecção de erros.

2.9 Acesso ao meio

A camada de enlace fornece serviços para suportar os processos de comunicação no meio para o qual o dado deve ser transmitido.

Quando ocorre a transmissão entre dois nós, embora do ponto de vista de rede tenhamos uma origem e um destino bem definidos, no enlace podem ocorrer numerosas transições. Em cada salto ao longo do caminho, um dispositivo intermediário - geralmente um roteador - aceita quadros de um meio, desencapsula-os e, então, encaminha o pacote em um novo e apropriado quadro ao meio daquele segmento de rede física.

Observe a figura 2.4. O PCA, localizado no Rio de Janeiro, deseja acessar o servidor Internet localizado em São Paulo. Podemos notar que cada *link* entre os dispositivos usa um meio diferente. Entre o PCA e o **Modem ADSL1**, temos um *link* UTP, a seguir temos a ligação entre os modens utilizando ADSL, o **Modem ADSL2** está ligado ao **roteador1** via um *link* UTP, entre os **roteadores** temos uma linha serial e, finalmente, temos novamente dois *links* UTP ligando o **switch** ao **roteador2** e ao **servidor Internet**,

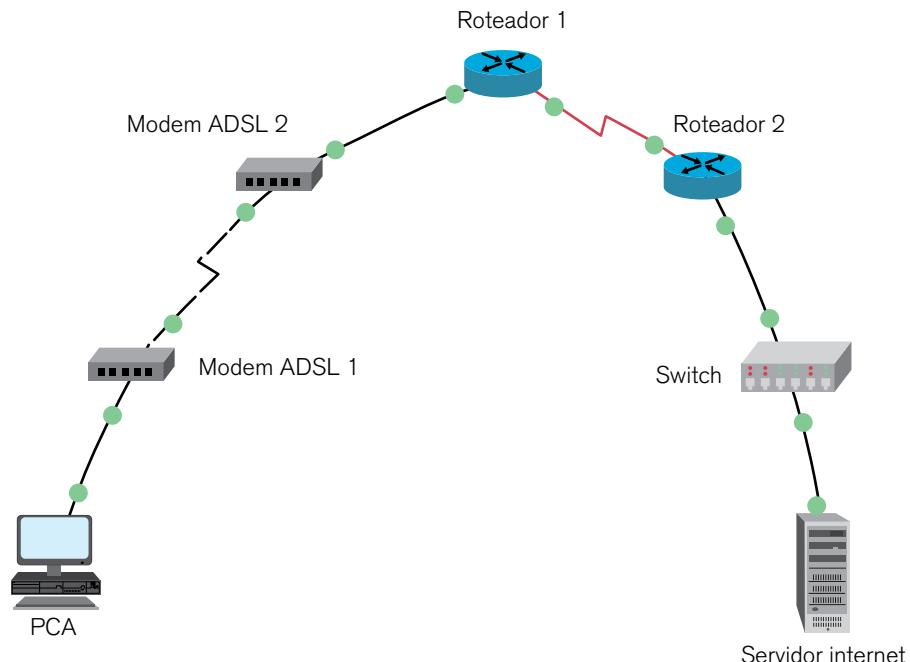


Figura 2.4 – Transmissão de Dados. Fonte: elaborado pelo autor.

À medida que o pacote navega de PCA até o **modem ADSL1**, ele será encapsulado em um quadro **Ethernet**, desencapsulado, processado e, então, encapsulado na tecnologia utilizada entre os modens e assim sucessivamente.

Podemos notar então que, embora os dois nós (PCA e servidor Internet) estejam se comunicando com seus protocolos para da camada de rede (IP), numerosos protocolos da camada de enlace estão sendo utilizados para transmitir os pacotes IP através dos vários tipos de *LANs* e *WANs*. Esta troca de pacotes exige que a camada de enlace trabalhe com uma diversidade de protocolos, pois cada transição de meio físico pode exigir um protocolo da camada de enlace.



ATENÇÃO

Ethernet é uma arquitetura de rede local que, entre suas especificações, possui o cabeamento UTP.

Iremos estudar esta arquitetura mais à frente neste livro.

A camada de enlace isola, de modo efetivo, os processos de comunicação nas camadas superiores das transições de meio físico que podem ocorrer fim a fim. Um quadro é recebido e direcionado a um protocolo da camada superior, neste caso o IPv4, que não precisa estar a par de qual meio de comunicação ele usará.

2.10 Métodos de acesso ao meio (topologia lógica)

O método de acesso ao meio, também chamada de topologia lógica por alguns autores, de uma rede é a forma como os *hosts* ou nós de redes se comunicam através dos meios.

Cada protocolo da camada de enlace determina o seu método de controle de acesso ao meio. Estas técnicas de controle de acesso definem se e como os nós compartilham o meio.

Uma analogia para os métodos de controle de acesso ao meio são as regras de trânsito. Quando um veículo vai entrar em uma rodovia, ele deve obedecer a uma série de regras como: observar se não está vindo algum veículo, respeitar a sinalização etc. Se as regras não existissem, um veículo simplesmente poderia entrar em uma rodovia sem respeitar os demais automóveis. Devemos observar, entretanto, que cada via de trânsito possui características próprias que

implicam a adaptação das regras gerais à sua realidade como, por exemplo, um sinal de trânsito tem que estar aberto para que o veículo possa avançar, a sinalização de preferência etc.

Do mesmo modo, existem diferentes formas de regular a colocação dos quadros no meio.

Alguns métodos de controle de acesso ao meio baseiam-se em um controle estrito, enquanto outros baseiam-se em critérios mais simples.

Os dois métodos básicos de controle de acesso ao meio são:

- **Controlado:** cada nó tem um momento apropriado para usar o meio.
- **Baseados em contenção:** os nós competem pelo direito de transmitir utilizando o meio.

2.11 Acesso controlado

Neste método, os dispositivos se revezam no acesso ao meio seguindo uma sequência determinada. A forma mais comum é a utilização de um símbolo (*token* em inglês). O símbolo pode ser entendido como um bastão na corrida de revezamento. O nó que detém o símbolo é o único que pode realizar a transmissão naquele momento. Se o dispositivo não precisar acessar o meio, o símbolo será passado para o nó seguinte na rede.

Quando o dispositivo coloca um quadro no meio, nenhum outro dispositivo pode fazer o mesmo até que transmissão esteja concluída e o quadro tenha sido retirado pelo nó que o colocou. Após a retirada, o nó de origem, tipicamente, libera o símbolo para o próximo nó na rede.



ATENÇÃO

O acesso controlado também é denominado passagem de símbolo , (*token passing*) e foi utilizado na rede em anel *Token Ring* da IBM

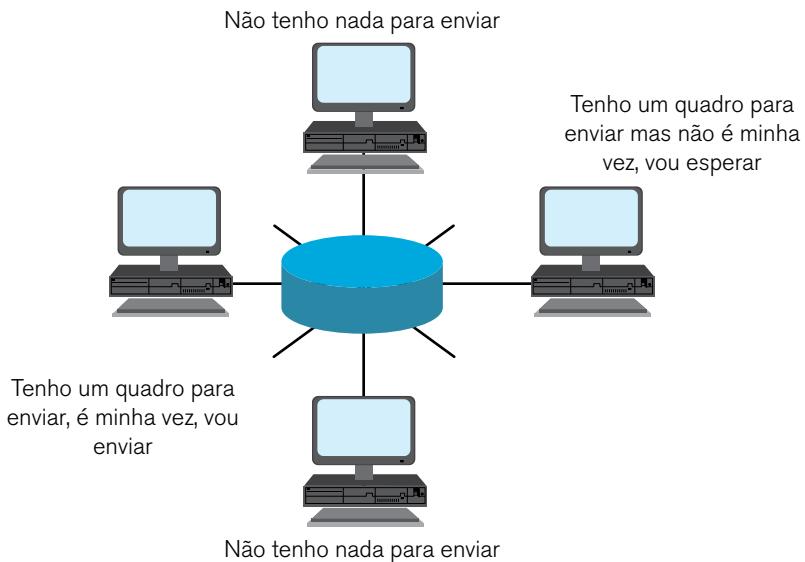


Figura 2.5 – Acesso controlado. Fonte: elaborado pelo autor.

2.12 Acesso baseado em contenção

Este método permite que qualquer dispositivo tente acessar o meio sempre que ele tenha dados para enviar. Posto desta forma, a tendência da rede é se tornar um caos completo, com vários nós transmitindo ao mesmo tempo e com as diversas transmissões misturando-se no meio físico e gerando **colisão de dados**, caso em que dados enviados pelos dispositivos serão corrompidos e deverão ser reenviados. Esta situação aconteceu muito nos primeiros protocolos como o **ALOHA**. Visando minimizar esta situação, foi desenvolvido um protocolo denominado ***carrier sense multiple access*** - **CSMA** (acesso múltiplo sensível à portadora), que funciona baseado no seguinte princípio: antes de tentar transmitir, o nó irá “ouvir” o cabo visando detectar se o meio já está transportando algum sinal, ou seja, ele vai verificar se existe uma **portadora** no cabo. Se um

sinal portador, colocado por outro nó, for detectado, isso significa que outro dispositivo está transmitindo dados. Então, o nó que deseja transmitir deve se “conter” e aguardar um curto período de tempo, quando então deverá verificar novamente se o meio está livre. Se nenhum sinal portador for detectado, o dispositivo transmitirá seus dados. As redes Ethernet e sem fio usam controle de acesso ao meio baseado em contenção.

Mesmo com o CSMA, é possível que dois dispositivos transmitam dados ao mesmo tempo. Isto pode ocorrer em situações como, por exemplo, quando dois nós que esperavam o término da transmissão de um terceiro percebem o meio “livre” e iniciam sua transmissão, gerando uma **colisão de dados**.

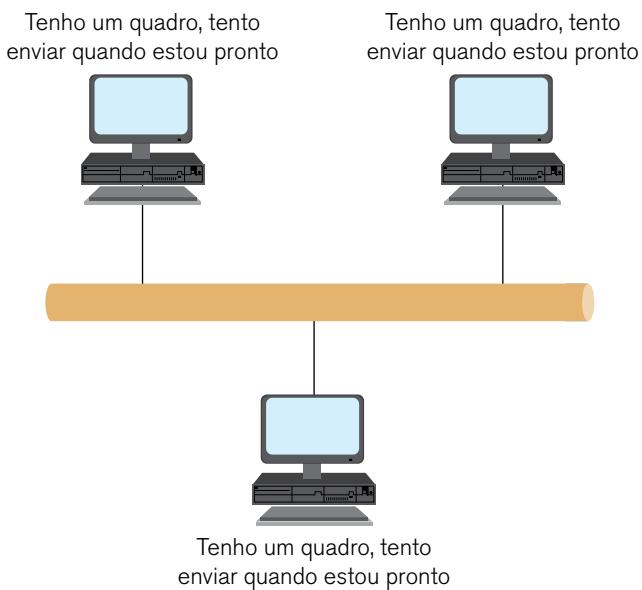


Figura 2.6 – Acesso baseado em contenção. Fonte: elaborada pelo autor.

Os métodos de controle de acesso ao meio baseados em contenção possuem um *overhead* menor que os métodos de acesso controlado, porém não trabalham bem em redes com uso massivo, ou seja, quando muitos nós desejam transmitir ao mesmo tempo, pois neste cenário a probabilidade de acesso

bem-sucedido ao meio sem colisão diminui. Adicionalmente, os mecanismos de recuperação necessários para corrigir erros devidos a essas colisões ainda diminuem o *throughput*.

O CSMA é geralmente implementado em conjunto com um método para resolução da contenção do meio. Os dois métodos geralmente usados são:

- ***Carrier sense multiple access / colision detection*** - CSMA/CD (detecção de colisão): utilizado em redes que seguem a arquitetura Ethernet, o dispositivo examina o meio para verificar a presença de sinal de dados. Se estiver livre, transmite-os, entretanto, ao perceber que ocorreu uma colisão, interrompe a transmissão, aguarda um tempo e tenta novamente mais tarde. Este método será objeto de estudo no capítulo 3 deste livro.

- ***Carrier sense multiple access / collision avoidance*** - CSMA/CA (prevenção de colisão): o dispositivo examina o meio para verificar a presença de sinal de dados. Se estiver livre, o dispositivo envia uma notificação através do meio com sua intenção de usá-lo. O dispositivo, então, envia os dados. Esse método é usado pelas tecnologias de rede sem fio 802.11 e será objeto de estudo no capítulo 7 deste livro.



ATIVIDADES

Acesse os *sites* e explore os recursos *on-line*.

Disponível em:

<http://wps.aw.com/br_kurose_redes_3/40/10271/2629589.cw/index.html>.

Animações do livro de Forouzan

Disponível em:

<http://highered.mheducation.com/sites/0072967722/student_view0/animations.html#>.



REFLEXÃO

Você viu nesta aula os principais elementos da camada de acesso à rede e como ela funciona.



LEITURA

Leia os capítulos 7, 11 e 12 do livro **Comunicação de dados e redes de computadores**, de Behrouz A. Forouzan.

Saiba mais

Assista aos vídeos a seguir:

Disponível em: <<https://www.youtube.com/watch?v=yNDVGcqYrbc>>.

Disponível em: <https://www.youtube.com/watch?v=xb0Wt1Oi2_4>.

Disponível em: <<https://www.youtube.com/watch?v=jP61J1TLGg4>>.



REFERÊNCIAS BIBLIOGRÁFICAS

FOROUZAN, Behrouz A. **Comunicação de dados e redes de computadores**. 4. ed. São Paulo: McGraw-Hill, 2008.

KUROSE, James F. e ROSS, Keith W. **Redes de computadores e a Internet**: uma abordagem top-down. 4. ed. São Paulo: Addison Wesley, 2009.

Tanenbaum, Andrew S. **Redes de computadores**. 5. ed. Rio de Janeiro: Campus, 2007.

3

Arquitetura Ethernet

A Ethernet é composta de padrões das camadas inferiores, física e enlace. Embora as especificações Ethernet suportem meios físicos diferentes, larguras de banda diferentes e outras variações das camadas física e de enlace, o formato básico de estrutura e esquema de endereço é o mesmo para todas as variedades da Ethernet.

Este capítulo examina as características e a operação Ethernet à medida que ela evoluiu de uma tecnologia de comunicação de dados de meio físico compartilhado com base em contenção para a tecnologia full-duplex de alta largura de banda atual.



OBJETIVOS

- Descrever a evolução da Ethernet.
 - Descrever a função e as características do método de controle de acesso ao meio utilizado pelo protocolo Ethernet.
 - Descrever os recursos da camada física e de enlace de dados da Ethernet.
 - Comparar e contrastar hubs e switches Ethernet.
 - Explicar o address resolution protocol (ARP).
-

3.1 Ethernet

A Ethernet foi primeira LAN do mundo. Sua versão original foi criada por **Robert Metcalfe** e seus colegas da Xerox há mais de 30 anos.

Seu primeiro padrão Ethernet foi publicado em 1980 e, como seus criadores desejavam que fosse um padrão compartilhado do qual todos pudessem se beneficiar, ela foi lançada como um padrão aberto, dando origem no início da década de 80 aos primeiros produtos comerciais.

O *Institute of Electrical and Electronics Engineers* (Instituto de Engenharia Elétrica e Eletrônica - IEEE) publicou, em 1985, padrões para *LANs* que começam com o número 802, sendo o da Ethernet o **IEEE 802.3**.

A Ethernet opera nas duas camadas inferiores do modelo OSI: a camada de enlace de dados e a camada física.

A Ethernet na Camada 1 envolve sinais, fluxos de *bits* que trafegam no meio, componentes físicos que colocam sinais no meio e várias topologias. A camada 1 da Ethernet desempenha um papel essencial na comunicação que ocorre entre os dispositivos, mas tem limitações que são corrigidas na camada de enlace, conforme descrito na tabela 3.1:

LIMITAÇÕES DA CAMADA 1	SOLUÇÃO NA CAMADA 2
Reconhece somente fluxos de bits.	Utiliza quadros para organizar os bits em grupos.
Não consegue identificar dispositivos.	Utiliza endereços físicos , para identificar os nós.
Não consegue controlar o acesso ao meio.	Controla o acesso ao meio utilizando o CSMA/CD .

Tabela 3.1 – Limitações da camada física Ethernet e soluções da camada de enlace.

3.2 Encapsulamento de dados

O encapsulamento de dados fornece três funções principais:

- Delimitação de quadros
- Endereçamento
- Detecção de erros

O processo de encapsulamento de dados inclui a montagem de quadros antes da transmissão e a análise de quadros em seu recebimento. Ao formar o quadro, a camada de enlace da Ethernet adiciona um cabeçalho e um trailer à PDU da Camada 3.

Ao realizar o enquadramento, podemos identificar os *bits* que compõem o quadro, através de delimitadores, o que favorece a sincronização entre os nós transmissores e receptores.

O processo de encapsulamento também fornece o endereçamento da camada de enlace de dados. Cada cabeçalho Ethernet adicionado ao quadro contém o endereço físico (endereço MAC) que permite que um quadro seja entregue a um nó de destino.

Uma função adicional do encapsulamento de dados é a detecção de erros. Cada quadro Ethernet contém um trailer com verificação de redundância cílica (CRC) do conteúdo do quadro. Este método permite que o receptor verifique se o quadro foi recebido sem erros.



CONEXÃO

Se desejar saber mais a respeito do funcionamento do CRC, assista aos videos:

Disponível em: <<https://www.youtube.com/watch?v=XWcJcybL3JQ>>.

Disponível em: <<https://www.youtube.com/watch?v=wyUNSzDbFjg>>.

3.3 O Controle de acesso ao meio físico

As implementações iniciais de Ethernet utilizavam, do ponto de vista lógico, uma topologia em barramento multiacesso. Isso significa que todos os nós (dispositivos) naquele segmento de rede compartilham o meio. Isso também

significa que todos os nós naquele segmento recebem todos os quadros transmitidos por qualquer nó.



ATENÇÃO

Como veremos mais à frente, a Ethernet original utilizava uma topologia física em barramento e mesmo implementações posteriores em estrela utilizavam um HUB, equipamento de camada 1, funcionando como um barramento do ponto de vista lógico.

Como todos os nós recebem todos os quadros, cada nó precisa determinar se um quadro deve ser aceito e processado. Para tal, deve existir algum método tipo de endereçamento no quadro, que é fornecido pelo endereço MAC.

O método de controle de acesso ao meio para a Ethernet clássica é o *Carrier sense multiple access with collision detection* (CSMA/CD). Este método está descrito mais adiante no capítulo.

3.4 Endereçamento de camada de enlace

Para permitir a comunicação entre computadores em uma rede, cada um precisa ser identificado de forma única. Assim, cada interface de rede de um computador tem um endereço físico, chamado de endereço media access control (ou endereço MAC), que está gravado na placa de rede.(figura 3.1)

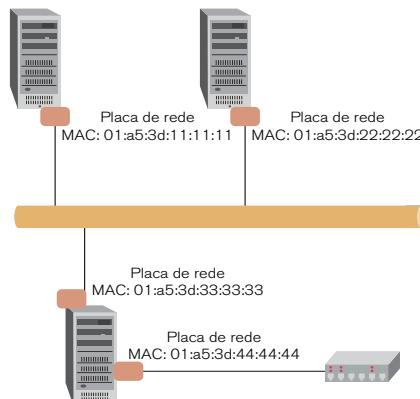


Figura 3.1 – Endereço MAC. Fonte: elaborado pelo autor.

Os endereços MAC têm 48 *bits* de comprimento e são expressos com doze dígitos hexadecimais. Os primeiros seis dígitos hexadecimais, administrados pelo IEEE, identificam o fabricante ou fornecedor e, portanto, compreendem o *organizational unique identifier*(OUI). Os seis dígitos hexadecimais restantes compreendem o número serial de interface ou outro valor administrado pelo fornecedor específico.

O fabricante da placa de rede atribui um endereço físico a cada uma delas. Esse endereço é gravado em um chip na placa de rede, portanto se a placa de rede fosse trocada em um computador, o endereço físico da estação mudaria para o novo endereço MAC.

Os endereços MAC devem ser únicos, ou seja, não podem existir no mundo duas placas de redes com o mesmo endereço físico. Sem eles, teríamos um conjunto de computadores sem identificação na rede.

O endereçamento é uma parte importante do encapsulamento e, em consequência do desencapsulamento. Cada quadro deve possuir os endereços MAC do nó origem e do nó destino. As informações não podem ser enviadas ou entregues corretamente em uma rede sem esses endereços. Devemos entender que, para o funcionamento da rede, a identificação correta dos computadores é fundamental e que os endereços MAC dão aos nós um nome exclusivo e permanente (o número de endereços possíveis não vai se esgotar tão cedo, já que há mais de 2 trilhões de endereços MAC possíveis).

Os endereços MAC têm uma enorme desvantagem, pois, por não terem estrutura, são considerados espaços de endereço contínuos. Fornecedores diferentes têm diferentes OUIs, mas elas são como números de identidade. Assim que sua rede atingir mais do que alguns poucos computadores, essa desvantagem se tornará um problema real.

Foi exatamente para resolver este problema que surgiu o endereçamento de rede (camada 3), que será objeto de estudo no próximo capítulo.

Temos três tipos de endereçamento

- **Broadcast:** neste tipo de endereçamento, o quadro é enviado para todos os nós do segmento de rede. Uma analogia seria uma pessoa falando em voz alta para todos os presentes ouvirem. O endereço MAC de broadcast é FF:FF:FF:FF:FF:FF

- **Multicast:** neste tipo de endereçamento, o quadro é enviado para um grupo de nós do segmento de rede. Uma analogia seria representada pelos *e-mails* enviados para um grupo

- **Unicast:** neste tipo de endereçamento, o quadro é enviado para um nó específico. Equivale a uma ligação telefônica para falar com uma pessoa.



ATENÇÃO

Devemos destacar que a analogia do *multicast* com o grupo de *e-mail* refere-se apenas à ideia de enviar algo para um determinado grupo, já que, no *e-mail*, cada pessoa tem seu próprio endereço *unicast* e, no *multicast*, existe um endereço específico para o grupo, ou seja, o próprio grupo possui um endereço.

3.5 Transmissão na camada de enlace

Quando um dispositivo em um segmento de rede quer enviar dados para outro dispositivo, ele pode endereçar o quadro colocando seu MAC como origem e o MAC do outro dispositivo como destino. Como esse quadro trafega pelos meios da rede, a placa de rede em cada dispositivo verifica se o seu endereço MAC corresponde ao endereço de destino físico carregado pelo quadro de dados. Se não corresponder, a placa de rede descarta o quadro de dados. Quando os dados passam pela estação de destino, a placa de rede dessa estação faz uma cópia, retira os dados do envelope e passa-os ao computador.

Observe a figura 3.2. Vamos supor que o computador à direita deseja mandar um pacote para o servidor de impressão:

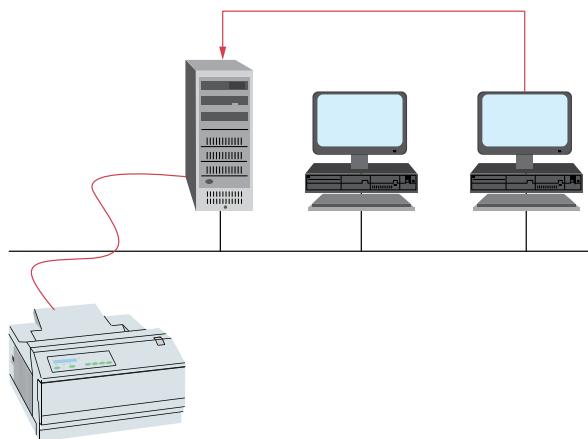


Figura 3.2 – Transmissão na camada 2. Fonte: elaborado pelo autor - Curso Network Esencial da Microsoft. Adaptado.

O pacote de dados descerá pelas várias camadas e, ao atingir a camada 2, será colocado no quadro o endereço de origem (02608c036592) e o endereço do destinatário (02608c428197).

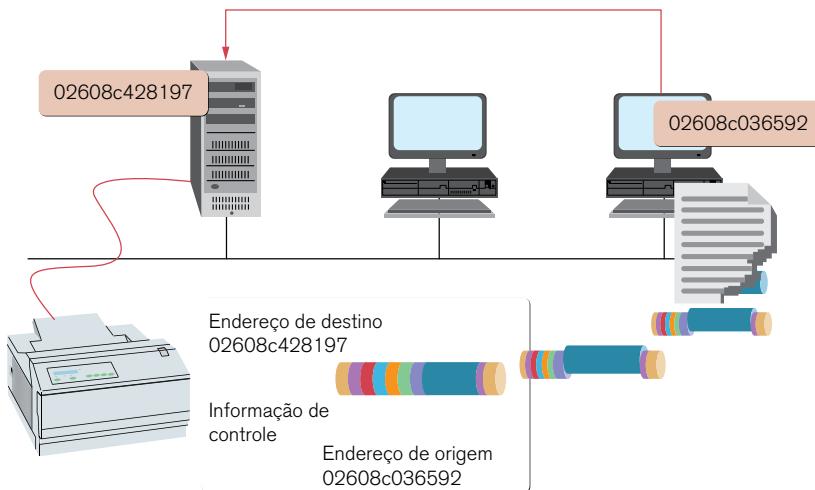


Figura 3.3 – Transmissão na camada 2. Fonte: Curso Network Essencial da Microsoft. Adaptado.

O quadro é, então, transmitido segundo as normas da camada 1.

Todo os computadores ligados ao meio recebem o quadro e cada um deles, ao recebê-lo, verifica a exatidão do endereço do destinatário.

Na figura 3.4, podemos observar que o computador do meio (endereço MAC 02608c741965) compara seu endereço com o endereço do destinatário (02608c428197). Como são diferentes, ele despreza o quadro.

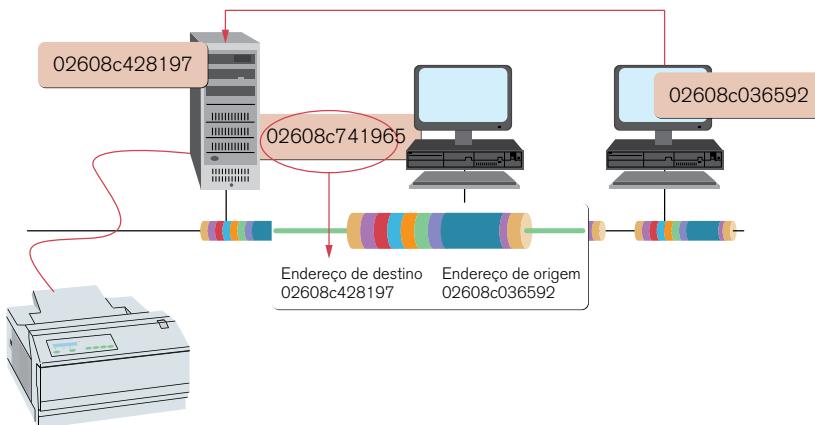


Figura 3.4 – Transmissão na camada 2. Fonte: Curso Network Essencial da Microsoft. Adaptado.

O pacote continua seu percurso no cabo e atinge o servidor de impressão. A placa de rede do servidor compara seu endereço MAC com o endereço do destinatário (02608c428197). Como são iguais, ela copia o quadro e inicia o processo de desencapsulamento (figura 3.5).

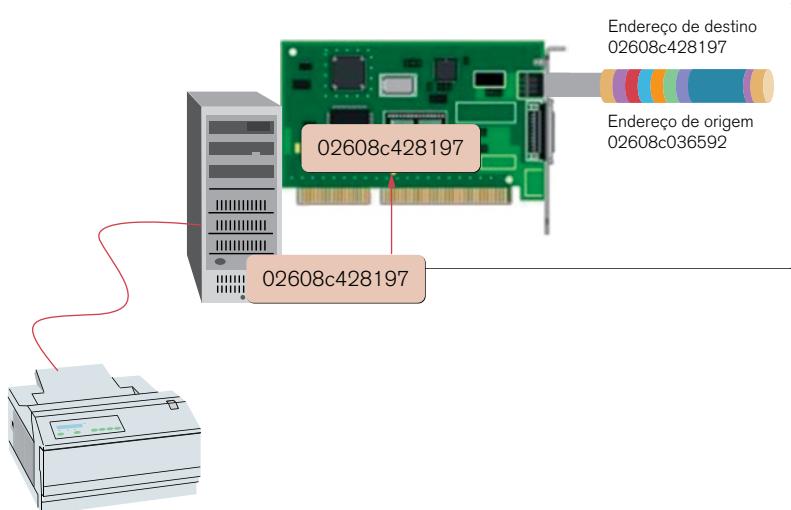


Figura 3.5 – Transmissão na camada 2. Fonte:Curso Network Essencial da Microsoft. Adaptado.

O pacote, então, sobe pelas camadas do modelo OSI, sendo desencapsulado. Ao atingir a camada de aplicação, temos os dados recuperados e o servidor de impressão pode, dessa maneira, encaminhar o documento para a impressora (figura 3.6).

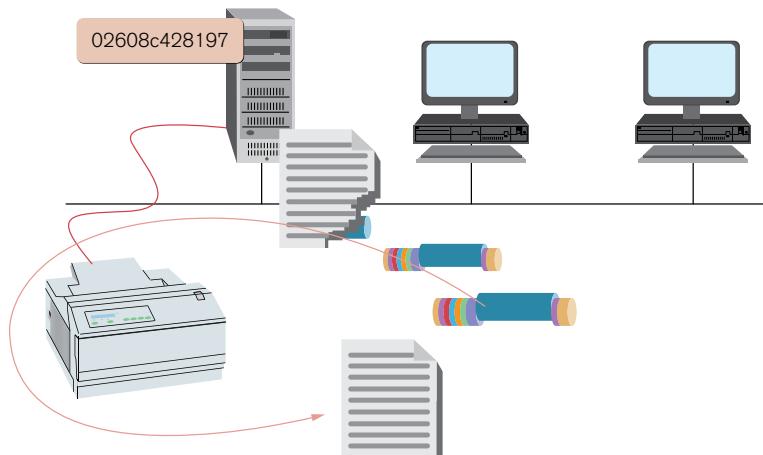


Figura 3.6 – Transmissão na camada 2. Fonte: Curso Network Essencial da Microsoft. Adaptado.

3.6 Evolução da Ethernet

Os primeiros padrões de Ethernet, conhecidos como *Thicknet* (10BASE5) e *Thinnet* (10BASE2), usavam cabo coaxial para conectar computadores em uma topologia de barramento. Cada computador era diretamente conectado ao *backbone*.

A 10BASE5 ou *Thicknet* utilizava um cabo coaxial grosso que permitia distâncias de cabeamento de até 500 metros antes que o sinal precisasse de um repetidor. A 10BASE2 ou *Thinnet* usava um cabo coaxial fino de diâmetro menor e mais flexível do que a *Thicknet* e que permitia distâncias de cabeamento de 185 metros.

Estes primeiros padrões foram feitos pensando em um ambiente de baixa largura de banda, sendo o acesso aos meios realizado pelo CSMA que evolui para o CSMA/CD. Além de ser uma topologia de barramento lógica na camada de enlace de dados, a Ethernet também usava uma topologia de barramento física.

Com a evolução da tecnologia, os meios físicos de cabo coaxial foram substituídos pelas primeiras categorias de cabos UTP. Os cabos UTP eram mais fáceis de trabalhar que os cabos coaxiais, mais leves e mais baratos, e deram origem ao padrão 10BASSET, onde o ponto central do segmento de rede normalmente era um *hub*.

CONCEITO

Os **hubs** concentram as conexões. Em outras palavras, eles tomam um grupo de nós e permitem que a rede os veja como uma só unidade. Quando o sinal(*bit*) chega a uma porta, é copiado para as outras portas para que todos os segmentos na LAN recebam o quadro. Utilizar o *hub*, cria uma topologia em estrela, em substituição ao barramento, o que aumentou a confiabilidade da rede ao permitir que qualquer cabo falhe sem interromper toda a rede. O *hub* fornece um meio compartilhado *half duplex*, que continua sujeito a colisões.

Durante períodos de baixa atividade de comunicação, as poucas colisões que ocorrem são gerenciadas pelo **CSMA/CD**, com pouco ou nenhum impacto no desempenho, no entanto, à medida que o número de dispositivos e o

consequente tráfego de dados cresce, o aumento das colisões pode ter impacto considerável no trabalho dos usuários.

Uma boa analogia é quando saímos para o trabalho ou para a escola de manhã, com as ruas relativamente vazias e sem congestionamento. Mais tarde, quando há mais carros, pode haver colisões e o tráfego fica mais lento.

A figura 3.7 mostra uma topologia estrela com *hub*. Nesta, PC1 tenta enviar um quadro para PC2 e, ao mesmo tempo, PC4 tenta enviar um quadro para PC3. Como o *hub* é *half-duplex*, ocorre uma colisão, representada na figura pelos pacotes em chama. Desta forma, podemos notar que todos os computadores da topologia estão no mesmo **domínio de colisão**.

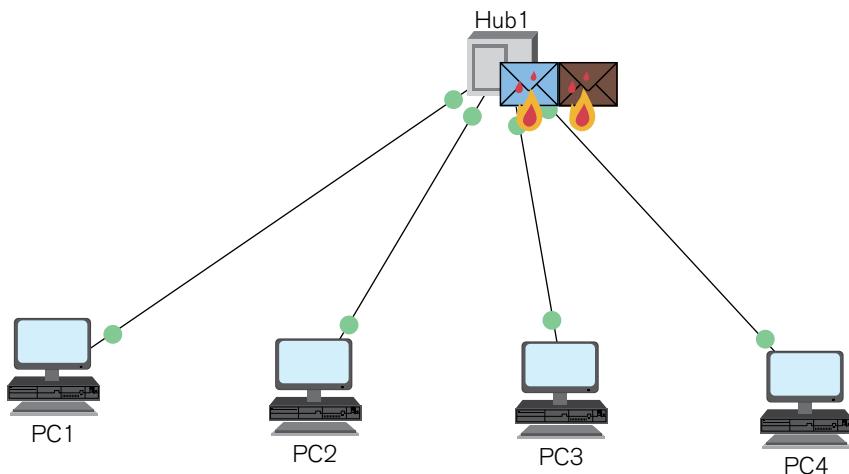


Figura 3.7 – Colisão. Fonte: elaborado pelo autor.



CONCEITO

Os dispositivos conectados que acessam um meio físico compartilhado por meio de um *hub* ou uma série de *hubs* diretamente conectados compõem o que chamamos de domínio de colisão. O domínio de colisão também é conhecido como segmento de rede, sendo composto por todos os nós que são afetados por uma colisão. Os *hubs* e repetidores contribuem para o aumento do tamanho do domínio de colisão.

3.7 CSMA/CD (*carrier sense multiple access with collision detection*)

O CSMA/CD é método de acesso padrão da Ethernet.

A parte CSMA do método determina que, quando uma estação deseja transmitir uma mensagem, ela “escuta” o canal. Se ele estiver livre, ela poderá transmitir (figura 3.8); se estiver ocupado; ela deverá esperar até que o meio esteja livre (figura 3.9). Esta regra diminui as colisões, mas não as impede, já que duas estações podem perceber o canal como livre ao mesmo tempo e realizarem a transmissão (figura 3.10), o que provoca uma colisão (figura 3.11).

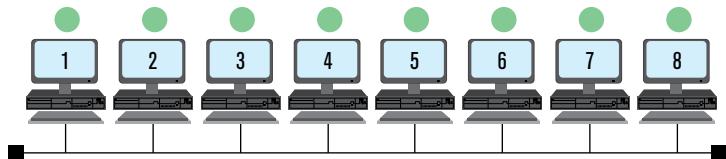


Figura 3.8 – CSMA – Meio livre. Fonte: elaborado pelo autor - Curso Network Essencial da Microsoft. Adaptado.

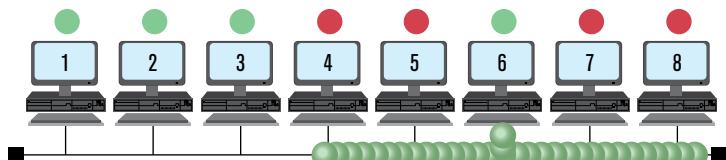


Figura 3.9 – CSMA – Meio ocupado. Fonte: elaborado pelo autor - Curso Network Essencial da Microsoft. Adaptado.

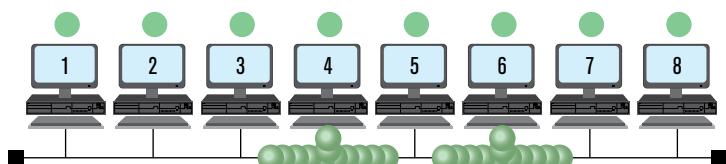


Figura 3.10 – CSMA – Duas estações percebem o meio livre e transmitem a mensagem..
Fonte: elaborado pelo autor - Curso Network Essencial da Microsoft. Adaptado.

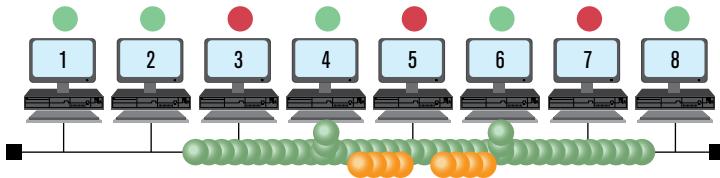


Figura 3.11 – CSMA – Colisão. Fonte: elaborado pelo autor - Curso Network Essencial da Microsoft. Adaptado.

A parte CD do método estabelece que a detecção de **colisão** é realizada durante a transmissão. Ao transmitir, uma estação fica o tempo todo escutando o meio e, notando uma colisão, aborta a transmissão (figura 3.12). Detectada a colisão, a estação espera por um **tempo aleatório** para tentar a retransmissão (figura 3.13 e figura 3.14).

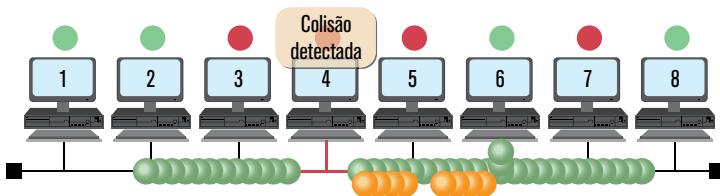


Figura 3.12 – CSMA/CD – Detecção de colisão. Fonte: elaborado pelo autor - Curso Network Essencial da Microsoft. Adaptado.

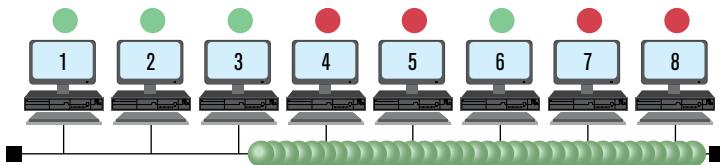


Figura 3.13 – CSMA/CD – Estação 6 retransmite. Fonte: elaborado pelo autor - Curso Network Essencial da Microsoft. Adaptado.

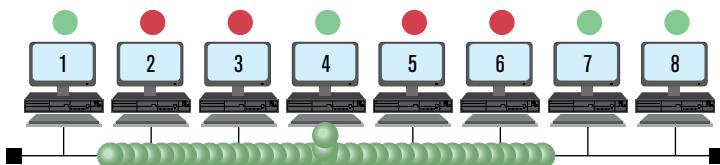


Figura 3.14 – CSMA/CD – Estação 4 retransmite. Fonte: elaborado pelo autor - Curso Network Essencial da Microsoft. Adaptado.



ATENÇÃO

Se as estações envolvidas na colisão tentassem retransmitir esperando o mesmo tempo, ocorreria uma nova colisão. Por isso, o tempo que cada uma espera para tentar a retransmissão deve ser diferente.

3.8 Ethernet comutada

A evolução tecnológica levou à substituição dos *hubs* pelos comutadores (*switches*) em redes Ethernet. Os comutadores podem controlar o fluxo de dados ao isolar cada porta e enviar um quadro apenas a seu destino adequado (se este for conhecido), em vez de enviar cada quadro a cada dispositivo.

A figura 3.15 mostra uma topologia estrela com *switch*. Nesta PC1, tenta enviar um quadro para PC2 e, ao mesmo tempo, PC4 tenta enviar um quadro para PC3. Como o comutador pode chavear entre os destinos diferentes não ocorre a colisão, o que melhora o desempenho da rede.

O comutador reduz o número de dispositivos que recebe cada quadro, o que, por sua vez, diminui ou minimiza a possibilidade de colisões. Isso e a introdução posterior das comunicações *full-duplex* (ter uma conexão que possa transmitir e receber sinais ao mesmo tempo) permitiram o desenvolvimento da Ethernet 1 Gbps e, na prática, eliminou as colisões.

Na mesma situação da figura 3.15, considere agora que o PC1 tente enviar um quadro para PC2 e, ao mesmo tempo, PC4 tenta enviar um quadro para PC1. Note que PC1 precisará transmitir e receber ao mesmo tempo. Como o *switch* é *full-duplex*, não ocorre a colisão e a transmissão ocorre simultaneamente nos dois sentidos.

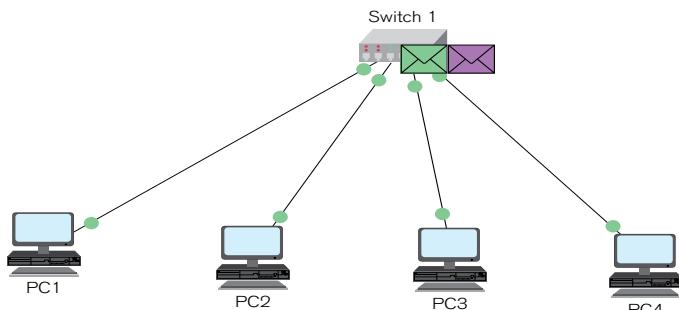


Figura 3.15 – Ethernet com comutador – livre de colisão. Fonte: elaborado pelo autor.

3.9 Endereços MAC e IP

Há dois endereços principais atribuídos a um dispositivo de host:

- Endereço físico (o endereço MAC)
- Endereço lógico (o endereço IP)

Tanto o endereço MAC como o IP trabalham juntos para identificar um dispositivo na rede. O processo de usar os endereços MAC e IP para localizar um computador é semelhante ao processo de usar o nome e o endereço de uma pessoa para enviar uma carta.

O nome da pessoa geralmente não muda, o endereço, entretanto, por referir-se ao local onde mora, pode ser alterado.

Assim como o nome de uma pessoa, o endereço MAC de um host não muda; ele é atribuído fisicamente à placa de rede do host e é conhecido como endereço físico. O endereço físico permanece igual, independentemente de onde o *host* esteja colocado.

O endereço IP é semelhante ao endereço de uma pessoa. Esse endereço baseia-se no local em que o *host* realmente se encontra. Por meio desse endereço, é possível que um quadro determine o local para o qual um quadro deve ser enviado. O endereço IP ou o endereço de rede é conhecido como um endereço lógico por ser atribuído logicamente. Ele é atribuído a cada *host* por um administrador de rede com base na rede local em que o host está conectado.

Os endereços MAC físico e IP lógico são necessários para que um computador se comunique em uma rede hierárquica, assim como o nome e o endereço de uma pessoa são necessários para enviar uma carta.

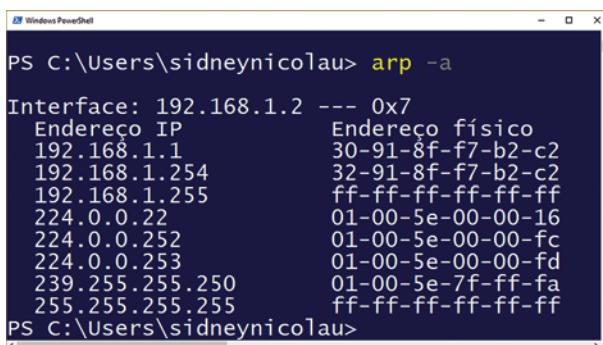
3.10 *Address resolution protocol – ARP* (protocolo para resolução de endereços)

Cada nó em uma rede IP tem um endereço MAC e um endereço IP. Para enviar dados, o nó deve usar esses dois endereços. O nó deve usar seus próprios endereços MAC e IP nos campos origem e deve fornecer um endereço MAC e um endereço IP para o destino. Enquanto o endereço IP destino será fornecido por uma camada superior, o nó emissor precisará de uma maneira para localizar o

endereço MAC destino para um determinado *link* de Ethernet. Essa é a finalidade do ARP.

O ARP baseia-se em determinados tipos de mensagens de *broadcast* Ethernet e mensagens *unicast* Ethernet, chamadas solicitações ARP e respostas ARP.

Para que um quadro seja colocado no meio físico da LAN, ele deve possuir um endereço MAC de destino. Quando um pacote é enviado à camada de enlace para ser encapsulado em um quadro, o nó consulta uma tabela em sua memória para encontrar o endereço da camada de enlace que é mapeado ao endereço IPv4 de destino. Essa tabela é chamada de **Tabela ARP** ou de **ARP Cache** (figura 3.16). A tabela ARP é armazenada na RAM do dispositivo.



```
PS C:\Users\sidneynicolau> arp -a
Interface: 192.168.1.2 --- 0x7
Endereço IP      Endereço físico
192.168.1.1      30-91-8f-f7-b2-c2
192.168.1.254    32-91-8f-f7-b2-c2
192.168.1.255    ff-ff-ff-ff-ff-ff
224.0.0.22        01-00-5e-00-00-16
224.0.0.252       01-00-5e-00-00-fc
224.0.0.253       01-00-5e-00-00-fd
239.255.255.250  01-00-5e-7f-ff-fa
255.255.255.255  ff-ff-ff-ff-ff-ff
PS C:\Users\sidneynicolau>
```

Figura 3.16 – ARP CACHE. Fonte: elaborado pelo autor.

Cada entrada ou linha da tabela ARP possui um par de valores: um endereço IP e um endereço MAC. Nós 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 gera a *cache* de mapeamento para os dispositivos na rede local

Para começar o processo, um nó de transmissão tenta localizar na tabela ARP o endereço MAC mapeado a um destino IPv4. Se este mapa estiver em *cache* na tabela, o nó usa o endereço MAC como o MAC de destino no quadro que encapsula o pacote IPv4. O quadro é, então, codificado no meio físico de rede.

Quando o ARP recebe uma solicitação para mapear um endereço IPv4 a um endereço MAC, ele procura um mapa em cache na sua tabela ARP. Se não

encontrar uma entrada, o encapsulamento do pacote de IPv4 falha e os processos de camada 2 notificam o ARP que precisa de um mapa. (figura 3.17).

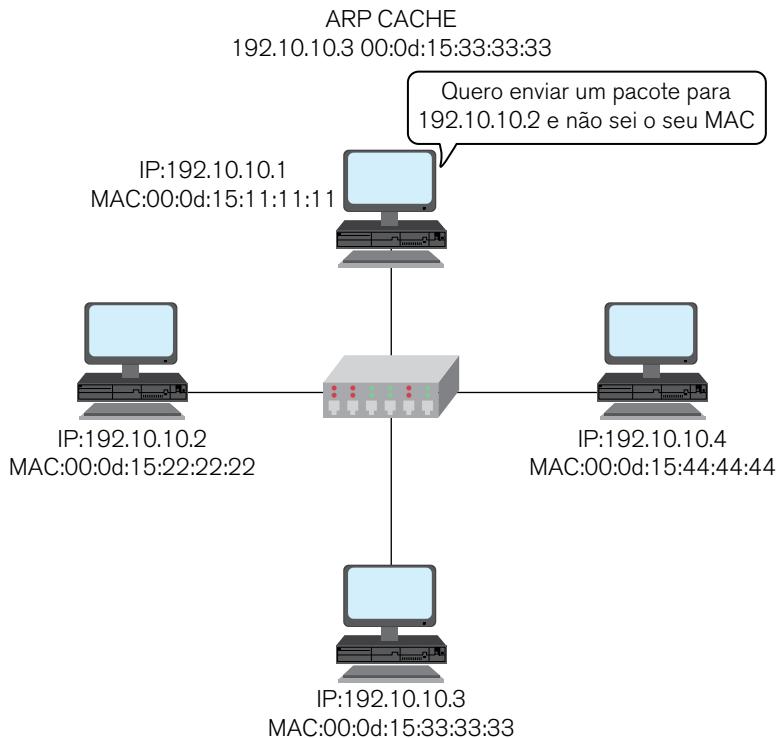


Figura 3.17 – Endereço não mapeado no cache. Fonte: elaborado pelo autor.

Os processos ARP enviam, então, um pacote de solicitação ARP para descobrir o endereço MAC do dispositivo de destino na rede local. Esta solicitação denomina-se **ARP Request** (figura 3.18).



ATENÇÃO

O ARP Request é enviado para o endereço MAC de destino FF:FF:FF:FF:FF:FF que corresponde ao MAC de broadcast, o que faz com que todos os computadores do segmento de rede aceitem o quadro.

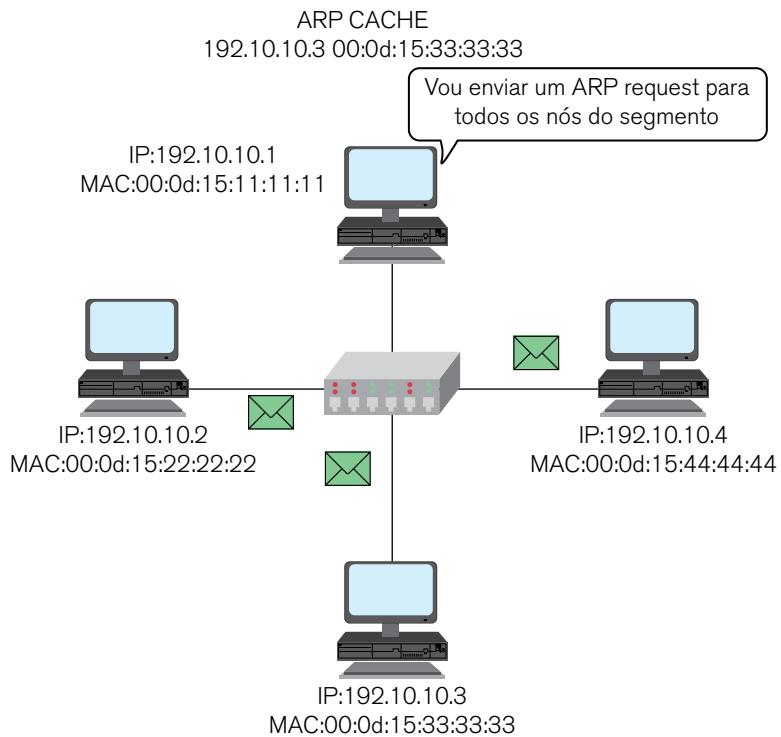


Figura 3.18 – ARP Request. Fonte: elaborado pelo autor.

Se o dispositivo que está recebendo a solicitação tiver o endereço IP de destino, ele responderá com uma resposta ARP (**ARP Reply**). Este dispositivo aproveita para criar uma entrada em seu ARP *cache* com o MAC do solicitante (figura 3.19).

ATENÇÃO

O **ARP Reply** é enviado tendo como endereço MAC de destino o da máquina solicitante utilizando endereçamento *Unicast*.

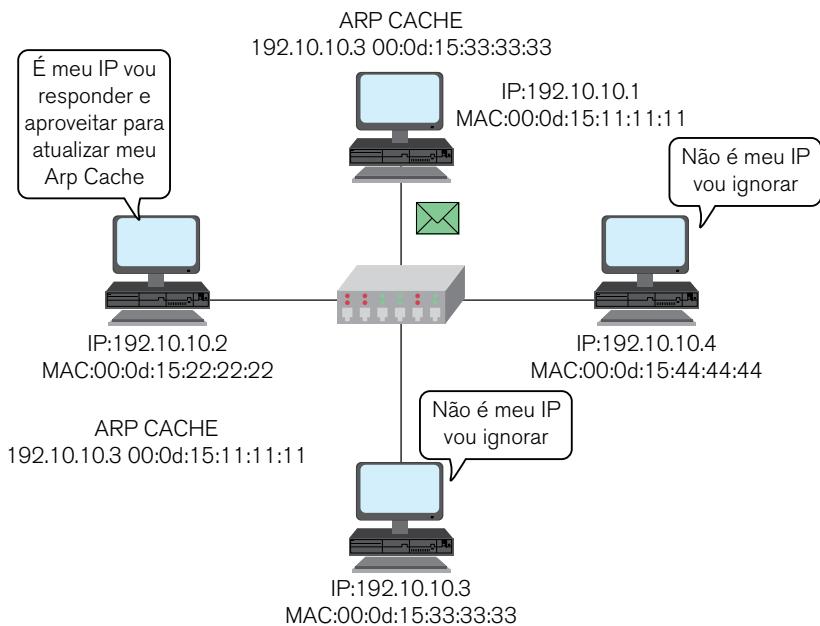


Figura 3.19 – ARP Reply. Fonte: elaborado pelo autor.

Os pacotes para o endereço IPv4 podem, agora, ser encapsulados em quadros. Se nenhum dispositivo responder à solicitação ARP, o pacote será abandonado porque o quadro não poderá ser criado. Essa falha de encapsulamento é informada para as camadas superiores do dispositivo. Se o dispositivo for um dispositivo intermediário como, por exemplo, um roteador, as camadas superiores poderão optar por responder ao *host* de origem com um erro, através de um pacote ICMPv4.

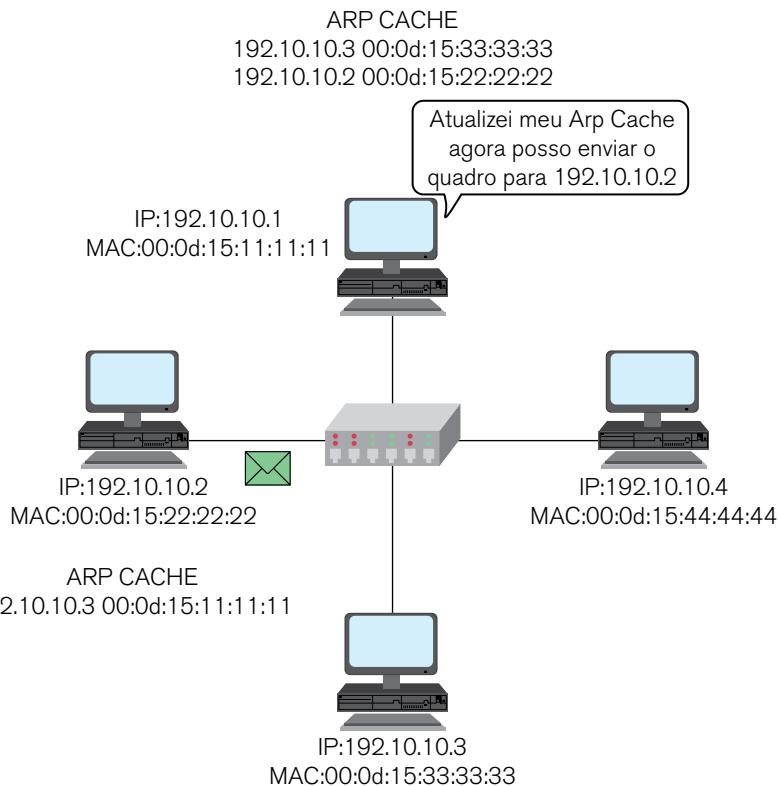


Figura 3.20 – Envio do quadro. Fonte: elaborado pelo autor.



ATIVIDADES

Assista aos vídeos abaixo:

Disponível em: <<https://www.youtube.com/watch?v=4LE-40SC6Rc>>.

Disponível em: <<https://www.youtube.com/watch?v=t2kIOZcXZqc>>.

Disponível em: <<https://www.youtube.com/watch?v=8LKspzz-zQo>>.

Disponível em: <<https://www.youtube.com/watch?v=7xa7TjEebEM>>.

Disponível em: <<https://www.youtube.com/watch?v=EjxFVP0pDGU>>.

Acesse os sites e explore os recursos on-line.

Disponível em:

<http://wps.aw.com/br_kurose_redes_3/40/10271/2629589.cw/index.html>.

Animações do livro de Forouzan

Disponível em:

<http://highered.mheducation.com/sites/0072967722/student_view0/animations.html#>.



REFLEXÃO

Você viu nesta aula como funciona a principal arquitetura de redes locais, a Ethernet.



LEITURA

Leia o capítulo 13 do livro **Comunicação de dados e redes de computadores**, de Behrouz A. Forouzan.



REFERÊNCIAS BIBLIOGRÁFICAS

FOROUZAN, Behrouz A. **Comunicação de dados e redes de computadores**. 4. ed. São Paulo: McGraw-Hill, 2008.

KUROSE, James F. e ROSS, Keith W. **Redes de computadores e a Internet: uma abordagem top-down**. 4. ed. São Paulo: Addison Wesley, 2009.

Tanenbaum, Andrew S. **Redes de computadores**. 5. ed. Rio de Janeiro: Campus, 2007.

4

Camada de Rede da Internet

A camada de redes é responsável pelo roteamento, ou seja, por encontrar o caminho (rota) entre o nó ou host de origem e o nó ou host de destino.

É nesta camada também que encontramos o protocolo IP e seu esquema de endereçamento, que nos permite determinar não somente o endereço do host, como também a rede a que ele pertence.

Ao longo deste capítulo, iremos abordar o endereçamento IP e os princípios que regem o roteamento.



OBJETIVOS

- Identificar os tipos de endereço IP.
 - Conhecer o roteamento.
-

4.1 Camada de rede

Realiza o transporte do pacote da estação remetente à receptora. Para tal, todas as estação e equipamentos no caminho necessitam ter o mesmo protocolo de rede.

O nível de rede provê os meios funcionais e procedurais para a transmissão de dados com conexão orientada ou não orientada.



ATENÇÃO

Na arquitetura TCP/IP, a camada de redes trabalha apenas sem conexão

Todo o transporte de pacotes, desde a origem até o destino, passando por todo um caminho que pode conter vários nós e sub-redes, é função do nível de redes

A figura 4.1 mostra os dois tipos de sistemas existentes em uma rede de **dispositivos finais** (no caso os computadores) que trabalham todas as camadas do RMOSI e os **dispositivos intermediários** (no caso os roteadores) que trabalham apenas até a camada de rede

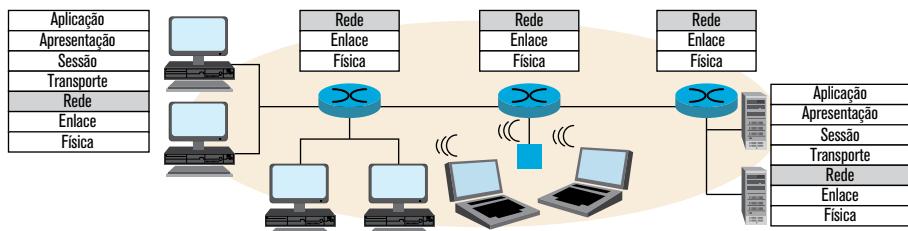


Figura 4.1 – Camada de rede. Fonte: elaborado pelo Autor - Kurose 2009. Adaptado.



CONCEITO

Dispositivos finais: também conhecidos como hosts, são os computadores, os telefones, as impressoras de rede ou quaisquer dispositivos utilizados pelo usuário final.

Dispositivos intermediários: são os dispositivos que direcionam o caminho dos dados sem, contudo, alterá-los, como, por exemplo, os hubs, os switches e os roteadores.

A camada de rede tem três funções principais

- Determinação do caminho: rota seguida por pacotes da origem ao destino
- algoritmos de roteamento.
- Comutação: mover pacotes dentro do roteador da entrada à saída apropriada.
- Estabelecimento da chamada: algumas arquiteturas de rede requerem que se determine o caminho antes de enviar os dados.

A camada de rede pode fornecer dois tipos de serviços:

- Circuito virtual: orientado à conexão
- Datagrama: não orientado à conexão

4.1.1 Circuito virtual (CV)

- A rota origem-destino se comporta de forma similar a um circuito telefônico.
- Orientado ao desempenho.
- A rede atua ao longo de toda a rota.
- Ocorre o estabelecimento de cada chamada antes do envio dos dados.
- Cada pacote carrega identificação do CV e não endereços de origem e de destino.
- Cada roteador, ao longo da rota, deve manter informações do estado de cada conexão estabelecida.
- Recursos de enlace, roteador (banda, *buffers*) podem ser alocados ao CV para permitir desempenho como o de um circuito.
- Usado pelas redes ATM, *frame-relay*, X.25.
- Não utilizado na *Internet*.

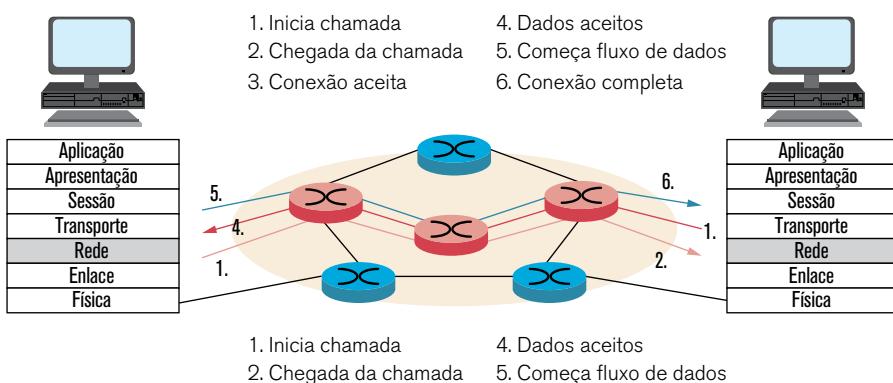


Figura 4.2 – Circuito virtual. Fonte: elaborado pelo Autor - Kurose 2009. Adaptado.

4.1.2 Datagrama

- O modelo da Internet
- Não requer estabelecimento de chamada na camada de rede.
- Roteadores: não guardam estado sobre conexões fim a fim.
- Não existe o conceito de "conexão" na camada de rede.
- Pacotes são roteados tipicamente usando endereços de destino.
- Dois pacotes entre o mesmo par origem-destino podem seguir caminhos diferentes.

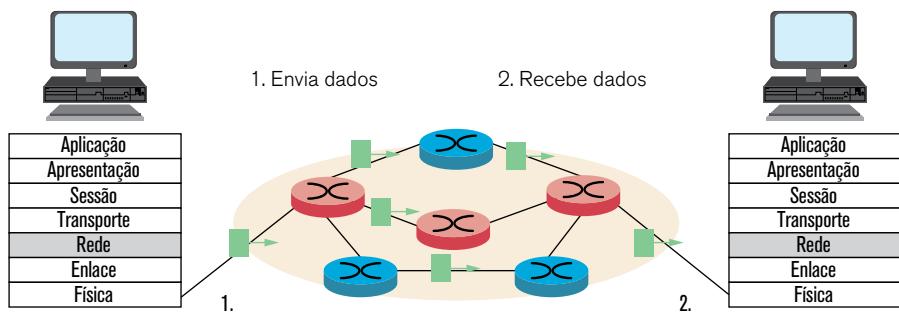


Figura 4.3 – Rede de datagramas. Fonte: elaborado pelo Autor - Kurose 2009. Adaptado.

4.2 Protocolo IP

Na arquitetura TCP/IP, a camada de rede é denominada inter-rede e seu protocolo mais importante é o IP, que, devido à popularização da *Internet*, tornou-se o protocolo-padrão de fato para a camada 3(rede).

O protocolo IP é um protocolo de datagrama, sem conexão, considerado de melhor esforço, ou seja, ele “jura de pés juntos” que fará o melhor possível para entregar o pacote enviado, mas não garante nada, nem a entrega nem a integridade dos dados enviados. Provê desta forma um serviço não confiável, cabendo às camadas superiores (transporte e/ou aplicação) garantir a confiabilidade da entrega e a integridade dos dados.

O protocolo IP fornece:

- Um esquema de endereçamento lógico independentemente do endereçamento da camada de enlace e da topologia física da rede;

- O roteamento dos pacotes pela rede, ou seja, a determinação do caminho entre as redes de origem e de destino.

Os **ativos de rede** responsáveis por interligar duas ou mais redes distintas são chamados de roteadores. Estas redes podem ser locais ou de longa distância. Um roteador para poder funcionar necessita de duas ou mais interfaces de rede, cada uma com seu próprio endereço específico, e de redes distintas (figura 4.4). Um roteador pode ser um equipamento específico ou um computador de uso geral com mais de uma interface de rede.

CONCEITO

Ativos de redes são equipamentos que geram ou regeneram sinais em uma rede como *hubs*, *switches* e roteadores.

Temos também os passivos de rede que se caracterizam por darem suporte ao transporte dos sinais gerados pelos ativos. Como exemplo temos *patch panel*, conectores e mídia física.

Já o dispositivo de rede que é apenas a origem ou destino de um datagrama IP (não realiza a função de roteamento) é chamado de *host*.

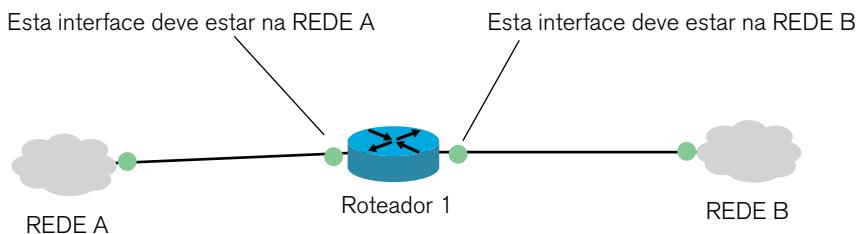


Figura 4.4 – Roteador e suas interfaces. Fonte: elaborado pelo autor.

4.3 Endereço IP

Um endereço IP é formado por 32 *bits* (4 *bytes*), em que cada *byte* é chamado de **octeto**, ou seja, o endereço IP é formado por 4 octetos (os campos W, X, Y, Z na figura 4.5).

O endereço IP funciona como o identificador lógico para uma interface de rede, caracterizando-se como um endereço hierárquico, pois sabe em qual rede a máquina está (id de rede ou *network id*) e qual o identificador da máquina naquela rede (id *host* ou *host id*). Para isso, parte dos octetos irá definir o id da rede e parte o id do *host* (figura 4.5).

Desta forma, ao contrário do endereço físico da interface, o endereço IP muda à medida que deslocamos o host de uma rede para outra.

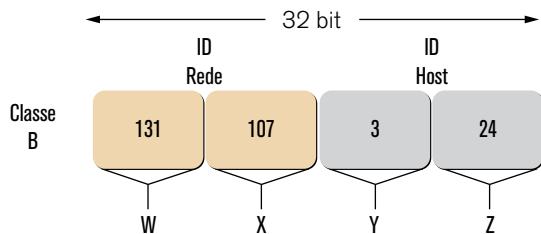


Figura 4.5 – Endereço IP. Fonte: elaborado pelo autor.

O endereço IP utiliza uma notação chamada notação decimal pontuada, em que cada octeto é representado por um número decimal (de 0 a 255) separados por um ponto ":".

O endereço IP: 11010000 11110101 00011100 10000011, por exemplo, é representado por 208.245.28.131.

Vejamos como isso é feito:

- Inicialmente separamos os 32 bits nos 4 octetos que compõem o endereço.
- A seguir transformamos o número binário formado pelo octeto em decimal.
- Por último, juntamos os números decimais e os separamos por um ":".

Endereço original 11010000 11110101 00011100 10000011

Octetos 1º. 2º. 3º. 4º.

Binário 11010000 11110101 00011100 10000011

Decimal 208 245 28 131

Representação final 208.245.28.131

A tabela 4.1 mostra como é realizada a conversão de binário para decimal.

128 2 ⁷	64 2 ⁶	32 2 ⁵	16 2 ⁴	8 2 ³	4 2 ²	2 2 ¹	1 2 ⁰	Decimal
0	0	0	0	0	0	0	0	0+0+0+0+0+0+0+0=0
0x128	0x64	0x32	0x16	0x8	0x4	0x2	0x1	
0	0	0	0	1	0	1	0	0+0+0+0+8+0+2+0=10
0x128	0x64	0x32	0x16	1x8	0x4	1x2	0x1	
0	0	1	0	1	1	0	0	0+0+32+0+8+4+0+0=44
0x128	0x64	1x32	0x16	1x8	1x4	0x2	0x1	
0	1	0	0	0	0	1	1	0+64+0+0+0+0+2+1=67
0x128	1x64	0x32	0x16	0x8	0x4	1x2	1x1	
0	1	1	0	0	1	0	1	0+64+32+0+0+4+0+1=101
0x128	1x64	1x32	0x16	0x8	1x4	0x2	1x1	
1	0	0	1	0	1	1	0	128+0+0+16+0+4+2+0=150
1x128	0x64	0x32	1x16	0x8	1x4	1x2	0x1	

Tabela 4.1 – Método de conversão de binário para decimal. Fonte: Prof. Antônio Sérgio Alves Cavalcante (cedido ao autor).



ATENÇÃO

Um octeto pode possuir valores de 0 a 255 em decimal, já que em binário pode ir de 00000000 (8 zeros) a 11111111 (8 uns).

Se tiver dúvidas na forma de conversão de binários para decimal, assista ao vídeo:

Disponível em: <<https://www.youtube.com/watch?v=cmR54KiSjFo>>.

Como vimos, o endereço IP possui informações de qual é a rede da estação e qual o id do *host* naquela rede. Como o endereço IP tem tamanho fixo, uma das opções seria dividir o endereço IP em duas metades, dois octetos para identificar a rede e dois octetos para o *host* (figura 4.5). Isto, entretanto, engessaria o endereçamento, pois só poderíamos ter $65536(2^{16})$ redes, cada uma com $65536(2^{16})$ *hosts*. Uma rede que possuísse apenas 100 *hosts* estaria utilizando um endereçamento de rede com capacidade de 65536 estações, o que também seria um desperdício.

4.4 Endereçamento por classes (*classfull*)

A forma original encontrada para determinar a porção rede e a porção *host* do endereço foi adotar **classes de endereço**.

As classes originalmente utilizadas na *Internet* são A, B, C, D e E, conforme mostrado na tabela 4.2.

As classes A, B e C são utilizadas para endereçar *host*. A classe D é uma classe especial para identificar endereços de grupo (*multicast*) e a classe E é reservada.

	Classes	Faixa (range) das classes (1º octeto)			Regra N bits de rede e H bits de host
End. de internet (unicast)	A	00000000 0	A	01111111 127	8 bits rede e 24 bits de host NNNNNNNN HHHHHHHH HHHHHHHH HHHHHHHH
					16 bits rede e 16 bits host NNNNNNNN NNNNNNNN HHHHHHHH HHHHHHHH
					16 bits rede e 16 bits host NNNNNNNN NNNNNNNN HHHHHHHH HHHHHHHH
					24 bits rede e 8 bits host NNNNNNNN NNNNNNNN NNNNNNNN HHHHHHHH
	D	11100000 224	A	11101111 239	Cada endereço representa um grupo multicast IP
	E	11110000 240	A	11111111 255	Endereços para teste ou uso futuro.

Tabela 4.2 – Classes de endereço IP. Fonte: Prof. Antônio Sérgio Alves Cavalcante (cedido ao autor).

A classe A utiliza 1 octeto para *network id* e 3 octetos para *host id*. A classe B utiliza 2 octetos para *network id* e 2 octetos para *host id*, enquanto um endereço de classe C utiliza 3 octetos para rede e 1 octeto para *host id*. Devemos observar que os octetos para *network id* são sempre os primeiros a partir a esquerda, por exemplo, no IP a classe a 10.15.30.50, o *network id* 10 e o *host id* 15.30.50

A distinção entre as classes de endereço é realizada pelo valor do primeiro octeto (mais à esquerda) do endereço. Veja na figura 4.6 o range de endereços de cada classe.

Com esta divisão, é possível acomodar um pequeno número de redes muito grandes (classe A) e um grande número de redes pequenas (classe C).

A Classe A possui endereços suficientes para endereçar 126 redes diferentes com até 16 777 214 *hosts* (estações) cada uma.

A Classe B possui endereços suficientes para endereçar 16 384 redes diferentes com até 65 535 *hosts* (estações) cada uma.

A Classe C possui endereços suficientes para endereçar 2 097 152 redes diferentes com até 254 *hosts* (estações) cada uma.

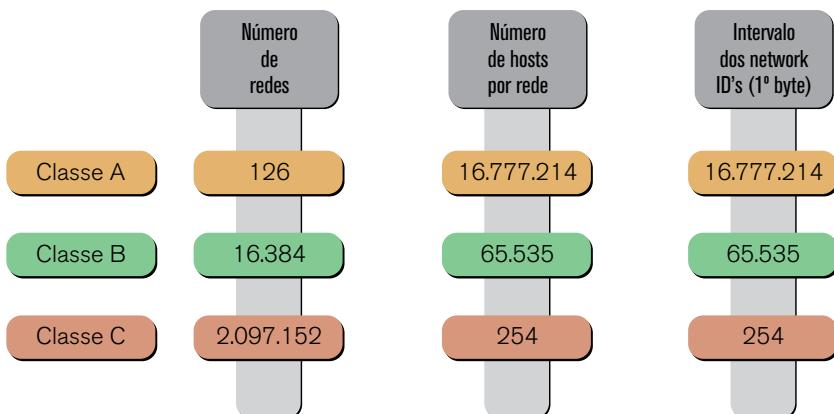


Figura 4.6 – Classes de endereço para hosts. Fonte: elaborado pelo Autor

Os *hosts* com mais de uma *interface de rede* (caso dos roteadores ou de máquinas interligadas a mais de uma rede, mas que não efetuam função de roteamento) possuem um endereço IP para cada uma. Um endereço IP identifica não uma máquina, mas sim uma conexão à rede.



ATENÇÃO

O endereçamento baseado em classes não é mais empregado na *Internet*. Hoje o endereçamento é chamado sem classe (*classless*), assunto que iremos estudar logo a seguir

Alguns endereços são reservados para funções especiais:

Endereço de rede: Identifica a própria rede e não uma *interface* de rede específica, representado por todos os *bits* de *host id* com o valor zero.

Exemplos de endereços:

- 19.0.0.0 - identifica a rede 19 (endereço classe A).
- 139.40.0.0 - identifica a rede 139.40 (endereço classe B).
- 199.27.90.0 - identifica a rede 199.27.90 (endereço classe C).

Endereço de broadcast: Identifica todas as máquinas na rede específica, representado por todos os *bits* de *host id* com o valor um. Exemplos de endereços:

- 19.255.255.255 - endereço de broadcast na rede 19.0.0.0
- 139.40.255.255 - endereço de broadcast na rede 139.40.0.0
- 199.27.90.255 - endereço de broadcast na rede 199.27.90.0

Em cada rede A, B ou C, são reservados o primeiro endereço e o último, sendo que eles não podem, portanto, serem usados por *interfaces* de rede. A tabela 4.3 exemplifica a situação.

Classe A				
115 01110011	0 00000000	0 00000000	0 00000000	End. REDE
115 01110011	255 11111111	255 11111111	255 11111111	End. BROADCAST da REDE

Classe B				
165 10100101	32 00100000	0 00000000	0 00000000	End. REDE
165 10100101	32 00100000	255 11111111	255 11111111	End. BROAD-CAST da REDE
Classe C				
192 11000000	255 11111111	255 11111111	0 00000000	End. REDE
192 11000000	255 11111111	255 11111111	255 11111111	End. BROAD-CAST da REDE

Tabela 4.3 – Endereços de rede e broadcast. Fonte: Prof. Antônio Sérgio Alves Cavalcante (cedido ao autor).

Endereço de *broadcast limitado*: identifica um *broadcast* na própria rede, sem especificar a que rede pertence, representado por todos os *bits* do endereço iguais a um = 255.255.255.255.

Endereço de *loopback*: também chamado *localhost*: identifica a própria máquina. Serve para enviar uma mensagem para a própria máquina rotear para ela mesma, ficando a mensagem no nível IP, sem ser enviada à rede. Este endereço é 127.0.0.1. Permite a comunicação interprocessos (entre aplicações) situados na mesma máquina.

Vejamos alguns exemplos de endereçamento de máquinas situadas na mesma rede e em redes diferentes.



EXEMPLO 1

Observe na figura 4.7 que o endereço dos dois hosts (estações A e B) começam por 200, eles são, portanto, de classe C, onde os três primeiros octetos identificam a rede. Como ambos os hosts possuem o endereço começando por 200.18.171, elas estão na mesma rede.

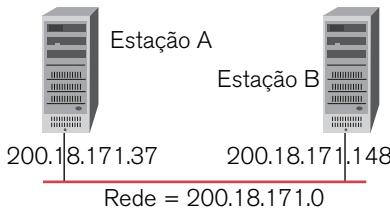


Figura 4.7 – Exemplo de endereçamento. Fonte: elaborado pelo autor.



EXEMPLO 2

Observe a figura 4.8.

Neste exemplo também observamos que tanto o endereço das estações A e B como o do roteador começam com 200 (classe C), o que significa que os 3 primeiros octetos identificam a rede.

Ao contrário do exemplo anterior, a estação A tem como endereço de rede 200.18.171 e a estação B 200.18.200, estando, portanto, em redes distintas. Para poder se comunicar, as duas necessitam que o pacote seja roteado. Para tal, deverão encaminhar o pacote para o roteador que fará a transferência do pacote de uma rede para outra.

Para que o esquema funcione, é necessário, conforme já vimos, que o roteador tenha uma interface em cada uma das redes. Observe na figura 4.11 que isto acontece, pois o roteador tem uma interface com endereço na rede da estação A (200.18.171.148) e outra com endereço na rede da estação B (200.18.180.10).

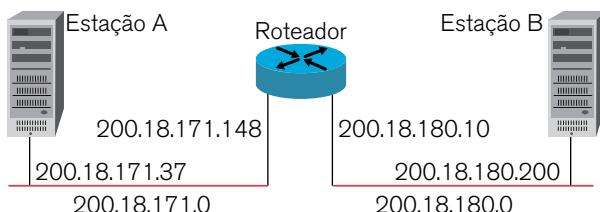


Figura 4.8 – Exemplo de endereçamento. Fonte: elaborado pelo autor.

Devemos observar que não existe necessidade de os endereços de redes adjacentes serem correlacionados. Uma rede classe A pode ser adjacente a uma classe C ou B e vice-versa. Cabe ao roteamento encontrar o caminho entre as diversas redes.

Podemos desta forma definir rede IP como um conjunto de computadores (*hosts*) com o mesmo ID de rede e se encontram em um mesmo **domínio de broadcast**.



CONCEITO

Domínio de broadcast é um segmento lógico de uma rede em que um computador ou qualquer outro dispositivo conectado à rede é capaz de se comunicar com outro sem necessidade de utilizar um dispositivo de roteamento.

Observe a figura 4.9.

Nesta figura, podem ser observados 2 domínios de *broadcast*, materializado pelo roteador com 2 *interfaces*. Cada *interface* de rede do roteador está em um domínio de *broadcast* diferente, logo 2 redes IP ou redes lógicas diferentes, 200.1.1.0 e 200.2.2.0.

O domínio de *broadcast* tecnicamente é a rede lógica e o equipamento de rede que separa os domínios de *broadcast* ou redes lógicas é o roteador e este trabalha na camada de redes (3 do modelo OSI ou 2 do TCP/IP). Resumindo: possui a função de encaminhar os pacotes ou datagramas IP.

Na figura 4.9, foram delimitadas a rede 1 à esquerda, com o prefixo de rede 200.1.1 (ID de rede) e a rede 2 à direita, com o pré-fixo de rede 200.2.2 (ID de rede).

A última observação quanto à figura é de que o endereço da porta do roteador é o *default gateway* da respectiva rede, ou seja, é quem interliga a rede local (LAN) a outras redes.

Rede 200.1.1.0 *default gateway* 200.1.1.254 e rede 200.2.2.0 *default gateway* 200.2.2.254. O endereço do roteador pode ser qualquer endereço válido na rede.

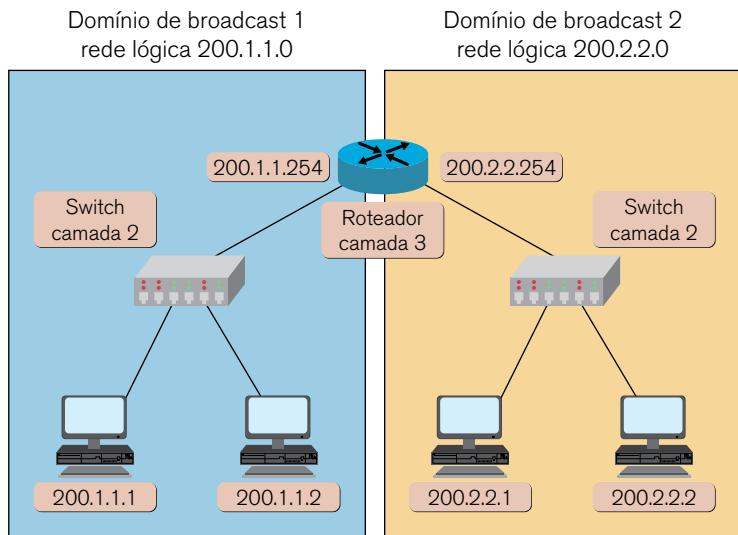


Figura 4.9 – Endereços de rede e broadcast. Fonte: Prof. Antônio Sérgio Alves Cavalcante (cedido ao autor).

4.5 Endereçamento sem classes (*classless*)

O endereçamento por classes (*classfull*), visto na seção anterior, não era eficiente na distribuição de endereços. Cada rede na *Internet*, tenha ela 5, 200, 2 000 ou 30 máquinas, deveria ser compatível com uma das classes de endereços. Desta forma, uma rede com 10 estações receberia um endereço do tipo classe C, com capacidade de endereçar 254 *hosts*, mais dois endereços, um para rede e outro de *broadcast*, totalizando 256 IP possíveis. Isto significa um desperdício de 244 endereços. Da mesma forma, uma rede com 2 000 hosts receberia uma rede do tipo classe B e, desta forma, causaria um desperdício de mais de 63 500 endereços.

Com o crescimento da *Internet*, o número de redes a serem interconectadas aumentou dramaticamente, causando o agravamento do problema de disponibilidade de endereços IP, especialmente o desperdício de endereços em classes C e B. Visando diminuir o desperdício, aumentando a quantidade de endereços

disponíveis sem afetar o funcionamento dos sistemas existentes, decidiu-se flexibilizar o conceito de classes - assim a divisão entre rede e host ocorre somente a cada 8 bits.

Para conseguir esta flexibilização, foi criada a **máscara de sub-rede**, que, além de dividir a rede em sub-redes, permitiu realizar o endereçamento sem classes, já que determina a porção rede (*network id*) e a porção host (*host id*) do endereço.

A máscara de sub-rede, da mesma forma que o endereço IP, é formada por 4 octetos com uma sequência contínua de 1's, seguida de uma sequência de 0's. A porção de *bits* em 1 identifica quais *bits* são utilizados para identificar a rede no endereço e a porção de *bits* em 0 identifica os *bits* do endereço que identificam a estação.

Obs.: a máscara pode ser compreendida também como um número inteiro que diz a quantidade de *bits* um utilizados. Por exemplo, uma máscara com valor 255.255.255.192 poderia ser representada como /26, o que significa que os 26 primeiros *bits*, contados da esquerda para a direita, estão ligados (valor 1) e os 6 últimos desligados (valor 0).

Este mecanismo está representado na figura 4.10.

	0	7	15	23	31
	Octeto 1	Octeto 2	Octeto 3	Octeto 4	
End.	11 00 10 00	00 01 00 10	10 10 00 00	10	XX XX XX
	200.	18.	160		128-191
Mask	11 11 11 11	11 11 11 11	11 11 11 11	11	00 00 00
	255.	255.	255.		192

Figura 4.10 – Máscara de sub-rede. Kurose 2009. Fonte: elaborado pelo autor.

No endereço da figura 4.12, 200.18.160.X, o *network id* possui 26 *bits* e o *host id* os 6 *bits* restantes. Desta forma, o endereço 200.18.160.0 da antiga classe C pode ser dividido em quatro redes com as identificações a seguir. Note que os 4 endereços de rede são independentes entre si. Elas podem ser empregadas em redes completamente separadas e até mesmo utilizadas em instituições distintas.

200.18.160.[00XXXXXX]
200.18.160.[01XXXXXX]
200.18.160.[10XXXXXX] e
200.18.160.[11XXXXXX]

Em termos de identificação da rede, utilizam-se os mesmos critérios anteriores, ou seja, todos os *bits* de identificação do *host* são 0. Quando os *bits* do *host* são todos 1, isto identifica um *broadcast* naquela rede específica. Desta forma, temos as seguintes identificações para endereço de rede:

200.18.160.0
200.18.160.64
200.18.160.128 e
200.18.160.192

Os endereços de *broadcast* nas redes são:

200.18.160.63
200.18.160.127
200.18.160.191 e
200.18.160.255

Os possíveis endereços de estação em cada rede são:

200.18.160.[1-62]
200.18.160.[65-126]
200.18.160.[129-190] e
200.18.160.[193-254]

Uma conclusão que se pode obter da análise da utilização de **sub-redes** é que a identificação de uma rede, composta de um endereço de rede e uma máscara (p.ex. 200.18.171.64 e máscara 255.255.255.192) é, na verdade, um espaço de endereçamento que pode ser usado da forma mais indicada.



CONCEITO

Sub-rede: é um subconjunto de uma rede.

Vejamos um exemplo passo a passo. Observe a figura 4.11

Nela, podemos observar duas redes distintas:

- 200.1.1.0 à esquerda
- 200.2.2.0 à direita

Esta mesma topologia poderia ser endereçada como uma única rede classe C?

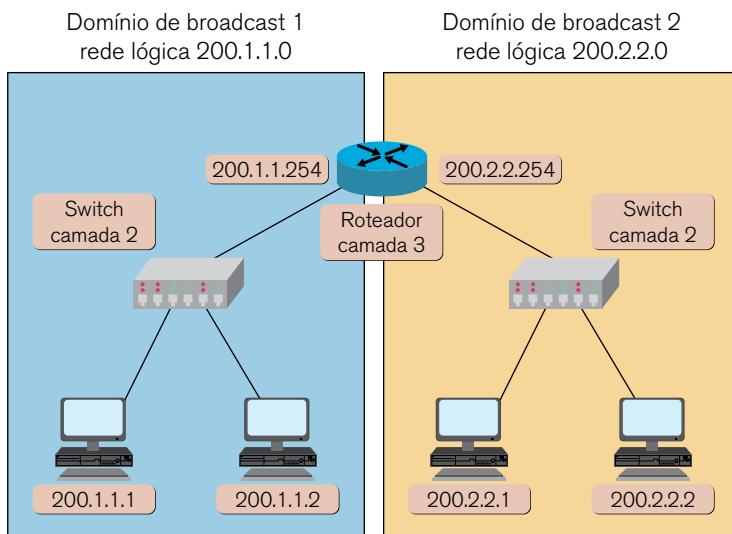


Figura 4.11 – Topologia de exemplo. Fonte: Prof. Antônio Sérgio Alves Cavalcante (cedido ao autor).

O endereço classe C possui 256 endereços possíveis, ou seja, 2^8 (28), que é a quantidade de *bits* disponíveis de endereços, de 0 a 255.

Matemática bem simplista, 256 endereços divididos em 2 subconjuntos = 128 endereços cada. Como o subconjunto de uma rede é uma sub-rede, o endereçamento da topologia ficaria da seguinte forma (figura 4.12):

- A rede 200.1.1.0 (à esquerda) será dividida em 2 subredes.
- Os endereços de 0 a 127 farão parte da 1^a subrede (esquerda).
- Os endereços de 128 a 255 farão parte da 2^a subrede (direita).

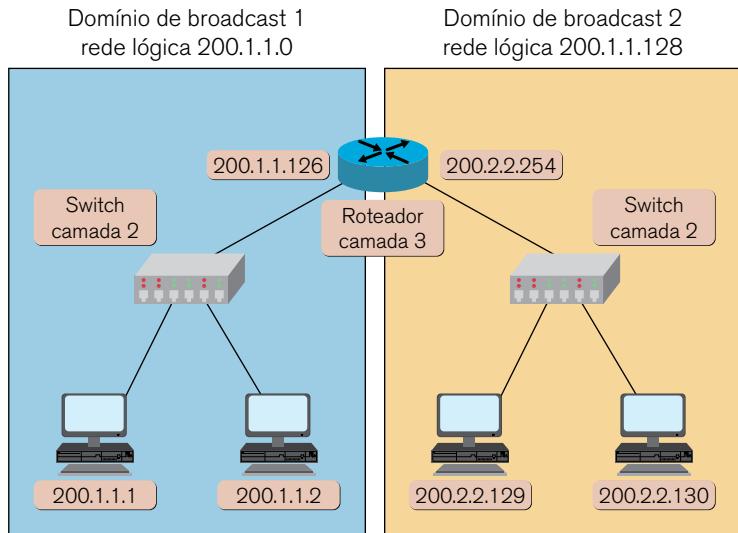


Figura 4.12 – Topologia após a divisão das sub-redes. Fonte: Prof. Antônio Sérgio Alves Cavalcante (cedido ao autor).

O problema que se apresenta então é: qual máscara de sub-rede deve ser utilizada para fazer esta divisão?

Observe a tabela 4.4 apresentando os dois conjuntos em que foi dividida a rede 200.1.1.0

Conjunto ou subrede de 0 a 127				
200	1	1	0	
11001000	00000001	00000001	00000000	End. da subrede 0
11111111	11111111	11111111	10000000	Máscara de subrede binário
255	255	255	128	Máscara de subrede decimal
200	1	1	127	
11001000	00000001	00000001	01111111	End. de BROADCAST da subrede 0
11111111	11111111	11111111	10000000	Máscara de subrede binário
255	255	255	128	Máscara de subrede decimal
Conjunto ou subrede de 128 a 255				
200	1	1	128	
11001000	00000001	00000001	10000000	End. da subrede 1
11111111	11111111	11111111	10000000	Máscara de subrede binário
255	255	255	128	Máscara de subrede decimal
200	1	1	255	
11001000	00000001	00000001	11111111	End. de BROADCAST da subrede
11111111	11111111	11111111	10000000	Máscara de subrede binário
255	255	255	128	Máscara de subrede decimal

Tabela 4.4 – Tabela com a divisão das sub-redes. Fonte: Prof. Antônio Sérgio Alves Cavalcante (cedido ao autor).



ATENÇÃO

Ao utilizar a divisão da rede em sub-rede, usaremos *bits* de host para representar a sub-rede, **nunca** *bits* do ID de **rede**. Se o ID de *rede* for alterado, o endereço deixará de pertencer à rede.

Para indicar a sub-rede, devemos observar a tabela da figura 4.16 e verificar que o *bit* de maior ordem de *host* foi ligado na máscara de sub-rede, dividindo em 2 sub-redes:

- **Sub-rede 0:** o último octeto varia de 0 a 127 e, para não ocorrerem valores superiores a 127, o *bit* mais significativo do *host* permaneceu zerado.
- **Sub-rede 1:** o último octeto varia de 128 a 255 e, para não ocorrerem valores inferiores a 128, o *bit* mais significativo do *host* permaneceu ligado.

Assim, esse *bit* de maior ordem dos *bits* de *host* pode representar uma das sub-redes quando seu valor for 0 e outra quando seu valor for 1.

Pensada a solução, a implementação ficou por conta da máscara de sub-rede, que tem o objetivo de deixar zerados os *bits* de *host* para assim extrair o endereço de rede e ou de sub-rede.

Resumindo, mascarar qualquer valor que esteja no *host* deixando todos os *bits* de *host* zerados, o que equivale ao endereço de rede.

Para entender como funciona, devemos primeiro ver como a operação é realizada em binário.

A operação entre o endereço IP e a máscara de sub-rede é realizada operando *bit a bit* a operação lógica *And*, em que o *bit* 0 equivale a falso e o *bit* a verdadeiro (tabela 4.5).

TABELA VERDADE					TABELA VERDADE $V = 1 \quad E \quad F = 0$				
V	and	V	=	V	1	and	1	=	1
V	and	F	=	F	1	and	0	=	0
F	and	V	=	F	0	and	1	=	0
F	and	F	=	F	0	and	0	=	0

Tabela 4.5 – Tabela verdade do And. Fonte: Prof. Antônio Sérgio Alves Cavalcante (cedido ao autor).

Desta forma, ao fazer a operação entre o endereço IP da rede 200.1.1.0 com a máscara, obteremos a máscara /25 (tabela 4.6).

Como descobrimos isso?

Note que, com o primeiro *bit* do último octeto selado como um, todos os valores do último octeto do endereço entre 0 (00000000) e 127 (01111111) resolveram a rede como 0, pois somente quando o primeiro *bit* do octeto for um decimal entre 128 (10000000) e 255(11111111) o endereço de rede será mudado e terá como resultado 128

Subrede 0 host 1 00000001 = 1 decimal				
200	1	1		1
11001000	00000001	00000001	0	0000001
11111111	11111111	11111111	1	0000000
11001000	00000001	00000001	0	0000000
200	1	1		0
Subrede 1 host 1 10000001 = 129 decimal				
200	1	1		129
11001000	00000001	00000001	1	0000001
11111111	11111111	11111111	1	0000000
11001000	00000001	00000001	1	0000000
200	1	1		128

Tabela 4.6 – Operação do prefixo de rede com a máscara. Fonte: Prof. Antônio Sérgio Alves Cavalcante (cedido ao autor).

Para transformar a máscara de binário em decimal, basta dividí-la em octetos e calcular seu valor em decimal (figura 4.13), dando 255.255.255.128 ou /25. Repare que em binários são 25 *bits* um a partir da esquerda.

111111111111111111111111110000000
 11111111 . 11111111 . 11111111 . 10000000
 255 . 255 . 255 . 128

Figura 4.13 – Máscara em decimal. Fonte: Prof. Antônio Sérgio Alves Cavalcante (cedido ao autor)

Para consolidar o conhecimento, vamos a mais um exemplo.

Considere novamente a topologia da figura 4.14. Vamos agora dividir a rede 200.2.2.0 em 4 sub-redes.

Quanto ao endereço 200.2.2.0, pode-se afirmar que se trata de um endereço da classe C.

- Sua composição normal é de 24 *bits* de rede e 8 *bits* de *host* (o ID de rede não pode ser modificado).
- Essa rede é um classe C e os 8 *bits* finais são de *host*. Se não tivesse sido dividida em sub-redes, a máscara-padrão do endereço dessa classe seria: 255. 255. 255. 0

Vamos a um passo a passo para dividir a rede:

1. Saber quantos bits nos pertence? Os 8 bits de host.
2. Quantos bits eu necessito para ter 4 variações? $2^1 = 2$, $2^2 = 4$ (o expoente é o número de bits necessário para a quantidade de variações). Exemplos:
 - 2.1.** Se fôssemos dividir em 10 subredes? $2^1 = 2$, $2^2 = 4$, $2^3 = 8$, $2^4 = 16$ (para endereçar 10 sub-redes, serão necessários no mínimo 4 bits).
 - 2.2.** Se fôssemos dividir em 32 sub-redes? $2^5 = 32$
3. Qual seria a nova máscara de sub-rede? A figura 4.19 mostra o resultado

11111111	.	11111111	.	11111111	.	11000000
255	.	255	.	255	.	192

Figura 4.14 – Máscara para divisão em quatro sub-redes. Fonte: Prof. Antônio Sérgio Alves Cavalcante (cedido ao autor)

4. Quais as sub-redes possíveis (00, 01, 10 e 11)? O raciocínio é realizado nos 2 *bits* transformados de *host* que foram ligados para representar as 4 sub-redes (tabela 4.7).

Subrede 00 00000000 0 decimal				
200	2	2		0
11001000 11111111	00000010 11111111	00000010 11111111	00 11	000000 000000
255	255	255		192

Subrede 10 10000000 128 decimal

200	2	2		128
11001000 11111111	00000010 11111111	00000010 11111111	10 11	000000 000000
255	255	255		192

Subrede 01 01000000 64 decimal

200	2	2		64
11001000 11111111	00000010 11111111	00000010 11111111	01 11	000000 000000
255	255	255		192

Subrede 11 11000000 192 decimal

200	2	2		192
11001000 11111111	00000010 11111111	00000010 11111111	11 11	000000 000000
255	255	255		192

Tabela 4.7 – Divisão das sub-redes. Fonte: Prof. Antônio Sérgio Alves Cavalcante (cedido ao autor).

A figura 4.15 mostra uma possível topologia obtida com esta divisão

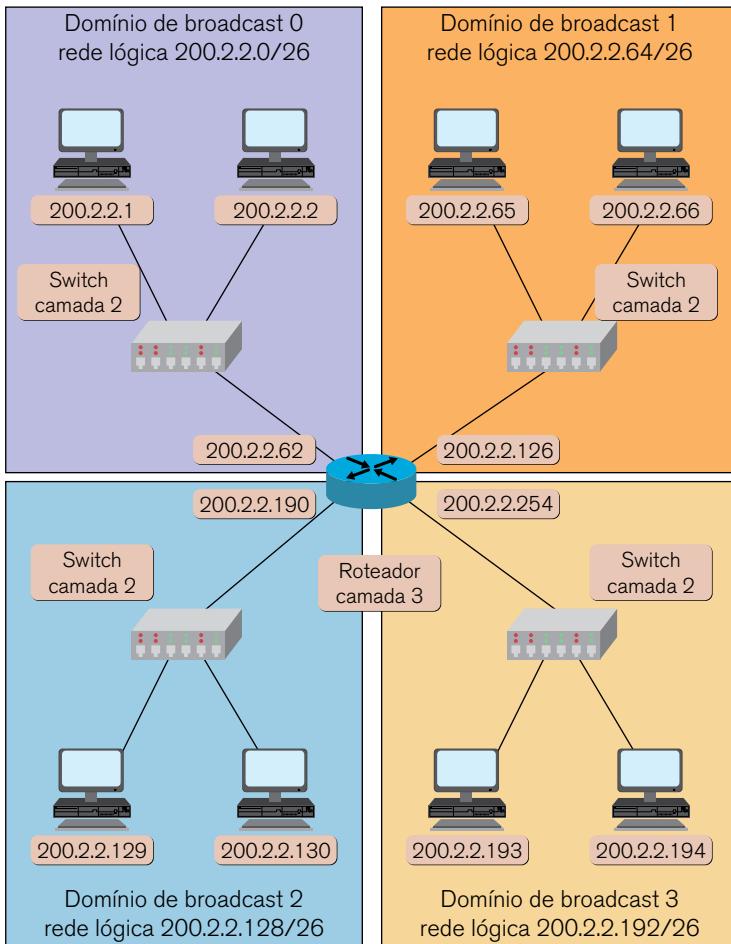


Figura 4.15 – Topologia com a divisão em 4 sub-redes. Fonte: Prof. Antônio Sergio Alves Cavalcante (cedido ao autor).

Em resumo: não importa o valor em decimal do octeto, desde que ele represente o binário que se quer informar ao computador (*host*). 4º octeto:

- 00000000 sub-rede zero (00) *host* zero - o 4º octeto em decimal 0
- 01000000 sub-rede um (01) *host* zero - o 4º octeto em decimal 64
- 10000000 sub-rede dois (10) *host* zero - o 4º octeto em decimal 128
- 11000000 sub-rede três (11) *host* zero - o 4º octeto em decimal 192

(Para ser o endereço da rede, todos os *bits* de *host* tem que estar zerados: 0000000.)

A identificação do endereço de *broadcast* da sub-rede é semelhante ao de rede, quando todos os *bits* de *hosts* estiverem ligados “1” (tabela 4.8).

SUBREDE	BROADCAST SUBREDE
200.2.2.0	00000000
200.2.2.64	01000000
200.2.2.128	10000000
200.2.2.192	11000000

Tabela 4.8 – Definição dos endereços de broadcast. Fonte: Prof. Antônio Sergio Alves Cavalcante (cedido ao autor).

Finalmente, os endereços que podemos utilizar para *host* vão do primeiro após o endereço de rede até o último antes do *broadcast*. Por exemplo, no caso da rede 200.2.2.192 da figura 4.22 com *broadcast* 200.2.2.255, os IP de *hosts* vão de 200.2.2.193 até 200.2.2.254 em um total de 62 endereços de *host*, o que em outras palavras significa que a rede poderá ter até 62 máquinas.

4.6 Roteamento IP

O destino de um pacote enviado por uma máquina pode ser o próprio *host*, um *host* na mesma rede ou um *host* em uma rede diferente. No primeiro caso, o pacote é enviado ao nível IP que o retorna para os níveis superiores. No segundo caso, é realizado o mapeamento por meio de ARP e o pacote é encaminhado para a rede local. Já no terceiro caso, o pacote deve ser enviado ao *default gateway* da rede para ser roteado para a rede de destino.

Para encaminhar o pacote ao roteador, o *host* de origem endereça, em nível de camada de rede, o pacote com o IP da máquina de destino que se encontra na outra rede e, em nível de enlace, coloca no quadro como MAC de destino o endereço físico da interface do roteador que está em sua rede.

Ao receber o quadro com o seu MAC no destino, o roteador realiza as seguintes operações:

- Desencapsula-o.
- Acessa o endereçamento em nível de rede e identifica o IP de destino.
- Determina a rede a que ele pertence.
- Consulta sua tabela de rotas para encontrar um caminho para o destino.
- Encapsula novamente o datagrama IP em um quadro.
- Encaminha o quadro para o próximo roteador na rota.

Este processo se repete em cada roteador ao longo do caminho até que o pacote chegue ao destino final. Este tipo de roteamento é chamado de *next-hop routing*, já que um pacote é sempre enviado para o próximo roteador no caminho.

Neste tipo de roteamento, não há necessidade de que um roteador conheça a rota completa até o destino. Cada roteador deve conhecer apenas o próximo roteador para o qual deverá enviar a mensagem. Observe a figura 4.16.

Quando uma estação, como a A, deseja enviar uma mensagem IP para outra rede, como a estação B, ela deverá realizar os seguintes passos:

1. Determinar que a/o *host* de destino esteja em outra rede e, por isto, a mensagem deverá ser enviada para um roteador.
2. Determinar, por meio da tabela de rotas da máquina origem, qual roteador é o correto para se enviar a mensagem.
3. Descobrir, por meio do protocolo ARP, o endereço MAC do roteador.
4. Enviar o quadro tendo como MAC de destino o endereço físico do roteador com o endereço de destino no pacote IP da estação.
5. O roteador, ao receber o quadro com o seu endereço MAC, mas com um endereço de rede (IP) que não é o seu, irá rotear o pacote. Para isso, ele observa o endereço IP de destino e verifica para qual rede ele está endereçado.
6. No caso da figura, como o roteador atende às duas redes (origem e destino), ele descobrirá o endereço MAC da estação de destino (via ARP).
7. Finalmente, encapsula-se o pacote em quadro com o endereço MAC da Estação B (0D.0A.12.07.71.FF) e transmite-o na rede.

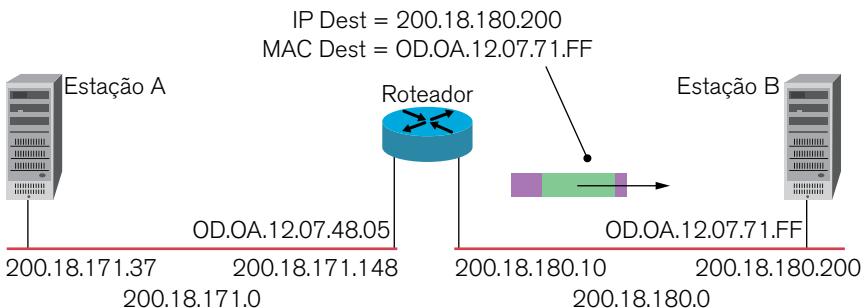


Figura 4.16 – Exemplo de roteamento. Tannenbaum 2007. Adaptado.

Vejamos agora mais um exemplo utilizando vários roteadores.

A figura 4.17 mostra a topologia.

Quando o *host* 200.1.1.1 deseja enviar uma informação dentro de um datagrama IP para o *host* de destino 200.2.2.1, ocorre o seguinte passo a passo:

1. O *host* 200.1.1.1 pertence à rede 200.1.1.0 e necessita se comunicar com o *host* 200.2.2.1, pertencente à outra rede (200.2.2.0).
2. Como o destinatário não se encontra na mesma rede, necessita encaminhar o datagrama IP(pacote IP) ao equipamento que o interliga a outras redes, nesse caso o roteador A, conhecido como *default gateway* ou roteador *default etc*. O *default gateway* da 200.1.1.0/24 é o roteador A. Os endereços IP do datagrama são mantidos, tanto a origem host 200.1.1.1, quanto o destino *host* 200.2.2.1.
3. O roteador A, ao receber o datagrama IP através da *interface* de entrada, vai analisar sua tabela de rotas, tomar uma decisão de roteamento e encaminhar para o roteador B, realizando sua tarefa que é o roteamento de datagramas IP ou pacotes IP. O datagrama IP será encaminhado para o próximo salto ou próximo roteador até que chegue a seu destino (200.2.2.1).
4. O roteador B, da mesma forma, irá analisar sua tabela de rotas e encaminhar o datagrama IP para o roteador D.
5. O roteador D, por sua vez, vai analisar sua tabela de rotas e encaminhar o datagrama IP para o roteador E.
6. O roteador E também vai analisar sua tabela de rotas e encaminhar o datagrama IP para o roteador F.
7. O roteador F verifica que uma de suas *interfaces* se encontra na rede 200.2.2.0/24 e entrega o datagrama ao 200.2.2.1.

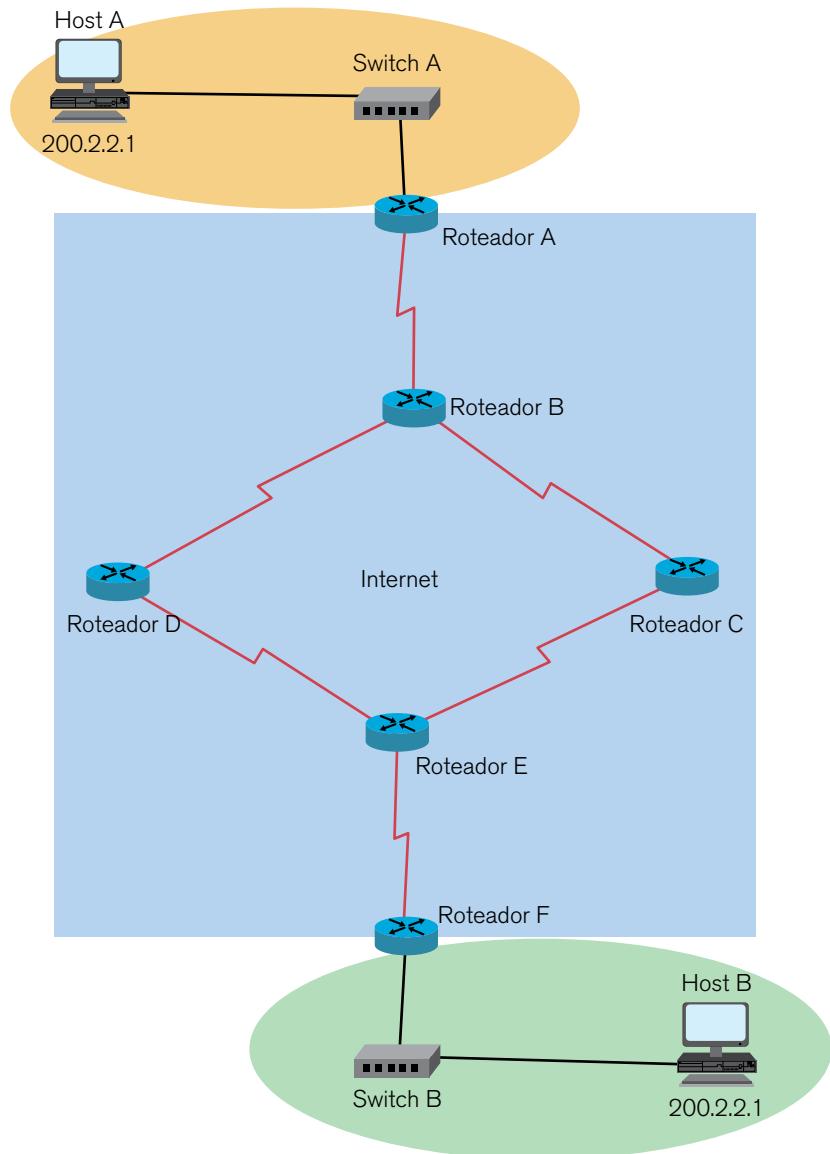


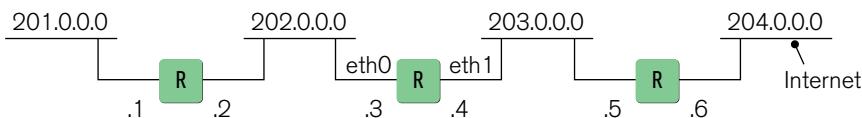
Figura 4.17 – Exemplo de roteamento. Fonte: Prof. Antônio Sérgio Alves Cavalcante (cedido ao autor).

Para deixar bem claro, a decisão de roteamento realizado por um roteador ocorre quando o datagrama IP entra por uma *interface* do roteador. Com base no **endereço IP de destino**, define a *interface* de saída que o datagrama IP deverá seguir para alcançar seu destino. Esse ato de entrar por uma *interface*, tomar

a decisão de roteamento e sair por outra *interface* também pode ser dito repasse entre as *interfaces* de entrada e saída.

A figura 4.18 a seguir ilustra uma estrutura de redes e a tabela de rotas dos roteadores. As tabelas de rotas de cada roteador são diferentes uma da outra. Note nestas tabelas a existência de rotas diretas, que são informações redundantes para identificar a capacidade de acessar a própria rede à qual os roteadores estão conectados. Este tipo de rota, apesar de parecer redundante, é útil para mostrar de forma semelhante as rotas diretas para as redes conectadas diretamente no roteador.

Outra informação relevante é a existência de uma rota *default*. Esta rota é utilizada durante a decisão de roteamento no caso de não existir uma rota específica para a rede destino da mensagem IP. A rota *default* pode ser considerada como um resumo de diversas rotas encaminhadas pelo mesmo próximo roteador. Sem a utilização da rota *default*, a tabela de rotas deveria possuir uma linha para cada rede que pudesse ser endereçada. Em uma rede como a *Internet*, isto seria completamente impossível.



REDE DESTINO	ROTEADOR (GATEWAY)	HOPS
201.0.0.0	eth0 (rota direta)	0
202.0.0.0	eth1 (rota direta)	0
203.0.0.0	202.0.0.3	1
204.0.0.0	203.0.0.3	2
default	203.0.0.3	-

Roteador da esquerda.

REDE DESTINO	ROTEADOR (GATEWAY)	HOPS
202.0.0.0	eth0 (rota direta)	0
203.0.0.0	eth1 (rota direta)	0
201.0.0.0	202.0.0.2	1
204.0.0.0	203.0.0.5	1
default	203.0.0.5	-

Rotedor da central.

REDE DESTINO	ROTEADOR (GATEWAY)	HOPS
203.0.0.0	eth0 (rota direta)	0
204.0.0.0	eth1 (rota direta)	0
202.0.0.0	203.0.0.4	1
201.0.0.0	203.0.0.4	1

REDE DESTINO	ROTEADOR (GATEWAY)	HOPS
default	204.0.0.7**	--

Roteador da direita.

A rota default geralmente é representada nos sistemas operacionais como a rede 0.0.0.0

** não mostrado na figura

Figura 4.18 – Exemplo de roteamento. Tannenbaum 2007. Adaptado.

A alimentação das informações na tabela de rotas pode ser de modo estático ou dinâmico ou ambos simultaneamente. Na alimentação estática, as rotas são preenchidas manualmente, geralmente pela configuração inicial da máquina. Na alimentação dinâmica, protocolos como RIP, RIP2, OSPF ou BGP são responsáveis pela aquisição de informações sobre a topologia da rede e a publicação de rotas na tabela de rotas dos roteadores envolvidos.



CONEXÃO

Acesse o *link* < http://pt.wikipedia.org/wiki/Rede_de_computadores> e aprenda mais a respeito de redes de computadores.



ATIVIDADES

Acesse os *sites*:

Calculadoras de IP *on-line*

Disponível em: <<http://meuip.net.br/calculadora-ip.asp>>.

Disponível em: <<http://www.joao.pro.br/aplicativos/netcalc.htm>>.

Disponível em: <<http://www.subnet-calculator.com/>>.

Responda às questões *on-line* de endereço IP.

Disponível em: <<https://www.aprovaconcursos.com.br/questoes-de-concurso/disciplina/redes-de-computadores>>.

Disponível em: <<http://www.mapadaprova.com.br/questoes/de/tecnologia-da-informacao/redes-de-computadores/enderecamento-e-protocolos-tcp-ip>>.

Disponível em: <<https://www.gabaritou.com.br/Questao?AreaConhecimentoID=8&DisciplinalID=11&AssuntoID=935>>.



REFLEXÃO

Você viu nesta aula os principais elementos da camada de acesso à rede e como eles funcionam.



LEITURA

Leia os capítulos 7, 11 e 12 do livro **Comunicação de dados e redes de computadores**, de Behrouz A. Forouzan.

Saiba mais

Assista aos seguintes vídeos:

Disponível em: <<https://www.youtube.com/watch?v=XPWd08tLAuo>>.

Disponível em: <<https://www.youtube.com/watch?v=0v0OwZm1-lk>>.

Disponível em: <<https://www.youtube.com/watch?v=IANothAhsCY>>.

Disponível em: <<https://www.youtube.com/watch?v=EG9mSXIMTU4>>

Disponível em: <<https://www.youtube.com/watch?v=7-6-7VREEeg>>.

Disponível em: <<https://www.youtube.com/watch?v=HNQD0qJ0TC4>>.



REFERÊNCIAS BIBLIOGRÁFICAS

FOROUZAN, Behrouz A. **Comunicação de dados e redes de computadores.** 4. ed. São Paulo: McGraw-Hill, 2008.

KUROSE, James F. e ROSS, Keith W. **Redes de computadores e a Internet:** uma abordagem top-down. 4. ed. São Paulo: Addison Wesley, 2009.

Tanenbaum, Andrew S. **Redes de computadores.** 5. ed. Rio de Janeiro: Campus, 2007.

5

Camadas de Transporte e de Aplicação da Internet

Quando enviamos um pacote de uma máquina para outra, desejamos ter certeza de que ele chegou a seu destino, de forma íntegra e sem erros.

Este tipo de controle é responsabilidade da camada de transporte da Arquitetura TCP/IP, que iremos estudar neste capítulo.

O pacote enviado, via de regra, é resultado da utilização de algum aplicativo como browsers para acessar páginas Web, programas de e-mail, para envio e recebimento de correspondência eletrônica etc.

Estes programas funcionam baseados em protocolos da camada de aplicação, que também iremos estudar neste capítulo.



OBJETIVOS

- Conhecer os protocolos TCP e UDP.
 - Conhecer os principais protocolos da camada de aplicação.
-

5.1 Camada de Transporte

Esta camada reúne os protocolos que realizam as funções de transporte de dados fim a fim, ou seja, considera apenas a origem e o destino da comunicação, sem se preocupar com os elementos intermediários.

Na arquitetura TCP/IP, a camada de transporte possui dois protocolos: o UDP (*user datagram protocol*) e TCP (*transmission control protocol*).

O protocolo UDP realiza apenas a multiplexação para que várias aplicações possam acessar o sistema de comunicação de forma coerente.

O protocolo TCP realiza, além da multiplexação, uma série de funções para tornar a comunicação entre origem e destino mais confiável. São responsabilidades do protocolo TCP o controle de fluxo, o controle de erro, a sequenciação e a multiplexação de mensagens.

A camada de transporte oferece para o nível de aplicação um conjunto de funções e procedimentos para acesso ao sistema de comunicação, de modo a permitir a criação e a utilização de aplicações de forma independente da implementação. Desta forma, as interfaces *socket* (ambiente *Unix*) e *Winsock* (ambiente *Windows*) fornecem um conjunto de funções-padrão para permitir que as aplicações possam ser desenvolvidas independentemente do sistema operacional no qual serão rodadas.

5.1.1 Protocolo UDP

O protocolo UDP fornece uma forma simples de acesso ao sistema de comunicação, provendo um serviço sem conexão, sem confiabilidade e sem correção de erros. A principal função do nível de transporte implementada em UDP é a capacidade de multiplexação de acesso ao sistema de comunicação. Esta função permite que vários processos ou programas que estão sendo executados em um computador possam acessar o sistema de comunicação e o tráfego de dados respectivo a cada um deles e sejam corretamente identificados, separados por meio de *buffers* individuais.

Processo é o programa que implementa uma aplicação do sistema operacional, que pode ser uma aplicação do nível de aplicação TCP/IP.

A forma de identificação de um ponto de acesso de serviço (SAP) do modelo OSI é a porta de protocolo em TCP/IP. A porta é a unidade que permite identificar o tráfego de dados destinado a diversas aplicações. A identificação única

de um processo acessando os serviços TCP/IP é, então, o endereço IP da máquina e a porta ou portas usadas pela aplicação. Cada processo pode utilizar mais de uma porta simultaneamente, mas uma porta só pode ser utilizada por uma aplicação em um dado momento. Uma aplicação que deseja utilizar os serviços de comunicação deverá requisitar uma ou mais portas para realizar a comunicação. A mesma porta usada por uma aplicação pode ser usada por outra, desde que a primeira tenha terminado de utilizá-la.

5.1.2 Portas

Tanto o TCP quanto o UDP usam números de porta (ou soquete) para passar as informações às camadas superiores. Os números de portas são usados para manter o registro de diferentes conversações que cruzam a rede ao mesmo tempo. Os desenvolvedores de aplicações de *software* concordaram em usar os números de portas bem conhecidos que estão definidos no RFC1700. Toda conversação destinada à aplicação HTTP usa o número de porta-padrão 80. Conversações que não envolvem aplicações com números de portas bem conhecidos recebem números de porta que foram selecionados aleatoriamente em um conjunto específico. Esses números de portas são usados como endereços de origem e destino no segmento TCP.

Algumas portas são reservadas no TCP e no UDP, embora possa não haver aplicações para suportá-las. Os números de portas têm os seguintes conjuntos atribuídos:

- Portas conhecidas (números 0 a 1023): esses números estão reservados para serviços e aplicações. Eles são comumente usados para aplicações como o HTTP (servidor *Web*), SMTP (envio de *e-mails*) e DNS (resolução de nomes de domínio). Por meio da definição destas portas conhecidas para aplicações de servidor, aplicações de clientes podem ser programadas para solicitar uma conexão com essa porta específica e seu serviço associado.
- Portas registradas (números 1024 a 49151): Esses números de portas são designados para processos ou aplicações de usuário. Estes processos são principalmente aplicações individuais que um usuário escolheu para instalar em vez de aplicações comuns que receberiam uma porta conhecida. Quando não

usadas para um recurso de servidor, estas portas podem também ser dinamicamente selecionadas por um cliente como sua porta de origem.

- Portas dinâmicas ou privadas (números 49152 a 65535): elas são geralmente designadas de forma dinâmica a aplicações de clientes quando se inicia uma conexão. Não é muito comum um cliente se conectar a um serviço usando uma porta dinâmica ou privada (embora alguns programas de compartilhamento de arquivos *peer-to-peer* desempenhem essa função). Os sistemas finais usam números de portas para selecionar as aplicações corretas. Os números de portas de origem são atribuídos dinamicamente pelo host de origem e normalmente são maiores do que 1023.

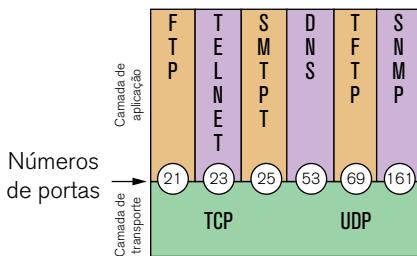


Figura 5.1 – Portas Tannenbaum 2007. Adaptado pelo autor.

A forma de utilização de portas mostra uma distinção entre a parte cliente e a parte servidora de uma aplicação TCP/IP. O programa cliente pode utilizar um número de porta qualquer, já que nenhum programa na rede terá necessidade de enviar uma mensagem para ele. Já uma aplicação servidora deve utilizar um número de porta bem conhecido (*Well-known ports*), de modo que um cliente qualquer, querendo utilizar os serviços do servidor, tenha de saber apenas o endereço IP da máquina onde este está sendo executado.

Se não houvesse a utilização de um número de porta bem conhecido, a arquitetura TCP/IP deveria possuir um mecanismo de diretório para que um cliente pudesse descobrir o número da porta associado ao servidor. Para evitar este passo intermediário, utilizam-se números de porta bem conhecidos e o cliente já possui pré-programado em seu código o número de porta que irá usar.

A figura 5.2 ilustra a multiplexação/demultiplexação realizada pelo protocolo UDP, camada de transporte:

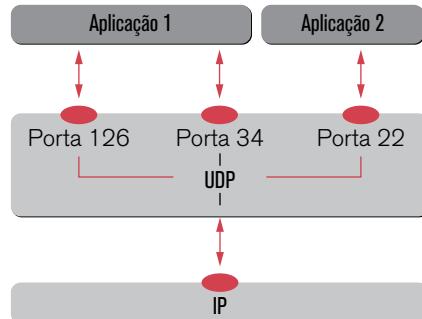


Figura 5.2 – Endereçamento de porta. Tannenbaum 2007. Adaptado pelo autor.

5.1.3 Protocolo TCP

O protocolo TCP trabalha no mesmo nível que o protocolo UDP, mas oferece serviços mais complexos, que incluem controle de erros e fluxo, serviço com conexão e envio de fluxo de dados.

O protocolo TCP oferece as seguintes características:

- controle de fluxo e erro fim a fim
- serviço confiável de transferência de dados
- comunicação *full-duplex* fim a fim
- fluxo de bytes enviado para a aplicação
- ordenação de mensagens
- opção de envio urgente de dados

As aplicações mais comuns que usam TCP são: Telnet, FTP, SMTP, HTTP.

O TCP utiliza o mesmo conceito de porta de UDP. Para TCP, uma conexão é formada pelo par (End. IP. origem, porta origem) e (End. IP destino, porta destino).

A conexão TCP é ilustrada na figura 5.3.

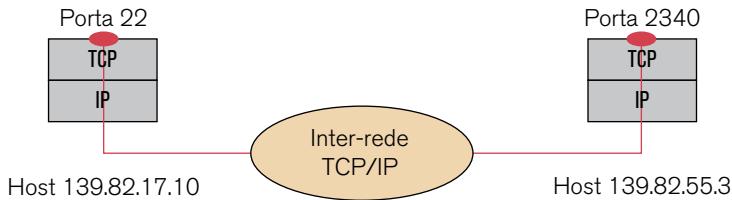


Figura 5.3 – Conexão TCP. Tannenbaum 2007. Adaptado pelo autor.

Uma conexão TCP é formada por três fases: estabelecimento de conexão, troca de dados e finalização da conexão, conforme ilustrado na figura 5.4 a seguir:

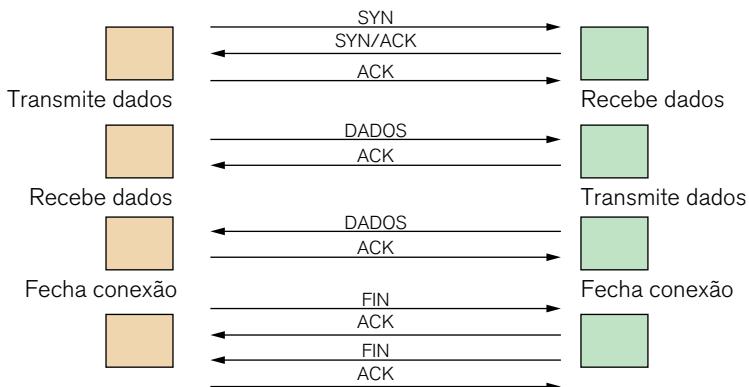


Figura 5.4 – Conexão TCP. Tannenbaum 2007. Adaptado pelo autor.

Vejamos um exemplo:

Observe a figura 5.5. Quando a estação de trabalho A solicita uma sessão de emulação de terminal Telnet com o *host Z*, ela envia um segmento de inicio de estabelecimento de sessão SYN com os campos *source port* e *destination port* preenchidos da seguinte forma:

- **Destination port:** identifica o processo servidor e para Telnet o valor é 23.

- **Source port:** contém um endereço gerado randomicamente que identifica o processo cliente, no caso 1028.

O host Z, ao receber este segmento, irá verificar se a aplicação está ativa antes de dar o aceite do pedido de estabelecimento de sessão por meio do segmento SYN-ACK.

Cada segmento TCP enviado tem um número de sequência para que o módulo TCP no host destino possa reordená-los na chegada.

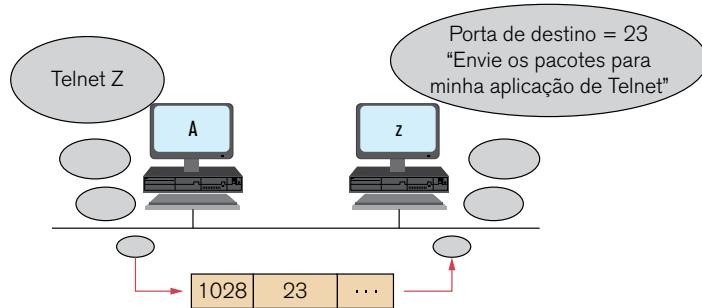


Figura 5.5 – Funcionamento TCP. Tannenbaum 2007. Adaptado pelo autor.

Observe agora a figura 5.6. Quando o nó destino recebe um segmento, envia uma confirmação por meio de um segmento TCP com o campo *acknowledgement* preenchido. Neste campo, está o número de sequência do próximo segmento esperado, indicando para o nó origem o correto recebimento dos pacotes anteriores pelo nó destino.

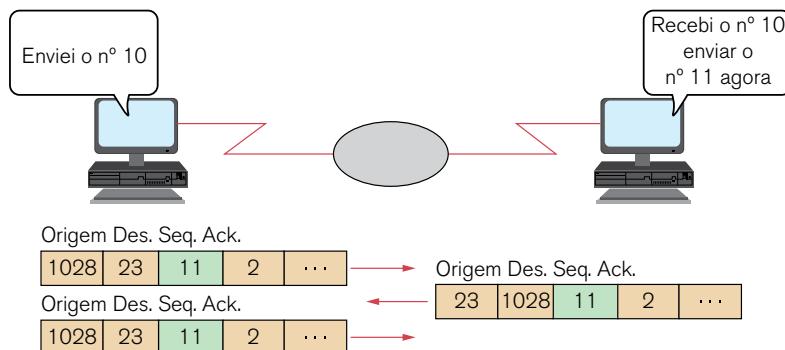


Figura 5.6 – Funcionamento TCP. Tannenbaum 2007. Adaptado pelo autor.

O sequenciamento dos pacotes TCP é orientado a *byte*. O número de sequência do segmento é sempre igual ao número de sequência do segmento anteriormente transmitido, somado ao número de *bytes* transmitidos. O primeiro número de sequência é gerado randomicamente e é determinado no estabelecimento da conexão TCP.

A confirmação de entrega dos segmentos TCP é também orientada a *byte*. O valor do campo *acknowledgement* de um segmento é sempre igual ao número de sequência do segmento que está sendo confirmado somado ao número de *bytes* recebidos (gráfico à esquerda).

Este valor indica para o nó origem o número de sequência do próximo segmento que o nó destino espera receber (figura 5.7).

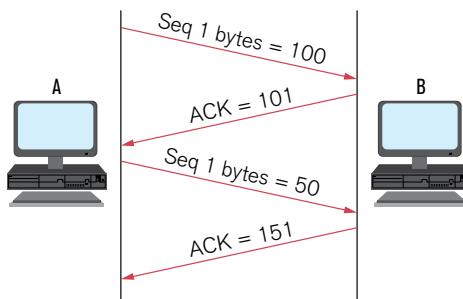


Figura 5.7 – Funcionamento TCP. Tannenbaum 2007. Adaptado pelo autor.

Após o envio dos dados, a sessão TCP pode ser encerrada elegantemente por qualquer uma das partes (cliente ou servidor) com um segmento FIN. Este segmento não possui dados, sendo reconhecido por ter o bit FIN do campo *flag* do cabeçalho TCP "ligado" (figura 5.8).

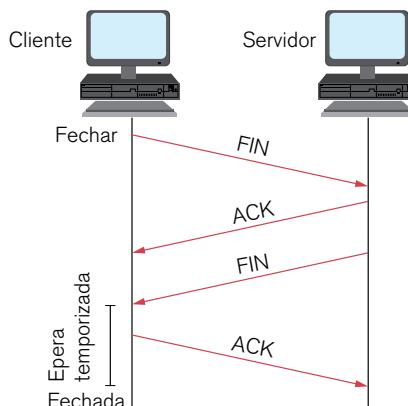


Figura 5.8 – Funcionamento TCP – Fechamento de Conexão. Tannenbaum 2007. Adaptado pelo autor.

O controle de fluxo do TCP é implementado por um mecanismo de janela. A janela define quantos *bytes* podem ser enviados sem necessidade do recebimento de uma confirmação. Esta janela está relacionada ao tamanho do *buffer* de recepção do destinatário e seu valor inicial é informado no estabelecimento da sessão TCP.

Resumo das características dos protocolos de transporte

TCP

- Fornece um circuito virtual entre aplicações do usuário final.
- É orientado para conexão.
- É confiável.
- Divide as mensagens enviadas em segmentos.
- Reagrupa as mensagens na estação de destino.
- Reenvia tudo que não foi recebido.
- Reagrupa as mensagens nos segmentos recebidos.

UDP

- Transporta dados sem confiabilidade entre *hosts*.
- Não apresenta conexão.
- Transmite mensagens (chamado de datagramas do usuário).
- Não fornece verificação de *software* para a entrega da mensagem (não é confiável).
 - Não reagrupa as mensagens de entrada.
 - Não usa confirmações.
 - Não fornece controle de fluxo.

5.2 Camada de aplicação

A camada de aplicação é a camada mais próxima do sistema final e determina se existem recursos suficientes para a comunicação entre os sistemas. Sem a camada de aplicação, não haveria nenhum suporte à comunicação de rede. A camada de aplicação não fornece serviços a nenhuma outra camada, no entanto ela fornece serviços aos processos de aplicação de usuários como programas

de planilhas, programas de processamento de textos e programas de terminais bancários.

Em um ambiente LAN, o suporte de rede de aplicações indiretas é uma função cliente-servidor. Se um cliente quiser salvar um arquivo de processador de texto em um servidor da rede, o redirecionador permitirá que a aplicação processadora de texto se torne um cliente da rede.

Redirecionador

O redirecionador é um protocolo que trabalha com sistemas operacionais de computadores e clientes de rede ao invés de programas de aplicações específicos.

O processo do redirecionador é o seguinte:

1. O cliente solicita que o servidor de arquivo da rede permita que o arquivo de dados seja armazenado.
2. O servidor responde salvando o arquivo no seu disco ou rejeitando a solicitação do cliente.

O redirecionador permite que um administrador de rede atribua recursos remotos a nomes lógicos no cliente local. Quando você selecionar um desses nomes lógicos para realizar uma operação, como salvar ou imprimir um arquivo, o redirecionador da rede enviará o arquivo selecionado ao recurso remoto apropriado na rede para processamento. Se o recurso estiver em um computador local, o redirecionador ignorará a solicitação e permitirá que o sistema operacional local processe a solicitação.

A vantagem de usar um redirecionador de rede em um cliente local é que as aplicações no cliente nunca precisam reconhecer a rede. Além disso, a aplicação que solicita serviço está localizada no computador local e o redirecionador roteia novamente a solicitação para o recurso de rede apropriado, enquanto a aplicação trata-a como uma solicitação local.

Exemplo: um redirecionador (solicitante) permite que um computador local, por meio de mapeamentos de unidades lógicas, use dispositivos de armazenamento da rede como se estivessem conectados localmente ao computador cliente. Estas unidades lógicas são representadas da mesma forma que as unidades físicas do cliente.

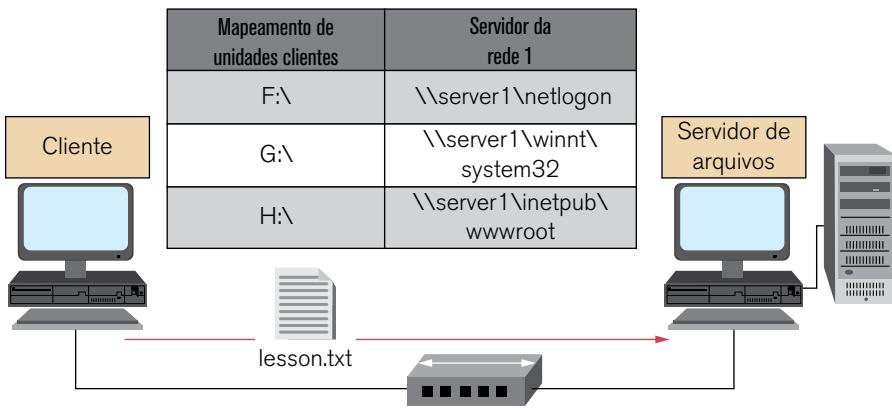


Figura 5.9 – Redirecionamento de gravação de arquivo. Tannenbaum 2007. Adaptado pelo autor.

Protocolos de nível de aplicação TCP/IP

Os protocolos de aplicação TCP/IP são aqueles que realizam as funções de alto nível e que utilizam os serviços da camada de transporte UDP ou TCP para a comunicação.

Os protocolos de aplicação podem realizar funções diretamente acessíveis pelo usuário como FTP, HTTP, SMTP, POP3, IMAP, Telnet e outros. Além disto, podem também realizar funções mais próximas do sistema de comunicação, tais como os protocolos DNS, DHCP e outros.

As aplicações estão ilustradas na figura 5.10:

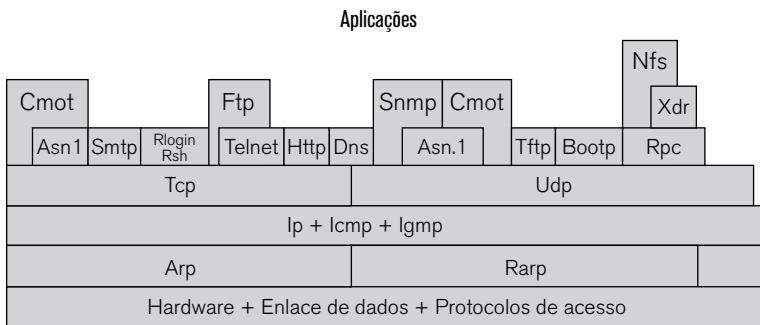


Figura 5.10 – Alguns protocolos de aplicação. Fonte: elaborado pelo autor.

5.2.1 DNS

O protocolo **DNS** (*domain name system*) especifica duas partes principais: regras de sintaxe para a definição de domínios e o protocolo utilizado para a consulta de nomes.

O DNS é basicamente um mapeamento entre endereços IP e nomes (*hostnames*).

A estrutura de nomes na Internet tem o formato de uma árvore invertida em que a raiz não possui nome. Os ramos imediatamente inferiores à raiz são chamados de TLDs (*top-level domain names*) e são, por exemplo, .com, .edu., .org, .gov, .net, .mil, .br, .fr, .us, uk, etc... Os TLDs que não designam países são utilizados nos EUA. Os diversos países utilizam a sua própria designação para as classificações internas. No Brasil, por exemplo, temos os nomes .com.br., .gov.br, .net.br, .org.br e outros.

Cada ramo completo até a raiz como, por exemplo, eme.eb.mil.br, acme.com.br, nasa.gov e outros são chamados de domínios (figura 5.11).

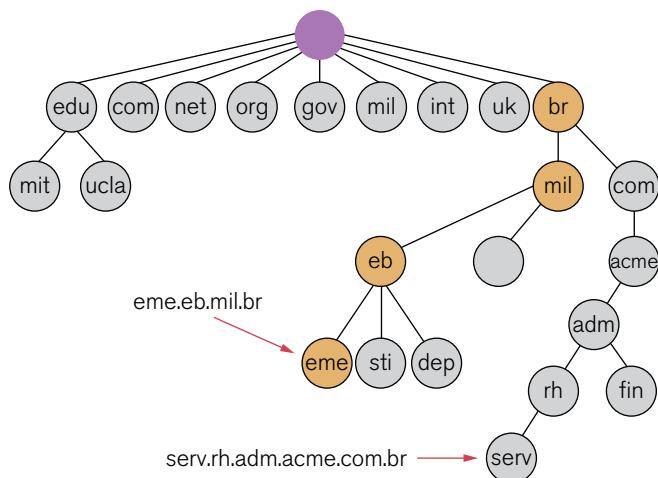


Figura 5.11 – Exemplo de árvore DNS. Fonte: elaborado pelo autor.

Domínio é a área administrativa englobando ele próprio e os subdomínios abaixo dele, por exemplo, o domínio .br engloba todos os subdomínios do Brasil. O domínio acme.com.br responsabiliza-se por todos os domínios abaixo dele. A delegação de responsabilidade de um domínio é a capacidade do

DNS de simplificar a administração. Ao invés de o domínio .br ser responsável diretamente por todos os seus subdomínios e os que vierem abaixo deles, há, na verdade, uma delegação na atribuição de nomes para os diversos subdomínios. No exemplo dado, a empresa Acme possui a responsabilidade de administração do domínio acme.com.br.

Os domínios principais genéricos, chamados de GTLDs (*generic top level domain names*) que são .net, .com e .org são administrados pelo Internic (*Internet Network Information Center*), que também é responsável pela administração do espaço de endereçamento IP. Os domínios são completamente independentes da estrutura de rede utilizada. Não existe necessariamente relacionamento entre eles. O DNS possui uma estrutura inversa para poder representar o endereçamento de rede ou permitir que seja feito o mapeamento do endereço IP correspondente a um nome (*hostname*).

Esta estrutura possui como raiz principal a notação .arpa e como único ramo o .in-addr. Abaixo deste, são colocados em ordem os bytes do endereço IP.

Implementação do DNS

O DNS é um serviço cliente/servidor, no entanto é diferente de outros serviços cliente/servidor. Enquanto outros serviços utilizam um cliente que é uma aplicação (como navegador Web, cliente de e-mail), o cliente DNS é executado como um serviço. O cliente DNS, às vezes chamado de resolvedor DNS, suporta a resolução de nome para outras aplicações de rede e outros serviços que precisam dele.

Ao configurar um dispositivo de rede, geralmente fornecemos um ou mais endereços de Servidor DNS que o cliente DNS pode utilizar para resolução de nome. Normalmente, o provedor de serviço de Internet fornece os endereços a serem utilizados para os servidores DNS. Quando a aplicação de um usuário solicita uma conexão a um dispositivo pelo nome, o cliente DNS solicitante consulta um desses servidores de nome para atribuir o nome a um endereço numérico.

Um servidor de DNS pode ser responsável pela resolução de um ou mais nomes de domínios (ex. acme.com.br, presid.acme.com.br). Seu escopo de atuação define a zona de atuação de um servidor DNS, por exemplo, para resolver o domínio acme.com.br e seus subdomínios existem três zonas: a primeira resolve o próprio domínio principal e os subdomínios mktg.acme e vendas.acme;

a segunda resolve os domínios engen.acme e prod.engen.acme; e a terceira resolve o domínio lab.engen.acme. Cada zona possui um servidor de nomes principal ou primário, que mantém em tabelas o mapeamento dos nomes em endereços IP daquele domínio. Uma zona pode ter servidores secundários que podem substituir os primários em caso de falha. Os secundários, apesar de não possuírem fisicamente as tabelas de mapeamento, carregam regularmente as informações do primário.

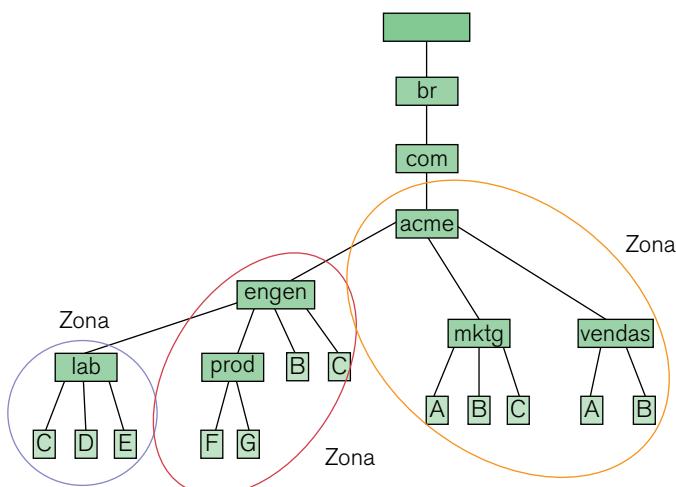


Figura 5.12 – Exemplo de árvore DNS. Fonte: elaborado pelo autor.

5.2.2 Correio eletrônico

O correio eletrônico permite enviar mensagens entre computadores conectados. O procedimento para enviar um documento de correio eletrônico envolve dois processos separados. O primeiro é enviar as mensagens de correio eletrônico à agência de correio do usuário e o segundo é entregar as mensagens de correio eletrônico dessa agência ao cliente de correio eletrônico do usuário (ou seja, o destinatário).

As etapas a seguir vão ajudá-lo a compreender o processo de envio de uma mensagem de correio eletrônico:

1. Iniciar seu programa de correio eletrônico.
2. Digitar o endereço do correio eletrônico do destinatário.

3. Digitar o assunto.
4. Digitar uma letra.

Agora, examine o endereço de correio eletrônico. Esse é um exemplo de como ele pode ser: `tutoria@cep.ensino.eb.br`. Ele consiste em duas partes: o nome do destinatário (localizado antes do símbolo @) e o endereço da agência de correio do destinatário (após o símbolo @). O nome do destinatário é importante apenas após a mensagem ter chegado ao endereço da agência de correio, que é uma entrada DNS que representa o endereço IP do servidor.

A parte do endereço de correio eletrônico que contém o nome do destinatário torna-se importante neste ponto. O servidor extrai essa parte da mensagem de correio eletrônico e verifica se o destinatário é um membro da sua agência de correio. Se o endereço for um membro, o servidor armazenará a mensagem na caixa de correio do destinatário até que alguém a recupere. Se o endereço não for de um membro, a agência de correio gerará uma mensagem de erro e enviará a mensagem de correio eletrônico de volta para o remetente.

A segunda parte do processo de funcionamento do correio eletrônico é o processo de recebimento. Os destinatários de mensagens de correio eletrônico usam o *software* cliente de correio eletrônico em seus computadores para estabelecer solicitações às agências de correio eletrônico. Quando os destinatários das mensagens clicam nos botões "Receber mensagens" ou "Recuperar mensagens" no cliente de correio eletrônico, geralmente é solicitada uma senha. Após terem inserido a senha e clicado em "OK", o *software* de correio eletrônico cria uma solicitação aos servidores da agência de correio, que extraem o endereço da agência dos dados de configuração que foram inseridos quando o *software* de correio eletrônico dos destinatários foi configurado. O processo usa, então, uma outra pesquisa do DNS para localizar os endereços IP dos servidores. Finalmente, as solicitações são segmentadas e colocadas em sequência pela camada de transporte.

Os pacotes de dados trafegam pelo restante das camadas do modelo OSI (por exemplo, camadas da rede, de enlace de dados, física) e são transmitidos pela Internet à agência de correio eletrônico de destino. Nessa agência, os pacotes são reagrupados, na sequência apropriada, e são verificados quaisquer erros de transmissão de dados.

Na agência de correio, as solicitações são examinadas e os nomes dos usuários e as senhas são verificados. Se tudo estiver correto, os servidores da agência transmitem todas as mensagens de correio eletrônico aos computadores, onde as mensagens são, novamente, segmentadas, colocadas em sequência e encapsuladas como quadros de dados, para serem enviadas ao computador do cliente ou do destinatário do correio eletrônico.

Após as mensagens de correio eletrônico terem chegado a um computador, você pode abri-las e lê-las. Se você clicar no botão "Responder" ou no botão "Encaminhar", para enviar respostas às mensagens, todo o processo será novamente iniciado. As mensagens de correio eletrônico, em si, são normalmente enviadas como texto ASCII, mas os anexos, que às vezes são incluídos nelas, podem ser dados de áudio, de vídeo, de figuras ou muitos outros tipos de dados. Para receber e enviar corretamente os anexos, os esquemas de codificação devem ser os mesmos do computador emissor e do computador receptor.

O correio eletrônico utiliza dois tipos diferentes de protocolos (figura 5.13).

1. Protocolo para o envio de correio – SMTP (*simple mail transfer protocol*)
2. Protocolo para recebimento de correio eletrônico – POP3 (*post office protocol*) ou IMAP (*Internet message access protocol*)

Protocolo SMTP

O SMTP transfere e-mails de forma confiável e eficiente. Para que os aplicativos de SMTP funcionem corretamente, a mensagem de e-mail deve ser formatada corretamente e processos SMTP devem ser executados no cliente e no servidor.

Os formatos de mensagens SMTP exigem um cabeçalho da mensagem e um corpo da mensagem. Enquanto o corpo da mensagem pode conter qualquer valor de texto, o cabeçalho da mensagem deve ter o endereço de e-mail de destinatário devidamente formatado e o endereço de remetente. Qualquer outra informação de cabeçalho é opcional.

Quando um cliente envia e-mail, o processo de SMTP do cliente se conecta com um processo SMTP do servidor na porta 25 conhecida. Depois que a conexão é feita, o cliente tenta enviar o e-mail para o servidor através da conexão. Quando o servidor recebe a mensagem, ele a coloca em uma conta local, se o

destinatário for local, ou encaminha-a usando o mesmo processo de conexão SMTP para outro servidor de entrega.

Protocolo POP

O protocolo POP permite que uma estação de trabalho recupere o e-mail de um servidor. Com o POP, o e-mail será transferido do servidor ao cliente e, por padrão, excluído no servidor.



ATENÇÃO

O usuário pode eventualmente configurar o POP para deixar uma cópia no servidor.

O servidor inicia o serviço POP ao ouvir de forma passiva na porta TCP 110 para solicitações de conexão do cliente. Quando um cliente deseja utilizar o serviço, ele envia uma solicitação para estabelecer uma conexão TCP com o servidor. Quando a conexão é estabelecida, o servidor POP envia uma saudação. O cliente e o servidor POP trocam comandos e respostas até que a conexão seja fechada ou cancelada.

Protocolo IMAP

O IMAP, que utiliza a porta 143, é outro protocolo que descreve um método para recuperar mensagens de e-mail, entretanto, ao contrário do POP, quando o usuário se conecta a um servidor IMAP, as cópias das mensagens são transferidas à solicitação do cliente. As mensagens originais são mantidas no servidor até que sejam excluídas manualmente. Os usuários exibem cópias das mensagens em seu *software* cliente de e-mail.

Os usuários podem criar uma hierarquia do arquivo no servidor para organizar e armazenar o e-mail. A estrutura de arquivo é também duplicada no cliente de e-mail. Quando um usuário decide excluir uma mensagem, o servidor sincroniza essa ação e a exclui do servidor.

5.2.3 Telnet

O *software* de emulação de terminal (Telnet) utiliza a porta 23 e provê o acesso de forma remota a outro computador. Isso permite que você efetue o logon em um *host* da Internet e execute comandos. Um cliente Telnet é chamado de *host* local e um servidor Telnet, que usa um *software* especial denominado daemon, é chamado de *host* remoto.

Para fazer a conexão de um cliente Telnet, você deve selecionar uma opção de conexão. Uma caixa de diálogo solicita um "Nome de *host*" e um "tipo de terminal". O nome do *host* é o endereço IP (DNS) do computador remoto ao qual você deseja se conectar e o tipo de terminal descreve o tipo de emulação terminal que você deseja que seja executado pelo computador.

A operação Telnet não usa nenhuma capacidade de processamento do computador de transmissão. Em vez disso, ela transmite as teclas pressionadas ao *host* remoto e envia a saída de tela resultante de volta ao monitor local. Todo o processamento e o armazenamento ocorrem no computador remoto.

5.2.4 FTP (*file transfer protocol*)

O protocolo de transferência de arquivos (FTP) é projetado para fazer o *download* ou *upload* de arquivos de um *host* cliente para um *host* servidor. A capacidade de fazer o *download* e o *upload* de arquivos na Internet é um dos recursos mais valiosos que a Internet tem a oferecer, especialmente para as pessoas que dependem do computador para várias finalidades e quando *drivers* e atualizações de *software* podem ser imediatamente necessários. Os administradores de rede raramente podem esperar, mesmo alguns dias, para obter os *drivers* necessários que permitam que os servidores de rede voltem a funcionar. A Internet pode fornecer esses arquivos imediatamente pelo uso do FTP.

O FTP é uma aplicação cliente-servidor tal como o correio eletrônico e o Telnet. Ele exige um *software* servidor sendo executado em um *host* que pode ser acessado pelo *software* cliente.

Uma sessão do FTP é estabelecida da mesma maneira que uma sessão Telnet. Tal como o Telnet, a sessão do FTP é mantida até que o cliente a termine ou haja algum tipo de erro de comunicação.

Tendo estabelecido uma conexão com um *daemon* do FTP, você deve fornecer uma ID de *logon* e uma senha. Normalmente, você usaria **anonymous** como a ID de *logon* e seu endereço de correio eletrônico como senha. Esse tipo de conexão é conhecido como FTP anônimo. Ao estabelecer sua identidade, um *link* de comandos se abre entre a máquina cliente e o servidor de FTP. Esse recurso permite criar e alterar pastas, apagar e renomear arquivos ou executar muitas outras funções associadas ao gerenciamento de arquivos.

A finalidade principal do FTP é transferir arquivos de um computador para outro, copiando e movendo arquivos dos servidores para os clientes e dos clientes para os servidores. Ao copiar arquivos de um servidor, o FTP estabelece uma segunda conexão, um enlace de dados entre os computadores, através da qual os dados são transferidos.

A transferência de dados pode ocorrer no modo ASCII ou no modo binário. Esses dois modos determinam como o arquivo de dados deverá ser transferido entre as estações. Após a transferência de arquivos ser encerrada, a conexão dos dados será automaticamente finalizada. Após ter concluído toda a sessão de cópia e movimentação dos arquivos, você pode efetuar *logoff*, fechando, assim, o *link* de comandos e terminando a sessão. Um outro protocolo que tem a capacidade de fazer o *download* de arquivos é o HTTP, que será estudado na próxima seção.

5.2.5 HTTP

O *hyper text transfer protocol* (HTTP) utiliza a porta 80 e trabalha com a *World Wide Web*, que é a parte da Internet que tem crescido mais rapidamente e a mais usada. Uma das razões principais do extraordinário crescimento da *Web* é a facilidade com que ela permite o acesso às informações.

Um navegador da *Web* (juntamente com todas as outras aplicações da rede tratadas neste capítulo) é uma aplicação cliente-servidor, o que significa que ele exige um componente cliente e um componente servidor para funcionar.

Um navegador da *Web* apresenta os dados em formato multimídia nas páginas da *Web* que usam texto, imagens, som e vídeo. As páginas da *Web* são criadas com uma linguagem de formato chamada linguagem de marcação de

hipertexto (HTML). A HTML formata a aparência de uma página Web, de forma a orientar o navegador como ela deve ser exibida. Para isso, a HTML especifica locais para a colocação de textos, arquivos e objetos que serão transferidos do servidor da *Web* para o navegador da *Web*.

Os *hiperlinks* facilitam a navegação na *World Wide Web*. Um *hiperlink* é um objeto (por exemplo, uma palavra, frase ou figura) em uma página da *Web* que, quando clicado, transfere você para uma nova página da *Web*. A página da *Web* contém (dentro de sua descrição HTML, frequentemente oculta) um local de endereço conhecido como localizador uniforme de recursos (URL).

Quando você abre um navegador da *Web*, a primeira coisa que normalmente se vê é uma página inicial (ou "*home page*"). O URL da *home page* já foi armazenado na área de configuração do navegador da *Web* e pode ser alterado a qualquer momento. Na página inicial, você pode clicar em um dos *hiperlinks* da página da *Web* ou digitar um URL na barra de endereços do navegador. O navegador da *Web*, então, examina o protocolo para determinar se ele precisa abrir outro programa e determina o endereço IP do servidor da *Web*. Em seguida, a camada de transporte (protocolo TCP) inicia uma sessão com o servidor da *Web*. Os dados que são transferidos para o servidor HTTP contêm o nome da pasta do local da página da *Web* (observação: os dados podem também conter um nome de arquivo específico para uma página HTML). Se não for fornecido nenhum nome, o servidor usará um nome-padrão (conforme especificado na configuração do servidor).

O servidor responde à solicitação enviando todos os arquivos de áudio, vídeo e imagens, como especificado nas instruções HTML, ao cliente da *Web*. O navegador cliente reagrupa todos os arquivos para criar uma visualização da página da *Web* e, depois, termina a sessão. Se você clicar em uma outra página que esteja localizada no mesmo servidor ou em um servidor diferente, o processo todo vai começar novamente.

Embora o HTTP seja notavelmente flexível, não é um protocolo seguro. As mensagens solicitadas enviam informações ao servidor em texto simples que podem ser interceptadas e lidas. Da mesma forma, as respostas do servidor, normalmente páginas HTML, também não são criptografadas.

Para comunicação segura pela Internet, o protocolo HTTP seguro (HTTPS) é utilizado para acessar ou enviar informações para o servidor *Web*. O HTTPS pode utilizar autenticação e criptografia para proteger dados que viajam entre o cliente e o servidor. O HTTPS especifica regras adicionais para a passagem de

dados entre a camada de aplicação e a de transporte. O HTTPS usa o mesmo processo de solicitação do cliente-resposta do servidor do HTTP, mas o fluxo de dados é criptografado com protocolo SSL antes de ser transportado pela rede. O HTTPS cria carga e tempo de processamento adicionais no servidor, devido à criptografia e à descriptografia dos dados transmitidos.



ATIVIDADE

Acesse os *sites* e responda às questões *on-line* de redes.

Disponível em:

<<https://www.qconcursos.com/questoes-de-concursos/disciplinas/tecnologia-da-informacao-redes-de-computadores>>.

Disponível em:

<<https://www.aprovaconcursos.com.br/questoes-de-concurso/disciplina/redes-de-computadores>>.

Disponível em: <<https://www.gabaritou.com.br/Questao?DisciplinalD=11>>.

Acesse os *sites* e explore os recursos *on-line*.

Disponível em:

<http://wps.aw.com/br_kurose_redes_3/40/10271/2629589.cw/index.html>.

Animações do livro de Forouzan

Disponível em:

<http://highered.mheducation.com/sites/0072967722/student_view0/animations.html#>.



REFLEXÃO

Você viu nesta aula os principais protocolos das camadas de transporte e aplicação e a forma como eles funcionam.



LEITURA

Leia os capítulos 23, 25, 26 e 27 do livro Comunicação de dados e redes de computadores, de Behrouz A. Forouzan.

Saiba mais

Assista aos vídeos abaixo:

Disponível em: <<https://www.youtube.com/watch?v=E4gcWJaw8aQ>>.

Disponível em: <<https://www.youtube.com/watch?v=epWv0-eqRMw>>.

Disponível em: <<https://www.youtube.com/watch?v=ACGuo26MswI>>.

Disponível em: <https://www.youtube.com/watch?v=ZYsjMEISR6E&list=PLOJJrpFkn-9JANRUbetyOH_nOazAwYQdX5>.

Disponível em: <<https://www.youtube.com/watch?v=QyOhW-cOpT0>>.

Disponível em: <<https://www.youtube.com/watch?v=gZRYDxWuYpk>>.



REFERÊNCIAS BIBLIOGRÁFICAS

FOROUZAN, Behrouz A. *Comunicação de dados e redes de computadores*. 4. ed. São Paulo: McGraw-Hill, 2008.

KUROSE, James F. e ROSS, Keith W. *Redes de computadores e a Internet: uma abordagem top-down*. 4. ed. São Paulo: Addison Wesley, 2009.

Tanenbaum, Andrew S. *Redes de computadores*. 5. ed. Rio de Janeiro: Campus, 2007.

6

Redes SOHO

Redes de pequenas empresas e de empresas domésticas possuem sérias limitações quanto ao custo de equipamentos. A contratação de um *link* dedicado é inviável neste ambiente, de forma que meios de acesso à Internet com menor custo, utilização de equipamento de comutação mais baratos (*switches SOHO*) e configurações simplificadas de redes são amplamente bem vistos neste cenário.

É dentro deste contexto que iremos abordar as redes SOHO neste capítulo.



OBJETIVOS

- Descrever o acesso à Internet via modem.
 - Identificar as funções da placa de rede.
 - Descrever o funcionamento do *switch*.
 - Configurar *hosts*.
 - Descrever o funcionamento do NAT.
 - Descrever o funcionamento do DHCP.
-

6.1 Redes SOHO

Redes SOHO do inglês ***Small Office Home Office*** refere-se às soluções de redes para pequenas empresas ou para usuários domésticos e constituem a maior parte das redes existentes no mundo.

Neste tipo de solução de rede, o acesso à Internet é realizado via algum tipo de conexão de banda larga, como ADSL ou *cable modem*.

Além disso, a rede, se cabeada com UTP, adota uma solução de padrão Ethernet (tipicamente ***fast Ethernet***) utilizando comutadores e cabos UTP. Outra possibilidade é a utilização de redes sem fio ou, ainda, uma mistura das duas soluções (parte da rede cabeada e parte sem fio).



ATENÇÃO

A rede *fast Ethernet* possui uma largura de banda de 100 Mbps, embora existam no mercado soluções de giga Ethernet (1000 Mbps) ou 10giga (10000Mbps). Estas são muito caras de forma que a rede SOHO típica continua a utilizar a *fast Ethernet*.

Podemos prever, que devido ao barateamento do *hardware*, a tendência é a solução-padrão tornar-se a giga Ethernet em um prazo relativamente curto.

6.2 Soluções de acesso à Internet

6.2.1 Endereçamento IP privado

Conforme vimos no capítulo 4, o endereço IP evoluiu do endereçamento por classes para o endereçamento sem classes, visando poupar endereços.

Além deste aspecto, foi também adotado o conceito de **IP privado** e **IP público**.

O IP público é aquele válido na Internet, ou seja, aquele que um *host* deve possuir para poder navegar. Este IP é fornecido pelo **ISP** que prove seu acesso à Web.



CONCEITO

ISP: – ***Internet service provider*** – provedor de serviço de Internet são empresas que, como o nome diz, oferecem diversos tipos de serviço ligados à Internet como hospe-

dagem de sites, armazenamento na nuvem ou acesso à rede, sendo este último o que oferece o IP público.

IP's privados são utilizados em endereçamento de redes locais. Eles não são válidos na Internet.

As faixas de endereços IP privados são as seguintes:

- 10.0.0.0/8 – IP 10.0.0.0 a 10.255.255.255
- 172.16.0.0/12 – IP 172.16.0.0 a 172.31.255.255
- 192.168.0.0/16 – IP 192.168.0.0 a 192.168.255.255

Quando vamos configurar o endereçamento de uma rede local, os *hosts* recebem IP privados de uma das faixas acima. Para poder navegar na Internet, eles terão que utilizar algum tipo de artifício, pois seus IP's não são válidos. Alguma máquina na rede, normalmente o roteador, ficará responsável por permitir a navegação na Internet utilizando **NAT**.

CONCEITO

NAT: – **Network Address Translation** – é um protocolo que, como o próprio nome diz (tradução de endereço de rede), faz a tradução dos endereços IP privados e portas TCP/UDP da rede local para a Internet (IP públicos). Iremos estudar NAT mais à frente neste capítulo.

6.2.2 Equipamentos de acesso

Redes residenciais ou de pequenas empresas não utilizam, devido ao custo, linhas de transmissão dedicadas. O cenário típico nestes casos é a contratação de soluções comerciais de banda larga baseada nas tecnologias **ADSL** ou **cable modem**.



Figura 6.1 – Modem ADSL e cable modem.



ATENÇÃO

As soluções de ADSL são conhecidas com nomes comerciais como Velox, Live Tim etc., enquanto as de *cable modem* possuem como exemplo o Virtua.

As duas soluções utilizam modens cuja principal diferença é a fonte de entrada dos sinais. No ADSL, é uma linha telefônica normal, enquanto no *cable modem* é um coaxial de televisão a cabo (figura 6.1).

Estes modens possuem tipicamente um conjunto de luzes que indicam o seu funcionamento e são administrados via uma interface Web (figura 6.2).

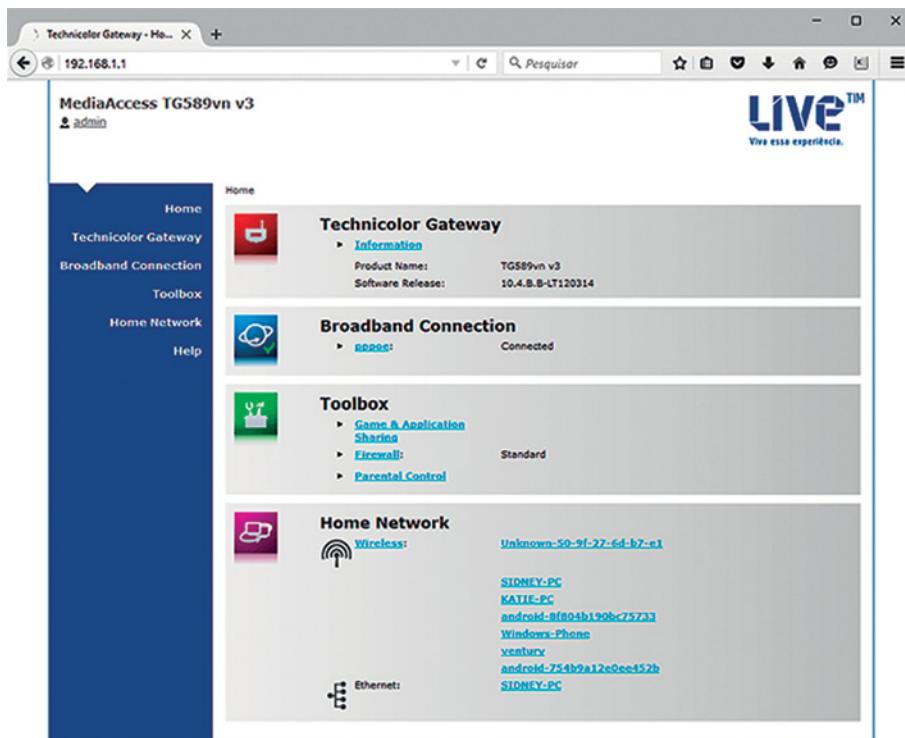


Figura 6.2 – Exemplo de interface de administração de modens. Fonte: elaborado pelo autor.



CONEXÃO

Para saber como administrar vários modens, acesse o *site* da Associação Brasileira dos Usuários de Acesso Rápido, onde você encontra tutoriais e manuais de vários equipamentos: <<http://www.abusar.org.br/>>.

Os modens podem funcionar de dois modos básicos

1. Modo ponte (*bridge mode*)
2. Modo roteador (*router mode*)

6.2.2.1 Modo ponte (*bridge mode*)

Quando um modem está configurado em modo ponte, ele envia diretamente ao computador em que está conectado os pacotes recebidos, fazendo apenas as conversões de protocolos necessários entre as camadas de enlace e física da WAN (*cable modem* ou ADSL) e da LAN (cabo UTP) ligando a estação ao modem.

Neste tipo de configuração, o usuário deve comandar a conexão a partir de sua máquina, utilizando um programa discador, e o IP público fica na máquina (figura 6.3).

Este modelo de configuração atua na camada 2 do modelo OSI.

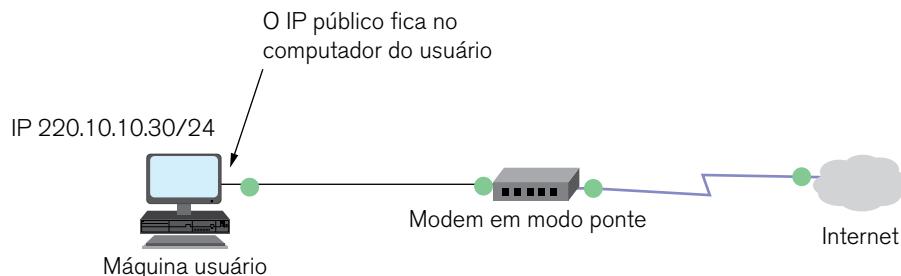


Figura 6.3 – Modem em modo ponte. Fonte: elaborado pelo autor.

6.2.2.2 Modo roteador (*router mode*)

Quando um modem está configurado em modo roteador, ele atua independentemente de outras máquinas, faz a conexão na rede do ISP por conta própria e re-

cebe um endereço IP público que fica em sua porta de WAN. A partir deste ponto, ele trabalha como um roteador, encaminhando os pacotes da rede local para a Internet e vice-versa. Normalmente, os modems que suportam este modo de operação possuem agregados em seu hardware um switch de 4 portas e rede sem fio.

Para que a rede possa funcionar corretamente, o modem fará **NAT** e irá, normalmente, trabalhar também como servidor **DHCP** da rede (figura 6.4).

Este modelo de configuração atua na camada 3 do modelo OSI.

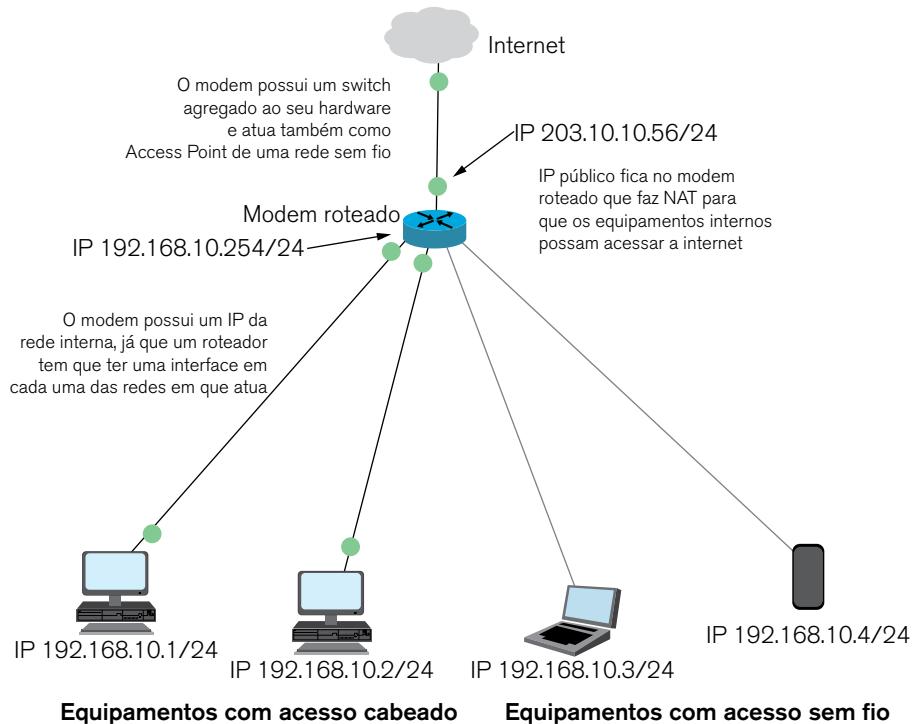


Figura 6.4 – Modem em modo roteador. Fonte: elaborado pelo autor.

CONCEITO

DHCP: *Dynamic Host Configuration Protocol* (protocolo de configuração dinâmica de host) é um protocolo de serviço TCP/IP que oferece configuração dinâmica de terminais, com concessão de endereços IP de host, máscara de sub-rede, *default gateway* (*gateway* padrão) e DNS. Iremos estudar **DHCP** mais à frente neste capítulo.

6.3 Ativos de redes

6.3.1 Placa de rede

Placa de rede é uma placa de circuito impresso (figura 6.5) que se encaixa no *slot* de expansão de um barramento em uma placa-mãe do computador ou em um dispositivo periférico. Sua função é adaptar o dispositivo de *host* ao meio da rede.



Figura 6.5 – Placa de rede Ethernet barramento PCI. Disponível em:< https://commons.wikimedia.org/wiki/File:Ethernet_pci_card.jpg>.

As placas de rede são consideradas dispositivos da camada 2 porque cada placa de rede em todo o mundo transporta um código exclusivo, chamado endereço *media access control* (MAC). Esse endereço é usado para controlar as comunicações de dados do host na rede. Você depois vai aprender mais sobre o endereço MAC. Como o nome sugere, a placa de rede controla o acesso do *host* ao meio físico (cabeamento).

Funções:

- Preparar dados do computador para o cabo de rede.
- Enviar dados para outro computador.
- Controlar o fluxo de dados entre o computador e o sistema de cabeamento.

A placa e o fluxo de bits

Os dados trafegam dentro dos computadores pelos barramento, caracterizando uma transmissão em paralelo, já nos cabos de rede, os bits trafegam um após outro (fluxo).

A placa de rede deve fazer a conversão entre dois tipos de transmissão. Para isso:

- a placa de rede capta os dados;
- reestrutura-os de paralelo para serial (um bit por vez).

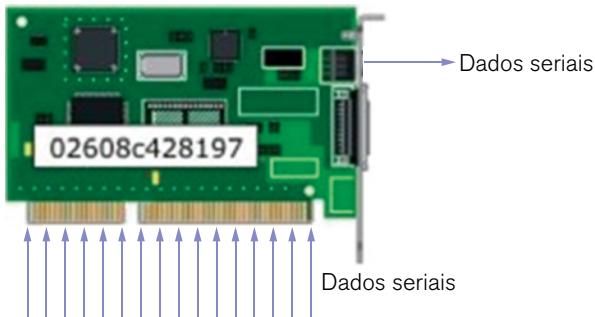


Figura 6.6 – Fluxo de bits na placa de rede. Curso Network Essencial da Microsoft. Adaptado pelo autor.

A placa de rede é considerada um transceptor (transmissor / receptor) que converte sinais digitais do computador para sinais elétricos que podem trafegar nos cabos da rede.

Para que ocorra a transmissão, duas placas de redes devem estabelecer antes alguns parâmetros de funcionamento, tais como:

- Tamanho máximo dos grupos de dados a serem enviados
- Quantidade de dados a serem enviados antes da confirmação
- Intervalo de tempo entre os envios de porções de dados
- Período de tempo a esperar antes da confirmação
- Tamanho do *buffer* de cada placa
- Velocidade de transmissão

Obs.: placas com velocidades diferentes ajustam-se ao nível mais baixo, ou seja, uma placa gigaEthernet (1000 Mbps), ao sincronizar uma *fast*Ethernet(100 Mbps), irá funcionar na velocidade mais baixa.

6.3.2 Switch

São dispositivos que filtram e encaminham pacotes entre segmentos de redes locais. Operam na camada de enlace (camada 2) do modelo OSI, devendo ser independentes dos protocolos de camada superior (figura 6.7).



Figura 6.7 – Switch Ethernet. Disponível em: <https://commons.wikimedia.org/wiki/File:Cisco_small_business_SG300-28_28-port_Gigabit_Ethernet_rackmount_switch.jpg>.

Redes locais que usam *switches* para denominadas LAN's comutadas

Os *switches* examinam os quadros do tráfego de entrada, acessam o endereço MAC de origem do quadro e apreendem quais estações estão conectadas a cada uma de suas portas, construindo desta forma uma tabela MAC, associando os endereços MAC das estações às suas portas. Este método de aprendizagem é chamado de **autoaprendizagem**.

O *switch*, para cada quadro de entrada, analisa o endereço MAC de destino no cabeçalho do quadro e o compara à lista de endereços na tabela MAC. Se uma correspondência for encontrada, a porta na tabela que está relacionada com o endereço MAC será usada como a porta de saída para o quadro (fig. 6.8).

Desta forma, os quadros recebidos são enviados apenas para a porta correspondente ao endereço de destino e não para todas as portas como no *Hub*.

VLAN	Mac Address	Port
1	0001.1111.1111	FastEthernet0/1
1	0002.2222.2222	FastEthernet0/2
1	0003.3333.3333	FastEthernet0/3
1	0004.4444.4444	FastEthernet0/4

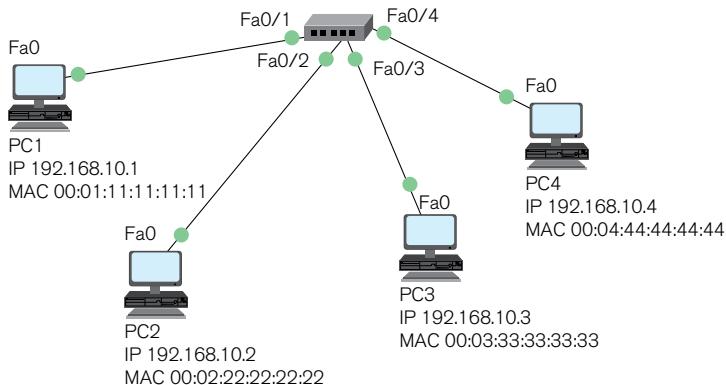


Figura 6.8 – Switch com tabela Mac. Fonte: elaborado pelo autor.



CONEXÃO

Para entender a autoaprendizagem do *switch*, assista ao vídeo disponível em:
[<http://video.rnp.br/portal/video.action?idItem=22107>](http://video.rnp.br/portal/video.action?idItem=22107).

Operação do *switch*

Para conseguir seu objetivo, os *switches LAN* usam cinco operações básicas:

- Aprendizado
- Envelhecimento
- Inundação
- Encaminhamento
- Filtragem

Aprendizado

A tabela MAC deve ser povoada com endereços MAC e suas portas correspondentes. O processo de aprendizado permite que esses mapeamentos sejam adquiridos de maneira dinâmica durante a operação normal.

À medida que cada quadro entra no *switch*, este examina o endereço MAC de origem. Usando um procedimento de pesquisa, o *switch* determina se a tabela já contém uma entrada para aquele endereço MAC. Se não houver entrada, o *switch* criará uma nova entrada na tabela MAC usando o endereço MAC de origem associado à porta em que o quadro chegou. O *switch* pode agora usar esse mapeamento para enviar quadros a este nó.

Envelhecimento

As entradas na tabela MAC adquiridas pelo processo de aprendizado são rotuladas com o horário do registro. Esse rótulo é usado como meio de remover entradas antigas da tabela MAC. Após uma entrada ser feita na tabela MAC, um procedimento inicia uma contagem, usando o horário registrado como valor inicial. Após o valor atingir 0, a entrada na tabela será atualizada quando o *switch* receber um quadro do nó na mesma porta.

Inundação

Se o *switch* não souber para qual porta enviar um quadro porque o endereço MAC de destino não está na tabela MAC, ele o enviará a todas as portas exceto para a porta na qual o quadro chegou. O processo de envio de um quadro a todos os segmentos é conhecido como inundação. O *switch* não envia o quadro à porta na qual ele chegou porque qualquer destino nesse segmento já terá recebido o quadro. A Inundação também é usada para quadros enviados para o endereço MAC de *broadcast*.

Encaminhamento

Encaminhamento é o processo onde se examina o endereço MAC de destino de um quadro, encaminhando-o para a porta adequada. Essa é a função principal do *switch*. Quando um quadro de um nó chega ao *switch* para o qual o *switch*

já aprendeu o endereço MAC, esse endereço é comparado a uma entrada na tabela MAC e o quadro é encaminhado para a porta correspondente. Em vez de inundar o quadro para todas as portas, o *switch* envia o quadro ao nó de destino por sua porta designada. Essa ação é chamada de encaminhamento.

Filtragem

Em alguns casos, um quadro não é encaminhado. Esse processo é chamado de filtragem de quadro. A utilização da filtragem já foi descrita: um *switch* não encaminha um quadro para a mesma porta na qual ele chegou. Um *switch* também irá abandonar um quadro corrompido. Se um quadro falhar na verificação CRC, o quadro será abandonado. Um outro motivo para filtrar um quadro é segurança. Um *switch* possui configurações de segurança para bloquear quadros para e/ou endereços MAC selecionados ou portas específicas.

Classificação dos *switches*

Quanto ao método de encaminhamento dos pacotes

- **Store-and-forward**

Switches store-and-forward armazenam cada quadro de entrada em um *buffer* e daí calcula o CRC. Se o quadro tiver sido corrompido durante a transmissão, o CRC irá falhar, gerará um erro e o quadro será descartado. Outra verificação feita é quanto ao tamanho do quadro: se for ou muito pequeno ou muito grande (um quadro Ethernet tem de 64 bytes a 1 518 bytes), o quadro também será descartado. Se estiver tudo OK, o quadro será encaminhado para a porta de saída.

Apesar de assegurar operações sem erro, este método adiciona uma grande latência devido ao tempo necessário para guardar e checar cada quadro. Esta latência é proporcional ao tamanho dos quadros, por isso quanto maior ele for, maior será o atraso.

- **Cut-through**

Os *switches cut-through* foram projetados para reduzir essa latência. Eles leem apenas os 6 primeiros bytes do quadro, ou seja, apenas o endereço de destino, encaminhando a seguir o quadro. Este tipo de processamento reduz bastante o atraso.

Esse *switch*, contudo, não detecta pacotes corrompidos causados por colisões (conhecidas como *runt*s), nem erros de CRC. Quanto maior for o número

de colisões na rede, maior será a largura de banda gasta com o encaminho de pacotes corrompidos.

O segundo tipo de *switch cut-through*, *fragment free*, foi projetado para eliminar esse problema. Nesse caso, o *switch* sempre lê os primeiros 64 bytes de cada pacote, assegurando que o quadro tenha pelo menos o tamanho mínimo, evitando o encaminhamento de *runt*s pela rede.

- ***Adaptative cut-through***

Os *switches* que processam pacotes no modo adaptativo suportam tanto *store-and-forward* quanto *cut-through*. Qualquer dos modos pode ser ativado pelo gerente da rede ou o *switch* pode ser inteligente o bastante para escolher entre os dois métodos, baseado no número de quadros com erro passando pelas portas.

Quando o número de quadros corrompidos atinge certo nível, o *switch* pode mudar do modo *cut-through* para *store-and-forward*, voltando ao modo anterior quando a rede se normalizar.

Apenas os *switches store-and-forward* ou *adaptative cut-through* podem suportar diferentes tipos de LAN em suas portas (como, por exemplo, giga Ethernet e fast Ethernet), pois como “bufferizam” os quadros, podem fazer a conversão do formato do quadro MAC ou do método de sinalização.

Forma de segmentação das sub-redes

- ***Layer 2 switches***

São os tradicionais, utilizados para dividir uma LAN em diversos domínios de colisão.

Eles suportam múltiplas transmissões simultâneas, já que a transmissão em um segmento de rede não interfere nos outros segmentos. Os *switches* de camada 2 não conseguem, porém, filtrar broadcasts e quadros, cujo MAC de destino ainda não tenha sido incluído em sua tabela de endereçamento.

- ***Layer 3 switches***

São *switches* que incorporam algumas funções de roteamento aos serviços oferecidos pela camada 2.

Este tipo de *switch* pode, baseado em informações de camada de rede (camada 3), realizar o encaminhamento com base no endereço IP, validação do cabeçalho da camada 3 por *checksum* e suporte aos protocolos de roteamento tradicionais (RIP, OSPF etc.).

Os *switches* de camada 3 permitem, também, a implementação de **redes virtuais (VLAN's)**, roteando entre eles diretamente, dispensando o uso de um roteador externo.



CONCEITO

Uma **rede local virtual**, normalmente denominada de **VLAN**, é uma rede logicamente independente. Várias VLANs podem coexistir em um mesmo comutador (*switch*), de forma a dividir uma rede local (física) em mais de uma rede (virtual), criando domínios de *broadcast* separados. Uma VLAN também torna possível colocar em um mesmo domínio de *broadcast hosts* com localizações físicas distintas e ligados a *switches* diferentes.

Redes virtuais operam na camada 2 do modelo OSI, no entanto uma VLAN geralmente é configurada para mapear diretamente uma rede ou sub-rede IP, o que dá a impressão de que a camada 3 está envolvida.

Enlaces *switch-switch* e *switch-roteador* são chamados de troncos. Um roteador ou switch de camada 3 serve como interligador para o tráfego que passa em VLANs diferentes.

Apesar da semelhança entre si, *switches* de camada 3 e roteadores, possuem algumas características distintas, conforme podemos verificar na tabela comparativa:

CARACTERÍSTICAS	SWITCH DE CAMADA 3	ROTEADOR TRADICIONAL
Roteamento IP	Sim	Sim
Definição de sub-rede	Por porta ou Grupo de portas	Por Porta
Implementação do repasse	Hardware (ASIC)	Software / Microprocessadores
Suporte RMON	Sim	Não

CARACTERÍSTICAS	SWITCH DE CAMADA 3	ROTEADOR TRADICIONAL
Custo	+ Baixo	+ Alto
Suporte WAN	Não	Sim
Desempenho	Relativamente + alto	Relativamente + baixo
Escalabilidade	+ Escalável	- Escalável

Tabela 6.1 – Principais diferenças entre switches de camada 3 e roteadores.

6.3.3 Roteador

O roteador (*router*) é um equipamento de interconexão de redes que implementa funcionalidade até a camada de rede. O roteador, diferentemente do *switch*, isola o tráfego entre os segmentos pelo endereçamento lógico.



Figura 6.9 – Roteador aberto. Disponível em: <<https://commons.wikimedia.org/wiki/File:Cisco-2503-router-hdr-0a.jpg>>.

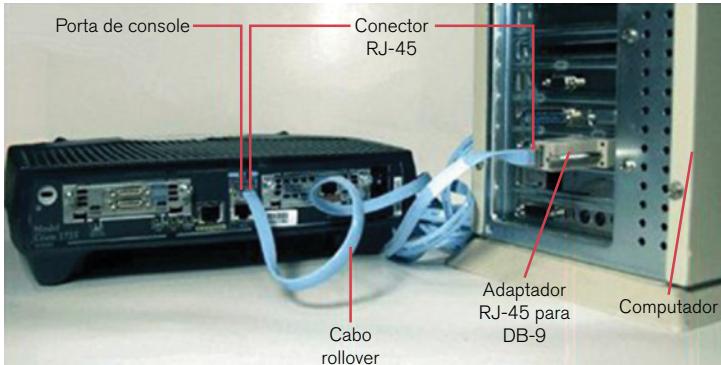


Figura 6.10 – Roteador. Disponível em: <https://commons.wikimedia.org/wiki/File:Roteador_Cisco_1700_ligado_ao_computador.jpg>.

São "computadores" dedicados, ligados a mais de uma rede física, sendo que uma de suas funções é destinar os pacotes para a rede correspondente. Conhecem os endereços de algumas redes e sabem o caminho que levará os pacotes até elas.

A vantagem de usar roteadores dedicados é que eles são construídos exatamente para isto, não existindo outros processos concorrendo com a tarefa de roteamento, como acontece em computadores comuns. Atualmente, os roteadores são multiprotocolares e suportam múltiplas tecnologias de enlace, tanto de rede local (LAN) quanto de longa distância (WAN).

Por entender os diversos protocolos de rede, o roteador possibilita um tratamento diferenciado por arquitetura de rede. Em outras palavras, o roteador permite não só filtrar as aplicações dentro de cada arquitetura de rede, como também priorizá-las.

Os roteadores propiciam a criação de uma estrutura lógica de endereçamento e o controle de acesso à rede. Além de criar domínios de *broadcast*, o roteador implementa uma visão lógica de endereçamento na rede por meio do suporte aos diversos protocolos roteáveis.

A implantação de um esquema de endereçamento hierárquico viabiliza a summarização de endereços (rotas), reduzindo o tamanho das tabelas de roteamento e, consequentemente, o tráfego para divulgação das rotas.

Com a implantação de listas de acesso ou filtros de pacotes, o roteador trabalha como componente da arquitetura de **firewall**, implantando uma barreira de segurança.



CONCEITO

Firewall é uma solução de segurança baseada em *hardware* ou *software* (mais comum) que, por meio de um conjunto de regras ou instruções, analisa o tráfego de rede para determinar quais operações de transmissão ou recepção de dados podem ser executadas. "Parede de fogo", tradução literal do nome, já deixa claro que o *firewall* se enquadra em uma espécie de barreira de defesa. A sua missão, por assim dizer, consiste basicamente em bloquear o tráfego de dados indesejados e liberar acessos bem-vindos.

Um *firewall* pode impedir uma série de ações maliciosas: um *malware* que utiliza determinada porta para se instalar em um computador sem consentimento do usuário, um programa que envia dados sigilosos para a Internet ou uma tentativa de acesso à rede proveniente de computadores externos não autorizados, por exemplo.

O roteador permite, ainda, o controle do comportamento de determinados protocolos que geram muito tráfego ou muitos *broadcasts* na rede, oferecendo serviços de **proxy** (procurador) para os *hosts* que os utilizam.



CONCEITO

Em redes de computadores, um **Proxy** (em português procurador) é um servidor (um sistema de computador ou uma aplicação) que age como intermediário para requisições de clientes solicitando recursos de outros servidores. Um cliente conecta-se ao servidor *proxy*, solicitando arquivo, conexão, página Web ou outros recursos disponíveis de um servidor diferente. O *proxy*, então, avalia a solicitação como um meio de simplificar e controlar sua complexidade. Os *proxies* foram inventados para adicionar estrutura e encapsulamento a sistemas distribuídos. Hoje, a maioria dos *proxies* é *proxy Web*, facilitando o acesso ao conteúdo na World Wide Web e fornecendo anonimato.

6.4 Configuração de host

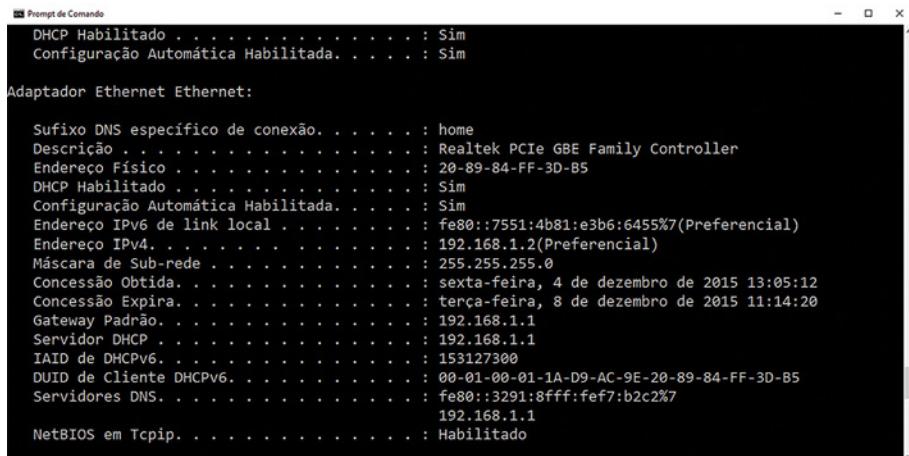
Um *host*, para poder navegar na Internet, deve ser configurado com os seguintes dados:

1. Endereço IP: endereço do *host*
2. Máscara de sub-rede: para determinar a rede.

3. *Gateway*-padrão: roteador que atende o *host* e permite que ele se comunique com outra rede

4. Servidor DNS: resolve as URL para o *host* devolvendo o IP que se deseja acessar.

A figura 6.11 mostra a configuração IP de um *host* obtida pelo comando *ipconfig /all* no *prompt* de comando de uma máquina rodando Windows 10.



Prompt de Comando

```
DHCP Habilitado . . . . . : Sim
Configuração Automática Habilitada. . . . . : Sim

Adaptador Ethernet Ethernet:

Sufixo DNS específico de conexão. . . . . : home
Descrição . . . . . : Realtek PCIe GBE Family Controller
Endereço Físico . . . . . : 20-89-84-FF-3D-B5
DHCP Habilitado . . . . . : Sim
Configuração Automática Habilitada. . . . . : Sim
Endereço IPv6 de link local . . . . . : fe80::7551:4b81:e3b6:6455%7(Preferencial)
Endereço IPv4 . . . . . : 192.168.1.2(Preferencial)
Máscara de Sub-rede . . . . . : 255.255.255.0
Concessão Obtida. . . . . : sexta-feira, 4 de dezembro de 2015 13:05:12
Concessão Expira. . . . . : terça-feira, 8 de dezembro de 2015 11:14:20
Gateway Padrão. . . . . : 192.168.1.1
Servidor DHCP . . . . . : 192.168.1.1
IAID de DHCPv6. . . . . : 153127300
DUID de Cliente DHCPv6. . . . . : 00-01-00-01-1A-D9-AC-9E-20-89-84-FF-3D-B5
Servidores DNS. . . . . : fe80::3291:8fff:fef7:b2c2%7
192.168.1.1
NetBIOS em Tcpip. . . . . : Habilitado
```

Figura 6.11 – *Host* configurado. Fonte: elaborado pelo autor

Repare no endereço IP 192.168.1.1 – privado identificando o *host* e informando em qual rede ele está.

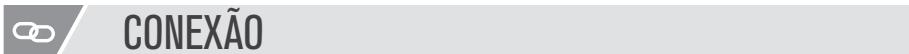
Na máscara de sub rede – 255.255.255.0 – máscara-padrão da classe C que permite determinar que a rede é a 192.160.1.0.

No *Gateway*-padrão: 192.168.1.1 que, no caso, é o IP do modem ADSL da rede.

No Servidor DNS – 192.168.1.1 – é também o modem ADSL da rede.

Estas configurações podem ser feitas manualmente, **IP Fixo**, ou dinamicamente obtendo uma **configuração automática** via **DHCP**.

Observe na figura 6.11 que, neste caso, está habilitado o DHCP e a configuração automática.



Veja como configurar um IP fixo ou automático no Windows, assistindo ao vídeo:

<<https://www.youtube.com/watch?v=XGopVLAEQLY>>.

6.4.1 DHCP - Dynamic Host Configuration Protocol (Protocolo de Configuração Dinâmica de Host)

Em redes locais maiores ou em lugares onde a população de usuários muda frequentemente, o DHCP é preferível à configuração manual, já que novos usuários podem chegar com computadores móveis ou smartphones e se autoconfigurarem sem necessidade de intervenção humana.

Os endereços distribuídos pelo DHCP não são atribuídos permanentemente aos *hosts*, pois existe a possibilidade de o servidor retirar de um pool um endereço disponível e "aluga-o por certo tempo" ao *host* (veja na figura 6.11 que constam o dia e a hora da expiração de concessão).

Se o *host* for desativado ou removido da rede, o endereço volta ao pool para reutilização. Isso é especialmente útil com usuários móveis que vêm e vão em uma rede. Os usuários podem se mover livremente de local a local e restabelecer conexões de rede. O *host* pode obter um endereço IP quando a conexão ao *hardware* for feita, via LAN, com ou sem fio.

Em redes SOHO, o servidor DHCP da LAN normalmente fica localizado no Modem ADSL ou no *cable modem*. Já a interface WAN do modem recebe do ISP uma configuração automática, também via DHCP, com as informações necessárias para acessar a Internet (figura 6.12).

O endereço dinâmico e o estático têm seu lugar no projeto de redes. Muitas redes utilizam DHCP e endereçamento estático. O DHCP é utilizado para *hosts* de finalidade geral como dispositivos de usuário final e endereços fixos são usados para dispositivos de rede, como *gateways*, *switches*, servidores e impressoras.

Sem o DHCP, os usuários devem inserir o endereço IP, máscara de sub-rede e outras configurações de rede manualmente para entrar na rede. O servidor DHCP mantém um *pool* de endereços IP e aluga um endereço a qualquer cliente habilitado por DHCP quando o cliente é ativado. Como os endereços IP são dinâmicos (alugados) em vez de estáticos (atribuídos permanentemente), os endereços em desuso são automaticamente retornados ao *pool* para realocação.

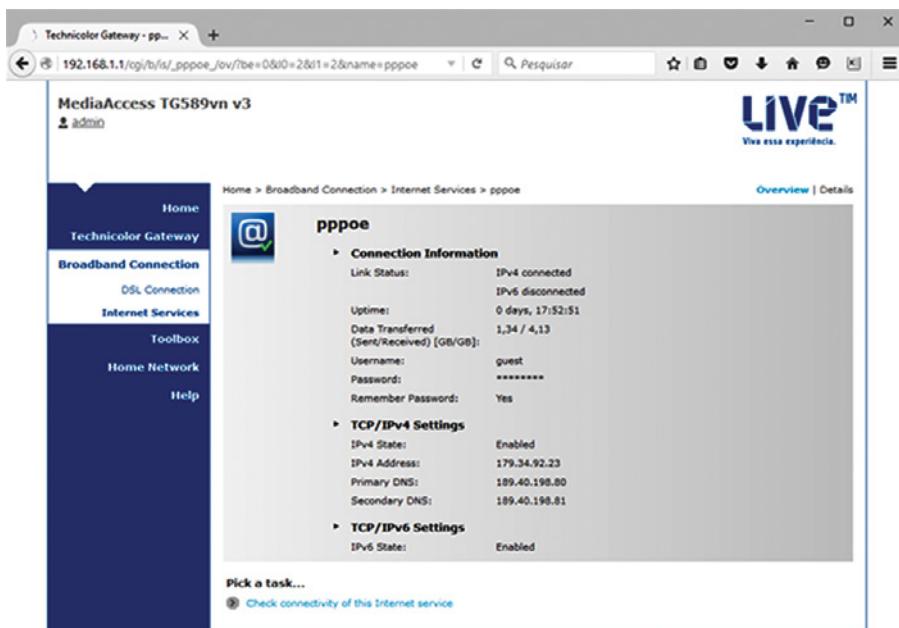


Figura 6.12 – Configuração do modem ADSL. Fonte: elaborado pelo autor.

Funcionamento DHCP

1. Quando um dispositivo com o DHCP *Client* configurado se inicializa ou se conecta à rede, o cliente transmite um pacote DHCP *Discover* (DescobertaDHCP) para identificar qualquer servidor DHCP disponível na rede.
2. Um servidor DHCP responde com um DHCP *Offer* (Oferta DHCP), que é uma mensagem de oferta de aluguel com informações do endereço IP atribuído, máscara de sub-rede, servidor DNS e *gateway*-padrão, além da duração do aluguel.
3. O cliente pode receber diversos pacotes DHCP *Offer* se houver mais de um servidor DHCP na rede local. Assim, ele deve escolher um entre eles e transmitir um pacote DHCP *Request* (Solicitação DHCP) que identifique o servidor explícito e a oferta de aluguel que o cliente está aceitando.

4. Presumindo que o endereço IP solicitado pelo cliente ou oferecido pelo servidor ainda seja válido, o servidor retornará uma mensagem DHCP *Ack* (Reconhecimento DHCP) que confirma ao cliente que o aluguel foi finalizado. Se a oferta não for mais válida, talvez devido ao encerramento ou à alocação do aluguel por outro cliente, o servidor selecionado responderá com uma mensagem DHCP *Nak* (*Negative acknowledgement* - confirmação negativa). Se uma mensagem DHCP *Nak* for retornada, o processo de seleção deverá recomeçar com uma nova mensagem DHCP *Discover* sendo transmitida.

Obs.: Quando o cliente tiver o aluguel, este deverá ser renovado antes do vencimento por outra mensagem DHCP *Request*.

O servidor DHCP garante que todos os endereços IP sejam exclusivos (um endereço IP não pode ser atribuído a dois dispositivos de rede diferentes simultaneamente). Utilizar o DHCP permite que os administradores de rede facilmente reconfigurem endereços IP de clientes sem ter que fazer manualmente alterações nos clientes. A maioria dos provedores de Internet utiliza o DHCP para alocar endereços a seus clientes que não precisam de endereço estático

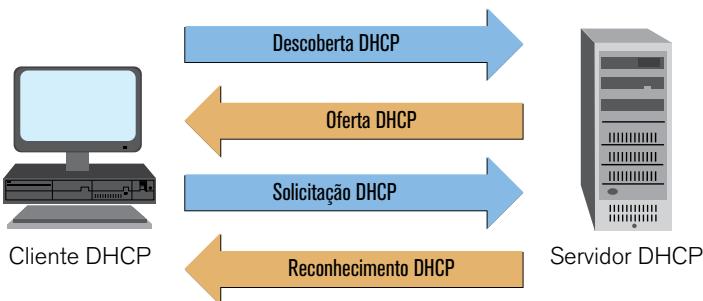


Figura 6.13 – Funcionamento DHCP. Fonte: elaborado pelo autor.

CONEXÃO

Assista ao vídeo do link e aprenda a configurar o DHCP em um modem/roteador:
<https://www.youtube.com/watch?v=MR4DR6e0bIE>.

6.5 NAT

Não há endereços IPv4 públicos o suficiente para designar um endereço exclusivo para cada dispositivo conectado à Internet. As redes são executadas geralmente com endereços IPv4 privados.

Esses endereços privados são usados em uma organização ou em um local para permitir que os dispositivos se comuniquem localmente, entretanto os endereços IPv4 privados não podem ser roteados pela Internet. Para permitir que um dispositivo com IPv4 privado acesse dispositivos e recursos de fora da rede local, o endereço privado deve primeiro ser convertido em endereço público.

O NAT fornece a conversão de endereços privados para endereços públicos. Isso permite a um dispositivo com endereço IPv4 privado acessar recursos fora de sua rede local, como aqueles encontrados na Internet. O NAT combinado com o endereço IPv4 privado provou ser um método útil de preservar endereços IPv4 públicos. Um único IPv4 público pode ser compartilhado por centenas e até mesmo por milhares de dispositivos, cada um configurado com um IPv4 privado original.

Os roteadores ativados para NAT podem ser configurados com um ou mais endereços IPv4 públicos válidos. Esses endereços públicos são conhecidos como o pool de NATs. Quando um dispositivo interno enviar o tráfego fora da rede, o roteador ativado para NAT converterá o IPv4 interno do dispositivo para um endereço público do *pool* de NATs. Para dispositivos externos, todo o tráfego que entra e sai da rede parece ter um endereço IPv4 público do *pool* de endereços fornecido.

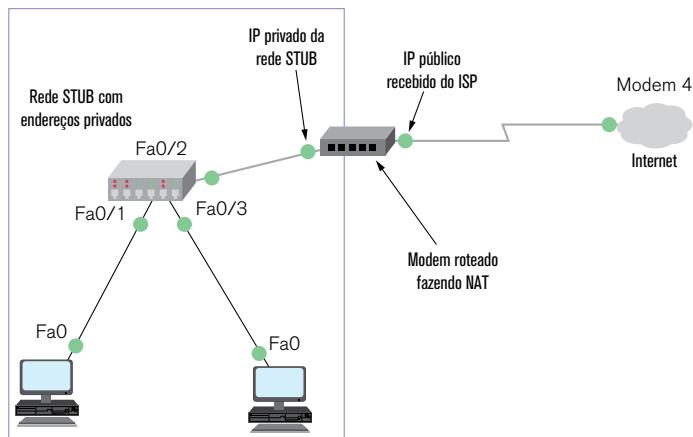


Figura 6.14 – Modem rateado fazendo NAT. Fonte: elaborado pelo autor.

Quando um dispositivo da rede local quer se comunicar com um dispositivo fora de sua rede, o pacote é encaminhado para o roteador que realiza o processo de NAT, convertendo o endereço privado interno do dispositivo em endereço público, externo e roteável.

Com a utilização do NAT, os endereços IPv4 têm designações diferentes, dependendo de sua localização na rede privada ou na rede pública (Internet) e se o tráfego é de entrada ou saída.

O NAT inclui quatro tipos de endereço:

- Endereço local interno
- Endereço global interno
- Endereço local externo
- Endereço global externo

Na determinação do tipo de endereço usado, é importante lembrar que a terminologia NAT é sempre aplicada sob a perspectiva do dispositivo com o endereço convertido:

- **Endereço interno:** o endereço do dispositivo convertido pelo NAT.
- **Endereço externo:** o endereço do dispositivo destino

O NAT também usa o conceito de local ou global com relação aos endereços:

- **Endereço local:** endereço local é qualquer endereço que aparece na parte interna da rede.
- **Endereço global:** endereço global é qualquer endereço que aparece na parte externa da rede.

Observe a figura 6.15.

Considere que PC1(IP 192.168.10.1) deseja acessar o servidor Web (IP 220.30.510.10)

No pacote que sai de PC1 em direção ao modem/roteador, temos o seguinte:

Endereço de origem 192.168.10.1 Endereço interno local	Endereço de destino 220.30.50.10 Endereço externo local
--	---

No pacote que sai do modem/roteador para a Internet, temos:

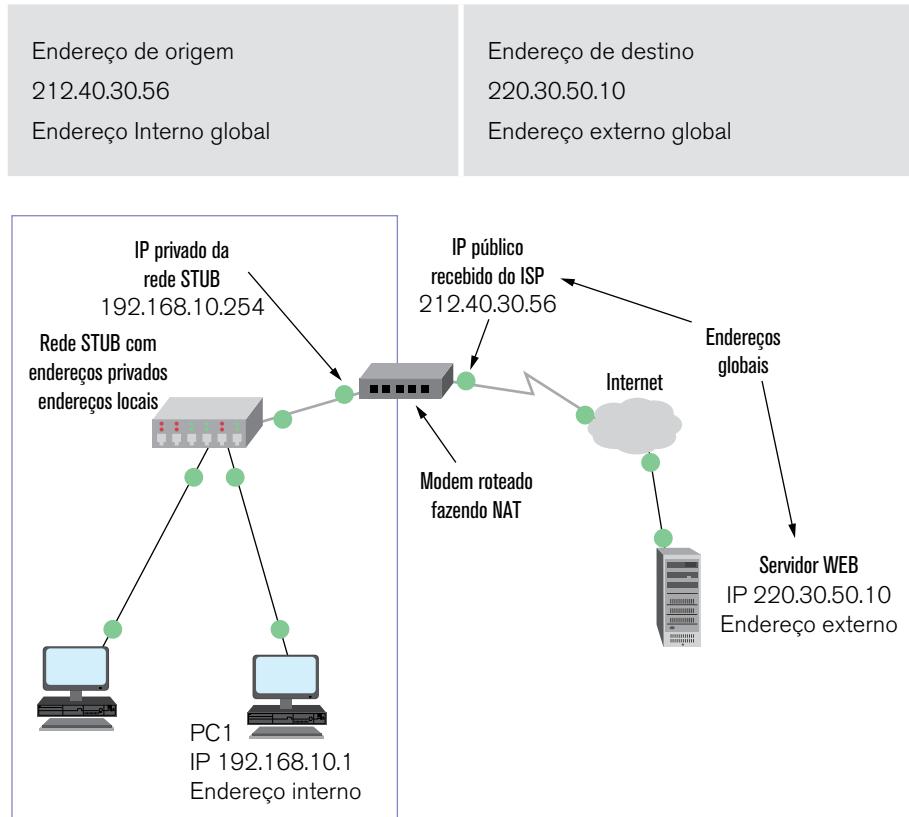


Figura 6.15 – Tipos de endereço NAT. Fonte: elaborado pelo autor.

A *port address translation* (PAT), também conhecida como sobrecarga do NAT ou NAPT (*network address and port translation*), mapeia os endereços IPv4 privados para um único endereço IPv4 público ou alguns endereços. Isso é o que a maioria dos roteadores residenciais fazem. O ISP atribui um endereço ao roteador, porém vários membros da casa podem acessar simultaneamente a Internet. Esta é a forma mais comum de NAT.

Com o PAT, vários endereços podem ser mapeados para um ou mais endereços, pois cada endereço privado é também seguido de um número de porta. Quando um dispositivo inicia uma sessão TCP/IP, ele gera valor de uma porta origem TCP ou UDP para identificar excepcionalmente a sessão. Quando o

roteador de NAT recebe um pacote do cliente, usa seu número de porta origem para identificar excepcionalmente a conversão do NAT específico.

O PAT garante que os dispositivos utilizem um número de porta diferente do TCP para cada sessão com um servidor na Internet. Quando uma resposta volta do servidor, o número de porta origem, que se torna o número de porta destino na viagem de ida e volta, determina os dispositivos para os quais o roteador deverá encaminhar os pacotes. O processo de PAT também valida que os pacotes de entrada tenham sido solicitados, adicionando, portanto, um nível de segurança à sessão.

O PAT usa números de portas origem exclusivos no endereço IP global interno para distinguir essas conversões.

Comparação de NAT e PAT

Resumir as diferenças entre NAT e PAT ajuda você a entender cada um deles.

- O NAT converte os endereços IPv4 em uma base de 1:1 entre os endereços IPv4 privados e os endereços IPv4 públicos, entretanto o PAT modifica o endereço e o número de porta.

- O NAT encaminha os pacotes de entrada para seu destino interno fazendo referência à origem de entrada do endereço IPv4 fornecido pelo *host* na rede pública. Com o PAT, há normalmente apenas um ou poucos endereços IPv4 publicamente expostos. Os pacotes que chegam à rede pública são roteados para os destinos da rede privada com referência a uma tabela no roteador de NAT. Esta tabela rastreia os pares de portas públicos e privados. Isso é chamado de rastreamento de conexão.

Encaminhamento de portas

O encaminhamento de portas (às vezes chamado túnel) é o ato de encaminhar uma porta de rede de um nó de rede para outro. Essa técnica permite que um usuário externo acesse uma porta no endereço IPv4 privado (dentro de uma LAN) externo, com um roteador ativado para NAT.

Normalmente, os programas de compartilhamento de arquivos de ponto a ponto, como o serviço da Web e FTP de saída, exigem que as portas do roteador sejam encaminhadas ou abertas para permitir que esses aplicativos funcionem, como mostrado na figura 1. Como o NAT oculta os endereços internos, o ponto a ponto funcionará somente de dentro para fora, onde o NAT poderá mapear solicitações contra respostas de entrada.

O problema é que o NAT não permite solicitações iniciadas externamente. Essa situação pode ser resolvida com intervenção manual. O encaminhamento de portas pode ser configurado para identificar as portas específicas que podem ser encaminhadas aos *hosts* internos.

Lembre-se de que os aplicativos de *software* da Internet interagem com as portas de usuários que precisam estar abertas ou disponíveis para esses aplicativos. Diferentes aplicativos usam diferentes portas. Isso torna previsível para aplicativos e para roteadores a identificação de serviços de rede, por exemplo, HTTP opera através da conhecida porta 80.

Se um número de porta diferente for necessário, ele poderá ser adicionado ao URL separado por dois-pontos (:), por exemplo, se o servidor Web aguardar na porta 8080, o usuário digitará <http://www.example.com:8080>.

O encaminhamento de portas permite que os usuários na Internet acessem servidores internos usando o endereço de porta WAN do roteador e do número da porta externa correspondente. Os servidores internos são normalmente configurados com endereços IPv4 privados de RFC 1918. Quando uma solicitação é enviada ao endereço IPv4 da porta WAN via Internet, o roteador encaminha a solicitação ao servidor adequado na LAN. Por motivo de segurança, os roteadores de banda larga não permitem por padrão o encaminhamento de nenhuma solicitação externa de rede para um *host* interno.



CONEXÃO

Para aprender a abrir portas em um modem/roteador, assista ao vídeo:
[<https://www.youtube.com/watch?v=Cgx5fJsmXP0>](https://www.youtube.com/watch?v=Cgx5fJsmXP0).

6.6 VPN

Virtual private network ou rede privada virtual é uma rede privada construída sobre a infraestrutura de uma rede pública, normalmente a Internet.

A utilização da Internet como infraestrutura de conexão entre *hosts* da rede privada barateia os custos, já que não será necessário contratar *links* dedicados, mas tem como desvantagem comprometer a privacidade e segurança dos

dados trafegados, pois, sendo a Internet uma rede pública, os dados em trânsito podem ser lidos por qualquer equipamento.

Para resolver esta situação, utiliza-se a criptografia.

Ao incorporar a criptografia na comunicação entre *hosts* da rede privada, se os dados forem capturados durante a transmissão não terão utilidade para o invasor. Os túneis virtuais habilitam o tráfego de dados criptografados pela Internet e esses dispositivos são capazes de entender os dados criptografados, formando uma rede virtual segura sobre a rede Internet.

Basicamente, uma VPN pode ser feita de duas formas:

A primeira forma é um simples *host* em trânsito que se conecta a provedor Internet e, por meio dessa conexão, estabelece um túnel com a rede remota. A figura 6.14 demonstra essa forma.

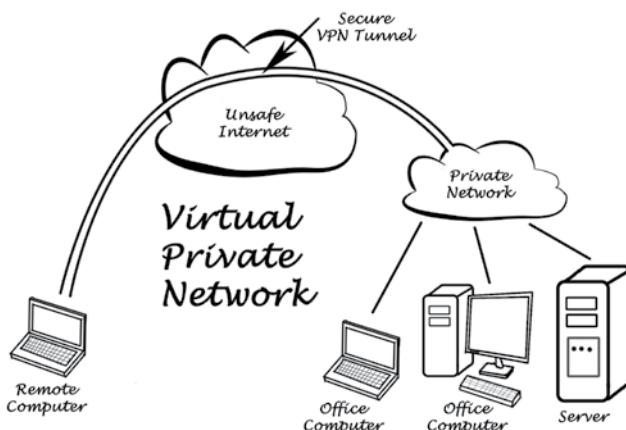


Figura 6.16 – Túnel VPN.

Na segunda forma, duas redes se interligam por *hosts* com *link* dedicado ou discado via Internet, formando assim um túnel entre as duas redes.

Os protocolos utilizados no túnel virtual são (IPSec) *Internet protocol security*, (L2TP) *layer 2 tunneling protocol*, (L2F) *layer 2 forwarding* e o (PPTP) *point-to-point tunneling protocol*. O protocolo escolhido será o responsável pela conexão e pela criptografia entre os *hosts* da rede privada. Eles podem ser normalmente habilitados por um servidor *Firewall* ou RAS que esteja trabalhando agregado com um deles.



ATIVIDADE

Acesse os seguintes sites.

Para aprender soluções de redes domésticas e equipamentos de acesso de banda larga :
<<http://www.abusar.org.br/>>.

Responda às questões on-line de redes:

<<https://www.qconcursos.com/questoes-de-concursos/disciplinas/tecnologia-da-informacao-redes-de-computadores>>.

<<https://www.aprovaconcursos.com.br/questoes-de-concurso/disciplina/redes-de-computadores>>.

<<https://www.gabaritou.com.br/Questao?DisciplinalD=11>>.

Explore os recursos on-line:

<http://wps.aw.com/br_kurose_redes_3/40/10271/2629589.cw/index.html>.

Animações do livro de Forouzan

Disponível em:

<http://highered.mheducation.com/sites/0072967722/student_view0/animations.html#>.



REFLEXÃO

Neste capítulo, conhecemos as principais soluções cabeadas para redes SOHO. No próximo capítulo, conheceremos as redes sem fio.



LEITURA

Leia o capítulos 13 do livro *Comunicação de dados e redes de computadores*, de Behrouz A. Forouzan.

Saiba mais

Assista aos vídeos abaixo:

Disponível em: <<https://www.youtube.com/watch?v=a6CCxIKseus>>.

Disponível em: <<https://www.youtube.com/watch?v=TlJqLyPmEFs>>.

Disponível em: <https://www.youtube.com/watch?v=OPBcD_d4ejo>.

Disponível em: <<https://www.youtube.com/watch?v=jAzFwfK3hF8>>.

Disponível em: <<https://www.youtube.com/watch?v=Bs3Hx1z0qrA>>.

Disponível em: <https://www.youtube.com/watch?v=cdmkq8pQx_g>.



REFERÊNCIAS BIBLIOGRÁFICAS

FOROUZAN, Behrouz A. *Comunicação de dados e redes de computadores*. 4. ed. São Paulo: McGraw-Hill, 2008.

KUROSE, James F. e ROSS, Keith W. *Redes de computadores e a Internet: uma abordagem top-down*. 4. ed. São Paulo: Addison Wesley, 2009.

Tanenbaum, Andrew S. *Redes de computadores*. 5. ed. Rio de Janeiro: Campus, 2007.

7

Redes Sem Fio

As redes sem fio e os serviços móveis relacionados que elas possibilitam vieram para ficar. Do ponto de vista de rede, os desafios propostos por essas redes, particularmente nas camadas de enlace e de rede, são diferentes dos desafios de redes de computadores cabeadas.

Neste capítulo, iremos ver os usuários móveis, os enlaces e as redes sem fio e sua relação com as redes maiores (normalmente cabeadas) às quais se conectam. Veremos ainda aspectos ligados à segurança de redes sem fio e o protocolo CSMA/CA.



OBJETIVOS

- Descrever o funcionamento de uma rede sem fio.
 - Identificar os componentes de uma rede sem fio.
 - Implementar segurança em uma rede sem fio.
-

7.1 Redes sem fio

Quando falamos de redes sem fio, pensamos logo em mobilidade, existem porém muitos ambientes de redes nos quais os nós da rede são sem fio, mas não móveis (por exemplo, redes residências sem fio ou redes de escritórios onde se desejou evitar o custo da instalação do cabeamento).

A figura 7.1 mostra o cenário no qual consideraremos os tópicos de comunicação de dados e mobilidade sem fio.

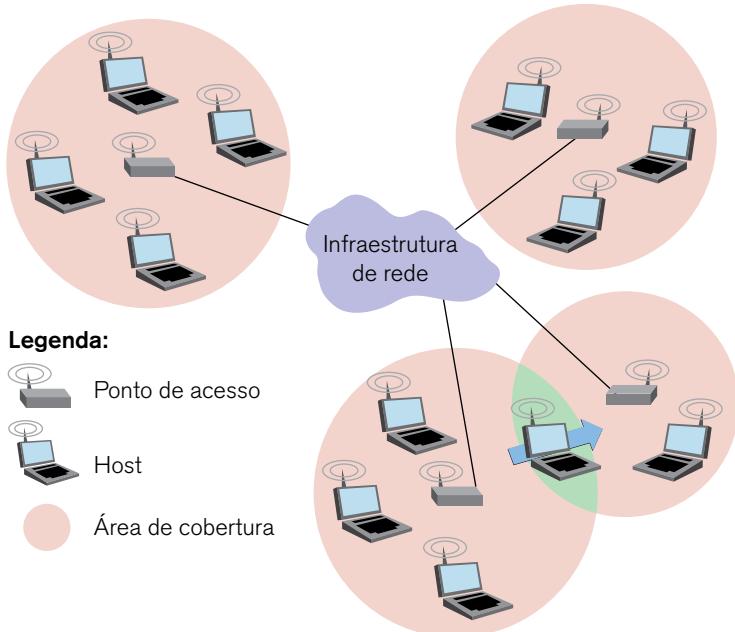


Figura 7.1 – Elementos de uma rede sem fio. Kurose 2009. Adaptado.

Podemos identificar os seguintes elementos em uma rede sem fio:

Host sem fio: como no caso de redes cabeadas (ou com fio), são os sistemas finais que executam aplicações. Um *host* sem fio pode ser um laptop, um palmtop, um PDA, um smartphone ou um computador de mesa.

Enlaces sem fio: são a ligação entre os *hosts* e um ponto de acesso. Diferentes tecnologias de enlace sem fio possuem taxas de transmissão distintas, bem como área de cobertura de tamanhos diferentes.

Ponto de acesso (Access point): É parte fundamental de uma rede sem fio. Ele é responsável pelo envio e recebimento de dados (por exemplo, pacotes) de

e para hosts sem fio que estão associados com ele. Um ponto de acesso será responsável pela coordenação da transmissão de vários *hosts* sem fio com os quais está associado.



ATENÇÃO

Um *host* sem fio está associado a um ponto de acesso, quando está dentro do alcance de comunicação sem fio do ponto de acesso e utiliza-o para retransmitir dados entre ele e o restante da rede.

Na figura 7.1, o ponto de acesso está conectado à rede maior (isto é, a Internet, à rede empresarial e residencial ou à rede telefônica), portanto funciona como uma retransmissora de camada de enlace entre o *host* sem fio e o resto do mundo.

Infraestrutura de rede: é a rede maior com a qual um *host* sem fio pode querer se comunicar. Repare que, na figura 7.1, os pontos de acesso se ligam à infraestrutura de rede via cabo.

7.2 Características de enlace sem fio

Imagine uma rede residencial cabeada na topologia estrela com um *switch* central. Se, ao invés do *switch*, tivéssemos um ponto de acesso ocorreriam mudanças nas camadas 1 e 2 como substituição da placa de rede e mudança no método de acesso ao meio, mas, na camada de rede ou acima dela, praticamente nenhuma mudança seria necessária. Podemos observar então que é nas camadas inferiores que devemos procurar as principais diferenças entre redes com fio e sem fio, dentre as quais temos:

- **Redução da força do sinal:** radiações eletromagnéticas são atenuadas quando atravessam algum tipo de matéria (por exemplo, um sinal de rádio ao atravessar uma parede). O sinal se dispersará mesmo ao ar livre, resultando na redução de sua força (às vezes denominada atenuação de percurso) à medida que aumenta a distância entre emissor e receptor.

- **Interferência de outras fontes:** várias fontes de rádio transmitindo na mesma banda de frequência sofrerão interferênciaumas das outras, por exemplo, telefones sem fio de 2,4 GHz e LANs sem fio 802.11 transmitem na mesma banda de frequência. Assim, o usuário de uma LAN sem fio 802.11b que estiver se comunicando por um telefone sem fio de 2,4 GHz pode esperar que nem a rede nem o telefone funcionem particularmente bem. Além da interferência de fontes transmissoras, o ruído eletromagnético presente no ambiente (por exemplo, um motor ou um equipamento de micro-ondas próximo) pode causar interferência.

- **Propagação multivias:** A propagação multivias (ou multicaminhos) ocorre quando partes da onda eletromagnética se refletem em objetos e no solo e tomam caminhos de comprimentos diferentes entre um emissor e um receptor. Isso resulta no embaralhamento do sinal recebido no destinatário. Objetos que se movimentam entre o emissor e o receptor podem fazer com que a propagação multivias mude ao longo do tempo.

As características anteriores indicam que erros de bit serão mais comuns em enlaces sem fio do que em enlaces com fio. Por essa razão, talvez não seja nenhuma surpresa que protocolos de enlace sem fio, como o protocolo 802.11, empreguem não só poderosos códigos de detecção de erros por CRC, mas também protocolos de transferência de dados confiável em nível de enlace, que retransmitem quadros corrompidos.

7.3 WI-FI: LANS sem fio 802.11

LAN sem fio IEEE 802.11, também conhecida como Wi-Fi, possui diversos padrões dentre os quais 802.11b, 802.11a e 802.11g. A tabela 7.1 apresenta um resumo das principais características desses padrões. 802.11g é, de longe, a tecnologia mais popular. Estão também disponíveis diversos mecanismos de modo duplo (802.11a/g) e de modo triplo (802.11 a/b/g).

Todos os padrões apresentados possuem as seguintes características:

- Utilizam CSMA/CA como protocolo de acesso ao meio.
- Usam quadro de camada de enlace.
- Reduzem sua taxa de transmissão para alcançar distâncias maiores.

Conforme mostra a tabela 7.1, eles, contudo, apresentam algumas diferenças importantes na camada física.

PADRÃO	FAIXA DE FREQUÊNCIA (EUA)	TAXA DE DADOS
802.11 b	2,4 - 2,485 GHz	até 11 Mbits/s
802.11 a	5,1 - 5,8 GHz	até 54 Mbits/s
802.11 g	2,4 - 2,485 GHz	até 54 Mbits/s

Tabela 7.1 – Resumo dos padrões IEEE 802.11. Kurose 2009.

O padrão 802.11n, mais recente, utiliza antenas de entrada múltipla e saída múltipla (mimo), ou seja, duas ou mais antenas no lado remetente e duas ou mais antenas no lado destinatário que estão transmitindo/recebendo sinais diferentes. Esta tecnologia pode alcançar taxas de transmissão de centenas de megabits por segundo.

7.4 Arquitetura 802.11

Observe a figura 7.2. Ela mostra os componentes da arquitetura de LAN sem fio 802.11 que tem como elemento básico o conjunto básico de serviço (*basic service set* - BSS). Um BSS contém um ou mais *hosts* sem fio e um ponto de acesso (*access point* - AP).

Repare que existe um AP em cada um dos dois BSSs conectando-se a um dispositivo de interconexão (tal como um comutador ou um roteador), que, por sua vez, leva-o à Internet.

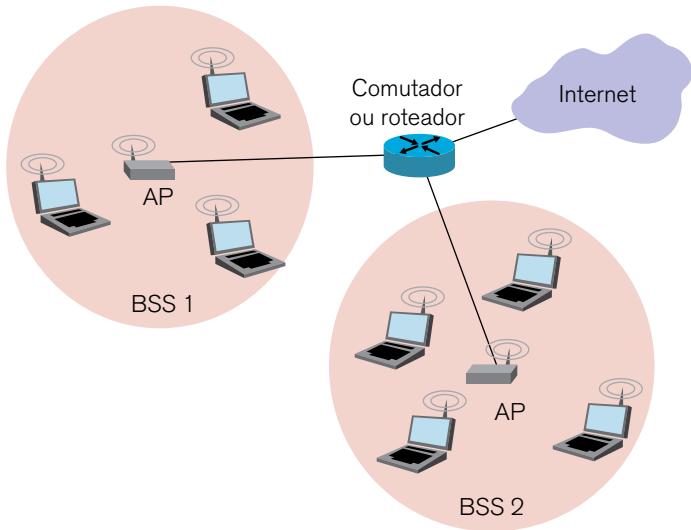


Figura 7.2 – Arquitetura de LAN IEEE 802.11. Kurose 2009.

Em uma rede residencial típica, há apenas um AP e um roteador (normalmente integrados como uma unidade, como em um modem ADSL) que conecta o BSS à Internet. (figura 7.3).



Figura 7.3 – Roteador sem fio.

Seguindo o padrão da Ethernet, tanto as estações sem fio 802.11 como o AP possuem um endereço MAC de 6 bytes, armazenado no *firmware* da placa de rede sem fio, sendo, em teoria, globalmente exclusivos.

LANs sem fio que disponibilizam APs em geral são denominadas LANs sem fio de infraestrutura e, nesse contexto, "infraestrutura" significa os APs junto com a infraestrutura de Ethernet cabeada que interconecta os APs e um roteador.

A figura 7.4 mostra que estações IEEE 802.11 também podem se agrupar e formar uma rede *ad hoc* - rede sem nenhum controle central e sem nenhuma conexão com o "mundo exterior". Nesse caso, a rede é formada, conforme a necessidade, por dispositivos móveis que, por acaso, estão próximos uns dos outros, têm necessidade de se comunicar e não dispõem de infraestrutura de rede no lugar em que se encontram.

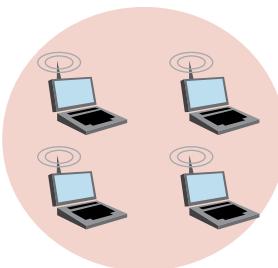


Figura 7.4 – Rede *ad hoc* IEEE 802.11. Kurose, 2009.

7.5 Associação

Em 802.11, cada estação sem fio precisa se associar com um AP antes de poder enviar ou receber dados da camada de rede.

Ao instalar um AP, um administrador de rede designa ao ponto de acesso um identificador de conjunto de serviços (*service set identifier* - SSID) composto de uma ou duas palavras. (O comando "veja redes disponíveis" no Microsoft Windows, por exemplo, apresenta uma lista que mostra o SSID de todos os APs ordenado por faixa.)

O AP envia periodicamente quadros com a informação de seu SSID e seu endereço MAC. Uma estação sem fio busca estes quadros e, ao tomar conhecimento do AP, busca se associar a ele. Para tal, envia um quadro de solicitação de associação ao AP e este responde com um quadro de resposta de associação.

Para criar uma associação com um determinado AP, a estação sem fio talvez tenha de se autenticar perante o AP: LANs sem fio 802.11 dispõem de várias alternativas para autenticação e acesso. Uma abordagem usada por muitas empresas é permitir o acesso a uma rede sem fio com base no endereço MAC de uma estação. Uma segunda abordagem, usada por muitos cafés Internet, emprega nomes de usuários e senhas.

7.6 O protocolo MAC 802.11

Após realizada a associação ao AP, o *host*pode começar a enviar e a receber quadros de dados de e para o ponto de acesso, porém, como várias estações podem querer transmitir quadros de dados ao mesmo tempo, é preciso um protocolo de acesso múltiplo para coordenar as transmissões.

O protocolo tipicamente utilizado é o CSMA com prevenção de colisão ou, mais sucintamente, CSMA/CA. De forma similar ao CSMA/CD da Ethernet, estudado no capítulo 3, "CSMA" de CSMA/CA quer dizer "acesso múltiplo por detecção de portadora", o que significa que cada estação sonda o canal antes de transmitir e abstém-se de transmitir quando percebe que o canal está ocupado.

Embora tanto a Ethernet quanto o 802.11 usem acesso por detecção de portadora, os dois protocolos MAC apresentam diferenças importantes. Primeiro, em vez de usar detecção de colisão, o 802.11 usa técnicas de prevenção de colisão. Segundo, por causa das taxas relativamente altas de erros de bits em canais sem fio, o 802.11. (ao contrário da Ethernet) usa um esquema de reconhecimento/retransmissão que utiliza **ARQ** de camada de enlace.



CONCEITO

Automatic Repeat Request (ARQ) é um método para controle de erros em transmissão de dados que utiliza reconhecimento positivo (*acknowledgements* ou *ack*), que se constitui no envio ao transmissor de uma mensagem informando que o quadro foi recebido corretamente. Se o transmissor não receber o *ack* dentro de um determinado limite de tempo, ele retransmite o quadro.

7.7 Prevenção de colisão

Ao contrário do protocolo Ethernet 802.3, o padrão 802.11 não implementa detecção de colisão. Em consequência, quando uma estação começa a transmitir um quadro, ela o transmite integralmente, isto é, tão logo uma estação inicie, não há volta. É claro que transmitir quadros inteiros (em particular os longos), quando existe grande possibilidade de colisão, pode degradar significativamente o desempenho de um protocolo de acesso múltiplo. Para reduzir a probabilidade de colisões, o 802.11 emprega diversas técnicas de prevenção de colisão.

Funcionamento CSMA/CA

Suponha que uma estação (pode ser uma estação sem fio ou um AP) tenha um quadro para transmitir.

1. Se, inicialmente, a estação perceber que o canal está ocioso, ela transmitirá seu quadro após um curto período de tempo conhecido como espaçamento interquadros distribuído (distributed inter-frame space - DIFS), conforme figura 7.5.
2. Caso contrário, a estação escolherá um valor aleatório de recuo, usando o recuo exponencial binário, e fará a contagem regressiva a partir desse valor quando perceber que o canal está ocioso. Se a estação perceber que o canal está ocupado, o valor do contador permanecerá congelado.
3. Quando o contador chegar a zero (note que isso pode ocorrer somente quando a estação percebe que o canal está ocioso), a estação transmitirá o quadro inteiro e, então, ficará esperando o reconhecimento.
4. Se receber o reconhecimento, a estação transmissora saberá que o quadro foi corretamente recebido na estação de destino. Se a estação tiver outro quadro para transmitir, iniciará o protocolo CSMA/CA na etapa 2. Se não receber o reconhecimento, a estação entrará de novo na fase de recuo na etapa 2 e escolherá um valor aleatório em um intervalo maior.

Note que, ao contrário do CSMA/CD, onde uma estação começa a transmitir tão logo percebe que o canal está ocioso, no CSMA/CA a estação realiza a contagem regressiva e só transmite quando esta termina, mesmo quando percebe que o canal está ocioso.

Por que o CSMA/CD e o CSMA/CA adotam essas abordagens diferentes aqui?

Para responder a essa pergunta, vamos considerar um cenário com duas estações em que cada uma tem um quadro a transmitir, mas nenhuma o transmite imediatamente porque percebe que uma terceira estação já está transmitindo. Com o CSMA/CD da Ethernet, cada uma das duas estações transmitiria o quadro tão logo detectasse que a terceira estação terminou de transmiti-lo, o que causaria uma colisão, que não é um problema sério em CSMA/CD, já que ambas as estações abortariam suas transmissões e, assim, evitariam a transmissão inútil do restante dos seus quadros. Com 802.11, a situação é bem diferente. Como o 802.11 não detecta uma colisão nem aborta transmissão, um quadro que sofra uma colisão será transmitido integralmente. Assim, a meta do 802.11 é evitar colisões sempre que possível. Com esse protocolo, se duas estações perceberem que o canal está ocupado, ambas entrarão imediatamente em **backoff** aleatório e, esperamos, escolherão valores diferentes de retardo. Se esses valores forem, de fato, diferentes, assim que o canal ficar ocioso, uma das duas começará a transmitir antes da outra e a "estação perdedora" ouvirá o sinal da "estação vencedora", interromperá seu contador e não transmitirá até que a estação vencedora tenha concluído sua transmissão. Desse modo, é evitada uma colisão dispendiosa.



CONCEITO

Backoff: Refere-se ao tempo que um dispositivo de transmissão de dados aguarda para realizar uma nova transmissão, após a ocorrência de um problema na primeira tentativa.

7.8 Reconhecimento/Retransmissão (ARQ)

Como em um LAN sem fio, devido à utilização de ondas de rádio, a probabilidade de ocorrer um erro é grande, o protocolo MAC 802.11 usa reconhecimentos de camada de enlace, como ilustrado na figura 7.5.

Quando o quadro chega ao destino, a estação verifica se houve erro utilizando o CRC. Se tudo estiver correto, ela irá esperar um curto período de tempo, conhecido como espaçamento curto interquadros (*short inter-frame spacing - SIFS*) e, então, devolverá um quadro de reconhecimento.

Se a estação transmissora não receber um reconhecimento em dado período de tempo, ela admitirá que ocorreu um erro e retransmitirá o quadro usando de novo o protocolo CSMA/CA para acessar o canal. Se a estação transmissora não receber um reconhecimento após certo número fixo de retransmissões, desistirá e descartará o quadro.

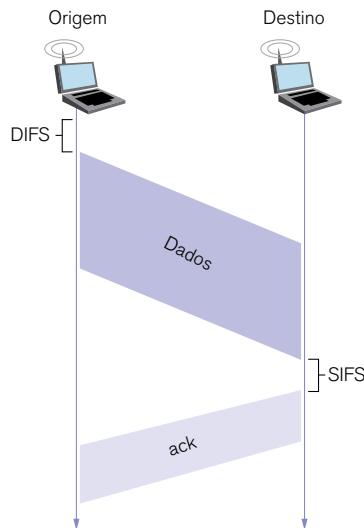
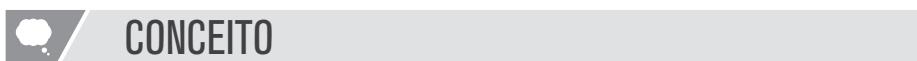


Figura 7.5 – Reconhecimentos da camada de enlace. Kurose 2009.

7.9 Segurança

Algumas das medidas de segurança básicas em uma rede sem fio incluem:

- Alterar os valores padrão do SSID, o nome do usuário e as senhas-padrão do administrador do AP.
- Desativar a transmissão de SSID.
- Configurar a **criptografia** usando WEP, WPA ou WPA2 .



Criptografia é o processo de transformar dados, de modo que, se forem interceptados, eles tornem-se ininteligíveis, por isso inutilizáveis.

WEP (*wired equivalency protocol*)

O WEP criptografa os dados a serem transmitidos pela rede. Para tal, ele usa chaves pré-configuradas para criptografar e descriptografar dados.

Uma chave WEP é inserida como uma *string* de números e letras e geralmente tem 64 bits ou 128 bits, podendo em alguns casos chegar a 256 bits. Para simplificar a criação e a inserção dessas chaves, muitos dispositivos incluem uma opção de frase secreta. A frase secreta é uma maneira fácil de lembrar a palavra ou a frase usada para gerar automaticamente uma chave.

Para que o WEP funcione, o AP e as estações sem fio deverão ter a mesma chave WEP inserida. Sem essa chave, os dispositivos não poderão entender as transmissões sem fio.

Há pontos fracos no WEP, incluindo o uso de uma chave estática em todos os dispositivos habilitados para WEP. Há aplicativos disponíveis para os invasores que podem ser usados para detectar a chave WEP. Esses aplicativos estão prontamente disponíveis na Internet. Quando o invasor extrair a chave, ele terá acesso total a todas as informações transmitidas.

Uma maneira de contornar essa vulnerabilidade é alterar a senha frequentemente. Outra maneira é usar uma forma mais avançada e mais segura de criptografia conhecida como WPA (Wi-Fi *protected access*).

WPA (Wi-Fi *protected access*)

O WPA também usa chaves de criptografia de 64 bits até 256 bits. O WPA, ao contrário do WEP, gera novas chaves dinâmicas, cada vez que um cliente estabelece uma conexão com o AP. Por esse motivo, o WPA é considerado mais seguro do que o WEP, pois é significativamente mais difícil de burlar.

7.10 Configurando o roteador integrado

A maioria das redes SOHO não exige dispositivos de alto volume como roteadores e *switches* dedicados. Em relação aos dispositivos de menor escala, quanto que forneçam a mesma funcionalidade de roteamento e *switching*, eles dispensam outras necessidades. Por esse motivo, muitas redes residenciais e

de pequenas empresas utilizam o serviço de um dispositivo multifuncional, o roteador integrado (figura 7.3).

Um roteador integrado é como ter vários dispositivos diferentes conectados, por exemplo, a conexão entre o *switch* e o roteador ainda ocorre, mas internamente. Quando um pacote é encaminhado de um dispositivo para outro na mesma rede local, o *switch* integrado automaticamente encaminha-o para o dispositivo de destino. Se, no entanto, um pacote for encaminhado para um dispositivo em uma rede remota, o *switch* integrado irá encaminhá-lo para a conexão do roteador interno. Em seguida, o roteador interno determinará o melhor caminho e o encaminhará devidamente para fora.

A maioria dos roteadores integrados oferece recursos de *switching* com fio e de conectividade sem fio e atua como o ponto de acesso (AP) na rede sem fio. A conectividade sem fio é uma maneira popular, flexível e econômica para residências e empresas de fornecer serviços de rede a dispositivos finais.

Além de oferecer suporte ao roteamento, ao *switching* e à conectividade sem fio, muitos outros recursos podem estar disponíveis em um roteador integrado, incluindo o serviço DHCP, NAT, *firewall* etc (figura 7.6).

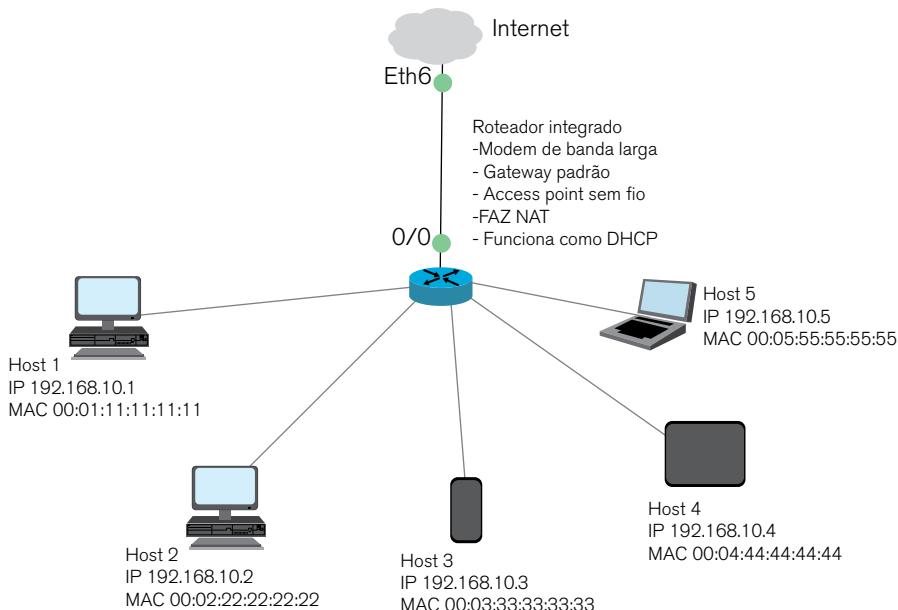


Figura 7.6 – Roteador integrado. Fonte: elaborado pelo autor.



CONEXÃO

Acesse o *link* e veja um vídeo que mostra a maneira como configurar uma rede sem fio.

Disponível em: <<http://www.tecmundo.com.br/wi-fi/1074-como-configurar-uma-rede-sem-fio-wireless-video-.htm>>.



ATIVIDADE

Acesse os *sites* e responda às questões *on-line* de redes.

Disponível em: <<https://www.qconcursos.com/questoes-de-concursos/disciplinas/tecnologia-da-informacao-redes-de-computadores>>.

Disponível em: <<https://www.aprovaconcursos.com.br/questoes-de-concurso/disciplina/redes-de-computadores>>.

Disponível em: <<https://www.gabaritou.com.br/Questao?DisciplinalID=11>>.

Acesse os *sites* e explore os recursos *on-line*.

Disponível em:

<http://wps.aw.com/br_kurose_redes_3/40/10271/2629589.cw/index.htm>.

Animações do livro de Forouzan

Disponível em: <http://highered.mheducation.com/sites/0072967722/student_view0/animations.html#>.

Para aprender soluções de redes domésticas e equipamentos de acesso, acesse:

<<http://www.abusar.org.br/>>.

Para conhecer equipamentos sem FIO cisco, acesse:

<<http://www.cisco.com/web/BR/produtos/wireless/index.html>>.



REFLEXÃO

Você viu nesta aula os fundamentos de redes sem fio.

Chegamos assim ao final de nosso livro. Espero que as informações nele contidas tenham sido bem aproveitadas.



LEITURA

Leia o capítulo 14 do livro *Comunicação de dados e redes de computadores*, de Behrouz A. Forouzan.

Saiba mais

Assista aos vídeos abaixo:

Disponível em: <<http://olhardigital.uol.com.br/video/aprenda-a-configurar-uma-rede-wi-fi-na-sua-casa/38613>>.

Disponível em: <<https://www.youtube.com/watch?v=jxnJ02x66ps>>.

Disponível em: <<https://www.youtube.com/watch?v=V4yXNivwzz4>>.

Disponível em: <<https://www.youtube.com/watch?v=VKjLHZCptLw>>.

Disponível em: <<https://www.youtube.com/watch?v=AJe2zRVkWE0>>.

Disponível em: <<https://www.youtube.com/watch?v=pe9SyXkUUl8>>.



REFERÊNCIAS BIBLIOGRÁFICAS

FOROUZAN, Behrouz A. *Comunicação de dados e redes de computadores*. 4. ed. São Paulo: McGraw-Hill, 2008.

KUROSE, James F. e ROSS, Keith W. *Redes de computadores e a Internet: uma abordagem top-down*. 4. ed. São Paulo: Addison Wesley, 2009.

Tanenbaum, Andrew S. *Redes de computadores*. 5. ed. Rio de Janeiro: Campus, 2007.



ANOTAÇÕES



ANOTAÇÕES



ANOTAÇÕES



ANOTAÇÕES