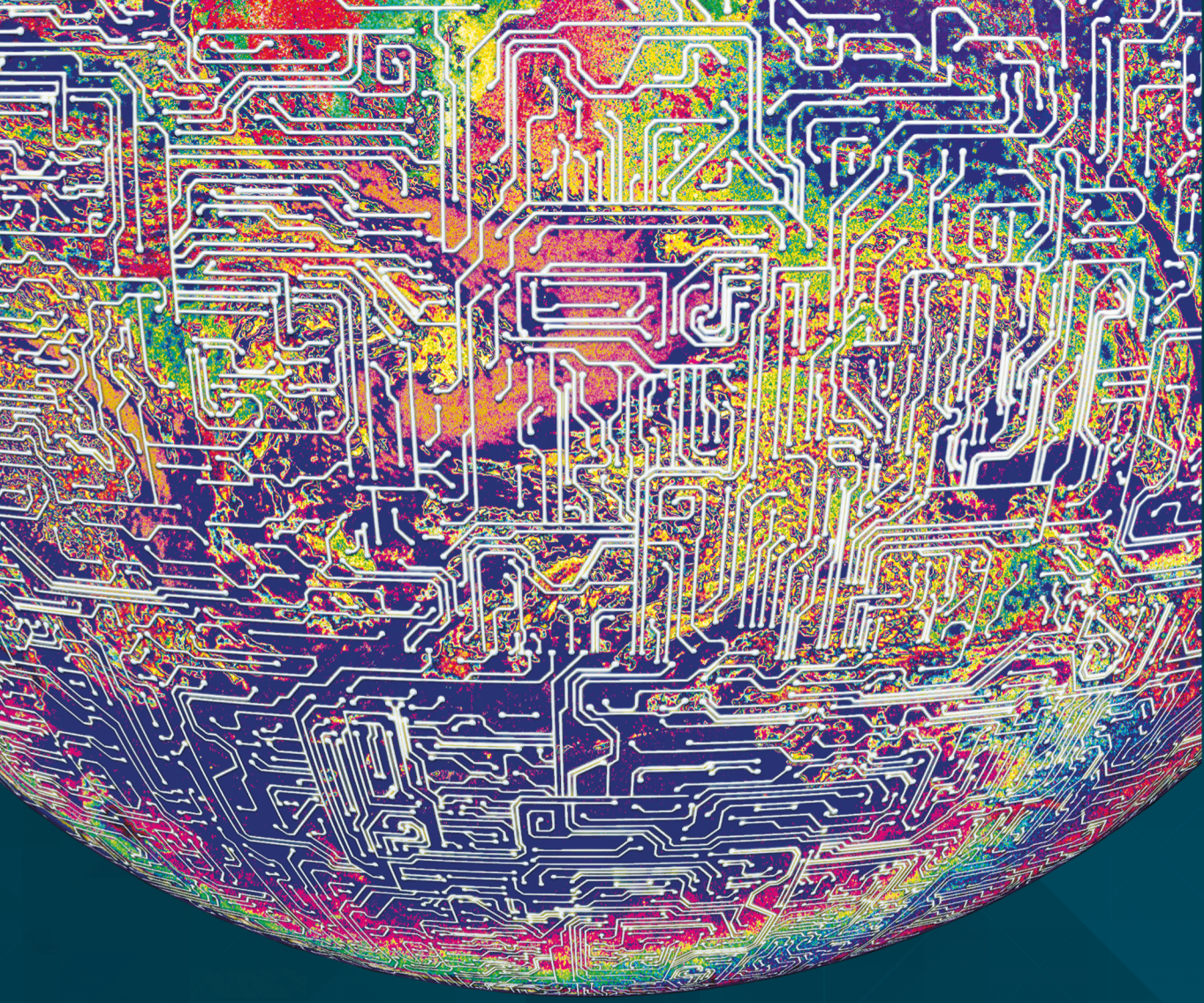

Redes Locais de Computadores

Luciano Tadeu Esteves Pansanato

Editora UTFPR

Redes Locais de Computadores

Luciano Tadeu Esteves Pansanato

Redes Locais de Computadores

Curitiba
UTFPR Editora
2016

Disponível também em: <http://repositorio.utfpr.edu.br/jspui/>.

Dados Internacionais de Catalogação na Publicação

P196 Pansanato, Luciano Tadeu Esteves
Redes locais de computadores. / Luciano Tadeu Esteves Pansanato. —Curitiba: Ed. UTFPR, 2016.
102 p. : il. ; 23 cm.
ISBN: 978-85-7014-160-6
1. Redes locais de computadores. 2. Redes locais sem fio. 3. Arquitetura de rede de computador. 4. IEEE 802.11 (Normas). 5. Ethernet (Redes locais de computadores). I. Título.

CDD (23. ed.) 003.72

Bibliotecária: Maria Emília Pecktor de Oliveira CRB-9/1510

Coordenação editorial
Camila Lopes Ferreira
Emanuelle Torino

Projeto gráfico, capa e editoração eletrônica
Marco Tulio Braga de Moraes

Normalização
Camila Lopes Ferreira

Revisão
Adão de Araújo

UTFPR Editora
Av. Sete de Setembro, 3165
80230-901 Curitiba – PR
www.utfpr.edu.br

SUMÁRIO

APRESENTAÇÃO

Caro leitor:

O assunto redes locais de computadores é bastante vasto e complexo e envolve muitos conceitos, protocolos e tecnologias. O livro *Redes locais de computadores* aborda os conceitos fundamentais e as principais tecnologias de redes locais de computadores ao longo de sete capítulos. O objetivo é apoiar professores, estudantes e profissionais de redes de computadores nos seus estudos sobre o tema.

As redes locais de computadores têm uma história bastante rica e fascinante. Assim, neste livro existe um esforço especial de contextualizar as diversas questões envolvendo as redes locais, o qual foi materializado em inserções de história ao longo do texto. Você certamente se sentirá estimulado por esses acontecimentos históricos.

Um grande abraço!
Luciano Pansanato

1 INTRODUÇÃO A REDES LOCAIS

Objetivos:

- Compreender os conceitos e terminologia relacionados a redes locais de computadores;
- Diferenciar os principais componentes de uma rede local.

1.1 CONCEITOS

As redes locais (ou LANs, do inglês *Local Area Networks*) de computadores são redes de propriedade privada que operam dentro e próximas a um único edifício como uma residência, um escritório ou uma indústria (TANENBAUM; WETHERALL, 2011). O termo **de propriedade privada** significa que as redes locais geralmente estão restritas a uma organização. O caráter privado das redes locais garante uma maior flexibilidade na escolha das tecnologias utilizadas para a sua implementação e operação (GIOZZA et al., 1986).

Além das redes locais, na terminologia de redes de computadores também são comuns as redes metropolitanas (ou MANs, do inglês *Metropolitan Area Networks*) e as redes de longa distância (ou WANs, do inglês *Wide Area Networks*). Tanenbaum e Wetherall (2011) também incluem nessa classificação as redes pessoais (ou PANs, do inglês *Personal Area Networks*) e a internet (a rede mundial de computadores). Essa classificação, mostrada no Quadro 1, considera principalmente a distância física (escala) entre o conjunto de computadores interconectados.

Distância entre computadores	Computadores localizados em	Exemplo
1 m	Metro quadrado	Rede pessoal
10 m	Sala	Rede local
100 m	Prédio	
1 km	Câmpus	
10 km	Cidade	Rede metropolitana
100 km	País	Rede de longa distância
1.000 km	Continente	
10.000 km	Planeta	Internet

Quadro 1 – Classificação de computadores interconectados segundo a escala
Fonte: Adaptado de Tanenbaum e Wetherall (2011, p. 11).

A definição de rede local com base principalmente nas distâncias envolvidas é bastante vaga. Em geral, considera-se **área geográfica pequena** as distâncias entre 10 m

e 1 km, muito embora as limitações associadas às tecnologias utilizadas em redes locais não imponham limites a essas distâncias.

Outras características típicas encontradas e geralmente associadas a redes locais são: altas taxas de transmissão e baixas taxas de erro (TANENBAUM; WETHERALL, 2011; SOARES; LEMOS; COLCHER, 1995). É importante notar que os termos **área geográfica pequena, altas taxas de transmissão e baixas taxas de erro** são suscetíveis à evolução tecnológica, isto é, quaisquer valores associados a estes termos estão ligados à tecnologia atual e certamente não serão mais os mesmos dentro de poucos anos.

As redes locais são amplamente utilizadas para conectar computadores com o objetivo de permitir o compartilhamento de recursos e o intercâmbio de dados. Nesse contexto, podem ser considerados recursos os periféricos de custo alto, por exemplo, um disco de alta capacidade ou uma impressora mais rápida.

O termo intercâmbio de dados não significa somente troca de arquivos, mas também o acesso para consulta e/ou alteração de qualquer informação armazenada em outro computador de uma rede local (TORRES, 2001). Por exemplo, em um supermercado cada caixa registradora é um computador que, além de somar o valor a ser pago pelo produto, também atualiza automaticamente o controle de estoque mantido em outro computador.

O meio de transmissão utilizado na conexão entre os computadores é normalmente o cabo (fio de cobre ou fibra óptica), mas o uso de ondas eletromagnéticas também tem sido muito disseminado. O cabo coaxial (de fio de cobre) foi um dos primeiros tipos de cabo utilizados em redes, mas o par trançado (também de fio de cobre) é o tipo de cabo de rede mais utilizado atualmente. A preferência por fibra óptica ocorre quando o objetivo é evitar interferências eletromagnéticas (que não ocorrem no tráfego da luz) e/ou superar os limites (de distância e velocidade) dos cabos de fio de cobre.

A transmissão física dos dados é executada por um conjunto de regras, chamado de protocolo. Essas regras (protocolo) são implementadas no adaptador de rede (ou placa de rede), que está instalado dentro de cada equipamento de uma rede local. No caso mais simples, o meio de transmissão interconecta o adaptador de um computador diretamente ao do outro computador, conforme mostra a Figura 1.

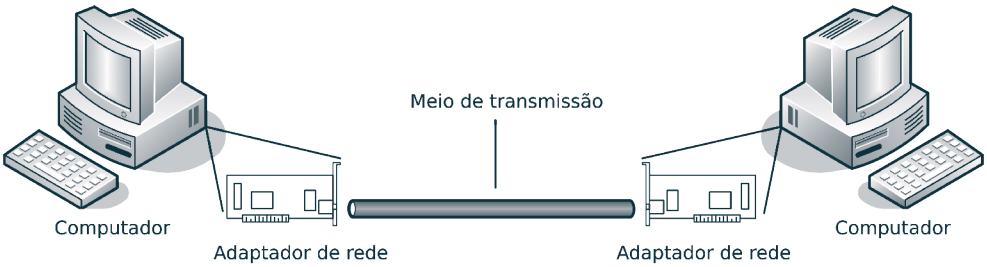

Figura 1 – Interconexão de computadores
Fonte: Autoria própria (2014).

A-Z

Glossário: Adaptador de rede, também chamado de placa de rede ou interface de rede (NIC, do inglês *Network Interface Card*), é um dispositivo de hardware responsável pela comunicação entre os computadores de uma rede.

Provavelmente a maneira mais fácil de entender o conceito de protocolo utilizado em redes de computadores é fazendo analogias com um protocolo humano, visto que as pessoas utilizam protocolos o tempo todo (KUROSE; ROSS, 2013).

Considere o exemplo de perguntar as horas a uma pessoa; um diálogo comum entre duas pessoas poderia ser o seguinte:

A: Oi!

B: Oi!

A: Que horas são, por favor?

B: Duas horas.

O protocolo humano recomenda que, ao iniciar uma comunicação com uma pessoa, primeiramente diga um cumprimento (o primeiro **oi**). A resposta comum para um **oi** é outro **oi**. Implicitamente, uma resposta cordial é considerada como uma indicação de que é possível prosseguir e perguntar as horas. Uma resposta diferente ao **oi** inicial poderia indicar falta de vontade ou incapacidade de comunicação. Nesse caso, o recomendado pelo protocolo humano seria não perguntar as horas. Às vezes, não se recebe nenhuma resposta para uma pergunta, caso em que normalmente se desiste de perguntar as horas à pessoa.

Nesse protocolo humano, existem mensagens específicas que são enviadas e ações específicas que são realizadas em reação às respostas recebidas ou a outros eventos (como não receber uma resposta após certo tempo). As mensagens, ações e outros eventos desempenham um papel central em um protocolo humano. Se as pessoas utilizarem protocolos diferentes, os protocolos não interagem e nenhum trabalho útil pode ser realizado. Por exemplo, se uma pessoa é cordial ou não; se uma delas entende o conceito de horas, mas a outra não.

Um protocolo para redes de computadores é semelhante a um protocolo humano. A única diferença é que as entidades que trocam mensagens e realizam ações são componentes de hardware ou software de algum equipamento (por exemplo, computador, roteador ou outro dispositivo de rede). Resumindo, duas (ou mais) entidades em comunicação devem executar o mesmo protocolo para que uma tarefa seja realizada.

1.2 COMPONENTES DE UMA REDE LOCAL

Os componentes mais importantes de uma rede local são (CYCLADES BRASIL, 2002):

a) estações;

b) servidores;

c) sistema operacional de rede;

d) meio de transmissão;

e) dispositivo de rede;

f) protocolos de comunicação.

1.2.1 Estações e Servidores

As estações e servidores são os computadores em uma rede local. O que determina se um computador tem a função de estação ou de servidor é o software instalado e a sua configuração.

As estações individuais de trabalho, ou clientes, são computadores pessoais (ou PCs, do inglês *Personal Computers*) – de mesa (*desktops*) ou portáteis (*notebooks*) – nos quais seus usuários executam suas tarefas locais e têm acesso, quando necessário, aos recursos disponíveis em servidores.

Em geral, nas estações são executadas tarefas de usuário como a edição de textos e planilhas, criação de gráficos e de apresentações, entre outras. Ao trabalhar em uma estação, não existe diferença entre usar os recursos de um servidor ou da própria estação. Com o software cliente adequado, os usuários podem executar tarefas na rede. Essas tarefas geralmente incluem o mapeamento de unidades de disco, captura de portas de impressora, envio de mensagens e acesso a arquivos.

O servidor é um computador com capacidade de processamento superior à capacidade das estações e a sua função é fornecer serviços à rede.

O servidor provê e gerencia o acesso aos recursos compartilhados, como discos e impressoras. Em geral, esse equipamento processa grandes volumes de dados, requerendo processadores de alto desempenho e dispositivos de armazenamento de alta capacidade e de acesso rápido, bem como mecanismos para evitar possíveis falhas. O dimensionamento do hardware do servidor depende totalmente da quantidade, do tipo e da finalidade dos serviços que serão executados.

Os serviços que um servidor normalmente oferece à rede são (CYCLADES BRASIL, 2002):

a) servidor de aplicação (*application server*);

b) servidor de arquivos (*file server*);

c) servidor de impressão (*print server*);

d) servidor de banco de dados (*database server*).

Existem dois tipos de servidores: dedicados e não dedicados. Um servidor dedicado é um computador utilizado exclusivamente para a execução de tarefas de rede.

Em geral, o uso de servidores dedicados se deve aos altos requisitos de memória e processamento dos sistemas operacionais de rede e/ou de determinados serviços oferecidos. Um computador com *Windows Server* (da Microsoft®) é um exemplo de servidor dedicado.

Um servidor não dedicado é aquele em que o computador pode agir como um servidor e como uma estação ao mesmo tempo. Em uma rede local do tipo *peer-to-peer*, todos os computadores têm o potencial de compartilhar recursos com os demais. Um exemplo de servidor não dedicado é um computador com o sistema operacional *Microsoft Windows* (versão 7 ou superior).

Os servidores não dedicados podem ser conectados a outros servidores e podem utilizar seus recursos, da mesma forma que as estações. Por exemplo, quando o usuário

está trabalhando em um servidor não dedicado, outros usuários podem usar a impressora jato de tinta conectada ao seu computador enquanto este está usando a impressora laser conectada a um servidor dedicado.

As redes locais do tipo *peer-to-peer* são pequenas redes nas quais cada estação pode funcionar como um servidor, permitindo a todos os usuários compartilhar recursos em todos os equipamentos.

Esse tipo de rede é geralmente fácil de instalar e gerenciar, mas os servidores dedicados têm melhor desempenho e podem manipular altos volumes de requisições de serviços. Em geral, as redes locais grandes utilizam múltiplos servidores dedicados.

1.2.2 Sistema Operacional de Rede

O sistema operacional de rede é um software de controle usado para compartilhar recursos e executar todas as demais atividades de conexão entre o servidor e os clientes (estações). O sistema operacional de rede está instalado no servidor; uma parte desse software está instalada em cada cliente (estação) para permitir o acesso aos recursos e demais funcionalidades oferecidas pelo servidor. Os sistemas mais adotados no mercado são o *Windows Server* e os sistemas baseados em Unix, como as distribuições GNU[1] Linux e os sistemas proprietários (por exemplo, o HP-UX da *Hewlett-Packard* – HP – e o AIX[2] da *International Business Machines* – IBM).

O sistema operacional de rede no cliente possui características mais simples, voltadas para a utilização de serviços, enquanto que o sistema no servidor possui uma maior quantidade de recursos necessários para executar os serviços que são oferecidos aos clientes.

Portanto, os sistemas operacionais de rede podem ser considerados uma extensão dos sistemas operacionais locais, complementando-os com o conjunto de funções básicas e de uso geral, necessárias à operação das estações, de forma a tornar transparente o uso dos recursos compartilhados.

---

1 GNU é o nome de um projeto lançado em 27 de setembro de 1983 por Richard Stallman e que atualmente é mantido pela *Free Software Foundation* (FSF). O objetivo do projeto era criar um sistema operacional parecido com o Unix, chamado GNU, totalmente baseado em software livre. O termo GNU é um acrônimo recursivo para GNUs Not Unix (GNU não é Unix) e também o nome do animal que representa o projeto, um grande mamífero nativo do continente africano.

2 *Advanced Interactive Executive* (AIX) é uma versão da IBM para o sistema operacional Unix que é executado em computadores IBM de médio porte. AIX é um sistema comercial de código fonte fechado com base no Unix System V e é muito utilizado em grandes corporações. Antes do produto ser comercializado, o acrônimo AIX era uma abreviação de Advanced IBM Unix ou, em português, Unix Avançado da IBM.

A-Z

Glossário: Transparência é a característica de livrar o usuário de qualquer conhecimento sobre como o sistema executa suas tarefas (TANENBAUM, 2009).

A transparência é um dos requisitos fundamentais dos sistemas operacionais de rede. Nesse sentido, os sistemas operacionais de rede devem atuar de forma que os usuários utilizem os recursos da rede como se estivessem operando localmente.

A solução encontrada para estender o sistema operacional das estações sem modificar sua operação local foi a introdução de um módulo redirecionador.

O redirecionador funciona interceptando as chamadas feitas pelas aplicações ao sistema operacional local e desviando as que dizem respeito a recursos de rede para o módulo do sistema operacional de rede responsável pelos serviços de comunicação, conforme ilustrado na Figura 2. Para as aplicações dos usuários, a instalação do sistema operacional de rede é percebida apenas pela adição de novos recursos aos que existiam anteriormente.

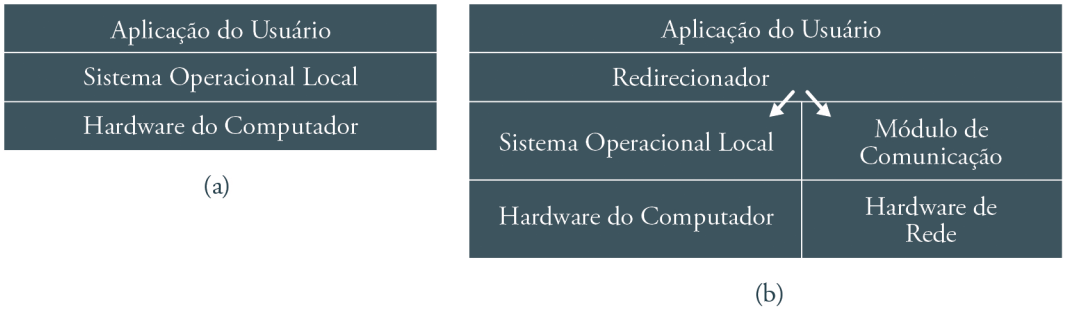

Figura 2 – Sistema operacional local sem redirecionador (a) e com redirecionador (b)
Fonte: Autoria própria (2014).

Os sistemas operacionais de rede são fundamentais na definição de uma rede local. Um estudo criterioso deve ser feito visando à escolha do sistema operacional mais adequado às necessidades de uma rede local. Esse estudo deve considerar diversos aspectos, como distribuição e quantidade de estações, aplicações, necessidades de interface com outros sistemas operacionais das estações, aderência/conformidade a padrões, desempenho, segurança, entre outros.

1.2.3 Meio de Transmissão

O meio de transmissão é o meio físico utilizado para o transporte dos dados em uma rede local. Basicamente, a transmissão pode ser realizada por três meios físicos (SOUSA, 1999):

a) transmissão por fios ou cabos de cobre, na qual os dados são transmitidos por sinais elétricos que se propagam pelo metal;

b) transmissão por fibras ópticas, na qual os dados são transmitidos por sinais luminosos que se propagam pelo vidro ou plástico que formam a fibra óptica;

c) transmissão por irradiação eletromagnética (ondas), em que os dados são transmitidos por sinais elétricos irradiados através do ar por antenas (ou mesmo pelo espaço, quando do uso de satélites).

Uma rede local, quanto ao meio de transmissão, pode ser cabeada (*wired*) ou sem fio (*wireless*). Os tipos mais comuns de cabos utilizados em redes locais cabeadas são o par trançado e a fibra óptica. O cabo de par trançado é um meio de transmissão com um ou mais pares trançados de condutores de cobre isolados delimitados por uma única capa de plástico. O cabo de fibra óptica é um cabo feito de fibra de vidro muito fina, no interior da qual são refletidos os sinais de luz.

Os tipos mais comuns de redes locais sem fio são as baseadas em ondas eletromagnéticas (ou ondas de rádio), como as tecnologias conhecidas como *Bluetooth* e *Wi-Fi*, que operam da mesma forma que os telefones celulares e televisões. A tecnologia *Bluetooth* provê uma maneira de conectar e trocar informações entre dispositivos como telefones celulares, *tablets*, *notebooks* e *desktops*, impressoras, câmeras digitais e consoles de videogames digitais através de uma frequência de rádio de curto alcance. A tecnologia *Wi-Fi* conecta computadores e outros dispositivos de rede por meio de frequências iguais ou maiores do que 2,4 GHz, consideravelmente mais altas que as frequências usadas para telefones celulares e televisões.

1.2.4 Dispositivos de Rede

Os dispositivos de rede são equipamentos para a comunicação entre os diversos componentes da rede local. Os comutadores (*switches*) e os roteadores (*routers*) são exemplos de dispositivos de rede.

Os dispositivos de rede conhecidos como repetidores (*hubs*) e pontes (*bridges*) estão ultrapassados e não são mais comercializados; os comutadores (*switches*) incorporaram as suas funcionalidades.

Em geral, os dispositivos de rede são empregados para a interconexão de computadores em uma rede local (*switches*), para a interconexão de duas ou mais redes locais (*switches*) e para a interconexão entre redes diferentes que estão distantes geograficamente (*routers*).

1.2.5 Protocolos de Comunicação

Um protocolo é um conjunto de regras e convenções que controla a forma como é realizada a comunicação entre duas entidades (GIOZZA et al., 1986; ZACKER; DOYLE, 2000). As sociedades humanas desenvolveram protocolos em diversos níveis. Por exemplo, as linguagens são protocolos formulados para permitir a comunicação entre pessoas.

O uso impróprio da linguagem resulta em mal-entendidos ou impede que seja estabelecida qualquer comunicação. As redes também possuem certos protocolos definidos, especificando o comportamento apropriado para a comunicação entre computadores e outros dispositivos de rede. Quando qualquer hardware ou software viola as regras, não é possível estabelecer uma comunicação adequada por meio da rede.

As mensagens geradas por um computador que não se adaptam a protocolos aceitos não serão reconhecidas por outros computadores. Da mesma maneira que com as pessoas, essas mensagens serão consideradas como se fossem ruídos e serão ignoradas.

A especificação de um protocolo contém informações suficientes para permitir o desenvolvimento do software ou a construção do hardware de modo que as mensagens sejam transmitidas corretamente de acordo com a sintaxe e semântica do protocolo.

A sintaxe de um protocolo se refere ao formato das mensagens que são trocadas pelas entidades. O formato especifica os campos que contêm dados e outras informações de controle, assim como a maneira como são codificados.

A semântica de um protocolo se refere ao significado de cada mensagem trocada e as ações que são realizadas pelas entidades. Em outras palavras, a semântica está relacionada ao funcionamento do protocolo.

Resumo

Neste capítulo foram abordados diversos conceitos relacionados a redes de computadores. Uma definição para redes locais foi apresentada com base nas distâncias envolvidas. Os principais meios de transmissão são o fio de cobre e a fibra óptica, mas as ondas eletromagnéticas são muito utilizadas em redes sem fio. A interconexão de computadores é geralmente realizada por meio de adaptador de rede e meio de transmissão. A noção de protocolo foi apresentada de maneira intuitiva. De maneira mais formal, protocolo é um conjunto de regras e convenções que controla a forma como é realizada a comunicação. Na segunda parte deste capítulo introdutório, os principais componentes de uma rede local foram relacionados e descritos com algum detalhe. Estações, servidores, sistema operacional de rede, meio de transmissão e dispositivo de rede são os principais componentes. Os protocolos de comunicação foram novamente abordados, pois esse conceito é fundamental para compreender outros conceitos que envolvem as redes de computadores.

Atividades de aprendizagem

1. Quais as distâncias envolvidas na definição de rede local (LAN) e rede de longa distância (WAN)?
2. Quais são os principais objetivos para a interconexão de computadores em uma rede local?
3. Quais as características dos principais meios de transmissão empregados em redes locais?
4. Qual a função do adaptador de rede na interconexão de computadores?
5. A palavra protocolo é muito utilizada para descrever relações diplomáticas. Dê um exemplo de um protocolo diplomático.
6. Descreva cada um dos principais componentes que podem estar envolvidos em uma rede local: estação, servidor, sistema operacional de rede, meio de transmissão, dispositivo de rede e protocolo de comunicação.

2 HISTÓRICO E EVOLUÇÃO DAS REDES LOCAIS

Objetivos:

- Identificar os principais acontecimentos na história das redes de computadores;
- Compreender a evolução das redes locais e a sua relação com as redes de longa distância.

2.1 HISTÓRICO DAS REDES

A história das redes de computadores e da internet (a rede mundial de computadores) pode ser dividida em quatro partes (KUROSE; ROSS, 2013): de 1961 a 1972, comutação de pacotes e as primeiras redes de computadores; de 1972 a 1980, redes proprietárias e as primeiras redes locais; de 1980 a 1990, proliferação das redes; e a década de 1990, explosão da internet e da *web*. Ao longo do histórico apresentado neste capítulo, é possível observar que, cronologicamente, as redes de longa distância (WANs) surgiram antes das redes locais (LANs).

A-Z

Glossário: A internet é um conjunto de redes interconectadas por roteadores e que utiliza protocolos que a fazem funcionar como uma única rede de alcance global.

2.1.1 1961-1972: Comutação de Pacotes e as Primeiras Redes de Computadores

Na década de 1950, o custo dos primeiros computadores era alto e a utilização estava restrita a organizações governamentais e grandes empresas. Os computadores eram utilizados quando a demanda das aplicações por processamento rápido de informações justificava o investimento. Em geral, a operação do computador era realizada de maneira centralizada, procurando aperfeiçoar e compartilhar o seu uso entre as aplicações dos diversos usuários.

Desde o início da década de 1960, a rede telefônica era a rede de comunicação dominante no mundo inteiro. A rede de telefonia utiliza a comutação de circuitos para transmitir informações entre uma origem e um destino. A comutação de circuitos fornece um caminho dedicado para a comunicação entre origem e destino.

Em uma chamada telefônica, o equipamento de comutação procura por um caminho físico no trajeto que vai do telefone de origem até o telefone de destino. Essa descrição é, obviamente, muito simplificada, pois alguns dos trechos do caminho físico entre dois telefones podem ser feitos por conexões nas quais milhares de chamadas são multiplexadas. No entanto, a ideia básica permanece válida: uma vez estabelecida uma chamada, haverá um caminho dedicado entre ambas as extremidades até que a chamada seja finalizada.

A-Z

Glossário: Multiplexação é uma técnica que consiste na transmissão de várias comunicações diferentes ao mesmo tempo através de um único meio físico de transmissão.

A crescente demanda e uso de computadores nas universidades e laboratórios de pesquisa no início da década de 1960 e o advento de computadores com multiprogramação (*time-sharing*) originou a questão de como interconectar computadores para que pudessem ser compartilhados entre diversos usuários.

O tráfego gerado por esses usuários provavelmente era intermitente, isto é, com períodos de atividade, como o envio de um comando a um computador remoto, seguido de períodos de inatividade, como a espera por uma resposta ou a análise de uma resposta recebida. Esse tipo de tráfego é conhecido como tráfego em rajadas.

A-Z

Glossário: Multiprogramação é um modo de operação de um computador que permite a execução intercalada no tempo de vários programas num único processador.

Em 1964, a comutação de pacotes começou a ser inventada de maneira independente por três grupos de pesquisa como uma alternativa eficiente à comutação de circuitos. A comutação de pacotes não fornece um caminho dedicado entre origem e destino. Ao contrário, quando a origem possui um bloco de dados (pacote) a ser enviado, este é armazenado no primeiro equipamento de comutação e, em seguida, é passado adiante.

No caso de tráfego intermitente (em rajadas), a comutação de pacotes é mais adequada do que a comutação por circuitos, porque permite que vários usuários compartilhem o caminho ao mesmo tempo.

A-Z

Glossário: Pacote é uma unidade de transmissão de dados. A informação a ser transmitida geralmente é dividida em diversos pacotes que são então transmitidos.

Leonard Kleinrock, doutorando do *Massachusetts Institute of Technology* (MIT), Estados Unidos, publicou o primeiro trabalho sobre técnicas de comutação de pacotes, demonstrando a eficácia da abordagem de comutação de pacotes para fontes de tráfego intermitente.

Paul Baran, do *Rand Institute*, Estados Unidos, começou a investigar a utilização de comutação de pacotes na transmissão de voz com segurança pelas redes militares, ao

mesmo tempo em que Donald Davies e Roger Scantlebury desenvolviam suas ideias sobre o mesmo assunto no *National Physical Laboratory*, Inglaterra. Esses trabalhos são considerados o alicerce da internet.

Joseph Licklider e Lawrence Roberts, colegas de Kleinrock no MIT, continuaram o trabalho e lideraram o programa de ciência de computadores na *Advanced Research Projects Agency* (ARPA). A ARPA é uma agência do Departamento de Defesa dos Estados Unidos, posteriormente renomeada para *Defence* ARPA (DARPA), responsável pelo desenvolvimento de novas tecnologias para uso pelos militares. Roberts publicou um plano geral para a ARPANET, a primeira rede de computadores por comutação de pacotes.

Os primeiros comutadores de pacotes eram conhecidos como processadores de mensagens de interface (IMPs, do inglês *Interface Message Processors*). Em 1969, o primeiro IMP foi instalado na *University of California Los Angeles* (UCLA) sob a supervisão de Kleinrock. Em seguida, três IMPs adicionais foram instalados no *Stanford Research Institute* (SRI), na *University of California Santa Barbara* (UFSB), e na *University of Utah* (UTAH). Em 1972, a ARPANET tinha 25 nós e foi apresentada publicamente pela primeira vez por Robert Kahn em uma conferência internacional sobre comunicação por computadores.

A-Z

Glossário: Comutadores de pacotes são equipamentos que encaminham pacotes recebidos em uma de suas conexões de entrada para uma das suas conexões de saída. Os roteadores são exemplos de comutadores de pacotes.

2.1.2 1972-1980: Redes Proprietárias e as Primeiras Redes Locais

A ARPANET inicial era uma rede fechada. A comunicação entre computadores somente poderia ocorrer se ambos estivessem ligados a um IMP da ARPANET. Do início a meados da década de 1970, novas redes por comutação de pacotes foram desenvolvidas: ALOHANET, uma rede da DARPA que interligava universidades das ilhas do Havaí; Telenet, uma rede comercial desenvolvida com base na tecnologia da ARPANET; Cyclades, uma rede pioneira na França que operava de maneira muito similar ao que viria a ser a internet; *Systems Network Architecture* (SNA), uma rede da IBM utilizada para a interconexão de terminais e computadores (*mainframes*).

A-Z

Glossário: Um *mainframe* é um computador de grande porte, dedicado ao processamento de um volume grande de informações. Os *mainframes* são capazes de oferecer serviços de processamento a milhares de usuários através de terminais conectados diretamente ou através de uma rede. O termo ***mainframe*** se refere ao gabinete principal que alojava a unidade central de processamento nos primeiros computadores.

Em 1974 surgiu a primeira especificação do protocolo *Transmission Control Protocol/Internet Protocol* (TCP/IP), que depois se tornaria o protocolo definitivo para uso na ARPANET (e mais tarde na internet).

A rede ARPANET interligou diversas universidades e levou ao desenvolvimento de muitos recursos, alguns destes utilizados até hoje, como os protocolos para correio eletrônico, terminal remoto e transferência de arquivos, que permitiam aos usuários conectados trocar informações, acessar outros computadores remotamente e compartilhar arquivos.

Na época, os *mainframes* com um bom poder de processamento eram raros e muito caros, de forma que estes acabavam sendo compartilhados entre diversos pesquisadores e técnicos, que podiam estar situados em qualquer ponto da rede.

Além do crescimento da oferta de redes proprietárias e das pesquisas que levariam à internet, outras atividades importantes relacionadas às redes de computadores estavam em desenvolvimento. As primeiras redes locais (LANs) foram criadas no final de 1970 e eram usadas para a criação de conexões de alta velocidade entre grandes computadores centralizados em uma mesma área geográfica, por exemplo, no mesmo prédio ou câmpus universitário. Os sistemas mais populares para redes locais eram a *Ethernet* e a ARCNET.

Em 1976, Bob Metcalfe e David Boggs, do *Palo Alto Research Center* (PARC) da Xerox, desenvolveram a *Ethernet*, uma tecnologia de comutação de pacotes para redes compartilhadas utilizando fios de cobre. Essa tecnologia teve como base o trabalho de Norman Abramson. Em 1970, Abramson e seus colegas da Universidade do Havaí desenvolveram o ALOHA, o primeiro protocolo de acesso múltiplo que permitiu o compartilhamento de um único meio de transmissão por usuários distribuídos em diferentes localizações geográficas (neste caso, o meio de transmissão compartilhado foi uma frequência de rádio).

A motivação para o trabalho de Metcalfe e Boggs foi a necessidade de conectar vários computadores com a finalidade de compartilhamento de recursos.

A ARCNET foi desenvolvida pelo engenheiro John Murphy na *Datapoint Corporation* em 1976, e anunciada em 1977. Na época, a ARCNET era mais flexível e barata que a *Ethernet*, o que tornou a arquitetura bastante popular até fins da década de 1980.

As redes locais ARCNET utilizavam uma topologia de estrela, que lembra bastante a topologia das redes atuais, com o uso de um concentrador e um cabo individual para cada estação. Além disso, os cabos podiam ter até 610 m, mais do que em qualquer padrão *Ethernet* para fios de cobre.

Os dois grandes problemas do ARCNET eram a baixa taxa de transmissão, apenas 2,5 Mbps, e o fato de o padrão ser proprietário, o que limitou o número de fabricantes produzindo equipamentos e impediu que os preços caíssem na mesma velocidade que os da *Ethernet*.

A maioria das redes eram sistemas proprietários. A passagem para sistemas abertos (não proprietários) começou como uma resposta ao domínio das grandes empresas e suas redes proprietárias. Em 1978, a Xerox, a Intel e a Digital, com o aval de Metcalfe, trabalharam para estabelecer a *Ethernet* como um padrão aberto.

Em 1979, o Modelo de Referência *Open Systems Interconnection* (OSI) foi publicado para promover a padronização internacional de arquiteturas de rede visando à interconexão de sistemas abertos. Metcalfe deixou a Xerox em 1979 para estimular o uso de computadores pessoais e de redes locais, criando para isso a empresa 3Com.

2.1.3 1980-1990: Proliferação das Redes

Na década de 1980, o avanço da microeletrônica levou a uma redução contínua do custo dos equipamentos, culminando com o surgimento dos mini e microcomputadores de baixo custo, acessíveis a pequenas empresas e até mesmo a uma pessoa comum. Essa evolução da tecnologia mudou a organização da atividade de processamento de dados nas empresas e universidades, passando a ser comum a existência de mini e microcomputadores instalados no local de trabalho do usuário final.

Nesse contexto, as tecnologias de redes locais representaram uma etapa importante para o trabalho em redes de computadores. Cada rede local conectava vários computadores, impressoras e discos compartilhados concentrados em uma área geográfica, como um prédio ou um câmpus universitário. À medida que o número de redes locais aumentava, a necessidade de interconectar essas redes foi se tornando cada vez mais importante.

Na década de 1980, duas categorias de tecnologia de redes locais eram populares em ambientes de trabalho. A primeira categoria consistia nas redes locais *Ethernet*, que eram redes de acesso aleatório em barramento. A *Ethernet* será estudada em detalhes no Capítulo 6.

A segunda categoria de redes locais compreendia as tecnologias de passagem de permissão em anel, incluindo a *Token Ring*, desenvolvida pela IBM por volta de 1980, e a *Fiber Distributed Data Interface* (FDDI), um padrão internacional estabelecido pelo *American National Standards Institute* (ANSI) em 1987.

A *Token Ring* chegou perto de dominar as redes empresariais, devido principalmente aos grandes investimentos e influência da IBM nesse mercado. A FDDI adota uma tecnologia de passagem de permissão em anel idêntica à das redes *Token Ring*, mas utiliza cabos de fibra óptica que permitem atingir altas capacidades de transmissão e longas distâncias.

Assim, a FDDI era indicada para redes locais de maior alcance geográfico, incluindo as denominadas redes metropolitanas (MANs), e era utilizada principalmente para servir de rede principal (*backbone*) para a interconexão de diversas redes locais.

A-Z

Glossário: *Backbone* significa **espinha dorsal** (tradução direta) e é o termo utilizado para identificar a rede principal pela qual outras redes menores são conectadas.

A década de 1980 também foi marcada pelo crescimento das redes parecidas com a internet, em grande parte como consequência dos esforços distintos para criar redes de computadores para interligar as universidades. A rede BITNET processava mensagens de correio eletrônico (*e-mail*) e fazia transferência de arquivos entre diversas universidades dos Estados Unidos.

A rede *Computer Science Network* (CSNET) foi formada para interligar pesquisadores de universidades que não tinham acesso à ARPANET. Em 1986, a NSFNET foi criada para prover acesso a centros de supercomputação patrocinados pela *National Science Foundation* (NSF). Inicialmente com uma velocidade de 56 Kbps, a NSFNET estaria funcionando a 1,5 Mbps ao final da década de 1980 e servindo como rede principal (*backbone*) para a interligação de redes regionais.

Saiba mais: A Rede Nacional de Ensino e Pesquisa (RNP) foi criada pelo Ministério da Ciência e Tecnologia (MCT) com o objetivo de construir uma infraestrutura de rede internet nacional de âmbito acadêmico. Para conhecer a evolução do *backbone* da RNP, veja o histórico disponível em: <http://www.rnp.br/institucional/nossa-historia>.

Até meados da década de 1980, estavam sendo definidos muitos dos componentes finais da arquitetura da ARPANET. Em 1983, o TCP/IP foi adotado oficialmente como o novo padrão de protocolo para a ARPANET, em substituição ao protocolo *Network Control Protocol* (NCP). No final da década de 1980, algumas extensões importantes foram agregadas ao TCP para a implementação de controle de congestionamento.

Além disso, também ocorreu o desenvolvimento do sistema de nomes de domínios (DNS, do inglês *Domain Name System*) utilizado para mapear os nomes para seus endereços IP.

Paralelamente ao desenvolvimento da ARPANET, no início da década de 1980 a França lançou o projeto Minitel, cujo objetivo era levar as redes para todas as residências.

O sistema Minitel era patrocinado pelo governo e consistia em uma rede pública de comutação de pacotes, em servidores Minitel e em terminais de baixo custo com dispositivos de transmissão de dados (*modems*) de baixa velocidade embutidos.

Em 1984, o Minitel se transformou em um enorme sucesso, quando o governo da França forneceu um terminal gratuito para toda residência francesa que desejasse participar da rede. O Minitel incluía serviços de livre acesso, como o de lista telefônica, e também outros serviços que cobravam uma taxa de cada usuário com base no tempo de utilização.

Em meados da década de 1990, o Minitel oferecia mais de vinte mil serviços e estava presente em grande parte das residências francesas dez anos antes que a maioria dos norte-americanos ouvissem falar de internet (KUROSE; ROSS, 2013).

2.1.4 Década de 1990: Explosão da Internet e da *Web*

No início da década de 1990, ocorreram alguns eventos que indicavam a evolução contínua da internet. A ARPANET foi extinta, devido ao crescimento de outras redes que passaram a carregar a maior parte do tráfego do Departamento de Defesa dos Estados Unidos, e também devido ao uso da NSFNET como uma rede

principal (*backbone*) para conectar as redes regionais nos Estados Unidos com as redes nacionais de outros países.

Em 1991, a NSFNET eliminou as restrições para a sua utilização com finalidades comerciais. No entanto, a NSF perderia o controle da rede em 1995, quando o tráfego principal (*backbone*) passou a ser transmitido por provedores de serviços de internet (ISPs, do inglês *Internet Service Providers*).

O papel principal das redes locais no contexto da internet é o de rede de acesso, isto é, o papel de conectar o computador do usuário ao primeiro roteador da infraestrutura de rede com acesso à internet. Em outras palavras, quando um usuário tem acesso à internet a partir de uma residência ou de uma empresa, este acesso é quase sempre feito por meio de uma rede local.

Especificamente, o acesso ocorre do computador do usuário para a rede local, para o roteador, para o provedor de serviços de internet (ISP), para o *backbone* nacional da internet, e assim por diante.

O surgimento do serviço *world wide web* (WWW ou simplesmente *web*) é considerado o principal acontecimento da década de 1990, que motivou a instalação de acesso à internet em residências e empresas do mundo todo. A *web* também foi utilizada como plataforma de acesso a centenas de novas aplicações, incluindo serviços de recuperação de informações, serviços bancários *on-line* e serviços multimídia em tempo real.

O final da década de 1990 foi um período de crescimento e inovação para a internet, com a criação de novos produtos e serviços. Esse período também é marcado pelo domínio pela tecnologia *Ethernet* do mercado de redes locais com fio e pelo surgimento da tecnologia *Ethernet* de alta velocidade (1 Gbps), que passou a ser utilizada frequentemente como rede principal (*backbone*) para interconectar diversas redes locais de 10 Mbps e 100 Mbps. A partir de 2001, a velocidade de transmissão da tecnologia *Ethernet* foi ampliada com produtos a 10, 40 e 100 Gbps, estendendo a tecnologia aos enlaces ponto a ponto de redes de longa distância (WANs).

2.2 PRESENTE E FUTURO

A rede ARPANET e a *Ethernet* deram origem, respectivamente, à internet e às redes locais. Essas duas inovações podem ser consideradas as que mais revolucionaram

a computação moderna. Atualmente, é difícil imaginar o trabalho diário sem a internet e sem as redes locais.

O acesso à *web* se tornou tão comum, que é cada vez mais difícil encontrar utilidade para um computador desconectado de uma rede local que forneça acesso à internet. Além disso, as redes de computadores continuam cumprindo seu papel, como uma forma de compartilhar recursos entre diversos computadores, permitindo o acesso remoto a dados e periféricos.

A área de redes de computadores continua em desenvolvimento. Em todas as frentes existem avanços, incluindo o desenvolvimento de novas aplicações, distribuição de conteúdo multimídia, telefonia via internet, velocidades de transmissão mais altas em redes locais e roteadores mais rápidos. No contexto das redes locais, a disseminação de redes de acesso de alta velocidade merece atenção especial.

O aumento cada vez maior do acesso residencial à internet, por meio de sistema a cabo ou pela linha telefônica, está criando o cenário ideal para uma variedade grande de novas aplicações multimídia, como o vídeo por demanda em tempo real e video-conferência interativa de alta qualidade. A crescente presença de redes sem fio públicas de alta velocidade e redes de telefonia celular de média velocidade está possibilitando acesso à internet com a conexão constante e permitindo a criação de novos serviços específicos para determinadas localizações geográficas. As redes locais sem fio serão abordadas no Capítulo 7.

Resumo

A evolução dos computadores iniciou-se na década de 1970. O destaque é para a rede ARPANET, que originou a internet, conhecida atualmente como a rede mundial de computadores. O desenvolvimento da *Ethernet* é considerado um marco muito importante na história das redes de computadores, pois esse acontecimento deu origem às redes locais como são amplamente utilizadas nos dias atuais. Na década de 1980, ocorreu a proliferação das redes de computadores, com destaque para as redes locais *Ethernet*, *Token Ring* e FDDI (também para redes metropolitanas), e para as redes de longa distância CSNET e NSFNET. A década de 1990 foi marcada pela evolução contínua da internet e o surgimento da *web*.

Atividades de aprendizagem

1. Construa uma linha de tempo com os principais acontecimentos da história das redes de computadores (locais e de longa distância).
2. Qual a diferença entre comutação de circuitos e comutação de pacotes?
3. O que é a ARPANET?
4. Qual o significado de **rede proprietária**?
5. O que estimulou o desenvolvimento das redes locais?
6. Qual é considerado o principal acontecimento da década de 1990?
7. Qual a relação entre redes locais, provedores de serviços internet (ISP) e a internet?
8. Qual a principal direção futura das redes locais?

3 TOPOLOGIAS

Objetivos:

- Compreender o conceito de topologia;
- Identificar as diferentes topologias físicas e lógicas;
- Compreender a necessidade de controle de acesso e como este é realizado nas topologias existentes.

3.1 CONCEITOS

A estrutura geral de uma rede de computadores é formada por um conjunto de módulos processadores interligados por um sistema de comunicação, conforme ilustrado na Figura 3. Os módulos processadores, frequentemente chamados de nós de uma rede, podem ser estações, servidores e outros dispositivos de rede.

Figura 3 – Um conjunto de módulos processadores interligados por um sistema de comunicação
Fonte: Soares, Lemos e Colcher (1995, p. 11).

O sistema de comunicação constitui um arranjo topológico, ou topologia, interligando os vários módulos processadores através de conexões físicas e de um conjunto de regras e convenções com o objetivo de organizar a comunicação (protocolos) (SOARES; LEMOS; COLCHER, 1995). Em outras palavras, a topologia é o padrão no qual a rede de computadores está organizada.

A escolha de qual topologia deve ser utilizada, entre as alternativas existentes, é uma questão vital na construção de um sistema de comunicação. Naturalmente, as alternativas dependerão do tipo de rede (LAN, MAN ou WAN) (SOARES; LEMOS; COLCHER, 1995), pois determinadas topologias são mais adequadas para um tipo de rede. Além disso, a topologia de uma rede frequentemente também influencia nas questões relacionadas à eficiência, flexibilidade e segurança.

As conexões físicas em uma topologia podem ser de dois tipos: ponto a ponto e multiponto. Na conexão física ponto a ponto, dois módulos processadores (ou nós) estão ligados através de um meio de transmissão qualquer que permite a troca direta de dados, conforme ilustrado na Figura 4.

Figura 4 – Ponto a ponto
Fonte: Autoria própria (2014).

Na multiponto, três ou mais módulos processadores (ou nós) estão ligados de forma a permitir a utilização do mesmo meio de transmissão, conforme ilustrado na Figura 5. As diversas topologias são formadas a partir destes dois tipos de conexões físicas: ponto a ponto e multiponto.

Figura 5 – Multiponto
Fonte: Autoria própria (2014).

Existem duas categorias básicas de topologia de rede: física e lógica. A topologia física de uma rede refere-se à forma como os módulos processadores e as conexões físicas estão organizados. A topologia lógica de uma rede refere-se à maneira como os dados são transmitidos a partir de um módulo processador para outro sem considerar a interligação física.

3.2 TOPOLOGIAS FÍSICAS

As topologias físicas mais utilizadas e conhecidas são as do tipo (SOARES; LEMOS; COLCHER, 1995; SOUSA, 1999):

a) barramento;

b) anel;

c) estrela;

d) malha irregular.

3.2.1 Barramento

A topologia barramento é formada por um único segmento do meio de transmissão ao longo do qual os nós são conectados, conforme exemplificado na Figura 6. Os dados são transmitidos por difusão (*broadcast*) no meio de transmissão e são recebidos por todos os nós. Qualquer um dos nós pode utilizar o meio de transmissão para transmitir dados, mas somente um nó pode transmitir por vez. Essa característica (compartilhamento do meio de transmissão) exige a utilização de mecanismos para controlar o acesso dos nós ao meio de transmissão.

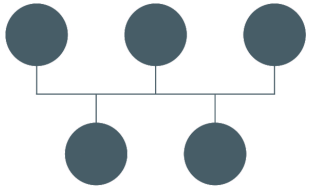

Figura 6 – Barramento
Fonte: Autoria própria (2014).

Mídias integradas: Assista à animação **Bus Topology** disponível em: <http://www.webclasses.net/3comu/intro/units/unit02/a_BusTopology.html>. Demonstre que você entendeu a animação descrevendo o caminho percorrido pelo sinal de transmissão.

Uma das vantagens dessa topologia é o baixo custo, considerando que a implementação do hardware das conexões pode ser simplificada, pois os dados são trocados pelos nós sem a participação de intermediários. Outra vantagem é a facilidade de adicionar novos nós à topologia, pois basta conectar o novo nó ao meio de transmissão compartilhado.

A desvantagem da topologia barramento é que, se o segmento do meio de transmissão partir em algum ponto, toda a rede é interrompida. Além disso, o ponto de falha é difícil de ser localizado.

3.2.2 Anel

A topologia anel é formada por vários segmentos de transmissão ponto a ponto entre pares de nós adjacentes, conforme ilustrado na Figura 7. A topologia anel é carac-

terizada pela participação dos nós intermediários, que funcionam como repetidores, na transmissão de dados entre dois nós não adjacentes.

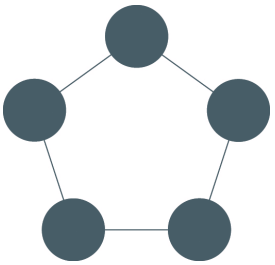

Figura 7 – Anel
Fonte: Autoria própria (2014).

O fluxo dos dados é unidirecional, isto é, o sinal é transmitido e segue em apenas um sentido ao longo de todo o anel, para todos os nós. Como o meio de transmissão é compartilhado pelos nós, essa topologia também exige a utilização de mecanismos de controle de acesso.

Mídias integradas: Assista à animação **Ring Topology**, disponível em: <http://www.webclasses.net/3comu/intro/units/unit02/a_RingTopology.html>. Demonstre que você entendeu a animação, descrevendo o caminho percorrido pelo sinal de transmissão.

A desvantagem dessa topologia é que a confiabilidade da rede depende da confiabilidade individual dos nós intermediários. Caso um nó da rede pare de funcionar, a transmissão dos dados no anel é interrompida, afetando toda a rede.

3.2.3 Estrela

A topologia estrela é formada por vários segmentos de transmissão ponto a ponto que conectam um nó central a nós secundários, conforme ilustrado na Figura 8. As decisões de encaminhamento dos dados para o nó de destino são concentradas no nó central. Cada nó secundário é conectado fisicamente apenas ao nó central.

A dependência de um nó centralizado, característica da topologia estrela, pode ser uma desvantagem. Caso ocorra falha nesse ponto central da rede, toda a rede fica prejudicada. Além desse problema, a complexidade do nó central aumenta de acordo com o número de nós secundários. O gerenciamento das transmissões simultâneas entre os diferentes nós secundários exige um módulo processador de alto desempenho para atuar como nó central.

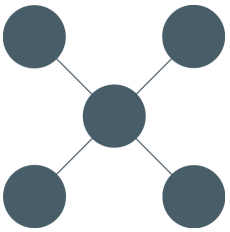

Figura 8 – Estrela
Fonte: Autoria própria (2014).

Mídias integradas: Assista à animação **Star Topology**, disponível em: <http://www.webclasses.net/3comu/intro/units/unit02/a_Startopology.html>. Demonstre que você entendeu a animação, descrevendo o caminho percorrido pelo sinal de transmissão.

3.2.4 Malha Irregular

A topologia malha irregular é a mais geral possível. Nessa topologia, cada nó pode ser conectado diretamente a um número variável de outros nós, dando origem a uma estrutura irregular de interconexão, conforme exemplificado na Figura 9.

A variedade de caminhos para a transmissão de dados de um nó para outro é a característica da topologia malha irregular e introduz a necessidade de decisões de encaminhamento em cada um dos nós. Ao receber uma transmissão por uma conexão de entrada, cada nó intermediário deve decidir em qual das suas conexões de saída os dados serão encaminhados. Assim, devido a essa característica, é necessário que os nós dessa topologia tenham uma capacidade de processamento adequada.

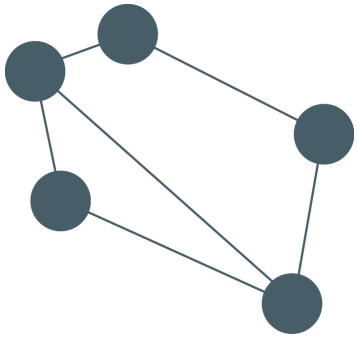

Figura 9 – Malha irregular
Fonte: Autoria própria (2014).

3.3 TOPOLOGIAS LÓGICAS

A topologia lógica de uma rede refere-se à maneira como os dados são transmitidos a partir de um módulo processador (nó) para outro sem considerar a interligação física. Existem três topologias lógicas básicas (CHIOZZOTO; SILVA, 1999):

a) barramento;

b) anel;

c) estrela.

3.3.1 Barramento

Na topologia lógica barramento (ou barramento lógico), os dados são transmitidos simultaneamente para todos os nós. Esse critério define a topologia lógica barramento. Cada um dos nós verifica os dados recebidos para determinar se é ou não o destino da transmissão. Como qualquer nó pode transmitir a qualquer momento, são necessários mecanismos para controlar o acesso dos nós ao meio de transmissão.

A Figura 10 mostra um exemplo de topologia lógica barramento. O sinal de transmissão referente aos dados (mostrado pelas setas) parte do nó transmissor e segue em todas as direções, para todas as partes do meio de transmissão.

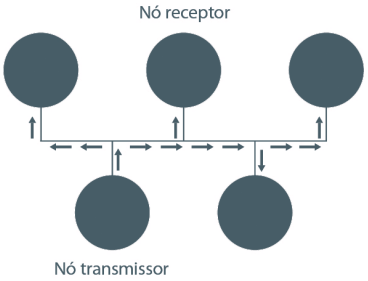

Figura 10 – Topologia lógica barramento
Fonte: Autoria própria (2014).

O método de controle de acesso ao meio de transmissão utilizado na topologia lógica barramento é geralmente um método de contenção, isto é, os nós devem esperar (em estado de contenção) caso esteja ocorrendo uma transmissão.

Quando um nó deseja transmitir, deve-se primeiro verificar se outro nó não está realizando uma transmissão (isto é, se o meio de transmissão não está ocupado). Caso outro nó esteja realizando uma transmissão, o nó que deseja transmitir espera pela conclusão.

Quando o meio se torna livre, o nó em espera inicia a transmissão. Se dois ou mais nós determinarem que o meio está livre e transmitirem simultaneamente, ocorrerá uma colisão. Nesse caso, todos os nós que estão transmitindo detectam a colisão, interrompem a transmissão e esperam passar um tempo aleatório antes de tentar transmitir novamente.

3.3.2 Anel

Na topologia lógica anel (ou anel lógico), os dados são transmitidos em uma direção até que passem em cada um dos nós. Cada nó no anel recebe os dados do nó antecessor e os repete para o nó posterior.

Assim, os dados circulam ao longo do anel através de cada nó até que cheguem ao nó receptor e sejam recebidos. Em seguida, o nó receptor adiciona uma confirmação de recebimento aos dados.

Os dados mais a confirmação continuam a circular ao longo do anel, até retornarem para o nó transmissor, que verifica a confirmação e remove os dados (sinal de transmissão) do anel.

A Figura 11 mostra um exemplo de topologia lógica anel. O sinal de transmissão (mostrado pelas setas) referente aos dados parte do nó transmissor e segue em uma única direção, isto é, em apenas um sentido.

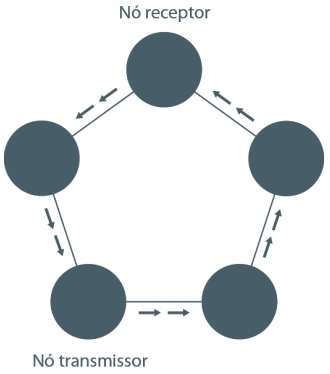

Figura 11 – Topologia lógica anel
Fonte: Autoria própria (2014).

O método de controle de acesso para a topologia lógica anel é quase sempre fundamentado em uma forma de passagem de permissão (*token*). Esse tipo de método também é conhecido como acesso ordenado sem contenção.

Quando um nó deseja transmitir, primeiro deve ser obtida a permissão. Além disso, um nó pode reter a permissão somente por um determinado tempo e depois deve passar a permissão para o próximo nó; quando nenhum nó deseja realizar transmissões, o sinal de transmissão referente à permissão fica circulando no anel.

Quando um nó obtém a permissão, este pode transmitir até que acabe o tempo estabelecido ou até que não tenha mais o que transmitir; em ambos os casos, a permissão deve ser transmitida depois para o próximo nó.

3.3.3 Estrela

Na topologia lógica estrela (ou estrela lógica), as transmissões ficam restritas a uma parte específica do meio de transmissão. Essa restrição do caminho de transmissão é a característica principal que identifica uma topologia lógica estrela.

A Figura 12 apresenta um exemplo de topologia lógica estrela. Nessa figura, o nó central é responsável pelo encaminhamento do sinal de transmissão referente aos dados diretamente entre os dois nós secundários envolvidos, sem que os demais nós tenham conhecimento da transmissão.

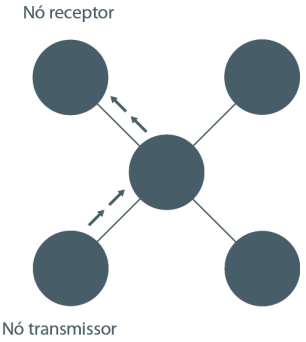

Figura 12 – Topologia lógica estrela
Fonte: Autoria própria (2014).

Na forma básica da topologia lógica estrela, o nó central fornece um caminho de transmissão dedicado para cada nó secundário. Quando um nó realiza uma transmissão para outro nó qualquer, o nó central mantém o sinal de transmissão referente aos dados somente sobre os dois caminhos que conectam o nó transmissor e o nó receptor. Como o meio de transmissão não é compartilhado, não existe a necessidade de mecanismos de controle de acesso.

O nó central é responsável por tomar as decisões de encaminhamento do sinal de transmissão referente aos dados, isto é, para qual dos caminhos disponíveis os dados serão encaminhados. Esses caminhos são geralmente chamados de rotas.

A topologia lógica estrela é um exemplo de como os dados podem ser transmitidos a partir de um nó para outro de maneira diferente da interligação física dos nós, isto é, da topologia física. Assim, uma topologia lógica é fortemente dependente da implementação (software e hardware) dos módulos processadores que formam o sistema de comunicação.

Resumo

A topologia é o padrão no qual a rede de computadores está organizada. As conexões físicas em uma topologia podem ser de dois tipos: ponto a ponto e multiponto. A topologia física de uma rede refere-se à forma como os computadores e as conexões físicas estão organizados. As principais topologias físicas são barramento, anel, estrela e malha irregular. Em uma topologia física na qual o meio de transmissão é compartilhado, é importante a utilização de mecanismos para controlar o acesso ao meio de transmissão. A topologia lógica de uma rede refere-se à maneira como os dados são transmitidos a partir de um computador para outro sem considerar a interligação física. As principais topologias lógicas são barramento, anel e estrela. O controle de acesso em uma topologia lógica pode ser realizado por meio de um método de contenção, como no barramento, ou por um método de passagem de permissão, como no anel. Na estrela (lógica) não existe a necessidade de controle de acesso, pois o meio de transmissão não é compartilhado.

Atividades de aprendizagem

1. O que é topologia?
2. Qual a diferença entre topologia física e topologia lógica?
3. Para uma rede com dez nós interconectados em uma topologia física barramento, qual a quantidade de conexões com o meio de transmissão?
4. Para uma rede com dez nós interconectados em uma topologia física anel, qual a quantidade de conexões com o meio de transmissão?
5. Qual a principal desvantagem da topologia física estrela em relação às topologias barramento e anel?
6. Qual a desvantagem das topologias físicas barramento e anel?
7. Explique o método de controle de acesso geralmente utilizado em uma topologia lógica barramento.
8. Explique o método de controle de acesso geralmente utilizado em uma topologia lógica anel.
9. Por que a topologia lógica estrela não precisa de controle de acesso?

4 ARQUITETURA

Objetivos:

- Compreender os conceitos relacionados à arquitetura de redes de computadores;
- Compreender o funcionamento da transmissão por meio de camadas de protocolos;
- Conhecer as principais arquiteturas de rede e a sua relação com as redes locais.

4.1 INTRODUÇÃO

As redes de computadores são sistemas que possuem muitos componentes diferentes. A tarefa de permitir a comunicação entre aplicações executadas em computadores distintos envolve uma série de detalhes que devem ser cuidadosamente observados para que esta comunicação ocorra de maneira precisa, segura e livre de erros. São exemplos desses detalhes:

a) sinalização dos bits para o envio através do meio de transmissão;

b) detecção e correção de erros de transmissão, pois a maioria dos meios de transmissão é passível de interferências;

c) endereçamento de computadores e de dispositivos de rede;

d) roteamento dos pacotes de dados, desde sua origem até o seu destino, podendo passar por várias redes intermediárias;

e) tratamento da sintaxe e semântica da informação, de modo que a aplicação possa entender os dados recebidos da maneira como foram transmitidos pela aplicação.

As redes de computadores modernas são projetadas de forma altamente estruturada. Da experiência obtida no projeto de redes, vários princípios surgiram, permitindo que novos projetos fossem desenvolvidos de uma forma mais estruturada que os anteriores. Neste capítulo são apresentados alguns desses princípios, que são importantes para o estudo de redes de computadores, em particular, de redes locais. Além disso, também serão apresentadas algumas arquiteturas de rede e conceitos relacionados que serão usados depois como referência para a introdução dos protocolos e arquiteturas abordadas em outros capítulos.

4.2 ARQUITETURA DE CAMADAS

Para reduzir a complexidade do projeto, a maioria das redes de computadores é estruturada em uma série de camadas (ou níveis), cada camada desempenhando uma função específica dentro do objetivo maior, que é a comunicação entre aplicações de computadores distintos. As camadas são construídas umas sobre as outras, cada qual oferece seus serviços para as camadas superiores, ocultando os detalhes de como os serviços oferecidos são implementados de fato (TANENBAUM; WETHERALL, 2011).

A-Z

Glossário: Serviço é um conjunto de funções oferecido por uma camada *n* (provedora) para a camada *n* + 1 (usuária). O serviço define as operações que a camada está preparada para executar e atender seus usuários.

Uma arquitetura de camadas permite o trabalho com uma parte específica e bem definida de um sistema grande e complexo (KUROSE; ROSS, 2013). Essa divisão em camadas torna muito mais fácil modificar a implementação do serviço prestado pela camada.

Portanto, desde que uma camada forneça o mesmo serviço para a camada acima dela e use os mesmos serviços da camada abaixo dela, o restante do sistema permanece inalterado quando a sua implementação é modificada, a exemplo da substituição de cabos de fio de cobre por fibras ópticas. Para sistemas grandes e complexos atualizados com frequência, a capacidade de modificar a implementação de um serviço sem afetar outros componentes do sistema é uma vantagem importante do uso de uma arquitetura de camadas.

Uma rede de computadores com dois computadores (origem e destino) e uma arquitetura de cinco camadas é ilustrada na Figura 13.

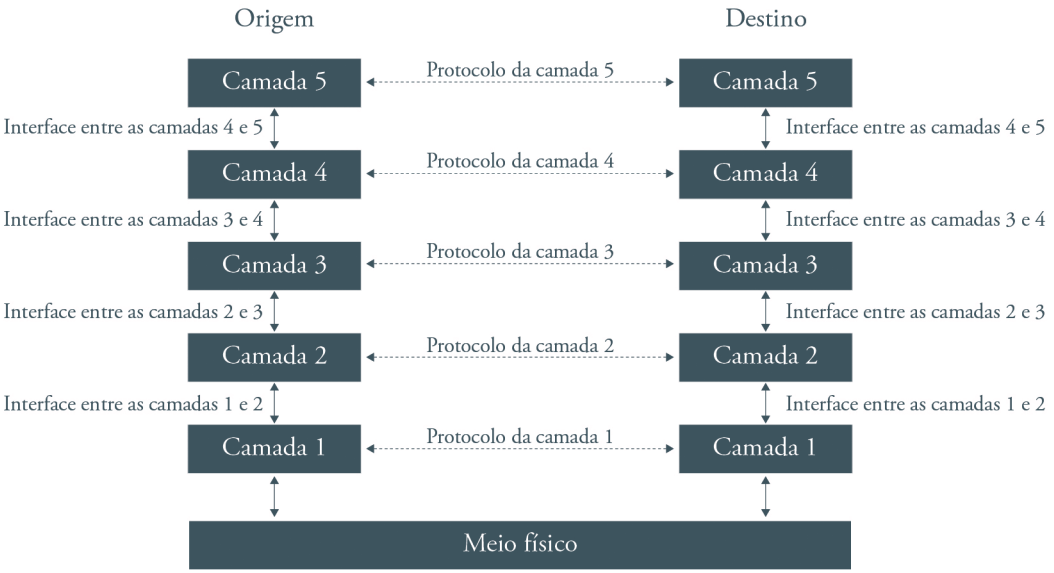

Figura 13 – Uma rede de computadores com dois computadores e uma arquitetura de cinco camadas
Fonte: Adaptado de Tanenbaum e Wetherall (2011, p. 18).

A camada *n* de um computador se comunica com a camada *n* de outro computador. As regras e convenções utilizadas nessa comunicação são chamadas de protocolo da camada *n*.

As funções de cada camada são executadas por entidades. Uma entidade pode ser uma entidade de software (como um programa ou processo) ou uma entidade de hardware (como um circuito integrado). As entidades de uma mesma camada em diferentes computadores são chamadas de pares. Em outras palavras, são os pares que se comunicam usando o protocolo (TANENBAUM; WETHERALL, 2011).

Na realidade, os dados não são transferidos diretamente da camada *n* do computador de origem para a camada *n* do computador de destino. Em vez disso, cada camada do computador de origem passa os dados e informações de controle para a camada imediatamente abaixo até atingir a última camada. A comunicação de fato ocorre através do meio físico que conecta os dois computadores (origem e destino).

No computador de destino os dados percorrem o caminho inverso, da camada mais inferior para a mais superior, com cada camada retirando e analisando as informações de controle colocadas pela sua camada correspondente no computador de origem. As informações de controle correspondem ao protocolo da camada *n*.

Na Figura 13 existe uma interface entre cada par de camadas adjacentes. A interface define os serviços que são oferecidos por uma camada para a camada imediatamente acima dela. Uma das considerações mais importantes no projeto de uma rede com arquitetura de camadas é a definição de interfaces claras entre as camadas, isto é, cada camada precisa executar um conjunto de funções (serviço) bem definido.

As interfaces bem definidas simplificam a substituição de uma camada por uma implementação completamente diferente, pois a nova implementação para a camada somente precisa oferecer exatamente o mesmo serviço para a camada imediatamente acima dela.

4.3 CAMADAS DE PROTOCOLOS

Os protocolos de uma rede de computadores, assim como o software e o hardware que implementam os protocolos, são organizados em camadas. Um conjunto de camadas de protocolos é chamado de arquitetura de rede (TANENBAUM; WETHERALL, 2011).

A especificação de uma arquitetura deve conter informações suficientes para permitir o desenvolvimento do software ou a construção do hardware referente a cada camada, de modo que os protocolos correspondentes às camadas sejam utilizados corretamente. O conjunto de protocolos utilizados por uma determinada rede de computadores, um protocolo por camada, é chamado de pilha de protocolos.

Na Figura 14 consta um exemplo de como acontece a comunicação entre dois computadores (origem e destino) conectados diretamente por algum meio de transmissão. Essa figura também apresenta o caminho percorrido pelos dados: para baixo na pilha de protocolos do computador de origem, segue como bits pelo meio de transmissão e, então, para cima na pilha de protocolos do computador de destino.

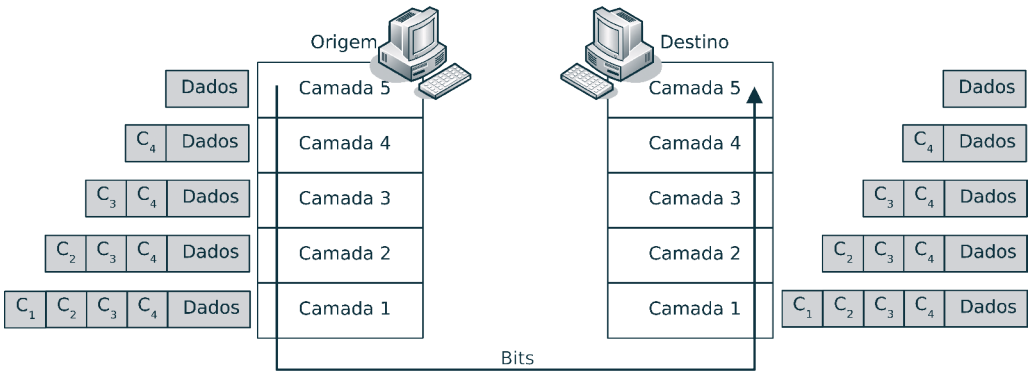

Figura 14 – Exemplo de comunicação em uma rede de computadores com cinco camadas
Fonte: Adaptado de Tanenbaum e Wetherall (2011, p. 20) e de Kurose e Ross (2013, p. 54).

Na Figura 14 também é ilustrado o conceito de encapsulamento (KUROSE; ROSS, 2013). Os dados da Camada 5 no computador de origem são passados para a Camada 4. No caso mais simples, a Camada 4 adiciona um cabeçalho, C_4, com informações de controle que serão utilizadas pela Camada 4 do computador de destino.

Os dados da Camada 5 e o cabeçalho da Camada 4, juntos, constituem a unidade de dados de protocolo (PDU, do inglês *Protocol Data Unit*) da Camada 4, que encapsula os dados da Camada 5. A unidade de dados de protocolo consiste em um bloco de dados transmitido entre duas entidades da mesma camada.

O cabeçalho adicionado por uma camada inclui as informações de controle necessárias para a camada correspondente no computador de destino executar uma fun-

ção relacionada ao protocolo. Por exemplo, entregar os dados para a aplicação adequada ou detectar algum erro que possa ter ocorrido durante a transmissão.

A Camada 4 então passa a sua unidade de dados para a Camada 3, que adiciona o seu cabeçalho, C_3, para criar a unidade de dados do protocolo da Camada 3.

A Camada 3 então passa a sua unidade de dados para a Camada 2 que, por sua vez, adiciona seu cabeçalho, C_2, para criar a unidade de dados do protocolo da Camada 2. Finalmente, esta última unidade de dados é passada para a Camada 1 também incluir o seu cabeçalho, C_1, e realizar a transmissão na forma de bits através do meio físico.

No computador de destino, a transmissão recebida será movida para cima, de camada em camada, com os cabeçalhos sendo retirados e utilizados pela camada correspondente de acordo com o seu protocolo.

O encapsulamento pode ser muito mais complexo do que o descrito anteriormente. Por exemplo, uma quantidade grande de dados da Camada 5 pode ser dividida em partes pela Camada 4 segundo o seu protocolo. No computador de destino, cada uma das partes individuais deve ser reunida para reconstruir os dados da Camada 5.

Adicionalmente, a Camada 3 também pode dividir a unidade de dados passada pela Camada 4 de acordo com o seu próprio protocolo. Resumindo, o encapsulamento significa que cada unidade de dados de uma camada do computador de origem contém informações de controle que são utilizadas pela camada correspondente no computador de destino.

4.4 ARQUITETURAS DE REDE

A quantidade e o nome das camadas, o conjunto de funções, os serviços oferecidos e o protocolo de cada camada variam de uma arquitetura de rede para outra. As primeiras arquiteturas de rede foram desenvolvidas por fabricantes de equipamentos que desenvolviam soluções para a interconexão apenas de seus produtos, sem a preocupação com a compatibilidade de comunicação com os equipamentos de outros fabricantes; por exemplo, a IBM, com a arquitetura de rede SNA e a *Digital Equipment Corporation* (DEC), com a *Digital Network Architecture* (DNA). Essas arquiteturas de rede são denominadas arquiteturas proprietárias porque são controladas por uma única organização: o fabricante.

As arquiteturas de rede proprietárias não eram uma boa solução porque seu objetivo era permitir o intercâmbio de informações entre computadores de um mesmo fabricante enquanto que o conjunto de computadores instalado na maioria das organizações era composto de equipamentos de fornecedores distintos. Assim, era necessário definir uma arquitetura aberta para permitir o intercâmbio de informações entre computadores de fabricantes diferentes.

Nas duas subseções seguintes são brevemente descritas duas arquiteturas de rede importantes: O Modelo de Referência OSI e a arquitetura TCP/IP. O objetivo principal é estabelecer uma relação dessas arquiteturas de rede com as redes locais de computadores.

4.4.1 Modelo OSI

O Modelo de Referência OSI, normalmente citado como modelo OSI, propõe uma estrutura com sete camadas, conforme ilustrado na Figura 15. O modelo OSI foi definido com base em uma proposta desenvolvida pela *International Standards Organization* (ISO), como um primeiro passo na direção da padronização internacional dos protocolos utilizados em arquiteturas de rede em camadas (TANENBAUM; WETHERALL, 2011). O nome do modelo é uma referência à interconexão de sistemas abertos, isto é, sistemas que estão abertos à comunicação com outros sistemas.

Figura 15 – Modelo de Referência OSI
Fonte: Adaptado de Comer (2006, p. 103).

O modelo OSI isolado não define uma arquitetura de rede, porque não especifica os serviços e os protocolos de cada camada. Em vez disso, o modelo apenas informa as funções de cada camada. No entanto, a ISO produziu padrões para todas as camadas, publicados como padrões internacionais distintos e não pertencem diretamente ao modelo de referência.

As principais funções das sete camadas do modelo OSI são:

a) camada 7 – Aplicação: fornece acesso a serviços especializados que são utilizados pelos aplicativos do usuário final. Por exemplo, serviços de transferência de arquivos e de correio eletrônico. A unidade de dados intercambiada (isto é, transferida da camada na origem para a camada correspondente no destino) é chamada de Unidade de Dados do Protocolo de Aplicação (APDU, do inglês *Application Protocol Data Unit*);

b) camada 6 – Apresentação: fornece serviços para fazer o tratamento da sintaxe (formato) e da semântica (significado) das informações transmitidas. Por exemplo, serviços de conversão entre codificações diferentes, compressão de dados e de criptografia. A unidade de dados é chamada de Unidade de Dados do Protocolo de Apresentação (PPDU, do inglês *Presentation Protocol Data Unit*);

c) camada 5 – Sessão: fornece serviços para permitir que duas aplicações em computadores diferentes estabeleçam uma sessão de comunicação. Por exemplo, serviços de gerenciamento de sessão e de sincronização. A unidade de dados é chamada de Unidade de Dados do Protocolo de Sessão (SPDU, do inglês *Session Protocol Data Unit*);

d) camada 4 – Transporte: fornece acesso a serviços para garantir que os dados transmitidos cheguem ao seu destino com integridade. Por exemplo, mecanismos de estabelecimento de conexão, multiplexação, controle de fluxo e de correção de erros. A unidade de dados é chamada de Unidade de Dados do Protocolo de Transporte (TPDU, do inglês *Transport Protocol Data Unit*);

e) camada 3 – Rede: fornece serviços para controlar a operação da rede entre a origem e o destino, considerando as conexões intermediárias. Por exemplo, serviços de endereçamento (global), roteamento e de controle de congestionamento. A unidade de dados é chamada de Pacote (*packet*);

f) camada 2 – Enlace de Dados: fornece serviços para garantir que os dados transmitidos de um computador cheguem com integridade ao outro computador conectado diretamente. Por exemplo, serviços de endereçamento (local), controle de fluxo e de correção de erros. A unidade de dados é chamada de Quadro (*frame*);

g) camada 1 – Física: abrange especificações mecânicas, elétricas e físicas para fornecer serviços de transmissão e recepção de bits através de um meio físico (canal de comunicação). Por exemplo, serviços de codificação e decodificação de símbolos e caracteres em sinais que serão transportados pelo meio físico. A unidade de dados é o Bit.

O modelo OSI foi projetado inicialmente para uso em redes de longa distância (WANs) que utilizam principalmente conexões ponto a ponto. Quando surgiram as redes locais (LANs), o modelo teve de ser ajustado para permitir a adequação das diferenças.

Portanto, a aplicabilidade do modelo OSI em redes locais não pôde deixar de considerar as características dessas redes.

As redes locais possuem características que afetam principalmente as camadas mais baixas do modelo OSI (física e de enlace de dados). Essas camadas podem considerar as características de redes locais como distância limitada, alto desempenho, baixa taxa de erros e encaminhamento de dados simples (em geral único).

Devido à distância limitada, o meio de transmissão utilizado em redes locais permite alto desempenho e baixa taxa de erros. Assim, não é necessária (na camada de enlace de dados) a introdução de bits adicionais para a correção de erros. Além disso, muitas vezes, nem a recuperação por retransmissão é desejável, considerando que os requisitos de tempo real são bem mais importantes para algumas aplicações do que um excesso de confiabilidade da transmissão.

Por essas razões, no protocolo da camada de enlace de dados, pode ser implementado apenas um esforço máximo para entregar os dados da camada superior sem erros, mas não a sua recuperação caso algum erro ocorra (por exemplo, a recuperação por meio de retransmissão devido à ausência de confirmação de recebimento).

Em redes locais, as regras que disciplinam o acesso compartilhado ao meio físico para a transmissão de dados são chamadas de protocolo de controle de acesso ao meio. Em geral, a transmissão dos dados é feita por difusão (*broadcast*) (todas as estações recebem os dados), ou possuem encaminhamento único (por exemplo, as redes com topologia lógica anel).

Portanto, os protocolos de controle de acesso ao meio poderiam ser colocados na camada de enlace de dados, uma vez que tratam do envio de dados de um computador para outro, mas poderiam ser igualmente colocados na camada de rede, uma vez que se trata do envio de dados do computador de origem para o destino.

Os comitês de padronização colocam esses protocolos como parte da camada de enlace de dados (como será verificado no Capítulo 5). O objetivo é liberar a camada de rede para sua função principal: enviar dados da origem para o destino considerando as conexões intermediárias.

4.4.2 Arquitetura TCP/IP

A existência simultânea de várias redes heterogêneas, locais e de longa distância, tornou necessário definir arquiteturas direcionadas para a interconexão dessas redes. Uma arquitetura importante no contexto de interconexão de redes heterogêneas é a arquitetura da internet (Figura 16), construída com base em um conjunto de protocolos. Essa arquitetura tornou-se conhecida como TCP/IP devido a seus dois principais protocolos: TCP e IP.

Figura 16 – Arquitetura TCP/IP
Fonte: Adaptado de Comer (2006, p. 105).

A arquitetura TCP/IP é composta por quatro camadas, cujas principais funções são:

a) camada de aplicação: contém protocolos de alto nível utilizados pelas aplicações do usuário (por exemplo: protocolos *HyperText Transfer Protocol* – HTTP –, *Simple Mail Transfer Protocol* – SMTP –, *File Transfer Protocol* – FTP –, *Simple Network Management Protocol* – SNMP –, TELNET). A unidade de dados é chamada de mensagem (*message*);
b) camada de transporte: contém protocolos para permitir a comunicação fim a fim entre origem e destino (por exemplo: protocolos TCP e *User Datagram Protocol* – UDP). A unidade de dados é chamada de segmento (*segment*);

c) camada de internet: contém protocolos para a transferência de dados através de redes intermediárias, desde a origem até o destino (por exemplo: protocolos IP, *Internet Group Management Protocol* – IGMP –, *Internet Control Message Protocol* – ICMP – e *Address Resolution Protocol* – ARP). A unidade de dados é chamada de datagrama (*datagram*);

d) camada de interface de rede: não contém protocolos específicos, apenas indica que deve existir uma interface compatível com a tecnologia de rede utilizada para a transmissão da unidade de dados do protocolo IP.

O foco da arquitetura TCP/IP é a interconexão de diferentes tecnologias de redes (COMER, 2006). A ideia subjacente a essa arquitetura é que não existe nenhuma tecnologia de rede que atenda aos anseios de todos os usuários. Alguns usuários precisam de redes de alta velocidade que normalmente cobrem uma área geográfica restrita.

Outros usuários ficam satisfeitos com redes de baixa velocidade que conectam equipamentos distantes milhares de quilômetros uns dos outros. Portanto, a maneira de permitir que todos esses usuários possam trocar informações é interconectar as diferentes redes às quais eles estão conectados, formando uma internet ou rede interligada. O termo **internet** é utilizado nesse caso em um sentido genérico, embora a camada de internet esteja presente na internet (a rede mundial de computadores) (TANENBAUM; WETHERALL, 2011).

A arquitetura TCP/IP não faz nenhuma restrição às redes (locais ou de longa distância) que são interconectadas para formar a internet. Portanto, qualquer tipo de rede pode ser utilizado, desde que seja desenvolvida uma interface que compatibilize a tecnologia de rede específica com o protocolo IP.

Essa compatibilização é a função da camada de interface de rede, que recebe os datagramas IP da camada de internet e os transmite através de uma rede específica (seja local ou de longa distância). Para realizar essa tarefa, nessa camada, os endereços IP, que são endereços lógicos, são traduzidos para os endereços físicos dos computadores e outros dispositivos conectados à rede.

Resumo

Neste capítulo foram apresentados alguns dos princípios do projeto de redes de computadores, como o de arquitetura de camadas e o de camadas de protocolos, que são importantes para o estudo das redes, em particular, de redes locais. A arquitetura em camadas é importante para reduzir a complexidade do projeto de redes de computadores e permitir o trabalho com uma parte específica e bem definida. O conjunto de protocolos utilizados por uma determinada rede de computadores é organizado em camadas, formando camadas de protocolos. Um conjunto de camadas de protocolos é chamado de arquitetura de rede. Neste capítulo, também foram apresentadas brevemente duas arquiteturas de rede importantes: o Modelo de Referência OSI e a Arquitetura TCP/IP. Essas duas arquiteturas são usadas posteriormente como referência para a introdução dos protocolos e arquiteturas abordadas em outros capítulos.

Atividades de aprendizagem

1. Por que as redes de computadores modernas são projetadas utilizando uma arquitetura em camadas?
2. Explique a capacidade de uma arquitetura de camadas de modificar a implementação de um serviço sem afetar outros componentes do sistema.
3. O que são entidades pares?
4. Como os dados são transferidos de uma camada do computador de origem para a mesma camada no computador de destino?
5. O que é uma arquitetura de rede?
6. Explique o conceito de encapsulamento em uma rede de computadores que utiliza o princípio de camadas de protocolos.
7. O que é o Modelo de Referência OSI?
8. Qual a relação do modelo OSI com as redes locais?
9. O que é a Arquitetura TCP/IP?
10. Qual a relação da arquitetura TCP/IP com as redes locais?

5 PADRÃO IEEE 802

Objetivos:

- Conhecer a arquitetura do padrão IEEE 802;
- Compreender o formato da unidade de dados do padrão IEEE 802.3;
- Compreender o funcionamento do protocolo de controle de acesso ao meio de transmissão do padrão 802.3.

5.1 HISTÓRICO

O Projeto IEEE 802 nasceu com o objetivo de elaborar padrões para redes locais de computadores e ficou a cargo de um comitê instituído em fevereiro de 1980 pelo *Institute of Electrical and Electronics Engineers* (IEEE) (SOARES; LEMOS; COLCHER, 1995). O comitê publicou um conjunto de padrões, adotados como padrões nacionais americanos pelo ANSI. Esses padrões foram posteriormente revisados e republicados como padrões internacionais pela ISO com a designação ISO 8802.

O modelo de referência elaborado pelo comitê responsável pelo Projeto IEEE 802 define uma arquitetura com três camadas. Para entender esse modelo é preciso observar que as funções de comunicação mínimas e essenciais de uma rede local correspondem às camadas 1 (física) e 2 (enlace de dados) do modelo OSI.

Essas funções incluem:

a) fornecer um ou mais pontos de acesso aos serviços (SAPs, do inglês *Service Access Points*) disponíveis para os usuários (camadas superiores);

b) na transmissão, montar os dados a serem transmitidos em quadros com campos de endereço e para detecção de erros;

c) na recepção, desmontar os quadros, efetuando o reconhecimento de endereço e a detecção de erros;

d) gerenciar a comunicação no enlace.

Essas quatro funções são fornecidas pela camada de enlace de dados do modelo OSI. A primeira função e as subfunções relacionadas foram agrupadas na camada Controle de Enlace Lógico (LLC, do inglês *Logical Link Control*).

As três restantes foram tratadas em uma camada separada, chamada controle de acesso ao meio (MAC, do inglês *Medium Access Control*). Essa divisão teve como objetivo permitir a definição de várias opções para a camada MAC, que podem então ser adaptadas para as diferentes tecnologias de redes locais, mantendo uma interface única para os usuários dos serviços da rede local, a interface da camada LLC.

Em um nível mais baixo estão as funções normalmente associadas à camada física: a codificação/decodificação de sinais, geração e remoção de preâmbulos para sincronização e a transmissão/recepção de bits. Como no modelo OSI, essas funções foram atribuídas à camada física no modelo de referência elaborado pelo comitê responsável pelo Projeto IEEE 802.

Na Figura 17 é apresentada a relação entre o modelo OSI e alguns dos principais padrões definidos pelo Projeto IEEE 802. O padrão IEEE 802.1 é um documento que descreve o relacionamento entre os diversos padrões IEEE 802 e o relacionamento destes com o modelo OSI.

Esse documento também contém padrões para gerenciamento da rede e informações para a interconexão de redes. O padrão 802.2 descreve a subcamada superior da camada de enlace de dados, que utiliza o protocolo LLC.

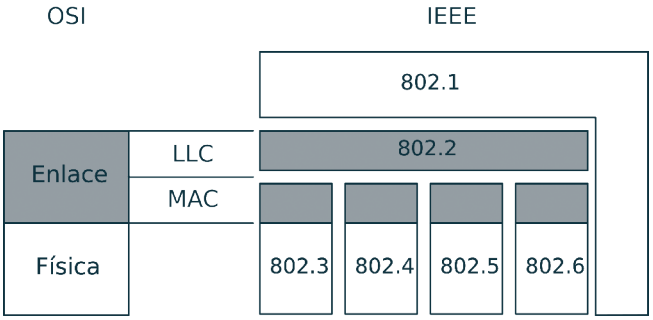

Figura 17 – Relação entre os padrões IEEE 802 e o modelo OSI/ISO
Fonte: Soares, Lemos e Colcher (1995, p. 141).

Os outros padrões que aparecem na Figura 17 especificam as diferentes opções para a camada física e os protocolos da subcamada MAC para diferentes tecnologias de redes locais:

a) padrão IEEE 802.3 (ISO 8802/3): rede em barramento utilizando contenção (espera) como método de controle de acesso;
b) padrão IEEE 802.4 (ISO 8802/4): rede em barramento utilizando passagem de permissão como método de controle de acesso;
c) padrão IEEE 802.5 (ISO 8802/5): rede em anel utilizando passagem de permissão como método de controle de acesso;
d) padrão IEEE 802.6 (ISO 8802/6): rede em barramento utilizando filas como método de controle de acesso.

Na próxima seção são apresentadas algumas considerações sobre o padrão 802.3 por causa da sua importância. Os demais padrões não serão apresentados porque estão inativos ou são considerados obsoletos (TANENBAUM; WETHERALL, 2011).

5.2 PADRÃO IEEE 802.3

O IEEE 802.3 (ISO 8802/3) é o padrão para redes locais em barramento utilizando como base o protocolo *Carrier Sense Multiple Access with Collision Detection* (CSMA/CD) como método de controle de acesso ao meio de transmissão. O padrão IEEE 802.3 foi definido com base no padrão *Ethernet* de 10 Mbps criado pela Xerox, DEC e Intel (TANENBAUM; WETHERALL, 2011).

O formato do quadro da subcamada MAC do padrão IEEE 802.3 é mostrado na Figura 18. Resumindo, esse formato define a sintaxe do protocolo da subcamada MAC do padrão IEEE 802.3, isto é, define os campos que contêm dados e outras informações de controle utilizadas pelo protocolo, assim como a maneira como são codificados.

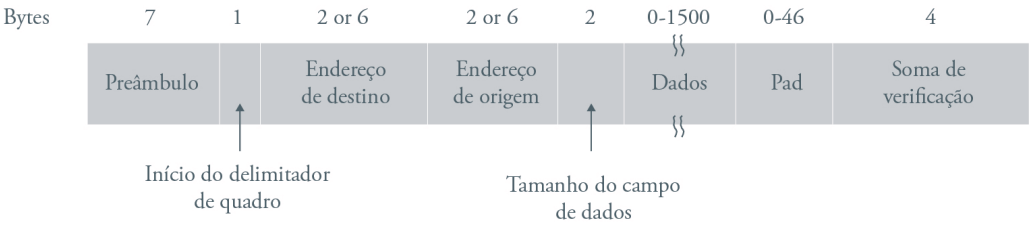

Figura 18 – Formato do quadro da subcamada MAC do padrão IEEE 802.3
Fonte: Tanenbaum (1997, p. 320).

Os campos existentes no quadro são os seguintes:

a) preâmbulo: o campo preâmbulo é utilizado para a sincronização entre o transmissor e o receptor de acordo com a codificação para a transmissão física dos bits utilizada pelo padrão;

b) início do delimitador de quadro: corresponde ao byte 10101011 e indica o início de um quadro;

c) endereço de destino: corresponde ao endereço do receptor do quadro;

d) endereço de origem: corresponde ao endereço do transmissor do quadro;

e) tamanho do campo de dados: indica quantos bytes existem no campo de dados;

f) dados: contém os dados enviados pela subcamada LLC;

g) enchimento (*pad*): é utilizado para preencher o quadro até o tamanho mínimo definido pelo padrão;

h) soma de verificação: contém o código para o controle de correção de erros.

A semântica do protocolo da subcamada MAC do padrão IEEE 802.3 segue exatamente o especificado pelo método de controle de acesso CSMA/CD. Basicamente, quando uma estação deseja transmitir um quadro, esta deve verificar o meio de transmissão; se o meio de transmissão estiver ocupado, a estação aguardará até que este fique livre; caso contrário, a estação começará a transmissão imediatamente.

Caso duas ou mais estações começarem a transmitir simultaneamente em um meio de transmissão desocupado, haverá uma colisão. Nesse caso, todas as estações interrompem as suas transmissões, aguardam durante um tempo aleatório e repetem o processo inteiro novamente (TANENBAUM; WETHERALL, 2011).

O termo colisão, quando utilizado, faz parecer que algo de errado está ocorrendo com a rede. No entanto, a colisão é um processo normal e desejável, pois é parte do funcionamento do método CSMA/CD. Como cada estação gerará um valor aleatório diferente para o tempo de espera, possivelmente não ocorrerá novamente outra colisão, pois uma estação começará a sua transmissão antes e as demais verificarão que o meio de transmissão está ocupado.

O problema é que sempre existe a possibilidade de haver novas colisões, caso outras estações que não estavam envolvidas na primeira colisão tentem uma transmissão justamente no mesmo momento em que terminou o tempo de espera de uma das estações envolvidas na colisão. No padrão IEEE 802.3, o tempo aleatório quando ocorre uma colisão é determinado por um algoritmo chamado de recuo binário exponencial (*binary exponential backoff*) (TANENBAUM; WETHERALL, 2011).

Depois de uma colisão, o tempo é dividido em períodos (*slots*) distintos, cujo tamanho está relacionado ao tempo de propagação no meio de transmissão. Depois da primeira colisão, cada estação espera 0 ou 1 período de tempo antes de tentar novamente.

Se duas estações colidirem e selecionarem o mesmo número aleatório, ocorrerá novamente uma colisão. Depois da segunda colisão, cada uma das estações seleciona aleatoriamente 0, 1, 2 ou 3 e aguarda durante esse número de períodos de tempo. Se ocorrer uma terceira colisão, na próxima vez, o número de períodos de tempo será escolhido aleatoriamente dentro do intervalo de 0 a $2^3 - 1$.

Em geral, depois de *i* colisões, é escolhido um número aleatório entre 0 e $2^i - 1$, que fornece o próximo número de períodos de tempo no qual haverá uma nova tentativa de transmissão. Entretanto, após dez colisões, o intervalo para escolha aleatória do número é congelado em um máximo de 1.023 períodos de tempo. Depois de 16 colisões, o adaptador de rede (hardware) informa o erro para a camada superior, que deverá ser responsável pela recuperação. A relação entre o número de colisões seguidas e o número de períodos de tempo é apresentada na Tabela 1.

Tabela 1 – Tempo aleatório no algoritmo recuo binário exponencial

Número de colisões seguidas	Número de períodos de tempo
1	0 ... 1
2	0 ... 3
i	0 ... 2^i-1
10 ...	0 ... 1023
16	falha

Fonte: Adaptado de Tanenbaum e Wetherall (2011, p. 285).

Esse algoritmo é escolhido para adaptar ao número de estações que estão tentando realizar uma transmissão. Aumentando exponencialmente o intervalo para escolha aleatória do tempo de espera à medida que cada vez mais colisões ocorram, o algoritmo assegura um pequeno retardo quando ocorrer colisões com poucas estações, mas também que as colisões serão resolvidas em um intervalo razoável quando ocorrer colisões com muitas estações.

Mídias integradas: Assista às animações sobre a rede local *Ethernet* disponíveis em <http://www.datacottage.com/nch/eoperation.htm>. Demonstre que você entendeu as animações, descrevendo o método de controle de acesso utilizado.

O padrão IEEE 802.3 define várias opções de meio físico e taxa de transmissão.

Essas opções são especificadas da seguinte forma (SOARES; LEMOS; COLCHER, 1995): <taxa de transmissão em Mbps><técnica de sinalização><tamanho máximo do segmento x 100>. Por exemplo, a especificação 10Base5 significa que a

taxa de transmissão é de 10 Mbps, a técnica de sinalização é banda básica (*baseband*) e o comprimento máximo do segmento é de 500 metros. As principais especificações definidas para a camada física são apresentadas na Tabela 2.

Tabela 2 – Opções e principais características do padrão IEEE 802.3 para a camada física

Opção	Tipo de cabo	Quantidade máxima de estações	Comprimento máximo do segmento
10Base5	Coaxial grosso	100	500 m
10Base2	Coaxial fino	30	200 m
10Base-T	Par trançado	1.024	100 m
10Base-F	Fibra óptica	1.024	2.000 m

Fonte: Adaptado de Tanenbaum (2003, p. 289).

Resumo

Neste capítulo foi descrito o padrão para redes locais IEEE 802, composto por diversas especificações para redes locais de topologias diferentes. O IEEE 802.3 é o padrão para redes em barramento utilizando CSMA/CD como método de controle de acesso ao meio de transmissão. Para esse padrão foram descritos o formato do quadro e a semântica do protocolo de controle de acesso ao meio de transmissão da subcamada MAC. Além disso, foram apresentadas as principais características referentes à camada física.

Atividades de aprendizagem

1. Qual o objetivo do IEEE ao dividir a camada de enlace de dados em duas subcamadas (LLC e MAC)?

2. Qual a finalidade do campo preâmbulo no padrão IEEE 802.3?

3. Por que, eventualmente, no padrão IEEE 802.3 o campo enchimento (*pad*) deve ser utilizado?

4. Por que ocorrem colisões no padrão IEEE 802.3?

5. Explique o método de tratamento de colisões do padrão IEEE 802.3.

6. Quais as opções para o meio físico de transmissão que são especificadas pelo padrão IEEE 802.3?

6 *ETHERNET*

Objetivos:

- Conhecer a história da *Ethernet*;
- Compreender o princípio proposto pela *Ethernet* original;
- Identificar as diferentes tecnologias *Ethernet* de alta velocidade;
- Conhecer os dispositivos de rede *Ethernet*;
- Compreender como são realizadas as interconexões de redes *Ethernet*.

6.1 HISTÓRICO

A *Ethernet* é a tecnologia de rede local mais adotada mundialmente. Na década de 1980 e início da década de 1990, a *Ethernet* enfrentou muitos desafios de outras tecnologias para redes locais, que conseguiram conquistar uma parte do mercado de redes locais durante alguns anos.

No entanto, desde a sua invenção, em meados da década de 1970, a *Ethernet* continuou a se desenvolver e conservou a sua posição dominante no mercado. Atualmente, é considerada a principal tecnologia de rede local com fio e é provável que continue assim por muitos anos (KUROSE; ROSS, 2013; COMER, 2006).

As razões para o sucesso da *Ethernet* são muitas (KUROSE; ROSS, 2013):

a) a *Ethernet* foi a primeira rede local de alta velocidade amplamente disseminada. Os administradores de rede ficaram bastante familiarizados com a *Ethernet* e relutaram em mudar para outras tecnologias de rede local quando estas surgiram no mercado;

b) as outras tecnologias para redes locais são mais complexas e mais caras do que a *Ethernet*. Os administradores de rede ficaram ainda mais desencorajados na questão da mudança;

c) a razão mais interessante para mudar para outra tecnologia de rede local normalmente era obter velocidades mais altas. A *Ethernet* sempre produziu versões que funcionavam a velocidades iguais às de outras tecnologias, ou mais altas;

d) a *Ethernet* se tornou a tecnologia de rede local mais popular do mercado. O hardware para a *Ethernet* se tornou um produto muito comum, de custo muito baixo.

A *Ethernet* original foi inventada em meados da década de 1970 por Bob Metcalfe e David Boggs no PARC, um instituto de pesquisa da Xerox. O desenho esquemático de Metcalfe para a *Ethernet* é mostrado na Figura 19. Nessa figura é possível notar que a *Ethernet* original utilizava um barramento para interconectar os nós da rede. A *Ethernet* de Metcalfe e Boggs executava a 2,94 Mbps e interligava até 256 estações a distâncias de até 1,5 km.

O termo **ether** era usado para descrever o meio de transmissão dos sinais em um sistema. Na proposta original, o **ether** era um cabo coaxial, mas em outros padrões poderia ser usado um cabo de fibra óptica, ou mesmo ondas eletromagnéticas, no caso das redes sem fio.

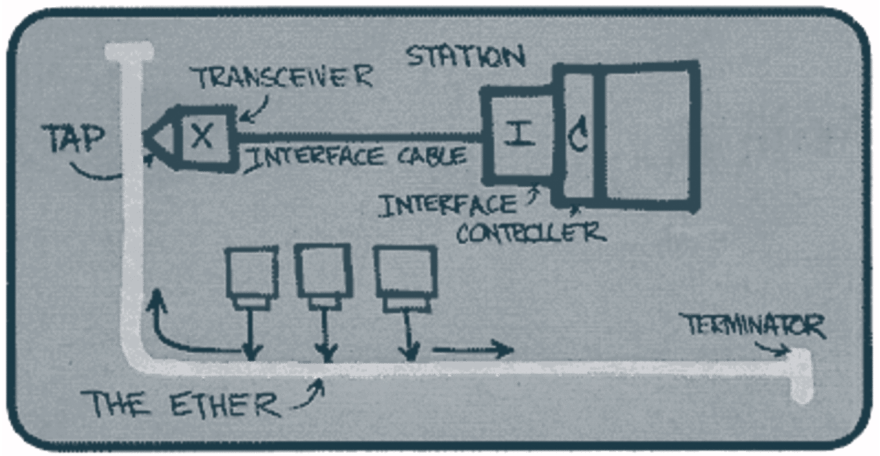

Figura 19 – O projeto original de Metcalfe que levou ao padrão *Ethernet*
Fonte: Kurose e Ross (2006, p. 356).

O termo foi escolhido para enfatizar que o padrão *Ethernet* não era dependente do meio de transmissão e podia ser adaptado para trabalhar com outras mídias.

Em 1978, com o aval de Metcalfe, a Xerox, a Intel e a Digital padronizaram a *Ethernet* de 10 Mbps como um padrão ratificado pelo IEEE usando o número 802.3. A Xerox não demonstrou muito interesse em comercializar a *Ethernet*. Em 1979, Metcalfe abriu sua própria empresa, a 3Com, para desenvolver e comercializar tecnologia de rede, incluindo a tecnologia *Ethernet*. A 3Com desenvolveu e comercializou adaptadores de rede *Ethernet* no início da década de 1980 para os PCs da IBM, muito populares na época. Metcalfe deixou a 3Com em 1990, quando a empresa tinha dois mil funcionários e 400 milhões de dólares de receita (KUROSE; ROSS, 2013).

A topologia física barramento persistiu durante toda a década de 1980 e por grande parte da década de 1990. Em particular, a tecnologia *Ethernet* 10Base2, com um cabo coaxial fino para o barramento, era muito popular na década de 1990. No entanto, exceto por alguma instalação antiga, quase todas as instalações *Ethernet* posteriores passaram a utilizar a topologia física estrela (Figura 20). O dispositivo no centro da topologia estrela era conhecido como repetidor multiporta (*hub*).

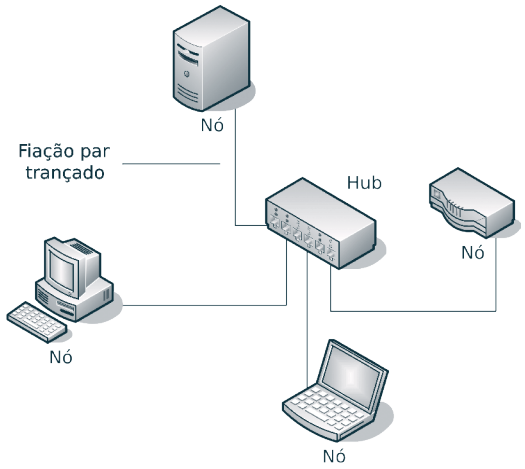

Figura 20 – Ilustração da topologia estrela para *Ethernet* utilizando fiação par trançado
Fonte: Autoria própria (2014).

A tecnologia *Ethernet* passou a permitir que um computador tivesse acesso a uma rede utilizando fios de cobre convencionais não blindados, conhecidos como cabo par trançado. As principais vantagens do uso da fiação de par trançado (conhecida principalmente como cabo de categoria 5) são a redução de custo e a facilidade de instalação (em relação ao cabo coaxial).

A primeira *Ethernet* de par trançado ficou conhecida formalmente como 10Base-T e operava a 10 Mbps, da mesma maneira como a *Ethernet* original com cabo coaxial. Nesse caso, a fiação par trançado era utilizada para conectar cada computador a um *hub* (Figura 20). Do conjunto de oito fios (quatro pares) de um cabo par trançado de categoria 5, somente quatro eram usados: um par para transportar dados do computador para o *hub* e outro para transportar dados do *hub* para o computador.

No final da década de 1970, quando a *Ethernet* foi padronizada, uma rede local operando a 10 Mbps tinha capacidade mais que suficiente para muitos computadores, pois as velocidades dos processadores disponíveis e o hardware dos adaptadores de rede impediam um determinado computador de transmitir dados rapidamente. Na década de 1990, as velocidades dos processadores tinham aumentado muito, assim como o uso

das redes de computadores. Consequentemente, uma *Ethernet* operando a 10 Mbps não tinha capacidade suficiente para atuar como a rede principal (*backbone*) de uma organização. Nesse contexto, a *Ethernet* se tornou um gargalo, isto é, a velocidade da tecnologia *Ethernet* estava comprometendo o desempenho da rede local.

6.2 TECNOLOGIAS *ETHERNET*: *FAST* E *GIGABIT ETHERNET*

As versões mais rápidas da *Ethernet*, comercializadas como *Fast Ethernet* (100 Mbps) e *Gigabit Ethernet* (1 Gbps), foram projetadas para aumentar a vazão (*throughput*) e assim contornar o problema de gargalo. Conhecidas formalmente como 100Base-T e 1000Base-T, as versões mais rápidas utilizam a mesma fiação de par trançado de categoria 5 utilizada para a versão 10Base-T. O aumento na velocidade é obtido usando mais dois fios para transportar dados e alterando o mecanismo de sinalização (COMER, 2006).

Além do *Gigabit Ethernet* por fio de cobre, o IEEE definiu um padrão para *Ethernet* por fibra óptica, conhecido como 1000Base-X. Essa tecnologia converte um quadro *Ethernet* em pulsos de luz, que são transferidos por uma fibra óptica. As principais vantagens da fibra óptica são a maior capacidade de transmissão e a imunidade a interferência elétrica.

Como a capacidade da fibra óptica é suficiente para atingir taxas muito mais altas do que 1 Gbps, estão sendo desenvolvidas tecnologias *Ethernet* de 10 a 40 Gbps.

O aumento da velocidade de transmissão tem dois pontos importantes:

a) embora tenham se tornado mais rápidos, poucos computadores conseguem transmitir dados a uma taxa constante próxima de 1 Gbps;

b) as novas versões da *Ethernet* não mudaram outras partes do padrão (o tamanho máximo do quadro, por exemplo, permanece igual ao do 10Base-T).

Esses dois pontos implicam que as tecnologias *Ethernet* de alta velocidade não foram otimizadas para prover a maior vazão possível entre um par de computadores. Ao invés disso, o projeto é otimizado para permitir mais estações e mais tráfego total.

Depois do desenvolvimento da *Fast Ethernet*, os fabricantes começaram a criar dispositivos de rede que poderiam aceitar uma conexão a 10 ou 100 Mbps, e posteriormente também a 10, 100 ou 1000 Mbps. A tecnologia conhecida como 10/100/1000

Ethernet está disponível para adaptadores e comutadores (*switches*). Além disso, um dispositivo 10/100/1000 negocia automaticamente, quando conectado, para determinar a velocidade máxima que pode ser utilizada pelo outro lado da conexão. Em essência, o hardware envia sinais extras que o outro lado da conexão pode usar para determinar a configuração correta.

A negociação automática e a conservação do formato original do quadro significam que um computador pode ser movido de um *switch Ethernet* de 10 Mbps para um de 1 Gbps sem a necessidade de reconfiguração de software ou de alteração do *driver* de dispositivo. Resumindo, o hardware e o cabeamento das tecnologias *Ethernet* de alta velocidade somente mudam a velocidade com que os quadros podem ser enviados. Assim, as tecnologias *Ethernet* de alta velocidade permitem o intercâmbio dos quadros.

A-Z

Glossário: Driver de Dispositivo é um software que permite ao sistema operacional usar as funcionalidades de um determinado dispositivo.

6.3 PROTOCOLO *ETHERNET*

O protocolo *Ethernet* é um protocolo da camada de enlace de dados para conexão entre computadores (ou estações). Portanto, a *Ethernet* transmite um quadro, isto é, transmite a unidade de dados da camada de enlace de dados (segundo o modelo OSI). O termo quadro (*frame*) advém da comunicação por linhas seriais em que o transmissor **emoldura** os dados acrescentando caracteres especiais antes e depois dos dados transmitidos.

Os quadros *Ethernet* são de tamanho variável, não sendo menores que 64 bytes nem maiores que 1.518 bytes (cabeçalho, dados e soma de verificação). O formato do quadro *Ethernet* é definido pelo padrão IEEE 802.3 conforme a Figura 18 (Capítulo 5).

Cada quadro *Ethernet* contém um campo para o endereço de origem e um campo para o endereço de destino. A *Ethernet* define um endereçamento padrão de 48 bits. Ainda na fábrica, cada adaptador *Ethernet* (ou placa de interface de rede) recebe um número de 48 bits exclusivo, conhecido como endereço *Ethernet* ou endereço MAC. Para atribuir endereços, os fabricantes compram blocos de endereços e atribuem em sequência ao hardware durante a sua fabricação. O endereço é gravado no hardware do

adaptador e não pode ser alterado pelo usuário. Portanto, dois adaptadores não terão o mesmo endereço. O IEEE é responsável pelo controle do espaço de endereços do padrão *Ethernet* (COMER, 2006).

Cada quadro *Ethernet*, além de identificar a origem e o destino, também contém um preâmbulo, campo de tipo, campo de dados e uma soma de verificação. O preâmbulo consiste em 64 bits de 0s e 1s alternados para auxiliar o sincronismo na recepção. O campo de tipo de quadro contém um inteiro de 16 bits que identifica o tipo de dado transportado no quadro (campo de dados).

O software de rede examina esse campo de tipo de quadro de cada quadro recebido para decidir como processar o conteúdo. A soma de verificação é um código *Cyclic Redundancy Check* (CRC) de 32 bits para auxiliar o adaptador a detectar erros de transmissão.

O transmissor calcula o CRC como uma função dos dados do quadro, e o receptor recalcula o CRC e compara os valores para verificar se o quadro foi recebido intacto.

A *Ethernet* foi projetada para ser uma tecnologia de barramento compartilhado, com mecanismo de entrega pelo melhor esforço e com controle de acesso distribuído (COMER, 2006).

O termo **barramento compartilhado** é utilizado porque o meio de transmissão é compartilhado por todas as estações, tornando possível transmitir um quadro para todas as estações ao mesmo tempo.

A **entrega pelo melhor esforço** é utilizada para caracterizar a *Ethernet* porque o hardware não fornece informações ao transmissor sobre a entrega ou não do quadro enviado. Por exemplo, se o computador de destino de uma transmissão for desligado, os quadros enviados para ele serão perdidos e o transmissor não será notificado do ocorrido.

O termo **controle de acesso distribuído** significa que a *Ethernet* não possui autoridade central para conceder acesso ao meio de transmissão, diferentemente de outras tecnologias de rede. O método utilizado para controle de acesso é chamado de acesso múltiplo por detecção de portadora com detecção de colisão (CSMA/CD). O método é CSMA porque várias estações podem ter acesso simultaneamente, e cada estação determina se o meio de transmissão está ocupado, verificando a presença de uma onda portadora (sinal de transmissão).

Quando um adaptador tem um quadro para transmitir, entra em modo de monitoramento para identificar se está ocorrendo uma transmissão, isto é, realiza a verificação de portadora. Se nenhuma transmissão é identificada, o adaptador inicia a transmissão do quadro. Cada transmissão é limitada em duração, pois existe um tamanho máximo de quadro. Além disso, o hardware precisa aguardar um tempo mínimo entre as transmissões, o que significa que nenhum par isolado de estações em comunicação pode usar o meio de transmissão sem oferecer às outras estações uma oportunidade para acesso.

Quando uma estação inicia a transmissão, o sinal não alcança todas as partes do meio de transmissão simultaneamente. Assim, é possível que duas estações verifiquem que o meio está ocioso e comecem uma transmissão simultaneamente.

Quando os dois sinais elétricos se cruzam, eles se misturam e nenhum permanece significativo. Esses incidentes são chamados de colisões.

A *Ethernet* realiza o tratamento das colisões. Cada estação monitora o meio enquanto está transmitindo, para verificar se outro sinal interfere na sua transmissão. Em termos técnicos, o monitoramento é chamado de detecção de colisão (CD).

Quando uma colisão é detectada, o adaptador da estação interrompe a transmissão, espera que a atividade termine e tenta transmitir novamente.

A *Ethernet* também utiliza uma política de contenção para evitar a situação na qual todas as estações tentam transmitir o tempo inteiro, e cada transmissão produz uma colisão. Essa política consiste na espera pelo transmissor de um tempo, chamado de recuo, depois da primeira colisão, dobrando o intervalo de escolha aleatória do tempo se uma segunda tentativa de transmitir também produzir uma colisão, e assim por diante.

A motivação para o emprego desse recuo exponencial é que, se em um dado momento, muitas estações tentarem transmitir simultaneamente, pode haver uma situação de engarrafamento de tráfego. Nessa situação, existe grande probabilidade de duas estações escolherem recuos arbitrários muito próximos. Consequentemente, a probabilidade de outra colisão é alta. Dobrando o intervalo de escolha aleatória do tempo, a estratégia rapidamente espalha as tentativas das estações de transmitir por um período de tempo razoavelmente longo, tornando extremamente pequena a probabilidade de outras colisões.

6.4 DISPOSITIVOS DE REDE *ETHERNET*

Um dispositivo de rede, conforme definido no Capítulo 1, é um equipamento para a comunicação entre os diversos componentes de uma rede local. Os dispositivos mais comuns em redes locais *Ethernet* são os comutadores (*switches*). Atualmente, esses dispositivos são empregados para a interconexão de computadores e para a interconexão de redes locais.

Antes da popularização dos comutadores (*switches*), os dispositivos de rede conhecidos como repetidores (*hubs*) e pontes (*bridges*) eram os dispositivos utilizados para a interconexão de computadores e para a interconexão de redes locais.

Quando foram lançados, os comutadores substituíram os repetidores e pontes porque incorporaram as funcionalidades destes dispositivos: oferecer duas ou mais interfaces (portas) para conectar computadores em uma topologia física estrela, principal funcionalidade de um repetidor; e conectar dois segmentos de rede e encaminhar quadros de um segmento para outro, principal funcionalidade de uma ponte.

Um comutador (*switch*) é um dispositivo que incorpora e estende o conceito de ponte (*bridge*) (COMER, 2006), além de possuir várias conexões, denominadas de portas, para permitir a conexão de estações e dispositivos de rede.

Um comutador usa o endereço de origem e o endereço de destino, contidos no quadro, para tomar decisões de encaminhamento de quadros. O endereço de origem existente no quadro é utilizado para determinar qual computador se conecta a cada porta no comutador e o endereço de destino é utilizado para determinar para qual computador o quadro deve ser enviado.

Cada conexão entre um comutador e uma rede *Ethernet* segue as regras do CSMA/CD, de modo que as colisões e os atrasos de propagação em um segmento permanecem isolados de outro segmento. Como resultado, uma quantidade grande de redes *Ethernet* pode ser conectada utilizando comutadores.

A maioria dos comutadores faz muito mais do que replicar quadros de um segmento para outro; por exemplo, os comutadores tomam decisões inteligentes sobre quais quadros são encaminhados. Em outras palavras, um comutador utiliza os endereços de origem para descobrir quais computadores estão em qual segmento de rede, e combina informações aprendidas com endereços de destino para eliminar o encaminhamento quando necessário. Como não encaminha tráfego desnecessariamente, um comutador auxilia a melhorar o desempenho de uma rede sobrecarregada, isolando o tráfego em segmentos específicos.

Os comutadores funcionam excepcionalmente bem se uma rede puder ser dividida fisicamente em dois segmentos de rede que contêm, em cada um deles, um conjunto de computadores que se comunicam com frequência.

Por exemplo, cada segmento contém um conjunto de estações de trabalho junto com um servidor, e as estações de trabalho direcionam a maior parte do seu tráfego para o servidor.

A maioria dos comutadores comerciais são muito mais sofisticados e robustos do que a descrição que foi apresentada. Os comutadores, quando ligados inicialmente, procuram outros comutadores e descobrem a topologia da rede. Os comutadores utilizam um algoritmo distribuído para decidir como encaminhar os quadros.

Em particular, os comutadores decidem como propagar quadros de difusão (*broadcast*) de modo que somente uma cópia de um quadro *broadcast* seja entregue a cada segmento de rede. Sem esse algoritmo, comutadores conectados em *loop* produziriam resultados indesejáveis, pois encaminhariam quadros de *broadcast* nas duas direções simultaneamente.

Os comutadores também oferecem características para facilitar o gerenciamento de rede (KUROSE; ROSS, 2013). Por exemplo, se um adaptador não está funcionando corretamente e está enviando quadros continuamente, um comutador pode detectar o problema e desconectar internamente o adaptador com defeito. Assim, os administradores de rede não precisam corrigir o problema imediatamente.

A maioria dos comutadores também pode coletar estatísticas sobre o uso da capacidade de transmissão (largura de banda), taxas de colisão, tipos de tráfego, entre outras informações de gerenciamento. Os administradores de rede podem usar essas informações não somente para analisar e corrigir problemas, mas também para planejar como a rede local deverá evoluir no futuro.

6.5 INTERCONEXÃO DE REDES *ETHERNET*

Em geral, as organizações (empresas, universidades, entre outras) são constituídas de muitos departamentos, e cada departamento tem e administra a sua própria rede local *Ethernet*. Naturalmente, uma organização tem interesse na interconexão entre os seus segmentos de redes locais departamentais. Nesta seção será considerada a abordagem de interconexão com *switches Ethernet*.

Na Figura 21 é ilustrado como três departamentos de uma universidade podem interconectar suas redes locais. Nessa figura, cada um dos três departamentos (Engenharia elétrica, Ciência da computação e Engenharia de sistemas) tem um *switch Ethernet* que fornece acesso à rede local para docentes, pessoal administrativo e estudantes do departamento. Cada estação em um departamento tem uma conexão ponto a ponto com o *switch* do departamento. Um quarto *switch*, denominado de *switch* de *backbone*, tem conexões ponto a ponto com os *switches* dos departamentos, interconectando as redes locais dos três departamentos.

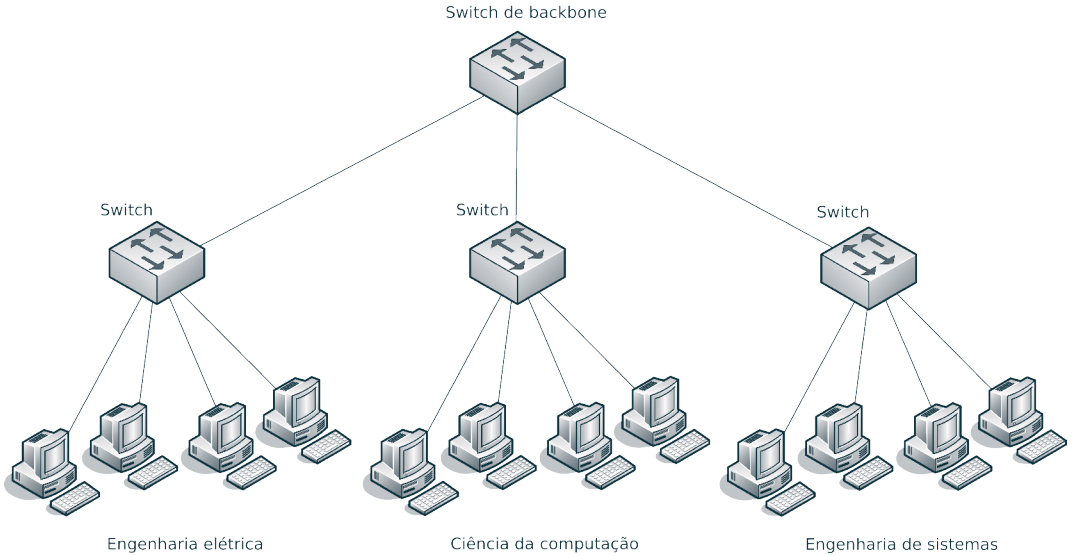

Figura 21 – Três redes locais departamentais interconectadas com um switch
Fonte: Adaptado de Kurose e Ross (2006, p. 366).

O desenho mostrado na Figura 21 é um projeto multinível (ou hierárquico) porque os *switches* estão organizados hierarquicamente (KUROSE; ROSS, 2006; OPPENHEIMER, 1999). Nesse sentido, projetos multiníveis com mais de dois níveis também podem ser criados. Por exemplo, um nível para os departamentos, um nível para as faculdades (faculdade de engenharia, faculdade de administração, entre outras) e um nível mais alto para o câmpus universitário. Em um projeto multinível, o termo **segmento de rede** é empregado para fazer referência a cada uma das redes locais departamentais (isto é, o *switch* e as estações de um mesmo departamento).

Uma rede local departamental interconectada a um *switch* de *backbone* tem muitos benefícios (KUROSE; ROSS, 2006).

Primeiro, a interconexão das redes locais permite a comunicação entre as estações dos vários departamentos.

Segundo, amplia a distância máxima entre qualquer par de estações da rede local. Por exemplo, com uma *Ethernet* a 10 Mbps, a distância máxima entre uma estação e seu *switch* é 100 metros; portanto, para um único segmento de rede, a distância máxima entre qualquer par de estações é de 200 metros. Interconectando os *switches*, essa distância máxima pode ser aumentada, visto que a distância entre *switches* diretamente conectados também pode ser de 100 metros quando são utilizados pares trançados (e ainda maior quando são utilizadas fibras ópticas).

Um terceiro benefício é que o projeto multinível pode evitar determinadas falhas. Especificamente, se qualquer um dos *switches* departamentais começar a funcionar mal, o *switch* de *backbone* poderá detectar o problema e desconectar o switch departamental; desse modo, os departamentos restantes continuam funcionando enquanto o *switch* departamental com problema é reparado ou substituído.

Além desses benefícios, um *switch* pode interconectar diferentes tecnologias *Ethernet*, incluindo as de 10 Mbps, 100 Mbps e de 1 Gbps. Um exemplo de uma rede local que utiliza uma combinação de *switches* de diferentes tecnologias *Ethernet* é mostrado na Figura 22. Nessa rede local, cada um dos três departamentos tem o seu próprio segmento de rede de 10 Mbps com o seu próprio *switch*.

Como cada *switch* de departamento está interconectado com o *switch* utilizado como rede principal (*backbone*), todo o tráfego interdepartamental fica confinado no segmento de rede do departamento. Cada um dos servidores tem acesso dedicado de 100 Mbps com o *switch* de *backbone*. Esse *switch* tem, no mínimo, três interfaces (portas) de 10 Mbps e três interfaces de 100 Mbps (ou seis interfaces de tecnologia 10/100 *Ethernet*). O roteador fornece o acesso à internet e também possui acesso dedicado de 100 Mbps.

Uma maneira de melhorar a vazão total da rede local mostrada na Figura 22 seria substituir o *switch* de *backbone* de 100 Mbps por um *switch* de 1 Gbps. Assim, os pontos da rede mais próximos de gargalo, o roteador e os servidores, seriam beneficiados pelo acesso dedicado de alta velocidade. Além disso, os *switches* de departamento poderiam ser substituídos por switches de maior velocidade para melhorar o acesso das estações. A substituição dos *switches* de departamento poderia ser gradual para evitar um custo alto inicial.

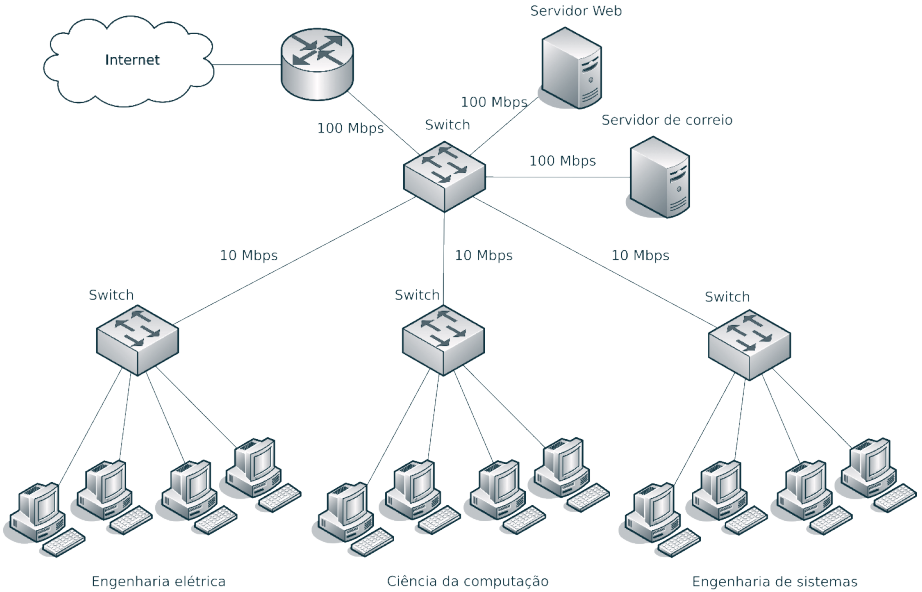

Figura 22 – Exemplo de uma rede local que utiliza uma combinação de switches
Fonte: Adaptado de Kurose e Ross (2006, p. 367).

Resumo

Neste capítulo foi apresentada uma breve história da *Ethernet* com ênfase nas razões para o seu sucesso e na trajetória desde a especificação original que utiliza topologia barramento até as versões mais modernas de topologia estrela com par trançado e que operam em velocidades na ordem de *gigabits*. O protocolo *Ethernet*, CSMA/CD, é fundamentado no acesso múltiplo por detecção de portadora com controle distribuído e detecção de colisão. Os campos do formato de quadro do protocolo *Ethernet* também foram descritos. Ao final do capítulo, as funções dos principais dispositivos de rede *Ethernet* foram descritas e exemplos de interconexão de redes locais foram apresentados e discutidos.

Atividades de aprendizagem

1. Quais as razões para o sucesso da *Ethernet*?
2. Qual topologia física é utilizada pela *Ethernet* original?
3. Quais as vantagens em redes *Ethernet* do uso de cabo par trançado em topologia estrela ao invés de cabo coaxial em topologia barramento?
4. Explique o problema de gargalo que ocorreu na década de 1990 com as redes *Ethernet* operando a 10 Mbps.
5. O que são as tecnologias *Fast Ethernet* e *Gigabit Ethernet*?
6. Qual o objetivo da tecnologia conhecida por 10/100/1000 *Ethernet*?
7. Por que não é possível que dois adaptadores tenham o mesmo endereço *Ethernet*?
8. Qual o método de controle de acesso ao meio utilizado pela *Ethernet*?
9. Como a *Ethernet* realiza o tratamento das colisões?
10. O que é um projeto de rede multinível?
11. Em um projeto multinível, o que é considerado um segmento de rede?
12. Quais as vantagens do uso de um *switch* como rede principal (*backbone*)?

7 REDES LOCAIS SEM FIO

Objetivos:

- Compreender os conceitos relacionados a redes sem fio;
- Identificar os elementos de uma rede local sem fio;
- Conhecer os problemas relacionados aos enlaces sem fio;
- Conhecer a arquitetura e o princípio do protocolo do padrão IEEE 802.11;
- Compreender como são realizadas as interconexões de redes sem fio.

7.1 CONCEITOS

O termo **sem fio** (*wireless*) abrange genericamente todo tipo de tecnologia de comunicação que não utiliza um meio físico sólido para a transmissão de informação, isto é, a transmissão é realizada por ondas eletromagnéticas que se propagam pelo ar (ou mesmo pelo espaço, no caso do uso de satélites) (CYCLADES BRASIL, 2002).

As tecnologias sem fio são utilizadas em diversos tipos de aplicações, como em serviços de voz e mensagem (telefonia celular), radiodifusão (rádio e televisão), sistemas de navegação (GPS, do inglês *Global Positioning System*), uso doméstico (controle remoto de equipamentos), transmissão de dados entre computadores, entre outras aplicações.

O ponto comum a todas as aplicações de tecnologias sem fio é a não competição direta com as tecnologias que utilizam meio físico sólido de comunicação (por exemplo, fio de cobre ou fibra óptica).

As tecnologias sem fio geralmente são aplicadas onde o uso de cabos é inviável economicamente (por exemplo, em regiões rurais ou não atendidas por uma infraestrutura de cabeamento), ou mesmo quando impraticável (por exemplo, em ambientes hostis e edifícios históricos).

Como as tecnologias sem fio têm muitas maneiras de uso em aplicações de comunicação, somente o uso em redes locais sem fio (WLANs, do inglês *Wireless* LANs) é abordado neste capítulo. Além disso, é necessário apresentar alguns conceitos importantes relacionados com as tecnologias sem fio que serão utilizados ao longo deste capítulo.

Um possível cenário para redes locais sem fio é ilustrado na Figura 23. Os seguintes elementos podem ser identificados em uma rede local sem fio (KUROSE; ROSS, 2013):

a) estação sem fio (*wireless station*). As estações são computadores em uma rede local que executam as aplicações dos usuários. Uma estação sem fio pode ser um *notebook* ou *laptop*, *tablet*, telefone celular ou até mesmo um computador de mesa;

b) estação base (*base station*). Uma estação base é responsável pela transmissão de dados para as estações sem fio com as quais está associada. Uma estação sem fio está associada com uma estação base quando a estação sem fio está dentro do alcance de comunicação da estação base (isto é, dentro da sua área de cobertura) e a estação sem fio utiliza a estação base para retransmitir os seus dados para a rede cabeada. As torres

de telefonia celular e os pontos de acesso (APs, do inglês *Access Points*) em redes locais sem fio são exemplos de estação base;

c) enlace sem fio (*wireless link*). Uma estação sem fio se conecta a uma estação base ou a outra estação sem fio por meio de um enlace sem fio. As diferentes tecnologias de enlace sem fio têm taxas de transmissão diferentes e podem transmitir a distâncias diferentes.

Na Figura 23, a estação base (ponto de acesso sem fio) está conectada à rede cabeada, isto é, está conectada à rede empresarial ou residencial ou diretamente à rede telefônica para, por exemplo, ter acesso à internet.

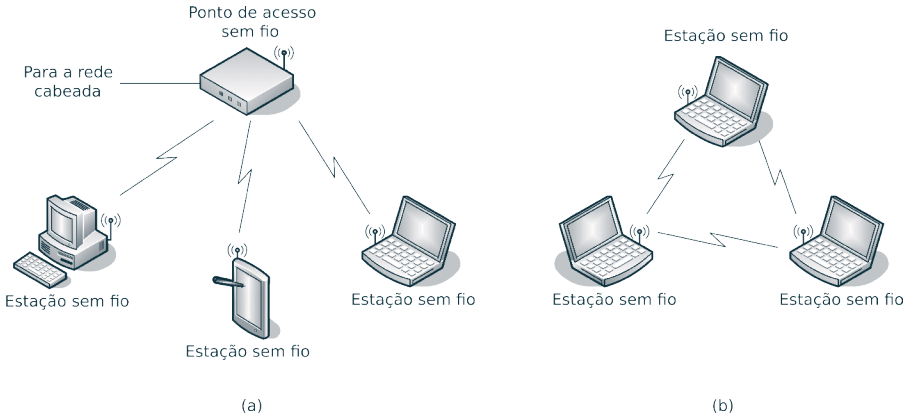

Figura 23 – Cenário para redes locais sem fio: (a) rede local com um ponto de acesso e (b) rede *ad hoc*
Fonte: Adaptado de Tanenbaum e Wetherall (2011, p. 188).

Quando as estações sem fio estão associadas com uma estação base, é comum dizer que estão operando em modo de infraestrutura, uma vez que todos os serviços tradicionais de rede (por exemplo, atribuição de endereço e roteamento) são fornecidos pela rede com a qual estão conectadas por meio da estação base. Nas redes que operam no modo *ad hoc*, as estações sem fio não dispõem de uma infraestrutura desse tipo.

As condições do ambiente complicam continuamente a transmissão em um enlace sem fio, pois variam com cada pequena mudança ocorrida no ambiente. Para identificar as principais características dos enlaces sem fio, considere o seguinte cenário de uma rede cabeada simples: uma rede residencial com estações conectadas a um mesmo comutador (*switch*) *Ethernet* por meio de cabos do tipo par trançado.

Para substituir essa rede cabeada por uma rede sem fio, é necessário trocar cada adaptador de rede das estações por um adaptador sem fio e o comutador por um ponto de acesso; essas alterações acontecem no nível da camada de enlace de dados. Nas demais camadas superiores, nenhuma alteração seria necessária.

Existem algumas diferenças importantes entre um enlace com fio e um enlace sem fio. Essas diferenças, apresentadas a seguir, caracterizam os enlaces sem fio (KUROSE; ROSS, 2013):

a) redução da força do sinal: as irradiações eletromagnéticas são atenuadas quando atravessam algum tipo de matéria (por exemplo, um sinal de rádio ao atravessar uma parede). O sinal se dispersa mesmo ao ar livre, resultando na redução de sua força (às vezes denominada de atenuação de percurso) à medida que aumenta a distância entre transmissor e receptor;

b) interferência de outras fontes: as várias fontes que transmitem na mesma frequência sofrem interferência umas das outras (por exemplo, telefone sem fio e rede local sem fio). Além da interferência de fontes transmissoras, o ruído eletromagnético presente no ambiente pode resultar em interferência (por exemplo, um motor ou um forno de micro-ondas que esteja próximo);

c) 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 transmissor e receptor. Esses **ecos** provocam a alteração do sinal recebido no destino. Além disso, os objetos que se movimentam entre o transmissor e o receptor também podem fazer com que a propagação multivias mude ao longo do tempo.

De acordo com as características dos enlaces sem fio apresentadas anteriormente, os erros de bits são mais comuns em enlaces sem fio do que em enlaces com fio (que utilizam cabeamento).

Portanto, protocolos de enlace sem fio utilizam códigos de detecção de erros por CRC e também técnicas de recuperação de erros com base na retransmissão de quadros corrompidos.

Os erros de bits que podem ocorrer nos quadros não são as únicas diferenças entre um enlace com fio e um enlace sem fio.

Na transmissão por difusão (*broadcast*) em uma rede cabeada, todos os nós recebem as transmissões de todos os outros nós. No caso de enlaces sem fio, podem ocorrer os problemas ilustrados na Figura 24.

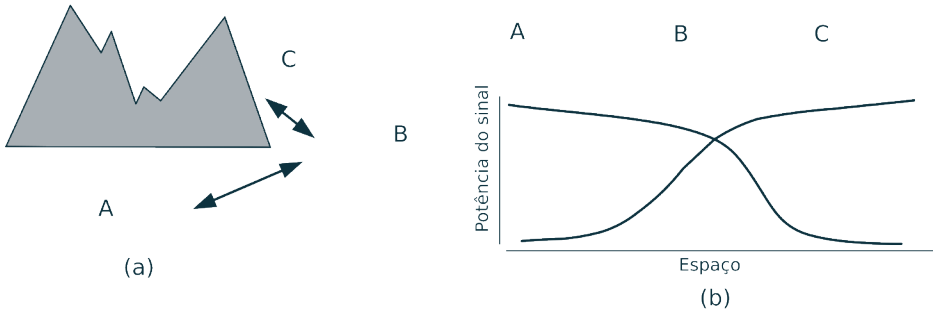

Figura 24 – Problemas em enlaces sem fio: (a) problema do terminal oculto e (b) problema do desvanecimento
Fonte: Adaptado de Kurose e Ross (2013, p. 386).

O problema do terminal oculto e o problema do desvanecimento da força do sinal tornam o controle de acesso ao meio em uma rede sem fio consideravelmente mais complexo do que em uma rede cabeada.

O problema do terminal oculto é ilustrado na Figura 24 (a). Considere que a estação A esteja transmitindo para a estação B. Considere também que a estação C esteja transmitindo para a estação B. As obstruções físicas presentes no ambiente (por exemplo, uma montanha ou paredes de um edifício) podem impedir que A e C escutem as transmissões de um e de outro, mesmo que as transmissões de A e C estejam interferindo em B, isto é, mesmo que esteja ocorrendo uma colisão que é detectada somente por B.

Um segundo cenário que resulta em colisões que não são detectadas é causado pelo desvanecimento da força do sinal à medida que ocorre a propagação pelo meio sem fio. Na Figura 24 (b) é ilustrado o caso em que as estações A e C estão localizadas de maneira que as potências de seus sinais não são suficientes para que detectem as transmissões de um e de outro. No entanto, as potências são suficientemente fortes para interferir uma com a outra na estação B.

7.2 PADRÃO IEEE 802.11

As redes locais sem fio são bastante populares e estão presentes em residências, escritórios, bares, restaurantes, bibliotecas, aeroportos, entre outros locais. Atualmente, as redes locais sem fio são consideradas uma das mais importantes tecnologias de rede de acesso do usuário à internet.

Apesar de muitas tecnologias e padrões para redes locais sem fio tenham sido desenvolvidas na década de 1990, o principal é o padrão IEEE 802.11, também conhecido como *Wi-Fi*. Na realidade, existem diversos padrões IEEE 802.11 para redes locais sem fio, por exemplo: 802.11b, 802.11a, 802.11g e 802.11n. Na Tabela 3 é apresentado um resumo das principais características de alguns dos padrões.

Tabela 3 – Resumo dos padrões IEEE 802.11

Padrão	Faixa de frequência	Taxa de dados	Área de cobertura
802.11b	2,4 – 2,485 GHz	5 – 11 Mbps	10 – 30m
802.11a	5,1 – 5,8 GHz	54 Mbps	(interna)
802.11g	2,4 – 2,485 GHz	54 Mbps	50 – 200m
802.11n	2,4 – 5 GHz	200 Mbps	(externa)

Fonte: Adaptado de Kurose e Ross (2013, p. 383).

Os padrões IEEE 802.11 têm muitas características em comum:

a) os padrões utilizam o mesmo protocolo de controle de acesso ao meio denominado acesso múltiplo por detecção de portadora com prevenção de colisão (CSMA/CA, do inglês CSMA with *Collision Avoidance*);

b) utilizam o mesmo formato para os quadros de camada de enlace de dados;

c) podem reduzir a taxa de transmissão para alcançar distâncias maiores;

d) permitem o modo de infraestrutura e o modo *ad hoc*.

Os padrões apresentam algumas diferenças importantes na camada física:

a) o padrão 802.11b tem uma taxa de transmissão de 11 Mbps, suficiente para a maioria das redes residenciais com acesso à internet por modem a cabo ou *Asynchronus Digital Subscriber Line* (ADSL);

b) o padrão 802.11b opera na faixa de frequência que compete com telefones sem fio e fornos de micro-ondas;

c) o padrão 802.11a funciona com taxas de transmissão significativamente mais altas, mas opera em frequências mais altas, exigindo distâncias mais curtas para um dado nível de potência, além de serem mais suscetíveis à propagação multivias;

d) o padrão 802.11g utiliza a mesma faixa de frequência mais baixa do padrão 802.11b, mas com taxas de transmissão semelhantes às do padrão 802.11a;

e) o padrão 802.11n utiliza duas ou mais antenas no lado transmissor e duas ou mais antenas no lado receptor que podem estar transmitindo/recebendo sinais diferentes; dependendo da modulação utilizada, é possível alcançar taxas de transmissão de centenas de Mbps.

Os produtos que implementam esses padrões estão disponíveis no mercado. Nos próximos anos, as redes locais sem fio de velocidades mais altas deverão alcançar distribuição bem mais significativa (KUROSE; ROSS, 2013).

7.2.1 Arquitetura 802.11

As redes 802.11 podem ser utilizadas em dois modos (TANENBAUM; WETHERALL, 2011):

a) modo de infraestrutura;

b) modo *ad hoc*.

O mais utilizado, o modo de infraestrutura, é formado por uma ou mais estações sem fio e uma estação base. Cada uma das estações é associada à estação base, denominada de ponto de acesso (AP), que por sua vez é conectado a outra rede, por exemplo, uma rede com acesso à internet. As estações enviam e recebem dados por meio do AP.

Em uma rede residencial típica, existe apenas um AP e um roteador (quase sempre acompanhado de um modem ADSL, formando um pacote) que conecta o conjunto à internet. Em uma rede corporativa, diversos APs podem ser interconectados, geralmente por uma rede cabeada, para formar uma única rede local.

O modo *ad hoc* permite a construção de uma rede sem nenhum controle central e sem nenhuma conexão externa. Nesse caso, a rede é formada conforme a necessidade, por equipamentos móveis que, por acaso, estão próximos uns dos outros, têm a necessidade de se comunicar e não dispõem de infraestrutura de rede no local. Por exemplo, uma rede *ad hoc* pode ser formada quando pessoas com computadores portáteis estão reunidas e querem trocar dados.

Embora as redes *ad hoc* tenham despertado grande interesse, estas redes não são muito populares uma vez que o acesso à internet é a principal aplicação para as redes sem fio (TANENBAUM; WETHERALL, 2011). Por essa razão, este capítulo é direcionado para as redes 802.11 operando no modo de infraestrutura.

7.2.2 Protocolo 802.11

Uma estação sem fio, depois de associada com um AP, pode começar a enviar quadros para o AP e receber quadros do AP. No entanto, como várias estações (e o próprio AP) podem querer transmitir quadros ao mesmo tempo sobre o mesmo meio de transmissão, é preciso um protocolo de controle de acesso para coordenar as transmissões.

Devido ao sucesso da *Ethernet* e do seu protocolo de acesso aleatório, os projetistas do padrão IEEE 802.11 escolheram um protocolo também de acesso aleatório denominado acesso múltiplo por detecção de portadora com prevenção de colisão (CSMA/CA).

Do mesmo modo que o CSMA/CD da *Ethernet*, o CSMA de CSMA/CA significa que cada estação realiza o monitoramento do meio de transmissão antes de transmitir e aguarda quando identifica que o meio está ocupado.

Embora ambos os protocolos, *Ethernet* e 802.11, utilizem acesso múltiplo por detecção de portadora, os dois protocolos possuem duas diferenças importantes. Primeiro, ao invés de utilizar detecção de colisão, o protocolo 802.11 utiliza técnicas de prevenção de colisão. Segundo, devido às taxas altas de erros de bits em enlaces sem fio, o protocolo 802.11 emprega um mecanismo de confirmação/retransmissão na camada de enlace de dados.

O protocolo 802.11 não implementa a detecção de colisão devido a duas razões importantes (KUROSE; ROSS, 2013):

a) a capacidade de detectar colisões exige as capacidades de enviar (o próprio sinal da estação) e de receber (para determinar se outra estação está transmitindo) ao mesmo tempo. Como a potência do sinal recebido normalmente é muito pequena em relação à potência do sinal transmitido no adaptador 802.11, o custo para construir um hardware que possa detectar colisões é muito alto;

b) mesmo que o adaptador 802.11 pudesse transmitir e receber ao mesmo tempo (e interromper transmissões quando o meio de transmissão estivesse ocupado), ainda assim não seria capaz de detectar todas as colisões devido ao problema do terminal oculto e ao problema do desvanecimento da força do sinal.

Em um enlace sem fio, um quadro transmitido por uma estação pode não ser recebido intacto por vários motivos (discutidos anteriormente). Para trabalhar com essa probabilidade de falha, o protocolo 802.11 utiliza um mecanismo de confirmação/retransmissão na camada de enlace de dados.

Como ilustrado na Figura 25, quando a estação de destino recebe um quadro de dados intacto (representado na figura por DADOS), esta espera um curto período de tempo, chamado de espaçamento curto interquadros (SIFS, do inglês *Short Inter-Frame Spacing*). Em seguida, devolve um quadro de confirmação (representado na figura por ACK, do inglês *Acknowledgement*).

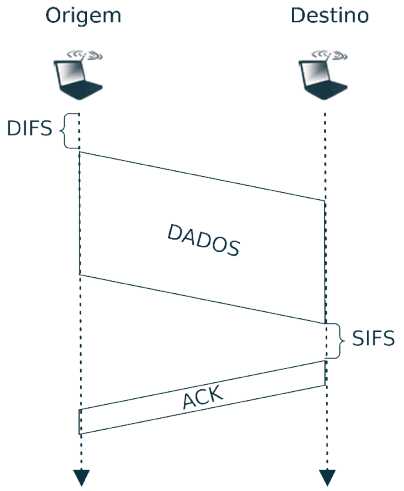

Figura 25 – Confirmação no protocolo 802.11
Fonte: Kurose e Ross (2013, p. 395).

Se a estação de origem não receber uma confirmação dentro de um determinado período de tempo, esta considera que ocorreu um erro e o quadro será retransmitido. Se a estação de origem não receber uma confirmação após um número fixo de retransmissões, esta desiste da transmissão e descarta o quadro.

Uma estação com um quadro para transmitir executa o protocolo CSMA/CA segundo as seguintes etapas (KUROSE; ROSS, 2006):

a) se inicialmente a estação identificar que o meio está ocioso, o quadro será transmitido após um curto período de tempo denominado de espaçamento interquadros distribuído (DIFS, do inglês *Distributed Inter-Frame Spacing*), conforme ilustrado na Figura 25;

b) caso contrário, a estação escolherá um valor aleatório de espera (*backoff*) e fará a contagem regressiva a partir desse valor quando identificar que o meio está ocioso. Se a estação identificar que o meio está ocupado, o valor do contador permanecerá inalterado;

c) quando o contador chegar ao zero, a estação transmitirá o quadro inteiro e então ficará esperando uma confirmação;

d) se receber uma confirmação, a estação de origem saberá que esse quadro foi corretamente recebido na estação de destino. Se a estação tiver outro quadro para transmitir, iniciará o protocolo CSMA/CA na etapa b. Se não receber uma confirmação, a estação de origem entrará novamente na fase de espera (*backoff*) na etapa b e escolherá um valor aleatório dentro de um intervalo maior.

Mídias integradas: Faça a simulação **CSMA/CA sem terminais ocultos**, disponível em: <http://www.ccs-labs.org/teaching/rn/animations/csma/>. Demonstre que você entendeu a simulação, descrevendo as suas escolhas e o resultado.

No protocolo CSMA/CA, ao contrário do CSMA/CD da *Ethernet*, a estação escolhe um valor aleatório de espera e inicia uma contagem regressiva, atrasando a sua transmissão, mesmo que perceba que o meio está ocioso (no CSMA/CD, uma estação transmite sempre que o meio estiver ocioso). Como o CSMA/CA não detecta uma colisão nem interrompe a transmissão, um quadro em uma colisão é transmitido integralmente.

O objetivo do CSMA/CA é evitar as colisões sempre que possível. Se duas estações identificarem que o meio está ocupado, ambas entrarão imediatamente em espera aleatória e, no melhor caso, escolherão valores diferentes de espera.

Se esses valores forem diferentes de fato, assim que o meio ficar ocioso, uma das duas estações começará a transmitir antes da outra; a estação em espera ouvirá o sinal

da outra, interromperá seu contador e não transmitirá até que a transmissão seja concluída. No entanto, ainda podem ocorrer colisões nesse caso: as estações podem estar ocultas uma da outra ou podem escolher valores idênticos de espera aleatória.

Para evitar o problema do terminal oculto, o protocolo 802.11 permite que uma estação utilize um quadro de controle de solicitação para envio (RTS, do inglês *Request to Send*) e um quadro de controle de pronto para envio (CTS, do inglês *Clear to Send*) para reservar o acesso ao meio de transmissão. Os quadros de controle RTS e CTS são curtos.

Quando uma estação quer enviar um quadro DADOS, pode enviar primeiramente um quadro RTS ao AP indicando o tempo total necessário para transmitir o quadro DADOS e o quadro de confirmação (ACK). Quando o AP recebe o quadro RTS, responde fazendo a transmissão por difusão (*broadcast*) de um quadro CTS. Esse quadro CTS tem duas finalidades: fornece ao transmissor uma permissão explícita para enviar e também informa as outras estações a não enviar durante o tempo reservado.

A Figura 26 mostra um exemplo de prevenção de colisão usando os quadros de controle RTS e CTS. Antes de transmitir um quadro DADOS, a estação de origem primeiramente faz uma transmissão *broadcast* de um quadro RTS, que é recebido por todas as estações que estiverem dentro do seu alcance, incluindo a estação de destino (que pode ser um AP), mas não é recebido por uma estação que esteja oculta. A estação de destino então responde com um quadro CTS, que é recebido por todas as estações dentro de seu alcance (incluindo, é claro, a estação de origem). Como recebeu o CTS, uma estação oculta deixa de transmitir durante o tempo especificado no quadro CTS.

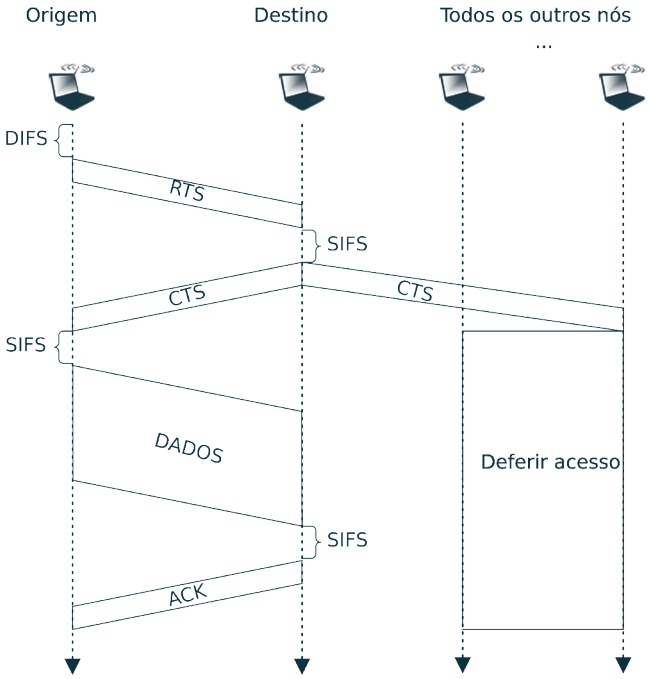

Figura 26 – Prevenção de colisão usando os quadros RTS e CTS
Fonte: Adaptado de Kurose e Ross (2013, p. 397).

A utilização dos quadros RTS e CTS pode melhorar o desempenho de uma rede 802.11 de dois modos importantes (KUROSE; ROSS, 2013):

a) o problema do terminal oculto é atenuado, pois um quadro longo DADOS somente é transmitido após o meio de transmissão ter sido reservado;

b) como os quadros RTS e CTS são curtos, uma colisão que envolva um quadro RTS ou CTS terá apenas a duração desses quadros. Uma vez que os quadros RTS e CTS sejam corretamente transmitidos, os quadros DADOS e ACK subsequentes deverão ser transmitidos sem colisões.

Mídias integradas: Faça a simulação **CSMA/CA com terminais ocultos**, disponível em: <http://www.ccs-labs.org/teaching/rn/animations/csma/>. Demonstre que você entendeu a simulação, descrevendo as suas escolhas e o resultado.

Embora o intercâmbio de quadros RTS e CTS possa auxiliar a reduzir colisões, também introduz atraso e consome o tempo de uso do meio de transmissão. Por essa razão, esse intercâmbio é utilizado apenas para reservar o meio para a transmissão de um quadro longo de dados.

Na prática, cada estação sem fio pode estabelecer um limite de quadro de dados para que os quadros RTS e CTS sejam utilizados somente quando o quadro a ser transmitido for mais longo que o limite. Para muitas estações sem fio, o valor padrão desse limite é maior que o comprimento máximo do quadro, de modo que os quadros RTS e CTS não são utilizados para todos os quadros enviados.

7.3 INTERCONEXÃO DE REDES 802.11

A motivação inicial para a disseminação das redes sem fio, em especial as redes 802.11, foi a flexibilidade para o acesso à infraestrutura de rede em ambientes com alta mobilidade de usuários. Naturalmente, existe o interesse na interconexão de redes sem fio à rede empresarial ou residencial para o compartilhamento de recursos e acesso à internet.

Uma rede local pode ser totalmente implementada com a tecnologia 802.11. Nessa rede, todas as estações (computadores portáteis ou de mesa) têm um adaptador de rede 802.11 e deve existir um AP, também de tecnologia 802.11, para interconectar as estações.

Essa é uma configuração típica de uma rede 802.11 operando no modo de infraestrutura e é frequentemente utilizada em redes residenciais. Para acesso à internet, geralmente o AP é conectado a um roteador que, por sua vez, é conectado a um modem ADSL (ou a cabo), conforme ilustrado na Figura 27. Dependendo do fabricante, um mesmo equipamento pode realizar as funções de modem ADSL, roteador e AP.

A utilização da tecnologia 802.11 também pode ser parcial, somente para as estações móveis, conforme ilustrado na Figura 28. Nesse caso, muito comum em redes empresariais ou em redes de câmpus universitário, o AP também opera em modo de infraestrutura e está interconectado diretamente ao comutador (*switch*) da rede principal (*backbone*) para formar uma única rede.

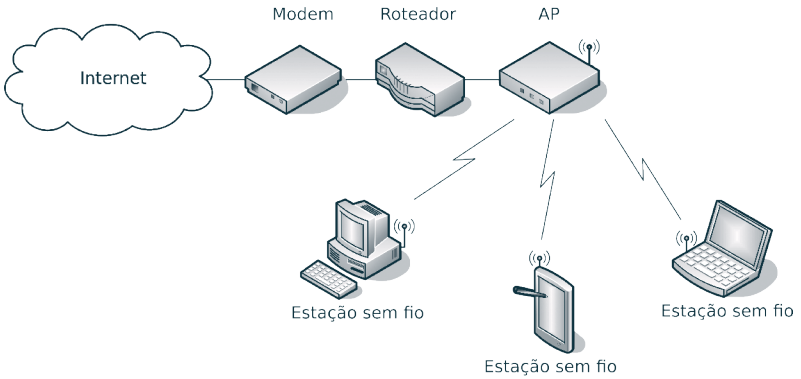

Figura 27 – Exemplo de uma configuração típica para uma rede residencial
Fonte: Adaptado de Tanenbaum e Wetherall (2011, p. 188).

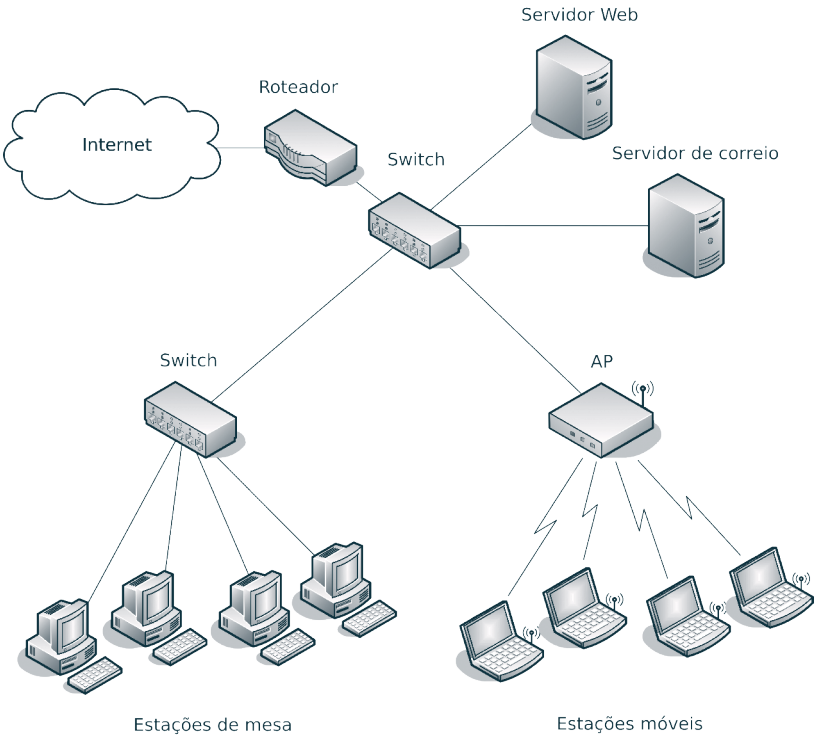

Figura 28 – Exemplo de uma configuração típica para uma rede empresarial
Fonte: Adaptado de Kurose e Ross (2006, p. 367).

A tecnologia 802.11 também pode ser utilizada para a interconexão entre dois segmentos de redes locais, conforme ilustrado na Figura 29. Nesse caso, cada um dos APs funciona como uma ponte (*bridge*) 802.11, encaminhando quadros de um segmento para o outro.

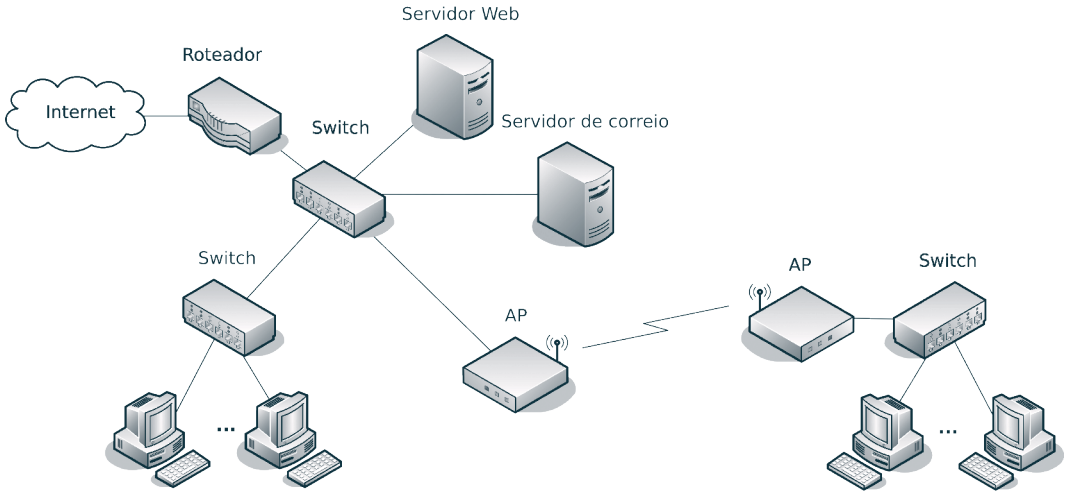

Figura 29 – Exemplo de interconexão de segmentos de redes locais
Fonte: Adaptado de Cyclades Brasil (2002, p. 150).

A interconexão mostrada na Figura 29 é realizada, essencialmente, por um enlace ponto a ponto. Os quadros são transmitidos diretamente de um AP para o outro AP, não ocorrendo o compartilhamento do meio de transmissão. Nesse caso, uma antena direcional pode ser utilizada em cada um dos APs e que cada uma esteja dirigida uma para a outra. A utilização de antenas direcionais e uma maior potência de transmissão permitem que a tecnologia 802.11 seja utilizada para prover conexões sem fio ponto a ponto por dezenas de quilômetros.

Resumo

Neste capítulo foram apresentados os conceitos relacionados a redes sem fio. Estação sem fio, enlace sem fio e estação base são os principais elementos em uma rede local sem fio. Os enlaces sem fio são suscetíveis ao ambiente e possuem os problemas de redução da força do sinal, interferência de outras fontes e de propagação multivias. O problema do terminal oculto e o problema do desvanecimento da força do sinal também devem ser tratados pelo protocolo da camada de enlace de dados. O principal padrão de redes locais sem fio é o IEEE 802.11, também conhecido como *Wi-Fi*. As redes 802.11 podem ser utilizadas em modo de infraestrutura e em modo *ad hoc*. O protocolo utilizado no padrão IEEE 802.11 é o CSMA/CA, que utiliza técnicas de prevenção de colisão em vez de utilizar detecção de colisão. Ao final do capítulo, foram apresentadas algumas formas de interconexão de redes sem fio.

Atividades de aprendizagem

1. Quais as principais aplicações das tecnologias sem fio?
2. Descreva os principais elementos de uma rede local sem fio.
3. Qual a diferença entre a operação de uma rede local sem fio no modo de infraestrutura e no modo *ad hoc*?
4. Quais os principais problemas que podem ocorrer em enlaces sem fio?
5. Explique o problema do terminal oculto, muito comum em redes sem fio.
6. Explique o problema do desvanecimento que pode ocorrer nas transmissões das estações em uma rede sem fio.
7. Quais as semelhanças entre os padrões 802.11b, 802.11a, 802.11g e 802.11n?
8. Quais as diferenças entre os padrões 802.11b, 802.11a, 802.11g e 802.11n?
9. Descreva um cenário para uma rede 802.11 operando em modo de infraestrutura.
10. Qual a principal diferença entre o protocolo CSMA/CA (do padrão 802.11) e o CSMA/CD (do padrão *Ethernet*)?
11. Por que o protocolo 802.11 não implementa a detecção de colisão?
12. Explique o mecanismo de confirmação/retransmissão na camada de enlace de dados utilizada pelo protocolo 802.11.
13. Como o protocolo 802.11 evita o problema do terminal oculto?
14. Descreva um cenário para uma rede local residencial com tecnologia sem fio.
15. Como uma rede local sem fio pode ser interconectada com uma rede local cabeada?

REFERÊNCIAS

CHIOZZOTO, M.; SILVA, L. A. P. **TCP/IP:** tecnologia e implementação. 2. ed. São Paulo: Érica, 1999.

COMER, D. E. **Interligação de redes com TCP/IP:** princípios, protocolos e arquitetura. 5. ed. Rio de Janeiro: Elsevier, 2006.

CYCLADES BRASIL. **Guia internet de conectividade.** 9. ed. São Paulo: SENAC São Paulo, 2002.

GIOZZA, W. F. et al. **Redes locais de computadores:** tecnologia e aplicações. São Paulo: McGraw-Hill, 1986.

KUROSE, J. F.; ROSS, K. W. **Redes de computadores e a internet:** uma abordagem top-down. 3. ed. São Paulo: Pearson Addison Wesley, 2006.

KUROSE, J. F.; ROSS, K. W. **Redes de computadores e a internet:** uma abordagem top-down. 6. ed. São Paulo: Pearson Education do Brasil, 2013.

OPPENHEIMER, P. **Projeto de redes top-down.** 2. ed. Rio de Janeiro: Campus, 1999.

SOARES, L. F. G.; LEMOS, G.; COLCHER, S. **Redes de computadores:** das LANs, MANs e WANs às redes ATM. Rio de Janeiro: Campus, 1995.

SOUSA, L. B. **Redes de computadores:** dados, voz e imagem. São Paulo: Érica, 1999.

TANENBAUM, A. S. **Redes de computadores.** 3. ed. Rio de Janeiro: Campus, 1997.

TANENBAUM, A. S. **Redes de computadores.** 4. ed. Rio de Janeiro: Elsevier, 2003.

TANENBAUM, A. S. **Sistemas operacionais modernos.** 3. ed. São Paulo: Pearson Prentice Hall, 2009.

TANENBAUM, A. S.; WETHERALL, D. J. **Redes de computadores.** 5. ed. São Paulo: Pearson Prentice Hall, 2011.

TORRES, G. **Redes de computadores curso completo.** Rio de Janeiro: Axcel Books, 2001.

ZACKER, C.; DOYLE, P. **Redes de computadores:** configuração, manutenção e expansão. São Paulo: Makron Books, 2000.

Capa: Papel triplex 250 gramas
Miolo: Papel couché 115 gramas
Fonte: Adobe Garamend Pro
Tiragem: 500 exemplares
Impresso na Gráfica Radial Ltda.
Curitiba
2016
Impresso no Brasil
Printed in Brazil

O livro Redes Locais de Computadores traz os conceitos e tecnologias relacionados às redes locais de computadores com a finalidade de apoiar professores, estudantes e profissionais de Redes de Computadores. A obra aborda os conceitos fundamentais e as principais tecnologias de redes locais de computadores ao longo de sete capítulos. O primeiro capítulo apresenta um resumo geral sobre redes locais, com a introdução de muitos conceitos e terminologias. O segundo capítulo aborda o histórico e a evolução das redes locais para facilitar a compreensão de como as tecnologias se desenvolveram até o estágio atual. O terceiro capítulo apresenta as topologias para diferentes tipos de redes de computadores. As principais topologias físicas e lógicas são apresentadas e discutidas. No quarto capítulo, o assunto é arquitetura de redes locais, cujos conceitos relacionados são importantes para a compreensão dos capítulos seguintes. O quinto e o sexto capítulo abordam padrões específicos para redes locais, com destaque para a tecnologia Ethernet, que é a tecnologia de rede local mais adotada mundialmente. Finalmente, o sétimo e último capítulo trata das redes locais sem fio. No final de cada capítulo, exercícios são propostos como atividade de aprendizagem dos principais tópicos.

Agência Brasileira do ISBN
ISBN 978-85-7014-160-6
9 788570 141606