Coleção UAB–UFSCar

Sistemas de Informação

Luis Carlos Trevelin

Redes de computadores

Redes de computadores

UAB-UFSCar
Universidade Federal de São Carlos
Rodovia Washington Luís, km 235
13565-905 - São Carlos, SP, Brasil
Telefax (16) 3351-8420
www.uab.ufscar.br
uab@ufscar.br

Luis Carlos Trevelin

Redes de computadores

São Carlos
2014

Concepção Pedagógica
Daniel Mill

Supervisão
Douglas Henrique Perez Pino

Equipe de Revisão Linguística
Clarissa Galvão Bengtson
Daniel William Ferreira de Camargo
Juliana Carolina Barcelli
Kamilla Vinha Carlos

Equipe de Editoração Eletrônica
Izis Cavalcanti

Equipe de Ilustração
Catarine Santana Ohnuma

Capa e Projeto Gráfico
Luís Gustavo Sousa Sguissardi

SUMÁRIO

UNIDADE 1

Redes de computadores

1.1 Introdução

Este material apresenta uma breve introdução às redes de computadores e seu principal intuito é motivar o aluno a estudar esse conteúdo de forma mais detalhada. De início, apresentamos algumas questões importantes sobre a evolução tecnológica e as demandas para a criação de redes, considerando as necessidades de informações. Mostramos, também, como ocorreu a evolução da *internet* a partir de projetos e eventos importantes ocorridos desde 1960. Na sequência, iniciamos a caracterização de aspectos importantes na construção de redes e aprofundaremos neste assunto à medida que o curso avançar. Novos conceitos serão introduzidos e, partindo da estrutura física de interconexão de computadores, onde trataremos dos dispositivos de rede e dos meios físicos, compreenderemos como as aplicações de usuário e os Sistemas de Informação se executam no ambiente de redes.

1.2 Roteiro da unidade

- Evolução das redes de computadores;
- Classificação das redes de computadores;
- Topologias das redes de computadores;
- Caracterização das redes de computadores;
- Taxonomia das redes de computadores;
- Protocolos de comunicação;
- Pilhas de protocolos e modelos de referência.

1.3 Evolução das redes de computadores

Tudo começa com a necessidade inerente do ser humano de trocar informações. Toda atividade humana está baseada nesta troca e, por essa razão, diferentes mecanismos são propostos, conforme a sociedade evolui social e tecnologicamente.

A troca de informações ocorre por meio de mecanismos de comunicação desenvolvidos pelo homem. A fala (as diferentes línguas), os sinais e a escrita (o papiro, o papel, a imprensa etc.) foram os precursores desta necessidade. Na história, notamos eventos importantes relacionados à comunicação. Desde os primórdios, o homem utilizou-se de sinais em cavernas e de sinais de fumaça como forma de indicar algum conhecimento.

Figura 1. Evolução das formas de comunicação.

Na Grécia antiga, a maratona nos mostra que homens eram usados como portadores de notícias e informações estratégicas. Na primeira guerra, tivemos o uso de pombos-correios como veículos de comunicação entre o *front* de batalha e os quartéis. Veículos também foram amplamente utilizados (e ainda são) como meios de comunicação (correios) e até aviões fazem hoje esse papel.

No século 19, na ocupação do oeste americano, vimos a expansão das ferrovias acompanhadas das linhas de telegrafia, onde o telégrafo (instrumento de sinalização usando código binário, de traços e pontos, proposto por Samuel Morse em 1830) levava informação textual na forma de telegramas.

Outra forma de comunicação de grande destaque é o telefone, proposto por Alexandre Grahan Bell ainda na década de 1870:

> [...] Em Boston continuou a sua pesquisa no mesmo campo, e esforçou-se para produzir um telefone que emitisse não somente notas musicais, mas articulasse a fala.
>
> Com financiamento do seu sogro americano, em 7 de Março de 1876, o Escritório de Patentes dos Estados Unidos concedeu-lhe a patente número 174.465 que cobre "o método de, e o instrumento para, transmitir sons vocais ou outros telegraficamente, causando ondulações eléctricas, similares às vibrações do ar que acompanham o som vocal.", ou seja o telefone. Após ter obtido a patente para o telefone, Bell continuou suas experiências em comunicação, que culminaram na invenção da photophone - transmissão do som num feixe de luz - um percursor dos sistemas de fibra óptica actuais. Também trabalhou na pesquisa médica e inventou técnicas para ensinar o discurso aos surdos [...] (WIKIPÉDIA, 2013).

A telefonia ganhou grande popularidade e passou a ser um elemento presente na vida de qualquer pessoa, seja para comunicação informal, seja para realização de negócios. O mundo todo adotou a comunicação via telefone que passou por uma surpreendente evolução tecnológica, até os dias atuais, com a telefonia celular (1G, 2G e 3G) misturando-se hoje com os serviços da *internet*. O telefone baseava-se no conceito de comutação (ou chaveamento) de circuitos físicos (cabos) para estabelecimento de um *link* de comunicação entre dois indivíduos remotamente localizados. Essa tecnologia, evoluída das conexões ponto

a ponto entre cada dois indivíduos, já buscava eliminar cabos pelo compartilhamento de linhas usando chaveadores (*switches*) de circuitos (as famosas centrais de telefonia).

Na década de 1950, tivemos o início dos projetos da rede ARPA (Advanced Research Project Agency), do departamento de defesa americano, que resultaram em uma rede de pesquisas de diversas universidades, utilizando a tecnologia de comutação por pacotes em contraposição a comutação por circuitos e dando, assim, um passo adiante no compartilhamento pelo uso otimizado dos meios físicos de comunicação. Surgiram, deste projeto, as BBS (Bulletin Board Systems) que eram repositórios de dados em servidores de rede, disponíveis para acesso compartilhado, via *upload* e *download* de arquivos eletrônicos, por meio da rede. Surgiu, também, o *e-mail*, correio eletrônico pela rede, que rapidamente ganhou inúmeros adeptos pela facilidade e rapidez na troca de mensagens.

Na década de 1990, com o desenvolvimento da World Wide Web (WWW), a *internet* se afirmou como rede mundial, já com milhares de pontos de acesso e diversos usuários em todo o mundo. Nessa evolução das redes até a *internet*, outras tecnologias de rede coexistiram no projeto da rede ARPA. Algumas delas foram sendo incorporadas e outras sendo abandonadas, na evolução natural da tecnologia.

Mas, enfim, o que são redes de comunicação? Dois aspectos são considerados aqui:

- Do ponto de vista do usuário:
  - As redes devem oferecer o serviço básico para transportar a informação;
  - Devem oferecer, também, diferentes serviços baseados em sua abordagem tecnológica, diferenciando-os por meio de alguns aspectos, tais como: latência (ou tempo médio de transporte de uma unidade de dados de um extremo a outro); largura de banda (capacidade de trafegar mais de uma unidade de dados, de diferentes conexões, em paralelo); número de usuários conectados simultaneamente e interface de invocação dos serviços (como invocar?).

- Do ponto de vista da infraestrutura:
  - A informação é vista como *elétrons* (comunicação eletromagnética) ou *fótons* (comunicação óptica) que trafegam por um meio de propagação, ligando dois extremos remotos;
  - Cabos de cobre, fibras ópticas ou mesmo o ar como meios físicos de interconexão, ligando dispositivos remotos;

- Comutadores (ou chaveadores) mecânicos, eletrônicos ou ópticos com capacidade de operar a mudança no circuito por onde deverão ser transferidos os bits ou ainda os pacotes de dados a serem transferidos de uma origem para um destino qualquer;
- Protocolos, ou regras de estabelecimento da comunicação, para troca de unidades de dados (pacotes, mensagens etc.) entre origem e destino;
- Funcionalidades de sinalização pelos meios físicos de conexão de unidades de dados, enlace lógico entre os dispositivos conectados (*links*), controle de transferência de dados, controle de congestionamento, qualidade de serviço (QoS), dentre outros;
- Aplicações de rede (por exemplo, *chat* de mensagens, correio eletrônico, transferência de arquivos e *web*).

A evolução dos meios de comunicação originou as redes de comunicação de dados e, por decorrência, as redes de computadores, entendidas aqui como um conjunto de computadores interconectados por uma rede de comunicação de dados e cujo propósito é possibilitar a troca organizada de informações entre aplicações hospedadas nestes computadores.

Diante dessas considerações, as redes de computadores têm os seguintes objetivos:

- Compartilhamento de informações (dados) entre elementos remotamente localizados;
- Compartilhamento de recursos (meios físicos, computadores, arquivos);
- Comunicação remota entre indivíduos (*e-mail*, *chat*, voz digital);
- Utilização remota de computadores;
- Compartilhamento de processamento (processamento distribuído);
- Gerenciamento centralizado de recursos distribuídos;
- Economia em escala de recursos compartilhados;
- Computação colaborativa;
- Segurança de dados.

Para acompanharmos a evolução das redes de computadores, vamos a alguns pontos históricos:

Antecedentes sócio-políticos e tecnológicos

- 1917: Revolução Russa;
- 1930: Telégrafo (Samuel Morse);
- 1939-1945: II Grande Guerra;

- 1957: em 4 de outubro a URSS (União das Repúblicas Socialistas Soviéticas) lança o Sputnik I e em 3 de novembro lança o Sputnik II e a cadela Laika;
- 1957: o presidente dos Estados Unidos da América (EUA), Eisenhower, inicia a Advanced Research Projects Agency (ARPA);
- 1958: primeiro cabo transatlântico, o qual fica em serviço somente por alguns dias.

Aqui começam as ações para a criação da rede mundial, a *internet*. A agência de projetos avançados de pesquisa, criada em 1957, foi o marco decisivo para iniciar o projeto da rede ARPA de comutação de pacotes. Esta rede visava atender aos militares, interligando suas bases com uma tecnologia nova e confiável, diferente das redes até então desenvolvidas.

- 1961: Leonard Kleinrock do Massachusetts Institute of Technology (MIT) publica o Information Flow in Large Communication Nets, o primeiro documento sobre comutação de pacotes;
- 1962: Dr. Joseph Carl Robnett Licklider torna-se diretor de pesquisa para o uso militar de computadores na ARPA;
- 1965: o MIT inicia um estudo sobre as redes de computadores;
- 1968: inicia a ARPANet (Advanced Research Project Agency Network);
- 1969: a ARPANet é composta por 4 nodos (UCLA, UCSB, U.Utah e Stanford Research Institute) com *links* de 50Kbits/s;
- 1970: desenvolvimento do Network Control Protocol (NCP), o predecessor do TCP, o primeiro protocolo fim a fim;
- 1971: surge o programa de *e-mail*;
- 1973: surgem as primeiras conexões internacionais. A tese de doutorado de Bob Metcalfe delineia a ideia para a Ethernet. O *e-mail* representa 75% do tráfego;
- 1974: criada a especificação do TCP;
- 1975: ligações via satélite cruzam o oceano (Hawai e Inglaterra). Realização de testes do TCP;
- 1976: Semour Cray demonstra o primeiro processador vetorial: o Cray-1. Elizabeth II, rainha do Reino Unido, envia um *e-mail*, em fevereiro, do Royal Signals and Radar Establishment (RSRE), em Malvern;
- 1977: desenvolvimento do X.25, um protocolo com conceito de circuito virtual (CCITT). Steve Wozniak e Steve Jobs anunciam a Apple II;
- 1978: o TCP é dividido em TCP e IP;
- 1979: em 12 de abril, Kevin MacKenzie envia um *e-mail* ao MsgGroup

com uma sugestão de adicionar alguma emoção ao texto seco do *e-mail*. Sugestões tais como o "-)" para indicar que a sentença era irônica e ":)" para expressar alegria. Surgem, então, os *emoticons*. Larry Landweber discute com outras universidades a criação de uma rede universitária: a Computer Sciences Research Network (CSNet);

- Na década de 1980 proliferam-se as LAN (Local Area Network): Ethernet e Token Ring;
- 1981: início da Because It´s Time Network (BITNet);
- 1982: início da discussão sobre a falta de acesso a supercomputadores;
- 1983: divisão entre ARPANet (pesquisa) e MILNet (militar). Ocorre também a mudança do NCP para o TCP em toda rede (1/1);
- 1984: surge o Domain Name Service (DNS);
- 1985: a National Science Foundation (NSF) cria 5 centros de supercomputação acessíveis via rede (Cornell, Princeton, Illinois, Pittsburg e San Diego);
- 1986: é criada a National Science Foundation Network (NSFNet), conectando os centros NSF com *links* de 56Kbps;
- 1987: a NSF inicia implementação de *links* T1, com 1.544Mbps. Surge o SNMP (Simple Network Management Protocol);
- 1989: o número de máquinas (*hosts*) cresce de 80.000 (janeiro) para 130.000 em julho, indo a 160.000 em novembro. No CERN (Suíça), Berners Lee propõe o uso de hipertexto em sistemas distribuídos por meio do protocolo HTTP: surge a WWW.

No final dos anos 1980 proliferam-se as redes com fibra óptica, a Fiber Distributed Data Interface (FDDI) com velocidades de 100Mb/s;

Na década de 1990, surgem as redes de alta velocidade: ATM com velocidades de 150Mb/s ou mais. O foco está em: novas aplicações; redes locais sem fio e comercialização eletrônica;

- 1990: o Brasil se conecta à *internet*;
- 1991: a Universidade de Minnesota lança a Gopher (protocolo de rede de computadores) e mais de 100 países já estão conectados;
- 1992: estudantes trabalham sobre proposta de Berners Lee e surge o navegador MOSAIC, o predecessor do NESTCAPE;
- 1993: a NCSA (National Center for Supercomputing Applications) Mosaic torna a *internet* como um furacão. Já é possível pedir *pizza* pela *internet*;
- 1994: já são cerca de 2.200.000 *hosts* na rede mundial de computadores;
- 1995: a *internet* alcança o número de 4.900.000 *hosts* conectados;

- 1996: são 9.500.000 *hosts* interligados na rede mundial de computadores;
- 1997: o domínio business.com é vendido por US$ 150.000;

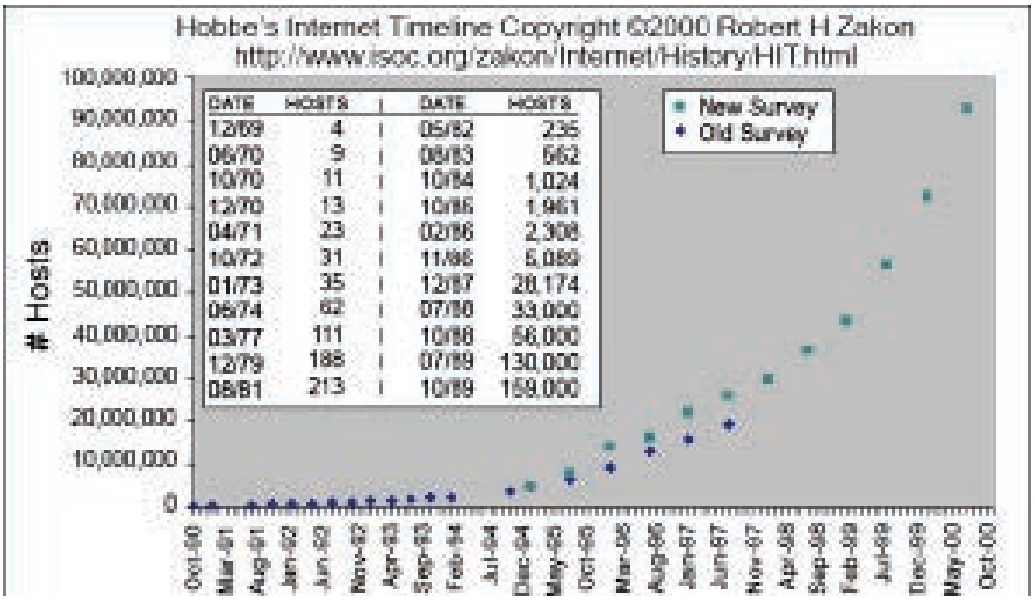


Figura 2. Quantidade de máquinas conectadas.

- 1998: a Compaq paga US$ 3.300.000 pelo altavista.com;
- 2000: desenvolvimento e popularização dos serviços de compartilhamento de arquivos e dados (Napster). Surge também uma explosão dos vírus e vermes por *e-mail*. Começam os serviços de banda larga (xDSL, satélite, cabo);
- 2001: desenvolvimento e popularização dos serviços ponto a ponto: Gnutella e Morpheus;
- 2002: aparecem as redes de alta velocidade, redes sem fio e grades computacionais.

A essa altura, a *internet* já era realidade. A rede ARPA ficou com o objetivo inicial por meio da MILNet e a *internet* não dependia mais dela. A partir daí, o crescimento da *internet* e a economia decorrente foi impressionante.

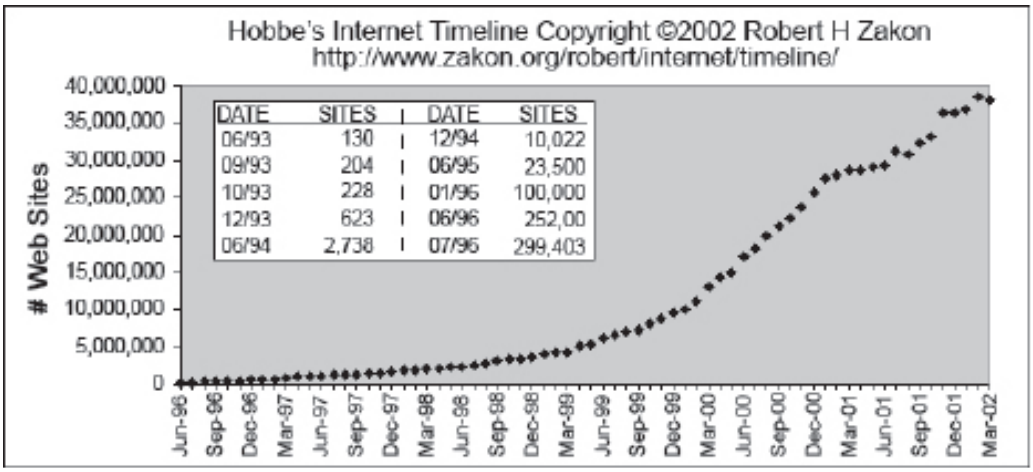


Figura 3. Quantidade de *web sites*.

- 2003: desenvolvimento da mobilidade, computação ubíqua e redes de sensores;
- 2004: surgimento da computação dirigida por contexto e das redes embarcadas;
- 2005: início do uso das redes de comutação óptica e dos web services;

A *internet* teve, e ainda tem, a proposta de ser um sistema aberto livre para a conexão e o desenvolvimento de aplicações dos mais variados tipos. Entretanto, ela é regulamentada por comitês compostos por representantes dos países e dos diversos setores da sociedade, da indústria e da academia.

- IETF – Internet Engineering Task Force: cuida da especificação e desenvolvimento de protocolos. Especifica as RFC (Request For Comments) e os documentos de especificação de novos padrões de protocolos e serviços;
- IRTF – Inernet Research Task Force: constituído por grupos de pesquisa de longa duração para estudos e desenvolvimento de novas propostas submetidas, no final, ao IETF;
- IAB – Internet Architcture Board: responsável pela definição e pelo estabelecimento da arquitetura geral da *internet*. A IAB orienta os trabalhos do IETF;
- IESG – Inernet Engineering Stearing Group: é responsável pelo gerenciamento técnico das atividades e os processos de padronização do IETF.
- ICANN – Internet Corporation for Assigned Names and Numbers: responsável por gerir a atribuição de endereços de rede à ISP (provedores de serviços de *internet*) e instituições públicas ou privadas nos diferentes

países, atendendo à arquitetura e ao modelo hierárquico da *internet*.

1.4 Classificação das redes de computadores

A *internet* se caracteriza pela interligação de diferentes redes com modelos de arquitetura e tamanhos distintos. Estas redes interligadas abrangem desde as redes locais de qualquer instituição pública ou privada, passando pelas redes metropolitanas (atuais redes metro), até as grandes redes continentais com a finalidade básica de transporte de dados entre cidades, estados e até países diferentes.

A dimensão das redes é uma característica que também determina a tecnologia empregada em sua construção. A finalidade da rede, que pode variar dependendo da situação, está relacionada à sua dimensão. Dentro deste conceito temos:

- Redes Locais (LAN – Local Area Networks): redes de pequeno alcance (uma planta industrial, um campus, um prédio etc.) tipicamente proprietárias e pertencentes a uma instituição ou empresa. Uma LAN é composta por dezenas ou até centenas de computadores de uma empresa interligados por um meio veloz de conexão, com baixa taxa de erros de transmissão.
- Redes Metropolitanas (MAN – Metropolitan Area Networks): redes de alcance médio, de cobertura de uma ou algumas cidades, com a finalidade de permitir acesso por empresas, instituições e ISP por meio de suas redes LAN. Uma MAN tem taxas de comunicação bastante razoáveis, com linhas proprietárias ou alugadas de concessionárias de telecomunicações;
- Redes de Longa Distância (WAN – Wide Area Networks): são redes de longo alcance que podem cobrir um continente, ou até mesmo interligar continentes, por meio de linhas de comunicação de grandes operadoras de telecomunicações (*carriers*), com a finalidade de promover conexão de MAN e LAN diferentes;
- A *internet* é a interligação dessas redes WAN, MAN e LAN por meio de um padrão de comunicação presente em todas elas.

Existem outras categorias para definir alguns tipos particulares de redes, que até se enquadrariam nas categorias já definidas, mas que, por terem características próprias, foram também categorizadas. São elas:

- Redes Pessoais (PAN – Personal Area Networks): as redes pessoais ou de pequenos escritórios são redes que usam tipicamente uma tecnologia sem fio para transmissão de dados;

- Intranets: segmentos internos de uma rede LAN, acessíveis apenas pelos usuários internos da corporação;
- Extranets: redes com possibilidade de acesso externo à rede LAN por usuários externos autorizados;
- Redes Virtuais Privativas (VPN – Virtual Private Networks): segmentos de redes organizados de modo a constituírem uma LAN mapeada sobre diversas outras redes. Uma VPN faz uso de mecanismos de tunelamento de dados, de modo a se apresentar como outra rede, e é acessível remotamente.

Um aspecto considerado importante na organização das redes diz respeito à forma de transmissão dos dados. Esta pode ser:

- Por difusão (Multicast): as mensagens são propagadas igualmente a todos os computadores da rede pelas linhas de comunicação;
- Direcionados (Unicast): as mensagens são propagadas unidirecionalmente da origem para um dos destinos (identificado por um endereço).

Essa forma de encaminhamento ou transmissão de mensagens está relacionada à tecnologia de comunicação provinda pelos meios físicos utilizados e pela topologia usada na construção da rede.

1.5 Topologias de redes de computadores

A topologia é o modelo estrutural utilizado para interconexão dos elementos da rede (computadores e comutadores ou roteadores), baseados nos meios físicos disponíveis e nas formas de transmissão dos dados que ela proporciona. As principais topologias de redes são:

Topologia em árvore:

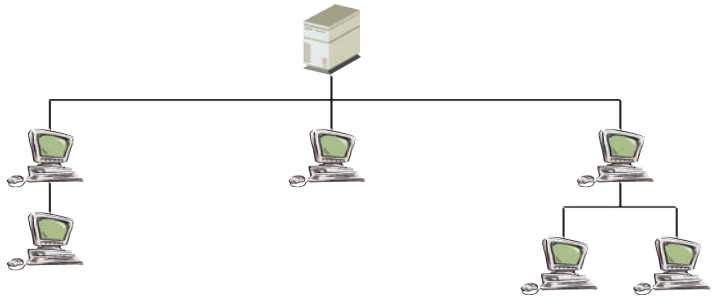


Figura 4. Topologia de rede em árvore.

Suas características são:

- Comumente utilizada em redes de longa distância;
- Se a maioria das tarefas é associada ao nó do topo, então ele poderá se tornar um gargalo;
- Se o nó do topo sai de operação (por uma falha), então toda a rede será desabilitada;
- Nós adicionais podem ser facilmente colocados na parte de baixo da árvore.

Topologia em estrela:

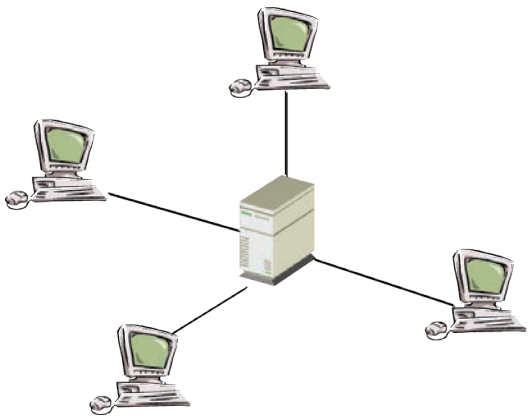


Figura 5. Topologia de rede em estrela.

Suas características são:

- Geralmente utilizada em redes de longa distância, mas existem também redes locais com essa topologia;

- Fácil de configurar;
- O roteamento não é uma tarefa complexa;
- Os recursos compartilhados devem estar conectados ao nó central.

Topologia em anel:

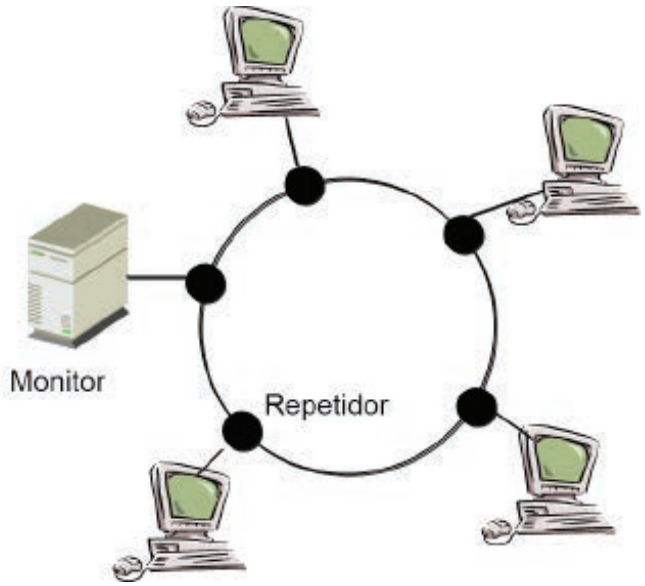


Figura 6. Topologia de rede em anel.

Suas características são:

- São inerentemente sistemas de difusão (broadcast);
- Cada estação está conectada à rede via um repetidor;
- A maioria dos anéis possui um monitor para remover pacotes corrompidos ou indesejados da rede;
- São rápidas e confiáveis. Podem continuar operando mesmo que alguns nós falhem;
- Se o anel for interrompido, toda a rede para.

Topologia em barramento:

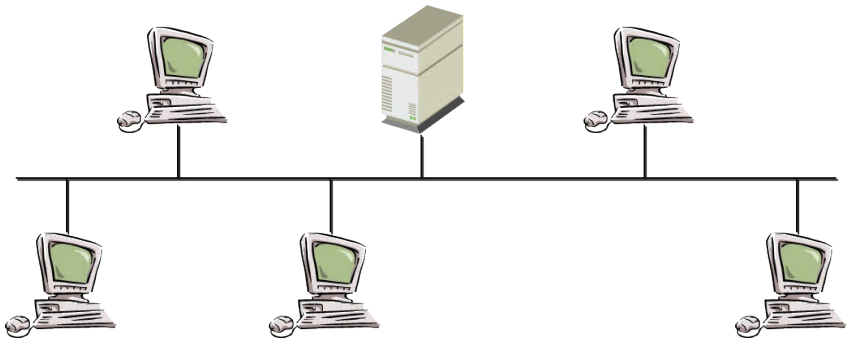


Figura 7. Topologia de rede em barramento.

Suas características são:

- São inerentemente sistemas de difusão (broadcast);
- O cabo deve possuir terminadores para evitar eco;
- Apenas uma mensagem pode estar no barramento em um instante;
- Geralmente utilizada para redes locais;
- Baixo custo e fáceis de configurar.

Topologia em malha:

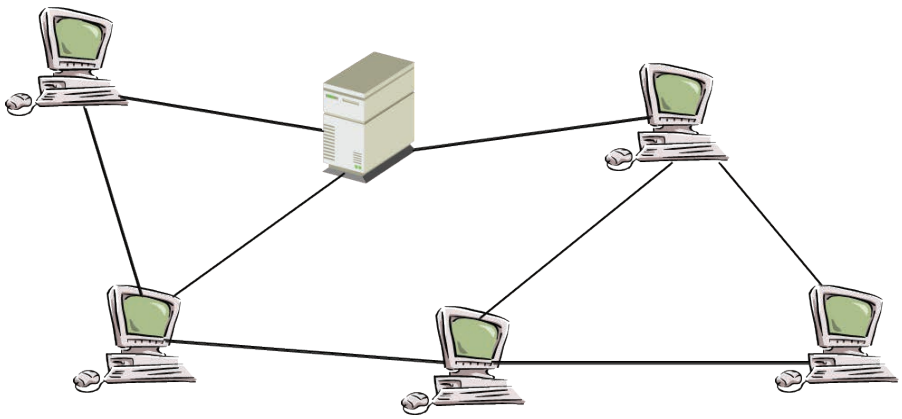


Figura 8. Topologia de rede em malha.

Suas características são:

- Utilizadas em redes de longa distância;
- Se todos os nós estão conectados entre si em uma rede, essa rede está

totalmente conectada;

- Relativamente imunes a gargalos e falha de componentes;
- Como existe uma variedade de caminhos, o tráfego pode ser roteado evitando os nós com defeito;
- Podem ter alto custo.

Outras possibilidades decorrentes da combinação dessas topologias ainda são possíveis, definindo as topologias híbridas.

1.6 Taxonomia das redes de computadores

Baseadas na maneira como os nodos trocam informações, podemos também classificar as redes segundo uma taxonomia:

- Redes de comunicação chaveadas: as informações são propagadas por mecanismos de comutação de linhas que podem ser:
  - Por circuito: como nas redes de telefonia, a comutação por circuito sempre usa a mesma rota entre uma origem e um destino;
  - Por pacotes: como na rede ARPA, as unidades de dados (pacotes) compartilham as linhas de conexão. Podem ser de dois tipos:
    - Datagramas: operam como telegramas (pacotes independentes), seguindo rotas individuais entre a origem e o destino;
    - Circuitos virtuais: todos os pacotes seguem pelo mesmo caminho definido previamente entre a origem e o destino.
- Redes de comunicação por difusão: as informações são propagadas por todas as linhas até todos os computadores de destino (por exemplo, redes sem fio).

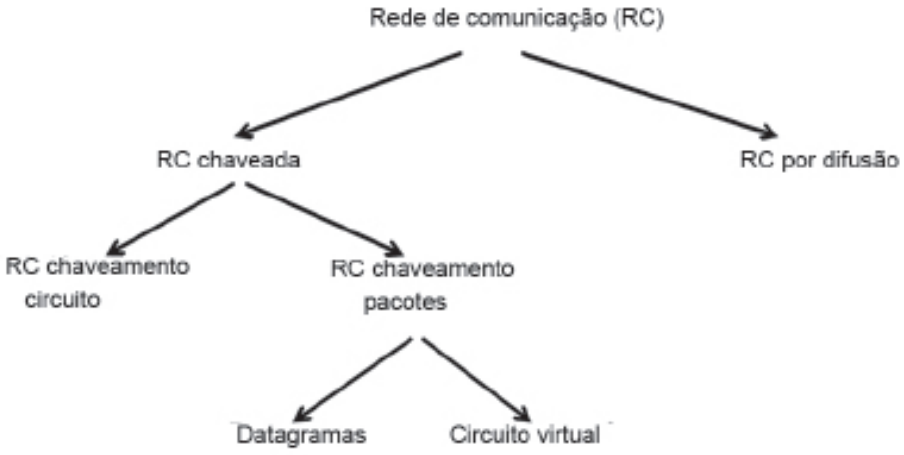


Figura 9. Troca de informações entre redes.

Nas redes de comunicação chaveadas, as informações são transmitidas a um subgrupo de nós designados. Um exemplo dessas redes é uma WAN (rede de telefonia, *internet*) e o problema que surge nesta categoria é como conduzir a informação até os nós designados.

Nas redes de comunicação chaveada por circuito, a comunicação se dá em três fases: estabelecimento do circuito; transferência de dados e encerramento do circuito. Os recursos fim a fim são reservados para a chamada e de forma não compartilhada. Um exemplo dessas redes é uma ISDN (Integrated Services Digital Networks) e uma rede de telefonia.

O compartilhamento de um meio físico de interconexão sugere o uso por diversos canais lógicos (*links*) através desse meio, significando que mensagens de cada canal são intercaladas para a transmissão (multiplexação de mensagens). Duas possibilidades se apresentam para podermos compartilhar o mesmo meio por diferentes *links*:

- Multiplexação pela divisão no tempo (TDM – Time Division Multiplex): meio onde as mensagens de mesmo tamanho são alternadamente transmitidas e que, de forma circular, ocupam espaços (*slots*) temporais de uma única frequência (banda estreita);
- Multiplexação pela divisão em frequências (FDM – Frequency Division Multiplex): meio onde a faixa de frequência disponível para a transmissão dos dados é subdividida em diferentes faixas menores e, um dos *links* de transmissão de mensagens (banda larga), é associado a cada uma dessas faixas, tal como nas estações de rádio ou TV.

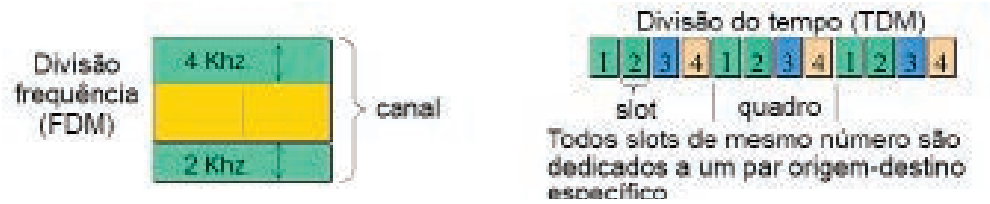


Figura 10. FDM x TDM.

Nas **redes de comunicação chaveadas por pacotes**, as mensagens são transmitidas como unidades de dados chamadas de pacotes, cujos conteúdos possuem um formato definido e são estruturadas em campos identificados e com funções bem determinadas:

- Cabeçalho: é um campo que identifica e controla a transferência de pacotes de dados;
- Dados (ou carga útil transportada): são os dados propriamente ditos a serem

enviados;

- Terminador (*trailer*): identifica o final do pacote e, em geral, possui um contador para conferência da integridade dos dados do pacote.

Os pacotes têm a seguinte estrutura:

Figura 11. Estrutura de um pacote.

Cada pacote é passado pela rede nó a nó ao longo do caminho (roteamento) e a cada nó o pacote inteiro é recebido, armazenado brevemente e então enviado ao próximo nó (redes armazena-envia). Pode haver congestionamento, caso a demanda agregada de recursos exceda a quantidade disponível.

O envio de pacotes pode obedecer a duas possibilidades:

- O envio como datagramas que, em analogia aos telegramas dos correios, constituem-se de pacotes de mensagens que são encaminhados individualmente e independentemente. Cada um desses pacotes segue a sua própria rota até o destino e esta pode diversificar dependendo da variação do tráfego na rede. Não há qualquer negociação prévia de qualidade de serviço (QoS) entre a origem e o destino, nem mesmo a garantia de entrega do pacote (entrega não confiável);

- O envio como circuito virtual, onde um pacote de controle é previamente encaminhado até o destino e estabelece e marca uma rota na qual todos os demais pacotes daquela conexão seguirão. Nessa modalidade há a possibilidade de negociação de QoS como alocação prévia de *buffers*, verificação e controle de erros, mecanismos de confirmação de recepção etc. que garantem o envio confiável dos pacotes e a sincronização entre a origem e o destino. Vale notar que uma conexão aqui é puramente lógica, pois os meios físicos são compartilhados por outras conexões (usando TDM ou FDM). Sua duração naquela rota é, a princípio, apenas enquanto durar a conexão (ou sessão de troca de mensagens).

O chaveamento de pacotes, se comparado ao de circuitos, traz uma série de vantagens, pois as linhas nunca são monopolizadas ou de propriedade de alguma conexão. Entretanto, o chaveamento de pacotes traz mais dificuldades no gerenciamento da alocação dos segmentos compartilhados.

Nas redes de comunicação por difusão, as informações transmitidas para qualquer nó são recebidas por qualquer outro nó da rede. Um exemplo dessas redes é uma LAN sem fio. O problema que surge nessa categoria é como coordenar o acesso de todos os nós ao meio de comunicação compartilhado.

1.7 Caracterização das redes de computadores

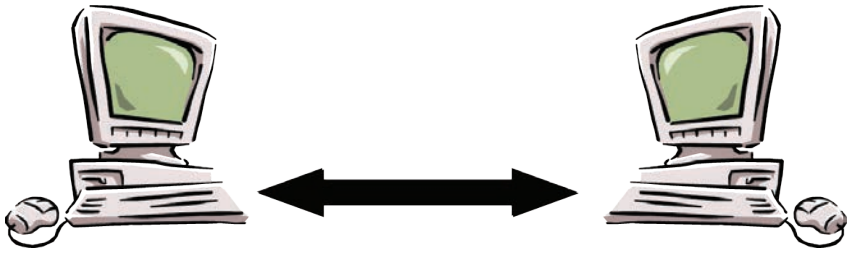


Figura 12. Comunicação em redes.

Foi dito, anteriormente, que o que caracteriza a rede é o aspecto ou a propriedade tecnológica dos meios físicos utilizados para conexão entre os elementos da rede. Mais especificamente, a respeito de:

- Largura de banda: é a taxa de bits que a rede consegue enviar ao destino por unidade de tempo. A largura de banda é definida pelas faixas de frequências que o meio físico suporta para transmissão dos dados. Desta maneira definimos a banda estreita, quando é usada uma faixa única (único canal ou *link*) e banda larga, quando são usadas várias subfaixas dentro da faixa de frequência operacional do meio, alocadas cada uma para um canal (ou *link*) de conexão diferente;
- Latência: definida pelo tempo que leva para um bit percorrer a extensão do meio físico de um extremo ao outro. Geralmente é medido em micro ou milissegundos.
- Confiabilidade: é a medida da quantidade de dado que é perdida pela rede em sua jornada da fonte para a origem. A confiabilidade é definida como a taxa de erros decorrentes de interferências na transmissão. Os erros poderão ser provenientes de destarte, onde o pacote é descartado pelos elementos ativos da rede ou poderão ser provenientes de corrupção, aonde o pacote chega, mas seus dados se alteraram;
- Protocolo: definido como a forma, ou regras, de comunicação usada naquele tipo de meio físico, seja para a sinalização dos bits pelo *link*, para a definição do *link* propriamente dito, para o controle do acesso a ele ou, ainda, para a definição da estrutura dos pacotes que nele são transmitidos.

1.8 Protocolos de comunicação em redes de computadores

A comunicação entre humanos não acontece de forma aleatória, por isso, as pessoas não disparam a falar intempestivamente e a qualquer momento. Existem regras de etiqueta e bom senso que, embora não sejam estabelecidas nem ensinadas formalmente, as pessoas as utilizam para que possa haver uma comunicação efetiva entre elas. Por exemplo, quando um fala o outro escuta e depois retruca (embora isso nem sempre seja verdade).

Numa chamada telefônica, existe uma série de etapas para que a conversa seja efetiva. Primeiro, ao pegarmos o telefone, aguardamos pelo sinal (nem sempre) indicador de que ele está conectado e ativo, digitamos o número, que identifica o outro extremo (o aparelho) e aguardamos alguns toques de chamada até sermos atendidos. Se isso ocorre, ouvimos uma expressão indicadora do tipo “Alô [...]” ou algo similar e, é nesse momento, que sabemos que podemos iniciar nossa fala, o que ocorre tentando identificar ou acionar o destinatário quando perguntamos: “A Maria está?”. Nesse ponto, após recebermos a confirmação de que a Maria se encontra ativa do outro lado é que iniciamos a conversa propriamente dita, com repetições eventuais para correção de erro de transmissão. Por fim, para encerrarmos, não desligamos simplesmente batendo o telefone (embora às vezes isso ocorra), mas, sim, nos despedimos e aguardamos o outro lado se despedir para, então, desligarmos o aparelho.

Nas redes também se processam as comunicações da mesma forma, isto é, um conjunto de regras formais é utilizado para permitir que a comunicação ocorra de forma não ambígua. As regras desse conjunto são chamadas de protocolos de comunicação e são definidas para cada fase ou nível da comunicação entre os elementos da rede, sejam eles meios físicos de transmissão, equipamentos comutadores, roteadores, computadores hospedeiros das aplicações ou as aplicações propriamente ditas. Para cada caso existe um conjunto de regras ou protocolos próprios, estabelecidos para ele.

Em redes de computadores, para que duas aplicações (processos) possam se comunicar utilizam-se de protocolos que definem, por exemplo, o formato dos pacotes, a semântica das mensagens trocadas e o tratamento de erros durante a comunicação. Obviamente, ao nível de sinalização no meio físico, as regras têm um propósito e ao nível das aplicações, outro. Ou seja, existem diferentes protocolos, um para cada nível da comunicação ocorrendo na rede.

Figura 13. Protocolos humanos *x* Protocolos de rede de computadores.

1.9 Pilhas de protocolos e modelos de referência

A organização dos protocolos, em cada nível, permite que um nível superior utilize os serviços implementados pelo protocolo do nível abaixo. Assim, utilizando sucessivamente esse conceito, temos uma estrutura hierárquica de protocolos empilhados uns sobre os outros, partindo desde o nível dos meios físicos até ao das aplicações.

A organização em camadas permite que se organize os serviços desde os mais básicos até os mais complexos à medida que sobem da camada física até a das aplicações, de tal maneira que, se assim não fosse, cada aplicação teria que implementar todos os protocolos, como na figura abaixo:

Figura 14. Organização não-estruturada.

Com a organização em camadas, a pilha de protocolos atua como um *middleware* entre o meio físico e as aplicações. Isso traz modularidade de forma que os protocolos sejam mais fáceis de administrar e manter, além de garantir a independência de implementação. Com essas vantagens, níveis inferiores podem ser mudados sem afetar os níveis superiores e componentes funcionais das camadas inferiores podem ser reutilizados nas camadas superiores. Com o uso da pilha de protocolos, o nível intermediário provê uma única abstração para vários tecnologias de rede.

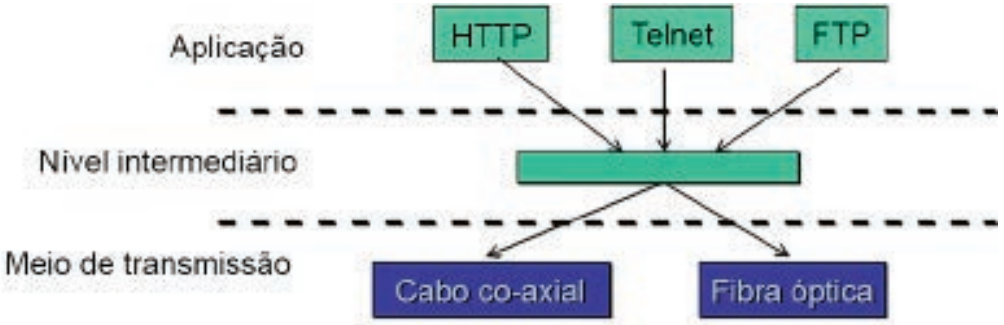


Figura 15. Organização em camadas.

Visando permitir a padronização dos protocolos e serviços oferecidos em cada camada, a ISO (International Standards Organization), um comitê internacional de padronizações, propôs um Modelo de Referência para Interconexão de Sistemas Abertos (RM-OSI) organizado em sete camadas. Esse modelo de referência especifica protocolos, serviços e interfaces para as camadas: física, enlace, rede, transporte, sessão, apresentação e aplicação. Esse modelo ficou conhecido como Modelo de Referência ISO/OSI e a organização de suas camadas pode ser visualizada na figura que segue:

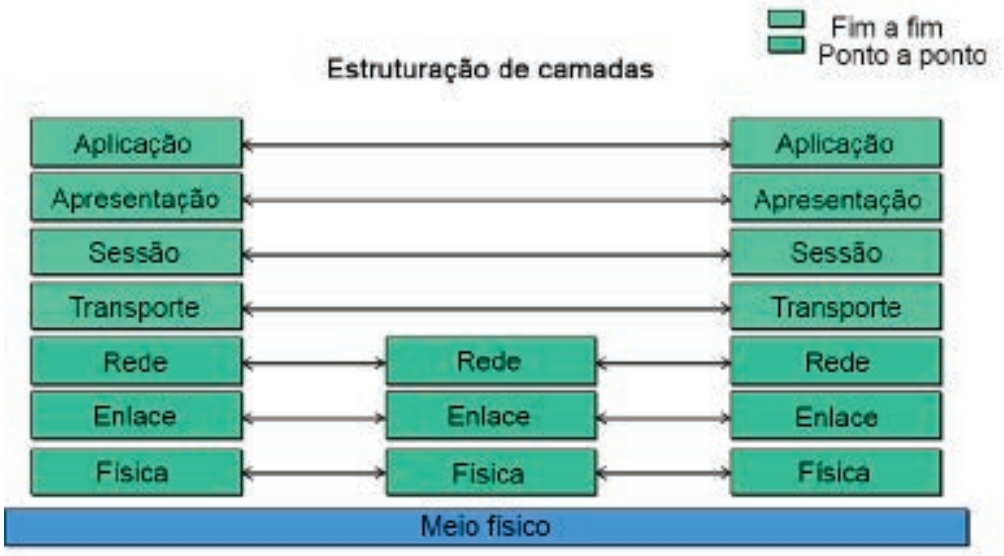


Figura 16. Modelo de Referência ISSO/OSI.

Em cada camada é definida uma unidade de dados (PDU – Protocol Data Unit) trocada entre as entidades do protocolo dessa camada e transportada como dados na camada imediatamente inferior (encapsulamento) e, assim, sucessivamente até serem sinalizados como uma sequência de bits na camada física. Para que a comunicação entre unidades pares num nível possa ocorrer, é preciso que uma conexão no nível inferior tenha sido estabelecida entre os sistemas comunicantes.

Alguns conceitos importantes:

- Serviço: diz o que uma camada faz;
- Interface: diz como acessar o serviço;
- Protocolo: diz como a interface é implementada.

Para cada camada são especificados o serviço provido, a interface de acesso e o protocolo propriamente dito. A partir de agora, vamos descrever, sucintamente, cada camada.

Primeira camada – FÍSICA:

São especificados os três aspectos sobre a conexão física e a sinalização de bits em cada tipo de meio físico existente (cabos metálicos, fibras ópticas e radiodifusão), em todas as suas variantes tecnológicas.

Na camada física, o **serviço** provê os meios mecânicos, elétricos e funcionais de procedimentos para ativar, manter e desativar conexões físicas para a transmissão de bits entre as entidades. A **interface** especifica como enviar um bit de informação e o **protocolo** indica o esquema de codificação utilizado para representar um bit, níveis de voltagem, duração de um bit etc.

Segunda camada – ENLACE (ou *link*) LÓGICO:

São definidos três aspectos para a comunicação entre os elementos vizinhos conectados por um segmento de meio físico, para o qual já existe um protocolo de sinalização de bits. O protocolo de enlace lógico define o primeiro nível lógico de uma comunicação, estabelecendo uma estrutura de quadros (*frames*) constituída de um *buffer* delimitado por bytes indicadores de início e fim, com campos de controle do protocolo e dos dados da camada superior (carga útil) transportados no quadro. Os serviços básicos implementados no enlace dizem respeito ao sequenciamento dos quadros, controle de erros e confirmações (*acknowledgment*) de envio.

A transferência de quadros é feita por meio de seu envio com as sequências de bits entre endereços físicos providos pelas interfaces de conexão física entre os elementos conectados.

No caso das redes LAN, quando há mais de uma estação conectada, principalmente por meios de difusão, há a necessidade de disciplinar o acesso ao meio e, neste caso, uma subcamada intermediária entre a física e o enlace é inserida (Camada MAC – de controle de acesso ao meio).

Na camada de enlace, o **serviço** controla a geração de quadros de informação, além de controlar o envio e recebimento de dados através do meio físico, detectando e corrigindo erros e garantindo o sequenciamento correto dos dados, quando este é requerido. A **interface** especifica como enviar uma unidade de dados (quadro) para uma máquina conectada ao mesmo meio físico e o **protocolo** utiliza endereços do nível físico e implementa o controle de acesso ao meio (MAC), por exemplo, como ocorre com a CSMA/CD.

Terceira camada – REDE:

Trata do endereçamento global dos elementos na rede (computadores hospedeiros de aplicações ou estações de usuário) e de roteadores (comutadores), além do roteamento de pacotes entre esses elementos. A função de roteamento é que permite a um pacote ser enviado a qualquer destinatário na rede de forma automática. Tabelas de rotas existentes nos roteadores permitem calcular por quais *links* os pacotes deverão ser enviados para procederem até o destino desejado.

Existem diversos algoritmos de roteamento que foram propostos para diferentes projetos de redes e usados em diferentes fases do roteamento, principalmente na *internet*. Esses protocolos de roteamento fazem uso, em cada elemento intermediário do grafo da rede, dos serviços da camada de enlace para, depois de consultada a tabela de rotas, encaminhar ao próximo elemento na rota estabelecida e, assim, prosseguir até atingir o seu destino.

Na camada de rede, o **serviço** envia pacotes transparentemente para outros usuários da camada de rede num destino específico (que pode ser em outra rede física). Ela pode, ainda, segmentar e remontar pacotes. A **interface** especifica como enviar um pacote para um destino específico e o **protocolo** define um esquema de endereçamento global.

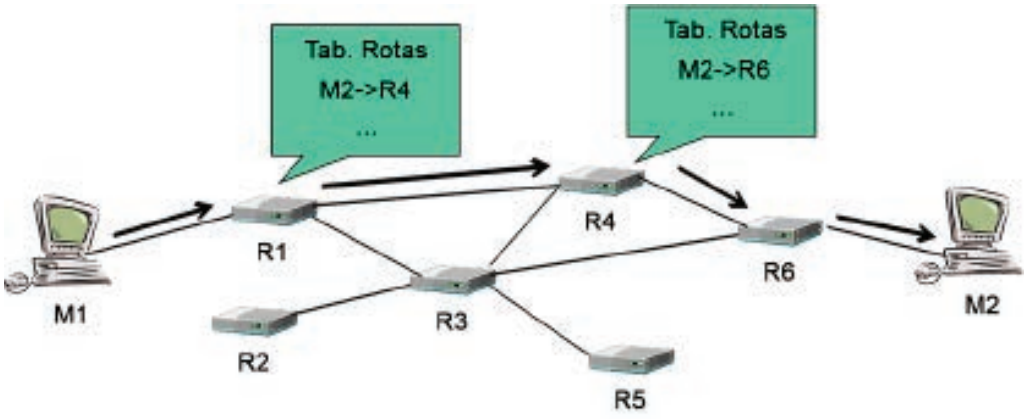


Figura 17. Exemplo de roteamento: pacotes de M1 para M2.

Quarta camada – TRANSPORTE:

É responsável pela comunicação fim a fim entre dois processos em execução nos computadores de origem e de destino, interligados por meio da rede. Como a camada de rede consegue entregar pacotes entre estes computadores, os pacotes daquela camada carregam mensagens de transporte que identificam os processos (por meio de identificadores chamados portas de comunicação dos processos) e implementam a comunicação entre eles, abstraindo a existência da rede.

Na camada de transporte, o **serviço** provê uma conexão fim a fim livre de erros e com controle de fluxo, além de multiplexar várias conexões de transporte numa conexão de rede. O **serviço** da camada de transporte é capaz de prover comunicação orientada a conexão. A **interface** especifica como enviar um pacote para um destino específico e o **protocolo** implementa a confiabilidade (recuperação de erros) e controle de fluxo.

Quinta camada – SESSÃO:

A camada de sessão estabelece e gerencia o diálogo entre processos remotos que se comunicam pela rede. Ela implementa o modelo cliente/servidor, no qual processos ditos servidores executam tarefas (ou aplicações) como serviços, invocados por outros processos remotos ditos clientes desses serviços, num mecanismo de Chamada Remota de Procedimentos – RPC (ou invocação remota de métodos – RMI).

Na camada de sessão, o **serviço** provê, aos usuários dos seus serviços, meios para estabelecer conexões, chamadas sessões, e transferir dados de uma maneira ordenada. As sessões são conexões identificadas de uma forma particular. Podem, por exemplo, conter a identificação do usuário. A **interface** é dependente do serviço e o **protocolo** controla o acesso ao nível de usuários, pontos de checagem (*checkpoints*) e possíveis ações de reversão (*rollback*).

Sexta camada – APRESENTAÇÃO:

Numa rede composta por sistemas (*hardware* e/ou *software*) de diferentes tecnologias (por exemplo: *Windows*, *Linux* etc.) é necessário que se estabeleça uma interface padrão de objetos (dados, arquivos, serviços, dispositivos etc.) comum a todos os sistemas interconectados para que, numa comunicação, as interpretações na origem e no destino não sejam diferentes.

Esta camada visa, portanto, estabelecer os padrões dos objetos trocados

na rede, bem como suas interfaces, de modo a homogeneizar esses objetos quanto ao seu significado. Padrões de especificação de objetos são usados para tanto (por exemplo: a linguagem de notação sintática abstrata ASN.1).

Na camada de apresentação, o **serviço** converte dados entre diversas representações, preservando o significado dos dados transportados. A **interface** é dependente do serviço e o **protocolo** define os formatos de dados e as regras para converter de um formato para outro.

Sétima camada - APLICAÇÃO:

A camada mais alta da pilha de protocolos tem a função de definir as interfaces e os serviços disponíveis na rede para utilização pelas aplicações de usuários. São os serviços que a rede dispõe aos usuários. Por exemplo, pode-se citar a Transferência de Arquivos (protocolo FTP), a comunicação por telefonia IP (VoIP), a troca de mensagens de *e-mail* (serviço SMTP) etc. Na camada de aplicação o **serviço,** a **interface** e o **protocolo** são dependentes da aplicação.

O modelo ISO/OSI, embora tenha sido proposto como referência e aceito a princípio pela comunidade de desenvolvimento das redes, tem alguns problemas: não contempla a interligação natural entre redes diferentes, pois pressupõe apenas uma grande rede e a sua interconexão ocorre, por meio de elementos (*gateways*), com todas as camadas em ambas as redes. Além disso, não teve, ao longo do tempo, a definição de um padrão para todas as camadas.

Com o projeto da rede ARPANet, dando ênfase à comutação por pacotes, houve um processo de definição detalhada de algumas camadas relativas ao modelo ISO/OSI, principalmente enfocando a camada de redes como inter-redes (*internet*) onde, por meio do protocolo IP do conjunto TCP/IP, adotado como padrão, é possível, a qualquer rede que utilize estes protocolos, se conectar a outra.

Desta forma, definiu-se um novo modelo de apenas 4 camadas, tecnologia de interconexão (físico e enlace), inter-redes (IP), transporte (TCP-UDP) e aplicação, que foi adotado para a *internet*, prevalecendo sobre o modelo ISO/OSI e que acabou servindo como referência teórica para comparação de projetos.

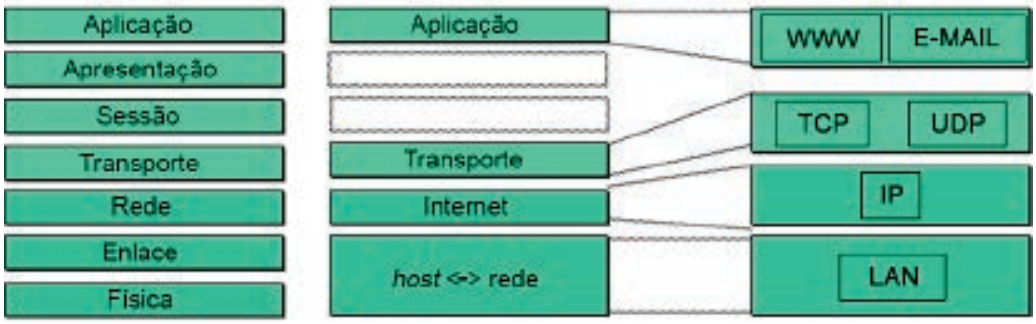


Figura 18. Modelo ISO/OSI *x* Modelo TCP/IP.

Enquanto o modelo OSI conceitualmente define serviço, interface e protocolo, o modelo TCP/IP provê uma implementação bem sucedida. Vejamos alguns de seus protocolos:

- Protocolo IP (Internet Protocol):
  - Protocolo de baixo nível utilizado para a transmissão de pacotes entre *hosts* fonte e destino através de meios heterogêneos;
  - Inclui facilidades de segmentação e remontagem de pacotes;
  - Implementa diversos sinais de controle em seus cabeçalhos;
  - Implementa um tempo de vida (TTL);
  - Normalmente não é utilizado diretamente pelas aplicações.
- Protocolo TCP (Transmition Control Protocol):
  - Protocolo com o maior uso na *internet* atualmente;
  - Colocado no topo do IP, formando o TCP/IP;
  - Implementa confiabilidade;
  - Verifica integridade dos dados (*check-sum*) e retransmissão de dados;
  - Implementa controle de fluxo.
- Protocolo UDP (User Datagram Protocol):
  - Transmissão não orientada a conexão;
  - Politica de *best-efforts*;
  - Semântica de dados orientada a pacotes;
  - Protocolo leve e eficiente;
  - Requer consideravelmente menos processamento que o TCP;
  - Dados enviados para aplicação assim que chegam.

O Modelo TCP/IP engloba, na realidade, diversos outros protocolos associados à quatro camadas, permitindo a interconexão de diversas tecnologias de redes, desde as redes PAN, LAN, até as redes WAN, provedores (ISP) e redes

de acesso (METRO), todas interligadas formando a estrutura da *internet*.

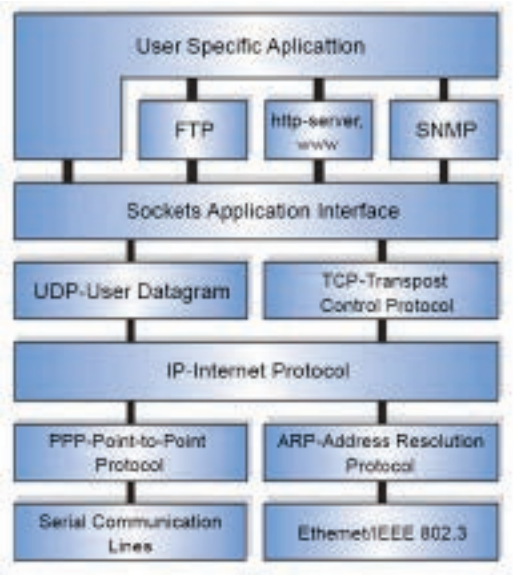


Figura 19. Organização dos protocolos no modelo TCP/IP.

1.10 Referências

ALEXANDER GRAHAM BELL. In: *WIKIPÉDIA*, a enciclopédia livre. Flórida: Wikimedia Foundation, 2013. Disponível em: <http://pt.wikipedia.org/w/index.php?title=Alexander_Graham_Bell&oldid=37211390>. Acesso em: 19 nov. 2013.

BRISA. *Sociedade Brasileira para Interconexão de Sistemas Abertos*. Arquitetura de Redes de Computadores OSI e TCP/IP, 2a ed. Makron, 1997.

COMMER, D. *Redes de Computadores e Internet*, 2a ed. Bookman, 2001.

KUROSE, J. F.; ROSS, K. W. *Redes de Computadores e a Internet*: uma abordagem top-down. Tradução da 3a ed. Pearson, 2006.

HUMMEL S. *Network Planning and Design Guide*, 1a ed. Design Series, 2005.

OLIFER, N.; OLIFER, V. *Redes de Computadores*: Princípio, Tecnologias e Protocolos para o Projeto de Redes. Tradução da 1a ed. LTC, 2008.

OPPENHEIMER, P. *Top-down Network Design*, 2a ed. Campus, 2004.

TANENBAUM, A. S. *Redes de Computadores*. Tradução da 4a ed. Rio de Janeiro: Campus, 2003.

STALLINGS, W. *Local & Metropolitan Area Networks*, 5a ed. Prentice Hall, 1997.

UNIDADE 2

Meios físicos, tecnologias de transmissão de dados e protocolos de enlace

2.1 Primeiras palavras

Nesta segunda unidade, iniciamos os estudos dos aspectos das camadas físicas e de enlace introduzindo conceitos relativos ao processo de sinalização nos meios físicos, tipos de meios e tecnologias de conexão de redes e aspectos de padronização. Analisamos a camada de enlace enfocando os principais protocolos de controle de acesso ao meio (protocolos da camada MAC – Medium Access Control) e protocolos de enlace, além de aspectos relativos ao projeto de protocolos. Nosso objetivo aqui é estudar como podemos transferir dados entre elementos vizinhos conectados por algum meio físico.

2.2 Introdução

A comunicação entre diferentes elementos de uma rede ocorre sempre por meio de algum tipo de meio físico que interconecta esses elementos. Numa arquitetura de rede mais complexa, vemos diferentes elementos (hospedeiros e comutadores/roteadores) interligados por diversos segmentos de meio físico (linhas telefônicas, pares de cobre, fibras ópticas, rádios, satélites, cabo de TV, cabo de energia elétrica etc.) por meio dos quais os dados fluem verdadeiramente, como sequências de bits que são transmitidas entre um elemento de origem e outro de destino interconectados. Cada meio físico utiliza uma forma se sinalização que lhe é própria para demarcar esses bits. O processo de envio segue um protocolo que depende do enlace e do meio, por exemplo, uma rede Ethernet pode utilizar como meio físico tanto um par trançado quanto um cabo coaxial, de fibra óptica ou um rádio (*wireless*). Para cada meio, esta rede utilizará uma técnica diferente de sinalização de bits, porém o protocolo de controle do enlace, entre os elementos para troca dos quadros de informação (formado por sequências de bits a serem trocados), é o mesmo.

2.3 Roteiro da unidade

- Teoria básica de transmissão de dados;
- Meios físicos abertos e guiados;
- Protocolos de acesso a redes locais e protocolos de enlace;
- Padronização das tecnologias de redes.

2.4 A camada física

A conexão entre um elemento da rede, por exemplo, um computador (hospedeiro ou *host*) e o meio físico que ela utiliza ocorre por meio de uma interface de conexão (NIC – Network Interface Card) caracterizada por um cartão (circuito) composto de um encaixe, no barramento do computador, de circuitos que promovem protocolos de controle de acesso e circuitos de sinalização e leitura do meio físico.

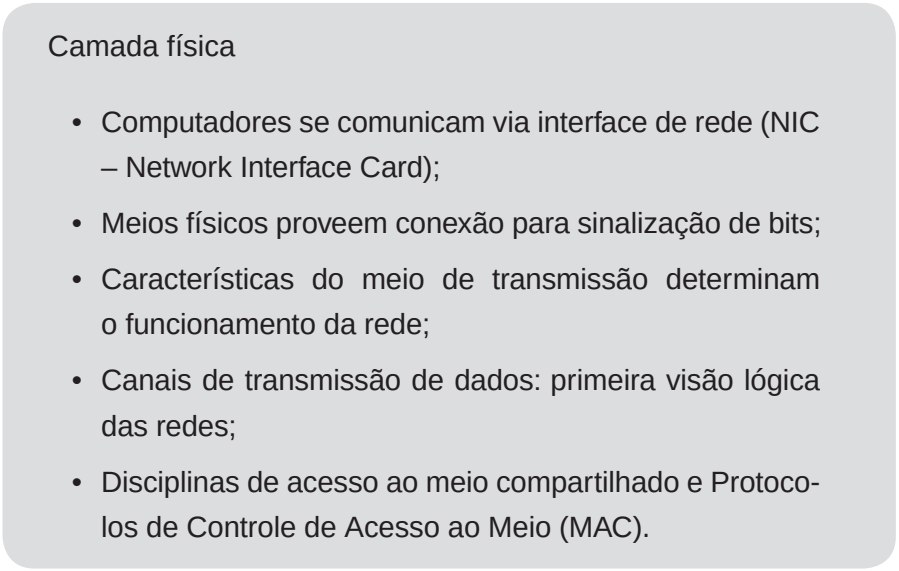


Figura 1. Introdução à camada física.

O controle do meio físico é então feito pela troca de quadros que são enviados como sequências de bits. Esse controle é que promove a visão lógica da interconexão (*link* lógico), dando uma ideia de existência de um canal, entre os dois elementos de origem e de destino, por onde fluem os quadros.

Entretanto, dependendo da tecnologia de interconexão e do meio físico utilizado, o funcionamento das redes pode ser diferente. Por exemplo, numa rede em anel, temos conexões ponto a ponto entre os elementos e os quadros que circulam numa dada direção passando por todos os *links* e formando um ciclo. Já nas redes Ethernet, um meio único (barramento) interconecta todos os elementos, sendo por eles compartilhado, o que sugere a necessidade de arbitração para decidir quem tem direito de transmitir a cada instante. Neste caso, usa-se um protocolo chamado CSMA/CD, que veremos mais à frente.

Análise de Fourier (1904) – espectro de sinal:

- Qualquer função g(t) periódica, com período T, pode ser escrita como uma soma de senos e cossenos cujos termos são as amplitudes dos senos e cossenos da n--ésima harmônica;
- Sinais limitados pela largura de banda;
- Largura de banda diz respeito à faixa de frequências onde um sinal pode ser transmitido sem atenuação. É medida em Hertz (Hz) ou em bits por segundo (bps);
- Taxa máxima de dados num canal;
- Teoremas de Nyquist e Shannon (1948): depende da taxa de frequência máxima possível de transmitir-se no meio e da relação sinal/ruído.

Figura 2. Base teórica da comunicação de dados na camada física.

A análise de Fourier (1822) permite expressar uma função periódica g(t), representante de um sinal, como uma soma de harmônicos desse sinal. Desta forma, se soubermos quais são os coeficientes dos senos e cossenos que definem as harmônicas, podemos recuperar a função e, portanto, o sinal no receptor.

$$g(t) = \frac{1}{2}c + \sum_{n=1}^{\infty}\left(a_n \text{sen}(2\grave{A}nft)\right) + \sum_{n=1}^{\infty}\left(b_n \cos(2\grave{A}nft)\right)$$

onde

$f = \frac{1}{T}$ é a frequência fundamental, e são as amplitudes do seno e do cosseno do n-ésimo harmônico, uma constante (num meio físico, é 2/3 da velocidade da luz, aproximadamente 3×10^8 m/s).

Um sinal de dados com duração finita é visto como uma repetição de um padrão único em intervalos idênticos: T, 2T, 3T etc.

Como exemplo, em Tanenbaum (2003) é apresentada uma análise da transmissão do caractere ASCII “b”, codificado como um byte de 8 bits. Assim, o padrão a ser transmitido é 01100010. A figura 3 (na página 41) mostra a saída de voltagem do computador transmissor e as amplitudes de médias quadráticas $\sqrt{an^2 + bn^2}$ dos primeiros termos, proporcionais à energia transmitida.

Como nenhuma transmissão é possível sem perda de parte da energia ao longo do meio físico, reduzindo os coeficientes da série de Fourier e gerando distorções no sinal obtido (medido), as amplitudes são consideradas até uma frequência de corte (f_c), sendo todas frequências acima disso atenuadas.

Por definição, então, a largura de banda (LB) de cada meio refere-se à faixa de frequências na qual um sinal pode ser transmitido sem ser atenuado, isto é, diminuído. Frequências são medidas em ciclos por segundo (ou Hertz, em homenagem a seu descobridor), ou ainda em bits por segundo (bps), pela capacidade de sinalização de bits. Quanto maior a frequência, maior a taxa de bits sinalizados por segundo.

A largura de banda é uma propriedade física do meio e depende de parâmetros, tais como o comprimento, a espessura, o material utilizado etc. Na prática, usam-se filtros para delimitar a LB para o cliente como forma de simplificar o processo de transmissão e limitar o uso de recursos. Como exemplo, podemos citar a transmissão de voz humana em meios telefônicos que, embora possam operar a 1MHz de faixa de frequências, é limitado 3.100Hz para fins de simplificação e melhor eficiência de voz.

Nyquist (1924) e Shannon (1948) estabeleceram expressões que delimitam a taxa máxima de bits num dado canal, em função de sua LB, considerando a relação sinal/ruído existente em qualquer meio físico de transmissão. Assim, a LB operacional de um meio é delimitada por essas expressões:

Número máximo de bits/s = $H \log_2 (1 + S/N)$,

onde H_{Hz} é a LB e S/N é a relação sinal ruído.

2.4.1 O espectro eletromagnético

Maxwell (1865) e Hertz (1887) observaram que o movimento de *elétrons* num campo gera ondas eletromagnéticas que podem se propagar até no vácuo. O número de oscilações por segundo em que estas ondas se propagam ou de sua frequência (f) de oscilação é medido em Hertz (ou ciclos/segundo). O comprimento de uma onda é a distância entre dois pontos equivalentes de amplitude de oscilação (λ)

No vácuo, uma onda se propaga à velocidade da luz (c = aproximadamente $3X10^8$ m/s), mas num meio físico essa velocidade é cerca de 2/3 desse valor.

A relação fundamental entre f, λ e c é: $\lambda f = c$.

Como c é uma constante, dada λ temos f e vice-versa.

O espectro eletromagnético é a faixa total de frequências conhecidas que

são medidas em escala de potências de 10Hz.

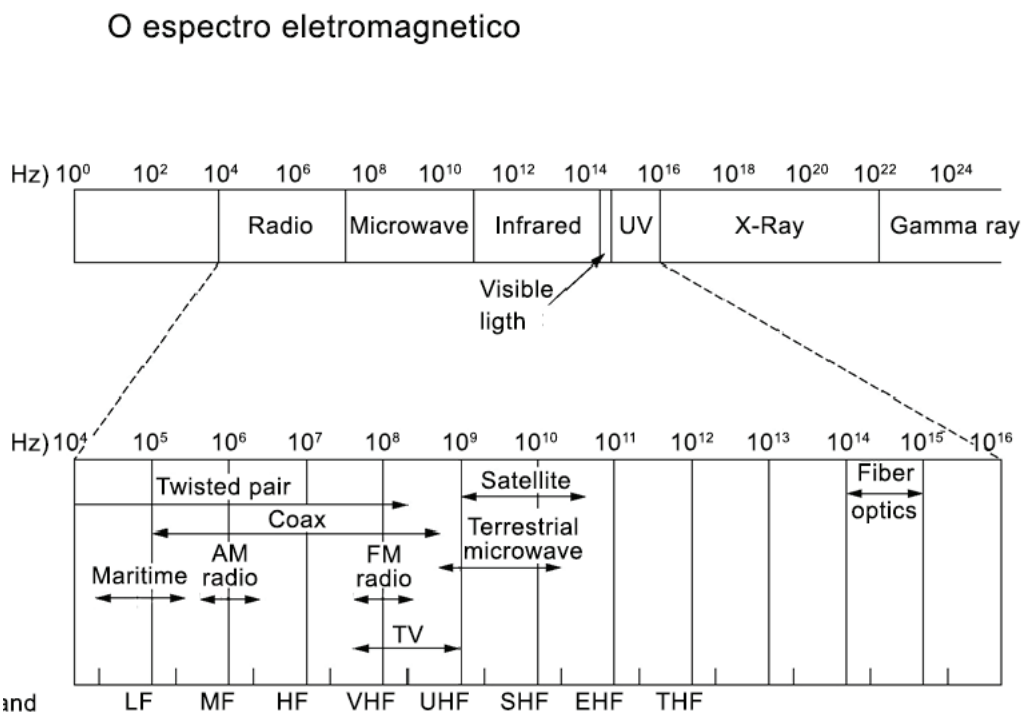


Figura 3. Espectro eletromagnético.

Observa-se, na figura, que a partir de 10^4 tem-se as várias faixas e os diferentes meios de transmissão conhecidos (de radio, TV (VHF e UHF), micro-ondas, infravermelho e luz visível), desde o rádio marítimo até as fibras ópticas e, na medida em que as frequências se elevam, a transmissão no meio é mais rápida. Acima da luz visível, temos as faixas de ultravioleta (UV), raios X e raios gama (da radiação nuclear) que são prejudiciais à saúde e, portanto, de pouco provável utilização. O volume de informações que um meio pode transportar é proporcional à sua LB. Atualmente é possível codificar-se alguns bits por Hertz, sendo comum a codificação de 8bits em altas frequências. Desta forma, um cabo com LB de 750MHz é capaz de transmitir alguns Gbps. Uma fibra de 1.3 *microns* opera em frequências de cerca de 30THz, a 8bits/Hz, e resultaria numa capacidade de transmissão de 240Tbps.

2.4.2 Meios físicos guiados (cabos)

Os meios físicos possíveis são baseados em cabos (os meios guiados eletromagnéticos e ópticos) e os meios abertos baseados em radiodifusão ou laser.

Iniciando pelos meios guiados temos:

2.4.2.1 Par trançado:

Consiste em pares de fios trançados (TP – Twisted Pair) para dar proteção contra interferências eletromagnéticas externas, pois a inversão dos cabos tende a anulá-las. Seu uso mais conhecido é no sistema telefônico. A LB, nesses cabos, depende do comprimento e da espessura do fio e permite transmitir tanto sinais analógicos quanto digitais, podendo transmitir diversos Megabits/s por alguns quilômetros. Possuem um custo relativamente baixo.

O padrão de cabo de par trançado é definido por categorias que indicam o número de vezes em que foram trançados por centímetro. Para redes, os de interesse são: a) o de categoria 3 (UTP – Unshielded Twisted Pair), LB de 16MHz, com 4 pares formando um cordão envolto numa capa plástica, transmitindo em Kbps. Interliga computadores a um armário de fiação em cada andar de um edifício; b) o de categoria 5, LB de 100MHz, com mais voltas por centímetro, tem melhor imunidade a interferências e menor taxa de erros de transmissão. Permite maior velocidade de transmissão (Mbps); c) os de categorias 6 e 7, ainda em processo de padronização, para redes de alta velocidade, com LB de 250Mhz e 600MHz, permitem atingir velocidades de transmissão de até Gigabps.

Figura 4. (a) categoria 3 UTP; (b) categoria 5 UTP.

Existem três tipos principais:

- *Unscreened*: os cabos estão apenas trançados, sem outra proteção. Baixo custo e fácil manipulação. Alta taxa de erros e distâncias mais curtas;
- *Screened*: os cabos são envolvidos numa fita metálica. Reduz erros, mas aumenta-se o custo;
- Uniforme: recente. Os pares são trançados uniformemente na fabricação. Bastante imune a ruídos e custo mais alto.

2.4.2.2 Cabo coaxial:

Consiste em um cabo composto por um núcleo isolado e blindado por uma malha externa de proteção (gaiola de Faraday) que lhe oferece maior proteção e lhe permite comprimentos maiores que o par trançado. Sua estrutura de proteção, com a malha aterrada, lhe oferece uma LB de 1Gbps e boa imunidade a ruído. Cabos de 50Ω eram usados para LAN e 75Ω para TV a cabo e redes metropolitanas.

Possuem duas formas principais:

Cabo grosso: também conhecido como “cabo amarelo”, é a forma original. Sua capacidade em termos de velocidade e distância é grande (500m), mas seu custo é alto e sua espessura dificulta sua passagem.

Cabo fino: foi criado para reduzir custos. Está associado principalmente às redes Ethernet. Sua capacidade de distância é reduzida (180m).

2.4.2.3 Fibra óptica:

Consiste na transferência de luz por meio de um cabo composto por um fio fino de vidro transparente envolto em uma camada de proteção. A transmissão ocorre pela injeção de luz por Diodo (LED – Light Emitting Diode) num extremo. Sua reflexão, dentro da fibra, e recepção da luz, por uma célula fotoelétrica na saída, converte o sinal recebido em pulsos elétricos, indicando um bit 1 ou nada, indicando bit 0, num modelo unidirecional de transmissão. O posicionamento adequado do LED permite que nenhuma luz seja refratada e perdida, permitindo que esta caminhe por longas distâncias. Por ser um meio bastante puro e uniforme, a fibra permite comprimentos de quilômetros sem atenuação significativa do sinal.

Cada ângulo permite que um raio de luz diferente possa ser introduzido na mesma fibra, assim, dizemos que cada raio associado a um comprimento de onda define um modo e, dessa forma, temos fibras monomodo, isto é, que transmitem apenas um comprimento de onda e multimodo que transmitem diversos comprimentos de onda. Com diâmetro reduzido a alguns comprimentos de onda (alguns *micros*) a luz será guiada pela fibra, como em linha reta sem atenuação, podendo chegar a taxas superiores a 50GBps em 100Kms, sem amplificadores de sinal.

Como é feita de vidro, a atenuação da luz no vidro depende do comprimento de onda da luz (cor), podendo ser medida em decibéis por quilômetro linear de fibra. A comunicação por fibra óptica utiliza três bandas de comprimentos

de ondas, centralizadas em 0.85, 1.30 e 1.55 *micron* respectivamente, com LB entre 25.000 e 30.000GHz.

Os cabos de fibra se assemelham aos metálicos, no sentido de que são agrupadas diversas fibras em cada cabo. No centro de cada cabo tem-se um núcleo de 50 *microns* (fio de cabelo) nas fibras multimodo ou 10 *microns* para as monomodo. Esse núcleo é revestido por vidro com índice de refração inferior ao do núcleo, de modo a reter a luz dentro dele, e por uma cobertura plástica de revestimento de cada cabo. Para proteção, as fibras dentro de um cabo têm ainda uma capa plástica externa.

A conexão por fibras pode ser feita de três maneiras:

- Por meio de conectores de fibras: existe uma variedade deles, cada um para um uso específico que depende de comprimento, modo, velocidade de transferência etc.;
- Através de junções mecânicas (luvas): mecanismos de junção de duas fibras que permitem estender o segmento pela fixação de uma fibra em frente à outra finamente direcionadas de modo a não perder luz;
- Por meio de fusão de fibras: as fibras são aquecidas nas pontas por um mecanismo que as funde formando uma única peça. Exceto pela pequena atenuação no local, a fusão é a que menor perda de luz oferece.

A sinalização ocorre por meio da emissão de luz via dois dispositivos emissores possíveis: o LED (Light Emitting Diode) que consiste num diodo iluminável com luz relativamente direcional; e os lasers, com potência muito maior de emissão de luz direcional.

Já a recepção ocorre através de um fotodiodo, dispositivo sensível a certos comprimentos de luz, capaz de emitir um pulso elétrico quando excitado por ela. O tempo de resposta do fotodiodo determina a taxa de transmissão (exemplo: 1Gbps para diodos de 1 nanosegundo de tempo).

As fibras podem ser usadas tanto para conexões de redes LAN quanto de redes WAN. Como cada fibra transmite numa única direção, pois tem um transmissor de um lado e um receptor do outro, é necessário um par delas para transmissões bidirecionais.

Muito mais eficientes que os meios metálicos, as fibras, entretanto, são mais caras, razão pela qual ainda não são plenamente utilizadas.

Diversas alternativas para redes de fibras ópticas foram propostas. Em outro segmento do texto abordamos redes de comutação totalmente óptica (DWDM).

2.4.2.4 Sistemas de cabeamento estruturado:

Com a evolução dos meios físicos, surgiu também a necessidade de estabelecer modelos e normas para cabeamento de redes em edifícios. Para isso, foi criado o Sistema de Cabeamento Estruturado (SCS – Structured Cabling System) que consiste em um conjunto de elementos de comutação (cabos, quadros, conectores, soquetes, mesas e armários) e métodos para sua utilização, de modo a construir estruturas de comunicação facilmente extensíveis e replicáveis. Baseada na estrutura dos edifícios, a estrutura dos sistemas de cabeamento estruturado consiste numa hierarquia de blocos funcionais utilizados pelo projetista de redes para construção de uma configuração de rede padrão. Tal processo permite expansão e manutenção adequadas.

A estrutura básica de um sistema de cabeamento estruturado é formada por:

a) Subsistemas horizontais: conectam quadros de comutação nos andares dos edifícios aos soquetes de usuários finais nas salas;

b) Subsistemas verticais: conectam os quadros de comutação em cada andar à sala de equipamentos daquele edifício;

c) Subsistemas de campus: interligam os diversos edifícios de um campus (ou planta industrial) à sala de equipamentos central do campus. Este subsistema é denominado *backbone* da rede do campus.

Se bem estruturada, a rede de uma empresa pode integrar tráfego de dados, telefonia, sistemas de monitoramento (sensores, câmeras etc.) tudo pelo mesmo conjunto de meios físicos compartilhados, promovendo economia, organização, gerenciamento, facilidade de manutenção e de estabelecimento de políticas de uso e de expansão.

O custo de uma rede é definido mais pelo custo de sua instalação (obras) que pelo custo dos cabos. Assim, um projeto bem elaborado, estruturado e com previsão de crescimento pode ser determinante tanto no desempenho da rede quanto no custo final.

Ao longo do texto, teremos mais detalhes acerca da abordagem do projeto estruturado de redes.

- Elementos de conexão e comutação de dados organizados segundo padrões específicos;
- Estrutura hierárquica:
  - Subsistemas horizontais: conectam cada andar de um edifício e seus usuários;
  - Subsistemas verticais: conectam andares à central de equipamentos de comunicação do edifício;
  - Subsistemas de campus (*backbone*): conectam diferentes edifícios.

Figura 5. Sistemas estruturados de cabeamento.

2.4.3 Meios físicos abertos

O lançamento de cabos nem sempre é possível. Dependendo do local são necessárias outras alternativas e a demanda pela integração das pessoas às redes (inclusão digital) cresce dia a dia.

Considerando situação geográfica, distâncias e a mobilidade proporcionada por dispositivos atuais cada vez mais ubíquos (exemplos: celulares, embarcados, *notebooks* etc.), as alternativas residem na possibilidade do uso de mídia não cabeada, baseadas na radiofrequência e na emissão de luz.

2.4.3.1 Radiofrequências:

- Transmissões de rádio;
- Luz visível;
- Micro-ondas;
- Satélites;
- Telefonia;
- Infravermelho.

Figura 6. Meios físicos abertos: radiofrequências.

No campo da transmissão por rádio (ou transmissão sem fio – *wireless*) temos diversas tecnologias possíveis que englobam desde a radiodifusão, micro-ondas, satélites de comunicação, telefonia móvel celular, infravermelho e *bluetooth*.

2.4.3.2 Transmissão por ondas de rádio:

Ondas de rádio são muito utilizadas em comunicações, pois são fáceis de serem geradas, se propagam por longas distâncias e penetram bem nos edifícios. Por serem omnidirecionais, isto é, se propagam por todas as direções, não necessitam de alinhamento entre transmissor e receptor. Suas propriedades estão diretamente relacionadas às frequências em que elas são geradas. Em frequências baixas elas são de comprimento λ, (longas dezenas de metros) e, portanto, atravessam obstáculos sem perda significativa de sinal, mas com perda rápida de potência ($1/r^2$ no ar) à medida que se afasta da fonte. Em altas frequências, seu comprimento é muito curto (micro-ondas) e tendem a viajar em linha reta, necessitando alinhamento do receptor com a fonte. Elas ricocheteiam nos prédios e são facilmente absorvidas inclusive palas moléculas de água (que se aquecem com ela), sendo imprópria para transmissão na chuva. Além disso, ondas de rádio são suscetíveis a interferências eletromagnéticas como as de motores, indutores e outros equipamentos elétricos.

A distância percorrida por uma onda de rádio depende de sua potência. Por isso, as emissoras de rádio são limitadas, neste aspecto, pelos órgãos reguladores (no Brasil, a ANATEL). Nas bandas de frequências VLF, LF e MF do espectro, as ondas de rádio trafegam próximas do solo e acabam absorvidas por ele, dada a curvatura da terra, propagando-se até cerca de 1000km. As ondas na banda HF e VHF podem se projetar para o espaço, sendo refletidas pela ionosfera e retornam à terra, podendo dar a volta em todo o globo por este processo de reflexão.

2.4.3.3 Micro-ondas

Em frequências superiores a 100MHz, as ondas têm comprimento de poucos centímetros e trafegam em linha reta, com todos os problemas já citados de absorção e ricocheteamento em obstáculos, além da necessidade de alinhamento (visada). Entretanto, pode ser encaminhada por uma faixa estreita, o que possibilita concentrar toda energia de uma transmissão em um feixe por meio de uma antena parabólica, oferecendo uma boa relação sinal/ruído. Essa possibilidade é que permitiu o uso de sistemas de comunicação por micro-ondas pelas torres e antenas, formando um *backbone* entre bancos, empresas, concessionárias de telefonia etc.

Considerando a curvatura da terra, é necessário o uso de repetidores entre pontos muito distantes de micro-ondas (uma torre de 100m a cada 80km). As faixas operacionais de micro-ondas são acima de 4GHz. Porém, nesta faixa ocorre a absorção pela água e refração pela atmosfera quando aquecida, provocando retardamento de ondas e diferenças de fase, com cancelamento de sinal (*multipath*

fading). De todo modo é uma tecnologia barata se comparada com as fibras ópticas e permite transmitir em locais onde o uso de meios cabeados seja impossível.

- Acima de 100MHz, praticamente em linha reta;
- Muito usada em telefonia à distância, celulares e TV;
- Devido à curvatura da Terra, necessita de repetidoras;
- Custo baixo. Não necessita de cabeamento;
- Quanto mais altas as torres, mais distantes pode-se estar uma das outras;
- Não atravessam bem obstáculos;
- Pode haver atenuação nas camadas mais baixas da atmosfera;
- Devido às condições atmosféricas e à frequência, pode ocorrer esmaecimento de vários caminhos (*multipath fading*);
- A partir de 4GHz sobre absorção pela água;
- Solução: criação de rotas alternativas para emergências.

Figura 7. Micro-ondas.

2.4.3.4 Infravermelho

Com comprimento de poucos milímetros, o infravermelho trata de ondas em frequências na faixa de 10^{12} a 10^{14}Hz, beirando a luz visível. Esta faixa permite comunicação de curto alcance, típico dos aparelhos de controle remoto usados em televisores, portões automáticos etc.

Sua desvantagem é não atravessar nenhum elemento sólido (exemplos: paredes, pessoas etc.), sendo possível ser usado em situações limitadas, em geral. Entretanto, tem sido utilizado para redes pessoais PAN (visando eliminar cabos de conexão, conectando computadores aos seus periféricos (como impressoras, por exemplo). Necessita de boa visada. Opera nas faixas não licenciadas, porém com baixa frequência e curtas distâncias, portanto.

- Curto alcance;
- Exemplo: controle remoto;
- Não atravessa objetos;
- Vantagens: não precisa de regulamentação;
- Usado em dispositivos de segurança.

Figura 8. Transmissão em infravermelho.

2.4.3.5 Ondas de luz – *lasers:*

Em faixas de frequência pouco acima de 10^{14}Hz, numa banda de 25.000GHZ, temos a luz visível com seu espectro variando do vermelho ao violeta. Nessa banda, se situam as ondas de comprimento 0.8 e 1.8 *microns*. E nesta faixa que se emprega os lasers como mecanismo de envio concentrado de luz direcional de alta potência e coerência. É possível transmitir usando feixe de laser de 1mm a distâncias da ordem de 500m com uso de lentes para desfocarem o feixe e aumentarem seu diâmetro, visando possibilitar o alinhamento da fonte e do receptor.

- Unidirecional: cada lado precisa possuir seu próprio laser e fotodetector;
- Difícil alinhamento;
- Para facilitar, utiliza-se lentes;
- Calor pode desviar o feixe.

Figura 9. Transmissão por luz sem guia: *lasers*

A dificuldade no uso de lasers está em sua absorção na chuva ou neblina espessa e o desvio do feixe pela ação de convecção no ar devido ao aquecimento provocado pela luz solar.

2.4.3.6 Satélites:

Com início na década de 1950, os satélites deram um avanço bastante grande nas telecomunicações, principalmente com o lançamento do satélite geossíncrono TELSTAR em 1962. As telecomunicações passaram a partir daí a movimentar milhões de dólares pela possibilidade da conexão entre indivíduos localizados em diferentes continentes, tanto para telefonia como para TV e

computadores.

Inicialmente, as pesquisas utilizaram balões meteorológicos metalizados como refletores de sinais de volta à terra, sem muito sucesso. Um satélite caracteriza-se por um repetidor de sinais de micro-ondas colocado em órbita, retransmitindo os sinais a ele dirigidos por um canal de subida (*upload*), por meio de inúmeros canais de descida (*download*), via *transponders* (receptores-amplificadores-emissores) que "ouvem" uma dada faixa de frequências, amplificando-a e retransmitindo-a em outras faixas, cobrindo uma área ampla (parte da superfície da terra) ou mesmo estreita (centenas de quilômetros de diâmetro). Sua altura determina o período da órbita, isto é, o tempo de exposição ou cobertura de uma região na terra.

O posicionamento do satélite em órbita depende de diversos fatores. Seu período, área de cobertura, altitude, relacionada ao tempo de subida e descida e potência do sinal e, ainda, fatores geo-espaciais como os cinturões de Van-Allen, anéis de partículas sólidas presas ao redor da terra por ação da gravidade, capazes de destruí-los, definem três altitudes para o posicionamento, em órbita, de satélites:

- Satélites GEO (Geostationary Earth Orbit). Situados a cerca de 35.800km de altitude, com órbita no equador, têm velocidade orbital igual a da terra, pairando sempre no mesmo ponto e o céu. O primeiro foi o Telstar, lançado em 1962. Cobrem uma área de 3/4 da terra, sendo necessários apenas três desses para cobertura total. Pelo espaçamento necessário de 2 graus entre eles, é possível ter no máximo 180 satélites GEO simultaneamente em órbita. O controle dos *slots* (espaços) para cada satélite e das frequências que eles utilizam é regulamentado pelo ITU (International Telecommunication Union);
- A comunicação ocorre por meio de antenas (VSAT – Vey Small Aperture Terminals) para envio do sinal de subida a 19,2Kbps e recepção do retorno a 512Kbps. Os usos mais comuns são telefonia, transmissão de TV e *internet*. Empresas alugam canais para comunicação interna.

- Idealizados em 1945 pelo escritor de ficção científica Arthur C. Clarke;
- Descritos como dispositivos que trafegam a 35.800km de altitude, acompanhando a rotação da Terra;
- Primeiro a ser lançado: Telstar em 1962;
- Atuais: Intelsat, Brasiltat etc.;
- 4 satélites GEO podem cobrir toda a Terra (3 para as regiões habitadas);
- Mesmo na velocidade da luz há um atraso significativo (aproximadamente 0,27 segundos);
- 5 bandas operacionais:

Band	Downlink	Uplink	Bandwidth	Problems
L	1.5 GHz	1.6 GHz	15 MHz	Low bandwidth; crowded
S	1.9 GHz	2.2 GHz	70 MHz	Low bandwidth; crowded
C	4.0 GHz	6.0 GHz	500 MHz	Terrestrial intereference
Ku	11 GHz	14 GHz	500 MHz	Rain
Ka	20 GHz	30 GHz	3500 MHz	Rain; equipament cost

Figura 10. Satélites GEO (Geostationary Earth Orbit). O atraso de *round trip* (viagem) do sinal é de 0,37 segundos.

- Satélites MEO (Medium Earth Orbit): satélites de órbita média, situados entre 5000 e 12000km de altitude, com velocidade angular 5 vezes maior que o da terra, passando pelo mesmo ponto a cada 6 horas. Cobre áreas de cerca de 10000 a 15000km quadrados. Tem atraso de *round trip* de menos de 50ms, porém somente são visíveis por algumas horas a cada passagem. Isso implica na necessidade de *handoff*, isto é, transferência de conexão entre satélites diferentes para manutenção da conexão (semelhante à telefonia celular). Os satélites de GPS se encontram nessa órbita.

- Altitude entre 5000km e 12000km;
- Período orbital de 6 horas;
- Cobertura de 1000km a 15000km quadrados;
- Atraso de *round-trip* de menos de 50ms;
- Visível por algumas horas;
- É necessário *handoff*;
- Aplicações: voz digital, dados e serviços de mensagens;
- Exemplo: GPS (24 satélites a uma altitude de 20200km).

Figura 11. Satélites MEO (Medium Earth Orbit).

- O terceiro tipo são os LEO (Low Earth Orbit): satélites de órbita baixa, situados a menos de 2000km de altitude. Seu período orbital é de cerca de 1 hora e meia a 2 horas, com velocidade angular muito maior que a da terra, ficando visível por cerca de 20 minutos a cada passada. Cobre cerca de 8000kms quadrados e tem *round-trip* de menos de 20ms. Os satélites atuais possuem cerca de 40 transponders, cada um operando numa banda de até 80MHz, cada uma operando por divisão no tempo, ampliando a capacidade de comunicação. A vida útil de um satélite é de cerca de 10 anos. Para organizar o uso das frequências, as bandas de frequências disponíveis foram organizadas em intervalos crescente L, S, C, Ku e Ka.

  - Menos de 2000km de altitude;
  - Período orbital de 1 hora e meia a 2 horas;
  - Cobertura de 8000km;
  - Atraso do *round-trip* de menos de 20ms;
  - Visível por aproximadamente 20 minutos.

Figura 12. Satélites LEO (Low Earth Orbit).

- Três grandes projetos foram propostos para uso de satélites LEO:
  - O Iridium (Motorola) com 66 satélites e 1628 células mapeadas sobre toda a terra. A comunicação, neste caso, entre dois usuários localizados no solos, ocorre por meio da retransmissão entre satélites;
  - O Globalstar com 48 satélites e um conjunto de antenas repetidoras em terra, onde fica a parte mais complexa do sistema;

- Um terceiro projeto seria o Teledesic (Craig Mcaw e Bill Gates) esperando fornecer acesso à *internet* de alta velocidade via satélites LEO (*uplink* de 100Mbps e *downlink* de 720Mps) via antenas VSAT de 1m de diâmetro. Entretanto, foi suspenso em 2002.

2.4.4 Transmissão de dados por *links* telefônicos: a rede pública de telefonia comutada

A conexão de computadores próximos é feita em geral via cabos. Entretanto, quando estão distantes uns dos outros ou os cabos têm que cruzar estradas, ruas ou mesmo cidades, o cabeamento privativo fica inviável, seja por razões financeiras, técnicas ou legais. As soluções passam então a considerar o uso de *links* das operadoras de telecomunicações, ou *links* telefônicos, do sistema de telefonia pública comutada.

No princípio, após Alexander Grhan Bell ter patenteado a invenção do telefone em 1876, cada aparelho tinha que instalar o cabo até o outro aparelho para estabelecer comunicação. Para falar com outros, haveria de lançar fios para todos. Isso levou rapidamente a um caos de cabeamento nas cidades, num modelo totalmente conectado. Em 1878, foi criada a Bell Telephone Company que instalou as primeiras comutadoras num modelo em estrela. Daí o modelo evoluiu para interconexões e comutação em diferentes níveis (hierarquia).

Atualmente esta hierarquia tem cinco níveis, mas os sistemas têm três componentes principais:

1. Loop local: par trançado que conecta o aparelho do usuário à estação comutadora;
2. Troncos: fibras ópticas conectando estações de comutação (chaveamento);
3. Estações comutadoras: que transferem as chamadas entre diferentes linhas.
    - A comunicação de voz é analógica enquanto a transmissão de dados é digital. O uso de Modem, Aparelho Modulador e Demodulador de Sinais, permite transferir dados digitais como tons (som) de sinais de voz. O funcionamento dos Modems permite conectar um computador do usuário via linhas telefônicas a um provedor de serviços *internet* (ISP – Internet Service Provider) na cidade para acesso discado à *internet* com taxa de 56Kbps.
    - Sinais digitais são representados por ondas quadradas, isto é, uma composição de um conjunto grande de frequências que sofrem efeitos de atenuação e distorção. Usando uma onda regular como base de transmissão, na faixa de 1000 a 2000Hz, é modulada o sinal digital

(bits). A modulação desses sinais pode ser feita de várias maneiras. Por variação da amplitude, onde duas amplitudes (0 ou 1) definem os bits. Por variação da frequência, onde duas frequências definem os bits zero e um, com duração fixa. Por modulação de fase, onde deslocamentos da onda portadora (0 ou 180 graus) permite determinar dois estados (2bits).

- O número de símbolos enviados por segundo é dito baud (por exemplo, uma linha de 2400bauds envia um bit a cada 416667 microssegundos). Técnicas de aproveitamento do sinal permitem aumentar o número de bits/baud (por exemplo, se usarmos 3 voltagens diferentes, podemos ter 2bits/símbolo, dobrando a taxa de transmissão para 4800bps, de modo análogo, com quatro deslocamentos da fase, novamente 2bits/símbolos dobrando a taxa de bits. Esta técnica é chamada de QSPK – Quadrature Phase Shift Keying). Esses parâmetros definem a taxa de transferência de um meio.

2.4.4.1 ADSL – Linhas Digitais Assimétricas de Assinante

É uma técnica que transmite dados digitais pelas linhas telefônicas por meio da divisão da LB das linhas separando-as em canais de voz (300 a 3400Hz) e canais de dados (4000Hz a 1MHz). O meio físico de telefonia (par trançado) possui LB de 1MHz, mas são limitados a apenas 300 a 3100Hz para voz, por simplicidade e eficiência. O excesso de banda permite aplicar a técnica de Divisão por Frequências (FDM), permitindo velocidades maiores que as providas pelos Modems. Com esta divisão pode-se obter taxas de até 5000Mbps, embora as emendas de segmentos e a distância reduzam drasticamente estes valores (hoje o serviço é limitado a 8Mbps, sendo oferecido a partir de 512Kbps).

No sistema DMT (Discrete Multi Tone) a banda de 1MHz das linhas é dividida em 256 canais de 4312Hz cada com: 1 canal de voz (POTS – Plain Old Telephone system), 5 canais de separação (para evitar interferência de harmônicos), 1 canal de dados *upstream* e 250 *downstream*.

O modelo de funcionamento da ADSL é o DSLAM – Digital Subscriber Line Multiplexer, onde no lado cliente tem-se um NID – Network Interfce Device (comumente confundido com um Modem) que possui um filtro divisor de frequências para separar a voz analógica dos dados digitais. No lado da operadora, há um divisor equivalente e um banco de Modems ADSL que recebem e processam os dados de cada cliente enviando-os ao provedor (ISP) de *internet* (mecanismo DSLAM).

2.4.4.2 Troncos e multiplexação

Quando tratamos do modelo de sistema de telefonia, abordamos a hierarquia de troncos de conexão (conjunto concentrado de linhas de transmissão, ligando comutadoras). No capítulo de introdução (unidade 1), falamos da multiplexação de mensagens nas linhas como forma de compartilhamento destas para diferentes usuários. A economia em escala exerce um importante papel na telefonia, pois os custos de instalação dos cabos tem um impacto maior do que o tipo de cabo instalado (par trançado ou fibra). Em consequência, procurando aperfeiçoar o uso dos segmentos de meio lançados, foram desenvolvidos basicamente as seguintes técnicas de multiplexação (alocações múltiplas) dos segmentos:

1. Multiplexação pela divisão da banda em frequências (FDM – Frequency Division Multiplexing): como já apresentado na introdução, a banda de frequências é dividida em um conjunto de subcanais, cada um alocado a uma fonte de maneira análoga a radiodifusão, onde cada estação transmite em uma frequência diferente (exemplo: banda de FM de 70 a 110MHz).

Uma forma semelhante de divisão de frequências, no caso das fibras ópticas (ou transmissão por meio de luz) é o WDM – Wave Lenght Multiplexing ou transmissão pela divisão de comprimentos de onda (λ). Cada cor corresponde uma frequência que tem um comprimento λ correspondente. Na transmissão, um misturador combina as diferentes cores (e λ) e as transmite juntas pela fibra compartilhada. No outro extremo, um conjunto de filtros separadores de cores deixa passar cada comprimento para uma fibra de saída.

2. Multiplexação pela divisão do tempo (TDM – Time Division Multiplexing): como já vimos na introdução, um meio de banda estreita (com apenas um canal) pode ser multiplexado pela divisão de tempo em pequenos intervalos (*slots*) atribuídos a cada conexão e passando por aquele meio de modo circular, isto é, após todas as fontes transmitirem um quadro, o processo se repete.

Cabos telefônicos transmitem voz analógica, usando alguma das técnicas já mencionadas de modulação. Já vimos que os Modems, por exemplo, transmitem *bits* modulando nestes canais. O compartilhamento de um segmento de voz em diferentes fontes é possível pela digitalização da voz em conjuntos de 8bits por meio de um método de modulação por codificação de pulsos (PCM – Pulse Code Modulation) no qual um dispositivo chamado CODEC cria segmentos com 8000 amostras de 8bits por segundo (125μ/amostra) apropriados para um canal telefônico de 4KHz.

Utilizando canais de voz agrupados em conjuntos, temos *links* multiplexados

amostrados por PCM. Por exemplo, um canal T1 agrupa 24 canais de voz amostrados por PCM. Assim, a cada 125μs 24bytes de 8bits são transmitidos, resultando uma taxa de dados de 1544Mbps.

Outros canais existem em taxas distintas (exemplo: SONET e SDH, em taxas que variam de 51,84Mbps até 995328Gbps, usando cabos metálicos ou fibras).

2.4.5 Sistema de telefonia móvel

A necessidade de comunicação em trânsito trouxe o desenvolvimento de sistemas de comunicação móveis e sem fio. A telefonia móvel teve início aproximadamente em 1946, com sistemas de telefonia para automóveis nos EUA.

- Sistemas sem fio (celulares):
- 4 gerações:
  - First-generation:
    Voz analógica (push-to-talk/IMTS/AMPS);
    Células contíguas -> Handoff;
    MTSO/MSC -> Canais;
  - Second-generation:
    Voz digital (D_AMPS/GSM/CDMA/PDC);
  - Third-generation:
    Voz digital e dados;
    WCDMA/GPRS/EDGE;
  - Fourth-generation:
    Dados e voz dobre dados;
    LTE/Wimax.

Figura 13. O sistema de telefonia móvel.

Os telefones móveis passaram por 4 gerações distintas:

1ª geração: voz analógica.

Iniciada pelo sistema de acionamento de um botão para liberar a direção da conversa (push-to-talk) e seguida pelo sistema IMTS (Improved Mobile Telephone System) que usava duas frequências bidirecionais. Em 1982, a Bell Systems lançou o sistema AMPS (Advanced Mobile Phone System) que reutilizava

frequências e definia áreas de alcance curtas chamadas células para ampliar a capacidade de chamadas simultâneas. Foi o início dos sistemas celulares.

2ª geração: voz digital.

O sistema AMPS evolui para o D-AMPS (Digital AMPS) e outros sistemas aparecem no mercado (GSM – Global System for Mobile, CDMA – Code Division Multiple Access e PDC ou D-AMPS japonês). Utilizavam a banda de 1900MHz e basicamente ampliaram a capacidade de comunicação celular por meios digitais.

3ª geração: voz e dados digitais.

Convergindo as indústrias de telefonia, entretenimento e informática, esta geração agrega serviços de dados digitais e voz digital em dispositivos (telefones) com arquitetura muito mais próxima de um computador e com muito mais capacidade. GPS, acelerômetros e tela sensível ao toque foram apenas algumas das tecnologias atualmente incorporadas. Aplicações como jogos multiusuários, imagens, fotos e vídeos são possíveis nessa geração e integram os telefones.

A ideia é que a nova geração de telefones (os smartphones) integre todas as funções de acesso à *internet*, tais como e-mail, google, youtube, redes sociais (tweeter, linkedin, facebook etc.), rádio e TV digitais, além, é claro, de permitir as funções de telefonia.

4ª geração: dados e voz sobre IP.

A quarta geração utiliza um dos padrões desenvolvidos até então para esta finalidade: Wimax e LTE. O segundo vem conquistando a preferência de fabricantes, em detrimento do Wimax que tende a cair em desuso.

A principal característica da quarta geração é que não existe mais a separação entre dados e voz. Conceitualmente, todas as chamadas são de dados, transportando a voz digitalizada.

2.4.6 *Internet* via transmissão por TV a cabo

O mercado de acesso à rede é bastante amplo e atraente, a ponto das operadoras de TV a cabo se interessarem em participar dele.

Iniciada na década de 1940, os sistemas de TV a cabo começaram com o modelo CATV (Communit Antenna Television) onde uma antena recebia sinais de emissoras e os retransmitiam localmente aos clientes. Este é o sistema mais comum até hoje.

Com a evolução das fibras ópticas, esse sistema foi evoluído para o HFC

(Hybrid Fiber Coax) que estende o serviço CATV usando fibras no *backbone* principal e cabos coaxiais nas residências.

A divisão de frequências para as estações de TV permite que centenas de canais sejam transmitidos na mesma fibra, porém, para prover acesso à *internet*, é necessário que os clientes também possam usar a banda para receber e/ou transmitir dados.

A divisão então é feita de forma análoga à ADSL, onde a banda passante do sistema é dividida em canais de dados *upstream*, FM, TV e dados *downstream*.

Para transmissão nas redes a cabo, um dispositivo capaz de sinalizar nos canais *up* e *downstream* chamado Modem a cabo é utilizado, respeitando um padrão de comunicação chamado DOCSYS (Data Over Cable Service Interface Specification), oferecendo uma interface Ethernet ou USB.

No lado da rede a cabo, em linhas muito gerais, o Modem se conecta com o dispositivo final da rede (Head End) enviando sua identificação e recebendo os *slots* de frequência *up* e *downstream* para então iniciar suas comunicações.

Existem, também, as redes FTTH que entregam conexões de fibra óptica para cada cliente, dispensando o uso de cabos coaxiais. Nesse caso, é instalado um equipamento onde chega a fibra e saem cabo telefônico, cabo UTP e cabo de som/vídeo.

2.4.7 Resumo

A camada física trata então dos aspectos de conexão física entre os elementos da rede, isto é, da sinalização de bits entre dois elementos conectados por algum segmento de meio físico. Define padrões para conexão (interfaceamento) e codificação dos bits (sinalização, tempo de duração do sinal de 1bit etc. Trata a questão do compartilhamento do meio pelos diversos canais (multiplexação e comutação) nas diferentes tecnologias.

- Diz respeito às interfaces de acesso aos meios físicos e aos sistemas de sinalização de dados digitais (bits);
- Frequência e largura de banda são importantes e dependem de características do meio;
- Diversas tecnologias em meios guiados e abertos;
- Conexões ponto a ponto e multiponto ou difusão.

Figura 14. Resumo da camada física.

Aspectos como largura de banda (banda estreita: 1 canal e banda larga: múltiplos canais) e frequência de operação, bem como características físicas e químicas dos meios (material, comprimento, espessura etc.) são considerados e padronizados.

Classifica os tipos de meios físicos como guiados e abertos e define as várias formas de sua utilização tanto para conexão ponto a ponto (entre pares) quanto para conexão multiponto (em grupos).

2.5 A camada de enlace (*link*) lógica

No nível 2 da pilha de protocolos encontramos a primeira camada lógica: a camada de enlace. Nesta camada iniciamos os primeiros controles do que é transmitido entre dois elementos vizinhos, isto é, interconectados por algum segmento de meio físico.

- Introdução;
- Detecção e correção de erros de transmissão;
- Controle de acesso ao meio: a subcamada MAC;
- Endereçamento físico de estações;
- Protocolos de enlace;
- Redes sem fio;
- Dispositivos de interconexão de LAN;
- Virtualização de enlaces;
- Padronização.

Figura 15. A camada de enlace: projeto, protocolos e serviços.

Tratamos de definir, também, nesta camada, o primeiro protocolo considerado nos elementos fonte e destino, estabelecendo aspectos de formato dos dados e seu significado (são transmitidos quadros e não mais puras sequências de bits), detecção e correção de erros de transmissão, interfaceamento do serviço (definição do ponto de acesso ao serviço de enlace, suas primitivas e parâmetros), mecanismos de disciplina (protocolos) no acesso ao meio em cada tipo de rede e tipos de enlace possíveis.

- Motivação e questões de projeto:
  - Necessidade de interface bem definida;
  - Serviço de troca de dados com vizinhos (conectados por um segmento de meio físico);
  - Controle de erro e de fluxo.
- Serviços oferecidos pela camada de enlace de dados:
  - Datagrama não confiável (sem conexão e sem confirmação);
  - Datagrama com confirmação (sem conexão);
  - Serviço orientado a conexão.
- Formas de enquadramento:
  - Orientada a caractere;
  - Orientada a bit.

Figura 16. A camada de enlace: introdução.

A interconexão de dois elementos vizinhos, ou enlace, é entendida aqui como duas máquinas interligadas por um canal de comunicação que pode ser representado conceitualmente por um fio, isto é, um par trançado, um cabo coaxial, uma fibra ou um *link* ponto a ponto de rádio. O que torna o canal conceitualmente um fio é o fato de que, por meio dele, os bits são entregues na mesma ordem com que são enviados. Entretanto, embora pareça simples, isto não é trivial, na medida em que erros ocasionais de comunicação ocorrem nos circuitos de transmissão e, além disso, existem aspectos limitantes como o tempo de propagação do sinal no meio e taxa finita de transferência dos bits, acarretam uma série de problemas e influem na eficiência desse processo.

Dentre as funções executadas na camada de enlace, pelos seus protocolos, podemos citar:

a) Fornecimento de uma interface bem definida de acesso aos serviços de enlace, à camada de rede;

b) Administrar os possíveis erros de transmissão;

c) Regular os processos de envio e recepção de tal modo que o fluxo de dados gerados pelo emissor não sature um receptor mais lento, por exemplo.

Como meio de estruturar a troca de dados, a camada de enlace estabelece que pacotes de dados da camada de rede estejam encapsulados e estruturados no formato de quadros que contêm um cabeçalho (*header*) de controle do envio, um campo de carga útil (ou o pacote da camada de rede) e um campo

final (*trailer*) de controle dos dados. O gerenciamento do envio de quadros constitui a atividade principal da camada de enlace.

Uma vez montados os quadros, são enviados ao receptor pela interface da camada física (exemplo: To-physical_layer(end, q)) que tratará de enviá-lo pelo canal, bit após bit.

A camada de enlace pode transferir os quadros de diversas maneiras, o que caracteriza os tipos de serviços oferecidos por ela à camada de rede, os quais podem ser:

a) Serviço sem conexão e sem confirmação: é o mais simples, significando que o enlace não efetua nenhuma ação prévia para o envio (sincronização entre emissor e receptor, negociação de condições para a troca etc.). O envio é simplesmente feito e cabe à camada de rede estar preparada no receptor para receber o quadro enviado. Também não há confirmação do receptor do recebimento correto dos quadros enviados.

b) Serviço sem conexão e com confirmação: neste caso, os quadros recebidos são confirmados ao emissor, positiva (*acknowledged*), quando recebido corretamente, ou negativamente (*not acknowledged*), quando possui algum erro.

c) Serviço orientado a conexão e com confirmação: ocorre uma sincronização inicial entre o emissor e o receptor, com negociação prévia das condições para troca dos quadros, os quais são confirmados quando recebidos. Os quadros são numerados e a ordem sequencial de envio é garantida. No caso de erro de transferência, o quadro confirmado negativamente é retransmitido. Mecanismos de temporização (*time-out*) são utilizados para garantir que a confirmação, que ocorre por meio de um quadro de ACK ou NotACK, ou mesmo a ausência dela, permita ao emissor retransmitir quadros recebidos com erros ou não recebidos, garantindo, assim, seu sequenciamento, oferecendo, desta forma, um fluxo confiável.

   1) Cabe notar que, por ser um controle entre o emissor e o receptor, independente do meio físico (ou do canal) utilizado, as mesmas técnicas usadas no enlace são usufruídas na camada de transporte, como iremos ver quando estudando aquela camada, pois lá o controle também é fim a fim, independente da rede subjacente.

   2) Mecanismos de enquadramento: a camada física, conforme já foi apresentado, tem a função de transferir sequências de bits pelo canal, ativando as interfaces de sinalização, sem nenhum controle de erros, de sequência ou de recepção. O fluxo de bits recebido no destino pode, portanto, conter eventuais erros e a verificação destes erros fica a cargo do enlace. A maneira encontrada para melhor gerenciar a transferência dos bits foi agrupá-los em *buffers* finitos chamados

quadros com um campo de verificação (*check-sum* ou CRC – Código de Redundância Cíclica) que permite checar a ocorrência de alguns tipos de erros e corrigi-los de alguma maneira.

Dentre as várias alternativas de enquadramento, foram propostas: inserir um intervalo de tempo entre cada quadro, como delimitador; inserir contadores de caracteres (bytes) do quadro; inserir bytes especiais (flag) de sinalização de início e fim, com inserção de caracteres (scapes) no quadro para garantir a não ocorrência de um flag dentro deste; inserir caracteres especiais (flags) com sequência específica (padrão) de bits (01111110), como delimitadores de início e fim de quadro, com inserção de bit 0, quando ocorrem sequências de mesmo padrão do flag no meio do quadro (note que agora a inserção é de somente um bit); ou por violações na codificação do sinal da camada física.

Não vamos discutir aqui cada uma delas, mas nas referências existe uma fonte rica de detalhes sobre o assunto.

O formato padrão de quadro de enlace utiliza flags tipo 01111110 para delimitação e inserção de bit 0. Um campo de endereço permite identificar a origem e o destino, pois pode haver mais de um, no caso de meio de difusão, ou mesmo ponto a ponto, com diversas linhas em um concentrador de conexões. Um campo de controle, para sequenciamento e identificação do tipo de quadro, permite gerenciar o fluxo trocado. Um campo de dados (ou carga útil) que leva o pacote da camada de redes (ou um fragmento dele, como discutiremos mais tarde) e um campo de verificação (CRC) que confirma todos os bits do quadro, exceto os flags.

Formato geral de um quadro (frame):

flag	endereço	controle	dados	CRC	flag	
1	1 ou 2	1 ou 2	> 0	1 ou 2	1	bytes

- Flag (01111110): delimita início e fim do quadro;
- Endereço: identifica fonte e destino;
- Controle: identifica os tipos de quadros trocados, gerencia a troca de dados e controla erros e fluxo;
- Dados: carga útil transportada (da camada de rede);
- CRC: *check-sum* dos dados para detecção de erros de transmissão (código de redundância cíclica).

Figura 17. Enquadramento.

Dentre os controles do enlace, como o meio é passível de erros, há a necessidade de controlar erros e o próprio fluxo. Esses podem ser corrigidos por duas estratégias distintas:

1. Detecção de erros e retransmissão: consiste em verificar a ocorrência de erro por meio do CRC e confirmar negativamente o pacote, no caso de incorreção, para que seja retransmitido o quadro. Isso funciona bem em linhas com baixa taxa de erros. Neste caso, como a correção é mais custosa que a retransmissão, considerando a ocorrência eventual, é mais eficiente confirmar negativo e retransmitir;
2. Detecção de erros e correção: consiste em verificar a ocorrência de erro por meio do CRC e corrigi-lo. Neste caso, é preciso aplicar algum método de codificação dos dados que permita efetuar sua correção. Esta técnica é aplicada em meios ruidosos (exemplo: redes em meio aberto), onde a simples retransmissão não garante o sucesso.

O tratamento de erros demanda uma compreensão exata do que seja um. No livro do Tanenbaum (2003), há uma explicação detalhada deste procedimento que resumimos aqui: num quadro de, por exemplo, *m* bits de dados são acrescentados mais *r* bits de redundância (ou verificação), totalizando *n* bits (*n* = *m* + *r*) e formando uma palavra de código (*codeword*) *n* bits longa. Dadas duas palavras de código, podemos determinar em quantos e quais bits elas diferem simplesmente aplicando uma operação OR exclusiva e contar quantos bits 1 resultam dela. (exemplo, sejam 11001110 e 11001001 as duas palavras). Pela operação OR exclusivo teremos como resultado 00000111, indicando haver 3 diferenças, nos três últimos bits). Este número de posições em que duas palavras de mesmo comprimento diferem é chamado de Distância de Hamming e indica o número de bits a serem corrigidos para igualá-las. Um exemplo de código de correção é uso de bit de paridade: um bit de paridade é acrescentado à palavra de código de modo que o número de bits 1 da palavra seja zero (paridade par) ou um (paridade ímpar). Assim, no exemplo, teremos para 11001110 de acrescentar um bit 1 formando 110011101 com seis bits 1, portanto, com paridade par. Se na recepção houver paridade diferente, significa que houve um erro pela inversão de um bit durante a transmissão. Este bit de paridade tem distância de Hamming igual a 2, pois qualquer inversão de 1 bit traça a paridade, permitindo detectar erros isolados.

Nas transmissões ocorrem, geralmente, erros de rajadas atingindo mais de um bit adjacente, assim outros métodos, como paridade cruzada, em blocos, de Hamming etc., são métodos difundidos na literatura sobre detecção e correção de erros.

O método mais difundido acabou sendo o método Polinomial, ou do Código de Redundância Cíclica (CRC), onde a palavra de código é vista como coeficiente binário de um polinômio no qual, para k bits, teríamos um polinômio de grau k-1, isto é, com k termos iniciando em x^{k-1} até x^0 (exemplo: 11001110 equivale a $x^7+x^6+x^3+x^2+x$).

- Distância de Hamming (1950):
  - Número em posições de bits que duas palavras de código se diferem entre si;
  - Define as propriedades de um método de detecção e/ou correção de erros de um código.
- Detecção e correção de erros:
  - Em meios com alta taxa de erros é melhor tentar corrigir;
  - Em meios com baixa taxa é melhor retransmitir;
  - Códigos de Hamming permitem corrigir erros simples.
- Tipos de métodos de detecção:
  - Bits de paridade;
  - Código de Redundância Cíclica ou Polinomial (CRC):
    - Utiliza o total de verificação de r bits adicionais ao código (*check-sum*);
    - Utiliza um polinômio gerador (G(x)) que divide o polinômio gerado pelo código mais os r bits do *check-sum*;
    - O campo de *check-sum* é verificado na recepção e identifica erros nos bits recebidos.

Figura 18. A camada de enlace: técnicas de detecção e correção de erros.

Tanto o emissor quanto o receptor utilizam um mesmo polinômio chamado gerador (G(x)) com ambos, o primeiro (de mais alta ordem) e último, bits iguais a 1. O total de verificação (ou *check-sum*) do polinômio gerado pela palavra de código (M(x)), com *m* bits, é calculado acrescentando-se, ao final da palavra, *r* bits, tais que o polinômio obtido, acrescentando os *r* bits, seja divisível por G(x). Desta forma, ao receber o quadro (T(x)), com $n = m + r$ bits, a divisão por G(x) deve resultar nula, caso contrário houve erro por inversão de bits. A obtenção de um polinômio divisível por G(x) é simples se considerarmos que podemos subtrair o resto da divisão binária de T(x)/G(x) de T(x). Um algoritmo para este procedimento é:

1. Seja *r* o grau e G(x). Acrescente *r* bits a M(x) como bits de mais baixa ordem, obtendo $x^rM(x)$;
2. Divida a *string* binária $x^rM(x)$ por G(x) usando divisão binária;

3. Subtraia de $x^r M(x)$ o resto da divisão (com *r* ou menos bits) obtendo T(x), a *string* a ser transmitida.

Com esta técnica é possível mostrar que erros de rajada de até *r* bits são detectados e, para estes tipos de erros de rajada de *r + 1* bits, a probabilidade de não detecção é $1/2^r$, assumindo que todos os padrões de bits sejam igualmente prováveis. Assim, como resultado da padronização, o IEEE 802 definiu o polinômio $G(x) = x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x^1 + 1$ como padrão para protocolos de LAN. Ele tem a propriedade de detectar todas as rajadas de até 32 bits e todas as rajadas com um número ímpar de bits.

2.5.1 Verificação de protocolos

A programação de protocolos é tarefa bastante complexa. A garantia de funcionamento correto é tema de diversas pesquisas e propostas de modelos formais de especificação e ferramentas de verificação.

Dois modelos são destacados aqui, conforme proposto em Tanenbaum (2003), porém existem inúmeras outras alternativas. São as máquinas de estados finitos e as redes de Petri.

2.5.1.1 Máquinas de estados finitos:

- É representada por uma quádrupla (S, M, I, T) onde:
- S = conjunto finito de estados que os processos (emissor ou receptor) e o canal podem estar;
- M = conjunto de quadros trocados;
- I = conjunto de estados iniciais dos processos;
- T = conjunto de transições entre estados.

Uma MEF de um protocolo bastante simples (protocolo 3) é o *stop-and-wait*. Este protocolo se caracteriza por alternar a identificação das mensagens por um bit 0 ou 1 enviado de volta na confirmação, de modo que, se ela for corrompida ou perdida, o emissor pode retransmiti-la e recuperar o erro. No canal existem 3 estados apenas: bit 0 sendo enviado, bit 1 sendo enviado ou Ack sendo enviado. R é o receptor e S (*sender*) o emissor. A Ack é a confirmação e 0 ou 1 o quadro (bit alternante) transmitido.

Em geral, os estados são escolhidos com os instantes em que a máquina de protocolos está esperando (*wait*) pela ocorrência do evento seguinte. Um

estado inicial indica a situação quando inicia uma corrida (0, 0, 0). Transições definem as mudanças possíveis de estado. Cada estado é representado por 3 caracteres SRC, onde S é 0 ou 1, dependendo do quadro que enviar, R também é 0 ou 1, dependendo do que espera receber e C é 0, 1, A ou -- (vazio), dependendo do quadro e sendo transmitido pelo canal.

Máquinas de estados finitos podem ter o problema de impasse (*DeadLock*) que impede a progressão do funcionamento do protocolo. Evitar este problema requer uma modelagem adequada.

2.5.1.2 Modelos de redes de Petri:

Redes de Petri se caracterizam por um modelo de estados, onde é possível observar-se a dinâmica do sistema sendo modelado por meio de sequências de disparos das transições entre eles. Uma rede de Petri é um grafo composto por lugares (nodos representativos de um estado do sistema que são modelados e representados por círculos) e transições (representados por uma barra). Arcos direcionados partem de lugares de entrada (estado de origem) para transições e destas para lugares de saída (estado de destino após esta transição ser disparada). Uma transição tem zero ou mais arcos de entrada e zero ou mais arcos de saída. A mudança entre estados ocorre por meio do disparo de uma transição ativa, o que ocorre quando em cada lugar(es) de entrada (estado atual) existe pelo menos um *token* (marca ou ficha que são indicados como bolas pretas ou coloridas dependendo da rede) que é removido a cada disparo, sendo colocado um em cada lugar de saída. Não há conservação do número de *tokens* retirados. Se duas transições estiverem ativas, qualquer uma delas poderá ser disparada. A escolha de quem dispara é aleatória, neste caso, favorece a representação da dinâmica dos protocolos. A sequência de disparos é representada por um mecanismo de marcações da rede que registra a situação de cada lugar a cada disparo.

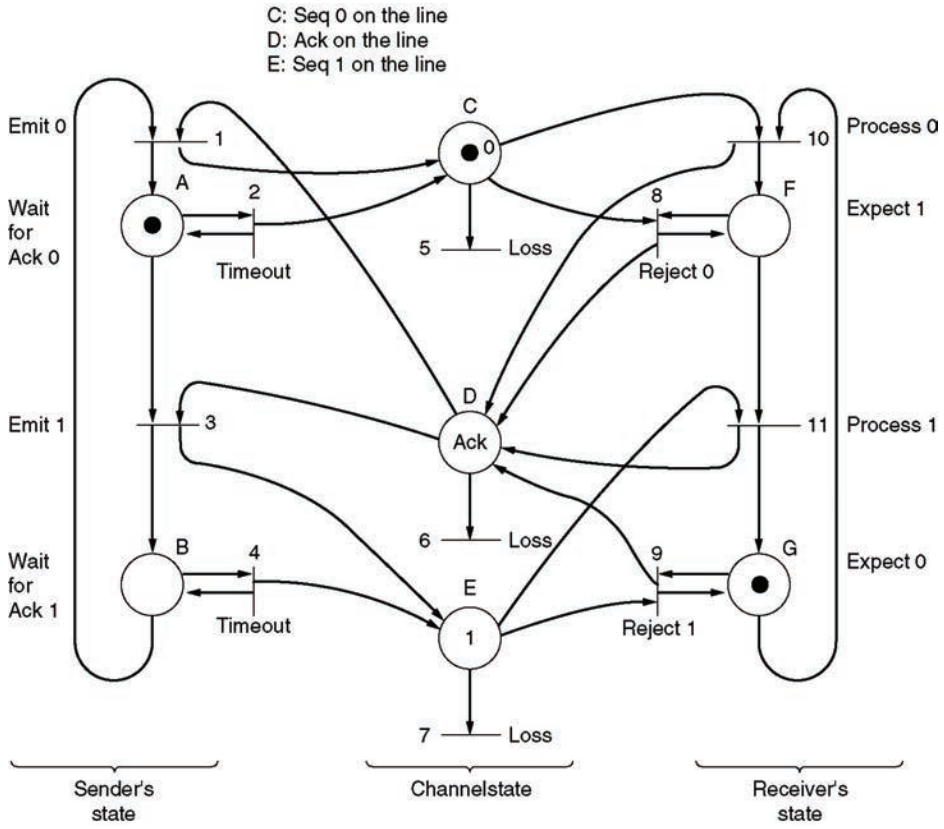


Figura 19. Uma rede de Petri para um protocolo *stop-and-wait*.

2.5.2 Exemplos de protocolos de enlace

O livro de Tanenbaum (2003) apresenta uma implementação para seis protocolos de enlace, variando desde um mais simples (protocolo 1), que considera um canal unidirecional (simplex), livre de erros e com disponibilidade infinita de *buffers* para recepção e incluindo mecanismos de controle, por janelas deslizantes, sobre os pacotes a serem transferidos até um protocolo tipo GO--Back-N (protocolo 5) de retransmissão da janela pendente e um protocolo com retransmissão seletiva de quadros (protocolo 6). Essas implementações são interessantes, pois permitem discutir a implementação de um protocolo de enlace. Dois protocolos de enlace bastante significativos: o HDLC – High Level Data Link Protocol e o PPP – Point–to-Point Protocol são também apresentados, pois o primeiro deles foi utilizado por muito tempo em diversas redes. Já o segundo é o atualmente usado para acesso à *internet*, para computadores domésticos.

- HDLC: High-level Data Link Control:
  - Família de protocolos (SDLC, ADCCP, HDLC, LABP);
  - Orientado a bit;
  - Full duplex;
  - Janela e Piggy-Backing (confirmação e carona).
- The Data Link Layer in the *internet*:
  - Protocolo PPP (Point-to-Point Protocol) RFC1661;
  - Implementação baseada no HDLC para datagramas;
  - 3 recursos de serviço;
  - Padrão atual para *internet*.

Figura 20. Exemplos de protocolos de enlace.

O HDLC identifica uma família de protocolos orientados a bit e usa a técnica de inserção de bit, derivados de um protocolo proposto pela IBM, o SDLC – Synchronous DataLink Control, para comunicação com computadores de grande porte. Submetido para padronização à ISO e ANSI, ele recebeu algumas adaptações e ganhou o nome de ADCCP – Advancedd Data Communication Control Procedure pela ANSI, e HDLC pela ISO. O CCITT ainda modificou o HDLC para uso em redes X.25 (padrão de redes com protocolo de comutação de pacotes, usando datagramas sobre canais telefônicos, que implementa as três primeiras camadas). Ele recebeu então o nome LAP – Link Access Procedure, para enlace nessas redes X.25 e, mais tarde, ainda de LAPB.

Protocolos orientados a bit utilizam a estrutura de quadros, apresentada anteriormente, com flags delimitadores de início e fim. O campo de endereço é usado para identificar diferentes linhas (ou terminais) conectadas ou então para diferenciar comando de resposta. O campo de controle é usado para sequenciação dos quadros trocados, confirmações e outras finalidades de controle. O campo dados pode conter uma informação de qualquer tamanho, o que impacta diretamente nos totais de verificação e na probabilidade de erros em rajadas. O campo total de verificação é uma variação do CRC. Um quadro mínimo tem 32bits, excluídos os flags. Quando a linha está ativa, porém ociosa (nada sendo transmitido), pares de flags são enviados continuamente para garantir a atividade.

Três tipos de quadros (de informação, supervisor e os não numerados) são possíveis. O conteúdo do campo de controle de cada tipo de quadro está descrito na figura abaixo.

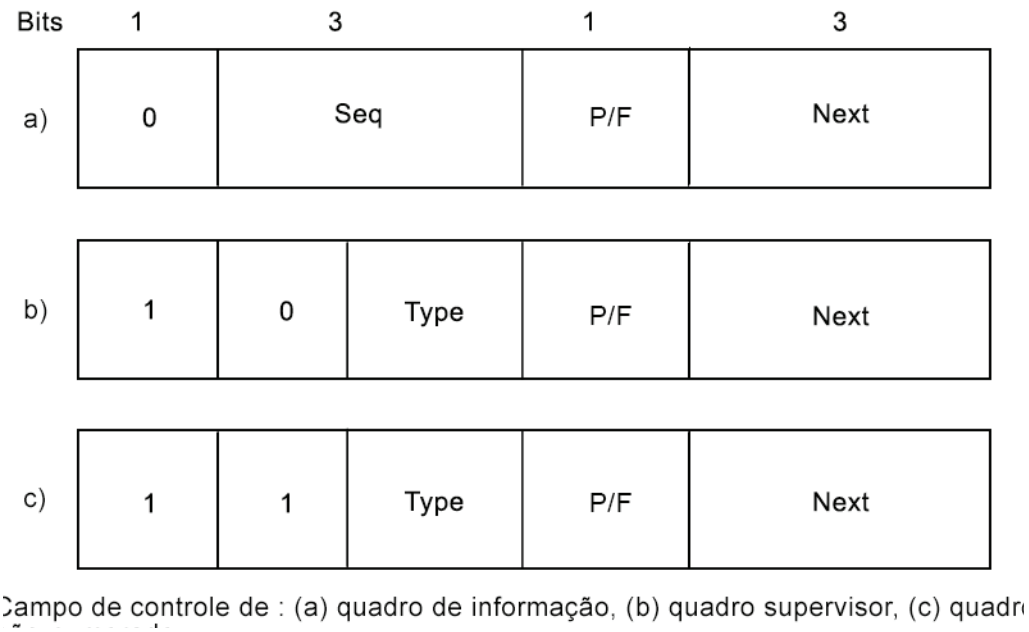


Figura 21. Protoloco de enlace.

Nos quadros de informação, o primeiro bit (valor zero) identifica o tipo, 3bits (sequência), indica o número de sequência do quadro, um bit de P/F (Poll/Final) e permite interrogar o estado do receptor (um quadro com P/F = 1 pede respostas com P/F = 1 até o último quadro de resposta que terá P/F = 0). Também serve para solicitar envio imediato de quadro supervisor pelo destino, ao invés de aguardar o tráfego reverso para receber os Akcs (Piggy-Backing ou confirmação por carona). O campo *Next* traz (de carona) a confirmação do último quadro enviado, indicando o próximo quadro guardado dentro da janela de transmissão.

Os diversos tipos de quadro supervisor são identificados pelo campo tipo: Tipo = 0, identifica um quadro de Ack (chamado *RECEIVE READY*) usado para indicar o próximo quadro esperado. Utilizado quando não há tráfego no sentido reverso para portar os acks.

- Tipo = 1, indica um NAck (confirmação negativa). Indica erro na transmissão e solicita ao emissor retransmitir todos os quadros pendentes a partir desse mesmo quadro (janela – protocolo 5).
- Tipo = 2, *RECEIVE NOT READY* confirma todos os quadros já recebidos (menos o indicado em próximo) e solicita suspensão no envio reverso até receber um receive ready. É uma forma de contornar problemas eventuais no receptor (como falta de *buffers* de armazenamento de quadros, por exemplo).
- Tipo = 3, *SECTIVE REJECT* solicita a retransmissão do quadro indicado, apenas, e não da janela pendente (protocolo 6), para reposição de um quadro com erro.

A terceira classe é a de quadros não numerados, usada tanto para controle da conexão quanto para troca de dados em uma rede não confiável. Possui 5bits (32 possibilidades), porém implementa apenas alguns comandos: DISC – Disconnect, para indicar a intenção de desconexão (lógica) de uma máquina; SNRM – Set Normal Responde Mode, anuncia que uma estação está se conectando (logicamente) na rede, porém em modo mestre-escravo, isto é, um irá comandar e outro responder. SABM – Set Asynchronous Balance Mode, reestabelece a conexão, porém com ambos os extremos em modo equivalente (ambos podem iniciar o enlace); FRMR – Frame Reject, para rejeitar um quadro enviado, informando o tipo de erro ocorrido no campo de dados; UA – UnNumbered Acknowledgement, para confirmar um quadro recebido e UI – UnNumbered Information, para informações arbitrárias de controle. Apenas os dados dos pacotes de informação são passados à camada de rede.

2.5.2.1 Protocolo PPP – a camada de enlace na *internet*

A conexão de computadores na *internet* ocorre de duas formas distintas: por meio de LANs, conectadas via roteadores à rede do provedor, ou por meio de linhas ponto a ponto, individuais, geralmente utilizando linhas privativas por alguma operadora de telecomunicações. Em ambos os casos existe uma linha conectando roteadores, ou um computador, a um roteador por meio de um Modem, como na figura abaixo.

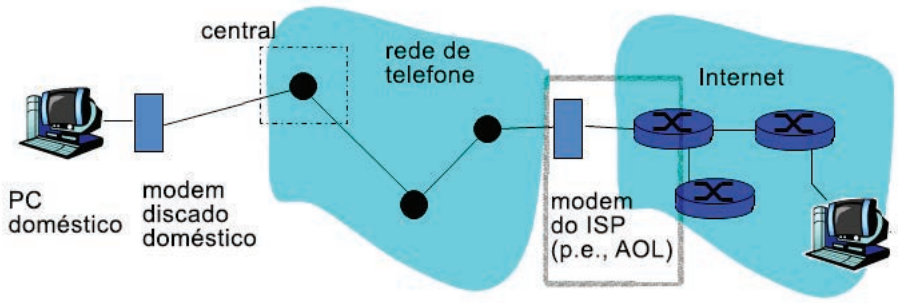


Figura 22. Roteadores conectados a um Modem.

O protocolo PPP, definido pela RFC 1661, além de outras complementares, trata do estabelecimento do enlace, da detecção de erros e da negociação de endereços IP em tempo de estabelecimento de conexão, além de trocar pacotes de outros protocolos.

O PPP é estruturado em três módulos funcionais:

1. Um método de enquadramento, com delimitação de início e fim de quadro, com detecção de erro;

2. Um protocolo de enlace (LCP – Link Control Protocol) de ativação e desativação de circuitos síncronos e assíncronos de dados, testes e ativação de linhas;
3. Um processo de negociação de opções da camada de rede (NCP – Network Control Protocol), independente do protocolo de rede sendo usado (por exemplo, o protocolo IP).

Estabelecida a conexão física, via Modem pela linha telefônica, por exemplo, entre o computador do usuário e o do provedor de acesso à *internet* (ISP), inicia-se a troca de pacote LCP por meio dos quadros PPP (carga útil). Uma vez estabelecido o enlace, pacotes NCP são trocados, agora, no nível da camada de rede, estabelecendo sua configuração.

A partir deste ponto, o computador do usuário está conectado na rede IP (*internet*) e pode trocar pacotes pelo enlace estabelecido com o ISP.

2.5.3 A sub-camada MAC

A interconexão de redes LAN, diferentemente da conexão ponto a ponto, por linhas discadas ou privativas, demanda uma ação a mais da camada de enlace que é a disciplina de acesso ao meio pelas máquinas que fazem parte da rede local. É o caso típico de empresas ou instituições com redes próprias (corporativas ou de campus) interligadas a *internet* por meio de uma conexão negociada com o provedor de acesso. As diferentes tecnologias de redes LAN definem diferentes disciplinas para controle do acesso de seus computadores ao meio físico compartilhado. No caso das redes ponto a ponto, esse controle não é necessário, pois, via de regra, não há compartilhamento.

A sub-camada MAC – Medium Access Control cuida de definir, para cada topologia de rede LAN, qual a política de controle de acesso. Assim, vamos tratar de analisar algumas questões relativas a essas políticas, mais precisamente de:

- Diferentes tecnologias de LAN;
- Protocolos de acesso múltiplo e a divisão do canal de comunicação para compartilhamento;
- A sub-camada MAC nas diferentes tecnologias.

Vamos apresentar os aspectos principais das tecnologias mais atuais de redes LAN.

- Redes ponto a ponto:
  - ATM;
  - Estrela/hierárquicas;
  - Ópticas;
  - Anel.
- Redes multiponto ou de difusão:
  - Barramento (Ethernet);
  - WLAN;
  - Satélites.

Figura 23. A sub-camada MAC: tecnologias de LAN.

Das diferentes tecnologias de LAN, podemos classificá-las em:

- Redes de conexão ponto a ponto, que possuem conexão por um meio direto entre cada par de elementos da rede. É o caso das redes com topologias hierárquicas ou em estrela, redes ópticas, redes em anel e ATM;
- Redes de conexão multiponto, que possuem um meio compartilhado por um conjunto de nodos, ou redes de difusão, abrangendo a todos os nodos. Tais como as redes Ethernet, WLAN e satélites.

Quando o meio físico é compartilhado, alguma estratégia de compartilhamento deve ser estabelecida, de modo que todos os enlaces que passem por ele possam transmitir seus quadros. É o problema da alocação de canais.

2.5.3.1 A alocação estática do canal

Semelhante ao caso da alocação de canais em um tronco telefônico, a alocação estática pode ser por FDM, divisão em frequências, ou TDM, divisão no tempo.

Mas as divisões estáticas somente funcionam bem se o número de compartilhamentos for pequeno, pois alocados os *slots*, pode haver perda de recursos (*slot* não utilizado) pelo fato do tráfego ser por rajada (em intervalos alternados de pacotes e silêncio).

Da teoria de filas, podemos demonstrar, para o caso da FDM, como o desempenho é fraco:

Supondo: T = atraso médio de transferência, para um meio com capacidade C bps, uma taxa de chegadas de pacotes de λ pacotes/segundo e pacotes

com comprimento médio obtidos de uma função de distribuição exponencial de 1/μ bits/quadro.

Com estes parâmetros e aplicando as expressões da teoria de filas, temos que:

$$T_{FDM} = \frac{1}{\mu\left(\frac{C}{N}\right) - \left(\frac{\lambda}{N}\right)} = \frac{1}{\mu(c - \lambda)} = NT$$

Isso implica afirmar que o atraso médio para transferência é de N vezes o tempo de transferência de uma mensagem. Ou seja, é N vezes pior do que se houvesse uma fila única de transferência. Com a divisão, cada canal, dos N canais que dividem a LB, agora tem capacidade C/N.

O mesmo ocorre com TDM.

2.5.3.2 Alocação dinâmica do canal

Baseia-se em cinco premissas fundamentais:

1. *Premissa do modelo de estação*: supõe haver N estações independentes gerando quadros para transmissão, a uma taxa de λ quadros/segundo, isto é, a probabilidade de um quadro ser gerado num intervalo $\Delta\tau$ é $\lambda\,\Delta t$. Uma vez gerado um quadro, a estação é bloqueada e aguarda até ele ser transmitido;
2. *Premissa de canal único*: há um único canal compartilhado pelas N estações, para transmitir ou receber;
3. *Premissa de colisão*: se dois quadros são transmitidos simultaneamente no canal, irão sobrepor seus sinais e se corromperem mutuamente. Isto é chamado de colisão de sinais que pode ser detectada e os quadros retransmitidos;
4. *Premissa de tempo (contínuo ou discreto)*: a transmissão pode começar a qualquer instante de tempo (contínuo) sem um relógio marcador de tempo, ou então, só ocorre em instantes de tempo marcados como início de um intervalo (*slot*) discreto de tempo;
5. *Premissa de detecção (ou não) de portadora*: as estações têm condição (ou não) de detectar se o canal está sendo usado ou está livre para transmissão. Se ocupado, as estações prontas para transmitir aguardam até que ele fique livre, seguindo alguma estratégia.

Baseado nessas premissas, vários algoritmos foram propostos para compartilhamento do meio pela alocação dinâmica de canais.

Tais protocolos são organizados em diversas categorias, incluindo aí o ALOHA, CSMA, Collision-Free, contenção limitada, WDM e WLAN.

- Alocação estática de canais:
  - TDM (Time Division Multiplexing) e FDM (Frequency Division Multiplexing);
  - Baixo desempenho: o atraso médio para N estações é N vezes pior do que se houvesse uma fila única;
  - Não serve para tráfego em rajadas.
- Alocação dinâmica de canais:
  - Busca otimizar o processo.

Figura 24. O problema da alocação de canais.

Protocolos de acesso múltiplo:

- ALOHA;
- CSMA (Carrier Sense Multiple Access Protocols);
- Colision-Free Protocols;
- Limited-Contention Protocols;
- (WDM) Wavelength Division Multiple Access Protocols;
- MACAW (Wireless LAN Protocols).

Figura 25. Protocolos de acesso múltiplo.

ALOHA

O Primeiro algoritmo é o ALOHA (Abramson, 1970).

Na universidade do Havaí, foi proposto um protocolo de comunicação via rádio entre os pesquisadores nas ilhas e o computador central via duas frequências: f1 das ilhas para o central e f2 do central para as ilhas. Duas formas foram desenvolvidas:

1. ALOHA puro:

Usuários nas ilhas transmitem em f1 sempre que estiverem prontos. Não conseguem ouvir o meio, pois somente escutam f2. Isso implica em possibilidade

de colisões em qualquer um dos bits transmitidos. A certeza da transmissão bem sucedida é via confirmação (ACK) em f2, de seu pacote. Caso tenha colidido (não recebeu o ACK), as estações esperam tempos aleatoriamente diferentes (para não tornarem a colidir) e tentam novamente. Este sistema, pela alta probabilidade de colisões, tem um desempenho muito baixo. Apenas 18% da capacidade do canal são utilizados, em média, com sucesso.

2. SLOTTED ALOHA:

Uma alternativa para duplicar o desempenho reduzindo as colisões foi dividir o tempo em intervalos iguais, de duração de 1 quadro, chamados *slots*, e sinalizar o início de cada transmissão, de tal modo que apenas as estações prontas na sinalização podem tentar enviar. As demais devem aguardar novo *slot*. Isso faz com que as colisões somente ocorram no início de cada *slot*. Desta forma, com o Slotted ALOHA a utilização do canal passou para 37%.

Este algoritmo é usado também em sistemas de transmissão por satélites.

CSMA – Carrier Sense Multiple Access

Com a possibilidade nas LAN de ouvir o meio antes de iniciar a transmissão é possível reduzir ainda mais o número de colisões, dispensando o sinalizador de início de *slots*. Assim, este algoritmo emprega a premissa da detecção da portadora (*carrier sense*) e tem diversas variantes.

CSMA persistente e não persistente

- O primeiro algoritmo proposto é o 1-persistente, isto é, o emissor escuta o meio e, se este estiver livre, inicia a transmissão com probabilidade 1. Caso esteja ocupado, aguarda até que fique livre. O problema com ele é que não prevê que estações poderão colidir (sentindo o meio livre simultaneamente).
- O seguinte é o não persistente. Nele, o emissor escuta o meio e, se estiver livre, inicia sua transmissão, porém, se estiver ocupado, aguarda por um tempo aleatório e torna a tentar. Com isso, dá chance de distribuir melhor no tempo as estações que aguardam pelo canal, melhorando a utilização deste.
- O terceiro é o P-persistente. Foi desenvolvido para canais que operam por *slots* (discretizados ou *slotted channels*) e define probabilidade de envio, funcionando da seguinte maneira: o emissor, quando pronto, escuta o meio. Se este estiver livre, a estação inicia a transmissão com probabilidade *p* ou aguarda o próximo *slot* com *1-p*. Novamente aplica a mesma regra. Se o meio estiver ocupado, espera um tempo aleatório e reinicia o procedimento.
- CSMA/CD – o CSMA com detecção de colisão (collision detection): claramente os CSMA são melhores que os ALOHA, pois não iniciam a

transmissão se o canal estiver ocupado. Porém, se houver uma colisão (e ela acontecerá apenas no tempo de envio do primeiro bit), eles não irão notar e continuarão a transmitir todo o restante do pacote em colisão. A percepção de que houve colisão (CD – Collision Detection) só é possível com a introdução de um mecanismo de "escuta-enquanto--transmite", que compara o bit sendo transmitido e o que está em propagação no meio. É o protocolo base das redes locais Ethernet. Os estados da rede, neste método, se revezam entre transmitindo (ocupando o meio), disputando (em contenção) ou ocioso. Depois de detectada uma colisão, a estação aborta sua transmissão, sinaliza a todos a ocorrência (tempo de mais 1 bit) e inicia sua espera durante um tempo aleatório, deixando o meio livre para ser utilizado por outros emissores. Após sua espera aleatória, ela volta a aplicar o algoritmo do CSMA/CD.

- Colisões interrompem as transmissões correntes imediatamente;
- Mecanismo de "escuta-enquanto-transmite" detecta colisão no tempo do primeiro bit.

Figura 26. CSMA/CD.

Supondo que o tempo de propagação de um bit por todo o meio (cabo) seja τ, uma colisão irá ocorrer se uma segunda estação iniciar sua transmissão num tempo $\tau - \in$, inferior a τ, pois a transmissão iniciada ainda não teria chegado até ela nem ao fim do cabo. Entretanto, a indicação de ocorrência da colisão demoraria os mesmos $\tau - \in$ para chegar à primeira estação, totalizando 2τ, para que toda a rede tome conhecimento. Isso pode ser modelado como Slotted ALOHA com *slots* de comprimento 2τ. Por exemplo, aplicando este modelo num cabo coaxial de 1000m, teríamos $\tau = 5\mu s$, como tempo de envio de 1bit.

Protocolos livres de colisão (collision-free)

Embora uma colisão não mais ocorra no CSMA/CD, após adquirido o canal (em 2τ), ela ainda pode ocorrer neste período de disputa (no início da transmissão), o que afeta o desempenho do sistema em função do comprimento do quadro e da capacidade do meio. Por outro lado, nem todo meio permite o uso de CSMA/CD. Assim, por meio de uma disciplina colocada sobre o acesso, é possível resolver o período de disputa substituindo-o por algum método de reserva. Nenhum é usado na prática atualmente, mas dão origem, por exemplo, ao protocolo de redes sem fio.

O primeiro é o de reserva por mapa de bits (BitMap).

Nele, antes de uma sequência de transmissões onde as N estações das redes estão ativas, há um período de reserva que consiste na propagação da intenção de transmiti-las por meio de um bit de marcação, recebido por todas as demais estações. Findo o período, todas as estações prontas (com quadro) a transmitir fizeram, na ordem, suas marcações. Em seguida, todas transmitem, na ordem marcada, garantindo assim a ocupação do meio sem desperdício de banda.

- Evitam colisão por meio de métodos de disciplina de acesso;
- Antes de transmitir, a estação manifesta sua intenção e reserva o canal;
- As estações alternam períodos de transmissão com períodos de marcação (*slots* de disputa).

Figura 27. Protocolos *colision-free*.

Outros protocolos são o de contagem regressiva binária, o de disputa limitada, o percurso em árvore, o WDM etc.

2.5.3.3 Redes Ethernet

O projeto da rede Ethernet, conforme falado na unidade 1, evoluiu do projeto ALOHA pela possibilidade de sentir o meio físico e de detectar colisões. As redes Ethernet operam com o protocolo CSMA/CD e são padronizadas pelo padrão IEEE802. É uma tecnologia muito econômica, gasta-se menos de R$ 20 para 100Mbps. Acompanhou aumento de velocidade: 10, 100 e 1000Mbps. Utiliza como meio físico o cabo coaxial (fino e grosso, ambos em desuso atualmente), par trançado e fibras ópticas:

- 10base5 – para cabo coaxial grosso (*yelow cable*, padrão AUI) de 500m, 100 nodos/segmento, obsoleto;
- 10base2 – para cabo coaxial fino (padrão de conexão BNC) de 185m, 30 nodos/segmento, sem uso de *hub*;
- 10baseT – para cabo de par trançado (UTP) categoria 5, de 100m com uso de *hub*;
- 10baseF – para cabo de fibra óptica multimodo, de 2000m, permitindo até 1024 estações conectadas, usando *hub*.

A interface do emissor encapsula o datagrama IP (ou outro pacote da camada de rede) em um **frame Ethernet** que contém: preâmbulo, cabeçalho, dados e CRC.

O preâmbulo de 8bytes:

- **7bytes** com o padrão **10101010** seguidos por **um byte** com o padrão **10101011.**
- É usado para sincronizar receptor ao *clock* do remetente.

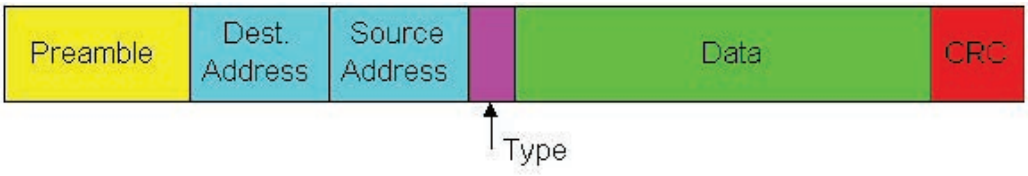


Figura 28. Preâmbulo de 8bytes de um frame Ethernet.

Um frame Ethernet completo DIX (DEC, Intel e Xerox) tem a forma:

802.3 MAC Frame

Preamble	Start-of-Frame-Delimiter	MAC destination	MAC source	Ethertype/Length	Payload (Data and padding)	CRC32	Interframe gap
7 octets of 10101010	1 octet of 10101011	6 octets	6 octets	2 octets	46-1500 octets	4 octets	12 octets
		64-1518 octets					
72-1526 octets							

Figura 29. Frame Ethernet completo.

Padding (preenchimento):

Para evitar problemas e permitir a distinção de quadros válidos, o tamanho do frame, que vai do *destination addres* até o *check-sum*, deve ser maior ou igual a 64 bytes.

Se a parte de dados (*payload*) de um quadro for menor que 45bytes, este campo deve ser preenchido com 0s até o tamanho mínimo. Outra razão para *padding* é evitar que a transmissão do quadro se conclua antes de seu primeiro bit ter atingido o extremo do cabo.

Transmissão em banda básica e codificação Manchester:

As versões da Ethernet utilizam esquema de codificação denominada Manchester, onde o período de sinalização de um bit 1 no meio físico é dividido em dois intervalos iguais, com voltagem alta no primeiro e baixa no segundo. Já o bit 0 é sinalizado de modo inverso. Desta maneira, o receptor facilmente identifica as transmissões e sincroniza-se melhor com o emissor. A desvantagem é a necessidade de consumir o dobro da banda pelos dois períodos.

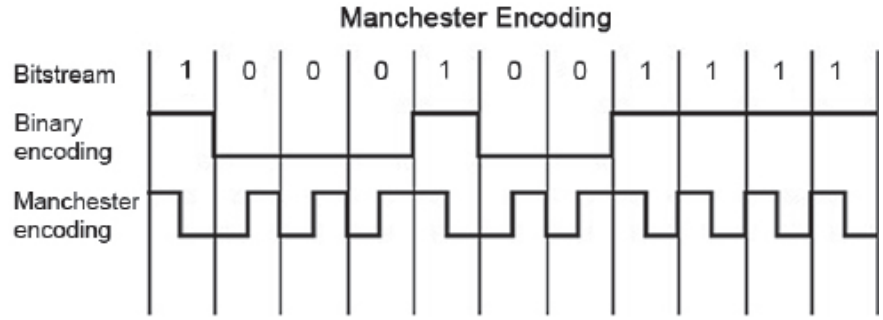


Figura 30. Codificação Manchester.

Uma variante é a codificação Manchester diferencial, que indica o bit 1 sem transição inicial e o bit 0 com transição. Mas não é usado na Ethernet.

Banda básica significa que não se usa modulação de portadora. Os bits são codificados, usando **codificação Manchester** e transmitidos diretamente, modificando a voltagem de sinal de corrente contínua. A codificação Manchester garante que ocorra uma transição de voltagem a cada intervalo de bit, ajudando a sincronização entre relógios do remetente e receptor.

Algoritmo da subcamada MAC Ethernet:

```
A: escuta canal;
SE ocioso ENTÃO {
   transmite e monitora o canal;
   SE detectou outra transmissão  ENTÃO {
      aborta e envia sinal de “jam”;
      atualiza número de colisões;
      retarda de acordo com o algoritmo de retardamento exponencial;
      vai para A
   } SENÃO {
      terminado este quadro;
      zera  número de colisões;
   }
} SENÃO{
   espera o final da transmissão atual e vai para A
}
```

onde:

- Sinal *Jam*:
  - Para garantir que todos os outros transmissores tomem conhecimento da colisão → sinal possui 48bits;
- Retardamento exponencial:

- A meta é adaptar a taxa oferecida por transmissores à estimativa da carga atual, isto é, retardar quando carga da rede estiver elevada;
- Depois da primeira colisão, escolhe *K aleatoriamente* entre *{0,1};*
- O retardo é de *K* x 512 BTT: [1 BTT = tempo para transmitir 1 bit];
- Depois da segunda colisão, escolhe *K* de *{0, 1, 2, 3…};*
- Depois de dez ou mais colisões, escolhe *K* de *{0, 1, 2, 3, 4,…,1023}.*

• Nota-se que neste esquema um novo quadro tem uma chance de sucesso na primeira tentativa, mesmo com tráfego pesado.

• **Eficiência Ethernet** com tráfego pesado e número grande de nós:
- Eficiência tende a ***1*** quando t_{prop} tende a 0;
- Tende a ***1*** quando t_{trans} tende ao infinito;
- Muito melhor do que o ALOHA, ainda é descentralizado, simples e econômico.

Exercício: determinar o rendimento em porcentagem (%) do CSMA/CD em uma situação de alta carga de tráfego na rede.

$$\text{Eficiência} = \frac{1}{1+\left(5 * \frac{t_{prop}}{t_{trans}}\right)}$$

Ethernet 10baseT e 100baseT:

• Taxas de transmissão de 10 e 100Mbps; este último é chamado de *fast ethernet;*

• ***T*** significa par trançado (*twisted pair*);

• Usa concentrador (*hub*) ao qual os nós estão ligados por cabos individuais de 2 pares trançados, mostrando, portanto, uma *topologia em estrela*;

• CSMA/CD implementado no *hub*;

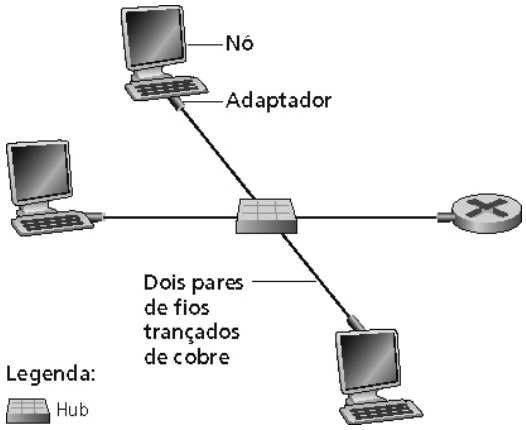


Figura 31. Giga bit Ethernet.

- Usa formato do quadro Ethernet padrão;
- Admite enlaces ponto a ponto e canais de difusão compartilhados;
- Em modo compartilhado, usa-se CSMA/CD. Para ser eficiente, as distâncias entre os nós devem ser curtas (poucos metros);
- Os *hubs* usados são chamados de distribuidores com *buffers* (*buffered distributors*);
- *Full-Duplex* em 1Gbps para enlaces ponto a ponto;
- O uso de enlaces ponto a ponto também foi estendido a 10base-T e 100base-T.

2.5.3.4 Redes locais sem fio:

Introdução

Cada vez mais populares, as LAN sem fio têm sido usadas em diversos ambientes, desde escritórios, hotéis, aeroportos e edifícios públicos. Elas podem operar em modo infraestruturado (por meio de um ponto de acesso) ou não infraestruturado, em configuração *ad-hoc*. O ponto de acesso age como uma ponte entre a rede sem fio e a rede cabeada.

Utilizam o protocolo MACAW (Medium Access with Collion Avoidance Wireless), que é livre de colisões na transmissão, e faz a disputa pelo meio através de um mecanismo de RTS-CTS (Request to Send/Clear to Send). Uma vez confirmado o RTS com um CTS, todas as estações na área de cobertura sabem que uma das estações solicitou e apoderou-se do direito de transmitir.

Redes *wi-fi* – o padão 802.11

As redes *wi-fi* seguem o padrão IEEE802.11, nas formas A, B e G que especifica técnicas de sinalização para a camada física (rádio).

- Infravermelho a 1 e 2Mbps, porém com muita interferência;
- FHSS (Fequency Hopping Spread Spectrum) de 2Mbps, com saltos de frequências em 79 diferentes canais;
- DSSS (Direct Sequence Spread Specrum) 11Mbps, com saltos em uma dada sequência predeterminada de canais, usando sequências de *Barker*, onde cada bit é transmitido como 11 chips (CDMA);
- OFDM (Orthogonal Frequency Division Multiplexing) 54Mbps, em 2.4GHz;
- HR_DSSS (High Rate DSSS) utilizando 11 milhões de chips/s para uma velocidade de 11Mbps.
    - Na camada MAC, utiliza CSMA/CA, em dois modos de operação, DCF – Distribured Coordinating Function, sem controle central e PCF – Point Cordination Function, por meio de uma estação base de rádio (ponto de acesso) que controla as atividades da célula;
    - O CSMA/CA opera no modo do protocolo MACAW, com CTS/RTS.

As redes sem fio, dada a configuração em células, sofrem do problema da estação oculta, isto é, fora do alcance do emissor, mas no alcance do receptor e da estação exposta. Em outras palavras, entre duas estações que não se veem. O mecanismo de CTS/RTS resolve estes problemas.

Serviços oferecidos:

O padrão 802.11 define 9 serviços em duas categorias: 5 de distribuição, fornecido pela estação base e 4 de estação ou intracelular:

- Distribuição:
    1. Associação;
    2. Desassociação;
    3. Reassociação;
    4. Distribuição;
    5. Integração:
        - Intracelular:
        - 1. Autenticação;
        - 2. Desautenticação;
        - 3. Privacidade;
        - 4. Entrega dos dados.

O padrão WIMAX: (IEEE 802.16)

O IEEE 802 não trata apenas de protocolos para redes LAN em suas diferentes tecnologias. Na realidade, outras redes acabaram sendo padronizadas neste

projeto. É o caso das redes de banda larga, para acesso à *internet*. O padrão IEEE 802.16 oferece os resultados dos estudos para redes chamadas WIMAX.

Aprovado em 2002, o padrão oferece uma estrutura de acesso para redes locais, tanto de uso doméstico quanto empresarial de banda larga. Este padrão permite ampliar a possibilidade de conexão, via rádio, de lugares com maiores dificuldades de implementar infraestrutura de acesso via cabos ou serviços telefônicos e de TV a cabo.

As redes WIMAX utilizam diferentes formas de modulação, em função da distância das estações, no sentido de melhor aproveitar a banda disponível e a potência dos transmissores.

As redes *bluetooth*

Apresentada em 1994 pela ERICSON, a proposta de investigar protocolos que permitissem a integração de equipamentos típicos de escritório (impressoras, PDAs, telefones, IPODs etc.) acabou atraindo o interesse de outras empresas com a IBM, a Nokia, a Intel e a Toshiba que formaram um SIG (grupo de interesse especial) para desenvolvimento de uma solução. O projeto foi denominado *bluetooth* em homenagem ao rei Harald Blataand II (o Bluetooth – 940-981, na Dinamarca e Noruega) e propunha protocolo para interconexão próxima de dispositivos sem fio de baixo alcance, baixa potência e baixo custo.

Em 1999, o IEEE 802.15 acabou por padronizar uma versão pouco modificada desta proposta nas camadas físicas e de enlace e ainda trabalha neste processo.

Com um modelo de arquitetura limitado para interligação de pequenos dispositivos, o *bluetooth* é bastante utilizado hoje em inúmeras aplicações de redes PAN.

2.5.4 Comutação na camada de enlace

Dispositivos de interconexão, como os HUBs, PONTES e COMUTADORES (*switches*), são usados para estender as características das redes locais: cobertura geográfica, número de nós, funcionalidade administrativa etc. Diferem entre si em respeito a:

- Isolamento de domínios de colisão;
- Camada em que operam.

Diferentes de roteadores, são *plug and play* e não proveem roteamento ótimo de pacotes IP.

2.5.4.1 Hubs:

Dispositivos da camada **física**, basicamente são repetidores operando ao nível de bit, repetindo os bits recebidos numa interface para as demais interfaces.

Hubs podem ser dispostos numa hierarquia (ou **projeto de múltiplos níveis**), com um *hub backbone* na raiz.

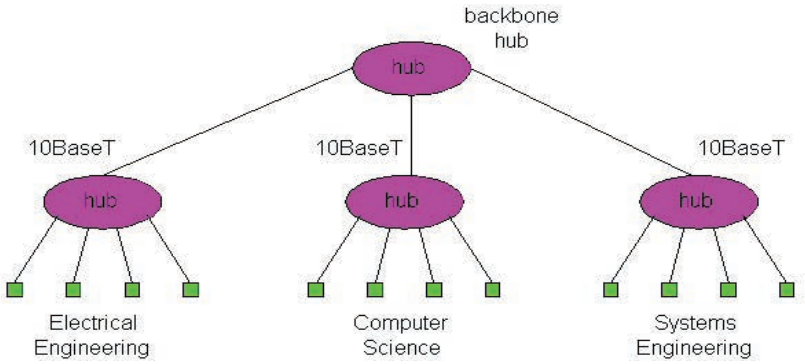


Figura 32. Segmentos de rede local.

Cada rede local ligada é chamada de **segmento** de rede local.

Hubs **não isolam** domínios de colisão. Um nó pode colidir com qualquer outro nó residido em qualquer segmento da rede local.

- Vantagens de *hubs*:
  - Dispositivos simples e de baixo custo;
  - Configuração em múltiplos níveis e provê degradação paulatina: porções da rede local continuam a operar se um dos *hubs* parar de funcionar;
  - Estende a distância máxima entre pares de nós (100m por *hub*).
- Limitações de *hubs*:
  - Domínio de colisão único resulta em nenhum aumento na vazão máxima. A vazão no caso de múltiplos níveis é igual a do segmento único;
  - Restrições em redes locais individuais põem limites no número de nós no mesmo domínio de colisão (portanto, por *hub* ou coleção de *hubs*) e na cobertura geográfica total permitida;
  - Não se pode misturar tipos diferentes de Ethernet (por exemplo, 10baseT e 100baseT).

2.5.5 Pontes ou Bridges

Dispositivos da camada de enlace operam em quadros Ethernet, examinando o cabeçalho do quadro e reencaminhando, seletivamente, um quadro com base no seu endereço de destino.

Ponte **isola domínios de colisão,** pois armazena e reencaminha os quadros.

Quando se quer reencaminhar um quadro num segmento, a ponte usa CSMA/CD para fazer acesso ao segmento e transmitir.

Vantagens de pontes:

- Isola domínios de colisões, o que resulta em aumento de vazão máxima total e não limita nem o número de nós e nem a cobertura geográfica;
- Pode interligar tipos diferentes de Ethernet, pois é um dispositivo "armazena e reencaminha";
- Transparente: não requer nenhuma modificação aos adaptadores dos nós da rede local.

2.5.5.1 Comutadores (*switches*) Ethernet:

Um comutador Ethernet (*Ethernet switch*) é um dispositivo que estende funções normais de ponte para incluir "conexões dedicadas" ponto a ponto.

Uma estação ligada a um comutador, por meio de uma conexão dedicada ponto a ponto, sempre detecta que o meio está ocioso: **não haverá colisões entre duas portas**.

Os comutadores Ethernet proveem de combinações de conexões compartilhadas/dedicadas, a 10, 100 e 1000Mbps.

Alguns *switches* suportam comutação *cut-through*:

- O quadro é reencaminhado imediatamente ao destino, sem esperar a montagem do quadro inteiro no *buffer* do comutador;
- Há uma pequena redução na latência.

Switches Ethernet variam em tamanho:

- Os mais rápidos incorporam uma rede de interconexão (chamada de *backplane*) de alta capacidade.

Interconexão de *switches* com *Hubs*:

Hub de *backbone* interconecta segmentos de LAN;

- Estende a distância máxima entre os nós;
- Mas domínios de colisão individuais tornam-se um único e grande domínio de colisão;
- Não pode interconectar 10baseT e 100baseT;

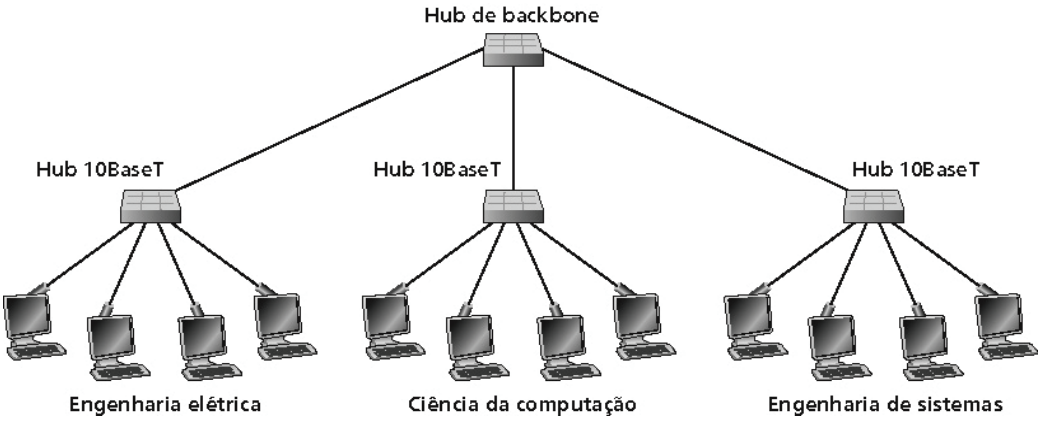


Figura 33. Exemplo de LAN segmentada.

- Dispositivo de camada de enlace;
- Armazena e encaminha quadros Ethernet;
- Examina o cabeçalho do quadro e seletivamente encaminha o quadro **baseado no endereço MAC de destino**;
- Quando um quadro está para ser encaminhado no segmento, usa CSMA/CD para acessar o segmento;
- Transparente;
- Hospedeiros são inconscientes da presença dos *switches*;
- *Plug-and-play* e *self-learning* (autoaprendizado);
- *Switches* não precisam ser configurados.
    - Encaminhamento:
        - Como determinar para qual segmento da LAN encaminhar o quadro?
        - Parece um problema de roteamento.
    - *Self-learning* (autoaprendizado):
        - Um *switch* possui uma tabela de comutação.
        - Entrada na tabela do *switch*:
            - Endereço MAC, interface e marca de tempo;
            - Entradas expiradas na tabela são descartadas.

- (TTL – Time to Live pode ser 60min):
- *Switch* “aprende” quais hospedeiros podem ser alcançados por meio de suas interfaces.
  - Quando recebe um quadro, o *switch* “aprende” a localização do transmissor;
  - Registra o par [transmissor/localização] na tabela.

- Filtragem/encaminhamento:
  - Quando um *switch* recebe um quadro:
  - Indexa a tabela do *switch* usando end. MAC de destino:
    - **If** entrada for encontrada para o destino
    - **then{**
    - **if** destino no segmento deste quadro que chegou
    - **then** descarta o quadro
    - **else** encaminha o quadro na interface indicada
    - }
    - **else** flood (enchente -> encaminha a todas as portas)
- Isolamento de tráfego:
  - A instalação do *switch* quebra as sub-redes em segmentos de LAN:
    - *Switch* filtra pacotes:
    - Alguns quadros do mesmo segmento de LAN não são usualmente encaminhados para outros segmentos de LAN;
    - Segmentos se tornam separados em domínios de colisão.

2.5.6 O Protocolo da camada de enlace para LAN: padrão IEEE 802.2 – LLC – Logical Link Control

No início desta unidade (atividade prática), vimos vários protocolos que permitem que duas máquinas se comuniquem de forma confiável por meio de uma linha não confiável, usando diversos protocolos de enlace que oferecem soluções para cada tipo de situação (erros, capacidade finita de *buffers*, simples ou f*ull-duplex* etc.) pelo uso de confirmações, temporização e janelas deslizantes.

Nas redes LAN, a camada de enlace depende do controle de acesso ao meio provido pela camada MAC, porém esta não se trata do enlace, mas sim do controle de acesso ao meio compartilhado. O padrão 802 oferece apenas um transporte de datagramas não confiável, para levar pacotes (por exemplo, IP) da

camada de rede. É necessário, portanto, algum controle de erro e de fluxo para ser agregado a esta capacidade de envio de quadros provida pelo IEEE802 na camada MAC. É o 802.2 LLC – Logical Link Control que efetua o controle de enlace lógico da conexão, acima do protocolo MAC.

O LLC recebe os pacotes da camada de rede, forma um quadro e o repassa à camada MAC para envio pela camada física.

Desta forma, ele oculta as diferenças entre as diversas redes LAN e oferece uma interface única para a camada de rede. Ele se baseia muito no protocolo HDLC e o envio, antes de usar uma primitiva tipo To-Physical_layer(), repassa o quadro à camada MAC que então, por meio de seu protocolo, o encaminha pela camada física.

O LLC oferece três opções de serviço:

- Serviço de datagramas não confiáveis;
- Serviço de datagramas com confirmação;
- Serviço orientado a conexão e com confirmação.

O cabeçalho LLC tem 3 campos:

- Ponto de acesso destino;
- Ponto de acesso origem;
- Campo de controle.

Os pontos de acesso informam de qual processo o quadro partiu e para qual deve ser entregue, substituindo o campo TIPO do DIX. O controle tem número de sequência e controle de ACK, semelhantes aos do HDLC e é usado para entrega confiável de quadros.

Desta forma, um pacote da camada de rede recebe um cabeçalho LLC formando um quadro e quando submetido à camada MAC recebe o cabeçalho MAC. Na recepção, os cabeçalhos MAC são retirados e o LLC faz o controle de recepção, como no HDLC, retira o cabeçalho LLC e entrega o pacote à camada de rede, mantendo uma interface comum para esta camada, seja para conexões ponto a ponto (linhas discadas, ADSL, cabo Modem etc.), seja pelas redes LAN.

2.5.7 Padronização de LAN – padrão IEEE 802:

O esforço de padronização do IEEE (Institute for Electrical and Electronic Engineering) tem resultado nas diversas tecnologias tanto das redes LAN (objetivo principal) quanto de outras propostas (PAN, METRO-MAN etc.). Deste esforço resultaram os padrões listados na tabela abaixo que resume tudo o que está padronizado, ativo ou em processo de padronização.

Number	Topic
802.1	Overview and architecture of LANs
802.2 ↓	Logical link control
802.3 *	Ethernet
802.4 ↓	Token bus (was briefly used in manufacturing plants)
802.5	Token ring (IBM's entry into the LAN world)
802.6 ↓	Dual queue dual bus (early metropolitan area network)
802.7 ↓	Technical advisory group on broadband technologies
802.8 †	Technical advisory group on fiber optic technologies
802.9 ↓	Isochronous LANs (for real-time applications)
802.10 ↓	Virtual LANs and security
802.11 *	Wireless LANs
802.12 ↓	Demand priority (Hewlett-Packard's AnyLAN)
802.13	Unlucky number. Nobody wanted it
802.14 ↓	Cable modems (defunct: an industry consortium got there first)
802.15 *	Personal area networks (Bluetooth)
802.16 *	Broadband wireless
802.17	Resilient packet ring

Figura 34. Padrão IEEE 802

2.6 Camada de enlace: considerações finais

Nesta camada foram tratadas questões relativas aos algoritmos de alocação de canais e padrões de tecnologias de LAN, desde os esquemas mais simples de TDM e FDM, passando por métodos mais complexos como ALOHA, CSMA, MACAW, DSSS, FHSS, bem como (D)WDM, CDMA etc.

Foram analisadas as diferentes LAN (cabeadas, metálicas e ópticas e as sem fio), bem como seus padrões de protocolos (IEE 802.x), as pontes e *switches*.

2.7 Referências

COMMER, D. *Redes de Computadores e Internet*, 2a ed. Bookman, 2001.

KUROSE, J. F.; ROSS, K. W. *Redes de Computadores e a Internet*: uma abordagem top-down. Tradução da 3a ed. Pearson, 2006.

HUMMEL S. *Network Planning and Design Guide*, 1a ed. Design Series, 2005.

OLIFER, N.; OLIFER, V. *Redes de Computadores*: Princípio, Tecnologias e Protocolos para o Projeto de Redes. Tradução da 1a ed. LTC, 2008.

OPPENHEIMER, P. *Top-down Network Design*, 2a ed. Campus, 2004.

TANENBAUM, A. S. *Redes de Computadores*. Tradução da 4a ed. Rio de Janeiro: Campus, 2003.

STALLINGS, W. *Local & Metropolitan Area Networks*, 5a ed. Prentice Hall, 1997.

UNIDADE 3

A camada de inter-redes:

projeto e roteamento

3.1 Primeiras palavras

Nesta terceira unidade, trabalharemos os aspectos relativos às questões de projeto da camada de redes, questões de roteamento e de endereçamento e questões da interligação de redes diferentes. Analisaremos, ainda, aspectos do controle de congestionamento.

3.2 Introdução

A camada de inter-redes cuida da transferência de pacotes entre os *hosts* de origem e os de destino. Para se alcançar determinado destino, roteadores intermediários poderão ser utilizados e podem pertencer a diferentes redes intermediárias. A escolha dos roteadores que deverão ser percorridos, isto é, a rota que será seguida, é função desta camada.

A camada de enlace, que estudamos na unidade anterior, apenas troca quadros entre elementos vizinhos interconectados por algum meio físico, mas não detém a noção de rota, uma vez que não mantém a visão global da rede. Desta forma, entende-se que a camada inter-redes é a primeira na pilha que cuida da transmissão fim a fim entre *hosts* de origem e destino na borda da rede.

Essa camada precisa conhecer a topologia da rede (ou redes) e identificar os roteadores disponíveis para o melhor encaminhamento dos pacotes. Na camada de inter-redes, alguns algoritmos de roteamento são elaborados com o objetivo de aperfeiçoar as rotas adotadas pelos pacotes, de forma a controlar o congestionamento nos roteadores.

Nesta unidade, trataremos das redes que operam em modo datagrama e das redes que operam em modo circuito virtual. Analisaremos como funciona a *internet* ao nível da camada de inter-rede e abordaremos aspectos das redes de alta velocidade.

3.3 Roteiro da unidade

- Introdução;
- Algoritmos de roteamento;
- Roteadores;
- Roteamento na *internet*: os protocolos IP, ICMP, OSPF e BGP;
- DHCP e NAT;
- Controle de congestionamento e QoS;

- Princípios gerais de controle de congestionamento;
- Políticas de prevenção de congestionamento;
- Controle de congestionamento em sub-redes V.C.;
- Controle de congestionamento em sub-redes datagrama;
- Escoamento de carga (*load shedding*);
- Controle de flutuação (*jitter control*).

3.3.1 Questões de projeto da camada de redes:

Os protocolos da camada de rede operam num contexto de comunicação fim a fim, passando por todos os roteadores existentes pelo caminho. O objetivo é definir os serviços oferecidos à camada de transporte e como eles são implementados no âmbito interno da rede.

Neste contexto, devemos tratar de:

- Comutação de pacotes *store-and-forward* entre *hosts*;
- Quais os serviços serão providos à camada de transporte;
- Implementação de serviço sem conexão;
- Implementação de serviço orientado a conexão;
- Comparação de sub-redes de circuito virtual e datagramas.

Exigências que devem ser atendidas:

- Suportar pilhas de protocolos inferiores diferentes;
- Admitir camadas inferiores **heterogêneas**;
- Admitir organização em múltiplos domínios.

Requisitos ainda em desenvolvimento:

- Qualidade de Serviço (QoS);
- Mobilidade total (roteamento *wireless*).

Os protocolos da camada de rede estão presentes em *hosts* e em roteadores. Eles possuem três funções importantes: **determinação do caminho**, ou seja, a rota seguida pelos pacotes da origem ao destino; **comutação**, mover os pacotes dentro do roteador, da entrada até a saída apropriada; e **estabelecimento da chamada**, algumas arquiteturas de rede requerem determinar o caminho antes de enviar os dados.

Como a função da camada de rede é transportar pacotes entre *hosts* (origem-destino), no lado do transmissor os segmentos são encapsulados em datagramas e no lado do receptor, os datagramas recebidos são convertidos novamente em segmentos e entregues a camada de transporte.

Neste processo, cada pacote pode ser enviado de roteador a roteador, onde é inteiramente recebido, armazenado e verificado quanto a erros, e só então, encaminhado para o próximo elemento da rede segundo o algoritmo definido pela tabela de roteamento. Este processo de comutação é dito armazena-e-encaminha (*store-and-forward*) e é o modo de operação dos roteadores.

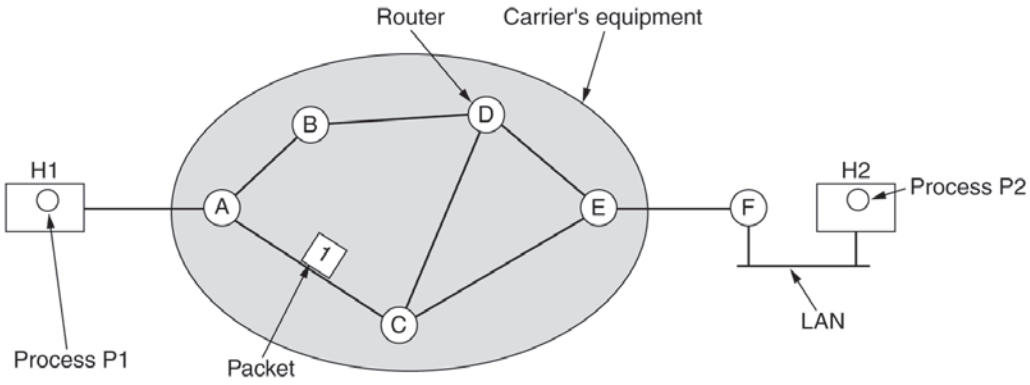


Figura 1. Comutação de pacotes armazena-e-encaminha (*store-and-forward*).

3.3.2 Interação entre comutação e roteamento:

A comutação consiste em mover pacotes dentro do roteador, da **entrada** para a **saída** apropriada. O roteamento consiste em determinar a **rota** a ser seguida pelos pacotes.

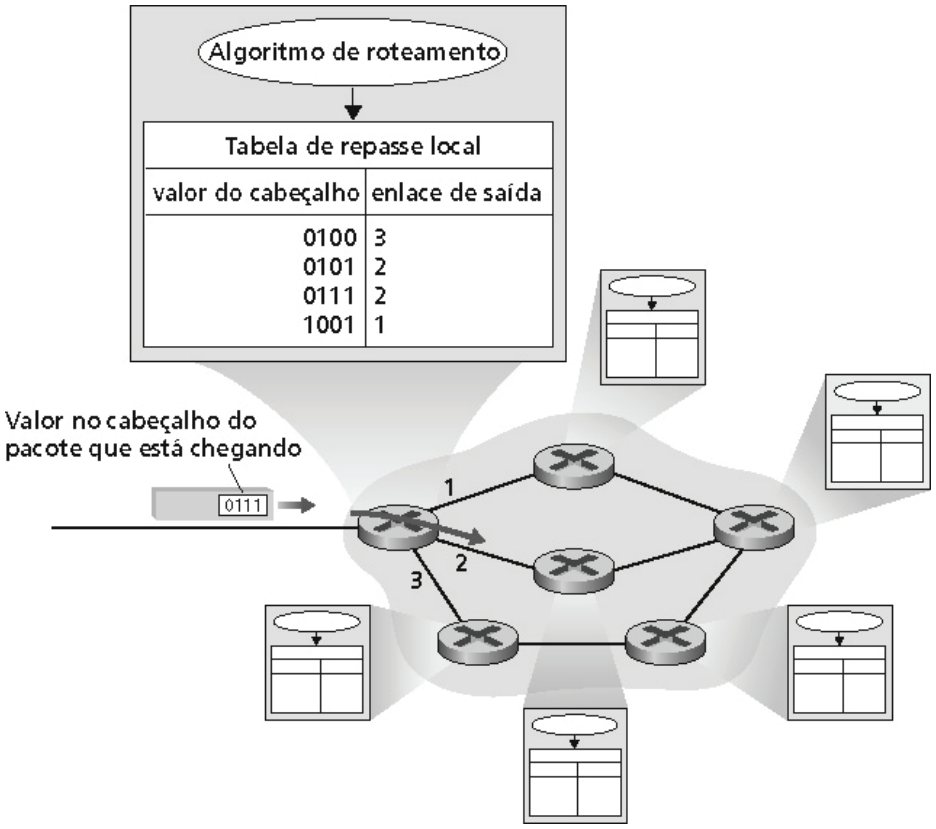


Figura 2. Roteamento de pacotes.

3.3.3 Serviços providos à camada de transporte:

- Transporte transparente de pacotes entre *hosts* fim a fim (roteamento);
- Serviços independentes de tecnologia de rede e roteadores;
- Isolamento do número, tipo e topologia dos roteadores;
- Plano de endereçamento global e uniforme para *hosts* em LAN e WAN;

A camada de rede oferece tais serviços à camada de transporte por meio de dois modos de operação:

- Serviço sem conexão: pelo envio de datagramas não confiáveis;
- Serviço orientado a conexão: pela definição de circuitos virtuais.

Cabe lembrar que estes serviços devem estar independentes da tecnologia de roteadores, da topologia da rede e do número de roteadores presentes na rede. Os endereços de rede, que identificam os *hosts* e roteadores, devem obedecer a um plano de numeração uniforme, seja nas WAN como nas LAN e *hosts*.

3.3.4 Roteamento numa sub-rede de datagrama:

Nos serviços de datagramas, cada pacote segue seu caminho de forma independente, sendo tratado e roteado, a cada novo roteador, de acordo com a tabela que é especificada pelo algoritmo de roteamento implementado. Vejamos algumas características desses serviços:

- Não existe o conceito de “conexão” na camada de rede;
- Não guarda estado sobre transmissões;
- Pacotes são roteados usando endereços de destino;
- Dois pacotes podem seguir caminhos diferentes até chegarem ao mesmo destino.

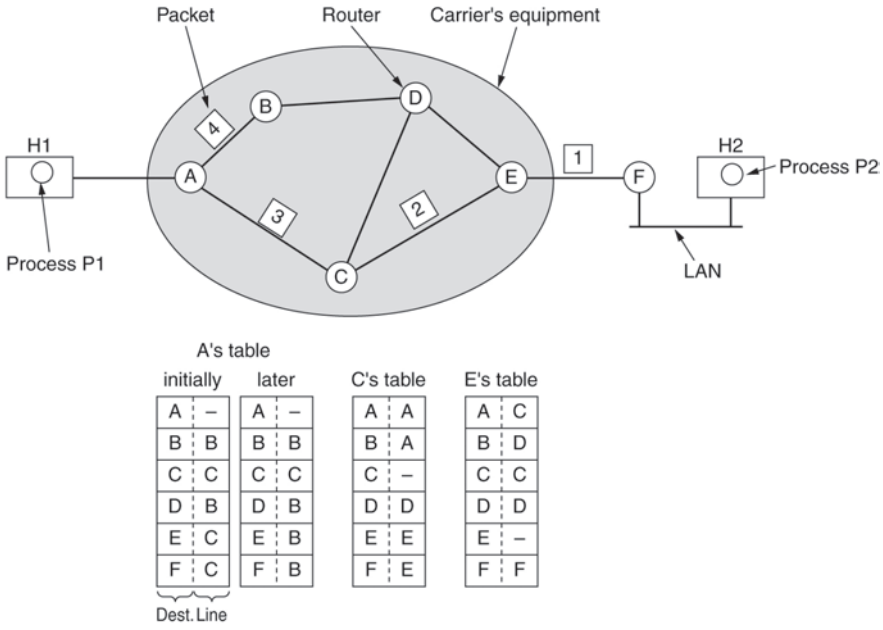


Figura 3. Roteamento numa sub-rede de datagrama.

3.3.5 Roteamento numa sub-rede de circuito virtual:

No serviço de circuito virtual, um pacote inicial de abertura do circuito é roteado, passando pelos roteadores ao longo da rota e registrando neles o circuito. Depois de concluída esta etapa inicial, onde também são negociadas as condições para o circuito que está sendo estabelecido, os pacotes de dados são encaminhados pelo circuito identificado para eles, e todos seguem a mesma rota. Ao final, um pacote de controle de encerramento desfaz em cada roteador o circuito estabelecido, liberando os recursos alocados a ele.

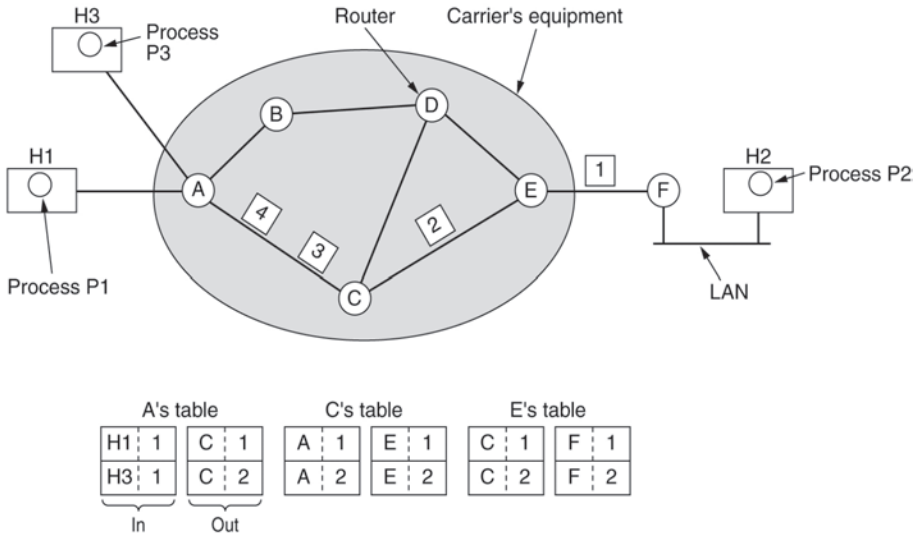


Figura 4. Roteamento numa sub-rede de circuito virtual.

Pergunta: *é possível montar uma camada de rede sobre outra?*

A tabela seguinte mostra uma comparação entre esses dois modos de encaminhamento.

Tabela 1. Comparativo entre sub-redes de datagrama e circuito virtual.

Questão	Sub-rede de datagrama	Sub-rede de circuito virtual
Configuração do circuito	Não é necessário	Necessário
Estado da informação	Os roteadores não mantêm o estado da informação sobre as conexões	Cada circuito virtual requer um espaço na tabela do roteador para cada conexão
Roteamento	Cada pacote é roteado de forma independente	A rota é escolhida quando o circuito virtual é configurado. Todos os pacotes seguem o mesmo caminho
Efeito de falhas no roteador	Nada acontece, exceto para o pacote perdido durante a falha	Todos os circuitos virtuais que utilizarem o roteador serão encerrados
Qualidade de Serviço (QoS)	Difícil de implementar	Fácil de implementar se os recursos puderem ser alocados previamente para cada circuito virtual
Controle de congestionamento	Difícil de implementar	Fácil de implementar se os recursos puderem ser alocados previamente para cada circuito virtual

3.4 Algoritmos de roteamento

Roteamento: visa planejar e determinar a rota ou o caminho a ser seguido pelos pacotes.

Comutação ou repasse: visa mover pacotes dentro do roteador, da entrada para a saída apropriada.

O roteamento tem como propósito definir qual a melhor rota que o pacote deve seguir para chegar a seu destino. Esta definição de melhor rota passa por uma descrição de rotas ótimas (caminhos mais curtos), sem considerar diretamente a topologia ou o tráfego. É o princípio da **otimização**. Ele estabelece que, se um roteador J estiver no caminho ótimo entre os roteadores I e K, então, o caminho ótimo entre J e K também estará na mesma rota (Exercício: *Tente provar - por negação!*).

Como consequência, observa-se que o conjunto de rotas ótimas de todas as origens até um dado destino forma uma árvore de rotas com raiz no destino. Esta árvore é chamada de árvore de escoamento.

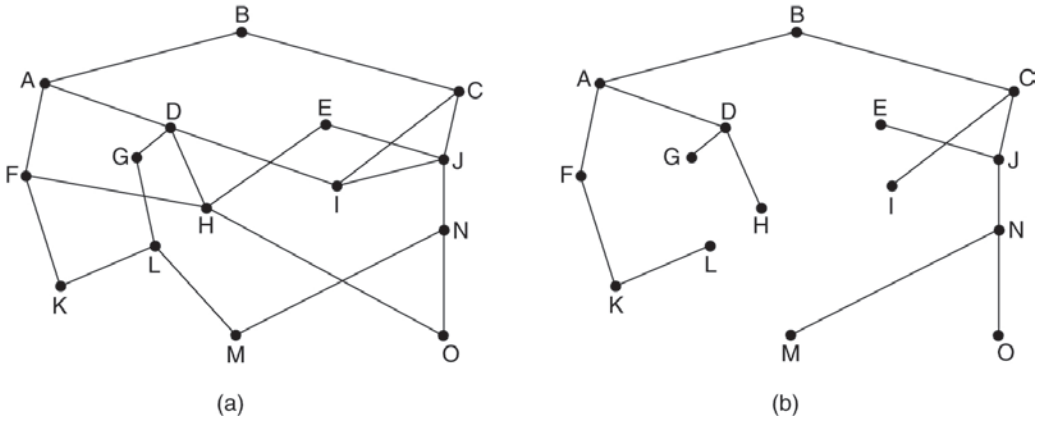


Figura 5. (a) Sub-rede; (b) árvore de escoamento para o roteador B.

3.4.1 Roteamento pelo caminho mais curto (Shortest Path Routing):

Neste algoritmo, a sub-rede (de roteadores) é vista como um grafo, sendo que cada nodo é visto como um roteador e cada arco como um *link* de enlace. A ideia é escolher o caminho mais curto entre um par de roteadores (de origem e de destino). O conceito de caminho mais curto está relacionado a alguma métrica, tais como o número de *hops* (saltos), a distância física (extensão) ou a latência devido ao enfileiramento e ao atraso de transmissão.

Dijkstra, em 1959, propôs um algoritmo, no qual, a partir de um nodo de origem, se escolhe o segmento (próximo nodo) de menor distância acumulada

desde a origem. Em cada arco está associada a distância relativa a ele. Entre parênteses tem-se a distância da origem e o nodo de onde o caminho vem. As setas indicam as escolhas de menor distância. Na figura a seguir, parte-se do nodo A, escolhe-se o nodo B com distância 2 desde A. Em seguida, escolhe--se o nodo E (4, B) , depois o G (5, E), e assim por diante, até o nodo D (10, H). O caminho mais curto resultante é, portanto, ABEFHD, com custo 10. Os primeiros 5 passos usados no cômputo do caminho mais curto de A até D é apresentado na figura abaixo:

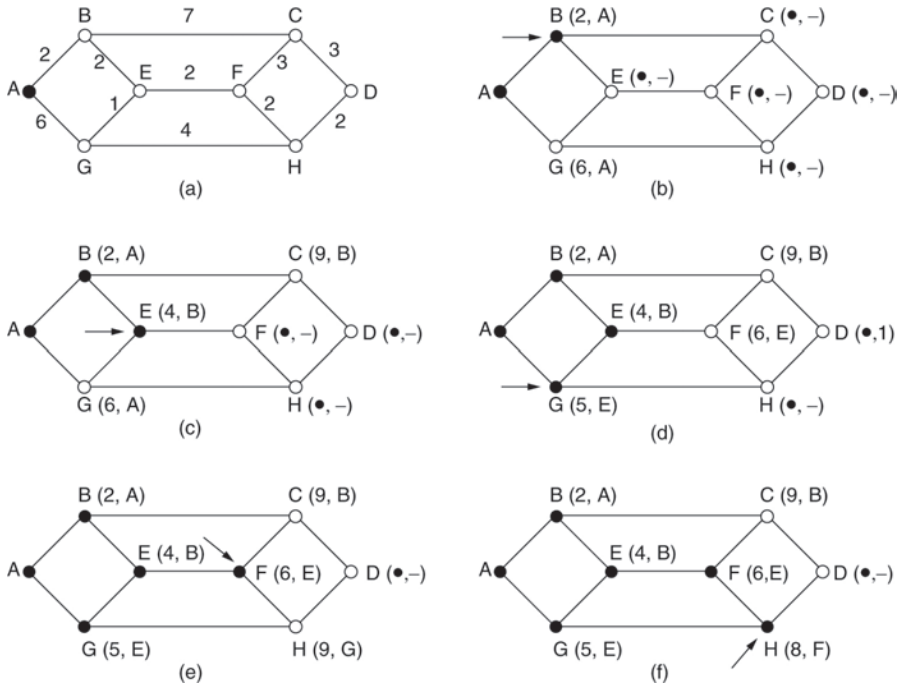


Figura 6. Roteamento pelo caminho mais curto (Shortest Path Routing).

Vejamos agora o algoritmo:

```
#define MAX_NODES 1024                  /* maximum number of nodes */
#define INFINITY 1000000000             /* a number larger than every maximum path */
int n, dist[MAX_NODES][MAX_NODES];/* dist[i][j] is the distance from i to j */

void shortest_path(int s, int t, int path[])
{ struct state {                        /* the path being worked on */
      int predecessor;                  /* previous node */
      int length;                       /* length from source to this node */
      enum {permanent, tentative} label; /* label state */
  } state[MAX_NODES];

  int i, k, min;
  struct state *p;

  for (p = &state[0]; p < &state[n]; p++) { /* initialize state */
      p->predecessor = -1;
      p->length = INFINITY;
      p->label = tentative;
  }
  state[t].length = 0;  state[t].label = permanent;
  k = t;                                /* k is the initial working node */
  do {                                  /* Is there a better path from k? */
      for (i = 0; i < n; i++)           /* this graph has n nodes */
          if (dist[k][i] != 0 && state[i].label == tentative) {
              if (state[k].length + dist[k][i] < state[i].length) {
                  state[i].predecessor = k;
                  state[i].length = state[k].length + dist[k][i];
              }
          }

      /* Find the tentatively labeled node with the smallest label. */
      k = 0; min = INFINITY;
      for (i = 0; i < n; i++)
          if (state[i].label == tentative && state[i].length < min) {
              min = state[i].length;
              k = i;
          }
      state[k].label = permanent;
  } while (k != s);

  /* Copy the path into the output array. */
  i = 0;  k = s;
  do {path[i++] = k; k = state[k].predecessor; } while (k >= 0);
}
```

3.4.2 Roteamento por inundação (*flooding*):

Uma alternativa para roteamento é enviar uma cópia do pacote por todas as linhas de saída de cada roteador e eliminar as duplicatas recebidas até atingir o nodo de destino. Este processo é dito inundação ou enchente controlada. Uma forma de controle é adicionar um contador de *hops* nos pacotes e o decrementar a cada nodo (*hop*). Claro que o contador deve ter inicialmente o comprimento até o destino, ou no pior caso, o diâmetro (maior caminho) da rede.

Algoritmos de inundação não são eficientes e, portanto, são pouco utilizados, mas existem situações onde são aplicáveis.

3.4.3 Roteamento por vetor de distâncias (Bellman-Ford e Ford-Fulkerson):

É um processo dinâmico e adaptativo de estabelecimento das tabelas de rotas. Cada nodo "aprende" sobre os custos de encaminhamento por todos os demais nodos, saindo pelos seus nodos vizinhos e difundindo esses custos para estes, os quais recalculam periodicamente em suas tabelas num processo contínuo e periódico de atualizações que leva em conta a variação das filas de transmissão em cada nodo.

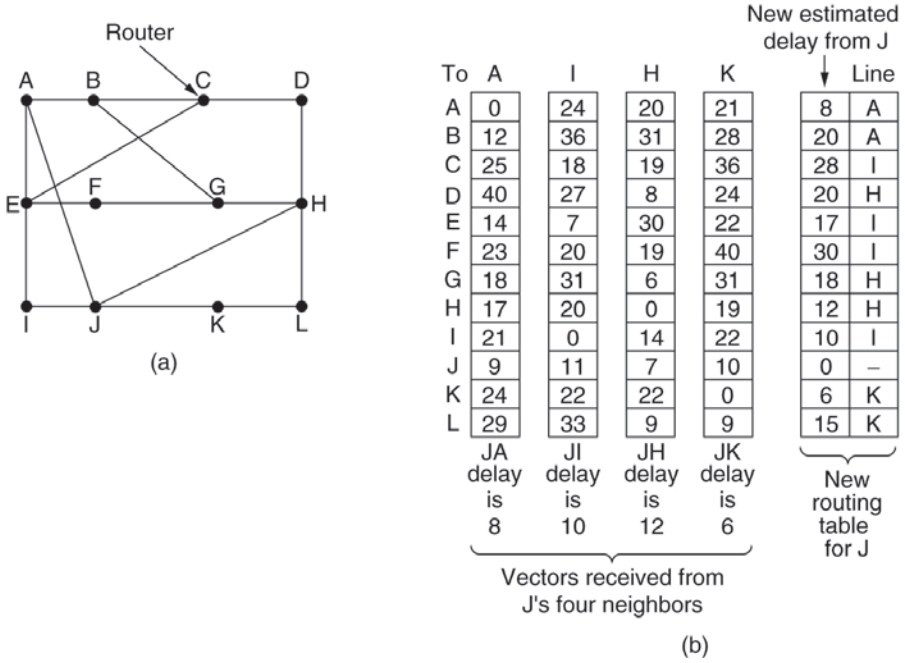


Figura 7. Roteamento por vetor de distâncias: (a) sub-rede; (b) entradas de A, I, H, K e a nova tabela de J.

Também chamado de algoritmo de Bellman-Ford (1957) e Ford-Fulkerson (1962) pelos seus proponentes, foi o algoritmo original da *internet* com o nome de RIP (Routing Internet Protocol). O algoritmo por vetor de distâncias reage bem às boas notícias e lento às más. Posteriormente foi detectado que esse algoritmo apresentava o problema da contagem até o infinito, isto é, ele pode convergir para uma situação de erro em alguns casos. Por esta razão foi abandonado.

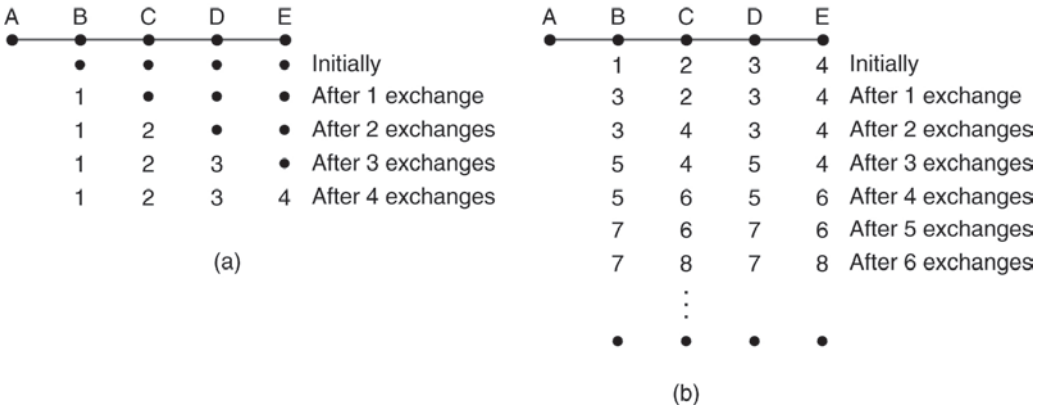


Figura 8. Roteamento por vetor de distâncias: (a) nodo A entra em serviço; (b) queda do nodo A.

3.4.4 Roteamento pelo estado de enlace:

É outra técnica proposta e que consiste de 5 passos principais:

1. Descobrir quem são seus vizinhos e "aprender" seus endereços de rede;
2. Medir o atraso (ou custo) até cada um deles;
3. Criar um pacote com essas informações para informar a todos o que ele acabou de "aprender";
4. Difundir para todos os nodos (roteadores);
5. Fazer cálculo do caminho mais curto até cada um dos demais nodos e atualizar sua tabela.

A medição do custo até os vizinhos pode ser feita monitorando a rede. De posse das informações de quem são os vizinhos de quem, um grafo pode ser montado e o cálculo da tabela pode ser obtido aplicando o algoritmo de Dijikstra (1959) localmente.

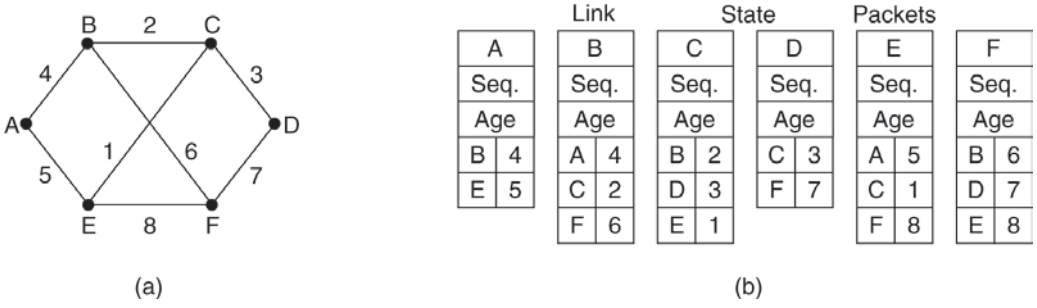
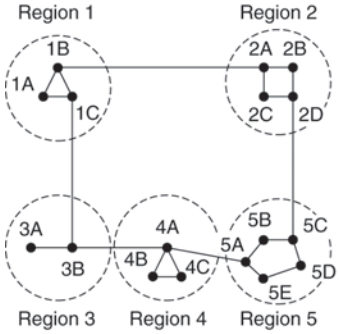


Figura 9. Roteamento pelo estado de enlace: (a) sub-rede; e (b) os pacotes de estado de enlace para essa sub-rede.

3.4.5 Roteamento hierárquico:

Conforme as redes vão crescendo, as tabelas de roteamento tendem a ficar muito grandes. Uma alternativa é agregar nodos de uma dada região em nodos que os representem. Dessa forma, têm-se dois ou mais níveis de roteamento: entre regiões e intra-região. As tabelas em cada nível ficam muito mais simples e curtas.

Numa rede com N nodos, o número ideal de níveis é ln N (logaritmo de N), conforme estudos de Kleinrock e Kamoun, em 1979, num total de ln N entradas na tabela.



(a)

Full table for 1A

Dest.	Line	Hops
1A	–	–
1B	1B	1
1C	1C	1
2A	1B	2
2B	1B	3
2C	1B	3
2D	1B	4
3A	1C	3
3B	1C	2
4A	1C	3
4B	1C	4
4C	1C	4
5A	1C	4
5B	1C	5
5C	1B	5
5D	1C	6
5E	1C	5

(b)

Hierarchical table for 1A

Dest.	Line	Hops
1A	–	–
1B	1B	1
1C	1C	1
2	1B	2
3	1C	2
4	1C	3
5	1C	4

(c)

Figura 10. Modelo de roteamento em 2 níveis e 5 regiões (TANENBAUM, 2003).

3.4.6 Roteamento por difusão (*multi* ou *broadcasting*):

Eventualmente, algumas aplicações implicam em um nodo ter que enviar o mesmo pacote a vários nodos, senão a todos (por exemplo, o *network time*, relatório sobre o clima). Isto é chamado de difusão e várias técnicas foram propostas:

- Uma maneira seria o nodo ter uma lista de todos os demais e criar uma cópia para cada um e encaminhar. Este método claramente desperdiça recursos da rede e é lento;
- Outra forma é a inundação que também consome recursos demais;
- Uma terceira alternativa é o encaminhamento para vários destinos, onde um nodo define um conjunto de outros nodos para onde enviar, e esse o faz ao inserir um mapa de endereços de destino no pacote. A cada nodo

intermediário deste mapa é verificado quais linhas levam a destinos e o pacote é duplicado e transmitido nelas;

- Um quarto algoritmo é o da árvore de amplitude, o qual usa a árvore de escoamento (*sink tree*) do roteador e inicia a difusão, ao copiar um pacote em cada linha dessa árvore. O problema é conhecer a árvore.
- O quinto e último, é o algoritmo do encaminhamento reverso (r*everse path forwarding*) que funciona de modo muito simples: quando um pacote de difusão chega a um nodo, é verificado se chegou, pela linha normal de envio de pacotes, à origem da difusão. Se for o caso, há a possibilidade de ser a primeira cópia, pois veio pela melhor rota e, neste caso, é dado prosseguimento pelas linhas de saída da árvore. Caso contrário, é descartado como duplicata.

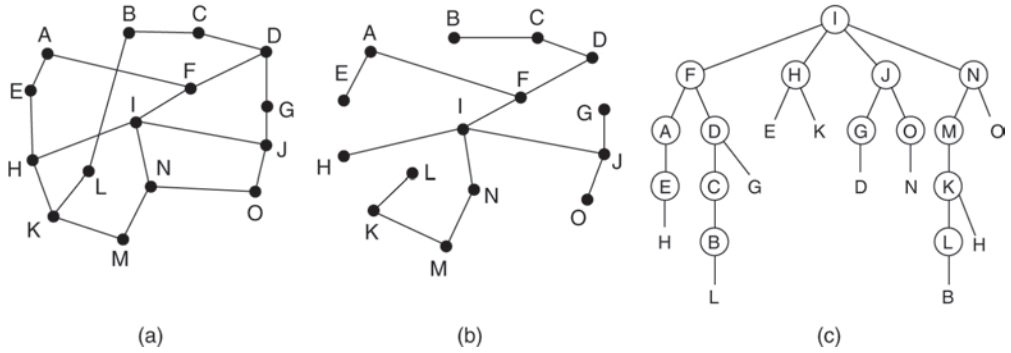


Figura 11. (a) sub-rede; (b) árvore de escoamento (*sink tree*); e (c) árvore construída pelo encaminhamento reverso.

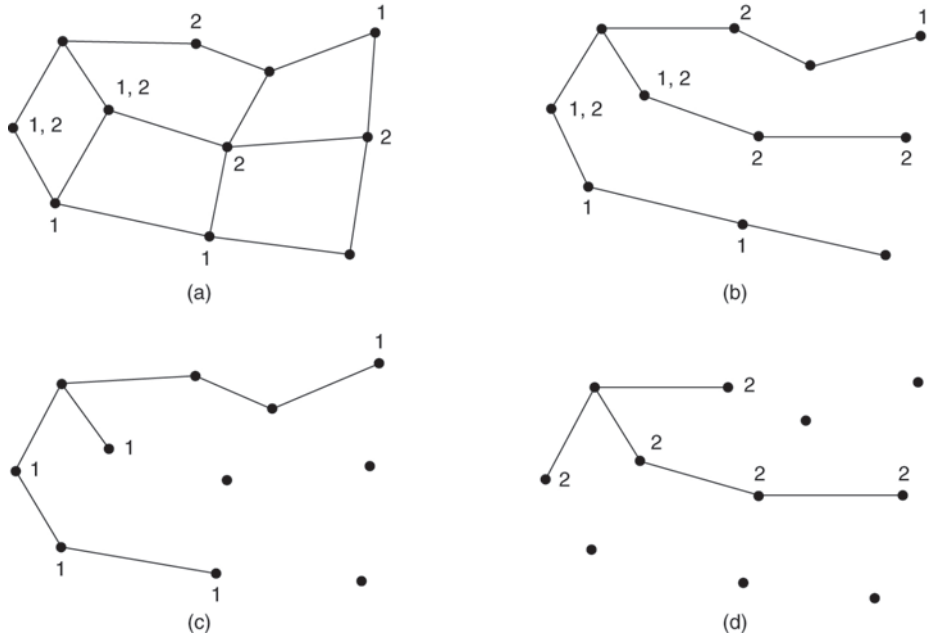


Figura 12. (a) a rede com 2 grupos *multicast* 1 e 2; (b) a árvore de expansão (*spanning* para o roteador mais à esquerda); (c) a árvore *multicast* do grupo 1; e (d) a árvore *multicast* do grupo 2.

3.4.7 Roteamento para *hosts* móveis:

Com a evolução e o uso crescente de computadores portáteis, os usuários passaram a requerer acesso a seus arquivos independentemente de onde estejam. Isso cria um complicador, pois é preciso localizar tais *hosts* antes do envio de pacotes.

Na figura a seguir é apresentado um modelo de interconexão de diferentes redes WAN, MAN, LAN e células de redes sem fio.

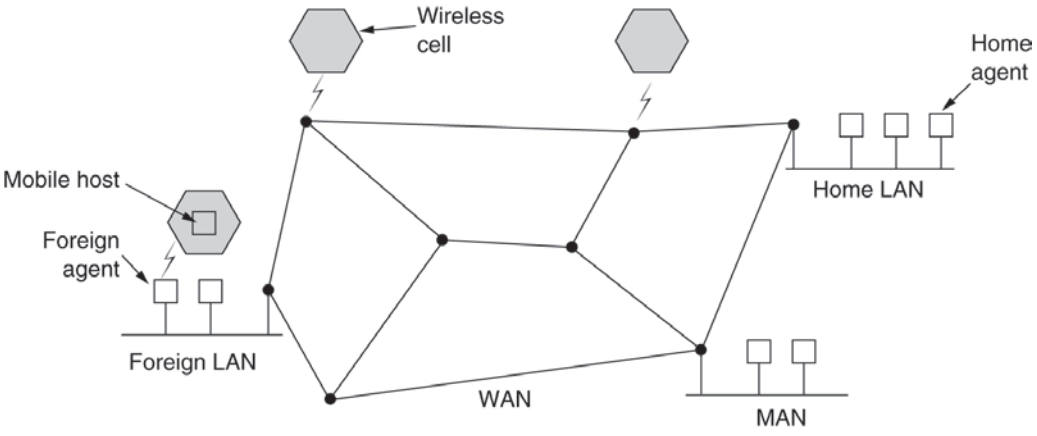


Figura 13. Roteamento para *hosts* móveis.

Hosts que não se movimentam são chamados de estacionários. Quando se movem, são ditos *hosts* migrantes e se deslocam de um local fixo a outro, de tempos em tempos, acessando a rede quando estão fisicamente conectados. Isso ocorre por meio de cabos elétricos ou ópticos. Um terceiro tipo são os *hosts* visitantes, que utilizam a rede mesmo estando em trânsito. Todo *host* tem uma base original e um endereço original (*home address*), tal como a telefonia celular.

O objetivo do roteamento agora é poder enviar pacotes a *hosts* que estão fora de suas bases de forma eficiente. O principal problema é determinar sua localização que pode mudar com o tempo. No modelo de interconexão, cada rede LAN ou célula sem fio é considerada uma área diferente, e em cada área tem-se um agente externo (*foreign agent*) que são processos que gerenciam os visitantes, externos à área. Também existe o processo agente local (*home agent*) que controla os processos desta base que se encontram fora.

Quando um novo *host* se conecta numa área, seja por cabo seja sem fio, ele deve se registrar com o agente externo desta área, da seguinte maneira:

1. Periodicamente o agente externo difunde um pacote anunciando sua existência e seu endereço. Um *host* recém-chegado ou aguarda esta mensagem de anúncio ou difunde uma consulta de “existe algum agente externo aí?”;

2. O *host* se registra no agente externo fornecendo seu endereço base, seu endereço atual de enlace e algumas informações de segurança;
3. O agente externo se comunica com o agente local deste *host* informando sua presença, o endereço da rede, fornecendo informações de segurança que autenticam o *host* e um timbre de hora;
4. O agente local autentica o *host* e confirma a migração e o registro;
5. O agente externo atualiza sua tabela de *hosts* externos e confirma ao *host* o registro.

Normalmente, quando deixa a área, o *host* móvel deve informar ao agente externo sua saída, o que nem sempre ocorre, podendo ser abruptamente desconectado quando o equipamento é desligado pelo usuário (*soft* e *hard handoff*).

Pacotes enviados ao *host* móvel vão inicialmente a sua rede base, pois seu endereço de origem é lá. O agente local encapsula este pacote e o remete ao agente externo da área onde ele se encontra (tunelamento) que o entrega ao *host*. Ao mesmo tempo, o agente local envia a origem o endereço atual do *host* que irá encapsular os novos pacotes dirigidos a ele no campo de carga e os enviará diretamente ao agente externo daquela área, completando o processo.

3.4.8 Roteamento em redes ad-hoc (ou MANets – Mobile ad-hoc Nets):

Uma classe de redes especiais e interessantes para o roteamento é a das redes ad-hocs. Nessas redes, em geral, não há infraestrutura de ponto de acesso e os *hosts* se movem todos ao mesmo tempo, mesmo que a topologia varie. Nestes casos, cada *host* é ao mesmo tempo um *host* e um roteador para os demais. Vejamos alguns exemplos que demandam roteadores móveis:

- Veículos militares no campo de batalha:
  - Sem infraestrutura.
- Uma frota de navios no mar:
  - Todos se movendo a todo o tempo.
- Equipes de emergência em terremotos:
  - A infraestrutura foi destruída.
- Um grupo de pessoas com seus *notebooks*:
  - Sem uma rede 802.11 (ponto de acesso).

Um algoritmo proposto para redes ad-hoc é o AODV – ad-hoc Distance Vector (Perkins e Royer, 1999) que é uma adaptação do algoritmo de vetor de distâncias para redes ad-hoc. Conexões existem entre dois nodos (*host* e roteador) se estiverem ao alcance do rádio. Um processo em A que deseja enviar um dado para outro em I deve, primeiramente, calcular uma rota até I.

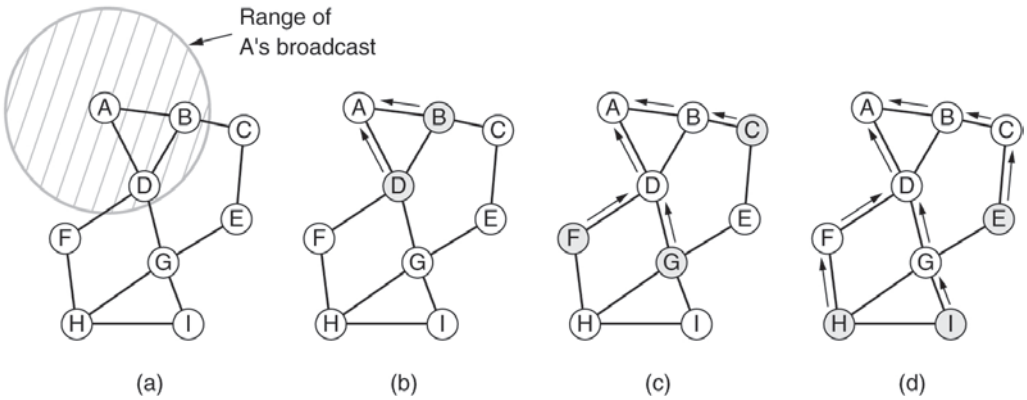


Figura 14. Descoberta de rota. (a) área hachurada trata-se da área de alcance de A; (b) após B e D terem recebido a difusão de A; (c) após C, F, e G terem recebido a difusão de A; (d) após E, H, e I terem recebido a difusão de A. Os nodos em cinza são novos receptores e as setas mostram as rotas reversas possíveis.

Um pacote tipo ROUTE-REQUEST procura encontrar a rota. Uma vez atingido o nodo destino, I, um pacote ROUTE REPLY é retornado à origem.

Source address	Request ID	Destination address	Source sequence #	Destination sequence #	Hop count

Figura 15. Formato de um pacote de ROUTE REQUEST.

Source address	Destination address	Destination sequence #	Hop count	Lifetime

Figura 16. Formato de um pacote de ROUTE REPLY.

Como a topologia pode mudar repentinamente, dado a mobilidade dos nodos, os nodos difundem periodicamente um pacote de HELLO para ver se seus vizinhos ainda estão lá. Se estiverem, eles respondem. Caso contrário, a rota pode ser recalculada.

3.5 Roteadores

Os roteadores possuem duas funções chave:

- Executar algoritmos e protocolos de roteamento: RIP, OSPF, BGP, dentre outros;
- Repassar datagramas da interface de entrada para a saída.

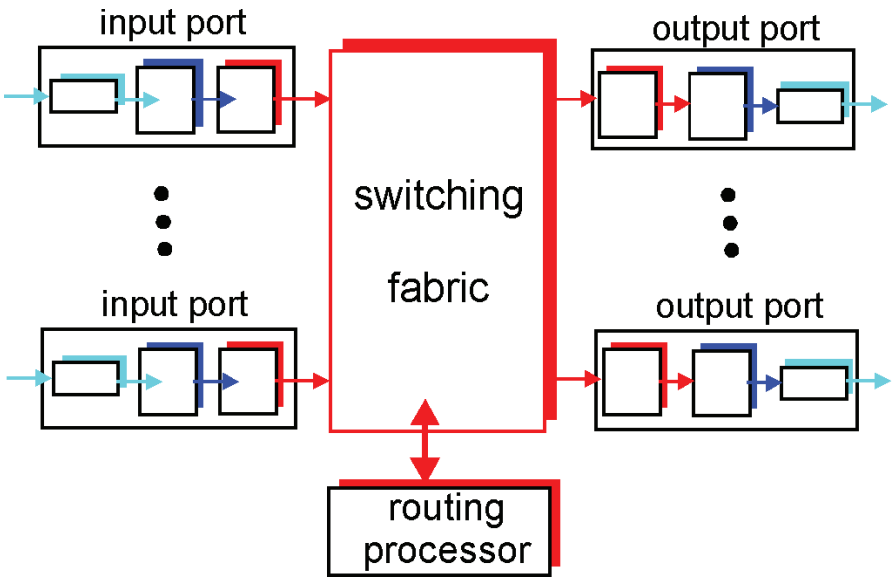


Figura 17. Arquitetura dos roteadores.

Dentro de um roteador existe uma das 3 estruturas principais de comutação: comutação via memória, comutação via barramento e comutação via *cross-bar*.

A comutação via memória esteve presente nos roteadores da primeira geração, onde o pacote era copiado para a memória pelo processador do sistema. A velocidade estava limitada pela largura de banda da memória.

Na comutação via barramento, o datagrama viaja da memória da porta de entrada à memória da porta de saída, via um barramento compartilhado. A taxa de comutação está limitada pela largura de banda do barramento.

Na comutação via *cross-bar*, as portas podem “conversar” ao mesmo tempo na matriz. Essa comutação supera as limitações dos barramentos. Suas taxas de comutação podem variar de 100 a 200Gbps pela rede de interconexão.

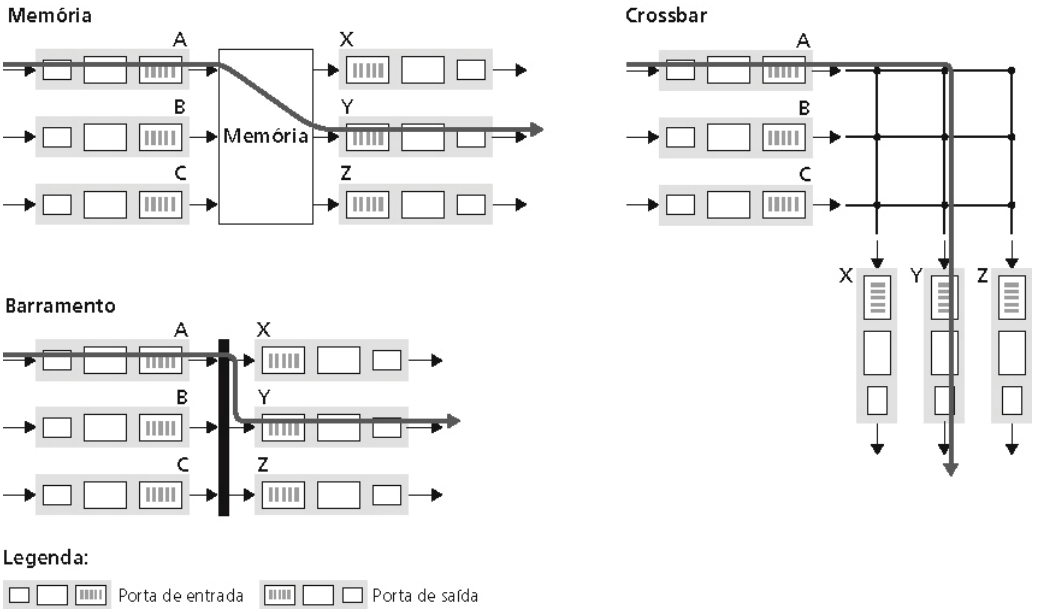


Figura 18. Estruturas de comutação.

3.6 Roteamento na *internet*

Vamos ver agora como os aspectos relativos à camada de rede foram aplicados a *internet*. Cabe notar que a *internet* é uma rede em modo datagrama de comutação de pacotes IP. Veremos aspectos do protocolo, endereçamento, controle da rede e evolução. O estudo de roteamento na *internet* envolve o estudo de:

- Protocolo IP;
- Endereçamento IP;
- Internet Control Protocols;
- Interior Gateway Routing Protocol;
- Exterior Gateway Routing Protocol;
- Internet Multicasting;
- Mobile IP;
- IPv6.

A estrutura geral da camada de redes na *internet* é como ilustra a figura a seguir:

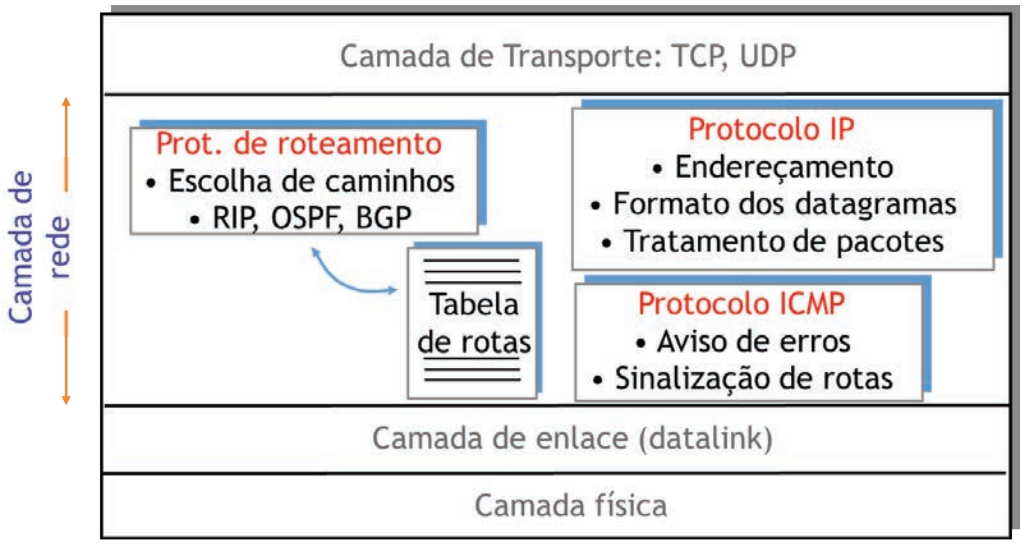


Figura 19. Estrutura da camada de rede.

O projeto da *internet* obedece a alguns princípios básicos:

- Garantir que a rede funcione;
- Mantê-la simples e fazer escolhas claras;
- Explorar modularidade;
- Esperar heterogeneidade;
- Evitar opções e parâmetros estáticos;
- Procurar por um bom projeto;
- Ser restrito quando enviando e tolerante quando recebido;
- Pensar em escalabilidade;
- Considerar performance e custo.

A camada de rede é vista como uma coleção de sistemas autônomos (SAs) interconectados. Não há uma estrutura padrão, mas apenas a interconexão de diferentes *backbones* continentais e/ou nacionais com ampla largura de banda e roteadores rápidos (nível superior). Interconectados a estes *backbones* estão as redes regionais ou nacionais menores (nível intermediário). E, por fim, ligados a estas redes regionais têm-se MAN e LAN de empresas, governos, acadêmicas e provedores de serviços (ISPs).

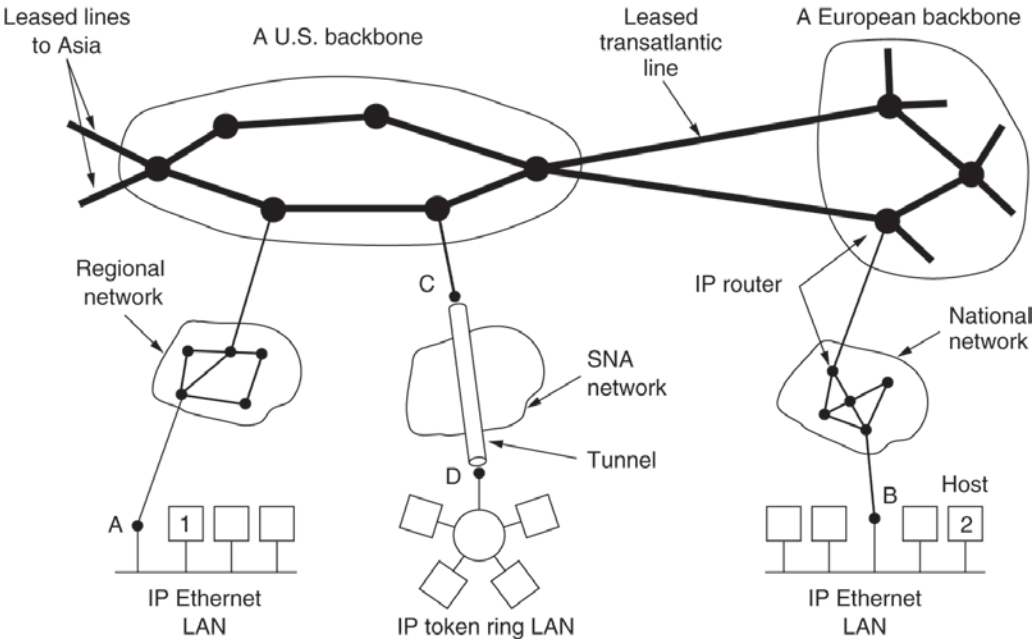


Figura 20. A *internet*: uma coleção de sub-redes.

O elemento comum entre todas estas redes é o protocolo IP (Internet Protocol).

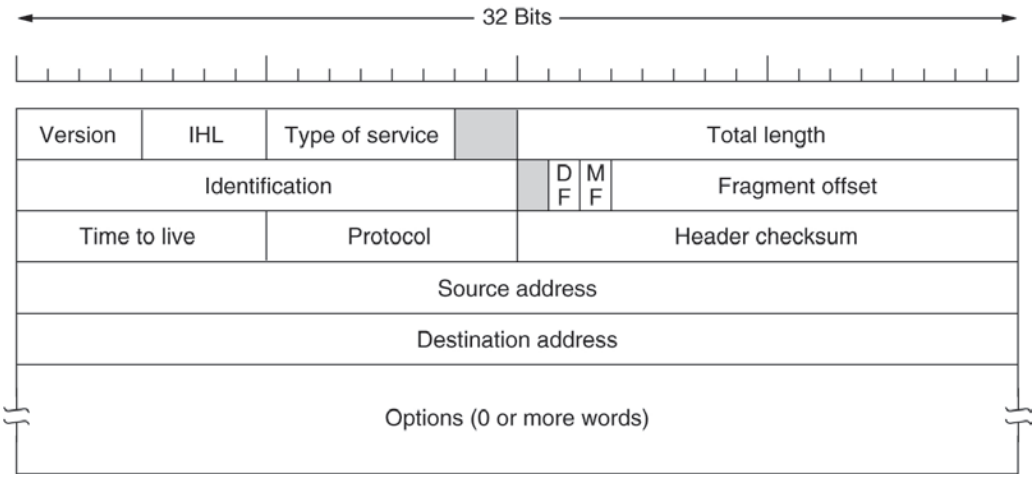


Figura 21. Cabeçalho do IPv4.

Um pacote IP é um *buffer* que tem um cabeçalho como o da figura acima, organizado em linhas de 32bits, onde:

- **Version**: indica a versão utilizada do protocolo (atualmente é 4, mas estamos migrando para 6);
- **IHL**: indica o tamanho, em palavras de 32bits, do cabeçalho que varia em cada pacote. O mínimo é 5;
- **Type of service**: identifica a classe de serviço sendo utilizada. Relaciona aspectos de desempenho e confiabilidade;

- **Total lenght**: indica o tamanho do datagrama IP completo. É limitado a 65.535bytes;
- **Identification**: permite que o destino determine a qual pacote um fragmento de pacote pertence. Todos os fragmentos de um mesmo pacote têm a mesma identificação;
- **DF e MF**: são bits indicadores de fragmentação, ou seja, DF indica que o datagrama não deve ser fragmentado e MF indica que este é um fragmento e que existem outros. O último fragmento tem esse bit zerado;
- **Fragment offset**: indica a posição relativa deste fragmento no datagrama quando há fragmentação, isto é, MF = 1;
- **Time to live (TTL)**: é um contador de tempo de vida útil do datagrama. É limitado a 255 e é decrementado em cada *hop* que o datagrama pode fazer para chegar ao destino. Se chegar a zero é descartado, gerando um pacote de advertência à origem e relatando a ele o fato (destino inatingível);
- **Protocol**: informa a que protocolo da camada de transporte ele deve ser entregue;
- **Header check-sum**: permite verificar erros no cabeçalho em cada roteador;
- **Source address e destination address**: indicam respectivamente os endereços de rede da origem e do destino, mostrando a rede e seu número de *host*;
- **Options**: definem opções e especificam algumas características do envio do datagrama.

Option	Description
Security	Specifies how secret the datagram is
Strict source routing	Gives the complete path to be followed
Loose source routing	Gives a list of routers not to be missed
Record route	Makes each router append its IP address
Timestamp	Makes each router append its address and timestamp

Figura 22. Opções do protocolo IP.

Na *internet*, cada dispositivo (*host* ou roteador) é identificado por meio de um endereço único, contendo um campo de identificação da rede e da estação na rede. Na realidade, os endereços identificam uma interface de rede e não a estação propriamente dita. Roteadores possuem múltiplos endereços, um para cada rede onde se encontram.

Inicialmente os endereços foram agrupados em 5 classes chamadas endereços de classe completa. A atribuição dos endereços é feita pela Internet Corporation for Assigned Names and Numbers (ICANN). Ela libera endereços para autoridades regionais que os atribuem a provedores, empresas e outras instituições. No Brasil, estas funções foram delegadas ao Registro Nacional (http://registro.br), sediado na FAPESP (SP), comandado pelo Comitê Gestor Internet BR (CGI-Br) (www.cgi.br).

Os endereços são organizados em 5 classes (A, B, C, D e E) e descritos em 4bytes separados por pontos, em notação decimal: 200.137.44.25. Cada campo varia de 000 a 255.

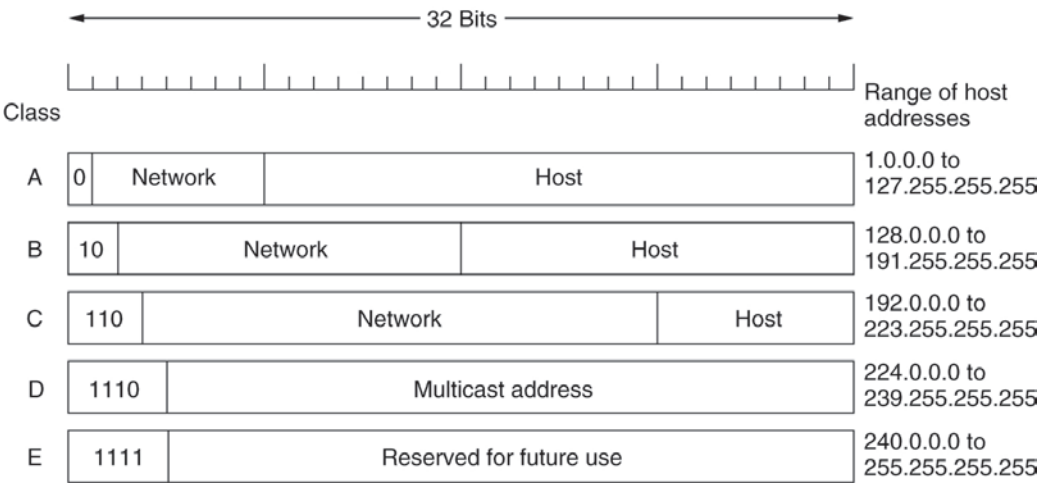


Figura 23. Formato dos endereços IP.

Alguns endereços têm significado especial, conforme apresentado na figura:

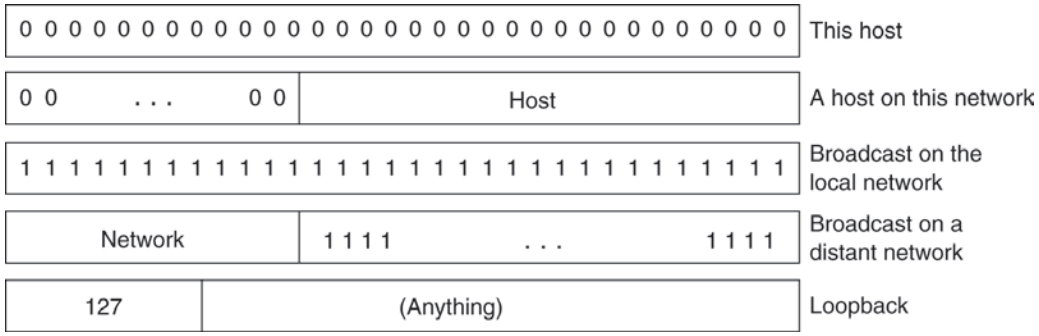


Figura 24. Endereços IP especiais.

Um endereço IP consiste em 32bits, divididos em dois campos:

- Número de rede (network number);
- Número do *host* (host number).

Ou três campos (*subneting* ou sub-redes):

- Número de rede (network number);
- Número de sub-rede (subnet number);
- Número de *host* (host number).

Os endereços IP são escritos em notação decimal:

xxx . yyy . zzz . kkk
223 . 1 . 1 . 1
11011111 00000001 00000001 00000001

O grupo decimal (entre os pontos decimais) é conhecido como um **octeto**, ou seja, o **decimal** equivalente aos **8bits** do endereço binário. Desta forma, o endereço IP é um endereço de 4 octetos (4 grupos de 8bits). Exemplos:

- 68.18.1.36 a o número decimal 68 representa o campo de rede do endereço;
- 137.4.80.1 a o número decimal 137.4 representa o campo de rede do endereço.

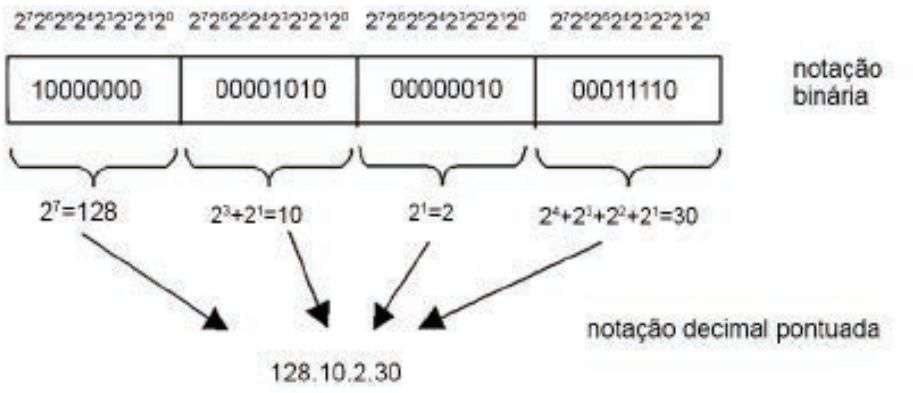


Figura 25. Conversão entre notações de um endereço IP.

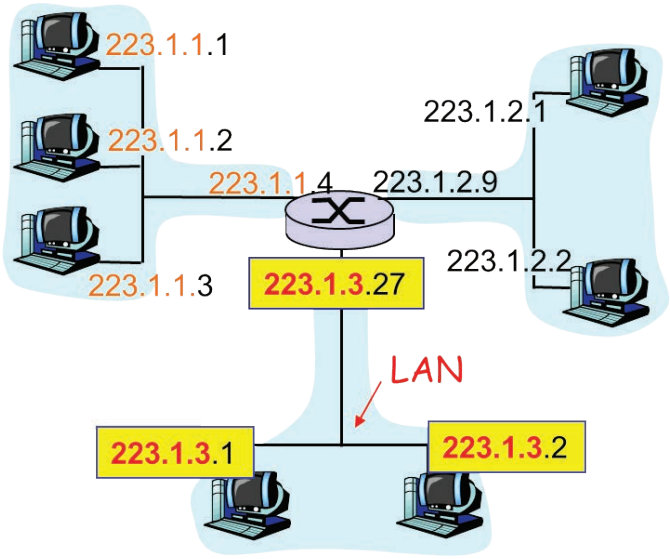


Figura 26. Endereçamento IP.

A rede da figura 26 consiste em 3 redes IP: 223.1.1.X; 223.1.2.X e 223.1.3.X. Os primeiros 24bits são a parte de rede e os demais representam o endereço dos *host*.

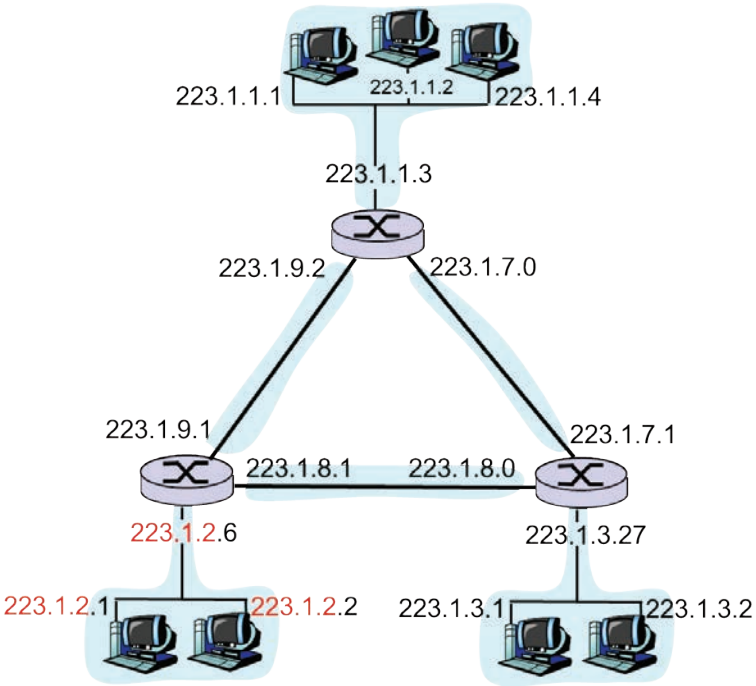


Figura 27. Identificação das redes.

Como achar as redes? Por dissociação de cada interface de seu roteador ou estação e pela criação de ilhas de redes isoladas. Uma rede (com uma classe de endereços) pode ser subdividida em sub-redes internamente.

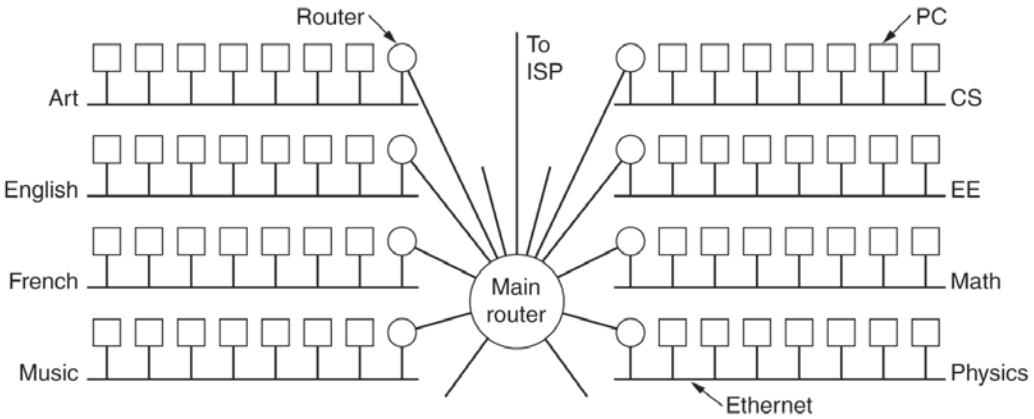


Figura 28. Uma rede de um campus consistindo de LAN para vários departamentos.

Alocando alguns bits da parte de endereço de *host*, pode-se identificar cada sub-rede. Quando um pacote chega ao roteador principal, pode determinar a qual sub-rede o pacote pertence por meio de uma operação "ou" (*booleana or*) com uma máscara de sub-redes (por exemplo, uma máscara 255.255.252.0), indicando a sub-rede e o *host* nessa sub-rede. Usando 6bits para sub-redes e 10bits para estações, tem-se até 64 sub-redes com até 1022 *hosts* para um endereço de classe B.

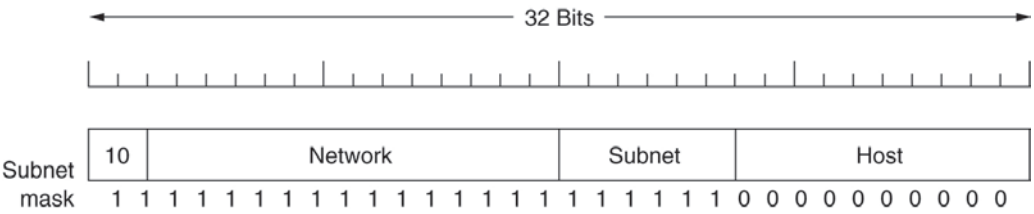


Figura 29. Uma rede da classe B organizada em 64 sub-redes.

Devido à organização em classes, se por um lado ficou fácil organizar os domínios na *internet*, por outro, essa associação deixa muitos endereços sem atribuição, fazendo a *internet* parecer um grande queijo suíço, cheio de buracos. Por exemplo, uma rede LAN que recebe uma classe C pode conectar até 256 máquinas, mas pode ter apenas duas ou três, retendo os demais endereços na classe (que identifica a rede). Isso provoca uma grande falta de endereços na *internet*.

Dentre as alternativas para contornar este problema, a Classless Inter-Domain Routing (CIDR) ou Roteamento entre Domínios sem atribuição de Classe (RFC 1519) aloca os endereços IP restantes em blocos de tamanhos variáveis, desconsiderando a organização em classes. Se, por exemplo, um *site* necessita de 2000 endereços, ele receberá 2048 (múltiplos de 8). Entretanto, isso complica o sistema de roteamento, pois foge do mecanismo rede/*host*. Nesse caso, a tabela de roteamento terá, agora, que conter todas as 2048 entradas.

University	First address	Last address	How many	Written as
Cambridge	194.24.0.0	194.24.7.255	2048	194.24.0.0/21
Edinburgh	194.24.8.0	194.24.11.255	1024	194.24.8.0/22
(Available)	194.24.12.0	194.24.15.255	1024	194.24.12/22
Oxford	194.24.16.0	194.24.31.255	4096	194.24.16.0/20

Figura 30. Tabela de atribuição de endereços IP com CIDR.

O Internet Control Message Protocol (ICMP) é um protocolo de controle da troca de datagramas na *internet*. Além do protocolo IP, outros protocolos de controle existem na *internet* (ICMP, ARP, RARP, BOOTP e DHCP) para auxiliar o seu funcionamento. Usado para teste e controle da *internet*, o ICMP possui uma dezena de tipos de pacotes usados para este fim.

Message type	Description
Destination unreachable	Packet could not be delivered
Time exceeded	Time to live field hit 0
Parameter problem	Invalid header field
Source quench	Choke packet
Redirect	Teach a router about geography
Echo request	Ask a machine if it is alive
Echo reply	Yes, I am alive
Timestamp request	Same as Echo request, but with timestamp
Timestamp reply	Same as Echo reply, but with timestamp

Figura 31. Principais tipos de mensagens ICMP.

O Address Resolution Protocol (ARP) é um protocolo que tem a função de mapear um endereço IP no endereço de enlace correspondente. Uma vez que o datagrama (pacote) IP chega à rede de destino, é necessário mapear o endereço IP do receptor no seu endereço local de rede (endereço físico ou de enlace, pois a camada de enlace não reconhece endereços IP), para que o roteador local possa fazer a entrega. O protocolo ARP mapeia os endereços IP nos endereços físicos dos *host* locais por meio de tabelas na memória do roteador, geradas sob demanda.

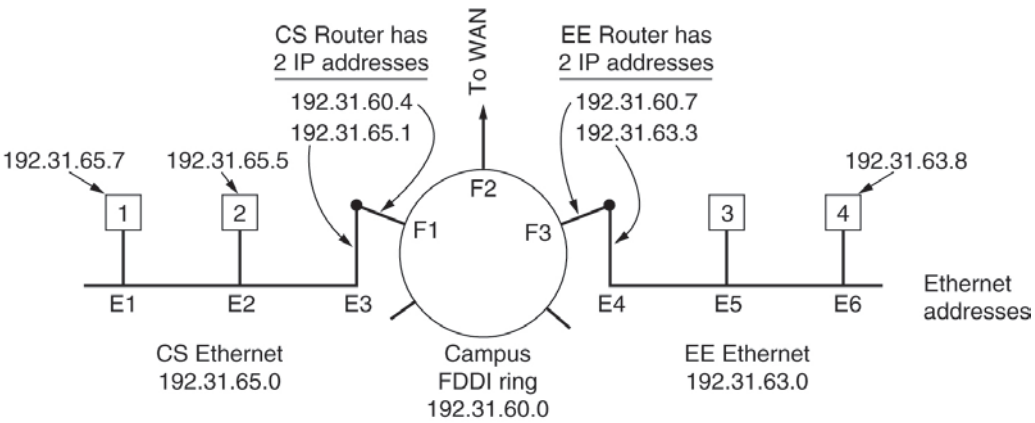


Figura 32. 3 redes/24 interconectadas: 2 Ethernet e 1 FDDI ring.

Do mesmo modo, uma estação que acorda e não sabe seu endereço IP, pode perguntar ao roteador seu endereço (que deve estar na tabela) usando o Reverse ARP (RARP), (RFC 903). Entretanto, o RARP tem o problema de necessitar de um servidor em cada segmento de rede (sub-rede da rede total), pois usa difusão limitada para descobrir o roteador.

Outras soluções derivadas foram propostas, como o BOOTP e o DHCP. O BOOTP (RFC 951, 1048, 1084) usa mensagens UDP que podem ser encaminhadas entre roteadores, demandando apenas um servidor de endereços na LAN. Entretanto, ele também traz o problema de exigir configuração manual dos endereços disponíveis.

Assim, foi proposto o Dynamic Host Configuration Protocol (DHCP) (RFC 2131, 2132). Além da atribuição manual, ele permite a atribuição dinâmica de endereços IP aos *host* da LAN. Além disso, ele pode estar fora da LAN, onde são atribuídos os endereços por meio de Agentes de Atribuição DHCP.

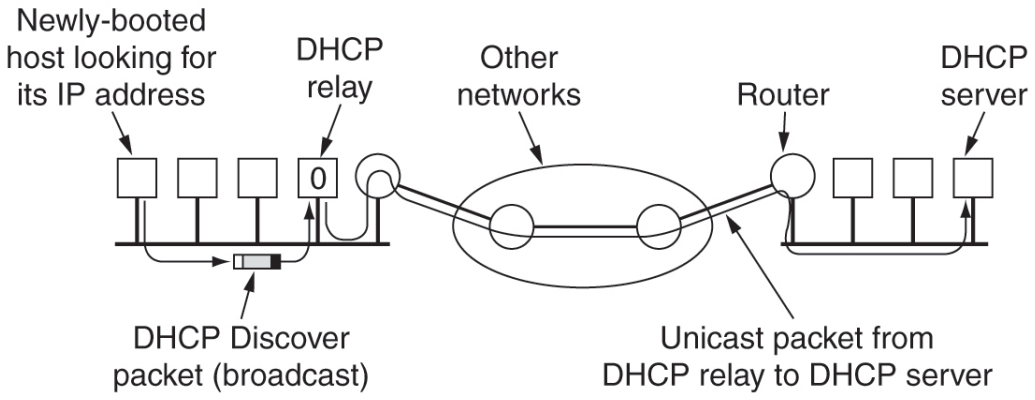


Figura 33. Funcionamento do DHCP.

3.6.1 Roteamento na *internet*:

A *internet* é formada por um número grande de sistemas autônomos (SAs). Cada SA é operado por uma organização diferente que pode usar seu próprio algoritmo de roteamento, dependente da topologia e da tecnologia de rede de cada uma. Um algoritmo de roteamento interno de um SA é dito Protocolo de Gateway Interior e um algoritmo para roteamento entre SAs de Protocolo de Gateway Exterior. Os Interior Gateway Protocols (IGP) ou protocolos de roteamento interno mais comuns são:

- Routing Information Protocol (RIP);
- Open Shortest Path First (OSPF);
- Interior Gateway Routing Protocol (IGRP): proprietário da Cisco.

3.6.1.1 Protocolo Open Shortest Path First (OSPF)/Interior Gateway Routing Protocol (IGRP)

Originalmente usava-se como protocolo de gateway interior da *internet* o Routing Internet Protocol (RIP), baseado no protocolo de vetor de distâncias, originário da ARPANet. Ele tinha problemas de escalabilidade, além do problema da contagem até o infinito, isto é, de convergência lenta. A partir de 1979, o IETF adotou o Open Shortest Path First (OSPF) (RFC 2328) que é baseado no protocolo de estado de enlace e que se tornou padrão em 1990, sendo adotado em todos os roteadores.

O OSPF funciona considerando a rede como um grafo orientado, com custos associados a cada arco, e calculando os caminhos mais curtos desse grafo usando o protocolo de Dikstra. Visando facilitar a administração de SAs grandes, o OSPF permite que eles sejam organizados em áreas numeradas. Uma área é uma rede ou um conjunto de redes contíguas que não se sobrepõem e não precisam ser completas, isto é, podem estar ligadas por roteadores intermediários. Fora de uma área, a topologia interna fica invisível. Cada SA possui uma área de *backbone* (área 0) que interliga outras áreas, hierarquicamente.

O OSPF define quatro classes de roteadores:

- Roteadores internos a uma área;
- Roteadores de borda de uma área;
- Roteadores de *backbone*;
- Roteadores de fronteira do SA.

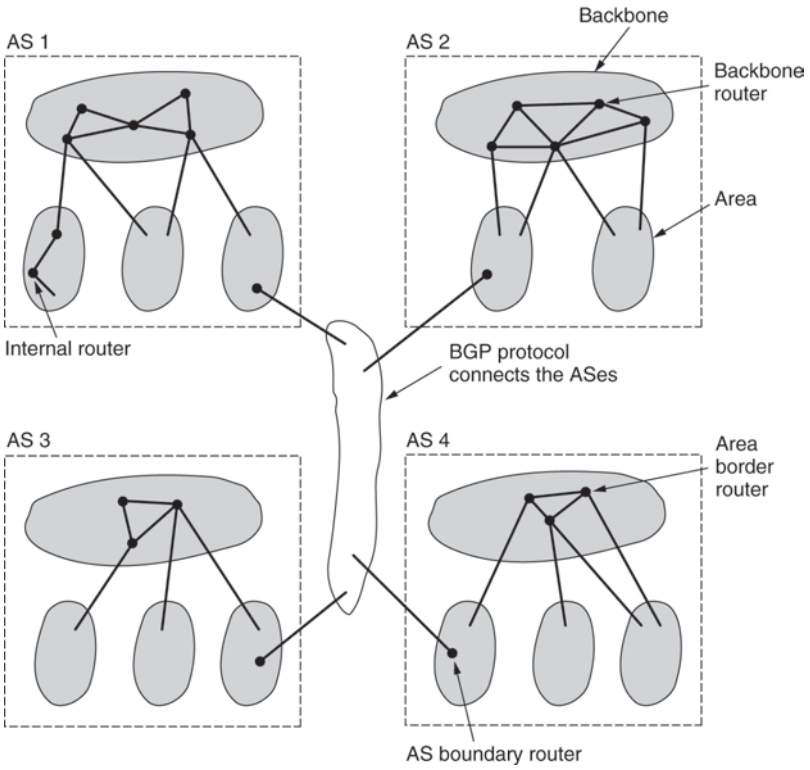


Figura 34. Relação entre ASs, *backbones* e áreas no OSPF (TANENBAUM, 2003).

Usando pacotes do tipo HELLO, um roteador descobre seus vizinhos e, com o link state update, atualiza os custos das linhas.

Message type	Description
Hello	Used to discover who the neighbors are
Link state update	Provides the sender's costs to its neighbors
Link state ack	Acknowledges link state update
Database description	Announces which updates the sender has
Link state request	Requests information from the partner

Figura 35. Tipos de mensagens do OSPF.

O *database description* permite gerenciar as atualizações dos dados e o *linkstat request* serve para receber os estados de enlace dos nodos adjacentes.

3.6.2 Protocolo Board Gateway Protocol (BGP):

É o protocolo de roteamento entre SAs e difere nos objetivos do OSPF. No BGP, há uma preocupação maior com a política de encaminhamento entre SAs. Por exemplo, políticas, economia e segurança são aspectos considerados. Podemos considerar os seguintes requisitos:

1. Nenhum tráfego externo deve passar por um dado AS;
2. Não deve ser usado como rota iniciada num SA A, certo SA B;
3. Efetuar troca de tráfego entre SAs sempre que tiverem uma conexão direta, evitando propagar tráfego desnecessário;
    - O tráfego que inicia e termina num dado SA A nunca deve passar pelo SA B.

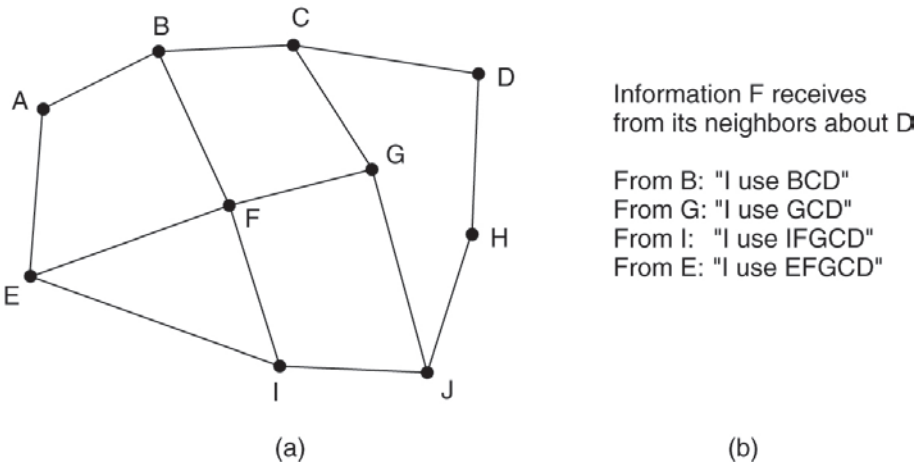


Figura 36. (a) um conjunto de roteadores BGP; (b) informação enviada a F (TANENBAUM, 2003).

O BGP, por ser um *backbone* pequeno, utiliza o protocolo RIP com certo sucesso.

3.7 Network Address Translation (NAT)

Como os endereços IP estão cada vez mais escassos, criou-se a possibilidade de, internamente a uma empresa, fazer uso de endereços fictícios. Com o NAT, um processo no roteador de saída da rede LAN da empresa traduz um endereço fictício interno para o seu próprio e encaminha o pacote com ele, registrando, em uma tabela, o endereço interno do dono daquele pacote. No retorno da mensagem para aquele *host*, o pacote vem com o endereço do NAT que, ao procurar na tabela, encaminha o pacote internamente ao destinatário. Na figura 37, a classe de endereços usada é a 10.0.0.x.

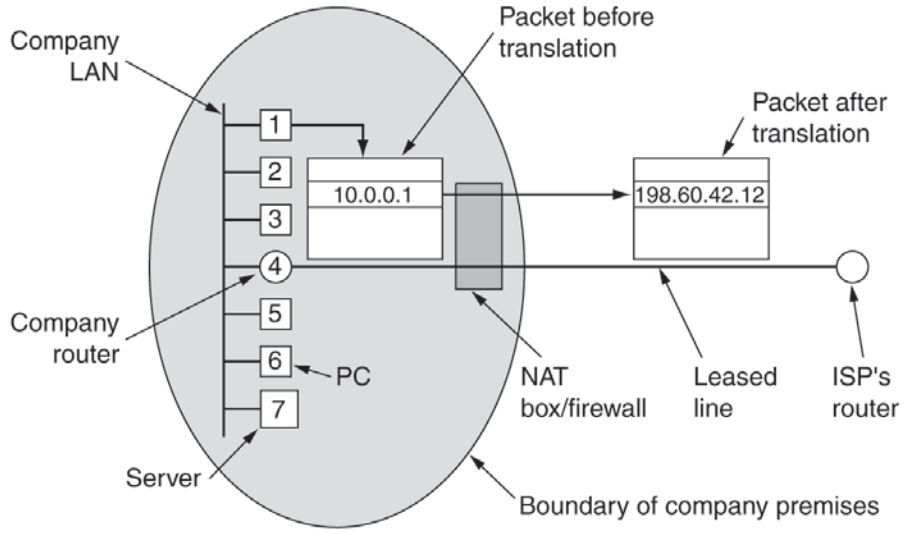


Figura 37. Implantação e operação de um NAT.

Uma maneira de implementar o NAT é usar o número de porta da camada de transporte do pacote como índice na tabela de registro do endereço interno do *host* para encaminhá-la como endereço de transporte. No retorno, o endereço de transporte do pacote serve de entrada para tabela de registros que retorna o endereço IP do emissor. O problema é que aplicações, que rodam com o acesso à porta de retorno, passadas nos dados (carga útil) não funcionam neste caso.

3.8 IPv6

IPv6 – nova versão do protocolo IP.

Com os problemas de endereços escassos, segurança e mobilidade na *internet*, em 1990 iniciou-se um estudo para a adoção de outra verão do protocolo IP. Foi a versão 6.

Os objetivos do IPv6 são:

1. Aceitar bilhões de *host* expandindo o número de bits de endereçamento;
2. Reduzir os tamanhos das tabelas de roteamento;
3. Simplificar o protocolo visando maior desempenho nos roteadores;
4. Oferecer maior segurança em termos de privacidade e autenticação;
5. Dar maior importância ao tipo de serviço (por exemplo, de tempo real);
6. Permitir multidifusão com possibilidade de definição de escopos;
7. Permitir mobilidade transparente;

8. Permitir que o protocolo possa evoluir no futuro;
9. Permitir a coexistência entre as diferentes versões do protocolo.

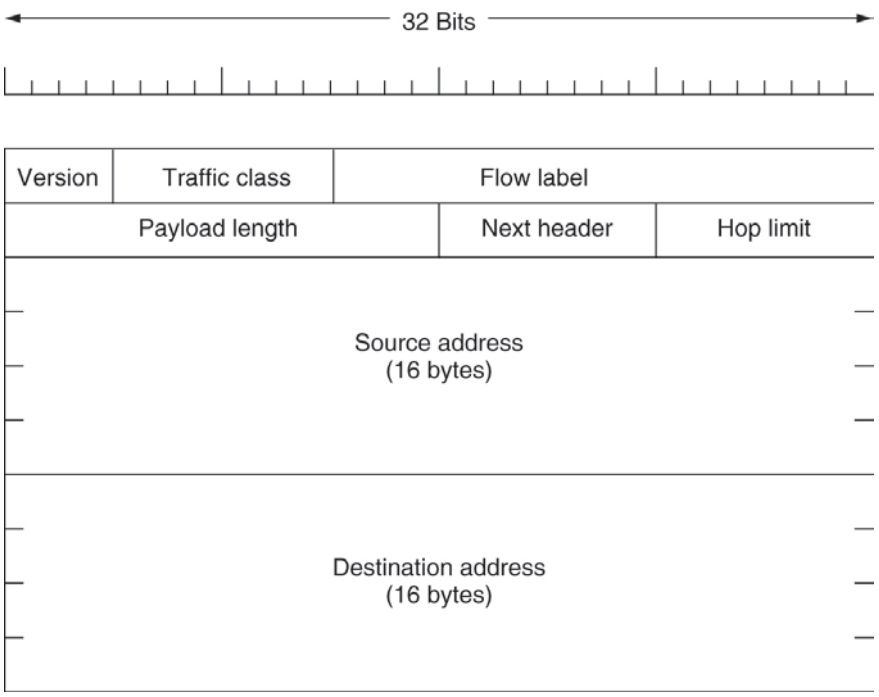


Figura 38. Cabeçalho principal do IPv6.

O cabeçalho do IPv6 é bastante mais simples que o atual (IPv4). O campo de endereço (origem e destino) tem agora 16bytes ou 128bits.

Extension header	Description
Hop-by-hop options	Miscellaneous information for routers
Destination options	Additional information for the destination
Routing	Loose list of routers to visit
Fragmentation	Management of datagram fragments
Authentication	Verification of the sender's identity
Encrypted security payload	Information about the encrypted contents

Figura 39. Cabeçalho de extensão do IPv6.

Cabeçalhos de extensão permitem especificar características adicionais e específicas do pacote.

Next header	0	194	4
Jumbo payload length			

Figura 40. Cabeçalho de extensão para datagramas grandes (*jumbograms*).

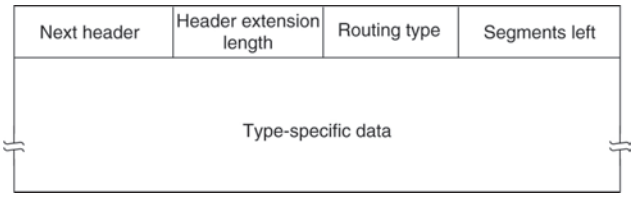


Figura 41. Cabeçalho de extensão para roteamento.

Existem, inclusive, extensões para roteamento.

3.9 Controle de congestionamento em redes e qualidade de serviço (QoS)

Devido às limitações físicas de capacidade dos meios (largura de banda), número e configuração de roteadores (por exemplo, memória), e de topologia (estrutura de interconexão), as redes possuem uma capacidade calculada de tráfego simultâneo de pacotes. É possível dimensionar a capacidade das redes baseada em modelos estatísticos. A inserção de pacotes, além da capacidade da rede ou de seus dispositivos, provoca a queda do desempenho local e global da rede, levando a uma situação de congestionamento dos *links* e consequente travamento.

Quando o tráfego de mensagens gerado pelas conexões está dentro dos limites de capacidade das linhas e dos roteadores, todos os pacotes são entregues (considerando-se as possibilidades de retransmissões devido aos possíveis erros). À medida que o número de pacotes cresce, os atrasos devidos ao enfileiramento também crescem proporcionalmente, até o limite de capacidade da rede. O ideal é trabalharmos sempre dentro da curva de capacidade. Ao ultrapassarmos este limite, inicia um processo de crescimento das filas até a situação de travamento por congestionamento.

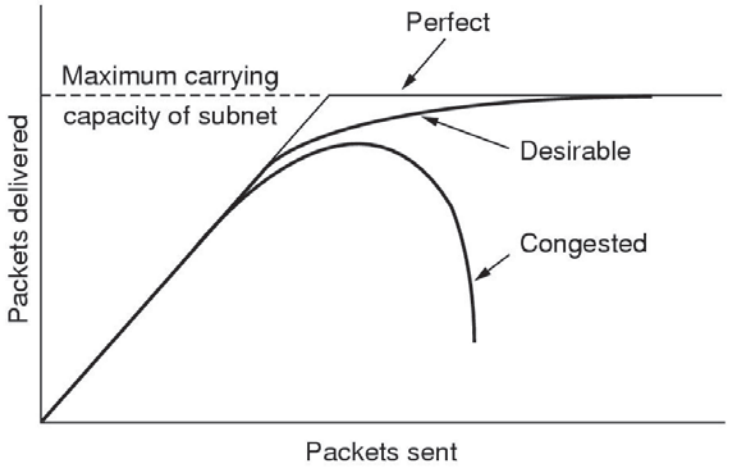


Figura 42. Níveis de tráfego e geração de congestionamento.

Na prática, o congestionamento pode ser causado por diversos fatores:

- Se diversos fluxos, num dado instante, chegarem a um mesmo roteador e precisarem compartilhar uma mesma linha de saída, isto poderá provocar a saturação das filas do roteador se a linha não tiver LB suficiente para acomodar todo o fluxo. A fila deverá crescer ao ponto de perder pacotes por falta de espaço em memória para recebê-los. O aumento de memória ajuda até certo limite. De acordo com Nagle (1987), o aumento da capacidade de memória dos roteadores pode levar a um problema de, se a fila for muito longa, os *timeouts* provocarem retransmissões e mais carga no sistema, piorando ainda mais o desempenho.

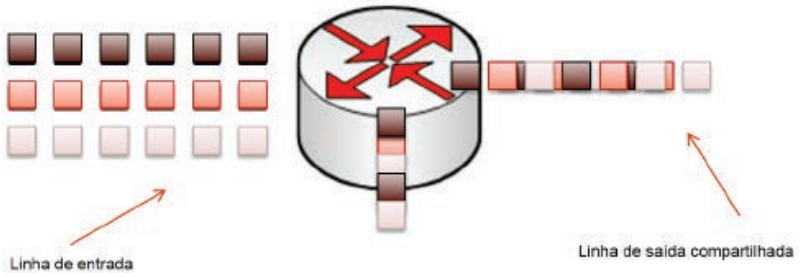


Figura 43. Controle de congestionamento.

- Processadores lentos nos roteadores podem contribuir para uma baixa vazão e gerar o mesmo problema para pacotes enfileirados por muito tempo;
- Baixa LB das linhas também contribui para o atraso.

Atualizações parciais (das linhas ou então dos roteadores) acabam por transferir o local de ocorrência de gargalos e não resolve o problema. É importante que o sistema esteja equilibrado entre as linhas e os dispositivos de roteamento. A engenharia de tráfego de redes busca manter este equilíbrio no sistema.

Existe outro aspecto da transferência de pacotes que se confunde com congestionamento que é o controle de fluxo. Este é decorrente do desbalanceamento entre a fonte e o destinatário. Um emissor com maior capacidade que o receptor acaba por saturar sua capacidade de reter pacotes, gerando filas, esgotamento de memória e propagação deste processo nos roteadores, os quais acabam tendo que retransmitir seus pacotes, levando à situação de congestionamento da mesma forma.

O controle de fluxo recebe o *feedback* do receptor e gerencia a criação de pacotes na origem, baseando-se nestas informações de retorno.

3.9.1 Princípios gerais do controle de congestionamento:

Usando uma abordagem da teoria de controle, podemos dividir o problema do controle de congestionamento em dois grupos:

- *Loops* abertos e
- *Loops* fechados.

Em *loops* abertos, a ideia é tentar resolver o problema com um bom projeto (dimensionamento) e garantir que o problema não ocorra. Uma vez posto em operação, o sistema não sofre correções. Ferramentas de controle, neste caso usadas para decidir sobre admissão de mais tráfego, descarte de pacotes e/ou momentos de entrada em ação, não consideram o estado corrente da rede, mas sim algum algoritmo previamente estabelecido, baseado em algum dado histórico e estatístico.

Em *loops* fechados, a ideia é usar um mecanismo de realimentação (*feedback*) que informa o andamento do sistema e que permite ajustá-lo. Consiste então em três passos:

1. Monitoramento para detecção de ocorrência (ou tendência) de congestionamento. Verificar o espaço em *buffer*, média do comprimento da fila, média do retardo na rede etc. para identificar quando e onde ocorre congestionamento;
2. Envio de informações aos pontos de congestionamento para a tomada de decisão e desenvolvimento de ações de correção;
3. Ajuste da operação do sistema para correção do problema.

Dentre os aspectos considerados para o monitoramento, destacam-se o percentual de descarte de pacotes devido à falta de *buffers*, dos comprimentos médios de filas, à quantidade de retransmissões por estouro de tempo de vida de pacotes e ao atraso médio de pacotes, assim como seu desvio padrão. Claro que, se são crescentes, esses valores indicam a convergência deste sistema para uma condição de congestionamento.

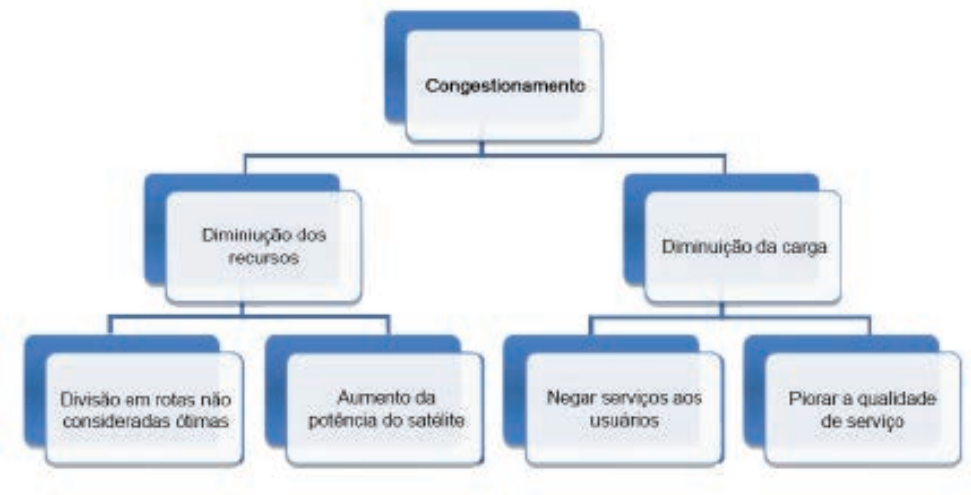


Figura 44. Princípios gerais para o controle de congestionamento.

Dentre as possibilidades estão: a redução dos recursos disponíveis ao usuário pela divisão da carga por rotas não ótimas ou o aumento de recursos, como o crescimento da potência do satélite, por exemplo; a redução da carga pela negação de determinado serviço ao usuário, ou mesmo a redução da QoS, por exemplo, pela redução da janela de pacotes em transferência. Existem opções de monitoramento local dos roteadores e informação periódica. O período não pode ser longo pela possibilidade da correção se tornar inviável.

3.9.2 Políticas de prevenção:

Para sistemas de *loop* aberto, preventivos por natureza, desenvolvem-se políticas que podem garantir o não congestionamento. Tais políticas estão nas três camadas: enlace, rede e transporte e podem afetar o sistema.

Tabela 2. Políticas de prevenção de congestionamento

Camadas	Políticas
Transporte	Política de retransmissão; Política de cache fora de ordem; Política de confirmação; Política de controle de fluxo; Determinação de *timeout.*
Rede	Circuitos virtuais em comparação com datagramas dentro da sub-rede; Política de serviço e de enfileiramento de pacotes; Política de descarte de pacotes; Algoritmos de roteamento; Gerenciamento do tempo de vida do pacote.

Tabela 2. *Continuação...*

Camadas	Políticas
Enlace de dados	Política de retransmissão; Política de cache fora de ordem; Política de confirmação; Política de controle de fluxo.

Nas sub-redes de circuitos virtuais podemos controlar dinamicamente o congestionamento com ações específicas:

1. Controle de admissão: impede a criação de novo circuito virtual até que o congestionamento esteja resolvido. Consiste em desabilitar a camada de transporte e iniciar novas conexões (é semelhante a suspender o sinal de discagem nas comutadoras telefônicas). O controle de admissão impede o aumento do congestionamento;
2. Permitir que novos circuitos sejam criados apenas pelas rotas não problemáticas;
3. Negociação de um acordo entre o *host* e a sub-rede (roteadores) que definam a reserva de recursos previamente. Embora seja simples, tende a desperdiçar recursos pela alocação prévia desnecessária ou acima da necessária.

Nas sub-redes de datagramas, as estratégias mais conhecidas são as do bit de advertência e a de pacotes reguladores.

Cada roteador tem a capacidade de monitorar o uso de suas linhas de comunicação e outros recursos, tais como espaço de memória para mensagens e filas, que podem, por exemplo, associar uma variável real digamos *u,* de utilização de um dado recurso, a cada recurso disponível. Ela recebe valores entre 0.0 e 1.0, refletindo sua taxa de utilização a cada momento. Uma expressão de *u* em função do tempo pode ser a seguinte:

$$u_{nova} = ku_{antiga} + (1-k)f$$

Onde f (0, 1) é uma função de medição da utilização de recurso no intervalo de atualização e a constante *k* indica a velocidade com que o roteador atualiza suas informações. Sempre que a taxa de uso atingir certo limite, a linha de saída entra em modo de advertência. O sistema verifica, para cada pacote, a utilização de sua linha de saída e toma uma das ações que veremos a seguir.

3.9.3 Bit de advertência:

Usado em redes como a DECNET e a FRAME-RELAY. O estado de advertência é assinalado por qualquer roteador do caminho, ativando um bit de advertência no pacote. A entidade destino repassa esse bit à origem por meio de confirmação e esta interrompe o envio de pacotes até receber uma confirmação sem o bit ativado. Isso permite calcular a fração de sobrecarga a reduzir ou a aumentar na taxa de envio, visando ajustar o tráfego.

3.9.4 Pacotes reguladores:

Um roteador envia um pacote regulador de tráfego diretamente ao nodo de origem, informando sua condição de advertência. O pacote originário desse pacote regulador é marcado para não gerar novos reguladores à frente. O *host* de origem toma a mesma ação do bit de advertência, reduzindo a entrada de tráfego por um percentual de X% durante um intervalo fixo *t* ms. Outros pacotes reguladores para o mesmo destino nesse período serão ignorados. Após esse tempo, ele reinicia um novo período, transmitindo em condição normal. Caso tenha recebido mais pacotes reguladores no período, reduzirá novamente o fluxo em X%.

O valor X de redução é função de vários estudos e propostas. Por exemplo, pode ser 25% e pode ser 1 segundo. O mecanismo de implementação é o tamanho da janela de transmissão.

3.9.5 Pacotes reguladores HOP-a-HOP:

Em redes de alta velocidade ou muito longas, esses esquemas anteriores não funcionam muito bem dado o tamanho dos intervalos envolvidos, o que pode levar a rede ao travamento. A opção, neste caso, é fazer com que o pacote regulador atue sobre cada *hop* por onde passa sua viagem até a origem. Cada roteador anterior reduz seu fluxo, retendo pacotes para envio e aliviando o roteador da frente até que o congestionamento se normalize. Isso dá alívio em cadeia ao problema, embora consuma mais *buffers*.

3.9.6 Escoamento de carga:

É uma abordagem mais agressiva, para o caso de não conseguir resolver o problema de congestionamento. Consiste em descartar pacotes deliberadamente. O roteador pode adotar diversas estratégias para isso, desde

a aleatória até aquelas onde há análise das aplicações sendo trafegadas. Por exemplo, aplicações multimídia podem perder pacotes mais antigos em detrimento de novos.

Para viabilizar estas estratégias, as aplicações devem poder marcar seus pacotes com um indicador de importância do tipo: NUNCA DESCARTAR, DESCARTÁVEL etc. Outras estratégias dizem respeito ao uso da LB do circuito, podendo aumentar além do negociado, desde que haja folga ou seja reduzida se houver congestionamento (Frame-relay, ADSL etc.).

3.9.7 Detecção aleatória prematura:

Trata-se de uma estratégia que busca atuar logo no início, detectando a convergência para o congestionamento antes de ele estar formado. O algoritmo Random Early Detection (RED) 1993, parte da ideia de que se há uma tendência de crescimento das filas e, para isso, é melhor reduzir a velocidade antes de congestionar. Consiste em manter o tamanho médio histórico das filas e tomar ações sempre que ele for excedido. A ação mais apropriada é o descarte aleatório de um pacote que deverá ser retransmitido posteriormente, desacelerando o fluxo e mantendo a rede estável. A origem que teve seu pacote descartado pode ainda reduzir seu fluxo, contribuindo com a convergência à estabilidade e retornando após um tempo se não houver mais descartes. Note que, por ser aleatória, a fonte geradora de congestionamento pode demorar ou nunca ser penalizada.

Esta estratégia não funciona em redes *wireless*, pois nelas a maior causa de perdas de pacotes é o ruído do meio e não o congestionamento.

3.9.8 Controle de flutuação (Jitter):

Aplicações do tipo de envio de áudio e vídeo não se importam muito se o tempo de transmissão é relativamente longo, desde que mantenha uma taxa constante (por exemplo, 30 quadros por segundo). A variação nos tempos de chegada dos pacotes (desvio-padrão) é dita flutuação (ou jitter). Se o jitter for muito grande, haverá ruído no áudio ou na exibição de um vídeo.

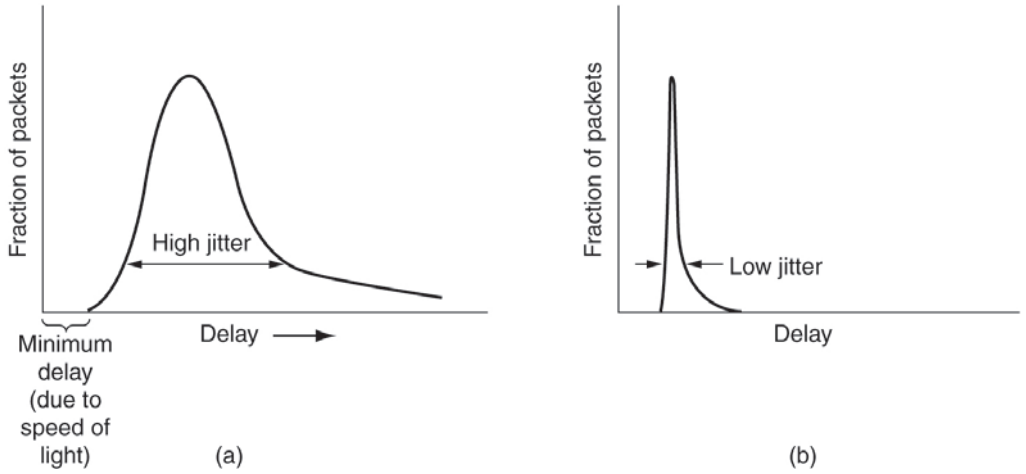


Figura 45. (a) jitter alta; (b) jitter baixa.

A flutuação é calculada pelo número de *hops*, pela LB disponível e pela latência do meio usado. Isso resulta numa média negociada no estabelecimento da conexão. O algoritmo de roteamento pode decidir acelerar, colocando na frente das filas, pacotes mais atrasados em detrimento dos mais recentes, que estejam antecipados no tempo médio de envio, como forma de reduzir o *jitter*.

A moldagem de fluxo é mais efetiva quando o transmissor, o receptor e a sub-rede concordam em relação a ela. Esse acordo é chamado de especificação de fluxo.

Tabela 3. Exemplo de especificação de fluxo

Características de entrada	Serviço desejado
Tamanho máximo do pacote (bytes)	Sensibilidade a perdas (bytes)
Taxa do balde de *tokens* (bytes)	Intervalo de perda (microssegundos)
Tamanho do balde de *tokens* (bytes)	Sensibilidade a perdas em rajadas (pacotes)
Taxa máxima de transmissão	Retardo mínimo percebido (microssegundos)
	Variação de retardo máximo (microssegundos)
	Garantia de qualidade

Uma maneira encontrada nas aplicações, principalmente nas de vídeo sob demanda, é a utilização de *buffers* reguladores de *jitter*. O número de *buffers* pré-alocados é calculado com base na flutuação média do caminho. No entanto, aplicações interativas como VoIP, videoconferência etc. não permitem essa abordagem e dependem da qualidade da rede.

3.9.9 Qualidade de serviço (QoS):

As estratégias analisadas até agora tratam da questão de controle de congestionamento das redes de transporte de dados para as aplicações. Porém,

com a evolução e o uso das redes para tráfego multimídia, outras medidas têm sido propostas.

Quando falamos na qualidade do serviço que a rede proporciona, estamos falando de requisitos para uma boa QoS. Um fluxo é uma sequência de pacotes entre uma origem e um destino. Numa rede orientada a conexão, o fluxo é único, pois todos os pacotes seguem a mesma rota ao passo que numa rede de datagramas cada pacote segue seu caminho independentemente. Os requisitos de qualidade de cada fluxo dependem de parâmetros, tais como: confiabilidade, atraso (latência), flutuação e LB. Juntos, estes parâmetros definem o conceito de QoS.

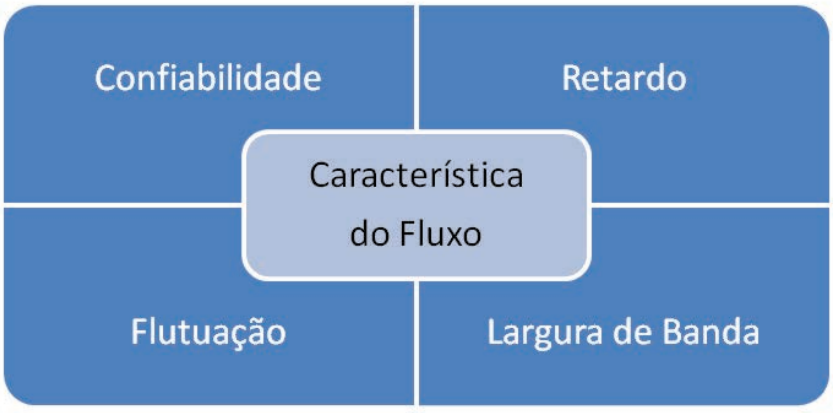


Figura 46. Requisitos de QoS.

Diversas aplicações têm seus requisitos diferentes, dependendo de suas características. A figura abaixo mostra um exemplo:

Tabela 4. Exemplos de requisitos de QoS

Aplicação	Confiabilidade	Retardo	Flutuação	Largura de banda
Correio Eletrônico	Alta	Baixa	Baixa	Baixa
Transferência de arquivos	Alta	Baixa	Baixa	Média
Telefonia	Baixa	Alta	Alta	Baixa
Videoconferência	Baixa	Alta	Alta	Alta

Como não existe uma fórmula específica ou única para QoS, várias propostas foram apresentadas. Vejamos algumas técnicas para se alcançar QoS:

- Superdimensionamento;
- Armazenamento em *buffers*;
- Moldagem de tráfego;
- Algoritmo do balde furado;

- Algoritmos do balde de símbolos;
- Reserva de recursos;
- Controle de admissão;
- Roteamento proporcional;
- Programação de pacotes.

O superdimensionamento propõe oferecer condições tão amplas de recursos nos roteadores que não haveria problemas de desempenho, congestionamento etc. Com isso, aumentamos a capacidade da rede. A dificuldade aqui está no custo. Uma rede superdimensionada é muito mais cara.

No armazenamento em *buffers,* os fluxos podem ser armazenados nos receptores antes de serem entregues à aplicação. Isso não afeta a confiabilidade ou a LB, apenas aumenta o atraso, mas por outro lado, suaviza a flutuação. Na figura 47 tem-se um exemplo de pré-alocação de *buffers*. Um intervalo de envio de pacotes garante o preenchimento desses *buffers* e, após um intervalo (t = 10), iniciam sua reprodução. Nesse momento já se tem certo número (6) de pacotes nos *buffers* que podem, então, ser usados como reguladores da flutuação.

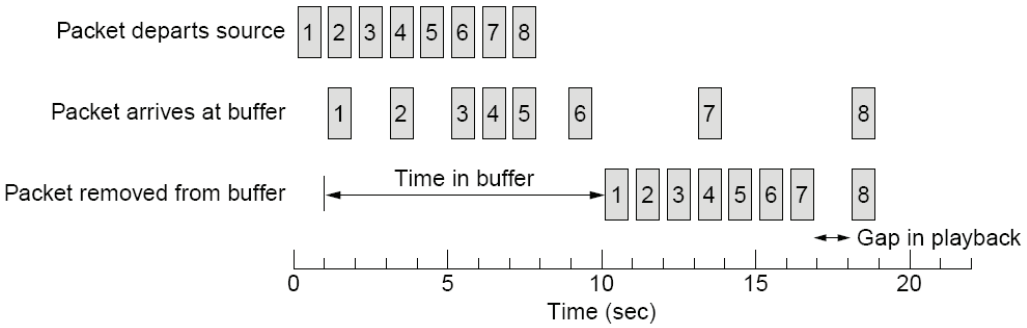


Figura 47. Armazenamento em *buffer*.

Na moldagem de tráfego é tratado sobre o uso estatístico dos parâmetros, isto é, regulando a taxa média de envio (volume) de pacotes e podendo determinar níveis de serviço a serem negociados na rede. Os Service Level Agreements (SLAs), ou acordo de nível de serviço, são contratos de prestação de serviço que definem para o cliente o quanto de recursos ele terá para a transmissão de seus dados. As concessionárias fazem esses contratos, inclusive como forma de tarifar os usuários pelo uso. Isso permite dimensionar os serviços de acordo com a capacidade da rede, reduzindo o congestionamento. A partir desse contrato, cabe à concessionária monitorar o cumprimento do SLA contratado. Este monitoramento é conhecido como policiamento de tráfego.

Uma das principais causas de congestionamento é o tráfego em rajadas.

Se *hosts* transmitissem em taxas constantes seria ideal. A ideia da moldagem de tráfego é forçar a transmissão dos pacotes em uma taxa mais previsível por meio do estabelecimento de um "acordo" de nível de serviço entre o cliente e a concessionária sobre o padrão de transmissão.

O algoritmo do balde furado (1986) usa o princípio da disciplina de tráfego, independente de sua geração, pela autorização segundo uma dada taxa a rede. Funciona como mostrada na figura 48, onde um furo no fundo do balde permite apenas um fluxo fixo, independente da taxa de entrada. O excesso de pacotes implicará no descarte logo na saída.

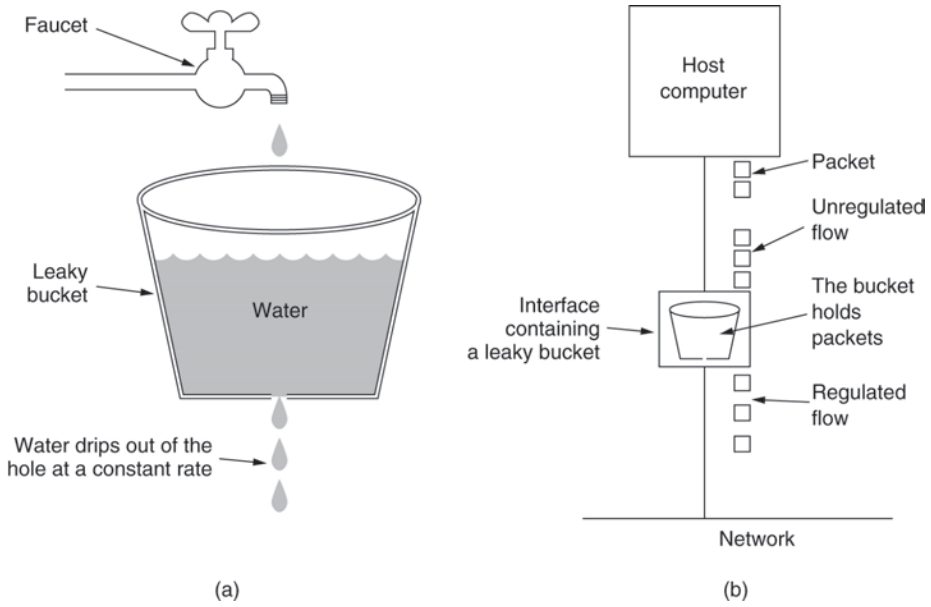


Figura 48. (a) algoritmo do balde furado com água; (b) algoritmo do balde furado com pacotes.

Neste sistema de enfileiramento com um único servidor e com o tempo de serviço constante, o computador pode inserir na rede um pacote a cada *clock*, que passa a ser um fluxo regular de pacotes. Essa técnica suaviza as rajadas e reduz a possibilidade de congestionamento. Cada *host* tem seu balde (fila interna) e um SLA associado. Se um pacote chegar e encontrar a fila cheia, será descartado. Caso contrário, aguardará sua vez na fila que obedece a uma vazão fixa.

O algoritmo do balde furado acabou sendo substituído pelo algoritmo do balde de símbolos (*token bucket*) na medida em que associa, aos fluxos, um conjunto de símbolos ou fichas (*token*). Tais símbolos são gerados por um relógio, num intervalo de um símbolo, a cada Δt segundos, de forma a permitir que o emissor envie seus pacotes até a esse limite. Para ser transmitido, um pacote deve obter um símbolo que é destruído com sua transmissão. A taxa de geração de símbolos, ao contrário do balde furado, pode variar, dependendo da ociosidade da rede.

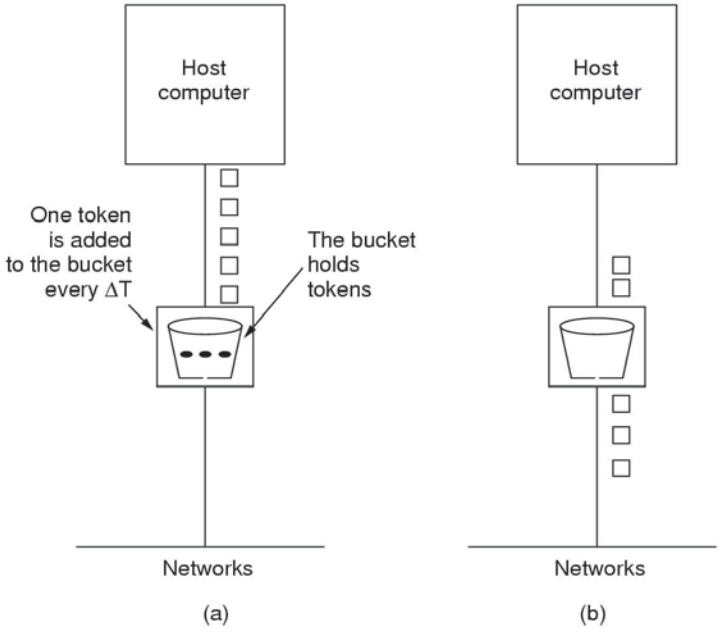


Figura 49. Algoritmo do balde de *tokens* (TANENBAUM, 2003).

Tabela 5. Comparativo entre algoritmo do balde furado e algoritmo do balde de *tokens*

Algoritmo balde furado	Algoritmo do balde de *tokens*
Não deixa que os *hosts* inativos poupem permissões para enviar rajadas maiores	Economiza até um tamanho máximo do balde
Descarta pacotes	Descarta *tokens*, mas nunca descarta pacotes
Quando o tamanho dos pacotes é variável a opção é permitir um número fixo de bytes por pulso	Variante: cada *token* representa o direito de enviar “k” bytes (pode ser mais de um pacote)

Basicamente, o balde de *tokens* permite rajadas até um certo comprimento máximo controlado. O problema deste algoritmo é que ele permite grandes rajadas. Para um tráfego mais suave, é possível inserir um balde furado original depois de um balde de *tokens*.

A reserva de recursos parte do pressuposto de que com uma rota específica, onde todos os pacotes de um fluxo seguem a mesma rota, é possível reservar recursos ao longo da mesma para garantir que a capacidade necessária esteja disponível. Existem três tipos de recursos que podem ser reservados:

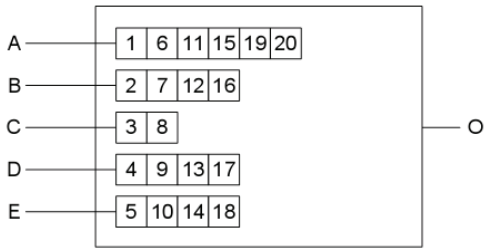
- Largura de banda;
- Espaço de *buffer*: alguns *buffers* podem ser reservados para um fluxo específico;
- Ciclos de CPU: até com cargas ligeiramente baixas, podem acontecer retardos e atrasos.

No controle de admissão, a decisão de aceitar ou não os fluxos não é trivial. Algumas aplicações são muito mais tolerantes à perda ocasional de um prazo que outras e algumas podem negociar parâmetros de fluxo e outras não. Se vários participantes estão envolvidos na negociação de fluxos, estes devem ser descritos com precisão em termos de parâmetros específicos que podem ser negociados.

Parameter	Unit
Token bucket rate	Bytes/sec
Token bucket size	Bytes
Peak data rate	Bytes/sec
Minimum packet size	Bytes
Maximum packet size	Bytes

Figura 50. Exemplo de especificação de *tokens* por fluxo no controle de admissão.

Na programação de pacotes, as filas estão separadas em linhas de saída, uma para cada fluxo. Quando a linha fica ociosa, o roteador varre as filas em rodízio, tomando o primeiro pacote da fila seguinte. O seu maior problema é o favorecimento de *hots* que utilizam pacotes grandes. Uma solução possível é o rodízio byte a byte.



Packet	Finishing time
C	8
B	16
D	17
E	18
A	20

Figura 51. Programação de pacotes.

Na figura 52, temos um roteador com cinco pacotes enfileirados para a saída O. Nas colunas à direita, temos os cinco pacotes e o tempo de término deles.

Quanto aos serviços integrados, o IETF dedicou um grande esforço na criação de uma arquitetura para multimídia de fluxo. Esse trabalho resultou em mais de duas dezenas de RFC. O nome genérico desse trabalho é algoritmos baseados no fluxo, ou serviços integrados, e tem como objetivo aplicações unidifusão e multidifusão.

3.9.10 Resource reSerVation Protocol (RSVP):

Este protocolo permite que diversos emissores transmitam para vários grupos de receptores. O RSVP possibilita que receptores individuais mudem livremente de canal e otimiza o uso da largura de banda enquanto elimina o congestionamento. O protocolo utiliza roteamento *multicast* com *spanning tree* (árvore de amplitude). Cada grupo deve receber um endereço próprio.

Para melhorar a recepção, uma reserva é solicitada pelo transmissor. O pedido é passado em cada *hop* que reserva a banda necessária e, se essa largura de banda não for disponibilizada, ele reporta à falha, fazendo com que a reserva seja feita em toda a *spanning tree*.

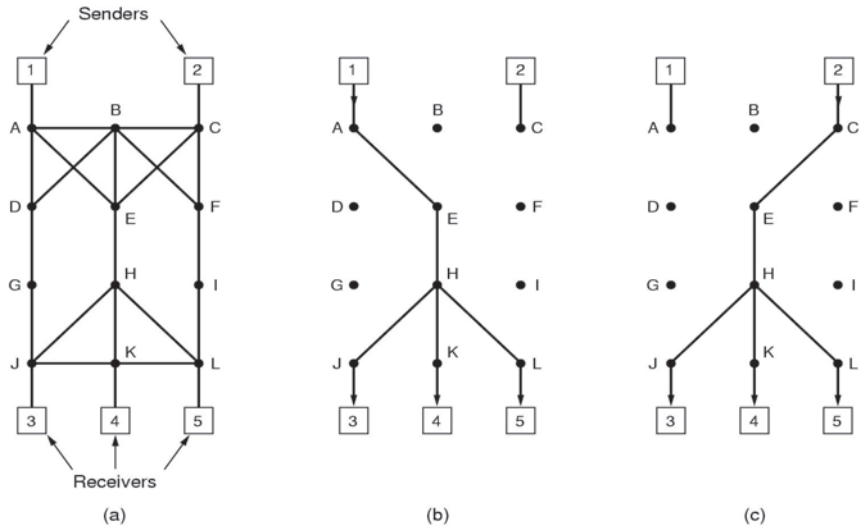


Figura 52. Protocolo RSVP.

Para obter uma melhor recepção e eliminar o congestionamento, qualquer receptor de um grupo pode enviar uma mensagem de reserva para o transmissor. A mensagem é propagada com a utilização do algoritmo de encaminhamento pelo caminho inverso.

3.10 Algoritmo de encaminhamento pelo caminho inverso

Quando um pacote de difusão chega a um roteador, este verifica se o pacote chegou pela linha que normalmente é utilizada para o envio de pacotes à origem da difusão. Caso confirme, há uma excelente possibilidade de que os pacotes de difusão tenham seguido a melhor rota e seja, portanto, a primeira cópia a chegar ao roteador. Se for esse o caso, o roteador encaminhará cópias do pacote para todas as linhas, exceto aquela pela qual ele chegou. Porém, se

o pacote tiver chegado por uma linha diferente da preferencial, ele é descartado como uma provável duplicata.

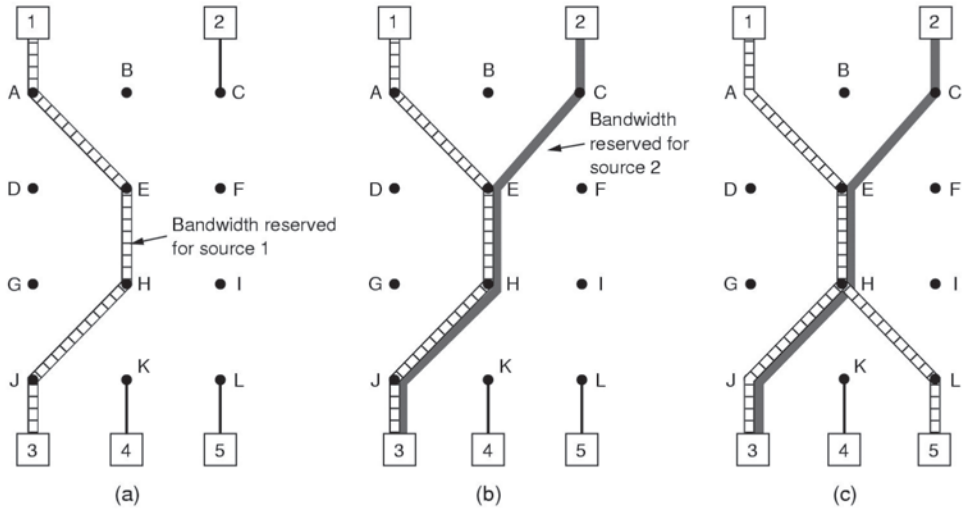


Figura 53. (a) o *host* 3 solicita um canal ao *host* 1; (b) em seguida, o *host* 3 solicita um segundo canal ao *host* 2; (c) O *host* 5 solicita um canal ao *host* 1.

3.10.1 Serviços diferenciados (SD):

Algoritmos baseados em fluxo proporcionam boa qualidade de serviço. Mas exigem configuração antecipada para cada fluxo. O estado desses fluxos é mantido nos roteadores e estes poderão falhar. Por essa razão, o IETF criou uma abordagem mais simplificada. A qualidade de serviço passou a ser baseada na classe e não mais no fluxo. Essa estratégia pode ser implementada em grande parte localmente, em cada roteador, sem configuração antecipada e sem ter de envolver todo o caminho.

Os SDs podem ser oferecidos por um conjunto de roteadores de domínio administrativo (exemplo um ISP ou uma empresa de telecomunicação). A administração define um conjunto de classes de serviço com regras de encaminhamento correspondentes e, se um cliente fizer a assinatura para SD, os pacotes do cliente que entrarem no domínio poderão incluir o campo TIPO DE SERVIÇO, sendo oferecido um serviço melhor a alguma classe.

Esse esquema não exige nenhuma configuração antecipada, nenhuma reserva de recursos e nenhuma negociação demorada de fim a fim para cada fluxo. As classes de serviços podem diferir em termos de: retardo, flutuação e probabilidade de descarte dos pacotes.

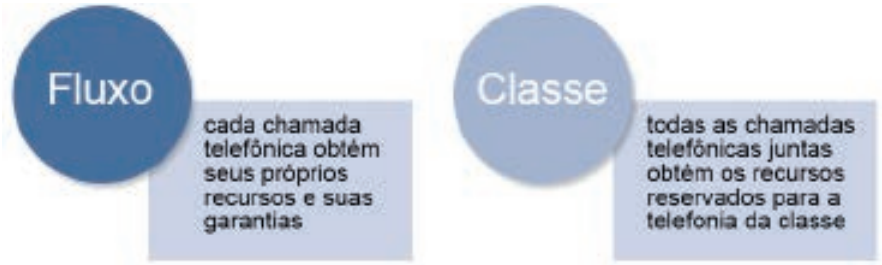


Figura 54. Fluxo *x* Classe: exemplo da telefonia na *internet.*

3.10.2 Encaminhamento garantido:

No encaminhamento garantido, temos 3 etapas principais:

- Etapa1: classificar os pacotes em uma das quatro classes de prioridade;
- Etapa 2: marcação dos pacotes de acordo com sua classe;
- Etapa 3: fazer os pacotes passarem por um filtro modelador/regulador que pode retardar ou descartar alguns deles para modelar os quatro fluxos em formas aceitáveis.

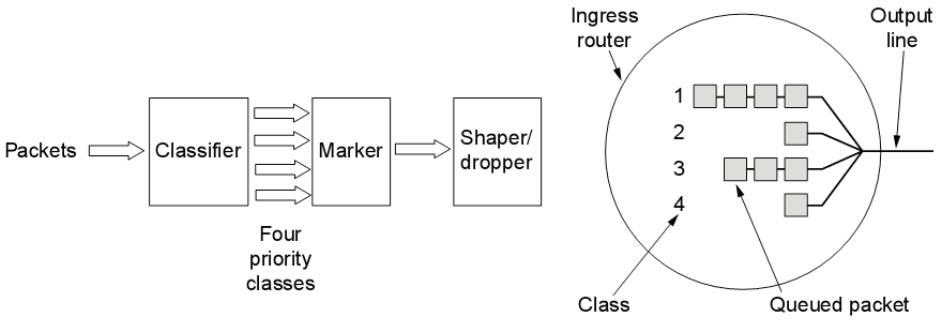


Figura 55. Encaminhamento garantido.

3.10.3 Multiprotocolo Label Switching (MPLS):

O MPLS separa plano de controle do plano de envio, definindo o envio de dados baseados em rótulos anexados aos pacotes. Os rótulos permitem múltiplas formas de roteamento, tal como as rotas explícitas *hop-by-hop*. Cada roteador Label Switching Router (LSR) mantém uma base de dados de envio que mapeia um par interface/rótulo de entrada a um par interface/rótulo de saída. O MPLS está sendo modificado para suportar outras tecnologias.

3.11 Interligação de redes

Até agora, estudamos uma única rede homogênea com os mesmos protocolos em cada camada. Mas essa é uma situação real?

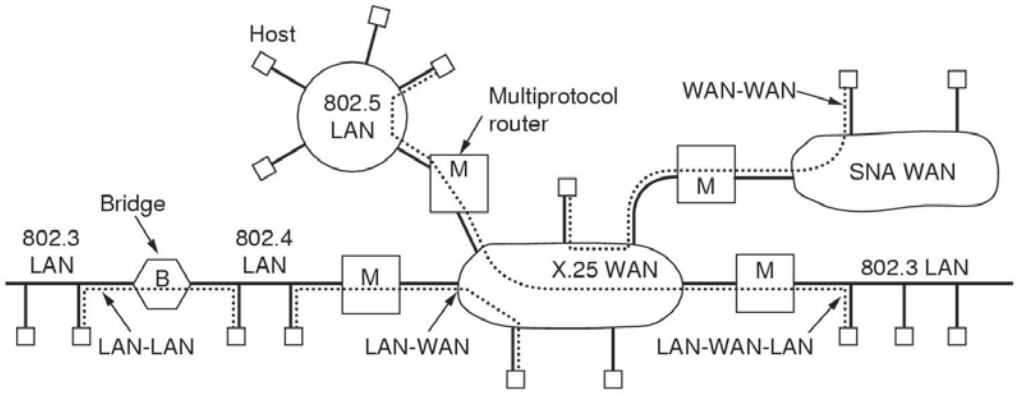


Figura 56. Interligação de redes;

A resposta para a pergunta anterior é que sempre haverá uma variedade de rede com características e protocolos distintos, pois a base instalada dos diferentes tipos de rede é muito grande. A finalidade de interconectar todas essas redes é permitir a comunicação entre seus usuários.

Tabela 6. Diferenças entre redes

Item	Algumas possibilidades
Serviço oferecido	Orientado à conexão e sem conexão
Protocolos	IP, IPX, Decnet etc.
Endereçamento	Simples (802) e hierárquico (IP)
Multicast	Presente ou ausente (também difusão)
Tamanho do pacote	Todas as redes têm seu próprio tamanho máximo
Qualidade do serviço	Pode estar presente ou ausente; muitos tipos diferentes
Tratamento de erros	Confiável, entrega com ou sem ordenação
Controle de fluxo	Janela deslizante, controle de taxa, outros ou nenhum
Controle de congestionamento	Balde furado, pacotes reguladores etc.
Segurança	Regras de privacidade, criptografia etc.
Parâmetros	Diferentes *timeouts*, especificações de fluxo etc.
Contabilidade	Por tempo de conexão, por pacote, por byte ou nenhuma

3.11.1 Conexões entre redes:

No caminho da origem até o destino podem ocorrer vários problemas: pacotes de uma rede orientada à conexão precisam passar por uma rede não

orientada à conexão (podem ser reordenados, por exemplo); conversões de protocolos, já que nem sempre existe a mesma funcionalidade; conversões de endereços; redes que não permitem *multicast*; diferença de tamanho máximo de pacote e garantia de tempo de entrega em redes que não possuem esse serviço.

Para a conexão entre redes, precisamos conhecer alguns nomes comuns dos equipamentos que realizam essa ligação:

- Na camada física, temos os repetidores que apenas amplificam ou regeneram o sinal;
- Na camada de enlace, temos as pontes (*bridges*) que podem encaminhar os quadros para uma rede diferente;
- Na camada de rede, temos os roteadores multiprotocolos que atuam de forma semelhante às *bridges*, mas atuam na camada de rede;
- Na camada de transporte, temos os *gateways* de transporte que estabelecem conexão entre duas redes na camada de transporte;
- Acima da camada de transporte, temos os *gateways* de aplicação. Por exemplo: o correio eletrônico.

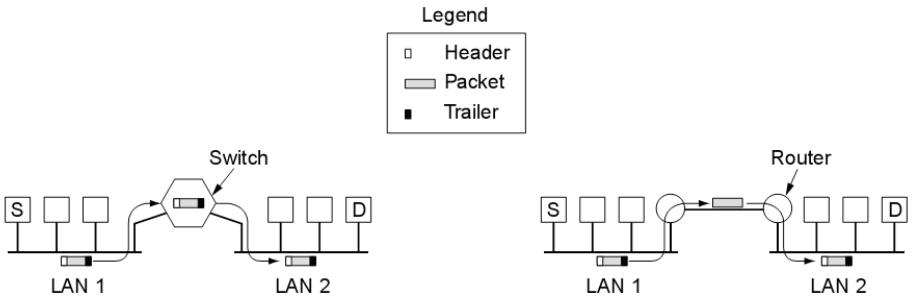


Figura 57. A máquina de origem S deseja enviar um pacote à máquina de destino D.

Com um *switch* ou uma ponte, o quadro inteiro é transportado de acordo com seu MAC. Não precisam ter o conhecimento dos protocolos usados para comutar pacotes. Com um roteador, o pacote é extraído do quadro e seu endereço é analisado para decidir qual caminho deve seguir. Precisam reconhecer o protocolo de cada rede que está sendo utilizado.

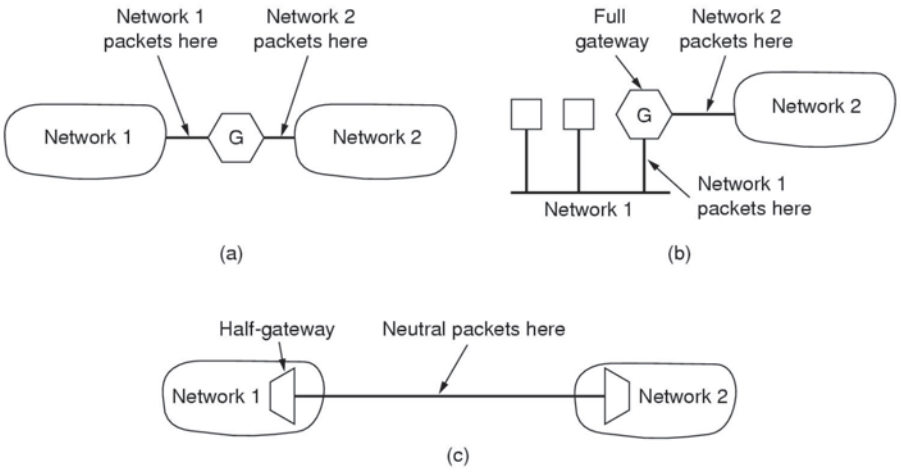


Figura 58. (a) um *gateway* completo entre 2 WAN; (b) um *gateway* entre uma LAN e uma WAN; (c) dois semi-*gateways*.

Quem gerencia o *gateway*? Essa situação é mais complicada na prática, onde muitos equipamentos misturam a funcionalidade de ponte e de roteador.

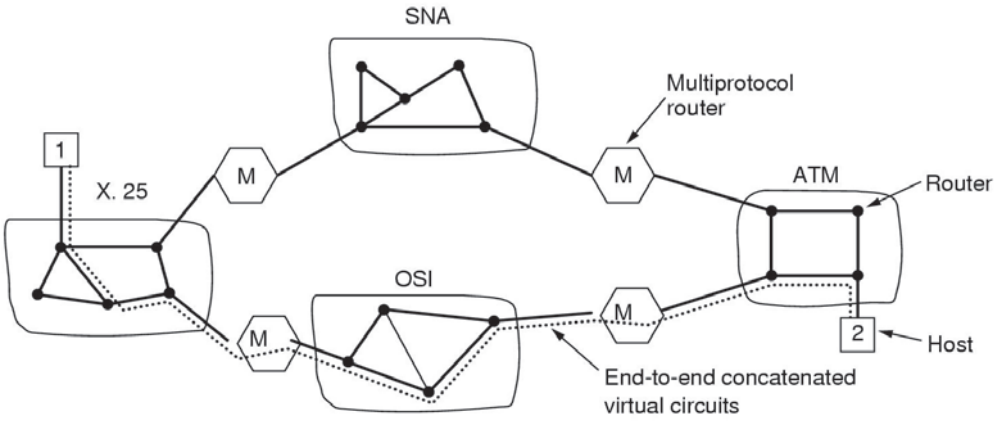


Figura 59. Ligação de inter-redes usando circuitos virtuais concatenados.

Nos circuitos virtuais concatenados, têm-se as vantagens: da reserva de *buffers* com antecedência, garantia da ordem de sequência na entrega dos pacotes; do uso de cabeçalhos mais curtos e da redução de problemas causados por pacotes atrasados e duplicados. Em contrapartida, apresentam algumas desvantagens, tais como: a necessidade de um espaço de tabela para cada conexão aberta e a inexistência de roteamento alternativo, pois, se um roteador cair, será necessário outro estabelecimento de circuito e, se uma rede for de datagrama, torna-se complicado implementar a ligação inter-redes via circuito virtual concatenado.

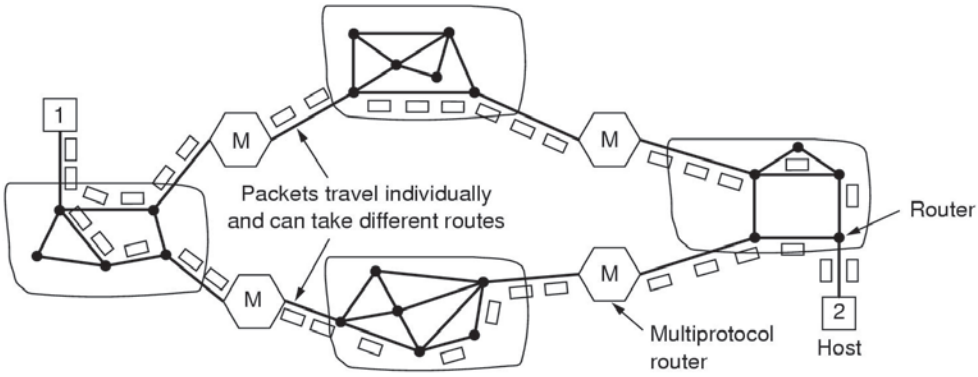


Figura 60. Ligação de inter-redes sem conexão.

Na ligação de inter-redes por datagrama, há um maior potencial para o congestionamento, um maior potencial para adaptação, uma maior robustez à falhas do roteador e uma maior necessidade de cabeçalhos mais longos. Uma inter-rede por datagrama pode conter vários algoritmos de roteamento adaptativos e pode ser usada em sub-redes que não implementam circuitos virtuais.

O único serviço que a camada de rede oferece à camada de transporte é o de envio de datagramas, mas essa não é uma tarefa trivial. Vejamos algumas situações: se cada rede possui seu próprio protocolo de camada de rede, não é possível que um pacote de uma rede transite por outra; como o endereçamento será tratado?; é preciso projetar um pacote inter-rede universal. O IP nasceu com essa ideia, mas como forçar todos a utilizarem o mesmo padrão?

Supondo que os *hosts* origem e destino tenham o mesmo tipo de rede e que há uma rede de outro tipo entre eles, pode-se aplicar uma técnica conhecida como tunelamento.

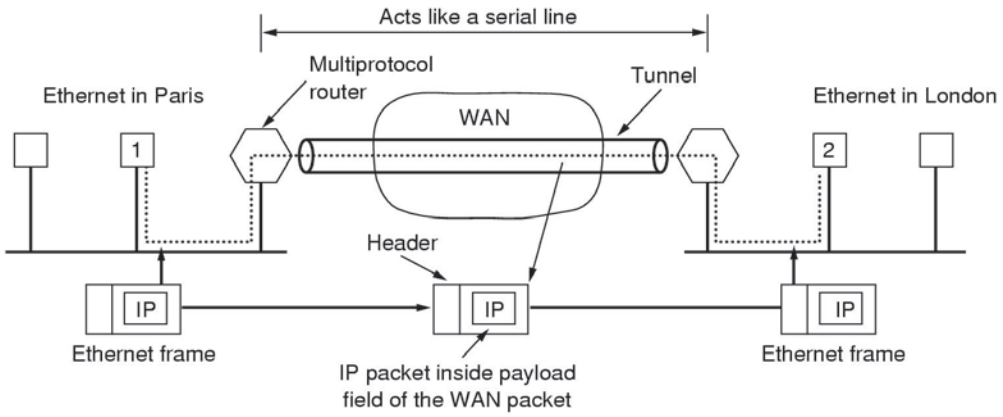


Figura 61. Tunelamento.

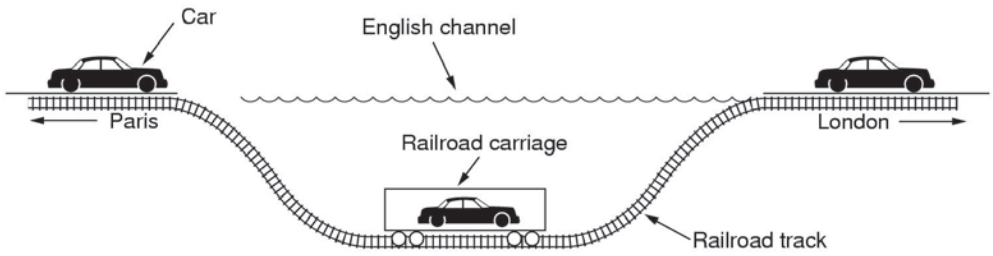


Figura 62. Tunelamento: analogia ao Euro-Túnel.

3.11.2 Roteamento inter-redes:

Em cada rede é utilizado um protocolo de *gateway* interno (interior *gateway* protocol). Entre as redes é utilizado um protocolo de *gateway* externo (exterior *gateway* protocol). Como todas as redes são independentes e podem utilizar diferentes algoritmos são chamadas de Sistemas Autônomos (Autonomous System – AS).

Fragmentação:

Ocorre limitação de tamanho máximo de pacote por várias causas:

- *Hardware* (exemplo: largura de um *slot* de transmissão);
- Sistema operacional (exemplo: *buffers* de 512bytes);
- Protocolos (exemplo: número de bits);
- Compatibilidade com algum padrão;
- Reduzir as retransmissões;
- Evitar que o pacote ocupe um canal por muito tempo.

A fragmentação é necessária quando os tamanhos de pacotes são diferentes para cada tipo de rede (48bytes (células ATM), 65515bytes (pacotes IP)). A primeira ideia para resolver esse problema foi não enviar nenhum pacote maior do que se pode tratar. Entretanto, os *gateways* podem dividir os pacotes em fragmentos e enviar como um pacote inter-rede separado. Para isso, existem duas possibilidades:

- Transparente: são remontados nos *gateways* intermediários e mais simples, mas têm algumas desvantagens:
  - O *gateway* que recebeu os fragmentos tem que saber que todos já chegaram e precisa conhecer o final de fragmento ou o número de fragmentos;
  - Todos os pacotes têm que passar pelo mesmo *gateway*;

- *Overhead* necessário para remontar e fragmentar um pacote grande repetidas vezes.

• Não transparente: remontado somente no destino. Pode usar vários *gateways*, mas tem algumas desvantagens:
  - Todos os *hosts* devem ter capacidade de remontar o pacote;
  - Se um pacote muito grande é fragmentado, o *overhead* do cabeçalho vai se propagar por toda a rede.

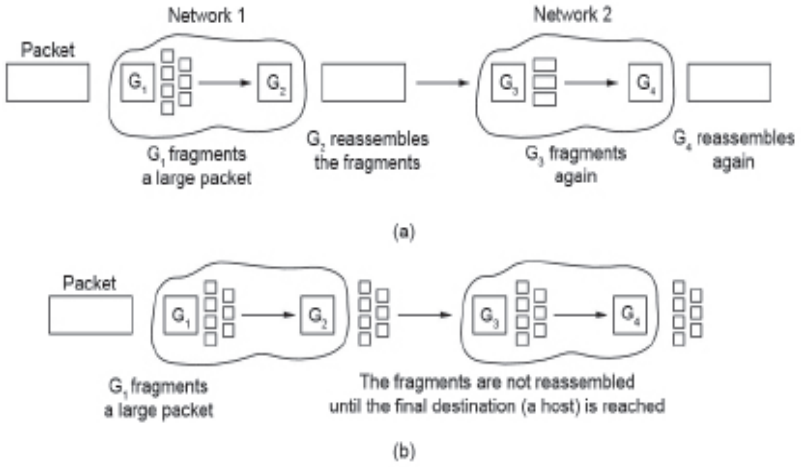


Figura 63. Fragmentação.

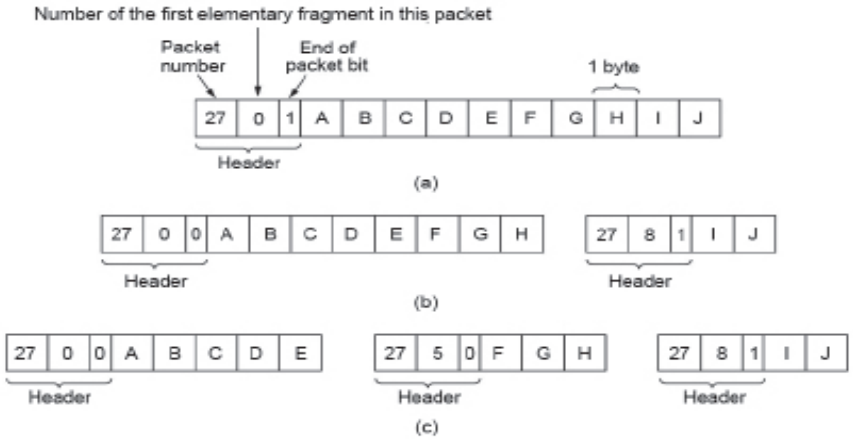


Figura 64. Processo de fragmentação.

Na figura 64 é apresentada uma fragmentação quando o tamanho de dados é de 1byte. Nesta figura (a) temos o pacote original, contendo 10bytes de dados; (b) temos os fragmentos depois da passagem por uma rede cujo tamanho de pacote máximo é 8bytes e (c) temos os fragmentos depois da passagem por *gateway* de tamanho 5.

Fragmentação e remontagem:

Cada rede tem um tamanho de Maximum Trasmit Unit (MTU) ou Unidade Máxima de Transmissão. Algumas decisões importantes de projeto são:

- Fragmente quando necessário (MTU < datagrama);
- Evite fragmentação no *host* de origem;
- Refragmente, se possível;
- Fragmentos são datagramas auto contidos;
- Adie a remontagem para o *host* de destino;
- Não recupere fragmentos perdidos.

3.12 Conclusões

Na camada de inter-rede, mostramos como a rede pode conhecer a topologia da rede (ou redes) e identificar os roteadores disponíveis para o melhor encaminhamento dos pacotes.

Nesta camada, alguns algoritmos de roteamento foram mostrados com o objetivo de compreender como as rotas adotadas pelos pacotes são aperfeiçoadas de forma a controlar o congestionamento nos roteadores.

Tratamos das redes de comutação de pacotes que operam nos modos datagrama e circuito virtual e analisamos o funcionamento da *internet* ao nível da camada de inter-rede, bem como abordamos alguns aspectos das redes de alta velocidade.

A essa altura da disciplina, temos condições de discutir sobre os aspectos relativos à tecnologia de redes desde os meios físicos de interconexão, as formas de enlace lógico entre os nodos (sejam hospedeiros de aplicações na borda da rede, fazendo acesso, sejam roteadores no núcleo, promovendo encaminhamento de pacotes) e até o roteamento de pacotes.

3.13 Referências

COMMER, D. *Redes de Computadores e Internet*, 2a ed. Bookman, 2001.

HUMMEL S. *Network Planning and Design Guide*, 1a ed. Design Series, 2005.

OLIFER, N.; OLIFER, V. *Redes de Computadores*: Princípio, Tecnologias e Protocolos para o Projeto de Redes. Tradução da 1a ed. LTC, 2008.

OPPENHEIMER, P. *Top-down Network Design*, 2a ed. Campus, 2004.

TANENBAUM, A. S. *Redes de Computadores*. Tradução da 4a ed. Rio de Janeiro: Campus, 2003.

STALLINGS, W. *Local & Metropolitan Area Networks*, 5a ed. Prentice Hall, 1997.

Este livro foi impresso pelo Departamento de Produção Gráfica – UFSCar.